FireSIGHT システム ユーザ ガイド

バージョン 5.4.1
2015 年 1 月 22日

Cisco Systems, Inc.
www.cisco.com
シスコは世界各国 200 箇所にオフィスを開設しています。
各オフィスの住所、電話番号、FAX 番号は当社の
Web サイト（www.cisco.com/go/offices）をご覧ください。

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

CONTENTS

CHAPTER 3

Cisco FireSIGHT システムの概要

Cisco FireSIGHT® システムは、専用プラットフォームで展開されるか、ソフトウェア ソリューションとして展開される、ネットワーク セキュリティおよびトラフィック管理製品の統合スイートです。

システムは、組織のセキュリティ ポリシー（ネットワークを保護するためのガイドライン）に準拠する方法でネットワーク トラフィックを処理できるように設計されています。セキュリティ ポリシーにはアクセプタブル ユース ポリシー（AUP）も含まれていることがあります。AUP は、組織のシステムの使用方法に関するガイドラインを従業員に提供します。

一般的な展開では、ネットワーク セグメントにインストールされた複数のトラフィック検知管理対象*デバイス*が分析対象のトラフィックをモニタし、管理を行う*Defense Center*® にレポートします。インライン展開の場合、デバイスがトラフィックのフローに影響を与える場合があります。

ヒント デバイスおよび Defense Center には複数のモデルがあります。管理対象デバイスには、物理および仮想 FirePOWER アプライアンス、Cisco NGIPS for Blue Coat X-Series、Cisco ASA with FirePOWER Services（ASA FirePOWER）が含まれます。Defense Center は、物理または仮想アプライアンスとして展開することもできます。必要に応じて、アプライアンス モデルはさらにシリーズおよびファミリに分類されます。通常、システム機能はモデルおよびライセンスによって異なります。

Defense Centerでは、集中管理コンソールの Web インターフェイスを使用して管理、分析、およびレポート タスクを実行できます。物理管理対象デバイスにも、初期セットアップ、基本的な分析と設定タスクを実行するために使用できる Web インターフェイスがあります。仮想管理対象デバイス、Cisco NGIPS for Blue Coat X-Series、および ASA FirePOWER デバイスには、FireSIGHT システムの Web インターフェイスがありません。これらのデバイスでは、管理を行う Defense Center を使用して実行できないタスクは CLI を使用して実行する必要があります。

このガイドでは、FireSIGHT システムの特徴と機能について説明します。各章の説明、図、および手順には、ユーザ インターフェイスをナビゲートする、システム パフォーマンスを最大にする、問題をトラブルシューティングする、といったことに役に立つ詳細な情報が記載されています。

以降のトピックでは、FireSIGHT システムの概要、主要なコンポーネント、およびこのマニュアルの使用方法について説明します。

- マニュアル リソース（1-20 ページ）
- 表記法（1-20 ページ）
- IP アドレスの表記規則（1-23 ページ）

管理対象デバイスの概要

ネットワーク セグメントにインストールされている管理対象デバイスは、分析のためにトラフィックを監視します。パッシブな展開の場合、管理対象デバイスは、ホスト、オペレーティング システム、アプリケーション、ユーザ、送信されたファイル（マルウェアを含む）、脆弱性など、組織の資産に関する詳細情報を収集します。FireSIGHT システムがこの情報を分析用に関連付けることで、ユーザがアクセスする Web サイトと使用するアプリケーションをモニタし、トラフィック パターンを評価して、侵入や他の攻撃の通知を受信できます。

インラインで展開されたシステムは、*アクセス コントロール*を使用してトラフィックのフローに影響を与えることができ、これによって、ネットワークに出入りしたり通過するトラフィックを処理する方法を詳細に指定することができます。ネットワーク トラフィックについて収集したデータおよびそのデータから収集したすべての情報は、次に基づいてそのトラフィックをフィルタ処理および制御するために使用できます。

- シンプルで容易に決定されるトランスポート層およびネットワーク層の特性（送信元と宛先、ポート、プロトコルなど）
- レピュテーション、リスク、ビジネスとの関連性、使用されたアプリケーション、または訪問した URL などの特性を含む、トラフィックに関する最新のコンテキスト情報
- 組織の Microsoft Active Directory LDAP ユーザ（ユーザごとに異なるアクセス レベルを付与できます）
- 暗号化されたトラフィックの特性（このトラフィックを復号化してさらに分析することもできます）
- 暗号化されていないトラフィックまたは復号化されたトラフィックに、禁止されているファイル、検出されたマルウェア、または侵入イベントが存在するかどうか

各タイプのトラフィックのインスペクションと制御は、最大限の柔軟性とパフォーマンスを得るのに最も有用である場合に行われます。たとえば、レピュテーション ベースのブラックリスト登録は、単純な送信元と宛先のデータを使用するため、プロセスの早期に禁止されたトラフィックをブロックできる一方で、侵入およびエクスプロイトの検出とブロックは最後の防衛ラインとなります。

アクセス コントロールに加えて、シリーズ 3 デバイスでネットワーク管理機能を使用すると、スイッチドおよびルーテッド環境での対応、ネットワーク アドレス変換（NAT）の実行が可能になります。また、設定した仮想ルータ間でセキュアなバーチャル プライベート ネットワーク（VPN）トンネルを構築できます。バイパス インターフェイス、集約インターフェイス、高速パス ルール、厳密な TCP の適用を設定することもできます。

詳細については、以下を参照してください。

- シリーズ 2 およびシリーズ 3 管理対象デバイス（1-3 ページ）
- 64 ビット仮想管理対象デバイス（1-3 ページ）
- Blue Coat X-Series 向け Cisco NGIPS（1-4 ページ）
- Cisco ASA with FirePOWER Services（1-4 ページ）
- Snort プロセスを再開する構成（1-8 ページ）
- Snort の再開によるトラフィックへの影響（1-9 ページ）

シリーズ 2 およびシリーズ 3 管理対象デバイス

Cisco FirePOWER 7000 シリーズ および 8000 シリーズのすべてのデバイスを含むシリーズ 3 デバイスは、FireSIGHT システム専用の物理デバイスの第 3 シリーズです。シリーズ 3 デバイスのスループットはさまざまですが、多数の同じ機能を共有します。一般に、8000 シリーズ デバイスは 7000 シリーズよりも高性能で、高速パス ルール、リンク集約、およびスタックなどの追加機能もサポートします。

Defense Centerとシリーズ 3 デバイスは、どちらもブランディング遷移中であることをご了承ください。Defense Center は FireSIGHT Management Center とも呼ばれ、シリーズ 3 デバイスは FirePOWER デバイスとも呼ばれます。Defense Center の製品識別番号は、DC ではなく FS で始まる場合があります。同様に、シリーズ 3 デバイスの製品識別番号は 3D ではなく FP で始まる場合があります。その他の点ではモデル番号の変更はありません。たとえば、DC4000 および FS4000 は同じ Defense Center を指します。

シリーズ 2 は物理管理対象デバイスの第 2 シリーズです。シリーズ 2 デバイスは、Protection ライセンスに関連する機能のほとんど（侵入検知と防御、ファイル制御、および単純なネットワーク ベースのアクセス制御）を自動的に保有します。

ただしリソースおよびアーキテクチャの制限により、シリーズ 2 デバイスは Protection ライセンスで使用できる機能の一部しかサポートしません。シリーズ 2 デバイスは、アーカイブ ファイル内にネストされたファイルに対して、セキュリティ インテリジェンス フィルタリングおよびファイル制御を実行できません。また、シリーズ 2 デバイスでは、FireSIGHT ライセンス付きの Defense Center を使用しても、位置情報ベースのアクセス制御を実行することはできません。シリーズ 2 デバイスでライセンスを取得した他の機能を有効にすることは**できません**。

Ciscoでは今後新しいシリーズ 2 アプライアンスを出荷しませんが、以前のバージョンのシステムを実行するシリーズ 2 デバイスをバージョン 5.4.1 に更新または再イメージ化することができます。再イメージ化によって、アプライアンスのほとんど**すべて**の設定とイベント データが消失することに注意してください。詳細については、『*FireSIGHT システム インストレーション ガイド*』を参照してください。

ヒント　バージョン 4.10.3 の配置環境からバージョン 5.2 の配置環境に特定の設定とイベント データを移行してから、バージョン 5.4.1 に更新できます。詳細については、バージョン 5.2 の『*FireSIGHT System Migration Guide*』を参照してください。

64 ビット仮想管理対象デバイス

VMware vSphere Hypervisor または VMware vCloud Director 環境を使用して ESXi ホストとして 64 ビット仮想デバイスを展開できます。サポート対象のすべての ESXi バージョンで VMware Tools を有効化できます。サポートされているバージョンのリストについては、『*FireSIGHT System Virtual Installation Guide*』を参照してください。VMware ツールのすべての機能については、VMware の Web サイト（http://www.vmware.com/）を参照してください。

仮想アプライアンスでは e1000（1 ギガビット/秒）インターフェイスが使用されますが、VMware vSphere Client を使用してデフォルトのセンシングおよび管理インターフェイスを vmxnet3（10 ギガビット/秒）インターフェイスに置き換えることもできます。また、VMware vSphere Client を使用して、仮想Defense Centerで追加の管理インターフェイスを作成できます。詳細については、『*FireSIGHT System Virtual Installation Guide*』を参照してください。

インストールおよび適用されているライセンスに関係なく、仮想アプライアンスはシステムのハードウェアベースの機能（冗長性、リソース共有、スイッチング、ルーティングなど）をサポートしません。また、仮想デバイスには FireSIGHT システムの Web インターフェイスがありません。

Blue Coat X-Series 向け Cisco NGIPS

Cisco NGIPS for Blue Coat X-Series を Blue Coat X-Series プラットフォームにインストールできます。このソフトウェア ベースのアプライアンスは、仮想管理対象デバイスと同じように機能します。インストールおよび適用されているライセンスに関係なく、Cisco NGIPS for Blue Coat X-Series は FireSIGHT システムの次の機能をサポートしません。

- Cisco NGIPS for Blue Coat X-Series は、高度なマルウェア対策（AMP）、アプリケーション制御、ユーザ制御、システムのハードウェアベースの機能（クラスタリング、スタッキング、スイッチング、ルーティング、VPN、NAT など）を含む、Malware または Control ライセンスで使用できる機能をサポートしません。
- Cisco NGIPS for Blue Coat X-Series を使用して、暗号化されたトラフィックを復号化または検査（SSL インスペクション）することはできません。
- Cisco NGIPS for Blue Coat X-Series を使用して、発信元または宛先の国や大陸に基づいてネットワーク トラフィックをフィルタ処理すること（位置情報ベースのアクセス コントロール）はできません。
- Defense Center Web インターフェイスを使用して、Cisco NGIPS for Blue Coat X-Series インターフェイスを設定することはできません。
- Defense Centerを使用して、Cisco NGIPS for Blue Coat X-Series プロセスをシャットダウン、再起動、その他の方法で管理することはできません。
- Defense Centerを使用して、Cisco NGIPS for Blue Coat X-Series のバックアップを作成/復元することはできません。
- Cisco NGIPS for Blue Coat X-Series にヘルス ポリシーやシステム ポリシーを適用することはできません。これには時刻設定の管理が含まれます。

Cisco NGIPS for Blue Coat X-Series には Web インターフェイスがありません。ただし、X-Series プラットフォームに固有のコマンド ライン インターフェイス（CLI）があります。この CLI を使用して、システムをインストールしたり、次のようなプラットフォーム固有の管理タスクを実行することができます。

- X-Series プラットフォームのロード バランシングと冗長性の利点（Ciscoの物理デバイス クラスタリングと同等）を活用できる Virtual Appliance Processor（VAP）グループの作成
- パッシブおよびインライン センシング インターフェイスの設定。インターフェイスの最大伝送ユニット（MTU）の設定を含みます。
- プロセスの管理
- NTP 設定を含む時刻設定の管理

Cisco ASA with FirePOWER Services

Cisco ASA with FirePOWER Services（ASA FirePOWER デバイス）は、管理対象デバイスと同様に機能します。この配置環境では、ASA デバイスは最も重要なシステム ポリシーを提供し、アクセス制御、侵入検知と防御、ディスカバリ、および高度なマルウェア対策のためにトラフィックを FireSIGHT システムに渡します。

インストールおよび適用されているライセンスに関係なく、ASA FirePOWER デバイスは FireSIGHT システムの次の機能をサポートしません。

- ASA FirePOWER デバイスは、FireSIGHT システムのハードウェアベースの機能（クラスタリング、スタッキング、スイッチング、ルーティング、VPN、NAT など）をサポートしません。ただし、ASA プラットフォームにはこれらの機能が備わっており、ASA CLI と ASDM を使ってこれらを設定できます。詳細については、ASA のマニュアルを参照してください。
- ASA FirePOWER デバイスは SSL 検査をサポートしません。
- Defense Centerの Web インターフェイスを使用して ASA FirePOWER のインターフェイスを設定することはできません。
- Defense Centerを使用して、ASA FirePOWER プロセスをシャットダウン、再起動、その他の方法で管理することはできません。
- Defense Centerを使用して、ASA FirePOWER デバイスのバックアップを作成/復元することはできません。
- VLAN タグ条件を使用してトラフィックを照合するアクセス コントロール ルールを作成することはできません。

ASA FirePOWER デバイスには、FireSIGHT Web インターフェイスがありません。ただし、ASA プラットフォームに固有のソフトウェアとコマンド ライン インターフェイス（CLI）があります。これらの ASA 固有のツールを使用して、システムをインストールしたり、プラットフォーム固有の他の管理タスクを実行したりすることができます。詳細については、ASA FirePOWER モジュールのドキュメントを参照してください。

スタンドアロン デバイスまたは管理対象デバイスとして ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5516-X、および ISA 3000 デバイスを管理できます。スタンドアロンの ASA FirePOWER モジュールは ASDM の ASA FirePOWER 構成で管理し、管理対象の ASA FirePOWER モジュールはDefense Centerで管理します。デバイスがDefense Centerに登録されている場合、ASA FirePOWER モジュールを ASDM で管理することはできません。

ASA FirePOWER デバイスを編集し、マルチ コンテキスト モードからシングル コンテキスト モード（またはその逆）に切り替えると、デバイスによってすべてのインターフェイスの名前が変更されることに注意してください。更新された ASA FirePOWER のインターフェイス名を使用する、すべての FireSIGHT システム セキュリティ ゾーン、相関ルール、および関連する設定の再設定が**必要**です。

注　Defense Centerでは、ASA FirePOWER デバイスが SPAN ポート モードで展開されている場合、ASA インターフェイスを表示しません。

Cisco ISA 3000

Cisco ISA 3000 はファイアウォール、脅威に対する防御、および VPN サービスを提供する、DIN レールに取り付ける高耐久性産業セキュリティ アプライアンスです。これはギガビット イーサネットと専用管理ポートを備えた、低消費電力、ファンなしのデバイスです。次の 2 つの SKU があります。

• Copper SKU（管理ポートの付いた 4x10/100/1000Base-T を装備）

• Fiber SKU（2x1GbE SFP および管理ポートの付いた 2x10/100/1000Base-T を装備）

Cisco ISA 3000 には、業界屈指の脅威と拡張マルウェア保護を組み合わせた Cisco ASA ファイアウォール保護が付属します。Cisco ISA 3000 は Cisco ASA with FirePOWER Services を実行します。詳細については、Cisco ASA with FirePOWER Services（1-4 ページ）を参照してください。

管理対象デバイスの各モデルでサポートされる機能の概要

バージョン 5.4.1 を実行している場合、FireSIGHT システム デバイスのスループットと機能はモデルおよびライセンスによって異なります。

Defense Centerとシリーズ 3 デバイスは、どちらもブランディング遷移中であることをご了承ください。Defense Centerは FireSIGHT Management Center とも呼ばれ、シリーズ 3 デバイスは FirePOWER デバイスとも呼ばれます。Defense Centerの製品識別番号は、DC ではなく FS で始まる場合があります。同様に、シリーズ 3 デバイスの製品識別番号は 3D ではなく FP で始まる場合があります。その他の点ではモデル番号の変更はありません。たとえば、DC4000 および FS4000 は同じDefense Centerを指します。

バージョン 5.4.1 デバイスの管理にはどのバージョン 5.4.1 Defense Centerでも使用できますが、DC500（および範囲がより狭い DC750 まで）がサポートする FireSIGHT システムの機能は制限されています。詳細については、Defense Centerの各モデルでサポートされる機能の概要（1-10 ページ）を参照してください。

次の表では、システムの主なアクセス制御機能とネットワーク管理機能を、それらの機能をサポートする管理対象デバイスおよび有効にする必要があるライセンスに対応付けています。これらの機能の簡単な説明は、FireSIGHT システムのコンポーネント（1-14 ページ）を参照してください。

表 1-1　各デバイス モデルでサポートされるアクセス制御機能

機能	シリーズ 2 デバイス	シリーズ 3 デバイス	ASA FirePOWER デバイス	仮想デバイス	X-Series デバイス	ライセンス
アクセス制御：基本的なネットワーク制御	yes	yes	VLAN 制御なし	yes	yes	いずれか
アクセス制御：リテラル URL	no	yes	yes	yes	yes	いずれか
アクセス制御：SSL インスペクション	no	yes	no	no	no	いずれか
ネットワーク検出：ホスト、ユーザ、アプリケーション	yes	yes	yes	yes	yes	FireSIGHT
アクセス制御：位置情報ベースのフィルタリング	no	yes	yes	yes	no	FireSIGHT
Security Intelligence フィルタリング	no	yes	yes	yes	yes	Protection
侵入検知および防御（IPS）	yes	yes	yes	yes	yes	Protection
ファイル制御：ファイル タイプ別	yes	yes	yes	yes	yes	Protection
ファイル制御：アーカイブ ファイルのインスペクション	no	yes	yes	yes	yes	Protection
高度なマルウェア防御（AMP）	no	yes	yes	yes	no	Malware
アクセス コントロール：アプリケーション制御	no	yes	yes	yes	no	Control

表 1-1　各デバイス モデルでサポートされるアクセス制御機能（続き）

機能	シリーズ 2 デバイス	シリーズ 3 デバイス	ASA FirePOWER デバイス	仮想デバイス	X-Series デバイス	ライセンス
アクセス コントロール:ユーザ制御	no	yes	yes	yes	no	Control
アクセス制御:カテゴリおよびレピュテーション別の URL フィルタリング	no	yes	yes	yes	yes	URL Filtering

表 1-2　各デバイス モデルでサポートされる管理およびネットワーク管理機能

機能	シリーズ 2 デバイス	シリーズ 3 デバイス	ASA FirePOWER デバイス	仮想デバイス	X-Series デバイス	ライセンス
トラフィック チャネル	no	yes	no	no	no	いずれか
複数の管理インターフェイス	no	yes	no	no	no	いずれか
リンク集約	no	yes	no	no	no	いずれか
FireSIGHT システム Web インターフェイス	limited	limited	no	no	no	いずれか
制限されたコマンドライン インターフェイス(CLI)	no	yes	yes	yes	no	いずれか
外部認証	yes	yes	no	no	no	いずれか
eStreamer クライアントへの接続	yes	yes	yes	no	no	いずれか
自動アプリケーション バイパス	yes	yes	yes	yes	no	いずれか
タップ モード	no	yes	no	no	no	いずれか
高速パス ルール	no	8000 シリーズ	no	no	no	いずれか
厳密な TCP 強制	no	yes	no	no	no	Protection
インライン セットのバイパス モード	yes	NetMod/SFP によって異なる	no	no	no	Protection
マルウェア ストレージ パック	no	yes	no	no	no	Malware
スイッチング、ルーティング、スイッチドおよびルーテッド集約インターフェイス	no	yes	no	no	no	Control
NAT ポリシー	no	yes	no	no	no	Control
デバイス スタック構成	no	3D8140 82xx ファミリ 83xx ファミリ	no	no	no	いずれか
デバイス クラスタリング	no	yes	no	no	X-Series ベース	Control（X-Seriesを除く）

表 1-2　各デバイス モデルでサポートされる管理およびネットワーク管理機能（続き）

機能	シリーズ 2 デバイス	シリーズ 3 デバイス	ASA FirePOWER デバイス	仮想デバイス	X-Series デバイス	ライセンス
クラスタ化スタック	no	3D8140 82xx ファミリ 83xx ファミリ	no	no	no	Control
VPN	no	yes	no	no	no	VPN

Snort プロセスを再開する構成

Snort® プロセスは、下記のいずれかの構成を適用すると、必ず再開されます。

注意　構成の一部を適用するときに、Snort プロセスの再開が要求され、これにより一時的にトラフィック検査が中断します。この中断中にトラフィックがドロップされるか、それ以上検査が行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

アクセス コントロール ポリシー

- 最初に管理対象デバイスにアクセス コントロール ポリシーを適用
- [Inspect Traffic During Policy Apply] を無効にしてアクセス コントロール ポリシーを適用
- 適応型プロファイルを有効化または無効化
- ファイルおよびマルウェアの詳細設定のデフォルト値を置換
- 右クリック メニューで [Whitelist Now] または [Blacklist Now] オプションを選択した場合を除き、セキュリティ インテリジェンス リストを変更
- SSL ポリシーをアクセス コントロール ポリシーに関連付けるか、または [None] を選択してポリシーの関連付けを後から解除
- 侵入ポリシーまたはファイル ポリシーをアクセス コントロール ポリシーに関連付けるか、または [None] を選択してポリシーの関連付けを後から解除
- 最初にカテゴリまたはレピュテーション URL 条件をアクセス コントロール ルールに追加
- [Default Network Analysis Policy] として選択または選択解除したカスタム ネットワーク分析ポリシーで、またはネットワーク分析ルールに関連付けまたは関連付け解除したカスタム ネットワーク分析ポリシーで、IMAP、POP、または SMTP プリプロセッサの [Base64 Decoding Depth]、[7-Bit/8-Bit/Binary Decoding Depth]、[Quoted-Printable Decoding Depth]、または [Unix-to-Unix Decoding Depth] の値を変更

ファイル ポリシー

- ファイルのアーカイブを有効化または無効化
- ファイル タイプまたはファイルのカテゴリをファイル ルールに追加、あるいはルールから削除
- ファイル ルール アクションを [Detect Files] または [Block Malware] に変更
- ファイル ルールで [Store Files] を有効化または無効化

デバイス管理

- センシング インターフェイスの MTU の値（シリーズ 2）または最高値（シリーズ 3）を変更

- VPN 展開を追加または変更
- ハイ アベイラビリティ状態の共有オプションの変更

システム更新

バイナリの変更を含むシステム更新プログラムまたはパッチをインストールします。バイナリの変更には、Snort、プリプロセッサ、または脆弱性データベース（VDB）に対する変更が含まれている場合があります。管理対象デバイスの場合は、バイナリの変更が含まれていないパッチを適用すると、Snort を再開しなければならないことがあります。

Snort の再開によるトラフィックへの影響

次の表に示すように、トラフィックに対する Snort の再開の影響は、管理対象デバイスのモデルおよびデバイスによるトラフィックの処理方法に応じて異なります。

表 1-3　再開によるトラフィックへの影響（管理対象デバイスのモデル別）

モデル	設定	再開中のトラフィック
シリーズ 2、シリーズ 3、仮想	インライン、Failsafe 有効または無効	検査なしで受け渡される*
	パッシブ	該当なし（ドロップされる）
3D9900、シリーズ 3	インライン、タップ モード	検査なしで受け渡される*
シリーズ 3	ルーテッド、スイッチド、透過	ドロップされる
ASA FirePOWER	フェールオープン（トラフィック許可）状態のルーテッドまたは透過	検査なしで受け渡される
	フェールクローズ（トラフィック クローズ）状態のルーテッドまたは透過	ドロップされる

*シリーズ 2 は、センシング インターフェイスで MTU を変更すると、トラフィックをドロップします。それ以外の場合は、トラフィックを検査なしで受け渡します。

Defense Centerの概要

Defense Centerは、FireSIGHT システム展開の集中管理コンソールおよびデータベース リポジトリを提供します。Defense Centerは、侵入、ファイル、マルウェア、ディスカバリ、接続、およびパフォーマンスのデータを集約して相互に関連付け、特定のホストに対するイベントの影響を評価し、ホストに侵害の痕跡を付けます。これにより、デバイス間で交わされる情報の監視、ネットワーク上で発生するアクティビティ全体の評価や制御が可能になります。Defense Centerは、デバイスのネットワーク管理機能（スイッチング、ルーティング、NAT、VPN など）も制御します。

Defense Centerの主な機能は次のとおりです。

- デバイス、ライセンス、ポリシーの管理
- テーブル、グラフ、チャートに表示されるイベント情報と状況情報
- ヘルスとパフォーマンスのモニタリング
- 外部通知とアラート

- リアルタイムに脅威に対処するための関連付け、侵害の痕跡、および修復機能
- カスタムおよびテンプレートベースのレポート
- 運用の継続性を確保するハイ アベイラビリティ（冗長性）機能

シリーズ 2 およびシリーズ 3 Defense Centerは、Ciscoが提供するフォールトトレラントな専用の物理ネットワーク アプライアンスです。VMware vSphere Hypervisor または VMware vCloud Director 環境を使用して ESXi ホストとして 64 ビット仮想Defense Centerを展開することもできます。Defense Centerは、すべてのタイプ（物理、仮想、Cisco ASA with FirePOWER Services、および Cisco NGIPS for Blue Coat X-Series）のデバイスを管理できます。

Defense Centerは、さまざまなデバイス管理、イベント保存、ホスト モニタリング、およびユーザ モニタリング機能を備えています。リソースおよびアーキテクチャの制限により、DC500（および範囲がより狭い DC750 まで）は FireSIGHT システム機能の一部しかサポートしないことに注意してください。

Defense Centerとシリーズ 3 デバイスは、どちらもブランディング遷移中であることをご了承ください。Defense Centerは FireSIGHT Management Center とも呼ばれ、シリーズ 3 デバイスは FirePOWER デバイスとも呼ばれます。Defense Centerの製品識別番号は、DC ではなく FS で始まる場合があります。同様に、シリーズ 3 デバイスの製品識別番号は 3D ではなく FP で始まる場合があります。その他の点ではモデル番号の変更はありません。たとえば、DC4000 および FS4000 は同じDefense Centerを指します。

注　Ciscoでは今後新しいシリーズ 2 Defense Centerを出荷しませんが、バージョン 5.4.1 に更新するか再イメージ化することができます。再イメージ化によって、アプライアンスのほとんど**すべて**の設定とイベント データが消失することに注意してください。詳細については、『*FireSIGHT システム インストレーション ガイド*』を参照してください。

Defense Centerの各モデルでサポートされる機能の概要

バージョン 5.4.1 を実行している場合、すべてのDefense Centerには、同様の機能がありますが、容量と速度が主な違いとなります。Defense Centerのモデルによって、管理できるデバイス数、保存できるイベント数、およびモニタできるホスト数とユーザ数が異なります。詳細については、以下を参照してください。

- デバイスの管理（4-1 ページ）
- データベース イベント制限の設定（63-16 ページ）
- FireSIGHTホストおよびユーザ ライセンスの制限について（65-9 ページ）

バージョン 5.4.1 デバイスの管理にはどのバージョン 5.4.1 Defense Centerでも使用できますが、DC500（および範囲がより狭い DC750 まで）がサポートする FireSIGHT システムの機能は制限されています。また、**デバイス**のライセンスおよびモデルによって多くのシステム機能が制限されます。管理対象デバイスの各モデルでサポートされる機能の概要（1-6 ページ）を参照してください。

DC 2000 および DC4000 では、Ciscoのユニファイド コンピューティング システム（UCS）プラットフォームが FireSIGHT システムに導入されます。DC2000 および DC4000 は、ベースボード管理コントローラ（BMC）上で UCS Manager や Cisco Integrated Management Controller（CIMC）などのツールを使用するCiscoの機能をサポートしないことに注意してください。次の表では、システムのアクセス制御およびネットワーク管理の主な機能に、それらの機能をサポートするDefense Centerおよび有効にする必要があるライセンスを対応付けます。これらの機能の簡単な説明は、FireSIGHT システムのコンポーネント（1-14 ページ）を参照してください。

表 1-4　Defense Centerの各モデルでサポートされるアクセス制御機能

機能	シリーズ 2 Defense Center	シリーズ 3 Defense Center	仮想 Defense Center	ライセンス
単純なネットワークベースのアクセス制御を実行するデバイスを管理する	yes	yes	yes	いずれか
リテラル(手動入力)URL 別の URL 制御を実行するデバイスを管理する	yes	yes	yes	いずれか
SSL インスペクションを実行するデバイスを管理する	yes	yes	yes	いずれか
管理対象デバイスから報告された検出データ(ホスト、アプリケーション、およびユーザ)を収集して、組織のネットワーク マップを作成する	yes	yes	yes	FireSIGHT
位置情報(国および大陸)データによる検出を強化し、位置情報ベースのアクセス制御を実行するデバイスを管理する	DC1000、DC3000	yes	yes	FireSIGHT
セキュリティ インテリジェンス フィルタリング(ブラックリスト登録)を実行するデバイスを管理する	DC1000、DC3000	yes	yes	Protection
侵入検知および防御(IPS)展開を管理する	yes	yes	yes	Protection
ファイル タイプによる単純なファイル制御を実行しているデバイスを管理する	yes	yes	yes	Protection
アーカイブ ファイルのインスペクションを実行するデバイスを管理する	DC1000、DC3000	yes	yes	Protection
アプリケーション制御を実行しているデバイスを管理する	yes	yes	yes	Control
ユーザ制御を実行するデバイスを管理する	DC1000、DC3000	yes	yes	Control
カテゴリおよびレピュテーション別の URL フィルタリングを実行するデバイスを管理する	DC1000、DC3000	yes	yes	URL フィルタリング
高度なマルウェア対策(AMP)の展開を管理し、マルウェア ストレージ パックをインストールする	DC1000、DC3000	yes	yes	Malware
FireAMP 展開からエンドポイントベースのマルウェア(FireAMP)イベントを受信する	yes	yes	yes	FireAMPサブスクリプション
eStreamer、ホスト入力、またはデータベース クライアントに接続する	yes	yes	yes	いずれか

表 1-5　Defense Centerの各モデルでサポートされるネットワーク管理および冗長性機能

機能	シリーズ 2 Defense Center	シリーズ 3 Defense Center	仮想 Defense Center	ライセンス
トラフィック チャネルを使用して内部トラフィックと外部トラフィックを分離および管理する	no	yes	yes	いずれか
複数の管理インターフェイスを使用して別々のネットワーク上のトラフィックを分離および管理する	no	yes	yes	いずれか
Defense Centerの冗長性（ハイ アベイラビリティ）を確立する	DC1000、DC3000	DC1500、DC2000、DC3500、DC4000	no	いずれか
デバイスベースの冗長性とリソース共有（スタック、クラスタ、およびクラスタ化スタック）を管理する	yes	yes	yes	Control
ハードウェア依存のネットワーク管理機能（高速パス ルール、厳密な TCP の適用、バイパス モード、タップ モード、スイッチングおよびルーティング、NAT、VPN）を使用してデバイスを管理する	yes	yes	yes	機能に応じて異なる

バージョン 5.4.X で提供されるDefense Centerとデバイス

次の表に、Ciscoがバージョン 5.4.X の FireSIGHT システムで提供するDefense Centerと管理対象デバイスを示します。

表 1-6　バージョン 5.4.1 FireSIGHT システムのDefense Centerおよびデバイス

モデル/ファミリ	シリーズ	タイプ	バージョン 5.4.x
70xx ファミリ： • 3D7010/7020/7030/7050	シリーズ 3 FirePOWER（7000 シリーズ）	デバイス	バージョン 5.4.0.x
71xx ファミリ： • 3D7110/7120 • 3D7115/7125 • AMP7150	シリーズ 3 FirePOWER（7000 シリーズ）	デバイス	バージョン 5.4.0.x
81xx ファミリ： • 3D8120/8130/8140 • AMP8150	シリーズ 3 FirePOWER（8000 シリーズ）	デバイス	バージョン 5.4.0.x
82xx ファミリ： • 3D8250 • 3D8260/8270/8290	シリーズ 3 FirePOWER（8000 シリーズ）	デバイス	バージョン 5.4.0.x

表 1-6　バージョン 5.4.1 FireSIGHT システムのDefense Centerおよびデバイス（続き）

モデル/ファミリ	シリーズ	タイプ	バージョン 5.4.x
83xx ファミリ： • 3D8350 • 3D8360/8370/8390 • AMP8350 • AMP8360/8370/8390	シリーズ 3 FirePOWER（8000 シリーズ）	デバイス	バージョン 5.4.0.x
64 ビット仮想デバイス	n/a	デバイス	バージョン 5.4.0.x
Cisco NGIPS for Blue Coat X-Series	n/a	デバイス	バージョン 5.4.0.x
ASA FirePOWER： • ASA5512-X • ASA5515-X • ASA5525-X • ASA5545-X • ASA5555-X • ASA5585-X-SSP-10 • ASA5585-X-SSP-20 • ASA5585-X-SSP-40 • ASA5585-X-SSP-60	n/a	デバイス	バージョン 5.4.0.x
ASA FirePOWER： • ASA5506-X • ASA5506H-X • ASA5506W-X • ASA5508-X • ASA5516-X • ISA 3000	n/a	デバイス	バージョン 5.4.1.x
シリーズ 3 Defense Center： • DC750/1500/3500 • DC2000/4000	シリーズ 3	Defense Center	バージョン 5.4.1.x
64 ビット仮想Defense Center	n/a	Defense Center	バージョン 5.4.1.x

Defense Centerとシリーズ 3 デバイスは、どちらもブランディング遷移中であることをご了承ください。Defense Centerは FireSIGHT Management Center とも呼ばれ、シリーズ 3 デバイスは FirePOWER デバイスとも呼ばれます。Defense Centerの製品識別番号は、DC ではなく FS で始まる場合があります。同様に、シリーズ 3 デバイスの製品識別番号は 3D ではなく FP で始まる場合があります。その他の点ではモデル番号の変更はありません。たとえば、DC4000 および FS4000 は同じDefense Centerを指します。

Ciscoは新しい シリーズ 2 アプライアンスを出荷しませんが、以前のバージョンのシステムを実行する シリーズ 2 デバイスおよびDefense Centerを バージョン 5.4.1 に更新または再イメージ化できます。再イメージ化によって、アプライアンスのほとんど**すべて**の設定とイベント データが消失することに注意してください。詳細については、『*FireSIGHT System Installation Guide*』を参照してください。

ヒント　バージョン 4.10.3 の配置環境からバージョン 5.2 の配置環境に特定の設定とイベント データを移行してから、バージョン 5.4.1 に更新できます。詳細については、バージョン 5.2 の『*FireSIGHT System Migration Guide*』を参照してください。

FireSIGHT システムのコンポーネント

以下のトピックでは、組織のセキュリティ、アクセプタブル ユース ポリシー、およびトラフィック管理戦略に役立つ FireSIGHT システムの主要機能の一部について説明します。

- 冗長性とリソース共有（1-14 ページ）
- ネットワーク トラフィック管理（1-15 ページ）
- FireSIGHT（1-16 ページ）
- アクセス コントロール（1-16 ページ）
- SSL インスペクション（1-17 ページ）
- 侵入検知と防御（1-17 ページ）
- 高度なマルウェア防御とファイル制御（1-18 ページ）
- アプリケーション プログラミング インターフェイス（1-19 ページ）

ヒント　FireSIGHT システムの多くの機能は、アプライアンス モデル、ライセンス、およびユーザ ロールに依存します。このマニュアルには、各機能に必要な FireSIGHT システムのライセンスとデバイス、および各手順を実行する権限を持つユーザ ロールに関する情報が含まれています。詳細については、表記法（1-20 ページ）を参照してください。

冗長性とリソース共有

FireSIGHT システムの冗長性とリソース共有の機能によって、運用の継続性を確保し、複数の物理デバイスの処理リソースを統合することができます。

Defense Centerのハイ アベイラビリティ

運用の継続性を確保するため、Defense Centerの*ハイ アベイラビリティ*機能によって、冗長なDC1000、DC1500、DC2000、DC3000、DC3500、または DC4000 Defense Centerを指定してデバイスを管理できます。イベント データは管理対象デバイスから両方のDefense Centerにストリームされ、特定の設定要素が両方のDefense Centerで保持されます。一方のDefense Centerで障害が発生した場合は、もう一方のDefense Centerを使用して中断することなくネットワークをモニタできます。

デバイス スタッキング

*デバイス スタッキング*によって、2 ～ 4 台の物理デバイスをスタック構成で接続し、ネットワーク セグメントで検査されるトラフィックの量を増やすことができます。スタック構成を確立すると、スタックに含まれる各デバイスのリソースが単一の共有設定に結合されることになります。

デバイス クラスタリング

デバイス クラスタリング(デバイスのハイ アベイラビリティとも呼ばれる)によって、2 台以上のシリーズ 3 デバイスまたはスタック間のネットワーキング機能と設定データの冗長性を確立できます。2 台以上のピア デバイスまたはスタックをクラスタ化すると、ポリシー適用、システム更新、および登録の対象となる単一の論理システムが生成されます。デバイス クラスタリングでは、システムを手動または自動でフェイルオーバーできます。

ほとんどの場合、SFRP を使用することによって、デバイスをクラスタ化せずにレイヤ 3 の冗長性を実現できます。SFRP を使用すると、デバイスは指定された IP アドレスに対する冗長ゲートウェイとして機能することが可能になります。ネットワークの冗長性によって、同じネットワーク接続を提供するように 2 台以上のデバイスまたはスタックを設定することで、ネットワーク上の他のホストに対する接続を確保できます。

Cisco NGIPS for Blue Coat X-Series によるロード バランシング

X-Series プラットフォーム上で複数メンバーからなる VAP グループ内の個々の VAP として Cisco NGIPS for Blue Coat X-Series を展開することで、X-Series プラットフォームのロード バランシングと冗長性の利点(Ciscoの物理デバイス クラスタリングと同等)を活用できます。その場合は、Defense Centerを使用してそれらの VAP グループを管理します。詳細については、『*Cisco NGIPS for Blue Coat X-Series Installation and Configuration Guide*』を参照してください。

ネットワーク トラフィック管理

FireSIGHT システムのネットワーク トラフィック管理機能によって、管理対象デバイスを組織のネットワーク インフラストラクチャの一部として機能させることができます。シリーズ 3デバイスを設定して、スイッチド、ルーテッド、またはハイブリッド(スイッチドおよびルーテッド)環境でのサービス提供、ネットワーク アドレス変換(NAT)の実行、およびセキュアなバーチャル プライベート ネットワーク(VPN)トンネルの構築を行うことができます。

スイッチング

レイヤ 2 配置では、2 つ以上のネットワーク セグメント間でパケット スイッチングを提供するように FireSIGHT システムを設定できます。レイヤ 2 配置では、スタンドアロン ブロードキャスト ドメインとして動作するようにスイッチド インターフェイスと管理対象デバイスの仮想スイッチを設定します。仮想スイッチは、ホストの MAC アドレスを使用してパケットの送信先を決定します。複数の物理インターフェイスを単一の論理リンクにグループ化することで、ネットワークの 2 つのエンドポイント間でパケット スイッチングが可能になります。エンドポイントは、2 台の FirePOWER 管理対象デバイス、またはサードパーティ アクセス スイッチに接続している 1 台の FirePOWER 管理対象デバイスである場合があります。

ルーティング

レイヤ 3 配置では、2 つ以上のインターフェイス間でトラフィックをルーティングするように FireSIGHT システムを設定できます。レイヤ 3 配置では、トラフィックを受信および転送するため、管理対象デバイスでルーテッド インターフェイスと仮想ルータを設定します。システムは宛先 IP アドレスに従ってパケット転送を決定し、パケットをルーティングします。ルータは転送基準に基づいて発信インターフェイスから宛先を取得し、適用するセキュリティ ポリシーはアクセス制御ルールによって指定されます。

仮想ルータを設定するときは、スタティック ルートを定義できます。さらに、ダイナミック ルーティング プロトコルとして Routing Information Protocol（RIP）および Open Shortest Path First（OSPF）を設定できます。スタティック ルートと RIP、またはスタティック ルートと OSPF を組み合わせて設定することもできます。ユーザが設定した仮想ルータごとに、DHCP リレーを設定できます。

Ciscoアプライアンスの設定で仮想スイッチと仮想ルータの両方を使用する場合は、それらの間のトラフィックをブリッジングするために関連するハイブリッド インターフェイスを設定できます。これらのユーティリティはトラフィックを分析して、トラフィックのタイプと適切な応答（ルーティング、スイッチング、その他）を特定します。複数の物理インターフェイスを単一の論理リンクにグループ化することで、ネットワークの 2 つのエンドポイント間でトラフィックがルーティングされます。エンドポイントは、2 台の FirePOWER 管理対象デバイス、またはサードパーティ ルータに接続している 1 台の FirePOWER 管理対象デバイスである場合があります。

NAT

レイヤ 3 配置では、ネットワーク アドレス変換（NAT）を設定できます。内部サーバを外部ネットワークに公開したり、内部ホストまたはサーバを外部アプリケーションに接続したりできます。また、IP アドレスのブロックを使用するか、または IP アドレスの制限付きブロックとポート変換を使用して、プライベート ネットワーク アドレスを外部ネットワークから隠蔽するように NAT を設定することもできます。

VPN

バーチャル プライベート ネットワーク（VPN）は、公開ソース（インターネットやその他のネットワーク）を介してエンドポイント間のセキュアなトンネルを確立するネットワーク接続です。シリーズ 3 デバイスの仮想ルータ間にセキュアな VPN トンネルを構築するように FireSIGHT システムを設定できます。

FireSIGHT

FireSIGHT™ はCiscoの検出および認識テクノロジーです。ユーザがネットワーク全体を把握できるように、ホスト、オペレーティング システム、アプリケーション、ユーザ、ファイル、ネットワーク、位置情報、および脆弱性に関する情報を収集します。

Defense Centerの Web インターフェイスを使用して、収集されたデータを表示および分析することができます。また、このデータを使用することで、アクセス コントロールを実施し、侵入ルールの状態を修正できます。さらに、ホストの相関イベント データに基づいてネットワーク上のホストに対する侵害の痕跡を生成し、追跡できます。

アクセス コントロール

*アクセス制御*はポリシーベースの機能で、ユーザはこれを使用してネットワークを横断できるトラフィックを指定、検査、および記録することが可能です。*アクセス制御ポリシー*は、システムがネットワーク上のトラフィックを処理する方法を決定します。

最も単純なアクセス コントロール ポリシーでは、*デフォルト アクション*を使用してすべてのトラフィックを処理するターゲット デバイスを指定します。このデフォルト アクションは、詳細な検査を行わずにすべてのトラフィックをブロックまたは信頼するように設定することも、侵入および検出データについてトラフィックを検査するように設定することもできます。

より複雑なアクセス コントロール ポリシーはセキュリティ インテリジェンス データに基づいてトラフィックをブラックリスト登録することができ、また、*アクセス コントロール ルール*を使用してネットワーク トラフィックのロギングおよび処理を細かく制御することができます。これらのルールは単純にすることも複雑にすることもでき、複数の基準を使用してトラフィックを照合および検査します。セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、およびユーザ別にトラフィックを制御できます。高度なアクセス コントロール オプションには、復号化、前処理、およびパフォーマンスが含まれます。

各アクセス コントロール ルールには*アクション*も含まれており、一致するトラフィックをモニタ、信頼、ブロック、または許可するかどうかを決定します。トラフィックを許可するときは、システムが侵入ポリシーまたはファイル ポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出る前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

SSL インスペクション

*SSL インスペクション*はポリシーベースの機能です。暗号化されたトラフィックを復号化せずに処理したり、暗号化されたトラフィックを復号化して詳細なアクセス制御検査を行ったりすることができます。トラフィックの復号化や詳細な分析を行わずに信頼できない暗号化トラフィックの送信元をブロックすることも、暗号化されたトラフィックを復号化する代わりにアクセス制御を使用して検査することもできます。

暗号化されたトラフィックをさらに調査するため、システムにアップロードした公開キー証明書とペア化された秘密キーを使用して、ネットワークを通過する暗号化トラフィックを復号化し、暗号化されていない場合と同様に復号化したトラフィックをアクセス制御によって検査できます。復号化されたトラフィックのポスト分析をブロックしない場合、トラフィックは再暗号化されて宛先ホストに渡されます。システムは、暗号化された接続に対応する際にその詳細をログに記録できます。

侵入検知と防御

侵入検知および侵入防御は、トラフィックが宛先に許可される前のシステムの最後の防御ラインです。*侵入ポリシー*は、アクセス コントロール ポリシーによって呼び出される侵入検知および侵入防御の設定の定義済みセットです。*侵入ルール*およびその他の設定を使用して、これらのポリシーはセキュリティ違反がないかトラフィックを検査し、インライン展開では、悪意のあるトラフィックをブロックまたは変更できます。

Cisco は、複数の侵入ポリシーを FireSIGHT システム と共に提供します。システムによって提供されるポリシーを使用して、Cisco 脆弱性調査チーム（VRT）のエクスペリエンスを活用することができます。これらのポリシーでは、VRT は侵入ルールおよびプリプロセッサ ルールの状態を設定し（有効または無効）、他の詳細設定の初期設定も提供します。ルールを有効にすると、システムはそのルールと一致するトラフィックに対する侵入イベントを生成します（そして場合によってブロックします）。

システムによって提供されるポリシーが組織のセキュリティのニーズに完全に対応していない場合は、カスタム ポリシーを作成することで、環境内のシステムのパフォーマンスを向上させ、ネットワーク上で発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューを提供できます。設定できるカスタム ポリシーを作成および調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

高度なマルウェア防御とファイル制御

マルウェアの影響を特定して軽減しやすくするため、FireSIGHT システムのファイル制御、ネットワーク ファイル トラジェクトリ、および高度なマルウェア対策の各コンポーネントによって、ネットワーク トラフィック内のファイル（マルウェア ファイル、アーカイブ ファイル内にネストされたファイルを含む）の伝送を検出、追跡、キャプチャ、分析、および必要に応じてブロックできます。

ファイル制御

*ファイル制御*によって、管理対象デバイスはユーザが特定のアプリケーション プロトコルを介して特定のタイプのファイルをアップロード（送信）またはダウンロード（受信）するのを検出してブロックできます。ファイル制御は、全体的なアクセス制御設定の一部として設定します。アクセス制御ルールに関連付けられたファイル ポリシーによって、ルールの条件を満たすネットワーク トラフィックが検査されます。

ネットワークベースの高度なマルウェア対策（AMP）

ネットワークベースの*高度なマルウェア対策*（AMP）によって、複数のファイル タイプのマルウェアに関してネットワーク トラフィックを検査できます。アプライアンスは、検出されたファイルをさらに分析するために、ハード ドライブまたは（モデルによっては）マルウェア ストレージ パックに保存することができます。

検出されたファイルは、保存済みかどうかに関係なく、ファイルの SHA-256 ハッシュ値を使用して単純な既知の性質の検索を行うために Collective Security Intelligence クラウド に送信できます。また、脅威スコアを算出する*動的分析*用にファイルを送信することもできます。このコンテキスト情報を使用して、特定のファイルをブロックまたは許可するようにシステムを設定できます。

マルウェア対策は、全体的なアクセス制御設定の一部として設定します。アクセス制御ルールに関連付けられたファイル ポリシーによって、ルールの条件を満たすネットワーク トラフィックが検査されます。

FireAMP 統合

FireAMP はCiscoのエンタープライズクラスの高度なマルウェア分析および防御ソリューションで、高度なマルウェアの発生、高度で継続的な脅威、および標的型攻撃を検出、認識、ブロックします。

組織に FireAMP のサブスクリプションがある場合は、個々のユーザが自分のコンピュータやモバイル デバイス（*エンドポイント*とも呼ばれる）に*FireAMP コネクタ*をインストールします。これらの軽量エージェントはCisco クラウドと通信し、さらにクラウドがDefense Centerと通信します。

組織のセキュリティ ポリシーで従来型クラウド サーバ接続の使用が許可されていない場合、Ciscoのプライベート オンプレミス クラウド ソリューションである、FireAMP Private Cloud を入手して設定できます。これは、圧縮された、パブリック Cisco クラウドのローカル バージョンとして機能する仮想マシンです。

Defense Centerをクラウドに接続するように設定した後でDefense Centerの Web インターフェイスを使用して、組織のエンドポイントでのスキャン、検出、および検疫の結果として生成されたエンドポイントベースのマルウェア イベントを表示することができます。また、Defense Center は FireAMP データを使用してホスト侵害の兆候を生成および追跡することに加えて、ネットワーク ファイル トラジェクトリを表示します。

FireAMP 展開を設定するには、*FireAMP ポータル*（http://amp.sourcefire.com/）を使用します。このポータルは、マルウェアをすばやく識別して検疫するのに役立ちます。感染を発生した時点で識別し、そのトラジェクトリを追跡し、その影響を把握し、適切な回復方法を習得できます。FireAMP を使用すると、カスタム保護の作成、グループ ポリシーに基づく特定のアプリケーションの実行のブロック、カスタム ホワイトリストの作成も可能です。

ネットワーク ファイル トラジェクトリ

ネットワーク ファイル トラジェクトリ機能によって、ネットワーク内のファイルの伝送パスを追跡できます。システムは SHA-256 ハッシュ値を使用してファイルを追跡します。このため、システムはファイルを追跡するために次のいずれかの処理を行う必要があります。

- ファイルの SHA-256 ハッシュ値を計算し、その値を使用してマルウェアのクラウド検索を実行する
- Defense Centerと組織の FireAMP サブスクリプションの統合を使用して、そのファイルに関するエンドポイントベースの脅威および検疫データを受信する

各ファイルには、ファイルの転送経過の視覚的表示とファイルに関する追加情報を含むトラジェクトリ マップが関連付けられています。

アプリケーション プログラミング インターフェイス

アプリケーション プログラミング インターフェイス（API）を使用してシステムとやりとりするには、いくつかの方法があります。詳細については、次のいずれかのサポート サイトから追加資料をダウンロードできます。

- **シスコ：**（http://www.cisco.com/cisco/web/support/index.html）

eStreamer

Event Streamer（eStreamer）を使用すると、Cisco アプライアンスからの数種類のイベント データを、カスタム開発されたクライアント アプリケーションにストリーム配信できます。作成したクライアント アプリケーションを eStreamer サーバ（Defense Centerまたは物理管理対象デバイス）に接続し、eStreamer サービスを起動してデータ交換を開始することができます。

eStreamer の統合では、カスタム プログラミングが必要になりますが、アプライアンスから特定のデータを要求することができます。たとえば、いずれかのネットワーク管理アプリケーション内でネットワーク ホストのデータを表示する場合は、Defense Centerからホストの重要度または脆弱性データを取得し、その情報を表示に追加するプログラムを作成できます。

外部データベースへのアクセス

データベース アクセス機能によって、JDBC SSL 接続をサポートするサードパーティ製クライアントを使用してDefense Center上の複数のデータベース テーブルを照会できます。

Crystal Reports、Actuate BIRT、JasperSoft iReport などの業界標準のレポート作成ツールを使用してクエリを作成し、送信することができます。または、Ciscoのデータを照会するように独自のカスタム アプリケーションを設定できます。たとえば、侵入とディスカバリのイベント データを定期的に報告するサーブレットや、アラート ダッシュボードを更新するサーブレットを構築できます。

ホスト入力

ホスト入力機能では、スクリプトまたはコマンドライン ファイルを使用してサードパーティのソースからデータをインポートすることにより、ネットワーク マップの情報を増やすことができます。

Web インターフェイスにもホスト入力機能があります。オペレーティング システムやアプリケーション プロトコルの ID の変更、脆弱性の有効化や無効化、およびネットワーク マップからの各種項目（クライアントとサーバ ポートを含む）の削除を行うことができます。

修復

システムには、ネットワークの状況が関連する相関ポリシーやコンプライアンスのホワイトリストに違反したときにDefense Centerが自動的に起動する*修復*を作成できる API が含まれています。これにより、ユーザが攻撃をただちに解決できないときに自動的に攻撃を軽減できるだけでなく、システムが組織のセキュリティ ポリシーに準拠し続けていることを確認することもできます。ユーザが作成した修復に加えて、Defense Centerには複数の事前定義された修復モジュールが付属しています。

マニュアル リソース

FireSIGHT システムのマニュアル セットには、オンライン ヘルプと PDF ファイルが含まれています。オンライン ヘルプには、Web インターフェイスから次のようにしてアクセスできます。

- 各ページの状況依存ヘルプ リンクをクリックする
- [Help] > [Online] を選択する

オンライン ヘルプには、Defense Centerまたはデバイスの Web インターフェイスを使用して実行できるタスク（システム管理、ポリシー管理、イベント分析を含む）に関する情報が含まれています。

PDF ドキュメントの最新バージョンには、次のいずれかのサポート サイトからアクセスできます。

- **シスコ：**（http://www.cisco.com/cisco/web/support/index.html）

そのようなドキュメントには、次のようなものがあります。

- *FireSIGHT システムユーザ ガイド*（オンライン ヘルプと同じ内容が含まれていますが、印刷が簡単な形式）
- *FireSIGHT System Installation Guide*（Cisco のアプライアンスをインストールするための情報、およびハードウェア仕様特有の情報と安全に関する情報が含まれる）
- *FireSIGHT System Virtual Installation Guide*（仮想デバイスおよび仮想Defense Centerのインストール、管理、およびトラブルシューティングに関する情報が含まれる）
- *Cisco NGIPS for Blue Coat X-Series Installation and Configuration Guide*（Cisco NGIPS for Blue Coat X-Series のインストール、管理、およびトラブルシューティングに関する情報が含まれる）
- 各種の API ガイドおよび補足資料

表記法

このドキュメントには、各機能に対して FireSIGHT システム のどのライセンスとアプライアンス モデルが必要か、各手順を完了するための権限を持っているのはどのユーザ ロールかについての情報が含まれています。詳細については、次の項を参照してください。

- ライセンスの表記規則（1-21 ページ）
- サポートされるデバイスとDefense Centerの表記規則（1-22 ページ）
- アクセスの表記規則（1-22 ページ）

ライセンスの表記規則

項の先頭に記載されているライセンス文は、この項に記載されている機能を使用するのに必要なライセンスを示しています。具体的なライセンスは次のとおりです。

FireSIGHT

FireSIGHT ライセンスはDefense Centerに含まれており、ホスト、アプリケーション、およびユーザ ディスカバリの実行に必要です。Defense CenterでのFireSIGHT ライセンスは、Defense Centerとその管理対象デバイスで監視可能なホストおよびユーザの数、ユーザ制御を実行ために使用可能なユーザの数を決定します。

Protection

Protectionライセンスでは、管理対象デバイスで侵入の検出および防御、ファイル制御、セキュリティ インテリジェンスのフィルタリングを実行することができます。このライセンスは、管理対象デバイスの購入時に自動的に付属する保護（TA）サブスクリプションに対応します。

Control

Controlライセンスでは、管理対象デバイスでユーザおよびアプリケーションの制御を実行することができます。また、デバイスがスイッチングおよびルーティング（DHCP リレーを含む）や NAT を実行したり、デバイスおよびスタックをクラスタ化したりできます。Controlライセンスにはは Protectionライセンスが必要です。このライセンスは、管理対象デバイスの購入時に自動的に付属します。

URL Filtering

URL Filtering ライセンスでは、管理対象デバイスが定期的に更新されるクラウドベースのカテゴリおよびレピュテーション データを使用して、監視対象ホストが要求した URL に基づいて、ネットワークを通貨できるトラフィックを判別できます。URL Filteringライセンスにはは Protectionライセンスが必要です。このライセンスは、保護（TAC または TAMC）と組み合わせたサービス サブスクリプションとして購入できます。また、保護（TA）が既に有効になっているデバイスの場合は、アドオン サブスクリプション（URL）として購入できます。

Malware

Malware ライセンスでは、管理対象デバイスがネットワークベースの高度なマルウェア防御（AMP）を実行できます。これは、ネットワーク上で転送されるファイルに含まれるマルウェアを検出、取得、およびブロックし、動的な分析のためにこれらのファイルを送信することができる機能です。また、ネットワーク上で転送されるファイルを追跡するトラジェクトリを表示することもできます。Malwareライセンスにはは Protectionライセンスが必要です。マルウェア ライセンスは、保護（TAM または TAMC）と組み合わせたサービス サブスクリプションとして購入できます。また、保護（TA）が既に有効になっているデバイスの場合は、アドオン サブスクリプション（AMP）として購入できます。

VPN

VPN ライセンスでは、Cisco の管理対象デバイスの仮想ルータ間で安全な VPN トンネルを構築することができます。VPN ライセンスにはは ProtectionおよびControlライセンスが必要です。VPN ライセンスを購入するには、販売担当者までお問い合わせください。

ライセンス付きの機能の多くは追加機能であるため、このドキュメントでは、各機能で最も必要なライセンスについてのみ記載しています。たとえば、ある機能で FireSIGHT、Protection、およびControlのライセンスが必要な場合、Controlのみが記載されています。

ライセンス文の「または」という語は、この項に記載されている機能を使用するには特定のライセンスが必要であるが、追加のライセンスで機能を追加することができることを示しています。たとえば、あるファイル ポリシーで、一部のファイル ルール アクションにはProtectionライセンスが必要であり、その他のファイル ルール アクションではMalware ライセンスが必要であるとします。この場合、そのファイル ルールの説明のライセンス文には、「ProtectionまたはMalware」と示されます。

アーキテクチャとリソースの制限により、すべての管理対象デバイスにすべてのライセンスが適用できるわけではないことに注意してください。一般に、デバイスがサポートしていない機能のライセンスは付与できません。管理対象デバイスの各モデルでサポートされる機能の概要（1-6 ページ）を参照してください。詳細については、ライセンスについて（65-1 ページ）を参照してください。

サポートされるデバイスとDefense Centerの表記規則

項の先頭に記載されているサポートされるデバイス文は、ある機能が特定のデバイス シリーズ、ファミリ、またはモデルでのみサポートされていることを示しています。たとえば、スタッキングは シリーズ 3 のデバイスでのみサポートされています。項にサポートされるデバイス文が記載されていない場合は、機能がすべてのデバイスでサポートされているか、またはその項が管理対象デバイスに適用されないことを表しています。

このリリースでサポートされているプラットフォームの詳細については、Defense Centerの概要（1-9 ページ）を参照してください。

アクセスの表記規則

このドキュメントの各手順の先頭に記載されているアクセス文は、手順の実行に必要な事前定義のユーザ ロールを示しています。複数のロールを区切るスラッシュは、記載されているどのロールでも手順を実行できることを示しています。次の表は、アクセス文で使用される共通の用語について定義しています。

表 1-7　アクセスの表記規則

アクセスの用語	意味
Access Admin	ユーザは Access Control Admin ロールを持っている必要がある
Admin	ユーザは Administrator ロールを持っている必要がある
いずれか	ユーザはいずれのロールを持っていてもよい
Any/Admin	ユーザはいずれのロールを持っていてもよいが、Administrator ロールのみが無制限のアクセス権を持つ（プライベートとして保存された他のユーザのデータを参照できるなど）
Any Security Analyst	ユーザは、Security Analyst または Security Analyst（読み取り専用）のロールのいずれかを持つことができる
データベース	ユーザは External Database ロールを持っている必要がある
Discovery Admin	ユーザは Discovery Admin ロールを持っている必要がある
Intrusion Admin	ユーザは Intrusion Admin ロールを持っている必要がある
Maint	ユーザは Maintenance User ロールを持っている必要がある
Network Admin	ユーザは Network Admin ロールを持っている必要がある

表 1-7　アクセスの表記規則（続き）

アクセスの用語	意味
Security Analyst	ユーザは Security Analyst ロールを持っている必要がある
Security Approver	ユーザは Security Approver ロールを持っている必要がある

カスタム ロールを持っているユーザは、事前定義されたロールとは異なる権限セットを持つことができます。事前定義のロールを使用して、ある手順に対するアクセス要件を示す場合は、類似の権限を持つカスタム ロールもアクセス権限を持っています。カスタム ロールを持っているユーザは、設定ページにアクセスするために使用するメニュー パスが若干異なる場合があります。たとえば、侵入ポリシー権限のみを付与されたカスタム ロールを持つユーザは、アクセス コントロール ポリシーを使用する標準パスではなく侵入ポリシーを経由してネットワーク分析ポリシーにアクセスします。カスタム ユーザ ロールの詳細については、カスタム ユーザ ロールの管理（61-55 ページ）を参照してください。

IP アドレスの表記規則

IPv4 Classless Inter-Domain Routing（CIDR）の表記、および IPv6 の類似のプレフィックス長の表記を使用して、FireSIGHT システム の多数の個所におけるアドレス ブロックを定義することができます。

CIDR 表記は、ネットワーク IP アドレスとビット マスクを組み合わせて使用し、指定されたアドレス ブロック内の IP アドレスを定義します。たとえば次の表に、プライベート IPv4 アドレス空間を CIDR 表記で示します。

表 1-8　CIDR 表記の構文例

CIDR ブロック	CIDR ブロックの IP アドレス	Subnet Mask	IP アドレスの数
10.0.0.0/8	10.0.0.0 - 10.255.255.255	255.0.0.0	16,777,216
172.16.0.0/12	172.16.0.0 - 172.31.255.255	255.240.0.0	1,048,576
192.168.0.0/16	192.168.0.0 - 192.168.255.255	255.255.0.0	65,536

同様に、IPv6 はネットワーク IP アドレスとプレフィックス長を組み合わせて使用し、指定されたブロック内の IP アドレスを定義します。たとえば 2001:db8::/32 は、プレフィックス長が 32 ビットの 2001:db8:: ネットワーク内の IPv6 アドレスを表します。つまり、2001:db8:: ～ 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff を表します。

CIDR またはプレフィックス長の表記を使用して IP アドレスのブロックを指定する場合、FireSIGHT システム は、マスクまたはプレフィックス長で指定されたネットワーク IP アドレスの部分**のみ**を使用します。たとえば、10.1.2.3/8 と入力した場合、FireSIGHT システム では 10.0.0.0/8 が使用されます。

つまり Cisco は、CIDR またはプレフィックス長の表記を使用する場合に、ビット境界上でネットワーク IP アドレスを使用する標準の方法を推奨していますが、FireSIGHT システム ではこれは必要ありません。

FireSIGHT システムへのログイン

この章では、FireSIGHT システムへのログインおよびログアウトのために、アプライアンスベースの Web インターフェイスおよびコマンドライン インターフェイス（CLI）を使用して実行する必要がある手順について説明します。また、LDAP または RADIUS クレデンシャルを使用する外部で認証されるユーザ アカウントを設定することもできます。

Web インターフェイスにログインした後、特定の領域の上にポインタを置くと、*コンテキスト メニュー*の機能によって追加情報および有益なナビゲーション リンクが提供されます。

詳細については、次の項を参照してください。

アプライアンスへのログイン

ライセンス： すべて

FireSIGHT システムDefense Centerには、管理および分析タスクを実行するために使用できる Web インターフェイスがあります。物理管理対象デバイスにも、初期セットアップ、基本的な分析と設定タスクを実行するために使用できる Web インターフェイスがあります。ブラウザ要件の詳細については、このバージョンの FireSIGHT システムのリリース ノートを参照してください。

仮想管理対象デバイスには、Web インターフェイスがありません。これらのデバイス（シリーズ 3 デバイスも同様）では、デバイスの管理Defense Centerを使用して完了できないすべてのタスクを実行するために使用できるインタラクティブ CLI が FireSIGHT システムによって提供されます。

Cisco NGIPS for Blue Coat X-Series にも Web インターフェイスはありません。ただし、X-Series プラットフォームに固有の CLI があります。この CLI を使用して、システムをインストールしたり、その他のプラットフォーム固有の管理タスクを実行したりします。X-Series プラットフォーム CLI へのログイン方法を含む詳細については、『*Cisco NGIPS for Blue Coat X-Series Installation and Configuration Guide*』を参照してください。

ASA FirePOWER デバイスには、独自の管理アプリケーション（ASDM と CSM）と ASA デバイスを設定するための CLI があります。また、FireSIGHT システムでは、デバイスの管理Defense Center で実行できないタスクを実行するために使用できるインタラクティブ CLI が提供されます。ASA 固有のツールを使用して、システムをインストールしたり、その他のプラットフォーム固有の管理タスクを実行したりします。詳細については、ASA のマニュアルを参照してください。

注　FirePOWER アプライアンスはユーザ アカウントに基づいてユーザ アクティビティを監査するため、ユーザが正しいアカウントでシステムにログインしていることを確認してください。

ユーザ名とパスワードを入力して、アプライアンスの Web インターフェイス、CLI、またはシェルへのアクセスを取得する必要があります。アプライアンスにログインすると、アクセスできる機能はユーザ アカウントに付与されている特権によって制御されます。詳細については、ユーザ アカウントの管理（61-46 ページ）を参照してください。

組織が認証に共通アクセス カード（CAC）を使用している場合は、CAC クレデンシャルを使用してアプライアンスの Web インターフェイスにアクセスすることもできます。CAC 認証および許可の詳細については、CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。

注意　クレデンシャルを間違えて複数回指定すると、シェル アクセス アカウントがロックされることがあります。正しいクレデンシャルを入力してもログインが拒否される場合、ログインを繰り返し試行せずに、システム管理者に連絡してください。

Web セッション中に初めてアプライアンスのホーム ページにアクセスする際、そのアプライアンスでの前回のログイン セッションに関する情報を表示できます。前回のログインに関する以下の情報を表示できます。

- ログインの曜日、月、日、年
- ログイン時のアプライアンスのローカル時間（24 時間表記）
- アプライアンスにアクセスするため最後に使用されたホストおよびドメイン名

セッション タイムアウトが適用されないように設定しない限り、デフォルトでは、非アクティブな状態が 1 時間続くとセッションは自動的にログアウトします。管理者ロールを持つユーザは、システム ポリシーのセッション タイムアウト間隔を変更できます。詳細については、ユーザ ログイン設定の管理（61-51 ページ）およびユーザ インターフェイスの設定（63-30 ページ）を参照してください。

かなり多くの時間がかかる一部のプロセスでは、Web ブラウザに、スクリプトが応答不能になったことを示すメッセージが表示されることがあります。このメッセージが表示された場合は、スクリプトが完了するまで続行させます。

注　アプライアンスにシステムを新規インストール（新規または再イメージング）する場合、管理（admin）ユーザ アカウントを使用してログインし、初期セットアップ プロセスを完了する必要があります。『*FireSIGHT System Installation Guide*』を参照してください。新しいユーザ アカウントの追加（61-47 ページ）の説明に従って他のユーザ アカウントを作成した後は、そのユーザも他のユーザもそれらのアカウントを使用して Web インターフェイスにログインする必要があります。

ヒント　ネットワークのユーザが CAC クレデンシャルを使用して [CAC Login] ページにログインできるようにするには、CAC 認証および許可を設定する**必要があります**。詳細については、CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。

Web インターフェイスを介して、アプライアンスにログインする方法：

アクセス： すべて

ステップ 1　ブラウザで `https://hostname/` にアクセスします。ここで、*hostname* はアプライアンスのホスト名です。

[Login] ページが表示されます。

ステップ 2　[Username] および [Password] フィールドにユーザ名とパスワードを入力します。ユーザ名は、大文字と小文字が区別されます。

組織でログイン時に SecurID® トークンが使用されている場合、ログインするには SecurID PIN にトークンを付加してパスワードとして使用します。たとえば PIN が `1111` で、SecurID トークンが `222222` の場合は、`1111222222` と入力します。FireSIGHT システムにログインする前に、SecurID PIN を生成しておく必要があります。

ステップ 3　[Login] をクリックします。

デフォルトの開始ページが表示されます。ユーザ アカウントにカスタム ホーム ページを選択した場合、そのページが代わりに表示されます。詳細については、「ホーム ページの指定（71-3 ページ）」を参照してください。

ヒント　Web インターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらうか、管理者アクセス権を持つユーザーとしてログインし、アカウントの特権を変更します。詳細については、ユーザ特権とオプションの変更（61-58 ページ）を参照してください。

ページの上部に表示されるメニューおよびメニュー オプションは、自分のユーザ アカウントの特権に基づきます。ただし、デフォルト ホーム ページのリンクには、ユーザ アカウントの特権の範囲全体にわたるオプションが含まれます。アカウントに付与された特権とは異なる特権を必要とするリンクをクリックした場合、次の警告メッセージが表示されます。

```
You are attempting to view an unauthorized page.This activity has been logged.
```

選択可能なメニューから別のオプションを選択するか、またはブラウザ ウィンドウで [Back] をクリックして前のページに戻ります。

CAC クレデンシャルを使用して Web インターフェイスを介してアプライアンスにログインする方法：

アクセス： すべて

ステップ 1　組織の指示に従って CAC を挿入します。

ステップ 2　ブラウザで `https://hostname/` にアクセスします。ここで、*hostname* はアプライアンスのホスト名です。

ステップ 3　プロンプトが表示されたら、手順1で挿入した CAC に関連付けられた PIN を入力します。

PIN が受け入れられます。

ステップ 4　プロンプトが表示されたら、ドロップダウン リストから該当する証明書を選択します。

ブラウザが選択内容を受け入れると、[CAC Login page] ページが表示されます。

ステップ 5　CAC クレデンシャルを使用して認証するには、[Continue] をクリックします。

ユーザ名とパスワードを使用して認証するには、[Username] と [Password] フィールドにそれらを入力します。ユーザ名は、大文字と小文字が区別されます。

デフォルトの開始ページが表示されます。ユーザ アカウントにカスタム ホーム ページを選択した場合、そのページが代わりに表示されます。詳細については、「ホーム ページの指定（71-3 ページ）」を参照してください。

ヒント Web インターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらうか、管理者アクセス権を持つユーザーとしてログインし、アカウントの特権を変更します。詳細については、ユーザ特権とオプションの変更（61-58 ページ）を参照してください。

ページの上部に表示されるメニューおよびメニュー オプションは、自分のユーザ アカウントの特権に基づきます。ただし、デフォルト ホーム ページのリンクには、ユーザ アカウントの特権の範囲全体にわたるオプションが含まれます。アカウントに付与された特権とは異なる特権を必要とするリンクをクリックした場合、次の警告メッセージが表示されます。

```
You are attempting to view an unauthorized page.This activity has been logged.
```

選択可能なメニューから別のオプションを選択するか、またはブラウザ ウィンドウで [Back] をクリックして前のページに戻ります。

注 ブラウズ セッションがアクティブな間は、CAC を削除**しない**でください。セッション中に CAC を置換または削除すると、Web ブラウザはセッションを終了し、システムによって Web インターフェイスからログアウトされます。

コマンド ライン経由で シリーズ 3、仮想デバイス、または ASA FirePOWER にログインする方法：

アクセス： CLI 基本設定

ステップ 1 シリーズ 3 および仮想デバイスの場合、*hostname* でアプライアンスへの SSH 接続を開きます。ここで、*hostname* はアプライアンスのホスト名です。ASA FirePOWER デバイスの場合、管理アドレスで ASA FirePOWER モジュールへの SSH 接続を開きます。

[login as:] コマンド プロンプトが表示されます。

ステップ 2 ユーザー名を入力し、Enter キーを押します。

[Password:] プロンプトが表示されます。

ステップ 3 パスワードを入力し、Enter キーを押します。

組織でログイン時に SecurID® トークンが使用されている場合、ログインするには SecurID PIN にトークンを付加してパスワードとして使用します。たとえば PIN が `1111` で、SecurID トークンが `222222` の場合は、`1111222222` と入力します。FireSIGHT システムにログインする前に、SecurID PIN を生成しておく必要があります。

ログイン バナーが表示され、その後に `>` プロンプトが表示されます。

コマンドライン アクセスのレベルによって許可されるコマンドを使用できます。使用可能な CLI コマンドの詳細については、コマンドライン リファレンス（D-1 ページ）を参照してください。

アプライアンスからのログアウト

ライセンス： すべて

Ciscoは、もう Web インターフェイスを使用しなくなったときにはログアウトすることを推奨します。これは、短時間 Web ブラウザから離れる場合でもです。ログアウトすることによって Web セッションは終了し、誰もそのクレデンシャルでアプライアンスを使用できなくなります。

セッション タイムアウトが適用されないように設定しない限り、デフォルトでは、非アクティブな状態が 1 時間続くとセッションは自動的にログアウトします。管理者ロールを持つユーザは、システム ポリシーのセッション タイムアウト間隔を変更できます。詳細については、ユーザ ログイン設定の管理（61-51 ページ）およびユーザ インターフェイスの設定（63-30 ページ）を参照してください。

アプライアンスからログアウトする方法：

アクセス： すべて

ステップ 1　ツールバーの [Logout] をクリックします。

コンテキスト メニューの使用

ライセンス： 機能によって異なる

操作の利便性を高めるため、Web インターフェイスのいくつかのページではポップアップ コンテキスト メニューをサポートしています。これは、FireSIGHT システムの他の機能にアクセスする際のショートカットとして使用できます。メニューの内容は、*ホットスポット*（アクセスする場所で、ページだけでなく特定のデータも含まれます）によって異なります。

たとえば、イベント ビュー、侵入イベントのパケット ビュー、ダッシュボード、および Context Explorer における *IP アドレスのホットスポット*では、追加オプションが提供されます。ホットスポットを右クリックして IP アドレスのコンテキスト メニューを使用し、そのアドレスに関連付けられたホストについて詳細を調べます。これには、使用可能な whois およびホスト プロファイル情報も含まれます。セキュリティ インテリジェンス フィルタリングをサポートしていない DC500 Defense Center以外では、個々の IP アドレスをセキュリティ インテリジェンスのグローバル ホワイトリストまたはブラックリストに追加することもできます。

別の例として、イベント ビューおよびダッシュボードの *SHA-256 値のホットスポット*によって、ファイルの SHA-256 ハッシュ値をクリーン リストまたはカスタム検出リストに追加するか、コピーするためにハッシュ値全体を表示することができます。この機能も、DC500 Defense Center ではサポートされないことに注意してください。

以下のリストは、Web インターフェイスのさまざまなページのコンテキスト メニューで利用できるオプションについて説明します。Cisco コンテキスト メニューがサポートされていないページまたは場所では、ブラウザの標準のコンテキスト メニューが表示されます。

アクセス コントロール、SSL、および NAT ポリシー エディタ

アクセス コントロール、SSL、および NAT ポリシー エディタには、各ルール上のホットスポットが含まれます。コンテキスト メニューを使用して、新しいルールとカテゴリの挿入、ルールの切り取り、コピー、貼り付け、ルール状態の設定、およびルールの編集を実行できます。

侵入ルール エディタ

侵入ルール エディタには、各侵入ルール上のホットスポットが含まれます。コンテキスト メニューを使用して、ルールの編集、ルール状態の設定（ルールの無効化を含む）、しきい値と抑制オプションの設定、およびルール ドキュメントの表示を実行できます。

Event Viewer

イベント ページ（ドリルダウン ページとテーブル ビュー）には、各イベント、IP アドレス、および特定の検出ファイルの SHA-256 ハッシュ値のホットスポットが含まれます。ほとんどのイベント タイプについて、コンテキスト メニューを使用して、Context Explorer に関連情報を表示したり、新しいウィンドウにイベント情報をドリルダウンしたりできます。イベント フィールドにすべてを表示するには長すぎるテキスト（SHA-256 のハッシュ値、脆弱性に関する説明、URL など）が含まれる場所では、コンテキスト メニューを使用してテキスト全体を表示することができます。

キャプチャしたファイル、ファイル イベント、およびマルウェア イベントの場合、コンテキスト メニューを使用して、クリーン リストまたはカスタム検出リストでのファイルの追加または削除、ファイルのコピーのダウンロード、アーカイブ ファイル内にネストされたファイルの表示、ネストされたファイルの親アーカイブ ファイルのダウンロード、または動的分析のための Collective Security Intelligence クラウドへのファイルの送信を実行できます。

侵入イベントについて、コンテキスト メニューを使用して、侵入ルール エディタまたは侵入ポリシーのタスクに似たタスクを実行することができます。トリガー ルールの編集、ルール状態の設定（ルールの無効化を含む）、しきい値と抑制オプションの設定、およびルール ドキュメントの表示を実行できます。

パケット ビュー

侵入イベントのパケット ビューには、IP アドレスのホットスポットが含まれます。パケット ビューでは、右クリック メニューの代わりに左クリック コンテキスト メニューを使用することに注意してください。

ダッシュボード

多くのダッシュボード ウィジェットには、Context Explorer に関連情報を表示するホットスポットが含まれます。ダッシュボード ウィジェットには、IP アドレスと SHA-256 値のホットスポットも含めることができます。

Context Explorer

Context Explorer には、グラフ、表、およびグラフ上にホットスポットが含まれます。Context Explorer で可能なものよりも詳しくグラフやリストのデータを調べたい場合、関連データのテーブル ビューにドリル ダウンできます。また、関連するホスト、ユーザ、アプリケーション、ファイル、および侵入ルール情報を表示することもできます。

Context Explorer では、Context Explorer に固有のフィルタリングやその他のオプションを含む左クリック コンテキスト メニューを使用することに注意してください。詳細については、Context Explorer データのドリルダウン（56-40 ページ）を参照してください。

コンテキスト メニューにアクセスする方法：

アクセス： すべて

ステップ 1　Web インターフェイスのホットスポット対応ページで、ポインタをホットスポットに合わせます。

Context Explorer を除いて、「`Right-click for menu`」というメッセージが表示されます。

ステップ 2　以下のようにして、コンテキスト メニューを起動します。

- Context Explorer またはパケット ビューで、ポインタを合わせたデバイスを左クリックします。
- ホットスポット対応の他のすべてのページでは、ポインタを合わせたデバイスを右クリックします。

ポップアップ コンテキスト メニューが表示され、ホットスポットに適したオプションが示されます。

ステップ 3　オプションの名前を左クリックして、いずれかのオプションを選択します。

アクセス コントロール ポリシー エディタまたは NAT ポリシー エディタを使用している場合、ルールが変更されます。それ以外の場合は、選択したオプションに基づいて、新しいブラウザ ウィンドウが開きます。

再利用可能なオブジェクトの管理

柔軟性を高めて、Web インターフェイスを使用しやすくするために、FireSIGHT システムでは名前付き*オブジェクト*を作成できます。これは、名前を値と関連付ける再使用可能な設定であり、値を使用する必要がある場合に、代わりに名前付きオブジェクトを使用できます。

次のタイプのオブジェクトを作成できます。

- ネットワークベースのオブジェクト。このオブジェクトによって、IP アドレスとネットワーク、ポート/プロトコルのペア、VLAN タグ、セキュリティ ゾーン、および送信側/宛先の国（位置情報）を表します。
- レピュテーションベースのオブジェクト。このオブジェクトによって、セキュリティ インテリジェンスのフィードとリスト、カテゴリとレピュテーションに基づくアプリケーション フィルタ、ファイル リストを表します。
- レピュテーションベース以外のオブジェクト（URL カテゴリなど）
- 侵入ポリシーに関連付ける変数を含む侵入ポリシーの変数セット
- 暗号化スイート、公開キー証明書や秘密キーのペア、および証明書の識別名を含む、暗号化トラフィックを処理するためのオブジェクト。

これらのオブジェクトは、アクセス コントロール ポリシー、ネットワーク分析ポリシー、侵入ポリシーやルール、ネットワーク検出ルール、イベント検索、レポート、ダッシュボードなど、システムの Web インターフェイスのさまざまな場所で使用できます。

オブジェクトをグループ化すると、複数のオブジェクトを 1 つの設定で参照できます。ネットワーク、ポート、VLAN タグ、URL、および公開キー インフラストラクチャ（PKI）オブジェクトをグループ化できます。

注 ほとんどの場合、ポリシーで使用されるオブジェクトを編集するには、変更を反映するためにポリシーの再適用が必要になります。セキュリティ ゾーンを編集する場合にも、適切なデバイスの設定を再適用する必要があります。

詳細については、次の項を参照してください。

- オブジェクト マネージャの使用（3-2 ページ）
- ネットワーク オブジェクトの操作（3-4 ページ）
- セキュリティ インテリジェンス リストとフィードの操作（3-5 ページ）
- ポート オブジェクトの操作（3-13 ページ）
- VLAN タグ オブジェクトの操作（3-14 ページ）
- URL オブジェクトの操作（3-15 ページ）

オブジェクト マネージャの使用

ライセンス： すべて

オブジェクト マネージャ（[Objects] > [Object Management]）を使用して、アプリケーション フィルタ、変数セット、およびセキュリティ ゾーンなどのオブジェクトを作成および管理します。ネットワーク、ポート、VLAN タグ、URL、および PKI オブジェクトをグループ化できます。さらに、オブジェクトおよびオブジェクト グループのリストをソート、フィルタ、参照することもできます。

詳細については、以下を参照してください。

- オブジェクトのグループ化（3-2 ページ）
- オブジェクトの参照、ソート、およびフィルタ（3-3 ページ）

オブジェクトのグループ化

ライセンス： すべて

ネットワーク、ポート、VLAN タグ、URL、および PKI オブジェクトをグループ化できます。システムでは、Web インターフェイスでオブジェクトおよびオブジェクト グループを交互に使用することができます。たとえば、ポート オブジェクトを使用する場合はいつでも、ポート オブジェクト グループも使用できます。同じタイプのオブジェクトおよびオブジェクト グループには、同じ名前を付けることはできません。

ヒント　暗号スイートをグループ化するには、暗号スイートのリストを設定します。詳細については、暗号スイート リストの操作（3-43 ページ）を参照してください。

ポリシーで使用されるオブジェクト グループ（たとえば、アクセス コントロール ポリシーで使用されるネットワーク オブジェクト グループ）を編集する場合、変更を有効にするためにポリシーを再適用する必要があります。

グループを削除しても、グループ内のオブジェクトは削除されず、相互の関連性だけが削除されます。さらに、使用中のグループは削除できません。たとえば、保存されたアクセス コントロール ポリシーの VLAN 条件で使用している VLAN タグのグループは削除できません。

再利用可能なオブジェクトをグループ化するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　次の選択肢があります。

- グループ化するオブジェクト タイプ [Network]、[Port]、[VLAN Tag]、[URL]、または [Distinguished Name] で、[Object Groups] を選択します。
- [PKI] で、グループ化する PKI オブジェクトのタイプとして [Internal CA Groups]、[Trusted CA Groups]、[Internal Cert Groups]、または [External Cert Groups] を選択します。

グループ化するオブジェクト タイプのページが表示されます。

ステップ 3　グループ化するオブジェクトに対応する [Add] ボタンをクリックします。

グループを作成するためのポップアップ ウィンドウが表示されます。

ステップ 4　グループの**名前**を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　1 つ以上のオブジェクトを選択し、[Add] をクリックします。

- 複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、右クリックして [Select All] を選択します。
- 含める既存のオブジェクトを検索するには、フィルタ フィールド（  ）を使用します。このフィールドは入力に従って更新され、一致する項目が表示されます。検索文字列をクリアするには、検索フィールドの上にある再ロード アイコン（  ）をクリックするか、検索フィールド内のクリア アイコン（  ）をクリックします。
- 既存のオブジェクトがニーズを満たさない場合、ただちにオブジェクトを作成するには、追加アイコン（  ）をクリックします。

ステップ 6　[Save] をクリックします。

グループが作成されます。

オブジェクトの参照、ソート、およびフィルタ

ライセンス： すべて

オブジェクト マネージャには、ページあたり 20 のオブジェクトまたはグループが表示されます。オブジェクトまたはグループのタイプが 20 を超える場合は、ページ下部のナビゲーション リンクを使用して追加ページを表示します。特定のページにアクセスしたり、更新アイコン（）にアクセスしてビューを更新したりすることもできます。

デフォルトでは、オブジェクトとグループはページで、アルファベット順に名前でリストされます。ただし、表示されている任意の列でオブジェクトまたはグループの各タイプをソートできます。列見出しの横にある上（▲）または下（▼）矢印は、ページがその列でその方向にソートされていることを示します。ページのオブジェクトは、名前によってフィルタすることもできます。オブジェクトのタイプによっては、同じフィルタが名前または値に一致することがあります。

オブジェクトまたはグループをソートする方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　カラムの見出しをクリックします。反対方向でソートするには、見出しを再度クリックします。

オブジェクトまたはグループをフィルタする方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Filter] フィールドのフィルタ条件を入力します。

ページは入力に従って更新され、一致する項目が表示されます。次のメタ文字を使用できます。

- アスタリスク（*）文字は、ある文字の 0 回以上のオカレンスに一致します。
- キャレット記号（^）は文字列の先頭のコンテンツと一致します。
- ドル記号（$）は文字列の末尾と一致します。

ネットワーク オブジェクトの操作

ライセンス： すべて

ネットワーク オブジェクトは、個別に、またはアドレス ブロックとして指定できる 1 つ以上の IP アドレスを表します。ネットワーク オブジェクトおよびグループ（オブジェクトのグループ化 (3-2 ページ)を参照）を、アクセス コントロール ポリシー、ネットワークの変数、侵入ルール、ネットワーク検出ルール、イベント検索、レポートなど、システムの Web インターフェイスのさまざまな場所で使用できます。

また、使用中のネットワーク オブジェクトは削除できません。さらに、アクセス コントロール、ネットワーク検出、または侵入ポリシーで使用されるネットワーク オブジェクトを編集した場合は、変更を有効にするためにポリシーを再適用する必要があります。

ネットワーク オブジェクトを作成する方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[Network] で、[Individual Objects] を選択します。

ステップ 3　[Add Network] をクリックします。

[Network Objects] ポップアップ ウィンドウが表示されます。

ステップ 4　[Name] にネットワーク オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　ネットワーク オブジェクトに追加する IP アドレスまたはアドレス ブロックごとに、値を入力して [Add] をクリックします。

ステップ 6　[Save] をクリックします。

ネットワーク オブジェクトが追加されます。

セキュリティ インテリジェンス リストとフィードの操作

ライセンス: Protection

サポートされるデバイス: すべて（シリーズ 2 を除く）

サポートされる防御センター: DC500 を除くいずれか

セキュリティ インテリジェンス機能を使用すると、アクセス コントロール ポリシーごとに、送信元または宛先 IP アドレスに基づいてネットワークをトラバースできるトラフィックを指定できます。これは、トラフィックがアクセス コントロール ルールによって分析される前に、特定の IP アドレスをブラックリストに入れる（トラフィックの送受信を拒否する）場合に特に役立ちます。同様に、IP アドレスをホワイトリストに追加して、アクセス コントロールを使用してシステムに接続を強制的に処理させることができます。

特定の IP アドレスをブラックリストに入れるかどうか決めていない場合は、「監視のみ」設定を使用できます。この場合、システムはアクセス コントロールを使用して接続を処理できますが、接続の一致はブラックリストに記録されます。

*グローバル ホワイトリスト*および*グローバル ブラックリスト*は、デフォルトですべてのアクセス コントロール ポリシーに含まれており、すべてのゾーンに適用されます。また、各アクセス コントロール ポリシー内で、ネットワーク オブジェクトとグループの組み合わせを使用して個別のホワイトリストおよびブラックリストや、セキュリティ インテリジェンスのリストとフィードを作成できます。ユーザはこれらすべてをセキュリティ ゾーン別に抑制することができます。

注　デフォルトで、シリーズ 2 デバイスは他のすべての Protection 機能がある場合でも、セキュリティ インテリジェンス フィルタリングを実行できません。

フィードとリストの比較

セキュリティ インテリジェンス *フィード*は、ユーザが設定した間隔でDefense Centerが HTTP または HTTPS サーバからダウンロードする IP アドレスの動的コレクションです。フィードは定期的に更新されるため、システムは最新の情報を使用してネットワーク トラフィックをフィルタできます。ブラックリストの作成に役立つように、Ciscoでは、Cisco VRT によってレピュテーションが低いと判断された IP アドレスを表す*インテリジェンス フィード*（別名「*Sourcefire インテリジェンス フィード*」）を提供しています。

Defense Centerは、更新されたフィード情報をダウンロードすると、管理対象デバイスを自動的に更新します。フィードの更新が導入環境全体に反映されるまで数分かかる場合がありますが、フィードの作成または変更後、またはスケジュールされたフィードの更新後に、アクセス コントロール ポリシーを再適用する必要はありません。

注　Defense Centerがインターネットからフィードをダウンロードするタイミングを厳密に制御する場合は、そのフィードの自動更新を無効にすることができます。ただし、Ciscoは自動更新の許可を推奨します。手動でオンデマンド更新を行うことはできますが、システムで定期的にフィードをダウンロードできるようにすれば、最新の関連データを入手できます。

フィードとは対照的に、セキュリティ インテリジェンスの *リスト*はDefense Centerに手動でアップロードする IP アドレスの簡単な静的リストです。フィードおよびグローバル ホワイトリストやブラックリストを増加および微調整するには、カスタム リストを使用します。カスタム リストの編集（ネットワーク オブジェクトの編集およびグローバル ホワイトリストまたはブラックリストからの IP アドレスの削除）を行う場合、変更を反映させるためにアクセス コントロール ポリシーを適用する必要があることに注意してください。

フィード データの書式設定や破損

フィードとリストのソースは、1 行につき 1 つの IP アドレスまたはアドレス ブロックを持つ、最大 500 MB の単純なテキスト ファイルでなければなりません。コメント行は # 文字で始める必要があります。リストのソース ファイルは .txt 拡張子を使用する必要があります。

Defense Centerが破損したフィードまたは認識不能な IP アドレスを持つフィードをダウンロードした場合、システムは古いフィード データを引き続き使用します（これが初回のダウンロードである場合を除く）。ただし、システムがフィード内の IP アドレスを 1 つでも認識できる場合、Defense Centerは、認識できるアドレスで管理対象デバイスを更新します。

デフォルトのヘルス ポリシーには、セキュリティ インテリジェンス モジュールが含まれています。これは、Defense Centerがフィードを更新できない場合や、フィードが破損していたり、認識できない IP アドレスが含まれていたりする場合など、セキュリティ インテリジェンス フィルタリングが関係する一部の状態でアラートを出します。

インターネット アクセスとハイ アベイラビリティ

システムは、ポート 443/HTTPS を使用してインテリジェンス フィードをダウンロードし、443/HTTP または 80/HTTP を使用してカスタムまたはサードパーティのフィードをダウンロードします。フィードを更新するには、Defense Centerでインバウンドとアウトバンド両方の適切なポートを開く必要があります。フィード サイトへのダイレクト アクセスを持っていない場合、Defense Centerはプロキシ サーバを使用できます（管理インターフェイスの構成（64-9 ページ）を参照してください）。

注　Defense Centerはカスタム フィードのダウンロード時にピア SSL 証明書の検証を実行**しません**。また、システムは、証明書のバンドルまたは自己署名証明書を使用したリモート ピアの検証もサポートしていません。

ハイ アベラビリティの導入環境では、セキュリティ インテリジェンス オブジェクトはDefense Center間で同期されますが、プライマリDefense Centerだけがフィードの更新をダウンロードします。プライマリDefense Centerが失敗した場合、セカンダリDefense Centerがフィード サイトへのアクセス権を持っていることを確認するだけでなく、セカンダリDefense Centerの Web インターフェイスを使用してアクセス権のレベルを [Active] に上げる必要があります。詳細については、ハイ アベイラビリティ ステータスのモニタリングおよび変更（4-16 ページ）を参照してください。

フィードとリストの管理

セキュリティ インテリジェンスのリストとフィード（総称してセキュリティ インテリジェンス オブジェクトと呼ばれる）は、オブジェクト マネージャのセキュリティ インテリジェンス ページを使用して作成および管理します。（ネットワーク オブジェクトおよびグループの作成および管理の詳細については、ネットワーク オブジェクトの操作（3-4 ページ）を参照してください。）

保存または適用されているアクセス コントロール ポリシーで現在使用されているカスタム リストまたはフィードは削除できないことに注意してください。さらに、個別の IP アドレスは削除できますが、グローバル リストは削除できません。同様に、インテリジェンス フィードは削除できませんが、編集することによって更新の頻度を無効にしたり、変更したりできます。

セキュリティ インテリジェンス オブジェクトのクイック リファレンス

次の表に、セキュリティ インテリジェンスのフィルタリングを実行する場合に使用できるオブジェクトのクイック リファレンスを示します。

表 3-1　セキュリティ インテリジェンス オブジェクトの機能

機能	グローバル ホワイトリストまたはブラックリスト	インテリジェンス フィード	カスタム フィード	カスタム リスト	ネットワーク オブジェクト
使用方法	デフォルトで、アクセス コントロール ポリシーで	ホワイトリストまたはブラックリスト オブジェクトとして任意のアクセス コントロール ポリシーで			
セキュリティ ゾーンで制約することができるか	no	yes	yes	yes	yes
削除できるか	no	no	はい（保存または適用されているアクセス コントロール ポリシーで現在使用されている場合を除く）		
オブジェクト マネージャの編集機能	IP アドレスのみを削除する（コンテキスト メニューを使用して IP アドレスを追加する）	更新の頻度を無効にするか、変更する	完全に変更する	変更されたリストのみをアップロードする	完全に変更する
変更時にアクセス ポリシー コントロールの再適用が必要か	削除する場合は yes（IP アドレスを追加する場合は、再適用する必要はありません）	no	no	yes	yes

セキュリティ インテリジェンスのリストおよびフィードの作成、管理、および使用の詳細については、以下を参照してください。

- グローバル ホワイトリストおよびブラックリストの操作（3-7 ページ）
- インテリジェンス フィードの操作（3-9 ページ）
- カスタム セキュリティ インテリジェンス フィードの操作（3-10 ページ）
- 手動によるセキュリティ インテリジェンス フィードの更新（3-11 ページ）
- カスタム セキュリティ インテリジェンスのリストの操作（3-11 ページ）
- セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録（13-1 ページ）

グローバル ホワイトリストおよびブラックリストの操作

ライセンス： Protection

サポートされるデバイス： すべて（シリーズ 2 を除く）

サポートされる防御センター： DC500 を除くいずれか

分析の過程で、イベント ビュー、コンテキスト エクスプローラ、またはダッシュボードで IP アドレスのコンテキスト メニューを使用し、セキュリティ インテリジェンスの*グローバル ブラックリスト*を作成できます。たとえば、エクスプロイトの試行に関連した侵入イベントでルーティング可能な IP アドレスのセットに気付いた場合、それらの IP アドレスを即時にブラックリストに入れることができます。また、同じ方法で*グローバル ホワイトリスト*も作成できます。

システムのグローバル ホワイトリストおよびブラックリストは、デフォルトですべてのアクセス コントロール ポリシーに含まれており、すべてのゾーンに適用されます。ポリシーのそれぞれについて、これらのグローバル リストを使用しないように選択することができます。

グローバル リストに IP アドレスを追加すると、Defense Centerは自動的に管理対象デバイスを更新します。導入環境全体で変更を反映するには数分かかる場合がありますが、グローバル リストに IP アドレスを追加した後は、アクセス コントロール ポリシーを再適用する必要はありません。逆に、グローバル ホワイトリストまたはブラックリストから IP アドレスを削除した後は、変更を反映するためにアクセス コントロール ポリシーを適用する必要があります。

ネットマスク /0 のネットワーク オブジェクトはホワイトリストまたはブラックリストに追加できますが、ネットマスク /0 を使用したアドレス ブロックは無視され、これらのアドレスに基づいたホワイトリストおよびブラックリスト フィルタリングは行われないことに注意してください。セキュリティ インテリジェンス フィードからのネットマスク /0 のアドレス ブロックも無視されます。すべてのトラフィックを監視またはブロックする場合は、セキュリティ インテリジェンス フィルタリングの代わりに、[Monitor] または [Block] ルール アクションでアクセス コントロール ルールを使用し、[Source Networks] および [Destination Networks] の [any] のデフォルト値をそれぞれ使用します。

IP アドレスをグローバル ホワイトリストまたはブラックリストに追加すると、アクセス コントロールに影響を与えるため、次のいずれかを持っている必要があります。

- 管理者アクセス
- デフォルト ロールの組み合わせ:Network Admin または Access Admin に加えて Security Analyst および Security Approver
- Modify Access Control Policy と Apply Access Control Policy の両方の権限を持つカスタム ロール。カスタム ユーザ ロールによる展開の管理（12-4 ページ）を参照してください。

コンテキスト メニューを使用して IP アドレスをグローバル ホワイトリストまたはブラックリストに追加する方法:

アクセス: Admin/Custom

ステップ 1　イベント ビュー、パケット ビュー、コンテキスト エクスプローラ、またはダッシュボードでは、ポインタを IP アドレスのホットスポットの上に移動します。

ヒント　イベント ビューまたはダッシュボードで、ポインタを左側のホスト アイコン（  ）ではなく、IP アドレスの上に移動します。

ステップ 2　コンテキスト メニューを次のように起動します。

- イベント ビューまたはダッシュボードの場合は、右クリックします。
- コンテキスト エクスプローラまたはパケット ビューの場合は、左クリックします。

ステップ 3　コンテキスト メニューから、[Whitelist Now] または [Blacklist Now] を選択します。

コンテキスト メニューの他のオプションの詳細については、コンテキスト メニューの使用（2-5 ページ）を参照してください。

ステップ 4　IP アドレスをホワイトリストまたはブラックリストに登録することを確認します。

Defense Centerがユーザの追加を管理対象デバイスに通知すると、導入環境ではその変更に従ってトラフィックのフィルタが開始されます。

IP アドレスをグローバル ホワイトリストまたはブラックリストから削除する方法:

アクセス: Admin/Network Admin

ステップ 1　オブジェクト マネージャのセキュリティ インテリジェンス ページで、グローバル ホワイトリストまたはブラックリストの横にある編集アイコン( )をクリックします。

[Global Whitelist] または [Global Blacklist] ポップアップ ウィンドウが表示されます。

ステップ 2　リストから削除する IP アドレスの横にある削除アイコン( )アイコンをクリックします。

複数の IP アドレスを同時に削除するには、Shift キーおよび Ctrl キーを使用してそれらを選択し、右クリックして [Delete] を選択します。

ステップ 3　[Save] をクリックします。

変更は保存されますが、それを有効にするにはアクセス コントロール ポリシーを適用する必要があります。

インテリジェンス フィードの操作

ライセンス: Protection

サポートされるデバイス: すべて（シリーズ 2 を除く）

サポートされる防御センター: DC500 を除くいずれか

ブラックリストの作成に役立つように、Ciscoでは *インテリジェンス フィード* (別名「*Sourcefire インテリジェンス フィード*」) を提供しています。このフィードは VRT によってレピュテーションが低いと判断された IP アドレスの複数のリストから構成されており、リストは定期的に更新されます。インテリジェンス フィードの各リストは特定のカテゴリ（オープン リレー、既知の攻撃者、偽の IP アドレス（bogon）など）を表しています。アクセス コントロール ポリシーでは、カテゴリのいずれかまたはすべてをブラックリストに登録できます。

インテリジェンス フィードは定期的に更新されるため、システムは最新の情報を使用してネットワーク トラフィックをフィルタできます。ただし、セキュリティに対する脅威（マルウェア、スパム、ボットネット、スパム、フィッシングなど）を表す不正な IP アドレスが現れては消えるペースが早すぎて、新しいポリシーを更新して適用するには間に合わないこともあります。

インテリジェンス フィードは削除できませんが、編集することによって更新の頻度を変更できます。デフォルトで、フィードは 2 時間ごとに更新されます。

インテリジェンス フィードの更新頻度の変更方法:

アクセス: Admin/Network Admin

ステップ 1　オブジェクト マネージャの [Security Intelligence] ページで、[Sourcefire Intelligence Feed] の横にある編集アイコン( )をクリックします。

[Sourcefire Intelligence Feed] ポップアップ ウィンドウが表示されます。

ステップ 2　[Update Frequency] を編集します。

2 時間から 1 週間までの範囲で、さまざまな間隔から選択できます。フィードの更新を無効にすることもできます。

ステップ 3　[Save] をクリックします。

変更が保存されます。

カスタム セキュリティ インテリジェンス フィードの操作

ライセンス： Protection

サポートされるデバイス： すべて（シリーズ 2 を除く）

サポートされる防御センター： DC500 を除くいずれか

カスタムまたはサードパーティのセキュリティ インテリジェンス フィードを使用すると、インターネット上で定期的に更新される他の信頼できるホワイトリストおよびブラックリストによって、インテリジェンス フィードを拡大することができます。内部フィードをセットアップすることもできます。これは、1 つのソース リストを使用して導入環境で複数のDefense Centerを更新する場合に役立ちます。

フィードを設定する場合は、URL を使用して場所を指定します。この URL は Punycode エンコードすることができません。デフォルトで、Defense Centerは、設定した間隔でフィード ソース全体をダウンロードし、管理対象デバイスを自動更新します。

オプションで、md5 チェックサムを使用して、更新フィードをダウンロードするかどうか判断するようにシステムを設定できます。Defense Centerが最後にフィードをダウンロードした以降にチェックサムが変更されていない場合は、システムによってフィードを再ダウンロードする必要はありません。特に内部フィードが大きい場合には、md5 チェックサムを使用することができます。md5 チェックサムは、チェックサムのみを含む単純なテキスト ファイルに保存する必要があります。コメントはサポートされていません。

セキュリティ インテリジェンス フィードを設定する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　オブジェクト マネージャの [Security Intelligence] ページで、[Add Security Intelligence] をクリックします。

[Security Intelligence] ポップアップ ウィンドウが表示されます。

ステップ 2　[Name] にフィードの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 3　[Type] ドロップダウン リストから、[Feed] を設定することを指定します。

ポップアップ ウィンドウが新しいオプションで更新されます。

ステップ 4　[Feed URL] を指定し、オプションで [MD5 URL] を指定します。

ステップ 5　[Update Frequency] を選択します。

2 時間から 1 週間までの範囲で、さまざまな間隔から選択できます。フィードの更新を無効にすることもできます。

ステップ 6　[Save] をクリックします。

セキュリティ インテリジェンス フィードのオブジェクトが作成されます。フィードの更新を無効にした場合を除き、Defense Centerは、フィードをダウンロードして検証しようとします。これで、アクセス コントロール ポリシーでフィード オブジェクトを使用できるようになりました。

手動によるセキュリティ インテリジェンス フィードの更新

ライセンス： Protection

サポートされるデバイス： すべて（シリーズ 2 を除く）

サポートされる防御センター： DC500 を除くいずれか

手動でセキュリティ インテリジェンス フィードを更新すると、インテリジェンス フィードを含め、すべてのフィードが更新されます。

すべてのセキュリティ インテリジェンス フィードを更新する方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　オブジェクト マネージャの [Security Intelligence] ページで、[Update Feeds] をクリックします。

ステップ 2　すべてのフィードを更新することを確認します。

更新が有効になるまで数分かかる場合があることを警告する確認ダイアログが表示されます。

ステップ 3　[OK] をクリックします。

フィードの更新をダウンロードして検証した後、Defense Centerはすべての変更内容を管理対象デバイスに通知します。導入環境では、更新されたフィードを使用してトラフィックのフィルタリングが開始されます。

カスタム セキュリティ インテリジェンスのリストの操作

ライセンス： Protection

サポートされるデバイス： すべて（シリーズ 2 を除く）

サポートされる防御センター： DC500 を除くいずれか

セキュリティ インテリジェンスのリストは、Defense Centerに手動でアップロードする IP アドレスおよびアドレス ブロックのシンプルな静的リストです。カスタム リストは、1 つのDefense Centerの管理対象デバイスに対して、フィードやいずれかのグローバル リストを増加したり微調整する場合に役立ちます。

アドレス ブロックのネットマスクは、IPv4 および IPv6 の場合、それぞれ 0 から 32、または 0 から 128 までの整数になることに注意してください。

たとえば、信頼できるフィードが重要なリソースへのアクセスを誤ってブロックしているものの、このフィードが全体的に組織にとって有用である場合、セキュリティ インテリジェンス フィード オブジェクトをアクセス コントロール ポリシーのブラックリストから削除する代わりに、誤って分類された IP アドレスだけが含まれるカスタム ホワイトリストを作成できます。

セキュリティ インテリジェンスのリストを変更するには、ソース ファイルを変更して、新しいコピーをアップロードする必要があることに注意してください。詳細については、セキュリティ インテリジェンス リストの更新（3-12 ページ）を参照してください。

新しいセキュリティ インテリジェンスをDefense Centerにアップロードする方法:

アクセス: Admin/Access Admin/Network Admin

ステップ 1 オブジェクト マネージャの [Security Intelligence] ページで、[Add Security Intelligence] をクリックします。

[Security Intelligence] ポップアップ ウィンドウが表示されます。

ステップ 2 [Name] にリストの名前を入力します。縦線(|)と中カッコ({})を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 3 [Type] ドロップダウンリストから、[List] をアップロードすることを指定します。

ポップアップ ウィンドウが新しいオプションで更新されます。

ステップ 4 [Browse] をクリックしてリストから .txt ファイルを検索し、[Upload] をクリックします。

リストがアップロードされます。ポップアップ ウィンドウに、システムがリスト内で検出した IP アドレスとアドレス ブロックの総数が表示されます。

番号が予期したものでない場合は、ファイルの書式設定を調べ、再試行してください。

ステップ 5 [Save] をクリックします。

セキュリティ インテリジェンス リストのオブジェクトが保存されます。これで、アクセス コントロール ポリシーでリスト オブジェクトを使用できるようになりました。

セキュリティ インテリジェンス リストの更新

ライセンス: Protection

サポートされるデバイス: すべて(シリーズ 2 を除く)

サポートされる防御センター: DC500 を除くいずれか

セキュリティ インテリジェンス リストを編集するには、ソース ファイルを変更して、新しいコピーをアップロードする必要があります。Defense Centerの Web インターフェイスを使用してファイルの内容を変更することはできません。ソース ファイルへのアクセス権がない場合は、Defense Centerからコピーをダウンロードできます。

セキュリティ インテリジェンス リストを変更する方法:

アクセス: Admin/Access Admin/Network Admin

ステップ 1 オブジェクト マネージャの [Security Intelligence] ページで、更新するリストの横にある編集アイコン( )をクリックします。

[Security Intelligence] ポップアップ ウィンドウが表示されます。

ステップ 2 編集するリストのコピーが必要な場合、[Download] をクリックして、ブラウザのプロンプトに従ってリストをテキスト ファイルとして保存します。

ステップ 3 必要に応じてリストを変更します。

ステップ 4 [Security Intelligence] ポップアップ ウィンドウで、[Browse] をクリックして、変更されたリストを参照し、[Upload] をクリックします。

リストがアップロードされます。

ステップ 5　[Save] をクリックします。

変更が保存されます。アクティブなアクセス コントロール ポリシーでリストが使用されている場合、変更を有効にするにはポリシーを適用する必要があります。

ポート オブジェクトの操作

ライセンス： すべて

ポート オブジェクトは、異なるプロトコルをそれぞれ少し異なる方法で表します。

- TCP および UDP の場合、ポート オブジェクトは、カッコ内にプロトコル番号が記載されたトランスポート層プロトコルと、オプションの関連ポートまたはポート範囲を表します。例：`TCP(6)/22`。
- ICMP および ICMPv6（IPv6 ICMP）の場合、ポート オブジェクトはインターネット層プロトコルおよびオプションのタイプとコードを表します。例：`ICMP(1):3:3`
- ポート オブジェクトは、ポートを使用しない他のプロトコルを表すこともできます。

Ciscoが既知のポート用にデフォルトのポート オブジェクトを提供することに注意してください。これらのオブジェクトは変更または削除できますが、Ciscoは代わりにカスタム ポート オブジェクトを作成することを推奨します。

ポート オブジェクトおよびグループ（オブジェクトのグループ化（3-2 ページ）を参照）を、アクセス コントロール ポリシー、ネットワーク検出ルール、ポート変数、およびイベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。たとえば、組織が特定のポート範囲を使用するカスタム クライアントを使用して、システムで過剰なイベントや誤解を与えるイベントが発生した場合、それらのポートの監視を除外するようネットワーク検出ポリシーを設定できます。

使用中のポート オブジェクトは削除できません。さらに、アクセス コントロール ポリシーまたはネットワーク検出ポリシーで使用されるポート オブジェクトを編集した場合は、変更を有効にするためにポリシーを再適用する必要があります。

アクセス コントロール ルールの送信元ポートの条件には TCP/UDP 以外のプロトコルを追加できないことに注意してください。さらに、送信元ポートと宛先ポートの両方のポート条件をルールで設定する場合、トランスポート プロトコルを混在させることはできません。

送信元ポートの条件で使用されるポート オブジェクト グループにサポート対象外のプロトコルを追加した場合、使用されるルールはポリシー適用中の管理対象デバイスには適用されません。さらに、TCP と UDP の両方のポートを含むポート オブジェクトを作成してから、ルールの送信元ポートの条件としてそのポート オブジェクトを追加した場合、宛先ポートを追加することはできません。その逆もまた同様です。

ポート オブジェクトを作成する方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[Port] で、[Individual Objects] を選択します。

ステップ 3　[Add Port] をクリックします。

[Port Objects] ポップアップ ウィンドウが表示されます。

ステップ 4　[Name] にポート オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　[Protocol] を選択します。

[TCP]、[UDP]、[IP]、[ICMP]、または [IPv6-ICMP] から選択するか、[Other] ドロップダウン リストを使用して別のプロトコルまたは [All] プロトコルを選択できます。

ステップ 6　オプションで、[Port] またはポート範囲を使用して TCP または UDP ポート オブジェクトを制限します。

1 ～ 65535 までの任意のポートを指定するか、すべてのポートと一致するように [any] を指定できます。ポートの範囲を指定するには、ハイフンを使用します。

ステップ 7　オプションで、[Type] および、該当する場合は関連する [Code] を使用して、ICMP または IPV6-ICMP ポート オブジェクトを制限します。

ICMP または IPv6-ICMP オブジェクトを作成する場合、タイプ、および該当する場合はコードを指定できます。ICMP のタイプとコードの詳細については、次の URL を参照してください。

- http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
- http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml

任意のタイプと一致するようにタイプに any を設定するか、指定したタイプの任意のコードと一致するようにコードに any を設定できます。

ステップ 8　オプションで、[Other] を選択し、ドロップダウン リストからプロトコルを選択します。[All] プロトコルを選択した場合は、[Port] フィールドにポート番号を入力します。

ステップ 9　[Save] をクリックします。

ポート オブジェクトが追加されます。

VLAN タグ オブジェクトの操作

ライセンス： すべて

設定した各 VLAN タグ オブジェクトは、VLAN タグまたはタグの範囲を表します。VLAN タグ オブジェクトおよびグループ（オブジェクトのグループ化（3-2 ページ）を参照）を、アクセス コントロール ポリシーおよびイベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。たとえば、特定の VLAN だけに適用されるアクセス コントロール ルールを作成することもできます。

使用中の VLAN タグ オブジェクトは削除できません。さらに、アクセス コントロール ポリシーで使用される VLAN タグ オブジェクトを編集した場合は、変更を有効にするためにポリシーを再適用する必要があります。

VLAN タグ オブジェクトを追加する方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[VLAN Tag] で、[Individual Objects] を選択します。

ステップ 3　[Add VLAN Tag] をクリックします。

[VLAN Tag] ポップアップ ウィンドウが表示されます。

ステップ 4　[Name] に、VLAN タグの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　[VLAN Tag] フィールドに VLAN タグの値を入力します。

1 ～ 4094 の任意の VLAN タグを指定できます。VLAN タグの範囲を指定するには、ハイフンを使用します。

ステップ 6　[Save] をクリックします。

VLAN タグのオブジェクトが追加されます。

URL オブジェクトの操作

ライセンス： すべて

サポートされるデバイス： すべて（シリーズ 2 を除く）

サポートされる防御センター： DC500 を除くいずれか

設定した各 URL オブジェクトは、単一の URL または IP アドレスを表します。URL オブジェクトおよびグループ（オブジェクトのグループ化（3-2 ページ）を参照）を、アクセス コントロール ポリシーおよびイベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。たとえば、特定の Web サイトをブロックするアクセス コントロール ルールを作成することもできます。

URL オブジェクトを作成する際に、特に暗号化トラフィックを復号化またはブロックする SSL インスペクションを設定しない場合は、次の事項に留意してください。

- アクセス コントロール ルールで URL オブジェクトを使用して HTTPS トラフィックを照合することを計画している場合は、トラフィックの暗号化に使用される公開キー証明書内でサブジェクトの共通名を使用するオブジェクトを作成します。なお、システムはサブジェクトの共通名に含まれるドメインを無視するため、サブドメイン情報は含めないでください。たとえば、www.example.com ではなく、example.com を使用します。
- URL 条件を含むアクセス コントロール ルールを使用して Web トラフィックを照合する場合、システムは暗号化プロトコル（HTTP 対 HTTPS）を無視します。つまり、アプリケーション条件を使用してルールを調整しない限り、Web サイトをブロックすると、その Web サイトへの HTTP と HTTPS の両方のトラフィックがブロックされます。URL オブジェクトを作成する場合は、オブジェクトの作成時にプロトコルを指定する必要はありません。たとえば、`http://example.com/` ではなく、`example.com` を使用します。

詳細については、トラフィック復号化の概要（19-1 ページ）および URL のブロッキング（16-9 ページ）を参照してください。

使用中の URL オブジェクトは削除できません。さらに、アクセス コントロール ポリシーで使用される URL オブジェクトを編集した場合は、変更を有効にするためにポリシーを再適用する必要があります。

URL オブジェクトを追加する方法:

アクセス: Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[URL] で、[Individual Objects] を選択します。

ステップ 3　[Add URL] をクリックします。

[URL Objects] ポップアップ ウィンドウが表示されます。

ステップ 4　[Name] に URL オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　URL オブジェクトの [URL] または IP アドレスを入力します。このフィールドでは、ワイルドカード（*）は使用**できません**。

ステップ 6　[Save] をクリックします。

URL オブジェクトが追加されます。

アプリケーション フィルタの操作

ライセンス: FireSIGHT

サポートされるデバイス: すべて（シリーズ 2 を除く）

FireSIGHT システムは IP トラフィックを分析するときに、ネットワーク上でよく使用されているアプリケーションを特定しようとします。アプリケーション認識は、アプリケーション ベースのアクセス コントロールを行うために不可欠です。システムは多くのアプリケーションに対応するディテクタとともに配布されており、Ciscoは頻繁に更新を提供し、システムおよび脆弱性データベース（VDB）の更新を通じてディテクタをさらに追加します。また、独自のアプリケーション プロトコル ディテクタを作成して、システムの検出機能を強化することもできます。

アプリケーション フィルタは、アプリケーションのリスク、ビジネス関連性、タイプ、カテゴリ、タグなどに関連付けられている条件に従ってアプリケーションをグループ化します（表 45-2 (45-12 ページ)を参照）。アプリケーション プロトコル ディテクタを作成する場合、これらの基準を使用してアプリケーションを特徴付ける必要もあります。アプリケーション フィルタを使用すると、アプリケーションを個別に検索および追加する必要がないため、アクセス コントロール ルール用のアプリケーション条件を素早く作成できます。詳細については、トラフィックとアプリケーション フィルタの一致(16-4 ページ)を参照してください。

アプリケーション フィルタを使用する別の利点は、新しいアプリケーションを変更または追加する場合にフィルタを使用するアクセス コントロール ルールを更新する必要がないことです。たとえば、すべてのソーシャル ネットワーキング アプリケーションをブロックするようにアクセス コントロール ポリシーを設定し、VDB の更新に新しいソーシャル ネットワーキング アプリケーション ディテクタが含まれる場合、ポリシーは VDB の更新時に更新されます。システムが新しいアプリケーションをブロックする前にポリシーを再適用する必要がありますが、アプリケーションをブロックするアクセス コントロール ルールを更新する必要はありません。

Cisco 提供のアプリケーション フィルタがユーザのニーズに応じてアプリケーションをグループ化しない場合、独自のフィルタを作成することができます。ユーザ定義フィルタでは、Cisco 提供のフィルタをグループ化して結合できます。たとえば、非常にリスクが高く、ビジネス関連性が低いアプリケーションをすべてブロックするフィルタを作成することができます。個々のア

プリケーションを手動で指定することによってもフィルタを作成できますが、これらのフィルタは、システム ソフトウェアまたは VDB を更新しても自動的に更新**されない**ことを覚えておいてください。

Cisco 提供のアプリケーション フィルタと同様、ユーザ定義のアプリケーション フィルタもアクセス コントロール ルールで使用できます。また、ユーザ定義フィルタを次の方法でも使用できます。

- イベント ビューアを使用してアプリケーションを検索する場合は、検索でのオブジェクトとアプリケーション フィルタの使用（60-5 ページ）を参照してください
- レポート テンプレートでテーブル ビューを抑制する場合は、レポート テンプレート セクションの検索設定の操作（57-18 ページ）を参照してください
- [Custom Analysis] ダッシュボード ウィジェットでアプリケーション統計情報をフィルタする場合は、Custom Analysis ウィジェットの設定（55-15 ページ）を参照してください

アプリケーション フィルタを作成および管理する場合は、オブジェクト マネージャ（[Objects] > [Object Management]）を使用します。アプリケーションの条件をアクセス コントロール ルールに追加しながら、アプリケーション フィルタをすぐに作成できることに注意してください。

[Application Filters] リストには、独自のフィルタを作成するために選択できる Cisco 提供のアプリケーション フィルタが含まれています。表示されるフィルタは検索文字列を使用することによって抑制できます。これは、カテゴリとタグの場合に特に役立ちます。

[Available Applications] リストには、選択したフィルタ内の個別のアプリケーションが含まれます。また、検索ストリングを使用して、表示されるアプリケーションを抑制することもできます。

システムは、OR 演算を使用して同じフィルタ タイプの複数のフィルタをリンクします。中リスク フィルタに 100 のアプリケーションが含まれており、高リスク フィルタに 50 のアプリケーションが含まれているシナリオについて考えてみてください。両方のフィルタを選択すると、システムは使用可能な 150 のアプリケーションを表示します。

システムは、AND 演算を使用して異なるタイプのフィルタをリンクします。たとえば、中リスクおよび高リスクのフィルタと中レベルおよび高レベルのビジネス関連性のフィルタを選択した場合、システムは、中リスクまたは高リスクで、かつ中レベルおよび高レベルのビジネス関連性があるアプリケーションを表示します。

ヒント　関連するアプリケーションについての詳細は情報アイコン（ ）をクリックします。詳細情報を表示するには、表示されるポップアップでインターネット検索リンクのいずれかをクリックします。

フィルタに追加するアプリケーションを決定したら、それらを個別に追加するか、アプリケーション フィルタを選択した場合は、[All apps matching the filter] を追加することができます。[Selected Applications and Filters] リストにあるアイテムの合計数が 50 を超えない限り、複数のフィルタおよび複数のアプリケーションを任意の組み合わせで追加できます。

アプリケーション フィルタを作成すると、オブジェクト マネージャの [Application Filters] ページにリストされます。このページには、各フィルタを構成する条件の合計数が表示されます。

表示されるアプリケーション フィルタのソートとフィルタの詳細については、オブジェクト マネージャの使用（3-2 ページ）を参照してください。使用中のアプリケーション フィルタは削除できないことに注意してください。さらに、アクセス コントロール ポリシーで使用されるアプリケーション フィルタを編集した場合は、変更を有効にするためにポリシーを再適用する必要があります。

アプリケーション フィルタを作成する方法:

アクセス: Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[Application Filters] をクリックします。

[Application Filters] セクションが表示されます。

ステップ 3　[Add Application Filter] をクリックします。

[Application Filter] ポップアップ ウィンドウが表示されます。

ステップ 4　[Name] にフィルタの名前を指定します。縦線(|)と中カッコ({})を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　オプションで、[Application Filters] リストにある Cisco 提供のフィルタを使用して、フィルタに追加するアプリケーションのリストを絞り込みます。

- リストを展開および縮小するには、各フィルタ タイプの横にある矢印をクリックします。
- フィルタ タイプを右クリックし、[Check All] または [Uncheck All] をクリックします。このリストには、各タイプで選択したフィルタ数が示されることに注意してください。
- 表示されるフィルタを絞り込むには、[Search by name] フィールドに検索文字列を入力します。これは、カテゴリとタグの場合に特に有効です。検索をクリアするには、クリア アイコン( )をクリックします。
- フィルタのリストを更新し、選択したフィルタをすべてクリアするには、リロード アイコン( )をクリックします。
- すべてのフィルタと検索フィールドをクリアするには、[Clear All Filters] をクリックします。

選択したフィルタに一致するアプリケーションが [Available Applications] リストに表示されます。リストには一度に 100 のアプリケーションが表示されます。

ステップ 6　[Available Applications] リストから、フィルタに追加するアプリケーションを選択します。

- 前の手順で指定した制約を満たすすべてのアプリケーションを追加するには、[All apps matching the filter] を選択します。
- 表示される個別のアプリケーションを絞り込むには、[Search by name] フィールドに検索文字列を入力します。検索をクリアするには、クリア アイコン( )をクリックします。
- 使用可能な個別のアプリケーションのリストを参照するには、リストの下部にあるページング アイコンを使用します。
- 複数の個別オブジェクトを選択するには、Shift キーまたは Ctrl キーを使用します。現在表示されている個別のアプリケーションを選択するには、右クリックして [Select All] を選択します。
- アプリケーションのリストを更新し、選択したアプリケーションをすべてクリアするには、リロード アイコン( )をクリックします。

個別のアプリケーションと [All apps matching the filter] は同時に選択できません。

ステップ 7　選択したアプリケーションをフィルタに追加します。クリックしてドラッグするか、[Add to Rule] をクリックできます。

結果は次のもので構成されています。

- 選択したアプリケーション フィルタ
- 選択した個別の使用可能なアプリケーション、または [All apps matching the filter]

フィルタには最大 50 のアプリケーションおよびフィルタを追加できます。選択したアプリケーションからアプリケーションまたはフィルタを削除するには、該当するな削除アイコン( )をクリックします。1 つ以上のアプリケーションおよびフィルタを選択するか、または右クリックして [Select All] を選択してから、右クリックして [Delete Selected] を選択することもできます。

ステップ 8　[Save] をクリックします。

アプリケーション フィルタが保存されます。

変数セットの操作

ライセンス： Protection

変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスおよびポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制、適応プロファイル、および動的ルール状態にある IP アドレスを表すこともできます。

ヒント　プリプロセッサ ルールは、侵入ルールで使用されるネットワーク変数で定義されたホストにかかわらず、イベントをトリガーできます。

変数セットを使用して、変数を管理、カスタマイズ、およびグループ化します。Cisco提供のデフォルトの変数セットを使用するか、独自のカスタム セットを作成することができます。どのセットでも、定義済みのデフォルトの変数を変更し、ユーザ定義の変数を追加および変更することができます。

ほとんどの shared object rule、および FireSIGHT システムが提供する 標準テキスト ルール は、定義済みのデフォルト変数を使用して、ネットワークおよびポート番号を定義します。たとえば、ルールの大半は、保護されたネットワークを指定するために変数 `$HOME_NET` を使用して、保護されていない(つまり外部の)ネットワークを指定するために変数 `$EXTERNAL_NET` を使用します。さらに、特殊なルールでは、他の定義済みの変数がしばしば使用されます。たとえば、Web サーバに対するエクスプロイトを検出するルールは、`$HTTP_SERVERS` 変数および `$HTTP_PORTS` 変数を使用します。

ルールがより効率的なのは、変数がユーザのネットワーク環境をより正確に反映する場合です。少なくとも、定義済みのデフォルトの変数の最適化(3-20 ページ) で説明されているように、デフォルトのセットにあるデフォルトの変数を変更する必要があります。`$HOME_NET` などの変数がネットワークを正しく定義し、`$HTTP_SERVERS` にネットワーク上のすべての Web サーバが含まれるようにするには、処理は最適化され、疑わしいアクティビティがないかどうかすべての関連システムが監視されます。

変数を使用するには、変数セットをアクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに関連付けられている侵入ポリシーにリンクします。デフォルトでは、デフォルトの変数セットは、アクセス コントロール ポリシーによって使用されるすべての侵入ポリシーにリンクされています。

詳細については、次の項を参照してください。

- 定義済みのデフォルトの変数の最適化(3-20 ページ)
- 変数セットについて(3-22 ページ)
- 変数セットの管理(3-24 ページ)
- 変数の管理(3-25 ページ)

定義済みのデフォルトの変数の最適化

ライセンス：Protection

FireSIGHT システムはデフォルトで、定義済みのデフォルト変数で構成される単一のデフォルトの変数セットを提供します。Ciscoの脆弱性調査チーム（VRT）はルールの更新を使用して、デフォルト変数を含む、新規および更新された侵入ルール、および他の侵入ポリシー要素を提供します。詳細については、「ルールの更新とローカル ルール ファイルのインポート（66-16 ページ）」を参照してください。

Ciscoで提供される多くの侵入ルールは定義済みのデフォルト変数を使用するため、これらの変数に対して適切な値を設定する必要があります。変数セットを使用してネットワーク上のトラフィックを特定する方法によっては、任意またはすべての変数セットにあるこれらのデフォルト変数の値を変更することができます。詳細については、「変数の追加および編集（3-27 ページ）」を参照してください。

注意　アクセス コントロールまたは侵入ポリシーをインポートすると、デフォルトの変数セットにある既存のデフォルト変数が、インポートされたデフォルト変数でオーバーライドされます。既存のデフォルト変数セットに、インポートされたカスタム変数セットに存在しないカスタム変数が含まれる場合、一意的な変数が保持されます。詳細については、設定のインポート（A-5 ページ）を参照してください。

以下の表は、Ciscoで提供される変数について説明し、ユーザが通常変更する変数を示します。変数をご使用のネットワークに合わせて調整する方法を決定するには、プロフェッショナル サービスまたはサポートに問い合わせてください。

表 3-2　Ciscoによって提供される変数

変数名	説明	変更しますか
$AIM_SERVERS	既知の AOL Instant Messenger（AIM）サーバを定義し、チャットベースのルールおよび AIM エクスプロイトを検索するルールで使用されます。	不要。
$DNS_SERVERS	ドメイン ネーム サービス（DNS）サーバを定義します。DNS サーバに特に影響するルールを作成する場合、$DNS_SERVERS 変数を宛先または送信元 IP アドレスとして使用できます。	現在のルール セットでは不要です。
$EXTERNAL_NET	保護されていないネットワークとして FireSIGHT システムが表示するネットワークを定義し、外部ネットワークを定義するために多くのルールで使用されます。	はい。$HOME_NET を適切に定義してから、$EXTERNAL_NET の値として $HOME_NET を除外する必要があります。
$FILE_DATA_PORTS	ネットワーク ストリームでファイルを検出する侵入ルールで使用される、暗号化されていないポートを定義します。	不要。

表 3-2　Ciscoによって提供される変数（続き）

変数名	説明	変更しますか
$FTP_PORTS	ネットワーク上の FTP サーバのポートを定義し、FTP サーバのエクスプロイト ルールに使用されます。	FTP サーバがデフォルト ポート以外のポートを使用する場合は変更します（Web インターフェイスでデフォルト ポートを確認できます）。
$GTP_PORTS	パケット デコーダが GTP（General Packet Radio Service [GPRS] トンネリング プロトコル）PDU 内部でペイロードを取得するデータ チャネル ポートを定義します。	不要。
$HOME_NET	関連した侵入ポリシーが監視するネットワークを定義し、内部ネットワークを定義するために多くのルールで使用されます。	内部ネットワークの IP アドレスを指定する場合は変更します。
$HTTP_PORTS	ネットワーク上の Web サーバのポートを定義し、Web サーバのエクスプロイト ルールに使用されます。	Web サーバがデフォルト ポート以外のポートを使用する場合は変更します（Web インターフェイスでデフォルト ポートを確認できます）。
$HTTP_SERVERS	ネットワーク上の Web サーバを定義します。Web サーバのエクスプロイト ルールで使用されます。	HTTP サーバを実行する場合は変更します。
$ORACLE_PORTS	ネットワーク上で Oracle データベース サーバのポートを定義し、Oracle データベースでの攻撃をスキャンするルールで使用されます。	Oracle サーバを実行する場合は変更します。
$SHELLCODE_PORTS	システムにシェル コードのエクスプロイトをスキャンさせるポートを定義し、シェル コードを使用するエクスプロイトを検出するルールで使用されます。	不要。
$SIP_PORTS	ネットワーク上の SIP サーバのポートを定義し、SIP のエクスプロイト ルールに使用されます。	不要。
$SIP_SERVERS	ネットワーク上で SIP サーバを定義し、SIP をターゲットとしたエクスプロイトを解決するルールで使用されます。	はい。SIP サーバを実行している場合は、$HOME_NET を適切に定義してから、$SIP_SERVERS の値として $HOME_NET を含める必要があります。
$SMTP_SERVERS	ネットワーク上で SMTP サーバを定義し、メール サーバをターゲットとするエクスプロイトを解決するルールで使用されます。	SMTP サーバを実行する場合は変更します。
$SNMP_SERVERS	ネットワーク上で SNMP サーバを定義し、SNMP サーバでの攻撃をスキャンするルールで使用されます。	SNMP サーバを実行する場合は変更します。
$SNORT_BPF	システム上のバージョン 5.3.0 より前の FireSIGHT システム ソフトウェア リリースに存在し、その後バージョン 5.3.0 以上にアップグレードされた場合にのみ表示されるレガシー拡張変数を識別します。拡張変数について（3-35 ページ）を参照してください。	変更しません。この変数は表示または削除のみが可能です。削除後に、編集または復元することはできません。
$SQL_SERVERS	ネットワーク上でデータベース サーバを定義し、データベースをターゲットとしたエクスプロイトを解決するルールで使用されます。	SQL サーバを実行する場合は変更します。

表 3-2　Ciscoによって提供される変数（続き）

変数名	説明	変更しますか
$SSH_PORTS	ネットワーク上の SSH サーバのポートを定義し、SSH サーバのエクスプロイト ルールに使用されます。	SSH サーバがデフォルト ポート以外のポートを使用する場合は変更します（Web インターフェイスでデフォルト ポートを確認できます）。
$SSH_SERVERS	ネットワーク上で SSH サーバを定義し、SSH をターゲットとしたエクスプロイトを解決するルールで使用されます。	はい。SSH サーバを実行している場合は、$HOME_NET を適切に定義してから、$SSH_SERVERS の値として $HOME_NET を含める必要があります。
$TELNET_SERVERS	ネットワーク上で既知の Telnet サーバを定義し、Telnet サーバをターゲットとしたエクスプロイトを解決するルールで使用されます。	Telnet サーバを実行する場合は変更します。
$USER_CONF	本来は Web インターフェイスを介して使用できない 1 つ以上の機能を設定できる一般ツールを提供します。拡張変数について（3-35 ページ）を参照してください。 **注意**　$USER_CONF の設定が競合または重複していると、システムは停止します。拡張変数について（3-35 ページ）を参照してください。	機能の説明で指示されている場合や、サポートによる指示があった場合を除き、変更しません。

変数セットについて

ライセンス：Protection

変数を任意のセットに追加すると、それはすべてのセットに追加されます。つまり、各変数セットは、システムで現在設定されているすべての変数のコレクションになります。どの変数セットでも、ユーザ定義の変数を追加し、任意の変数の値をカスタマイズすることができます。

FireSIGHT システムは初めに、定義済みのデフォルト値で構成される単一のデフォルトの変数セットを提供します。デフォルト設定では、各変数は最初はそのデフォルト値に設定されています。定義済みの変数の場合、このデフォルト値は VRT によって設定され、ルール更新で提供される値です。

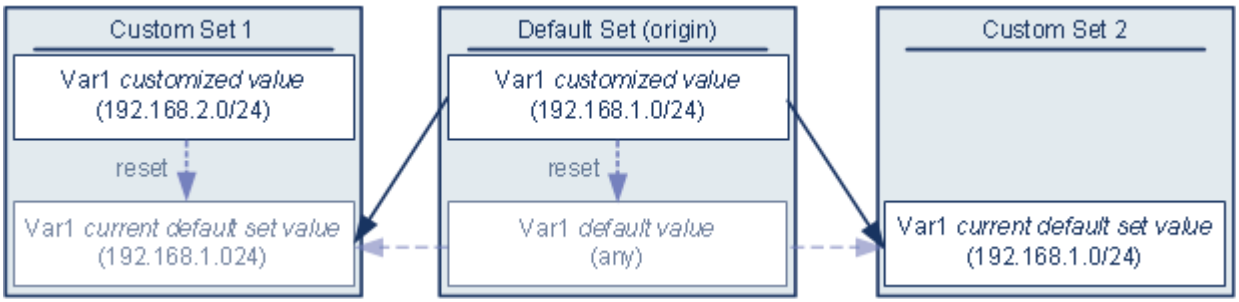
定義済みのデフォルト変数は、デフォルト値のままにすることもできますが、Ciscoは定義済みのデフォルトの変数の最適化（3-20 ページ）で説明されているように、定義済みの変数のサブセットを変更することを推奨します。

変数はデフォルト セットでのみ使用できますが、多くの場合、1 つ以上のカスタム設定を追加し、異なるセットで異なる変数の値を設定し、場合によっては新しい変数を追加することによって、最大限に活用できます。

複数のセットを使用する場合は、デフォルトのセットにある任意の変数の*現在値*によって、他のすべてのセットの変数の*デフォルト値*が決まることに注意してください。

例:デフォルト セットにユーザ定義変数を追加する

次の図は、値が 192.168.1.0/24 のデフォルト セットにユーザ定義の変数 Var1 を追加した場合のセットのインタラクションを示しています。



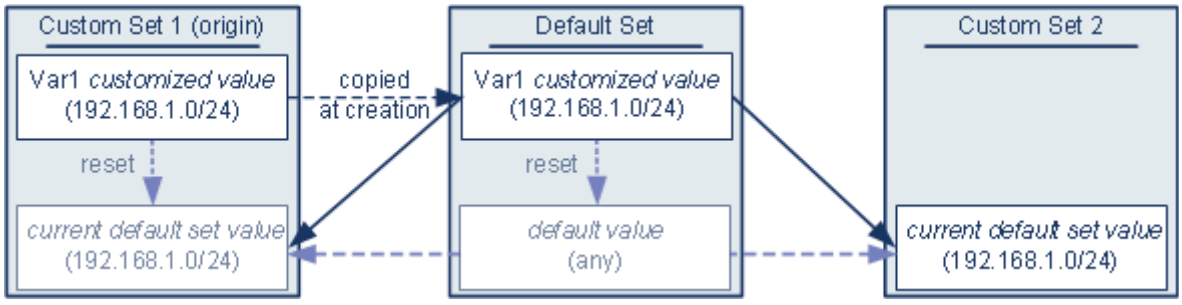
オプションで、任意のセットの Var1 値をカスタマイズできます。Var1 がカスタマイズされていない Custom Set 2 では、この値は 192.168.1.0/24 です。Custom Set 1 では、Var1 のカスタマイズ値 192.168.2.0/24 はデフォルト値をオーバーライドします。デフォルト設定では、ユーザ定義変数をリセットすると、すべてのセットのデフォルト値が any にリセットされます。

この例では、Custom Set 2 で Var1 を更新しなかった場合、デフォルト セットで Var1 をカスタマイズまたはリセットすると、Custom Set 2 の現在のデフォルト値 Var1 が更新され、変数セットにリンクされているすべての侵入ポリシーに影響を与えることに注意してください。

この例では示されていませんが、セット間の相互作用は、ユーザ定義変数およびデフォルト変数に対して同じです。ただし、デフォルト セットのデフォルト変数をリセットした場合、デフォルト変数は、現在のルール アップデートでCiscoによって設定された値にリセットされます。

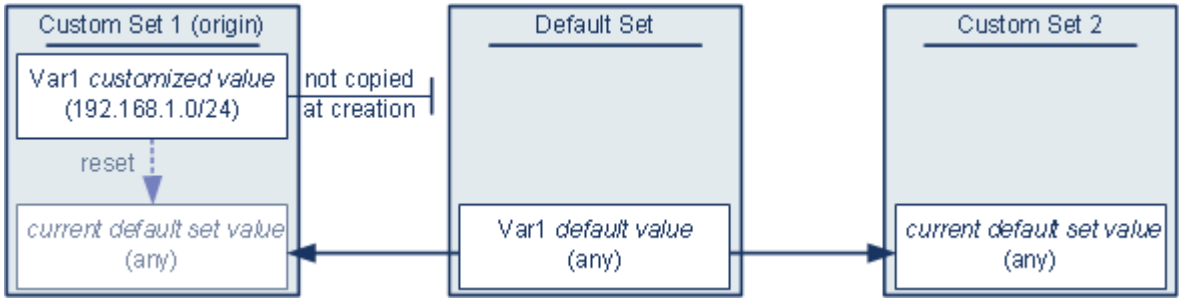
例:カスタム セットにユーザ定義変数を追加する

次の 2 つの例は、カスタム セットにユーザ定義変数を追加した場合の変数セットのインタラクションについて示しています。新しい変数を保存すると、設定値を他のセットのデフォルト値として使用するかどうかを尋ねるプロンプトが出されます。次の例では、設定値を**使用する**という選択がなされています。



Custom Set 1 からの Var1 の発信元を除き、この例は　Var1 をデフォルト セットに追加した上述の例と同じであることに注意してください。Var1 のカスタマイズ値 192.168.1.0/24 を Custom Set 1 に追加すると、値はデフォルト値 any を持つカスタマイズ値としてデフォルト セットにコピーされます。その後、Var1 の値とインタラクションは、Var1 をデフォルト セットに追加した場合と同じになります。前述の例と同様、デフォルト セットで Var1 をカスタマイズまたはリセットすると、Custom Set 2 の現在のデフォルト値 Var1 が更新され、変数セットにリンクされているすべての侵入ポリシーに影響を与えることに注意してください。

次の例では、前述の例にあるように値が 192.168.1.0/24 の Var1 を Custom Set 1 に追加しますが、Var1 の設定値を他のセットのデフォルト値として**使用しない**ことを選択します。



このアプローチでは、Var1 をデフォルト値 any を持つすべてのセットに追加します。Var1 を追加したら、任意のセットでその値をカスタマイズできます。このアプローチの利点は、デフォルト セットで Var1 を最初にカスタマイズしないことによって、デフォルト セットの値をカスタマイズし、Var1 をカスタマイズしていない Custom Set 2 などのセット内の現在の値を意図せずに変更してしまうリスクが軽減されます。

変数セットの管理

ライセンス： Protection

[Object Manager] ページ（[Objects] > [Object Management]）で [Variable Sets] を選択した場合、オブジェクト マネージャは、デフォルトの変数セットとユーザが作成したカスタム セットをリストします。

新しくインストールされたシステムで、デフォルトの変数セットは、Ciscoで定義済みのデフォルト変数だけで構成されます。

各変数セットには、Ciscoによって提供されるデフォルト変数と、任意の変数セットから追加したすべてのカスタム変数が含まれます。デフォルト設定は編集できますが、デフォルト セットの名前を変更したり、削除したりすることはできないことに注意してください。

注意　アクセス コントロールまたは侵入ポリシーをインポートすると、デフォルトの変数セットにある既存のデフォルト変数が、インポートされたデフォルト変数でオーバーライドされます。既存のデフォルト変数セットに、インポートされたカスタム変数セットに存在しないカスタム変数が含まれる場合、一意的な変数が保持されます。詳細については、設定のインポート（A-5 ページ）を参照してください。

次の表に、変数セットを管理するために実行できるアクションを要約します。

表 3-3　変数セットの管理アクション

目的	操作
変数セットを表示する	[Objects] > [Object Management] を選択し、[Variable Set] を選択します。
変数セットを名前でフィルタする	名前の入力を開始します。入力するにつれて、ページが更新され、一致する名前が表示されます。
名前のフィルタリングをクリアする	フィルタ フィールドのクリア アイコン（ ✖ ）をクリックします。

表 3-3　変数セットの管理アクション（続き）

目的	操作
カスタム変数セットを追加する	[Add Variable Set] をクリックします。 便宜を図るため、新しい変数セットには、現在定義されているすべてのデフォルト変数とカスタマイズ変数が含まれます。 **注**　変数セット名には、縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。
変数セットを編集する	編集する変数セットの横にある編集アイコン（）をクリックします。 **ヒント**　変数セットの行内で右クリックし、[Edit] を選択することもできます。
カスタム変数セットを削除する	変数セットの横にある削除アイコン（）をクリックしてから、[Yes] をクリックします。デフォルトの変数セットは削除できません。削除する変数セットで作成された変数は、他のセットで削除されたり他の方法で影響を受けたりしないことに注意してください。 **ヒント**　変数セットの行内で右クリックし、[Delete] を選択してから、[Yes] をクリックすることもできます。複数のセットを選択するには、Ctrl キーと Shift キーを使用します。

変数セットを設定した後、それらを侵入ポリシーにリンクできます。

変数セットを編集または作成する方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[Variable Set] を選択します。

ステップ 3　変数セットを追加したり、既存のセットを編集したりするには、次の手順に従います。

- 変数セットを追加するには、[Add Variable Set] をクリックします。
- 変数セットを編集するには、変数セットの横にある編集アイコン（）をクリックします。

新規の変数セット ページ、または変数セットの編集ページが表示されます。変数セットの命名には、縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。変数セット内の変数を追加および編集する方法の詳細については、変数の追加および編集（3-27 ページ）を参照してください。

変数の管理

ライセンス： Protection

変数セット内の新規の変数セット ページ、または変数セットの編集ページで変数を管理します。すべての変数セットの変数ページでは、変数は [Customized Variables] ページ領域と [Default Variables] ページ領域に分かれています。

*デフォルトの変数*は、Ciscoによって提供される変数です。デフォルト変数の値をカスタマイズすることができます。デフォルト変数の名前変更または削除はできません。また、デフォルト値を変更することもできません。

*カスタマイズされた変数*は、次のいずれかになります。

- カスタマイズされたデフォルト変数

  デフォルト変数の値を編集すると、システムはその変数を [Default Variables] 領域から [Customized Variables] 領域に移動します。デフォルト セットの変数値によってカスタム セットの変数のデフォルト値が決まるため、デフォルト セットのデフォルト変数をカスタマイズすると、他のすべてのセットの変数のデフォルト値が変更されます。

- ユーザ定義変数

  独自の変数を追加および削除したり、異なる変数セット内の値をカスタマイズしたり、カスタマイズされた変数をそのデフォルト値にリセットしたりできます。ユーザ定義変数をリセットすると、それは [Customized Variables] 領域に残ります。

次の表に、変数を作成または編集するために実行できるアクションを要約します。

表 3-4　　変数の管理アクション

目的	操作
変数のページを表示する	変数セット ページで、[Add Variable Set] をクリックして新しい変数セットを作成するか、編集する変数セットの横にある編集アイコン( )をクリックします。
変数セットに名前を付け、オプションで説明を加える	[Name] および [Description] フィールドにスペースや特殊文字を含む、英数字文字列を入力します。 **注**　変数セット名には、縦線(	)と中カッコ({ })を除き、印字可能な任意の標準 ASCII 文字を使用できます。
変数の完全な値を表示する	変数の横にある [Value] 列の値にポインタを移動します。 **注**　変数値には最大で 8192 文字まで格納できます。ただし、この制限は変数の拡張値のサイズに適用されることに注意してください。1 つ以上の変数を使用して別の変数を定義する場合、すべての変数値の文字やスペースの合計数は 8192 文字を超えてはいけません。
変数を追加する	[Add] をクリックします。 詳細については、「変数の追加および編集 (3-27 ページ)」を参照してください。
変数を編集する	編集する変数の横にある編集アイコン( )をクリックします。 詳細については、「変数の追加および編集 (3-27 ページ)」を参照してください。
変更された変数をデフォルト値にリセットする	変更された変数の横にあるリセット アイコン( )をクリックします。影付きリセット アイコンは、現在の値がすでにデフォルト値であることを示します。 **ヒント**　アクティブなリセット アイコンの上にポインタを移動して、デフォルト値を表示します。
ユーザ定義のカスタマイズされた変数を削除する	変数セットの横にある削除アイコン( )をクリックします。変数の追加後に変数セットを保存した場合は、[Yes] をクリックして変数を削除することを確認します。 デフォルト変数は削除できません。また、侵入ルールまたは他の変数によって使用されているユーザ定義変数は削除できません。
変数セットへの変更を保存する	変数セットがアクセス コントロール ポリシーで使用されている場合は [Save] をクリックしてから、[Yes] をクリックして変更を保存することを確認します。 デフォルト セットの現在の値によって他のすべてのセットのデフォルト値が決まるため、デフォルト セットの変数を変更またはリセットすると、デフォルト値がカスタマイズされていない他のセットの現在の値が変更されます。

変数セットの変数を表示する方法:

アクセス: Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[Variable Set] を選択します。

ステップ 3　変数セットを追加したり、既存のセットを編集したりするには、次の手順に従います。

- 変数セットを追加するには、[Add Variable Set] をクリックします。
- 変数セットを編集するには、変数セットの横にある編集アイコン( )をクリックします。

新規の変数セット ページ、または変数セットの編集ページが表示されます。変数セットの命名には、縦線(|)と中カッコ({})を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 4　変数を追加したり、既存の変数を編集したりするには、次の手順に従います。

- 変数を追加するには、[Add] をクリックします。
- 変数を編集するには、変数の横にある編集アイコン( )をクリックします。

新規の変数ページ、または変数の編集ページが表示されます。

変数セット内の変数を追加および編集する方法の詳細については、変数の追加および編集(3-27 ページ)を参照してください。

変数の追加および編集

ライセンス: Protection

任意のカスタム セットで変数を変更できます。

カスタム 標準テキスト ルール を作成する場合、独自のユーザ定義変数を追加して、トラフィックをより正確に反映したり、ショートカットとしてルール作成プロセスを単純化することもできます。たとえば、「緩衝地帯」(つまり DMZ)でのみトラフィックを検査するルールを作成する場合、公開されているサーバの IP アドレスが値にリストされる変数 $DMZ を作成できます。こうして、この地帯で作成された任意のルールで $DMZ 変数を使用できます。

変数セットに変数を追加すると、他のすべてのセットにもその変数が追加されます。以下に説明されている 1 つの例外を除き、変数はデフォルト値として他のセットに追加され、その後ユーザはそれをカスタマイズできます。

カスタム セットから変数を追加すると、設定値をデフォルト セットのカスタマイズ値として使用するかどうかを決定する必要があります。

- 設定値(たとえば、192.168.0.0/16)を**使用する**場合、変数は、デフォルト値 any を持つカスタマイズ値として設定値を使用するデフォルト セットに追加されます。デフォルト セットの現在の値によって他のセットのデフォルト値が決まるため、他のカスタム セットの初期のデフォルト値は設定値(この例では 192.168.0.0/16)になります。
- 設定値を**使用しない**場合、変数はデフォルト値 any のみを使用してデフォルト セットに追加され、こうして、他のカスタム セットの初期のデフォルト値は any になります。

詳細については、「変数セットについて(3-22 ページ)」を参照してください。

変数セット内の変数の追加は [New Variable] ページで行い、既存の変数の編集は [Edit Variable] ページで行います。これら 2 つのページは、既存の変数を編集する場合に、変数名または変数タイプを変更できないこと以外は、同じように使用します。

各ページは主に次の 3 つのウィンドウで構成されます。

- 既存のネットワークまたはポート変数、オブジェクト、およびネットワーク オブジェクト グループを含む、使用可能な項目
- 変数定義に包含するネットワークまたはポート
- 変数定義から除外するネットワークまたはポート

次の 2 種類の変数を作成または編集できます。

- *ネットワーク*変数は、ネットワーク トラフィックのホストの IP アドレスを指定します。ネットワーク変数の操作（3-31 ページ）を参照してください。
- *ポート* 変数は、ネットワーク トラフィックの TCP または UDP ポートを指定するもので、いずれかのタイプを意味する値 `any` を指定することもできます。ポート変数の操作（3-33 ページ）を参照してください。

ネットワーク変数タイプを追加するのか、ポート変数タイプを追加するのかを指定すると、ページが更新され、使用可能な項目がリストされます。リストの上部にある検索フィールドを使用してリストを制約できます。これは、入力するにつれて更新されます。

項目のリストから使用可能な項目を選択してドラッグし、包含または除外することができます。また、項目を選択し、[Include] または [Exclude] ボタンをクリックすることもできます。複数の項目を選択するには、Ctrl キーと Shift キーを使用します。包含または除外された項目のリストの下にある設定フィールドを使用して、ネットワーク変数にリテラル IP アドレスおよびアドレス ブロック、およびポート変数にポートおよびポート範囲を指定できます。

ネットワーク変数の場合、包含または除外する項目のリストは、リテラル文字列や既存の変数、オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせで構成できます。

次の表に、変数を作成または編集するために実行できるアクションを要約します。

表 3-5　　変数の編集アクション

目的	操作
変数のページを表示する	変数セットのページで、[Add] をクリックして新しい変数を追加するか、既存の変数の横にある編集アイコン（）をクリックします。
変数に名前を付ける	[Name] フィールドに、下線文字（_）以外の特殊文字が含まれない、大文字と小文字が区別される一意の英数字文字列を入力します。 変数名では大文字と小文字が区別されるので注意してください。たとえば、`var` と `Var` はそれぞれ一意です。
ネットワーク変数またはポート変数を指定する	[Type] ドロップダウンリストから [Network] または [Port] を選択します。 ネットワーク変数およびポート変数を使用して設定する方法の詳細については、ネットワーク変数の操作（3-31 ページ）およびポート変数の操作（3-33 ページ）を参照してください。
利用可能なネットワークのリストから選択できるように、個別のネットワーク オブジェクトを追加する	[Type] ドロップダウンリストから [Network] を選択し、追加アイコン（  ）をクリックします。オブジェクト マネージャを使用してネットワーク オブジェクトを追加する方法の詳細については、ネットワーク オブジェクトの操作（3-4 ページ）を参照してください。

表 3-5　変数の編集アクション（続き）

目的	操作
利用可能なポートのリストから選択できるように、個別のポート オブジェクトを追加する	[Type] ドロップダウンリストから [Port] を選択し、追加アイコン（）をクリックします。 任意のポート タイプを追加できますが、いずれかのタイプを意味する値 any を含め、TCP および UDP ポートだけが有効な変数値であり、使用可能なポートのリストにはこれらの値タイプを使用する変数のみが表示されます。オブジェクト マネージャを使用してポート オブジェクトを追加する方法の詳細については、ポート オブジェクトの操作（3-13 ページ）を参照してください。
使用可能なポート項目またはネットワーク項目を名前で検索する	使用可能な項目のリストの上にある検索フィールドで名前を入力していきます。入力するに従ってページが更新され、一致する名前が表示されます。
名前の検索をクリアする	検索フィールドの上のリロード アイコン（  ）、または検索フィールド内のクリア アイコン（）をクリックします。
使用可能な項目を区別する	変数アイコン（  ）、ネットワーク オブジェクト アイコン（  ）、ポート アイコン（  ）、およびオブジェクト グループ アイコン（  ）の横にある項目を探します。 ポート グループではなく、ネットワーク グループだけが使用可能であることに注意してください。
変数定義に含める（または除外する）オブジェクトを選択する	使用可能なネットワークまたはポートのリストにあるオブジェクトをクリックします。複数のオブジェクトを選択するには、Ctrl キーと Shift キーを使用します。
含まれる（または除外される）ネットワークまたはポートのリストに、選択した項目を追加する	選択した項目をドラッグ アンド ドロップします。あるいは、[Include] または [Excluede] をクリックします。 使用可能な項目のリストから、ネットワークやポートの変数とオブジェクトを追加できます。また、ネットワーク オブジェクト グループを追加することもできます。
リテラル ネットワークまたはポートを含める（または除外する）ために、ネットワークまたはポートのリストに追加する	クリックしてリテラル [Network] または [Port] フィールドからプロンプトを削除し、ネットワーク変数の場合はリテラル IP アドレスまたはアドレス ブロック、ポート変数の場合はリテラル ポートまたはポート範囲をそれぞれ入力して、[Add] をクリックします。 ドメイン名やリストを入力できないことに注意してください。複数の項目を追加するには、それぞれを個別に追加します。
値が any の変数を追加する	変数に名前を付け、変数タイプを選択してから、値を設定せずに [Save] をクリックします。 **注**　変数名は一意の英数字文字列でなければなりません。この文字列では、大文字と小文字が区別され、下線文字（_）以外の特殊文字は使用できません。
包含/除外リストから変数またはオブジェクトを削除する	変数の横にある削除アイコン（  ）をクリックします。
新規または変更された変数を保存する	[Save] をクリックします。カスタム セットから変数を追加している場合は、[Yes] をクリックすると設定値が他のセットのデフォルト値として使用され、[No] をクリックするとデフォルト値 any が使用されます。

詳細については、次の項を参照してください。

- ネットワーク変数の操作（3-31 ページ）
- ポート変数の操作（3-33 ページ）

変数を追加または編集する方法:

アクセス: Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[Variable Set] を選択します。

ステップ 3　変数セットを追加したり、既存のセットを編集したりするには、次の手順に従います。

- 変数セットを追加するには、[Add Variable Set] をクリックします。
- 既存の変数セットを編集するには、変数セットの横にある編集アイコン( )をクリックします。

新しい変数セットのページ、または変数セットの編集ページが表示されます。変数セットの命名には、縦線(|)と中カッコ({})を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 4　新しい変数を追加したり、既存の変数を編集したりするには、次の手順に従います。

- 新しい変数を追加するには、[Add] をクリックします。
- 既存の変数を編集するには、変数の横にある編集アイコン( )をクリックします。

新しい変数のページ、または変数の編集ページが表示されます。

ヒント　変数ページで、右クリックのコンテキスト メニューを使用して項目を選択または削除できます(コンテキスト メニューの使用(2-5 ページ)を参照)。

ステップ 5　新しい変数を追加している場合は

- [Name] に一意の変数名を入力します。

  英数字およびアンダースコア(_)文字を使用できます。
- ドロップダウンリストから、変数の [Type] として[Network] または [Port] を選択します。

ステップ 6　オプションで、使用可能なネットワークまたはポートのリストから、包含または除外項目リストに項目を移動します。

1 つ以上の項目を選択してから、ドラッグ アンド ドロップするか、[Include] または [Exclude] をクリックできます。複数の項目を選択するには、Ctrl キーと Shift キーを使用します。

ヒント　ネットワーク変数またはポート変数の包含リストと除外リストにあるアドレスやポートが重複している場合、除外されているアドレスまたはポートが優先されます。

ステップ 7　オプションで、1 つのリテラル値を入力し、[Add] をクリックします。

ネットワーク変数の場合、単一の IP アドレスまたはアドレス ブロックを入力できます。ポート変数の場合、単一ポートまたはポート範囲を追加できます。ポート範囲は上限値と下限値をハイフン(-)で区切ります。

複数のリテラル値を入力する場合は、必要に応じてこの手順を繰り返します。

ステップ 8　[Save] をクリックして変数を保存します。カスタム セットから新しい変数を追加する場合、次のオプションがあります。

- [Yes] をクリックすると、設定値を使用する変数がデフォルト セットのカスタマイズ値として追加され、結果として他のカスタム セットのデフォルト値として追加されます。

- [No] をクリックすると、変数はデフォルト セットのデフォルト値 any として追加され、結果として他のカスタム セットのデフォルト値として追加されます。

ステップ 9　変更を終えたら、変数セットを保存するために [Save] をクリックして、[Yes] をクリックします。

変更内容が保存され、変数セットにリンクされているアクセス コントロール ポリシーに失効ステータスが表示されます。変更を反映させるには、変数セットが侵入ポリシーに関連付けられているアクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

ネットワーク変数の操作

ライセンス： Protection

ネットワーク変数で表される IP アドレスを、侵入ポリシーで有効になった侵入ルール、侵入ポリシー ルール抑制、動的ルール状態、および適応型プロファイルで使用することができます。ネットワーク変数とネットワーク オブジェクトおよびネットワーク オブジェクト グループとの相違点として、ネットワーク変数は侵入ポリシーおよび侵入ルールに固有のものです。一方、ネットワーク オブジェクトおよびグループを使用すると、アクセス コントロール ポリシー、ネットワーク変数、侵入ルール、ネットワーク検出 ルール、イベント検索、レポートなど、システムの Web インターフェイスのさまざまな場所で IP アドレスを表すことができます。詳細については、「ネットワーク オブジェクトの操作（3-4 ページ）」を参照してください。

次の設定でネットワーク変数を使用して、ネットワーク上のホストの IP アドレスを指定できます。

- 侵入ルール

  侵入ルールの [Source IPs] および [Destination IPs] 見出し フィールドを使用すると、パケット インスペクションを、特定の送信元または宛先 IP アドレスを持つパケットに制限することができます。侵入ルールでの IP アドレスの指定（36-5 ページ）を参照してください。

- 抑制

  送信元または宛先の侵入ルール抑制の [Network] フィールドを使用すると、特定の 1 つの IP アドレスまたは IP アドレス範囲が侵入ルールやプリプロセッサをトリガーした場合の侵入イベント通知を抑制できます。侵入ポリシー単位の抑制の設定（32-30 ページ）を参照してください。

- 動的ルール状態

  送信元または宛先の動的ルール状態の [Network] フィールドを使用すると、指定時間内に発生した侵入ルールやプリプロセッサ ルールの一致数が多すぎる場合に、それを検出できます。動的ルール状態の追加（32-33 ページ）を参照してください。

- 適応型プロファイル

  適応型プロファイルの [Networks] フィールドは、パッシブ展開でのパケット フラグメントと TCP ストリームの再構築リアセンブリを改善させる必要があるネットワーク マップ内のホストを特定します。パッシブ展開における前処理の調整（30-1 ページ）を参照してください。

このセクションで示されるフィールドで変数を使用する場合、侵入ポリシーにリンクされた変数セットは、侵入ポリシーを使用するアクセス コントロール ポリシーで処理されるネットワーク トラフィックでの変数値を決定します。

次のネットワーク設定を任意に組み合わせて変数に追加できます。

- 使用可能なネットワーク リストから選択したネットワーク変数、ネットワーク オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせ

  オブジェクト マネージャを使用して個別のネットワーク オブジェクトとグループ ネットワーク オブジェクトを作成する方法については、ネットワーク オブジェクトの操作（3-4 ページ）を参照してください。

- [New Variable] または [Edit Variable] ページから追加した個々のネットワーク オブジェクト（独自の変数や、他の既存の変数、さらに今後の変数にこれらを追加できます）

- リテラルの単一 IP アドレスまたはアドレス ブロック

  それぞれを個別に追加することにより、複数のリテラル IP アドレスとアドレス ブロックをリストできます。IPv4 および IPv6 アドレスとアドレス ブロックを単独で、または任意に組み合わせてリストできます。IPv6 アドレスを指定するときには、RFC 4291 で定義された任意のアドレス指定規則を使用できます。

追加する変数での包含ネットワークのデフォルト値は `any` で、これは任意の IPv4 または IPv6 アドレスを示します。除外ネットワークのデフォルト値は `none` で、ネットワークがないことを示しています。また、リテラル値の中でアドレス `::` を指定すると、包含ネットワーク リストで任意の IPv6 アドレスを指定でき、除外リストでは IPv6 アドレスなしを指定できます。

除外リストにネットワークを追加すると、指定されたアドレスおよびアドレス ブロックが拒否されます。つまり、除外された IP アドレスやアドレス ブロックを除き、任意の IP アドレスに一致させることができます。

たとえば、リテラル アドレス `192.168.1.1` を除外すると 192.168.1.1 以外の任意の IP アドレスが指定され、`2001:db8:ca2e::fa4c` を除外すると 2001:db8:ca2e::fa4c 以外の任意の IP アドレスが指定されます。

リテラル ネットワークまたは使用可能なネットワークを任意に組み合わせて、除外で使用できます。たとえば、リテラル値 `192.168.1.1` および `192.168.1.5` を除外すると、192.168.1.1 と 192.168.1.5 以外の任意の IP アドレスが *含まれ*ます。つまり、システムはこの構文を「192.168.1.1 **でなく、しかも** 192.168.1.5 **でない**」と解釈し、大カッコ内に列挙されたものを除くすべての IP アドレスに一致させます。

ネットワーク変数を追加または編集するときには、次の点に注意してください。

- 論理的に言って、値 `any` を除外することはできません。any を除外すると「アドレスなし」を意味することになります。たとえば、除外ネットワーク リストに、値 `any` を持つ変数を追加することはできません。

- ネットワーク変数は、指定された侵入ルールおよび侵入ポリシー機能に関するトラフィックを識別します。プリプロセッサ ルールは、侵入ルールで使われているネットワーク変数で定義されたホストとは無関係に、イベントをトリガーできることに注意してください。

- 除外される値は、包含される値のサブセットに解決される必要があります。たとえば、アドレス ブロック 192.168.5.0/24 を包含し、192.168.6.0/24 を除外することはできません。エラー メッセージが表示され、問題となっている変数が明示されます。包含される値の範囲外となる値を除外した場合は、変数セットを保存できません。

ネットワーク変数の追加および編集の詳細については、変数の追加および編集（3-27 ページ）を参照してください。

ポート変数の操作

ライセンス：Protection

ポート変数は、侵入ポリシーで有効になった侵入ルールの [Source Port] および [Destination Port] 見出し フィールドで使用できる TCP ポートと UDP ポートを表します。ポート変数とポート オブジェクトおよびポート オブジェクト グループとの相違点は、ポート変数が侵入ルール固有のものであることです。TCP や UDP 以外のプロトコル用にポート オブジェクトを作成し、ポート変数、アクセス コントロール ポリシー、ネットワーク検出 ルール、イベント検索など、システムの Web インターフェイスのさまざまな場所でポート オブジェクトを使用できます。詳細については、「ポート オブジェクトの操作（3-13 ページ）」を参照してください。

侵入ルールの [Source Port] および [Destination Port] 見出し フィールドでポート変数を使用すると、パケット インスペクションを、特定の送信元または宛先 TCP/UDP ポートを持つパケットに制限することができます。

これらのフィールドで変数を使用した場合、アクセス コントロール ルールまたはポリシーに関連付けられた侵入ポリシーにリンクされる変数セットは、アクセス コントロール ポリシーが適用されるネットワーク トラフィックでのこれらの変数の値を決定します。

次のポート設定を任意に組み合わせて変数に追加できます。

- 使用可能なポート リストから選択したポート変数およびポート オブジェクトの任意の組み合わせ

  使用可能なポート リストには、ポート オブジェクト グループが表示されず、したがってこれらを変数に追加できないことに注意してください。オブジェクト マネージャを使用してポート オブジェクトを作成する方法については、ポート オブジェクトの操作（3-13 ページ）を参照してください。

- [New Variable] または [Edit Variable] ページから追加した個々のポート オブジェクト（独自の変数や、他の既存の変数、さらに今後の変数にこれらを追加できます）

  有効な変数値は TCP および UDP ポートのみです（どちらのタイプでも値 `any` を含む）。新しい変数のページまたは変数の編集ページを使用して、有効な変数値ではない有効なポート オブジェクトを追加した場合、オブジェクトはシステムに追加されますが、使用可能なオブジェクト リストには表示されません。オブジェクト マネージャを使用して、変数で使われるポート オブジェクトを編集する場合、有効な変数値にのみ値を変更できます。

- 単一のリテラル ポート値とポート範囲

  ポート範囲はダッシュ（-）を使って区切る必要があります。下位互換性のために、コロンで指定されるポート範囲もサポートされていますが、作成するポート変数ではコロンを使用できません。

  複数のリテラル ポートの値および範囲をリストするには、それぞれを個別に追加して任意に組み合わることができます。

ポート変数を追加または編集するときには、次の点に注意してください。

- 追加する変数での包含ポートのデフォルト値は `any` で、これは任意のポートまたはポート範囲を示します。除外ポートのデフォルト値は `none` で、これは「ポートなし」を示します。

ヒント　値 `any` を持つ変数を作成するには、特定の値を追加せずに変数に名前を付けて保存します。

- 論理的に言って、値 `any` を除外することはできません。any を除外すると「ポートなし」を意味することになります。たとえば、値 `any` を持つ変数を除外ポート リストに追加した場合、変数セットを保存することはできません。

- 除外リストにポートを追加すると、指定されたポートおよびポート範囲が拒否されます。つまり、除外されたポートまたはポート範囲を除き、任意のポートに一致させることができます。
- 除外される値は、包含される値のサブセットに解決される必要があります。たとえば、ポート範囲 10 から 50 を包含し、ポート 60 を除外することはできません。エラー メッセージが表示され、問題となっている変数が明示されます。包含される値の範囲外となる値を除外した場合は、変数セットを保存できません。

ポート変数の追加および編集の詳細については、変数の追加および編集（3-27 ページ）を参照してください。

変数のリセット

ライセンス： Protection

変数セットの新しい変数ページまたは変数の編集ページで、変数をデフォルト値にリセットできます。次の表に、変数をリセットするときの基本原則を要約します。

表 3-6　　変数のリセット値

リセットする変数のタイプ	それが含まれるセット タイプ	リセット後の値
デフォルト	デフォルト	ルール更新値
ユーザ定義	デフォルト	any
デフォルトまたはユーザ定義	custom	現在のデフォルト セット値（変更/未変更にかかわらず）

カスタム セットの変数をリセットすると、単にデフォルト セット内のその変数の現在値にリセットされます。

逆に、デフォルト セットの変数の値をリセットまたは変更すると、すべてのカスタム セット内のその変数のデフォルト値が常に更新されます。リセット アイコンがグレー表示され、その変数をリセットできないことを示している場合、そのセットでは変数のカスタマイズ値が存在しないことを意味します。カスタム セット内の変数の値をすでにカスタマイズした場合を除き、デフォルト セットの変数を変更すると、変数セットがリンクされた侵入ポリシーで使われている値が更新されます。

注　デフォルト セット内の変数を変更するときには、その変更により、リンクされたカスタム セットの変数を使用する侵入ポリシーがどのような影響を受けるか評価するのが適切です（特に、カスタム セット内の変数値をカスタマイズしていない場合）。

変数セット内のリセット アイコン（）の上にポインタを置くと、リセット値を確認できます。カスタマイズされた値とリセット値が同じである場合は、次のいずれかを示しています。

- カスタム セットまたはデフォルト セットの中で、値 any を持つ変数を追加した
- カスタム セットの中で、明示的な値を持つ変数を追加し、設定した値をデフォルト値として使用することを選択した

変数セットを侵入ポリシーにリンクさせる

ライセンス：Protection

デフォルトは、FireSIGHT システムは、アクセス コントロール ポリシーで使用されるすべての侵入ポリシーにデフォルト変数セットをリンクします。侵入ポリシーを使用するアクセス コントロール ポリシーを適用すると、その侵入ポリシー内で有効になった侵入ルールは、リンクされた変数セットの変数値を使用します。

アクセス コントロール ポリシー内の侵入ポリシーで使われるカスタム変数セットを変更すると、[Access Control] ページにそのポリシーのステータスが「失効」と表示されます。変数セットの変更内容を反映させるには、アクセス コントロール ポリシーを再適用する必要があります。デフォルト セットを変更すると、侵入ポリシーを使用するすべてのアクセス コントロール ポリシーのステータスが「失効」と示され、変更内容を反映させるにはすべてのアクセス コントロール ポリシーを再適用する必要があります。

情報については、次の各項を参照してください。

- デフォルト セット以外の変数セットをアクセス コントロール ルールにリンクさせるには、侵入防御を実行するアクセス コントロール ルールの設定（18-8 ページ）の手順を参照してください。
- デフォルト セット以外の変数セットをアクセス コントロール ポリシーのデフォルト アクションにリンクさせるには、デフォルトの処理の設定およびネットワーク トラフィックのインスペクション（12-7 ページ）を参照してください。
- 変数セットを侵入ポリシーにリンクさせるポリシーを含むアクセス コントロール ポリシーを適用するには、アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

拡張変数について

ライセンス：Protection

拡張変数を使用すると、他の方法では Web インターフェイスで設定できない機能を設定することができます。現在、FireSIGHT システムには 2 つの拡張変数だけが備わっており、そのうち USER_CONF 拡張変数のみを編集できます。

USER_CONF

USER_CONF は、Web インターフェイスで通常設定できない 1 つ以上の機能を設定するための汎用ツールです。

注意　機能の説明またはサポート担当の指示に従う場合を除き、拡張変数 USER_CONF を使用して侵入ポリシー機能を設定**しないで**ください。競合または重複する設定が存在すると、システムが停止します。

USER_CONF を編集するときには、1 行に合計 4096 文字まで入力できます。行は自動的に折り返します。変数の最大長 8192 文字、またはディスク スペースなどの物理制限に達するまで、任意の数の有効な指示または行数を含めることができます。コマンド ディレクティブでは、完全な引数の後にバックスラッシュ（\）行連結文字を使用します。

USER_CONF をリセットすると、空になります。

SNORT_BPF

SNORT_BPF はレガシー拡張変数です。バージョン 5.3.0 以降にアップグレードされる前の旧バージョンの FireSIGHT システム ソフトウェア リリースのときにシステムでこの変数が設定された場合にのみ、これが表示されます。この変数を表示または削除することだけが可能です。削除後に、編集または復元することはできません。

この変数を使用すると、Berkeley Packet Filter（BPF）を適用して、システムに到達する前のトラフィックをフィルタできました。SNORT_BPF に備わっていたフィルタリング機能を今後も適用するには、この変数の代わりにアクセス コントロール ルールを使用してください。この変数は、システム アップグレード前に存在していた設定でのみ表示されます。

ファイル リストの操作

ライセンス： Malware

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

サポートされる防御センター： DC500 を除くいずれか

ネットワークベースの拡張マルウェア対策（AMP）を使用している場合、Collective Security Intelligence クラウド によってファイルの性質が誤って認識されたときに、SHA256 ハッシュ値を使ってそのファイルを *ファイル リスト* に追加すると、その後、ファイルがより適切に検出されるようになります。ファイル リストのタイプに応じて、次の操作を実行できます。

- クラウドがクリーンの性質を割り当てた場合と同じ方法でファイルを扱うには、*クリーン リスト* にファイルを追加します。
- クラウドがマルウェアの性質を割り当てた場合と同じ方法でファイルを扱うには、*カスタム検出リスト* にファイルを追加します。

これらのファイルのブロッキング動作は手動で指定されるため、そのファイルがクラウドによってマルウェアと識別されるような場合でも、システムはマルウェア クラウド ルックアップを実行しません。ファイルの SHA 値を計算するには、**マルウェア クラウド ルックアップ** アクションと **マルウェア ブロック** アクションのどちらか、および一致するファイル タイプを使用して、ファイル ポリシー内のルールを設定する必要があることに注意してください。詳細については、ファイル ルールの操作（37-19 ページ）を参照してください。

システムのクリーン リストとカスタム検出リストは、デフォルトですべてのファイル ポリシーに含まれています。ポリシーごとに、いずれかまたは両方のリストを使用しないことを選択できます。

注意　実際にマルウェアであるファイルをこのリストに**含めない**でください。クラウドがそのファイルのマルウェアの性質を割り当てた場合、またはファイルをカスタム検出リストに追加した場合でも、システムはそれをブロックしません。

各ファイル リストには、一意の SHA-256 値を最大 10000 個まで含めることができます。ファイルをファイル リストに追加するには、次の操作を実行できます。

- イベント ビューアのコンテキスト メニューを使用して SHA-256 値を追加する。
- ファイルをアップロードする。これにより、システムはそのファイルの SHA256 値を計算してそれを追加します。
- ファイルの SHA-256 値を直接入力する。
- 複数の SHA-256 値を含むコンマ区切り値（CSV）ソース ファイルを作成してアップロードする。重複しないすべての SHA-256 値がこのファイル リストに追加されます。

ファイル リストにファイルを追加したり、ファイル リスト内の SHA-256 値を編集したり、ファイル リストから SHA-256 値を削除したりした場合、変更を有効にするには、そのリストを使用するファイル ポリシーを含むアクセス コントロール ポリシーをすべて再適用する必要があります。

ファイル リストにファイルを追加するとアクセス コントロールに影響を与えるため、ユーザは、ファイル リストのすべての側面を管理する次のいずれかを持っている必要があります。

- 管理者アクセス
- [Network Admin] または [Access Admin] アクセス権（ファイル リストを編集する場合）、[Security Approver] アクセス権（アクセス コントロール ポリシーを再適用する場合）、および [Security Analyst] または [Security Analyst（RO）] アクセス権（イベント ビューから SHA-256 値を使用してファイルを追加する場合）の組み合わせ
- [Modify Access Control Policy] および [Object Manager]（ファイル リストを編集する場合）、[Apply Access Control Policy]（アクセス コントロール ポリシーを再適用する場合）、および [Modify File Events]（イベント ビューから SHA-256 値を使用してファイルを追加する場合）権限を持つカスタム ロール。カスタム ユーザ ロールによる展開の管理（12-4 ページ）を参照してください。

ファイル リストの使用の詳細については、次のトピックを参照してください。

- コンテキスト メニューの使用（2-5 ページ）
- ファイル リストに複数の SHA-256 値をアップロードする（3-37 ページ）
- 個別のファイルをファイル リストにアップロードする（3-39 ページ）
- ファイル リストに SHA-256 値を追加する（3-39 ページ）
- ファイル リスト上のファイルの変更（3-40 ページ）
- ファイル リストからソース ファイルをダウンロードする（3-41 ページ）

ファイル リストに複数の SHA-256 値をアップロードする

ライセンス： Malware

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

サポートされる防御センター： DC500 を除くいずれか

SHA-256 値のリストと説明を含むコンマ区切り値（CSV）ソース ファイルをアップロードすることによって、複数の SHA-256 値をファイル リストに追加できます。Defense Centerはその内容を検証し、有効な SHA-256 値をファイル リストに入れます。

ソース ファイルは、ファイル名拡張子 .csv の単純なテキスト ファイルである必要があります。見出しはポンド記号（#）で始まる必要があります。これはコメントとして処理され、アップロードされません。各エントリには、1 つの SHA-256 値の後に（最大 256 個の英文字または特殊文字からなる）説明が含まれる必要があり、LF または CR+LF 改行文字で終わる必要があります。システムはエントリ内のこれ以外の情報をすべて無視します。

次の点に注意してください。

- ファイル リストからソース ファイルを削除すると、それに関連付けられているすべての SHA-256 ハッシュもファイル リストから削除されます。
- ソース ファイルのアップロードに成功した結果、10000 個を超える個別の SHA-256 値がファイル リストに含まれる場合は、複数のファイルをファイル リストにアップロードすることはできません。

- システムは、アップロード時に 256 文字を超える説明を最初の 256 文字で切り捨てます。説明にコンマを含める場合は、エスケープ文字（\）を使用する必要があります。説明が含まれていない場合、代わりにソース ファイル名が使用されます。
- すでにファイル リストに存在する SHA-256 値を含むソース ファイルをアップロードした場合、新しくアップロードされた値によって既存の SHA256 値が変更されることはありません。SHA-256 値に関連するキャプチャ済みファイル、ファイル イベント、またはマルウェア イベントを表示するとき、個々の SHA-256 値から脅威名または説明が得られます。
- システムはソース ファイル内の無効な SHA-256 値をアップロードしません。
- アップロードされた複数のソース ファイル内に同じ SHA256 値に関するエントリが含まれる場合、システムは最も新しい値を使用します。
- 1 つのソース ファイル内に同じ SHA-256 値のエントリが複数含まれる場合、システムは最後のものを使用します。
- オブジェクト マネージャ内でソース ファイルを直接編集することはできません。変更を行うには、最初にソース ファイルを直接変更し、システム上のコピーを削除した後、変更済みソース ファイルをアップロードする必要があります。詳細については、「ファイル リストからソース ファイルをダウンロードする（3-41 ページ）」を参照してください。

ソース ファイルをファイル リストにアップロードする方法：

アクセス： Admin/Any Security Analyst

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[File List] をクリックします。

[File List] セクションが表示されます。

ステップ 3　ソース ファイルからの値の追加先となるファイル リストの横にある編集アイコン（  ）をクリックします。

[File List] ポップアップ ウィンドウが表示されます。

ステップ 4　[Add by] フィールドから [List of SHAs] を選択します。

ポップアップ ウィンドウが更新され、新しいフィールドが含まれます。

ステップ 5　オプションで、[Description] フィールドにソース ファイルの説明を入力します。

説明を入力しない場合、システムはファイル名を使用します。

ステップ 6　[Browse] をクリックしてソース ファイルを参照してから、[Upload and Add List] をクリックしてリストを追加します。

ソース ファイルがファイル リストに追加されます。SHA-256 カラムには、ファイルに含まれる SHA-256 値の数がリストされます。

ステップ 7　[Save] をクリックします。

ステップ 8　ファイル リストを使用するファイル ポリシーを含んでいるすべてのアクセス コントロール ポリシーを再適用します。

ポリシーが適用されると、システムはファイル リスト内のファイルに対してマルウェア クラウド ルックアップを実行しなくなります。

個別のファイルをファイル リストにアップロードする

ライセンス： Malware

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

サポートされる防御センター： DC500 を除くいずれか

ファイル リストに追加するファイルのコピーがある場合、分析用にファイルをDefense Centerにアップロードできます。システムはファイルの SHA-256 値を計算し、ファイルをリストに追加します。SHA256 を計算するとき、システムはファイル サイズを制限しません。

Defense Centerに SHA-256 値を計算させることによってファイルを追加する方法：

アクセス： Admin/Network Admin

ステップ 1　オブジェクト マネージャの [File List] ページで、ファイルの追加場所となるクリーン リストまたはカスタム検出リストの横の編集アイコン（  ）をクリックします。

[File List] ポップアップ ウィンドウが表示されます。

ステップ 2　[Add by] フィールドから [Calculate SHA] を選択します。

ポップアップ ウィンドウが更新され、新しいフィールドが含まれます。

ステップ 3　オプションで、[Description] フィールドにファイルの説明を入力します。

説明を入力しない場合、アップロード時にファイル名が説明として使用されます。

ステップ 4　[Browse] をクリックしてソース ファイルを参照してから、[Calculate and Add SHA] をクリックしてリストを追加します。

ファイルがファイル リストに追加されます。

ステップ 5　[Save] をクリックします。

ステップ 6　ファイル リストを使用するファイル ポリシーを含んでいるすべてのアクセス コントロール ポリシーを再適用します。

ポリシーが適用されると、システムはファイル リスト内のファイルに対してマルウェア クラウド ルックアップを実行しなくなります。

ファイル リストに SHA-256 値を追加する

ライセンス： Malware

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

サポートされる防御センター： DC500 を除くいずれか

ファイルの SHA-256 値を送信して、それをファイル リストに追加できます。重複する SHA256 値は追加できません。

ヒント　イベント ビューからファイルまたはマルウェア イベントを右クリックし、コンテキスト メニューで [Show Full Text] を選択し、ファイルの SHA-256 値全体を表示してコピーします。

ファイルの SHA-256 値を手動で入力することによってファイルを追加する方法:

アクセス: Admin/Network Admin

ステップ 1　オブジェクト マネージャの [File List] ページで、ファイルの追加場所となるクリーン リストまたはカスタム検出リストの横の編集アイコン( )をクリックします。

[File List] ポップアップ ウィンドウが表示されます。

ステップ 2　[Add by] フィールドから [Enter SHA Value] を選択します。

ポップアップ ウィンドウが更新され、新しいフィールドが含まれます。

ステップ 3　[Description] フィールドにソース ファイルの説明を入力します。

ステップ 4　ファイルの SHA-256 値全体を入力するか、貼り付けます。システムでは値の部分的な一致はサポートされません。

ステップ 5　ファイルを追加するには、[Add] をクリックします。

ファイルがファイル リストに追加されます。

ステップ 6　[Save] をクリックします。

ステップ 7　ファイル リストを使用するファイル ポリシーを含んでいるすべてのアクセス コントロール ポリシーを再適用します。

ポリシーが適用されると、システムはファイル リスト内のファイルに対してマルウェア クラウド ルックアップを実行しなくなります。

ファイル リスト上のファイルの変更

ライセンス: Malware

サポートされるデバイス: すべて（シリーズ 2 または X-Series を除く）

サポートされる防御センター: DC500 を除くいずれか

ファイル リストの個々の SHA256 値を編集または削除することができます。オブジェクト マネージャ内でソース ファイルを直接編集できないことに注意してください。変更を行うには、最初にソース ファイルを直接変更し、システム上のコピーを削除した後、変更済みソース ファイルをアップロードする必要があります。詳細については、「ファイル リストからソース ファイルをダウンロードする (3-41 ページ)」を参照してください。ファイル リスト上のファイルを編集する方法:

アクセス: Admin/Network Admin

ステップ 1　オブジェクト マネージャの [File List] ページで、変更するファイルが入っているクリーン リストまたはカスタム検出リストの横の編集アイコン( )をクリックします。

[File List] ポップアップ ウィンドウが表示されます。

ステップ 2　編集する SHA256 値の横にある編集アイコン( )をクリックします。

[Edit SHA-256] ポップアップ ウィンドウが表示されます。

ヒント　リストからファイルを削除することもできます。削除するファイルの横にある削除アイコン( )をクリックしてください。

ステップ 3　[SHA256] 値または [Description] を更新します。

ステップ 4　[Save] をクリックします。

[File List] ポップアップ ウィンドウが表示されます。リスト内のファイル エントリが更新されます。

ステップ 5　[Save] をクリックします。

ステップ 6　ファイル リストを使用するファイル ポリシーを含んでいるすべてのアクセス コントロール ポリシーを再適用します。

ポリシーが適用されると、システムはファイル リスト内のファイルに対してマルウェア クラウド ルックアップを実行しなくなります。

ファイル リストからソース ファイルをダウンロードする

ライセンス： Malware

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

サポートされる防御センター： DC500 を除くいずれか

ファイル リスト上の既存のソース ファイル エントリを表示、ダウンロード、または削除できます。いったんアップロードされたソース ファイルを編集することはできません。まずファイル リストからソース ファイルを削除し、更新後のファイルをアップロードする必要があります。ソース ファイルをアップロードする方法については、ファイル リストに複数の SHA-256 値をアップロードする (3-37 ページ) を参照してください。

ソース ファイルに関連付けられたエントリ数とは、個別の SHA-256 値の数です。ファイル リストからソース ファイルを削除すると、ファイル リストに含まれる SHA-256 エントリの合計数は、ソース ファイル内の有効なエントリ数だけ減少します。

ソース ファイルをダウンロードする方法：

アクセス： Admin/Network Admin

ステップ 1　オブジェクト マネージャの [File List] ページで、ソースファイルのダウンロード対象となるクリーン リストまたはカスタム検出リストの横の編集アイコン（  ）をクリックします。

[File List] ポップアップ ウィンドウが表示されます。

ステップ 2　ダウンロードするソース ファイルの横にある表示アイコン（  ）をクリックします。

[View SHA-256's in list] ポップアップ ウィンドウが表示されます。

ステップ 3　[Download SHA List] をクリックし、プロンプトに従ってソース ファイルを保存します。

ステップ 4　[Close] をクリックします。

[File List] ポップアップ ウィンドウが表示されます。

セキュリティ ゾーンの操作

ライセンス： すべて

*セキュリティ ゾーン*は、1 つ以上のインライン、パッシブ、スイッチ型、ルーティング型、または ASA インターフェイスからなるグループです。これを使用すると、さまざまなポリシーと設定でトラフィック フローを管理および分類できます。1 つのゾーン内のインターフェイスは、複数デバイスにまたがる場合があります。また、1 つのデバイスで複数のゾーンを設定することもできます。これにより、ネットワークを複数セグメントに分割して、さまざまなポリシーをそれらに適用できます。トラフィックをセキュリティ ゾーンと照合するには、少なくとも 1 つのインターフェイスをそのセキュリティ ゾーンに割り当てる必要があり、各インターフェイスは 1 つのゾーンのみに属することができます。

セキュリティ ゾーンを使用してインターフェイスをグループ化することに加えて、アクセス コントロール ポリシー、ネットワーク検出 ルール、イベント検索など、システムの Web インターフェイスのさまざまな場所でゾーンを使用できます。たとえば、特定の送信元または宛先ゾーンにのみ適用されるアクセス コントロール ルールを作成したり、ネットワーク検出を、特定のゾーンに送受信されるトラフィックに限定したりすることができます。

セキュリティ ゾーン オブジェクトを更新すると、システムはオブジェクトの新しいリビジョンを保存します。この結果、同じセキュリティ ゾーン内に、いくつかの異なるリビジョンのセキュリティ ゾーンオブジェクトを含む管理対象デバイスが存在する場合は、接続の重複と思われる項目をログに記録できます。接続の重複が報告されていることに気づいた場合、同じリビジョンのオブジェクトを使用するよう、すべての管理対象デバイスを更新できます。オブジェクト マネージャでセキュリティ ゾーンを選択して、すべての管理対象デバイスを削除し、オブジェクトを保存し、管理対象デバイスを再び追加して、オブジェクトを再び保存します。次に、影響を受けるすべてのデバイス ポリシーを再適用します。デバイス ポリシーの適用の詳細については、デバイスへの変更の適用（4-27 ページ）を参照してください。

次のいずれかの方法でセキュリティ ゾーンを作成します。

- 初期設定時にデバイスで選択した検出モードに応じて、デバイス登録時にシステムがセキュリティ ゾーンを作成します。たとえば、パッシブ展開ではシステムはパッシブ ゾーンを作成し、インライン展開では外部ゾーンと内部ゾーンを作成します。
- 管理対象デバイスでインターフェイスを設定するときに、その場でセキュリティ ゾーンを作成できます。
- オブジェクト マネージャを使用してセキュリティ ゾーンを作成できます（[Objects] > [Object Management]）。

オブジェクト マネージャの [Security Zones] ページには、管理対象デバイスで設定されたゾーンがリストされます。また、このページには、各ゾーンのインターフェイスのタイプも表示され、各ゾーンを展開すると、どのデバイスのどのインターフェイスが各ゾーンに属するかを表示できます。

注　1 つのセキュリティ ゾーン内のすべてのインターフェイスは同じタイプ（つまり、すべてインライン、パッシブ、スイッチ型、ルーティング型、または ASA）でなければなりません。さらに、セキュリティ ゾーンを作成した後、それに含まれるインターフェイスのタイプを変更することはできません。

ASA セキュリティ コンテキストを変更して、シングル コンテキスト モードからマルチコンテキスト モード（またはその逆）に切り替えると、セキュリティ ゾーンの設定からすべてのインターフェイスが削除されます。

使用中のセキュリティ ゾーンは削除できません。インターフェイスをゾーンで追加または削除した後は、インターフェイスが存在するデバイスにデバイス設定を再適用する必要があります。また、ゾーンを使用するアクセス コントロール ポリシーおよびネットワーク検出ポリシーを再適用する必要もあります。

セキュリティ ゾーンを追加する方法:

アクセス: Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[Security Zones] を選択します。

ステップ 3　[Add Security Zone] をクリックします。

[Security Zones] ポップアップ ウィンドウが表示されます。

ステップ 4　[Name] に、ゾーンの名前を入力します。中カッコ（{}）、縦線（|）、セミコロン（;）、ポンド記号（#）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　[Type] で、ゾーンのインターフェイスのタイプを選択します。

セキュリティ ゾーンの作成後に、タイプを変更することはできません。

ステップ 6　[Device] > [Interfaces] ドロップダウン リストから、ゾーンに追加するインターフェイスを含んでいるデバイスを選択します。

ステップ 7　1 つ以上のインターフェイスを選択します。

複数のオブジェクトを選択するには、Ctrl キーと Shift キーを使用します。管理対象デバイスでインターフェイスをまだ設定していない場合は、空のゾーンを作成し、後でそこにインターフェイスを追加できます。手順10 に進みます。

ステップ 8　[Add] をクリックします。

選択したインターフェイスがゾーンに追加され、デバイス別にグループ化されます。

ステップ 9　他のデバイスのインターフェイスをゾーンに追加するには、手順 6 から 8 までを繰り返します。

ステップ 10　[Save] をクリックします。

セキュリティ ゾーンが追加されます。

暗号スイート リストの操作

ライセンス: すべて

サポートされるデバイス: シリーズ 3

暗号スイート リストは複数の暗号スイートからなるオブジェクトです。各定義済み暗号スイートの値は、SSL または TLS 暗号化セッションのネゴシエーションに使われる暗号スイートを表しています。暗号スイートおよび暗号スイート リストを SSL ルールで使用すると、クライアントとサーバが暗号スイートを使って SSL セッションをネゴシエートしたかどうかに基づいて暗号化トラフィックを制御できます。SSL ルールに暗号スイート リストを追加すると、リスト内のいずれかの暗号スイートでネゴシエートされた SSL セッションがルールに一致します。

注　Web インターフェイスでは暗号スイート リストと同じ場所で暗号スイートを使用できますが、暗号スイートを追加、変更、削除することはできません。

使用中の暗号スイート リストは削除できません。さらに、SSL ポリシーで使用される暗号スイート リストを編集した後、変更内容を有効にするには、関連するアクセス コントロール ポリシーを再適用する必要があります。

暗号スイート リストを作成する方法:

アクセス: Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[Cipher Suite List] を選択します。

ステップ 3　[Add Cipher Suites] をクリックします。

[Cipher Suite List] ポップアップ ウィンドウが表示されます。

ステップ 4　[Name] に、暗号スイート リストの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　1 つ以上の暗号スイートを選択して、[Add] をクリックします。

- 複数の暗号スイートを選択するには、Ctrl キーまたは Shift キーを使用するか、右クリックして [Select All] を選択します。
- リストに含める既存の暗号スイートを検索するにはフィルタ フィールド（  ）を使用できます。入力していくとフィールドが更新され、一致する項目が表示されます。検索ストリングをクリアするには、検索フィールドの上にあるの再ロード アイコン（  ）をクリックするか、検索フィールド内のクリア アイコン（  ）をクリックします。

ステップ 6　[Save] をクリックします。

暗号スイート リストが作成されます。

識別名オブジェクトの操作

ライセンス: すべて

サポートされるデバイス: シリーズ 3

それぞれの識別名オブジェクトは、公開鍵証明書のサブジェクトまたは発行元にリストされた識別名を表します。SSL ルールで識別名オブジェクトとグループ（オブジェクトのグループ化 (3-2 ページ)を参照）を使用すると、サブジェクトまたは発行元として識別名を含むサーバ証明書を使ってクライアントとサーバが SSL セッションをネゴシエートしたかどうかに基づき、暗号化トラフィックを制御できます。

識別名オブジェクトには、共通名属性（**CN**）を含めることができます。「CN=」なしで共通名を追加すると、システムはオブジェクトを保存する前に「CN=」を追加します。

さらに、次の表にリストされている、コンマで区切られた属性を含む識別名を追加することもできます。

表 3-7　識別名の属性

属性	説明	使用可能な値
C	Country Code	2 つの英字
CN	Common Name	最大 64 文字の英数字、バックスラッシュ (\)、ハイフン (-)、引用符 (")、アスタリスク (*)、スペース文字
O	マニュアルの構成	
OU	組織単位	

ワイルドカードとして 1 つ以上のアスタリスク (*) を属性に定義できます。共通名属性では、ドメイン名ラベルごとに 1 つ以上のアスタリスクを定義できます。ワイルド カードはそのラベル内でのみ照合されますが、ワイルド カードを使用して複数のラベルを定義できます。例については、以下の表を参照してください。

表 3-8　共通名属性のワイルドカードの例

属性	Matches	一致しない
CN=”*ample.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”exam*.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”*xamp*.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”*.example.com”	mail.example.com	example.com example.text.com ampleexam.com
CN=”*.com”	example.com ampleexam.com	mail.example.com example.text.com
CN=”*.*.com”	mail.example.com example.text.com	example.com ampleexam.com

使用中の識別名オブジェクトは削除できません。さらに、SSL ポリシーで使用される識別名オブジェクトを編集した後、変更内容を有効にするには、関連するアクセス コントロール ポリシーを再適用する必要があります。

識別名オブジェクトを追加する方法:

アクセス: Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[Distinguished Name] の下で、[Individual Objects] を選択します。

ステップ 3　[Add Distinguished Name] をクリックします。

[Distinguished Name] ポップアップ ウィンドウが表示されます。

ステップ 4　[Name] に、識別名オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　[DN] フィールドに、識別名または共通名の値を入力します。次の選択肢があります。

- 識別名を追加する場合は、表 3-7（3-45 ページ）に示されている属性をカンマで区切って含めることができます。
- 共通名を追加する場合は、複数のラベルとワイルドカードを含めることができます。

ステップ 6　[Save] をクリックします。

識別名オブジェクトが追加されます。

PKI オブジェクトの操作

ライセンス： すべて

サポートされるデバイス： シリーズ 3

PKI オブジェクトは、SSL インスペクション展開をサポートするために必要な公開鍵証明書、およびペアになった秘密鍵を表します。内部 CA オブジェクトおよび信頼できる CA オブジェクトは、認証局（CA）証明書で構成されます。また、内部 CA オブジェクトには、証明書とペアになった秘密鍵も含まれます。内部証明書オブジェクトおよび外部証明書オブジェクトは、サーバ証明書で構成されます。また、内部証明書オブジェクトには、証明書とペアになった秘密鍵も含まれます。SSL のルールでこれらのオブジェクトを使用すると、次のものを復号化できます。

- 発信トラフィック：内部 CA オブジェクトを使ってサーバ証明書を再署名することによって復号化します
- 受信トラフィック：内部証明書オブジェクトにある既知の秘密鍵を使用して復号化します

さらに、SSL ルールを作成して、次のものを使って暗号化されたトラフィックを照合することができます。

- 外部証明書オブジェクト内の証明書
- 信頼できる CA オブジェクトの CA によって署名された証明書、または信頼できる CA チェーン内で署名された証明書

証明書とキーの情報を手動で入力し、その情報を含むファイルをアップロードします。場合によっては、新しい CA 証明書や秘密キーを生成することができます。

オブジェクト マネージャで PKI オブジェクトのリストを表示すると、システムは証明書のサブジェクト識別名をオブジェクト値として表示します。証明書の完全なサブジェクト識別名を表示するには、値の上にポインタを移動してください。証明書に関する他の詳細を表示するには、PKI オブジェクトを編集します。

注　Defense Centerおよび管理対象デバイスは、内部 CA オブジェクトと内部証明書オブジェクトに保存されるすべての秘密鍵を、保存前にランダムに生成された鍵を使って暗号化します。パスワード保護されている秘密キーをアップロードすると、アプライアンスはユーザ提供のパスワードを使って秘密キーを復号化し、ランダムに生成されたキーを使ってそれを再暗号化してから保存します。

詳細については、次の項を参照してください。

- 内部認証局オブジェクトの使用（3-47 ページ）
- 信頼できる認証局オブジェクトの使用（3-52 ページ）
- 外部証明書オブジェクトの使用（3-54 ページ）
- 内部証明書オブジェクトの使用（3-55 ページ）

内部認証局オブジェクトの使用

ライセンス： すべて

サポートされるデバイス： シリーズ 3

設定されたそれぞれの内部認証局（CA）オブジェクトは、組織で制御される CA の CA 公開鍵証明書を表します。このオブジェクトは、オブジェクト名、CA 証明書、およびペアになった秘密鍵からなります。SSL ルールで内部 CA オブジェクトとグループ（オブジェクトのグループ化（3-2 ページ）を参照）を使用すると、内部 CA によってサーバ証明書に再署名することにより、発信する暗号化トラフィックを復号化できます。

注　[Decrypt - Resign] SSL ルールで内部 CA オブジェクトを参照する場合、ルールが暗号化セッションに一致すると、SSL ハンドシェイクのネゴシエート中は証明書を信頼できないという警告がユーザのブラウザに表示されることがあります。これを回避するには、信頼できるルート証明書のクライアントまたはドメイン リストに内部 CA オブジェクト証明書を追加します。

次の方法で内部 CA オブジェクトを作成できます。

- RSA ベースまたは楕円曲線ベースの既存の CA 証明書と秘密キーをインポートする
- 新しい RSA ベースの自己署名 CA 証明書と秘密キーを生成する
- RSA ベースの未署名の CA 証明書と秘密キーを生成する内部 CA オブジェクトを使用する前に、証明書に署名するために証明書署名要求（CSR）を別の CA に送信する必要があります。

署名付き証明書を含む内部 CA オブジェクトを作成した後で、CA 証明書と秘密鍵をダウンロードできるようになります。システムは、ダウンロードされた証明書と秘密キーをユーザ提供のパスワードで暗号化します。

システムで生成された場合でも、ユーザによって作成された場合でも、内部 CA オブジェクトの名前は変更できますが、他のオブジェクト プロパティは変更できません。

使用中の内部 CA オブジェクトは削除できません。さらに、SSL ポリシーで使用される内部 CA オブジェクトを編集すると、関連するアクセス コントロール ポリシーが失効します。変更を反映させるには、アクセス コントロール ポリシーを再適用する必要があります。

詳細については、次の項を参照してください。

- CA 証明書と秘密キーのインポート（3-48 ページ）
- 新しい CA 証明書と秘密キーの生成（3-49 ページ）
- 新しい署名付き証明書の取得およびアップロード（3-49 ページ）
- CA 証明書と秘密キーのダウンロード（3-51 ページ）

CA 証明書と秘密キーのインポート

ライセンス： すべて

サポートされるデバイス： シリーズ 3

X.509 v3 CA 証明書と秘密キーをインポートすることによって、内部 CA オブジェクトを設定できます。サポートされる次のいずれかの形式でエンコードされたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

秘密キー ファイルがパスワード保護されている場合は、復号化パスワードを提供できます。証明書とキーが PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

適切な証明書または鍵の情報を含んでいる、相互にペアになっているファイルのみをアップロードできます。システムはオブジェクトを保存する前にペアを検証します。

注　ルールに [Decrypt - Resign] アクションを設定すると、そのルールでは、設定されているルール条件に加えて、参照される内部 CA 証明書の暗号化アルゴリズムのタイプに基づいてトラフィックが照合されます。たとえば、楕円曲線ベースのアルゴリズムで暗号化された発信トラフィックを復号化するには、楕円曲線ベースの CA 証明書をアップロードする必要があります。詳細については、復号化アクション：さらに検査するためにトラフィックを復号化（21-11 ページ）を参照してください。

内部 CA 証明書と秘密鍵をインポートする方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[PKI] で、[Internal CAs] を選択します。

ステップ 3　[Import CA] をクリックします。

[Import Internal Certificate Authority] ポップアップ ウィンドウが表示されます。

ステップ 4　[Name] に、内部 CA オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　[Certificate Data] フィールドの上部にある [Browse] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

ステップ 6　[Key] フィールドの上部にある [Browse] をクリックして、DER または PEM でエンコードされたペアの秘密キー ファイルをアップロードします。

ステップ 7　アップロード ファイルがパスワード保護されている場合は、[Encrypted, and the password is:] チェック ボックスをオンにして、パスワードを入力します。

ステップ 8　[Save] をクリックします。

内部 CA オブジェクトが追加されます。

新しい CA 証明書と秘密キーの生成

ライセンス：すべて

サポートされるデバイス：シリーズ 3

識別情報を提供することにより、RSA ベースの自己署名 CA 証明書と秘密キーを生成するように内部 CA オブジェクトを設定できます。次の表に、証明書を生成するために提供する識別情報について説明します。

表 3-9　生成される内部 CA の属性

フィールド	使用可能な値	必須
Country Name（2 文字コード）	2 つの英字	yes
State or Province	最大 64 文字の英数字、バックスラッシュ（\）、ハイフン（-）、引用符（"）、アスタリスク（*）、ピリオド（.）、スペース文字	no
Locality or City		
マニュアルの構成		
組織単位		
Common Name		

生成される CA 証明書の有効期間は 10 年です。[Valid From] の日付は、生成の一週間前です。

自己署名 CA 証明書の生成方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[PKI] で、[Internal CAs] を選択します。

ステップ 3　[Generate CA] をクリックします。

[Generate Internal Certificate Authority] ポップアップ ウィンドウが表示されます。

ステップ 4　[Name] に、内部 CA オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　表 3-9（3-49 ページ）の説明に従って、識別属性を入力します。

ステップ 6　[Generate self-signed CA] をクリックします。

内部 CA オブジェクトが追加されます。

新しい署名付き証明書の取得およびアップロード

ライセンス：すべて

サポートされるデバイス：シリーズ 3

署名付き証明書を CA から取得することによって、内部 CA オブジェクトを設定できます。これは、次の 2 段階からなります。

- 内部 CA オブジェクトを設定するための識別情報を指定します。これにより、未署名の証明書およびペアになった秘密鍵が生成され、指定した CA に対する証明書署名要求（CSR）が作成されます。
- CA により署名付き証明書が発行されたら、それを内部 CA オブジェクトにアップロードして、未署名の証明書と置き換えます。

署名付き証明書が含まれている場合にのみ、SSL ルールで内部 CA オブジェクトを参照できます。

未署名の CA 証明書と CSR を作成する方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[PKI] で、[Internal CAs] を選択します。

ステップ 3　[Generate CA] をクリックします。

[Generate Internal Certificate Authority] ポップアップ ウィンドウが表示されます。

ステップ 4　[Name] に、内部 CA オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　表 3-9（3-49 ページ）の説明に従って、識別属性を入力します。

ステップ 6　[Generate CSR] をクリックします。

[Generate Internal Certificate Authority] ポップアップ ウィンドウが表示されます。

ステップ 7　CA に送信するために CSR をコピーします。

ステップ 8　[OK] をクリックします。

CA オブジェクトが作成されます。これを使用する前に、まず CA によって発行された署名付き証明書をアップロードする必要があることに注意してください。

CSR への応答として発行された署名付き証明書をアップロードする方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[PKI] で、[Internal CAs] を選択します。

ステップ 3　CSR を待機している未署名の証明書を含む CA オブジェクトの横の編集アイコン（  ）をクリックします。

[Edit Internal Certificate Authority] ポップアップ ウィンドウが表示されます。

ステップ 4　[Install Certificate] をクリックします。

[Install Internal Certificate Authority] ポップアップ ウィンドウが表示されます。

ステップ 5　[Certificate Data] フィールドの上部にある [Browse] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

ステップ 6　アップロードされるファイルがパスワード保護されている場合は、[Encrypted, and the password is:] チェック ボックスを選択し、パスワードを入力します。

ステップ 7　[Save] をクリックします。

CA オブジェクトに署名付き証明書が含まれ、SSL ルールでこれを参照できます。

CA 証明書と秘密キーのダウンロード

ライセンス： すべて

サポートされるデバイス： シリーズ 3

証明書および鍵の情報を含むファイルを内部 CA オブジェクトからダウンロードすることにより、CA 証明書およびペアになった秘密鍵をバックアップまたは転送できます。

注意　ダウンロードされた鍵情報は必ず安全な場所に保存してください。

システムは、内部 CA オブジェクトに保存されている秘密鍵をディスクに保存する前に、ランダムに生成された鍵を使って暗号化します。証明書および秘密鍵を内部 CA オブジェクトからダウンロードすると、システムはまず情報を復号化してから、証明書および秘密鍵の情報を含むファイルを作成します。その後、ダウンロード ファイルを暗号化するためにシステムで使われるパスワードを提供する必要があります。

注意　システム バックアップの一部としてダウンロードされる秘密鍵は、復号化されてから、非暗号化バックアップ ファイルに保存されます。詳細については、バックアップ ファイルの作成（70-2 ページ）を参照してください。

内部 CA 証明書と秘密鍵をダウンロードする方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[PKI] で、[Internal CAs] を選択します。

ステップ 3　証明書および秘密鍵をダウンロードする対象となる内部 CA オブジェクトの横の編集アイコン（）をクリックします。

[Edit Internal Certificate Authority] ポップアップ ウィンドウが表示されます。

ステップ 4　[Download] をクリックします。

[Encrypt Download File] ポップアップ ウィンドウが表示されます。

ステップ 5　[Password] および [Confirm Password] フィールドに、暗号化パスワードを入力します。

ステップ 6　[OK] をクリックします。

ファイルを保存するよう求められます。

信頼できる認証局オブジェクトの使用

ライセンス： すべて

サポートされるデバイス： シリーズ 3

設定済みの、信頼できる認証局（CA）オブジェクトはそれぞれ、組織外の信頼できる CA に属する CA 公開鍵証明書を表します。このオブジェクトは、オブジェクト名と CA 公開鍵証明書からなります。SSL ポリシーで外部 CA オブジェクトとグループ（オブジェクトのグループ化（3-2 ページ）を参照）を使用すると、信頼できる CA またはトラスト チェーン内の任意の CA によって署名された証明書を使って暗号化されたトラフィックを制御できます。

信頼できる CA オブジェクトを作成した後で、その名前を変更したり、証明書失効リスト（CRL）を追加したりすることはできますが、他のオブジェクト プロパティを変更することはできません。オブジェクトに追加できる CRL の数には制限がありません。オブジェクトにアップロード済みの CRL を変更するには、オブジェクトをいったん削除して再作成する必要があります。

使用中の信頼できる CA オブジェクトを削除することはできません。さらに、SSL ポリシーで使用されている信頼できる CA オブジェクトを編集すると、関連するアクセス コントロール ポリシーが失効します。変更を反映させるには、アクセス コントロール ポリシーを再適用する必要があります。

詳細については、次の項を参照してください。

- 信頼できる CA オブジェクトの追加（3-52 ページ）
- 信頼できる CA オブジェクトへの証明書失効リストの追加（3-53 ページ）

信頼できる CA オブジェクトの追加

ライセンス： すべて

サポートされるデバイス： シリーズ 3

X.509 v3 CA 証明書をアップロードすることによって、外部 CA オブジェクトを設定できます。次のサポートされている形式のいずれかでエンコードしたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

ファイルがパスワード保護されている場合は、復号化パスワードを提供する必要があります。証明書が PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

ファイルに適切な証明書情報が含まれる場合にのみ、CA 証明書をアップロードできます。システムはオブジェクトを保存する前に証明書を検証します。

信頼できる CA 証明書をインポートする方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[PKI] で、[Trusted CAs] を選択します。

ステップ 3　[Add Trusted CAs] をクリックします。

[Import Trusted Certificate Authority] ポップアップ ウィンドウが表示されます。

ステップ 4　[Name] に、信頼できる CA オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　[Certificate Data] フィールドの上部にある [Browse] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

ステップ 6　ファイルがパスワード保護されている場合は、[Encrypted, and the password is:] チェック ボックスをオンにして、パスワードを入力します。

ステップ 7　[OK] をクリックします。

信頼できる CA オブジェクトが追加されます。

信頼できる CA オブジェクトへの証明書失効リストの追加

ライセンス： すべて

サポートされるデバイス： シリーズ 3

信頼できる CA オブジェクトに CRL をアップロードできます。信頼できる CA オブジェクトを SSL ポリシーの中で参照すると、セッションの暗号化証明書を発行した CA がその後で証明書を取り消したかどうかに基づいて、暗号化されたトラフィックを制御できます。サポートされる次のいずれかの形式でエンコードされたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

CRL を追加した後、失効した証明書のリストを表示することができます。オブジェクトにアップロード済みの CRL を変更するには、オブジェクトをいったん削除して再作成する必要があります。

適切な CRL を含んでいるファイルのみをアップロードできます。信頼できる CA オブジェクトに追加できる CRL の数には制限がありません。ただし、CRL をアップロードした場合、別の CRL を追加する前に、オブジェクトをその都度保存する必要があります。

CRL をアップロードする方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[PKI] で、[Trusted CAs] を選択します。

ステップ 3　信頼できる CA オブジェクトの横にある編集アイコン（ ）をクリックします。

[Edit Trusted Certificate Authority] ポップアップ ウィンドウが表示されます。

ステップ 4　[Add CRL] をクリックして、DER または PEM でエンコードされた CRL ファイルをアップロードします。

ステップ 5　[OK] をクリックします。

変更が保存されます。

外部証明書オブジェクトの使用

ライセンス： すべて

サポートされるデバイス： シリーズ 3

設定済みのそれぞれの外部証明書オブジェクトは、組織に属さないサーバ公開鍵証明書を表します。このオブジェクトは、オブジェクト名と証明書からなります。SSL ルールで外部証明書オブジェクトとグループ（オブジェクトのグループ化（3-2 ページ）を参照）を使用すると、サーバ証明書で暗号化されたトラフィックを制御できます。たとえば、信頼できる自己署名サーバ証明書をアップロードできますが、信頼できる CA 証明書を使って検証することはできません。

X.509 v3 サーバ証明書をアップロードすることによって、外部証明書オブジェクトを設定できます。サポートされている次のいずれかの形式のファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

適切なサーバ証明書情報を含んでいるファイルだけをアップロードできます。システムはオブジェクトを保存する前にファイルを検証します。証明書が PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

外部証明書オブジェクトを作成した後、その名前を変更することはできますが、他のオブジェクト プロパティを変更することはできません。

使用中の外部証明書オブジェクトは削除できません。さらに、SSL ポリシーで使用されている外部証明書オブジェクトを編集すると、関連するアクセス コントロール ポリシーが失効します。変更を反映させるには、アクセス コントロール ポリシーを再適用する必要があります。

外部証明書オブジェクトを追加する方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[PKI] で、[External Certs] を選択します。

ステップ 3　[Add External Cert] をクリックします。

[Add Known External Certificate] ポップアップ ウィンドウが表示されます。

ステップ 4　[Name] に、外部証明書オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　[Certificate Data] フィールドの上部にある [Browse] をクリックして、DER または PEM でエンコードされた X.509 v3 サーバ証明書ファイルをアップロードします。

ステップ 6　[Save] をクリックします。

内部 CA オブジェクトが追加されます。

内部証明書オブジェクトの使用

ライセンス：すべて

サポートされるデバイス：シリーズ 3

設定済みのそれぞれの内部証明書オブジェクトは、組織に属するサーバ公開鍵証明書を表します。このオブジェクトは、オブジェクト名、公開鍵証明書、およびペアになった秘密鍵からなります。SSL ルールで内部証明書オブジェクトとグループ（オブジェクトのグループ化（3-2 ページ）を参照）を使用すると、既知の秘密鍵を使用して組織のいずれかのサーバに着信するトラフィックを復号化することができます。

X.509 v3 RSA ベースまたは楕円曲線ベースのサーバ証明書およびペアの秘密キーをアップロードすることにより、内部証明書オブジェクトを設定できます。サポートされている次のいずれかの形式のファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

ファイルがパスワード保護されている場合は、復号化パスワードを提供する必要があります。証明書とキーが PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

適切な証明書または鍵の情報を含んでいる、相互にペアになっているファイルのみをアップロードできます。システムはオブジェクトを保存する前にペアを検証します。

内部証明書オブジェクトを作成した後、その名前を変更することはできますが、他のオブジェクト プロパティを変更することはできません。

使用中の内部証明書オブジェクトは削除できません。さらに、SSL ポリシーで使用されている内部証明書オブジェクトを編集すると、関連するアクセス コントロール ポリシーが失効します。変更を反映させるには、アクセス コントロール ポリシーを再適用する必要があります。

内部証明書オブジェクトを追加する方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　[PKI] で、[Internal Certs] を選択します。

ステップ 3　[Add Internal Cert] をクリックします。

[Add Known Internal Certificate] ポップアップ ウィンドウが表示されます。

ステップ 4　[Name] に内部証明書オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　[Certificate Data] フィールドの上部にある [Browse] をクリックして、DER または PEM でエンコードされた X.509 v3 サーバ証明書ファイルをアップロードします。

ステップ 6　[Key] フィールドの上部にある [Browse] をクリックして、DER または PEM でエンコードされたペアの秘密キー ファイルをアップロードします。

ステップ 7　アップロードする秘密キー ファイルがパスワード保護されている場合は、[Encrypted, and the password is:] チェック ボックスをオンにして、パスワードを入力します。

ステップ 8　[Save] をクリックします。

内部証明書オブジェクトが追加されます。

位置情報オブジェクトの操作

ライセンス： FireSIGHT

サポートされるデバイス： シリーズ 3、仮想、ASA FirePOWER、

サポートされる防御センター： 任意（DC500 を除く）

設定済みの位置情報（ジオロケーション）オブジェクトは、管理対象ネットワーク上のトラフィックの送信元または宛先としてシステムで識別された 1 つ以上の国または大陸を表します。アクセス コントロール ポリシー、SSL ポリシー、イベント検索など、システムの Web インターフェイスのさまざまな場所で位置情報オブジェクトを使用できます。たとえば、特定の国が送信元/宛先であるトラフィックをブロックするアクセス コントロール ルールを作成できます。地理的な場所によるトラフィックのフィルタリングについては、ネットワークまたは地理的位置によるトラフィックの制御（15-4 ページ）を参照してください。地理的な場所による暗号化トラフィックのフィルタリングの詳細については、ネットワークまたは地理的位置による暗号化トラフィックの制御（22-4 ページ）を参照してください。

常に最新の情報を使用してネットワーク トラフィックをフィルタ処理できるように、Cisco では、位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。GeoDB の更新をダウンロードおよびインストールする方法については、地理情報データベースについて（66-30 ページ）を参照してください。

使用中の位置情報オブジェクトは削除できません。さらに、アクセス コントロール ポリシーまたは SSL ポリシーで使用される位置情報オブジェクトを編集した後、変更内容を有効にするには、関連するアクセス コントロール ポリシーを再適用する必要があります。

位置情報オブジェクトを追加する方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Objects] > [Object Management] を選択します。

[Object Management] ページが表示されます。

ステップ 2　位置情報を示す [Geolocation] を選択します。

[Geolocation Objects] ページが表示されます。

ステップ 3　[Add Geolocation] をクリックします。

[Geolocation Object] ポップアップ ウィンドウが表示されます。

ステップ 4　[Name] に、位置情報オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　位置情報オブジェクトに含める国および大陸のチェック ボックスを選択します。

大陸を選択すると、その大陸内のすべての国、および GeoDB 更新によってその大陸に今後追加されるすべての国が選択されます。大陸の下でいずれかの国を選択解除すると、その大陸が選択解除されます。国と大陸を任意に組み合わせて選択できます。

ステップ 6　[Save] をクリックします。

位置情報オブジェクトが追加されます。

デバイスの管理

Defense Centerは、FireSIGHT システムの主要コンポーネントです。FireSIGHT システムを構成するあらゆるデバイスを管理したり、ネットワーク上で検出された脅威を集約し、分析して対処するために、Defense Centerを使用できます。

Defense Centerを使用してデバイスを管理すると、以下の利点があります。

- すべてのデバイスのポリシーを一箇所から設定できるため、設定の変更が容易になります。
- さまざまなタイプのソフトウェア アップデートをデバイスにインストールできます。
- ヘルス ポリシーを管理対象デバイスに適用して、Defense Centerからデバイスのヘルス ステータスを監視できます。

Defense Centerは、侵入イベント、ネットワーク検出情報、およびデバイスのパフォーマンス データを集約して相互に関連付けます。そのため、ユーザはデバイスが相互の関連でレポートする情報を監視して、ネットワーク上で行われている全体的なアクティビティを評価することができます。

詳細については、次の項を参照してください。

- 管理の概念（4-2 ページ）では、Defense Centerを使用したデバイスの管理に関連する機能および制約事項について説明しています。
- 管理インターフェイスについて（4-4 ページ）では、トラフィック チャネルと複数の管理インターフェイスを使用してパフォーマンスを向上させる方法、および異なるネットワーク上にあるデバイス間のトラフィックを分離する方法について説明しています。
- NAT 環境での作業（4-8 ページ）では、ネットワーク アドレス変換（NAT）環境でデバイスの管理をセットアップする際の原則について説明しています。
- ハイ アベイラビリティの設定（4-9 ページ）では、運用を継続できるように 2 つのDefense Centerをハイ アベイラビリティ ペアとしてセットアップする方法について説明しています。
- デバイスの操作（4-19 ページ）では、デバイスとDefense Center間の接続を確立する方法と、無効にする方法について説明しています。また、管理対象デバイスを追加および削除する方法と、管理対象デバイスの状態を変更する方法についても説明しています。
- デバイス グループの管理（4-29 ページ）では、デバイス グループを作成する方法と、デバイス グループのデバイスを追加または削除する方法について説明しています。
- デバイスのクラスタリング（4-31 ページ）では、2 つの管理対象デバイス間でハイ アベイラビリティを確立および管理する方法について説明しています。
- デバイス設定の編集（4-53 ページ）では、ユーザが編集できるデバイス属性と、それらの属性を編集する方法について説明しています。

- スタックに含まれるデバイスの管理（4-46 ページ）では、管理対象デバイスのスタックを構成する方法と、スタックからデバイスを削除する方法について説明しています。
- センシング インターフェイスの設定（4-64 ページ）では、管理対象デバイスでインターフェイスを設定する方法について説明しています。

管理の概念

Defense Centerを使用することで、デバイス動作のほぼすべての側面を管理できます。デバイスを管理するために必要なDefense Centerは 1 つだけですが、2 つ目のDefense Centerをハイアベイラビリティ ペアの一方として使用することもできます。以下の項で、FireSIGHT システムの展開を計画する際に知っておくべき概念のいくつかを説明します。

- Defense Centerで管理できるデバイス（4-2 ページ）
- ポリシーとイベント以外の機能（4-3 ページ）
- 冗長Defense Centerの使用（4-4 ページ）

Defense Centerで管理できるデバイス

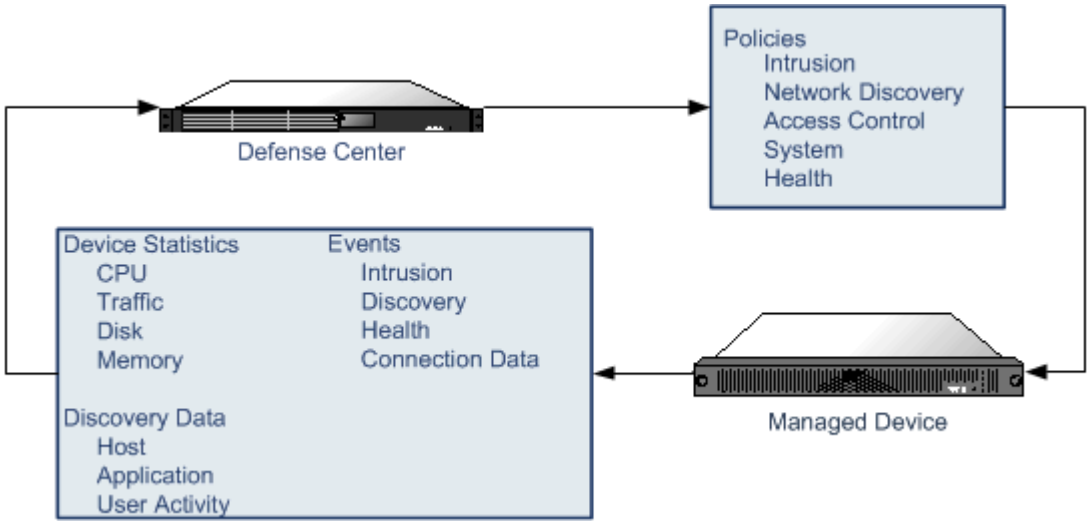
FireSIGHT システムの展開環境の中央管理ポイントとしてDefense Centerを使用することで、以下のデバイスを管理できます。

- FirePOWER 管理対象デバイス
- Cisco ASA with FirePOWER Services デバイス
- ソフトウェア ベースのデバイス（仮想デバイスや Cisco NGIPS for Blue Coat X-Series など）

注　Ciscoでは、DC500 モデルのDefense Centerで管理するデバイスを最大 3 台（ソフトウェア ベースのデバイスを含む）に制限することを推奨しています。DC500 データベースに伴う制約事項の詳細については、データベース イベントの制限の表を参照してください。

デバイスを管理する際の情報は、SSL で暗号化された TCP トンネルを介して、Defense Centerとデバイスの間で送信されます。

以下の図に、Defense Centerと管理対象デバイスの間で送信される情報をリストします。アプライアンス間で送信されるポリシーとイベントのタイプは、デバイス タイプによって異なることに注意してください。



ポリシーとイベント以外の機能

ライセンス: すべて

Defense Centerでは、ポリシーをデバイスに適用したり、デバイスからイベントを受信するだけでなく、以下のデバイス関連のタスクも実行できます。

デバイスのバックアップ

仮想管理対象デバイス、Cisco NGIPS for Blue Coat X-Series、Cisco ASA with FirePOWER Services用にバックアップ ファイルを作成したり復元することは**できません**。

物理管理対象デバイス自体からそのバックアップを実行する場合は、デバイス設定**のみ**をバックアップできます。設定データと統合ファイル(任意)をバックアップするには、管理用のDefense Centerを使用してデバイスのバックアップを実行します。

イベント データをバックアップするには、管理用のDefense Centerのバックアップを実行します。詳細については、バックアップ ファイルの作成(70-2 ページ)を参照してください。

デバイスの更新

Ciscoでは適宜、FireSIGHT システムのアップデートをリリースしています。これらのアップデートには以下が含まれます。

- 侵入ルールの更新(新しいルールや更新された侵入ルールが含まれる場合があります)
- 脆弱性データベースの更新
- ジオロケーションの更新
- ソフトウェア パッチおよびアップデート

Defense Centerを使用して、管理対象デバイスにアップデートをインストールできます。

冗長Defense Centerの使用

ライセンス： すべて

サポートされる防御センター： DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

2 つのDefense Centerをハイ アベイラビリティ ペアとしてセットアップできます。これにより、いずれか一方のDefense Centerで障害が発生したとしても、冗長機能を確保できます。ポリシーやユーザ アカウントなどが 2 つのDefense Center間で共有されます。イベントは両方のDefense Centerに自動的に送信されます。詳細については、ハイ アベイラビリティの設定（4-9 ページ）を参照してください。

管理インターフェイスについて

管理インターフェイスは、防御センターが管理するすべてのデバイスとDefense Centerの間の通信手段を提供します。アプライアンス間のトラフィック制御を正常に維持することが、展開の成功に不可欠です。

シリーズ 3 アプライアンスおよび仮想Defense Centerでは、デフォルトの設定を変更してDefense Centerまたはデバイス（あるいは両方）の管理インターフェイスを有効にすることで、アプライアンス間のトラフィックを 2 つのトラフィック チャネルに分けることができます。管理トラフィック チャネルは、すべての内部トラフィック（アプライアンスおよびシステムの管理専用のデバイス間トラフィックなど）を伝送し、イベント トラフィック チャネルは、すべてのイベント トラフィック（Web イベントなど）を伝送します。トラフィックを 2 つのチャネルに分割することにより、アプライアンス間に 2 つの接続ポイントが作成され、スループットが増加してパフォーマンスが向上します。それぞれが固有の IP アドレス（IPv4 または IPv6）とホスト名を持つ*複数の管理インターフェイス*を使用することで、トラフィック チャネルを別々に管理し、スループットを増加させることができます。

また、複数の管理インターフェイスを使用すると、1 つのDefense Centerだけを使用して、さまざまなネットワークからのトラフィックをそれぞれ分離して管理できます。特定のネットワークのトラフィックを他のネットワークのトラフィックから分離するには、管理インターフェイスを使用して特定の宛先ネットワークへの静的ルートを追加し、個々の管理インターフェイスにデバイスを登録します。同じインターフェイスで両方のトラフィック チャネルを伝送することもできますし、追加の管理インターフェイスが十分にある場合は、ネットワーク トラフィックを切り分けて各管理インターフェイスが 1 つのトラフィック チャネルだけを伝送するように設定することもできます。

通常、管理インターフェイスは、アプライアンスの背面に配置されています。詳細については、『*FireSIGHT System Installation Guide*』の「Identifying the Management Interfaces」を参照してください。管理インターフェイスの詳細については、以下の項を参照してください。

- 1 つの管理インターフェイスの使用（4-5 ページ）
- 複数の管理インターフェイスの使用（4-5 ページ）
- トラフィック チャネルの使用（4-6 ページ）
- ネットワーク ルートの使用（4-7 ページ）

1 つの管理インターフェイスの使用

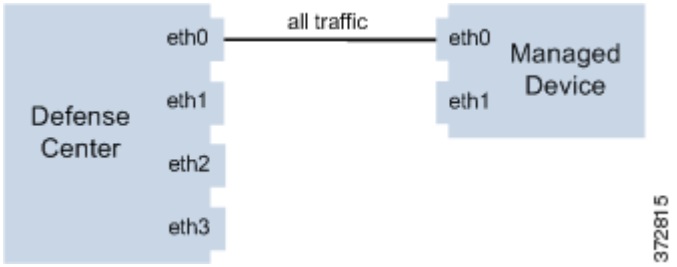
ライセンス： すべて

サポートされるデバイス： すべて

サポートされる防御センター： すべて

デバイスをDefense Centerに登録すると、Defense Center上の管理インターフェイスとデバイス上の管理インターフェイスとの間のすべてのトラフィックを伝送する単一通信チャネルが確立されます。

以下の図に、デフォルトの単一通信チャネルを示します。1 つのインターフェイスにより、管理トラフィックとイベント トラフィックの両方が 1 つの通信チャネルで伝送されます。



複数の管理インターフェイスの使用

ライセンス： すべて

サポートされるデバイス： シリーズ 3

サポートされる防御センター： シリーズ 3、仮想

複数の管理インターフェイスを有効化および設定して、それぞれに固有の IPv4 または IPv6 アドレス（および必要に応じてホスト名）を割り当て、各トラフィック チャネルを異なる管理インターフェイスに送信することによって、トラフィック スループットを著しく向上させることができます。負荷が軽い管理トラフィックの搬送用には小さなインターフェイスを構成し、負荷が大きいイベント トラフィックの搬送用には大きなインターフェイスを構成します。デバイスを別々の管理インターフェイスに登録し、同一のインターフェイスに対して両方のトラフィック チャネルを構成したり、Defense Centerによって管理されるすべてのデバイスのイベント トラフィック チャネルを専用の管理インターフェイスで伝送することができます。

Defense Center上の特定の管理インターフェイスから別のネットワーク上のデバイスまでのルートを作成できます。デフォルト以外の管理インターフェイスに他のネットワークのデバイスを登録すると、そのデバイスのトラフィックは、デフォルトの管理インターフェイス（`eth0`）に登録されているデバイスのトラフィックから分離されます。詳細については、「ネットワーク ルートの使用（4-7 ページ）」を参照してください。

デフォルト以外の管理インターフェイスは、デフォルトの管理インターフェイスと同じ機能を多数備えています（Defense Center間のハイ アベイラビリティの使用など）。ただし、次の例外があります。

- DHCP は、デフォルト（`eth0`）管理インターフェイスにのみ設定できます。追加のインターフェイス（`eth1` など）には、固有の静的 IP アドレスとホスト名が必要です。

- デフォルト以外の管理インターフェイスを使用してDefense Centerと管理対象デバイスを接続する場合、それらのアプライアンスが NAT デバイスによって分離されているならば、同じ管理インタフェースを使用するよう両方のトラフィック チャネルを設定する必要があります。
- Lights-Out 管理は、デフォルトの管理インターフェイスでのみ使用できます。
- 70xx ファミリでは、トラフィックを 2 つのチャネルに分離して、Defense Center上の 1 つ以上の管理インターフェイスにトラフィックを送信するようにそれらのチャネルを設定できます。ただし、70xx ファミリには 1 つの管理インターフェイスしかないため、デバイスは唯一の管理インターフェイス上でDefense Centerから送信されたトラフィックを受信します。

トラフィック チャネルの使用

ライセンス： すべて

サポートされるデバイス： シリーズ 3

サポートされる防御センター： シリーズ 3、仮想

1 つの管理インターフェイス上で 2 つのトラフィック チャネルを使用する場合、Defense Center と管理対象デバイスの間に 2 つの接続を作成します。同じインターフェイス上の 2 つのチャネルのうちの一方が管理トラフィックを伝送し、もう一方がイベント トラフィックを伝送します。

次の例は、同じインターフェイス上に 2 つの独立したトラフィック チャネルを持つ通信チャネルを示しています。

複数の管理インターフェイスを使用する場合、トラフィック チャネルを 2 つの管理インターフェイスに分割することによりパフォーマンスを向上できます。それによって両方のインターフェイス容量が増し、トラフィック フローが増加します。一方のインターフェイスで管理トラフィック チャネルを伝送し、もう一方のインターフェイスでイベント トラフィック チャネルを伝送します。いずれかのインターフェイスで障害が発生した場合は、すべてのトラフィックがアクティブ インターフェイスに再ルーティングされるため、接続が維持されます。

次の図は、2 つの管理インターフェイス上にある管理トラフィック チャネルとイベント トラフィック チャネルを示しています。

専用の管理インターフェイスを使用して、複数のデバイスからのイベント トラフィックのみを伝送することができます。この設定では、管理トラフィック チャネルを伝送する別の管理インターフェイスに各デバイスを登録し、すべてのデバイスからのすべてのイベント トラフィックを、Defense Center上の 1 つの管理インターフェイスで伝送します。インターフェイスで障害が発生した場合は、トラフィックがアクティブ インターフェイスに再ルーティングされるため、接続が維持されます。すべてのデバイスのイベント トラフィックが同じインターフェイスで伝送されることから、トラフィックはネットワーク間で分離されないことに注意してください。

以下の図では、2 台のデバイスが別々の管理チャネル トラフィック インターフェイスを使用し、イベント トラフィック チャネルに対しては同じ専用インターフェイスを共有しています。

1 つの管理インターフェイス上で 2 つのトラフィック チャネルを使用する場合、Defense Centerと管理対象デバイスの間に 2 つの接続を作成します。同じインターフェイス上の 2 つのチャネルのうちの一方が管理トラフィックを伝送し、もう一方がイベント トラフィックを伝送します。複数の管理インターフェイスを使用する場合は、トラフィック チャネルを 2 つの管理インターフェイスに分けることができます。それによって両方のインターフェイスの容量が増し、トラフィック フローが増えるため、さらにパフォーマンスが向上します。一方のインターフェイスで管理トラフィック チャネルを伝送し、もう一方のインターフェイスでイベント トラフィック チャネルを伝送します。いずれかのインターフェイスで障害が発生した場合は、すべてのトラフィックがアクティブ インターフェイスに再ルーティングされるため、接続が維持されます。

複数のデバイスからのイベント トラフィックだけを伝送する専用の管理インターフェイスを使用することもできます。この設定では、管理トラフィック チャネルを伝送する別の管理インターフェイスに各デバイスを登録し、すべてのデバイスからのすべてのイベント トラフィックを、Defense Center上の 1 つの管理インターフェイスで伝送します。インターフェイスで障害が発生した場合は、トラフィックがアクティブ インターフェイスに再ルーティングされるため、接続が維持されます。すべてのデバイスのイベント トラフィックが同じインターフェイスで伝送されることから、トラフィックはネットワーク間で分離されないことに注意してください。

ネットワーク ルートの使用

ライセンス： すべて

サポートされるデバイス： シリーズ 3

サポートされる防御センター： シリーズ 3、仮想

Defense Center上の特定の管理インターフェイスから別のネットワークまでのルートを作成できます。そのネットワークのデバイスをDefense Center上の指定された管理インターフェイスに登録すると、別のネットワーク上のデバイスとDefense Centerの間で独立した接続が実現されます。両方のトラフィック チャネルが同じ管理インターフェイスを使用するように設定することで、そのデバイスからのトラフィックが他のネットワーク上のデバイス トラフィックから確実に分離された状態を維持できます。ルーテッド インターフェイスはDefense Center上の他のすべてのインターフェイスから分離されているため、ルーテッド管理インターフェイスに障害が発生した場合、接続が失われます。

ヒント Ciscoでは、デフォルトの管理インターフェイス（eth0）以外の管理インターフェイスを使用してDefense Centerとそのデバイスを登録する場合は、静的 IP アドレスを使用することを推奨しています。DHCP は、デフォルトの管理インターフェイスだけでサポートされています。

Defense Centerをインストールした後に、Web インターフェイスを使用して、複数の管理インターフェイスを設定します。詳しくは、『*FireSIGHT システム ユーザ ガイド*』の「アプライアンス設定の構成」を参照してください。

次の図では、2 つのデバイスですべてのトラフィックに対して別々の管理インターフェイスを使用することにより、ネットワーク トラフィックを分離しています。さらに管理インターフェイスを追加して、デバイスごとに独立した管理トラフィック チャネル インターフェイスとイベント トラフィック チャネル インターフェイスを構成できます。

NAT 環境での作業

ライセンス： すべて

ネットワーク アドレス変換（NAT）とは、ルータを介したネットワーク トラフィックの送受信方式であり、ルータ経由でトラフィックがパススルーされるときに送信元または宛先 IP アドレスの再割り当てが行われます。NAT を使用した標準的なアプリケーションでは、プライベート ネットワーク上の複数のホストが、単一のパブリック IP アドレスを使用してパブリック ネットワークにアクセスできます。

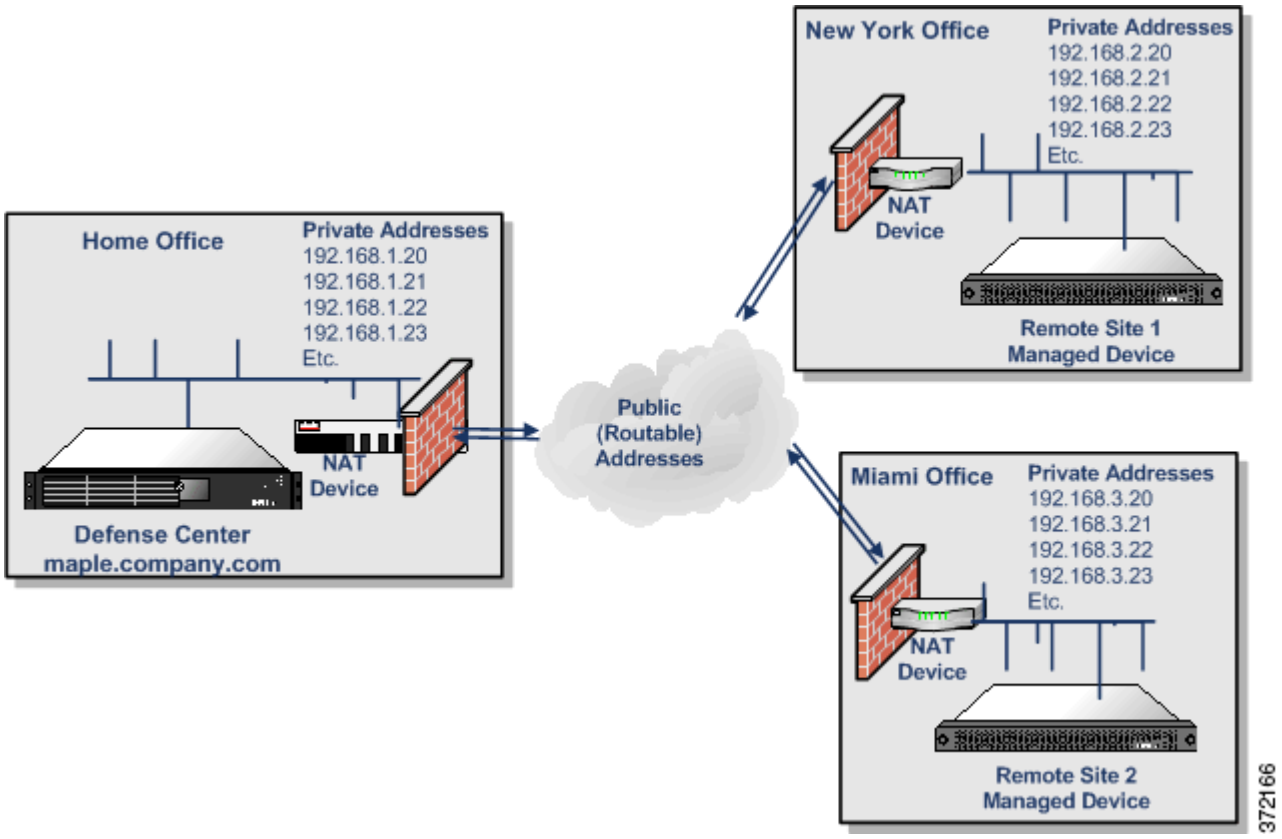
デバイスをDefense Centerに追加するときには、アプライアンス間の通信を確立します。通信を確立するために必要な情報は、その環境が NAT を使用するかどうかによって異なります。

- NAT を使用していない環境では、登録キーと IP アドレス、または両方のアプライアンスの完全修飾ドメイン名が必要です。
- NAT を使用している環境では、登録キーと一意の NAT ID が必要です。

注 NAT ID は、デバイスをDefense Centerに登録するために使用されているすべての NAT ID の間で**一意でなければなりません**。

デフォルト以外の管理インターフェイスを使用してDefense Centerと管理対象デバイスを接続していて、これらのアプライアンスが NAT デバイスによって分離されている場合、両方のトラフィック チャネルが同じ管理インターフェイスを使用するように設定する必要があります。

以下の図は、NAT 環境で 2 つのデバイスを管理するDefense Centerを示しています。登録キーは一意である必要はないため、同じ登録キーを使用して両方のデバイスを追加できます。ただし、デバイスをDefense Centerに追加する際には、**一意の** NAT ID を使用する必要があります。



ハイ アベイラビリティの設定

ライセンス: すべて

サポートされる防御センター: DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

運用の継続性を確保するために、ハイ アベイラビリティ機能を使用して、冗長Defense Centerでデバイスを管理するように指定することができます。特定の設定要素と、管理対象デバイスから両方のDefense Centerに送信されるイベント データ ストリームは、両方のDefense Centerで保持されます。一方のDefense Centerで障害が発生した場合は、もう一方のDefense Centerを使用して、中断することなくネットワークをモニタできます。

注意 システムでは一部の機能をプライマリDefense Centerに制限しているため、そのアプライアンスで障害が発生した場合は、セカンダリDefense Centerをアクティブ ステータスにプロモートする必要があります。ハイ アベイラビリティ ステータスのモニタリングおよび変更 (4-16 ページ) を参照してください。

ハイ アベイラビリティをセットアップする方法の詳細については、以下の項を参照してください。

- ハイ アベイラビリティの使用（4-10 ページ）では、ハイ アベイラビリティの実装時に共有される設定と共有されない設定をリストしています。
- ハイ アベイラビリティを実装する際のガイドライン（4-14 ページ）では、ハイ アベイラビリティを実装する場合に従わなければならないガイドラインを概説しています。
- ハイ アベイラビリティのセットアップ（4-15 ページ）では、プライマリおよびセカンダリ Defense Centerを指定する方法を説明しています。
- ハイ アベイラビリティ ステータスのモニタリングおよび変更（4-16 ページ）では、リンクされたDefense Centerのステータスを確認する方法、およびプライマリDefense Centerに障害が発生した場合にDefense Centerのロールを変更する方法を説明しています。
- ハイ アベイラビリティの無効化とデバイスの登録解除（4-18 ページ）では、リンクされた Defense Center間のリンクを完全に削除する方法を説明しています。
- ペアにされたDefense Center間での通信の一時停止（4-19 ページ）では、リンクされたDefense Center間の通信を一時停止する方法を説明しています。
- ペアにされたDefense Center間での通信の再開（4-19 ページ）では、リンクされたDefense Center間の通信を再開する方法を説明しています。

ハイ アベイラビリティの使用

ライセンス： すべて

サポートされる防御センター： DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

DC1500、DC2000、DC3500 および DC4000 はハイ アベイラビリティ構成をサポートしていますが、DC750 および仮想Defense Centerはサポートしていません。Ciscoでは、ハイ アベイラビリティ ペアの両方のDefense Centerに同じモデルを使用することを**強く**推奨しています。異なるDefense Centerモデル間にハイ アベイラビリティをセットアップ**しないでください**。

ハイ アベイラビリティ モードでは、2 つのDefense Centerがそれぞれ*プライマリ*、*セカンダリ*として指定されますが、どちらのDefense Centerに対してもポリシーやその他の変更を行うことができます。ただし、Ciscoでは、設定の変更はプライマリDefense Centerに対して**のみ**行い、セカンダリDefense Centerはバックアップとして保持することを推奨しています。

Defense Centerは、互いの設定に対する変更を定期的に更新するため、ユーザが一方のDefense Centerに対して行った変更は、もう一方のDefense Centerに 10 分以内に適用されます。（各Defense Centerには 5 分の同期サイクルが設定されていますが、このサイクル自体が最大 5 分間同期しないことがあるため、変更は 5 分のサイクル 2 回分の間に行われます。）この10 分間では、それぞれの Defense Centerの設定が異なっているように見える場合があります。

たとえば、プライマリDefense Centerでポリシーを作成し、セカンダリDefense Centerでも管理されるデバイスにそのポリシーを適用した場合、Defense Center間で通信が行われる前に、デバイスがセカンダリDefense Centerに接続する可能性があります。この場合、デバイスに適用されているポリシーは、セカンダリDefense Centerではまだ認識していないため、Defense Centerが同期するまでは、セカンダリDefense Centerに「unknown」という名前の新しいポリシーが表示されます。

また、Defense Centerの同期が行われる前の同じ期間に両方のDefense Centerに対してポリシーやその他の変更を行った場合は、Defense Centerがプライマリまたはセカンダリのどちらに指定されているかに関係なく、最後に行われた変更が優先されます。

ハイ アベイラビリティ ペアを設定する前に、以下の前提条件を確認してください。

- 両方のDefense Centerに、管理者特権が割り当てられた admin という名前のユーザ アカウントがあること。これらのアカウントは同じパスワードを使用する必要があります。
- admin アカウントの他には、2 つのDefense Centerに同じユーザ名を持つユーザ アカウントがないこと。重複するユーザ アカウントがある場合は、ハイ アベイラビリティを設定する前に、一方のユーザ アカウントを削除するか、名前を変更してください。

ハイ アベイラビリティ ペアとして設定する 2 つのDefense Centerは、信頼された同じ管理ネットワーク上に存在する必要も、同じ地理的ロケーションに存在する必要もありません。

運用の継続性を確保するためには、ハイ アベイラビリティ ペアの両方のDefense Centerがインターネットにアクセス可能である必要があります。インターネット アクセスの要件（E-2 ページ）を参照してください。特定の機能では、プライマリDefense Centerがインターネットに接続した上で、同期プロセス中にセカンダリと情報を共有します。したがって、プライマリに障害が発生した場合は、ハイ アベイラビリティ ステータスのモニタリングおよび変更（4-16 ページ）の説明に従ってセカンダリをアクティブ ステータスにプロモートする必要があります。

ハイ アベイラビリティ ペアのメンバ間で共有される設定と共有されない設定の詳細については、以下の項を参照してください。

- 共有される設定（4-11 ページ）
- ヘルス ポリシーとシステム ポリシー（4-12 ページ）
- 相関応答（4-12 ページ）
- ライセンス（4-13 ページ）
- URL Filtering および Security Intelligence（4-13 ページ）
- クラウド接続およびマルウェア情報（4-13 ページ）
- ユーザ エージェント（4-14 ページ）

共有される設定

ライセンス： すべて

サポートされる防御センター： DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

ハイ アベイラビリティ ペアのDefense Centerは、以下の情報を共有します。

- ユーザ アカウントの属性、認証設定、カスタム ユーザ ロール
- ユーザ アカウントおよびユーザ識別のための認証オブジェクトと、アクセス コントロール ルールでユーザ条件に使用可能なユーザおよびグループ
- カスタム ダッシュボード
- カスタム ワークフローおよびテーブル
- デバイス属性（デバイスのホスト名など）、デバイスが生成するイベントの保存先、デバイスが属するグループ
- アクセス コントロール、SSL、ネットワーク分析、侵入、ファイル、およびネットワーク検出ポリシー
- ローカル侵入ルール
- カスタム侵入ルールの分類
- ネットワーク検出ポリシー

- ユーザ定義のアプリケーション プロトコル ディテクタと、それらのディテクタによって検出されるアプリケーション
- アクティブ化されたカスタム フィンガープリント
- ホスト属性
- ネットワーク検出ユーザ フィードバック（注意およびホスト重要度、ネットワーク マップからのホスト、アプリケーション、ネットワークの削除、脆弱性の非アクティブ化または変更など）
- 相関ポリシーおよびルール、コンプライアンス ホワイトリスト、トラフィック プロファイル
- 変更調整スナップショットおよびレポート設定
- 侵入ルール、ジオロケーション データベース（GeoDB）、および脆弱性データベース（VDB）の更新
- 上記の設定のいずれかに関連付けられている再利用可能なオブジェクト（変数セットなど）

ヘルス ポリシーとシステム ポリシー

ライセンス： すべて

サポートされる防御センター： DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

Defense Centerおよび管理対象デバイスのヘルス ポリシーとシステム ポリシーは、ハイ アベイラビリティ ペアで共有されます。新しくアクティブ化されたDefense Centerで、ヘルス ポリシー、モジュール、ブラックリストに関する情報が同期されるように十分な時間を設けてください。

注　システム ポリシーは、ハイ アベイラビリティ ペアのDefense Centerで共有されますが、自動的には適用されません。両方のDefense Centerで同一のシステム ポリシーを使用するには、同期後にポリシーを適用します。

ハイ アベイラビリティ ペアのDefense Centerは、以下のシステムおよびヘルス ポリシー情報を共有します。

- システム ポリシー
- システム ポリシー設定（適用されるポリシーおよびその適用対象）
- ヘルス ポリシー
- ヘルス モニタリング設定（適用されるポリシーおよびその適用対象）
- ヘルス モニタリングからブラックリスト化されるアプライアンス
- 個々のヘルス モニタリング ポリシーでブラックリスト化されるアプライアンス

相関応答

ライセンス： すべて

サポートされる防御センター： DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

相関ポリシー、ルール、および応答は、Defense Centerの間で共有されますが、相関ルールとその応答の間の*関連付け*は、Defense Centerの間で共有されません。これは、相関ポリシー違反が発生した場合に重複する応答が起動されないようにするためです。

修正を相関ポリシーに関連付けられるようにするには、その前に、セカンダリDefense Centerですべてのカスタム修正モジュールをアップロードしてインストールし、修正インスタンスを設定する必要があります。運用の継続性を確保するために、プライマリDefense Centerで障害が発生した場合は、ただちにセカンダリDefense Centerで相関ポリシーを適切な応答と修正に関連付けるだけでなく、セカンダリDefense Centerの Web インターフェイスを使用してセカンダリをアクティブにする必要があります。詳細については、ハイ アベイラビリティ ステータスのモニタリングおよび変更（4-16 ページ）を参照してください。相関応答の詳細については、相関ポリシーの作成（51-49 ページ）および修復の作成（54-1 ページ）を参照してください。

セカンダリDefense Centerでルールまたはホワイトリストとその応答および修正の間の関連付けを作成していた場合、障害発生後にプライマリDefense Centerを復元する際に、必ず関連付けを削除し、プライマリDefense Centerだけが応答と修正を生成するようにしてください。

ライセンス

ライセンス： すべて

サポートされる防御センター： DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

ハイ アベイラビリティ ペアのDefense Centerは、ライセンスを**共有しません**。ペアの各メンバに同等のライセンスを追加する必要があります。詳細については、ライセンスについて（65-1 ページ）を参照してください。

URL Filtering および Security Intelligence

ライセンス： URL FilteringまたはProtection

サポートされるデバイス： シリーズ 3、仮想、X-Series、ASA FirePOWER

サポートされる防御センター： DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

URL フィルタリングとセキュリティ インテリジェンスの設定および情報は、ハイ アベイラビリティ展開のDefense Centerの間で同期されます。ただし、プライマリDefense Centerだけが、URL カテゴリおよびレピュテーション データとセキュリティ インテリジェンスのフィード更新をダウンロードします。

プライマリDefense Centerに障害が発生した場合は、セカンダリDefense Centerが URL フィルタリング クラウドとその他すべての設定済みフィード サイトにアクセスできることを確認するだけでなく、セカンダリDefense Centerの Web インターフェイスを使用してセカンダリをアクティブ にプロモートする必要もあります。詳細については、ハイ アベイラビリティ ステータスのモニタリングおよび変更（4-16 ページ）を参照してください。

クラウド接続およびマルウェア情報

ライセンス： すべてまたは Malware

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

サポートされる防御センター： DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

ハイ アベイラビリティ ペアのDefense Centerは、ファイル ポリシーおよび関連する設定を共有しますが、Collective Security Intelligence クラウド 接続とマルウェア性質はいずれも共有しません。運用の継続性を確保し、検出されたファイルのマルウェア性質が両方のDefense Centerで同じであるようにするためには、プライマリとセカンダリ両方のDefense Centerがクラウドにアクセスできなければなりません。詳細については、マルウェア対策とファイル制御について（37-2 ページ）を参照してください。

ユーザ エージェント

ライセンス： FireSIGHT

サポートされる防御センター： DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

ユーザ エージェントは同時に最大 5 つのDefense Centerに接続できます。エージェントの接続先は、プライマリDefense Centerでなければなりません。プライマリDefense Centerに障害が発生した場合、すべてのエージェントがセカンダリDefense Centerと通信できることを確認する必要があります。詳細については、「Active Directory のログインを報告するためのユーザ エージェントの使用（17-11 ページ）」を参照してください。

ハイ アベイラビリティを実装する際のガイドライン

ライセンス： すべて

サポートされる防御センター： DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

ハイ アベイラビリティを利用するには、以下の項のガイドラインに従う必要があります。

プライマリおよびセカンダリDefense Centerの要件

一方のDefense Centerをプライマリとして指定し、もう一方のDefense Centerをセカンダリとして指定する必要があります。アプライアンスがアクティブから非アクティブ化（またはその逆）に切り替わるときには、プライマリおよびセカンダリの指定はそのまま維持されます。

プライマリまたはセカンダリのどちらに指定するかに関わらず、ハイ アベイラビリティをセットアップする前に、両方のDefense Centerにポリシー、ルール、管理対象デバイスなどを設定できます。

混乱を避けるために、セカンダリDefense Centerは元の状態から開始してください。つまり、ポリシーの作成や変更、新しいルールの作成、管理対象のデバイスの設定が行われていない状態から開始します。確実にセカンダリDefense Centerが元の状態であるようにするには、工場出荷時のデフォルトに復元します。その場合、イベントと構成データもDefense Centerから削除されることに注意してください。詳細については、『*FireSIGHT System Installation Guide*』を参照してください。

バージョン要件

両方のDefense Centerで実行しているソフトウェアとルールは、同じアップデート バージョンでなければなりません。また、このソフトウェア バージョンは、管理対象デバイスのソフトウェア バージョン以降でなければなりません。

通信要件

デフォルトでは、ペアとなっているDefense Centerは、ポート 8305/tcp を使用して通信します。ポートを変更するには、管理ポートの変更（4-24 ページ）で説明している手順に従ってください。

2 つのDefense Centerが同じネットワーク セグメント上に存在する必要はありませんが、Defense Centerが互いに通信可能であり、共有するデバイスとも通信可能でなければなりません。つまり、プライマリDefense Centerは、セカンダリDefense Centerの独自の管理インターフェイスの IP アドレスでセカンダリDefense Centerと通信できること、およびその逆も可能であることが必要です。さらに、それぞれのDefense Centerが管理対象のデバイスと通信できること、あるいは管理対象デバイスがDefense Centerと通信できることも必要です。

ハイ アベイラビリティのセットアップ

ライセンス： すべて

サポートされる防御センター： DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

ハイ アベイラビリティを使用するには、一方のDefense Centerをプライマリとして指定し、同じモデルのもう一方のDefense Centerをセカンダリとして指定する必要があります。2 つのアプライアンス間のリモート管理通信を編集する方法については、リモート管理の編集（4-23 ページ）を参照してください。

注意 Ciscoでは、設定の変更はプライマリDefense Centerに対して**のみ**行い、セカンダリDefense Centerはバックアップとして使用することを推奨しています。

必ず、ハイ アベイラビリティを設定する前に、リンクするDefense Centerの間で時刻設定を同期してください。時刻を設定する方法の詳細については、時刻の同期（63-27 ページ）を参照してください。

設定されているポリシーとカスタム標準テキスト ルールの数に応じて、すべてのルールとポリシーが両方のDefense Centerに表示されるまでに 10 分程度かかることがあります。[High Availability] ページを表示して、2 つのDefense Center間のリンクのステータスを確認できます。また、[Task Status] をモニタして、プロセスが完了するタイミングを確認することもできます。ハイ アベイラビリティ ステータスのモニタリングおよび変更（4-16 ページ）を参照してください。

ハイ アベイラビリティ ペアのいずれかのDefense Centerのイメージを再生成しなければならない場合は、最初にハイ アベイラビリティ リンクを無効にします。Defense Centerのイメージを再生成した後、ハイ アベイラビリティ ペアを再確立すると、既存のDefense Centerのデータが新たに追加されたDefense Centerに同期されます。Defense Centerのイメージを再生成できない場合は（たとえば、アプライアンスに障害が発生した場合）、サポートに連絡してください。

2 つのDefense Centerのハイ アベイラビリティをセットアップするには、以下を行います。

アクセス： Admin

ステップ 1　セカンダリDefense Centerとして指定するDefense Centerにログインします。

ステップ 2　[System] > [Local] > [Registration] を選択します。

[Registration] ページが表示されます。

ステップ 3　[High Availability] をクリックします。

[High Availability] ページが表示されます。

ステップ 4　[secondary Defense Center] オプションをクリックします。

[Secondary Defense Center Setup] ページが表示されます。

ステップ 5　[Primary DC Host] テキスト ボックスに、プライマリ Defense Centerのホスト名または IP アドレスを入力します。

注意 ネットワークで IP アドレスの割り当てに DHCP を使用している場合は、IP アドレスではなく、必ずホスト名を使用してください。

ルーティング可能アドレスが管理ホストにない場合は、[Primary DC Host] フィールドを空のままにして構いません。その場合は、[Registration Key] と [Unique NAT ID] の両方のフィールドを使用します。

ステップ 6　[Registration Key] テキスト ボックスに、1 回限り使用する登録キーを入力します。

ステップ 7　必要に応じて、[Unique NAT ID] フィールドに、プライマリ Defense Centerを識別するために使用する、英数字による一意の登録 ID を入力します。スタックに含まれるデバイスの管理（4-46 ページ）は参照しないでください。詳細については、4-8 ページの「NAT 環境での作業」を参照してください。

ステップ 8　[Register] をクリックします。

成功メッセージが表示され、[Peer Manager] ページに、セカンダリ Defense Centerの現在の状態が示されます。

ステップ 9　管理者アクセス権限を持つアカウントを使用して、プライマリとして指定するDefense Centerにログインします。

ステップ 10　[System] > [Local] > [Registration] を選択します。

[Registration] ページが表示されます。

ステップ 11　[High Availability] をクリックします。

[High Availability] ページが表示されます。

ステップ 12　[primary Defense Center] オプションをクリックします。

[Primary Defense Center Setup] ページが表示されます。

ステップ 13　[Secondary DC Host] テキスト ボックスに、セカンダリ Defense Centerのホスト名または IP アドレスを入力します。

注意　ネットワークで IP アドレスの割り当てに DHCP を使用している場合は、IP アドレスではなく、必ずホスト名を使用してください。

ステップ 14　[Registration Key] テキスト ボックスに、ステップ 6 で入力した 1 回限り使用する登録キーと同じものを入力します。

ステップ 15　セカンダリ Defense Centerで一意の NAT ID を使用した場合は、ステップ 7 で入力したのと同じ登録 ID を [Unique NAT ID] テキスト ボックスに入力します。

ステップ 16　[Register] をクリックします。

成功メッセージが表示され、[Peer Manager] ページに、プライマリ Defense Centerの現在の状態が示されます。

ハイ アベイラビリティ ステータスのモニタリングおよび変更

ライセンス： すべて

サポートされる防御センター： DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

プライマリとセカンダリの防御センターを特定した後、ハイ アベイラビリティ ペアのいずれかのアプライアンスから、ローカル防御センターとそのピアに関する次の情報を確認できます。

- ピアの IP アドレスまたはホスト名
- ピアの製品モデル
- ピアのソフトウェア バージョン
- ピアのオペレーティング システム

- ハイ アベイラビリティ ペアのメンバーが最後に同期されてから経過した時間
- ローカル アプライアンスのロールとステータス（アクティブおよびプライマリ、非アクティブおよびプライマリ、非アクティブおよびセカンダリ、アクティブおよびセカンダリ）

プライマリDefense Centerに障害が発生した場合は、[High Availability] ページを使用してDefense Centerのロールを変更することもできます。システムでは以下の機能をプライマリDefense Centerに制限しているため、そのアプライアンスで障害が発生した場合は、セカンダリDefense Centerをアクティブにプロモートする必要があります。

- URL カテゴリおよびレピュテーション データの更新。詳細については、URL Filtering および Security Intelligence（4-13 ページ）を参照してください。
- セキュリティ インテリジェンス フィードの更新。詳細については、URL Filtering および Security Intelligence（4-13 ページ）を参照してください。
- 相関ルールと応答の関連付け。詳細については、相関応答（4-12 ページ）を参照してください。

ハイ アベイラビリティ ステータスを確認するには、以下を行います。

アクセス： Admin

ステップ 1　ハイ アベイラビリティを使用してリンクしたDefense Centerのいずれか一方にログインします。

ステップ 2　[System] > [Local] > [Registration] を選択します。

[Registration] ページが表示されます。

ステップ 3　[High Availability] をクリックします。

[High Availability] ページが表示されます。

ステップ 4　[High Availability Status] に、ハイ アベイラビリティ ペアのDefense Centerに関する以下の情報が一覧表示されます。

- ピアの IP アドレスまたはホスト名
- ピアの製品モデル
- ピアのソフトウェア バージョン
- ピアのオペレーティング システム
- ハイ アベイラビリティ ペアのメンバーが最後に同期されてから経過した時間
- ローカル アプライアンスのロールとステータス（アクティブおよびプライマリ、非アクティブおよびプライマリ、非アクティブおよびセカンダリ、アクティブおよびセカンダリ）
- 2 つの防御センター間でロールを切り替えるためのオプション

ステップ 5　共有機能に影響する操作が行われると、10 分以内に（各Defense Centerごとに 5 分間）、2 つのDefense Centerが自動的に同期されます。たとえば、一方のDefense Centerで新しいポリシーを作成すると、そのポリシーは 5 分以内にもう一方のDefense Centerと自動的に共有されます。ただし、ポリシーを即時に同期させる必要がある場合は、[Synchronize] をクリックします。

注　ハイ アベイラビリティ ペアとして設定されたDefense Centerからデバイスを削除し、そのデバイスを再び追加する場合、Ciscoでは、削除してから追加するまでに少なくとも 5 分間待つことを推奨しています。この間隔を空けることにより、ハイ アベイラビリティ ペアがあらかじめ再同期されることが確実になります。5 分間待たないと、1 回の同期サイクルでは、デバイスが両方のDefense Centerに追加されない場合があります。

ステップ 6　[Switch Roles] をクリックして、ローカル ロールをアクティブから非アクティブ、または非アクティブからアクティブに変更します。

プライマリまたはセカンダリの指定は変更されずに、2 つのピア間でロールが切り替わります。

ステップ 7　ツールバーの [Peer Manager] をクリックします。

[Peer Manager] ページが表示されます。

以下の情報を確認できます。

- ハイ アベイラビリティ ペアのもう一方のDefense Centerの IP アドレス
- 通信リンクのステータス（登録済みまたは登録解除済み）
- ハイ アベイラビリティ ペアの状態（有効または無効）

2 つのアプライアンス間のリモート管理通信を編集する方法については、リモート管理の編集（4-23 ページ）を参照してください。

ハイ アベイラビリティの無効化とデバイスの登録解除

ライセンス： すべて

サポートされる防御センター： DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

ハイ アベイラビリティ ペアからいずれかのDefense Centerを削除するには、その前に、この 2 つをリンクするハイ アベイラビリティ リンクを無効にする必要があります。

ハイ アベイラビリティ ペアを無効にするには、以下を行います。

アクセス： Admin

ステップ 1　ハイ アベイラビリティ ペアのいずれか一方のDefense Centerにログインします。

ステップ 2　[System] > [Local] > [Registration] を選択します。

[Registration] ページが表示されます。

ステップ 3　[High Availability] をクリックします。

[High Availability] ページが表示されます。

ステップ 4　[Handle Registered Devices] ドロップダウン リストから、以下のいずれかのオプションを選択します。

- このページでアクセスしているDefense Centerを使用してすべての管理対象デバイスを制御する場合は、[Unregister devices on the other peer] を選択します。
- もう一方のDefense Centerを使用してすべての管理対象デバイスを制御する場合は、[Unregister devices on this peer] を選択します。
- デバイスの管理を完全に停止する場合は、[Unregister devices on both peers] を選択します。

ステップ 5　[Break High Availability] をクリックします。

「Do you really want to Break High Availability?」という質問に [OK] を選択して応答すると、ハイ アベイラビリティが無効になり、選択したオプションに従って、管理対象デバイスがDefense Centerから削除されます。

別のDefense Centerを使用してハイ アベイラビリテを有効にできます。この手順については、ハイ アベイラビリティのセットアップ（4-15 ページ）を参照してください。

ペアにされたDefense Center間での通信の一時停止

ライセンス：すべて

サポートされる防御センター：DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

一時的にハイ アベイラビリティを無効にする場合は、Defense Center間の通信チャネルを無効にします。

ハイ アベイラビリティ ペアの通信チャネルを無効にするには、以下を行います。

アクセス：Admin

ステップ 1　[Peer Manager] をクリックします。

[Peer Manager] ページが表示されます。

ステップ 2　2 つのDefense Center間の通信チャネルを無効にするには、スライダをクリックします。

2 つのアプライアンス間のリモート管理通信を編集する方法については、リモート管理の編集 (4-23 ページ) を参照してください。

ペアにされたDefense Center間での通信の再開

ライセンス：すべて

サポートされる防御センター：DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

ハイ アベイラビリティを一時的に無効にした場合、Defense Center間の通信チャネルを有効にすることで、ハイ アベイラビリティを再開できます。

ハイ アベイラビリティ ペアの通信チャネルを有効にするには、以下を行います。

アクセス：Admin

ステップ 1　[Peer Manager] をクリックします。

[Peer Manager] ページが表示されます。

ステップ 2　2 つのDefense Center間の通信チャネルを有効にするには、スライダをクリックします。

2 つのアプライアンス間のリモート管理通信を編集する方法については、リモート管理の編集 (4-23 ページ) を参照してください。

デバイスの操作

ライセンス：すべて

Defense Centerを使用して、FireSIGHT システムを構成するさまざまなデバイスを管理できます。デバイスを管理するには、Defense Centerとデバイスの間に双方向の SSL 暗号化通信チャネルをセットアップします。Defense Centerはこのチャネルを使用して、ネットワーク トラフィックの分析および管理方法に関する情報をデバイスに送信します。

デバイスはトラフィックを評価すると、イベントを生成し、同じチャネルを使用してそれらのイベントをDefense Centerに送信します。

デバイスを管理する方法の詳細については、以下の項を参照してください。

- [Device Management] ページについて（4-20 ページ）
- リモート管理の設定（4-21 ページ）
- Defense Centerへのデバイスの追加（4-24 ページ）
- リモート管理の設定（4-21 ページ）
- デバイス グループの管理（4-29 ページ）
- デバイスのクラスタリング（4-31 ページ）
- デバイス設定の編集（4-53 ページ）
- センシング インターフェイスの設定（4-64 ページ）

[Device Management] ページについて

ライセンス： すべて

[Device Management] ページには、登録されたデバイス、デバイス クラスタおよびデバイス グループを管理するために使用できる、一連の情報とオプションが表示されます。このページには、現在Defense Centerに登録されているすべてのデバイスのリストが表示されます。

このアプライアンスのリストは、必要に応じて、[sort-by] ドロップダウン リストを使用してソートできます。アプライアンス リストには、ユーザが選択するカテゴリ別にグループ化されたデバイスが表示されます。以下のソート基準を使用できます。

- グループ（つまり、デバイス グループ）。詳細については、デバイス グループの管理（4-29 ページ）を参照してください。
- タイプ（つまり、デバイスに適用されるライセンスのタイプ）。詳細については、FireSIGHT システムのライセンス（65-1 ページ）を参照してください。
- モデル（つまり、Defense Centerで管理されているデバイスのモデル）
- ヘルス ポリシー。詳細については、ヘルス モニタリングの使用（68-1 ページ）を参照してください。
- システム ポリシー。詳細については、システム ポリシーの管理（63-1 ページ）を参照してください。
- アクセス コントロール ポリシー。詳細についてはアクセス コントロール ポリシーの管理（12-12 ページ）を参照してください。

デバイス グループに属するデバイスのリストは、展開または縮小表示できます。デフォルトでは、このリストは縮小表示されます。

アプライアンス リストの詳細については、以下の表を参照してください。

表 4-1　　アプライアンス リストのフィールド

フィールド	説明
名前	各デバイスのホスト名、IP アドレス、デバイス モデル、およびソフトウェア バージョンのリスト。アプライアンスの左側にあるステータス アイコンが、そのアプライアンスの現在のヘルス ステータスを示します。
License Type	管理対象デバイスで有効なライセンス。

表 4-1　アプライアンス リストのフィールド（続き）

フィールド	説明
Health Policy	デバイスに現在適用されているヘルス ポリシー。ヘルス ポリシーの名前をクリックすると、そのポリシーの読み取り専用バージョンが表示されます。既存のヘルス ポリシーを変更する方法については、正常性ポリシーの編集（68-33 ページ）を参照してください。
System Policy	デバイスに現在適用されているシステム ポリシー。システム ポリシーの名前をクリックすると、そのポリシーの読み取り専用バージョンが表示されます。詳細については、「システム ポリシーの管理（63-1 ページ）」を参照してください。
Access Control Policy	現在適用されているアクセス コントロール ポリシーへのリンク。アクセス コントロール ポリシーの管理（12-12 ページ）を参照してください。

詳細については、次の項を参照してください。

- リモート管理の設定（4-21 ページ）
- Defense Centerへのデバイスの追加（4-24 ページ）
- デバイス グループの管理（4-29 ページ）
- デバイスのクラスタリング（4-31 ページ）
- スタックに含まれるデバイスの管理（4-46 ページ）

リモート管理の設定

ライセンス： すべて

ある FireSIGHT システム アプライアンスと別のアプライアンスを相互に管理できるようにするには、その前に、2 つのアプライアンスの間に双方向の SSL 暗号化通信チャネルをセットアップする必要があります。このチャネルを使用して、両方のアプライアンスが設定とイベント情報を共有します。ハイ アベイラビリティ ピアも、このチャネルを使用します。このチャネルは、デフォルトではポート 8305/tcp に位置します。

管理対象のアプライアンス、つまりDefense Centerで管理するデバイス上には、リモート管理を設定する必要があります。リモート管理を設定した後、管理側アプライアンスの Web インターフェイスを使用して、管理対象アプライアンスを展開環境に追加できます。

この項の手順では、FirePOWER の物理アプライアンス上にリモート管理を設定する方法について説明していることに注意してください。

2 つのアプライアンス間の通信を可能にするためには、アプライアンスが互いを認識する手段を提供しなければなりません。通信を許可するために、FireSIGHT システムでは 3 つの基準を使用します。

- 通信を確立する対象のアプライアンスのホスト名または IP アドレス

  NAT 環境では、ルーティング可能なアドレスがもう一方のアプライアンスにないとしても、リモート管理を設定する際、または管理対象アプライアンスを追加する際には、ホスト名または IP アドレスのいずれかを指定する必要があります。

- 接続を識別するために自己生成される、最大 37 文字の英数字による登録キー

- FireSIGHT システムが NAT 環境で通信を確立するために利用できる、オプションの一意の英数字による NAT ID

  NAT ID は、管理対象アプライアンスを登録するために使用されているすべての NAT ID の間で**一意でなければなりません**。詳細については、NAT 環境での作業（4-8 ページ）を参照してください。

管理対象デバイスをDefense Centerに登録する際に、デバイスに適用するアクセス コントロール ポリシーを選択できます。ただし、デバイスがポリシーに準拠していない場合は、ポリシーの適用に失敗します。この不適合には、複数の要因が考えられます。たとえば、ライセンスの不一致、モデルの制限、パッシブとインラインの問題、その他の構成ミスなどです。最初のアクセス制御ポリシーが失敗すると、最初のネットワーク ディスカバリ ポリシーの適用も失敗します。障害の原因となる問題を解決した後は、アクセス制御ポリシーおよびネットワーク ディスカバリ ポリシーを手動でデバイスに適用する必要があります。アクセス コントロール ポリシーの適用に失敗する原因となる問題の詳細については、アクセス コントロール ポリシーおよびルールのトラブルシューティング（12-25 ページ）を参照してください。

ローカル アプライアンスのリモート管理を設定するには、以下を行います。

アクセス： Admin

ステップ 1　管理するデバイスの Web インターフェイスで、[System] > [Local] > [Registration] を選択します。

[Remote Management] ページが表示されます。

注意　Ciscoでは、管理ポートの値を変更しないことを**強く**推奨しています。変更する場合は、展開環境のすべてのアプライアンスで同じ変更を行わなければなりません。それには、アプライアンス間の相互通信が必要になります。詳細については、管理ポートの変更（4-24 ページ）を参照してください。

ステップ 2　[Add Manager] をクリックします。

[Add Remote Management] ページが表示されます。

ステップ 3　[Management Host] に、このアプライアンスを管理するために使用するアプライアンスの IP アドレスまたはホスト名を入力します。

ホスト名は、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前です。

NAT 環境では、管理対象アプライアンスを追加する際に IP アドレスまたはホスト名を指定する予定の場合、ここで IP アドレスまたはホスト名を指定する必要はありません。その場合、FireSIGHT システムは後で指定される NAT ID を使用して、管理対象アプライアンスの Web インターフェイス上のリモート マネージャを識別します。

注意　ネットワークで IP アドレスの割り当てに DHCP を使用している場合は、IP アドレスではなく、ホスト名を使用します。

ステップ 4　[Registration Key] フィールドに、アプライアンス間の通信をセットアップするために使用する登録キーを入力します。

ステップ 5　NAT 環境の場合は、[Unique NAT ID] フィールドに、アプライアンス間の通信をセットアップするために使用する、英数字による**一意**の NAT ID を入力します。

ステップ 6　[Save] をクリックします。

アプライアンスが相互に通信できることを確認すると、ステータスとして [Pending Registration] が表示されます。

ステップ 7　管理側アプライアンスの Web インターフェイスを使用して、このアプライアンスを展開環境に追加します。

詳細については、Defense Centerへのデバイスの追加（4-24 ページ）を参照してください。

注　NAT を使用する一部のハイ アベイラビリティ展開では、デバイスのリモート管理を有効にする際に、セカンダリDefense Centerをマネージャとして追加しなければならない場合もあります。詳細については、サポートにお問い合わせください。

リモート管理の編集

ライセンス： すべて

管理側アプライアンスのホスト名または IP アドレスを編集するには、以下の手順を使用します。また、管理側アプライアンスの表示名を変更することもできます。表示名は、FireSIGHT システムのコンテキスト内でのみ使用されます。ホスト名をアプライアンスの表示名として使用することもできますが、別の表示名を入力してもホスト名は変更されません。

デバイスが実行しているソフトウェアのバージョンが、Defense Centerで実行しているソフトウェアのメジャー バージョンより 1 つ以上低い場合、そのデバイスを追加することはできません。たとえば、Defense Centerがバージョン 5.4.0 を実行している場合、バージョン 5.3.x 以降を実行しているデバイスを追加することはできますが、バージョン 5.2.x を実行しているデバイスは追加できません。

ヒント　スライダをクリックすることで、管理対象デバイスの管理を有効または無効にできます。管理を無効化すると、防御センターとデバイス間の接続がブロックされますが、防御センターからデバイスは削除**されません**。デバイスを管理する必要がなくなった場合は、デバイスの削除（4-28 ページ）を参照してください。

リモート管理を編集するには、以下を行います。

アクセス： Admin

ステップ 1　デバイスの Web インターフェイスで、[System] > [Local] > [Registration] を選択します。

[Remote Management] ページが表示されます。

ステップ 2　リモート管理設定を編集するマネージャの横にある編集アイコン（）をクリックします。

[Edit Remote Management] ページが表示されます。

ステップ 3　[Name] フィールドで、管理側アプライアンスの表示名を変更します。

ステップ 4　[Host] フィールドで、管理側アプライアンスの IP アドレスまたはホスト名を変更します。

ホスト名は、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前です。

ステップ 5　[Save] をクリックします。

変更が保存されます。

管理ポートの変更

ライセンス： すべて

FireSIGHT システム アプライアンスは、双方向の SSL 暗号化通信チャネルを使用して通信します。このチャネルは、デフォルトではポート 8305 に位置します。

Ciscoでは、デフォルト設定のままにしておくことを**強く**推奨していますが、管理ポートがネットワーク上の他の通信と競争する場合は、別のポートを選択できます。通常、管理ポートの変更は、FireSIGHT システムのインストール時に行います。

注意　管理ポートを変更した場合は、展開環境のすべてのアプライアンスで同じ変更を行わなければなりません。それには、アプライアンス間の相互通信が必要になります。

管理ポートを変更するには、以下を行います。

アクセス： Admin

ステップ 1　デバイスの Web インターフェイスで、[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 2　[Network] をクリックします。

[Network Settings] ページが表示されます。

ステップ 3　[Remote Management Port] フィールドに、使用するポート番号を入力します。

ステップ 4　[Save] をクリックします。

管理ポートが変更されます。

ステップ 5　このアプライアンスと通信する必要がある、展開環境内のすべてのアプライアンスについて、この手順を繰り返します。

Defense Centerへのデバイスの追加

ライセンス： すべて

デバイスを管理するには、Defense Centerとデバイスの間に双方向の SSL 暗号化通信チャネルをセットアップします。Defense Centerはこのチャネルを使用して、ネットワーク トラフィックの分析方法に関する情報をデバイスに送信します。デバイスはトラフィックを評価すると、イベントを生成し、同じチャネルを使用してそれらのイベントをDefense Centerに送信します。チャネルの設定の詳細については、リモート管理の設定（4-21 ページ）を参照してください。

デバイスが実行しているソフトウェアのバージョンが、Defense Centerで実行しているソフトウェアのメジャー バージョンより 1 つ以上低い場合、そのデバイスを追加することはできません。たとえば、Defense Centerがバージョン 5.4 を実行している場合、バージョン 5.3.x 以降を実行しているデバイスは追加できますが、バージョン 5.2.x を実行しているデバイスは追加できません。

Defense Centerでデバイスを管理する前に、そのデバイスでネットワーク設定が正しく設定されていることを確認する必要があります。この確認は、一般にインストール プロセスの一環として行われます。詳細については、「管理インターフェイスの構成（64-9 ページ）」を参照してください。

IPv4 を使用しているDefense Centerとデバイスを登録しており、それらを IPv6 に変換する場合は、デバイスをいったん削除してから再登録する必要があります。

管理対象デバイスをDefense Centerに登録する際に、デバイスに適用するアクセス コントロール ポリシーを選択できます。ただし、デバイスがポリシーに準拠していない場合は、ポリシーの適用に失敗します。この不適合には、複数の要因が考えられます。たとえば、ライセンスの不一致、モデルの制限、パッシブとインラインの問題、その他の構成ミスなどです。最初のアクセス制御ポリシーが失敗すると、最初のネットワーク ディスカバリ ポリシーの適用も失敗します。障害の原因となる問題を解決した後は、アクセス制御ポリシーおよびネットワーク ディスカバリ ポリシーを手動でデバイスに適用する必要があります。アクセス コントロール ポリシーの適用に失敗する原因となる問題の詳細については、アクセス コントロール ポリシーおよびルールのトラブルシューティング（12-25 ページ）を参照してください。

デバイス クラスタまたはデバイス スタックを登録するときに、ライセンスを選択することはできますが、それらのライセンスをデバイスの登録時に適用することはできません。これは、ライセンスの不一致による劣化を回避するために、クラスタまたはスタックに適切なライセンスを実行させるための措置です。登録の完了後に、[Device Management] ページの一般プロパティ（クラスタの場合）またはスタック プロパティ（スタックの場合）でライセンスを評価できます。詳細については、デバイス クラスタの設定（4-34 ページ）またはデバイス スタックの確立（4-48 ページ）を参照してください。

シリーズ 2 デバイスを登録するときに、ライセンスを選択することはできますが、デバイスの登録時には、選択したライセンスはいずれも適用されません。シリーズ 2 デバイスでは、セキュリティ インテリジェンス フィルタリングを除き、Protection 機能が自動的に有効になります。これらの機能を無効にすることも、他のライセンスをシリーズ 2 デバイスに適用することもできません。

ヒント　デバイスの詳細な設定を変更するには、デバイスの横にある編集アイコン（ ）をクリックします。詳細については、デバイス設定の編集（4-53 ページ）およびセンシング インターフェイスの設定（4-64 ページ）を参照してください。

デバイスをDefense Centerに追加するには、以下を行います。

アクセス： Admin/Network Admin

ステップ 1　デバイスをDefense Centerの管理対象として設定します。

FirePOWER デバイスの場合は、リモート管理の設定（4-21 ページ）で説明している手順を使用します。デバイスがDefense Centerとの通信を確認すると、ステータスが [Pending Registration] として表示されます。

仮想デバイス、Cisco NGIPS for Blue Coat X-Series、および ASA FirePOWER デバイスの場合は、デバイスのコマンド ライン インターフェイス（CLI）を使用してリモート管理インターフェイスを設定します。

注　ネットワーク アドレス変換（NAT）が使用される一部のハイ アベイラビリティ展開では、セカンダリDefense Centerをマネージャとして追加しなければならない場合もあります。詳細については、サポートにお問い合わせください。

ステップ 2　Defense Centerの Web インターフェイスで、[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 3　[Add] ドロップダウン メニューから、[Add Device] を選択します。

[Add Device] ポップアップ ウィンドウが表示されます。

ステップ 4　[Host] フィールドに、追加するデバイスの IP アドレスまたはホスト名を入力します。

デバイスのホスト名は、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前です。

NAT 環境では、Defense Centerの管理対象としてデバイスを設定するときにDefense Centerの IP アドレスまたはホスト名をすでに指定した場合、デバイスの IP アドレスまたはホスト名を指定する必要はありません。詳細については、NAT 環境での作業（4-8 ページ）を参照してください。

注意　ネットワークで IP アドレスの割り当てに DHCP を使用している場合は、IP アドレスではなく、ホスト名を使用します。

ステップ 5　[Registration Key] フィールドに、Defense Centerの管理対象としてデバイスを設定したときに使用したのと同じ登録キーを入力します。

ステップ 6　（任意）[Group] ドロップダウン リストからデバイス グループを選択し、そのグループにデバイスを追加します。

デバイス グループの詳細については、デバイス グループの管理（4-29 ページ）を参照してください。

ステップ 7　[Access Control Policy] ドロップダウン リストから、デバイスに適用する初期ポリシーを選択します。

- [Default Access Control] ポリシーは、すべてのトラフィックをネットワークからブロックします。
- [Default Intrusion Prevention] ポリシーは、Balanced Security and Connectivity 侵入ポリシーにも合格したすべてのトラフィックを許可します。
- [Default Network Discovery] ポリシーは、すべてのトラフィックを許可し、ネットワーク検出のみでトラフィックを検査します。
- 既存のユーザ定義アクセス コントロール ポリシーを選択することもできます。

詳細については、アクセス コントロール ポリシーの管理（12-12 ページ）を参照してください。

ステップ 8　デバイスに適用するライセンスを選択します。次の点に注意してください。

- ControlMalware、および URL Filtering ライセンスには、Protection ライセンスが必要です。
- VPN ライセンスは、仮想デバイス、Cisco NGIPS for Blue Coat X-Series、または ASA FirePOWER デバイスで有効にすることはできません。
- Cisco NGIPS for Blue Coat X-Series では、Control ライセンスを有効にできません。
- 仮想デバイスや ASA FirePOWER デバイスでは Control ライセンスを有効にすることができますが、これらのデバイスは Fast-Path ルール、スイッチング、ルーティング、スタック構成、クラスタリングを**サポートしていません**。
- クラスタを構成するデバイスでのライセンス設定を変更することはできません。
- スタックに含まれるデバイスの場合、アプライアンス エディタの [Stack] ページで、スタックに対してラインセンスを有効または無効にします。

- シリーズ 2 デバイスを登録する場合、デバイスの登録時に、選択したライセンスはいずれも適用されません。シリーズ 2 デバイスでは、セキュリティ インテリジェンス フィルタリングを除き、Protection 機能が自動的に有効になります。これらの機能を無効にすることも、他のライセンスをシリーズ 2 デバイスに適用することもできません。

詳細については、FireSIGHT システムのライセンス（65-1 ページ）を参照してください。

ステップ 9　デバイスをDefense Centerの管理対象として設定するときに、NAT ID を使用してデバイスを識別した場合は、[Advanced] セクションを展開して、[Unique NAT ID] フィールドに同じ NAT ID を入力します。

ステップ 10　デバイスにDefense Centerへのパケット転送を許可するには、[Transfer Packets] チェック ボックスをオンにします。

このオプションは、デフォルトで有効です。無効にすると、Defense Centerへのパケット転送が完全に禁止されます。

ステップ 11　[Register] をクリックします。

デバイスがDefense Centerに追加されます。Defense Centerがデバイスのハートビートを確認して通信を確立するまでに、最大 2 分かかる場合があります。

デバイスへの変更の適用

ライセンス： すべて

デバイス、デバイス クラスタ、またはデバイス スタックの設定に変更を加えた後、それらの変更を適用するまでは、システム全体に変更が反映されません。デバイスが変更適用前の状態でなければ、このオプションは無効になります。

注意　構成の一部を適用するときに、Snort プロセスの再開が要求され、これにより一時的にトラフィック検査が中断します。この検査中にトラフィックがドロップされるか、それ以上検査が行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。Snort プロセスを再開する構成（1-8 ページ）を参照してください。

ヒント　デバイスの変更を適用するには、[Device Management] ページまたはアプライアンス エディタの [Interfaces] タブを使用します。

変更をデバイスに適用するには、以下を行います。

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　変更を適用するデバイスの横にある適用アイコン（）をクリックします。

ステップ 3　プロンプトが出されたら、[Apply] をクリックします。

デバイスの変更が適用されます。

ヒント　必要に応じて、[Apply Device Changes] ダイアログ ボックスで [View Changes] をクリックします。新しいブラウザ ウィンドウに [Device Management Revision Comparison Report] ページが表示されます。詳細については、デバイス管理のリビジョン比較レポートの使用（4-28 ページ）を参照してください。

ステップ 4　[OK] をクリックします。

[Device Management] ページに戻ります。

デバイス管理のリビジョン比較レポートの使用

ライセンス：すべて

デバイス管理の比較レポートを使用して、変更を確認してから、アプライアンスに適用できます。このレポートには、現在のアプライアンスの設定と、変更適用後のアプライアンスの設定との間の差異がすべて表示されます。これにより、設定の潜在的なエラーを検出することができます。

変更適用前と適用後のアプライアンスを比較するには、以下を行います。

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　変更を適用するアプライアンスの横にある適用アイコン（  ）をクリックします。

[Apply Device Changes] ポップアップ ウィンドウが表示されます。アプライアンスが変更適用前の状態でなければ、適用アイコンは無効になります。

ステップ 3　[View Changes] をクリックします。

新しいウィンドウに [Device Management Revision Comparison Report] ページが表示されます。

ステップ 4　[Previous] と [Next] をクリックして、現在のアプライアンスの設定と変更適用後のアプライアンスの設定との間のすべての差異を確認します。

ステップ 5　必要に応じて、レポートの PDF バージョンを生成するには、[Comparison Report] をクリックします。

デバイスの削除

ライセンス：すべて

デバイスを管理する必要がなくなった場合、Defense Centerからそのデバイスを削除できます。デバイスを削除すると、Defense Centerとそのデバイスとの間のすべての通信が切断されます。後日、削除したデバイスを再び管理するには、もう一度そのデバイスをDefense Centerに追加する必要があります。

注　ハイ アベイラビリティ ペアとして設定されたDefense Centerからデバイスを削除し、そのデバイスを再び追加する場合、Ciscoでは、削除してから追加するまでに少なくとも 5 分間待つことを推奨しています。この間隔を空けることにより、ハイ アベイラビリティ ペアが確実に再同期して、両方のDefense Centerが削除を認識します。5 分間待たないと、1 回の同期サイクルでは、デバイスが両方のDefense Centerに追加されない場合があります。

デバイスをDefense Centerから削除するには、以下を行います。

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　削除するデバイスの横にある削除アイコン（ ）をクリックします。

プロンプトが出されたら、デバイスを削除することを確認します。デバイスとDefense Centerとの間の通信が切断され、デバイスが [Device Management] ページから削除されます。デバイスのシステム ポリシーにより、デバイスで NTP を介してDefense Centerから時刻が受信されるようになっている場合、デバイスはローカル時刻の管理に戻ります。

デバイス グループの管理

ライセンス： すべて

Defense Centerでデバイスをグループ化すると、複数のデバイスへのポリシーの適用やアップデートのインストールを簡単に行えます。グループに属するデバイスのリストは、展開または縮小表示できます。デフォルトでは、このリストは縮小表示されます。

詳細については、次の項を参照してください。

- デバイス グループの追加（4-29 ページ）
- デバイス グループの編集（4-30 ページ）
- デバイス グループの削除（4-31 ページ）

デバイス グループの追加

ライセンス： すべて

以下の手順では、デバイス グループを追加して、複数のデバイスへのポリシーの適用やアップデートのインストールを簡単に行う方法について説明します。

スタック内またはクラスタ内のプライマリ デバイスをグループに追加すると、両方のデバイスがグループに追加されます。デバイスのスタック構成またはクラスタ構成を解除しても、これらのデバイスは両方ともグループに属したままになります。

デバイス グループを作成してグループにデバイスを追加するには、以下を行います。

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　[Add] ドロップダウン メニューから、[Add Group] を選択します。

[Add Group] ポップアップ ウィンドウが表示されます。

ステップ 3　[Name] フィールドに、グループの名前を入力します。

ステップ 4　[Available Devices] から、デバイス グループに追加するアプライアンスを 1 つ以上選択します。複数のアプライアンスを選択するには、Ctrl キーまたは Shift キーを押しながらクリックします。

ステップ 5　[Add] をクリックして、選択したアプライアンスをデバイス グループに追加します。

ステップ 6　[OK] をクリックします。

デバイス グループが追加されます。

デバイス グループの編集

ライセンス：すべて

任意のデバイス グループに含まれるデバイス一式を変更できます。アプライアンスが現在グループに属している場合は、現行のグループから削除してからでないと、アプライアンスを新しいグループに追加することはできません。

アプライアンスを新しいグループに移動しても、そのアプライアンスのポリシーが、新しいグループに既に適用されているポリシーに変更される訳ではありません。デバイスのポリシーを変更するには、新しいポリシーをデバイスまたはデバイス グループに適用する必要があります。

スタック内またはクラスタ内のプライマリ デバイスをグループに追加すると、両方のデバイスがグループに追加されます。デバイスのスタック構成またはクラスタ構成を解除しても、これらのデバイスは両方ともグループに属したままになります。

デバイス グループを編集するには、以下を行います。

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　編集するデバイス グループの横にある編集アイコン（ ）をクリックします。

[Edit Group] ポップアップ ウィンドウが表示されます。

ステップ 3　必要に応じて、[Name] フィールドに、グループの新しい名前を入力します。

ステップ 4　[Available Devices] から、デバイス グループに追加するアプライアンスを 1 つ以上選択します。複数のアプライアンスを選択するには、Ctrl キーまたは Shift キーを押しながらクリックします。

ステップ 5　[Add] をクリックして、選択したアプライアンスをデバイス グループに追加します。

ステップ 6　選択したアプライアンスをデバイス グループから削除するには、削除アイコン（ ）をクリックします。

ステップ 7　[OK] をクリックします。

デバイス グループの変更が保存されます。

デバイス グループの削除

ライセンス： すべて

削除するデバイス グループにデバイスが含まれている場合、それらのデバイスは [Device Management] ページの [Ungrouped] カテゴリに移動されます。Defense Centerからは削除されません。

デバイス グループを削除するには、以下を行います。

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　削除するデバイス グループの横にある削除アイコン（ ）をクリックします。

ステップ 3　プロンプトが出されたら、デバイス グループを削除することを確認します。

デバイス グループが削除されます。

デバイスのクラスタリング

ライセンス： Control

サポートされるデバイス： シリーズ 3

デバイスのクラスタリング（ハイ アベイラビリティとも呼ばれます）を利用することで、2 つのピア デバイス間または 2 つのデバイス スタック間のネットワーキング機能と構成データの冗長性を確立できます。デバイス スタックを構成する方法の詳細については、スタックに含まれるデバイスの管理（4-46 ページ）を参照してください。

2 つのピア デバイスまたは 2 つのピア デバイス スタックでクラスタを構成し、そのクラスタを単一の論理システムとして、ポリシーの適用、システムの更新、および登録を行うことで、構成の冗長性を確立できます。その他の構成データは、システムによって自動的に同期されます。

クラスタリングの要件

デバイス クラスタを構成するには、両方のデバイスまたは両方のデバイス スタックのプライマリ メンバが同じモデルであり、同一の銅線またはファイバ インターフェイスを備えていなければなりません。両方のデバイスまたはデバイス スタックが同じソフトウェアを実行し、同じライセンスが有効になっていることも要件となります。デバイス スタックのハードウェア構成は同一でなければなりませんが、インストール済みのマルウェア ストレージ パックについてはその限りではありません。たとえば、3D8290 と 3D8290 でクラスタを構成する場合、一方のスタックに、マルウェア ストレージ パックがインストールされているデバイスがなくても、あるいは 1 つまたはすべてのデバイスにマルウェア ストレージ パックがインストールされていても構いま

せん。デバイスが NAT ポリシーのターゲットとなっている場合、両方のピアに同じ NAT ポリシーを適用する必要があります。デバイス クラスタを構成した後は、クラスタを構成する個々のデバイスのライセンス オプションを変更することはできませんが、クラスタ全体のライセンスは変更できます。詳細については、「デバイス クラスタの設定（4-34 ページ）」を参照してください。

注意 Ciscoから提供されたものではないハード ドライブをデバイスに取り付けないでください。サポートされていないハード ドライブを取り付けると、デバイスが破損する可能性があります。マルウェア ストレージ パック キットは、Ciscoから**のみ**購入でき、8000 シリーズ デバイスで**のみ**使用できます。マルウェア ストレージ パック のサポートが必要な場合は、サポートにお問い合わせください。詳細については、『*FireSIGHT System Malware Storage Pack Guide*』を参照してください。

クラスタのフェールオーバーおよびメンテナンス モード

デバイス クラスタのフェールオーバーは、手動または自動で行われます。手動でフェールオーバーをトリガーするには、クラスタを構成するデバイスまたはスタックのいずれかでメンテナンス モードを開始します。メンテナンス モードの詳細については、クラスタを構成するデバイスのメンテナンス モードの開始（4-39 ページ）を参照してください。

自動フェールオーバーは、アクティブ デバイスまたはアクティブ スタックの正常性が損なわれた場合、システム更新時、または管理権限によりデバイスがシャットダウンされた場合に発生します。また、自動フェールオーバーは、アクティブ デバイスまたはデバイス スタックで NMSB 障害、NFE 障害、ハードウェア障害、ファームウェア障害、重大なプロセス障害、ディスク フル エラー、または 2 つのスタック型デバイス間のリンク障害が起きた場合にも発生します。バックアップ デバイスまたはバックアップ スタックの正常性が同じように損なわれている場合は、フェールオーバーは行われず、クラスタはデグレード状態になります。また、いずれかのデバイスまたはデバイス スタックがメンテナンス モードになっている場合も、フェールオーバーは行われません。アクティブ スタックからスタック ケーブルを切断すると、そのスタックはメンテナンス モードに入ることに注意してください。アクティブ スタックのセカンダリ デバイスをシャットダウンした場合も、スタックはメンテナンス モードに入ります。

注 アクティブ クラスタのメンバーがメンテナンス モードになり、アクティブ ロールが他のクラスタ メンバーにフェールオーバーされた場合、元のアクティブ クラスタのメンバーは、通常動作に復帰したときに自動的にアクティブ ロールを再要求しません。

ポリシーおよび更新の適用

ポリシーを適用する際には、個々のデバイスやデバイス スタックではなく、デバイス クラスタにポリシーを適用します。ポリシーの適用が失敗すると、システムはいずれのデバイスまたはスタックにもポリシーを適用しません。ポリシーは最初にアクティブ デバイスまたはスタックに適用されてから、バックアップに適用されます。したがって、クラスターでは常に、ピアのいずれかがネットワーク トラフィックを処理しています。

更新は、個々のデバイスやスタックが受信するのではなく、クラスタを構成するデバイスが単一のエンティティとして受信します。更新が開始されると、システムは最初にバックアップ デバイスまたはスタックに更新を適用します。それによって、バックアップ デバイスまたはスタックはメンテナンス モードに入ります。この状態は、必要なプロセスが再開してデバイスがトラフィックの処理を再び開始するまで維持されます。システムは、アクティブなデバイスまたはスタックに更新を適用し、同じプロセスを行います。

デバイス クラスタなしの冗長性の確立

通常は、Cisco冗長性プロトコル（SFRP）を使用することで、デバイス クラスタを構成することなく、レイヤ 3 の冗長性を実現できます。SFRP を使用すると、デバイスは指定された IP アドレスに対する冗長ゲートウェイとして機能することが可能になります。ネットワーク冗長性では、2 つのデバイスまたは 2 つのスタックが同一のネットワーク接続を提供するように設定することで、ネットワーク上の他のホストに対する接続を維持できます。SFRP の詳細については、SFRP の設定（7-8 ページ）を参照してください。

デバイスのハイ アベイラビリティを設定する方法は、FireSIGHT システム展開（パッシブ、インライン、ルーテッド、またはスイッチド）に応じて決定します。同時に複数のロールを持たせてシステムを展開することもできます。4 つの展開タイプのうち、冗長性をもたらすためにデバイスまたはスタックのクラスタリングが必要になるのは、パッシブ展開のみです。他の展開タイプでは、デバイス クラスタを使用しても使用しなくてもネットワーク冗長性を確立できます。以下の項で、各タイプの展開でのハイ アベイラビリティの概要を説明します。

パッシブ展開での冗長性

一般に、パッシブ インターフェイスは中央スイッチのタップ ポートに接続されます。この場合、スイッチを通過するトラフィックのすべてを、パッシブ インターフェイスで分析することが可能になります。複数のデバイスが同じタップ フィードに接続されている場合、システムはそれぞれのデバイスからイベントを生成します。クラスタを構成するデバイスはアクティブまたはバックアップのいずれかとして機能するため、システムはシステム障害が発生したとしてもトラフィックを分析できると同時に、重複するイベントを防止できます。

インライン展開での冗長性

インライン セットは、自身を通過するパケットのルーティングを制御できないため、展開環境で常にアクティブになっていなければなりません。したがって、冗長性を確立できるかどうかは、外部システムがトラフィックを適切にルーティングするかどうかに依存します。冗長インライン セットは、デバイス クラスタを使用しても使用しなくても設定できます。

冗長インライン セットを配置するには、循環ルーティングを防止する一方で、トラフィックがインラインセットのいずれか 1 つだけを通過できるようにネットワーク トポロジーを設定します。インライン セットのいずれかで障害が発生すると、周辺ネットワーク インフラストラクチャがゲートウェイ アドレスへの接続が切断されたことを検出し、ルートを調整して冗長セット経由でトラフィックを送信します。

ルーテッド展開での冗長性

IP ネットワーク内のホストは、既知のゲートウェイ アドレスを使用してトラフィックをさまざまなネットワークに送信する必要があります。ルーテッド展開で冗長性を確立するには、ルーテッド インターフェイスがゲートウェイ アドレスを共有し、そのアドレスに対するトラフィックを常に 1 つのインターフェイスだけが処理するようにしなければなりません。そのためには、仮想ルータで同じ数の IP アドレスを維持する必要があります。1 つのインターフェイスがアドレスをアドバタイズします。そのインターフェイスがダウンすると、バックアップ インターフェイスがアドレスのアドバタイズを開始します。

クラスタに含まれていないデバイスの場合は、SFRP を使用して、複数のルーテッド インターフェイス間で共有されるゲートウェイの IP アドレスを設定することで、冗長性を確立します。SFRP は、デバイス クラスタを使用しても使用しなくても設定できます。また、OSPF や RIP などの動的ルーティングを使用して冗長性を確立することもできます。

スイッチド展開での冗長性

スイッチド展開では、Spanning Tree Protocol（STP）を使用して冗長性を確立します。STP は、ブリッジ型ネットワーク トポロジを管理するプロトコルです。このプロトコルは、バックアップ リンクを設定することなく、冗長リンクでスイッチド インターフェイスの自動バックアップを

行えるように設計されています。スイッチド展開でのデバイスは、STP に依存して、冗長インターフェイス間のトラフィックを管理します。同じブロードキャスト ネットワークに接続されている 2 つのデバイスは、STP によって計算されたトポロジに基づいてトラフィックを受信します。STP を有効にする方法の詳細については、仮想スイッチの詳細設定（6-8 ページ）を参照してください。

注　Cisco では、デバイス クラスタに展開する予定の仮想スイッチを設定する場合は、STP を有効にすることを強く推奨しています。

デバイスおよびスタックのクラスタリングの詳細については、以下の項を参照してください。

- デバイス クラスタの設定（4-34 ページ）
- デバイス クラスタの編集（4-36 ページ）
- クラスタ内の個々のデバイスの設定（4-37 ページ）
- クラスタ内の個々のデバイス スタックの設定（4-37 ページ）
- クラスタを構成するデバイスでのインターフェイスの設定（4-38 ページ）
- クラスタ内のアクティブ ピアの切り替え（4-39 ページ）
- クラスタを構成するデバイスのメンテナンス モードの開始（4-39 ページ）
- クラスタを構成するスタック内のデバイスの交換（4-40 ページ）
- クラスタ状態共有の設定（4-41 ページ）
- クラスタ状態共有のトラブルシューティング（4-43 ページ）
- クラスタを構成するデバイスの分離（4-46 ページ）
- SFRP の設定（7-8 ページ）
- HA リンク インターフェイスの設定（4-68 ページ）

デバイス クラスタの設定

ライセンス： Control

サポートされるデバイス： シリーズ 3

デバイス クラスタを確立する前に、以下の前提条件を満たす必要があります。

- 各デバイスまたはスタック内の各プライマリ デバイスにインターフェイスを設定します。
- クラスタに含める各デバイスまたはデバイス スタック内のプライマリ メンバは、同じモデルであり、同一の銅線またはファイバ インターフェイスを備えている必要があります。
- 両方のデバイスまたはデバイス スタックが正常なヘルス ステータスであり、同じソフトウェアを実行し、同じライセンスが有効になっている必要があります。詳細については、「ヘルス モニタの使用（68-45 ページ）」を参照してください。特に、デバイスでのハードウェア障害は許容されません。ハードウェア障害が発生すると、デバイスがメンテナンス モードに入り、フェールオーバーがトリガーされます。
- デバイスとスタックを混在させてクラスタを構成することはできません。単一のデバイスと単一のデバイスでクラスタを構成するか、ハードウェア構成が同じ（ただし、マルウェア ソフトウェア パックの有無を除く）デバイス スタックとデバイス スタックでクラスタを構成する必要があります。たとえば、3D8290 と 3D8290 でクラスタを構成する場合、一方のスタックに、マルウェア ストレージ パックがインストールされているデバイスがなくても、あ

るいは 1 つまたはすべてのデバイスにマルウェア ストレージ パックがインストールされていても構いません。マルウェア ストレージ パックの詳細については、『*FireSIGHT System Malware Storage Pack Guide*』を参照してください。

注意 Ciscoから提供されたものではないハード ドライブをデバイスに取り付けないでください。サポートされていないハード ドライブを取り付けると、デバイスが破損する可能性があります。マルウェア ストレージ パック キットは、Ciscoから**のみ**購入でき、8000 シリーズ デバイスで**のみ**使用できます。マルウェア ストレージ パック のサポートが必要な場合は、サポートにお問い合わせください。詳細については、『*FireSIGHT System Malware Storage Pack Guide*』を参照してください。

- デバイスが NAT ポリシーのターゲットとなっている場合、両方のピアに同じ NAT ポリシーを適用する必要があります。

デバイス クラスタを確立する際には、デバイスまたはスタックのうちの一方をアクティブとして指定し、もう一方をバックアップとして指定します。システムは、マージした設定を、クラスタを構成するデバイスに適用します。競合が存在する場合、システムはアクティブとして指定されたデバイスまたはスタックの設定を適用します。

デバイス クラスタを構成した後は、クラスタを構成する個々のデバイスのライセンス オプションを変更することはできませんが、クラスタ全体のライセンスは変更できます。詳細については、「デバイス クラスタの編集（4-36 ページ）」を参照してください。スイッチド インターフェイスまたはルーテッド インターフェイスで設定しなければならないインターフェイス属性がある場合、システムはクラスタを確立しますが、そのステータスを保留中に設定します。ユーザが必要な属性を設定した後、システムはデバイス クラスタを完成させて、正常なステータスに設定します。

デバイスまたはスタックを、クラスタを構成するペアとして設定すると、そのペアは、[Device Management] ページで単一のデバイスとして扱われます。デバイス クラスタには、アプライアンスのリストでクラスタ アイコン（ ）が表示されます。ユーザが行った設定変更は、いずれもクラスタを構成するデバイスの間で同期されます。[Device Management] ページには、クラスタ内のどのデバイスまたはスタックがアクティブであるかが表示されます。アクティブなデバイスまたはスタックは、手動または自動フェールオーバーが発生すると変更されます。手動フェールオーバーの詳細については、クラスタを構成するデバイスのメンテナンス モードの開始（4-39 ページ）を参照してください。

デバイス クラスタの登録をDefense Centerから削除すると、その登録は両方のデバイスまたはスタックから削除されます。デバイス クラスタをDefense Centerから削除する方法は、個々の管理対象デバイスを削除する場合の方法と同じです。詳細については、「デバイスの削除（4-28 ページ）」を参照してください。

登録が削除されたクラスタは、別のDefense Centerに登録できます。クラスタを構成する単一のデバイスを登録するには、クラスタ内のアクティブ デバイスにリモート管理を追加してから、そのデバイスをDefense Centerに追加します。これにより、クラスタ全体が追加されます。クラスタを構成するスタック内のデバイスを登録するには、いずれかのスタックのプライマリ デバイスにリモート管理を追加してから、そのデバイスをDefense Centerに追加します。これにより、クラスタ全体が追加されます。詳細については、「Defense Centerへのデバイスの追加（4-24 ページ）」を参照してください。

デバイス クラスタを確立した後、HA リンク インターフェイスの設定（4-68 ページ）で説明している手順に従って、ハイ アベイラビリティ リンク インターフェイスを設定できます。

デバイスまたはデバイス スタックでクラスタを構成するには、以下を行います。

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　[Add] ドロップダウン メニューから、[Add Cluster] を選択します。

[Add Cluster] ポップアップ ウィンドウが表示されます。

ステップ 3　[Name] フィールドに、クラスタの名前を入力します。

英数字と特殊文字を入力できます。ただし、+、(、)、{、}、#、&、\、<、>、?、‘、および “ の文字は無効です。

ステップ 4　[Active] で、クラスタのアクティブ デバイスまたはスタックを選択します。

ステップ 5　[Backup] で、クラスタのバックアップデバイスまたはスタックを選択します。

ステップ 6　[Cluster] をクリックします。

デバイス クラスタが追加されます。このプロセスではシステム データの同期が行われるため、プロセスが完了するまでに数分かかります。

デバイス クラスタの編集

ライセンス： Control

サポートされるデバイス： シリーズ 3

デバイス クラスタを確立した後は、デバイスの設定を変更すると、通常はクラスタ全体の設定も変更されます。

[General] セクションのステータス アイコンにマウスのポインタを合わせると、クラスタのステータスが表示されます。また、クラスタ内のデバイスまたはスタックのどれがアクティブ ピアで、どれがバックアップ ピアであるかも確認できます。

詳細については、次の項を参照してください。

- 一般なデバイス設定の編集（4-53 ページ）
- デバイス ライセンスの有効化と無効化（4-54 ページ）
- クラスタ状態共有の設定（4-41 ページ）
- 高度なデバイス設定の編集（4-59 ページ）

デバイス クラスタを編集するには、以下を行います。

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　設定を編集するデバイス クラスタの横にある編集アイコン（）をクリックします。

[Cluster] ページが表示されます。

ステップ 3　[Cluster] ページのセクションを使用して、単一のデバイス設定を変更する場合と同じように、クラスタ構成の設定を変更します。

クラスタ内の個々のデバイスの設定

ライセンス： Control

サポートされるデバイス： シリーズ 3

デバイス クラスタを確立した後でも、クラスタ内の個々のデバイスに対して設定できる属性がいくつかあります。クラスタを構成するデバイスに変更を加える方法は、単一のデバイスに変更を加える場合の方法と同じです。

詳細については、次の項を参照してください。

- 一般なデバイス設定の編集（4-53 ページ）
- デバイス システム設定の編集（4-55 ページ）
- デバイスのヘルスの確認（4-57 ページ）
- デバイス管理設定の編集（4-57 ページ）

クラスタ内の個々のデバイスを設定するには、以下を行います。

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　設定を編集するデバイス クラスタの横にある編集アイコン（  ）をクリックします。

[Cluster] ページが表示されます。

ステップ 3　[Devices] をクリックします。

[Devices] ページが表示されます。

ステップ 4　[Selected Device] ドロップダウン リストから、変更するデバイスを選択します。

ステップ 5　[Devices] ページのセクションを使用して、単一のデバイスに対して変更を加える場合と同じように、クラスタを構成する個々のデバイスに変更を加えます。

クラスタ内の個々のデバイス スタックの設定

ライセンス： Control

サポートされるデバイス： シリーズ 3

スタックに含まれるデバイスのペアでクラスタを構成した後は、編集可能なスタック属性が限られてきます。クラスタを構成するスタックの名前は編集できます。また、クラスタを構成するデバイスでのインターフェイスの設定（4-38 ページ）で説明している手順に従って、スタックのネットワーク設定を編集できます。

クラスタ内のスタックの名前を編集するには、以下を行います。

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　設定を編集するデバイス クラスタの横にある編集アイコン（）をクリックします。

[Cluster] ページが表示されます。

ステップ 3　[Stacks] をクリックします。

[Stacks] ページが表示されます。

[Selected Device] ドロップダウン リストから、変更するスタックを選択します。

ステップ 4　[General] セクションの横にある編集アイコン（）をクリックします。

[General] ポップアップ ウィンドウが表示されます。

ステップ 5　[Name] フィールドに、スタックに割り当てる新しい名前を入力します。

英数字と特殊文字を入力できます。ただし、+、(、)、{、}、#、&、\、<、>、?、‘、および “ の文字は無効です。

ステップ 6　[Save] をクリックします。

新しい名前が保存されます。スタック設定を適用するまでは、変更は反映されません。詳細については、デバイスへの変更の適用（4-27 ページ）を参照してください。

クラスタを構成するデバイスでのインターフェイスの設定

ライセンス：Control

サポートされるデバイス：シリーズ 3

クラスタ内の個々のデバイスに、インターフェイスを設定できます。ただし、その場合には、クラスタ内のピア デバイスにも同等のインターフェイスを設定する必要があります。クラスタを構成するスタックの場合は、スタックのプライマリ デバイスのそれぞれに、同じインターフェイスを設定する必要があります。仮想ルータを設定するときに、その仮想ルータを設定するスタックを選択します。詳細については、「仮想ルータの設定（7-9 ページ）」を参照してください。

クラスタを構成するデバイスの [Interfaces] ページに、個々のデバイスのハードウェアおよびインターフェイスのビューが含まれています。詳細については、「センシング インターフェイスの設定（4-64 ページ）」を参照してください。

クラスタを構成するデバイスにインターフェイスを設定するには、以下を行います。

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　インターフェイスを設定するデバイス クラスタの横にある編集アイコン（）をクリックします。

[Cluster] ページが表示されます。

ステップ 3　[Interfaces] をクリックします。

[Interfaces] ページが表示されます。

ステップ 4　[Selected Device] ドロップダウン リストから、変更するデバイスを選択します。

ステップ 5　個々のデバイスに設定する場合と同じようにインターフェイスを設定します。詳細については、「センシング インターフェイスの設定（4-64 ページ）」を参照してください。

クラスタ内のアクティブ ピアの切り替え

ライセンス： Control

サポートされるデバイス： シリーズ 3

デバイス クラスタを確立した後、アクティブなピア デバイスまたはスタックをバックアップに、またはその逆に手動で切り替えることができます。

クラスタ内のアクティブ ピアを切り替えるには、以下を行います。

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　アクティブ ピアを変更するデバイス クラスタの横にある、アクティブ ピア切り替えアイコン（  ）をクリックします。

[Switch Active Peer] ポップアップ ウィンドウが表示されます。

ステップ 3　クラスタ内のバックアップ デバイスを即時にアクティブ デバイスに切り替える場合は、[Yes] をクリックします。キャンセルして [Device Management] ページに戻る場合は、[No] をクリックします。

クラスタを構成するデバイスのメンテナンス モードの開始

ライセンス： Control

サポートされるデバイス： シリーズ 3

クラスタを確立した後に、デバイスのメンテナンスを行うために手動でフェールオーバーをトリガーするには、クラスタを構成するデバイスまたはスタックをメンテナンス モードに切り替えます。メンテナンス モードでは、システムが管理上、管理インターフェイスを除くすべてのインターフェイスをダウンさせます。メンテナンスの完了後、デバイスを再び有効にして、通常の動作を再開できます。

注　クラスタの両方のメンバーを同時にメンテナンス モードにしないでください。これを行うと、そのクラスタでトラフィックを検査できなくなります。

クラスタを構成するデバイスでメンテナンス モードを開始するには、以下を行います。

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　クラスタを構成するデバイスのうち、メンテナンス モードを開始するデバイスの横にあるメンテナンス モード切り替えアイコン（）をクリックします。

[Confirm Maintenance Mode] ポップアップ ウィンドウが表示されます。

ステップ 3　[Yes] をクリックしてメンテナンス モードを確認するか、[No] をクリックしてキャンセルします。

ステップ 4　メンテナンス モード切り替えアイコン（）を再度クリックすると、デバイスのメンテナンス モードが終了します。

クラスタを構成するスタック内のデバイスの交換

ライセンス：Control

サポートされるデバイス：シリーズ 3

クラスタのメンバとなっているスタックをメンテナンス モードに切り替えた後、スタック内のセカンダリ デバイスを別のデバイスと交換できます。この場合、選択できるデバイスは、現在スタックのメンバにも、クラスタのメンバにもなっていないデバイスのみです。新しいデバイスは、デバイス スタックを確立する場合と同じガイドラインに従っている必要があります。デバイス スタックの確立（4-48 ページ）を参照してください。

クラスタを構成するスタック内のデバイスを交換するには、以下を行います。

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　メンテナンス モードを開始するスタック メンバの横にあるメンテナンス モード切り替えアイコン（）をクリックします。

[Confirm Maintenance Mode] ポップアップ ウィンドウが表示されます。

ステップ 3　[Yes] をクリックしてメンテナンス モードを確認するか、[No] をクリックしてキャンセルします。

ステップ 4　デバイス交換アイコン（）をクリックします。

[Replace Device] ポップアップ ウィンドウが表示されます。

ステップ 5　ドロップダウン リストから [Replacement Device] を選択します。

ステップ 6　デバイスを交換するには、[Replace] をクリックします。現在のデバイスを保持して [Device Management] ページに戻るには、[Cancel] をクリックします。

ステップ 7　メンテナンス モード切り替えアイコン（）を再度クリックすると、スタックのメンテナンス モードが即時に終了します。

デバイス設定を再適用する必要はありません。

クラスタ状態共有の設定

ライセンス： Control

サポートされるデバイス： シリーズ 3

クラスタ状態共有を使用すると、クラスタを構成するデバイス間、またはクラスタを構成するスタック間で、可能な限り状態を同期できます。したがって、いずれか一方のデバイスまたはスタックで障害が発生しても、もう一方のピアがトラフィック フローを中断せずに引き継ぐことができます。状態共有を使用しない場合、以下の機能が適切にフェールオーバーしない可能性があります。

- 厳密な TCP 適用
- 単方向アクセス コントロール ルール
- ブロッキングの永続性

ただし、状態共有を有効にすると、システム パフォーマンスが低下することに注意してください。

クラスタ化された状態共有を設定するには、あらかじめクラスタ内の両方のデバイスまたはプライマリ スタック デバイスで HA リンク インターフェイスを設定し、有効にする必要があります。82xx ファミリおよび 83xx ファミリには 10G の HA リンクが必要ですが、他のモデルのデバイスには 1G の HA リンクで十分です。詳細については、「HA リンク インターフェイスの設定 (4-68 ページ)」を参照してください。

注 クラスタを構成するデバイスでフェールオーバーが発生した場合は、アクティブ デバイス上の既存の SSL 暗号化セッションがすべて終了されます。クラスタ状態共有を設定しているとしても、これらのセッションをバックアップ デバイスで再ネゴシエートする必要があります。SSL セッションを確立しているサーバがセッションの再利用をサポートしている場合でも、バックアップ デバイスに SSL セッション ID がないと、セッションを再ネゴシエートできません。詳細については、デバイスのクラスタリング (4-31 ページ) を参照してください。

厳密な TCP 適用

ドメインに対して厳密な TCP 適用を有効にすると、システムは TCP セッションで正常ではないパケットをすべてドロップします。たとえば、未確立の接続で受信した SYN 以外のパケットはドロップされます。状態共有が有効な場合、厳密な TCP 適用が有効にされているとしても、クラスタ内のデバイスは、フェールオーバー後に接続を再び確立することなく TCP セッションを続行できます。厳密な TCP 適用は、インライン セット、仮想ルータ、および仮想スイッチで有効にすることができます。

単方向アクセス コントロール ルール

単方向アクセス コントロール ルールを設定している場合、システムがフェールオーバーの後に接続ミッドストリームを再評価する際に、ネットワーク トラフィックが意図されたものとは異なるアクセス コントロール ルールに一致する可能性があります。たとえば、ポリシーに以下の 2 つのアクセス コントロール ルールが含まれているとします。

```
Rule 1: Allow from 192.168.1.0/24 to 192.168.2.0/24
Rule 2: Block all
```

状態共有が有効でない場合、フェールオーバーの後に 192.168.1.1 ～ 192.168.2.1 からの許可される接続がまだアクティブになっているために、次のパケットが応答パケットとしてみなされると、システムは接続を拒否します。状態共有が有効であれば、ミッドストリーム ピックアップが既存の接続に一致することになり、接続が引き続き許可されます。

ブロッキングの永続性

アクセス コントロール ルールやその他の要素に基づいて、最初のパケットで多数の接続がブロックされるとしても、システムが接続のブロッキングを決定する前に、いくつかのパケットを許可する場合があります。状態共有が有効な場合、システムはピア デバイスまたはスタックでも即時に接続をブロックします。

クラスタ状態共有を設定する際には、以下のオプションを設定できます。

Enabled

状態共有を有効にするには、このチェック ボックスをクリックします。チェック ボックスをクリアすると、状態共有が無効になります。

Minimum Flow Lifetime

最小セッション時間（ミリ秒）を指定します。この時間を経過すると、システムがセッションの同期メッセージを送信します。0 ～ 65535 の整数を使用できます。この最小フロー有効期間に達しないセッションは、いずれも同期されず、接続のパケットを受信した時点でのみ、同期が行われます。

Minimum Sync.Interval

セッションの更新メッセージ間隔（ミリ秒）を指定します。0 ～ 65535 の整数を使用できます。最小同期間隔を設定することで、特定の接続が最小有効期間に達した後、その接続に対して、設定された値より頻繁に同期メッセージが送信されないようにします。

Maximum HTTP URL Length

クラスタを構成するデバイス間で同期する、URL の最大文字数を指定します。0 ～ 225 の整数を使用できます。

注　Ciscoでは、展開で値を変更する正当な理由がない限り、デフォルト値を使用することを推奨しています。値を小さくすると、クラスタを構成するピアの準備が向上し、値を大きくすると、パフォーマンスが向上します。

クラスタ状態共有を設定するには、以下を行います。

アクセス： Admin/Network Admin

ステップ 1　クラスタ内のデバイスごとに HA リンク インターフェイスを設定します。

詳細については、「HA リンク インターフェイスの設定（4-68 ページ）」を参照してください。

ステップ 2　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 3　編集するデバイス クラスタの横にある編集アイコン（  ）をクリックします。

[Cluster] ページが表示されます。

ステップ 4　[State Sharing] セクションの横にある編集アイコン（  ）をクリックします。

[State Sharing] ポップアップ ウィンドウが表示されます。

ステップ 5　このセクションで前に説明したように、状態共有を設定します。

ステップ 6　[OK] をクリックします。

変更が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

クラスタ状態共有のトラブルシューティング

ライセンス： Control

サポートされるデバイス： シリーズ 3

状態共有を有効にした後は、[Cluster] ページの [State Sharing] セクションで、設定に関する以下の情報を確認できます。

- 使用されている HA リンク インターフェイスおよび現在のリンク状態
- 問題のトラブルシューティングに使用できる、同期に関する詳細な統計情報

状態共有の統計情報は、主に、クラスタで送受信された同期トラフィックのさまざまな側面に対するカウンタです。その他に、いくつかのエラー カウンタもあります。さらに、クラスタ内のデバイスごとの最新システム ログも表示できます。

各デバイスに関して確認できる統計情報、およびそれらの情報を使用してクラスタ状態共有設定のトラブルシューティングを行う方法の詳細については、以下の項を参照してください。

Messages Received (Unicast)

クラスタを構成するピアから受信した、クラスタ同期メッセージの数です。

値は、ピアが送信したメッセージ数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。トラフィックが停止すると、値は安定し、受信したメッセージ数が送信されたメッセージ数と一致します。

トラブルシューティングを行う場合は、受信したメッセージ数と送信されたメッセージ数の両方を確認して増加率を比較し、両方の値が同等であることを確認します。各ピアでの送信数の値は、対応するピアでの受信数の値とほぼ同じ率で増えていなければなりません。

受信したメッセージの数が増加しなくなった場合、または増加率がピアから送信されたメッセージ数に追いついていない場合は、サポートに連絡してください。

Packets Received

システムはオーバーヘッドを低減させるために、複数のメッセージを単一のパケットにまとめます。[Packets Received] カウンタは、デバイスが受信したこれらのデータ パケットとその他の制御パケットの数を表示します。

値は、ピア デバイスが送信したパケット数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。受信メッセージの数は、ピアが送信したメッセージ数と同等で、同じ率で増加していなければなりません。したがって、受信したパケットの数も同じ動作となるはずです。

トラブルシューティングを行う場合は、受信したパケットと送信されたメッセージの両方を確認して増加率を比較し、値が同じ率で増加していることを確認します。クラスタを構成するピアでの送信の値が増えている場合、デバイスでの受信の値も同じ率で増えているはずです。

受信したパケットの数が増加しなくなった場合、または増加率がピアから送信されたメッセージ数に追いついていない場合は、サポートに連絡してください。

Total Bytes Received

ピアで受信されたパケットの合計バイト数です。

値は、もう一方のピアが送信したバイト数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。

トラブルシューティングを行う場合は、受信した合計バイト数と送信されたメッセージ数の両方を確認して増加率を比較し、両方の値が同じ率で増えていることを確認します。クラスタを構成するピアでの送信の値が増えている場合、デバイスでの受信の値も同じ率で増えているはずです。

受信バイト数が増加しなくなった場合、または増加率がピアから送信されたメッセージ数に追いついていない場合は、サポートに連絡してください。

Protocol Bytes Received

受信したプロトコル オーバーヘッドのバイト数です。この数には、セッション状態同期メッセージのペイロードを除くすべてが含まれます。

値は、ピアが送信したバイト数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。

トラブルシューティングを行う場合は、受信した合計バイト数を確認してプロトコル データと比較し、実際の状態データがどれだけ共有されているのかを調べます。プロトコル データが送信されるデータの大部分を占めている場合は、最小同期間隔を調整できます。

受信したプロトコル バイト数が、受信した合計バイト数と同等の割合で増えている場合は、サポートに連絡してください。受信したプロトコル バイト数が受信した合計バイト数に占める割合は、最小限でなければなりません。

Messages Sent

クラスタを構成するピアに送信した、クラスタ同期メッセージの数です。

このデータは、受信メッセージ数との比較で役立ちます。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。

トラブルシューティングを行う場合は、受信したメッセージ数と送信されたメッセージ数の両方を確認して増加率を比較し、両方の値が同等であることを確認します。

送信したメッセージ数が、受信した合計バイト数と同等の割合で増えている場合は、サポートに連絡してください。

送信バイト数

ピアに送信したクラスタ同期メッセージの合計送信バイト数です。

このデータは、受信メッセージ数との比較で役立ちます。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。ピアで受信されたバイト数は、この値と同等であり、それより大きい値にはなっていないはずです。

受信した合計バイト数が、送信されたバイト数と同じような比率で増えていない場合は、サポートに連絡してください。

Tx Errors

システムがクラスタを構成するピアに送信するメッセージ用にスペースを割り当てるときに発生した、メモリ割り当ての失敗数です。

この値は両方のピアで常にゼロでなければなりません。この数がゼロでない場合、あるいは着実に増加している場合（これは、システムにメモリ割り当てが不可能なエラーが発生していることを示します）は、サポートに連絡してください。

Tx Overruns

システムがメッセージをトランジット キューに入れようとして失敗した回数です。

この値は両方のピアで常にゼロでなければなりません。値がゼロでない場合、あるいは着実に増加している場合、これは、システムが HA リンクの間で過剰なデータを共有していて、データの送信に時間がかかりすぎていることを示します。

HA リンク MTU がデフォルト値（9918 または 9922）未満に設定されている場合は、値を増やす必要があります。最小フロー有効期間と最小同期間隔の設定を変更することで、HA リンク間で共有されるデータ量を減らし、この数の増加を防ぐことができます。

この値がゼロにならない場合、または増加し続けている場合は、サポートに連絡してください。

Recent Logs

システム ログには、最新のクラスタ同期メッセージが表示されます。ログには、ERROR または WARN メッセージが示されていてはなりません。ログの内容は、常にピア間で同等でなければなりません（接続ソケットの数が同じであるなど）。

ただし、場合によっては、対照的なデータが表示されることもあります。たとえば、一方のピアがもう一方のピアから接続を受信したことをレポートしている場合、それぞれのログで参照される IP アドレスは異なります。このログから、クラスタ状態共有接続を包括的に理解し、接続で発生したすべてのエラーを確認できます。

ログに、ERROR または WARN メッセージ、あるいは単なる通知目的ではないようなメッセージが示されている場合は、サポートに連絡してください。

クラスタ状態共有に関する統計情報を表示するには、以下を行います。

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　編集するデバイス クラスタの横にある編集アイコン（）をクリックします。

デバイス クラスタの [Cluster] ページが表示されます。

ステップ 3　[State Sharing] セクションで、統計情報表示アイコン（  ）をクリックします。

[State Sharing Statistics] ポップアップ ウィンドウが表示されます。

ステップ 4　必要に応じて、[Device] を選択して、クラスタがデバイス スタックで構成されているかどうかを確認します。

ステップ 5　必要に応じて、[Refresh] をクリックして統計情報を更新します。

ステップ 6　必要に応じて、[View] をクリックして、クラスタを構成する各デバイスの最新データ ログを表示します。

クラスタを構成するデバイスの分離

ライセンス： Control

サポートされるデバイス： シリーズ 3

デバイス クラスタを解除しても、アクティブ デバイスまたはスタックは、完全な展開機能を維持します。バックアップ デバイスまたはスタックは、インターフェイス設定を失い、アクティブ デバイスまたはスタックにフェールオーバーします。ただし、インターフェイス設定をアクティブに維持することを選択すると、バックアップ デバイスまたはスタックは通常の動作を再開します。クラスタを解除すると、バックアップ デバイスのパッシブ インターフェイス設定は必ず削除されます。メンテナンス モードのデバイスは、クラスタが解除された時点で通常の動作を再開します。

クラスタを構成するデバイスを分離するには、以下を行います。

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　解除するデバイス クラスタの横にあるクラスタ解除アイコン（  ）をクリックします。

[Confirm Break] ポップアップ ウィンドウが表示されます。

ステップ 3　必要に応じて、バックアップ デバイスまたはスタックのインターフェイス設定を削除するチェック ボックスをオンにします。この場合、管理インターフェイスを除くすべてのインターフェイスが管理上、ダウン状態になります。

ステップ 4　[Yes] をクリックします。

デバイス クラスタが解除されます。

スタックに含まれるデバイスの管理

ライセンス： すべて

サポートされるデバイス： 3D8140、3D8200 ファミリ、3D8300 ファミリ、AMP8300 ファミリ、ASM3D9900

スタック構成に含まれるデバイスを使用して、ネットワーク セグメントで検査されるトラフィックの量を増やすことができます。それぞれのスタック構成では、スタックに含まれるすべてのデバイスが同じハードウェアを使用していなければなりません。ただし、スタックに 3D9900 が含まれない場合、マルウェア ストレージ パックがインストールされたデバイスがなくても、一部またはすべてのデバイスにマルウェア ストレージ パックがインストールされていても構いません。また、以下のスタック構成に従って、同じデバイス ファミリのデバイスを使用する必要があります。

シリーズ 2 および 81xx ファミリの場合：

- 2 つの 3D8140
- 2 つの 3D9900

82xx ファミリの場合：

- 最大 4 つの 3D8250
- 1 つの 3D8260（プライマリ デバイスおよびセカンダリ デバイス）
- 1 つの 3D8270（容量 40G のプライマリ デバイスと 2 つのセカンダリ デバイス）
- 1 つの 3D8290（容量 40G のプライマリ デバイスと 3 つのセカンダリ デバイス）

83xx ファミリの場合：

- 最大 4 つの 3D8350
- 1 つの 3D8360（容量 40G のプライマリ デバイスとセカンダリ デバイス）
- 1 つの 3D8370（容量 40G のプライマリ デバイスと 2 つのセカンダリ デバイス）
- 1 つの 3D8390（容量 40G のプライマリ デバイスと 3 つのセカンダリ デバイス）
- 最大 4 つの AMP8350
- 1 つの AMP8360（容量 40G のプライマリ デバイスとセカンダリ デバイス）
- 1 つの AMP8370（容量 40G のプライマリ デバイスと 2 つのセカンダリ デバイス）
- 1 つの AMP8390（容量 40G のプライマリ デバイスと 3 つのセカンダリ デバイス）

スタック構成の詳細については、『*FireSIGHT System Installation Guide*』を参照してください。マルウェア ストレージ パックの詳細については、『*FireSIGHT System Malware Storage Pack Guide*』を参照してください。

注意 Ciscoから提供されたものではないハード ドライブをデバイスに取り付けないでください。サポートされていないハード ドライブを取り付けると、デバイスが破損する可能性があります。マルウェア ストレージ パック キットは、Ciscoから**のみ**購入でき、8000 シリーズ デバイスで**のみ**使用できます。マルウェア ストレージ パック のサポートが必要な場合は、サポートにお問い合わせください。詳細については、『*FireSIGHT System Malware Storage Pack Guide*』を参照してください。

スタック構成を確立すると、スタックに含まれる各デバイスのリソースが単一の共有設定に結合されることになります。

1 つのデバイスを*プライマリ* デバイスとして指定し、そのデバイスにスタック全体のインターフェイスを設定します。その他のデバイスは*セカンダリ*デバイスとして指定します。セカンダリ デバイスは、現在トラフィックを検知していないデバイスで、かつインターフェイス上にリンクがないデバイスでなければなりません。

単一のデバイスを設定する場合と同じように、プライマリ デバイスを分析対象のネットワーク セグメントに接続します。詳細については、「センシング インターフェイスの設定（4-64 ページ）」を参照してください。『*FireSIGHT システム Installation Guide*』で説明されているスタックに含まれるデバイスの配線手順に従って、セカンダリ デバイスをプライマリ デバイスに接続します。

スタックに含まれるすべてのデバイスは、同じハードウェアを使用し、同じソフトウェア バージョンを実行し、同じライセンスが適用されている必要があります。デバイスが NAT ポリシーのターゲットとなっている場合は、プライマリ デバイスとセカンダリ デバイスの両方に同じ NAT ポリシーを適用する必要があります。詳細については、「NAT ポリシーの管理（11-8 ページ）」を参照してください。更新は、Defense Centerからスタック全体に対して適用する必要があります。スタックに含まれる 1 つ以上のデバイスで更新に失敗した場合、スタックはバージョンが混在した状態になります。バージョンが混在するスタックには、ポリシーを適用することも、更新を適用することもできません。この状態を修正するには、スタックを解除するか、バージョン

が異なる個々のデバイスを削除し、それらのデバイスを個別に更新してからスタック構成を再確立します。デバイスをスタックに入れた後は、ライセンスの変更は、スタック全体に対してのみ行うことができます。

スタック構成を確立した後は、スタックに含まれるすべてのデバイスが単一の共有構成のように機能します。プライマリ デバイスで障害が発生した場合、トラフィックはセカンダリ デバイスに渡されません。この場合、セカンダリ デバイスでスタック ハートビートが失敗したことを通知する、ヘルス アラートが生成されます。詳細については、「ヘルス モニタリングの使用（68-1 ページ）」を参照してください。

スタック内のセカンダリ デバイスで障害が発生すると、設定可能なバイパスが有効になっているインライン セットがプライマリ デバイス上でバイパス モードになります。それ以外のすべての設定では、システムは、失敗したセカンダリ デバイスへ継続してトラフィックをロード バランシングします。いずれの場合も、リンクが失われたことを示すためのヘルス アラートが生成されます。

デバイス スタックは展開内で単一のデバイスと同じように使用できますが、いくつかの例外があります。クラスタを構成するデバイスが存在する場合、デバイス クラスタや、クラスタ ペアとなっているデバイスをスタックに含めることはできません。詳細については、「デバイスのクラスタリング（4-31 ページ）」を参照してください。また、デバイス スタックに NAT を設定することもできません。

注　スタックに含まれるデバイスからのイベント データを、eStreamer を使用して外部クライアント アプリケーションに配信する場合は、各デバイスからデータを収集して、各デバイスが同じように設定されていることを確認します。eStreamer 設定は、スタック内のデバイス間で自動的に同期されません。

詳細については、次の項を参照してください。

- デバイス スタックの確立（4-48 ページ）
- デバイス スタックの編集（4-50 ページ）
- スタックに含まれる個々のデバイスの設定（4-51 ページ）
- スタックに含まれるデバイスの分離（4-52 ページ）

デバイス スタックの確立

ライセンス： すべて

サポートされるデバイス： 3D8140、3D8200 ファミリ、3D8300 ファミリ、AMP8300 ファミリ、3D9900

ネットワーク セグメントで検査されるトラフィック量を増やすには、ファイバベースの 3D9900（2 つ）、3D8140 デバイス（2 つ）、3D8250（最大 4 つ）、3D8260、3D8270、3D8290、3D8350（最大 4 つ）、3D8360、3D8370、3D8390、AMP8350（最大 4 つ）、AMP8360、AMP8370、または AMP8390 から成るスタックを構成し、それらのリソースを結合して単一の共有構成で使用します。始める前に、次の手順を実行する必要があります。

- プライマリ デバイスとして指定するユニットを決定します。
- プライマリとセカンダリの関係を指定する前に、適切にユニット間の配線を行います。配線については、『*FireSIGHT システム Installation Guide*』を参照してください。

注　クラスタを構成するデバイスが存在する場合、デバイス クラスタや、クラスタ ペアとなっているデバイスをスタックに含めることはできません。ただし、デバイス スタックでクラスタを構成することはできます。詳細については、「デバイスのクラスタリング（4-31 ページ）」を参照してください。

デバイス スタックを確立すると、これらのデバイスは、[Device Management] ページで単一のデバイスとして扱われます。デバイス スタックには、アプライアンスのリストでスタック アイコン（ ）が表示されます。

デバイス スタックの登録をDefense Centerから削除すると、その登録は両方のデバイスから削除されます。スタックに含まれるデバイスをDefense Centerから削除する方法は、単一の管理対象デバイスを削除する場合と同じです。削除したスタックは、別のDefense Centerに登録できます。新しいDefense Centerに、スタックに含まれるデバイスのいずれか 1 つを登録するだけで、スタック全体が表示されるようになります。詳細については、デバイスの削除（4-28 ページ）および Defense Centerへのデバイスの追加（4-24 ページ）を参照してください。

デバイス スタックを確立した後は、スタックを解除して再確立しない限り、デバイスのプライマリまたはセカンダリとしての役割を変更することはできません。ただし、次の作業を実行できます。

- スタックで許容される最大 4 つの 3D8250 になるまで、2 つまたは 3 つの 3D8250、3D8260、または 3D8270 からなる既存のスタックにセカンダリ デバイスを追加します。
- スタックで許容される最大 4 つの 3D8350 になるまで、2 つまたは 3 つの 3D8350、3D8360、または 3D8370 からなる既存のスタックにセカンダリ デバイスを追加します。
- スタックで許容される最大 4 つの AMP8350 になるまで、2 つまたは 3 つの AMP8350、AMP8360、または AMP8370 からなる既存のスタックにセカンダリ デバイスを追加します。

デバイスを追加する場合、スタックのプライマリ デバイスに、追加のデバイスを配線するために必要なスタック NetMods がなければなりません。たとえば、プライマリに単一のスタック NetMod しかない 3D8260 を使用している場合、このスタックに別のセカンダリ デバイスを追加することはできません。セカンダリ デバイスを既存のスタックに追加する方法は、最初にスタックに含まれるデバイスの設定を確立したときの方法と同じです。

デバイスのスタック構成を確立するには、以下を行います。

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　[Add] ドロップダウン メニューから、[Add Stack] を選択します。

[Add Stack] ポップアップ ウィンドウが表示されます。

ステップ 3　[Primary] ドロップダウン リストから、プライマリ デバイスとして運用するために配線したデバイスを選択します。

注　プライマリ デバイスとして配線されていないデバイスを編集すると、以降の手順を実行できなくなります。

ステップ 4　[Name] フィールドに、スタックの名前を入力します。英数字と特殊文字を入力できます。ただし、+、(、)、{、}、#、&、\、<、>、?、‘、および “ の文字は無効です。

ステップ 5　[Add] をクリックして、スタックに含めるデバイスを選択します。

[Add Secondary Connection] ポップアップ ウィンドウが表示されます。以下の図に、3D8140 のプライマリ デバイスの正面図を示します。

ステップ 6　[Slot on Primary Device] ドロップダウン リストから、プライマリ デバイスをセカンダリ デバイスに接続するスタック構成ネットワーク モジュールを選択します。

ステップ 7　[Secondary Device] ドロップダウン リストから、セカンダリ デバイスとして運用するために配線したデバイスを選択します。

注　スタックに含まれるすべてのデバイスは、同じハードウェア モデルでなければなりません（たとえば、3D9900 と 3D9900、3D8140 と 3D8140 など）。82xx ファミリおよび83xx ファミリでは、合計 4 つのデバイス（1 つのプライマリ デバイスと最大 3 つのセカンダリ デバイス）でスタックを構成できます。

ステップ 8　[Slot on Secondary Device] ドロップダウン リストから、セカンダリ デバイスをプライマリ デバイスに接続するスタック構成ネットワーク モジュールを選択します。

ステップ 9　[Add] をクリックします。

[Add Stack] ウィンドウが再表示されて、新しいセカンダリ デバイスがリストされます。

ステップ 10　（任意）3D8250 の既存のスタック、3D8260、3D8270、3D8350 の既存のスタック、3D8360、3D8370、AMP8350 の既存のスタック、AMP8360、または AMP8370 にセカンダリ デバイスを追加するには、ステップ 5 から 9 を繰り返します。

ステップ 11　[Stack] をクリックします。

デバイス スタックが確立されるか、セカンダリ デバイスが追加されます。このプロセスではシステム データの同期が行われるため、プロセスが完了するまでに数分かかることに注意してください。

デバイス スタックの編集

ライセンス： すべて

サポートされるデバイス： 3D8140、3D8200 ファミリ、3D8300 ファミリ、AMP8300 ファミリ、3D9900

デバイス スタックを設定した後は、デバイスの設定を変更すると、通常はスタック全体の設定も変更されます。単一のデバイスの [Device] ページで設定を変更する場合と同じように、アプライアンス エディタの [Stack] ページで、スタック設定に変更を加えることができます。

このページでは、スタックの表示名の変更、ライセンスの有効化と無効化、システム ポリシーとヘルス ポリシーの表示、Automatic Application Bypass の設定、Fast-Path ルールの設定を行うことができます。

詳細については、次の項を参照してください。

- 一般なデバイス設定の編集（4-53 ページ）
- デバイス ライセンスの有効化と無効化（4-54 ページ）
- 高度なデバイス設定の編集（4-59 ページ）

スタック構成の設定を編集するには、以下を行います。

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　設定を編集する、スタックに含まれるデバイスの横にある編集アイコン（）をクリックします。

そのデバイスの [Stack] ページが表示されます。

ステップ 3　[Stack] ページのセクションを使用して、単一のデバイス設定を変更する場合と同じように、スタック構成の設定を変更します。

スタックに含まれる個々のデバイスの設定

ライセンス：すべて

サポートされるデバイス：3D8140、3D8200 ファミリ、3D8300 ファミリ、AMP8300 ファミリ、3D9900

デバイス スタックを確立した後でも、スタック内の個々のデバイスに対して設定できる属性がいくつかあります。アプライアンス エディタの [Devices] ページで、単一デバイスの [Device] ページの場合と同じように、スタックに含まれる個々のデバイスに変更を加えることができます。

このページでは、デバイスの表示名の変更、システム設定の表示、デバイスのシャットダウンまたは再起動、ヘルス情報の表示、およびデバイス管理設定の編集を行うことができます。

詳細については、次の項を参照してください。

- 一般なデバイス設定の編集（4-53 ページ）
- デバイス システム設定の編集（4-55 ページ）
- デバイスのヘルスの確認（4-57 ページ）
- デバイス管理設定の編集（4-57 ページ）

スタックに含まれる個々のデバイスを設定するには、以下を行います。

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　設定を編集する、スタックに含まれるデバイスの横にある編集アイコン（）をクリックします。

そのデバイスの [Stack] ページが表示されます。

ステップ 3　[Devices] をクリックします。

[Devices] ページが表示されます。

ステップ 4　[Selected Device] ドロップダウン リストから、変更するデバイスを選択します。

ステップ 5　[Devices] ページのセクションを使用して、単一のデバイスに対して変更を加える場合と同じように、スタックに含まれる個々のデバイスに変更を加えます。

スタックに含まれるデバイスでのインターフェイスの設定

ライセンス：すべて

サポートされるデバイス：3D8140、3D8200 ファミリ、3D8300 ファミリ、AMP8300 ファミリ、3D9900

管理インターフェイスを除き、スタックに含まれるデバイスにインターフェイスを設定するには、スタックのプライマリ デバイスの [Interfaces] ページを使用します。管理インターフェイスを設定する場合は、スタックに含まれる任意のデバイスを選択できます。詳細については、「管理インターフェイスの構成（64-9 ページ）」を参照してください。

スタックに含まれるシリーズ 3 デバイスの [Interfaces] ページに、個々のデバイスのハードウェアおよびインターフェイスのビューがあります。3D9900 の [Interfaces] ページには、これらのビューは含まれていません。詳細については、「センシング インターフェイスの設定（4-64 ページ）」を参照してください。

スタックに含まれるデバイスにインターフェイスを設定するには、以下を行います。

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　インターフェイスを設定する、スタックに含まれるデバイスの横にある編集アイコン（  ）をクリックします。

そのデバイスの [Stack] ページが表示されます。

ステップ 3　[Interfaces] をクリックします。

[Interfaces] ページが表示されます。

ステップ 4　[Selected Device] ドロップダウン リストから、変更するデバイスを選択します。

ステップ 5　個々のデバイスに設定する場合と同じようにインターフェイスを設定します。詳細については、「センシング インターフェイスの設定（4-64 ページ）」を参照してください。

スタックに含まれるデバイスの分離

ライセンス：すべて

サポートされるデバイス：3D8140、3D8200 ファミリ、3D8300 ファミリ、AMP8300 ファミリ、3D9900

デバイスのスタック構成を使用する必要がなくなった場合、スタックを解除してデバイスを分離できます。

スタックに含まれるデバイスを分離するには、以下を行います。

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　解除するデバイス スタックの横にあるスタック解除アイコン（ ）をクリックします。

[Confirm Break] ポップアップ ウィンドウが表示されます。

ヒント　スタックを解除せずに、3 つ以上の 3D8250 デバイスで構成されるスタックからセカンダリ デバイスを削除するには、スタックから削除アイコン（ ）をクリックします。セカンダリ デバイスを削除すると、システムがそのデバイス抜きで動作するスタックを再設定する間、トラフィック インスペクション、トラフィック フロー、またはリンク状態が短時間中断されます。

ステップ 3　[Yes] をクリックします。

デバイス スタックが解除されます。

デバイス設定の編集

ライセンス： すべて

アプライアンス エディタの [Device] ページには、詳細なデバイス設定および情報が表示されます。また、デバイス設定の一部（ライセンスの有効化と無効化、デバイスのシャットダウンと再起動、管理の変更、Fast-Path ルールの設定など）を変更することもできます。

詳細については、次の項を参照してください。

- 一般なデバイス設定の編集（4-53 ページ）
- デバイス ライセンスの有効化と無効化（4-54 ページ）
- デバイス システム設定の編集（4-55 ページ）
- デバイスのヘルスの確認（4-57 ページ）
- デバイス管理設定の編集（4-57 ページ）
- 高度なデバイス設定について（4-58 ページ）

一般なデバイス設定の編集

ライセンス： すべて

[Device] タブの [General] セクションには、以下の変更可能な管理対象デバイスの設定が表示されます。

名前

管理対象デバイスに割り当てる名前。

Transfer Packets

パケット データをDefense Centerに転送してイベントと共に保存するかどうかを指定します。

一般的デバイス設定の編集方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　割り当てられた名前を編集するデバイスの横にある編集アイコン（）をクリックします。

そのデバイスの [Interfaces] ページが表示されます。

ステップ 3　[Device] をクリックします。

[Device] ページが表示されます。

ヒント　スタックに含まれるデバイスの場合、アプライアンス エディタの [Stack] ページで、スタックでデバイスに割り当てられている名前を編集します。アプライアンス エディタの [Devices] ページでは、個々のデバイスに割り当てられているデバイス名を編集できます。

ステップ 4　[General] セクションの横にある編集アイコン（）をクリックします。

[General] ポップアップ ウィンドウが表示されます。

ステップ 5　[Name] フィールドに、デバイスに割り当てる新しい名前を入力します。英数字と特殊文字を入力できます。ただし、+、(、)、{、}、#、&、\、<、>、?、‘、および “ の文字は無効です。

ステップ 6　パケット データをイベントと一緒にDefense Centerに保存できるようにするには、[Transfer Packets] チェック ボックスをオンにします。管理対象デバイスがイベントと一緒にパケット データを送信できないようにするには、このチェック ボックスをオフにします。

ステップ 7　[Save] をクリックします。

これにより、変更内容が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

デバイス ライセンスの有効化と無効化

ライセンス： すべて

サポートされるデバイス： シリーズ 3、仮想、X-Series、ASA FirePOWER

Defense Centerで使用可能なライセンスがある場合、デバイスでそのライセンスを有効にすることができます。次の点に注意してください。

- Control、Malware、および URL Filtering ライセンスには、Protection ライセンスが必要です。
- VPN ライセンスは、仮想デバイス、Cisco NGIPS for Blue Coat X-Series、または ASA FirePOWER デバイスで有効にすることはできません。
- Control ライセンスを仮想デバイス、Cisco NGIPS for Blue Coat X-Series、または ASA FirePOWER で有効にすることはできますが、これらのデバイスでは Fast-Path ルール、スイッチング、ルーティング、スタック構成、クラスタリングを**サポートしていません**。Cisco NGIPS for Blue Coat X-Seriesは、アプリケーションやユーザの制御もサポートしていません。

- クラスタを構成するデバイスでのライセンス設定を変更することはできません。
- シリーズ 2 デバイスには、セキュリティ インテリジェンス フィルタリングを除く Protection 機能が自動的に有効になるため、これらの機能を無効にすることも、シリーズ 2 デバイスに他のライセンスを適用することもできません。

詳細については、FireSIGHT システムのライセンス（65-1 ページ）を参照してください。

デバイス ライセンスを有効または無効にするには、以下を行います。

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　ライセンスを有効または無効にするデバイスの横にある編集アイコン（）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Device] をクリックします。

[Devices] タブが表示されます。

ヒント　スタックに含まれるデバイスの場合、アプライアンス エディタの [Stack] ページで、スタックに対してラインセンスを有効または無効にします。

ステップ 4　[License] セクションの横にある編集アイコン（）をクリックします。

[License] ポップアップ ウィンドウが表示されます。

ステップ 5　次の選択肢があります。

- ライセンスを有効にする場合は、ライセンス名の横にあるチェック ボックスをオンにします。
- ライセンスを無効にする場合は、ライセンス名の横にあるチェック ボックスをオフにします。

ステップ 6　[Save] をクリックします。

これにより、変更内容が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

デバイス システム設定の編集

ライセンス： すべて

[Device] タブの [System] セクションには、システム情報の読み取り専用テーブルが表示されます。表示される情報は以下のとおりです。

表 4-2　[System] セクション テーブルのフィールド

フィールド	説明
モデル	管理対象デバイスのモデル名と番号。
シリアル（Serial）	管理対象デバイスのシャーシのシリアル番号。

表 4-2　[System] セクション テーブルのフィールド（続き）

フィールド	説明
時刻	デバイスの現在のシステム時刻。
Version	管理対象デバイスに現在インストールされているソフトウェアのバージョン。
ポリシー（Policy）	管理対象デバイスに現在適用されているシステム ポリシーへのリンク。

デバイスをシャットダウンまたは再起動することもできます。

注　FireSIGHT システム ユーザ インターフェイスが設定されている X-Series または ASA FirePOWER デバイスをシャットダウンしたり、再起動したりすることはできません。それぞれのデバイスをシャット ダウンする方法の詳細については、『*Cisco NGIPS for Blue Coat X-Series Installation Guide*』または ASA の資料を参照してください。

管理対象デバイスをシャットダウンおよび再起動するには、以下を行います。

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　再起動するデバイスの横にある編集アイコン（ ）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Device] をクリックします。

[Devices] タブが表示されます。

ヒント　スタックに含まれるデバイスの場合、アプライアンス エディタの [Devices] ページで、個々のデバイスをシャット ダウンまたは再起動します。

ステップ 4　デバイスをシャット ダウンするには、デバイスのシャット ダウン アイコン（ ）をクリックします。

ステップ 5　プロンプトが出されたら、デバイスをシャットダウンすることを確認します。

[Device Management] ページに戻ります。

ステップ 6　デバイスを再起動するには、デバイスの再起動アイコン（ ）をクリックします。

ステップ 7　プロンプトが出されたら、デバイスを再起動することを確認します。

デバイスが再起動されます。

デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

デバイスのヘルスの確認

ライセンス： すべて

[Device] タブの [Health] セクションには、ヘルス関連の情報が表示されます。管理対象デバイスの現在のヘルス ステータスを示すアイコンを確認できます。また、アイコンをクリックして、そのデバイスの [Health Monitor] ページに移動することもできます。詳細については、「ヘルス モニタ ステータスの解釈（68-45 ページ）」を参照してください。

[Policy] リンクをクリックすると、現在適用されているヘルス ポリシーの読み取り専用バージョンが表示されます。詳細については、「正常性ポリシーの編集（68-33 ページ）」を参照してください。

また、[Blacklist] リンクをクリックすると、[Health Blacklist] ページが表示されます。このページで、ヘルス ブラックリスト モジュールを有効または無効にすることができます。詳細については、「個別の正常性ポリシー モジュールのブラックリストへの登録（68-41 ページ）」を参照してください。

デバイス管理設定の編集

ライセンス： すべて

[Device] の [Management] セクションには、以下のリモート管理情報が表示されます。

ホスト

デバイスの現在の管理ホスト名または IP アドレス。この設定を使用して、管理ホストを指定したり、仮想 IP を再生成することができます。

注　場合によっては、（デバイスの LCD パネルまたは CLI などを使用して）別の方法でデバイスのホスト名や IP アドレスを編集する場合は、次の手順を実行して、管理用のDefense Centerでホスト名や IP アドレスを手動で更新する必要があります。

Status（ステータス）

Defense Centerと管理対象デバイス間の通信チャネルのステータスを指定します。

ヒント　スライダをクリックすることで、管理対象デバイスの管理を有効または無効にできます。管理を無効化すると、防御センターとデバイス間の接続がブロックされますが、防御センターからデバイスは削除**されません**。デバイスを管理する必要がなくなった場合は、デバイスの削除（4-28 ページ）を参照してください。

デバイス管理オプションを変更する方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　管理オプションを変更するデバイスの横にある編集アイコン（ ）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Device] をクリックします。

[Devices] タブが表示されます。

ヒント　スタックに含まれるデバイスの場合、アプライアンス エディタの [Devices] ページで、個々のデバイスの管理オプションを変更します。

ステップ 4　[Management] セクションの横にある編集アイコン（）をクリックします。

[Management] ポップアップ ウィンドウが表示されます。

ステップ 5　[Host] フィールドに、管理ホストの名前または IP アドレスを入力します。

ステップ 6　[Save] をクリックします。

変更が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

高度なデバイス設定について

ライセンス： すべて

サポートされるデバイス： 機能によって異なる

[Device] タブの [Advanced] セクションには、次の詳細設定を含むテーブルが表示されます。

表 4-3　[Advanced] セクション テーブルのフィールド

フィールド	説明	サポートされるデバイス数
Application Bypass	デバイスでの Automatic Application Bypass の状態。	シリーズ 2、シリーズ 3、仮想
Bypass Threshold	Automatic Application Bypass のしきい値（ミリ秒）。	シリーズ 2、シリーズ 3、仮想
Inspect Local Router Traffic	デバイスで、ルーテッド インターフェイスで受信した自己を宛先とするトラフィック（ICMP、DHCP、および OSPF トラフィックなど）を検査するかどうかを示します。	シリーズ 3
Fast-Path Rules	デバイス上に作成されている Fast-Path ルールの数。	8000 シリーズ、3D9900

上記の設定は、いずれも [Advanced] セクションを使用して編集できます。詳細については、次の項を参照してください。

- Automatic Application Bypass（4-59 ページ）
- 高度なデバイス設定の編集（4-59 ページ）
- Fast-Path ルールの設定（4-60 ページ）

Automatic Application Bypass

ライセンス： すべて

Automatic Application Bypass（AAB）機能は、インターフェイスでのパケット処理時間に制限を設け、この時間を超過した場合、パケットに検出のバイパスを許可します。この機能は任意の展開で使用できますが、インライン展開ではとりわけ価値があります。

パケット処理の遅延は、ネットワークで許容できるパケット レイテンシとバランスを取って調整します。Snort 内での不具合やデバイスの誤った設定が原因で、トラフィックの処理時間が指定のしきい値を超えると、AAB により、その障害発生から 10 分以内に Snort が再起動され、トラブルシューティング データが生成されます。このデータを分析することで、過剰な処理時間の原因を調査できます。

バージョン 5.4.1 以降での AAB オプションのデフォルト動作は、デバイスによって以下のように異なります。

- シリーズ 3：オフ
- シリーズ 2 および仮想：オン
- ASA FirePOWER：未サポート
- X-Series：未サポート

5.3 より前のバージョンからアップグレードする場合は、既存の設定が保持されます。このオプションが選択されている場合は、バイパスしきい値を変更できます。デフォルト設定は 3000 ミリ秒（ms）です。有効な範囲は 250 ms ～ 60,000 ms です。

一般に、レイテンシしきい値を超えた後は、Fast-Path パケットに対して侵入ポリシーの Rule Latency Thresholding を使用します。Rule Latency Thresholding により、エンジンがシャットダウンされたり、しきい値データが生成されることはありません。詳細については、パケットおよび侵入ルール遅延しきい値の設定（18-14 ページ）を参照してください。

注　AAB がアクティブ化されるのは、単一パケットに過剰な処理時間がかかっている場合のみです。AAB がアクティブになると、システムはすべての Snort プロセスをキルします。

検出がバイパスされると、デバイスがヘルス モニタリング アラートを生成します。このヘルス モニタリング アラートの詳細については、ヘルス モニタの使用（68-45 ページ）を参照してください。

Automatic Application Bypass を有効にしてバイパスしきい値を設定する方法の詳細については、高度なデバイス設定の編集（4-59 ページ）を参照してください。

高度なデバイス設定の編集

ライセンス： すべて

サポートされるデバイス： 機能によって異なる

[Devices] タブの [Advanced] セクションを使用して、[Automatic Application Bypass] および [Inspect Local Router Traffic] の設定を変更できます。また、Fast-Path ルールの設定（4-60 ページ）で説明する手順に従って、Fast-Path ルールを設定することもできます。

次の点に注意してください。

- Fast-Path ルールを設定できるのは、8000 シリーズ および 3D9900 デバイスのみです。
- [Inspect Local Router Traffic] を設定できるのは、シリーズ 3 デバイスのみです。

高度なデバイス設定を変更するには、以下を行います。

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　高度なデバイス設定を編集するデバイスの横にある編集アイコン（）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Device] をクリックします。

[Devices] タブが表示されます。

ヒント　スタックに含まれるデバイスの場合、アプライアンス エディタの [Stack] ページで、スタックの高度なデバイス設定を編集します。

ステップ 4　[Advanced] セクションの横にある編集アイコン（）をクリックします。

[Advanced] ポップアップ ウィンドウが表示されます。

ステップ 5　ネットワークがレイテンシの影響を受けやすい場合は、必要に応じて、[Automatic Application Bypass] を選択します。Automatic Application Bypass は、インライン展開でとりわけ役立ちます。詳細については、Automatic Application Bypass（4-59 ページ）を参照してください。

ステップ 6　[Automatic Application Bypass] オプションを選択すると、[Bypass Threshold] にバイパスしきい値（ミリ秒）を入力できるようになります。デフォルト設定は 3000 ms です。有効な範囲は 250 ms ～ 60,000 ms です。

ステップ 7　ルータとして展開されている場合は、必要に応じて [Inspect Local Router Traffic] チェック ボックスをオンにして例外トラフィックを検査します。

ステップ 8　（任意）Fast-Path ルールを設定します。詳細については、Fast-Path ルールの設定（4-60 ページ）を参照してください。

ステップ 9　[Save] をクリックします。

変更が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

Fast-Path ルールの設定

ライセンス： すべて

サポートされるデバイス： 8000 シリーズ、3D9900

Fast-Path ルールを作成すると、さらに検査することなく、デバイスを介して直接トラフィックを送信できます。Fast-Path ルールは、分析する必要のないトラフィックを方向転換してデバイスをバイパスさせます。Fast-Path ルールは、トラフィックを（インターフェイス外の）Fast-Path に送信するか、あるいは引き続きデバイスに送信してさらに分析を行えるようにします。これを使用する利点は、トラフィックに適切なパスを判断する速度にあります。Fast-Path ルールはハードウェア レベルで機能するため、パケットに関する限られた情報だけを確認します。

詳細については、次の項を参照してください。

- IPv4 Fast-Path ルールの追加（4-61 ページ）
- IPv6 Fast-Path ルールの追加（4-62 ページ）
- Fast-Path ルールの削除（4-64 ページ）

IPv4 Fast-Path ルールの追加

ライセンス： すべて

サポートされるデバイス： 8000 シリーズ、3D9900

Fast-Path ルールは、トラフィックを（インターフェイス外の）Fast-Path に送信するか、あるいはデバイスに送信してさらに分析を行えるようにします。Fast-Path に転送して検査を行わない IPv4 トラフィックを、以下の基準を使用して選択できます。

- 発信側または応答側の IP アドレスまたは CIDR ブロック
- protocol
- 発信側または応答側ポート（TCP または UDP プロトコルの場合）
- VLAN ID
- 双方向オプション

Fast-Path ルールには、最も外側の ID が使用されるので注意してください。

ヒント　既存の Fast-Path ルールを編集するには、ルールの横にある編集アイコン（）をクリックします。

IPv4 Fast-Path ルールの作成または編集方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　Fast-Path ルールを追加するデバイスの横にある編集アイコン（）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Device] をクリックします。

[Devices] タブが表示されます。

ステップ 4　[Advanced] セクションの横にある編集アイコン（）をクリックします。

[Advanced] ポップアップ ウィンドウが表示されます。

ステップ 5　Fast-Path ルールを追加するには、[New IPv4 Rule] をクリックします。

[New IPv4 Rule] ポップアップ ウィンドウが表示されます。

ステップ 6　[Domain] ドロップダウン リストから、インライン セットまたはパッシブ セキュリティ ゾーンを選択します。詳細については、「IPS デバイスのセットアップ（5-1 ページ）」を参照してください。

ステップ 7　[Initiator] および [Responder] フィールドに、パケットが以後の分析をバイパスする発信側または応答側の IP アドレスを、CIDR 表記を使用して指定します。

指定された発信側からのパケット、または指定された応答側へのパケットを、ルールに突き合わせます。FireSIGHT システムでの CIDR 表記の使用の詳細については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ステップ 8　(任意)[Protocol] ドロップダウン リストから、ルールの対象となるプロトコルを選択するか、[All] を選択してリストのあらゆるプロトコルのトラフィックを照合するようにします。

ステップ 9　ステップ 8 で TCP または UDP プロトコルを選択した場合は、必要に応じて、[Initiator Port] および [Responder Port] フィールドに発信側と応答側のポートを入力して、対象とするポートを指定します。

ヒント　ルールごとに、カンマで区切ったポート番号のリストを入力できます。IPv4 Fast-Path ルールでは、ポート範囲を使用できません。空白のポート値は、任意として扱われることに注意してください。

[Bidirectional] オプションも選択した場合は、発信側ポートからのパケットまたは応答側へのパケットにフィルタ基準を絞り込みます。

ステップ 10　必要に応じて、[VLAN] フィールドに VLAN ID を入力します。

その VLAN のトラフィックのみを、ルールに突き合わせます。空白の VLAN 値は、任意として扱われることに注意してください。

ステップ 11　必要に応じて、指定した発信側 IP アドレスと応答側 IP アドレスの間で送受信されるすべてのトラフィックをフィルタリングするには、[Bidirectional] オプションを選択します。指定した発信側 IP アドレスから指定した応答側 IP アドレスへのトラフィックのみをフィルタリングする場合は、このオプションをクリアします。

ステップ 12　[Save] をクリックします。

[Advanced] ポップアップ ウィンドウの [Fast-Path Rules] にルールが追加されます。ルールが追加されても、[Save] をクリックしなければルールは保存されません。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください(詳しくはデバイスへの変更の適用 (4-27 ページ)を参照してください)。

IPv6 Fast-Path ルールの追加

ライセンス: すべて

サポートされるデバイス: シリーズ 3、3D9900

Fast-Path ルールは、トラフィックを(インターフェイス外の)Fast-Path に送信するか、あるいはデバイスに送信してさらに分析を行えるようにします。Fast-Path に転送して検査を行わない IPv6 トラフィックを、以下の基準を使用して選択できます。

- 発信側または応答側の IP アドレスまたはアドレス ブロック
- protocol
- 発信側または応答側ポート(TCP または UDP プロトコルの場合)
- VLAN ID
- 双方向オプション

Fast-Path ルールには、最も外側の VLAN ID が使用されるので注意してください。

ヒント　既存の Fast-Path ルールを編集するには、ルールの横にある編集アイコン( )をクリックします。

IPv6 Fast-Path ルールの追加方法：

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　Fast-Path ルールを追加するデバイスの横にある編集アイコン（ ）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Device] をクリックします。

[Devices] タブが表示されます。

ステップ 4　[Advanced] セクションの横にある編集アイコンをクリックします。

[Advanced] ポップアップ ウィンドウが表示されます。

ステップ 5　Fast-Path ルールを追加するには、[New IPv6 Rule] をクリックします。

[New IPv6 Rule] ポップアップ ウィンドウが表示されます。発信側と応答側のフィールドは固定されていることに注意してください。これらのフィールドは、発信側または応答側の IPv6 パケットにフィルタが適用されることを示しています。

ステップ 6　[Domain] ドロップダウン リストから、インライン セットまたはパッシブ セキュリティ ゾーンを選択します。詳細については、「IPS デバイスのセットアップ（5-1 ページ）」を参照してください。

ステップ 7　パケットが以後の分析をバイパスする発信側または応答側の IP アドレスに関して、[Initiator] または [Responder] フィールドに、IP アドレスを入力するか、または IPv6 プレフィクス長の表記を使用してアドレス ブロックを指定します。

指定された発信側からのパケット、または指定された応答側へのパケットを、ルールに突き合わせます。FireSIGHT システムで IPv6 プレフィクス長の表記を使用する方法については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ステップ 8　（任意）[Protocol] ドロップダウン リストから、ルールの対象となるプロトコルを選択するか、[All] を選択してリストのあらゆるプロトコルのトラフィックを照合するようにします。

選択したプロトコルのパケットだけが Fast-Path ルールと照合されます。

ステップ 9　ステップ 7 で TCP または UDP プロトコルを選択した場合は、必要に応じて、[Initiator Port] および [Responder Port] フィールドに発信側と応答側のポートを入力して、対象とするポートを指定します。

ヒント　ルールごとに、カンマで区切ったポート番号のリストを入力できます。IPv6 Fast-Path ルールでは、ポート範囲を使用できません。空白のポート値は、任意として扱われることに注意してください。

ステップ 10　必要に応じて、[VLAN] フィールドに VLAN ID を入力します。

その VLAN のトラフィックのみを、ルールに突き合わせます。空白の VLAN 値は、任意として扱われることに注意してください。

ステップ 11　必要に応じて、[Bidirectional] を選択して、指定した発信側と応答側のポート間で送受信されるすべてのトラフィックをフィルタリングします。発信側ポートからのパケットのみ、または応答側ポートへのパケットのみをルールに突き合わせることを指定する場合は、このオプションをクリアします。

ステップ 12　[Save] をクリックします。

[Advanced] ポップアップ ウィンドウの [Fast-Path Rules] にルールが追加されます。

ステップ 13　[Advanced] ポップアップ ウィンドウで、[Save] をクリックします。

ルールが保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

Fast-Path ルールの削除

ライセンス： すべて

サポートされるデバイス： 8000 シリーズ、3D9900

以下の手順では、IPv4 または IPv6 Fast-Path ルールを削除する方法について説明します。

Fast-Path ルールの削除方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　Fast-Path ルールを削除するデバイスの横にある編集アイコン（）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Device] をクリックします。

[Devices] タブが表示されます。

ステップ 4　[Advanced] セクションの横にある編集アイコン（  ）をクリックします。

[Advanced] ポップアップ ウィンドウが表示されます。

ステップ 5　削除する Fast-Path ルールの横にある削除アイコン（  ）をクリックします。

ステップ 6　プロンプトが出されたら、ルールを削除することを確認します。

ルールが [Advanced] ポップアップ ウィンドウから削除されます。

ステップ 7　[Save] をクリックします。

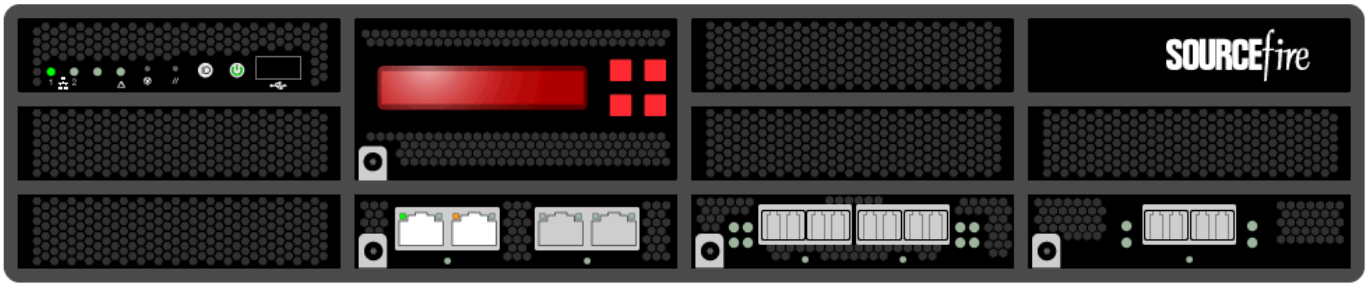
変更が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

センシング インターフェイスの設定

ライセンス： すべて

アプライアンス エディタの [Interfaces] ページで、FireSIGHT システム の展開に応じて、管理対象デバイスのセンシング インターフェイスを設定できます。

[Interfaces] ページの上部に、管理対象のシリーズ 3 デバイスの物理ハードウェア ビューが表示されます。シリーズ 2、仮想デバイス、Cisco NGIPS for Blue Coat X-Series、および ASA FirePOWER デバイスには、物理ハードウェアのビューはありません。以下のグラフィックは、3D8250 のハードウェア ビューを示しています。



以下の表では、物理ハードウェア ビューの使用法について説明しています。

表 4-4　　ハードウェア ビューの使用法

目的	操作
ネットワーク モジュールのタイプ、部品番号、およびシリアル番号を確認する	ネットワーク モジュールの左下隅にある暗い円の上にマウスのカーソルを重ねます。
インターフェイス テーブル ビューでインターフェイスを選択する	インターフェイスをクリックします。
インターフェイス エディタを開く	インターフェイスをダブルクリックします。
インターフェイスの名前、タイプ、リンクの有無、速度設定、およびインターフェイスがバイパス モードになっているかを確認する	インターフェイスの上にマウスのカーソルを重ねます。
エラーまたは警告の詳細を参照する	ネットワーク モジュールの該当するポートの上にマウスのカーソルを重ねます。

シリーズ 3 ハードウェア ビューの下にあるインターフェイス テーブル ビューには、デバイスで使用可能なすべてのインターフェイスが一覧表示されます。テーブル内のナビゲーション ツリーを展開すると、設定されているすべてのインターフェイスを表示できます。インターフェイスの横にある矢印アイコンをクリックして、インターフェイスを縮小または展開することで、サブコンポーネントの非表示/表示を切り替えることができます。このインターフェイス テーブル ビューには、各インターフェイスに関する以下の要約情報が表示されます。[MAC Address] 列と [IP Address] 列が表示されるのは、8000 シリーズ デバイスのみです。詳細については、以下の表を参照してください。

表 4-5　インターフェイス テーブル ビューのフィールド

フィールド	説明
名前	各インターフェイス タイプは、タイプとリンク ステート（該当する場合）を示す固有のアイコンによって表されます。名前またはアイコンの上にマウス ポインタを移動すると、インターフェイス タイプ、速度、デュプレックス モード（該当する場合）がツールチップに表示されます。インターフェイス アイコンについては、表 4-6（4-67 ページ）で説明されています。 アイコンでは、インターフェイスの現在のリンク ステートを示す表示方法が使用されています。次の 3 つの状態のいずれかが表示されます。 • エラー（  ） • 障害（  ） • 利用不可（  ） 論理インターフェイスのリンク状態は、親物理インターフェイスのリンク状態と同じです。Cisco NGIPS for Blue Coat X-Series および ASA FirePOWER デバイスには、リンク状態は表示されません。無効化されたインターフェイスは、半透明のアイコンで表されます。 アイコンの右側に表示されるインターフェイス名は自動生成されます。ただし、ハイブリッド インターフェイスと ASA FirePOWER インターフェイスの名前はユーザによって定義されます。ASA FirePOWER インターフェイスについては、有効で、名前が付けられており、リンクを持つインターフェイスのみが表示されることに注意してください。 物理インターフェイスでは、物理インターフェイスの名前が表示されます。論理インターフェイスでは、物理インターフェイスの名前と、割り当てられている VLAN タグが表示されます。 ASA FirePOWER インターフェイスでは、複数のセキュリティ コンテキストがある場合は、セキュリティ コンテキストの名前とインターフェイスの名前が表示されます。セキュリティ コンテキストが 1 つしかない場合は、インターフェイスの名前のみが表示されます。
Security Zone	インターフェイスが割り当てられているセキュリティ ゾーン。セキュリティ ゾーンを追加または編集するには、編集アイコン（  ）をクリックします。
Used by	インターフェイスが割り当てられているインライン セット、仮想スイッチ、または仮想ルータ。ASA FirePOWER デバイスには、[Used by] 列は表示されません。
MAC アドレス	スイッチド機能およびルーテッド機能で有効にされているインターフェイスに対して表示される MAC アドレス。 仮想デバイスの場合、表示された MAC アドレスにより、デバイス上に設定されたネットワーク アダプタと、[Interfaces] ページに表示されるインターフェイスを対応させることができます。Cisco NGIPS for Blue Coat X-Series および ASA FirePOWER デバイスには、MAC アドレスは表示されません。
IP Addresses	インターフェイスに割り当てられた IP アドレス。マウスのポインタを IP アドレスの上に重ねると、その IP アドレスがアクティブであるか非アクティブであるかを確認できます。非アクティブな IP アドレスはグレー表示されます。ASA FirePOWER デバイスには、IP アドレスは表示されません。

表 4-6　インターフェイス アイコンのタイプと説明

アイコン	インターフェイス タイプ	詳細情報の参照先
	物理的:未設定の物理インターフェイス。	—
	パッシブ:パッシブ展開でトラフィックを分析するように設定されているセンシング インターフェイス。	パッシブ インターフェイスの設定(5-2 ページ)
	インライン:インライン展開でトラフィックを処理するように設定されているセンシング インターフェイス。	インライン インターフェイスの設定(5-3 ページ)
	スイッチド:レイヤ 2 展開でトラフィックを切り替えるように設定されているインターフェイス。	スイッチ型インターフェイスの設定(6-2 ページ)
	ルーテッド:レイヤ 3 展開でトラフィックをルーティングするように設定されているインターフェイス。	ルーテッド インターフェイスの設定(7-1 ページ)
	HA:デバイス間で冗長通信チャネルとして機能するように設定されている、デバイスのクラスタ ペア メンバー上のインターフェイス(別名「ハイ アベイラビリティ リンク インターフェイス」)。	HA リンク インターフェイスの設定(4-68 ページ)
	集約:1 つの論理リンクとして設定されている複数の物理インターフェイス。	集約インターフェイスのセットアップ(8-1 ページ)
	集約スイッチド:レイヤ 2 展開で 1 つの論理リンクとして設定されている複数の物理インターフェイス。	集約スイッチド インターフェイスの追加(8-5 ページ)
	集約ルーテッド:レイヤ 3 展開で 1 つの論理リンクとして設定されている複数の物理インターフェイス。	集約ルーテッド インターフェイスの追加(8-8 ページ)
	ハイブリッド:仮想ルータと仮想スイッチ間でトラフィックをブリッジするように設定されている論理インターフェイス。	論理ハイブリット インターフェイスの追加(9-1 ページ)
	ASA FirePOWER:ASA FirePOWER モジュールがインストールされた ASAデバイスに設定されているインターフェイス。	Cisco ASA with FirePOWER Servicesインターフェイスの管理(4-70 ページ)

管理対象の FirePOWER デバイスには、合計 1024 個のインターフェイスを設定できることに注意してください。

注　Defense Centerでは、ASA FirePOWER デバイスが SPAN ポート モードで展開されている場合、ASA インターフェイスを表示しません。

デバイスにインターフェイスを設定するさまざまな方法の詳細については、以下の項を参照してください。

- HA リンク インターフェイスの設定(4-68 ページ)
- 管理対象デバイスの MTU の範囲(4-69 ページ)
- Cisco ASA with FirePOWER Servicesインターフェイスの管理(4-70 ページ)

- インターフェイスの無効化（4-71 ページ）
- 重複する接続ロギングの防止（4-71 ページ）
- IPS デバイスのセットアップ（5-1 ページ）
- 仮想スイッチのセットアップ（6-1 ページ）
- 仮想ルータのセットアップ（7-1 ページ）
- 集約インターフェイスのセットアップ（8-1 ページ）
- ハイブリッド インターフェイスの設定（9-1 ページ）

HA リンク インターフェイスの設定

ライセンス： すべて

サポートされるデバイス： シリーズ 3

デバイス クラスタを確立した後、物理インターフェイスをハイ アベイラビリティ（HA）リンク インターフェイスとして設定できます。このリンクは、クラスタを構成するデバイス間でヘルス情報を共有するために使用する、冗長通信チャネルとして機能します。1 つのデバイスに HA リンク インターフェイスを設定すると、自動的に 2 番目のデバイスにインターフェイスが設定されます。同じブロードキャスト ドメインに、両方の HA リンクを設定する必要があります。詳細については、「デバイスのクラスタリング（4-31 ページ）」を参照してください。

ダイナミック NAT は、他の IP アドレスとポートにマップする IP アドレスとポートの動的割り当てに依存します。HA リンクがなければ、これらのマッピングはフェールオーバーで失われます。その場合、変換されたすべての接続はクラスター内で新しくアクティブになったデバイスを介してルーティングされることになるため、それらの接続は失敗します。

注意　センシング インターフェイスまたはインライン セットの MTU の任意の値（シリーズ 2）または最高値（シリーズ 3）を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック検査が一時的に中断されます。この検査中にデバイスがトラフィックをドロップするか、それ以上検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

HA リンク インターフェイスを設定するには、以下を行います。

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　HA リンク インターフェイスを設定する、クラスタを構成するデバイスの横にある編集アイコン（）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　HA リンク インターフェイスとして設定するインターフェイスの横にある編集アイコン（）をクリックします。

[Edit Interface] ポップアップ ウィンドウが表示されます。

ステップ 4　[HA Link] をクリックして HA オプションを表示します。

ステップ 5　[Enabled] チェック ボックスをオンにして、HA リンク インターフェイスがリンクを提供できるようにします。

このチェック ボックスをオフにすると、インターフェイスは無効になり、管理上はダウンした状態になります。

ステップ 6　[Mode] ドロップダウン リストからリンク モードを指定するオプションを選択するか、[Autonegotiation] を選択して、速度とデュプレックスの設定を自動ネゴシエートするようにインターフェイスを設定します。

ステップ 7　[MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または Auto-MDIX のいずれかを指定するオプションを選択します。

通常、[MDI/MDIX] は [Auto-MDIX] に設定します。これにより、MDI と MDIX の間の切り替えが自動的に処理され、リンクが確立されます。

ステップ 8　[MTU] フィールドに、最大伝送ユニット (MTU) を入力して、パケットの最大許容サイズを指定します。

設定可能な MTU の範囲は、FireSIGHT システムのデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、「管理対象デバイスの MTU の範囲（4-69 ページ）」を参照してください。

ステップ 9　[Save] をクリックします。

変更が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

管理対象デバイスの MTU の範囲

ライセンス：すべて

注意　センシング インターフェイスまたはインライン セットの MTU の任意の値（シリーズ 2）または最高値（シリーズ 3）を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック検査が一時的に中断されます。この検査中にデバイスがトラフィックをドロップするか、それ以上検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

Cisco NGIPS for Blue Coat X-Series の場合は、Cisco NGIPS for Blue Coat X-Series CLI を使用してインターフェイス MTU を設定することに注意してください。詳細については、『*Cisco NGIPS for Blue Coat X-Series Installation Guide*』を参照してください。

注　システムは、設定された MTU 値から自動的に 18 バイトを削減するため、IPv6 の場合、1298 未満の値は MTU の最小値である 1280 に準拠しません。IPv4 の場合は、594 未満の値は MTU の最小値 576 に準拠しません。たとえば、構成値 576 は自動的に 558 に削減されます。

以下の表に、管理対象デバイスの MTU 設定範囲をリストします。

表 4-7　デバイスごとの MTU 範囲

デバイス モデル	MTU 範囲
シリーズ 2（3D6500、3D9900 を除く）	576 ～ 1518（すべてのインターフェイス、インライン セット）
3D6500、3D9900、仮想	576 ～ 9018（すべてのインターフェイス、インライン セット）
シリーズ 3	576 ～ 9234（管理インターフェイス） 576 ～ 10172（インライン セット、パッシブ インターフェイス） 576 ～ 9922（その他）

Cisco ASA with FirePOWER Servicesインターフェイスの管理

ライセンス： Protection

サポートされるデバイス： ASA FirePOWER

ASA FirePOWER インターフェイスを編集する際に、FireSIGHT Defense Centerから設定できるのは、インターフェイスのセキュリティ ゾーンのみです。詳細については、「セキュリティ ゾーンの操作（3-42 ページ）」を参照してください。

ASA FirePOWER インターフェイスを完全に設定するには、ASA 専用ソフトウェアおよび CLI を使用します。ASA FirePOWER デバイスを編集して、マルチ コンテキスト モードからシングル コンテキスト モード（またはその逆）に切り替えると、デバイスはそのインターフェイスの名前をすべて変更します。ASA FirePOWER の更新されたインターフェイス名を使用するように、すべての FireSIGHT システム セキュリティ ゾーン、相関ルール、関連する設定を再設定する必要があります。ASA FirePOWER インターフェイスの設定の詳細については、ASA のマニュアルを参照してください。

注　ASA FirePOWER インターフェイスのタイプは変更できません。また、FireSIGHT Defense Center からインターフェイスを無効にすることもできません。

ASA FirePOWER インターフェイスを編集するには、以下を行います。

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　インターフェイスを編集するデバイスの横にある編集アイコン（）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　編集するインターフェイスの横にある編集アイコン（）をクリックします。

[Edit Interface] ポップアップ ウィンドウが表示されます。

ステップ 4　[Security Zone] ドロップダウンリストから、既存のセキュリティ ゾーンを選択するか、または [New] を選択して、新しいセキュリティ ゾーンを追加します。

ステップ 5　[Save] をクリックします。

セキュリティ ゾーンが設定されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

インターフェイスの無効化

ライセンス： すべて

インターフェイス タイプを [None] に設定することで、インターフェイスを無効にすることができます。無効にされたインターフェイスは、インターフェイス リストでグレー表示されます。

注　ASA FirePOWER インターフェイスのタイプは変更できません。また、FireSIGHT Defense Center からインターフェイスを無効にすることもできません。

インターフェイスを無効にするには、以下を行います。

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　インターフェイスを無効にするデバイスの横にある編集アイコン（）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　無効にするインターフェイスの横にある編集アイコン（）をクリックします。

[Edit Interface] ポップアップ ウィンドウが表示されます。

ステップ 4　[None] をクリックします。

ステップ 5　[Save] をクリックします。

変更が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

重複する接続ロギングの防止

ライセンス： すべて

セキュリティ ゾーン オブジェクトを更新すると、システムはそのオブジェクトの新しいリビジョンを保存します。その結果、同じセキュリティ ゾーン内の管理対象デバイスに、インターフェイスで設定されたセキュリティ オブジェクトの異なるリビジョンがある場合、接続が重複しているようなログが記録される可能性があります。

接続の重複が報告されていることに気づいた場合、同じリビジョンのオブジェクトを使用するよう、すべての管理対象デバイスを更新できます。

デバイス全体でセキュリティ ゾーン オブジェクトのリビジョンを同期するには、以下を行います。

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

注意　同期させるすべてのデバイスでインターフェイスのゾーン設定を編集するまでは、管理対象デバイスの変更を他のデバイスに再適用しないでください。

ステップ 2　セキュリティ ゾーンの選択を更新するデバイスの横にある編集アイコン（  ）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　重複する接続のイベントを記録しているインターフェイスのそれぞれについて、[Security Zone] を別のゾーンに変更して [Save] をクリックした後、目的のゾーンに再び設定し、もう一度 [Save] をクリックします。

ステップ 4　重複イベントを記録しているデバイスごとに、ステップ 2 から 3 を繰り返します。

ステップ 5　すべてのデバイスのすべてのインターフェイスを編集した後、デバイスの変更を同時にすべての管理対象デバイスに適用します。

IPS デバイスのセットアップ

パッシブまたはインラインのいずれかの IPS 展開でデバイスを設定できます。パッシブ展開では、ネットワーク トラフィックのフローからアウトオブバンドでシステムを展開します。インライン展開では、2 つのポートを一緒にバインドすることで、ネットワーク セグメント上でシステムを透過的に設定します。

以下の項では、FireSIGHT システムのパッシブ展開とインライン展開用にデバイスを設定する方法について説明します。

パッシブ IPS 展開について

ライセンス： Protection

パッシブ（受動）IPS 展開では、FireSIGHT システムは、スイッチ SPAN またはミラー ポートを使用してネットワークを流れるトラフィックを監視します。SPAN またはミラー ポートでは、スイッチ上の他のポートからトラフィックをコピーできます。これにより、ネットワーク トラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。パッシブ展開で設定された場合、システムはトラフィックのブロッキングやシェーピングなど、特定のアクションを実行することができません。パッシブ インターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信されたトラフィックは再送されません。

注 アウトバウンド トラフィックにはフロー制御パケットが含まれています。そのため、アプライアンスのパッシブ インターフェイスにアウトバウンド トラフィックが表示されることがあり、設定によっては、イベントが生成されることもあります。これは正常な動作です。

パッシブ インターフェイスの設定

ライセンス： Protection

管理対象デバイス上の 1 つ以上の物理ポートをパッシブ インターフェイスとして設定できます。

Cisco パッケージのインストール時に、Cisco NGIPS for Blue Coat X-Series インターフェイスをパッシブまたはインラインのいずれかに設定します。FireSIGHT システム Web インターフェイスを使用して、Cisco NGIPS for Blue Coat X-Series インターフェイスを再設定することはできません。詳細については、Blue Coat X シリーズ インターフェイス用の Cisco NGIPS の設定（5-12 ページ）を参照してください。

注意　センシング インターフェイスまたはインライン セットの MTU の任意の値（シリーズ 2）または最高値（シリーズ 3）を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック検査が一時的に中断されます。この検査中にデバイスがトラフィックをドロップするか、それ以上検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

パッシブ インターフェイスを設定する方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　パッシブ インターフェイスを設定するデバイスの横にある編集アイコン（  ）をクリックします。

[Interfaces] タブが表示されます。

ステップ 3　パッシブ インターフェイスとして設定するインターフェイスの横にある編集アイコン（  ）をクリックします。

[Edit Interface] ポップアップ ウィンドウが表示されます。

ステップ 4　[Passive] をクリックして、パッシブ インターフェイスのオプションを表示させます。

ステップ 5　オプションで、[Security Zone] ドロップダウン リストから既存のセキュリティ ゾーンを選択するか、または [New] を選択して新しいセキュリティ ゾーンを追加します。

ステップ 6　[Enabled] チェック ボックスをオンにして、パッシブ インターフェイスがトラフィックを監視できるようにします。

このチェック ボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

ステップ 7　[Mode] ドロップダウン リストからリンク モードを指定するオプションを選択するか、または [Autonegotiation] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようにインターフェイスを設定します。モード設定は銅線インターフェイス専用であることに注意してください。

注　8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。

ステップ 8　[MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または Auto-MDIX のいずれかを指定するオプションを選択します。MDI/MDIX 設定は銅線インターフェイス専用であることに注意してください。

デフォルトでは、MDI/MDIX は **Auto-MDIX** に設定され、MDI と MDIX の間のスイッチングを自動的に処理してリンクを確立します。

ステップ 9　[MTU] フィールドに、最大伝送ユニット (MTU) を入力して、パケットの最大許容サイズを指定します。

設定可能な MTU の範囲は、FireSIGHT システムのデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、「管理対象デバイスの MTU の範囲（4-69 ページ）」を参照してください。

ステップ 10　[Save] をクリックします。

パッシブ インターフェイスが設定されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

インライン IPS 展開について

ライセンス： Protection

インライン展開では、2 つのポートを一緒にバインドすることで、ネットワーク セグメント上で FireSIGHT システムを透過的に設定します。これによって、隣接するネットワーク デバイスの設定がなくても、任意のネットワーク環境にシステムをインストールすることができます。インライン インターフェイスはすべてのトラフィックを無条件に受信しますが、これらのインターフェイスで受信されたすべてのトラフィックは、明示的にドロップされない限り、インライン セットの外部に再送信されます。

インライン インターフェイスの設定

ライセンス： Protection

管理対象デバイス上の 1 つ以上の物理ポートをインライン インターフェイスとして設定できます。インライン展開でトラフィックを処理するには、その前に、インライン セットにインライン インターフェイスのペアを割り当てる必要があります。

インライン ペアのインターフェイスをそれぞれ異なる速度に設定した場合、またはインターフェイスが異なる速度にネゴシエートされる場合は、システムによって警告が出されることに注意してください。

Cisco パッケージのインストール時に、Cisco NGIPS for Blue Coat X-Series インターフェイスをパッシブまたはインラインのいずれかに設定します。FireSIGHT システム Web インターフェイスを使用して、Cisco NGIPS for Blue Coat X-Series インターフェイスを再設定することはできません。詳細については、Blue Coat X シリーズ インターフェイス用の Cisco NGIPS の設定（5-12 ページ）を参照してください。

注　あるインターフェイスをインライン インターフェイスとして設定した場合、ペアを完成させるために、NetMod の隣接ポートもまた自動的にインライン インターフェイスになります。

仮想デバイスでインライン インターフェイスを設定するには、隣接するインターフェイスを使用してインライン ペアを作成する必要があります。

インライン インターフェイスを設定する方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　インライン インターフェイスを設定するデバイスの横にある編集アイコン（）をクリックします。

[Interfaces] タブが表示されます。

ステップ 3　インライン インターフェイスとして設定するインターフェイスの横にある編集アイコン（）をクリックします。

[Edit Interface] ポップアップ ウィンドウが表示されます。

ステップ 4　[Inline] をクリックして、インライン インターフェイスのオプションを表示させます。

ステップ 5　オプションで、[Security Zone] ドロップダウン リストから既存のセキュリティ ゾーンを選択するか、または [New] を選択して新しいセキュリティ ゾーンを追加します。

ステップ 6　[Inline Set] ドロップダウン リストから既存のインライン セットを選択するか、または [New] を選択して新しいインライン セットを追加します。

新しいインライン セットを追加した場合は、インライン インターフェイスのセットアップ後に、そのインライン セットを [Device Management] ページ（[Devices] > [Device Management] > [Inline Sets]）で設定する必要があることに注意してください。詳細については、インライン セットの追加（5-7 ページ）を参照してください。

ステップ 7　[Enabled] チェック ボックスをオンにして、インライン インターフェイスがトラフィックを処理できるようにします。

このチェック ボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

ステップ 8　[Mode] ドロップダウン リストからリンク モードを指定するオプションを選択するか、または [Autonegotiation] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようにインターフェイスを設定します。モード設定は銅線インターフェイスにのみ使用できることに注意してください。

注　8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。

ステップ 9　[MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または Auto-MDIX のいずれかを指定するオプションを選択します。MDI/MDIX 設定は銅線インターフェイス専用であることに注意してください。

デフォルトでは、MDI/MDIX は **Auto-MDIX** に設定され、MDI と MDIX の間のスイッチングを自動的に処理してリンクを確立します。

ステップ 10　[Save] をクリックします。

インライン インターフェイスが設定されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

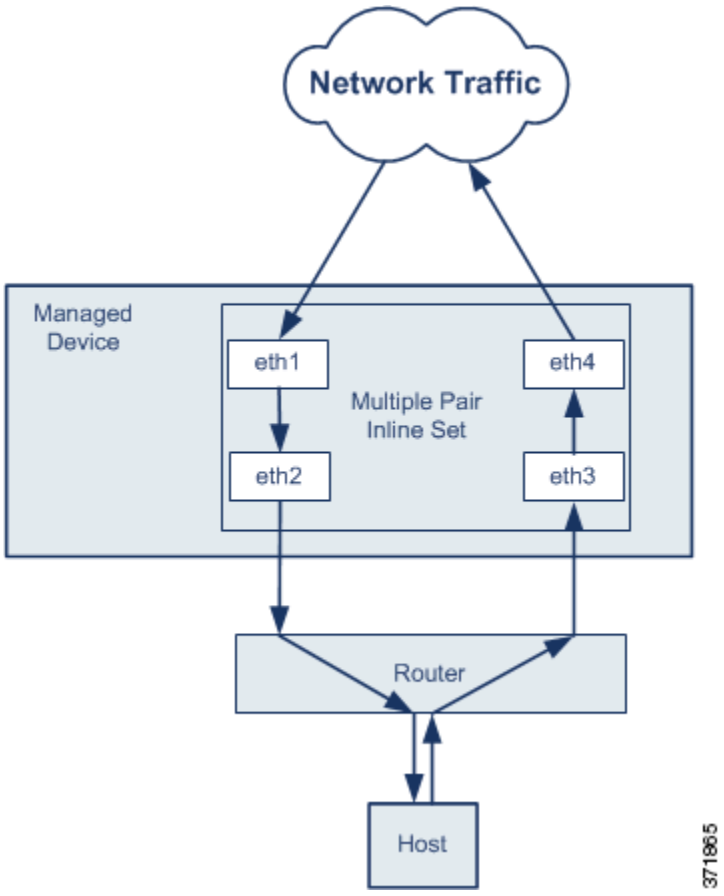
インライン セットの設定

ライセンス： Protection

インライン展開でインライン インターフェイスを使用するには、その前に、インライン セットを設定してインライン インターフェイス ペアをそれらに割り当てる必要があります。インライン セットは、デバイス上の 1 つ以上のインライン インターフェイス ペアからなるグループです。インライン インターフェイス ペアは、同時に 1 つのインライン セットにのみ属することができます。

デバイス トラフィックがインバウンドであるかアウトバウンドであるかに応じて、異なるインライン インターフェイス ペアを介してネットワーク上のホストと外部ホスト間のトラフィックをルーティングするように、管理対象デバイスのインターフェイスを設定できます。これは *非同期ルーティング*設定です。非同期ルーティングを展開し、インライン セットに 1 つのインターフェイス ペアしか含めないと、デバイスがトラフィックの半分しか認識しないため、ネットワーク トラフィックが適切に分析されない可能性があります。同じインライン インターフェイス セットに複数のインライン インターフェイス ペアを追加すると、システムがインバウンド トラフィックとアウトバウンド トラフィックを同じトラフィック フローの一部として識別できるようになります。これは、同じセキュリティ ゾーンにインターフェイス ペアを含めることによっても実現できます。

非同期ルーティング構成を通過するトラフィックから接続イベントが生成された場合、そのイベントは同じインライン インターフェイス ペアの入力インターフェイスと出力インターフェイスを識別できます。たとえば、次の図の構成では、**eth3** を入力インターフェイス、**eth2** を出力インターフェイスとして識別する接続イベントが生成されます。これは、この構成の予期される動作です。



注　単一のインライン インターフェイス セットに複数のインターフェイス ペアを割り当てたときに、重複トラフィックの問題が発生した場合は、システムがパケットを一意に識別できるように再設定します。たとえば、別のインライン セットにインターフェイス ペアを再度割り当てるか、セキュリティ ゾーンを変更することができます。

インライン セットを使用するデバイスでは、デバイス再起動後にパケットを転送するようソフトウェア ブリッジが自動的にセットアップされます。デバイスが再起動しているときには、実行中のソフトウェア ブリッジがありません。インライン セットでバイパス モードを有効にすると、デバイスの再起動中にハードウェア バイパスになります。その場合、システムが停止して再起動する際に、デバイスとのリンクの再ネゴシエーションが原因で数秒間のパケットが失われる可能性があります。ただし、Snort の再起動中にシステムはトラフィックを通過させます。

フェール オープンまたはハードウェア バイパス モードで有効にしたデバイスは、システムを再起動するか、インライン セットの設定を編集して適用するか、またはポリシーを適用したときに、ハードウェア バイパス モードを自動的に終了することに注意してください。

注意　センシング インターフェイスまたはインライン セットの MTU の任意の値（シリーズ 2）または最高値（シリーズ 3）を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック検査が一時的に中断されます。この検査中にデバイスがトラフィックをドロップするか、それ以上検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

詳細については、次の項を参照してください。

- インライン セットの表示（5-6 ページ）
- インライン セットの追加（5-7 ページ）
- インライン セットの詳細オプションの設定（5-8 ページ）
- インライン セットの削除（5-12 ページ）

インライン セットの表示

ライセンス： Protection

[Device Management] ページの [Inline Sets] タブには、デバイスに設定されているすべてのインライン セットのリストが表示されます。仮想デバイスまたは Cisco NGIPS for Blue Coat X-Series で、バイパス モードになるようインライン セットを設定できないことに注意してください。「インライン セット テーブル ビューのフィールド」表には、各セットの要約情報が含まれています。

表 5-1　インライン セット テーブル ビューのフィールド

フィールド	説明
名前	インライン セットの名前。
Interface Pairs	インライン セットに割り当てられたインライン インターフェイスのすべてのペアを示すリスト。[Interfaces] タブでペアのいずれかのインターフェイスを無効にした場合、そのペアは含まれません。
Bypass	インライン セットの設定済みバイパス モード。

インライン セットの追加

ライセンス：Protection

[Device Management] ページの [Inline Sets] タブからインライン セットを追加できます。または、インライン インターフェイスを設定するときにインライン セットを追加できます。

インライン セットにはインライン インターフェイス ペア**のみ**を割り当てることができます。管理対象デバイスでインライン インターフェイスを設定する前にインライン セットを作成する必要がある場合は、空のインライン セットを作成し、あとでそれにインターフェイスを追加できます。

インライン セットを追加する方法：

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　インライン セットを追加するデバイスの横にある編集アイコン（ ）をクリックします。

[Interfaces] タブが表示されます。

ステップ 3　[Inline Sets] をクリックします。

[Inline Sets] タブが表示されます。

ステップ 4　[Add Inline Set] をクリックします。

[Add Inline Set] ポップアップ ウィンドウが表示されます。

ステップ 5　[Name] フィールドに、インライン セットの名前を入力します。英数字とスペースを使用できます。

ステップ 6　インライン セットに追加するインライン インターフェイス ペアを選択する方法として、次の 2 つのオプションがあります。

- [Interfaces] の横で、1 つ以上のインライン インターフェイス ペアを選択し、選択項目の追加アイコン（ ）をクリックします。複数のインライン インターフェイス ペアを選択するには、Ctrl キーまたは Shift キーを使用します。
- すべてのインターフェイス ペアをインライン セットに追加するには、「すべてを追加」アイコン（ ）をクリックします。

ヒント　インライン セットからインライン インターフェイスを削除するには、1 つ以上のインライン インターフェイス ペアを選択して、選択項目の削除アイコン（ ）をクリックします。インライン セットからすべてのインターフェイス ペアを削除するには、「すべてを削除」アイコン（ ）をクリックします。また、[Interfaces] タブでペアのいずれかのインターフェイスを無効にすると、ペアが削除されます。

ステップ 7　[MTU] フィールドに、最大伝送ユニット (MTU) を入力して、パケットの最大許容サイズを指定します。

設定可能な MTU の範囲は、FireSIGHT システムのデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、「管理対象デバイスの MTU の範囲（4-69 ページ）」を参照してください。

ステップ 8　(任意)トラフィックが検出をバイパスしてデバイスを引き続き通過することを許可するには、[Failsafe] を選択します。管理対象デバイスは、内部トラフィック バッファを監視し、それらのバッファが満杯である場合は検出をバイパスします。

内部トラフィック バッファがいっぱいになったが、特定の状況下でデバイスがまだパケットをドロップする可能性がある場合は、インライン セットまたはパッシブ インターフェイスでデバイスの [Failsafe] を有効にすると、ドロップされたパケットのリスクが大幅に軽減されます。最悪の場合は、デバイスで一時的にネットワークが停止することがあります。

なお、このオプションは、シリーズ 3 デバイスでのみ使用できます。

ステップ 9　インターフェイスでの障害発生時にインライン インターフェイスのリレーがどのように応答するかを設定するために、次のようにバイパス モードを選択します。

- トラフィックがインターフェイスを通過し続けることを許可するには、[Bypass] を選択します。

フェール オープンまたはハードウェア バイパス モードで有効にしたデバイスは、システムを再起動するか、インライン セットの設定を編集して適用するか、またはポリシーを適用したときに、ハードウェア バイパス モードを自動的に終了することに注意してください。

- トラフィックをブロックするには、[Non-Bypass] を選択します。

注　バイパス モードでは、アプライアンスのリブート時に少数のパケットが失われることがあります。また、クラスタ デバイス上のインライン セット、仮想デバイスまたは Cisco NGIPS for Blue Coat X-Series 上のインライン セット、8000 シリーズ デバイス上の非バイパス NetMod、および 3D7115 または 3D7125 デバイス上の SFP モジュールに対しては、バイパス モードを設定できないので注意してください。

ステップ 10　[OK] をクリックします。

インライン セットが追加されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください(詳しくはデバイスへの変更の適用(4-27 ページ)を参照してください)。

ヒント　タップ モード、リンク ステート伝達、トランスペアレント インライン モードなど、インライン セットの詳細設定については、インライン セットの詳細オプションの設定(5-8 ページ)を参照してください。

インライン セットの詳細オプションの設定

ライセンス: Protection

サポートされるデバイス: 機能によって異なる

インライン セットを設定する際に考慮できるオプションがいくつかあります。各オプションの詳細については、後述の項を参照してください。

タップ モード

サポートされるデバイス: シリーズ 3

シリーズ 3 デバイスでは、インライン(またはフェール オープン付きインライン)インターフェイス セットを作成するときにタップ モードを使用できます。

タップ モードの場合、デバイスはインラインで展開されますが、パケットがデバイスを通過する代わりに各パケットのコピーがデバイスに送信され、ネットワーク トラフィック フローは影響を受けません。パケット自体ではなくパケットのコピーを処理するため、ドロップするように設定したルール、および置換キーワードを使用するルールはパケット ストリームに影響を与えません。ただし、これらのタイプのルールでは、トリガーされた侵入イベントが生成され、侵入イベントのテーブル ビューには、トリガーの原因となったパケットがインライン展開でドロップされたことが示されます。

インライン展開されたデバイスでタップ モードを使用することには、利点があります。たとえば、デバイスがインラインであるかのようにデバイスとネットワークの間の配線をセットアップし、デバイスが生成するタイプの侵入イベントを分析することができます。その結果に基づいて、効率性に影響を与えることなく最適なネットワーク保護を提供するように、侵入ポリシーを変更して廃棄ルールを追加できます。デバイスをインラインで展開する準備ができたら、タップ モードを無効にして、デバイスとネットワークの間の配線を再びセットアップすることなく、不審なトラフィックをドロップし始めることができます。

同じインライン セットでこのオプションと厳密な TCP 強制を有効にすることはできないことに注意してください。

リンク ステートの伝搬

サポートされるデバイス： シリーズ 2、シリーズ 3

リンク ステート伝播は、インライン セットのペアの両方で状態を追跡できるよう、バイパス モードで設定されるインライン セットの機能です。リンク ステート伝搬は、銅線および光ファイバの両方の設定可能なバイパス インターフェイスで使用できます。

リンク ステート伝播によって、インライン セットのインターフェイスの 1 つが停止した場合、インライン インターフェイス ペアのもう 2 番目のインターフェイスも自動的に停止されます。停止したインターフェイスが再び起動すると、2 番目のインターフェイスも自動的に起動します。つまり、1 つのインターフェイスのリンク ステートが変化すると、アプライアンスはその変化を検知し、それに合わせて他のインターフェイスのリンク ステートを更新します。ただし、アプライアンスがリンク ステートの変更を伝達するのに最大 4 秒かかります。

注　リンク ステート伝達がトリガーされると、シリーズ 2 デバイスでフェール オープンとして設定された光ファイバ インライン セットは、ハードウェア バイパス モードをアクティブ化します。この場合、関連するインターフェイス カードのバイパスは自動的に終了しません。バイパス モードを手動で解除する必要があります。インライン セットの光ファイバ インターフェイスおよびハードウェア バイパスの詳細については、フェール オープンに設定された光ファイバ インライン セットでのバイパス モードの除去（5-11 ページ）を参照してください。

障害状態のネットワーク デバイスを避けてトラフィックを自動的に再ルーティングするようルータが設定された復元力の高いネットワーク環境では、リンク ステート伝播が特に有効です。

クラスタ化されたデバイスで設定されたインライン セットのリンク ステートの伝達を無効にすることはできません。

仮想デバイス、Cisco NGIPS for Blue Coat X-Series、および Cisco ASA with FirePOWER Services では、リンク ステートの伝達がサポートされないので注意してください。

トランスペアレント インライン モード

トランスペアレント インライン モード オプションを使用すると、デバイスは「Bump In The Wire」として機能できます。これは、送信元/宛先に関係なく、認識されるすべてのネットワーク トラフィックをデバイスが転送することを意味します。シリーズ 3 および 3D9900 のデバイスではこのオプションを無効にできないことに注意してください。

厳密な TCP 強制

サポートされるデバイス： シリーズ 3

最大の TCP セキュリティを実現するには、厳密な強制を有効にできます。この機能は、3 ウェイ ハンドシェイクが完了していない接続をブロックします。厳密な適用では次のパケットもブロックされます。

- 3 ウェイ ハンドシェイクが完了していない接続の非 SYN TCP パケット
- 応答側が SYN-ACK を送信する前に TCP 接続の発信側から送信された非 SYN/RST パケット
- SYN の後ではあるがセッションの確立前に TCP 接続の応答側から送信された非 SYN-ACK/RST パケット
- イニシエータまたはレスポンダからの、確立済みの TCP 接続上の SYN パケット

シリーズ 2、仮想デバイス、および Cisco NGIPS for Blue Coat X-Series では、このオプションがサポートされないことに注意してください。また、同じインライン セットで、このオプションとタップ モードを有効にすることはできません。

高度なインライン セット オプションを設定する方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　インライン セットを編集するデバイスの横にある編集アイコン( )をクリックします。

[Interfaces] タブが表示されます。

ステップ 3　[Inline Sets] をクリックします。

[Inline Sets] タブが表示されます。

ステップ 4　編集するインライン セットの横にある編集アイコン( )をクリックします。

[Edit Inline Set] ポップアップ ウィンドウが表示されます。

ステップ 5　[Advanced] をクリックします。

[Advanced] タブが表示されます。

ステップ 6　オプションで、シリーズ 3 デバイスのインライン インターフェイスでタップ モードを有効にするために [Tap Mode] を選択します。

仮想デバイス、Cisco NGIPS for Blue Coat X-Series、および シリーズ 2 デバイス（3D9900 を除く）ではこのオプションがサポートされないことに注意してください。さらに、同じインライン セットで、[Tap Mode] と [Strict TCP Enforcement] を有効にすることはできません。

ステップ 7　オプションで、シリーズ 2 またはシリーズ 3 デバイスで [Propagate Link State] を選択します。停止したネットワーク デバイスを避けてトラフィックを再ルーティングする機能がネットワークのルータに備わっている場合、このオプションが特に便利です。

クラスタ化されたデバイスで設定されたインライン セットのリンク ステートの伝達を無効にすることはできません。

仮想デバイスおよび Cisco NGIPS for Blue Coat X-Series では、このオプションがサポートされないことに注意してください。

ステップ 8　オプションで、シリーズ 3 デバイスで厳密な TCP 強制を有効にするために [Strict TCP Enforcement] を選択します。

シリーズ 2、仮想デバイス、および Cisco NGIPS for Blue Coat X-Series では、このオプションがサポートされないことに注意してください。また、同じインライン セットで、[Strict TCP Enforcement] と [Tap Mode] を有効にすることはできません。

ステップ 9　オプションで、[Transparent Inline Mode] を選択します。

シリーズ 3 デバイスではこのオプションを無効にできないことに注意してください。

ステップ 10　[OK] をクリックします。

変更が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

フェール オープンに設定された光ファイバ インライン セットでのバイパス モードの除去

ライセンス： Protection

サポートされるデバイス： シリーズ 2

フェール オープンに設定された光ファイバ インライン セットを持つシリーズ 2 デバイスでリンク ステート伝達が有効になっている場合、そのデバイスがバイパス モードになると、すべてのネットワーク トラフィックは分析されずにインライン セットを通過します。リンクが復元した場合、フェール オープンに設定されているほとんどの光ファイバ インライン セットは、自動的にはバイパスから戻りません。コマンド ライン ツールを使用して、インライン セットのバイパス モードを強制的に解除できます。

このツールは、フェール オープンに設定された光ファイバ インライン インターフェイスを持つインライン セットに対して機能します。フェール オープンに設定された銅線インライン インターフェイスを持つインライン セットでこのツールを使用する必要はありません。

注　デバイス上でフェール オープンに設定されたインライン セットに問題がある場合は、サポート担当に連絡してください。

デバイス上で、フェール オープンに設定された光ファイバ インライン セットのバイパス モードを強制的に解除する方法：

アクセス： Admin/Network Admin

ステップ 1　デバイスでターミナル ウィンドウを開き、admin ユーザとしてサインインします。

ステップ 2　コマンドラインに次のように入力します。

```
sudo /var/sf/bin/unbypass_cards.sh
```

パスワードを求めるプロンプトが表示されます。

ステップ 3　インターフェイスを切り替えてバイパス モードを解除すると、デバイスがトラフィックを分析していることを示すメッセージが syslog に表示されます。次に例を示します。

```
Fiber pair has been reset by un_bypass
```

インライン セットの削除

ライセンス：Protection

インライン セットを削除すると、そのセットに割り当てられたインライン インターフェイスを別のセットに含めることができるようになります。それらのインターフェイスは削除されません。

インライン セットを削除する方法：

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　インライン セットを削除するデバイスの横にある編集アイコン（ ）をクリックします。

[Interfaces] タブが表示されます。

ステップ 3　[Inline Sets] をクリックします。

[Inline Sets] タブが表示されます。

ステップ 4　削除するインライン セットの横にある削除アイコン（ ）をクリックします。

ステップ 5　プロンプトが表示されたら、インライン セットを削除することを確認します。

インライン セットが削除されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

Blue Coat X シリーズ インターフェイス用の Cisco NGIPS の設定

ライセンス：Protection

サポートされるデバイス：X-Series

Cisco NGIPS for Blue Coat X-Series パッケージを展開するとき、またはパッケージをインストールした後で、パッシブ インターフェイスまたはインライン インターフェイスを作成します。Cisco NGIPS for Blue Coat X-Series をDefense Centerに追加するときには、これらのインターフェイスがすでに設定済みです。Cisco NGIPS for Blue Coat X-Series は、高度な設定オプションをサポートしていません。

FireSIGHT システム Web インターフェイスを使用して、Cisco NGIPS for Blue Coat X-Series インターフェイスを再設定することはできません。再設定するには、まずDefense Centerから現在のインターフェイスを削除した後、新しいインターフェイスを作成する必要があります。インターフェイスの作成と削除の詳細については、『*Cisco NGIPS for Blue Coat X-Series Installation Guide*』を参照してください。

Cisco NGIPS for Blue Coat X-Series でインターフェイスを設定する方法：

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　設定するデバイスの横にある編集アイコン()をクリックします。

[Interfaces] タブが表示されます。すべての Cisco NGIPS for Blue Coat X-Series インターフェイスで、リンクが常にアクティブ()と表示されることに注意してください。

ステップ 3　設定するインターフェイスの横にある編集アイコン()をクリックします。

ステップ 4　[Security Zone] ドロップダウンリストから、既存のセキュリティ ゾーンを選択するか、または [New] を選択して、新しいセキュリティ ゾーンを追加します。

ステップ 5　(任意)インライン インターフェイスの場合は、[Inline Set] ドロップダウン リストから既存のインライン セットを選択するか、[New] を選択して新しいインライン セットを追加します。

新しいインライン セットを追加した場合は、インライン インターフェイスのセットアップ後に、そのインライン セットを [Device Management] ページ([Devices] > [Device Management] > [Inline Sets])で設定する必要があることに注意してください。詳細については、インライン セットの追加(5-7 ページ)を参照してください。

ステップ 6　[Save] をクリックします。

インターフェイスが設定されます。メニュー バーの右上にある [Apply Changes] をクリックしてデバイス設定を適用するまでは、変更内容が有効になりません。

仮想スイッチのセットアップ

複数ネットワーク間のパケット スイッチングを提供できるように、レイヤ 2 展開で管理対象デバイスを設定することができます。レイヤ 2 展開では、ネットワークをいくつかの論理セグメントに分割して、スタンドアロン型ブロードキャスト ドメインとして機能するよう、管理対象デバイス上の仮想スイッチを設定できます。仮想スイッチは、ホストからの Media Access Control（MAC）アドレスを使用して、パケットの送信先を判別します。

仮想スイッチを設定すると、そのスイッチは最初、スイッチ内にある使用可能なすべてのポートを介してパケットをブロードキャストします。時間の経過とともに、スイッチはタグ付きリターン トラフィックを使用して、各ポートに接続しているネットワーク上にどのホストが存在するかを学習します。

仮想スイッチには、トラフィックを処理する複数のスイッチ型インターフェイスが含まれている必要があります。仮想スイッチごとに、トラフィックは、スイッチ型インターフェイスとして設定されたいくつかのポートに限定されます。たとえば、4 つのスイッチ型インターフェイスのある仮想スイッチを設定した場合、ブロードキャスト用に 1 つのポートを介して送入されるパケットは、そのスイッチ上の残る 3 つのポートからのみ送出可能です。

物理スイッチ型インターフェイスを設定するときには、仮想スイッチにそれを割り当てる必要があります。また、必要に応じて、物理ポート上に追加の論理スイッチ型インターフェイスを定義することもできます。シリーズ 3 管理対象デバイスでは、複数の物理インターフェイスを Link Aggregation Group（LAG）と呼ばれる単一の論理スイッチド インターフェイスにグループ化できます。このように 1 つに集約された論理リンクは、帯域幅と冗長性の向上および、2 つのエンドポイント間でのロードバランシングを実現します。

注意 何らかの理由でレイヤ 2 展開に障害が発生した場合、デバイスはトラフィックを通過させなくなります。

レイヤ 2 展開の設定についての詳細情報は、次の項を参照してください。

- スイッチ型インターフェイスの設定（6-2 ページ）
- 仮想スイッチの設定（6-6 ページ）
- LAG の設定（8-1 ページ）

スイッチ型インターフェイスの設定

ライセンス： Control

サポートされるデバイス： シリーズ 3

物理設定または論理設定を備えるよう、スイッチ型インターフェイスをセットアップできます。タグなし VLAN トラフィックを処理するよう物理スイッチ型インターフェイスを設定できます。また、VLAN タグが指定されたトラフィックを処理するよう論理スイッチ型インターフェイスを作成することもできます。

レイヤ 2 展開では、外部の物理インターフェイス上でトラフィックを受信した場合、それを待機しているスイッチ型インターフェイスがなければ、システムはそのトラフィックをドロップします。VLAN タグのないパケットを受信した場合、そのポート用の物理スイッチ型インターフェイスが未設定であれば、システムはパケットをドロップします。システムが VLAN タグ付きのパケットを受信した場合、論理スイッチ型インターフェイスが設定されていなければ、同じくパケットはドロップされます。

スイッチ型インターフェイスで VLAN タグ付きで受信されたトラフィックをシステムが処理するときには、ルールの評価や転送の決定を行う前に、入力における最も外側の VLAN タグを取り除きます。VLAN タグ付き論理スイッチ型インターフェイスを介してデバイスから出るパケットは、出力において関連する VLAN タグ付きでカプセル化されます。

親の物理インターフェイスをインラインまたはパッシブ（受動）に変更すると、関連付けられているすべての論理インターフェイスがシステムによって削除されることに注意してください。

詳細については、次の項を参照してください。

- 物理スイッチ型インターフェイスの設定（6-2 ページ）
- 論理スイッチ型インターフェイスの追加（6-4 ページ）
- 論理スイッチ型インターフェイスの削除（6-5 ページ）

物理スイッチ型インターフェイスの設定

ライセンス： Control

サポートされるデバイス： シリーズ 3

管理対象デバイス上の 1 つ以上の物理ポートをスイッチ型インターフェイスとして設定できます。トラフィックを処理できるようにするには、その前に、物理スイッチ型インターフェイスを仮想スイッチに割り当てる必要があります。

注意　センシング インターフェイスまたはインライン セットの MTU の任意の値（シリーズ 2）または最高値（シリーズ 3）を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック検査が一時的に中断されます。この検査中にデバイスがトラフィックをドロップするか、それ以上検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

物理スイッチ型インターフェイスを設定する方法:

アクセス: Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　スイッチ型インターフェイスを設定するデバイスの横にある編集アイコン( )をクリックします。

[Interfaces] タブが表示されます。

ステップ 3　スイッチ型インターフェイスとして設定するインターフェイスの横にある編集アイコン( ) をクリックします。

[Edit Interface] ポップアップ ウィンドウが表示されます。

ステップ 4　[Switched] をクリックして、スイッチ型インターフェイスのオプションを表示させます。

ステップ 5　オプションで、[Security Zone] ドロップダウン リストから既存のセキュリティ ゾーンを選択するか、または [New] を選択して新しいセキュリティ ゾーンを追加します。

ステップ 6　オプションで、[Virtual Switch] ドロップダウン リストから既存の仮想スイッチを選択するか、[New] を選択して新しい仮想スイッチを追加します。

新しい仮想スイッチを追加する場合は、スイッチ型インターフェイスのセットアップ後に、[Device Management] ページの [Virtual Switches] タブ ([Devices] > [Device Management] > [Virtual Switches]) でそのスイッチを設定する必要があることに注意してください。仮想スイッチの追加 (6-7 ページ) を参照してください。

ステップ 7　[Enabled] チェック ボックスを選択して、スイッチ型インターフェイスがトラフィックを処理できるようにします。

このチェック ボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

ステップ 8　[Mode] ドロップダウン リストからリンク モードを指定するオプションを選択するか、または [Autonegotiation] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようインターフェイスを設定します。モード設定は銅線インターフェイス専用であることに注意してください。

注　8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。

ステップ 9　[MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI (メディア依存型インターフェイス)、MDIX (メディア依存型インターフェイス クロスオーバー)、または Auto-MDIX のいずれかを指定するオプションを選択します。MDI/MDIX 設定は銅線インターフェイス専用であることに注意してください。

デフォルトでは、MDI/MDIX は自動 MDI に設定され、MDI と MDIX の間のスイッチングを自動的に処理してリンクを確立します。

ステップ 10　[MTU] フィールドに、最大伝送ユニット (MTU) を入力して、パケットの最大許容サイズを指定します。

設定可能な MTU の範囲は、FireSIGHT システムのデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、「管理対象デバイスの MTU の範囲 (4-69 ページ)」を参照してください。

ステップ 11　[Save] をクリックします。

物理スイッチ型インターフェイスが設定されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

論理スイッチ型インターフェイスの追加

ライセンス： Control

サポートされるデバイス： シリーズ 3

物理スイッチ型インターフェイスごとに、複数の論理スイッチ型インターフェイスを追加できます。物理インターフェイスで受信される VLAN タグ付きトラフィックを処理するには、各論理インターフェイスをその特定のタグに関連付ける必要があります。トラフィックを処理するには、論理スイッチ型インターフェイスを仮想スイッチに割り当てる必要があります。

注意　センシング インターフェイスまたはインライン セットの MTU の任意の値（シリーズ 2）または最高値（シリーズ 3）を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック検査が一時的に中断されます。この検査中にデバイスがトラフィックをドロップするか、それ以上検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

既存の論理スイッチ型インターフェイスを編集するには、インターフェイスの横にある編集アイコン（）をクリックします。

論理スイッチ型インターフェイスを追加する方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　スイッチ型インターフェイスを追加するデバイスの横にある編集アイコン（）をクリックします。

[Interfaces] タブが表示されます。

ステップ 3　[Add Interface] をクリックします。

[Add Interface] ポップアップ ウィンドウが表示されます。

ステップ 4　[Switched] をクリックして、スイッチ型インターフェイスのオプションを表示させます。

ステップ 5　[Interface] ドロップダウン リストから、VLAN タグ付きトラフィックを受信する物理インターフェイスを選択します。

ステップ 6　[VLAN Tag] フィールドで、このインターフェイス上のインバウンド/アウトバウンド トラフィックに割り当てるタグ値を入力します。この値には、1 ～ 4094 の任意の整数を指定できます。

ステップ 7　オプションで、[Security Zone] ドロップダウン リストから既存のセキュリティ ゾーンを選択するか、または [New] を選択して新しいセキュリティ ゾーンを追加します。

ステップ 8　オプションで、[Virtual Switch] ドロップダウン リストから既存の仮想スイッチを選択するか、[New] を選択して新しい仮想スイッチを追加します。

新しい仮想スイッチを追加する場合は、スイッチ型インターフェイスのセットアップ後に、[Device Management] ページ（[Devices] > [Device Management] > [Virtual Switches]）でそのスイッチを設定する必要があることに注意してください。仮想スイッチの追加（6-7 ページ）を参照してください。

ステップ 9　[Enabled] チェック ボックスを選択して、スイッチ型インターフェイスがトラフィックを処理できるようにします。

このチェック ボックスをオフにすると、インターフェイスは無効になり、管理上はダウンした状態になります。物理インターフェイスを無効にする場合、それに関連付けられているすべての論理インターフェイスも無効にします。

ステップ 10　[MTU] フィールドに、許容される最大のパケット サイズを指定する、最大伝送単位（MTU）を入力します。

設定可能な MTU の範囲は、FireSIGHT システムのデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、「管理対象デバイスの MTU の範囲（4-69 ページ）」を参照してください。

ステップ 11　[Save] をクリックします。

論理スイッチ型インターフェイスが追加されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

注　1 つの物理インターフェイスを無効化すると、その物理インターフェイスに関連付けられた論理インターフェイスも無効化されます。

論理スイッチ型インターフェイスの削除

ライセンス： Control

サポートされるデバイス： シリーズ 3

論理スイッチ型インターフェイスを削除すると、それが存在する物理インターフェイスから、および関連付けられている仮想スイッチとセキュリティ ゾーンからそれが削除されます。

スイッチ型インターフェイスを削除する方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　削除するスイッチ型インターフェイスが含まれる管理対象デバイスを選択し、そのデバイスの編集アイコン（ ）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　削除する論理スイッチ型インターフェイスの横にある削除アイコン（ ）をクリックします。

ステップ 4　プロンプトに応じて、インターフェイスを削除することを確認します。

インターフェイスが削除されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

仮想スイッチの設定

ライセンス： Control

サポートされるデバイス： シリーズ 3

レイヤ 2 展開でスイッチ型インターフェイスを使用できるようにするには、その前に仮想スイッチを設定して、スイッチ型インターフェイスを割り当てます。仮想スイッチは、ネットワーク経由のインバウンド/アウトバウンド トラフィックを処理する複数のスイッチ型インターフェイスからなるグループです。

仮想スイッチの設定についての詳細情報は、次の項を参照してください。

仮想スイッチの表示

ライセンス： Control

サポートされるデバイス： シリーズ 3

[Device Management] ページの [Virtual Switches] タブには、デバイス上で設定済みのすべての仮想スイッチのリストが表示されます。このページには、次の表に示すように、各スイッチに関する要約情報が含まれます。

表 6-1　仮想スイッチの表形式ビューのフィールド

フィールド	説明
名前	仮想スイッチの名前。
インターフェイス	仮想スイッチに割り当てられたすべてのスイッチ型インターフェイス。[Interfaces] タブで無効にしたインターフェイスは表示されません。
Hybrid Interface	仮想スイッチを仮想ルータに結合する、オプション設定のハイブリッド インターフェイス。
Unicast Packets	次の項目を含む、仮想スイッチのユニキャスト パケット統計： • 受信されたユニキャスト パケット • 転送されたユニキャスト パケット（ホストによるドロップを除く） • 誤ってドロップされたユニキャスト パケット
Broadcast Packets	次の項目を含む、仮想スイッチのブロードキャスト パケット統計： • 受信されたブロードキャスト パケット • 転送されたブロードキャスト パケット • 誤ってドロップされたブロードキャスト パケット

仮想スイッチの追加

ライセンス：Control

サポートされるデバイス：シリーズ 3

[Device Management] ページの [Virtual Switches] タブから仮想スイッチを追加できます。また、スイッチ型インターフェイスを設定するときにスイッチを追加することもできます。

仮想スイッチには、スイッチ型インターフェイスだけ割り当てることができます。管理対象デバイス上でスイッチ型インターフェイスを設定する前に仮想スイッチを作成する必要がある場合は、空の仮想スイッチを作成し、あとでそれにインターフェイスを追加できます。

ヒント　既存の仮想スイッチを編集するには、スイッチの横にある編集アイコン（ ）をクリックします。

仮想スイッチを追加する方法：

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　仮想スイッチを追加するデバイスの横にある編集アイコン（ ）をクリックします。

[Interfaces] タブが表示されます。

ステップ 3　[Virtual Switches] をクリックします。

[Virtual Switches] タブが表示されます。

ステップ 4　[Add Virtual Switch] をクリックします。

[Add Virtual Switch] ポップアップ ウィンドウが表示されます。

ステップ 5　[Name] フィールドに、仮想スイッチの名前を入力します。英数字とスペースを使用できます。

ステップ 6　[Available] で、仮想スイッチに追加される 1 つ以上のスイッチ型インターフェイスを選択します。

ヒント　[Interfaces] タブですでに無効にしたインターフェイスは使用できません。インターフェイスを追加した後で無効にすると、設定からそれが削除されます。

ステップ 7　[Add] をクリックします。

ステップ 8　オプションで、[Hybrid Interface] ドロップダウン リストから、仮想スイッチを仮想ルータに結合するハイブリッド インターフェイスを選択します。詳細については、ハイブリッド インターフェイスの設定（9-1 ページ）を参照してください。

ステップ 9　[Save] をクリックします。

仮想スイッチが追加されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

ヒント　スタティック MAC エントリやスパニング ツリー プロトコルなどの詳細なスイッチ設定を構成するには、仮想スイッチの詳細設定（6-8 ページ）を参照してください。

仮想スイッチの詳細設定

ライセンス： Control

サポートされるデバイス： シリーズ 3

仮想スイッチを追加したり編集したりするときには、スタティック MAC エントリの追加、スパニング ツリー プロトコル (STP) の有効化、ブリッジ プロトコル データ ユニット (BPDU) のドロップ、厳密な TCP 強制の有効化を行うことができます。

時間の経過とともに、仮想スイッチは、ネットワークからのリターン トラフィックにタグを付けることで MAC アドレスを学習します。オプションで、手動でスタティック MAC エントリを追加できます。これにより、MAC アドレスが特定のポート上にあることを指定します。そのポートからトラフィックを受信するかどうかにかかわらず、MAC アドレスはテーブル内で静的な状態を保ちます。仮想スイッチごとに 1 つ以上のスタティック MAC アドレスを指定できます。

STP は、ネットワーク ループを防止するために使われるネットワーク プロトコルです。BPDU は、ネットワーク ブリッジに関する情報を伝送し、ネットワークを介して交換されます。ネットワーク内に冗長リンクがある場合、プロトコルは BPDU を使用して最も高速なネットワーク リンクを識別し、選択します。ネットワーク リンクに障害が発生した場合、スパニング ツリーは既存の代替リンクにフェールオーバーします。

仮想スイッチが複数 VLAN 間でトラフィックをルーティングする場合、ルータ オン ア スティックと同様に、BPDU はさまざまな論理スイッチ型インターフェイスを介してデバイスを出入りしますが、物理スイッチ型インターフェイスは同一です。その結果、STP はデバイスを冗長ネットワーク ループとして識別します。特定のレイヤ 2 配置ではこれにより問題が生じる場合があります。それを防ぐには、トラフィックのモニタリング時にデバイスが BPDU をドロップするよう、ドメイン レベルで仮想スイッチを設定できます。

注　デバイス クラスタに展開される予定の仮想スイッチを設定する際には、STP を有効にするよう、Ciscoは強く推奨します。

最大の TCP セキュリティを実現するには、厳密な強制を有効にできます。この機能は、3 ウェイ ハンドシェイクが完了していない接続をブロックします。厳密な適用では次のパケットもブロックされます。

- 3 ウェイ ハンドシェイクが完了していない接続の非 SYN TCP パケット
- 応答側が SYN-ACK を送信する前に TCP 接続の発信側から送信された非 SYN/RST パケット
- SYN の後ではあるがセッションの確立前に TCP 接続の応答側から送信された非 SYN-ACK/RST パケット
- イニシエータまたはレスポンダからの、確立済みの TCP 接続上の SYN パケット

仮想スイッチを論理ハイブリッド インターフェイスに関連付けると、そのスイッチでは、論理ハイブリッド インターフェイスに関連付けられた仮想ルータと同じ厳密な TCP 強制設定が使用されることに注意してください。この場合、スイッチで厳密な TCP 強制を指定することはできません。

仮想スイッチの詳細設定を構成する方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　編集する仮想スイッチが含まれるデバイスの横にある編集アイコン()をクリックします。

[Interfaces] タブが表示されます。

ステップ 3　[Virtual Switches] をクリックします。

[Virtual Switches] タブが表示されます。

ステップ 4　編集する仮想スイッチの横にある編集アイコン()をクリックします。

[Edit Virtual Switch] ポップアップ ウィンドウが表示されます。

ステップ 5　[Advanced] をクリックします。

[Advanced] タブが表示されます。

ステップ 6　スタティック MAC エントリを追加するには、[Add] をクリックします。

[Add Static MAC Address] ポップアップ ウィンドウが表示されます。

ステップ 7　[MAC Address] フィールドで、2 桁の 16 進数 6 組をコロンで区切った標準形式を使用して、アドレスを入力します(たとえば 01:23:45:67:89:AB)。

注　ブロードキャスト アドレス(00:00:00:00:00:00 と FF:FF:FF:FF:FF:FF)をスタティック MAC アドレスとして追加することはできません。

ステップ 8　[Interface] ドロップダウン リストから、MAC アドレスを割り当てるインターフェイスを選択します。

ステップ 9　[Add] をクリックします。

MAC アドレスが Static MAC Entries テーブルに追加されます。

MAC アドレスを編集するには、編集アイコン()をクリックします。MAC アドレスを削除するには、削除アイコン()をクリックします。

ステップ 10　オプションで、スパニング ツリー プロトコルを有効にするには、[Enable Spanning Tree Protocol] を選択します。仮想スイッチが複数のネットワーク インターフェイス間でトラフィックを切り替える場合にのみ、[Enable Spanning Tree Protocol] を選択してください。

[Enable Spanning Tree Protocol] をクリアしない限り、[Drop BPDUs] を選択することはできません。

ステップ 11　オプションで、[Strict TCP Enforcement] を選択して、厳密な TCP 強制を有効にします。

仮想スイッチを論理ハイブリッド インターフェイスに関連付けると、このオプションは表示されず、論理ハイブリッド インターフェイスに関連付けられた仮想ルータと同じ設定がスイッチで使用されます。

ステップ 12　オプションで、[Drop BPDUs] を選択して、ドメイン レベルで BPDU をドロップします。仮想スイッチが 1 つの物理インターフェイス上の VLAN 間でトラフィックをルーティングする場合にのみ、[Drop BPDUs] を選択してください。

[Drop BPDUs] をクリアしない限り、[Enable Spanning Tree Protocol] を選択することはできません。

ステップ 13　[Save] をクリックします。

変更が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください(詳しくはデバイスへの変更の適用(4-27 ページ)を参照してください)。

仮想スイッチの削除

ライセンス： Control

サポートされるデバイス： シリーズ 3

仮想スイッチを削除すると、そのスイッチに割り当てられたスイッチ型インターフェイスを別のスイッチに含めることができるようになります。

仮想スイッチを削除する方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　削除する仮想スイッチが含まれる管理対象デバイスを選択し、そのデバイスの編集アイコン（ ）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Virtual Switches] をクリックします。

[Virtual Switches] タブが表示されます。

ステップ 4　削除する仮想スイッチの横にある削除アイコン（ ）をクリックします。

ステップ 5　プロンプトに応じて、仮想スイッチを削除することを確認します。

仮想スイッチが削除されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

仮想ルータのセットアップ

複数のインターフェイス間のトラフィックをルーティングするようにレイヤ 3 の管理対象デバイスを設定できます。各インターフェイスに IP アドレスを割り当て、トラフィックをルーティングする仮想ルータにインターフェイスを割り当てます。シリーズ 3 管理対象デバイスでは、複数の物理インターフェイスを Link Aggregation Group（LAG）と呼ばれる単一の論理ルーテッド インターフェイスにグループ化できます。このように 1 つに集約された論理リンクは、帯域幅と冗長性の向上および、2 つのエンドポイント間でのロードバランシングを実現します。

宛先アドレスに従ってパケット転送の決定を行うことにより、パケットをルーティングするようにシステムを設定できます。ルーテッド インターフェイスとして設定されるインターフェイスは、レイヤ 3 トラフィックを受信し、転送します。ルータは転送基準に基づいて発信インターフェイスから宛先を取得し、アクセス コントロール ルールが、適用するセキュリティ ポリシーを指定します。

レイヤ 3 配置では、スタティック ルートを定義できます。さらに、Routing Information Protocol（RIP）および Open Shortest Path First（OSPF）のダイナミック ルーティング プロトコルを設定できます。また、スタティック ルートと RIP、またはスタティック ルートと OSPF の組み合わせを設定することもできます。

注意 レイヤ 3 配置に何らかの理由で障害が発生した場合、デバイスはそれ以後トラフィックを転送しません。

レイヤ 3 配置の設定に関する詳細については、次の項を参照してください。

- ルーテッド インターフェイスの設定（7-1 ページ）
- 仮想ルータの設定（7-9 ページ）
- LAG の設定（8-1 ページ）

ルーテッド インターフェイスの設定

ライセンス： Control

サポートされるデバイス： シリーズ 3

ルーテッド インターフェイスのセットアップは物理設定または論理設定のいずれかで行うことができます。タグなし VLAN のトラフィックを処理するために物理ルーテッド インターフェイスを設定できます。また、指定 VLAN タグを持つトラフィックを処理するために論理ルーテッド インターフェイスを作成することもできます。

レイヤ 3 配置では、システムは待機するルーテッド インターフェイスがない外部物理インターフェイスで受信されるすべてのトラフィックをドロップします。システムが VLAN タグなしのパケットを受信し、そのポートの物理ルーテッド インターフェイスを設定しなかった場合、パケットはドロップされます。システムが VLAN タグ付きのパケットを受信した場合、論理ルーテッド インターフェイスが設定されていなければ、同じくパケットはドロップされます。

システムは、すべてのルール評価または転送決定の前に、入力の最も外側の VLAN タグを取り除くことによって、スイッチド インターフェイスで受信した VLAN タグ付きのトラフィックを処理します。VLAN タグ付きの論理ルーテッド インターフェイスを通ってデバイスから離れるパケットは出力で関連付けられた VLAN タグによりカプセル化されます。システムは除去プロセスが完了した後、VLAN タグ付きで受信するすべてのトラフィックをドロップします。

親の物理インターフェイスをインラインまたはパッシブに変更すると、システムは関連するすべての論理インターフェイスを削除することに注意してください。

詳細については、次の項を参照してください。

- 物理ルーテッド インターフェイスの設定（7-2 ページ）
- 論理ルーテッド インターフェイスの追加（7-5 ページ）
- 論理ルーテッド インターフェイスの削除（7-7 ページ）
- SFRP の設定（7-8 ページ）

物理ルーテッド インターフェイスの設定

ライセンス： Control

サポートされるデバイス： シリーズ 3

ルーテッド インターフェイスとして管理対象デバイスの 1 つ以上の物理ポートを設定できます。トラフィックをルーティングする前に、物理ルーテッド インターフェイスを仮想ルータに割り当てる必要があります。

ルーテッド インターフェイスに Address Resolution Protocol (ARP) スタティック エントリを追加できます。外部ホストがトラフィックを送信する、ローカル ネットワーク上の宛先 IP アドレスの MAC アドレスを知る必要がある場合、ARP 要求を送信します。スタティック ARP エントリを設定すると、仮想ルータは IP アドレスおよび関連付けられている MAC アドレスで応答します。

ルーテッド インターフェイスの [ICMP Enable Responses] オプションを無効にしても、すべてのシナリオで ICMP 応答を防ぐことはできません。宛先 IP がルーテッド インターフェイスの IP で、プロトコルが ICMP であるパケットをドロップするように、アクセス コントロール ポリシーにルールを追加できます。ネットワークベースのルールによるトラフィックの制御（15-1 ページ）を参照してください。

管理対象デバイスの [Inspect Local Router Traffic] オプションを有効にした場合、パケットはホストに到達する前にドロップされるため、すべての応答を防ぐことができます。ローカル ルータ トラフィックの検査の詳細については、高度なデバイス設定について（4-58 ページ）を参照してください。

注意　センシング インターフェイスまたはインライン セットの MTU の任意の値（シリーズ 2）または最高値（シリーズ 3）を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック検査が一時的に中断されます。この検査中にデバイスがトラフィックをドロップするか、それ以上検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

物理ルーテッド インターフェイスの設定:

アクセス: Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　ルーテッド インターフェイスを設定するデバイスの横にある編集アイコン( )をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　ルーテッド インターフェイスとして設定するインターフェイスの横にある編集アイコン( )をクリックします。

[Edit Interface] ポップアップ ウィンドウが表示されます。

ステップ 4　[Routed] をクリックして、ルーテッド インターフェイス オプションを表示します。

ステップ 5　オプションで、[Security Zone] ドロップダウン リストから既存のセキュリティ ゾーンを選択するか、または [New] を選択して新しいセキュリティ ゾーンを追加します。

ステップ 6　オプションで、[Virtual Router] ドロップダウン リストから既存の仮想ルータを選択するか、または [New] を選択して新しい仮想ルータを追加します。

新しい仮想ルータを追加する場合、ルーテッド インターフェイスをセットアップした後で、[Device Management] ページ([Devices] > [Device Management] > [Virtual Routers])の [Virtual Routers] タブで設定する必要があることに注意してください。仮想ルータの追加(7-10 ページ)を参照してください。

ステップ 7　[Enabled] チェック ボックスをオンにして、ルーテッド インターフェイスがトラフィックを処理することを許可します。

このチェック ボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

ステップ 8　[Mode] ドロップダウン リストからリンク モードを指定するオプションを選択するか、または [Autonegotiation] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようインターフェイスを設定します。モード設定は銅線インターフェイス専用であることに注意してください。

注　8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。

ステップ 9　[MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI(メディア依存型インターフェイス)、MDIX(メディア依存型インターフェイス クロスオーバー)、または Auto-MDIX のいずれかを指定するオプションを選択します。MDI/MDIX 設定は銅線インターフェイス専用であることに注意してください。

通常、[MDI/MDIX] は [Auto-MDIX] に設定します。これにより、MDI と MDIX の間の切り替えが自動的に処理され、リンクが確立されます。

ステップ 10　[MTU] フィールドに、許容される最大のパケット サイズを指定する、最大伝送単位(MTU)を入力します。MTU はレイヤ 2 MTU/MRU であり、レイヤ 3 MTU ではないことに注意してください。

設定可能な MTU の範囲は、FireSIGHT システムのデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、「管理対象デバイスの MTU の範囲(4-69 ページ)」を参照してください。

ステップ 11　[ICMP] の横にある [Enable Responses] チェック ボックスをオンにして、インターフェイスを ping や traceroute などの ICMP トラフィックに応答可能にします。

ステップ 12　[IPv6 NDP] の横にある [Enable Router Advertisement] チェック ボックスをオンにして、インターフェイスがルータ アドバタイズメントを伝送できるようにします。

ステップ 13　IP アドレスを追加するには、[Add] をクリックします。

[Add IP Address] ポップアップ ウィンドウが表示されます。

ステップ 14　[Address] フィールドに、ルーテッド インターフェイスの IP アドレスとサブネット マスクを CIDR 表記で入力します。次の点に注意してください。

- ネットワークおよびブロードキャスト アドレス、またはスタティック MAC アドレス 00:00:00:00:00:00 および FF:FF:FF:FF:FF:FF は追加できません。
- サブネット マスクに関係なく、仮想ルータのインターフェイスに同じ IP アドレスを追加できません。

ステップ 15　オプションで、IPv6 アドレスを使用している場合は、[IPv6] フィールドの横にある [Address Autoconfiguration] チェック ボックスをオンにして、インターフェイスの IP アドレスを自動的に設定します。

ステップ 16　[Type] には、[Normal] または [SFRP] を選択します。

SFRP オプションの詳細についてはSFRP の設定（7-8 ページ）を参照してください。

ステップ 17　[OK] をクリックします。

IP アドレスが追加されます。

IP アドレスを編集するには、編集アイコン（ ）をクリックします。IP アドレスを削除するには、削除アイコン（ ）をクリックします。

注　IP アドレスをクラスタ デバイスのルーテッド インターフェイスに追加する場合、クラスタ ピアのルーテッド インターフェイスに対応する IP アドレスを追加する必要があります。

ステップ 18　スタティック ARP エントリを追加するには、[Add] をクリックします。

[Add Static ARP Entry] ポップアップ ウィンドウが表示されます。

ステップ 19　[IP Address] フィールドに、スタティック ARP エントリの IP アドレスを入力します。

ステップ 20　[MAC Address] フィールドに、IP アドレスに関連付ける MAC アドレスを入力します。2 桁の 16 進数の 6 個のグループをコロンで区切る標準形式を使用して、アドレスを入力します（たとえば、01:23:45:67:89:AB）。

ステップ 21　[OK] をクリックします。

スタティック ARP エントリが追加されます。

ヒント　スタティック ARP エントリを編集するには、編集アイコン（ ）をクリックします。スタティック ARP エントリを削除するには、削除アイコン（ ）をクリックします。

ステップ 22　[Save] をクリックします。

物理ルーテッド インターフェイスが設定されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

論理ルーテッド インターフェイスの追加

ライセンス：Control

サポートされるデバイス：シリーズ 3

各物理ルーテッド インターフェイスで、複数の論理ルーテッド インターフェイスを追加できます。物理インターフェイスで受信される VLAN タグ付きトラフィックを処理するには、各論理インターフェイスをその特定のタグに関連付ける必要があります。トラフィックをルーティングする仮想ルータに論理ルーテッド インターフェイスを割り当てる必要があります。

ルーテッド インターフェイスの [ICMP Enable Responses] オプションを無効にしても、すべてのシナリオで ICMP 応答を防ぐことはできません。宛先 IP がルーテッド インターフェイスの IP で、プロトコルが ICMP であるパケットをドロップするように、アクセス コントロール ポリシーにルールを追加できます。ネットワークベースのルールによるトラフィックの制御（15-1 ページ）を参照してください。

管理対象デバイスの [Inspect Local Router Traffic] オプションを有効にした場合、パケットはホストに到達する前にドロップされるため、すべての応答を防ぐことができます。ローカル ルータ トラフィックの検査の詳細については、高度なデバイス設定について（4-58 ページ）を参照してください。

注意　センシング インターフェイスまたはインライン セットの MTU の任意の値（シリーズ 2）または最高値（シリーズ 3）を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック検査が一時的に中断されます。この検査中にデバイスがトラフィックをドロップするか、それ以上検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

既存のルーテッド インターフェイスを編集するには、インターフェイスの横にある編集アイコン（  ）をクリックします。

論理ルーテッド インターフェイスの追加：

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　ルーテッド インターフェイスを追加するデバイスの横にある編集アイコン（）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Add Interface] をクリックします。

[Add Interface] ポップアップ ウィンドウが表示されます。

ステップ 4　[Routed] をクリックして、ルーテッド インターフェイス オプションを表示します。

ステップ 5　[Interface] ドロップダウン リストから、論理インターフェイスを追加する物理インターフェイスを選択します。

ステップ 6　[VLAN Tag] フィールドで、このインターフェイス上のインバウンド/アウトバウンド トラフィックに割り当てるタグ値を入力します。この値には、1 ～ 4094 の任意の整数を指定できます。

ステップ 7　オプションで、[Security Zone] ドロップダウン リストから既存のセキュリティ ゾーンを選択するか、または [New] を選択して新しいセキュリティ ゾーンを追加します。

ステップ 8　オプションで、[Virtual Router] ドロップダウン リストから既存の仮想ルータを選択するか、または [New] を選択して新しい仮想ルータを追加します。

新しい仮想ルータを追加する場合、ルーテッド インターフェイスをセットアップした後で、[Device Management] ページ（[Devices] > [Device Management] > [Virtual Routers]）で設定する必要があることに注意してください。仮想ルータの追加（7-10 ページ）を参照してください。

ステップ 9　[Enabled] チェック ボックスをオンにして、ルーテッド インターフェイスがトラフィックを処理することを許可します。

このチェック ボックスをオフにすると、インターフェイスは無効になり、管理上はダウンした状態になります。物理インターフェイスを無効にする場合、それに関連付けられているすべての論理インターフェイスも無効にします。

ステップ 10　[MTU] フィールドに、許容される最大のパケット サイズを指定する、最大伝送単位（MTU）を入力します。MTU はレイヤ 2 MTU/MRU であり、レイヤ 3 MTU ではないことに注意してください。

設定可能な MTU の範囲は、FireSIGHT システムのデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、「管理対象デバイスの MTU の範囲（4-69 ページ）」を参照してください。

ステップ 11　[ICMP] の横にある [Enable Responses] チェック ボックスをオンにして、他のルータ、中間デバイス、またはホストに更新またはエラー情報を伝送します。

ステップ 12　[IPv6 NDP] の横にある [Enable Router Advertisement] チェック ボックスをオンにして、インターフェイスがルータ アドバタイズメントを伝送できるようにします。

ステップ 13　IP アドレスを追加するには、[Add] をクリックします。

[Add IP Address] ポップアップ ウィンドウが表示されます。

ステップ 14　[Address] フィールドに、IP アドレスを CIDR 表記で入力します。次の点に注意してください。

- ネットワークおよびブロードキャスト アドレス、またはスタティック MAC アドレス 00:00:00:00:00:00 および FF:FF:FF:FF:FF:FF は追加できません。
- サブネット マスクに関係なく、仮想ルータのインターフェイスに同じ IP アドレスを追加できません。

ステップ 15　オプションで、IPv6 アドレスを使用している場合は、[IPv6] フィールドの横にある [Address Autoconfiguration] チェック ボックスをオンにして、インターフェイスの IP アドレスを自動的に設定します。

ステップ 16　[Type] には、[Normal] または [SFRP] を選択します。

SFRP オプションの詳細についてはSFRP の設定（7-8 ページ）を参照してください。

ステップ 17　[OK] をクリックします。

IP アドレスが追加されます。

IP アドレスを編集するには、編集アイコン（）をクリックします。IP アドレスを削除するには、削除アイコン（）をクリックします。

注　IP アドレスをクラスタ デバイスのルーテッド インターフェイスに追加する場合、クラスタ ピアのルーテッド インターフェイスに対応する IP アドレスを追加する必要があります。

ステップ 18　スタティック ARP エントリを追加するには、[Add] をクリックします。

[Add Static ARP Entry] ポップアップ ウィンドウが表示されます。

ステップ 19　[IP Address] フィールドに、スタティック ARP エントリの IP アドレスを入力します。

ステップ 20　[MAC Address] フィールドに、IP アドレスに関連付ける MAC アドレスを入力します。2 桁の 16 進数の 6 個のグループをコロンで区切る標準形式を使用して、アドレスを入力します（たとえば、01:23:45:67:89:AB）。

ステップ 21　[OK] をクリックします。

スタティック ARP エントリが追加されます。

ヒント　スタティック ARP エントリを編集するには、編集アイコン（ ）をクリックします。スタティック ARP エントリを削除するには、削除アイコン（ ）をクリックします。

ステップ 22　[Save] をクリックします。

論理ルーテッド インターフェイスが追加されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

注　1 つの物理インターフェイスを無効化すると、その物理インターフェイスに関連付けられた論理インターフェイスも無効化されます。

論理ルーテッド インターフェイスの削除

ライセンス： Control

サポートされるデバイス： シリーズ 3

論理ルーテッド インターフェイスを削除すると、帰属する物理インターフェイスのほか、割り当てられた仮想ルータおよびセキュリティ ゾーンからも削除されます。

ルーテッド インターフェイスの削除：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　ルーテッド インターフェイスを削除するデバイスの横にある編集アイコン（ ）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　削除する論理ルーテッド インターフェイスの横にある削除アイコン（ ）をクリックします。

ステップ 4　入力を求められた場合、インターフェイスを削除することを確認します。

インターフェイスが削除されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

SFRP の設定

ライセンス： Control

サポートされるデバイス： シリーズ 3

Cisco冗長プロトコル（SFRP）を設定して、デバイスのクラスタまたは個別のデバイスのハイ アベイラビリティを得るためのネットワーク冗長性を実現できます。SFRP は IPv4 と IPv6 の両方のアドレスのゲートウェイ冗長性を提供します。ルーテッド インターフェイスおよびハイブリッド インターフェイスの SFRP を設定できます。

インターフェイスが個別のデバイスに設定される場合、同じブロードキャスト ドメインに存在する必要があります。インターフェイスのうち少なくとも 1 つをマスターに指定し、同じ数のバックアップを指定する必要があります。システムは IP アドレスごとに 1 つのマスターと 1 つのバックアップのみをサポートします。ネットワーク接続が失われた場合、システムは自動的にバックアップをマスターに昇格し、接続を維持します。

SFRP に設定するオプションは、SFRP インターフェイス グループのすべてのインターフェイスで同じにする必要があります。グループ内の複数の IP アドレスのマスターとバックアップの状態は同じである必要があります。そのため、IP アドレスを追加または編集する場合、そのアドレスに設定する状態はグループ内のすべてのアドレスに適用されます。セキュリティのために、グループ内のインターフェイス間で共有される [Group ID] と [Shared Secret] の値を入力する必要があります。

仮想ルータの SFRP の IP アドレスを有効にするには、少なくとも 1 つの非 SFRP IP アドレスを設定する必要があります。

クラスタ デバイスの場合、共有秘密を指定すると、SFRP の IP 設定とともにクラスタ ピアにコピーされます。共有秘密は、ピアのデータを認証します。

注　クラスタ化された シリーズ 3 デバイスのルーティングされたインターフェイスまたはハイブリッド インターフェイスで SFRP IP アドレスが既に 1 つ構成されている場合、複数の非 SFRP IP アドレスを有効にすることは推奨しません。クラスタ化された シリーズ 3 デバイスでスタンバイ モード中にフェールオーバーが発生すると、システムは NAT を実行しません。

クラスタ デバイスの詳細については、デバイスのクラスタリング（4-31 ページ）を参照してください。

SFRP を設定する方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　SFRP を設定するデバイスの横にある編集アイコン（）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　SFRP を設定するインターフェイスの横にある編集アイコン（）をクリックします。

[Edit Interface] ポップアップ ウィンドウが表示されます。

ステップ 4　SFRP を設定するインターフェイスのタイプを選択します。

- [Routed] をクリックして、ルーテッド インターフェイス オプションを表示します。
- [Hybrid] をクリックして、ハイブリッド インターフェイス オプションを表示します。

ステップ 5　IP アドレスを追加または編集するときに SFRP を設定できます。

- IP アドレスを追加するには、[Add] をクリックします。
- IP アドレスを編集するには、編集アイコン（  ）をクリックします。

[Add IP Address] ポップアップ ウィンドウまたは [Edit IP Address] ポップアップ ウィンドウが表示されます。

ステップ 6　[Type] に [SFRP] を選択して SFRP オプションを表示します。

ステップ 7　[Group ID] フィールドに、SFRP 用に設定されたマスターまたはバックアップ インターフェイス グループを指定する値を入力します。

ステップ 8　[Priority] に [Master] または [Backup] のどちらかを選択して、優先するインターフェイスを指定します。

- 個別のデバイスの場合、1 つのデバイスにマスターへのインターフェイスを 1 個設定し、2 番目のデバイスにバックアップへのインターフェイスを設定する必要があります。
- デバイスのクラスタの場合、マスターとして 1 個のインターフェイスを設定すると、もう 1 個のインターフェイスは自動的にバックアップになります。

ステップ 9　[Shared Secret] フィールドに、共有秘密を入力します。

[Shared Secret] フィールドには、デバイスのクラスタ内のグループに関するデータが自動的に入力されます。

ステップ 10　[Adv. Interval (seconds)] フィールドに、レイヤ 3 トラフィックのルート アドバタイズメントの間隔を入力します。

ステップ 11　[OK] をクリックします。

IP アドレスが追加または編集されます。

ステップ 12　[Save] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

仮想ルータの設定

ライセンス： Control

サポートされるデバイス： シリーズ 3

レイヤ 3 配置でルーテッド インターフェイスを使用する前に、仮想ルータを設定し、ルーテッド インターフェイスを割り当てる必要があります。仮想ルータはレイヤ 3 トラフィックをルーティングするルーテッド インターフェイスのグループです。

仮想ルータの設定の詳細については、次の項を参照してください。

- 仮想ルータの表示（7-10 ページ）
- 仮想ルータの追加（7-10 ページ）
- 仮想ルータ統計情報の表示（7-33 ページ）
- 仮想ルータの削除（7-34 ページ）

仮想ルータの表示

ライセンス： Control

サポートされるデバイス： シリーズ 3

[Device Management] ページ（[Devices] > [Device Management] > [Virtual Routers]）の [Virtual Routers] タブには、デバイスに設定されているすべての仮想ルータのリストが表示されます。このテーブルには次の表に示すように、各ルータに関するサマリー情報が含まれます。

表 7-1　仮想ルータのテーブル ビュー フィールド

フィールド	説明
名前	仮想ルータの名前。
インターフェイス	仮想ルータに割り当てられたすべてのルーテッド インターフェイスのリスト。[Interfaces] タブからインターフェイスを無効にすると削除されます。
プロトコル	仮想ルータによって現在使用されているプロトコル。次のいずれかです。 • スタティック • スタティック、RIP • スタティック、OSPF

仮想ルータの追加

ライセンス： Control

サポートされるデバイス： シリーズ 3

[Device Management] ページの [Virtual Routers] タブから仮想ルータを追加できます。ルーテッド インターフェイスを設定するときに、ルータを追加することもできます。

1 つの仮想ルータに割り当てることができるのは、ルーテッド インターフェイスとハイブリッド インターフェイスのみです。管理対象デバイスのインターフェイスを設定する前に仮想ルータを作成する場合は、空の仮想ルータを作成し、後でインターフェイスを追加できます。

最大の TCP セキュリティを実現するには、厳密な強制を有効にできます。この機能は、3 ウェイ ハンドシェイクが完了していない接続をブロックします。厳密な適用では次のパケットもブロックされます。

- 3 ウェイ ハンドシェイクが完了していない接続の非 SYN TCP パケット
- 応答側が SYN-ACK を送信する前に TCP 接続の発信側から送信された非 SYN/RST パケット
- SYN の後ではあるがセッションの確立前に TCP 接続の応答側から送信された非 SYN-ACK/RST パケット
- 発信側または応答側のどちらかから送信された、確立された TCP 接続の SYN パケット

レイヤ 3 インターフェイスの設定を非レイヤ 3 インターフェイスに変更したり、仮想ルータからレイヤ 3 インターフェイスを削除したりすると、ルータは無効な状態になる場合があることに注意してください。たとえば、DHCPv6 で使用されている場合、アップストリームとダウンストリームの不一致が生じることがあります。既存の仮想ルータに対する変更により、デバイスのトラフィックが中断される可能性があります。

ヒント　既存の仮想ルータを編集するには、ルータの横にある編集アイコン（ ）をクリックします。

一般的なオプションに加え、いくつかの異なる方法で仮想ルータを設定できます。これらの設定の詳細については、次の項を参照してください。

- DHCP リレーのセットアップ（7-12 ページ）
- スタティック ルートのセットアップ（7-14 ページ）
- ダイナミック ルーティングのセットアップ（7-16 ページ）
- RIP 設定のセットアップ（7-16 ページ）
- OSPF 設定のセットアップ（7-22 ページ）
- 仮想ルータ フィルタのセットアップ（7-30 ページ）
- 仮想ルータ認証プロファイルの追加（7-32 ページ）

仮想ルータの追加：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　仮想ルータを追加するデバイスの横にある編集アイコン（ ）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Virtual Routers] をクリックします。

[Virtual Routers] タブが表示されます。

ヒント　デバイスがクラスタ スタック配置にある場合、[Selected Device] ドロップダウン リストから、変更するスタックを選択します。

ステップ 4　[Add Virtual Router] をクリックします。

[Add Virtual Router] ポップアップ ウィンドウが表示されます。

ステップ 5　[Name] フィールドに仮想ルータの名前を入力します。英数字とスペースを使用できます。

ステップ 6　仮想ルータで IPv6 スタティック ルーティング、OSPFv3、および RIPng を有効にするには、[IPv6 Support] チェック ボックスをオンにします。これらの機能を無効にするには、チェック ボックスをオフにします。

ステップ 7　オプションで、厳密な TCP 適用を有効にしない場合は、[Strict TCP Enforcement] をオフにします。

このオプションは、デフォルトで有効です。

ステップ 8　[Interfaces] の下の [Available] リストには、仮想ルータに割り当てることが可能なデバイス上のすべての有効なレイヤ 3 インターフェイス（ルーテッドおよびハイブリッド）が含まれます。仮想ルータに割り当てる 1 つ以上のインターフェイスを選択して、[Add] をクリックします。

ヒント　仮想ルータからルーテッドまたはハイブリッド インターフェイスを削除するには、削除アイコン（ ）をクリックします。[Interfaces] タブで、設定したインターフェイスを無効にすることによっても削除できます。

ステップ 9　[Save] をクリックします。

仮想ルータが追加されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

DHCP リレーのセットアップ

ライセンス： Control

サポートされるデバイス： シリーズ 3

DHCP はインターネット ホストに設定パラメータを提供します。IP アドレスを未取得のDHCP クライアントは、ブロードキャスト ドメインの外にある DHCP サーバと直接通信できません。DHCP クライアントが DHCP サーバと通信できるようにするには、クライアントがサーバと同じブロードキャスト ドメイン内にない状況に対応できるように DHCP リレー インスタンスを設定します。

ユーザが設定した各仮想ルータの DHCP リレーを設定できます。デフォルトでは、この機能はディセーブルになっています。DHCPv4 リレーまたは DHCPv6 リレーのどちらかを有効にできます。

詳細については、次の項を参照してください。

- DHCPv4 リレーのセットアップ（7-12 ページ）
- DHCPv6 リレーのセットアップ（7-13 ページ）

DHCPv4 リレーのセットアップ

ライセンス： Control

サポートされるデバイス： シリーズ 3

次の手順は、仮想ルータで DHCPv4 リレーを設定する方法について説明します。

DHCPv4 リレーの設定：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　DHCP リレーを設定するデバイスの横にある編集アイコン（）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Virtual Routers] をクリックします。

[Virtual Routers] タブが表示されます。

ステップ 4　DHCP リレーを設定する仮想ルータの横にある編集アイコン（）をクリックします。

[Edit Virtual Router] ポップアップ ウィンドウが表示されます。

ステップ 5　DHCPv4 の DHCP リレーを設定するには、[DHCPv4] チェック ボックスをオンにします。

ステップ 6　[Servers] フィールドの下に、サーバの IP アドレスを入力します。

ステップ 7　[Add] をクリックします。

[Servers] フィールドにIP アドレスが追加されます。最大 4 台の DHCP サーバを追加できます。

ヒント　DHCP サーバを削除するには、サーバの IP アドレスの横にある削除アイコン（ ）をクリックします。

ステップ 8　[Max Hops] フィールドに 1 ～ 255 の最大ホップ カウントを入力します。

ステップ 9　[Save] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

DHCPv6 リレーのセットアップ

ライセンス： Control

サポートされるデバイス： シリーズ 3

次の手順は、仮想ルータで DHCPv6 リレーを設定する方法について説明します。

注　同じデバイスで実行中の複数の仮想ルータを介して DHCPv6 リレー チェーンを実行することはできません。

DHCPv6 リレーの設定：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　DHCP リレーを設定するデバイスの横にある編集アイコン（ ）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Virtual Routers] をクリックします。

[Virtual Routers] タブが表示されます。

ステップ 4　DHCP リレーを設定する仮想ルータの横にある編集アイコン（ ）をクリックします。

[Edit Virtual Router] ポップアップ ウィンドウが表示されます。

ステップ 5　DHCPv6 の DHCP リレーを設定するには、[DHCPv6] チェック ボックスをオンにします。

ステップ 6　[Interfaces] フィールドで、仮想ルータに割り当てられている 1 つ以上のインターフェイスの横にあるチェック ボックスをオンにします。

ヒント　DHCPv6 リレー用に設定されているインターフェイスは、[Interfaces] タブから無効にできません。最初に [DHCPv6 Relay interfaces] チェック ボックスをオフにして、設定を保存する必要があります。

ステップ 7　選択したインターフェイスの横にあるドロップダウン アイコンをクリックし、インターフェイスが DHCP 要求をリレーする方式として、[Upstream]、[Downstream]、または [Both] を選択します。

少なくとも 1 つのダウンストリーム インターフェイスと 1 つのアップストリーム インターフェイスを含める必要があることに注意してください。両方を選択することは、インターフェイスはダウンストリームおよびアップストリームの両方であることを意味します。

ステップ 8　[Max Hops] フィールドに 1 ～ 255 の最大ホップ カウントを入力します。

ステップ 9　[Save] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

スタティック ルートのセットアップ

ライセンス： Control

サポートされるデバイス： シリーズ 3

スタティック ルーティングにより、ルータを通過するトラフィックの IP アドレスに関するルールを作成することができます。これはネットワークの現在のトポロジに関して他のルータとの通信がないため、仮想ルータのパス選択を設定する最も簡単な方法です。

詳細については、次の項を参照してください。

- スタティック ルート テーブル ビューについて（7-14 ページ）
- スタティック ルートの追加（7-15 ページ）

スタティック ルート テーブル ビューについて

ライセンス： Control

サポートされるデバイス： シリーズ 3

仮想ルータ エディタの [Static Routes] タブには、仮想ルータに設定されているすべてのスタティック ルートのリストが表示されます。このテーブルには次の表に示すように、各ルートに関するサマリー情報が含まれます。

表 7-2　スタティック ルート テーブル ビュー フィールド

フィールド	説明
イネーブル	このルートが現在有効であるか、無効であるかを示します。
名前	スタティック ルートの名前。
Destination	トラフィックがルーティングされる宛先ネットワーク。
タイプ	このルートに対して実行するアクションを指定します。次のいずれかです。 • IP：パケットが、隣接ルータのアドレスに転送されることを指定します。 • Interface：そのインターフェイスを介してトラフィックが直接接続されたネットワーク上のホストにルーティングされるインターフェイスにパケットが転送されることを指定します。 • Discard：スタティック ルートがパケットをドロップすることを指定します。

表 7-2　スタティック ルート テーブル ビュー フィールド（続き）

フィールド	説明
Gateway	スタティック ルートのタイプとして IP を選択した場合はターゲット IP アドレス、またはスタティック ルート タイプとしてインターフェイスを選択した場合はインターフェイス。
優先順位	ルート選択を決定します。同じ宛先に対する複数のルートが存在する場合、より高い優先順位のルートが選択されます。

スタティック ルートの追加

ライセンス： Control

サポートされるデバイス： シリーズ 3

次の手順は、スタティック ルートを追加する方法について説明します。

スタティック ルートを編集するには、編集アイコン（）をクリックします。スタティック ルートを削除するには、削除アイコン（）をクリックします。

スタティック ルートの追加：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　スタティック ルートを追加するデバイスの横にある編集アイコン（）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Virtual Routers] をクリックします。

[Virtual Routers] タブが表示されます。

ステップ 4　スタティック ルートを追加する仮想ルータの横にある編集アイコン（）をクリックします。

[Edit Virtual Router] ポップアップ ウィンドウが表示されます。

ステップ 5　[Static] をクリックして、スタティック ルートのオプションを表示します。

ステップ 6　[Add Static Route] をクリックします。

[Add Static Route] ポップアップ ウィンドウが表示されます。

ステップ 7　[Route Name] フィールドに、スタティック ルートの名前を入力します。英数字とスペースを使用できます。

ステップ 8　[Enabled] チェック ボックスをオンにして、ルートが現在有効であることを指定します。

ステップ 9　[Preference] フィールドに、ルート選択を決定するための 1 ～ 65535 の数値を入力します。

同じ宛先に対する複数のルートが存在する場合、より高い優先順位のルートが選択されます。

ステップ 10　[Type] ドロップダウン リストから、設定するスタティック ルートのタイプを選択します。

ステップ 11　[Destination] フィールドに、トラフィックがルーティングされる宛先ネットワークの IP アドレスを入力します。

ステップ 12　[Gateway] フィールドでは、次の 2 つの選択肢があります。

- スタティック ルート タイプとして [IP] を選択した場合は、IP アドレスを入力します。

- スタティック ルート タイプとして [Interface] を選択した場合は、ドロップダウン リストから有効なインターフェイスを選択します。

ヒント　[Interfaces] タブから無効にしたインターフェイスは使用できません。追加したインターフェイスを無効にすると、設定から削除されます。

ステップ 13　[OK] をクリックします。

スタティック ルートが追加されます。

ステップ 14　[Save] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

ダイナミック ルーティングのセットアップ

ライセンス： Control

サポートされるデバイス： シリーズ 3

ダイナミックつまり適応型のルーティングは、ルーティング プロトコルを使用して、ルートが取るパスをネットワーク条件の変化に応じて変更します。この適応は、できるだけ多くのルートの有効性を維持し、変更に応じて宛先に到達可能とすることを目的としたものです。このため、他のパスを選択できる限り、ネットワークはノードまたはノード間の接続の損失といった障害を「迂回」することができます。ダイナミック ルーティングなしでルータを設定することも、Routing Information Protocol（RIP）または Open Shortest Path First（OSPF）のルーティング プロトコルを設定することもできます。

詳細については、次の項を参照してください。

- RIP 設定のセットアップ（7-16 ページ）
- OSPF 設定のセットアップ（7-22 ページ）

RIP 設定のセットアップ

ライセンス： Control

サポートされるデバイス： シリーズ 3

Routing Information Protocol（RIP）はホップ カウントを使用してルートを決定する、小規模な IP ネットワーク向けのダイナミック ルーティング プロトコルです。最適なルートは最小数のホップを使用します。RIP で許可されるホップの最大数は 15 です。このホップ制限により、RIP がサポートできるネットワークのサイズも制限されます。

RIP 設定の詳細については、次の項を参照してください。

- RIP 設定用インターフェイスの追加（7-17 ページ）
- RIP 設定の認証設定（7-18 ページ）
- RIP の高度な設定（7-18 ページ）
- RIP 設定のインポート フィルタの追加（7-20 ページ）
- RIP 設定へのエクスポート フィルタの追加（7-21 ページ）

RIP 設定用インターフェイスの追加

ライセンス：Control

サポートされるデバイス：シリーズ 3

RIP を設定する際、RIP を設定する仮想ルータにすでに含まれているインターフェイスを選択する必要があります。無効になっているインターフェイスを使用することはできません。

RIP インターフェイスを編集するには、編集アイコン（  ）をクリックします。RIP インターフェイスを削除するには、削除アイコン（  ）をクリックします。

RIP 設定でインターフェイスの追加：

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　RIP インターフェイスを追加するデバイスの横にある編集アイコン（  ）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Virtual Routers] をクリックします。

[Virtual Routers] タブが表示されます。

ステップ 4　RIP インターフェイスを追加する仮想ルータの横にある編集アイコン（  ）をクリックします。

[Edit Virtual Router] ポップアップ ウィンドウが表示されます。

ステップ 5　[Dynamic Routing] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6　[RIP] をクリックして、RIP オプションを表示します。

ステップ 7　[Interfaces] の下で、追加アイコン（  ）をクリックします。

[Add an Interface] ポップアップ ウィンドウが表示されます。

ステップ 8　[Name] ドロップダウン リストから、RIP を設定するインターフェイスを選択します。

ヒント　[Interfaces] タブから無効にしたインターフェイスは使用できません。追加したインターフェイスを無効にすると、設定から削除されます。

ステップ 9　[Metric] フィールドに、インターフェイスのメトリックを入力します。異なる RIP インスタンスからのルートを使用可能で、すべてが同じ設定である場合、メトリックが最小のルートが優先ルートになります。

ステップ 10　[Mode] ドロップダウン リストから、次のいずれかのオプションを選択します。

- [Multicast]：RIP が指定されたアドレスですべての隣接ルータにルーティング テーブル全体をマルチキャストするデフォルトのモード。
- [Broadcast]：マルチキャスト モードが可能な場合でも、RIP にブロードキャスト（RIPv1 など）の使用を強制します。
- [Quiet]：RIP は、このインターフェイスに定期メッセージを送信しません。
- [No Listen]：RIP は、このインターフェイスに送信しますが、リッスンしません。

ステップ 11　[Save] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

RIP 設定の認証設定

ライセンス： Control

サポートされるデバイス： シリーズ 3

RIP 認証では、仮想ルータに設定した認証プロファイルの 1 つが使用されます。認証プロファイルの設定に関する詳細については、仮想ルータ認証プロファイルの追加（7-32 ページ）を参照してください。

RIP 設定の認証設定：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　RIP 認証プロファイルを追加するデバイスの横にある編集アイコン（  ）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Virtual Routers] をクリックします。

[Virtual Routers] タブが表示されます。

ステップ 4　RIP 認証プロファイルを追加する仮想ルータの横にある編集アイコン（  ）をクリックします。

[Edit Virtual Router] ポップアップ ウィンドウが表示されます。

ステップ 5　[Dynamic Routing] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6　[RIP] をクリックして、RIP オプションを表示します。

ステップ 7　[Authentication] の下の [Profile] ドロップダウン リストを使用して、既存の仮想ルータ認証プロファイルを選択するか、または [None] を選択します。

ステップ 8　[Save] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

RIP の高度な設定

ライセンス： Control

サポートされるデバイス： シリーズ 3

プロトコルの動作に影響するさまざまなタイムアウト値およびその他の機能に関していくつかの高度な RIP 設定を構成できます。

注意　不正な値に対する高度な RIP 設定を変更すると、ルータが他の RIP ルータと正常に通信することを妨げる場合があります。

RIP の高度な設定：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　RIP の詳細設定を編集するデバイスの横にある編集アイコン（  ）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Virtual Routers] をクリックします。

[Virtual Routers] タブが表示されます。

ステップ 4　RIP の詳細設定を編集する仮想ルータの横にある編集アイコン（  ）をクリックします。

[Edit Virtual Router] ポップアップ ウィンドウが表示されます。

ステップ 5　[Dynamic Routing] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6　[RIP] をクリックして、RIP オプションを表示します。

ステップ 7　[Preference] フィールドに、ルーティング プロトコルの優先度の数値（高いほど優先される）を入力します。システムはスタティック ルートよりも RIP を使用して学習したルートを優先します。

ステップ 8　[Period] フィールドに、定期的な更新間隔（秒単位）を入力します。低い数値は高速なコンバージェンスを示しますが、ネットワーク負荷が大きくなります。

ステップ 9　[Timeout Time] フィールドに、到達不能とみなされるまでのルートの存続時間（秒単位）を指定する数値を入力します。

ステップ 10　[Garbage Time] フィールドに、破棄されるまでのルートの存続時間（秒単位）を指定する数値を入力します。

ステップ 11　[Infinity] フィールドに、コンバージェンスの計算で無限間隔の値を指定する数値を入力します。値が大きいほど、プロトコル コンバージェンスが遅くなります。

ステップ 12　[Honor] ドロップダウン リストから、ルーティング テーブルをダンプする要求がいつ実行されるかを指定する、次のいずれかのオプションを選択します。

- [Always]：常に要求を実行する
- [Neighbor]：直接接続されたネットワーク上のホストから送信された要求のみを実行する
- [Never]：要求を実行しない

ステップ 13　[Save] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

RIP 設定のインポート フィルタの追加

ライセンス：Control

サポートされるデバイス：シリーズ 3

ルート テーブルに対して RIP からの受け入れまたは拒否を行うルートを指定するために、インポート フィルタを追加できます。インポート フィルタはテーブルに表示される順に適用されます。

インポート フィルタを追加するときは、仮想ルータに設定したフィルタの 1 つを使用します。フィルタの設定の詳細については、仮想ルータ フィルタのセットアップ（7-30 ページ）を参照してください。

ヒント　RIP インポート フィルタを編集するには、編集アイコン（）をクリックします。RIP インポート フィルタを削除するには、削除アイコン（）をクリックします。

RIP 設定へのインポート フィルタの追加：

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　RIP 仮想ルータ フィルタを追加するデバイスの横にある編集アイコン（）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Virtual Routers] をクリックします。

[Virtual Routers] タブが表示されます。

ステップ 4　RIP 仮想ルータ フィルタを追加する仮想ルータの横にある編集アイコン（）をクリックします。

[Edit Virtual Router] ポップアップ ウィンドウが表示されます。

ステップ 5　[Dynamic Routing] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6　[RIP] をクリックして、RIP オプションを表示します。

ステップ 7　[Import Filters] の下で、追加アイコン（）をクリックします。

[Add an Import Filter] ポップアップ ウィンドウが表示されます。

ステップ 8　[Name] ドロップダウン リストから、インポート フィルタとして追加するフィルタを選択します。

ステップ 9　[Action] の横にある [Accept] または [Reject] を選択します。

ステップ 10　[OK] をクリックします。

インポート フィルタが追加されます。

ヒント　インポート フィルタの順序を変更するには、必要に応じて、上へ移動するアイコン（）または下へ移動するアイコン（）をクリックします。リスト内でフィルタを上下にドラッグすることもできます。

ステップ 11　[Save] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

RIP 設定へのエクスポート フィルタの追加

ライセンス：Control

サポートされるデバイス：シリーズ 3

ルート テーブルから RIP に対しての受け入れまたは拒否を行うルートを定義するために、エクスポート フィルタを追加できます。エクスポート フィルタはテーブルに表示される順に適用されます。

エクスポート フィルタを追加するときは、仮想ルータに設定したフィルタの 1 つを使用します。フィルタの設定の詳細については、仮想ルータ フィルタのセットアップ（7-30 ページ）を参照してください。

RIP 設定へのエクスポート フィルタの追加：

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　RIP 仮想ルータ フィルタを追加するデバイスの横にある編集アイコン（ ）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Virtual Routers] をクリックします。

[Virtual Routers] タブが表示されます。

ステップ 4　RIP 仮想ルータ フィルタを追加する仮想ルータの横にある編集アイコン（ ）をクリックします。

[Edit Virtual Router] ポップアップ ウィンドウが表示されます。

ステップ 5　[Dynamic Routing] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6　[RIP] をクリックして、RIP オプションを表示します。

ステップ 7　[Export Filters] の下で、追加アイコン（ ）をクリックします。

[Add an Export Filter] ポップアップ ウィンドウが表示されます。

ステップ 8　[Name] ドロップダウン リストから、エクスポート フィルタとして追加するフィルタを選択します。

ステップ 9　[Action] の横にある [Accept] または [Reject] を選択します。

ステップ 10　[OK] をクリックします。

エクスポート フィルタが追加されます。

ヒント　エクスポート フィルタの順序を変更するには、必要に応じて、上へ移動するアイコン（ ）または下へ移動するアイコン（ ）をクリックします。リスト内でフィルタを上下にドラッグすることもできます。

ステップ 11　[Save] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

OSPF 設定のセットアップ

ライセンス： Control

サポートされるデバイス： シリーズ 3

Open Shortest Path First（OSPF）は、他のルータから情報を取得し、リンク ステート アドバタイズメントを使用してルートを他のルータにアドバタイズすることで、ルートを動的に定義する適応型ルーティング プロトコルです。ルータは、それ自体と宛先との間のリンクに関する情報を維持し、ルーティングを決定します。OSPF は、各ルーテッド インターフェイスにコストを割り当て、コストが最低のルータを最適であるとみなします。

詳細については、次の項を参照してください。

- OSPF ルーティング エリアのセットアップ（7-22 ページ）
- OSPF 設定のインポート フィルタの追加（7-28 ページ）
- OSPF 設定へのエクスポート フィルタの追加（7-29 ページ）

OSPF ルーティング エリアのセットアップ

ライセンス： Control

サポートされるデバイス： シリーズ 3

OSPF ネットワークは、管理を簡略化し、トラフィックおよびリソースの使用を最適化するために、ルーティング エリアに構造化つまり分割することができます。エリアは、単純な 10 進数またはよく使用されるオクテットベースのドット付き 10 進数表記のいずれかで表現される 32 ビットの数字により識別されます。

慣習により、エリア ゼロつまり 0.0.0.0 は OSPF ネットワークのコアまたはバックボーン エリアを表します。他のエリアも指定できます。多くの場合、管理者はエリアのメイン ルータの IP アドレスをエリア ID として選択します。追加の各エリアはバックボーンの OSPF エリアに直接または仮想接続できる必要があります。そうした接続は、エリア境界ルータ（ABR）と呼ばれる相互接続ルータによって保持されます。ABR は、管轄する各エリアの個々のリンクステート データベースを管理し、ネットワーク内のすべてのエリアの集約ルートを保守します。

OSPF エリアのセットアップの詳細については、次の項を参照してください。

- OSPF エリアの追加（7-22 ページ）
- OSPF エリア インターフェイスの追加（7-24 ページ）
- OSPF エリア vlink の追加（7-27 ページ）

OSPF エリアの追加

ライセンス： Control

サポートされるデバイス： シリーズ 3

次の手順は、OSPF エリアを追加し、一般設定を構成する方法について説明します。

OSPF エリアの追加：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　OSPF の一般オプションを編集するデバイスの横にある編集アイコン( )をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Virtual Routers] をクリックします。

[Virtual Routers] タブが表示されます。

ステップ 4　OSPF の一般オプションを編集する仮想ルータの横にある編集アイコン( )をクリックします。

[Edit Virtual Router] ポップアップ ウィンドウが表示されます。

ステップ 5　[Dynamic Routing] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6　[OSPF] をクリックして、OSPF オプションを表示します。

ステップ 7　[Areas] の下で、追加アイコン( )をクリックします。

[Add OSPF Area] ポップアップ ウィンドウが表示されます。

ステップ 8　[Area Id] フィールドに、エリアを表す数値を入力します。この値には整数または IPv4 アドレスを指定できます。

ステップ 9　オプションで、[Stubnet] チェック ボックスをオンにし、エリアが自律システムの外部のルータ アドバタイズメントを受信せず、エリア内のルーティングは完全にデフォルト ルートに基づくことを指定します。チェック ボックスをオフにすると、このエリアはバックボーン エリアになります。それ以外の場合は、非スタブ エリアになります。

[Default cost] フィールドと [Stubnet] フィールドが表示されます。

ステップ 10　[Default cost] フィールドに、エリアのデフォルト ルートに関連付けられたコストを入力します。

ステップ 11　[Stubnets] の下で、追加アイコン( )をクリックします。

ステップ 12　[IP Address] フィールドに、IP アドレスを CIDR 表記で入力します。

ステップ 13　[Hidden] チェック ボックスをオンにして、スタブネットが非表示であることを示します。非表示のスタブネットは別のエリアに伝播されません。

ステップ 14　[Summary] チェック ボックスをオンにして、このスタブネットのサブネットワークであるデフォルトのスタブネットが非表示となるように指定します。

ステップ 15　[Stub cost] フィールドに、このスタブ ネットワークへのルーティングに関連付けられたコストを定義する値を入力します。

ステップ 16　[OK] をクリックします。

スタブネットが追加されます。

ヒント　スタブネットを編集するには、編集アイコン( )をクリックします。スタブネットを削除するには、削除アイコン( )をクリックします。

ステップ 17　オプションで、[Networks] の下の追加アイコン( )をクリックします。

ステップ 18　[IP Address] フィールドに、ネットワークの IP アドレスを CIDR 表記で入力します。

ステップ 19　[Hidden] チェック ボックスをオンにして、ネットワークが非表示であることを示します。非表示のネットワークは別のエリアに伝播されません。

ステップ 20　[OK] をクリックします。

ネットワークが追加されます。

ヒント　ネットワークを編集するには、編集アイコン( )をクリックします。ネットワークを削除するには、削除アイコンをクリックします( )。

ステップ 21　[Save] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

OSPF エリア インターフェイスの追加

ライセンス： Control

サポートされるデバイス： シリーズ 3

OSPF 用に仮想ルータに割り当てられたインターフェイスのサブセットを設定できます。次のリストに、各インターフェイスで指定できるオプションを示します。

インターフェイス

OSPF を設定するインターフェイスを選択します。[Interfaces] タブから無効にしたインターフェイスは使用できません。

タイプ

次のオプションから、OSPF インターフェイスのタイプを選択します。

- Broadcast：ブロードキャスト ネットワークでは、フラッディングおよび hello メッセージはマルチキャストを使用し、すべてのネイバーに対して 1 つのパケットで送信されます。このオプションは、ルータがリンク ステート データベースと同期し、ネットワーク リンク ステート アドバタイズメントを発信するように指定します。このネットワーク タイプは、物理的なノンブロードキャスト マルチプル アクセス（NBMP）ネットワークと適切な IP プレフィクスなしのアンナンバード ネットワークには使用できません。
- Point-to-Point (PtP)：ポイントツーポイント ネットワークでは、2 台のルータのみを接続します。選定は実行されず、ネットワーク リンク ステート アドバタイズメントは発生しないので、より単純かつ高速に確立されます。このネットワーク タイプは物理的な PtP インターフェイスだけでなく、PtP リンクとして使用されるブロードキャスト ネットワークにも役立ちます。このネットワーク タイプは物理的な NBMP ネットワークでは使用できません。
- Non-Broadcast：NBMP ネットワークで、パケットはマルチキャスト機能がないために各ネイバーに別々に送信されます。ブロードキャスト ネットワークと同様に、このオプションはリンク ステート アドバタイズメント伝播で中心的な役割を果たすルータを指定します。このネットワーク タイプはアンナンバード ネットワークでは使用できません。
- Autodetect：システムは指定されたインターフェイスに基づいて正しいタイプを判別します。

コスト

インターフェイスの出力コストを指定します。

Stub

インターフェイスが OSPF トラフィックをリッスンし、独自のトラフィックを送信する必要があるかどうかを指定します。

プライオリティ

指定ルータの選定に使用される優先度を示す数値を入力します。多重アクセス ネットワークごとに、システムはルータおよびバックアップ ルータを指定します。これらのルータには、フラッディング プロセスでの特別な機能があります。優先度を高くすると、この選定での優先順位が上がります。優先度 0 でルータを設定することはできません。

Nonbroadcast

hello パケットが任意の未定義のネイバーに送信されるかどうかを指定します。このスイッチは、任意の NBMA ネットワークでは無視されます。

認証

仮想ルータに設定した認証プロファイルの 1 つからこのインターフェイスが使用する OSPF 認証プロファイルを選択するか、または [None] を選択します。認証プロファイルの設定に関する詳細については、仮想ルータ認証プロファイルの追加（7-32 ページ）を参照してください。

Hello Interval

hello メッセージの送信間隔（秒単位）を入力します。

Poll

NBMA ネットワーク上の一部のネイバーに対する hello メッセージの送信間隔（秒単位）を入力します。

Retrans Interval

確認応答されていないアップデートの再送信間隔（秒単位）を入力します。

Retrans Delay

インターフェイス経由でのリンクステート アップデート パケットの送信に要する推定秒数を入力します。

Wait Time

ルータが選定の開始と隣接関係の構築の間で待機する秒数を入力します。

Dead Interval

ルータがネイバーからのメッセージを受信しない場合に、ネイバーの停止を宣言するまで待機する秒数を入力します。この値が定義されている場合、dead カウントから計算された値はオーバーライドされます。

Dead Count

hello 間隔と乗算されるときに、ルータがネイバーからのメッセージを受信しない場合に、ネイバーの停止を宣言するまで待機する秒数を指定する、数値を入力します。

OSPF エリア インターフェイスを編集するには、編集アイコン（ ）をクリックします。
OSPF エリア インターフェイスを削除するには、削除アイコン（ ）をクリックします。
[Interfaces] タブで設定されたインターフェイスを無効にすると削除されます。

注　OSPF エリアで使用するインターフェイスは 1 つのみ選択できます。

OSPF エリア インターフェイスの追加:

アクセス: Admin/Network Admin

ステップ 1 [Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2 OSPF インターフェイスを追加するデバイスの横にある編集アイコン( )をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3 [Virtual Routers] をクリックします。

[Virtual Routers] タブが表示されます。

ステップ 4 OSPF インターフェイスを追加する仮想ルータの横にある編集アイコン( )をクリックします。

[Edit Virtual Router] ポップアップ ウィンドウが表示されます。

ステップ 5 [Dynamic Routing] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [OSPF] をクリックして、OSPF オプションを表示します。

ステップ 7 [Areas] の下で、追加アイコン( )をクリックします。

[Add OSPF Area] ポップアップ ウィンドウが表示されます。

ステップ 8 [Interfaces] をクリックします。

[Interfaces] タブが表示されます。

ステップ 9 追加アイコン( )をクリックします。

[Add OSPF Area Interface] ポップアップ ウィンドウが表示されます。

ステップ 10 OSPF エリア インターフェイスの追加 (7-24 ページ) で説明されているアクションのいずれかを実行します。

ステップ 11 オプションで、[Neighbors] の下の追加アイコン( )をクリックします。

ステップ 12 [IP address] フィールドに、このインターフェイスから非ブロードキャスト ネットワークの hello メッセージを受信するネイバーの IP アドレスを入力します。

ステップ 13 [Eligible] チェック ボックスをオンにして、ネイバーがメッセージを受け取る資格があることを示します。

ステップ 14 [OK] をクリックします。

ネイバーが追加されます。

ヒント ネイバーを編集するには、編集アイコン( )をクリックします。ネイバーを削除するには、削除アイコン( )をクリックします。

ステップ 15 [OK] をクリックします。

OSPF エリア インターフェイスが追加されます。

ステップ 16 [Save] をクリックします。

OSPF エリアが保存されます。

ステップ 17 [Save] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用 (4-27 ページ) を参照してください。

OSPF エリア vlink の追加

ライセンス：Control

サポートされるデバイス：シリーズ 3

OSPF 自律システムのすべてのエリアは、物理的にバックボーン エリアと接続されている必要があります。この物理接続が不可能である場合は、vlink を使用して、非バックボーン エリアを経由してバックボーンに接続できます。また vlink を使用して、非バックボーン エリアを経由し、分割されたバックボーンの 2 つの部分を接続することもできます。

vlink を追加するには、最低 2 つの OSPF エリアを追加しておく必要があります。

OSPF エリア vlink の追加：

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　OSPF vlink を追加するデバイスの横にある編集アイコン（ ）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Virtual Routers] をクリックします。

[Virtual Routers] タブが表示されます。

ステップ 4　OSPF インターフェイスを追加する仮想ルータの横にある編集アイコン（ ）をクリックします。

[Edit Virtual Router] ポップアップ ウィンドウが表示されます。

ステップ 5　[Dynamic Routing] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6　[OSPF] をクリックして、OSPF オプションを表示します。

ステップ 7　[Areas] の下で、追加アイコン（ ）をクリックします。

[Add OSPF Area] ポップアップ ウィンドウが表示されます。

ステップ 8　[Vlinks] をクリックします。

[Vlinks] タブが表示されます。

ステップ 9　追加アイコン（ ）をクリックします。

[Add OSPF Area Vlink] ポップアップ ウィンドウが表示されます。

ステップ 10　[Router ID] フィールドに、ルータの IP アドレスを入力します。

ステップ 11　[Authentication] ドロップダウン リストから、vlink が使用する認証プロファイルを選択します。

ステップ 12　[Hello Interval] フィールドに、hello メッセージの送信間隔（秒単位）を入力します。

ステップ 13　[Retrans Interval] フィールドに、確認応答されていないアップデートの再送信間隔（秒単位）を入力します。

ステップ 14　[Wait Time] フィールドに、ルータが選定の開始と隣接関係の構築の間で待機する秒数を入力します。

ステップ 15　[Dead Interval] フィールドに、ルータがネイバーからのメッセージを受信しない場合に、ネイバーの停止を宣言するまで待機する秒数を入力します。この値が定義されている場合、dead カウントから計算された値はオーバーライドされます。

ステップ 16　[Dead Count] フィールドに、hello 間隔と乗算されるときに、ルータがネイバーからのメッセージを受信しない場合に、ネイバーの停止を宣言するまで待機する秒数を指定する、数値を入力します。

ステップ 17　[OK] をクリックします。

OSPF エリア vlink が追加されます。

ステップ 18　[Save] をクリックします。

OSPF エリアが保存されます。

ステップ 19　[Save] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

OSPF 設定のインポート フィルタの追加

ライセンス： Control

サポートされるデバイス： シリーズ 3

ルート テーブルに対して OSPF からの受け入れまたは拒否を行うルートを定義するために、インポート フィルタを追加できます。インポート フィルタはテーブルに表示される順に適用されます。

インポート フィルタを追加するときは、仮想ルータに設定したフィルタの 1 つを使用します。フィルタの設定の詳細については、仮想ルータ フィルタのセットアップ（7-30 ページ）を参照してください。

OSPF 設定のインポート フィルタの追加：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　OSPF 仮想ルータ フィルタを追加するデバイスの横にある編集アイコン（）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Virtual Routers] をクリックします。

[Virtual Routers] タブが表示されます。

ステップ 4　OSPF 仮想ルータ フィルタを追加する仮想ルータの横にある編集アイコン（）をクリックします。

[Edit Virtual Router] ポップアップ ウィンドウが表示されます。

ステップ 5　[Dynamic Routing] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6　[OSPF] をクリックして、OSPF オプションを表示します。

ステップ 7　[Import Filters] の下で、追加アイコン（）をクリックします。

[Add Import Filter] ポップアップ ウィンドウが表示されます。

ステップ 8　[Name] ドロップダウン リストから、インポート フィルタとして追加するフィルタを選択します。

ステップ 9　[Action] の横にある [Accept] または [Reject] を選択します。

ステップ 10　[OK] をクリックします。

インポート フィルタが追加されます。

ヒント　インポート フィルタの順序を変更するには、必要に応じて、上へ移動するアイコン（ ）または下へ移動するアイコン（ ）をクリックします。リスト内でフィルタを上下にドラッグすることもできます。

ステップ 11　[Save] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

OSPF 設定へのエクスポート フィルタの追加

ライセンス： Control

サポートされるデバイス： シリーズ 3

ルート テーブルから OSPF に対しての受け入れまたは拒否を行うルートを定義するために、エクスポート フィルタを追加できます。エクスポート フィルタはテーブルに表示される順に適用されます。

エクスポート フィルタを追加するときは、仮想ルータに設定したフィルタの 1 つを使用します。フィルタの設定の詳細については、仮想ルータ フィルタのセットアップ（7-30 ページ）を参照してください。

OSPF 設定へのエクスポート フィルタの追加：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　OSPF 仮想ルータ フィルタを追加するデバイスの横にある編集アイコン（ ）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Virtual Routers] をクリックします。

[Virtual Routers] タブが表示されます。

ステップ 4　OSPF 仮想ルータ フィルタを追加する仮想ルータの横にある編集アイコン（ ）をクリックします。

[Edit Virtual Router] ポップアップ ウィンドウが表示されます。

ステップ 5　[Dynamic Routing] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6　[OSPF] をクリックして、OSPF オプションを表示します。

ステップ 7　[Export Filters] の下で、追加アイコン（ ）をクリックします。

[Add an Export Filter] ポップアップ ウィンドウが表示されます。

ステップ 8　[Name] ドロップダウン リストから、エクスポート フィルタとして追加するフィルタを選択します。

ステップ 9　[Action] の横にある [Accept] または [Reject] を選択します。

ステップ 10　[OK] をクリックします。

エクスポート フィルタが追加されます。

ヒント　エクスポート フィルタの順序を変更するには、必要に応じて、上へ移動するアイコン（ ）または下へ移動するアイコン（ ）をクリックします。リスト内でフィルタを上下にドラッグすることもできます。

ステップ 11　[Save] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

仮想ルータ フィルタのセットアップ

ライセンス： Control

サポートされるデバイス： シリーズ 3

フィルタは、仮想ルータのルート テーブルへのインポートおよびルートのダイナミック プロトコルへのエクスポートを行うために、ルートを照合する方法を提供します。フィルタのリストを作成および管理できます。各フィルタは特定の基準を定義し、静的に定義されるか、またはダイナミック プロトコルから受信したルートを検索します。

ヒント　仮想ルータ フィルタを編集するには、編集アイコン（ ）をクリックします。仮想ルータ フィルタを削除するには、削除アイコンをクリックします（ ）。

仮想ルータ エディタの [Filter] タブには、仮想ルータに設定したすべてのフィルタを含むテーブルが表示されます。このテーブルには次の表に示すように、各フィルタに関するサマリー情報が含まれます。

表 7-3　仮想ルータ フィルタ テーブル ビュー フィールド

フィールド	説明
名前	フィルタの名前。
Protocol	ルートが発生するプロトコル。 • [Static]：ルートはローカル スタティック ルートとして発生します。 • [RIP]：ルートはダイナミックな RIP 設定から発生します。 • [OSPF]：ルートはダイナミックな OSPF 設定から発生します。
From Router	このフィルタがルートで一致を試みるルータの IP アドレス。スタティック フィルタおよび RIP フィルタに対してこの値を入力する必要があります。
Next Hop	このルートを使用するパケットが転送されるネクスト ホップ。スタティック フィルタおよび RIP フィルタに対してこの値を入力する必要があります。
Destination Type	パケットが送信される宛先のタイプ。 • ルータ • デバイス • 廃棄
Destination Network	このフィルタがルートで一致を試みるネットワーク。

表 7-3　仮想ルータ フィルタ テーブル ビュー フィールド（続き）

フィールド	説明
OSPF Path Type	OSPF プロトコルにのみ適用されます。パス タイプは次のいずれかです。 • Ext-1 • Ext-2 • Inter Area • Intra Area
OSPF Router ID	OSPF プロトコルにのみ適用されます。ルート/ネットワークをアドバタイズするルータのルータ ID。

仮想ルータ フィルタの追加:

アクセス: Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　仮想フィルタ ルータを追加するデバイスの横にある編集アイコン（）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Virtual Routers] をクリックします。

[Virtual Routers] タブが表示されます。

ステップ 4　仮想フィルタ ルータを追加する仮想ルータの横にある編集アイコン（）をクリックします。

[Edit Virtual Router] ポップアップ ウィンドウが表示されます。

ステップ 5　[Filter] をクリックして、フィルタ オプションを表示します。

ステップ 6　[Add Filter] をクリックします。

[Create Filter] ポップアップ ウィンドウが表示されます。

ステップ 7　[Name] フィールドにフィルタの名前を入力します。英数字のみを使用できます。

ステップ 8　[Protocol] で、[All] を選択するか、フィルタに適用するプロトコルを選択します。

ステップ 9　プロトコルとして [All]、[Static]、または [RIP] を選択した場合、[From Router] で、このフィルタがルートで一致を試みるルータ IP アドレスを入力します。

IPv4 アドレスに対する /32 の CIDR ブロックと IPv6 アドレスに対する /128 のプレフィクス長も入力可能であることに注意してください。他のすべてのアドレス ブロックは、このフィールドでは無効です。

ステップ 10　[Add] をクリックします。

[From Router] フィールドに値が入力されます。

ステップ 11　プロトコルとして [All]、[Static]、または [RIP] を選択した場合、[Next Hop] で、このフィルタがルートで一致を試みるゲートウェイの IP アドレスを入力します。

IPv4 アドレスに対する /32 の CIDR ブロックと IPv6 アドレスに対する /128 のプレフィクス長も入力可能であることに注意してください。他のすべてのアドレス ブロックは、このフィールドでは無効です。

ステップ 12　[Add] をクリックします。

[Next Hop] フィールドに値が入力されます。

ステップ 13　[Destination Type] で、フィルタに適用するオプションを選択します。

ステップ 14　[Destination Network] で、このフィルタがルートで一致を試みるネットワークの IP アドレスを入力します。

ステップ 15　[Add] をクリックします。

[Destination Network] フィールドに値が入力されます。

ステップ 16　プロトコルとして [All] または [OSPF] を選択した場合、[Path Type] で、フィルタに適用するオプションを選択します。

少なくとも 1 つのパス タイプを選択する必要があります。

ステップ 17　プロトコルとして [OSPF] を選択した場合、[Router ID] で、ルート/ネットワークをアドバタイズするルータのルータ ID の役割を持つ IP アドレスを入力します。

ステップ 18　[Add] をクリックします。

[Router ID] フィールドに値が入力されます。

ステップ 19　[OK] をクリックします。

フィルタが追加されます。

ステップ 20　[Save] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用 (4-27 ページ) を参照してください。

仮想ルータ認証プロファイルの追加

ライセンス： Control

サポートされるデバイス： シリーズ 3

RIP および OSPF の設定で使用する認証プロファイルをセットアップできます。簡易パスワードを設定するか、共有暗号キーを指定できます。簡易パスワードでは、すべてのパケットが 8 バイトのパスワードを伝送できます。システムはこのパスワードが欠如している受信パケットを無視します。暗号キーでは検証が可能で、パスワードから生成される 16 バイト長のダイジェストがすべてのパケットに付加されます。

OSPF の場合、各エリアは異なる認証方式を使用できることに注意してください。そのため、多くのエリア間で共有できる認証プロファイルを作成します。OSPFv3 の認証は追加できません。

ヒント　認証プロファイルを編集するには、編集アイコン（）をクリックします。認証プロファイルを削除するには、削除アイコン（）をクリックします。

仮想ルータ認証プロファイルの追加：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　仮想ルータ認証プロファイルを追加するデバイスの横にある編集アイコン（）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Virtual Routers] をクリックします。

[Virtual Routers] タブが表示されます。

ステップ 4　仮想ルータ認証プロファイルを追加する仮想ルータの横にある編集アイコン( )をクリックします。

[Edit Virtual Router] ポップアップ ウィンドウが表示されます。

ステップ 5　[Authentication Profile] をクリックします。

[Authentication Profile] タブが表示されます。

ステップ 6　[Add Authentication Profile] をクリックします。

[Add Authentication Profile] ポップアップ ウィンドウが表示されます。

ステップ 7　[Authentication Profile Name] フィールドに、認証プロファイルの名前を入力します。

ステップ 8　[Authentication Type] ドロップダウン リストから、[simple] または [cryptographic] を選択します。

ステップ 9　[Password] フィールドに、安全なパスワードを入力します。

ステップ 10　確認のために [Confirm Password] フィールドにもう一度パスワードを入力します。

ステップ 11　[OK] をクリックします。

認証プロファイルが追加されます。

ステップ 12　[Save] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

仮想ルータ統計情報の表示

ライセンス： Control

サポートされるデバイス： シリーズ 3

各仮想ルータの実行時統計情報を表示できます。統計情報にはユニキャスト パケット、ドロップされたパケット、IPv4 および IPv6 アドレスの個別のルーティング テーブルが表示されます。

仮想ルータの統計情報の表示：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　仮想ルータ統計情報を表示するデバイスの横にある編集アイコン( )をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Virtual Routers] をクリックします。

[Virtual Routers] タブが表示されます。

ステップ 4　ルータ統計情報を表示する仮想ルータの横にある表示アイコン( )をクリックします。

[Statistics] ポップアップ ウィンドウが表示されます。

ステップ 5　[OK] をクリックしてウィンドウを閉じます。

仮想ルータの削除

ライセンス：Control

サポートされるデバイス：シリーズ 3

仮想ルータを削除すると、ルータに割り当てられているすべてのルーテッド インターフェイスを他のルータに含めることができるようになります。

仮想ルータの削除：

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　仮想ルータを削除するデバイスの横にある編集アイコン（  ）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Virtual Routers] をクリックします。

[Virtual Routers] タブが表示されます。

ステップ 4　削除する仮想ルータの横にある削除アイコン（  ）をクリックします。

ステップ 5　入力を求められた場合、仮想ルータを削除することを確認します。

仮想ルータが削除されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

集約インターフェイスのセットアップ

シリーズ 3 管理対象デバイスが、ネットワーク間にパケット スイッチングを提供するレイヤ 2 展開、またはインターフェイス間にトラフィックをルーティングするレイヤ 3 展開に設定されている場合、複数の物理イーサネット インターフェイスを管理対象デバイス上の 1 つの論理リンクにグループ化できます。このように 1 つに集約された論理リンクは、帯域幅と冗長性の向上および、2 つのエンドポイント間でのロードバランシングを実現します。

集約リンクを作成するには、スイッチドまたはルーテッド リンク集約グループ（LAG）を作成します。集約グループを作成すると、集約インターフェイスと呼ばれる論理インターフェイスが作成されます。上位層エンティティである LAG は単一の論理リンクに似ており、データ トラフィックは集約インターフェイスを介して送信されます。集約リンクは、複数のリンクの帯域幅をまとめて追加することによって帯域幅を増加させます。また、使用可能なすべてのリンクのトラフィックをロードバランシングすることで、冗長性を実現します。リンクの 1 つで障害が発生すると、トラフィックは残りのリンク全体にロードバランシングされます。

LAG のエンドポイントは、2 つの FirePOWER 管理対象デバイス（上記の図を参照）、またはサードパーティ製アクセス スイッチまたはルータに接続されている 1 つの FirePOWER 管理対象デバイスです。2 つのデバイスは一致している必要はありませんが、同じ物理構成を備え、IEEE 802.ad リンク集約標準をサポートしている必要があります。LAG の一般的な展開は、2 つの管理対象デバイス間のアクセス リンクを集約するか、管理対象デバイスとアクセス スイッチまたはルータ間にポイントツーポイント接続を確立します。

仮想管理対象デバイス、Cisco ASA with FirePOWER Services デバイス、Cisco NGIPS for Blue Coat X-Series デバイスには集約インターフェイスを設定できないので注意してください。

集約インターフェイスの設定方法については、LAG の設定（8-1 ページ）を参照してください。

LAG の設定

ライセンス： Control

サポートされるデバイス： シリーズ 3

集約インターフェイスには 2 つのタイプがあります。スイッチドはレイヤ 2 集約インターフェイス、ルーテッドはレイヤ 3 集約インターフェイスです。リンク集約は、リンク集約グループ（LAG）を使用して実装します。LAG を設定するには、集約スイッチドまたはルーテッド インターフェイスを作成して、一連の物理インターフェイスをリンクに関連付けます。すべての物理インターフェイスは同じ速度とメディアでなければなりません。

集約リンクは動的または静的に作成します。動的リンク集約では、IEEE 802.ad リンク集約標準のコンポーネットである Link Aggregation Control Protocol（LACP）が使用されますが、静的リンク集約では使用されません。LACP は、LAG の両端の各デバイスでリンクおよびシステムの情報を交換できるようにして、集約でアクティブに使用するリンクを決定します。静的 LAG 構成では、手動でリンク集約を維持し、ロード バランシング ポリシーとリンク選択ポリシーを適用する必要があります。

スイッチドまたはルーテッド集約インターフェイスを作成すると、同じタイプのリンク集約グループが自動的に作成され、それに番号が付けられます。たとえば、最初の LAG（スイッチドまたはルーテッド）を作成すると、その集約インターフェイスは、管理対象デバイスの [Interfaces] タブの **lag0** ラベルによって識別できます。物理インターフェイスと論理インターフェイスをこの LAG に関連付けると、それらは階層ツリー メニューのプライマリ LAG の下にネスト表示されます。ただし、スイッチド LAG にはスイッチド物理インターフェイスのみを含めることができ、ルーテッド LAG にはルーテッド物理インターフェイスのみを含めることができます。

LAG を設定する際は、以下の要件を考慮してください。

- FireSIGHT システムは、最大 14 の LAG をサポートし、各 LAG インターフェイスに 0 ～ 13 の一意の ID を割り当てます。LGA ID は設定できません。
- リンクの両側に LAG を設定し、どちらの側のインターフェイスも同じ速度に設定する必要があります。
- 各 LAG ごとに少なくとも 2 つの物理インターフェイスを関連付ける必要があります（最大 8 つ）。物理インターフェイスは複数の LAG に属することはできません。
- LAG の物理インターフェイスは、他の動作モードでインラインまたはパッシブとして使用できず、タグ付きトラフィックの別の論理インターフェイスの一部として使用することもできません。
- LAG の物理インターフェイスは複数の NetMods にまたがることが可能ですが、複数のセンサーにまたがることはできません（すべての物理インターフェイスが同じデバイス上に存在する必要があります）。
- LAG にはスタック構成の NetMod を含めることができません。

注　リンク集約はデバイス クラスタではサポートされません。

詳細については、次の項を参照してください。

- ロード バランシング アルゴリズムの指定（8-3 ページ）
- リンク選択ポリシーの指定（8-3 ページ）
- LACP の設定（8-4 ページ）
- 集約スイッチド インターフェイスの追加（8-5 ページ）
- 集約ルーテッド インターフェイスの追加（8-8 ページ）
- 論理集約インターフェイスの追加（8-11 ページ）
- 集約インターフェイス統計情報の表示（8-13 ページ）
- 集約インターフェイスの削除（8-14 ページ）

ロード バランシング アルゴリズムの指定

ライセンス: Control

サポートされるデバイス: シリーズ 3

LAG バンドルのメンバー リンクへのトラフィックの分散方法を決定する出口ロード バランシング アルゴリズムを LAG に割り当てます。ロード バランシング アルゴリズムは、レイヤ 2 MAC アドレス、レイヤ 3 IP アドレス、レイヤ 4 ポート番号（TCP/UDP トラフィック）など、さまざまなパケット フィールドの値に基づいてハッシュを決定します。選択したロード バランシング アルゴリズムは、LAG バンドルのメンバー リンクすべてに適用されます。

LAG を設定する場合は、次のオプションから展開シナリオに対応するロード バランシング アルゴリズムを選択します。

- Destination IP
- 宛先 MAC
- 宛先ポート
- Source IP
- 送信元 MAC
- 送信元ポート
- Source and Destination IP
- Source and Destination MAC
- Source and Destination Port

注　LAG の両端に同じロード バランシング アルゴリズムを設定する必要があります。必要に応じて、上位層のアルゴリズムが下位層のアルゴリズムにバックオフされます（例：ICMP トラフィックに対してレイヤ 3 にバックオフされるレイヤ 4 アルゴリズムなど）。

リンク選択ポリシーの指定

ライセンス: Control

サポートされるデバイス: シリーズ 3

リンク集約では、両方のエンドポイントで各リンクの速度とメディアが同じである必要があります。リンク プロパティを動的に変更できるので、リンク選択ポリシーは、システムによるリンク選択プロセスの管理方法を決定する上で役立ちます。最大ポート数を最大化するリンク選択ポリシーはリンク冗長性をサポートし、総帯域幅を最大化するリンク選択ポリシーを全体的なリンク速度をサポートします。安定したリンク選択ポリシーは、リンク状態の過剰な変更を最小限に抑えようとします。

注　LAG の両端に同じリンク選択ポリシーを設定する必要があります。

LAG を設定する場合は、次のオプションから展開シナリオに対応するリンク選択ポリシーを選択します。

- [Highest Port Count]：冗長性を向上させる最大アクティブ ポート数を割り当てるには、このオプションを選択します。

- [Highest Total Bandwidth]：集約リンクに最大合計帯域幅を割り当てるには、このオプションを選択します。
- [Stable]：最大の課題がリンクの安定性と信頼性である場合は、このオプションを選択します。LAG を設定すると、アクティブ リンクは、ポート数や帯域幅が追加された場合ではなく、どうしても必要な場合（リンク障害などの場合）にのみ変更されます。
- [LACP Priority]：LAG でアクティブにするリンクを LACP アルゴリズムにより決定するには、このオプションを選択します。この設定は、展開目標が未定義の場合や、LAG の一端のデバイスが FirePOWER 以外のデバイスである場合に適しています。

  LACP が有効な場合、LACP プライオリティに基づくリンク選択ポリシーでは、以下の 2 つの LACP プライオリティ（システム プライオリティとリンク プライオリティ）が使用されます。

  - LACP システム プライオリティ。リンク集約において優位なデバイスを判断するには、LACP を実行している各パートナー デバイスにこの値を設定します。値が小さいシステムほど、システム プライオリティが高くなります。動的リンク集約では、最初に、LACP システム プライオリティの高いシステム側でメンバー リンクに選択された状態が設定され、次に、プライオリティの低いシステムでメンバー リンクが適宜設定されます。0 ～ 65535 を指定できます。値を指定しない場合、デフォルトのプライオリティは 32768 になります。
  - LACP リンク プライオリティ。集約グループに属する各リンクにこの値を設定します。リンク プライオリティによって、LAG におけるアクティブ リンクとスタンバイ リンクが決まります。値が小さいリンクほどプライオリティが高くなります。アクティブ リンクがダウンすると、最もプライオリティの高いスタンバイ リンクが選択され、ダウンしたリンクと交換されます。ただし、複数のリンクの LACP リンク プライオリティが同じである場合は、物理ポート番号が最も小さいリンクがスタンバイ リンクとして選択されます。0 ～ 65535 を指定できます。値を指定しない場合、デフォルトのプライオリティは 32768 になります。

LACP は、動的リンク集約をサポートするリンク選択方式の自動化における主要部分です。詳細については、LACP の設定（8-4 ページ）を参照してください。

LACP の設定

ライセンス： Control

サポートされるデバイス： シリーズ 3

IEEE 802.3ad のコンポーネントであるリンク集約制御プロトコル（LACP）は、LAG バンドルを作成して維持するためにシステムおよびポートの情報を交換する 1 つの方式です。LACP を有効にすると、LAG の両端の各デバイスは LACP を使用して、集約においてアクティブに使用されているリンクを特定します。LACP は、リンク間で LACP パケット（または制御メッセージ）を交換することによって、アベイラビリティと冗長性を実現します。このプロトコルは、リンクの能力を動的に学習し、他のポートに通知します。LACP は、適合するリンクを特定すると、それらのリンクを LAG にグループ化します。あるリンクで障害が発生した場合、トラフィックは他のリンクで継続されます。リンクを機能させるには、LAG の両端で LACP を有効にする必要があります。

LACP を有効にする場合は、LAG の両端で転送モードを選択して、デバイスの間での LACP パケットの交換方法を指定する必要があります。LACP モードには次の 2 つのオプションがあります。

- [Active]：デバイスをアクティブ ネゴシエーション ステートにするにはこのモードを選択します。このモードでは、デバイスは LACP パケットを送信することにより、リモート リンクとのネゴシエーションを開始します。

- [Passive]：デバイスをパッシブ ネゴシエーション ステートにするにはこのモードを選択します。このモードでは、デバイスは受信した LACP パケットには応答しますが、LCAP ネゴシエーションを開始しません。

注　どちらのモードでも、LACP はリンク間でネゴシエートして、それらのリンクがポート速度などの基準に基づいてリンク バンドルを形成可能かどうかを判定できます。ただし、パッシブ対パッシブの構成は避けるようにしてください。そのような構成では、基本的に LAG の両端がリスニング モードになります。

LACP には、デバイス間での LACP パケットの送信頻度を定義するタイマーがあります。LACP は次のレートでパケットを交換します。

- [Slow]：30 秒
- [Fast]：1 秒

このオプションが適用されたデバイスは、LAG の反対側のパートナー デバイスからこの頻度で LACP パケットを受信することを予期します。

注　LAG がデバイス スタック内の管理対象デバイスに設定されている場合は、プライマリ デバイスだけがパートナー システムとの LACP 通信に参加します。すべてのセカンダリ デバイスは、LACP メッセージをプライマリ デバイスに転送します。プライマリ デバイスは、動的な LAG の変更をセカンダリ デバイスにリレーします。

集約スイッチド インターフェイスの追加

ライセンス： Control

サポートされるデバイス： シリーズ 3

管理対象デバイスの 2 ～ 8 つの物理ポートを組み合わせて、スイッチド LAG インターフェイスを作成できます。トラフィックを処理できるようにするには、その前に、スイッチド LAG インターフェイスを仮想スイッチに割り当てる必要があります。管理対象デバイスは、最大 14 の LAG インターフェイスをサポートできます。

注意　センシング インターフェイスまたはインライン セットの MTU の任意の値（シリーズ 2）または最高値（シリーズ 3）を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック検査が一時的に中断されます。この検査中にデバイスがトラフィックをドロップするか、それ以上検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

既存のスイッチド LAG インターフェイスを編集するには、インターフェイスの横にある編集アイコン（ ）をクリックします。

スイッチド LAG インターフェイスの設定方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　スイッチド LAG インターフェイスを設定するデバイスの横にある、編集アイコン（ ）をクリックします。

[Interfaces] タブが表示されます。

ステップ 3　[Add] ドロップダウン メニューから、[Add Aggregate Interface] を選択します。

ステップ 4　[Switched] をクリックして、スイッチド LAG インターフェイスのオプションを表示します。

ステップ 5　オプションで、[Security Zone] ドロップダウン リストから既存のセキュリティ ゾーンを選択するか、または [New] を選択して新しいセキュリティ ゾーンを追加します。

ステップ 6　[Virtual Switch] ドロップダウン リストから既存の仮想スイッチを選択するか、[New] を選択して新しい仮想スイッチを追加します。

注　新しい仮想スイッチを追加する場合は、スイッチド インターフェイスをセットアップした後に、[Device Management] ページの [Virtual Switches] タブ（[Devices] > [Device Management] > [Virtual Switches]）でそのスイッチを設定する必要があります。仮想スイッチの追加（6-7 ページ）を参照してください。

ステップ 7　[Enabled] チェック ボックスをオンにして、スイッチド LAG インターフェイスがトラフィックを処理できるようにします。

このチェック ボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

ステップ 8　[Mode] ドロップダウン リストからリンク モードを指定するオプションを選択するか、または [Autonegotiation] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようインターフェイスを設定します。モード設定は銅線インターフェイス専用であることに注意してください。

注　8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。リンクが自動的に速度をネゴシエートする場合は、同じ速度設定に基づいて LAG のすべてのアクティブ リンクが選択されます。

ステップ 9　[MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または Auto-MDIX のいずれかを指定するオプションを選択します。MDI/MDIX 設定は銅線インターフェイス専用であることに注意してください。

デフォルトでは、MDI/MDIX は自動 MDI に設定され、MDI と MDIX の間のスイッチングを自動的に処理してリンクを確立します。

ステップ 10　[MTU] フィールドに、最大伝送ユニット (MTU) を入力して、パケットの最大許容サイズを指定します。

設定可能な MTU の範囲は、FireSIGHT システムのデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、「管理対象デバイスの MTU の範囲（4-69 ページ）」を参照してください。

ステップ 11　[Link Aggregation] には、LAG バンドルに追加する物理インターフェイスを選択するための 2 つのオプションがあります。

- [Available Interfaces] の横で、1 つ以上のインターフェイスを選択し、選択項目の追加アイコン（ ）をクリックします。複数の物理インターフェイスを選択するには、**Ctrl** キーまたは **Shift** キーを使用します。
- すべてのインターフェイス ペアを LAG バンドルに追加するには、すべてを追加アイコン（ ）をクリックします。

ヒント　LAG バンドルから物理インターフェイスを削除するには、1 つ以上の物理インターフェイスを選択して、選択項目の削除アイコン（ ）をクリックします。LAG バンドルからすべての物理インターフェイスを削除するには、すべてを削除アイコン（ ）をクリックします。[Interfaces] タブから LAG インターフェイスを削除すると、そのインターフェイスも削除されます。

ステップ 12　[Load-Balancing Algorithm] ドロップダウン リストから、展開シナリオに対応するオプションを選択します。詳細については、「ロード バランシング アルゴリズムの指定（8-3 ページ）」を参照してください。

ステップ 13　[Link Selection Policy] ドロップダウン リストから、展開シナリオに対応する次のオプションを選択します。[Highest Port Count]（冗長性）、[Highest Total Bandwidth]（速度）、[Stable]（過剰な変更を避けて、リンク ステートを維持）、または [LACP Priority]（自動リンク集約）。

[LACP Priority] を選択する場合は、[System Priority] の値を割り当てる必要があります。次に、[Configure Interface Priority] リンクをクリックして、LAG の各インターフェイスにプライオリティ値を割り当てます。0 ～ 65535 を指定できます。値を指定しない場合、デフォルトのプライオリティは 32768 になります。詳細については、「リンク選択ポリシーの指定（8-3 ページ）」を参照してください。

注　FireSIGHT システム デバイスとサードパーティ製ネットワーク デバイスとの間に集約インターフェイスを設定する場合は、[LACP Priority] を選択します。

ステップ 14　[Tunnel Level] ドロップダウン リストから、展開シナリオに対応するオプション（[Inner] または [Outer]）を選択します。

レイヤ 3 ロード バランシングが設定されている場合、トンネル レベルは IPv 4 トラフィックにのみ適用されるので注意してください。外部トンネルは常に、レイヤ 2 と IPv6 トラフィックに使用されます。[Tunnel Level] が明示的に設定されていない場合、デフォルトは [Outer] になります。

ステップ 15　[LACP] で [Enabled] チェック ボックスをオンにして、スイッチド LAG インターフェイスがリンク集約制御プロトコルを使用してトラフィックを処理できるようにします。詳細については、「LACP の設定（8-4 ページ）」を参照してください。

このチェックボックスをオフにすると、LAG インターフェイスは静的設定になり、FireSIGHT システム は選択されたすべての物理インターフェイスを集約に使用します。

ステップ 16　[Rate] オプション ボタンをクリックし、パートナー デバイスから LACP 制御メッセージを受信する頻度を設定します。

- パケットを 30 秒ごとに受信するには、[Slow] を選択します。
- パケットを 1 秒ごとに受信するには、[Fast] を選択します。

ステップ 17　[Mode] オプション ボタンをクリックし、デバイスのリスニング モードを設定します。

- パートナー デバイスに LACP パケットを送信してリモート リンクとのネゴシエーションを開始するには、[Active] を選択します。
- 受信した LACP パケットに応答するには、[Passive] を選択します。

ステップ 18　[Save] をクリックします。

スイッチド LAG インターフェイスが設定されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

集約ルーテッド インターフェイスの追加

ライセンス： Control

サポートされるデバイス： シリーズ 3

管理対象デバイスの 2 ～ 8 つの物理ポートを組み合わせて、ルーテッド LAG インターフェイスを作成できます。トラフィックをルーティングする前に、ルーテッド LAG インターフェイスを仮想ルータに割り当てる必要があります。管理対象デバイスは、最大 14 の LAG インターフェイスをサポートできます。

ルーテッド LAG インターフェイスに Address Resolution Protocol（ARP）スタティック エントリを追加できます。外部ホストがトラフィックを送信する、ローカル ネットワーク上の宛先 IP アドレスの MAC アドレスを知る必要がある場合、ARP 要求を送信します。スタティック ARP エントリを設定すると、仮想ルータは IP アドレスおよび関連付けられている MAC アドレスで応答します。

ルーテッド LAG インターフェイスの [ICMP Enable Responses] オプションを無効にしても、すべてのシナリオで ICMP 応答が抑制されるわけではありません。宛先 IP がルーテッド インターフェイスの IP で、プロトコルが ICMP であるパケットをドロップするように、アクセス コントロール ポリシーにルールを追加できます。ネットワークベースのルールによるトラフィックの制御（15-1 ページ）を参照してください。

管理対象デバイスの [Inspect Local Router Traffic] オプションを有効にした場合、パケットはホストに到達する前にドロップされるため、すべての応答を防ぐことができます。ローカル ルータ トラフィックの検査の詳細については、高度なデバイス設定について（4-58 ページ）を参照してください。

注意　センシング インターフェイスまたはインライン セットの MTU の任意の値（シリーズ 2）または最高値（シリーズ 3）を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック検査が一時的に中断されます。この検査中にデバイスがトラフィックをドロップするか、それ以上検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

既存のルーテッド LAG インターフェイスを編集するには、インターフェイスの横にある編集アイコン（  ）をクリックします。

ルーテッド LAG インターフェイスの設定方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　ルーテッド LAG インターフェイスを設定するデバイスの横にある、編集アイコン（）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Add] ドロップダウン メニューから、[Add Aggregate Interface] を選択します。

ステップ 4　[Routed] をクリックして、ルーテッド LAG インターフェイス オプションを表示します。

ステップ 5　オプションで、[Security Zone] ドロップダウン リストから既存のセキュリティ ゾーンを選択するか、または [New] を選択して新しいセキュリティ ゾーンを追加します。

ステップ 6　（任意）[Virtual Router] ドロップダウン リストから既存の仮想ルータを選択するか、または [New] を選択して新しい仮想ルータを追加します。

注　新しい仮想ルータを追加する場合は、ルーテッド インターフェイスをセットアップした後に、[Device Management] ページの [Virtual Routers] タブ（[Devices] > [Device Management] > [Virtual Routers]）でそのルータを設定する必要があります。仮想ルータの追加（7-10 ページ）を参照してください。

ステップ 7　[Enabled] チェック ボックスをオンにして、ルーテッド LAG インターフェイスがトラフィックを処理できるようにします。

このチェック ボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

ステップ 8　[Mode] ドロップダウン リストからリンク モードを指定するオプションを選択するか、または [Autonegotiation] を選択して、速度とデュプレックス設定を自動的にネゴシエートするよう LAG インターフェイスを設定します。モード設定は銅線インターフェイス専用であることに注意してください。

注　8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。リンクが自動的に速度をネゴシエートする場合は、同じ速度設定に基づいて LAG のすべてのアクティブ リンクが選択されます。

ステップ 9　[MDI/MDIX] ドロップダウン リストから、LAG インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または Auto-MDIX のいずれかを指定するオプションを選択します。MDI/MDIX 設定は銅線インターフェイス専用であることに注意してください。

通常、[MDI/MDIX] は [Auto-MDIX] に設定します。これにより、MDI と MDIX の間の切り替えが自動的に処理され、リンクが確立されます。

ステップ 10　[MTU] フィールドに、許容される最大のパケット サイズを指定する、最大伝送単位（MTU）を入力します。MTU はレイヤ 2 MTU/MRU であり、レイヤ 3 MTU ではないことに注意してください。

設定可能な MTU の範囲は、FireSIGHT システムのデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、「管理対象デバイスの MTU の範囲（4-69 ページ）」を参照してください。

ステップ 11　[ICMP] の横にある [Enable Responses] チェック ボックスをオンにして、LAG インターフェイスが ping や traceroute などの ICMP トラフィックに応答できるようにします。

ステップ 12　[IPv6 NDP] の横にある [Enable Router Advertisement] チェック ボックスをオンにして、LAG インターフェイスがルータ アドバタイズメントを伝送できるようにします。

ステップ 13　IP アドレスを追加するには、[Add] をクリックします。

[Add IP Address] ポップアップ ウィンドウが表示されます。

ステップ 14　[Address] フィールドで、CIDR 表記を使用して、ルーテッド LAG インターフェイスの IP アドレスとサブネット マスクを入力します。次の点に注意してください。

- ネットワークおよびブロードキャスト アドレス、またはスタティック MAC アドレス 00:00:00:00:00:00 および FF:FF:FF:FF:FF:FF は追加できません。
- サブネット マスクに関係なく、仮想ルータのインターフェイスに同じ IP アドレスを追加できません。

ステップ 15　(任意)組織で IPv6 アドレスを使用している場合は、[IPv6] フィールドの横にある [Address Autoconfiguration] チェック ボックスをオンにすると、LAG インターフェイスの IP アドレスが自動的に設定されます。

ステップ 16　[Type] には、[Normal] または [SFRP] を選択します。

SFRP オプションの詳細についてはSFRP の設定(7-8 ページ)を参照してください。

ステップ 17　[OK] をクリックします。

IP アドレスが追加されます。

IP アドレスを編集するには、編集アイコン( )をクリックします。IP アドレスを削除するには、削除アイコン( )をクリックします。

注　IP アドレスをクラスタ デバイスのルーテッド インターフェイスに追加する場合、クラスタ ピアのルーテッド インターフェイスに対応する IP アドレスを追加する必要があります。

ステップ 18　スタティック ARP エントリを追加するには、[Add] をクリックします。

[Add Static ARP Entry] ポップアップ ウィンドウが表示されます。

ステップ 19　[IP Address] フィールドに、スタティック ARP エントリの IP アドレスを入力します。

ステップ 20　[MAC Address] フィールドに、IP アドレスに関連付ける MAC アドレスを入力します。2 桁の 16 進数の 6 個のグループをコロンで区切る標準形式を使用して、アドレスを入力します(たとえば、01:23:45:67:89:AB)。

ステップ 21　[OK] をクリックします。

スタティック ARP エントリが追加されます。

ヒント　スタティック ARP エントリを編集するには、編集アイコン( )をクリックします。スタティック ARP エントリを削除するには、削除アイコン( )をクリックします。

ステップ 22　[Link Aggregation] には、LAG バンドルに追加する物理インターフェイスを選択するための 2 つのオプションがあります。

- [Available Interfaces] の横で、1 つ以上のインターフェイスを選択し、選択項目の追加アイコン( )をクリックします。複数の物理インターフェイスを選択するには、**Ctrl** キーまたは **Shift** キーを使用します。
- すべてのインターフェイス ペアを LAG バンドルに追加するには、すべてを追加アイコン( )をクリックします。

ヒント　LAG バンドルから物理インターフェイスを削除するには、1 つ以上の物理インターフェイスを選択して、選択項目の削除アイコン( )をクリックします。LAG バンドルからすべての物理インターフェイスを削除するには、すべてを削除アイコン( )をクリックします。[Interfaces] タブから LAG インターフェイスを削除すると、そのインターフェイスも削除されます。

ステップ 23　[Load-Balancing Algorithm] ドロップダウン リストから、展開シナリオに対応するオプションを選択します。詳細については、「ロード バランシング アルゴリズムの指定(8-3 ページ)」を参照してください。

ステップ 24　[Link Selection Policy] ドロップダウン リストから、展開シナリオに対応する次のオプションを選択します。[Highest Port Count](冗長性)、[Highest Total Bandwidth](速度)、[Stable](過剰な変更を避けて、リンク ステートを維持)、または [LACP Priority](自動リンク集約)。

[LACP Priority] を選択する場合は、[System Priority] の値を割り当てる必要があります。次に、[Configure Interface Priority] リンクをクリックして、LAG の各インターフェイスにプライオリティ値を割り当てます。0 ～ 65535 を指定できます。値を指定しない場合、デフォルトのプライオリティは 32768 になります。詳細については、「リンク選択ポリシーの指定（8-3 ページ）」を参照してください。

注　FireSIGHT システム デバイスとサードパーティ製ネットワーク デバイスとの間に集約インターフェイスを設定する場合は、[LACP Priority] を選択します。

ステップ 25　[Tunnel Level] ドロップダウン リストから、展開シナリオに対応するオプション（[Inner] または [Outer]）を選択します。

レイヤ 3 ロード バランシングが設定されている場合、トンネル レベルは IPv 4 トラフィックにのみ適用されるので注意してください。外部トンネルは常に、レイヤ 2 と IPv6 トラフィックに使用されます。[Tunnel Level] が明示的に設定されていない場合、デフォルトは [Outer] になります。

ステップ 26　[LACP] で [Enabled] チェック ボックスをオンにして、スイッチド LAG インターフェイスがリンク集約制御プロトコルを使用してトラフィックを処理できるようにします。詳細については、「LACP の設定（8-4 ページ）」を参照してください。

このチェックボックスをオフにすると、LAG インターフェイスは静的設定になり、FireSIGHT システム はすべての物理インターフェイスを集約に使用します。

ステップ 27　[Rate] オプション ボタンをクリックし、パートナー デバイスから LACP 制御メッセージを受信する頻度を設定します。

- パケットを 30 秒ごとに受信するには、[Slow] を選択します。
- パケットを 1 秒ごとに受信するには、[Fast] を選択します。

ステップ 28　[Mode] オプション ボタンをクリックし、デバイスのリスニング モードを設定します。

- パートナー デバイスに LACP パケットを送信してリモート リンクとのネゴシエーションを開始するには、[Active] を選択します。
- 受信した LACP パケットに応答するには、[Passive] を選択します。

ステップ 29　[Save] をクリックします。

ルーテッド LAG インターフェイスが設定されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

論理集約インターフェイスの追加

ライセンス： Control

サポートされるデバイス： シリーズ 3

各スイッチドまたはルーテッド集約インターフェイスごとに、複数の論理スイッチド インターフェイスを追加できます。論理 LAG インターフェイスで受信した VLAN タグ付きトラフィックを処理するには、各論理 LAG インターフェイスをその特定のタグに関連付ける必要があります。物理スイッチドまたはルーテッド インターフェイスに追加するのと同じ方法で、論理インターフェイスをスイッチドまたはルーテッド集約インターフェイスに追加します。

注　LAG インターフェイスを作成すると、デフォルトで「タグなし」論理インターフェイスが作成されます。このインターフェイスは **lag*n.0*** ラベルによって識別されます（***n*** は 0 ～ 13 の整数）。動作させるには、各 LAG にこの論理インターフェイスが少なくとも 1 つ必要です。LAG に追加の論理インターフェイスを関連付けて、VLAN タグ付きトラフィックを処理できます。追加する各論理インターフェイスには固有の VLAN タグが必要です。FireSIGHT システムは 1 ～ 4094 の VLAN タグをサポートします。

論理ルーテッド インターフェイスには、SFRP を設定することもできます。詳細については、「SFRP の設定（7-8 ページ）」を参照してください。

論理ルーテッド LAG インターフェイスの [ICMP Enable Responses] オプションを無効にしても、すべてのシナリオで ICMP 応答が抑制されるわけではありません。宛先 IP がルーテッド インターフェイスの IP で、プロトコルが ICMP であるパケットをドロップするように、アクセス コントロール ポリシーにルールを追加できます。ネットワークベースのルールによるトラフィックの制御（15-1 ページ）を参照してください。

管理対象デバイスの [Inspect Local Router Traffic] オプションを有効にした場合、パケットはホストに到達する前にドロップされるため、すべての応答を防ぐことができます。ローカル ルータ トラフィックの検査の詳細については、高度なデバイス設定について（4-58 ページ）を参照してください。

注意　センシング インターフェイスまたはインライン セットの MTU の任意の値（シリーズ 2）または最高値（シリーズ 3）を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック検査が一時的に中断されます。この検査中にデバイスがトラフィックをドロップするか、それ以上検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

既存の論理 LAG インターフェイスを編集するには、インターフェイスの横にある編集アイコン（）をクリックします。

論理 LAG インターフェイスの追加方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　論理 LAG インターフェイスを追加するデバイスの横にある、編集アイコン（）をクリックします。

[Interfaces] タブが表示されます。

ステップ 3　[Add] ドロップダウン メニューから、[Add Logical Interface] を選択します。

[Add Interface] ポップアップ ウィンドウが表示されます。

ステップ 4　[Switched] をクリックしてスイッチド インターフェイス オプションを表示するか、[Routed] をクリックしてルーテッド インターフェイス オプションを表示します。

LAG の論理インターフェイスを作成するときは、[Interface] ドロップダウン リストから使用可能な LAG を選択します。集約インターフェイスは **lag*n*** ラベルによって識別されます（***n*** は 0 ～ 13 の整数）。

スイッチド インターフェイスへの論理インターフェイスの追加方法については、論理スイッチ型インターフェイスの追加（6-4 ページ）を参照してください。

ルーテッド インターフェイスへの論理インターフェイスの追加方法については、論理ルーテッド インターフェイスの追加（7-5 ページ）を参照してください。

注　集約インターフェイスを無効化すると、集約インターフェイスに関連付けられる論理インターフェイスも無効になります。

集約インターフェイス統計情報の表示

ライセンス： Control

サポートされるデバイス： シリーズ 3

各集約インターフェイスのプロトコルおよびトラフィックの統計情報を表示できます。統計情報には、LACP キーとパートナー情報などの LACP プロトコル情報、受信パケット、転送パケット、ドロップ パケットが表示されます。統計情報は、メンバー インターフェイスごとに詳細化されており、ポート単位でトラフィックとリンクの情報が表示されます。

集約インターフェイス情報は、事前定義されたウィジェットを介してダッシュボードにも表示されます。Current Interface Status ウィジェットは、有効になっているか未使用のアプライアンスのすべてのインターフェイスのステータスを示します。Interface Traffic ウィジェットには、ダッシュボードの時間範囲においてアプライアンスのインターフェイスで送受信された受信（Rx）トラフィックと送信（Tx）トラフィックの割合が示されます。事前定義されたウィジェットについて（55-7 ページ）を参照してください。

集約インターフェイス統計情報の表示方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　論理集約インターフェイス統計情報を表示するデバイスの横にある、編集アイコン（ ）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　インターフェイス統計情報を表示するインターフェイスの横にある、表示アイコン（ ）をクリックします。

[Statistics] ポップアップ ウィンドウが表示されます。

ステップ 4　[OK] をクリックしてウィンドウを閉じます。

集約インターフェイスの削除

ライセンス： Control

サポートされるデバイス： シリーズ 3

以下の手順は、集約インターフェイスの削除方法を示しています。

集約インターフェイスの削除方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　集約インターフェイスを削除するデバイスの横にある、編集アイコン（ ）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　削除する集約インターフェイスの横にある、削除アイコン（ ）をクリックします。

集約インターフェイスは **lag*n*** ラベルによって識別できます（***n*** は 0 ～ 13 の整数）。

ステップ 4　プロンプトが表示されたら、集約インターフェイスを削除することを確認します。

インターフェイスが削除されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

ハイブリッド インターフェイスの設定

FireSIGHT システムが仮想ルータと仮想スイッチ間のトラフィックをブリッジングできるようにする論理ハイブリッド インターフェイスを、管理対象デバイスに設定できます。仮想スイッチのインターフェイスで受信した IP トラフィックが、関連付けられているハイブリッド論理インターフェイスの MAC アドレスにアドレス指定されている場合、システムはそれをレイヤ 3 トラフィックとして処理して、送信先 IP アドレスに応じてトラフィックをルーティングするかまたはトラフィックに応答します。それ以外のトラフィックを受信すると、システムはそれをレイヤ 2 トラフィックとして扱い、適切にスイッチングします。仮想管理対象デバイスや Cisco NGIPS for Blue Coat X-Series に論理ハイブリッド インターフェイスを設定することはできません。

ハイブリッド インターフェイスを設定する方法の詳細については、論理ハイブリット インターフェイスの追加（9-1 ページ）を参照してください。

論理ハイブリット インターフェイスの追加

ライセンス： Control

サポートされるデバイス： シリーズ 3

レイヤ 2 とレイヤ 3 の間でトラフィックを中継するには、論理ハイブリッド インターフェイスを仮想ルータと仮想スイッチに関連付ける必要があります。仮想スイッチに関連付けることができるハイブリッド インターフェイスは 1 つだけです。一方、仮想ルータには複数のハイブリッド インターフェイスを関連付けることができます。

論理ハイブリッド インターフェイスには、SFRP を設定することもできます。詳細については、「SFRP の設定（7-8 ページ）」を参照してください。

ハイブリッド インターフェイスの [ICMP Enable Responses] オプションを無効にしても、すべてのシナリオで ICMP 応答が抑止されるわけではありません。宛先 IP がハイブリッド インターフェイスの IP で、プロトコルが ICMP であるパケットをドロップするように、アクセス コントロール ポリシーにルールを追加することができます。ネットワークベースのルールによるトラフィックの制御（15-1 ページ）を参照してください。

管理対象デバイスの [Inspect Local Router Traffic] オプションを有効にした場合、パケットはホストに到達する前にドロップされるため、すべての応答を防ぐことができます。ローカル ルータ トラフィックの検査の詳細については、高度なデバイス設定について（4-58 ページ）を参照してください。

注意　センシング インターフェイスまたはインライン セットの MTU の任意の値（シリーズ 2）または最高値（シリーズ 3）を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック検査が一時的に中断されます。この検査中にデバイスがトラフィックをドロップするか、それ以上検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

既存のハイブリッド インターフェイスを編集するには、インターフェイスの横にある編集アイコン（）をクリックします。

論理ハイブリッド インターフェイスを追加する方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　ハイブリッド インターフェイスを追加するデバイスの横にある編集アイコン（）をクリックします。

[Interfaces] タブが表示されます。

ステップ 3　[Add] ドロップダウン メニューから、[Add Logical Interface] を選択します。

[Add Interface] ポップアップ ウィンドウが表示されます。

ステップ 4　[Hybrid] をクリックして、ハイブリッド インターフェイス オプションを表示します。

ステップ 5　[Name] フィールドに、インターフェイスの名前を入力します。英数字とスペースを使用できます。

ステップ 6　[Virtual Router] ドロップダウン リストから既存の仮想ルータを選択し、[None] を選択するか、または [New] を選択して新しい仮想ルータを追加します。

新しい仮想ルータを追加する場合は、ハイブリッド インターフェイスのセットアップが完了した後に、[Device Management] ページ（[Devices] > [Device Management] > [Virtual Routers]）で、その仮想ルータを設定する必要があることに注意してください。仮想ルータの追加（7-10 ページ）を参照してください。

ステップ 7　[Virtual Switch] ドロップダウン リストから既存の仮想スイッチを選択し、[None] を選択するか、または [New] を選択して新しい仮想スイッチを追加します。

新しい仮想スイッチを追加する場合は、ハイブリッド インターフェイスのセットアップが完了した後に、[Device Management] ページ（[Devices] > [Device Management] > [Virtual Switches]）で、その仮想スイッチを設定する必要があることに注意してください。仮想スイッチの追加（6-7 ページ）を参照してください。

ステップ 8　ハイブリッド インターフェイスにトラフィックを処理させるには、[Enabled] チェック ボックスをオンにします。

このチェック ボックスをオフにすると、インターフェイスは無効になり、管理上はダウンした状態になります。

ステップ 9　[MTU] フィールドに、パケットの最大許容サイズを示す最大伝送単位（MTU）を入力します。

設定可能な MTU の範囲は、FireSIGHT システムのデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、「管理対象デバイスの MTU の範囲（4-69 ページ）」を参照してください。

ステップ 10　[ICMP] の横にある [Enable Responses] チェック ボックスをオンにして、インターフェイスを ping や traceroute などの ICMP トラフィックに応答可能にします。

ステップ 11　[IPv6 NDP] の横にある [Enable Router Advertisement] チェック ボックスをオンにして、インターフェイスがルータ アドバタイズメントを伝送できるようにします。

このオプションを選択できるのは、IPv6 アドレスを追加した場合のみです。

ステップ 12　IP アドレスを追加するには、[Add] をクリックします。

[Add IP Address] ポップアップ ウィンドウが表示されます。

ステップ 13　[Address] フィールドに、IP アドレスとサブネット マスクを入力します。次の点に注意してください。

- ネットワークおよびブロードキャスト アドレス、またはスタティック MAC アドレス 00:00:00:00:00:00 および FF:FF:FF:FF:FF:FF は追加できません。
- サブネット マスクに関係なく、仮想ルータのインターフェイスに同じ IP アドレスを追加できません。

ステップ 14　IPv6 アドレスがある場合、オプションで、[IPv6] フィールドの横にある [Address Autoconfiguration] チェック ボックスをオンにして、インターフェイスの IP アドレスを自動的に設定します。

ステップ 15　[Type] には、[Normal] または [SFRP] を選択します。

SFRP オプションの詳細についてはSFRP の設定（7-8 ページ）を参照してください。

ステップ 16　[OK] をクリックします。

IP アドレスが追加されます。

ヒント　IP アドレスを編集するには、編集アイコン（ ）をクリックします。IP アドレスを削除するには、削除アイコン（ ）をクリックします。

ステップ 17　[Save] をクリックします。

論理ハイブリッド インターフェイスが追加されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

論理ハイブリッド インターフェイスの削除

ライセンス： Control

サポートされるデバイス： シリーズ 3

以下の手順で、論理ハイブリッド インターフェイスを削除する方法を説明します。

ハイブリッド インターフェイスを削除する方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　論理ハイブリッド インターフェイスを削除するデバイスの横にある編集アイコン（ ）をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　削除する論理ハイブリッド インターフェイスの横にある削除アイコン( )をクリックします。

ステップ 4　プロンプトが出されたら、インターフェイスを削除することを確認します。

インターフェイスが削除されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

ゲートウェイ VPN の使用

バーチャル プライベート ネットワーク（VPN）は、インターネットや他のネットワークなどのパブリック ソースを介したエンドポイント間でセキュアなトンネルを確立するネットワーク接続です。FireSIGHT システムを設定して、Ciscoの管理対象デバイスの仮想ルーター間に、セキュアな VPN トンネルを構築することができます。システムは、インターネット プロトコル セキュリティ（IPSec）プロトコル スイートを使用してトンネルを構築します。

Ciscoの VPN 展開でエンドポイントとして使用できるのは、Ciscoの管理対象デバイスのみです。サードパーティ製のエンドポイントはサポートされません。

VPN 接続が確立されると、ローカル ゲートウェイの背後にあるホストはセキュアな VPN トンネルを介して、リモート ゲートウェイの背後にあるホストに接続することができます。接続は、2 つのゲートウェイの IP アドレスとホスト名、その背後のサブネット、および相互認証のための 2 つのゲートウェイの共有秘密で構成されます。

VPN エンドポイントは、Internet Key Exchange（IKE）のバージョン 1 またはバージョン 2 のいずれかのプロトコルを使用して相互に認証し、トンネルに対してセキュリティ アソシエーションを作成します。システムは IPSec 認証見出し（AH）プロトコルまたは IPSec カプセル化セキュリティ ペイロード（ESP）プロトコルのいずれかを使用して、トンネルに入るデータを認証します。ESP プロトコルは、AH と同じ機能を提供する他にデータの暗号化も行います。

展開にアクセス コントロール ポリシーが存在する場合、システムは、VPN トラフィックがアクセス コントロールを通過するまで VPN トラフィックを送信しません。またシステムは、トンネルが停止している場合は、トンネルのトラフィックをパブリック ソースに送信しません。

VPN 展開を設定および適用するには、該当する対象管理デバイスで VPN ライセンスを有効にしておく必要があります。また、VPN 機能は シリーズ 3 デバイスでのみ使用できます。

VPN 展開の作成および管理の詳細については、以下の項を参照してください。

IPSec について

IPSec プロトコル スイートは、VPN トンネルにおいて、IP パケットが ESP または AH セキュリティ プロトコルでどのようにハッシュ、暗号化、およびカプセル化されるかを定義します。FireSIGHT システムはハッシュ アルゴリズムおよび Security Association（SA）の暗号キーを使用しますが、これは、Internet Key Exchange（IKE）プロトコルによって 2 つのゲートウェイ間で確立されています。

セキュリティ アソシエーション（SA）は 2 つのデバイス間で共有のセキュリティ属性を確立し、VPN エンドポイントがセキュアな通信をサポートできるようにします。SA は、2 つの VPN エンドポイントが、VPN トンネルがどのようにセキュアにされているかを表すパラメータを処理することができます。

システムは、IPSec 接続のネゴシエーションの最初の段階で Internet Security Association and Key Management Protoco（ISAKMP）を使用し、エンドポイントと認証キー交換の間で VPN を確立します。IKE プロトコルは ISAKMP 内にあります。IKE プロトコルの詳細については、IKE について（10-2 ページ）を参照してください。

AH セキュリティ プロトコルは、パケット 見出しとデータを保護しますが、暗号化はできません。ESP はパケットを暗号化および保護しますが、最も外側の IP 見出しをセキュアにすることはできません。多くの場合、この保護は必要なく、大半の VPN 展開は、（暗号化の機能により）AH よりも頻繁に ESP を使用します。VPN はトンネル モードのみで動作するため、システムはレイヤ 3 からのパケット全体を暗号化および認証し、ESP プロトコル内で稼動します。トンネル モードの ESP は、後者の暗号化機能だけでなく、データを暗号化します。

IKE について

FireSIGHT システムは、トンネルに対して SA をネゴシエートする他に、IKE プロトコルを使用して 2 つのゲートウェイを相互に手動で認証します。プロセスは、次の 2 つのフェーズで構成されます。

IKE フェーズ 1 では、Diffie-Hellman キー交換によってセキュアに認証された通信チャネルを確立し、より多くの IKE 通信を暗号化するために事前共有キーを生成します。このネゴシエーションにより、双方向の ISAKMP セキュリティ アソシエーションが生じます。ユーザは、事前共有キーを使用して認証を行うことができます。フェーズ 1 はメイン モードで機能します。このフェーズでは、ネゴシエーションの間にすべてのデータを保護しようとしますが、ピアのアイデンティティも保護します。

IKE フェーズ 2 では、IKE ピアが、フェーズ 1 で確立されたセキュアなチャネルを使用して、IPSec の代わりにセキュリティ アソシエーションにネゴシエートします。ネゴシエーションにより、最低 2 つの単方向セキュリティ アソシエーション（一方は着信、他方は発信）が生じます。

VPN 展開について

VPN 展開は、VPN に含まれているエンドポイントおよびネットワークを指定し、それらが相互にどのように接続しているかを指定します。VPN 展開を設定したら、その展開を管理対象デバイス、または他の Defense Centerで管理されているデバイスに適用することができます。

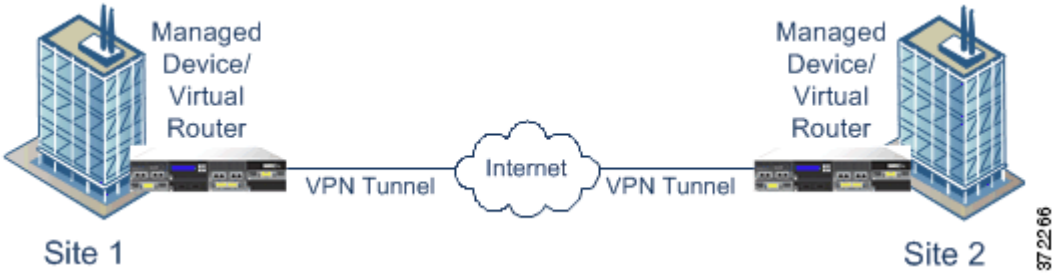
システムでは、3 つのタイプの VPN 展開（ポイントツーポイント、スター、メッシュ）をサポートしています。これらの VPN 展開の詳細については、以下の項を参照してください。

- ポイントツーポイントの VPN 展開について（10-3 ページ）
- スター VPN 展開について（10-3 ページ）
- メッシュ VPN 展開について（10-4 ページ）

ポイントツーポイントの VPN 展開について

ポイントツーポイントの VPN 展開では、2 つのエンドポイントが相互に直接通信します。2 つのエンドポイントをピア デバイスとして設定し、いずれかのデバイスでセキュアな接続を開始することができます。この設定の各デバイスは、VPN 対応の管理対象デバイスであることが必要です。

次の図は、一般的なポイントツーポイントの VPN 展開を示しています。



詳細については、「ポイントツーポイント VPN 展開の設定（10-6 ページ）」を参照してください。

スター VPN 展開について

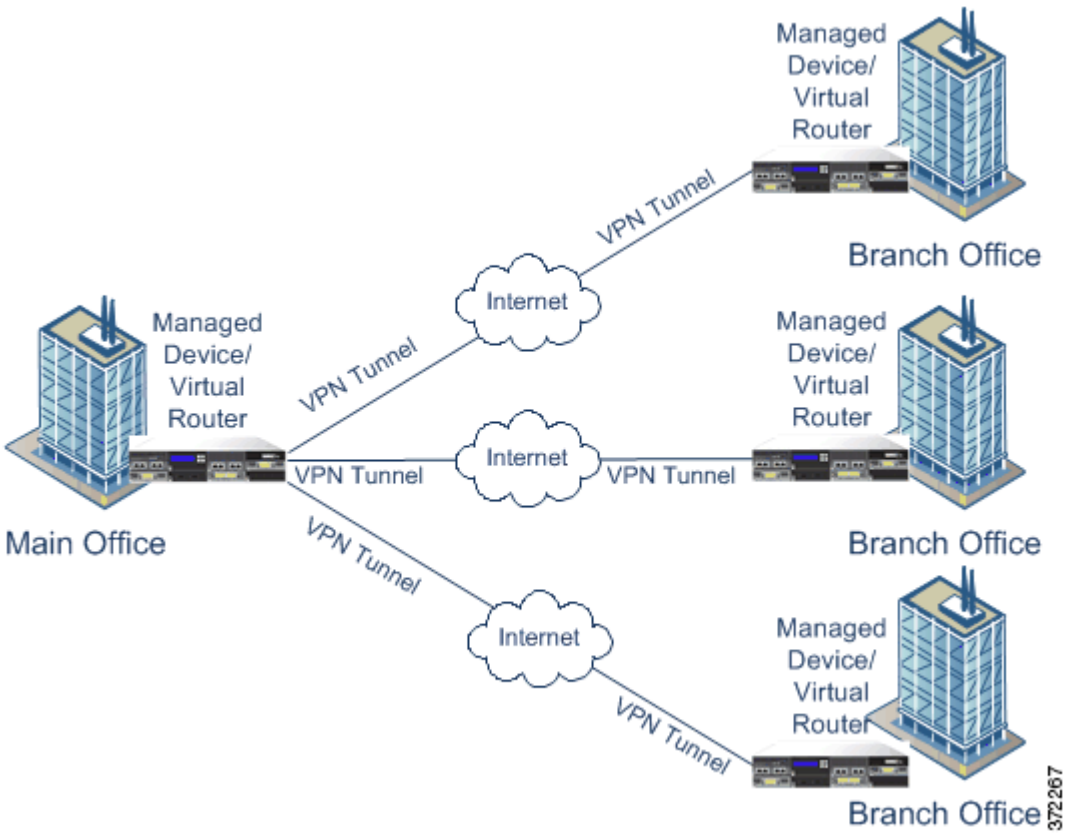
スター VPN 展開では、中央のエンドポイント（ハブ ノード）が、複数のリモート エンドポイント（リーフ ノード）とのセキュアな接続を確立します。ハブ ノードと個々のリーフ ノード間のそれぞれの接続は、別の VPN トンネルです。いずれかのリーフ ノードの背後にあるホストは、ハブ ノードを介して互いに通信できます。

スター型の展開は一般的に、インターネットや他のサードパーティのネットワークを介してセキュアな接続を使用している組織の本店と支店を接続する VPN を表します。スター VPN 展開は、すべての従業員に対して、組織のネットワークへのコントロールされたアクセスを提供します。

一般的なスター型の展開では、ハブ ノードは本社に配置します。リーフ ノードは支店に配置し、大半のトラフィックを開始します。各ノードは、VPN 対応の管理対象デバイスであることが必要です。

スター型の展開は、IKE バージョン 2 のみをサポートしていることに注意してください。

次の図は、一般的なスター VPN 展開を示しています。

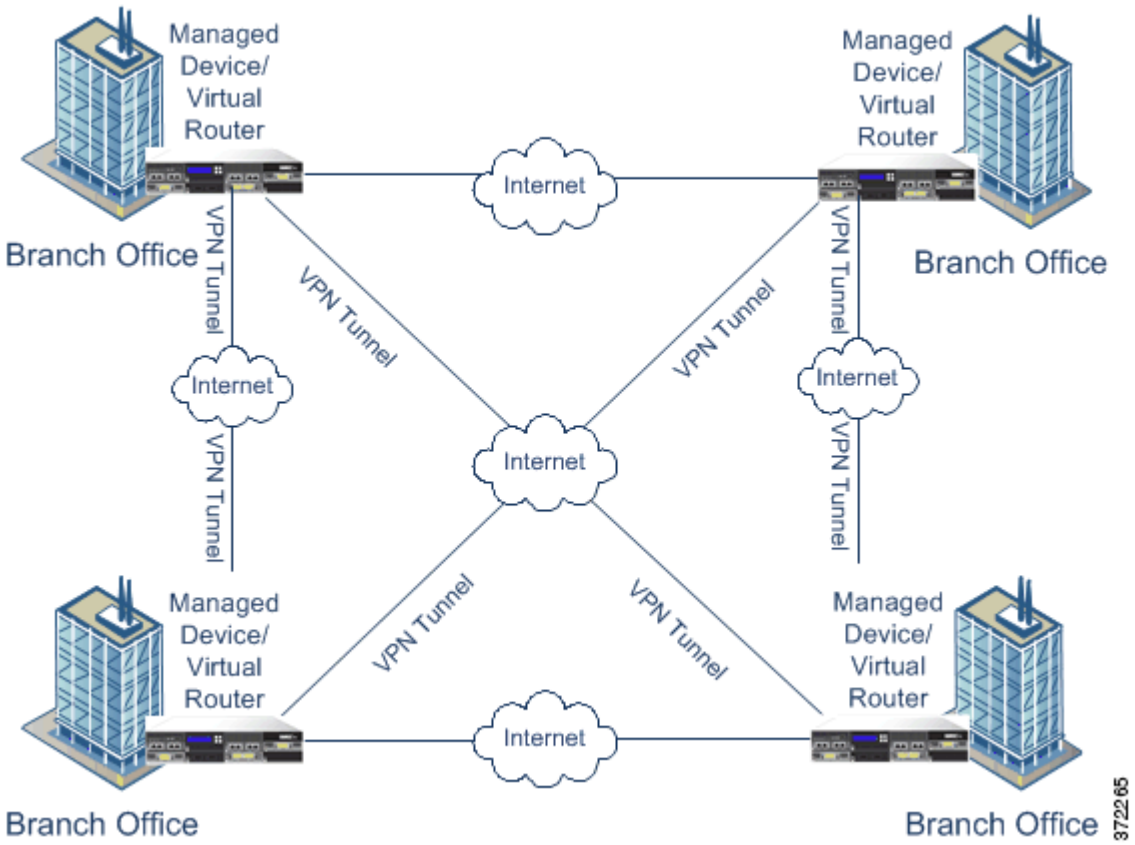


詳細については、「スター VPN 展開の設定（10-9 ページ）」を参照してください。

メッシュ VPN 展開について

メッシュ VPN 展開では、すべてのエンドポイントが個々の VPN トンネルによって他のエンドポイントと通信できます。メッシュ型の展開では 1 つのエンドポイントで障害が発生しても残りのエンドポイントが相互に通信できるように、冗長性を備えています。このタイプの展開は一般的に、分散した支店が配置されたグループを接続する VPN を表します。この設定で展開する VPN 対応の管理対象デバイスの数は、必要な冗長性のレベルによって異なります。各エンドポイントは、VPN 対応の管理対象デバイスであることが必要です。

次の図は、一般的なメッシュ VPN 展開を示しています。



詳細については、「メッシュ VPN 展開の設定（10-11 ページ）」を参照してください。

VPN 展開の管理

ライセンス： VPN

サポートされるデバイス： シリーズ 3

[VPN] ページ（[Devices] > [VPN]）で、現行のすべての VPN 展開を、展開に含まれている名前およびエンドポイントごとに表示することができます。このページでのオプションで、VPN 展開のステータスを表示する、新しい展開を作成する、展開を適用する、展開を修正または削除する、といったことができます。

注意　デバイスをDefense Centerに登録するときにデフォルトのアクセス コントロール ポリシーを選択した場合は、デフォルトのアクセス コントロール ルールがすべてのトラフィックをブロックします。デバイス上で VPN 展開を設定すると、展開は失敗します。

デバイスをDefense Centerに登録すると、適用した VPN 展開は、登録中はDefense Centerと同期することに注意してください。

以下の表で、[VPN] ページで展開を管理するために実行できる操作について説明します。

表 10-1　VPN 展開の管理操作

目的	操作
新しい VPN 展開を作成する	[Add] をクリックします。詳細については、「VPN 展開の設定（10-6 ページ）」を参照してください。
既存の VPN 展開の設定を変更する	編集アイコン（）をクリックします。詳細については、「VPN 展開の設定（10-6 ページ）」を参照してください。
既存の VPN 展開のステータスを表示する	ステータス アイコンをクリックします。詳細については、「VPN 展開のステータスの表示（10-16 ページ）」を参照してください。
VPN 展開を、展開内で対象とするすべてのデバイスに適用する	適用アイコン（  ）をクリックします。詳細については、「VPN 展開の適用（10-15 ページ）」を参照してください。
VPN 展開を削除する	削除アイコン（）をクリックして [Yes] をクリックします。展開を削除しない場合は [No] をクリックします。

VPN 展開の設定

ライセンス： VPN

サポートされるデバイス： シリーズ 3

新しい VPN 展開を作成する場合には、最小限の処理として、一意の名前と展開のタイプを指定し、事前共有キーを指定する必要があります。次の 3 つのタイプの展開から選択することができます。それぞれの展開には、VPN トンネルが含まれています。

- ポイントツーポイント（PTP）型の展開は、2 つのエンドポイント間で VPN トンネルを確立します。
- スター型の展開は VPN トンネルのグループを確立し、ハブ エンドポイントをリーフ エンドポイントのグループに接続します。
- メッシュ型の展開は、エンドポイントのセット内で VPN トンネルのグループを確立します。

Ciscoの VPN 展開でエンドポイントとして使用できるのは、Ciscoの管理対象デバイスのみです。サードパーティ製のエンドポイントはサポートされません。

VPN 認証に対して事前共有キーを定義する必要があります。展開内で生成したすべての VPN 接続で使用するデフォルトのキーを指定できます。ポイントツーポイント型の展開では、各エンドポイントのペアに事前共有キーを指定できます。

各タイプの VPN 展開の作成の詳細については、次の項を参照してください。

- ポイントツーポイント VPN 展開の設定（10-6 ページ）
- スター VPN 展開の設定（10-9 ページ）
- メッシュ VPN 展開の設定（10-11 ページ）

ポイントツーポイント VPN 展開の設定

ライセンス： VPN

サポートされるデバイス： シリーズ 3

ポイントツーポイント VPN 展開を設定する場合は、エンドポイント ペアのグループを定義し、各ペアの 2 つのノード間に VPN を作成します。詳細については、ポイントツーポイントの VPN 展開について（10-3 ページ）を参照してください。

次に、展開で指定できるオプションについて示します。

名前

展開に一意の名前を指定します。

タイプ

ポイントツーポイント型の展開を設定するには、[PTP] をクリックします。

Pre-shared Key

認証に対して一意の事前共有キーを定義します。各エンドポイント ペアに対して事前共有キーを指定しない場合は、システムで展開内のすべての VPN に対してこのキーが使用されます。

デバイス

展開のエンドポイントとして、デバイス スタックやクラスタなどの管理対象デバイスを選択できます。使用しているDefense Centerで管理されていないCiscoの管理対象デバイスの場合は、[Other] を選択し、エンドポイントの IP アドレスを指定します。

Virtual Router

エンドポイントとして管理対象デバイスを選択した場合は、選択したデバイスに適用されている仮想ルータを選択します。複数のエンドポイントに同じ仮想ルータを選択することはできません。

インターフェイス

エンドポイントとして管理対象デバイスを選択した場合は、選択した仮想ルータに割り当てられているルーテッド インターフェイスを選択します。

IP Address

- エンドポイントとして管理対象デバイスを選択した場合は、選択したルーテッド インターフェイスに割り当てられている IP アドレスを選択します。
- 管理対象デバイスがデバイス クラスタの場合は、SFRP の IP アドレスのリストからのみ選択できます。
- 選択した管理対象デバイスがDefense Centerで管理されて**いない**場合は、エンドポイントに IP アドレスを指定します。

Protected Networks

暗号化された展開でネットワークを指定します。各ネットワークに対して CIDR ブロックでサブネットを入力します。IKE バージョン 1 は、保護された単一のネットワークのみサポートしています。

VPN エンドポイントは同じ IP アドレスを持つことはできません。また、VPN エンドポイント ペアの保護されたネットワークは重複することはできないことに注意してください。エンドポイントについて保護されたネットワークのリストに 1 つ以上の IPv4 または IPv6 エントリが含まれている場合、他のエンドポイントの保護されたネットワークは、同じタイプ（IPv4 または IPv6）のエントリを少なくとも 1 つ持っていることが必要です。このようなエントリを持っていない場合、他のエンドポイントの IP アドレスが同じタイプであること、および保護されたネットワーク内でエントリが重複しないことが必要です（IPv4 については /32 CIDR アドレスを使用し、IPv6 については /128 CIDR アドレス ブロックを使用します）。これらの両方のチェックに失敗すると、エンドポイントのペアは機能しません。

Internal IP

エンドポイントが、ネットワーク アドレス変換を備えたファイアウォールの背後に配置されている場合は、このチェック ボックスをオンにします。

Public IP

[Internal IP] を選択した場合は、ファイアウォールに対してパブリック IP アドレスを指定します。エンドポイントが応答側の場合は、この値を指定する必要があります。

Public IKE Port

[Internal IP] を選択した場合は、内部のエンドポイントにポート転送されているファイアウォール上の UDP ポートに対して、1～65535 の数値を指定します。エンドポイントが応答側で、転送されているファイアウォール上のポートが 500 または 4500 ではない場合、この値を指定する必要があります。

Use Deployment Key

展開に対して定義されている事前共有キーを使用する場合は、チェック ボックスをオンにします。このエンドポイント ペアに対して VPN 認証の事前共有キーを指定するには、チェック ボックスをオフにします。

Pre-shared Key

[Use Deployment Key] チェック ボックスをオフにした場合は、このフィールドに事前共有キーを指定します。

ヒント　既存のポイントツーポイント型の展開を編集するには、展開の隣にある編集アイコン( )をクリックします。展開を最初に保存した後で、展開のタイプを編集することはできません。2 人のユーザが同じ展開について同時に編集**してはいけません**。ただし、Web インターフェイスでは同時編集を防止していないことに注意してください。

ポイントツーポイント VPN 展開を設定する方法

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [VPN] を選択します。

[VPN] ページが表示されます。

ステップ 2　[Add] をクリックします。

[Create New VPN Deployment] ポップアップ ウィンドウが表示されます。

ステップ 3　展開に一意の [Name] を指定します。

スペースや特殊文字を含めて、印刷可能なすべての文字を使用できます。

ステップ 4　[Type] として [PTP] が選択されていることを確認します。

ステップ 5　展開に一意の [Pre-shared Key] を指定します。

ステップ 6　[Node Pairs] の隣の追加アイコン( )クリックします。

[Add New Endpoint Pair] ポップアップ ウィンドウが表示されます。

ステップ 7　この項で説明したとおりに、VPN 展開を設定します。

ステップ 8　[Node A] の下の [Protected Networks] の隣にある追加アイコン( )をクリックします。

[Add Network] ポップアップ ウィンドウが表示されます。

ステップ 9　保護されたネットワークの CIDR ブロックを入力します。

ステップ 10　[OK] をクリックします。

保護されたネットワークが追加されます。

ステップ 11　[Node B] に対して手順 8～10 を繰り返します。

ステップ 12　[Save] をクリックします。

エンドポイントのペアが展開に追加され、[Create New VPN Deployment] ポップアップ ウィンドウがもう一度表示されます。

ステップ 13　[Save] をクリックして展開の設定を終了すると、[VPN] ページがもう一度表示されます。

内容を反映させるには、展開を適用する必要があることに注意してください。VPN 展開の適用（10-15 ページ）を参照してください。

スター VPN 展開の設定

ライセンス： VPN

サポートされるデバイス： シリーズ 3

スター VPN 配置を設定する場合は、1 つのハブ ノード エンドポイント、およびリーフ ノード エンドポイントのグループを定義します。展開を設定するには、ハブ ノード エンドポイントと、少なくとも 1 つのリーフ ノード エンドポイントを定義する必要があります。詳細については、スター VPN 展開について（10-3 ページ）を参照してください。

次に、展開で指定できるオプションについて示します。

名前

展開に一意の名前を指定します。

タイプ

スター型の展開を設定するには、[Star] をクリックします。

Pre-shared Key

認証に対して一意の事前共有キーを定義します。

デバイス

展開のエンドポイントとして、デバイス スタックやクラスタなどの管理対象デバイスを選択できます。使用しているDefense Centerで管理されていないCiscoの管理対象デバイスの場合は、[Other] を選択し、エンドポイントの IP アドレスを指定します。

Virtual Router

エンドポイントとして管理対象デバイスを選択した場合は、選択したデバイスに適用されている仮想ルータを選択します。複数のエンドポイントに同じ仮想ルータを選択することはできません。

インターフェイス

エンドポイントとして管理対象デバイスを選択した場合は、選択した仮想ルータに割り当てられているルーテッド インターフェイスを選択します。

IP Address

- エンドポイントとして管理対象デバイスを選択した場合は、選択したルーテッド インターフェイスに割り当てられている IP アドレスを選択します。
- 管理対象デバイスがデバイス クラスタの場合は、SFRP の IP アドレスのリストからのみ選択できます。
- 選択した管理対象デバイスがDefense Centerで管理されて**いない**場合は、エンドポイントに IP アドレスを指定します。

Protected Networks

暗号化された展開でネットワークを指定します。各ネットワークに対して CIDR ブロックでサブネットを入力します。

VPN エンドポイントは同じ IP アドレスを持つことはできません。また、VPN エンドポイント ペアの保護されたネットワークは重複することはできないことに注意してください。エンドポイントについて保護されたネットワークのリストに 1 つ以上の IPv4 または IPv6 エントリが含まれている場合、他のエンドポイントの保護されたネットワークは、同じタイプ（IPv4 または IPv6）のエントリを少なくとも 1 つ持っていることが必要です。このようなエントリを持っていない場合、他のエンドポイントの IP アドレスが同じタイプであること、および保護されたネットワーク内でエントリが重複しないことが必要です（IPv4 については /32 CIDR アドレスを使用し、IPv6 については /128 CIDR アドレス ブロックを使用します）。これらの両方のチェックに失敗すると、エンドポイントのペアは機能しません。

Internal IP

エンドポイントが、ネットワーク アドレス変換を備えたファイアウォールの背後に配置されている場合は、このチェック ボックスをオンにします。

Public IP

[Internal IP] を選択した場合は、ファイアウォールに対してパブリック IP アドレスを指定します。エンドポイントが応答側の場合は、この値を指定する必要があります。

Public IKE Port

[Internal IP] を選択した場合は、内部のエンドポイントにポート転送されているファイアウォール上の UDP ポートに対して、1～65535 の数値を指定します。エンドポイントが応答側で、転送されているファイアウォール上のポートが 500 または 4500 ではない場合、この値を指定する必要があります。

ヒント　既存のスター型の展開を編集するには、展開の隣にある編集アイコン（ ）をクリックします。展開を最初に保存した後で、展開のタイプを編集することはできません。展開のタイプを変更するには、展開を削除してから新しい展開を作成する必要があります。2 人のユーザが同じ展開について同時に編集**してはいけません**。ただし、Web インターフェイスでは同時編集を防止していないことに注意してください。

スター型の展開を設定する方法

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [VPN] を選択します。

[VPN] ページが表示されます。

ステップ 2　[Add] をクリックします。

[Create New VPN Deployment] ポップアップ ウィンドウが表示されます。

ステップ 3　展開に一意の [Name] を指定します。

スペースや特殊文字を含めて、印刷可能なすべての文字を使用できます。

ステップ 4　[Type] を指定して [Star] をクリックします。

ステップ 5　展開に一意の [Pre-shared Key] を指定します。

ステップ 6　[Hub Nod] の隣の追加アイコン（ ）クリックします。

[Add Hub Node] ポップアップ ウィンドウが表示されます。

ステップ 7　この項で説明したとおりに、VPN 展開を設定します。

ステップ 8　[Protected Networks] の隣の追加アイコン（ ）クリックします。

[Add Network] ポップアップ ウィンドウが表示されます。

ステップ 9　保護されたネットワークの IP アドレスを入力します。

ステップ 10　[OK] をクリックします。

保護されたネットワークが追加されます。

ステップ 11　[Save] をクリックします。

ハブ ノードが展開に追加され、[Create New VPN Deployment] ポップアップ ウィンドウがもう一度表示されます。

ステップ 12　[Leaf Nodes] の隣の追加アイコン（ ）クリックします。

[Add Leaf Node] ポップアップ ウィンドウが表示されます。

ステップ 13　リーフ ノードを完了するには、手順 7～10 を繰り返します。これにより、ハブ ノードと同じオプションが設定されます。

ステップ 14　[Save] をクリックします。

リーフ ノードが展開に追加され、[Create New VPN Deployment] ポップアップ ウィンドウがもう一度表示されます。

ステップ 15　[Save] をクリックして展開の設定を終了すると、[VPN] ページがもう一度表示されます。

内容を反映させるには、展開を適用する必要があることに注意してください。VPN 展開の適用（10-15 ページ）を参照してください。

メッシュ VPN 展開の設定

ライセンス： VPN

サポートされるデバイス： シリーズ 3

メッシュ VPN 展開を設定する場合は、VPN のグループを定義して、特定のエンドポイント セットに任意の 2 つのポイントをリンクさせます。詳細については、メッシュ VPN 展開について（10-4 ページ）を参照してください。

次に、展開で指定できるオプションについて示します。

名前

展開に一意の名前を指定します。

タイプ

メッシュ型の展開を設定するには、[Mesh] をクリックします。

Pre-shared Key

認証に対して一意の事前共有キーを定義します。

デバイス

展開のエンドポイントとして、デバイス スタックやクラスタなどの管理対象デバイスを選択できます。使用しているDefense Centerで管理されていないCiscoの管理対象デバイスの場合は、[Other] を選択し、エンドポイントの IP アドレスを指定します。

Virtual Router

エンドポイントとして管理対象デバイスを選択した場合は、選択したデバイスに適用されている仮想ルータを選択します。複数のエンドポイントに同じ仮想ルータを選択することはできません。

インターフェイス

エンドポイントとして管理対象デバイスを選択した場合は、選択した仮想ルータに割り当てられているルーテッド インターフェイスを選択します。

IP Address

- エンドポイントとして管理対象デバイスを選択した場合は、選択したルーテッド インターフェイスに割り当てられている IP アドレスを選択します。
- 管理対象デバイスがデバイス クラスタの場合は、SFRP の IP アドレスのリストからのみ選択できます。
- 選択した管理対象デバイスがDefense Centerで管理されて**いない**場合は、エンドポイントに IP アドレスを指定します。

Protected Networks

暗号化された展開でネットワークを指定します。各ネットワークに対して CIDR ブロックでサブネットを入力します。IKE バージョン 1 は、保護された単一のネットワークのみサポートしています。

VPN エンドポイントは同じ IP アドレスを持つことはできません。また、VPN エンドポイント ペアの保護されたネットワークは重複することはできないことに注意してください。エンドポイントについて保護されたネットワークのリストに 1 つ以上の IPv4 または IPv6 エントリが含まれている場合、他のエンドポイントの保護されたネットワークは、同じタイプ（IPv4 または IPv6）のエントリを少なくとも 1 つ持っていることが必要です。このようなエントリを持っていない場合、他のエンドポイントの IP アドレスが同じタイプであること、および保護されたネットワーク内でエントリが重複しないことが必要です（IPv4 については /32 CIDR アドレスを使用し、IPv6 については /128 CIDR アドレス ブロックを使用します）。これらの両方のチェックに失敗すると、エンドポイントのペアは機能しません。

Internal IP

エンドポイントが、ネットワーク アドレス変換を備えたファイアウォールの背後に配置されている場合は、このチェック ボックスをオンにします。

Public IP

[Internal IP] を選択した場合は、ファイアウォールに対してパブリック IP アドレスを指定します。エンドポイントが応答側の場合は、この値を指定する必要があります。

Public IKE Port

[Internal IP] を選択した場合は、内部のエンドポイントにポート転送されているファイアウォール上の UDP ポートに対して、1～65535 の数値を指定します。エンドポイントが応答側で、転送されているファイアウォール上のポートが 500 または 4500 ではない場合、この値を指定する必要があります。

ヒント　既存のメッシュ型の展開を編集するには、展開の隣にある編集アイコン（）をクリックします。展開を最初に保存した後で、展開のタイプを編集することはできません。展開のタイプを変更するには、展開を削除してから新しい展開を作成する必要があります。2 人のユーザが同じ展開について同時に編集**してはいけません**。ただし、Web インターフェイスでは同時編集を防止していないことに注意してください。

メッシュ VPN 展開を設定する方法

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [VPN] を選択します。

[VPN] ページが表示されます。

ステップ 2　[Add] をクリックします。

[Create New VPN Deployment] ポップアップ ウィンドウが表示されます。

ステップ 3　展開に一意の [Name] を指定します。

スペースや特殊文字を含めて、印刷可能なすべての文字を使用できます。

ステップ 4　[Type] を指定して [Mesh] をクリックします。

ステップ 5　展開に一意の [Pre-shared Key] を指定します。

ステップ 6　[Nodes] の隣の追加アイコン（）をクリックします。

[Add Endpoint] ポップアップ ウィンドウが表示されます。

ステップ 7　この項で説明したとおりに、VPN 展開を設定します。

ステップ 8　[Protected Networks] の隣の追加アイコン（）クリックします。

[Add Network] ポップアップ ウィンドウが表示されます。

ステップ 9　保護されたネットワークの CIDR ブロックを入力します。

ステップ 10　[OK] をクリックします。

保護されたネットワークが追加されます。

ステップ 11　[Save] をクリックします。

エンドポイントが展開に追加され、[Create New VPN Deployment] ポップアップ ウィンドウがもう一度表示されます。

ステップ 12　エンドポイントをさらに追加するには、手順 6～11 を繰り返します。

ステップ 13　[Save] をクリックして展開の設定を終了すると、[VPN] ページがもう一度表示されます。

内容を反映させるには、展開を適用する必要があることに注意してください。VPN 展開の適用（10-15 ページ）を参照してください。

高度な VPN 展開を設定する方法

ライセンス：VPN

サポートされるデバイス：シリーズ 3

VPN の展開には、展開内の VPN で共有できる一般的な設定がいくつか含まれています。各 VPN では、デフォルトの設定を使用するか、またはそのデフォルトの設定を上書きすることができます。通常、詳細設定はほとんど、あるいはまったく変更する必要がありません。詳細設定は導入環境ごとに異なります。

次に、展開で指定できる高度なオプションについて示します。

Other Algorithm Allowed

[Algorithm] リストに記載されていないものの、リモート ピアで提案されているアルゴリズムに対して自動ネゴシエーションを有効にするには、このチェック ボックスをオンにします。

アルゴリズム

展開内でデータをセキュアにするための、フェーズ 1 とフェーズ 2 のアルゴリズムの提案を指定します。両方のフェーズに対して、[Cipher]、[Hash]、および [Diffie-Hellman]（[DH]）グループ認証のメッセージを選択します。

IKE Life Time

IKE SA の最大のネゴシエーション間隔に対して数値を指定し、時間単位を選択します。最低 15 分、最大 30 日まで指定できます。

IKE v2

システムで IKE バージョン 2 を使用する場合は、このチェック ボックスを選択します。このバージョンでは、スター型の展開と保護された複数のネットワークをサポートしています。

Life Time

SA の最大の再ネゴシエーション間隔に対して数値を指定し、時間単位を選択します。最低 5 分、最大 24 時間まで指定できます。

Life Packets

有効期間が終了する前に、IPsec SA を介して伝送できるパケット数を指定します。0～18446744073709551615 の整数を使用できます。

Life Bytes

有効期間が終了する前に、IPsec SA を介して伝送できるバイト数を指定します。0～18446744073709551615 の整数を使用できます。

AH

システムで、保護されるデータに対して認証見出しのセキュリティ プロトコルを使用することを指定するには、このチェック ボックスをオンにします。暗号化サービス ペイロード（ESP）プロトコルを使用する場合は、このチェック ボックスをオフにします。各プロトコルを使用する場合のガイダンスについては、IPSec について（10-1 ページ）を参照してください。

高度な VPN 展開を設定する方法

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [VPN] を選択します。

[VPN] ページが表示されます。

ステップ 2　[Add] をクリックします。

[Create New VPN Deployment] ポップアップ ウィンドウが表示されます。

ステップ 3　[Advanced] タブをクリックします。

ステップ 4　この項で説明したとおりに、高度な設定を行います。

ステップ 5　[Algorithms] の隣の追加アイコン（  ）をクリックします。

[Add IKE Algorithm Proposal] ポップアップ ウィンドウが表示されます。

ステップ 6　両方のフェーズに対して、[Cipher]、[Hash]、および [Diffie-Hellman]（[DH]）グループ認証のメッセージを選択します。

ステップ 7　[OK] をクリックします。

IKE アルゴリズムの提案が追加されます。

ステップ 8　[Save] をクリックします。

変更が保存され、[VPN] ページが表示されます。

内容を反映させるには、展開を適用する必要があることに注意してください。VPN 展開の適用（10-15 ページ）を参照してください。

VPN 展開の適用

ライセンス：VPN

サポートされるデバイス：シリーズ 3

VPN 展開に対して設定または変更した後は、1 つ以上のデバイスに展開を適用して、展開に指定した設定を実装する必要があります。

注意　VPN 展開を追加または変更すると、Snort プロセスが再開され、構成変更を適用する際、一時的にトラフィック検査が中断されます。この検査中にシステムがトラフィックをドロップするか、検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、「Snort の再開によるトラフィックへの影響（1-9 ページ）」を参照してください。

VPN 展開を適用する方法

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [VPN] を選択します。

[VPN] ページが表示されます。

ステップ 2　適用する VPN 展開の隣の適用アイコン（  ）をクリックします。

ステップ 3　プロンプトが表示されたら、[Yes] をクリックします。

VPN 展開が適用されます。

ヒント　オプションで、[Apply VPN deployment] ダイアログ ボックスから [View Changes] をクリックします。新しいブラウザのウィンドウに [VPN Comparison View] ページが表示されます。詳細については、VPN 展開の比較ビューの使用（10-18 ページ）を参照してください。

ステップ 4　[OK] をクリックします。

[VPN] ページに戻ります。

VPN 展開のステータスの表示

ライセンス： VPN

サポートされるデバイス： シリーズ 3

VPN 展開を設定した後で、設定した VPN トンネルのステータスを表示できます。[VPN] ページに、適用されたそれぞれの VPN 展開に対するステータス アイコンが表示されます。

- （  ）アイコンは、すべての VPN エンドポイントが稼動していることを表します。
- （  ）アイコンは、すべての VPN エンドポイントが停止していることを表します。
- （）アイコンは、稼動しているエンドポイントと停止しているエンドポイントがあることを表します。

ステータス アイコンをクリックして、展開のステータス、および展開内のエンドポイントに関する基本情報（エンドポイント名や IP アドレスなど）を表示することができます。VPN ステータスは、毎分、または（エンドポイントが停止した、または稼動したなど）ステータスの変更が生じた場合に更新されます。

VPN のステータスを表示する方法

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [VPN] を選択します。

[VPN] ページが表示されます。

ステップ 2　ステータスを表示する展開の隣にある、VPN ステータス アイコンをクリックします。

[VPN Status] ポップアップ ウィンドウが表示されます。

ステップ 3　[OK] をクリックして [VPN] ページに戻ります。

VPN の統計およびログの表示

ライセンス：VPN

サポートされるデバイス：シリーズ 3

VPN 展開を設定した後で、設定した VPN トンネルを通過するデータの統計を表示することができます。また、各エンドポイントについて最新の VPN システムと IKE ログを表示することができます。

システムには、次の統計情報が表示されます。

エンドポイント

VPN エンドポイントとして指定されたルーテッド インターフェイスおよび IP アドレスへのデバイス パス。

Status（ステータス）

VPN 接続の状態（稼動または停止のどちらか）。

Protocol

暗号化で使用されるプロトコル（ESP または AH）。

Packets Received

IPsec SA ネゴシエーション中に VPN トンネルが受信する、インターフェイスあたりのパケット数。

Packets Forwarded

IPsec SA ネゴシエーション中に VPN トンネルが送信する、インターフェイスあたりのパケット数。

受信バイト数

IPsec SA ネゴシエーション中に VPN トンネルが受信する、インターフェイスあたりのバイト数。

Bytes Forwarded

IPsec SA ネゴシエーション中に VPN トンネルが送信する、インターフェイスあたりのバイト数。

Time Created

VPN 接続が作成された日時。

Time Last Used

ユーザが最後に VPN 接続を開始した時間。

NAT Traversal

[Yes] が表示されている場合、ネットワーク アドレス変換を備えたデバイスの背後に少なくとも 1 つの VPN エンドポイントが存在します。

IKE State

IKE SA の状態（接続、確立、削除、または廃棄）。

IKE Event

IKE SA イベント（再認証、またはキー再生成）。

IKE Event Time

次のイベントが発生する時間（秒）。

IKE Algorithm

VPN 展開で使用されている IKE アルゴリズム。

IPSec State

IPSec SA の状態（インストール中、インストール済み、更新中、キー再生成、削除、および廃棄）。

IPSec Event

IPSec SA イベントがキーを再生成するタイミングの通知。

IPSec Event Time

次のイベントが発生するまでの時間（秒）。

IPSec Algorithm

VPN 展開で使用されている IPSec アルゴリズム。

VPN の統計情報を表示する方法

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [VPN] を選択します。

[VPN] ページが表示されます。

ステップ 2　VPN の統計情報を表示する展開の隣にある、VPN ステータス アイコンをクリックします。

[VPN Status] ポップアップ ウィンドウが表示されます。

ステップ 3　統計情報の表示アイコン（  ）をクリックします。

[VPN Statistics] ポップアップ ウィンドウが表示されます。

ステップ 4　[Refresh] をクリックして、VPN の統計情報を更新することもできます。

ステップ 5　[View Recent Log] をクリックして、各エンドポイントの最新のデータ ログを表示することもできます。

クラスタ化されたデバイスおよびスタック デバイスのログを表示するには、アクティブ/プライマリ、またはバックアップ/セカンダリのいずれかのデバイスへのリンクを選択します。

VPN 展開の比較ビューの使用

ライセンス： VPN

サポートされるデバイス： シリーズ 3

VPN 展開の比較ビューを使用して、展開を適用する前に、展開に対して行った変更を表示することができます。レポートでは、現在の展開と提案された展開の違いがすべて表示されます。これにより、設定の潜在的なエラーを検出することができます。

比較ビューには 2 つの展開が左右に分かれて表示され、比較ビューの両側のタイトル バーには、それぞれの展開が名前で識別されて示されます。展開名とともに、最後に変更した時間と、最後に変更したユーザが表示されます。

2 つの展開の相違は、次のように強調されます。

- 青は、2 つの展開において強調された設定が異なっていることを表し、相違点は赤で示されています。
- 緑は、強調された設定が一方展開に存在し、他方の設定にはないことを表します。

次の表に、実行できる操作を記載します。

表 10-2　　VPN 展開の比較ビューの操作

目的	操作
変更に個別にナビゲートする	タイトル バーの上の [Previous] または [Next] をクリックします。 左側と右側の間にある二重矢印アイコン（）が移動し、表示している違いを示す [Difference] 番号が変わります。
展開の比較レポートを生成する	[Comparison Report] をクリックします。 展開の比較レポートでは、2 つのポリシー間の違いのみが示された PDF ドキュメントが作成されます。

NAT ポリシーの使用

ネットワーク アドレス変換（NAT）ポリシーは、システムがネットワーク アドレス変換を使用してルーティングを達成する方法を定めます。1 つ以上の NAT ポリシーを設定して、1 つ以上の管理対象デバイスに適用できます。各デバイスに同時に適用できるポリシーは 1 つだけです。

ポリシーに NAT ルールを追加して、システムがネットワーク アドレス変換を処理する方法を制御します。各ルールは、変換する特定のトラフィックを識別する、条件のセットを含みます。次のタイプのルールを作成できます。

- スタティック。宛先ネットワークと任意選択のポートおよびプロトコルで 1 対 1 変換を提供します。
- ダイナミック IP。多対多の送信元ネットワークを変換しますが、ポートおよびプロトコルを維持します
- ダイナミック IP およびポート。多対 1 または多対多の送信元ネットワークとポートおよびプロトコルを変換します。

システムはダイナミック変換を検査する前に、スタティック変換に対してトラフィックを照合します。次に、トラフィックはダイナミック NAT ルールに対して順番に照合されます。最初に一致したルールによってトラフィックが処理されます。詳細については、「NAT ポリシー内のルールの編成（11-6 ページ）」を参照してください。

展開にアクセス コントロール ポリシーが存在する場合、システムはアクセス制御を通過するまでトラフィックを変換しません。

アプライアンスで NAT ポリシーを設定および適用するには、適用先の各管理対象デバイスで Control ライセンスが有効になっている必要があります。また、NAT ポリシーを適用できるのは、仮想ルータまたはハイブリッド インターフェイスが設定された シリーズ 3 デバイスのみです。

NAT ポリシーを設定および展開した後、管理対象デバイスのコマンドライン インターフェイス（CLI）を使用して、展開のトラブルシューティングを行うことができます。CLI には設定、ルール定義、およびアクティブな変換という 3 種類の NAT 情報が表示されます。詳細については、「コマンドライン リファレンス（D-1 ページ）」を参照してください。

NAT ポリシーの作成および管理の詳細については、次の項を参照してください。

NAT ポリシーの計画と実装

ライセンス： すべて

特定のネットワーク ニーズを管理するためにさまざまな方法で NAT ポリシーを設定できます。この項では、NAT ポリシーを展開する方法の一部について説明します。

注意　クラスタ構成で、NAT 変換により影響を受けるすべてのネットワークがプライベートの場合、クラスタ デバイスのスタティック NAT ルールに対して、個別のピア インターフェイスのみを選択します。パブリック ネットワークとプライベート ネットワーク間のトラフィックに影響するスタティック NAT ルールに対してこの設定を使用**しない**でください。

NAT を設定して、内部サーバを外部ネットワークに公開できます。この設定では、外部 IP アドレスから内部 IP アドレスへのスタティック変換を定義するため、システムはネットワーク外部から内部サーバにアクセスできます。サーバに送信されるトラフィックは、外部 IP アドレスまたは IP アドレスとポートを対象とし、内部 IP アドレスまたは IP アドレスとポートに変換されます。サーバからのリターン トラフィックは、外部アドレスに再度変換されます。

NAT を設定して、内部ホストまたはサーバが外部アプリケーションに接続することを許可できます。この設定では、内部アドレスから外部アドレスへのスタティック変換を定義します。この定義により、内部ホストまたはサーバは、内部ホストまたはサーバが特定の IP アドレスおよびポートを持っていると予期する外部アプリケーションへの接続を開始できます。したがって、システムは内部ホストまたはサーバのアドレスを動的に割り当てることはできません。

NAT を設定して、IP アドレスのブロックを使用することにより、外部ネットワークからプライベート ネットワーク アドレスを隠すことができます。これは内部ネットワーク アドレスをマスクする場合、内部ネットワークのニーズを満たす十分な外部 IP アドレスがをある場合に便利です。この設定では、すべての発信トラフィックの送信元 IP アドレスを、外部に面する IP アドレスのうち未使用の IP アドレスに自動的に変換するダイナミック変換を作成します。

NAT を設定して、IP アドレスおよびポート変換の限定的なブロックを使用することにより、外部ネットワークからプライベート ネットワーク アドレスを隠すことができます。これは内部ネットワーク アドレスをマスクする場合で、内部ネットワークのニーズを満たす十分な外部 IP アドレスがない場合に便利です。この設定では、発信トラフィックの送信元 IP アドレスとポートを、外部に面する IP アドレスのうち未使用の IP アドレスとポートに自動的に変換するダイナミック変換を作成します。

NAT ポリシーの設定

ライセンス： Control

サポートされるデバイス： シリーズ 3

NAT ポリシーを設定するには、ポリシーに一意の名前を付け、ポリシーを適用するデバイスつまり *ターゲット*を特定する必要があります。また、NAT ルールを追加、編集、削除、有効化、および無効化することができます。NAT ポリシーを作成または変更した後、ターゲット デバイスのすべてまたは一部にポリシーを適用できます。

スタンドアロン デバイスと同様に、NAT ポリシーをクラスタ スタックを含むデバイス クラスタに適用できます。ただし、個別のクラスタ デバイスまたはクラスタ全体でインターフェイスのスタティック NAT ルールを定義し、送信元ゾーン内でインターフェイスを使用できます。ダイナミック ルールの場合、送信元ゾーンまたは宛先ゾーンでクラスタ全体のインターフェイスのみを使用できます。

注意　クラスタ構成で、NAT 変換により影響を受けるすべてのネットワークがプライベートの場合、クラスタ デバイスのスタティック NAT ルールに対して、個別のピア インターフェイスのみを選択します。パブリック ネットワークとプライベート ネットワーク間のトラフィックに影響するスタティック NAT ルールに対してこの設定を使用**しない**でください。

HA リンク インターフェイスが確立されていないデバイス クラスタでダイナミック NAT を設定した場合、両方のクラスタ デバイスは別々にダイナミック NAT エントリを割り当て、システムはデバイス間でエントリを同期できません。詳細については、「HA リンク インターフェイスの設定（4-68 ページ）」を参照してください。

スタンドアロン デバイスと同様に、NAT ポリシーをデバイス スタックに適用できます。NAT ポリシーに含まれ、スタックのメンバーであるセカンダリ デバイスのインターフェイスに関連付けられているルールを持ったデバイスからデバイス スタックを確立した場合、セカンダリ デバイスのインターフェイスは NAT ポリシーに残ります。インターフェイスを持つポリシーを保存および適用できますが、ルールは変換を実現しません。詳細については、「スタックに含まれるデバイスの管理（4-46 ページ）」を参照してください。

次の表は、NAT ポリシーの [Edit] ページで実行可能な設定アクションを示します。

表 11-1　NAT ポリシーの設定アクション

目的	操作
ポリシーの名前または説明を変更する	[Name] フィールドまたは [Description] フィールドをクリックして、必要に応じて文字を削除し、新しい名前または説明を入力します。
ポリシーの適用対象を管理する	詳細については、NAT ポリシー ターゲットの管理（11-4 ページ）を参照してください。
ポリシーの変更を保存する	[Save] をクリックします。
ポリシーを保存し、適用する	[Save and Apply] をクリックします。詳細については、「NAT ポリシーの適用（11-15 ページ）」を参照してください。
ポリシーの変更をキャンセルする	[Cancel] をクリックします。変更を行った場合は、次に [OK] をクリックします。
ポリシーにルールを追加する	[Add Rule] をクリックします。詳細については、「NAT ルールの作成と編集（11-17 ページ）」を参照してください。 **ヒント**　既存のルールを右クリックし、[Insert new rule] を選択することもできます。
既存のルールを編集する	ルールの横にある編集アイコン（  ）をクリックします。詳細については、「NAT ルールの作成と編集（11-17 ページ）」を参照してください。 **ヒント**　ルールを右クリックして、[Edit] を選択することもできます。
ルールを削除する	ルールの横にある削除アイコン（  ）をクリックし、[OK] をクリックします。 **ヒント**　1 つ以上のルールを選択して削除するには、選択したルールの行の空白部分を右クリックし、[Delete] を選択して [OK] をクリックします。

表 11-1　NAT ポリシーの設定アクション（続き）

目的	操作
既存のルールを有効または無効にする	選択したルールを右クリックして [State] を選択した後、[Disable] または [Enable] を選択します。無効なルールはグレーで表示され、ルール名の下に [(disabled)] というマークが付きます。
特定のルール属性の設定ページを表示する	ルールの行で、該当する条件のカラムに示されている名前、値、またはアイコンをクリックします。たとえば、[Source Network] 列の名前または値をクリックすると、選択したルールの [Source Network] ページが表示されます。詳細については、「NAT ルールのさまざまな条件タイプの使用（11-26 ページ）」を参照してください。

NAT ポリシー ターゲットの管理

ライセンス： Control

サポートされるデバイス： シリーズ 3

NAT ポリシーを適用するには、その前に、ポリシーを適用するデバイス スタック、クラスタ、またはグループなどの管理対象デバイスを識別する必要があります。ポリシーを適用する管理対象デバイスは、ポリシーを作成または編集する際に特定できます。使用可能なデバイス、スタック、およびクラスタのリストを検索して、選択したデバイスのリストに追加できます。また、選択したデバイスをドラッグ アンド ドロップしたり、2 つのリスト間のボタンを使用してデバイスを追加したりすることもできます。

異なるバージョンの FireSIGHT システムを実行中のスタック デバイスをターゲットにすることはできません（たとえば、デバイスのいずれかでのアップグレードが失敗します）。詳細については、「スタックに含まれるデバイスの管理（4-46 ページ）」を参照してください。

次の表では、対象のデバイスを管理する場合に実行可能な操作の概要を説明しています。

表 11-2　対象のデバイス管理アクション

目的	操作
使用可能なデバイス、スタック、およびクラスタのリストを検索する	検索フィールド内をクリックし、検索文字列を入力します。検索文字列を入力すると、デバイスのリストが更新されて、検索文字列に一致するデバイス名が表示されます。
使用可能なデバイスの検索をクリアする	検索フィールドのクリア アイコン（ ✖ ）をクリックします。
選択されているターゲットのリストに追加するための使用可能なデバイス、スタック、またはクラスタを選択する	デバイス名をクリックします。複数のデバイスを選択するには、Ctrl キーまたは Shift キーを押しながらクリックします。 **ヒント**　使用可能なデバイスを右クリックして、[Select All] をクリックすることもできます。
選択したデバイス、スタック、またはクラスタを追加する	[Add to Policy] をクリックします。 **ヒント**　選択済みデバイスのリストにドラッグ アンド ドロップするという方法もあります。

表 11-2　対象のデバイス管理アクション（続き）

目的	操作
[Selected Devices] リストから単一のデバイス、スタック、またはクラスタを削除する	デバイスの横にある削除アイコン（ ）をクリックします。 **ヒント**　デバイスを右クリックして、[Delete] を選択することもできます。
選択済みデバイスのリストから複数のデバイスを削除する	Ctrl キーまたは Shift キーを押しながら複数のデバイスをクリックして選択したら、選択したデバイスの行を右クリックして強調表示し、次に [Delete Selected] をクリックします。
設定を保存する	[Save] をクリックします。
変更を保存せずに設定を廃棄する	[Cancel] をクリックします。

次の手順では、対象デバイスを管理するための NAT ポリシーの設定方法について説明します。NAT ポリシーを編集するための詳細な手順については NAT ポリシーの編集（11-10 ページ）を参照してください。

NAT ポリシーで対象のデバイスを管理する方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [NAT] を選択します。

[NAT] ページが表示されます。

ステップ 2　設定する NAT ポリシーの横にある編集アイコン（ ）をクリックします。

[NAT Policy Editor] ページが表示されます。

ステップ 3　[Targets] タブをクリックします。

[Targets] ページが表示されます。

ステップ 4　（任意）[Available Devices] リストの上にある [Search] プロンプトをクリックして、名前を入力します。

検索文字列を入力すると、リストが更新されて、検索文字列に一致するデバイスが表示されます。クリア アイコン（ ）をクリックすることで、リストをクリアできます。

ステップ 5　追加するデバイス、スタック、クラスタ、またはデバイス グループをクリックします。複数のデバイスを選択するには、Ctrl キーまたは Shift キーを使用します。

ヒント　使用可能なデバイスを右クリックして、[Select All] をクリックすることもできます。

ステップ 6　[Add to Policy] をクリックします。

選択したデバイスが追加されます。

ヒント　ドラッグ アンド ドロップしてデバイスを追加することもできます。

ステップ 7　(任意)削除アイコン( )をクリックして、選択済みデバイスのリストからデバイスを削除します。または、Ctrl キーまたは Shift キーを押しながら複数のデバイスをクリックして選択し、選択したデバイスを右クリックして [Delete Selected] を選択します。

ステップ 8　[Save] をクリックして、設定を保存します。または、[Cancel] をクリックして、設定を廃棄します。

NAT ポリシー内のルールの編成

ライセンス: すべて

NAT ポリシー の [Edit] ページにはスタティックな NAT ルールとダイナミックな NAT ルールが別々に表示されます。スタティック ルールは名前のアルファベット順に並べ替えられ、表示順序を変更できません。同一の照合値を持つスタティック ルールは作成できません。システムの照合では、ダイナミック変換を検査する前に、スタティック変換を検査します。

ダイナミック ルールは番号順に処理されます。各ダイナミック ルールの番号位置は、ページ左側のルールの横に表示されます。ダイナミック ルールは移動または挿入したり、ルールの順序を変更したりすることができます。たとえば、ダイナミック ルール 10 をダイナミック ルール 3 の下に移動した場合、ルール 10 がルール 4 になり、後に続くすべての番号が順次繰り上がります。

システムはポリシーの [Edit] ページ上のルールの番号順にパケットとダイナミック ルールを比較するので、ダイナミック ルールの位置は重要です。パケットがダイナミック ルールのすべての条件を満たすと、システムはパケットにそのルール条件を適用し、そのパケットに対する後続の規則はすべて無視します。

オプションで、ダイナミック ルールを追加または編集する際、ダイナミック ルールの番号の位置を指定できます。新しいダイナミック ルールを追加する前にダイナミック ルールを強調表示して、強調表示したルールの下に新しいルールを挿入することもできます。NAT ルールの作成と編集(11-17 ページ)を参照してください。

ルールの行内の空白部分をクリックすることにより、1 つ以上のダイナミック ルールを選択できます。選択したダイナミック ルールを新しい場所にドラッグ アンド ドロップできます。これにより、移動したルールと後続のすべてのルールの位置が変更されます。

選択したルールを既存のルールの上または下にカット アンド ペーストできます。スタティック ルールは [Static Translations] リストにのみ、ダイナミック ルールは [Dynamic Translations] リストにのみ貼り付けることができます。また、選択したルールを削除したり、既存のルール リスト内の任意の場所に新しいルールを挿入したりすることもできます。

注　スタティック ルールはコピーできますが、切り取ることはできません。

先行ルールが優先して適用されるために決して一致することがないルールを示す、説明的な警告メッセージを表示することもできます。

展開にアクセス コントロール ポリシーが存在する場合、システムはアクセス制御を通過するまでトラフィックを変換しません。

次の表に、ルールを編成するために実行できる操作を要約します。

表 11-3　NAT ルール編成アクション

目的	操作
ルールを選択する	ルールの行の空白部分をクリックします。複数のルールを選択するには、Ctrl キーまたは Shift キーを押しながらクリックします。選択したルールが強調表示されます。
ルールの選択をクリアする	ページの右下にある再ロード アイコン（）をクリックします。個別のルールをクリアするには、Ctrl キーを押しながら各ルールの行内の空白部分をクリックします。
選択したルールを切り取る、またはコピーする	選択したルールの行の空白部分を右クリックし、[Cut] または [Copy] を選択します。 **ヒント**　スタティック ルールはコピーできますが、切り取ることはできません。
切り取ったルールまたはコピーしたルールをルール リストに貼り付ける	選択したルールを貼り付けるルールの行の空白部分を右クリックし、[Paste above] または [Paste below] を選択します。 **ヒント**　スタティック ルールは [Static Translations] リストにのみ、ダイナミック ルールは [Dynamic Translations] リストにのみ貼り付けることができます。
選択したルールを移動する	選択したルールを新しい場所の下にドラッグ アンド ドロップします。ドラッグしたときにポインタの上に青い横線が表示される場所が移動先です。
ルールを削除する	ルールの横にある削除アイコン（）をクリックし、[OK] をクリックします。 **ヒント**　選択したルールの行の空白部分を右クリックして [Delete] を選択した後、[OK] をクリックして、選択した 1 つ以上のルールを削除するという方法もあります。
警告を表示する	[Show Warnings] をクリックします。NAT ルールの警告とエラーの操作（11-7 ページ）を参照してください。

NAT ルールの警告とエラーの操作

ライセンス：すべて

NAT ルールの条件が後続のルールによるトラフィックの照合をプリエンプション処理する場合があります。どのようなタイプのルール条件でも、後続のルールを回避する可能性があります。

あるルールとその後続のルールがまったく同じで、いずれもすべて同じ条件が設定されている場合、後続のルールは回避されます。いずれかの条件が異なっていた場合、後続のルールはプリエンプション処理されません。

次の表に、警告の表示および消去を行うために実行可能なアクションを示します。

表 11-4　プリエンプション処理されたルールの警告アクション

目的	操作
警告を表示する	[Show Warnings] をクリックします。ページが更新され、プリエンプション処理された各ルールの横に警告アイコン（）が表示されます。
ルールの警告を表示する	ルールの横の警告アイコン（）の上にポインタを移動します。ルールをプリエンプション処理するルールを示すメッセージが表示されます。
警告を消去する	[Hide Warnings] をクリックします。ページが更新され、警告が消えます。 **ヒント**　ルールの追加または編集など、ページを更新する任意のアクションの実行、またはリロード アイコン（）のクリックでも、警告は消えます。

NAT ポリシーの適用が失敗するルールを作成した場合、ルールの横にエラー アイコン( )が表示されます。スタティック ルールに矛盾がある場合、または現時点で無効となるポリシーで使用されるネットワーク オブジェクトを編集した場合、エラーが発生します。たとえば、IPv6 アドレスのみを使用するようにネットワーク オブジェクトを変更した結果、少なくとも 1 つのネットワークが必要な状況で、そのオブジェクトを使用するルールに有効なネットワークがなくなると、エラーが発生します。エラー アイコンは自動的に表示されます。[Show Warnings] をクリックする必要はありません。

NAT ポリシーの管理

ライセンス： Control

サポートされるデバイス： シリーズ 3

NAT ポリシーのページ（[Devices] > [NAT]）で、オプションの説明と次のステータス情報と共に、現在のすべての NAT ポリシーを名前別に表示できます。

- ターゲット デバイスに対してポリシーが最新の状態になっている（緑のテキスト）
- ターゲット デバイスに対してポリシーが失効している（赤のテキスト）

このページのオプションを使用して、ポリシーの比較、新しいポリシーの作成、ターゲット デバイスへのポリシーの適用、ポリシーのコピー、各ポリシーで最後に保存されたすべての設定を示すレポートの表示、およびポリシーの編集を行うことができます。

注　管理対象デバイスに NAT ポリシーを適用した後は、期限切れであってもポリシーを削除できません。その代わり、ルールを持たない NAT ポリシーを適用して、適用済みの NAT ルールを管理対象デバイスから削除する必要があります。

次の表に、NAT ポリシーのページでポリシーを管理するために実行可能なアクションについて説明します。

表 11-5　NAT ポリシー管理アクション

目的	操作
新しい NAT ポリシーを作成する	[New Policy] をクリックします。詳細については、「NAT ポリシーの作成（11-9 ページ）」を参照してください。
既存の NAT ポリシーの設定を変更する	編集アイコン( )をクリックします。詳細については、「NAT ポリシーの編集（11-10 ページ）」を参照してください。
ポリシーのターゲットであるすべてのデバイスに NAT ポリシーを適用する	ポリシー適用アイコン( )をクリックします。詳細については、「NAT ポリシーの適用（11-15 ページ）」を参照してください。
NAT ポリシーをコピーする	コピー アイコン( )をクリックします。詳細については、「NAT ポリシーのコピー（11-11 ページ）」を参照してください。
NAT ポリシーの現在の設定を示す PDF レポートを表示する	レポート アイコン( )をクリックします。詳細については、「NAT ポリシーの表示（11-11 ページ）」を参照してください。
NAT ポリシーを比較する	[Compare Policies] をクリックします。詳細については、「2 つの NAT ポリシーの比較（11-12 ページ）」を参照してください。

表 11-5　NAT ポリシー管理アクション（続き）

目的	操作
NAT ポリシーを削除する	削除アイコン（ ）をクリックして [OK] をクリックするか、または、ポリシーを削除しない場合は [Cancel] をクリックします。続行するかどうかを尋ねるプロンプトで、ポリシー内に別のユーザの未保存の変更が存在するかどうかも通知されます。 **注**　管理対象デバイスに NAT ポリシーを適用した後は、デバイスからそのポリシーを削除できません。その代わり、ルールを持たない NAT ポリシーを適用して、適用済みの NAT ルールを管理対象デバイスから削除する必要があります。また、どのターゲット デバイスでも、最後に適用されたポリシーは期限切れであっても削除できません。ポリシーを完全に削除する前に、それらのターゲットに異なるポリシーを適用する必要があります。

NAT ポリシーの作成

ライセンス：Control

サポートされるデバイス：シリーズ 3

新しい NAT ポリシーを作成する場合、少なくとも一意の名前を付ける必要があります。ポリシーの作成時にポリシー ターゲットを特定する必要はありませんが、ポリシーを適用する前には、この手順に実行する必要があります。NAT ポリシー ターゲットの管理（11-4 ページ）を参照してください。ルールを持たない NAT ポリシーをデバイスに適用すると、そのデバイスからすべての NAT ルールが削除されます。

NAT ポリシーを作成する方法：

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [NAT] を選択します。

[NAT] ページが表示されます。

ステップ 2　[New Policy] をクリックします。

[New NAT Policy] ポップアップ ウィンドウが表示されます。

ステップ 3　[Name] に一意のポリシー名を入力し、オプションで [Description] にポリシーの説明を入力します。

スペースや特殊文字を含めて、印刷可能なすべての文字を使用できます。

ステップ 4　[Available Devices] から、ポリシーを適用するデバイスを選択します。

複数のデバイスを選択するには、Ctrl キーまたは Shift キーを押しながらクリックするか、または右クリックをして [Select All] を選択します。表示されるデバイスを絞り込むには、[Search] フィールドに検索文字列を入力します。検索をクリアするには、クリア アイコン（ ）をクリックします。

ステップ 5　[Selected Devices] に、選択したデバイスを追加します。それには、クリックしてドラッグするか、[Add to Policy] をクリックします。

ステップ 6　[Save] をクリックします。

[NAT policy Edit] ページが表示されます。ルールの追加を含め、新しいポリシーの設定方法については、NAT ポリシーの編集（11-10 ページ）を参照してください。ポリシーを有効にするには適用する必要があることに注意してください。NAT ポリシーの適用（11-15 ページ）を参照してください。

NAT ポリシーの編集

ライセンス： Control

サポートされるデバイス： シリーズ 3

[NAT policy Edit] ページで、ポリシーを設定できます。詳細については、NAT ポリシーの設定（11-2 ページ）を参照してください。

設定を変更すると、変更がまだ保存されていないことを通知するメッセージが表示されます。変更を維持するには、[NAT policy Edit] ページを終了する前にポリシーを保存する必要があります。変更を保存しないでポリシーの [Edit] ページを終了しようとすると、変更がまだ保存されていないことを警告するメッセージが表示されます。この場合、変更を破棄してポリシーを終了するか、ポリシーの [Edit] ページに戻るかを選択できます。

セッションのプライバシーを保護するために、ポリシーの編集ページが非アクティブになってから 60 分後に、ポリシーの変更は廃棄され、NAT ページに戻ります。非アクティブの最初の 30 分後にメッセージが表示され、変更が廃棄されるまでの残り時間（分）が定期的に更新されます。ページで何らかの操作を行うとタイマーはリセットされます。

2 つのブラウザ ウィンドウで同じポリシーを編集しようとすると、新しいウィンドウで編集を再開するか、元のウィンドウでの変更を破棄して新しいウィンドウで編集を続けるか、または 2 番目のウィンドウをキャンセルしてポリシーの [Edit] ページに戻るかを選択するよう求めるプロンプトが出されます。

複数のユーザが同じポリシーを同時に編集する場合、各ユーザに対して、ポリシーの編集ページにメッセージが表示され、他のユーザによる未保存の変更があることが通知されます。変更を保存しようとするすべてのユーザに、変更を保存すると他のユーザの変更が上書きされることが警告されます。複数のユーザが同じポリシーを保存した場合は、最後に保存された変更が保持されます。

インターフェイスのタイプを、そのインターフェイスがあるデバイスを対象とする NAT ポリシーでの使用が無効なタイプに変更した場合、ポリシーはそのインターフェイスに削除済みのラベルを付けます。NAT ポリシーの [Save] をクリックすると、インターフェイスはポリシーから自動的に削除されます。

NAT ポリシーを編集する方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [NAT] を選択します。

[NAT] ページが表示されます。

ステップ 2　設定する NAT ポリシーの横にある編集アイコン（  ）をクリックします。

[NAT policy Edit] ページが表示されます。

ステップ 3　ポリシーを設定するには、NAT ポリシーの設定（11-2 ページ）で説明しているいずれかの操作を実行します。

ステップ 4　設定を保存または廃棄します。次の選択肢があります。

- 変更を保存し、編集を続行する場合は、[Save] をクリックします。
- 変更を保存し、ポリシーを適用する場合は、[Save and Apply] をクリックします。NAT ポリシーの適用（11-15 ページ）を参照してください。

  変更を有効にするには、ポリシーを適用する必要があります。
- 変更を廃棄する場合は、[Cancel] をクリックし、プロンプトが出たら [OK] をクリックします。

  変更は廃棄され、[NAT] ページが表示されます。

NAT ポリシーのコピー

ライセンス： Control

サポートされるデバイス： シリーズ 3

NAT ポリシーをコピーして、名前を変更できます。ポリシーをコピーすると、そのポリシーのすべてのルールと設定がコピーされます。

NAT ポリシーをコピーする方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [NAT] を選択します。

[NAT] ページが表示されます。

ステップ 2　設定する NAT ポリシーの横にあるコピー アイコン（  ）をクリックします。

[Copy NAT Policy] ポップアップ ウィンドウが表示されます。

ステップ 3　[Name] に一意のポリシー名を入力します。

スペースや特殊文字を含めてすべての印刷可能な文字を使用できます。

ステップ 4　[OK] をクリックします。

コピーしたポリシーは [NAT] ページに名前のアルファベット順に表示されます。

NAT ポリシーの表示

ライセンス： Control

サポートされるデバイス： シリーズ 3

NAT ポリシー レポートは、特定の時点でのポリシーとルール設定の記録です。このレポートは、監査目的や、現行の設定を調べるために使用できます。

ヒント　また、ポリシーを現在適用されているポリシーまたは別のポリシーと比較する NAT 比較レポートを生成することもできます。詳細については、2 つの NAT ポリシーの比較（11-12 ページ）を参照してください。

NAT ポリシー レポートには、次の表で説明するセクションが含まれます。

表 11-6　NAT ポリシー レポートのセクション

セクション	説明
Title Page	ポリシー レポートの名前、ポリシーの最終変更日時、ポリシーの最終変更ユーザ名を示します。
目次	レポートの内容が記載されます。
Policy Information	ポリシーの名前と説明、ポリシーを最後に変更したユーザの名前、ポリシーが最後に変更された日時が記載されます。NAT ポリシーの編集（11-10 ページ）を参照してください。
Device Targets	ポリシーがターゲットとする管理対象デバイスがリストされます。NAT ポリシー ターゲットの管理（11-4 ページ）を参照してください。
ルール	ポリシーの各ルールのルール タイプと条件を示します。NAT ルールの作成と編集（11-17 ページ）を参照してください。
Referenced Objects	ポリシーで使用されているすべての個別オブジェクトとグループ オブジェクトの名前および設定を、オブジェクトが設定された条件のタイプ（ゾーン、ネットワーク、およびポート）別に示します。

NAT ポリシー レポートを表示する方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [NAT] を選択します。

[NAT] ページが表示されます。

ステップ 2　レポートの生成対象とするポリシーの横にあるレポート アイコン（  ）をクリックします。NAT ポリシー レポートを生成する前に、すべての変更を保存してください。保存された変更のみがレポートに表示されます。

システムによってレポートが生成されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。

2 つの NAT ポリシーの比較

ライセンス： Control

サポートされるデバイス： シリーズ 3

ポリシーの変更を確認するために、2 つの NAT ポリシーの違いを調べることができます。任意の 2 つのポリシーを比較することも、現在適用されているポリシーを別のポリシーと比較することもできます。オプションで、比較した後に PDF レポートを生成することで、2 つのポリシーの間の差異を記録できます。

ポリシーを比較するために使用できるツールは 2 つあります。

- 比較ビューは、2 つのポリシーを左右に並べて表示し、その差異のみを示します。比較ビューの左右のタイトル バーに、それぞれのポリシーの名前が示されます。ただし、[Running Configuration] を選択した場合、現在アクティブなポリシーは空白のバーで表されます。

  このツールを使用すると、Web インターフェイスで 2 つのポリシーを表示してそれらに移動するときに、差異を強調表示することができます。

- 比較レポートは、ポリシー レポートと同様の形式ですが、2 つのポリシーの間の差異だけが、PDF 形式で記録されます。

  これを使用して、ポリシーの比較の保存、コピー、出力、共有を行って、さらに検証することができます。

ポリシーの比較ツールの内容と使用方法の詳細については、次の項を参照してください。

- NAT ポリシー比較ビューの使用（11-13 ページ）
- NAT ポリシー比較レポートの使用（11-14 ページ）

NAT ポリシー比較ビューの使用

ライセンス： Control

サポートされるデバイス： シリーズ 3

比較ビューには、両方のポリシーが左右に並べて表示されます。それぞれのポリシーは、比較ビューの左右のタイトル バーに示される名前で特定されます。現在実行されている設定ではない 2 つのポリシーを比較する場合、最後に変更された日時とその変更を行ったユーザがポリシー名と共に表示されます。

2 つのポリシーの違いは、次のように強調表示されます。

- 青は、強調表示されている設定項目が 2 つのポリシー間で異なっていることを示し、異なっている部分は赤のテキストで表示されます。
- 緑色は強調表示された設定が一方のポリシーには存在するが、他方には存在しないことを示します。

次の表に、実行できる操作を記載します。

表 11-7　NAT ポリシー比較のビューのアクション

目的	操作
変更に個別にナビゲートする	タイトル バーの上の [Previous] または [Next] をクリックします。 左側と右側の間にある二重矢印アイコン（）が移動し、表示している違いを示す [Difference] 番号が変わります。
新しいポリシー比較ビューを生成する	[New Comparison] をクリックします。 [Select Comparison] ウィンドウが表示されます。詳細については、「NAT ポリシー比較レポートの使用（11-14 ページ）」を参照してください。
ポリシー比較レポートを生成する	[Comparison Report] をクリックします。 ポリシー比較レポートは、2 つのポリシーの間の差異だけをリストした PDF ドキュメントです。

NAT ポリシー比較レポートの使用

ライセンス： Control

サポートされるデバイス： シリーズ 3

NAT ポリシー比較レポートは、ポリシー比較ビューによって示される 2 つの NAT ポリシー間または 1 つのポリシーと現在適用されているポリシーの間のすべての差異を PDF 形式で表示する記録です。このレポートを使用することで、2 つのポリシー設定の間の違いをさらに調べ、調査結果を保存して共有できます。

アクセス可能な任意のポリシーに関して、比較ビューから NAT ポリシー比較レポートを生成できます。ポリシー レポートを生成する前に、必ずすべての変更を保存してください。レポートには、保存されている変更だけが表示されます。

ポリシー比較レポートの形式はポリシー レポートと同じですが、1 つだけ例外があります。ポリシー レポートはポリシーのすべての設定を含みますが、ポリシー比較レポートはポリシー間で異なる設定のみを示します。NAT ポリシー比較レポートには、NAT ポリシー レポートのセクションの表で説明しているセクションが含まれます。

2 つの NAT ポリシーを比較する方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [NAT] を選択します。

[NAT] ページが表示されます。

ステップ 2　[Compare Policies] をクリックします。

[Select Comparison] ウィンドウが表示されます。

ステップ 3　[Compare Against] ドロップダウンリストから、比較するタイプを次のように選択します。

- 異なる 2 つのポリシーを比較するには、[Other Policy] を選択します。

  ページが更新されて、[Policy A] と [Policy B] という 2 つのドロップダウンリストが表示されます。
- 2 つのリビジョンを比較するには、[Other Revision] を選択します。

  ページが更新され、[Policy]、[Revision A]、[Revision B] ドロップダウン リストが表示されます。
- 現在アクティブなポリシーと別のポリシーを比較するには、[Running Configuration] を選択します。

  ページが更新されて、[Target/Running Configuration A] と [Policy B] という 2 つのドロップダウンリストが表示されます。

ステップ 4　選択した比較タイプによって、次の選択肢があります。

- 2 つの異なるポリシーを比較する場合は、[Policy A] と [Policy B] ドロップダウン リストから比較するポリシーを選択します。
- 2 つの異なるリビジョンを比較する場合、[Revision A] ドロップダウン リストと [Revision B] ドロップダウン リストから比較するリビジョンを選択します。
- 実行中の設定を別のポリシーと比較する場合は、[Policy B] ドロップダウン リストから 2 番目のポリシーを選択します。

ステップ 5　ポリシー比較ビューを表示するには、[OK] をクリックします。

比較ビューが表示されます。

ステップ 6　オプションで、[Comparison Report] をクリックして、NAT ポリシー比較レポートを生成します。

NAT ポリシー比較レポートが表示されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。

NAT ポリシーの適用

ライセンス： Control

サポートされるデバイス： シリーズ 3

NAT ポリシーに変更を加えたら、ポリシーを 1 つ以上のデバイスに適用し、デバイスによって監視するネットワーク上に設定変更を実装する必要があります。ポリシーを適用するには、その前に、ポリシーを適用するターゲット デバイスを指定する必要があります。NAT ポリシー ターゲットの管理（11-4 ページ）を参照してください。

NAT ポリシーを適用する場合は、次の点に注意してください。

- Defense Centerでは複数の NAT ポリシーを設定および保持できますが、1 つのデバイスに一度に適用可能なポリシーは 1 つだけです。
- デバイスがいずれも複数のポリシーのターゲットであっても、2 つの異なる NAT ポリシーを異なるデバイスに適用できます。
- 複数の異なるバージョンの FireSIGHT システムを実行中のスタック デバイスに NAT ポリシーを適用することはできません（たとえば、一方のデバイスでアップグレードに失敗した場合など）。詳細については、「スタックに含まれるデバイスの管理（4-46 ページ）」を参照してください。
- 適用が保留されているポリシーがある場合、新しい NAT ポリシーを適用できません。
- NAT ポリシーのインターフェイスに影響するデバイス設定を適用すると、インターフェイスの変更を含め、デバイスの NAT ポリシーが再適用されます。ただし、ポリシーは DC で変更されず、インターフェイスにはエラー アイコン（）が表示されます。

注　空の NAT ポリシーを適用すると、デバイスからすべての NAT ルールが削除されます。

詳細については、次の項を参照してください。

- 完全な NAT ポリシーの適用（11-15 ページ）ではクイック適用オプションを使用して NAT ポリシーを適用する方法について説明します。
- 選択したポリシー設定の適用（11-16 ページ）では NAT ポリシー内の設定を選択して適用する方法について説明します。

完全な NAT ポリシーの適用

ライセンス： Control

サポートされるデバイス： シリーズ 3

NAT ポリシーはいつでも適用できます。NAT ポリシーを適用すると、関連するルール設定、オブジェクト、およびポリシーの変更もポリシーの対象となるデバイスに適用されます。ポップアップ ウィンドウを使用し、すべての変更を 1 つのクイック適用アクションとして適用できます。

完全な NAT ポリシーをクイック適用する方法:

アクセス: Admin/Network Admin

ステップ 1　[Devices] > [NAT] を選択します。

[NAT] ページが表示されます。

ステップ 2　適用するポリシーの横にある適用アイコン（）をクリックします。

[Apply NAT Rules] ポップアップ ウィンドウが表示されます。

または、ポリシーの [Edit] ページで [Save and Apply] をクリックするという方法もあります。NAT ポリシーの編集（11-10 ページ）を参照してください。

ステップ 3　[Apply All] をクリックします。

ポリシー適用タスクがキューに入れられます。[OK] をクリックして、[NAT] ページに戻ります。

ヒント　ポリシー適用タスクの進行状況は、[Task Status] ページ（[System] > [Monitoring] > [Task Status]）でモニタできます。

選択したポリシー設定の適用

ライセンス: Control

サポートされるデバイス: シリーズ 3

詳細なポリシー適用ページを使用して、NAT ポリシーおよび任意の指定ターゲット デバイスに変更を適用できます。詳細ページには、ポリシーのターゲットである各デバイスが表示され、デバイス別に NAT ポリシーを表す列が含まれます。期限切れの各ターゲット デバイスに対して、NAT ポリシーに変更を適用するかどうかを指定できます。

選択した NAT ポリシー設定を適用する方法:

アクセス: Admin/Network Admin

ステップ 1　[Devices] > [NAT] を選択します。

[NAT] ページが表示されます。

ステップ 2　適用するポリシーの横にある適用アイコン（）をクリックします。

[Apply NAT Rules] ポップアップ ウィンドウが表示されます。

または、ポリシーの [Edit] ページで [Save and Apply] をクリックするという方法もあります。NAT ポリシーの編集（11-10 ページ）を参照してください。

ステップ 3　[Details] をクリックします。

詳細な [Apply NAT Rules] ポップアップ ウィンドウが表示されます。

ヒント　[NAT] ページ（[Devices] > [NAT]）で、ポリシーの [Status] 列の期限切れメッセージをクリックして、ポップアップ ウィンドウを開くこともできます。

ステップ 4　デバイス名の横の [NAT policy] チェック ボックスをオンまたはオフにして、ターゲット デバイスに NAT ポリシーを適用するかどうかを指定します。

ステップ 5　[Apply Selected Configurations] をクリックします。

ポリシー適用タスクがキューに入れられます。[OK] をクリックして、[NAT] ページに戻ります。

ヒント　ポリシー適用タスクの進行状況は、[Task Status] ページ（[System] > [Monitoring] > [Task Status]）でモニタできます。

NAT ルールの作成と編集

ライセンス： Control

サポートされるデバイス： シリーズ 3

NAT ルールは次の働きを持つ設定および条件のセットです。

- ネットワーク トラフィックを限定する
- 条件に一致するトラフィックの変換方法を指定する

既存の NAT ポリシーから NAT ルールを作成および編集します。各ルールは 1 つのポリシーにのみ属します。

ルールの追加と編集は同様の Web インターフェイスで行います。ページの上部でルールの名前、状態、タイプ、および位置（ダイナミックの場合）を指定します。ページの左側のタブを使用して、条件を構築します。条件タイプごとに独自のタブがあります。

次のリストは、NAT ルールの設定可能なコンポーネントを示しています。

名前

各ルールに一意の名前を付けます。スタティック NAT ルールでは、最大 22 文字を使用します。ダイナミック NAT ルールでは、最大 30 文字を使用します。スペースや特殊文字（「:」は除く）など、印刷可能文字を使用できます。

Rule State

デフォルトでは、ルールが有効状態になります。ルールを無効にすると、変換用のネットワーク トラフィックの評価に使用されません。NAT ポリシーのルール リストを表示すると、無効なルールはグレー表示されますが、変更は可能です。

タイプ

ルールのタイプによって、ルールの条件に一致するトラフィックの処理方法が決まります。NAT ルールを作成および編集する際、設定可能なコンポーネントはルール タイプによって異なります。

ルール タイプとそれらが変換およびトラフィック フローに与える影響の詳細については、NAT ルール タイプについて（11-19 ページ）を参照してください。

Position（ダイナミック ルールのみ）

NAT ポリシーのダイナミック ルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で、NAT ルールを上から順にトラフィックと照合します。

ルールをポリシーに追加する際、参照ポイントとしてルール番号を使用し、特定のルールの**上**または**下**に配置することによって位置を指定します。既存のルールを編集するときには、同様の方法でルールを**移動**できます。詳細については、NAT ポリシー内のルールの編成（11-6 ページ）を参照してください。

条件

ルール条件は変換する特定のトラフィックを識別します。条件はセキュリティ ゾーン、ネットワーク、および転送プロトコルのポートなど、複数の属性を任意に組み合わせてトラフィックと照合できます。

条件の追加の詳細については、NAT ルール条件と条件のしくみについて（11-21 ページ）および NAT ルールのさまざまな条件タイプの使用（11-26 ページ）を参照してください。

NAT ルールを作成または編集する方法：

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [NAT] を選択します。

[NAT] ページが表示されます。

ステップ 2　ルールを追加する NAT ポリシーの横にある編集アイコン（  ）をクリックします。

[NAT policy Edit] ページが表示されます。

ステップ 3　次のように新しいルールを追加するか、既存のルールを編集します。

- 新しいルールを追加するには、[Add Rule] をクリックします。
- 既存のルールを編集するには、そのルールの横にある編集アイコン（  ）をクリックします。

[Add Rule] ページまたは [Editing Rule] ページが表示されます。

ヒント　右クリック コンテキスト メニューを使用して、さまざまなルール作成/管理操作を実行することができます（コンテキスト メニューの使用（2-5 ページ）を参照）。また、ルールをドラッグ アンド ドロップして順序を変更することもできます。

ステップ 4　前述の方法で、ルールのコンポーネントを設定します。次の設定をするか、デフォルト設定をそのまま使用することができます。

- ルールに一意の名前 [Name] を付ける必要があります。
- ルールを有効にするかどうか [Enabled] を指定します。
- ルール タイプを [Type] から選択します。
- ルールの位置（ダイナミック ルールのみ）を指定します。
- ルールの条件を設定します。

  スタティック ルールは元の宛先ネットワークを含む必要があります。

  ダイナミック ルールは変換された送信元ネットワークを含む必要があります。

ステップ 5　[Add] または [Save] をクリックします。

変更が保存されます。変更内容を有効にするには、NAT ポリシーを適用する必要があります。NAT ポリシーの適用（11-15 ページ）を参照してください。

NAT ルール タイプについて

ライセンス： すべて

すべての NAT ルールには次の働きを持つタイプが関連付けられています。

- ネットワーク トラフィックを限定する
- 条件に一致するトラフィックの変換方法を指定する

次に、NAT ルール タイプの概要を示します。

スタティック

スタティック ルールは宛先ネットワークと任意選択のポートおよびプロトコルで 1 対 1 変換を提供します。スタティック変換を設定する場合、送信元ゾーン、宛先ネットワーク、および宛先ポートを設定できます。宛先ゾーンまたは送信元ネットワークを設定できません。

元の宛先ネットワークを指定する**必要**があります。宛先ネットワークでは、単一の IP アドレスを含むネットワーク オブジェクトおよびグループを選択するか、または単一の IP アドレスを表すリテラル IP アドレスを入力することのみが可能です。元の宛先ネットワークと変換後の宛先ネットワークはそれぞれ 1 つのみ指定できます。

必要に応じて、元の宛先ポートと変換後の宛先ポートをそれぞれ 1 つ指定できます。元の宛先ポートを指定するには、その前に、元の宛先ネットワークを指定する必要があります。さらに、元の宛先ポートを指定しない場合は、変換後の宛先ポートを指定できません。また、変換後の値は、元の値のプロトコルと一致する必要があります。

注意　クラスタ デバイスのスタティック NAT に関して、NAT 変換で影響を受けるすべてのネットワークがプライベートの場合、個別のピア インターフェイスのみを選択します。パブリック ネットワークとプライベート ネットワーク間のトラフィックに影響するスタティック NAT ルールに対してこの設定を使用**しない**でください。

ダイナミック IP 専用

ダイナミック IP 専用ルールは多対多の送信元ネットワークを変換しますが、ポートおよびプロトコルを維持しますダイナミック IP 専用変換を設定する場合、ゾーン、送信元ネットワーク、元の宛先ネットワーク、および元の宛先ポートを設定できます。変換後の宛先ネットワークまたは変換後の宛先ポートは設定できません。

変換後の送信元ネットワークを少なくとも 1 つ指定する**必要**があります。変換後の送信元ネットワーク値の数が元の送信元ネットワークの数よりも小さい場合、元のアドレスがすべて照合される前に変換後のアドレスが不足する可能性があるという警告がルールに表示されます。

同じパケットに一致する条件を持つルールが複数個ある場合、優先度の低いルールはデッド ルールとなり、トリガーされなくなります。デッド ルールにも警告が表示されます。ツールチップを表示して、デッド ルールに代わるルールを判別できます。

注　デッド ルールを持つポリシーを保存し、適用することは可能ですが、ルールは変換を実現できません。

場合によっては、範囲の広いルールよりも優先される、範囲が限定されたルールを作成することをお勧めします。次に例を示します。

```
Rule 1: Match on address A and port A/Translate to address B
Rule 2: Match on address A/Translate to Address C
```

この例で、ルール 1 はルール 2 にも一致するいくつかのパケットに一致します。したがって、ルール 2 が完全に無効ではありません。

必要に応じて、元の宛先ポートだけを指定できます。変換後の宛先ポートは指定できません。

ダイナミック IP およびポート

ダイナミック IP およびポート ルールは多対 1 または多対多の送信元ネットワークとポートおよびプロトコルを変換します。ダイナミック IP およびポート変換を設定する場合、ゾーン、送信元ネットワーク、元の宛先ネットワーク、および元の宛先ポートを設定できます。変換後の宛先ネットワークまたは変換後の宛先ポートは設定できません。

変換後の送信元ネットワークを少なくとも 1 つ指定する**必要**があります。同じパケットに一致する条件を持つルールが複数個ある場合、優先度の低いルールはデッド ルールとなり、トリガーされなくなります。デッド ルールにも警告が表示されます。ツールチップを表示して、デッド ルールに代わるルールを判別できます。

注　デッド ルールを持つポリシーを保存し、適用することは可能ですが、ルールは変換を実現できません。

必要に応じて、元の宛先ポートだけを指定できます。変換後の宛先ポートは指定できません。

注　ダイナミック IP およびポート ルールを作成し、システムがポートを使用しないトラフィックを渡す場合、そのトラフィックに対して変換は発生しません。たとえば、送信元ネットワークに一致する IP アドレスからの ping（ICMP）は、ICMP がポートを使用しないため、マッピングされません。

次の表に、指定された NAT ルール タイプに基づいて設定可能な NAT ルールの条件タイプをまとめています。

表 11-8　NAT ルール タイプごとに使用可能な NAT ルールの条件タイプ

条件	スタティック	ダイナミック（IP 専用または IP およびポート）
送信元ゾーン	任意	任意
宛先ゾーン	不可	任意
元の送信元ネットワーク	不可	任意
変換後の送信元ネットワーク	不可	**必須**
元の宛先ネットワーク	**必須**	任意
変換後の宛先ネットワーク	オプション。単一アドレスのみ	不可
元の宛先ポート	オプション。単一ポートでのみ、元の宛先ネットワークを定義する場合のみ可能	任意
変換後の宛先ポート	オプション。単一ポートでのみ、元の宛先ポートを定義する場合のみ可能	不可

NAT ルール条件と条件のしくみについて

ライセンス： すべて

ルールに一致するトラフィックのタイプを識別するために NAT ルールに条件を追加できます。それぞれの条件タイプごとに、使用可能条件リストから、ルールに追加する条件を選択します。条件フィルタを適用できる場合は、条件フィルタを使って使用可能な条件を限定できます。使用可能な条件リスト、および選択した条件リストは、1 つの条件だけを含む場合も、数ページに及ぶ場合もあります。使用可能な条件は検索することができ、名前や値を入力するとそれに一致する条件だけが表示され、入力していくにつれてそのリストが更新されます。

条件のタイプに応じて、使用可能条件リストには、Ciscoから直接提供された条件と、他の FireSIGHT システム機能を使って設定された条件が一緒に含まれることがあります。その中には、オブジェクト マネージャ（[Objects] > [Object Management] ）を使って作成されたオブジェクト、個別の条件ページから直接作成されたオブジェクト、およびリテラル条件が含まれます。

ルール条件の指定については、次の項を参照してください。

- NAT ルール条件について（11-21 ページ）に、さまざまなタイプのルール条件の定義を示します。
- NAT ルールへの条件の追加（11-22 ページ）に、ルール条件を選択および追加するためのコントロールを示しています。
- NAT ルール条件リストの検索（11-24 ページ）では、使用可能な条件の検索方法を説明します。入力した名前や値に一致する条件だけが表示され、入力していくにつれてそのリストが更新されます。
- NAT ルールへのリテラル条件の追加（11-25 ページ）に、リテラル条件をルールに追加する方法の説明を示します。
- NAT ルール条件でのオブジェクトの使用（11-25 ページ）では、該当する条件タイプの設定ページから個別のオブジェクトをシステムに追加する方法について説明します。

NAT ルール条件について

ライセンス： すべて

次の表で説明されている条件のいずれかを満たすトラフィックを照合するための NAT ルールを設定できます。

表 11-9　NAT ルールの条件タイプ

条件	説明	サポートされる Defense Center	サポートされるデバイス数
ゾーン	NAT ポリシーを適用できる 1 つ以上のルーテッド インターフェイスの設定。ゾーンは、送信元インターフェイスと宛先インターフェイスでトラフィックを分類するメカニズムであり、ルールに送信元のゾーン条件と宛先のゾーン条件を追加することができます。オブジェクト マネージャを使ってゾーンを作成する方法については、セキュリティ ゾーンの操作（3-42 ページ）を参照してください。	いずれか	シリーズ 3

表 11-9　NAT ルールの条件タイプ（続き）

条件	説明	サポートされる Defense Center	サポートされるデバイス数
Networks	明示的に指定された、またはネットワーク オブジェクトとグループ（ネットワーク オブジェクトの操作（3-4 ページ）を参照）を使って指定された、個別の IP アドレス、CIDR ブロック、およびプレフィクス長からなる任意の組み合わせ。NAT ルールに送信元ネットワークおよび宛先ネットワークの条件を追加できます。	いずれか	シリーズ 3
宛先ポート	トランスポート プロトコルに基づいて作成される、個別のポート オブジェクトとグループ ポート オブジェクトを含むトランスポート プロトコル ポート。オブジェクト マネージャを使用して個別のトランスポート プロトコル オブジェクトとグループ トランスポート プロトコル オブジェクトを作成する方法については、ポート オブジェクトの操作（3-13 ページ）を参照してください。	いずれか	シリーズ 3

NAT ルールへの条件の追加

ライセンス： すべて

NAT ルールへの条件の追加は基本的にどの条件のタイプでも同じです。左側の使用可能な条件のリストから選択して、右側で選択した条件の 1 つまたは 2 つのリストに、選択した条件を追加します。

すべての条件タイプで、使用可能な個々の条件を 1 つまたは複数クリックすると、それが強調表示され、選択状態になります。2 つのタイプのリスト間にあるボタンをクリックして選択した使用可能な条件を選択した条件のリストに追加するか、または選択した使用可能な条件を選択した条件のリストにドラッグ アンド ドロップします。

選択済み条件リストには、タイプごとに最大 50 個までの条件を追加できます。たとえばアプライアンスの上限に達するまで、最大 50 個の送信元ゾーン条件、最大 50 個の宛先ゾーン条件、最大 50 個の送信元ネットワーク条件などを追加できます。

次の表に、条件を選択してルールに追加する際に実行できる操作の説明を示します。

表 11-10　NAT ルールへの条件の追加

目的	操作
使用可能な条件を選択して、選択済み条件のリストに追加する	使用可能な条件をクリックします。複数の条件を選択するには Ctrl キーと Shift キーを使用します。
リストされたすべての使用可能な条件を選択する	いずれかの使用可能な条件の行を右クリックし、[Select All] をクリックします。
使用可能な条件またはフィルタのリストを検索する	検索フィールド内をクリックし、検索文字列を入力します。詳細については、「NAT ルール条件リストの検索（11-24 ページ）」を参照してください。
使用可能な条件やフィルタを検索しているときに検索内容をクリアする	検索フィールドの上のリロード アイコン（ ）、または検索フィールド内のクリア アイコン（ ）をクリックします。

表 11-10　NAT ルールへの条件の追加（続き）

目的	操作
使用可能な条件のリストから選択したゾーン条件を、選択した送信元または宛先の条件のリストに追加する	[Add to Source] または [Add to Destination] をクリックします。詳細については、「NAT ルールへのゾーン条件の追加（11-26 ページ）」を参照してください。
使用可能な条件のリストから選択したネットワークとポートの条件を、選択した元または変換後の条件のリストに追加する	[Add to Original] または [Add to Translated] をクリックします。詳細については、ダイナミック NAT ルールへの送信元ネットワーク条件の追加（11-28 ページ）、NAT ルールへの宛先ネットワーク条件の追加（11-30 ページ）、または NAT ルールへのポート条件の追加（11-31 ページ）を参照してください。
選択した使用可能な条件を、選択済み条件リストにドラッグ アンド ドロップする	選択した条件をクリックし、選択した条件のリストにドラッグ アンド ドロップします。
リテラル フィールドを使用して、選択済み条件リストにリテラル条件を追加する	クリックしてリテラル フィールドからプロンプトを除去し、リテラル条件を入力して、[Add] をクリックします。ネットワーク条件は、リテラル条件を追加するためのフィールドを提供します。
ドロップダウン リストを使用して、選択済み条件リストにリテラル条件を追加する	ドロップダウン リストから条件を選択して、[Add] をクリックします。ポート条件には、リテラル条件を追加するためのドロップダウン リストがあります。詳細については、「NAT ルールへのポート条件の追加（11-31 ページ）」を参照してください。
個々のオブジェクトまたは条件フィルタを追加して、使用可能条件リストからそれを選択できるようにする	追加アイコン（  ）をクリックします。オブジェクト マネージャを使ってオブジェクトを追加する方法については、再利用可能なオブジェクトの管理（3-1 ページ）を参照してください。
選択済み条件リストから 1 つの条件を削除する	条件の横にある削除アイコン（  ）をクリックします。
選択済み条件リストから 1 つの条件を削除する	1 つの選択済み条件の行を右クリックして強調表示し、[Delete] をクリックします。
選択済み条件リストから複数の条件を削除する	Shift キーまたは Ctrl キーを押しながら複数の条件をクリックして選択するか、右クリックして [Select All] を選択します。次に、いずれかの選択済み条件の行を右クリックして強調表示し、[Delete Selected] をクリックします。

該当する条件ページとポリシー編集ページで、ポインタを 1 つの個別オブジェクトの上に置くとそのオブジェクトの内容が表示され、グループ オブジェクトの上に置くと、グループ内の個々のオブジェクトの数が表示されます。

新しいルールに条件を追加する基本的な手順を次に示します。ルールの追加と変更に関する詳しい説明は、NAT ルールの作成と編集（11-17 ページ）を参照してください。

使用可能な条件を選択済み条件リストに追加する方法：

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [NAT] を選択します。

[NAT] ページが表示されます。

ステップ 2　変更する NAT ポリシーの横にある編集アイコン（  ）をクリックします。

ポリシーの [Edit] ページが表示されます。

ステップ 3　[Add Rule] をクリックします。

[Add Rule] ページが表示されます。

ステップ 4　ルールに追加する条件タイプに対応したタブをクリックします。

選択した条件のタイプに対応する条件ページが表示されます。

ステップ 5　NAT ルールへの条件の追加表に含まれているいずれかのアクションを実行します。

ステップ 6　設定を保存するには、[Add] をクリックします。

ルールが追加され、ポリシー編集ページが表示されます。

NAT ルール条件リストの検索

ライセンス：すべて

使用可能な NAT ルール条件のリストをフィルタして、リストに表示される項目の数を制限できます。入力していくと、リストが更新されて一致する項目が表示されます。

オプションで、オブジェクト名およびオブジェクトに設定されている値を検索対象にすることができます。たとえば `Texas Office` という名前の個別ネットワーク オブジェクトがあり、`192.168.3.0/24` という値が設定されていて、`US Offices` というグループ オブジェクトに含まれる場合、`Tex` などの部分的または完全な検索文字列を入力するか、または `3` などの値を入力することにより、両方のオブジェクトを表示できます。

新しいルールでリストをフィルタ処理する基本的な手順を次に示します。ルールの追加と変更に関する詳しい説明は、NAT ルールの作成と編集（11-17 ページ）を参照してください。

使用可能な条件のリストを検索する方法：

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [NAT] を選択します。

[NAT] ページが表示されます。

ステップ 2　変更する NAT ポリシーの横にある編集アイコン（  ）をクリックします。

ポリシーの [Edit] ページが表示されます。

ステップ 3　[Add Rule] をクリックします。

[Add Rule] ページが表示されます。

ステップ 4　リストを検索するには、検索フィールド内部をクリックしてプロンプトをクリアした後、検索文字列を入力します。

入力していくとリストが更新され、一致する項目とクリア アイコン（ ）が検索フィールドに表示されます。検索文字列に一致する項目がない場合、リストが更新されて、リストには何も表示されません。

ステップ 5　オプションで、[Search] フィールドの上のリロード アイコン（ ）をクリックするか、[Search] フィールド内のクリア アイコン（ ）をクリックして、検索文字列を消去します。

完全なリストが表示されます。

ステップ 6　設定を保存するには、[Add] をクリックします。

ルールが追加され、ポリシー編集ページが表示されます。

NAT ルールへのリテラル条件の追加

ライセンス： すべて

次の条件タイプについて、元のおよび変換後の条件のリストにリテラル値を追加できます。

- Networks
- ポート

ネットワーク条件の場合、元のまたは変換後の条件リストの下にある設定フィールドにリテラル値を入力します。

ポート条件では、ドロップダウン リストからプロトコルを選択します。プロトコルが [All] の場合、またオプションでプロトコルが [TCP] または [UDP] の場合、設定フィールドにポート番号を入力します。

該当するそれぞれの条件ページには、リテラル値を追加するために必要なコントロールがあります。設定フィールドに入力した値が無効である場合や、まだ有効と認識されていない場合は、赤いテキストとして表示されます。入力時に有効と認識された値は青色に変わります。有効な値が認識されると、グレー表示の [Add] ボタンがアクティブになります。追加したリテラル値は、選択済み条件リストにただちに表示されます。

それぞれのタイプのリテラル値を追加する詳しい方法については、次を参照してください。

- ダイナミック NAT ルールへの送信元ネットワーク条件の追加（11-28 ページ）
- NAT ルールへの宛先ネットワーク条件の追加（11-30 ページ）
- NAT ルールへのポート条件の追加（11-31 ページ）

NAT ルール条件でのオブジェクトの使用

ライセンス： すべて

オブジェクト マネージャ（[Objects] > [Object Management]）で作成されたオブジェクトは、使用可能な NAT ルール条件の関連リストからすぐに選択可能になります。詳細については、再利用可能なオブジェクトの管理（3-1 ページ）を参照してください。

NAT ポリシーから直接オブジェクトを作成することもできます。該当する条件ページ上のコントロールでは、オブジェクト マネージャでの設定コントロールと同じ機能を利用できます。

直接作成された個別のオブジェクトは使用可能なオブジェクトのリストにすぐに表示されます。それらを現在のルールと他の既存および将来のルールに追加できます。該当する条件ページとポリシー編集ページで、ポインタを 1 つの個別オブジェクトの上に置くとそのオブジェクトの内容が表示され、グループ オブジェクトの上に置くと、グループ内の個々のオブジェクトの数が表示されます。

NAT ルールのさまざまな条件タイプの使用

ライセンス： すべて

トラフィックを 1 つまたは複数のルール条件と照合できます。詳細については、次の項を参照してください。

- NAT ルールへのゾーン条件の追加（11-26 ページ）ではオブジェクト マネージャを使用して作成したセキュリティ ゾーンにより、トラフィックを照合する方法について説明します。
- ダイナミック NAT ルールへの送信元ネットワーク条件の追加（11-28 ページ）およびNAT ルールへの宛先ネットワーク条件の追加（11-30 ページ）では IP アドレスまたはアドレス ブロックによりトラフィックを照合する方法について説明します。
- NAT ルールへのポート条件の追加（11-31 ページ）では指定した転送プロトコル ポートにより、トラフィックを照合する方法について説明します。

NAT ルールへのゾーン条件の追加

ライセンス： すべて

システムのセキュリティ ゾーンは、管理対象デバイス上のインターフェイスで構成されます。NAT ルールに追加するゾーンは、それらのゾーン内にルーテッド またはハイブリッド インターフェイスを持つネットワーク上のデバイスへのルールをターゲットにします。NAT ルールの条件として、ルーテッド またはハイブリッド インターフェイスを持つセキュリティ ゾーンのみを追加できます。オブジェクト マネージャを使ってセキュリティ ゾーンを作成する方法については、セキュリティ ゾーンの操作（3-42 ページ）を参照してください。

現在仮想ルータに割り当てられているゾーンまたはスタンドアロン インターフェイスのどちらかを NAT ルールに追加できます。デバイス設定が適用されていないデバイスがある場合、[Zones] ページの使用可能なゾーン リストの上に警告アイコン（⚠）が表示され、適用済みのゾーンおよびインターフェイスのみが表示されることが示されます。ゾーンの横にある矢印アイコン（▷）をクリックして、ゾーンを縮小または展開し、そのインターフェイスを非表示または表示することができます。

インターフェイスがクラスタ デバイス上にある場合、使用可能なゾーンのリストに、そのインターフェイスからの追加のブランチが表示されると共に、クラスタ内の他のインターフェイスがクラスタ内のアクティブなデバイスのプライマリ インターフェイスの子として表示されます。矢印アイコン（▷）をクリックして、クラスタ インターフェイスを縮小または展開し、そのインターフェイスを非表示または表示することもできます。

注　無効にされたインターフェイスを持つポリシーを保存して適用できますが、インターフェイスが有効になるまでルールは変換を実現できません。

右側の 2 つのリストは、NAT ルールによって照合目的に使用される送信元ゾーンと宛先のゾーンです。すでにルールに値が設定されている場合、ルールを編集する際、これらのリストには既存の値が表示されます。送信元ゾーンのリストが空の場合、ルールは任意のゾーンまたはインターフェイスからのトラフィックを照合します。宛先ゾーンのリストが空の場合、ルールは任意のゾーンまたはインターフェイス宛てのトラフィックを照合します。

対象のデバイスでトリガーされることがないゾーンの組み合わせを持つルールに対しては警告が表示されます。

注　これらのゾーンの組み合わせを持つポリシーを保存して適用できますが、ルールは変換を実現しません。

ゾーン内の項目を選択するか、またはスタンドアロン インターフェイスを選択することによって、個別のインターフェイスを追加できます。割り当てられているゾーンがまだ送信元ゾーンまたは宛先ゾーンのリストに追加されていない場合のみ、ゾーン内のインターフェイスを追加できます。これらの個別に選択されたインターフェイスは、削除して別のゾーンに追加した場合でも、ゾーンに対する変更に影響されません。インターフェイスがクラスタのプライマリ メンバーであり、ダイナミック ルールを設定する場合、プライマリ インターフェイスのみを送信元ゾーンまたは宛先ゾーンのリストに追加できます。スタティック ルールの場合、送信元ゾーンのリストに個別のクラスタ メンバー インターフェイスを追加できます。プライマリ クラスタ インターフェイスは、その子がまったく追加されていない場合だけ、リストに追加できます。また、個別のクラスタ インターフェイスは、プライマリが追加されていない場合だけ追加できます。

ゾーンを追加すると、ルールはゾーンに関連付けられたすべてのインターフェイスを使用します。ゾーンに対してインターフェイスを追加または削除すると、インターフェイスが存在するデバイスにデバイス設定が再適用されるまで、ルールはゾーンの更新バージョンを使用しません。

注　スタティック NAT ルールでは、送信元ゾーンのみを追加できます。ダイナミック NAT ルールでは、送信元ゾーンと宛先ゾーンの両方を追加できます。

次の手順では、NAT ルールの追加または編集の際に、送信元と宛先のゾーン条件を追加する方法について説明します。詳細については、NAT ルール条件と条件のしくみについて（11-21 ページ）を参照してください。

ゾーン条件を NAT ルールに追加する方法：

アクセス： Admin/Network Admin

ステップ 1　ルール編集ページの [Zones] タブを選択します。

[Zones] ページが表示されます。

ステップ 2　必要に応じて、[Available Zones] リストの上にある [Search by name] プロンプトをクリックし、名前か値を入力します。

入力していくと、リストが更新されて一致する条件が表示されます。詳細については、「NAT ルール条件リストの検索（11-24 ページ）」を参照してください。

ステップ 3　[Available Zones] リスト内のゾーンまたはインターフェイスをクリックします。Shift キーまたは Ctrl キーを押しながら複数の条件をクリックして選択するか、右クリックして [Select All] をクリックします。

選択した条件が強調表示されます。

ステップ 4　次の選択肢があります。

- 送信元ゾーンによりトラフィックを照合するには、[Add to Source] をクリックします。
- 宛先ゾーンによりトラフィックを照合するには、[Add to Destination] をクリックします。

オプションで、選択した条件を [Source Zones] リストまたは [Destination Zones] リストにドラッグ アンド ドロップできます。

選択した条件が追加されます。無効になっているインターフェイスを NAT ルールに追加できますが、ルールは変換を実現しないことに注意してください。

注　スタティック NAT ルールには送信元ゾーンのみを追加できます。

ステップ 5　ルールを保存するか、編集を続けます。

変更内容を有効にするには、NAT ポリシーを適用する必要があります。NAT ポリシーの適用（11-15 ページ）を参照してください。

ダイナミック NAT ルールへの送信元ネットワーク条件の追加

ライセンス： すべて

パケットの送信元 IP アドレスの照合値と変換値を設定します。元の送信元ネットワークが設定されていない場合、すべての送信元 IP アドレスがダイナミック NAT ルールに一致します。スタティック NAT ルールの送信元ネットワークは設定できないことに注意してください。パケットが NAT ルールに一致すると、システムは変換後の送信元ネットワークの値を使用して、送信元 IP アドレスの新しい値を割り当てます。ダイナミック ルール用に少なくとも 1 つの値を持つ変換後の送信元ネットワークを設定する必要があります。

注意　ネットワーク オブジェクトまたはオブジェクト グループが NAT ルールで使用されている場合に、オブジェクトまたはグループを変更または削除すると、ルールが無効になる可能性があります。

ダイナミック NAT ルールに、次の種類の送信元ネットワーク条件を追加できます。

- オブジェクト マネージャを使って作成した個別およびグループのネットワーク オブジェクト

  オブジェクト マネージャを使用して個別のネットワーク オブジェクトとグループ ネットワーク オブジェクトを作成する方法については、ネットワーク オブジェクトの操作（3-4 ページ）を参照してください。
- 送信元ネットワーク条件のページから追加し、ユーザのルールと他の既存および将来のルールに追加可能な個別のネットワーク オブジェクト

  詳細については、「NAT ルール条件でのオブジェクトの使用（11-25 ページ）」を参照してください。
- リテラル、単一 IP アドレス、範囲、またはアドレス ブロック

  詳細については、「NAT ルールへのリテラル条件の追加（11-25 ページ）」を参照してください。

次の手順では、ダイナミック NAT ルールの追加または編集の際に、送信元ネットワーク条件を追加する方法について説明します。詳細については、NAT ルール条件と条件のしくみについて（11-21 ページ）を参照してください。

ネットワーク条件をダイナミック NAT ルールに追加する方法：

アクセス： Admin/Network Admin

ステップ 1　ルールの編集ページの [Source Networks] タブを選択します。

[Source Network] ページが表示されます。

ステップ 2　必要に応じて、[Available Networks] リストの上にある [Search by name or value] プロンプトをクリックし、名前か値を入力します。

入力していくと、リストが更新されて一致する条件が表示されます。詳細については、「NAT ルール条件リストの検索（11-24 ページ）」を参照してください。

ステップ 3　[Available Networks] リスト内の条件をクリックします。Shift キーまたは Ctrl キーを押しながら複数の条件をクリックして選択するか、右クリックして [Select All] をクリックします。

選択した条件が強調表示されます。

ステップ 4　次の選択肢があります。

- 元の送信元ネットワークによりトラフィックを照合するには、[Add to Original] をクリックします。
- 変換後の送信元ネットワークと照合するトラフィックの変換値を指定するには、[Add to Translated] をクリックします。

または、選択した条件を [Original Source Network] リストまたは [Translated Source Network] リストにドラッグ アンド ドロップできます。

選択した条件が追加されます。

ステップ 5　オプションで、[Available Networks] リストの上にある追加アイコン（  ）をクリックし、個別のネットワーク オブジェクトを追加します。

各ネットワーク オブジェクトに複数の IP アドレス、CIDR ブロック、およびプレフィクス長を追加できます。

その後、オプションで、追加済みのオブジェクトを選択できます。詳細については、ネットワーク オブジェクトの操作（3-4 ページ）およびNAT ルール条件でのオブジェクトの使用（11-25 ページ）を参照してください。

ステップ 6　オプションで、[Original Source Network] リストまたは [Translated Source Network] リストの下の [Enter an IP address] プロンプトをクリックします。次に、IP アドレス、範囲、またはアドレス ブロックを入力して、[Add] をクリックします。

範囲は、下位の IP アドレス-上位の IP アドレスの形式で追加します。例：
`179.13.1.1-179.13.1.10`。

リストが更新されて、それらのエントリが表示されます。詳細については、「NAT ルールへのリテラル条件の追加（11-25 ページ）」を参照してください。

ステップ 7　ルールを保存するか、編集を続けます。

注　適用されているポリシーで使用中のダイナミック ルールのネットワーク条件を更新すると、既存の変換済みアドレス プールを使用しているネットワーク セッションがドロップされます。

変更内容を有効にするには、NAT ポリシーを適用する必要があります。NAT ポリシーの適用（11-15 ページ）を参照してください。

NAT ルールへの宛先ネットワーク条件の追加

ライセンス： すべて

パケットの宛先 IP アドレスの照合値と変換値を設定します。ダイナミック NAT ルールの変換後の宛先ネットワークを設定できないことに注意してください。

スタティック NAT ルールは 1 対 1 変換であるため、[Available Networks] リストには単一の IP アドレスのみを含むネットワーク オブジェクトおよびグループのみが含まれます。スタティック変換用に、単一のオブジェクトまたはリテラル値のみを [Original Destination Network] リストと [Translated Destination Network] リストの両方に追加できます。

注意　ネットワーク オブジェクトまたはオブジェクト グループが NAT ルールで使用されている場合に、オブジェクトまたはグループを変更または削除すると、ルールが無効になる可能性があります。

NAT ルールに、次の種類の宛先ネットワーク条件を追加できます。

- オブジェクト マネージャを使って作成した個別およびグループのネットワーク オブジェクト

  オブジェクト マネージャを使用して個別のネットワーク オブジェクトとグループ ネットワーク オブジェクトを作成する方法については、ネットワーク オブジェクトの操作（3-4 ページ）を参照してください。

- 宛先ネットワーク条件のページから追加し、ユーザのルールと他の既存および将来のルールに追加可能な個別のネットワーク オブジェクト

  詳細については、「NAT ルール条件でのオブジェクトの使用（11-25 ページ）」を参照してください。

- リテラル、単一 IP アドレス、範囲、またはアドレス ブロック

  スタティック NAT ルールでは、リストにまだ値がない場合に限り、CIDR とサブネット マスク /32 のみを追加できます。

  詳細については、「NAT ルールへのリテラル条件の追加（11-25 ページ）」を参照してください。

次の手順では、NAT ルールの追加または編集の際に、宛先ネットワーク条件を追加する方法について説明します。詳細については、NAT ルール条件と条件のしくみについて（11-21 ページ）を参照してください。

宛先ネットワーク条件を NAT ルールに追加する方法：

アクセス： Admin/Network Admin

ステップ 1　ルールの編集ページの [Destination Network] タブを選択します。

[Destination Network] ページが表示されます。

ステップ 2　必要に応じて、[Available Networks] リストの上にある [Search by name or value] プロンプトをクリックし、名前か値を入力します。

入力していくと、リストが更新されて一致する条件が表示されます。詳細については、「NAT ルール条件リストの検索（11-24 ページ）」を参照してください。

ステップ 3　[Available Networks] リスト内の条件をクリックします。Shift キーまたは Ctrl キーを押しながら複数の条件をクリックして選択するか、右クリックして [Select All] をクリックします。

選択した条件が強調表示されます。

ステップ 4　次の選択肢があります。

- 元の宛先ネットワークによりトラフィックを照合するには、[Add to Original] をクリックします。
- 変換後の宛先ネットワークと照合するトラフィックの変換値を指定するには、[Add to Translated] をクリックします。

または、選択した条件を [Original Destination Network] リストまたは [Translated Destination Network] リストにドラッグ アンド ドロップできます。

選択した条件が追加されます。

ステップ 5　オプションで、[Available Networks] リストの上にある追加アイコン（ ）をクリックし、個別のネットワーク オブジェクトを追加します。

ダイナミック ルールの場合、各ネットワーク オブジェクトに複数の IP アドレス、CIDR ブロック、およびプレフィクス長を追加できます。スタティック ルールの場合、単一の IP アドレスのみを追加できます。その後、オプションで、追加済みのオブジェクトを選択できます。詳細については、ネットワーク オブジェクトの操作（3-4 ページ）およびNAT ルール条件でのオブジェクトの使用（11-25 ページ）を参照してください。

ステップ 6　オプションで、[Original Destination Network] リストまたは [Translated Destination Network] リストの下の [Enter an IP address] プロンプトをクリックし、次に、IP アドレスまたはアドレス ブロックを入力して、[Add] をクリックします。

リストが更新されて、それらのエントリが表示されます。詳細については、「NAT ルールへのリテラル条件の追加（11-25 ページ）」を参照してください。

ステップ 7　ルールを保存するか、編集を続けます。

注　適用されているポリシーで使用中のダイナミック ルールのネットワーク条件を更新すると、既存の変換済みアドレス プールを使用しているネットワーク セッションがドロップされます。

変更内容を有効にするには、NAT ポリシーを適用する必要があります。NAT ポリシーの適用（11-15 ページ）を参照してください。

NAT ルールへのポート条件の追加

ライセンス： すべて

ルールにポート条件を追加し、元と変換後の宛先ポートおよび変換用の転送プロトコルに基づいて、ネットワーク トラフィックを照合できます。元のポートが設定されていない場合、すべての宛先ポートがルールに一致します。パケットが NAT ルールに一致し、変換後の宛先ポートが設定されている場合、システムはその値にポートを変換します。ダイナミック ルールでは元の宛先ポートのみを指定できることに注意してください。スタティック ルールの場合、変換後の宛先ポートを定義できますが、元の宛先ポート オブジェクトまたはリテラル値と同じプロトコルを持つオブジェクトでのみ可能です。

システムは宛先ポートを、スタティック ルールの元の宛先ポート リスト内のポート オブジェクトまたはリテラル ポートの値、またはダイナミック ルールの複数の値と照合します。

スタティック NAT ルールは 1 対 1 変換であるため、[Available Ports] リストには単一のポートのみを含むポート オブジェクトおよびグループのみが含まれます。スタティック変換用に、単一のオブジェクトまたはリテラル値のみを [Original Port] リストと [Translated Port] リストの両方に追加できます。

ダイナミック ルールの場合は、ポートの範囲を追加できます。たとえば、元の宛先ポートを指定する場合、リテラル値として 1000-1100 を追加できます。

注意　ポート オブジェクトまたはオブジェクト グループが NAT ルールで使用されている場合に、オブジェクトまたはグループを変更または削除すると、ルールが無効になる可能性があります。

NAT ルールに、次の種類のポート条件を追加できます。

- オブジェクト マネージャを使って作成した個別およびグループのポート オブジェクト

  オブジェクト マネージャを使用して個別のポート オブジェクトとグループ ポート オブジェクトを作成する方法については、ポート オブジェクトの操作（3-13 ページ）を参照してください。

- 宛先ポート条件のページから追加し、ユーザのルールと他の既存および将来のルールに追加可能な個別のポート オブジェクト

  詳細については、「NAT ルール条件でのオブジェクトの使用（11-25 ページ）」を参照してください。

- TCP、UDP、またはすべて（TCP および UDP）の転送プロトコルとポートから構成されるリテラル ポート値

  詳細については、「NAT ルールへのリテラル条件の追加（11-25 ページ）」を参照してください。

次の手順では、NAT ルールの追加または編集の際に、ポート条件を追加する方法について説明します。詳細については、NAT ルール条件と条件のしくみについて（11-21 ページ）を参照してください。

宛先ポート条件を NAT ルールに追加する方法：

アクセス： Admin/Network Admin

ステップ 1　ルールの編集ページの [Destination Port] タブを選択します。

[Destination Port] ページが表示されます。

ステップ 2　必要に応じて、[Available Ports] リストの上にある [Search by name or value] プロンプトをクリックし、名前または値を入力します。

入力していくと、リストが更新されて一致する条件が表示されます。詳細については、「NAT ルール条件リストの検索（11-24 ページ）」を参照してください。

ステップ 3　[Available Ports] リスト内の条件をクリックします。Shift キーまたは Ctrl キーを押しながら複数の条件をクリックして選択するか、右クリックしてすべての条件を選択します。なお、最大で 50 個の条件を追加できます。

選択した条件が強調表示されます。

ステップ 4　次の選択肢があります。

- [Add to Original] をクリックして、選択したポートを [Original Ports] リストに追加します。
- [Add to Translated] をクリックして、選択したポートを [Translated Ports] リストに追加します。

- 使用可能なポートをリストにドラッグ アンド ドロップします。

ステップ 5　オプションで、個別のポート オブジェクトを作成して追加するには、[Available Ports] リストの上の追加アイコン（ ）をクリックします。

追加する各ポート オブジェクトの 1 つのポートまたはポート範囲を指定できます。その後、ルールの条件として追加するオブジェクトを選択できます。詳細については、「NAT ルール条件でのオブジェクトの使用（11-25 ページ）」を参照してください。

スタティック ルールの場合、単一のポートを持つポート オブジェクトのみを使用できます。

ステップ 6　（任意）リテラル ポートを追加するには、[Original Port] リストまたは [Translated Port] リストの [Protocol] ドロップダウン リストからエントリを選択します。

ポートを入力し、[Add] をクリックします。0 から 65535 までのポート番号を指定できます。ダイナミック ルールの場合、単一のポートまたは範囲を指定できます。

リストが更新され、選択内容が表示されます。詳細については、「NAT ルールへのリテラル条件の追加（11-25 ページ）」を参照してください。

選択した条件が追加されます

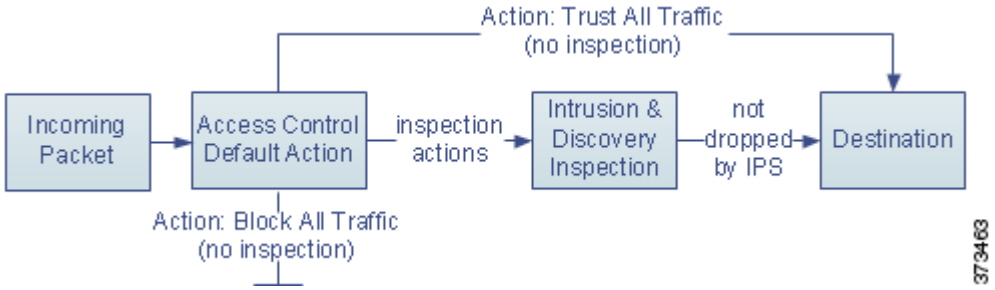
ステップ 7　ルールを保存するか、編集を続けます。

変更内容を有効にするには、NAT ポリシーを適用する必要があります。NAT ポリシーの適用（11-15 ページ）を参照してください。

アクセス コントロール ポリシーの開始

*アクセス コントロール ポリシー*は、ネットワーク上の非高速パスを通るトラフィックを、システムでどのように処理するかを決定します。ユーザは 1 つ以上のアクセス コントロール ポリシーを設定して、設定したポリシーを 1 つ以上の管理対象デバイスに適用できます。各デバイスに同時に適用できるポリシーは 1 つだけです。

最も単純なアクセス コントロール ポリシーでは、*デフォルト アクション*を使用してすべてのトラフィックを処理するターゲット デバイスを指定します。このデフォルト アクションは、詳細な検査を行わずにすべてのトラフィックをブロックまたは信頼するように設定することも、侵入および検出データについてトラフィックを検査するように設定することもできます。



インライン展開されたデバイスだけがトラフィックのフローに影響を与える場合があることに注意してください。トラフィックをブロックまたは変更するように設定されたアクセス コントロール ポリシーをパッシブに展開されたデバイスに適用すると、予期しない結果になることがあります。場合によっては、インライン設定をパッシブに展開されたデバイスに適用することがシステムによって阻害されます。

この章では、単純なアクセス コントロール ポリシーを作成して適用する方法について説明します。また、アクセス コントロール ポリシーの管理に関する基本情報（編集、更新、比較など）も含まれています。詳細については、以下を参照してください。

- アクセス コントロール ポリシーおよびルールのトラブルシューティング（12-25 ページ）
- 現在のアクセス コントロール設定のレポートの生成（12-29 ページ）
- アクセス コントロール ポリシーの比較（12-30 ページ）

より複雑なアクセス コントロール ポリシーはセキュリティ インテリジェンス データに基づいてトラフィックをブラックリスト登録することができ、また、*アクセス コントロール ルール*を使用してネットワーク トラフィックのロギングおよび処理を細かく制御することができます。これらのルールは単純または複雑にすることができ、複数の基準を使用してトラフィックを照合および検査できます。高度なアクセス コントロール ポリシー オプションは、復号化、前処理、パフォーマンス、および他の一般設定を制御します。

基本的なアクセス コントロール ポリシーを作成した後、それをご自身の展開環境に合わせる方法については次の章を参照してください。

- セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録（13-1 ページ）では、最新のレピュテーション インテリジェンスに基づいて接続を即座にブラックリスト登録（ブロック）する方法について説明します。
- トラフィック復号化の概要（19-1 ページ）では、SSL ポリシーを使用して、暗号化されたトラフィックを検査することなくブロックしたり、アクセス コントロール ルールに渡す（場合によっては復号化した後に）方法について説明します。
- ネットワーク分析ポリシーまたは侵入ポリシーについて（23-1 ページ）では、システムの侵入検知および防止機能の一部として、ネットワーク分析および侵入ポリシーがパケットを前処理し確認する方法について説明します。
- アクセス コントロール ルールを使用したトラフィック フローの調整（14-1 ページ）では、複数の管理対象デバイスでネットワーク トラフィックを処理する詳細な方法をアクセス コントロール ルールが提供する方法について説明します。
- 侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（18-1 ページ）では、侵入、禁止されたファイルおよびマルウェアを検出しオプションでブロックすることによって、トラフィックがその宛先に許可される前に、最後の防衛ラインを侵入ポリシーおよびファイル ポリシーが提供する方法について説明します。

アクセス コントロールのライセンスおよびロール要件

Defense Center でのライセンスに関係なくアクセス コントロール ポリシーを作成できますが、多くの機能では、ポリシーを適用する前に適切なライセンスを有効にする必要があります。また、一部の機能は、特定のモデルでのみ使用できます。

また、使用可能なアクセス コントロール関連の機能とアクションは、ユーザ ロールによって異なることに注意してください。さまざまな管理者やアナリスト用のユーザ ロールが事前定義されていますが、それ以外にも特殊なアクセス権限を持たせたカスタム ユーザ ロールを作成できます。

詳細については、以下を参照してください。

- アクセス コントロールのライセンスおよびモデルの要件（12-3 ページ）
- カスタム ユーザ ロールによる展開の管理（12-4 ページ）

アクセス コントロールのライセンスおよびモデルの要件

アクセス コントロール ポリシーは、Defense Centerでのライセンスに関係なく作成できます。ただし、アクセス コントロールのある側面では、ポリシーを適用する前にターゲット デバイスで特定のライセンス交付対象の機能を有効化する必要があります。また、一部の機能は、特定のモデルでのみ使用できます。

警告アイコンおよび確認ダイアログ ボックスは、ご使用の展開環境でサポートされない機能を示します。詳細については、警告アイコンの上にポインタを置き、アクセス コントロール ポリシーおよびルールのトラブルシューティング（12-25 ページ）を参照してください。

次の表に、アクセス コントロール ポリシーを適用する際のライセンスおよびアプライアンス モデル要件を記載します。シリーズ 2 デバイスは、ほとんどのProtection機能を自動的に有効にするため、デバイスで明示的にProtectionを有効にする必要はありません。

表 12-1　　アクセス コントロールのライセンスおよびモデルの要件

以下を実行するアクセス コントロール ポリシーを適用する場合	ライセンス	サポートされる Defense Center	サポートされるデバイス数
ゾーン、ネットワーク、VLAN、またはポートに基づいてアクセス コントロールを実行する リテラル URL および URL オブジェクトを使用して URL フィルタリングを実行する	いずれか	いずれか	以下を除くすべて: • シリーズ 2 デバイスは、URL フィルタリングを実行できません • ASA FirePOWER デバイスは、VLAN フィルタリングを実行できません
SSL インスペクションを実行する（表 12-2（12-4 ページ）を参照）	いずれか	任意。例外として、DC500 はネットワーク、アプリケーション、および SSL 関連の制御に限定されています	シリーズ 3
位置情報データ（発信元または宛先の国/大陸）に基づいてアクセス コントロールを実行する	FireSIGHT	すべて（DC500 を除く）	シリーズ 3 Virtual ASA FirePOWER
侵入検知および侵入防御、ファイル コントロール、またはセキュリティ インテリジェンス フィルタリングを実行するポリシー	Protection	いずれか	任意：例外として、シリーズ 2 デバイスではセキュリティ インテリジェンス フィルタリングを実行できません。
高度なマルウェア対策としてネットワークベースのマルウェア検出およびブロッキングを実行するポリシー	Malware	すべて（DC500 を除く）	すべて（シリーズ 2 または X-Series を除く）
ユーザ制御またはアプリケーション制御を実行するポリシー	Control	任意：例外として、DC500 ではユーザ制御を実行できません。	すべて（シリーズ 2 または X-Series を除く）
カテゴリとレピュテーション データを使用して URL フィルタリングを実行するポリシー	URL Filtering	すべて（DC500 を除く）	すべて（シリーズ 2 を除く）

次の表では、SSL ポリシーを呼び出すことで SSL インスペクションを実行するアクセス コントロール ポリシーを適用する必要があるライセンスについて説明します。

表 12-2　SSL インスペクションのライセンスとモデルの要件

SSL ポリシーの機能	ライセンス	サポートされる Defense Center	サポートされるデバイス数
ゾーン、ネットワーク、VLAN、ポート、または SSL 関連の条件に基づいて暗号化トラフィックを処理する	いずれか	いずれか	シリーズ 3
位置情報のデータを使用して暗号化トラフィックを処理する	FireSIGHT	すべて（DC500 を除く）	シリーズ 3
アプリケーションまたはユーザの条件を使用して暗号化トラフィックを処理する	Control	任意：例外として、DC500 ではユーザ制御を実行できません。	シリーズ 3
URL カテゴリおよびレピュテーション データを使用して暗号化トラフィックをフィルタリングする	URL Filtering	すべて（DC500 を除く）	シリーズ 3

カスタム ユーザ ロールによる展開の管理

ライセンス： 機能によって異なる

カスタム ユーザ ロールの管理（61-55 ページ）で説明しているように、カスタム ユーザ ロールを作成して専用のカスタム特権を割り当てることができます。カスタム ユーザ ロールには、メニューベースのアクセス許可およびシステム アクセス許可の任意のセットを割り当てることができます。また、最初から独自に作成したり、事前定義されたユーザ ロールを基に作成したりできます。アクセス コントロール関連の機能に対するカスタム ロールにより、ユーザがアクセス コントロール ポリシー、侵入ポリシー、ファイル ポリシーを表示、変更、適用できるかどうか、また、管理者ルール カテゴリまたは root ルール カテゴリのルールを挿入または変更できるかどうかが決まります。

次の表に、FireSIGHT システム ユーザが操作できるアクセス コントロール関連の機能を決定する、5 つのカスタム ロールの例を記載します。この表には、各カスタム ロールに必要な権限が、カスタム ユーザ ロール を作成するときに表示される順でリストされています。

表 12-3　アクセス コントロールのカスタム ロールの例

カスタム ロールの権限	アクセス コントロールおよび SSL エディタ	侵入およびネットワーク分析エディタ	ファイル ポリシーの編集	ポリシーの適用（すべて）	侵入ポリシーの適用
アクセス コントロール	yes	no	no	yes	yes
アクセス コントロール リスト	yes	no	no	yes	yes
アクセス コントロール ポリシーの変更	yes	no	no	no	no
侵入ポリシーの適用	no	no	no	yes	yes
アクセス コントロール ポリシーの適用	no	no	no	yes	no

表 12-3　アクセス コントロールのカスタム ロールの例（続き）

カスタム ロールの権限	アクセス コントロールおよび SSL エディタ	侵入およびネットワーク分析エディタ	ファイル ポリシーの編集	ポリシーの適用（すべて）	侵入ポリシーの適用
侵入（ネットワーク分析権限も付与されます）	no	yes	no	no	no
侵入ポリシー	no	yes	no	no	no
侵入ポリシーの変更	no	yes	no	no	no
ファイル ポリシー	no	no	yes	no	no
ファイル ポリシーの変更	no	no	yes	no	no
SSL	yes	no	no	no	no
Modify SSL Policy	yes	no	no	no	no
Apply SSL Policy	no	no	no	yes	no

ただし、FireSIGHT システム のユーザ アカウントのロールが侵入ポリシーまたは修正侵入ポリシーに限定されている場合は、ネットワーク分析ポリシーに加えて、侵入ポリシーを作成して編集できます。

システムがレンダリングする Web インターフェイスは、ユーザが完全なアクセス コントロール ポリシー（侵入ポリシーを含む）を適用できるか、侵入ポリシーのみを適用できるか、あるいはいずれも適用できないかによって異なります。たとえば、上記の表の「侵入ポリシーの適用」が可能なユーザには、アクセス コントロール ポリシーの表示と侵入ポリシーの適用が許可されますが、いずれも編集はできません。また、アクセス コントロール ポリシーを適用することはできず、ファイル ポリシーまたは SSL ポリシーを表示することもできません。この場合、Web インターフェイスでは、

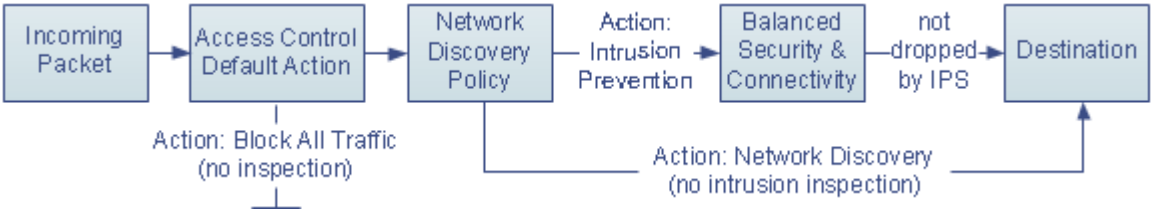
- [Access Control Policy] ページで、編集アイコン（ ）は非表示になります
- [Access Control Policy] ページで、削除アイコン（ ）は非表示になります
- クイック適用のポップアップ ウィンドウは、侵入ポリシーだけに適用されます
- 詳細適用ポップアップ ウィンドウで、アクセス コントロール ポリシーのチェック ボックスが無効になります

基本的なアクセス コントロール ポリシーの作成

ライセンス： すべて

新しいアクセス コントロール ポリシーを作成するには、そのポリシーに一意の名前を付けて、デフォルト アクションを指定する必要があります。この時点で、デフォルト アクションはポリシーのターゲット デバイスがすべての非高速パスを通るトラフィックを処理する方法について決定します。後でトラフィック フローに影響する他の設定を追加します。ポリシーの作成時にポリシー ターゲットを特定する必要はありませんが、このステップを実行してからでないと、ポリシーを適用することはできません。

新しいポリシーを作成すると、次の図に示すように、追加のインスペクションなしですべてのトラフィックをブロックするか、または侵入および検出データがないかトラフィックを検査するようにデフォルト アクションを設定できます。



ヒント　最初にアクセス コントロール ポリシーを作成する場合は、デフォルト アクションとしてトラフィックを信頼するように選択することはできません。すべてのトラフィックをデフォルトで信頼する場合は、ポリシーを作成した後にデフォルト アクションを変更します。

新規のアクセス コントロール ポリシーを作成したり、既存のアクセス コントロール ポリシーを管理するには、[Access Control Policy] ページ（[Policies] > [Access Control]）を使用します。Defense Center にデバイスを登録しているか、またその登録方法によって、2 つの事前定義済みアクセス コントロール ポリシーのいずれかが表示され、デバイスにすでに適用されている場合があります。

- デフォルトのアクセス コントロール ポリシーは、追加のインスペクションなしですべてのトラフィックをブロックします。
- デフォルトの侵入防御ポリシーはすべてのトラフィックを許可しますが、Balanced Security and Connectivity 侵入ポリシーおよびデフォルトの侵入変数セットを使用して検査も実行します。

これらのアクセス コントロール ポリシーのいずれかを使用および変更できます。これらのデフォルト ポリシーではいずれも、ロギングが有効になっていないことに注意してください。

注意　アクセス コントロール ポリシーを初めて適用すると、Snort プロセスが再開され、構成変更を適用する際、一時的にトラフィック検査が中断されます。この検査中にシステムがトラフィックをドロップするか、検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、「Snort の再開によるトラフィックへの影響 (1-9 ページ)」を参照してください。

アクセス コントロール ポリシーの作成方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ヒント　この Defense Center から既存のポリシーをコピーするか、または他の Defense Center からポリシーをインポートすることもできます。ポリシーをコピーするには、コピー アイコン（ ）をクリックします。ポリシーをインポートするには、設定のインポートおよびエクスポート (A-1 ページ)を参照してください。

ステップ 2　[New Policy] をクリックします。

[New Access Control Policy] ポップアップ ウィンドウが表示されます。

ステップ 3　[Name] に一意のポリシー名を入力し、オプションで [Description] にポリシーの説明を入力します。

印刷可能なすべての文字を使用できます。これにはスペースと特殊文字も含まれますが、番号記号（#）、セミコロン（;）、または波カッコ（{}）は使用できません。名前には少なくとも 1 つのスペース以外の文字が含まれている必要があります。

ステップ 4　最初の**デフォルト アクション**を指定します。

- [Block all traffic] を選択して、[Access Control: Block All Traffic] をデフォルト アクションとして使用するポリシーを作成する
- [Intrusion Prevention] を選択して、[Intrusion Prevention: Balanced Security and Connectivity] をデフォルト アクションとして使用するポリシーを作成する
- [Network Discovery] を選択して、[Network Discovery Only] をデフォルト アクションとして使用するポリシーを作成する

最初のデフォルト アクションを選択する手順、および後でそれを変更する手順については、デフォルトの処理の設定およびネットワーク トラフィックのインスペクション（12-7 ページ）を参照してください。

ステップ 5　[Available Devices] から、ポリシーを適用するデバイスを選択します。

複数のデバイスを選択するには、Ctrl キーまたは Shift キーを押しながらクリックするか、または右クリックをして [Select All] を選択します。表示されるデバイスを絞り込むには、[Search] フィールドに検索文字列を入力します。ターゲット デバイスの追加を省略する場合は、後でそれらを追加する方法について、アクセス コントロール ポリシーのターゲット デバイスの設定（12-10 ページ）を参照してください。

ステップ 6　[Add to Policy] をクリックして、選択したデバイスを追加します。

選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 7　[Save] をクリックします。

アクセス コントロール ポリシー エディタが表示されます。新しいポリシーの設定方法については、アクセス コントロール ポリシーの編集（12-13 ページ）を参照してください。ポリシーを有効にするには適用する必要があることに注意してください。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

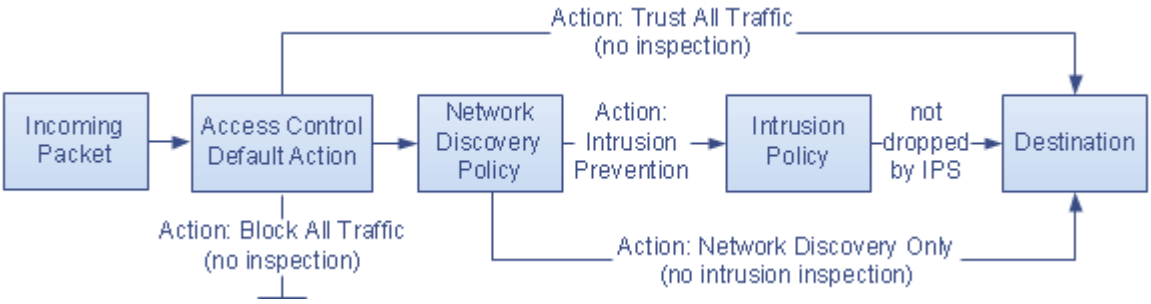
デフォルトの処理の設定およびネットワーク トラフィックのインスペクション

ライセンス： すべて

アクセス コントロール ポリシーを作成する場合は、デフォルト アクションを選択する必要があります。アクセス コントロール ポリシーのデフォルト アクションは、次のトラフィックをシステムで処理する方法を決定します。

- セキュリティ インテリジェンスによってブラックリスト登録されていないトラフィック
- SSL インスペクションによってブロックされていないトラフィック（暗号化トラフィックのみ）
- ポリシー内のルールのいずれにも一致しないトラフィック（トラフィックの照合とロギングは行うが、処理または検査はしないモニタ ルールを除く）

したがって、アクセス コントロール ルールまたはセキュリティ インテリジェンスの設定が含まれておらず、暗号化されたトラフィックの処理に SSL ポリシーを呼び出さないアクセス コントロール ポリシーを適用する場合、デフォルト アクションが、ネットワーク上のすべてのトラフィックの処理方法を決定します。追加のインスペクションなしですべてのトラフィックをブロックまたは信頼するか、または侵入および検出データがないかトラフィックを検査できます。オプションを次の図に示します。



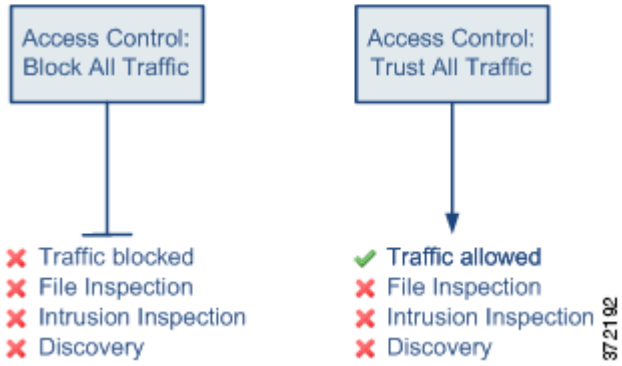
次の表に、さまざまなデフォルト アクションがトラフィックを処理する方法を示し、各デフォルト アクションで処理されるトラフィックで実行できるインスペクションのタイプを示します。デフォルト アクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行**できない**ことに注意してください。詳細については、侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（18-1 ページ）を参照してください。

:

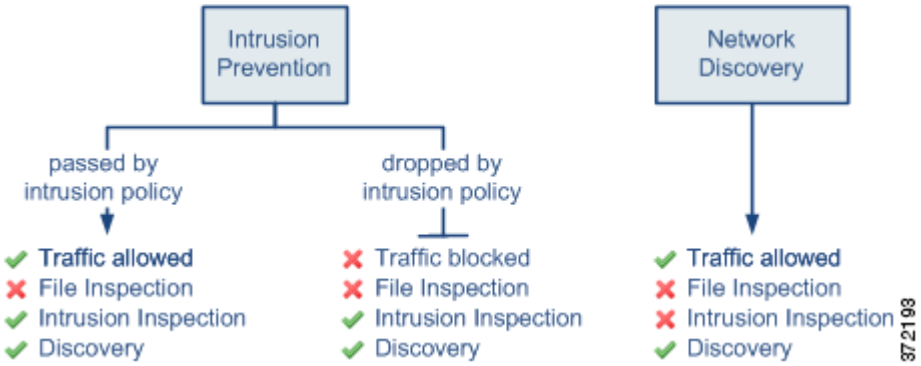
表 12-4　　アクセス コントロール ポリシーのデフォルト アクション

デフォルト アクション	トラフィックに対して行う処理	インスペクション タイプとポリシー
Access Control: Block All Traffic	それ以上のインスペクションは行わずにブロックする。	none
Access Control: Trust All Traffic	信頼（追加のインスペクションなしで最終宛先に許可）	none
Intrusion Prevention	ユーザが指定した侵入ポリシーに合格する限り、許可する（Protection が必要）	intrusion、指定した侵入ポリシーおよび関連する変数セットを使用、および discovery、ネットワーク検出ポリシーを使用
ネットワーク検出のみ	allow	discovery のみ、ネットワーク検出ポリシーを使用

次の図は、**Block All Traffic** および **Trust All Traffic** デフォルト アクションを示しています。



次の図は、[Intrusion Prevention] および [Network Discovery Only] のデフォルト アクションを説明しています。



ヒント　[Network Discovery Only] の目的は、検出のみの展開でパフォーマンスを向上させることです。侵入検知および防御のみを目的としている場合は、さまざまな設定で検出を無効にできます。従うべき他のガイドラインを含む詳細については、IPS または検出のみのパフォーマンスの考慮事項（12-22 ページ）を参照してください。

初めてアクセス コントロール ポリシーを作成する際、デフォルト アクションで処理される接続のロギングはデフォルトで無効になっています。侵入インスペクションを実行するデフォルト アクションを選択すると、システムはデフォルトの侵入変数セットを選択した侵入ポリシーに自動的に関連付けます。ポリシーを作成した後に、これらのオプションのどちらか、およびデフォルト アクション自体を変更できます。

アクセス コントロール ポリシーのデフォルト アクションと関連オプションを変更するには、次の手順を実行します。

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　設定するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3　[Default Action] を選択します。

- すべてのトラフィックをブロックする場合は、[Access Control: Block All Traffic] を選択します。
- すべてのトラフィックを信頼する場合は、[Access Control: Trust All Traffic] を選択します。
- すべてのトラフィックを許可し、ネットワーク検出を使用してインスペクションする場合は、[Network Discovery Only] を選択します。
- すべてのトラフィックをネットワーク検出と侵入ポリシーの両方を使用してインスペクションする場合は、侵入ポリシーを選択します。侵入ポリシーは、いずれも Intrusion Prevention というラベルで始まります。侵入ポリシーによってトラフィックがブロックされる可能性があることに注意してください。

注意　Ciscoの担当者から指示された場合を除き、`Experimental Policy 1` は使用**しないで**ください。Ciscoでは、試験用にこのポリシーを使用します。

ステップ 4　**侵入防御**のデフォルト アクションを選択した場合は、変数アイコン（  ）をクリックし、選択した侵入ポリシーに関連付けられている変数セットを変更します。

表示されるポップアップ ウィンドウで、新しい変数セットを選択して [OK] をクリックします。編集アイコン（  ）をクリックして、新しいウィンドウで設定されている変数セットを編集することもできます。変数セットを変更しない場合は、システムはデフォルトのセットを使用します。詳細については、変数セットの操作（3-19 ページ）を参照してください。

ステップ 5　ロギング アイコン（  ）をクリックして、デフォルト アクションによって処理される接続のロギング オプションを変更します。

デフォルト アクションによっては、一致する接続の開始、終了、またはその両方でロギングできます。接続のログは、Defense Center データベース、外部のシステム ログ（Syslog）または SNMP トラップ サーバに記録できます。詳細については、アクセス コントロールのデフォルト アクションによって処理された接続のロギング（38-19 ページ）を参照してください。

アクセス コントロール ポリシーのターゲット デバイスの設定

ライセンス： すべて

アクセス コントロール ポリシーを適用するには、その前に、ポリシーを適用する管理対象デバイスを特定する必要があります。ポリシーを適用するデバイスは、ポリシーの作成時に特定できます。または、後で追加することもできます。

次の表では、対象のデバイスを管理する場合に実行可能な操作の概要を説明しています。

表 12-5　対象のデバイス管理アクション

目的	操作
使用可能なデバイスのリストを検索する	検索フィールド内をクリックし、検索文字列を入力します。検索文字列を入力すると、デバイスのリストが更新されて、検索文字列に一致するデバイス名が表示されます。
使用可能なデバイスの検索をクリアする	検索フィールドのクリア アイコン（  ）をクリックします。

表 12-5　対象のデバイス管理アクション（続き）

目的	操作
使用可能なデバイスを選択し、選択済みターゲットのリストに追加する	デバイス名をクリックします。複数のデバイスを選択するには、Ctrl キーまたは Shift キーを押しながらクリックします。使用可能なデバイスを右クリックして、[Select All] をクリックすることもできます。
選択したデバイスを追加する	[Add to Policy] をクリックするか、または選択されたデバイスのリストにドラッグ アンド ドロップします。
選択済みデバイスのリストから単一のデバイスを削除する	デバイスの横にある削除アイコン（）をクリックするか、またはデバイスを右クリックし、[Delete] を選択します。
選択済みデバイスのリストから複数のデバイスを削除する	Ctrl キーまたは Shift キーを押しながら複数のデバイスをクリックして選択したら、選択したデバイスの行を右クリックして強調表示し、次に [Delete Selected] をクリックします。

異なるバージョンのシステムを実行中のスタック デバイスをターゲットにすることはできません（たとえば、デバイスのいずれかでアップグレードが失敗した場合）。デバイス スタックをターゲットにすることはできますが、スタック内の個々のデバイスをターゲットにすることはできません。詳細については、「スタックに含まれるデバイスの管理（4-46 ページ）」を参照してください。

アクセス コントロール ポリシーのターゲット デバイスを管理する方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　設定するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3　デバイス ターゲットのリンクをクリックし、[Manage Targets] をクリックします。

[Manage Device Targets] ポップアップ ウィンドウが表示されます。

ステップ 4　ターゲット リストを作成します。

表 12-5（12-10 ページ） に要約されているアクションを使用します。

ステップ 5　[OK] をクリックします。

設定がポリシーに追加され、アクセス コントロール ポリシー エディタが表示されます。

アクセス コントロール ポリシーの管理

ライセンス： すべて

[Access Control Policy] ページ（[Policies] > [Access Control]）で、現在のカスタム アクセス コントロール ポリシーを次の情報とともに（適切な場合）表示できます。

- トラフィックの検査に各アクセス コントロール ポリシーを使用しているデバイスの数。ポリシーがそのターゲットの一部にのみ適用されているか、またはそのポリシーが現在ターゲットとしていないデバイスに適用されているかに関する情報も含まれます。
- 各ポリシーが失効しているターゲット デバイスの数、および各ポリシーを現在編集している人に関する情報（いる場合）

作成したカスタム ポリシーに加えて、システムによって 3 つのカスタム ポリシー（デフォルトのアクセス コントロール ポリシー、デフォルトの侵入防御ポリシー、およびデフォルトのネットワーク検出ポリシー）が提供される場合があります。初期設定時にデバイスで選択した検出モードに応じて、システムは最初のデバイス登録時にこれらのポリシーを作成します。これらのシステム付属のカスタム ポリシーは編集して使用できます。デバイスの検出モードはユーザが後から変更できない設定で、設定時にユーザが選択するだけのオプションです。このオプションの選択により、システムはデバイスの初期設定を調整することができます。

[Access Control Policy] ページ上のオプションを使用して、次の表にあるアクションを実行できます。

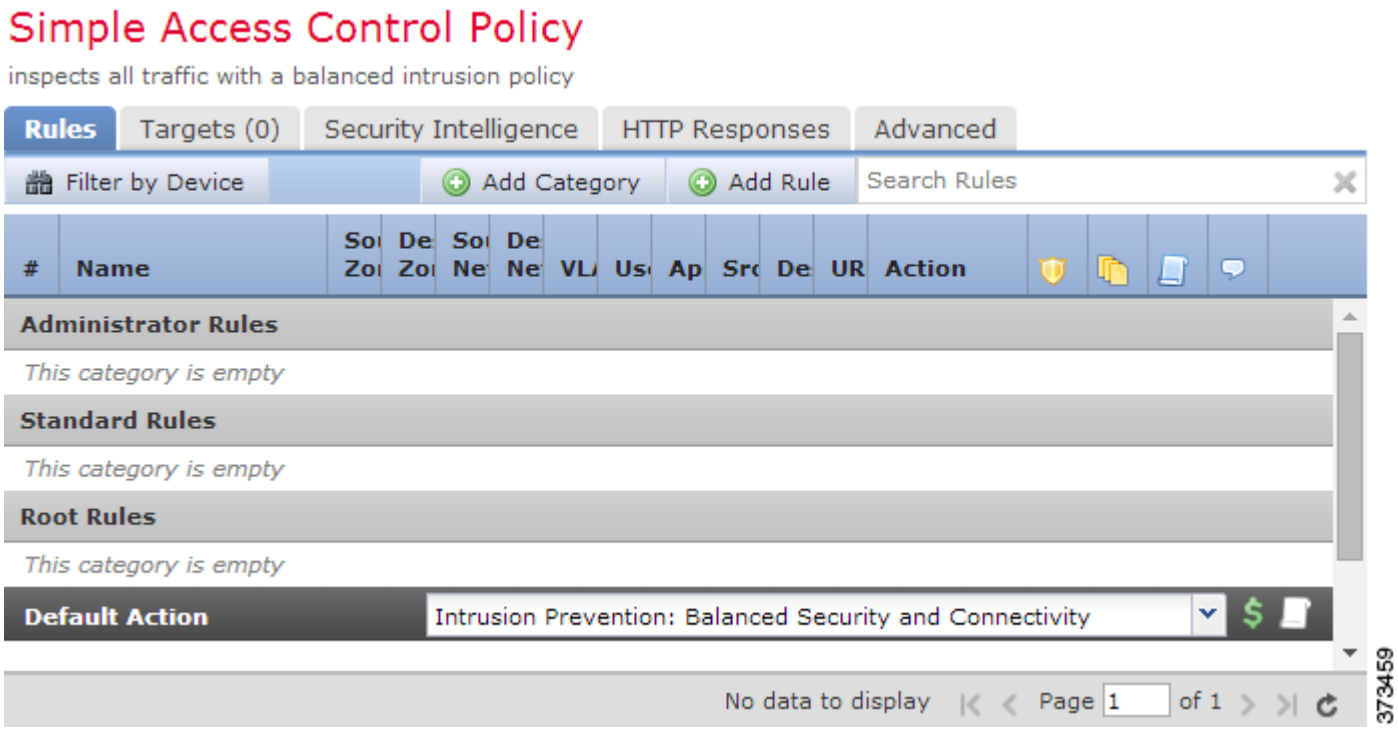
表 12-6　　アクセス コントロール ポリシーの管理操作

目的	操作	参照先
新しいアクセス コントロール ポリシーを作成する	[New Policy] をクリックします。	基本的なアクセス コントロール ポリシーの作成（12-5 ページ）
既存のアクセス コントロール ポリシーを編集する	編集アイコン（）をクリックします。	アクセス コントロール ポリシーの編集（12-13 ページ）
アクセス コントロール ポリシーを管理対象デバイスに再適用する	適用アイコン（  ）をクリックします。	アクセス コントロール ポリシーの適用（12-17 ページ）
アクセス コントロール ポリシーをエクスポートして別の Defense Center にインポートする	エクスポート アイコン（  ）をクリックします。	設定のエクスポート（A-1 ページ）
アクセス コントロール ポリシーの現行の設定をリストする PDF レポートを表示する	レポート アイコン（  ）をクリックします。	現在のアクセス コントロール設定のレポートの生成（12-29 ページ）
アクセス コントロール ポリシーを比較する	[Compare Policies] をクリックします。	アクセス コントロール ポリシーの比較（12-30 ページ）
アクセス コントロール ポリシーを削除する	削除アイコン（  ）をクリックし、ポリシーを削除することを確認します。適用されたアクセス コントロール ポリシーまたは現在適用しているアクセス コントロール ポリシーは削除できません。	

アクセス コントロール ポリシーの編集

ライセンス： すべて

新しいアクセス コントロール ポリシーを初めて作成する場合、アクセス コントロール ポリシー エディタが表示され、[Rules] タブに焦点が置かれています。次の図に、新しく作成されたポリシーを示します。新しいポリシーにはルールやその他の設定がまだ存在しないため、デフォルト アクションはすべてのトラフィックを処理します。この場合、デフォルト アクションは、暗号化されていないトラフィックを最終宛先に許可する前に、システムが提供する Balanced Security and Connectivity 侵入ポリシーを使用して検査します。デフォルトでは、システムは暗号化されたペイロードでファイルおよび侵入のインスペクションを無効にすることに注意してください。



ルールの追加および整理、ポリシーを使用するデバイスの指定などを行うには、アクセス コントロール ポリシー エディタを使用します。次のリストでは、変更可能なポリシー設定に関する情報を提供します。

名前と説明

ポリシーの名前と説明を変更するには、該当するフィールドをクリックし、新しい名前または説明を入力します。

ターゲット

アクセス コントロール ポリシーを適用するには、その前に [Targets] タブを使用して、ポリシーを適用する管理対象デバイス（デバイス グループを含む）を特定します。詳細については、アクセス コントロール ポリシーのターゲット デバイスの設定（12-10 ページ）を参照してください。

セキュリティ インテリジェンス

セキュリティ インテリジェンスは、悪意のあるインターネット コンテンツに対する最初の防御ラインです。この機能を使用して、最新のレピュテーション インテリジェンスに基づいて接続を即座にブラックリスト登録(ブロック)することができます。重要なリソースへの継続的なアクセスを確保するために、ブラックリストをカスタム ホワイトリストで上書きできます。このトラフィック フィルタリングは、ルールやデフォルト アクションを含む、他のどのポリシー ベースのインスペクション、分析、またはトラフィック処理よりも**先に**行われます。詳細については、セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録(13-1 ページ)を参照してください。

ルール

ルールでは、ネットワーク トラフィックを処理する詳細な方法が提供されます。アクセス コントロール ポリシー内の各ルールには、1 から始まる番号が付きます。システムは、ルール番号の昇順で先頭から順にアクセス コントロール ルールをトラフィックと照合します。

ほとんどの場合、システムは、*すべて*のルールの条件がトラフィックに一致する場合、*最初の*アクセス コントロール ルールに従ってネットワーク トラフィックを処理します。これらの条件には、セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、またはユーザが含まれています。条件は単純または複雑にできます。条件の使用は特定のライセンスおよびアプライアンス モデルによって異なります。

ルールを追加、分類、有効化、無効化、フィルタリング、または管理するには、[Rules] タブを使用します。詳細については、アクセス コントロール ルールを使用したトラフィック フローの調整(14-1 ページ)を参照してください。

Default Action

デフォルト アクションは、セキュリティ インテリジェンスによってブラックリスト登録されず、いずれのアクセス コントロール ルールにも一致しないトラフィックをシステムが処理する方法を決定します。デフォルト アクションを使用して、追加のインスペクションなしですべてのトラフィックをブロックまたは信頼でき、または侵入および検出データがないかトラフィックを検査できます。また、カスタム変数セットを作成している場合はそれを選択し、デフォルト アクションによって処理される接続のロギングを有効または無効にできます。

詳細については、デフォルトの処理の設定およびネットワーク トラフィックのインスペクション(12-7 ページ)およびアクセス コントロールの処理に基づく接続のロギング(38-17 ページ)を参照してください。

HTTP 応答

ユーザの Web サイト要求をシステムがブロックした場合にブラウザに表示するものを指定できます。一般的なシステムによって提供される応答ページを表示するか、カスタム HTML を入力するかを指定できます。ユーザに警告するページを表示することもできますが、ユーザはボタンをクリックして最初に要求されたサイトをロードするためにページの続行または更新を行うことも可能です。詳細については、ブロックされた URL のカスタム Web ページの表示(16-20 ページ)を参照してください。

アクセス コントロールの詳細オプション

通常、アクセス コントロール ポリシーの詳細設定を変更する必要はほとんど、あるいはまったくありません。ほとんどの展開環境には、デフォルト設定が適切です。変更できる詳細設定には次のものがあります。

- ユーザが要求した各 URL に対し、Defense Center データベースに保存する文字数。接続で検出された URL のロギング(38-21 ページ)を参照してください。

- ユーザが最初のブロックをバイパスした後に Web サイトを再度ブロックするまでの時間間隔。ブロックされた Web サイトのユーザ バイパス タイムアウトの設定（16-19 ページ）を参照してください。
- セキュア ソケット レイヤ（SSL）または Transport Layer Security（TLS）で暗号化されたアプリケーション層プロトコル トラフィックをモニタ、復号化、ブロック、または許可する SSL ポリシー。アクセス コントロールを使用した復号化設定の適用（20-9 ページ）を参照してください
- ポリシー適用時にトラフィック インスペクションを許可する、またはセキュアな接続に対するトラフィック インスペクションを無効にする。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください
- ネットワーク分析ポリシーおよび侵入ポリシーの設定。この設定では、ネットワーク、ゾーン、および VLAN に対する多くの前処理オプションを調整し、デフォルトの侵入インスペクション動作を設定できます。トラフィックの前処理のカスタマイズ（25-1 ページ）を参照してください。
- トランスポートおよびネットワークのプリプロセッサの詳細設定。この設定は、アクセス コントロール ポリシーを適用するすべてのネットワーク、ゾーン、および VLAN にグローバルに適用されます。トランスポート/ネットワークの詳細設定の構成（29-2 ページ）を参照してください。
- ユーザのネットワークのホスト オペレーティング システムに基づいて、パッシブ展開でパケット フラグメントおよび TCP ストリームの再構成を改善する適応型プロファイル。パッシブ展開における前処理の調整（30-1 ページ）を参照してください。
- 侵入インスペクション、ファイル制御、ファイル ストレージ、ダイナミック分析、および高度なマルウェア防御のパフォーマンス オプション。侵入防御パフォーマンスの調整（18-10 ページ）および ファイルおよびマルウェアのインスペクション パフォーマンスおよびストレージの調整（18-22 ページ）を参照してください。

アクセス コントロール ポリシーを編集すると、変更がまだ保存されていないことを示すメッセージが表示されます。変更を維持するには、ポリシー エディタを終了する前にポリシーを保存する必要があります。変更を保存しないでポリシー エディタを終了しようとすると、変更がまだ保存されていないことを警告するメッセージが表示されます。この場合、変更を破棄してポリシーを終了するか、ポリシー エディタに戻るかを選択できます。

セッションのプライバシーを保護するために、ポリシー エディタで 60 分間操作が行われないと、ポリシーの変更が破棄されて、[Access Control Policy] ページに戻されます。30 分間操作が行われなかった時点で、変更が破棄されるまでの分数を示すメッセージが表示されます。以降、このメッセージは定期的に更新されて残りの分数を示します。ページで何らかの操作を行うと、タイマーがキャンセルされます。

2 つのブラウザ ウィンドウで同じポリシーを編集しようとすると、新しいウィンドウで編集を再開するか、元のウィンドウでの変更を破棄して新しいウィンドウで編集を続ける か、または 2 番目のウィンドウをキャンセルしてポリシー エディタに戻るかを選択するよう求めるプロンプトが出されます。

複数のユーザが同じポリシーを同時に編集する際、各ユーザに対し、ポリシー エディタに変更を保存していない他のユーザを特定するメッセージが表示されます。いずれかのユーザが変更を保存しようとすると、その変更によって他のユーザの変更が上書きされることを警告するメッセージが表示されます。同一のポリシーを複数のユーザが保存する場合、最後に保存された変更が維持されます。

アクセス コントロール ポリシーの編集方法:

アクセス: Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　設定するアクセス コントロール ポリシーの横にある編集アイコン( )をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3　ポリシーを編集します。上記で要約されたアクションのいずれかを実行します。

ステップ 4　設定を保存または廃棄します。

- 変更を保存し、編集を続行する場合は、[Save] をクリックします。
- 変更を保存し、ポリシーを適用する場合は、[Save and Apply] をクリックします。アクセス コントロール ポリシーの適用(12-17 ページ)を参照してください。
- 変更を廃棄する場合は、[Cancel] をクリックし、プロンプトが出たら [OK] をクリックします。

失効したポリシーの警告について

ライセンス: すべて

[Access Control Policy] ページ([Policies] > [Access Control])で、失効したポリシーには、ポリシーの更新に必要なターゲット デバイスの数を示した赤色のステータス テキストが付いています。

ほとんどの場合、アクセス コントロール ポリシーを変更した場合は、変更を有効にするために再度適用する必要があります。アクセス コントロール ポリシーが他のポリシーを呼び出したり、または他の設定に依存する場合、それらを変更すると、アクセス コントロール ポリシーを再度適用する必要があります(または、侵入ポリシーの変更の場合は、侵入ポリシーだけを再度適用できます)。

ポリシーの再適用が必要な設定変更には次のものがあります。

- アクセス コントロール ポリシー自体の変更:アクセス コントロール ルール、デフォルト アクション、ポリシー ターゲット、セキュリティ インテリジェンス フィルタリング、NAP ルールなどの詳細オプションの変更。
- アクセス コントロール ポリシーが呼び出すポリシーの変更:SSL ポリシー、ネットワーク分析ポリシー、侵入ポリシー、およびファイル ポリシー。
- アクセス コントロール ポリシーで使用される再利用可能なオブジェクトまたは設定、またはアクセス コントロール ポリシーが呼び出すポリシーの変更:ネットワーク、ポート、VLAN タグ、URL、および位置情報オブジェクト、セキュリティ インテリジェンスのリストとフィード、アプリケーション フィルタまたはディテクタ、侵入ポリシーの変数セット、ファイル リスト、復号化関連オブジェクト、セキュリティ ゾーンなど。
- システム ソフトウェア、侵入ルール、または脆弱性データベース(VDB)の更新。

Web インターフェイスの複数の場所からこれらの設定の一部を変更できることに留意してください。たとえば、オブジェクト マネージャ([Objects] > [Object Management])を使用してセキュリティ ゾーンを変更できますが、デバイスの設定([Devices] > [Device Management])でインターフェイスのタイプを変更すると、ゾーンも変更され、ポリシーの再適用が必要になります。

次の更新では、ポリシーの再適用は必要**ありません**。

- セキュリティ インテリジェンス フィードへの自動更新およびコンテキスト メニューを使用したセキュリティ インテリジェンスのグローバル ブラックリストおよびホワイトリストへの追加
- URL フィルタリング データへの自動更新
- スケジュールされた位置情報データベース（GeoDB）の更新

アクセス コントロールまたは侵入ポリシーが失効した理由を確認するには、比較ビューアを使用します。

アクセス コントロール ポリシーが失効した理由を確認するには、次の手順を実行します。

アクセス： Admin/Security Approver

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。失効したポリシーには、ポリシーの更新を必要とするターゲット デバイスの数を示した赤色のステータス テキストが付いています。

ステップ 2　失効したポリシーのポリシー ステータスをクリックします。

詳細な [Apply Access Control Policy] ポップアップ ウィンドウが表示されます。

ステップ 3　該当する変更されたコンポーネントの横にある [Out-of-date] をクリックします。

ポリシーの比較レポートが新しいウィンドウに表示されます。詳細については、アクセス コントロール ポリシーの比較（12-30 ページ）および2 つの侵入ポリシーまたはリビジョンの比較（31-11 ページ）を参照してください。

ステップ 4　オプションで、ポリシーを再度適用します。

次の項、アクセス コントロール ポリシーの適用を参照してください。

アクセス コントロール ポリシーの適用

ライセンス： すべて

アクセス コントロール ポリシーを変更した後、そのポリシーを 1 つ以上のターゲット デバイスに適用することで、デバイスがモニタ対象とするネットワークでその変更を実装できます。アクセス コントロール ポリシーおよび関連する侵入ポリシーは任意の組み合わせで適用することができますが、アクセス コントロール ポリシーを適用すると、そのポリシーに関連付けられたすべての SSL ポリシー、ネットワーク分析ポリシー、およびファイル ポリシーが自動的に適用されます。これらのポリシーを個別に適用することはできません。

注意　アクセス コントロール ポリシーを適用した場合、リソースを要求すると、いくつかのパケットが検査なしでドロップされることがあります。さらに、構成の一部を適用するときに、Snort プロセスの再開が要求され、これにより一時的にトラフィック検査が中断されます。この検査中にトラフィックがドロップされるか、それ以上検査が行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。Snort プロセスを再開する構成（1-8 ページ）を参照してください。

ヒント インラインで Cisco NGIPS for Blue Coat X-Series を配置していて、ロード バランシングおよび冗長性のためにマルチ VAP VAP グループを設定している場合、デバイスが再起動するまで影響を受ける VAP をロード バランス リストから削除し、再起動した後に再インストールすることで、処理の中断を防ぐことができます。

インライン展開されたデバイスだけがトラフィックのフローに影響を与える場合があることに注意してください。トラフィックをブロックまたは変更するように設定されたアクセス コントロール ポリシーをパッシブに展開されたデバイスに適用すると、予期しない結果になることがあります。たとえば、ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

場合によっては、タップ モードのインライン デバイスを含むパッシブに展開されたデバイスにインライン設定を適用することがシステムによって阻害されます。たとえば、パッシブ展開では、暗号化されたトラフィックをブロックする SSL ポリシー、または復号化されたトラフィックに再署名するよう設定された SSL ポリシーを参照するアクセス コントロール ポリシーを適用することはできません。またパッシブ展開では、一時 Diffie-Hellman（DHE）および楕円曲線 Diffie-Hellman（ECDHE）暗号スイートを使った暗号化トラフィックの復号化をサポートしていません。

アクセス コントロール ポリシーを適用する際には、次の点に注意してください。

- 一部の機能には、特定のライセンス、最小バージョンのシステム、または特定のデバイス モデルが必要です。詳細については、アクセス コントロールのライセンスおよびモデルの要件（12-3 ページ）と、管理対象デバイスで実行しているシステムのバージョンのリリース ノートを参照してください。アクセス コントロール ポリシーに、最近適用されたデバイス設定によって有効になるライセンスが必要な場合、システムはそのデバイス設定の適用が完了するまで、アクセス コントロール ポリシー適用タスクをキューに入れます。
- 異なるバージョンのシステムを実行しているスタック デバイスにアクセス コントロール ポリシーを適用することはできません（たとえば、デバイスの 1 つでアップグレードが失敗した場合など）。
- アクセス コントロール ポリシーを適用すると、システムはすべてのルールをまとめて評価し、ネットワーク トラフィックを評価するためにターゲット デバイスが使用する条件の拡張セットを作成します。ターゲット デバイスでサポートされるアクセス コントロール ルールまたは侵入ポリシーの最大数を超えていることを警告するポップアップ ウィンドウが表示される場合があります。この最大値は、デバイスの物理メモリやプロセッサ数などの、さまざまな要因によって異なります。コンピューティング リソースが少ないデバイスでは、制限されたメモリには、アクセス コントロール ポリシー全体で侵入ポリシーを 3 つしか選択できない場合があることに注意してください。詳細については、パフォーマンスを向上させるためのルールの簡素化（12-26 ページ）を参照してください。
- アプリケーション制御を実行する場合は、アクセス コントロール ルールまたは SSL ルールで条件として使用するアプリケーションごとに少なくとも 1 つのディテクタを有効にする必要があります。有効になっているディテクタがないアプリケーションについては、システム提供のすべてのディテクタが自動的に有効になります。ディテクタが存在しない場合は、そのアプリケーションについて最後に変更されたユーザ定義ディテクタが有効になります。
- 侵入ルール更新をインポートすると、インポートの完了後にアクセス コントロール ポリシーおよび侵入ポリシーを自動的に再適用できます。これにより、最新の侵入ルールおよび詳細設定だけでなく、プリプロセッサ ルールおよびプリプロセッサ設定を使用できます。これは、ルールの更新によってシステムにより提供される基本ポリシーが変更されることを許可する場合に特に役立ちます。また、ルールの更新によって、アクセス コントロール ポリ

シーの高度な前処理およびパフォーマンスのオプションのデフォルト値を変更することもできます。詳細については、ルールの更新とローカル ルール ファイルのインポート（66-16 ページ）を参照してください。

- メモリが制限されているデバイスでは、侵入ポリシーの数が、複数の変数セットとペアにならない可能性があります。1 つの侵入ポリシーのみを参照するアクセス コントロール ポリシーを適用できる場合は、この侵入ポリシーに対するすべての参照が、同一の変数セットとペアになっていることを確認してください。

詳細については、次の項を参照してください。

- 完全なポリシーの適用（12-19 ページ）では、クイック適用オプションを使用して、アクセス コントロール ポリシーを関連するすべての SSL ポリシー、ネットワーク分析ポリシー、侵入ポリシー、およびファイル ポリシーと併せて適用する方法について説明しています。
- 選択したポリシーの設定の適用（12-20 ページ）では、個々の侵入ポリシーを含む、特定のアクセス コントロール ポリシーを適用する方法について説明しています。

完全なポリシーの適用

ライセンス： すべて

サポートされるデバイス：

アクセス コントロール ポリシーは、任意の時点でターゲット デバイスに適用することができます。アクセス コントロール ポリシーを適用すると、現在実行しているものとは異なる関連付けられたポリシーも適用されます。

- SSL ポリシー
- ネットワーク分析ポリシー
- 侵入ポリシー
- ファイル ポリシー

単一のクイック適用操作として、ポップアップ ウィンドウを使用してすべてのポリシーをまとめて適用することができます。クイック適用オプションを使用する場合、変更されていないポリシーは適用されません。

クイック適用ポップアップ ウィンドウの適用ボタンのラベルは、アクセス コントロール ポリシー、侵入ポリシー、またはその両方の適用を許可されているかによって異なります。カスタム ユーザ ロールによる展開の管理（12-4 ページ）を参照してください。

完全なアクセス コントロール ポリシーのクイック適用を実行するには、次の手順を実行します。

アクセス： Admin/Security Approver

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　適用するポリシーの横にある適用アイコン（ ）をクリックします。

[Apply Access Control Policy] ポップアップ ウィンドウが表示されます。

または、ポリシーの編集中に [Save and Apply] をクリックできます。アクセス コントロール ポリシーの編集（12-13 ページ）を参照してください。

ステップ 3　[Apply All] をクリックします。

ポリシー適用タスクがキューに入れられます。[OK] をクリックして [Access Control Policy] ページに戻ります。ポリシー適用タスクの進行状況は、[Task Status] ページ（[System] > [Monitoring] > [Task Status]）でモニタできます。

選択したポリシーの設定の適用

ライセンス： すべて

ポリシー適用の詳細ページを使用して、アクセス コントロール ポリシーや関連する侵入ポリシーに変更を適用できます。詳細ページには、ポリシーがターゲットとするデバイスがリストされ、デバイス別のアクセス コントロール ポリシーおよびそれに関連付けられた侵入ポリシーの各カラムが表示されます。ターゲット デバイスごとに、変更をアクセス コントロール ポリシー、個々の侵入ポリシーまたはその組み合わせ、あるいはその両方に適用するかどうかを指定できます。

次の場合には、アクセス コントロール ポリシーとそれに関連付けられた侵入ポリシーの両方を適用する必要があります。

- アクセス コントロール ポリシーが初めてデバイスに適用される場合
- アクセス コントロール ポリシーに新しく侵入ポリシーが追加される場合

いずれの場合も、アクセス コントロール ポリシーの状態と侵入ポリシーの状態はリンクされます。つまり、両方とも適用するか、どちらも適用しないかのいずれかを選択する必要があります。

どの侵入ポリシーを適用するかに関わらず、アクセス コントロール ポリシーを適用すると、そのポリシーがターゲットとするデバイスで現在実行されているものとは別の関連付けられているすべての SSL ポリシー、ネットワーク分析ポリシー、およびファイル ポリシーが自動的に適用されます。これらのポリシーを個別に適用することはできません。

[Access Control Policy] カラム

[Access Control Policy] カラムには、アクセス コントロール ポリシーを適用するかどうかを指定するチェック ボックスがあります。

ヒント　タスク キューにまだ入っているポリシー、つまり適用タスクがまだ完了していないポリシーを再び適用することもできますが、それには何の利点もありません。

ステータス メッセージには、ポリシーが現在最新の状態であるか、失効しているかどうかが示されます。ポリシーが失効している場合は、新しいブラウザ ウィンドウで、そのポリシーと現在実行中のポリシーとの比較結果を表示できます。この比較には、アクセス コントロール ポリシーに関連付けられている侵入ポリシーでの差異は含まれません。

[Intrusion Policies] カラム

[Intrusion Policies] カラムには、アクセス コントロール ポリシーに関連付けられている侵入ポリシーをデバイスに適用するかどうかを指定する 1 つ以上のチェック ボックスがあります。単一のグレー表示されたチェック ボックスは、関連付けられているすべての侵入ポリシーが、現在実行されているポリシーと同じであることを意味します。この場合、チェック ボックスはクリアされていて、選択することはできません。変更されていない侵入ポリシーを適用することはできま

せん。このカラムには、変更されている侵入ポリシーだけがリストされ、個別に選択できるようになっています。ポリシーに含まれる複数のルールに同じ侵入 ポリシーが関連付けられている場合、その侵入ポリシーはデバイスごとに一度だけリストされます。

前述したようにアクセス コントロール ポリシーと侵入ポリシーを一緒に適用しなければならない場合、侵入ポリシーのチェック ボックスは選択された状態でグレー表示され、変更することができません。これに該当するのは次のような場合です。

- アクセス コントロール ポリシーが初めてデバイスに適用される場合
- アクセス コントロール ポリシーに新しく侵入ポリシーが追加される場合

ステータス メッセージには、侵入ポリシーが現在最新の状態であるか、失効しているかどうかが示されます。侵入ポリシーが、リストされたデバイスで現在実行されている侵入ポリシーと同じでない場合、その侵入ポリシーは失効していることになります。侵入ポリシーがデバイス上の侵入ポリシーとまったく同じであれば、その侵入ポリシーは最新の状態です。ポリシーが失効している場合は、新しいブラウザ ウィンドウで、そのポリシーと現在実行中のポリシーとの比較結果を表示できます。

選択したアクセス コントロール ポリシー設定を適用する方法:

アクセス: Admin/Security Approver

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　適用するポリシーの横にある適用アイコン( )をクリックします。

[Apply Access Control Policy] ポップアップ ウィンドウが表示されます。

または、ポリシーの編集中に [Save and Apply] をクリックできます。アクセス コントロール ポリシーの編集（12-13 ページ）を参照してください。

ステップ 3　[Details] をクリックします。

詳細な [Apply Access Control Policy] ポップアップ ウィンドウが表示されます。このポップアップ ウィンドウは、[Access Control Policy] ページ（[Policies] > [Access Control]）から開くこともできます。それには、ポリシーの [Status] カラムに示されている失効メッセージをクリックします。

ステップ 4　デバイス名の横にあるアクセス コントロール ポリシーのチェック ボックスを選択するかクリアにして、アクセス コントロール ポリシーをターゲット デバイスに適用するかどうかを指定します。

ステップ 5　デバイス名の横にある侵入ポリシーのチェック ボックスを選択するかクリアして、侵入ポリシーをターゲット デバイスに適用するかどうかを指定します。

ステップ 6　[Apply Selected Configurations] をクリックします。

ポリシー適用タスクがキューに入れられます。[OK] をクリックして [Access Control Policy] ページに戻ります。

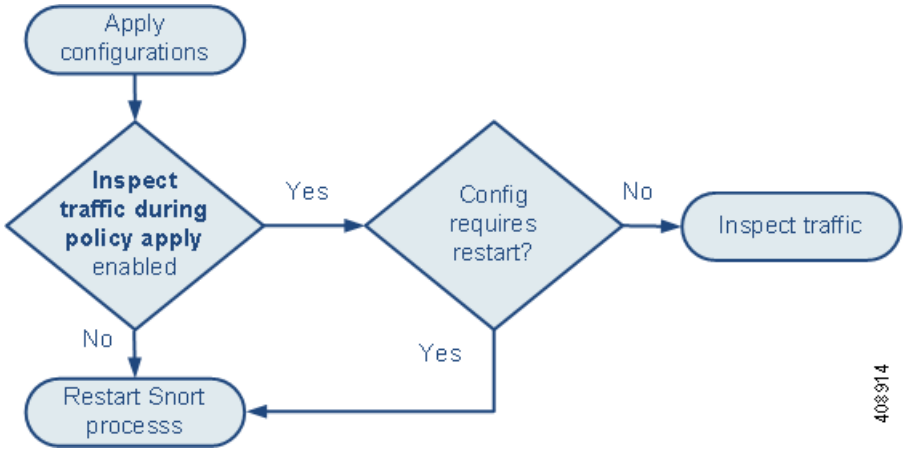
デバイスでサポートされる侵入ポリシーの最大数を超えていることを警告するポップアップ ウィンドウが表示される場合があることに注意してください。アクセス コントロール ポリシーを再評価し、侵入ポリシーを統合する必要があります。関連付けられている侵入ポリシーの数（デフォルト アクションを含む）が最大値以内に収まるまで、アクセス コントロール ポリシーは適用できません。

ポリシー適用タスクの進行状況は、[Task Status] ページ（[System] > [Monitoring] > [Task Status]）でモニタできます。

アクセス コントロール ポリシー適用中のトラフィック検査

次の図は、拡張アクセス コントロール ポリシー オプション [Inspect traffic during policy apply] を有効または無効にしたときに Snort プロセスがどのように再開されるかを示しています。

注意 Snort プロセスを再開すると、一時的にトラフィック検査が中断されます。この中断中に、トラフィックがドロップされるか、検査なしで受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。Snort プロセスを再開する構成（1-8 ページ）を参照してください。



次の点に注意してください。

- [Inspect traffic during policy apply] を有効にした場合は、次のようになります。
  - 一部の構成で、Snort プロセスの再開が要求されることがあります。
  - 適用した構成で Snort の再開が要求されない場合、システムはまず最初に、現在適用されているアクセス コントロール ポリシーを使用してトラフィックを検査し、アプリケーション プロセス中に、適用されたポリシーに切り替えます。
- [Inspect traffic during policy apply] を無効にすると、ポリシーを適用する際に必ず Snort プロセスが再開されます。
- Snort の再開がトラフィックにどのように影響するかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

IPS または検出のみのパフォーマンスの考慮事項

ライセンス： FireSIGHT または Protection

FireSIGHT ライセンスは Defense Center に含まれており、ホスト、アプリケーション、およびユーザ検出を実行できます。検出データを使用して、システムはネットワークの完全な最新プロファイルを作成できます。管理対象デバイスに適用されている Protection ライセンスを使用して、システムは侵入検知と侵入防御システム（IPS）として機能できます。侵入とエクスプロイトの有無についてネットワーク トラフィックを分析できます。またオプションで違反パケットをドロップできます。

検出と IPS を組み合わせることで、ネットワーク アクティビティにコンテンツが提供され、次のような多くの機能を利用することができます。

- 侵害の影響フラグと表示。これによって、どのホストが特定のエクスプロイト、攻撃、またはマルウェアに対して脆弱であるかが示されます。
- 適応型プロファイルと FireSIGHT の推奨事項。これを使用して、宛先ホストに応じてトラフィックを個別に検査できます。
- 相関。これによって、影響を受けるホストに応じて別々に侵入（およびその他のイベント）に応答できます。

ただし、組織が IPS または検出のみを実行することを目的としている場合は、次の項に示すように、システムのパフォーマンスを最適化できる設定がいくつかあります。

- ネットワーク検出のみの展開の最適化（12-23 ページ）
- 検出なしの侵入検知と防御の実行（12-24 ページ）

ネットワーク検出のみの展開の最適化

ライセンス： FireSIGHT

*検出*機能では、ネットワーク トラフィックをモニタして、ネットワーク上のホストの数とタイプ（ネットワーク デバイスを含む）だけでなく、それらのホスト上のオペレーティング システム、アクティブなアプリケーション、およびオープン ポートを判断できます。管理対象デバイスとユーザ エージェントをネットワークのユーザ アクティビティをモニタするように設定することもできます。検出データを使用して、トラフィック プロファイリングを実行し、ネットワーク コンプライアンスを評価し、ポリシー違反に応答できます。

基本的な展開（検出と単純なネットワークベースのアクセス制御のみ）では、アクセス コントロール ポリシーの設定時にいくつかの重要なガイドラインに従うことで、デバイスのパフォーマンスを向上させることができます。

注　それが単にすべてのトラフィックを許可する場合であっても、アクセス コントロール ポリシーを適用する必要があります。ネットワーク検出ポリシーが実行できるのは、アクセス コントロール ポリシーが通過を許可したトラフィックを検査することのみです。

最初に、アクセス コントロール ポリシーは複雑な処理を必要とせず、単純なネットワークベースの基準のみを使用してネットワーク トラフィックを処理することを確認します。次のすべてのガイドラインを実装する必要があります。これらのオプションのいずれかを誤って設定すると、パフォーマンス上の利点がなくなります。

- セキュリティ インテリジェンス機能を使用しないでください。入力されたグローバル ホワイトリストまたはブラックリストをポリシーのセキュリティ インテリジェンスの設定から削除します。
- モニタ アクションまたはインタラクティブ ブロック アクションにアクセス コントロール ルールを含めないでください。許可、信頼、およびブロック ルールのみを使用します。許可されたトラフィックは検出によって検査できますが、信頼されたトラフィックとブロックされたトラフィックは検査できないことに留意してください。
- デバイスが適切にライセンス済みであっても、アプリケーション、ユーザ、URL、または位置情報ベースのネットワーク条件にアクセス コントロール ルールを含めないでください。単純なネットワークベースの条件（ゾーン、IP アドレス、VLAN タグ、およびポート）のみを使用します。

- デバイスが適切にライセンス済みであっても、ファイル、マルウェア、または侵入のインスペクションを実行するアクセス コントロール ルールを含めないでください。つまり、ファイル ポリシーまたは侵入ポリシーをアクセス コントロール ルールに関連付けないでください。
- アクセス コントロール ポリシーのデフォルトの侵入ポリシーが [No Rules Active] に設定されていることを確認します。アクセス コントロールのデフォルト侵入ポリシーの設定（25-1 ページ）を参照してください。
- ポリシーのデフォルト アクションとして [Network Discovery Only] を選択します。侵入インスペクションを実行するポリシーのデフォルト アクションを選択しないでください。

位置情報ベースのアクセス制御を除き、上記のオプションには少なくとも 1 つの Protection ライセンスが必要であることに注意してください。FireSIGHT ライセンスが 1 つだけある場合、これらの機能を使用したアクセス コントロール ポリシーの適用がシステムによって阻害されます。

アクセス コントロール ポリシーを設定して適用した後、ネットワーク検出ポリシーを設定して適用できます。このポリシーは、システムが検出データについて検査をするネットワーク セグメント、ポート、およびゾーンを指定し、ホスト、アプリケーション、およびユーザがセグメント、ポート、およびゾーンで検出されるかどうかを指定します。

検出なしの侵入検知と防御の実行

ライセンス： Protection

侵入検知と防御の機能によって、侵入とエクスプロイトの有無についてネットワーク トラフィックを分析できます。またオプションで違反パケットをドロップできます。侵入インスペクションを実行するが検出データを利用する必要がない場合は、検出を無効にして、デバイスのパフォーマンスを向上させることができます。

注　アプリケーション、ユーザ、または URL の制御を実行する場合は、パフォーマンス上の利点を得るために検出を無効にすることは**できません**。システムが検出データを保存しないようにすることはできますが、システムはそれらの機能を実行するために検出データを収集して検査する**必要があります**。

検出を無効にするには、次の**すべての**ガイドラインを実行します。いずれかでも誤って設定すると、パフォーマンス上の利点がなくなります。

- アクセス コントロール ポリシーでは、デバイスが適切にライセンス済みであっても、アプリケーション、ユーザ、URL、または位置情報ベースのネットワーク条件にルールを含めないでください。単純なネットワークベースの条件（ゾーン、IP アドレス、VLAN タグ、およびポート）のみを使用します。
- ネットワーク検出ポリシーからすべてのルールを削除します。

アクセス コントロール ポリシーを適用してからネットワーク検出ポリシーを適用すると、新しい検出がターゲット デバイスで停止します。システムは、ネットワーク検出ポリシーで指定されたタイムアウト期間に応じて、ネットワーク マップ内の情報を段階的に削除します。または、すべての検出データを即座に消去できます。データベースからの検出データの消去（B-1 ページ）を参照してください。

アクセス コントロール ポリシーおよびルールのトラブルシューティング

ライセンス： すべて

アクセス コントロール ポリシーの適切な設定、特に、アクセス コントロール ルールの作成と順序付けは複雑なタスクです。しかし、これは効果的な展開を構築するために必要なタスクです。ポリシーを慎重に計画しないと、ルールが他のルールをプリエンプション処理したり、ルールに無効な設定が含まれている場合があります。ルールおよび他のポリシー設定にはどちらも追加ライセンスが必要な場合があります。

システムが想定どおりにトラフィックを確実に処理できるように、アクセス コントロール ポリシー インターフェイスには強力なフィードバック システムがあります。アクセス コントロール ポリシーおよびルール エディタのアイコンは、アクセス コントロールのエラー アイコン の表に示すように、警告とエラーを示します。警告、エラー、または情報のテキストを確認するには、マウスのポインタをアイコンの上に重ねます。

ヒント　アクセス コントロール ポリシー エディタで、ポリシーのすべての警告を表示するポップアップ ウィンドウを表示するには [Show Warnings] をクリックします。

また、トラフィックの分析およびフローに影響を与える可能性がある問題の適用時には、システムによって警告が表示されます。

表 12-7　アクセス コントロールのエラー アイコン

アイコン	説明	詳細
	エラー	ルールまたは設定にエラーがある場合、影響を受けるルールを無効にしても、問題を修正するまでポリシーを適用できません。
	警告	ルールまたはその他の警告を表示するアクセス コントロール ポリシーを適用できます。しかし、警告とマークされている誤った設定には影響しません。 たとえば、プリエンプション処理されたルールまたは誤った設定（空のオブジェクト グループを使用した条件、アプリケーションに一致しないアプリケーション フィルタ、クラウド通信を有効にしないまま行った URL 条件の設定など）によってトラフィックを照合できないルールを含むポリシーを適用できます。これらのルールは、トラフィックを評価しません。警告が出されているルールを無効にすると、警告アイコンが消えます。潜在する問題を修正せずにルールを有効にすると、警告アイコンが再表示されます。 別の例としては、多くの機能で特定のライセンスまたはデバイス モデルが必要です。アクセス コントロール ポリシーは、対象となるターゲット デバイスのみに正常に適用されます。
	情報	情報アイコンは、トラフィックのフローに影響する可能性がある設定に関する有用な情報を伝送します。これらの問題によってポリシーの適用が阻まれることはありません。 たとえば、アプリケーション制御または URL フィルタリングを実行している場合、システムはその接続でアプリケーションまたは Web トラフィックを識別するまで、接続の最初の数パケットを複数のアクセス コントロール ルールと照合するのをスキップする場合があります。これにより、アプリケーションと HTTP 要求が識別されるように接続が確立されます。詳細については、アプリケーション制御の制約事項（16-8 ページ）およびURL の検出とブロッキングの制約事項（16-16 ページ）を参照してください。

アクセス コントロール ポリシーおよびルールを適切に設定することで、ネットワーク トラフィックの処理に必要なリソースも減らすことができます。複雑なルールの作成、多数のさまざまな侵入ポリシーの呼び出し、およびルールの誤った順序付けはすべて、パフォーマンスに影響する可能性があります。

詳細については、以下を参照してください。

- アクセス コントロールのライセンスおよびロール要件（12-2 ページ）
- パフォーマンスを向上させるためのルールの簡素化（12-26 ページ）
- ルールのプリエンプションと無効な設定の警告について（12-27 ページ）
- パフォーマンスを向上させプリエンプションを回避するためのルールの順序付け（12-28 ページ）

パフォーマンスを向上させるためのルールの簡素化

複雑なアクセス コントロール ポリシーおよびルールは、重要なリソースを消費する可能性があります。アクセス コントロール ポリシーを適用すると、システムはすべてのルールをまとめて評価し、ネットワーク トラフィックを評価するためにターゲット デバイスが使用する条件の拡張セットを作成します。ターゲット デバイスでサポートされるアクセス コントロール ルールまたは侵入ポリシーの最大数を超えていることを警告するポップアップ ウィンドウが表示される場合があります。この最大値は、デバイスの物理メモリやプロセッサ数などの、さまざまな要因によって異なります。

アクセス コントロール ルールの簡素化

次のガイドラインは、アクセス コントロール ルールを簡素化し、パフォーマンスを向上させるのに役立ちます。

- ルールを構築するときは、条件内で使用する個々の要素は可能な限り少なくします。たとえば、ネットワーク条件では、個々の IP アドレスではなく IP アドレス ブロックを使用します。ポート条件では、ポート範囲を使用します。アプリケーション制御および URL フィルタリングを実行する場合はアプリケーション フィルタと URL カテゴリおよびレピュテーションを使用し、ユーザ制御を実行する場合は LDAPユーザ グループを使用します。

  アクセス コントロール ルールの条件で使用する要素をオブジェクトに組み合わせてもパフォーマンスは向上しないことに注意してください。たとえば、50 の個別の IP アドレスを含むネットワーク オブジェクトを使用しても、その条件内のそれらの IP アドレスに対するものを含む、組織的な（パフォーマンスではない）利点が個別に与えられるだけです。
- できる限り、セキュリティ ゾーンごとにルールを制限します。デバイスのインターフェイスがゾーン制限されたルールのゾーンの 1 つにない場合、ルールはそのデバイスのパフォーマンスに影響を与えません。
- ルールを過度に設定しないでください。1 つの条件が処理するトラフィックに一致するのに十分な場合は、2 つ使用しないでください。

侵入ポリシーと変数セットの急増の回避

アクセス コントロール ポリシーでトラフィックを検査するために使用できる一意の侵入ポリシーの数は、デバイス上のリソースとポリシーの複雑度によって異なります。1 つの侵入ポリシーを各許可ルールおよびインタラクティブ ブロック ルール、さらにデフォルト アクションに関連付けることができます。侵入ポリシーと変数セットの固有の**ペア**はすべて、1 つのポリシーとしてカウントされます。

デバイスでサポートされる侵入ポリシーの数を超えた場合、アクセス コントロール ポリシーを再評価してください。いくつかの侵入ポリシーまたは変数セットを統合すると、複数のアクセス コントロール ルールに 1 つの侵入ポリシーと変数セットのペアを関連付けることができます。

アクセス コントロール ポリシーの次の場所のそれぞれで、選択したポリシーの数と、それらのポリシーが使用する変数セットの数を確認します。アクセス コントロール ポリシーの詳細設定の [Intrusion Policy used before Access Control rule is determined] オプション、アクセス コントロール ポリシーのデフォルト アクション、およびポリシー内のアクセス コントロール ルールのインスペクション設定。

ルールのプリエンプションと無効な設定の警告について

ライセンス： すべて

アクセス コントロール ルール（および、高度な展開ではネットワーク分析ルール）の適切な設定と順序付けは、効果的な展開を構築するために必須です。アクセス コントロール ポリシー内では、アクセス コントロール ルールが他のルールをプリエンプション処理したり、ルールに無効な設定が含まれている場合があります。同様に、アクセス コントロール ポリシーの詳細設定を使用して設定するネットワーク分析ルールにも同じ問題が存在する可能性があります。システムは、警告とエラーのアイコンを使用してこれらをマークします。

ルールのプリエンプションの警告について

アクセス コントロール ルールの条件が後続のルールよりも優先して適用され、後続のルールによるトラフィックの照合が回避される場合があります。次に例を示します。

```
Rule 1: allow Admin users
Rule 2: block Admin users
```

上記の 2 番目のルールによってトラフィックがブロックされることはありません。なぜなら、最初のルールによってトラフィックは既に許可されるためです。

どのようなタイプのルール条件でも、後続のルールを回避する可能性があります。次の例では、最初のルールでの VLAN 範囲に 2 番目のルールでの VLAN が含まれるため、最初のルールが 2 番目のルールよりも優先して適用されることになります。

```
Rule 1: allow VLAN 22-33
Rule 2: block VLAN 27
```

次の例では、VLAN が設定されていないルール 1 はあらゆる VLAN と一致します。そのため、ルール 1 が優先して適用され、ルール 2 での VLAN 2 の照合は行われません。

```
Rule 1: allow Source Network 10.4.0.0/16
Rule 2: allow Source Network 10.4.0.0/16, VLAN 2
```

あるルールとその後続のルールがまったく同じで、いずれもすべて同じ条件が設定されている場合、後続のルールは回避されます。次に例を示します。

```
Rule 1: allow VLAN 1 URL www.example.com
Rule 2: allow VLAN 1 URL www.example.com
```

条件が 1 つでも異なる場合は、後続のルールが回避されることはありません。次に例を示します。

```
Rule 1: allow VLAN 1 URL www.example.com
Rule 2: allow VLAN 2 URL www.example.com
```

無効な設定の警告について

アクセス コントロール ポリシーが依存する外部の設定は変更される可能性があるため、有効であったアクセス コントロール ポリシー設定が無効になる場合があります。次の例について考えてみます。

- URL フィルタリングを実行するルールは、URL Filtering ライセンスがないデバイスを対象とするまで有効になっている可能性があります。その時点で、ルールの横にエラー アイコンが表示され、ポリシーをそのデバイスに適用できなくなります。適用可能にするには、このルールを編集または削除するか、ポリシーのターゲットを変更するか、または適切なライセンスを有効にする必要があります。
- ルールの送信元ポートにポート グループを追加し、その後そのポート グループを変更して ICMP ポートを含めると、ルールは無効になり、その横に警告アイコンが表示されます。ポリシーをまだ適用することはできますが、ルールはネットワーク トラフィックに影響を与えません。
- ルールにユーザを追加し、その後 LDAP ユーザ認識設定を変更してそのユーザを除外すると、ユーザはアクセス コントロールの対象ユーザではなくなるため、そのルールは効力を持たなくなります。

パフォーマンスを向上させプリエンプションを回避するためのルールの順序付け

ライセンス: すべて

アクセス コントロール ポリシー内の各ルールには、1 から始まる番号が付きます。システムは、ルール番号の昇順で、ルールを上から順にトラフィックと照合します。モニタ ルールを除き、トラフィックが一致する最初のルールがそのトラフィックを処理するルールになります。

アクセス コントロール ルールの順序を適切にすることで、ネットワーク トラフィックの処理に必要なリソースが減り、ルールのプリエンプションを回避できます。ユーザが作成するルールはすべての組織と展開に固有のものですが、ユーザのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。

重要性が最も高いルールから最も低いルールへの順序付け

最初に、組織のニーズに適するルールを順序付けする必要があります。すべてのトラフィックに適用する必要があるプライオリティ ルールをポリシーの先頭部分付近に配置します。たとえば、ある 1 人のユーザからのトラフィックに侵入がないかを検査する（許可ルールを使用）が、部門内の他のすべてのユーザは信頼する（信頼ルールを使用）場合は、その順序に 2 つのアクセス コントロール ルールを配置します。

特定のルールから一般的なルールへの順序付け

特定のルール、つまり、処理するトラフィックを狭く定義するルールを先に配置することで、パフォーマンスを向上できます。これは、広範な条件を持つルールが多くのさまざまなタイプのトラフィックを照合し、後でより多くの特定のルールをプリエンプション処理することができるという理由からも重要です。

ほとんどのソーシャル ネットワーキング サイトをブロックする一方で、特定の他の部分へのアクセスを許可する場合のシナリオを考えます。たとえば、グラフィック デザイナーに Creative Commons Flickr および deviantART コンテンツへのアクセスを許可したいが、Facebook や Google+ などの他のサイトへのアクセスは許可したくない場合があります。ルールを次のように順序付けする必要があります。

```
Rule 1: Allow Flickr, deviantART for the "Design" LDAP user group
Rule 2: Block social networking
```

ルールを入れ替える場合は次のようになります。

```
Rule 1: Block social networking
Rule 2: Allow Flickr, deviantART for the "Design" LDAP user group
```

最初のルールは、Flickr および deviantART を含むすべてのソーシャル ネットワーキング トラフィックをブロックします。トラフィックが 2 番目のルールに一致しないため、利用可能にしたかったコンテンツにデザイナーはアクセスできません。

トラフィックを後で検査するルールの配置

検出、侵入、ファイルおよびマルウェアのインスペクションにはリソースの処理が必要なため、トラフィックのインスペクションを行うルール（許可、インタラクティブ ブロック）の前にトラフィックを検査しないルール（信頼、ブロック）を配置することで、パフォーマンスを向上させることができます。これは、信頼ルールおよびブロック ルールは、システムが別の方法で検査をした可能性があるトラフィックを迂回させることができるためです。他の要素がすべて同等、つまり、より重要なものがなくプリエンプションが問題ではない場合にルールのセットを与えると仮定すると、次の順序でルールを配置することを検討します。

- 一致する接続はロギングするが、トラフィックで他のアクションは実行しないモニタ ルール
- 追加のインスペクションなしでトラフィックを処理する信頼ルールおよびブロック ルール
- トラフィックの追加のインスペクションを行わない許可ルールおよびインタラクティブ ブロック ルール
- マルウェア、侵入、またはその両方がないか任意でトラフィックを検査する許可ルールおよびインタラクティブ ブロック ルール

現在のアクセス コントロール設定のレポートの生成

ライセンス： すべて

アクセス コントロール ポリシー レポートとは、特定の時点でのポリシーおよびルールの設定を記録したものです。このレポートには、次の情報が含まれており、監査目的や現在の設定を調べるために使用できます。

表 12-8　アクセス コントロール ポリシー レポートのセクション

セクション	説明
Policy Information	ポリシーの名前と説明、ポリシーを最後に変更したユーザの名前、ポリシーが最後に変更された日時が記載されます。
Device Targets	ポリシーがターゲットとする管理対象デバイスがリストされます。
HTTP Block Response HTTP Interactive Block Response	ポリシーを使用して Web サイトをブロックするときにユーザに表示されるページの詳細が提供されます。
セキュリティ インテリジェンス	ポリシーのセキュリティ インテリジェンスのホワイトリストおよびブラックリストの詳細が提供されます。
Default Action	デフォルト アクションと関連する変数セット（存在する場合）が示されます。
ルール	ポリシーの各アクセス コントロール ルールが示され、その設定の詳細が提供されます。

表 12-8　アクセス コントロール ポリシー レポートのセクション（続き）

セクション	説明
Advanced Settings	次のようなポリシーの詳細設定の情報 • アクセス コントロール ポリシーのトラフィックを前処理するために使用されるネットワーク分析ポリシー、およびグローバル前処理オプション • パッシブ展開用の適合型プロファイル設定 • ファイル、マルウェアおよび侵入を検出するためのパフォーマンス設定 • 他のポリシー全体の設定
Referenced Objects	侵入ポリシーの変数セットおよび SSL ポリシーで使用されるオブジェクトなど、アクセス コントロール ポリシーによって参照される再利用可能なオブジェクトに関する詳細が提供されます。

また、ポリシーを現在適用されているポリシーや別のポリシーと比較する、アクセス コンロトール比較レポートを生成することもできます。詳細については、アクセス コントロール ポリシーの比較（12-30 ページ）を参照してください。

アクセス コントロール ポリシー レポートの表示方法:

アクセス: Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　レポートの生成対象とするポリシーの横にあるレポート アイコン（  ）をクリックします。アクセス コントロール ポリシー レポートを生成する前に、必ずすべての変更を保存してください。レポートには、保存された変更のみが表示されます。

システムによってレポートが生成されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。

アクセス コントロール ポリシーの比較

ライセンス: すべて

組織の標準に準拠しているかを確認する目的や、システム パフォーマンスを最適化する目的でポリシーの変更を検討するために、2 つのアクセス コントロール ポリシーの差異を調べることができます。任意の 2 つのポリシーを比較することも、現在適用されているポリシーを別のポリシーと比較することもできます。オプションで、比較した後に PDF レポートを生成することで、2 つのポリシーの間の差異を記録できます。

ポリシーを比較するために使用できるツールは 2 つあります。

- 比較ビューは、2 つのポリシーを左右に並べて表示し、その差異のみを示します。比較ビューの左右のタイトル バーに、それぞれのポリシーの名前が示されます。ただし、[Running Configuration] を選択した場合、現在アクティブなポリシーは空白のバーで表されます。

このツールを使用すると、Web インターフェイスで 2 つのポリシーを表示してそれらに移動するときに、差異を強調表示することができます。

- 比較レポートは、ポリシー レポートと同様の形式ですが、2 つのポリシーの間の差異だけが、PDF 形式で記録されます。

  これを使用して、ポリシーの比較の保存、コピー、出力、共有を行って、さらに検証することができます。

ポリシー比較ツールの概要と使用法の詳細については、次の項を参照してください。

- アクセス コントロール ポリシー比較ビューの使用（12-31 ページ）
- アクセス コントロール ポリシー比較レポートの使用（12-31 ページ）

アクセス コントロール ポリシー比較ビューの使用

ライセンス： すべて

比較ビューには、両方のポリシーが左右に並べて表示されます。それぞれのポリシーは、比較ビューの左右のタイトル バーに示される名前で特定されます。現在実行されている設定ではない 2 つのポリシーを比較する場合、最後に変更された日時とその変更を行ったユーザがポリシー名と共に表示されます。

2 つのポリシーの間の差異は、次のように強調表示されます。

- 2 つのポリシーの間で異なっている設定は、青色で強調表示され、その差異が赤いテキストで示されます。
- 一方のポリシーにはあり、他方のポリシーにはない設定は、緑色で強調表示されます。

次の表に、実行できる操作を記載します。

表 12-9　　アクセス コントロール ポリシー比較ビューの操作

目的	操作
個々の変更の間を移動する	またはタイトル バーの上にある [Previous] または [Next] をクリックします。 左側と右側の間にある二重矢印アイコン（◂▸）が移動し、表示している違いを示す [Difference] 番号が変わります。
新しいポリシー比較ビューを生成する	[New Comparison] をクリックします。 [Select Comparison] ウィンドウが表示されます。詳細については、「アクセス コントロール ポリシー比較レポートの使用（12-31 ページ）」を参照してください。
ポリシー比較レポートを生成する	[Comparison Report] をクリックします。 ポリシー比較レポートは、2 つのポリシーの間の差異だけをリストした PDF ドキュメントです。

アクセス コントロール ポリシー比較レポートの使用

ライセンス： すべて

アクセス コントロール ポリシー比較レポートとは、ポリシー比較ビューで識別された、2 つのアクセス コントロール ポリシーの間、またはポリシーと現在適用中のポリシーの間にあるすべての差異を、PDF 形式で記録したものです。このレポートを使用することで、2 つのポリシー設定の間の違いをさらに調べ、調査結果を保存して共有できます。

ユーザは、アクセス権限が与えられている任意のポリシーの比較ビューから、アクセス コントロール ポリシー比較レポートを生成できます。ポリシー レポートを生成する前に、必ずすべての変更を保存してください。レポートには、保存されている変更だけが表示されます。

ポリシー比較レポートの形式は、ポリシー レポートと同様です。唯一異なる点は、ポリシー レポートにはポリシーのすべての設定が記載される一方、ポリシー比較レポートにはポリシー間で異なる設定だけがリストされることです。アクセス コントロール ポリシー比較レポートは、表 12-8（12-29 ページ）に記載されているセクションから成ります。

ヒント　同様の手順を使用して、SSL ポリシー、ネットワーク分析ポリシー、侵入ポリシー、ファイル ポリシー、システム ポリシー、またはヘルス ポリシーを比較できます。

2 つのアクセス コントロール ポリシーを比較する方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　[Compare Policies] をクリックします。

[Select Comparison] ウィンドウが表示されます。

ステップ 3　[Compare Against] ドロップダウンリストから、比較するタイプを次のように選択します。

- 異なる 2 つのポリシーを比較するには、[Other Policy] を選択します。

  ページが更新されて、[Policy A] と [Policy B] という 2 つのドロップダウンリストが表示されます。
- 現在のアクティブ ポリシーを他のポリシーに対して比較するには、[Running Configuration] を選択します。

  ページが更新されて、[Target/Running Configuration A] と [Policy B] という 2 つのドロップダウンリストが表示されます。

ステップ 4　選択した比較タイプに応じて、次のような選択肢があります。

- 2 つの異なるポリシーを比較する場合は、[Policy A] および [Policy B] ドロップダウンリストのそれぞれから、比較するポリシーを選択します。
- 現在実行されている設定を別のポリシーと比較する場合は、[Policy B] ドロップダウンリストから 2 つ目のポリシーを選択します。

ステップ 5　ポリシー比較ビューを表示するには、[OK] をクリックします。

比較ビューが表示されます。

ステップ 6　オプションで、[Comparison Report] をクリックして、アクセス コントロール ポリシー比較レポートを生成します。

アクセス コントロール ポリシー比較レポートが表示されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。

CHAPTER 13

セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録

悪意のあるインターネット コンテンツに対する第一の防衛ラインとして、FireSIGHT システムにはセキュリティ インテリジェンス機能があり、それを使用することで、最新のレピュテーション インテリジェンスに基づいて接続を即座にブラックリスト登録(ブロック)することができ、リソースを集中的に使用する詳細な分析の必要がなくなります。セキュリティ インテリジェンスのフィルタリングには、Protection ライセンスが必要で、シリーズ 2 を除くすべての管理対象デバイスでサポートされます。

セキュリティ インテリジェンスは、既知の良くないレピュテーションが含まれる IP アドレスを送信元/宛先とするトラフィックをブロックすることにより機能します。このトラフィック フィルタリングは、他のどのポリシー ベースのインスペクション、分析、またはトラフィック処理よりも**前に**行われます(ただし高速パスなどのハードウェア レベルの処理の後に発生します)。

IP アドレスでトラフィックを手動で制限することで、セキュリティ インテリジェンス フィルタリングと同様の機能を実行するアクセス コントロール ルールを作成することができます。ただし、アクセス コントロール ルールは対象範囲が広く、設定の難易度が高いだけでなく、動的フィードを使用した自動更新に対応できません。

セキュリティ インテリジェンスによってブラックリスト登録されたトラフィックは即座にブロックされるため、他のさらなるインスペクションの対象にはなりません(侵入、エクスプロイト、マルウェアなどの有無だけでなくネットワーク検出についても)。オプションで、セキュリティ インテリジェンス フィルタリングには「モニタ専用」設定を使用できます。パッシブ展開環境では、この設定が推奨されます。この設定では、ブラックリスト登録されるはずの接続をシステムが分析できるだけでなく、ブラックリストに一致する接続がログに記録され、接続終了セキュリティ インテリジェンス イベントが生成されます。

注意 シリーズ 3 デバイスによって処理されるトラフィックの場合は、システムはアクセス コントロール ポリシーのセキュリティ インテリジェンス ブラックリストの前に特定の信頼ルールを処理します。これによって、ブラックリスト登録されたトラフィックは検査されないまま通過することができます。詳細については、シリーズ 3 デバイスを使用したトラフィックの信頼またはブロックへの制限事項(14-13 ページ)を参照してください。

便宜上、Cisco は*インテリジェンス フィード*(*Sourcefire インテリジェンス フィード*とも呼ばれます)を提供します。これは、VRT によってレピュテーションに欠けると判断された IP アドレスのコレクションからなり、これらのコレクションは定期的に更新されます。インテリジェンス フィードは、オープン リレー、既知の攻撃者、偽の IP アドレス(bogon)などを追跡します。この機能を組織の固有のニーズに適するようにカスタマイズできます。例を次に示します。

- **サードパーティ フィード**：インテリジェンス フィードをサードパーティのレピュテーション フィードで補足できます。そのフィードはシステムが Cisco フィードと同様に自動的に更新できます。
- **カスタム ブラックリスト**：システムは、ユーザが自身のニーズに応じてさまざまな方法で特定の IP アドレスを手動でブラックリスト登録することを許可します。
- **セキュリティ ゾーンによるブラックリスト登録の強制**：パフォーマンスを向上させるには、スパムのブラックリスト登録を電子メール トラフィックを処理するゾーンに制限するなどして、強制を適用することができます。
- **ブラックリスト登録の代わりにモニタリング**：特にパッシブ展開で、展開を実装する前のフィードのテストに有用です。違反しているセッションをブロックする代わりに単にモニタして、接続終了イベントを生成できます。
- **誤検出をなくすためのホワイトリスト登録**：ブラックリストの範囲が広すぎる場合、または（たとえば、重要なリソースに）許可するトラフィックを誤ってブロックした場合、ブラックリストをカスタム ホワイトリストで上書きできます。

セキュリティ インテリジェンス フィルタリングを実行するためにアクセス コントロール ポリシーを設定する方法、およびこのフィルタリングが生成するイベント データを表示する方法については、次の項を参照してください。

- セキュリティ インテリジェンス戦略の選択（13-2 ページ）
- セキュリティ インテリジェンスのホワイトリストおよびブラックリストの作成（13-4 ページ）
- セキュリティ インテリジェンス（ブラックリスト登録）の決定のロギング（38-12 ページ）
- 接続およびセキュリティ インテリジェンス のデータの使用（39-1 ページ）

セキュリティ インテリジェンス戦略の選択

ライセンス： Protection

サポートされるデバイス： すべて（シリーズ 2 を除く）

サポートされる防御センター： DC500 を除くいずれか

ブラックリストを作成する最も簡単な方法は、オープン リレーとなることが分かっている IP アドレス、既知の攻撃者、不正な IP アドレス（bogon）などを追跡する、インテリジェンス フィードを使用することです。インテリジェンス フィードは定期的に更新されるため、インテリジェンス フィードを使用することで、システムがネットワーク トラフィックのフィルタリングに最新の情報を使用することが保証されます。ただし、セキュリティに対する脅威（マルウェア、スパム、ボットネット、スパム、フィッシングなど）を表す不正な IP アドレスが現れては消えるペースが早すぎて、新しいポリシーを更新して適用するには間に合わないこともあります。

インテリジェンス フィードを向上させるには、カスタムまたはサードパーティの IP アドレスのリストとフィードを使用してセキュリティ インテリジェンス フィルタリングを実行できます。

- *リスト* とは、Defense Centerにアップロードする IP アドレスの静的リストのことです。
- *フィード* とは、Defense Center が定期的にインターネットからダウンロードする、IP アドレスの動的リストのことです。インテリジェンス フィードは、特殊なタイプのフィードです。

高可用性およびインターネット アクセス要件を含め、セキュリティ インテリジェンスのリストとフィードを設定する方法の詳細については、セキュリティ インテリジェンス リストとフィードの操作（3-5 ページ）を参照してください。

セキュリティ インテリジェンスのグローバル ブラックリストの使用

分析の過程で、イベント ビュー、Context Explorer、またはダッシュボードで任意の IP アドレスを選択して*グローバル ブラックリスト*を作成することもできます。たとえば、エクスプロイトの試みに関連する侵入イベントで、一連のルーティング可能 IP アドレスに気付いた場合、これらの IP アドレスを直ちにブラックリスト登録することができます。Defense Center ではすべてのアクセス コントロール ポリシーで、このグローバル ブラックリスト（および関連する*ホワイトリスト*）を使用してセキュリティ インテリジェンス フィルタリングを行います。これらのグローバル リストを管理する方法の詳細については、グローバル ホワイトリストおよびブラックリストの操作（3-7 ページ）を参照してください。

注　グローバル ブラックリスト（またはグローバル ホワイトリスト。以下を参照）のフィードの更新および追加では、展開環境全体にわたって自動的にその変更が実装されますが、セキュリティ インテリジェンス オブジェクトに対するその他の変更には、アクセス コントロール ポリシーの再適用が必要になります。詳細については、表 3-1（3-7 ページ）を参照してください。

ネットワーク オブジェクトの使用

さらに、ブラックリストを作成するもう 1 つの簡単な方法として、IP アドレス、IP アドレス ブロック、あるいは IP アドレスのコレクションを表す*ネットワーク オブジェクトまたはネットワーク オブジェクト グループ*を使用することもできます。ネットワーク オブジェクトの作成および変更の詳細については、ネットワーク オブジェクトの操作（3-4 ページ）を参照してください。

セキュリティ インテリジェンスのホワイトリストの使用

ブラックリストに加え、各アクセス コントロール ポリシーにはホワイトリストが関連付けられます。ホワイトリストにも、セキュリティ インテリジェンス オブジェクトを取り込むことができます。ポリシーでは、ホワイトリストがブラックリストをオーバーライドします。つまり、システムは、送信元または宛先の IP アドレスがホワイトリストに登録されているトラフィックは、たとえそれらの IP アドレスがブラックリストにも登録されているとしても、そのトラフィックをアクセス コントロール ルールを使用して評価します。通常、ブラックリストがまだ有用であっても、その適用範囲があまりにも広く、インスペクション対象のトラフィックを誤ってブロックする場合には、ホワイトリストを使用してください。

たとえば、信頼できるフィードにより、重要なリソースへのアクセスが不適切にブロックされたが、そのフィードが全体としては組織にとって有用である場合は、そのフィード全体をブラックリストから削除するのではなく、不適切に分類された IP アドレスだけをホワイトリストに登録するという方法を取ることができます。

セキュリティ ゾーンを基準としたセキュリティ インテリジェンス フィルタリングの適用

さらに細かく制御するには、接続の送信元または宛先 IP アドレスが特定のセキュリティ ゾーン内にあるかどうかに基づいて、セキュリティ インテリジェンス フィルタリングを適用することができます。

上述のホワイトリストの例を拡張するとしたら、不適切に分類された IP アドレスをホワイトリストに登録した後、組織でそれらの IP アドレスにアクセスする必要があるユーザが使用しているセキュリティ ゾーンを使用して、ホワイトリストのオブジェクトを制限するという方法が考えられます。この方法では、ビジネス ニーズを持つユーザだけが、ホワイトリストに登録された IP アドレスにアクセスできます。別の例として、サードパーティのスパム フィードを使用して、電子メール サーバのセキュリティ ゾーンでトラフィックをブラックリスト登録することもできます。

接続のモニタリング（ブラックリスト登録ではなく）

特定の IP アドレスまたはアドレス一式をブラックリスト登録する必要があるかどうかわからない場合は、「モニタ専用」設定を使用できます。この設定では、システムが一致する接続をアクセス コントロール ルールに渡せるだけでなく、ブラックリストと一致する接続がログに記録され、接続終了セキュリティ インテリジェンス イベントが生成されます。注意する点として、グローバル ブラックリストをモニタ専用に設定することはできません。詳細については、次のサイトを参照してください。

たとえば、サードパーティのフィードを使用したブロッキングを実装する前に、そのフィードをテストする必要があるとします。フィードをモニタ専用に設定すると、ブロックされるはずの接続をシステムで詳細に分析できるだけでなく、そのような接続のそれぞれをログに記録して、評価することもできます。

パッシブ展開環境では、パフォーマンスを最適化するために、Ciscoでは常にモニタ専用の設定を使用することを推奨しています。パッシブに展開された管理対象デバイスはトラフィック フローに影響を与えることができないため、トラフィックをブロックするようにシステムを構成しても何のメリットもありません。また、ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

セキュリティ インテリジェンスのホワイトリストおよびブラックリストの作成

ライセンス： Protection

サポートされるデバイス： すべて（シリーズ 2 を除く）

サポートされる防御センター： DC500 を除くいずれか

ホワイトリストとブラックリストを作成するには、ネットワーク オブジェクトとグループの任意の組み合わせに加え、セキュリティ ゾーン別に制約することができる、セキュリティ インテリジェンスのフィードとリストを入力します。

注意　右クリック メニューで [Whitelist Now] または [Blacklist Now] オプションを選択した場合を除き、セキュリティ インテリジェンス リストを変更すると、Snort プロセスが再開され、構成変更を適用する際、一時的にトラフィック検査が中断されます。この検査中にシステムがトラフィックをドロップするか、検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、「Snort の再開によるトラフィックへの影響（1-9 ページ）」を参照してください。

デフォルトでは、アクセス コントロール ポリシーは、任意のゾーンに適用される、Defense Center のグローバル ホワイトリストおよびブラックリストを使用します。これらのリストはアナリストによって入力されます。アナリストは、コンテキスト メニューを使用して、簡単に個々の IP アドレスを追加できます。ポリシーのそれぞれについて、これらのグローバル リストを使用しないように選択することができます。

注　入力したグローバル ホワイトリストまたはブラックリストを使用するアクセス コントロール ポリシーを シリーズ 2 デバイス（または Protection のライセンスがない他のデバイス）に適用することはできません。いずれかのグローバル リストに IP アドレスを追加した場合は、ポリシーのセキュリティ インテリジェンス設定から空でないリストを削除してから**でないと**、ポリシーを適用できません。詳細については、グローバル ホワイトリストおよびブラックリストの操作（3-7 ページ）を参照してください。

ホワイトリストとブラックリストを作成した後は、ブラックリスト登録された接続のロギングが可能になります。フィードとリストを含め、ブラックリスト登録された個々のオブジェクトをモニタ専用に設定することもできます。この設定では、システムがブラックリスト登録された IP アドレスを使用する接続をアクセス コントロールによって処理できるだけでなく、ブラックリストと一致する接続をログに記録することもできます。

ホワイトリスト、ブラックリスト、およびロギング オプションを設定するには、アクセス コントロール ポリシーの [Security Intelligence] タブを使用します。このページには、ホワイトリストまたはブラックリストのいずれかで使用できるオブジェクトのリスト（[Available Objects]）と、ホワイトリスト登録およびブラックリスト登録されたオブジェクトを制約するために使用できるゾーンのリスト（[Available Zones]）が表示されます。オブジェクトまたはゾーンのタイプは、異なるアイコンによって見分けられるようになっています。Cisco アイコン（  ）でマークされたオブジェクトは、インテリジェンス フィードの各種カテゴリを表します。

セキュリティ インテリジェンス カテゴリ	カテゴリ定義
Attacker	悪意のあるアウトバウンド アクティビティが認識されているアクティブなスキャナおよびブラックリスト ホスト
Malware	マルウェアのバイナリをホストまたはキットをエクスプロイトするサイト
Phishing	フィッシング ページをホストするサイト
Spam	スパム送信が認識されているメール ホスト
BOT	バイナリ マルウェア ドロッパをホストするサイト
CnC	ボットネットのコマンド サーバと制御サーバをホストするサイト
OpenProxy	匿名 Web ブラウジングを許可するオープン プロキシ
OpenRelay	スパムに使用されることが認識されているオープン メール リレー
TorExitNode	Tor 終了ノード
Bogon	Bogon ネットワークおよび未割り当ての IP アドレス

ブラックリストでは、ブロックするように設定されたオブジェクトはブロック アイコン（  ）でマークされ、モニタ専用オブジェクトはモニタ アイコン（  ）でマークされます。ホワイトリストがブラックリストをオーバーライドするため、両方のリストに同じオブジェクトを追加すると、ブラックリスト登録されたオブジェクトに取り消し線が表示されます。

ホワイトリストとブラックリストには、最大 255 個のオブジェクトを追加できます。つまり、ホワイトリストのオブジェクトとブラックリストのオブジェクトを合計した数は 255 以下でなければなりません。

ネットマスク /0 のネットワーク オブジェクトはホワイトリストまたはブラックリストに追加できますが、それらのオブジェクトでネットマスク /0 を使用したアドレス ブロックは無視され、これらのアドレスに基づいたホワイトリストおよびブラックリスト フィルタリングは行われないことに注意してください。セキュリティ インテリジェンス フィードからのネットマスク /0 のアドレス ブロックも無視されます。ポリシーがターゲットとするすべてのトラフィックをモニタまたはブロックする場合は、セキュリティ インテリジェンス フィルタリングの代わりに、[Monitor] または [Block] ルール アクションでアクセス コントロール ルールを使用し、[Source Networks] および [Destination Networks] の [any] のデフォルト値をそれぞれ使用します。

アクセス コントロール ポリシーのセキュリティ インテリジェンス ホワイトリストおよびブラックリストを作成する方法:

アクセス: Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　設定するアクセス コントロール ポリシーの横にある編集アイコン( )をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3　[Security Intelligence] タブを選択します。

アクセス コントロール ポリシーのセキュリティ インテリジェンス設定が表示されます。

ステップ 4　オプションで、ブラックリスト登録された接続をログに記録するには、ロギング アイコン( )をクリックします。

ロギングを有効にしてからでないと、ブラックリスト登録されたオブジェクトをモニタ専用に設定することはできません。詳細については、セキュリティ インテリジェンス(ブラックリスト登録)の決定のロギング(38-12 ページ)を参照してください。

ステップ 5　1 つ以上の**使用可能なオブジェクト**を選択して、ホワイトリストおよびブラックリストの作成を開始します。

複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、右クリックして [Select All] を選択します。

ヒント　リストに含める既存のオブジェクトを検索できます。組織のニーズを満たす既存のオブジェクトがない場合は、その場でオブジェクトを作成することもできます。詳細については、ホワイトリストまたはブラックリストに追加するオブジェクトの検索(13-7 ページ)およびホワイトリストまたブラックリストに追加するオブジェクトの作成(13-7 ページ)を参照してください。

ステップ 6　オプションで、**使用可能なゾーン**を選択して、ゾーン別に選択したオブジェクトを制約します。

デフォルトでは、オブジェクトは制約されません。つまり、オブジェクトのゾーンは [Any] に設定されます。[Any] を使用しない場合、制約の基準にできるゾーンは 1 つだけです。複数のゾーンでオブジェクトのセキュリティ インテリジェンス フィルタリングを適用するには、ゾーンのそれぞれについて、オブジェクトをホワイトリストまたはブラックリストに追加する必要があります。また、グローバル ホワイトリストまたはブラックリストをゾーンによって制約することはできません。

ステップ 7　[Add to Whitelist] または [Add to Blacklist] をクリックします。

また、オブジェクトをクリックして選択し、いずれかのリストにドラッグすることもできます。

選択したオブジェクトは、ホワイトリストまたはブラックリストに追加されます。

ヒント　オブジェクトをリストから削除するには、そのオブジェクトの削除アイコン( )をクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [Select All] を選択した後、右クリックして [Delete Selected] を選択します。グローバル リストを削除する場合は、選択した操作を確認する必要があります。ホワイトリストまたはブラックリストからオブジェクトを排除しても、そのオブジェクトは Defense Center から削除されません。

ステップ 8　オブジェクトをホワイトリストまたはブラックリストに追加し終わるまで、ステップ 5 ～ 7 を繰り返します。

ステップ 9　オプションで、ブラックリスト登録されたオブジェクトをモニタ専用に設定するには、[Blacklist] にリストされている該当するオブジェクトを右クリックし、[Monitor-only (do not block)] を選択します。

パッシブ展開環境の場合、Ciscoではすべてのブラックリスト登録されたオブジェクトをモニタ専用に設定することを推奨します。ただし、グローバル ブラックリストをモニタ専用に設定することはできません。

ステップ 10　[Save] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

ホワイトリストまたはブラックリストに追加するオブジェクトの検索

ライセンス： Protection

サポートされるデバイス： すべて（シリーズ 2 を除く）

サポートされる防御センター： DC500 を除くいずれか

複数のネットワーク オブジェクト、グループ、フィード、およびリストを使用する場合は、検索機能を使用して、ブラックリストまたはホワイトリストに追加するオブジェクトを絞り込むことができます。

ブラックリストまたはホワイトリストに追加するオブジェクトを検索する方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Search by name or value] フィールドにクエリを入力します。

検索文字列を入力すると、[Available Objects] リストが更新されて、検索文字列と一致する項目が表示されます。検索文字列をクリアするには、検索フィールドの上にあるリロード アイコン（ ）をクリックするか、検索フィールド内のクリア アイコン（ ）をクリックします。

ネットワーク オブジェクトの名前、またはネットワーク オブジェクトに設定されている値を基準に検索できます。たとえば、`Texas Office` という名前で `192.168.3.0/24` という設定値を持つ個別ネットワーク オブジェクトがあり、そのオブジェクトが `US Offices` というグループ オブジェクトに含まれている場合、検索文字列の一部または全部（たとえば `Tex`）を入力するか、値（たとえば `3`）を入力することで、両方のオブジェクトを表示できます。

ホワイトリストまたブラックリストに追加するオブジェクトの作成

ライセンス： Protection

サポートされるデバイス： すべて（シリーズ 2 を除く）

サポートされる防御センター： DC500 を除くいずれか

アクセス コントロール ポリシーの編集中に、ホワイトリストやブラックリストで使用するオブジェクト（ネットワーク オブジェクトや、セキュリティ インテリジェンスのリストまたはフィード）をその場で作成できます。ネットワーク オブジェクトをグループ化する場合、またはネットワーク オブジェクト グループを作成する場合は、オブジェクト マネージャーを使用する必要があります。

ホワイトリストまたはブラックリストに追加するオブジェクトを作成する方法:

アクセス: Admin/Access Admin/Network Admin

ステップ 1 追加アイコン( )をクリックして、作成するオブジェクトのタイプを選択します。

- セキュリティ インテリジェンスのリストまたはフィードを作成する場合は、[Add IP List] を選択します。セキュリティ インテリジェンス リストとフィードの操作(3-5 ページ)を参照してください。
- ネットワーク オブジェクトを追加する場合は、[Add Network Object] を選択します。ネットワーク オブジェクトの操作(3-4 ページ)を参照してください。

CHAPTER 14

アクセス コントロール ルールを使用したトラフィック フローの調整

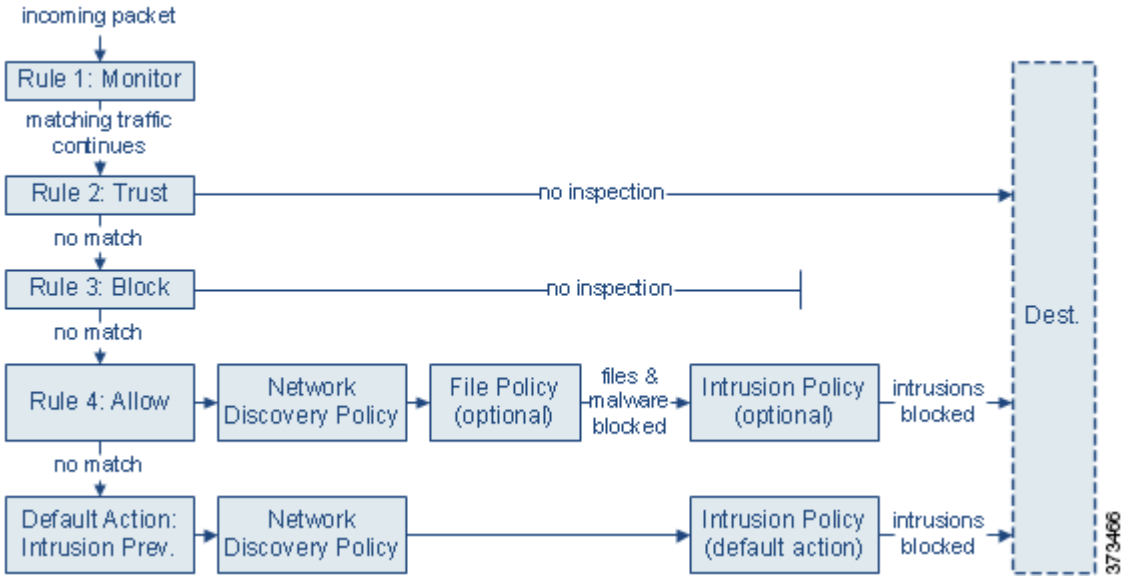
アクセス コントロール ポリシー内で、*アクセス コントロール ルール*は複数の管理対象デバイスでネットワーク トラフィックを処理する詳細な方法を提供しています。

注 ハードウェアベースの高速パス ルール、セキュリティ インテリジェンス ベースのトラフィック フィルタリング、および一部の復号化と前処理は、ネットワーク トラフィックがアクセス コントロール ルールによって評価される**前に**行われます。また、*SSL インスペクション*機能を設定すると、暗号化されたトラフィックをアクセス コントロール ルールが評価する前にブロックしたり復号化したりできます。

システムは、指定した順にアクセス コントロール ルールをトラフィックと照合します。ほとんどの場合、システムは、*すべて*のルールの条件がトラフィックに一致する場合、*最初*のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。条件は単純または複雑にできます。セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、およびユーザごとにトラフィックを制御できます。

各ルールには*アクション*も含まれており、一致するトラフィックをモニタ、信頼、ブロック、または許可するかどうかを決定します。トラフィックを許可するときは、システムが侵入ポリシーまたはファイル ポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出る前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。ただし、システムはトラフィックを信頼またはブロックした後は、追加のインスペクションを実行**しません**。

次のシナリオでは、インラインの侵入防御展開環境で、アクセス コントロール ルールによってトラフィックを評価できる方法を要約しています。



このシナリオでは、トラフィックは次のように評価されます。

- **ルール 1:モニタ**はトラフィックを最初に評価します。モニタ ルールはネットワーク トラフィックを追跡してログに記録しますが、トラフィック フローには影響しません。システムはトラフィックと追加ルールの照合を継続して、許可するか拒否するかを決定します。
- **ルール 2:信頼**はトラフィックを 2 番目に評価します。一致するトラフィックは、追加のインスペクションなしでその宛先への通過を許可されます。一致しなかったトラフィックは、次のルールへと進められます。
- **ルール 3:ブロック**はトラフィックを 3 番目に評価します。一致したトラフィックは、それ以上のインスペクションは行わずに、ブロックされます。一致しないトラフィックは、引き続き最後のルールと照合されます。
- **ルール 4:許可**は最後のルールです。このルールの場合、一致するトラフィックは許可されますが、そのトラフィック内の禁止されたファイル、マルウェア、侵入およびエクスプロイトは検出されてブロックされます。残りの禁止されていない悪意のないトラフィックは宛先に許可されます。ファイル インスペクションのみを実行する、または侵入インスペクションのみを実行する、もしくは両方とも実行しない追加の許可ルールを割り当てることができることに留意してください。
- **デフォルト アクション**はルールのいずれにも一致しないすべてのトラフィックを処理します。このシナリオでは、デフォルト アクションは、悪意のないトラフィックの通過を許可する前に侵入防御を実行します。別の展開では、追加のインスペクションなしですべてのトラフィックを信頼またはブロックするデフォルト アクションが存在する場合があります。(デフォルト アクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行できません。)

アクセス コントロール ルールまたはデフォルト アクションによって許可したトラフィックは、自動的にホスト、アプリケーション、およびユーザ データについてネットワーク検出ポリシーによるインスペクションの対象になります。明示的に検出を有効にしなくても、それを拡張または無効にできます。ただし、トラフィックを許可すると、検出データの収集は自動的に保証されません。システムは、ネットワーク検出ポリシーによって明示的にモニタされる IP アドレスを含む接続に対してのみ、検出を実行します。また、アプリケーション検出は、暗号化されたセッションに限定されます。詳細については、ネットワーク検出の概要(45-1 ページ)を参照してください。

暗号化されたトラフィックの通過が SSL インスペクション設定で許可される場合、または SSL インスペクションが設定されていない場合は、そのトラフィックがアクセス コントロール ルールによって処理されることに注意してください。ただし、一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルールが少なくなる場合があります。また、暗号化されたペイロードの侵入およびファイル インスペクションは、デフォルトで無効になっています。これにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。詳細については、トラフィック復号化の概要（19-1 ページ）およびSSL プリプロセッサの使用（27-75 ページ）を参照してください。

アクセス コントロール ルールの詳細については、以下を参照してください。

- アクセス コントロール ルールの作成および編集（14-3 ページ）
- ポリシー内のアクセス コントロール ルールの管理（14-15 ページ）
- アクセス コントロール ポリシーおよびルールのトラブルシューティング（12-25 ページ）

アクセス コントロール ルールの作成および編集

ライセンス： すべて

アクセス コントロール ポリシー内で、アクセス コントロール ルールは複数の管理対象デバイスでネットワーク トラフィックを処理する詳細な方法を提供しています。一意の名前に加え、各アクセス コントロール ルールには次の基本コンポーネントがあります。

状態

デフォルトでは、ルールが有効状態になります。無効にしたルールはネットワーク トラフィックの評価には使用されなくなり、そのルールの場合の警告とエラーの生成が停止されます。

位置

アクセス コントロール ポリシー内の各ルールには、1 から始まる番号が付きます。システムは、ルール番号の昇順で、ルールを上から順にトラフィックと照合します。モニタ ルールを除き、トラフィックが一致する最初のルールがそのトラフィックを処理するルールになります。

条件

条件は、ルールで処理する特定のトラフィックを指定します。条件は、セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、またはユーザ別にトラフィックを照合できます。条件は単純または複雑にできます。条件の使用は、多くの場合ターゲット デバイスのライセンスおよびモデルによって異なります。

Action

ルールのアクションは、一致したトラフィックの処理方法を決定します。一致するトラフィックをモニタ、信頼、ブロック、または許可（追加のインスペクションあり/なしで）することができます。システムは、信頼されたトラフィックとブロックされたトラフィックに対してインスペクションを実行**しない**ことに注意してください。

インスペクション

アクセス コントロール ルールのインスペクション オプションは、何も行われなければユーザが許可していたであろう悪意のあるトラフィックをシステムが検査およびブロックする方法を制御します。ルールを使用してトラフィックを許可するときは、システムが侵入ポリ

シーまたはファイル ポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出る前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

ロギング

ルールのロギング設定は、システムが処理するトラフィックのレコードの維持を制御します。各ルールに一致したトラフィックのレコードを維持できます。一般に、接続の開始時または終了時（またはその両方）でセッションをログに記録できます。接続のログは、Defense Center データベースの他に、システム ログ（Syslog）または SNMP トラップ サーバに記録できます。

注

アクセス コントロール ルールで変更を保存するたびに、コメントを追加できます。

アクセス コントロール ルールを追加および編集するには、アクセス コントロール ルール エディタを使用します。アクセス コントロール ポリシー エディタの [Rules] タブからルール エディタにアクセスします。ルール エディタで、次の操作を実行します。

- エディタの上部で、ルールの名前、状態、位置、アクションなどの基本的なプロパティを設定します。
- エディタの左下にあるタブを使用して、条件を追加します。
- インスペクションおよびロギングのオプションを設定し、さらにルールにコメントを追加するには、右下にあるタブを使用します。便宜上、どのタブを表示しているかに関係なく、エディタにはルールのインスペクションおよびロギングのオプションがリストされます。

注 アクセス コントロール ルールの適切な作成と順序付けは複雑なタスクですが、効果的な展開を構築するためには必須なものです。慎重なポリシーの設計を怠ると、他のルールをプリエンプション処理したり、追加ライセンスが必要となったり、無効な設定を含んだルールになる可能性があります。システムが想定どおりにトラフィックを確実に処理できるように、アクセス コントロール ポリシー インターフェイスにはルールに対する強力な警告およびエラーのフィードバック システムがあります。詳細については、アクセス コントロール ポリシーおよびルールのトラブルシューティング（12-25 ページ）を参照してください。

アクセス コントロール ルールを作成または変更するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　ルールの追加先にするアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

ポリシー ページが表示され、[Rules] タブに焦点が置かれています。

ステップ 3　次の選択肢があります。

- 新しいルールを追加するには、[Add Rule] をクリックします。
- 既存のルールを編集するには、そのルールの横にある編集アイコン（）をクリックします。

アクセス コントロール ルール エディタが表示されます。

ステップ 4　[Name] にルールの名前を入力します。

各ルールには一意の名前が必要です。30 文字までの印刷可能文字を使用できます。スペースや特殊文字を含めることができますが、コロン(:)は使用できません。

ステップ 5　前述の説明に従い、ルール コンポーネントを設定します。次の設定をするか、デフォルト設定をそのまま使用することができます。

- ルールを有効にするかどうか [Enabled] を指定します。
- ルールの位置を指定します。「ルールの評価順序の指定(14-5 ページ)」を参照してください。
- ルールの [Action] を選択します。「ルール アクションを使用したトラフィックの処理とインスペクションの決定(14-8 ページ)」を参照してください。
- ルールの条件を設定します。「ルールが処理するトラフィックを指定するための条件の使用(14-6 ページ)」を参照してください。
- 許可ルールおよびインタラクティブ ブロック ルールの場合は、ルールの**インスペクション** オプションを設定します。侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御(18-1 ページ)を参照してください。
- [Logging] オプションを指定します。「ネットワーク トラフィックの接続のロギング(38-1 ページ)」を参照してください。
- **コメント**を追加します。ルールへのコメントの追加(14-14 ページ)を参照してください。

ステップ 6　[Save] をクリックしてルールを保存します。

ルールが保存されます。削除アイコン( )をクリックすると、ルールを削除できます。変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります(アクセス コントロール ポリシーの適用(12-17 ページ)を参照してください)。

ルールの評価順序の指定

ライセンス: すべて

最初にアクセス コントロール ルールを作成するときに、ルール エディタで [Insert] ドロップダウンリストを使用してその位置を指定します。アクセス コントロール ポリシー内の各ルールには、1 から始まる番号が付きます。システムは、ルール番号の昇順で先頭から順にアクセス コントロール ルールをトラフィックと照合します。

ほとんどの場合、システムは、*すべて*のルールの条件がトラフィックに一致する場合、*最初*のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。モニタ ルール(トラフィックをログに記録するがトラフィック フローには影響しないルール)の場合を除き、システムは、そのトラフィックがルールに一致した後、追加の優先順位の低いルールに対してトラフィックを評価し続けることは**ありません**。

ヒント　アクセス コントロール ルールの順序を適切にすることで、ネットワーク トラフィックの処理に必要なリソースが減り、ルールのプリエンプションを回避できます。ユーザが作成するルールはすべての組織と展開に固有のものですが、ユーザのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。詳細については、パフォーマンスを向上させプリエンプションを回避するためのルールの順序付け(12-28 ページ)を参照してください。

ルールは数値で順序付けするだけでなく、カテゴリ別にグループ化することもできます。デフォルトで、システムには 3 つのカテゴリ（管理者、標準、ルート）があります。カスタム カテゴリを追加できますが、Cisco 提供のカテゴリを削除したり、それらの順序を変更したりすることはできません。既存のルールの位置またはカテゴリの変更の詳細については、「ルールの位置またはカテゴリの変更（14-18 ページ）」を参照してください。

ルールの編集や作成中にルールをカテゴリに追加する手順：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　アクセス コントロール ルール エディタで、[Insert] ドロップダウンリストから、[Into Category] を選択し、使用するカテゴリを選択します。

ルールを保存すると、そのカテゴリの最後に配置されます。

ルールの編集や作成中にルールの位置を数値で指定する手順：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　アクセス コントロール ルール エディタで、[Insert] ドロップダウンリストから、[above rule] または [below rule] を選択し、適切なルール番号を入力します。

ルールを保存すると、指定した位置に配置されます。

ルールが処理するトラフィックを指定するための条件の使用

ライセンス： 機能によって異なる

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

アクセス コントロール ルールの条件によって、ルールが処理するトラフィックのタイプが識別されます。条件は単純または複雑にできます。セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、およびユーザごとにトラフィックを制御できます。

条件をアクセス コントロール ルールに追加する場合は、次の点に注意してください。

- 1 つのルールにつき複数の条件を設定できます。ルールがトラフィックに適用されるには、トラフィックがそのルールの**すべての**条件に一致する必要があります。たとえば、特定のホストの URL フィルタリング（URL 条件）を実行する単一のルールを使用できます（ゾーンまたはネットワーク条件）。
- ルールの条件ごとに、最大 50 の基準を追加できます。条件の基準の**いずれかに**一致するトラフィックはその条件を満たします。たとえば、単一のルールを使用して、最大 50 のユーザおよびグループのユーザ制御を実行できます。

最大 50 の送信元の基準と最大 50 の宛先の基準を使用して、送信元と宛先ごとにゾーンおよびネットワークの条件を制約できます。送信元基準と宛先基準の両方をゾーンまたはネットワーク条件に追加する場合、一致するトラフィックは指定された送信元ゾーン/ネットワークの 1 つから発生し、宛先ゾーン/ネットワークの 1 つを通って出力する必要があります。つまり、システムは、同じタイプの複数の条件基準を OR 演算でリンクし、複数の条件タイプを AND 演算でリンクします。たとえば、次のようなルール条件の場合、

```
Source Networks: 10.0.0.0/8, 192.168.0.0/16
Application Category: peer to peer
```

ルールは、プライベートな IPv4 ネットワークの 1 つでホストからのピアツーピア アプリケーション トラフィックを照合します。パケットはいずれか一方**または**他の送信元ネットワークから発生し、ピアツーピア アプリケーション トラフィックを表す必要があります。次の接続の両方がルールをトリガーします。

```
10.42.0.105 to anywhere, using LimeWire
192.168.42.105 to anywhere, using Kazaa
```

ルールに特定の条件を設定しない場合、その条件によるトラフィック照合は行われません。たとえば、ネットワーク条件を持つがアプリケーション条件を持たないルールは、セッションで使用されるアプリケーションに関係なく、送信元または宛先に基づいてトラフィックを評価します。

注　アクセス コントロール ポリシーを適用すると、システムはすべてのルールを評価し、ネットワーク トラフィックを評価するためにターゲット デバイスが使用する基準の拡張セットを作成します。複雑なアクセス コントロール ポリシーおよびルールは、重要なリソースを消費する可能性があります。アクセス コントロール ルールを簡素化するヒントと、パフォーマンスを改善する他の方法については、アクセス コントロール ポリシーおよびルールのトラブルシューティング（12-25 ページ）を参照してください。

アクセス コントロール ルールを追加または編集するときは、ルール エディタの左下にあるタブを使用してルール条件を追加および編集します。次の表に、追加できる条件のタイプを示します。

表 14-1　アクセス コントロール ルール条件のタイプ

これらの条件	トラフィックの照合	Details
ゾーン	特定のセキュリティ ゾーン内のインターフェイスを介したデバイスへの着信またはデバイスからの発信トラフィック	「セキュリティ ゾーン」とは、展開方法やセキュリティ ポリシーに基づいて構成される 1 つ以上のインターフェイスの論理グループを指します。ゾーン内のインターフェイスが複数のデバイス間に配置される場合もあります。ゾーン条件の作成については、セキュリティ ゾーンによるトラフィックの制御（15-2 ページ）を参照してください。
Networks	その送信元または宛先の IP アドレス、国、または大陸で区別されるトラフィック	明示的に IP アドレスまたはアドレス ブロックを指定できます。位置情報の機能では、送信元または宛先となる国や大陸を基準にしたトラフィック制御もできます。ネットワーク条件の作成については、ネットワークまたは地理的位置によるトラフィックの制御（15-4 ページ）を参照してください。
VLAN タグ	VLAN によりタグ付けされたトラフィック	VLAN によるパケットの識別に最内部の VLAN タグが使用されます。VLAN 条件の作成については、VLAN トラフィックの制御（15-6 ページ）を参照してください。
ポート	送信元ポートまたは宛先ポート	TCP および UDP の場合、トランスポート層プロトコルに基づいてトラフィックを制御できます。ICMP および ICMPv6（IPv6 ICMP）の場合、インターネット層プロトコルと、オプションのタイプおよびコードに基づいてトラフィックを制御できます。ポート条件を使用して、ポートを使用しない他のプロトコルでトラフィックを制御することもできます。ポート条件の作成については、「ポートおよび ICMP コードによるトラフィックの制御（15-8 ページ）」を参照してください。
アプリケーション	セッションで検出されるアプリケーション	基本的な特性であるタイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグに応じて、個々のアプリケーションへのアクセスまたはフィルタ アクセスを制御できます。アプリケーション条件の作成については、「アプリケーション トラフィックの制御（16-2 ページ）」を参照してください。

表 14-1　アクセス コントロール ルール条件のタイプ（続き）

これらの条件	トラフィックの照合	Details
URL	セッションで要求された URL による	ネットワーク上のユーザが個別にまたは URL の一般的な分類とリスク レベルに基づいてアクセスできる Web サイトを制限できます。URL 条件の作成については、「URL のブロッキング（16-9 ページ）」を参照してください。
ユーザ	セッションに参加しているユーザ	モニタ対象セッションに参加するホストにログインした LDAP ユーザに基づいてトラフィックを制御できます。Microsoft Active Directory サーバから取得された個別ユーザまたはグループに基づいてトラフィックを制御できます。ユーザ条件の作成については、「ユーザに基づくトラフィックの制御（17-1 ページ）」を参照してください。

任意のライセンスを使ってアクセス コントロール ルールを作成できますが、ルール条件によっては、ポリシーを適用する前に、アクセス コントロール ポリシーのターゲット デバイスで特定のライセンス機能を有効にする必要があることに注意してください。詳細については、アクセス コントロールのライセンスおよびモデルの要件（12-3 ページ）を参照してください。

ルール アクションを使用したトラフィックの処理とインスペクションの決定

ライセンス： すべて

すべてのアクセス コントロール ルールには、一致するトラフィックについて次のことを決定する *アクション* があります。

- 処理：まず第一に、ルール アクションは、システムがルールの条件に一致するトラフィックをモニタ、信頼、ブロック、または許可するかどうかを制御します。
- インスペクション：特定のルール アクションでは、適切にライセンス付与されている場合、通過を許可する前に一致するトラフィックをさらに検査することができます。
- ロギング：ルール アクションによって、一致するトラフィックの詳細をいつ、どのようにログに記録できるかが決まります。

アクセス コントロール ポリシーの *デフォルト アクション* は、モニタ以外のどのアクセス コントロール ルールの条件にも一致しないトラフィックを処理します（デフォルトの処理の設定およびネットワーク トラフィックのインスペクション（12-7 ページ）を参照）。

インラインで展開されたデバイスのみがトラフィックをブロックまたは変更できることに留意してください。パッシブに展開されたデバイスまたはタップ モードで展開されたデバイスは、トラフィックのフローを分析およびロギングできますが、影響を与えることはできません。ルール アクションの詳細と、ルール アクションがトラフィックの処理、インスペクション、およびロギングにどのように影響するかについては、次の項を参照してください。

- モニタ アクション：アクションの遅延とログの確保（14-9 ページ）
- 信頼アクション：インスペクションなしでのトラフィックの通過（14-9 ページ）
- ブロッキング アクション：インスペクションなしでトラフィックをブロック（14-10 ページ）
- インタラクティブ ブロッキング アクション：ユーザが Web サイト ブロックをバイパスすることを許可する（14-11 ページ）
- 許可アクション：トラフィックの許可および検査（14-11 ページ）

- シリーズ 3 デバイスを使用したトラフィックの信頼またはブロックへの制限事項（14-13 ページ）
- 侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（18-1 ページ）
- アクセス コントロールの処理に基づく接続のロギング（38-17 ページ）

モニタ アクション：アクションの遅延とログの確保

ライセンス：すべて

モニタ アクションはトラフィック フローに影響を与えません。つまり、一致するトラフィックが直ちに許可または拒否されることはありません。その代わり、追加のルールに照らしてトラフィックが照合され、許可/拒否が決定されます。モニタ ルール以外の一致する最初のルールが、トラフィック フローおよび追加のインスペクションを決定します。さらに一致するルールがない場合、システムはデフォルト アクションを使用します。

モニタ ルールの主な目的はネットワーク トラフィックのトラッキングなので、システムはモニタ対象トラフィックの接続終了イベントを自動的にログに記録します。つまり、トラフィックが他のルールに一致せず、デフォルト アクションでロギングが有効になっていない場合でも、接続はログに記録されます。詳細については、モニタされた接続のロギングについて（38-7 ページ）を参照してください。

注　ローカル内トラフィックがレイヤ 3 展開のモニタ ルールに一致する場合、そのトラフィックはインスペクションをバイパスすることがあります。トラフィックのインスペクションを確実に実行するには、トラフィックをルーティングしている管理対象デバイスの詳細設定で [Inspect Local Router Traffic] を有効にします。詳細については、高度なデバイス設定について（4-58 ページ）を参照してください。

信頼アクション：インスペクションなしでのトラフィックの通過

ライセンス：すべて

信頼アクションでは、トラフィックはいかなる種類の追加のインスペクションなしで通過を許可されます。

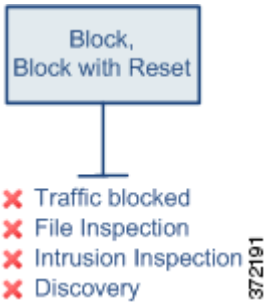
信頼されたネットワーク トラフィックは、接続の開始および終了の両方でログに記録できます。システムは、接続を検出したデバイスのモデルに応じて異なる信頼ルールによって処理される TCP 接続をロギングすることに注意してください。詳細については、信頼されている接続のロギングについて（38-7 ページ）を参照してください。

注意　シリーズ 3 デバイスによって処理されるトラフィックの場合は、システムはアクセス コントロール ポリシーのセキュリティ インテリジェンス ブラックリストの前に特定の信頼ルールを処理します。これによって、ブラックリスト登録されたトラフィックは検査されないまま通過することができます。詳細については、シリーズ 3 デバイスを使用したトラフィックの信頼またはブロックへの制限事項（14-13 ページ）を参照してください。

ブロッキング アクション：インスペクションなしでトラフィックをブロック

ライセンス：すべて

ブロック アクションおよび**リセット付きブロック** アクションはトラフィックを拒否し、いかなる種類の追加のインスペクションも行われません。リセット付きブロック ルールでは接続のリセットも行います。



暗号化されていない HTTPS トラフィックの場合、システムが Web 要求をブロックすると、デフォルトのブラウザまたはサーバのページを、接続が拒否されたことを説明するカスタム ページでオーバーライドすることができます。システムではこのカスタム ページを *HTTP 応答*ページと呼んでいます。ブロックされた URL のカスタム Web ページの表示（16-20 ページ）を参照してください。

復号化および暗号化された（HTTPS）トラフィックの場合、インタラクティブ ブロック ルールはインタラクションなしで一致する接続をブロックし、システムは応答ページを表示**しません**。

シリーズ 3 デバイスによって処理された一部の正常にブロックされたトラフィックに対し、システムは設定された応答ページを表示しないことに注意してください。その代わりに、ユーザの要求する禁止された URL の接続は、リセットまたはタイムアウトされます。詳細については、シリーズ 3 デバイスを使用したトラフィックの信頼またはブロックへの制限事項（14-13 ページ）を参照してください。

ブロックされたネットワーク トラフィックは、接続の開始時にのみログに記録できます。インライン で展開されたデバイスのみがトラフィックをブロックできることに注意してください。ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。詳細については、ブロックされた接続およびインタラクティブにブロックされた接続のロギングについて（38-8 ページ）を参照してください。

注意　サービス妨害（DoS）攻撃の間にブロックされた TCP 接続をロギングすると、システム パフォーマンスに影響し、複数の同様のイベントによってデータベースが過負荷になる可能性があります。ブロック ルールに対してロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたは DoS 攻撃を受けやすい他のインターフェイス上のトラフィックをモニタするかどうかを検討します。

インタラクティブ ブロッキング アクション：ユーザが Web サイト ブロックをバイパスすることを許可する

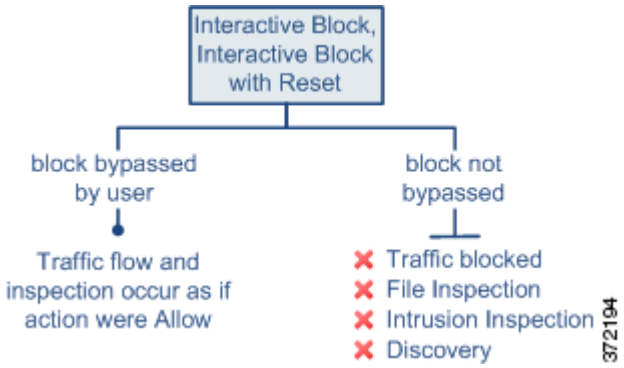
ライセンス：すべて

暗号化されていない HTTPS トラフィックの場合、**インタラクティブ ブロック** アクションおよび**リセット付きインタラクティブ ブロック** アクションを使用すると、ユーザはカスタマイズ可能な警告ページ（*HTTP 応答*ページと呼ばれます）をクリック スルーすることで、Web サイトのブロックをバイパスすることができます。リセット付きインタラクティブ ブロック ルールでは接続のリセットも行います。

注　復号化および暗号化された（HTTPS）トラフィックの場合、インタラクティブ ブロック ルールはインタラクションなしで一致する接続をブロックし、システムは応答ページを表示**しません**。トラフィックを復号化する SSL インスペクション機能を設定する詳細については、トラフィック復号化の概要（19-1 ページ）を参照してください。

インタラクティブにブロックされたすべてのトラフィックに対し、システムの処理、インスペクション、およびロギングは、ユーザがブロックをバイパスするかどうかによって異なります。

- ユーザがブロックをバイパスしない（できない）場合は、ルールはブロック ルールを模倣します。一致するトラフィックは追加のインスペクションなしで拒否され、接続の開始のみをロギングできます。これらの接続開始イベントには、`Interactive Block` または `Interactive Block with Reset` アクションが付きます。
- ユーザがブロックをバイパスする場合は、ルールは許可ルールを模倣します。このため、一方のタイプのインタラクティブ ブロック ルールをファイルおよび侵入ポリシーに関連付け、このユーザ許可されたトラフィックを検査できます。システムは、ネットワーク検出を使用してトラフィックを検査することもでき、接続の開始および終了イベントの両方をログに記録できます。これらの接続イベントには`Allow` アクションが付きます。



許可アクション：トラフィックの許可および検査

ライセンス：すべて

許可アクションにより、一致するトラフィックの通過が許可されます。トラフィックを許可すると、関連付けられた侵入ポリシーまたはファイル ポリシー（またはその両方）を使用して、暗号化されていないまたは復号化されたネットワーク トラフィックをさらに検査してブロックすることができます。

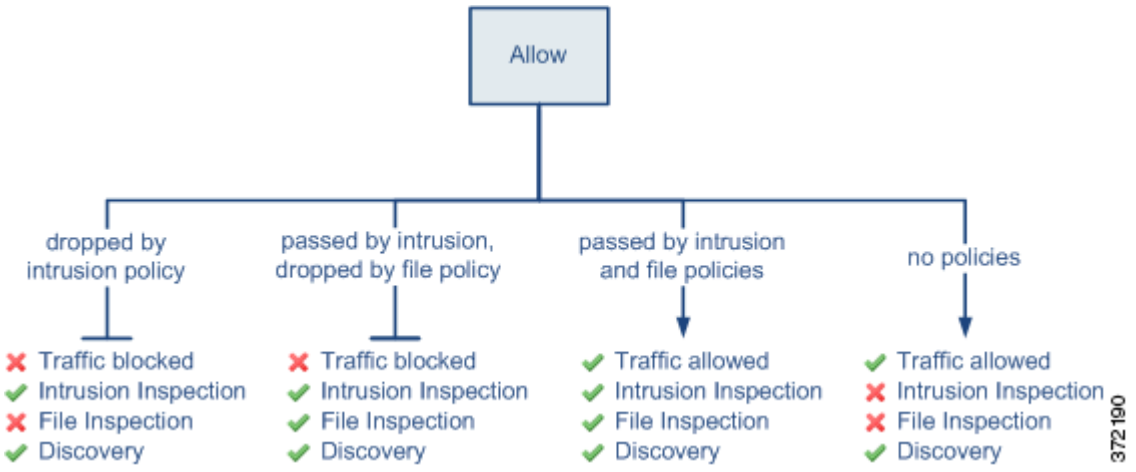
- Protection ライセンスを使用すると、侵入ポリシーを使用して、侵入検知および防御の設定に従ってネットワーク トラフィックを分析し、必要に応じて、有害なパケットをドロップできます。
- また、Protection ライセンスを使用すると、ファイル ポリシーを使用してファイル制御を実行できます。ファイル制御により、ユーザが特定のアプリケーション プロトコルを介して特定のタイプのファイルをアップロード（送信）またはダウンロード（受信）するのを検出およびブロックすることができます。
- Malware ライセンスを使用すると、この場合もファイル ポリシーを使用して、ネットワークベースの高度なマルウェア防御（AMP）を実行できます。ネットワークベースの AMP は、マルウェアの有無についてファイルを検査し、必要に応じて検出されたマルウェアをブロックできます。

侵入ポリシーまたはファイル ポリシーをアクセス コントロール ルールに関連付ける方法については、侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（18-1 ページ）を参照してください。

下の図に、許可ルールの条件（またはユーザによりバイパスされるインタラクティブ ブロック ルール（インタラクティブ ブロッキング アクション：ユーザが Web サイト ブロックをバイパスすることを許可する（14-11 ページ）を参照）の条件）を満たすトラフィックに対して実行されるインスペクションの種類を示します。侵入インスペクションの前にファイル インスペクションが行われることに注意してください。そこでブロックされたファイルに対しては、侵入関連の exploit は検査されません。

単純化のために、侵入ポリシーとファイル ポリシーの両方がアクセス コントロール ルールに関連付けられている状態（またはどちらも関連付けられていない状態）のトラフィック フローを図に示しています。ただし、いずれか一方を設定して他方は設定なしにすることもできます。ファイル ポリシーがない場合、トラフィック フローは侵入ポリシーが決定します。侵入ポリシーがない場合、トラフィック フローはファイル ポリシーが決定します。

トラフィックが侵入ポリシーとファイル ポリシーのどちらかによって検査またはドロップされるかどうかに関わらず、システムはネットワーク検出を使ってトラフィックを検査できます。ただし、トラフィックを許可することは検出インスペクションが自動的に保証されることではありません。システムは、ネットワーク検出ポリシーによって明示的にモニタされる IP アドレスを含む接続に対してのみ、検出を実行します。また、アプリケーション検出は、暗号化されたセッションに限定されます。詳細については、ネットワーク検出の概要（45-1 ページ）を参照してください。



許可されたネットワーク トラフィックは、接続の開始および終了の両方でログに記録することができます。

シリーズ 3 デバイスを使用したトラフィックの信頼またはブロックへの制限事項

ライセンス： すべて

サポートされるデバイス： シリーズ 3

シリーズ 3 デバイスにアクセス コントロール ポリシーを適用すると、システムは特定の基準を満たすアクセス コントロール ルールを*昇格させる*場合があります。昇格したルールは、シリーズ 3 デバイスで専用ハードウェアを使用して、ディープ パケット インスペクションを必要としないトラフィックを即座に転送またはブロックします。これを使用する利点は、トラフィックに適切なパスを判断する速度にあります。

この評価はハードウェア レベルで行われるため、システムは制限された情報を使用するだけで、ルールを昇格させることで接続を迅速に処理できます。シリーズ 3 デバイスは、次の基準をすべて満たすルールを昇格させます。

- **信頼**、**ブロック**、または**リセット付きブロック** アクションがある
- 単純でネットワークベースの条件（セキュリティ ゾーン、IP アドレス、VLAN タグ、およびポート）**のみ**を使用する
- ディープ パケット インスペクションを実行する、つまり、アプリケーション、URL、ユーザ、または位置情報ベースの条件を持つ他の**すべての**アクセス コントロール ルール（アクションに関係なく）の上に配置される
- また、**すべての**モニタ ルールの上に配置される

そのため、パフォーマンスが向上するために昇格されたルールは、アクセス コントロール ポリシー（下位番号を持つルール）の上部付近、または単純でネットワークベースのルールのみを使用するポリシーの任意の場所に配置される単純な信頼ルールまたはブロック ルールである可能性が高いです。しかし、ルールのプロモーションで実現されるパフォーマンス上の利点により、予期しない動作が発生する可能性があります。

セキュリティ インテリジェンスのプリエンプション処理

システムは、アクセス コントロール ポリシーのセキュリティ インテリジェンス ブラックリストの前に昇格したルールを処理します。これは、昇格した信頼ルールを使用して、ブラックリスト登録されたトラフィックが検査されることなく シリーズ 3 デバイスを通過できることを意味します。セキュリティ インテリジェンスの詳細については、セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録（13-1 ページ）を参照してください。

HTTP 応答ページの表示の阻止

システムがトラフィックを正常にブロックした場合でも、昇格したブロック ルールによってブロックされた Web トラフィックによってシステムが設定されている HTTP 応答ページをユーザに表示することはありません。その代わりに、ユーザの要求する禁止された URL の接続は、リセットまたはタイムアウトされます。応答ページの設定の詳細については、ブロックされた URL のカスタム Web ページの表示（16-20 ページ）を参照してください。

IPv6 トラフィックの処理

システムは、IPv4 トラフィックと IPv6 トラフィックの両方を検査できます。IPv6 インスペクションには 4in6、6in4、6to4、および 6in6 トンネリング方式が含まれます。また、UDP ヘッダーがポート 3544 を指定している場合は、Teredo トンネリングも含まれます。IP アドレス条件を持つアクセス コントロール ルールを使用してトラフィックを評価する際、ほとんどのケースで、シリーズ 3 デバイスはユーザが指定した IP アドレスを最内部のパケット ヘッダー内の IP アドレスと照合します。

しかし、そのトラフィックがトンネル化されているかどうかにかかわらず、また、IPv6 ヘッダーが最内部または最外部にあるかどうかにかかわらず、昇格したルールは**最外部の**ヘッダー内の IP アドレスを使用して IPv6 トラフィックを評価します。つまり、昇格したルールがトンネル化されたトラフィックを評価する場合、4in4 トラフィックのみが最内部のヘッダーを使用してアクセス コントロール ルールの基準と照合します。

たとえば、IPv4 ネットワークで送信された 6in4 トンネル化トラフィックの検査に シリーズ 3 デバイスを使用しているシナリオを考えます。特定の IPv6 アドレスで送受信されるトラフィックをブロックする単純なネットワークベースのアクセス コントロール ルールを作成します。システムがアクセス コントロール ポリシー内のその位置の結果としてルールを昇格させると、ルールは無効になります。これは、システムはトンネル化されたパケットの最外部の IPv4 ヘッダーを、決してトリガーされない IPv6 ルール条件に照合するためです。システムは、後続のアクセス コントロール ルールまたはポリシーのデフォルト アクション を使用して、ルールが存在していなかったかのようにトラフィックを処理します。

ルールへのコメントの追加

ライセンス： すべて

アクセス コントロール ルールを作成または編集するときは、コメントを追加できます。たとえば、他のユーザのために設定全体を要約したり、ルールの変更日と変更理由を記したりすることができます。あるルールの全コメントのリストを表示し、各コメントを追加したユーザやコメント追加日を確認することができます。

ヒント アクセス コントロール ルールを保存するときに、コメントを入力するように FireSIGHT システム ユーザにプロンプトを表示する（または強制する）には、アクセス コントロール ポリシー設定の構成（63-8 ページ）を参照してください。

ルールを保存すると、最後に保存してから追加されたすべてのコメントは読み取り専用になります。

コメントをルールに追加する方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1 アクセス コントロール ルール エディタで、[Comments] タブを選択します。

[Comments] ページが表示されます。

ステップ 2 [New Comment] をクリックします。

[New Comment] ポップアップ ウィンドウが表示されます。

ステップ 3 コメントを入力し、[OK] をクリックします。

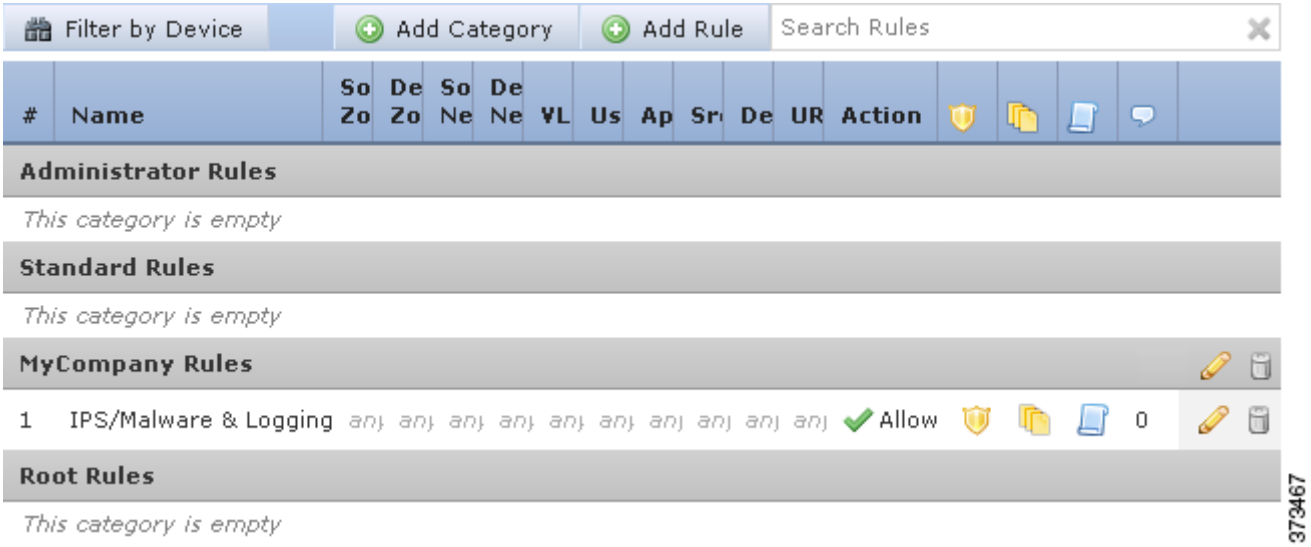
コメントが保存されます。ルールを保存するまでこのコメントを編集または削除できます。

ステップ 4 ルールを保存するか、編集を続けます。

ポリシー内のアクセス コントロール ルールの管理

ライセンス： すべて

次の図に示すアクセス コントロール ポリシー エディタの [Rules] タブでは、ポリシー内のアクセス コントロール ルールを追加、編集、検索、移動、有効化、無効化、削除、または管理できます。



各ルールで、ポリシー エディタには、ルールの名前、条件の概要、ルール アクション、およびルールのインスペクションおよびロギングのオプションを示すアイコンが表示されます。その他のアイコンは、次の表で説明するように、コメント、警告、エラー、およびその他の重要な情報を表します。無効なルールはグレーで表示され、ルール名の下に [(disabled)] というマークが付きます。

表 14-2　　アクセス コントロール ポリシー エディタについて

アイコン	説明	操作
	侵入インスペクション	ルールのインスペクション オプションを編集するには、アクティブな（黄色）インスペクション アイコンをクリックします。侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（18-1 ページ）を参照してください。アイコンが非アクティブ（白）の場合、そのタイプのポリシーがルールに選択されていません。
	ファイルおよびマルウェアのインスペクション	
	ロギング	ルールのロギング オプションを編集するには、アクティブな（青色）ロギング アイコンをクリックします。アクセス コントロールの処理に基づく接続のロギング（38-17 ページ）を参照してください。アイコンが非アクティブ（白）の場合、接続ロギングがそのルールで無効になっています。
	comment	ルールにコメントを追加するには、コメント列の数字をクリックします。ルールへのコメントの追加（14-14 ページ）を参照してください。数字は、ルールにすでに含まれているコメントの数を示します。

表 14-2　アクセス コントロール ポリシー エディタについて（続き）

アイコン	説明	操作
	warning	警告、エラーまたは情報のテキストを確認するにはアイコンにポインタを合わせます。アクセス コントロール ポリシーおよびルールのトラブルシューティング（12-25 ページ）を参照してください。
	error	
	情報	

アクセス コントロール ルールの管理については、以下を参照してください。

- アクセス コントロール ルールの作成および編集（14-3 ページ）
- アクセス コントロール ルールの検索（14-16 ページ）
- 影響を受けるデバイス別のルールの表示（14-17 ページ）
- ルールのイネーブル化とディセーブル化（14-17 ページ）
- ルールの位置またはカテゴリの変更（14-18 ページ）

アクセス コントロール ルールの検索

ライセンス： すべて

スペースおよび印刷可能な特殊文字を含む英数字文字列を使用して、アクセス コンロトール ルールのリストで一致する値を検索できます。この検索では、ルール名およびルールに追加したルール条件が検査されます。ルール条件の場合は、条件タイプ（ゾーン、ネットワーク、アプリケーションなど）ごとに追加できる任意の名前または値が検索照合されます。これには、個々のオブジェクト名または値、グループ オブジェクト名、グループ内の個々のオブジェクト名または値、およびリテラル値が含まれます。

検索文字列のすべてまたは一部を使用できます。照合ルールごとに、一致する値のカラムが強調表示されます。たとえば、`100Bao` という文字列のすべてまたは一部を基準に検索すると、少なくとも、100Bao アプリケーションを追加した各ルールの [Applications] カラムが強調表示されます。100Bao という名前のルールもある場合は、[Name] カラムと [Applications] カラムの両方が強調表示されます。

1 つ前または次の照合ルールに移動することができます。ステータス メッセージには、現行の一致および合計一致数が表示されます。

複数ページのルール リストでは、どのページでも一致が検出される可能性があります。最初の一致が検出されたのが最初のページではない場合は、最初の一致が検出されたページが表示されます。最後の一致が現行の一致となっている場合、次の一致を選択すると、最初の一致が表示されます。また、最初の一致が現行の一致となっている場合、前の一致を選択すると、最後の一致が表示されます。

ルールの検索方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　検索するポリシーのアクセス コントロール ポリシー エディタで、[Search Rules] プロンプトをクリックして、検索文字列を入力し、Enter を押します。検索を開始するには、Tab キーを使用するか、ページの空白部分をクリックします。

一致する値を含むルールのカラムが強調表示されます。表示されている（最初の）一致は、他とは区別できるように強調表示されます。

ステップ 2　目的のルールを探すには次の操作が利用できます。

- 照合ルールの間を移動する場合は、次の一致アイコン（ ）または前の一致アイコン（ ）をクリックします。
- ページを更新し、検索文字列および強調表示をクリアする場合は、クリア アイコン（ ）をクリックします。

影響を受けるデバイス別のルールの表示

ライセンス： すべて

アクセス コントロール ポリシーにリストされたアクセス コントロール ルールをフィルタリングし、1 つ以上の指定したデバイスのトラフィックを管理するルールのみを表示できます。

デバイスに影響を与えるルールを決定するために、システムはアクセス コントロール ルールのゾーン条件を使用します。セキュリティ ゾーンはインターフェイスの論理グループなので、ゾーン条件にインターフェイスが含まれている場合、そのインターフェイスが配置されているトラフィックを処理するデバイスは、そのルールの影響を受けます。ゾーン条件のないルールは任意のゾーンに適用されるので、すべてのデバイスに適用されることになります。

フィルタは、新しいルールを追加したり、既存のルールを編集して保存したりするとクリアされることに注意してください。

デバイスまたはデバイス グループを基準にルールをフィルタリングする方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　ルールをフィルタリングするポリシーのアクセス コントロール ポリシー エディタで、ルールのリストの上にある [Filter by Device] をクリックします。

[Filter by Device] ポップアップ ウィンドウが表示されます。ポリシーにデバイスまたはデバイス グループを追加してある場合は、ターゲットのデバイスおよびデバイス グループのリストが表示されます。

ステップ 2　1 つまたは複数のチェック ボックスをオンにして、これらのデバイスまたはグループに適用されるルールだけを表示します。リセットしてすべてのルールを表示するには、[All] チェック ボックスを選択します。

ステップ 3　[OK] をクリックします。

ページが更新されて、選択したデバイスおよびデバイス グループのルールが表示され、選択しなかったデバイスおよびデバイス グループのルールが非表示になります。

ルールのイネーブル化とディセーブル化

ライセンス： すべて

アクセス コントロール ルールを作成すると、デフォルトで有効になります。無効にしたルールはネットワーク トラフィックの評価には使用されなくなり、そのルールについての警告とエラーが停止されます。アクセス コントロール ポリシーでルールのリストを表示するとき、無効状態のルールはグレーで表示されますが、変更は可能です。また、ルール エディタを使用してアクセス コントロール ルールを有効化または無効化することもできます。アクセス コントロール ルールの作成および編集（14-3 ページ）を参照してください。

アクセス コントロール ルールの状態を変更するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　有効化または無効化するルールを含むポリシーのアクセス コントロール ポリシー エディタで、ルールを右クリックして、ルールの状態を選択します。

- 非アクティブなルールをイネーブルにするには、[State] > [Enable] を選択します。
- アクティブなルールを無効にするには、[State] > [Disable] を選択します。

ステップ 2　[Save] をクリックしてポリシーを保存します。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

ルールの位置またはカテゴリの変更

ライセンス： すべて

アクセス コントロール ルールを整理しやすくするために、すべてのアクセス コントロール ポリシーにはシステムによって提供された 3 つのルール カテゴリ（管理者ルール、標準ルール、ルート ルール）があります。これらのカテゴリの移動、削除、名前変更はできませんが、カスタム カテゴリの作成は可能です。

デフォルトでは、アクセス コントロール ポリシーの変更を許可する定義済みユーザ ロールによって、ルールのカテゴリ内またはカテゴリ間でアクセス コントロール ルールを移動および変更することもできます。ただし、ユーザによるルールの移動と変更を制限するカスタム ロールの作成も可能です。

詳細については、以下を参照してください。

- ルールの移動（14-18 ページ）
- 新しいルール カテゴリの追加（14-19 ページ）

ルールの移動

ライセンス： すべて

アクセス コントロール ルールの順序を適切にすることで、ネットワーク トラフィックの処理に必要なリソースが減り、ルールのプリエンプションを回避できます。デフォルトでは、アクセス コントロール ポリシーの変更を許可する定義済みユーザ ロールによって、ルールのカテゴリ内またはカテゴリ間でアクセス コントロール ルールを移動することもできます。ただし、システム提供のカテゴリにあるルールのユーザによる移動を制限するカスタム ロールの作成も可能です。

次の手順では、アクセス コントロール ポリシー エディタを使用して 1 つ以上のルールを同時に移動する方法について説明します。また、ルール エディタを使用して個々のアクセス コントロール ルールを移動することもできます。アクセス コントロール ルールの作成および編集（14-3 ページ）を参照してください。

規則を移動するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　移動するルールを含むポリシーのアクセス コントロール ポリシー エディタで、各ルールの空白領域をクリックしてルールを選択します。複数のルールを選択するには、Ctrl キーと Shift キーを使用します。

選択したルールは強調表示されます。

ステップ 2　ルールを移動します。カット アンド ペーストおよびドラッグ アンド ドロップを使用することもできます。

新しい場所にルールをカット アンド ペーストするには、選択したルールを右クリックし、[Cut] を選択します。次に、貼り付けたい位置に隣接するルールの空白部分を右クリックし、[Paste above] または [Paste below] を選択します。2 つの異なるアクセス コントロール ポリシー間ではアクセス コントロール ルールをコピー アンド ペーストできないことに注意してください。

ステップ 3　[Save] をクリックしてポリシーを保存します。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

新しいルール カテゴリの追加

ライセンス： すべて

アクセス コントロール ルールを整理しやすくするために、すべてのアクセス コントロール ポリシーにはシステムによって提供された 3 つのルール カテゴリ（管理者ルール、標準ルール、ルート ルール）があります。これらのカテゴリの移動、削除、名前変更はできませんが、Standard Rules と Root Rules 間でのカスタム カテゴリの作成は可能です。

カスタム カテゴリを追加すると、追加のポリシーを作成しなくても、ルールをさらに細かく編成できます。追加したカテゴリは、名前変更と削除ができます。これらのカテゴリの移動はできませんが、ルールのカテゴリ間およびカテゴリ内外への移動は可能です。

ユーザがシステムによって提供されるカテゴリ内のルールを移動したり変更しないように制限するカスタム ロールを作成できますが、アクセス コントロール ポリシーの変更権限が割り当てられているユーザは、制限なく、カスタム カテゴリにルールを追加したり、カテゴリ内のルールを変更したりできます。

新しいカテゴリを追加するには、次の手順に従います。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　ルール カテゴリを追加するポリシーのアクセス コントロール ポリシー エディタで、[Add Category] をクリックします。

ヒント　ポリシーにルールがすでに含まれている場合は、追加する前に既存のルールの行の空白部分をクリックすることで、新しいカテゴリの位置を設定できます。既存のルールを右クリックし、[Insert new category] を選択することもできます。

[Add Category] ポップアップ ウィンドウが表示されます。

ステップ 2　[Name] に、一意のカテゴリ名を入力します。

最大 30 文字の英数字の名前を入力できます。名前には、スペース、および印刷可能な特殊文字を含めることができます。

ステップ 3　次の選択肢があります。

- 既存のカテゴリのすぐ上に新しいカテゴリを配置する場合は、最初の [Insert] ドロップダウン リストから [above Category] を選択した後、2 番目のドロップダウン リストからカテゴリを選択します。ここで選択したカテゴリの上にルールが配置されます。
- 既存のルールの下に新しいカテゴリを配置する場合は、ドロップダウン リストから [below rule] を選択した後、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。
- 既存のルールの上にルールを配置する場合は、ドロップダウン リストから [above rule] を選択した後、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。

ステップ 4　[OK] をクリックします。

カテゴリが追加されます。名前を編集するには、カスタム カテゴリの横にある編集アイコン（ ）をクリックします。カテゴリを削除するには、削除アイコン（ ）をクリックします。削除するカテゴリに含まれるルールは、その上にあるカテゴリに追加されます。

ステップ 5　[Save] をクリックしてポリシーを保存します。

ネットワークベースのルールによるトラフィックの制御

*アクセス コントロール ポリシー*の*アクセス コントロール ルール*を設定すると、ネットワーク トラフィックのロギングや処理を詳細に制御できます。ネットワークベースの条件を使用して、ネットワークを通過するトラフィックを管理できます。以下の条件を使用できます。

- 送信元と宛先のセキュリティ ゾーン
- 送信元と宛先の IP アドレスまたは地理的位置
- パケット最内部の VLAN タグ
- トランスポート層プロトコルおよび ICMP コード オプションを含む、送信元と宛先のポート

ネットワークベースの複数の条件を組み合わせたり、他のタイプの条件と組み合わせたりして、アクセス コントロール ルールを作成できます。これらのアクセス コントロール ルールは単純にも複雑にも設定でき、複数の条件を使用してトラフィックを照合および検査できます。アクセス コントロール ルールの詳細については、アクセス コントロール ルールを使用したトラフィック フローの調整（14-1 ページ）を参照してください。

注 ハードウェアベースの高速パス ルール、セキュリティ インテリジェンス ベースのトラフィック フィルタリング、および一部の復号化と前処理は、ネットワーク トラフィックがアクセス コントロール ルールによって評価される**前に**行われます。また、*SSL インスペクション*機能を設定すると、暗号化されたトラフィックをアクセス コントロール ルールが評価する前にブロックしたり復号化したりできます。

すべての FireSIGHT システム アプライアンスおよびすべてのライセンスでほとんどのネットワークベースのアクセス制御を実行できます。ただし、位置情報ベースのアクセス制御には FireSIGHT ライセンスが必要で、多くの シリーズ 2 アプライアンスでサポートされておらず、Cisco NGIPS for Blue Coat X-Series でもサポートされていません。また、ASA FirePOWER デバイスは、VLAN によるアクセス制御をサポートしていません。

表 15-1　ネットワークベースのアクセス コントロール ルールのライセンスおよびモデルの要件

要件	グループ化	位置情報制御	他のすべてのネットワーク ベースの制御
license	いずれか	FireSIGHT	いずれか
devices	すべて（ASA FirePOWER を除く）	シリーズ 3 virtual ASA FirePOWER	いずれか
Defense Center	いずれか	すべて（DC500 を除く）	いずれか

ネットワークベースのアクセス コントロール ルールの作成については、以下を参照してください。

- セキュリティ ゾーンによるトラフィックの制御（15-2 ページ）
- ネットワークまたは地理的位置によるトラフィックの制御（15-4 ページ）
- VLAN トラフィックの制御（15-6 ページ）
- ポートおよび ICMP コードによるトラフィックの制御（15-8 ページ）

セキュリティ ゾーンによるトラフィックの制御

ライセンス： すべて

アクセス コントロール ルールでゾーン条件を設定すると、トラフィックの送信元および宛先のセキュリティ ゾーンに応じてそのトラフィックを制御できます。*セキュリティ ゾーン*とは、1 つ以上のインターフェイスの論理グループを指します。ゾーン内のインターフェイスが複数のデバイス間に配置される場合もあります。デバイスの初回セットアップ時に選択する *検出モード* オプションによって、デバイスで最初に設定されるインターフェイスおよびこれらのインターフェイスが属するセキュリティ ゾーンが決定されます。

単純な例として、**インライン**検出モードを選択したデバイスでは、Defense Centerにより内部と外部の 2 つのゾーンが作成され、そのデバイスの最初のインターフェイスのペアがそれらのゾーンに割り当てられます。内部側ネットワークに接続されたホスト群が、保護されたアセットに相当します。

このシナリオを拡張すると、同等に設定された追加デバイス（同じDefense Centerによって管理されるもの）を展開して、複数の異なるロケーションで同様のリソースを保護できます。最初のデバイスと同様に、これらのデバイスも内部セキュリティ ゾーンのアセットを保護します。

ヒント　内部（または外部）のすべてのインターフェイスを 1 つのゾーンにグループ化する必要はありません。展開方法およびセキュリティ ポリシーに適したグループ化を選択できます。ゾーン作成の詳細については、セキュリティ ゾーンの操作（3-42 ページ）を参照してください。

この展開では、これらのホストにインターネットへの無制限アクセスを提供できますが、着信トラフィックで侵入およびマルウェアの有無を検査してホストを保護しなければなりません。

アクセス コントロールを使用してこれを実現するには、[Destination Zone] を [Internal] に設定したゾーン条件をアクセス コントロール ルールに定義します。この単純なアクセス コントロール ルールでは、内部ゾーンのいずれかのインターフェイスからデバイスを離れるトラフィックが照合されます。

一致するトラフィックが侵入やマルウェアついて確実に検査されるようにするには、ルール アクションとして **Allow** を選択し、そのルールを侵入ポリシーとファイル ポリシーに関連付けます。詳細については、ルール アクションを使用したトラフィックの処理とインスペクションの決定（14-8 ページ）および侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（18-1 ページ）を参照してください。

より複雑なルールを作成する場合は、1 つのゾーン条件で [Source Zones] および [Destination Zones] それぞれに対し、最大 50 のゾーンを追加できます。

- 特定のゾーンのインターフェイスからデバイスを*離れる*トラフィックを照合するには、そのゾーンを [Destination Zones] に追加します。

  パッシブに展開されたデバイスはトラフィックを送信しないので、パッシブ インターフェイスで構成されるゾーンを [Destination Zones] 条件で使用することはできません。
- 特定のゾーンのインターフェイスからデバイスに*入る*トラフィックを照合するには、そのゾーンを [Source Zones] に追加します。
- 送信元（Source）ゾーン条件と宛先（Destination）ゾーン条件の両方をルールに追加する場合、送信元ゾーンから発信され**かつ**宛先ゾーンを介して出力されるトラフィックにルールが適用されます。

ゾーン内のすべてのインターフェイスが同じタイプ（インライン、パッシブ、スイッチド、またはルーテッド）である必要があるため、アクセス コントロール ルールのゾーン条件で使用されているすべてのゾーンが同じタイプでなければならないことに注意してください。つまり、異なるタイプのゾーンを送信元/宛先とするトラフィックを照合する単一ルールを定義することはできません。

無効なゾーン条件設定が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。また、アクセス コントロール ポリシーおよびルールのトラブルシューティング（12-25 ページ）を参照してください。

ゾーン条件に基づいてトラフィックを制御するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　ゾーンに応じたトラフィック制御を設定するデバイス用のアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集（14-3 ページ）を参照してください。

ステップ 2　ルール エディタで、[Zones] タブを選択します。

[Zones] タブが表示されます。

ステップ 3　[Available Zones] で、追加するゾーンを選択します。

追加するゾーンを検索するには、[Available Zones] リストの上にある [Search by name] プロンプトをクリックし、ゾーン名を入力します。ゾーン名の入力を開始するとリストが更新され、一致するゾーンが表示されます。

ゾーンをクリックして選択します。複数のゾーンを選択するには、Shift キーまたは Ctrl キーを使用します。すべてのゾーンを選択するには、右クリックして [Select All] を選択します。

ステップ 4　[Add to Source] または [Add to Destination] をクリックして、選択したゾーンを適切なリストに追加します。

選択したゾーンをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5　ルールを保存するか、編集を続けます。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

ネットワークまたは地理的位置によるトラフィックの制御

ライセンス： 機能によって異なる

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

アクセス コントロール ルールでネットワーク条件を設定すると、トラフィックの送信元および宛先の IP アドレスに応じてそのトラフィックを制御できます。次のいずれかの操作を実行できます。

- 制御するトラフィックの送信元および宛先の IP アドレスを明示的に指定する。
- IP アドレスを地理的位置に関連付ける位置情報機能を使用して、その送信元または宛先の国または大陸に基づいてトラフィックを制御する。

ネットワークベースのアクセス コントロール ルールの条件を作成する場合、IP アドレスと地理的位置を手動で指定できます。または、ネットワークおよび位置情報の*オブジェクト*を使用してネットワーク条件を設定することもできます。これらのオブジェクトは、いくつかの IP アドレス、アドレス ブロック、国、大陸などに名前を付けて再利用可能にしたものを指します。

ヒント　ネットワーク オブジェクトや位置情報オブジェクトを作成しておくと、それを使用してアクセス コントロール ルールを作成したり、Web インターフェイスのさまざまな場所で IP アドレスを表すオブジェクトとして使用したりできます。これらのオブジェクトはオブジェクト マネージャを使用して作成できます。また、アクセス コントロール ルールの設定時にネットワーク オブジェクトを作成することもできます。詳細については、再利用可能なオブジェクトの管理（3-1 ページ）を参照してください。

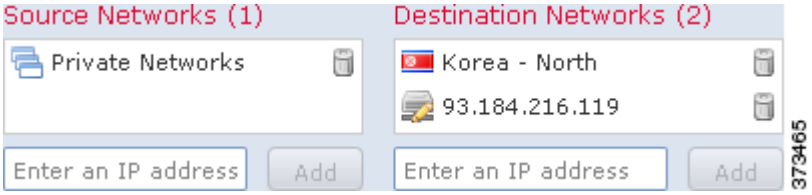
地理的位置別にトラフィックを制御するルールを作成する場合は、確実に最新の位置情報データを使用してトラフィックをフィルタ処理する必要があります。このため、CiscoではDefense Centerの位置情報データベース（GeoDB）を定期的に更新することを**強く**推奨しています。地理情報データベースについて（66-30 ページ）を参照してください。

また、すべての FireSIGHT システム アプライアンスおよびすべてのライセンスで単純な IP アドレス ベースのアクセス制御を実行できます。ただし、位置情報ベースのアクセス制御には FireSIGHT ライセンスが必要で、多くの シリーズ 2 アプライアンスでサポートされておらず、Cisco NGIPS for Blue Coat X-Series でもサポートされていません。

表 15-2　ネットワーク条件のライセンスおよびモデルの要件

要件	位置情報制御	IP アドレス制御
license	FireSIGHT	いずれか
devices	シリーズ 3、仮想、ASA FirePOWER	いずれか
Defense Center	すべて（DC500 を除く）	いずれか

次の図は、内部ネットワークから発生し、北朝鮮または 93.184.216.119（example.com）のリソースにアクセスしようとする接続をブロックするアクセス コントロール ルールのネットワーク条件を示しています。



この例で、「Private Networks」と呼ばれるネットワーク オブジェクト グループ（図に示されていない IPv4 および IPv6 プライベート ネットワークのネットワーク オブジェクトから構成されます）は、内部ネットワークを表します。また、example.com の IP アドレスを手動で指定し、システムが提供する北朝鮮の位置情報オブジェクトを使用して北朝鮮の IP アドレスを表しています。

1 つのネットワーク条件で [Source Networks] および [Destination Networks] それぞれに最大 50 の項目を追加でき、ネットワークベースの設定と位置情報ベースの設定を組み合わせることができます。

- 特定の IP アドレスまたは地理的位置からのトラフィックを照合するには、[Source Networks] を設定します。
- 特定の IP アドレスまたは地理的位置へのトラフィックを照合するには、[Destination Networks] を設定します。

送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信され**かつ**宛先 IP アドレスに送信されるトラフィックにルールが適用されます。

無効なネットワーク条件設定が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。また、アクセス コントロール ポリシーおよびルールのトラブルシューティング（12-25 ページ）を参照してください。

ネットワークまたは地理的位置の条件に応じてトラフィックを制御するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　ネットワークに応じたトラフィック制御を設定するデバイス用のアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集（14-3 ページ）を参照してください。

ステップ 2　ルール エディタで、[Networks] タブを選択します。

[Networks] タブが表示されます。

ステップ 3　[Available Networks] で、追加するネットワークを選択します。

- [Networks] タブをクリックすると追加可能なネットワーク オブジェクトとグループが表示され、[Geolocation] タブをクリックすると位置情報オブジェクトが表示されます。
- ここでネットワーク オブジェクトを作成してリストに追加するには、[Available Networks] リストの上にある追加アイコン（ ）をクリックし、ネットワーク オブジェクトの操作（3-4 ページ）の手順に従います。

- 追加するネットワーク オブジェクトまたは位置情報オブジェクトを検索するには、適切なタブを選択し、[Available Networks] リストの上にある [Search by name or value] プロンプトをクリックして、オブジェクト名またはオブジェクトのいずれかの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

オブジェクトをクリックして選択します。複数のオブジェクトを選択するには、Shift キーまたは Ctrl キーを使用します。すべてのオブジェクトを選択するには、右クリックして [Select All] を選択します。

ステップ 4　[Add to Source] または [Add to Destination] をクリックして、選択したオブジェクトを適切なリストに追加します。

選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5　手動で指定する送信元または宛先の IP アドレスまたはアドレス ブロックを追加します。

[Source Networks] リストまたは [Destination Networks] リストの下にある [Enter an IP address] プロンプトをクリックし、IP アドレスまたはアドレス ブロックを入力して [Add] をクリックします。

ステップ 6　ルールを保存するか、編集を続けます。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

VLAN トラフィックの制御

ライセンス： すべて

サポートされるデバイス： すべて（ASA FirePOWER を除く）

アクセス コントロール ルールで VLAN 条件を設定すると、トラフィックの VLAN タグに応じてそのトラフィックを制御できます。VLAN によるパケットの識別に最内部の VLAN タグが使用されます。

VLAN ベースのアクセス コントロール ルール条件を作成するときは、VLAN タグを手動で指定できます。または、VLAN タグ *オブジェクト*を使用して VLAN 条件を設定することもできます。VLAN タグ オブジェクトとは、いくつかの VLAN タグに名前を付けて再利用可能にしたものを指します。

ヒント　VLAN タグ オブジェクトを作成しておくと、それを使用してアクセス コントロール ルールを作成したり、Web インターフェイスのさまざまな場所で VLAN タグを表すオブジェクトとして使用したりできます。VLAN タグ オブジェクトはオブジェクト マネージャを使用して作成できます。また、アクセス コントロール ルールの設定時に作成することもできます。詳細については、VLAN タグ オブジェクトの操作（3-14 ページ）を参照してください。

次の図は、特定の公開 VLAN（VLAN タグ オブジェクト グループで指定）および手動で追加した VLAN「42」上のトラフィックに一致するアクセス コントロール ルールの VLAN タグ条件を示しています。

1 つの VLAN タグ条件で、[Selected VLAN Tags] に最大 50 の項目を追加できます。無効な VLAN タグ条件設定が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。また、アクセス コントロール ポリシーおよびルールのトラブルシューティング（12-25 ページ）を参照してください。

VLAN タグに基づいてトラフィックを制御するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　VLAN タグに応じたトラフィック制御を設定するデバイス用のアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集（14-3 ページ）を参照してください。

ステップ 2　ルール エディタで、[VLAN Tags] タブを選択します。

[VLAN Tags] タブが表示されます。

ステップ 3　[Available VLAN Tags] で、追加する VLAN を選択します。

- ここで VLAN タグ オブジェクトを作成してリストに追加するには、[Available VLAN Tags] リストの上にある追加アイコン（ ）をクリックし、VLAN タグ オブジェクトの操作（3-14 ページ）の手順に従います。
- 追加する VLAN タグ オブジェクトおよびグループを検索するには、[Available VLAN Tags] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクト名またはオブジェクトの VLAN タグの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

オブジェクトをクリックして選択します。複数のオブジェクトを選択するには、Shift キーまたは Ctrl キーを使用します。すべてのオブジェクトを選択するには、右クリックして [Select All] を選択します。

ステップ 4　[Add to Rule] をクリックして、選択したオブジェクトを [Selected VLAN Tags] リストに追加します。

選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5　手動で指定する VLAN タグを追加します。

[Selected VLAN Tags] リストの下にある [Enter a VLAN Tag] プロンプトをクリックし、VLAN タグまたはその範囲を入力して、[Add] をクリックします。1 から 4094 までの任意の VLAN タグを指定できます。VLAN タグの範囲を指定するにはハイフンを使用します。

ステップ 6　ルールを保存するか、編集を続けます。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

ポートおよび ICMP コードによるトラフィックの制御

ライセンス： すべて

アクセス コントロール ルールでネットワーク条件を設定すると、トラフィックの送信元および宛先のポートに応じてそのトラフィックを制御できます。このセクションで「ポート」は次のいずれかを指します。

- TCP および UDP の場合、トランスポート層プロトコルに基づいてトラフィックを制御できます。この設定では、カッコ内の数値がプロトコル番号を示し、その後にオプションの関連ポートまたはポート範囲が続きます。例：TCP(6)/22。
- ICMP および ICMPv6（IPv6 ICMP）の場合、インターネット層プロトコルと、オプションのタイプおよびコードに基づいてトラフィックを制御できます。例：ICMP(1):3:3。
- ポートを使用しない他のプロトコルを使用してトラフィックを制御できます。

ポートベースのアクセス コントロール ルールの条件を作成するときは、手動でポートを指定できます。または、ポート *オブジェクト*を使用してポート条件を設定することもできます。ポート オブジェクトとは、いくつかのポートに名前を付けて再利用可能にしたものを指します。

ヒント　ポート オブジェクトを作成しておくと、それを使用してアクセス コントロール ルールを作成したり、Web インターフェイスのさまざまな場所でポートを表すオブジェクトとして使用したりできます。ポート オブジェクトは、オブジェクト マネージャを使用して作成できます。また、アクセス コントロール ルールの設定時に作成することもできます。詳細については、ポート オブジェクトの操作（3-13 ページ）を参照してください。

1 つのネットワーク条件で [Selected Source Ports] および [Selected Destination Ports] リストそれぞれに対し、最大 50 の項目を追加できます。

- 特定のポート*から*のトラフィックを照合するには、[Selected Source Ports] を設定します。

  条件に送信元ポートだけを追加する場合は、異なるトランスポート プロトコルを使用するポートを追加できます。たとえば、DNS over TCP および DNS over UDP の両方を 1 つのアクセス コントロール ルールの送信元ポート条件として追加できます。

- 特定のポート*へ*のトラフィックを照合するには、[Selected Destination Ports] を設定します。

  条件に宛先ポートだけを追加する場合は、異なるトランスポート プロトコルを使用するポートを追加できます。

- [Selected Source Ports] および [Selected Destination Ports] の両方を設定すると、特定の送信元（Source）ポートから発信され*かつ*特定の宛先（Destination）ポートに送信されるトラフィックが照合されます。

  送信元ポートと宛先ポートの両方を条件に追加する場合は、単一のトランスポート プロトコル（TCP または UDP）を使用するポートのみを追加できます。たとえば、送信元ポートとして DNS over TCP を追加する場合、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat（UDP）は追加できません。

ポート条件を作成するときは、次の点に注意してください。

- タイプ 0 が設定された宛先 ICMP ポート、またはタイプ 129 が設定された宛先 ICMPv6 ポートを追加すると、要求されていないエコー応答だけがアクセス コントロール ルールで照合されます。ICMP エコー要求への応答として送信される ICMP エコー応答は無視されます。ルールですべての ICMP エコーに一致させるには、ICMP タイプ 8 または ICMPv6 タイプ 128 を使用してください。
- 宛先ポート条件として GRE（47）プロトコルを使用する場合、アクセス コントロール ルールに追加できるのは、他のネットワークベースの条件（つまりゾーン、ネットワーク、および VLAN タグ条件）のみです。レピュテーションまたはユーザ ベースの条件を追加する場合は、ルールを保存できません。

無効なポート条件が検出されると、警告アイコンが表示されます。たとえば、既存のポート オブジェクトをオブジェクト マネージャで編集すると、それらのオブジェクト グループを使用するルールが無効になります。アイコンの上にポインタを置くと詳細が表示されます。また、アクセス コントロール ポリシーおよびルールのトラブルシューティング（12-25 ページ）を参照してください。

ポート条件に基づいてトラフィックを制御するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　ポートに応じたトラフィック制御を設定するデバイス用のアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集（14-3 ページ）を参照してください。

ステップ 2　ルール エディタで、[Ports] タブを選択します。

[Ports] タブが表示されます。

ステップ 3　[Available Ports] で、追加するポートを選択します。

- ここでポート オブジェクトを作成してリストに追加するには、[Available Ports] リストの上にある追加アイコン（）をクリックし、ポート オブジェクトの操作（3-13 ページ）の手順に従います。
- 追加するポート オブジェクトおよびグループを検索するには、[Available Ports] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクトの名前またはオブジェクトのポートの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。たとえば、「80」と入力すると、Cisco提供の HTTP ポート オブジェクトがDefense Centerに表示されます。

  オブジェクトをクリックして選択します。複数のオブジェクトを選択するには、Shift キーまたは Ctrl キーを使用します。すべてのオブジェクトを選択するには、右クリックして [Select All] を選択します。

ステップ 4　[Add to Source] または [Add to Destination] をクリックして、選択したオブジェクトを適切なリストに追加します。

選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5　手動で指定する送信元または宛先のポートを追加します。

- 送信元ポートの場合は、[Selected Source Ports] リストの下の [Protocol] ドロップダウンリストから [TCP] または [UDP] を選択します。次に、[Port] にポート番号を入力します。0 ～ 65535 の値を持つ 1 つのポートを指定できます。

- 宛先ポートの場合は、[Selected Destination Ports] リストの下の [Protocol] ドロップダウンリストからプロトコル（すべてのプロトコルの場合は [All]）を選択します。リストに表示されない未割り当てのプロトコルのポート番号を入力することもできます。

  [ICMP] または [IPv6-ICMP] を選択すると、タイプと関連コードを選択するためのポップアップ ウィンドウが表示されます。ICMP のタイプとコードの詳細については、http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml および http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml を参照してください。

  プロトコルを指定しない場合、またはオプションで TCP または UDP を指定した場合は、[Port] にポート番号を入力します。0 ～ 65535 の値を持つ 1 つのポートを指定できます。

[Add] をクリックします。Defense Centerでは、無効なポート設定はルール条件に追加されません。

ステップ 6　ルールを保存するか、編集を続けます。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

レピュテーション ベースのルールによるトラフィックの制御

*アクセス コントロール ポリシー*の*アクセス コントロール ルール*を設定すると、ネットワーク トラフィックのロギングや処理を詳細に制御できます。アクセス コントロール ルールのレピュテーション ベースの条件を使用することで、ネットワーク トラフィックを文脈によって解釈可能にし、必要に応じて制限することで、ネットワークを通過できるトラフィックを管理できます。アクセス コントロール ルールは、次のタイプのレピュテーション ベースの制御を管理します。

- アプリケーション条件を使用することで、*アプリケーション制御*を実行できます。これによって、個々のアプリケーションだけでなく、アプリケーションの基本的な特性であるタイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグに基づいてアプリケーション トラフィックが制御されます。
- URL 条件を使用することで、*URL フィルタリング*を実行できます。これによって、個々の Web サイトだけでなく、Web サイトのシステムによって割り当てられたカテゴリおよびレピュテーションに基づいて Web トラフィックが制御されます。

レピュテーション ベースの条件を互いに組み合わせたり、他のタイプの条件と組み合わせて、アクセス コントロール ルールを作成することができます。これらのアクセス コントロール ルールは単純にも複雑にも設定でき、複数の条件を使用してトラフィックを照合および検査できます。アクセス コントロール ルールの詳細については、アクセス コントロール ルールを使用したトラフィック フローの調整（14-1 ページ）を参照してください。

注 ハードウェアベースの高速パス ルール、セキュリティ インテリジェンス ベースのトラフィック フィルタリング、および一部の復号化と前処理は、ネットワーク トラフィックがアクセス コントロール ルールによって評価される**前に**行われます。また、*SSL インスペクション*機能を設定すると、暗号化されたトラフィックをアクセス コントロール ルールが評価する前にブロックしたり復号化したりできます。

レピュテーション ベースのアクセス コントロールには、次のライセンス、デバイス、および Defense Center が必要です。

表 16-1　レピュテーション ベースのアクセス コントロール ルールのライセンスおよびモデルの要件

要件	アプリケーション管理	URL フィルタリング（カテゴリおよびレピュテーション）	URL フィルタリング（手動）
license	Control	URL Filtering	いずれか
デバイス	すべて（シリーズ 2 または X-Series を除く）	すべて（シリーズ 2 を除く）	すべて（シリーズ 2 を除く）
Defense Center	いずれか	すべて（DC500 を除く）	いずれか

アクセス コントロール ルールにレピュテーション ベースの条件を追加する方法については、以下を参照してください。

- アプリケーション トラフィックの制御（16-2 ページ）
- URL のブロッキング（16-9 ページ）

FireSIGHT システム は、他のタイプのレピュテーション ベースの制御を実行できますが、アクセス コントロール ルールを使用してこれらを設定しないでください。詳細については、以下を参照してください。

- セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録（13-1 ページ）では、最初の防御ラインとして、接続の発信元または宛先のレピュテーションに基づいてトラフィックを制限する方法について説明します。
- 侵入防御パフォーマンスの調整（18-10 ページ）では、マルウェアおよび他のタイプの禁止されたファイルの送信を検出、追跡、保存、分析、およびブロックする方法について説明します。

アプリケーション トラフィックの制御

ライセンス： Control

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

FireSIGHT システム が IP トラフィックを分析するときは、ネットワークで一般的に使用されるアプリケーションを識別および分類できます。システムがこの検出ベースの *アプリケーション認識*機能を使用することで、ユーザはネットワーク上でアプリケーション トラフィックを制御できます。

アプリケーション制御について

アクセス コントロール ルールのアプリケーション条件を使用することで、この *アプリケーション制御*を実行することができます。1 つのアクセス コントロール ルール内には、トラフィックを制御するアプリケーションを指定する方法がいくつかあります。

- 各アプリケーションを個別に選択する（カスタム アプリケーションを含む）。
- システムによって提供される *アプリケーション フィルタ*を使用できます。このフィルタは、アプリケーションの基本的な特性であるタイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグに基づいて編成されたアプリケーションの名前付きセットです。
- カスタム アプリケーション フィルタを作成して使用する。このフィルタでは、任意の方法でアプリケーションをグループ化できます（カスタム アプリケーションを含む）。

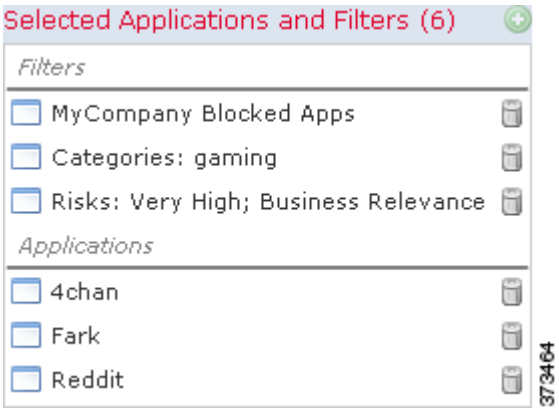
アプリケーション フィルタを使用することで、アクセス コントロール ルールに対しアプリケーション条件をすぐに作成することができます。これによりポリシーの作成と管理が簡素化され、Web トラフィックを意図したとおりに制御できます。たとえば、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックするアクセス コントロール ルールを作成できます。ユーザがそれらのアプリケーションの 1 つを使用しようとすると、セッションがブロックされます。

さらに、Ciscoでは、システムおよび脆弱性データベース（VDB）の更新を通して頻繁にディテクタを更新し追加しています。独自のディテクタを作成して、検出するアプリケーションの特性（リスク、関連性など）を割り当てることも可能です。アプリケーション特性に基づくフィルタを使用すると、最新のディテクタを使用してアプリケーション トラフィックをモニタできます。

アプリケーション条件の作成

トラフィックがアプリケーション条件を持つアクセス コントロール ルールに一致するには、トラフィックが [Selected Applications and Filters] リストに追加したフィルタまたはアプリケーションの 1 つに一致している必要があります。

次の図は、MyCompany のアプリケーションのカスタム グループ、リスクが高くビジネスとの関連性が低いすべてのアプリケーション、ゲーム アプリケーション、および個々に選択されたいくつかのアプリケーションをブロックするアクセス コントロール ルールのアプリケーション条件を示しています。



1 つのアプリケーション条件で [Selected Applications and Filters] リストに最大 50 の項目を追加できます。1 つの項目として扱われるものは以下のとおりです。

- [Application Filters] リストにある 1 つまたは複数のフィルタ（個別または組み合わせたもの）。この項目は、特性を基準にグループ化されたアプリケーションのセットです。
- [Available Applications] リストでアプリケーションの検索を保存することで作成されるフィルタ。この項目は、アプリケーション名の一部の一致によってグループ化されたアプリケーションのセットです。
- [Available Applications] リストにある個別のアプリケーション。

Web インターフェイス上では、条件に追加したフィルタが個別に追加したアプリケーションの上に一覧表示されます。

アプリケーション条件を持つ各ルールに対し、アクセス コントロール ポリシーを追加すると、システムは一意のアプリケーションのリストを生成して照合することに留意してください。このため、重複するフィルタと個別指定のアプリケーションを使用して、意図したとおりのアプリケーション セットにポリシーを適用できます。

注　暗号化されたトラフィックの場合、システムは [SSL Protocol] とタグ付けされたアプリケーションだけを使用して、トラフィックを識別およびフィルタリングできます。このタグがないアプリケーションは、暗号化されていないまたは復号化されたトラフィックでのみ検出できます。また、システムは、復号化されたトラフィック（暗号化されたまたは暗号化されていないトラフィックではなく）のみで検出を行うことができるアプリケーションに **decrypted traffic** タグを割り当てます。SSL インスペクション機能を使用して、システムがアクセス コントロール ルールと照合する前に暗号化されたトラフィックを復号化またはブロックする方法については、トラフィック復号化の概要（19-1 ページ）を参照してください。

詳細については、次の項を参照してください。

- トラフィックとアプリケーション フィルタの一致（16-4 ページ）
- 個々のアプリケーションとトラフィックの照合（16-5 ページ）
- アクセス コントロール ルールへのアプリケーション条件の追加（16-7 ページ）
- アプリケーション制御の制約事項（16-8 ページ）

トラフィックとアプリケーション フィルタの一致

ライセンス： Control

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

アクセス コントロール ルールでアプリケーション条件を作成するときは、[Application Filters] リストを使用して、特性によってグループ化されたトラフィックを照合するアプリケーションのセットを作成します。

アプリケーションの検出基準について詳しくは、表 45-2（45-12 ページ）を参照してください。これらの基準をフィルタとして使用したり、独自の組み合わせでカスタム フィルタを作成したりしてアプリケーションを制御できます。

アクセス コントロール ルール内でアプリケーションをフィルタリングするメカニズムは、オブジェクト マネージャを使用して再利用可能なカスタム アプリケーション フィルタを作成するメカニズムと同じです。アプリケーション フィルタの操作（3-16 ページ）を参照してください。また、アクセス コントロール ルールの設定時に作成する各種のフィルタを、新規のフィルタとして保存して再利用することもできます。ユーザ作成のフィルタを入れ子にすることはできないため、別のユーザ定義フィルタを含んでいるフィルタを保存することはできません。

フィルタの組み合わせについて

フィルタを単独または他のフィルタと組み合わせて選択すると、[Available Applications] リストが更新され、選択したフィルタの条件を満たすアプリケーションだけが表示されます。システム提供のフィルタは自由に組み合わせることができますが、カスタム フィルタを組み合わせることはできません。

システムは、OR 演算を使用して同じフィルタ タイプの複数のフィルタをリンクします。たとえば、Risks（リスク）タイプの下の Medium（中）および High（高）フィルタを選択すると、結果として次のようなフィルタになります。

```
Risk: Medium OR High
```

Medium フィルタに 110 個のアプリケーション、High フィルタに 82 個のアプリケーションが含まれる場合、システムはこれら 192 個のアプリケーションすべてを [Available Applications] リストに表示します。

システムは AND 演算を使用して、異なるタイプのフィルタをリンクします。たとえば Risks タイプで Medium および High フィルタを選択し、Business Relevance（業務との関連性）タイプで Medium および High フィルタを選択した場合、結果として次のようなフィルタになります。

```
Risk: Medium OR High
AND
Business Relevance: Medium OR High
```

この場合、Risk タイプの Medium または High と、Business Relevance タイプの Medium または High の両方に含まれるアプリケーションだけが表示されます。

フィルタの検索および選択

フィルタを選択するには、フィルタ タイプの横にある矢印をクリックして展開し、各フィルタの横のチェック ボックスをオンまたはオフにしてアプリケーションを表示したり非表示にしたりします。また、システムによって提供されるフィルタ タイプ（[Risks]、[Business Relevance]、[Types]、[Categories]、または [Tags]）を右クリックして、[Check All] または [Uncheck All] を選択します。

フィルタを検索するには、[Available Filters] リストの上にある [Search by name] プロンプトをクリックし、フィルタ名を入力します。入力を開始するとリストが更新され、一致するフィルタが表示されます。

フィルタの選択が完了したら、[Available Applications] リストを使用してこれらのフィルタをルールに追加します。個々のアプリケーションとトラフィックの照合（16-5 ページ）を参照してください。

個々のアプリケーションとトラフィックの照合

ライセンス： Control

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

アクセス コントロール ルールでアプリケーション条件を作成するときは、[Available Applications] リストを使用して、トラフィックを照合するアプリケーションを作成します。

アプリケーションのリストの参照

作成済みの条件がない場合、検出されたすべてのアプリケーションが 100 個ずつリストに表示されます。

- アプリケーションの次のページを閲覧するには、リストの下の矢印をクリックします。
- アプリケーションの横にある情報アイコン（  ）をクリックするとポップアップ ウィンドウが開き、アプリケーションの特性に関する概要とインターネット検索用のリンクが表示されます。

一致するアプリケーションの検索

目的のアプリケーションを検索しやすくするため、[Available Applications] リストに表示されるアプリケーションを制限することができます。

- アプリケーションを検索するには、リストの上にある [Search by name] プロンプトをクリックし、アプリケーション名を入力します。入力を開始するとリストが更新され、一致するアプリケーションが表示されます。
- フィルタを適用して表示を制限するには、[Application Filters] リストを使用します（トラフィックとアプリケーション フィルタの一致（16-4 ページ）を参照してください）。フィルタを適用すると [Available Applications] リストが更新されます。便宜上、システムはロック解除

アイコン()を使用して、復号化されたトラフィック(暗号化されているトラフィックまたは暗号化されていないトラフィックではなく)でのみ識別できるアプリケーションをマークします。

制限を適用すると、[Available Applications] リストの上に [All apps matching the filter] オプションが表示されます。このオプションを使用すると、制限したリストに表示されているすべてのアプリケーションをまとめて [Selected Applications and Filters] リストに追加できます。

注　[Application Filters] リストでいくつかのフィルタを選択し、さらに [Available Applications] リストでアプリケーションを検索した場合、選択フィルタと検索条件が AND 演算で結合され、両方の条件に一致するアプリケーションが [Available Applications] リストに表示されます。つまり、[All apps matching the filter] 条件には、[Available Applications] リストに表示されている個々のすべての条件と、[Available Applications] リストの上で入力された検索条件が含まれます。

条件に一致する単一アプリケーションの選択

目的のアプリケーションが見つかったら、それをクリックして選択します。複数のアプリケーションを選択するには、Shift キーまたは Ctrl キーを使用します。表示されているすべてのアプリケーションを選択するには、右クリックして [Select All] を選択します。

単一のアプリケーション条件では、それらを個別に選択することで、最大 50 のアプリケーションを照合できます。50 を超えるアプリケーションを追加するには、複数のアクセス コントロール ルールを作成するか、またはフィルタを使用してアプリケーションをグループ化します。

条件のフィルタに一致するすべてのアプリケーションの選択

検索または [Application Filters] リストのフィルタによる制限を適用すると、[Available Applications] リストの上に [All apps matching the filter] オプションが表示されます。

このオプションを使用すると、制限した [Available Applications] リストに表示されているすべてのアプリケーションをまとめて [Selected Applications and Filters] リストに追加できます。アプリケーションを個別に追加するのとは対照的に、このアプリケーションのセットを追加すると、そのセットを構成する個々のアプリケーションの数にかかわらず、最大 50 のアプリケーションに対してただ 1 つのアイテムとしてカウントされます。

この方法でアプリケーション条件を作成すると、[Selected Applications and Filters] リストに追加したフィルタに「フィルタ タイプ + 各タイプの最大 3 フィルタの名前」形式の名前が付きます。同じタイプのフィルタが 3 個を超える場合は、その後に省略記号(...)が表示されます。たとえば次のフィルタ名には、Risks タイプの 2 つのフィルタと Business Relevance タイプの 4 つのフィルタが含まれています。

```
Risks: Medium, High Business Relevance: Low, Medium, High,...
```

[All apps matching the filter] で追加したフィルタに特定のタイプが設定されていない場合、そのタイプ名は追加したフィルタ名に使用されません。[Selected Applications and Filters] リスト内のフィルタ名の上にポインタを置くと、これらのフィルタのタイプとして [any] が表示されます。つまり、これらのフィルタ タイプはリストの表示を制限しないため、任意の値が許容されます。

1 つのアプリケーション条件には [All apps matching the filter] のインスタンスを複数追加でき、これらの各インスタンスは [Selected Applications and Filters] リストで個別の項目としてカウントされます。たとえば、リスクが高いアプリケーションのすべてを 1 つの項目として追加し、この選択をクリアしてから、ビジネスとの関連性の低いアプリケーションのすべてをもう 1 つの項目として追加することが可能です。このアプリケーション条件に一致するのは、リスクが高いアプリケーション、またはビジネスとの関連性の低いアプリケーションになります。

アクセス コントロール ルールへのアプリケーション条件の追加

ライセンス：Control

サポートされるデバイス：すべて（シリーズ 2 または X-Series を除く）

トラフィックがアプリケーション条件を持つアクセス コントロール ルールに一致するには、トラフィックが [Selected Applications and Filters] リストに追加したフィルタまたはアプリケーションの 1 つに一致している必要があります。

1 つの条件に最大 50 の項目を追加することができ、条件に追加したフィルタが個別に追加したアプリケーションの上に一覧表示されます。無効なアプリケーション条件が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。また、アクセス コントロール ポリシーおよびルールのトラブルシューティング（12-25 ページ）を参照してください。

アプリケーション トラフィックを制御するには、次の手順を実行します。

アクセス：Admin/Access Admin/Network Admin

ステップ 1　アプリケーション別にトラフィックを制御するデバイスを対象とするアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか、または既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集（14-3 ページ）を参照してください。

ステップ 2　ルール エディタで、[Applications] タブを選択します。

[Applications] タブが表示されます。

ステップ 3　必要に応じて、フィルタを使用して [Available Applications] リストに表示されるアプリケーション リストを限定します。

[Application Filters] リストで、1 つまたは複数のフィルタを選択します。詳細については、トラフィックとアプリケーション フィルタの一致（16-4 ページ）を参照してください。

ステップ 4　[Available Applications] で、追加するアプリケーションを選択します。

個々のアプリケーションを検索して選択したり、リストの表示を制限した場合は [All apps matching the filter] をクリックしてすべてを選択したりできます。ロック解除アイコン（  ）は、システムが復号化されたトラフィック（暗号化されているトラフィックまたは暗号化されていないトラフィックではなく）でのみ識別できるアプリケーションを示します。詳細については、個々のアプリケーションとトラフィックの照合（16-5 ページ）を参照してください。

ステップ 5　[Add to Rule] をクリックして、選択したアプリケーションを [Selected Applications and Filters] リストに追加します。

選択したアプリケーションやフィルタをドラッグ アンド ドロップでリストに追加することもできます。フィルタは [Filters] という見出しの下に表示され、アプリケーションは [Applications] という見出しの下に表示されます。

ヒント　このアプリケーション条件に別のフィルタを追加する場合は、[Clear All Filters] をクリックして既存の選択をクリアしておきます。

ステップ 6　必要に応じて、[Selected Applications and Filters] リストの上にある追加アイコン（  ）をクリックすると、リストに現在含まれている個々のすべてのアプリケーションおよびフィルタからなるカスタム フィルタを保存できます。

このオンザフライで作成されたフィルタを管理するには、オブジェクト マネージャを使用します。アプリケーション フィルタの操作（3-16 ページ）を参照してください。別のユーザが作成したフィルタを含むフィルタは保存できないことに注意してください。ユーザが作成したフィルタはネストできません。

ステップ 7　ルールを保存するか、編集を続けます。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

アプリケーション制御の制約事項

ライセンス： Control

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

アプリケーション制御を実行する場合は、次の点に注意してください。

アプリケーション識別の速さ

システムは、以下の動作の前にアプリケーション制御を実行することはできません。

- モニタ対象の接続がクライアントとサーバの間で確立される前
- システムがセッションでアプリケーションを識別する前

この識別は 3 ～ 5 パケット以内で、またはトラフィックが暗号化されている場合は、SSL ハンドシェイクのサーバ証明書交換の後に発生する必要があります。これらの最初のパケットの 1 つがアプリケーション条件を含むアクセス コントロール ルール内の他のすべての条件に一致するが、識別が完了していない場合、アクセス コントロール ポリシーはパケットの通過を許可します。この動作により接続が確立され、アプリケーションの識別が可能になります。この問題の影響を受けるルールには、情報アイコン（  ）が表示されます。

許可されたパケットは、アクセス コントロール ポリシーの*デフォルト*の侵入ポリシー（*デフォルト アクション*侵入ポリシーでもほぼ一致するルールの侵入ポリシーでもない）により検査されます。詳細については、アクセス コントロールのデフォルト侵入ポリシーの設定（25-1 ページ）を参照してください。

システムは識別を終えると、アクセス コントロール ルール アクションおよび関連付けられている侵入ポリシーおよびファイル ポリシーをそのアプリケーション条件に一致する残りのセッション トラフィックに適用します。

暗号化されたトラフィックの処理

システムは、SMTPS、POP、FTPS、TelnetS および IMAPS など StartTLS を使用して、暗号化される前のアプリケーション トラフィックを識別し、フィルタリングできます。また、サーバ証明書サブジェクトの識別名の値または TLS クライアントの hello メッセージの Server Name Indication に基づいて、特定の暗号化アプリケーションを識別します。

これらのアプリケーションは、[SSL Protocol] とタグ付けされています。このタグがないアプリケーションは、暗号化されていないまたは復号化されたトラフィックでのみ検出できます。SSL インスペクション機能を使用して、システムがアクセス コントロール ルールと照合する前に暗号化されたトラフィックを復号化またはブロックする方法については、トラフィック復号化の概要（19-1 ページ）を参照してください。

ペイロードのないアプリケーション トラフィック パケットの処理

システムは、アプリケーションが識別される接続内にペイロードがないパケットに対してデフォルト ポリシー アクションを適用します。

参照されるトラフィックの処理

Web サーバによって参照されるトラフィック（たとえばアドバタイズメント トラフィック）を処理するルールを作成するには、参照元アプリケーションではなく、参照されるアプリケーションに関する条件を追加します。詳細については、特記事項：照会先 Web アプリケーション（45-16 ページ）を参照してください。

アプリケーション ディテクタの自動有効化

ポリシー内のアプリケーション ルール条件ごとに、少なくとも 1 つのディテクタを有効にする必要があります（ディテクタのアクティブ化と非アクティブ化（46-30 ページ）を参照）。有効になっているディテクタがないアプリケーションについては、システム提供のすべてのディテクタが自動的に有効になります。ディテクタが存在しない場合は、そのアプリケーションについて最後に変更されたユーザ定義ディテクタが有効になります。

複数のプロトコルを使用するアプリケーション トラフィックの制御（Skype）

システムは、Skype の複数のタイプの アプリケーション トラフィックを検出できます。Skype のトラフィックを制御するためのアプリケーション条件を作成する場合は、個々のアプリケーションを選択するのではなく、[Application Filters] リストから [Skype] タグを選択します。これにより、システムは同じ方法で Skype のすべてのトラフィックを検出して制御できるようになります。詳細については、トラフィックとアプリケーション フィルタの一致（16-4 ページ）を参照してください。

URL のブロッキング

ライセンス： 機能によって異なる

サポートされるデバイス： すべて（シリーズ 2 を除く）

サポートされる防御センター： 機能によって異なる

アクセス コントロール ルールの URL 条件を使用することで、ネットワーク上のユーザがアクセスできる Web サイトを制限することができます。この機能は、*URL フィルタリング*と呼ばれます。アクセス コントロールを使用してブロックする（または逆に許可する）URL を指定するには 2 つの方法があります。

- 各ライセンスを使用して、個々の URL または URL のグループを手動で指定することで、Web トラフィックへのきめ細かなカスタム コントロールを実現できます。
- URL Filtering ライセンスを使用して、URL の一般的な分類、または*カテゴリ*、およびリスク レベル、または*レピュテーション*に基づいて、Web サイトへのアクセスを制御することもできます。システムは接続ログ、侵入イベント、およびアプリケーションの詳細にこのカテゴリとレピュテーション データを表示します。

注　イベントで URL カテゴリおよびレピュテーション情報を表示するには、URL 条件を使用して少なくとも 1 つのアクセス コントロール ルールを作成する必要があります。

Web サイトをブロックするときは、ユーザのブラウザにデフォルト動作を許可するか、またはシステムによって提供される一般的なページまたはカスタム ページを表示できます。また、警告ページをクリック スルーすることで Web サイトのブロックをバイパスする機会をユーザに与えることができます。

暗号化された Web トラフィックの処理

暗号化されたトラフィックを復号化するように SSL インスペクション（トラフィック復号化の概要（19-1 ページ）を参照）を設定した場合、アクセス コントロール ルールは復号化されたトラフィックを暗号化されていないかのように評価します。しかし、SSL インスペクションの設定によって、暗号化された接続が復号化されていないトラフィックの通過を許可する場合、または SSL インスペクションを設定していない場合は、アクセス コントロール ルールは暗号化されたトラフィックを評価します。

URL 条件を持つアクセス コントロール ルールを使用して Web トラフィックを評価する場合、システムはトラフィックを暗号化するために使用された公開キー証明書のサブジェクト共通名に基づいて HTTPS トラフィックを照合します。また、システムはサブジェクト共通名内のサブドメインを無視するので、HTTPS URL を手動でフィルタリングする際は、サブドメイン情報を含めないでください。たとえば、`www.example.com` ではなく `example.com` を使用します。

また、システムは暗号化プロトコル（HTTP または HTTPS）を無視します。これは、手動およびレピュテーション ベース両方の URL 条件で発生します。つまり、アクセス コントロール ルールは、次の Web サイトへのトラフィックを同じように扱います。

- http://example.com/
- https://example.com/

HTTP または HTTPS トラフィックのみに一致するアクセス コントロール ルールを設定するには、アプリケーション条件をルールに追加します。たとえば、あるサイトへの HTTPS アクセスを許可する一方で、HTTP アクセスを許可しないようにできます。そのためには、2 つのアクセス コントロール ルールを作成し、それぞれにアプリケーションと URL の条件を割り当てます。

最初のルールは Web サイトへの HTTPS トラフィックを許可します。

```
Action: Allow
Application: HTTPS
URL: example.com
```

2 番目のルールは同じ Web サイトへの HTTP アクセスをブロックします。

```
Action: Block
Application: HTTP
URL: example.com
```

注　デフォルトでは、システムはセッションを暗号化する試みを検出すると、暗号化されたペイロードの侵入およびファイルのインスペクションを即座に無効にします。これにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。詳細については、SSL プリプロセッサの使用（27-75 ページ）を参照してください。

いずれかのライセンスを持つ シリーズ 2 以外のアプライアンスを使用して URL を手動でブロックできますが、カテゴリおよびレピュテーション ベースの URL フィルタリングには URL Filtering ライセンスが必要で、DC500 ではサポートされていません。

表 16-2　URL フィルタリングのライセンスおよびモデルの要件

要件	カテゴリおよびレピュテーション ベース	手動
license	URL Filtering	いずれか
devices	すべて（シリーズ 2 を除く）	すべて（シリーズ 2 を除く）
Defense Center	すべて（DC500 を除く）	いずれか

詳細については、以下を参照してください。

- レピュテーション ベースの URL ブロックの実行（16-11 ページ）
- 手動による URL ブロッキングの実行（16-14 ページ）
- URL の検出とブロッキングの制約事項（16-16 ページ）
- ユーザが URL ブロックをバイパスすることを許可する（16-18 ページ）
- ブロックされた URL のカスタム Web ページの表示（16-20 ページ）

レピュテーション ベースの URL ブロックの実行

ライセンス： URL Filtering

サポートされるデバイス： すべて（シリーズ 2 を除く）

サポートされる防御センター： すべて（DC500 を除く）

URL Filtering ライセンスを使用して、FireSIGHT システム が Cisco クラウドから取得する要求された URL のカテゴリおよびレピュテーションに基づいて、Web サイトへのユーザのアクセスを制御できます。

- URL *カテゴリ*とは、URL の一般的な分類です。たとえば ebay.com は [Auctions] カテゴリ、monster.com は [Job Search] カテゴリに属します。1 つの URL は複数のカテゴリに属することができます。
- URL *レピュテーション*は、組織のセキュリティ ポリシーに反する目的でその URL が使用される可能性を表します。各 URL のリスク範囲は、**ハイ リスク**（レベル 1）から**有名**（レベル 5）です。

注　カテゴリおよびレピュテーション ベースの URL 条件を持つアクセス コントロール ルールを有効にする前に、Cisco クラウドとの通信を有効にする**必要があります**。これにより、Defense Center による URL データの取得が可能になります。詳細については、クラウド通信の有効化（64-30 ページ）を参照してください。

レピュテーション ベースの URL ブロッキングの利点

URL のカテゴリおよびレピュテーションにより、アクセス コントロール ルールの URL 条件をすぐに作成することができます。たとえば、[Abused Drugs] カテゴリ内の**ハイ リスク** URL をすべて識別してブロックするアクセス コントロール ルールを作成できます。ユーザがそのカテゴリとレピュテーションの組み合わせで URL を閲覧しようとすると、セッションがブロックされます。

Cisco クラウドからカテゴリ データおよびレピュテーション データを使用することで、ポリシーの作成と管理も簡素化されます。この方法では、システムが Web トラフィックを期待通りに確実に制御します。さらに、このクラウド上のデータは常に更新されて新しい URL が追加され、既存の URL も新しいカテゴリとリスクで更新されるため、常に最新の情報に基づいて URL がフィルタ処理されるようになります。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表す悪意のあるサイトは、組織でポリシーを更新したり新規ポリシーを適用したりするペースを上回って次々と現れては消える可能性があります。

次に例をいくつか示します。

- ルールですべてのゲーム サイトをブロックする場合、新しいドメインが登録されて**ゲーム**に分類されると、これらのサイトをシステムで自動的にブロックできます。
- ルールがすべてのマルウェア サイトをブロックし、あるブログ ページがマルウェアに感染すると、クラウドはその URL を [Blog] から [Malware] に再分類でき、システムはそのサイトをブロックできます。
- ルールがリスクの高いソーシャル ネットワーキング サイトをブロックし、だれかがプロファイル ページに悪意のあるペイロードへのリンクが含まれるリンクを掲載すると、クラウドはそのページのレピュテーションを [Benign sites] から [High Risk] に変更でき、システムでそれをブロックできます。

なお、URL のカテゴリやレピュテーションがクラウドで不明な場合、または Defense Center がクラウドと通信できない場合には、カテゴリやレピュテーションに基づく URL 条件を含むアクセス コントロール ルールが URL によってトリガー**されない**ことに注意してください。URL に手動でカテゴリやレピュテーションを割り当てることはできません。

URL 条件の作成

次の図は、すべてのマルウェア サイト、すべてのハイ リスク サイト、およびすべての有害なソーシャル ネットワーキング サイトをブロックするアクセス コントロール ルールの URL 条件を示しています。また、単一サイト example.com（URL オブジェクトによって表されます）もブロックされます。

1 つの URL 条件で、照合する最大 50 の項目を [Selected URLs] に追加できます。各 URL カテゴリは、レピュテーションを追加した場合も含め、1 つの項目としてカウントされます。URL 条件でリテラル URL および URL オブジェクトを使用することもできますが、これらの項目はレピュテーションで制限できないことに注意してください。詳細については、手動による URL ブロッキングの実行（16-14 ページ）を参照してください。

次の表では、上記の条件をどのように設定するかを示しています。URL オブジェクトおよびリテラル URL にレピュテーションを追加できないことに注意してください。

表 16-3　例:URL 条件の作成

ブロック対象	選択するカテゴリまたは URL オブジェクト	レピュテーション
マルウェア サイト、レピュテーションは無関係	Malware Sites	いずれか
ハイ リスク(レベル 1)のすべての URL	いずれか	1 - ハイ リスク
リスクが無害(benign)より大きいソーシャル ネットワーキング サイト(レベル 1 ～ 3)	Social Network	3 - セキュリティ リスクのある無害(benign)サイト
example.com	example.com という名前の URL オブジェクト	none

無効な URL 条件が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。また、アクセス コントロール ポリシーおよびルールのトラブルシューティング(12-25 ページ)を参照してください。

注意　最初にカテゴリまたはレピュテーション URL 条件をアクセス コントロール ルールに追加すると、Snort プロセスが再開され、構成変更を適用する際、一時的にトラフィック検査が中断されます。この検査中にシステムがトラフィックをドロップするか、検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、「Snort の再開によるトラフィックへの影響(1-9 ページ)」を参照してください。

カテゴリとレピュテーション データを使用して要求された URL でトラフィックを制御するには、次の手順を実行します。

アクセス: Admin/Access Admin/Network Admin

ステップ 1　URL 別にトラフィックを制御するデバイスを対象とするアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか、または既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集(14-3 ページ)を参照してください。

ステップ 2　ルール エディタで、[URLs] タブを選択します。

[URLs] タブが表示されます。

ステップ 3　[Categories and URLs] リストから追加する URL のカテゴリを見つけて選択します。カテゴリに関係なく Web トラフィックを照合するには、[Any] カテゴリを選択します。

追加するカテゴリを検索するには、[Categories and URLs] リストの上にある [Search by name or value] プロンプトをクリックし、カテゴリ名を入力します。入力を開始するとリストが更新され、一致するカテゴリが表示されます。

カテゴリをクリックして選択します。複数のカテゴリを選択するには、Shift キーまたは Ctrl キーを使用します。

ヒント　右クリックして**すべてのカテゴリを選択**できますが、このようにすべてのカテゴリを追加すると、1 つのアクセス コントロール ルールに対する項目の最大値 50 を超えます。代わりに [Any] を使用してください。

ステップ 4　オプションで、[Reputations] リストのレピュテーション レベルをクリックして、選択したカテゴリに追加します。レピュテーション レベルを指定しない場合、デフォルトですべてのレベルを意味する [Any] が適用されます。

選択できるレピュテーション レベルは 1 つのみです。レピュテーション レベルを選択すると、アクセス コントロール ルールはその目的に応じて異なる動作をします。

- ルールによって Web アクセスをブロックまたはモニタする場合（ルール アクションが [Block]、[Block with reset]、[Interactive Block]、[Interactive Block with reset]、または [Monitor]）、レピュテーション レベルを選択すると、そのレベルよりも厳しいレピュテーションもすべて選択されます。たとえば**疑わしいサイト**（レベル 2）をブロックまたはモニタするようルールを設定した場合、**ハイ リスク**（レベル 1）のサイトも自動的にブロックまたはモニタされます。
- ルールによって Web アクセスがそれを信頼またはさらに検査するかどうかを許可する場合（ルール アクションが [Allow] または [Trust]）、レピュテーション レベルを選択すると、そのレベルよりも厳しさが弱いレピュテーションもすべて選択されます。たとえば**無害なサイト**（レベル 4）を許可するようルールを設定した場合、**有名**（レベル 5）サイトもまた自動的に許可されます。

ルールのアクションを変更した場合、システムは、上記の点に従って URL 条件のレピュテーション レベルを自動的に変更します。

ステップ 5　[Add to Rule] をクリックするか、または選択した項目をドラッグ アンド ドロップして、[Selected URLs] リストに追加します。

ステップ 6　ルールを保存するか、編集を続けます。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

手動による URL ブロッキングの実行

ライセンス： すべて

サポートされるデバイス： すべて（シリーズ 2 を除く）

カテゴリおよびレピュテーションで URL フィルタリングを補完するか、または選択的に上書きするには、手動で個々の URL または URL のグループを指定することで、Web トラフィックを制御できます。これにより、許可またはブロックされた Web トラフィックに対するきめ細かなカスタム制御を行うことができます。特殊なライセンスなしでこのタイプの URL フィルタリングを実行することもできます。

アクセス コントロール ルールに許可またはブロックする URL を手動で指定するには、単一のリテラル URL を入力できます。または、再利用可能で名前を URL または IP アドレスに関連付ける URL オブジェクトを使用して URL 条件を設定できます。

ヒント　URL オブジェクトを作成した後、それを使用してアクセス コントロール ルールを作成するだけでなく、他のさまざまな場所の URL をシステムの Web インターフェイスに表すことができます。これらのオブジェクトはオブジェクト マネージャを使用して作成できます。また、アクセス コントロール ルールの設定時に URL オブジェクトをオンザフライで作成することもできます。詳細については、URL オブジェクトの操作（3-15 ページ）を参照してください。

URL 条件で URL を手動で指定する

手動で入力することで、許可またはブロックされる Web トラフィックに対する正確な制御が実現できますが、手動で指定した URL をレピュテーションで制限することはできません。また、ルールに予期しない結果がないことを確認する必要があります。ネットワーク トラフィックが URL 条件に一致するかどうか判別するために、システムは単純な部分文字列マッチングを実行します。URL オブジェクトまたは手動で入力した URL の値が、モニタ対象ホストから要求された URL の一部に一致する場合、アクセス コントロール ルールの URL 条件が満たされます。

したがって、URL 条件（URL オブジェクトを含む）に URL を手動で指定する場合は、影響を受ける可能性がある他のトラフィックを慎重に考慮する必要があります。たとえば example.com へのすべてのトラフィックを許可する場合、ユーザは次の URL を含むサイトを参照できます。

- http://example.com/
- http://example.com/newexample
- http://www.example.com/

別の例として、ign.com（ゲーム サイト）を明示的にブロックする場合を考えてください。部分文字列マッチングにより *ign.com* 自体だけでなく veris*ign.com* もブロックされることになり、意図しない動作が生じる可能性があります。

暗号化された Web トラフィックの手動ブロッキング

SSL インスペクションの設定によって通過が許可されている場合、または SSL インスペクションが設定されていない場合は、アクセス コントロール ルールは暗号化されたトラフィックを処理することに注意してください。トラフィック復号化の概要（19-1 ページ）を参照してください。アクセス コントロール ルールの URL 条件は以下を行います。

- Web トラフィック（HTTP または HTTPS）の暗号化プロトコルを無視します。

  たとえば、アクセス コントロール ルールは、http://example.com/ へのトラフィックを https://example.com/ へのトラフィックと同じものとして処理します。HTTP または HTTPS トラフィックのみに一致するアクセス コントロール ルールを設定するには、アプリケーション条件をルールに追加します。詳細については、URL のブロッキング（16-9 ページ）を参照してください。

- トラフィックを暗号化するために使用する公開キー証明書のサブジェクト共通名に基づいて HTTPS トラフィックを照合し、また、サブジェクト共通名に含まれるサブドメインを無視します。

  手動で HTTPS トラフィックをフィルタリングする場合は、サブドメイン情報を含めないでください。

無効な URL 条件が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。また、アクセス コントロール ポリシーおよびルールのトラブルシューティング（12-25 ページ）を参照してください。

許可またはブロックする URL を手動で指定して Web トラフィックを制御するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　URL 別にトラフィックを制御するデバイスを対象とするアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか、または既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集（14-3 ページ）を参照してください。

ステップ 2　ルール エディタで、[URLs] タブを選択します。

[URLs] タブが表示されます。

ステップ 3　[Categories and URLs] リストから追加する URL オブジェクトおよびグループを見つけて選択します。

- URL オブジェクトをオンザフライで追加するには（後で条件に追加できます）、[Categories and URLs] リストの上にある追加アイコン（  ）をクリックします。URL オブジェクトの操作（3-15 ページ）を参照してください。
- 追加する URL オブジェクトおよびグループを検索するには、[Categories and URLs] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクトの名前またはオブジェクト内の URL または IP アドレスの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

オブジェクトをクリックして選択します。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用します。右クリックして**すべての URL オブジェクトおよびカテゴリを選択**できますが、このように URL を追加すると、1 つのアクセス コントロール ルールに対する項目の最大値 50 を超えます。

ステップ 4　[Add to Rule] をクリックするか、または選択した項目を [Selected URLs] リストに追加します。

選択した項目をドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5　手動で指定するリテラル URL を追加します。このフィールドでは、ワイルドカード（*）は使用**できません**。

[Selected URLs] リストの下にある [Enter URL] プロンプトをクリックし、URL または IP アドレスを入力して、[Add] をクリックします。

ステップ 6　ルールを保存するか、編集を続けます。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

URL の検出とブロッキングの制約事項

ライセンス： すべて

サポートされるデバイス： すべて（シリーズ 2 を除く）

URL の検出とブロックを行う場合は、次の点に注意してください。

URL 識別の速さ

システムは以下の動作の前に URL をフィルタリングできません。

- モニタしている接続がクライアントとサーバ間で確立される。

- システムがセッションで HTTP または HTTPS アプリケーションを識別する前
- システムが要求された URL を識別する前（クライアントの hello メッセージまたはサーバ証明書から暗号化されたセッションの場合）

この識別は 3 ～ 5 パケット以内で、またはトラフィックが暗号化されている場合は、SSL ハンドシェイクのサーバ証明書交換の後に発生する必要があります。これらの最初のパケットの 1 つが URL 条件を含むアクセス コントロール ルール内の他のすべての条件に一致するが、識別が完了していない場合、アクセス コントロール ポリシーはパケットの通過を許可します。このため、URL を識別できるように接続が確立されます。この問題の影響を受けるルールには、情報アイコン（  ）が表示されます。

許可されたパケットは、アクセス コントロール ポリシーの *デフォルトの侵入ポリシー*（*デフォルト アクション*侵入ポリシーでもほぼ一致するルールの侵入ポリシーでもない）により検査されます。詳細については、アクセス コントロールのデフォルト侵入ポリシーの設定（25-1 ページ）を参照してください。

システムは識別を終えると、アクセス コントロール ルール アクションおよび関連付けられている侵入ポリシーおよびファイル ポリシーをその URL 条件に一致する残りのセッション トラフィックに適用します。

暗号化された Web トラフィックの処理

URL 条件を持つアクセス コントロール ルールを使用して暗号化された Web トラフィックを評価する際、システムは以下を行います。

- 暗号化プロトコルを無視します。ルールに URL 条件はあるがプロトコルを指定するアプリケーション条件はない場合、アクセス コントロール ルールは HTTPS および HTTP 両方のトラフィックを照合します。
- トラフィックを暗号化するために使用する公開キー証明書のサブジェクト共通名に基づいて HTTPS トラフィックを照合し、サブジェクト共通名に含まれるサブドメインを無視します。
- HTTP 応答ページを表示しません（設定したとしても）。

HTTP 応答ページ

HTTP 応答ページは、Web トラフィックが以下の条件でブロックされた場合は表示されません。

- 加えて、セッションが暗号化されている、または暗号化されていた場合
- 昇格したアクセス コントロール ルールの結果として、シリーズ 3 デバイスによる場合
- 前述の通り、接続が確立され、少量のパケットの通過が許可されるまで、システムが接続内の要求された URL を識別しない場合

詳細については、ブロックされた URL のカスタム Web ページの表示（16-20 ページ）を参照してください。

URL での検索クエリ パラメータ

URL 条件の照合では、URL 内の検索クエリ パラメータが使用されません。たとえば、すべてのショッピング トラフィックをブロックする場合を考えます。amazon.com を探すために Web 検索を使用してもブロックされませんが、amazon.com を閲覧しようとするとブロックされます。

ユーザが URL ブロックをバイパスすることを許可する

ライセンス： すべて

サポートされるデバイス： すべて（シリーズ 2 を除く）

アクセス コントロール ルールを使用してユーザの HTTP Web 要求をブロックする場合は、ルール アクションを [Interactive Block] または [Interactive Block with reset] に設定することで、ユーザは警告 *HTTP 応答*ページをクリック スルーすることによりブロックをバイパスできます。システムによって提供される汎用応答ページを表示するか、またはカスタム HTML を入力できます。

デフォルトでは、システムによってユーザは後続のアクセスで警告ページを表示することなく、10 分（600 秒）間ブロックをバイパスすることができます。期間を 1 年に設定したり、ユーザに毎回ブロックをバイパスするように強制できます。

ユーザがブロックをバイパスしない場合、一致したトラフィックは追加のインスペクションなしで拒否されます。また、接続をリセットすることもできます。一方、ユーザがブロックをバイパスすると、システムによってトラフィックが許可されます。このトラフィックを許可するということは、侵入、マルウェア、禁止されたファイル、および検出データの有無について暗号化されていないペイロードを引き続き検査できることを意味します。ブロックをバイパスした後、ロードされなかったページの要素をロードするために、ページを更新しなければならない場合があることに注意してください。

インタラクティブ HTTP 応答ページは、ブロック ルールに設定する応答ページとは別に設定することに注意してください。たとえば、インタラクションなしでセッションがブロックされたユーザにはシステムによって提供されるページを表示できますが、クリックして続行できるユーザに対しては、カスタム ページを表示できます。詳細については、ブロックされた URL のカスタム Web ページの表示（16-20 ページ）を参照してください。

次の状況では、セッションがインタラクティブ ブロック ルールに一致する場合であっても、応答ページは表示**されず**、トラフィックはインタラクションなしでブロックされることに注意してください。

- セッションが暗号化されていた、または暗号化されている場合。これには、システムによって復号化されたセッションも含まれます。
- 接続が確立され、少量のパケットの通過が許可された後。システムは、要求された URL とアプリケーションの詳細についてその接続を検査できます。アクセス コントロール ポリシーおよびルールのトラブルシューティング（12-25 ページ）を参照してください。

ヒント アクセス コントロール ポリシーのすべてのルールに対してインタラクティブ ブロッキングを素早く無効にするには、システムによって提供されるページもカスタム ページも表示しないでください。これにより、システムはインタラクションなしでインタラクティブ ブロック ルールに一致するすべての接続をブロックします。

ユーザに Web サイト ブロックをバイパスするように許可するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　URL 条件を持つ Web トラフィックに一致するアクセス コントロール ルールを作成します。

レピュテーション ベースの URL ブロックの実行（16-11 ページ）および手動による URL ブロッキングの実行（16-14 ページ）を参照してください。

ステップ 2　アクセス コントロール ルール アクションが [Interactive Block] または [Interactive Block with reset] であることを確認します。

ルール アクションを使用したトラフィックの処理とインスペクションの決定（14-8 ページ）を参照してください。

ステップ 3　ユーザがブロックをバイパスし、ルールに対してインスペクションおよびロギング オプションを必要に応じて選択すると仮定します。許可ルールと同様に次のようになります。

- いずれかのタイプのインタラクティブ ブロック ルールをファイルおよび侵入ポリシーに関連付けることができます。また、システムはディスカバリを使用して、ユーザ許可されたこのトラフィックを検査できます。詳細については、侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（18-1 ページ）を参照してください。
- インタラクティブ ブロックされるトラフィックに関するロギング オプションは、許可されたトラフィックに関するオプションと同じですが、ユーザがインタラクティブ ブロックをバイパスしない場合、システムがログに記録できるのは接続開始イベントだけであることに注意してください。

  システムが最初にユーザに警告すると、ロギングされた接続開始イベントを Interactive Block または Interactive Block with reset アクションでマークすることに留意してください。ユーザがブロックをバイパスすると、セッションが記録される追加の接続イベントに Allow アクションが付きます。詳細については、アクセス コントロールの処理に基づく接続のロギング（38-17 ページ）を参照してください。

ステップ 4　オプションで、システムが警告ページを再表示する前にユーザがブロックをバイパスしてから経過する時間を設定します。

ブロックされた Web サイトのユーザ バイパス タイムアウトの設定（16-19 ページ）を参照してください。

ステップ 5　オプションで、ユーザにブロックをバイパスすることを許可するために表示するカスタム ページを作成し、使用します。

ブロックされた URL のカスタム Web ページの表示（16-20 ページ）を参照してください。

ブロックされた Web サイトのユーザ バイパス タイムアウトの設定

ライセンス： すべて

デフォルトでは、システムによってユーザは後続のアクセスで警告ページを表示することなく、10 分（600 秒）間インタラクティブ ブロックをバイパスすることができます。期間を 1 年に設定したり、ゼロに設定してユーザに毎回ブロックをバイパスするように強制できます。この制限は、ポリシー内のすべてのインタラクティブ ブロック ルールに適用されます。ルールごとに制限を設定することはできません。

ユーザ バイパスの期限が切れるまでの時間の長さをカスタマイズするには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　設定するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3　[Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ 4　[General Settings] の横にある編集アイコン（ ）をクリックします。

[General Settings] ポップアップ ウィンドウが表示されます。

ステップ 5　[Allow an Interactive Block to bypass blocking for (seconds)] フィールドに、ユーザ バイパスの期限が切れるまでの経過時間を秒数で入力します。

0 ～ 31536000（1 年）の間の任意の数を指定できます。ゼロを指定すると、ユーザはブロックを毎回強制的にバイパスします。

ステップ 6　[OK] をクリックします。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ 7　[Save] をクリックします。

変更を反映するには、アクセス コントロール ポリシーを適用する必要があります。詳細については、アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

ブロックされた URL のカスタム Web ページの表示

ライセンス： すべて

サポートされるデバイス： すべて（シリーズ 2 を除く）

システムによってユーザの HTTP Web 要求がブロックされたときに、ユーザのブラウザに表示される内容は、アクセス コントロール ルールのアクションを使用して、セッションをどのようにブロックするかによって異なります。次から選択できます。

- 接続を拒否するには、[Block] または [Block with reset]。ブロックされたセッションがタイムアウトになると、[Block with reset] の場合は、システムが接続をリセットします。ただし、いずれのブロック アクションの場合でも、デフォルトのブラウザまたはサーバのページを、接続が拒否されたことを説明するカスタム ページでオーバーライドすることができます。システムではこのカスタム ページを*HTTP 応答*ページと呼んでいます。
- ユーザに警告する*インタラクティブ HTTP 応答*ページを表示する一方、ユーザがボタンをクリックすることで、処理を続行あるいはページを更新して、要求された元のサイトをロードできるようにする場合は、[Interactive Block] または [Interactive Block with reset]。応答ページをバイパスした後、ロードされなかったページの要素をロードするために、ページを最新表示しなければならない場合があります。

システムによって提供される汎用応答ページを表示するか、またはカスタム HTML を入力できます。カスタム テキストを入力する際には、使用した文字数がカウンタで示されます。

各アクセス コントロール ポリシーで、インタラクティブ HTTP 応答ページは、インタラクションなしで、つまりブロック ルールを使用してトラフィックをブロックするために使用する応答ページとは別に設定します。たとえば、インタラクションなしでセッションがブロックされたユーザにはシステムによって提供されるページを表示できますが、クリックして続行できるユーザに対しては、カスタム ページを表示できます。

HTTP 応答ページをユーザに確実に表示できるかは、ネットワーク設定、トラフィック負荷、およびページのサイズによって異なります。カスタム応答ページを作成する場合は、より小さいページが正常に表示されやすいことに留意してください。

応答ページは、Web トラフィックが以下の条件でブロックされた場合は表示されないことに注意してください。

- セキュリティ インテリジェンスのブラックリストによる場合
- 加えて、セッションが元々暗号化されていた場合。これには、SSL インスペクション機能によってブロックされた暗号化された接続、およびブロックまたはインタラクティブ ブロックのアクセス コントロール ルールに一致する復号化または暗号化されたトラフィックが含まれます。
- 昇格したアクセス コントロール ルールの結果として、シリーズ 3 デバイスによる場合。シリーズ 3 デバイスを使用したトラフィックの信頼またはブロックへの制限事項（14-13 ページ）を参照してください。
- 接続が確立され、少量のパケットの通過が許可された後。システムは、要求された URL とアプリケーションの詳細についてその接続を検査できます。アクセス コントロール ポリシーおよびルールのトラブルシューティング（12-25 ページ）を参照してください。

HTTP 応答ページの設定方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　Web トラフィックをモニタするデバイスを対象とするアクセス コントロール ポリシーを編集します。

詳細については、アクセス コントロール ポリシーの編集（12-13 ページ）を参照してください。

ステップ 2　[HTTP Responses] タブを選択します。

アクセス コントロール ポリシーの HTTP 応答ページ設定が表示されます。

ステップ 3　[Block Response Page] および [Interactive Block Response Page] の場合、ドロップダウンリストから応答を選択します。各ページには、次の選択肢があります。

- 汎用の応答を使用する場合は、[System-provided] を選択します。表示アイコン（  ）をクリックすると、このページの HTML コードが表示されます。
- カスタム応答を作成する場合は、[Custom] を選択します。

  ポップアップ ウィンドウが表示されます。このウィンドウに事前入力されているシステムによって提供されるコードを置換または変更できます。完了したら、変更を保存します。カスタム ページは、編集アイコン（  ）をクリックすると編集できます。
- システムに HTTP 応答ページを表示させない場合は、[None] を選択します。インタラクティブにブロックされるセッションに対してこのオプションを選択すると、ユーザはクリックして続行することができなくなります。セッションはインタラクションなしでブロックされます。

ステップ 4　[Save] をクリックします。

変更を反映するには、アクセス コントロール ポリシーを適用する必要があります。詳細については、アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

ユーザに基づくトラフィックの制御

*アクセス コントロール ポリシー*の*アクセス コントロール ルール*を設定すると、ネットワーク トラフィックのロギングや処理を詳細に制御できます。アクセス コントロール ルールのユーザ条件を使用することで、*ユーザ制御*を実行し、ホストにログインする LDAP ユーザに基づいてトラフィックを制限することによって、ネットワークを通過できるトラフィックを管理できます。

ユーザ制御は、*アクセス制御されたユーザ*を IP アドレスに関連付けることで機能します。この機能では、ホストにログインまたはホストからログアウトするとき、または他の理由で Active Directory 認証を行うときに、特定のユーザをモニタするエージェントを展開します。たとえば、アプリケーションやサービスでの認証を Active Directory で一元管理している組織では、このトラフィック制御方法を検討できます。

トラフィックがユーザ条件を持つアクセス コントロール ルールに一致するには、モニタ対象のセッション内の送信元ホストまたは宛先ホストいずれかの IP アドレスがログインしているアクセス制御されたユーザに関連付けられている必要があります。この機能では、特定のユーザまたはユーザ グループに基づいてトラフィックを制御できます。

ユーザ条件を互いに組み合わせたり、他のタイプの条件と組み合わせて、アクセス コントロール ルールを作成することができます。これらのアクセス コントロール ルールは単純にも複雑にも設定でき、複数の条件を使用してトラフィックを照合および検査できます。アクセス コントロール ルールの詳細については、アクセス コントロール ルールを使用したトラフィック フローの調整（14-1 ページ）を参照してください。

注 ハードウェアベースの高速パス ルール、セキュリティ インテリジェンス ベースのトラフィック フィルタリング、および一部の復号化と前処理は、ネットワーク トラフィックがアクセス コントロール ルールによって評価される**前に**行われます。また、*SSL インスペクション*機能を設定すると、暗号化されたトラフィックをアクセス コントロール ルールが評価する前にブロックしたり復号化したりできます。

ユーザ制御には Control ライセンスが必要であり、ユーザ エージェントのモニタリング Microsoft Active Directory サーバによって報告されるログインおよびログアウトのレコードを使用している、LDAP ユーザおよびグループ（アクセス制御されたユーザ）に対してのみサポートされます。

しかし、FireSIGHT ライセンスのみを使用して、ユーザ制御の基盤である*ユーザ認識*を引き続き活用できます。ユーザ認識によって、管理対象デバイスが検出データについて許可されたネットワーク トラフィックを検査するときにシステムが検出できる、エージェントによって報告されたユーザ アクティビティ、および*アクセス制御されていないユーザ*の追加のアクティビティを表示できます。システムは、さまざまなプロトコル（AIM、IMAP、LDAP、Oracle、POP3、SIP、FTP、HTTP および MDNS）を介したログイン試行を識別できます。

システムによって報告されたユーザ アクティビティにコンテキストを追加するには、展開環境で LDAP サーバにクエリを行い、アクセス制御されたユーザだけでなく、一部のアクセス制御されていないユーザ（ユーザ検出によって検出された POP3 および IMAP ユーザ、およびアクティビティがユーザ検出またはユーザ エージェントによって検出される LDAP ユーザ）のメタデータを取得できます。

ユーザ認識によって、「何が」の背後にある「誰が」を決定するためのすべてのタイプの展開が可能になります。たとえば、以下について決定できます。

- ホスト重要度の高いサーバの不正アクセスを試みている人物
- 不合理な容量の帯域幅を使用している人物
- 重要なオペレーティング システム更新を適用しなかった人物
- 会社の IT ポリシーに違反してインスタント メッセージング ソフトウェアまたはピアツーピア ファイル共有アプリケーションを使用している人物
- 脆弱（レベル 1：赤）影響レベル（Protection が必要）の侵入イベントの対象になっているホストの所有者
- 内部攻撃またはポート スキャンを開始した人物（Protection が必要）

この情報を入手すれば、リスクを軽減したり、その他の人を混乱させない措置を講じたりするための的を絞ったアプローチを取ることができます。ユーザ制御によって、LDAP ユーザとユーザ アクティビティをブロックする機能が追加されます。また、ユーザ認識および制御の機能によって、監査制御が大幅に向上し、法規制の遵守が強化されます。詳細については、ユーザ データ収集について（45-3 ページ）を参照してください。

次の表に、ユーザ認識および制御に関する要件を示します。ユーザ エージェントの詳細および最新情報については、『*User Agent Configuration Guide*』を参照してください。

表 17-1　　ユーザ認識および制御の要件

要件	ユーザ認識	ユーザ制御
license	FireSIGHT	Control
devices	いずれか	すべて（シリーズ 2 または X-Series を除く）
Defense Center	いずれか	すべて（DC500 を除く）
ユーザ エージェント	モニタする Defense Center および Microsoft Active Directory サーバとの間の TCP/IP アクセスが行われる、次のいずれかを実行している Windows コンピュータに、バージョン 2.2 のユーザ エージェントをインストールします。 • Windows Vista、Windows 7、または Windows 8 • Windows Server 2003、2008、または 2012 また、Microsoft .NET Framework バージョン 4.0 クライアント プロファイルと Microsoft SQL Server Compact（SQL CE）バージョン 3.5 もインストールする必要があります。	

表 17-1　ユーザ認識および制御の要件（続き）

要件	ユーザ認識	ユーザ制御
ユーザのメタデータ取得のための LDAP サーバ	Defense Center からの TCP/IP アクセスがある、次のいずれか。 • Windows Server 2003 と Windows Server 2008 上の Microsoft Active Directory（ユーザ制御に必要） • Windows Server 2003 と Windows Server 2008 上の Oracle Directory Server Enterprise Edition 7.0（ユーザ認識のみ） • Linux 上の OpenLDAP（ユーザ認識のみ） これらのサーバは、リアルタイム モニタリングをサポートしない Windows Server 2003 を除き、ユーザ エージェントによるリアルタイム モニタリングおよび定期的にスケジュールされたポーリングをサポートしています。	

詳細については、以下を参照してください。

- アクセス コントロール ルールへのユーザ条件の追加（17-3 ページ）
- アクセス制御されたユーザおよび LDAP ユーザのメタデータの取得（17-5 ページ）
- Active Directory のログインを報告するためのユーザ エージェントの使用（17-11 ページ）

アクセス コントロール ルールへのユーザ条件の追加

ライセンス： Control

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

サポートされる防御センター： すべて（DC500 を除く）

FireSIGHT システム のユーザ制御機能は、アクセス制御されたユーザをホストの IP アドレスに関連付けることで機能します。配置されたユーザ エージェントは、指定したユーザが Microsoft Active Directory クレデンシャルで認証するときにモニタします。トラフィックがユーザ条件を持つアクセス コントロール ルールに一致するには、モニタ対象のセッション内の送信元ホストまたは宛先ホストいずれかの IP アドレスがログインしているアクセス制御されたユーザに関連付けられている必要があります。

ユーザ制御を実行する前に、以下を行う必要があります。

- Defense Center と Microsoft Active Directory サーバとの間に接続を設定します。アクセス制御されたユーザおよび LDAP ユーザのメタデータの取得（17-5 ページ）を参照してください。
- Active Directory サーバへの TCP/IP アクセスがある Microsoft Windows コンピュータにユーザ エージェントをインストールします。Active Directory のログインを報告するためのユーザ エージェントの使用（17-11 ページ）を参照してください。

注意　モニタする多数のユーザ グループを設定する場合、またはネットワークでホストにマップされるユーザ数が非常に多い場合、システムはメモリ制限のためにグループに基づいてユーザ マッピングをドロップすることがあります。その結果、ユーザ グループに基づくアクセス コントロール ルールが想定どおりに起動しない可能性があります。

1 つのユーザ条件で、最大 50 のユーザおよびグループを [Selected Users] に追加できます。ユーザ グループを持つ条件は、そのグループのメンバー（サブグループのメンバーを含む）のいずれかが送信元/宛先であるトラフィックを照合します。ただし、個別に除外されたユーザと、除外されたサブグループのメンバーは含まれません。

注　グループの条件を使用してユーザ制御を実行する前に、システムはそのグループ内の少なくとも 1 人のユーザからのアクティビティを検出する必要があります。この最初の接続は、一致するアクセス コントロール ルールによって処理**されません**が、代わりに一致する次のルール、またはアクセス コントロール ポリシーのデフォルト アクションによって処理されます。

ユーザ条件を作成する際、警告アイコンは無効な設定を示します。アイコンの上にポインタを置くと詳細が表示されます。また、アクセス コントロール ポリシーおよびルールのトラブルシューティング（12-25 ページ）を参照してください。

ユーザ トラフィックを制御するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　LDAP ユーザまたはグループ別にトラフィックを制御するデバイスを対象とするアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか、または既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集（14-3 ページ）を参照してください。

ステップ 2　ルール エディタで、[Users] タブを選択します。

[Users] タブが表示されます。

ステップ 3　[Available Users] リストから追加するユーザおよびグループを見つけて選択します。

ユーザおよびグループは異なるアイコンでマークされます。追加するユーザおよびグループを検索するには、[Available Users] リストの上にある [Search by name or value] プロンプトをクリックし、ユーザまたはグループの名前を入力します。入力していくと、リストが更新されて一致する項目が表示されます。

項目を選択するには、その項目をクリックします。複数の項目を選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [Select All] を選択します。

ステップ 4　[Add to Rule] をクリックし、選択したユーザおよびグループを [Selected Users] リストに追加します。

選択したユーザおよびグループをドラッグ アンド ドロップすることもできます。

ステップ 5　ルールを保存するか、編集を続けます。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

アクセス制御されたユーザおよび LDAP ユーザのメタデータの取得

ライセンス： FireSIGHTまたはControl

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

ユーザ制御を実行する（つまり、ユーザ条件を含むアクセス コントロール ルールを作成する）前に、Defense Center と組織の 1 つ以上の Microsoft Active Directory サーバ間の接続を設定する必要があります。Defense Center は、定期的かつ自動的に LDAP サーバに問い合わせを行い、アクセス制御されたユーザ（つまり、ユーザ エージェントでアクティビティをモニタするユーザおよびグループ、およびトラフィックの制限時に条件として使用できるユーザおよびグループ）のメタデータを更新します。Defense Center は、アクティビティがユーザ エージェントによってすでに報告されているアクセス制御されていないユーザのメタデータも取得します。または、オンデマンド クエリを実行できます。

ユーザ制御を実行していない場合は、追加のタイプの LDAP サーバに問い合わせを行い、ユーザ認識データ（POP3 および IMAP ユーザのみならず、アクティビティがユーザ エージェントによって報告されるものではなくユーザ検出によって検出される LDAP ユーザに関連付けられているメタデータ）を取得できます。システムは、POP3 および IMAP ログイン内の電子メール アドレスを使用して、Active Directory、OpenLDAP、または Oracle Directory Server Enterprise Edition サーバ上の LDAP ユーザに関連付けます。この場合、Defense Center は定期的に LDAP サーバに問い合わせを行い、アクティビティが最後のクエリ以降にシステムによって検出されたユーザの新規および更新されたメタデータを取得します。

詳細については、以下を参照してください。

- ユーザ認識および制御のための LDAP サーバへの接続（17-5 ページ）
- オンデマンドによるユーザ制御パラメータの更新（17-9 ページ）
- LDAP サーバとの通信の一時停止（17-10 ページ）

ユーザ認識および制御のための LDAP サーバへの接続

ライセンス： FireSIGHTまたはControl

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

Defense Center と組織の LDAP サーバとの間の接続によって以下を行うことができます。

- アクセス制御されたユーザおよびグループ（ユーザ エージェントでアクティビティをモニタするユーザおよびグループ、およびアクセス コントロール ルールによるトラフィックの制限時に条件として使用できるユーザおよびグループ）を指定します。
- アクセス制御されたユーザと、一部のアクセス制御されていないユーザ（ユーザ検出によって検出される POP3 および IMAP ユーザ、およびアクティビティがユーザ検出またはユーザ エージェントによって検出される LDAP ユーザ）のメタデータ取得のためにサーバに問い合わせることができます。

これらの接続、または*ユーザ認識オブジェクト*は、LDAP サーバに対して接続設定および認証フィルタ設定を指定します。これらは、FireSIGHT システム の Web インターフェイスへの外部認証を管理するために設定する認証オブジェクトに似ています。認証オブジェクトの管理（61-5 ページ）を参照してください。

ユーザ制御を実行するには、Microsoft Active Directory LDAP サーバに接続する**必要があります**。LDAP ユーザ メタデータを簡単に取得したい場合、システムは他のタイプの LDAP サーバへの接続をサポートします。表 17-1（17-2 ページ）を参照してください。

システムがユーザ アクティビティを検出すると、システムはそのユーザのレコードを Defense Center ユーザ データベース（ユーザ識別データベースとも呼ばれます）に追加できます。Defense Center は、定期的に LDAP サーバに問い合わせを行い、最後のクエリ以降にアクティビティが検出された新しいユーザおよび更新されたユーザのメタデータを取得します。ユーザがデータベースにすでに存在している場合、システムはメタデータが過去 12 時間更新されていなければ更新します。システムが新しいユーザ ログインを検出してから、Defense Center がユーザ メタデータで更新するまで数分かかる場合があります。

システムは、POP3 と IMAP ログイン内の電子メール アドレスを使用して LDAP サーバ上のユーザに関連付けます。たとえば、LDAP ユーザと電子メール アドレスが同じユーザの POP3 ログインを管理対象デバイスが検出すると、システムは LDAP ユーザのメタデータをそのユーザに関連付けます。

注　LDAP サーバからシステムによって検出されたユーザを削除しても、Defense Centerはユーザ データベースからそのユーザを削除**しません**。そのため、手動で削除する必要があります。ただし、LDAP 変更は、Defense Center が次にアクセス制御されたユーザのリストを更新したときにアクセス コントロール ルールに反映**されます**。

次の表に、モニタ対象ユーザに関連付けることができる LDAP メタデータを示します。LDAP サーバからユーザのメタデータを正常に取得するには、サーバはこの表にリストされている LDAP フィールド名を使用する**必要がある**ことに注意してください。LDAP サーバ上のフィールド名を変更すると、Defense Centerはそのフィールドの情報を使ってデータベースに入力できなくなります。

表 17-2　Cisco フィールドへの LDAP フィールドのマッピング

メタデータ	Defense Center	Active Directory	Oracle Directory Server	OpenLDAP
LDAP ユーザ名	[Username]	samaccountname	cn uid	cn uid
first name	名（First Name）	givenname	givenname	givenname
last name	姓（Last Name）	sn	sn	sn
電子メール アドレス	電子メール	mail userprincipalname（mail に値が設定されていない場合）	mail	mail
department	部門	部門 distinguishedname（department に値が設定されていない場合）	部門	ou
電話番号	Phone	telephonenumber	n/a	telephonenumber

LDAP 管理者と密に連携し、LDAP サーバが正しく設定され、そのサーバに接続して LDAP 接続の作成時に提供する必要がある情報を確実に取得できるようにします。

サーバ タイプ、IP アドレス、およびポート

プライマリ LDAP サーバ（オプションでバックアップ LDAP サーバも）のサーバ タイプ、IP アドレスまたはホスト名、およびポートを指定する必要があります。ユーザ制御を実行する場合は、Microsoft Active Directory サーバを使用する**必要があります**。

LDAP 固有パラメータ

Defense Center が認証サーバ上のユーザ情報を取得するために LDAP サーバを検索する場合は、その検索の出発点が必要です。ベース識別名、すなわち*ベース DN* を提供することで検索する*名前空間*またはディレクトリ ツリーを指定できます。通常、ベース DN には、企業ドメインおよび部門を示す基本構造があります。たとえば、Example 社のセキュリティ（Security）部門のベース DN は、`ou=security,dc=example,dc=com` となります。プライマリ サーバを特定したら、そのサーバから使用可能なベース DN のリストが自動的に取得され、該当するベース DN を選択できることに注意してください。

取得するユーザ情報に適切な権限を持っているユーザのユーザ資格情報を指定する必要があります。指定したユーザの識別名はディレクトリ サーバのディレクトリ情報ツリーで一意でなければならないことに注意してください。

また、LDAP 接続の暗号化方式を指定することもできます。認証に証明書が使用される場合は、証明書内の LDAP サーバの名前と Defense Center Web インターフェイスで指定したホスト名が一致する**必要がある**ことに注意してください。たとえば、LDAP 接続を設定するときに `10.10.10.250` を使用し、証明書内で `computer1.example.com` を使用した場合は、接続が失敗します。

最後に、無応答の LDAP サーバへの接続の試みがバックアップ接続にロールオーバーされるタイムアウト期間を指定する必要があります。

ユーザ アクセス コントロール パラメータとグループ アクセス コントロール パラメータ

ユーザ制御を実行するには、アクセス コントロール ルールで条件として使用するグループを指定します。

グループを含めると、自動的に、すべてのサブグループのメンバーを含む、そのグループのすべてのメンバーが含まれます。ただし、アクセス コントロール ルールでサブグループを使用する場合は、明示的にサブグループを含める必要があります。また、グループと個別のユーザを除外することもできます。グループを除外すると、ユーザが他のグループのメンバーであっても、そのグループのすべてのメンバーが除外されます。

アクセス コントロールで使用可能なユーザの最大数は FireSIGHT ライセンスによって異なります。含めるユーザとグループを選択するときに、ユーザの総数が FireSIGHT のユーザ ライセンス数より少ないことを確認します。アクセス コントロール パラメータの範囲が広すぎる場合、Defense Centerはできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザ数をタスク キューで報告します。

注　含めるグループを指定しなかった場合、システムは指定された LDAP パラメータと一致するすべてのグループのユーザ データを取得します。パフォーマンス上の理由から、Ciscoでは、アクセス コントロールで使用するユーザを代表するグループだけを明示的に含めることを推奨しています。ユーザ グループまたはドメイン ユーザ グループを含めることは**できない**ことに注意してください。

また、Defense Centerがアクセス コントロールで使用する新しいユーザを取得するために LDAP サーバに問い合わせる頻度を指定する必要もあります。

LDAP 接続を作成した後、削除アイコン( )をクリックして、選択内容を確認することで、その接続を削除できます。LDAP 接続を変更するには、編集アイコン( )をクリックします。接続が有効になっている場合は、Defense Center が次に LDAP サーバに問い合わせたときに保存した変更が反映されます。

ユーザ認識またはユーザ制御用の LDAP 接続を作成するには、次の手順を実行します。

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Users] の順に選択します。

[Users Policy] ページが表示されます。

ステップ 2　[Add LDAP Connection] をクリックします。

[Create User Awareness Authentication Object] ページが表示されます。

ステップ 3　オブジェクトの [Name] と [Description] を入力します。

ステップ 4　LDAP [Server Type] を選択します。

ユーザ制御を実行する場合は、Microsoft Active Directory サーバを使用する**必要があります**。

注　ユーザ エージェントは `$` 記号で終わる Active Directory ユーザ名を Defense Centerに送信できません。これらのユーザをモニタする場合は、最後の `$` の文字を削除する必要があります。

ステップ 5　プライマリ LDAP サーバ(オプションで、バックアップ LDAP サーバも)の [IP Address] または [Host Name] を指定します。

ステップ 6　LDAP サーバが認証トラフィックに使用する [Port] を指定します。

ステップ 7　ユーザがアクセスする LDAP ディレクトリの [Base DN] を指定します。

たとえば、Example 社の Security 組織で名前を認証するには、`ou=security,dc=example,dc=com` と入力します。

ヒント　使用可能なすべてのドメインのリストを取得するには、[Fetch DNs] をクリックして、ドロップダウンリストから該当するベース識別名を選択します。

ステップ 8　LDAP ディレクトリへのアクセスを検証するために使用する識別 [User Name] と [Password] を指定します。パスワードを確認します。

たとえば、ユーザ オブジェクトに `uid` 属性が設定されており、Example 社の Security 部門の管理者用のオブジェクトの `uid` 値が `NetworkAdmin` である OpenLDAP サーバに接続している場合は、`uid=NetworkAdmin,ou=security,dc=example,dc=com` と入力することになります。

ステップ 9　[Encryption] 方式を選択します。暗号化を使用する場合は、[SSL Certificate] を追加できます。

証明書内のホスト名は、ステップ 5 で指定した LDAP サーバのホスト名と一致する**必要があります**。

ステップ 10　無応答の LDAP サーバへの接続の試みがバックアップ接続にロールオーバーされるタイムアウト期間(秒単位)を [Timeout] に指定する必要があります。

ステップ 11　オプションで、オブジェクトのユーザ認識設定を指定する前に、[Test] をクリックして接続をテストします。

ステップ 12　ステップ 4 で選択した LDAP サーバのタイプによって 2 つの選択肢があります。

- Active Directory サーバに接続している場合は、[User/Group Access Control Parameters] を有効にして、アクセス コントロールで使用するユーザを指定できます。次の手順に進んでください。
- 他の種類のサーバに接続している場合、または、ユーザ制御を実行しない場合は、ステップ 17 までスキップします。

ステップ 13　[Fetch Groups] をクリックし、指定した LDAP パラメータを使用して、使用可能なグループ リストに値を入力します。

ステップ 14　グループを追加または除外するための右矢印ボタンと左矢印ボタンを使用して、アクセス コントロールで使用するユーザを指定します。

グループを含めると、自動的に、すべてのサブグループのメンバーを含む、そのグループのすべてのメンバーが含まれます。ただし、アクセス コントロール ルールでサブグループを使用する場合は、明示的にサブグループを含める必要があります。グループを除外すると、ユーザが他のグループのメンバーであっても、そのグループのすべてのメンバーが除外されます。

ステップ 15　特定の [User Exclusions] を指定します。

ユーザを除外すると、そのユーザを条件として使用するアクセス コントロール ルールを作成できなくなります。複数のユーザはカンマで区切ります。このフィールドでは、アスタリスク（*）をワイルドカード文字として使用できます。

ステップ 16　LDAP サーバに問い合わせて新しいユーザとグループの情報を取得する頻度を指定します。

デフォルトでは、Defense Centerは 1 日 1 回午前零時にサーバに問い合わせます。

- [Start At] ドロップダウン リストを使用して、クエリを実行するタイミングを指定します。**0** は午前零時を意味し、**1** は午前 1 時を意味します。
- [Update Interval] ドロップダウンリストを使用して、サーバに問い合わせる頻度を時間単位で指定します。

ステップ 17　[Save] をクリックします。

ユーザ アクセス コントロール パラメータとグループ アクセス コントロール パラメータを追加または変更したら、変更の実行を確認します。オブジェクトが保存され、[Users Policy] ページが再度表示されます。

ステップ 18　作成した接続の横にあるスライダをクリックして接続を有効にします。

接続を有効にして、接続にユーザ アクセス コントロール パラメータとグループ アクセス コントロール パラメータが含まれている場合は、すぐに LDAP サーバに問い合わせてユーザとグループの情報を取得するかどうかを選択します。すぐに LDAP サーバに問い合わせない場合は、クエリはスケジュールされた時刻に実行されます。タスク キュー（[System] > [Monitoring] > [Task Status]）で、クエリの進捗をモニタすることができます。

オンデマンドによるユーザ制御パラメータの更新

ライセンス： Control

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

サポートされる防御センター： すべて（DC500 を除く）

LDAP 接続内のユーザ アクセス コントロール パラメータとグループ アクセス コントロール パラメータを変更する場合、または、LDAP サーバ上のユーザまたはグループを変更しその変更をすぐにユーザ制御に反映させたい場合は、Active Directory サーバからのオンデマンド ユーザ データ取得の実行を Defense Center に強制できます。

Defense Centerがサーバから取得可能なユーザの最大数は FireSIGHT ライセンスによって異なります。LDAP 接続内のアクセス コントロール パラメータの範囲が広すぎる場合、Defense Center はできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザ数をタスク キューで報告します。

オンデマンド ユーザ データ取得を実行するには、次の手順を実行します。

アクセス： Admin/Discovery Admin

ステップ 1　[Policies] > [Users] の順に選択します。

[Users Policy] ページが表示されます。

ステップ 2　LDAP サーバへの問い合わせに使用する LDAP 接続の横にあるダウンロード アイコン（ ）をクリックします。

クエリーが開始されます。タスク キュー（[System] > [Monitoring] > [Task Status]）で進捗を監視することができます。

LDAP サーバとの通信の一時停止

ライセンス： FireSIGHTまたはControl

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

LDAP 接続が有効になっていなければ、Defense Center が LDAP サーバに問い合わせることができません。クエリーを停止するには、それらを削除するのではなく、一時的に LDAP 接続を無効にします。

アクセス制御に使用される LDAP 接続を再度有効にすると、すぐにサーバに問い合わせて更新されたユーザおよびグループの情報を取得するように Defense Center に強制するか、または最初に予定されているクエリが行われるまで待機することができます。

LDAP 接続を無効または再度有効にするには、次の手順を実行します。

アクセス： Admin/Discovery Admin

ステップ 1　[Policies] > [Users] の順に選択します。

[Users Policy] ページが表示されます。

ステップ 2　作成した接続の横にあるスライダをクリックして、接続を一時停止または再度有効にします。

接続を再度有効にして、接続にユーザ アクセス コントロール パラメータとグループ アクセス コントロール パラメータが含まれている場合は、すぐに LDAP サーバに問い合わせてユーザとグループの情報を取得するかどうかを選択します。すぐに LDAP サーバに問い合わせない場合は、クエリーがスケジュールされた時刻に実行されます。タスク キュー（[System] > [Monitoring] > [Task Status]）で、クエリの進捗をモニタすることができます。

Active Directory のログインを報告するためのユーザ エージェントの使用

ライセンス：FireSIGHT

Microsoft Windows のコンピュータに導入されたユーザ エージェントは、Microsoft Active Directory サーバをモニタし、組織の LDAP ユーザがホストにログインおよびホストからログアウトしたとき、または他の理由で Active Directory クレデンシャルで認証したときに Defense Center に通知できます。たとえば、アプリケーションやサービスでの認証を Active Directory で一元管理している組織では、このトラフィック制御方法を検討できます。

このエージェントによって報告される情報は、組織におけるユーザ アクティビティの記録としてだけでなく、ユーザ制御の基盤として役立ちます。トラフィックがユーザ条件を持つアクセス コントロール ルールに一致するには、モニタ対象のセッション内の送信元ホストまたは宛先ホストいずれかの IP アドレスがログインしているアクセス制御されたユーザに関連付けられている必要があります。この機能では、特定のユーザまたはユーザ グループに基づいてトラフィックを制御できます。

注　ユーザ制御を実行する場合は、ユーザ エージェントをインストールして使用する**必要があります**。ただし、ユーザ エージェントは Active Directory の認証に関連するユーザ アクティビティのみ報告します。ユーザ認識によって、エージェントによって報告されたすべてのユーザ アクティビティ、および管理対象デバイスごとの許可されたネットワーク トラフィックで検出された他のアクティビティを表示できます。システムは、検出機能を使用して、さまざまなプロトコル（AIM、IMAP、LDAP、Oracle、POP3、SIP、FTP、HTTP および MDNS）を介したログイン試行を識別できます。詳細については、ユーザ データ収集について（45-3 ページ）を参照してください。

ユーザ認識またはユーザ制御のためにユーザ エージェントを使用して LDAP ユーザ認証レコードを取得するには、最初にエージェントからの接続を許可するように各 Defense Center を設定します。ハイ アベイラビリティ展開では、プライマリ Defense Center とセカンダリ Defense Center の両方でエージェント通信を有効にします。ユーザ エージェントは同時に最大 5 つのDefense Centerに接続できます。Defense Center でユーザ エージェントの通信を有効にした後、Windows コンピュータにエージェントをインストールできます。表 17-1（17-2 ページ）を参照してください。

最後に、Microsoft Active Directory サーバからデータを取得してその情報を Defense Center に報告するようにユーザ エージェントを設定します。また、レポートから特定のユーザ名および IP アドレスを除外したり、ローカル イベント ログまたは Windows アプリケーション ログにステータス メッセージをロギングするようにエージェントを設定できます。ユーザ エージェントのステータス モニタ ヘルス モジュールは、Defense Center に接続されたエージェントをモニタします。ユーザ エージェント ステータス モニタリングの設定（68-31 ページ）を参照してください。

ユーザ エージェントに接続するようにDefense Centerを設定するには、以下を行います。

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Users] の順に選択します。

[Users Policy] ページが表示されます。

ステップ 2　[Add User Agent] をクリックします。

[Add User Agent] ポップアップ ウィンドウが表示されます。

ステップ 3　エージェントの**名前**を入力します。

ステップ 4　エージェントをインストールするコンピュータの**ホスト名またはアドレス**を入力します。IPv4 アドレスを使用する必要があります。IPv6 アドレスを使用してユーザ エージェントに接続するように Defense Center を設定することは**できません**。

ステップ 5　[Add User Agent] をクリックします。

これで、Defense Center は指定したコンピュータ上のユーザ エージェントに接続できます。接続を削除するには、削除アイコン（ ）をクリックして、その削除を確認します。

ステップ 6　指定したコンピュータにユーザ エージェントをインストールします。Microsoft Active Directory サーバからデータを取得してその情報を Defense Center に報告するように設定します。

詳細および最新情報については、『*User Agent Configuration Guide*』を参照してください。

侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御

侵入ポリシーとファイル ポリシーは、FireSIGHT システム の一部として連携し、トラフィックがその宛先に許可される前の最後の防御ラインとして機能します。

- **侵入ポリシー**は、システムの侵入防御機能を制御します。ネットワーク分析ポリシーまたは侵入ポリシーについて（23-1 ページ）を参照してください。
- **ファイル ポリシー**は、システムのネットワークベースのファイル制御および高度なマルウェア防御（AMP）機能を制御します。ファイル ポリシーの概要と作成（37-10 ページ）を参照してください。

ハードウェア ベースの高速パス、セキュリティ インテリジェンス ベースのトラフィック フィルタリング（ブラックリスト登録）、SSL インスペクション ベースの決定、およびトラフィックの復号化と前処理は、ネットワーク トラフィックが侵入、禁止されたファイル、およびマルウェアの有無を検査される**前に**発生します。アクセス コントロール ルールおよびアクセス コントロールのデフォルト アクションによって、侵入ポリシーおよびファイル ポリシーで検査されるトラフィックが決まります。

侵入ポリシーまたはファイル ポリシーをアクセス コントロール ルールに関連付けることで、アクセス コントロール ルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイル ポリシー（またはその両方）を使ってトラフィックを検査するよう、システムに指示できます。

注 デフォルトでは、暗号化ペイロードの侵入およびファイル インスペクションは無効化されます。これにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。詳細については、トラフィック復号化の概要（19-1 ページ）およびSSL プリプロセッサの使用（27-75 ページ）を参照してください。

侵入防御および AMP では、次の表に示すように、アクセス コントロール ポリシーのターゲット デバイスで特定のライセンス済み機能を有効にする必要があります。

表 18-1　侵入インスペクションおよびファイル インスペクションのライセンスおよびモデルの要件

機能	説明	ライセンス	サポートされる Defense Center	サポートされるデバイス数
侵入防御	侵入およびエクスプロイトを検出し、任意でブロックします	Protection	いずれか	いずれか
ファイル制御	ファイル タイプの伝送を検出し、任意でブロックします	Protection	いずれか	いずれか
高度なマルウェア防御（AMP）	マルウェアの伝送を検出、保存、追跡し、任意でブロックします キャプチャしたファイルを Cisco クラウドに送信し、マルウェアの分析を行います	Malware	すべて（DC500 を除く）	すべて（シリーズ 2 または X-Series を除く）

また、お客様の組織で FireAMP サブスクリプションをご利用の場合、Defense Center は、Cisco クラウドからエンドポイント ベースのマルウェア検出データを受信することもできます。Defense Center は、このデータを、ネットワークベースのファイルおよびシステム生成のマルウェア データとともに提示します。FireAMP データのインポートには、FireAMP サブスクリプションに加えてライセンスは必要ありません。詳細については、FireAMP 用のクラウド接続の操作（37-27 ページ）を参照してください。

侵入、禁止されたファイル、およびマルウェアの有無についてトラフィックを検査する詳細については、以下を参照してください。

- 許可されたトラフィックに対する侵入およびマルウェアの有無のインスペクション（18-2 ページ）
- 侵入防御パフォーマンスの調整（18-10 ページ）
- ファイルおよびマルウェアのインスペクション パフォーマンスおよびストレージの調整（18-22 ページ）

許可されたトラフィックに対する侵入およびマルウェアの有無のインスペクション

ライセンス： ProtectionまたはMalware

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

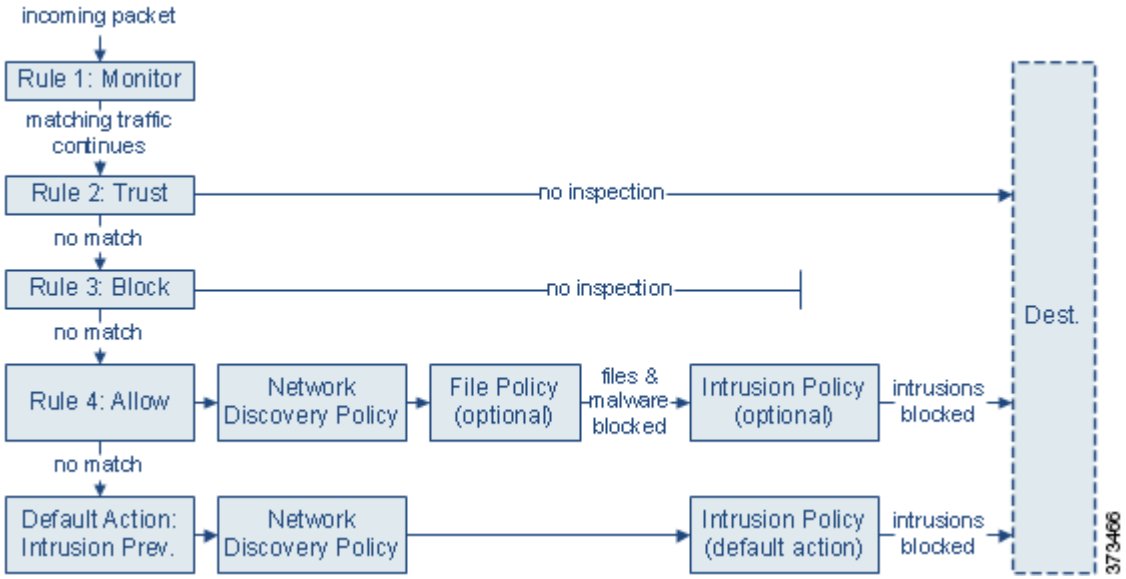
侵入ポリシーおよびファイル ポリシーは、トラフィックがその宛先に許可される前の最後の防衛ラインとして、システムの侵入防御、ファイル制御、および AMP 機能を制御します。ハードウェア ベースの高速パス ルール、セキュリティ インテリジェンス ベースのトラフィック フィルタリング、SSL インスペクションの決定（復号化を含む）、復号化および前処理、およびアクセス コントロール ルールの選択は、侵入およびファイルのインスペクションの**前に**発生します。

アクセス コントロール ルールは、複数の管理対象デバイス間でネットワーク トラフィックを処理する詳細な方法を提供します。侵入ポリシーまたはファイル ポリシーをアクセス コントロール ルールに関連付けることで、アクセス コントロール ルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイル ポリシー（またはその両方）を使ってトラフィッ

クを検査するよう、システムに指示できます。アクセス コントロール ルールの条件は単純または複雑にできます。セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、およびユーザごとにトラフィックを制御できます。

システムは、指定した順にアクセス コントロール ルールをトラフィックと照合します。ほとんどの場合、システムは、*すべて*のルールの条件がトラフィックに一致する場合、*最初*のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。アクセス コントロール ルールの *アクション*によって、システムが一致するトラフィックをどのように処理するかが決まります。一致するトラフィックをモニタ、信頼、ブロック、または許可（追加のインスペクションあり/なしで）することができます。ルール アクションを使用したトラフィックの処理とインスペクションの決定（14-8 ページ）を参照してください。

次の図は、4 つの異なるタイプのアクセス コントロール ルールとデフォルト アクションを含むアクセス コントロール ポリシーによって制御されている、インラインの侵入防御と AMP の展開におけるトラフィックのフローを示します。



上記のシナリオでは、ポリシー内の最初の 3 つのアクセス コントロール ルール（モニタ、信頼およびブロック）は一致するトラフィックを検査できません。モニタ ルールはネットワーク トラフィックの追跡とロギングを行いますが検査はしないので、システムは引き続きトラフィックを追加のルールと照合し、許可または拒否を決定します。信頼ルールおよびブロック ルールは、どのような種類のインスペクションも追加で行うことなく一致するトラフィックを処理しますが、一致しないトラフィックは引き続き次のアクセス コントロール ルールに照合されます。

ポリシー内の 4 番目と最後のルールである許可ルールは、次の順序で他のさまざまなポリシーを呼び出し、一致するトラフィックを検査および処理します。

- **検出：ネットワーク検出ポリシー：**最初に、ネットワーク検出ポリシーは検出データについてトラフィックを検査します。検出はパッシブ分析で、トラフィックのフローに影響しません。明示的に検出を有効にしなくても、それを拡張または無効にできます。ただし、トラフィックを許可すると、検出データの収集は自動的に保証されません。システムは、ネットワーク検出ポリシーによって明示的にモニタされる IP アドレスを含む接続に対してのみ、ディスカバリを実行します。詳細については、ネットワーク検出の概要（45-1 ページ）を参照してください。

- **高度なマルウェア防御およびファイル制御:ファイル ポリシー:**トラフィックが検出によって検査された後、システムは禁止されたファイルやマルウェアについてトラフィックを検査できます。ネットワークベースの AMP は、PDF、Microsoft Office 文書など多数のファイル タイプに潜むマルウェアを検出し、オプションでブロックできます。組織がマルウェア ファイル伝送のブロックに加えて、(ファイルにマルウェアが含まれるかどうかにかかわらず)特定のタイプのすべてのファイルをブロックする必要がある場合は、*ファイル制御*機能により、特定のファイル タイプの伝送についてネットワーク トラフィックをモニタし、ファイルをブロックまたは許可することができます。
- **侵入防御:侵入ポリシー:**ファイル インスペクションの後、システムは侵入およびエクスプロイトについてトラフィックを検査できます。侵入ポリシーは、パターンに基づいて攻撃の有無について復号化されたパケットを検査し、悪意のあるトラフィックをブロックまたは変更できます。侵入ポリシーは*変数セット*とペアになっており、これにより、ユーザは指定された値を使用してネットワーク環境を正確に反映できます。
- **宛先:**前述のすべてのチェックを通過したトラフィックは、その宛先に渡されます。

インタラクティブ ブロック ルール(この図には表示されていません)には、許可ルールと同じインスペクション オプションがあることに留意してください。これにより、あるユーザが警告ページをクリック スルーすることによってブロックされた Web サイトをバイパスした場合に、悪意のあるコンテンツがないかトラフィックを検査できます。詳細については、インタラクティブ ブロッキング アクション:ユーザが Web サイト ブロックをバイパスすることを許可する(14-11 ページ)を参照してください。

ポリシー内のモニタ以外のアクセス コントロール ルールのいずれにも一致しないトラフィックは、デフォルト アクションによって処理されます。このシナリオでは、デフォルト アクションは侵入防御アクションとなり、トラフィックは指定された侵入ポリシーを通過する限りその最終宛先に許可されます。別の展開では、追加のインスペクションなしですべてのトラフィックを信頼またはブロックするデフォルト アクションが存在する場合があります。表 12-4(12-8 ページ)を参照してください。システムはデフォルト アクションによって許可されたトラフィックに対し検出データおよび侵入の有無を検査できますが、禁止されたファイルまたはマルウェアの有無は検査できないことに注意してください。アクセス コントロールのデフォルト アクションにファイル ポリシーを関連付けることは**できません**。

注　場合によっては、接続がアクセス コントロール ポリシーによって分析される場合、システムはトラフィックを処理するアクセス コントロール ルール(存在する場合)を決定する前に、その接続の最初の数パケットを処理し**通過を許可する**必要があります。しかし、これらのパケットは検査されないまま宛先に到達することはないので、デフォルト侵入ポリシーと呼ばれる侵入ポリシーを使用して、パケットを検査し侵入イベントを生成できます。詳細については、アクセス コントロールのデフォルト侵入ポリシーの設定(25-1 ページ)を参照してください。

上記のシナリオの詳細と、ファイル ポリシーおよび侵入ポリシーをアクセス コントロール ルールおよびアクセス コントロールのデフォルト アクションに関連付ける手順については、以下を参照してください。

- ファイル インスペクションおよび侵入インスペクションの順序について(18-5 ページ)
- AMP またはファイル制御を実行するアクセス コントロール ルールの設定(18-7 ページ)
- 侵入防御を実行するアクセス コントロール ルールの設定(18-8 ページ)
- デフォルトの処理の設定およびネットワーク トラフィックのインスペクション(12-7 ページ)

ファイル インスペクションおよび侵入インスペクションの順序について

ライセンス： ProtectionまたはMalware

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

許可されたトラフィックに対する侵入およびマルウェアの有無のインスペクション（18-2 ページ）のシナリオでは、ファイル ポリシーと侵入ポリシーの両方に関連付けられている許可ルールを含む、各タイプのアクセス コントロール ルールを 1 つ示しています。アクセス コントロール ポリシーで、複数の許可ルールとインタラクティブ ブロック ルールを異なる侵入ポリシーおよびファイル ポリシーに関連付けて、インスペクション プロファイルをさまざまなタイプのトラフィックに照合できます。

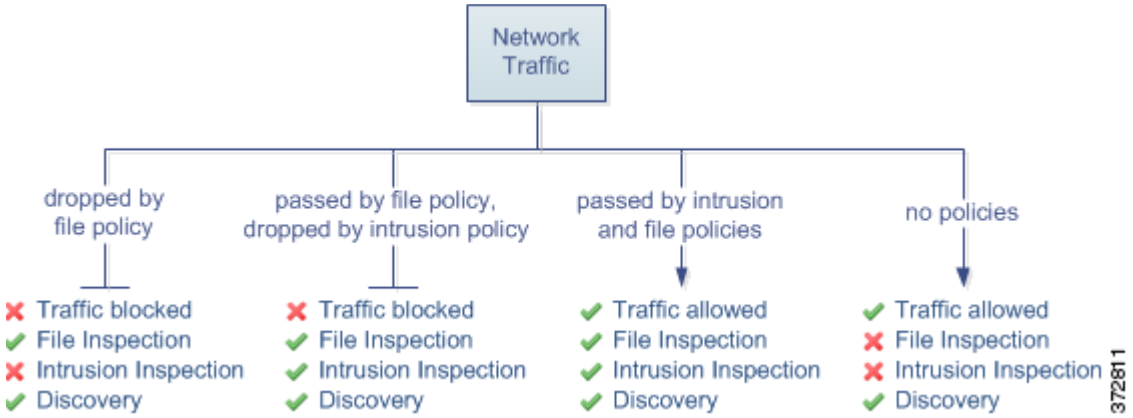
注　侵入防御またはネットワーク検出のみのデフォルト アクションによって許可されたトラフィックは、検出データおよび侵入の有無について検査されますが、禁止されたファイルまたはマルウェアの有無については検査されません。アクセス コントロールのデフォルト アクションにファイル ポリシーを関連付けることは**できません**。

同じルールでファイル インスペクションと侵入インスペクションの両方を実行する必要はありません。許可ルールまたはインタラクティブ ブロック ルールに一致する接続の場合：

- ファイル ポリシーがない場合、トラフィック フローは侵入ポリシーによって決まります
- 侵入ポリシーがない場合、トラフィック フローはファイル ポリシーによって決まります
- どちらもない場合、許可されたトラフィックはネットワーク検出のみで検査されます

ヒント　システムは、信頼されたトラフィックに対してはどんなインスペクションも実行しません。侵入ポリシーもファイル ポリシーも含めずに許可ルールを設定すると、信頼ルールの場合と同様にトラフィックが通過しますが、許可ルールでは一致するトラフィックに対してディスカバリを実行できます。

以下の図は、「許可」アクセス コントロール ルール、またはユーザによりバイパスされた「インタラクティブ ブロック」アクセス コントロール ルールのどちらかの条件を満たすトラフィックに対して実行できるインスペクションの種類を示しています。単純化のために、侵入/ファイル ポリシーの両方が 1 つのアクセス コントロール ルールに関連付けられている（またはどちらも関連付けられていない）状態でのトラフィック フローを図に示しています。



アクセス コントロール ルールによって処理される単一接続の場合、ファイル インスペクションは侵入インスペクションの前に行われます。つまり、システムは侵入のためファイル ポリシーによってブロックされたファイルを検査しません。ファイル インスペクション内では、タイプによる単純なブロッキングの方が、マルウェア インスペクションおよびブロッキングよりも優先されます。

たとえば、アクセス コントロール ルールで定義された特定のネットワーク トラフィックを正常に許可するシナリオを考えてください。ただし、予防措置として、実行可能ファイルのダウンロードをブロックし、ダウンロードされた PDF のマルウェア インスペクションを行って検出された場合はブロックし、トラフィックに対して侵入インスペクションを実行する必要があるとします。

一時的に許可するトラフィックの特性に一致するルールを持つアクセス コントロール ポリシーを作成し、それを侵入ポリシーとファイル ポリシーの両方に関連付けます。ファイル ポリシーはすべての実行可能ファイルのダウンロードをブロックし、マルウェアを含む PDF も検査およびブロックします。

- まず、システムはファイル ポリシーで指定された単純なタイプ マッチングに基づいて、すべての実行可能ファイルのダウンロードをブロックします。それらはすぐにブロックされるため、これらのファイルはマルウェア クラウド ルックアップの対象にも侵入インスペクションの対象にもなりません。
- 次に、システムは、ネットワーク上のホストにダウンロードされた PDF に対するマルウェア クラウド ルックアップを実行します。マルウェア ファイルの性質を持つ PDF はすべてブロックされ、侵入インスペクションの対象にはなりません。
- 最後に、システムはアクセス コントロール ルールに関連付けられている侵入ポリシーを使用して、ファイル ポリシーでブロックされなかったファイルを含む残りのトラフィック全体を検査します。

注　ファイルがセッション内で検出されてブロックされるまで、そのセッションからのパケットは侵入インスペクションの対象となる場合があります。

AMP またはファイル制御を実行するアクセス コントロール ルールの設定

ライセンス： ProtectionまたはMalware

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

アクセス コントロール ポリシーは、複数のアクセス コントロール ルールをファイル ポリシーに関連付けることができます。ファイル インスペクションを許可アクセス コントロール ルールまたはインタラクティブ ブロック アクセス コントロール ルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なるファイルおよびマルウェアのインスペクション プロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムはファイル ポリシーの設定に従って禁止されたファイル（マルウェアを含む）を検出すると、イベントを Defense Center データベースに自動的にロギングします。ログ ファイルまたはマルウェア イベントが必要ない場合は、アクセス コントロール ルールごとにこのロギングを無効にできます。アクセス コントロール ルールにファイル ポリシーを関連付けた後、アクセス コントロール ルール エディタの [Logging] タブで [Log Files] チェックボックスをオフにします。詳細については、許可された接続のファイルおよびマルウェア イベント ロギングの無効化（38-10 ページ）を参照してください。

また、システムは、呼び出し元のアクセス コントロール ルールのロギング設定にかかわらず、関連付けられた接続の終了を Defense Center データベースにロギングします。ファイル イベントとマルウェア イベントに関連付けられた接続（自動）（38-4 ページ）を参照してください。

注意　ファイル ポリシーをアクセス コントロール ルールに関連付けるか、または [None] を選択してポリシーの関連付けを後から解除すると、Snort プロセスが再開され、構成変更を適用する際に一時的にトラフィック検査が中断されます。この検査中にシステムがトラフィックをドロップするか、検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、「Snort の再開によるトラフィックへの影響（1-9 ページ）」を参照してください。

アクセス コントロール ルールにファイル ポリシーを関連付けるには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　アクセス コントロール ルールを使用して AMP またはファイル制御を設定するアクセス コントロール ポリシーの横にある編集アイコン（  ）をクリックします。

ステップ 3　新しいルールを作成するか、または既存のルールを編集します。アクセス コントロール ルールの作成および編集（14-3 ページ）を参照してください。

アクセス コントロール ルール エディタが表示されます。

ステップ 4　ルール アクションが [Allow]、[Interactive Block]、または [Interactive Block with reset] に設定されていることを確認します。

ステップ 5　[Inspection] タブを選択します。

[Inspection] タブが表示されます。

ステップ 6　アクセス コントロール ルールに一致するトラフィックを検査する場合は [File Policy] を選択し、または一致するトラフィックに対するファイル インスペクションを無効にする場合は [None] を選択します。

表示される編集アイコン（）をクリックし、新しいブラウザ タブでポリシーを編集できます。ファイル ポリシーの作成（37-18 ページ）を参照してください。

ステップ 7　[Add] をクリックしてルールを保存します。

ルールが保存されます。変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

侵入防御を実行するアクセス コントロール ルールの設定

ライセンス： Protection

アクセス コントロール ポリシーは、複数のアクセス コントロール ルールを侵入ポリシーに関連付けることができます。侵入インスペクションを許可アクセス コントロール ルールまたはインタラクティブ ブロック アクセス コントロール ルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なる侵入インスペクション プロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムが侵入ポリシーを使用してトラフィックを評価する場合、システムは関連付けられた*変数セット*を使用します。セット内の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスおよびポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

ヒント　システムによって提供される侵入ポリシーを使用する場合であっても、Cisco は、正確にネットワーク環境を反映するためにシステムの侵入変数を設定することを**強く**推奨します。少なくとも、デフォルトのセットにあるデフォルトの変数を変更します。定義済みのデフォルトの変数の最適化（3-20 ページ）を参照してください。

1 つのアクセス コントロール ポリシーで使用可能な固有の侵入ポリシーの数は、ターゲット デバイスのモデルによって異なります。より強力なデバイスは、より多数のポリシーを処理できます。侵入ポリシーと変数セットの固有の**ペア**はすべて、1 つのポリシーとしてカウントされます。異なる侵入ポリシー変数セットのペアを各許可ルールおよびインタラクティブ ブロック ルール（およびデフォルト アクション）と関連付けることができますが、ターゲット デバイスが設定されたとおりにインスペクションを実行するのに必要なリソースを不足している場合は、アクセス コントロール ポリシーを適用できません。詳細については、パフォーマンスを向上させるためのルールの簡素化（12-26 ページ）を参照してください。

システムによって提供される侵入ポリシーとカスタム侵入ポリシーについて

Cisco は、複数の侵入ポリシーを FireSIGHT システム と共に提供します。システムによって提供される侵入ポリシーを使用して、Cisco 脆弱性調査チーム（VRT）のエクスペリエンスを活用することができます。これらのポリシーでは、VRT は侵入ルールおよびプリプロセッサ ルールの状態を設定し、詳細設定の初期設定も提供します。システムによって提供されるポリシーをそのまま使用するか、またはカスタム ポリシーのベースとして使用できます。カスタム ポリシーを作成すれば、環境内のシステムのパフォーマンスを向上させ、ネットワーク上で発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューを提供できます。

お客様が独自に作成するカスタム ポリシーに加えて、システムは初期インライン ポリシーと初期パッシブ ポリシーの 2 つのカスタム ポリシーを提供しています。これらの 2 つの侵入ポリシーは、ベースとして Balanced Security and Connectivity 侵入ポリシーを使用します。両者の唯一の相違点は、[Drop When Inline] 設定です。インライン ポリシーではドロップ動作が有効化され、パッシブ ポリシーでは無効化されています。詳細については、システム付属ポリシーとカスタム ポリシーの比較（23-8 ページ）を参照してください。

接続イベントおよび侵入イベントのロギング

アクセス コントロール ルールによって呼び出された侵入ポリシーが侵入を検出して侵入イベントを生成すると、そのポリシーはそのイベントを Defense Center データベースに保存します。また、システムはアクセス コントロール ルールのロギング設定に関係なく、侵入が発生した接続の終了を Defense Center データベースに自動的にロギングします。侵入に関連付けられる接続（自動）（38-4 ページ）を参照してください。

注意　侵入ポリシーをアクセス コントロール ルールに関連付けるか、または [None] を選択してポリシーの関連付けを後から解除すると、Snort プロセスが再開され、構成変更を適用する際に一時的にトラフィック検査が中断されます。この検査中にシステムがトラフィックをドロップするか、検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、「Snort の再開によるトラフィックへの影響（1-9 ページ）」を参照してください。

アクセス コントロール ルールに侵入ポリシーを関連付けるには、次の手順を実行します。

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　アクセス コントロール ルールを使用して侵入インスペクションを設定するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

ステップ 3　新しいルールを作成するか、または既存のルールを編集します。アクセス コントロール ルールの作成および編集（14-3 ページ）を参照してください。

アクセス コントロール ルール エディタが表示されます。

ステップ 4　ルール アクションが [Allow]、[Interactive Block]、または [Interactive Block with reset] に設定されていることを確認します。

ステップ 5　[Inspection] タブを選択します。

[Inspection] タブが表示されます。

ステップ 6　システムによって提供されるまたはカスタムの**侵入ポリシー**を選択するか、またはアクセス コントロール ルールに一致するトラフィックに対する侵入インスペクションを無効にするには [None] を選択します。

カスタム侵入ポリシーを選択する場合は、表示される編集アイコン（）をクリックし、新しいブラウザ タブでポリシーを編集できます。侵入ポリシーの編集（31-4 ページ）を参照してください。

注意　Ciscoの担当者から指示された場合を除き、`Experimental Policy 1` を選択**しないでください**。Ciscoでは、試験用にこのポリシーを使用します。

ステップ 7　オプションで、侵入ポリシーに関連付けられている**変数セット**を変更します。

表示される編集アイコン（）をクリックし、新しいブラウザ タブで変数セットを編集できます。変数セットの操作（3-19 ページ）を参照してください。

ステップ 8　[Save] をクリックしてルールを保存します。

ルールが保存されます。変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

侵入防御パフォーマンスの調整

ライセンス： Protection

Ciscoには、侵入行為のトラフィックを分析する際のシステムのパフォーマンスを向上するための機能が備わっています。これらのパフォーマンス設定は、各アクセス コントロール ポリシーごとに設定し、その設定はその親のアクセス コントロール ポリシーによって呼び出されるすべての侵入ポリシーに適用されます。

詳細については、以下を参照してください。

- 侵入に対するパターン一致の制限（18-10 ページ）では、イベント キューで許可されるパケット数を指定し、より大きなストリームに再構築されるパケットのインスペクションを有効または無効にする方法を説明します。
- 侵入ルールの正規表現制限のオーバーライド（18-11 ページ）では、Perl 適合正規表現（PCRE）のデフォルトの一致および再帰の制限をオーバーライドする方法を説明します。
- パケットごとに生成される侵入イベントの制限（18-13 ページ）では、ルール処理イベント キュー設定を構成する方法を説明します。
- パケットおよび侵入ルール遅延しきい値の設定（18-14 ページ）では、デバイスの遅延をパケットおよびルール遅延しきい値構成の許容レベルで保持する必要性とセキュリティのバランスを実現する方法を説明します。
- 侵入パフォーマンス統計情報のロギングの設定（18-21 ページ）では、管理対象デバイスの基本的なパフォーマンス モニタリングおよびレポート パラメータを設定する方法について説明します。

侵入に対するパターン一致の制限

ライセンス： Protection

イベント キューで許可するパケット数を指定できます。ストリーム再構成の前後に、より大きなストリームに再構築されるパケットのインスペクションを有効または無効にできます。

イベント キューの設定：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　編集するアクセス コントロール ポリシーの横にある編集アイコン( )をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3　[Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[Performance Settings] の横にある編集アイコン( )をクリックし、表示されるポップアップ ウィンドウで [Pattern Matching Limits] タブを選択します。

ステップ 5　次のオプションを修正できます。

- [Maximum Pattern States to Analyze Per Packet] フィールドに、キューに含めるイベントの最大値の値を入力します。
- ストリーム再構成の前後で、データのより大きなストリームに再構築されるパケットを検査するには、[Disable Content Checks on Traffic Subject to Future Reassembly] を選択します。再構成の前後の検査はより多くの処理オーバーヘッドを必要とするため、パフォーマンスが低下する可能性があります。
- ストリーム再構成の前後で、データのより大きなストリームに再構築されるパケットのインスペクションを無効にするには、[Disable Content Checks on Traffic Subject to Future Reassembly] をオフにします。検査を無効にすると、ストリームの検査の処理オーバーヘッドが減少し、パフォーマンスが向上する場合があります。

ステップ 6　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

侵入ルールの正規表現制限のオーバーライド

ライセンス：Protection

パケット ペイロードの内容を検査するための侵入ルールで使用される PCRE のデフォルトの一致および再帰の制限をオーバーライドできます。侵入ルールにおける `pcre` キーワードの使用については、PCRE を使用したコンテンツの検索（36-38 ページ）を参照してください。デフォルトの制限によってパフォーマンスの最低レベルが確保されます。これらの制限をオーバーライドすると、セキュリティが向上する可能性がありますが、非効率的な正規表現に対してパケット評価を許可することで、パフォーマンスが著しく影響を受ける可能性もあります。

注意　非効率的なパターンの影響に関する知識があり、侵入ルールの作成経験が豊富であるユーザー以外は、デフォルトの PCRE の制限をオーバーライドしないでください。

次の表に、デフォルトの制限をオーバーライドするように設定できるオプションを示します。

表 18-2　正規表現の制約オプション

オプション	説明
Match Limit State	[Match Limit] をオーバーライドするかどうかを指定します。次の選択肢があります。 • [Default] を選択して、[Match Limit] に設定した値を使用する • [Unlimited] を選択して、無制限の数の試行を許可する • [Custom] を選択して、[Match Limit] に対して 1 以上の制限を指定するか、または PCRE の一致の評価を完全に無効化するために 0 を指定する
Match Limit	PCRE 正規表現で定義されたパターンに一致することを試行する回数を指定します。
Match Recursion Limit State	[Match Recursion Limit] をオーバーライドするかどうかを指定します。次の選択肢があります。 • [Default] を選択して、[Match Recursion Limit] に設定した値を使用する • [Unlimited] を選択して、無制限の数の再帰を許可する • [Custom] を選択して、[Match Recursion Limit] に対して 1 以上の制限を指定するか、または PCRE の再帰を完全に無効化するために 0 を指定する [Match Recursion Limit] が意味を持つためには、[Match Limit] よりも小さい必要があることに注意してください。
Match Recursion Limit	パケット ペイロードに対して PCRE 正規表現を評価する際の再帰数を指定します。

PCRE オーバーライドの設定：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　編集するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3　[Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[Performance Settings] の横にある編集アイコン（）をクリックし、表示されるポップアップ ウィンドウで [Regular Expression Limits] タブを選択します。

ステップ 5　正規表現の制約オプションの表の任意のオプションを変更できます。

ステップ 6　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

パケットごとに生成される侵入イベントの制限

ライセンス：Protection

ルール エンジンがルールに対してトラフィックを評価する場合、特定のパケットまたはパケット ストリームに生成されたイベントをイベント キューに配置し、キュー内の上位のイベントをユーザ インターフェイスに報告します。複数のイベントが発生した場合、ルール エンジンが 1 個のパケットまたはパケット ストリームに対して複数のイベントを記録するように選択できます。これらのイベントのロギングにより、報告されたイベントを超えて情報を収集することができます。このオプションを設定する場合、キュー内に配置可能なイベントの数および記録されるイベントの数を指定できます。また、キュー内のイベントの順序を決定する条件を選択できます。

次の表に、1 個のパケットまたはストリームに対して記録されるイベントの数を決定するために設定できるオプションを示します。

表 18-3　侵入イベント ロギング制限のオプション

オプション	説明
Maximum Events Stored Per Packet	特定のパケットまたはパケット ストリームに対して保存できるイベントの最大数。
Maximum Events Logged Per Packet	特定のパケットまたはパケット ストリームに対して記録されるイベントの数。これは、[Maximum Events Stored Per Packet] 値を超えてはいけません。
Prioritize Event Logging By	イベント キュー内のイベントの順序を決定するために使用する値。最上位のイベントがユーザ インターフェイスから報告されます。次の中から選択できます。 • `priority`。イベントの優先順位によってキュー内のイベントを並べ替えます。 • `content_length`。最も長い識別コンテンツの一致によってイベントを並べ替えます。イベントがコンテンツ長によって並べ替えられる場合、ルール イベントは常にデコーダ イベントおよびプリプロセッサ イベントよりも優先されます。

1 個のパケットまたはストリームに対して記録されるイベント数の設定：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　編集するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3　[Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[Performance Settings] の横にある編集アイコン（）をクリックし、表示されるポップアップ ウィンドウで [Intrusion Event Logging Limits] タブを選択します。

ステップ 5　侵入イベント ロギング制限のオプションの表の任意のオプションを変更できます。

ステップ 6　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

パケットおよび侵入ルール遅延しきい値の設定

ライセンス： Protection

デバイスの遅延をパケットおよびルール遅延しきい値構成の許容レベルで保持する必要性とセキュリティのバランスを保つことができます。詳細については、以下を参照してください。

- パケット遅延しきい値構成について（18-14 ページ）
- パケット遅延しきい値構成の設定（18-16 ページ）
- パケット遅延しきい値構成を無効にするには、次の手順を実行します。（18-17 ページ）
- ルール遅延しきい値構成の設定（18-19 ページ）

パケット遅延しきい値構成について

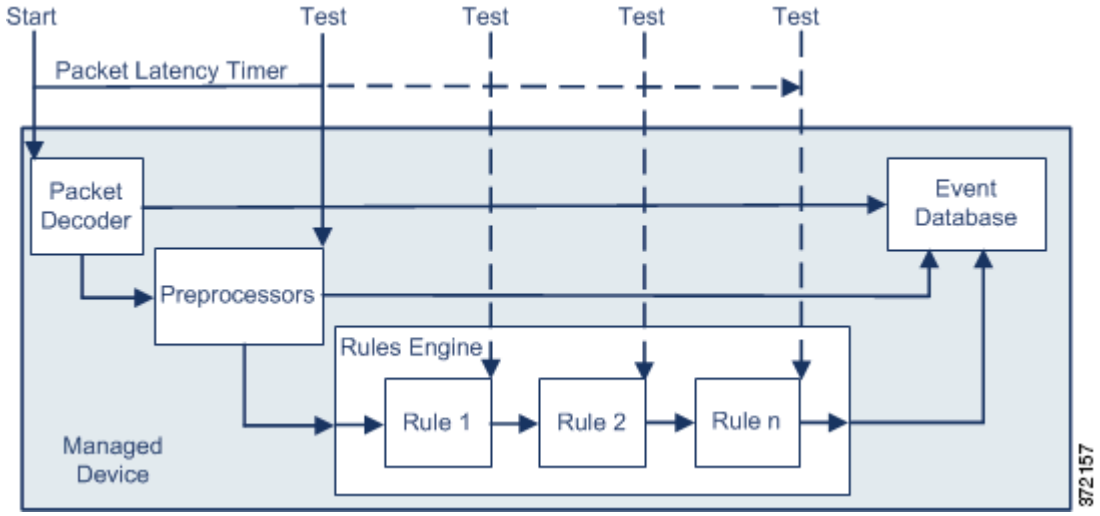
ライセンス： Protection

パケット遅延しきい値構成を有効にすることで、遅延を許容レベルで保持する必要性とセキュリティのバランスを取ることができます。パケット遅延しきい値構成は、該当するデコーダ、プリプロセッサ、およびルールによるパケット処理の総経過時間を測定し、処理時間が設定可能なしきい値を超えるとパケットのインスペクションを終了します。

パケット遅延しきい値構成は、ルールがパケットを処理する際に必要な実際の時間をより正確に反映するために、処理時間のみでなく、経過時間を測定します。ただし、遅延しきい値構成は、厳密なタイミングを強制しないソフトウェア ベースの遅延実装です。

遅延しきい値構成から生じるパフォーマンスと遅延のメリットに関するトレードオフは、未検査パケットに攻撃が含まれる可能性があることです。ただし、パケット遅延しきい値構成では、セキュリティと接続性のバランスを取るために使用可能なツールが用意されています。

デコーダの処理の開始時に各パケットのタイマーが起動します。タイミングは、パケットのすべての処理が終了するか、または処理時間がタイミング テスト ポイントでしきい値を超えるまで継続します。



上の図に示すように、パケット遅延タイミングは次のテスト ポイントでテストされます。

- すべてのデコーダおよびプリプロセッサの処理の完了後、ルールの処理が開始される前
- 各ルールによる処理の後

処理時間がいずれかのテスト ポイントでしきい値を超えると、パケット インスペクションは終了します。

ヒント　パケットの合計処理時間にルーチン TCP ストリームまたは IP フラグメント再構成の時間は含まれません。

パケット遅延しきい値構成は、パケットを処理するデコーダ、プリプロセッサ、またはルールによってトリガーされるイベントに影響を与えません。該当するデコーダ、プリプロセッサ、またはルールは、パケットが完全に処理されるか、または遅延しきい値を超えたためにパケット処理が終了されるか、どちらか先に発生した時点まで通常通りトリガーされます。廃棄ルールがインライン展開の侵入を検知すると、その廃棄ルールがイベントをトリガーし、パケットは廃棄されます。

注　パケット遅延しきい値違反のためにパケットの処理が終了した後は、ルールに対してパケットは評価されません。イベントを引き起こす可能性があったルールはそのイベントをトリガーできず、廃棄ルールに対してパケットを廃棄できません。

廃棄ルールの詳細については、ルール状態の設定（32-22 ページ）を参照してください。

パケット遅延しきい値構成は、パッシブとインラインの両方の展開でシステムのパフォーマンスを向上することができます。また、過剰な処理時間を必要とするパケットのインスペクションを停止することで、インライン展開の遅延を減らすことができます。これらのパフォーマンスのメリットは、たとえば次の場合に得られる可能性があります。

- パッシブ展開およびインライン展開の両方で、複数のルールによるパケットの順次検査に長時間かかる場合
- インライン展開で、ユーザーが非常に大きなファイルをダウンロードするときなど、ネットワーク パフォーマンスの低下がパケット処理を遅らせる場合

パッシブ展開では、パケットの処理を停止しても、処理が単に次のパケットに移るだけで、ネットワーク パフォーマンスの回復につながらない可能性があります。

パケット遅延しきい値構成の設定

ライセンス：Protection

遅延ベースのパフォーマンス設定は、システムによって提供される Balanced Security and Connectivity 侵入ポリシーによってデフォルトで有効になっています。次の表に、パケット遅延しきい値構成でユーザが設定できるオプションを示します。

表 18-4　パケット遅延しきい値構成オプション

オプション	説明
Threshold (microseconds)	パケットのインスペクションが終了する時間をマイクロ秒単位で指定します。推奨される最小しきい値の設定については、最小のパケット遅延しきい値設定の表を参照してください。

ルール 134:3 を有効にして、パケット遅延しきい値を超えたためにシステムがパケットのインスペクションを終了するイベントを生成できます。詳細については、侵入イベントの表示（41-9 ページ）およびルール状態の設定（32-22 ページ）を参照してください。

システム パフォーマンスおよびパケット遅延の測定に影響する要因は、CPU 速度、データ レート、パケット サイズ、プロトコル タイプなど多数あります。このため Cisco は、ユーザ独自の計算によってご自身のネットワーク環境に合った設定を行うまで、次の表のしきい値設定を使用することを推奨します。

表 18-5　最小のパケット遅延しきい値設定

データ レート	最小しきい値設定（マイクロ秒）
1 Gbps	100
100 Mbps	250
5 Mbps	1000

独自の設定を計算する場合は、次の項目を決定します。

- 1 秒あたりの平均パケット数
- 1 パケットあたりの平均マイクロ秒数

パケット インスペクションを不必要に中断することがないように、ネットワークの 1 パケットあたりの平均マイクロ秒数に重要な安全係数を乗算します。

たとえば、最小のパケット遅延しきい値設定の表では、1 ギガビット環境で 100 マイクロ秒の最小パケット遅延しきい値を推奨しています。この最小推奨値は、1 秒あたり平均 250,000 パケットを示すテスト データに基づいています。これは、1 マイクロ秒あたり 0.25 パケット、言い換えると 1 パケットあたり 4 マイクロ秒に相当します。25 倍すると推奨最小しきい値の 100 マイクロ秒が得られます。

パケット遅延しきい値の設定:

アクセス: Admin/Access Admin/Network Admin

ステップ 1 [Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 編集するアクセス コントロール ポリシーの横にある編集アイコン( )をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4 [Latency-Based Performance Settings] の横にある編集アイコン( )をクリックし、表示されるポップアップ ウィンドウで [Packet Handling] タブを選択します。

ヒント デフォルトでは、パケット遅延しきい値構成が有効になっています。遅延しきい値構成を完全に無効にするには、[Enable] チェックボックスをオフにします。

ステップ 5 推奨される最小しきい値の設定については、最小のパケット遅延しきい値設定の表を参照してください。

ステップ 6 [OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。アクセス コントロール ポリシーの適用 (12-17 ページ) を参照してください。

パケット遅延しきい値構成を無効にするには、次の手順を実行します。

アクセス: Admin/Access Admin/Network Admin

ステップ 1 [Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 編集するアクセス コントロール ポリシーの横にある編集アイコン( )をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4 [Latency-Based Performance Settings] の横にある編集アイコン( )をクリックし、表示されるポップアップ ウィンドウで [Packet Handling] タブを選択します。

ステップ 5 推奨される最小しきい値の設定については、最小のパケット遅延しきい値設定の表を参照してください。

ステップ 6 [OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。アクセス コントロール ポリシーの適用 (12-17 ページ) を参照してください。

ルール遅延しきい値構成について

ライセンス：Protection

ルール遅延しきい値構成を有効にすることで、遅延を許容レベルで保持する必要性とセキュリティのバランスを取ることができます。ルール遅延しきい値構成は、各ルールが個別のパケットの処理に費やした時間を測定し、処理時間が遅延しきい値ルールをある回数（設定可能）連続して超えた場合は、そのルールに違反した処理を、関連するルールのグループとともに指定された期間中断し、中断期間終了後にルールを回復します。

ルール遅延しきい値構成は、ルールがパケットを処理する際に必要な実際の時間をより正確に反映するために、処理時間のみでなく、経過時間を測定します。ただし、遅延しきい値構成は、厳密なタイミングを強制しないソフトウェア ベースの遅延実装です。

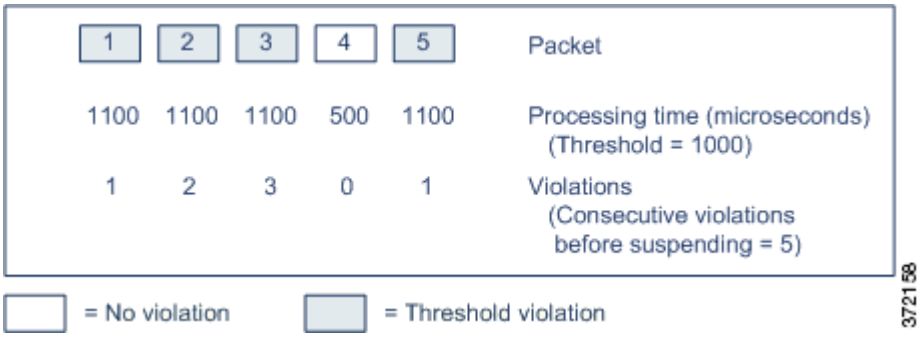
遅延しきい値構成から生じるパフォーマンスと遅延のメリットに関するトレードオフは、未検査パケットに攻撃が含まれる可能性があることです。ただし、ルール遅延しきい値構成では、セキュリティと接続性のバランスを取るために使用可能なツールが用意されています。

パケットがルールのグループに対して処理されるたびに、タイマーが処理時間を測定します。ルール処理時間が指定されたルール遅延しきい値を超えると、システムでカウンタが増加します。連続したしきい値違反の数が指定した数に達すると、システムは次のアクションを実行します。

- 指定された時間、ルールを一時停止する
- ルールが一時停止されたことを示すイベントをトリガーとして使用する
- 一時停止期間が過ぎたらルールを再度有効にする
- ルールが再び有効になったことを示すイベントをトリガーとして使用する

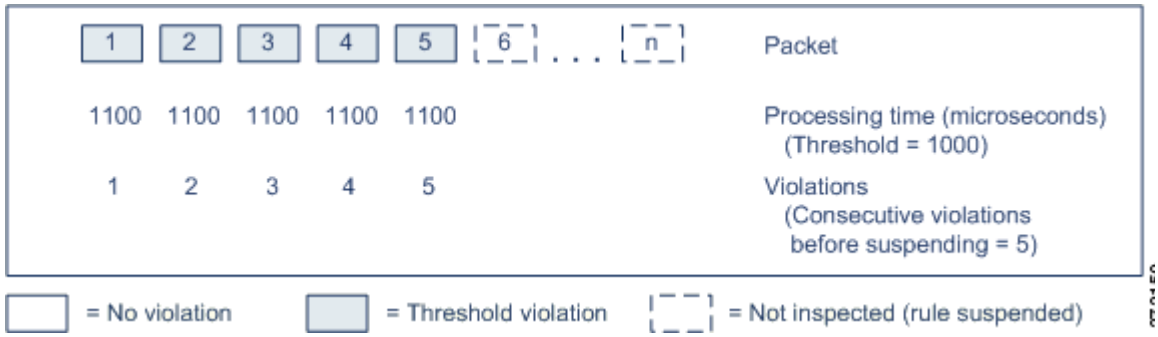
ルールのグループが一時停止しているか、またはルール違反が連続していない場合は、カウンタがゼロになります。ルールを一時停止する前に連続する違反の一部を許可することにより、パフォーマンスへの影響がわずかであると考えられる散発的なルール違反を無視し、繰り返しルール遅延しきい値を超えるルールのより重大な影響に焦点を当てることができます。

次の例は、ルールが一時停止にならない、5 つの連続したルール処理時間を示します。



上の例で、最初の 3 個の各パケットの処理に必要な時間は 1000 マイクロ秒というルール遅延しきい値に違反し、違反カウンタは各違反のたびに増加します。4 個目のパケット処理はしきい値に違反しないので、違反カウンタはゼロにリセットされます。5 個目のパケットはしきい値に違反し、違反カウンタは 1 から再開します。

次の例は、ルールが一時停止になる、5 つの連続したルール処理時間を示します。



2 番目の例で、5 個のパケットのそれぞれの処理に必要な時間は 1000 マイクロ秒というルール遅延しきい値に違反します。各パケットの 1100 マイクロ秒というルール処理時間が指定された連続する 5 回の違反に対する 1000 マイクロ秒というしきい値に違反するため、ルールのグループは一時停止されます。図中のパケット 6 から n で表される後続のパケットは、一時停止期間が経過するまで、一時停止されたルールに対して検査されません。ルールが再有効化された後にさらにパケットが発生すると、違反カウンタはゼロから再開されます。

ルール遅延しきい値構成は、パケットを処理するルールによってトリガーされる侵入イベントに影響を及ぼしません。ルール処理時間がしきい値を超えるかどうかにかかわらず、パケット内で検出されるすべての侵入に対して、ルールはイベントをトリガーします。侵入を検知するルールがインライン展開の廃棄ルールである場合、パケットは廃棄されます。廃棄ルールがパケット内で侵入を検出し、その結果ルールが一時停止されると、廃棄ルールは侵入イベントをトリガーし、パケットは廃棄され、そのルールと関連するすべてのルールが一時停止されます。廃棄ルールの詳細については、ルール状態の設定（32-22 ページ）を参照してください。

注　パケットは一時停止されたルールに対して評価されません。イベントを引き起こす可能性があった一時停止ルールはそのイベントをトリガーできず、廃棄ルールに対してパケットを廃棄できません。

ルール遅延しきい値構成は、パッシブとインラインの両方の展開でシステムのパフォーマンスを向上することができます。また、パケットの処理に最も多くの時間を必要とするルールを一時停止することで、インライン展開の遅延を減らすことができます。設定可能な時間が過ぎるまで、パケットは一時停止されたルールに対して再度評価されず、過負荷のデバイスに回復の時間が与えられます。これらのパフォーマンスのメリットは、たとえば次の場合に得られる可能性があります。

- 短期間で作成され、ほとんどテストされていないルールが過剰な処理時間を必要とする場合
- ユーザーが非常に大きなファイルをダウンロードするときなど、ネットワーク パフォーマンスの低下がパケット インスペクションを遅らせる場合

ルール遅延しきい値構成の設定

ライセンス：Protection

ルール遅延しきい値、一時停止されるルールの一時停止時間、ルールを一時停止する前に発生する必要がある連続したしきい値違反の回数の変更を行うことができます。

ルールによるパケット処理時間が、[Consecutive Threshold Violations Before Suspending Rule] で指定された回数連続して [Threshold] を超えると、ルール遅延しきい値構成は [Suspension Time] で指定された時間、ルールを一時停止します。

ルール 134:1 を有効にして、ルールが一時停止されるときにイベントを生成できます。また、ルール 134:2 を有効にして、一時停止されたルールが有効化されるときにイベントを生成できます。詳細については、侵入イベントの表示（41-9 ページ）およびルール状態の設定（32-22 ページ）を参照してください。

次の表に、ルール遅延しきい値構成でユーザが設定できるオプションを示します。

表 18-6　ルール遅延しきい値構成オプション

オプション	説明
Threshold	ルールがパケットを検査する際に超えることができない時間をマイクロ秒単位で指定します。推奨される最小しきい値の設定については、最小のルール遅延しきい値設定の表を参照してください。
Consecutive Threshold Violations Before Suspending Rule	ルールが一時停止される前に、ルールによるパケットの検査時間が [Threshold] で設定された時間を超えることができる、連続した回数を指定します。
Suspension Time	ルールのグループを一時停止する秒数を指定します。

システム パフォーマンスの測定に影響する要因は、CPU 速度、データ レート、パケット サイズ、プロトコル タイプなど多数あります。このため Cisco は、ユーザ独自の計算によってご自身のネットワーク環境に合った設定を行うまで、次の表のしきい値設定を使用することを推奨します。

表 18-7　最小のルール遅延しきい値設定

データ レート	最小しきい値設定（マイクロ秒）
1 Gbps	500
100 Mbps	1250
5 Mbps	5000

独自の設定を計算する場合は、次の項目を決定します。

- 1 秒あたりの平均パケット数
- 1 パケットあたりの平均マイクロ秒数

ルールを不必要に一時停止することがないように、ネットワークの 1 パケットあたりの平均マイクロ秒数に重要な安全係数を乗算します。

ルール遅延しきい値の設定：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　編集するアクセス コントロール ポリシーの横にある編集アイコン（  ）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3　[Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[Latency-Based Performance Settings] の横にある編集アイコン（）をクリックし、表示されるポップアップ ウィンドウで [Rule Handling] タブを選択します。

ステップ 5　ルール遅延しきい値構成オプション の表の任意のオプションを設定できます。

推奨される最小しきい値の設定については、最小のルール遅延しきい値設定の表を参照してください。

ステップ 6　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

侵入パフォーマンス統計情報のロギングの設定

ライセンス：Protection

デバイスがそのパフォーマンスを監視および報告する動作に関する基本的なパラメータを設定できます。次のオプションを設定することにより、システムがデバイスのパフォーマンス統計情報を更新する間隔を指定できます。

サンプル時間（秒）とパケットの最小数

パフォーマンス統計情報の各更新の間で指定した秒数が経過すると、システムは指定したパケット数を分析したかを検証します。分析していた場合、システムはパフォーマンス統計情報を更新します。それ以外の場合、システムは指定したパケット数を分析するまで待機します。

トラブルシューティング オプション：Log Session/Protocol Distribution

トラブルシューティングの電話中に、プロトコル分布、パケット長、およびポートの統計情報のログを取るようにサポートから依頼される場合があります。

注意　このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイダンスに従って実行してください。

トラブルシューティング オプション：Summary

トラブルシューティングの電話中に、Snort® プロセスのシャット ダウンまたは再起動時に限り、パフォーマンス統計情報を計算するようにシステムを設定するようにサポートから依頼される場合があります。このオプションを有効にするには、[Log Session/Protocol Distribution] トラブルシューティング オプションも有効にする必要があります。

注意　このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイダンスに従って実行してください。

基本的なパフォーマンス統計情報パラメータの設定:

アクセス: Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　編集するアクセス コントロール ポリシーの横にある編集アイコン(✎)をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3　[Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[Performance Settings] の横にある編集アイコン(✎)をクリックし、表示されるポップアップ ウィンドウで [Performance Statistics] タブを選択します。

ステップ 5　前述のように、[Sample time] または [Minimum number of packets] を変更します。

ステップ 6　任意で、サポートによって求められた場合にのみ、[Troubleshoot Options] セクションを展開し、そのオプションを変更します。

ステップ 7　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。アクセス コントロール ポリシーの適用(12-17 ページ)を参照してください。

ファイルおよびマルウェアのインスペクション パフォーマンスおよびストレージの調整

ライセンス: ProtectionまたはMalware

サポートされるデバイス: 機能によって異なる

サポートされる防御センター: 機能によって異なる

ファイル制御、ファイル ストレージ、動的分析、あるいはマルウェアの検出またはブロッキングを行うためにファイル ポリシーを使用する場合は、次の表にリストするオプションを設定できます。ファイル サイズを増やすと、システムのパフォーマンスに影響を与える可能性があることに注意してください。

注意　アクセス コントロール ポリシーの拡張設定 [Files and Malware Settings] のデフォルト値を置き換えると、Snort プロセスが再開され、構成変更を適用する際、一時的にトラフィック検査が中断されます。この検査中にシステムがトラフィックをドロップするか、検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、「Snort の再開によるトラフィックへの影響(1-9 ページ)」を参照してください。

表 18-8　アクセス コントロール ファイルおよびマルウェア検出の詳細オプション

フィールド	説明	デフォルト値	範囲	注意
Limit the number of bytes inspected when doing file type detection	ファイル タイプを検出するときに検査するバイト数を指定します。	1460 バイト、または TCP パケットの最大セグメント サイズ	0 ～ 4294967295（4GB）	制限を取り除くには、0 に設定します。 ほとんどの場合、システムは最初のパケットによって、一般的なファイル タイプを特定できます。
Do not calculate SHA-256 hash values for files larger than (in bytes)	システムが特定のサイズを超えるファイルを保管すること、ファイルでCollective Security Intelligence クラウド ルックアップを実行すること、またはカスタム検出リストに追加されたファイルをブロックすることを防止します。	10485760（10MB）	0 ～ 4294967295（4GB）	制限を取り除くには、0 に設定します。 この値は、[Maximum file size to store (bytes)] および [Maximum file size for dynamic analysis testing (bytes)] の値以上に設定する必要があります。
Allow file if cloud lookup for Block Malware takes longer than (seconds)	マルウェア クラウド ルックアップの実行中に、システムが [Block Malware] ルールに一致し、性質がキャッシュに入れられていないファイルを保持する期間を指定します。システムが性質を取得する前にこの期間が満了すると、ファイルが渡されます。「使用不可」の性質はキャッシュに入れられません。	2 秒	0 ～ 30 秒	このオプションは最大 30 秒に設定できますが、Ciscoではデフォルト値を使用して、接続失敗によってトラフィックがブロックされないようにすることを推奨します。サポートに連絡することなくこのオプションを 0 に設定**しない**でください。
Minimum file size to store (bytes)	システムがファイル ルールを使用して保管できるファイルの最小サイズを指定します。	6144（6KB）	0 ～ 10485760（10MB）	ファイル ストレージを無効にするには、0 に設定します。 このフィールドは、[Maximum file size to store (bytes)] および [Do not calculate SHA-256 hash values for files larger than (in bytes)] の値以下に設定する必要があります。
Maximum file size to store (bytes)	システムがファイル ルールを使用して保管できるファイルの最大サイズを指定します。	1048576（1MB）	0 ～ 10485760（10MB）	ファイル ストレージを無効にするには、0 に設定します。 このフィールドは、[Minimum file size to store (bytes)] の値以上、および [Do not calculate SHA256 hash values for files larger than (in bytes)] の値以下に設定する必要があります。

表 18-8　アクセス コントロール ファイルおよびマルウェア検出の詳細オプション（続き）

フィールド	説明	デフォルト値	範囲	注意
Minimum file size for dynamic analysis testing (bytes)	システムがクラウドに動的分析対象として送信できるファイルの最小サイズを指定します。	6144（6KB）	6144（6KB）～ 2097152（2MB）	このフィールドは、[Maximum file size for dynamic analysis testing (bytes)] および [Do not calculate SHA-256 hash values for files larger than (in bytes)] の値以下に設定する必要があります。 システムはクラウドをチェックして、送信可能なファイルの最小サイズが更新されているかどうかを調べます（最大で 1 日 1 回）。新しい最小サイズが現在の値より大きい場合、現在の値が新しい最小サイズに更新され、ポリシーは古いポリシーとしてマークされます。
Maximum file size for dynamic analysis testing (bytes)	システムがクラウドに動的分析対象として送信できるファイルの最大サイズを指定します。	1048576（1MB）	6144（6KB）～ 2097152（2MB）	このフィールドは、[Minimum file size for dynamic analysis testing (bytes)] の値以上、[Do not calculate SHA256 hash values for files larger than (in bytes)] の値以下に設定する必要があります。 システムはクラウドをチェックして、送信可能なファイルの最大サイズが更新されているかどうかを調べます（最大で 1 日 1 回）。新しい最大サイズが現在の値より小さい場合、現在の値が新しい最大サイズに更新され、ポリシーは古いポリシーとしてマークされます。

DC500 では Malware ライセンスを使用できず、シリーズ 2 デバイスまたは Cisco NGIPS for Blue Coat X-Series で Malware ライセンスを有効にすることもできないことに注意してください。このため、これらのアプライアンスを使用して個別のファイルをキャプチャ、保存、ブロックしたり、アーカイブ ファイルの内容を分析したり、動的分析用にファイルを送信したり、マルウェア クラウド ルックアップの対象となるファイルの伝送経路を表示したりすることはできません。

ファイルおよびマルウェアのインスペクション パフォーマンスおよびストレージを設定するには、次の手順を実行します。

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　編集するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3　[Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[Files and Malware Settings] の横にある編集アイコン（  ）をクリックします。

[Files and Malware Settings] ポップアップ ウィンドウが表示されます。

ステップ 5　アクセス コントロール ファイルおよびマルウェア検出の詳細オプション の表の任意のオプションを設定できます。

ステップ 6　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

CHAPTER 19

トラフィック復号化の概要

デフォルトでは、セキュア ソケット レイヤ（SSL）または Transport Layer Security（TLS）プロトコルで暗号化されたトラフィックは検査されません。アクセス コントロールの一部として *SSL インスペクション*機能を使用すると、暗号化トラフィックのインスペクションを実行せずにブロックしたり、暗号化または復号化されたトラフィックをアクセス コントロールで検査したりできます。暗号化されたセッションをシステムが処理するときは、トラフィックの詳細がログに記録されます。暗号化トラフィックのインスペクションと暗号化セッションのデータ分析を組み合わせることで、暗号化されたアプリケーションやトラフィックをより詳細に把握したり制御したりできます。

システムで TCP 接続での SSL または TLS ハンドシェイクが検出されると、そのトラフィックを復号化できるかどうかが判定されます。復号化できない場合は、設定されたアクションが適用されます。以下のアクションを設定できます。

- 暗号化されたトラフィックをブロックし、オプションで TCP 接続をリセットする。
- 暗号化されたトラフィックを復号化しない。

暗号化されたトラフィックの通過が SSL インスペクション設定で許可される場合、または SSL インスペクションが設定されていない場合は、そのトラフィックがアクセス コントロール ルールによって処理されることに注意してください。ただし、一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルールが少なくなる場合があります。また、暗号化されたペイロードの侵入およびファイル インスペクションは、デフォルトで無効になっています。これにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。詳細については、アクセス コントロール ルールの作成および編集（14-3 ページ）およびSSL プリプロセッサの使用（27-75 ページ）を参照してください。

システムによるトラフィックの復号化が可能な場合は、それ以上のインスペクションなしでトラフィックをブロックするか、復号化されていないトラフィックをアクセス コントロールによって評価するか、あるいは次のいずれかの方法を使用して復号化します。

- 既知の秘密キーを使用して復号化する。外部ホストがネットワーク上のサーバとの SSL ハンドシェイクを開始すると、交換されたサーバ証明書とアプライアンスにアップロード済みのサーバ証明書が照合されます。次に、アップロード済みの秘密キーを使用してトラフィックを復号化します。
- サーバ証明書の再署名によって復号化する。ネットワーク上のホストが外部サーバとの SSL ハンドシェイクを開始すると、交換されたサーバ証明書がアップロード済みの認証局（CA）証明書で再署名されす。次に、アップロード済みの秘密キーを使用してトラフィックを復号化します。

復号化されたトラフィックに対しては、暗号化されていないトラフィックと同じ処理と分析が施されます。これには、ネットワーク、レピュテーション、ユーザ ベースのアクセス コントロール、侵入の検知と防止、高度なマルウェア防御、およびディスカバリが該当します。復号化されたトラフィックのポスト分析をブロックしない場合、トラフィックは再暗号化されて宛先ホストに渡されます。

注 トラフィックのブロックや発信トラフィックの復号化など、いくつかの SSL インスペクション アクションはトラフィックのフローを変更します。これらのアクションを実行できるのは、インラインに配置されたデバイスです。パッシブまたはタップ モードで配置されたデバイスは、トラフィック フローを変更できません。ただし、これらのデバイスでも着信トラフィックを復号化することは可能です。詳細については、例: パッシブ展開でのトラフィック復号化（19-6 ページ）を参照してください。

詳細については、次の項を参照してください。

- SSL インスペクションの要件（19-2 ページ）
- SSL インスペクション アプライアンス展開の分析（19-5 ページ）

SSL インスペクションの要件

ライセンス: 機能によって異なる

サポートされるデバイス: シリーズ 3

SSL インスペクションは、特定のアプライアンス モデルでのみサポートされます。構成時の設定やライセンスに加え、アプライアンスをネットワーク上にどのように展開しているかにより、暗号化トラフィックの制御や復号化に適用できるアクションが異なります。

SSL インスペクションの設定に使用できる機能やアクションは、各自のユーザ ロールに依存します。さまざまな管理者やアナリスト用のユーザ ロールが事前定義されていますが、それ以外にも特殊なアクセス権限を持たせたカスタム ユーザ ロールを作成できます。

SSL インスペクションの一部の機能では、公開キー証明書と秘密キーのペアが必要です。暗号化セッションの特性に応じてトラフィックを復号化したり制御したりするためには、証明書および秘密キーのペアをDefense Centerにアップロードする必要があります。

詳細については、次の項を参照してください。

- SSL インスペクションをサポートするアプライアンスの展開（19-2 ページ）
- SSL インスペクションに必要なライセンスの特定（19-3 ページ）
- カスタム ユーザ ロールによる SSL インスペクション展開の管理（19-4 ページ）
- SSL ルールを設定するために必要な情報の収集（19-4 ページ）

SSL インスペクションをサポートするアプライアンスの展開

ライセンス: すべて

サポートされるデバイス: シリーズ 3

SSL インスペクションにはシリーズ 3 デバイスが必要です。

インライン、ルーティング、スイッチド、またはハイブリッドのインターフェイスで設定および展開されたデバイスでは、トラフィック フローの変更が可能です。これらのデバイスでは、着信および発信トラフィックのモニタリング、ブロック、許可、および復号化を行えます。

パッシブまたはインライン（タップ モード）のインターフェイスで設定および展開されたデバイスでは、トラフィック フローを変更することはできません。これらのデバイスで行えるのは、着信トラフィックのモニタリング、許可、および復号化だけです。パッシブ展開では、一時 Diffie-Hellman（DHE）および楕円曲線 Diffie-Hellman（ECDHE）の暗号スイートを使用した暗号化トラフィックの復号化がサポートされません。

最適な展開タイプを決定するときは、マッピングされたアクション、既存のネットワーク展開、および全体的な要件のリストを確認してください。詳細については、「SSL インスペクション アプライアンス展開の分析（19-5 ページ）」を参照してください。

SSL インスペクションに必要なライセンスの特定

ライセンス： 機能によって異なる

ライセンスによっては、いくつかの条件を組み合わせて暗号化トラフィックの処理方法を決定できます。Defense Centerでのライセンスに関係なく SSL ポリシーを作成できますが、一部の SSL インスペクションに関しては、ポリシーを適用する前に特定のライセンスが必要な機能をターゲット デバイス上で有効にしておく必要があります。Defense Centerでは、ご使用の展開環境でサポートされない機能を示すために、警告アイコン（⚠）および確認ダイアログ ボックスを使用します。警告アイコンの上にポインタを置くと詳細が表示されます。

アクセス コントロール ポリシーの一部として管理対象デバイスに SSL ポリシーを適用すると、SSL ポリシーで復号化されたトラフィックがこのアクセス コントロール ポリシーにより検査されます。アクセス コントロールのライセンスの詳細については、アクセス コントロールのライセンスおよびロール要件（12-2 ページ）を参照してください。

次の表に、アクセス コントロール ポリシーの一部として SSL ポリシーを適用するためのライセンス要件を示します。

表 19-1　SSL インスペクションのライセンスとモデルの要件

SSL ポリシーの機能	ライセンス	サポートされる Defense Center	サポートされるデバイス数
ゾーン、ネットワーク、VLAN、ポート、または SSL 関連の条件に基づいて暗号化トラフィックを処理する	いずれか	いずれか	シリーズ 3
位置情報のデータを使用して暗号化トラフィックを処理する	FireSIGHT	すべて（DC500 を除く）	シリーズ 3
アプリケーションまたはユーザの条件を使用して暗号化トラフィックを処理する	Control	任意：例外として、DC500 ではユーザ制御を実行できません。	シリーズ 3
URL カテゴリおよびレピュテーション データを使用して暗号化トラフィックをフィルタリングする	URL Filtering	すべて（DC500 を除く）	シリーズ 3

カスタム ユーザ ロールによる SSL インスペクション展開の管理

ライセンス：すべて

カスタム ユーザ ロールの管理（61-55 ページ）で説明しているように、カスタム ユーザ ロールを作成して専用のカスタム特権を割り当てることができます。カスタム ユーザ ロールには、メニューベースのアクセス許可およびシステム アクセス許可の任意のセットを割り当てることができます。また、最初から独自に作成したり、事前定義されたユーザ ロールを基に作成したりできます。次の表は、SSL インスペクションの設定と展開を行うためのユーザ権限を決定するロール アクセス許可を示しています。

表 19-2　SSL インスペクション関連のユーザ ロールのアクセス許可

ユーザのアクセス許可	説明
Object Manager	SSL インスペクション関連のオブジェクトを作成、変更、削除できます。
SSL	SSL ポリシーのレポートを生成し、SSL ポリシーまたはポリシー リビジョンの比較ができます。
Modify SSL Policy	SSL ポリシーを表示、作成、変更、削除でき、管理者ルール カテゴリや root ルール カテゴリに含まれない SSL ルールを作成、変更、削除できます。
Modify Administrator Rules	管理者ルール カテゴリの SSL ルールを作成、変更、削除できます。
Modify Root Rules	root ルール カテゴリの SSL ルールを作成、変更、削除できます。
Apply SSL Policy	アクセス コントロール ポリシーの適用時に、関連付けられた SSL ポリシーを適用できます。
アクセス コントロール リスト	アクセス コントロール ポリシーの一覧を表示できます。
アクセス コントロール ポリシーの変更	アクセス コントロール ポリシーに SSL ポリシーを関連付けることができます。
アクセス コントロール ポリシーの適用	SSL ポリシーが関連付けられたアクセス コントロール ポリシーを適用できます。

詳細については、アクセス コントロールのライセンスおよびロール要件（12-2 ページ）を参照してください。

SSL ルールを設定するために必要な情報の収集

ライセンス：機能によって異なる

SSL インスペクションは、サポートする公開キー インフラストラクチャ（PKI）の多くの情報に依存しています。照合ルールの条件を設定するときは、その組織におけるトラフィック パターンについて検討する必要があります。次の表に示す情報を収集しておく必要があります。

表 19-3　SSL ルール条件の設定に必要な情報

一致対象	必要な情報
自己署名サーバ証明書を含む、検出されたサーバ証明書	サーバ証明書
信頼できるサーバ証明書	CA 証明書
検出されたサーバ証明書のサブジェクトまたは発行元	サーバ証明書のサブジェクト DN または発行元 DN

詳細については、SSL ルールを使用したトラフィック復号化の調整（22-1 ページ）を参照してください。

ルールの適用先となる暗号化トラフィックの復号化、ブロック、モニタリングが不要かどうか、または復号化が必要かどうかについて検討します。その結果を、SSL ルールのアクション、復号化できないトラフィックのアクション、および SSL ポリシーのデフォルト アクションに反映させます。トラフィックを復号化する場合は、次の表に示す情報を収集しておく必要があります。

表 19-4　SSL 復号化に必要な情報

復号化の対象	必要な情報
制御対象のサーバへの着信トラフィック	サーバ証明書のファイルと秘密キー ファイルのペア
外部サーバへの発信トラフィック	CA 証明書のファイルと秘密キー ファイルのペア CA 証明書と秘密キーを生成することもできます。

詳細については、ルール アクションを使用した暗号化トラフィックの処理と検査の決定（21-9 ページ）を参照してください。

これらの情報を収集したら、システムにアップロードして、再利用可能なオブジェクトを設定します。詳細については、「再利用可能なオブジェクトの管理（3-1 ページ）」を参照してください。

SSL インスペクション アプライアンス展開の分析

ライセンス： 機能によって異なる

サポートされるデバイス： シリーズ 3

ここでは Life Insurance Example, Inc.（LifeIns）という架空の生命保険会社で使われる複数のシナリオを例にして、同社のプロセス監査で利用されている暗号化トラフィックの SSL インスペクションについて解説します。LifeIns はそのビジネス プロセスに基づいて、以下の展開を計画しています。

- カスタマー サービス部門では、単一のシリーズ 3 管理対象デバイスをパッシブ展開する。
- 契約審査部門では、単一のシリーズ 3 管理対象デバイスをインライン展開する。
- 上記の両方のデバイスを単一のDefense Centerで管理する。

カスタマー サービスのビジネス プロセス

LifeIns はすでに顧客対応用の Web サイトを構築済みです。LifeIns は、保険契約に関する加入見込み客からの暗号化された質問や要求を、この Web サイトおよび電子メールで受け取ります。LifeIns のカスタマー サービスは、これらの要求を処理して 24 時間以内に必要な情報を返信しなければなりません。カスタマー サービスでは、着信するコンタクト メトリックのコレクションを拡張したいと思っています。LifeIns では、すでにカスタマー サービスに対する内部監査用のレビューが確立されています。

また、LifeIns は暗号化された申請書もオンラインで受信します。カスタマー サービス部門は申請書を 24 時間以内に処理し、申請書類のファイルを契約審査部門に送信しなければなりません。カスタマー サービスでは、オンライン フォームからの不正な申請をすべて除外するようにしていますが、この作業が同部門での作業のかなりの部分を占めています。

契約審査部門のビジネス プロセス

LifeIns の契約審査担当者は、Medical Repository Example, LLC（MedRepo）という医療データ リポジトリに、オンラインで暗号化された医療情報要求を送信します。MedRepo はこれらの要求を評価し、LifeIns に暗号化されたレコードを 72 時間以内に送信します。その後は契約審査担当者が申請書類を査定し、保険契約および保険料に関連する判定を送信します。契約審査部門では、そのメトリック コレクションを拡張したいと思っています。

最近、不明な送信元からのスプーフィング（なりすまし）応答が LifeIns に送られてくるようになりました。LifeIns の契約審査担当者はインターネット使用に関する適切なトレーニングを受けていますが、LifeIns の IT 部門はまず、医療応答の形式で送られてくる暗号化トラフィックをすべて分析し、すべてのスプーフィング行為をブロックしたいと思っています。

LifeIns では、経験の浅い契約審査担当者に対して 6 ヵ月のトレーニング期間を設けています。最近、こうした契約審査担当者が MedRepo のカスタマー サービス部門への暗号化された医療規制リクエストの送信を正しく行わない事例がありました。そのため MedRepo から LifeIns に複数の苦情が提出されています。LifeIns は、新任の契約審査担当者用のトレーニング期間を延長し、契約審査担当者から MedRepo への要求についても監査を入れることを計画しています。

詳細については、次の項を参照してください。

- 例：パッシブ展開でのトラフィック復号化（19-6 ページ）
- 例：インライン展開でのトラフィック復号化（19-11 ページ）

例：パッシブ展開でのトラフィック復号化

ライセンス： 機能によって異なる

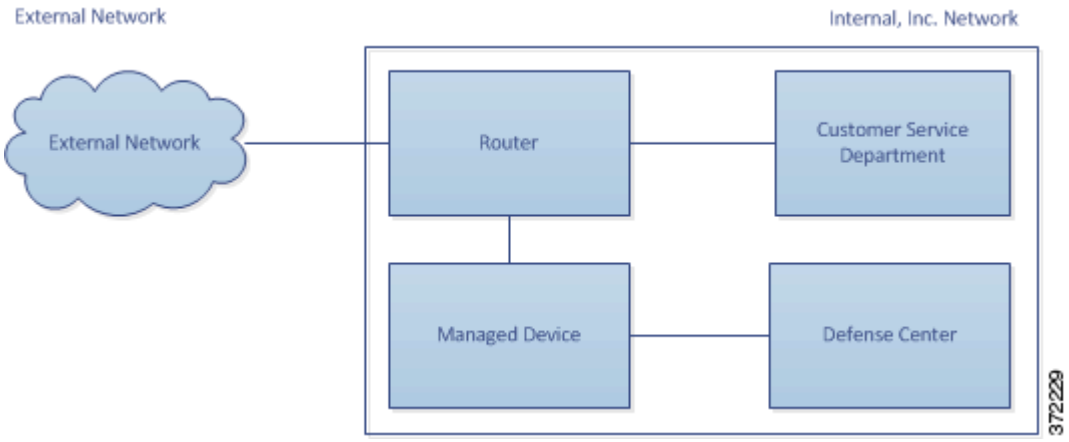
サポートされるデバイス： シリーズ 3

LifeIns のビジネス要件では、カスタマー サービスに次の要求をしています。

- すべての要求と申請書類を 24 時間以内に処理する。
- 着信するコンタクト メトリックのコレクション プロセスを改善する。
- 着信した不正な申請書類を特定して廃棄する。

カスタマー サービス部門では、追加の監査用レビューを必要としません。

LifeIns のカスタマー サービス部門では、管理対象デバイスのパッシブ展開を計画しています。次の図は、LifeIns のパッシブ展開を示しています。



外部ネットワークからのトラフィックは LifeIns のルータに送信されます。ルータはトラフィックをカスタマー サービス部門にルーティングし、検査用にトラフィックのコピーを管理対象デバイスに送信します。

管理するDefense Centerでは、Access Control および SSL Editor のカスタム ロールを持つユーザにより、次の SSL インスペクションの設定を行います。

- カスタマー サービス部門に送信された暗号化トラフィックをすべてログに記録する。
- オンラインの申請フォームからカスタマー サービスに送信された暗号化トラフィックを復号化する。
- カスタマー サービスに送信された他の暗号化トラフィックは、オンライン リクエスト フォームからのトラフィックも含め、すべて復号化しない。

さらに、復号化された申請フォーム トラフィック中に偽の申請データが含まれていないかを検査し、検出された場合はログに記録するためのアクセス コントロールも設定します。

次のシナリオでは、ユーザからカスタマー サービスにオンライン フォームが送信されます。ユーザのブラウザは、サーバとの TCP 接続を確立してから、SSL ハンドシェイクを開始します。管理対象デバイスは、このトラフィックのコピーを受信します。クライアントとサーバが SSL ハンドシェイクを完了することで、暗号化されたセッションが確立されます。システムは、ハンドシェイクと接続の詳細に応じて、接続ログの記録および、暗号化トラフィックのコピーを処理します。

詳細については、次の説明を参照してください。

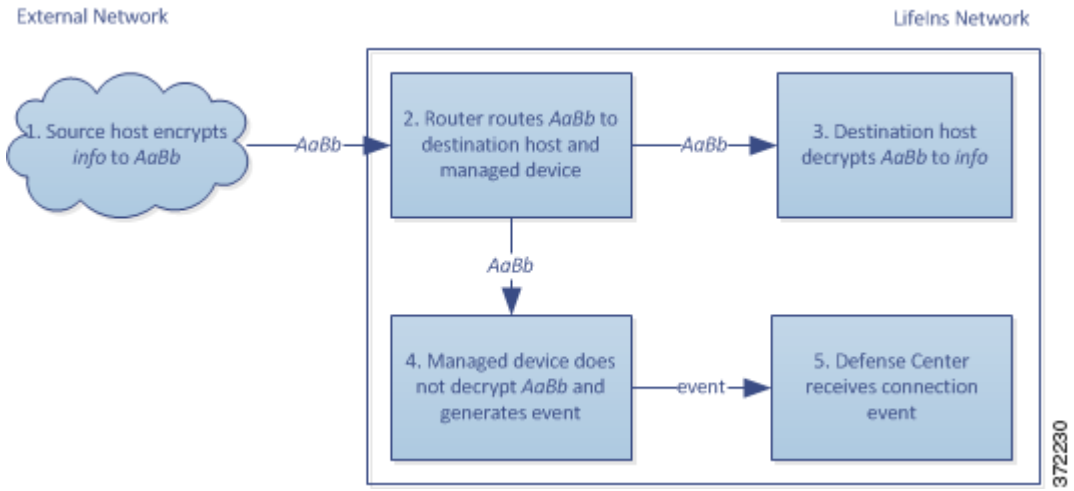
- パッシブ展開で暗号化トラフィックをモニタする（19-7 ページ）
- パッシブ展開で暗号化トラフィックを復号化しない（19-8 ページ）
- パッシブ展開で暗号化トラフィックを秘密キーで検査する（19-9 ページ）

パッシブ展開で暗号化トラフィックをモニタする

ライセンス： すべて

サポートされるデバイス： シリーズ 3

システムは、カスタマー サービスに送信されるすべての SSL 暗号化トラフィックについて、接続のログを記録します。次の図は、暗号化トラフィックをシステムがモニタする状況を示しています。



次のステップが実行されます。

1. ユーザがプレーン テキストの要求（`info`）を送信します。クライアントがこれを暗号化（`AaBb`）し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、管理対象デバイスにそのトラフィックのコピーを送信します。
3. カスタマー サービス部門のサーバが、暗号化された情報の要求（`AaBb`）を受信し、これをプレーン テキスト（`info`）に復号化します。
4. 管理対象デバイスはトラフィックを復号化しません。

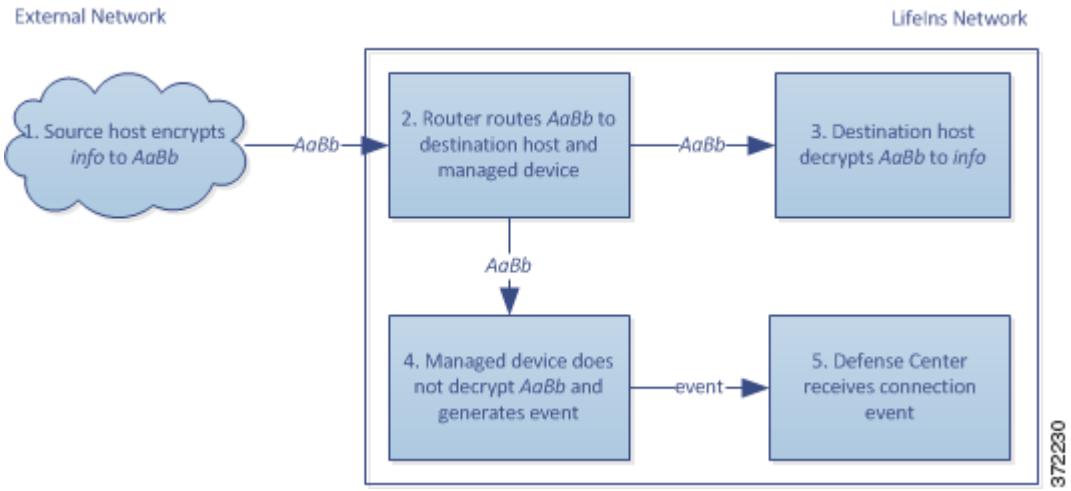
   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行し、これを許可します。セッション終了後、デバイスは接続イベントを生成します。
5. Defense Centerが接続イベントを受信します。

パッシブ展開で暗号化トラフィックを復号化しない

ライセンス： すべて

サポートされるデバイス： シリーズ 3

保険契約に関する要求を含むすべての SSL 暗号化トラフィックは復号化されずに許可され、接続のログが記録されます。次の図は、追加の検査を行わずに暗号化トラフィックを許可する状況を示しています。



次のステップが実行されます。

1. ユーザがプレーン テキストの要求（`info`）を送信します。クライアントがこれを暗号化（`AaBb`）し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、管理対象デバイスにそのトラフィックのコピーを送信します。
3. カスタマー サービス部門のサーバが、暗号化された情報の要求（`AaBb`）を受信し、これをプレーン テキスト（`info`）に復号化します。
4. 管理対象デバイスはトラフィックを復号化しません。

   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行し、これを許可します。セッション終了後、デバイスは接続イベントを生成します。
5. Defense Centerが接続イベントを受信します。

パッシブ展開で暗号化トラフィックを秘密キーで検査する

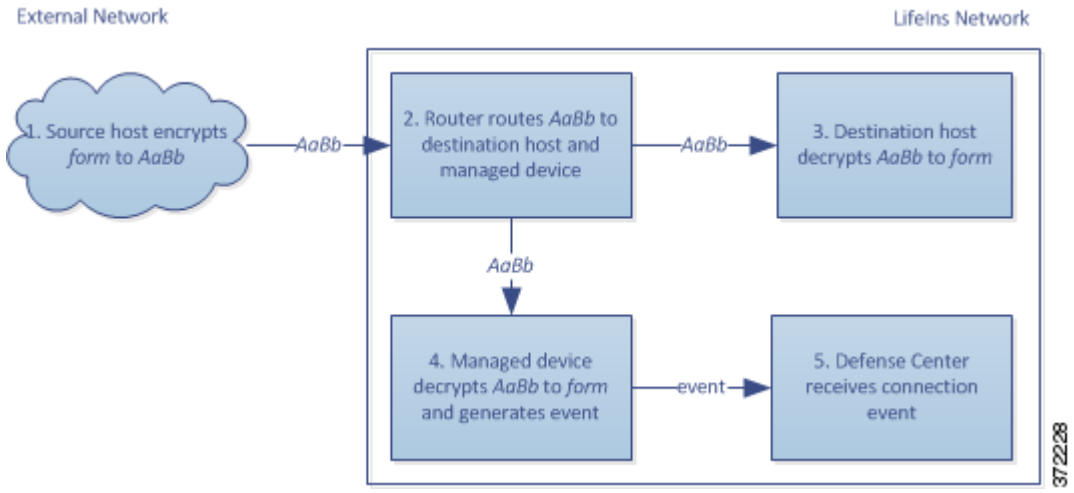
ライセンス： すべて

サポートされるデバイス： シリーズ 3

申請フォームのデータを含むすべての SSL 暗号化トラフィックは復号化され、接続のログが記録されます。

注　パッシブ展開の場合、DHE または ECDHE 暗号スイートで暗号化されたトラフィックは、既知の秘密キーを使って復号化することはできません。

有効な申請フォームの情報を含むトラフィックについては、接続のログが記録されます。次の図は、既知の秘密キーによりトラフィックを復号化する状況を示しています。

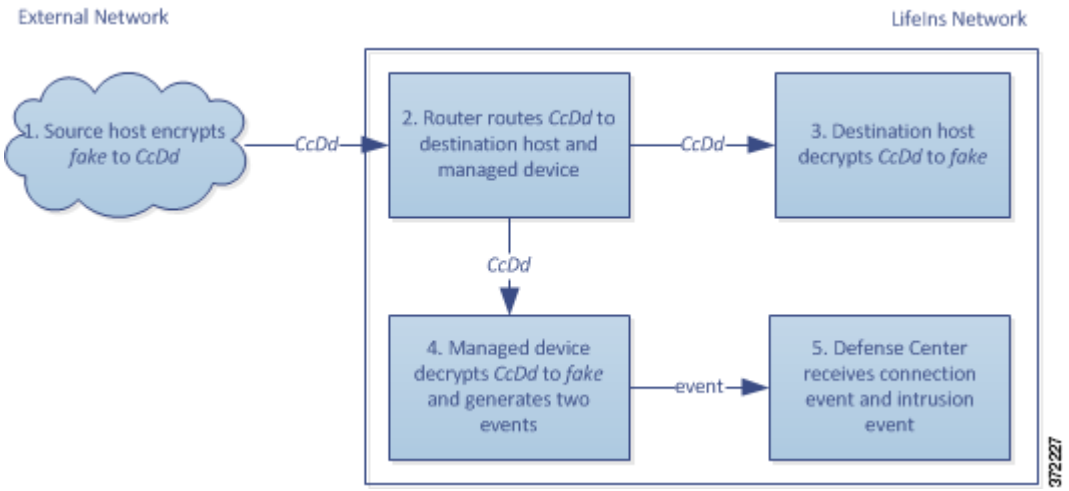


次のステップが実行されます。

1. ユーザがプレーン テキストの要求（`form`）を送信します。クライアントがこれを暗号化（`AaBb`）し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、管理対象デバイスにそのトラフィックのコピーを送信します。
3. カスタマー サービス部門のサーバが、暗号化された情報の要求（`AaBb`）を受信し、これをプレーン テキスト（`form`）に復号化します。
4. 管理対象デバイスは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、暗号化トラフィックをプレーン テキスト（`form`）に復号化します。

   アクセス コントロール ポリシーは、復号化されたトラフィックの処理を継続します。偽の申請書であることを示す情報は検出されません。セッション終了後、デバイスは接続イベントを生成します。
5. Defense Centerは、暗号化および復号化されたトラフィックの情報とともに、接続イベントを受信します。

これに対し、復号化されたトラフィックに偽の申請データが含まれていた場合、接続および偽のデータについてのログが記録されます。次の図は、既知の秘密キーにより、偽の申請データを含んでいる着信トラフィックを復号化する状況を示しています。



次のステップが実行されます。

1. ユーザがプレーン テキストの要求（`fake`）を送信します。クライアントがこれを暗号化（`CcDd`）し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、管理対象デバイスにそのトラフィックのコピーを送信します。
3. カスタマー サービス部門のサーバが、暗号化された情報の要求（`CcDd`）を受信し、これをプレーン テキスト（`fake`）に復号化します。
4. 管理対象デバイスは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、暗号化トラフィックをプレーン テキスト（`fake`）に復号化します。

   アクセス コントロール ポリシーは、復号化されたトラフィックの処理を継続して、偽の申請書であることを示す情報を検出します。デバイスが侵入イベントを生成します。セッション終了後、デバイスは接続イベントを生成します。
5. Defense Centerは、暗号化および復号化されたトラフィックの情報とともに、接続イベントおよび偽の申請データの侵入イベントを受信します。

例：インライン展開でのトラフィック復号化

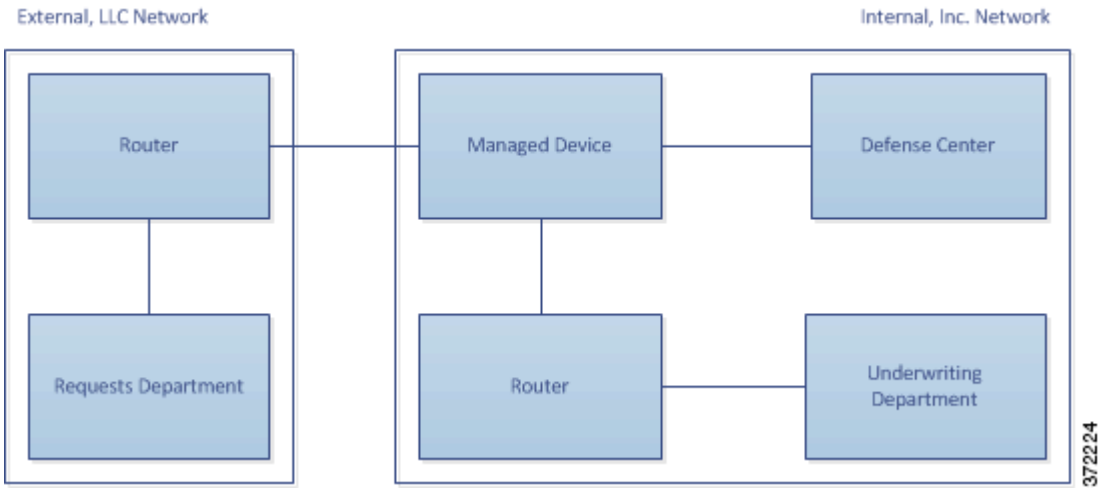
ライセンス： 機能によって異なる

サポートされるデバイス： シリーズ 3

LifeIns のビジネス要件では、契約審査部門に次の要求をしています。

- 新採用および経験の浅い契約審査担当者を監査し、MedRepo への情報要求が適切なすべての規則に準じていることを検証する。
- その契約審査によるメトリック コレクション プロセスを改善する。
- MedRepo が送信元と思われるすべての要求を調査し、スプーフィング行為を排除する。
- 契約審査部門から MedRepo のカスタマー サービス部門へのすべての不適切な規制要求を排除する。
- 経験豊富な契約審査担当者は監査しない。

LifeIns の契約審査部門では、デバイスのインライン展開を計画しています。次の図は、LifeIns のインライン展開を示しています。



MedRepo のネットワークからのトラフィックは、MedRepo のルータに流されます。そこから LifeIns のネットワークにトラフィックがルーティングされます。管理対象デバイスはトラフィックを受信し、許可されたトラフィックを LifeIns のルータに転送して、管理している Defense Centerにイベントを送信します。LifeIns のルータは、トラフィックを宛先ホストにルーティングします。

管理するDefense Centerでは、Access Control および SSL Editor のカスタム ロールを持つユーザにより、次の SSL インスペクションの設定を行います。

- 契約審査部門に送信された暗号化トラフィックをすべてログに記録する。
- LifeIns の契約審査部門から MedRepo のカスタマー サービス部門に不正に送信された暗号化トラフィックをすべてブロックする。
- MedRepo から LifeIns の契約審査部門宛て、および LifeIns の経験の浅い契約審査担当者から MedRepo のリクエスト部門宛てに送信される暗号化トラフィックをすべて復号化する。
- 経験豊富な契約審査担当者から送信される暗号化トラフィックは復号化しない。

さらに、カスタムの侵入ポリシーと以下の設定を使用して、復号化トラフィックを検査するアクセス コントロールを設定します。

- 復号化トラフィックでスプーフィング行為が検出された場合はそのトラフィックをブロックし、スプーフィング行為をログに記録する。
- 規制に準拠しない情報を含んでいる復号化トラフィックをブロックし、不適切な情報をログに記録する。
- 他の暗号化および復号化されたトラフィックをすべて許可する。

許可された復号化トラフィックは、再暗号化されて宛先ホストに転送されます。

次のシナリオでは、ユーザが情報をオンラインでリモート サーバに送信します。ユーザのブラウザは、サーバとの TCP 接続を確立してから、SSL ハンドシェイクを開始します。管理対象デバイスはこのトラフィックを受信し、ハンドシェイクと接続の詳細に応じて、システムが接続ログの記録およびトラフィックの処理をします。システムがトラフィックをブロックした場合、TCP 接続も切断されます。トラフィックがブロックされない場合、クライアントとサーバが SSL ハンドシェイクを完了することで、暗号化されたセッションが確立されます。

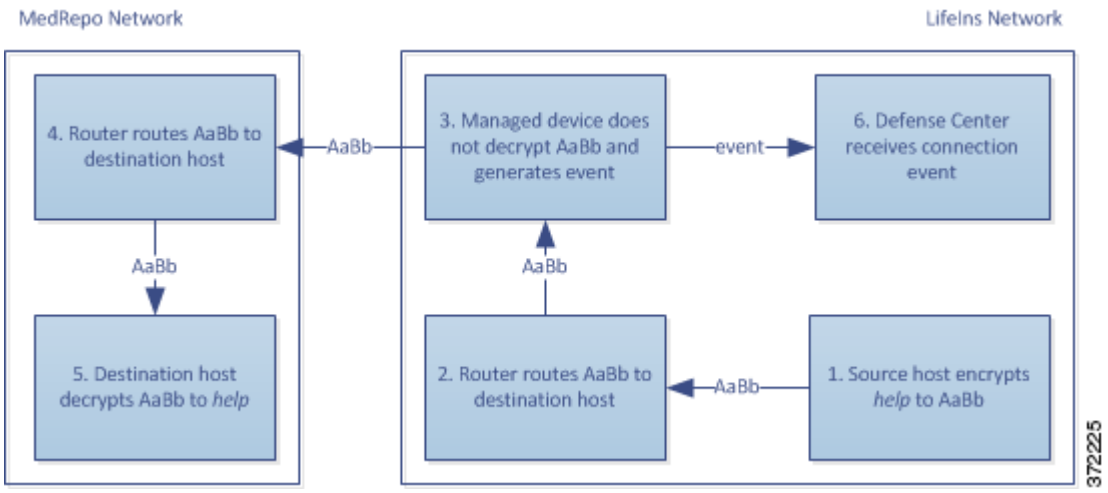
詳細については、次の説明を参照してください。

インライン展開で暗号化トラフィックをモニタする

ライセンス： すべて

サポートされるデバイス： シリーズ 3

契約審査部門で送受信されるすべての SSL 暗号化トラフィックについて、接続のログが記録されます。次の図は、暗号化トラフィックをシステムがモニタする状況を示しています。



次のステップが実行されます。

1. ユーザがプレーン テキストの要求（`help`）を送信します。クライアントがこれを暗号化（`AaBb`）し、MedRepo のリクエスト部門のサーバに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、リクエスト部門のサーバにルーティングします。
3. 管理対象デバイスはトラフィックを復号化しません。

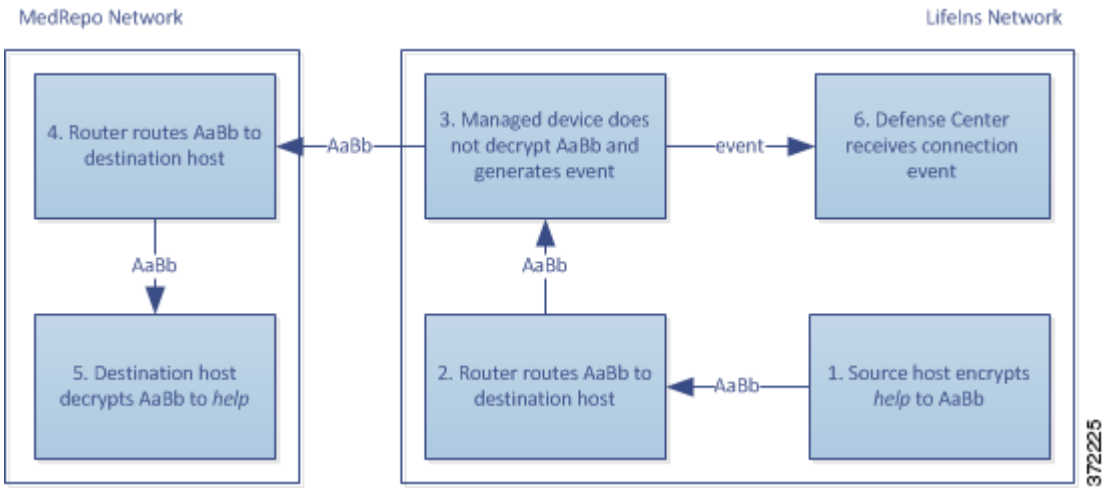
   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行してこれを許可し、セッション終了後に接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
5. 契約審査部門のサーバは、暗号化された情報の要求（`AaBb`）を受信し、これをプレーン テキスト（`help`）に復号化します。
6. Defense Centerが接続イベントを受信します。

インライン展開で特定ユーザからの暗号化トラフィックを許可する

ライセンス： Control

サポートされるデバイス： シリーズ 3

経験豊富な契約審査担当者から送信されるすべての SSL 暗号化トラフィックは復号化されずに許可され、接続のログが記録されます。次の図は、暗号化トラフィックをシステムが許可する状況を示しています。



次のステップが実行されます。

1. ユーザがプレーン テキストの要求（`help`）を送信します。クライアントがこれを暗号化（`AaBb`）し、MedRepo のリクエスト部門のサーバに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、リクエスト部門のサーバにルーティングします。
3. 管理対象デバイスはこのトラフィックを復号化しません。

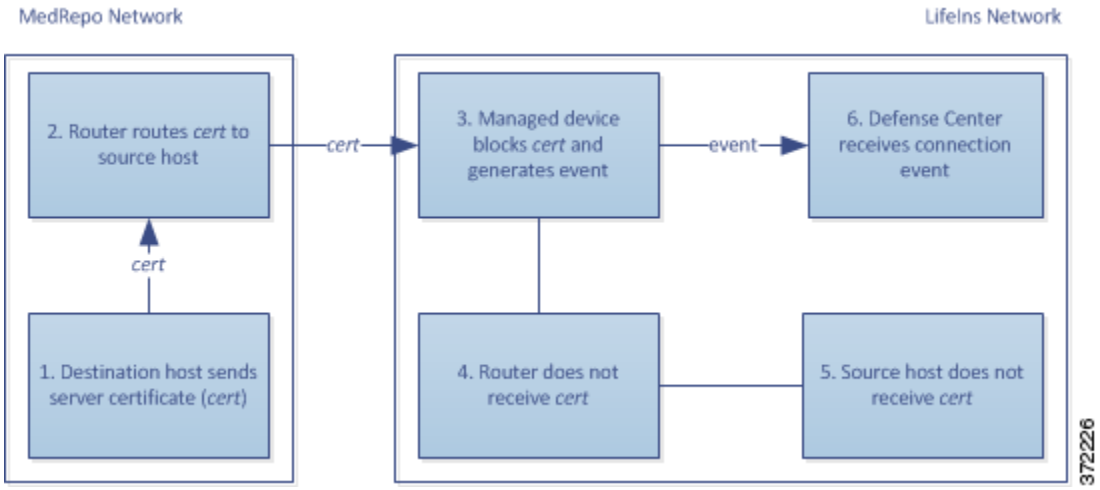
   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行してこれを許可し、セッション終了後に接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
5. リクエスト部門のサーバは、暗号化された情報の要求（`AaBb`）を受信し、これをプレーン テキスト（`help`）に復号化します。
6. Defense Centerが接続イベントを受信します。

インライン展開で暗号化トラフィックをブロックする

ライセンス： すべて

サポートされるデバイス： シリーズ 3

LifeIns の契約審査部門から MedRepo のカスタマー サービス部門に不正に送信されるすべての SMTPS 電子メール トラフィックは SSL ハンドシェイク時にブロックされ、追加の検査なしで接続のログが記録されます。次の図は、暗号化トラフィックをシステムがブロックする状況を示しています。



次のステップが実行されます。

1. カスタマー サービス部門のサーバは、クライアント ブラウザから SSL ハンドシェイクの確立要求を受信すると、SSL ハンドシェイクの次のステップとして、サーバ証明書（`cert`）を LifeIns の契約審査担当者に送信します。
2. MedRepo のルータが証明書を受信し、これを LifeIns の契約審査担当者にルーティングします。
3. 管理対象デバイスは追加の検査を行わずにトラフィックをブロックし、TCP 接続を終了します。これにより、接続イベントが生成されます。
4. 内部ルータは、ブロックされたトラフィックを受信しません。
5. 契約審査担当者は、ブロックされたトラフィックを受信しません。
6. Defense Centerが接続イベントを受信します。

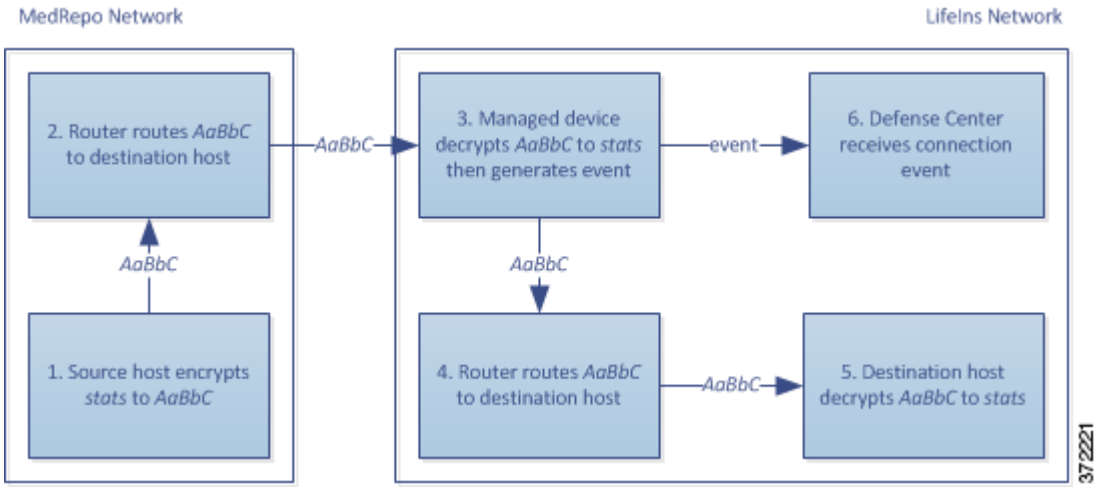
インライン展開で暗号化トラフィックを秘密キーで検査する

ライセンス： すべて

サポートされるデバイス： シリーズ 3

MedRepo から LifeIns の契約審査部門に送信されるすべての SSL 暗号化トラフィックは復号化され、接続のログが記録されます。復号化には、アップロードされたサーバ秘密キーを使って取得されたセッション キーが使用されます。正規のトラフィックは許可され、再暗号化されて契約審査部門に送信されます。

次の図は、既知の秘密キーを使用して暗号化トラフィックを復号化した後、アクセス コントロールを使用してトラフィックを検査して、復号化されたトラフィックを許可する状況を示しています。

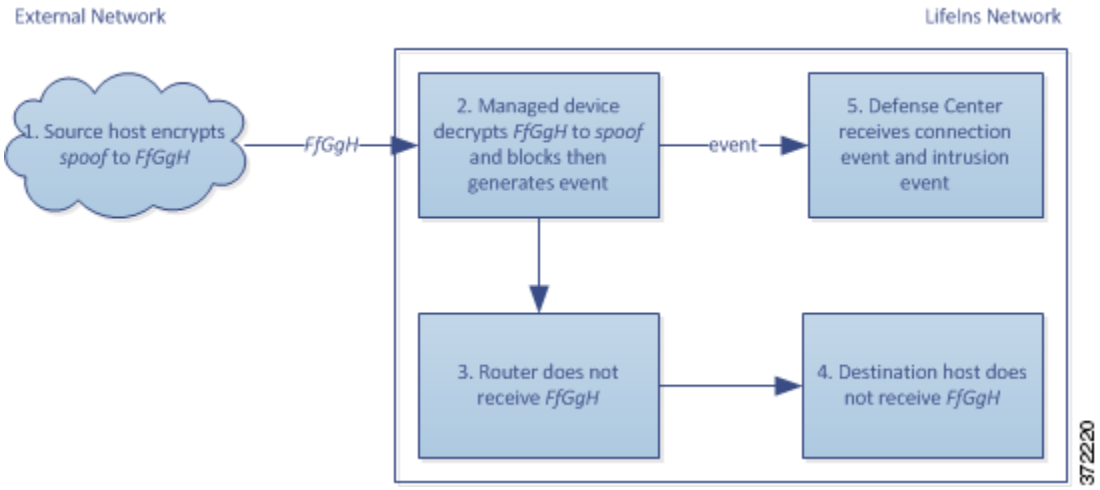


次のステップが実行されます。

1. ユーザがプレーン テキストの要求（stats）を送信します。クライアントがこれを暗号化（AaBbC）し、契約審査部門のサーバに暗号化トラフィックを送信します。
2. 外部ルータがトラフィックを受信し、これを契約審査部門のサーバにルーティングします。
3. 管理対象デバイスは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（stats）に復号化します。

   アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号化トラフィックの処理を継続します。スプーフィング行為は検出されません。デバイスは暗号化トラフィック（AaBbC）を転送し、セッション終了後に接続イベントを生成します。
4. 内部ルータがトラフィックを受信し、これを契約審査部門のサーバにルーティングします。
5. 契約審査部門のサーバは、暗号化された情報（AaBbC）を受信し、これをプレーン テキスト（stats）に復号化します。
6. Defense Centerは、暗号化および復号化されたトラフィックの情報とともに、接続イベントを受信します。

これに対し、スプーフィング行為の復号化トラフィックはすべてドロップされ、接続およびスプーフィング行為についてのログが記録されます。次の図は、既知の秘密キーを使用して暗号化トラフィックを復号化した後、アクセス コントロール ポリシーを使用してトラフィックを検査して、復号化されたトラフィックをブロックする状況を示しています。



次のステップが実行されます。

1. ユーザがプレーン テキストの要求（spoof）を送信しますが、このトラフィックは改変されており、発信元が MedRepo, LLC であるかのように偽装されています。クライアントがこれを暗号化（FfGgH）し、契約審査部門のサーバに暗号化トラフィックを送信します。
2. 管理対象デバイスは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（spoof）に復号化します。

   アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号化トラフィックの処理を継続し、スプーフィング行為を検出します。デバイスはトラフィックをブロックし、侵入イベントを生成します。セッション終了後、接続イベントを生成します。
3. 内部ルータは、ブロックされたトラフィックを受信しません。
4. 契約審査部門のサーバは、ブロックされたトラフィックを受信しません。
5. Defense Centerは、暗号化および復号化されたトラフィックの情報とともに、接続イベントおよびスプーフィング行為の侵入イベントを受信します。

インライン展開で特定ユーザの暗号化トラフィックを再署名証明書で検査する

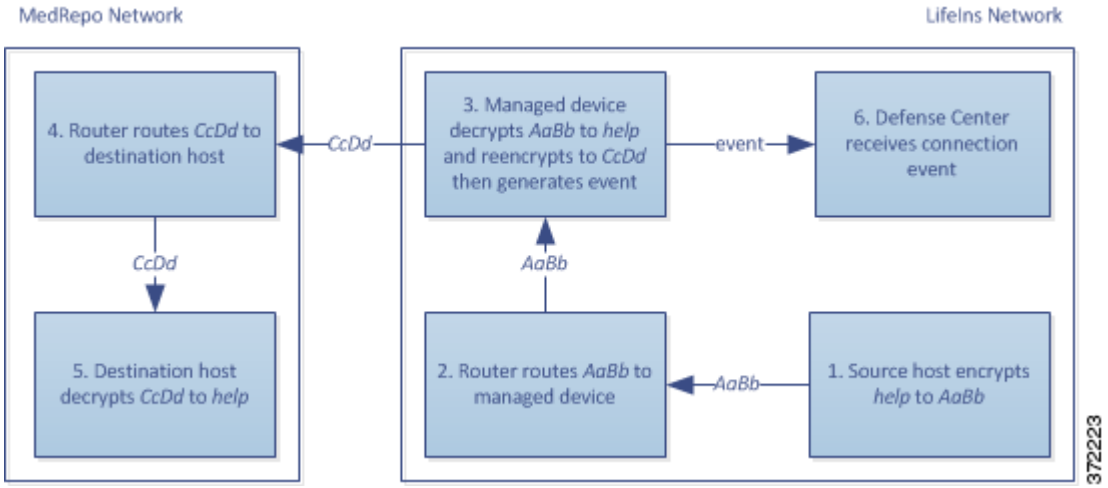
ライセンス： Control

サポートされるデバイス： シリーズ 3

新任および経験の浅い契約審査担当者から MedRepo のリクエスト部門に送信されるすべての SSL 暗号化トラフィックは復号化され、接続のログが記録されます。復号化には、再署名されたサーバ証明書を使って取得されたセッション キーが使用されます。正規のトラフィックは許可され、再暗号化されて MedRepo に送信されます。

注　インライン展開においてサーバ証明書の再署名によりトラフィックを復号化する場合、デバイスは中間者（man-in-the-middle）として機能します。ここでは 2 つの SSL セッションが作成され、1 つはクライアントと管理対象デバイスの間、もう 1 つは管理対象デバイスとサーバの間で使用されます。その結果、暗号セッションの詳細はセッションごとに異なります。

次の図は、再署名されたサーバ証明書と秘密キーを使用して暗号化トラフィックを復号化した後、アクセス コントロールを使用してトラフィックを検査して、復号化されたトラフィックを許可する状況を示しています。



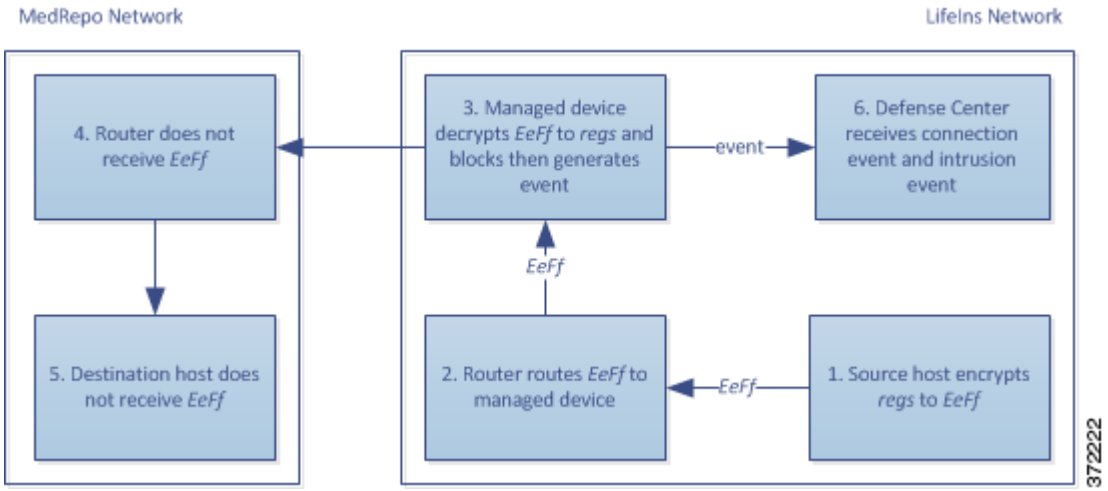
次のステップが実行されます。

1. ユーザがプレーン テキストの要求（help）を送信します。クライアントがこれを暗号化（AaBb）し、リクエスト部門のサーバに暗号化トラフィックを送信します。
2. 内部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
3. 管理対象デバイスは、再署名されたサーバ証明書と秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（help）に復号化します。

   アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号化トラフィックの処理を継続します。不適切な要求は検出されません。デバイスはトラフィックを再暗号化（CcDd）して、送信を許可します。セッション終了後、接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
5. リクエスト部門のサーバは、暗号化された情報（CcDd）を受信し、これをプレーン テキスト（help）に復号化します。
6. Defense Centerは、暗号化および復号化されたトラフィックの情報とともに、接続イベントを受信します。

注　再署名されたサーバ証明書で暗号化されたトラフィックにより、信頼できない証明書についての警告がクライアントのブラウザに表示されます。この問題を避けるには、組織のドメイン ルートにある信頼できる証明書ストアまたはクライアントの信頼できる証明書ストアに CA 証明書を追加します。

これに対し、規制要件を満たさない情報を含んでいる復号化トラフィックは、すべてドロップされます。接続および非準拠情報についてのログが記録されます。次の図は、再署名されたサーバ証明書と秘密キーを使用して暗号化トラフィックを復号化した後、アクセス コントロール ポリシーを使用してトラフィックを検査して、復号化されたトラフィックをブロックする状況を示しています。



次のステップが実行されます。

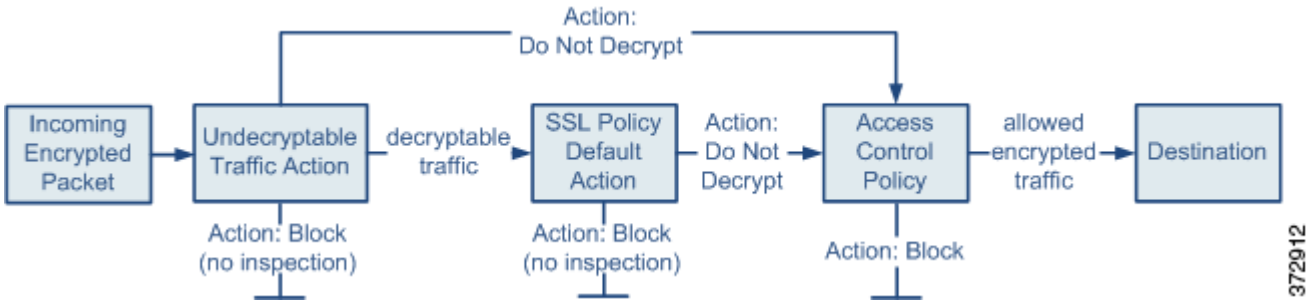
1. ユーザが規制要件に準拠していない要求をプレーン テキスト（`regs`）で送信します。クライアントがこれを暗号化（`EeFf`）し、リクエスト部門のサーバに暗号化トラフィックを送信します。
2. 内部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
3. 管理対象デバイスは、再署名されたサーバ証明書と秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（`regs`）に復号化します。

   アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号化トラフィックの処理を継続し、不適切な要求を検出します。デバイスはトラフィックをブロックし、侵入イベントを生成します。セッション終了後、接続イベントを生成します。
4. 外部ルータは、ブロックされたトラフィックを受信しません。
5. リクエスト部門のサーバは、ブロックされたトラフィックを受信しません。
6. Defense Centerは、暗号化および復号化されたトラフィックの情報とともに、接続イベントおよび不適切な要求の侵入イベントを受信します。

SSL ポリシー クイック スタート ガイド

*SSL ポリシー*は、ネットワーク上の暗号化トラフィックをシステムがどのように処理するかを決定します。SSL ポリシーを、1 つまたは複数設定できます。SSL ポリシーをアクセス コントロール ポリシーに関連付け、そのアクセス コントロール ポリシーを管理対象デバイスに適用します。デバイスで TCP ハンドシェイクが検出されると、アクセス コントロール ポリシーは最初にトラフィックの処理と検査をします。次に TCP 接続上で SSL 暗号化セッションが識別された場合は、SSL ポリシーが引き継いで、暗号化トラフィックの処理および復号化を行います。シリーズ 3 デバイスで同時に適用できる SSL ポリシーは 1 つだけです。

最も単純な SSL ポリシーは、次の図のように、単一のデフォルト アクションで暗号化トラフィックを処理するように適用先のデバイスに指示します。デフォルト アクションは、それ以上のインスペクションなしで復号可能なトラフィックをブロックするか、あるいは復号可能なトラフィックを復号化されていない状態でアクセス コントロールによって検査するように設定できます。システムは、暗号化されたトラフィックを許可するか、またはブロックできます。デバイスは復号化できないトラフィックを検出すると、トラフィックをそれ以上のインスペクションなしでブロックするか、あるいは復号化しないままにして、アクセス コントロールによる検査を行います。



この章では、単純な SSL ポリシーを作成して適用する方法について説明します。また、編集、更新、比較などの SSL ポリシー管理の基本情報も含まれています。詳細については、以下を参照してください。

- 基本 SSL ポリシーの作成（20-2 ページ）
- SSL ポリシーの編集（20-7 ページ）
- アクセス コントロールを使用した復号化設定の適用（20-9 ページ）
- 現在のトラフィック復号化設定のレポートの生成（20-10 ページ）
- SSL ポリシーの比較（20-11 ページ）

より複雑な SSL ポリシーでは、各種の復号化できないトラフィックをさまざまなアクションで処理することが可能であり、認証局（CA）が証明書を発行したか、または暗号化証明書を信頼するかどうかに応じてトラフィックを制御したり、SSL ルールを使ってきめ細かな暗号化トラフィックの制御およびログの記録を行ったりできます。これらのルールには、単純なものや複雑なものがあり、複数の基準を使用して暗号化トラフィックの照合および検査を行います。基本的な SSL ポリシーの作成後は、個々の展開環境に応じた調整法の詳細について、次の章を参照してください。

- 「再利用可能なオブジェクトの管理（3-1 ページ）」では、再利用可能な公開キー インフラストラクチャ（PKI）オブジェクトおよびその他の SSL インスペクション関連オブジェクトを設定して、トラフィックの復号化や暗号化トラフィックの制御を強化する方法を説明しています。
- 「ネットワーク トラフィックの接続のロギング（38-1 ページ）」では、復号可能および復号化できない暗号化トラフィックに対するログの設定法を説明しています。
- 「アクセス コントロールを使用した復号化設定の適用（20-9 ページ）」では、SSL ポリシーをアクセス コントロール ポリシーに関連付ける方法を説明しています。
- 「アクセス コントロール ポリシーの開始（12-1 ページ）」では、アクセス コントロール ポリシーをデバイスに適用する方法を説明しています。
- 「アクセス コントロール ルールを使用したトラフィック フローの調整（14-1 ページ）」では、復号化トラフィックを検査するアクセス コントロール ルールの設定法を説明しています。
- 「SSL ルール クイック スタート ガイド（21-1 ページ）」では、暗号化トラフィックの処理とログを記録する SSL ルールの設定法を説明しています。
- 「SSL ルールを使用したトラフィック復号化の調整（22-1 ページ）」では、特定の暗号化トラフィックと SSL ルール条件の一致度を向上させる設定法を説明しています。

基本 SSL ポリシーの作成

ライセンス： すべて

サポートされるデバイス： シリーズ 3

新しい SSL ポリシーを作成するために最低限必要な操作は、そのポリシーに一意の名前を付けて、ポリシーのデフォルト アクションを指定することです。新しいポリシーのデフォルト アクションを選択する際には、次のオプションがあります。

- **Do not decrypt** は Do not decrypt デフォルト アクションでポリシーを作成します。
- **Block** は Block デフォルト アクションでポリシーを作成します。
- **Block with reset** は Block with reset デフォルト アクションでポリシーを作成します。

デフォルト アクションは、SSL ポリシーを作成した後で変更できます。デフォルト アクションの選択に関するガイダンスについては、暗号化トラフィックのデフォルトの処理と検査の設定（20-4 ページ）を参照してください。

新しい SSL ポリシーにはシステムが復号化できないトラフィックのデフォルト アクションも含まれています。ユーザが復号化できないトラフィックに対して選択したデフォルト アクションを継承する、ブロックする、あるいはトラフィックを復号化せずアクセス コントロールで検査するなどのアクションです。復号化できないトラフィックに対するアクションは、SSL ポリシーの作成後に変更できます。復号化できないトラフィック アクションの選択に関するガイダンスについては、復号化できないトラフィックのデフォルト処理の設定（20-5 ページ）を参照してください。

SSL ポリシーのページ（[Policies] > [SSL]）で、オプションの説明とともに、現在のすべての SSL ポリシーを名前別に表示できます。このページのオプションを使用して、さまざまな操作を行うことができます。具体的には、ポリシーの比較、新規ポリシーの作成、ポリシーのコピー、各ポリシーに最近保存された設定をすべてリストするレポートの表示、ポリシーの編集、ポリシーの削除などです。

ヒント　展開環境の他のDefense Centerに対して、SSL ポリシーをエクスポート/インポートすることもできます。詳細については、「設定のインポートおよびエクスポート（A-1 ページ）」を参照してください。

次の表で、SSL ポリシーのページでポリシーを管理するために実行可能なアクションについて説明します。

表 20-1　SSL ポリシー管理アクション

目的	操作
新しい SSL ポリシーを作成する	[New Policy] をクリックします。詳細については、「基本 SSL ポリシーの作成（20-2 ページ）」を参照してください。
既存の SSL ポリシーの設定を変更する	編集アイコン（ ）をクリックします。詳細については、「SSL ポリシーの編集（20-7 ページ）」を参照してください。
SSL ポリシーを比較する	[Compare Policies] をクリックします。詳細については、「SSL ポリシーの比較（20-11 ページ）」を参照してください。
SSL ポリシーをコピーする	コピー アイコン（ ）をクリックします。コピーしたポリシーの編集の詳細については、SSL ポリシーの編集（20-7 ページ）を参照してください。
SSL ポリシーの現在の設定を示す PDF レポートを表示する	レポート アイコン（ ）をクリックします。詳細については、「現在のトラフィック復号化設定のレポートの生成（20-10 ページ）」を参照してください。
SSL ポリシーを削除する	アイコン（ ）をクリックし、[OK] をクリックします。続行するかどうかを尋ねるプロンプトで、ポリシー内に別のユーザの未保存の変更が存在するかどうかも通知されます。

SSL ポリシーを作成する手順：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [SSL] を選択します。

[SSL Policy] ページが表示されます。

ステップ 2　[New Policy] をクリックします。

[New SSL Policy] ポップアップ ウィンドウが表示されます。

ステップ 3　[Name] に一意のポリシー名を入力し、オプションで [Description] にポリシーの説明を入力します。

印刷可能なすべての文字を使用できます。これにはスペースと特殊文字も含まれます。

ステップ 4　[Default Action] で、デフォルト アクションを指定します。

選択したデフォルト アクションは、SSL ポリシーの作成後に変更できることに注意してください。詳細については、「暗号化トラフィックのデフォルトの処理と検査の設定（20-4 ページ）」を参照してください。

ステップ 5　[Save] をクリックします。

[SSL Policy Editor] ページが表示されます。詳細については、「SSL ポリシーの編集（20-7 ページ）」を参照してください。

暗号化トラフィックのデフォルトの処理と検査の設定

ライセンス： すべて

サポートされるデバイス： シリーズ 3

SSL ポリシーのデフォルト アクションは、ポリシーのモニタ以外のルールと一致しない復号可能な暗号化トラフィックについてシステムがどのように処理するかを決定します。SSL ルールがまったく含まれない SSL ポリシーを適用する場合、ネットワーク上のすべての復号可能トラフィックの処理方法を、デフォルト アクションが決定します。システムが復号化できない暗号化トラフィックを処理する方法の詳細については、復号化できないトラフィックのデフォルト処理の設定（20-5 ページ）を参照してください。

次の表に、選択可能なデフォルト アクションとそれが暗号化トラフィックに対して行う処理をリストします。デフォルト アクションでブロックされた暗号化トラフィックに対しては、システムはいかなる種類のインスペクションも行わないことに注意してください。

:

表 20-2　SSL ポリシーのデフォルト アクション

デフォルト アクション	暗号化トラフィックに対して行う処理
ブロック	それ以上のインスペクションは行わずに SSL セッションをブロックする。
リセット付きブロック	それ以上のインスペクションは行わずに SSL セッションをブロックし、TCP 接続をリセットする。
復号化しない	アクセス コントロールを使用して暗号化トラフィックを検査する。

SSL ポリシーを最初に作成する場合、デフォルト アクションによって処理される接続のログは、デフォルトでは無効化されています。デフォルト アクションと同様に、この設定もポリシー作成後に変更できます。

次の手順で、ポリシーの編集の際に SSL ポリシーのデフォルト アクションを設定する方法を説明します。SSL ポリシーを編集するための詳細な手順についてはSSL ポリシーの編集（20-7 ページ）を参照してください。

SSL ポリシーのデフォルト アクションを設定する方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [SSL] を選択します。

SSL ポリシーのページが表示されます。

ステップ 2　設定する SSL ポリシーの横にある編集アイコン（）をクリックします。

SSL ポリシー エディタが表示されます。

ステップ 3　[Default Action] を選択します。詳細については、SSL ポリシーのデフォルト アクションの表を参照してください。

ステップ 4　「SSL ルールによる復号可能接続のロギング（38-14 ページ）」の説明に従って、デフォルト アクションのロギング オプションを設定します。

ステップ 5　[Save] をクリックします。

[SSL Policy Editor] ページが表示されます。詳細については、「SSL ポリシーの編集（20-7 ページ）」を参照してください。

復号化できないトラフィックのデフォルト処理の設定

ライセンス： すべて

サポートされるデバイス： シリーズ 3

システムによる復号化や検査ができない特定タイプの暗号化トラフィックの処理については、SSL ポリシー レベルで、復号化できないトラフィック用のアクションを設定できます。SSL ルールがまったく含まれない SSL ポリシーを適用する場合、ネットワーク上のすべての復号化できない暗号化トラフィックの処理方法は、復号化できないトラフィック用のアクションが決定します。

復号化できないトラフィックのタイプによって、次の選択ができます。

- 接続をブロックする。
- 接続をブロックした後でリセットする。
- アクセス コントロールを使用して暗号化トラフィックを検査する。
- SSL ポリシーのデフォルト アクションを継承する。

次の表に、復号化できないトラフィックのタイプを示します。

表 20-3　復号化できないトラフィック タイプ

タイプ	説明	デフォルト アクション	利用可能なアクション
圧縮されたセッション	SSL セッションはデータ圧縮メソッドを適用します。	デフォルト アクションを継承	復号化しない ブロック リセット付きブロック デフォルト アクションを継承
SSLv2 セッション	セッションは SSL バージョン 2 で暗号化されます。 トラフィックが復号可能となるのは、クライアントの HELLO メッセージが SSL 2.0 で、送信トラフィックの残りが SSL 3.0 である場合なので注意してください。	デフォルト アクションを継承	復号化しない ブロック リセット付きブロック デフォルト アクションを継承

表 20-3　復号化できないトラフィック タイプ

タイプ	説明	デフォルト アクション	利用可能なアクション
不明な暗号スイート	システムが認識できない暗号スイートです。	デフォルト アクションを継承	復号化しない ブロック リセット付きブロック デフォルト アクションを継承
サポートされていない暗号スイート	検出された暗号スイートに基づく復号化を、システムはサポートしていません。	デフォルト アクションを継承	復号化しない ブロック リセット付きブロック デフォルト アクションを継承
セッションが未キャッシュ	SSL セッションでセッションの再利用が有効化されており、クライアントとサーバがセッション識別子を使ってセッションを再確立しているのに、システムでセッション識別子がキャッシュされていません。	デフォルト アクションを継承	復号化しない ブロック リセット付きブロック デフォルト アクションを継承
ハンドシェイク エラー	SSL ハンドシェイクのネゴシエーション中にエラーが発生しました。	デフォルト アクションを継承	復号化しない ブロック リセット付きブロック デフォルト アクションを継承
復号化エラー	トラフィックの復号化中にエラーが発生しました。	ブロック	ブロック リセット付きブロック

SSL ポリシーを最初に作成する場合、デフォルト アクションによって処理される接続のログは、デフォルトでは無効化されています。復号化できないトラフィックの処理ではデフォルト アクションのログ設定も適用されるため、復号化できないトラフィック用のアクションで処理される接続のログは、デフォルトでは無効化されています。デフォルトのロギング設定の詳細については、「SSL ルールによる復号可能接続のロギング（38-14 ページ）」を参照してください。

注　クライアントと管理対象デバイスの間に HTTP プロキシがあって、クライアントとサーバが CONNECT HTTP メソッドを使用してトンネル SSL 接続を確立する場合、システムはトラフィックを復号化できません。このトラフィックのシステムによる処理法は、ハンドシェイク エラー（**Handshake Errors**）の復号化できないアクションが決定します。詳細については、「復号化アクション：さらに検査するためにトラフィックを復号化（21-11 ページ）」を参照してください。

ブラウザが証明書ピニングを使用してサーバ証明書を確認する場合は、サーバ証明書に再署名しても、このトラフィックを復号化できないことに注意してください。このトラフィックはアクセス コントロールを使用して引き続き検査できるため、復号化できないトラフィック アクションでは処理されません。このトラフィックを許可するには、サーバ証明書の共通名または識別名と突き合わせるように、Do not decrypt アクションを使用して SSL ルールを設定します。

復号化できないトラフィックのデフォルト処理を設定する方法:

アクセス: Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [SSL] を選択します。

[SSL Policy] ページが表示されます。

ステップ 2　設定する SSL ポリシーの横にある編集アイコン( )をクリックします。

SSL ポリシー エディタが表示されます。

ステップ 3　[Undecryptable Actions] タブを選択します。

[Undecryptable Actions] タブが表示されます。

ステップ 4　各フィールドで、復号化できないトラフィック タイプで実行するアクションを選択するか、あるいは SSL ポリシーのデフォルト アクションを適用するかを指定します。詳細については、SSL ポリシーのデフォルト アクションの表を参照してください。

ステップ 5　[Save] をクリックして変更を保存します。

変更を反映させるには、関連付けたアクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

SSL ポリシーの編集

ライセンス: すべて

サポートされるデバイス: シリーズ 3

SSL ポリシー エディタ ページでは、ポリシーの設定と SSL ルールの編成ができます。SSL ポリシーの設定では、ポリシーに一意の名前を付け、デフォルト アクションを指定する必要があります。次のことも実行できます。

- SSL ルールの追加、編集、削除、有効化/無効化
- 信頼できる CA 証明書を追加する
- システムが復号化できない暗号化トラフィックに対する処理の指定
- デフォルト アクションおよび復号化できないトラフィック アクションで処理されるトラフィックのログ

SSL ポリシーの作成または変更後は、SSL ポリシーをアクセス コントロール ポリシーに関連付け、そのアクセス コントロール ポリシーを適用します。カスタム ユーザ プロファイルを作成して、ユーザーごとに、ポリシーの設定、編成、適用のための異なる権限を割り当てることもできます。

次の表は、SSL ポリシー エディタで実行可能な設定アクションを示しています。

表 20-4　SSL ポリシーの設定アクション

目的	操作
ポリシーの名前または説明を変更する	[Name] フィールドまたは [Description] フィールドをクリックして、必要に応じて文字を削除し、新しい名前または説明を入力します。
デフォルト アクションを設定する	詳細については、暗号化トラフィックのデフォルトの処理と検査の設定（20-4 ページ）を参照してください。

表 20-4　SSL ポリシーの設定アクション（続き）

目的	操作
復号化できないトラフィックのデフォルト処理を設定する	詳細については、復号化できないトラフィックのデフォルト処理の設定（20-5 ページ）を参照してください。
デフォルト アクションと復号化できないトラフィック アクションの接続をログに記録する	詳細については、SSL ルールによる復号可能接続のロギング（38-14 ページ）を参照してください。
信頼できる CA 証明書を追加する	詳細については、外部認証局の信頼（22-25 ページ）を参照してください。
ユーザごとに異なる権限を割り当てる	詳細については、カスタム ユーザ ロールによる SSL インスペクション展開の管理（19-4 ページ）を参照してください。
ポリシーの変更を保存する	[Save] をクリックします。
ポリシーの変更をキャンセルする	[Cancel] をクリックします。変更を行った場合は、次に [OK] をクリックします。
ポリシーにルールを追加する	[Add Rule] をクリックします。詳細については、「SSL ルールの概要と作成（21-4 ページ）」を参照してください。 **ヒント**　ルールの行の空白部分を右クリックし、[Insert new rule] を選択するという方法もあります。
既存のルールを編集する	ルールの横にある編集アイコン（）をクリックします。詳細については、「SSL ルールの概要と作成（21-4 ページ）」を参照してください。 **ヒント**　ルールを右クリックして、[Edit] を選択することもできます。
ルールを削除する	ルールの横にある削除アイコン（  ）をクリックし、[OK] をクリックします。 **ヒント**　選択したルールの行の空白部分を右クリックして [Delete] を選択した後、[OK] をクリックして、選択した 1 つ以上のルールを削除するという方法もあります。
既存のルールを有効または無効にする	選択したルールを右クリックして [State] を選択した後、[Disable] または [Enable] を選択します。無効なルールはグレーで表示され、ルール名の下に [(disabled)] というマークが付きます。
特定のルール属性の設定ページを表示する	ルールの行で、該当する条件のカラムに示されている名前、値、またはアイコンをクリックします。たとえば、[Source Networks] カラムに示されている名前または値をクリックすると、選択したルールの [Networks] ページが表示されます。詳細については、「SSL ルールを使用したトラフィック復号化の調整（22-1 ページ）」を参照してください。

設定を変更すると、変更がまだ保存されていないことを通知するメッセージが表示されます。変更を維持するには、ポリシー エディタを終了する前にポリシーを保存する必要があります。変更を保存しないでポリシー エディタを終了しようとすると、変更がまだ保存されていないことを警告するメッセージが表示されます。この場合、変更を破棄してポリシーを終了するか、ポリシー エディタに戻るかを選択できます。

セッションのプライバシーを保護するために、ポリシー エディタで 60 分間操作が行われないと、ポリシーの変更が破棄されて、[SSL Policy] ページに戻されます。30 分間操作が行われなかった時点で、変更が破棄されるまでの分数を示すメッセージが表示されます。以降、このメッセージは定期的に更新されて残りの分数を示します。ページで何らかの操作を行うと、タイマーがキャンセルされます。

2 つのブラウザ ウィンドウで同じポリシーを編集しようとすると、新しいウィンドウで編集を再開するか、元のウィンドウでの変更を破棄して新しいウィンドウで編集を続ける か、または 2 番目のウィンドウをキャンセルしてポリシー エディタに戻るかを選択するよう求めるプロンプトが出されます。

複数のユーザが同じポリシーを同時に編集する際、ポリシー エディタに変更を保存していない他のユーザを特定するメッセージが表示されます。いずれかのユーザが変更を保存しようとすると、その変更によって他のユーザの変更が上書きされることを警告するメッセージが表示されます。同一のポリシーを複数のユーザが保存する場合、最後に保存された変更が維持されます。

SSL ポリシーを編集する手順：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [SSL] を選択します。

[SSL Policy] ページが表示されます。

ステップ 2　設定する SSL ポリシーの横にある編集アイコン（ ）をクリックします。

SSL ポリシー エディタ ページが表示されます。

ステップ 3　次の選択肢があります。

- ポリシーを設定する場合は、SSL ポリシーの設定アクションの表で説明されているすべての操作を使用できます。
- ポリシー ルールを編成する場合は、ポリシー内の SSL ルールの管理（21-13 ページ）の表で説明されているすべての操作を使用できます。

ステップ 4　設定を保存または廃棄します。次の選択肢があります。

- 変更を保存し、編集を続行する場合は、[Save] をクリックします。
- 変更を廃棄する場合は、[Cancel] をクリックし、プロンプトが出たら [OK] をクリックします。

  変更は廃棄され、[SSL Policy] ページが表示されます。

アクセス コントロールを使用した復号化設定の適用

ライセンス： すべて

サポートされるデバイス： シリーズ 3

SSL ポリシーに何らかの変更をした後は、関連付けられたアクセス コントロール ポリシーの適用が必要です。詳細については、アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

注意　SSL ポリシーをアクセス コントロール ポリシーと関連付けるか、または [None] を選択してポリシーの関連付けを後から解除すると、Snort プロセスが再開され、構成変更を適用する際、一時的にトラフィック検査が中断されます。この検査中にシステムがトラフィックをドロップするか、検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、「Snort の再開によるトラフィックへの影響（1-9 ページ）」を参照してください。

SSL ポリシーを適用する場合は、次の点に注意してください。

- 適用された SSL ポリシー、または現在適用されている SSL ポリシーを削除することはできません。
- アクセス コントロール ポリシーを適用すると、関連付けられた SSL ポリシーが自動的に適用されます。SSL ポリシーを個別に適用することはできません。

注　パッシブ展開では、システムがトラフィック フローに影響を与えることはありません。適用しようとするアクセス コントロール ポリシーが参照する SSL ポリシーに、暗号化トラフィックのブロックまたは、サーバ証明書の再署名によるトラフィックの復号化が設定されている場合、システムから警告が出されます。またパッシブ展開では、一時 Diffie-Hellman（DHE）および楕円曲線 Diffie-Hellman（ECDHE）暗号スイートを使った暗号化トラフィックの復号化をサポートしていません。

SSL ポリシーとアクセス コントロール ポリシーを関連付ける方法：

アクセス： Admin/Security Approver

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　設定するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3　[Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ 4　[General Settings] の横にある編集アイコン（）をクリックします。

[General Settings] ポップアップ ウィンドウが表示されます。

ステップ 5　[SSL Policy to use for inspecting encrypted connections] ドロップダウンから SSL ポリシーを選択します。

ステップ 6　[OK] をクリックします。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ 7　[Save] をクリックして変更を保存します。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

現在のトラフィック復号化設定のレポートの生成

ライセンス： すべて

SSL ポリシー レポートは、特定の時点でのポリシーとルール設定の記録です。このレポートは、監査目的や、現行の設定を調べるために使用できます。

ヒント　また、ポリシーを現在適用されているポリシーまたは別のポリシーと比較する SSL 比較レポートを生成することもできます。詳細については、SSL ポリシーの比較（20-11 ページ）を参照してください。

SSL ポリシー レポートには、次の表で説明するセクションが含まれます。

表 20-5　SSL ポリシー レポートのセクション

セクション	説明
Title Page	ポリシー レポートの名前、ポリシーが最後に変更された日時、その変更を行ったユーザの名前が記載されます。
目次	レポートの内容が記載されます。
Policy Information	ポリシーの名前と説明、ポリシーを最後に変更したユーザの名前、ポリシーが最後に変更された日時が記載されます。
Default Action	デフォルト アクションが記載されます。
Default Logging	デフォルト接続ログの設定が記載されます。
ルール	ルール カテゴリ別に、ポリシーに含まれる各ルールのルール アクションおよび条件が記載されます。
Trusted CA Certificates	自動的に信頼できる CA 証明書が記載されます。該当するのは、検出されたトラフィックの暗号化にそうした証明書が使用されている場合、あるいは信頼のチェーン内にある他の証明書が使用されている場合です。
Undecryptable Actions	復号化できないトラフィック タイプが検出された場合に適用されるアクションが記載されます。
Referenced Objects	ポリシーで使用されている個々のすべてのオブジェクトおよびグループ オブジェクトの名前と設定が、各オブジェクトが設定されている条件タイプ別（ネットワーク、VLAN、タグなど）に記載されます。

SSL ポリシー レポートを表示する方法：

アクセス： Admin/Access Admin/Network Admin/Security Approver

ステップ 1　[Policies] > [SSL] を選択します。

[SSL Policy] ページが表示されます。

ステップ 2　レポートの生成対象とするポリシーの横にあるレポート アイコン（  ）をクリックします。SSL ポリシー レポートを生成する前に、すべての変更を保存してください。保存された変更のみがレポートに表示されます。

システムによってレポートが生成されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。

SSL ポリシーの比較

ライセンス： すべて

ポリシー変更が組織の標準に準拠しているかどうかを確認するため、またはシステムのパフォーマンスを最適化するために、2 つの SSL ポリシーの違いを確認することができます。任意の 2 つのポリシーを比較することも、現在適用されているポリシーを別のポリシーと比較することもできます。オプションで、比較した後に PDF レポートを生成することで、2 つのポリシーの間の差異を記録できます。

ポリシーを比較するために使用できるツールは 2 つあります。

- 比較ビューは、2 つのポリシーを左右に並べて表示し、その差異のみを示します。比較ビューの左右のタイトル バーに、それぞれのポリシーの名前が示されます。ただし、[Running Configuration] を選択した場合、現在アクティブなポリシーは空白のバーで表されます。

  このツールを使用すると、Web インターフェイスで 2 つのポリシーを表示してそれらに移動するときに、差異を強調表示することができます。

- 比較レポートは、ポリシー レポートと同様の形式ですが、2 つのポリシーの間の差異だけが、PDF 形式で記録されます。

  これを使用して、ポリシーの比較の保存、コピー、出力、共有を行って、さらに検証することができます。

ポリシー比較ツールの概要と使用法の詳細については、次の項を参照してください。

- SSL ポリシー比較ビューの使用（20-12 ページ）
- SSL ポリシー比較レポートの使用（20-13 ページ）

SSL ポリシー比較ビューの使用

ライセンス： すべて

比較ビューには、両方のポリシーが左右に並べて表示されます。それぞれのポリシーは、比較ビューの左右のタイトル バーに示される名前で特定されます。現在実行されている設定ではない 2 つのポリシーを比較する場合、最後に変更された日時とその変更を行ったユーザがポリシー名と共に表示されます。2 つのポリシーの違いは、次のように強調表示されます。

- 青は、強調表示されている設定項目が 2 つのポリシー間で異なっていることを示し、異なっている部分は赤のテキストで表示されます。
- 緑色は強調表示された設定が一方のポリシーには存在するが、他方には存在しないことを示します。

次の表に、実行できる操作を記載します。

表 20-6　SSL ポリシー比較のビューのアクション

目的	操作
変更に個別にナビゲートする	タイトル バーの上の [Previous] または [Next] をクリックします。 左側と右側の間にある二重矢印アイコン（）が移動し、表示している違いを示す [Difference] 番号が変わります。
新しいポリシー比較ビューを生成する	[New Comparison] をクリックします。 [Select Comparison] ウィンドウが表示されます。詳細については、「SSL ポリシー比較レポートの使用（20-13 ページ）」を参照してください。
ポリシー比較レポートを生成する	[Comparison Report] をクリックします。 ポリシー比較レポートは、2 つのポリシーの間の差異だけをリストした PDF ドキュメントです。

SSL ポリシー比較レポートの使用

ライセンス：すべて

SSL ポリシー比較レポートは、ポリシー比較ビューによって示される 2 つの SSL ポリシー間または 1 つのポリシーと現在適用されているポリシーの間のすべての差異を PDF 形式で表示する記録です。このレポートを使用することで、2 つのポリシー設定の間の違いをさらに調べ、調査結果を保存して共有できます。

アクセス可能な任意のポリシーに関して、比較ビューから SSL ポリシー比較レポートを生成できます。ポリシー レポートを生成する前に、必ずすべての変更を保存してください。レポートには、保存されている変更だけが表示されます。

ポリシー比較レポートの形式は、ポリシー レポートと同様です。唯一異なる点は、ポリシー レポートにはポリシーのすべての設定が記載される一方、ポリシー比較レポートにはポリシー間で異なる設定だけがリストされることです。SSL ポリシー比較レポートには、「現在のトラフィック復号化設定のレポートの生成（20-10 ページ）」で説明しているセクションが含まれます。

ヒント　同様の手順を使用して、アクセス コントロール ポリシー、ネットワーク解析ポリシー、侵入ポリシー、ファイル ポリシー、システム ポリシー、またはヘルス ポリシーを比較できます。

2 つの SSL ポリシーを比較する方法：

アクセス：Admin/Access Admin/Network Admin/Security Approver

ステップ 1　[Policies] > [SSL] を選択します。

[SSL Policy] が表示されます。

ステップ 2　[Compare Policies] をクリックします。

[Select Comparison] ウィンドウが表示されます。

ステップ 3　[Compare Against] ドロップダウンリストから、比較するタイプを次のように選択します。

- 異なる 2 つのポリシーを比較するには、[Other Policy] を選択します。

  ページが更新されて、[Policy A] と [Policy B] という 2 つのドロップダウンリストが表示されます。

- 現在アクティブなポリシーと別のポリシーを比較するには、[Running Configuration] を選択します。

  ページが更新されて、[Target/Running Configuration A] と [Policy B] という 2 つのドロップダウンリストが表示されます。

ステップ 4　選択した比較タイプによって、次の選択肢があります。

- 2 つの異なるポリシーを比較する場合は、[Policy A] および [Policy B] ドロップダウンリストのそれぞれから、比較するポリシーを選択します。
- 現在実行されている設定を別のポリシーと比較する場合は、[Policy B] ドロップダウンリストから 2 つ目のポリシーを選択します。

ステップ 5　ポリシー比較ビューを表示するには、[OK] をクリックします。

比較ビューが表示されます。

ステップ 6　オプションで、[Comparison Report] をクリックして、SSL ポリシー比較レポートを生成します。

SSL ポリシー比較レポートが表示されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。

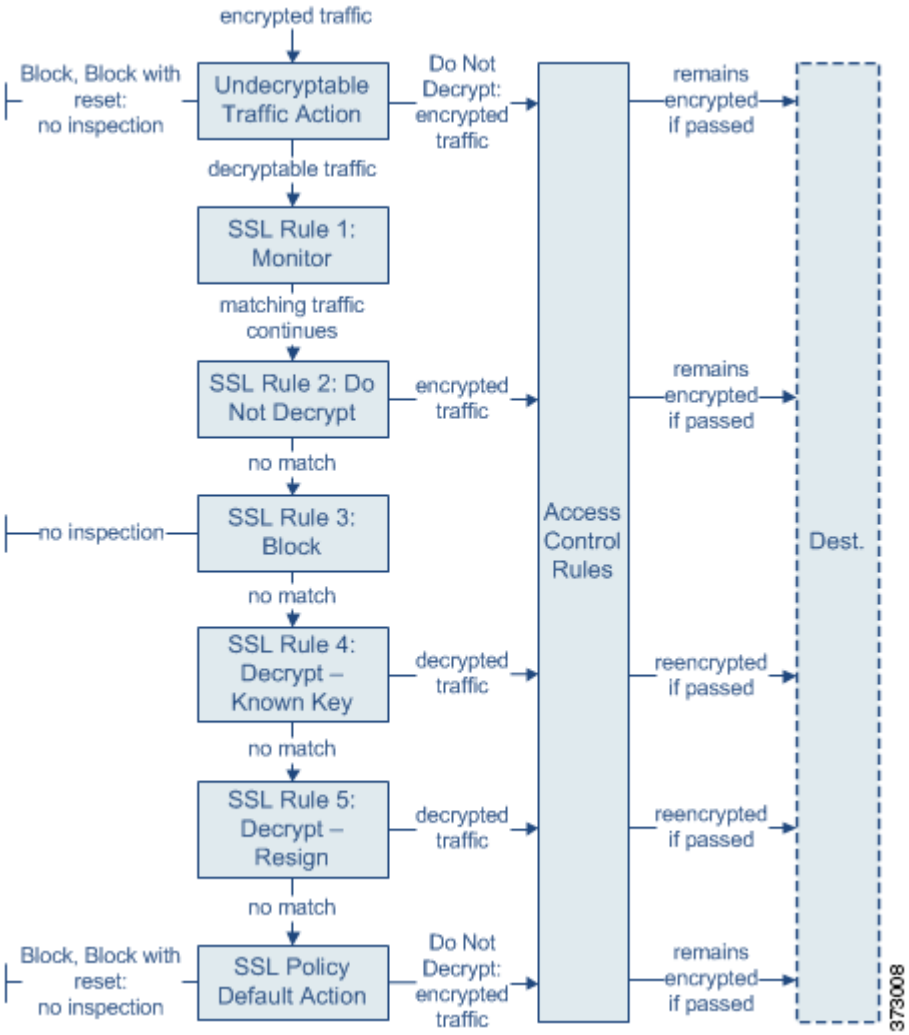
SSL ルール クイック スタート ガイド

1 つの SSL ポリシー内に各種の *SSL ルール*を設定することで、それ以上のインスペクションなしでトラフィックをブロックする、トラフィックを復号化せずにアクセス コントロールで検査する、あるいはアクセス コントロールでの分析用にトラフィックを復号化するなど、複数の管理対象デバイスをカバーしたきめ細かな暗号化トラフィックの処理メソッドを構築できます。

システムは指定した順序で SSL ルールをトラフィックと照合します。ほとんどの場合、システムによる暗号化トラフィックの処理は、*すべて*のルールの条件がトラフィックに一致する*最初の* SSL ルールに従って行われます。こうした条件には、単純なものと複雑なものがあります。セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、ユーザ、証明書、証明書の識別名、証明書ステータス、暗号スイート、暗号化プロトコル バージョンなどによってトラフィックを制御できます。

また、各ルールには 1 つの *アクション*があり、一致するトラフィックの復号化後にオプションでモニタするか、ブロックするか、または一致したトラフィックをアクセス コントロールで検査するかを決定します。システムがブロックした暗号化トラフィックは、それ以上のインスペクションが**行われない**ことに注意してください。暗号化後および復号化できないトラフィックは、アクセス コントロールを使用して検査します。ただし、一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルールが少なくなる場合があります。また、暗号化されたペイロードの侵入およびファイル インスペクションは、デフォルトで無効になっています。

次のシナリオは、インライン展開での SSL ルールによるトラフィックの処理を示します。



このシナリオでは、トラフィックは次のように評価されます。

- **復号化できないトラフィック アクション（Undecryptable Traffic Action）**は、暗号化されたトラフィックを最初に評価します。復号化できないトラフィックについてシステムは、それ以上のインスペクションなしでブロックするか、あるいはアクセス コントロールによる検査用に渡します。一致しなかった暗号化トラフィックは、次のルールへと進められます。
- **SSL ルール 1：モニタ（SSL Rule 1: Monitor）**は、暗号化トラフィックを次に評価します。モニタ ルールは、暗号化トラフィックのログ記録と追跡を行いますが、トラフィック フローには影響しません。システムはトラフィックと追加ルールの照合を継続して、許可するか拒否するかを決定します。
- **SSL ルール 2：復号化しない（SSL Rule 2: Do Not Decrypt）**は、暗号化トラフィックを 3 番目に評価します。一致したトラフィックは復号化されません。システムはこのトラフィックをアクセス コントロールにより検査しますが、ファイルや侵入インスペクションは行いません。一致しなかったトラフィックは、次のルールへと進められます。
- **SSL ルール 3：ブロック（SSL Rule 3: Block）**は、暗号化トラフィックを 4 番目に評価します。一致したトラフィックは、それ以上のインスペクションは行わずに、ブロックされます。一致しなかったトラフィックは、次のルールへと進められます。

- **SSL ルール 4：復号化 - 既知のキー（SSL Rule 4: Decrypt - Known Key）**は、暗号化トラフィックを 5 番目に評価します。ネットワークへの着信トラフィックで一致したものは、ユーザのアップロードする秘密キーを使用して復号化されます。復号化トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号化されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加検査の結果、システムがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。SSL ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **SSL ルール 5：復号化 - 再署名（SSL Rule 5: Decrypt - Resign）**は、最後のルールです。トラフィックがこのルールに一致した場合、システムはアップロードされた CA 証明書を使用してサーバ証明書を再署名してから、中間者（man-in-the-middle）としてトラフィックを復号化します。復号化トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号化されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加検査の結果、システムがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。SSL ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **SSL ポリシーのデフォルト アクション（SSL Policy Default Action）**は、他の SSL ルールに一致しなかったすべてのトラフィックを処理します。デフォルト アクションでは、暗号化トラフィックをそれ以上のインスペクションなしでブロックするか、あるいは復号化しないままにして、アクセス コントロールによる検査を行います。

詳細については、次の項を参照してください。

- サポートする検査情報の設定（21-3 ページ）
- SSL ルールの概要と作成（21-4 ページ）
- ポリシー内の SSL ルールの管理（21-13 ページ）

サポートする検査情報の設定

ライセンス： すべて

暗号化セッションの特性に基づいた暗号化トラフィックの制御および暗号化トラフィックの復号化には、再利用可能な公開キー インフラストラクチャ（PKI）オブジェクトの作成が必要です。この情報の追加は、信頼できる認証局（CA）の証明書の SSL ポリシーへのアップロード、SSL ルール条件の作成、およびプロセスでの関連オブジェクトの作成時に、臨機応変に実行できます。ただし、これらのオブジェクトを事前に設定しておくと、不適切なオブジェクトが作成される可能性を抑制できます。

証明書とキー ペアによる暗号化トラフィックの復号化

セッション暗号化に使用するサーバ証明書と秘密キーをアップロードして内部証明書オブジェクトを設定しておくと、システムは着信する暗号化トラフィックを復号化できます。**Decrypt - Known Key** アクションが設定された SSL ルールでそのオブジェクトを参照し、当該ルールにトラフィックが一致すると、システムはアップロードされた秘密キーを使用してセッションを復号化します。

CA 証明書と秘密キーをアップロードして内部 CA オブジェクトを設定した場合、システムは発信トラフィックの復号化もできます。**Decrypt - Resign** アクションが設定された SSL ルールでそのオブジェクトを参照し、当該ルールにトラフィックが一致すると、システムはクライアント ブラウザに渡されたサーバ証明書を再署名した後、中間者（man-in-the-middle）としてセッションを復号化します。

詳細については、次の各項を参照してください。

- 内部証明書オブジェクトの使用（3-55 ページ）
- 内部認証局オブジェクトの使用（3-47 ページ）

暗号化セッションの特性に基づいたトラフィック制御

システムによる暗号化トラフィックの制御は、セッション ネゴシエートに使用されたサーバ証明書または暗号スイートに基づいて実行できます。複数の異なる再利用可能オブジェクトの 1 つを設定し、SSL ルール条件でオブジェクトを参照しトラフィックを照合することができます。次の表に、設定できる再利用可能なオブジェクトのタイプを示します。

設定する内容	暗号化トラフィック制御に使用する条件
1 つまたは複数の暗号スイートが含まれる暗号スイートのリスト	暗号化セッションのネゴシエートに使う暗号スイートが、暗号スイート リストにある暗号スイートのいずれかに一致する。
組織の信頼する CA 証明書のアップロードによる信頼できる CA オブジェクト	この信頼できる CA は、次のいずれかにより、セッションの暗号化に使用されたサーバ証明書を信頼する。 • CA が証明書を直接発行した。 • サーバ証明書を発行した中間 CA に CA が証明書を発行した。
サーバ証明書のアップロードによる外部証明書オブジェクト	セッションの暗号化に使用されたサーバ証明書が、アップロードされたサーバ証明書と一致する。
発行元の識別名または証明書サブジェクトを含む識別名オブジェクト	セッション暗号化に使用された証明書で、サブジェクトまたは発行元の共通名、国、組織、組織単位のいずれかが、設定された識別名に一致する。

詳細については、次の各項を参照してください。

- 暗号スイート リストの操作（3-43 ページ）
- 信頼できる認証局オブジェクトの使用（3-52 ページ）
- 外部証明書オブジェクトの使用（3-54 ページ）
- 識別名オブジェクトの操作（3-44 ページ）

SSL ルールの概要と作成

ライセンス： すべて

サポートされるデバイス： シリーズ 3

SSL ポリシー内で、SSL ルールによって複数の管理対象デバイスにわたるネットワーク トラフィックを処理するためのきめ細かなメソッドが提供されます。各 SSL ルールには、一意の名前以外にも、次の基本コンポーネントがあります。

状態

デフォルトでは、ルールが有効状態になります。無効にしたルールはネットワーク トラフィックの評価には使用されなくなり、そのルールの場合の警告とエラーの生成が停止されます。

位置

SSL ポリシーのルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で、ルールを上から順にトラフィックと照合します。モニタ ルールを除き、トラフィックが一致する最初のルールがそのトラフィックを処理するルールになります。

条件

条件は、ルールで処理する特定のトラフィックを指定します。こうした条件では、セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、ユーザ、証明書、証明書のサブジェクトまたは発行元、証明書ステータス、暗号スイート、暗号化プロトコル バージョンなどによってトラフィックを照合できます。条件には、単純なものと複雑なものがあり、ターゲット デバイスのライセンスによって用途が異なります。

Action

ルールのアクションは、一致したトラフィックの処理方法を決定します。一致したトラフィックに対して行える処理は、モニタする、信頼する、ブロックする、あるいは復号化するです。復号化したトラフィックには、さらにインスペクションが適用されます。システムは、ブロックされた暗号化トラフィックと信頼された暗号化トラフィックに対してインスペクションを実行**しない**ことに注意してください。

ロギング

ルールのロギング設定は、システムが処理するトラフィックのレコードの維持を制御します。各ルールに一致したトラフィックのレコードを維持できます。SSL ポリシーでの設定に従って、システムが暗号化セッションをブロックするか、あるいはインスペクションなしで渡すことを許可するときに、その接続をログに記録できます。アクセス コントロール ルールに従ってより詳細な評価のために復号化した場合の接続ログを記録するようにシステムを強制することも可能で、これはその後でどのような処理やトラフィックの検査がされるかとは無関係です。接続のログは、Defense Center データベースの他に、システム ログ（Syslog）または SNMP トラップ サーバに記録できます。

ヒント SSL ルールを適切に作成して順序付けることは複雑な作業ですが、これは効果的な展開を構築する上で不可欠な要素です。慎重なポリシーの設計を怠ると、他のルールをプリエンプション処理したり、追加ライセンスが必要となったり、無効な設定を含んだルールになる可能性があります。予期したとおりにトラフィックが確実に処理されるようにするために、SSL ポリシー インターフェイスには、ルールに関する強力な警告およびエラーのフィードバック システムが用意されています。詳細については、SSL ルールのトラブルシューティング（21-18 ページ）を参照してください。

SSL ルールを作成または変更する手順:

アクセス: Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [SSL] を選択します。

[SSL Policy] ページが表示されます。

ステップ 2　ルールを追加する SSL ポリシーの横にある編集アイコン（）をクリックします。

SSL ポリシー エディタが表示され、[Rules] タブにフォーカスが移動します。

ステップ 3　次の選択肢があります。

- 新しいルールを追加するには、[Add Rule] をクリックします。
- 既存のルールを編集するには、そのルールの横にある編集アイコン（）をクリックします。

SSL ルール エディタが表示されます。

ステップ 4　[Name] にルールの名前を入力します。

各ルールには一意の名前が必要です。30 文字までの印刷可能文字を使用できます。スペースや特殊文字を含めることができますが、コロン(:)は使用できません。

ステップ 5　前述の説明に従い、ルール コンポーネントを設定します。次の設定をするか、デフォルト設定をそのまま使用することができます。

- ルールを有効にするかどうか [Enabled] を指定します。
- ルールの位置を指定します。「SSL ルールの評価順序の指定(21-6 ページ)」を参照してください。
- ルールの [Action] を選択します。「ルール アクションを使用した暗号化トラフィックの処理と検査の決定(21-9 ページ)」を参照してください。
- ルールの条件を設定します。「条件を使用したルールによる暗号化トラフィックの処理の指定(21-7 ページ)」を参照してください。
- [Logging] オプションを指定します。「SSL ルールによる復号可能接続のロギング(38-14 ページ)」を参照してください。

ステップ 6　[Save] をクリックしてルールを保存します。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります(アクセス コントロール ポリシーの適用(12-17 ページ)を参照してください)。

SSL ルールの評価順序の指定

ライセンス: すべて

サポートされるデバイス: シリーズ 3

SSL ルールを最初に作成するときに、ルール エディタの [Insert] ドロップダウン リストを使用して、その位置を指定します。SSL ポリシーの SSL ルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で、SSL ルールを上から順にトラフィックと照合します。

ほとんどの場合、システムによるネットワーク トラフィックの処理は、*すべて*のルールの条件がトラフィックに一致する*最初の* SSL ルールに従って行われます。Monitor ルールの場合を除き(トラフィックをログに記録するが、トラフィック フローには影響しない)、いずれかのルールとトラフィックが一致した後、システムは優先順位の低い追加ルールに対してトラフィックの評価を継続**しません**。

ヒント　適切な SSL ルールの順序は、ネットワーク トラフィックの処理に必要なリソースを軽減し、ルールのプリエンプションを回避します。ユーザが作成するルールはすべての組織と展開に固有のものですが、ユーザのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。詳細については、SSL ルールの順序指定によるパフォーマンス向上とプリエンプション回避(21-20 ページ)を参照してください。

ルールは数値で順序付けするだけでなく、カテゴリ別にグループ化することもできます。デフォルトで、システムには 3 つのカテゴリ（管理者、標準、ルート）があります。カスタム カテゴリを追加できますが、システム提供のカテゴリを削除したり、それらの順序を変更したりすることはできません。既存のルールの位置またはカテゴリの変更の詳細については、「SSL ルールの位置またはカテゴリの変更（21-16 ページ）」を参照してください。

ルールの編集や作成中にルールをカテゴリに追加する手順：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　SSL ルール エディタの [Insert] ドロップダウン リストで [Into Category] を選択し、適用するカテゴリを選択します。

ルールを保存すると、そのカテゴリの最後に配置されます。

ルールの編集や作成中にルールの位置を数値で指定する手順：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　SSL ルール エディタの [Insert] ドロップダウン リストで [above rule] または [below rule] を選択し、適切なルール番号を入力します。

ルールを保存すると、指定した位置に配置されます。

条件を使用したルールによる暗号化トラフィックの処理の指定

ライセンス： 機能によって異なる

サポートされるデバイス： シリーズ 3

SSL ルールの条件は、ルールで処理する暗号化トラフィックのタイプを特定します。条件には、単純なものと複雑なものがあり、ルールごとに複数の条件タイプを指定できます。トラフィックにルールが適用されるのは、トラフィックがルールの条件をすべて満たしている場合だけです。

ルールに特定の条件を設定しない場合、その条件によるトラフィック照合は行われません。たとえば、証明書の条件が設定されバージョンの条件が設定されていないルールは、セッション ネゴシエーションに使用されるサーバ証明書に基づいてトラフィックを評価し、セッション SSL または TLS のバージョンは関係しません。

SSL ルールを追加および編集するときは、ルール エディタ下部の左側にあるタブを使用して、ルール条件の追加と編集を行います。SSL ルールに追加できる条件を次の表に示します。

表 21-1　SSL ルールの条件タイプ

条件	一致する暗号化トラフィック	Details
ゾーン	特定のセキュリティ ゾーン内のインターフェイスを介したデバイスへの着信またはデバイスからの発信トラフィック	「セキュリティ ゾーン」とは、展開方法やセキュリティ ポリシーに基づいて構成される 1 つ以上のインターフェイスの論理グループを指します。ゾーン内のインターフェイスが複数のデバイス間に配置される場合もあります。ゾーン条件の作成については、ネットワーク ゾーンによる暗号化トラフィックの制御（22-2 ページ）を参照してください。
Networks	その送信元または宛先の IP アドレス、国、または大陸で区別されるトラフィック	特定の IP アドレスを明示的に指定できます。位置情報の機能では、送信元または宛先となる国や大陸を基準にしたトラフィック制御もできます。ネットワーク条件の作成については、ネットワークまたは地理的位置による暗号化トラフィックの制御（22-4 ページ）を参照してください。
VLAN タグ	VLAN によりタグ付けされたトラフィック	VLAN によるパケットの識別に最内部の VLAN タグが使用されます。VLAN 条件の作成については、「暗号化された VLAN トラフィックの制御（22-6 ページ）」を参照してください。
ポート	送信元ポートまたは宛先ポート	TCP ポートに基づいて暗号化トラフィックを制御できます。ポート条件の作成については、「ポートによる暗号化トラフィックの制御（22-7 ページ）」を参照してください。
ユーザ	セッションに参加しているユーザ	暗号化されたモニタ対象セッションの関連ホストにログインしている LDAP ユーザに基づいて暗号化トラフィックを制御できます。Microsoft Active Directory サーバから取得された個別ユーザまたはグループに基づいてトラフィックを制御できます。ユーザ条件の作成については、「ユーザ ベースの暗号化トラフィックの制御（22-9 ページ）」を参照してください。
アプリケーション	セッションで検出されるアプリケーション	タイプ、リスク、ビジネスとの関連性、カテゴリの基本的な特性に従って、フィルタ アクセスまたは暗号化セッションの各アプリケーションへのアクセスを制御できます。アプリケーション条件の作成については、「アプリケーション ベースの暗号化トラフィックの制御（22-11 ページ）」を参照してください。
カテゴリ	証明書サブジェクトの識別名に基づいてセッションで要求される URL	URL の一般分類とリスク レベルに基づいて、ネットワークのユーザがアクセスできる Web サイトを制限できます。URL 条件の作成については、「URL カテゴリおよびレピュテーションによる暗号化トラフィックの制御（22-17 ページ）」を参照してください。
Distinguished Names	暗号化セッションのネゴシエートに使用されたサーバ証明書のサブジェクトまたは発行元の識別名	サーバ証明書を発行した CA またはサーバ証明書ホルダーに基づいて、暗号化トラフィックを制御できます。識別名条件の作成については、「証明書の識別名による暗号化トラフィックの制御（22-21 ページ）」を参照してください。
証明書	暗号化セッションのネゴシエートに使用されるサーバ証明書	暗号化セッションのネゴシエート用にユーザのブラウザに渡されるサーバ証明書に基づいて、暗号化されたトラフィックを制御できます。証明書条件の作成については、「証明書ステータスによる暗号化トラフィックの制御（22-25 ページ）」を参照してください。

表 21-1　SSL ルールの条件タイプ（続き）

条件	一致する暗号化トラフィック	Details
証明書のステータス	暗号化セッションのネゴシエートに使用されるサーバ証明書のプロパティ	サーバ証明書のステータスに基づいて、暗号化トラフィックを制御できます。証明書ステータス条件の作成については、「証明書ステータスによる暗号化トラフィックの制御（22-25 ページ）」を参照してください。
暗号スイート	暗号化セッションのネゴシエートに使用する暗号スイート	暗号化セッションのネゴシエート用にサーバで選択された暗号スイートに基づいて、暗号化トラフィックを制御できます。暗号スイート条件の作成については、「暗号スイートによる暗号化トラフィックの制御（22-30 ページ）」を参照してください。
Versions	セッションの暗号化に使用される SSL または TLS のバージョン	セッションの暗号化に使用される SSL または TLS のバージョンに基づいて、暗号化トラフィックを制御できます。バージョン条件の作成については、「暗号化プロトコルのバージョンによるトラフィックの制御（22-31 ページ）」を参照してください。

シリーズ 3デバイスでの暗号化トラフィックの制御と確認は可能ですが、トラフィックの制御に、検出されたアプリケーション、URL カテゴリ、またはユーザを使用するには追加ライセンスが必要です。また過度に複雑なルールは、多くのリソースを消費し、状況によってはポリシーを適用できなくなる場合があります。詳細については、SSL ルールのトラブルシューティング（21-18 ページ）を参照してください。

ルール アクションを使用した暗号化トラフィックの処理と検査の決定

ライセンス： すべて

サポートされるデバイス： シリーズ 3

すべての SSL ルールには、一致する暗号化トラフィックに対して次の判定をする関連アクションがあります。

- 処理：まず第一に、ルール アクションはルールの条件に一致する暗号化トラフィックに対して、モニタ、信頼、ブロック、または復号化を行うかどうかを判定します。
- ロギング：ルール アクションは一致する暗号化トラフィックの詳細をいつ、どのようにログに記録するかを判定します。

SSL インスペクション設定では、次のように復号化されたトラフィックの処理、検査、ログ記録を行います。

- SSL ポリシーの復号化できないアクションは、システムが復号化できないトラフィックを処理します。「復号化できないトラフィックのデフォルト処理の設定（20-5 ページ）」を参照してください。
- ポリシーのデフォルト アクションは、Monitor 以外のどの SSL ルールの条件にも一致しないトラフィックを処理します。「暗号化トラフィックのデフォルトの処理と検査の設定（20-4 ページ）」を参照してください。

システムが暗号化セッションを信頼またはブロックしたときに、接続イベントをログに記録できます。アクセス コントロール ルールに従ってより詳細な評価のために復号化した場合の接続ログを記録するようにシステムを強制することも可能で、これはその後でどのような処理やト

ラフィックの検査がされるかとは無関係です。暗号化セッションの接続ログには、セッションの暗号化に使用される証明書など、暗号化の詳細が含まれます。ただし次の場合は、接続の終了（end-of-connection）イベントだけをログに記録できます。

- ブロックされた接続（Block、Block with reset）の場合、システムは即座にセッションを終了してイベントを生成します。
- 信頼された接続（Do not decrypt）の場合、システムはセッション終了時にイベントを生成します。

ルール アクションの詳細および、ルール アクションが処理とログに与える影響の詳細については、次のセクションを参照してください。

- モニタ アクション：アクションの遅延とログの確保（21-10 ページ）
- 復号化しない（Do Not Decrypt）アクション：暗号化トラフィックを検査なしで転送（21-10 ページ）
- ブロッキング（Block）アクション：検査なしで暗号化トラフィックをブロック（21-11 ページ）
- 復号化アクション：さらに検査するためにトラフィックを復号化（21-11 ページ）
- ポリシー内の SSL ルールの管理（21-13 ページ）

モニタ アクション：アクションの遅延とログの確保

ライセンス： すべて

サポートされるデバイス： シリーズ 3

モニタ アクションは暗号化トラフィック フローに影響を与えません。つまり、一致するトラフィックがただちに許可または拒否されることはありません。その代わり、追加のルールが存在する場合はそのルールに照らしてトラフィックが照合され、信頼するか、ブロックするか、復号化するかが決定されます。モニタ ルール以外の一致する最初のルールが、トラフィック フローおよび追加のインスペクションを決定します。さらに一致するルールがない場合、システムはデフォルト アクションを使用します。

モニタ ルールの主な目的はネットワーク トラフィックのトラッキングなので、システムはモニタ対象トラフィックの接続終了イベントを自動的にログに記録します。つまり、ルールのロギング設定または後で接続を処理するデフォルト アクションとは無関係に、システムはDefense Centerデータベース接続の終了時に常にログに記録します。言い換えると、パケットが他のルールに一致せず、デフォルト アクションでロギングが有効になっていない場合でも、パケットがモニタ ルールに一致すれば必ず接続がロギングされます。

復号化しない（Do Not Decrypt）アクション：暗号化トラフィックを検査なしで転送

ライセンス： すべて

サポートされるデバイス： シリーズ 3

復号化しない（**Do Not Decrypt**）アクションは、アクセス コントロール ポリシーのルールおよびデフォルト アクションに従って暗号化トラフィックを評価するため転送します。一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、こうしたトラフィックに一致するルール数が少なくなる場合があります。侵入やファイル インスペクションなど、暗号化トラフィックのディープ インスペクションは実行できません。

ブロッキング（Block）アクション：検査なしで暗号化トラフィックをブロック

ライセンス：すべて

サポートされるデバイス：シリーズ 3

Block および **Block with reset** アクションは、アクセス コントロール ルールのブロックとリセット付きブロック アクション（Block および Block with reset）に類似したものです。これらのアクションは、クライアントとサーバによる SSL 暗号化セッションの確立と暗号化トラフィックの転送を防止します。リセット付きブロック ルールでは接続のリセットも行います。

ブロックされた暗号化トラフィックについては、設定された応答ページが表示されないので注意してください。その代わりに、ユーザの要求する禁止された URL の接続は、リセットまたはタイムアウトされます。詳細については、「ブロックされた URL のカスタム Web ページの表示（16-20 ページ）」を参照してください。

ヒント　パッシブまたはインライン（タップ モード）展開では、デバイスがトラフィックを直接検査しないので、ブロックおよびリセット付きブロック（Block および Block with reset）アクションを使用できないことに注意してください。パッシブまたはインライン（タップ モード）インターフェイスを含むセキュリティ ゾーン条件内で、ブロックおよびリセット付きブロック（Block および Block with reset）アクションを使用したルールを作成すると、ポリシー エディタでルールの横に警告アイコン（⚠）が表示されます。

復号化アクション：さらに検査するためにトラフィックを復号化

ライセンス：すべて

サポートされるデバイス：シリーズ 3

Decrypt - Known Key および **Decrypt - Resign** アクションは、暗号化トラフィックを復号化します。復号化されたトラフィックは、アクセス コントロールを使用して検査されます。アクセス コントロール ルールは、復号化されたトラフィックと暗号化されていないトラフィックで同じ処理をします。ここではデータの確認に加えて、侵入、禁止ファイル、マルウェアの検出とブロックができます。システムは、許可されたトラフィックを再暗号化してから宛先に渡します。

Decrypt - Known アクションを設定した場合は、1 つまたは複数のサーバ証明書と秘密キー ペアをアクションに関連付けることができます。トラフィックがルールに一致して、トラフィックの暗号化に使用された証明書とアクションに関連付けられた証明書が一致した場合、システムは適切な秘密キーを使用してセッションの暗号化と復号化キーを取得します。秘密キーへのアクセスが必要なため、このアクションが最も適しているのは、組織の管理下にあるサーバへの入力トラフィックを復号化する場合です。

同様に **Decrypt - Resign** アクションには、1 つの認証局証明書と秘密キーを関連付けることができます。トラフィックがこのルールに一致した場合、システムは CA 証明書を使用してサーバ証明書を再署名してから、中間者（man-in-the-middle）として機能します。ここでは 2 つの SSL セッションが作成され、1 つはクライアントと管理対象デバイスの間、もう 1 つは管理対象デバイスとサーバの間で使用されます。各セッションにはさまざまな暗号セッションの詳細が含まれており、システムはこれを使用することでトラフィックの復号化と再暗号化が行えます。このアクションは、証明書の秘密キーを各自の管理下にあるキーに置き換えてセッション キーを取得するため、発信トラフィックに適しています。

サーバ証明書の再署名では、証明書の公開キーを CA 証明書の公開キーに置き換えるか、あるいは証明書全体が置き換えられます。通常、サーバ証明書全体を置き換える場合は、SSL 接続が確立された時点で、証明書が信頼できる認証局によって署名されていないことがクライアント ブラウザで警告されます。ただし、その CA をクライアント ブラウザで信頼できることがポリシーに設定されている場合、ブラウザは証明書が信頼できないことの警告をしません。オリジナルのサーバ証明書が自己署名の場合、システムは証明書全体を置き換えて再署名する CA を信頼しますが、ユーザのブラウザは証明書が自己署名されていることを警告しません。この場合、サーバ証明書の公開キーを交換するだけで、クライアント ブラウザは証明書が自己署名であることを警告します。

Decrypt - Resign アクションを設定した場合、ルールによるトラフィックの照合は、設定したすべてのルール条件に加えて、参照される内部 CA 証明書の署名アルゴリズム タイプに基づいて実施されます。各 **Decrypt - Resign** アクションにはそれぞれ 1 つの CA 証明書が関連付けられるので、暗号化の署名アルゴリズムが異なる複数タイプの発信トラフィックを復号化する SSL ルールは作成できません。また、ルールに追加する暗号スイートと外部証明書のオブジェクトのすべては、関連する CA 証明書の暗号化アルゴリズム タイプに一致する必要があります。

たとえば、楕円曲線暗号（EC）アルゴリズムで暗号化された発信トラフィックが **Decrypt - Resign** ルールに一致するのは、アクションが EC ベースの CA 証明書を参照している場合だけです。証明書と暗号スイートのルール条件を作成するには、ルールに EC ベースの外部証明書と暗号スイートを追加する必要があります。同様に、RSA ベースの CA 証明書を参照する **Decrypt - Resign** ルールは、RSA アルゴリズムで暗号化された発信トラフィックのみを照合します。EC アルゴリズムで暗号化された発信トラフィックは、設定した他のすべてのルール条件が一致したとしても、このルールには一致しません。

次の点に注意してください。

- SSL 接続確立用の暗号スイートで一時 Diffie-Hellman（DHE）または楕円曲線 Diffie-Hellman（ECDHE）キー交換アルゴリズムが使用されている場合、パッシブ展開では **Decrypt - Known Key** アクションを使用できません。SSL ポリシーのターゲット デバイスにパッシブまたはインライン（タップ モード）インターフェイスがあり、そこに含まれる **Decrypt - Known Key** ルールで DHE または ECDHE の暗号スイート条件が使われている場合、ルールの横に情報アイコン（ ）が表示されます。パッシブまたはインライン（タップ モード）インターフェイスを含む SSL ルールに後からゾーン条件を追加すると、警告アイコン（ ）が表示されます。
- デバイスがトラフィックを直接検査しないため、パッシブまたはインライン（タップ モード）展開では **Decrypt - Resign** アクションを使用できません。セキュリティ ゾーン内にパッシブまたはインライン（タップ モード）インターフェイスを含む **Decrypt - Resign** アクションを使用したルールを作成した場合、ポリシー エディタでルールの横に警告アイコン（ ）が表示されます。SSL ポリシーのターゲット デバイスにパッシブまたはインライン（タップ モード）インターフェイスがあり、そこに **Decrypt - Resign** ルールが含まれる場合、ルールの横に情報アイコン（ ）が表示されます。パッシブまたはインライン（タップ モード）インターフェイスを含む SSL ルールに後からゾーン条件を追加すると、警告アイコン（ ）が表示されます。パッシブまたはインライン（タップ モード）インターフェイスを含むデバイスに、Decrypt - Resign ルールを含む SSL ポリシーを適用した場合、このルールに一致する SSL セッションはすべて失敗します。
- サーバ証明書の再署名に使用する CA をクライアントが信頼していない場合、証明書が信頼できないことの警告がユーザに出されます。これを防ぐには、クライアントの信頼できる CA ストアに CA 証明書をインポートします。または組織にプライベート PKI がある場合は、組織の全クライアントで自動的に信頼されるルート CA が署名する中間 CA 証明書を発行して、その CA 証明書をデバイスにアップロードすることもできます。
- 匿名の暗号スイートで暗号化されたトラフィックは復号化できません。匿名の暗号スイートを **Cipher Suite** 条件に追加した場合、SSL ルールに **Decrypt - Resign** または **Decrypt - Known Key** アクションを使用できません。

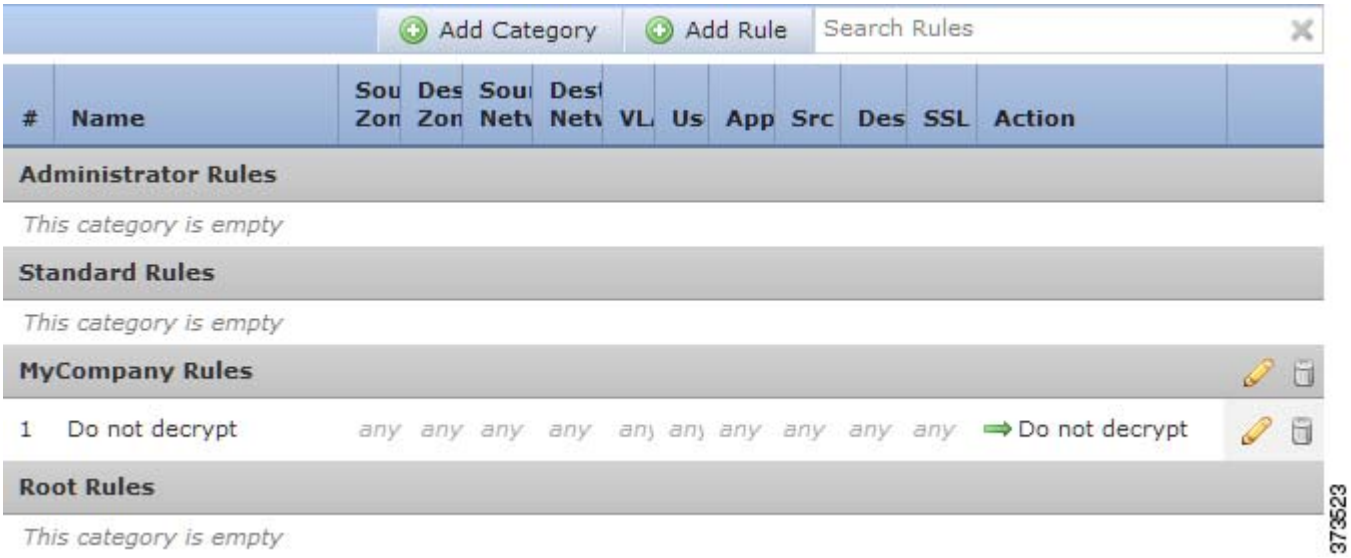
- クライアントと管理対象デバイスの間に HTTP プロキシがあって、クライアントとサーバが CONNECT HTTP メソッドを使用してトンネル SSL 接続を確立する場合、システムはトラフィックを復号化できません。このトラフィックのシステムによる処理法は、ハンドシェイク エラー（**Handshake Errors**）の復号化できないアクションが決定します。詳細については、「復号化できないトラフィックのデフォルト処理の設定（20-5 ページ）」を参照してください。
- SSL ルールに **Decrypt - Known Key** アクションを付けて作成した場合、**Distinguished Name** または **Certificate** 条件による照合はできません。ここでの前提は、このルールがトラフィックと一致する場合、証明書、サブジェクト DN、および発行元 DN は、ルールに関連付けられた証明書とすでに一致済みであることです。詳細については、ルール アクションを使用した暗号化トラフィックの処理と検査の決定（21-9 ページ）を参照してください。
- 内部 CA オブジェクトを作成して証明書署名要求（CSR）の生成を選択した場合、オブジェクトに署名付き証明書をアップロードするまで、この CA は **Decrypt - Resign** アクションに使用できません。詳細については、新しい署名付き証明書の取得およびアップロード（3-49 ページ）を参照してください。
- **Decrypt - Resign** アクションのルールを設定して、1 つまたは複数の外部証明書オブジェクトまたは暗号スイートで署名アルゴリズム タイプの不一致が生じた場合、ポリシー エディタでルールの横に情報アイコン（  ）が表示されます。すべての外部証明書オブジェクトまたはすべての暗号スイートで署名アルゴリズム タイプの不一致が生じた場合、ポリシーのルールの横には警告アイコン（  ）が表示され、SSL ポリシーに関連付けたアクセス コントロール ポリシーは適用できなくなります。詳細については、証明書による暗号化トラフィックの制御（22-23 ページ）および暗号スイートによる暗号化トラフィックの制御（22-30 ページ）を参照してください。
- **Interactive Block** または **Interactive Block with reset** アクションのアクセス コントロール ルールと復号化トラフィックが一致する場合、システムは一致する接続をインタラクションなしでブロックし、応答ページを表示**しません**。
- インライン正規化プリプロセッサで **Normalize Excess Payload** オプションをイネーブルにすると、プリプロセッサによる復号化トラフィックの標準化時に、パケットがドロップされてトリミングされたパケットに置き換えられる場合があります。これは SSL セッションを終了させません。トラフィックが許可された場合、SSL セッションの一部としてトリミングされたパケットは暗号化されます。このオプションの詳細については、「インライン トラフィックの正規化（29-7 ページ）」を参照してください。
- ブラウザが証明書ピニングを使用してサーバ証明書を確認する場合は、サーバ証明書に再署名しても、このトラフィックを復号化できません。このトラフィックを許可するには、サーバ証明書の共通名または識別名と突き合わせるように、Do not decrypt アクションを使用して SSL ルールを設定します。

ポリシー内の SSL ルールの管理

ライセンス： すべて

サポートされるデバイス： シリーズ 3

SSL ポリシー エディタの [Rules] タブでは、以下の図に示すように、ポリシー内の SSL ルールの追加、編集、検索、移動、有効化、無効化、削除、その他の管理が行えます。



各ルールについて、ポリシー エディタでは、その名前、条件のサマリー、およびルール アクションが表示されます。警告、エラー、その他の重要な情報がアイコンで示されます。無効なルールはグレーで表示され、ルール名の下に [(disabled)] というマークが付きます。アイコンの詳細については、「SSL ルールのトラブルシューティング（21-18 ページ）」を参照してください。

SSL ルールの管理の詳細については、次を参照してください。

- SSL ルールの検索（21-14 ページ）
- SSL ルールのイネーブル化とディセーブル化（21-15 ページ）
- SSL ルールの位置またはカテゴリの変更（21-16 ページ）

SSL ルールの検索

ライセンス： すべて

サポートされるデバイス： シリーズ 3

スペースおよび印刷可能な特殊文字を含む英数字文字列を使用して、SSL ルールのリストで一致する値を検索できます。この検索では、ルール名およびルールに追加したルール条件が検査されます。ルール条件の場合は、条件タイプ（ゾーン、ネットワーク、アプリケーションなど）ごとに追加できる任意の名前または値が検索照合されます。これには、個々のオブジェクト名または値、グループ オブジェクト名、グループ内の個々のオブジェクト名または値、およびリテラル値が含まれます。

検索文字列のすべてまたは一部を使用できます。照合ルールごとに、一致する値のカラムが強調表示されます。たとえば、`100Bao` という文字列のすべてまたは一部を基準に検索すると、少なくとも、100Bao アプリケーションを追加した各ルールの [Applications] カラムが強調表示されます。`100Bao` という名前のルールもある場合は、[Name] カラムと [Applications] カラムの両方が強調表示されます。

1 つ前または次の照合ルールに移動することができます。ステータス メッセージには、現行の一致および合計一致数が表示されます。

複数ページのルール リストでは、どのページでも一致が検出される可能性があります。最初の一致が検出されたのが最初のページではない場合は、最初の一致が検出されたページが表示されます。最後の一致が現行の一致となっている場合、次の一致を選択すると、最初の一致が表示されます。また、最初の一致が現行の一致となっている場合、前の一致を選択すると、最後の一致が表示されます。

ルールの検索方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　検索するポリシーの SSL ポリシー エディタで、[Search Rules] プロンプトをクリックし、検索文字列を入力してから Enter を押します。検索を開始するには、Tab キーを使用するか、ページの空白部分をクリックします。

一致する値を含むルールのカラムが強調表示されます。表示されている（最初の）一致は、他とは区別できるように強調表示されます。

ステップ 2　目的のルールを探すには次の操作が利用できます。

- 照合ルールの間を移動する場合は、次の一致アイコン（ ）または前の一致アイコン（ ）をクリックします。
- ページを更新し、検索文字列および強調表示をクリアする場合は、クリア アイコン（ ）をクリックします。

SSL ルールのイネーブル化とディセーブル化

ライセンス： すべて

サポートされるデバイス： シリーズ 3

作成した SSL ルールは、デフォルトでイネーブルになっています。無効にしたルールはネットワーク トラフィックの評価には使用されなくなり、そのルールについての警告とエラーが停止されます。SSL ポリシーのルール リストを表示すると、無効なルールはグレー表示されますが、変更は可能です。またはルール エディタを使用して SSL ルールをイネーブルまたはディセーブルにできることに注意してください。「SSL ルールの概要と作成（21-4 ページ）」を参照してください。

SSL ルールの状態を変更するには、次の手順に従います。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　イネーブルまたはディセーブルにするルールを含むポリシーの SSL ポリシー エディタで、ルールを右クリックして、ルールの状態を選択します。

- 非アクティブなルールをイネーブルにするには、[State] > [Enable] を選択します。
- アクティブなルールをディセーブルにするには、[State] > [Disable] を選択します。

ステップ 2　[Save] をクリックしてポリシーを保存します。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

SSL ルールの位置またはカテゴリの変更

ライセンス： すべて

サポートされるデバイス： シリーズ 3

SSL ルールを編成しやすいように、SSL ポリシーには、Administrator Rules（管理者ルール）、Standard Rules（標準ルール）、Root Rules（ルート ルール）という、システムが提供する 3 つのルール カテゴリが用意されています。これらのカテゴリの移動、削除、名前変更はできませんが、カスタム カテゴリの作成は可能です。

デフォルトでは、SSL ポリシーの変更を許可する定義済みユーザ ロールはすべて、ルール カテゴリ内およびカテゴリ間での SSL ルールの移動および変更も行えます。ただし、ユーザによるルールの移動と変更を制限するカスタム ロールの作成も可能です。

詳細については、以下を参照してください。

- SSL ルールの移動（21-16 ページ）
- 新しい SSL ルール カテゴリの追加（21-17 ページ）

SSL ルールの移動

ライセンス： すべて

サポートされるデバイス： シリーズ 3

適切な SSL ルールの順序は、ネットワーク トラフィックの処理に必要なリソースを軽減し、ルールのプリエンプションを回避します。デフォルトでは、SSL ポリシーの変更を許可する定義済みユーザ ロールはすべて、ルール カテゴリ内およびカテゴリ間での SSL ルールの移動も行えます。ただし、システム提供のカテゴリにあるルールのユーザによる移動を制限するカスタム ロールの作成も可能です。

次の手順は、SSL ポリシー エディタを使用して 1 つまたは複数のルールを同時に移動する方法を説明しています。またはルール エディタを使用して個々の SSL ルールを移動することもできます。「SSL ルールの概要と作成（21-4 ページ）」を参照してください。

規則を移動するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　移動するルールを含むポリシーの SSL ポリシー エディタで、ルールごとに空白部分をクリックして、ルールを選択します。複数のルールを選択するには、Ctrl キーと Shift キーを使用します。

選択したルールは強調表示されます。

ステップ 2　ルールを移動します。カット アンド ペーストおよびドラッグ アンド ドロップを使用することもできます。

新しい場所にルールをカット アンド ペーストするには、選択したルールを右クリックし、[Cut] を選択します。次に、貼り付けたい位置に隣接するルールの空白部分を右クリックし、[Paste above] または [Paste below] を選択します。2 つの異なる SSL ポリシーの間では、SSL ルールのコピー アンド ペーストはできないことに注意してください。

ステップ 3　[Save] をクリックしてポリシーを保存します。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

新しい SSL ルール カテゴリの追加

ライセンス： すべて

サポートされるデバイス： シリーズ 3

SSL ルールを編成しやすいように、SSL ポリシーには、Administrator Rules（管理者ルール）、Standard Rules（標準ルール）、Root Rules（ルート ルール）という、システムが提供する 3 つのルール カテゴリが用意されています。これらのカテゴリの移動、削除、名前変更はできませんが、Standard Rules と Root Rules 間でのカスタム カテゴリの作成は可能です。

カスタム カテゴリを追加すると、追加のポリシーを作成しなくても、ルールをさらに細かく編成できます。追加したカテゴリは、名前変更と削除ができます。これらのカテゴリの移動はできませんが、ルールのカテゴリ間およびカテゴリ内外への移動は可能です。

ロールに追加したユーザ権限に基づいて、システム提供のカテゴリにあるルールのユーザによる移動および変更を制限するカスタム ロールの作成も可能です。詳細については、アカウント特権について（61-60 ページ）を参照してください。

新しいカテゴリを追加するには、次の手順に従います。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　ルール カテゴリを追加するポリシーの SSL ポリシー エディタで、[Add Category] をクリックします。

ヒント　ポリシーにルールがすでに含まれている場合は、追加する前に既存のルールの行の空白部分をクリックすることで、新しいカテゴリの位置を設定できます。既存のルールを右クリックし、[Insert new category] を選択することもできます。

[Add Category] ポップアップ ウィンドウが表示されます。

ステップ 2　[Name] に、一意のカテゴリ名を入力します。

最大 30 文字の英数字の名前を入力できます。名前には、スペース、および印刷可能な特殊文字を含めることができます。

ステップ 3　次の選択肢があります。

- 既存のカテゴリのすぐ上に新しいカテゴリを配置する場合は、最初の [Insert] ドロップダウン リストから [above Category] を選択した後、2 番目のドロップダウン リストからカテゴリを選択します。ここで選択したカテゴリの上にルールが配置されます。
- 既存のルールの下に新しいカテゴリを配置する場合は、ドロップダウン リストから [below rule] を選択した後、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。
- 既存のルールの上にルールを配置する場合は、ドロップダウン リストから [above rule] を選択した後、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。

ステップ 4　[OK] をクリックします。

カテゴリが追加されます。名前を編集するには、カスタム カテゴリの横にある編集アイコン（ ）をクリックします。カテゴリを削除するには、削除アイコン（ ）をクリックします。削除するカテゴリに含まれるルールは、その上にあるカテゴリに追加されます。

ステップ 5　[Save] をクリックしてポリシーを保存します。

SSL ルールのトラブルシューティング

ライセンス： すべて

サポートされるデバイス： シリーズ 3

SSL ルールを適切に作成して順序付けることは複雑な作業ですが、これは効果的な展開を構築する上で不可欠な要素です。慎重なポリシーの設計を怠ると、他のルールをプリエンプション処理したり、追加ライセンスが必要となったり、無効な設定を含んだルールになる可能性があります。予期したとおりにトラフィックが確実に処理されるようにするために、SSL ポリシー インターフェイスには、ルールに関する強力な警告およびエラーのフィードバック システムが用意されています。

各ルールについては、次の表に示すように、ポリシー エディタのアイコンによる警告とエラーの表示がされます。アイコンにポインタを合わせると、警告、エラー、情報の内容を示すテキストを確認できます。

表 21-2　SSL のエラー アイコン

アイコン	説明	Details
	warning	問題によっては、ルールやその他の警告を示している SSL ポリシーであっても、適用が可能な場合があります。この場合、間違いのある設定は機能しません。たとえば、プリエンプションされたルールはトラフィックを評価しません。ただし、警告アイコンがライセンス エラーまたはモデルの不一致を示している場合は、問題が解消されるまでそのポリシーは適用できません。 警告が出されているルールを無効にすると、警告アイコンが消えます。潜在する問題を修正せずにルールを有効にすると、警告アイコンが再表示されます。
	error	ルールまたはその他の SSL ポリシー設定にエラーがある場合、問題が解消されるまでそのポリシーは適用できません。
	情報	情報アイコンは、トラフィックのフローに影響する可能性がある設定に関する有用な情報を伝送します。これらの問題は重大ではなく、ポリシーの適用を妨げません。

SSL ルールを適切に設定することは、ネットワーク トラフィックの処理に必要なリソースの軽減にも寄与します。複雑なルールを作成したりルールの順番が不適切であると、パフォーマンスに影響する場合があります。

詳細については、以下を参照してください。

- SSL ルールの警告とエラーの概要（21-19 ページ）
- ルールのプリエンプションと無効な設定の警告について（21-19 ページ）
- SSL ルールの順序指定によるパフォーマンス向上とプリエンプション回避（21-20 ページ）

SSL ルールの警告とエラーの概要

ライセンス: 機能によって異なる

サポートされるデバイス: シリーズ 3

SSL ルールは任意のライセンスを使って作成できますが、ルール条件とインスペクション オプションによっては、ターゲット デバイスで特定のライセンス機能を有効化する必要があります。ライセンスが必要な機能を使用するポリシーを、ライセンス供与されていないデバイスに適用することはできません。ライセンス供与されていない機能については、これを示す警告アイコンおよび確認ダイアログが表示されます。警告アイコンの上にポインタを置くと詳細が表示されます。

次の表に、SSL ルールの使用に必要となるライセンスを示します。

表 21-3　SSL ルールのライセンス要件

ルールの用途	ライセンス	サポートされる Defense Center	サポートされるデバイス数
ゾーン、ネットワーク、VLAN、ポート、証明書、DN、証明書ステータス、暗号スイート、またはバージョンの条件	いずれか	いずれか	シリーズ 3
位置情報データを使用するネットワーク条件	FireSIGHT	すべて（DC500 を除く）	シリーズ 3
アプリケーション条件またはユーザ条件を使用するルール	Control	任意：例外として、DC500 ではユーザ制御を実行できません。	シリーズ 3
URL カテゴリおよびレピュテーション データを使用するカテゴリ条件	URL Filtering	すべて（DC500 を除く）	シリーズ 3

ルールのプリエンプションと無効な設定の警告について

ライセンス: すべて

サポートされるデバイス: シリーズ 3

SSL ルールを適切に設定して順序付けることは、効果的な展開を構築する上で不可欠な要素です。SSL ポリシーの内部では、SSL ルール間で他のルールのプリエンプションが発生したり、無効な設定を含んだ状態になる場合があります。これらの問題については、警告およびエラーのアイコンが表示されます。

ルールのプリエンプションの警告について

SSL ルールの条件が後続のルールによるトラフィックの照合をプリエンプション処理する場合があります。次に例を示します。

```
Rule 1: do not decrypt Administrators
Rule 2: block Administrators
```

上記の 2 番目のルールによってトラフィックがブロックされることはありません。なぜなら、最初のルールによってトラフィックは既に許可されるためです。

どのようなタイプのルール条件でも、後続のルールを回避する可能性があります。次の例では、最初のルールでの VLAN 範囲に 2 番目のルールでの VLAN が含まれるため、最初のルールが 2 番目のルールよりも優先して適用されることになります。

```
Rule 1: do not decrypt VLAN 22-33
Rule 2: block VLAN 27
```

次の例では、VLAN が設定されていないルール 1 はあらゆる VLAN と一致します。そのため、ルール 1 が優先して適用され、ルール 2 での VLAN 2 の照合は行われません。

```
Rule 1: do not decrypt Source Network 10.4.0.2/16
Rule 2: do not decrypt Source Network 10.4.0.2/16, VLAN 2
```

あるルールとその後続のルールがまったく同じで、いずれもすべて同じ条件が設定されている場合、後続のルールは回避されます。次に例を示します。

```
Rule 1: do not decrypt VLAN 1 URL www.example.com
Rule 2: do not decrypt VLAN 1 URL www.example.com
```

条件が 1 つでも異なる場合は、後続のルールが回避されることはありません。次に例を示します。

```
Rule 1: do not decrypt VLAN 1 URL www.example.com
Rule 2: do not decrypt VLAN 2 URL www.example.com
```

無効な設定の警告について

SSL ポリシーが依存する外部の設定は変更される可能性があるため、有効であった SSL ポリシー設定が無効になる場合があります。次の例について考えてみます。

- URL カテゴリ条件を含むルールで、それまで有効であったものが、URL Filtering ライセンスを持たないデバイスをターゲットにすることで無効になる場合があります。その時点で、ルールの横にエラー アイコンが表示され、ポリシーをそのデバイスに適用できなくなります。適用可能にするには、このルールを編集または削除するか、ポリシーのターゲットを変更するか、または適切なライセンスを有効にする必要があります。
- Decrypt-Resign ルールを作成した後からパッシブ インターフェイスでセキュリティ ゾーンをゾーン条件に追加した場合、ルールの横に警告アイコンが表示されます。パッシブ展開では証明書の再署名によるトラフィックの復号化はできないので、パッシブ インターフェイスをルールから削除するか、またはルール アクションを変更するまで、このルールは機能しません。
- ルールにユーザを追加した後、LDAP ユーザ認識設定を変更してそのユーザを除外すると、ユーザはアクセス コントロールの対象ユーザではなくなるため、そのルールは効果がなくなります。

SSL ルールの順序指定によるパフォーマンス向上とプリエンプション回避

ライセンス: すべて

サポートされるデバイス: シリーズ 3

SSL ポリシーのルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で、ルールを上から順にトラフィックと照合します。モニタ ルールを除き、トラフィックが一致する最初のルールがそのトラフィックを処理するルールになります。

適切な SSL ルールの順序は、ネットワーク トラフィックの処理に必要なリソースを軽減し、ルールのプリエンプションを回避します。ユーザが作成するルールはすべての組織と展開に固有のものですが、ユーザのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。

重要性が最も高いルールから最も低いルールへの順序付け

最初に、組織のニーズに適するルールを順序付けする必要があります。すべてのトラフィックに適用する必要があるプライオリティ ルールをポリシーの先頭部分付近に配置します。たとえば、ある一人のユーザからの発信トラフィックは詳細な解析用に復号化するが（Decrypt-Resign ルールを使用）、その部門の他のすべてのユーザからのトラフィックは復号化しない場合は（Do not decrypt ルールを使用）、この順序で 2 つの SSL ルールを配置します。

特定のルールから一般的なルールへの順序付け

特定のルール、つまり、処理するトラフィックを狭く定義するルールを先に配置することで、パフォーマンスを向上できます。これは、広範な条件を持つルールが多くのさまざまなタイプのトラフィックを照合し、後でより多くの特定のルールをプリエンプション処理することができるという理由からも重要です。

ここで 1 つのシナリオとして、信頼できる CA（Good CA）が悪意のあるエンティティ（Bad CA）に間違って CA 証明書を発行してしまい、その証明書を取り消していない状況を考えてみましょう。信頼できない CA によって発行された証明書で暗号化されたトラフィックはブロックしたいが、信頼できる CA の信頼チェーン内にあるそれ以外のトラフィックは許可したいとします。ここで必要となるのは、CA 証明書およびすべての中間 CA 証明書をアップロードし、その後に次のようにルールを順序付けることです。

```
Rule 1: Block issuer CN=www.badca.com
Rule 2: Do not decrypt issuer CN=www.goodca.com
```

ルールを入れ替える場合は次のようになります。

```
Rule 1: Do not decrypt issuer CN=www.goodca.com
Rule 2: Block issuer CN=www.badca.com
```

最初のルールは Good CA によって信頼されたすべてのトラフィックに一致し、その中には Bad CA によって信頼されたトラフィックも含まれます。どのトラフィックも 2 番目のルールに一致しないため、悪意のあるトラフィックはブロックされずに許可される可能性があります。

証明書でピニングしたサイトからのトラフィックを許可するルールの配置

証明書のピニングを行うと、SSL セッションが確立される前に、サーバの公開キー証明書が、サーバに既に関連付けられているブラウザの証明書と一致しているかどうかを、クライアントのブラウザが強制的に確認します。Decrypt - Resign アクションにはサーバ証明書を変更してからクライアントに渡すという動作が含まれているため、ブラウザが既にその証明書をピニングしている場合は、変更された証明書が拒否されます。

たとえば、クライアント ブラウザが、証明書ピニングを使用するサイト `windowsupdate.microsoft.com` に接続されており、そのトラフィックと一致する SSL ルールを Decrypt - Resign アクションを使用して設定すると、システムはサーバ証明書に再署名してから、クライアント サーバに渡します。この変更されたサーバ証明書は、ブラウザでピニングした `windowsupdate.microsoft.com` の証明書と一致しないため、クライアント ブラウザは接続を拒否します。

このトラフィックを許可するには、サーバ証明書の共通名または識別名と突き合わせるように、Do not decrypt アクションを使用して SSL ルールを設定します。SSL ポリシーでは、このルールを、トラフィックと一致するすべての Decrypt - Resign ルールの前に配置してください。Web サイトに正常に接続された後で、クライアント ブラウザから、ピニングされた証明書を取得できます。接続が成功した場合も、失敗した場合も、ログに記録された接続イベントから証明書を表示できます。

トラフィックを復号化するルールは後方に配置する

トラフィックの復号化はリソースを必要とする処理なので、これを実行しないルール（Do not decrypt、Block）を実行するルール（Decrypt-Known Key、Decrypt-Resign）より前に配置することで、パフォーマンスが向上する場合があります。この理由は、トラフィック復号化のコマンドには多量のリソースを消費するものがあるからです。また Block ルールは、復号化やインスペクションの対象となるはずのトラフィックをそらす可能性があります。他の要素がすべて同等、つまり、より重要なものがなくプリエンプションが問題ではない場合にルールのセットを与えると仮定すると、次の順序でルールを配置することを検討します。

- 一致する接続はロギングするが、トラフィックで他のアクションは実行しないモニタ ルール
- それ以上のインスペクションなしでトラフィックをブロックする Block ルール

- 暗号化トラフィックを復号化しない Do not decrypt ルール
- 既知の秘密キーを使用して着信トラフィックを復号化する Decrypt-Known Key ルール
- サーバ証明書の再署名によって発信トラフィックを復号化する Decrypt-Resign ルール

パフォーマンスを改善する SSL インスペクション設定

ライセンス: すべて

サポートされるデバイス: シリーズ 3

複雑な SSL ポリシーおよびルールのコマンドには、多量のリソースを消費するものがあります。SSL ポリシーが適用されると、システムはすべてのルールをまとめて評価し、ネットワーク トラフィックの評価にターゲット デバイスが使用する 1 つの拡張セットとして一連の条件を統合します。ターゲット デバイスでサポートされる SSL ルールの最大数を超えていることを警告するポップアップ ウィンドウが表示される場合があります。この最大値は、デバイスの物理メモリやプロセッサ数などの、さまざまな要因によって異なります。

ルールの単純化

次のガイドラインは、SSL ルールの単純化とパフォーマンスの向上に役立ちます。

- ルールを構築するときは、条件内で使用する個々の要素は可能な限り少なくします。たとえば、ネットワーク条件では、個々の IP アドレスではなく IP アドレス ブロックを使用します。ポート条件では、ポート範囲を使用します。アプリケーション制御および URL フィルタリングを実行する場合はアプリケーション フィルタと URL カテゴリおよびレピュテーションを使用し、ユーザ制御を実行する場合は LDAPユーザ グループを使用します。

  SSL ルール条件で使用するオブジェクトに要素を結合してもパフォーマンスは向上しないことに注意してください。たとえば、50 の個別の IP アドレスを含むネットワーク オブジェクトを使用しても、その条件内のそれらの IP アドレスに対するものを含む、組織的な（パフォーマンスではない）利点が個別に与えられるだけです。

- できる限り、セキュリティ ゾーンごとにルールを制限します。デバイスのインターフェイスがゾーン制限されたルールのゾーンの 1 つにない場合、ルールはそのデバイスのパフォーマンスに影響を与えません。
- ルールを過度に設定しないでください。1 つの条件が処理するトラフィックに一致するのに十分な場合は、2 つ使用しないでください。

トラフィック復号化の設定

トラフィック復号化を設定する際は、次の注意事項に従ってください。

- トラフィックの復号化は、トラフィックを復号化してアクセス コントロールによるチェックを実行するため、リソースを必要とする処理です。処理対象を絞り込んだ復号化ルールを作成することは、処理対象が広範な復号化ルールよりも復号化するトラフィック量が減るので、その結果として、トラフィック復号化に必要な処理のリソースも削減されます。トラフィックをいったん復号化した後にアクセス コントロール ルールを使用して許可またはブロックするのではなく、暗号化トラフィックはできるだけブロックするか復号化しないことを選択するようにします。
- ルート発行元 CA に基づいてトラフィックを信頼するように証明書ステータスの条件を設定する場合は、ルート CA 証明書およびルート CA 信頼チェーン内のすべての中間 CA 証明書を SSL ポリシーにアップロードするようにします。信頼できる CA の信頼チェーン内のすべてのトラフィックは復号化なしで許可されるようになり、不要な復号化は実施されません。

SSL ルールを使用したトラフィック復号化の調整

デバイスで検査されるすべての暗号化トラフィックには、基本的な SSL ルールに基づいたアクションが適用されます。暗号化トラフィックをより詳細に復号化および制御するには、特定タイプのトラフィックの処理およびログ記録を制御するルール条件を設定します。各 SSL ルールには 0 個、1 個、または複数の条件を設定できますが、トラフィックに SSL ルールが適用されるのは、そのルールのすべての条件にトラフィックが一致する場合のみです。

注 トラフィックがルールに一致すると、そのルールのアクションがトラフィックに適用されます。ログの記録が指定されている場合、接続が終了した時点でトラフィックに関するログが記録されます。詳細については、ルール アクションを使用した暗号化トラフィックの処理と検査の決定（21-9 ページ）および暗号化された接続のロギング（38-14 ページ）を参照してください。

各ルール条件には、照合するトラフィックのプロパティを 1 つまたは複数指定できます。たとえば、以下のプロパティを指定できます。

- 通過するセキュリティ ゾーン、IP アドレスおよびポート、送信元または宛先の国、送信元または宛先の VLAN などのトラフィック フロー
- 検出された IP アドレスに関連付けられたユーザ
- トラフィックで検出されたアプリケーションなどのトラフィック ペイロード
- 接続の暗号化に使用された SSL/TLS プロトコル バージョン、暗号スイート、サーバ証明書などの接続暗号化
- サーバ証明書の識別名に指定された URL のカテゴリおよびレピュテーション

詳細については、次の項を参照してください。

- SSL ルールによる復号可能接続のロギング（38-14 ページ）
- ネットワーク ベースの条件による暗号化トラフィックの制御（22-2 ページ）
- レピュテーションによる暗号化トラフィックの制御（22-10 ページ）
- 暗号化のプロパティに基づいたトラフィックの制御（22-21 ページ）

ネットワーク ベースの条件による暗号化トラフィックの制御

ライセンス： すべて

サポートされるデバイス： シリーズ 3

*SSL ポリシー*に追加する SSL *ルール*により、暗号化トラフィックの処理やログ記録を詳細に制御できます。ネットワークベースの条件を使用して、ネットワークを通過する暗号化トラフィックを管理できます。以下の条件を使用できます。

- 送信元と宛先のセキュリティ ゾーン
- 送信元と宛先の IP アドレスまたは地理的位置
- パケット最内部の VLAN タグ
- 送信元と宛先のポート

ネットワークベースの複数の条件を組み合わせたり、他のタイプの条件と組み合わせたりして、SSL ルールを作成できます。これらの SSL ルールは単純にも複雑にも設定でき、複数の条件を使用してトラフィックを照合および検査できます。SSL ルールの詳細については、SSL ルール クイック スタート ガイド（21-1 ページ）を参照してください。

詳細については、次の項を参照してください。

- ネットワーク ゾーンによる暗号化トラフィックの制御（22-2 ページ）
- ネットワークまたは地理的位置による暗号化トラフィックの制御（22-4 ページ）
- 暗号化された VLAN トラフィックの制御（22-6 ページ）
- ポートによる暗号化トラフィックの制御（22-7 ページ）

ネットワーク ゾーンによる暗号化トラフィックの制御

ライセンス： すべて

サポートされるデバイス： シリーズ 3

SSL ルールでゾーン条件を設定すると、暗号化トラフィックの送信元および宛先のセキュリティ ゾーンに応じてそのトラフィックを制御できます。

*セキュリティ ゾーン*とは、1 つ以上のインターフェイスの論理グループを指します。ゾーン内のインターフェイスが複数のデバイス間に配置される場合もあります。デバイスの初回セットアップ時に選択する*検出モード*オプションによって、デバイスで最初に設定されるインターフェイスおよびこれらのインターフェイスが属するセキュリティ ゾーンが決定されます。

単純な例として、**インライン**検出モードを選択したデバイスでは、Defense Center により内部と外部の 2 つのゾーンが作成され、そのデバイスの最初のインターフェイスのペアがそれらのゾーンに割り当てられます。内部側ネットワークに接続されたホスト群が、保護されたアセットに相当します。

このシナリオを拡張すると、同等に設定された追加デバイス（同じ Defense Center によって管理されるもの）を展開して、複数の異なるロケーションで同様のリソースを保護できます。最初のデバイスと同様に、これらのデバイスも内部セキュリティ ゾーンのアセットを保護します。

ヒント 内部（または外部）のすべてのインターフェイスを 1 つのゾーンにグループ化する必要はありません。展開方法およびセキュリティ ポリシーに適したグループ化を選択できます。ゾーン作成の詳細については、セキュリティ ゾーンの操作（3-42 ページ）を参照してください。

この展開では、これらのホストにインターネットへの無制限アクセスを提供できますが、着信する暗号化トラフィックを復号化および検査してホストを保護しなければなりません。

SSL インスペクションでこれを実現するには、[Destination Zone] を [Internal] に設定したゾーン条件を SSL ルールに定義します。この単純な SSL ルールでは、内部ゾーンのいずれかのインターフェイスからデバイスを離れるトラフィックが照合されます。

より複雑なルールを作成する場合は、1 つのゾーン条件で [Source Zones] および [Destination Zones] それぞれに対し、最大 50 のゾーンを追加できます。

- 特定のゾーンのインターフェイスからデバイスを*離れる*暗号化トラフィックを照合するには、そのゾーンを [Destination Zones] に追加します。

  パッシブに展開されたデバイスはトラフィックを送信しないので、パッシブ インターフェイスで構成されるゾーンを [Destination Zones] 条件で使用することはできません。
- 特定のゾーンのインターフェイスからデバイスに*入る*暗号化トラフィックを照合するには、そのゾーンを [Source Zones] に追加します。

送信元（Source）ゾーン条件と宛先（Destination）ゾーン条件の両方をルールに追加する場合、送信元ゾーンから発信され**かつ**宛先ゾーンを介して出力されるトラフィックにルールが適用されます。

ゾーン内のすべてのインターフェイスが同じタイプ（インライン、パッシブ、スイッチド、またはルーテッド）である必要があるため、SSL ルールのゾーン条件で使用されているすべてのゾーンが同じタイプでなければならないことに注意してください。つまり、異なるタイプのゾーンを送信元/宛先とする暗号化トラフィックを照合する単一ルールを定義することはできません。

ゾーンにインターフェイスが含まれていないなど、無効な設定が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。

ゾーン条件に基づいて暗号化トラフィックを制御するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1 ゾーンに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（21-4 ページ）を参照してください。

ステップ 2 SSL ルール エディタで、[Zones] タブを選択します。

[Zones] タブが表示されます。

ステップ 3 [Available Zones] で、追加するゾーンを選択します。

追加するゾーンを検索するには、[Available Zones] リストの上にある [Search by name] プロンプトをクリックし、ゾーン名を入力します。ゾーン名の入力を開始するとリストが更新され、一致するゾーンが表示されます。

ゾーンをクリックして選択します。複数のゾーンを選択するには、Shift キーまたは Ctrl キーを使用します。すべてのゾーンを選択するには、右クリックして [Select All] を選択します。

ステップ 4 [Add to Source] または [Add to Destination] をクリックして、選択したゾーンを適切なリストに追加します。

選択したゾーンをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5　ルールを保存するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

ネットワークまたは地理的位置による暗号化トラフィックの制御

ライセンス： すべて

サポートされるデバイス： シリーズ 3

SSL ルールでネットワーク条件を設定すると、暗号化トラフィックの送信元および宛先の IP アドレスに応じてそのトラフィックを制御および復号化できます。次のいずれかの操作を実行できます。

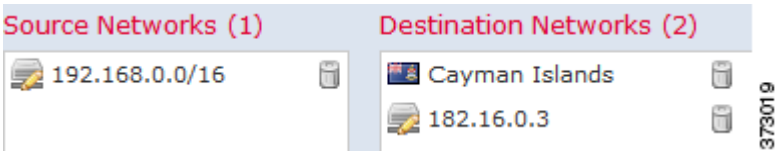
- 制御する暗号化トラフィックの送信元および宛先の IP アドレスを明示的に指定する。
- IP アドレスを地理的位置に関連付ける位置情報機能を使用して、その送信元または宛先の国または大陸に基づいて暗号化トラフィックを制御する。

ネットワークベースの SSL ルールの条件を作成する場合、IP アドレスと地理的位置を手動で指定できます。または、ネットワークおよび位置情報の*オブジェクト*を使用してネットワーク条件を設定することもできます。これらのオブジェクトは、いくつかの IP アドレス、アドレス ブロック、国、大陸などに名前を付けて再利用可能にしたものを指します。

ヒント　ネットワーク オブジェクトや位置情報オブジェクトを作成しておくと、それを使用して SSL ルールを作成したり、Web インターフェイスのさまざまな場所で IP アドレスを表すオブジェクトとして使用したりできます。これらのオブジェクトはオブジェクト マネージャを使用して作成できます。また、SSL ルールの設定時にネットワーク オブジェクトを作成することもできます。詳細については、再利用可能なオブジェクトの管理（3-1 ページ）を参照してください。

地理的位置別にトラフィックを制御するルールを作成する場合は、確実に最新の位置情報データを使用してトラフィックをフィルタ処理する必要があります。このため、CiscoではDefense Centerの位置情報データベース（GeoDB）を定期的に更新することを**強く**推奨しています。地理情報データベースについて（66-30 ページ）を参照してください。

次の図は、内部ネットワークから発信され、ケイマン諸島（Cayman Islands）または海外にある持ち株会社のサーバ（182.16.0.3）のリソースにアクセスしようとする暗号化接続をブロックする SSL ルールのネットワーク条件を示しています。



この例では、持ち株会社のサーバの IP アドレスを手動で指定し、ケイマン諸島の IP アドレスを表すシステム提供の位置情報オブジェクト Cayman Islands を使用しています。

1 つのネットワーク条件で [Source Networks] および [Destination Networks] それぞれに最大 50 の項目を追加でき、ネットワークベースの設定と位置情報ベースの設定を組み合わせることができます。

- 特定の IP アドレスまたは地理的位置からの暗号化トラフィックを照合するには、[Source Networks] を設定します。
- 特定の IP アドレスまたは地理的位置への暗号化トラフィックを照合するには、[Destination Networks] を設定します。

送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信され**かつ**宛先 IP アドレスに送信される暗号化トラフィックにルールが適用されます。

無効なネットワーク条件設定が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。

ネットワークまたは地理的位置の条件に応じてトラフィックを制御するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　ネットワークに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（21-4 ページ）を参照してください。

ステップ 2　SSL ルール エディタで、[Zones] タブを選択します。

[Networks] タブが表示されます。

ステップ 3　[Available Networks] で、追加するネットワークを選択します。

- [Networks] タブをクリックすると追加可能なネットワーク オブジェクトとグループが表示され、[Geolocation] タブをクリックすると位置情報オブジェクトが表示されます。
- ここでネットワーク オブジェクトを作成してリストに追加するには、[Available Networks] リストの上にある追加アイコン（  ）をクリックし、ネットワーク オブジェクトの操作（3-4 ページ）の手順に従います。
- 追加するネットワーク オブジェクトまたは位置情報オブジェクトを検索するには、適切なタブを選択し、[Available Networks] リストの上にある [Search by name or value] プロンプトをクリックして、オブジェクト名またはオブジェクトのいずれかの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

オブジェクトをクリックして選択します。複数のオブジェクトを選択するには、Shift キーまたは Ctrl キーを使用します。すべてのオブジェクトを選択するには、右クリックして [Select All] を選択します。

ステップ 4　[Add to Source] または [Add to Destination] をクリックして、選択したオブジェクトを適切なリストに追加します。

選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5　手動で指定する送信元または宛先の IP アドレスまたはアドレス ブロックを追加します。

[Source Networks] リストまたは [Destination Networks] リストの下にある [Enter an IP address] プロンプトをクリックし、IP アドレスまたはアドレス ブロックを入力して [Add] をクリックします。

ステップ 6　ルールを保存するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

暗号化された VLAN トラフィックの制御

ライセンス： すべて

サポートされるデバイス： シリーズ 3

SSL ルールで VLAN 条件を設定すると、トラフィックの VLAN タグに応じてそのトラフィックを制御できます。VLAN によるパケットの識別に最内部の VLAN タグが使用されます。

VLAN ベースの SSL ルール条件を作成するときは、1 ～ 4094 の VLAN タグを手動で指定できます。または、VLAN タグ *オブジェクト*を使用して VLAN 条件を設定することもできます。VLAN タグ オブジェクトとは、いくつかの VLAN タグに名前を付けて再利用可能にしたものを指します。

ヒント　VLAN タグ オブジェクトを作成しておくと、それを使用して SSL ルールを作成したり、Web インターフェイスのさまざまな場所で VLAN タグを表すオブジェクトとして使用したりできます。VLAN タグ オブジェクトはオブジェクト マネージャを使用して作成できます。また、アクセス コントロール ルールの設定時に作成することもできます。詳細については、VLAN タグ オブジェクトの操作（3-14 ページ）を参照してください。

次の図は、特定の公開 VLAN（VLAN タグ オブジェクト グループで指定）および手動で追加した VLAN「42」上の暗号化トラフィックに一致する SSL ルールの VLAN タグ条件を示しています。

1 つの VLAN タグ条件で、[Selected VLAN Tags] に最大 50 の項目を追加できます。無効な VLAN タグ条件設定が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。

VLAN タグに基づいてトラフィックを制御するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　VLAN タグに応じたトラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（21-4 ページ）を参照してください。

ステップ 2　SSL ルール エディタで、[VLAN Tags] タブを選択します。

[VLAN Tags] タブが表示されます。

ステップ 3　[Available VLAN Tags] で、追加する VLAN を選択します。

- ここで VLAN タグ オブジェクトを作成してリストに追加するには、[Available VLAN Tags] リストの上にある追加アイコン（ ）をクリックし、VLAN タグ オブジェクトの操作（3-14 ページ）の手順に従います。

- 追加する VLAN タグ オブジェクトおよびグループを検索するには、[Available VLAN Tags] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクト名または オブジェクトの VLAN タグの値を入力します。入力を開始するとリストが更新され、一致する オブジェクトが表示されます。

オブジェクトをクリックして選択します。複数のオブジェクトを選択するには、Shift キーまたは Ctrl キーを使用します。すべてのオブジェクトを選択するには、右クリックして [Select All] を選択します。

ステップ 4　[Add to Rule] をクリックして、選択したオブジェクトを [Selected VLAN Tags] リストに追加します。

選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5　手動で指定する VLAN タグを追加します。

[Selected VLAN Tags] リストの下にある [Enter a VLAN Tag] プロンプトをクリックし、VLAN タグまたはその範囲を入力して、[Add] をクリックします。1 から 4094 までの任意の VLAN タグを指定できます。VLAN タグの範囲を指定するにはハイフンを使用します。

ステップ 6　ルールを保存するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

ポートによる暗号化トラフィックの制御

ライセンス： すべて

サポートされるデバイス： シリーズ 3

SSL ルールでポート条件を設定すると、暗号化トラフィックの送信元および宛先の TCP ポートに応じてそのトラフィックを制御できます。ポートベースの SSL ルールの条件を作成するときは、手動で TCP ポートを指定できます。または、ポート *オブジェクト*を使用してポート条件を設定することもできます。ポート オブジェクトとは、いくつかのポートに名前を付けて再利用可能にしたものを指します。

ヒント　ポート オブジェクトを作成しておくと、それを使用して SSL ルールを作成したり、Web インターフェイスのさまざまな場所でポートを表すオブジェクトとして使用したりできます。ポート オブジェクトは、オブジェクト マネージャを使用して作成できます。また、SSL ルールの設定時に作成することもできます。詳細については、ポート オブジェクトの操作（3-13 ページ）を参照してください。

1 つのネットワーク条件で [Selected Source Ports] および [Selected Destination Ports] リストそれぞれに対し、最大 50 の項目を追加できます。

- 特定の TCP ポート*から*の暗号化トラフィックを照合するには、[Selected Source Ports] を設定します。
- 特定の TCP ポート*へ*の暗号化トラフィックを照合するには、[Selected Destination Ports] を設定します。
- [Selected Source Ports] および [Selected Destination Ports] の両方を設定すると、特定の送信元（Source）TCP ポートから発信されかつ特定の宛先（Destination）TCP ポートに送信される暗号化トラフィックが照合されます。

[Selected Source Ports] および [Selected Destination Ports] リストで設定できるのは TCP ポートだけです。非 TCP ポートを含んでいるポート オブジェクトは、[Available Ports] リストでグレー表示されます。

無効なポート条件が検出されると、警告アイコンが表示されます。たとえば、既存のポート オブジェクトをオブジェクト マネージャで編集すると、それらのオブジェクト グループを使用するルールが無効になります。アイコンの上にポインタを置くと詳細が表示されます。

ポート条件に基づいてトラフィックを制御するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　TCP ポートに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（21-4 ページ）を参照してください。

ステップ 2　SSL ルール エディタで、[Ports] タブを選択します。

[Ports] タブが表示されます。

ステップ 3　[Available Ports] で、追加する TCP ポートを選択します。

- ここで TCP ポート オブジェクトを作成してリストに追加するには、[Available Ports] リストの上にある追加アイコン（  ）をクリックし、ポート オブジェクトの操作（3-13 ページ）の手順に従います。
- 追加する TCP ベースのポート オブジェクトおよびグループを検索するには、[Available Ports] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクトの名前またはオブジェクトのポートの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。たとえば、「443」と入力すると、システム提供の HTTPS ポート オブジェクトがDefense Centerに表示されます。

TCP ベースのポート オブジェクトをクリックして選択します。複数のオブジェクトを選択するには、Shift キーまたは Ctrl キーを使用します。すべてのオブジェクトを選択するには、右クリックして [Select All] を選択します。非 TCP ベースのポートを含んでいるオブジェクトは、ポート条件に追加できません。

ステップ 4　[Add to Source] または [Add to Destination] をクリックして、選択したオブジェクトを適切なリストに追加します。

選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5　送信元または宛先のポートを手動で指定するには、[Selected Source Ports] または [Selected Destination Ports] リストの下にある [Port] にポート番号を入力します。0 ～ 65535 の値を持つ 1 つのポートを指定できます。

ステップ 6　[Add] をクリックします。

Defense Centerでは、無効なポート設定はルール条件に追加されません。

ステップ 7　ルールを保存するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

ユーザ ベースの暗号化トラフィックの制御

ライセンス： Control

サポートされるデバイス： シリーズ 3

SSL ルールでユーザ条件を設定すると、Microsoft Active Directory サーバから取得されるユーザに応じてそのトラフィックを制御できます。SSL ルールのユーザ条件をでは、ホストにログインする LDAP ユーザに基づいてトラフィックのネットワーク通過を許可する*ユーザ制御*が可能になります。

ユーザ制御は、*アクセス制御されたユーザ*と IP アドレスを関連付けることによって機能します。この機能では、ホストにログインまたはホストからログアウトするとき、または他の理由で Active Directory 認証を行うときに、特定のユーザをモニタするエージェントを展開します。たとえば、アプリケーションやサービスでの認証を Active Directory で一元管理している組織では、このトラフィック制御方法を検討できます。

ユーザ条件を設定した SSL ルールとトラフィックを一致させるには、モニタ対象のセッションにおける送信元または宛先ホストの IP アドレスと、ログインする「アクセス制御されたユーザ」を関連付ける必要があります。この機能では、特定のユーザまたはユーザ グループに基づいてトラフィックを制御できます。

複数のユーザ条件を組み合わせたり、他のタイプの条件と組み合わせたりして、SSL ルールを作成できます。これらの SSL ルールは単純にも複雑にも設定でき、複数の条件を使用してトラフィックを照合および検査できます。SSL ルールの詳細については、SSL ルールの概要と作成（21-4 ページ）を参照してください。

ユーザ制御機能を使用するには、Control ライセンスが必要です。また、サポートされるのは LDAP ユーザとグループ（*アクセス制御されたユーザ*）だけで、Microsoft Active Directory サーバをモニタするユーザ エージェントからのログインおよびログアウト レコードが使用されます。

ユーザ条件を含む SSL ルールを作成する前に、組織内の少なくとも 1 つの Microsoft Active Directory サーバと Defense Center との間の接続を設定しておく必要があります。この設定は認証オブジェクトと呼ばれ、サーバの接続設定と認証フィルタ設定が含まれています。また、ユーザ条件で使用できるユーザも指定されます。詳細については、アクセス制御されたユーザおよび LDAP ユーザのメタデータの取得（17-5 ページ）を参照してください。

さらに、ユーザ エージェントをインストールする必要もあります。エージェントは、Active Directory 資格情報で認証するユーザをモニタし、このようなログインのレコードを Defense Center に送信します。これらのレコードによりユーザが IP アドレスに関連付けられ、これに基づいてユーザ条件を含んでいる SSL ルールが照合可能になります。詳細については、Active Directory のログインを報告するためのユーザ エージェントの使用（17-11 ページ）を参照してください。

ユーザ条件に基づいて暗号化トラフィックを制御するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　ユーザに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（21-4 ページ）を参照してください。

ステップ 2　SSL ルール エディタで、[Users] タブを選択します。

[Users] タブが表示されます。

ステップ 3　追加するユーザを検索するには、[Available Users] リストの上にある [Search by name or value] プロンプトをクリックし、ユーザ名を入力します。入力を開始するとリストが更新され、一致するユーザが表示されます。

ユーザをクリックして選択します。複数のユーザを選択するには、Shift キーまたは Ctrl キーを使用します。すべてのユーザを選択するには、右クリックして [Select All] を選択します。

ステップ 4　[Add to Rule] をクリックして、選択したユーザを [Selected Users] リストに追加します。

選択したユーザをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5　ルールを保存するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

レピュテーションによる暗号化トラフィックの制御

ライセンス： ControlまたはURL Filtering

サポートされるデバイス： シリーズ 3

SSL ルールでレピュテーション ベース条件を設定すると、ネットワーク トラフィックをコンテキスト化して状況に応じて制限することで、ネットワーク通過を許可する暗号化トラフィックを管理できます。SSL ルールでのレピュテーション ベースの制御には、以下のタイプがあります。

- アプリケーション条件による *アプリケーション制御* では、個々のアプリケーションだけでなく、アプリケーションの基本的な特性（タイプ、リスク、ビジネスとの関連性、およびカテゴリ）に基づいてアプリケーション トラフィックを制御できます。
- URL 条件では、Web サイトに割り当てられたカテゴリおよびレピュテーションに基づいて Web トラフィックを制御できます。

レピュテーションベースの複数の条件を組み合わせたり、他のタイプの条件と組み合わせたりして、SSL ルールを作成できます。これらの SSL ルールは単純にも複雑にも設定でき、複数の条件を使用してトラフィックを照合および検査できます。

次の表は、レピュテーション ベースの SSL インスペクションに必要なライセンス、デバイス、およびDefense Centerを示しています。

表 22-1　レピュテーション ベースの SSL ルールのライセンスとアプライアンスの要件

要件	アプリケーション管理	URL フィルタリング（カテゴリおよびレピュテーション）
license	Control	URL Filtering
devices	シリーズ 3	シリーズ 3
Defense Center	シリーズ 3、仮想	シリーズ 3、仮想

詳細については、次の項を参照してください。

- アプリケーション ベースの暗号化トラフィックの制御（22-11 ページ）
- URL カテゴリおよびレピュテーションによる暗号化トラフィックの制御（22-17 ページ）

アプリケーション ベースの暗号化トラフィックの制御

ライセンス: Control

サポートされるデバイス: シリーズ 3

FireSIGHT システムは、暗号化された IP トラフィックを分析するときに、ネットワーク上で一般的に使用されている暗号化アプリケーションを識別および分類してから暗号化セッションを復号化します。こうした検出ベースの *アプリケーション認識*機能を使用して、ネットワーク上の暗号化されたアプリケーション トラフィックを制御できます。

SSL ルールのアプリケーション条件では、この *アプリケーション制御*を行います。1 つのルールにおいて、トラフィックの制御対象とするアプリケーションを複数の方法で指定できます。

- 各アプリケーションを個別に選択する（カスタム アプリケーションを含む）。
- システム提供の *アプリケーション フィルタ*を使用する。このフィルタは、基本的な特性（タイプ、リスク、ビジネスとの関連性、およびカテゴリ）に基づいてアプリケーションをグループ化して名前を付けたものを指します。
- カスタム アプリケーション フィルタを作成して使用する。このフィルタでは、任意の方法でアプリケーションをグループ化できます（カスタム アプリケーションを含む）。

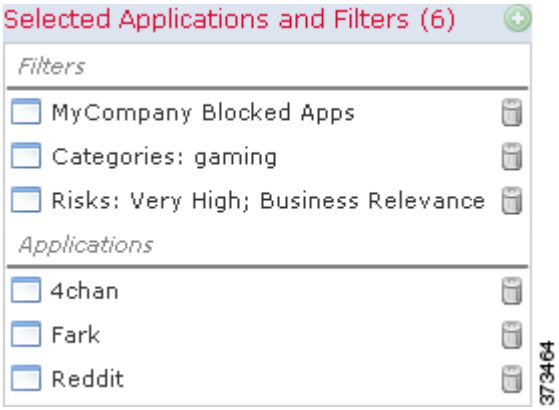
注 アクセス コントロール ルールを使用してアプリケーション トラフィックをフィルタ処理する場合、フィルタ条件としてアプリケーション タグを使用できます。ただし、暗号化トラフィックはアプリケーション タグでフィルタ処理できません。暗号化トラフィックのアプリケーションを検出するにはタグ付きの **SSL プロトコル**である必要があり、このタグが付けられていないアプリケーションは、非暗号化トラフィックまたは復号化されたトラフィックでしか検出できません。

アプリケーション フィルタを利用すると、SSL ルールのアプリケーション条件を簡単に作成できます。これによりポリシーの作成と管理が簡素化され、Web トラフィックを意図したとおりに制御できます。たとえば、リスクが高くビジネスとの関連性の低いアプリケーションをすべて識別して復号化する SSL ルールを作成できます。ユーザがこれらのアプリケーションの使用を試みると、アクセス コントロールによってセッションが復号化されて検査されます。

さらに、Ciscoでは、システムおよび脆弱性データベース（VDB）の更新を通して頻繁にディテクタを更新し追加しています。独自のディテクタを作成して、検出するアプリケーションの特性（リスク、関連性など）を割り当てることも可能です。アプリケーション特性に基づくフィルタを使用すると、最新のディテクタを使用してアプリケーション トラフィックをモニタできます。

アプリケーション条件を設定した SSL ルールとトラフィックを一致させるには、[Selected Applications and Filters] リストに追加したいずれかのアプリケーションまたはフィルタにトラフィックが一致する必要があります。

次の図は、MyCompany のアプリケーション、リスクが高くビジネスとの関連性の低いすべてのアプリケーション、ゲーム アプリケーション、およびいくつかの指定アプリケーションからなるカスタム グループを復号化する、SSL ルールのアプリケーション条件を示しています。



1 つのアプリケーション条件で [Selected Applications and Filters] リストに最大 50 の項目を追加できます。1 つの項目として扱われるものは以下のとおりです。

- [Application Filters] リストにある 1 つまたは複数のフィルタ（個別または組み合わせたもの）。この項目は、特性を基準にグループ化されたアプリケーションのセットです。
- [Available Applications] リストにあるアプリケーションの検索結果を保存することで作成されたフィルタ。この項目は、アプリケーション名の一部の一致によってグループ化されたアプリケーションのセットです。
- [Available Applications] リストにある個別のアプリケーション。

Web インターフェイス上では、条件に追加したフィルタが個別に追加したアプリケーションの上に一覧表示されます。

SSL ポリシーの適用時には、一致するアプリケーションのリストがルールごとに生成されます。このため、重複するフィルタと個別指定のアプリケーションを使用して、意図したとおりのアプリケーション セットにポリシーを適用できます。

詳細については、次の項を参照してください。

- アプリケーション フィルタと暗号化トラフィックの照合（22-12 ページ）
- 個々のアプリケーションとトラフィックの照合（22-13 ページ）
- SSL ルールへのアプリケーション条件の追加（22-15 ページ）
- 暗号化されたアプリケーションの制御に対する制限（22-16 ページ）

アプリケーション フィルタと暗号化トラフィックの照合

ライセンス： Control

サポートされるデバイス： シリーズ 3

SSL ルールのアプリケーション条件を作成するには、[Application Filters] リストを使用して、照合するトラフィックの特性を基にアプリケーションをグループ化します。

アプリケーションの検出基準について詳しくは、アプリケーション検出について（45-11 ページ）を参照してください。これらの基準をフィルタとして使用したり、独自の組み合わせでカスタム フィルタを作成したりしてアプリケーションを制御できます。

SSL ルールでのアプリケーション フィルタの機能は、オブジェクト マネージャを使用した再利用可能なカスタム アプリケーション フィルタの作成と同じです（アプリケーション フィルタの操作（3-16 ページ）を参照してください）。また、アクセス コントロール ルールの設定時に作成する各種のフィルタを、新規のフィルタとして保存して再利用することもできます。ユーザ作成のフィルタを入れ子にすることはできないため、別のユーザ定義フィルタを含んでいるフィルタを保存することはできません。

フィルタの組み合わせについて

フィルタを単独または他のフィルタと組み合わせて選択すると、[Available Applications] リストが更新され、選択したフィルタの条件を満たすアプリケーションだけが表示されます。システム提供のフィルタは自由に組み合わせることができますが、カスタム フィルタを組み合わせることはできません。

システムは、OR 演算を使用して同じフィルタ タイプの複数のフィルタをリンクします。たとえば、Risks（リスク）タイプの下の Medium（中）および High（高）フィルタを選択すると、結果として次のようなフィルタになります。

```
Risk: Medium OR High
```

Medium フィルタに 110 個のアプリケーション、High フィルタに 82 個のアプリケーションが含まれる場合、[Available Applications] リストにはこれら 192 個のアプリケーションがすべて表示されます。

システムは AND 演算を使用して、異なるタイプのフィルタをリンクします。たとえば Risks タイプで Medium および High フィルタを選択し、Business Relevance（業務との関連性）タイプで Medium および High フィルタを選択した場合、結果として次のようなフィルタになります。

```
Risk: Medium OR High
AND
Business Relevance: Medium OR High
```

この場合、Risk タイプの Medium または High と、Business Relevance タイプの Medium または High の両方に含まれるアプリケーションだけが表示されます。

フィルタの検索および選択

フィルタを選択するには、フィルタ タイプの横にある矢印をクリックして展開し、各フィルタの横のチェック ボックスをオンまたはオフにしてアプリケーションを表示したり非表示にしたりします。Cisco提供のフィルタ タイプ（[Risks]、[Business Relevance]、[Types]、または [Categories]）を右クリックして、[Check All] または [Uncheck All] を選択することもできます。

フィルタを検索するには、[Available Filters] リストの上にある [Search by name] プロンプトをクリックし、フィルタ名を入力します。入力を開始するとリストが更新され、一致するフィルタが表示されます。

フィルタの選択が完了したら、[Available Applications] リストを使用してこれらのフィルタをルールに追加します。個々のアプリケーションとトラフィックの照合（22-13 ページ）を参照してください。

個々のアプリケーションとトラフィックの照合

ライセンス： Control

サポートされるデバイス： シリーズ 3

SSL ルールのアプリケーション条件を作成するには、[Available Applications] リストを使用して、照合するトラフィックのアプリケーションを選択します。

アプリケーションのリストの参照

作成済みの条件がない場合、検出されたすべてのアプリケーションが 100 個ずつリストに表示されます。

- アプリケーションの次のページを閲覧するには、リストの下の矢印をクリックします。
- アプリケーションの横にある情報アイコン( )をクリックするとポップアップ ウィンドウが開き、アプリケーションの特性に関する概要とインターネット検索用のリンクが表示されます。

一致するアプリケーションの検索

目的のアプリケーションを検索しやすくするため、[Available Applications] リストに表示されるアプリケーションを制限することができます。

- アプリケーションを検索するには、リストの上にある [Search by name] プロンプトをクリックし、アプリケーション名を入力します。入力を開始するとリストが更新され、一致するアプリケーションが表示されます。
- フィルタを適用して表示を制限するには、[Application Filters] リストを使用します(アプリケーション フィルタと暗号化トラフィックの照合(22-12 ページ)を参照してください)。フィルタを適用すると [Available Applications] リストが更新されます。

制限を適用すると、[Available Applications] リストの上に [All apps matching the filter] オプションが表示されます。このオプションを使用すると、制限したリストに表示されているすべてのアプリケーションをまとめて [Selected Applications and Filters] リストに追加できます。

注　[Application Filters] リストでいくつかのフィルタを選択し、さらに [Available Applications] リストでアプリケーションを検索した場合、選択フィルタと検索条件が AND 演算で結合され、両方の条件に一致するアプリケーションが [Available Applications] リストに表示されます。つまり、[All apps matching the filter] 条件には、[Available Applications] リストに表示されている個々のすべての条件と、[Available Applications] リストの上で入力された検索条件が含まれます。

条件に一致する単一アプリケーションの選択

目的のアプリケーションが見つかったら、それをクリックして選択します。複数のアプリケーションを選択するには、Shift キーまたは Ctrl キーを使用します。表示されているすべてのアプリケーションを選択するには、右クリックして [Select All] を選択します。

1 つのアプリケーション条件において、アプリケーションの個別選択で追加できる最大数は 50 です。50 を超えるアプリケーションを追加するには、複数の SSL ルールを作成するか、フィルタを使用してアプリケーションをグループ化する必要があります。

条件のフィルタに一致するすべてのアプリケーションの選択

検索または [Application Filters] リストのフィルタによる制限を適用すると、[Available Applications] リストの上に [All apps matching the filter] オプションが表示されます。

このオプションを使用すると、制限した [Available Applications] リストに表示されているすべてのアプリケーションをまとめて [Selected Applications and Filters] リストに追加できます。アプリケーションを個別に追加するのとは異なり、このアプリケーションのセットは、含まれているアプリケーションの数にかかわらず 1 項目としてカウントされます。このため、結果的に 50 を超える数のアプリケーションを条件に追加できます。

この方法でアプリケーション条件を作成すると、[Selected Applications and Filters] リストに追加したフィルタに「フィルタ タイプ + 各タイプの最大 3 フィルタの名前」形式の名前が付きます。同じタイプのフィルタが 3 個を超える場合は、その後に省略記号（...）が表示されます。たとえば次のフィルタ名には、Risks タイプの 2 つのフィルタと Business Relevance タイプの 4 つのフィルタが含まれています。

```
Risks: Medium, High Business Relevance: Low, Medium, High,...
```

[All apps matching the filter] で追加したフィルタに特定のタイプが設定されていない場合、そのタイプ名は追加したフィルタ名に使用されません。[Selected Applications and Filters] リスト内のフィルタ名の上にポインタを置くと、これらのフィルタのタイプとして [any] が表示されます。つまり、これらのフィルタ タイプはリストの表示を制限しないため、任意の値が許容されます。

1 つのアプリケーション条件には [All apps matching the filter] のインスタンスを複数追加でき、これらの各インスタンスは [Selected Applications and Filters] リストで個別の項目としてカウントされます。たとえば、リスクが高いアプリケーションのすべてを 1 つの項目として追加し、この選択をクリアしてから、ビジネスとの関連性の低いアプリケーションのすべてをもう 1 つの項目として追加することが可能です。このアプリケーション条件に一致するのは、リスクが高いアプリケーション、またはビジネスとの関連性の低いアプリケーションになります。

SSL ルールへのアプリケーション条件の追加

ライセンス： Control

サポートされるデバイス： シリーズ 3

アプリケーション条件を設定した SSL ルールと暗号化トラフィックを一致させるには、[Selected Applications and Filters] リストに追加したいずれかのアプリケーションまたはフィルタにトラフィックが一致する必要があります。

1 つの条件に最大 50 の項目を追加することができ、条件に追加したフィルタが個別に追加したアプリケーションの上に一覧表示されます。無効なアプリケーション条件が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。

アプリケーション条件に基づいて暗号化トラフィックを制御するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　アプリケーションに応じたトラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（21-4 ページ）を参照してください。

ステップ 2　SSL ルール エディタで、[Applications] タブを選択します。

[Applications] タブが表示されます。

ステップ 3　必要に応じて、フィルタを使用して [Available Applications] リストに表示されるアプリケーション リストを限定します。

[Application Filters] リストで、1 つまたは複数のフィルタを選択します。詳細については、アプリケーション フィルタと暗号化トラフィックの照合（22-12 ページ）を参照してください。

ステップ 4　[Available Applications] で、追加するアプリケーションを選択します。

個々のアプリケーションを検索して選択したり、リストの表示を制限した場合は [All apps matching the filter] をクリックしてすべてを選択したりできます。詳細については、個々のアプリケーションとトラフィックの照合（22-13 ページ）を参照してください。

ステップ 5　[Add to Rule] をクリックして、選択したアプリケーションを [Selected Applications and Filters] リストに追加します。

選択したアプリケーションやフィルタをドラッグ アンド ドロップでリストに追加することもできます。フィルタは [Filters] という見出しの下に表示され、アプリケーションは [Applications] という見出しの下に表示されます。

ヒント　このアプリケーション条件に別のフィルタを追加する場合は、[Clear All Filters] をクリックして既存の選択をクリアしておきます。

ステップ 6　ルールを保存するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

暗号化されたアプリケーションの制御に対する制限

ライセンス： Control

サポートされるデバイス： シリーズ 3

アプリケーション制御を実行する場合は、次の点に注意してください。

暗号化されたアプリケーションの識別

このシステムでは、StartTLS を使用して暗号化される非暗号化アプリケーションを識別できます。これには、SMTPS、POPS、FTPS、TelnetS、IMAPS などのアプリケーションが含まれます。また、サーバ証明書サブジェクトの識別名の値または TLS クライアントの hello メッセージの Server Name Indication に基づいて、特定の暗号化アプリケーションを識別します。

アプリケーション識別の速さ

暗号化トラフィックのアプリケーション制御は、以下のすべての処理が完了するまで実行されません。

- 暗号化された接続がクライアントとサーバ間で確立される。
- 暗号化セッション内のアプリケーションがシステムにより識別される。

この識別が行われるのは、サーバ証明書が交換された後です。ハンドシェイク中に交換されるトラフィックでアプリケーションの識別が完了する前に、アプリケーション条件を含んでいる SSL ルール内の他のすべての条件に一致してしまうと、SSL ポリシーによりそのパケットの通過が許可されます。このため、アプリケーションを識別できるように接続が確立されます。この問題の影響を受けるルールには、情報アイコン（ⓘ）が表示されます。

システムによる識別が完了すると、アプリケーション条件に一致する残りのセッション トラフィックに SSL ルールのアクションが適用されます。

アプリケーション ディテクタの自動有効化

ポリシー内のアプリケーション ルール条件ごとに、少なくとも 1 つのディテクタを有効にする必要があります（ディテクタのアクティブ化と非アクティブ化（46-30 ページ）を参照）。有効になっているディテクタがないアプリケーションについては、システム提供のすべてのディテクタが自動的に有効になります。デテクタが存在しない場合は、そのアプリケーションについて最後に変更されたユーザ定義ディテクタが有効になります。

URL カテゴリおよびレピュテーションによる暗号化トラフィックの制御

ライセンス： URL Filtering

サポートされるデバイス： シリーズ 3

SSL ルールの URL 条件では、ネットワーク上のユーザからアクセス可能な暗号化 Web サイト トラフィックの処理と復号化を行います。要求された URL は、SSL ハンドシェイク時に提供される情報に基づいて検出されます。URL Filteringライセンスでは、URL の一般的な分類である *カテゴリ* と、リスク レベルである *レピュテーション* に基づいた Web サイトへのアクセス制御が可能です。

注 特定の URL に対するトラフィックの処理と復号化は、識別名の SSL ルール条件を定義することで行えます。証明書のサブジェクト識別名にある共通名属性には、サイトの URL が含まれています。詳細については、証明書の識別名による暗号化トラフィックの制御（22-21 ページ）を参照してください。

詳細については、以下を参照してください。

- レピュテーション ベースの URL ブロックの実行（22-17 ページ）
- URL 検出とブロッキングの制約事項（22-20 ページ）

レピュテーション ベースの URL ブロックの実行

ライセンス： URL Filtering

サポートされるデバイス： シリーズ 3

URL Filteringライセンスでは、要求された URL のカテゴリおよびレピュテーションに基づいて、Web サイトへのユーザ アクセスを制御できます。

- URL *カテゴリ* とは、URL の一般的な分類です。たとえば ebay.com は [Auctions] カテゴリ、monster.com は [Job Search] カテゴリに属します。1 つの URL は複数のカテゴリに属することができます。
- URL *レピュテーション* は、組織のセキュリティ ポリシーに反する目的でその URL が使用される可能性を表します。各 URL のリスク範囲は、**ハイ リスク**（レベル 1）から**有名**（レベル 5）です。

URL のカテゴリおよびレピュテーションは FireSIGHT システムがCiscoクラウドから取得するもので、これを利用して SSL ルールの URL 条件を簡単に作成できます。たとえば、[Abused Drugs] カテゴリの**ハイ リスク** URL をすべて識別してブロックする SSL ルールを作成できます。ユーザが暗号化接続でこのカテゴリおよびレピュテーションの URL にアクセスすると、そのセッションはブロックされます。

注 カテゴリとレピュテーション ベースの URL 条件の SSL ルールを使用するには、Ciscoクラウドとの通信を**有効**にしておく必要があります。これにより、Defense Centerによる URL データの取得が可能になります。詳細については、クラウド通信の有効化（64-30 ページ）を参照してください。

Ciscoクラウドのカテゴリおよびレピュテーション データを使用すると、ポリシーの作成と管理がより簡単になります。また、暗号化された Web トラフィックの制御についての信頼度も向上します。さらに、このクラウド上のデータは常に更新されて新しい URL が追加され、既存の URL も新しいカテゴリとリスクで更新されるため、常に最新の情報に基づいて URL がフィルタ処理されるようになります。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表す悪意のあるサイトは、組織でポリシーを更新したり新規ポリシーを適用したりするペースを上回って次々と現れては消える可能性があります。

次に例を示します。

- ルールですべてのゲーム サイトをブロックする場合、新しいドメインが登録されて [Gaming] に分類されると、これらのサイトをシステムで自動的にブロックできます。
- ルールですべてのマルウェアをブロックする場合、あるブログ ページがマルウェアに感染すると、クラウドはその URL のカテゴリを [Blog] から [Malware] に変更することができ、システムはそのサイトをブロックできます。
- リスクの高いソーシャル ネットワーキング サイトをブロックするルールを使用する場合、ある参加者がプロファイル ページに悪意のあるペイロードへのリンクを掲載すると、そのページのレピュテーションがクラウドで**無害なサイト**から**ハイ リスク**に変更され、システムでそれをブロックできます。

なお、URL のカテゴリやレピュテーションがクラウドで不明な場合、またはDefense Centerがクラウドと通信できない場合、カテゴリやレピュテーションに基づく URL 条件を含む SSL ルールがトリガー**されない**ことに注意してください。URL にカテゴリやレピュテーションを手動で割り当てることはできません。

次の図は、すべてのマルウェア サイト、すべてのハイ リスク サイト、およびすべての有害なソーシャル ネットワーキング サイトをブロックするアクセス コントロール ルールの URL 条件を示しています。

ヒント　トラフィックを復号化してからアクセス コントロールでブロックする場合、ユーザは警告ページをクリックして閉じることでブロックをバイパスできます。詳細については、「インタラクティブ ブロッキング アクション：ユーザが Web サイト ブロックをバイパスすることを許可する (14-11 ページ)」を参照してください。

1 つの URL 条件で [Selected Categories] リストに最大 50 の項目を追加できます。各 URL カテゴリは、レピュテーションを追加した場合も含め、1 つの項目としてカウントされます。

次の表では、上記の条件をどのように設定するかを示しています。URL オブジェクトおよびリテラル URL にレピュテーションを追加できないことに注意してください。

表 22-2　例:URL 条件の作成

ブロック対象	選択するカテゴリまたは URL オブジェクト	レピュテーション
マルウェア サイト、レピュテーションは無関係	Malware Sites	いずれか
ハイ リスク(レベル 1)のすべての URL	いずれか	1 - ハイ リスク
リスクが無害(benign)より大きいソーシャル ネットワーキング サイト(レベル 1 ～ 3)	Social Network	3 - セキュリティ リスクのある無害(benign)サイト

無効な URL 条件が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。また、アクセス コントロール ポリシーおよびルールのトラブルシューティング(12-25 ページ)を参照してください。

カテゴリとレピュテーション データを使用して要求された URL でトラフィックを制御するには、次の手順を実行します。

アクセス: Admin/Access Admin/Network Admin

ステップ 1　URL に応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成(21-4 ページ)を参照してください。

ステップ 2　SSL ルール エディタで、[Categories] タブを選択します。

[Categories] タブが表示されます。

ステップ 3　[Categories] リストで、追加する URL カテゴリを選択します。カテゴリを指定せずにすべての暗号化 Web トラフィックと一致させるには、[Any] カテゴリを選択します。

追加可能なカテゴリを検索するには、[Categories] リストの上にある [Search by name or value] プロンプトをクリックし、カテゴリ名を入力します。入力を開始するとリストが更新され、一致するカテゴリが表示されます。

カテゴリをクリックして選択します。複数のカテゴリを選択するには、Shift キーまたは Ctrl キーを使用します。

ヒント　右クリックで表示される [Select All] も利用できますが、この方法ですべてのカテゴリを追加すると、SSL ルールの最大項目数 50 を超えてしまいます。代わりに [Any] を使用してください。

ステップ 4　オプションで、[Reputations] リストのレピュテーション レベルをクリックして、選択したカテゴリに追加します。レピュテーション レベルを指定しない場合、デフォルトですべてのレベルを意味する [Any] が適用されます。

選択できるレピュテーション レベルは 1 つのみです。レピュテーションのレベルを選択すると、SSL ルールはその目的に応じて異なる動作をします。

- ルールで Web アクセスのブロックまたはトラフィックの復号化を行う場合（ルール アクションが、**Block**、**Block with reset**、**Decrypt - Known Key**、**Decrypt - Resign**、または **Monitor**の場合）、選択したレピュテーション レベルよりも厳しいすべてのレピュテーションも自動的に選択されます。たとえば**疑わしいサイト**（レベル 2）をブロックするようルールを設定した場合、**ハイ リスク**（レベル 1）のサイトも自動的にブロックされます。
- ルールで Web アクセスを許可して、アクセス コントロールに従わせる場合（ルール アクションが **Do not decrypt**の場合）、選択したレピュテーション レベルよりも厳しくないすべてのレピュテーションも自動的に選択されます。たとえば**無害なサイト**（レベル 4）を許可するようルールを設定した場合、**有名**（レベル 5）サイトもまた自動的に許可されます。

ルールのアクションを変更した場合、システムは、上記の点に従って URL 条件のレピュテーション レベルを自動的に変更します。

ステップ 5　[Add to Rule] をクリックして、選択した項目を [Selected Categories] リストに追加します。

選択した項目をドラッグ アンド ドロップでリストに追加することもできます。

ステップ 6　ルールを保存するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

URL 検出とブロッキングの制約事項

ライセンス： URL Filtering

サポートされるデバイス： シリーズ 3

URL の検出とブロックを行う場合は、次の点に注意してください。

URL 識別の速さ

システムによる URL のカテゴリ分類は、以下のすべての処理が完了するまで実行されません。

- モニタしている接続がクライアントとサーバ間で確立される。
- セッション内の HTTPS アプリケーションがシステムにより識別される。
- 要求された URL のシステムによる識別は、クライアントの hello メッセージまたはサーバ証明書に基づいて行われます。

この識別が行われるのは、サーバ証明書が交換された後です。ハンドシェイク中に交換されるトラフィックで URL 識別が完了する前に、URL 条件を含んでいる SSL ルール内の他のすべての条件に一致してしまうと、SSL ポリシーによりそのパケットの通過が許可されます。このため、URL を識別できるように接続が確立されます。この問題の影響を受けるルールには、情報アイコン（ ）が表示されます。

システムによる識別が完了すると、URL 条件に一致する残りのセッション トラフィックに SSL ルールのアクションが適用されます。

URL での検索クエリ パラメータ

URL 条件の照合では、URL 内の検索クエリ パラメータが使用されません。たとえば、すべてのショッピング トラフィックをブロックする場合を考えます。amazon.com を探すために Web 検索を使用してもブロックされませんが、amazon.com を閲覧しようとするとブロックされます。

暗号化のプロパティに基づいたトラフィックの制御

ライセンス： すべて

サポートされるデバイス： シリーズ 3

暗号化接続の特性に基づいて暗号化トラフィックの処理および復号化を行う SSL ルールを作成できます。セッションの暗号化に使用されている暗号スイートまたはプロトコル バージョンを検出して、それに応じてトラフィックを処理できます。また、サーバ証明書を検出して、以下の特性に基づいてトラフィックを処理することもできます。

- サーバ証明書自体。
- 証明書が CA で発行されているか自己署名されているか。
- 証明書のホルダー。
- 証明書ステータス。証明書が有効であるか、発行元の CA により無効にされているかなど。

複数の暗号スイートを 1 つのルールで検出したり、証明書の発行元や証明書ホルダーを検出する場合は、再利用可能な暗号スイートのリストおよび識別名オブジェクトを作成してルールに追加できます。サーバ証明書および特定の証明書ステータスを検出するには、ルール用の外部証明書と外部 CA オブジェクトの作成が必要です。

詳細については、次の項を参照してください。

- 証明書の識別名による暗号化トラフィックの制御（22-21 ページ）
- 証明書による暗号化トラフィックの制御（22-23 ページ）
- 証明書ステータスによる暗号化トラフィックの制御（22-25 ページ）
- 暗号スイートによる暗号化トラフィックの制御（22-30 ページ）
- 暗号化プロトコルのバージョンによるトラフィックの制御（22-31 ページ）

証明書の識別名による暗号化トラフィックの制御

ライセンス： すべて

サポートされるデバイス： シリーズ 3

SSL ルールで識別名条件を設定すると、証明書ホルダーまたはサーバ証明書を発行した CA に応じて暗号化トラフィックを処理および検査できます。発行元の識別名を基準にすると、サイトのサーバ証明書を発行した CA に基づいてトラフィックを処理できます。

ルール条件を設定する場合は、手動でリテラル値を指定するか、識別名オブジェクトを参照するか、または複数のオブジェクトを含んでいる識別名グループを参照できます。

注　**Decrypt - Known Key** アクションを選択した場合、識別名条件を設定することはできません。このアクションでは、トラフィック復号化用のサーバ証明書の選択が必要であり、トラフィックの照合はすでにこの証明書で行われることになります。詳細については、「復号化アクション：さらに検査するためにトラフィックを復号化（21-11 ページ）」を参照してください。

複数のサブジェクトおよび発行元の識別名との一致を単一の証明書ステータスのルール条件で行うことも可能ですが、ルールとの照合で一致する必要があるのは 1 つの共通名または識別名だけです。

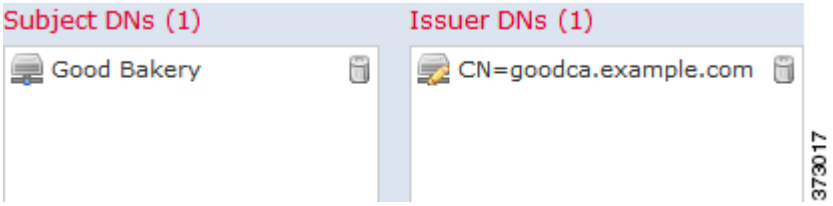
識別名を手動で追加する場合、共通名属性（**CN**）を含めることができます。「CN=」なしで共通名を追加すると、オブジェクトの保存時に「CN=」が追加されます。

さらに、次の表にリストされている、コンマで区切られた属性を含む識別名を追加することもできます。

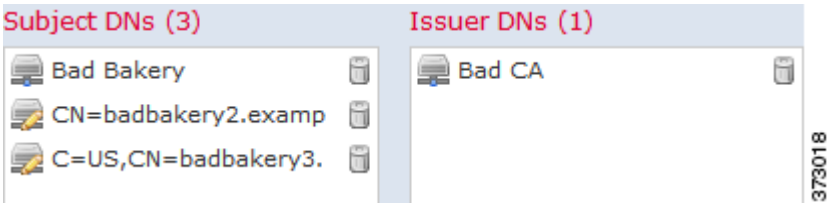
表 22-3　識別名の属性

属性	説明	使用可能な値
C	Country Code	2 つの英字
CN	Common Name	最大 64 個の英数字、バックスラッシュ (\)、ハイフン (-)、引用符 (")、アスタリスク (*)、ピリオド (.)、またはスペース文字
O	マニュアルの構成	
OU	組織単位	

次の図は、goodbakery.example.com に対して発行された証明書および goodca.example.com によって発行された証明書を検索する識別名ルール条件を示しています。これらの証明書で暗号化されたトラフィックは許可され、アクセス コントロールにより制御されます。



次の図は、badbakery.example.com および関連ドメインに対して発行された証明書および badca.example.com によって発行された証明書を検索する識別名ルール条件を示しています。これらの証明書で暗号化されたトラフィックは、再署名された証明書を使用して復号化されます。



1 つの識別名条件で、[Subject DNs] リストおよび [Issuer DNs] リストにそれぞれ最大 50 のリテラル値および識別名オブジェクトを追加できます。

システム提供の識別名オブジェクト グループである Sourcefire Undecryptable Sites には、システムで復号化できないトラフィックの Web サイトが含まれています。このグループを識別名条件に追加すると、該当する Web サイトとのトラフィックがブロックしたり復号化を無効にしたりでき、これらのトラフィックの復号化に使用されるシステム リソースの浪費を回避できます。グループ内の各エントリは変更できますが、このグループを削除することはできません。システムによる更新によりこのリストのエントリが変更されることがありますが、ユーザによる変更は保持されます。

証明書のサブジェクトまたは発行元の識別名に基づいて暗号化トラフィックを検査するには、次の手順を実行します。

アクセス：Admin/Access Admin/Network Admin

ステップ 1　証明書のサブジェクトまたは発行元の識別名に応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（21-4 ページ）を参照してください。

ステップ 2　SSL ルール エディタで、[DN] タブを選択します。

[DN] タブが表示されます。

ステップ 3　[Available DNs] で、追加する識別名を選択します。

- ここで識別名オブジェクトを作成してリストに追加するには、[Available DNs] リストの上にある追加アイコン（  ）をクリックし、識別名オブジェクトの操作（3-44 ページ）の手順に従います。
- 追加する識別名オブジェクトおよびグループを検索するには、[Available DNs] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

オブジェクトをクリックして選択します。複数のオブジェクトを選択するには、Shift キーまたは Ctrl キーを使用します。すべてのオブジェクトを選択するには、右クリックして [Select All] を選択します。

ステップ 4　次の選択肢があります。

- [Add to Subject] をクリックして、選択したオブジェクトを [Subject DNs] リストに追加します。
- [Add to Issuer] をクリックして、選択したオブジェクトを [Issuer DNs] リストに追加します。

選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5　手動で指定するリテラル共通名または識別名がある場合は、それらを追加します。

[Subject DNs] または [Issuer DNs] リストの下にある [Enter DN or CN] プロンプトをクリックし、共通名または識別名を入力して [Add] をクリックします。

ステップ 6　ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

証明書による暗号化トラフィックの制御

ライセンス：すべて

サポートされるデバイス：シリーズ 3

SSL ルールで証明書条件を設定すると、トラフィックの暗号化に使用されているサーバ証明書に応じて暗号化トラフィックを処理および検査できます。1 つの条件に 1 つまたは複数の証明書を設定でき、トラフィックの証明書がいずれかの条件の証明書と一致するとそのルールが適用されます。

証明書ベースの SSL ルール条件を作成するときにサーバ証明書をアップロードしたり、再利用可能な外部証明書オブジェクトとして保存してサーバ証明書の名前を関連付けたりできます。また、既存の外部証明書オブジェクトやオブジェクト グループを使用して証明書条件を設定することもできます。

ルール条件の [Available Certificates] フィールドでは、外部証明書オブジェクトやオブジェクト グループを証明書の識別名ニ関する以下の特性に基づいて検索できます。

- サブジェクトまたは発行元の共通名（CN）
- サブジェクトまたは発行元の組織（O）
- サブジェクトまたは発行元の組織単位（OU）

1 つの証明書のルール条件で複数の証明書に一致させることもでき、トラフィックの暗号化に使用されている証明書がアップロードされた証明書のいずれかと一致した場合、その暗号化トラフィックはルールに一致したと判定されます。

1 つの証明書条件で、[Selected Certificates] リストに最大 50 の外部証明書オブジェクトおよび外部証明書オブジェクト グループを追加できます。

次の点に注意してください。

- **Decrypt - Known Key** アクションを選択した場合、証明書条件を設定することはできません。このアクションでは、トラフィック復号化用のサーバ証明書の選択が必要であり、トラフィックの照合はすでにこの証明書で行われることになります。詳細については、「復号化アクション：さらに検査するためにトラフィックを復号化（21-11 ページ）」を参照してください。
- 証明書条件に外部証明書オブジェクトを設定する場合、暗号スイート条件に追加する暗号スイートまたは **Decrypt - Resign** アクションに関連付ける内部 CA オブジェクトのいずれかが、外部証明書の署名アルゴリズム タイプと一致する必要があります。たとえば、ルールの証明書条件で EC ベースのサーバ証明書を参照する場合、追加する暗号スイートまたは **Decrypt - Resign** アクションに関連付ける CA 証明書も EC ベースである必要があります。署名アルゴリズム タイプの不一致が検出されると、ポリシー エディタでルールの横に警告アイコンが表示されます。詳細については、暗号スイートによる暗号化トラフィックの制御（22-30 ページ）および復号化アクション：さらに検査するためにトラフィックを復号化（21-11 ページ）を参照してください。

サーバ証明書に基づいて暗号化トラフィックを検査するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　サーバ証明書に応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（21-4 ページ）を参照してください。

ステップ 2　SSL ルール エディタで、[Certificate] タブを選択します。

[Certificate] タブが表示されます。

ステップ 3　[Available Certificates] で、追加するサーバ証明書を選択します。

- ここで外部証明書オブジェクトを作成してリストに追加するには、[Available Certificates] リストの上にある追加アイコン（  ）をクリックし、外部証明書オブジェクトの使用（3-54 ページ）の手順に従います。
- 追加する証明書オブジェクトおよびグループを検索するには、[Available Certificates] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

オブジェクトをクリックして選択します。複数のオブジェクトを選択するには、Shift キーまたは Ctrl キーを使用します。すべてのオブジェクトを選択するには、右クリックして [Select All] を選択します。

ステップ 4　[Add to Rule] をクリックして、選択したオブジェクトを [Subject Certificates] リストに追加します。

選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5　ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

証明書ステータスによる暗号化トラフィックの制御

ライセンス： すべて

サポートされるデバイス： シリーズ 3

SSL ルールで証明書ステータス条件を設定すると、トラフィックの暗号化に使用されているサーバ証明書のステータス（有効、失効済み、有効期限切れ、未有効化、自己署名、信頼できる CA によって署名済みなど）に応じて暗号化トラフィックの処理および検査できます。

CA が証明書を発行したか失効したかを確認するには、ルートおよび中間 CA 証明書とその CRL をオブジェクトとしてアップロードする必要があります。その後で SSL ポリシーの信頼できる CA 証明書のリストに、これらの信頼できる CA のオブジェクトを追加します。

証明書ステータスの SSL ルール条件では、各ステータスの有無を基準にしたトラフィックの照合ができます。1 つのルール条件で複数のステータスを選択でき、いずれかのステータスと証明書が一致すれば、ルールとトラフィックが一致したと判定されます。

詳細については、以下を参照してください。

- 外部認証局の信頼（22-25 ページ）
- 証明書ステータスでのトラフィックの照合（22-27 ページ）

外部認証局の信頼

ライセンス： すべて

サポートされるデバイス： シリーズ 3

SSL ポリシーでルートおよび中間 CA 証明書を追加することで信頼できる CA が設定され、トラフィックの暗号化に使用されているサーバ証明書の検証に、これらの信頼できる CA を使用できるようにになります。検証されたサーバ証明書には、信頼できる CA によって署名された証明書が含まれます。

信頼できる CA 証明書の中にアップロードされた証明書失効リスト（CRL）が含まれている場合は、信頼できる CA により暗号化証明書が失効されているかどうかも確認できます。詳細については、「信頼できる CA オブジェクトへの証明書失効リストの追加（3-53 ページ）」を参照してください。

SSL ポリシーに信頼できる CA 証明書を追加した後は、トラフィックと一致させるさまざまな証明書ステータス条件を SSL ルールに設定することができます。詳細については、信頼できる認証局オブジェクトの使用（3-52 ページ）および証明書ステータスによる暗号化トラフィックの制御（22-25 ページ）を参照してください。

ヒント　信頼できるルート CA の信頼チェーン内にあるすべての証明書を、信頼できる CA 証明書のリストにアップロードしますが、これにはルート CA 証明書およびすべての中間 CA 証明書が含まれます。これを行わないと、中間 CA から発行された信頼できる証明書の検出が困難になります。

SSL ポリシーを作成すると、[Trusted CA Certificates] タブにデフォルトの信頼できる CA オブジェクト グループ Sourcefire Trusted Authorities が入力されます。このグループ内の各エントリは変更が可能で、SSL ポリシーにこのグループを含めるかどうかを選択できます。このグループを削除することはできません。システムによる更新によりこのリストのエントリが変更されることがありますが、ユーザによる変更は保持されます。詳細については、「基本 SSL ポリシーの作成（20-2 ページ）」を参照してください。

ポリシーに信頼できる CA を追加するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [SSL] を選択します。

[SSL Policy] ページが表示されます。

ステップ 2　設定する SSL ポリシーの横にある編集アイコン（ ）をクリックします。

SSL ポリシー エディタが表示されます。

ステップ 3　[Trusted CA Certificates] タブを選択します。

[Trusted CA Certificates] ページが表示されます。

ステップ 4　[Available Trusted CAs] で追加する信頼できる CA を選択します。

- ここで信頼できる CA のオブジェクトを作成してリストに追加するには、[Available Trusted CAs] リストの上にある追加アイコン（ ）をクリックし、信頼できる認証局オブジェクトの使用（3-52 ページ）の手順に従います。
- 追加する信頼できる CA オブジェクトおよびグループを検索するには、[Available Trusted CAs] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

オブジェクトをクリックして選択します。複数のオブジェクトを選択するには、Shift キーまたは Ctrl キーを使用します。すべてのオブジェクトを選択するには、右クリックして [Select All] を選択します。

ステップ 5　[Add to Rule] をクリックして、選択したオブジェクトを [Selected Trusted CAs] リストに追加します。

選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 6　ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

証明書ステータスでのトラフィックの照合

ライセンス: すべて

サポートされるデバイス: シリーズ 3

証明書ステータス ベースのルール条件を設定すると、トラフィックの暗号化に使用されているサーバ証明書のステータスに基づいて暗号化トラフィックを照合できます。次の作業を実行できます。

- サーバ証明書のステータスをチェックする。
- 証明書にステータスがないことをチェックする。
- 証明書ステータスの有無のチェックをスキップする。

複数の証明書ステータスの有無との一致を単一の証明書ステータスのルール条件で選択することも可能ですが、ルールとの照合で証明書が一致する必要があるのは 1 つの基準だけです。

次の表は、暗号化用のサーバ証明書のステータスを基準に、システムが暗号化トラフィックを評価する方法を示しています。

表 22-4　証明書ステータスのルール条件の基準

ステータス チェック	Yes を設定	No を設定
Revoked	ポリシーは、サーバ証明書を発行した CA を信頼しており、ポリシーにアップロードされた CA 証明書にはこのサーバ証明書を失効させる CRL が含まれています。	ポリシーは、サーバ証明書を発行した CA を信頼しており、ポリシーにアップロードされた CA 証明書にはこのサーバ証明書を失効させる CRL が含まれていません。
Self-signed	検出されたサーバ証明書が、同じサブジェクトと発行元の識別名を含んでいます。	検出されたサーバ証明書が、異なるサブジェクトと発行元の識別名を含んでいます。
Valid	以下のすべてを満たしています。 • 証明書を発行した CA をポリシーが信頼しています。 • 署名が有効です。 • 発行元が有効です。 • ポリシーの信頼できる CA のいずれも証明書を失効させていません。 • 現在の日付が証明書の有効期限の開始日と終了日の範囲内にあります。	以下の 1 つ以上を満たしています。 • 証明書を発行した CA をポリシーが信頼していません。 • 署名が無効です。 • 発行元が無効です。 • ポリシーの信頼できる CA の 1 つが証明書を失効させています。 • 現在の日付が証明書の有効期限の開始日より前です。 • 現在の日付が証明書の有効期限の終了日より後です。
Invalid signature	証明書の内容に対して証明書の署名が適切に検証されません。	証明書の内容に対して証明書の署名が適切に検証されます。
Invalid issuer	発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されていません。	発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されています。
Expired	現在の日付が証明書の有効期限の終了日より後です。	現在の日付が証明書の有効期限の終了日であるかそれより前です。
Not yet valid	現在の日付が証明書の有効期限の開始日より前です。	現在の日付が証明書の有効期限の開始日であるかそれより後です。

次の例について考えてみます。組織は Verified Authority という認証局を信頼しています。組織は Spammer Authority という認証局を信頼していません。システム管理者は、Verified Authority の証明書および、Verified Authority の発行した中間 CA 証明書をアップロードします。Verified Authority が以前に発行した証明書の 1 つを失効させたため、システム管理者は Verified Authority から配布された CRL をアップロードします。

次の図は、有効な証明書をチェックする証明書ステータスのルール条件を示しています。これにより、Verified Authority から発行されたが CRL には登録されておらず、現状で有効期限の開始日と終了日の範囲内にあるかどうかがチェックされます。この設定では、これらの証明書で暗号化されたトラフィックはアクセス コントロールにより復号化および検査されません。

次の図は、ステータスの不在をチェックする証明書ステータスのルール条件を示しています。この設定では、期限切れになっていない証明書を使用して暗号化されたトラフィックに一致し、そのトラフィックをモニタします。

次の図は、さまざまなステータスの有無に一致する証明書ステータスのルール条件を示しています。この設定でルールが一致するのは、着信トラフィックを暗号化した証明書が無効なユーザが発行元、自己署名、無効、または期限切れであった場合で、そうしたトラフィックを既知のキーで復号化します。

1 つの証明書が複数のステータスに一致する場合でも、ルールがトラフィックに行うアクションは一度に 1 つだけであることに注意してください。

サーバ証明書のステータスで暗号化トラフィックを検査するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　サーバ証明書のステータスに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（21-4 ページ）を参照してください。

ステップ 2　SSL ルール エディタで、[Cert Status] タブを選択します。

[Cert Status] タブが表示されます。

ステップ 3　各証明書ステータスには次のオプションがあります。

- 該当する証明書ステータスが存在するときに一致させる場合は [Yes] を選択します。
- 該当する証明書ステータスが存在しないときに一致させる場合は [No] を選択します。
- 該当する証明書ステータスと照合させない場合は [Do Not Match] を選択します。

ステップ 4　ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

暗号スイートによる暗号化トラフィックの制御

ライセンス： すべて

サポートされるデバイス： シリーズ 3

SSL ルールで暗号スイート条件を設定すると、暗号化セッションのネゴシエートに使用される暗号スイートに応じて暗号化トラフィックを処理および検査できます。暗号スイートのルール条件に追加できるCisco定義の暗号スイートが提供されています。複数の暗号スイートを含む、暗号スイートのリストのオブジェクトを追加することもできます。暗号スイートのリストの詳細については、暗号スイート リストの操作（3-43 ページ）を参照してください。

注　新しい暗号スイートを追加することはできません。定義済みの暗号スイートは変更も削除もできません。

1 つの暗号スイート条件で、[Selected Cipher Suites] リスト最大 50 の暗号スイートおよび暗号スイート リストを追加できます。

次の点に注意してください。

- 展開でサポートされていない暗号スイートを追加した場合、その SSL ポリシーに関連付けられたアクセス コントロール ポリシーを適用することはできません。たとえば、パッシブ展開では、一時 Diffie-Hellman（DHE）および一時的楕円曲線 Diffie-Hellman（ECDHE）暗号スイートを使用したトラフィックの復号化がサポートされません。これらの暗号スイートでルールを作成した場合、アクセス コントロール ポリシーは適用できません。
- 暗号スイート条件に暗号スイートを設定する場合、証明書条件に追加する外部証明書オブジェクトまたは **Decrypt - Resign** アクションに関連付ける内部 CA オブジェクトのいずれかが、暗号スイートの署名アルゴリズム タイプと一致する必要があります。たとえば、ルールの暗号スイート条件で EC ベースの暗号スイートを参照する場合、追加するサーバ証明書または **Decrypt - Resign** アクションに関連付ける CA 証明書も EC ベースである必要があります。署名アルゴリズム タイプの不一致が検出されると、ポリシー エディタでルールの横に警告アイコンが表示されます。詳細については、暗号スイートによる暗号化トラフィックの制御（22-30 ページ）および復号化アクション：さらに検査するためにトラフィックを復号化（21-11 ページ）を参照してください。
- 匿名の暗号スイートで暗号化されたトラフィックは復号化できません。匿名の暗号スイートを **Cipher Suite** 条件に追加した場合、SSL ルールに **Decrypt - Resign** または **Decrypt - Known Key** アクションを使用できません。

暗号化トラフィックを暗号スイートで検査するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　暗号スイートに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（21-4 ページ）を参照してください。

ステップ 2　SSL ルール エディタで、[Cipher Suite] タブを選択します。

[Cipher Suite] タブが表示されます。

ステップ 3　[Available Cipher Suites] で、追加する暗号スイートを選択します。

- ここで暗号スイート リストを作成してリストに追加するには、[Available Cipher Suites] リストの上にある追加アイコン（ ）をクリックし、暗号スイート リストの操作（3-43 ページ）の手順に従います。
- 追加する暗号スイートおよびリストを検索するには、[Available Cipher Suites] リストの上にある [Search by name or value] プロンプトをクリックし、暗号スイートの名前または暗号スイートの値を入力します。入力を開始するとリストが更新され、一致する暗号スイートが表示されます。

暗号スイートをクリックして選択します。複数の暗号スイートを選択するには、Shift キーまたは Ctrl キーを使用します。すべての暗号スイートを選択するには、右クリックして [Select All] を選択します。

ステップ 4　[Add to Rule] をクリックして、選択した暗号スイートを [Selected Cipher Suites] リストに追加します。

選択した暗号スイートをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5　ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

暗号化プロトコルのバージョンによるトラフィックの制御

ライセンス： すべて

サポートされるデバイス： シリーズ 3

SSL ルールでセッション条件を設定すると、トラフィックの暗号化に使用されている SSL または TLS のバージョンに応じて暗号化トラフィックを検査できます。SSL バージョン 3.0 または TLS バージョン 1.0、1.1、1.2 のいずれかで暗号化されたトラフィックとの照合を選択できます。デフォルトでは、ルールの作成時にすべてのプロトコルのバージョンが選択されます。複数のバージョンが選択されている場合、いずれかのバージョンと一致する暗号化トラフィックがルールに一致したと判定されます。ルール条件を保存するには、最低 1 つのプロトコル バージョンを選択する必要があります。

注　バージョンのルール条件で SSL バージョン 2.0 を選択することはできません。これは、SSL バージョン 2.0 で暗号化されたトラフィックの復号化がサポートされていないためです。復号化できないアクションを設定すれば、それ以上のインスペクションなしで、これらのトラフィックを許可またはブロックできます。詳細については、SSL ルールによる復号可能接続のロギング（38-14 ページ）を参照してください。

暗号化トラフィックを SSL または TLS のバージョンで検査するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　暗号化プロトコルのバージョンに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（21-4 ページ）を参照してください。

ステップ 2　SSL ルール エディタで、[Version] タブを選択します。

[Version] タブが表示されます。

ステップ 3　照合するプロトコル バージョンを選択します。**SSL v3.0**、**TLS v1.0**、**TLS v1.1**、または **TLS v1.2** を選択できます。

ステップ 4　ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

ネットワーク分析ポリシーまたは侵入ポリシーについて

ネットワーク分析ポリシーと侵入ポリシーは、FireSIGHT システム の侵入検知および防御機能の一部として連携して動作します。*侵入検知*という用語は、一般に、ネットワーク トラフィックへの侵入の可能性を受動的に分析し、セキュリティ分析用に攻撃データを保存するプロセスを指します。*侵入防御*という用語には、侵入検知の概念が含まれますが、さらにネットワークを通過中の悪意のあるトラフィックをブロックしたり変更したりする機能も追加されます。

侵入防御展開では、システムがパケットを検査するときに、以下が実行されます。

- **ネットワーク分析ポリシー**は、トラフィックの*デコード*と*前処理*の方法を管理し、特に、侵入を試みている兆候がある異常なトラフィックについて、さらに評価できるようにします。
- **侵入ポリシー**では*侵入およびプリプロセッサ ルール*(総称的に「*侵入ポリシー ルール*」とも呼ばれる)を使用し、パターンに基づく攻撃について、デコードされたパケットを検査します。侵入ポリシーは*変数セット*とペアになっており、これにより、ユーザは指定された値を使用してネットワーク環境を正確に反映できます。

ネットワーク分析ポリシーと侵入ポリシーは、どちらも親のアクセス コントロール ポリシーによって呼び出されますが、呼び出されるタイミングが異なります。システムでトラフィックが分析される際には、侵入防御(追加の前処理と侵入ルール)フェーズよりも前に、別にネットワーク分析(デコードと前処理)フェーズが実行されます。ネットワーク分析ポリシーと侵入ポリシーを一緒に使用すると、広範囲で詳細なパケット インスペクションを行うことができます。これらのポリシーは、ホストとそのデータの可用性、整合性、機密性を脅かす可能性のあるネットワーク トラフィックの検知、アラート、防御に役立ちます。

FireSIGHT システム は、連携して相互補完する、同様の名前(Balanced Security and Connectivity など)が付いた複数のネットワーク分析ポリシーおよび侵入ポリシーと共に提供されます。システム付属のポリシーを使用することで、Cisco脆弱性調査チーム(VRT)の経験を活用できます。これらのポリシーでは、VRT は侵入ルールおよびプリプロセッサ ルールの状態を設定し、プリプロセッサおよび他の詳細設定の初期設定も提供します。

また、カスタムのネットワーク分析ポリシーや侵入ポリシーも作成できます。カスタム ポリシーの設定を調整することで、各自にもっとも役立つ方法でトラフィックを検査できます。これによって、管理対象デバイスのパフォーマンスが向上し、ユーザは生成されたイベントにさらに効率的に対応できるようになります。

Web インターフェイスで同様のポリシーエディタを使用し、ネットワーク分析ポリシーや侵入ポリシーを作成、編集、保存、管理します。いずれかのタイプのポリシーを編集するときには、Web インターフェイスの左側にナビゲーション パネルが表示され、右側にさまざまな設定ページが表示されます。

この章では、ネットワーク分析ポリシーおよび侵入ポリシーによって管理される各種設定の概要、ポリシーが連携してトラフィックを検査し、ポリシー違反のレコードを生成するしくみ、および、ポリシー エディタの基本的な操作方法について説明します。また、カスタム ポリシーとシステム付属ポリシーを比較して、それらの使用上の利点と制約についても説明します。詳細については、次の項を参照してください。

- ポリシーが侵入についてトラフィックを検査するしくみ（23-2 ページ）
- システム付属ポリシーとカスタム ポリシーの比較（23-8 ページ）
- ナビゲーション パネルの使用（23-15 ページ）
- 競合の解決とポリシー変更の確定（23-17 ページ）

侵入防御展開をカスタマイズするには、以下の該当する手順を参照してください。

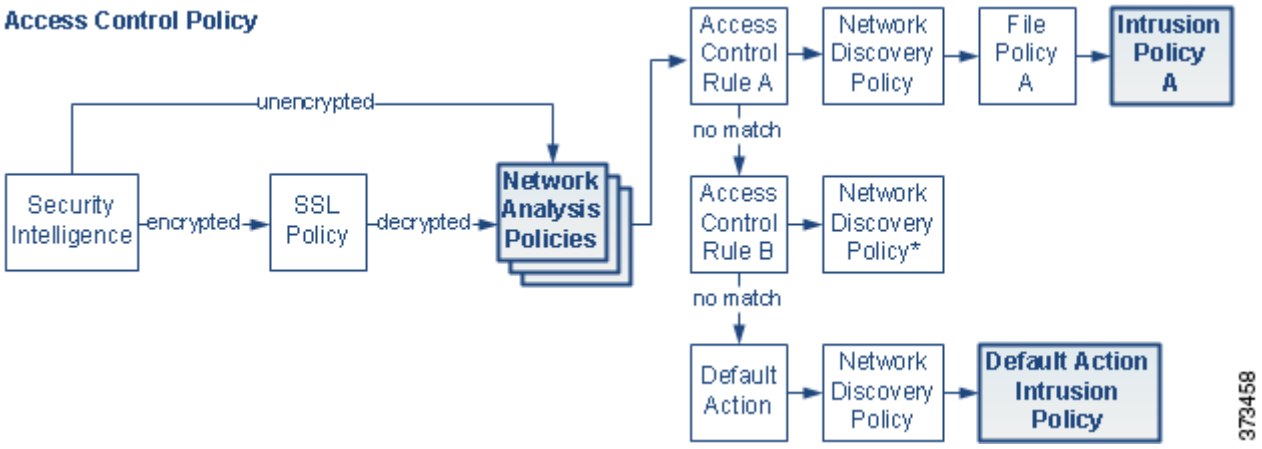
- 変数セットの操作（3-19 ページ）には、ネットワーク環境を正確に反映させるためのシステムの侵入変数の設定方法が記載されています。カスタム ポリシーを使用しない場合でも、Ciscoでは、デフォルトの変数セットのデフォルト変数を変更することを**強く**推奨します。上級ユーザはカスタム変数セットを作成して、1 つ以上のカスタム侵入ポリシーと組合わせることができます。
- 侵入ポリシーの開始（31-1 ページ）では、単純なカスタム侵入ポリシーの作成および編集方法を説明しています。
- 侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（18-1 ページ）には、親アクセス コントロール ポリシーに侵入ポリシーを関連付け、侵入ポリシーを使用して対象トラフィックのみを検査するためのシステムの設定方法が記載されています。また、侵入ポリシーの高度なパフォーマンス オプションの設定方法も記載されています。
- トランスポート/ネットワークの詳細設定の構成（29-2 ページ）には、アクセス コントロール ポリシーのターゲット デバイスで処理されるすべてのトラフィックに適用される、トランスポートおよびネットワーク プリプロセッサの詳細設定の設定方法が記載されています。これらの詳細設定は、ネットワーク分析ポリシーや侵入ポリシーではなく、アクセス コントロール ポリシーで設定します。
- ネットワーク分析ポリシーの開始（26-1 ページ）では、単純なカスタム ネットワーク分析ポリシーの作成および編集方法を説明しています。
- ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）では、デフォルトのネットワーク分析ポリシーの変更方法を説明しています。また、上級ユーザ向けに前処理の調整方法も記載されています。一致したトラフィックの前処理にカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティ ゾーン、ネットワーク、VLAN に合わせて前処理を調整します。
- ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）には、大規模な組織や複雑な展開において、ポリシー *レイヤ*という基本構成要素を使用することにより、複数のネットワーク分析ポリシーや侵入ポリシーをさらに効率的に管理する方法が記載されています。

ポリシーが侵入についてトラフィックを検査するしくみ

ライセンス： Protection

システムがアクセス コントロール展開の一部としてトラフィックを分析する際には、侵入防御（侵入ルールと詳細設定）フェーズよりも前に、別にネットワーク分析（デコードと前処理）フェーズが実行されます。

次の図は、インラインの侵入防御および高度なマルウェア防御（AMP）展開におけるトラフィック分析の順序を簡略的に示しています。アクセス コントロール ポリシーが他のポリシーを呼び出してトラフィックを検査するしくみ、およびそれらのポリシーが呼び出される順序を示しています。ネットワーク分析ポリシーと侵入ポリシーの選択フェーズは強調表示されています。



インライン展開では、図示したプロセスの大部分のステップでさらに検査することなく、システムはトラフィックをブロックできます。セキュリティ インテリジェンス、SSLポリシー、ネットワーク分析ポリシー、ファイル ポリシー、および侵入ポリシーのすべてで、トラフィックをドロップまたは変更できます。唯一の例外として、パッシブにパケットを検査するネットワーク検出ポリシーは、トラフィック フローに影響を与えることができません。

同様に、プロセスの各ステップで、パケットによってシステムがイベントを生成する場合があります。侵入およびプリプロセッサ イベント（総称的に「*侵入イベント*」とも呼ばれる）は、パケットまたはそのコンテンツがセキュリティ リスクを含んでいる可能性を示唆しています。

ヒント　SSL インスペクションの設定で暗号化トラフィックの通過が許可されている場合や、SSL インスペクションが設定されていない場合について、この図は、そのような場合のアクセス コントロール ルールによる暗号化トラフィックの処理を反映していません。デフォルトでは、暗号化ペイロードの侵入およびファイル インスペクションは無効化されます。これにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。詳細については、トラフィック復号化の概要（19-1 ページ）およびSSL プリプロセッサの使用（27-75 ページ）を参照してください。

単一の接続の場合は、図に示すように、アクセス コントロール ルールよりも前にネットワーク分析ポリシーが選択されますが、いくつかの前処理（特にアプリケーション層の前処理）はアクセス コントロール ルールの選択後に実行されます。これは、カスタム ネットワーク分析ポリシーでの前処理の設定方法に**影響しません**。

詳細については、以下を参照してください。

- デコード、正規化、前処理：ネットワーク分析ポリシー（23-4 ページ）
- アクセス コントロール ルール：侵入ポリシーの選択（23-5 ページ）
- 侵入インスペクション：侵入ポリシー、ルール、変数セット（23-6 ページ）
- 侵入イベントの生成（23-7 ページ）

デコード、正規化、前処理：ネットワーク分析ポリシー

ライセンス：Protection

デコードと前処理を実行しないと、プロトコルの相違によってパターン マッチングを行えなくなるので、侵入についてシステムでトラフィックを適切に評価できなくなります。ポリシーが侵入についてトラフィックを検査するしくみ（23-2 ページ）の図に示すように、ネットワーク分析ポリシーは、次のように、これらのトラフィック処理タスクを制御します。

- 暗号化トラフィックがセキュリティ インテリジェンスによってフィルタリングされた**後**
- 暗号化トラフィックがオプションの SSL ポリシーによって復号化された**後**
- ファイルまたは侵入ポリシーによってトラフィックを検査できるようになる**前**

ネットワーク分析ポリシーは、フェーズでのパケット処理を制御します。まず、最初の 3 つの TCP/IP レイヤを経由するパケットがデコードされ、続いて、標準化、前処理、プロトコルの異常の検出が行われます。

- パケット デコーダは、パケット ヘッダーやペイロードを、プリプロセッサや以降の侵入ルールで簡単に使用できる形式に変換します。TCP/IP スタックの各レイヤのデコードは、データリンク層から開始され、ネットワーク層、トランスポート層へと順番に行われます。パケット デコーダは、パケット ヘッダーからさまざまな異常動作を検出します。詳細については、パケットのデコードについて（29-18 ページ）を参照してください。
- インライン展開では、インライン正規化プリプロセッサは、攻撃者が検出を免れる可能性を最小限にするために、トラフィックを再フォーマット（正規化）します。その他のプリプロセッサや侵入ルールによる検査に向けてパケットを準備し、システムで処理されるパケットがネットワーク上のホストで受信されるパケットと同じものになるようにします。詳細については、インライン トラフィックの正規化（29-7 ページ）を参照してください。

ヒント　パッシブな展開の場合、Ciscoでは、ネットワーク分析レベルでインライン正規化を行うのではなく、アクセス コントロール ポリシー レベルで適応型プロファイルを設定することを推奨しています。詳細については、パッシブ展開における前処理の調整（30-1 ページ）を参照してください。

- ネットワーク層とトランスポート層のさまざまなプリプロセッサは、IP フラグメントを悪用する攻撃を検出したり、チェックサム検証を実行したり、TCP および UDP セッションの前処理を実行したりします（トランスポート層およびネットワーク層の前処理の使用（29-1 ページ）を参照）。

  トランスポートおよびネットワーク プリプロセッサの一部の詳細設定は、アクセス コントロール ポリシーのターゲット デバイスで処理されるすべてのトラフィックにグローバルに適用されます。これらは、ネットワーク分析ポリシーではなく、アクセス コントロール ポリシーで設定します（トランスポート/ネットワークの詳細設定の構成（29-2 ページ）を参照）。
- アプリケーション層プロトコル デコーダは、特定タイプのパケット データをルール エンジンで分析可能な形式に正規化します。アプリケーション層プロトコルのエンコードを正規化することによって、システムはデータの表し方が異なる複数のパケットに同じコンテンツ関連の侵入ルールを適用し、大きな結果を得ることができます。詳細については、アプリケーション層プリプロセッサの使用（27-1 ページ）を参照してください。
- Modbus と DNP3 のプリプロセッサは、トラフィックの異常を検出し、データを侵入ルールに提供します。Supervisory Control and Data Acquisition（SCADA）プロトコルは、製造、水処理、配電、空港、輸送システムなどの工業プロセス、インフラストラクチャ プロセス、および設備プロセスからのデータをモニタ、制御、取得します。詳細については、SCADA 前処理の設定（28-1 ページ）を参照してください。

- 複数のプリプロセッサを使用して、Back Orifice、ポートスキャン、SYN フラッド、その他のレート ベース攻撃などの脅威を検出できます（特定の脅威の検出（34-1 ページ）を参照）。

  侵入ルールにセンシティブ データ プリプロセッサを設定します。このプリプロセッサは、ASCII テキストのクレジット カード番号や社会保障番号などのセンシティブ データを検出します（センシティブ データの検出（34-20 ページ）を参照）。

新たに作成されたアクセス コントロール ポリシーでは、1 つのデフォルト ネットワーク分析ポリシーが、同じ親アクセス コントロール ポリシーによって呼び出される *すべての*侵入ポリシー向けの *すべての*トラフィックについて、前処理を制御します。最初に、デフォルトでは Balanced Security and Connectivity ネットワーク分析ポリシーが使用されますが、別のシステム付属ポリシーやカスタム ネットワーク分析ポリシーに変更できます。より複雑な展開では、上級ユーザは、一致したトラフィックの前処理にさまざまなカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティ ゾーン、ネットワーク、VLAN に合わせてトラフィックの前処理オプションを調整できます。詳細については、システム付属ポリシーとカスタム ポリシーの比較（23-8 ページ）を参照してください。

アクセス コントロール ルール：侵入ポリシーの選択

ライセンス： Protection

最初の前処理の後、トラフィックはアクセス コントロール ルール（設定されている場合）によって評価されます。ほとんどの場合、パケットが一致した最初のアクセス コントロール ルールがそのトラフィックを処理することになります。ユーザは一致したトラフィックをモニタ、信頼、ブロック、または許可することができます。

アクセス コントロール ルールでトラフィックを許可すると、ディスカバリ データ、マルウェア、禁止ファイル、侵入について、この順序でトラフィックを検査できます。アクセス コントロール ルールに一致しないトラフィックは、アクセス コントロール ポリシーのデフォルト アクションによって処理されます。デフォルト アクションでは、ディスカバリ データと侵入についても検査できます。

注　どのネットワーク分析ポリシーによって処理されるかに**関わらず**、すべてのパケットは、設定されたアクセス コントロール ルールと上から順に照合されます（したがって、侵入ポリシーによる検査の対象となります）。詳細については、カスタム ポリシーの制限（23-13 ページ）を参照してください。

ポリシーが侵入についてトラフィックを検査するしくみ（23-2 ページ）の図は、インラインの侵入防御および AMP 展開でデバイスを通過する、次のようなトラフィックのフローを示しています。

- アクセス コントロール ルール A により、一致したトラフィックの通過が許可されます。次にトラフィックは、ネットワーク検出ポリシーによるディスカバリ データの検査、ファイル ポリシーA による禁止ファイルおよびマルウェアの検査、侵入ポリシー A による侵入の検査を受けます。
- アクセス コントロール ルール B も一致したトラフィックを許可します。ただし、このシナリオでは、トラフィックは侵入（あるいは、ファイルまたはマルウェア）について検査されないので、ルールに関連付けられている侵入ポリシーやファイル ポリシーはありません。通過を許可されたトラフィックは、デフォルトでネットワーク検出ポリシーによって検査されます。したがって、これを設定する必要はありません。

- このシナリオでは、アクセス コントロール ポリシーのデフォルト アクションは一致したトラフィックを許可します。次に、トラフィックはネットワーク検出ポリシーによって検査されてから、侵入ポリシーによって検査されます。アクセス コントロール ルールまたはデフォルト アクションに侵入ポリシーを関連付けるときに、必要に応じて、別の侵入ポリシーを使用できます。

ブロックされたトラフィックや信頼済みトラフィックは検査されないので、図の例には、ブロック ルールや信頼ルールは含まれていません。詳細については、ルール アクションを使用したトラフィックの処理とインスペクションの決定（14-8 ページ）およびデフォルトの処理の設定およびネットワーク トラフィックのインスペクション（12-7 ページ）を参照してください。

侵入インスペクション：侵入ポリシー、ルール、変数セット

ライセンス： Protection

トラフィックが宛先に向かうことを許可する前に、システムの最終防御ラインとして侵入防御を使用できます。侵入ポリシーは、セキュリティ違反に関するトラフィックの検査方法を制御し、インライン展開では、悪意のあるトラフィックをブロックまたは変更することができます。侵入ポリシーの主な機能は、有効にする侵入ルールとプリプロセッサ ルールの選択および設定方法を管理することです。

侵入ルールとプリプロセッサ ルール

侵入ルールはキーワードと引数のセットとして指定され、ネットワーク上の脆弱性を悪用する試みを検出します。システムは侵入ルールを使用してネットワーク トラフィックを分析し、トラフィックがルールの条件に合致しているかどうかをチェックします。システムが各ルール内で指定された条件とパケットを照らし合わせます。そして、パケット データとルール内で指定されたすべての条件が一致した場合に、ルールがトリガーとして使用されます。

システムには、VRT により作成された次のようなタイプのルールが含まれています。

- *共有オブジェクト侵入ルール*：コンパイルされており、変更できません（ただし、送信元と宛先のポートや IP アドレスなどのルール ヘッダー情報を除く）
- *標準テキスト侵入ルール*：ルールの新しいカスタム インスタンスとして保存および変更できます。
- *プリプロセッサ ルール*：ネットワーク分析ポリシーのプリプロセッサおよびパケット デコーダ検出オプションに関連付けられています。プリプロセッサ ルールはコピーまたは編集できません。ほとんどのプリプロセッサ ルールはデフォルトで無効になっています。プリプロセッサを使用してイベントを生成したり、インライ展開で違反パケットをドロップするには、これらのルールを有効にする必要があります。

システムで侵入ポリシーに従ってパケットを処理するとき、最初にルール オプティマイザが、基準（トランスポート層、アプリケーション プロトコル、保護されたネットワークへの入出力方向など）に基づいて、サブセット内のすべてのアクティブなルールを分類します。次に、侵入ルール エンジンが、各パケットに適用する適切なルールのサブセットを選択します。最後に、マルチ ルール検索エンジンが 3 種類の検索を実行して、トラフィックがルールに一致するかどうかを検査します。

- プロトコル フィールド検索は、アプリケーション プロトコル内の特定のフィールドでの一致を検索します。
- 汎用コンテンツ検索は、パケット ペイロードの ASCII またはバイナリ バイトでの一致を検索します。
- パケット異常検索では、特定のコンテンツを含んでいるかどうかではなく、確立されたプロトコルに違反しているパケット ヘッダーやペイロードが検索されます。

カスタム侵入ポリシーでは、ルールを有効化/無効化することに加え、独自の標準テキスト ルールを作成して追加することにより、検出を調整できます。FireSIGHT 推奨機能を使用して、ネットワーク上で検出されたオペレーティング システム、サーバ、およびクライアント アプリケーション プロトコルを、それらの資産を保護するために作成されたルールに関連付けることができます。

Variable Sets

システムが侵入ポリシーを使用してトラフィックを評価する場合、システムは関連付けられた*変数セット*を使用します。大部分の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスおよびポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

システムには、定義済みのデフォルト変数から構成される 1 つのデフォルト変数セットが含まれています。大部分のシステム付属のshared object ruleと標準テキスト ルールは、定義済みのデフォルト変数を使用して、ネットワークおよびポート番号を定義します。たとえば、ルールの大半は、保護されたネットワークを指定するために変数 `$HOME_NET` を使用して、保護されていない（つまり外部の）ネットワークを指定するために変数 `$EXTERNAL_NET` を使用します。さらに、特殊なルールでは、他の定義済みの変数がしばしば使用されます。たとえば、Web サーバに対するエクスプロイトを検出するルールは、`$HTTP_SERVERS` 変数および `$HTTP_PORTS` 変数を使用します。

ヒント　システム付属の侵入ポリシーを使用する場合でも、Ciscoでは、デフォルトセットの主要なデフォルト変数を変更すること**強く**推奨します。ネットワーク環境を正確に反映する変数を使用すると、処理が最適化され、システムによって疑わしいアクティビティに関連するシステムをモニタできます。上級ユーザはカスタム変数セットを作成して、1 つ以上のカスタム侵入ポリシーと組合わせることができます。詳細については、定義済みのデフォルトの変数の最適化（3-20 ページ）を参照してください。

侵入イベントの生成

ライセンス：Protection

侵入されている可能性を特定すると、システムは*侵入イベントまたはプリプロセッサ イベント*（総称的に「*侵入イベント*」とも呼ばれる）を生成します。管理対象デバイスはDefense Centerにイベントを送信します。ここで、集約データを確認し、ネットワーク アセットに対する攻撃を的確に把握できます。インライン展開では、管理対象デバイスは、有害であると判明しているパケットをドロップまたは置き換えることがきます。

データベース内の各侵入イベントにはイベント ヘッダーがあり、イベント名と分類、送信元と宛先の IP アドレス、ポート、イベントを生成したプロセス、およびイベントの日時に関する情報が含まれています。パケットベースのイベントの場合は、システム イベントをトリガーしたパケットのデコードされたパケット ヘッダーとペイロードのコピーも記録されます。

パケット デコーダ、プリプロセッサ、および侵入ルール エンジンはすべて、システムによるイベントの生成を引き起こします。次に例を示します。

- （ネットワーク分析ポリシーで設定された）パケット デコーダが 20 バイト（オプションやペイロードのない IP データグラムのサイズ）未満の IP パケットを受け取った場合、デコーダはこれを異常なトラフィックと解釈します。以降、パケットを検査する侵入ポリシーで付随するデコーダ ルールが有効な場合は、システムによってプリプロセッサ イベントが生成されます。
- IP 最適化プリプロセッサが重複する一連の IP フラグメントを検出した場合、プリプロセッサはこれを潜在的な攻撃と解釈し、付随するプリプロセッサ ルールが有効な場合はシステムによってプリプロセッサ イベントが生成されます。

- 侵入ルール エンジンでは、大部分の標準テキスト ルールとshared object ruleは、パケットによってトリガーされたときに侵入イベントを生成するように記述されています。

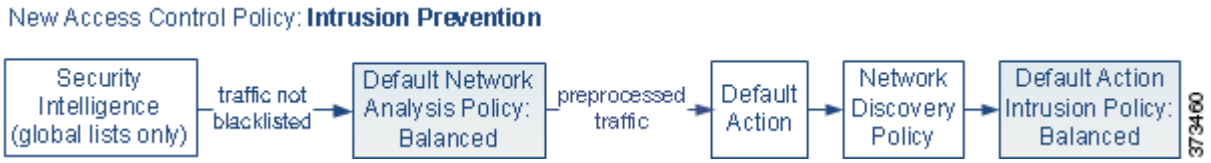
データベースに侵入イベントが蓄積されると、ユーザは攻撃の可能性について分析を開始できます。システムには、侵入イベントを検討し、それらがネットワーク環境やセキュリティ ポリシーの観点から重要かどうかを評価するために必要なツールが備わっています。

システム付属ポリシーとカスタム ポリシーの比較

ライセンス： Protection

新しいアクセス コントロール ポリシーを作成することは、FireSIGHT システムを使用してトラフィック フローを管理する最初のステップの 1つです。デフォルトでは、新たに作成されたアクセス コントロール ポリシーは、システム付属のネットワーク分析ポリシーと侵入ポリシーを呼び出してトラフィックを検査します。

次の図は、インラインの侵入防御展開で、新たに作成されたアクセス コントロール ポリシーが最初にトラフィックを処理するしくみを示しています。前処理と侵入防御フェーズは強調表示されています。



以下のしくみについて注意してください。

- デフォルトのネットワーク分析ポリシーによって、アクセス コントロール ポリシーで処理されるすべてのトラフィックの前処理が制御されます。最初は、システム付属の *Balanced Security and Connectivity ネットワーク分析ポリシー*がデフォルトになります。
- アクセス コントロール ポリシーのデフォルト アクションは、システム付属の *Balanced Security and Connectivity 侵入ポリシー*による検査に従って、悪意のないトラフィックをすべて許可します。デフォルト アクションはトラフィックの通過を許可するので、侵入ポリシーが悪意のあるトラフィックを検査して潜在的にブロックする前に、検出機能によって、ホスト、アプリケーション、ユーザ データについてトラフィックを検査できます。
- ポリシーは、デフォルトのセキュリティ インテリジェンス オプション（グローバルなホワイトリストとブラックリストのみ）を使用し、SSL ポリシーによる暗号化トラフィックの復号化や、アクセス コントロール ルールによるネットワーク トラフィックの特別な処理や検査を実行しません。

侵入防御展開を調整するために実行できる簡単な手順は、システム付属のネットワーク分析ポリシーと侵入ポリシーの別のセットをデフォルトとして使用することです。Ciscoでは、FireSIGHT システム と共にこれらのポリシーを提供しています。

または、カスタム ポリシーを作成して使用することで、侵入防御展開を調整できます。それらのポリシーに設定されたプリプロセッサ オプション、侵入ルール、およびその他の詳細設定が、ネットワークのセキュリティ ニーズに適合しない場合があります。設定可能なネットワーク分析ポリシーと侵入ポリシーを調整することにより、システムがネットワーク上のトラフィックを処理し、侵入について検査する方法を非常にきめ細かく設定できます。

詳細については、以下を参照してください。

- システム付属のポリシーについて（23-9 ページ）
- カスタム ポリシーの利点（23-10 ページ）
- カスタム ポリシーの制限（23-13 ページ）

システム付属のポリシーについて

ライセンス：Protection

Ciscoでは、ネットワーク分析ポリシーと侵入ポリシーの複数のペアを FireSIGHT システム と共に提供しています。システムによって提供されるネットワーク分析ポリシーおよび侵入ポリシーを使用して、Cisco 脆弱性調査チーム（VRT）のエクスペリエンスを活用することができます。これらのポリシーでは、VRT は侵入ルールおよびプリプロセッサ ルールの状態を設定し、プリプロセッサおよび他の詳細設定の初期設定も提供します。システムによって提供されるポリシーをそのまま使用するか、またはカスタム ポリシーのベースとして使用できます。

ヒント　システム付属のネットワーク分析ポリシーと侵入ポリシーを使用する場合でも、ネットワーク環境を正確に反映するように、システムの侵入変数を設定する必要があります。少なくとも、デフォルト セットの主要なデフォルト変数を変更してください（定義済みのデフォルトの変数の最適化（3-20 ページ）を参照）。

新たな脆弱性が発見されると、VRT は侵入ルールのアップデートをリリースします。これらのルール アップデートにより、システム付属のネットワーク分析ポリシーや侵入ポリシーが変更され、侵入ルールとプリプロセッサ ルールの新規作成または更新、既存ルールの状態の変更、およびデフォルトのポリシー設定の変更が実施されます。ルール アップデートでは、システム付属のポリシーからルールが削除されたり、新しいルール カテゴリが提供されたり、さらにデフォルトの変数セットが変更されることもあります。

ルール アップデートによって展開が影響を受けると、Web インターフェイスは影響を受けた侵入ポリシーやネットワーク分析ポリシー、およびそれらの親のアクセス コントロール ポリシーを失効として扱います。変更を有効にするには、更新されたポリシーを再適用する必要があります。

便宜を図るために、影響を受けた侵入ポリシーを単独でまたは影響を受けたアクセス コントロール ポリシーと組み合わせて、自動的に再適用するように、ルール アップデートを設定できます。これにより、展開を自動的に最新な状態に保ち、新たに検出されたエクスプロイトや侵入から保護することができます。

前処理の設定を確実に最新の状態にするには、アクセス コントロール ポリシーを再適用する**必要があります**。これにより、現在実行されているものとは異なる関連する SSL ポリシー、ネットワーク分析ポリシー、ファイル ポリシーが再適用され、高度な前処理とパフォーマンス オプションのデフォルト値も更新できます。詳細については、ルールの更新とローカル ルール ファイルのインポート（66-16 ページ）を参照してください。

Ciscoでは、次のネットワーク分析ポリシーと侵入ポリシーを FireSIGHT システム と共に提供しています。

Balanced Security and Connectivity ネットワーク分析ポリシーと侵入ポリシー

これらのポリシーは、速度と検出の両方を目的として作成されています。一緒に使用すると、ほとんどの組織および展開タイプにとって最適な出発点となります。ほとんどの場合、システムは Balanced Security and Connectivity ポリシーと設定をデフォルトとして使用します。

Connectivity Over Security ネットワーク分析ポリシーと侵入ポリシー

これらのポリシーは、(すべてのリソースに到達可能な)接続がネットワーク インフラストラクチャのセキュリティよりも優先される組織向けに作成されています。この侵入ポリシーは、Security over Connectivity ポリシー内で有効になっているルールよりもはるかに少ないルールを有効にします。トラフィックをブロックする最も重要なルールだけが有効にされます。

Security over Connectivity ネットワーク分析ポリシーと侵入ポリシー

これらのポリシーは、ネットワーク インフラストラクチャのセキュリティがユーザの利便性よりも優先される組織向けに作られています。この侵入ポリシーは、正規のトラフィックにアラートを発したり、それらのトラフィックをドロップする可能性のある膨大な数のネットワーク異常侵入ルールを有効にします。

No Rules Active 侵入ポリシー

No Rules Active 侵入ポリシーでは、すべての侵入ルールと詳細設定が無効化されます。このポリシーは、他のシステム付属ポリシーのいずれかで有効になっているルールに基づくのではなく、独自のポリシーを作成する場合の出発点となります。

注意　Ciscoでは、試験用の別のポリシーとして `Experimental Policy 1` を使用します。Ciscoの担当者から指示された場合を除き、このポリシーは使用しないでください。

カスタム ポリシーの利点

ライセンス：Protection

システム付属のネットワーク分析ポリシーと侵入ポリシーに設定されているプリプロセッサ オプション、侵入ルール、およびその他の詳細設定が、組織のネットワークのセキュリティ ニーズに完全に合致しない場合があります。

カスタム侵入ポリシーを作成すると、環境内のシステムのパフォーマンスを向上させ、ネットワークで発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューを提供できます。設定できるカスタム ポリシーを作成および調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

すべてのカスタム ポリシーには基本ポリシー(別名「基本レイヤ」)があり、それによって、ポリシー内のすべてのコンフィギュレーションのデフォルト設定が定義されます。レイヤは、複数のネットワーク分析ポリシーや侵入ポリシーを効率的に管理するために使用できる基本構成要素です(ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用(24-1 ページ)を参照)。

ほとんどの場合、カスタム ポリシーはシステム付属のポリシーに基づきますが、別のカスタム ポリシーを使用することもできます。ただし、すべてのカスタム ポリシーには、ポリシー チェーンの最終的なベースとしてシステム付属ポリシーが含まれています。システム付属のポリシーはルールアップデートによって変更される可能性があるので、カスタム ポリシーを基本として使用している場合でも、ルール アップデートをインポートするとポリシーに影響が及びます。ルール アップデートによって展開が影響を受けると、Web インターフェイスは影響を受けたポリシーを失効として扱います。詳細については、ルール更新がシステムによって提供される基本ポリシーを変更することを許可する(24-4 ページ)を参照してください。

ユーザが作成するカスタム ポリシーに加えて、システムには、初期インライン ポリシーと初期パッシブ ポリシーという 2 つのカスタム侵入ポリシーと 2 つのネットワーク分析ポリシーが用意されています。これらのポリシーは、該当する「Balanced Security and Connectivity」ポリシーを基本ポリシーとして使用します。両者の唯一の相違点は*ドロップ動作*です。インライン ポリシーではトラフィックのブロックと変更が有効化され、パッシブ ポリシーでは無効化されます。これらのシステム付属のカスタム ポリシーは編集して使用できます。

詳細については、以下を参照してください。

- カスタム ネットワーク分析ポリシーの利点（23-11 ページ）
- カスタム侵入ポリシーの利点（23-12 ページ）

カスタム ネットワーク分析ポリシーの利点

ライセンス：Protection

デフォルトでは、1 つのネットワーク分析ポリシーによって、アクセス コントロール ポリシーで処理されるすべての暗号化されていないトラフィックが前処理されます。これは、侵入ポリシー（および侵入ルール セット）に関係なく、すべてのパケットが同じ設定に基づいてデコードされ、処理されることを意味します。

最初は、システム付属の Balanced Security and Connectivity ネットワーク分析ポリシーがデフォルトになります。前処理を簡単に調整するには、デフォルトとしてカスタムのネットワーク分析ポリシーを作成して使用します。詳しくは、アクセス コントロールのデフォルト ネットワーク分析ポリシーの設定（25-4 ページ）を参照してください。

使用可能な調整オプションはプリプロセッサによって異なりますが、プリプロセッサとデコーダを調整するいくつかの方法として、以下を実行できます。

- モニタしているトラフィックに適用されないプリプロセッサを無効にします。たとえば、HTTP Inspect プリプロセッサは HTTP トラフィックを正規化します。ネットワークに Microsoft Internet Information Services（IIS）を使用する Web サーバが含まれていないことが確実な場合は、IIS 特有のトラフィックを検出するプリプロセッサ オプションを無効にすることで、システム処理のオーバーヘッドを軽減できます。

注　カスタム ネットワーク分析ポリシーでプリプロセッサが無効化されているときに、システムがパケットを有効な侵入ルールまたはプリプロセッサ ルールと照合して評価するために、プリプロセッサを使用する必要がある場合、システムはプリプロセッサを有効にして使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

- 必要に応じて、特定のプリプロセッサのアクティビティを集中させるポートを指定します。たとえば、DNS サーバの応答や暗号化 SSL セッションをモニタするための追加ポートを特定したり、Telnet、HTTP、SMTP トラフィックをデコードするポートを特定できます。

複雑な展開を管理する上級ユーザの場合は、複数のネットワーク分析ポリシーを作成して、それぞれが異なるトラフィックを前処理するように設定できます。さらに、トラフィックのセキュリティ ゾーン、ネットワーク、または VLAN に応じて前処理が制御されるようにこれらのポリシーを設定できます。（ASA FirePOWER デバイスでは、VLAN に応じて前処理を制限することはできません。）

注　カスタム ネットワーク分析ポリシー（特に複数のネットワーク分析ポリシー）を使用して前処理を調整することは、高度なタスクです。前処理と侵入インスペクションは非常に密接に関連しているため、単一のパケットを検査するネットワーク分析ポリシーと侵入ポリシーが相互補完することを許可する場合は、注意する**必要があります**。詳細については、カスタム ポリシーの制限（23-13 ページ）を参照してください。

カスタム侵入ポリシーの利点

ライセンス：Protection

侵入防御を実行するように設定されている、新規に作成されたアクセス コントロール ポリシーでは、デフォルト アクションはすべてのトラフィックを許可しますが、最初にシステム付属の Balanced Security and Connectivity 侵入ポリシーでトラフィックをチェックします。アクセス コントロール ルールを追加するか、デフォルト アクションを変更しない限り、すべてのトラフィックがその侵入ポリシーによって検査されます。システム付属ポリシーとカスタム ポリシーの比較（23-8 ページ）の図を参照してください。

侵入防御の展開をカスタマイズするために、複数のネットワーク分析ポリシーを作成し、それぞれがトラフィックを異なる方法で処理するように調整できます。次に、どのポリシーがどのトラフィックを検査するかを指定するルールを、アクセス コントロール ポリシーに設定します。アクセス コントロール ルールは単純でも複雑でもかまいません。セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、またはユーザなど、複数の基準を使用してトラフィックを照合および検査します。ポリシーが侵入についてトラフィックを検査するしくみ（23-2 ページ）のシナリオは、トラフィックが 2 つの侵入ポリシーの一方によって検査される展開を示しています。

侵入ポリシーの主な機能は、次のように、有効にする侵入ルールとプリプロセッサ ルールの選択および設定方法を管理することです。

- 各侵入ポリシーで、環境に適用されるすべてのルールが有効であることを確認し、環境に適用されないルールを無効化することによって、パフォーマンスを向上させます。インライン展開では、どのルールによって悪質なパケットをドロップまたは変更するかを指定できます。詳細については、ルール状態の設定（32-22 ページ）を参照してください。
- FireSIGHT 推奨機能を使用すると、ネットワーク上で検出されたオペレーティング システム、サーバ、およびクライアント アプリケーション プロトコルを、それらの資産を保護するために作成されたルールに関連付けることができます（ネットワーク資産に応じた侵入防御の調整（33-1 ページ）を参照）。
- 必要に応じて、既存のルールを変更したり、新しい標準テキスト ルールを作成して、新たなエクスプロイトの検出あるいは侵入ポリシーの適用を実行できます（侵入ルールの概要と作成（36-1 ページ）を参照）。

侵入ポリシーに対して実行する可能性があるその他のカスタマイズは、次のとおりです。

- 機密データ プリプロセッサは、ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出します。特定の脅威（バック オリフィス攻撃、複数のポート スキャン タイプ、および過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレート ベース攻撃）を検出する他のプリプロセッサは、ネットワーク分析ポリシーで設定されることに留意してください。詳細については、特定の脅威の検出（34-1 ページ）を参照してください。
- グローバルしきい値を設定すると、侵入ルールに一致するトラフィックが、指定期間内に特定のアドレスまたはアドレス範囲で送受信される回数に基づいて、イベントが生成されます。これにより、大量のイベントによってシステムに過剰な負荷がかかることを回避できます。詳細については、侵入イベントのロギングのグローバルな制限（35-1 ページ）を参照してください。
- また、個々のルールまたは侵入ポリシー全体に対して、侵入イベント通知を抑制し、しきい値を設定することで、大量のイベントによってシステムに過剰な負荷がかかることを回避することもできます。詳細については、ポリシー単位の侵入イベント通知のフィルタ処理（32-25 ページ）を参照してください。

- Web インターフェイス内での侵入イベントをさまざまな形式で表示することに加えて、syslog ファシリティへのロギングを有効にしたり、イベント データを SNMP トラップ サーバに送信したりできます。ポリシーごとに、侵入イベントの通知限度を指定したり、外部ロギング ファシリティに対する侵入イベントの通知をセットアップしたり、侵入イベントへの外部応答を設定したりできます。これらのポリシー単位のアラート設定に加えて、各ルールまたはルール グループの侵入イベントを通知する電子メール アラートをグローバルに有効化/無効化できます。どの侵入ポリシーがパケットを処理するかに関わらず、ユーザの電子メール アラート設定が使用されます。詳細については、侵入ルールの外部アラートの設定 (44-1 ページ)を参照してください。

カスタム ポリシーの制限

ライセンス： Protection

前処理と侵入インスペクションは非常に密接に関連しているため、単一のパケットを処理および検査する、ネットワーク分析ポリシーと侵入ポリシーが相互補完することを設定で許可する場合は、注意する**必要があります**。

デフォルトでは、システムは、管理対象デバイスでアクセス コントロール ポリシーにより処理されるすべてのトラフィックを、1 つのネットワーク分析ポリシーを使用して前処理します。次の図は、インラインの侵入防御展開で、新たに作成されたアクセス コントロール ポリシーが最初にトラフィックを処理するしくみを示しています。前処理と侵入防御フェーズは強調表示されています。

アクセス コントロール ポリシーで処理される*すべて*のトラフィックの前処理が、デフォルトのネットワーク分析ポリシーによってどのように制御されるのか注意してください。最初は、システム付属の Balanced Security and Connectivity ネットワーク分析ポリシーがデフォルトになります。

前処理を調整する簡単な方法は、カスタム ネットワーク分析ポリシーを作成し、それをデフォルトとして使用することです（カスタム ネットワーク分析ポリシーの利点 (23-11 ページ)の概要を参照）。ただし、カスタム ネットワーク分析ポリシーでプリプロセッサが無効化されているときに、システムが前処理されたパケットを有効な侵入ルールまたはプリプロセッサ ルールと照合して評価する必要がある場合、システムはプリプロセッサを有効にして使用します。この場合、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

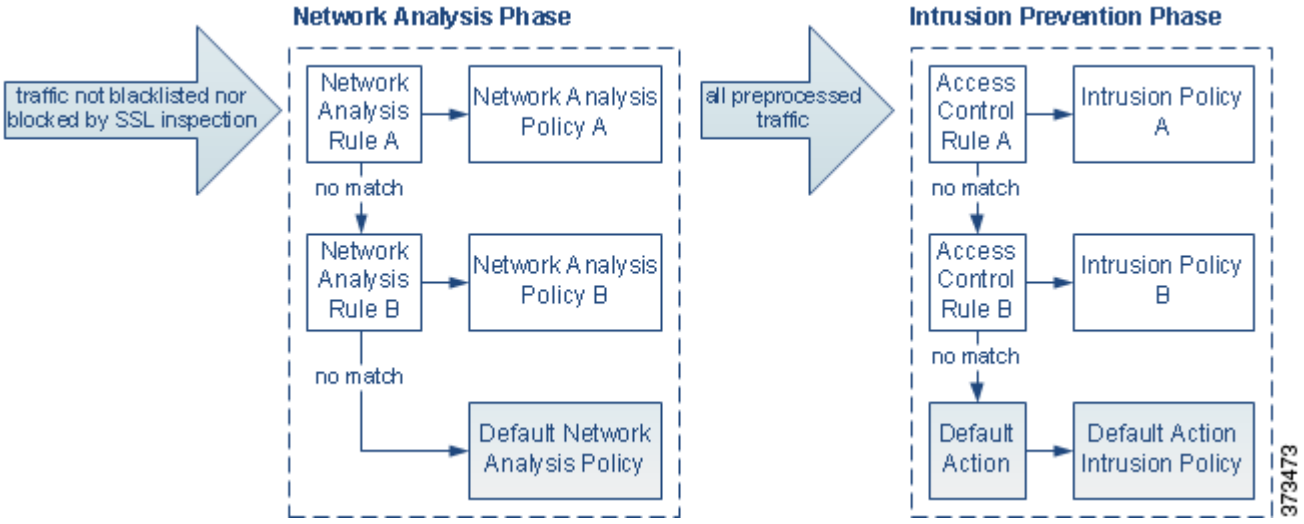
注　プリプロセッサを無効化してパフォーマンスを向上させるには、どの侵入ポリシーでもプリプロセッサを要求するルールが有効になっていないことを確認する**必要があります**。

複数のカスタム ネットワーク分析ポリシーを使用する場合は、さらに課題があります。複雑な展開内の上級ユーザの場合は、一致したトラフィックの前処理にカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティ ゾーン、ネットワーク、VLAN に合わせて前処理を調整できます。（ASA FirePOWER デバイスでは、VLAN に応じて前処理を制限することはできません。）これを行うには、アクセス コントロール ポリシーにカスタムの*ネットワーク分析ルール*を追加します。各ルールには、ルールに一致したトラフィックの前処理を制御するネットワーク分析ポリシーが関連付けられています。

ヒント　アクセス コントロール ポリシーの詳細設定としてネットワーク分析ルールを設定します。FireSIGHT システム の他のタイプのルールとは異なり、ネットワーク分析ルールは、ネットワーク分析ポリシーに含まれているのではなく、それを呼び出します。

システムは、ルール番号の昇順で、設定済みネットワーク分析ルールとパケットを照合します。ネットワーク分析ルールルーに一致しなかったトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。これにより非常に柔軟にトラフィックを前処理できます。ただし、留意すべき点として、パケットがどのネットワーク分析ポリシーによって前処理されるかに**関係なく**、すべてのパケットは、アクセス コントロール ルール独自のプロセスで引き続きアクセス コントロール ルールと照合されます(つまり、侵入ポリシーにより検査される可能性があります)。つまり、特定のネットワーク分析ポリシーでパケットを前処理しても、そのパケットが確実に特定の侵入ポリシーで検査されるわけでは**ありません**。適切なネットワーク分析ポリシーと侵入ポリシーを呼び出して特定のパケットを評価するように、注意してアクセス コントロール ポリシーを設定する**必要があります**。

次の図は、侵入防御(ルール)フェーズよりも前に、別にネットワーク分析ポリシー(前処理)の選択フェーズが発生するしくみを詳細に示しています。簡略化するために、図では検出フェーズとファイル/マルウェア インスペクション フェーズが省かれています。また、デフォルトのネットワーク分析ポリシーとデフォルト アクションの侵入ポリシーは強調表示されています。



このシナリオでは、アクセス コントロール ポリシーに、2 つのネットワーク分析ルールとデフォルトのネットワーク分析ポリシーが設定されています。

- ネットワーク分析ルール A は、ネットワーク分析ポリシー A とトラフィックとの照合を前処理します。その後、このトラフィックを侵入ポリシー A によって検査できます。
- ネットワーク分析ルール B は、ネットワーク分析ポリシー B とトラフィックとの照合を前処理します。その後、このトラフィックを侵入ポリシー B によって検査できます。
- 残りのトラフィックはすべて、デフォルトのネットワーク分析ポリシーにより前処理されます。その後、アクセス コントロール ポリシーのデフォルト アクションに関連付けられている侵入ポリシーによってこのトラフィックを検査できます。

システムはトラフィックを前処理した後、侵入についてトラフィックを検査できます。図は、2 つのアクセス コントロール ルールとデフォルト アクションが設定されたアクセス コントロール ポリシーを示しています。

- アクセス コントロール ルール A は、一致したトラフィックを許可します。その後、トラフィックは侵入ポリシーA により検査されます。
- アクセス コントロール ルール B は、一致したトラフィックを許可します。その後、トラフィックは侵入ポリシー B により検査されます。
- アクセス コントロール ポリシーのデフォルト アクションは一致したトラフィックを許可します。その後、トラフィックはデフォルト アクションの侵入ポリシーによって検査されます。

各パケットの処理は、ネットワーク分析ポリシーと侵入ポリシーのペアにより制御されますが、このペアはユーザに合わせて調整**されません**。アクセス コントロール ポリシーが誤って設定されているため、ネットワーク分析ルール A とアクセス コントロール ルール A が同じトラフィックを処理しない場合を想定してください。たとえば、特定のセキュリティ ゾーンのトラフィックの処理を制御するポリシー ペアを意図していた場合に、誤って、異なるゾーンを使用するように 2 つのルールの条件を設定したとします。この誤設定により、トラフィックが誤って前処理される可能性があります。このような理由から、ネットワーク分析ルールとカスタム ポリシーを使用して前処理を調整することは、**高度な**タスクです。

単一の接続の場合、アクセス コントロール ルールよりも前にネットワーク分析ポリシーが選択されますが、いくつかの前処理（特にアプリケーション層の前処理）はアクセス コントロール ルールの選択後に実行されます。これは、カスタム ネットワーク分析ポリシーでの前処理の設定方法に**影響しません**。

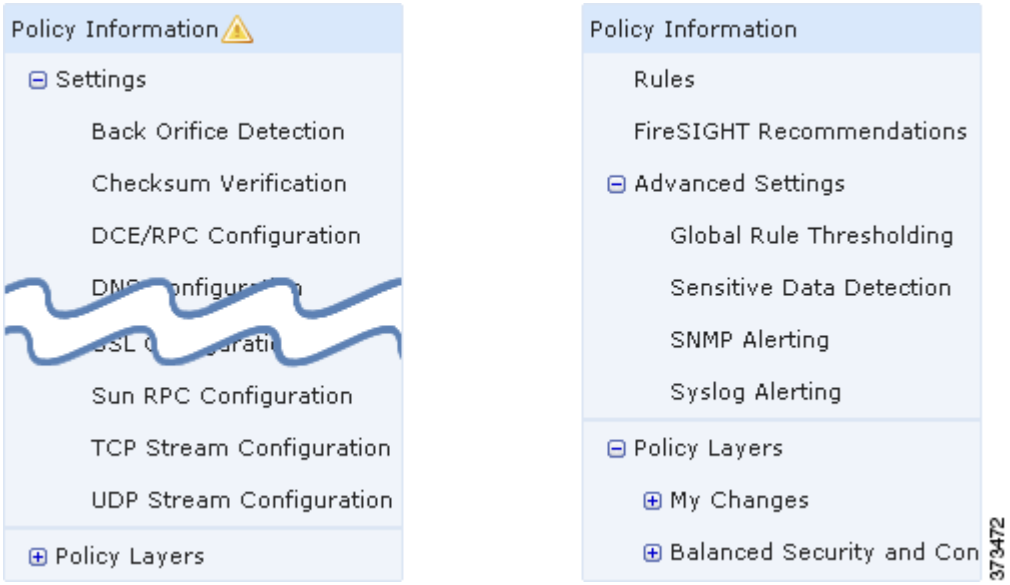
ナビゲーション パネルの使用

ライセンス： Protection

ネットワーク分析ポリシーと侵入ポリシーは同様の Web インターフェイスを使用して、設定への変更を編集して保存します。

- ネットワーク分析ポリシーの編集（26-4 ページ）
- 侵入ポリシーの編集（31-4 ページ）

いずれかのタイプのポリシーを編集するときに、Web インターフェイスの左側にナビゲーション パネルが表示されます。次の図は、ネットワーク分析ポリシー（左）と侵入ポリシー（右）のナビゲーション パネルを示しています。



境界線が、ポリシー層との直接対話を使用して構成可能なポリシー設定へのリンク（下側）とポリシー層との直接対話を使用せずに構成可能なポリシー設定へのリンク（上側）にナビゲーション パネルを分割します。いずれかの設定ページに移動するには、ナビゲーション パネル内の名前をクリックします。ナビゲーション パネルで影付きで強調表示されている項目は、現在の設定ページを示しています。たとえば、上の図では、[Policy Information] ページがナビゲーション パネルの右側に表示されます。

Policy Information

[Policy Information] ページには、一般的に使用される設定の設定オプションが表示されます。上記のネットワーク分析ポリシー パネルの図に示すように、ポリシーに未保存の変更がある場合は、ナビゲーション パネルの [Policy Information] の横にポリシー変更アイコン（⚠）が表示されます。このアイコンは、変更を保存すると表示されなくなります。

Rules（侵入ポリシーのみ）

侵入ポリシーの [Rules] ページでは、shared object rule、標準テキスト ルール、およびプリプロセッサ ルールのルール状態とその他の設定項目を設定できます。詳細については、ルールを使用した侵入ポリシーの調整（32-1 ページ）を参照してください。

FireSIGHT Recommendations（侵入ポリシーのみ）

侵入ポリシーの [FireSIGHT Recommendations] ページでは、ネットワーク上で検出されたオペレーティング システム、サーバ、およびクライアント アプリケーション プロトコルを、それらの資産を保護するために作成されたルールに関連付けることができます。これにより、モニタ対象のネットワークの特定ニーズに合わせて侵入ポリシーを調整できます。詳細については、ネットワーク資産に応じた侵入防御の調整（33-1 ページ）を参照してください。

Settings（ネットワーク分析ポリシーのみ）と Advanced Settings（侵入ポリシーのみ）

ネットワーク分析ポリシーの [Settings] ページでは、プリプロセッサとアクセス プリプロセッサの設定ページを有効または無効にすることができます。[Settings] リンクを展開すると、ポリシー内で有効になっているすべてのプリプロセッサを個々に設定する設定ページへのサブリンクが表示されます。詳細については、ネットワーク分析ポリシーでのプリプロセッサの設定（26-7 ページ）を参照してください。

侵入ポリシーの [Advanced Settings] ページでは、詳細設定ページと詳細設定のアクセス設定ページを有効または無効にすることができます。[Advanced Settings] リンクを展開すると、ポリシー内で有効になっているすべての詳細設定を個々に設定する設定ページへのサブリンクが表示されます。詳細については、侵入ポリシーの詳細設定の設定（31-7 ページ）を参照してください。

Policy Layers

[Policy Layers] ページには、ネットワーク分析ポリシーまたは侵入ポリシーを構成するレイヤの要約が表示されます。[Policy Layers] リンクを展開すると、ポリシー内のレイヤに関するサマリページへのサブリンクが表示されます。各レイヤのサブリンクを展開すると、レイヤで有効になっているすべてのルール、プリプロセッサ、または詳細設定を個々に設定する設定ページへのサブリンクが表示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）を参照してください。

競合の解決とポリシー変更の確定

ライセンス：Protection

ネットワーク分析ポリシーや侵入ポリシーを編集するときに、ポリシーに未保存の変更がある場合は、そのことを示すために、ナビゲーション パネルの [Policy Information] の横にポリシー変更アイコン（）が表示されます。変更をシステムに認識させるには、変更を保存（*確定*）する必要があります。

注　保存後は、変更を反映させるためにネットワーク分析ポリシーまたは侵入ポリシーを適用する必要があります。保存しないでポリシーを適用すると、最後に保存された設定が使用されます。侵入ポリシーは個別に再適用できますが、ネットワーク分析ポリシーは親アクセス コントロール ポリシーで適用されます。

編集の競合の解決

[Network Analysis Policy] ページ（[Policies] > [Access Control] を選択し、[Network Analysis] をクリック）と [Intrusion Policy] ページ（[Policies] > [Intrusion Policy] > [Intrusion Policy]）には、ポリシーに未保存の変更があるかどうか、および現在ポリシーを編集しているユーザの情報が表示されます。Cisco では、同時に 1 人だけがポリシーを編集することを推奨しています。同時編集を実行すると、次のようになります。

- ネットワーク分析ポリシーまたは侵入ポリシーを編集しているときに、同時に他のユーザが同じポリシーを編集し、ポリシーへの変更を保存した場合、ポリシーを確定すると、他のユーザの変更が上書きされることを警告するメッセージが表示されます。
- 同一ユーザとして複数の Web インターフェイス経由で同じネットワーク分析ポリシーまたは侵入ポリシーを編集し、1 つのインスタンスの変更を保存すると、他のインスタンスの変更を保存できなくなります。

設定の依存関係の解決

特定の分析を実行する場合、多くのプリプロセッサ ルールとセキュリティ ルールでは、最初に特定の方法でトラフィックをデコードまたは前処理するか、他の依存関係を割り当てる必要があります。ネットワーク分析ルールまたは侵入ポリシーを保存すると、システムは必要な設定を自動的に有効にするか、または警告を発して、設定を無効化してもトラフィックに影響がないことを示します。

- SNMP ルール アラートを追加しても、SNMP アラートを設定しなかった場合は、侵入ポリシーを保存できません。SNMP アラートを設定するかルール アラートを無効化してから、再度保存する必要があります。

- 侵入ポリシーに有効なセンシティブ データ ルールが含まれているときに、センシティブ データ プリプロセッサが有効になっていない場合は、侵入ポリシーを保存できません。システムがプリプロセッサを有効化してポリシーを保存することを許可するか、ルールを無効化して再度保存する必要があります。
- ネットワーク分析ポリシーで必要なプリプロセッサを無効化しても、まだポリシーを保存できます。ただし、ネットワーク分析ポリシーの Web インターフェイスでプリプロセッサは無効になっていても、システムは無効になっているプリプロセッサを自動的に現在の設定で使用します。詳細については、カスタム ポリシーの制限（23-13 ページ）を参照してください。
- ネットワーク分析ポリシーでインライン モードを無効にして、インライン正規化プリプロセッサを有効化した場合は、ポリシーを保存できます。ただし、正規化設定が無視されることが警告されます。インライン モードを無効化すると他の設定が無視されるので、プリプロセッサは、チェックサム検証やレート ベース攻撃の防御を含めて、トラフィックを変更またはブロックできます。詳細については、インライン展開でプリプロセッサがトラフィックに影響を与えることを許可する（26-6 ページ）およびインライン トラフィックの正規化（29-7 ページ）を参照してください。

ポリシーの変更の確定、破棄、キャッシュ

ネットワーク分析ポリシーまたは侵入ポリシーの編集時に、変更を保存しないでポリシー エディタを終了した場合、それらの変更はシステムによってキャッシュされます。変更は、システムからログアウトしたり、システム クラッシュが発生したりした場合でもキャッシュされます。システム キャッシュには、ユーザごとに 1 つのネットワーク分析ポリシーと 1 つの侵入ポリシーの未保存の変更しか格納されないため、同じタイプの別のポリシーを編集する場合は、その前に、行った変更を確定または破棄する必要があります。最初のポリシーに対する変更を保存せずに別のポリシーを編集した場合や、侵入ルールのアップデートをインポートした場合は、キャッシュされている変更が破棄されます。

ネットワーク分析ポリシーまたは侵入ポリシーのエディタの [Policy Information] ページで、ポリシーの変更を確定または破棄できます（ネットワーク分析ポリシーの編集（26-4 ページ）および侵入ポリシーの編集（31-4 ページ）を参照）。

次の表は、ネットワーク分析ポリシーまたは侵入ポリシーへの変更を保存または破棄する方法を要約して示しています。

表 23-1　ネットワーク分析ポリシーまたは侵入ポリシーへの変更の確定

目的	[Policy Information] ページでは、次の操作を実行できます
ポリシーへの変更を保存する	[Commit Changes] をクリックします。 システム ポリシーの設定によって、ネットワーク分析ポリシーまたは侵入ポリシーへの変更を確定するときに、それに関するコメントを入力するかどうか（または、コメントが必要かどうか）が決まります。システム ポリシーによって、監査ログに変更やコメントを記録するかどうかも決まります。詳細については、ネットワーク解析ポリシーの設定の構成（63-21 ページ）および侵入ポリシー設定の構成（63-22 ページ）を参照してください。
すべての未保存の変更を破棄する	[Discard Changes] をクリックしてから [OK] をクリックし、変更を破棄して、[Intrusion Policy] ページに移動します。変更を破棄しない場合は、[Cancel] をクリックして [Policy Information] ページに戻ります。
ポリシーを終了し、変更をキャッシュする	任意のメニューまたは別のページへの他のパスを選択します。終了時に、表示されたプロンプトで [Leave page] をクリックするか、[Stay on page] をクリックして高度なエディタに残ります。

CHAPTER 24

ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用

多数の管理対象デバイスが存在する大規模な組織では、さまざまな部署や事業部門、場合によってはさまざまな企業の固有のニーズをサポートするために、多数の侵入ポリシーやネットワーク分析ポリシーが存在することがあります。両方のポリシー タイプでの設定は*レイヤ*と呼ばれるビルディング ブロックに含まれており、それを使用することで効率的に複数のポリシーを管理することができます。

侵入ポリシーおよびネットワーク分析ポリシーのレイヤは、原則的に同じ方法で動作します。ポリシー タイプの作成および編集は、レイヤを意識せずに行えます。ポリシー設定を変更でき、ポリシーにユーザ レイヤを追加していない場合は、システムによって自動的に変更内容が単一の設定可能なレイヤ（最初は ***My Changes*** という名前が付けられています）に含められます。必要に応じて、最大 200 までレイヤを追加できます。それらのレイヤでは、設定の組み合わせを自由に設定できます。ユーザ レイヤのコピー、マージ、移動、削除を実行できます。最も重要なこととして、個々のユーザ レイヤを同じタイプの他のポリシーと共有できます。

詳細については、次の項を参照してください。

- レイヤ スタックについて（24-1 ページ） では、基本ポリシーを構成するユーザ設定可能な組み込み型のレイヤについて説明します。
- レイヤの管理（24-7 ページ） では、ポリシー内でレイヤを使用する方法について説明します。

レイヤ スタックについて

ライセンス： Protection

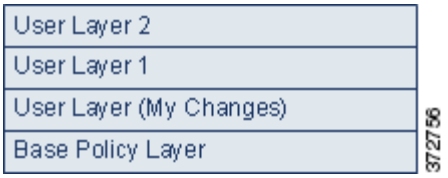
レイヤを追加していないネットワーク分析ポリシーまたは侵入ポリシーには、組み込み型で読み取り専用の基本ポリシー階層と、デフォルトで「My Changes」という名前が付けられているユーザ設定可能な単一のレイヤが含まれます。ユーザ設定可能なレイヤのコピー、マージ、移動、または削除を実行できます。また、任意のユーザ設定可能なレイヤを同じタイプの他のポリシーと共有できるように設定できます。

各ポリシー階層には、ネットワーク分析ポリシー内のすべてのプリプロセッサまたは侵入ポリシー内のすべての侵入ルールと詳細設定の完全な設定が含まれます。最下部の基本ポリシー階層には、ポリシーの作成時に選択した基本ポリシーのすべての設定が含まれます。上位レイヤの設定は、下位レイヤの同じ設定よりも優先されます。レイヤで明示的に設定されていない機能は、明示的に設定されている次の高いレイヤから設定を*継承します*。

システムはレイヤを*フラット化*します。つまり、ネットワーク トラフィックの処理時にすべての設定の蓄積効果のみを適用します。

ヒント　基本ポリシーのデフォルト設定にのみ基づいて、侵入ポリシーまたはネットワーク分析ポリシーを作成できます。侵入ポリシーの場合は、必要に応じて、FireSIGHT のルール状態の推奨を使用することもできます。

次の図は、基本ポリシー階層と初期設定の My Changes レイヤに加え、2 つのユーザ設定可能なレイヤ *User Layer 1* と *User Layer 2* が示されたレイヤ スタックの例を示しています。この図では、ユーザが追加したユーザ設定可能な各レイヤは、スタックの最上位のレイヤに配置されていることに注目してください。図の User Layer 2 は、最後に追加され、スタックの最上位にあります。



複数のレイヤを使用する場合は、次の点に注意してください。

- 以下のいずれかを実行する場合、ポリシー内の最上位のレイヤが読み取り専用レイヤであるか、または ポリシー間のレイヤの共有（24-11 ページ）で説明されてる共有レイヤであるときに、ユーザ設定可能なレイヤが最上位のレイヤとして侵入ポリシーに自動的に追加されます。
  - 侵入ポリシーの [Rules] ページからルール操作（つまり、ルール状態、イベント フィルタリング、動的状態、または警告）を変更する。詳細については、「ルールを使用した侵入ポリシーの調整（32-1 ページ）」を参照してください。
  - プリプロセッサ、侵入ルール、または詳細設定の有効化、無効化、または変更を実行する。

  システムによって追加されたレイヤのすべての設定は、新しいレイヤで発生した変更を除いてすべて継承されます。
- 最上位レイヤが共有レイヤの場合、次のアクションのいずれかを実行すると、システムはレイヤを追加します。
  - 他のポリシーとの最上位レイヤの共有
  - ポリシーへの共有レイヤの追加
- ルール アップデートにポリシーの変更を許可しているかどうかに関わらず、ルール アップデートでの変更は、レイヤで行った変更を上書きしません。これは、ルール アップデートでの変更が、基本ポリシー レイヤのデフォルト設定を決定する基本ポリシーで行われるためです。変更は常により上位のレイヤに加えられ、その変更によって、ルール アップデートが基本ポリシーに加えた変更が上書きされます。詳細については、「ルールの更新とローカル ルール ファイルのインポート（66-16 ページ）」を参照してください。

詳細については、次の項を参照してください。

- 基本レイヤについて（24-3 ページ）
- FireSIGHT 推奨レイヤについて（24-6 ページ）

基本レイヤについて

ライセンス：Protection

侵入ポリシーまたはネットワーク分析ポリシーの基本レイヤ（基本ポリシーとも呼ばれる）は、ポリシー内のすべてのコンフィギュレーションのデフォルト設定を定義するポリシーの最下位レイヤです。新しいポリシーを作成し、新しいレイヤを追加しないで設定を変更すると、その変更は My Changes レイヤに保存され、基本ポリシーの設定を上書きしますが変更はしません。

詳細については、次の項を参照してください。

- システムによって提供される基本ポリシーについて（24-3 ページ）
- カスタム基本ポリシーについて（24-3 ページ）
- 基本ポリシーの変更（24-4 ページ）
- ルール更新がシステムによって提供される基本ポリシーを変更することを許可する（24-4 ページ）

システムによって提供される基本ポリシーについて

ライセンス：Protection

Ciscoでは、ネットワーク分析ポリシーと侵入ポリシーの複数のペアを FireSIGHT システム と共に提供しています。システムによって提供されるネットワーク分析ポリシーおよび侵入ポリシーを使用して、Cisco 脆弱性調査チーム（VRT）のエクスペリエンスを活用することができます。これらのポリシーでは、VRT は侵入ルールおよびプリプロセッサ ルールの状態を設定し、プリプロセッサおよび他の詳細設定の初期設定も提供します。これらのシステムによって提供されるポリシーをそのまま使用したり、カスタム ポリシーのベースとして使用することができます。

システムによって提供されるポリシーをベースとして使用する場合、ルール更新をインポートすると、基本ポリシー内の設定が変更される場合があります。しかし、これらの変更内容をシステムによって提供される基本ポリシーに自動的に反映しないようにカスタム ポリシーを設定できます。これにより、ルール更新のインポートとは関係ないスケジュールで、システムによって提供される基本ポリシーを手動で更新できます。いずれの場合も、ルール更新が基本ポリシーに加えた変更によって My Changes または他のレイヤの設定が変更または上書きされることはありません。詳細については、ルール更新がシステムによって提供される基本ポリシーを変更することを許可する（24-4 ページ）を参照してください。

システムによって提供される侵入ポリシーおよびネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、Balanced Security and Connectivity ネットワーク分析ポリシーおよび Balanced Security and Connectivity 侵入ポリシーは共に機能し、侵入ルールの更新の際に両方とも更新できます。詳細については、システム付属のポリシーについて（23-9 ページ）を参照してください。

カスタム基本ポリシーについて

ライセンス：Protection

ネットワーク分析ポリシーまたは侵入ポリシーでシステムによって提供されるポリシーを基本ポリシーとして使用しない場合は、カスタム ポリシーをベースとして使用できます。カスタム ポリシーの設定を調整することで、最も役立つ方法でトラフィックを検査できます。これによって、管理対象デバイスのパフォーマンスが向上し、ユーザは生成されたイベントにさらに効率的に対応できるようになります。

最大 5 つのカスタム ポリシーをチェーンすることができます。5 つのうちの 4 つのポリシーで事前に作成されたポリシーが基本ポリシーとして使用され、5 つ目のポリシーでシステムによって提供されたポリシーをベースとして使用する必要があります。

別のポリシーのベースとして使用するカスタム ポリシーに加えた変更は、ベースとして使用するポリシーのデフォルト設定として自動的に使用されます。また、すべてのポリシーにはポリシー チェーン内の最終的なベースとしてシステムによって提供されるポリシーがあるので、カスタム基本ポリシーを使用していてもルール更新のインポートがポリシーに影響を与える場合があります。チェーン内の最初のカスタム ポリシー（システムによって提供されるポリシーをベースとして使用するポリシー）によってルール更新がそのベース ポリシーを変更することが許可されている場合は、ポリシーは影響を受ける可能性があります。この設定の変更の詳細については、ルール更新がシステムによって提供される基本ポリシーを変更することを許可する（24-4 ページ）を参照してください。

これらの設定に関係なく、基本ポリシーへの変更（ルール更新による変更、または基本ポリシーとして使用するカスタム ポリシーを変更する場合）によって My Changes または他のレイヤの設定が変更または上書きされることはありません。

基本ポリシーの変更

ライセンス：Protection

ネットワーク分析ポリシーまたは侵入ポリシーに対し異なる基本ポリシーを選択できます。また、オプションで、上位レイヤの変更に影響を与えることなく、ルール更新がシステムによって提供される基本ポリシーを変更することを許可することができます。

基本ポリシーを変更するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　ポリシーの編集中に、ナビゲーション パネルで [Policy Information] をクリックします。

[Policy Information] ページが表示されます。

ステップ 2　[Base Policy] ドロップダウンリストから基本ポリシーを選択します。

ステップ 3　オプションで、システムによって提供される基本ポリシーを選択する場合は、[Manage Base Policy] をクリックして、侵入ルールの更新によって基本ポリシーが自動的に変更されるかどうかを指定します。

詳細については、ルール更新がシステムによって提供される基本ポリシーを変更することを許可する（24-4 ページ）を参照してください。

ステップ 4　ポリシーの保存、編集の続行、変更の破棄、基本ポリシーのデフォルト設定の回復、またはシステム キャッシュ内の変更をそのままにした終了を行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

ルール更新がシステムによって提供される基本ポリシーを変更することを許可する

ライセンス：Protection

インポートするルール更新によって、システムによって提供されるポリシーには、ネットワーク分析プリプロセッサの設定変更、侵入ポリシーの詳細設定の変更、新規および更新済みの侵入ルール、および既存ルールの状態の変更が提供されます。ルール更新では、ルールを削除したり、新しいルール カテゴリとデフォルト変数を提供したりすることもできます。詳細については、「ルールの更新とローカル ルール ファイルのインポート（66-16 ページ）」を参照してください。

ルール更新は、プリプロセッサ、詳細設定およびルールの変更とともに、システムによって提供されるポリシーを常に変更します。デフォルト変数とルール カテゴリに対する変更はシステム レベルで処理されます。詳細については、「システムによって提供される基本ポリシーについて (24-3 ページ)」を参照してください。

システムによって提供されるポリシーを基本ポリシーとして使用するときは、ルール更新が基本ポリシー(この場合はシステムによって提供されるポリシーのコピー)を変更することを許可することができます。ルール更新で基本ポリシーの更新を許可する場合は、新しいルール更新によって、基本ポリシーとして使用するシステムによって提供されるポリシー対する変更と同じ変更が基本ポリシーにも加えられます。対応する設定を変更しなかった場合は、基本ポリシー内の設定によって、ポリシー内の設定が決定されます。ただし、ルール更新では、ポリシー内で行った変更は上書きされません。

ルール更新で基本ポリシーの更新を許可しない場合は、1 つ以上のルール更新のインポート後に、基本ポリシーを手動で更新できます。

ルール更新では、侵入ポリシー内のルール状態またはルール更新で基本の侵入ポリシーの更新が許可されているかどうかに関係なく、VRT が削除した侵入ルールが常に削除されます。ネットワーク トラフィックに変更を再適用するまで、現在適用されている侵入ポリシー ルールは次のように動作します。

- 無効になっているルールは無効のままになります。
- [Generate Events] に設定されたルールでは、トリガーされたときのイベントの生成が継続されます。
- [Drop and Generate Events] に設定されたルールでは、トリガーされたときのイベントの生成と違反パケットのドロップが継続されます。

次の両方の条件が満たされていない限り、ルール更新でカスタム基本ポリシーは変更されません。

- ルール更新が親ポリシーのシステムによって提供される基本ポリシー(つまり、カスタム基本ポリシーの起源となるポリシー)を変更することを許可している。
- 親の基本ポリシー内の対応する設定が上書きされる親ポリシー内の変更を実施していない。

両方の条件が満たされている場合は、親ポリシーを保存したときに、ルール更新内の変更が子ポリシー(つまり、カスタム基本ポリシーを使用したポリシー)に渡されます。

たとえば、ルール更新で以前に無効になっていた侵入ルールを有効にして、親の侵入ポリシー内のルール状態を変更していない場合は、親ポリシーを保存したときに、変更されたルール状態が基本ポリシーに渡されます。

同様に、ルール更新でデフォルトのプリプロセッサ設定を変更し、親のネットワーク分析ポリシーの設定を変更していない場合は、変更された設定は親ポリシーを保存したときに基本ポリシーに渡されます。

詳細については、「基本ポリシーの変更 (24-4 ページ)」を参照してください。

ルール更新がシステムによって提供される基本ポリシーを変更することを許可するには、次の手順を実行します。

アクセス: Admin/Intrusion Admin

ステップ 1　システムによって提供されるポリシーを基本ポリシーとして使用するポリシーの編集時に、ナビゲーション パネルで [Policy Information] をクリックします。

[Policy Information] ページが表示されます。

ステップ 2　[Manage Base Policy] をクリックします。

[Base Policy] 概要ページが表示されます。

ステップ 3　[Update when a new Rule Update is installed] チェックボックスをオンまたはオフにします。

このチェック ボックスをオフにしてポリシーを保存してから、ルール更新をインポートすると、[Base Policy] 概要ページに [Update Now] ボタンが表示され、そのページ上のステータス メッセージが更新されて、ポリシーが期限切れであることが示されます。必要に応じて、[Update Now] をクリックして、最近インポートしたルール更新内の変更で基本ポリシーを更新できます。

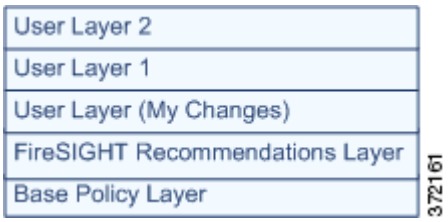
ステップ 4　ポリシーを保存するか、編集を続けるか、変更を破棄するか、基本ポリシーのデフォルト構成設定に戻すか、あるいはシステム キャッシュに変更を残して終了します。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

FireSIGHT 推奨レイヤについて

ライセンス： Protection

侵入ポリシーでルール状態の推奨を生成する場合は、その推奨に基づいてルール状態を自動的に変更するかどうかを選択できます。詳細については、ネットワーク資産に応じた侵入防御の調整（33-1 ページ）を参照してください。

下記の図に示すように、推奨されたルール状態を使用すると、侵入ポリシーの基本レイヤのすぐ上に読み取り専用の組み込み FireSIGHT 推奨システム レイヤが追加されます。



このレイヤは侵入ポリシー固有のものです。

それ以後、推奨されたルール状態を使用しないことを選択すると、FireSIGHT 推奨システム レイヤは削除されます。このレイヤは手動で削除できませんが、推奨されるルール状態を使用するかどうかを選択することで、サービスを追加したり削除することができます。

FireSIGHT 推奨レイヤを追加すると、ナビゲーション パネルの [Policy Layers] の下に FireSIGHT 推奨リンクが追加されます。このリンクから FireSIGHT 推奨レイヤ ページの読み取り専用ビューにアクセスして、[Rules] ページの推奨でフィルタリングされたビューを読み取り専用モードで表示できます。[Rules] ページでのルールの使用の詳細については、ルールを使用した侵入ポリシーの調整（32-1 ページ）を参照してください。

推奨されたルール状態を使用すると、ナビゲーション パネルの FireSIGHT 推奨リンクの下に [Rules] サブリンクも追加されます。[Rules] サブリンクから、FireSIGHT 推奨レイヤの [Rules] ページの読み取り専用画面にアクセスできます。このビューでは次の点に注意してください。

- 状態列にルール状態のアイコンがない場合、状態は基本ポリシーから継承されます。
- このビューまたは他の [Rules] ページ ビューの FireSIGHT 推奨列にルール状態のアイコンがない場合、このルールに対する推奨は存在しません。

ヒント　ルール状態が推奨されていない場合は、そのルールのオーバーヘッド評価が、推奨が生成されたときの [Recommendation Threshold (By Rule Overhead)] の設定値よりも高くなっています。詳細については、「ルール オーバーヘッドについて（33-3 ページ）」を参照してください。

レイヤの管理

ライセンス：Protection

[Policy Layers] ページでは、ネットワーク分析ポリシーまたは侵入ポリシーの完全なレイヤ スタックの単一ページの概要を示します。このページでは、共有レイヤおよび非共有レイヤの追加、レイヤのコピー、マージ、移動、および削除、各レイヤの概要ページへのアクセス、各レイヤ内の有効、無効、および上書きされている設定の設定ページへのアクセスを行うことができます。

各レイヤについて、次の情報が表示されます。

- レイヤが組み込み型レイヤ、共有ユーザ レイヤ、または非共有ユーザ レイヤであるかどうか
- どのレイヤに最上位の（つまり効果的な）プリプロセッサまたは詳細設定が含まれているか（機能名別に）
- 侵入ポリシーで、状態がレイヤで設定されている侵入ルールの数、および各ルール状態に設定されているルールの数

各レイヤのサマリにある機能名は、以下のように、設定がレイヤで有効、無効、上書き、または継承されているかを示します。

機能が以下の場合	機能名は以下となります
レイヤで有効	プレーン テキストで表示
レイヤで無効	取り消し線が引かれる
上位レイヤの設定によって上書きされる	イタリック テキストで表示
下位レイヤから継承される	表示されない

このページには、有効なすべてのプリプロセッサ（ネットワーク分析）または詳細設定（侵入）、また侵入ポリシーの場合は侵入ルールの最終的な効果の概要も示されます。

次の表に、[Policy Layers] ページで使用できるアクションを示します。

表 24-1　ネットワーク分析レイヤおよび侵入ポリシー レイヤの設定アクション

目的	操作
[Policy Information] ページの表示	[Policy Summary] をクリックします。 [Policy Information] ページで実行できる操作については、ルールを使用した侵入ポリシーの調整（32-1 ページ）、ネットワーク分析ポリシーの開始（26-1 ページ）、および 侵入ポリシーの開始（31-1 ページ）を参照してください。
レイヤのサマリ ページの表示	レイヤの行でレイヤ名をクリックするか、またはユーザ レイヤの横にある編集アイコン（  ）をクリックします。表示アイコン（  ）をクリックして、共有レイヤの読み取り専用のサマリ ページにアクセスすることもできます。 レイヤのサマリ ページで実行できる操作については、ポリシー間のレイヤの共有（24-11 ページ）、レイヤ内のプリプロセッサと詳細設定の設定（24-16 ページ）、および レイヤでの侵入ルールの設定（24-12 ページ）を参照してください。
レイヤ レベルのプリプロセッサまたは詳細設定の設定ページへのアクセス	レイヤの行で機能名をクリックします。基本ポリシーと共有レイヤでは、設定ページが読み取り専用であることに注意してください。詳細については、「レイヤ内のプリプロセッサと詳細設定の設定（24-16 ページ）」を参照してください。

表 24-1　ネットワーク分析レイヤおよび侵入ポリシー レイヤの設定アクション（続き）

目的	操作
ルール状態のタイプ別にフィルタリングされたレイヤ レベルのルール設定ページへのアクセス	レイヤのサマリでドロップおよび生成イベント（✖）、生成イベント（➡）、または無効（➡）のアイコンをクリックします。レイヤに選択したルール状態に設定されているルールが含まれていない場合は、ルールは表示されません。
ポリシーへのレイヤの追加	レイヤの追加（24-8 ページ）を参照してください。
別のポリシーからの共有レイヤの追加	ポリシー間のレイヤの共有（24-11 ページ）を参照してください。
レイヤの名前または説明の変更	レイヤの名前および説明の変更（24-9 ページ）を参照してください。
レイヤの移動、コピー、または削除	レイヤの移動、コピー、および削除（24-9 ページ）を参照してください。
すぐ下のレイヤとのレイヤのマージ	レイヤのマージ（24-10 ページ）を参照してください。

[Policy Layers] ページを使用するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] をクリックします。

[Policy Layers] サマリ ページが表示されます。

ステップ 2　ネットワーク分析レイヤおよび侵入ポリシー レイヤの設定アクション の表にある操作を実行できます。

ステップ 3　ポリシーの保存、編集の続行、変更の破棄、基本ポリシーのデフォルト設定の回復、またはシステム キャッシュ内の変更をそのままにした終了を行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

レイヤの追加

ライセンス：Protection

最大 200 のレイヤをネットワーク分析ポリシーまたは侵入ポリシーに追加できます。レイヤを追加すると、ポリシーで最上位レイヤとして表示されます。初期状態はすべての機能に対して [Inherit] で、侵入ポリシーでは、イベントのフィルタリング、動的状態、またはルール アクションのアラートは設定されません。

レイヤをネットワーク分析ポリシーまたは侵入ポリシーに追加するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] をクリックします。

[Policy Layers] ページが表示されます。

ステップ 2　[User Layers] の横にあるレイヤの追加アイコン（  ）をクリックします。

[Add Layer] ポップアップ ウィンドウが表示されます。

ステップ 3　一意のレイヤの**名前**を入力し、[OK] をクリックします。

新しいレイヤが [User Layers] の下に最上位レイヤとして表示されます。

ステップ 4　ポリシーの保存、編集の続行、変更の破棄、基本ポリシーのデフォルト設定の回復、またはシステム キャッシュ内の変更をそのままにした終了を行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

レイヤの名前および説明の変更

ライセンス： Protection

ネットワーク分析ポリシーまたは侵入ポリシー内のユーザ設定可能なレイヤの名前を変更できます。また、オプションで、レイヤの編集時に表示される説明を追加または変更できます。

レイヤの名前を変更する、および説明を追加または変更するには、次の手順を実行します。

アクセス： Admin/Intrusion Admin

ステップ 1　ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] をクリックします。

[Policy Layers] ページが表示されます。

ステップ 2　編集するユーザ レイヤの横にある編集アイコン（  ）をクリックします。

レイヤのサマリ ページが表示されます。

ステップ 3　次の操作を実行できます。

- レイヤの**名前**を変更します。
- レイヤの**説明**を追加または変更します。

ステップ 4　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

レイヤの移動、コピー、および削除

ライセンス： Protection

初期の My Changes レイヤを含む、ネットワーク分析ポリシーまたは侵入ポリシー内のユーザ レイヤをコピー、移動、または削除できます。以下の点に注意してください。

- レイヤをコピーすると、そのコピーが最上位レイヤとして表示されます。
- 共有レイヤをコピーすると、非共有コピーが作成されます。そのコピーは、任意で後で他のポリシーと共有できます。
- 共有レイヤは削除できません。共有が有効になっているレイヤで別のポリシーと共有していないものは、共有レイヤではありません。

レイヤをコピー、移動、または削除するには、次の手順を実行します。

アクセス： Admin/Intrusion Admin

ステップ 1　ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] をクリックします。

[Policy Layers] ページが表示されます。

ステップ 2　次の操作を実行できます。

- レイヤをコピーするには、コピーするレイヤのコピー アイコン（）をクリックします。

  ページが更新され、レイヤのコピーが最上位のレイヤとして表示されます。
- レイヤを [User Layers] ページ領域内で上下に移動させるには、レイヤ サマリ内の任意の空いている場所をクリックし、位置矢印（）が移動するレイヤの上または下の行を指すまでドラッグします。

  画面が更新され、レイヤが新しい場所に表示されます。
- レイヤを削除するには、削除するレイヤの削除アイコン（）をクリックし、[OK] をクリックします。

  ページが更新され、レイヤは削除されます。

ステップ 3　ポリシーの保存、編集の続行、変更の破棄、基本ポリシーのデフォルト設定の回復、またはシステム キャッシュ内の変更をそのままにした終了を行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

レイヤのマージ

ライセンス： Protection

ネットワーク分析ポリシーまたは侵入ポリシー内のユーザ設定可能なレイヤを、その下にある次のユーザ レイヤとマージできます。マージされたレイヤは、どちらかのレイヤに固有だったすべての設定を保持します。また、両方のレイヤに同じプリプロセッサ、侵入ルール、または詳細設定が含まれていた場合、上位のレイヤの設定を受け入れます。マージされたレイヤでは、下位レイヤの名前が保持されます。

他のポリシーに追加する共有レイヤを作成するポリシーでは、共有レイヤのすぐ上の非共有レイヤと共有レイヤをマージできますが、共有レイヤをその下の非共有レイヤとマージすることはできません。

別のポリシーに作成した共有レイヤを追加するポリシーでは、共有レイヤをそのすぐ下の非共有レイヤとマージできますが、作成されたレイヤは共有されなくなります。非共有レイヤをその下の共有レイヤにマージすることはできません。

ユーザ レイヤをその下にあるユーザ レイヤとマージするには、次の手順を実行します。

アクセス： Admin/Intrusion Admin

ステップ 1　ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] をクリックします。

[Policy Layers] ページが表示されます。

ステップ 2　2 つのレイヤの上部にあるマージ アイコン（）をクリックし、[OK] をクリックします。

ページが更新され、レイヤがその下のレイヤとマージされます。

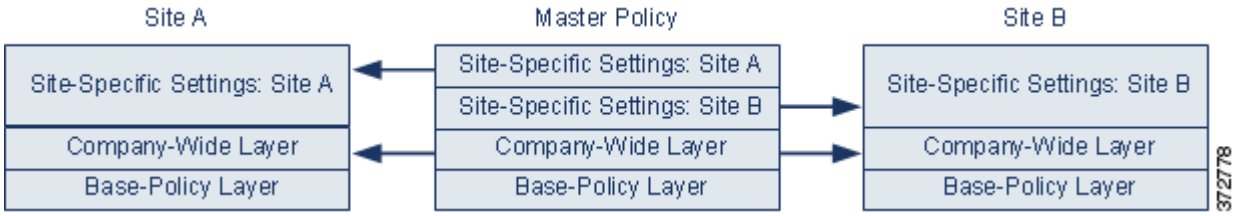
ステップ 3　ポリシーの保存、編集の続行、変更の破棄、基本ポリシーのデフォルト設定の回復、またはシステム キャッシュ内の変更をそのままにした終了を行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

ポリシー間のレイヤの共有

ライセンス：Protection

ユーザ設定可能なレイヤを同じタイプの他のポリシー（侵入またはネットワーク分析）と共有できます。共有レイヤ内の設定を変更し、変更をコミットすると、システムは共有レイヤを使用するすべてのポリシーを更新し、影響を受けたすべてのポリシーのリストが提供されます。レイヤを作成したポリシー内の共有レイヤ機能の設定のみを変更できます。

以下の図には、サイト固有のポリシーのソースとして機能するマスター ポリシーの例が示されています。



図のマスター ポリシーには、Site A と Site B のポリシーに適用可能な設定を持つ全社的レイヤが含まれます。また、各ポリシーのサイト固有のレイヤも含まれます。たとえば、ネットワーク分析ポリシーの場合、Site A には監視対象ネットワークに Web サーバがないため、保護したり、HTTP インスペクション プリプロセッサのオーバーヘッドを処理したりする必要はありませんが、両方のサイトで TCP ストリームの前処理が必要になる場合があります。両方のサイトで共有する全社的レイヤで TCP ストリーム処理を有効にし、Site A で共有するサイト固有のレイヤで HTTP Inspect プリプロセッサを無効にして、Site B で共有するサイト固有のレイヤで HTTP Inspect プリプロセッサを有効にできます。サイト固有のポリシーで上位レイヤの設定を編集することで、必要に応じて、設定の調整によって各サイトのポリシーをさらに調整することもできます。

この例のマスター ポリシーでフラット化された設定値そのものがトラフィックを監視するのに役立つ訳ではありませんが、サイト固有のポリシーを設定および更新する際に時間が節約されるため、ポリシーのレイヤで活用することができます。

その他にも多くのレイヤ設定が可能です。たとえば、企業、部門、ネットワーク、さらにはユーザごとにポリシーのレイヤを定義できます。侵入ポリシーの場合は、一方のレイヤに詳細設定を含め、もう一方にルール設定を含めることもできます。

ヒント　基本ポリシーが共有するレイヤが作成されたカスタム ポリシーである場合、ポリシーに共有レイヤを追加することはできません。変更を保存しようとすると、ポリシーに循環依存関係が含まれていることを示すエラー メッセージが表示されます。詳細については、「カスタム基本ポリシーについて（24-3 ページ）」を参照してください。

他のポリシーとレイヤを共有するには、次の手順を実行する必要があります。

- 共有するレイヤのレイヤ サマリ ページで共有を有効にします。
- 共有するポリシーの [Policy Layers] ページで共有レイヤを追加します。

別のポリシーで使用されているレイヤの共有を無効にすることはできません。まずレイヤを他のポリシーから削除するか、他のポリシーを削除する必要があります。

他のポリシーとのレイヤの共有を有効または無効にするには、次の手順を実行します。

アクセス： Admin/Intrusion Admin

ステップ 1　ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] をクリックします。

[Policy Layers] ページが表示されます。

ステップ 2　その他のポリシーと共有するレイヤの横にある編集アイコン（  ）をクリックします。

レイヤのサマリ ページが表示されます。

ステップ 3　[Sharing] チェックボックスをオン（有効）またはオフ（無効）にします。

ステップ 4　ポリシーの保存、編集の続行、変更の破棄、基本ポリシーのデフォルト設定の回復、またはシステム キャッシュ内の変更をそのままにした終了を行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

共有レイヤをポリシーに追加するには、次の手順を実行します。

アクセス： Admin/Intrusion Admin

ステップ 1　ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] をクリックします。

[Policy Layers] ページが表示されます。

ステップ 2　[User Layers] の横にある共有レイヤの追加アイコン（  ）をクリックします。

[Add Shared Layer] ポップアップ ウィンドウが表示されます。

ステップ 3　[Add Shared Layer] ドロップダウンリストから追加する共有レイヤを選択し、[OK] をクリックします。

[Policy Layers] サマリ ページが表示され、選択した共有レイヤがポリシーの最上位レイヤとして表示されます。

その他のポリシーに共有レイヤがない場合、ドロップダウンリストは表示されません。ポップアップ ウィンドウで [OK] または [Cancel] をクリックすると、[Policy Layers] サマリ ページに戻ります。

ステップ 4　ポリシーの保存、編集の続行、変更の破棄、基本ポリシーのデフォルト設定の回復、またはシステム キャッシュ内の変更をそのままにした終了を行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

レイヤでの侵入ルールの設定

ライセンス： Protection

侵入ポリシーでは、ユーザ設定可能な任意のレイヤで、ルールのルール状態、イベント フィルタリング、動的状態、アラート、およびルール コメントを設定できます。変更を加えるレイヤにアクセスした後、そのレイヤの [Rules] ページの設定を、侵入ポリシーの [Rules] ページの設定と同じように追加します。ルールを使用した侵入ポリシーの調整（32-1 ページ）を参照してください。

レイヤの [Rules] ページで個々のレイヤ設定を表示することも、[Rules] ページのポリシー ビューですべての設定の最終的な効果を表示することもできます。[Rules] ページのポリシー ビューのルール設定を変更する場合、ポリシーの最上位のユーザ設定可能なレイヤを変更します。[Rules] ページにあるレイヤ ドロップダウンリストを使用して、別のレイヤに切り替えることができます。

次の表では、複数のレイヤで同じ種類の設定を構成した場合の結果について説明しています。

表 24-2　レイヤ ルールの設定

設定可能なレイヤ数	設定の種類	目的
1	ルールの状態	下位レイヤのルールに対して設定されたルール状態を上書きします。また、下位レイヤで設定されたそのルールのすべてのしきい値、抑制、レートベースのルール状態、およびアラートを無視します。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。 基本ポリシーまたは下位レイヤからルールのルール状態を継承したい場合は、ルール状態を [Inherit] に設定します。侵入ポリシーの [Rules] ページで作業している場合は、ルール状態を [Inherit] に設定できないことに注意してください。 また、特定のレイヤについてルール状態の設定を [Rules] ページで表示すると色分けされて表示されることにも留意してください。有効な状態が下位レイヤで設定されているルールは黄色でハイライトされ、有効な状態が上位レイヤで設定されているルールは赤色でハイライトされ、有効な状態が現在のレイヤで設定されている場合は強調表示されません。侵入ポリシーの [Rules] ページはすべてのルール設定の最終的な効果の複合ビューであるため、ルール状態はこのページでは色分けされません。
1	threshold SNMP アラート	下位レイヤのルールの同じ種類の設定を上書きします。しきい値を設定すると、レイヤのルールの既存のしきい値が上書きされることに注意してください。詳細については、イベントしきい値の設定（32-25 ページ）およびSNMP アラートの追加（32-36 ページ）を参照してください。
1 つ以上	抑制 レート ベースのルール状態	選択した各ルールの同じ種類の設定を、ルール状態がそのルールに対して設定された最初の下位レイヤまで累積的に組み合わせます。ルール状態が設定されているレイヤより下の設定は無視されます。詳細については、侵入ポリシー単位の抑制の設定（32-30 ページ）および動的ルール状態の追加（32-33 ページ）を参照してください。
1 つ以上	comment	ルールにコメントを追加します。コメントは、ポリシー固有またはレイヤ固有ではなく、ルール固有です。任意のレイヤの 1 つのルールに 1 つ以上のコメントを追加できます。詳細については、「ルールに関するルール コメントの追加（32-10 ページ）」を参照してください。

たとえば、あるレイヤでルール状態を [Drop and Generate Events] に設定し、それよりも上位のレイヤで [Disabled] に設定した場合、侵入ポリシーの [Rules] ページには、ルールが無効であることが示されます。

別の例として、あるレイヤでルールの送信元ベースの抑制を 192.168.1.1 に設定し、別のレイヤでそのルールの宛先ベースの抑制を 192.168.1.2 に設定した場合、[Rules] ページには、送信元アドレス 192.168.1.1 と宛先アドレス 192.168.1.2 に関するイベントを抑制する累積的な結果が示されます。抑制およびレート ベースのルール状態の設定では、選択した各ルールの同じ種類の設定が、ルール状態がそのルールに対して設定された最初の下位レイヤまで累積的に組み合わせられることに注意してください。ルール状態が設定されているレイヤより下の設定は無視されます。

レイヤでルールを変更するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　侵入ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] を展開し、変更するポリシー レイヤを展開します。

ステップ 2　変更するポリシー レイヤのすぐ下にある [Rules] をクリックします。

レイヤの [Rules] ページが表示されます。

表レイヤ ルールの設定のいずれかの設定を変更できます。侵入ルールの設定の詳細については、ルールを使用した侵入ポリシーの調整（32-1 ページ）を参照してください。

編集可能なレイヤから個々の設定を削除するには、そのレイヤの [Rules] ページでルール メッセージをダブルクリックして、ルールの詳細を表示します。削除する設定の横にある [Delete] をクリックして [OK] を 2 回クリックします。

ステップ 3　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

マルチレイヤ ルール設定の削除

ライセンス：Protection

侵入ポリシーの [Rules] ページで 1 つ以上のルールを選択し、侵入ポリシーの複数のレイヤから特定のタイプのイベント フィルタ、動的状態、またはアラートを同時に削除できます。

システムは、すべての設定を削除するか、ルール状態がルールに対して設定されているレイヤに遭遇するまで、下位方向にある各レイヤの同じ種類の設定を削除します。ルール状態が設定されているレイヤに遭遇したら、そのレイヤから設定を削除し、設定タイプの削除を停止します。

共有レイヤまたは基本ポリシーで同じタイプの設定に遭遇したときに、ポリシーの最上位のレイヤが編集可能である場合、システムはそのルールの残りの設定およびルール状態をその編集可能なレイヤにコピーします。そうではない場合、ポリシーの最上位のレイヤが共有レイヤであれば、システムは新しい編集可能なレイヤをその共有レイヤの上に作成し、そのルールの残りの設定およびルール状態をその編集可能なレイヤにコピーします。

注　共有レイヤまたは基本ポリシーから派生したルール設定を削除すると、下位レイヤまたは基本ポリシーからこのルールへの変更は無視されます。下位レイヤまたは基本ポリシーからの変更を無視しないようにするには、最上位のレイヤのサマリ ページでルール状態を [Inherit] に設定します。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

複数のレイヤでルール設定を削除するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　侵入ポリシーの編集中に、ナビゲーション パネルで [Policy Information] のすぐ下にある [Rules] をクリックします。

ヒント　また、任意のレイヤの [Rules] ページでレイヤのドロップダウンリストから [Policy] を選択するか、[Policy Information] ページの [Manage Rules] を選択することもできます。

侵入ポリシーの [Rules] ページが表示されます。

ステップ 2　複数の設定を削除するルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、列の一番上にあるチェック ボックスをオンにします。

ルールの検索については、侵入ポリシー内のルール フィルタ処理について（32-11 ページ）および 侵入ポリシー内のルール フィルタの設定（32-21 ページ）を参照してください。

ステップ 3　次の選択肢があります。

- ルールのすべてのしきい値を削除するには、[Event Filtering] > [Remove Thresholds] を選択します。
- ルールのすべての抑制を削除するには、[Event Filtering] > [Remove Suppressions] を選択します。
- ルールのすべてのレートベースのルール状態を削除するには、[Dynamic State] > [Remove Rate-Based Rule States] を選択します。
- ルールのすべての SNMP アラート設定を削除するには、[Alerting] > [Remove SNMP Alerts] を選択します。

確認のポップアップ ウィンドウが表示されます。

注　共有レイヤまたは基本ポリシーから派生したルール設定を削除すると、下位レイヤまたは基本ポリシーからこのルールへの変更は無視されます。下位レイヤまたは基本ポリシーからの変更を無視しないようにするには、最上位のレイヤのサマリ ページでルール状態を [Inherit] に設定します。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

ステップ 4　[OK] をクリックします。

システムは選択された設定を削除し、ルールの残りの設定をポリシーの最上位の編集可能なレイヤにコピーします。システムが残りの設定をコピーする方法に影響を与える条件については、この手順の概要を参照してください。

ステップ 5　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

カスタム基本ポリシーからのルール変更の受け入れ

ライセンス： Protection

レイヤを追加していないカスタム ネットワーク分析ポリシーまたは侵入ポリシーが別のカスタム ポリシーを基本ポリシーとして使用するとき、以下を行う場合は、そのルール状態を継承するようにルールを設定する必要があります。

- 基本ポリシーのルールに設定されたイベント フィルタ、動的状態、または SNMP アラートを削除する場合
- 基本ポリシーとして使用する他のカスタム ポリシー内のルールに行った後続の変更をルールが受け入れるようにする場合

次の手順では、これを実現する方法について説明します。階層を追加したポリシーでこれらのルールの設定を受け入れるには、マルチレイヤ ルール設定の削除（24-14 ページ）を参照してください。

レイヤを追加しなかったポリシー内のルール変更を受け入れるには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　侵入ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] リンクを展開し、[My Changes] リンクを展開します。

ステップ 2　[My Changes] のすぐ下にある [Rules] リンクをクリックします。

My Changes レイヤの [Rules] ページが表示されます。

ステップ 3　設定を受け入れるルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、列の一番上にあるチェック ボックスをオンにします。

ルールの検索については、侵入ポリシー内のルール フィルタ処理について（32-11 ページ）および 侵入ポリシー内のルール フィルタの設定（32-21 ページ）を参照してください。

ステップ 4　[Rule State] ドロップダウンリストから、[Inherit] を選択します。

ステップ 5　ポリシーを保存するか、編集を続行するか、変更内容を破棄するか、ベース ポリシーのデフォルト設定に戻すか、またはシステム キャッシュの変更を反映せずに終了します。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

レイヤ内のプリプロセッサと詳細設定の設定

ライセンス：Protection

ネットワーク分析ポリシーでプリプロセッサを設定するときと、侵入ポリシーで詳細詳細を設定するときのメカニズムは同様です。プリプロセッサの有効化および無効化はネットワーク分析の [Settings] ページで行うことができ、侵入ポリシーの詳細設定の有効化および無効化は侵入ポリシーの [Advanced Settings] ページで行うことができます。これらのページでは、すべての関連機能の有効な状態の概要も示されます。たとえば、ネットワーク分析 SSL プリプロセッサが、あるレイヤでは無効になっていて上位レイヤでは有効になっている場合、[Settings] ページにはプリプロセッサが有効であるとして表示されます。これらのページで行った変更は、ポリシーの最上位レイヤに表示されます。

また、プリプロセッサまたは詳細設定を有効化または無効化したり、ユーザ設定可能なレイヤのサマリ ページの設定ページにアクセスしたりできます。このページで、レイヤの名前および説明を変更し、レイヤを同じタイプの他のポリシーと共有するかどうかを設定できます。詳細については、ポリシー間のレイヤの共有（24-11 ページ）を参照してください。ナビゲーション パネルの [Policy Layers] の下のレイヤの名前を選択することによって、別のレイヤのサマリ ページに切り替えることができます。

プリプロセッサまたは詳細設定を有効にすると、その機能の設定ページへのサブリンクがナビゲーション パネルのレイヤの名前の下に表示され、編集アイコン（  ）がそのレイヤのサマリ ページの機能の横に表示されます。レイヤで機能を無効にしたり、[Inherit] に設定した場合はこれらは表示されません。

プリプロセッサまたは詳細設定の状態（有効または無効）を設定すると、下位レイヤでのその機能の状態と構成設定が上書きされます。プリプロセッサまたは詳細設定についてその状態と設定を基本ポリシーまたは下位レイヤから継承する場合、状態を [Inherit] に設定します。[Settings] または [Advanced Settings] ページで操作するときには、[Inherit] の選択項目は使用できないことに注意してください。

各レイヤのサマリ ページに表示される色分けは、次のように有効な設定が上位レイヤ、下位レイヤ、または現在のレイヤにあることを示します。

- 赤色：有効な設定は上位レイヤにあります
- 黄色：有効な設定は下位レイヤにあります
- 陰影なし：有効な設定は現在のレイヤにあります

[Settings] および [Advanced Settings] ページは、関連するすべての設定の複合ビューであるため、これらのページは有効な設定の位置を示すためにカラー コーディングを使用しません。

システムは、機能が有効にされている最上位レイヤの設定を使用します。設定を明示的に変更しなかった場合は、デフォルト設定が使用されます。たとえば、あるレイヤでネットワーク分析 DCE/RPC プリプロセッサを有効にして変更し、それより上位のレイヤでプリプロセッサを有効にするが変更はしない場合、システムは上位レイヤのデフォルト設定を使用します。

次の表に、ユーザ設定可能なレイヤのサマリ ページで実行できる操作を示します。

表 24-3　[Layer] サマリ ページの操作

目的	操作
レイヤの名前または説明の変更	[Name] または [Description] の新しい値を入力します。
他の侵入ポリシーとのレイヤの共有	[Allow this layer to be used by other policies] を選択します。 詳細については、「ポリシー間のレイヤの共有（24-11 ページ）」を参照してください。
現在のレイヤのプリプロセッサ/詳細設定の有効化または無効化	機能の横にある [Enabled] または [Disabled] をクリックします。 有効にすると、設定ページへのサブリンクがナビゲーション パネルのレイヤ名の下に表示され、編集アイコン（  ）が機能の横のサマリ ページに表示されます。 無効にすると、サブリンクと編集アイコンは削除されます。
現在のレイヤの下にある最上位レイヤの設定からのプリプロセッサ/詳細設定の状態および設定の継承	[Inherit] をクリックします。 ページが更新され、機能を有効にした場合は、ナビゲーション パネルでの機能のサブリンクと編集アイコンは表示されなくなります。
有効なプリプロセッサ/詳細設定の設定ページへのアクセス	現在の設定を変更するには、編集アイコン（  ）または機能のサブリンクをクリックします。 Back Orifice プリプロセッサにはユーザ設定可能なオプションがないことに注意してください。

ユーザ レイヤでプリプロセッサ/詳細設定を変更するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] を展開し、変更するレイヤの名前をクリックします。

レイヤのサマリ ページが表示されます。

ステップ 2　[Layer] サマリ ページの操作 の表にある操作を実行できます。

ステップ 3　ポリシーを保存するか、編集を続けるか、変更を破棄するか、基本ポリシーのデフォルト構成設定に戻すか、あるいはシステム キャッシュに変更を残して終了します。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

トラフィックの前処理のカスタマイズ

アクセス コントロール ポリシーにおける詳細設定の多くでは、侵入検知設定と予防設定についての専門的な知識が必要です。通常、詳細設定はほとんど、あるいはまったく変更する必要がありません。詳細設定は導入環境ごとに異なります。

この章では、次の設定を行う方法について説明します。

- アクセス コントロールのデフォルト侵入ポリシーの設定（25-1 ページ）では、アクセス コントロール ポリシーのデフォルトの侵入ポリシーを変更する方法について説明します。このポリシーはトラフィックの最初の検査に適用され、その後でトラフィックの詳細な検査方法が決定されます。
- ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）では、一致するトラフィックを前処理するためのカスタムのネットワーク分析ポリシーを割り当てて、特定のセキュリティ ゾーン、ネットワーク、および VLAN に対する特定のトラフィックの前処理オプションをカスタマイズする方法について説明します。

他の章では、アクセス コントロール ポリシーに対するポリシー全体の前処理とパフォーマンスのオプションについて説明します。詳細については、以下を参照してください。

- トランスポート/ネットワークの詳細設定の構成（29-2 ページ）
- パッシブ展開における前処理の調整（30-1 ページ）
- 侵入防御パフォーマンスの調整（18-10 ページ）
- ファイルおよびマルウェアのインスペクション パフォーマンスおよびストレージの調整（18-22 ページ）

アクセス コントロールのデフォルト侵入ポリシーの設定

ライセンス： すべて

各アクセス コントロール ポリシーには、*デフォルトの侵入ポリシー*があります。トラフィックはまずこのポリシーに基づいて検査され、その後でそのトラフィックの詳細な検査方法がシステムにより決定されます。トラフィックに適用するアクセス コントロール ルールを決定する前に、そのトラフィックの最初の数パケットの**通過を許可**しなければならない場合があるため、デフォルトの侵入ポリシーが必要になります。これらの通過パケットが未検査のまま宛先に到達することがないように、デフォルト侵入ポリシーでパケットを検査し、侵入イベントを生成されます。

デフォルトの侵入ポリシーは、アプリケーション制御および URL フィルタリングを実行する場合に特に有用です。これは、クライアントとサーバの間の接続が未確立な状態でアプリケーションを識別したり URL をフィルタ処理したりすることができないためです。たとえば、特定のアプリケーションまたは URL の条件が定義されたアクセス コントロール ルールの他のすべての条件にパケットが一致する場合、そのパケットと後続のパケット（通常は 3 ～ 5 パケット）は、接続が確立してアプリケーションまたは URL の識別が完了するまで通過が許可されます。

通過が許可されたパケットは、デフォルトの侵入ポリシーに基づいて検査されます。これにより、イベントを生成したり、悪意のあるトラフィックをブロックしたり（インライン配置の場合）できます。接続に適用されるアクセス コントロール ルールまたはデフォルト アクションが決定されると、その接続の残りのパケットが適宜処理および検査されます。

アクセス コントロール ポリシーを作成する場合、そのデフォルトの侵入ポリシーは**最初に**選択したデフォルト アクションに基づいて設定されます。アクセス コントロールのデフォルト侵入ポリシーは、まず以下のように設定されます。

- 最初に [Intrusion Prevention] デフォルト アクションを選択した場合、アクセス コントロール ポリシーのデフォルトの侵入ポリシーは Balanced Security and Connectivity（システムによって提供されるポリシー）になります。
- 最初に [Block all traffic] または [Network Discovery] デフォルト アクションを選択した場合、アクセス コントロール ポリシーのデフォルトの侵入ポリシーは No Rules Active になります。このオプションを選択すると、前述の許可パケットでの侵入インスペクションが無効になります。ただし、侵入データの検査が必要でない場合は、これによりパフォーマンスが向上します。

注　Protection のライセンスが不要な検出のみの展開など、侵入インスペクションを実行していない場合は、デフォルトの侵入ポリシーとして No Rules Active ポリシーを使用してください。詳細については、IPS または検出のみのパフォーマンスの考慮事項（12-22 ページ）を参照してください。

アクセス コントロール ポリシーを作成した後でデフォルト アクションを変更する場合は、デフォルトの侵入ポリシーが自動的に変更**されない**ことに注意してください。手動で変更するには、アクセス コントロール ポリシーの詳細オプションを使用します。

アクセス コントロール ポリシーのデフォルトの侵入ポリシーを変更するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　デフォルトの侵入ポリシーを変更するアクセス コントロール ポリシーで [Advanced] タブを選択し、[Network Analysis and Intrusion Policies] セクションの横にある編集アイコン（）をクリックします。

[Network and Analysis Policies] ダイアログボックスが表示されます。

ステップ 2　[Intrusion Policy used before Access Control rule is determined] ドロップダウンリストから、デフォルトの侵入ポリシーを選択します。システムによって提供されたポリシーまたはユーザが作成したポリシーを選択できます。

ユーザが作成したポリシーを選択した場合は、編集アイコン（  ）をクリックして、新しいウィンドウでポリシーを編集できます。システムによって提供されたポリシーは編集できません。

注意　Ciscoの担当者から指示された場合を除き、`Experimental Policy 1` は使用**しないで**ください。Ciscoでは、試験用にこのポリシーを使用します。

ステップ 3　選択したポリシーと一致する変数設定を選択します。

オプションで、[Intrusion Policy Variable Set] ドロップ ダウンを使用して、選択した侵入ポリシーに関連付けられている変数セットを変更します。編集アイコン（）をクリックして、新しいウィンドウで設定されている変数セットを編集することもできます。変数セットを変更しない場合は、システムはデフォルトのセットを使用します。詳細については、変数セットの操作（3-19 ページ）を参照してください。

ステップ 4　[OK] をクリックして変更を保存します。

変更を反映するには、アクセス コントロール ポリシーを適用する必要があります。

ネットワーク分析ポリシーによる前処理のカスタマイズ

ライセンス： すべて

サポートされるデバイス： 機能によって異なる

*ネットワーク分析ポリシー*では、特に侵入しようとしている怪しいトラフィックなどをより詳細に評価できるように、トラフィックを復号化および前処理する方法を制御します。トラフィックの前処理は、セキュリティ インテリジェンスのブラックリスト登録およびトラフィックの復号化の後、侵入ポリシーによるパケット インスペクションの前に行われます。デフォルトでは、システムによって提供される Balanced Security and Connectivity ネットワーク分析ポリシーが、アクセス コントロール ポリシーによって処理される*すべて*のトラフィックに適用されます。

ヒント　システムによって提供される Balanced Security and Connectivity ネットワーク分析ポリシーおよび Balanced Security and Connectivity 侵入ポリシーは連携して機能し、どちらも侵入ルールと一緒に更新できます。しかし、ネットワーク分析ポリシーは前処理オプションの大部分を制御するのに対し、侵入ポリシーは侵入ルールの大部分を制御します。

前処理を簡単に調整するには、デフォルトとしてカスタムのネットワーク分析ポリシーを作成して使用します。詳しくは、カスタム ネットワーク分析ポリシーの作成（26-2 ページ）を参照してください。使用可能な調整オプションは、プリプロセッサによって異なります。

複雑な展開を管理する上級ユーザの場合は、複数のネットワーク分析ポリシーを作成して、それぞれが異なるトラフィックを前処理するように設定できます。さらに、トラフィックのセキュリティ ゾーン、ネットワーク、または VLAN に応じて前処理が制御されるようにこれらのポリシーを設定できます。（ASA FirePOWER デバイスでは、VLAN に応じて前処理を制限することはできません。）

これを行うには、アクセス コントロール ポリシーにカスタムの*ネットワーク分析ルール*を追加します。各ルールに含まれる内容は、次のとおりです。

- 一連のルール条件。前処理の対象となる特定のトラフィックを識別します。
- 関連付けられたネットワーク分析ポリシー。すべてのルールの条件を満たすトラフィックを前処理するときに使用されます。

システムがトラフィックを前処理する時間になると、ネットワーク分析ルールの番号順（昇順）にパケットが照合されます。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。

注　プリプロセッサを無効にしても、前処理されたパケットを有効な侵入ルールまたはプリプロセッサ ルールと照合して評価する必要がある場合は、システムによりプリプロセッサが自動的に有効になります。ただし、ネットワーク分析ポリシーの Web インターフェイスでは、プリプロセッサが無効として表示されます。特に複数のカスタム ネットワーク分析ポリシーを使用した前処理の調整は、**高度な**タスクです。前処理と侵入インスペクションは密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーが互いに補完することを許可する場合は慎重になる**必要があります**。詳細については、カスタム ポリシーの制限（23-13 ページ）を参照してください。

詳細については、次の項を参照してください。

- アクセス コントロールのデフォルト ネットワーク分析ポリシーの設定（25-4 ページ）
- 前処理するトラフィックのネットワーク分析ルールによる指定（25-5 ページ）
- ネットワーク分析ルールの管理（25-10 ページ）

アクセス コントロールのデフォルト ネットワーク分析ポリシーの設定

ライセンス： すべて

デフォルトでは、システムによって提供される Balanced Security and Connectivity ネットワーク分析ポリシーは、アクセス コントロール ポリシーによって処理されるすべてのトラフィックに適用されます。トラフィックの前処理オプションを調整するネットワーク分析ルールを追加した場合、そのルールで処理されないすべてのトラフィックがデフォルトのネットワーク分析ポリシーに基づいて前処理されます。

このデフォルトのポリシーを変更するには、アクセス コントロール ポリシーの詳細設定を使用します。

アクセス コントロール ポリシーのデフォルト ネットワーク分析ポリシーを変更するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　デフォルトのネットワーク分析ポリシーを変更するアクセス コントロール ポリシーで、[Advanced] タブを選択し、[Network Analysis and Intrusion Policies] セクションの横にある編集アイコン（  ）をクリックします。

[Network and Analysis Policies] ダイアログボックスが表示されます。

ステップ 2　[Default Network Analysis Policy] ドロップダウンリストから、デフォルトのネットワーク分析ポリシーを選択します。システムによって提供されたポリシーまたはユーザが作成したポリシーを選択できます。

ユーザが作成したポリシーを選択した場合は、編集アイコン（  ）をクリックして、新しいウィンドウでポリシーを編集できます。システムによって提供されたポリシーは編集できません。

注意　Ciscoの担当者から指示された場合を除き、`Experimental Policy 1` は使用**しないで**ください。Ciscoでは、試験用にこのポリシーを使用します。

ステップ 3　[OK] をクリックして、変更を保存します。

変更を反映するには、アクセス コントロール ポリシーを適用する必要があります。

前処理するトラフィックのネットワーク分析ルールによる指定

ライセンス： すべて

サポートされるデバイス： 機能によって異なる

アクセス コントロール ポリシーの詳細設定では、ネットワーク分析ルールを使用してネットワーク トラフィックの前処理設定を調整できます。アクセス コントロール ルールと同様に、ネットワーク分析ルールには 1 から始まる番号が付いています。

システムがトラフィックを前処理する時間になると、ネットワーク分析ルールの番号順（昇順）にパケットが照合され、すべての条件が一致した最初のルールに基づいてトラフィックが前処理されます。次の表は、ルールに追加できる条件を示しています。

表 25-1　ネットワーク分析ルールの条件タイプ

条件	照合されるトラフィック	詳細
ゾーン	特定のセキュリティ ゾーン内のインターフェイスを介したデバイスへの着信またはデバイスからの発信トラフィック	「セキュリティ ゾーン」とは、展開方法やセキュリティ ポリシーに基づいて構成される 1 つ以上のインターフェイスの論理グループを指します。ゾーン内のインターフェイスが複数のデバイス間に配置される場合もあります。ゾーン条件の作成については、ゾーンの条件によるトラフィックの前処理（25-6 ページ）を参照してください。
Networks	その送信元または宛先の IP アドレス、国、または大陸で区別されるトラフィック	特定の IP アドレスを明示的に指定できます。ネットワーク条件の作成については、ネットワークの条件によるトラフィックの前処理（25-8 ページ）を参照してください。
VLAN タグ	VLAN によりタグ付けされたトラフィック	VLAN によるパケットの識別に最内部の VLAN タグが使用されます。ASA FirePOWER では、VLAN に応じて前処理を制限することはできません。VLAN 条件の作成については、VLAN の条件によるトラフィックの前処理（25-9 ページ）を参照してください。

ルールに特定の条件を設定しない場合、その条件によるトラフィック照合は行われません。たとえば、ルールにネットワーク条件を設定してゾーン条件を設定しない場合、トラフィックの入力または出力インターフェイスは照合されず、送信元または宛先の IP アドレスに基づいてトラフィックが評価されます。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。

カスタム ネットワーク分析ルールを追加するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　カスタムの前処理設定を作成するアクセス コントロール ポリシーで、[Advanced] タブを選択して、[Intrusion and Network Analysis Policies] セクションの横にある編集アイコン（  ）をクリックします。

[Network and Analysis Policies] ダイアログボックスが表示されます。カスタムのネットワーク分析ルールを追加していない場合、Web インターフェイスには**No Custom Rules**（カスタム ルールがない）が示され、追加済みの場合はそれらのルールの数が表示されます。

ヒント　[Network Analysis Policy List] をクリックします。[Network Analysis Policy] ページが新しいウィンドウで表示されます。このページでカスタムのネットワーク分析ポリシーを表示および編集します。詳しくは、ネットワーク分析ポリシーの管理（26-3 ページ）を参照してください。

ステップ 2　[Network Analysis Rules] の横にある、カスタム ルールの数を示すステートメントをクリックします。

ダイアログボックスが展開され、設定済みのカスタム ルールが表示されます。

ステップ 3　[Add Rule] をクリックします。

ネットワーク分析ルール エディタが表示されます。

ステップ 4　ルールの条件を作成します。次の基準を使用して、NAP の前処理を制限できます。

- ゾーンの条件によるトラフィックの前処理（25-6 ページ）
- ネットワークの条件によるトラフィックの前処理（25-8 ページ）
- VLAN の条件によるトラフィックの前処理（25-9 ページ）

ステップ 5　ネットワーク分析ポリシーをルールに関連付けます。これを行うには、[Network Analysis] タブをクリックし、[Network Analysis Policy] ドロップダウンリストからポリシーを選択します。

ここで選択したネットワーク分析ポリシーに基づいて、すべてのルールの条件に合致したトラフィックが前処理されます。ユーザが作成したポリシーを選択した場合は、編集アイコン（  ）をクリックして、新しいウィンドウでポリシーを編集できます。システムによって提供されたポリシーは編集できません。

注意　Ciscoの担当者から指示された場合を除き、`Experimental Policy 1` は使用**しないで**ください。Ciscoでは、試験用にこのポリシーを使用します。

ステップ 6　[Add] をクリックします。

一覧の末尾にルールが追加されます。ルールの評価順序を変更する場合は、ネットワーク分析ルールの管理（25-10 ページ）を参照してください。

ゾーンの条件によるトラフィックの前処理

ライセンス： すべて

ネットワーク分析ルールでゾーン条件を設定すると、トラフィックの送信元および宛先のセキュリティ ゾーンに応じてそのトラフィックを前処理できます。セキュリティ ゾーンはいくつかのインターフェイスで構成されるグループで、展開方法やセキュリティ ポリシーにより複数のデバイス間に配置される場合もあります。ゾーン作成の詳細については、セキュリティ ゾーンの操作（3-42 ページ）を参照してください。

1 つのゾーン条件で [Source Zones] および [Destination Zones] それぞれに対し、最大 50 のゾーンを追加できます。

- 特定のゾーンのインターフェイスからデバイスを*離れる*トラフィックを照合するには、そのゾーンを [Destination Zones] に追加します。パッシブに展開されたデバイスはトラフィックを送信しないので、パッシブ インターフェイスで構成されるゾーンを [Destination Zones] 条件で使用することはできません。
- 特定のゾーンのインターフェイスからデバイスに入るトラフィックを照合するには、そのゾーンを [Source Zones] に追加します。

送信元（Source）ゾーン条件と宛先（Destination）ゾーン条件の両方をルールに追加する場合、送信元ゾーンから発信されて宛先ゾーンを介して出力されるトラフィックにルールが適用されます。

ゾーン内のすべてのインターフェイスが同じタイプ（インライン、パッシブ、スイッチド、またはルーテッド）である必要があるため、ネットワーク分析ルールのゾーン条件で使用されているすべてのゾーンが同じタイプでなければならないことに注意してください。つまり、異なるタイプのゾーンを送信元/宛先とするトラフィックを照合する単一ルールを定義することはできません。

ゾーンにインターフェイスが含まれていないなど、無効な設定が検出されると、警告アイコン（  ）が表示されます。アイコンの上にポインタを置くと詳細が表示されます。

ゾーン条件に基づいてトラフィックを前処理するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　ゾーンに応じた前処理を設定するアクセス コントロール ポリシーで、新しいネットワーク分析ルールを作成するか既存のルールを編集します。

詳細な手順については、前処理するトラフィックのネットワーク分析ルールによる指定（25-5 ページ）を参照してください。

ステップ 2　ネットワーク分析ルール エディタで、[Zones] タブを選択します。

[Zones] タブが表示されます。

ステップ 3　[Available Zones] で、追加するゾーンを選択します。

追加するゾーンを検索するには、[Available Zones] リストの上にある [Search by name] プロンプトをクリックし、ゾーン名を入力します。ゾーン名の入力を開始するとリストが更新され、一致するゾーンが表示されます。

ゾーンをクリックして選択します。複数のゾーンを選択するには、**Shift** キーまたは **Ctrl** キーを使用します。すべてのゾーンを選択するには、右クリックして [Select All] を選択します。

ステップ 4　[Add to Source] または [Add to Destination] をクリックして、選択したゾーンを適切なリストに追加します。

選択したゾーンをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5　ルールを保存するか、編集を続けます。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

ネットワークの条件によるトラフィックの前処理

ライセンス： すべて

ネットワーク分析ルールでネットワーク条件を設定すると、トラフィックの送信元および宛先の IP アドレスに応じてそのトラフィックを前処理できます。前処理するトラフィックの送信元と宛先の IP アドレスを手動で指定したり、ネットワーク オブジェクトでネットワーク条件を設定したりできます。ネットワーク オブジェクトとは、いくつかの IP アドレスやアドレス ブロックに名前を付けて再利用可能にしたものを指します。

ヒント　ネットワーク オブジェクトを作成しておくと、それを使用してネットワーク分析ルールを作成したり、Web インターフェイスのさまざまな場所で IP アドレスを表すオブジェクトとして使用したりできます。これらのオブジェクトはオブジェクト マネージャを使用して作成できます。また、ネットワーク分析ルールの設定時にネットワーク オブジェクトを作成することもできます。詳細については、ネットワーク オブジェクトの操作（3-4 ページ）を参照してください。

1 つのネットワーク条件で [Source Networks] および [Destination Networks] それぞれに対し、最大 50 の項目を追加できます。

- 特定の IP アドレスからのトラフィックを照合するには、[Source Networks] を設定します。
- 特定の IP アドレスへのトラフィックを照合するには、[Destination Networks] を設定します。

送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから宛先 IP アドレスに送信されるトラフィックにルールが適用されます。

無効なネットワーク条件設定が検出されると、警告アイコン（  ）が表示されます。アイコンの上にポインタを置くと詳細が表示されます。

ネットワーク条件に基づいてトラフィックを前処理するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　ネットワークに応じた前処理を設定するアクセス コントロール ポリシーで、新しいネットワーク分析ルールを作成するか既存のルールを編集します。

詳細な手順については、前処理するトラフィックのネットワーク分析ルールによる指定（25-5 ページ）を参照してください。

ステップ 2　ネットワーク分析ルール エディタで、[Networks] タブを選択します。

[Networks] タブが表示されます。

ステップ 3　[Available Networks] で、追加するネットワークを選択します。

- ここでネットワーク オブジェクトを作成してリストに追加するには、[Available Networks] リストの上にある追加アイコン（  ）をクリックし、ネットワーク オブジェクトの操作（3-4 ページ）の手順に従います。
- 追加するネットワークを検索するには、[Available Networks] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクト名またはオブジェクトのいずれかの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

オブジェクトをクリックして選択します。複数のオブジェクトを選択するには、Shift キーまたは Ctrl キーを使用します。すべてのオブジェクトを選択するには、右クリックして [Select All] を選択します。

ステップ 4　[Add to Source] または [Add to Destination] をクリックして、選択したオブジェクトを適切なリストに追加します。

選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5　手動で指定する送信元または宛先の IP アドレスまたはアドレス ブロックを追加します。

[Source Networks] リストまたは [Destination Networks] リストの下にある [Enter an IP address] プロンプトをクリックし、IP アドレスまたはアドレス ブロックを入力して [Add] をクリックします。

ステップ 6　ルールを保存するか、編集を続けます。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

VLAN の条件によるトラフィックの前処理

ライセンス： すべて

サポートされるデバイス： すべて（ASA FirePOWER を除く）

ネットワーク分析ルールで VLAN 条件を設定すると、トラフィックの VLAN タグに応じてそのトラフィックを前処理できます。VLAN によるパケットの識別に最内部の VLAN タグが使用されます。ASA FirePOWER デバイスでは、VLAN に応じて前処理を制限することはできません。

VLAN ベースのネットワーク分析条件を作成するときは、VLAN タグを手動で指定できます。または、VLAN タグ オブジェクトを使用して VLAN 条件を設定することもできます。VLAN タグ オブジェクトとは、いくつかの VLAN タグに名前を付けて再利用可能にしたものを指します。

ヒント　VLAN タグ オブジェクトを作成しておくと、それを使用してネットワーク分析ルールを作成したり、Web インターフェイスのさまざまな場所で VLAN タグを表すオブジェクトとして使用したりできます。VLAN タグ オブジェクトはオブジェクト マネージャを使用して作成できます。また、ネットワーク分析ルールの設定時に作成することもできます。詳細については、VLAN タグ オブジェクトの操作（3-14 ページ）を参照してください。

1 つの VLAN タグ条件で、[Selected VLAN Tags] に最大 50 の項目を追加できます。無効な VLAN タグ条件設定が検出されると、警告アイコン（⚠）が表示されます。アイコンの上にポインタを置くと詳細が表示されます。

VLAN タグ条件に基づいてトラフィックを前処理するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　VLAN タグに応じた前処理を設定するアクセス コントロール ポリシーで、新しいネットワーク分析ルールを作成するか既存のルールを編集します。

詳細な手順については、前処理するトラフィックのネットワーク分析ルールによる指定（25-5 ページ）を参照してください。

ステップ 2　ネットワーク分析ルール エディタで、[VLAN Tags] タブを選択します。

[VLAN Tags] タブが表示されます。

ステップ 3　[Available VLAN Tags] で、追加する VLAN を選択します。

- ここで VLAN タグ オブジェクトを作成してリストに追加するには、[Available VLAN Tags] リストの上にある追加アイコン（ ）をクリックし、VLAN タグ オブジェクトの操作（3-14 ページ）の手順に従います。
- 追加する VLAN タグ オブジェクトおよびグループを検索するには、[Available VLAN Tags] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクト名またはオブジェクトの VLAN タグの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。
- オブジェクトをクリックして選択します。複数のオブジェクトを選択するには、Shift キーまたは Ctrl キーを使用します。すべてのオブジェクトを選択するには、右クリックして [Select All] を選択します。

ステップ 4　[Add to Rule] をクリックして、選択したオブジェクトを [Selected VLAN Tags] リストに追加します。選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5　手動で指定する VLAN タグを追加します。

[Selected VLAN Tags] リストの下にある [Enter a VLAN tag] プロンプトをクリックし、VLAN タグまたはその範囲を入力して、[Add] をクリックします。1 から 4094 までの任意の VLAN タグを指定できます。VLAN タグの範囲を指定するにはハイフンを使用します。

ステップ 6　ルールを保存するか、編集を続けます。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（「アクセス コントロール ポリシーの適用」を参照してください）。

ネットワーク分析ルールの管理

ライセンス： すべて

ネットワーク分析ルールはいくつかの設定および条件のセットであり、これらの条件に一致するトラフィックをどのように前処理するかを指定します。既存のアクセス コントロール ポリシーの詳細オプションでネットワーク分析ルールを作成および編集します。各ルールは 1 つのポリシーにのみ属します。

カスタム ネットワーク分析ルールを編集するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　カスタム前処理設定を変更するアクセス コントロール ポリシーで、[Advanced] タブを選択して、[Intrusion and Network Analysis Policies] セクションの横にある編集アイコン（ ）をクリックします。

[Network and Analysis Policies] ダイアログボックスが表示されます。カスタムのネットワーク分析ルールを追加していない場合、Web インターフェイスには**No Custom Rules**（カスタム ルールがない）が示され、追加済みの場合はそれらのルールの数が表示されます。

ステップ 2　[Network Analysis Rules] の横にある、カスタム ルールの数を示すステートメントをクリックします。

ダイアログボックスが展開され、設定済みのカスタム ルールが表示されます。

ステップ 3　カスタム ルールを編集します。次の選択肢があります。

- ルールの条件を編集したり、ルールによって呼び出されるネットワーク分析ポリシーを変更したりするには、そのルールの横にある編集アイコン( )をクリックします。
- ルールの評価順序を変更するには、ルールをドラッグして並べ替えます。複数のルールを選択するには、Shift キーまたは Ctrl キーを使用します。
- ルールを削除するには、ルールの横にある削除アイコン( )をクリックします。

ヒント　ルールを右クリックするとコンテキスト メニューが表示され、新しいネットワーク分析ルールの切り取り、コピー、貼り付け、編集、および追加を行うことができます。

ステップ 4　[OK] をクリックして変更を保存します。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります(アクセス コントロール ポリシーの適用(12-17 ページ)を参照してください)。

CHAPTER 26

ネットワーク分析ポリシーの開始

*ネットワーク分析ポリシー*は、多数のトラフィックの前処理オプションを制御し、アクセス コントロール ポリシーの詳細設定で呼び出されます。ネットワーク分析に関連する前処理は、Security Intelligence によるブラックリスト化や SSL 復号化の後、侵入またはファイル検査の開始前に実行されます。

デフォルトでは、システムは *Balanced Security and Connectivity* ネットワーク分析ポリシーを使用して、アクセス コントロール ポリシーによって処理されるすべてのトラフィックを前処理します。ただし、この前処理を実行するために別のデフォルトのネットワーク分析ポリシーを選択できます。ユーザの利便性を考え、いくつかの変更できないネットワーク分析ポリシーが用意されています。これらのポリシーは、Cisco 脆弱性調査チーム（VRT）によってセキュリティおよび接続性の一定のバランスがとれるように調整されています。カスタム前処理設定を使用して、このデフォルト ポリシーをカスタム ネットワーク分析ポリシーに置換することもできます。

ヒント システムによって提供される侵入ポリシーおよびネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、Balanced Security and Connectivity ネットワーク分析ポリシーおよび Balanced Security and Connectivity 侵入ポリシーは共に機能し、侵入ルールの更新の際に両方とも更新できます。しかし、ネットワーク分析ポリシーは前処理オプションの大部分を制御するのに対し、侵入ポリシーは侵入ルールの大部分を制御します。ネットワーク分析ポリシーまたは侵入ポリシーについて（23-1 ページ） では、ネットワーク分析ポリシーと侵入ポリシーがトラフィックの検査に対してどのように連動するか、また、ナビゲーション パネルの使用、競合の解決、および変更のコミットに関するいくつかの基本について説明します。

複数のカスタム ネットワーク分析ポリシーを作成し、それらに異なるトラフィックの前処理を割り当てることによって、特定のセキュリティ ゾーン、ネットワーク、VLAN 用に前処理オプションを調整できます。（ASA FirePOWER デバイスでは、VLAN に応じて前処理を制限することはできません。）

注 特に複数のカスタム ネットワーク分析ポリシーを使用した前処理の調整は、**高度な**タスクです。前処理インスペクションと侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは互いに補完する**必要があります**。システムはユーザに合わせてポリシーを**調整しません**。詳細については、カスタム ポリシーの制限（23-13 ページ）を参照してください。

この章では、単純なカスタムネットワーク分析ポリシーを作成する方法について説明します。この章には、ネットワーク分析ポリシーの管理（編集、比較など）に関する基本情報も含まれています。詳細については、以下を参照してください。

カスタム ネットワーク分析ポリシーの作成

ライセンス： Protection

新しいネットワーク分析ポリシーを作成するときは、一意の名前を付け、基本ポリシーを指定し、*インライン モード*を選択する必要があります。

基本ポリシーはネットワーク分析ポリシーのデフォルト設定を定義します。新しいポリシーで設定を変更すると、基本ポリシーの設定が上書きされますが、変更はされません。基本ポリシーとしてシステムによって提供されるポリシーまたはカスタム ポリシーを使用できます。詳細については、基本レイヤについて（24-3 ページ）を参照してください。

ネットワーク分析ポリシーのインライン モードでは、プリプロセッサがトラフィックを変更（正規化）およびドロップし、攻撃者が検出を免れる可能性を最小限にすることができます。パッシブな展開では、インライン モードに関係なく、システムはトラフィック フローに影響を与えることができないことに注意してください。詳細については、インライン展開でプリプロセッサがトラフィックに影響を与えることを許可する（26-6 ページ）を参照してください。

ネットワーク分析ポリシーを作成するには、次の手順を実行します。

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

FireSIGHT システム のユーザ アカウントのロールが侵入ポリシーまたは修正侵入ポリシーに限定されている場合は、ネットワーク分析ポリシーに加えて、侵入ポリシーを作成して編集できます。[Network Analysis Policy] ページにアクセスするには、[Policies] > [Intrusion] を選択し、[Network Analysis Policy] をクリックします。詳細については、カスタム ユーザ ロールの管理（61-55 ページ）を参照してください。

ステップ 2　[Create Policy] をクリックします。

別のポリシー内に未保存の変更が存在する場合は、[Network Analysis Policy] ページに戻るかどうか尋ねられたときに [Cancel] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Create Network Analysis Policy] ポップアップ ウィンドウが表示されます。

ステップ 3　[Name] に一意のポリシー名を入力し、オプションで [Description] にポリシーの説明を入力します。

ステップ 4　最初の**基本ポリシー**を指定します。

基本ポリシーとしてシステムによって提供されるポリシーまたはカスタム ポリシーを使用できます。

注意　Ciscoの担当者から指示された場合を除き、`Experimental Policy 1` は使用**しないで**ください。Ciscoでは、試験用にこのポリシーを使用します。

ステップ 5　プリプロセッサがインライン展開でトラフィックに影響を与えるようにするかどうかを指定します。

- プリプロセッサがトラフィックに影響を与えるようにするには、[Inline Mode] を有効にします。
- プリプロセッサがトラフィックに影響を与えないようにするには、[Inline Mode] を無効にします。

ステップ 6　ポリシーを作成します。

- 新しいポリシーを作成して [Network Analysis Policy] ページに戻るには、[Create Policy] をクリックします。新しいポリシーには基本ポリシーと同じ設定が付与されます。
- ポリシーを作成し、高度なネットワーク分析ポリシー エディタで開いて編集するには、[Create and Edit Policy] をクリックします。ネットワーク分析ポリシーの編集（26-4 ページ）を参照してください。

ネットワーク分析ポリシーの管理

ライセンス： Protection

[Network Analysis Policy] ページ（[Policies] > [Access Control] を選択し、[Network Analysis Policy] をクリック）で、現在のカスタム ネットワーク分析ポリシーと共に次の情報を表示できます。

- ポリシーが最後に変更された日時（ローカル時間）とそれを変更したユーザ
- プリプロセッサがトラフィックに影響を与えることを許可する [Inline Mode] 設定が有効になっているかどうか
- どのアクセス コントロール ポリシーとデバイスが、ネットワーク分析ポリシーを使用してトラフィックを前処理しているか
- ポリシーに保存されていない変更があるかどうか、およびポリシーを現在編集している人（いれば）に関する情報

お客様が独自に作成するカスタム ポリシーに加えて、システムは初期インライン ポリシーと初期パッシブ ポリシーの 2 つのカスタム ポリシーを提供しています。これら 2 つのネットワーク分析ポリシーは、基本ポリシーとして「Balanced Security and Connectivity」ネットワーク分析ポリシーを使用します。両者の唯一の相違点はインライン モードの設定です。インライン ポリシーではプリプロセッサによるトラフィックの影響が有効化され、パッシブ ポリシーでは無効化されています。これらのシステム付属のカスタム ポリシーは編集して使用できます。

[Network Analysis Policy] ページのオプションを使用することで、次の表にあるアクションを実行できます。

表 26-1　ネットワーク分析ポリシーの管理操作

目的	操作	参照先
新しいネットワーク分析ポリシーを作成する	[Create Policy] をクリックします。	カスタム ネットワーク分析ポリシーの作成（26-2 ページ）。
既存のネットワーク分析ポリシーを編集する	編集アイコン（  ）をクリックします。	ネットワーク分析ポリシーの編集（26-4 ページ）。
ネットワーク分析ポリシー内の現在の構成設定がリストされた PDF レポートを表示する	レポート アイコン（  ）をクリックします。	現在のネットワーク分析設定のレポートの生成（26-9 ページ）
2 つのネットワーク分析ポリシーまたは同じポリシーの 2 つのリビジョンの設定を比較する	[Compare Policies] をクリックします。	2 つのネットワーク分析ポリシーまたはリビジョンの比較（26-10 ページ）。
ネットワーク分析ポリシーを削除する	削除アイコン（  ）をクリックし、ポリシーを削除することを確認します。アクセス コントロール ポリシーが参照しているネットワーク分析ポリシーは削除できません。	

ただし、FireSIGHT システム のユーザ アカウントのロールが侵入ポリシーまたは修正侵入ポリシーに限定されている場合は、ネットワーク分析ポリシーに加えて、侵入ポリシーを作成して編集できます。[Network Analysis Policy] ページにアクセスするには、[Policies] > [Intrusion] を選択し、[Network Analysis Policy] をクリックします。詳細については、カスタム ユーザ ロールの管理（61-55 ページ）を参照してください。

ネットワーク分析ポリシーの編集

ライセンス：Protection

新しいネットワーク分析ポリシーを作成すると、そのポリシーには基本ポリシーと同じ設定が付与されます。次の表に、ニーズに合わせて新しいポリシーを調整するために実行できる最も一般的なアクションを示します。

表 26-2　ネットワーク分析ポリシーの編集操作

目的	操作	参照先
プリプロセッサがトラフィックを編集またはドロップすることを許可する	[Policy Information] ページで [Inline Mode] チェック ボックスをオンにします。	インライン展開でプリプロセッサがトラフィックに影響を与えることを許可する（26-6 ページ）
基本ポリシーを変更する	[Policy Information] ページの [Base Policy] ドロップダウン リストから基本ポリシーを選択します。	基本ポリシーの変更（24-4 ページ）
基本ポリシーの設定を表示する	[Policy Information] ページで [Manage Base Policy] をクリックします。	基本レイヤについて（24-3 ページ）

表 26-2　ネットワーク分析ポリシーの編集操作（続き）

目的	操作	参照先
プリプロセッサの設定を有効化、無効化、または編集する	ナビゲーション パネルで [Settings] をクリックします。	ネットワーク分析ポリシーでのプリプロセッサの設定（26-7 ページ）
ポリシー層を管理する	ナビゲーション パネルで [Policy Layers] をクリックします。	ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）

ネットワーク分析ポリシーの調整時、特にプリプロセッサを無効化するときは、プリプロセッサおよび侵入ルールによってはトラフィックをある方法で最初に復号化または前処理する必要があることに留意してください。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

注　前処理インスペクションと侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは互いに補完する**必要があります**。特に複数のカスタム ネットワーク分析ポリシーを使用した前処理の調整は、**高度な**タスクです。詳細については、カスタム ポリシーの制限（23-13 ページ）を参照してください。

システムは、ユーザ 1 人あたり 1 つのネットワーク分析ポリシーをキャッシュします。ネットワーク分析ポリシーの編集中に、任意のメニューまたは別のページへの他のパスを選択した場合、変更内容はそのページを離れてもシステム キャッシュにとどまります。上の表に示す実行できるアクションの他に、ネットワーク分析ポリシーまたは侵入ポリシーについて（23-1 ページ）では、ナビゲーション パネルの使用、競合の解決、および変更のコミットに関する情報を記載しています。

ネットワーク分析ポリシーを編集するには、次の手順を実行します。

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　設定するネットワーク分析ポリシーの横にある編集アイコン（）をクリックします。

ネットワーク分析ポリシー エディタが表示され、[Policy Information] ページに焦点が置かれ、左側にナビゲーション パネルがあります。

ステップ 3　ポリシーを編集します。上記で要約されたアクションのいずれかを実行します。

ステップ 4　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残した状態での終了を行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

インライン展開でプリプロセッサがトラフィックに影響を与えることを許可する

ライセンス：Protection

インライン展開では、プリプロセッサによってはトラフィックを変更およびブロックできます。次に例を示します。

- インライン正規化プリプロセッサは、パケットを正規化し、他のプリプロセッサおよび侵入ルール エンジンで分析されるようにパケットを準備します。ユーザは、プリプロセッサの [Allow These TCP Options] と [Block Unrecoverable TCP Header Anomalies] オプションを使用して、特定のパケットをブロックすることもできます。詳細については、インライン トラフィックの正規化（29-7 ページ）を参照してください。
- システムは無効なチェックサムを持つパケットをドロップできます。チェックサムの検証（29-6 ページ）を参照してください。
- システムはレート ベースの攻撃防御設定に一致するパケットをドロップできます。レート ベース攻撃の防止（34-10 ページ）を参照してください。

ネットワーク分析ポリシーで設定したプリプロセッサがトラフィックに影響を与えるようにするには、プリプロセッサを有効化して適切に設定し、さらに管理対象デバイスを適切にインライン展開する（つまり、インライン インターフェイス セットを設定する）必要があります。最後に、ネットワーク分析ポリシーの [Inline Mode] 設定を有効にします。

設定がインライン展開で実際にトラフィックを変更することなくどのように機能するかを評価する場合は、インライン モードを無効にできます。パッシブ展開またはタップ モードでのインライン展開では、インライン モードであっても、システムはトラフィックに影響を与えることはできません。

インライン モードを無効化すると、侵入イベントのパフォーマンス統計グラフが影響を受けることがあるので注意してください。インライン展開でインライン モードが有効になっている場合、[Event Performance] ページ（[Overview] > [Summary] > [Intrusion Event Performance]）には、正規化されたパケットとブロックされたパケットを示すグラフが表示されます。インライン モードを無効化した場合またはパッシブ展開の場合は、正規化またはドロップされた可能性があるトラフィックに関するデータが多数のグラフに表示されます。詳細については、侵入イベントのパフォーマンス統計グラフの生成（41-5 ページ）を参照してください。

ヒント　インライン展開では、Cisco はインライン モードを有効にし、[Normalize TCP Payload] オプションを有効にしたままインライン正規化プリプロセッサを設定することを推奨します。パッシブ展開の場合、Cisco は、適応型プロファイルを設定することを推奨しています。

プリプロセッサがインライン展開でトラフィックに影響を与えることを許可するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（）をクリックします。

[Policy Information] ページが表示されます。

ステップ 3　プリプロセッサがトラフィックに影響を与えるようにするかどうかを指定します。

- プリプロセッサがトラフィックに影響を与えるようにするには、[Inline Mode] を有効にします。
- プリプロセッサがトラフィックに影響を与えないようにするには、[Inline Mode] を無効にします。

ステップ 4　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残した状態での終了を行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

ネットワーク分析ポリシーでのプリプロセッサの設定

ライセンス： Protection

*プリプロセッサ*は、トラフィックを正規化し、プロトコルの異常を識別することで、トラフィックがさらに検査されるように準備します。プリプロセッサは、設定されたプリプロセッサ オプションがパケットによりトリガーされたときに、プリプロセッサ イベントを生成できます（プリプロセッサ イベントの読み取り（41-41 ページ）を参照）。デフォルトで有効になるプリプロセッサや、それぞれのデフォルト設定は、ネットワーク分析ポリシーの基本ポリシーに応じて決まります。

ネットワーク分析ポリシーのナビゲーション パネルで [Settings] を選択すると、ポリシーによってタイプ別のプリプロセッサがリストされます。[Settings] ページで、ネットワーク分析ポリシーのプリプロセッサを有効または無効にしたり、プリプロセッサの設定ページにアクセスしたりできます。

プリプロセッサを設定するには、それを有効にする必要があります。プリプロセッサを有効にすると、そのプリプロセッサに関する設定ページへのサブリンクがナビゲーション パネル内の [Settings] リンクの下に表示され、この設定ページへの [Edit] リンクが [Settings] ページのプリプロセッサの横に表示されます。

ヒント　プリプロセッサの設定を基本ポリシーの設定に戻すには、プリプロセッサ設定ページで [Revert to Defaults] をクリックします。プロンプトが表示されたら、戻すことを確認します。

プリプロセッサを無効にすると、サブリンクと [Edit] リンクは表示されなくなりますが、設定は保持されます。特定の分析を実行するには、多くのプリプロセッサおよび侵入ルールで、トラフィックをある方法で最初に復号化または前処理する必要があることに注意してください。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

注　多くの場合、プリプロセッサの設定には特定の専門知識が必要で、通常は、ほとんどあるいはまったく変更を必要としません。特に複数のカスタム ネットワーク分析ポリシーを使用した前処理の調整は、**高度な**タスクです。前処理インスペクションと侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは互いに補完する**必要があります**。詳細については、カスタム ポリシーの制限（23-13 ページ）を参照してください。

プリプロセッサの設定を変更するには、その設定とネットワークへの潜在的影響を理解する必要があります。次の項では、プリプロセッサごとに固有の設定の詳細情報へのリンクを記述します。

アプリケーション層プリプロセッサ

アプリケーション層プロトコル デコーダは、特定のタイプのパケット データを、侵入ルール エンジンで分析できる形式に正規化します。

表 26-3　アプリケーション層プリプロセッサの設定

設定	参照先
DCE/RPC の設定	DCE/RPC トラフィックのデコード (27-2 ページ)
DNS の設定	DNS ネーム サーバ応答におけるエクスプロイトの検出 (27-16 ページ)
FTP および Telnet の設定	FTP および Telnet トラフィックのデコード (27-20 ページ)
HTTP の設定	HTTP トラフィックのデコード (27-33 ページ)
Sun RPC の設定	Sun RPC プリプロセッサの使用 (27-49 ページ)
SIP の設定	Session Initiation Protocol のデコード (27-51 ページ)
GTP コマンド チャネルの設定	GTP コマンド チャネルの設定 (27-55 ページ)
IMAP の設定	IMAP トラフィックのデコード (27-57 ページ)
POP の設定	POP トラフィックのデコード (27-60 ページ)
SMTP の設定	SMTP トラフィックのデコード (27-63 ページ)
SSH の設定	SSH プロプロセッサによるエクスプロイトの検出 (27-71 ページ)
SSL Configuration	SSL プリプロセッサの使用 (27-75 ページ)

SCADA プリプロセッサ

Modbus と DNP3 のプリプロセッサは、トラフィックの異常を検出し、インスペクションのためにデータを侵入ルール エンジンに提供します。

表 26-4　SCADA プリプロセッサの設定

設定	参照先
Modbus の設定	Modbus プリプロセッサの設定 (28-1 ページ)
DNP3 の設定	DNP3 プリプロセッサの設定 (28-3 ページ)

トランスポート層/ネットワーク層プリプロセッサ

ネットワーク層とトランスポート層のプリプロセッサは、ネットワーク層とトランスポート層でエクスプロイトを検出します。パケットがプリプロセッサに送信される前に、パケット デコーダにより、パケット ヘッダーとペイロードが、プリプロセッサや侵入ルール エンジンで簡単に使用できる形式に変換されます。また、パケット ヘッダー内でさまざまな異常動作が検出されます。

表 26-5　トランスポート層とネットワーク層のプリプロセッサの設定

設定	参照先
チェックサムの検証	チェックサムの検証（29-6 ページ）
インライン正規化	インライン トラフィックの正規化（29-7 ページ）
IP の最適化	IP パケットのデフラグ（29-12 ページ）
パケットの復号化	パケットのデコードについて（29-18 ページ）
TCP ストリームの設定	TCP ストリームの前処理の使用（29-22 ページ）
UDP ストリームの設定	UDP ストリームの前処理の使用（29-34 ページ）

トランスポート/ネットワーク プリプロセッサの詳細設定は、アクセス コントロール ポリシーが適用されるすべてのネットワーク、ゾーン、VLAN にグローバルに適用されることに注意してください。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセス コントロール ポリシーで設定します。トランスポート/ネットワークの詳細設定の構成（29-2 ページ）を参照してください。

特定の脅威の検出

Back Orifice プリプロセッサは、Back Orifice マジック クッキーについて UDP トラフィックを分析します。スキャン アクティビティを報告するようにポートスキャン ディテクタを設定できます。レート ベースの攻撃防御は、ネットワークを圧迫するように設計された SYN フラッドや膨大な同時接続からネットワークを保護するのに役立ちます。

表 26-6　特定の脅威の検出の設定

設定	参照先
Back Orifice の検出	バック オリフィスの検出（34-2 ページ）
ポートスキャンの検出	ポートスキャンの検出（34-3 ページ）
レート ベースの攻撃防御	レート ベース攻撃の防止（34-10 ページ）

侵入ポリシーで、ASCII テキストのクレジット カード番号や社会保障番号などのセンシティブ データを検出するセンシティブ データ プリプロセッサを設定することに注意してください。詳細については、センシティブ データの検出（34-20 ページ）を参照してください。

現在のネットワーク分析設定のレポートの生成

ライセンス：Protection

ネットワーク分析ポリシー レポートは、特定の時点でのポリシー設定の記録です。システムは、基本ポリシー内の設定とポリシー層の設定を統合して、基本ポリシーに起因する設定とポリシー層に起因する設定を区別しません。

このレポートには、次の情報が含まれており、監査目的や現在の設定を調べるために使用できます。

表 26-7　ネットワーク分析ポリシー レポートのセクション

セクション	説明
Policy Information	ポリシーの名前と説明、ポリシーを最後に変更したユーザの名前、ポリシーが最後に変更された日時が記載されます。また、インライン正規化を有効にできるかどうか、現在のルール更新のバージョン、および基本ポリシーが現在のルール更新にロックされているかどうかも記載されます。
Settings	有効なすべてのプリプロセッサの設定とその構成を表示します。

また、2 つのネットワーク分析ポリシーまたは同じポリシーの 2 つのリビジョンを比較する比較レポートを生成することもできます。詳細については、2 つのネットワーク分析ポリシーまたはリビジョンの比較（26-10 ページ）を参照してください。

ネットワーク分析ポリシー レポートを表示するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　レポートの生成対象とするポリシーの横にあるレポート アイコン（  ）をクリックします。ネットワーク分析ポリシー レポートを生成する前に、変更をコミットするのを忘れないでください。コミットされた変更だけがレポートに表示されます。

システムによってレポートが生成されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。

2 つのネットワーク分析ポリシーまたはリビジョンの比較

ライセンス：Protection

組織の標準に準拠しているかを確認する目的や、システム パフォーマンスを最適化する目的でポリシーの変更を検討するために、2 つのネットワーク分析ポリシーの差異を調べることができます。2 つのネットワーク分析ポリシーまたは同じネットワーク分析ポリシーの 2 つのリビジョンを比較できます。比較した後に、必要に応じて、2 つのポリシーまたはポリシー リビジョン間の違いを記録した PDF レポートを生成できます。

ネットワーク分析ポリシーまたはポリシーのリビジョンを比較するために使用できる 2 つのツールがあります。

- 比較ビューには、2 つのネットワーク分析ポリシーまたはネットワーク分析ポリシー リビジョン間の違いだけが並べて表示されます。各ポリシーまたはポリシー リビジョンの名前が比較ビューの左右のタイトル バーに表示されます。

  これを使用して、Web インターフェイスで相違点を強調表示したまま、両方のポリシーのリビジョンを表示し移動することができます。

- 比較レポートは、2 つのネットワーク分析ポリシーまたはネットワーク分析ポリシー リビジョン間の違いのみを記録したもので、PDF 形式であるという以外は、ネットワーク分析ポリシー レポートと類似した形式になっています。

  これは、ポリシー比較を保存、コピー、出力、および共有して、詳しく調査するために使用できます。

ポリシー比較ツールの概要と使用法の詳細については、次の項を参照してください。

- ネットワーク分析ポリシー比較ビューの使用（26-11 ページ）
- ネットワーク分析ポリシー比較レポートの使用（26-12 ページ）

ネットワーク分析ポリシー比較ビューの使用

ライセンス：Protection

比較ビューには、両方のポリシーまたはポリシー リビジョンが並べて表示されます。それぞれのポリシーまたはポリシー リビジョンは、比較ビューの左右のタイトル バーに表示された名前で識別されます。ポリシー名とともに、最後に変更した時間と、最後に変更したユーザが表示されます。

2 つのポリシーの違いは、次のように強調表示されます。

- 青色は強調表示された設定が 2 つのポリシーで異なることを示し、差異は赤色で示されます。
- 緑色は強調表示された設定が一方のポリシーには存在するが、他方には存在しないことを示します。

次の表に、実行できる操作を記載します。

表 26-8　ネットワーク分析ポリシー比較ビューの操作

目的	操作
個別の変更を移動する	タイトル バーの上の [Previous] または [Next] をクリックします。 左側と右側の間にある二重矢印アイコン（）が移動し、表示している違いを示す [Difference] 番号が変わります。
特定のプリプロセッサの設定を含む階層を特定する	表示する設定の横にある詳細設定アイコン（  ）の上にカーソルを移動します。 ウィンドウに、プリプロセッサの設定が含まれている階層の名前が表示されます。
新しいポリシー比較ビューを生成する	[New Comparison] をクリックします。 [Select Comparison] ウィンドウが表示されます。詳細については、「ネットワーク分析ポリシー比較レポートの使用（26-12 ページ）」を参照してください。
ポリシー比較レポートを生成する	[Comparison Report] をクリックします。 ポリシー比較レポートは、2 つのポリシーまたはポリシー リビジョン間の違いのみをリストする PDF ドキュメントを作成します。

ネットワーク分析ポリシー比較レポートの使用

ライセンス：Protection

ネットワーク分析ポリシー比較レポートは、ネットワーク分析ポリシー比較ビューで特定された 2 つネットワーク分析ポリシー間または同じネットワーク分析ポリシーの 2 つのリビジョン間のすべての違いの記録を、PDF として提供するものです。このレポートを使用して、2 つのネットワーク分析ポリシーの設定の間の相違点をさらに調べ、その結果を保存して配信することができます。

アクセス可能な任意のポリシーに関して、比較ビューからネットワーク分析ポリシー比較レポートを生成できます。ポリシー レポートを生成する前に、必ずすべての変更を保存してください。レポートには、保存されている変更だけが表示されます。

ポリシー比較レポートの形式は、ポリシー レポートと同様です。唯一異なる点は、ポリシー レポートにはポリシーのすべての設定が記載される一方、ポリシー比較レポートにはポリシー間で異なる設定だけがリストされることです。ネットワーク分析ポリシー比較レポートは、表 26-7（26-10 ページ）に記載されているセクションから成ります。

ヒント　同様の手順で、SSL、アクセス コントロール、侵入、ファイル、システム、またはヘルスのポリシーを比較できます。

2 つのネットワーク分析ポリシーまたはポリシー リビジョンを比較するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　[Compare Policies] をクリックします。

[Select Comparison] ウィンドウが表示されます。

ステップ 3　[Compare Against] ドロップダウンリストから、比較するタイプを次のように選択します。

- 異なる 2 つのポリシーを比較するには、[Other Policy] を選択します。

  ページが更新されて、[Policy A] と [Policy B] という 2 つのドロップダウンリストが表示されます。
- 同じポリシーの 2 つのリビジョンを比較するには、[Other Revision] を選択します。

  ページが更新され、[Policy]、[Revision A] および [Revision B] ドロップダウンリストが表示されます。

ステップ 4　選択した比較タイプに応じて、次のような選択肢があります。

- 2 つの異なるポリシーを比較する場合は、[Policy A] および [Policy B] ドロップダウンリストのそれぞれから、比較するポリシーを選択します。
- 同じポリシーの 2 つのリビジョンを比較する場合は、[Policy] を選択し、[Revision A] および [Revision B] ドロップダウンリストから比較するタイムスタンプ付きリビジョンを選択します。

ステップ 5　ポリシー比較ビューを表示するには、[OK] をクリックします。

比較ビューが表示されます。

ステップ 6　必要に応じて、ネットワーク分析ポリシー比較レポートを生成するには [Comparison Report] をクリックします。

ネットワーク分析ポリシー比較レポートが表示されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。

アプリケーション層プリプロセッサの使用

侵入ポリシーで有効になっているルールを使用してインスペクション用にトラフィックを準備するネットワーク分析ポリシーのアプリケーション層プリプロセッサを設定します。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーについて（23-1 ページ）」を参照してください。

アプリケーション層プロトコルにより、同一データをさまざまな方法で表すことができます。Ciscoは、特定タイプのパケット データを侵入ルール エンジンが分析可能なフォーマットに正規化する、アプリケーション層プロトコル デコーダを提供しています。アプリケーション層プロトコル エンコーディングを正規化することで、ルール エンジンは、データがさまざまな方法で表現されるパケットに同じコンテンツ関連ルールを効果的に適用し、有意な結果を得ることができます。

侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。詳細については、カスタム ポリシーの制限（23-13 ページ）を参照してください。

注意 カスタム ユーザ ロールを持つ一部のユーザは、標準メニュー パス（[Policies] > [Access Control] > [Network Analysis Policy]）からネットワーク分析ポリシーにアクセスできません。これらのユーザは、侵入ポリシーを介してネットワーク分析ポリシーにアクセスできます（[Policies] > [Intrusion] > [Intrusion Policy] > [Network Analysis Policy]）カスタム ユーザ ロールの詳細については、カスタム ユーザ ロールの管理（61-55 ページ）を参照してください。

ほとんどの場合、侵入ポリシーで関連するプリプロセッサ ルールを有効にしていない場合、プリプロセッサはイベントを生成しない点に注意してください。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

詳細については、次の項を参照してください。

- DCE/RPC トラフィックのデコード（27-2 ページ）では、DCE/RPC プリプロセッサについて説明し、回避の試行を防いで DCE/RPC トラフィックでの異常を検出するようにプリプロセッサを設定する方法を説明します。
- DNS ネーム サーバ応答におけるエクスプロイトの検出（27-16 ページ）では、DNS プリプロセッサについて説明し、DNS ネームサーバ応答における 3 種類のエクスプロイトを検出するようにプリプロセッサを設定する方法について説明します。
- FTP および Telnet トラフィックのデコード（27-20 ページ）では、FTP/Telnet デコーダについて説明し、FTP および Telnet トラフィックを正規化およびデコードするようにデコーダを設定する方法について説明します。

- HTTP トラフィックのデコード (27-33 ページ) では、HTTP デコーダについて説明し、HTTP トラフィックを正規化するようにデコーダを設定する方法について説明します。
- Sun RPC プリプロセッサの使用 (27-49 ページ) では、RPC デコーダについて説明し、RPC トラフィックを正規化するようにデコーダを設定する方法について説明します。
- Session Initiation Protocol のデコード (27-51 ページ) では、SIP プリプロセッサを使用して SIP トラフィックをデコードし、SIP トラフィックの異常を検出する方法を説明します。
- GTP コマンド チャネルの設定 (27-55 ページ) では、GTP プリプロセッサを使用して、パケット デコーダによって抽出された GTP コマンド チャネル メッセージをルール エンジンに提供する方法について説明します。
- IMAP トラフィックのデコード (27-57 ページ) では、IMAP プリプロセッサを使用して IMAP トラフィックをデコードし、IMAP トラフィックの異常を検出する方法を説明します。
- POP トラフィックのデコード (27-60 ページ) では、POP プリプロセッサを使用して POP トラフィックをデコードし、POP トラフィックの異常を検出する方法を説明します。
- SMTP トラフィックのデコード (27-63 ページ) では、SMTP デコーダについて説明し、SMTP トラフィックをデコードおよび正規化するようにデコーダを設定する方法について説明します。
- SSH プロプロセッサによるエクスプロイトの検出 (27-71 ページ) では、SSH 暗号化トラフィックでエクスプロイトを特定し処理する方法について説明します。
- SSL プリプロセッサの使用 (27-75 ページ) では、SSL プリプロセッサを使用して暗号化トラフィックを特定し、そのトラフィックのインスペクションを停止して誤検出を排除する方法について説明します。
- SCADA 前処理の設定 (28-1 ページ) では、Modbus および DNP3 プリプロセッサを使用して、対応するトラフィックの異常を検出し、特定のプロトコル フィールドを検査するためにデータを侵入ルール エンジンに提供する方法を説明します。

DCE/RPC トラフィックのデコード

ライセンス： Protection

DCE/RPC プロトコルにより、別々のネットワーク ホスト上のプロセスが、同一ホストに配置されている場合と同様に通信できます。通常、このようなプロセス間通信はホスト間で TCP および UDP 経由で転送されます。TCP 転送では、DCE/RPC が Windows Server Message Block（SMB）プロトコルまたは Samba にさらにカプセル化されることがあります。Samba は、Windows および UNIX 系または Linux 系のオペレーティング システムで構成される混合環境でのプロセス間通信に使用されるオープンソース SMB 実装です。また、ネットワーク上の Windows IIS Web サーバが、IIS RPC over HTTP を使用することがあります。IIS RPC over HTTP は、プロキシ TCP により伝送される DCE/RPC トラフィックに対し、ファイアウォールを介した分散通信を提供します。

DCE/RPC プリプロセッサ オプションとその機能の説明には、Microsoft による DCE/RPC の実装である MSRPC が含まれることに注意してください。SMB のオプションと機能についての説明は、SMB と Samba の両方に当てはまります。

ほとんどの DCE/RPC エクスプロイトは、DCE/RPC サーバ（ネットワーク上の Windows または Samba が稼働している任意のホスト）を対象とした DCE/RPC クライアント要求で発生します。またエクスプロイトはサーバ応答でも発生することがあります。DCE/RPC プリプロセッサは、TCP、UDP、および SMB トランスポートでカプセル化された DCE/RPC 要求と応答を検出します。これには、RPC over HTTP バージョン 1 を使用して TCP により伝送される DCE/RPC があります。プリプロセッサは DCE/RPC データ ストリームを分析し、DCE/RPC トラフィックにおける異常な動作と回避技術を検出します。また、SMB データ ストリームを分析し、異常な SMB 動作と回避技術を検出します。

DCE/RPC プリプロセッサは、IP 最適化プリプロセッサにより提供される IP 最適化および TCP ストリーム プリプロセッサによって提供される TCP ストリームの再構成のほかに、SMB のセグメント化解除および DCE/RPC の最適化も行います。TCP ストリームの前処理の使用（29-22 ページ）およびIP パケットのデフラグ（29-12 ページ）を参照してください。

最後に、DCE/RPC プリプロセッサはルール エンジンで処理できるように DCE/RPC トラフィックを正規化します。特定の DCE/RPC ルール キーワードを使用してDCE/RPC サービス、操作、およびスタブ データを検出する方法については、DCE/RPC キーワード（36-64 ページ）を参照してください。

DCE/RPC プリプロセッサを設定するには、プリプロセッサの機能を制御するグローバル オプションを変更するか、IP アドレスと稼働している Windows または Samba のバージョンによってネットワーク上の DCE/RPC サーバを識別する 1 つ以上のターゲットベース サーバ ポリシーを指定します。

ジェネレータ ID（GID）が 132 または 133 の DCE/RPC プリプロセッサ ルールを使用してイベントを生成する場合は、これらのルールを有効にする必要があります。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

詳細については、次の項を参照してください。

- グローバル DCE/RPC オプションの選択（27-3 ページ）
- ターゲットベース DCE/RPC サーバ ポリシーについて（27-5 ページ）
- DCE/RPC トランスポートについて（27-6 ページ）
- DCE/RPC ターゲットベース ポリシー オプションの選択（27-9 ページ）
- DCE/RPC プリプロセッサの設定（27-13 ページ）

グローバル DCE/RPC オプションの選択

ライセンス：Protection

グローバル DCE/RPC プリプロセッサ オプションは、プリプロセッサの機能を制御します。[Memory Cap Reached] オプション以外のこれらのオプションを変更すると、パフォーマンスまたは検出機能に悪影響を及ぼす可能性があります。プリプロセッサについて、またプリプロセッサと有効にされている DCE/RPC ルールとの間の相互作用について十分に理解していない場合は、これらのオプションを変更しないでください。特に [Maximum Fragment Size] オプションと [Reassembly Threshold] オプションは、ルールが検出する必要がある深さと同じかそれ以上にしてください。詳細については、コンテンツ一致の制約（36-19 ページ）およびByte_Jump と Byte_Test の使用（36-33 ページ）を参照してください。

次の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

Maximum Fragment Size

[Enable Defragmentation] が選択されている場合、DCE/RPC フラグメントの許容最大長を 1514 バイトから 65535 バイトまでの範囲で指定します。これよりも大きなフラグメントの場合、プリプロセッサは処理のためにフラグメントの一部を切り捨て、指定のサイズにしてから最適化を行いますが、実際のパケットは変更されません。空白フィールドの場合、このオプションは無効になります。

Reassembly Threshold

[Enable Defragmentation] が選択されている場合、0 を指定するとこのオプションは無効になり、1 バイトから 65535 バイトの範囲内の値を指定すると、それが、フラグメント化された DCE/RPC の最小バイト数となります。また該当する場合は、再構成されたパケットをルール エンジンに送信する前にキューに入れるセグメント化 SMB のバイト数が指定されます。低い値を指定すると、早期検出の可能性が高くなりますが、パフォーマンスに悪影響を及ぼす可能性があります。このオプションを有効にする場合は、パフォーマンスの影響をテストしておく必要があります。

Enable Defragmentation

フラグメント化された DCE/RPC トラフィックを最適化するかどうかを指定します。無効にすると、プリプロセッサは引き続き異常を検出して DCE/RPC データをルール エンジンに送信しますが、フラグメント化された DCE/RPC データでのエクスプロイトを見落とすリスクがあります。

このオプションには、DCE/RPC トラフィックを最適化しないという柔軟性がありますが、ほとんどの DCE/RPC エクスプロイトでは、フラグメント化を利用してエクスプロイトを隠ぺいする試みが行われます。このオプションを無効にすると、ほとんどの既知のエクスプロイトがバイパスされ、検出漏れが大量に発生します。

Memory Cap Reached

プリプロセッサに割り当てられた最大メモリ制限に達したか、またはこの制限を超過したことを検出します。最大メモリ制限に達したか、またはこの制限を超過した場合、プリプロセッサはメモリ キャップ イベントを引き起こしたセッションに関連付けられているすべての保留データを解放し、セッションのそれ以降の部分を無視します。

このオプションのイベントを生成するには、ルール 133:1 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Auto-Detect Policy on SMB Session

SMB `Session Setup AndX` 要求および応答に指定されている Windows または Samba のバージョンを検出します。検出されたバージョンが、[Policy] 設定オプションで設定されている Windows または Samba のバージョンと異なる場合、そのセッションに限り、検出されたバージョンが設定バージョンをオーバーライドします。詳細については、「ターゲットベース DCE/RPC サーバ ポリシーについて（27-5 ページ）」を参照してください。

たとえば、[Policy] に Windows XP を設定した場合に、プリプロセッサが Windows Vista を検出すると、プリプロセッサはそのセッションでは Windows Vista ポリシーを使用します。その他の設定は引き続き有効です。

DCE/RPC トランスポートが SMB ではない場合は（トランスポートが TCP または UDP の場合）、バージョンを検出できず、ポリシーを自動的に設定できません。

このオプションを有効にするには、ドロップダウンリストで次のいずれかを選択します。

- サーバ/クライアント トラフィックでポリシー タイプを検査するには、[Client] を選択します。
- クライアント/サーバ トラフィックでポリシー タイプを検査するには、[Server] を選択します。
- サーバ/クライアント トラフィックとクライアント/サーバ トラフィックの両方でポリシー タイプを検査するには、[Both] を選択します。

ターゲットベース DCE/RPC サーバ ポリシーについて

ライセンス：Protection

ターゲットベース サーバ ポリシーを 1 つ以上作成することにより、指定されたタイプのサーバが処理するのと同様の方法で DCE/RPC トラフィックを検査するように、DCE/RPC プリプロセッサを設定することができます。ターゲットベース ポリシーの設定では、ネットワーク上の指定するホストで稼働している Windows または Samba のバージョンの識別、トランスポート プロトコルの有効化、DCE/RPC トラフィックをこれらのホストへ伝送するポートの指定、その他のサーバ固有オプションの設定などを行います。

Windows および Samba の DCE/RPC の実装は大きく異なります。たとえば、Windows のすべてのバージョンは、DCE/RPC トラフィックの最適化時に最初のフラグメントの DCE/RPC コンテキスト ID を使用しますが、Samba のすべてのバージョンは、最後のフラグメントのコンテキスト ID を使用します。また、特定の関数呼び出しを識別するために、Windows Vista では最初のフラグメントの opnum（操作番号）見出し フィールドを使用しますが、Samba とその他のすべてのバージョンの Windows では最後のフラグメントの opnum フィールドを使用します。

Windows と Samba の SMB の実装にも、大きな違いがあります。たとえば、Windows は名前付きパイプの操作時に SMB OPEN および READ コマンドを認識しますが、Samba はこれらのコマンドを認識しません。

DCE/RPC プリプロセッサを有効にすると、デフォルトのターゲットベース ポリシーが自動的に有効になります。オプションで、異なるバージョンの Windows または Samba が稼働している他のホストを対象とするターゲットベース ポリシーを追加できます。このためには、[Policy] ドロップダウンリストから適切なバージョンを選択します。デフォルトのターゲットベース ポリシーは、別のターゲットベース ポリシーに含まれていないホストに適用されます。

それぞれのターゲットベース ポリシーでは、1 つ以上のトランスポートを有効にし、それぞれについて*検出ポート*を指定できます。また、*自動検出ポート*を有効にして指定できます。詳細については、「DCE/RPC トランスポートについて（27-6 ページ）」を参照してください。

その他のターゲットベースのポリシー オプションも設定できます。指定した 1 つ以上の共有 SMB リソースへの接続が試行された場合にそれを検出するように、プリプロセッサを設定できます。SMB トラフィックでファイルを検出し、検出されたファイルで指定のバイト数のデータを検査するように、プリプロセッサを設定できます。また、SMB プロトコルに関する知識を持つユーザだけが変更すべき拡張オプションを変更できます。このオプションでは、連結された SMB ANDX コマンドの数が指定された最大数を超えた場合にそのことを検出するようにプリプロセッサを設定できます。

各ターゲットベースのポリシーでは次の設定が可能です。

- 1 つ以上のトランスポートを有効にし、それぞれについて*検出ポート* を指定します。
- *自動検出ポート*を有効にして指定します。詳細については、「DCE/RPC トランスポートについて（27-6 ページ）」を参照してください。
- 指定した 1 つ以上の共有 SMB リソースへの接続が試行された場合にそのことを検出するように、プリプロセッサを設定します。
- SMB トラフィックでファイルを検出し、検出されたファイルで指定された数のバイトを検査するように、プリプロセッサを設定します。
- SMB プロトコルの知識を持つユーザだけが変更すべき拡張オプションを変更できます。このオプションでは、連結された SMB ANDX コマンドの数が指定された最大数を超えた場合にそのことを検出するようにプリプロセッサを設定します。

[Auto-Detect Policy on SMB Session] グローバル オプションを有効にすることにより、SMB が DCE/RPC トランスポートの場合に、ターゲット ポリシーに対して設定されているポリシー タイプをセッションごとに自動的にオーバーライドできることに注意してください。Auto-Detect Policy on SMB Session（27-4 ページ）を参照してください。

DCE/RPC プリプロセッサで SMB トラフィック ファイル検出を有効にする他に、オプションでこれらのファイルを検出してブロックするか、または動的分析のために Collective Security Intelligence クラウド に送信するように、ファイル ポリシーを設定できます。そのポリシー内で、[Action] として [Detect Files] または [Block Files] を選択し、[Application Protocol] として [Any] または [NetBIOS-ssn (SMB)] を選択して、ファイル ルールを作成する必要があります。詳細については、ファイル ポリシーの作成（37-18 ページ）およびファイル ルールの操作（37-19 ページ）を参照してください。

DCE/RPC トランスポートについて

ライセンス： Protection

各ターゲットベース ポリシーでは、TCP、UDP、SMB、および RPC over HTTP トランスポートのうち 1 つ以上を有効にできます。トランスポートを有効にする場合は、1 つ以上の *検出ポート*（DCE/RPC トラフィックを伝送することがわかっているポート）を指定する必要があります。オプションで、*自動検出ポート*（プリプロセッサが、DCE/RPC トラフィックを伝送するかどうかを判別するためにまずテストし、DCE/RPC トラフィックを検出した場合にのみ処理を続行するポート）を有効にして指定できます。

Cisco は、ウェルノウン ポートまたは一般に使用されているポートであるデフォルト検出ポートを各プロトコルで使用することを推奨します。検出ポートを追加するのは、デフォルト以外のポートで DCE/RPC トラフィックを検出した場合だけです。

自動検出ポートを有効にする場合は、エフェメラル ポート範囲全体に対応するよう、自動検出ポートが 1024 から 65535 までのポート範囲に設定されていることを確認してください。[RPC over HTTP Proxy Auto-Detect Ports] オプションまたは [SMB Auto-Detect Ports] オプションで自動検出ポートを有効にしたり指定したりすることはほとんどないことに注意してください。これは、指定されているデフォルト検出ポートを除き、どちらの場合もトラフィックが発生することはほとんどなく、その見込みも少ないためです。また、自動検出は、トランスポート検出ポートによって識別されていないポートでのみ発生する点にも注意してください。トランスポートごとに自動検出ポートを有効または無効にする際の推奨事項については、DCE/RPC ターゲットベース ポリシー オプションの選択（27-9 ページ）を参照してください。

Windows のターゲットベース ポリシーでは、ネットワークのトラフィックに一致するように、1 つ以上の任意のトランスポートのポートを任意の組み合わせで指定できます。しかし、Samba のターゲットベース ポリシーでは SMB トランスポートのポートだけを指定できます。

少なくとも 1 つのトランスポートが有効になっている DCE/RPC ターゲットベース ポリシーを追加した場合を除き、デフォルトの ターゲットベース ポリシーでは少なくとも 1 つの DCE/RPC トランスポートを有効にする必要があります。たとえば、すべての DCE/RPC 実装用のホストを指定し、未指定のホストにはデフォルトのターゲットベース ポリシーを適用しないでおくことがあります。この場合、デフォルトのターゲットベース ポリシーのトランスポートを有効にしません。

詳細については、次の項を参照してください。

- コネクションレス型およびコネクション型 DCE/RPC トラフィックについて（27-7 ページ）
- RPC over HTTP トランスポートについて（27-8 ページ）

コネクションレス型およびコネクション型 DCE/RPC トラフィックについて

ライセンス：Protection

DCE/RPC メッセージは、2 種類の DCE/RPC Protocol Data Unit（PDU）の 1 つに準拠します。

- コネクション型 DCE/RPC PDU プロトコル

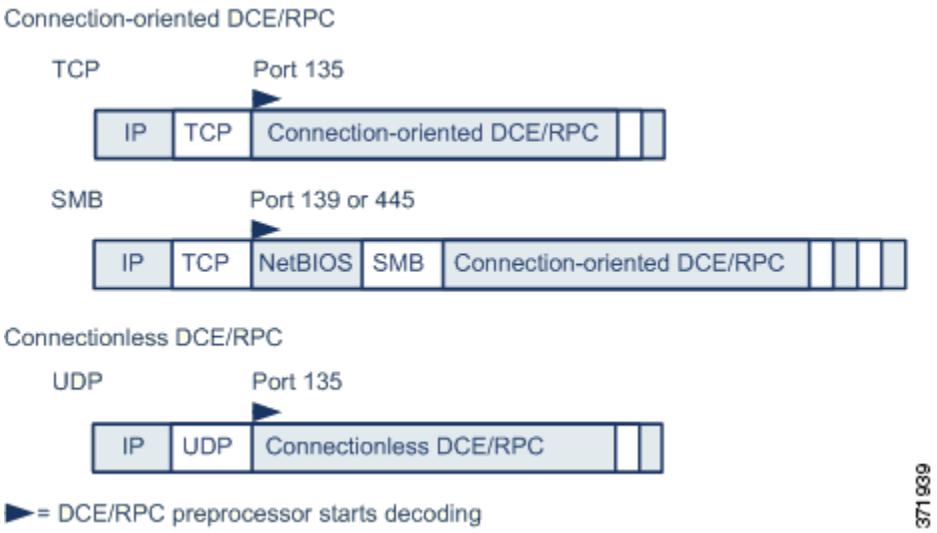
  DCE/RPC プリプロセッサは、TCP、SMB、および RPC over HTTP トランスポートでコネクション型 DCE/RPC を検出します。

- コネクションレス型 DCE/RPC PDU プロトコル

  DCE/RPC プリプロセッサは、UDP トランスポートでコネクションレス型 DCE/RPC を検出します。

この 2 つの DCE/RPC PDU プロトコルには、それぞれ固有の見出しとデータ特性があります。たとえば、コネクション型 DCE/RPC ヘッダーの長さは通常は 24 バイトであり、コネクションレス型 DCE/RPC ヘッダーの長さは 80 バイト（固定）です。また、フラグメント化コネクションレス型 DCE/RPC のフラグメントの正しい順序は、コネクションレス型トランスポートでは処理できないため、代わりにコネクションレス型 DCE/RPC ヘッダー値により維持される必要があります。これとは対照的に、コネクション型 DCE/RPC の正しいフラグメント順序はトランスポート プロトコルによって維持されます。DCE/RPC プリプロセッサは、これらや他のプロトコル固有の特性を使用して、両方のプロトコルで異常やその他の回避技術をモニタし、トラフィックをデコードおよび最適化してからルール エンジンに渡します。

次の図は、DCE/RPC プリプロセッサが各種トランスポートの DCE/RPC トラフィックの処理を開始するポイントを示します。



この図の次の点に注意してください。

- ウェルノウン TCP または UDP ポート 135 は、TCP および UDP トランスポートの DCE/RPC トラフィックを特定します。
- この図には RPC over HTTP は含まれていません。

  RPC over HTTP の場合、HTTP 経由での初期セットアップ シーケンスの後で、コネクション型 DCE/RPC は図に示すように TCP 経由で直接伝送されます。詳細については、「RPC over HTTP トランスポートについて（27-8 ページ）」を参照してください。

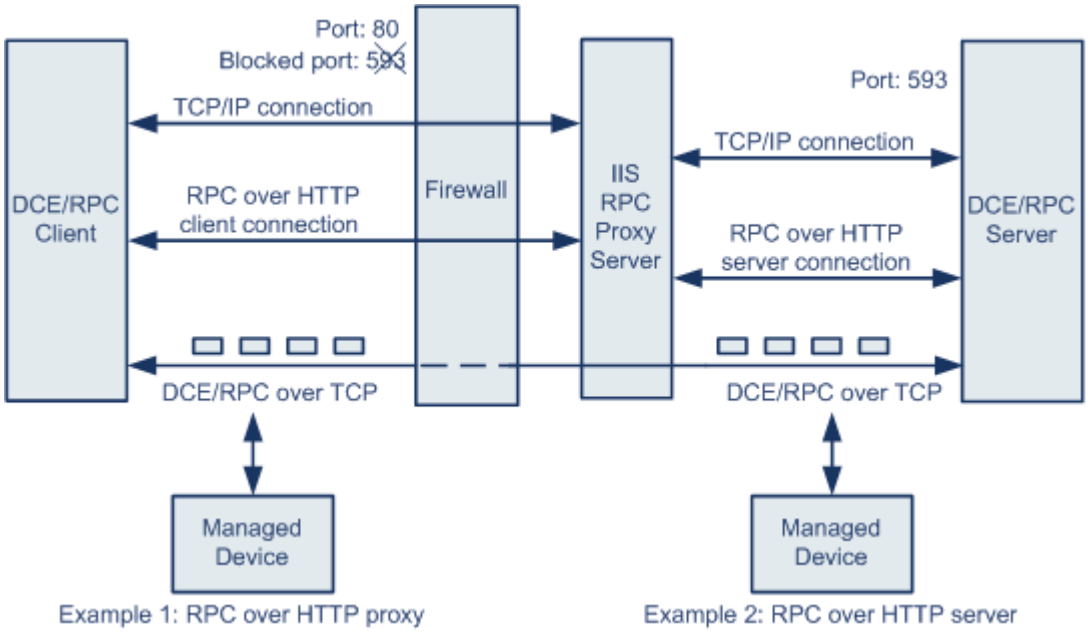
- DCE/RPC プリプロセッサは通常、NetBIOS セッション サービス用のウェルノウン TCP ポート 139 か、同様に実装されたウェルノウン Windows ポート 445 で SMB トラフィックを受信します。

  SMB には DCE/RPC 伝送以外にも多数の機能があるため、プリプロセッサは SMB トラフィックが DCE/RPC トラフィックを伝送しているかどうかをまず検査します。伝送していない場合は処理を停止し、伝送している場合は処理を続行します。
- IP によりすべての DCE/RPC トランスポートがカプセル化されます。
- TCP は、すべてのコネクション型 DCE/RPC を伝送します。
- UDP はコネクションレス型 DCE/RPC を伝送します。

RPC over HTTP トランスポートについて

ライセンス：Protection

Microsoft RPC over HTTP では、次の図に示すように、DCE/RPC トラフィックをトンネリングして、ファイアウォールを通過させることができます。DCE/RPC プリプロセッサは Microsoft RPC over HTTP バージョン 1 を検出します。



Microsoft IIS プロキシ サーバと DCE/RPC サーバは、同じホストまたは別々のホストにインストールできます。いずれの場合でも、個別のプロキシ オプションとサーバ オプションがあります。この図の次の点に注意してください。

- DCE/RPC サーバはポート 593 で DCE/RPC クライアント トラフィックをモニタしますが、ファイアウォールはこのポート 593 をブロックします。

  通常、ファイアウォールではデフォルトでポート 593 がブロックされます。
- RPC over HTTP は、ファイアウォールが通常許可するウェルノウン HTTP ポート 80 を使用して、HTTP 経由で DCE/RPC を伝送します。
- 例 1 のように、DCE/RPC クライアントと Microsoft IIS RPC プロキシ サーバの間のトラフィックをモニタする場合は [RPC over HTTP proxy] オプションを選択できます。

- 例 2 のように、Microsoft IIS RPC プロキシ サーバと DCE/RPC サーバが別々のホストにあり、デバイスが 2 つのサーバ間のトラフィックをモニタしている場合は、[RPC over HTTP server] オプションを選択できます。
- RPC over HTTP により DCE/RPC クライアントとサーバ間でのプロキシ セットアップが完了した後は、トラフィックは TCP を経由したコネクション型 DCE/RPC だけで構成されます。

DCE/RPC ターゲットベース ポリシー オプションの選択

ライセンス： Protection

各ターゲットベース ポリシーでは、次に示すさまざまなオプションを指定できます。[Memory Cap Reached] および [Auto-Detect Policy on SMB Session] オプション以外のオプションを変更すると、パフォーマンスまたは検出機能に悪影響を及ぼす可能性があります。プリプロセッサについて、またプリプロセッサと有効にされている DCE/RPC ルールとの間の相互作用について十分に理解していない場合は、これらのオプションを変更しないでください。

次の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

[Networks]

DCE/RPC ターゲットベース サーバ ポリシーを適用するホストの IP アドレス。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をコンマで区切ったリストを指定できます。デフォルト ポリシーを含め、最大で合計 255 個のプロファイルを指定できます。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの指定については、次を参照してください。

デフォルト ポリシーの**デフォルト**設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィクス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、**すべて** を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

また、ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となるネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、「ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）」を参照してください。

ポリシー

モニタ対象ネットワーク セグメントのターゲット ホストが使用する Windows または Samba DCE/RPC の実装。これらのポリシーの詳細については、ターゲットベース DCE/RPC サーバ ポリシーについて（27-5 ページ）を参照してください。

[Auto-Detect Policy on SMB Session] グローバル オプションを有効にすることで、SMB が DCE/RPC トランスポートの場合に、このオプションの設定をセッション単位で自動的にオーバーライドできることに注意してください。Auto-Detect Policy on SMB Session（27-4 ページ）を参照してください。

SMB Invalid Shares

1 つ以上の SMB 共有リソースを識別する、大文字と小文字を区別しない英数字テキスト文字列です。指定した共有リソースへの接続が試行されると、プリプロセッサがそのことを検出します。複数の共有をカンマで区切って指定できます。またオプションで、共有を引用符で囲むこともできます。これは、以前のソフトウェア バージョンでは必須でしたが、現在は必須ではありません。次に例を示します。

```
"C$", D$, "admin", private
```

SMB ポートと SMB トラフィックの両方の検出が有効に設定されている場合、プリプロセッサは SMB トラフィックで無効な共有を検出します。

ほとんどの場合、Windows により名前が指定されたドライブを無効な共有として指定するには、このドライブにドル記号を付加する必要があることに注意してください。たとえば、ドライブ C は C$ または "C$" として指定します。

このオプションのイベントを生成するには、ルール 133:26 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

SMB Maximum AndX Chain

連結された SMB AndX コマンドの最大数（0 から 255）です。通常、多数の連結 AndX コマンドは異常な動作を表し、場合によっては回避試行を示している可能性があります。連結コマンドを許可しない場合は 1 を指定し、連結コマンドの数の検出を無効にするには 0 を指定します。

プリプロセッサは最初に連結コマンドの数をカウントし、関連する SMB プリプロセッサ ルールが有効であり、連結コマンドの数が設定されている値と等しいかそれ以上の場合にはイベントを生成することに注意してください。その後処理が続行されます。

注　SMB プロトコルに詳しいユーザだけがこのオプションのデフォルト設定を変更するようにしてください。

このオプションのイベントを生成するには、ルール 133:20 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

RPC proxy traffic only

[RPC over HTTP Proxy Ports] が有効である場合、検出されるクライアント側の RPC over HTTP トラフィックがプロキシ トラフィックのみであるか、または他の Web サーバ トラフィックを含んでいる可能性があるかどうかを示します。たとえば、ポート 80 はプロキシ トラフィックとその他の Web サーバ トラフィックの両方を伝送する可能性があります。

このオプションが無効になっている場合は、プロキシ トラフィックとその他の Web サーバ トラフィックの両方が想定されます。たとえばサーバが専用プロキシ サーバである場合などに、このオプションを有効にします。有効にすると、プリプロセッサはトラフィックを調べて DCE/RPC を伝送しているかどうかを判別し、伝送していない場合はそのトラフィックを無視し、伝送している場合は処理を続行します。このオプションを有効にすることで機能が追加されるのは、[RPC over HTTP Proxy Ports] チェック ボックスも有効にされている場合だけであることに注意してください。

RPC over HTTP Proxy Ports

管理対象デバイスが DCE/RPC クライアントと Microsoft IIS RPC プロキシ サーバの間に配置されている場合に、指定の各ポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの検出を有効にします。RPC over HTTP トランスポートについて（27-8 ページ）を参照してください。

有効である場合、DCE/RPC トラフィックが確認されるポートを追加できますが、Web サーバは一般に DCE/RPC トラフィックとその他のトラフィックの両方にデフォルト ポートを使用するため、この操作が必要になることはあまりありません。有効である場合、[RPC over HTTP Proxy Auto-Detect Ports] は有効にしませんが、検出されるクライアント側の RPC over HTTP トラフィックがプロキシ トラフィックのみであり、その他の Web サーバ トラフィックを含んでいない場合は、[RPC Proxy Traffic Only] を有効にします。

RPC over HTTP Server Ports

Microsoft IIS RPC プロキシ サーバおよび DCE/RPC サーバが異なるホスト上に配置されており、デバイスがこの 2 つのサーバ間のトラフィックをモニタしている場合、指定の各ポートで RPC over HTTP によりトンネリングされている DCE/RPC トラフィックの検出を有効にします。RPC over HTTP トランスポートについて（27-8 ページ）を参照してください。

一般に、このオプションを有効にするときは、ネットワーク上にプロキシ Web サーバを認識していない場合であっても、1025 から 65535 までのポート範囲で [RPC over HTTP Server Auto-Detect Ports] も有効にする必要があります。場合によっては RPC over HTTP サーバ ポートを再設定することがあり、その際には再設定したサーバ ポートをこのオプションのポート リストに追加する必要があることに注意してください。

TCP Ports

指定の各ポートでの TCP の DCE/RPC トラフィックの検出を有効にします。

正当な DCE/RPC トラフィックとエクスプロイトは、さまざまなポートを使用する可能性があります。ポート 1024 より大きい番号のポートが一般的です。通常、このオプションを有効にする場合は、1025 から 65535 までのポート範囲で [TCP Auto-Detect Ports] も有効にする必要があります。

UDP Ports

指定の各ポートでの UDP の DCE/RPC トラフィックの検出を有効にします。

正当な DCE/RPC トラフィックとエクスプロイトは、さまざまなポートを使用する可能性があります。ポート 1024 より大きい番号のポートが一般的です。通常、このオプションを有効にする場合は、1025 から 65535 までのポート範囲で [UDP Auto-Detect Ports] も有効にする必要があります。

SMB Ports

指定の各ポートでの SMB の DCE/RPC トラフィックの検出を有効にします。

デフォルトの検出ポートを使用した SMB トラフィックが発生することがあります。他のポートはほとんどありません。通常はデフォルト設定を使用してください。

RPC over HTTP Proxy Auto-Detect Ports

管理対象デバイスが DCE/RPC クライアントと Microsoft IIS RPC プロキシ サーバの間に配置されている場合に、指定のポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの自動検出を有効にします。RPC over HTTP トランスポートについて（27-8 ページ）を参照してください。

有効である場合は、一時ポート範囲全体をカバーするため、一般にポート範囲として 1025 から 65535 を指定します。

RPC over HTTP Server Auto-Detect Ports

Microsoft IIS RPC プロキシ サーバおよび DCE/RPC サーバが異なるホスト上に配置されており、デバイスがこの 2 つのサーバ間のトラフィックをモニタしている場合、指定のポートで RPC over HTTP によりトンネリングされている DCE/RPC トラフィックの自動検出を有効にします。RPC over HTTP トランスポートについて（27-8 ページ）を参照してください。

TCP Auto-Detect Ports

指定のポートで TCP の DCE/RPC トラフィックの自動検出を有効にします。

UDP Auto-Detect Ports

指定の各ポートで UDP の DCE/RPC トラフィックの自動検出を有効にします。

SMB Auto-Detect Ports

SMB の DCE/RPC トラフィックの検出を有効にします。

SMB File Inspection

ファイル検出のための SMB トラフィックの インスペクションを有効にします。次の選択肢があります。

- ファイル インスペクションを無効にするには、[Off] を選択します。
- SMB でファイル データを検査するが、DCE/RPC トラフィックは検査しない場合は、[Only] を選択します。このオプションを選択すると、ファイルと DCE/RPC トラフィックの両方を検査する場合よりもパフォーマンスが向上する可能性があります。
- SMB でファイルと DCE/RPC トラフィックの両方を検査するには、[On] を選択します。このオプションを選択すると、パフォーマンスに影響する可能性があります。

SMB トラフィックでの次のファイルについてのインスペクションはサポートされていません。

- SMB 2.x および SMB 3.x で転送されたファイル
- このオプションを有効にしてポリシーを適用する前に確立された TCP または SMB セッションで転送されたファイル
- 1 つの TCP または SMB セッションで同時に転送されたファイル
- 複数の TCP または SMB セッションにわたって転送されたファイル
- メッセージ署名のネゴシエート時など、非連続データを使用して転送されたファイル
- 同一オフセットに異なるデータが含まれており、データがオーバーラップしている転送ファイル
- リモート クライアントがファイル サーバに保存し、そのクライアントで編集用に開かれたファイル

SMB File Inspection Depth

[SMB File Inspection] が [Only] または [On] に設定されている場合に、SMB トラフィックでファイルが検出された時に検査されるデータのバイト数です。次のいずれかを指定します。

- `1` から `2147483647`（約 2GB）までの範囲内の整数
- `0`:ファイル全体を検査する場合
- `-1`:ファイル インスペクションを無効にする場合

このフィールドには、アクセス コントロール ポリシーで定義されている値と等しいか、それよりも小さい値を入力します。[Limit the number of bytes inspected when doing file type detection] で定義されている値よりも大きい値をこのオプションに設定すると、アクセス コントロール ポリシーの設定が、有効な最大値として使用されます。詳細については、ファイルおよびマルウェアのインスペクション パフォーマンスおよびストレージの調整（18-22 ページ）参照してください。

[SMB File Inspection] が [Off] に設定されている場合、このフィールドは無効になります。

DCE/RPC プリプロセッサの設定

ライセンス： Protection

DCE/RPC プリプロセッサのグローバル オプションと、1 つ以上のターゲットベース サーバ ポリシーを設定できます。

ジェネレータ ID（GID）133 のルールを有効にしていない場合、プリプロセッサはイベントを生成しません。特定の検出オプションに関連付けられているルールについては、グローバル DCE/RPC オプションの選択（27-3 ページ）、DCE/RPC ターゲットベース ポリシー オプションの選択（27-9 ページ）、および ルール状態の設定（32-22 ページ）を参照してください。

さらに、ほとんどの DCE/RPC プリプロセッサ ルールでは、SMB、コネクション型 DCE/RPC、またはコネクションレス型 DCE/RPC のトラフィックで異常や回避技術が検出されると、イベントが生成されます。トラフィック タイプ別に有効にできるルールを次の表に示します。

表 27-1　　トラフィック関連 DCE/RPC ルール

Traffic	プリプロセッサ ルール GID：SID
SMB	133:2 ～ 133:26、133:48 ～ 133:57
コネクション型 DCE/RPC	133:27 ～ 133:39
コネクションレス型 DCE/RPC の検出	133:40 ～133:43

DCE/RPC プリプロセッサを設定する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Application Layer Preprocessors] の下の [DCE/RPC Configuration] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効である場合は、[Enabled] をクリックし、次に [Edit] をクリックします。

[DCE/RPC Configuration] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　グローバル DCE/RPC オプションの選択（27-3 ページ）で説明するオプションを変更できます。

ステップ 6　次の 2 つのオプションから選択できます。

- 新しいターゲットベースのポリシーを追加します。ページの左側で [Servers] の横にある追加アイコン（  ）をクリックします。[Add Target] ポップアップ ウィンドウが表示されます。1 つ以上の IP アドレスを [Server Address] フィールドに指定し、[OK] をクリックします。

  単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をコンマで区切ったリストを指定できます。FireSIGHT システムで IPv4 および IPv6 アドレス ブロックを使用する方法の詳細については、IP アドレスの表記規則（1-23 ページ）を参照してください。

  デフォルト ポリシーを含め、最大 255 個のポリシー を設定できます。

  ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となるネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、「ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）」を参照してください。

  ページの左側のサーバ リストに新しい項目が表示され、選択されていることを示すために強調表示されます。[Configuration] セクションが更新され、追加したプロフィールの現行設定が反映されます。

- 既存のターゲットベースのポリシーの設定を変更します。ページ左側の [Servers] の下で追加したポリシーの設定済みアドレスをクリックするか、または [default] をクリックします。

  選択したエントリが強調表示され、[Configuration] セクションが更新されて、選択したポリシーの現在の設定が表示されます。既存のポリシーを削除するには、削除するポリシーの横にある削除アイコン（  ）をクリックします。

ステップ 7　変更できるターゲットベース ポリシー オプションを次に示します。

- DCE/RPC のターゲットベース サーバ ポリシーを適用する 1 つ以上のホストを指定するには、[Networks] フィールドに、1 つの IP アドレスまたはアドレス ブロック、あるいはこのいずれかまたは両方をカンマで区切ったリストを入力します。

  デフォルト ポリシーを含め、最大で合計 255 個のプロファイルを指定できます。デフォルト ポリシーでは [Networks] の設定を変更できないことに注意してください。デフォルト ポリシーは、別のポリシーで指定されていないネットワーク内のすべてのサーバに適用されます。

- ネットワーク セグメントの指定のホストに適用するポリシーのタイプを指定するには、[Policy] ドロップダウンリストから、Windows または Samba ポリシー タイプの 1 つを選択します。

  [Auto-Detect Policy on SMB Session] グローバル オプションを有効にすることで、SMB が DCE/RPC トランスポートの場合に、このオプションの設定をセッション単位で自動的にオーバーライドできることに注意してください。Auto-Detect Policy on SMB Session（27-4 ページ）を参照してください。

- 指定の共有 SMB リソースへの接続が試行された場合にそのことを検出するようにプリプロセッサを設定するには、[SMB Invalid Shares] フィールドに、共有リソースを示す文字列を 1 つまたは複数指定します。文字列の大文字と小文字は区別されず、複数の文字列はカンマで区切って指定します。オプションで、個々の文字列を引用符で囲むこともできます。これは、以前のソフトウェア バージョンでは必須でしたが、現在は必須ではありません。

  たとえば、C$、D$、admin、および private という名前の共有リソースを検出するには、次のように入力します。

  ```
  "C$", D$, "admin", private
  ```

  SMB の無効な共有を検出するには、[SMB Ports] または [SMB Auto-Detect Ports] も有効にし、[SMB Traffics] グローバル オプションを有効にする必要があることに注意してください。

  ほとんどの場合、Windows により名前が指定されたドライブを無効な共有として指定するには、このドライブにドル記号を付加する必要があることにも注意してください。たとえば、ドライブ C を指定するには `C$` または `"C$"` と入力します。

- SMB の DCE/RPC トラフィックで検出されたファイルを検査し、DCE/RPC トラフィックの分析はしない場合は、[SMB File Inspection] ドロップダウン リストから [Only] を選択します。SMB の DCE/RPC トラフィックで検出されたファイルと DCE/RPC トラフィックを検査するには、[SMB File Inspection] ドロップダウン リストから [On] を選択します。[SMB File Inspection Depth] フィールドに、検出されたファイル内の検査対象バイト数を入力します。検出されたファイル全体を検査するには、`0` を入力します。

- 連結された SMB AndX コマンドの最大許容数を指定するには、[SMB Maximum AndX Chains] のフィールドに 0 ～ 255 を入力します。連結されたコマンドを許可しない場合は `1` を指定します。この機能を無効にするには、`0` を入力するか、またはこのオプションを空白のままにします。

注　SMB プロトコルに詳しいユーザだけが [SMB Maximum AndX Chains] オプションのデフォルト設定を変更するようにしてください。

- Windows ポリシー トランスポートの DCE/RPC トラフィックを伝送することが判明しているポートで、DCE/RPC トラフィックを処理できるようにするには、検出トランスポートの横のチェック ボックスをオンまたはオフにします。またオプションで、伝送用のポートを追加または削除できます。

  Windows ポリシー用に、[RPC over HTTP Proxy Ports]、[RPC over HTTP Server Ports]、[TCP Ports]、および [UDP Ports] のいずれか 1 つまたは任意の組み合わせを選択します。[RPC over HTTP proxy] が有効であり、検出されるクライアント側の RPC over HTTP トラフィックがプロキシ トラフィックのみである（つまり他の Web サーバ トラフィックを含んでいない）場合は、[RPC Proxy Traffic Only] を選択します。

  Samba ポリシー用に [SMB Ports] を選択します。

  ほとんどの場合はデフォルト設定を使用します。詳細については、DCE/RPC トランスポートについて（27-6 ページ）、RPC over HTTP トランスポートについて（27-8 ページ）、および DCE/RPC ターゲットベース ポリシー オプションの選択（27-9 ページ）を参照してください。

  1 つのポートか、ダッシュ（-）を使用して区切ったポート番号の範囲、またはポート番号と範囲をカンマで区切ったリストを入力できます。

- 指定のポートが DCE/RPC トラフィックを伝送するかどうかを調べ、伝送する場合は処理を続行するには、自動検出トランスポートの横のチェック ボックスをオンまたはオフにします。またオプションで、伝送用のポートを追加または削除します。

  Windows ポリシー用に、[RPC over HTTP Server Auto-Detect Ports]、[TCP Auto-Detect Ports]、および [UDP Auto-Detect Ports] のいずれかまたは任意の組み合わせを選択します。

[RPC over HTTP Proxy Auto-Detect Ports] または [SMB Auto-Detect Ports] を選択することはほとんどない点に注意してください。

通常、エフェメラル ポート範囲全体をカバーするために、有効にする自動検出ポートに対し 1025 から 65535 までのポート範囲を指定します。詳細については、DCE/RPC トランスポートについて（27-6 ページ）、RPC over HTTP トランスポートについて（27-8 ページ）、および DCE/RPC ターゲットベース ポリシー オプションの選択（27-9 ページ）を参照してください。

詳細については、「DCE/RPC ターゲットベース ポリシー オプションの選択（27-9 ページ）」を参照してください。

ステップ 8　ポリシーを保存するか、編集を続けるか、変更を破棄するか、基本ポリシーのデフォルト構成設定に戻すか、あるいはシステム キャッシュに変更を残して終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

DNS ネーム サーバ応答におけるエクスプロイトの検出

ライセンス： Protection

DNS プリプロセッサは、DNS ネーム サーバ応答を検査し、次に示す特定のエクスプロイトがあるかどうかを確認します。

- RData テキスト フィールドに対するオーバーフローの試行
- 古い DNS リソース レコード タイプ
- 試験的な DNS リソース レコード タイプ

詳細については、次の項を参照してください。

- DNS プリプロセッサ リソース レコード インスペクションについて（27-16 ページ）
- RData テキスト フィールドに対するオーバーフローの試行の検出（27-17 ページ）
- 古い DNS リソース レコード タイプの検出（27-18 ページ）
- 試験的な DNS リソース レコード タイプの検出（27-18 ページ）
- DNS プリプロセッサの設定（27-19 ページ）

DNS プリプロセッサ リソース レコード インスペクションについて

ライセンス： Protection

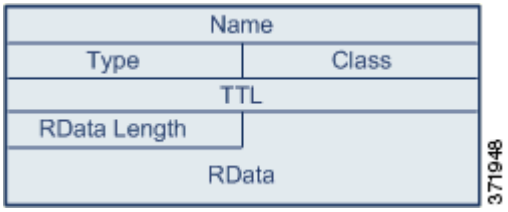
最も一般的なタイプの DNS ネーム サーバ応答には、応答を求めたクエリ内のドメイン名に対応する 1 つ以上の IP アドレスが示されています。その他のタイプのサーバ応答には、たとえば、電子メール メッセージの宛先や、元のクエリの対象のサーバからは取得できない情報を提供できるネームサーバの位置などが記述されています。

DNS 応答は、メッセージ 見出し、1 つ以上の要求を含む [Question] セクション、および [Question] セクションの要求に対応する 3 つのセクション（[Answer]、[Authority]、および [Additional Information]）で構成されます。この 3 セクションの応答には、ネーム サーバに保持されている *リソース レコード*（RR）の情報が反映されます。次の表で、これらの 3 つのセクションについて説明します。

表 27-2　DNS ネーム サーバ RR 応答

セクション	内容	例
回答	クエリに対する特定の回答を提供する 1 つ以上のリソース レコード（オプション）	ドメイン名に対応する IP アドレス
権限	権威ネーム サーバを指し示す 1 つ以上のリソース レコード（オプション）	応答の権威ネームサーバの名前
その他の情報	[Answer] セクションに関連する追加情報を提供する 1 つ以上のリソース レコード（オプション）	クエリ対象の別のサーバの IP アドレス

さまざまなタイプのリソース レコードがありますが、これらはすべて一貫して次の構造を保っています。



理論上、すべてのタイプのリソース レコードを、ネーム サーバ応答メッセージの [Answer]、[Authority]、または [Additional Information] セクションで使用できます。DNS プリプロセッサは、検出されたエクスプロイトについて、3 つの各応答セクションのすべてのリソース レコードを検査します。

[Type] および [RData] リソース レコード フィールドは、DNS プリプロセッサでは特に重要です。[Type] フィールドは、リソース レコードのタイプを示します。[RData]（リソース データ）フィールドは、応答の内容を示します。[RData] フィールドのサイズと内容は、リソース レコードのタイプによって異なります。

DNS メッセージは通常、UDP トランスポート プロトコルを使用しますが、信頼性のある配信を必要とするメッセージ タイプである場合や、メッセージ サイズが UDP で処理可能なサイズを超えている場合は、TCP を使用します。DNS プリプロセッサは、UDP および TCP の両方のトラフィックで DNS サーバ応答を検査します。

DNS プリプロセッサは、ミッドストリームで検出された TCP セッションを検査せず、ドロップされたパケットが原因でセッションの状態が失われるとインスペクションを終了します。

DNS プリプロセッサに設定する一般的なポートは、ウェルノウン ポート 53 です。これは、DNS ネーム サーバが UDP および TCP の両方で DNS メッセージに使用するポートです。

RData テキスト フィールドに対するオーバーフローの試行の検出

ライセンス：Protection

リソース レコード タイプが TXT（テキスト）の場合、[RData] フィールドは、可変長の ASCII テキスト フィールドです。

DNS プリプロセッサの [Detect Overflow attempts on RData Text fields] オプションが選択されている場合、MITRE の Current Vulnerabilities and Exposures データベースの CVE20063441 項目で指定されている特定の脆弱性が検出されます。これは、Microsoft Windows 2000 Service Pack 4、Windows XP Service Pack 1 および Service Pack 2、Windows Server 2003 Service Pack 1 の既知の脆弱性です。攻撃者はこの脆弱性を悪用して、[RData] テキスト フィールドの長さの誤算を引き起こし、結果としてバッファ オーバーフローを発生させるよう悪意をもって作られたネーム サーバ応答をホストに送信するか受信させることで、ホストを完全に制御できます。

アップグレードによってこの脆弱性が修正されていないオペレーティング システムが稼働しているホストがネットワーク内に含まれている可能性がある場合は、この機能を有効にする必要があります。

このオプションのイベントを生成するには、ルール 131:3 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

古い DNS リソース レコード タイプの検出

ライセンス：Protection

RFC 1035 ではさまざまなリソース レコード タイプが古いタイプとして指定されています。これらは古いレコード タイプであるため、一部のシステムはこれらのレコード タイプに対応しておらず、エクスプロイトの対象となることがあります。このようなレコード タイプを含めるようにネットワークを意図的に設定している場合を除き、通常の DNS 応答でこのようなレコード タイプが検出されることは想定されません。

既知の古いリソース レコード タイプを検出するようにシステムを設定できます。次の表に、これらのレコード タイプとその説明を示します。

表 27-3　古い DNS 応答レコード タイプ

RR タイプ	コード	説明
3	MD	メールの宛先
4	MF	メールのフォワーダ

このオプションのイベントを生成するには、ルール 131:1 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

試験的な DNS リソース レコード タイプの検出

ライセンス：Protection

RFC 1035 ではさまざまなリソース レコード タイプが試験的なタイプとして指定されています。これらは試験的なレコード タイプであるため、一部のシステムはこれらのレコード タイプに対応しておらず、エクスプロイトの対象となることがあります。このようなレコード タイプを含めるようにネットワークを意図的に設定している場合を除き、通常の DNS 応答でこのようなレコード タイプが検出されることは想定されません。

既知の試験的なレコード タイプを検出するようにシステムを設定できます。次の表に、これらのレコード タイプとその説明を示します。

表 27-4　試験的な DNS リソース レコード タイプ

RR タイプ	コード	説明
7	MB	メールボックスのドメイン名
8	MG	メール グループ メンバー
9	MR	メール リネーム ドメイン名
10	NUL	空白のリソース レコード

このオプションのイベントを生成するには、ルール 131:2 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

DNS プリプロセッサの設定

ライセンス：Protection

DNS プリプロセッサを設定するには、次の手順に従います。このページのオプションの設定の詳細については、RData テキスト フィールドに対するオーバーフローの試行の検出（27-17 ページ）、古い DNS リソース レコード タイプの検出（27-18 ページ）、および 試験的な DNS リソース レコード タイプの検出（27-18 ページ）を参照してください。

DNS プリプロセッサを設定するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Application Layer Preprocessors] の下の [DNS Configuration] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効である場合は、[Enabled] をクリックし、次に [Edit] をクリックします。

[DNS Configuration] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　オプションで、[Settings] エリアに表示されている次の項目のいずれかを変更できます。

- [Ports] フィールドに、DNS プリプロセッサが DNS サーバ応答をモニタする 1 つ以上の送信元ポートを指定します。複数のポートを指定する場合は、カンマで区切ります。

- RData テキスト フィールドでのバッファ オーバーフロー試行の検出を有効にするには、[Detect Overflow Attempts on RData Text fields] チェック ボックスをオンにします。
- 古いリソース レコード タイプを検出できるようにするには、[Detect Obsolete DNS RR Types] チェック ボックスをオンにします。
- 試験的なリソース レコード タイプを検出できるようにするには、[Detect Experimental DNS RR Types] チェック ボックスをオンにします。

ステップ 6　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

FTP および Telnet トラフィックのデコード

ライセンス： Protection

FTP/Telnet デコーダは FTP および Telnet データ ストリームを分析して、ルール エンジンによる処理の前に FTP および Telnet コマンドを正規化します。

ジェネレータ ID（GID）125 および 126 の FTP および Telnet プリプロセッサ ルールを使用してイベントを生成する場合は、これらのルールを有効にする必要があります。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

詳細については、次のトピックを参照してください。

グローバル FTP および Telnet オプションについて

ライセンス： Protection

FTP/Telnet デコーダがパケットのステートフル インスペクションまたはステートレス インスペクションを実行するかどうか、デコーダが暗号化 FTP または Telnet セッションを検出するかどうか、およびデコーダが暗号化データの検出後にデータ ストリームの検査を続行するかどうかを決定するグローバル オプションを設定できます。

次の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

Stateful Inspection

選択されている場合、FTP/Telnet デコーダは状態を保存し、各パケットにセッション コンテキストを提供し、再構成されたセッションだけを検査します。選択されていない場合、セッション コンテキストなしで個々のパケットを分析します。

FTP データ転送を検査するには、このオプションを選択する必要があります。

Detect Encrypted Traffic

暗号化 Tenet および FTP セッションを検出します。

このオプションのイベントを生成するには、ルール 125:7 および 126:2 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Continue to Inspect Encrypted Data

プリプロセッサに対し、データ ストリームの暗号化後もデータ ストリームの検査を続行し、最終的にデコードされたデータを検索するように指示します。

グローバル FTP/Telnet オプションの設定

ライセンス：Protection

ステートレスまたはステートフル インスペクションを実行するかどうか、暗号化トラフィックを検出するかどうか、および暗号化されていると判断されたデータ ストリームの暗号化データの検査をデコーダが続行するかどうかを制御するため、FTP/Telnet デコーダのグローバル オプションを設定する必要があります。グローバル設定の詳細については、グローバル FTP および Telnet オプションについて（27-20 ページ）を参照してください。

グローバル オプションを設定するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

[Advanced Settings] ページが表示されます。

ステップ 4　[Application Layer Preprocessors] の下の [FTP and Telnet Configuration] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効である場合は、[Enabled] をクリックし、次に [Edit] をクリックします。

[FTP and Telnet Configuration] ページが表示されます。

ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ヒント　このページのその他オプションの設定の詳細については、Telnet オプションの設定（27-23 ページ）、サーバレベルの FTP オプションの設定（27-27 ページ）、および クライアント レベル FTP オプションの設定（27-31 ページ）を参照してください。

ステップ 5　オプションで、[Global Settings] ページ領域に表示されている次の項目のいずれかを変更できます。

- FTP パケットを含む再構成された TCP ストリームを検査するには、[Stateful Inspection] を選択します。再構成されていないパケットだけを検査するには、[Stateful Inspection] をクリアします。
- 暗号化トラフィックを検出するには、[Detect Encrypted Traffic] を選択します。暗号化トラフィックを無視するには、[Detect Encrypted Traffic] をクリアします。
- 必要に応じて、ストリームが再度復号化され処理可能になる場合に備えて、暗号化後もストリームの検査を続行する場合は、[Continue] を選択します。

ステップ 6　ポリシーを保存するか、編集を続行するか、変更内容を破棄するか、ベース ポリシーのデフォルト設定に戻すか、またはシステム キャッシュの変更を反映せずに終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

Telnet オプションについて

ライセンス： Protection

FTP/Telnet デコーダによる Telnet コマンドの正規化を有効または無効にし、特定の異常ケースを有効または無効にし、許容可能な Are You There（AYT）攻撃数のしきい値を設定できます。

次の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

Telnet トラフィックを正規化するポートを示します。インターフェイスで、複数のポートをカンマで区切って指定します。

Normalize

指定のポートへの Telnet トラフィックを正規化します。

Detect Anomalies

対応する SE（サブネゴシエーション終了）がない Telnet SB（サブネゴシエーション開始）の検出を有効にします。

Telnet がサポートするサブネゴシエーションは、SB（サブネゴシエーション開始）で開始し SE（サブネゴシエーション終了）で終了していなければなりません。しかし、一部の Telnet サーバ実装では、対応する SE のない SB が無視されます。これは、回避事例につながるおそれのある異常な動作です。FTP はコントロール接続で Telnet プロトコルを使用するため、FTP もこの動作の影響を受けます。

この異常が Telnet トラフィックで検出される場合にイベントを生成するにはルール 126:3 を有効にし、FTP コマンド チャネルで検出される場合にイベントを生成するにはルール 125:9 を有効にできます。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Are You There Attack Threshold Number

連続する AYT コマンドの数が指定のしきい値を超えた場合にそのことを検出します。Cisco は、AYT しきい値に 20 以下の値を設定することを推奨します。

このオプションのイベントを生成するには、ルール 126:1 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Telnet オプションの設定

ライセンス：Protection

正規化を有効または無効にし、特定の異常ケースを有効または無効にし、許容可能な Are You There（AYT）攻撃数のしきい値を制御することができます。Telnet オプションの詳細については、Telnet オプションについて（27-22 ページ）を参照してください。

Telnet オプションを設定するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Application Layer Preprocessors] の下の [FTP and Telnet Configuration] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効である場合は、[Enabled] をクリックし、次に [Edit] をクリックします。

[FTP and Telnet Configuration] ページが表示されます。

ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ヒント　このページのその他オプションの設定の詳細については、グローバル FTP/Telnet オプションの設定（27-21 ページ）、サーバレベルの FTP オプションの設定（27-27 ページ）、および クライアントレベル FTP オプションの設定（27-31 ページ）を参照してください。

ステップ 5　オプションで、[Telnet Settings] ページ領域に表示されている次の項目のいずれかを変更できます。

- [Ports] フィールドに、Telnet トラフィックをデコードする 1 つ以上のポートを指定します。通常、Telnet は TCP ポート 23 に接続します。複数のポートを指定する場合は、カンマで区切ります。

注意　暗号化トラフィック（SSL）はデコードできないので、ポート 22（SSH）を追加すると、予想外の結果が生じる可能性があります。

- Telnet 正規化を有効または無効にするには、Telnet プロトコル オプションの [Normalize] チェック ボックスをオンまたはオフにします。
- 異常検出を有効または無効にするには、Telnet プロトコル オプションの [Detect Anomalies] チェック ボックスをオンまたはオフにします。
- 許容する連続 ATY コマンドの数を [Are You There Attack Threshold Number] に指定します。

ヒント　Ciscoは、AYT しきい値としてデフォルト値以下の値を設定することを推奨します。

ステップ 6　ポリシーを保存するか、編集を続けるか、変更を破棄するか、基本ポリシーのデフォルト構成設定に戻すか、あるいはシステム キャッシュに変更を残して終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

サーバレベルの FTP オプションについて

ライセンス： Protection

複数の FTP サーバでデコード オプションを設定できます。作成する各サーバ プロファイルには、トラフィックをモニタするサーバのサーバ IP アドレスとポートが含まれます。検証する FTP コマンドと、特定のサーバで無視する FTP コマンドを指定し、コマンドの最大パラメータ長を設定できます。また、デコーダが特定のコマンドで検証する特定のコマンド構文を設定し、代替最大コマンド パラメータ長を設定することもできます。

次の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

Networks

FTP サーバの 1 つ以上の IP アドレスを指定するには、このオプションを使用します。

単一 IP アドレスまたはアドレス ブロック、あるいはこのいずれかまたは両方をカンマで区切ったリストを指定できます。設定できる最大文字数は 1024 文字です。デフォルト プロファイルを含め最大 255 個のプロファイルを設定できます。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-23 ページ）を参照してください。

デフォルト ポリシーの**デフォルト**設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたはアドレス ブロックは指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、**すべて**を表すアドレス表記（0.0.0.0/0 または ::/0）を使用することはできません。

また、ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となるネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、「ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）」を参照してください。

ポート

管理対象デバイスがトラフィックをモニタする FTP サーバのポートを指定するには、このオプションを使用します。インターフェイスで、複数のポートをカンマで区切って指定します。

File Get Commands

サーバからクライアントにファイルを転送するために使用する FTP コマンドを定義するには、このオプションを使用します。サポートからの指示がない限り、これらの値を変更しないでください。

File Put Commands

クライアントからサーバにファイルを転送するために使用する FTP コマンドを定義するには、このオプションを使用します。サポートからの指示がない限り、これらの値を変更しないでください。

Additional FTP Commands

デコーダが検出するコマンドを追加で指定するには、この行を使用します。複数のコマンドを追加する場合は、コマンドをスペースで区切ってください。

Default Max Parameter Length

代替最大パラメータ長が設定されていないコマンドの最大パラメータ長を検出するには、このオプションを使用します。

このオプションのイベントを生成するには、ルール 125:3 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Alternate Max Parameter Length

異なる最大パラメータ長を検出するコマンドを指定し、それらのコマンドの最大パラメータ長を指定するには、このオプションを使用します。[Add] をクリックして行を追加し、特定のコマンドで検出する異なる最大パラメータ長を指定します。

Check Commands for String Format Attacks

指定されたコマンドでフォーマット文字列攻撃を検査するには、このオプションを使用します。

このオプションのイベントを生成するには、ルール 125:5 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Command Validity

特定のコマンドの有効な形式を入力するには、このオプションを使用します。FTP 通信の一部として受信したパラメータの構文を検証する FTP コマンド パラメータ検証ステートメントの作成については、FTP コマンド パラメータ検証ステートメントの作成（27-26 ページ）を参照してください。[Add] をクリックして、コマンド検証行を追加します。

このオプションのイベントを生成するには、ルール 125:2 および 125:4 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Ignore FTP Transfers

データ転送チャネルで状態インスペクション以外のすべてのインスペクションを無効にして FTP データ転送のパフォーマンスを改善するには、このオプションを使用します。

Detect Telnet Escape Codes within FTP Commands

FTP コマンド チャネルで Telnet コマンドが使用された場合にそのことを検出するには、このオプションを使用します。

このオプションのイベントを生成するには、ルール 125:1 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Ignore Erase Commands during Normalization

[Detect Telnet Escape Codes within FTP Commands] が選択されている場合に、FTP トラフィックの正規化時に Telnet の文字および行の消去コマンドを無視するには、このオプションを使用します。この設定は、FTP サーバによる Telnet 消去コマンドの処理方法と一致する必要があります。一般に、新しい FTP サーバは Telnet 消去コマンドを無視しますが、ほとんどの古いサーバは Telnet 消去コマンドを処理する点に注意してください。

トラブルシューティング オプション：Log FTP Command Validation Configuration

トラブルシューティングの電話中に、サーバに表示される各 FTP コマンドの設定情報を印刷するようにシステムを設定するようにサポートから依頼される場合があります。

注意　このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずサポートのガイダンスに従う必要があります。

FTP コマンド パラメータ検証ステートメントの作成

ライセンス：Protection

FTP コマンドに対する検証ステートメントを設定するときには、複数の代替パラメータをスペースで区切って指定できます。2 つのパラメータ間にバイナリ OR 関係を作成するには、検証ステートメントでこの 2 つのパラメータをパイプ文字（|）で区切って指定します。パラメータを大カッコ（[]）で囲むと、これらのパラメータがオプションであることを示します。パラメータを中カッコ（{}）で囲むと、これらのパラメータが必須であることを示します。

FTP 通信の一部として受信したパラメータの構文を検証する FTP コマンド パラメータ検証ステートメントを作成できます。詳細については、「サーバレベルの FTP オプションについて（27-24 ページ）」を参照してください。

FTP コマンド パラメータ検証ステートメントに使用できるパラメータを次の表に示します。

表 27-5　FTP コマンド パラメータ

使用するパラメータ	実行される検証
int	示されるパラメータが整数である必要があります。
number	示されるパラメータが1 ～ 255 の範囲内の整数である必要があります。

表 27-5　FTP コマンド パラメータ（続き）

使用するパラメータ	実行される検証
`char` *_chars*	示されるパラメータが単一文字であり、かつ *_chars* 引数に指定した文字の 1 つである必要があります。 たとえば、検証引数 `char` *SBC* を使用して `MODE` のコマンド検証を定義すると、`MODE` コマンドのパラメータが、文字 `S`（Stream モードを示す）、文字 `B`（Block モードを示す）、または文字 `C`（Compressed モードを示す）を含んでいるかどうかが検証されます。
`date` *_datefmt*	*_datefmt* に `#` が含まれている場合、示されるパラメータは数値である必要があります。 *_datefmt* に `C` が含まれている場合、示されるパラメータは文字である必要があります。 *_datefmt* にリテラル文字列が含まれている場合、示されるパラメータはリテラル文字列に一致している必要があります。
`string`	示されるパラメータが文字列である必要があります。
`host_port`	示されるパラメータは、RFC 959（Network Working Group による File Transfer Protocol 仕様）で定義されている有効なホスト ポート指定子である必要があります。

上記の表の構文を必要に応じて組み合わせることにより、トラフィックを検証する必要がある各 FTP コマンドを正しく検証するパラメータ検証ステートメントを作成できます。

注　TYPE コマンドに複合式を含める場合は、式をスペースで囲んでください。また、式内の各オペランドをスペースで囲んでください。たとえば、`char A|B` ではなく `char A | B` と入力します。

サーバレベルの FTP オプションの設定

ライセンス：Protection

サーバレベルでさまざまなオプションを設定できます。追加する FTP サーバごとに、モニタ対象のポート、検証対象のコマンド、コマンドのデフォルト最大パラメータ長、特定のコマンドの代替パラメータ長、および特定のコマンドの検証構文を指定できます。また、FTP チャネルでフォーマット文字列攻撃や Telnet コマンドを調べるかどうか、および各コマンドの設定情報を出力するかどうかを選択できます。サーバレベルの FTP オプションの詳細については、サーバレベルの FTP オプションについて（27-24 ページ）を参照してください。

サーバレベルの FTP オプションを設定するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Application Layer Preprocessors] の下の [FTP and Telnet Configuration] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効である場合は、[Enabled] をクリックし、次に [Edit] をクリックします。

[FTP and Telnet Configuration] ページが表示されます。

ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ヒント　このページのその他オプションの設定の詳細については、グローバル FTP/Telnet オプションの設定（27-21 ページ）、Telnet オプションの設定（27-23 ページ）、および クライアントレベル FTP オプションの設定（27-31 ページ）を参照してください。

ステップ 5　次の 2 つのオプションから選択できます。

- 新しいサーバ プロファイルを追加します。ページの左側で [FTP Server] の横にある追加アイコン( )をクリックします。[Add Target] ポップアップ ウィンドウが表示されます。クライアントの 1 つ以上の IP アドレスを [Server Address] フィールドに指定し、[OK] をクリックします。

  単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をコンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト ポリシーを含め最大 255 個のポリシーを設定できます。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-23 ページ）を参照してください。

  ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となるネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、「ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）」を参照してください。

  ページの左側の FTP サーバ リストに新しい項目が表示され、選択されていることを示すために強調表示されます。[Configuration] セクションが更新され、追加したプロフィールの現行設定が反映されます。

- 既存のサーバ プロファイルの設定を変更します。ページ左側の [FTP Server] の下で追加したプロファイルの設定済みアドレスをクリックするか、または [default] をクリックします。

  選択した項目が強調表示され、[Configuration] セクションが更新され、選択したプロファイルの現行設定が表示されます。既存のプロファイルを削除するには、削除するプロファイルの横にある削除アイコン( )をクリックします。

ステップ 6　オプションで、[Configuration] ページ領域に表示されている次の項目のいずれかを変更できます。

- [Networks] フィールドにリストされているアドレスを変更し、ページの他の領域をクリックします。

  ページの左側で、強調表示されているアドレスが更新されます。

  デフォルト プロファイルでは [Network] の設定を変更できないことに注意してください。デフォルト プロファイルは、別のプロファイルで指定されていないネットワーク上のすべてのサーバに適用されます。
- FTP トラフィックをモニタするポートを指定します。ポート 21 は FTP トラフィック用のウェルノウン ポートです。
- [File Get Commands] フィールドで、サーバからクライアントにファイルを転送するために使用される FTP コマンドを更新します。
- [File Put Commands] フィールドで、クライアントからサーバにファイルを転送するために使用される FTP コマンドを更新します。

注　サポートからの指示がない限り、[File Get Commands] フィールドと [File Put Commands] フィールドの値は変更しないでください。

- FTP/Telnet プリプロセッサによりデフォルトで検査される FTP コマンド以外に、追加の FTP コマンドを検出するには、[Additional FTP Commands] フィールドに、コマンドをスペースで区切って入力します。

  追加 FTP コマンドは、必要な数だけ追加できます。

注　追加できるコマンドには、`XPWD`、`XCWD`、`XCUP`、`XMKD`、`XRMD` があります。これらのコマンドの詳細については、RFC 775（Network Working Group によるディレクトリに基づく FTP コマンドの仕様）を参照してください。

- [Default Max Parameter Length] フィールドに、コマンド パラメータの最大長をバイト数で指定します。
- 特定のコマンドで異なる最大パラメータ長を検出するには、[Alternate Max Parameter Length] の横の [Add] をクリックします。表示される行の最初のテキスト ボックスに、最大パラメータ長を指定します。2 番目のテキスト ボックスに、この代替最大パラメータ長を適用するコマンドをスペースで区切って指定します。

  代替最大パラメータ長は、必要な数だけ追加できます。
- 特定のコマンドでフォーマット文字列攻撃を検査するには、[Check Commands for String Format Attacks] テキスト ボックスにコマンドをスペースで区切って指定します。
- コマンドの有効な形式を指定するには、[Command Validity] の横の [Add] をクリックします。検証対象のコマンドを指定してから、コマンド パラメータの検証ステートメントを入力します。検証ステートメントの構文の詳細については、サーバレベルの FTP オプションについて（27-24 ページ）を参照してください。
- データ転送チャネルで状態インスペクション以外のすべてのインスペクションを無効にして、FTP データ転送のパフォーマンスを改善するには、[Ignore FTP Transfers] を有効にします。

注　データ転送を検査するには、グローバル FTP/Telnet オプション [Stateful Inspection] を選択する必要があります。グローバル オプションの設定の詳細については、グローバル FTP および Telnet オプションについて（27-20 ページ）を参照してください。

- Telnet コマンドが FTP コマンド チャネルで使用された場合にそのことを検出するには、[Detect Telnet Escape Codes within FTP Commands] を選択します。
- FTP トラフィックの正規化時に Telnet の文字消去コマンドおよび行消去コマンドを無視するには、[Ignore Erase Commands during Normalization] を有効にします。

ステップ 7　サポートから指示された場合にのみ、オプションで、関連するトラブルシューティング オプションを変更します。そのためには、[Troubleshooting] オプションの横にある [+] 記号をクリックします。

ステップ 8　ポリシーを保存するか、編集を続行するか、変更内容を破棄するか、ベース ポリシーのデフォルト設定に戻すか、またはシステム キャッシュの変更を反映せずに終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

クライアントレベルの FTP オプションについて

ライセンス： Protection

FTP クライアントのプロファイルを作成できます。各プロファイル内で、クライアントからの FTP 応答の最大応答長を指定できます。また、デコーダが特定のクライアントの FTP コマンド チャネルでのバウンス攻撃と telnet コマンドの使用を検出するかどうかを設定できます。

次の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

Networks

FTP クライアントの 1 つ以上の IP アドレスを指定するには、このオプションを使用します。

単一 IP アドレスまたはアドレス ブロック、あるいはこのいずれかまたは両方をカンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト プロファイルを含め最大 255 個のプロファイルを設定できます。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-23 ページ）を参照してください。

デフォルト ポリシーの**デフォルト**設定では、別のターゲット ベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたはアドレス ブロックは指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、**すべて**を表すアドレス表記（0.0.0.0/0 または ::/0）を使用することはできません。

また、ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となるネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、「ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）」を参照してください。

Max Response Length

FTP クライアントからの応答文字列の最大長を指定するには、このオプションを使用します。

このオプションのイベントを生成するには、ルール 125:6 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Detect FTP Bounce Attempts

FTP バウンス攻撃を検出するには、このオプションを使用します。

このオプションのイベントを生成するには、ルール 125:8 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Allow FTP Bounce to

FTP PORT コマンドを FTP バウンス攻撃として扱わない追加のホストとそれらのホスト上のポートのリストを設定するには、このオプションを使用します。

Detect Telnet Escape Codes within FTP Commands

FTP コマンド チャネルで Telnet コマンドが使用された場合にそのことを検出するには、このオプションを使用します。

このオプションのイベントを生成するには、ルール 125:1 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Ignore Erase Commands During Normalization

[Detect Telnet Escape Codes within FTP Commands] が選択されている場合に、FTP トラフィックの正規化時に Telnet の文字および行の消去コマンドを無視するには、このオプションを使用します。この設定は、FTP クライアントによる Telnet 消去コマンドの処理方法に一致している必要があります。一般に、新しい FTP クライアントは Telnet 消去コマンドを無視しますが、ほとんどの古いクライアントは Telnet 消去コマンドを処理する点に注意してください。

クライアントレベル FTP オプションの設定

ライセンス：Protection

クライアントからの FTP トラフィックをモニタするように、FTP クライアントのクライアント プロファイルを設定できます。クライアントをモニタするために設定できるオプションの詳細については、クライアントレベルの FTP オプションについて（27-30 ページ）を参照してください。Telnet オプションの詳細については、Telnet オプションについて（27-22 ページ）を参照してください。その他の FTP オプションの詳細については、サーバレベルの FTP オプションについて（27-24 ページ）および グローバル FTP および Telnet オプションについて（27-20 ページ）を参照してください。

クライアントレベルの FTP オプションを設定するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Application Layer Preprocessors] の下の [FTP and Telnet Configuration] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効である場合は、[Enabled] をクリックし、次に [Edit] をクリックします。

[FTP and Telnet Configuration] ページが表示されます。

ステップ 5　次の 2 つのオプションから選択できます。

- 新しいクライアント プロファイルを追加します。ページの左側で [FTP Client] の横にある追加アイコン（  ）をクリックします。[Add Target] ポップアップ ウィンドウが表示されます。クライアントの 1 つ以上の IP アドレスを [Client Address] フィールドに指定し、[OK] をクリックします。

  単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をコンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト ポリシーを含め最大 255 個のポリシーを設定できます。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-23 ページ）を参照してください。

  ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となるネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、「ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）」を参照してください。

  ページの左側の FTP クライアント リストに新しい項目が表示され、選択されていることを示すために強調表示されます。[Configuration] セクションが更新され、追加したプロフィールの現行設定が反映されます。

- 既存のクライアント プロファイルの設定を変更します。ページ左側の [FTP Client] の下で追加したプロファイルの設定済みアドレスをクリックするか、または [default] をクリックします。

  選択した項目が強調表示され、[Configuration] セクションが更新され、選択したプロファイルの現行設定が表示されます。既存のプロファイルを削除するには、削除するプロファイルの横にある削除アイコン（）をクリックします。

ステップ 6　オプションで、[Configuration] ページ領域に表示されている次の項目のいずれかを変更できます。

- オプションで、[Networks] フィールドにリストされているアドレスを変更し、ページの他の領域をクリックします。

  ページの左側で、強調表示されているアドレスが更新されます。

  デフォルト プロファイルでは [Network] の設定を変更できないことに注意してください。デフォルト プロファイルは、別のプロファイルで指定されていないネットワーク上のすべてのクライアント ホストに適用されます。

- [Max Response Length] フィールドに、FTP クライアントからの応答の最大長をバイト単位で指定します。
- FTP バウンス攻撃を検出するには、[FTP] を選択します。

  FTP/Telnet デコーダは、FTP PORT コマンドが発行されたとき、指定のホストがクライアントの指定のホストと一致しない場合にそのことを検出します。

- FTP PORT コマンドを FTP バウンス攻撃として扱わない追加のホストとポートのリストを設定するには、[Allow FTP Bounce to] フィールドに、各ホスト（または CIDR 形式のネットワーク）、コロン（:）、およびポートまたはポート範囲をこの順序で指定します。ホストのポート範囲を入力するには、範囲の開始ポートと範囲の最終ポートをダッシュ（-）でつなげて表します。複数のホストを入力するには、ホスト項目をカンマで区切って入力します。

  たとえば、ホスト 192.168.1.1 に対する FTP PORT コマンドをポート 21 で許可し、ホスト 192.168.1.2 に対するコマンドをポート 22 ～ 1024 のいずれかで許可するには、次のように入力します。

  ```
  192.168.1.1:21, 192.168.1.2:22-1024
  ```

  FireSIGHT システムでの CIDR 表記とプレフィクス長の使用法については、IP アドレスの表記規則（1-23 ページ）を参照してください。

注　1 つのホストの個々の複数のポートを指定するには、ポート定義ごとにホストの IP アドレスを繰り返す必要があります。たとえば、192.168.1.1 のポート 22 と 25 を指定するには、`192.168.1.1:22, 192.168.1.1:25` と入力します。

- Telnet コマンドが FTP コマンド チャネルで使用された場合にそのことを検出するには、[Detect Telnet Escape Codes within FTP Commands] を選択します。
- FTP トラフィックの正規化時に Telnet の文字消去コマンドおよび行消去コマンドを無視するには、[Ignore Erase Commands During Normalization] を選択します。

ステップ 7　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

HTTP トラフィックのデコード

ライセンス： Protection

HTTP Inspect プリプロセッサは、次の処理を行います。

- ネットワーク上の Web サーバに送信される HTTP 要求と Web サーバから受信する HTTP 応答をデコードおよび正規化する。
- HTTP 関連の侵入ルールのパフォーマンス向上のため、Web サーバに送信されたメッセージを URI、非 cookie ヘッダー、cookie ヘッダー、メソッド、メッセージ ボディの各コンポーネントに分ける。
- HTTP 関連の侵入ルールのパフォーマンス向上のため、Web サーバから受信したメッセージをステータス コード、ステータス メッセージ、非 set-cookie ヘッダー、cookie ヘッダー、および応答ボディの各コンポーネントに分ける。
- URI エンコード攻撃の可能性を検出する。
- 正規化データを追加ルール処理に使用できるようにする。

HTTP トラフィックはさまざまな形式でエンコードされている可能性があり、このことが、ルールによる適切な検査の実施を困難にしています。HTTP Inspect は 14 種類のエンコードをデコードし、HTTP トラフィックが最良のインスペクションを受けられるようにします。

HTTP Inspect のオプションは、グローバルに設定するか、1 つのサーバで設定するか、またはサーバ リストに対して設定することができます。

HTTP Inspect プリプロセッサを使用するときは、次の点に注意してください。

- プリプロセッサ エンジンは HTTP の正規化を*ステートレス*に実行します。つまり、パケット単位で HTTP 文字列を正規化し、TCP ストリーム プリプロセッサにより再構成された HTTP 文字列のみを処理できます。
- ジェネレータ ID（GID）119 の HTTP プリプロセッサ ルールを使用してイベントを生成する場合は、これらのルールを有効にする必要があります。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

詳細については、次の項を参照してください。

- グローバル HTTP 正規化オプションの選択（27-34 ページ）
- グローバル HTTP 設定オプションの設定（27-35 ページ）
- サーバレベル HTTP 正規化オプションの選択（27-36 ページ）
- サーバレベル HTTP 正規化エンコード オプションの選択（27-44 ページ）
- HTTP サーバ オプションの設定（27-46 ページ）
- 追加の HTTP Inspect プリプロセッサ ルールの有効化（27-48 ページ）

グローバル HTTP 正規化オプションの選択

ライセンス： Protection

HTTP Inspect プリプロセッサのグローバル HTTP オプションは、プリプロセッサの機能を制御します。Web サーバ ポートとして指定されていないポートが HTTP トラフィックを受信する場合の HTTP 正規化を有効または無効にするには、このオプションを使用します。

次の点に注意してください。

- [Unlimited Decompression] を有効にすると、変更のコミット時に [Maximum Compressed Data Depth] および [Maximum Decompressed Data Depth] オプションが自動的に 65535 に設定されます。詳細については、「サーバレベル HTTP 正規化オプションの選択（27-36 ページ）」を参照してください。
- アクセス コントロール ポリシーのデフォルト アクションに関連付けられている侵入ポリシーと、アクセス コントロール ルールに関連付けられている侵入ポリシーで、[Maximum Compressed Data Depth] と [Maximum Decompressed Data Depth] オプションの値が異なる場合は、最も大きな値が使用されます。

次の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

Detect Anomalous HTTP Servers

Web サーバ ポートとして指定されていないポートに送信された HTTP トラフィックまたはこのポートで受信した HTTP トラフィックを検出します。

注　このオプションをオンにする場合は、[HTTP Configuration] ページで、HTTP トラフィックを受信するすべてのポートがサーバ プロファイルにリストされていることを確認してください。確認せずにこのオプションと関連するプリプロセッサ ルールを有効にすると、サーバとの間の通常のトラフィックによってイベントが生成されます。デフォルトのサーバ プロファイルには、HTTP トラフィックに一般に使用されるすべてのポートが含まれていますが、このプロファイルを変更した場合は、イベントの生成を防ぐために別のプロファイルにそれらのポートを追加する必要があります。

このオプションのイベントを生成するには、ルール 120:1 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Detect HTTP Proxy Servers

[Allow HTTP Proxy Use] オプションで定義されていないプロキシ サーバを使用する HTTP トラフィックを検出します。

このオプションのイベントを生成するには、ルール 119:17 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Maximum Compressed Data Depth

[Inspect Compressed Data]（およびオプションで [Decompress SWF File (LZMA)]、[Decompress SWF File (Deflate)]、または [Decompress PDF File (Deflate)]）が有効になっている場合は、圧縮解除する圧縮データの最大サイズを設定します。指定できるバイト数は 1 ～ 65535 です。

Maximum Decompressed Data Depth

[Inspect Compressed Data]（およびオプションで [Decompress SWF File (LZMA)]、[Decompress SWF File (Deflate)]、または [Decompress PDF File (Deflate)]）が有効になっている場合は、正規化された圧縮解除データの最大サイズを設定します。指定できるバイト数は 1 ～ 65535 です。

グローバル HTTP 設定オプションの設定

ライセンス：Protection

非標準ポートへの HTTP トラフィックとプロキシ サーバを使用する HTTP トラフィックの検出を設定できます。グローバル HTTP 設定オプションの詳細については、グローバル HTTP 正規化オプションの選択（27-34 ページ）を参照してください。

グローバル HTTP 設定オプションを設定するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Application Layer Preprocessors] の下の [HTTP Configuration] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効である場合は、[Enabled] をクリックし、次に [Edit] をクリックします。

[HTTP Configuration] ページが表示されます。

ステップ 5　グローバル HTTP 正規化オプションの選択（27-34 ページ）で説明するグローバル オプションを変更できます。

ステップ 6　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

サーバレベル HTTP 正規化オプションの選択

ライセンス： Protection

サーバレベルのオプションは、モニタ対象サーバごとに設定するか、すべてのサーバに対してグローバルに設定するか、またはサーバ リストに対して設定することができます。また、事前定義のサーバ プロファイルを使用してこれらのオプションを設定するか、またはご使用の環境のニーズに合わせて個別に設定することができます。これらのオプション、またはこれらのオプションを設定するデフォルト プロファイルの 1 つを使用して、トラフィックを正規化する HTTP サーバ ポート、正規化するサーバ応答ペイロードの量、および正規化するエンコードのタイプを指定します。

次の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

Networks

1 つ以上のサーバの IP アドレスを指定するには、このオプションを使用します。単一 IP アドレスまたはアドレス ブロック、あるいはこのいずれかまたは両方をカンマで区切ったリストを指定できます。

プロファイルの合計数はデフォルト プロファイルを含めて 255 までであることに加え、HTTP サーバ リストに指定できる文字数は496 文字（項目にして約 26 個分）まで、またすべてのサーバ プロファイルに対して指定できるアドレス項目の合計数は 256 個までです。FireSIGHT システムでの IPv4 CIDR 表記と IPv6 プレフィクス長の使用法については、IP アドレスの表記規則（1-23 ページ）を参照してください。

デフォルト ポリシーの**デフォルト**設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィクス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、**すべて** を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

また、ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となるネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、「ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）」を参照してください。

ポート

プリプロセッサ エンジンが HTTP トラフィックを正規化するポート。複数のポート番号を指定する場合は、カンマで区切ります。

Oversize Dir Length

指定された値よりも長い URL ディレクトリを検出します。

このオプションのイベントを生成するには、ルール 119:15 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Client Flow Depth

[Ports] で定義されているクライアント側 HTTP トラフィックで、ルールにより検査される raw HTTP パケットのバイト数（ヘッダーとペイロード データを含む）を指定します。ルール内の HTTP コンテンツ ルール オプションによって要求メッセージの特定の部分が検査される場合は、[Client Flow Depth] は適用されません。詳細については、「HTTP コンテンツ オプション（36-25 ページ）」を参照してください。

-1 ～ 1460 の値を指定できます。Cisco は、[Client Flow Depth] をその最大値に設定することを推奨しています。次のいずれかを指定します。

- 1 ～ 1460 を指定すると、最初のパケットで指定のバイト数が検査されます。最初のパケットのバイト数が指定のバイト数よりも少ない場合は、パケット全体が検査されます。指定された値は、セグメント化されたパケットと再構成されたパケットの両方に適用されることに注意してください。

  また、値 300 を指定すると、通常は、多くのクライアント要求見出しの終わりにある大きな HTTP Cookie のインスペクションが排除されることにも注意してください。
- 0 を指定すると、すべてのクライアント側トラフィックが検査されます。これにはセッション内の複数のパケットが含まれ、必要な場合には 1460 バイトの制限を超えることもあります。この値はパフォーマンスに影響する可能性があることに注意してください。
- -1 を指定すると、クライアント側のすべてのトラフィックが無視されます。

Server Flow Depth

[Ports] で指定されたサーバ側 HTTP トラフィックで、ルールにより検査される raw HTTP パケットのバイト数を指定します。[Inspect HTTP Responses] が無効である場合は raw 見出しとペイロードが検査され、[Inspect HTTP Response] が有効である場合は、raw 応答ボディのみが検査されます。

Server Flow Depth は、[Ports] で定義されているサーバ側 HTTP トラフィックで、ルールにより検査されるセッション内の raw サーバ応答データのバイト数を指定します。このオプションを使用して、HTTP サーバ応答データのインスペクションのレベルとパフォーマンスのバランスを調整できます。ルール内の HTTP コンテンツ オプションによって要求メッセージの特定の部分が検査される場合は、Server Flow Depth は適用されません。詳細については、「HTTP コンテンツ オプション（36-25 ページ）」を参照してください。

Client Flow Depth とは異なり、Server Flow Depth では、ルールが検査するバイト数を、HTTP 要求パケットごとではなく、HTTP 応答ごとのバイト数として指定します。

-1 ～ 65535 の値を指定できます。Cisco は、[Server Flow Depth] をその最大値に設定することを推奨しています。次のいずれかの値を指定できます。

- 1 ～ 65535 の範囲の値:

  [Inspect HTTP Responses] が**有効**である場合、raw HTTP 応答ボディのみが検査され、raw HTTP 見出しは検査されません。また、[Inspect Compressed Data] が有効である場合は、圧縮解除データも検査されます。

  [Inspect HTTP Responses] が**無効**である場合、raw パケット 見出しとペイロードが検査されます。

セッションの応答バイト数が指定の値よりも少ない場合は、そのセッションで、ルールにより（必要に応じて複数パケットにわたって）すべての応答パケットが完全に検査されます。セッションの応答バイト数が指定の値よりも多い場合、そのセッションで、ルールにより（必要に応じて複数パケットにわたって）指定のバイト数だけが検査されます。

Flow Depth の値が小さい場合、[Ports] で定義されているサーバ側トラフィックを対象とするルールで、検出漏れが発生する可能性があります。これらのルールのほとんどは HTTP ヘッダーまたはコンテンツ（これは多くの場合非ヘッダー データの先頭の約 100 バイト内にあります）を対象とします。通常見出しの長さは 300 バイト未満ですが、見出し サイズは異なることがあります。

指定された値は、セグメント化されたパケットと再構成されたパケットの両方に適用されることにも注意してください。

- 0 を指定すると、[Port] で定義されているすべての HTTP サーバ側トラフィックでパケット全体が検査されます。これにはセッションでの 65535 バイトよりも大きな応答データも含まれます。

  この値はパフォーマンスに影響する可能性があることに注意してください。

- -1：

  [Inspect HTTP Responses] が**有効**な場合、raw HTTP 見出しだけが検査され、raw HTTP 応答ボディは検査されません。

  [Inspect HTTP Responses] が**無効**である場合、[Ports] で定義されているすべてのサーバ側トラフィックは無視されます。

Maximum Header Length

[Inspect HTTP Responses] が有効である場合は、HTTP 要求、および HTTP 応答で、指定されている最大バイト数よりも長い見出し フィールドを検出します。値 0 を指定すると、このオプションが無効になります。有効にするには、1 ～ 65535 の値を指定します。

このオプションのイベントを生成するには、ルール 119:19 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Maximum Number of Headers

HTTP 要求で見出し数がこの設定を超えている場合にそのことを検出します。有効にするには、1 ～ 1024 の値を指定します。

このオプションのイベントを生成するには、ルール 119:20 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Maximum Number of Spaces

折りたたみ行のスペースの数が HTTP 要求のこの設定と等しいか、超えている場合にそのことを検出します。値 0 を指定すると、このオプションが無効になります。有効にするには、1 ～ 65535 の値を指定します。

このオプションのイベントを生成するには、ルール 119:26 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

HTTP Client Body Extraction Depth

HTTP クライアント要求のメッセージ ボディから抽出するバイト数を指定します。侵入ルールを使用して抽出データを検査するには、`content` または `protected_content` キーワードを [HTTP Client Body] オプションと共に選択します。詳細については、「HTTP コンテンツ オプション（36-25 ページ）」を参照してください。

-1 ～ 65495 の値を指定します。クライアント ボディを無視するには、-1 を指定します。クライアント ボディ全体を抽出するには、0 を指定します。抽出対象のバイト数を指定すると、システム パフォーマンスが向上することがある点に注意してください。また、侵入ルールで [HTTP Client Body] オプションが機能するためには、0 ～ 65495 の値を指定する必要があります。

Small Chunk Size

チャンクが小さいとみなされるサイズの最大バイト数を指定します。1 ～ 255 の値を指定します。値 0 を指定すると、異常な小さなセグメントの連続の検出が無効になります。詳細については、[Consecutive Small Chunks] オプションを参照してください。

Consecutive Small Chunks

チャンク転送エンコードを使用するクライアント トラフィックまたはサーバ トラフィックで異常に大量であるとみなされる、連続する小さなチャンクの数を指定します。[Small Chunk Size] オプションは、小さなチャンクの最大サイズを指定します。

たとえば、10 バイト以下のチャンクが 5 つ連続していることを検出するには、[Small Chunk Size] に 10 を設定し、[Consecutive Small Chunks] に 5 を設定します。

大量の小さなチャンクが検出される場合にイベントをトリガーするには、クライアント トラフィックの場合はプリプロセッサ ルール 119:27 を有効にし、サーバ トラフィックの場合はルール 120:7 を有効にします。[Small Chunk Size] が有効であり、このオプションが 0 または 1 に設定されている場合にこれらのルールを有効にすると、指定されたサイズ以下のすべてのチャンクでイベントがトリガーとして使用されます。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

HTTP メソッド

システムがトラフィックで検出すると予期される、GET および POST 以外の HTTP 要求メソッドを指定します。複数の値はカンマで区切ります。

侵入ルールは、HTTP メソッドのコンテンツを検索するため、`content` または `protected_content` キーワードをその **HTTP Method** 引数で使用します。HTTP コンテンツ オプション（36-25 ページ）を参照してください。GET、POST、およびこのオプションで設定されているメソッド以外のメソッドがトラフィックで検出される場合にイベントを生成するには、ルール 119:31 を有効にします。

No Alerts

関連するプリプロセッサ ルールが有効である場合に、侵入イベントを無効にします。

注　このオプションでは、HTTP 標準テキスト ルールとshared object ruleは無効に**なりません**。

Normalize HTTP Headers

[Inspect HTTP Responses] が有効である場合は、要求ヘッダーと応答ヘッダーで非 cookie データの正規化が有効になります。[Inspect HTTP Responses] が有効**ではない**場合は、要求見出しと応答見出しで cookie を含む HTTP 見出し全体の正規化が有効になります。

Inspect HTTP Cookies

HTTP 要求見出しからの cookie の抽出を有効にします。また、[Inspect HTTP Responses] が有効である場合は、応答ヘッダーの set-cookie データの抽出も有効になります。cookie の抽出が不要な場合は、このオプションを無効にするとパフォーマンスが向上します。

Cookie: および Set-Cookie: の見出し名、見出し行の先頭のスペース、および見出し行の末尾の CRLF は、cookie の一部ではなく見出しの一部として検査されます。

Normalize Cookies in HTTP headers

HTTP 要求見出しの cookie の正規化を有効にします。[Inspect HTTP Responses] が有効である場合は、応答ヘッダーで set-cookie データの正規化も有効になります。このオプションを選択する前に、[Inspect HTTP Cookies] を選択する必要があります。

Allow HTTP Proxy Use

モニタ対象 Web サーバを HTTP プロキシとして使用できるようにします。このオプションは、HTTP 要求のインスペクションでのみ使用されます。

Inspect URI Only

正規化された HTTP 要求パケットの URI 部分のみを検査します。

Inspect HTTP Responses

HTTP 応答の拡張インスペクションが有効になり、プリプロセッサは、HTTP 要求メッセージのデコードと正規化の他に、ルール エンジンによるインスペクションのために応答フィールドを抽出します。このオプションを有効にすると、応答ヘッダー、ボディ、ステータス コードなどがシステムにより抽出されます。また [Inspect HTTP Cookies] が有効である場合は、set-cookie データも抽出されます。詳細については、HTTP コンテンツ オプション（36-25 ページ）、HTTP エンコードのタイプと位置によるイベントの生成（36-102 ページ）、特定のペイロード タイプを指し示す（36-105 ページ）を参照してください。

このオプションのイベントを生成するには、ルール 120:2 および 120:3 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Normalize UTF Encodings to UTF-8

[Inspect HTTP Responses] が有効である場合、HTTP 応答で UTF-16LE、UTF-16BE、UTF-32LE、および UTF32-BE エンコーディングが検出され、UTF8 に正規化されます。

このオプションのイベントを生成するには、ルール 120:4 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Inspect Compressed Data

[Inspect HTTP Responses] が有効である場合、HTTP 応答ボディでの gzip および deflate 互換圧縮データの圧縮解除と、正規化された圧縮解除データのインスペクションが有効になります。システムは、チャンク HTTP 応答データと非チャンク HTTP 応答データを検査します。システムは、必要に応じて複数のパケットにわたり圧縮解除データをパケット単位で検査します。つまり、システムが異なるパケットの圧縮解除データをインスペクションのために結合させることはありません。[Maximum Compressed Data Depth]、[Maximum Decompressed Data Depth]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[Unlimited Decompression] を選択していない場合は、[Server Flow Depth] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、file_data ルール キーワードを使用できます。詳細については、特定のペイロード タイプを指し示す（36-105 ページ）を参照してください。

Unlimited Decompression

[Inspect Compressed Data]（およびオプションで [Decompress SWF File (LZMA)]、[Decompress SWF File (Deflate)]、または [Decompress PDF File (Deflate)]）が有効である場合、複数パケットにわたって [Maximum Decompressed Data Depth] がオーバーライドされます。つまり、このオプションにより、複数パケットにわたる無制限の圧縮解除が有効になります。このオプショ

ンを有効にしても、単一パケット内での [Maximum Compressed Data Depth] または [Maximum Decompressed Data Depth] には影響しないことに注意してください。また、このオプションを有効にすると、変更のコミット時に、[Maximum Compressed Data Depth] と [Maximum Decompressed Data Depth] が 65535 に設定されることにも注意してください。グローバル HTTP 正規化オプションの選択（27-34 ページ）を参照してください。

Normalize Javascript

[Inspect HTTP Responses] が有効な場合、HTTP 応答ボディ内での Javascript の検出と正規化を有効にします。プリプロセッサは unescape 関数や decodeURI 関数、String.fromCharCode メソッドなどの難読化 Javascript データを正規化します。プリプロセッサは、unescap、decodeURI、および decodeURIComponent 関数内の次のエンコードを正規化します。

- %XX
- %uXXXX
- 0xXX
- \xXX
- \uXXXX

プリプロセッサは連続するスペースを検出し、1 つのスペースに正規化します。このオプションが有効である場合、設定フィールドでは、難読化 Javascript データで許容する連続スペースの最大数を指定できます。入力できる値は、1 ～ 65535 です。値 0 を指定すると、このフィールドに関連付けられているプリプロセッサ ルール（120:10）が有効かどうかに関係なく、イベントの生成が無効になります。

プリプロセッサは、Javascript の正符号（+）演算子も正規化し、この演算子を使用して文字列を連結します。

`file_data` キーワードを使用して、侵入ルールに対し正規化された Javascript データを指し示すことができます。詳細については、「特定のペイロード タイプを指し示す（36-105 ページ）」を参照してください。

このオプションのイベントを生成するには、次に示すように、ルール 120:9、120:10、および 120:11 を有効にします。

表 27-6　Normalize Javascript Option Rules

ルール	イベントがトリガーとして使用される条件
120:9	プリプロセッサ内の難読化レベルが 2 以上である。
120:10	Javascript 難読化データで連続するスペースの数が、許容される連続スペースの最大数として設定された値以上である。
120:11	エスケープされたデータまたはエンコードされたデータに、複数のエンコード タイプが含まれている。

詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Decompress SWF File (LZMA) および Decompress SWF File (Deflate)

[HTTP Inspect Responses] が有効な場合、これらのオプションによって HTTP 要求の HTTP 応答ボディ内にあるファイルの圧縮された部分が圧縮解除されます。

注　圧縮解除できるのは、HTTP GET 応答で見つかったファイルの圧縮された部分**のみ**です。

- [Decompress SWF File (LZMA)] によって、Adobe ShockWave Flash（.swf）ファイルの LZMA に互換性がある圧縮された部分が圧縮解除されます。
- [Decompress SWF File (Deflate)] によって、Adobe ShockWave Flash（.swf）ファイルの deflate に互換性がある圧縮された部分が圧縮解除されます。

[Maximum Compressed Data Depth]、[Maximum Decompressed Data Depth]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[Unlimited Decompression] を選択していない場合は、[Server Flow Depth] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、file_data ルール キーワードを使用できます。詳細については、特定のペイロード タイプを指し示す（36-105 ページ）を参照してください。

このオプションのイベントを生成するには、次に示すように、ルール 120:12 および 120:13 を有効にします。

表 27-7　SWF ファイルの圧縮解除オプションのルール

ルール	イベントがトリガーとして使用される条件
120:12	deflate ファイルの圧縮解除が失敗します。
120:13	LZMA ファイルの圧縮解除が失敗します。

Decompress PDF File (Deflate)

[HTTP Inspect Responses] が有効な場合、[Decompress PDF File (Deflate)] によって、HTTP 要求の HTTP 応答ボディ内にある Portable Document Format（.pdf）ファイルの deflate に互換性がある圧縮された部分が圧縮解除されます。システムが圧縮解除できるのは、/FlateDecode ストリーム フィルタが付いた PDF ファイルのみです。他のストリーム フィルタ（/FlateDecode /FlateDecode など）はサポートされません。

注　圧縮解除できるのは、HTTP GET 応答で見つかったファイルの圧縮された部分**のみ**です。

[Maximum Compressed Data Depth]、[Maximum Decompressed Data Depth]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[Unlimited Decompression] を選択していない場合は、[Server Flow Depth] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、file_data ルール キーワードを使用できます。詳細については、特定のペイロード タイプを指し示す（36-105 ページ）を参照してください。

このオプションのイベントを生成するには、次に示すように、ルール 120:14、120:15、120:16 および 120:17 を有効にします。

表 27-8　PDF ファイル（Deflate）の圧縮解除オプションのルール

ルール	イベントがトリガーとして使用される条件
120:14	ファイルの圧縮解除が失敗します。
120:15	サポートされていない圧縮タイプのためファイルの圧縮解除が失敗します。
120:16	サポートされていない PDF ストリーム フィルタのためファイルの圧縮解除が失敗します。
120:17	ファイルの解析が失敗します。

Extract Original Client IP Address

X-Forwarded-For（XFF）、True-Client-IP またはカスタム定義された HTTP ヘッダーから、元のクライアント IP アドレスを抽出できるようにします。侵入イベント テーブル ビューで、抽出された元のクライアント IP アドレスを表示できます。詳細については、「侵入イベントについて（41-11 ページ）」を参照してください。

このオプションのイベントを生成するには、ルール 119:23、119:29、および 119:30 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

XFF Header Priority

[Extract Original Client IP Address] が有効な場合、システムが元のクライアント IP HTTP ヘッダーを処理する順序を指定します。モニタ対象ネットワークで、X-Forwarded-For (XFF) または True-Client-IP 以外の元のクライアント IP ヘッダーが発生すると予測される場合は、[Add] をクリックしてプライオリティ リストに追加のヘッダー名を追加できます。その後、各ヘッダー タイプの横にある上下の矢印アイコンを使用して、優先順位を調整できます。複数の XFF ヘッダーが HTTP 要求に表示されている場合、システムは最も優先順位が高いヘッダーのみを処理することに注意してください。

Log URI

raw URI が存在する場合に、HTTP 要求パケットから raw URI を抽出できるようにし、このセッションで生成されるすべての侵入イベントにこの URI を関連付けます。

このオプションが有効である場合、侵入イベント テーブル ビューの [HTTP URI] 列に、抽出された URI の先頭 50 文字を表示できます。パケット ビューでは、URI 全体（最大 2048 バイト）を表示できます。詳細については、侵入イベントについて（41-11 ページ）およびイベント情報の表示（41-25 ページ）を参照してください。

Log Hostname

ホスト名が存在する場合に、HTTP 要求の Host 見出しから raw URI を抽出できるようにし、このセッションで生成されるすべての侵入イベントにこのホスト名を関連付けます。複数の Host 見出しがある場合は、1 番目の見出しからホスト名を抽出します。

このオプションが有効である場合、侵入イベント テーブル ビューの [HTTP Hostname] 列に、抽出されたホスト名の先頭 50 文字を表示できます。パケット ビューでは、ホスト名全体（最大 256 バイト）を表示できます。詳細については、侵入イベントについて（41-11 ページ）およびイベント情報の表示（41-25 ページ）を参照してください。

このオプションのイベントを生成するには、ルール 119:25 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

プリプロセッサとルール 119:24 が有効である場合は、HTTP 要求で複数の Host 見出しが検出される場合でも、プリプロセッサはこのオプションの設定に関係なく、侵入イベントを生成することに注意してください。詳細については、「追加の HTTP Inspect プリプロセッサ ルールの有効化（27-48 ページ）」を参照してください。

Profile

HTTP トラフィック向けに正規化されたエンコードのタイプを指定します。システムには、ほとんどのサーバに適用できるデフォルト プロファイル、Apache サーバと IIS サーバ用のデフォルト プロファイル、およびモニタ対象トラフィックのニーズに合わせて調整できるカスタムのデフォルト設定があります。詳細については、「サーバレベル HTTP 正規化エンコード オプションの選択（27-44 ページ）」を参照してください。

サーバレベル HTTP 正規化エンコード オプションの選択

ライセンス：Protection

HTTP トラフィック向けに正規化されているエンコード タイプを指定し、このタイプのエンコードを含むトラフィックに対してシステムがイベントを生成するようにするには、サーバレベルの HTTP 正規化オプションを選択できます。

次の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ASCII Encoding

エンコードされた ASCII 文字をデコードし、ルール エンジンが ASCII エンコード URI でイベントを生成するかどうかを指定します。

このオプションのイベントを生成するには、ルール 119:1 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

UTF-8 Encoding

URI の標準 UTF8 Unicode シーケンスをデコードします。

このオプションのイベントを生成するには、ルール 119:6 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Microsoft %U Encoding

%u とその後に続く 4 文字を使用する IIS %u エンコード スキームをデコードします。この 4 文字は、IIS Unicode コードポイントと相関する 16 進数のエンコード値です。

ヒント 正規のクライアントが %u エンコードを使用することはほとんどないため、Ciscoは、%u エンコードによってエンコードされている HTTP トラフィックをデコードすることを推奨します。

このオプションのイベントを生成するには、ルール 119:3 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Bare Byte UTF-8 Encoding

ベア バイト エンコードをデコードします。ベア バイト エンコードは、UTF8 値のデコード時に非 ASCII 文字を有効な値として使用します。

ヒント ベア バイト エンコードにより、ユーザは IIS サーバをエミュレートし、非標準エンコードを正しく解釈することができます。正規のクライアントはこの方法で UTF8 をエンコードしないため、Cisco は、このオプションを有効にすることを推奨します。

このオプションのイベントを生成するには、ルール 119:4 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Microsoft IIS Encoding

Unicode コードポイント マッピングを使用してデコードします。

ヒント これは主に攻撃と回避の試行で見られるため、Ciscoはこのオプションを有効にすることを推奨します。

このオプションのイベントを生成するには、ルール 119:7 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Double Encoding

要求 URI を 2 回通過し、それぞれでデコードを実行するようにすることで、IIS 二重エンコード トラフィックをデコードします。これは通常は攻撃シナリオでのみ検出されるため、Cisco はこのオプションを有効にすることを推奨します。

このオプションのイベントを生成するには、ルール 119:2 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Multi-Slash Obfuscation

1 つの行内の複数のスラッシュを 1 つのスラッシュに正規化します。

このオプションのイベントを生成するには、ルール 119:8 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

IIS Backslash Obfuscation

バックスラッシュをスラッシュに正規化します。

このオプションのイベントを生成するには、ルール 119:9 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Directory Traversal

ディレクトリ トラバーサルおよび自己参照用ディレクトリを正規化します。一部の Web サイトはディレクトリ トラバーサルを使用してファイルを参照するため、このタイプのトラフィックに対してイベントを生成するために、関連するプリプロセッサ ルールを有効にすると、誤検出が発生する可能性があります。

このオプションのイベントを生成するには、ルール 119:10 および 119:11 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Tab Obfuscation

スペース区切り記号としてタブを使用する非 RFC 標準を正規化します。Apache やその他の IIS 以外の Web サーバは、URL の区切り文字としてタブ文字（0x09）を使用します。

注　このオプションの設定に関係なく、空白文字（0x20）がタブの前にある場合、HTTP Inspect プリプロセッサはそのタブをスペースとして扱います。

このオプションのイベントを生成するには、ルール 119:12 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Invalid RFC Delimiter

URI データの改行（\ n）を正規化します。

このオプションのイベントを生成するには、ルール 119:13 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Webroot Directory Traversal

URL の初期ディレクトリを越えて横断するディレクトリ トラバーサルを検出します。

このオプションのイベントを生成するには、ルール 119:18 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Tab URI Delimiter

URI の区切り文字としてタブ文字（0x09）を有効にします。Apache、新しいバージョンの IIS、およびその他の一部の Web サーバは、URL の区切り文字としてタブ文字を使用します。

注　このオプションの設定に関係なく、空白文字（0x20）がタブの前にある場合、HTTP Inspect プリプロセッサはそのタブをスペースとして扱います。

Non-RFC characters

対応するフィールドに追加する非 RFC 文字リストが、着信または発信 URI データ内に含まれている場合にそれを検出します。このフィールドを変更する場合は、バイト文字を表す 16 進表記を使用します。このオプションを設定する場合は、値を慎重に設定してください。非常に一般的な文字を使用すると、イベントが大量に発生する可能性があります。

このオプションのイベントを生成するには、ルール 119:14 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Max Chunk Encoding Size

URI データで異常に大きなチャンク サイズを検出します。

このオプションのイベントを生成するには、ルール 119:16 および 119:22 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Disable Pipeline Decoding

パイプライン処理された要求の HTTP デコードを無効にします。このオプションが無効である場合、パイプラインで待機する HTTP 要求には、デコードおよび分析は行われず、汎用パターン マッチングを使用した検査のみが行われるため、パフォーマンスが向上します。

Non-Strict URI Parsing

Non-Strict URI 解析を有効にします。このオプションは、「GET /index.html abc xo qr \n」という形式の非標準 URI を受け入れるサーバのみで使用します。このオプションを使用すると、デコーダは URI が 1 番目のスペースと 2 番目のスペースで囲まれているものと想定します。これは、2 番目のスペースの後に有効な HTTP 識別子がない場合でも同様です。

Extended ASCII Encoding

HTTP 要求 URI の拡張 ASCII 文字の解析を有効にします。このオプションは、カスタム サーバ プロファイルでのみ使用可能であり、Apache、IIS、またはすべてのサーバ向けに提供されるデフォルト プロファイルでは使用できないことに注意してください。

HTTP サーバ オプションの設定

ライセンス： Protection

HTTP サーバ オプションを設定するには、次の手順に従います。HTTP サーバ オプションの詳細については、サーバレベル HTTP 正規化オプションの選択（27-36 ページ）および サーバレベル HTTP 正規化エンコード オプションの選択（27-44 ページ）を参照してください。

サーバレベルの HTTP 設定オプションを設定するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Application Layer Preprocessors] の下の [HTTP Configuration] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効である場合は、[Enabled] をクリックし、次に [Edit] をクリックします。

[HTTP Configuration] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　次の 2 つのオプションから選択できます。

- 新しいサーバ プロファイルを追加します。ページの左側で [Servers] の横にある追加アイコン（  ）をクリックします。[Add Target] ポップアップ ウィンドウが表示されます。クライアントの 1 つ以上の IP アドレスを [Server Address] フィールドに指定し、[OK] をクリックします。

  単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をコンマで区切ったリストを指定できます。リストに入力できる文字数は最大 496 文字、すべてのサーバ プロファイルで指定できるアドレス項目の総数は 256、作成できるプロファイルの総数はデフォルト プロファイルを含めて 255 です。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-23 ページ）を参照してください。

  ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となるネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、「ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）」を参照してください。

  ページの左側のサーバ リストに新しい項目が表示され、選択されていることを示すために強調表示されます。[Configuration] セクションが更新され、追加したプロフィールの現行設定が反映されます。

- 既存のプロファイルの設定を変更します。ページ左側の [Servers] の下で追加したプロファイルの設定済みアドレスをクリックするか、または [default] をクリックします。

  選択した項目が強調表示され、[Configuration] セクションが更新され、選択したプロファイルの現行設定が表示されます。既存のプロファイルを削除するには、削除するプロファイルの横にある削除アイコン（  ）をクリックします。

ステップ 6　オプションで、[Networks] フィールドにリストされているアドレスを変更し、ページの他の領域をクリックします。

ページの左側で、強調表示されているアドレスが更新されます。

デフォルト プロファイルでは [Networks] の設定を変更できないことに注意してください。デフォルト プロファイルは、別のプロファイルで指定されていないネットワーク上のすべてのサーバに適用されます。

ステップ 7　[Ports] フィールドに、HTTP Inspect でトラフィックを検査するポートを指定します。複数のポートを指定する場合は、カンマで区切ります。

ステップ 8　サーバレベル HTTP 正規化オプションの選択（27-36 ページ）で説明するその他のオプションを変更できます。

ステップ 9　次の手順に従ってサーバ プロファイルを選択します。

- 独自のサーバ プロファイルを作成するには、[Custom] を選択します（詳細については、サーバレベル HTTP 正規化エンコード オプションの選択（27-44 ページ）を参照）。
- すべてのサーバに対して適切な標準のデフォルト プロファイルを使用するには、[All] を選択します。
- デフォルトの IIS プロファイルを使用するには、[IIS] を選択します。
- デフォルトの Apache プロファイルを使用するには、[Apache] を選択します。

ステップ 10　[Custom] を選択すると、カスタム オプションが表示されます。

ステップ 11　プロファイルで、使用する HTTP デコード オプションを設定します。

使用可能な正規化オプションの詳細についてはサーバレベル HTTP 正規化オプションの選択（27-36 ページ）、参照してください。

ステップ 12　ポリシーを保存するか、編集を続行するか、変更内容を破棄するか、ベース ポリシーのデフォルト設定に戻すか、またはシステム キャッシュの変更を反映せずに終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

追加の HTTP Inspect プリプロセッサ ルールの有効化

ライセンス：Protection

特定の設定オプションに関連付けられていない HTTP Inspect プリプロセッサ ルールのイベントを生成するには、次の表の「プリプロセッサ ルール GID:SID」列のルールを有効にできます。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

表 27-9　追加の HTTP Inspect プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
120:5	HTTP 応答トラフィックで UTF7 エンコードが検出されるとイベントが生成されます。UTF7 は、SMTP トラフィックなど、7 ビット パリティが必要な場合にだけ使用する必要があります。
119:21	HTTP 要求ヘッダーに複数の `content-length` フィールドがある場合に、イベントが生成されます。
119:24	HTTP 要求に複数の Host 見出しがある場合に、イベントが生成されます。

表 27-9　追加の HTTP Inspect プリプロセッサ ルール（続き）

プリプロセッサ ルール GID:SID	説明
119:28 120:8	これらのルールを有効にする場合、イベントは生成されません。
119:32	トラフィックで HTTP バージョン 0.9 が検出されると、イベントが生成されます。TCP ストリームの設定も有効にする必要があることに注意してください。TCP ストリームの前処理の使用（29-22 ページ）を参照してください。
119:33	エスケープされていないスペースが HTTP URI に含まれている場合に、イベントが生成されます。
119:34	TCP 接続に 24 以上のパイプライン処理された HTTP 要求が含まれている場合に、イベントが生成されます。

Sun RPC プリプロセッサの使用

ライセンス：Protection

RPC（Remote Procedure Call）正規化では、フラグメント化された RPC レコードが 1 つのレコードに正規化されるので、ルール エンジンがそのレコード全体を検査できます。たとえば、攻撃者が RPC `admind` が実行されているポートの検出を試行するとします。一部の UNIX ホストは、RPC `admind` を使用してリモート分散システム タスクを実行します。ホストが弱い認証を実行する場合、悪意のあるユーザがリモート管理のコントロールを獲得できることがあります。Snort ID（SID）が 575 の標準テキスト ルール（ジェネレータ ID:1）は、この攻撃を検出するために、特定のロケーションでコンテンツを検索し、不適切な `portmap GETPORT` 要求を特定します。

ポート

トラフィックを正規化するポートを示します。インターフェイスで、複数のポートをカンマで区切って指定します。一般的な RPC ポートは 111 および 32771 です。ネットワークが他のポートに RPC トラフィックを送信する場合は、それらのポートの追加を検討してください。

Detect fragmented RPC records

RPC フラグメント化レコードを検出します。

このオプションのイベントを生成するには、ルール 106:1 および 106:5 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Detect multiple records in one packet

パケット（または再構成されたパケット）ごとに、複数の RPC 要求を検出します。

このオプションのイベントを生成するには、ルール 106:2 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Detect fragmented record sums which exceed one fragment

現在のパケット長を超える再構成されたフラグメント化レコード長を検出します。

このオプションのイベントを生成するには、ルール 106:3 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Detect single fragment records which exceed the size of one packet

部分的なレコードを検出します。

このオプションのイベントを生成するには、ルール 106:4 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Sun RPC プリプロセッサの設定

ライセンス：Protection

Sun RPC プリプロセッサを設定するには、次の手順を使用できます。Sun RPC プリプロセッサ設定オプションの詳細については、Sun RPC プリプロセッサの使用（27-49 ページ）を参照してください。

Sun RPC プリプロセッサを設定するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Application Layer Preprocessors] の下の [Sun RPC Configuration] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効である場合は、[Enabled] をクリックし、次に [Edit] をクリックします。

[Sun RPC Configuration] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　[Ports] フィールドに、RPC トラフィックをデコードするポートの番号を入力します。複数のポートを指定する場合は、カンマで区切ります。

ステップ 6　[Sun RPC Configuration] ページの次の検出オプションを選択またはクリアできます。

- **[Detect fragmented RPC records]**
- **[Detect multiple records in one packet]**
- **[Detect fragmented record sums which exceed one packet]**
- **[Detect single fragment records which exceed the size of one packet]**

ステップ 7　ポリシーを保存するか、編集を続行するか、変更内容を破棄するか、ベース ポリシーのデフォルト設定に戻すか、またはシステム キャッシュの変更を反映せずに終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

Session Initiation Protocol のデコード

ライセンス：Protection

Session Initiation Protocol（SIP）は、インターネット テレフォニー、マルチメディア会議、インスタント メッセージング、オンライン ゲーム、ファイル転送などのクライアント アプリケーションの 1 人以上のユーザに対し、1 つ以上のセッションのコール設定、変更、およびティアダウンを提供します。各 SIP 要求の *method* フィールドは要求の目的を示し、Request-URI により要求の送信先が指定されます。各 SIP 応答のステータス コードは、要求されたアクションの結果を示します。

SIP を使用してコールがセットアップされた後、後続の音声およびビデオによる通信は Real-time Transport Protocol（RTP）により処理されます。セッションのこの部分は、コール チャネル、データ チャネル、または音声/ビデオ データ チャネルと呼ばれることがあります。RTP は、データチャネル パラメータ ネゴシエーション、セッション通知、およびセッションへの招待のための SIP メッセージ ボディ内で Session Description Protocol（SDP）を使用します。

SIP プリプロセッサは次の処理を実行します。

- SIP 2.0 トラフィックのデコードおよび分析
- SDP データが存在する場合はこのデータを含む SIP 見出しとメッセージ ボディを抽出し、抽出したデータを今後のインスペクションのためにルール エンジンに受け渡す
- 条件（SIP パケットにおける異常または既知の脆弱性、順序が正しくないコール シーケンス、または無効なコール シーケンス）が検出され、対応するプリプロセッサ ルールが有効である場合にイベントを生成する
- コール チャネルを無視する（オプション）

プリプロセッサは、SIP メッセージ ボディに組み込まれている SDP メッセージに示されているポートに基づいて RTP チャネルを識別しますが、RTP プロトコル インスペクションを実行しません。

SIP プリプロセッサを使用するときは、次の点に注意してください。

- UDP は通常、SIP でサポートされるメディア セッションを伝送します。UDP ストリームの前処理により、SIP プリプロセッサに対し SIP セッション トラッキングが提供されます。
- SIP ルール キーワードにより、SIP パケット 見出しまたはメッセージ ボディを指し示し、検出対象を特定の SIP メソッドまたはステータス コードのパケットに限定できます。詳細については、SIP キーワード（36-67 ページ）を参照してください。
- 有効である場合、関連するルール（ジェネレータ ID（GID）140）も有効にしていないと、抽出したデータをルール エンジンに送信するまで、プリプロセッサはイベントを生成しません。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

詳細については、次の項を参照してください。

- SIP プリプロセッサ オプションの選択（27-51 ページ）
- SIP プリプロセッサの設定（27-53 ページ）
- 追加の SIP プリプロセッサ ルールの有効化（27-54 ページ）

SIP プリプロセッサ オプションの選択

ライセンス：Protection

変更できる SIP プリプロセッサ オプションについて以下で説明します。

[Maximum Request URI Length]、[Maximum Call ID Length]、[Maximum Request Name Length]、[Maximum From Length]、[Maximum To Length]、[Maximum Via Length]、[Maximum Contact Length]、および [Maximum Content Length] オプションでは、1 ～ 65535 バイト、または 0 バイトを指定できます。0 を指定すると、関連するルールが有効であるかかどうかに関係なく、このオプションのイベント生成が無効になります。

次の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

SIP トラフィックを検査するポートを指定します。0 ～ 65535 の整数を指定できます。複数のポート番号を指定する場合は、カンマで区切ります。

Methods to Check

検出する SIP メソッドを指定します。次に示す現在定義されている SIP メソッドを指定できます。

```
ack, benotify, bye, cancel, do, info, invite, join, message,
notify, options, prack, publish, quath, refer, register,
service, sprack, subscribe, unsubscribe, update
```

メソッドでは大文字と小文字が区別されません。メソッド名には英字、数字、下線文字を使用できます。その他の特殊文字は使用できません。複数のメソッドを指定する場合は、カンマで区切ります。

新しい SIP メソッドが今後定義される可能性があるため、設定には、現在定義されていない英字文字列を含めることができます。システムでは最大 32 個のメソッド（現在定義されている 21 個のメソッドと追加の 11 個のメソッド）がサポートされます。システムは、設定される未定義のメソッドをすべて無視します。

合計 32 個のメソッドには、このオプションに指定するメソッドの他に、侵入ルールで `sip_method` キーワードを使用して指定するメソッドも含まれます。詳細については、「sip_method（36-68 ページ）」を参照してください。

Maximum Dialogs within a Session

ストリーム セッション内で許容されるダイアログの最大数を指定します。この数より多くのダイアログが作成されると、ダイアログの数が、指定されている最大数以下になるまで、最も古いダイアログから順に削除されます。また、ルール 140:27 が有効である場合にもイベントがトリガーとして使用されます。

1 ～ 4194303 の整数を指定できます。

Maximum Request URI Length

[Request-URI] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:3 が有効である場合、URI がこれよりも長いとイベントがトリガーとして使用されます。要求の [URI] フィールドは、要求の宛先のパスまたはページを示します。

Maximum Call ID Length

要求または応答の [Call-ID] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:5 が有効である場合、Call-ID がこれよりも長いとイベントがトリガーとして使用されます。[Call-ID] フィールドは、要求および応答内で SIP セッションを一意に識別します。

Maximum Request Name Length

要求名で許容される最大バイト数を指定します。要求名は、CSeq トランザクション ID に指定されるメソッドの名前です。ルール 140:7 が有効である場合、要求名がこれよりも長いとイベントがとして使用されます。

Maximum From Length

要求または応答の [From] 見出し フィールドで許容される最大バイト数を指定します。ルール 140:9 が有効である場合、From がこれよりも長いとイベントがトリガーとして使用されます。[From] フィールドは、メッセージの発信側を識別します。

Maximum To Length

要求または応答の [To] 見出し フィールドで許容される最大バイト数を指定します。ルール 140:11 が有効である場合、To がこれよりも長いとイベントがトリガーとして使用されます。[To] フィールドは、メッセージの受信側を識別します。

Maximum Via Length

要求または応答の [Via] 見出し フィールドで許容される最大バイト数を指定します。ルール 140:13 が有効である場合、Via がこれよりも長いとイベントがトリガーとして使用されます。[Via] フィールドには要求がたどるパスが示され、応答の場合は受信者情報が示されます。

Maximum Contact Length

要求または応答の [Contact] 見出し フィールドで許容される最大バイト数を指定します。ルール 140:15 が有効である場合、Contact がこれよりも長いとイベントがトリガーとして使用されます。[Contact] フィールドには、後続のメッセージについての連絡先を指定する URI が示されます。

Maximum Content Length

要求または応答のメッセージ ボディのコンテンツで許容される最大バイト数を指定します。ルール 140:16 が有効である場合、コンテンツがこれよりも長いとイベントがトリガーとして使用されます。

Ignore Audio/Video Data Channel

データ チャネル トラフィックのインスペクションを有効または無効にします。このオプションを有効にすると、プリプロセッサはその他の非データ チャネル SIP トラフィックのインスペクションを続行することに注意してください。

SIP プリプロセッサの設定

ライセンス： Protection

SIP プリプロセッサを設定するには、次の手順に従います。

SIP プリプロセッサの設定方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Application Layer Preprocessors] の下の [SIP Configuration] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効である場合は、[Enabled] をクリックし、次に [Edit] をクリックします。

[SIP Configuration] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　SIP プリプロセッサ オプションの選択（27-51 ページ）で説明するオプションを変更できます。

ステップ 6　ポリシーを保存するか、編集を続行するか、変更内容を破棄するか、ベース ポリシーのデフォルト設定に戻すか、またはシステム キャッシュの変更を反映せずに終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

追加の SIP プリプロセッサ ルールの有効化

ライセンス：Protection

次の表に示す SIP プリプロセッサ ルールは、特定の設定オプションに関連付けられていません。その他の SIP プリプロセッサ ルールと同様に、これらのルールによってイベントを生成する場合は、これらのルールを有効にする必要があります。ルールの有効化については、ルール状態の設定（32-22 ページ）を参照してください。

表 27-10　追加の SIP プリプロセッサ ルール

プリプロセッサ ルール GID：SID	説明
140:1	プリプロセッサがモニタしている SIP セッションの数が、システムで許容される最大数である場合に、イベントが生成されます。
140:2	SIP 要求で [Request_URI] 必須フィールドが空である場合に、イベントが生成されます。
140:4	SIP 要求または応答で [Call-ID] ヘッダー フィールドが空である場合に、イベントが生成されます。
140:6	SIP 要求または応答で [CSeq] フィールドのシーケンス番号値が、231 未満の 32 ビット符号なし整数ではない場合に、イベントが生成されます。
140:8	SIP 要求または応答で [From] 見出し フィールドが空である場合に、イベントが生成されます。
140:10	SIP 要求または応答で [To] 見出し フィールドが空である場合に、イベントが生成されます。
140:12	SIP 要求または応答で [Via] 見出し フィールドが空である場合に、イベントが生成されます。
140:14	SIP 要求または応答で [Contact] 必須見出し フィールドが空である場合に、イベントが生成されます。

表 27-10　追加の SIP プリプロセッサ ルール（続き）

プリプロセッサ ルール GID:SID	説明
140:17	UDP トラフィック内の 1 つの SIP 要求または応答パケットに複数のメッセージが含まれている場合に、イベントが生成されます。SIP の旧バージョンでは複数メッセージがサポートされていますが、SIP 2.0 ではパケットあたり 1 メッセージだけがサポートされていることに注意してください。
140:18	UDP トラフィック内の SIP 要求または応答のメッセージ ボディの実際の長さが、SIP 要求または応答の [Content-Length] ヘッダー フィールドに指定されている値と一致しない場合に、イベントが生成されます。
140:19	プリプロセッサが SIP 応答の [CSeq] フィールドのメソッド名を認識しない場合に、イベントが生成されます。
140:20	SIP サーバが、認証済み招待メッセージに対してチャレンジを送信しない場合に、イベントが生成されます。これは InviteReplay 請求攻撃の場合に発生することに注意してください。
140:21	コール セットアップの前にセッション情報が変更されると、イベントが生成されます。これは FakeBusy 請求攻撃の場合に発生することに注意してください。
140:22	応答ステータス コードが 3 桁の数値ではない場合に、イベントが生成されます。
140:23	[Content-Type] ヘッダー フィールドにコンテンツ タイプが指定されておらず、メッセージ ボディにデータが含まれている場合に、イベントが生成されます。
140:24	SIP バージョンが 1、1.1、または 2.0 のいずれでもない場合に、イベントが生成されます。
140:25	SIP 要求で、[CSeq] 見出しで指定されたメソッドとメソッド フィールドが一致しない場合に、イベントが生成されます。
140:26	プリプロセッサが SIP 要求のメソッド フィールドに指定されたメソッドを認識しない場合に、イベントが生成されます。

GTP コマンド チャネルの設定

ライセンス：Protection

General Packet Radio Service（GPRS）Tunneling Protocol（GTP）により、GTP コア ネットワークを介した通信が実現します。GTP プリプロセッサは、GTP トラフィックの異常を検出し、コマンド チャネル シグナリング メッセージをインスペクションのためにルール エンジンに転送します。GTP コマンド チャネル トラフィックでエクスプロイトがあるかどうかを検査するには、`gtp_version`、`gtp_type`、および `gtp_info` ルール キーワードを使用します。

1 つの構成オプションで、プリプロセッサが GTP コマンド チャネル メッセージを検査するポートのデフォルト設定を変更できます。

イベントを生成するには、次の表に示す GTP プリプロセッサ ルールを有効にする必要があります。ルールの有効化については、ルール状態の設定（32-22 ページ）を参照してください。

表 27-11　GTP プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
143:1	プリプロセッサが無効なメッセージの長さを検出すると、イベントが生成されます。
143:2	プリプロセッサが無効な情報要素の長さを検出すると、イベントが生成されます。
143:3	プリプロセッサが誤った順序の情報要素を検出すると、イベントが生成されます。

GTP プリプロセッサが GTP コマンド メッセージをモニタするポートを変更するには、次の手順を使用します。

GTP コマンド チャネルを設定するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Application Layer Preprocessors] の下の [GTP Command Channel Configuration] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効である場合は、[Enabled] をクリックし、次に [Edit] をクリックします。

[GTP Command Channel Configuration] ページが表示されます。

ステップ 5　オプションで、プリプロセッサが GTP コマンド メッセージを検査するポートを変更します。0 ～ 65535 の整数を指定できます。複数のポートを指定する場合はカンマで区切ります。

ステップ 6　ポリシーを保存するか、編集を続行するか、変更内容を破棄するか、ベース ポリシーのデフォルト設定に戻すか、またはシステム キャッシュの変更を反映せずに終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

IMAP トラフィックのデコード

ライセンス：Protection

Internet Message Application Protocol（IMAP）は、リモート IMAP サーバから電子メールを取得するときに使用されます。IMAP プリプロセッサはサーバ/クライアント IMAP4 トラフィックを検査し、関連するプリプロセッサ ルールが有効である場合は異常なトラフィックがあるとイベントを生成します。プリプロセッサは、クライアント/サーバ IMAP4 トラフィックの電子メール添付ファイルを抽出してデコードし、添付ファイル データをルール エンジンに送信することもできます。添付ファイル データを指し示すには、侵入ルールで `file_data` キーワードを使用します。詳細については、「特定のペイロード タイプを指し示す（36-105 ページ）」を参照してください。

抽出とデコードでは、複数の添付ファイル（存在する場合）や、複数パケットにまたがる大きな添付ファイルなども処理されます。

IMAP プリプロセッサ ルールによりイベントを生成するには、それらのルールを有効にする必要があります。IMAP プリプロセッサ ルールのジェネレータ ID（GID）は 141 です。詳細については、ルール状態の設定（32-22 ページ）を参照してください。

詳細については、次の項を参照してください。

- IMAP プリプロセッサ オプションの選択（27-57 ページ）
- IMAP プリプロセッサの設定（27-58 ページ）
- 追加の IMAP プリプロセッサ ルールの有効化（27-60 ページ）

IMAP プリプロセッサ オプションの選択

ライセンス：Protection

変更できる IMAP プリプロセッサ オプションを以下で説明します。

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル（存在する場合）および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 Decoding Depth]、[7-Bit/8-Bit/Binary Decoding Depth]、[Quoted-Printable Decoding Depth]、または [Unix-to-Unix Decoding Depth] オプションの値が次の点で異なる場合に最も大きな値が使用されることにも注意してください。

- デフォルトのネットワーク分析ポリシー
- 同じアクセス コントロール ポリシーのネットワーク分析ルールによって呼び出される他のカスタム ネットワーク分析ポリシー

詳細については、アクセス コントロールのデフォルト ネットワーク分析ポリシーの設定（25-4 ページ）および前処理するトラフィックのネットワーク分析ルールによる指定（25-5 ページ）を参照してください。

注意　[Base64 Decoding Depth]、[7-Bit/8-Bit/Binary Decoding Depth]、[Quoted-Printable Decoding Depth]、または [Unix-to-Unix Decoding Depth] の値を変更すると、Snort プロセスが再開され、構成変更を適用する際、一時的にトラフィック検査が中断されます。この検査中にシステムがトラフィックをドロップするか、検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、「Snort の再開によるトラフィックへの影響（1-9 ページ）」を参照してください。

次の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

IMAP トラフィックを検査するポートを指定します。0 ～ 65535 の整数を指定できます。複数のポート番号を指定する場合は、カンマで区切ります。

Base64 Decoding Depth

各 Base 64 エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、すべての Base64 データをデコードする場合は 0 を指定します。Base64 データを無視するには、-1 を指定します。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

Base64 デコードが有効である場合、ルール 141:4 を有効にして、デコードの失敗時にイベントを生成することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。

7-Bit/8-Bit/Binary Decoding Depth

デコードを必要としない各 MIME 電子メール添付ファイルから抽出するデータの最大バイト数を指定します。これらの添付ファイル タイプには、7 ビット、8 ビット、バイナリー、およびさまざまなマルチパート コンテンツ タイプ（プレーンテキスト、jpeg イメージ、mp3 ファイルなど）があります。1 ～ 65535 バイトを指定するか、または、パケットのすべてのデータを抽出する場合は 0 を指定します。非デコード データを無視するには、-1 を指定します。

Quoted-Printable Decoding Depth

各 quoted-printable（QP）エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、パケットのすべての QP エンコード データをデコードする場合は 0 を指定します。QP エンコード データを無視するには、-1 を指定します。

quoted-printable デコードが有効な場合、ルール 141:6 を有効にして、デコードの失敗時にイベントを生成することができます。デコードが失敗するのは、エンコードが誤っている場合やデータが破損している場合などです。

Unix-to-Unix Decoding Depth

各 Unix-to-Unix エンコード（UU エンコード）電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、パケットのすべての UU エンコード データをデコードする場合は 0 を指定します。UU エンコード データを無視するには、-1 を指定します。

Unix-to-Unix デコードが有効である場合、ルール 141:7 を有効にして、デコードの失敗時にイベントを生成することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。

IMAP プリプロセッサの設定

ライセンス： Protection

IMAP プリプロセッサを設定するには、次の手順に従います。IMAP プリプロセッサ設定オプションの詳細については、IMAP プリプロセッサ オプションの選択（27-57 ページ）を参照してください。

IMAP プリプロセッサの設定方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Application Layer Preprocessors] の下の [IMAP Configuration] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効である場合は、[Enabled] をクリックし、次に [Edit] をクリックします。

[IMAP Configuration] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　IMAP トラフィックをデコードする必要があるポートを指定します。複数のポート番号を指定する場合は、カンマで区切ります。

ステップ 6　次に示す電子メール添付ファイル タイプの任意の組み合わせから抽出してデコードするデータの最大バイト数を指定します。

- **Base64 Decoding Depth**
- **7-Bit/8-Bit/Binary Decoding Depth**（プレーン テキスト、jpeg イメージ、mp3 ファイルなどの各種マルチパート コンテンツ タイプを含む）
- **Quoted-Printable Decoding Depth**
- **Unix-to-Unix Decoding Depth**

タイプごとに 1 ～ 65535 バイトを指定するか、または、パケットのすべてのデータを抽出し、必要に応じてデコードする場合は 0 を指定します。添付ファイル タイプのデータを無視するには、-1 を指定します。

添付ファイル データを検査するには、侵入ルールで `file_data` キーワードを使用できます。詳細については、「特定のペイロード タイプを指し示す（36-105 ページ）」を参照してください。

ステップ 7　ポリシーを保存するか、編集を続行するか、変更内容を破棄するか、ベース ポリシーのデフォルト設定に戻すか、またはシステム キャッシュの変更を反映せずに終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

追加の IMAP プリプロセッサ ルールの有効化

ライセンス：Protection

次の表に示す IMAP プリプロセッサ ルールは、特定の設定オプションに関連付けられていません。その他の IMAP プリプロセッサ ルールと同様に、これらのルールによってイベントを生成する場合は、これらのルールを有効にする必要があります。ルールの有効化については、ルール状態の設定（32-22 ページ）を参照してください。

表 27-12　追加の IMAP プリプロセッサ ルール

プリプロセッサ ルール GID：SID	説明
141:1	プリプロセッサが RFC 3501 に定義されていないクライアント コマンドを検出すると、イベントが生成されます。
141:2	プリプロセッサが RFC 3501 に定義されていないサーバ応答を検出すると、イベントが生成されます。
141:3	プリプロセッサが使用しているメモリの量が、システムでの最大許容量に達している場合に、イベントが生成されます。この時点で、プリプロセッサはメモリが使用可能になるまでデコードを停止します。

POP トラフィックのデコード

ライセンス：Protection

Post Office Protocol（POP）は、リモート POP メール サーバから電子メールを取得するときに使用されます。POP プリプロセッサはサーバ/クライアント POP3 トラフィックを検査し、関連するプリプロセッサ ルールが有効である場合は異常なトラフィックがあるとイベントを生成します。プリプロセッサは、クライアント/サーバ POP3 トラフィックで電子メール添付ファイルを抽出してデコードし、添付ファイル データをルール エンジンに送信することもできます。添付ファイル データを指し示すには、侵入ルールで `file_data` キーワードを使用します。詳細については、「特定のペイロード タイプを指し示す（36-105 ページ）」を参照してください。

抽出とデコードでは、複数の添付ファイル（存在する場合）や、複数パケットにまたがる大きな添付ファイルなども処理されます。

POP プリプロセッサ ルールによりイベントを生成するには、それらのルールを有効にする必要があります。POP プリプロセッサ ルールのジェネレータ ID（GID）は 142 です。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

詳細については、次の項を参照してください。

- POP プリプロセッサ オプションの選択（27-60 ページ）
- POP プリプロセッサの設定（27-62 ページ）
- 追加の POP プリプロセッサ ルールの有効化（27-63 ページ）

POP プリプロセッサ オプションの選択

ライセンス：Protection

変更できる POP プリプロセッサ オプションを以下で説明します。

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル（存在する場合）および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 Decoding Depth]、[7-Bit/8-Bit/Binary Decoding Depth]、[Quoted-Printable Decoding Depth]、または [Unix-to-Unix Decoding Depth] の各オプションの値が、アクセス コントロール ポリシーに関連付けられている侵入ポリシーと、アクセス コントロール ルールに関連付けられている侵入ポリシーの間で異なる場合は、最も大きな値が使用されることに注意してください。

注意

[Base64 Decoding Depth]、[7-Bit/8-Bit/Binary Decoding Depth]、[Quoted-Printable Decoding Depth]、または [Unix-to-Unix Decoding Depth] の値を変更すると、Snort プロセスが再開され、構成変更を適用する際、一時的にトラフィック検査が中断されます。この検査中にシステムがトラフィックをドロップするか、検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、「Snort の再開によるトラフィックへの影響（1-9 ページ）」を参照してください。

次の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

POP トラフィックを検査するポートを指定します。0 ～ 65535 の整数を指定できます。複数のポート番号を指定する場合は、カンマで区切ります。

Base64 Decoding Depth

各 Base 64 エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、すべての Base64 データをデコードする場合は 0 を指定します。Base64 データを無視するには、-1 を指定します。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

Base64 デコードが有効である場合、ルール 142:4 を有効にして、デコードの失敗時にイベントを生成することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

7-Bit/8-Bit/Binary Decoding Depth

デコードを必要としない各 MIME 電子メール添付ファイルから抽出するデータの最大バイト数を指定します。これらの添付ファイル タイプには、7 ビット、8 ビット、バイナリー、およびさまざまなマルチパート コンテンツ タイプ（プレーンテキスト、jpeg イメージ、mp3 ファイルなど）があります。1 ～ 65535 バイトを指定するか、または、パケットのすべてのデータを抽出する場合は 0 を指定します。非デコード データを無視するには、-1 を指定します。

Quoted-Printable Decoding Depth

各 quoted-printable（QP）エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、パケットのすべての QP エンコード データをデコードする場合は 0 を指定します。QP エンコード データを無視するには、-1 を指定します。

quoted-printable デコードが有効な場合、ルール 142:6 を有効にして、デコードの失敗時にイベントを生成することができます。デコードが失敗するのは、エンコードが誤っている場合やデータが破損している場合などです。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Unix-to-Unix Decoding Depth

各 Unix-to-Unix エンコード（UU エンコード）電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、パケットのすべての UU エンコード データをデコードする場合は 0 を指定します。UU エンコード データを無視するには、-1 を指定します。

Unix-to-Unix デコードが有効である場合、ルール 142:7 を有効にして、デコードの失敗時にイベントを生成することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

POP プリプロセッサの設定

ライセンス： Protection

POP プリプロセッサを設定するには、次の手順に従います。POP プリプロセッサ設定オプションの詳細については、POP プリプロセッサ オプションの選択（27-60 ページ）を参照してください。

POP プリプロセッサの設定方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Application Layer Preprocessors] の下の [POP Configuration] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効である場合は、[Enabled] をクリックし、次に [Edit] をクリックします。

[POP Configuration] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　IMAP トラフィックをデコードする必要があるポートを指定します。複数のポート番号を指定する場合は、カンマで区切ります。

ステップ 6　次に示す電子メール添付ファイル タイプの任意の組み合わせから抽出してデコードするデータの最大バイト数を指定します。

- **Base64 Decoding Depth**
- **7-Bit/8-Bit/Binary Decoding Depth**（プレーン テキスト、jpeg イメージ、mp3 ファイルなどの各種マルチパート コンテンツ タイプを含む）

- **Quoted-Printable Decoding Depth**
- **Unix-to-Unix Decoding Depth**

タイプごとに 1 ～ 65535 バイトを指定するか、または、パケットのすべてのデータを抽出し、必要に応じてデコードする場合は 0 を指定します。添付ファイル タイプのデータを無視するには、-1 を指定します。

添付ファイル データを検査するには、侵入ルールで `file_data` キーワードを使用できます。詳細については、「特定のペイロード タイプを指し示す（36-105 ページ）」を参照してください。

ステップ 7　ポリシーを保存するか、編集を続行するか、変更内容を破棄するか、ベース ポリシーのデフォルト設定に戻すか、またはシステム キャッシュの変更を反映せずに終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

追加の POP プリプロセッサ ルールの有効化

ライセンス：Protection

次の表に示す POP プリプロセッサ ルールは、特定の設定オプションに関連付けられていません。その他の POP プリプロセッサ ルールと同様に、これらのルールによってイベントを生成する場合は、これらのルールを有効にする必要があります。ルールの有効化については、ルール状態の設定（32-22 ページ）を参照してください。

表 27-13　追加の POP プリプロセッサ ルール

プリプロセッサ ルール GID：SID	説明
142:1	プリプロセッサが RFC 1939 に定義されていないクライアント コマンドを検出すると、イベントが生成されます。
142:2	プリプロセッサが RFC 1939 に定義されていないサーバ応答を検出すると、イベントが生成されます。
142:3	プリプロセッサが使用しているメモリの量が、システムでの最大許容量に達している場合に、イベントが生成されます。この時点で、プリプロセッサはメモリが使用可能になるまでデコードを停止します。

SMTP トラフィックのデコード

ライセンス：Protection

SMTP プリプロセッサはルール エンジンに対し、SMTP コマンドを正規化するように指示します。このプリプロセッサは、クライアント/サーバ トラフィックで電子メール添付ファイルを抽出してデコードします。またソフトウェアのバージョンによっては、SMTP トラフィックによりトリガーとして使用された侵入イベントを表示するときにコンテキストを提供するため、電子メール ファイル名、アドレス、およびヘッダー データを抽出します。

SMTP プリプロセッサを使用するときは、次の点に注意してください。

- ジェネレータ ID（GID）124 の SMTP プリプロセッサ ルールを使用してイベントを生成する場合は、これらのルールを有効にする必要があります。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

詳細については、次の項を参照してください。

- SMTP デコードについて（27-64 ページ）
- SMTP デコードの設定（27-68 ページ）
- SMTP 最大デコード メモリ アラートの有効化（27-71 ページ）

SMTP デコードについて

ライセンス：Protection

正規化を有効または無効にし、SMTP デコーダが検出する異常トラフィックのタイプを制御するオプションを設定できます。

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル（存在する場合）および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 Decoding Depth]、[7-Bit/8-Bit/Binary Decoding Depth]、[Quoted-Printable Decoding Depth]、または [Unix-to-Unix Decoding Depth] の各オプションの値が、アクセス コントロール ポリシーに関連付けられている侵入ポリシーと、アクセス コントロール ルールに関連付けられている侵入ポリシーの間で異なる場合は、最も大きな値が使用されることに注意してください。

注意 [Base64 Decoding Depth]、[7-Bit/8-Bit/Binary Decoding Depth]、[Quoted-Printable Decoding Depth]、または [Unix-to-Unix Decoding Depth] の値を変更すると、Snort プロセスが再開され、構成変更を適用する際、一時的にトラフィック検査が中断されます。この検査中にシステムがトラフィックをドロップするか、検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、「Snort の再開によるトラフィックへの影響（1-9 ページ）」を参照してください。

次の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

SMTP トラフィックを正規化するポートを指定します。0 ～ 65535 の整数を指定できます。複数のポートを指定する場合は、カンマで区切ります。

Stateful Inspection

選択されている場合、SMTP デコーダは状態を保存し、各パケットのセッション コンテキストを提供し、再構成されたセッションだけを検査します。選択されていない場合、セッション コンテキストなしで個々のパケットを分析します。

Normalize

[All] に設定すると、すべてのコマンドが正規化されます。コマンドの後に複数のスペース文字があるかどうかを確認します。

[None] に設定すると、コマンドは正規化されません。

[Cmds] に設定すると、[Custom Commands] にリストされているコマンドが正規化されます。

Custom Commands

[Normalize] が [Cmds] に設定されている場合に、リストされているコマンドが正規化されます。

正規化する必要があるコマンドをテキスト ボックスに指定します。コマンドの後に複数のスペース文字があるかどうかを確認します。

スペース文字（ASCII 0x20）とタブ文字（ASCII 0x09）は、正規化の ためにスペース文字としてカウントされます。

Ignore Data

メール データを処理せず、MIME メール 見出し データだけを処理します。

Ignore TLS Data

Transport Layer Security プロトコルで暗号化されたデータを処理しません。

No Alerts

関連するプリプロセッサ ルールが有効である場合に、侵入イベントを無効にします。

Detect Unknown Commands

SMTP トラフィックで不明なコマンドを検出します。

このオプションのイベントを生成するには、ルール124:5 および 124:6 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Max Command Line Len

SMTP コマンドラインがこの値より長い場合にそのことを検出します。コマンドラインの長さを検出しない場合は、0 を指定します。

RFC 2821（Network Working Group による Simple Mail Transfer Protocol 仕様）では、コマンドラインの最大長として 512 が推奨されています。

このオプションのイベントを生成するには、ルール 124:1 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Max Header Line Len

SMTP データ 見出し行がこの値より長い場合にそのことを検出します。データ 見出し行の長さを検出しない場合は、0 を指定します。

このオプションのイベントを生成するには、ルール124:2 および 124:7 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Max Response Line Len

SMTP 応答行がこの値より長い場合にそのことを検出します。応答行の長さを検出しない場合は、0 を指定します。

RFC 2821 では、応答行の最大長として 512 が推奨されています。

このオプションのイベントを生成するには、ルール 124:3 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Alt Max Command Line Len

指定のコマンドの SMTP コマンドラインがこの値より長い場合にそのことを検出します。指定したコマンドのコマンドライン長を検出しない場合は、0 を指定します。多数のコマンドに対して、さまざまなデフォルト ライン長が設定されています。

この設定は、指定されたコマンドの [Max Command Line Len] の設定をオーバーライドします。

このオプションのイベントを生成するには、ルール 124:3 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Invalid Commands

これらのコマンドがクライアント側から送信された場合にそのことを検出します。

このオプションのイベントを生成するには、ルール124:5 および 124:6 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Valid Commands

このリストのコマンドを許可します。

このリストが空の場合でも、プリプロセッサにより許可される有効なコマンドは、ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SIZE SOML STARTTLS TICK TIME TURN TURNME VERB VRFY XADR XAUTH XCIR XEXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE XSTA XTRN XUSR です。

注 RCPT TO および MAIL FROM は SMTP コマンドです。プリプロセッサ設定では、コマンド名 RCPT と MAIL がそれぞれ使用されます。プリプロセッサはコード内で RCPT および MAIL を正しいコマンド名にマッピングします。

このオプションのイベントを生成するには、ルール 124:4 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Data Commands

RFC 5321 に基づく SMTP DATA コマンドによるデータの送信と同じ方法でデータ送信を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

Binary Data Commands

RFC 3030 に基づく BDATA コマンドによるデータの送信と類似の方法でデータ送信を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

Authentication Commands

クライアントおよびサーバ間で認証交換を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

Detect xlink2state

X-Link2State Microsoft Exchange バッファ データ オーバーフロー攻撃の一部であるパケットを検出します。インライン展開では、システムはこれらのパケットをドロップすることもできます。

このオプションのイベントを生成するには、ルール 124:8 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Base64 Decoding Depth

[Ignore Data] が無効である場合、各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、すべての Base64 データをデコードする場合は 0 を指定します。Base64 データを無視するには、-1 を指定します。[Ignore Data] が選択されている場合、プリプロセッサはデータをデコードしません。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

Base64 デコードが有効である場合、ルール 124:10 を有効にして、デコードの失敗時にイベントを生成することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

このオプションは、廃止されたオプション [Enable MIME Decoding] および [Maximum MIME Decoding Depth] の代わりに使用されます。廃止されたこれらのオプションは、既存の侵入ポリシーでは後方互換性を維持する目的で引き続きサポートされています。

7-Bit/8-Bit/Binary Decoding Depth

[Ignore Data] が無効である場合、デコードを必要としない各 MIME 電子メール添付ファイルから抽出する最大バイト数を指定します。これらの添付ファイル タイプには、7 ビット、8 ビット、バイナリー、およびさまざまなマルチパート コンテンツ タイプ（プレーンテキスト、jpeg イメージ、mp3 ファイルなど）があります。1 ～ 65535 バイトを指定するか、または、パケットのすべてのデータを抽出する場合は 0 を指定します。非デコード データを無視するには、-1 を指定します。[Ignore Data] が選択されている場合、プリプロセッサはデータを抽出しません。

Quoted-Printable Decoding Depth

[Ignore Data] が無効である場合、各 quoted-printable（QP）エンコード MIME 電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。

1 ～ 65535 バイトを指定するか、または、パケットのすべての QP エンコード データをデコードする場合は 0 を指定します。QP エンコード データを無視するには、-1 を指定します。[Ignore Data] が選択されている場合、プリプロセッサはデータをデコードしません。

quoted-printable デコードが有効な場合、ルール 124:11 を有効にして、デコードの失敗時にイベントを生成することができます。デコードが失敗するのは、エンコードが誤っている場合やデータが破損している場合などです。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Unix-to-Unix Decoding Depth

[Ignore Data] が無効である場合、各 Unix-to-Unix エンコード（UU エンコード）電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、パケットのすべての UU エンコード データをデコードする場合は 0 を指定します。UU エンコード データを無視するには、-1 を指定します。[Ignore Data] が選択されている場合、プリプロセッサはデータをデコードしません。

Unix-to-Unix デコードが有効である場合、ルール 124:13 を有効にして、デコードの失敗時にイベントを生成することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Log MIME Attachment Names

MIME Content-Disposition ヘッダーからの MIME 添付ファイル名の抽出を有効にし、セッションで生成されるすべての侵入イベントをこのファイル名に関連付けます。複数ファイル名がサポートされています。

このオプションが有効である場合、侵入イベントのテーブル ビューの [Email Attachment] 列に、イベントに関連付けられているファイル名が表示されます。詳細については、「侵入イベントについて（41-11 ページ）」を参照してください。

Log To Addresses

SMTP RCPT TO コマンドからの受信者の電子メール アドレスの抽出を有効にし、セッションで生成されるすべての侵入イベントにこの受信者アドレスに関連付けます。複数の受信者がサポートされます。

このオプションが有効である場合、侵入イベントのテーブル ビューの [Email Recipient] 列に、イベントに関連付けられている受信者が表示されます。詳細については、「侵入イベントについて（41-11 ページ）」を参照してください。

Log From Addresses

SMTP MAIL FROM コマンドからの送信者の電子メール アドレスの抽出を有効にし、セッションで生成されるすべての侵入イベントにこの送信者アドレスを関連付けます。複数の送信者アドレスがサポートされます。

このオプションが有効である場合、侵入イベントのテーブル ビューの [Email Sender] 列に、イベントに関連付けられている送信者が表示されます。詳細については、「侵入イベントについて（41-11 ページ）」を参照してください。

Log Headers

電子メール 見出しの抽出を有効にします。抽出されるバイト数は、[Header Log Depth] に指定されている値によって決まります。

キーワード `content` または `protected_content` を使用して、電子メール ヘッダー データをパターンとして使用する侵入ルールを作成できます。侵入イベント パケット ビューに、抽出された電子メール 見出しが表示されます。詳細については、コンテンツ一致の制約（36-19 ページ）およびパケット ビューの使用（41-23 ページ）を参照してください。

Header Log Depth

[Log Headers] が有効である場合、抽出する見出しのバイト数を指定します。0 ～ 20480 バイトを指定できます。値 0 を指定すると、[Log Headers] が無効になります。

SMTP デコードの設定

ライセンス： Protection

侵入ポリシーの [SMTP Configuration]ページを使用して、SMTP 正規化を設定できます。SMTP プリプロセッサ設定オプションの詳細については、SMTP デコードについて（27-64 ページ）を参照してください。

SMTP デコード オプションの設定方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Application Layer Preprocessors] の下の [SMTP Configuration] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効である場合は、[Enabled] をクリックし、次に [Edit] をクリックします。

[SMTP Configuration] ページが表示されます。次の図は、Defense Center パケット ビューを示します。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　SMTP トラフィックをデコードする必要があるポートを、カンマで区切って指定します。

ステップ 6　SMTP パケットを含む再構成された TCP ストリームを調べるには、[Stateful Inspection] を選択します。再構成されていない SMTP パケットだけを検査するには、[Stateful Inspection] をクリアします。

ステップ 7　正規化オプションを設定します。

- すべてのコマンドを正規化するには、[All] を選択します。
- [Custom Commands] に指定されているコマンドだけを正規化するには、[Cmds] を選択して、正規化するコマンドを指定します。複数のコマンドはスペースで区切ります。
- コマンドを正規化しない場合は、[None] を選択します。
- MIME メール 見出し データ以外のメール データを無視するには、[Ignore Data] をオンにします。
- Transport Security Layer プロトコルで暗号化されたデータを無視するには、[Ignore TLS Data] をオンにします。
- 関連するプリプロセッサ ルールが有効である場合にイベント生成を無効にするには、[No Alerts] をオンにします。
- SMTP データで不明なコマンドを検出するには、[Detect Unknown Commands] を選択します。

ステップ 8　[Max Command Line Len] フィールドに、コマンドラインの最大長を指定します。

ステップ 9　[Max Header Line Len] フィールドに、データ 見出し行の最大長を指定します。

ステップ 10　[Max Response Line Len] フィールドに、応答行の最大長を指定します。

注　RCPT TO および MAIL FROM は SMTP コマンドです。プリプロセッサ設定では、コマンド名 RCPT と MAIL がそれぞれ使用されます。プリプロセッサはコード内で RCPT および MAIL を正しいコマンド名にマッピングします。

ステップ 11　必要に応じて、[Alt Max Command Line Len] の横にある [Add] をクリックして、代替最大コマンドライン長を指定するコマンドを追加します。続いてライン長を指定し、このライン長を適用するコマンドをスペースで区切って指定します。

ステップ 12　[Invalid Commands] フィールドに、無効として扱う検出対象コマンドを指定します。複数のコマンドはスペースで区切ります。

ステップ 13　[Valid Commands] フィールドに、有効として扱うコマンドを指定します。複数のコマンドはスペースで区切ります。

注　[Valid Commands] リストが空の場合でも、プリプロセッサにより有効なコマンドとして許可されるコマンドは、ATRN、AUTH、BDAT、DATA、DEBUG、EHLO、EMAL、ESAM、ESND、ESOM、ETRN、EVFY、EXPN、HELO、HELP、IDENT、MAIL、NOOP、QUIT、RCPT、RSET、SAML、SOML、SEND、ONEX、QUEU、STARTTLS、TICK、TIME、TURN、TURNME、VERB、VRFY、X-EXPS、X-LINK2STATE、XADR、XAUTH、XCIR、XEXCH50、XGEN、XLICENSE、XQUE、XSTA、XTRN、XUSR です。

ステップ 14　[Data Commands] フィールドに、RFC 5321 に基づく SMTP DATA コマンドによるデータの送信と同じ方法でデータ送信を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

ステップ 15　[Binary Data Commands] フィールドに、RFC 3030 に基づく BDATA コマンドによるデータの送信と類似の方法でデータ送信を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

ステップ 16　[Authentication Commands] フィールドに、クライアントとサーバの間で認証交換を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

ステップ 17　X-Link2State Microsoft Exchange バッファ データ オーバーフロー攻撃の一部であるパケットを検出するには、[Detect xlink2state] を選択します。

ステップ 18　各種電子メール添付ファイルで抽出およびデコードするデータの最大バイト数を指定するには、次に示す添付ファイル タイプの値を指定します。

- **Base64 Decoding Depth**
- **7-Bit/8-Bit/Binary Decoding Depth**（プレーン テキスト、jpeg イメージ、mp3 ファイルなどの各種マルチパート コンテンツ タイプを含む）
- **Quoted-Printable Decoding Depth**
- **Unix-to-Unix Decoding Depth**

1 ～ 65535 バイトを指定するか、または、当該タイプのパケットのすべてのデータを抽出し、必要に応じてデコードする場合は 0 を指定します。添付ファイル タイプのデータを無視するには、-1 を指定します。

抽出したデータを検査するには、侵入ルールで `file_data` キーワードを使用できます。詳細については、「特定のペイロード タイプを指し示す（36-105 ページ）」を参照してください。

また、クロスパケット データまたは複数の TCP セグメントにわたるデータを抽出してデコードするには、SMTP [Stateful Inspection] オプションも選択する必要があります。

ステップ 19　SMTP トラフィックによりトリガーとして使用された侵入イベントとコンテキスト情報を関連付けるためのオプションを設定します。

- 侵入イベントに関連付ける MIME 添付ファイル名を抽出できるようにするには、[Log MIME Attachment Names] を選択します。
- 受信者の電子メール アドレスを抽出できるようにするには、[Log To Addresses] を選択します。
- 侵入イベントに関連付ける送信者の電子メール アドレスを抽出できるようにするには、[Log From Addresses] を選択します。
- 侵入イベントに関連付ける電子メール 見出しを抽出し、電子メール 見出しを検査するルールを作成できるようにするには、[Log Headers] を選択します。

見出し情報は侵入イベント パケット ビューに表示されることに注意してください。また、電子メール ヘッダー データと共にキーワード `content` または `protected_content` をパターンとして使用する侵入ルールを作成できることにも注意してください。詳細については、イベント情報の表示（41-25 ページ）およびコンテンツ一致の検索（36-16 ページ）を参照してください。

オプションで [Header Log Depth] に、抽出する電子メール 見出しのバイト数 0 ～ 20480 を指定できます。値 0 を指定すると、[Log Headers] が無効になります。

ステップ 20　ポリシーを保存するか、編集を続行するか、変更内容を破棄するか、ベース ポリシーのデフォルト設定に戻すか、またはシステム キャッシュの変更を反映せずに終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

SMTP 最大デコード メモリ アラートの有効化

ライセンス： Protection

有効になっているプリプロセッサが次のタイプのエンコード データのデコードに使用しているメモリの容量がシステムの最大許容メモリ量に達した場合にイベントを生成するには、SMTP プリプロセッサ ルール 124:9 を有効にします。

- Base64
- 7-bit/8-bit/binary
- Quoted-printable
- Unix-to-Unix

最大デコード メモリを超えた場合、メモリが使用可能になるまで、プリプロセッサはこれらのタイプのエンコード データのデコードを停止します。このプリプロセッサ ルールは、1 つの特定の設定オプションに関連付けられていません。ルールの有効化については、ルール状態の設定（32-22 ページ）を参照してください。

SSH プロプロセッサによるエクスプロイトの検出

ライセンス： Protection

SSH プリプロセッサは、チャレンジレスポンス バッファ オーバーフロー エクスプロイト、CRC32 エクスプロイト、SecureCRT SSH クライアント バッファ オーバーフロー エクスプロイト、プロトコル不一致、不正な SSH メッセージ方向を検出します。このプリプロセッサは、バージョン 1 または 2 ではないバージョン文字列も検出します。

チャレンジレスポンス バッファ オーバーフロー攻撃と CRC32 攻撃は鍵交換の後に発生するので、暗号化されています。いずれの攻撃でも、20 KB を超える普通よりも大きなペイロードが認証チャレンジ直後にサーバに送信されます。CRC32 攻撃の対象となるのは SSH バージョン 1 のみであり、チャレンジレスポンス バッファ オーバーフロー エクスプロイトの対象となるのは SSH バージョン 2 のみです。バージョン文字列は、セッションの開始時に読み取られます。バージョン文字列の違いを除き、この両方の攻撃は同様に扱われます。

SecureCRT SSH エクスプロイトとプロトコル不一致攻撃は、鍵交換前に接続をセキュリティで保護しようとするときに発生します。SecureCRT エクスプロイトでは、非常に長いプロトコル ID 文字列がクライアントに送信され、これが原因でバッファ オーバーフローが発生します。プロトコル不一致は、非 SSH クライアント アプリケーションがセキュア SSH サーバに接続しようとした場合、またはサーバとクライアントのバージョン番号が一致しない場合に発生します。

指定のポートまたは一連のポートでトラフィックを検査するか、または SSH トラフィックを自動的に検出するように、プリプロセッサを設定できます。指定のバイト数内で指定の数の暗号化パケットが渡されるか、または指定のパケット数内で指定の最大バイト数を超えるまで、SSH トラフィックの検査が続行されます。最大バイト数を超えた場合、CRC32（SSH バージョン 1）または チャレンジレスポンス バッファ オーバーフロー（SSH バージョン 2）攻撃が発生したものと想定されます。また、SecureCRT エクスプロイト、プロトコル不一致、および不正なメッセージ方向を検出できます。プリプロセッサは、設定していない場合でもバージョン 1 または 2 以外のバージョン文字列を検出することに注意してください。

SSH プリプロセッサを使用するときは、次の点に注意してください。

- ジェネレータ ID（GID）128 の SSH プリプロセッサ ルールを使用してイベントを生成する場合、これらのルールを有効にする必要があります。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。
- SSH プリプロセッサは、ブルート フォース攻撃には対処しません。ブルート フォース攻撃の試行については、動的ルール状態の追加（32-33 ページ）を参照してください。

詳細については、次の項を参照してください。

- SSH プリプロセッサ オプションの選択（27-72 ページ）
- SSH プリプロセッサの設定（27-74 ページ）

SSH プリプロセッサ オプションの選択

ライセンス： Protection

このセクションでは、SSH プリプロセッサを設定するときに使用できるオプションについて説明します。

次のいずれかが発生すると、プリプロセッサはセッションのトラフィックの検査を停止します。

- この数の暗号化パケットで、サーバとクライアント間で有効な交換が行われた場合。接続は続行します。
- 検査対象の暗号化パケットの数に達する前に、[Number of Bytes Sent Without Server Response] に達した場合。この場合、攻撃があったものと想定されます。

[Number of Encrypted Packets to Inspect] に達するまでの有効な各サーバ応答により、[Number of Bytes Sent Without Server Response] がリセットされ、パケット カウントが続行します。

次に示す SSH のプリプロセッサの設定例で説明します。

- [Server Ports]：22
- [Autodetect Ports]：off
- [Maximum Length of Protocol Version String]：80
- [Number of Encrypted Packets to Inspect]：25
- [Number of Bytes Sent Without Server Response]：19,600
- 検出オプションはすべて有効です。

この例では、プリプロセッサはポート 22 のトラフィックだけを検査します。つまり自動検出が無効であるため、指定のポートでのみ検査をします。

また、次のいずれかが発生すると、この例のプリプロセッサはトラフィックの検査を停止します。

- クライアントが 25 個の暗号化パケットを送信したが、すべてのパケットのデータ合計が 19,600 バイト以下であった。攻撃はなかったと想定されます。

- クライアントが、25 個の暗号化パケットで 19,600 バイトを超えるデータを送信した。この場合、この例のセッションは SSH バージョン 2 セッションであるため、プリプロセッサはこの攻撃がチャレンジレスポンス バッファ オーバーフロー エクスプロイトであるとみなします。

この例のプリプロセッサは、トラフィックの処理時に以下の状況が発生しているかどうかも検出します。

- 80 バイトより長いバージョン文字列によりトリガーとして使用されるサーバ オーバーフロー（これは SecureCRT エクスプロイトを示します）
- プロトコルの不一致
- 誤った方向に流れるパケット

最後に、プリプロセッサは、バージョン 1 または 2 以外のすべてのバージョン文字列を自動的に検出します。

次の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

サーバ ポート

SSH プリプロセッサがトラフィックを検査する必要があるポートを指定します。

1 つのポートか、複数ポートをカンマで区切ったリストを設定できます。

Autodetect Ports

SSH トラフィックを自動的に検出するようにプリプロセッサを設定します。

このオプションが選択されている場合、プリプロセッサはすべてのトラフィックで SSH バージョン番号を検査します。クライアント パケットにもサーバ パケットにもバージョン番号が含まれていない場合は、処理が停止します。無効である場合、プリプロセッサは [Server Ports] オプションで指定されているトラフィックだけを検査します。

Number of Encrypted Packets to Inspect

セッションあたりの検査対象の暗号化パケットの数を指定します。

このオプションをゼロに設定すると、すべてのトラフィックの通過が許可されます。

検査対象の暗号化パケットの数を減らすと、一部の攻撃が検出されなくなることがあります。検査対象の暗号化パケットの数を増やすと、パフォーマンスに悪影響を及ぼす可能性があります。

Number of Bytes Sent Without Server Response

SSH クライアントが、応答なしでサーバに送信できる最大バイト数を指定します。この最大バイト数を超えると、チャレンジレスポンス バッファ オーバーフロー攻撃または CRC32 攻撃が想定されます。

プリプロセッサがチャレンジレスポンス バッファ オーバーフローまたは CRC32 エクスプロイトを誤検出する場合は、このオプションの値を増やしてください。

Maximum Length of Protocol Version String

サーバのバージョン文字列の最大許容バイト数を指定します。この値を超えると、SecureCRT エクスプロイトとみなされます。

Detect Challenge-Response Buffer Overflow Attack

チャレンジレスポンス バッファ オーバーフロー エクスプロイトの検出を有効または無効にします。

このオプションのイベントを生成するには、ルール 128:1 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Detect SSH1 CRC-32 Attack

CRC32 エクスプロイトの検出を有効または無効にします。

このオプションのイベントを生成するには、ルール 128:2 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Detect Server Overflow

SecureCRT SSH クライアント バッファ オーバーフロー エクスプロイトの検出を有効または無効にします。

このオプションのイベントを生成するには、ルール 128:3 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Detect Protocol Mismatch

プロトコル不一致の検出を有効または無効にします。

このオプションのイベントを生成するには、ルール 128:4 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Detect Bad Message Direction

トラフィックのフロー方向が正しくない場合（つまり、推定されるサーバがクライアント トラフィックを生成したり、クライアントがサーバ トラフィックを生成したりした場合）の検出を有効または無効にします。

このオプションのイベントを生成するには、ルール 128:5 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Detect Payload Size Incorrect for the Given Payload

SSH パケットに指定された長さが IP 見出しに指定されている合計長と矛盾する場合や、メッセージが切り捨てられる場合、つまり完全な SSH 見出しを形成できる十分なデータがない場合などの、誤ったペイロード サイズのパケットの検出を有効または無効にします。

このオプションのイベントを生成するには、ルール 128:6 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Detect Bad Version String

有効である場合、プリプロセッサは、設定していない場合でもバージョン 1 または 2 以外のバージョン文字列を検出することに注意してください。

このオプションのイベントを生成するには、ルール 128:7 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

SSH プリプロセッサの設定

ライセンス： Protection

このセクションでは、SSH プリプロセッサを設定する方法について説明します。

SSH プリプロセッサの設定方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Application Layer Preprocessors] の下の [SSH Configuration] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効である場合は、[Enabled] をクリックし、次に [Edit] をクリックします。

[SSH Configuration] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　[SSH Configuration] プリプロセッサ ページのすべてのオプションを変更できます。詳細については、「SSH プリプロセッサ オプションの選択（27-72 ページ）」を参照してください。

ステップ 6　ポリシーを保存するか、編集を続行するか、変更内容を破棄するか、ベース ポリシーのデフォルト設定に戻すか、またはシステム キャッシュの変更を反映せずに終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

SSL プリプロセッサの使用

ライセンス： 機能によって異なる

SSL プリプロセッサでは SSL インスペクションを設定できます。SSL インスペクションは、暗号化トラフィックのブロック、暗号化トラフィックの復号化、アクセス コントロールによるトラフィックの検査を実行します。SSL インスペクションが設定されているかどうかに関わらず、SSL プリプロセッサは、トラフィックで検出された SSL ハンドシェイク メッセージを分析し、セッションを暗号化するタイミングを決定します。暗号化トラフィックを識別することにより、システムは暗号化ペイロードの侵入およびファイル インスペクションを停止できます。これによって、誤検出が減少し、パフォーマンスが向上します。詳細については、トラフィック復号化の概要（19-1 ページ）およびアクセス コントロール ルールの作成および編集（14-3 ページ）を参照してください。

SSL プリプロセッサは、暗号化トラフィックを検査して Heartbleed バグを悪用する試みを検出し、そのような悪用を検出するとイベントを生成します。

SSL プリプロセッサを使用して暗号化トラフィックを復号化する場合、ライセンスは必要ありません。マルウェアや侵入に対する暗号化ペイロードのインスペクションの停止、Heartbleed バグの悪用の検出を含め、すべての SSL プリプロセッサ機能には Protection ライセンスが必要です。

注　システム付属のネットワーク分析ポリシーは、デフォルトで SSL プリプロセッサを有効にします。暗号化トラフィックがネットワークを通過することを予想している場合は、カスタム展開で SSL プリプロセッサを無効にしないことを推奨します。

詳細については、次の項を参照してください。

- SSL 前処理について（27-76 ページ）
- SSL プリプロセッサ ルールの有効化（27-77 ページ）
- SSL プリプロセッサの設定（27-77 ページ）

SSL 前処理について

ライセンス： Protection

SSL インスペクションを設定すると、SSL プリプロセッサは暗号化データに対する侵入およびファイル インスペクションを停止して、SSL ポリシーにより暗号化トラフィックを検査します。これにより誤検出を排除できます。SSL プリプロセッサは、SSL ハンドシェイクを検査するときに状態情報を保持し、そのセッションの状態と SSL バージョンの両方を追跡します。セッションの状態が暗号化されていることをプリプロセッサが検出すると、そのセッションのトラフィックは暗号化されているものとしてシステムによりマークされます。暗号化が確定した場合に暗号化セッションにおけるすべてのパケット処理を停止し、Heartbleed のバグを悪用する試みが検出された場合にイベントを生成するように、システムを設定できます。

パケットごとに、IP 見出し、TCP 見出し、および TCP ペイロードがトラフィックに含まれており、このトラフィックが SSL 前処理用に指定されているポートで発生することが SSL プリプロセッサにより確認されます。次に示す状況では、対象トラフィックについて、トラフィックが暗号化されているかどうかが判別されます。

- システムがセッションのすべてのパケットを監視し、[Server side data is trusted] が有効にされておらず、サーバとクライアントの両方からの完了メッセージ、および Application レコードが存在するが Alert レコードがない各側からの 1 つ以上のパケットが、セッションに含まれている。
- システムがトラフィックの一部を検出せず、[Server side data is trusted] が有効にされておらず、Alert レコードによる応答がない Application レコードが存在する各側からの 1 つ以上のパケットが、セッションに含まれている。
- システムがセッションのすべてのパケットを監視し、[Server side data is trusted] が有効であり、クライアントからの完了メッセージ、および Application レコードが存在するが Alert レコードがないクライアントからの 1 つ以上のパケットが、セッションに含まれている。
- システムがトラフィックの一部を検出せず、[Server side data is trusted] が有効であり、Alert レコードによる応答がない Application レコードが存在するクライアントからの 1 つ以上のパケットが、セッションに含まれている。

暗号化トラフィックの処理を停止することを選択する場合、セッションが暗号化されているものとしてマークされると、そのセッションのその後のパケットは無視されます。

また、SSL ハンドシェイク時、プリプロセッサはハートビート要求および応答をモニタします。プリプロセッサは、以下を検出したときにイベントを生成します。

- ペイロード自体より大きなペイロード長の値を含むハートビート要求
- [Max Heartbeat Length] フィールドに保存された値よりも大きいハートビート応答

注　ルール内で SSL 状態またはバージョン情報を使用するには、キーワード `ssl_state` および `ssl_version` をルールに追加します。詳細については、セッションからの SSL 情報の抽出（36-59 ページ）を参照してください。

SSL プリプロセッサ ルールの有効化

ライセンス：Protection

有効である場合、SSL プリプロセッサは、SSL セッション開始時に交換されるハンドシェイクと鍵交換メッセージの内容を検査します。セッションが暗号化されると、侵入やマルウェア対するトラフィックの検査を一時停止できます。SSL インスペクションを設定した場合、SSL プリプロセッサは、ユーザがアクセス コントロールによって復号化、ブロック、暗号化、検査できる暗号化トラフィックも識別します。

ジェネレータ ID（GID）137 の SSL プリプロセッサ ルールを使用してイベントを生成する場合は、これらのルールを有効にする必要があることに注意してください。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

次の表に、有効にできる SSL プリプロセッサ ルールを示します。

表 27-14　SSL プリプロセッサ ルール

プリプロセッサ ルール GID：SID	説明
137:1	server hello の後の client hello（これは無効で、異常な動作とみなされる）を検出します。
137:2	[Server side data is trusted] が無効な場合に、client hello のない server hello を検出します。これは無効であり、異常な動作としてみなされます。詳細については、「SSL プリプロセッサの設定（27-77 ページ）」を参照してください。
137:3	[Max Heartbeat Length] フィールドにゼロ以外の値が含まれている場合に、ペイロード自体よりも大きいペイロード長の値を含むハートビート要求を検出します。このようなハートビート要求は、Heartbleed バグを悪用する試みを示しています。
137:4	[Max Heartbeat Length] フィールドで指定されているゼロ以外の値よりも大きいハートビート要求を検出します。このようなハートビート要求は、Heartbleed バグを悪用する試みを示しています。

SSL プリプロセッサの設定

ライセンス：Protection

SSL インスペクションを設定しないと、システムは、復号化せずに、マルウェアと侵入について暗号化トラフィックを検査します。SSL プリプロセッサを有効にすると、セッションが暗号化されたときにそのことを検出します。SSL プリプロセッサが有効にされると、ルール エンジンがこのプリプロセッサを呼び出し、SSL の状態およびバージョン情報を取得できるようになります。侵入ポリシーでキーワード `ssl_state` および `ssl_version` を使用してルールを有効にする場合は、そのポリシーで SSL プリプロセッサも有効にする必要があります。

また、暗号化セッションによるインスペクションと再構成を無効にするには、[Stop inspecting encrypted traffic] オプションを有効にします。SSL プリプロセッサによりセッションの状態が維持されるため、セッションのすべてのトラフィックのインスペクションを無効にできます。システムが暗号化セッションのトラフィックのインスペクションを停止するのは、SSL 前処理が有効であり、**かつ** [Stop inspecting encrypted traffic] オプションが選択されている場合だけです。[Stop inspecting encrypted traffic] オプションをオフにした場合は、[Server side data is trusted] オプションを変更できません。

サーバ トラフィックのみに基づいて暗号化トラフィックを識別するには、[Server side data is trusted] オプションを有効にできます。つまり、トラフィックが暗号化されていることを示すサーバ側のデータが信頼されます。SSL プリプロセッサは通常、クライアント トラフィックと、そのトラフィックに対するサーバの応答の両方を調べ、セッションが暗号化されているかどうかを判別します。ただし、セッションの両側を検出できない場合には、システムはトランザクションを暗号化されているものとしてマークしないため、セッションが暗号化されていることを示す SSL サーバを信頼できます。[Server side data is trusted] オプションを有効にする場合は、[Stop inspecting encrypted traffic] オプションも有効にして、システムが暗号化セッションのトラフィックの検査を続行しないようにする必要があることに注意してください。

SSL ハンドシェイク内のハートビート要求および応答を調べることで、Heartbleed バグを悪用しようとする試みを検出するようにプリプロセッサの [Max Heartbeat Length] オプションを設定できます。ペイロード長が実際のペイロード長よりも大きいハートビート要求、または [Max Heartbeat Length] の値よりもサイズが大きいハートビート応答をプリプロセッサが検出すると、プリプロセッサはイベントを生成します。

プリプロセッサがトラフィックで暗号化セッションをモニタするポートを指定できます。

注　SSL プリプロセッサは、SSL モニタの対象として指定されたポートで SSL 以外のトラフィックを検出すると、そのトラフィックを SSL トラフィックとしてデコードすることを試みた後、破損しているものとしてマークします。

SSL プリプロセッサの設定方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Application Layer Preprocessors] の下の [SSL Configuration] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効である場合は、[Enabled] をクリックし、次に [Edit] をクリックします。

[SSL Configuration] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　SSL プリプロセッサが、暗号化されたセッションのトラフィックをモニタする必要があるポートを、カンマで区切って入力します。[Ports] フィールドに指定されるポートでのみ、暗号化トラフィックが検査されます。

ステップ 6　[Stop inspecting encrypted traffic] チェック ボックスをクリックして、セッションが暗号化されているものとしてマークされた後のそのセッションでのトラフィックのインスペクションを有効または無効にします。

ステップ 7　[Server side data is trusted] チェック ボックスをクリックして、クライアント側のトラフィックだけに基づく暗号化トラフィックの識別を有効または無効にします。

ステップ 8　[Max Heartbeat Length] フィールドにバイト数を入力し、Heartbleed バグを悪用する試みに対する SSL ハンドシェイク内のハートビート要求と応答の検査を有効にします。`1` ～ `65535` の整数を指定できます。このオプションを無効にする場合は `0` を入力します。

ステップ 9　ポリシーを保存するか、編集を続行するか、変更内容を破棄するか、ベース ポリシーのデフォルト設定に戻すか、またはシステム キャッシュの変更を反映せずに終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

SCADA 前処理の設定

侵入ポリシーで有効になっているルールを使用してインスペクション用にトラフィックを準備するネットワーク分析ポリシーの Supervisory Control and Data Acquisition（SCADA）プリプロセッサを設定します。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーについて（23-1 ページ）」を参照してください。

（SCADA）プロトコルは、製造、水処理、配電、空港、輸送システムなどの工業プロセス、インフラストラクチャ プロセス、および設備プロセスからのデータをモニタ、制御、取得します。FireSIGHT システム には、ネットワーク分析ポリシーの一部として設定できる、Modbus および DNP3 SCADA プロトコル用のプリプロセッサがあります。

注意 カスタム ユーザ ロールを持つ一部のユーザは、標準メニュー パス（[Policies] > [Access Control] > [Network Analysis Policy]）からネットワーク分析ポリシーにアクセスできません。これらのユーザは、侵入ポリシーを介してネットワーク分析ポリシーにアクセスできます（[Policies] > [Intrusion] > [Intrusion Policy] > [Network Analysis Policy]）カスタム ユーザ ロールの詳細については、カスタム ユーザ ロールの管理（61-55 ページ）を参照してください。

対応する侵入ポリシーで Modbus または DNP3 キーワードを含むルールを有効にすると、Modbus または DNP3 プロセッサがその現在の設定で自動的に使用されます。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。詳細については、Modbus キーワード（36-79 ページ）および DNP3 キーワード（36-81 ページ）を参照してください。

詳細については、次の項を参照してください。

- Modbus プリプロセッサの設定（28-1 ページ）
- DNP3 プリプロセッサの設定（28-3 ページ）

Modbus プリプロセッサの設定

ライセンス： Protection

Modbus プロトコルは 1979 年に Modicon が初めて発表した、広く利用されている SCADA プロトコルです。Modbus プリプロセッサは、Modbus トラフィックの異常を検出し、ルール エンジンによる処理のために Modbus プロトコルをデコードします。ルール エンジンは Modbus キーワードを使用して特定のプロトコル フィールドにアクセスします。詳細については、「Modbus キーワード（36-79 ページ）」を参照してください。

1 つの構成オプションで、プリプロセッサが Modbus トラフィックを検査するポートのデフォルト設定を変更できます。

イベントを生成するには、次の表に示す Modbus プリプロセッサ ルールを有効にする必要があります。ルールの有効化については、ルール状態の設定（32-22 ページ）を参照してください。

表 28-1　Modbus プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
144:1	Modbus の見出しの長さが、Modbus 機能コードに必要な長さと一致していない場合に、イベントが生成されます。 各 Modbus 機能の要求と応答には期待される形式があります。メッセージの長さが、期待される形式と一致しない場合に、このイベントが生成されます。
144:2	Modbus プロトコル ID がゼロ以外の場合に、イベントが生成されます。プロトコル ID フィールドは、Modbus と共にその他のプロトコルを多重伝送するために使用されます。プリプロセッサはこのような他のプロトコルを処理しないため、代わりにこのイベントが生成されます。
144:3	プリプロセッサが予約済み Modbus 機能コードを検出すると、イベントが生成されます。

Modbus プリプロセッサの使用に関しては、ネットワークに Modbus 対応デバイスが含まれていない場合、トラフィックに適用するネットワーク分析ポリシーでこのプリプロセッサを有効にしないでください。

Modbus プリプロセッサがモニタするポートを変更するには、次の手順を使用します。

Modbus プリプロセッサの設定方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[SCADA Preprocessors] の下の [Modbus Configuration] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効になっている場合は、[Edit] をクリックします。
- 設定が無効である場合は、[Enabled] をクリックし、次に [Edit] をクリックします。

[Modbus Configuration] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　オプションで、プリプロセッサが Modbus トラフィックを検査するポートを変更します。0 ～ 65535 の整数を指定できます。複数のポートを指定する場合はカンマで区切ります。

ステップ 6　ポリシーを保存するか、編集を続けるか、変更を破棄するか、基本ポリシーのデフォルト構成設定に戻すか、あるいはシステム キャッシュに変更を残して終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

DNP3 プリプロセッサの設定

ライセンス：Protection

Distributed Network Protocol（DNP3）は、もともとは発電所間で一貫性のある通信を実現する目的で開発された SCADA プロトコルです。DNP3 も、水処理、廃棄物処理、輸送などさまざまな産業分野で幅広く利用されるようになっています。

DNP3 プリプロセッサは、DNP3 トラフィックの異常を検出し、ルール エンジンによる処理のために DNP3 プロトコルをデコードします。ルール エンジンは DNP3 キーワードを使用して特定のプロトコル フィールドにアクセスします。詳細については、「DNP3 キーワード（36-81 ページ）」を参照してください。

イベントを生成するには、次の表に示す DNP3 プリプロセッサ ルールを有効にする必要があります。ルールの有効化については、ルール状態の設定（32-22 ページ）を参照してください。

表 28-2　DNP3 プリプロセッサ ルール

プリプロセッサ ルール GID：SID	説明
145:1	[Log bad CRC] が有効である場合に、無効なチェックサムを含むリンク層フレームがプリプロセッサにより検出されると、イベントが生成されます。
145:2	無効な長さの DNP3 リンク層フレームがプリプロセッサにより検出されると、イベントが生成され、パケットがブロックされます。
145:3	再構成中に無効なシーケンス番号のトランスポート層セグメントがプリプロセッサにより検出されると、イベントが生成され、パケットがブロックされます。
145:4	完全なフラグメントを再構成する前に DNP3 再構成バッファがクリアされると、イベントが生成されます。このことは、FIR フラグを伝送するセグメントが、他のセグメントがキューに入れられた後で現れる場合に発生します。
145:5	予約済みアドレスを使用する DNP3 リンク層フレームをプリプロセッサが検出すると、イベントが生成されます。
145:6	予約済み機能コードを使用する DNP3 要求または応答をプリプロセッサが検出すると、イベントが生成されます。

DNP3 プリプロセッサの使用に関しては、ネットワークに DNP3 対応デバイスが含まれていない場合、トラフィックに適用するネットワーク分析ポリシーでこのプリプロセッサを有効にしないでください。詳細については、「TCP ストリームの前処理の設定（29-32 ページ）」を参照してください。

設定できる DNP3 プリプロセッサ オプションを以下で説明します。

ポート

指定された各ポートでの DNP3 トラフィックのインスペクションを有効にします。1 つのポートか、複数ポートをカンマで区切ったリストを指定できます。各ポートに 0 ～ 65535 の値を指定できます。

Log bad CRCs

有効である場合、DNP3 リンク層フレームに含まれているチェックサムが検証されます。無効なチェックサムを含むフレームは無視されます。

無効なチェックサムが検出されたときにイベントを生成するには、ルール 145:1 を有効にします。

DNP3 プリプロセッサの設定方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[SCADA Preprocessors] の下の [DNP3 Configuration] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効な場合、[Edit] をクリックします。
- 設定が無効である場合は、[Enabled] をクリックし、次に [Edit] をクリックします。

[DNP3 Configuration] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　オプションで、プリプロセッサが DNP3 トラフィックを検査するポートを変更します。0 ～ 65535 の整数を指定できます。複数のポートを指定する場合はカンマで区切ります。

ステップ 6　オプションで、[Log bad CRCs] チェック ボックスをオンまたはオフにして、DNP3 リンク層フレームに含まれているチェックサムを検証し、無効なチェックサムのフレームを無視するかどうかを指定します。

ステップ 7　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、ネットワーク分析ポリシーの編集操作の表を参照してください。

トランスポート層およびネットワーク層の前処理の使用

侵入ポリシーで有効になっているルールを使用してインスペクション用にトラフィックを準備するネットワーク分析ポリシーのネットワーク層プリプロセッサでほとんどのトランスポートを設定します。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーについて（23-1 ページ）」を参照してください。

トランスポート層およびネットワーク層のプリプロセッサは、IP フラグメント、チェックサム検証、TCP および UDP セッションの前処理を悪用する攻撃を検出します。パケットがプリプロセッサに送信される前に、パケット デコーダはパケット ヘッダーとペイロードを、プリプロセッサおよび侵入ルール エンジンで簡単に使用できるフォーマットに変換し、パケット ヘッダー内でさまざまな変則的動作を検出します。インライン正規化プリプロセッサは、パケットをデコードした後、他のプリプロセッサにパケットを送信する前に、インライン型展開を対象にトラフィックを正規化します。

侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。詳細については、カスタム ポリシーの制限（23-13 ページ）を参照してください。

注意 カスタム ユーザ ロールを持つ一部のユーザは、標準メニュー パス（[Policies] > [Access Control] > [Network Analysis Policy]）からネットワーク分析ポリシーにアクセスできません。これらのユーザは、侵入ポリシーを介してネットワーク分析ポリシーにアクセスできます（[Policies] > [Intrusion] > [Intrusion Policy] > [Network Analysis Policy]）カスタム ユーザ ロールの詳細については、カスタム ユーザ ロールの管理（61-55 ページ）を参照してください。

ネットワーク分析ポリシーで設定したトランスポート層/ネットワーク層プリプロセッサの設定を VLAN、ゾーン、またはネットワークによって調整できます。一部のトランスポート層およびネットワーク層の設定はすべてのトラフィックにグローバルに適用され、アクセス コントロール ポリシーでこれらを設定します。

トランスポート/ネットワークの詳細設定の構成

ライセンス： Protection

トランスポートおよびネットワークのプリプロセッサの詳細設定は、アクセス コントロール ポリシーを適用するすべてのネットワーク、ゾーン、および VLAN にグローバルに適用されます。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセス コントロール ポリシーで設定します。

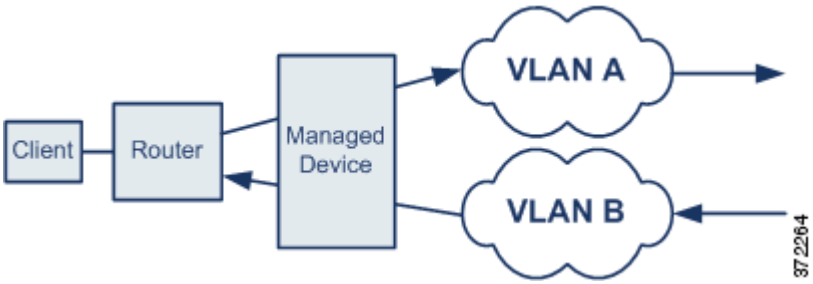
次の項では、これらの設定について説明します。

VLAN 見出しの無視

ライセンス： Protection

サポートされるデバイス： すべて（ASA FirePOWER を除く）

同じ接続で異なる方向に流れるトラフィックの VLAN タグが異なると、トラフィックの再アセンブリやルールの処理に影響を与える場合があります。たとえば、以下の図では、同じ接続のトラフィックを VLAN A で送信し、VLAN B で受信できます。



[Ignore the VLAN header when tracking connections] を有効にすると、VLAN ヘッダーが無視されるので、展開に応じて適切にパケットを処理できます。

VLAN 見出しを無視するには、以下を行います。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　編集するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3　[Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[Transport/Network Layer Preprocessor Settings] の横にある編集アイコン（ ）をクリックします。

[Transport/Network Layer Preprocessor Settings] ポップアップ ウィンドウが表示されます。

ステップ 5　次の選択肢があります。

- 展開されているデバイスが、異なる方向に流れるトラフィックで同じ接続に対して異なる VLAN タグを検出する可能性がある場合は、[Ignore the VLAN header when tracking connections] チェック ボックスをオンにして、トラフィックを識別するときに VLAN ヘッダーを無視するようにします。
- 展開されているデバイスが、異なる方向に流れるトラフィックで同じ接続に対して異なる VLAN タグを検出する可能性がない場合は、[Ignore the VLAN header when tracking connections] チェック ボックスをオフにして、トラフィックを識別するときに VLAN ヘッダーを考慮するようにします。

ステップ 6　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

侵入廃棄ルールでのアクティブ応答の開始

ライセンス：Protection

廃棄ルールは、ルール状態が [Drop and Generate Events] に設定された侵入ルールまたはプリプロセッサ ルールです。インライン展開では、システムは TCP または UDP 廃棄ルールに応答するために、トリガーしたパケットをドロップし、そのパケットが開始されたセッションをブロックします。パッシブ展開の場合、システムがパケットをドロップすることはできません。また、セッションをブロックすることもありませんが、アクティブ応答を使用する場合はその限りではありません。

ヒント　UDP データ ストリームは一般に*セッション*という観点では考慮されないため、ストリーム プリプロセッサがカプセル化 IP データグラム 見出しの送信元および宛先 IP アドレス フィールドと UDP 見出しのポート フィールドを使用してフローの方向を判別し、UDP セッションを識別する方法については、UDP ストリームの前処理の使用（29-34 ページ）で詳しく説明しています。

[Maximum Active Responses] オプションを設定することで、問題のあるパケットによって TCP または UDP 廃棄ルールがトリガーされた時点で、1 つ以上の *アクティブ応答*を開始して、より正確かつ明示的に TCP 接続または UDP セッションを閉じることができます。

インライン展開でアクティブ応答が有効にされている場合、システムは TCP 廃棄ルールへの応答として、トリガーしたパケットをドロップし、クライアントとサーバの両方のトラフィックに TCP リセット（RST）パケットを挿入します。システムはパッシブ展開でパケットをドロップできません。アクティブ応答がパッシブ展開で有効になっている場合、システムは TCP 接続のクライアント側とサーバー側の両方に TCP リセットを送信することによって TCP 廃棄ルールに応答します。インライン展開またはパッシブ展開でアクティブ応答が有効にされていると、システムはセッションの両端に ICMP 到達不能パケットを送信することによって UDP セッションを閉じます。リセットは接続やセッションに影響を与えるのに間に合うまでに到着する可能性が高いため、アクティブ応答はインライン展開で最も効果を発揮します。

[Maximum Active Responses] オプションの設定方法によっては、接続またはセッションのいずれかの側からさらにトラフィックが発生しているようであれば、システムが追加のアクティブ応答を開始することもできます。システムは、指定された間隔（秒数）で、指定された最大回数まで追加のアクティブ応答を開始します。

アクティブ応答の最大数を設定する方法については、TCP グローバル オプションの選択（29-23 ページ）を参照してください。

[Maximum Active Responses] の設定とは関係なく、**resp** または **react** ルールがトリガーされた場合にも、アクティブ応答が開始されることに注意してください。ただし、[Maximum Active Responses] は、廃棄ルールに対するアクティブ応答の最大数を制御するのと同じ方法で、**resp** および **react** ルールに対して追加のアクティブ応答をシステムが開始するかどうかを制御します。詳細については、「ルール キーワードを使用したアクティブ応答の開始（36-90 ページ）」を参照してください。

`config response` コマンドを使用して、使用するアクティブ応答インターフェイス、およびパッシブ展開で試行する TCP リセットの回数を設定することもできます。詳細については、「アクティブ応答のリセット試行とインターフェイスの設定（36-93 ページ）」を参照してください。

プリプロセッサ ルールは、次のオプションに関連付けられていません。

Maximum Active Responses

TCP 接続あたりのアクティブ応答の最大数を 1 ～ 25 の範囲で指定します。アクティブ応答が開始された接続でさらにトラフィックが発生し、前のアクティブ応答を送信してから [Minimum Response Seconds] を超えるトラフィックが発生した場合、システムは指定された最大数に達するまで、別のアクティブ応答を送信します。0 を設定すると、廃棄ルールによってトリガーされるアクティブ応答が無効になり、**resp** または **react** ルールによってトリガーされる追加のアクティブ応答も無効になります。詳細については、侵入廃棄ルールでのアクティブ応答の開始（29-3 ページ）およびルール キーワードを使用したアクティブ応答の開始（36-90 ページ）を参照してください。

Minimum Response Seconds

[Maximum Active Responses] に達するまで、システムがアクティブ応答を開始した接続で発生した追加のトラフィックに対して次のアクティブ応答を送信するまで待機する時間を 1 ～ 300 秒の範囲で指定します。

廃棄ルールでアクティブ応答を開始するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　編集するアクセス コントロール ポリシーの横にある編集アイコン（  ）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3　[Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[Transport/Network Layer Preprocessor Settings] の横にある編集アイコン（  ）をクリックします。

[Transport/Network Layer Preprocessor Settings] ポップアップ ウィンドウが表示されます。

ステップ 5　次の選択肢があります。

- TCP 接続 1 つあたりの [Maximum Active Responses] を 1 ～ 25 の値で指定します。0 を設定すると、廃棄ルールによってトリガーされるアクティブ応答が無効になり、**resp** または **react** ルールによってトリガーされる追加のアクティブ応答も無効になります。
- [Maximum Active Responses] が発生するか、またはシステムがアクティブ応答を開始した接続で追加のトラフィックが次のアクティブ応答をもたらすまで待機する [Minimum Response Seconds] を 1 ～ 300 の値で指定します。

ステップ 6　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

トラブルシューティング：セッション終了メッセージのロギング

ライセンス：Protection

トラブルシューティングの電話中に、個別の接続が指定したしきい値を超えた場合にメッセージを記録するようにシステムを設定するようにサポートから依頼される場合があります。このオプションの設定を変更するとパフォーマンスに影響するので、必ずサポートのガイダンスに従って実行してください。

セッション終了メッセージのログを記録するには、次の手順を実行します。

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　編集するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3　[Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[Transport/Network Layer Preprocessor Settings] の横にある編集アイコン（）をクリックします。

[Transport/Network Layer Preprocessor Settings] ポップアップ ウィンドウが表示されます。

ステップ 5　[Troubleshooting Options] を展開します。

ステップ 6　セッションが終了し、指定した数を超過した場合に記録されるメッセージのバイト数を [Session Termination Logging Threshold] で指定します。

上限は 1GB ですが、管理対象デバイス上でストリーム処理のために割り振られるメモリの量によっても制限されます。

ステップ 7　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

チェックサムの検証

ライセンス： Protection

システムは、あらゆるプロトコル レベルのチェックサムを検証することで、IP、TCP、UDP、および ICMP による送信データが完全に受信されていることを確認できます。さらに基本的なレベルで、パケットが転送中に改ざんされたり、誤って変更されたりしていないことも確認できます。チェックサムはアルゴリズムを使用して、パケットでのプロトコルの整合性を検証します。システムが終端のホストでパケットに書き込まれた値を計算し、それがチェックサムと同じであれば、そのパケットは変更されていないと見なされます。

チェックサムの検証を無効にすると、ネットワークがインジェクション攻撃にさらされる危険があります。システムは、チェックサム検証イベントを生成しないことに注意してください。インライン展開では、パケットのチェックサムが正しくない場合、そのパケットをドロップするようにシステムを設定できます。

チェックサム検証を設定するには、以下を行います。

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーでまだ保存されていない変更がある場合、それらの変更を破棄して続行するには [OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Edit Policy] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Transport/Network Layer Preprocessors] で [Checksum Verification] が有効にされているかどうかによって、以下の 2 つの選択肢があります。

- この設定が有効にされている場合、[Edit] をクリックします。
- この設定が無効にされている場合、[Enabled] をオンにしてから、[Edit] をクリックします。

[Checksum Verification] ページが表示されます。ページ下部のメッセージは、設定を含むポリシー層を示します。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　[Checksum Verification] セクションの以下のオプションはいずれも、パッシブまたはインライン展開では [Enabled] または [Disabled] に設定できます。インライン展開では、[Drop] に設定することもできます。

- **ICMP Checksums**
- **IP Checksums**
- **TCP Checksums**
- **UDP Checksums**

違反パケットをドロップするには、オプションを [Drop] に設定することに加え、関連付けられているネットワーク分析ポリシーの [Inline Mode] も有効にする必要があることに注意してください。詳細については、「インライン展開でプリプロセッサがトラフィックに影響を与えることを

許可する（26-6 ページ）」を参照してください。また、パッシブ展開またはタップ モードのインライン展開で上記のオプションを [Drop] に設定することは、オプションを [Enable] に設定した場合と同じ効果があることに注意してください。

ステップ 6　ポリシーを保存するか、編集を続けるか、変更を破棄するか、基本ポリシーのデフォルト構成設定に戻すか、あるいはシステム キャッシュに変更を残して終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

インライン トラフィックの正規化

ライセンス： Protection

インライン正規化プリプロセッサは、インライン展開で攻撃者が検出を免れる可能性を最小限にするために、トラフィックを正規化します。ネットワーク分析ポリシーでインライン正規化プリプロセッサを有効にすると、システムは次の 2 つの状態をテストして、ユーザがインライン展開を使用していることを確認します。

- [Inline Mode] がポリシーで有効になっている。インライン展開でプリプロセッサがトラフィックに影響を与えることを許可する（26-6 ページ）を参照してください。
- インライン正規化が有効化されているアクセス コントロール ポリシーは、インライン セットを使用しているインライン展開されたデバイスに適用されます。

上記の両方の条件に一致した場合のみ、プリプロセッサは指定されたトラフィックを正規化します。

IPv4、IPv6、ICMPv4、ICMPv6、TCP トラフィックを任意に組み合わせて正規化を指定できます。ほとんどの正規化は、パケット単位で行われ、インライン正規化プリプロセッサによって処理されます。ただし、TCP ストリーム プリプロセッサは、TCP ペイロードの正規化を含む、ほとんどの状態関連パケットおよびストリームの正規化を処理します。

インライン正規化は、パケット デコーダによるデコードの直後に行われます。その後で、別のプリプロセッサによる処理が行われます。正規化は、パケット層の内部から外部への方向で行われます。

インライン正規化プリプロセッサはイベントを生成しません。インライン正規化プリプロセッサの役割は、インライン展開の別のプリプロセッサおよびルール エンジンで使用できるようにパケットを準備することです。また、システムが処理するパケットが、ネットワーク上のホストで受信したパケットと同じであるようにする役割もあります。

ヒント　インライン展開の場合、Cisco では、インライン正規化プリプロセッサの設定で [Normalize TCP Payload] オプションを有効にするように推奨しています。パッシブ展開の場合、Cisco では、適応型プロファイルを設定するように推奨しています。詳細については、パッシブ展開における前処理の調整（30-1 ページ）を参照してください。

Minimum TTL

[Reset TTL] がこのオプションに設定する値 1 ～ 255 以上の値に設定されている場合、このオプションは以下を指定します。

- [Normalize IPv4] が有効にされている場合は、[IPv4 Time to Live (TTL)] フィールドの最小許容値。TTL のパケット値がこの値を下回る場合、[Reset TTL] に設定された値に正規化されます。

- [Normalize IPv6] が有効にされている場合は、[IPv6 Hop Limit] フィールドの最小許容値。ホップ リミットの値がこの値を下回る場合、[Reset TTL] に設定された値に正規化されます。

  このフィールドが空白の場合、システムは値が 1 であると想定します。

  デコーダ ルール カテゴリで以下のルールを有効にすると、このオプションに対するイベントを生成できます。

- 指定の最小値を下回る TTL が設定された IPv4 パケットが検出された場合にイベントを生成するには、ルール 116:428 を有効にします。
- 指定の最小値を下回るホップ リミットが設定された IPv6 パケットが検出された場合にイベントを生成するには、ルール 116:270 を有効にします。

  詳細については、パケットのデコードの設定（29-21 ページ）のパケット デコーダの [Detect Protocol Header Anomalies] オプションを参照してください。

Reset TTL

このオプションに設定した値 1 ～ 255 が [Minimum TTL] 値を上回る場合、以下のフィールドが正規化されます。

- [Normalize IPv4] が有効にされている場合は、[IPv4 TTL] フィールド
- [Normalize IPv6] が有効にされている場合は、[IPv6 Hop Limit] フィールド

パケット値が [Minimum TTL] を下回る場合、システムはパケットの TTL またはホップ リミットの値をこのオプションに対して設定された値に変更して、パケットを正規化します。このオプションを値 0 または [Minimum TTL] を下回る値に設定すると、オプションは無効になります。このフィールドが空白の場合、システムは値が 0 であると想定します。

Normalize IPv4

IPv4 トラフィックの正規化を有効にします。このオプションが有効にされていて、[Reset TTL] に設定された値が TTL 正規化を有効にしている場合、システムは必要に応じて TTL フィールドも正規化します。このオプションを有効にする場合、[Normalize Don’t Fragment Bits] および [Normalize Reserved Bits] オプションも有効にすることができます。

このオプションを有効にすると、システムは以下の基本の IPv4 正規化を実行します。

- 過剰なペイロードを持つパケットを、IP 見出しに指定されたデータグラム長まで切り捨てます。
- [Differentiated Services (DS)] フィールド（旧称 [Type of Service (TOS)] フィールド）をクリアします。
- すべてのオプション オクテットを 1（No Operation）に設定します。

Normalize Don't Fragment Bit

[IPv4 Flags] ヘッダー フィールドの単一ビットの [Don’t Fragment] サブフィールドをクリアします。このオプションを有効にすると、ダウンストリームのルータがパケットをドロップする代わりに、必要に応じてパケットをフラグメント化できます。また、このオプションを有効にすることで、ドロップされるパケットを巧妙に作成してポリシーを回避する試みを防ぐこともできます。このオプションを選択するには、[Normalize IPv4] を有効にする必要があります。

Normalize Reserved Bit

[IPv4 Flags] ヘッダー フィールドの単一ビットの [Reserved] サブフィールドをクリアします。通常は、このオプションを有効にします。このオプションを選択するには、[Normalize IPv4] を有効にする必要があります。

Normalize TOS Bit

1 バイトの [Differentiated Services]（旧称 [Type of Service]）フィールドをクリアします。このオプションを選択するには、[Normalize IPv4] を有効にする必要があります。

Normalize Excess Payload

過剰なペイロードを持つパケットを、IP 見出しに指定されたデータグラム長にレイヤ 2（たとえば、イーサネット）見出しを合計した長さにまで切り捨てます。ただし、最小フレーム長より小さく切り捨てることはしません。このオプションを選択するには、[Normalize IPv4] を有効にする必要があります。

Normalize IPv6

[Hop-by-Hop Options] および [Destination Options] 拡張ヘッダーに含まれるすべてのオプション タイプ フィールドを 00（スキップして処理を続行）に設定します。このオプションが有効にされていて、[Reset TTL] に設定された値が ホップ リミット正規化を有効にしている場合、システムは必要に応じてホップ リミット フィールドも正規化します。

Normalize ICMPv4

ICMPv4 トラフィックのエコー（要求）およびエコー応答メッセージで 8 ビットのコード フィールドをクリアします。

Normalize ICMPv6

ICMPv6 トラフィックのエコー（要求）およびエコー応答メッセージで 8 ビットのコード フィールドをクリアします。

Normalize/Clear Reserved Bits

TCP ヘッダーの予約ビットをクリアします。

Normalize/Clear Option Padding Bytes

TCP オプションのパディング バイトをクリアします。

Clear Urgent Pointer if URG=0

緊急（URG）制御ビットが設定されていない場合、16 ビットの TCP ヘッダー [Urgent Pointer] フィールドをクリアします。

Clear Urgent Pointer/URG on Empty Payload

ペイロードがない場合、TCP ヘッダー [Urgent Pointer] フィールドおよび URG 制御ビットをクリアします。

Clear URG if Urgent Pointer is Not Set

緊急ポインタが設定されていない場合、TCP ヘッダー URG 制御ビットをクリアします。

Normalize Urgent Pointer

ポインタがペイロード長を上回る場合、2 バイトの TCP ヘッダー [Urgent Pointer] フィールドをペイロード長に設定します。

Normalize TCP Payload

再送信されるデータの一貫性が確保されるように TCP データ フィールドの正規化を有効にします。正しく再アセンブルできないセグメントはすべてドロップされます。

Remove Data on SYN

TCP オペレーティング システム ポリシーが Mac OS **以外**の場合、同期（SYN）パケットのデータを削除します。

このオプションによって、ルール 129:2 のイベント生成も無効になります。

Remove Data on RST

TCP リセット（RST）パケットからデータを削除します。

Trim Data to Window

[TCP Data] フィールドを [Window] フィールドに指定されたサイズにまで切り捨てます。

Trim Data to MSS

ペイロードが MSS より長い場合、[TCP Data] フィールドを最大セグメント サイズ（MSS）にまで切り捨てます。

Block Unrecoverable TCP Header Anomalies

このオプションを有効にすると、システムは無効になり受信ホストによってブロックされる可能性が高い異常な TCP パケット（正規化されている場合）をブロックします。たとえば、システムは確立されたセッションの後に送信された SYN パケットをブロックします。

また、システムは、ルールが有効にされているかどうかに関係なく、以下に示す TCP ストリーム プリプロセッサ ルールのいずれかに一致するパケットもドロップします。

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14 ～129:19

[Total Blocked Packets] パフォーマンス グラフには、インライン展開でブロックされたパケットの数が示され、パッシブ展開とタップ モードでのインライン展開の場合は、インライン展開でブロックされる予想数が示されます。詳細については、「侵入イベントのパフォーマンス統計グラフの生成（41-5 ページ）」を参照してください。

Explicit Congestion Notification

明示的輻輳通知（ECN）フラグのパケット単位またはストリーム単位の正規化を以下のように有効にします。

- [Packet] を選択すると、ネゴシエーションに関係なく、パケット単位で ECN フラグがクリアされます。
- [Stream] を選択すると、ECN の使用がネゴシエートされていない場合、ストリーム単位で ECN フラグがクリアされます。

  [Stream] を選択した場合、この正規化が実行されるようにするには、TCP ストリーム プリプロセッサの [Require TCP 3-Way Handshake] オプションも有効にされている必要があります。詳細については、TCP ポリシーのオプションの選択（29-25 ページ）を参照してください。

Allow These TCP Options

トラフィックで許可する特定の TCP オプションの正規化を無効にします。

明示的に許可されたオプションは、正規化されません。オプションを [No Operation]（TCP オプション 1）に設定して明示的に許可していないオプションは、正規化されます。

最大セグメント サイズ（MSS）、ウィンドウ スケール、およびタイムスタンプ TCP のオプションは TCP パフォーマンスを最適化するために一般的に使用されるため、システムは、これらのオプションを常に許可します。システムは、[Allow These TCP Options] の設定に関係なく、これらの一般的に使用されるオプションを正規化します。他のそれほど一般的に使用されないオプションについては、システムは自動的に許可しません。

特定のオプションを許可するには、オプション キーワード、オプション番号、またはこの両方のカンマ区切りリストを設定します。以下に、一例を示します。

```
sack, echo, 19
```

オプション キーワードを指定するということは、そのキーワードと関連付けられた 1 つ以上の TCP オプションの番号を指定することと同じです。たとえば、`sack` を指定することは、TCP オプション 4（Selective Acknowledgment Permitted）および TCP オプション 5（Selective Acknowledgment）を指定することと同じです。オプション キーワードでは、大文字と小文字が区別されません。

また、`any` を指定すると、すべての TCP オプションが許可されるため、実質的にすべての TCP オプションの正規化が無効にされます。

次の表に、許可する TCP オプションを指定する方法を要約します。フィールドを空のままにすると、システムは MSS、ウィンドウ スケール、およびタイムスタンプのオプションのみを許可します。

指定するキーワード	許可されるオプション
sack	TCP オプション 4（Selective Acknowledgment Permitted）および 5（Selective Acknowledgment）
echo	TCP オプション 6（Echo Request）および 7（Echo Reply）
partial_order	TCP オプション 9（Partial Order Connection Permitted）および 10（Partial Order Service Profile）
conn_count	TCP 接続カウント オプション 11（CC）、12（CC.New）、および 13（CC.Echo）
alt_checksum	TCP オプション 14（Alternate Checksum Request）および 15（Alternate Checksum）
md5	TCP オプション 19（MD5 Signature）
オプション番号 2 ～ 255	キーワードのないオプションを含む、特定のオプション
any	すべての TCP オプション（この設定は、実質的に TCP オプションの正規化を無効にします。）

このオプションに `any` を指定しない場合、正規化には次のものが含まれます。

- MSS、ウィンドウ スケール、タイムスタンプ、およびその他の明示的に許可されたオプションを除き、すべてのオプションのバイトを [No Operation]（TCP オプション 1）に設定します。
- タイムスタンプは存在していても無効な場合、あるいは有効であってもネゴシエートされない場合、タイムスタンプ オクテットを [No Operation] に設定します。
- タイムスタンプがネゴシエートされるものの、存在しない場合、パケットをブロックします。

- 確認応答（ACK）制御ビットが設定されていない場合、[Time Stamp Echo Reply (TSecr)] オプション フィールドをクリアします。
- SYN 制御ビットが設定されていない場合、[MSS] および [Window Scale] オプションを [No Operation]（TCP オプション 1）に設定します。

インライン正規化プリプロセッサを設定するには、以下を行います。

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーでまだ保存されていない変更がある場合、それらの変更を破棄して続行するには [OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Edit Policy] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Transport/Network Layer Preprocessors] で [Inline Normalization] が有効にされているかどうかによって、以下の 2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- この設定が無効にされている場合、[Enabled] をオンにしてから、[Edit] をクリックします。

[Inline Normalization] ページが表示されます。ページ下部のメッセージは、設定を含むポリシー層を示します。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　インライン トラフィックの正規化（29-7 ページ）で説明されている任意のオプションを設定できます。

ステップ 6　ポリシーを保存するか、編集を続けるか、変更を破棄するか、基本ポリシーのデフォルト構成設定に戻すか、あるいはシステム キャッシュに変更を残して終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

IP パケットのデフラグ

ライセンス： Protection

最大伝送単位（MTU）より大きいために IP データグラムが複数の小さい IP データグラムに分割されると、その IP データグラムは*フラグメント化*されたことになります。単一の IP データグラム フラグメントには、隠れた攻撃を識別するのに十分な情報が含まれない場合があります。そのため、攻撃者はエクスプロイトの検出を免れるために、フラグメント化されるパケットで攻撃データを送信する可能性があります。IP デフラグ プリプロセッサは、ルール エンジンが IP データグラムに対してルールを実行する前に、パケットに仕込まれた攻撃をルールで識別しやすくするために、フラグメント化された IP データグラムを再アセンブリします。フラグメント化されたデータグラムを再アセンブルできない場合、それらのデータグラムに対しては、ルールが実行されません。

IP デフラグ プリプロセッサのルールにイベントを生成させるには、これらのルール（ジェネレータ ID（GID）が 123 のルール）を有効にする必要があります。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

詳細については、次の項を参照してください。

IP フラグメント化のエクスプロイトについて

ライセンス：Protection

IP デフラグを有効にすると、ネットワーク上のホストに対する攻撃（ディアドロップ攻撃など）や、システム自体に対するリソース消費攻撃（Jolt2 攻撃など）を検出するのに役立ちます。

ティアドロップ攻撃は、特定のオペレーティング システムのバグを悪用して、そのオペレーティング システムがオーバーラップした IP フラグメントを再アセンブルしようとするとクラッシュするように仕掛けます。IP デフラグ プリプロセッサを有効にして、オーバーラップしたフラグメントを識別するように設定すれば、該当するフラグメントを識別できます。IP デフラグ プリプロセッサは、ティアドロップ攻撃などのオーバーラップ フラグメント攻撃で、最初のパケットだけを検出するだけで、同じ攻撃での後続のパケットは検出しません。

Jolt2 攻撃では、IP デフラグ機能を酷使させるという方法でサービス拒絶攻撃を仕掛けるために、フラグメント化された同じ IP パケットのコピーを大量に送信します。IP デフラグ プリプロセッサでは、メモリ使用量の上限によって、このような攻撃を阻止し、包括的検査においてシステムを自己防衛状態にします。システムは攻撃によって過負荷にならず、運用可能な状態を維持し、ネットワーク トラフィックの検査を続行します。

フラグメント化されたパケットを再アセンブルする方法は、オペレーティング システムによって異なります。ホストがどのオペレーティング システムで実行されているのかを攻撃者が特定できれば、その攻撃者はターゲット ホストが特定の方法で再アセンブルするように不正なパケットをフラグメント化することも可能です。モニタ対象のネットワーク上でホストを実行しているオペレーティング システムは、システムには不明です。したがって、プリプロセッサがパケットを誤った方法で再アセンブリして検査し、それによってエクスプロイトが検出されないままパススルーする可能性があります。このような攻撃を軽減するために、ネットワーク上のホストごとに適切な方法でパケットをデフラグするよう、デフラグ プリプロセッサを設定できるようになっています。詳細については、「ターゲットベースのデフラグ ポリシー（29-14 ページ）」を参照してください。

パケットのターゲット ホストのオペレーティング システム情報に応じて、IP デフラグ プリプロセッサに適用するターゲットベースのポリシーが動的に選択されるように、適応型プロファイルを使用して設定できます。詳細については、パッシブ展開における前処理の調整（30-1 ページ）を参照してください。

ターゲットベースのデフラグ ポリシー

ライセンス：Protection

ホストのオペレーティング システムは、パケットを再アセンブルする際に優先するパケット フラグメントを判断するために、3 つの基準を使用します。それは、オペレーティング システムがフラグメントを受信した順序、フラグメントのオフセット（パケットの先頭からのフラグメントの距離（バイト単位））、オーバーラップ フラグメントとの相対開始位置および終了位置です。これらの基準はすべてのオペレーティング システムで使用されているものの、フラグメント化されたパケットを再アセンブルするときに優先するフラグメントは、オペレーティング システムによって異なります。したがって、ネットワーク上で異なるオペレーティング システムを使用する 2 台のホストが、同じオーバーラップ フラグメントをまったく異なる方法で再アセンブルする場合も考えられます。

いずれかのホストのオペレーティング システムを認識している攻撃者が、オーバーラップしたパケット フラグメントに不正なコンテンツを忍ばせて送信することによって、エクスプロイトの検出を免れ、そのホストを悪用する可能性があります。このパケットが他のホストで再アセンブルされて検査されても、パケットに害はないように見えますが、ターゲット ホストで再アセンブルされる場合には不正なエクスプロイトが含まれています。ただし、モニタ対象のネットワーク セグメントで稼働するオペレーティング システムを認識するように IP デフラグ プリプロセッサを設定すれば、このプリプロセッサがターゲット ホストと同じ方法でフラグメントを再アセンブルすることによって、攻撃を識別できます。

ターゲット ホストのオペレーティング システムに応じて、7 つのデフラグ ポリシーのうちのいずれかを使用するように IP デフラグ プリプロセッサを設定できます。以下の表に、7 つのポリシーと、それぞれのポリシーを使用するオペレーティング システムを記載します。First と Last というポリシー名は、これらのポリシーが元のオーバーラップ パケットまたは後続のオーバーラップ パケットのどちらを優先するかを反映しています。

表 29-1　ターゲットベースのデフラグ ポリシー

ポリシー（Policy）	オペレーティング システム
BSD	AIX
	FreeBSD
	IRIX
	VAX/VMS
BSD-right	HP JetDirect
First	Mac OS
	HP-UX
Linux	Linux
	OpenBSD
Last	Cisco IOS
Solaris	SunOS
Windows	Windows

デフラグ オプションの選択

ライセンス：Protection

IP デフラグを有効または無効にすることだけを選択することもできますが、Ciscoでは、それよりも粒度の細かいレベルで、有効にする IP デフラグ プリプロセッサの動作を指定するよう推奨しています。

次の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

グローバル [Preallocated Fragments] オプションを設定できます。

Preallocated Fragments

プリプロセッサが一度に処理できる個々のフラグメントの最大数。事前割り当てするフラグメント ノードの数を指定すると、静的メモリ割り当てが有効になります。

注意 個々のフラグメントの処理には、約 1550 バイトのメモリが使用されます。プリプロセッサで個々のフラグメントを処理するために必要なメモリが、管理対象デバイスに事前定義された使用可能なメモリ量の制限を上回る場合は、管理対象デバイスのメモリ制限が優先されます。

IP デフラグ ポリシーごとに、以下のオプションを設定できます。

Networks

デフラグ ポリシーを適用するホスト（複数可）の IP アドレス。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をコンマで区切ったリストを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のプロファイルを指定できます。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-23 ページ）を参照してください。

デフォルト ポリシーの**デフォルト**設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィクス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、**すべて** を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

また、ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となるネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、「ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）」を参照してください。

ポリシー（Policy）

モニタ対象ネットワーク セグメント上のホスト一式に使用するデフラグ ポリシー。7 つのポリシー（BSD、BSD-Right、First、Linux、Last、Solaris、Windows）の中から選択できます。これらのポリシーの詳細については、ターゲットベースのデフラグ ポリシー（29-14 ページ）を参照してください。

Timeout

プリプロセッサ エンジンがフラグメント化されたパケットを再アセンブルする際に使用できる最大時間（秒数）を指定します。指定された時間内にパケットを再アセンブルできない場合、プリプロセッサ エンジンはパケットの再アセンブリ試行を停止し、受信したフラグメントを破棄します。

Minimum TTL

パケットに許容される最小 TTL 値を指定します。このオプションは、TTL ベースの挿入攻撃を検出します。

このオプションに対するイベントを生成するには、ルール 123:1 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Detect Anomalies

オーバーラップ フラグメントのようなフラグメンテーション問題を識別します。

以下のルールを有効にすることで、このオプションに対するイベントを生成できます。

- 123:1 ～123:4
- 123:5（BSD ポリシー）
- 123:6 ～123:8

Overlap Limit

セッションでデフラグを停止する条件とする、セッションでのオーバーラップ セグメントの検出数を 0（無制限）～ 255 の範囲で指定します。このオプションを設定するには、[Detect Anomalies] を有効にする必要があります。値が空白の場合、このオプションを無効になります。

このオプションに対するイベントを生成するには、ルール 123:12 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Minimum Fragment Size

パケットを不正と見なす条件とする、検出されたフラグメント（最後のフラグメントを除く）の最小サイズを 0（無制限）～ 255 バイトの間で指定します。このオプションを設定するには、[Detect Anomalies] を有効にする必要があります。値が空白の場合、このオプションを無効になります。

このオプションに対するイベントを生成するには、ルール 123:13 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

IP デフラグの設定

ライセンス： Protection

IP デフラグ プリプロセッサを設定するには、次の手順を実行します。IP デフラグ プリプロセッサの設定オプションの詳細については、デフラグ オプションの選択（29-15 ページ）を参照してください。

IP デフラグを設定するには、以下を行います。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Edit Policy] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Transport/Network Layer Preprocessors] で [IP Defragmentation] が有効にされているかどうかによって、以下の 2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- この設定が無効にされている場合、[Enabled] をオンにしてから、[Edit] をクリックします。

[IP Defragmentation] ページが表示されます。ページ下部のメッセージは、設定を含むポリシー層を示します。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　必要に応じて、[Global Settings] ページ領域にある [Preallocated Fragments] の設定を変更できます。

ステップ 6　次の 2 つのオプションから選択できます。

- 新しいターゲットベースのポリシーを追加します。ページの左側で [Servers] の横にある追加アイコン（  ）をクリックします。[Add Target] ポップアップ ウィンドウが表示されます。[Host Address] フィールドに 1 つまたは複数の IP アドレスを指定し、[OK] をクリックします。

  単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をコンマで区切ったリストを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のターゲットベースのポリシーを作成できます。FireSIGHT システムで IP アドレス ブロックを使用する方法については、IP アドレスの表記規則（1-23 ページ）を参照してください。

  ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となるネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、「ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）」を参照してください。

  ページの左側にあるターゲットのリストに新しいエントリが表示されます。このエントリは、強調表示によって選択された状態であることが示されます。また、[Configuration] セクションが更新されて、追加したポリシーの現在の構成が反映されます。

- 既存のターゲットベースのポリシーの設定を変更します。ページの左側の [Hosts] に追加されているポリシーの設定済みアドレスをクリックするか、[default] をクリックします。

  選択したエントリが強調表示され、[Configuration] セクションが更新されて、選択したポリシーの現在の設定が表示されます。既存のターゲットベースのポリシーを削除するには、削除するポリシーの横にある削除アイコン（  ）をクリックします。

ステップ 7　オプションで、[Configuration] ページ領域にあるオプションのいずれかを変更できます。

ステップ 8　ポリシーを保存するか、編集を続けるか、変更を破棄するか、基本ポリシーのデフォルト構成設定に戻すか、あるいはシステム キャッシュに変更を残して終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

パケットのデコードについて

ライセンス： Protection

キャプチャしたパケットをプリプロセッサに送信する前に、システムはパケットをパケット デコーダに送信します。パケット デコーダは、プリプロセッサやルール エンジンが容易に使用できる形式に、パケット 見出しおよびペイロードを変換します。データ リンク層から開始して、ネットワーク層、トランスポート層へと、各スタック層が順にデコードされます。

注意すべき点として、パケット デコーダのルールにイベントを生成させるには、これらのルール（ジェネレータ ID（GID）が 116 のルール）を有効にする必要があります。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

次の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

Decode GTP Data Channel

カプセル化された GTP（General Packet Radio Service（GPRS）トンネリング プロトコル）データ チャネルをデコードします。デフォルトでは、デコーダはポート 3386 ではバージョン 0 のデータをデコードし、ポート 2152 ではバージョン 1 のデータをデコードします。GTP_PORTS デフォルト変数を使用して、カプセル化された GTP トラフィックを識別するポートを変更できます。詳細については、「定義済みのデフォルトの変数の最適化（3-20 ページ）」を参照してください。

このオプションに対するイベントを生成するには、ルール 116:297 および 116:298 を有効にします。

非標準ポートでの Teredo の検出

ポート 3544 以外の UDP ポートで識別される IPv6 トラフィックの Teredo トンネリングを検査します。

IPv6 トラフィックが存在する場合、システムは常にこのトラフィックを検査します。デフォルトでは、IPv6 インスペクションには 4in6、6in4、6to4、および 6in6 トンネリング方式が含まれます。また、UDP 見出しがポート 3544 を指定している場合は、Teredo トンネリングも含まれます。

IPv4 ネットワークでは、IPv4 ホストが Teredo プロトコルを使用して、IPv4 Network Address Translation（NAT）デバイスを介して IPv6 トラフィックをトンネリングできます。Teredo は、IPv6 パケットを IPv4 UDP データグラムにカプセル化して、IPv4 NAT デバイスの背後で IPv6 接続を許可します。システムは通常、UDP ポート 3544 を使用して Teredo トラフィックを識別します。ただし、攻撃者が検出を免れるために標準以外のポートを使用する可能性も考えられます。[Detect Teredo on Non-Standard Ports] を有効にすることで、システムに Teredo トンネリングのすべての UDP ペイロードを検査させることができます。

Teredo のデコードは、外側のネットワーク層に IPv4 が使用されている場合に限り、最初の UDP 見出しに対してのみ行われます。UDP データが IPv6 データにカプセル化されるため、Teredo IPv6 層の後に 2 つめの UDP 層が存在する場合、ルール エンジンは UDP 侵入ルールを使用して、内側および外側の両方の UDP 層を分析します。

policy-other ルール カテゴリの侵入ルール 12065、12066、12067、および 12068 は Teredo トラフィックを検出しますが、デコードはしないことに注意してください。必要に応じて、これらのルールを使用してインライン展開で Teredo トラフィックをドロップすることができます。ただし、[Detect Teredo on Non-Standard Ports] を有効にする場合は、これらのルールが無効にされるか、トラフィックをドロップせずにイベントを生成するように設定される必要があります。詳細については、侵入ポリシー内のルールのフィルタ処理（32-10 ページ）およびルール状態の設定（32-22 ページ）を参照してください。

Detect Excessive Length Value

パケット 見出しが実際のパケット長を超えるパケット長を指定しているかどうかを検出します。

このオプションに対するイベントを生成するには、ルール 116:6、116:47、116:97、および 116:275 を有効にします。

Detect Invalid IP Options

無効な IP オプションを使用したエクスプロイトを識別するために、無効な IP 見出し オプションを検出します。たとえば、ファイアウォールに対するサービス拒絶攻撃は、システムをフリーズさせる原因になります。ファイアウォールが無効なタイムスタンプおよび IP セキュリティ オプションを解析しようとして、ゼロ長のチェックに失敗すると、回復不可能な無限ループが発生します。ルール エンジンはゼロ長のオプションを識別し、ファイアウォールでの攻撃を軽減するために使用できる情報を提供します。

このオプションに対するイベントを生成するには、ルール 116:4 および 116:5 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Detect Experimental TCP Options

試験的 TCP オプションが設定された TCP 見出しを検出します。以下の表は、それらのオプションを示しています。

TCP オプション	説明
9	Partial Order Connection Permitted
10	Partial Order Service Profile
14	Alternate Checksum Request
15	Alternate Checksum Data
18	Trailer Checksum
20	Space Communications Protocol Standards（SCPS）
21	Selective Negative Acknowledgements（SCPS）
22	Record Boundaries（SCPS）
23	Corruption（SPCS）
24	SNAP
26	TCP Compression Filter

これらのオプションは試験的なものであるため、一部のシステムでは考慮されず、悪用される恐れがあります。

注　上記の表に記載されている試験的オプションに加えて、26 より大きいオプション番号を持つ TCP オプションは、試験的オプションと見なされます。

このオプションに対するイベントを生成するには、ルール 116:58 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Detect Obsolete TCP Options

廃止された TCP オプションが設定された TCP 見出しを検出します。これらのオプションは廃止されたものであるため、一部のシステムでは考慮されず、悪用される恐れがあります。以下の表は、それらのオプションを示しています。

TCP オプション	説明
6	Echo
7	Echo Reply
16	Skeeter
17	Bubba
19	MD5 Signature
25	未割り当て

このオプションに対するイベントを生成するには、ルール 116:57 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Detect T/TCP

CC.ECHO オプションが設定された TCP 見出しを検出します。CC.ECHO オプションは、TCP for Transactions (T/TCP) が使用されていることを確認します。T/TCP 見出し オプションは幅広く使用されてはいないため、一部のシステムでは考慮されず、悪用される恐れがあります。

このオプションに対するイベントを生成するには、ルール 116:56 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Detect Other TCP Options

他の TCP デコード イベント オプションでは検出されない無効な TCP オプションが設定された TCP 見出しを検出します。たとえば、このオプションは、無効な長さ、またはオプション データが TCP 見出しに収まらない長さの TCP オプションを検出します。

このオプションに対するイベントを生成するには、ルール 116:54、116:55、および 116:59 を設定します。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Detect Protocol Header Anomalies

より具体的な IP および TCP デコード オプションでは検出されない他のデコード エラーを検出します。たとえば、このデコーダは、不正な形式のデータ リンク プロトコル ヘッダーを検出する場合があります。

このオプションに対するイベントを生成するには、他のパケット デコーダ オプションに明示的に関連付けられていないパケット デコーダのルールを有効にします。詳細については、ルール状態の設定（32-22 ページ）を参照してください。

異常な IPv6 トラフィックによってトリガーされるイベントを生成するルールは、116:270 ～ 116:274、116:275 ～ 116:283、116:291、116:292、116:295、116:296、116:406、116:458、116:460、116:461 です。

インライン正規化プリプロセッサの [Minimum TTL] オプションに関連する以下のルールについても注意してください。

- 指定の最小値を下回る TTL が設定された IPv4 パケットが検出された場合にイベントを生成するには、ルール 116:428 を有効にします。
- 指定の最小値を下回るホップ リミットが設定された IPv6 パケットが検出された場合にイベントを生成するには、ルール 116:270 を有効にします。

詳細については、インライン トラフィックの正規化（29-7 ページ）のインライン正規化の [Minimum TTL] オプションを参照してください。

パケットのデコードの設定

ライセンス： Protection

パケットのデコードは、[Packet Decoding] 設定ページで設定できます。パケットのデコード設定オプションの詳細については、パケットのデコードについて（29-18 ページ）を参照してください。

パケットのデコードを設定するには、以下を行います。

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーで保存されていない変更がある場合は、[OK] をクリックして変更を破棄し、操作を続けます。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Edit Policy] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Transport/Network Layer Preprocessors] で [Packet Decoding] が有効にされているかどうかによって、以下の 2 つの選択肢があります。

- この設定が有効にされている場合、[Edit] をクリックします。
- この設定が無効にされている場合、[Enabled] をオンにしてから、[Edit] をクリックします。

[Packet Decoding] ページが表示されます。ページ下部のメッセージは、設定を含むポリシー層を示します。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

ステップ 5　[Packet Decoding] ページの任意の検出オプションを有効または無効にできます。詳細については、「パケットのデコードについて（29-18 ページ）」を参照してください。

ステップ 6　ポリシーを保存するか、編集を続行するか、変更内容を破棄するか、ベース ポリシーのデフォルト設定に戻すか、またはシステム キャッシュの変更を反映せずに終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

TCP ストリームの前処理の使用

ライセンス： Protection

TCP プロトコルは、接続で生じ得るさまざまな状態を定義します。各 TCP 接続は、送信元と宛先の IP アドレス、および送信元と宛先のポートによって識別されます。TCP では、接続パラメータ値が同じ接続は、一度に 1 つしか存在できません。

TCP ストリーム プリプロセッサのルールにイベントを生成させるには、それらのルール（ジェネレータ ID（GID）が 129 のルール）を有効にする必要があります。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

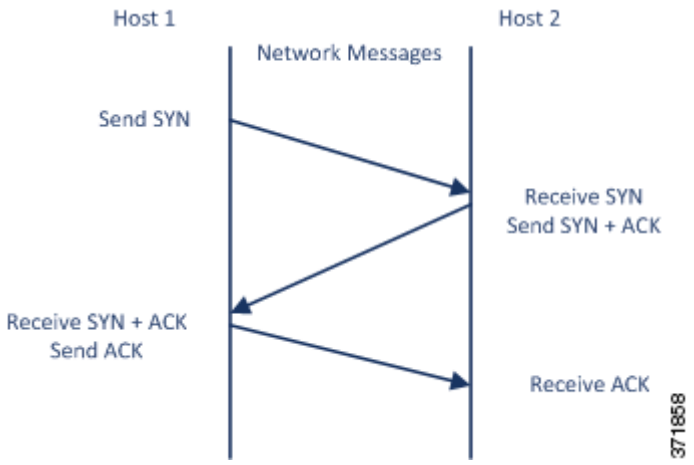
詳細については、次の項を参照してください。

- 状態関連の TCP エクスプロイトについて（29-22 ページ）
- 侵入廃棄ルールでのアクティブ応答の開始（29-3 ページ）
- TCP グローバル オプションの選択（29-23 ページ）
- ターゲットベースの TCP ポリシーについて（29-23 ページ）
- TCP ポリシーのオプションの選択（29-25 ページ）
- TCP ストリームの再アセンブリ（29-29 ページ）
- TCP ストリームの前処理の設定（29-32 ページ）

状態関連の TCP エクスプロイトについて

ライセンス： Protection

侵入ルールに `established` 引数と組み合わせた `flow` キーワードを追加すると、侵入ルール エンジンはステートフル モードでルールとフロー ディレクティブに一致するパケットを検査します。ステートフル モードでは、クライアントとサーバの間で正当なスリーウェイ ハンドシェイクによって確立された TCP セッションの一部であるトラフィックだけが評価されます。以下の図に、スリーウェイ ハンドシェイクを示します。



確立された TCP セッションの一部として識別できない TCP トラフィックをプリプロセッサが検出するように、システムを設定することは可能です。しかし、このようなイベントは、システムをすぐに過負荷状態に陥らせ、しかも意味のあるデータを提供しないため、通常の使用法では推奨されません。

Stick や Snot などの攻撃では、システムの自身に対する広範なルール セットとパケット インスペクションを悪用します。これらのツールは、Snort ベースの侵入ルールのパターンに基づいてパケットを生成し、ネットワークに送信します。ステートフル インスペクションに対して設定するルールに `flow` または `flowbits` キーワードを含めなければ、パケットのそれぞれがルールをトリガーするため、システムが過負荷状態になります。ステートフル インスペクションを使用することで、確立された TCP セッションに含まれず、意味のある情報を提供しないこれらのパケットを無視できます。ステートフル インスペクションを実行すると、ルール エンジンは確立された TCP セッションに含まれる攻撃のみを検出するため、アナリストが stick や snot によって大量に生成されるイベントに時間を取られることがなくなります。

TCP グローバル オプションの選択

ライセンス：Protection

TCP ストリーム プリプロセッサには、TCP ストリーム プリプロセッサの動作を制御するグローバル オプションが 1 つあります。

プリプロセッサ ルールは、このオプションに関連付けられていません。

Packet Type Performance Boost

送信元ポートおよび宛先ポートの両方を `any` に設定した TCP ルールで、`flow` または `flowbits` オプションが使用されている場合を除き、有効化された侵入ルールに指定されていないポートおよびアプリケーション プロトコルのすべてについて、TCP トラフィックを無視するように設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。

ターゲットベースの TCP ポリシーについて

ライセンス：Protection

オペレーティング システムによって、TCP の実装方法は異なります。たとえば、セッションをリセットするために、Windows やその他のオペレーティング システムの一部では TCP リセット セグメントに正確な TCP シーケンス番号を割り当てる必要があるのに対し、Linux や他のオペレーティング システムではシーケンス番号の範囲を使用できます。この例の場合、ストリーム プリプロセッサは、シーケンス番号に基づき、宛先ホストがリセットにどのように応答するかを正確に把握しなければなりません。ストリーム プリプロセッサがセッションの追跡を停止するのは、宛先ホストがリセットが有効であると見なした場合のみです。したがって、プリプロセッサがストリームの検査を停止した後は、パケットを送信することによって攻撃が検出を免れることはできません。TCP の実装方法の違いには、オペレーティング システムで TCP タイムスタンプ オプションを採用しているかどうか、採用している場合にはどのようにタイムスタンプを処理するか、そしてオペレーティング システムで SYN パケットのデータを受け入れるか、無視するかどうかも含まれます。

また、オーバーラップ TCP セグメントを再アセンブルする方法も、オペレーティング システムによって異なります。オーバーラップ TCP セグメントは、確認応答済み TCP トラフィックの通常の再送信を反映する場合があります。あるいは、ホストのオペレーティング システムを認識している攻撃者が、エクスプロイトの検出を免れるためにオーバーラップ セグメントに不正なコンテンツを忍ばせて送信し、そのホストを悪用しようとしている場合もあります。ただし、モニ

タ対象のネットワーク上で稼働するオペレーティング システムを認識するようにストリーム プリプロセッサを設定すれば、そのプリプロセッサがターゲット ホストと同じ方法でセグメントを再アセンブルすることによって、攻撃を識別できます。

モニタ対象のネットワーク セグメント上のさまざまなオペレーティング システムに合わせて TCP ストリーム インスペクションおよび再アセンブリを調整するために、1 つ以上の TCP ポリシーを作成することができます。ポリシーごとに、13 のオペレーティング システム ポリシーのうちの 1 つを特定します。異なるオペレーティング システムを使用するホストのいずれか、あるいはすべてを識別するために必要な数だけ TCP ポリシーを使用し、各 TCP ポリシーを特定の IP アドレスまたはアドレス ブロックにバインドします。デフォルトの TCP ポリシーは、他の TCP ポリシーで指定されていないモニタ対象ネットワーク上のすべてのホストに適用されます。したがって、デフォルトの TCP ポリシーに IP アドレス、CIDR ブロック、またはプレフィクス長を指定する必要はありません。

パケットのターゲット ホストのオペレーティング システム情報に応じて、TCP ストリーム プリプロセッサに適用するターゲットベースのポリシーが動的に選択されるように、適応型プロファイルを使用することもできます。詳細については、パッシブ展開における前処理の調整（30-1 ページ）を参照してください。

以下の表に、オペレーティング システム ポリシーとそれを使用するホスト オペレーティング システムをリストします。

表 29-2　TCP オペレーティング システム ポリシー

ポリシー（Policy）	オペレーティング システム
First	不明な OS
Last	Cisco IOS
BSD	AIX FreeBSD OpenBSD
Linux	Linux 2.4 カーネル Linux 2.6 カーネル
古い Linux	Linux 2.2 以前のカーネル
Windows	Windows 98 Windows NT の場合 Windows 2000 Windows XP
Windows 2003	Windows 2003
Windows Vista	Windows Vista
Solaris	Solaris OS SunOS
IRIX	SGI Irix
HPUX	HP-UX 11.0 以降
HPUX 10	HP-UX 10.2 以前
Mac OS	Mac OS 10（Mac OS X）

ヒント　First オペレーティング システム ポリシーは、ホストのオペレーティング システムが不明な場合にはある程度の保護対策になります。ただし、攻撃を見逃す可能性もあります。オペレーティング システムが既知であれば、ポリシーを編集して、その正しいオペレーティング システムを指定してください。

TCP ポリシーのオプションの選択

ライセンス： Protection

以下に、ストリーム プリプロセッサの検査対象とする TCP トラフィックを識別して制御するために設定できるオプションをリストし、説明します。

次の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ネットワーク

TCP ストリーム再アセンブリ ポリシーを適用するホストの IP アドレスを指定します。

単一の IP アドレスまたはアドレス ブロックを指定できます。デフォルト ポリシーを含め、最大で合計 255 個のプロファイルを指定できます。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-23 ページ）を参照してください。

デフォルト ポリシーの**デフォルト**設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィクス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、**すべて** を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

また、ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となるネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、「ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）」を参照してください。

ポリシー

TCP ポリシーを適用するターゲット ホスト（複数可）のオペレーティング システムを識別します。[Mac OS] 以外のポリシーを選択すると、システムは同期（SYN）パケットからデータを削除し、ルール 129:2 に対するイベントの生成を無効にします。

詳細については、ターゲットベースの TCP ポリシーについて（29-23 ページ）を参照してください。

Timeout

侵入ルール エンジンが非アクティブなストリームを状態テーブルで保持する秒数（1 ～ 86400 秒）。指定された期間内にストリームが再アセンブルされない場合、侵入ルール エンジンはそのストリームを状態テーブルから削除します。

注　ネットワーク トラフィックがデバイスの帯域幅制限に到達しやすいセグメントに、管理対象デバイスが展開されている場合は、処理のオーバーヘッド量を削減するために、この値を大きい値（たとえば、600 秒）に設定することを検討する必要があります。

Maximum TCP Window

受信側ホストで指定されている TCP ウィンドウの最大許容サイズを 1 ～ 1073725440 バイトの範囲で指定します。値を 0 に設定すると、TCP ウィンドウ サイズのチェックが無効になります。

注意　上限は RFC で許可される最大ウィンドウ サイズです。これは、攻撃者が検出を回避できないようにすることを目的としていますが、あまりにも大きな最大ウィンドウ サイズを設定すると、システム自体がサービス拒絶を招く可能性があります。

このオプションに対するイベントを生成するには、ルール 129:6 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Overlap Limit

セッションで許容するオーバーラップ セグメントの数を 0（無制限）～ 255 の範囲で指定します。セッションで、この指定された値に達すると、セグメントの再アセンブリが停止します。[Stateful Inspection Anomalies] が有効にされていて、それに付随するプリプロセッサ ルールが有効にされている場合、イベントも生成されます。

このオプションに対するイベントを生成するには、ルール 129:7 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Flush Factor

インライン展開では、ここで設定するサイズ減少なしのセグメントの数（1 ～ 2048）の後にサイズが減少したセグメントが検出されると、システムは検出用に累積されたセグメント データをフラッシュします。値を 0 に設定すると、要求または応答の終わりを示す可能性のあるこのセグメント パターンの検出が無効になります。このオプションを有効にするには、インライン正規化の [Normalize TCP Payload] オプションを有効にする必要があることに注意してください。詳細については、「インライン トラフィックの正規化（29-7 ページ）」を参照してください。

Stateful Inspection Anomalies

TCP スタックの異常な動作を検出します。付随するプリプロセッサ ルールが有効にされている場合、TCP/IP スタックが不完全に作成されていると、多数のイベントが生成される可能性があります。

以下のルールを有効にすることで、このオプションに対するイベントを生成できます。

- 129:1 ～129:5
- 129:6（Mac OS のみ）
- 129:8 ～129:11
- 129:13 ～129:19

詳細については、ルール状態の設定（32-22 ページ）を参照してください。

TCP Session Hijacking

スリーウェイ ハンドシェイク中に TCP 接続の両端から検出されたハードウェア（MAC）アドレスの有効性を、セッションで受信した後続のパケットに照合して検査することにより、TCP セッション ハイジャックを検出します。[Stateful Inspection Anomalies] が有効にされていて、2 つの対応するプリプロセッサ ルールのいずれかが有効にされている場合、接続のどちらかの側の MAC アドレスが一致しないと、システムがイベントを生成します。

このオプションに対するイベントを生成するには、ルール 129:9 および 129:10 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Consecutive Small Segments

[Stateful Inspection Anomalies] が有効にされている場合、連続する小さな TCP セグメントの許容数を 1 ～ 2048 の範囲で指定します。値を 0 に設定すると、連続する小さな TCP セグメントのチェックが無効になります。

このオプションは、[Small Segment Size] オプションと同時に設定し、両方とも無効にするか、両方にゼロ以外の値を設定する必要があります。通常は、それぞれのセグメントの長さが 1 バイトであったとしても、ACK が介在することなく 2000 個もの連続するセグメントを受信することはないので注意してください。

このオプションに対するイベントを生成するには、ルール 129:12 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

Small Segment Size

[Stateful Inspection Anomalies] が有効にされている場合、小さいと見なされる TCP セグメントのサイズを 1 ～ 2048 バイトの範囲で指定します。値を 0 に設定すると、小さいセグメントのサイズの指定が無効になります。

このオプションは、[Consecutive Small Segments] オプションと同時に設定し、両方とも無効にするか、両方にゼロ以外の値を設定する必要があります。2048 バイトの TCP セグメントは、標準的な 1500 バイトのイーサネット フレームより大きいことに注意してください。

Ports Ignoring Small Segments

[Stateful Inspection Anomalies]、[Consecutive Small Segments]、および [Small Segment Size] が有効にされている場合、必要に応じて、小さい TCP セグメントの検出を無視する 1 つ以上のポートのカンマ区切りリストを指定します。このオプションを空白のままにすると、ポートはすべて無視されないように指定されます。

リストには任意のポートを追加できますが、このリストが適用されるのは、TCP ポリシーの [Perform Stream Reassembly on] ポート リストに指定されているポートのみです。

Require TCP 3-Way Handshake

TCP スリーウェイ ハンドシェイクの完了時に確立されたセッションだけを処理することを指定します。パフォーマンスを向上させ、SYN フラッド攻撃から保護し、部分的に非同期の環境での運用を可能にするには、このオプションを無効にします。確立された TCP セッションには含まれていない情報を送信して誤検出を発生させようとする攻撃を回避するには、このオプションを有効にします。

このオプションに対するイベントを生成するには、ルール 129:20 を有効にします。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。

3-Way Handshake Timeout

[Require TCP 3-Way Handshake] が有効にされている場合、ハンドシェイクを完了するまでの時間制限を 0（無制限）～ 86400 秒（24 時間）の範囲で指定します。このオプションの値を変更するには、[Require TCP 3-Way Handshake] を有効にする必要があります。

Packet Size Performance Boost

再アセンブリ バッファで大きいパケットをキューに入れないようにプリプロセッサを設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。1 ～ 20 バイトの小さなパケットを使用した検出回避の試行から保護するには、このオプションを無効にします。すべてのトラフィックが非常に大きなパケットからなるため、そのような攻撃は起こらないと確信できる場合は、このオプションを有効にします。

Legacy Reassembly

パケットを再アセンブルする際に、廃止されたストリーム 4 プリプロセッサをエミュレートするようにストリーム プリプロセッサを設定します。これにより、ストリーム プリプロセッサで再アセンブルされたイベントを、ストリーム 4 プリプロセッサで再アセンブルされた、同じデータ ストリームに基づくイベントと比較できます。

Asynchronous Network

モニタ対象ネットワークが非同期ネットワーク（システムにトラフィックの半分だけが見えるネットワーク）であるかどうかを指定します。このオプションを有効にすると、システムは TCP ストリームを再アセンブリしないため、パフォーマンスが向上します。

Perform Stream Reassembly on Client Ports, Server Ports, Both Ports

ストリーム プリプロセッサの再アセンブリ対象とするトラフィックを識別するクライアント ポート、サーバ ポート、またはその両方のカンマ区切りリストを指定します。ストリームの再アセンブリのオプションの選択（29-29 ページ）を参照してください。

Perform Stream Reassembly on Client Services, Server Services, Both Services

ストリーム プリプロセッサの再アセンブリ対象とするトラフィックで識別するクライアント サービス、サーバ サービス、またはその両方のサービスを指定します。ストリームの再アセンブリのオプションの選択（29-29 ページ）を参照してください。

トラブルシューティング オプション：Maximum Queued Bytes

トラブルシューティングの電話中に、TCP 接続の片側でキューイングできるデータの量を指定するようにサポートから依頼される場合があります。値 0 は、無制限のバイト数を指定します。

注意　このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイダンスに従って実行してください。

トラブルシューティング オプション：Maximum Queued Segments

トラブルシューティングの電話中に、TCP 接続の片側でキューイングできるデータ セグメントの最大バイト数を指定するようにサポートから依頼される場合があります。値 0 は、無制限のデータ セグメント バイト数を指定します。

注意　このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイダンスに従って実行してください。

TCP ストリームの再アセンブリ

ライセンス：Protection

ストリーム プリプロセッサは、TCP セッションでのサーバからクライアントへの通信ストリーム、クライアントからサーバへの通信ストリーム、またはその両方の通信ストリームに含まれるすべてのパケットを収集して再アセンブルします。これにより、ルール エンジンは、特定のストリームに含まれる個々のパケットだけを検査するのではなく、ストリームを再アセンブルされた単一のエンティティとして検査できます。

詳細については、次の項を参照してください。

- ストリームベースの攻撃について（29-29 ページ）
- ストリームの再アセンブリのオプションの選択（29-29 ページ）

ストリームベースの攻撃について

ライセンス：Protection

ストリームの再アセンブリにより、ルール エンジンは、個々のパケットを検査する場合には検出できない可能性のあるストリームベースの攻撃を識別できます。ルール エンジンの再アセンブリ対象とする通信ストリームは、ネットワークのニーズに応じて指定できます。たとえば、Web サーバ上のトラフィックをモニタする際に、独自の Web サーバから不正なトラフィックを受信する可能性がほとんどないため、クライアント トラフィックだけを検査するという場合もあります。

ストリームの再アセンブリのオプションの選択

ライセンス：Protection

各 TCP ポリシーに、ストリーム プリプロセッサが再アセンブルするトラフィックを識別するポートのカンマ区切りのリストを指定できます。適応型プロファイルが有効にされている場合、再アセンブルするトラフィックを識別するサービスを、ポートの代わりとして、あるいはポートと組み合わせてリストすることもできます。適応型プロファイルを有効にして使用する方法については、パッシブ展開における前処理の調整（30-1 ページ）を参照してください。

ポート、サービス、またはその両方を指定できます。クライアント ポート、サーバー ポート、またはその両方を任意に組み合わせた個別のポート リストを指定できます。また、クライアント サービス、サーバ サービス、またはその両方を任意に組み合わせた個別のサービス リストを指定することもできます。たとえば、以下を再アセンブルする必要があるとします。

- クライアントからの SMTP（ポート 25）トラフィック
- FTP サーバ応答（ポート 21）
- 両方向の Telnet（ポート 23）トラフィック

この場合、以下のように設定できます。

- クライアント ポートとして、`23, 25` を指定
- サーバ ポートとして、`21, 23` を指定

あるいは、以下のように設定することもできます。

- クライアント ポートとして、`25` を指定
- サーバ ポートとして、`21` を指定
- 両方のポートとして、`23` を指定

さらに、ポートとサービスを組み合わせた以下の設定例は、適応型プロファイルが有効にされている場合、有効になります。

- クライアント ポートとして、23 を指定
- クライアント サービスとして、smtp を指定
- サーバ ポートとして、21 を指定
- サーバ サービスとして、telnet を指定

ポートを否定すると（!80 など）、そのポートのトラフィックが TCP ストリーム プリプロセッサで処理されなくなり、パフォーマンスが向上します。

all を引数として指定して、すべてのポートに対して再アセンブリを指定することもできますが、Ciscoではポートを all に設定しないよう推奨しています。この設定では、このプリプロセッサで検査するトラフィックの量が増え、不必要にパフォーマンスが低下するためです。

TCP 再アセンブリには、自動的かつ透過的にその他のプリプロセッサに追加するポートが含まれています。しかし、他のプリプロセッサの設定に追加した TCP 再アセンブリ リストにポートを明示的に追加する場合は、これらの追加したポートは通常処理されます。これには、次のプリプロセッサのポート リストが含まれています。

- FTP/Telnet（サーバ レベル FTP）
- DCE/RPC
- HTTP Inspect
- SMTP
- Session Initiation Protocol
- POP
- IMAP
- SSL

追加のトラフィック タイプ（クライアント、サーバ、両方）を再構成すると、リソースの需要が増大することに注意してください。

次の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

Perform Stream Reassembly on Client Ports

接続のクライアント側のポートに基づくストリームの再アセンブリを有効にします。つまり、Web サーバ、メール サーバ、または一般に $HOME_NET で指定された IP アドレスによって定義されたその他の IP アドレスを宛先とするストリームが再アセンブルされます。不正なトラフィックがクライアントから発生する可能性がある場合は、このオプションを使用します。

Perform Stream Reassembly on Client Services

接続のクライアント側のサービスに基づくストリームの再アセンブリを有効にします。不正なトラフィックがクライアントから発生する可能性がある場合は、このオプションを使用します。

選択するクライアント サービスごとに、少なくとも 1 つのクライアント ディテクタを有効にする必要があります（ディテクタのアクティブ化と非アクティブ化（46-30 ページ）を参照）。デフォルトでは、Ciscoが提供するすべてのディテクタはアクティブになっています。関連するクライアント アプリケーションに対して有効になっているディレクタがない場合、

システムは自動的にCisco提供のすべてのディテクタをアプリケーションに対して有効にします。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタをアプリケーションに対して有効にします。

この機能には、Protection および Control ライセンスが必要です。

Perform Stream Reassembly on Server Ports

接続のサーバ側のポートに基づくストリームの再アセンブリのみを有効にします。つまり、Web サーバ、メール サーバ、または一般に $EXTERNAL_NET で指定された IP アドレスによって定義されたその他の IP アドレスから発信されたストリームが再アセンブリされます。サーバ側の攻撃を監視する必要がある場合は、このオプションを使用します。ポートを指定しないことによって、このオプションを無効にできます。

Perform Stream Reassembly on Server Services

接続のサーバ側のサービスに基づくストリームの再アセンブリのみを有効にします。サーバ側の攻撃を監視する必要がある場合は、このオプションを使用します。サービスを指定しないことによって、このオプションを無効にできます。

選択するサービスごとに、少なくとも 1 つのディテクタを有効にする必要があります(ディテクタのアクティブ化と非アクティブ化(46-30 ページ)を参照デフォルトでは、Ciscoが提供するすべてのディテクタはアクティブになっています。サービスに対して有効になっているディレクタがない場合、システムは自動的にCisco提供のすべてのディテクタを関連するアプリケーション プロトコルに対して有効にします。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタをアプリケーション プロトコルに対して有効にします。

この機能には、Protection および Control ライセンスが必要です。

Perform Stream Reassembly on Both Ports

接続のクライアント側とサーバ側の両方のポートに基づくストリームの再アセンブリを有効にします。同じポートで、不正なトラフィックがクライアントとサーバー間のいずれの方向でも移動する可能性がある場合は、このオプションを使用します。ポートを指定しないことによって、このオプションを無効にできます。

Perform Stream Reassembly on Both Services

接続のクライアント側とサーバ側の両方のサービスに基づくストリームの再アセンブリを有効にします。同じサービスで、不正なトラフィックがクライアントとサーバー間のいずれの方向でも移動する可能性がある場合は、このオプションを使用します。サービスを指定しないことによって、このオプションを無効にできます。

選択するサービスごとに、少なくとも 1 つのディテクタを有効にする必要があります(ディテクタのアクティブ化と非アクティブ化(46-30 ページ)を参照デフォルトでは、Ciscoが提供するすべてのディテクタはアクティブになっています。関連するクライアント アプリケーションまたはアプリケーション プロトコルに対して有効になっているディレクタがない場合、システムは自動的にCisco提供のすべてのディテクタをアプリケーションまたはアプリケーション プロトコルに対して有効にします。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタをアプリケーションまたはアプリケーション プロトコルに対して有効にします。

この機能には、Protection および Control ライセンスが必要です。

TCP ストリームの前処理の設定

ライセンス：Protection

TCP ポリシーを含め、TCP ストリームの前処理を設定できます。TCP ストリーム プリプロセッサの設定オプションの詳細については、TCP ポリシーのオプションの選択（29-25 ページ）を参照してください。

TCP セッションを追跡するストリーム プリプロセッサを設定するには、以下を行います。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Edit Policy] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Transport/Network Layer Preprocessors] で [TCP Stream Configuration] が有効にされているかどうかによって、以下の 2 つの選択肢があります。

- この設定が有効にされている場合、[Edit] をクリックします。
- この設定が無効にされている場合、[Enabled] をオンにしてから、[Edit] をクリックします。

[TCP Stream Configuration] ページが表示されます。ページ下部のメッセージは、設定を含むポリシー層を示します。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　必要に応じて、[Global Settings] の下にある [Packet Type Performance Boost] を変更します。詳細については、「TCP グローバル オプションの選択（29-23 ページ）」を参照してください。

ステップ 6　次の 2 つのオプションから選択できます。

- 新しいターゲットベースのポリシーを追加します。ページの左側の [Hosts] の横にある追加アイコン（ ）をクリックします。[Add Target] ポップアップ ウィンドウが表示されます。[Host Address] フィールドに 1 つまたは複数の IP アドレスを指定し、[OK] をクリックします。

  単一の IP アドレスまたはアドレス ブロックを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のターゲットベースのポリシーを作成できます。FireSIGHT システムで IP アドレス ブロックを使用する方法については、IP アドレスの表記規則（1-23 ページ）を参照してください。

  ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となるネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、「ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）」を参照してください。

ページの左側にあるターゲットのリストに新しいエントリが表示されます。このエントリは、強調表示によって選択された状態であることが示されます。また、[Configuration] セクションが更新されて、追加したポリシーの現在の構成が反映されます。

- 既存のターゲットベースのポリシーの設定を変更します。ページの左側の [Hosts] に追加されているポリシーの設定済みアドレスをクリックするか、[default] をクリックします。

  選択したエントリが強調表示され、[Configuration] セクションが更新されて、選択したポリシーの現在の設定が表示されます。既存のターゲットベースのポリシーを削除するには、削除するポリシーの横にある削除アイコン( )をクリックします。

ステップ 7　必要に応じて、[Configuratio] にある任意の TCP ポリシー オプションを変更します。

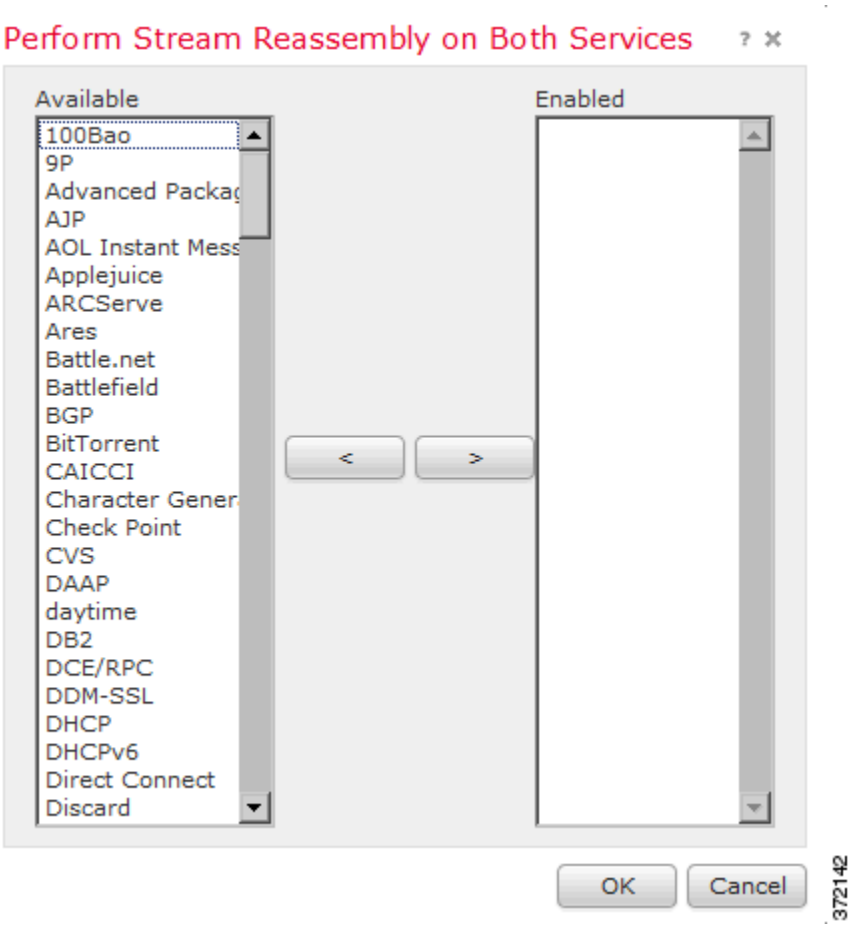
クライアント サービス、サーバ サービス、またはその両方に基づくストリームの再アセンブリの設定を変更するには、ステップ 8 に進みます。そうでない場合は、ステップ 11 に進みます。

詳細については、TCP ポリシーのオプションの選択（29-25 ページ）およびストリームの再アセンブリのオプションの選択（29-29 ページ）を参照してください。

ステップ 8　クライアント サービス、サーバ サービス、またはその両方に基づくストリームの再アセンブリの設定を変更するには、変更するフィールドの内側をクリックするか、そのフィールドの横にある [Edit] をクリックします。

選択したフィールドのポップアップ ウィンドウが表示されます。

たとえば、次の図は、[Perform Stream Reassembly on Both Services] ポップアップ ウィンドウを示しています。



適応型プロファイルを有効にすることで、ネットワークで検出されたサービスに基づいてストリーム プリプロセッサが再アセンブルするトラフィックをモニタできます。詳細については、サーバの使用（50-39 ページ）およびパッシブ展開における前処理の調整（30-1 ページ）を参照してください。

ステップ 9　次の 2 つの選択肢があります。

- モニタにサービスを追加するには、左側の [Available] リストで 1 つまたは複数のサービスを選択してから、右矢印（>）ボタンをクリックします。
- サービスを削除するには、右側の [Enabled] リストで削除するサービスを選択してから、左矢印（<）ボタンをクリックします。

複数のサービス ディテクタを選択するには、Ctrl キーまたは Shift キーを押しながらクリックします。また、クリック アンド ドラッグ操作で、複数の隣接するサービス ディテクタを選択することもできます。

ステップ 10　[OK] をクリックして、選択した項目を追加します。

[TCP Stream Configuration] ページが表示され、サービスが更新されます。

ステップ 11　任意で、サポートによって求められた場合にのみ、[Troubleshooting Options] を展開し、TCP ストリーム前処理ポリシー設定のいずれかを変更します。詳細については、TCP ポリシーのオプションの選択（29-25 ページ）を参照してください。

ステップ 12　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

UDP ストリームの前処理の使用

ライセンス： Protection

UDP ストリームの前処理が行われるのは、ルール エンジンがパケットを処理するために使用する UDP ルールに、以下の引数のいずれかを使用した `flow` キーワード（TCP または UDP クライアントまたはサーバ フローへのルールの適用（36-55 ページ）を参照）が含まれる場合です。

- `Established`
- `To Client`
- `From Client`
- `To Server`
- `From Server`

UDP はコネクションレス型プロトコルであり、2 つのエンドポイントが通信チャネルを確立してデータを交換し、チャネルを終了する手段は提供していません。UDP データ ストリームは一般に、*セッション*という観点で考慮されません。ただし、ストリーム プリプロセッサは、カプセル化 IP データグラム 見出しの送信元および宛先 IP アドレス フィールドと、UDP 見出しのポート フィールドを使用して、フローの方向を判断し、セッションを識別します。セッションが終了するのは、設定可能タイマを超過した時点か、または、いずれかのエンドポイントがもう一方のエンドポイントが到達不能であるか要求されたサービスが到達不能であることを通知する ICMP メッセージを受信した時点です。

システムは UDP ストリームの前処理に関連するイベントを生成しないことに注意してください。ただし、関連するパケット デコーダ ルールを有効にすることで、UDP プロトコル 見出しの異常を検出することができます。パケット デコーダによって生成されるイベントについては、パケットのデコードについて（29-18 ページ）を参照してください。

UDP ストリームの前処理の設定

ライセンス：Protection

UDP ストリームの前処理を設定できます。

UDP セッションを追跡するストリーム プリプロセッサを設定するには、以下を行います。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Edit Policy] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Transport/Network Layer Preprocessors] で [UDP Stream Configuration] が有効にされているかどうかによって、以下の 2 つの選択肢があります。

- この設定が有効にされている場合、[Edit] をクリックします。
- 設定が無効である場合は、[Enabled] をクリックし、次に [Edit] をクリックします。

[UDP Stream Configuration] ページが表示されます。ページ下部のメッセージは、設定を含むポリシー層を示します。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　必要に応じて、[Timeout] 値を設定し、プリプロセッサが非アクティブなストリームを状態テーブルに保持する期間を 1 ～ 86400 秒の範囲で指定します。指定した時間内に追加のデータグラムが現れなかった場合、プリプロセッサはそのストリームを状態テーブルから削除します。

ステップ 6　必要に応じて、[Packet Type Performance Boost] を選択し、送信元および宛先ポートの両方を `any` に設定した UDP ルールで `flow` または `flowbits` オプションが使用されている場合を除き、有効化されたルールに指定されていないポートおよびアプリケーション プロトコルのすべてについて、UDP トラフィックを無視するように設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。

ステップ 7　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

パッシブ展開における前処理の調整

通常、システムはネットワーク分析ポリシーの静的な設定を使用して、トラフィックの前処理と分析を行います。ただし、適応型プロファイル機能により、トラフィックをネットワーク マップから得られるホスト情報と関連付けてから処理することにより、ネットワーク トラフィックに対応できます。

ホストがトラフィックを受信すると、ホストで実行されているオペレーティング システムは IP フラグメントを再構成します。再構成に使用する順序は、オペレーティング システムによって異なります。同様に、各オペレーティング システムはさまざまな方法で TCP を実装することがあるため、TCP ストリームの再構成の方法も異なる可能性があります。プリプロセッサが宛先ホストのオペレーティング システムで使用されているものとは異なる形式を使用してデータを再構成すると、受信ホストでの再構成時に悪意のある可能性があるコンテンツをシステムが見逃す可能性があります。

ヒント パッシブ展開の場合、Cisco では、適応型プロファイルを設定するように推奨しています。インライン展開の場合、Cisco では、インライン正規化プリプロセッサの設定で [Normalize TCP Payload] オプションを有効にするように推奨しています。詳細については、インライン トラフィックの正規化（29-7 ページ）を参照してください。

適応型プロファイルを使用したパケット フラグメントと TCP ストリームの再構成の改善に関する詳細については、次のトピックを参照してください。

- 適応型プロファイルについて（30-1 ページ）
- 適応型プロファイルの設定（30-3 ページ）

適応型プロファイルについて

ライセンス： Protection

適応型プロファイルは、IP 最適化と TCP ストリームの前処理に最適なオペレーティング システム プロファイルの使用を可能にします。適応型プロファイルにより影響を受けるネットワーク分析ポリシーの側面の詳細については、IP パケットのデフラグ（29-12 ページ）およびTCP ストリームの前処理の使用（29-22 ページ）を参照してください。

システムはネットワーク検出または Nmap スキャンにより取得するか、またはホスト入力機能により追加されたホスト情報を使用して、処理動作を適応させることができます。

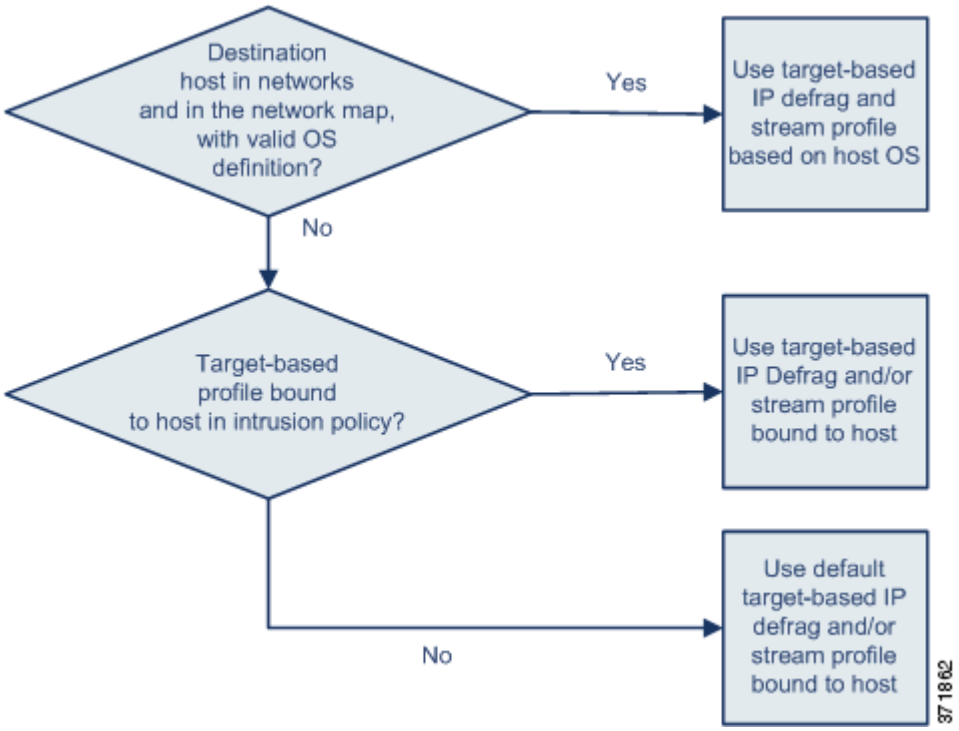
注　コマンドラインのインポート ユーティリティまたはホスト入力 API を使用してサードパーティ製アプリケーションからホスト情報を入力する場合、システムが適応型プロファイルで使用できるように、データを製品の定義にマッピングしておく必要があります。詳細については、サードパーティ製品マッピングの管理（46-33 ページ）を参照してください。

プリプロセッサによる適応型プロファイルの使用

ライセンス： Protection

適応型プロファイルは、ネットワーク分析ポリシーに設定可能なターゲット ベースのプロファイルと同様に、ターゲット ホストのオペレーティング システムと同じ方法で、IP パケットの最適化およびストリームの再構成を行うのに役立ちます。その後、侵入ルール エンジンは宛先ホストによって使用されるものと同じ形式でデータを分析します。

手動で設定されたターゲット ベースのプロファイルは、選択したデフォルトのオペレーティング システム プロファイルまたは特定のホストにバインドしたプロファイルにのみ適用されます。一方、適応型プロファイルは、次の図に示すように、ターゲット ホストのホスト プロファイルのオペレーティング システムに基づいて、適切なオペレーティング システム プロファイルに切り替わります。



たとえば、10.6.0.0/16 サブネットに適合型プロファイルを設定し、Linux にデフォルトの IP 最適化ターゲット ベース ポリシーを設定します。設定を構成する Defense Center には 10.6.0.0/16 サブネットを含むネットワーク マップがあります。

デバイスは、10.6.0.0/16 サブネットにないホスト A からのトラフィックを検出すると、Linux ターゲット ベース ポリシーを使用して IP フラグメントを再構成します。一方、10.6.0.0/16 サブネットにあるホスト B からのトラフィックを検出した場合、デバイスはネットワーク マップか

らホスト B のオペレーティング システムのデータを取得します。このマップには、ホスト B が Microsoft Windows XP Professional を実行していることが記述されています。システムは、Windows ターゲット ベース プロファイルを使用して、ホスト B に送信されるトラフィックの IP 最適化を実行します。

IP 最適化プリプロセッサの詳細については、IP パケットのデフラグ（29-12 ページ）を参照してください。ストリーム プリプロセッサの詳細については、TCP ストリームの前処理の使用（29-22 ページ）を参照してください。

適応型プロファイルとFireSIGHT推奨ルール

ライセンス： Protection

適応型プロファイルの機能はアクセス コントロール ポリシーの詳細設定で、そのアクセス コントロール ポリシーによって呼び出されるすべての侵入ポリシーにグローバルに適用されます。FireSIGHT 推奨ルールの機能は、設定する個々の侵入ポリシーに適用されます。

FireSIGHT 推奨ルールと同様に、適応型プロファイルはルールのメタデータをホスト情報と比較し、ルールを特定のホストに適用すべきかどうかを判別します。ただし、FireSIGHT 推奨ルールがその情報を使用してルールの有効化または無効化を行うための推奨事項を提供するのに対して、適応型プロファイルはその情報を使用して特定のトラフィックに特定のルールを適用します。

FireSIGHT 推奨ルールでは、提案された変更をルール状態に実装するために、ユーザーの対話が必要になります。一方、適応型プロファイルは侵入ポリシーを変更しません。ルールの適応処理はパケット単位で行われます。

さらに、FireSIGHT 推奨ルールによって、無効なルールが有効化される可能性があります。対照的に、適応型プロファイルは、侵入ポリシーですでに有効になっているルールの適用にだけ影響します。適応型プロファイルによってルールの状態が変更されることはありません。

適応型プロファイルと FireSIGHT 推奨ルールを組み合わせて使用できます。侵入ポリシーが適用されると、適応型プロファイルはルールの状態を使用して適用の候補に含めるかどうかを判別し、推奨事項の承認または拒否はそのルール状態に反映されます。両方の機能を使用して、監視対象の各ネットワークに最適なルールを有効化または無効化することができ、特定のトラフィックに対する有効化したルールの適用を最も効率的に行うことができます。

詳細については、「ネットワーク資産に応じた侵入防御の調整（33-1 ページ）」を参照してください。

適応型プロファイルの設定

ライセンス： Protection

ホスト情報を使用して IP 最適化および TCP ストリームの前処理に使用するターゲット ベース プロファイルを判別するために、適応型プロファイルを設定できます。

注意　適応型プロファイルを有効または無効にすると、Snort プロセスが再開され、構成変更を適用する際、一時的にトラフィック検査が中断されます。この検査中にシステムがトラフィックをドロップするか、検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、「Snort の再開によるトラフィックへの影響（1-9 ページ）」を参照してください。

適応型プロファイルを設定する際、適応型プロファイルを特定のネットワークにバインドする必要があります。正常に適応型プロファイルを使用するには、そのネットワークがネットワーク マップ内にあり、アクセス コントロール ポリシーを適用するデバイスでモニタされるセグメントにある必要があります。

注 適応型プロファイルを使用するには、保護するネットワークのネットワーク検出ポリシーでホスト検出を有効にし、ネットワーク検出ポリシーを再適用する必要があります。詳細については、ネットワーク検出ポリシーの作成（45-25 ページ）を参照してください。

IP アドレス、アドレスのブロック、またはアクセス コントロール ポリシーのデフォルトの侵入ポリシーにリンクされた変数セットにおいて、設定された適切な値を使用したネットワーク変数を指定することで、トラフィックの処理に適応型プロファイルが使用される、ネットワーク マップ内のホストを指定できます。詳細については、「アクセス コントロールのデフォルト侵入ポリシーの設定（25-1 ページ）」を参照してください。

これらのアドレス指定方法を単独で使用したり、次の例に示すように、IP アドレス、アドレス ブロック、または変数をカンマで区切ったリストとして組み合わせて使用したりすることができます。

```
192.168.1.101, 192.168.4.0/24, $HOME_NET
```

FireSIGHT システムにおけるアドレス ブロックの指定の詳細については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ヒント `any` という値の変数を使用するか、またはネットワーク値として `0.0.0.0/0` を指定することにより、適合型プロファイルをネットワーク マップ内のすべてのホストに適用できます。

また、Defense Center のネットワーク マップ データが管理対象デバイスと同期される頻度を制御することもできます。システムはデータを使用して、トラフィックを処理する際に使用するプロファイルを判別します。

適合型プロファイルの設定:

アクセス: Admin/Access Admin/Network Admin

ステップ 1 [Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 編集するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4 [Detection Enhancement Settings] の横にある編集アイコン（  ）をクリックします。

[Detection Enhancement Settings] ポップアップ ウィンドウが表示されます。

ステップ 5 [Adaptive Profiles - Enabled] を選択して、適合型プロファイルを有効にします。

ステップ 6 必要に応じて、[Adaptive Profiles - Attribute Update Interval] フィールドに、Defense Center から管理対象デバイスへのネットワーク マップ データの同期に必要な経過時間（分）を入力します。

注 このオプションの値を大きくすると、大規模なネットワークのパフォーマンスを向上できます。

ステップ 7　[Adaptive Profiles - Networks] フィールドに、適応型プロファイルを使用するネットワーク マップ内のホストを識別する、特定の IP アドレス、アドレス ブロック、または変数、またはこれらのアドレス指定方法を含むカンマ区切りのリストを入力します。

変数の設定の詳細については、変数セットの操作（3-19 ページ）を参照してください。ネットワーク マップの設定の詳細については、ネットワーク検出ポリシーの作成（45-25 ページ）を参照してください。

ステップ 8　[OK] をクリックして設定内容を維持します。

CHAPTER 31

侵入ポリシーの開始

*侵入ポリシー*は、侵入検知および侵入防御の設定の定義済みセットです。このポリシーは、セキュリティ違反がないかトラフィックを検査し、インライン展開では、悪意のあるトラフィックをブロックまたは変更できます。侵入ポリシーはアクセス コントロール ポリシーによって呼び出され、トラフィックが宛先に許可される前のシステムの最後の防御ラインです。

Cisco は、複数の侵入ポリシーを FireSIGHT システム と共に提供します。システムによって提供されるポリシーを使用して、Cisco 脆弱性調査チーム（VRT）のエクスペリエンスを活用することができます。これらのポリシーでは、VRT は侵入ルールおよびプリプロセッサ ルールの状態を設定し（有効または無効）、他の詳細設定の初期設定も提供します。ルールを有効にすると、システムはそのルールと一致するトラフィックに対する侵入イベントを生成します（そして場合によってブロックします）。ルールを無効にすると、ルールの処理が停止されます。

ヒント システムによって提供される侵入ポリシーおよびネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、Balanced Security and Connectivity ネットワーク分析ポリシーおよび Balanced Security and Connectivity 侵入ポリシーは共に機能し、侵入ルールの更新の際に両方とも更新できます。しかし、ネットワーク分析ポリシーは前処理オプションの大部分を制御するのに対し、侵入ポリシーは侵入ルールの大部分を制御します。ネットワーク分析ポリシーまたは侵入ポリシーについて（23-1 ページ）ネットワーク分析ポリシーと侵入ポリシーが連携してトラフィックを検査するしくみの概要、およびナビゲーション パネルの使用、競合の解決、変更のコミットに関する基本事項が記載されています。

カスタム侵入ポリシーを作成すると、次のことを行うことができます。

- ルールを有効化および無効化し、独自のルールを記述および追加することによる、検出の調整。
- FireSIGHT 推奨機能を使用して、ネットワーク上で検出されたオペレーティング システム、サーバ、およびクライアント アプリケーション プロトコルを、それらの資産を保護するために作成されたルールに関連付ける。
- 外部アラート、センシティブ データの前処理、およびグローバル ルールのしきい値構成など、さまざまな詳細設定の設定。
- 効率的に複数の侵入ポリシーを管理するためには、レイヤをビルディング ブロックとして使用します。

侵入ポリシーの調整時、特にルールを有効および追加するときは、侵入ルールによってはトラフィックをある方法で最初に復号化または前処理する必要があることに留意してください。侵入ポリシーがパケットを検査する前に、パケットはネットワーク分析ポリシーの設定に従って前処理されます。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

注　前処理インスペクションと侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは互いに補完する**必要があります**。特に複数のカスタム ネットワーク分析ポリシーを使用した前処理の調整は、**高度な**タスクです。詳細については、カスタム ポリシーの制限（23-13 ページ）を参照してください。

カスタム侵入ポリシーを設定した後は、侵入ポリシーを 1 つ以上のアクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに関連付けることで、アクセス コントロール設定の一部として使用できます。これにより、システムは強制的に侵入ポリシーを使用して、トラフィックが最終宛先に渡される前に特定の許可トラフィックを検査します。変数セットを侵入ポリシーとペアにすることで、ホーム ネットワーク、外部ネットワーク、および必要に応じてネットワーク上のサーバを正確に反映できます。詳細については、侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（18-1 ページ）を参照してください。

デフォルトでは、暗号化ペイロードの侵入インスペクションは無効化されます。これにより、侵入インスペクションが設定されているアクセス コントロール ルールと暗号化された接続を照合したときに、誤検出が減少し、パフォーマンスが向上します。詳細については、トラフィック復号化の概要（19-1 ページ）およびSSL プリプロセッサの使用（27-75 ページ）を参照してください。

この章では、単純なカスタム侵入ポリシーを作成する方法について説明します。この章には、侵入ポリシーの管理（編集、比較など）に関する基本情報も含まれています。詳細については、以下を参照してください。

- カスタム侵入ポリシーの作成（31-2 ページ）
- 侵入ポリシーの管理（31-3 ページ）
- 侵入ポリシーの編集（31-4 ページ）
- 侵入ポリシーの適用（31-9 ページ）
- 現在の侵入設定のレポートの生成（31-10 ページ）
- 2 つの侵入ポリシーまたはリビジョンの比較（31-11 ページ）

カスタム侵入ポリシーの作成

ライセンス： Protection

新しい侵入ポリシーを作成するときは、一意の名前を付け、基本ポリシーを指定し、ドロップ動作を指定する必要があります。

基本ポリシーは侵入ポリシーのデフォルト設定を定義します。新しいポリシーで設定を変更すると、基本ポリシーの設定が上書きされますが、変更はされません。基本ポリシーとしてシステムによって提供されるポリシーまたはカスタム ポリシーを使用できます。詳細については、基本レイヤについて（24-3 ページ）を参照してください。

侵入ポリシーのドロップ動作、または [Drop when Inline] 設定によって、システムが廃棄ルール（ルール状態が [Drop and Generate Events] に設定されている侵入ルールまたはプリプロセッサ ルール）を処理する方法、およびトラフィックに影響を与えるその他の侵入ポリシー設定が決まります。悪質なパケットをドロップまたは置換する場合は、インライン展開でドロップ動作を有効にする必要があります。パッシブな展開では、ドロップ動作に関係なく、システムはトラフィック フローに影響を与えることができないことに注意してください。詳細については、インライン展開でのドロップ動作の設定（31-6 ページ）を参照してください。

侵入ポリシーを作成するには、以下を行います。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion Policy] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ヒント　また、別のDefense Centerからポリシーをインポートすることもできます（設定のインポートおよびエクスポート（A-1 ページ）を参照）。

ステップ 2　[Create Policy] をクリックします。

別のポリシー内に未保存の変更が存在する場合は、[Intrusion Policy] ページに戻るかどうか尋ねられたときに [Cancel] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Create Intrusion Policy] ポップアップ ウィンドウが表示されます。

ステップ 3　[Name] に一意のポリシー名を入力し、オプションで [Description] にポリシーの説明を入力します。

ステップ 4　最初の**基本ポリシー**を指定します。

基本ポリシーとしてシステムによって提供されるポリシーまたはカスタム ポリシーを使用できます。

注意　Ciscoの担当者から指示された場合を除き、`Experimental Policy 1` は使用**しないで**ください。Ciscoでは、試験用にこのポリシーを使用します。

ステップ 5　インライン展開でのシステムのドロップ動作を設定します。

- 侵入ポリシーがトラフィックに影響し、イベントを生成することを許可するには、[Drop when Inline] を有効にします。
- 侵入ポリシーがイベントの生成中にトラフィックに影響しないようにするには、[Drop when Inline] を無効にします。

ステップ 6　ポリシーを作成します。

- 新しいポリシーを作成して [Intrusion Policy] ページに戻るには、[Create Policy] をクリックします。新しいポリシーには基本ポリシーと同じ設定が付与されます。
- ポリシーを作成し、高度な侵入ポリシー エディタで開いて編集するには、[Create and Edit Policy] をクリックします。侵入ポリシーの編集（31-4 ページ）を参照してください。

侵入ポリシーの管理

ライセンス：Protection

[Intrusion Policy] ページ（[Policies]> [Intrusion] > [Intrusion Policy]）では、現在のカスタム侵入ポリシーと共に以下の情報を表示できます。

- ポリシーが最後に変更された日時（ローカル時間）とそれを変更したユーザ
- インライン展開でトラフィックをドロップおよび変更できる [Drop when Inline] 設定を有効にするかどうか

- トラフィックの検査に侵入ポリシーを使用しているアクセス コントロール ポリシーとデバイス
- ポリシーに保存されていない変更があるかどうか、およびポリシーを現在編集している人（いれば）に関する情報

お客様が独自に作成するカスタム ポリシーに加えて、システムは初期インライン ポリシーと初期パッシブ ポリシーの 2 つのカスタム ポリシーを提供しています。これらの 2 つの侵入ポリシーは、ベースとして Balanced Security and Connectivity 侵入ポリシーを使用します。両者の唯一の相違点は、[Drop When Inline] 設定です。インライン ポリシーではドロップ動作が有効化され、パッシブ ポリシーでは無効化されています。これらのシステム付属のカスタム ポリシーは編集して使用できます。

[Intrusion Policy] ページのオプションを使用することで、次の表にあるアクションを実行できます。

表 31-1　侵入ポリシー管理操作

目的	操作	参照先
新しい侵入ポリシーを作成する	[Create Policy] をクリックします。	カスタム侵入ポリシーの作成（31-2 ページ）
既存の侵入ポリシーを編集する	編集アイコン（  ）をクリックします。	侵入ポリシーの編集（31-4 ページ）
侵入ポリシーを管理対象デバイスに再適用する	適用アイコン（  ）をクリックします。	侵入ポリシーの適用（31-9 ページ）
侵入ポリシーをエクスポートして別のDefense Centerにインポートする	エクスポート アイコン（  ）をクリックします。	設定のエクスポート（A-1 ページ）
侵入ポリシー内の現在の構成設定がリストされた PDF レポートを表示する	レポート アイコン（  ）をクリックします。	現在の侵入設定のレポートの生成（31-10 ページ）
2 つの侵入ポリシーまたは同じポリシーの 2 つのリビジョンの設定を比較する	[Compare Policies] をクリックします。	2 つの侵入ポリシーまたはリビジョンの比較（31-11 ページ）
侵入ポリシーを削除する	削除アイコン（  ）をクリックし、ポリシーを削除することを確認します。アクセス コントロール ポリシーが参照している侵入ポリシーは削除できません。	

侵入ポリシーの編集

ライセンス： Protection

新しい侵入ポリシーを作成すると、そのポリシーには基本ポリシーと同じ侵入ルールと詳細設定が付与されます。次の表では、侵入ポリシーの編集時に実行する最も一般的な操作について説明しています。

表 31-2　侵入ポリシーの編集操作

目的	操作	参照先
インライン展開でドロップ動作を指定する	[Policy Information] ページで [Drop when Inline] チェック ボックスをオンまたはオフにします。	インライン展開でのドロップ動作の設定（31-6 ページ）
基本ポリシーを変更する	[Policy Information] ページの [Base Policy] ドロップダウンリストから基本ポリシーを選択します。	基本ポリシーの変更（24-4 ページ）
基本ポリシーの設定を表示する	[Policy Information] ページで [Manage Base Policy] をクリックします。	基本レイヤについて（24-3 ページ）
侵入ルールを表示または設定する	[Policy Information] ページで [Manage Rules] をクリックします。	侵入ポリシー内のルールの表示（32-3 ページ）
現在のルール状態別に侵入ルールのフィルタ ビューを表示する、またオプションでそれらのルールを設定する	[Policy Information] ページで、[Manage Rules] の下の [Generate Events] または [Drop and Generate Events] に設定されているルールの番号の横にある [View] をクリックします。	侵入ポリシー内のルールのフィルタ処理（32-10 ページ）
FireSIGHT 推奨ルールを設定する	ナビゲーション パネルで [FireSIGHT Recommendations] をクリックします。	FireSIGHT 推奨の使用（33-4 ページ）
現在の推奨ルール状態によってフィルタリングした侵入ルールのビューを表示し、必要に応じて、これらのルールを設定する	[Policy Information] ページで、推奨事項を生成した後、以下を実行します。 • イベントの生成、イベントのドロップと生成、またはルールの無効化を行う推奨の番号の横にある [View] をクリックします。 • すべての推奨を表示するには、[View Recommended Changes] をクリックします。	FireSIGHT 推奨の使用（33-4 ページ）
詳細設定を有効化、無効化、または編集する	ナビゲーション パネルで [Advanced Settings] をクリックします。	侵入ポリシーの詳細設定の設定（31-7 ページ）
ポリシー層を管理する	ナビゲーション パネルで [Policy Layers] をクリックします。	ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）

侵入ポリシーの調整時、特にルールを有効および追加するときは、侵入ルールによってはトラフィックをある方法で最初に復号化または前処理する必要があることに留意してください。侵入ポリシーがパケットを検査する前に、パケットはネットワーク分析ポリシーの設定に従って前処理されます。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

注　前処理インスペクションと侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは互いに補完する**必要があります**。特に複数のカスタム ネットワーク分析ポリシーを使用した前処理の調整は、**高度な**タスクです。詳細については、カスタム ポリシーの制限（23-13 ページ）を参照してください。

システムは、ユーザごとに 1 つのセキュリティ ポリシーをキャッシュします。侵入ポリシーの編集中に、任意のメニューまたは別のページへの他のパスを選択した場合、変更内容はそのページを離れてもシステム キャッシュにとどまります。上記の表の実行可能な操作に加えて、ネットワーク分析ポリシーまたは侵入ポリシーについて（23-1 ページ）には、ナビゲーション パネル、競合の解決、変更のコミットの使用方法が記載されています。

侵入ポリシーを編集するには、次の手順を実行します。

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　設定する侵入ポリシーの横にある編集アイコン（  ）をクリックします。

侵入ポリシー エディタが表示され、[Policy Information] ページに焦点が置かれ、左側にナビゲーション パネルがあります。

ステップ 3　ポリシーを編集します。上記で要約されたアクションのいずれかを実行します。

ステップ 4　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残した状態での終了を行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

インライン展開でのドロップ動作の設定

ライセンス： Protection

インライン展開では、侵入ポリシーはトラフィックをブロックおよび変更できます。

- *廃棄ルール*は、一致するパケットをドロップし、侵入イベントを生成できます。侵入またはプリプロセッサの廃棄ルールを設定するには、その状態を [Drop and Generate Events] に設定します。ルール状態の設定（32-22 ページ）を参照してください。
- 侵入ルールは、`replace` キーワードを使用して悪意のあるコンテンツを置換できます。インライン展開でのコンテンツの置換（36-32 ページ）を参照してください。

侵入ルールがトラフィックに影響を与えるようにするには、廃棄ルールおよびコンテンツを置き換えるルールを適切に設定し、さらに管理対象デバイスを適切にインライン展開する（つまり、インライン インターフェイス セットを設定する）必要があります。最後に、侵入ポリシーの*ドロップ動作*、または [Drop when Inline] 設定を有効にする必要があります。

注　FTP を介したマルウェア ファイルの転送をブロックするには、ネットワークベースの高度なマルウェア防御（AMP）を正しく設定するだけでなく、アクセス コントロール ポリシーのデフォルトの侵入ポリシーで [Drop when Inline] を有効にする必要があります。デフォルトの侵入ポリシーを決定または変更するには、アクセス コントロールのデフォルト侵入ポリシーの設定（25-1 ページ）を参照してください。

設定がインライン展開で実際にトラフィックに影響を与えることなくどのように機能するかを評価する場合は、ドロップ動作を無効にできます。この場合、システムは侵入イベントを生成しますが、廃棄ルールをトリガーしたパケットをドロップしません。結果に問題がなければ、ドロップ動作を有効にできます。

パッシブ展開またはタップ モードでのインライン展開では、ドロップ動作に関わらず、システムはトラフィックに影響を与えることはできません。つまり、パッシブ展開では、[Drop and Generate Events] に設定されたルールは [Generate Events] に設定されたルールと同じ動作をします。システムは、侵入イベントを生成しますが、パケットをドロップできません。

侵入イベントを表示すると、ワークフローに*インライン結果*が含まれている場合があり、トラフィックが実際にドロップされたか、または単にドロップされるはずだったことが示されます。パケットが廃棄ルールに一致すると、インライン結果は次のようになります。

- ドロップ動作が有効な正しく設定されたインライン展開によりドロップされたドロップの場合は `Dropped`。
- `Would have dropped`:デバイスがパッシブ展開されているか、ドロップ動作が無効化されているために、パケットがドロップされなかった場合展開に関係なく、システムがプルーニングしている間に表示されるパケットのインライン結果は、常に `Would have dropped` であることに注意してください。

インライン展開で侵入ポリシーのドロップ動作を設定するには、次の手順を実行します。

アクセス: Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン( )をクリックします。

[Policy Information] ページが表示されます。

ステップ 3　ポリシーのドロップ動作を設定します。

- 侵入ルールがトラフィックに影響し、イベントを生成することを許可するには、[Drop when Inline] を有効にします。
- 侵入ルールがイベントの生成中にトラフィックに影響しないようにするには、[Drop when Inline] を無効にします。

ステップ 4　ポリシーの保存、編集の続行、変更の破棄を行うか、またはシステム キャッシュで変更をそのままにしながら終了します。詳細については、競合の解決とポリシー変更の確定(23-17 ページ)を参照してください。

侵入ポリシーの詳細設定の設定

ライセンス: Protection

侵入ポリシーの*詳細設定*には、設定のための特定の専門知識が必要です。デフォルトで有効になる詳細設定や、詳細設定ごとのデフォルトは、侵入ポリシーの基本ポリシーに応じて決まります。

侵入ポリシーのナビゲーション パネルで [Advanced Settings] を選択すると、ポリシーによってタイプ別の詳細設定がリストされます。[Advanced Settings] ページで、侵入ポリシーの詳細設定を有効または無効にしたり、詳細設定の設定ページにアクセスしたりできます。

詳細設定を行うには、それを有効にする必要があります。詳細設定を有効にすると、その詳細設定に関する設定ページへのサブリンクがナビゲーション パネル内の [Advanced Settings] リンクの下に表示され、この設定ページへの [Edit] リンクが [Advanced Settings] ページ上の詳細設定の横に表示されます。

ヒント　詳細設定の設定を基本ポリシーの設定に戻すには、詳細設定の設定ページで [Revert to Defaults] をクリックします。プロンプトが表示されたら、戻すことを確認します。

詳細設定を無効にすると、サブリンクと [Edit] リンクは表示されなくなりますが、設定は保持されます。一部の侵入ポリシー設定（侵入ルールのセンシティブ データ ルール、SNMP アラート）では、詳細設定を有効にして正しく設定している必要があります。このように誤って設定された侵入ポリシーは保存できません。競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

詳細設定を変更する場合、変更する設定と、その変更がネットワークに及ぼす可能性のある影響について理解していることが必要です。次の項では、詳細設定ごとに固有の設定の詳細情報へのリンクを記述します。

特定の脅威の検出

機密データ プリプロセッサは、ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出します。このプリプロセッサの設定については、センシティブ データの検出（34-20 ページ）を参照してください。

特定の脅威（バック オリフィス攻撃、複数のポート スキャン タイプ、および過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレート ベース攻撃）を検出する他のプリプロセッサは、ネットワーク分析ポリシーで設定されることに留意してください。詳細については、特定の脅威の検出（34-1 ページ）を参照してください。

侵入ルールのしきい値

グローバル ルールのしきい値を設定すると、しきい値を使用して、システムが侵入イベントを記録したり表示したりする回数を制限できるので、多数のイベントでシステムが圧迫されないようにすることができます。詳細については、侵入イベントのロギングのグローバルな制限（35-1 ページ）を参照してください。

外部応答

Web インターフェイス内での侵入イベントをさまざまな形式で表示することに加えて、システム ログ（syslog）ファシリティへのロギングを有効にしたり、イベント データを SNMP トラップ サーバに送信したりできます。ポリシーごとに、侵入イベントの通知限度を指定したり、外部ロギング ファシリティに対する侵入イベントの通知をセットアップしたり、侵入イベントへの外部応答を設定したりできます。詳細については、以下を参照してください。

- SNMP 応答の設定（44-3 ページ）
- syslog 応答の設定（44-6 ページ）

これらのポリシー単位のアラート設定に加えて、各ルールまたはルール グループの侵入イベントを通知する電子メール アラートをグローバルに有効化/無効化できます。どの侵入ポリシーがパケットを処理するかに関わらず、ユーザの電子メール アラート設定が使用されます。詳細については、電子メール アラートについて（44-7 ページ）を参照してください。

侵入ポリシーの適用

ライセンス： Protection

アクセス コントロールを使用している管理対象デバイスに侵入ポリシーを適用（アクセス コントロール ポリシーの適用（12-17 ページ）を参照）した場合は、その侵入ポリシーをいつでも再適用できます。これにより、アクセス コントロール ポリシーを再適用せずに、監視対象ネットワーク上で侵入ポリシーを変更できます。再適用中は、比較レポートを表示して、最後に侵入ポリシーが適用されてから加えられた変更を確認できます。

侵入ポリシーを再適用する際は次の点に注意してください。

- 侵入ポリシー再適用タスクは定期的に実行するようにスケジュールできます。侵入ポリシーの適用の自動化（62-7 ページ）を参照してください。
- 無効なターゲット デバイス上での侵入ポリシー再適用は失敗します。たとえば、既に適用されている侵入ポリシーをデバイスから削除するアクセス コントロール ポリシーを適用した場合、アクセス コントロール ポリシー適用タスクが解決される前に侵入ポリシーを再適用しようとすると、侵入ポリシー再適用が失敗します。
- FireSIGHT システムの違うバージョンを実行しているスタックされたデバイス（1 つのデバイス上のアップグレードが失敗した場合など）に侵入ポリシーを適用することはできません。侵入ポリシーをデバイス スタックに再適用することは可能ですが、スタック内の個別のデバイスに再適用することはできません。
- ルール更新をインポートするときに、インポートの完了後に自動的に侵入ポリシーを適用できます。このオプションを有効にしなかった場合は、ルール更新によって変更されたポリシーを手動で再適用する必要があります。詳細については、「ルールの更新とローカル ルール ファイルのインポート（66-16 ページ）」を参照してください。
- Defense Center上の Snort のバージョンが管理対象デバイスのものと異なる場合、アクセス コントロール ポリシーを適用せずに侵入ポリシーをデバイスに適用することはできません。侵入ポリシーの適用がこの理由で失敗した場合、代わりに、アクセス コントロール ポリシー全体を再適用します。
- メモリが制限されているデバイスでは、侵入ポリシーの数が、複数の変数セットとペアにならない可能性があります。1 つの侵入ポリシーのみを参照するアクセス コントロール ポリシーを適用できる場合は、この侵入ポリシーに対するすべての参照が、同一の変数セットとペアになっていることを確認してください。

侵入ポリシーを再適用するには、以下を行います。

アクセス： Admin/Security Approver

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　再適用するポリシーの横にある適用アイコン（  ）をクリックします。

[Reapply Intrusion Policy] ウィンドウが開いて、ポリシーが現在適用されているデバイスがリストされます。

ステップ 3　ポリシーを再適用するデバイスを指定します。

ヒント　デバイスが [Out-of-date] としてリストされている場合、必要に応じて、比較アイコン（  ）をクリックし、現在適用されている侵入ポリシーと更新された侵入ポリシーを比較するレポートを表示することもできます。

ステップ 4　[Reapply] をクリックします。

ポリシーが再適用されます。タスク キューを使用して適用のステータスを監視できます（[System] > [Monitoring] > [Task Status]）。詳細については、「タスク キューの表示（C-1 ページ）」を参照してください。

現在の侵入設定のレポートの生成

ライセンス：Protection

侵入ポリシー レポートは、特定の時点でのポリシー設定の記録です。システムは、基本ポリシー内の設定とポリシー層の設定を統合して、基本ポリシーに起因する設定とポリシー層に起因する設定を区別しません。

このレポートには、次の情報が含まれており、監査目的や現在の設定を調べるために使用できます。

表 31-3　侵入ポリシー レポートのセクション

セクション	説明
Policy Information	侵入ポリシーの名前と説明、ポリシーを最後に変更したユーザの名前、ポリシーが最後に変更された日時が記載されます。インライン展開でのパケットのドロップが有効になっているか無効になっているか、現在のルール更新のバージョン、基本ポリシーが現在のルール更新にロックされているかどうかも記載されます。
FireSIGHT Recommendations	ネットワーク上のホストとアプリケーションに基づく推奨ルール状態に関する情報を提供します。（任意）FireSIGHT の推奨事項の設定時にこの設定を有効にした場合は、推奨とルール状態との相違点が ポリシー レポートに含まれます。
Advanced Settings	有効なすべての侵入ポリシーの詳細設定とその構成を表示します。
ルール	有効になっているすべてのルールおよびそのアクションのリストが提供されます。

また、2 つの侵入ポリシーまたは同じポリシーの 2 つのリビジョンを比較する比較レポートを生成することもできます。詳細については、2 つの侵入ポリシーまたはリビジョンの比較（31-11 ページ）を参照してください。

侵入ポリシー レポートを表示するには、以下を行います。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　レポートを生成する侵入ポリシーの横にあるレポート アイコン（  ）をクリックします。侵入ポリシー レポートを生成する前に未確定の変更をコミットするのを忘れないでください。コミットされた変更だけがレポートに表示されます。

システムが侵入ポリシー レポートを生成します。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。

2 つの侵入ポリシーまたはリビジョンの比較

ライセンス：Protection

ポリシー変更が組織の標準に準拠しているかどうかを確認するため、またはシステムのパフォーマンスを最適化するために、2 つの侵入ポリシーの違いを確認することができます。アクセス可能な侵入ポリシーの場合は、2 つの侵入ポリシーまたは同じ侵入ポリシーの 2 つのリビジョンを比較できます。比較した後に、必要に応じて、2 つのポリシーまたはポリシー リビジョン間の違いを記録した PDF レポートを生成できます。

侵入ポリシーまたは侵入ポリシー リビジョンを比較するための 2 つのツールが用意されています。

- 比較ビューには、2 つの侵入ポリシーまたは侵入ポリシー リビジョン間の相違点のみが並べて表示されます。各ポリシーまたはポリシー リビジョンの名前が比較ビューの左右のタイトル バーに表示されます。

  これを使用して、Web インターフェイスで相違点を強調表示したまま、両方のポリシーのリビジョンを表示し移動することができます。

- 比較レポートは、2 つの侵入ポリシーまたは侵入ポリシー リビジョン間の違いのみを記録したもので、PDF であるという以外は、侵入ポリシー レポートと類似した形式になっています。

  これは、ポリシー比較を保存、コピー、出力、および共有して、詳しく調査するために使用できます。

侵入ポリシー比較ツールとその使い方の詳細については、以下を参照してください。

- 侵入ポリシー比較ビューの使用（31-11 ページ）
- 侵入ポリシー比較レポートの使用（31-12 ページ）

侵入ポリシー比較ビューの使用

ライセンス：Protection

比較ビューには、両方の侵入ポリシーまたはポリシー リビジョンが並べて表示されます。それぞれのポリシーまたはポリシー リビジョンは、比較ビューの左右のタイトル バーに表示された名前で識別されます。最終変更時刻と最終変更ユーザが、ポリシー名の右側に表示されます。[Intrusion Policy] ページにはポリシーが最後に変更された時刻が現地時間で表示されますが、侵入ポリシー レポートでは変更時刻が UTC でリストされることに注意してください。2 つの侵入ポリシーまたはポリシー リビジョン間の違いが強調表示されます。

- 青色は強調表示された設定が 2 つのポリシーまたはポリシー リビジョンで違うことを意味します。違いは赤色のテキストで表示されます。
- 緑色は強調表示された設定が 1 つのポリシーまたはポリシー リビジョンにだけ存在することを意味します。

次の表内の操作を実行できます。

表 31-4　侵入ポリシー比較ビューの操作

目的	操作
変更に個別にナビゲートする	タイトル バーの上の [Previous] または [Next] をクリックします。 左側と右側の間にある二重矢印アイコン（）が移動し、表示している違いを示す [Difference] 番号が変わります。
特定の詳細設定の構成を含む階層を特定する	表示する設定の横にある詳細設定アイコン（  ）の上にカーソルを移動します。 ウィンドウに、詳細構成を含む階層の名前が表示されます。
新しい侵入ポリシー比較ビューを生成する	[New Comparison] をクリックします。 [Select Comparison] ウィンドウが表示されます。詳細については、「侵入ポリシー比較レポートの使用」を参照してください。
侵入ポリシー比較レポートを生成する	[Comparison Report] をクリックします。 ポリシー比較レポートは、2 つのポリシーまたはポリシー リビジョン間の違いのみをリストする PDF を作成します。

侵入ポリシー比較レポートの使用

ライセンス：Protection

侵入ポリシー比較レポートは、PDF で提供される、侵入ポリシー比較ビューで特定された 2 つの侵入ポリシー間または同じ侵入ポリシーの 2 つのリビジョン間のすべての違いを記録したものです。このレポートは、2 つの侵入ポリシー構成間の違いをさらに調査し、その結果を保存して共有するために使用できます。

侵入ポリシー比較レポートは、アクセス可能な任意の侵入ポリシーの比較ビューから生成できます。侵入ポリシー レポートを生成する前に未確定の変更をコミットするのを忘れないでください。コミットされた変更だけがレポートに表示されます。

侵入ポリシー比較レポートの形式は 1 つの例外（侵入ポリシー レポートには侵入ポリシー内のすべての設定が含まれる）を除いて侵入ポリシー レポートと同じであり、侵入ポリシー比較レポートにはポリシー間で異なる設定のみがリストされます。

構成に応じて、侵入ポリシー比較レポートに侵入ポリシー レポートのセクションの表に示す 1 つ以上のセクションを含めることができます。

ヒント　同様の手順で、SSL、アクセス コントロール、ネットワーク分析、ファイル、システム、またはヘルスのポリシーを比較できます。

2 つの侵入ポリシーまたは同じポリシーの 2 つのリビジョンを比較するには、以下を行います。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　[Compare Policies] をクリックします。

[Select Comparison] ウィンドウが表示されます。

ステップ 3　[Compare Against] ドロップダウンリストから、比較するタイプを次のように選択します。

- 異なる 2 つのポリシーを比較するには、[Other Policy] を選択します。
- 同じポリシーの 2 つのリビジョンを比較するには、[Other Revision] を選択します。

侵入ポリシー レポートを生成する前に変更をコミットするのを忘れないでください。コミットされた変更だけがレポートに表示されます。

ステップ 4　選択した比較タイプに応じて、次のような選択肢があります。

- 2 つの異なるポリシーを比較する場合は、[Policy A] および [Policy B] ドロップダウンリストのそれぞれから、比較するポリシーを選択します。
- 同じポリシーの 2 つのリビジョンを比較する場合は、[Policy] ドロップダウンリストからポリシーを選択し、次に [Revision A] および [Revision B] ドロップダウンリストから比較するリビジョンを選択します。

ステップ 5　侵入ポリシー比較ビューを表示するには、[OK] をクリックします。

比較ビューが表示されます。

ステップ 6　侵入ポリシー比較レポートを生成するには、[Comparison Report] をクリックします。

ステップ 7　侵入ポリシー レポートが表示されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。

ルールを使用した侵入ポリシーの調整

侵入ポリシーの [Rules] ページを使用して、shared object rule、標準テキスト ルール、およびプリプロセッサ ルールに関するルール状態とその他の設定を構成できます。

ルールは、ルール状態を [Generate Events] または [Drop and Generate Events] に設定することによって有効にします。ルールを有効にすると、システムがそのルールと一致するトラフィックに対するイベントを生成します。ルールを無効にすると、ルールの処理が停止されます。オプションで、インライン展開で [Drop and Generate Events] に設定されたルールによって、一致するトラフィックに対するイベントが生成され、そのトラフィックが破棄されるように、侵入ポリシーを設定できます。詳細については、「インライン展開でのドロップ動作の設定（31-6 ページ）」を参照してください。パッシブ展開では、[Drop and Generate Events] に設定されたルールによって、一致するトラフィックに対するイベントが生成されるだけです。

ルールのサブセットを表示するようにルールをフィルタ処理することによって、ルール状態やルール設定を変更するルールのセットを正確に選択できます。

侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。詳細については、カスタム ポリシーの制限（23-13 ページ）を参照してください。

詳細については、次の項を参照してください。

- 侵入防御ルール タイプについて（32-2 ページ）では、侵入ポリシーで表示または設定可能な侵入ルールとプリプロセッサ ルールについて説明します。
- 侵入ポリシー内のルールの表示（32-3 ページ）では、[Rules] ページでルールの順序を変更したり、ページ上のアイコンを解釈したり、ルール詳細に焦点を当てたりするための方法について説明します。
- 侵入ポリシー内のルールのフィルタ処理（32-10 ページ）では、ルール フィルタを使用して、ルール設定を適用するルールを見つける方法について説明します。
- ルール状態の設定（32-22 ページ）では、[Rules] ページでルールを有効または無効にする方法について説明します。
- ポリシー単位の侵入イベント通知のフィルタ処理（32-25 ページ）では、特定のルールに対するイベント フィルタリングしきい値の設定方法と特定のルールの抑制方法について説明します。
- 動的ルール状態の追加（32-33 ページ）では、一致するトラフィックでレート異常が検出されたときに動的にトリガーとして使用されるルール状態の設定方法について説明します。
- SNMP アラートの追加（32-36 ページ） では、SNMP アラートを特定のルールに関連付ける方法について説明します。
- ルール コメントの追加（32-38 ページ）では、侵入ポリシー内のルールにコメントを追加する方法について説明します。

侵入防御ルール タイプについて

ライセンス：Protection

侵入ポリシーには、侵入ルールとプリプロセッサ ルールという 2 つのルール タイプが含まれています。

侵入ルールは、ネットワーク上の脆弱性を悪用する試みを検出するキーワードと引数の指定されたセットで、ネットワーク トラフィックを分析してルール内の基準が満たされているかどうかをチェックします。システムが各ルール内で指定された条件とパケットを照らし合わせます。そして、パケット データとルール内で指定されたすべての条件が一致した場合に、ルールがトリガーとして使用されます。システムには、Cisco脆弱性調査チーム（VRT）が作成した次の 2 種類の侵入ルールが付属しています。shared object ruleは、コンパイルされ、変更できません（送信元ポート、宛先ポート、IP アドレスなどのルール 見出し情報を除く）。標準テキスト ルールは、ルールの新しいカスタム インスタンスとして保存して変更できます。

システムには、プリプロセッサに関連付けられたルールであるプリプロセッサ ルールとパケット デコーダ検出オプションも付属しています。プリプロセッサ ルールはコピーまたは編集できません。ほとんどのプリプロセッサ ルールがデフォルトで無効になっているため、システムにプリプロセッサ ルールに対するイベントの生成とインライン展開での違反パケットの破棄を指示する場合は、これらのルールを有効にする（つまり、[Generate Events] または [Drop and Generate Events] に設定する）必要があります。

VRT が、システムに付属のデフォルト侵入ポリシー用のCiscoのshared object rule、標準テキスト ルール、およびプリプロセッサ ルールのデフォルト ルール状態を決定します。

次の表に、FireSIGHT システムに付属しているルール タイプの説明を示します。

表 32-1　ルール タイプ

タイプ	説明
shared object rule	C ソース コードからコンパイルされたバイナリ モジュールとして配布されるCisco脆弱性調査チーム（VRT）によって作成された侵入ルール。shared object ruleを使用して、標準テキスト ルールでは不可能な方法で攻撃を検出できます。shared object rule内のルール キーワードと引数は変更できません。実行できるのは、ルール内で使用されている変数の変更か、送信元ポート、宛先ポート、IP アドレスなどの要素の変更とカスタムshared object ruleとしてのルールの新しいインスタンスの保存のみです。shared object ruleには、GID（ジェネレータ ID）の 3 が割り当てられます。詳細については、「既存のルールの変更（36-111 ページ）」を参照してください。
標準テキスト ルール	VRT によって作成された侵入ルール、コピーされて新しいカスタム ルールとして保存された侵入ルール、ルール エディタを使用して作成された侵入ルール、またはユーザがローカル マシン上で作成してインポートしたローカル ルールとしてインポートされた侵入ルール。VRT によって作成された標準ルール内のルール キーワードと引数は変更できません。実行できるのは、ルール内で使用されている変数の変更か、送信元ポート、宛先ポート、IP アドレスなどの要素の変更とカスタム標準テキスト ルールとしてのルールの新しいインスタンスの保存のみです。詳細については、既存のルールの変更（36-111 ページ）、侵入ルールの概要と作成（36-1 ページ）、およびローカル ルール ファイルのインポート（66-22 ページ）を参照してください。VRT によって作成された標準テキスト ルールには、GID（ジェネレータ ID）の 1 が割り当てられます。ルール エディタを使用して作成した、または、ローカル ルールとしてインポートしたカスタム 標準テキスト ルール には 1000000 以上の SID（シグニチャ ID）が割り当てられます。
プリプロセッサ ルール	パケット デコーダの検出オプションまたは FireSIGHT システムに付属のプリプロセッサの 1 つに関連付けられたルール。プリプロセッサ ルールによってイベントを生成するには、プリプロセッサ ルールを有効にする必要があります。このルールには、デコーダ固有またはプリプロセッサ固有の GID（ジェネレータ ID）が割り当てられます。詳細については、ジェネレータ IDの表を参照してください。

侵入ポリシー内のルールの表示

ライセンス： Protection

侵入ポリシーでのルールの表示方法を調整でき、複数の条件によってルールをソートできます。特定のルールの詳細を表示して、ルール設定、ルール ドキュメント、およびその他のルール仕様を確認することもできます。

[Rules] ページには次の 4 つの主な機能領域があります。

- フィルタリング機能：詳細については、侵入ポリシー内のルールのフィルタ処理（32-10 ページ）を参照してください。
- ルール属性メニュー：詳細については、ルール状態の設定（32-22 ページ）、ポリシー単位の侵入イベント通知のフィルタ処理（32-25 ページ）、動的ルール状態の追加（32-33 ページ）、SNMP アラートの追加（32-36 ページ）、およびルール コメントの追加（32-38 ページ）を参照してください。
- ルール一覧：詳細については、[Rules] ページのカラム の表を参照してください。
- ルールの詳細：詳細については、ルール詳細の表示（32-5 ページ）を参照してください。

さまざまな基準に基づいてルールをソートすることもできます。詳細については、ルール画面のソート（32-4 ページ）を参照してください。

カラム見出しとして使用されているアイコンは、設定項目にアクセスするためのメニュー バー内のメニューに対応していることに注意してください。たとえば、[Rule State] メニューは、[Rule State] カラムと同じアイコン（  ）でマークされています。

次の表に、[Rules] ページのカラムの説明を示します。

表 32-2　[Rules] ページのカラム

見出し	説明	詳細情報の参照先
GID	ルールのジェネレータ ID（GID）を表す整数。	プリプロセッサ ジェネレータ ID の読み取り（41-42 ページ）
SID	ルールの一意の識別子として機能する Snort ID（SID）を表す整数。	プリプロセッサ ジェネレータ ID の読み取り（41-42 ページ）
Message	このルールによって生成されるイベントに含まれるメッセージ。ルールの名前としても機能する。	イベント メッセージの定義（36-12 ページ）
	ルールのルール状態。次の 3 つのうちのいずれか。 • ドロップしてイベントを生成する（  ） • イベントを生成する（） • 無効にする（） ルール状態アイコンをクリックすることによって、ルールの [Set rule state] ダイアログボックスにアクセスできることに注意してください。	ルール状態の設定（32-22 ページ）
	ルールの FireSIGHT推奨ルール状態。	ネットワーク資産に応じた侵入防御の調整（33-1 ページ）
	ルールに適用されるイベントしきい値やイベント抑制などのイベント フィルタ。	ポリシー単位の侵入イベント通知のフィルタ処理（32-25 ページ）

表 32-2　[Rules] ページのカラム（続き）

見出し	説明	詳細情報の参照先
	ルールの動的ルール状態。指定されたレート異常が発生した場合に有効になります。	動的ルール状態の追加（32-33 ページ）
	ルールに対して設定されたアラート（現在は SNMP アラートのみ）。	SNMP アラートの追加（32-36 ページ）
	ルールに追加されたコメント。	ルール コメントの追加（32-38 ページ）

レイヤのドロップダウンリストを使用して、ポリシー内の他のレイヤの [Rules] ページに切り替えることもできます。ポリシーにレイヤを追加しなかった場合にドロップダウンリストに表示される編集可能なビューはポリシーの [Rules] ページと、元は `My Changes` という名前だったポリシー階層の [Rules] ページだけであることに注意してください。これらのビューの一方を変更すると、もう一方も同じように変更されることにも注意してください。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。ドロップダウンリストには、読み取り専用の基本ポリシーの [Rules] ページも表示されます。基本ポリシーの詳細については、基本レイヤについて（24-3 ページ）を参照してください。

侵入ポリシー内のルールを表示する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Policy Information] ページで [Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ナビゲーション パネルの境界線の上にある [Rules] を選択すると、同じルール一覧が表示されることに注意してください。このビューでポリシー内のすべてのルール属性を表示して設定できます。

ルール画面のソート

ライセンス： Protection

[Rules] ページでは、見出しタイトルまたはアイコンをクリックすることによって、ルールをいずれかのカラムでソートできます。

見出しまたはアイコン上の上矢印（▲）または下矢印（▼）は、そのカラムを基準として、その方向にソートが実行されることを意味していることに注意してください。

侵入ポリシー内でルールをソートする方法:

アクセス: Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーでまだ保存されていない変更がある場合、それらの変更を破棄して続行するには [OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(23-17 ページ)を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4　ソートの基準とするカラムの一番上のタイトルまたはアイコンをクリックします。

ルールがそのカラムのカラム見出しに表示された矢印が示す方向でソートされます。反対方向でソートするには、見出しを再度クリックします。ソート順と矢印が反転します。

ルール詳細の表示

ライセンス: Protection

[Rule Detail] ビューで、ルール ドキュメント、FireSIGHT推奨、およびルール オーバーヘッドを表示できます。また、ルール固有の機能を表示および追加できます。

脆弱性にマップされていないローカル ルールにはオーバーヘッドがないことに注意してください。

表 32-3　ルールの詳細

項目	説明	詳細情報の参照先
概要	ルールの概要。ルール ベースのイベントでは、ルール ドキュメントに概要情報が含まれている場合にこの行が表示されます。	イベント情報の表示(41-25 ページ)
Rule State	ルールの現在のルール状態。ルール状態が設定された階層も示します。	ルール状態の設定(32-22 ページ)、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用(24-1 ページ)
FireSIGHT Recommendation	FireSIGHT推奨が生成されている場合のルールの推奨ルール状態。	ネットワーク資産に応じた侵入防御の調整(33-1 ページ)
Rule Overhead	システム パフォーマンスに対するルールの潜在的影響とルールが誤検出を引き起こす確率。	ルール オーバーヘッドについて(33-3 ページ)
しきい値	このルールに現在設定されているしきい値と、ルールのしきい値を追加するための機能。	ルールのしきい値の設定(32-7 ページ)

表 32-3　ルールの詳細（続き）

項目	説明	詳細情報の参照先
Suppressions	このルールに現在設定されている抑制設定と、ルールの抑制を追加するための機能。	ルールの抑制の設定（32-7 ページ）
Dynamic State	このルールに現在設定されているレート ベースのルール状態と、ルールの動的ルール状態を追加するための機能。	ルールの動的ルール状態の設定（32-8 ページ）
Alerts	このルールに現在設定されているアラートと、ルールのアラートを追加するための機能。現在は、SNMP アラートのみがサポートされています。	ルールの SNMP アラートの設定（32-9 ページ）
注	このルールに追加されたコメントと、ルールのコメントを追加するための機能。	ルールに関するルール コメントの追加（32-10 ページ）
マニュアル	Cisco脆弱性調査チーム（VRT）から提供される現在のルールのルール ドキュメント。	パケット ビュー アクションの使用（41-29 ページ）

ルール詳細を表示する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4　ルール詳細を表示するルールを強調表示します。

ステップ 5　[Show details] をクリックします。

[Rule Detail] ビューが表示されます。詳細を再度非表示にするには、[Hide details] をクリックします。

ヒント　[Rules] ビューでルールをダブル クリックすることによって、[Rule Detail] を開くこともできます。

ルールのしきい値の設定

ライセンス：Protection

[Rule Detail] ページで、ルールの単一のしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。しきい値設定の詳細については、イベントしきい値の設定（32-25 ページ）を参照してください。

無効な値を入力するとフィールドに復元アイコン（）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ルール詳細でしきい値を設定する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Thresholds] の横にある [Add] をクリックします。

[Set Threshold] ダイアログボックスが表示されます。

ステップ 2　[Type] ドロップダウンリストから、設定するしきい値のタイプを選択します。

- 指定された期間あたりのイベント インスタンス数に通知を制限する場合は、[Limit] を選択します。
- 指定された期間あたりのイベント インスタンス数ごとに通知を提供する場合は、[Threshold] を選択します。
- 指定されたイベント インスタンス数後に期間あたり 1 回ずつ通知を提供する場合は、[Both] を選択します。

ステップ 3　[Track By] ドロップダウンリストから、[Source] または [Destination] を選択し、イベント インスタンスが送信元 IP アドレスまたは宛先 IP アドレスのどちらによって追跡されるかを指定します。

ステップ 4　[Count] フィールドに、しきい値として使用するイベント インスタンスの数を入力します。

ステップ 5　[Seconds] フィールドで、イベント インスタンスをトラックする期間（秒数）を指定する 0 から 2147483647 までの数を入力します。

ステップ 6　[OK] をクリックします。

システムが、しきい値を追加し、[Event Filtering] カラムのルールの横にイベント フィルタ アイコン（  ）を表示します。ルールに複数のイベント フィルタを追加すると、アイコン上にイベント フィルタの数が表示されます。

ルールの抑制の設定

ライセンス：Protection

[Rule Detail] ページで、ルールの 1 つまたは複数の抑制を設定できます。抑制の詳細については、侵入ポリシー単位の抑制の設定（32-30 ページ）を参照してください。

無効な値を入力するとフィールドに復元アイコン（）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ルール詳細で抑制を設定する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Suppressions] の横にある [Add] をクリックします。

[Add Suppression] ダイアログボックスが表示されます。

ステップ 2　[Suppression Type] ドロップダウンリストから、次のいずれかのオプションを選択します。

- 選択したルールのイベントを完全に抑制する場合は、[Rule] を選択します。
- 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[Source] を選択します。
- 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[Destination] を選択します。

ステップ 3　抑制タイプに [Source] または [Destination] を選択した場合は、[Network] フィールドが表示されます。[Network] フィールドで、IP アドレス、アドレス ブロック、またはこれらを任意に組み合わせたカンマ区切りのリストを入力します。侵入ポリシーがアクセス コントロール ポリシーのデフォルト アクションに関連付けられている場合は、デフォルト アクション変数セットでネットワーク変数を指定または列挙することもできます。

FireSIGHT システムで IPv4 CIDR と IPv6 プレフィクス長アドレス ブロックを使用する方法については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ステップ 4　[OK] をクリックします。

システムが、抑制条件を追加し、抑制するルールの横にある [Event Filtering] カラムのルールの横にイベント フィルタ アイコン（  ）を表示します。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

ルールの動的ルール状態の設定

ライセンス： Protection

[Rule Detail] ページで、ルールの 1 つまたは複数の動的ルール状態を設定できます。最初に表示される動的ルール状態に最も高いプライオリティが割り当てられます。2 つの動的ルール状態が競合している場合は、最初のアクションが実行されることに注意してください。動的ルール状態の詳細については、動的ルール状態について（32-33 ページ）を参照してください。

無効な値を入力するとフィールドに復元アイコン（  ）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ルール詳細で動的ルール状態を設定する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Dynamic State] の横にある [Add] をクリックします。

[Add Rate-Based Rule State] ダイアログボックスが表示されます。

ステップ 2　[Track By] ドロップダウンリストから、ルール一致の追跡方法を指定するオプションを選択します。

- 特定の送信元または送信元のセットからのそのルールのヒット数を追跡する場合は、[Source] を選択します。

- 特定の宛先または宛先のセットへのそのルールのヒット数を追跡する場合は、[Destination] を選択します。
- そのルールのすべての一致を追跡する場合は、[Rule] を選択します。

ステップ 3　オプションで、[Track By] を [Source] または [Destination] に設定した場合は、[Network] フィールドに追跡する各ホストの IP アドレスを入力します。

FireSIGHT システムで IPv4 CIDR と IPv6 プレフィクス長表記を使用する方法については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ステップ 4　[Rate] の隣で、攻撃レートを設定する期間あたりのルール一致の数を指定します。

- [Count] フィールドで、0 ～ 2147483647 の整数を使用して、しきい値として使用するルール一致の数を指定します。
- [Seconds] フィールドで、0 ～ 2147483647 の整数を使用して、攻撃を追跡する期間を表す秒数を指定します。

ステップ 5　[New State] ドロップダウンリストから、条件が満たされたときに実行すべき新しいアクションを選択します。

- イベントを生成する場合は、[Generate Events] を選択します。
- インライン展開でイベントを生成し、イベントをトリガーしたパケットを破棄する場合、または、パッシブ展開でイベントを生成する場合は、[Drop and Generate Events] を選択します。
- アクションを実行しない場合は、[Disabled] を選択します。

ステップ 6　[Timeout] フィールドに、1 ～ 2147483647（約 68 年）の整数を使用して、新しいアクションを有効にしておく秒数を入力します。タイムアウトが発生すると、ルールが元の状態に戻ります。新しいアクションがタイムアウトしないようにする場合は、0 を指定します。

ステップ 7　[OK] をクリックします。

システムが、動的ルール状態を追加し、[Dynamic State] カラムのルールの横に動的状態アイコン（  ）を表示します。ルールに複数の動的ルール状態フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

必須フィールドを空白にした場合は、フィールドに値を入力する必要があることを伝えるエラー メッセージが表示されます。

ルールの SNMP アラートの設定

ライセンス： Protection

[Rule Detail] ページで、ルールの SNMP アラートを設定できます。SNMP アラートの詳細については、SNMP アラートの追加（32-36 ページ）を参照してください。

ルール詳細で SNMP アラートを追加する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Alerts] の横にある [Add SNMP Alert] をクリックします。

システムが、アラートを追加し、[Alerting] カラムのルールの横にアラート アイコン（  ）を表示します。ルールに複数のアラートを追加した場合は、アイコン上にアラートの数が表示されます。

ルールに関するルール コメントの追加

ライセンス：Protection

[Rule Detail] ページで、ルールに関するルール コメントを追加できます。ルール コメントの詳細については、ルール コメントの追加（32-38 ページ）を参照してください。

ルール詳細でコメントを追加する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Comments] の横にある [Add] をクリックします。

[Add Comment] ダイアログボックスが表示されます。

ステップ 2　[Comment] フィールドに、ルール コメントを入力します。

ステップ 3　[OK] をクリックします。

システムが、コメントを追加し、[Comments] カラムのルールの横にコメント アイコン（  ）を表示します。ルールに複数のコメントを追加した場合は、アイコン上の数字がコメントの数を示します。

ヒント　ルール コメントを削除するには、ルール コメント セクションで [Delete] をクリックします。侵入ポリシーの変更がコミットされていないコメントがキャッシュされている場合にだけ、コメントを削除できることに注意してください。侵入ポリシーの変更がコミットされた後は、ルール コメントを削除できなくなります。

侵入ポリシー内のルールのフィルタ処理

ライセンス：Protection

[Rules] ページに表示するルールは、1 つの基準または 1 つ以上の基準の組み合わせに基づいてフィルタ処理できます。

作成したフィルタが [Filter] テキスト ボックスに表示されます。フィルタ パネルでキーワードとキーワード引数をクリックしてフィルタを作成できます。複数のキーワードを選択した場合は、システムがそれらを AND ロジックを使用して結合し、複合検索フィルタを生成します。たとえば、[Category] で [preprocessor] を選択してから、[Rule Content] > [GID] の順に選択して、「116」と入力すると、プリプロセッサ ルールで、**かつ**、GID が 116 のすべてのルールを取得する「`Category: "preprocessor" GID:"116"`」というフィルタが返されます。

Category、Microsoft Vulnerabilities、Microsoft Worms、Platform Specific、Preprocessor、および Priority の各フィルタ グループを使用すれば、カンマで区切られたキーワードの複数の引数を送信できます。たとえば、Shift キーを押しながら、[Category] から [os-linux] と [os-windows] を選択すれば、`os-linux` カテゴリまたは `os-windows` カテゴリ内のルールを取得する「`Category:"os-windows,os-linux"`」というフィルタを作成できます。

フィルタ パネルを表示するには、表示アイコン（  ）をクリックします。

フィルタ パネルを非表示にするには、非表示アイコン（  ）をクリックします。

詳細については、次のトピックを参照してください。

- 侵入ポリシー内のルール フィルタ処理について（32-11 ページ）
- 侵入ポリシー内のルール フィルタの設定（32-21 ページ）

侵入ポリシー内のルール フィルタ処理について

ライセンス：Protection

ルール フィルタ キーワードは、ルール状態やイベント フィルタなどのルール設定を適用するルールを見つけやすくします。[Rules] ページのフィルタ パネルで必要な引数を選択することによって、キーワードでフィルタ処理すると同時に、キーワードの引数を選択することができます。

詳細については、次の項を参照してください。

- 侵入ポリシー ルール フィルタを作成するためのガイドライン（32-11 ページ）
- ルール構成フィルタについて（32-14 ページ）
- ルール コンテンツ フィルタについて（32-17 ページ）
- ルール カテゴリについて（32-19 ページ）
- ルール フィルタの直接編集（32-19 ページ）

侵入ポリシー ルール フィルタを作成するためのガイドライン

ライセンス：Protection

ほとんどの場合、フィルタを作成するときに、侵入ポリシー内の [Rules] ページの左側にあるフィルタ パネルを使用して必要なキーワード/引数を選択できます。

フィルタ パネルでは、ルール フィルタがルール フィルタ グループに分類されます。多くのルール フィルタ グループにサブ基準が含まれているため、探している特定のルールを簡単に見つけることができます。一部のルール フィルタには、展開して個別のルールにドリルダウンするための複数のレベルが設定されています。

フィルタ パネル内の項目は、場合によって、フィルタ タイプ グループを表したり、キーワードを表したり、キーワードの引数を表したりします。次の経験則をフィルタの作成に役立ててください。

- キーワード（Rule Configuration、Rule Content、Platform Specific、および Priority）以外のフィルタ タイプ グループ見出しを選択すると、そのグループが展開して使用可能なキーワードが一覧表示されます。

  基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定するためのポップアップ ウィンドウが表示されます。

  そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

  たとえば、フィルタ パネルの [Rule Configuration] > [Recommendation] で [Drop and Generate Events] をクリックすると、「`Recommendation:"Drop and Generate Events"`」がフィルタ テキスト ボックスに追加されます。その後で、[Rule Configuration] > [Recommendation] で [Generate Events] をクリックすると、フィルタが「`Recommendation:"Generate Events"`」に変更されます。
- キーワード（Category、Classifications、Microsoft Vulnerabilities、Microsoft Worms、Priority、および Rule Update）になっているフィルタ タイプ グループ見出しを選択すると、使用可能な引数が一覧表示されます。

このタイプのグループから項目を選択すると、適用される引数とキーワードがすぐにフィルタに追加されます。キーワードがすでにフィルタ内に存在していた場合は、そのグループに対応するキーワードの既存の引数が置き換えられます。

たとえば、フィルタ パネルの [Category] で [os-linux] をクリックすると、「`Category:"os-linux"`」がフィルタ テキスト ボックスに追加されます。その後で、[Category] で [os-windows] をクリックすると、フィルタが「`Category:"os-windows"`」に変更されます。

- [Rule Content] の下の [Reference] はキーワードであり、その下に特定の参照 ID タイプが列挙されます。参照キーワードのいずれかを選択すると、引数を指定するためのポップアップ ウィンドウが表示され、キーワードが既存のフィルタに追加されます。キーワードがすでにフィルタ内で使用されていた場合は、既存の引数が指定した新しい引数に置き換えられます。

  たとえば、フィルタ パネルで [Rule Content] > [Reference] > [CVE ID] の順にクリックすると、ポップアップ ウィンドウが開いて CVE ID を指定するよう示されます。「`2007`」と入力すると、「`CVE:"2007"`」がフィルタ テキスト ボックスに追加されます。別の例では、フィルタ パネルで [Rule Content] > [Reference] の順にクリックすると、ポップアップ ウィンドウが開いて、参照を指定するよう示されます。「`2007`」と入力すると、「`Reference:"2007"`」がフィルタ テキスト ボックスに追加されます。

- 複数のグループからルール フィルタ キーワードを選択した場合は、各フィルタ キーワードがフィルタに追加され、既存のキーワードが維持されます（同じキーワードの新しい値で上書きされなかった場合）。

  たとえば、フィルタ パネルの [Category] で [os-linux] をクリックすると、「`Category:"os-linux"`」がフィルタ テキスト ボックスに追加されます。その後で、[Microsoft Vulnerabilities] で [MS00-006] をクリックすると、フィルタが「`Category:"os-linux" MicrosoftVulnerabilities:"MS00-006"`」に変更されます。

- 複数のキーワードを選択した場合は、システムがそれらを AND ロジックを使用して結合し、複合検索フィルタを生成します。たとえば、[Category] で [preprocessor] を選択してから、[Rule Content] > [GID] の順に選択して、「`116`」と入力すると、プリプロセッサ ルールで、**かつ**、GID が 116 のすべてのルールを取得する「`Category: "preprocessor" GID:"116"`」というフィルタが返されます。

- Category、Microsoft Vulnerabilities、Microsoft Worms、Platform Specific、および Priority の各フィルタ グループを使用すれば、カンマで区切られたキーワードの複数の引数を送信できます。たとえば、Shift キーを押しながら、[Category] から [os-linux] と [os-windows] を選択すれば、`os-linux` カテゴリまたは `os-windows` カテゴリ内のルールを取得する「`Category:"os-windows,app-detect"`」というフィルタを作成できます。

複数のフィルタ キーワード/引数のペアで同じルールが取得される場合があります。たとえば、ルールが **dos** カテゴリでフィルタ処理された場合と **High** 優先度でフィルタ処理された場合はともに、DOS Cisco attempt rule（SID 1545）が表示されます。

注　Cisco VRT がルール更新メカニズムを使用してルール フィルタを追加または削除する場合があります。

[Rules] ページ上のルールは、shared object rule（ジェネレータ ID 3）と標準テキスト ルール（ジェネレータ ID 1）のどちらかであることに注意してください。次の表に、さまざまなルール フィルタの説明を示します。

表 32-4　ルール フィルタ グループ

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
Rule Configuration	ルールの設定に基づいてルールを検索します。ルール構成フィルタについて（32-14 ページ）を参照してください。	No	グループ	キーワード
Rule Content	ルールの内容に基づいてルールを検索します。ルール コンテンツ フィルタについて（32-17 ページ）を参照してください。	No	グループ	キーワード
カテゴリ	ルール エディタで使用されるルール カテゴリに基づいてルールを検索します。ローカル ルールはローカル サブグループに表示されることに注意してください。ルール カテゴリについて（32-19 ページ）を参照してください。	Yes	キーワード	引数
Classifications	ルールによって生成されるイベントのパケット画面内に表示される攻撃分類に基づいてルールを検索します。侵入イベントの検索（41-44 ページ）および侵入イベント分類の定義（36-13 ページ）を参照してください。	No	キーワード	引数
Microsoft Vulnerabilities	Microsoft セキュリティ情報番号に従ってルールを検索します。	Yes	キーワード	引数
Microsoft Worms	Microsoft Windows ホストに影響する特定のワームに基づいてルールを検索します。	Yes	キーワード	引数
Platform Specific	オペレーティング システムの特定のバージョンとの関連性に基づいてルールを検索します。 ルールが複数のオペレーティング システムまたは 1 つのオペレーティング システムの複数のバージョンに影響する場合があることに注意してください。たとえば、SID 2260 を有効にすると、Mac OS X、IBM AIX、およびその他のオペレーティング システムの複数のバージョンに影響します。	Yes	キーワード	引数 サブリストからいずれかの項目を選択すると、引数に修飾子が追加されることに注意してください。
Preprocessors	個別のプリプロセッサのルールを検索します。 プリプロセッサが有効になっている場合にプリプロセッサ オプションに対するイベントを生成するためには、そのオプションに関連付けられたプリプロセッサ ルールを有効にする必要があることに注意してください。ルール状態の設定（32-22 ページ）を参照してください。	Yes	グループ	サブグループ

表 32-4　ルール フィルタ グループ（続き）

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
プライオリティ	高、中、および低の優先度に基づいてルールを検索します。 ルールに割り当てられた分類によってその優先度が決定されます。これらのグループは、さらにルール カテゴリに分類されます。ローカル ルール（つまり、ユーザが作成したルール）は優先度グループに表示されないことに注意してください。	Yes	キーワード	引数 サブリストからいずれかの項目を選択すると、引数に修飾子が追加されることに注意してください。
Rule Update	特定のルール更新を通して追加または変更されたルールを検索します。ルール更新ごとに、更新内のすべてのルール、更新でインポートされた唯一の新しいルール、または更新によって変更された唯一の既存のルールを表示します。	No	キーワード	引数

ルール構成フィルタについて

ライセンス： Protection

[Rules] ページに表示されたルールをいくつかのルール構成設定でフィルタ処理できます。たとえば、ルール状態が推奨ルール状態と一致しない一連のルールを表示する場合は、[Does not match recommendation] を選択することによってルール状態をフィルタ処理できます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定するためのポップアップ ウィンドウが表示されます。

そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

たとえば、フィルタ パネルの [Rule Configuration] > [Recommendation] で [Drop and Generate Events] をクリックすると、「`Recommendation:"Drop and Generate Events"`」がフィルタ テキスト ボックスに追加されます。その後で、[Rule Configuration] > [Recommendation] で [Generate Events] をクリックすると、フィルタが「`Recommendation:"Generate Events"`」に変更されます。

フィルタ処理に使用可能なルール構成設定に関する詳細については、次の手順を参照してください。

ルール状態フィルタを使用する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Rule Configuration] で、[Rule State] をクリックします。

ステップ 2　[Rule State] ドロップダウンリストから、フィルタ条件のルール状態を選択します。

- イベントを生成するだけのルールを検索するには、[Generate Events] を選択して、[OK] をクリックします。
- イベントを生成して一致するパケットをドロップするよう設定されたルールを検索するには、[Drop and Generate Events] を選択して、[OK] をクリックします。

- 無効になっているルールを検索するには、[Disabled] を選択して、[OK] をクリックします。
- ルール状態が推奨状態と一致しないルールを検索するには、[Does not match recommendation] を選択して、[OK] をクリックします。

最新のルール状態に基づいてルールを表示するように [Rules] ページが更新されます。

推奨フィルタを使用する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Rule Configuration] で、[Recommendation] をクリックします。

ステップ 2　[Recommendation] ドロップダウン リストから、フィルタ条件となる FireSIGHT ルール状態の推奨事項を選択し、[OK] をクリックします。

推奨ルール状態に基づいてルールを表示するように [Rules] ページが更新されます。

しきい値フィルタを使用する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Rule Configuration] で、[Threshold] をクリックします。

ステップ 2　[Threshold] ドロップダウンリストから、フィルタ条件のしきい値設定を選択します。

- しきい値タイプが `limit` のルールを検索するには、[Limit] を選択して、[OK] をクリックします。
- しきい値タイプが `threshold` のルールを検索するには、[Threshold] を選択して、[OK] をクリックします。
- しきい値タイプが `both` のルールを検索するには、[Both] を選択して、[OK] をクリックします。
- しきい値が**送信元**によって追跡されるルールを検索するには、[Source] を選択して、[OK] をクリックします。
- しきい値が**宛先**によって追跡されるルールを検索するには、[Destination] を選択して、[OK] をクリックします。
- しきい値が設定された任意のルールを検索するには、[All] を選択して、[OK] をクリックします。

フィルタで指定されたしきい値のタイプがルールに適用されているルールを表示するように [Rules] ページが更新されます。

抑制フィルタを使用する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Rule Configuration] で、[Suppression] をクリックします。

ステップ 2　[Suppression] ドロップダウンリストから、フィルタ条件の抑制設定を選択します。

- イベントがそのルールによって検査されるパケットに抑制されたルールを検索するには、[By Rule] を選択して、[OK] をクリックします。

- イベントがトラフィックの送信元に基づいて抑制されるルールを検索するには、[By Source] を選択して、[OK] をクリックします。
- イベントがトラフィックの宛先に基づいて抑制されるルールを検索するには、[By Destination] を選択して、[OK] をクリックします。
- 抑制が設定された任意のルールを検索するには、[All] を選択して、[OK] をクリックします。

フィルタで指定された抑制のタイプがルールに適用されているルールを表示するように [Rules] ページが更新されます。

動的状態フィルタを使用する方法:

アクセス: Admin/Intrusion Admin

ステップ 1　[Rule Configuration] で、[Dynamic State] をクリックします。

ステップ 2　[Dynamic State] ドロップダウンリストから、フィルタ条件の抑制設定を選択します。

- 動的状態がそのルールによって検査されるパケットに設定されたルールを検索するには、[By Rule] を選択して、[OK] をクリックします。
- 動的状態がトラフィックの送信元に基づくパケットに設定されたルールを検索するには、[By Source] を選択して、[OK] をクリックします。
- 動的状態がトラフィックの宛先に基づいて設定されたルールを検索するには、[By Destination] を選択して、[OK] をクリックします。
- `Generate Events` の動的状態が設定されたルールを検索するには、[Generate Events] を選択して、[OK] をクリックします。
- `Drop and Generate Events` の動的状態が設定されたルールを検索するには、[Drop and Generate Events] を選択して、[OK] をクリックします。
- `Disabled` の動的状態が設定されたルールを検索するには、[Disabled] を選択して、[OK] をクリックします。
- 抑制が設定された任意のルールを検索するには、[All] を選択して、[OK] をクリックします。

フィルタで指定された動的ルール状態がルールに適用されているルールを表示するように [Rules] ページが更新されます。

アラート フィルタを使用するには、次の手順を実行します。

アクセス: Admin/Intrusion Admin

ステップ 1　[Rule Configuration] で、[Alert] をクリックします。

ステップ 2　[Alert] ドロップダウンリストから、**SNMP** 別にフィルタ処理するアラート設定を選択します。

ステップ 3　[OK] をクリックします。

[Rules] ページが更新され、アラート フィルタを適用したルールが表示されます。

コメント フィルタを使用する方法:

アクセス: Admin/Intrusion Admin

ステップ 1　[Rule Configuration] で、[Comment] をクリックします。

ステップ 2　[Comment] フィールドに、フィルタ条件のコメント テキスト文字列を入力し、[OK] をクリックします。

ルールに適用されるコメントにフィルタで指定された文字列が含まれているルールを表示するように [Rules] ページが更新されます。

ルール コンテンツ フィルタについて

ライセンス: Protection

[Rules] ページに表示されたルールをいくつかのルール コンテンツ項目でフィルタ処理できます。たとえば、ルールの SID を検索することによって、ルールをすばやく取得できます。特定の宛先ポートに送信されるトラフィックを検査するすべてのルールを検索することもできます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定するためのポップアップ ウィンドウが表示されます。

そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

たとえば、フィルタ パネルの [Rule Content] で [SID] をクリックすると、ポップアップ ウィンドウが開いて SID の入力が促されます。「1045」と入力すると、「SID:"1045"」がフィルタ テキスト ボックスに追加されます。その後で、再度 [SID] をクリックして、SID フィルタを「1044」に変更すると、フィルタが「SID:"1044"」に変更されます。

フィルタ処理に使用可能なルール コンテンツの詳細については、次の表を参照してください。

表 32-5　ルール コンテンツ フィルタ

このフィルタを使用する場合のクリック対象	結果	結果
メッセージ	フィルタ条件のメッセージ文字列を入力して、[OK] をクリックします。	メッセージ フィールドで指定された文字列を含むルールを検索します。
SID	フィルタ条件の SID 番号を入力して、[OK] をクリックします。	指定された SID が割り当てられたルールを検索します。
GID	フィルタ条件の GID 番号を入力して、[OK] をクリックします。	指定された GID が割り当てられたルールを検索します。
参照先	フィルタ条件の参照文字列を入力して、[OK] をクリックします。 フィルタ条件とする特定のタイプの参照に対する文字列を入力するには、[CVE ID]、[URL]、[Bugtraq ID]、[Nessus ID]、[Arachnids ID]、または [Mcafee ID] を選択し、文字列を入力して [OK] をクリックします。	参照フィールドで指定された文字列を含むルールを検索します。

表 32-5　ルール コンテンツ フィルタ（続き）

このフィルタを使用する場合のクリック対象	結果	結果
Action	フィルタ処理するアクションを選択します。 • アラート ルールを検索するには、[Alert] を選択して、[OK] をクリックします。 • パス ルールを検索するには、[Pass] を選択して、[OK] をクリックします。	`alert` または `pass` で始まるルールを検索します。
Protocol	フィルタ条件のプロトコル（[ICMP]、[IP]、[TCP]、または [UDP]）を選択し、[OK] をクリックします。	選択されたプロトコルを含むルールを検索します。
方向	フィルタ処理する方向設定を選択します。 • 特定の方向に移動するトラフィックを検査するルールを検索するには、[Directional] を選択して、[OK] をクリックします。 • 送信元と宛先の間をどちらの方向にも移動するトラフィックを検査するルールを検索するには、[Bidirectional] を選択して、[OK] をクリックしてします。	ルールに、指定された方向設定が含まれているかどうかに基づいてルールを検索します。
Source IP	フィルタ条件の送信元 IP アドレスを入力して、[OK] をクリックします。 有効な IP アドレス、CIDR ブロック/プレフィクス長、または `$HOME_NET` や `$EXTERNAL_NET` などの変数を使用してフィルタ処理できることに注意してください。	ルール内の送信元 IP アドレス宛先に指定されたアドレスまたは変数を使用するルールを検索します。
Destination IP	フィルタ条件の宛先 IP アドレスを入力して、[OK] をクリックします。 有効な IP アドレス、CIDR ブロック/プレフィクス長、または `$HOME_NET` や `$EXTERNAL_NET` などの変数を使用してフィルタ処理できることに注意してください。	ルール内の送信元 IP アドレス宛先に指定されたアドレスまたは変数を使用するルールを検索します。
送信元ポート	フィルタ条件の送信元ポートを入力して、[OK] をクリックします。 ポート値は、1 ～ 65535 の整数またはポート変数にする必要があります。	指定された送信元ポートを含むルールを検索します。

表 32-5　ルール コンテンツ フィルタ（続き）

このフィルタを使用する場合のクリック対象	結果	結果
宛先ポート	フィルタ条件の宛先ポートを入力して、[OK] をクリックします。 ポート値は、1 ～ 65535 の整数またはポート変数にする必要があります。	指定された宛先ポートを含むルールを検索します。
Rule Overhead	フィルタ条件のルール オーバーヘッドの量（[Low]、[Medium]、[High]、または [Very High]）を選択し、[OK] をクリックします。	選択されたルール オーバーヘッドを伴うルールを検索します。
メタデータ	フィルタ条件のメタデータのキーと値のペアをスペースで区切って入力し、[OK] をクリックします。 たとえば、HTTP アプリケーション プロトコルに関連するメタデータを使用したルールを検索するには、「`metadata:"service http"`」と入力します。	一致するキーと値のペアを含むメタデータを使用したルールを検索します。

ルール カテゴリについて

ライセンス：Protection

FireSIGHT システムは、ルールが検出するトラフィックのタイプに基づいてカテゴリにルールを配置します。[Rules] ページで、ルール カテゴリでフィルタ処理することによって、カテゴリ内のすべてのルールにルール属性を設定できます。たとえば、ネットワーク上に Linux ホストが存在しない場合は、**os-linux** カテゴリでフィルタ処理してから、表示されたすべてのルールを無効にすることによって、**os-linux** カテゴリ全体を無効にすることができます。

カテゴリ名の上にポインタを移動すると、そのカテゴリ内のルールの数を表示できます。

注　Cisco VRT がルール更新メカニズムを使用してルール カテゴリを追加または削除する場合があります。

ルール フィルタの直接編集

ライセンス：Protection

フィルタ パネルでフィルタをクリックしたときに入力される特殊なキーワードとその引数を変更するようにフィルタを編集できます。[Rules] ページのカスタム フィルタはルール エディタで使用されるものと同様に機能しますが、フィルタ パネルを通してフィルタを選択したときに表示される構文を使用して、[Rules] ページのフィルタに入力されたキーワードのいずれかを使用することもできます。今後使用するキーワードを決定するには、右側のフィルタ パネルで該当する引数をクリックします。フィルタ キーワードと引数構文がフィルタ テキスト ボックスに表示されます。

特定の値のみをサポートするキーワードの引数のリストを表示するには、ルール構成フィルタについて(32-14 ページ)、ルール コンテンツ フィルタについて(32-17 ページ)、およびルール カテゴリについて(32-19 ページ)を参照してください。キーワードのカンマ区切りの複数の引数は Category と Priority のフィルタ タイプでしかサポートされないことに注意してください。

引用符内のキーワードと引数、文字列、およびリテラル文字列と一緒に、複数のフィルタ条件を区切るスペースを使用できます。ただし、正規表現、ワイルドカード文字、または否定文字(!)、大なり記号(>)、小なり記号(<)などの特殊な演算子を含めることはできません。キーワードなし、キーワードの先頭文字の大文字表記なし、または引数の周りの引用符なしの検索語を入力すると、検索が文字列検索として扱われ、[Category]、[Message]、および [SID] の各フィールドで指定された単語が検索されます。

すべてのキーワード、キーワード引数、および文字列では大文字と小文字が区別されません。`gid` キーワードと `sid` キーワードを除くすべての引数と文字列が部分文字列として扱われます。`gid` と `sid` の引数は完全一致のみを返します。

ルール フィルタごとに、次の形式で 1 つ以上のキーワードを含めることができます。

`Keyword:"argument"`

ここで、*`Keyword`* はルール タイプ の表に示すフィルタ グループ内のキーワードのいずれかで、*`argument`* は二重引用符で囲まれ、キーワードに関連した特定のフィールド内で検索される単一の大文字と小文字が区別されない英数字文字列です。キーワードは先頭文字を大文字にして入力する必要があることに注意してください。

`gid` と `sid` を除くすべてのキーワードの引数が部分文字列として扱われます。たとえば、引数の `123` は、`"12345"`、`"41235"`、`"45123"` などを返します。`gid` と `sid` の引数は完全一致のみを返します。たとえば、`sid:3080` は `SID 3080` のみを返します。

各ルール フィルタに、1 つ以上の英数字文字列を含めることもできます。文字列はルールの [Message] フィールド、シグニチャ ID、およびジェネレータ ID を検索します。たとえば、文字列 `123` は、ルール メッセージ内の文字列 `"Lotus123"` や `"123mania"` などを返し、`SID 6123` や `SID 12375` なども返します。ルールの [Message] フィールドの詳細については、イベント メッセージの定義(36-12 ページ)を参照してください。ルールの SID と GID の詳細については、プリプロセッサ ジェネレータ ID の読み取り(41-42 ページ)を参照してください。1 つ以上の文字列でフィルタ処理することによって、SID を部分的に検索できます。

すべての文字列では大文字と小文字が区別されず、部分的な文字列として扱われます。たとえば、文字列 `ADMIN`、`admin`、または `Admin` はいずれも `"admin"`、`"CFADMIN"`、`"Administrator"` などを返します。

完全一致を返す場合は、文字列を引用符で囲む必要があります。たとえば、引用符付きのリテラル文字列 `"overflow attempt"` は完全一致のみを返しますが、引用符なしの 2 つの文字列 `overflow` と `attempt` で構成されたフィルタは `"overflow attempt"`、`"overflow multipacket attempt"`、`"overflow with evasion attempt"` などを返します。

キーワード、文字列、またはその両方の組み合わせをスペースで区切って入力することによって、フィルタ結果を絞り込むことができます。結果には、すべてのフィルタ条件と一致するすべてのルールが含まれます。

複数のフィルタ条件を任意の順序で入力できます。たとえば、次のすべてのフィルタが同じルールを返します。

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

侵入ポリシー内のルール フィルタの設定

ライセンス：Protection

[Rules] ページで、ルールのサブセットを表示するようにルールをフィルタ処理できます。その後で、いずれかのページ機能を使用できます。これには、コンテキスト メニューで使用可能な機能の選択も含まれます。これは、特定のカテゴリのすべてのルールのしきい値を設定する場合などに便利です。フィルタ処理されたリスト内のルールとフィルタ処理されていないリスト内のルールで同じ機能を使用できます。たとえば、新しいルール状態を、フィルタ処理されたリスト内のルールまたはフィルタ処理されていないリスト内のルールに適用できます。

侵入ポリシー内の [Rules] ページの左側にあるフィルタ パネルから事前定義のフィルタ キーワードを選択できます。フィルタを選択すると、ページに、すべての一致するルールが表示されるか、どのルールも一致しなかったことが表示されます。

使用可能なすべてのキーワードと引数の詳細と、フィルタ パネルでのフィルタの作成方法については、侵入ポリシー内のルール フィルタ処理について（32-11 ページ）を参照してください。

フィルタにキーワードを追加してさらに絞り込むことができます。入力されたすべてのフィルタが、ルール データベース全体を検索して、一致するすべてのルールを返します。ページに前回のフィルタ結果が表示されている状態でフィルタを入力すると、ページが消去され、代わりに新しいフィルタの結果が返されます。

また、フィルタを選択したとき、または、フィルタを選択後にその中の引数値を変更したときに指定したものと同じキーワードと引数の構文を使用してフィルタを入力することもできます。キーワードなし、キーワードの先頭文字の大文字表記なし、または引数の周りの引用符なしの検索語を入力すると、検索が文字列検索として扱われ、[Category]、[Message]、および [SID] の各フィールドで指定された単語が検索されます。

侵入ポリシー内の特定のルールに対してフィルタ処理する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4　左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。フィルタ内に存在するキーワードの引数をクリックすると、既存の引数が置き換えられることに注意してください。詳細については、次の各項を参照してください。

- 侵入ポリシー ルール フィルタを作成するためのガイドライン（32-11 ページ）
- ルール構成フィルタについて（32-14 ページ）
- ルール コンテンツ フィルタについて（32-17 ページ）
- ルール カテゴリについて（32-19 ページ）
- ルール フィルタの直接編集（32-19 ページ）

ページが、すべての一致するルールを表示するように更新され、フィルタと一致するルールの数がフィルタ テキスト ボックスの上に表示されます。

ステップ 5　新しい設定を適用する 1 つ以上のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6　オプションで、通常ページで行うような変更をルールに対して行えます。詳細については、次の項を参照してください。

- [Rules] ページ上でルールを有効または無効にする方法については、ルール状態の設定（32-22 ページ）を参照してください。
- ルールにしきい値設定と抑制を追加する方法については、ポリシー単位の侵入イベント通知のフィルタ処理（32-25 ページ）を参照してください。
- 一致するトラフィックでレート異常が発生したときにトリガされる動的ルール状態を設定する方法については、動的ルール状態の追加（32-33 ページ）を参照してください。
- SNMP アラートを特定のルールに追加する方法については、SNMP アラートの追加（32-36 ページ）を参照してください。
- ルールにルール コメントを追加する方法については、ルール コメントの追加（32-38 ページ）を参照してください。

ステップ 7　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。

詳細については、侵入ポリシーの管理（31-3 ページ）および侵入ポリシーの編集（31-4 ページ）を参照してください。

ルール状態の設定

ライセンス： Protection

Cisco脆弱性調査チーム（VRT）が、各デフォルト ポリシー内の侵入ルールとプリプロセッサ ルールのデフォルト状態を設定します。たとえば、ルールを Security over Connectivity デフォルト ポリシーでは有効にして、Connectivity over Security デフォルト ポリシーでは無効にすることができます。作成された侵入ポリシー ルールは、作成時に使用されたデフォルト ポリシー内のルールのデフォルト状態を継承します。

ルールを [Generate Events]、[Drop and Generate Events]、または [Disable] に個別に設定することも、状態を変更するルールを選択するためのさまざまな要素でルールをフィルタ処理することもできます。インライン展開では、インライン侵入展開で [Drop and Generate Events] ルール状態を使用して悪意のあるパケットをドロップできます。[Drop and Generate Events] ルール状態のルールはイベントを生成しますが、3D9900 または シリーズ 3 デバイスのインライン インターフェイス セットがタップ モードの場合を含むパッシブ展開ではパケットをドロップしないことに注意してください。ルールを [Generate Events] または [Drop and Generate Events] に設定すると、ルールが有効になります。ルールを [Disable] に設定すると、ルールが無効になります。

2 つのシナリオについて考えてみます。最初のシナリオでは、特定のルールのルール状態が [Generate Events] に設定されます。悪意のあるパケットがネットワークを通過してルールをトリガーすると、そのパケットが宛先に送信され、システムが侵入イベントを生成します。2 つ目のシナリオでは、同じルールのルール状態が、インライン展開で [Drop and Generate Events] に設定さ

れていると仮定します。この場合は、悪意のあるパケットがネットワークを通過すると、システムがそのパケットをドロップして、侵入イベントを生成します。パケットがターゲットに到達することはありません。

侵入ポリシーでは、ルールの状態を次のいずれかに設定できます。

- システムで特定の侵入試行を検出して、一致したトラフィックが見つかった時点で侵入イベントを生成する場合は、ルール状態を [Generate Events] に設定します。
- システムで特定の侵入試行を検出してから、インライン展開で一致するトラフィックが見つかった時点で攻撃を含むパケットをドロップし、侵入イベントを生成する場合、あるいは、3D9900 または シリーズ 3 デバイスのインライン インターフェイス セットがタップ モードの場合を含むパッシブ展開で一致するトラフィックが見つかった時点で侵入イベントを生成する場合は、ルール状態を [Drop and Generate Events] に設定します。

  システムでパケットをドロップする場合は、インライン展開で侵入ポリシーを廃棄ルールに設定する必要があることに注意してください。詳細については、インライン展開でのドロップ動作の設定（31-6 ページ）を参照してください。
- システムで一致するトラフィックを評価しない場合は、ルール状態を [Disable] に設定します。

廃棄ルールを使用するには、次の手順を実行する必要があります。

- 侵入ポリシーで [Drop when Inline] オプションを有効にします。
- ルールと一致するすべてのパケットをドロップする必要があるすべてのルールのルール状態を [Drop and Generate Events] に設定します。
- 侵入ポリシーに関連付けられたアクセス コントロール ルールを含むアクセス コントロール ポリシーを、インライン セットを使用する管理対象デバイスに適用します。

[Rules] ページのルールのフィルタ処理は、廃棄ルールとして設定するルールを探すときに役立ちます。詳細については、侵入ポリシー内のルールのフィルタ処理（32-10 ページ）を参照してください。

ルール構造、ルール キーワードとそのオプション、およびルール作成構文については、侵入ルールの概要と作成（36-1 ページ）を参照してください。

VRT がルール更新を使用してデフォルト ポリシー内の 1 つ以上のルールのデフォルト状態を変更する場合があります。ルール更新での基本ポリシーの更新を許可すると、ポリシーの作成時に使用されたデフォルト ポリシー（または基礎となるデフォルト ポリシー）のデフォルト状態が変更されたときの、そのポリシー内のルールのデフォルト状態の変更も許可することになります。ただし、ルール状態を変更している場合は、ルール更新でその変更が上書きされないことに注意してください。

1 つ以上のルールのルール状態を変更する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーでまだ保存されていない変更がある場合、それらの変更を破棄して続行するには [OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

このページには、有効なルールの総数、[Generate Events] に設定された有効なルールの総数、および [Drop and Generate Events] に設定された有効なルールの総数が表示されることに注意してください。また、パッシブ展開では、[Drop and Generate Events] に設定されたルールで行われるのはイベントの生成のみであることにも注意してください。

ステップ 3　[Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4　ルール状態を設定するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタ処理について（32-11 ページ）および侵入ポリシー内のルール フィルタの設定（32-21 ページ）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　ルール状態を設定する 1 つ以上のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6　次の選択肢があります。

- トラフィックが選択されたルールと一致したときにイベントを生成するには、[Rule State] > [Generate Events] の順に選択します。
- インライン展開でトラフィックが選択されたルールと一致したときにイベントを生成し、そのトラフィックをドロップするには、[Rule State] > [Drop and Generate Events] の順に選択します。
- 選択されたルールと一致するトラフィックを検査しないようにするには、[Rule State] > [Disable] の順に選択します。

注　Cisco では、侵入ポリシー内のすべての侵入ルールを有効に**しない**ことを**強く**推奨しています。すべてのルールが有効になっている場合は、管理対象デバイスのパフォーマンスが低下する可能性があります。代わりに、できるだけネットワーク環境に合わせてルール セットを調整してください。

ステップ 7　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。詳細については、侵入ポリシーの管理（31-3 ページ）および侵入ポリシーの編集（31-4 ページ）を参照してください。

ポリシー単位の侵入イベント通知のフィルタ処理

ライセンス：Protection

侵入イベントの重要度は、発生頻度、送信元 IP アドレス、または宛先 IP アドレスに基づいて設定できます。イベントが特定の回数発生するまで注意が必要ない場合もあります。たとえば、何者かがサーバにログインしようとしても、特定の回数失敗するまで、気にする必要はありません。一方、ほんの少数の発生を見れば、広範な問題があることを理解できる場合もあります。たとえば、Web サーバに対して DoS 攻撃が行われた場合は、少数の侵入イベントの発生を確認しただけで、その状況に対処しなければならないことが分かります。同じイベントが何百回も確認されれば、システムの機能が麻痺します。

詳細については、次の項を参照してください。

- イベントしきい値の設定（32-25 ページ）では、発生回数に基づくイベントの表示頻度を指定するしきい値の設定方法について説明します。イベント単位およびポリシー単位でしきい値を設定できます。
- 侵入ポリシー単位の抑制の設定（32-30 ページ）では、指定されたイベントの通知を各ポリシー内の送信元 IP アドレス単位または宛先 IP アドレス単位で抑制する方法について説明します。

イベントしきい値の設定

ライセンス：Protection

指定された期間内にイベントが生成された回数に基づいて、システムが侵入イベントを記録して表示する回数を制限するための個別のルールのしきい値を侵入ポリシー単位で設定できます。これにより、大量の同じイベントが原因で機能が麻痺するのを避けることができます。しきい値は、shared object rule 単位、標準テキスト ルール単位、またはプリプロセッサ ルール単位で設定できます。

詳細については、次の項を参照してください。

- イベントしきい値の設定について（32-25 ページ）
- 侵入イベントしきい値の追加と変更（32-27 ページ）
- 侵入イベントしきい値の表示と削除（32-28 ページ）
- ルールのしきい値の設定（32-7 ページ）

イベントしきい値の設定について

ライセンス：Protection

まず、しきい値タイプを指定する必要があります。次の表に示すオプションの中から選択できます。

表 32-6　しきい値設定オプション

オプション	説明
Limit	指定された数のパケット（カウント引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、イベントを記録して表示します。たとえば、タイプを [Limit] に、[Count] を 10 に、[Seconds] を 60 に設定し、14 個のパケットがルールをトリガーとして使用した場合、システムはその 1 分の間に発生した最初の 10 個を表示した後、イベントの記録を停止します。

表 32-6　しきい値設定オプション（続き）

オプション	説明
Threshold	指定された数のパケット（カウント引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、1 つのイベントを記録して表示します。イベントのしきい値カウントに達し、システムがそのイベントを記録した後、時間のカウンタは再び開始されることに注意してください。たとえば、タイプを [Threshold] に、[Count] を 10 に、[Seconds] を 60 に設定して、ルールが 33 秒間で 10 回トリガーされたとします。システムは、1 個のイベントを生成してから、[Seconds] と [Count] のカウンタをリセットします。次の 25 秒間にルールがさらに 10 回トリガーされたとします。33 秒でカウンタが 0 にリセットされたため、システムが別のイベントを記録します。
両方	指定された数（カウント）のパケットがルールをトリガーとして使用した後で、指定された期間ごとに 1 回イベントを記録して表示します。たとえば、タイプを [Both] に、[Count] を 2 に、[Seconds] を 10 に設定した場合、イベント数は以下のようになります。 • ルールが 10 秒間に 1 回トリガーされた場合、システムはイベントを生成しません（しきい値が満たされていない）。 • ルールが 10 秒間に 2 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回トリガーとして使用した場合、しきい値が満たされるため）。 • ルールが 10 秒間に 4 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値に達し、それ以降のイベントは無視される）。

次に、トラッキングを指定する必要があります。これにより、イベントしきい値が送信元 IP アドレス単位と宛先 IP アドレス単位のどちらで計算されるかが決まります。次の表の中から、システムがイベント インスタンスを追跡する方法を指定するためのオプションの 1 つを選択します。

表 32-7　IP しきい値設定オプション

オプション	説明
Source	送信元 IP アドレス単位でイベント インスタンス カウントを計算します。
Destination	宛先 IP アドレス単位でイベント インスタンス カウントを計算します。

最後に、しきい値を定義するインスタンスの数と期間を指定します。

表 32-8　しきい値のインスタンス/時間のオプション

オプション	説明
Count	しきい値を満たすために必要な、追跡する IP アドレス単位で指定された期間単位のイベント インスタンスの数。
Seconds	カウントがリセットされるまでの秒数。しきい値タイプを [limit] に、トラッキングを [Source IP] に、[count] を [10] に、[seconds] を [10] に設定した場合は、システムが指定された送信元ポートから 10 秒間に発生した最初の 10 のイベントを記録して表示します。最初の 10 秒で 7 個のイベントだけが発生した場合、システムはそれらを記録して表示します。最初の 10 秒で 40 個のイベントが発生した場合、システムは 10 個を記録して表示し、10 秒経過してからカウントを再度開始します。

侵入イベントのしきい値設定は、単独で使用することも、レート ベースの攻撃防御、`detection_filter` キーワード、および侵入イベント抑制のいずれかと組み合わせて使用することもできます。詳細については、動的ルール状態の追加（32-33 ページ）、イベントのフィルタリング（36-94 ページ）、および侵入ポリシー単位の抑制の設定（32-30 ページ）を参照してください。

詳細については、次の項を参照してください。

- 侵入イベントしきい値の追加と変更（32-27 ページ）
- ルールのしきい値の設定（32-7 ページ）
- 侵入イベントしきい値の表示と削除（32-28 ページ）

ヒント　侵入イベントのパケット ビューでしきい値を追加することもできます。詳細については、「イベント情報の表示（41-25 ページ）」を参照してください。

侵入イベントしきい値の追加と変更

ライセンス：Protection

1 つ以上の特定のルールのしきい値を設定できます。既存のしきい値設定を個別にまたは同時に変更することもできます。それぞれに 1 つずつのしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。

しきい値設定の表示方法と削除方法については、侵入イベントしきい値の表示と削除（32-28 ページ）を参照してください。

また、すべてのルールとプリプロセッサ生成イベントにデフォルトで適用されるグローバルしきい値を変更することもできます。詳細については、侵入イベントのロギングのグローバルな制限（35-1 ページ）を参照してください。

無効な値を入力するとフィールドに復元アイコン（  ）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ヒント　複数の CPU を搭載した管理対象デバイスでグローバルしきい値または個別のしきい値を設定すると、予想より多くのイベントが生成される場合があります。

イベントしきい値を追加または変更する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4　しきい値を設定するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタ処理について（32-11 ページ）および侵入ポリシー内のルール フィルタの設定（32-21 ページ）を参照してください。

ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　しきい値を設定する 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6　[Event Filtering] > [Threshold] の順に選択します。

[thresholding] ポップアップ ウィンドウが表示されます。

ステップ 7　[Type] ドロップダウンリストから、設定するしきい値のタイプを選択します。

- 指定された期間あたりのイベント インスタンス数に通知を制限する場合は、[Limit] を選択します。
- 指定された期間あたりのイベント インスタンス数ごとに通知を提供する場合は、[Threshold] を選択します。
- 指定されたイベント インスタンス数後に期間あたり 1 回ずつ通知を提供する場合は、[Both] を選択します。

ステップ 8　[Track By] ドロップダウンリストから、イベント インスタンスが**送信元** IP アドレスまたは**宛先** IP アドレスのどちらによって追跡されるかを選択します。

ステップ 9　[Count] フィールドで、しきい値として使用するイベント インスタンスの数を指定します。

ステップ 10　[Seconds] フィールドで、イベント インスタンスを追跡する期間を表す秒数を指定します。

ステップ 11　[OK] をクリックします。

システムが、しきい値を追加し、[Event Filtering] カラムのルールの横にイベント フィルタ アイコン（  ）を表示します。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がイベント フィルタの数を示します。

ステップ 12　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。

詳細については、侵入ポリシーの管理（31-3 ページ）および侵入ポリシーの編集（31-4 ページ）を参照してください。

侵入イベントしきい値の表示と削除

ライセンス：Protection

既存のしきい値設定を表示または削除することができます。[Rules Details] ビューを使用してしきい値の既存の設定を表示することによって、それらがシステムに適切かどうかを確認できます。そうでない場合は、新しいしきい値を追加して既存の値を上書きすることができます。

すべてのルールとプリプロセッサ生成イベントにデフォルトで適用されるグローバルしきい値を変更することもできることに注意してください。詳細については、「侵入イベントのロギングのグローバルな制限（35-1 ページ）」を参照してください。

しきい値を表示または削除する方法:

アクセス: Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(23-17 ページ)を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4　表示または削除する、しきい値が設定されたルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタ処理について(32-11 ページ)および侵入ポリシー内のルール フィルタの設定(32-21 ページ)を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　表示または削除する、しきい値が設定された 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6　選択したルールのしきい値を削除するには、[Event Filtering] > [Remove Thresholds] の順に選択します。表示される確認のポップアップ ウィンドウで [OK] をクリックします。

ヒント　特定のしきい値を削除するために、ルールを強調表示して、[Show Details] をクリックすることもできます。しきい値設定を展開して、削除するしきい値設定の横にある [Delete] をクリックします。[OK] をクリックして、設定の削除を確認します。

ページが更新され、しきい値が削除されます。

ステップ 7　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。詳細については、侵入ポリシーの管理(31-3 ページ)および侵入ポリシーの編集(31-4 ページ)を参照してください。

侵入ポリシー単位の抑制の設定

ライセンス：Protection

特定の IP アドレスまたは IP アドレス の範囲が特定のルールまたはプリプロセッサをトリガーしたときの侵入イベント通知を抑制できます。これは、誤検出を回避するのに役立ちます。たとえば、特定のエクスプロイトのように見えるパケットを伝送しているメール サーバが存在する場合は、そのメール サーバによってトリガーとして使用されたイベントに関するイベント通知を抑制できます。ルールはすべてのパケットに対してトリガーとして使用されますが、本物の攻撃に対するイベントだけが表示されます。

侵入イベント抑制は、単独で使用することも、レート ベースの攻撃防御、`detection_filter` キーワード、および侵入イベントしきい値構成のいずれかと組み合わせて使用することもできることに注意してください。詳細については、動的ルール状態の追加（32-33 ページ）、イベントのフィルタリング（36-94 ページ）、およびイベントしきい値の設定（32-25 ページ）を参照してください。

詳細については、次の項を参照してください。

- 侵入イベントの抑制（32-30 ページ）
- 抑制条件の表示と削除（32-32 ページ）

ヒント　侵入イベントのパケット ビューで抑制を追加することもできます。詳細については、「イベント情報の表示（41-25 ページ）」を参照してください。また、[Rule Editor] ページや任意の侵入イベント ページ（イベントが侵入ルールによってトリガーされた場合）で右クリック コンテキスト メニューを使用して、抑制設定にアクセスすることもできます。

侵入イベントの抑制

ライセンス：Protection

ルールに関する侵入イベント通知を抑制できます。ルールに関する通知が抑制されると、ルールはトリガーとして使用されますが、イベントは生成されません。ルールの 1 つまたは複数の抑制を設定できます。リスト内の最初の抑制に最も高いプライオリティが割り当てられます。2 つの抑制が競合している場合は、最初の抑制のアクションが実行されることに注意してください。

無効な値を入力するとフィールドに復元アイコン（）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

イベント表示を抑制する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4　抑制を設定するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタ処理について（32-11 ページ）および侵入ポリシー内のルール フィルタの設定（32-21 ページ）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　抑制条件を設定する 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6　[Event Filtering] > [Suppression] の順に選択します。

[suppression] ポップアップ ウィンドウが表示されます。

ステップ 7　次の [Suppression Type] オプションのいずれかを選択します。

- 選択したルールのイベントを完全に抑制する場合は、[Rule] を選択します。
- 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[Source] を選択します。
- 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[Destination] を選択します。

ステップ 8　抑制タイプとして [Source] または [Destination] を選択した場合は、[Network] フィールドに、IP アドレス、アドレス ブロック、または送信元 IP アドレスまたは宛先 IP アドレスとして指定する変数、あるいは、これらの任意の組み合わせで構成されたカンマ区切りのリストを入力します。

FireSIGHT システムで IPv4 CIDR と IPv6 プレフィクス長アドレス ブロックを使用する方法については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ステップ 9　[OK] をクリックします。

システムが、抑制条件を追加し、抑制するルールの横にある [Event Filtering] カラムのルールの横にイベント フィルタ アイコン（  ）を表示します。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がイベント フィルタの数を示します。

ステップ 10　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。

詳細については、侵入ポリシーの管理（31-3 ページ）および侵入ポリシーの編集（31-4 ページ）を参照してください。

抑制条件の表示と削除

ライセンス：Protection

既存の抑制条件を表示または削除することもできます。たとえば、メール サーバが悪用のように見えるパケットを普段から送信しているという理由で、そのメール サーバの IP アドレスから送信されたパケットに関するイベント通知を抑制できます。その後、そのメール サーバが使用停止になり、その IP アドレスが別のホストに再割り当てされたら、その送信元 IP アドレスの抑制条件を削除する必要があります。

定義された抑制条件を表示または削除する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、ページにはルールがメッセージのアルファベット順に一覧表示されます。

ステップ 4　抑制を表示または削除するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタ処理について（32-11 ページ）および侵入ポリシー内のルール フィルタの設定（32-21 ページ）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　抑制を表示または削除する 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6　次の 2 つのオプションから選択できます。

- ルールのすべての抑制を削除するには、[Event Filtering] > [Remove Suppressions] を選択します。表示される確認のポップアップ ウィンドウで [OK] をクリックします。
- 特定の抑制設定を削除するには、ルールを強調表示して、[Show Details] をクリックします。抑制設定を展開して、削除する抑制設定の横にある [Delete] をクリックします。[OK] をクリックして、選択した設定の削除を確認します。

ページが更新され、抑制設定が削除されます。

ステップ 7　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。詳細については、侵入ポリシーの管理（31-3 ページ）および侵入ポリシーの編集（31-4 ページ）を参照してください。

動的ルール状態の追加

ライセンス： Protection

レート ベースの攻撃は、ネットワークまたはホストに過剰なトラフィックを送信することによって、低速化または正規の要求の拒否を引き起こし、ネットワークまたはホストを混乱させようとします。レート ベースの防御を使用して、特定のルールの過剰なルール一致に対応してルール アクションを変更することができます。

詳細については、次の項を参照してください。

- 動的ルール状態について（32-33 ページ）
- 動的ルール状態の設定（32-34 ページ）

動的ルール状態について

ライセンス： Protection

一定期間に多すぎる数のルールの一致が発生した時点を検出するレート ベースのフィルタを含めるように侵入ポリシーを設定できます。インライン展開された管理対象デバイスでこの機能を使用すると、指定した時間だけレートベース攻撃をブロックし、その後、ルールが一致した場合にイベントの生成のみを行い、トラフィックをドロップしないルール状態に戻すことができます。

レート ベースの攻撃防御は、異常なトラフィック パターンを識別し、正規の要求に対するそのトラフィックの影響を最小限に抑えようとします。特定の宛先 IP アドレスに送信されるトラフィックまたは特定の送信元 IP アドレスから送信されるトラフィックの過剰なルール一致を識別できます。また、検出されたすべてのトラフィックを通して特定のルールの過剰な一致に対処することもできます。

侵入ポリシーでは、侵入ルールまたはプリプロセッサ ルールのレート ベースのフィルタを設定できます。レート ベースのフィルタは次の 3 つの要素で構成されます。

- 特定の秒数以内のルール一致のカウントとして設定されるルール一致率
- レートを超えた時点で実行される新しいアクション（Generate Events、Drop and Generate Events、および Disable の 3 種類がある）
- タイムアウト値として設定されるアクションの継続期間

新しいアクションは、開始されると、レートがその期間内に設定されたレートを下回っても、タイムアウトに達するまで継続されることに注意してください。タイムアウトに達すると、レートがしきい値を下回っていれば、ルールのアクションがルールの初期設定に戻ります。

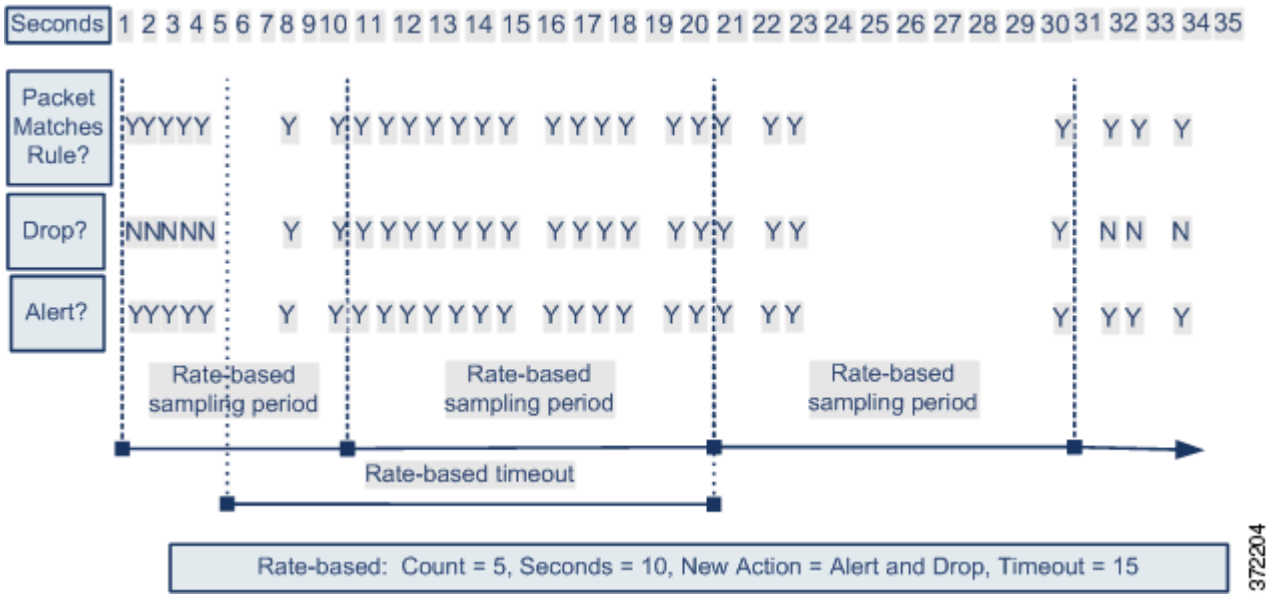
インライン展開のレート ベースの攻撃防御は、攻撃を一時的または永続的にブロックするように設定できます。レート ベースの設定を使用しない場合、[Generate Events] に設定されたルールはイベントを生成しますが、システムはそのようなルールに関するパケットをドロップしません。ただし、攻撃トラフィックが、レート ベースの基準が設定されたルールと一致した場合は、そのようなルールが最初から [Drop and Generate Events] に設定されていなかったとしても、レート アクションがアクティブな期間にパケットのドロップが実行されます。

注　レート ベースのアクションは、無効なルールを有効にしたり、無効なルールと一致したトラフィックをドロップしたりできません。

同じルールに対して複数のレート ベースのフィルタを定義できます。侵入ポリシーに列挙された最初のフィルタに最も高い優先度が割り当てられます。2 つのレート ベースのフィルタ アクションが競合している場合は、最初のレート ベースのフィルタのアクションが実行されることに注意してください。

次の図は、攻撃者がホストにアクセスしようとしている例を示しています。パスワードを検出しようとする試行が繰り返されると、レート ベース攻撃防止が設定されたルールがトリガーされます。レート ベースの設定は、ルール一致が 10 秒間に 5 回発生した時点で、ルール属性を [Drop and Generate Events] に変更します。新しいルール属性は 15 秒後にタイムアウトします。

タイムアウト後も、そのパケットは後続のレート ベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または過去のサンプリング期間のしきい値を上回っている場合は、新しいアクションが継続されます。新しいアクションは、サンプリング レートがしきい値レートを下回るサンプリング期間の終了後にのみ、[Generate Events] に戻ります。



動的ルール状態の設定

ライセンス：Protection

ルールと一致したすべてのパケットをドロップするのではなく、指定された期間に特定の一致率に達した場合にルールと一致したパケットをドロップするために、ルールを [Drop and Generate Events] 状態に設定しない場合があります。動的ルール状態を使用すれば、ルールのアクションの変更をトリガーするレート、あるレートに達したときに変更すべきアクション、および新しいアクションの継続時間を設定できます。

アクションの変更をトリガーするために特定のヒット数が発生する必要のあるカウントと秒数を指定することによって、そのルールのヒット数を設定します。加えて、タイムアウトが発生したらアクションをルールの以前の状態に戻すタイムアウトを設定できます。

同じルールに対して複数の動的状態フィルタを定義できます。侵入ポリシー内のルール詳細に列挙された最初のフィルタに最も高い優先度が割り当てられます。2 つのレート ベースのフィルタ アクションが競合している場合は、最初のレート ベースのフィルタのアクションが実行されることに注意してください。

無効な値を入力するとフィールドに復元アイコン( )が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

注　動的ルール状態は、無効なルールを有効にしたり、無効なルールと一致したトラフィックをドロップしたりできません。

動的ルール状態を追加する方法:

アクセス: Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Rules] をクリックします。

[Rules] ページが表示されます。

ステップ 4　動的ルール状態を追加するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタ処理について（32-11 ページ）および侵入ポリシー内のルール フィルタの設定（32-21 ページ）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　動的ルール状態を追加する 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6　[Dynamic State] > [Add Rate-Based Rule State] の順に選択します。

[Add Rate-Based Rule State] ダイアログボックスが表示されます。

ステップ 7　[Track By] ドロップダウンリストから、ルール一致の追跡方法を選択します。

- 特定の送信元または送信元のセットからのそのルールのヒット数を追跡する場合は、[Source] を選択します。
- 特定の宛先または宛先のセットへのそのルールのヒット数を追跡する場合は、[Destination] を選択します。
- そのルールのすべての一致を追跡する場合は、[Rule] を選択します。

ステップ 8　[Track By] を [Source] または [Destination] に設定した場合は、[Network] フィールドに追跡する各ホストのアドレスを入力します。

単一の IP アドレス、アドレス ブロック、変数、またはこれらの任意の組み合わせで構成されたカンマ区切りのリストを指定できます。FireSIGHT システムで IPv4 CIDR と IPv6 プレフィクス長アドレス ブロックを使用する方法については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ステップ 9　[Rate] の隣で、攻撃レートを設定する期間あたりのルール一致の数を指定します。

- [Count] フィールドで、1 ～ 2147483647 の整数を使用して、しきい値として使用するルール一致の数を指定します。
- [Seconds] フィールドで、1 ～ 2147483647 の整数を使用して、攻撃を追跡する期間を表す秒数を指定します。

ステップ 10　[New State] ドロップダウンリストから、条件が満たされたときに実行すべき新しいアクションを指定します。

- イベントを生成する場合は、[Generate Events] を選択します。
- インライン展開でイベントを生成し、イベントをトリガーしたパケットをドロップする場合、または、パッシブ展開でイベントを生成する場合は、[Drop and Generate Events] を選択します。
- アクションを実行しない場合は、[Disabled] を選択します。

ステップ 11　[Timeout] フィールドに、新しいアクションを有効にしておく秒数を入力します。タイムアウトが発生すると、ルールが元の状態に戻ります。新しいアクションのタイムアウトを阻止する場合は、[0] を指定するか、[Timeout] フィールドを空白のままにします。

ステップ 12　[OK] をクリックします。

システムが、動的ルール状態を追加し、[Dynamic State] カラムのルールの横に動的状態アイコン（  ）を表示します。ルールに複数の動的ルール状態フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

必須フィールドを空白にした場合は、フィールドに値を入力する必要があることを伝えるエラー メッセージが表示されます。

ヒント　一連のルールのすべての動的ルール設定を削除するには、[Rules] ページでルールを選択してから、[Dynamic State] > [Remove Rate-Based States] の順に選択します。また、ルールのルール詳細から個別のレート ベースのルール状態フィルタを削除するには、ルールを選択して、[Show Details] をクリックしてから、削除するレート ベースのフィルタのそばにある [Delete] をクリックします。

ステップ 13　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。

詳細については、侵入ポリシーの管理（31-3 ページ）および侵入ポリシーの編集（31-4 ページ）を参照してください。

SNMP アラートの追加

ライセンス： Protection

FireSIGHT システム に対して SNMP アラートを設定する場合は、ルールによってイベントが生成されたときに SNMP アラートを発生する特定のルールを設定できます。詳細については、SNMP 応答の使用（44-1 ページ）を参照してください。

SNMP アラートを設定する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Rules] をクリックします。

[Rules] ページが表示されます。

ステップ 4　SNMP アラートを設定するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタ処理について（32-11 ページ）および侵入ポリシー内のルール フィルタの設定（32-21 ページ）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　SNMP アラートを設定する 1 つまたは複数のルールを選択します。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6　[Alerting] > [Add SNMP Alert] の順に選択します。

システムが、アラートを追加し、[Alerting] カラムのルールの横にアラート アイコン（ ）を表示します。ルールに複数のアラート タイプを追加した場合は、アイコン上の数字がアラート タイプの数を示します。

ヒント　ルールから SNMP アラートを削除するには、そのルールの横にあるチェック ボックスをクリックして、[Alerting] > [Remove SNMP Alerts] の順に選択してから、[OK] をクリックして削除を確認します。

ステップ 7　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。詳細については、侵入ポリシーの管理（31-3 ページ）および侵入ポリシーの編集（31-4 ページ）を参照してください。

ルール コメントの追加

ライセンス：Protection

ルールにコメントを追加することができます。追加したコメントは、[Rules] ページ上の [Rule Details] ビューで確認できます。

コメントを含む侵入ポリシーの変更をコミットしてから、ルールの [Edit] ページで [Rule Comment] をクリックしてコメントを表示することもできます。ルールの編集方法については、既存のルールの変更（36-111 ページ）を参照してください。

コメントをルールに追加する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Rules] をクリックします。

[Rules] ページが表示されます。

ステップ 4　コメントを追加するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタ処理について（32-11 ページ）および侵入ポリシー内のルール フィルタの設定（32-21 ページ）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　コメントを追加する 1 つまたは複数のルールを選択します。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6　[Comments] > [Add Rule Comment] の順に選択します。

[Add Comment] ダイアログボックスが表示されます。

ステップ 7　[Comment] フィールドに、ルール コメントを入力します。

ステップ 8　[OK] をクリックします。

システムが、コメントを追加し、[Comments] カラムのルールの横にコメント アイコン（  ）を表示します。ルールに複数のコメントを追加した場合は、アイコン上の数字がコメントの数を示します。

ヒント　ルール コメントを削除するには、そのルールを強調表示して、[Show Details] をクリックしてから、[Comments] セクションで [Delete] をクリックします。侵入ポリシーの変更がコミットされていないコメントがキャッシュされている場合にだけ、コメントを削除できることに注意してください。侵入ポリシーの変更がコミットされた後は、ルール コメントを削除できなくなります。

ステップ 9　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。

詳細については、侵入ポリシーの管理（31-3 ページ）および侵入ポリシーの編集（31-4 ページ）を参照してください。

ネットワーク資産に応じた侵入防御の調整

FireSIGHT 推奨ルール機能を使用して、ネットワーク上で検出されたオペレーティング システム、サーバ、およびクライアント アプリケーション プロトコル（ネットワーク検出の概要（45-1 ページ）を参照）を、侵入ポリシーごとに、資産を保護するために特別に作成されたルールに関連付けることができます。これにより、モニタ対象のネットワークの特定ニーズに合わせて侵入ポリシーを調整できます。FireSIGHT 推奨ルール機能には、FireSIGHT および Protection のライセンスが必要です。

FireSIGHT推奨ルール機能を設定すると、システムがネットワーク資産に関連付けられた脆弱性から保護するルールの基本ポリシーを検索して、その基本ポリシー内のルールの現在の状態を特定します。その後で、システムは、ルール状態を推奨し、オプションで、次の表内の基準を使用してルールを推奨状態に設定します。

表 33-1　　脆弱性に基づく FireSIGHT ルール状態推奨

基本ポリシー ルール状態	ルールは検出された資産を保護するか	推奨ルール状態
Generate Events または Disable	yes	Generate Events
Drop and Generate Events	yes	Drop and Generate Events
any	no	Disable

Cisco脆弱性調査チーム（VRT）が、Ciscoから提供されるデフォルト ポリシー内の各ルールに適切な状態を決定します。つまり、基本ポリシーがCiscoから提供されるデフォルト ポリシーの場合は、システムでルールを FireSIGHT推奨ルール状態に設定できるようにすることによって、侵入ポリシー内のルールがネットワーク資産に対するCiscoの推奨設定と一致します。詳細については、「システム付属のポリシーについて（23-9 ページ）」を参照してください。

ルール状態推奨の生成は、推奨ルール状態を推奨の生成時に使用するのか、後で使用するのかを選択するのと同じぐらい簡単です。高度な推奨オプションを使用すると、設定をさらに調整することができます。推奨ルール状態を使用することを選択すると、読み取り専用の FireSIGHT 推奨レイヤが侵入ポリシーに追加されますが、後で、推奨ルール状態を使用しないことを選択すると、そのレイヤが削除されるので注意してください。ポリシー層を使用して複数の侵入ポリシーをより効率的に管理する方法については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）を参照してください。

システムは、通常、標準テキスト ルールとshared object ruleのルール状態の変更を推奨しますが、プリプロセッサ ルールとデコーダ ルールの変更も推奨できることに注意してください。

侵入ポリシーに最近保存された構成設定に基づいて自動的に推奨を生成するためのタスクをスケジュールできます。推奨ルール状態を生成するためのタスクをスケジュールする方法については、FireSIGHT 推奨の自動化（62-11 ページ）を参照してください。

詳細については、次の項を参照してください。

- 基本ルール状態推奨について
- 高度なルール状態推奨について
- FireSIGHT 推奨の使用

基本ルール状態推奨について

ライセンス： Protection + FireSIGHT

ポリシー内の推奨ルール状態を使用せずに推奨を生成できます。その後で、[Rules] ページの 3 つの絞り込まれたビューのいずれかを使用して、[Generate Events]、[Drop and Generate Events]、または [Disable] に設定するように推奨されているルールを表示できます。これにより、推奨ルール状態を使用した場合に変更されるルールを事前に確認できます。また、推奨を生成してすぐに使用するように選択することもできます。

推奨が絞り込まれた [Rules] ページを表示している最中に、あるいは、ナビゲーション パネルまたは [Policy Information] ページから [Rules] ページに直接アクセスした後に、手動で、ルール状態を設定したり、ルールをソートしたり、[Rules] ページで可能なその他の操作（ルールの抑制やルールしきい値の設定など）を実行することができます。選択したルールの状態を手動で変更する方法については、ルール状態の設定（32-22 ページ）を参照してください。侵入ポリシー内のルールを調整するための [Rules] ページで使用可能なその他の操作の詳細については、ルールを使用した侵入ポリシーの調整（32-1 ページ）を参照してください。

システムは、手動で設定されたルール状態を変更しません。推奨を生成しながら、推奨ルール状態を使用することにした場合：

- 推奨を生成する前に指定したルールの状態を手動で設定すると、その後、システムはそのルールの状態を変更できなくなる
- 推奨の生成後に指定したルールの状態を手動で設定すると、そのルールの推奨状態が上書きされる

ヒント　ルール状態が推奨状態と異なるルールのリストを侵入ポリシー レポートに含めることができます。詳細については、「現在の侵入設定のレポートの生成（31-10 ページ）」を参照してください。

FireSIGHT推奨ルールの詳細設定を変更せずに推奨を生成する場合は、システムが検出対象のネットワーク全体のすべてのホストのルール状態の変更を推奨することにも注意してください。また、デフォルトで、システムは、オーバーヘッドが低または中のルールに対してのみ推奨を生成し、ルールを無効にする推奨を生成することにも注意してください。詳細については、「高度なルール状態推奨について（33-2 ページ）」を参照してください。

高度なルール状態推奨について

ライセンス： ProtectionまたはProtection + FireSIGHT

詳細設定を使用すれば、システムが脆弱性を監視するネットワーク上のホストを再定義したり、システムがルールのオーバーヘッドに基づいてどのルールを推奨するかに影響を与えたり、ルールを無効にする推奨を生成するかどうかを指定したりできます。

ホスト情報に基づいて特定のパケットのアクティブ ルール処理を動的に適応させる場合は、適応型プロファイルを有効にすることもできます。詳細については、適応型プロファイルとFireSIGHT推奨ルール（30-3 ページ）を参照してください。

詳細については、次の項を参照してください。

- 検査するネットワークについて（33-3 ページ）
- ルール オーバーヘッドについて（33-3 ページ）

検査するネットワークについて

ライセンス：Protection + FireSIGHT

FireSIGHT推奨ルール機能は、ネットワーク マップ内で検査するネットワークを指定することによって、設定します。その後で、システムが、ネットワークを保護するためにアクティブにすることができるルールを推奨します。ネットワーク マップの詳細については、ネットワーク マップの使用（48-1 ページ）を参照してください。

推奨に対して検査するホストを使用して [Networks] フィールドを設定します。単一 IP アドレスまたはアドレス ブロック、あるいはこのいずれかまたは両方をカンマで区切ったリストを指定できます。

指定したホスト内のアドレスのリストは、否定以外の OR 演算でリンクされ、すべての OR 演算の実行後に AND 演算でリンクされます。

ルール オーバーヘッドについて

ライセンス：Protection

Ciscoでは、システム パフォーマンスに対するルールの潜在的影響およびルールによる誤検知の可能性に基づいて、各侵入ルールのオーバーヘッドを「なし」、「低い」、「中程度」、「高い」、または「非常に高い」と格付けしています。[Rules] ページのルール詳細ビューでルールのオーバーヘッド格付けを確認できます。詳細については、「ルール詳細の表示（32-5 ページ）」を参照してください。

指定したオーバーヘッド格付け以下のすべてのルールに基づいて、ルール状態の推奨を作成するようにシステムを設定できます。たとえば、オーバーヘッドが中程度のルールの推奨を生成する場合は、オーバーヘッド格付けが「なし」、「低い」、または「中程度」のすべてのルールに基づいて推奨が作成され、オーバーヘッドが「高い」ルールの推奨は作成されません。

システムは、イベントを生成する推奨またはイベントをドロップして生成する推奨にルール オーバーヘッドを組み込むことに注意してください。ルールを無効にする推奨にはルール オーバーヘッドを組み込みません。サードパーティの脆弱性にマップされていないローカル ルールにはオーバーヘッドがないことにも注意してください。詳細については、ローカル ルール ファイルのインポート（66-22 ページ）およびサードパーティ製品マッピングの管理（46-33 ページ）を参照してください。

特定の設定のオーバーヘッド格付けのルールの推奨を生成した場合でも、別のオーバーヘッドの推奨を生成してから、元のオーバーヘッド設定の推奨を生成し直すことができます。推奨を生成した回数や異なるオーバーヘッド設定の数に関係なく、同じルール セットの推奨を生成するたびに、オーバーヘッド設定ごとに同じルール状態推奨が生成されます。たとえば、オーバーヘッドを「中程度」に設定して推奨を生成し、次に「高い」推奨を生成してから、再び「中低度」の推奨を生成できます。ネットワーク上のホストとアプリケーションが変更されていない場合、オーバーヘッドが「中程度」に設定された両方の推奨は、そのルール セットに対して同じになります。

FireSIGHT 推奨の使用

ライセンス： FireSIGHT + Protection

推奨は、推奨ルール状態の使用の有無と、推奨を生成するための詳細設定の変更の有無に関係なく、生成できます。詳細については、基本ルール状態推奨について（33-2 ページ）および高度なルール状態推奨について（33-2 ページ）を参照してください。

推奨を生成したら、推奨ルール状態を使用できます。また、[Rules] ページで、推奨状態を表示して使用可能な機能を使用することもできます。

FireSIGHT ルール状態推奨を使用する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　次の 2 つのオプションから選択できます。

- 推奨を生成していない場合は、[No recommendations have been generated. Click here to set up **FireSIGHT** recommendations] を選択します。
- 推奨を生成した場合は、[Click to change recommendations] を選択します。

[FireSIGHT Recommended Rules Configuration] ページが表示されます。

ステップ 4　次の選択肢があります。

- 対応する侵入ポリシー レポートでルール メッセージ、推奨状態、および実際の状態が推奨状態と異なるすべてのルールの実際の状態を列挙するには、[Include all differences between recommendations and rule states in policy reports] を選択します。詳細については、「現在の侵入設定のレポートの生成（31-10 ページ）」を参照してください。
- デフォルト設定を使用して推奨事項を生成するには、手順 9 に進みます。
- 高度な推奨オプションを変更するには、ステップ 5 に進みます。

ステップ 5　プラス アイコン（ ）をクリックして [Advanced Settings] セクションを展開します。

高度な FireSIGHT推奨オプションが表示されます。

ステップ 6　[Networks to Examine] の [Networks] フィールドで、推奨に対して検査するネットワークを指定します。

FireSIGHT システムで使用する IP アドレス表記については、IP アドレスの表記規則（1-23 ページ）を参照してください。

アドレスのリストは、否定以外の OR 演算でリンクされ、すべての OR 演算の実行後に AND 演算でリンクされることに注意してください。詳細については、「検査するネットワークについて（33-3 ページ）」を参照してください。

ステップ 7　必要に応じて、[FireSIGHT Recommended Rules Configuration] で、[Recommendation Threshold (By Rule Overhead)] スライド バーをドラッグし、生成した推奨事項にルールによって含める必要があるオーバーヘッドの量を指定します。

スライド バーを右にドラッグすると、より高いオーバーヘッドがルールに含まれ、より多くの推奨が生成されますが、システム パフォーマンスに与える影響も大きくなります。詳細については、「ルール オーバーヘッドについて（33-3 ページ）」を参照してください。

ステップ 8　次の選択肢があります。

- ルールをディセーブルにする推奨事項を生成するには、[Accept Recommendations to Disable Rules] チェック ボックスをオンにします。

  ルールをディセーブルにする推奨を受け入れると、ルールの適用範囲が制限されることに注意してください。

- ルールをディセーブルにする推奨を生成しない場合は、[Accept Recommendations to Disable Rules] チェック ボックスをオフにします。

  ルールをディセーブルにする推奨を無視すると、ルールの適用範囲が拡大されることに注意してください。

ステップ 9　複数のオプションがあります。

- まだ推奨を生成しておらず、推奨の生成中に、ルール状態が自動的に推奨状態に変更されるようにする場合は、[Generate and Use Recommendations] をクリックします。

  システムが、推奨ルール状態の変更を生成し、自動的にルールを推奨状態に設定します。

- システムがルール状態を自動的に推奨状態に変更することなく、推奨を生成するようにする場合は、[Generate Recommendations] をクリックします。

  システムが、推奨ルール状態の変更を生成します。

- 以前に推奨を生成済みの場合は、[Update Recommendations] をクリックして既存の推奨を更新します。

  システムが、推奨ルール状態の変更を生成し、推奨が使用中の場合は、自動的にルールを推奨状態に設定します。推奨の数、推奨ルール状態変更を伴うホストの数、およびイベントを生成する推奨、イベントをドロップして生成する推奨、またはルールを無効にする推奨の数に関するステータスが更新されます。

- 過去に推奨を生成したことがある場合は、[Use Recommendations] をクリックして、生成したが使用していなかった推奨を使用します。

  システムが、自動的にルールを推奨状態に設定します。

- 推奨を生成してすでに使用している場合は、[Do Not Use Recommendations] をクリックして、現在使用中の推奨の使用を停止します。

  推奨の使用前に特定のルール状態がルールに適用されていなければ、シスシステムが自動的にルールをデフォルトのルール状態にリセットします。この場合は、ルールが特定のルール状態に戻ります。

システムは、Impact Qualification 機能を使用して無効にされた脆弱性に基づく侵入ルールのルール状態を推奨しないことに注意してください。詳細については、脆弱性の Impact Qualification の設定（49-32 ページ）を参照してください。

使用するポリシーを更新する点にも注意してない使用上の推奨事項は、ネットワークおよびルール セットのサイズによって、数分かかることがあります。

注　システムは、常に、ホストにマップされたサードパーティの脆弱性に関連付けられているローカル ルールを有効化することを推奨します。マップされていないローカル ルールに対する状態推奨は生成されません。詳細については、サードパーティ製品マッピングの管理（46-33 ページ）を参照してください。

ステップ 10　（任意）推奨タイプの横にある [View] をクリックすると、選択した推奨タイプの絞り込まれた推奨が [Rules] ページに表示されます。

ステップ 11　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残した状態での終了を行います。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

特定の脅威の検出

ネットワーク分析ポリシーでさまざまなプリプロセッサを使用して、モニタ対象ネットワークへの特定の攻撃、たとえば、バック オリフィス攻撃、複数のポートスキャン タイプ、過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレート ベース攻撃などを検出できます。ただし、侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。詳細については、カスタム ポリシーの制限（23-13 ページ）を参照してください。

注意 カスタム ユーザ ロールを持つ一部のユーザは、標準メニュー パス（[Policies] > [Access Control] > [Network Analysis Policy]）からネットワーク分析ポリシーにアクセスできません。これらのユーザは、侵入ポリシーを介してネットワーク分析ポリシーにアクセスできます（[Policies] > [Intrusion] > [Intrusion Policy] > [Network Analysis Policy]）カスタム ユーザ ロールの詳細については、カスタム ユーザ ロールの管理（61-55 ページ）を参照してください。

侵入ポリシーで設定するセンシティブ データ検出を使用して、センシティブな数値データの保護なし送信を検出することもできます。

特定の脅威の検出の詳細については、次の項を参照してください。

- バック オリフィスの検出（34-2 ページ）では、バック オリフィス攻撃の検出について説明しています。
- ポートスキャンの検出（34-3 ページ）では、各種のポートスキャンについて概説し、ポートスキャン検出を使用して、攻撃に発展する前にネットワークに対する脅威を識別する方法を説明しています。
- レート ベース攻撃の防止（34-10 ページ）では、サービス拒否（DoS）および SYN フラッド攻撃を制約する方法を説明しています。
- センシティブ データの検出（34-20 ページ）では、ASCII テキストのセンシティブ データ（クレジット カード番号や社会保障番号など）を検出してイベントを生成する方法を説明しています。

バック オリフィスの検出

ライセンス：Protection

FireSIGHT システムは、バック オリフィス プログラムの存在を検出するプリプロセッサを提供しています。バック オリフィス プログラムにより Windows ホストに対する管理者アクセス権を取得される可能性があります。バック オリフィス プリプロセッサは、UDP トラフィックを分析し、パケットの最初の 8 バイトにあり XOR で暗号化されている、バック オリフィス magic Cookie「*!*QWTY?」を調べます。

バック オリフィス プリプロセッサには設定ページがありますが、設定オプションはありません。バック オリフィス プリプロセッサが有効になっていても、以下の表にリストするプリプロセッサ ルールを有効にしなければ、対応するイベントは生成されません。詳細についは次の項を参照してください：詳細については、ルール状態の設定（32-22 ページ）を参照してください。

表 34-1　バック オリフィス GID:SID

プリプロセッサ ルール GID:SID	説明
105:1	バック オリフィス トラフィック検出
105:2	バック オリフィス クライアント トラフィック検出
105:3	バック オリフィス サーバ トラフィック検出
105:4	バック オリフィス Snort バッファ攻撃検出

[Back Orifice Detection] ページを表示する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] > [Access Control Policy] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルで [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Specific Threat Detection] の下の [Back Orifice Detection] が有効になっているかどうかによって、2 つの選択肢があります。

- プリプロセッサが有効になっている場合は、[Edit] をクリックします。
- プリプロセッサが無効になっている場合は、[Enabled] をクリックしてから、[Edit] をクリックします。

[Back Orifice Detection] ページが表示されます。ページ下部に表示されるメッセージに、この設定が含まれている侵入ポリシー レイヤが示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残した状態での終了を行います。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

ポートスキャンの検出

ライセンス：Protection

ポートスキャンとは、攻撃者が攻撃の準備段階としてよく使用する、ネットワーク調査の形式です。ポートスキャンでは、攻撃者が特別に細工したパケットをターゲット ホストに送信します。攻撃者は多くの場合、ホストが応答するパケットを調べることで、ホストでどのポートが開かれているか、そして開かれているポートでどのアプリケーション プロトコルが実行されているかを、直接あるいは推論によって判断できます。

ポートスキャン検出が有効になっていても、侵入ポリシーの [Rules] ページでジェネレータ ID（GID）が 122 に設定されたルールを有効にしなければ、ポートスキャン ディテクタの有効になっているポートスキャン タイプがポートスキャン イベントを生成しないことに注意してください。詳細については、ルール状態の設定（32-22 ページ）および表 34-5（34-8 ページ）を参照してください。

ポートスキャンは、それ自体では攻撃の証拠になりません。実際、攻撃者が使用するポートスキャン手法の中には、正当なユーザがネットワークで使用する可能性があるものもあります。Ciscoのポートスキャン ディテクタは、アクティビティのパターンを検出するという方法で、悪意のあるポートスキャンの可能性があるものを判別できるように設計されています。

攻撃者がネットワークを調査するために複数の手法を使用することはよくあります。通常、攻撃者は異なる複数のプロトコルを使用して、ターゲット ホストからさまざまな応答を引き出します。その目的は、ブロックされた特定タイプのプロトコルを基に、使用できる可能性のあるプロトコルを絞り込んでいくことです。以下の表に、ポートスキャン ディテクタでアクティブにできるプロトコルを記載します。

表 34-2　プロトコル タイプ

Protocol	説明
TCP	TCP プローブを検出します。たとえば、SYN スキャン、ACK スキャン、TCP connect() スキャン、および Xmas tree、FIN、NULL といった異常なフラグを組み合わせたスキャンなどです。
UDP	UDP プローブを検出します。たとえば、ゼロ バイトの UDP パケットなどです。
ICMP	ICMP エコー要求（ping）を検出します。
IP	IP プロトコル スキャンを検出します。これらのスキャンは、攻撃者が開いているポートを見つけようとしているのではなく、ターゲット ホストでサポートされている IP プロトコルを発見しようとするためのスキャンであるため、TCP スキャンおよび UDP スキャンとは異なります。

注　イベントがポートスキャン接続ディテクタによって生成され場合、プロトコル番号は 255 に設定されます。デフォルトでは、ポートスキャンに特定のプロトコルは関連付けられません。したがって、インターネット割り当て番号局（IANA）にはプロトコル番号が割り当てられません。IANA では 255 を予約番号として指定しているため、ポートスキャン イベントでは、そのイベントに関連付けられている番号がないことを示すために、この番号が使用されます。

一般に、ターゲット ホストの数、スキャン側ホストの数、およびスキャン対象のポートの数に応じて、ポートスキャンは 4 つのタイプに分けられます。以下の表に、検出できるポートスキャン アクティビティのタイプを記載します。

表 34-3　ポートスキャンのタイプ

タイプ	説明
ポート スキャン検出	1 対 1 のポートスキャン。攻撃者が 1 つまたは少数のホストを使用して、単一のターゲット ホスト上の複数のポートをスキャンする場合です。 1 対 1 の ポートスキャンには次のような特徴があります。 • 少数のホストを使用してスキャン • 単一のホストをスキャン • 多数のポートをスキャン このオプションでは、TCP、UDP、および IP ポートスキャンが検出されます。
ポートスイープ	1 対多のポートスイープ。攻撃者が 1 つまたは少数のホストを使用して、複数のターゲット ホスト上の単一のポートをスキャンする場合です。 ポートスイープには次のような特徴があります。 • 少数のホストを使用してスキャン • 多数のホストをスキャン • 少数の固有のポートをスキャン このオプションでは、TCP、UDP、ICMP、および IP ポートスイープが検出されます。
デコイ ポートスキャン	1 対 1 のポートスキャン。攻撃者がスプーフィングしたソース IP アドレスを実際のスキャン IP アドレスに混在させる場合です。 デコイ ポートスキャンには次のような特徴があります。 • 多数のホストを使用してスキャン • 少数のポートを一度だけスキャン • 単一（または少数）のホストをスキャン デコイ ポートスキャン オプションでは、TCP、UDP、および IP プロトコル ポートスキャンが検出されます。
分散型ポートスキャン	多対 1 のポートスキャン。複数のホストが単一のホストをクエリして開いているポートを調べる場合です。 分散型ポートスキャンには次のような特徴があります。 • 多数のホストを使用してスキャン • 多数のポートを一度だけスキャン • 単一（または少数）のホストをスキャン 分散型ポートスキャン オプションでは、TCP、UDP、および IP プロトコル ポートスキャンが検出されます。

ポートスキャン ディテクタは、主にプローブ対象ホストからの否定応答に基づいて、プローブに関する情報を取得します。たとえば、Web クライアントが Web サーバに接続するときに、クライアントはサーバのポート 80/tcp が開いていることを頼りに、そのポートを使用します。ただし、攻撃者がサーバを調査するときには、攻撃者にはそのサーバが Web サービスを提供するかどう

かについての事前知識はありません。ポートスキャン ディテクタは否定応答（つまり、ICMP 到達不能または TCP RST パケット）を見つけると、その応答を潜在的ポートスキャンとして記録します。否定応答をフィルタリングするデバイス（ファイアウォールやルータなど）の向こう側にターゲット ホストがある場合、このプロセスはさらに困難になります。この場合、ポートスキャン ディテクタは、選択された機密レベルに基づいて *フィルタリングされた* ポートスキャン イベントを生成することができます。

以下の表に、選択可能な 3 つの機密レベルを記載します。

表 34-4　機密レベル

レベル	説明
Low	ターゲット ホストからの否定応答だけが検出されます。誤検出を抑えるためには、この機密レベルを選択します。ただし、特定のタイプのポートスキャン（時間をかけたスキャン、フィルタリングされたスキャン）が見逃される可能性があることに注意してください。 このレベルを使用すると、ポートスキャン検出の所要時間が最短になります。
Medium	ホストへの接続数に基づいてポートスキャンが検出されます。したがって、フィルタリングされたポートスキャンを検出できます。ただし、ネットワーク アドレス変換プログラムやプロキシなど、ホストが非常にアクティブな場合は、誤検出が発生する可能性があります。 [Ignore Scanned] フィールドに、アクティブなホストの IP アドレスを追加すると、そのような誤検出を軽減できます。 このレベルを使用すると、ポートスキャン検出の所要時間が長くなります。
High	期間に基づいてポートスキャンが検出されます。したがって、時間ベースのポートスキャンを検出できます。ただし、このオプションを使用する場合は、[Ignore Scanned] および [Ignore Scanner] フィールドに IP アドレスを指定するという方法で、時間をかけて慎重にディテクタを調整してください。 このレベルを使用すると、ポートスキャン検出の所要時間が大幅に長くなります。

詳細については、次の項を参照してください。

- ポートスキャン検出の設定（34-5 ページ）
- ポートスキャン イベントについて（34-7 ページ）

ポートスキャン検出の設定

ライセンス： Protection

ポートスキャン検出の設定オプションを使用して、ポートスキャン ディテクタによるスキャン アクティビティのレポート方法を微調整できます。

ポートスキャン検出が有効になっていても、[Rules] ページでジェネレータ ID（GID）が 122 に設定されたルールを有効にしなければ、ポートスキャン ディテクタの有効になっているポートスキャン タイプがポートスキャン イベントを生成しないことに注意してください。詳細については、ルール状態の設定（32-22 ページ）およびポートスキャン検出 SID（GID:122）の表を参照してください。

ポートスキャン検出を設定する方法:

Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] > [Access Control Policy] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、続行します。別のポリシーで保存されていない変更内容を保存する詳細については、[was Committing Intrusion Policy Changes; update xref] を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルで [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Specific Threat Detection] の下の [Portscan Detection] が有効になっているかどうかによって、2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効になっている場合は、[Enabled] をクリックしてから、[Edit] をクリックします。

  [Portscan Detection] ページが表示されます。ページ下部に表示されるメッセージに、この設定が含まれている侵入ポリシー レイヤが示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用(24-1 ページ)」を参照してください。

ステップ 5　[Protocol] フィールドに、以下のプロトコルのうち、有効にするプロトコルを指定します。

- TCP
- UDP
- ICMP
- IP

Ctrl キーまたは Shift キーを押しながらクリックすることによって複数のプロトコルを選択するか、個々のプロトコルをクリアします。詳細については、プロトコル タイプの表を参照してください。

TCP を介してスキャンを検出するには TCP ストリーム処理が有効になっていること、UDP を介してスキャンを検出するには UDP ストリーム処理が有効になっていることが必要です。

ステップ 6　[Scan Type] フィールドに、以下の中から検出対象のポートスキャンを指定します。

- ポート スキャン検出
- ポートスイープ
- デコイ ポートスキャン
- 分散型ポートスキャン

複数のプロトコルを選択または選択解除するには、Ctrl キーまたは Shift キーを押しながらクリックします。詳細については、ポートスキャンのタイプの表を参照してください。

ステップ 7　[Sensitivity Level] リストで、使用するレベル(低、中、または高)を選択します。

詳細については、機密レベルの表を参照してください。

ステップ 8　オプションで、[Watch IP] フィールドに、ポートスキャン アクティビティの兆候を監視するホストを指定します。すべてのネットワーク トラフィックを監視する場合は、このフィールドを空白のままにします。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をコンマで区切ったリストを指定できます。FireSIGHT システムで IPv4 および IPv6 アドレス ブロックを使用する方法の詳細については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ステップ 9　オプションで、[Ignore Scanners] フィールドに、スキャナとしてのホストから除外するホストを指定します。ネットワーク上で特にアクティブになっていないホストを指定するには、このフィールドを使用します。このホスト リストは、時間経過とともに変更しなければならない場合があります。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をコンマで区切ったリストを指定できます。FireSIGHT システムで IPv4 および IPv6 アドレス ブロックを使用する方法の詳細については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ステップ 10　オプションで、[Ignore Scanned] フィールドに、スキャンのターゲットとしてのホストから除外するホストを指定します。ネットワーク上で特にアクティブになっていないホストを指定するには、このフィールドを使用します。このホスト リストは、時間経過とともに変更しなければならない場合があります。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をコンマで区切ったリストを指定できます。FireSIGHT システムで IPv4 および IPv6 アドレス ブロックを使用する方法の詳細については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ステップ 11　オプションで、ミッドストリームで取得されたセッションの監視を中断する場合は、[Detect Ack Scans] チェックボックスをオフにします。

注　ミッドストリーム セッションの検出は ACK スキャンの識別に役立ちますが、過大トラフィックで大量のパケットがドロップされるネットワークでは、誤ったイベントが生成されがちです。

ステップ 12　ポリシーの保存、編集の続行、変更の破棄を行うか、またはシステム キャッシュで変更をそのままにしながら終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

ポートスキャン イベントについて

ライセンス： Protection

ポートスキャン検出が有効になっていても、ジェネレータ ID（GID）122 と Snort® ID（SID）1 ～ 27 のどれかが設定されたルールを有効にしなければ、有効にした各ポートスキャン タイプのイベントは生成されません。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。以下の表の「プリプロセッサ ルール SID」列に、各ポートスキャン タイプに対して有効にする必要があるプリプロセッサ ルールの SID をリストします。

表 34-5　ポートスキャン検出 SID（GID:122）

ポートスキャン タイプ	プロトコル	機密レベル	プリプロセッサ ルール SID
ポート スキャン検出	TCP	Low	1
		Medium または High	5
	UDP	Low	17
		Medium または High	21
	ICMP	Low	イベントを生成しません。
		Medium または High	イベントを生成しません。
	IP	Low	9
		Medium または High	13
ポートスイープ	TCP	Low	3、27
		Medium または High	7
	UDP	Low	19
		Medium または High	23
	ICMP	Low	25
		Medium または High	26
	IP	Low	11
		Medium または High	15
デコイ ポートスキャン	TCP	Low	2
		Medium または High	6
	UDP	Low	18
		Medium または High	22
	ICMP	Low	イベントを生成しません。
		Medium または High	イベントを生成しません。
	IP	Low	10
		Medium または High	14
分散型ポートスキャン	TCP	Low	4
		Medium または High	8
	UDP	Low	20
		Medium または High	24
	ICMP	Low	イベントを生成しません。
		Medium または High	イベントを生成しません。
	IP	Low	12
		Medium または High	16

関連するプリプロセッサ ルールを有効にすると、ポートスキャン ディテクタによって侵入イベントが生成されるようになります。生成されたイベントは、他のすべての侵入イベントと同じように表示できます。ただし、ポートスキャン イベントのパケット ビューに表示される情報は、他のタイプの侵入イベントとは異なります。ここでは、ポートスキャン イベントのパケット ビューに表示されるフィールドと、これらのフィールドの情報を使用してネットワークで行われたプローブのタイプを把握する方法を説明します。

侵入イベント ビューを出発点に、ポートスキャン イベントのパケット ビューまでドリルダウンします。それには、侵入イベントの操作（41-1 ページ）の手順を使用できます。

各ポートスキャン イベントは複数のパケットに基づくため、単一のポートスキャン パケットをダウンロードすることはできません。ただし、ポートスキャン パケット ビューで、使用可能なすべてのパケット情報を確認できます。

注 イベントがポートスキャン接続ディテクタによって生成され場合、プロトコル番号は 255 に設定されます。デフォルトでは、ポートスキャンに特定のプロトコルは関連付けられません。したがって、インターネット割り当て番号局（IANA）にはプロトコル番号が割り当てられません。IANA では 255 を予約番号として指定しているため、ポートスキャン イベントでは、そのイベントに関連付けられている番号がないことを示すために、この番号が使用されます。

以下の表に、ポートスキャン イベントのパケット ビューに表示される情報を記載します。任意の IP アドレスをクリックしてコンテキスト メニューを表示し、[whois] を選択して、その IP アドレスに関するルックアップを実行するか、[View Host Profile] を選択して、そのホストのホスト プロファイルを表示できます。

表 34-6　ポートスキャン パケット ビュー

Information	説明
デバイス	イベントを検出したデバイス。
時刻	イベントが発生した時刻。
メッセージ	プリプロセッサによって生成されたイベント メッセージ。
Source IP	スキャン側ホストの IP アドレス。
Destination IP	スキャンされたホストの IP アドレス。
プライオリティ カウント	スキャンされたホストからの否定応答（TCP RST、ICMP 到達不能など）の数。否定応答の数が多ければ多いほど、プライオリティ カウントが高くなります。
接続カウント	ホスト上でアクティブな接続数。この値は、TCP や IP などの接続ベースのスキャンより正確です。
IP カウント	スキャン対象のホストに接続する IP アドレスが変更された回数。たとえば、最初の IP アドレスが 10.1.1.1、2 番目の IP アドレスが 10.1.1.2、3 番目の IP アドレスが 10.1.1.1 の場合、IP カウントは 3 となります。 プロキシや DNS サーバなどのアクティブ ホストでは、この数値はそれほど正確ではありません。
スキャナ/スキャン対象 IP 範囲	スキャン対象ホストまたはスキャン側ホスト（スキャンのタイプに依存）の IP アドレスの範囲。ポートスイープの場合、このフィールドにはスキャン対象ホストの IP アドレス範囲が示されます。ポートスキャンの場合は、スキャン側ホストの IP アドレス範囲が示されます。
ポート/プロトコル カウント	TCP および UDP ポートスキャンの場合は、スキャン対象のポートが変更された回数です。たとえば、スキャンされた最初のポートが 80、2 番目のポートが 8080、3 番目のポートが再び 80 の場合、ポート カウントは 3 となります。 IP プロトコル ポートスキャンの場合は、スキャン対象ホストに接続するために使用されたプロトコルが変更された回数です。
ポート/プロトコル範囲	TCP および UDP ポートスキャンの場合は、スキャンされたポートの範囲です。 IP プロトコル ポートスキャンの場合は、スキャン対象ホストへの接続試行で使用された IP プロトコル番号の範囲です。
オープン ポート	スキャン対象ホストで開かれた TCP ポート。このフィールドは、ポートスキャンで 1 つ以上の開かれたポートが検出された場合にのみ表示されます。

レート ベース攻撃の防止

ライセンス： Protection

レート ベース攻撃とは、接続の頻度または攻撃を行うための反復試行に依存する攻撃のことです。レート ベースの検出基準を使用することで、レート ベース攻撃が行われていることを検出し、攻撃が発生するごとに対応できます。また、攻撃が収まった後は、通常の検出設定に戻すことができます。レート ベースの検出を設定する方法の詳細については、以下のトピックを参照してください。

- レート ベース攻撃の防止について（34-10 ページ）
- レート ベース攻撃防止とその他のフィルタ（34-13 ページ）
- レート ベース攻撃防止の設定（34-18 ページ）
- 動的ルール状態について（32-33 ページ）
- 動的ルール状態の設定（32-34 ページ）

レート ベース攻撃の防止について

ライセンス： Protection

レート ベース フィルタを含めたネットワーク分析ポリシーを設定することで、ネットワーク上のホストを対象とした過剰なアクティビティを検出できます。インライン モードで展開されている管理対象デバイスでこの機能を使用すると、指定の期間だけレートベース攻撃をブロックし、その後イベントだけを生成してトラフィックをドロップしない状態に戻せます。

レート ベースの攻撃防御は、異常なトラフィック パターンを識別し、正規の要求に対するそのトラフィックの影響を最小限に抑えようとします。一般に、レート ベース攻撃には次のいずれかの特性があります。

- 任意のトラフィックで、ネットワーク上のホストに対して過剰な未完了接続が発生する。これは、SYN フラッド攻撃を意味します。

  SYN 攻撃の検出を設定するには、SYN 攻撃の防止（34-12 ページ）を参照してください。

- 任意のトラフィックで、ネットワーク上のホストに対して過剰な接続が発生する。これは、TCP/IP フラッド攻撃を意味します。

  同時接続の検出を設定するには、同時接続の制御（34-12 ページ）を参照してください。

- 1 つ以上の特定の宛先 IP アドレスへのトラフィック、または 1 つ以上の特定の送信元 IP アドレスからのトラフィックで、ルールとの一致が過剰に発生する。

  送信元または宛先ベースの動的ルール状態を設定するには、動的ルール状態の設定（32-34 ページ）を参照してください。

- すべてのトラフィックで、特定のルールとの一致が過剰に発生する。

  ルール ベースの動的ルール状態を設定するには、動的ルール状態の設定（32-34 ページ）を参照してください。

ネットワーク分析ポリシーでは、ポリシー全体に対して SYN フラッドまたは TCP/IP 接続フラッドの検出を設定できます。侵入ポリシーでは、個々の侵入ルールまたはプリプロセッサ ルールに対してレート ベース フィルタを設定できます。ルール 135:1 および 135:2 に手動でレート ベース フィルタを追加しても、効果はありません。GID:135 のルールでは、クライアントを送信元の値、サーバを宛先の値として使用します。詳細については、SYN 攻撃の防止（34-12 ページ）および同時接続の制御（34-12 ページ）を参照してください。

各レート ベース フィルタには、以下のコンポーネントが含まれます。

- ポリシー全体またはルール ベースの送信元/宛先の設定の場合、ネットワーク アドレスの指定
- ルールの一致レート（特定の秒数内でのルール一致カウントとして設定）
- レートを超過した場合に実行する新しいアクション

  ポリシー全体に対してレート ベースを設定すると、システムはレート ベース攻撃を検出した時点でイベントを生成します。インライン導入では、オプションでトラフィックをドロップすることもできます。個々のルールにレート ベース アクションを設定する場合は、[Generate Events]、[Drop and Generate Events]、[Disable] の 3 つのうちから選択できます。
- アクションの期間（タイムアウト値として設定）

新しいアクションが開始されると、タイムアウト値に達するまで、レートが設定されたしきい値未満になったとしても続行されます。タイムアウト期間が満了し、レートがしきい値を下回っている場合、ルールのアクションはそのルールに最初に設定されたアクションに戻ります。ポリシー全体に適用される設定の場合、アクションは、トラフィックと一致する個々のルールのアクションに戻ります。一致するアクションがなければ、アクションは停止されます。

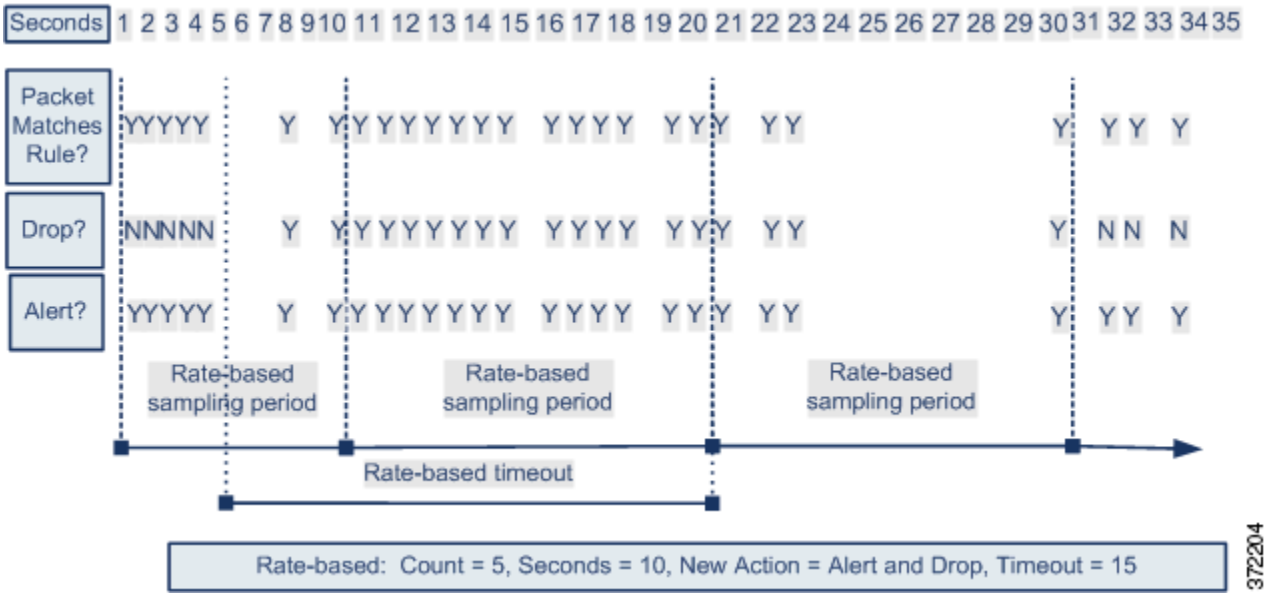
インライン展開のレート ベースの攻撃防御は、攻撃を一時的または永続的にブロックするように設定できます。レート ベースの設定が使用されていない場合、ルールが [Generate Events] に設定されていればイベントが生成されますが、パケットがドロップされることはありません。ただし、攻撃トラフィックが、レート ベースの基準が設定されたルールと一致した場合は、そのようなルールが最初から [Drop and Generate Events] に設定されていなかったとしても、レート アクションがアクティブな期間にパケットのドロップが実行されます。

注　レート ベースのアクションは、無効なルールを有効にしたり、無効なルールと一致したトラフィックをドロップしたりできません。ただし、ポリシー レベルでレート ベース フィルタを設定すると、指定した期間内の過剰な数の SYN パケットまたは SYN/ACK インタラクションを含むトラフィックに対してイベントを生成するか、イベントを生成してトラフィックをドロップすることができます。

同じルールに対して複数のレート ベースのフィルタを定義できます。侵入防御ポリシーで最初にリストされているフィルタに、最大のプライオリティが割り当てられます。2 つのレート ベース フィルタ アクションが競合する場合は、最初のレート ベース フィルタのアクションが実行されることに注意してください。同様に、ポリシー全体に対するレート ベース フィルタと個々のルールに設定されたレート ベース フィルタが競合する場合は、ポリシー全体のレート ベース フィルタが優先されます。

以下の図に、攻撃者がホストへのアクセスを試行する例を示します。パスワードを検出しようとする試行が繰り返されると、レート ベース攻撃防止が設定されたルールがトリガーされます。レート ベースの設定は、ルール一致が 10 秒間に 5 回発生した時点で、ルール属性を [Drop and Generate Events] に変更します。新しいルール属性は、15 秒後にタイムアウトになります。

タイムアウト後も、そのパケットは後続のレート ベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または前回のサンプリング期間中にしきい値を超えている場合は、新しいアクションが続行されます。新しいアクションが元の「イベントの生成」アクションに戻されるのは、サンプリング期間の完了時にサンプルリング レートがしきい値を下回っている場合のみです。



SYN 攻撃の防止

ライセンス：Protection

ネットワークのホストを SYN フラッドから保護するには、SYN 攻撃防止オプションを利用します。一定期間中に認められたパケットの数を基準に、個々のホストまたはネットワーク全体を保護することができます。パッシブ導入のデバイスでは、イベントを生成できます。インライン導入のデバイスでは、不正なパケットをドロップすることもできます。タイムアウト期間の満了時にレート条件に達しなくなっていれば、イベントの生成およびパケットのドロップが停止します。

たとえば、1 つの IP アドレスからの SYN パケットの最大許容数を 10 に設定し、このしきい値に達すると、その IP アドレスからの以降の接続を 60 秒間ブロックするように設定できます。

このオプションを有効にすると、ルール 135:1 もアクティブになります。このルールを手動でアクティブにしても効果はありません。ルール状態は常に [Disabled] として表示され、変更されることはありません。このオプションを有効にすると、定義されたレート条件を超過した時点で、ルールによってイベントが生成されます。

同時接続の制御

ライセンス：Protection

ネットワーク上のホストでの TCP/IP 接続数を制限することで、サービス拒否（DoS）攻撃や、ユーザによる過剰なアクティビティを防止できます。システムが、指定の IP アドレスまたはアドレス範囲で正常に行われている接続が設定された許容数に達したことを検出すると、以降の接続に対してイベントを生成します。タイムアウト期間が満了するまでは、レート条件に達しなくなっても、レート ベースのイベント生成が続行されます。インライン導入では、レート条件がタイムアウトになるまでパケットをドロップするように設定できます。

たとえば、1 つの IP アドレスからの同時接続の最大許容数を 10 に設定し、このしきい値に達すると、その IP アドレスからの以降の接続を 60 秒間ブロックするように設定できます。

このオプションを有効にすると、ルール 135:2 もアクティブになります。このルールを手動でアクティブにしても効果はありません。ルール状態は常に [Disabled] として表示され、変更されることはありません。このオプションを有効にすると、定義されたレート条件を超過した時点で、ルールによってイベントが生成されます。

レート ベース攻撃防止とその他のフィルタ

ライセンス： Protection

トラフィック自体またはシステムが生成するイベントをフィルタリングする手段としては、`detection_filter` キーワード、しきい値および抑制機能も使用できます。レート ベース攻撃防止は、単独で使用することも、しきい値構成、抑制、または `detection_filter` キーワードと任意に組み合わせて使用することもできます。

詳細については、以下の例を参照してください。

- レート ベース攻撃防止と検出フィルタリング（34-13 ページ）
- 動的ルール状態としきい値または抑制（34-14 ページ）
- ポリシー全体のレート ベース検出としきい値構成または抑制（34-16 ページ）
- 複数のフィルタリング方法によるレート ベース検出（34-17 ページ）

レート ベース攻撃防止と検出フィルタリング

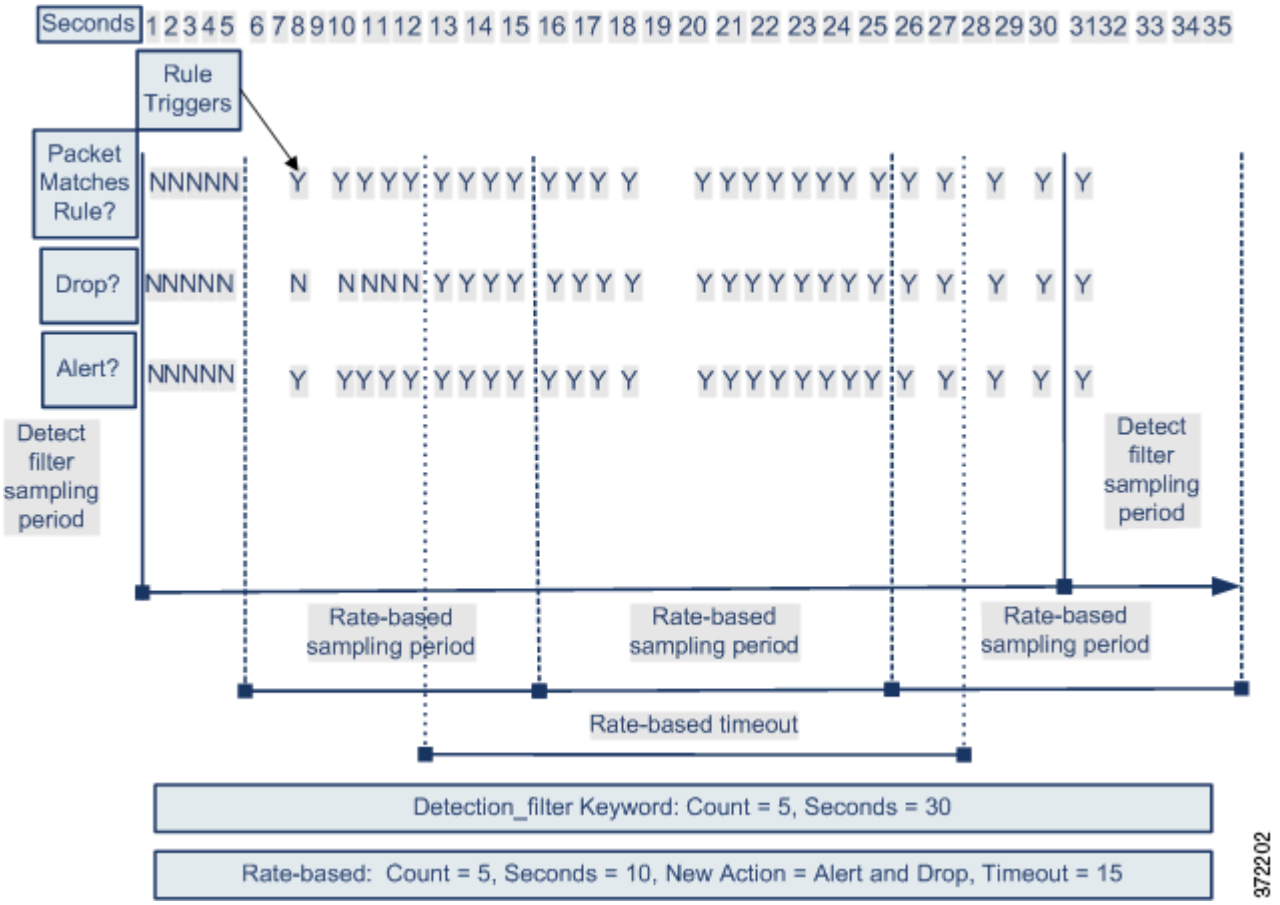
ライセンス： Protection

`detection_filter` キーワードを使用すると、指定の期間内にルール一致のしきい値に達するまで、ルールはトリガーされません。ルールに `detection_filter` キーワードが含まれている場合、システムは指定の期間、ルールのパターンに一致する着信パケットの数を追跡します。システムはそのルールについて、特定の送信元 IP アドレスからのヒット数、または特定の宛先 IP アドレスからのヒット数をカウントできます。レートがルールのレートを超過すると、そのルールに関するイベント通知が開始されます。

以下に、攻撃者がブルートフォース ログインを仕掛ける例を示します。パスワードの検出試行が繰り返されると、カウントが 5 に設定された `detection_filter` キーワードも含むルールがトリガーされます。このルールには、レート ベース攻撃防止が設定されています。10 秒以内にルールに 5 回ヒットすると、レート ベースの設定により、ルール属性が 20 秒間、[Drop and Generate Events] に変更されます。

図に示されているように、最初の 5 個のパケットがルールに一致しても、イベントは生成されません。それは、レートが `detection_filter` キーワードで指定されたレートを超過するまで、ルールはトリガーされないためです。ルールがトリガーされると、イベント通知が開始されますが、さらに 5 個のパケットが通過するまでは、レート ベースの基準によって新しいルールとして [Drop and Generate Events] がトリガーされることはありません。

レート ベースの基準に一致すると、イベントが生成されて、パケットがドロップされます。これは、レート ベースのタイムアウト期間が満了し、かつレートがしきい値未満になるまで続きます。20 秒が経過すると、レート ベース アクションがタイムアウトになります。タイムアウト後も、そのパケットは後続のレート ベースのサンプリング期間にドロップされることに注意してください。タイムアウトが発生した時点で、サンプリングされたレートは前のサンプリング期間のしきい値レートを超過しているため、レート ベースのアクションは続行されます。



この例には示されていませんが、[Drop and Generate Events] ルール状態を `detection_filter` キーワードと組み合わせて使用することで、ルールのヒット数が指定のレートに達するとトラフィックのドロップが開始されるようにすることができることにも注意してください。ルールにレート ベースの設定を使用するかどうかを決定する際は、ルールを [Drop and Generate Events] に設定した場合の結果と `detection_filter` キーワードを含めた場合の結果が同じであるかどうか、あるいは侵入防御ポリシーでレートとタイムアウトの設定を管理する必要があるかどうかを検討してください。詳細については、ルール状態の設定（32-22 ページ）を参照してください。

動的ルール状態としきい値または抑制

ライセンス： Protection

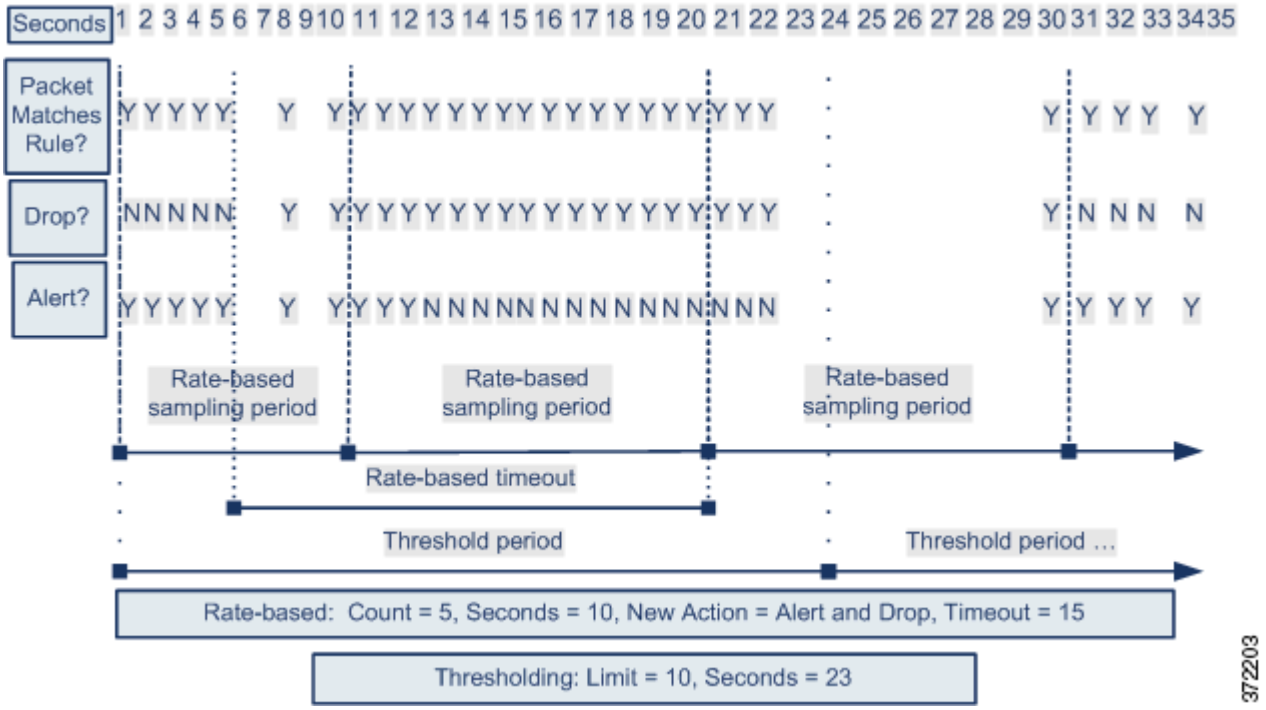
しきい値および抑制を使用して、ルールに関するイベント通知の数を制限するか、またはイベント通知を一切抑制することにより、過剰なイベントが生成されないようにすることができます。しきい値と抑制で使用可能なオプションの詳細については、イベントしきい値の設定（32-25 ページ）および侵入ポリシー単位の抑制の設定（32-30 ページ）を参照してください。

抑制をルールに適用すると、システムは、レート ベースのアクションが変更されたとしても、そのルールに関するイベント通知を、該当するすべての IP アドレスに対して抑制します。一方、しきい値とレート ベースの基準との間の相互作用はさらに複雑になります。

以下に、攻撃者がブルートフォース ログインを仕掛ける例を示します。パスワードを検出しようとする試行が繰り返されると、レート ベース攻撃防止が設定されたルールがトリガーされます。10 秒以内にルールに 5 回ヒットすると、レート ベースの設定により、ルール属性が15 秒間、[Drop and Generate Events] に変更されます。さらに、上限しきい値により、ルールで生成可能なイベントの数が 23 秒間で 10 に制限されます。

図に示されているように、最初の 5 個のパケットが一致すると、ルールはイベントを生成します。5 個のパケットがルールに一致した後、レート ベースの基準が新しいアクションとして [Drop and Generate Events] をトリガーし、次の 5 個のパケットがルールに一致した時点でイベントが生成され、パケットをドロップします。10 個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成することなくドロップします。

タイムアウト後も、そのパケットは後続のレート ベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または前回のサンプリング期間中にしきい値レートを超えた場合は、新しいアクションが続行されます。新しいアクションが元の [Generate Events] アクションに戻されるのは、サンプリング期間の完了時にサンプルリング レートがしきい値を下回っている場合のみです。



この例には示されていませんが、しきい値に達した*後に*、レート ベースの基準によって新しいアクションがトリガーされた場合、システムはアクションが変更されたことを示す単一のイベントを生成することに注意してください。したがって、たとえば上限しきい値の 10 に達してシステムがイベントの生成を停止し、14 番目のパケットでアクションが [Generate Events] から [Drop and Generate Events] に変更されると、システムはアクションが変更されたことを示す 11 番目のイベントを生成します。

ポリシー全体のレート ベース検出としきい値構成または抑制

ライセンス：Protection

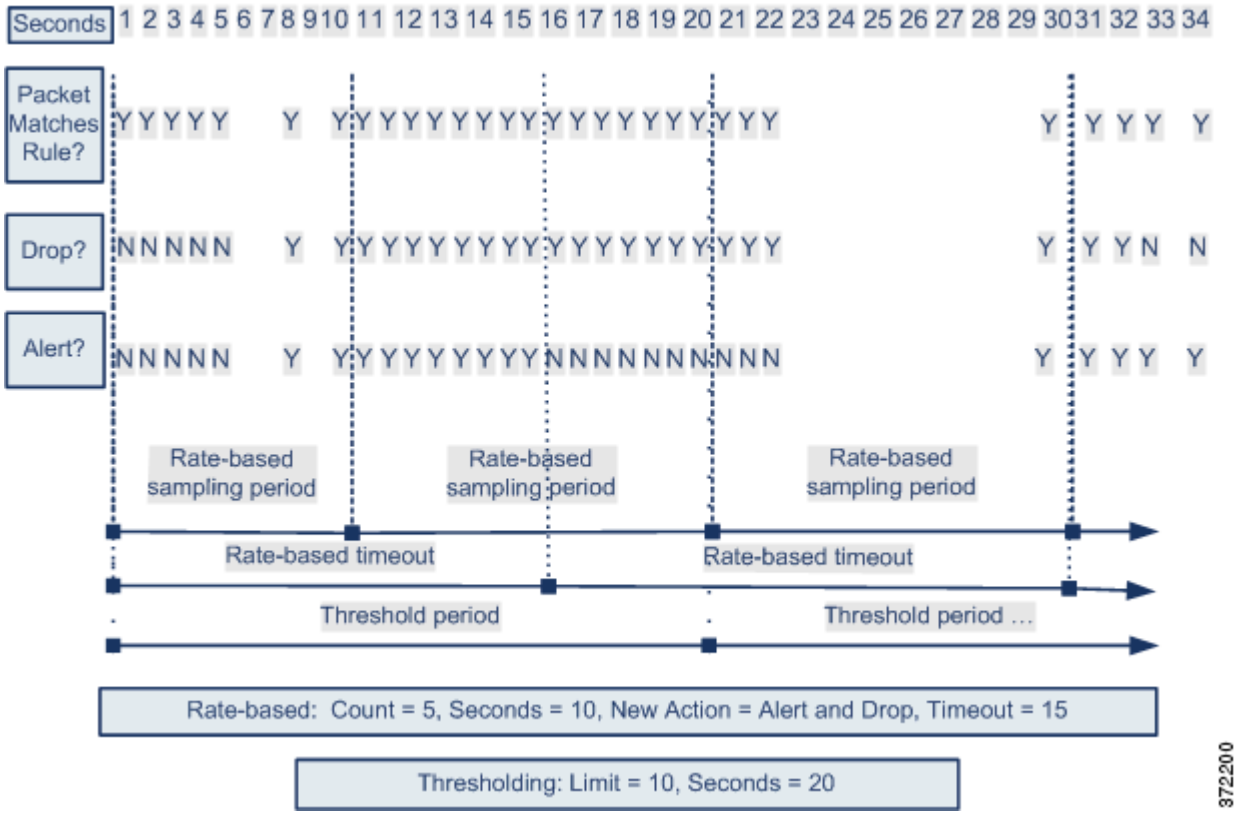
しきい値および抑制を使用して、送信元または宛先に関するイベント通知の数を制限するか、またはイベント通知を一切抑制することにより、過剰なイベントが生成されないようにすることができます。しきい値と抑制で使用可能なオプションの詳細については、グローバルしきい値の設定（35-3 ページ）、イベントしきい値の設定（32-25 ページ）、および侵入ポリシー単位の抑制の設定（32-30 ページ）を参照してください。

抑制がルールに適用されている場合、ポリシー全体またはルール固有のレート ベースの設定によって、レート ベースのアクションが変更されたとしても、該当するすべての IP アドレスに対してそのルールに関するイベント通知が抑制されます。一方、しきい値とレート ベースの基準との間の相互作用はさらに複雑になります。

以下に、ネットワーク上のホストに対して、攻撃者がサービス拒否（DoS）攻撃を仕掛ける例を示します。同じ送信元から多数のホストに対して同時接続が行われると、ポリシー全体の [Control Simultaneous Connections] 設定がトリガーされます。この設定は、1 つの送信元からの接続数が 10 秒間で 5 つに達すると、イベントを生成して悪意のあるトラフィックをドロップします。さらに、グローバル上限しきい値により、ルールまたは設定で生成可能なイベントの数が 20 秒間で 10 件に制限されます。

この図に示されているように、ポリシー全体の設定により、一致する最初の 10 個のパケットに対してイベントが生成され、トラフィックがドロップされます。10 個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成せずにドロップします。

タイムアウト後も、そのパケットは後続のレート ベースのサンプリング期間にドロップされることに注意してください。サンプリングされたレートが、現在または前のサンプリング期間のしきい値レートを超過している場合、レート ベースのアクションによるイベントの生成とトラフィックのドロップが続行されます。レート ベース アクションが停止するのは、サンプリング期間が完了した時点で、サンプリングされたレートがしきい値レートを下回っている場合のみです。



この例には示されていませんが、しきい値に達した*後に*、レート ベースの基準によって新しいアクションがトリガーされた場合、システムはアクションが変更されたことを示す単一のイベントを生成することに注意してください。したがって、たとえば上限しきい値の 10 に達してシステムがイベントの生成を停止し、14 番目のパケットでアクションが [Drop and Generate Events] に変更されると、システムはアクションが変更されたことを示す 11 番目のイベントを生成します。

複数のフィルタリング方法によるレート ベース検出

ライセンス：Protection

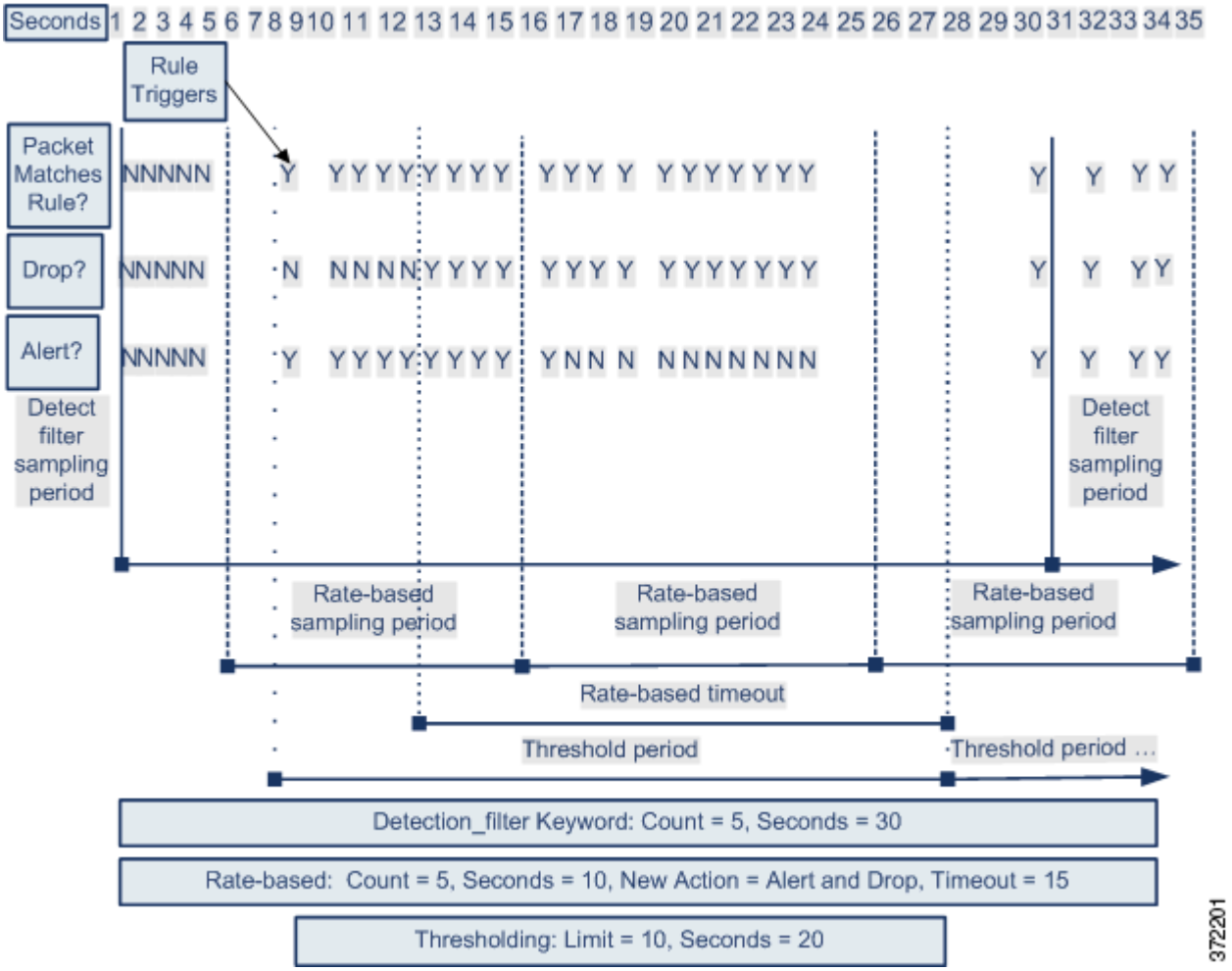
`detection_filter` キーワード、しきい値構成または抑制、およびレート ベースの基準のすべてが同じトラフィックに適用されるという状況が発生することもあります。抑制をルールに適用すると、レート ベースの変更が発生しても、指定の IP アドレスに対するイベントの生成は抑制されます。

以下に、攻撃者がブルートフォース ログインを仕掛ける例で、`detection_filter` キーワード、レート ベースのフィルタリング、およびしきい値が相互作用する場合を説明します。パスワードの検出試行が繰り返されると、カウントが 5 に設定された `detection_filter` キーワードを含むルールがトリガーされます。このルールには、レート ベース攻撃防止も設定されています。その設定では、15 秒間にルールのヒット数が 5 に達すると、ルール属性が 30 秒間、[Drop and Generate Events] に変更されます。さらに、上限しきい値により、ルールによって生成されるイベントは 30 秒間で 10 件に制限されます。

図に示されているように、最初の 5 個のパケットがルールに一致しても、イベント通知は行われません。それは、`detection_filter` キーワードで指定されたレートを超過するまで、ルールはトリガーされないためです。ルールがトリガーされると、イベント通知が開始されますが、さらに 5 個のパケットが通過するまでは、レート ベースの基準によって新しいルールとして [Drop and

Generate Events] がトリガーされることはありません。レート ベースの基準が満たされると、システムは 11 個目から 15 個目のパケットに対してイベントを生成し、パケットをドロップします。15 個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成せずにドロップします。

レート ベースのタイムアウトが発生した後は、それに続くレート ベースのサンプリング期間中、パケットが引き続きドロップされることに注意してください。サンプリング レートが前回のサンプリング期間中にしきい値レートを超えた場合は、新しいアクションが続行されます。



レート ベース攻撃防止の設定

ライセンス：Protection

ポリシー レベルでレート ベース攻撃防止を設定することで、SYN フラッド攻撃を阻止できます。特定の送信元からの過剰な接続、または特定の宛先への過剰な接続を阻止することもできます。

レート ベース攻撃防止を設定するには、次の手順を実行します。

Admin/Intrusion Admin

ステップ 1　[Policies] > [Access Control] > [Access Control Policy] を選択して [Access Control Policy] ページを表示し、[Network Analysis Policy] をクリックします。

[Network Analysis Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルで [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Specific Threat Detection] の下にある [Rate-Based Attack Prevention] が有効になっているかどうかによって、以下の 2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効である場合は、[Enabled] をクリックし、次に [Edit] をクリックします。

[Rate-Based Attack Prevention] ページが表示されます。ページ下部に表示されるメッセージに、この設定が含まれている侵入ポリシー層が示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　次の 2 つのオプションから選択できます。

- ホストのフラッディングを目的とする不完全な接続を防ぐには、[SYN Attack Prevention] の下にある [Add] をクリックします。

  [SYN Attack Prevention] ダイアログ ボックスが表示されます。
- 過剰な数の接続を防ぐには、[Control Simultaneous Connections] の下にある [Add] をクリックします。

  [Control Simultaneous Connections] ダイアログ ボックスが表示されます。

ステップ 6　トラフィックを追跡する方法を選択します。

- 特定の送信元または送信元の範囲からのすべてのトラフィックを追跡するには、[Track By] ドロップダウンリスから [Source] を選択し、[Network] フィールドに単一の IP アドレスまたはアドレス ブロックを入力します。
- 特定の宛先または宛先の範囲へのすべてのトラフィックを追跡するには、[Track By] ドロップダウンリスから [Destination] を選択し、[Network] フィールドに単一の IP アドレスまたはアドレス ブロックを入力します。

システムは、[Network] フィールドに含まれる各 IP アドレスのトラフィックを個別に追跡することに注意してください。ある特定の IP アドレスからの設定されたレートを超過するトラフィックがある場合、その IP アドレスに関するイベントだけが生成されることになります。例として、ネットワーク設定で `10.1.0.0/16` の送信元 CIDR ブロックを設定し、10 個の同時接続が開始された時点でイベントを生成するようにシステムを設定するとします。10.1.4.21 から 8 つの接続が開始され、10.1.5.10 から 6 つの接続が開始されている場合、いずれの送信元も開始されている接続がトリガーを引き起こす数になっていないため、システムはイベントを生成しません。一方、10.1.4.21 から 11 個の同時接続が開始されている場合、システムは 10.1.4.21 からの接続に対してだけイベントを生成します。

FireSIGHT システムで CIDR 表記およびプレフィクス長を使用する方法の詳細については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ステップ 7　レート追跡設定をトリガーとして使用するレートを指定します。

- SYN 攻撃に対する設定の場合は、[Rate] フィールドに、一定の秒数あたりの SYN パケット数を指定します。
- 同時接続に対する設定の場合は、[Count] フィールドに、接続数を指定します。

ステップ 8　レート ベース攻撃防止設定に一致するパケットをドロップするには、[Drop] を選択します。

ステップ 9　[Timeout] フィールドに、イベント生成のタイムアウト期間を指定します。この期間を経過すると、SYN または同時接続のパターンに一致するトラフィックに対するイベント生成が（該当する場合はドロップも）停止されます。

注意　タイムアウト値には 1 ～ 1,000,000 の整数を指定できます。ただし、インライン導入では、大きいタイムアウト値を指定するとホストへの接続が完全にブロックされる可能性があります。

ステップ 10　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

センシティブ データの検出

ライセンス： Protection

社会保障番号、クレジット カード番号、運転免許証番号などのセンシティブ データが、意図的に、あるいは誤ってインターネットに漏洩する場合があります。このシステムで提供している、ASCII テキストでのセンシティブ データを検出してイベントを生成できるセンシティブ データ プリプロセッサは、特に不測のデータ漏洩を検出する上で役立ちます。

このシステムは、暗号化または難読化されたセンシティブ データ、あるいは圧縮または符号化された形式のセンシティブ データ（たとえば、Base64 でエンコードされた電子メールの添付ファイルなど）の検出は行いません。たとえば、システムは電話番号 (555)1234567 を検出しますが、(5 5 5) 1 2 3 - 4 5 6 7 のようにスペースで難読化されたバージョン、あるいは (555)-1234567 のように HTML コードが介在するバージョンは検出しません。ただし、(555)1234567 のように、HTML にコーディングされた番号のパターンの途中にコードが入っていなければ検出されます。

ヒント　センシティブ データ プリプロセッサでは、FTP または HTTP を使用してアップロードおよびダウンロードされる暗号化されていない Microsoft Word ファイル内のセンシティブ データを検出できます。これが可能である理由は、Word ファイルが ASCII テキストとフォーマット設定コマンドを分けてグループ化する方式だからです。

システムは、TCP セッションごとに個々のデータ タイプとトラフィックを照合することによって、センシティブ データを検出します。侵入防御ポリシーの、各データ タイプのデフォルト設定およびすべてのデータ タイプに適用されるグローバル オプションのデフォルト設定は変更できます。Ciscoでは、事前定義された、よく使用されるデータ タイプを用意しています。カスタム データ タイプを作成することも可能です。

センシティブ データ プリプロセッサ ルールは、各データ タイプに関連付けられます。各データ タイプのセンシティブ データ検出とイベント生成を有効にするには、そのデータ タイプに対応するプリプロセッサ ルールを有効にします。設定ページのリンクを使用すると、センシティブ データ ルールにフィルタリングされたビューが [Rules] ページに表示されます。このビューで、ルールを有効または無効にしたり、その他のルール属性を設定したりできます。

変更を侵入防御ポリシーに保存する際に提示されるオプションによって、データ タイプに関連付けられたルールが有効になっていてセンシティブ データ検出が無効になっている場合には、自動的にセンシティブ データ プリプロセッサを有効にすることができます。

詳細については、次の項を参照してください。

- センシティブ データ検出の導入（34-21 ページ）
- グローバル センシティブ データ検出オプションの選択（34-21 ページ）
- 個別データ タイプ オプションの選択（34-22 ページ）
- 定義済みデータ タイプの使用（34-24 ページ）
- センシティブ データ検出の設定（34-25 ページ）
- モニタするアプリケーション プロトコルの選択（34-27 ページ）
- 特殊な場合：FTP トラフィックでのセンシティブ データの検出（34-29 ページ）
- カスタム データ タイプの使用（34-29 ページ）

センシティブ データ検出の導入

ライセンス： Protection

センシティブ データ検出は FireSIGHT システムのパフォーマンスに非常に大きな影響を与える可能性があるため、Cisco では以下のガイドラインに従うことを推奨しています。

- デフォルト ポリシー [No Rules Active] をベースになる侵入ポリシーとして選択します。詳細については、システムによって提供される基本ポリシーについて（24-3 ページ）を参照してください。
- 次の設定が対応するネットワーク分析ポリシーで有効になっていることを確認します。
  - [Application Layer Preprocessors] の下の [FTP and Telnet Configuration]
  - [Transport/Network Layer Preprocessors] の下の [IP Defragmentation] および [TCP Stream Configuration]
- センシティブ データ設定のある侵入防御ポリシーを含むアクセス コントロール ポリシーは、センシティブ データ検出用に予約済みの別個のデバイスに適用します。詳細については、アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

グローバル センシティブ データ検出オプションの選択

ライセンス： Protection

グローバル センシティブ データ プリプロセッサ オプションは、プリプロセッサの動作を制御します。以下のことを指定するグローバル オプションを変更できます。

- プリプロセッサが、ルールをトリガーしたパケットで、クレジット カード番号または社会保障番号の下位 4 桁を除くすべての桁を置換するかどうか
- センシティブ データをモニタする、ネットワーク上の宛先ホスト

- イベントの生成基準となる、単一のセッションでの全データ タイプの合計オカレンス数

グローバル センシティブ データ オプションはポリシーに固有であり、すべてのデータ タイプに適用されることに注意してください。

次のグローバルなセンシティブ データ検出オプションを設定できます。

Mask

ルールをトリガーしたパケットで、クレジット カード番号および社会保障番号の下位 4 桁を除くすべての桁を「X」に置換します。Web インターフェイスの侵入イベント パケット ビューおよびおよびダウンロードされたパケットでは、マスクされた番号が表示されます。詳細については、「パケット ビューの使用（41-23 ページ）」を参照してください。

Networks

センシティブ データをモニタする 1 つ以上の宛先ホストを指定します。単一の IP アドレス、アドレス ブロック、あるいはこのいずれかまたは両方のカンマ区切りリストを指定できます。空白のフィールドは、any として解釈されます。これは、任意の宛先 IP アドレスを意味します。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-23 ページ）を参照してください。

Global Threshold

グローバルしきい値イベントの生成基準となる、単一セッションでの全データ タイプの合計オカレンス数を指定します。データ タイプの組み合わせを問わず、プリプロセッサは指定された数のデータ タイプを検出すると、グローバルしきい値イベントを生成します。1 ～ 65535 の値を指定できます。

Ciscoでは、このオプションに、ポリシーで有効にする個々のデータ タイプに対するしきい値のどれよりも大きい値を設定することを推奨しています。詳細については、「個別データ タイプ オプションの選択（34-22 ページ）」を参照してください。

グローバルしきい値については、以下の点に注意してください。

- 複数のデータ タイプを合わせたオカレンス数を検出してイベントを生成するには、プリプロセッサ ルールの 139:1 を有効にする必要があります。侵入防御ポリシーでルールを有効にする方法については、ルール状態の設定（32-22 ページ）を参照してください。
- プリプロセッサが生成するグローバルしきい値イベントは、セッションあたり最大 1 件です。
- グローバルしきい値イベントと個別データ タイプ イベントは、互いに独立しています。つまり、グローバルしきい値に達すると、個別データ タイプに対するイベントしきい値に達しているかどうかに関わらず、プリプロセッサがイベントを生成します。その逆も当てはまります。

個別データ タイプ オプションの選択

ライセンス： Protection

個別のデータ タイプによって、指定した宛先ネットワーク トラフィックで検出しイベントを生成できるセンシティブ データを特定します。以下のことを指定するデータ タイプ オプションのデフォルト設定を変更できます。

- 検出されたデータ タイプに対して単一のセッションごとのイベントを生成する基準とするしきい値
- 各データ タイプをモニタする宛先ポート

- 各データ タイプをモニタするアプリケーション プロトコル

最低でも、データ タイプごとにイベントしきい値を指定し、モニタする少なくとも 1 つのポートまたはアプリケーション プロトコルを指定する必要があります。

Cisco で用意している各定義済みデータ タイプでは、デフォルト値が変更されない限り、アクセス不能な `sd_pattern` キーワードを使用して、トラフィックで検出する組み込みデータ パターンを定義します。定義済みデータ タイプのリストについては、表 34-8（34-24 ページ）を参照してください。カスタム データ タイプを作成して、そのデータ タイプに対し、単純な正規表現を使用して独自のデータ パターンを指定することもできます。詳細については、「カスタム データ タイプの使用（34-29 ページ）」を参照してください。

データ タイプの名前とパターンはシステム全体に適用されることに注意してください。その他すべてのデータ タイプ オプションはポリシーに固有です。

次の表に、設定できるデータ タイプ オプションを記載します。

表 34-7　個別データ タイプ オプション

オプション	説明
データ タイプ	データ タイプの一意の名前を表示します。
Threshold	イベント生成の基準とする、データ タイプのオカレンス数を指定します。有効にしたデータ タイプに対してしきい値を設定せずにポリシーを保存しようとすると、エラー メッセージが表示されます。1 ～ 255 の値を指定できます。 プリプロセッサが検出したデータ タイプに対して生成するイベント数は、セッションごとに 1 つであることに注意してください。グローバルしきい値イベントと個別データ タイプ イベントは、互いに独立していることにも注意してください。つまり、データ タイプ イベントしきい値に達すると、グローバルしきい値に達しているかどうかに関わらず、プリプロセッサがイベントを生成します。その逆も当てはまります。
宛先ポート	データ タイプでモニタする宛先ポートを指定します。単一のポート、複数のポートをカンマで区切ったリスト、または任意の宛先ポートを意味する `any` を指定できます。データ タイプのルールを有効にした場合、そのデータ タイプに対して少なくとも 1 つのポートまたはアプリケーション プロトコルを設定せずにポリシーを保存しようとすると、エラー メッセージが表示されます。
Application Protocols この機能には、Control ライセンスが必要です。	データ タイプでモニタする最大 8 つのアプリケーション プロトコルを指定します。データ タイプのルールを有効にした場合、そのデータ タイプに対して少なくとも 1 つのポートまたはアプリケーション プロトコルを設定せずにポリシーを保存しようとすると、エラー メッセージが表示されます。 選択するアプリケーション プロトコルごとに、少なくとも 1 つのディテクタを有効にする必要があります（ディテクタのアクティブ化と非アクティブ化（46-30 ページ）を参照）。デフォルトでは、Ciscoが提供するすべてのディテクタはアクティブになっています。アプリケーション プロトコルに対して有効になっているディレクタがない場合は、Cisco提供のすべてのディテクタがアプリケーションに対して自動的に有効になります。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタがアプリケーションに対して有効になります。 データ タイプのアプリケーション プロトコルを選択する方法の詳細については、モニタするアプリケーション プロトコルの選択（34-27 ページ）を参照してください。

表 34-7　個別データ タイプ オプション（続き）

オプション	説明
Pattern	カスタム データ タイプの場合、検出するパターンを指定します（Cisco提供のデータ タイプのデータ パターンは事前に定義されています）。詳細については、「カスタム データ タイプの使用（34-29 ページ）」を参照してください。Web インターフェイスには、定義済みデータ タイプの組み込みパターンは表示されません。 カスタム データ パターンと定義済みデータ パターンは、システム全体に適用されることに注意してください。

定義済みデータ タイプの使用

ライセンス：Protection

それぞれの侵入防御ポリシーには、よく使用されるデータ パターンを検出するために事前に定義されたデータ タイプが含まれています。これらのデータ パターンには、クレジット カード番号、電子メールアドレス、米国の 電話番号、および米国の 社会保障番号などがあります（番号にはハイフン付きのパターン、ハイフン抜きのパターンがあります）。各定義済みデータ タイプは、ジェネレータ ID（GID）が 138 に設定された単一のセンシティブ データ プリプロセッサに関連付けられます。ポリシーで使用する各データ タイプに対し、検出およびイベント生成を有効にするには、侵入ポリシーで関連付けられたセンシティブ データ ルールを有効にする必要があります。侵入防御ポリシーでルールを有効にする方法については、ルール状態の設定（32-22 ページ）を参照してください。

センシティブ データ ルールを有効にするには、設定ページに表示されるリンクを利用できます。このリンクを使用すると、すべての定義済みセンシティブ データ ルールおよびカスタム センシティブ データ ルールを表示するフィルタリングされたビューの [Rules] ページが表示されます。また、センシティブ データ ルールのフィルタ カテゴリを選択して、[Rules] ページに定義済みセンシティブ データ ルールだけを表示することもできます。詳細については、「侵入ポリシー内のルールのフィルタ処理（32-10 ページ）」を参照してください。定義済みセンシティブ データ ルールは、[Rule Editor] ページ（[Policies] > [Intrusion] > [Rule Editor]）にもリストされます。このページでは、センシティブ データ ルール カテゴリに属する定義済みセンシティブ データ ルールを確認できますが、これらのルールを編集することはできません。

以下の表に、データ タイプを記載し、各データ タイプを検出してイベントを生成するために有効にしなければならない、対応するプリプロセッサ ルールをリストします。

表 34-8　センシティブ データ タイプ

データ タイプ	説明	プリプロセッサルール GID:SID
クレジットカード番号	Visa®、MasterCard®、Discover®、および American Express® の 15 桁または 16 桁のクレジット カード番号（通常の区切り文字として使用されるハイフンまたはスペースが含まれるパターンと含まれないパターン）に一致します。また、Luhn アルゴリズムを使用してクレジット カード番号の検査数字を確認します。	138:2
電子メール アドレス	電子メール アドレスに一致します。	138:5
米国の 電話番号	米国の 電話番号（`(\d{3}) ?\d{3}-\d{4}` のパターンに準拠）に一致します。	138:6

表 34-8　センシティブ データ タイプ(続き)

データ タイプ	説明	プリプロセッサルール GID:SID
米国の 社会保障番号(ハイフンなし)	米国の 9 桁の 社会保障番号(有効な 3 桁のエリア番号と有効な 2 桁のグループ番号が含まれ、ハイフンを使用していない番号)に一致します。	138:4
米国の 社会保障番号(ハイフンあり)	米国の 9 桁の 社会保障番号(有効な 3 桁のエリア番号と有効な 2 桁のグループ番号が含まれ、ハイフンを使用した番号)に一致します。	138:3
Custom	指定されたトラフィックでユーザ定義のデータ パターンに一致します。詳細については、「カスタム データ タイプの使用 (34-29 ページ)」を参照してください。	138:>999999

社会保障番号以外の 9 桁の番号からの誤検出を軽減するために、プリプロセッサでは、各社会保障番号の 4 桁のシリアル番号の前にある 3 桁のエリア番号と 2 桁のグループ番号を検証するアルゴリズムを使用します。プリプロセッサは 2009 年 11 月末までの社会保障グループ番号を検証します。

センシティブ データ検出の設定

ライセンス: Protection

デフォルトのグローバル設定および個別データ タイプの設定を変更できます。検出する各データ タイプのプリプロセッサ ルールを有効にする必要もあります。

ポリシーでセンシティブ データ プリプロセッサ ルールを有効にして、センシティブ データ検出を有効にしていなければ、変更をポリシーに保存する際に、センシティブ データ検出を有効にするよう求めるプロンプトが出されます。詳細については、「競合の解決とポリシー変更の確定 (23-17 ページ)」を参照してください。

以下の表に、[Sensitive Data Detection] ページで実行できる操作を記載します。

表 34-9　センシティブ データ設定の操作

目的	操作
グローバル設定を変更する	ユーザが変更できるグローバル設定については、表 34-6 (34-9 ページ) を参照してください。
データ タイプ オプションを変更する	[Targets] ページ領域で、データ タイプの名前をクリックします。 [Configuration] ページ領域が更新され、データ タイプの現在の設定が表示されます。ユーザが変更できるオプションについては、個別データ タイプ オプションの表を参照してください。

表 34-9　センシティブ データ設定の操作（続き）

目的	操作
データ タイプでモニタするアプリケーション プロトコルを追加または削除する この機能には、Control ライセンスが必要です。	[Application Protocols] フィールド内をクリックするか、このフィールドの横にある [Edit] をクリックします。[Application Protocols] ポップアップ ウィンドウが表示されます。 • モニタするアプリケーション プロトコル（最大 8 つ）を追加するには、左側の [Available] リストからアプリケーション プロトコルを 1 つ以上選択して、右矢印（>）ボタンをクリックします。 • アプリケーション プロトコルを削除するには、右側の [Enabled] リストから削除するアプリケーション プロトコルを選択して、左矢印（<）ボタンをクリックします。 複数のアプリケーション プロトコルを選択するには、Ctrl キーまたは Shift キーを押しながらクリックします。クリックしてドラッグすることで、複数の連続するアプリケーション プロトコルを選択することもできます。 選択するアプリケーション プロトコルごとに、少なくとも 1 つのディテクタを有効にする必要があります（ディテクタのアクティブ化と非アクティブ化（46-30 ページ）を参照）。デフォルトでは、Ciscoが提供するすべてのディテクタはアクティブになっています。アプリケーション プロトコルに対して有効になっているディレクタがない場合は、Cisco提供のすべてのディテクタがアプリケーションに対して自動的に有効になります。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタがアプリケーションに対して有効になります。 **注**　FTP トラフィックでセンシティブ データを検出するには、`Ftp data` アプリケーション プロトコルを追加する必要があります。詳細については、「特殊な場合：FTP トラフィックでのセンシティブ データの検出（34-29 ページ）」を参照してください。
カスタム データ タイプを作成する	ページ左側の [Data Types] の横にある [+] 記号をクリックします。[Add Data Type] ポップアップ ウィンドウが表示されます。 データ タイプの一意の名前と、このデータ タイプで検出するパターンを指定して、[OK] をクリックします。編集を破棄するには [Cancel] をクリックします。詳細については、「カスタム データ タイプの使用（34-29 ページ）」を参照してください。
センシティブ データ プリプロセッサ ルールを表示する	[Global Settings] ページ領域の上に表示されている [Configure Rules for Sensitive Data Detection] リンクをクリックします。[Rules] ページの表示がフィルタリングされ、すべてのセンシティブ データ プリプロセッサ ルールのリストが表示されます。 オプションで、リストされているルールを有効または無効にすることができます。侵入防御ポリシーで使用する各データ タイプのセンシティブ データ プリプロセッサ ルールを有効にする必要があることに注意してください。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。 [Rules] ページで使用可能なその他の操作（ルールの抑制、レート ベース攻撃の防止など）のセンシティブ データ ルールの設定も行えます。詳細については、ルールを使用した侵入ポリシーの調整（32-1 ページ）を参照してください。 [Back] をクリックして [Sensitive Data Detection] ページに戻ります。

センシティブ データ検出を設定する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルにある [Advanced Settings] をクリックします。

[Advanced Settings] ページが表示されます。

ステップ 4　[Specific Threat Detection] の下にある [Sensitive Data Detection] が有効になっているかどうかによって、2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効になっている場合は、[Enabled] をクリックしてから、[Edit] をクリックします。

[Sensitive Data Detection] ページが表示されます。ページ下部に表示されるメッセージに、この設定が含まれている侵入ポリシー レイヤが示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　センシティブ データ設定の操作の表で説明されている操作を実行できます。

ステップ 6　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

モニタするアプリケーション プロトコルの選択

ライセンス：Control

各データ タイプでモニタするアプリケーション プロトコルを最大 8 つ指定できます。システムがネットワーク上で検出できるアプリケーション プロトコルの詳細については、サーバの使用（50-39 ページ）を参照してください。

選択するアプリケーション プロトコルごとに、少なくとも 1 つのディテクタを有効にする必要があります（ディテクタのアクティブ化と非アクティブ化（46-30 ページ）を参照）。デフォルトでは、Ciscoが提供するすべてのディテクタはアクティブになっています。アプリケーション プロトコルに対して有効になっているディレクタがない場合は、Cisco提供のすべてのディテクタがアプリケーションに対して自動的に有効になります。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタがアプリケーションに対して有効になります。

各データ タイプをモニタするアプリケーション プロトコルまたはポートを少なくとも 1 つ指定する必要があります。ただし、FTP トラフィックでセンシティブ データを検出する場合を除き、Ciscoでは最も包括的なカバレッジにするために、アプリケーション プロトコルを指定する際には対応するポートを指定することを推奨しています。たとえば、HTTP を指定するとしたら、既知の HTTP ポート 80 を設定することお勧めします。このように設定すると、ネットワークの新しいホストが HTTP を実装する場合には、システムは新しい HTTP アプリケーション プロトコルを検出する間、ポート 80 をモニタします。

FTP トラフィックでセンシティブ データを検出する場合は、`FTP data` アプリケーション プロトコルを指定する必要があります。ポート番号を指定する利点はありません。詳細については、「特殊な場合：FTP トラフィックでのセンシティブ データの検出（34-29 ページ）」を参照してください。

センシティブ データを検出するためにアプリケーション プロトコルを変更する方法:

Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーでまだ保存されていない変更がある場合、それらの変更を破棄して続行するには [OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(23-17 ページ)を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルにある [Advanced Settings] をクリックします。

[Advanced Settings] ページが表示されます。

ステップ 4　[Specific Threat Detection] の下にある [Sensitive Data Detection] が有効になっているかどうかによって、2 つの選択肢があります。

- この設定が有効にされている場合、[Edit] をクリックします。
- 設定が無効になっている場合は、[Enabled] をクリックしてから、[Edit] をクリックします。

[Sensitive Data Detection] ページが表示されます。

ページ下部に表示されるメッセージに、この設定が含まれている侵入ポリシー レイヤが示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用(24-1 ページ)」を参照してください。

ステップ 5　[Data Types] にリストされているデータ タイプ名をクリックして、変更するデータ タイプを選択します。

[Configuration] 領域が更新されて、選択したデータ タイプの現在の設定が表示されます。

ステップ 6　[Application Protocols] フィールド内をクリックするか、このフィールドの横にある [Edit] をクリックします。

[Application Protocols] ポップアップ ウィンドウが表示されます。

ステップ 7　次の 2 つの選択肢があります。

- モニタするアプリケーション プロトコル(最大 8 つ)を追加するには、左側の [Available] リストからアプリケーション プロトコルを 1 つ以上選択して、右矢印(**>**)ボタンをクリックします。
- アプリケーション プロトコルを削除するには、右側の [Enabled] リストから削除するアプリケーション プロトコルを選択して、左矢印(**<**)ボタンをクリックします。

複数のアプリケーション プロトコルを選択するには、Ctrl キーまたは Shift キーを押しながらクリックします。クリックしてドラッグすることで、複数の連続するアプリケーション プロトコルを選択することもできます。

注　FTP トラフィックでセンシティブ データを検出するには、`Ftp data` アプリケーション プロトコルを追加する必要があります。詳細については、「特殊な場合:FTP トラフィックでのセンシティブ データの検出(34-29 ページ)」を参照してください。

ステップ 8　[OK] をクリックしてアプリケーション プロトコルを追加します。

[Sensitive Data Detection] ページが表示され、アプリケーション プロトコルが更新されます。

特殊な場合:FTP トラフィックでのセンシティブ データの検出

ライセンス: Control

一般に、センシティブ データをモニタするトラフィックを決めるには、導入でのモニタ対象のポートを指定するか、あるいはオプションで、アプリケーション プロトコルを指定します。ただし、FTP トラフィックでセンシティブ データを検出するには、ポートまたはアプリケーション プロトコルを指定するだけでは不十分です。FTP トラフィックのセンシティブ データは、FTP アプリケーション プロトコルのトラフィックで検出されますが、FTP アプリケーション プロトコルは断続的に発生し、一時的なポート番号を使用するため、センシティブ データを検出するのが困難です。FTP トラフィックでセンシティブ データを検出するには、以下の設定を含めることが**必須**となります。

- `FTP data` アプリケーション プロトコルを指定します。

  `FTP data` アプリケーション プロトコルを指定すると、FTP でのセンシティブ データの検出が可能になります。詳細については、「モニタするアプリケーション プロトコルの選択（34-27 ページ）」を参照してください。

  FTP トラフィックでセンシティブ データを検出するという特殊な場合では、`FTP data` アプリケーション プロトコルを指定すると、検出が呼び出される代わりに、FTP トラフィックでセンシティブ データを検出するために FTP/Telnet プロセッサの高速処理が呼び出されます。詳細については、「FTP および Telnet トラフィックのデコード（27-20 ページ）」を参照してください。

- FTP データ ディテクタが有効であることを確認します（デフォルトで有効にされます）。

  ディテクタのアクティブ化と非アクティブ化（46-30 ページ）を参照してください。

- 設定に、センシティブ データをモニタするポートが少なくとも 1 つ含まれていることを確認します。

  FTP トラフィックでセンシティブ データを検出することだけが目的の場合を除き（そのような場合はほとんどありません）、FTP ポートを指定する必要はありません。通常のセンシティブ データ設定には、HTTP ポートや電子メール ポートなどの他のポートが含まれることになります。モニタ対象の FTP ポートを 1 つだけ指定し、他のポートを指定しない場合、Ciscoでは、FTP ポート `23`　を指定することを推奨しています。詳細については、センシティブ データ検出の設定（34-25 ページ）を参照してください。

カスタム データ タイプの使用

ライセンス: Protection

指定するデータ パターンを検出するためのカスタム データ タイプを作成および変更することができます。たとえば、病院で患者番号を保護するためのデータ タイプを作成したり、大学で固有の番号パターンを持つ学生番号を検出するためのデータ タイプを作成したりすることが考えられます。

作成するカスタム データ タイプごとに、単一のセンシティブ データ プリプロセッサ ルールも作成します。このルールのジェネレータ ID（GID）は 138 で、Snort ID は 1000000 以上（これは、ローカル ルールの SID）です。ポリシーで特定のデータ タイプを検出してイベントを生成するには、そのカスタム データ タイプに関連付けられたセンシティブ データ ルールを有効にする必要があります。侵入防御ポリシーでルールを有効にする方法については、ルール状態の設定（32-22 ページ）を参照してください。

センシティブ データ ルールを有効にするには、設定ページに表示されるリンクを利用できます。このリンクを使用すると、すべての定義済みセンシティブ データ ルールおよびカスタム センシティブ データ ルールを表示するフィルタリングされたビューの [Rules] ページが表示され

ます。また、ローカル ルールのフィルタ カテゴリを選択して、[Rules] ページにカスタム センシティブ データ ルールだけを表示することもできます。詳細については、「侵入ポリシー内のルールのフィルタ処理（32-10 ページ）」を参照してください。カスタム センシティブ データ ルールは、[Rule Editor] ページには表示されないことに注意してください。

作成するカスタム データ タイプは、すべての侵入防御ポリシーに追加されます。特定のカスタム データ タイプを検出してイベントを生成するには、使用するポリシーで、そのカスタム データ タイプに関連付けられたセンシティブ データ ルールを有効にする必要があります。

データ タイプとそのデータ タイプに関連付けるルールを作成するには、[Sensitive Data Detection] 設定ページを使用する必要があることに注意してください。ルール エディタを使用してセンシティブ データ ルールを作成することはできません。

詳細については、次の項を参照してください。

- カスタム データ タイプのデータ パターンの定義（34-30 ページ）
- カスタム データ タイプの設定（34-32 ページ）
- カスタム データ タイプの名前と検出パターンの編集（34-33 ページ）

カスタム データ タイプのデータ パターンの定義

ライセンス： Protection

カスタム データ タイプのデータ パターンを定義するには、以下の要素からなる単純な正規表現のセットを使用します。

- 3 つのメタ文字
- メタ文字をリテラル文字として使用するためのエスケープ文字
- 6 文字クラス

メタ文字とは、正規表現の中で特別な意味を持つ文字です。以下の表に、カスタム データ パターンを定義する際に使用できるメタ文字を記載します。

表 34-10　センシティブ データ パターンのメタ文字

メタ文字	説明	例
`?`	先行する文字またはエスケープ シーケンスのゼロまたは 1 つのオカレンスに一致します。つまり、先行する文字またはエスケープ シーケンスはオプションです。	`colou?r` は、`color` または `colour` に一致します。
`{n}`	先行する文字またはエスケープ シーケンスの *n* 回の繰り返しに一致します。	次に例を示します。 `\d{2}` は、`55`、`12` などに一致します。 `\l{3}` は、`AbC`、`www` などに一致します。 `\w{3}` は、`a1B`、25C などに一致します。 `x{5}` は、`xxxxx` に一致します。
`\`	メタ文字を実際の文字として使用できます。また、事前定義された文字クラスを指定するためにも使われます。センシティブ データ パターンで使用できる文字クラスについては、表 34-12（34-31 ページ）を参照してください。	`\?` は疑問符に一致します。 `\\` はバックスラッシュに一致します。 `\ d` は数字に一致します。

以下の表に記載する文字をリテラル文字としてセンシティブ データ プリプロセッサに正しく解釈させるには、バックスラッシュで文字をエスケープする必要があります。

表 34-11　センシティブ データ パターンのエスケープ文字

使用するエスケープ文字	表現されるリテラル文字
\?	?
\{	{
\}	}
\\	\

以下の表に、カスタム センシティブ データ パターンを定義する際に使用できる文字クラスを記載します。

表 34-12　センシティブ データ パターンの文字クラス

文字クラス	説明	文字クラスの定義
\d	ASCII 文字の数字 0 ～ 9 に一致します。	0 ～ 9
\D	ASCII 文字の数字ではないバイトに一致します。	0 ～ 9 以外
\l（小文字の「エル」）	任意の ASCII 文字に一致します。	a-zA-Z
\L	ASCII 文字ではないバイトに一致します。	a-zA-Z 以外
\w	任意の ASCII 英数字に一致します。 PCRE 正規表現とは異なり、アンダースコア（_）は含まれないことに注意してください。	a-zA-Z0-9
\W	ASCII 英数字でないバイトに一致します。	a ～ z、A ～ Z、および 0 ～ 9 以外

プリプロセッサは、そのまま入力された文字を、正規表現の一部ではなく、リテラル文字として扱います。たとえば、データ パターン 1234 は `1234` に一致します。

以下に、定義済みセンシティブ データ ルール 138:4 で使用するデータ パターンの例を示します。このパターンでは、エスケープされた数値の文字クラス、複数個を示すメタ文字およびオプション指定子のメタ文字、リテラル ハイフン（-）文字、および左右の括弧（）文字を使用して、米国の 電話番号を検出します。

```
(\d{3}) ?\d{3}-\d{4}
```

カスタム データ パターンを作成する際には注意が必要です。以下に、電話番号を検出するための別のデータ パターンを示します。このパターンでは有効な構文を使用しているものの、多数の誤検出が発生する可能性があります。

```
(?\d{3})??\d{3}-?\d{4}
```

上記の 2 番目の例では、オプションの括弧、オプションのスペース、オプションのハイフンを組み合わせているため、目的とする以下のパターンの電話番号が検出されます。

- `(555)123-4567`
- `555123-4567`
- `5551234567`

ただし、2 番目の例のパターンでは、以下の潜在的に無効な無効なパターンも検出されて、結果的に誤検出となります。

- `(555 1234567`
- `555)123-4567`
- `555) 123-4567`

最後に、説明目的の極端な例として、小規模な企業ネットワーク上のすべての宛先トラフィックで小さいイベントしきい値を使用して、小文字の a を検出するデータ パターンを作成するとします。このようなデータ パターンは、わずか数分で文字通り数百万ものイベントを生成することになり、システムを過負荷に陥らせる可能性があります。

カスタム データ タイプの設定

ライセンス：Protection

基本的には、カスタム データ タイプにも、定義済みデータ タイプを設定する場合と同じデータ タイプ オプションを設定します。すべてのデータ タイプに共通の設定オプションを設定する方法については、個別データ タイプ オプションの選択（34-22 ページ）を参照してください。また、カスタム データ タイプにも名前とデータ パターンを指定する必要があります。

カスタム データ タイプを作成すると、そのカスタム データ タイプに関連付けられたカスタム センシティブ データ プリプロセッサ ルールが作成されます。このルールは、カスタム データ タイプを使用する各ポリシーで有効にしなければならないことに注意してください。侵入防御ポリシーでルールを有効にする方法については、ルール状態の設定（32-22 ページ）を参照してください。

カスタム データ タイプを作成または変更する方法：

Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルにある [Advanced Settings] をクリックします。

[Advanced Settings] ページが表示されます。

ステップ 4　[Specific Threat Detection] の下にある [Sensitive Data Detection] が有効になっているかどうかによって、2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効になっている場合は、[Enabled] をクリックしてから、[Edit] をクリックします。

[Sensitive Data Detection] ページが表示されます。

ページ下部に表示されるメッセージに、この設定が含まれている侵入ポリシー レイヤが示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　次の選択肢があります。

- カスタム データ タイプを作成するには、ページ左側の [Data Types] の横にある [+] 記号をクリックします。[Add Data Type] ポップアップ ウィンドウが表示されます。

  データ タイプの一意の名前と、このデータ タイプで検出するパターンを指定して、[OK] をクリックします。編集を破棄するには [Cancel] をクリックします。詳細については、「カスタム データ タイプの名前と検出パターンの編集（34-33 ページ）」を参照してください。

  [Sensitive Data Detection] ページが表示されます。[OK] をクリックすると、ページが更新されて変更が反映されます。

- 定義済みデータ タイプとカスタム データ タイプに共通のオプションを変更するには、[Targets] ページ領域でデータ タイプ名をクリックします。

  [Configuration] ページ領域が更新され、データ タイプの現在の設定が表示されます。詳細については、「センシティブ データ検出の設定（34-25 ページ）」を参照してください。

- システム全体に適用されるカスタム データ タイプの名前およびデータ パターンを編集するには、カスタム データ タイプの名前と検出パターンの編集（34-33 ページ）を参照してください。

- カスタム データ タイプを削除するには、削除するデータ タイプの横にある削除アイコン（ ）をクリックしてから、[OK] をクリックします。データ タイプの削除を中止する場合は、[Cancel] をクリックします。

  データ タイプのセンシティブ データ ルールがいずれかの侵入防御ポリシーで有効にされている場合、そのデータ タイプを削除することはできません。カスタム データ タイプを削除すると、そのカスタム データ タイプはすべての侵入防御ポリシーから削除されます。

カスタム データ タイプの名前と検出パターンの編集

ライセンス：Protection

システム全体に適用されるカスタム センシティブ データ ルールの名前および検出パターンを変更できます。これらの設定を変更すると、システム上の他のすべてのポリシーに変更が適用されます。変更したカスタム データ タイプを使用する侵入防御ポリシーが含まれるアクセス コントロール ポリシーを再適用する必要があることにも注意してください。

カスタム データ タイプの名前とデータ パターンを除き、カスタム データ タイプと定義済みデータ タイプのすべてのデータ タイプ オプションは、ポリシーに固有です。カスタム データ タイプで名前とデータ パターンを除くオプションを変更する方法については、個別データ タイプ オプションの選択（34-22 ページ）を参照してください。

カスタム データ タイプの名前およびデータ パターンを編集する方法：

Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルにある [Advanced Settings] をクリックします。

[Advanced Settings] ページが表示されます。

ステップ 4　[Specific Threat Detection] の下にある [Sensitive Data Detection] が有効になっているかどうかによって、2 つの選択肢があります。

- 設定が有効である場合は、[Edit] をクリックします。
- 設定が無効になっている場合は、[Enabled] をクリックしてから、[Edit] をクリックします。

[Sensitive Data Detection] ページが表示されます。

ページ下部に表示されるメッセージに、この設定が含まれている侵入ポリシー レイヤが示されます。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　[Targets] ページ領域で、変更するカスタム データ タイプの名前をクリックします。

ページが更新されて、データ タイプの現在の設定が表示されます。また、[Configuration] ページ領域の右上隅に、[Edit Data Type Name and Pattern] リンクが表示されます。

ステップ 6　[Edit Data Type Name and Pattern] リンクをクリックします。

[Edit Data Type] ポップアップ ウィンドウが表示されます。

ステップ 7　データ タイプの名前、パターン、またはその両方を変更して、[OK] をクリックします。編集を破棄する場合は、[Cancel] をクリックします。データ パターンを指定する方法については、カスタム データ タイプのデータ パターンの定義（34-30 ページ）を参照してください。

[Sensitive Data Detection] ページが表示されます。[OK] をクリックすると、ページに変更が反映されます。

侵入イベントのロギングのグローバルな制限

システムが侵入イベントを記録して表示する回数を制限するしきい値を使用できます。侵入ポリシーの一部として設定するしきい値によって、指定された期間内でルールに一致するトラフィックが特定のアドレスまたはアドレス範囲から送受信される回数に基づいて、システムがイベントを生成します。これにより、多数のイベントでいっぱいになることを回避できます。この機能には Protection ライセンスが必要です。

イベント通知しきい値は、次の 2 種類の方法で設定できます。

- すべてのトラフィックに対するグローバルしきい値を設定して、指定された期間に特定の送信元または宛先からのイベントが記録され表示される頻度を制限できます。詳細については、しきい値について（35-1 ページ）およびグローバルしきい値の設定（35-3 ページ）を参照してください。
- 侵入ポリシー設定でのshared object rule、標準テキスト ルール、プリプロセッサ ルールごとにしきい値を設定できます。イベントしきい値の設定（32-25 ページ）を参照してください。

しきい値について

ライセンス： Protection

デフォルトでは、侵入ポリシーごとに、グローバル ルールしきい値が含まれます。デフォルトのしきい値では、各ルールのイベント生成が、同じ宛先に送られるトラフィックで 60 秒あたり 1 つのイベントに制限されます。このグローバルしきい値は、デフォルトですべての侵入ルールとプリプロセッサ ルールに適用されます。しきい値は侵入ポリシーの [Advanced Settings] ページで無効にできることに注意してください。

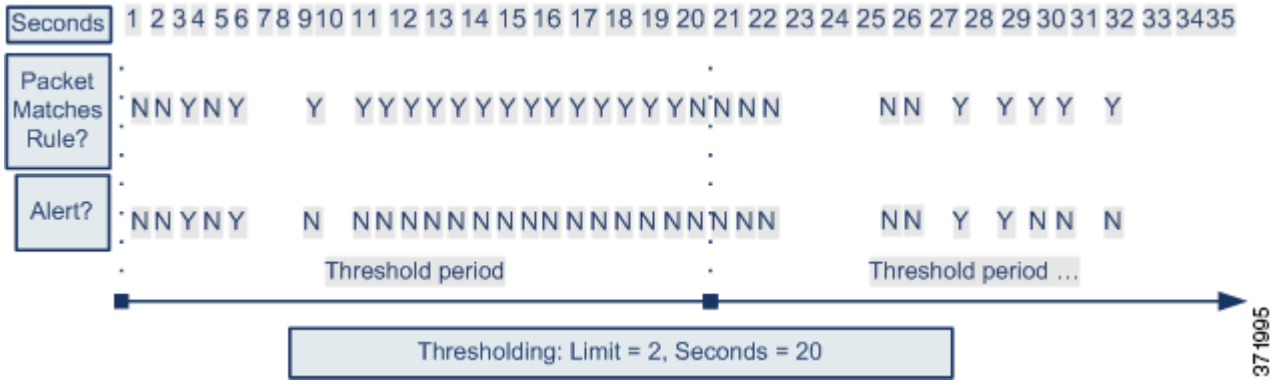
特定のルールで個々のしきい値を設定することにより、このしきい値を上書きすることもできます。たとえば、グローバル制限しきい値を 60 秒ごとに 5 個のイベントに設定してから、SID 1315 について特定のしきい値として 60 秒ごとに 10 個のイベントに設定できます。他のすべてのルールでは 60 秒ごとに 6 個以上のイベントは生成されませんが、SID 1315 ではシステムは 60 秒ごとに最大 10 個のイベントを生成します。

ルール ベースのしきい値の設定の詳細については、イベントしきい値の設定（32-25 ページ）を参照してください。

ヒント 複数の CPU を搭載した管理対象デバイスでグローバルしきい値または個別のしきい値を設定すると、予想より多くのイベントが生成される場合があります。

次の図は、特定のルールに関して攻撃を受けている例を示します。グローバル制限しきい値では、各ルールのイベント生成が、20 秒あたり 2 つのイベントに制限されます。

期間は 1 秒で始まり 21 秒で終わることに注意してください。期間が終了すると、サイクルが再び開始され、次の 2 つのルール一致によってイベントが生成されます。その後、その期間にさらにイベントが生成されることはありません。



しきい値のオプションについて

ライセンス：Protection

しきい値を使用することにより、期間内で特定の数のイベントのみ生成されるようにするか、またはイベントのセットにつき 1 つのイベントが生成されるようにすることにより、侵入イベントの生成を制限できます。グローバルしきい値構成を設定する場合、最初にしきい値構成のタイプを指定する必要があります。以下の表を参照してください。

表 35-1　しきい値設定オプション

オプション	説明
Limit	指定された数のパケット（カウント引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、イベントを記録して表示します。たとえば、タイプを [Limit] に、[Count] を 10 に、[Seconds] を 60 に設定し、14 個のパケットがルールをトリガーとして使用した場合、システムはその 1 分の間に発生した最初の 10 個を表示した後、イベントの記録を停止します。
Threshold	指定された数のパケット（カウント引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、1 つのイベントを記録して表示します。イベントのしきい値カウントに達し、システムがそのイベントを記録した後、時間のカウンタは再び開始されることに注意してください。たとえば、タイプを [Threshold] に、[Count] を 10 に、[Seconds] を 60 に設定して、ルールが 33 秒間で 10 回トリガーされたとします。システムは、1 個のイベントを生成してから、[Seconds] と [Count] のカウンタを 0 にリセットします。次の 25 秒間にルールがさらに 10 回トリガーされたとします。33 秒でカウンタが 0 にリセットされたため、システムが別のイベントを記録します。

表 35-1　しきい値設定オプション（続き）

オプション	説明
両方	指定された数（カウント）のパケットがルールをトリガーとして使用した後で、指定された期間ごとに 1 回イベントを記録して表示します。たとえば、タイプを [Both] に、[Count] を 2 に、[Seconds] を 10 に設定した場合、イベント数は以下のようになります。 • ルールが 10 秒間に 1 回トリガーされた場合、システムはイベントを生成しません（しきい値が満たされていない）。 • ルールが 10 秒間に 2 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回トリガーとして使用した場合、しきい値が満たされるため）。 • ルールが 10 秒間に 4 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回トリガーされると、しきい値が満たされ、以後のイベントは無視されるため）。

次に、イベント インスタンスの数を、送信元 IP アドレスまたは宛先 IP アドレスのどちらに基づいて計算するかを決定する、トラッキングを指定します。最後に、しきい値を定義するインスタンスの数と期間を指定します。

表 35-2　しきい値のインスタンス/時間のオプション

オプション	説明
Count	しきい値を満たすために必要な、トラッキング IP アドレスまたはアドレス範囲ごとの、指定された期間でのイベント インスタンスの数。
Seconds	カウントがリセットされるまでの秒数。しきい値タイプを [Limit] に、トラッキングを [Source] に、[Count] を 10 に、[Seconds] を 10 に設定した場合、特定のソース ポートで 10 秒間に発生した最初の 10 のイベントを記録し表示します。最初の 10 秒で 7 個のイベントだけが発生した場合、システムはそれらを記録して表示します。最初の 10 秒で 40 個のイベントが発生した場合、システムは 10 個を記録して表示し、10 秒経過してからカウントを再度開始します。

グローバルしきい値の設定

ライセンス：Protection

一定の期間に各ルールによって生成されるイベントの数を管理するために、グローバルしきい値を設定できます。グローバルしきい値を設定すると、特定のしきい値を上書きしない各ルールでそのしきい値が適用されます。しきい値の設定の詳細については、しきい値について（35-1 ページ）を参照してください。

デフォルトでは、グローバルしきい値がシステムで設定されます。デフォルト値は次のとおりです。

- **Type** — Limit
- **Track By** — Destination
- **Count** — 1
- **Seconds** — 60

グローバルしきい値の設定方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルにある [Advanced Settings] をクリックします。

[Advanced Settings] ページが表示されます。

ステップ 4　[Intrusion Rule Thresholds] の下の [Global Rule Thresholding] が有効かどうかに応じて、以下の 2 つの選択肢があります。

- 設定が有効な場合、[Edit] をクリックします。
- 設定が無効である場合、[Enabled] をクリックした後で、[Edit] をクリックします。

[Global Rule Thresholding] ページが表示されます。ページ下部のメッセージは、設定を含む侵入ポリシー層を示します。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　[Type] オプション ボタンから、seconds 引数で指定された時間にわたって適用するしきい値のタイプを選択します。詳細については、しきい値設定オプション の表を参照してください。

- カウント引数で指定された制限を超えるまで、ルールをトリガーとして使用したパケットごとにイベントを記録して表示する場合、[Limit] を選択します。
- ルールをトリガーとして使用し、カウント引数で設定されたしきい値と同じかその倍数であるインスタンスを表すパケットごとに 1 つのイベントを記録して表示する場合、[Threshold] を選択します。
- カウント引数によって指定された数のパケットがルールをトリガーとして使用した後に 1 つのイベントを記録して表示する場合、[Both] を選択します。

ステップ 6　[Track By] オプション ボタンからトラッキング方法を選択します。

- 特定の送信元 IP アドレスからのトラフィックでルールの一致を識別するには、[Source] を選択します。
- 特定の宛先 IP アドレスへのトラフィックでルールの一致を識別するには、[Destination] を選択します。

ステップ 7　[Count] フィールド。

- [Limit] しきい値の場合、しきい値を満たすために必要なトラッキング IP アドレスごとの、指定された期間でのイベント インスタンスの数を指定します。
- [Threshold] しきい値の場合、しきい値として使用するルールと一致する数を指定します。

ステップ 8　[Seconds] フィールド。

- [Limit] しきい値の場合、攻撃が追跡される期間の秒数を指定します。
- [Threshold] しきい値の場合、カウントがリセットされるまでの経過時間を秒数で指定します。指定された秒数が経過する前であっても、[Count] フィールドで示されている数のルールが一致すると、カウントはリセットされるのでご注意ください。

ステップ 9　ポリシーの保存、編集の続行、変更の破棄を行うか、またはシステム キャッシュで変更をそのままにしながら終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

グローバルしきい値の無効化

ライセンス：Protection

デフォルトでは、グローバル制限しきい値は、宛先へのトラフィックでのイベントの数を 60 秒あたり 1 個のイベントに制限しています。デフォルトで特定のルールに関するイベントにしきい値を適用し、すべてのルールにしきい値を適用しない場合、最高位のポリシー階層でグローバルしきい値を無効にできます。

グローバルしきい値の無効化：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4　[Intrusion Rule Thresholds] の下で、[Global Rule Thresholding] を無効にします。

ステップ 5　ポリシーの保存、編集の続行、変更の破棄を行うか、またはシステム キャッシュで変更をそのままにしながら終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

CHAPTER 36

侵入ルールの概要と作成

*侵入ルール*は特定のキーワードと引数のセットです。これを使用すると、ネットワーク トラフィックを分析してそれがルール内の基準を満たしているかどうか検査することにより、ネットワークの脆弱性を悪用しようとする試みを検出できます。システムが各ルール内で指定された条件とパケットを照らし合わせます。そして、パケット データとルール内で指定されたすべての条件が一致した場合に、ルールがトリガーとして使用されます。ルールが *アラート ルール*である場合は、侵入イベントが生成されます。*パス ルール*である場合は、トラフィックが無視されます。侵入イベントは、Defense Centerの Web インターフェイスから表示して評価できます。

注意 作成した侵入ルールを実稼働環境で使用する前に、制御されたネットワーク環境で必ずテストしてください。不適切に作成された侵入ルールは、システムのパフォーマンスに重大な影響を与える可能性があります。

次の点に注意してください。

- インライン展開の *ドロップ ルール*では、システムがパケットを破棄してイベントを生成します。廃棄ルールの詳細については、ルール状態の設定（32-22 ページ）を参照してください。
- Cisco提供の侵入ルールには、shared object ruleと標準テキスト ルールの 2 種類があります。Cisco脆弱性調査チーム（VRT）はshared object ruleを使用することで、従来の標準テキスト ルールでは不可能な方法で脆弱性に対する攻撃を検出できます。shared object ruleは作成できません。独自の侵入ルールを作成する場合は、標準テキスト ルールを作成します。

発生する可能性のあるイベントのタイプを調整するために、カスタム標準テキスト ルールを作成することができます。このマニュアルでは特定の exploit の検出を目的とするルールについて説明することもありますが、優秀なルールのほとんどは、特定の既知の exploit ではなく既知の脆弱性を悪用しようとするトラフィックをターゲットとすることに注意してください。ルールを作成してルールのイベント メッセージを指定することにより、攻撃とポリシー回避を示唆するトラフィックをより簡単に識別できます。イベントの評価の詳細については、侵入イベントの操作（41-1 ページ）を参照してください。

留意事項として、カスタム侵入ポリシーでカスタム標準テキスト ルールを有効にする場合、一部のルールのキーワードと引数では、最初に特定の方法でトラフィックをデコードして前処理する必要があります。この章では、前処理を制御するネットワーク分析ポリシーに設定する必要があるオプションについて説明します。注意点として、必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

注　前処理インスペクションと侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは互いに補完する**必要があります**。特に複数のカスタム ネットワーク分析ポリシーを使用した前処理の調整は、**高度な**タスクです。詳細については、カスタム ポリシーの制限（23-13 ページ）を参照してください。

詳細については、次の項を参照してください。

- ルール構造について（36-2 ページ）では、ルール 見出しやルール オプションなど、有効な標準テキスト ルールのコンポーネントについて説明します。
- ルール見出しについて（36-3 ページ）では、ルール 見出しの内容について詳しく説明します。
- ルールでのキーワードと引数について（36-10 ページ）では、FireSIGHT システムで使用可能な侵入ルール キーワードの使い方と構文について説明します。
- ルールの構築（36-109 ページ）では、ルール エディタを使用して新しいルールを作成する方法を説明します。
- ルールの検索（36-114 ページ）では、既存のルールの検索方法について説明します。
- ルール エディタ ページでのルールのフィルタ処理（36-116 ページ）では、特定のルールを見つけやすくするためにルールのサブセットを表示する方法について説明します。

ルール構造について

ライセンス： Protection

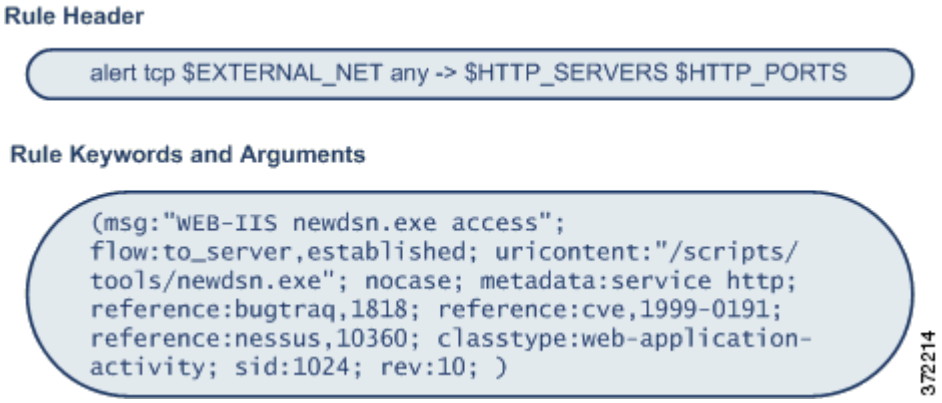
すべての標準テキスト ルールには、ルール 見出しとルール オプションという 2 つの論理セクションが含まれています。ルール 見出しの内容は次のとおりです。

- ルールのアクションまたはタイプ
- プロトコル
- 送信元および宛先の IP アドレスとネットマスク
- 送信元から宛先へのトラフィック フローを示す方向インジケータ
- 送信元ポートと宛先ポート

ルール オプション セクションの内容は次のとおりです。

- イベント メッセージ
- キーワードとそのパラメータおよび引数
- ルールをトリガーとして使用するためにパケットのペイロードが一致しなければならないパターン
- パケットのどの部分をルール エンジンで検査するかの指定

次の図に、ルールの構成要素を示します。

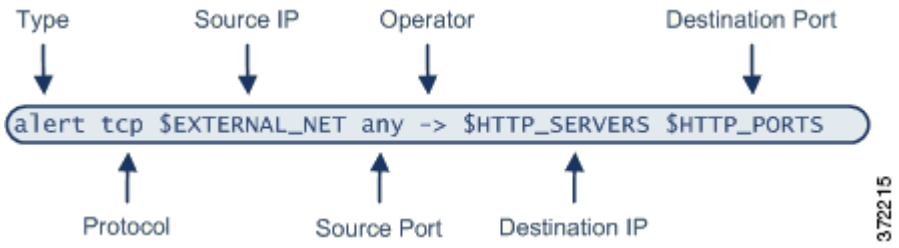


ルールのオプション セクションは、カッコで囲まれたセクションであることに注意してください。ルール エディタは、標準テキスト ルールの作成を支援する使いやすいインターフェイスを備えています。

ルール見出しについて

ライセンス：Protection

それぞれの標準テキスト ルールとshared object ruleには、パラメータと引数からなるルール 見出しが含まれています。ルール 見出しの構成要素を以下に示します。



次の表では、上記のルール 見出しの各部分について説明します。

表 36-1　　ルール 見出しの値

ルール 見出しのコンポーネント	値の例	機能
Action	`alert`	トリガー時に侵入イベントを生成します。
Protocol	`tcp`	TCP トラフィックのみをテストします。
Source IP Address	`$EXTERNAL_NET`	内部ネットワーク上に存在しないホストから送られてきたトラフィックをテストします。
送信元ポート	`any`	発信元ホスト上の任意のポートから送られてきたトラフィックをテストします。
Operator	`->`	(このネットワーク上の Web サーバに向かう)外部トラフィックをテストします。

表 36-1　ルール 見出しの値（続き）

ルール 見出しのコンポーネント	値の例	機能
Destination IP Address	$HTTP_SERVERS	この内部ネットワーク上の Web サーバとして指定された任意のホストに送られるトラフィックをテストします。
宛先ポート	$HTTP_PORTS	この内部ネットワーク上の HTTP ポートに送られるトラフィックをテストします。

注　前述の例では、ほとんどの侵入ルールの場合と同様に、デフォルト変数が使用されています。変数のリスト、機能、および設定方法の詳細については、変数セットの操作（3-19 ページ）を参照してください。

ルール 見出し パラメータの詳細については、以下の項を参照してください。

- ルール アクションの指定（36-4 ページ）では、ルール タイプについて説明し、ルールのトリガー時に実行されるアクションを指定する方法について説明します。
- プロトコルの指定（36-5 ページ）では、ルールによるテスト対象となるトラフィックのトラフィック プロトコルを定義する方法について説明します。
- 侵入ルールでの IP アドレスの指定（36-5 ページ）では、ルール 見出しで個別の IP アドレスと IP アドレス ブロックを定義する方法について説明します。
- 侵入ルールでのポートの定義（36-9 ページ）では、ルール 見出しで個別のポートとポート範囲を定義する方法について説明します。
- 方向の指定（36-10 ページ）では、使用可能な演算子について説明し、ルールでテストすべきトラフィック伝送方向を指定する方法について説明します。

ルール アクションの指定

ライセンス： Protection

各ルール 見出しには、パケットがルールをトリガーとして使用したときにシステムで行われるアクションを指定するパラメータが 1 つ含まれています。アクションが *alert* に設定されたルールは、それをトリガーとして使用したパケットに関する侵入イベントを生成し、そのパケットの詳細をログに記録します。アクションが *pass* に設定されたルールは、それをトリガーとして使用したパケットに関するイベントを生成せず、そのパケットの詳細も記録しません。

注　インライン展開において、ルール状態が [Drop and Generate Events] に設定されたルールは、それをトリガーとして使用したパケットに関する侵入イベントを生成します。また、パッシブ展開で廃棄ルールを適用した場合は、ルールがアラート ルールとして機能します。廃棄ルールの詳細については、ルール状態の設定（32-22 ページ）を参照してください。

デフォルトでは、パス ルールがアラート ルールをオーバーライドします。パス ルールを作成することで、アラート ルールを無効にする代わりに、パス ルールで定義された基準を満たすパケットが特定の状況でアラート ルールをトリガーとして使用しないことを指定できます。たとえば、ユーザ "anonymous" として FTP サーバにログインする試行を検索するルールをアクティ

ブのままにする必要があるとします。ただし、1 つ以上の正式な匿名 FTP サーバがネットワークに存在する場合、そのような特定のサーバで匿名ユーザにより最初のルールがトリガーとして使用されないことを指定するパス ルールを作成し、アクティブにすることができます。

ルール エディタで、[Action] リストからルール タイプを選択します。ルール エディタを使ってルール 見出しを作成する手順の詳細については、ルールの構築（36-109 ページ）を参照してください。

プロトコルの指定

ライセンス：Protection

各ルール 見出しで、ルールにより検査されるトラフィックのプロトコルを指定する必要があります。次のネットワーク プロトコルを分析対象として指定できます。

- ICMP（インターネット制御メッセージ プロトコル）
- IP（インターネット プロトコル）

注 プロトコルが `ip` に設定されている場合、システムは侵入ルール 見出し内のポート定義を無視します。詳細については、侵入ルールでのポートの定義（36-9 ページ）を参照してください。

- TCP（伝送制御プロトコル）
- UDP（ユーザ データグラム プロトコル）

TCP、UDP、ICMP、IGMP など、IANA によって割り当てられたすべてのプロトコルを検査するには、プロトコル タイプとして **IP** を使用します。IANA によって割り当てられたプロトコルの完全なリストについては、http://www.iana.org/assignments/protocol-numbers を参照してください。

注 現在のところ、IP ペイロード内の次の見出し（TCP 見出しなど）でパターンを照合するルールを作成することはできません。代わりに、最後にデコード されたプロトコルからコンテンツ照合が始まります。次善策として、ルール オプションを使用して TCP 見出し内のパターンを照合できます。

ルール エディタで、[Protocol] リストからプロトコル タイプを選択します。ルール エディタを使用してルール 見出しを作成する手順の詳細については、ルールの構築（36-109 ページ）を参照してください。

侵入ルールでの IP アドレスの指定

ライセンス：Protection

パケット検査の対象を、特定の IP アドレスから発信されたパケットまたは特定の IP アドレスに向かうパケットに制限すると、システムが実行しなければならないパケット検査の量が減ります。さらに、ルールをより具体化し、送信元および宛先 IP アドレスが疑わしい動作を示していないパケットに対してルールがトリガーとして使用される可能性をなくすと、誤検出も減ります。

ヒント システムは IP アドレスのみを認識し、送信元/宛先 IP アドレスのホスト名を受け入れません。

ルール エディタの [Source IPs] フィールドと [Destination IPs] フィールドで、送信元および宛先の IP アドレスを指定します。ルール エディタを使用してルール 見出しを作成する手順の詳細については、ルールの構築（36-109 ページ）を参照してください。

標準テキスト ルールの作成時には、必要に応じて、さまざまな方法で IPv4 アドレスと IPv6 アドレスを指定できます。単一の IP アドレス、any（オプション）、IP アドレス リスト、CIDR 表記、プレフィクス長、ネットワーク変数、またはネットワーク オブジェクトあるいはネットワーク オブジェクト グループを指定できます。加えて、1 つの特定の IP アドレスまたは複数 IP アドレスのセットを除外するうよう指定できます。IPv6 アドレスを指定するときには、RFC 4291 で定義された任意のアドレス指定規則を使用できます。

次の表では、送信元 IP アドレスと宛先 IP アドレスを指定するさまざまな方法を要約します。

表 36-2　送信元/宛先 IP アドレスの構文

指定する項目	使用するフィルタ	例
任意の IP アドレス	`any`	`any`
1 つの特定の IP アドレス	その IP アドレス 同じルール内に IPv4 と IPv6 の送信元アドレスと宛先アドレスを混在させないでください。	`192.168.1.1` `2001:db8::abcd`
IP アドレスのリスト	複数の IP アドレスをカンマで区切り、それを大カッコ（`[]`）で囲む	`[192.168.1.1,192.168.1.15]` `[2001:db8::b3ff, 2001:db8::0202]`
IP アドレスのブロック	IPv4 CIDR ブロックまたは IPv6 アドレス プレフィクス表記	`192.168.1.0/24` `2001:db8::/32`
特定の 1 つの IP アドレスまたはアドレス セットを除くすべて	拒否する IP アドレスの前に付ける「`!`」記号	`!192.168.1.15` `!2001:db8::0202:b3ff:fe1e`
特定の 1 つ以上の IP アドレスを除く、IP アドレス ブロック内のすべて	アドレス ブロックの後に、否定されるアドレスのリストまたはブロック	`[10.0.0/8, !10.2.3.4, !10.1.0.0/16]` `[2001:db8::/32, !2001:db8::8329, !2001:db8::0202]`
ネットワーク変数で定義された IP アドレス	`$` で始まる大文字の変数名 プリプロセッサ ルールは、侵入ルールで使われているネットワーク変数で定義されたホストとは無関係に、イベントをトリガーできることに注意してください。詳細については、「変数セットの操作（3-19 ページ）」を参照してください。	`$HOME_NET`
IP アドレス変数で定義されたアドレスを除く、すべての IP アドレス	大文字の変数名の前に `!$` を付ける 詳細については、「侵入ルールにおける IP アドレスの除外（36-8 ページ）」を参照してください。	`!$HOME_NET`
ネットワーク オブジェクトまたはネットワーク オブジェクト グループで定義された IP アドレス	`!{object_name}` という形式でオブジェクト名またはグループ名を指定する。 詳細については、「ネットワーク オブジェクトの操作（3-4 ページ）」を参照してください。	`${192.168sub16}`
ネットワーク オブジェクトまたはネットワーク オブジェクト グループで定義されたアドレスを除く、すべての IP アドレス	オブジェクト名またはグループ名を中カッコ（`{}`）で囲み、その前に `!$` を付ける。 詳細については、「ネットワーク オブジェクトの操作（3-4 ページ）」を参照してください。	`!${192.168sub16}`

送信元や宛先の IP アドレスの指定に使用できる構文の詳細、および変数を使って IP アドレスを指定する方法については、以下の項を参照してください。

- IP アドレスの表記規則（1-23 ページ）。
- 変数セットの操作（3-19 ページ）
- 任意の IP アドレスの指定（36-7 ページ）
- 複数の IP アドレスの指定（36-7 ページ）
- ネットワーク オブジェクトの指定（36-8 ページ）
- 侵入ルールにおける IP アドレスの除外（36-8 ページ）

任意の IP アドレスの指定

ライセンス： Protection

任意の IPv4 または IPv6 アドレスを示す「any」という単語を、ルールの送信元 IP アドレスまたは宛先 IP アドレスとして指定できます。

たとえば、次のルールでは [Source IPs] フィールドと [Destination IPs] フィールドで引数 **any** を使用して、任意の IPv4 または IPv6 の送信元または宛先アドレスを持つパケットを評価します。

```
alert tcp any any -> any any
```

また、任意の IPv6 アドレスを示すために :: を指定することもできます。

複数の IP アドレスの指定

ライセンス： Protection

次の例に示すように、複数の IP アドレスをカンマで区切ることで、個別の IP アドレスを列挙できます。必要に応じて、非拒否リストを大カッコで囲むこともできます。

```
[192.168.1.100,192.168.1.103,192.168.1.105]
```

IPv4 アドレスと IPv6 アドレスのいずれかだけを列挙することも、任意に組み合わせて列挙することもできます（次の例を参照）。

```
[192.168.1.100,2001:db8::1234,192.168.1.105]
```

以前のソフトウェア リリースでは IP アドレス リストを大カッコで囲む必要がありましたが、現在ではこれが必須でないことに注意してください。また、オプションで、リストを入力するときに各カンマの前または後にスペースを含めることができます。

注　否定リストは、大カッコで囲む必要があります。詳細については、「侵入ルールにおける IP アドレスの除外（36-8 ページ）」を参照してください。

また、IPv4 クラスレス ドメイン間ルーティング（CIDR）表記または IPv6 プレフィクス長を使用して、アドレス ブロックを指定することもできます。次に例を示します。

- 192.168.1.0/24 は、サブネット マスク 255.255.255.0 の 192.168.1.0 ネットワーク内の IPv4 アドレス、つまり 192.168.1.0 ～ 192.168.1.255 を指定します。詳細については、IP アドレスの表記規則（1-23 ページ）を参照してください。
- 2001:db8::/32 は、プレフィクス長 32 ビットの 2001:db8:: ネットワーク内の IPv6 アドレス、つまり 2001:db8:: ～ 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff を指定します。

ヒント IP アドレスのブロックを指定する必要があるが、CIDR またはプレフィクス長表記を単独で使ってそれを表現できない場合は、1 つの IP アドレス リスト内でいくつかの CIDR ブロックとプレフィクス長を使用できます。

ネットワーク オブジェクトの指定

ライセンス： Protection

次の構文を使用して、ネットワーク オブジェクトまたはネットワーク オブジェクト グループを指定できます。

```
${object_name | group_name}
```

値は次のとおりです。

- *object_name* はネットワーク オブジェクトの名前です
- *group_name* はネットワーク オブジェクト グループの名前です

ネットワーク オブジェクトとネットワーク オブジェクト グループの作成方法については、ネットワーク オブジェクトの操作（3-4 ページ）を参照してください。

`192.168sub16` という名前のネットワーク オブジェクトと `all_subnets` という名前のネットワーク オブジェクト グループをすでに作成済みであるとします。ネットワーク オブジェクトを使用して IP アドレスを特定するには、たとえば次のように指定できます。

```
${192.168sub16}
```

ネットワーク オブジェクト グループを使用するには、次のように指定できます。

```
${all_subnets}
```

さらに、ネットワーク オブジェクトとネットワーク オブジェクト グループで否定を使用することもできます。次に例を示します。

```
!${192.168sub16}
```

詳細については、「侵入ルールにおける IP アドレスの除外（36-8 ページ）」を参照してください。

侵入ルールにおける IP アドレスの除外

ライセンス： Protection

特定の IP アドレスを否定するために感嘆符（`!`）を使用できます。つまり、1 つ以上の特定の IP アドレスを除く、すべての IP アドレスに一致させることができます。たとえば、`!192.168.1.1` は 192.168.1.1 以外の任意の IP アドレスを、`!2001:db8:ca2e::fa4c` は 2001:db8:ca2e::fa4c 以外の任意の IP アドレスを指定します。

一連の IP アドレスを拒否するには、大かっこで囲んだ IP アドレスのリストの前に「`!`」記号を付けます。たとえば、`![192.168.1.1,192.168.1.5]` は 192.168.1.1 と 192.168.1.5 を除くすべての IP アドレスを定義します。

注 IP アドレスのリストを否定するには、大カッコを使用する必要があります。

否定文字と一緒に IP アドレス リストを使用する場合は注意が必要です。たとえば、192.168.1.1 と 192.168.1.5 を除くすべてのアドレスと一致させるために `[!192.168.1.1,!192.168.1.5]` を使用した場合、システムはこの構文を「192.168.1.1 以外のすべて、**または** 192.168.1.5 以外のすべて」と解釈します。

192.168.1.5 は 192.168.1.1 ではなく、192.168.1.1 は 192.168.1.5 ではないため、この両方の IP アドレスが `[!192.168.1.1,!192.168.1.5]` という IP アドレス値に一致します。つまり、実質的に「`any`」を使用するのと同じです。

代わりに `![192.168.1.1,192.168.1.5]` を使用してください。システムはこの構文を「192.168.1.1 **でなく、しかも** 192.168.1.5 **でない**」と解釈し、大カッコ内に列挙されたものを除くすべての IP アドレスに一致します。

論理的に言って、`any` と一緒に否定を使用できないことに注意してください。any を否定すると「アドレスなし」を意味することになります。

侵入ルールでのポートの定義

ライセンス： Protection

ルール エディタの [Source Port] フィールドと [Destination Port] フィールドで、送信元および宛先ポートを指定します。ルール エディタを使用してルール 見出しを作成する手順の詳細については、ルールの構築（36-109 ページ）を参照してください。

ルール 見出し内で使われるポート番号を定義するために、FireSIGHT システムは特殊なタイプの構文を使用します。

注　プロトコルが `ip` に設定されている場合、システムは侵入ルール 見出し内のポート定義を無視します。詳細については、プロトコルの指定（36-5 ページ）を参照してください。

次の例に示すように、カンマでポートを区切ることによって、ポートのリストを指定できます。

```
80, 8080, 8138, 8600-9000, !8650-8675
```

オプションで、次の例に示すように、ポート リストを大カッコで囲むこともできます（以前のソフトウェア バージョンではこれが必須でしたが、現在は必須ではありません）。

```
[80, 8080, 8138, 8600-9000, !8650-8675]
```

なお、次の例に示すように、ポート リストの否定を大カッコで囲む**必要がある**ことに注意してください。

```
![20, 22, 23]
```

また、侵入ルール内の送信元ポートや宛先ポートのリストには最大で 64 文字を含めることができます。

次の表に、使用可能な構文を要約します。

表 36-3　送信元/宛先ポートの構文

指定する項目	使用目的	例
任意のポート	`any`	`any`
1 つの特定のポート	そのポート番号	`80`
ポートの範囲	範囲内の最初のポート番号と最後のポート番号をダッシュでつなぐ	`80-443`
1 つの特定のポートに等しい、またはより小さいすべてのポート	ポート番号の前にダッシュを付ける	`-21`
1 つの特定のポートに等しい、またはより大きいすべてのポート	ポート番号の後ろにダッシュを付ける	`80-`

表 36-3　送信元/宛先ポートの構文（続き）

指定する項目	使用目的	例
1 つの特定のポートまたはポート範囲を除く、すべてのポート	拒否するポート、ポート リスト、またはポート範囲の前に「!」記号を付ける 論理的に言って、*any* を除くすべてのポート指定と一緒に否定を使用できます。any を否定すると「*アドレスなし*」を意味することに注意してください。	`!20`
ポート変数で定義されるすべてのポート	大文字の変数名の前に、`!$` を付ける 詳細については、「ポート変数の操作（3-33 ページ）」を参照してください。	`$HTTP_PORTS`
ポート変数で定義されるポートを除く、すべてのポート	大文字の変数名の前に `!$` を付ける	`!$HTTP_PORTS`

方向の指定

ライセンス：Protection

ルールによる検査対象となるパケットが進むべき方向を、ルール 見出し内で指定できます。このオプションについて、次の表で説明します。

表 36-4　ルール 見出し内の方向オプション

使用するフィルタ	テスト対象
指向性	指定された送信元 IP アドレスから指定された宛先 IP アドレスに向かうトラフィックのみ
双方向	指定された送信元 IP アドレスと宛先 IP アドレスの間を移動するすべてのトラフィック

ルール エディタを使用してルール 見出しを作成する手順の詳細については、ルールの構築（36-109 ページ）を参照してください。

ルールでのキーワードと引数について

ライセンス：Protection

ルール言語では、キーワードを組み合わせることによってルールの動作を指定できます。キーワードとそれに関連する値（*引数*と呼ばれる）を使用して、ルール エンジンで検査されるパケットやパケット関連値をシステムが評価する方法を指定します。FireSIGHT システムでは現在、コンテンツ マッチング、プロトコル固有のパターン マッチング、状態固有のマッチングなど、インスペクション機能を実行するためのキーワードがサポートされています。キーワードあたり最大 100 個の引数を定義し、互換性のある任意の数のキーワードを組み合わせて非常に具体的なルールを作成できます。これにより、誤検出や検出漏れの可能性が減少し、受け取った侵入情報に集中的に取り組むことができます。

また、適応型プロファイルを使用すると、ルール メタデータとホスト情報に基づいて特定のパケットに対するアクティブ ルール処理を動的に調整できます。詳細については、パッシブ展開における前処理の調整（30-1 ページ）を参照してください。

詳細については、次の項を参照してください。

- 侵入イベント詳細の定義（36-12 ページ）では、イベントのメッセージ、プライオリティ情報、およびルールで検出された exploit に関する外部情報への参照を定義するためのキーワードの構文と使用法について説明します。
- コンテンツ一致の検索（36-16 ページ）では、content または protected_content キーワードを使用して、パケット ペイロードのコンテンツを検査する方法について説明します。
- コンテンツ一致の制約（36-19 ページ）では、content または protected_content キーワードを変更するキーワードの使用方法について説明します。
- インライン展開でのコンテンツの置換（36-32 ページ）では、インライン展開で replace キーワードを使用して、長さの等しい指定されたコンテンツを置き換える方法について説明します。
- Byte_Jump と Byte_Test の使用（36-33 ページ）では、byte_jump キーワードと byte_test キーワードを使用して、パケット内のどの位置でルール エンジンがコンテンツ マッチング検査を開始すべきか、どのバイトを評価すべきかについて計算する方法を説明します。
- PCRE を使用したコンテンツの検索（36-38 ページ）では、pcre キーワードを使用して、ルール内で Perl 互換の正規表現を使用する方法について説明します。
- ルールにメタデータを追加する（36-45 ページ）では、metadata キーワードを使用して、ルールに情報を追加する方法について説明します。
- IP 見出し値の検査（36-49 ページ）では、パケットの IP 見出し内の値を検査するキーワードの構文と使用法について説明します。
- ICMP 見出し値の検査（36-52 ページ）では、パケットの ICMP 見出し内の値を検査するキーワードの構文と使用法について説明します。
- TCP 見出し値とストリーム サイズの検査（36-54 ページ）では、パケットの TCP 見出し内の値を検査するキーワードの構文と使用法について説明します。
- TCP ストリーム再構築の有効化と無効化（36-58 ページ）では、接続での検査対象トラフィックがルールの条件と一致した場合に、単一接続のストリーム再構築を有効/無効にする方法について説明します。
- セッションからの SSL 情報の抽出（36-59 ページ）では、暗号化されたトラフィックからバージョン情報と状態情報を抽出するキーワードの使用法と構文について説明します。
- パケット データをキーワード引数の中に読み込む（36-88 ページ）では、パケットから変数の中に値を読み込み、あとでそれを同じルール内で使用することにより、その値を特定の他のキーワードの引数として指定する方法を説明します。
- アプリケーション層プロトコル値の検査（36-61 ページ）では、アプリケーション層プロトコル プロパティを検査するキーワードの使用法と構文について説明します。
- パケット特性の検査（36-85 ページ）では、dsize、sameIP、isdataat、fragoffset および cvs キーワードの使用法と構文について説明します。
- ルール キーワードを使用したアクティブ応答の開始（36-90 ページ）では、resp キーワードを使用して TCP 接続または UDP セッションをアクティブに（能動的に）閉じる方法、react キーワードを使用して HTML ページを送信した後で TCP 接続をアクティブに閉じる方法、および config response コマンドを使用してアクティブ応答インターフェイスとパッシブ展開での TCP リセット試行回数を指定する方法について説明します。
- イベントのフィルタリング（36-94 ページ）では、指定された時間内に指定されたパケット数がルールの検出基準を満たさない限り、ルールでイベントがトリガーとして使用されないようにする方法を説明します。

- 攻撃後トラフィックの評価（36-95 ページ）では、ホストまたはセッションに関する追加のトラフィックをログに記録する方法について説明します。
- 複数のパケットに及ぶ攻撃の検出（36-96 ページ）では、単一セッション内の複数パケットに及ぶ攻撃からパケットに状態名を割り当てた後、その状態に応じてパケットを分析および警告する方法について説明します。
- HTTP エンコードのタイプと位置によるイベントの生成（36-102 ページ）では、正規化の前に、HTTP 要求や応答 URI、ヘッダー、または（set-cookie を含む）cookie 内のエンコード タイプに基づいてイベントを生成する方法について説明します。
- ファイル タイプとバージョンの検出（36-103 ページ）では、`file_type` キーワードまたは `file_group` キーワードを使用して、特定のファイル タイプまたはファイル バージョンを指し示す方法について説明します。
- 特定のペイロード タイプを指し示す（36-105 ページ）では、HTTP 応答エンティティ本体、SMTP ペイロード、またはエンコードされた電子メール添付ファイルの先頭を指し示す方法について説明します。
- パケット ペイロードの先頭を指し示す（36-107 ページ）では、パケット ペイロードの先頭を指し示す方法について説明します。
- Base64 データのデコードと検査（36-107 ページ）では、`base64_decode` キーワードと `base64_data` キーワードを使用して、特に HTTP 要求内の Base64 データをデコードして検査する方法について説明します。

侵入イベント詳細の定義

ライセンス： Protection

標準テキスト ルールを作成するときには、ルールで攻撃試行を検出する対象となる脆弱性についてのコンテキスト情報を含めることができます。また、脆弱性データベースへの外部参照を含めたり、組織内でイベントに設定するプライオリティを定義したりすることもできます。アナリストがイベントを認識すると、そのプライオリティ、exploit、および既知の対策についての情報をすぐに入手できます。

イベント関連のキーワードの詳細については、以下の項を参照してください。

- イベント メッセージの定義（36-12 ページ）
- イベント プライオリティの定義（36-13 ページ）
- 侵入イベント分類の定義（36-13 ページ）
- イベント参照の定義（36-15 ページ）

イベント メッセージの定義

ライセンス： Protection

ルールのトリガー時にメッセージとして表示される、意味のあるテキストを指定できます。メッセージを読むと、ルールで攻撃試行を検出する対象となった脆弱性の特性をすぐに理解できます。中カッコ（`{}`）を除く、印字可能な任意の標準 ASCII 文字を使用できます。システムは、メッセージ全体を囲んでいる引用符を取り除きます。

ヒント　ルール メッセージの指定は必須です。また、空白文字のみ、1 つ以上の引用符のみ、1 つ以上のアポストロフィのみ、あるいは空白文字/引用符/アポストロフィだけの組み合わせでメッセージを構成することはできません。

ルール エディタでイベント メッセージを定義するには、[Message] フィールドにイベント メッセージを入力します。ルール エディタを使用してルールを作成する方法については、ルールの構築（36-109 ページ）を参照してください。

イベント プライオリティの定義

ライセンス： Protection

デフォルトでは、ルールのイベント分類からルールのプライオリティが派生します。ただし、`priority` キーワードをルールに追加すると、ルールの分類プライオリティをオーバーライドできます。

ルール エディタを使ってプライオリティを指定するには、[Detection Options] リストから [priority] を選択して、ドロップダウン リストから [high]、[medium]、または [low] を選択します。たとえば、Web アプリケーション攻撃を検出するルールに **high** プライオリティを割り当てるには、`priority` キーワードをルールに追加して、プライオリティとして **high** を選択します。ルール エディタを使用してルールを作成する方法については、ルールの構築（36-109 ページ）を参照してください。

侵入イベント分類の定義

ライセンス： Protection

ルールごとに、イベントのパケット表示に含める攻撃分類を指定できます。次の表に、それぞれの分類の名前と番号を示します。

表 36-5　ルール分類

番号	分類名	説明
1	not-suspicious	不審ではないトラフィック
2	unknown	不明なトラフィック
3	bad-unknown	有害な可能性のあるトラフィック
4	attempted-recon	情報漏えいが試行された
5	successful-recon-limited	情報漏えいが発生
6	successful-recon-largescale	大規模な情報漏えい
7	attempted-dos	サービス拒否が試行された
8	successful-dos	サービス拒否が発生
9	attempted-user	ユーザ特権の獲得が試行された
10	unsuccessful-user	ユーザ特権の獲得が失敗した
11	successful-user	ユーザ特権の獲得に成功
12	attempted-admin	管理者特権の獲得が試行された
13	successful-admin	管理者特権の獲得に成功

表 36-5　ルール分類（続き）

番号	分類名	説明
14	rpc-portmap-decode	RPC クエリのデコード
15	shellcode-detect	実行可能コードが検出された
16	string-detect	疑わしい文字列が検出された
17	suspicious-filename-detect	疑わしいファイル名が検出された
18	suspicious-login	疑わしいユーザ名を使用したログイン試行が検出された
19	system-call-detect	システム コールが検出された
20	tcp-connection	TCP 接続が検出された
21	trojan-activity	ネットワーク トロイの木馬が検出された
22	unusual-client-port-connection	通常とは異なるポートをクライアントが使用していた
23	network-scan	ネットワーク スキャンの検出
24	denial-of-service	サービス拒否攻撃の検出
25	non-standard-protocol	非標準プロトコルまたはイベントの検出
26	protocol-command-decode	一般的なプロトコル コマンド デコード
27	web-application-activity	脆弱な可能性のある Web アプリケーションへのアクセス
28	web-application-attack	Web アプリケーション攻撃
29	misc-activity	その他のアクティビティ
30	misc-attack	その他の攻撃
31	icmp-event	一般的な ICMP イベント
32	inappropriate-content	不適切な内容が検出された
33	policy-violation	企業プライバシー侵害の可能性
34	default-login-attempt	デフォルトのユーザ名とパスワードによるログイン試行
35	sdf	機密データ
36	malware-cnc	既知のマルウェア コマンドと制御トラフィック
37	client-side-exploit	既知のクライアント側 exploit 試行
38	file-format	既知の有害ファイルまたはファイル ベースの exploit

ルール エディタで分類を指定するには、[Classification] リストから分類を 1 つ選択します。ルール エディタの詳細については、新しいルールの作成（36-109 ページ）を参照してください。

カスタム分類の追加

ライセンス：Protection

定義したルールによって生成されるイベントのパケット表示記述の内容をもっとカスタマイズする必要がある場合には、カスタム分類を作成します。

分類リストに分類を追加する方法:

アクセス: Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Rule Editor] の順に選択します。

[Rule Editor] ページが表示されます。

ステップ 2　[Create Rule] をクリックします。

[Create Rule] ページが表示されます。

ステップ 3　[Classification] ドロップダウン リストで、[Edit Classifications] をクリックします。

ポップアップ ウィンドウが表示されます。

ステップ 4　[Classification Name] フィールドに分類の名前を入力します。

最大で 255 文字の英数字を使用できますが、40 文字を超えるとページが読みにくくなります。<>()\'"&$; 文字および空白文字はサポートされていません。

ステップ 5　[Classification Description] フィールドに、分類の説明を入力します。

最大で 255 文字の英数字とスペースを使用できます。<>()\'"&$; 文字はサポートされていません。

ステップ 6　[Priority] リストからプライオリティを選択します。

[high]、[medium]、または [low] を選択できます。

ステップ 7　[Add] をクリックします。

新しい分類がリストに追加され、ルール エディタで使用できるようになります。

ステップ 8　[Done] をクリックします。

イベント参照の定義

ライセンス: Protection

`reference` キーワードを使用すると、イベントに関する外部 Web サイトや追加情報への参照を追加できます。参照を追加すると、アナリストは参照情報をすぐに利用できるため、パケットがルールをトリガーとして使用した理由を特定するのに役立ちます。次の表に、既知の exploit や攻撃についてのデータを提供する外部システムをいくつか示します。

表 36-6　外部攻撃識別システム

System ID	説明	ID の例
bugtraq	Bugtraq ページ	8550
cve	一般的な脆弱性および脅威のページ	CAN-2003-0702
mcafee	McAfee ページ	98574
url	Web サイト参照	www.example.com?exploit=14
msb	Microsoft セキュリティ情報	MS11-082

表 36-6　外部攻撃識別システム（続き）

System ID	説明	ID の例
nessus	Nessus ページ	10039
secure-url	セキュア Web サイト参照（https://...）	intranet/exploits/exploit=14 任意のセキュア Web サイトで secure-url を使用できることに注意してください。

ルール エディタを使用して参照を指定するには、[Detection Options] リストから [reference] を選択し、対応するフィールドに次のように値を入力します。

```
id_system,id
```

ここで、*id_system* はプレフィクスとして使用されるシステム、*id* は Bugtraq ID、CVE 番号、Arachnids ID、または URL（http:// なし）です。

たとえば、Bugtraq ID 17134 に記載されている Microsoft Commerce Server 2002 サーバ上の認証バイパス脆弱性を指定するには、**reference** フィールドに次のように入力します。

```
bugtraq,17134
```

参照をルールに追加するときには、次の点に注意してください。

- カンマの後ろにスペースを入力しないでください。
- システム ID に大文字を使用しないでください。

ルール エディタを使用してルールを作成する方法については、ルールの構築（36-109 ページ）を参照してください。

コンテンツ一致の検索

ライセンス：Protection

content キーワードまたは protected_content キーワードを使用すると、パケット内から検出するコンテンツを指定できます。詳細については、次の項を参照してください。

- content キーワードの使用（36-16 ページ）
- protected_content キーワードの使用（36-17 ページ）
- コンテンツ マッチングの設定（36-17 ページ）

content キーワードの使用

content キーワードを使用すると、ルール エンジンはパケット ペイロードまたはストリームでその文字列を検索します。たとえば、いずれかの content キーワードの値として /bin/sh と入力した場合、ルール エンジンはパケット ペイロード内で文字列 /bin/sh を検索します。

ASCII 文字列、16 進コンテンツ（バイナリ バイト コード）、またはその両方の組み合わせを使用してコンテンツを照合できます。キーワード値の中で 16 進コンテンツをパイプ文字（|）で囲みます。たとえば、|90C8 C0FF FFFF|/bin/sh のように 16 進コンテンツと ASCII コンテンツを混在させることができます。

1 つのルール内で複数のコンテンツ マッチングを指定できます。これを行うには、content キーワードの追加のインスタンスを使用します。コンテンツ マッチングごとに、ルールをトリガーとして使用させるにはパケット ペイロードまたはストリームでコンテンツ一致が見つからなければならないことを指定できます。

protected_content キーワードの使用

protected_content キーワードを使用すると、ルール引数を設定する前に、検索コンテンツ文字列をエンコードすることができます。キーワードを設定する前に、ルール作成者がハッシュ関数（SHA512、SHA256、または MD5）を使用して文字列をエンコードします。

content キーワードの代わりに protected_content キーワードを使用した場合でも、ルール エンジンがパケット ペイロードまたはストリームの中で文字列を検索する方法に違いはなく、ほとんどのキーワード オプションが想定どおりに機能します。次の表は、protected_content キーワード オプションと content キーワード オプションの間の例外的な相違点を要約しています。

表 36-7　protected_content オプションの例外

オプション	説明
Hash Type	protected_content ルール キーワードの新しいオプション。詳細については、Hash Type（36-20 ページ）を参照してください。
Case Insensitive	サポート対象外
Within	サポート対象外
奥行	サポート対象外
長さ	protected_content ルール キーワードの新しいオプション。詳細については、Length（36-23 ページ）を参照してください。
Use Fast Pattern Matcher	サポート対象外
Fast Pattern Matcher Only	サポート対象外
Fast Pattern Matcher Offset and Length	サポート対象外

Ciscoでは、protected_content キーワードを含むルールに 1 つ以上の content キーワードを含めることを推奨しています。こうすると、ルール エンジンが常に高速パターン マッチ機能を使用することで処理速度が上がり、パフォーマンスが向上します。ルール内の protected_content キーワードの前に content キーワードを配置します。ルールに 1 つ以上の content キーワードが含まれている場合は、content キーワードの Use Fast Pattern Matcher 引数が有効になっているかどうかに関係なく、ルール エンジンが高速パターン マッチ機能を使用することに注意してください。

コンテンツ マッチングの設定

ほとんどの場合、content または protected_content キーワードの後ろに修飾子を付けて、コンテンツを検索すべき場所、検索で大文字/小文字を区別するかどうか、およびその他のオプションを指定する必要があります。content および protected_content キーワードの修飾子の詳細については、コンテンツ一致の制約を参照してください。

ルールでイベントがトリガーとして使用されるためには、すべてのコンテンツ マッチングが真でなければならないことに注意してください。つまり、各コンテンツ マッチングは相互に AND 関係にあります。

また、インライン展開では、有害なコンテンツを照合した後でそれを同じ長さの独自のテキスト文字列に置き換えるルールをセットアップできることにも注意してください。詳細については、「インライン展開でのコンテンツの置換（36-32 ページ）」を参照してください。

照合するコンテンツを入力する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[content] フィールドに、検索する内容を入力します（たとえば `|90C8 C0FF FFFF|/bin/sh`）。

指定したコンテンツ**以外の**コンテンツを検索するには、[Not] チェック ボックスをオンにします。

注意　**Not** オプションが選択された 1 つの `content` キーワードだけを含むルールを作成した場合、侵入ポリシーの効果がなくなる可能性があります。詳細については、Not（36-21 ページ）を参照してください。

ステップ 2　オプションで、`content` キーワードを変更したり、キーワードの制約を追加したりするキーワードを追加します。他のキーワードの詳細については、ルールでのキーワードと引数について（36-10 ページ）を参照してください。

`content` キーワードの制約の詳細については、コンテンツ一致の制約（36-19 ページ）を参照してください。

ステップ 3　ルールの作成または編集を続けます。

詳細については、新しいルールの作成（36-109 ページ）または既存のルールの変更（36-111 ページ）を参照してください。

照合する保護されたコンテンツを入力する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　SHA512、SHA256、または MD5 ハッシュ ジェネレータを使用して、検索するコンテンツをエンコードします（たとえば、SHA512 ハッシュ ジェネレータを使って文字列 `Sample1` を実行します）。

ジェネレータが文字列のハッシュを出力します。

ステップ 2　protected_content フィールドに、ステップ 1 で生成したハッシュを入力します（たとえば `B20AABAF59605118593404BD42FE69BD8D6506EE7F1A71CE6BB470B1DF848C814BC5DBEC2081999F15691A71FAECA5FBA4A3F8B8AB56B7F04585DA6D73E5DD15`）。

指定したコンテンツ**以外の**コンテンツを検索するには、[Not] チェック ボックスをオンにします。

注意　**Not** オプションが選択された 1 つの `protected_content` キーワードだけを含むルールを作成した場合、侵入ポリシーの効果がなくなる可能性があります。詳細については、Not（36-21 ページ）を参照してください。

ステップ 3　[Hash Type] ドロップダウン リストから、ステップ 1 で使用したハッシュ関数（**SHA512** など）を選択します。なお、ステップ 2 で入力されたハッシュ内のビット数がハッシュ タイプと一致する**必要があります**。一致しない場合、システムはルールを保存しません。詳細については、Hash Type（36-20 ページ）を参照してください。

ヒント　Cisco設定の [Default] を選択した場合、システムはハッシュ関数として SHA512 を想定します。

ステップ 4　必須の [Length] フィールドに値を入力します。この値は、元の（ハッシュされていない）検索文字列の長さと一致している**必要があります**（たとえば、ステップ 2 の文字列 `Sample1` の長さは `7` です）。

詳細については、Length（36-23 ページ）を参照してください。

ステップ 5　[Offset] フィールドまたは [Distance] フィールドに値を入力します。1 つのキーワード設定内に [Offset] オプションと [Distance] オプションを混在させることはできません。

詳細については、protected_content キーワードでの検索位置オプションの使用（36-24 ページ）を参照してください。

ステップ 6　オプションで、`protected_content` キーワードを変更する制約オプションを追加します。

詳細については、コンテンツ一致の制約（36-19 ページ）を参照してください。

ステップ 7　オプションで、`protected_content` キーワードを変更する追加のキーワードを指定します。

詳細については、ルールでのキーワードと引数について（36-10 ページ）を参照してください。

ステップ 8　ルールの作成または編集を続けます。

詳細については、新しいルールの作成（36-109 ページ）または既存のルールの変更（36-111 ページ）を参照してください。

コンテンツ一致の制約

ライセンス：Protection

`content` または `protected_content` キーワードを変更するパラメータを使用すると、コンテンツ検索の位置や大文字/小文字の区別を制約できます。`content` または `protected_content` キーワードを変更するオプションを設定して、検索するコンテンツを指定します。

詳細については、次の項を参照してください。

- Case Insensitive（36-19 ページ）
- Hash Type（36-20 ページ）
- raw データ（36-20 ページ）
- Not（36-21 ページ）
- 検索位置オプション（36-22 ページ）
- HTTP コンテンツ オプション（36-25 ページ）
- Use Fast Pattern Matcher（36-29 ページ）

Case Insensitive

ライセンス：Protection

注　このオプションは `protected_content` キーワードの設定では**サポートされません**。詳細については、protected_content キーワードの使用（36-17 ページ）を参照してください。

ASCII 文字列でコンテンツ一致を検索するときに大文字/小文字の区別を無視するようルール エンジンに指示できます。検索で大文字/小文字を区別しないようにするには、コンテンツ検索を指定するときに [Case Insensitive] をオンにします。

コンテンツ検索時に [Case Insensitive] を指定する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　追加する `content` キーワードに関して [Case Insensitive] を選択します。

ステップ 2　ルールの作成または編集を続けます。

詳細については、コンテンツ一致の制約、コンテンツ一致の検索（36-16 ページ）、新しいルールの作成（36-109 ページ）、または既存のルールの変更（36-111 ページ）を参照してください。

Hash Type

ライセンス：Protection

注　このオプションは `protected_content` キーワードで**のみ**設定できます。詳細については、protected_content キーワードの使用（36-17 ページ）を参照してください。

[Hash Type] ドロップダウンを使用して、検索文字列のエンコードに使用されたハッシュ関数を特定します。システムは、`protected_content` 検索文字列のハッシュ方式として SHA512、SHA256、および MD5 をサポートしています。選択したハッシュ タイプとハッシュされたコンテンツの長さが一致しない場合、システムはルールを**保存しません**。

システムは自動的に、Cisco設定のデフォルト値を選択します。[Default] を選択した場合、ルールには特定のハッシュ関数が含まれず、システムはハッシュ関数として SHA512 を想定します。

保護されたコンテンツ検索の実行時にハッシュ関数を指定する方法：

ステップ 1　[Hash Type] ドロップダウン リストから、追加する `protected_content` キーワードのハッシュとして [Default]、[SHA512]、[SHA256]、または [MD5] を選択します。

ヒント　Cisco設定の [Default] を選択した場合、システムはハッシュ関数として SHA512 を想定します。詳細については、Hash Type（36-20 ページ）を参照してください。

ステップ 2　ルールの作成または編集を続けます。詳細については、コンテンツ一致の制約、コンテンツ一致の検索（36-16 ページ）、新しいルールの作成（36-109 ページ）、または既存のルールの変更（36-111 ページ）を参照してください。

raw データ

ライセンス：Protection

Raw Dataオプションを使用すると、ルール エンジンは、正規化されたペイロード データ（ネットワーク分析ポリシーによってデコードされたデータ）を分析する前に、オリジナルのパケット ペイロードを分析します。引数値は使用されません。正規化の前に、ペイロード内の Telnet ネゴシエーション オプションを検査するために Telnet トラフィックを分析する場合に、このキーワードを使用できます。

同じ content または protected_content キーワードで、**Raw Data**オプションを HTTP コンテンツ オプションと一緒に使用することはできません。詳細については、「HTTP コンテンツ オプション（36-25 ページ）」を参照してください。

ヒント HTTP トラフィック内で raw データを検査するかどうか、および検査する raw データの量を決定するために、HTTP Inspect プリプロセッサの [Client Flow Depth] オプションと [Server Flow Depth] オプションを設定できます。詳細については、サーバレベル HTTP 正規化オプションの選択（27-36 ページ）を参照してください。

raw データを分析する方法：

アクセス：Admin/Intrusion Admin

ステップ 1 追加する content または protected_content キーワードの [Raw Data] チェック ボックスをオンにします。

ステップ 2 ルールの作成または編集を続けます。詳細については、コンテンツ一致の制約、コンテンツ一致の検索（36-16 ページ）、新しいルールの作成（36-109 ページ）、または既存のルールの変更（36-111 ページ）を参照してください。

Not

ライセンス：Protection

指定したコンテンツと一致しないコンテンツを検索するには、**Not** オプションを選択します。[Not] オプションがオンになっている content または protected_content キーワードを含むルールを作成する場合は、そのルール内に、[Not] オプションがオフになっている別の content または protected_content キーワードを 1 つ以上含める必要があります。

注意 content または protected_content キーワードに対して [Not] オプションをオンにした場合は、そのキーワードだけを含むルールを作成しないでください。侵入ポリシーの効果がなくなる可能性があります。

たとえば、SMTP ルール 1:2541: 9 に 3 つの content キーワードが含まれており、そのうち 1 つで **Not** オプションが選択されているとします。**Not** オプションが選択されたキーワード以外のすべての content キーワードを仮に削除すると、このルールに基づくカスタム ルールが無効になります。このようなルールを侵入ポリシーに追加すると、そのポリシーの効果がなくなる可能性があります。

指定したコンテンツに一致しないコンテンツを検索する方法：

アクセス：Admin/Intrusion Admin

ステップ 1 追加する content または protected_content キーワードの [Not] チェック ボックスをオンにします。

ヒント 同じ content キーワードで、[Not] チェック ボックスと [Use Fast Pattern Matcher] チェック ボックスを同時に選択することはできません。

ステップ 2　[Not] オプションがオフになっている他の `content` または `protected_content` キーワードを 1 つ以上ルールに含めます。

ステップ 3　ルールの作成または編集を続けます。詳細については、コンテンツ一致の制約、コンテンツ一致の検索（36-16 ページ）、新しいルールの作成（36-109 ページ）、または既存のルールの変更（36-111 ページ）を参照してください。

検索位置オプション

ライセンス：Protection

検索位置オプションを使用すると、指定したコンテンツの検索をどこから開始するか、どこまで検索するかを指定できます。各オプションの詳細については、以下を参照してください。

- Depth（36-22 ページ）
- Distance（36-22 ページ）
- Length（36-23 ページ）
- Offset（36-23 ページ）
- Within（36-23 ページ）

`content` または `protected_content` キーワード内で検索位置オプションを使用する方法については、以下を参照してください。

- content キーワードでの検索位置オプションの使用（36-23 ページ）
- protected_content キーワードでの検索位置オプションの使用（36-24 ページ）

Depth

注　このオプションは、`content` キーワードを設定する場合に**のみ**サポートされます。詳細については、content キーワードの使用（36-16 ページ）を参照してください。

オフセット値の先頭からの（またはオフセットが設定されていない場合はパケット ペイロード先頭からの）コンテンツ検索の最大の深さをバイト単位で指定します。

たとえば、ルールのコンテンツ値が `cgi-bin/phf`、`offset` 値が `3`、`depth` 値が `22` である場合、ルール ヘッダーで指定されたパラメータに合致するパケットでは、`cgi-bin/phf` 文字列に一致する文字列の検索がバイト位置 3 から 開始され、22 バイト処理した後（バイト位置 25 で）停止します。

指定したコンテンツの長さ以上の、最大 65535 バイトまでの値を指定する必要があります。値 0 は指定できません。

デフォルトの深さは、「パケットの末尾まで検索」です。

Distance

以前に見つかったコンテンツ一致から数えて、指定されたバイト数の後に出現する後続のコンテンツ一致を見つけるようルール エンジンに指示します。

Distance（距離）カウンタはバイト 0 から始まるため、最後に見つかったコンテンツ一致から順方向に移動すべきバイト数よりも 1 つ少ない数値を指定してください。たとえば 4 を指定した場合、5 番目のバイトから検索が始まります。

-65535 ～ 65535 バイトを値として指定できます。負の Distance 値を指定した場合は、検索を開始するバイト位置がパケットの先頭から外れる可能性があります。実際にはパケットの第 1 バイトから検索が開始されますが、計算ではパケットの外側のバイトも考慮されます。たとえば、パケット内の現在の位置が第 5 バイトで、次のコンテンツ ルール オプションで Distance 値 -10 および Within 値 20 が指定された場合、検索はペイロードの先頭から開始され、Within オプションが 15 に調整されます。

デフォルトの距離は 0 で、これは最後のコンテンツ一致の後のパケット内の現在位置という意味です。

Length

注 このオプションは protected_content キーワードを設定する場合に**のみ**サポートされます。詳細については、protected_content キーワードの使用（36-17 ページ）を参照してください。

Length protected_content キーワード オプションは、ハッシュされていない検索文字列の長さをバイト単位で示します。

たとえば、コンテンツ Sample1 を使ってセキュア ハッシュを生成した場合には、**Length** 値として 7 を使用します。このフィールドに値を入力することは**必須**です。

Offset

パケット ペイロードの先頭を基準とする、コンテンツの検索を開始するパケット ペイロード内の位置をバイト単位で指定します。値として 65535 ～ 65535 バイトを指定できます。

オフセット カウンタはバイト 0 から始まるため、パケット ペイロードの先頭から順方向に移動すべきバイト数よりも 1 つ少ない数値を指定してください。たとえば 7 を指定した場合は、8 番目のバイトから検索が始まります。

デフォルトのオフセットは 0 で、これはパケットの先頭を意味します。

Within

注 このオプションは、content キーワードを設定する場合に**のみ**サポートされます。詳細については、content キーワードの使用（36-16 ページ）を参照してください。

Within オプションを使用すると、ルールをトリガーとして使用させるには、最後に見つかったコンテンツ一致の末尾以降、指定のバイト数以内に次のコンテンツ一致が発生する必要があることを指示できます。たとえば **Within** 値として 8 を指定した場合、次のコンテンツ一致がパケット ペイロードの次の 8 バイト以内に発生する必要があります。発生しない場合は、ルールをトリガーとして使用する基準が満たされません。

指定したコンテンツの長さ以上の、最大 65535 バイトまでの値を指定できます。

Within のデフォルトは「パケットの末尾まで検索」です。

content キーワードでの検索位置オプションの使用

次のように、2 つの content 位置ペアのいずれかを使用すると、指定したコンテンツの検索をどこから開始するか、どこまで検索するかを指定できます。

- パケット ペイロードの先頭を基準にして検索する場合は、**Offset** と **Depth** を一緒に使用します。
- 現在の検索位置を基準にして検索する場合は、**Distance** と **Within** を一緒に使用します。

ペアに含まれるオプションのどちらか 1 つだけを指定した場合は、そのペアのもう 1 つのオプションのデフォルトが想定されます。

Offset および **Depth** オプションと、**Distance** および **Within** オプションを混合することはできません。たとえば、**Offset** と **Within** をペアにすることはできません。1 つのルール内で任意の数の位置オプションを使用できます。

位置が指定されない場合は、**Offset** と **Depth** のデフォルトが想定されます。つまり、コンテンツ検索はパケット ペイロードの先頭から始まってパケットの末尾まで続きます。

また、既存の `byte_extract` 変数を使用して位置オプションの値を指定することもできます。詳細については、「パケット データをキーワード引数の中に読み込む（36-88 ページ）」を参照してください。

Web インターフェイスを使用して content キーワードで検索位置の値を指定する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　追加する `content` キーワードのフィールドに値を入力します。次の選択肢があります。

- **Offset**
- **奥行**
- **ディスタンス**
- **Within**

1 つのルール内で任意の数の位置オプションを使用できます。

ステップ 2　ルールの作成または編集を続けます。詳細については、コンテンツ一致の制約（36-19 ページ）、コンテンツ一致の検索（36-16 ページ）、新しいルールの作成（36-109 ページ）、または既存のルールの変更（36-111 ページ）を参照してください。

protected_content キーワードでの検索位置オプションの使用

次のように、必須の **Length** `protected_content` 位置オプションを **Offset** または **Distance** 位置オプションと組み合わせて使用すると、指定されたコンテンツの検索をどこから開始するか、どこまで検索するかを指定できます。

- パケット ペイロードの先頭を基準にして、保護された文字列を検索するには、**Length** と **Offset** を一緒に使用します。
- 現在の検索位置を基準にして、保護された文字列を検索するには、**Length** と **Distance** を一緒に使用します。

ヒント　1 つのキーワード設定内で **Offset** オプションと **Distance** オプションを混合することはできませんが、1 つのルール内では任意の数の位置オプションを使用できます。

位置が指定されない場合は、デフォルトが想定されます。つまり、コンテンツ検索はパケット ペイロードの先頭から始まってパケットの末尾まで続きます。

また、既存の `byte_extract` 変数を使用して位置オプションの値を指定することもできます。詳細については、パケット データをキーワード引数の中に読み込む（36-88 ページ）を参照してください。

Web インターフェイスを使用して protected_content キーワードで検索位置の値を指定する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　追加する protected_content キーワードのフィールドに値を入力します。次の選択肢があります。

- **Length**（必須）
- **Offset**
- **ディスタンス**

1 つの protected_content キーワード内で **Offset** オプションと **Distance** オプションを混在させることはできませんが、1 つのルール内では任意の数の位置オプションを使用できます。

ステップ 2　ルールの作成または編集を続けます。詳細については、コンテンツ一致の制約（36-19 ページ）、コンテンツ一致の検索（36-16 ページ）、新しいルールの作成（36-109 ページ）、または既存のルールの変更（36-111 ページ）を参照してください。

HTTP コンテンツ オプション

ライセンス：Protection

HTTP content または protected_content キーワード オプションを使用すると、HTTP Inspect プリプロセッサによってデコードされた HTTP メッセージ内の一致コンテンツを検索する位置を指定できます。

次の 2 つのオプションは、HTTP 応答内のステータス フィールドを検索します。

- **HTTP ステータス コード**
- **HTTP Status Message**

ルール エンジンは未加工の正規化されていないステータス フィールドを検索しますが、ここでは、他の未加工 HTTP フィールドと正規化された HTTP フィールドを併用する際に考慮すべき制限についての説明を簡略化するために、これらのオプションが別個に列挙されていることに注意してください。

次の 5 つのオプションは、必要に応じて HTTP 要求、応答、またはその両方の中で正規化フィールドを検索します（詳細については、HTTP コンテンツ オプション（36-25 ページ）を参照してください）。

- **HTTP URI**
- **HTTP メソッド**
- **HTTP Header**
- **HTTP Cookie**
- **HTTP Client Body**

次の 3 つのオプションは、必要に応じて HTTP 要求、応答、またはその両方で未加工の（正規化されていない）非ステータス フィールドを検索します（詳細については、HTTP コンテンツ オプション（36-25 ページ）を参照してください）。

- **HTTP Raw URI**
- **HTTP Raw Header**
- **HTTP Raw Cookie**

HTTP content オプションを選択する場合は、次のガイドラインに従ってください。

- HTTP content オプションは TCP トラフィックにのみ適用されます。
- パフォーマンスへの悪影響を避けるために、指定したコンテンツが出現する可能性のあるメッセージ部分だけを選択してください。

  たとえば、ショッピング カート メッセージの場合のように大きな cookie がトラフィックに含まれている可能性がある場合は、HTTP cookie ではなく HTTP 見出しの中で指定のコンテンツを検索することができます。
- HTTP Inspect プリプロセッサの正規化機能を活用し、パフォーマンスを向上させるには、作成するすべての HTTP 関連ルールの中に少なくとも 1 つの content または protected_content キーワードを含め、それに対して **HTTP URI**、**HTTP Method**、**HTTP Header**、または **HTTP Client Body** オプションを選択します。
- HTTP content または protected_content キーワード オプションと組み合わせて replace キーワードを使用することはできません。

単一の正規化された HTTP オプションまたはステータス フィールドを指定できます。または、複数の正規化 HTTP オプションとステータス フィールドを任意に組み合わせて、コンテンツ領域をマッチング対象にすることもできます。ただし、HTTP フィールド オプションを使用する場合には次の制限事項に注意してください。

- 同じ content または protected_content キーワード内で、**Raw Data** オプションと HTTP オプションを一緒に使用することはできません。
- 未加工 HTTP フィールド オプション（**HTTP Raw URI**、**HTTP Raw Header**、または **HTTP Raw Cookie**）と、それぞれに対応する正規化されたオプション（**HTTP URI**、**HTTP Header**、または **HTTP Cookie**）を同じ content または protected_content キーワード内で一緒に使用することはできません。
- **Use Fast Pattern Matcher** を、次の 1 つ以上の HTTP フィールド オプションと組み合わせて選択することはできません。

  HTTP Raw URI、**HTTP Raw Header**、**HTTP Raw Cookie**、**HTTP Cookie**、**HTTP Method**、**HTTP Status Message**、または **HTTP Status Code**

  ただし、次のいずれかの正規化フィールドを検索するために高速パターン マッチ機能を使用する content または protected_content キーワードでは、上記のオプションを含めることができます。

  HTTP URI、**HTTP Header**、または **HTTP Client Body**

  たとえば、**HTTP Cookie**、**HTTP Header**、および **Use Fast Pattern Matcher** を選択した場合、ルール エンジンは HTTP cookie と HTTP 見出しの両方でコンテンツを検索しますが、高速パターン マッチ機能は HTTP cookie ではなく、HTTP 見出しにのみ適用されます。
- 制限付きオプションと制限なしオプションを併用した場合、高速パターン マッチ機能は、指定された制限なしフィールドのみを検索することで、ルール エディタにルールを渡して（制限付きフィールドの評価を含む）完全な評価を行うべきかどうかを検査します。詳細については、「Use Fast Pattern Matcher（36-29 ページ）」を参照してください。

HTTP content および protected_content キーワード オプションに関する以下のリストでは、前述した制限事項が各オプションの説明に反映されています。

HTTP URI

正規化された要求 URI フィールド内でコンテンツ一致を検索するには、このオプションを選択します。

このオプションと pcre キーワードの HTTP URI（U）オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。詳細については、Snort 固有の正規表現後の修飾子の表を参照してください。

注 パイプライン処理された HTTP 要求パケットには複数の URI が含まれています。**HTTP URI** が選択されている場合、パイプライン処理された HTTP 要求パケットをルール エンジンが検出すると、そのパケット内のすべての URI でコンテンツ一致が検索されます。

HTTP Raw URI

正規化された要求 URI フィールド内でコンテンツ一致を検索するには、このオプションを選択します。

このオプションと pcre キーワードの HTTP URI(U)オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。詳細については、Snort 固有の正規表現後の修飾子の表を参照してください。

注 パイプライン処理された HTTP 要求パケットには複数の URI が含まれています。**HTTP URI** が選択されている場合、パイプライン処理された HTTP 要求パケットをルール エンジンが検出すると、そのパケット内のすべての URI でコンテンツ一致が検索されます。

HTTP Method

(URI で識別されるリソースに対して行う GET や POST などのアクションを特定する)要求メソッド フィールド内のコンテンツ一致を検索するには、このオプションを選択します。

HTTP Header

HTTP 要求内の(cookie を除く)正規化された見出し フィールドでコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [Inspect HTTP Responses] オプションが有効になっている場合は応答内でも検索されます。

このオプションと pcre キーワードの HTTP 見出し(H)オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。詳細については、Snort 固有の正規表現後の修飾子の表を参照してください。

HTTP Raw Header

HTTP 要求内の(cookie を除く)未加工見出し フィールドでコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [Inspect HTTP Responses] オプションが有効になっている場合は応答内でも検索されます。

このオプションと pcre キーワードの HTTP 未加工見出し(D)オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。詳細については、Snort 固有の正規表現後の修飾子の表を参照してください。

HTTP Cookie

正規化された HTTP クライアント要求ヘッダー内で識別される cookie でコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [Inspect HTTP Responses] オプションが有効になっている場合は応答 set-cookie データ内でも検索されます。システムは、メッセージ本文に含まれる cookie を本文の内容として扱うことに注意してください。

cookie 内だけで一致を検索するには、HTTP Inspect プリプロセッサの [Inspect HTTP Cookies] オプションを有効にする必要があります。これを有効にしない場合、ルール エンジンは cookie を含む見出し全体を検索します。詳細については、「サーバレベル HTTP 正規化オプションの選択(27-36 ページ)」を参照してください。

次の点に注意してください。

- このオプションと pcre キーワードの HTTP cookie(C)オプションを一緒に使用して、同じコンテンツを検索することはできません。詳細については、Snort 固有の正規表現後の修飾子の表を参照してください。
- Cookie: 見出し名と Set-Cookie: 見出し名、見出し行の先行スペース、および見出し行の終わりを示す CRLF は cookie の一部としてではなく、見出しの一部として検査されます。

HTTP Raw Cookie

未加工 HTTP クライアント要求ヘッダー内で識別される cookie でコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [Inspect HTTP Responses] オプションが有効になっている場合は応答 set-cookie データ内でも検索されます。システムは、メッセージ本文に含まれる cookie を本文の内容として扱うことに注意してください。

cookie 内だけで一致を検索するには、HTTP Inspect プリプロセッサの [Inspect HTTP Cookies] オプションを有効にする必要があります。これを有効にしない場合、ルール エンジンは cookie を含む見出し全体を検索します。詳細については、「サーバレベル HTTP 正規化オプションの選択（27-36 ページ）」を参照してください。

次の点に注意してください。

- このオプションと pcre キーワードの HTTP 未加工 cookie(K)オプションを一緒に使用して同じコンテンツを検索することはできません。詳細については、Snort 固有の正規表現後の修飾子の表を参照してください。
- Cookie: 見出し名と Set-Cookie: 見出し名、見出し行の先行スペース、および見出し行の終わりを示す CRLF は cookie の一部としてではなく、見出しの一部として検査されます。

HTTP Client Body

HTTP クライアント要求内のメッセージ本文でコンテンツ一致を検索するには、このオプションを選択します。

このオプションが機能するためには、HTTP Inspect プリプロセッサの [HTTP Client Body Extraction Depth] オプションで 0 ～ 65535 の値を指定する必要があることに注意してください。詳細については、「サーバレベル HTTP 正規化オプションの選択（27-36 ページ）」を参照してください。

HTTP Status Code

HTTP 応答内の 3 桁のステータス コードでコンテンツ一致を検索するには、このオプションを選択します。

このオプションで一致が返されるようにするには、HTTP Inspect プリプロセッサの [Inspect HTTP Responses] オプションを有効にする必要があります。詳細については、「サーバレベル HTTP 正規化オプションの選択（27-36 ページ）」を参照してください。

HTTP Status Message

HTTP 応答のステータス コードに付加されるテキスト記述の中でコンテンツ一致を検索するには、このオプションを選択します。

このオプションで一致が返されるようにするには、HTTP Inspect プリプロセッサの [Inspect HTTP Responses] オプションを有効にする必要があります。詳細については、「サーバレベル HTTP 正規化オプションの選択（27-36 ページ）」を参照してください。

TCP トラフィックのコンテンツ検索を実行する場合に HTTP content オプションを指定する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　(任意)HTTP Inspect プリプロセッサの正規化を活用して、パフォーマンスを向上させるには、以下を選択します。

- 追加する `content` または `protected_content` キーワードの少なくとも 1 つのオプション（**HTTP URI**、**HTTP Raw URI**、**HTTP Method**、**HTTP Header**、**HTTP Raw Header**、または **HTTP Client Body**）
- **HTTP Cookie** または **HTTP Raw Cookie** オプション

ステップ 2　ルールの作成または編集を続けます。詳細については、コンテンツ一致の制約（36-19 ページ）、コンテンツ一致の検索（36-16 ページ）、新しいルールの作成（36-109 ページ）、または既存のルールの変更（36-111 ページ）を参照してください。

Use Fast Pattern Matcher

ライセンス：Protection

注　これらのオプションは、`protected_content` キーワードの設定では**サポートされません**。詳細については、protected_content キーワードの使用（36-17 ページ）を参照してください。

高速パターン マッチ機能は、パケットをルール エンジンに渡す前に、どのルールを評価すべきかをすばやく決定します。この初期決定により、パケット評価で使用されるルール数が大幅に減るため、パフォーマンスが向上します。

デフォルトで、高速パターン マッチ機能は、ルールで指定された最長のコンテンツをパケットで検索します。これは、不必要なルール評価をできるだけ減らすためです。次の例のようなルール フラグメントがあるとします。

```
alert tcp any any -> any 80 (msg:"Exploit"; content:"GET";
http_method; nocase; content:"/exploit.cgi"; http_uri;
nocase;)
```

ほとんどすべての HTTP クライアント要求にはコンテンツ `GET` が含まれていますが、コンテンツ `/exploit.cgi` を含む要求は稀です。`GET` を高速パターン コンテンツとして使用した場合、ルール エンジンはほとんどのケースでこのルールを評価し、一致はほとんど検出されないでしょう。しかし、`/exploit.cgi` を使用するとほとんどのクライアントの `GET` 要求は評価されないため、パフォーマンスが向上します。

指定されたコンテンツが高速パターン マッチ機能で検出された場合にのみ、ルール エンジンはパケットをルールに照らして評価します。たとえば、ルール内の 1 つの `content` キーワードでコンテンツ `short` を指定し、別のキーワードで `longer`、さらに 3 番目のキーワードで `longest` を指定した場合、高速パターン マッチ機能はコンテンツ `longest` を使用し、ルール エンジンがペイロード内で `longest` を検出した場合にのみ、ルールが評価されます。

より短い検索パターンを高速パターン マッチ機能で使用するよう指定するには、**Use Fast Pattern Matcher** オプションを使用できます。理論的には、指定したパターンの方が最長パターンよりもパケット内で見つかる可能性が低いため、より的を絞って対象の exploit を識別できます。

Use Fast Pattern Matcher と他のオプションを同じ `content` キーワード内で選択する場合は、次の制限事項に注意してください。

- ルールごとに 1 回だけ、**Use Fast Pattern Matcher** を指定できます。

- **Use Fast Pattern Matcher** と **Not** を組み合わせて選択した場合は、**Distance**、**Within**、**Offset**、および **Depth** を使用できません。
- Use Fast Pattern Matcher を、次のいずれかの HTTP フィールド オプションと組み合わせて選択することはできません。

  HTTP Raw URI、**HTTP Raw Header**、**HTTP Raw Cookie**、**HTTP Cookie**、**HTTP Method**、**HTTP Status Message**、または **HTTP Status Code**

  ただし、次のいずれかの正規化フィールドを検索するために高速パターン マッチ機能を使用する `content` キーワードでは、上記のオプションを含めることができます。

  HTTP URI、**HTTP Header**、または **HTTP Client Body**

  たとえば、**HTTP Cookie**、**HTTP Header**、および **Use Fast Pattern Matcher** を選択した場合、ルール エンジンは HTTP cookie と HTTP 見出しの両方でコンテンツを検索しますが、高速パターン マッチ機能は HTTP cookie ではなく、HTTP 見出しにのみ適用されます。

  未加工 HTTP フィールド オプション（**HTTP Raw URI**、**HTTP Raw Header**、または **HTTP Raw Cookie**）と、それぞれに対応する正規化されたオプション（**HTTP URI**、**HTTP Header**、または **HTTP Cookie**）を同じ `content` キーワード内で一緒に使用できないことに注意してください。詳細については、「HTTP コンテンツ オプション（36-25 ページ）」を参照してください。

  制限付きオプションと制限なしオプションを併用した場合、高速パターン マッチ機能は、指定された制限なしフィールドのみを検索することで、ルール エンジンにパケットを渡して（制限付きフィールドの評価を含む）完全な評価を行うべきかどうかを検査します。
- オプションで、**Use Fast Pattern Matcher** を選択した場合には **Fast Pattern Matcher Only** または **Fast Pattern Matcher Offset and Length** を選択することもできますが、この両方は選択できません。
- Base64 データの検査時には高速パターン マッチ機能を使用できません（詳細については、Base64 データのデコードと検査（36-107 ページ）を参照してください）。

Fast Pattern Matcher Only の使用

Fast Pattern Matcher Only オプションを使用すると、`content` キーワードをルール オプションとしてではなく、高速パターン マッチ機能オプションとしてのみ使用できます。指定したコンテンツをルール エンジンで評価する必要がない場合、このオプションを使ってリソースを節約できます。たとえば、ペイロード内のいずれかの場所にコンテンツ `12345` が存在することだけを必要とするルールがあるとします。高速パターン マッチ機能でパターンが検出された場合に、ルール内の追加のキーワードに照らしてパケットを評価できます。パターン `12345` が含まれているかどうかを判断するために、ルール エンジンがパケットを再評価する必要はありません。

指定されたコンテンツに関連する他の条件がルールに含まれている場合は、このオプションを使用しないでください。たとえば、別のルール条件で `abcd` が `1234` の前に出現するかどうかを判断する場合には、このオプションを使ってコンテンツ `1234` を検索しないでください。**Fast Pattern Matcher Only** を指定すると、指定されたコンテンツがルール エンジンによって検索されないため、このケースではルール エンジンが相対的な位置を判断できません。

このオプションを使用するときには、次の条件に注意してください。

- 指定されたコンテンツは位置に依存しない、つまり、ペイロードのどこにでも出現する可能性があるため、位置オプション（**Distance**、**Within**、**Offset**、**Depth**、**Fast Pattern Matcher Offset and Length**）を使用することはできません。
- このオプションを **Not** と組み合わせて使用することはできません。
- このオプションを **Fast Pattern Matcher Offset and Length** と組み合わせて使用することはできません。

- すべてのパターンは、大文字/小文字を区別しない方法で、高速パターン マッチ機能に挿入されるため、指定したコンテンツは「大文字/小文字の区別なし」として扱われます。これは自動的に処理されるため、このオプションの選択時に [Case Insensitive] を選択する必要はありません。
- **Fast Pattern Matcher Only** オプションを使用する `content` キーワードの直後に、現在の検索位置を基準にして検索位置を設定する次のキーワードを続けないようにしてください。
- `isdataat`
- `pcre`
- `content`（**Distance** または **Within** が選択されている場合）
- `content`（**HTTP URI** が選択されている場合）
- `asn1`
- `byte_jump`
- `byte_test`
- `byte_extract`
- `base64_decode`

Fast Pattern Matcher Offset and Length の指定

Fast Pattern Matcher Offset and Length オプションを使用すると、検索するコンテンツの一部分を指定できます。これにより、パターンが非常に長く、ルールの一致の可能性を判断するのにパターンの一部分だけで十分な場合に、メモリ消費を抑えることができます。高速パターン マッチ機能によってルールが選択されたときに、パターン全体がルールに照らして評価されます。

次の構文に従い、検索を開始する位置（オフセット）およびコンテンツ内をどれほど検索するか（長さ）をバイト単位で指定することにより、高速パターン マッチ機能で使用する部分を決定します。

`offset,length`

たとえば、次のコンテンツに対して

```
1234567
```

次のようにオフセットと長さのバイト数を指定した場合、

```
1,5
```

高速パターン マッチ機能はコンテンツ `23456` のみを検索します。

このオプションを **Fast Pattern Matcher Only** と一緒に使用できないことに注意してください。

高速パターン マッチ機能で検索されるコンテンツを指定する方法:

アクセス: Admin/Intrusion Admin

ステップ 1　追加する `content` キーワードに関して [Use Fast Pattern Matcher] を選択します。

ステップ 2　オプションで、指定したパターンがパケット内に存在するかどうかをルール エンジン評価なしで判断するには [Fast Pattern Matcher Only] を選択します。

指定されたコンテンツが高速パターン マッチ機能で検出された場合にのみ、評価が開始されます。

ステップ 3　オプションで、次の構文に従い、コンテンツの検索場所となるパターンの部分を [Fast Pattern Matcher Offset and Length] で指定します。

`offset,length`

ここで、*`offset`* は検索の開始場所となるコンテンツ先頭からのバイト数を指定し、*`length`* は検索を続けるバイト数を指定します。

ステップ 4　ルールの作成または編集を続けます。詳細については、コンテンツ一致の制約（36-19 ページ）、PCRE を使用したコンテンツの検索（36-38 ページ）、新しいルールの作成（36-109 ページ）、または既存のルールの変更（36-111 ページ）を参照してください。

インライン展開でのコンテンツの置換

ライセンス： Protection

インライン展開で `replace` キーワードを使用すると、指定したコンテンツを置き換えることができます。

注　Cisco SSL アプライアンスによって検出された SSL トラフィック内のコンテンツを置き換えるために `replace` キーワードを使用することは**できません**。置換データではなく、元の暗号化データが送信されます。詳細については、『*Cisco SSL Appliance Administration and Deployment Guide*』を参照してください。

`replace` キーワードを使用するには、`content` キーワードを使って特定の文字列を検索するカスタム標準テキスト ルールを作成します。その後、`replace` キーワードを使用して、コンテンツを置き換える文字列を指定します。置換値とコンテンツ値は同じ長さである必要があります。

注　`protected_content` キーワード内でハッシュされたコンテンツを置き換えるために `replace` キーワードを使用することは**できません**。詳細については、protected_content キーワードの使用（36-17 ページ）を参照してください。

オプションで、以前の FireSIGHT システム ソフトウェア バージョンとの下位互換性を維持するために、置換文字列を引用符で囲むことができます。引用符を含めない場合は、それらが自動的にルールに追加されるため、構文的に正しいルールになります。置換テキストの一部として先行引用符または後続引用符を含めるには、次の例に示すように、バックスラッシュを使ってエスケープする必要があります。

```
"replacement text plus \"quotation\" marks""
```

1 つのルール内に複数の `replace` キーワードを含めることができますが、`content` キーワードごとに 1 つずつしか含めることができません。ルールによって検出されたコンテンツの最初のインスタンスだけが置き換えられます。

次に、`replace` キーワードの使用例を示します。

- exploit を含んでいる着信パケットをシステムが検出した場合、有害な文字列を無害な文字列に置き換えることができます。このテクニックは、有害なパケットを単に破棄するよりも効果的である場合があります。破棄されたパケットを攻撃者が単に再送信し続け、やがてネットワーク防御を通り抜けるか、ネットワークを氾濫させるという攻撃シナリオがあります。パケットを破棄する代わりに別の文字列に置き換えることで、脆弱ではないターゲットに対して攻撃が実行されたと攻撃者に思い込ませることができます。
- （たとえば Web サーバの）脆弱なバージョンが稼働しているかどうかを調べる偵察攻撃が懸念される場合は、発信パケットを検出して、バナーを独自のテキストに置き換えることができます。

注　置換ルールを使用するインライン侵入ポリシー内でルール状態が [Generate Events] に設定されていることを確認してください。ルールを [Drop and Generate events] に設定した場合はパケットが破棄され、コンテンツが置き換えられません。

文字列置換プロセスでは、宛先ホストがエラーなしでパケットを受信できるように、パケット チェックサムがシステムによって自動的に更新されます。

`replace` キーワードを HTTP 要求メッセージ `content` キーワード オプションと組み合わせて使用できないことに注意してください。詳細については、コンテンツ一致の検索（36-16 ページ）およびHTTP コンテンツ オプション（36-25 ページ）を参照してください。

インライン展開でコンテンツを置き換えるには：

アクセス： Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [content] を選択して、[Add Option] をクリックします。

`content` キーワードが表示されます。

ステップ 2　[content] フィールドで、検出するコンテンツを指定します。オプションで、該当する引数を選択します。HTTP 要求メッセージ `content` キーワード オプションを `replace` キーワードと一緒に使用できないことに注意してください。

ステップ 3　ドロップダウン リストから [replace] を選択して、[Add Option] をクリックします。

`replace` キーワードが `content` キーワードの下に表示されます。

ステップ 4　[replace:] フィールドで、指定したコンテンツに対する置換文字列を指定します。

Byte_Jump と Byte_Test の使用

ライセンス： Protection

`byte_jump` と `byte_test` を使用すると、パケット内のどの位置でルール エンジンがデータ マッチング検査を開始すべきか、どのバイトを評価すべきかを計算できます。

また、`byte_jump` および `byte_test` **DCE/RPC** 引数を使用すると、DCE/RPC プリプロセッサで処理されるトラフィック用にいずれかのキーワードを調整できます。**DCE/RPC** 引数を使用するときには、他の特定の DCE/RPC キーワードと組み合わせて `byte_jump` と `byte_test` を使用することもできます。詳細については、DCE/RPC トラフィックのデコード（27-2 ページ）およびDCE/RPC キーワード（36-64 ページ）を参照してください。

詳細については、次の項を参照してください。

- byte_jump（36-34 ページ）
- byte_test（36-36 ページ）

byte_jump

ライセンス：Protection

byte_jump キーワードは、指定されたバイト セグメントで定義されるバイト数を計算し、指定したオプションに応じて、指定されたバイト セグメントの末尾から順方向に、またはパケット ペイロードの先頭から、パケット内でそのバイト数だけスキップします。パケットの特定のバイト セグメントが、パケット内の可変データに含まれるバイト数を示す場合には、これが役立ちます。

次の表では、byte_jump キーワードで必要な引数を説明します。

表 36-8　byte_jump の必須の引数

引数	説明
Bytes	パケットから計算するバイト数。
Offset	ペイロード内で処理を開始するバイト数。offset カウンタはバイト 0 から始まるため、パケット ペイロードの先頭、または最後に見つかったコンテンツ一致から順方向にジャンプさせるバイト数から 1 を差し引いて offset 値を計算してください。 また、既存の byte_extract 変数を使用してこの引数の値を指定することもできます。詳細については、「パケット データをキーワード引数の中に読み込む（36-88 ページ）」を参照してください。

次の表で説明するオプションを使用すると、必須の引数に指定された値をシステムがどのように解釈するかを定義できます。

表 36-9　byte_jump の追加のオプション引数

引数	説明
Relative	最後に見つかったコンテンツ一致で検出された最後のパターンを基準にしてオフセットを計算します。
Align	変換されたバイト数を次の 32 ビット境界に切り上げます。
Multiplier	ルール エンジンで最終的な byte_jump 値を算出するために、パケットから得られた byte_jump 値に掛ける値を示します。 つまり、ルール エンジンは、指定されたバイト セグメントで定義されるバイト数だけスキップする代わりに、Multiplier 引数で指定される整数を乗算したバイト数だけスキップします。
Post Jump Offset	他の byte_jump 引数を適用した後に、順方向または逆方向にスキップするバイト数（63535 ～ 63535）。正の値は順方向にスキップし、負の値は逆方向にスキップします。無効にするには、フィールドを空白のままにするか、0 を入力します。 **DCE/RPC** 引数を選択したときに適用されない byte_jump 引数については、エンディアンネス引数の表の **DCE/RPC** 引数を参照してください。
From Beginning	スキップするバイト数を示すバイト セグメントの末尾からではなく、パケット ペイロードの先頭から数えて、指定されたバイト数だけペイロード内をスキップするようルール エンジンに指示します。

DCE/RPC、**Endian**、または **Number Type** のうち 1 つだけを指定できます。

byte_jump キーワードでどのようにバイト数を計算するかを定義するにはは、次の表に示す引数から選択できます(どの引数も指定されない場合は、ネットワーク バイト順が使用されます)。

表 36-10　エンディアンネス引数

引数	説明
Big Endian	デフォルトのネットワーク バイト順であるビッグ エンディアン バイト順でデータを処理します。
Little Endian	リトル エンディアン バイト順でデータを処理します。
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に byte_jump キーワードを指定します。詳細については、「DCE/RPC トラフィックのデコード (27-2 ページ)」を参照してください。 DCE/RPC プリプロセッサがビッグ エンディアンまたはリトル エンディアン バイト順を決定します。**Number Type**、**Endian**、および **From Beginning** 引数は適用されません。 この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて byte_jump を使用することもできます。詳細については、「DCE/RPC キーワード (36-64 ページ)」を参照してください。

次の表に示すいずれか 1 つの引数を使用して、パケット内のストリング データをシステムがどのように認識するかを定義します。

表 36-11　Number Type 引数

引数	説明
Hexadecimal String	変換後のストリング データを 16 進形式で表現します。
Decimal String	変換後のストリング データを 10 進形式で表現します。
Octal String	変換後のストリング データを 8 進形式で表現します。

たとえば、次のような値を byte_jump に設定した場合、

- Bytes = 4
- Offset = 12
- Relative enabled
- Align enabled

ルール エンジンは、最後に見つかったコンテンツ一致から 13 バイト後に出現する 4 つのバイトで記述される数値を計算して、そのバイト数だけパケット内を順方向にスキップします。たとえば、ある特定のパケット内で計算される 4 つのバイトが 00 00 00 1F である場合、ルール エンジンはこれを 31 に変換します。(次の 32 ビット境界まで移動するようエンジンに指示する)align が指定されているため、ルール エンジンはパケット内を 32 バイト先までスキップします。

あるいは、次のような値を byte_jump に設定した場合、

- Bytes = 4
- Offset = 12
- From Beginning enabled
- Multiplier = 2

ルール エンジンは、パケットの先頭から 13 バイト後に出現する 4 つのバイトで記述される数値を計算します。その後、その数値に 2 を掛けてスキップする総バイト数を計算します。たとえば、ある特定のパケット内で計算される 4 つのバイトが 00 00 00 1F である場合、ルール エンジンはこれを 31 に変換し、それに 2 を掛けて 62 にします。From Beginning が有効になっているため、ルール エンジンはパケット内の最初の 63 バイトをスキップします。

byte_jump を使用する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　ドロップダウン リストから [byte_jump] を選択して、[Add Option] をクリックします。

[byte_jump] セクションが、選択された最後のキーワードの下に表示されます。

byte_test

ライセンス： Protection

byte_test キーワードは、指定されたバイト セグメント内のバイト数を計算し、指定した演算子と値に基づいてそれらを比較します。

次の表に、byte_test キーワードで必要な引数を説明します。

表 36-12　byte_test の必須の引数

引数	説明
Bytes	パケットから計算するバイト数。1 ～ 10 バイトを指定できます。
Operator and Value	指定された値を <、>、=、!、&、^、!>、!<、!=、!&、または !^ で比較します。 たとえば !1024 と指定した場合、byte_test は指定された数値を変換し、それが 1024 と等しくなければイベントが生成されます（他のすべてのキーワード パラメータが一致する場合）。 「!」と「!=」は等価であることに注意してください。 また、既存の byte_extract 変数を使用してこの引数の値を指定することもできます。詳細については、「パケット データをキーワード引数の中に読み込む（36-88 ページ）」を参照してください。
Offset	ペイロード内で処理を開始するバイト数。offset カウンタはバイト 0 から始まるため、パケット ペイロードの先頭、または最後に見つかったコンテンツ一致から順方向に数えるバイト数から 1 を差し引いて offset 値を計算してください。 また、既存の byte_extract 変数を使用してこの引数の値を指定することもできます。詳細については、「パケット データをキーワード引数の中に読み込む（36-88 ページ）」を参照してください。

次の表に示す引数を使用すると、システムで byte_test 引数がどのように使用されるかをさらに定義できます。

表 36-13　byte_test の追加のオプション引数

引数	説明
Relative	最後に見つかったパターン一致を基準にしてオフセットを計算します。
Align	変換されたバイト数を次の 32 ビット境界に切り上げます。

DCE/RPC、**Endian**、または **Number Type** のうち 1 つだけを指定できます。

検査対象となるバイトを byte_test キーワードでどのように計算するか定義するには、次の表の中から引数を選択します。どの引数も指定しない場合は、ネットワーク バイト順が使用されます。

表 36-14　byte_test のエンディアンネス引数

引数	説明
Big Endian	デフォルトのネットワーク バイト順であるビッグ エンディアン バイト順でデータを処理します。
Little Endian	リトル エンディアン バイト順でデータを処理します。
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に byte_test キーワードを指定します。詳細については、「DCE/RPC トラフィックのデコード (27-2 ページ)」を参照してください。 DCE/RPC プリプロセッサがビッグ エンディアンまたはリトル エンディアン バイト順を決定します。**Number Type** 引数と **Endian** 引数は適用されません。 この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて byte_test を使用することもできます。詳細については、「DCE/RPC キーワード (36-64 ページ)」を参照してください。

次の表に示すいずれか 1 つの引数を使用して、パケット内のストリング データをシステムがどのように認識するかを定義できます。

表 36-15　Number Type byte-test 引数

引数	説明
Hexadecimal String	変換後のストリング データを 16 進形式で表現します。
Decimal String	変換後のストリング データを 10 進形式で表現します。
Octal String	変換後のストリング データを 8 進形式で表現します。

たとえば、次のような値を byte_test に指定した場合、

- Bytes = 4
- Operator and Value > 128
- Offset = 8
- Relative enabled

ルール エンジンは、最後に見つかったコンテンツ一致から（それを基準にして）9 バイト後に出現する 4 つのバイトで記述される数値を計算し、その計算値が 128 バイトを超えた場合に、ルールがトリガーとして使用されます。

byte_test を使用する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [byte_test] を選択して、[Add Option] をクリックします。

[byte_test] セクションが、選択された最後のキーワードの下に表示されます。

PCRE を使用したコンテンツの検索

ライセンス：Protection

`pcre` キーワードを使用すると、指定されたコンテンツをパケット ペイロード内で検査するために Perl 互換正規表現（PCRE）を使用できます。PCRE を使用すると、同じ内容のわずかなバリエーションにそれぞれ一致する複数のルールを作成する手間が省けます。

正規表現は、さまざまな方法で表現されることのあるコンテンツを検索する場合に役立ちます。パケットのペイロード内でコンテンツを検索するときには、コンテンツがさまざまな属性を持つ可能性があることを考慮すべき場合があります。

侵入ルールで使われる正規表現構文は完全な正規表現ライブラリのサブセットであり、完全なライブラリ内のコマンドで使用される構文とはいくつかの点で異なることに注意してください。ルール エディタを使用して `pcre` キーワードを追加するときには、次の形式で完全な値を入力します。

```
!/pcre/ ismxAEGRBUIPHDMCKSY
```

値は次のとおりです。

- 「!」は否定オプションです（正規表現に**一致しない**パターンを照合する場合に使用します）。
- `/pcre/` は Perl 互換正規表現です。
- `ismxAEGRBUIPHDMCKSY` は修飾子オプションの任意の組み合わせです。

また、次の表に示す文字をエスケープする必要があることに注意してください。これにより、パケット ペイロード内で特定のコンテンツを検索するために PCRE でこれらの文字を使用した場合、ルール エンジンがそれを正しく解釈するようになります。

表 36-16　エスケープする PCRE 文字

エスケープする必要のある文字	バックスラッシュを使用した場合	16 進コードを使用した場合
#（ナンバー記号）	\#	\x23
;（セミコロン）	\;	\x3B
|（縦棒）	\\|	\x7C
:（コロン）	\:	\x3A

ヒント　必要に応じて、Perl 互換正規表現を引用符で囲むこともできます（例：*pcre_expression* または "*pcre_expression*"）。引用符が任意ではなく必須であった旧バージョンに慣れている経験豊富なユーザのために、引用符を使用するオプションが提供されています。保存後のルールをルール エディタで表示すると、引用符が表示されません。

m?regex? を使用することもできます。ここで、? は「/」以外のデリミタです。正規表現内でスラッシュと一致させる必要があり、バックスラッシュを使ってそれをエスケープしたくない場合には、これを使用できます。たとえば、「m?*regex*? ismxAEGRBUIPHDMCKSY」のように使用できます。*regex* は Perl 互換正規表現、ismxAEGRBUIPHDMCKSY は修飾子オプションの任意の組み合わせです。正規表現の構文の詳細については、Perl 互換正規表現の基本（36-39 ページ）を参照してください。

以下の項では、有効な pcre キーワードの値を作成する方法について詳しく説明します。

- Perl 互換正規表現の基本（36-39 ページ）では、Perl 互換正規表現で使われる一般的な構文について説明します。
- PCRE 修飾子のオプション（36-41 ページ）では、正規表現を変更するために使用できるオプションについて説明します。
- PCRE キーワード値の例（36-44 ページ）では、ルールにおける pcre キーワードの使用例を示します。

Perl 互換正規表現の基本

ライセンス： Protection

pcre キーワードでは、標準の Perl 互換正規表現（PCRE）構文を使用できます。以下の項では、この構文について説明します。

ヒント　ここでは PCRE で使用可能な基本的な構文について説明しますが、Perl および PCRE 専用のオンライン リファレンスやブックで、さらに詳しい情報を参照することもできます。

メタ文字

ライセンス： Protection

メタ文字は正規表現内で特別な意味を持つリテラル文字です。メタ文字を正規表現内で使用するときには、その前にバックスラッシュを付けて「エスケープする」必要があります。

次の表に、PCRE で使用可能なメタ文字について説明し、それぞれの例を示します。

表 36-17　PCRE メタ文字

メタ文字	説明	例
.	改行以外の任意の文字と一致します。修飾オプションとして s が使用されている場合は、改行文字も含まれます。	abc. は、abcd、abc1、abc# などと一致します。
*	ある文字または式の 0 回以上の出現と一致します。	abc* は、abc、abcc、abccc、abccccc などと一致します。
?	ある文字または式の 0 回または 1 回の出現と一致します。	abc? は abc に一致します。
+	ある文字または式の 1 回以上の出現と一致します。	abc+ は、abc、abcc、abccc、abccccc などと一致します。

表 36-17　PCRE メタ文字（続き）

メタ文字	説明	例
()	式をグループ化します。	(abc)+ は、abc、abcabc、abcabcabc などと一致します。
{}	ある文字または式の一致回数の限度を指定します。下限と上限を設定する場合には、下限と上限をカンマで区切ります。	a{4,6} は、aaaa、aaaaa、または aaaaaa と一致します。 (ab){2} は abab と一致します。
[]	文字クラスを定義できます。セットの中で記述される任意の文字または文字の組み合わせに一致します。	[abc123] は、a または b または c などと一致します。
^	文字列の先頭でコンテンツを照合します。また、文字クラスの中で否定としても使用されます。	^in は、info 内の “in” と一致しますが、bin では一致しません。[^a] は、a を含まない任意の文字列と一致します。
$	文字列の末尾でコンテンツを照合します。	ce$ は、announce 内の “ce” と一致しますが、cent では一致しません。
|	OR 式を示します。	(MAILTO|HELP) は、MAILTO または HELP と一致します。
\	メタ文字を実際の文字として使用できます。また、事前定義された文字クラスを指定するためにも使われます。	\. はピリオドと一致し、* はアスタリスクと一致し、\\ はバックスラッシュと一致します。\d は数字と一致し、\w は英数字と一致します。PCRE での文字クラスの使用方法については、文字クラス（36-40 ページ）を参照してください。

文字クラス

ライセンス：Protection

文字クラスには、英字、数字、英数字、および空白文字があります。大カッコで囲んで独自の文字クラスを作成できます（メタ文字（36-39 ページ）を参照）。また、事前定義のクラスをさまざまな文字タイプのショートカットとして使用することもできます。追加の修飾子なしで文字クラスを使用すると、1 つの文字クラスは 1 桁または 1 文字に一致します。

次の表に、PCRE で使用できる事前定義の文字クラスの説明と例を示します。

表 36-18　PCRE 文字クラス

文字クラス	説明	文字クラスの定義
\d	数字（桁）と一致します。	[0-9]
\D	数字以外の任意の文字と一致します。	[^0-9]
\w	英数字（語）と一致します。	[a-zA-Z0-9_]
\W	英数字以外の任意の文字と一致します。	[^a-zA-Z0-9_]
\s	スペース、復帰、タブ、改行、および改ページを含む空白文字と一致します。	[\r\t\n\f]
\S	空白文字以外の任意の文字と一致します。	[^ \r\t\n\f]

PCRE 修飾子のオプション

ライセンス：Protection

pcre キーワードの値の中で正規表現構文を指定した後、修飾オプションを使用できます。これらの修飾子は、Perl、PCRE、および Snort 固有の処理機能を実行します。修飾子は、常に PCRE 値の末尾に、次の形式で出現します。

/*pcre*/ismxAEGRBUIPHDMCKSY

ここで、ismxAEGRBUPHMC には、次の表に示す任意の修飾オプションを含めることができます。

ヒント　オプションで、正規表現と修飾オプションを引用符で囲むことができます（たとえば "/pcre/ismxAEGRBUIPHDMCKSY"）。引用符が任意ではなく必須であった旧バージョンに慣れている経験豊富なユーザのために、引用符を使用するオプションが提供されています。保存後のルールをルール エディタで表示すると、引用符が表示されません。

次の表に、Perl 処理機能を実行するために使用できるオプションを説明します。

表 36-19　Perl 関連の正規表現後オプション

オプション	説明
i	正規表現で大文字と小文字を区別しないようにします。
s	ドット文字（.）は、改行または \n 文字を除くすべての文字を表します。オプションとして "s" を使用すると、これをオーバーライドして、改行文字を含むすべての文字をドット文字に一致させることができます。
m	デフォルトで、1 つの文字列は複数文字からなる単一行として扱われ、^ と $ は特定の文字列の先頭および末尾に一致します。オプションとして "m" を使用すると、^ および $ はバッファの先頭または末尾だけでなく、バッファ内の改行文字の直前または直後のコンテンツとも一致します。
x	エスケープされた（バックスラッシュが先行する）場合、および文字クラスに含まれる場合を除き、空白データ文字がパターン内に出現してもそれを無視します。

次の表に、正規表現の後ろに使用できる PCRE 修飾子の説明を示します。

表 36-20　PCRE 関連の正規表現後オプション

オプション	説明
A	文字列の先頭でパターンが一致する必要があります（正規表現で ^ を使用した場合と同じ）。
E	対象の文字列の末尾でのみ一致するように $ を設定します（E を伴わない $ は、それが改行である場合には最後の文字の直前とも一致しますが、他の改行文字の直前とは一致しません）。
G	デフォルトでは、* + と ? は「最長マッチ」を実行します。つまり、複数の一致が見つかった場合は最も長い一致が選択されます。G 文字を使用するとこの動作が変更され、常に最初の一致がこれらの文字で選択されます。ただし後ろに疑問符（?）が続く場合を除きます。たとえば、*?+? と ?? は G 修飾子を使った構造内で最長マッチを実行し、疑問符が付いていない *、+、または ? は最長マッチではありません。

次の表は、正規表現の後ろに付加できる Snort 固有の修飾子を示しています。

表 36-21　Snort 固有の正規表現後の修飾子

オプション	説明
R	ルール エンジンで見つかった最後の一致の末尾を基準にして、一致するコンテンツを検索します。
B	プリプロセッサによってデコードされる前のデータ内のコンテンツを検索します（このオプションは、`content` または `protected_content` キーワードで `Raw Data` 引数を使用する場合と似ています）。
U	HTTP Inspect プリプロセッサによってデコードされた正規化済み HTTP 要求メッセージの URI 内のコンテンツを検索します。このオプションと `content` または`protected_content` キーワードの **HTTP URI** オプションを一緒に使用して、同じコンテンツを検索することはできません。詳細については、「HTTP コンテンツ オプション（36-25 ページ）」を参照してください。 **注**　パイプライン処理された HTTP 要求パケットには複数の URI が含まれています。U オプションを含む PCRE 式を使用すると、ルール エンジンは、パイプライン処理された HTTP 要求パケット内の最初の URI でのみコンテンツ一致を検索します。パケット内のすべての URI を検索するには、**HTTP URI** を選択して `content` または `protected_content` キーワードを使用します。U オプションを含む PCRE 式を一緒に使用するかどうかは問いません。
I	HTTP Inspect プリプロセッサによってデコードされた未加工 HTTP 要求メッセージの URI 内のコンテンツを検索します。このオプションと `content` または`protected_content` キーワードの **HTTP Raw URI** オプションを一緒に使用して、同じコンテンツを検索することはできません。詳細については、「HTTP コンテンツ オプション（36-25 ページ）」を参照してください。
P	HTTP Inspect プリプロセッサによってデコードされた正規化済み HTTP 要求メッセージ本文の中でコンテンツを検索します。詳細については、HTTP コンテンツ オプション（36-25 ページ）で、`content` および `protected_content` キーワードの **HTTP Client Body** オプションを参照してください。
H	HTTP Inspect プリプロセッサによってデコードされた HTTP 要求または応答メッセージの（cookie を除く）見出し内のコンテンツを検索します。このオプションと `content` または `protected_content` キーワードの **HTTP Header** オプションを一緒に使用して、同じコンテンツを検索することはできません。詳細については、「HTTP コンテンツ オプション（36-25 ページ）」を参照してください。
D	HTTP Inspect プリプロセッサによってデコードされた未加工 HTTP 要求または応答メッセージの（cookie を除く）見出し内のコンテンツを検索します。このオプションと `content` または `protected_content` キーワードの **HTTP Raw Header** オプションを一緒に使用して、同じコンテンツを検索することはできません。詳細については、「HTTP コンテンツ オプション（36-25 ページ）」を参照してください。
M	HTTP Inspect プリプロセッサによってデコードされた正規化済み HTTP 要求メッセージのメソッド フィールド内のコンテンツを検索します。メソッド フィールドは、URI で識別されるリソースに対して実行すべきアクション（GET、PUT、CONNECT など）を特定します。詳細については、HTTP コンテンツ オプション（36-25 ページ）で、`content` および `protected_content` キーワードの **HTTP Method** オプションを参照してください。

表 36-21　Snort 固有の正規表現後の修飾子（続き）

オプション	説明
C	HTTP Inspect プリプロセッサの [Inspect HTTP Cookies] オプションが有効になっている場合は、HTTP 要求ヘッダーの cookie 内の正規化済みコンテンツを検索します。さらに、プリプロセッサの [Inspect HTTP Responses] オプションが有効になっている場合は、HTTP 応答ヘッダーの set-cookie 内も検索します。[Inspect HTTP Cookies] が有効になっていない場合は、cookie または set-cookie データを含めて、ヘッダー全体を検索します。 次の点に注意してください。 • メッセージ本文に含まれる cookie は、本文のコンテンツとして扱われます。 • このオプションと `content` または`protected_content` キーワードの **HTTP Cookie** オプションを一緒に使用して、同じコンテンツを検索することはできません。詳細については、「HTTP コンテンツ オプション（36-25 ページ）」を参照してください。 • `Cookie:` 見出し名と `Set-Cookie:` 見出し名、見出し行の先行スペース、および見出し行の終わりを示す `CRLF` は cookie の一部としてではなく、見出しの一部として検査されます。
K	HTTP Inspect プリプロセッサの [Inspect HTTP Cookies] オプションが有効になっている場合は、HTTP 要求ヘッダーの cookie 内の未加工コンテンツを検索します。さらに、プリプロセッサの [Inspect HTTP Responses] オプションが有効になっている場合は、HTTP 応答ヘッダーの set-cookie 内も検索します。[Inspect HTTP Cookies] が有効になっていない場合は、cookie または set-cookie データを含めて、ヘッダー全体を検索します。 次の点に注意してください。 • メッセージ本文に含まれる cookie は、本文のコンテンツとして扱われます。 • このオプションと `content` または`protected_content` キーワードの **HTTP Raw Cookie** オプションを一緒に使用して、同じコンテンツを検索することはできません。詳細については、「HTTP コンテンツ オプション（36-25 ページ）」を参照してください。 • `Cookie:` 見出し名と `Set-Cookie:` 見出し名、見出し行の先行スペース、および見出し行の終わりを示す `CRLF` は cookie の一部としてではなく、見出しの一部として検査されます。
S	HTTP 応答内の 3 桁のステータス コードを検索します。詳細については、HTTP コンテンツ オプション（36-25 ページ）で、`content` および `protected_content` キーワードの **HTTP Status Code** オプションを参照してください。
Y	HTTP 応答内のステータス コードに付加されるテキスト記述を検索します。詳細については、HTTP コンテンツ オプション（36-25 ページ）で、`content` および `protected_content` キーワードの **HTTP Status Message** オプションを参照してください。

注　U オプションと R オプションを組み合わせて使用しないでください。パフォーマンスの問題が発生する可能性があります。また、他の HTTP コンテンツ オプション（I、P、H、D、M、C、K、S、または Y）と組み合わせて U オプションを使用しないでください。

PCRE キーワード値の例

ライセンス：Protection

次に、pcre で入力できる値の例を示し、それぞれの例で何が一致するかを説明します。

- **/feedback[(\d{0,1})]?\.cgi/U**

  この例では、URI データにのみ配置された、feedback の後に 0 個または 1 個の数字、さらに .cgi が続くインスタンスをパケット ペイロード内で検索します。

  この例は以下のものと一致します。

- feedback.cgi
- feedback1.cgi
- feedback2.cgi
- feedback3.cgi

  この例は、以下のものとは**一致しません**。

- feedbacka.cgi
- feedback11.cgi
- feedback21.cgi
- feedbackzb.cgi
- **/^ez(\w{3,5})\.cgi/iU**

  この例では、先頭の ez の後に 3 ～ 5 文字の単語、さらに .cgi が続く文字列をパケット ペイロード内で検索します。この検索では大文字と小文字は区別されず、URI データだけが検索されます。

  この例は以下のものと一致します。

- EZBoard.cgi
- ezman.cgi
- ezadmin.cgi
- EZAdmin.cgi

  この例は、以下のものとは**一致しません**。

- ezez.cgi
- fez.cgi
- abcezboard.cgi
- ezboardman.cgi
- **/mail(file|seek)\.cgi/U**

  この例では、URI データ内の mail の後に file と seek のどちらかが続く インスタンスをパケット ペイロードで検索します。

  この例は以下のものと一致します。

- mailfile.cgi
- mailseek.cgi

  この例は、以下のものとは**一致しません**。

- MailFile.cgi
- mailfilefile.cgi
- **m?http\\x3a\x2f\x2f.*(\n|\t)+?U**

この例では、任意の数の文字の後ろにある、HTTP 要求内のタブまたは改行文字を示す URI コンテンツをパケット ペイロード内で検索します。この例では、式で `m?regex?` を使用して、`http\:\/\/` を使用しないようにしています。コロンの前にバックスラッシュがあることに注意してください。

この例は以下のものと一致します。

- `http://www.example.com?scriptvar=x&othervar=\n\..\..`
- `http://www.example.com?scriptvar=\t`

この例は、以下のものとは**一致しません**。

- `ftp://ftp.example.com?scriptvar=&othervar=\n\..\..`
- `http://www.example.com?scriptvar=|/bin/sh -i|`
- **`m?http\\x3a\x2f\x2f.*=\|.*\|+?sU`**

この例では、(改行を含む)任意の数の文字の後に 1 つの等号、さらに任意の数の文字または空白を含むパイプ文字が続くという構成の URL をパケット ペイロード内で検索します。この例では、式で `m?regex?` を使用して、`http\:\/\/` を使用しないようにしています。

この例は以下のものと一致します。

- `http://www.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?input=|cat /etc/passwd|`

この例は、以下のものとは**一致しません**。

- `ftp://ftp.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?value=x&input?|cat /etc/passwd|`
- **`/[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}/i`**

この例では、MAC アドレスをパケット ペイロード内で検索します。コロン文字がバックスラッシュでエスケープされていることに注意してください。

ルールにメタデータを追加する

ライセンス： Protection

`metadata` キーワードを使用すると、記述情報をルールに追加できます。追加した情報を使用して、ニーズに合う方法でルールを整理/識別したり、ルールを検索したりできます。

システムは次の形式に基づいてメタデータを検証します。

```
key value
```

ここで、*key* と *value* は、スペースで区切られた記述の組み合わせです。これは、Cisco提供のルールにメタデータを追加するために、Ciscoの VRT で使用されている形式です。

または、次の形式を使用することもできます。

```
key=value
```

たとえば、*key value* 形式で次のようにカテゴリとサブカテゴリを使用し、作成者と日付によってルールを識別できます。

```
author SnortGuru_20050406
```

1 つのルール内で複数の `metadata` キーワードを使用できます。また、以下の例に示すように、単一の `metadata` キーワード内で複数の *key value* ステートメントをカンマで区切ることもできます。

```
author SnortGuru_20050406, revised_by SnortUser1_20050707,
revised_by SnortUser2_20061003, revised_by
SnortUser1_20070123
```

使用できる形式は *key value* と *key=value* だけに限定されません。ただし、これらの形式に基づく検証に起因する制限事項を知っておく必要があります。

制限されている文字

ライセンス：Protection

次の文字制限に注意してください。

- `metadata` キーワード内でセミコロン(;)やコロン(:)を使用しないでください。
- カンマを使用する場合には、複数の *`key value`* または *`key=value`* ステートメントの区切り文字としてカンマが解釈されることに注意してください。次に例を示します。

```
key value, key value, key value
```

- 等号(=)または空白文字を使用する場合には、それらの文字が *`key`* と *`value`* の間の区切り文字として解釈されることに注意してください。次に例を示します。

```
key value
key=value
```

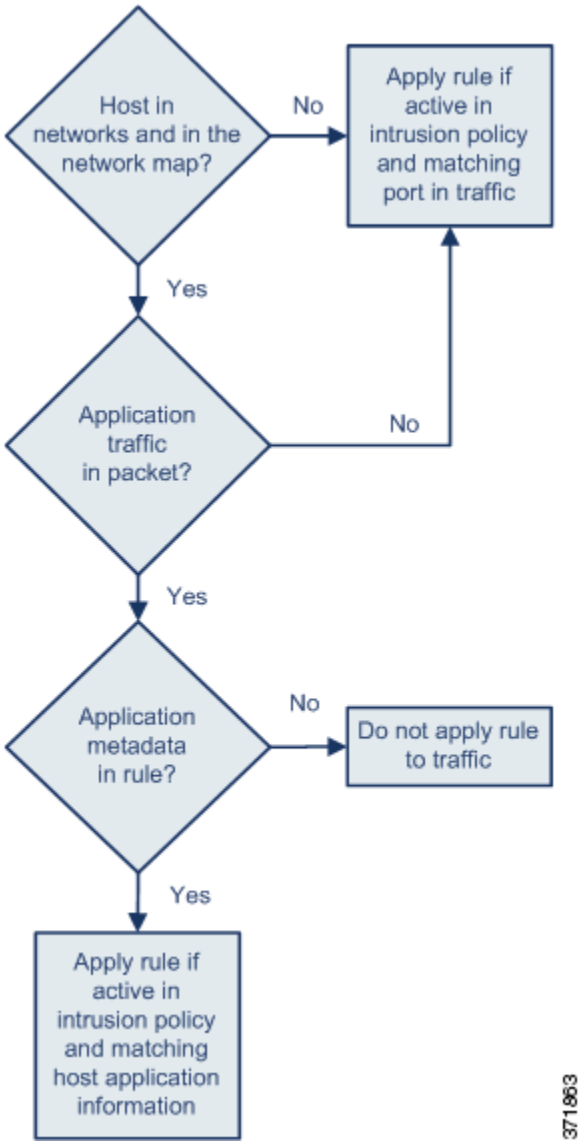
その他のすべての文字が使用可能です。

service メタデータの追加

ライセンス：Protection

ルール エンジンは、トラフィックを分析して処理するために、パケット内のホストに関するアプリケーション プロトコル情報に一致する `service` メタデータ付きのアクティブ ルールを適用します。これが一致しない場合、システムはルールをトラフィックに適用しません。ホストにアプリケーション プロトコル情報が存在しない場合、またはルールに `service` メタデータが含まれない場合、システムはルール内のポートに照らしてトラフィック内のポートを検査し、ルールをトラフィックに適用するかどうかを判断します。

次の図は、アプリケーション情報に基づくトラフィックとルールの照合を示しています。



アプリケーション プロトコルの識別によってルールを照合するには、`metadata` キーワードと *`key value`* ステートメントを定義する必要があります。その際、*`key`* として `service`、および *`value`* としてアプリケーションを指定します。たとえば、次に示す `metadata` キーワード内の *`key value`* ステートメントは、ルールを HTTP トラフィックに関連付けます。

```
service http
```

次の表では、最も一般的なアプリケーション値について説明します。

注　表に含まれないアプリケーションを定義するために支援が必要な場合は、サポート担当にお問い合わせください。

表 36-22　service 値

値	説明
dcerpc	分散コンピューティング環境/リモート プロシージャ コール システム
dns	Domain Name System; ドメイン ネーム システム
finger	Finger User Information Protocol
ftp	『File Transfer Protocol』
ftp-data	ファイル転送プロトコル(データ チャネル)
http	Hypertext Transfer Protocol
imap	Internet Message Access Protocol
isakmp	Internet Security Association and Key Management Protocol
netbios-dgm	NETBIOS Datagram Service
netbios-ns	NETBIOS Name Service
netbios-ssn	NETBIOS Session Service
nntp	Network News Transfer Protocol
oracle	Oracle Net Services
pop2	Post Office Protocol バージョン 2
pop3	Post Office Protocol バージョン 3
smtp	Simple Mail Transfer Protocol
ssh	セキュア シェル ネットワーク プロトコル
Telnet	Telnet ネットワーク プロトコル
tftp	『Trivial File Transfer Protocol』
x11	X Window システム

使用できない予約済みメタデータ

ライセンス: Protection

metadata キーワードでは、次の単語を単一の引数として、または *key value* ステートメント内のキーとして使用しないでください。これらは VRT 用に予約されています。

アプリケーション
engine
impact_flag
os
ポリシー
rule-type
rule-flushing
soid

注 ローカル ルールを適切に機能させるために制限付きメタデータをどうしても追加する必要がある場合は、サポート担当にお問い合わせください。詳細については、「ローカル ルール ファイルのインポート (66-22 ページ)」を参照してください。

メタデータを使用するルールの検索

ライセンス：Protection

metadata キーワードを使用するルールを検索するには、ルールの [Search] ページで metadata キーワードを選択して、オプションで、メタデータの一部分を入力します。たとえば次のように入力できます。

- author と入力すると、*key* として author が使用されているすべてのルールが表示されます。
- author snortguru と入力すると、*key* として author、*value* として SnortGuru がそれぞれ使用されているすべてのルールが表示されます。
- author s と入力すると、*key* として author、さらに *value* として SnortGuru、SnortUser1、SnortUser2 などの語が使用されているすべてのルールが表示されます。

ヒント　*key* と *value* の両方を検索するときには、ルール内の *key value* ステートメントで使用されているのと同じ接続演算子（等号 [=] または空白文字）を検索で使用してください。*key* の後に等号（=）と空白文字のどちらを入力するかに応じて、異なる結果が検索で返されます。

なお、メタデータ追加のために使用する形式とは無関係に、システムはメタデータ検索語を *key value* または *key=value* ステートメントの全部または一部として解釈します。たとえば、次に示すメタデータは *key value* または *key=value* 形式に従っていませんが、有効なメタデータです。

```
ab cd ef gh
```

ただし、この例に含まれる各スペースは key と value の間の区切り文字としてシステムで解釈されます。次に示す並列語や単一語を検索で使用すると、この例のメタデータを含むルールを正しく検出できます。

```
cd ef
ef gh
ef
```

一方、次の検索を使用した場合、単一の *key value* ステートメントとしてシステムによって解釈されるため、ルールを検出できません。

```
ab ef
```

詳細については、ルールの検索（36-114 ページ）を参照してください。

影響レベル 1 の設定

ライセンス：Protection

次に示す予約済み *key value* 文を metadata キーワードの中で使用できます。

```
impact_flag red
```

この *key value* ステートメントは、インポートしたローカル ルールまたはルール エディタを使って作成したカスタム ルールに関する影響フラグを赤（レベル 1）に設定します。

「送信元または宛先のホストがウイルス、トロイの木馬、その他の有害ソフトウェアによって侵害されている可能性があることを、ルールをトリガーしているパケットが示している」と判断した場合、VRT は Cisco提供のルールに impact_flag red ステートメントを含めます。詳細については、影響レベルを使用してイベントを評価する（41-39 ページ）を参照してください。

IP 見出し値の検査

ライセンス：Protection

キーワードを使用すると、パケットの IP 見出しの中で攻撃やセキュリティ ポリシー違反の可能性を識別できます。詳細については、次の項を参照してください。

フラグメント ビットと予約済みビットの検査

ライセンス： Protection

`fragbits` キーワードは、IP ヘッダーのフラグメント ビットと予約ビットを検査します。パケットごとに、予約ビット、More Fragments ビット、および Don't Fragment ビットを任意に組み合わせて検査できます。

表 36-23　Fragbits 引数の値

引数	説明
R	Reserved（予約済み）ビット
M	More Fragments ビット
D	Don’t Fragment ビット

`fragbits` キーワードを使ってルールを微調整するために、次の表に示す演算子をルール内の引数値の後ろに指定できます。

表 36-24　Fragbit 演算子

演算子	説明
プラス記号（`+`）	パケットは、指定されたすべてのビットと一致する必要があります。
アスタリスク（`*`）	パケットは、指定されたどのビットと一致することもできます。
感嘆符（`!`）	指定されたどのビットも設定されていない場合、パケットが基準を満たします。

たとえば、（他のビットの有無とは無関係に）少なくとも予約済みビットが設定されたパケットに対してイベントを生成するには、`fragbits` 値として `R+` を使用します。

IP 見出し識別値の検索

ライセンス： Protection

`id` キーワードは、IP ヘッダーのフラグメント識別フィールドを検査して、キーワード引数で指定された値と照合します。一部のサービス拒否ツールやスキャナは、このフィールドに容易に検出できる特定の番号を設定します。たとえば、Synscan ポート スキャンを検出する SID 630 では、`id` 値が `39426`（スキャナから伝送されるパケットの ID 番号として使われる静的な値）に設定されます。

注　`id` 引数値は数値でなければなりません。

指定された IP オプションの識別

ライセンス：Protection

IPopts キーワードを使用すると、指定された IP ヘッダー オプションをパケット内で検索できます。次の表に、使用可能な引数値を示します。

表 36-25　IPoption 引数

引数	説明
rr	経路を記録
eol	リストの末尾
nop	オペレーションなし
ts	タイム スタンプ
秒	IP セキュリティ オプション
lsrr	厳密でない送信元ルーティング
ssrr	厳密な送信元ルーティング
satid	ストリーム識別子

アナリストが最も頻繁に監視するのは、厳密な送信元ルーティングと厳密でない送信元ルーティングです。これらのオプションは送信元 IP アドレスのスプーフィングを示している可能性があるためです。

指定された IP プロトコル番号の識別

ライセンス：Protection

ip_proto キーワードを使用すると、キーワードの値として指定された IP プロトコルを含むパケットを識別できます。IP プロトコルは 0 ～ 255 の数値として指定できます。プロトコル番号の完全なリストについては、http://www.iana.org/assignments/protocol-numbers を参照してください。これらの番号を、<、>、または ! 演算子と組み合わせることができます。たとえば、ICMP 以外のプロトコルを使用しているトラフィックを検査するには、ip_proto キーワードの値として !1 を使用します。1 つのルール内で ip_proto キーワードを複数回にわたって使用できます。ただし、ルール エンジンはキーワードの複数インスタンスをブール和関係（AND）と解釈することに注意してください。たとえば、ip_proto:!3; ip_proto:!6 を含むルールを作成した場合、このルールは GGP プロトコルおよび TCP プロトコルを使用するトラフィックを無視します。

パケットのタイプ オブ サービスの検査

ライセンス：Protection

一部のネットワークでは、ネットワーク上を移動するパケットの優先度を設定するタイプ オブ サービス（ToS）値が使用されます。tos キーワードを使用すると、キーワードの引数で指定された値に照らしてパケットの IP 見出し ToS 値を検査できます。tos キーワードを使用するルールは、ToS が指定の値に設定され、しかもルール内の残りの基準を満たすパケットに対してトリガーとして使用されます。

注　tos の引数値は数値でなければなりません。

ToS フィールドは IP 見出し プロトコルでは非推奨になり、Differentiated Services Code Point（DSCP）フィールドに置き換えられています。

パケットの存続可能時間値の検査

ライセンス： Protection

パケットの存続可能時間（time-to-live、ttl）値は、パケットが破棄される前に生成できるホップ数を示します。ttl キーワードを使用すると、キーワードの引数として指定された値または値の範囲に照らしてパケットの IP 見出し ttl 値を検査できます。ttl キーワード パラメータを 0 や 1 などの低い値に設定すると役立つことがあります。低い存続可能時間値がトレースルートや侵入を回避する試みを示している場合があるからです（ただし、このキーワードの適切な値は、管理対象デバイスの配置やネットワーク トポロジによって異なります）。次のように構文を使用します。

- TTL 値に特定の 1 つの値を設定するには、0 ～ 255 の整数を使用します。値の前に等号（=）を付けることもできます（たとえば 5 または =5 を指定できます）。
- TTL 値の範囲を指定するには、ハイフン（-）を使用します（たとえば、0-2 は 0 ～ 2 のすべての値、-5 は 0 ～ 5 のすべての値、5- は 5 ～ 255 のすべての値をそれぞれ指定します）。
- 特定の値より大きい TTL 値を指定するには、「大なり」記号（>）を使用します（たとえば、>3 は 3 より大きいすべての値を指定します）。
- 特定の値以上の TTL 値を指定するには、「大なりイコール」記号（>=）を使用します（たとえば、>=3 は 3 以上のすべての値を指定します）。
- 特定の値より小さい TTL 値を指定するには、「小なり」記号（<）を使用します（たとえば、<3 は 3 より小さいすべての値を指定します）。
- 特定の値以下の TTL 値を指定するには、「小なりイコール」記号（<=）を使用します（たとえば、<=3 は 3 以下のすべての値を指定します）。

ICMP 見出し値の検査

ライセンス： Protection

FireSIGHT システムでサポートされるキーワードを使用すると、ICMP パケット 見出し内の攻撃やセキュリティ ポリシー違反を識別できます。なお、ほとんどの ICMP タイプおよびコードを検出する事前定義ルールがあることに注意してください。既存のルールの有効にするか、既存のルールに基づいてローカル ルールを作成することを考慮してください。ICMP ルールを最初から作成するよりも、ニーズを満たすルールを見つける方が時間の節約になる可能性があります。

ICMP 固有のキーワードの詳細については、以下の項を参照してください。

- 静的な ICMP ID 値とシーケンス値の識別（36-53 ページ）
- ICMP メッセージ タイプの検査（36-53 ページ）
- ICMP メッセージ コードの検査（36-53 ページ）

静的な ICMP ID 値とシーケンス値の識別

ライセンス：Protection

ICMP の識別番号とシーケンス番号は、ICMP 応答と ICMP 要求を関連付けるうえで役立ちます。通常のトラフィックでは、これらの値はパケットに動的に割り当てられます。一部のコバートチャネルおよび Distributed Denial of Server（DDoS）プログラムは、静的な ICMP ID およびシーケンス値を使用します。次のキーワードを使用すると、静的な値を含む ICMP パケットを識別できます。

icmp_id

`icmp_id` キーワードは、ICMP エコー要求または応答パケットの ICMP ID 番号を検査します。ICMP ID 番号に対応する数値を `icmp_id` キーワードの引数として使用してください。

icmp_seq

`icmp_seq` キーワードは、ICMP エコー要求または応答パケットの ICMP シーケンスを検査します。ICMP シーケンス番号に対応する数値を `icmp_id` キーワードの引数として使用してください。

ICMP メッセージ タイプの検査

ライセンス：Protection

`itype` キーワードを使用して、特定の ICMP メッセージ タイプ値を含むパケットを検索します。有効な ICMP タイプ値または無効な ICMP タイプ値を指定して、さまざまなタイプのトラフィックを検査できます（ICMP タイプ番号の完全なリストについては http://www.iana.org/assignments/icmp-parameters または http://www.faqs.org/rfcs/rfc792.html を参照してください）。たとえば、サービス拒否攻撃やフラッディング攻撃を発生させるために攻撃者が範囲外の ICMP タイプ値を設定することがあります。

「小なり」（<）と「大なり」（>）を使用して `itype` 引数値の範囲を指定できます。

次に例を示します。

- <35
- >36
- 3<>55

ヒント　ICMP タイプ番号の完全なリストについては、http://www.iana.org/assignments/icmp-parameters または http://www.faqs.org/rfcs/rfc792.html を参照してください。

ICMP メッセージ コードの検査

ライセンス：Protection

ICMP メッセージには、宛先が到達不能である場合の詳細を示すコード値が含まれることがあります（ICMP メッセージ コードの完全なリストと、それらを使用できる関連するメッセージ タイプについては、http://www.iana.org/assignments/icmp-parameters の第 2 項を参照してください）。

`icode` キーワードを使用すると、特定の ICMP コード値を含むパケットを識別できます。有効な ICMP コード値と無効な ICMP コード値のいずれかを指定することにより、さまざまなタイプのトラフィックを検査できます。

「小なり」（<）と「大なり」（>）を使用して `icode` 引数値の範囲を指定できます。

次に例を示します。

- 35 より小さい値を検索するには <35 と指定します。
- 36 より大きい値を検索するには >36 と指定します。
- 3 ～ 55 の間にある値を検索するには、3<>55 と指定します。

ヒント icode キーワードと itype キーワードを一緒に使用すると、両方に一致するトラフィックを識別できます。たとえば、ICMP 宛先到達不能コード タイプと ICMP ポート到達不能コード タイプを含む ICMP トラフィックを特定するには、値 3 の itype キーワード（宛先到達不能）と、値 3 の icode キーワード（ポート到達不能）を指定します。

TCP 見出し値とストリーム サイズの検査

ライセンス： Protection

FireSIGHT システムでは、パケットの TCP 見出しと TCP ストリーム サイズを使って試行される攻撃を識別するためのキーワードを使用できます。TCP 固有のキーワードの詳細については、以下の項を参照してください。

- TCP 確認応答値の検査（36-54 ページ）
- TCP フラグ組み合わせの検査（36-54 ページ）
- TCP または UDP クライアントまたはサーバ フローへのルールの適用（36-55 ページ）
- 静的な TCP シーケンス番号の識別（36-57 ページ）
- 特定のサイズの TCP ウィンドウの識別（36-57 ページ）
- 特定のサイズの TCP ストリームの識別（36-57 ページ）

TCP 確認応答値の検査

ライセンス： Protection

ack キーワードを使用して、パケットの TCP 確認応答番号と特定の値を比較できます。パケットの TCP 確認応答番号が、ack キーワードで指定された値と一致した場合に、ルールがトリガーされます。

ack の引数値は数値でなければなりません。

TCP フラグ組み合わせの検査

ライセンス： Protection

flags キーワードを使用すると、複数の TCP フラグを任意に組み合わせて指定できます。検査対象のパケットでこれらが設定されている場合、ルールがトリガーとして使用されます。

注 従来、flags の値として A+ を使用していたケースでは、代わりに flow キーワードおよび値 established を使用してください。一般に、フラグのすべての組み合わせが検出されるようにするには、フラグの使用時に flow キーワードおよび値 stateless を使用する必要があります。flow キーワードの詳細については、TCP または UDP クライアントまたはサーバ フローへのルールの適用（36-55 ページ）を参照してください。

次の表に示す flags キーワードの値を確認または無視することができます。

表 36-26　flags の引数

引数	TCP フラグ
Ack	データを確認応答します。
Psh	このパケットでデータが送信される必要があります。
Syn	新しい接続。
Urg	パケットに緊急データが含まれています。
Fin	接続が閉じられました。
Rst	接続が異常終了しました。
CWR	ECN 輻輳ウィンドウが減少しました。旧 R1 引数（下位互換性を維持するために引き続きサポートされています）。
ECE	ECN エコー。旧 R2 引数（下位互換性を維持するために引き続きサポートされています）。

ヒント　明示的輻輳通知（ECN）の詳細については、http://www.faqs.org/rfcs/rfc3168.html の情報を参照してください。

flags キーワードを使用する場合、複数のフラグに対する照合方法をシステムに指示するための演算子を使用できます。次の表に、これらの演算子の説明を示します。

表 36-27　flags と一緒に使用する演算子

演算子	説明	例
all	パケットは、指定されたすべてのフラグを含んでいる必要があります。	Urg と all を選択すると、パケットが緊急フラグを含んでいる必要があること、および他のフラグが含まれる可能性があることを指定できます。
any	パケットは、指定された任意のフラグを含むことができます。	Ack、Psh、および any を選択すると、ルールをトリガーとして使用するためには Ack と Psh のどちらか（または両方）のフラグが設定される必要があること、およびパケット内で他のフラグも設定されている可能性があることを指定できます。
not	パケットは、指定されたフラグ セットを**含んではなりません**。	Urg と not を選択すると、このルールをトリガーとして使用するパケットに関して緊急フラグが設定**されない**ことを指定できます。

TCP または UDP クライアントまたはサーバ フローへのルールの適用

ライセンス：Protection

flow キーワードを使用すると、セッション特性に基づいてルールで検査されるパケットを選択できます。flow キーワードを使用することで、ルールの適用対象となるトラフィック フロー方向を指定して、クライアント フローとサーバ フローのどちらかにルールを適用できます。flow キーワードによるパケット検査の方法を指定するには、分析すべきトラフィックの方向、検査するパケットの状態、およびパケットが再構築ストリームの一部かどうかを設定できます。

ルールの処理時に、パケットのステートフル インスペクションが実行されます。ステートレス トラフィック（セッション コンテキストが確立されていないトラフィック）を TCP ルールで無視するには、flow キーワードをルールに追加して、そのキーワードで **Established** 引数を選択する必要があります。UDP ルールでステートレス トラフィックを無視するには、flow キーワードをルールに追加して、**Established** 引数と方向引数のどちらか（または両方）を選択する必要があります。これにより、TCP または UDP ルールでパケットのステートフル インスペクションが実行されます。

方向引数を追加した場合、ルール エンジンは、指定された方向と一致するフローを伴う確立された状態のパケットだけを検査します。たとえば、TCP または UDP 接続が検出されたときトリガーとして使用されるルールに、flow キーワードおよび established 引数と From Client 引数を追加した場合、ルール エンジンはクライアントから送信されたパケットだけを検査します。

ヒント　パフォーマンスを最大にするには、必ず TCP ルールまたは UDP セッション ルールに flow キーワードを含めてください。

フローを指定するには、[Create Rule] ページの [Detection Options] リストで [flow] キーワードを選択し、[Add Option] をクリックします。次に、フィールドごとに表示されるリストから引数を選択します。

次の表は、flow キーワードで指定できるストリーム関連の引数を示しています。

表 36-28　状態に関連する flow 引数

引数	説明
Established	確立された接続でトリガーとして使用されます。
ステートレス	ストリーム プロセッサの状態に関係なくトリガーとして使用されます。

次の表に、flow キーワードで指定できる方向オプションの説明を示します。

表 36-29　flow の方向引数

引数	説明
To Client	サーバ応答でトリガーとして使用されます。
To Server	クライアント応答でトリガーとして使用されます。
From Client	クライアント応答でトリガーとして使用されます。
From Server	サーバ応答でトリガーとして使用されます。

From Server と To Client の機能が同じであること、および To Server と From Client の機能も同じであることに注意してください。これらのオプションは、ルールに文脈と読みやすさを加味するために提供されています。たとえば、サーバからクライアントへの攻撃を検出するよう設計されたルールを作成する場合は、From Server を使用します。一方、クライアントからサーバへの攻撃を検出するように設計されたルールを作成する場合は、From Client を使用します。

次の表は、flow キーワードで指定できるストリーム関連の引数を示しています。

表 36-30　flow のストリーム関連引数

引数	説明
Ignore Stream Traffic	再構築されたストリーム パケットでトリガーとして使用されません。
Only Stream Traffic	再構築されたストリーム パケットでのみトリガーとして使用されます。

たとえば、`flow` キーワードの値として `To Server, Established, Only Stream Traffic` を使用すると、ストリーム プリプロセッサで再構築された、確立済みセッションでクライアントからサーバに移動するトラフィックを検出できます。

静的な TCP シーケンス番号の識別

ライセンス：Protection

`seq` キーワードを使用すると、静的なシーケンス番号値を指定できます。パケットのシーケンス番号が、指定された引数と一致する場合、そのキーワードを含むルールがトリガーとして使用されます。このキーワードはあまり使用されませんが、静的シーケンス番号付きの生成済みパケットを使用する攻撃やネットワーク スキャンを識別するうえでこれが役立ちます。

特定のサイズの TCP ウィンドウの識別

ライセンス：Protection

`window` キーワードを使用すると、特定の TCP ウィンドウ サイズを指定できます。このキーワードを含むルールは、指定された TCP ウィンドウ サイズのパケットが検出されるたびにトリガーされます。このキーワードはあまり使用されませんが、静的 TCP ウィンドウ サイズ付きの生成済みパケットを使用する攻撃やネットワーク スキャンを識別するうえでこれが役立ちます。

特定のサイズの TCP ストリームの識別

ライセンス：Protection

次に示す形式で、`stream_size` キーワードとストリーム プリプロセッサを組み合わせて使用すると、TCP ストリームのサイズをバイト単位で特定できます。

direction,*operator*,*bytes*

ここで、*bytes* はバイト数です。引数内の各オプションはカンマ(,)で区切る必要があります。

次の表は、`stream_size` キーワードで指定できる大文字/小文字を区別しない方向オプションを示しています。

表 36-31　stream_size キーワードの方向引数

引数	説明
クライアント	指定されたストリーム サイズに一致するクライアントからのストリームでトリガーとして使用されます。
サーバ	指定されたストリーム サイズに一致するサーバからのストリームでトリガーとして使用されます。

表 36-31　stream_size キーワードの方向引数（続き）

引数	説明
both	指定されたストリーム サイズに一致するクライアントからのトラフィックとサーバからのトラフィックの両方によってトリガーとして使用されます。 たとえば `both, >, 200` という引数は、クライアントからのトラフィックが 200 バイトを超え、しかもサーバからのトラフィックが 200 バイトを超えている場合にトリガーとして使用されます。
either	指定されたストリーム サイズに一致するクライアントまたはサーバからのトラフィック（どちらか先に出現した方）によってトリガーとして使用されます。 たとえば `both, >, 200` という引数は、クライアントからのトラフィックが 200 バイトを超え、しかもサーバからのトラフィックが 200 バイトを超えている場合にトリガーとして使用されます。

次の表に、`stream_size` キーワードで使用できる演算子の説明を示します。

表 36-32　stream_size キーワードの引数演算子

Operator	説明
=	等しい
!=	等しくない
>	より大きい
<	より小さい
>=	以上
<=	以下

たとえば、クライアントからサーバに移動する 5001216 バイト以上の TCP ストリームを検出するには、`stream_size` キーワードの引数として `client, >=, 5001216` を使用できます。

TCP ストリーム再構築の有効化と無効化

ライセンス：Protection

`stream_reassemble` キーワードを使用すると、接続での検査対象トラフィックがルールの条件と一致した場合に、1 つの接続の TCP ストリーム再構築を有効/無効にすることができます。オプションで、このキーワードを 1 つのルール内で複数回使用することができます。

ストリーム再構築を有効または無効にするには、次の構文を使用します。

```
enable|disable, server|client|both, option, option
```

次の表に、`stream_reassemble` キーワードで使用できるオプション引数の説明を示します。

表 36-33　stream_reassemble のオプション引数

引数	説明
noalert	ルールで他にどの検出オプションが指定されているかに関係なく、イベントを生成しません。
fastpath	一致の検出時に残りの接続トラフィックを無視します。

たとえば、次のルールは、HTTP 応答で 200 OK ステータス コードが検出された接続に対してイベントを生成せずに、TCP クライアント側ストリームの再構築を無効にします。

```
alert tcp any 80 -> any any (flow:to_client, established; content: "200 OK";
stream_reassemble:disable, client, noalert
```

stream_reassemble を使用する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [stream_reassemble] を選択して、[Add Option] をクリックします。

[stream_reassemble] セクションが表示されます。

セッションからの SSL 情報の抽出

ライセンス： Protection

SSL ルール キーワードを使用すると、Secure Sockets Layer（SSL）プリプロセッサを呼び出し、暗号化セッションのパケットから SSL のバージョンとセッション状態に関する情報を抽出できます。

SSL または Transport Layer Security（TLS）を使用する暗号化セッションを確立するためにクライアントとサーバが通信するとき、ハンドシェイク メッセージが交換されます。セッション中に伝送されるデータは暗号化されますが、ハンドシェイク メッセージは暗号化されません。

SSL プリプロセッサは、特定のハンドシェイク フィールドから状態とバージョンの情報を抽出します。ハンドシェイク内の 2 つのフィールドは、セッション暗号化に使われる SSL または TLS のバージョンとハンドシェイクのステージを示します。

詳細については、次の項を参照してください。

- ssl_state（36-59 ページ）
- ssl_version（36-60 ページ）

ssl_state

ライセンス： Protection

`ssl_state` キーワードを使用すると、暗号化されたセッションの状態情報と照合することができます。同時に使用される複数の SSL バージョンを検査するには、1 つのルール内で複数の `ssl_version` キーワードを使用します。

ルールで `ssl_state` キーワードが使用されている場合、ルール エンジンは SSL プリプロセッサを呼び出して、トラフィック内の SSL 状態情報を検査します。

たとえば、チャレンジ長が非常に長く、データが多すぎる `ClientHello` メッセージを送信することによってサーバ上のバッファ オーバーフローを引き起そうとする攻撃者の試みを検出するには、`ssl_state` キーワードと引数 `client_hello` を使用し、異常に大きなパケットを検査することができます。

SSL 状態に関する複数の引数を指定するには、カンマ区切りリストを使用します。複数の引数を列挙した場合、システムは OR 演算子を使ってそれらを評価します。たとえば、引数として `client_hello` および `server_hello` を指定すると、システムは `client_hello` または `server_hello` のどちらかを含むトラフィックに照らしてルールを評価します。

次のように、引数を否定することもできます。

```
!client_hello,!unknown
```

接続が一連の状態のそれぞれに到達したことを確認するには、ssl_state ルール オプションを使用する複数のルールを使う必要があります。ssl_state キーワードは、次の識別子を引数として受け入れます。

表 36-34　ssl_state の引数

引数	目的
client_hello	クライアントが暗号化セッションを要求する、メッセージ タイプ ClientHello のハンドシェイク メッセージを照合します。
server_hello	クライアントからの暗号化セッション要求に対してサーバが応答する、メッセージ タイプ ServerHello のハンドシェイク メッセージを照合します。
client_keyx	サーバからのキーの受信を確認するためにクライアントがサーバにキーを伝送する、メッセージ タイプ ClientKeyExchange のハンドシェイク メッセージを照合します。
server_keyx	サーバからのキーの受信を確認するためにクライアントがサーバにキーを伝送する、メッセージ タイプ ServerKeyExchange のハンドシェイク メッセージを照合します。
unknown	任意のハンドシェイク メッセージ タイプを照合します。

ssl_version

ライセンス：Protection

ssl_version キーワードを使用すると、暗号化セッションのバージョン情報を照合できます。ルールで ssl_version キーワードが使用されている場合、ルール エンジンは SSL プリプロセッサを呼び出して、トラフィック内の SSL バージョン情報を検査します。

たとえば、SSL バージョン 2 にバッファ オーバーフロー脆弱性があることがわかっている場合、ssl_version キーワードで sslv2 引数を使用して、その SSL バージョンを使用するトラフィックを識別できます。

SSL バージョンに関する複数の引数を指定するには、カンマ区切りリストを使用します。複数の引数を列挙した場合、システムは OR 演算子を使ってそれらを評価します。たとえば、SSLv2 を使用していない暗号化トラフィックを識別するには、ssl_version:ssl_v3,tls1.0,tls1.1,tls1.2 をルールに追加できます。このルールは、SSL バージョン 3、TLS バージョン 1.0、TLS バージョン 1.1、または TLS バージョン 1.2 を使用するトラフィックを評価します。

ssl_version キーワードは、次の SSL/TLS バージョン識別子を引数として受け入れます。

表 36-35　ssl_version の引数

引数	目的
sslv2	Secure Sockets Layer（SSL）バージョン 2 を使用してエンコードされたトラフィックを照合します。
sslv3	Secure Sockets Layer（SSL）バージョン 3 を使用してエンコードされたトラフィックを照合します。
tls1.0	Transport Layer Security（TLS）バージョン 1.0 を使用してエンコードされたトラフィックを照合します。

表 36-35　ssl_version の引数（続き）

引数	目的
tls1.1	Transport Layer Security（TLS）バージョン 1.1 を使用してエンコードされたトラフィックを照合します。
tls1.2	Transport Layer Security（TLS）バージョン 1.2 を使用してエンコードされたトラフィックを照合します。

アプリケーション層プロトコル値の検査

ライセンス：Protection

アプリケーション層プロトコル値の正規化と検査はプリプロセッサによってほとんど実行されますが、以下の項で説明するキーワードを使用すると、アプリケーション層値をさらに検査できます。

- RPC（36-61 ページ）
- ASN.1（36-62 ページ）
- urilen（36-63 ページ）
- DCE/RPC キーワード（36-64 ページ）
- SIP キーワード（36-67 ページ）
- GTP キーワード（36-69 ページ）
- Modbus キーワード（36-79 ページ）
- DNP3 キーワード（36-81 ページ）

RPC

ライセンス：Protection

rpc キーワードは、TCP または UDP パケット内の Open Network Computing Remote Procedure Call（RPC ONC）サービスを識別します。これにより、ホスト上の RPC プログラムの識別試行を検出することができます。ネットワークで実行中のいずれかの RPC サービスを exploit できるかどうか判断するために、侵入者は RPC ポートマッパーを使用できます。また、ポートマッパーを使用せずに RPC を実行中の他のポートへのアクセスを試みることもできます。次の表に、rpc キーワードで使用できる引数を列挙します。

表 36-36　rpc キーワードの引数

引数	説明
アプリケーション	RPC アプリケーション番号
手順	呼び出される RPC プロシージャ
version	RPC バージョン

rpc キーワードの引数を指定するには、次の構文を使用します。

application,*procedure*,*version*

ここで、*application* は RPC アプリケーション番号、*procedure* は RPC プロシージャ番号、*version* は RPC バージョン番号です。rpc キーワードのすべての引数を指定する必要があります。引数のいずれかを指定できない場合は、アスタリスク(*)で置き換えてください。

たとえば、任意のプロシージャまたはバージョンの RPC ポートマッパー(100000 という番号で示される RPC アプリケーション)を検索するには、引数として 100000,*,* を使用します。

ASN.1

ライセンス：Protection

asn1 キーワードを使用すると、さまざまな有害エンコードを検索しながら、パケットまたはパケットの一部分をデコードできます。

次の表に、asn1 キーワードの引数について説明します。

表 36-37　asn.1 キーワードの引数

引数	説明
Bitstring Overflow	無効な、リモート exploit 可能なビットストリング エンコードを検出します。
Double Overflow	標準バッファより大きい二重 ASCII エンコードを検出します。これは Microsoft Windows のエクスプロイト可能な機能として知られていますが、現時点ではどのサービスか不明です。サービスはエクスプロイトされる可能性があります。
Oversize Length	指定された引数より大きい ASN.1 タイプ長を検出します。たとえば Oversize Length を 500 に設定した場合、500 を上回る ASN.1 タイプによってルールがトリガーとして使用されます。
Absolute Offset	パケット ペイロードの先頭からの絶対オフセットを設定します(offset カウンタがバイト 0 から始まることに注意してください)。たとえば SNMP パケットをデコードするには、Absolute Offset を 0 に設定し、Relative Offset を設定しません。Absolute Offset として正または負の値が可能です。
Relative Offset	これは、最後に見つかったコンテンツ一致、pcre、または byte_jump からの相対オフセットです。コンテンツ "foo" の直後の ASN.1 シーケンスをデコードするには、Relative Offset を 0 に設定し、Absolute Offset を設定しません。Relative Offset として正または負の値が可能です(オフセット カウンタが 0 から始まることに注意してください)。

たとえば、Microsoft ASN.1 ライブラリにおける既知の脆弱性ではバッファ オーバーフローが発生し、攻撃者は特別に細工した認証パケットを使ってその状態を exploit できます。システムが asn.1 データをデコードすると、パケット内のエクスプロイト コードがシステム レベル権限でホストで実行されたり、DoS 状態を引き起す場合があります。次のルールは、asn1 キーワードを使用して、この脆弱性を exploit する試みを検出します。

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 445
(flow:to_server, established; content:"|FF|SMB|73|"; nocase;
offset:4; depth:5;
asn1:bitstring_overflow,double_overflow,oversize_length
100,relative_offset 54;)
```

上記のルールの場合、任意のポートおよび $EXTERNAL_NET 変数で定義された任意の IP アドレスから発信され、ポート 445 を使用する $HOME_NET 変数で定義された任意の IP アドレスに向かう TCP トラフィックに対して、イベントが生成されます。加えて、サーバへの TCP 接続が確立された時点でのみルールを実行します。その後、ルールは特定の位置にある特定のコンテンツを検査します。最後に、ルールは `asn1` キーワードを使用して、ビットストリング エンコードと二重 ASCII エンコードを検出し、最後に見つかったコンテンツ一致の末尾から 55 バイト目以降、長さ 100 バイトを超える asn.1 タイプ長を識別します（`offset` カウンタがバイト 0 から始まることに注意してください）。

urilen

ライセンス：Protection

`urilen` キーワードと HTTP Inspect プリプロセッサを組み合わせて使用すると、特定の長さ、最大長を下回る、最小長を上回る、または指定された範囲内の URI を HTTP トラフィック内で検査できます。

HTTP Inspect プリプロセッサがパケットを正規化して検査した後、ルール エンジンはルールに照らしてそのパケットを評価し、`urilen` キーワードで指定された長さ条件に URI が一致するかどうか判断します。このキーワードを使用すると、URI 長の脆弱性を悪用しようとする試みを検出できます。たとえば、攻撃者は DoS 状態を引き起こしたり、システム レベル権限によりホストでコードを実行するために、バッファ オーバーフローを発生させようとします。

ルール内で `urilen` キーワードを使用するときには、次の点に注意してください。

- 必ず `flow:established` キーワードおよび他の 1 つ以上のキーワードを組み合わせて、`urilen` キーワードを使用してください。
- ルール プロトコルは常に TCP です。詳細については、「プロトコルの指定（36-5 ページ）」を参照してください。
- ターゲット ポートは常に HTTP ポートです。詳細については、侵入ルールでのポートの定義（36-9 ページ）および定義済みのデフォルトの変数の最適化（3-20 ページ）を参照してください。

URI 長を指定するときには、10 進のバイト数、「小なり」（<）、および「大なり」（>）を使用します。

次に例を示します。

- 5 バイト長の URI を検出するには、`5` を指定します。
- 5 バイト長を下回る URI を検出するには、`< 5`（1 つの空白文字で区切る）を指定します。
- 5 バイト長を上回る URI を検出するには、`> 5`（1 つの空白文字で区切る）を指定します。
- 3 ～ 5 バイト長の URI を検出するには、`3 <> 5`（`<>` の前後に空白文字を 1 つずつ含む）を指定します。

たとえば、Novell の eDirectory バージョン 8.8 に付属のサーバ モニタリングおよび診断ユーティリティ iMonitor バージョン 2.4 に脆弱性があることが知られています。長すぎる URI を含むパケットはバッファ オーバーフローを発生させます。攻撃者はそのような状況を悪用して、特別に細工したパケットをシステム レベル権限によりホスト上で実行したり、そのようなパケットで DoS 状態を引き起こしたりします。次のルールは、`urilen` キーワードを使用して、この脆弱性を悪用する試みを検出します。

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(msg:"EXPLOIT eDirectory 8.8 Long URI iMonitor buffer
overflow attempt";flow:to_server,established;
urilen:> 8192; uricontent:"/nds/"; nocase;
classtype:attempted-admin; sid:x; rev:1;)
```

上記のルールの場合、任意のポートおよび $EXTERNAL_NET 変数で定義された任意の IP アドレスから発信され、$HTTP_PORTS 変数で定義されたポートを使用して、$HOME_NET 変数で定義された任意の IP アドレスに向かう TCP トラフィックに対して、イベントが生成されます。さらに、サーバへの TCP 接続が確立された場合にのみ、パケットがルールに対して評価されます。ルールは、urilen キーワードを使用して、長さ 8192 バイトを超える URI を検出します。最後に、ルールは URI を検索して、大文字/小文字を区別しない特定のコンテンツ /nds/ を探します。

DCE/RPC キーワード

ライセンス：Protection

次の表に示す 3 つの DCE/RPC キーワードを使用すると、DCE/RPC セッション トラフィックで exploit を監視できます。これらのキーワードを含むルールを処理するとき、システムは DCE/RPC プリプロセッサを呼び出します。詳細については、「DCE/RPC トラフィックのデコード（27-2 ページ）」を参照してください。

表 36-38　DCE/RPC キーワード

使用するフィルタ	使用方法	検出対象
dce_iface	単独で	特定の DCE/RPC サービスを識別するパケット
dce_opnum	dce_iface の後ろ	特定の DCE/RPC サービス オペレーションを識別するパケット
dce_stub_data	dce_iface + dce_opnum の後ろ	特定の処理要求または応答を定義するスタブ データ

表に示されているように、dce_opnum の前に必ず dce_iface を配置し、dce_stub_data の前に必ず dce_iface + dce_opnum を配置する必要があることに注意してください。

また、これらの DCE/RPC キーワードを他のルール キーワードと組み合わせて使用することもできます。DCE/RPC ルールでは、**DCE/RPC** 引数が選択された状態で byte_jump、byte_test、byte_extract の各キーワードを使用することに注意してください。詳細については、Byte_Jump と Byte_Test の使用（36-33 ページ）およびパケット データをキーワード引数の中に読み込む（36-88 ページ）を参照してください。

Ciscoでは、DCE/RPC キーワードを含むルールに 1 つ以上の content キーワードを含めることを推奨しています。こうすると、ルール エンジンが常に高速パターン マッチ機能を使用することで処理速度が上がり、パフォーマンスが向上します。ルールに 1 つ以上の content キーワードが含まれている場合は、content キーワードの **Use Fast Pattern Matcher** 引数が有効になっているかどうかに関係なく、ルール エンジンが高速パターン マッチ機能を使用することに注意してください。詳細については、コンテンツ一致の検索（36-16 ページ）およびUse Fast Pattern Matcher（36-29 ページ）を参照してください。

次のケースでは、DCE/RPC バージョンおよび隣接見出し情報を一致コンテンツとして使用できます。

- ルールに他の content キーワードが含まれていない
- ルールにもう 1 つ content キーワードが含まれているが、DCE/RPC バージョンおよび隣接情報が、他方の content よりも特有のパターンを表している

  たとえば、DCE/RPC バージョンおよび隣接情報は通常、1 バイトのコンテンツよりも特有です。

次に示すバージョンおよび隣接情報コンテンツ一致のいずれか 1 つを使用して、ルール限定を終了する必要があります。

- コネクション型 DCE/RPC ルールでは、コンテンツ `|05 00 00|`（メジャー バージョン 05、マイナー バージョン 00、および要求 PDU（プロトコル データ ユニット）タイプ 00）を使用します。
- コネクションレス型 DCE/RPC ルールでは、コンテンツ `|04 00|`（バージョン 04、要求 PDU タイプ 00）を使用します。

いずれの場合も、DCE/RPC プリプロセッサで完了済みの処理を繰り返すことなく高速パターン マッチ機能を呼び出すために、ルール内の最後のキーワードとしてバージョンおよび隣接情報の `content` キーワードを配置してください。ルールの末尾に配置される `content` キーワードは、高速パターン マッチ機能を呼び出す手段として使われるバージョン コンテンツに当てはまりますが、ルール内の他のコンテンツ一致には必ずしも当てはまらないことに注意してください。

詳細については、次の項を参照してください。

- dce_iface（36-65 ページ）
- dce_opnum（36-66 ページ）
- dce_stub_data（36-67 ページ）

dce_iface

ライセンス： Protection

`dce_iface` キーワードを使用すると、特定の DCE/RPC サービスを識別できます。

オプションで、`dce_iface` キーワードを `dce_opnum` キーワードおよび `dce_stub_data` キーワードと組み合わせて使用すると、検査する DCE/RPC トラフィックをさらに限定することができます。詳細については、dce_opnum（36-66 ページ）およびdce_stub_data（36-67 ページ）を参照してください。

固定型 16 バイト Universally Unique Identifier（UUID）は、それぞれの DCE/RPC サービスに割り当てられているアプリケーション インターフェイスを識別します。たとえば、UUID 4b324fc8670-01d31278-5a47bf6ee188 は、srvsvc サービスとしても知られる DCE/RPC lanmanserver サービスを識別します。このサービスは、ピアツーピア プリンタ、ファイル、および SMB 名前付きパイプを共有するためのさまざまな管理機能を提供します。DCE/RPC プリプロセッサは UUID および関連する見出し値を使用して DCE/RPC セッションを追跡します。

インターフェイス UUID は、次のように、ハイフンで区切られた 5 つの 16 進文字列で構成されます。

```
<4hexbytes>-<2hexbytes>-<2hexbytes>-<2hexbytes>-<6hexbytes>
```

次に示す netlogon インターフェイスの UUID のように、ハイフンを含む UUID 全体を入力することで、インターフェイスを指定します。

```
12345678-1234-abcd-ef00-01234567cffb
```

UUID 内の最初の 3 つの文字列はビッグ エンディアン バイト順で指定される必要があることに注意してください。通常、公開されたインターフェイス リストやプロトコル アナライザには UUID が正しいバイト順で表示されますが、それを入力する前に UUID バイト順を変更しなければならない場合もあります。次に示すメッセンジャー サービス UUID の場合、リトル エンディアン バイト順の最初の 3 つの文字列を含む未加工 ASCII テキストで表示されることがあります。

```
f8 91 7b 5a 00 ff d0 11 a9 b2 00 c0 4f b6 e6 fc
```

この同じ UUID を `dce_iface` キーワードに指定するには、次のようにハイフンを挿入し、最初の 3 つの文字列をビッグ エンディアン バイト順で配置できます。

```
5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc
```

1 つの DCE/RPC セッションに複数のインターフェイスへの要求を含めることができますが、1 つのルールには 1 つの dce_iface キーワードだけを含めてください。追加のインターフェイスを検出するには、追加のルールを作成します。

DCE/RPC アプリケーション インターフェイスにはインターフェイス バージョン番号も割り当てられます。オプションで、インターフェイス バージョンを指定できます。その際、バージョンが指定値に等しい、等しくない、指定値より小さい、または大きいことを示す演算子を使用します。

TCP セグメンテーションや IP フラグメンテーションに加えて、コネクション型とコネクションレス型の両方の DCE/RPC をフラグメント化することができます。通常、先頭以外の DCE/RPC フラグメントを指定のインターフェイスに関連付けるのはあまり効率的ではありません。このようにすると、多数の誤検出が発生する可能性があります。ただし、柔軟性を維持するために、オプションで、指定されたインターフェイスに照らしてすべてのフラグメントを評価できます。

次の表に、dce_iface キーワードの引数を要約します。

表 36-39　dce_iface の引数

引数	説明
Interface UUID	DCE/RPC トラフィック内で検出対象となる特定のサービスのアプリケーション インターフェイスを識別する、ハイフンを含む UUID。指定されたインターフェイスに関連付けられたすべての要求がインターフェイス UUID に一致します。
Version	オプションで、アプリケーション インターフェイス バージョン番号 0 ～ 65535 と、検出対象のバージョンが指定値より大きい(>)、小さい(<)、等しい(=)、または等しくない(!)を示す演算子。
All Fragments	オプションで、関連するすべての DCE/RPC フラグメント内のインターフェイスの照合、およびインターフェイス バージョン(指定されている場合)での照合を有効にします。この引数はデフォルトで無効になっています。これは、最初のフラグメントまたはフラグメント化されていないパケット全体が指定のインターフェイスに関連付けられている場合にのみ、キーワードが一致することを意味します。この引数を有効にすると、誤検出が発生する可能性があることに注意してください。

dce_opnum

ライセンス：Protection

dce_opnum キーワードを DCE/RPC プリプロセッサと組み合わせて使用すると、DCE/RPC サービスが提供する 1 つ以上の特定のオペレーションを識別するパケットを検出できます。

クライアント関数呼び出しは、DCE/RPC 仕様で「*オペレーション*」と呼ばれる特定のサービス関数を要求します。オペレーション番号(opnum)は DCE/RPC 見出し内の特定のオペレーションを識別します。exploit は特定のオペレーションを標的にすることがあります。

たとえば UUID 12345678-1234-abcd-ef00-01234567cffb は、数十種類のオペレーションを提供する netlogon サービスのインターフェイスを識別します。その 1 つがオペレーション 6 (NetrServerPasswordSet オペレーション)です。

オペレーション用のサービスを識別するには、dce_opnum キーワードの前に dce_iface キーワードを指定する必要があります。詳細については、「dce_iface (36-65 ページ)」を参照してください。

特定のオペレーションを示す 1 つの 10 進数値(0 ～ 65535)、ハイフンで区切ったオペレーション範囲、またはカンマで区切ったオペレーション/範囲のリストを任意の順序で指定できます。

次の例は、すべて有効な netlogon オペレーション番号を表しています。

```
15
15-18
15, 18-20
15, 20-22, 17
15, 18-20, 22, 24-26
```

dce_stub_data

ライセンス：Protection

dce_stub_data キーワードを DCE/RPC プリプロセッサと組み合わせて使用すると、他のルール オプションとは無関係に、スタブ データの先頭からインスペクションを開始するようルール エンジンに指示できます。dce_stub_data キーワードの後に続くパケット ペイロード ルール オプションは、スタブ データ バッファを基準にして適用されます。

DCE/RPC スタブ データは、クライアント プロシージャ コールと DCE/RPC ランタイム システム（DCE/RPC の中核をなすルーチンとサービスを提供するメカニズム）の間にインターフェイスを提供します。DCE/RPC exploit は、DCE/RPC パケットのスタブ データ部分で識別されます。スタブ データは特定のオペレーションまたは関数呼び出しに関連付けられているため、必ず dce_stub_data の前に dce_iface と dce_opnum を指定して、関連するサービスとオペレーションを識別してください。

dce_stub_data キーワードには引数がありません。詳細については、dce_iface（36-65 ページ）および dce_opnum（36-66 ページ）を参照してください。

SIP キーワード

ライセンス：Protection

4 つの SIP キーワードを使用すると、SIP セッション トラフィックで exploit を監視できます。

SIP プロトコルはサービス拒否（DoS）攻撃に対して脆弱であることに注意してください。このような攻撃に対処するルールでは、レートベース攻撃防御機能を活用できます。詳細については、動的ルール状態の追加（32-33 ページ）およびレート ベース攻撃の防止（34-10 ページ）を参照してください。

詳細については、次の項を参照してください。

- sip_header（36-67 ページ）
- sip_body（36-68 ページ）
- sip_method（36-68 ページ）
- sip_stat_code（36-69 ページ）

sip_header

ライセンス：Protection

sip_header キーワードを使用すると、抽出された SIP 要求または応答見出しの先頭から検査を開始し、検査対象を見出し フィールドに限定することができます。

sip_header キーワードには引数がありません。詳細については、sip_method（36-68 ページ）および sip_stat_code（36-69 ページ）を参照してください。

次のサンプル ルール フラグメントは SIP 見出しを指し示し、CSeq 見出し フィールドに一致します。

```
alert udp any any -> any 5060 ( sip_header; content:"CSeq"; )
```

sip_body

ライセンス：Protection

sip_body キーワードを使用すると、抽出された SIP 要求または応答メッセージ本文の先頭から検査を開始し、検査対象をメッセージ本文に限定することができます。

sip_body キーワードには引数がありません。

次のサンプル ルール フラグメントは SIP メッセージ本文を指し示し、抽出された SDP データの c（接続情報）フィールド内の特定の IP アドレスに一致します。

```
alert udp any any -> any 5060 ( sip_body; content:"c=IN 192.168.12.14"; )
```

ルールが SDP コンテンツの検索だけに限定されないことに注意してください。SIP プリプロセッサはメッセージ本文全体を抽出し、それをルール エンジンで使用できるようにします。

sip_method

ライセンス：Protection

各 SIP 要求内の *method* フィールドは要求の目的を識別します。sip_method キーワードを使用すると、SIP 要求の中で特定のメソッドを検査することができます。複数のメソッドはカンマで区切ります。

次に示す、現在定義されている任意の SIP メソッドを指定できます。

```
ack、benotify、bye、cancel、do、info、invite、join、message、notify、options、prack、publish、quath、
refer、register、service、sprack、subscribe、unsubscribe、update
```

メソッドでは大文字と小文字が区別されません。複数のメソッドをカンマで区切ることができます。

今後、新しい SIP メソッドが定義される可能性があるため、カスタム メソッド、つまり現在定義されている SIP メソッド以外のメソッドを指定することもできます。可能なフィールド値は RFC 2616 で定義されています。=、(、) などの制御文字と区切り文字を除いて、すべての文字を使用できます。除外されている区切り文字の完全なリストについては、RFC 2616 を参照してください。指定されたカスタム メソッドがトラフィックで検出されると、システムはパケット 見出しを検査しますが、メッセージは検査されません。

現在定義されている 21 個のメソッドと追加の 11 個のメソッドを含む、最大 32 個のメソッドがシステムでサポートされます。未定義のメソッドを設定した場合、システムはそれを無視します。合計 32 個のメソッドには、**Methods to Check** SIP プリプロセッサ オプションを使って指定されるメソッドが含まれることに注意してください。詳細については、「SIP プリプロセッサ オプションの選択（27-51 ページ）」を参照してください。

否定を使用する場合は、1 つのメソッドだけを指定できます。次に例を示します。

```
!invite
```

ただし、1 つのルール内の複数の sip_method キーワードが **AND** 演算で結合されることに注意してください。たとえば、invite と cancel を除くすべての抽出されたメソッドを検査するには、次のような 2 つの否定付き sip_method キーワードを使用します。

```
sip_method: !invite
sip_method: !cancel
```

Ciscoでは、sip_method キーワードを含むルールに 1 つ以上の content キーワードを含めることを推奨しています。こうすると、ルール エンジンが常に高速パターン マッチ機能を使用することで処理速度が上がり、パフォーマンスが向上します。ルールに 1 つ以上の content キーワードが含まれている場合は、content キーワードの **Use Fast Pattern Matcher** 引数が有効になっているかどうかに関係なく、ルール エンジンが高速パターン マッチ機能を使用することに注意してください。詳細については、コンテンツ一致の検索（36-16 ページ）およびUse Fast Pattern Matcher（36-29 ページ）を参照してください。

sip_stat_code

ライセンス：Protection

各 SIP 応答内の 3 桁のステータス コードは、要求されたアクションの結果を示します。sip_stat_code キーワードを使用すると、SIP 応答の中で特定のステータス コードを検査することができます。

1 桁の応答タイプ番号（1 ～ 9）、特定の 3 桁の番号（100 ～ 999）、またはこれらを任意に組み合わせたカンマ区切りリストを指定できます。リスト内のいずれか 1 つの番号が SIP 応答内のコードに一致する場合、そのリストが一致します。

次の表に、指定可能な SIP ステータス コード値の説明を示します。

表 36-40　sip_stat_code 値

検出対象	指定する内容	例	検出結果
1 つの特定のステータス コード	3 桁のステータス コード	189	189
指定された 1 つの数字から始まる 3 桁のコード	1 桁	1	1xx、つまり 100、101、102 など
値のリスト	特定のコードと 1 つの数字を任意に組み合わせてカンマで区切ったもの	222, 3	222 および 300、301、302 など

また、ルールに content キーワードが含まれているかどうかに関係なく、sip_stat_code キーワードを使って指定された値を検索するためにルール エンジンが高速パターン マッチ機能を使用しないことにも注意してください。

GTP キーワード

ライセンス：Protection

3 つの GSRP トンネリング プロトコル（GTP）キーワードを使用すると、GTP バージョン、メッセージ タイプ、および情報要素をコマンド チャネル内で検査できます。content や byte_jump などの他の侵入ルール キーワードと組み合わせて GTP キーワードを使用することはできません。gtp_info または gtp_type キーワードを使用するそれぞれのルールで、gtp_version キーワードを使用する必要があります。

詳細については、次の項を参照してください。

- gtp_version（36-69 ページ）
- gtp_type（36-70 ページ）
- gtp_info（36-74 ページ）

gtp_version

gtp_version キーワードを使用すると、GTP 制御メッセージの中で GTP バージョン 0、1、または 2 を検査することができます。

定義されているメッセージ タイプと情報要素は GTP バージョンによって異なるため、gtp_type または gtp_info キーワードを使用するときには、このキーワードを使用する必要があります。値として 0、1、または 2 を指定できます。

GTP バージョンを指定する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [gtp_version] を選択して、[Add Option] をクリックします。

`gtp_version` キーワードが表示されます。

ステップ 2　GTP バージョンを特定するために、`0`、`1`、または `2` を指定します。

gtp_type

それぞれの GTP メッセージは、数値と文字列で構成されるメッセージ タイプによって識別されます。`gtp_type` キーワードを `gtp_version` キーワードと組み合わせて使用すると、トラフィック内で特定の GTP メッセージ タイプを検査できます。

次の例に示すように、メッセージ タイプとして定義済みの 10 進数値、定義済みの文字列、あるいはどちらか（または両方）を任意に組み合わせたカンマ区切りリストを指定できます。

```
10, 11, echo_request
```

リスト内のそれぞれの値または文字列を照合するとき、システムは OR 演算を使用します。値と文字列を列挙する順序は重要ではありません。リスト内のいずれか 1 つの値または文字列の一致により、キーワードが一致します。認識されない文字列または範囲外の値を含むルールを保存しようとすると、エラーが発生します。

表に示されているように、GTP バージョンに応じて、同じメッセージ タイプの値が異なる場合があることに注意してください。たとえば `sgsn_context_request` メッセージ タイプの値は GTPv0 と GTPv1 では 50 ですが、GTPv2 では 130 です。

パケット内のバージョン番号に応じて、`gtp_type` キーワードは異なる値と一致します。上記の例の場合、GTPv0 または GTPv1 パケットではキーワードがメッセージ タイプ値 50 と一致しますが、GTPv2 パケットでは値 130 と一致します。パケット内のメッセージ タイプ値が、パケットで指定されたバージョンの既知の値でない場合は、キーワードがパケットと一致しません。

メッセージ タイプに整数を指定した場合、パケット内で指定されたバージョンとは無関係に、キーワード内のメッセージ タイプが GTP パケット内の値と一致すればキーワードが一致します。

次の表に、GTP メッセージ タイプごとにシステムで認識される定義済みの値と文字列を示します。

表 36-41　GTP メッセージ タイプ

値	バージョン 0	バージョン 1	バージョン 2
1	echo_request	echo_request	echo_request
2	echo_response	echo_response	echo_response
3	version_not_supported	version_not_supported	version_not_supported
4	node_alive_request	node_alive_request	該当なし
5	node_alive_response	node_alive_response	該当なし
6	redirection_request	redirection_request	該当なし
7	redirection_response	redirection_response	該当なし
16	create_pdp_context_request	create_pdp_context_request	該当なし

表 36-41　GTP メッセージ タイプ（続き）

値	バージョン 0	バージョン 1	バージョン 2
17	create_pdp_context_response	create_pdp_context_response	該当なし
18	update_pdp_context_request	update_pdp_context_request	該当なし
19	update_pdp_context_response	update_pdp_context_response	該当なし
20	delete_pdp_context_request	delete_pdp_context_request	該当なし
21	delete_pdp_context_response	delete_pdp_context_response	該当なし
22	create_aa_pdp_context_request	init_pdp_context_activation_request	該当なし
23	create_aa_pdp_context_response	init_pdp_context_activation_response	該当なし
24	delete_aa_pdp_context_request	該当なし	該当なし
25	delete_aa_pdp_context_response	該当なし	該当なし
26	error_indication	error_indication	該当なし
27	pdu_notification_request	pdu_notification_request	該当なし
28	pdu_notification_response	pdu_notification_response	該当なし
29	pdu_notification_reject_request	pdu_notification_reject_request	該当なし
30	pdu_notification_reject_response	pdu_notification_reject_response	該当なし
31	該当なし	supported_ext_header_notification	該当なし
32	send_routing_info_request	send_routing_info_request	create_session_request
33	send_routing_info_response	send_routing_info_response	create_session_response
34	failure_report_request	failure_report_request	modify_bearer_request
35	failure_report_response	failure_report_response	modify_bearer_response
36	note_ms_present_request	note_ms_present_request	delete_session_request
37	note_ms_present_response	note_ms_present_response	delete_session_response
38	該当なし	該当なし	change_notification_request
39	該当なし	該当なし	change_notification_response
48	identification_request	identification_request	該当なし
49	identification_response	identification_response	該当なし
50	sgsn_context_request	sgsn_context_request	該当なし
51	sgsn_context_response	sgsn_context_response	該当なし
52	sgsn_context_ack	sgsn_context_ack	該当なし
53	該当なし	forward_relocation_request	該当なし
54	該当なし	forward_relocation_response	該当なし
55	該当なし	forward_relocation_complete	該当なし
56	該当なし	relocation_cancel_request	該当なし
57	該当なし	relocation_cancel_response	該当なし
58	該当なし	forward_srns_contex	該当なし
59	該当なし	forward_relocation_complete_ack	該当なし
60	該当なし	forward_srns_contex_ack	該当なし

表 36-41　GTP メッセージ タイプ（続き）

値	バージョン 0	バージョン 1	バージョン 2
64	該当なし	該当なし	modify_bearer_command
65	該当なし	該当なし	modify_bearer_failure_indication
66	該当なし	該当なし	delete_bearer_command
67	該当なし	該当なし	delete_bearer_failure_indication
68	該当なし	該当なし	bearer_resource_command
69	該当なし	該当なし	bearer_resource_failure_indication
70	該当なし	ran_info_relay	downlink_failure_indication
71	該当なし	該当なし	trace_session_activation
72	該当なし	該当なし	trace_session_deactivation
73	該当なし	該当なし	stop_paging_indication
95	該当なし	該当なし	create_bearer_request
96	該当なし	mbms_notification_request	create_bearer_response
97	該当なし	mbms_notification_response	update_bearer_request
98	該当なし	mbms_notification_reject_request	update_bearer_response
99	該当なし	mbms_notification_reject_response	delete_bearer_request
100	該当なし	create_mbms_context_request	delete_bearer_response
101	該当なし	create_mbms_context_response	delete_pdn_request
102	該当なし	update_mbms_context_request	delete_pdn_response
103	該当なし	update_mbms_context_response	該当なし
104	該当なし	delete_mbms_context_request	該当なし
105	該当なし	delete_mbms_context_response	該当なし
112	該当なし	mbms_register_request	該当なし
113	該当なし	mbms_register_response	該当なし
114	該当なし	mbms_deregister_request	該当なし
115	該当なし	mbms_deregister_response	該当なし
116	該当なし	mbms_session_start_request	該当なし
117	該当なし	mbms_session_start_response	該当なし
118	該当なし	mbms_session_stop_request	該当なし
119	該当なし	mbms_session_stop_response	該当なし
120	該当なし	mbms_session_update_request	該当なし
121	該当なし	mbms_session_update_response	該当なし
128	該当なし	ms_info_change_request	identification_request
129	該当なし	ms_info_change_response	identification_response
130	該当なし	該当なし	sgsn_context_request
131	該当なし	該当なし	sgsn_context_response
132	該当なし	該当なし	sgsn_context_ack

表 36-41　GTP メッセージ タイプ(続き)

値	バージョン 0	バージョン 1	バージョン 2
133	該当なし	該当なし	forward_relocation_request
134	該当なし	該当なし	forward_relocation_response
135	該当なし	該当なし	forward_relocation_complete
136	該当なし	該当なし	forward_relocation_complete_ack
137	該当なし	該当なし	forward_access
138	該当なし	該当なし	forward_access_ack
139	該当なし	該当なし	relocation_cancel_request
140	該当なし	該当なし	relocation_cancel_response
141	該当なし	該当なし	configuration_transfer_tunnel
149	該当なし	該当なし	detach
150	該当なし	該当なし	detach_ack
151	該当なし	該当なし	cs_paging
152	該当なし	該当なし	ran_info_relay
153	該当なし	該当なし	alert_mme
154	該当なし	該当なし	alert_mme_ack
155	該当なし	該当なし	ue_activity
156	該当なし	該当なし	ue_activity_ack
160	該当なし	該当なし	create_forward_tunnel_request
161	該当なし	該当なし	create_forward_tunnel_response
162	該当なし	該当なし	suspend
163	該当なし	該当なし	suspend_ack
164	該当なし	該当なし	resume
165	該当なし	該当なし	resume_ack
166	該当なし	該当なし	create_indirect_forward_tunnel_request
167	該当なし	該当なし	create_indirect_forward_tunnel_response
168	該当なし	該当なし	delete_indirect_forward_tunnel_request
169	該当なし	該当なし	delete_indirect_forward_tunnel_response
170	該当なし	該当なし	release_access_bearer_request
171	該当なし	該当なし	release_access_bearer_response
176	該当なし	該当なし	downlink_data
177	該当なし	該当なし	downlink_data_ack
179	該当なし	該当なし	pgw_restart
180	該当なし	該当なし	pgw_restart_ack
200	該当なし	該当なし	update_pdn_request
201	該当なし	該当なし	update_pdn_response
211	該当なし	該当なし	modify_access_bearer_request

表 36-41　GTP メッセージ タイプ（続き）

値	バージョン 0	バージョン 1	バージョン 2
212	該当なし	該当なし	modify_access_bearer_response
231	該当なし	該当なし	mbms_session_start_request
232	該当なし	該当なし	mbms_session_start_response
233	該当なし	該当なし	mbms_session_update_request
234	該当なし	該当なし	mbms_session_update_response
235	該当なし	該当なし	mbms_session_stop_request
236	該当なし	該当なし	mbms_session_stop_response
240	data_record_transfer_request	data_record_transfer_request	該当なし
241	data_record_transfer_response	data_record_transfer_response	該当なし
254	該当なし	end_marker	該当なし
255	pdu	pdu	該当なし

GTP メッセージ タイプを指定する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [gtp_type] を選択して、[Add Option] をクリックします。

`gtp_type` キーワードが表示されます。

ステップ 2　メッセージ タイプとして定義済みの 10 進数値（0 ～ 255 の範囲）、定義済み文字列、あるいはそのいずれか（または両方）を任意に組み合わせたカンマ区切りリストを指定します。システムで認識される値と文字列については、GTP メッセージ タイプの表を参照してください。

gtp_info

1 つの GTP メッセージには多数の情報要素が含まれることがあり、それぞれの要素は定義済み数値および定義済み文字列によって識別されます。`gtp_info` キーワードを `gtp_version` キーワードと組み合わせて使用すると、指定された情報要素の先頭から検査を開始し、検査対象を指定の情報要素に限定することができます。

情報要素に対して定義された 10 進数値と定義された文字列のどちらでも指定できます。単一の値または文字列を指定することも、1 つのルール内で複数の `gtp_info` キーワードを使って複数の情報要素を検査することもできます。

1 つのメッセージに同じタイプの複数の情報要素が含まれている場合は、すべてが照合対象として検査されます。情報要素が無効な順序で出現する場合は、最後のインスタンスだけが検査されます。

GTP バージョンに応じて、同じ情報要素の値が異なる場合があることに注意してください。たとえば `cause` 情報要素の値は GTPv0 と GTPv1 では 1 ですが、GTPv2 では 2 です。

パケット内のバージョン番号に応じて、`gtp_info` キーワードは異なる値と一致します。上記の例の場合、GTPv0 または GTPv1 パケットではキーワードが情報要素値 1 と一致しますが、GTPv2 パケットでは値 2 と一致します。パケット内の情報要素値が、パケットで指定されたバージョンの既知の値でない場合は、キーワードがパケットと一致しません。

情報要素に整数を指定した場合、パケット内で指定されたバージョンとは無関係に、キーワード内のメッセージ タイプが GTP パケット内の値と一致すればキーワードが一致します。

次の表に、GTP 情報要素ごとにシステムで認識される値と文字列を示します。

表 36-42　GTP 情報要素

値	バージョン 0	バージョン 1	バージョン 2
1	cause	cause	imsi
2	imsi	imsi	cause
3	rai	rai	recovery
4	tlli	tlli	該当なし
5	p_tmsi	p_tmsi	該当なし
6	qos	該当なし	該当なし
8	recording_required	recording_required	該当なし
9	認証	認証	該当なし
11	map_cause	map_cause	該当なし
12	p_tmsi_sig	p_tmsi_sig	該当なし
13	ms_validated	ms_validated	該当なし
14	recovery	recovery	該当なし
15	selection_mode	selection_mode	該当なし
16	flow_label_data_1	teid_1	該当なし
17	flow_label_signalling	teid_control	該当なし
18	flow_label_data_2	teid_2	該当なし
19	ms_unreachable	teardown_ind	該当なし
20	該当なし	nsapi	該当なし
21	該当なし	ranap	該当なし
22	該当なし	rab_context	該当なし
23	該当なし	radio_priority_sms	該当なし
24	該当なし	radio_priority	該当なし
25	該当なし	packet_flow_id	該当なし
26	該当なし	charging_char	該当なし
27	該当なし	trace_ref	該当なし
28	該当なし	trace_type	該当なし
29	該当なし	ms_unreachable	該当なし
71	該当なし	該当なし	apn
72	該当なし	該当なし	ambr
73	該当なし	該当なし	ebi
74	該当なし	該当なし	ip_addr
75	該当なし	該当なし	mei
76	該当なし	該当なし	msisdn

表 36-42　GTP 情報要素（続き）

値	バージョン 0	バージョン 1	バージョン 2
77	該当なし	該当なし	indication
78	該当なし	該当なし	pco
79	該当なし	該当なし	paa
80	該当なし	該当なし	bearer_qos
80	該当なし	該当なし	flow_qos
82	該当なし	該当なし	rat_type
83	該当なし	該当なし	serving_network
84	該当なし	該当なし	bearer_tft
85	該当なし	該当なし	tad
86	該当なし	該当なし	uli
87	該当なし	該当なし	f_teid
88	該当なし	該当なし	tmsi
89	該当なし	該当なし	cn_id
90	該当なし	該当なし	s103pdf
91	該当なし	該当なし	s1udf
92	該当なし	該当なし	delay_value
93	該当なし	該当なし	bearer_context
94	該当なし	該当なし	charging_id
95	該当なし	該当なし	charging_char
96	該当なし	該当なし	trace_info
97	該当なし	該当なし	bearer_flag
99	該当なし	該当なし	pdn_type
100	該当なし	該当なし	pti
101	該当なし	該当なし	drx_parameter
103	該当なし	該当なし	gsm_key_tri
104	該当なし	該当なし	umts_key_cipher_quin
105	該当なし	該当なし	gsm_key_cipher_quin
106	該当なし	該当なし	umts_key_quin
107	該当なし	該当なし	eps_quad
108	該当なし	該当なし	umts_key_quad_quin
109	該当なし	該当なし	pdn_connection
110	該当なし	該当なし	pdn_number
111	該当なし	該当なし	p_tmsi
112	該当なし	該当なし	p_tmsi_sig
113	該当なし	該当なし	hop_counter
114	該当なし	該当なし	ue_time_zone

表 36-42　GTP 情報要素（続き）

値	バージョン 0	バージョン 1	バージョン 2
115	該当なし	該当なし	trace_ref
116	該当なし	該当なし	complete_request_msg
117	該当なし	該当なし	guti
118	該当なし	該当なし	f_container
119	該当なし	該当なし	f_cause
120	該当なし	該当なし	plmn_id
121	該当なし	該当なし	target_id
123	該当なし	該当なし	packet_flow_id
124	該当なし	該当なし	rab_contex
125	該当なし	該当なし	src_rnc_pdcp
126	該当なし	該当なし	udp_src_port
127	charge_id	charge_id	apn_restriction
128	end_user_address	end_user_address	selection_mode
129	mm_context	mm_context	src_id
130	pdp_context	pdp_context	該当なし
131	apn	apn	change_report_action
132	protocol_config	protocol_config	fq_csid
133	gsn	gsn	channel
134	msisdn	msisdn	emlpp_pri
135	該当なし	qos	node_type
136	該当なし	authentication_qu	fqdn
137	該当なし	tft	ti
138	該当なし	target_id	mbms_session_duration
139	該当なし	utran_trans	mbms_service_area
140	該当なし	rab_setup	mbms_session_id
141	該当なし	ext_header	mbms_flow_id
142	該当なし	trigger_id	mbms_ip_multicast
143	該当なし	omc_id	mbms_distribution_ack
144	該当なし	ran_trans	rfsp_index
145	該当なし	pdp_context_pri	uci
146	該当なし	addi_rab_setup	csg_info
147	該当なし	sgsn_number	csg_id
148	該当なし	common_flag	cmi
149	該当なし	apn_restriction	service_indicator
150	該当なし	radio_priority_lcs	detach_type
151	該当なし	rat_type	ldn

表 36-42　GTP 情報要素（続き）

値	バージョン 0	バージョン 1	バージョン 2
152	該当なし	user_loc_info	node_feature
153	該当なし	ms_time_zone	mbms_time_to_transfer
154	該当なし	imei_sv	スロットリング
155	該当なし	camel	arp
156	該当なし	mbms_ue_context	epc_timer
157	該当なし	tmp_mobile_group_id	signalling_priority_indication
158	該当なし	rim_routing_addr	tmgi
159	該当なし	mbms_config	mm_srvcc
160	該当なし	mbms_service_area	flags_srvcc
161	該当なし	src_rnc_pdcp	nmbr
162	該当なし	addi_trace_info	該当なし
163	該当なし	hop_counter	該当なし
164	該当なし	plmn_id	該当なし
165	該当なし	mbms_session_id	該当なし
166	該当なし	mbms_2g3g_indicator	該当なし
167	該当なし	enhanced_nsapi	該当なし
168	該当なし	mbms_session_duration	該当なし
169	該当なし	addi_mbms_trace_info	該当なし
170	該当なし	mbms_session_repetition_num	該当なし
171	該当なし	mbms_time_to_data	該当なし
173	該当なし	bss	該当なし
174	該当なし	cell_id	該当なし
175	該当なし	pdu_num	該当なし
177	該当なし	mbms_bearer_capab	該当なし
178	該当なし	rim_routing_disc	該当なし
179	該当なし	list_pfc	該当なし
180	該当なし	ps_xid	該当なし
181	該当なし	ms_info_change_report	該当なし
182	該当なし	direct_tunnel_flags	該当なし
183	該当なし	correlation_id	該当なし
184	該当なし	bearer_control_mode	該当なし
185	該当なし	mbms_flow_id	該当なし
186	該当なし	mbms_ip_multicast	該当なし
187	該当なし	mbms_distribution_ack	該当なし
188	該当なし	reliable_inter_rat_handover	該当なし
189	該当なし	rfsp_index	該当なし

表 36-42　GTP 情報要素（続き）

値	バージョン 0	バージョン 1	バージョン 2
190	該当なし	fqdn	該当なし
191	該当なし	evolved_allocation1	該当なし
192	該当なし	evolved_allocation2	該当なし
193	該当なし	extended_flags	該当なし
194	該当なし	uci	該当なし
195	該当なし	csg_info	該当なし
196	該当なし	csg_id	該当なし
197	該当なし	cmi	該当なし
198	該当なし	apn_ambr	該当なし
199	該当なし	ue_network	該当なし
200	該当なし	ue_ambr	該当なし
201	該当なし	apn_ambr_nsapi	該当なし
202	該当なし	ggsn_backoff_timer	該当なし
203	該当なし	signalling_priority_indication	該当なし
204	該当なし	signalling_priority_indication_nsapi	該当なし
205	該当なし	high_bitrate	該当なし
206	該当なし	max_mbr	該当なし
251	charging_gateway_addr	charging_gateway_addr	該当なし
255	private_extension	private_extension	private_extension

GTP 情報要素を指定するには、次の手順に従います。

GTP 情報要素を指定する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [gtp_info] を選択して、[Add Option] をクリックします。

`gtp_info` キーワードが表示されます。

ステップ 2　情報要素に関する 1 つの定義済み 10 進数値（0 ～ 255）または 1 つの定義済み文字列を指定します。システムで認識される値と文字列については、GTP 情報要素の表を参照してください。

Modbus キーワード

ライセンス：Protection

Modbus キーワードを使用すると、Modbus 要求または応答内の Data フィールドの先頭を指し示したり、Modbus 機能コードと照合したり、Modbus ユニット ID と照合することができます。Modbus キーワードを単独で使用することも、`content` や `byte_jump` など他のキーワードと組み合わせて使用することもできます。

詳細については、次の項を参照してください。

- modbus_data（36-80 ページ）
- modbus_func（36-80 ページ）
- modbus_unit（36-81 ページ）

modbus_data

modbus_data キーワードを使用すると、Modbus 要求または応答内の Data フィールドの先頭を指し示すすことができます。

Modbus Data フィールドの先頭を指し示すには:

アクセス: Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [modbus_data] を選択して、[Add Option] をクリックします。

modbus_data キーワードが表示されます。

modbus_data キーワードには引数がありません。

modbus_func

modbus_func キーワードを使用すると、Modbus アプリケーション層要求または応答見出し内の Function Code（機能コード）フィールドを照合できます。Modbus 機能コードとして、1 つの定義済み 10 進数値または 1 つの定義済み文字列を指定できます。

次の表に、Modbus 機能コードとしてシステムで認識される定義済みの値と文字列を示します。

表 36-43　Modbus 機能コード

値	文字列
1	read_coils
2	read_discrete_inputs
3	read_holding_registers
4	read_input_registers
5	write_single_coil
6	write_single_register
7	read_exception_status
8	diagnostics
11	get_comm_event_counter
12	get_comm_event_log
15	write_multiple_coils
16	write_multiple_registers
17	report_slave_id
20	read_file_record
21	write_file_record

表 36-43　Modbus 機能コード（続き）

値	文字列
22	mask_write_register
23	read_write_multiple_registers
24	read_fifo_queue
43	encapsulated_interface_transport

Modbus 機能コードを指定する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [modbus_func] を選択して、[Add Option] をクリックします。

`modbus_func` キーワードが表示されます。

ステップ 2　機能コード用の 1 つの定義済み 10 進数値（0 ～ 255）または 1 つの定義済み文字列を指定します。システムで認識される値と文字列については、Modbus 機能コードの表を参照してください。

modbus_unit

`modbus_unit` キーワードを使用すると、Modbus 要求または応答見出し内の Unit ID フィールドで 1 つの 10 進数値を照合できます。

Modbus ユニット ID を指定する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [modbus_unit] を選択して、[Add Option] をクリックします。

`modbus_unit` キーワードが表示されます。

ステップ 2　10 進数値（0 ～ 255 の範囲）を 1 つ指定します。

DNP3 キーワード

ライセンス：Protection

DNP3 キーワードを使用すると、アプリケーション層フラグメントの先頭を指し示したり、DNP3 要求および応答での DNP3 機能コードやオブジェクトを照合したり、DNP3 応答での内部通知フラグを照合することができます。DNP3 キーワードを単独で使用することも、`content` や `byte_jump` などの他のキーワードと組み合わせて使用することもできます。

詳細については、次の項を参照してください。

- dnp3_data（36-82 ページ）
- dnp3_func（36-82 ページ）
- dnp3_ind（36-83 ページ）
- dnp3_obj（36-84 ページ）

dnp3_data

dnp3_data キーワードを使用すると、再構築された DNP3 アプリケーション層フラグメントの先頭を指し示すことができます。

DNP3 プリプロセッサが、リンク層フレームをアプリケーション層フラグメントに再構築します。dnp3_data キーワードは、各アプリケーション層フラグメントの先頭を指し示します。他のルール オプションは、16 バイトごとにデータを分離してチェックサムを追加せずに、フラグメント内の再構築されたデータを照合することができます。

再構築された DNP3 フラグメントの先頭を指すには:

アクセス: Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [modbus_data] を選択して、[Add Option] をクリックします。

dnp3_data キーワードが表示されます。

dnp3_data キーワードには引数がありません。

dnp3_func

dnp3_func キーワードを使用すると、DNP3 アプリケーション層要求または応答見出し内の Function Code（機能コード）フィールドを照合できます。DNP3 機能コードとして、1 つの定義済み 10 進数値または 1 つの定義済み文字列を指定できます。

次の表に、DNP3 機能コードとしてシステムで認識される定義済みの値と文字列を示します。

表 36-44　DNP3 機能コード

値	文字列
0	確認
1	読み取り
2	write
3	select
4	operate
5	direct_operate
6	direct_operate_nr
7	immed_freeze
8	immed_freeze_nr
9	freeze_clear
10	freeze_clear_nr
11	freeze_at_time
12	freeze_at_time_nr
13	cold_restart
14	warm_restart
15	initialize_data

表 36-44　DNP3 機能コード（続き）

値	文字列
16	initialize_appl
17	start_appl
18	stop_appl
19	save_config
20	enable_unsolicited
21	disable_unsolicited
22	assign_class
23	delay_measure
24	record_current_time
25	open_file
26	close_file
27	delete_file
28	get_file_info
29	authenticate_file
30	abort_file
31	activate_config
32	authenticate_req
33	authenticate_err
129	response
130	unsolicited_response
131	authenticate_resp

DNP3 機能コードを指定する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [dnp3_func] を選択して、[Add Option] をクリックします。

`dnp3_func` キーワードが表示されます。

ステップ 2　機能コード用の 1 つの定義済み 10 進数値（0 ～ 255）または 1 つの定義済み文字列を指定します。システムで認識される値と文字列については、DNP3 機能コードの表を参照してください。

dnp3_ind

`dnp3_ind` キーワードを使用すると、DNP3 アプリケーション層応答見出し内の Internal Indications（内部通知）フィールド内のフラグを照合できます。

1 つの既知のフラグ、または次の例のように、カンマで区切ったフラグのリストを指定できます。

```
class_1_events, class_2_events
```

複数のフラグを指定した場合、キーワードはリスト内の任意のフラグと一致することができます。いくつかのフラグの組み合わせを検出するには、1 つのルール内で dnp3_ind キーワードを複数回使用します。

定義済みの DNP3 内部通知フラグとしてシステムによって認識される文字列構文を以下に示します。

```
class_1_events
class_2_events
class_3_events
need_time
local_control
device_trouble
device_restart
no_func_code_support
object_unknown
parameter_error
event_buffer_overflow
already_executing
config_corrupt
reserved_2
reserved_1
```

DNP3 内部通知フラグを指定する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [dnp3_ind] を選択して、[Add Option] をクリックします。

dnp3_ind キーワードが表示されます。

ステップ 2　1 つの既知のフラグまたはカンマ区切ったフラグのリストを指定できます。

dnp3_obj

dnp3_obj キーワードを使用すると、要求または応答内の DNP3 オブジェクト 見出しを照合できます。

DNP3 データは、アナログ入力やバイナリ入力など、さまざまなタイプの一連の DNP3 オブジェクトで構成されます。各タイプは、それぞれ 10 進数値で識別される*グループ*を使って区別されます（アナログ入力グループ、バイナリ入力グループなど）。各グループ内のオブジェクトは、それぞれオブジェクト データ形式を特定する*オブジェクト バリエーション*（16 ビット整数、32 ビット整数、短精度浮動小数点など）によってさらに識別されます。また、オブジェクト バリエーションの各タイプは 10 進数値でも識別可能です。

オブジェクト 見出しを識別する際には、オブジェクト 見出し グループのタイプを示す 10 進数値とオブジェクト バリエーションのタイプを示す 10 進数値を指定します。この 2 つの組み合わせによって DNP3 オブジェクトの特定のタイプが定義されます。

DNP3 オブジェクトを指定する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [dnp3_obj] を選択して、[Add Option] をクリックします。

dnp3_obj キーワードが表示されます。

ステップ 2　既知のオブジェクト グループを識別するために 1 つの 10 進数値（0 ～ 255）を指定し、既知のオブジェクト バリエーション タイプを識別するために別の 10 進数値（0 ～ 255）を指定します。

パケット特性の検査

ライセンス：Protection

特定のパケット特性を持つパケットに対してのみイベントを生成するルールを作成できます。FireSIGHT システムには、パケット特性を評価するための次のキーワードが備わっています。

- dsize（36-85 ページ）
- isdataat（36-85 ページ）
- sameip（36-86 ページ）
- fragoffset（36-87 ページ）
- cvs（36-87 ページ）

dsize

ライセンス：Protection

`dsize` キーワードはパケット ペイロード サイズを検査します。「大なり」演算子と「小なり」演算子（`<`、`>`）を使って値の範囲を指定することができます。次の構文をに従って範囲を指定できます。

```
>number_of_bytes
<number_of_bytes
number_of_bytes<>number_of_bytes
```

たとえば、400 バイトを超えるパケット サイズを指定するには、`dtype` 値として `>400` を使用します。500 バイト未満のパケット サイズを指定するには、`<500` を使用します。400 ～ 500 バイトのパケットに対してルールをトリガーとして使用するよう指定するには、`400<>500` を使用します。

注意　`dsize` キーワードは、プリプロセッサによってデコードされる前のパケットを検査します。

isdataat

ライセンス：Protection

`isdataat` キーワードは、ペイロード内の特定の位置にデータが存在することを確認するよう、ルール エンジンに指示します。

次の表に、`isdataat` キーワードで使用可能な引数を列挙します。

表 36-45　isdataat の引数

引数	タイプ	説明
Offset	必須	ペイロード内の特定の位置。たとえば、パケット ペイロード内のバイト位置 50 にデータが出現することを検査するには、オフセット値として `50` を指定します。`!` 修飾子は `isdataat` 検査の結果を否定します。特定量のデータがペイロードに存在しない場合は警告が出されます。 また、既存の `byte_extract` 変数を使用してこの引数の値を指定することもできます。詳細については、「パケット データをキーワード引数の中に読み込む（36-88 ページ）」を参照してください。
Relative	任意	最後に見つかったコンテンツ一致を基準にして相対的な位置を計算します。相対位置を指定する場合は、カウンタがバイト 0 から始まることに注意してください。最後に見つかったコンテンツ一致から順方向に移動するバイト数から 1 を差し引いて位置を計算します。たとえば、最後に見つかったコンテンツ一致から 9 バイト後にデータが出現すべきことを指定するには、相対オフセットとして `8` を指定します。
Raw Data	任意	FireSIGHT システム プリプロセッサによるデコードやアプリケーション層正規化が行われる前の、元のパケット ペイロードにデータが配置されていることを指定します。前のコンテンツ一致が未加工パケット データ内に存在していた場合は、この引数を **Relative** と一緒に使用できます。

たとえば、`foo` というコンテンツを検索するルールで `isdataat` の値が次のように指定される場合、

- Offset = !10
- Relative = enabled

ルール エンジンが `foo` の後ろからペイロード末尾までに 10 バイトを検出しない場合、システムは警告を出します。

isdataat を使用する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [isdataat] を選択して、[Add Option] をクリックします。

[isdataat] セクションが表示されます。

sameip

ライセンス： Protection

`sameip` キーワードは、パケットの送信元 IP アドレスと宛先 IP アドレスが同じであることを検査します。このキーワードは引数を受け入れません。

fragoffset

ライセンス：Protection

fragoffset キーワードは、フラグメント化されたパケットのオフセットを検査します。一部のエクスプロイト（WinNuke サービス拒否攻撃など）では、特定のオフセットを持つ手動生成されたパケット フラグメントが使用されるので、このキーワードが役立ちます。

たとえば、フラグメント化されたパケットのオフセットが 31337 バイトかどうかを検査するには、fragoffset 値として 31337 を指定します。

fragoffset キーワードの引数を指定するときには、次の演算子を使用できます。

表 36-46　fragoffset キーワードの引数演算子

Operator	説明
!	not
>	より大きい
<	より小さい

否定（!）演算子を < や > と組み合わせて使用できないことに注意してください。

cvs

ライセンス：Protection

cvs キーワードは、Concurrent Versions System（CVS）トラフィック内で不正な形式の CVS エントリを検査します。攻撃者は不正な形式のエントリを使用して、ヒープ オーバーフローを強制的に発生させ、CVS サーバ上で有害コードを実行することができます。このキーワードを使用すると、2 つの既知の CVS 脆弱性 CVE-2004-0396（CVS 1.11.x ～ 1.11.15 と 1.12.x ～ 1.12.7）および CVS-2004-0414（CVS 1.12.x ～ 1.12.8 と 1.11.x ～ 1.11.16）に対する攻撃を識別できます。cvs キーワードは、正しい形式のエントリであることを検査して、不正な形式のエントリが検出された場合はアラートを生成します。

CVS が動作するポートをルールに含める必要があります。さらに、トラフィックが発生する可能性のあるポートを TCP ポリシー内のストリーム再構築用のポート リストに追加することで、CVS セッションの状態を保持できるようにする必要があります。ストリーム再構築が行われるクライアント ポートのリストには、TCP ポート 2401（pserver）と 514（rsh）が含まれています。ただし、サーバが xinetd サーバ（つまり pserver）として動作する場合は、任意の TCP ポート上で動作できることに注意してください。すべての非標準ポートを、ストリーム再構築の [Client Ports] リストに追加します。詳細については、ストリームの再アセンブリのオプションの選択（29-29 ページ）を参照してください。

不正な形式の CVS エントリを検出する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　cvs オプションをルールに追加し、キーワード引数として「invalid-entry」と入力します。

パケット データをキーワード引数の中に読み込む

ライセンス：Protection

byte_extract キーワードを使用すると、指定したバイト数をパケットから変数の中に読み込むことができます。後で、その変数を、同じルール内で他の検出キーワードの特定の引数の値として使用できます。

たとえば、パケット データに含まれるバイト数が特定のバイト セグメントで記述されている場合、パケットからデータ サイズを抽出するには、これが役立ちます。たとえば、特定のバイト セグメントにおいて、後続データが 4 バイト構成であると記述されている場合、データ サイズ 4 バイトを抽出して変数値として使用できます。

byte_extract を使用するとき、1 つのルール内で最大 2 つの異なる変数を同時に作成できます。byte_extract 変数を何回でも再定義できます。同じ変数名と別の変数定義を使って新しい byte_extract キーワードを入力した場合、その前の変数定義がオーバーライドされます。

次の表に、byte_extract キーワードで必要な引数について説明します。

表 36-47　byte_extract の必須引数

引数	説明
Bytes to Extract	パケットから抽出するバイト数。1、2、3、または 4 バイトを指定できます。
Offset	ペイロード内でデータの抽出を開始するバイト数。-65534 ～ 65535 バイトを指定できます。オフセット カウンタはバイト 0 から始まるため、順方向に数えるバイト数から 1 を差し引いてオフセット値を計算してください。たとえば、順方向に 8 バイト数えるには 7 を指定します。ルール エンジンは、パケット ペイロードの先頭から（**Relative** も一緒に指定した場合は最後に見つかったコンテンツ一致の後から）順方向に数えます。なお、負の数値を指定できるのは、**Relative** を一緒に指定した場合だけです。詳細については、byte_extract の追加のオプション引数の表を参照してください。
Variable Name	他の検出キーワードの引数で使用する変数名。英数字の文字列を指定できます（ただし文字で始まる必要があります）。

抽出対象のデータを見つける方法をさらに詳しく定義するには、次の表に示す引数を使用できます。

表 36-48　byte_extract の追加のオプション引数

引数	説明
Multiplier	パケットから抽出された値の乗数。0 ～ 65535 を指定できます。乗数を指定しない場合のデフォルト値は 1 です。
Align	抽出された値を最も近い 2 バイトまたは 4 バイト境界に切り上げます。**Multiplier** も一緒に選択した場合、システムはこの調整の前に乗数を適用します。
Relative	ペイロードの先頭ではなく、最後に見つかったコンテンツ一致の末尾を基準にして **Offset** を計算します。詳細については、byte_extract の必須引数の表を参照してください。

DCE/RPC、**Endian**、または **Number Type** のうち 1 つだけを指定できます。

検査対象となるバイトを byte_extract キーワードでどのように計算するか定義するには、次の表の中から引数を選択できます。どの引数も選択しない場合、ルール エンジンは ビッグ エンディアン バイト順を使用します。

表 36-49　byte_extract のエンディアンネス引数

引数	説明
Big Endian	デフォルトのネットワーク バイト順であるビッグ エンディアン バイト順でデータを処理します。
Little Endian	リトル エンディアン バイト順でデータを処理します。
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に byte_extract キーワードを指定します。詳細については、「DCE/RPC トラフィックのデコード (27-2 ページ)」を参照してください。 DCE/RPC プリプロセッサがビッグ エンディアンまたはリトル エンディアン バイト順を決定します。**Number Type** 引数と **Endian** 引数は、適用されません。 この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて byte_extract を使用することもできます。詳細については、「DCE/RPC キーワード (36-64 ページ)」を参照してください。

データを読み取るときの数値タイプを ASCII 文字列として指定できます。パケット内のストリング データをシステムがどのように認識するかを定義するには、次の表のいずれかの引数を選択できます。

表 36-50　byte_extract の Number Type 引数

引数	説明
Hexadecimal String	抽出されたストリング データを 16 進形式で読み取ります。
Decimal String	抽出されたストリング データを 10 進形式で読み取ります。
Octal String	抽出されたストリング データを 8 進形式で読み取ります。

たとえば、byte_extract の値を次のように指定した場合、

- Bytes to Extract = 4
- Variable Name = var
- Offset = 8
- Relative = enabled

ルール エンジンは、最後に見つかったコンテンツ一致から（それを基準にして）9 バイト後に出現する、4 バイトで表現される数値を var という名前の変数の中に読み込みます。後でこの変数を、特定のキーワード引数の値としてルール内で指定できます。

byte_extract キーワードで定義した変数を指定できるキーワード引数を、次の表に列挙します。

表 36-51　byte_extract 変数を使用できる引数

キーワード	引数	詳細情報の参照先
content	Depth、Offset、Distance、Within	コンテンツ一致の制約（36-19 ページ）
byte_jump	Offset	byte_jump（36-34 ページ）
byte_test	Offset、Value	byte_test（36-36 ページ）
isdataat	Offset	isdataat（36-85 ページ）

byte_extract を使用する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [byte_extract] を選択して、[Add Option] をクリックします。

[byte_extract] セクションが、選択した最後のキーワードの下に表示されます。

ルール キーワードを使用したアクティブ応答の開始

ライセンス：Protection

システムは、トリガーとして使用された TCP ルールに応答して TCP 接続を閉じるために、またはトリガーとして使用された UDP ルールに応答して UDP セッションを閉じるために、アクティブ応答を開始できます。2 つのキーワードにより、別々の方法でアクティブ応答を開始できます。どちらかのキーワードを含むルールをパケットがトリガーとして使用すると、システムは 1 つのアクティブ応答を開始します。また、`config response` コマンドを使用すると、使用するアクティブ応答インターフェイスおよびパッシブ展開での TCP リセット試行回数を設定できます。

アクティブ応答は、インライン展開で最も効果を発揮します。接続またはセッションに影響を与える時間内にリセットが到着する可能性がより高いためです。たとえば、インライン展開での `react` キーワードに応答して、システムは接続の両端用のトラフィックに TCP リセット（RST）パケットを直接挿入し、通常はこれによって接続が閉じます。

（パッシブ展開ではシステムがパケットを挿入できない、攻撃者がアクティブ応答を無視または回避するよう選択する可能性があるなど）さまざまな理由で、アクティブ応答はファイアウォールの代わりとして想定されていません。

アクティブ応答は戻って来ることがあるため、システムは TCP リセットによる TCP リセットの開始を許可しません。これにより、アクティブ応答が無限に続くことを防止できます。また、システムは、標準的な慣行に従って ICMP 到達不能パケットによる ICMP 到達不能パケットの開始を許可しません。

侵入ルールがアクティブ応答をトリガーとして使用した後、接続またはセッションで追加のトラフィックを検出するよう、TCP ストリーム プリプロセッサを設定できます。追加のトラフィックが検出されると、プリプロセッサは、指定された最大値まで、追加のアクティブ応答を接続またはセッションの両端に送信します。詳細については、「侵入廃棄ルールでのアクティブ応答の開始（29-3 ページ）」を参照してください。

アクティブ応答を開始するために使用できるキーワードに固有の情報については、以下の項を参照してください。

- タイプ別、方向別のアクティブ応答の開始（36-91 ページ）
- TCP リセット前の HTML ページの送信（36-92 ページ）
- アクティブ応答のリセット試行とインターフェイスの設定（36-93 ページ）

タイプ別、方向別のアクティブ応答の開始

ライセンス：Protection

`resp` キーワードを使用すると、ルール 見出しで TCP プロトコルと UDP プロトコルのどちらが指定されているかに基づいて、TCP 接続または UDP セッションにアクティブに（能動的に）応答できます。詳細については、「プロトコルの指定（36-5 ページ）」を参照してください。

キーワード引数を使用すると、パケットの方向、および TCP リセット（RST）パケットと ICMP 到達不能パケットのどちらをアクティブ応答として使用するかを指定できます。

任意の TCP リセット引数または ICMP 到達不能引数を使用して、TCP 接続を閉じることができます。UDP セッションを閉じるには、ICMP 到達不能引数だけを使用する必要があります。

また、さまざまな TCP リセット引数を使用することで、パケットの送信元、宛先、またはその両方にアクティブ応答を送ることができます。すべての ICMP 到達不能引数はパケット送信元に送られます。ICMP ネットワーク、ホスト、ポートのどの到達不能パケットを使用するか（または 3 つすべてを使用するか）を指定できます。

ルールがトリガーとして使用されたときに FireSIGHT システムで実行されるアクションを正確に指定するために、`resp` キーワードで使用できる引数を次の表に列挙します。

表 36-52　resp の引数

引数	説明
reset_source	ルールをトリガーとして使用したパケットを送信元エンドポイントに TCP リセット パケットを送ります。この代わりに、下位互換性のためにサポートされている `rst_snd` を指定することもできます。
reset_dest	ルールをトリガーとして使用したパケットの宛先であるエンドポイントに TCP リセット パケットを送ります。この代わりに、下位互換性のためにサポートされている `rst_rcv` を指定することもできます。
reset_both	送信側エンドポイントと受信側エンドポイントの両方に TCP リセット パケットを送ります。この代わりに、下位互換性のためにサポートされている `rst_all` を指定することもできます。
icmp_net	送信側に ICMP ネットワーク到達不能メッセージを送ります。
icmp_host	送信側に ICMP ホスト到達不能メッセージを送ります。
icmp_port	送信側に ICMP ポート到達不能メッセージを送ります。この引数は、UDP トラフィックを終了するために使われます。
icmp_all	送信側に次の ICMP メッセージを転送します。 • ネットワーク到達不能 • ホスト到達不能 • ポート到達不能

たとえば、ルールがトリガーとして使用されたときに接続の両側をリセットするようルールを設定するには、resp キーワードの値として reset_both を使用します。

次のように、カンマ区切りリストを使用して複数の引数を指定できます。

argument,*argument*,*argument*

使用するアクティブ応答インターフェイスおよびパッシブ展開での TCP リセット試行回数を設定するために config response コマンドを使用する方法については、アクティブ応答のリセット試行とインターフェイスの設定（36-93 ページ）を参照してください。

アクティブ応答を指定する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [resp] を選択して、[Add Option] をクリックします。

resp キーワードが表示されます。

ステップ 2　[resp] フィールドで、resp の引数の表にある引数を指定します。複数の引数を指定する場合は、カンマで区切ったリストを使用します。

TCP リセット前の HTML ページの送信

ライセンス： Protection

react キーワードを使用すると、パケットがルールをトリガーとして使用した時点でデフォルト HTML ページを TCP 接続クライアントに送信できます。HTML ページの送信後に、システムは TCP リセット パケットを使って接続の両端へのアクティブ応答を開始します。react キーワードは UDP トラフィックのアクティブ応答をトリガーとして使用しません。

オプションで、次の引数を指定できます。

msg

msg 引数を使用する react ルールがパケットによってトリガーとして使用されると、HTML ページにルール イベント メッセージが表示されます。イベント メッセージのフィールドについては、ルール構造について（36-2 ページ）を参照してください。

msg 引数を指定しない場合、HTML ページには次のメッセージが含まれます。

```
You are attempting to access a forbidden site.
Consult your system administrator for details.
```

注　アクティブ応答は戻って来ることがあるため、HTML 応答ページによって react ルールがトリガーとして使用されないようにしてください（結果としてアクティブ応答が無限に続く可能性があります）。Ciscoでは、react ルールを十分にテストしてから実稼動環境でアクティブにするよう推奨しています。

使用するアクティブ応答インターフェイスおよびパッシブ展開での TCP リセット試行回数を設定するために config response コマンドを使用する方法については、アクティブ応答のリセット試行とインターフェイスの設定（36-93 ページ）を参照してください。

アクティブ応答を開始する前に HTML ページを送信する方法:

アクセス: Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [react] を選択して、[Add Option] をクリックします。

`react` キーワードが表示されます。

ステップ 2　次の 2 つの選択肢があります。

- 接続を閉じる前に、ルール用に設定されたイベント メッセージを含む HTML ページをクライアントに送信するには、[react] フィールドに「`msg`」と入力します。
- 接続を閉じる前に、次のデフォルト メッセージを含む HTML ページをクライアントに送信するには、[react] フィールドを空白のままにします。

```
You are attempting to access a forbidden site.
Consult your system administrator for details
```

アクティブ応答のリセット試行とインターフェイスの設定

ライセンス: Protection

config response コマンドを使用すると、`resp` ルールと `react` ルールによって開始される TCP リセットの動作を詳細に設定できます。また、このコマンドは、廃棄ルールによって開始されるアクティブ応答の動作にも影響を与えます（詳細については、侵入廃棄ルールでのアクティブ応答の開始（29-3 ページ）を参照してください）。

config response コマンドを使用するには、高度な USER_CONF 変数内の別個の 1 行にこれを挿入します。USER_CONF 変数の使用方法については、拡張変数について（3-35 ページ）を参照してください。

注意　機能の説明またはサポート担当の指示に従う場合を除き、侵入ポリシー機能を設定するために高度な `USER_CONF` 変数を**使用しない**でください。競合または重複する設定が存在すると、システムが停止します。

アクティブ応答リセット試行、アクティブ応答インターフェイス、またはその両方を指定する方法:

アクセス: Admin/Intrusion Admin

ステップ 1　アクティブ応答の回数のみを指定するのか、アクティブ応答インターフェイスのみを指定するのか、またはその両方を指定するのかに応じて、高度な USER_CONF 変数内の別個の 1 行に `config response` コマンドの 1 つの形式を挿入します。次の選択肢があります。

- アクティブ応答の試行回数のみを指定するには、次のコマンドを挿入します。
  `config response: attempts att`

  例:`config response: attempts 10`
- アクティブ応答インターフェイスのみを指定するには、次のコマンドを挿入します。
  `config response: device dev`

  例:`config response: device eth0`
- アクティブ応答の試行回数とアクティブ応答インターフェイスの両方を指定するには、次のコマンドを挿入します。
  `config response: attempts att, device dev`

例：`config response: attempts 10, device eth0`

値は次のとおりです。

att は、受信側ホストにパケットを受け入れさせるために、現在の接続枠で各 TCP リセット パケットを挿入する試行回数（1 ～ 20）です。この*連続試行*はパッシブ展開でのみ効果があります。インライン展開の場合、システムはトリガー パケットの代わりにリセット パケットをストリームに直接挿入します。ICMP 到着可能な 1 つのアクティブ応答のみが送信されます。

dev は、パッシブ展開でシステムからアクティブ応答を送信したり、インライン展開でアクティブ応答を挿入したりするための代替インタフェースです。

イベントのフィルタリング

ライセンス： Protection

`detection_filter` キーワードを使用すると、指定された時間内に指定された数のパケットがルールをトリガーとして使用しない限り、ルールでイベントが生成されないようにすることができます。これにより、早すぎるタイミングでルールがイベントを生成することを回避できます。たとえば、数秒間にログイン試行が 2 ～ 3 回失敗することは想定の範囲内ですが、同じ時間内に多数の試行が発生した場合は総当たり攻撃を示唆している可能性があります。

`detection_filter` キーワードの必須の引数は、送信元/宛先のどちらの IP アドレスをシステムで追跡するか、イベントをトリガーすめたに検出基準が満たされるべき回数、およびカウントの継続時間を定義します。

イベントのトリガーを遅らせるには、次の構文を使用します。

```
track by_src/by_dst, count count, seconds number_of_seconds
```

`track` 引数は、ルールの検出基準を満たすパケット数をカウントするときに、パケットの送信元 IP アドレスと宛先 IP アドレスのどちらを使用するかを指定します。システムでイベント インスタンスを追跡する方法を指定するには、次の表の中から引数値を選択します。

表 36-53　detection_filter の追跡引数

引数	説明
by_src	送信元 IP アドレスによる検出基準カウント。
by_dst	宛先 IP アドレスによる検出基準カウント。

`count` 引数は、ルールでイベントを生成するために、指定された時間内に指定された IP アドレスのルールをトリガーすべきパケットの数を指定します。

`seconds` 引数は、ルールでイベントを生成するために、指定された数のパケットがルールをトリガーすべき時間枠を秒数で指定します。

パケット内でコンテンツ `foo` を検索するルールが、次の引数を含む `detection_filter` キーワードを使用するとします。

```
track by_src, count 10, seconds 20
```

この例のルールは、特定の送信元 IP アドレスから 20 秒以内に 10 個のパケットで `foo` を検出するまでは、イベントを生成しません。システムが最初の 20 秒以内に `foo` を含むパケットを 7 つしか検出しなかった場合は、イベントが生成されません。しかし、最初の 20 秒間で `foo` が 40 回出現した場合は、ルールで 30 個のイベントが生成され、20 秒が経過するとカウントが再開されます。

しきい値と detection_filter キーワードの比較

detection_filter キーワードは、非推奨の threshold キーワードに代わるものです。threshold キーワードは、下位互換性を維持するために引き続きサポートされていますが、侵入ポリシー内で設定されるしきい値と同じ機能です。

detection_filter キーワードは、パケットがルールをトリガーとして使用する前に適用される検出機能です。ルールは、指定されたパケット カウントの前に検出されたトリガー パケットに関してイベントを生成しません。また、インライン展開では、パケットを破棄するようルールで設定されていても、そのようなパケットを破棄しません。逆に、指定されたパケット カウントの後に出現する、ルールをトリガーとして使用するパケットに関してルールはイベントを生成します。また、インライン展開でパケットを破棄するよう設定されている場合は、そのようなパケットを破棄します。

しきい値は、検出アクションを発生させないイベント通知機能です。これは、パケットがイベントをトリガーとして使用した後に適用されます。インライン展開において、パケットを破棄するよう設定されたルールは、ルール しきい値とは無関係に、ルールをトリガーとして使用するすべてのパケットを破棄します。

侵入ポリシー内では、detection_filter キーワードを侵入イベントしきい値、侵入イベント抑制、レートベース攻撃防御機能と任意に組み合わせて使用できます。また、侵入ポリシー内の侵入イベントしきい値機能と組み合わせて非推奨の threshold キーワードを使用するインポートされたローカル ルールを有効にした場合、ポリシー検証が失敗することに注意してください。詳しくは、イベントしきい値の設定（32-25 ページ）、侵入ポリシー単位の抑制の設定（32-30 ページ）、動的ルール状態の設定（32-34 ページ）、およびローカル ルール ファイルのインポート（66-22 ページ）を参照してください。

攻撃後トラフィックの評価

ライセンス：Protection

ホストまたはセッションに関する追加のトラフィックをログに記録するようシステムに指示するには、tag キーワードを使用します。tag キーワードを使って検出するトラフィックのタイプと量を指定するときには、次の構文を使用します。

tagging_type, count, metric, optional_direction

次の 3 つの表に、その他の使用可能な引数について説明します。

2 つのタイプのタグ機能から選択できます。次の表に、これらのタグ機能の説明を示します。侵入ルールでルール 見出し オプションのみを設定した場合、session タグ引数タイプによって、同じセッションからのパケットが別のセッションからのパケットのように記録されることに注意してください。同じセッションからのパケットをまとめてグループ化するには、同じ侵入ルール内で 1 つ以上のルール オプション（flag キーワードや content キーワードなど）を設定します。

表 36-54　tag の引数

引数	説明
session	ルールをトリガーとして使用したセッション内のパケットをログに記録します。
ホスト	ルールをトリガーとして使用したパケットを送信したホストからのパケットをログに記録します。ホストからのトラフィックのみ（src）、またはホストへのトラフィックのみ（dst）を記録する方向修飾子を追加できます。

ログに記録するトラフィック量を指定するには、次の引数を使用します。

表 36-55　count 引数

引数	説明
count	ルールがトリガーとして使用された後にログに記録するパケット数または秒数。 この単位を指定するには、count 引数の後に測定基準引数を使用します。

次の表の中から、トラフィックの時間または量ごとにログで使用する測定基準を選択してください。

注意　高帯域ネットワークでは 1 秒あたり数千パケットが発生する可能性があり、大量のパケットにタグを付けるとパフォーマンスに重大な影響が及ぶ可能性があるため、必ずネットワーク環境に合わせてこの設定を調整してください。

表 36-56　ログの測定基準引数

引数	説明
パケット	ルールのトリガー後に、カウントで指定されるパケット数をログに記録します。
seconds	ルールのトリガー後に、カウントで指定される秒数の間、トラフィックを記録します。

たとえば、次の `tag` キーワード値を使用するルールがトリガーとして使用された場合、

```
host, 30, seconds, dst
```

次の 30 秒間にクライアントからホストに送信されるすべてのパケットがログに記録されます。

複数のパケットに及ぶ攻撃の検出

ライセンス：Protection

状態名をセッションに割り当てるには、`flowbits` キーワードを使用します。すでに名前が付けられた状態に基づいてセッション内の後続パケットを分析することにより、システムは単一セッション内で複数のパケットに及ぶ exploit を検出して警告を出すことができます。

`flowbits` 状態名は、セッションの特定部分のパケットに割り当てられるユーザ定義のラベルです。パケットの内容に基づいてパケットに状態名を付けると、警告の必要のないパケットと有害なパケットを区別しやすくなります。管理対象デバイスごとに最大 1024 個の状態名を定義できます。たとえば、ログイン成功後にのみ発生することがわかっている有害パケットについて警告するには、`flowbits` キーワードを使用して、初期ログイン試行を構成するパケットを除去することにより、有害パケットに焦点を絞ることができます。このような機能を実装するには、まず、セッション内のすべてのログイン確立済みパケットに `logged_in` 状態のラベルを付けるルールを作成した後、2 番目のルールを作成し、最初のルールで設定された状態を持つパケットを検査してそのようなパケットだけを処理する `flowbits` をそのルールに含めます。ユーザがログイン済みかどうかを判断するために `flowbits` を使用する例については、state_name を使用した flowbits の例（36-98 ページ）を参照してください。

オプションの *group name* を使用すると、状態のグループに状態名を含めることができます。1 つの状態名は複数のグループに属することができます。グループに関連付けられていない状態は相互排他的ではないため、トリガーとして使用されたルールがグループに関連付けられていない状態を設定した場合、現在設定されている他の状態には影響がありません。グループに状態名を含めて、同じグループ内の別の状態を解除することで誤検出を防止する方法については、誤検出を発生させる flowbits の例（36-99 ページ）の例を参照してください。

次の表に、flowbits キーワードで使用できる演算子、状態、およびグループのさまざまな組み合わせについて説明します。なお、状態名には、英数字、ピリオド(.)、アンダースコア(_)、およびダッシュ(-)を含めることができます。

表 36-57　flowbits のオプション

Operator	状態オプション	グループ	説明
セット	state_name	オプション	パケットに関する指定された状態を設定します。グループが定義されている場合は、指定されたグループ内で状態を設定します。
	state_name&state_name	オプション	パケットに関する、指定された複数の状態を設定します。グループが定義されている場合、指定されたグループ内で状態を設定します。
setx	state_name	必須	指定されたグループ内でパケットに関して指定された状態を設定し、グループ内の他のすべての状態を解除します。
	state_name&state_name	必須	指定されたグループ内でパケットに関して指定された複数の状態を設定し、グループ内の他のすべての状態を解除します。
unset	state_name	グループなし	パケットに関する指定された状態を解除します。
	state_name&state_name	グループなし	パケットに関する、指定された複数の状態を解除します。
	all	必須	指定されたグループ内のすべての状態を解除します。
toggle	state_name	グループなし	指定された状態が設定されている場合はそれを解除し、指定された状態が解除されている場合にはそれを設定します。
	state_name&state_name	グループなし	指定された複数の状態が設定されている場合はそれらを解除し、指定された複数の状態が解除されている場合はそれらを設定します。
	all	必須	指定されたグループ内で設定されているすべての状態を解除し、指定されたグループ内で解除されているすべての状態を設定します。
isset	state_name	グループなし	指定された状態がパケット内で設定されているかどうかを判別します。
	state_name&state_name	グループなし	指定された複数の状態がパケット内で設定されているかどうかを判別します。
	state_name|state_name	グループなし	指定されたいずれかの状態がパケット内で設定されているかどうかを判別します。
	any	必須	指定されたグループ内で、いずれかの状態が設定されているかどうかを判別します。
	all	必須	指定されたグループ内で、すべての状態が設定されているかどうかを判別します。

表 36-57　flowbits のオプション(続き)

Operator	状態オプション	グループ	説明
isnotset	state_name	グループなし	指定された状態がパケット内で設定されていないかどうかを判別します。
	state_name&state_name	グループなし	指定された複数の状態がパケット内で設定されていないかどうかを判別します。
	state_name|state_name	グループなし	指定されたいずれかの状態が、パケット内で設定されていないかどうかを判別します。
	any	必須	パケット内でいずれかの状態が設定されていないかどうかを判別します。
	all	必須	パケット内ですべての状態が設定されていないかどうかを判別します。
reset	(状態なし)	オプション	すべてのパケットのすべての状態を解除します。グループが指定される場合、グループ内のすべての状態を解除します。
noalert	(状態なし)	グループなし	イベント生成を抑制するには、これを他の演算子と組み合わせて使用します。

flowbits キーワードを使用するときには、次の点に注意してください。

- setx 演算子を使用する場合、指定した状態は、指定したグループ以外のグループに属することができません。
- setx 演算子を複数回定義して、それぞれのインスタンスで別々の状態と同じグループを指定できます。
- setx 演算子を使用してグループを指定する場合、そのグループに対して set、toggle、unset 演算子を使用することはできません。
- isset 演算子と isnotset 演算子は、指定された状態がグループに含まれるかどうかに関係なく、その状態を評価します。
- 侵入ポリシーの保存時、侵入ポリシーの再適用時、および(アクセス コントロール ポリシーで参照される侵入ポリシー数に関係なく)アクセス コントロール ポリシーの適用時には、グループ**指定のない** isset または isnotset 演算子を含むルールを有効にした場合、対応する状態名とプロトコルに関する flowbits 割り当て(set、setx、unset、toggle)に影響する 1 つ以上のルールを有効にしないと、対応する状態名の flowbits 割り当てに影響するすべてのルールが有効になります。
- 侵入ポリシーの保存時、侵入ポリシーの再適用時、および(アクセス コントロール ポリシーで参照される侵入ポリシー数に関係なく)アクセス コントロール ポリシーの適用時には、グループを**指定した** isset 演算子または isnotset 演算子を含むルールを有効にした場合、flowbits 割り当て(set、setx、unset、toggle)に影響し、対応するグループ名を定義するすべてのルールもまた有効になります。

state_name を使用した flowbits の例

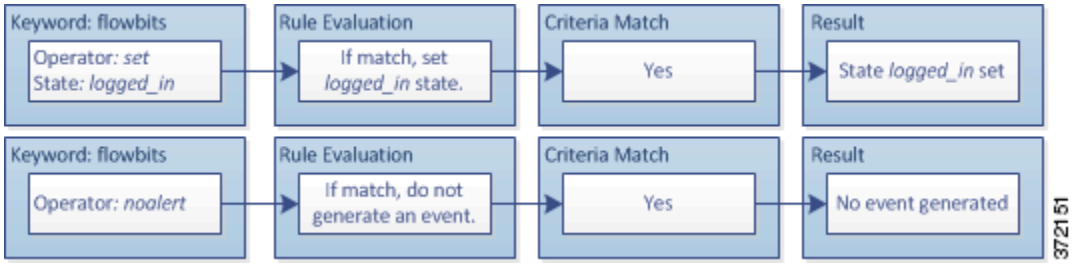
Bugtraq ID #1110 に記述されている IMAP 脆弱性について考えてみます。この脆弱性は、IMAP の実装(具体的には LIST、LSUB、RENAME、FIND、および COPY コマンド)で見られます。ただし、攻撃者がこの脆弱性を悪用するには、IMAP サーバにログインする必要があります。IMAP サーバからの LOGIN 確認とそれに続くエクスプロイトは必然的に別々のパケットに存在するため、このエクスプロイトを検出する非フロー ベースのルールを作成するのは困難です。flowbits キーワードを使って一連のルールを作成すると、ユーザが IMAP サーバにログイン済みかどう

かを追跡し、ログイン済みの場合は、いずれかの攻撃が検出された時点でイベントを生成することができます。ユーザがログイン済みでない場合、攻撃によって脆弱性が exploit されることはないため、イベントが生成されません。

下記の 2 つのルール フラグメントはこの例を示しています。最初のルール フラグメントは IMAP サーバからの IMAP ログイン確認を検索します。

```
alert tcp any 143 -> any any (msg:"IMAP login"; content:"OK
LOGIN"; flowbits:set,logged_in; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。

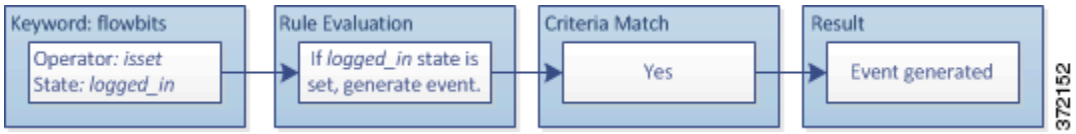


`flowbits:set` は `logged_in` 状態を設定しますが、`flowbits:noalert` がアラートを抑制することに注意してください。これは、IMAP サーバ上で多数の無害なログイン セッションが見つかる可能性があるためです。

次のルール フラグメントは LIST 文字列を検索しますが、セッション内の先行パケットの結果として logged_in 状態が設定済みでない限り、イベントを生成しません。

```
alert tcp any any -> any 143 (msg:"IMAP LIST";
content:"LIST"; flowbits:isset,logged_in;)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。



この場合、最初のフラグメントを含むルールが先行パケットによってトリガーとして使用した場合、2 番目のフラグメントを含むルールがトリガーとして使用し、イベントを生成します。

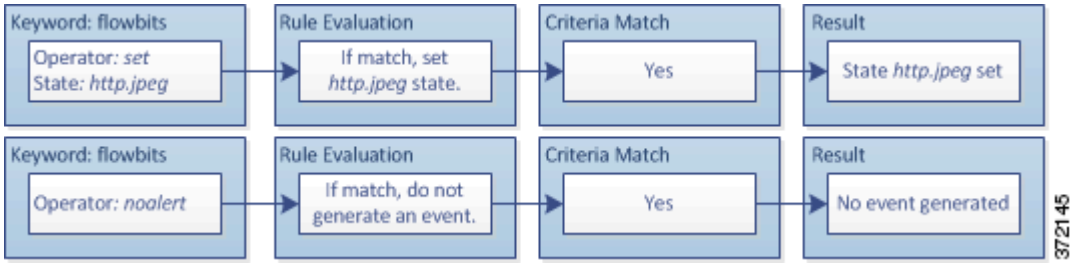
誤検出を発生させる flowbits の例

後続パケット内の、もはや無効になった状態を持つコンテンツがルールに一致することによって誤検出イベントが発生する可能性があります。これを防ぐには、複数のルールで設定された複数の状態名をグループに含めることができます。次の例は、複数の状態名をグループに含めない場合に誤検出が発生する可能性があることを示しています。

1 つのセッションで次の 3 つのルール フラグメントがこの順序でトリガーとして使用される場合を考えてみます。

```
(msg:"JPEG transfer"; content:"image/";pcre:"/^Content-
Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
flowbits:set,http.jpeg; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。

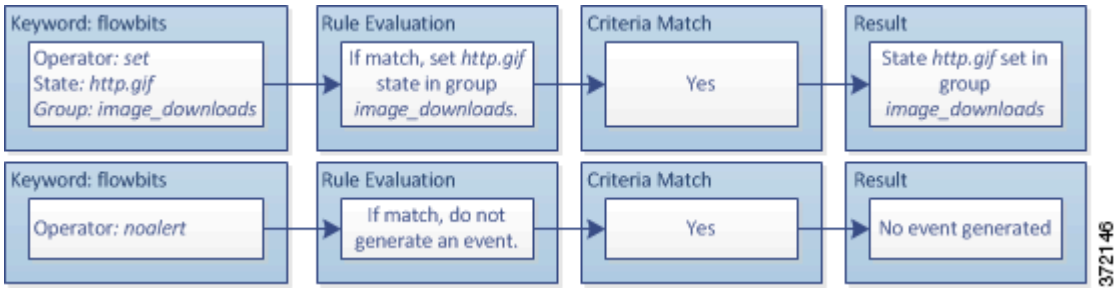


最初のルール フラグメント内の `content` キーワードと `pcre` キーワードが JPEG ファイル ダウンロードに一致し、`flowbits:set,http.jpeg` が `http.jpeg flowbits` 状態を設定し、`flowbits:noalert` はルールでのイベント生成を抑制します。イベントが生成されない理由は、このルールの目的がファイル ダウンロードを検出して `flowbits` 状態を設定することだからです。これにより、1 つ以上のコンパニオン ルールで状態名を検査して有害コンテンツを探し、有害コンテンツが検出された時点でイベントを生成できます。

次のルール フラグメントは、上記の JPEG ファイル ダウンロードに続く GIF ファイル ダウンロードを検出します。

```
(msg:"GIF transfer"; content:"image/"; pcre:"/^Content-
Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
flowbits:set,http.tif,image_downloads; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。

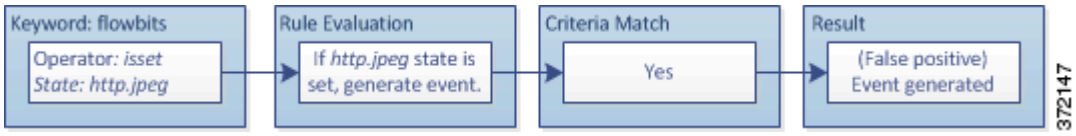


2 番目のルール内の `content` キーワードと `pcre` キーワードは GIF ファイル ダウンロードを照合し、`flowbits:set,http.tif` は `http.tif` flowbit ステートを設定し、`flowbits:noalert` はルールでのイベント生成を抑制します。最初のルール フラグメントで設定された `http.jpeg` 状態が不要になっても引き続き設定されていることに注意してください。これは、後続の GIF ダウンロードが検出されたときに JPEG ダウンロードが既に終了しているはずであるためです。

次に示す 3 番目のルール フラグメントは最初のルール フラグメントのコンパニオンです。

```
(msg:"JPEG exploit";
flowbits:isset,http.jpeg;content:"|FF|"; pcre:"
/\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。



3 番目のルール フラグメントでは、もはや無意味になった `http.jpeg` ステートが設定されていることを `flowbits:isset,http.jpeg` が判別し、`content` と `pcre` は（GIF ファイルでは無害でも）JPEG ファイル内では有害とみなされるコンテンツを照合します。3 番目のルール フラグメントによって、JPEG ファイル内に存在しない exploit に関する誤検出イベントが生成されます。

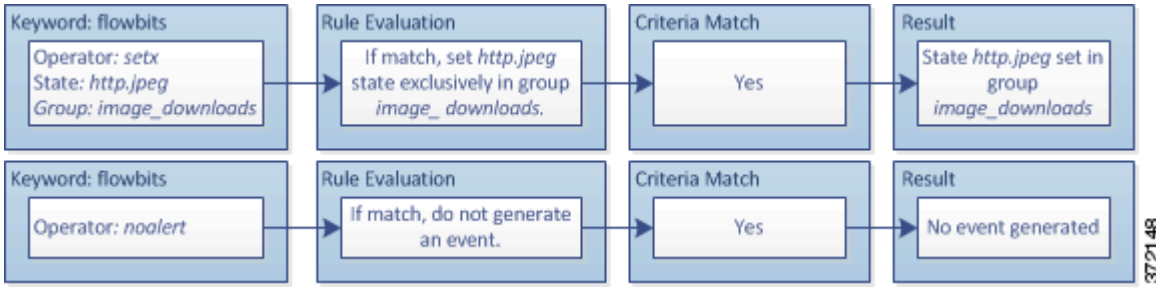
誤検出を防止するための flowbits の例

次の例は、状態名をグループに含めて setx 演算子を使用することで、どのように誤検出を防止できるかを示しています。

前の例とほぼ同じケースを考えます。ただし、最初の 2 つのルールで、同じ状態グループに 2 つの異なる状態名が含まれるようになった点が異なります。

```
(msg:"JPEG transfer"; content:"image/";pcre:"/^Content-
Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
flowbits:setx,http.jpeg,image_downloads; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける flowbits キーワードの効果を示しています。

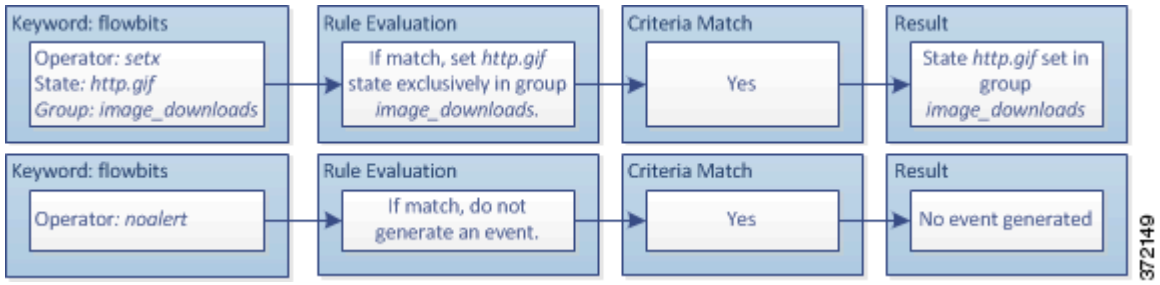


最初のルール フラグメントが JPEG ファイル ダウンロードを検出すると、flowbits:setx,http.jpeg,image_downloads キーワードが flowbits 状態を http.jpeg に 設定し、その状態を image_downloads グループに含めます。

その後、次のルールが後続の GIF ファイル ダウンロードを検出します。

```
(msg:"GIF transfer"; content:"image/"; pcre:"/^Content-
Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
flowbits:setx,http.tif,image_downloads; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける flowbits キーワードの効果を示しています。

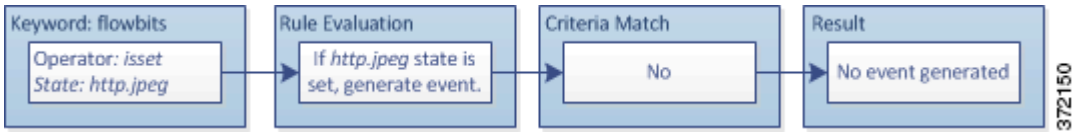


2 番目のルール フラグメントが GIF ダウンロードに一致すると、flowbits:setx,http.tif,image_downloads キーワードが http.tif flowbits ステートを設定し、グループ内の他のステートである http.jpeg を解除します。

次に示す 3 番目のルール フラグメントで誤検出は発生しません。

```
(msg:"JPEG exploit";
flowbits:isset,http.jpeg;content:"|FF|"; pcre:"/
\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

次の図は、上記のルール フラグメントにおける flowbits キーワードの効果を示しています。



`flowbits:isset,http.jpeg` が false であるため、ルール エンジンはルールの処理を停止し、イベントは生成されません。こうして、GIF ファイル内のコンテンツが JPEG ファイルに関する exploit コンテンツと一致した場合でも誤検出が回避されます。

HTTP エンコードのタイプと位置によるイベントの生成

ライセンス：Protection

`http_encode` キーワードを使用すると、HTTP URI、HTTP ヘッダーの非 cookie データ、HTTP 要求ヘッダーの cookie、HTTP 応答の set-cookie データのいずれかにおいて、正規化前の HTTP 要求または応答内のエンコード タイプに基づいてイベントを生成できます。

HTTP 応答と HTTP cookie を検査し、`http_encode` キーワードを使用しているルールに一致したものを返すように、HTTP Inspect プリプロセッサを設定する必要があります。詳細については、HTTP トラフィックのデコード（27-33 ページ）およびサーバレベル HTTP 正規化オプションの選択（27-36 ページ）を参照してください。

また、侵入ルール内の `http_encode` キーワードで特定のエンコード タイプによってイベントがトリガーとして使用されるようにするには、HTTP Inspect プリプロセッサ設定で個々の特定のエンコード タイプのデコード オプションとアラート オプションの両方を有効にする必要があります。詳細については、「サーバレベル HTTP 正規化エンコード オプションの選択（27-44 ページ）」を参照してください。

なお、base36 エンコード タイプは非推奨になりました。下位互換性を維持するために、既存のルールでは base36 引数を使用できますが、これによってルール エンジンが base36 トラフィックを検査することはありません。

次の表は、このオプションでイベントを生成できる、HTTP URI、ヘッダー、cookie、および set-cookie のエンコード タイプを示しています。

表 36-58　http_encode エンコード タイプ

エンコード タイプ	説明
utf8	HTTP Inspect プリプロセッサによるデコードで UTF8 エンコード タイプが有効になっている場合、指定された場所で UTF-8 エンコードを検出します。
double_encode	HTTP Inspect プリプロセッサによるデコードで二重エンコード タイプが有効になっている場合、指定された場所で二重エンコードを検出します。
non_ascii	非 ASCII 文字が検出されても、検出されたエンコード タイプが有効になっていない場合に、指定された場所で非 ASCII 文字を検出します。
uencode	HTTP Inspect プリプロセッサによるデコードで Microsoft %u エンコード タイプが有効になっている場合、指定された場所で Microsoft %u エンコードを検出します。
bare_byte	HTTP Inspect プリプロセッサによるデコードで空白バイト エンコード タイプが有効になっている場合、指定された場所で空白バイト エンコードを検出します。

侵入ルール内で HTTP エンコード タイプと位置を識別する方法:

アクセス: Admin/Intrusion Admin

ステップ 1　`http_encode` キーワードをルールに追加します。

ステップ 2　[Encoding Location] ドロップダウン リストで、指定したエンコード タイプを HTTP URI、ヘッダー、または cookie（set-cookie を含む）のいずれで検索するかを選択します。

ステップ 3　次のいずれかの形式を使用して、1 つ以上のエンコード タイプを指定します。

```
encode_type
encode_type|encode_type|encode_type...
!encode_type
```

ここで、*encode_type* は次のいずれかです。

```
utf8、double_encode、non_ascii、uencode、bare_byte
```

否定（!）演算子と OR（|）演算子を一緒に使用できないことに注意してください。

ステップ 4　オプションで、複数の `http_encode` キーワードを同じルールに追加すると、それぞれの条件が AND 結合されます。たとえば、次の条件を含む 2 つのキーワードを入力します。

最初のキーワード `http_encode` では:

- **Encoding Location**: `HTTP URI`
- **Encoding Type**: `utf8`

追加のキーワード `http_encode` では:

- **Encoding Location**: `HTTP URI`
- **Encoding Type**: `uencode`

この設定例では、HTTP URI で UTF8 および Microsoft IIS %u エンコードを検索します。

ファイル タイプとバージョンの検出

ライセンス: Protection

`file_type` と `file_group` キーワードを使用すると、タイプとバージョンに基づいて、FTP、HTTP、SMTP、IMAP、POP3、NetBIOS-ssn（SMB）を介して伝送されるファイルを検出できます。1 つの侵入ルール内で複数の `file_type` や `file_group` キーワードを**使用しないでください**。

ヒント　脆弱性データベース（VDB）を更新すると、最新のファイル タイプ、バージョン、およびグループがルール エディタに表示されます。詳細については、脆弱性データベースの更新（66-14 ページ）を参照してください。

`file_type` または `file_group` キーワードに一致するトラフィックに対して侵入イベントを生成するには、特定のプリプロセッサを有効にする**必要があります**。

表 36-59　file_type および file_group 侵入イベントの生成

伝送プロトコル	必要なプリプロセッサまたはプリプロセッサ オプション
FTP	FTP/Telnet プリプロセッサおよび [Normalize TCP Payload] インライン正規化プリプロセッサ オプション（FTP および Telnet トラフィックのデコード（27-20 ページ）およびインライン トラフィックの正規化（29-7 ページ）を参照）。
HTTP	HTTP Inspect プリプロセッサ（HTTP トラフィックのデコード（27-33 ページ）を参照）。
SMTP	SMTP プリプロセッサ（SMTP トラフィックのデコード（27-63 ページ）を参照）。
IMAP	IMAP プリプロセッサ（IMAP トラフィックのデコード（27-57 ページ）を参照）。
POP3	POP プリプロセッサ（POP トラフィックのデコード（27-60 ページ）を参照）。
NetBIOS-ssn（SMB）	[SMB File Inspection] DCE/RPC プリプロセッサ オプション（DCE/RPC トラフィックのデコード（27-2 ページ）を参照）。

詳細については、次の項を参照してください。

- file_type（36-104 ページ）
- file_group（36-105 ページ）

file_type

`file_type` キーワードを使用すると、トラフィック内で検出対象となるファイルのタイプとバージョンを指定できます。ファイル タイプ引数（**JPEG** や **PDF** など）は、トラフィックで検出するファイルの形式を識別します。

注　同じ侵入ルール内で `file_type` キーワードを別の `file_type` キーワードまたは `file_group` キーワードと一緒に**使用しないでください**。

デフォルトでは **Any Version** が選択されますが、一部のファイル タイプではバージョン オプション（たとえば PDF バージョン **1.7**）を選択することにより、トラフィックで検出対象となる特定のファイル タイプ バージョンを識別できます。

最新のファイル タイプとバージョンを表示して設定するには、VDB を更新してください。詳細については、脆弱性データベースの更新（66-14 ページ）を参照してください。

侵入ルール内でファイル タイプとバージョンを選択する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [file_type] を選択して、[Add Option] をクリックします。

`file_type` キーワードが表示されます。

ステップ 2　ドロップダウン リストから 1 つ以上のファイル タイプを選択します。ファイル タイプを選択すると、引数が自動的にルールに追加されます。

ルールからファイル タイプ引数を削除するには、削除するファイル タイプの横にある削除アイコン( )をクリックします。

ステップ 3　オプションで、各ファイル タイプのターゲット バージョンをカスタマイズします。デフォルトでは **Any Version** が選択されますが、いくつかのファイル タイプでは、個別のターゲット バージョンを選択できます。

注　VDB を更新すると、最新のファイル タイプとバージョンがルール エディタに表示されます。**Any Version** を選択した場合、新しいバージョンが今後の VDB 更新に追加されたときにそのバージョンを含めるよう、システムによってルールが設定されます。

file_group

`file_group` キーワードを使用すると、Ciscoにより定義された類似のファイル タイプから成るグループを選択して、トラフィック内で検出できます(**マルチメディア**、**オーディオ** など)。また、ファイル グループには、グループ内の各ファイル タイプに関するCisco定義のバージョンも含まれています。

注　同じ侵入ルール内で `file_group` キーワードを別の `file_group` キーワードまたは `file_type` キーワードと一緒に**使用しないでください**。

最新のファイル グループを表示して設定するには、VDB を更新してください。詳細については、脆弱性データベースの更新(66-14 ページ)を参照してください。

侵入ルール内でファイル グループを選択する方法:

アクセス: Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [file_group] を選択して、[Add Option] をクリックします。

`file_group` キーワードが表示されます。

ステップ 2　オプションで、グループ内のファイル タイプのバージョン情報を表示するには、ファイル グループの上にカーソルを移動し、[(Show Version Info)] をクリックします。

ファイル グループ情報が展開されて、バージョンが表示されます。

ステップ 3　ルールに追加するファイル グループを選択します。

特定のペイロード タイプを指し示す

ライセンス: Protection

`file_data` キーワードは、`content`、`byte_jump`、`byte_test`、`pcre` などの他のキーワードで使用可能な位置引数の参照として機能するポインタです。`file_data` キーワードが指し示すデータのタイプは、検出されるトラフィックによって決まります。`file_data`キーワードを使用すると、次のペイロード タイプの先頭を指し示すことができます。

- HTTP 応答本文

  HTTP 応答パケットを検査するには、HTTP Inspect プリプロセッサを有効にして、HTTP 応答を検査するようプリプロセッサを設定する必要があります。詳細については、HTTP トラフィックのデコード（27-33 ページ）、およびサーバレベル HTTP 正規化オプションの選択（27-36 ページ）の「**Inspect HTTP Responses**」を参照してください。HTTP Inspect プリプロセッサが HTTP 応答本文データを検出した場合に、`file_data` キーワードが一致します。

- 非圧縮 gzip ファイル データ

  HTTP 応答本文内の非圧縮 gzip ファイルを検査するには、HTTP Inspect プリプロセッサを有効にする必要があります。さらに、HTTP 応答を検査して HTTP 応答本文内の gzip 圧縮ファイルを復元するように、プリプロセッサを設定する必要があります。詳細については、HTTP トラフィックのデコード（27-33 ページ）、およびサーバレベル HTTP 正規化オプションの選択（27-36 ページ）の「**Inspect HTTP Responses**」と「**Inspect Compressed Data**」の各オプションを参照してください。`file_data` キーワードは、HTTP Inspect プリプロセッサが HTTP 応答本文内で非圧縮 gzip データを検出した場合に一致します。

- 正規化された Javascript

  正規化された JavaScript データを検査するには、HTTP Inspect プリプロセッサを有効にして、HTTP 応答を検査するようプリプロセッサを設定する必要があります。詳細については、HTTP トラフィックのデコード（27-33 ページ）、およびサーバレベル HTTP 正規化オプションの選択（27-36 ページ）の「**Inspect HTTP Responses**」を参照してください。`file_data` キーワードは、HTTP Inspect プリプロセッサが応答本文データ内で JavaScript を検出した場合に一致します。

- SMTP ペイロード

  SMTP ペイロードを検査するには、SMTP プリプロセッサを有効にする必要があります。詳細については、「SMTP デコードの設定（27-68 ページ）」を参照してください。`file_data` キーワードは、SMTP プリプロセッサが SMTP データを検出した場合に一致します。

- SMTP、POP、または IMAP トラフィック内のエンコードされた電子メール添付ファイル

  SMTP、POP、または IMAP トラフィック内の電子メール添付ファイルを検査するには、それぞれ SMTP、POP、または IMAP プリプロセッサを単独で、または任意に組み合わせて有効にする必要があります。その後、有効にしたプリプロセッサごとに、デコード対象のそれぞれの添付ファイル エンコード タイプをデコードするようプリプロセッサが設定されていることを確認する必要があります。プリプロセッサごとに設定可能な添付ファイル デコード オプションは、**Base64 Decoding Depth**、**7-Bit/8-Bit/Binary Decoding Depth**、**Quoted-Printable Decoding Depth**、および **Unix-to-Unix Decoding Depth** です。詳細については、IMAP トラフィックのデコード（27-57 ページ）、POP トラフィックのデコード（27-60 ページ）、およびSMTP トラフィックのデコード（27-63 ページ）を参照してください。

  1 つのルール内で複数の `file_data` キーワードを使用できます。

特定のペイロード タイプの先頭を指し示すには:

アクセス: Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [file_data] を選択して、[Add Option] をクリックします。

`file_data` キーワードが表示されます。

`file_data` キーワードには引数がありません。

パケット ペイロードの先頭を指し示す

ライセンス：Protection

pkt_data キーワードは、content、byte_jump、byte_test、pcre などの他のキーワードで使用可能な位置引数の参照として機能するポインタです。

正規化された FTP、Telnet、または SMTP トラフィックが検出された場合、pkt_data キーワードは、正規化されたパケット ペイロードの先頭を指します。その他のトラフィックが検出された場合、pkt_data キーワードは、未加工の TCP または UDP ペイロードの先頭を指します。

侵入ルールで検査するために、該当するトラフィックをシステムで正規化するには、次の正規化オプションを有効にする必要があります。

- FTP トラフィックを検査用に正規化するには、FTP & Telnet プリプロセッサの [Detect Telnet Escape codes within FTP commands] オプションを有効にする必要があります（サーバレベルの FTP オプションの設定（27-27 ページ）を参照）。
- Telnet トラフィックを検査用に正規化するには、FTP & Telnet プリプロセッサの [Normalize] Telnet オプションを有効にする必要があります（Telnet オプションについて（27-22 ページ）を参照）。
- SMTP トラフィックを検査用に正規化するには、SMTP プリプロセッサの [Normalize] オプションを有効にする必要があります（SMTP デコードについて（27-64 ページ）を参照）。

1 つのルール内で複数の pkt_data キーワードを使用できます。

パケット ペイロードの先頭を指し示すには：

アクセス：Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [pkt_data] を選択して、[Add Option] をクリックします。

pkt_data キーワードが表示されます。

pkt_data キーワードには引数がありません。

Base64 データのデコードと検査

ライセンス：Protection

base64_decode キーワードと base64_data キーワードを組み合わせて使用すると、指定したデータを Base64 データとしてデコードおよび検査するようルール エンジンに指示できます。この組み合わせは、HTTP PUT 要求や POST 要求内で Base64 エンコード HTTP 認証要求ヘッダーと Base64 エンコード データを検査する場合などに役立ちます。

これらのキーワードは特に、HTTP 要求内の Base64 データをデコードして検査するうえで役立ちます。また、長い見出し行を複数行に拡張するために HTTP で使われるのと同じ方法でスペース文字やタブ文字を使用する SMTP などのプロトコルでも、これらを使用できます。この行拡張（折り返し）を使用するプロトコル内に行拡張が存在しない場合、後続スペース/タブを伴わない復帰または改行が出現した箇所で検査が終了します。

詳細については、次の項を参照してください。

- base64_decode（36-108 ページ）
- base64_data（36-108 ページ）

base64_decode

ライセンス：Protection

base64_decode キーワードは、パケット データを Base64 データとしてデコードするようルール エンジンに指示します。オプションの引数を使用すると、デコードするバイト数と、デコードを開始するデータ内の位置を指定できます。

base64_decode キーワードは 1 つのルール内で 1 回だけ使用可能です。また、少なくとも 1 つの base64_data キーワードのインスタンスの前にこれを配置する必要があります。詳細については、「base64_data（36-108 ページ）」を参照してください。

Base64 データをデコードする前に、ルール エンジンは、複数行にわたって折り返された長い見出しを元どおりに広げます。ルール エンジンが次のいずれかに遭遇するとデコードが終了します。

- 見出し行の末尾
- デコード対象として指定されたバイト数
- パケットの末尾

次の表に、base64_decode キーワードで使用可能な引数の説明を示します。

表 36-60　base64_decode のオプション引数

引数	説明
Bytes	デコードするバイト数を指定します。これを指定しない場合、見出し行の末尾またはパケット ペイロード末尾のどちらかが先に出現するまでデコードが続行されます。ゼロ以外の正の値を指定できます。
Offset	パケット ペイロードの先頭を基準にしたオフセットを決定します。さらに **Relative** も指定した場合は、現在の検査位置を基準にしたオフセットを決定します。ゼロ以外の正の値を指定できます。
Relative	現在の検査位置を基準にして検査することを指定します。

Base64 データをデコードする方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [base64_decode] を選択して、[Add Option] をクリックします。

base64_decode キーワードが表示されます。

ステップ 2　オプションで、base64_decode のオプション引数の表に示す引数のいずれかを選択します。

base64_data

ライセンス：Protection

base64_data キーワードは、base64_decode キーワードを使ってデコードされた Base64 データを検査するための参照を提供します。base64_data キーワードは、デコードされた Base64 データの先頭から検査を開始するよう設定します。オプションで、content や byte_test などの他のキーワードで使用可能な位置引数を使用して、検査位置をさらに指定することもできます。

base64_decode キーワードを使用した後に base64_data キーワードを少なくとも 1 回使用する必要があります。オプションで、base64_data を複数回使用して、デコードされた Base64 データの先頭に戻ることができます。

Base64 データを検査するときには、次の点に注意してください。

- 高速パターン マッチ機能を使用できません（詳細については、Use Fast Pattern Matcher（36-29 ページ）を参照してください）。
- 中間的な HTTP コンテンツ引数を使ってルール内で Base64 検査を中断する場合は、Base64 データをさらに検査する前に、別の base64_data キーワードをルールに挿入する必要があります（詳細については、HTTP コンテンツ オプション（36-25 ページ）を参照してください）。

デコードされた Base64 データを検査する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Create Rule] ページで、ドロップダウン リストから [base64_data] を選択して、[Add Option] をクリックします。

base64_data キーワードが表示されます。

ルールの構築

ライセンス： Protection

独自のカスタム 標準テキスト ルールを作成することもできますが、shared object rule提供の既存の標準テキスト ルールやCiscoを変更して、それを新しいルールとして保存することもできます。Cisco提供のshared object ruleでは、送信元/宛先ポートおよび IP アドレスなどのルール 見出し情報だけを変更できることに注意してください。shared object rule内のルール キーワードとルール引数を変更することはできません。

詳細については、次の項を参照してください。

- 新しいルールの作成（36-109 ページ）
- 既存のルールの変更（36-111 ページ）
- ルールにコメントを追加する（36-112 ページ）
- カスタム ルールの削除（36-113 ページ）

新しいルールの作成

ライセンス： Protection

独自の標準テキスト ルールを作成できます。

カスタム標準テキスト ルールでは、ルール 見出し設定、ルール キーワード、およびルール引数を設定できます。オプションで、特定のプロトコルを使用する、特定の送信元/宛先 IP アドレスまたはポートを行き来するトラフィックだけをルールで照合するよう、ルール 見出しを設定できます。

新しいルールを作成した後、GID:SID:Rev という形式のルール番号を使用することで、そのルールをすばやく見つけることができます。すべての標準テキスト ルールの番号は 1 から始まります。ルール番号の 2 番目の部分である Snort ID（SID）は、それがローカル ルールまたはCisco提供のルールのどちらであるかを示します。新しいルールを作成すると、システムは、ローカル ルー

ルとして次に使用可能な Snort ID 番号をそのルールに割り当て、ローカル ルール カテゴリ内にルールを保存します。ローカル ルールの Snort ID 番号は 1,000,000 から始まり（ただし、ハイ アベイラビリティ ペアのセカンダリ Defense Center 上で作成された侵入ルールは 1,000,000,000 から始まり）、新しいローカル ルールが作成されるたびに SID が 1 ずつ増えます。ルール番号の最後の部分はリビジョン番号です。新しいルールのリビジョン番号は 1 です。カスタム ルールを変更するたびに、リビジョン番号が 1 ずつ増えます。

注　システムは、インポートされた侵入ポリシー内のカスタム ルールに新しい SID を割り当てます。詳細については、設定のインポートおよびエクスポート（A-1 ページ）を参照してください。

ルール エディタを使用してカスタム標準テキスト ルールを作成する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Rule Editor] の順に選択します。

[Rule Editor] ページが表示されます。

ステップ 2　[Create Rule] をクリックします。

[Create Rule] ページが表示されます。

ステップ 3　[Message] フィールドに、イベントと一緒に表示するメッセージを入力します。

イベント メッセージの詳細については、イベント メッセージの定義（36-12 ページ）を参照してください。

ヒント　ルール メッセージの指定は必須です。また、空白文字のみ、1 つ以上の引用符のみ、1 つ以上のアポストロフィのみ、あるいは空白文字/引用符/アポストロフィだけの組み合わせでメッセージを構成することはできません。

ステップ 4　[Classification] リストから、イベントのタイプを表す分類を選択します。

使用可能な分類の詳細については、侵入イベント分類の定義（36-13 ページ）を参照してください。

ステップ 5　[Action] リストから、作成するルールのタイプを選択します。次のいずれかを使用できます。

- トラフィックがルールをトリガーとして使用したときにイベントを生成するルールを作成するには、[alert] を選択します。
- ルールをトリガーとして使用したトラフィックを無視するルールを作成するには、[pass] を選択します。

ステップ 6　[Protocol] リストから、ルールで検査するパケットのトラフィック プロトコル（**tcp**、**udp**、**icmp**、または **ip**）を選択します。

プロトコル タイプの選択方法については、プロトコルの指定（36-5 ページ）を参照してください。

ステップ 7　[Source IPs] フィールドで、ルールをトリガーとして使用するトラフィックの送信元 IP アドレスまたはアドレス ブロックを入力します。[Destination IPs] フィールドで、ルールをトリガーとして使用するトラフィックの宛先 IP アドレスまたはアドレス ブロックを入力します。

ルール エディタで指定できる IP アドレス構文の詳細については、侵入ルールでの IP アドレスの指定（36-5 ページ）を参照してください。

ステップ 8　[Source Port] フィールドで、ルールをトリガーとして使用するトラフィックの送信元ポート番号を入力します。[Destination Port] フィールドで、ルールをトリガーとして使用するトラフィックの受信側ポート番号を入力します。

注　プロトコルが ip に設定されている場合、システムは侵入ルール 見出し内のポート定義を無視します。

ルール エディタで指定できるポート構文の詳細については、侵入ルールでのポートの定義（36-9 ページ）を参照してください。

ステップ 9　[Direction] リストから、ルールをトリガーとして使用するトラフィックの方向を示す演算子を選択します。次のいずれかを使用できます。

- [Directional]：送信元 IP アドレスから宛先 IP アドレスに移動するトラフィックを照合します
- [Bidirectional]：双方向に移動するトラフィックを照合します

ステップ 10　[Detection Options] リストから、使用するキーワードを選択します。

ステップ 11　[Add option] をクリックします。

ステップ 12　追加したキーワードで指定する引数を入力します。ルール キーワードとその使用方法については、ルールでのキーワードと引数について（36-10 ページ）を参照してください。

キーワードと引数を追加するときには、次の操作を実行することもできます。

- 追加した後のキーワードを並べ替えるには、移動するキーワードの横にある上矢印または下矢印をクリックします。
- キーワードを削除するには、そのキーワードの横にある [X] をクリックします。

追加するキーワード オプションごとに、ステップ 10 ～ 12 を繰り返します。

ステップ 13　ルールを保存するには、[Save as New] をクリックします。

システムは、ルール番号シーケンスの中でローカル ルールとして次に使用可能な Snort ID（SID）番号をルールに割り当て、ローカル ルール カテゴリ内にルールを保存します。

新しい（または変更された）ルールを適切な侵入ポリシー内で有効にして、侵入ポリシーをアクセス コントロール ポリシーの一部として適用するまでは、そのルールに照らしたトラフィックの評価が開始しません。詳細については、「アクセス コントロール ポリシーの適用（12-17 ページ）」を参照してください。

既存のルールの変更

ライセンス： Protection

カスタム標準テキスト ルールを変更できます。また、Cisco提供の標準テキスト ルールまたは shared object ruleを変更して保存すると、そのルールの 1 つ以上のインスタンスが新たに作成されます。

ルールを作成したり、Ciscoのルールを変更したりすると、新しいルールまたはリビジョンがローカル ルール カテゴリにコピーされ、100000 より大きい次に使用可能な Snort ID（SID）がそのルールに割り当てられます。

shared object ruleでは、ヘッダ情報だけを変更することができます。shared object rule内で使用されるルール キーワードやその引数を変更することはできません。shared object ruleの見出し情報を変更して変更内容を保存すると、ルールの新しいインスタンスが作成され、ジェネレータ ID（GID）3、およびカスタム ルールとして次に使用可能な SID が割り当てられます。ルール エディタは、shared object ruleの新しいインスタンスを予約済み soid キーワードにリンクします。これにより、作成したルールが VRT 作成のルールにマップされます。作成したshared object ruleのイ

ンスタンスを削除できますが、Cisco提供のshared object ruleは削除できません。詳細については、ルール見出しについて（36-3 ページ）およびカスタム ルールの削除（36-113 ページ）を参照してください。

注 shared object ruleのプロトコルを変更しないでください。変更した場合、ルールの効果がなくなる可能性があります。

ルールを変更する方法：

アクセス： Admin/Intrusion Admin

ステップ 1 [Policies] > [Intrusion] > [Rule Editor] の順に選択します。

[Rule Editor] ページが表示されます。

ステップ 2 変更する 1 つ以上のルールを探します。次の選択肢があります。

- ルール カテゴリを参照することによってルールを探すには、フォルダを通して該当するルールまで移動し、そのルールの横にある編集アイコン（）をクリックします。
- 検索機能によってルールを探すには、該当するルールの検索基準（最も単純なものは SID）を入力して [Search] をクリックします。検索によって返された該当するルールをクリックします。詳細については、「ルールの検索（36-114 ページ）」を参照してください。
- ページに表示するルールを絞り込むことによってルールを探すには、ルール リストの左上にあるフィルタ アイコン（）で示されるテキスト ボックスにルール フィルタを入力します。該当するルールまで移動して、そのルールの横にある編集アイコン（）をクリックします。詳細については、「ルール エディタ ページでのルールのフィルタ処理（36-116 ページ）」を参照してください。

ルール エディタが開いて、選択したルールが表示されます。

shared object ruleを選択した場合は、ルール 見出し情報だけがルール エディタに表示されることに注意してください。ルール エディタ ページでshared object ruleを識別するには、リストの中で数字の 3（GID）で始まる項目を探します（たとえば 3:1000004）。

ステップ 3 ルールを変更して（ルール オプションの詳細については 新しいルールの作成（36-109 ページ）を参照）、[Save as New] をクリックします。

ルールがローカル ルール カテゴリに保存されます。

ヒント システム ルールの代わりに、ローカルで変更したルールを使用するには、ルール状態の設定（32-22 ページ）の手順に従ってシステム ルールを非アクティブにした後、ローカル ルールをアクティブにします。

ステップ 4 変更を適用するには、アクセス コントロール ポリシーの適用（12-17 ページ）の説明に従って侵入ポリシーをアクセス コントロール ポリシーの一部として適用し、アクティブにします。

ルールにコメントを追加する

ライセンス： Protection

任意の侵入ルールにコメントを追加できます。これにより、ルールについて、およびルールで識別される exploit やポリシー違反についての追加のコンテキストと情報を提供できます。

コメントをルールに追加する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Rule Editor] の順に選択します。

[Rule Editor] ページが表示されます。

ステップ 2　注釈を付けるルールを探します。次の選択肢があります。

- ルール カテゴリを参照することによってルールを探すには、フォルダを通して該当するルールまで移動し、そのルールの横の編集アイコン（）をクリックします。
- 検索機能によってルールを探すには、該当するルールの検索基準（最も単純な基準は SID）を入力して [Search] をクリックします。検索で返された該当するルールをクリックします。詳細については、「ルールの検索（36-114 ページ）」を参照してください。
- ページに表示するルールを絞り込むことによってルールを探すには、ルール リストの左上にあるフィルタ アイコン（）で示されるテキスト ボックスでルール フィルタを入力します。該当するルールまで移動して、そのルールの横にある編集アイコン（）をクリックします。詳細については、「ルール エディタ ページでのルールのフィルタ処理（36-116 ページ）」を参照してください。

ルール エディタが表示されます。

ステップ 3　[Rule Comment] をクリックします。

[Rule Comment] ページが表示されます。

ステップ 4　テキスト ボックスにコメントを入力し、[Add Comment] をクリックします。

コメント テキスト ボックスにコメントが保存されます。

ヒント　また、侵入イベントのパケット ビューで、ルール コメントを追加して表示することもできます。詳細については、イベント情報の表示（41-25 ページ）を参照してください。

カスタム ルールの削除

ライセンス：Protection

侵入ポリシーで現在有効になっていないカスタム ルールを削除することができます。Cisco提供の標準テキスト ルールやshared object ruleは削除できません。

削除されたルールは削除済みカテゴリに保存されます。削除済みのルールを、新しいルールの基準として使用することができます。ルールの編集方法については、既存のルールの変更（36-111 ページ）を参照してください。

侵入ポリシーの [Rules] ページには削除済みカテゴリが表示されないため、削除したカスタム ルールを有効にすることはできません。

なお、[Rule Updates] ページですべてのローカル ルールを削除することもできます。たとえば、ワンタイム ルール更新の使用（66-18 ページ）を参照してください。

詳細については、次の項を参照してください。

- カスタム ルールの作成方法については、新しいルールの作成（36-109 ページ）を参照してください。

- ローカル ルールのインポート方法については、ルールの更新とローカル ルール ファイルのインポート（66-16 ページ）を参照してください。
- ルール状態の設定方法については、ルール状態の設定（32-22 ページ）を参照してください。

カスタム ルールを削除する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Rule Editor] の順に選択します。

[Rule Editor] ページが表示されます。

ステップ 2　次の 2 つの選択肢があります。

- [Delete Local Rules] をクリックしてから、[OK] をクリックします。

  変更内容が保存された侵入ポリシー内で現在有効になっていないすべてのルールは、ローカル ルール カテゴリから削除され、削除済みカテゴリに移動されます。
- フォルダを通してローカル ルール カテゴリまで移動します。ローカル ルール カテゴリをクリックして展開してから、削除するルールの横にある削除アイコン（ ）をクリックします。

  ルールがローカル ルール カテゴリから削除され、削除済みカテゴリに移動されます。

  カスタム標準テキスト ルールにはジェネレータ ID（GID）1 が割り当てられ（たとえば 1:1000012）、カスタムshared object ruleには GID として 3 が割り当てられる（たとえば 3:1000005）ことに注意してください。

ヒント　また、見出し情報を変更して保存したshared object ruleもローカル ルール カテゴリに保管され、それらは GID 3 で列挙されます。独自に変更したshared object ruleを削除できますが、元のshared object ruleは削除できません。

ルールの検索

ライセンス： Protection

FireSIGHT システムには何千もの標準テキスト ルールが含まれています。Cisco脆弱性調査チームは新しい脆弱性や exploit が発見されるたびにルールを追加し続けています。特定のルールを簡単に検索して、それをアクティブ化、非アクティブ化、または編集することができます。

次の表に、使用可能な検索オプションについて説明します。

表 36-61　ルール検索基準

オプション	説明
シグニチャ ID	Snort ID（シグネチャ ID とも呼ばれる）に基づいて 1 つのルールを検索するには、Snort ID 番号を入力します。複数のルールを検索するには、複数の Snort ID 番号をカンマで区切ったリストを入力します。このフィールドには 80 文字の制限があります。
ジェネレータ ID	標準テキスト ルールを検索するには、**1** を選択します。shared object ruleを検索するには、**3** を選択します。

表 36-61　ルール検索基準（続き）

オプション	説明
メッセージ	特定のメッセージを含むルールを検索するには、ルール メッセージの 1 つの単語を [Message] フィールドに入力します。たとえば、DNS exploit を検索するには「DNS」と入力し、バッファ オーバーフロー exploit を検索するには「overflow」と入力します。
Protocol	特定のプロトコルのトラフィックを評価するルールを検索には、プロトコルを選択します。プロトコルを選択しない場合、検索結果にはすべてのプロトコルのルールが含まれます。
送信元ポート	指定したポートからの発信パケットを検査するルールを検索するには、送信元ポート番号またはポート関連の変数を入力します。
宛先ポート	特定のポート宛てのパケットを検査するルールを検索するには、宛先ポート番号またはポート関連の変数を入力します。
Source IP	指定した IP アドレスからの発信パケットを検査するルールを検索するには、送信元 IP アドレスまたは IP アドレス関連の変数を入力します。
宛先 IP	指定した IP アドレス宛てのパケットを検査するルールを検索するには、宛先 IP アドレスまたは IP アドレス関連の変数を入力します。
キーワード	特定のキーワードを検索するには、キーワード検索オプションを使用できます。検索対象のキーワードとキーワード値を選択します。また、キーワード値の前に感嘆符（!）を付けると、指定した値以外の値を照合できます。
カテゴリ	特定のカテゴリ内のルールを検索するには、[Category] リストからカテゴリを選択します。
分類	特定の分類が設定されたルールを検索するには、[Classification] リストから分類名を選択します。
Rule State	特定のポリシー内のルールおよび特定のルール状態を検索するには、最初の [Rule State] リストからポリシーを選択し、2 番目のリストから状態を選択して、[Generate Events]、[Drop and Generate Events]、または [Disabled] に設定されたルールを検索します。

特定のルールを検索する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Rule Editor] の順に選択します。

[Rule Editor] ページが表示されます。

ステップ 2　ツールバーで [Search] をクリックします。

[Search] ページが表示されます。

ステップ 3　ルール検索基準の表に示すフィールドを使用して、検索基準を追加します。

注　ルールを検索するには、少なくとも 1 つの検索基準を指定する必要があります。

ステップ 4　特定のキーワードを含むルールを検索するには、次の手順に従います。

- [Keyword] セクションのドロップダウン リストから、検索するキーワードを選択します。

  使用可能なキーワードのリストについては、ルールでのキーワードと引数について（36-10 ページ）を参照してください。

- [Keyword] フィールドに、検索する引数を入力します。

ステップ 5　[Search] をクリックします。

ページがリロードされ、検索基準に一致するルールのリストが表示されます。

ステップ 6　ルール（システム ルールの場合はルールのコピー）を表示または編集するには、ハイパーリンクが付いたルール メッセージをクリックします。ルールの編集方法の詳細については、既存のルールの変更（36-111 ページ）を参照してください。

ルール エディタ ページでのルールのフィルタ処理

ライセンス： Protection

ルール エディタ ページ上でルールをフィルタ処理して、ルールのサブセットを表示させることができます。たとえば、あるルールまたはその状態を変更したいが、数千ものルールの中からそれを見つけるのが困難な場合に、この機能が役立つことがあります。

フィルタを入力すると、1 つ以上の一致するルールを含むフォルダがページに表示され、一致するルールがない場合はメッセージが表示されます。フィルタには、特殊なキーワードとその引数、文字列、引用符で囲んだリテラル文字列、さらに複数のフィルタ条件を区切るスペースを含めることができます。ただし、正規表現、ワイルドカード文字、および否定文字（!）、「大なり」記号（>）、「小なり」記号（<）などの特殊な演算子をフィルタに含めることはできません。

すべてのキーワード、キーワード引数、および文字列では大文字と小文字が区別されません。`gid` キーワードと `sid` キーワードを除き、すべての引数と文字列は部分的な文字列として扱われます。`gid` と `sid` の引数は、完全一致のみを返します。

オプションで、フィルタ処理前の元のページで 1 つのフォルダを展開すると、その後のフィルタ処理でそのフォルダ内の一致が返されるときにフォルダが展開したままになります。探しているルールが多数のルールを含むフォルダ内に存在する場合には、これが役立つことがあります。

1 つのフィルタを後続の別のフィルタで制約することはできません。入力されたフィルタは、ルール データベース全体を検索して、一致するすべてのルールを返します。前回のフィルタ結果がページに表示されている状態でフィルタを入力すると、そのページの内容が消去され、代わりに新しいフィルタの結果が返されます。

フィルタ処理されている場合もされていない場合も、リスト内のルールで同じ機能を使用できます。たとえば、ルール エディタ ページでは、リストがフィルタ処理されているかどうかに関わらず、リスト内のルールを編集できます。また、ページのコンテキスト メニューの任意のオプションを使用することもできます。

詳細については、次の項を参照してください。

- ルール フィルタでのキーワードの使用（36-117 ページ）
- ルール フィルタでの文字列の使用（36-118 ページ）
- ルール フィルタでのキーワードと文字列の組み合わせ（36-118 ページ）
- ルールのフィルタ処理（36-119 ページ）

ルール フィルタでのキーワードの使用

ライセンス：Protection

各ルール フィルタに、次の形式で 1 つ以上のキーワードを含めることができます。

keyword:*argument*

ここで、*keyword* はルール フィルタ キーワードの表のいずれかのキーワード、*argument* はキーワードに関連する特定のフィールドで検索する 1 つの英数字文字列です（大文字/小文字の区別はありません）。

gid と sid を除くすべてのキーワードの引数は、部分的な文字列として扱われます。たとえば、引数 123 によって "12345"、"41235"、"45123" などが返されます。gid と sid の引数は完全一致のみを返します。たとえば、sid:3080 によって SID 3080 のみが返されます。

ヒント　1 つ以上の文字列でフィルタ処理することによって、SID を部分的に検索できます。詳細については、「ルール フィルタでの文字列の使用（36-118 ページ）」を参照してください。

次の表に、ルールのフィルタ処理に使用できる特定のフィルタリング キーワードと引数を示します。

表 36-62　ルール フィルタ キーワード

キーワード	説明	例
arachnids	ルール参照内の Arachnids ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。詳細については、「イベント参照の定義（36-15 ページ）」を参照してください。	arachnids:181
bugtraq	ルール参照内の Bugtraq ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。詳細については、「イベント参照の定義（36-15 ページ）」を参照してください。	bugtraq:2120
cve	ルール参照内の CVE 番号全体またはその一部分に基づいて 1 つ以上のルールを返します。詳細については、「イベント参照の定義（36-15 ページ）」を参照してください。	cve:2003-0109
gid	引数 1 は標準テキスト ルールを返します。引数 3 はshared object ruleを返します。詳細については、プリプロセッサ ジェネレータ ID の読み取り（41-42 ページ）および表 32-1（32-2 ページ）を参照してください。	gid:3
mcafee	ルール参照内の McAfee ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。詳細については、「イベント参照の定義（36-15 ページ）」を参照してください。	mcafee:10566
msg	ルール Message フィールド（イベント メッセージとも呼ばれる）の全体またはその一部分に基づいて 1 つ以上のルールを返します。詳細については、「イベント メッセージの定義（36-12 ページ）」を参照してください。	msg:chat
nessus	ルール参照内の Nessus ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。詳細については、「イベント参照の定義（36-15 ページ）」を参照してください。	nessus:10737

表 36-62　ルール フィルタ キーワード（続き）

キーワード	説明	例
ref	ルール参照内またはルール Message フィールド内の単一の英数字文字列の全体または一部分に基づいて、1 つ以上のルールを返します。詳細については、イベント参照の定義（36-15 ページ）およびイベント メッセージの定義（36-12 ページ）を参照してください。	ref:MS03-039
sid	完全に一致するシグニチャ ID を持つルールを返します。詳細については、「プリプロセッサ ジェネレータ ID の読み取り（41-42 ページ）」を参照してください。	sid:235
url	ルール参照内の URL 全体またはその一部分に基づいて 1 つ以上のルールを返します。詳細については、「イベント参照の定義（36-15 ページ）」を参照してください。	url:faqs.org

ルール フィルタでの文字列の使用

ライセンス：Protection

各ルール フィルタに 1 つ以上の英数字文字列を含めることができます。文字列により、ルール **Message** フィールド、シグニチャ ID、およびジェネレータ ID が検索されます。たとえば、文字列 `123` を指定するとルール メッセージ内の文字列「`Lotus123`」や「`123mania`」などが返され、さらに SID 6123、SID 12375 なども返されます。ルール **Message** フィールドの詳細については、イベント メッセージの定義（36-12 ページ）を参照してください。ルール SID と GID の詳細については、プリプロセッサ ジェネレータ ID の読み取り（41-42 ページ）を参照してください。

すべての文字列では大文字と小文字が区別されず、部分的な文字列として扱われます。たとえば、文字列 `ADMIN`、`admin`、または `Admin` はすべて、「`admin`」、「`CFADMIN`」、「`Administrator`」などを返します。

文字列を引用符で囲むと、完全一致を返すことができます。たとえば、引用符付きのリテラル文字列 `"overflow attempt"` は完全一致のみを返しますが、引用符なしの 2 つの文字列 `overflow` と `attempt` で構成されるフィルタは「`overflow attempt`」、「`overflow multipacket attempt`」、「`overflow with evasion attempt`」などを返します。

ルール フィルタでのキーワードと文字列の組み合わせ

ライセンス：Protection

複数のキーワード、文字列、またはその両方をスペースで区切って任意に組み合わせて入力することで、フィルタ結果を絞り込むことができます。結果には、すべてのフィルタ条件に一致するルールが含まれます。

複数のフィルタ条件を任意の順序で入力できます。たとえば、次のフィルタはそれぞれ同じルールを返します。

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

ルールのフィルタ処理

ライセンス：Protection

ルール エディタ ページ上でルールをフィルタ処理して、ルールのサブセットを表示させると、特定のルールを見つけやすくなります。その後、コンテキスト メニューで使用可能な機能の選択など、任意のページ機能を使用できます。

特定のルールをフィルタ処理する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Rule Editor] の順に選択します。

[Rule Editor] ページが表示されます。

ルール フィルタ機能は、ルール エディタ ページで編集するルールを見つけるときに特に役立つことがあります。詳細については、「既存のルールの変更（36-111 ページ）」を参照してください。

ステップ 2　オプションで、[Group Rules By] リストで別のグループ化方法を選択します。

ヒント　すべてのサブグループ内のルールの総計が多い場合は、フィルタリングに時間がかかることがあります。これは、ルール自体の数が少なくても、1 つのルールが複数のカテゴリに属していることがあるためです。

ステップ 3　オプションで、展開するグループの横にあるフォルダをクリックします。

フォルダが展開されて、そのグループ内のルールが表示されます。ルール グループによっては、さらに展開可能なサブグループが存在します。

また、ルールがどのグループに含まれているか予想できる場合は、フィルタ処理前の元のページでそのグループを展開しておくと便利なことがあります。その後のフィルタ処理でそのフォルダ内の一致が返されるとき、およびフィルタ消去アイコン（ ）をクリックしてフィルタ処理前のページに戻ったときに、グループが展開されたままになります。

ステップ 4　フィルタ テキスト ボックスをアクティブにするには、ルール リストの左上にあるテキスト ボックス内のフィルタ アイコン（ ）の右側をクリックします。

ステップ 5　フィルタ制約を入力し、Enter キーを押します。

フィルタには、キーワードと引数、引用符付きまたは引用符なしの文字列、および複数の条件を区切るスペースを含めることができます。詳細については、「ルール エディタ ページでのルールのフィルタ処理（36-116 ページ）」を参照してください。

ページが更新されて、一致するルールを少なくとも 1 つ含むグループが表示されます。

ステップ 6　オプションで、まだ開いていないフォルダを開くと、一致するルールが表示されます。次のフィルタリング選択肢があります。

- 新しいフィルタを入力するには、フィルタ テキスト ボックス内にカーソルを移動してクリックし、そのボックスをアクティブにしてから、フィルタを入力して Enter キーを押します。
- フィルタ処理された現在のリストを消去してフィルタ処理前の元のページに戻すには、フィルタ消去アイコン（ ）をクリックします。

ステップ 7　オプションで、ページに表示されているルールを通常の方法で変更します。既存のルールの変更（36-111 ページ）を参照してください。

変更内容を有効にするには、アクセス コントロール ポリシーの適用（12-17 ページ）の説明に従って、アクセス コントロール ポリシーの侵入ポリシー部分を適用します。

CHAPTER 37

マルウェアと禁止されたファイルのブロッキング

悪意のあるソフトウェア、つまり *マルウェア*は、複数のルートで組織のネットワークに入る可能性があります。マルウェアの影響を特定して軽減するために、FireSIGHT システムのファイル制御、ネットワーク ファイル トラジェクトリ、および高度なマルウェア対策の各コンポーネントを使用すると、マルウェアやその他の種類のファイルがネットワーク トラフィックで伝送されるのを検出、追跡、保存、分析、および任意でブロックすることができます。また、システムは、アーカイブ ファイル内のネストされたファイルを分析して処理することができます(アーカイブ ファイル形式 `.zip` または `.rar`)。

全体的なアクセス制御設定の一部として、マルウェア対策とファイル制御を実行するようにシステムを設定できます。作成してアクセス コントロール ルールに関連付けた *ファイル ポリシー*は、ルールに一致するネットワーク トラフィックを処理します。そのトラフィックで検出されたファイルをダウンロードした後、ファイルのシグネチャの*動的分析*用にそのファイルを Cisco のマルウェア認識ネットワーク(*Collective Security Intelligence クラウド* と呼ばれる)に送信することで、そのファイルにマルウェアが含まれるかどうか判断できます。

コンテキスト エクスプローラとダッシュボードは、組織のネットワーク トラフィックで検出されたファイル(マルウェア ファイルを含む)のさまざまな概要表示を提供します。分析のターゲットをさらに絞り込むために、マルウェア ファイルの [network file trajectory] ページを使用して、ホスト間での個々の脅威の広がりを時系列で追跡できます。これにより、最も効果的なアウトブレイク制御と防止対策に集中できます。

ファイル ポリシーはどのライセンスでも作成可能ですが、マルウェア対策とファイル制御の一部の操作を行うには、次の表に示すように、ライセンス供与される特定の機能をターゲット デバイスで有効にする必要があります。

表 37-1　侵入インスペクションおよびファイル インスペクションのライセンスおよびアプライアンスの要件

機能	説明	追加する必要のあるライセンス	追加先となる Defense Center	それを以下のデバイスで有効にする
侵入防御	侵入およびエクスプロイトを検出し、任意でブロックします	Protection	いずれか	いずれか
ファイル制御	ファイル タイプの伝送を検出し、任意でブロックします	Protection	いずれか	いずれか

表 37-1　侵入インスペクションおよびファイル インスペクションのライセンスおよびアプライアンスの要件（続き）

機能	説明	追加する必要のあるライセンス	追加先となる Defense Center	それを以下のデバイスで有効にする
高度なマルウェア防御（AMP）	マルウェアの伝送を検出、保存、追跡し、任意でブロックします キャプチャしたファイルを Cisco クラウドに送信し、マルウェアの分析を行います	Malware	すべて（DC500 を除く）	すべて（シリーズ 2 または X-Series を除く）

また、お客様の組織で FireAMP サブスクリプションをご利用の場合、Defense Center は、Cisco クラウドからエンドポイント ベースのマルウェア検出データを受信することもできます。Defense Center は、このデータを、ネットワークベースのファイルおよびシステム生成のマルウェア データとともに提示します。FireAMP データのインポートには、FireAMP サブスクリプションに加えてライセンスは必要ありません。詳細については、FireAMP 用のクラウド接続の操作（37-27 ページ）を参照してください。

クラウドベースのファイルおよびマルウェア機能については、組織が追加のセキュリティを必要とする場合や、外部接続を制限したい場合に、標準のクラウド接続の代わりに FireAMP プライベート クラウドを使用できます。すべてのファイルおよびマルウェアのクラウド検索、および FireAMP エンドポイントからのイベント データの収集とリレーは、プライベート クラウドを介して処理されます。プライベート クラウドは、パブリックの Cisco クラウドに接続したときに、エンドポイント イベント データを送信しない匿名化されたプロキシ接続を介してこれらの処理を行います。

詳細については、以下を参照してください。

- マルウェア対策とファイル制御について（37-2 ページ）
- ファイル ポリシーの概要と作成（37-10 ページ）
- FireAMP 用のクラウド接続の操作（37-27 ページ）

マルウェア対策とファイル制御に関連するイベント データの評価の詳細については、マルウェアとファイル アクティビティの分析（40-1 ページ）を参照してください。

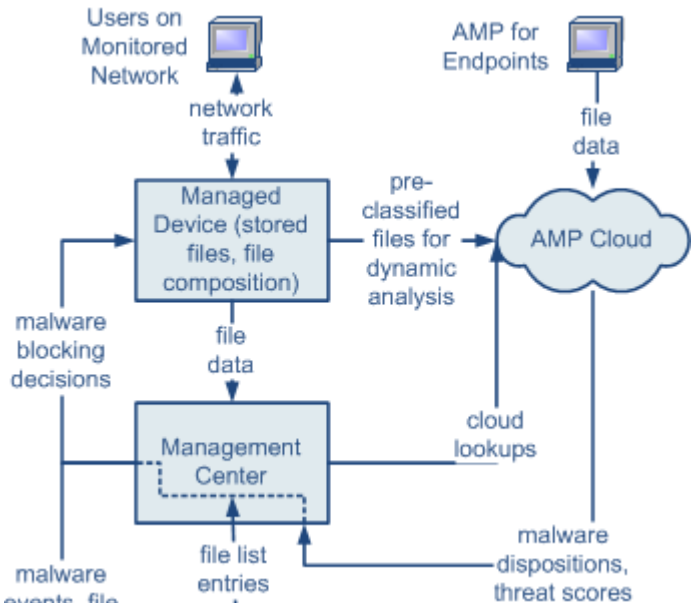
マルウェア対策とファイル制御について

ライセンス： Protection、Malware、または任意

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

*高度なマルウェア対策*機能を使用すると、次の図に示すように、ネットワークで伝送されるマルウェア ファイルを検出、保存、追跡、分析、および（オプションで）ブロックするよう FireSIGHT システムを設定できます。



システムは、PDF、Microsoft Office 文書など多数のファイル タイプに潜むマルウェアを検出し、オプションでブロックできます。管理対象デバイスは、特定のアプリケーション プロトコル ベースのネットワーク トラフィック内で、これらのファイル タイプの伝送を監視します。該当するファイルを検出した場合、デバイスはそのファイルの SHA256 ハッシュ値を Defense Center に送信できます。その後、その情報を使って*マルウェア クラウド ルックアップ*が実行されます。これらの結果に基づき、Cisco クラウドはDefense Centerにファイルの性質を返します。

システムがネットワーク トラフィック内でファイルを検出すると、デバイスは*ファイル ストレージ*機能を使用して、該当するファイルをハード ドライブまたはマルウェア ストレージ パックに保存できます。性質が不明な実行可能ファイルについては、デバイスでそのファイルを保存するかどうかに関係なく、*動的分析*のためにファイルを送信できます。クラウドはDefense Center に次の情報を返します。

- ファイルにマルウェアが含まれている可能性を記述する脅威スコア、および
- クラウドがその脅威スコアを割り当てた理由を詳述する動的分析概要レポート。

また、該当する実行可能ファイルが見つかった場合、デバイスはファイル構造のスペロ分析を実行し、結果として得られたスペロ シグネチャをクラウドに送信できます。クラウドはこのシグネチャを動的分析の補足情報として使用し、ファイルがマルウェアであるかどうかを判断します。

クラウドにあるファイルの性質が不正確だとわかっている場合、次のようにして、ファイルの SHA256 値をファイル リストに追加できます。

- クラウドがクリーンの性質を割り当てた場合と同じ方法でファイルを扱うには、*クリーン リスト*にファイルを追加します。
- クラウドがマルウェアの性質を割り当てた場合と同じ方法でファイルを扱うには、*カスタム検出リスト*にファイルを追加します。

あるファイルの SHA-256 値がファイル リスト内で検出されると、システムはマルウェア ルックアップの実行もファイルの性質の検査も行わずに、適切なアクションを実行します。ファイルの SHA 値を計算するには、**マルウェア クラウド ルックアップ** アクションと**マルウェア ブロック** アクションのどちらか、および一致するファイル タイプを使用して、ファイル ポリシー内のルールを設定する必要があることに注意してください。ファイル ポリシーごとに、クリーン リストまたはカスタム検出リストの使用を有効にできます。ファイル リストの管理の詳細については、ファイル リストの操作（3-36 ページ）を参照してください。

システムは、通常の圧縮されていないファイルを分析/処理するのと同じ方法で、アーカイブ ファイル（.zip や .rar アーカイブ ファイルなど）内のネストされたファイルを検査し、ブロックできます。ただし、システムがネストされたファイルをブロックすると、それを含むアーカイブ ファイル全体がブロックされることに注意してください。システムは、最も外側のアーカイブ ファイル（レベル 0）の下にネストされた最大 3 つのレベルのファイルを検査できます。指定したレベルのネストを超えるアーカイブ ファイルをブロックするようにファイル ポリシーを設定できます（最大 3 つのレベルまで）。

また、コンテンツが暗号化されているか、または検査できないアーカイブ ファイルをブロックするようにファイル ポリシーを設定することもできます。アーカイブ ファイルのインスペクションの詳細については、アーカイブ ファイルのインスペクション オプションの設定（37-22 ページ）を参照してください。

ファイルを検査またはブロックするには、ポリシーを適用する管理対象デバイスでProtectionライセンスを有効にする必要があります。また、ファイルの保存、マルウェア ファイルに関するマルウェア クラウド ルックアップと（オプションの）ブロック操作、動的分析のためのクラウドへのファイル送信、またはファイル リストへのファイルの追加を行うには、それらのデバイスに Malware ライセンスも有効にする必要があります。

ファイルの性質について

システムは、Cisco クラウドから返される性質に基づいてファイルの性質を決定します。Cisco クラウドから返された情報、ファイル リストへの追加操作、または脅威スコアに応じて、ファイルの性質は次のいずれかになります。

- **マルウェア**は、クラウドでそのファイルがマルウェアとして分類されていること、またはファイルの脅威スコアが、ファイル ポリシーで定義されたマルウェアしきい値を超えていることを示します。
- **クリーン**は、クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。
- **不明**は、クラウドが性質を割り当てる前にマルウェア クラウド ルックアップが行われたことを示します。クラウドはそのファイルをまだ分類していません。
- **カスタム検出**は、ユーザがカスタム検出リストにファイルを追加したことを示します。
- **使用不可**は、Defense Centerがマルウェア クラウド ルックアップを実行できなかったことを示します。この性質で見られるイベントはごくわずかである可能性があります。これは予期された動作です。

ヒント　高速連続で複数の**使用不可な**マルウェア イベントが発生した場合は、クラウド接続およびポート設定を確認してください。詳細については、セキュリティ、インターネット アクセス、および通信ポート（E-1 ページ）を参照してください。

アーカイブ ファイルの性質は、アーカイブ内部のファイルに割り当てられた性質に基づきます。内容に基づくアーカイブ ファイルの性質に、アーカイブに含まれるファイルのさまざまな組み合わせによって決定されるアーカイブ ファイルの性質を示します。識別されたマルウェア ファイルを含んでいる**すべて**のアーカイブは、**マルウェア**の性質になります。識別されたマルウェア ファイルを含んでいないアーカイブの場合、いずれかの不明なファイルが含まれていれば Unknown の性質、クリーン ファイルのみが含まれていれば Clean の性質になります。アーカイブ ファイルのインスペクションの詳細については、アーカイブ ファイルのインスペクション オプションの設定（37-22 ページ）を参照してください。他のファイルと同様に、アーカイブ ファイルには、その性質に関する条件が適用される場合、Custom Detection または Unavailable の性質が割り当てられる場合があります。

表 37-2　内容に基づくアーカイブ ファイルの性質

アーカイブ ファイルの性質	不明なファイルの数	クリーン ファイルの数	マルウェア ファイルの数
不明(Unknown)	1 つ以上	いずれか	0
Clean	0	1 つ以上	0
マルウェア	いずれか	いずれか	1 つ以上

ファイルの性質に基づき、ファイルをブロックするか、ファイルのダウンロード/アップロードを許可するよう、Defense Centerが管理対象デバイスに指示します。アーカイブ ファイル内のネストされたファイルがブロックされている場合は、システムはアーカイブ ファイル全体をブロックすることに注意してください。パフォーマンスを改善させるために、SHA256 値に基づくファイルの性質がシステムですでにわかっている場合、Defense Center は Cisco クラウドに照会する代わりに、キャッシュ済みの性質を使用します。

ファイルの性質は変更される可能性があることに注意してください。たとえば、クラウドによる判定の結果、以前はクリーンであると考えられていたファイルが今はマルウェアとして識別されるようになったり、その逆、つまりマルウェアと識別されたファイルが実際にはクリーンであったりする可能性があります。あるファイルに関するマルウェア ルックアップを先週実行した後、そのファイルの性質が変更された場合は、クラウドがDefense Centerに通知を送ります。これにより、そのファイルの伝送が次回検出されたときにシステムは適切なアクションを実行できます。変更されたファイルの性質は、*レトロスペクティブ*な性質と呼ばれます。

マルウェア クラウド ルックアップから戻されたファイルの性質、およびそれに関連する脅威スコアには、存続可能時間(TTL)値が割り当てられます。ファイルの性質が更新されないまま、TTL 値で指定された期間にわたって保持された後は、キャッシュ情報が消去されます。性質および関連する脅威スコアには次の TTL 値が割り当てられます。

- クリーン:4 時間
- 不明:1 時間
- マルウェア:1 時間

キャッシュに照らしたマルウェア クラウド ルックアップの結果、キャッシュ済み性質がタイムアウトになったことが識別されると、システムはファイルの性質を判別するために新しいルックアップを実行します。

ファイル制御について

マルウェア ファイル伝送のブロックに加えて、(マルウェアを含むかどうかにかかわらず)特定のタイプのすべてのファイルをブロックする必要がある場合は、*ファイル制御*機能により防御網を広げることができます。マルウェア対策の場合と同様に、管理対象デバイスはネットワーク トラフィック内で特定のファイル タイプの伝送を監視し、そのファイルをブロックまたは許可します。

システムでマルウェアを検出できるすべてのファイル タイプだけでなく、さらに多数のファイル タイプに対するファイル制御がサポートされています。これらのファイル タイプは、マルチメディア(swf、mp3)、実行可能ファイル(exe、トレント)、PDF などの基本的なカテゴリにグループ分けされます。ファイル制御はマルウェア対策とは異なり、Cisco クラウドへの照会を必要としないことに注意してください。

キャプチャされたファイル、ファイル イベント、およびマルウェア イベントを分析に使用する

ファイルが転送またはブロックされると、システムはマルウェア イベントやファイル イベントを生成します。また、システムは、管理対象デバイスでキャプチャされたファイルの情報を収集します。Defense Centerの Web インターフェイスを使用して、これらのイベントと情報を表示することができます。また、コンテキスト エクスプローラとダッシュボードには、組織で検出されたファイル(マルウェア ファイルを含む)のさまざまなタイプの概要が表示されます。

分析ターゲットをさらに絞り込むために、*ネットワーク ファイル トラジェクトリ*機能を使用すると、個々のファイルの転送パスを追跡できます。ファイルの伝搬経路ページには、ファイルの概要情報、ホスト間のファイル転送(ブロックされた転送も含む)を示すグラフィカル マップ、およびそれらのファイルの検出/ブロックに関連するマルウェア イベントまたはファイル イベントが表示されます。

DC500 では Malware ライセンスを使用できず、シリーズ 2 デバイスまたは Cisco NGIPS for Blue Coat X-Series で Malware ライセンスを有効にすることもできないので、これらのアプライアンスを使用して個別のファイルをキャプチャまたはブロックしたり、動的分析用にファイルを送信したり、マルウェア クラウド ルックアップの対象となるファイル トラジェクトリを表示したりすることはできないことに注意してください。

詳細については、次の項を参照してください。

- マルウェア対策とファイル制御の設定(37-6 ページ)
- マルウェア対策とファイル制御に基づくイベントのロギング(37-7 ページ)
- FireAMP と FireSIGHT システムの統合(37-8 ページ)
- ネットワークベースの AMP とエンドポイント ベースの FireAMP の比較(37-9 ページ)
- ネットワーク ファイル トラジェクトリの操作(40-37 ページ)

マルウェア対策とファイル制御の設定

ライセンス: ProtectionまたはMalware

サポートされるデバイス: 機能によって異なる

サポートされる防御センター: 機能によって異なる

ファイル ポリシーをアクセス コントロール ルールに関連付けることで、全体的なアクセス制御設定の一部として、マルウェア対策とファイル制御を設定します。この関連付けにより、アクセス コントロール ルールの条件と一致するトラフィック内のファイルを通過させる前に、システムは必ずファイルを検査するようになります。

ファイル ポリシーには、親アクセス コントロール ポリシーと同様に、各ルールの条件に一致するファイルの処理方法を決定するルールがいくつか含まれています。ファイル タイプ、アプリケーション プロトコル、転送方向の違いに応じて異なるアクションを実行する別個のファイル ルールを設定できます。

あるファイルがルールに一致する場合、ルールで以下を実行できます。

- 単純なファイル タイプ照合に基づいてファイルを許可またはブロックする
- マルウェア ファイルの性質に基づいてファイルをブロックする
- ファイルをキャプチャしてデバイスに保存する
- キャプチャされたファイルを動的分析のために送信する

さらに、ファイル ポリシーでは以下を実行できます。

- クリーン リストまたはカスタム検出リストのエントリに基づいて、ファイルがクリーンまたはマルウェアである場合と同じ方法で自動的にファイルを扱う

- ファイルの脅威スコアが、設定可能なしきい値を超えた場合、マルウェアと同じ方法でファイルを扱う
- アーカイブ ファイル（.zip や .rar など）の内容を検査する
- アーカイブ ファイルの内容が暗号化されている場合、アーカイブのネスト レベルが最大レベル指定値より深い場合、あるいはその反対で検査できない場合、アーカイブ ファイルをブロックする

単純な例として、ユーザによる実行可能ファイルのダウンロードをブロックするファイル ポリシーを導入できます。別の例として、ダウンロードされた PDF でマルウェアを検査し、見つかった場合はそれをブロックできます。ファイル ポリシーについて、およびファイル ポリシーとアクセス コントロール ルールとの関連付けについての詳細は、ファイル ポリシーの概要と作成（37-10 ページ）および侵入防御パフォーマンスの調整（18-10 ページ）を参照してください。

DC500 では Malware ライセンスを使用できないため、このアプライアンスを使用して、ネットワークベースのマルウェア防御やアーカイブ ファイルの内容の検査を行うファイル ポリシーを適用することはできません。同様に、シリーズ 2 デバイスまたは Cisco NGIPS for Blue Coat X-Series では Malware ライセンスを有効にできないため、ネットワークベースのマルウェア防御やアーカイブ ファイルの内容の検査を行うファイル ポリシーをこのアプライアンスに適用することはできません。

マルウェア対策とファイル制御に基づくイベントのロギング

ライセンス： ProtectionまたはMalware

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

Defense Centerは、システムでのファイル インスペクション レコードをログに記録し、次に示すキャプチャされたファイル、ファイル イベント、マルウェア イベントとしての処理を記録します。

- *キャプチャされたファイル*は、システムでキャプチャされたファイルを表します。
- *ファイル イベント*は、システムがネットワーク トラフィック内で検出した（さらにオプションでブロックした）ファイルを表します。
- *マルウェア イベント*は、システムがネットワーク トラフィック内で検出した（さらにオプションでブロックした）マルウェア ファイルを表します。
- *遡及的マルウェア イベント*は、マルウェア ファイルの性質が変更されたファイルを表します。

ファイル内のマルウェアを検出するために、システムはまずファイル自体を検出する必要があるため、ネットワーク トラフィック内のマルウェア検出/ブロックに基づいてシステムがマルウェア イベントを生成するときには、ファイル イベントも生成します。FireAMP コネクタによって生成されたエンドポイント ベースのマルウェア イベント（FireAMP と FireSIGHT システムの統合（37-8 ページ）を参照）には、対応するファイル イベントがないことに注意してください。同様に、システムがネットワーク トラフィック内でファイルをキャプチャするとき、システムはまずファイルを検出するため、ファイル イベントも生成されます。

Defense Centerを使用すると、キャプチャされたファイル、ファイル イベント、およびマルウェア イベントを表示、操作、分析して、分析内容を他のユーザに伝達できます。コンテキスト エクスプローラ、ダッシュボード、イベント ビューア、ネットワーク ファイル トラジェクトリ マップ、およびレポート機能を使用すると、検出/キャプチャ/ブロックされたファイルとマルウェアについてより詳しく理解できます。また、イベントを使用して相関ポリシー違反をトリガーしたり、電子メール、SMTP、または syslog によるアラートを発行したりすることもできます。ファイル イベントとマルウェア イベントの詳細については、ファイル イベントの操作（40-8 ページ）およびマルウェア イベントの操作（40-17 ページ）を参照してください。

DC500 では Malware ライセンスを使用できず、シリーズ 2 デバイスまたは Cisco NGIPS for Blue Coat X-Series では Malware ライセンスを有効にすることもできません。このため、これらのアプライアンスを使用して、マルウェア クラウド ルックアップまたはアーカイブ ファイルの内容に関連するキャプチャされたファイル、ファイル イベント、およびマルウェア イベントを生成/分析することはできません。

FireAMP と FireSIGHT システムの統合

ライセンス: すべて

FireAMP は Cisco のエンタープライズクラスの高度なマルウェア分析および防御ソリューションで、高度なマルウェアの発生、高度で継続的な脅威、および標的型攻撃を検出、認識、ブロックします。

お客様の組織で FireAMP サブスクリプションをご利用の場合、個々のユーザはエンドポイント（コンピュータとモバイル デバイス）に *FireAMP コネクタ*をインストールします。FireAMP コネクタはさまざまな機能を備えた軽量エージェントです。特に、アップロード、ダウンロード、実行、オープン、コピー、移動などの際にファイルを検査する機能があります。検査対象のファイルにマルウェアが含まれるかどうかを判断するために、これらのコネクタはCisco クラウドと通信します。

ファイルがマルウェアとして識別された場合、クラウドは脅威の識別情報をDefense Centerに送ります。さらにクラウドは、スキャン、検疫、実行のブロッキング、クラウド リコールなど、他の種類のデータをDefense Centerに送ることもできます。Defense Centerはこれらの情報をマルウェア イベントとしてログに記録します。

FireAMP 展開を使用すると、マルウェア イベントに基づいて Defense Center で開始される修復やアラート発行を設定できることに加えて、FireAMP ポータル（http://amp.sourcefire.com/）を使ってマルウェアの影響を軽減することもできます。ポータルに備わっている堅牢かつ柔軟な Web インターフェイスを使用すると、FireAMP 展開のすべての局面を制御し、アウトブレイクのすべての段階を管理できます。次の作業を実行できます。

- 組織全体のためにカスタム マルウェア検出ポリシーとプロファイルを設定し、すべてのユーザのファイルに対してフラッシュ スキャンおよび完全スキャンを実行する
- マルウェア分析の実行: ヒートマップ、詳細なファイル情報、ネットワーク ファイル トラジェクトリ、脅威の根本原因の表示など
- アウトブレイク制御のさまざまな局面を設定する: 自動検疫、検疫されていない実行可能ファイルの実行を停止するアプリケーション ブロッキング、除外リストなど
- カスタム保護の作成、グループ ポリシーに基づく特定のアプリケーションの実行ブロッキング、およびカスタム ホワイトリストの作成

詳細については、次の項を参照してください。

- ネットワークベースの AMP とエンドポイント ベースの FireAMP の比較（37-9 ページ）に、Cisco製品ファミリで使用可能なマルウェア対策戦略の比較を示します。
- FireAMP 用のクラウド接続の操作（37-27 ページ）では、Defense Center と Cisco クラウドの間の通信を直接確立する方法、または FireAMP プライベート クラウド接続によって確立する方法を説明します。

ヒント FireAMP の詳細については、FireAMP ポータルのオンライン ヘルプを参照してください。

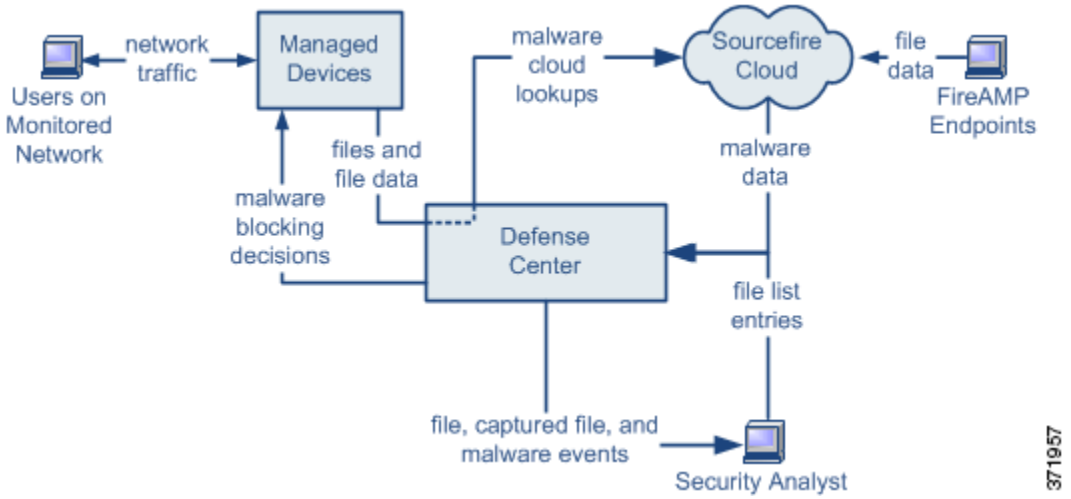
ネットワークベースの AMP とエンドポイント ベースの FireAMP の比較

ライセンス: Malware または任意

サポートされるデバイス: 機能によって異なる

サポートされる防御センター: 機能によって異なる

ネットワークベースの高度なマルウェア対策戦略と、エンドポイント ベースの FireAMP 戦略の両方からのデータをDefense Centerでどのように使用できるかを次の図に示します。



FireAMP のマルウェア検出はダウンロード時または実行時にエンドポイントで行われるのに対し、管理対象デバイスはネットワーク トラフィック内でマルウェアを検出するため、この 2 種類のマルウェア イベントの情報が異なることに注意してください。たとえば、エンドポイント ベースのマルウェア イベントには、ファイル パス、呼び出し元クライアント アプリケーションなどの情報が含まれるのに対して、ネットワーク トラフィックでのマルウェア検出には、ファイル伝送に使われた接続のポート、アプリケーション プロトコル、発信元 IP アドレス情報が含まれます。

別の例として、ネットワークベースのマルウェア イベントにおけるユーザ情報は、ネットワーク検出で判別されたマルウェア宛先ホストに最後にログインしたユーザを表します。一方、FireAMP で報告されるユーザは、ローカル コネクタで判別されるマルウェア検出場所のエンドポイントに現在ログインしているユーザを表します。

注　エンドポイント ベースのマルウェア イベントで報告された IP アドレスは、組織のネットワーク マップに含まれない可能性があり、モニタ対象のネットワークにも含まれない可能性があります。展開方法、ネットワーク アーキテクチャ、コンプライアンス レベル、その他の要因により、コネクタがインストールされているエンドポイントは、管理対象デバイスによってモニタされるのと同じホストでない可能性があります。

DC500 では Malware ライセンスを使用できず、シリーズ 2 デバイスまたは Cisco NGIPS for Blue Coat X-Series で Malware ライセンスを有効にすることもできません。したがって、これらのアプライアンスを使用して個別のファイルをキャプチャ/ブロックしたり、動的分析用にファイルを送信したり、アーカイブ ファイルの内容を検査したり、マルウェア クラウド ルックアップの対象となるファイルのトラジェクトリを表示したりすることはできません。

次の表に、2 つの戦略の違いをまとめます。

表 37-3　ネットワークベースとエンドポイント ベースのマルウェア対策戦略の比較

機能	ネットワークベース	エンドポイント ベース（FireAMP）
ファイル タイプの検出とブロッキングの方法（ファイル制御）	ネットワーク トラフィックで、アクセス コントロール ポリシーとファイル ポリシーを使用	未サポート
マルウェアの検出とブロッキングの方法	ネットワーク トラフィックで、アクセス コントロール ポリシーとファイル ポリシーを使用	個々のエンドポイントで、Cisco クラウドとの通信を行うインストール済みコネクタを使用
検査されるネットワーク トラフィック	管理対象デバイスを通過するトラフィック	なし（エンドポイントにインストールされたコネクタがファイルを直接検査します）
マルウェア検出の堅牢性	限定されたファイル タイプ	すべてのファイル タイプ
マルウェア分析の選択肢	Defense Center ベース、およびクラウドでの分析	Defense Center ベース、および FireAMP ポータルでの追加のオプション
マルウェアの影響軽減	ネットワーク トラフィックでのマルウェア ブロッキング、Defense Centerが開始する修復	FireAMP ベースの検疫およびアウトブレイク制御オプション、Defense Center が開始する修復
生成されるイベント	ファイル イベント、キャプチャされたファイル、マルウェア イベント、およびレトロスペクティブ マルウェア イベント	マルウェア イベント
マルウェア イベント内の情報	基本的なマルウェア イベント情報、および接続データ（IP アドレス、ポート、アプリケーション プロトコル）	詳細なマルウェア イベント情報（接続データなし）
ネットワーク ファイル トラジェクトリ	Defense Center ベース	Defense Center ベース、および FireAMP ポータルでの追加のオプション
必要なライセンスまたはサブスクリプション	ファイル制御を実行するにはProtection ライセンス、マルウェア対策を実行するには Malware ライセンス	FireAMP サブスクリプション（ライセンス ベースではない）

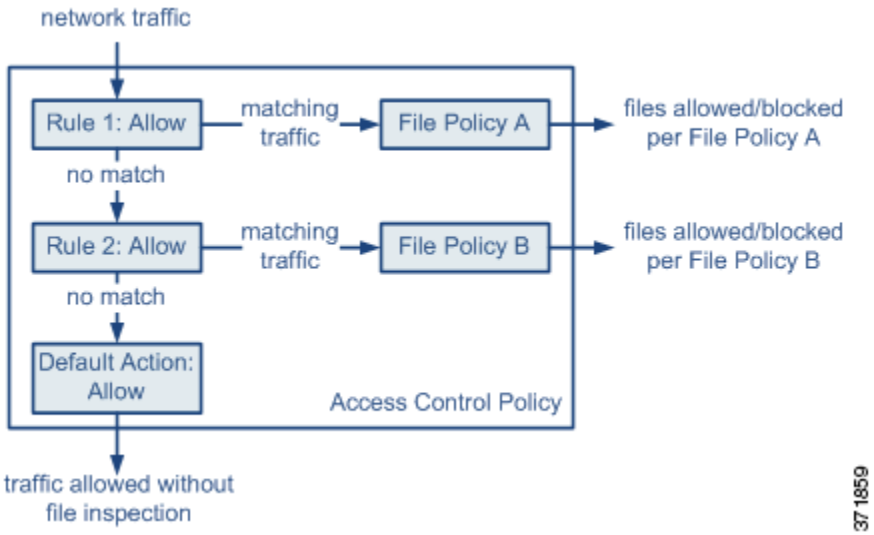
ファイル ポリシーの概要と作成

ライセンス： ProtectionまたはMalware

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

ファイル ポリシーは、いくつかの設定からなるセットです。システムは全体的なアクセス制御設定の一部としてこれを使用して、高度なマルウェア対策とファイル制御を実行できます。次の図のような、インライン展開での単純なアクセス コントロール ポリシーがあるとします。



このポリシーには 2 つのアクセス コントロール ルールがあり、両方とも許可アクションを使用し、ファイル ポリシーに関連付けられています。このポリシーのデフォルト アクションもまた「トラフィックの許可」ですが、ファイル ポリシー インスペクションはありません。このシナリオでは、トラフィックは次のように処理されます。

- **ルール** 1 に一致するトラフィックは**ファイル ポリシー** A で検査されます。
- **ルール** 1 に一致しないトラフィックは**ルール** 2 に照らして評価されます。**ルール** 2 に一致するトラフィックは**ファイル ポリシー** B で検査されます。
- どちらのルールにも一致しないトラフィックは許可されます。デフォルト アクションにファイル ポリシーを関連付けることはできません。

ファイル ポリシーには、親アクセス コントロール ポリシーと同様に、各ルールの条件に一致するファイルの処理方法を決定するルールがいくつか含まれています。ファイル タイプ、アプリケーション プロトコル、転送方向の違いに応じて異なるアクションを実行する別個のファイル ルールを設定できます。

ファイルがルールに一致する場合、ルールで以下を実行できます。

- 単純なファイル タイプ照合に基づいてファイルを許可またはブロックする
- マルウェア ファイルの性質に基づいてファイルをブロックする
- キャプチャされたファイルをデバイスに保存する
- キャプチャされたファイルを動的分析のために送信する

さらに、ファイル ポリシーでは以下を実行できます。

- クリーン リストまたはカスタム検出リストのエントリに基づいて、ファイルがクリーンまたはマルウェアである場合と同じ方法で自動的にファイルを扱う
- ファイルの脅威スコアが、設定可能なしきい値を超えた場合、マルウェアと同じ方法でファイルを扱う
- アーカイブ ファイル（.zip や .rar など）の内容を検査する
- アーカイブ ファイルの内容が暗号化されている場合、アーカイブのネスト レベルが最大レベル指定値より深い場合、あるいはその反対で検査できない場合、アーカイブ ファイルをブロックする

1 つのファイル ポリシーを、**許可**、**インタラクティブ ブロック**、または **リセット付きインタラクティブ ブロック** アクションを含むアクセス コントロール ルールに関連付けることができます。その後、システムはそのファイル ポリシーを使用して、アクセス コントロール ルールの条件を満たすネットワーク トラフィックを検査します。異なるファイル ポリシーを個々のアクセス コントロール ルールに関連付けることにより、ネットワークで伝送されるファイルを識別/ブロックする方法をきめ細かく制御できます。ただし、アクセス制御のデフォルト アクションによって処理されるトラフィックを検査するためにファイル ポリシーを使用**できない**ことに注意してください。詳細については、許可されたトラフィックに対する侵入およびマルウェアの有無のインスペクション（18-2 ページ）を参照してください。

ファイル ルール

ファイル ポリシーの中でファイル ルールを設定します。次の表に、ファイル ルールのコンポーネントを示します。

表 37-4　ファイル ルールのコンポーネント

ファイル ルールのコンポーネント	説明
アプリケーション プロトコル	システムは、FTP、HTTP、SMTP、IMAP、POP3、および NetBIOS-ssn（SMB）を介して伝送されるファイルを検出し、検査できます。パフォーマンスを向上させるには、ファイル ルールごとに、これらのアプリケーション プロトコルのうち 1 つだけでファイルを検出するよう限定できます。
転送の方向	ダウンロードされるファイルに対して、FTP、HTTP、IMAP、POP3、および NetBIOS-ssn（SMB）の着信トラフィックを検査できます。アップロードされるファイルに対しては、FTP、HTTP、SMTP、および NetBIOS-ssn（SMB）の発信トラフィックを検査できます。
ファイルのカテゴリとタイプ	システムは、さまざまなタイプのファイルを検出できます。これらのファイル タイプは、マルチメディア（swf、mp3）、実行可能ファイル（exe、トレント）、PDF などの基本的なカテゴリにグループ分けされます。個々のファイル タイプを検出したり、ファイル タイプ カテゴリ全体を検出したりするよう、ファイル ルールを設定できます。 たとえば、すべてのマルチメディア ファイルをブロックしたり、Shockwave Flash（swf）ファイルのみをブロックしたりできます。または、ユーザが BitTorrent（torrent）ファイルをダウンロードしたときにアラートを出すよう、システムを設定できます。 ⚠ **注意**　頻繁にトリガーされるファイル ルールは、システム パフォーマンスに影響を与える可能性があります。たとえば、HTTP トラフィックでマルチメディア ファイルを検出しようとすると（たとえば YouTube は多量の Flash コンテンツを伝送します）、膨大な数のイベントが生成される可能性があります。
ファイル ルール アクション	ファイル ルール アクションは、ルールの条件に一致するトラフィックがシステムによってどのように処理されるかを決定します。 **注**　複数のファイル ルールは（数値順ではなく）ルール アクション順に評価されます。詳細については、次の項（ファイル ルール アクションと評価順序）を参照してください。

ファイル ルール アクションと評価順序

各ファイル ルールには、ルールの条件に一致するトラフィックがシステムによってどのように処理されるかを決定する 1 つのアクションが関連付けられます。1 つのファイル ポリシー内に、ファイル タイプ、アプリケーション プロトコル、転送方向の違いに応じて異なるアクションを実行する別々のルールを設定できます。複数のルール アクションは、以下のようなルール アクション順になります。

- *ファイル ブロック* ルールを使用すると、特定のファイル タイプをブロックできます。
- *マルウェア ブロック* ルールを使用すると、特定のファイル タイプの SHA-256 ハッシュ値を計算した後、クラウド ルックアップ プロセスを使用して、ネットワークを通過するファイルにマルウェアが含まれているかどうかまず判断し、脅威を示すファイルをブロックできます。
- *マルウェア クラウド ルックアップ* ルールを使用すると、ネットワークを通過するファイルの伝送を許可しながら、クラウド ルックアップに基づいてそのファイルのマルウェアの性質をログに記録できます。
- *ファイル検出* ルールを使用すると、ファイルの伝送を許可しながら、特定のファイル タイプの検出をデータベースに記録できます。

各ファイル ルール アクションごとに、ファイル転送がブロックされたときに接続をリセットするオプション、キャプチャされたファイルを管理対象デバイスに保存するオプション、およびキャプチャされたファイルを動的分析とスペロ分析のためクラウドに送信するオプションを設定できます。次の表に、各ファイル アクションで使用可能なオプションの詳細を示します。

表 37-5　　ファイル ルール アクション

アクション	接続をリセットするか	ファイルを保存するか	動的分析をするか	MSEXE 用のスペロ分析をするか
ファイル ブロック	はい(推奨)	はい:一致するすべてのファイルを保存できます	いいえ	いいえ
マルウェア ブロック	はい(推奨)	はい:選択したファイルの性質に一致するファイル タイプを保存できます	はい:不明なファイルの性質の実行可能ファイルを送信できます	はい:実行可能ファイルを送信できます
ファイル検出	いいえ	はい:一致するすべてのファイルを保存できます	いいえ	いいえ
マルウェア クラウド ルックアップ	いいえ	はい:選択したファイルの性質に一致するファイル タイプを保存できます	はい:不明なファイルの性質の実行可能ファイルを送信できます	はい:実行可能ファイルを送信できます

ファイルとマルウェアの検出、キャプチャ、およびブロッキングに関する注意事項と制約事項

ファイルとマルウェアの検出、キャプチャ、およびブロッキングの動作に関して、以下の詳細および制限に注意してください。

- ファイルの終わりを示す End of File マーカーが検出されない場合、転送プロトコルとは無関係に、そのファイルは**マルウェア ブロック** ルールでもカスタム検出リストでもブロックされません。システムは、End of File マーカーで示されるファイル全体の受信が完了するまでファイルのブロックを待機し、このマーカーが検出された後にファイルをブロックします。

- FTP ファイル転送で End of File マーカーが最終データ セグメントとは別に伝送される場合、マーカーがブロックされ、ファイル転送失敗が FTP クライアントに表示されますが、実際にはそのファイルは完全にディスクに転送されます。
- FTP は、さまざまなチャネルを介してコマンドおよびデータを転送します。パッシブまたはインライン タップ モードの展開では、FTP データ セッションとその制御セッションからのトラフィックは同じ Snort に負荷分散されない場合があります。
- ファイルがアプリケーション プロトコル条件を持つルールに一致する場合、ファイル イベントの生成は、システムがファイルのアプリケーション プロトコルを正常に識別した後に行われます。識別されていないファイルは、ファイル イベントを生成しません。
- FTP に関する**マルウェア ブロック** ルールを持つファイル ポリシーを使用するアクセス コントロール ポリシーでは、[Drop when Inline] を無効にした侵入ポリシーをデフォルト アクションに設定した場合、システムはルールに一致するファイルやマルウェアの検出でイベントを生成しますが、ファイルをドロップしません。FTP ファイア転送をブロックし、ファイル ポリシーを選択するアクセス コントロール ポリシーのデフォルト アクションとして侵入ポリシーを使用するには、[Drop when Inline] を有効にした侵入ポリシーを選択する必要があります。
- **ファイル ブロック** アクションおよび **マルウェア ブロック** アクションを持つファイル ルールでは、最初のファイル転送試行後 24 時間で検出される、同じファイル、URL、サーバ、クライアント アプリケーションを使った新しいセッションをブロックすることにより、HTTP 経由のファイル ダウンロードの自動再開をブロックします。
- まれに、HTTP アップロード セッションからのトラフィックが不適切である場合、システムはトラフィックを正しく再構築できなくなり、トラフィックのブロックやファイル イベントの生成を行いません。
- **ファイル ブロック** ルールでブロックされる NetBios-ssn 経由ファイル転送（SMB ファイル転送など）の場合、宛先ホストでファイルが見つかることがあります。ただし、ダウンロード開始後にファイルがブロックされ、結果としてファイル転送が不完全になるため、そのファイルは使用できません。
- （SMB ファイル転送など）NetBIOS-ssn 経由で転送されるファイルを検出またはブロックするファイル ルールを作成した場合、ファイル ポリシーを呼び出すアクセス コントロール ポリシーの適用前に開始された、確立済み TCP または SMB セッションで転送されるファイルに対しては、検査が行われません。このため、これらのファイルは検出/ブロックされません。
- パッシブ展開でファイルをブロックするよう設定されたルールは、一致するファイルをブロックしません。接続ではファイル伝送が続行されるため、接続の開始をログに記録するルールを設定した場合、この接続に関して複数のイベントが記録されることがあります。
- POP3、POP、SMTP、または IMAP セッションでのすべてのファイル名の合計バイト数が 1024 を超えると、セッションのファイル イベントでは、ファイル名バッファがいっぱいになった後で検出されたファイルの名前が正しく反映されないことがあります。
- SMTP 経由でテキスト ベースのファイルを送信すると、一部のメール クライアントは改行を CRLF 改行文字標準に変換します。MAC ベースのホストは復帰（CR）文字を使用し、Unix/Linux ベースのホストは改行（LF）文字を使用するので、メール クライアントによる改行変換によってファイルのサイズが変更される場合があります。一部のメール クライアントは、認識できないファイル タイプを処理する際に改行変換を行うようデフォルト設定されていることに注意してください。
- Ciscoでは、**ファイル ブロック** アクションと **マルウェア ブロック** アクションで**接続のリセット**を有効にすることを推奨しています。これにより、ブロックされたアプリケーション セッションが TCP 接続リセットまで開いたままになることを防止できます。接続をリセットしない場合、TCP 接続が自身をリセットするまで、クライアント セッションが開いたままになります。

- **マルウェア クラウド ルックアップ** アクションまたは **マルウェア ブロック** アクションを使ってファイル ルールが設定されている場合、Defense Centerがクラウドとの接続を確立できないと、クラウド接続が復元されるまで、システムは設定済みルール アクション オプションを実行できません。
- 大量のトラフィックをモニタしている場合、キャプチャしたすべてのファイルを保存したり、動的分析用に送信したり**しないでください**。そのようにすると、システム パフォーマンスに悪影響が及ぶことがあります。

注　ファイルがセッションで検出されブロックされるまで、セッションからのパケットは侵入インスペクションの対象になります。

ファイル ルールの評価例

番号順にルールが評価されるアクセス コントロール ポリシーとは異なり、ファイル ポリシーではファイル ルール アクションと評価順序(37-13 ページ)に従ってファイルが処理されます。つまり、(優先度の高い順に)単純なブロッキング、次にマルウェア インスペクションとブロッキング、さらにその次に単純な検出とロギングとなります。例として、1 つのファイル ポリシー内に、PDF ファイルを処理する 4 つのルールがあるとします。Web インターフェイスで表示される順序に関係なく、これらのルールは次の順序で評価されます。

表 37-6　　ファイル ルールの評価順序の例

App.Protocol	方向	Action	アクションのオプション	結果
SMTP	Upload	ファイル ブロック	接続のリセット	ユーザが電子メールで PDF ファイルを送信することをブロックし、接続をリセットします。
FTP	Download	マルウェア ブロック	不明な性質のファイルを保存、接続のリセット	ファイル転送を介したマルウェア PDF ファイルのダウンロードをブロックし、不明なファイルの性質を持つファイルをデバイスに保存して、接続をリセットします。
POP3 IMAP	Download	マルウェア クラウド ルックアップ	不明な性質のファイルを保存、動的分析	電子メールで受信された PDF ファイルに対してマルウェア検査を行い、不明なファイルの性質持つファイルをデバイスに保存します。動的分析用に、Cisco クラウドにファイルを送信します。
いずれか	いずれか	ファイル検出	none	ユーザが Web 上で(つまり HTTP 経由で)PDF ファイルを表示すると、それを検出してログに記録しますが、トラフィックは許可します。

Defense Centerでは、矛盾するファイル ルールを示すために警告アイコン( )を使用します。警告アイコンの上にポインタを置くと詳細が表示されます。

システムで検出されるすべてのファイル タイプに対してマルウェア分析を実行できるわけではないことに注意してください。[Application Protocol] 、[Direction of Transfer]、および [Action] ドロップダウン リストで値を選択すると、システムはファイル タイプのリストを限定します。

DC500 ではMalware ライセンスを使用できないため、マルウェア ブロック アクションやマルウェア クラウド ルックアップ アクションを使用するファイル ルールを作成したり、それらのアクションを行うルールを含むファイル ポリシーを適用するためにこのアプライアンスを使用し

たりできないことに注意してください。同様に、シリーズ 2 デバイスまたは Cisco NGIPS for Blue Coat X-Series では Malware ライセンスを有効にできないため、これらのアクションを行うルールを含むファイル ポリシーをこのアプライアンスに適用することはできません。

キャプチャされたファイル、ファイル イベント、マルウェア イベントおよびアラートのロギング

ファイル ポリシーをアクセス コントロール ルールに関連付けると、一致するトラフィックに関するファイル イベントとマルウェア イベントのロギングが自動的に有効になります。また、ファイルをキャプチャ/保存するようファイル ポリシーが設定されている場合、ファイルがキャプチャされると、キャプチャされたファイルのロギングも自動的に有効になります。ファイルを検査するときに、システムは次のタイプのイベントを生成できます。

- *ファイル イベント*:検出またはブロックされたファイル、および検出されたマルウェア ファイルを表します
- *マルウェア イベント*:検出されたマルウェア ファイルを表します
- *レトロスペクティブ マルウェア イベント*:以前に検出されたファイルに関する「マルウェア」ファイルの性質が変更された場合に、生成されます

ファイル ポリシーでファイル イベントまたはマルウェア イベントが生成されるか、ファイルがキャプチャされると、システムは（起動元のアクセス コントロール ルールにおけるロギング設定とは無関係に）関連する接続の終了をDefense Center データベースに自動的に記録します。

注　NetBIOS-ssn（SMB）トラフィックの検査によって生成されるファイル イベントは、即座には接続イベントを生成しません。これは、クライアントとサーバが持続的接続を確立するためです。システムはクライアントまたはサーバがセッションを終了した後に接続イベントを生成します。

これらの接続イベントごとに、

- [Files] フィールドには、接続で検出されたファイル数（マルウェア ファイルを含む）を示すアイコン（  ）が含まれます。このアイコンをクリックすると、それらのファイルのリスト、およびマルウェア ファイルの性質が表示されます。
- [Reason] フィールドには、接続イベントがログに記録された理由が示されます。これはファイル ルール アクションに応じて次のように異なります。
- [File Monitor]:ファイル検出ルールおよびマルウェア クラウド ルックアップ ルールの場合、およびクリーン リスト内のファイルの場合
- [File Block]:ファイル ブロック ルールまたはマルウェア ブロック ルールの場合
- [File Custom Detection]: カスタム検出リストにあるファイルをシステムが検出した場合
- [File Resume Allow]:ファイル ブロック ルールまたはマルウェア ブロック ルールによってファイル伝送が最初にブロックされた場合。ファイルを許可する新しいアクセス コントロール ポリシーが適用された後、HTTP セッションが自動的に再開しました。
- [File Resume Block]:ファイル検出ルールまたはマルウェア クラウド ルックアップ ルールによってファイル伝送が最初に許可された場合。ファイルをブロックする新しいアクセス コントロール ポリシーが適用された後、HTTP セッションが自動的に停止しました。
- ファイルやマルウェアがブロックされた接続では、[Action] が [Block] になります。

Defense Centerの Web インターフェイスを使用すると、FireSIGHT システムで生成されるすべての種類のイベントと同様に、ファイル イベントとマルウェア イベントを表示、操作、および分析できます。また、マルウェア イベントを使用して相関ポリシー違反をトリガーしたり、電子メール、SMTP、または syslog によるアラートを発行したりすることもできます。

注　さらに、組織の FireAMP サブスクリプションを使用して、Defense Center でマルウェア イベントを受信することもできます。これらのマルウェア イベントはダウンロード時または実行時にエンドポイントで生成されるため、その情報はネットワークベースのマルウェア イベントの情報とは異なります。

接続イベント、ファイル イベント、マルウェア イベント、およびそれらのロギングの詳細については、以下を参照してください。

- ネットワーク トラフィックの接続のロギング（38-1 ページ）
- ファイル イベントの操作（40-8 ページ）
- マルウェア イベントの操作（40-17 ページ）
- 接続およびセキュリティ インテリジェンスのデータについて（39-2 ページ）

インターネット アクセスとハイ アベイラビリティ

システムはポート 443 を使用して、ネットワーク ベース AMP 用のマルウェア クラウド ルックアップを実行します。Defense Centerでこのポートをアウトバウンドに開く必要があります。

ハイ アベイラビリティ ペアのDefense Centerはファイル ポリシーおよび関連する設定を共有しますが、クラウド接続、キャプチャされたファイル、ファイル イベント、マルウェア イベントを共有することはありません。継続的な運用を維持し、検出されるファイルのマルウェアの性質が両方のDefense Centerで必ず同じになるようにするには、プライマリとセカンダリの両方のDefense Centerからクラウドにアクセスできる必要があります。

また、動的分析のためにクラウドにファイルを送信するには、デバイスでポート 443 をアウトバウンドに開く必要があります。

注　FireAMP プライベート クラウドには、Cisco のパブリック クラウド接続と同じオープン ポートを必要とし、同じハイ アベイラビリティ制限事項があることに注意してください。

ファイル ポリシーの管理

[File Policies] ページ（[Policies] > [Files]）でファイル ポリシーの作成、編集、削除、および比較を行います。ここには既存のファイル ポリシーのリストと、それらの最終更新日が表示されます。

ファイル ポリシーの適用アイコン（）をクリックするとダイアログ ボックスが表示され、そのファイル ポリシーを使用するアクセス コントロール ポリシーが示された後、[Access Control Policy] ページにリダイレクトされます。これは、ファイル ポリシーが親アクセス コントロール ポリシーの一部と見なされ、ファイル ポリシーを単独で適用できないためです。新しいファイル ポリシーを使用したり、既存のファイル ポリシーの変更内容を適用したりするには、親アクセス コントロール ポリシーを適用/再適用する必要があります。

次の点に注意してください。

- 動的分析の対象となるファイル タイプのリストが更新されたかどうか検査するために、システムはクラウドに照会します（多くても 1 日に 1 回）。対象となるファイル タイプのリストが変更された場合、これはファイル ポリシーの変更を意味します。このファイル ポリシーを使用するアクセス コントロール ポリシーがいずれかのデバイスに適用されている場合、そのアクセス コントロール ポリシーには失効マークが付けられます。更新されたファイル ポリシーをデバイスに適用するには、親アクセス コントロール ポリシーを再適用する必要があります。
- 保存済みまたは適用済みのアクセス コントロール ポリシーで使われているファイル ポリシーは削除できません。

ファイル ポリシーの管理の詳細については、次の項を参照してください。

- ファイル ポリシーの作成（37-18 ページ）
- ファイル ルールの操作（37-19 ページ）
- 2 つのファイル ポリシーの比較（37-26 ページ）

ファイル ポリシーの作成

ライセンス： ProtectionまたはMalware

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

ファイル ポリシーを作成して、その中でルールを設定すると、それをアクセス コントロール ポリシーで使用できるようになります。

DC500 ではMalware ライセンスを使用できないため、マルウェア ブロック アクションやマルウェア クラウド ルックアップ アクションを使用するファイル ルールを作成したり、それらのアクションを行うルールを含むファイル ポリシーを適用するためにこのアプライアンスを使用したりできないことに注意してください。同様に、シリーズ 2 デバイスまたは Cisco NGIPS for Blue Coat X-Series では Malware ライセンスを有効にできないため、これらのアクションを行うルールを含むファイル ポリシーをこのアプライアンスに適用することはできません。

ヒント 既存のファイル ポリシーのコピーを作成するには、コピー アイコン（）をクリックして、表示されるダイアログ ボックスで新しいポリシーの固有名を入力します。その後、そのコピーを変更できます。

ファイル ポリシーを作成する方法：

アクセス： Admin/Access Admin

ステップ 1　[Policies] > [Files] を選択します。

[File Policies] ページが表示されます。

ステップ 2　[New File Policy] をクリックします。

[New File Policy] ダイアログ ボックスが表示されます。

新しいポリシーの場合、ポリシーが使用中でないことが Web インターフェイスに示されます。使用中のファイル ポリシーを編集している場合は、そのファイル ポリシーを使用しているアクセス コントロール ポリシーの数が Web インターフェイスに示されます。どちらの場合も、テキストをクリックすると [Access Control Policies] ページに移動できます（アクセス コントロール ポリシーの開始（12-1 ページ）を参照）。

ステップ 3　新しいポリシーの [Name] とオプションの [Description] を入力してから、[Save] をクリックします。

[File Policy Rules] タブが表示されます。

ステップ 4　ファイル ポリシーに 1 つ以上のルールを追加します。

ファイル ルールを使用すると、ロギング、ブロック、またはマルウェア スキャンの対象となるファイル タイプを詳細に制御できます。ファイル ルールの追加については、ファイル ルールの操作（37-19 ページ）を参照してください。

DC500 ではMalware ライセンスを使用できないため、マルウェア ブロック アクションやマルウェア クラウド ルックアップ アクションを使用するファイル ルールを作成したり、それらのアクションを行うルールを含むファイル ポリシーを適用するためにこのアプライアンスを使用したりできません。同様に、シリーズ 2 デバイスまたは Cisco NGIPS for Blue Coat X-Series では Malware ライセンスを有効にできないため、これらのアクションを行うルールを含むファイル ポリシーをこのアプライアンスに適用することはできません。

ステップ 5　詳細オプションを設定します。詳細については、ファイル ポリシーの詳細オプション（General）の設定（37-21 ページ）およびアーカイブ ファイルのインスペクション オプションの設定（37-22 ページ）を参照してください。

ステップ 6　[Save] をクリックします。

新しいポリシーを使用するには、アクセス コントロール ルールにファイル ポリシーを追加してから、アクセス コントロール ポリシーを適用する必要があります。既存のファイル ポリシーを編集している場合は、そのファイル ポリシーを使用するすべてのアクセス コントロール ポリシーを再適用する必要があります。

ファイル ルールの操作

ライセンス： ProtectionまたはMalware

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

効果を発揮するには、ファイル ポリシーに 1 つ以上のルールが含まれている必要があります。新しいファイル ポリシーを作成するとき、または既存のポリシーを編集するときに表示される [File Policy Rules] ページで、ルールを作成、編集、および削除します。このページには、ポリシー内のすべてのルールがリストされ、各ルールの基本的な特性も示されます。

また、このページでは、このファイル ポリシーを使用するアクセス コントロール ポリシーの数も通知されます。この通知をクリックすると、親ポリシーのリストが表示され、オプションで [Access Control Policies] ページに進むことができます。

ファイル ルールを作成する方法：

アクセス： Admin/Access Admin

ステップ 1　[Policies] > [Files] を選択します。

[File Policies] ページが表示されます。

ステップ 2　次の選択肢があります。

- 新しいポリシーにルールを追加するには、[New File Policy] をクリックして、新しいポリシーを作成します（ファイル ポリシーの作成（37-18 ページ）を参照）。
- 既存のポリシーにルールを追加するには、ポリシーの横にある編集アイコン（  ）をクリックします。

ステップ 3　表示される [File Policy Rules] ページで、[Add File Rule] をクリックします。

[Add File Rule] ダイアログ ボックスが表示されます。

ステップ 4　[Application Protocol] を選択します。

デフォルトの [Any] は、HTTP、SMTP、IMAP、POP3、FTP、および NetBIOS-ssn（SMB）トラフィック内のファイルを検出します。

ステップ 5　[Direction of Transfer] を選択します。

ダウンロードされるファイルに関して、以下のタイプの着信トラフィックを検査できます。

- HTTP
- IMAP
- POP3
- FTP
- NetBIOS-ssn（SMB）

アップロードされるファイルに関して、以下のタイプの発信トラフィックを検査できます。

- HTTP
- FTP
- SMTP
- NetBIOS-ssn（SMB）

[Any] を使用すると、ユーザが送信しているか受信しているかには関係なく、多数のアプリケーション プロトコルを介したファイルが検出されます。

ステップ 6　ファイル ルールの [Action] を選択します。詳細については、ファイル ルール アクションの表を参照してください。

[Block Files] または [Block Malware] を選択すると、接続のリセットを示す [Reset Connection] がデフォルトで有効になります。ファイル転送のブロックが発生した接続をリセット**しない**ようにするには、このオプションをクリアします。

注　Ciscoでは、[Reset Connection] を有効のままにしておくことを推奨しています。これにより、ブロックされたアプリケーション セッションが TCP 接続リセットまで開いたままになることを防止できます。

ファイル ルールのアクションの詳細については、ファイル ルール アクションと評価順序（37-13 ページ）を参照してください。

DC500 ではMalware ライセンスを使用できないため、マルウェア ブロック アクションやマルウェア クラウド ルックアップ アクションを使用するファイル ルールを作成したり、それらのアクションを行うルールを含むファイル ポリシーを適用するためにこのアプライアンスを使用したりできないことに注意してください。同様に、シリーズ 2 デバイスまたは Cisco NGIPS for Blue Coat X-Series では Malware ライセンスを有効にできないため、これらのアクションを行うルールを含むファイル ポリシーをこのアプライアンスに適用することはできません。

ステップ 7　[File Types] を 1 つ以上選択します。複数のファイル タイプを選択するには、Shift キーと Ctrl キーを使用します。ファイル タイプのリストを、次のようにフィルタ処理できます。

- [File Type Categories] を 1 つ以上選択します。
- 名前または説明でファイル タイプを検索します。たとえば、Microsoft Windows 固有のファイルのリストを表示するには、[Search name and description] フィールドに `Windows` と入力します。

ヒント　ファイル タイプの上にポインタを移動すると、説明が表示されます。

注意　ファイル タイプまたはファイル カテゴリーを追加すると、Snort プロセスが再開され、構成変更を適用する際、一時的にトラフィック検査が中断されます。この検査中にシステムがトラフィックをドロップするか、検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、「Snort の再開によるトラフィックへの影響（1-9 ページ）」を参照してください。

ファイル ルールで使用できるファイル タイプは、[Application Protocol]、[Direction of Transfer]、および [Action] での選択内容に応じて変化します。

たとえば、[Direction of Transfer] で [Download] を選択すると、ファイル イベントが過剰になることを防止するために、[Graphics] カテゴリから [GIF]、[PNG]、[JPEG]、[TIFF]、および [ICO] が削除されます。

ステップ 8　選択したファイル タイプを [Selected Files Categories and Types] リストに追加します。

- [Add] をクリックすると、選択したファイル タイプがルールに追加されます。
- 1 つ以上のファイル タイプを [Selected Files Categories and Types] リストの中にドラッグ アンド ドロップします。
- カテゴリを選択して [All types in selected Categories] をクリックしてから、[Add] をクリックするか、選択項目を [Selected Files Categories and Types] リストの中にドラッグ アンド ドロップします。

ステップ 9　[Save] をクリックします。

ファイル ルールがポリシーに追加されます。既存のファイル ポリシーを編集している場合、変更内容を有効にするには、そのファイル ポリシーを使用するすべてのアクセス コントロール ポリシーを再適用する必要があります。

ファイル ポリシーの詳細オプション（General）の設定

ライセンス： Malware

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

ファイル ポリシーでは、[General] セクションにある以下の詳細オプションを設定できます。アーカイブ ファイル インスペクションの詳細オプションについては、アーカイブ ファイルのインスペクション オプションの設定（37-22 ページ）を参照してください。

表 37-7　ファイル ポリシーの詳細オプション（General）

フィールド	説明	デフォルト値
Enable Custom Detection List	これを選択すると、カスタム検出リストにあるファイルが検出されたときに、そのファイルをブロックします。	enabled
Enable Clean List	これを選択すると、クリーン リストにあるファイルが検出されたときに、そのファイルを許可します。	enabled

表 37-7　ファイル ポリシーの詳細オプション（General）（続き）

フィールド	説明	デフォルト値
Mark files as malware based on dynamic analysis threat score	しきい値を選択すると、そのスコア以上の脅威スコアを持つファイルが自動的にマルウェアと同じ方法で扱われます。これを無効にするには、[Disabled] を選択します。 しきい値に低い値を選択すると、マルウェアとして扱われるファイル数が増えることに注意してください。ファイル ポリシーで選択したアクションによっては、この結果として、ブロックされるファイル数が増える可能性があります。	Very High（76 以上）

DC500 ではMalware ライセンスを使用できないため、これらの設定を使用/変更できないことに注意してください。同様に、シリーズ 2 デバイスまたは Cisco NGIPS for Blue Coat X-Series で Malware ライセンスを有効にすることはできないため、これらの設定を有効にしたファイル ポリシーを適用することはできません。

ファイル ポリシーの詳細オプション（General）を設定するには、次の手順を実行します。

アクセス： Admin/Access Admin

ステップ 1　[Policies] > [Files] を選択します。

[File Policies] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

[File Policy Rule] ページが表示されます。

ステップ 3　[Advanced] タブを選択します。

[Advanced] タブが表示されます。

ステップ 4　[General] セクションで、ファイル ポリシーの詳細オプション（General）の表に示すように、オプションを変更します。

ステップ 5　[Save] をクリックします。

編集したファイル ポリシーを使用するすべてのアクセス コントロール ポリシーを再適用する必要があります。

アーカイブ ファイルのインスペクション オプションの設定

ライセンス： Malware

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

サポートされる防御センター： DC500 を除くいずれか

アーカイブ ファイル（`.zip` または `.rar` など）は多くの場合、モニタ対象トラフィックで現れます。正当な情報を圧縮して転送するための便利な方法にすぎないものもあれば、マルウェアや他の望ましくないファイルを隠そうとするものもあります。組織のニーズに合わせてアーカイブ ファイルを分析し、必要に応じてブロックできるように、アーカイブ ファイルの内容を検査するようにファイル ポリシーを設定できます。圧縮解除されたファイルに適用できるすべての機能（ダイナミック分析やファイル ストレージなど）は、アーカイブ ファイル内のネストされたファ

イルに使用可能です。コンテキスト メニューを使用して、イベント ビューアまたはファイル トラジェクトリ ビューアからアーカイブ ファイルの内容を表示できます。アーカイブ ファイルの内容の表示（37-24 ページ）を参照してください。

注　アーカイブ ファイルを含むトラフィックがセキュリティ インテリジェンスによってブラックリスト登録またはホワイトリスト登録された場合、またはトップレベルのアーカイブ ファイルの SHA-256 値がカスタム検出リストにある場合、システムはアーカイブ ファイルの内容を検査しません。ネストされたファイルがブラックリスト登録された場合、アーカイブ全体がブロックされます。しかし、ネストされたファイルがホワイトリスト登録された場合、アーカイブは自動的に渡されません（他のネストされたファイルおよび特性による）。詳細については、グローバル ホワイトリストおよびブラックリストの操作（3-7 ページ）を参照してください。

一部のアーカイブ ファイルには、追加のアーカイブ ファイル（など）が含まれています。ファイルがネストされるレベルは、その *アーカイブ ファイルの深さ* です。トップレベルのアーカイブ ファイルは深さの数で考慮されないことに注意してください。深さは最初にネストされたファイルで 1 から始まります。システムでは、ネストされたアーカイブ ファイルを最大 3 レベルまでしか検査できませんが、その深さ（または指定したそれより低い最大深さ）を超えるアーカイブ ファイルをブロックするようファイル ポリシーを設定できます。ネストされたアーカイブをさらに制限する場合は、2 または 1 のより低い最大ファイル深さを設定するオプションがあります。最大アーカイブ ファイルの深さ 3 を超えるファイルをブロックしないよう選択した場合、抽出可能な内容と深さ 3 以上でネストされた内容を含むアーカイブ ファイルがモニタ対象のトラフィックに現れると、システムは検査可能だったファイルについてのみデータを検査して報告します。

アーカイブ ファイルは、それに含まれているファイルの性質に基づいてファイルの性質を取得します。識別されたマルウェア ファイルを含んでいる**すべて**のアーカイブは、**マルウェア**の性質になります。識別されたマルウェア ファイルを含んでいないアーカイブの場合、いずれかの不明なファイルが含まれていれば `Unknown` の性質、クリーン ファイルのみが含まれていれば `Clean` の性質になります。ファイル性質の詳細については、ファイルの性質について（37-4 ページ）を参照してください。

次の表に、ファイル ポリシーで設定できるアーカイブ ファイルのインスペクション オプションを示します。

表 37-8　アーカイブ ファイルのインスペクション オプション

フィールド	説明	デフォルト値
Inspect Archives	アーカイブ ファイルの内容を検査する場合に選択します。このオプションがオフの場合、下のオプションはグレー表示となり使用できません。 **注意**　ファイルのアーカイブを有効または無効にすると、Snort プロセスが再開され、構成変更を適用する際、一時的にトラフィック検査が中断されます。この検査中にシステムがトラフィックをドロップするか、検査を行わずに受け渡すかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、「Snort の再開によるトラフィックへの影響（1-9 ページ）」を参照してください。	ディセーブル
Block Encrypted Archives	暗号化された内容があるアーカイブ ファイルをブロックする場合に選択します。	ディセーブル

表 37-8　アーカイブ ファイルのインスペクション オプション（続き）

フィールド	説明	デフォルト値
Block Uninspectable Archives	システムが暗号化以外の理由で検査できない内容を含むアーカイブ ファイルをブロックする場合に選択します（これは通常、何らかの理由で破損したファイル、または指定した最大アーカイブの深さを超えるファイルに適用されます）。	イネーブル
Max Archive Depth	ネストされたアーカイブ ファイルの最大深さを指定します。この深さを超えるアーカイブ ファイルはブロックされます。値は 1、2、または 3 にしてください。トップレベルのアーカイブ ファイルは数で考慮されません。深さは最初にネストされたファイルで 1 から始まります。	2

アーカイブ ファイルのインスペクション オプションを設定するには、次の手順を実行します。

アクセス： Admin/Access Admin

ステップ 1　[Policies] > [Files] を選択します。

[File Policies] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

[File Policy Rule] ページが表示されます。

ステップ 3　[Advanced] タブを選択します。

[Advanced] タブが表示されます。

ステップ 4　[Archive File Inspection] セクションで、アーカイブ ファイルのインスペクション オプション に示すように、オプションを変更します。

ステップ 5　[Save] をクリックします。

編集したファイル ポリシーを使用するすべてのアクセス コントロール ポリシーを再適用する必要があります。

アーカイブ ファイルの内容の表示

ライセンス： Malware

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

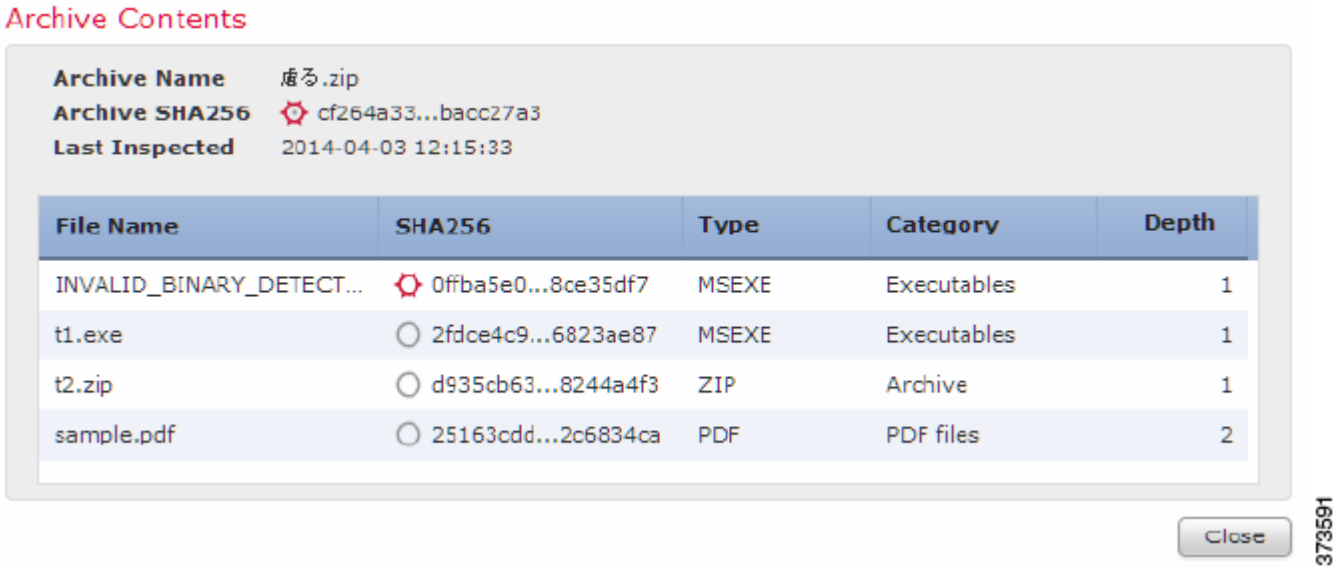
サポートされる防御センター： DC500 を除くいずれか

アーカイブ ファイルの内容を検査するようにファイル ポリシーが設定されている場合は、イベント ビューアのコンテキスト メニューおよびネットワーク ファイル トラジェクトリ ビューアを使用して、アーカイブ ファイルがファイル イベント、マルウェア イベントに現れた場合、またはキャプチャされたファイルとして現れた場合に、アーカイブ内のファイルに関する情報を表示できます。

詳細については、以下を参照してください。

- コンテキスト メニューの使用（2-5 ページ）
- ファイル イベントの表示（40-9 ページ）
- マルウェア イベントの表示（40-20 ページ）
- キャプチャ ファイルの表示（40-32 ページ）
- ネットワーク ファイル トラジェクトリの確認（40-38 ページ）

[Archive Contents] ウィンドウは 2 つの方法で表示できます。対象のアーカイブ ファイルを右クリックして、コンテキスト メニューから [View Archive Contents] を選択することでイベント ビューアから表示するか、または [Archive Contents] の下の表示アイコン（🔍）をクリックして、アーカイブ ファイルのファイル トラジェクトリ ビューから表示します。いずれの場合も、表示されるウィンドウは同じです。次の図は、[Archive Contents] ウィンドウの例を示しています。



アーカイブのすべてのファイル コンテンツは表形式でリストされます。そのリストには、名前、SHA-256 ハッシュ値、タイプ、カテゴリ、およびアーカイブの深さといった関連情報の概略が含まれています。ネットワーク ファイル トラジェクトリ アイコンは各ファイルごとに表示されます。そのアイコンをクリックすることで、ネットワーク トラジェクトリ機能を使用した特定のファイルに関する詳細な情報を表示することができます。

イベント ビューアからアーカイブされたファイルの内容を表示するには、次の手順を実行します。

アクセス： Admin/Access Admin

ステップ 1　選択したイベント ビューアに移動します。次の 3 つのオプションがあります。

- マルウェア イベントの場合は、[Analysis] > [Files] > [Malware Events] を選択します。
- ファイル イベントの場合は、[Analysis] > [Files] > [File Events] を選択します。
- キャプチャされたファイルの場合は、[Analysis] > [Files] > [Captured Files] を選択します。

デフォルトのイベント ワークフローの最初のページが表示されます。

ステップ 2　検査するアーカイブ ファイルが表示されるテーブルの行を右クリックします。

コンテキスト メニューが表示されます。

ステップ 3　コンテキスト メニューから、[View Archive Contents] をクリックします。

[Archive Contents] ウィンドウが表示されます。

ファイル トラジェクトリからアーカイブされたファイルの内容を表示するには、次の手順を実行します。

アクセス：Admin/Access Admin

ステップ 1　[Analysis] > [Files] > [Network File Trajectory] を選択します。

[Network File Trajectory List] ページが表示されます。

ステップ 2　検査するアーカイブ ファイルのファイル トラジェクトリ アイコン（）をクリックします。

そのファイルのファイル トラジェクトリ ページが表示されます。

ステップ 3　[Archive Contents] の下で、ビュー アイコン（）をクリックします。

[Archive Contents] ウィンドウが表示されます。

2 つのファイル ポリシーの比較

ライセンス：Protection

変更後のポリシーが組織の標準に準拠することを確かめたり、システム パフォーマンスを最適化したりする目的で、任意の 2 つのファイル ポリシー間の違いや、同じポリシーの 2 つのリビジョン間の違いを調べることができます。

ファイル ポリシーの*比較ビュー*には、2 つのポリシーまたはリビジョンが並んで表示され、各ポリシー名の横には最終変更時刻と最後に変更したユーザが表示されます。2 つのポリシーの間の差異は、次のように強調表示されます。

- 2 つのポリシーの間で異なっている設定は、青色で強調表示され、その差異が赤いテキストで示されます。
- グリーンは、強調表示されている設定項目が一方のポリシーに含まれ、もう一方のポリシーには含まれないことを示します。

[Previous] と [Next] をクリックすると、前後の相違箇所に移動できます。左側と右側の間にある二重矢印アイコン（）が移動し、表示している違いを示す [Difference] 番号が変わります。オプションで、ファイル ポリシーの*比較レポート*を生成できます。これは PDF 版の比較ビューです。

2 つのファイル ポリシーを比較する方法：

アクセス：Admin/Access Admin

ステップ 1　[Policies] > [Files] を選択します。

[File Policies] ページが表示されます。

ステップ 2　[Compare Policies] をクリックします。

[Select Comparison] ダイアログ ボックスが表示されます。

ステップ 3　[Compare Against] ドロップダウンリストから、比較するタイプを次のように選択します。

- 2 つの異なるポリシーを比較するには、[Running Configuration] または [Other Policy] を選択します。この 2 つのオプションの違いは、[Running Configuration] を選択した場合、現在適用されている一連のファイル ポリシーの中からのみ、比較対象の 1 つを選択できます。
- 同じポリシーのバージョン間を比較するには、[Other Revision] を選択します。

ダイアログ ボックスの表示が更新され、比較オプションが示されます。

ステップ 4　選択した比較タイプに応じて、次の選択肢があります。

- 2 つの異なるポリシーを比較する場合、比較対象のポリシーとして [Policy A] または [Target/Running Configuration A] のどちらかと、[Policy B] とを選択します。
- 同じポリシーのバージョン間を比較する場合、対象の [Policy] を選択してから、2 つのリビジョン [Revision A] と [Revision B] を選択します。リビジョンは、日付とユーザ名別にリストされます。

ステップ 5　[OK] をクリックします。

比較ビューが表示されます。

ステップ 6　必要に応じて、アクセス コントロール ポリシー比較レポートを生成するには [Comparison Report] をクリックします。

比較レポートが表示されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。

FireAMP 用のクラウド接続の操作

ライセンス： すべて

FireAMP は、Cisco が提供するエンタープライズ向けの高度なマルウェア分析/対策ソリューションです。お客様の組織で FireAMP サブスクリプションをご利用の場合、個々のユーザは自分のコンピュータやモバイル デバイスに FireAMP コネクタをインストールします。これらの軽量エージェントはCisco クラウドと通信し、さらにクラウドがDefense Centerと通信します。クラウドに接続するようDefense Centerを設定した後、スキャン、マルウェア検出、および検疫のレコードを受信できるようになります。レコードは、マルウェア イベントとしてDefense Center データベースに保存されます。詳細については、マルウェア対策とファイル制御について（37-2 ページ）を参照してください。

組織のセキュリティ ポリシーで従来型クラウド サーバ接続の使用が許可されていない場合、Ciscoのプライベート オンプレミス クラウド ソリューションである、FireAMP Private Cloud を入手して設定できます。これは、圧縮された、パブリック Cisco クラウドのローカル バージョンとして機能する仮想マシンです。この場合、データとアクション（FireAMP コネクタからのイベント、ファイルの性質 ルックアップ、レトロスペクティブ イベントなど）は、通常の方法でクラウド接続を経由する代わりに、組織のプライベート クラウドへのローカル接続によって処理されます。（ファイルの性質 ルックアップなどのために）外部クラウドへの接続が必要になったとき、プライベート クラウドは、Defense Center とパブリック Cisco クラウドとの間の匿名化されたプロキシとして機能します。プライベート クラウドでは、エンドポイント イベント データは外部接続で共有されません。プライベート クラウドの構成方法の詳細については、FireAMP プライベート クラウドの操作（37-30 ページ）を参照してください。

注　プライベート クラウドは、動的分析をサポートしていません。

また、FireAMP コネクタがインストールされたホストでは、侵害の兆候（IOC）タグを生成できます。これは、エンドポイント ベースのマルウェア検出アクティビティにより、あるホストでセキュリティ侵害が発生した可能性が示唆されたとき、そのホストに関して生成されます。Defense Center からホストのエンドポイント IOC 情報を表示するには、そのホストは Defense Center のネットワーク マップに表示される必要があります。Ciscoエンドポイント ベースのマルウェア イベントに関する新しい IOC タイプが開発される場合があります。お客様のシステムは、Cisco

クラウドからこれを自動的にダウンロードします。侵害の兆候の詳細については、侵害の兆候について（45-22 ページ） および エンドポイント ベースのマルウェア イベント IOC タイプ（45-22 ページ）を参照してください。

展開内のそれぞれのDefense Centerは、Cisco クラウドに接続できます。デフォルトで、クラウドは組織内のすべてのグループに関するマルウェア イベントを送信しますが、接続を設定するときにグループごとに制限できます。

インターネット アクセスとハイ アベイラビリティ

エンドポイント ベースのマルウェア イベントを受信するために、システムはポート 443/HTTPS を使用して Cisco クラウド（パブリックまたはプライベート）に接続します。Defense Centerで、このポートをインバウンドとアウトバウンドの両方に開く必要があります。また、Defense Centerはインターネットに直接アクセスできる必要があります。デフォルトのヘルス ポリシーに含まれる FireAMP ステータス モニタは、Defense Center からクラウドへの最初の接続が成功した後で接続できなくなった場合、または FireAMP ポータルを使って接続が登録解除された場合に警告を出します。

エンドポイント ベースのマルウェア イベントを受信するクラウド接続は、ハイ アベイラビリティ ペアのメンバ間では**共有されません**。継続的な運用を維持するには、プライマリとセカンダリの両方のDefense Centerをクラウドに接続してください。

クラウド接続の管理

Defense Center の [AMP Management] ページ（[AMP] > [AMP Management]）を使用すると、Cisco クラウドまたはプライベート クラウドへの接続の表示と作成、およびそれらの接続の無効化と削除を行うことができます。

回転する状態アイコンは、接続が保留中であることを示します。たとえば、Defense Centerで接続の設定がすでに完了した後、FireAMP ポータルを使って接続を承認しなければならない場合です。失敗または拒否を示すアイコン（）は、クラウドが接続を拒否したこと、または他の理由で接続が失敗したことを示します。

ヒント　いずれかのクラウド名をクリックすると、FireAMP ポータルが新しいブラウザ ウィンドウで開きます。

詳細については、以下を参照してください。

- Cisco クラウド接続の作成（37-28 ページ）
- クラウド接続の削除または無効化（37-29 ページ）
- FireAMP プライベート クラウドの操作（37-30 ページ）

Cisco クラウド接続の作成

ライセンス： すべて

Defense CenterとCisco クラウドの間の接続の作成は、2 段階からなるプロセスです。まず、クラウドに接続するようDefense Centerを設定します。次に、FireAMP ポータルにログインして接続を承認します。FireAMP サブスクリプションがない場合は、登録プロセスを完了できません。

出荷時の初期状態に復元されたDefense Center、またはクラウドへの登録中に取り消された防御センターを再登録するには、再び登録する前に FireAMP に接続し、Defense Centerを削除する必要があります。

FireAMP 用のCisco クラウド接続を作成する方法:

アクセス: Admin

ステップ 1　[AMP] > [AMP Management] を選択します。

[AMP Management] ページが表示されます。

ステップ 2　[Create FireAMP Connection] をクリックします。

[Create FireAMP Connection] ダイアログ ボックスが表示されます。

ステップ 3　[Cloud Name] ドロップダウン ボックスから、使用するクラウドを選択します。

- 欧州連合クラウドの場合、[EU Cloud] を選択します。
- 米国クラウドの場合、[US Cloud] を選択します。
- プライベート クラウドの場合、[Private Cloud] を選択し、FireAMP プライベート クラウドの操作（37-30 ページ）に示されている追加の手順に従います。

ステップ 4　[Register] をクリックします。

ステップ 5　FireAMP ポータルに移動してもよいことを確認し、ポータルにログインします。

ポータルの [Applications] ページが表示されます。このページを使用して、Cisco クラウドがマルウェア イベントをDefense Centerに送信することを承認します。

ステップ 6　オプションで、マルウェア イベントの受信対象となる組織内の特定のグループを選択できます。

受信するイベントを制限する必要がある場合にのみ、グループを選択してください。デフォルトで、Defense Centerはすべてのグループに関するマルウェア イベントを受信します。

ヒント　グループを管理するには、FireAMP ポータルで [Management] > [Groups] を選択します。詳細については、ポータルのオンライン ヘルプを参照してください。

ステップ 7　[Allow] をクリックします。

Defense Center の [FireAMP Management] ページに戻ります。接続が有効になり、Defense Centerはクラウドからマルウェア イベントを受信し始めます。

なお、[Deny] をクリックした場合にもDefense Centerに戻りますが、クラウド接続には拒否マークが付きます。同様に、接続を拒否/許可しないまま FireAMP ポータルの [Applications] ページから別のページに移動した場合、Defense Center の Web インターフェイスでは接続に保留中のマークが付きます。どちらの場合も、ヘルス モニタはアラートを出しません。あとでクラウドに接続するには、失敗した接続または保留中の接続を削除してから再作成する必要があります。

クラウド接続の削除または無効化

ライセンス: すべて

クラウドからマルウェア イベントを受信する必要がなくなった場合は、Cisco クラウド接続またはプライベート クラウド接続を削除します。一時的に特定の接続でのマルウェア イベント受信を停止するには、接続を削除するのではなく、接続を無効にすることができます。その場合、接続が再び有効にされるまでクラウドはイベントを保存し、有効になった後、保存済みイベントがクラウドから送信されます。

注意　まれに、イベント レートが非常に高い場合や接続が長期間無効になっていた場合など、接続無効中に生成されたすべてのイベントをクラウドで保存できないことがあります。

なお（Defense Center の Web インターフェイスではなく）FireAMP ポータルを使用して接続の登録を解除すると、イベント送信が停止しますが、Defense Center からは接続が削除されないことに注意してください。登録解除された接続は [FireAMP Management] ページで失敗状態として表示され、それを削除する必要があります。

Defense Centerを使用してクラウド接続を有効または無効にする方法:

アクセス: Admin

ステップ 1　[AMP Management] ページで、削除する接続の横のスライダをクリックしてから、接続を有効または無効にすることを確認します。

接続を有効にすると、クラウドはDefense Centerにイベントを送信し始めます。このとき、接続が無効だった間に発生したイベントも送信されます。クラウドは、無効化された接続のイベントを送信しません。

Defense Centerを使用してクラウド接続を削除する方法:

アクセス: Admin

ステップ 1　[AMP Managemenet] ページで、削除する接続の横の削除アイコン（ ）をクリックしてから、接続の削除を確認します。

接続が削除され、クラウドはDefense Centerへのイベントの送信を停止します。

FireAMP プライベート クラウドの操作

ライセンス: すべて

お客様の組織のプライバシーやセキュリティ上の理由で、モニタ対象ネットワークと外部クラウド サーバとの間で頻繁に接続することが困難、または不可能な場合があります。この場合、FireAMP プライベート クラウドを入手して設定することができます。これは Cisco 独自の仮想マシンであり、お客様のネットワークと Cisco FireAMP クラウドの間のセキュア メディエータとして機能します。多くのアプライアンスからの識別可能な接続の代わりに、パブリックの外部 Cisco クラウドへのすべての必要な接続が一括してプライベート クラウド経由で流れます。プライベート クラウドは匿名化されたプロキシとして動作することで、モニタ対象ネットワークのセキュリティとプライバシーを確保します。各プライベート クラウドは、最大で 10,000 個のコネクタをサポートできます。組織の必要に応じて、ネットワーク上に複数のプライベート クラウドを設定できます。

FireAMP プライベート クラウドは、クラウド ベースのファイルの性質 ルックアップ処理、エンドポイント ベースの FireAMP イベント取得、およびレトロスペクティブ マルウェア イベント生成を処理します。パブリック クラウドの代わりに機能するプライベート クラウドは、FireAMP コネクタのエンドポイントからマルウェア イベントを収集して、それらをDefense Centerに送り

ます。匿名化されたプロキシ プライベート クラウド接続を介して、(ファイルの性質や SHA256 値などを判別するための)パブリック Cisco クラウドへの照会だけが、ネットワークから発信されます。エンドポイント イベント データは、ネットワークから発信されません。

クラウド ベースのファイル機能およびマルウェア機能の詳細については、以下を参照してください。

- マルウェア対策とファイル制御について(37-2 ページ)
- FireAMP と FireSIGHT システムの統合(37-8 ページ)
- 動的分析の操作(40-5 ページ)
- エンドポイントベース(FireAMP)のマルウェア イベント(40-18 ページ)
- 遡及的マルウェア イベント(40-19 ページ)

本資料、およびプライベート クラウドでサポートされる機能に関する他の資料で「クラウド」または「Cisco クラウド」に言及する場合、特に明記されない限り、プライベート クラウドを介した接続も当てはまります。プライベート クラウドは標準のクラウド接続と同じオープン ポートを必要とし、同じハイ アベイラビリティ制限事項があります。

注　FireAMP プライベート クラウドは、マルウェア関連およびファイル関連のクラウド ベース機能のみをサポートします。クラウド接続を使用するその他の FireSIGHT システム機能(URL フィルタリングやセキュリティ インテリジェンスなど)はサポートされません。また、プライベート クラウドは動的分析機能をサポートしませんが、プライベート クラウドを使用して、Cisco がすでに動的に分析したファイルの脅威スコアを取得できます。

Defense Centerと FireAMP プライベート クラウドの間の接続を作成するには、まず FireAMP プライベート クラウドを設定する必要があります(サポート サイトで入手可能な『*FireAMP Private Cloud Administration Portal User Guide*』の手順に従います)。この設定中に、[FireAMP Console] フィールドに表示されるプライベート クラウド ホスト名を必ずメモしておいてください。プライベート クラウドを Defense Center に接続するために、このホスト名が必要になります。プライベート クラウドが正常に設定されると、設定済みのパブリック クラウド接続がある場合はそれがすべて自動的に無効化されることに注意してください。

Defense Centerと FireAMP プライベート クラウドの間の接続を作成する方法:

アクセス: Admin

ステップ 1　[AMP] > [AMP Management] を選択します。

[AMP Management] ページが表示されます。

ステップ 2　[Create FireAMP Connection] をクリックします。

[Create FireAMP Connection] ダイアログ ボックスが表示されます。

ステップ 3　[Cloud Name] ドロップダウンリストから [Private Cloud] を選択します。

追加のフィールドがダイアログ ボックスに表示されます。

ステップ 4　[Name] フィールドに、プライベート クラウド接続の名前を入力します。この名前は、マルウェア イベントを表示したときに FireAMP クラウド イベント フィールドに表示されます。

ステップ 5　[Host] フィールドに、プライベート クラウドのホスト名を入力します。これは、FireAMP プライベート クラウド仮想マシンを設定したときに [FireAMP Console] フィールドに表示されたものです。

ステップ 6　[Certificate Upload Path] フィールドで、プライベート クラウドの有効な TLS または SSL 暗号化証明書情報の場所を参照します。詳細については、『*FireAMP Private Cloud Administration Portal User Guide*』を参照してください。

ステップ 7　モニタ対象ネットワーク用に複数のプライベート クラウドが設定されている場合、どのプライベート クラウドでネットワークベースのマルウェア ルックアップを処理するかを決定するには、[Use For NetworkAMP] チェック ボックスをオンまたはオフにします。1 つのプライベート クラウドだけが設定されている場合、デフォルトでチェック ボックスがオンになり、オフにすることはできません。

ステップ 8　Defense Center で設定されたプロキシ接続があり、そのプロキシ接続をプライベート クラウドに使用する場合は、[Use Proxy for Connection] チェック ボックスを選択します。このオプションが選択されていない場合、プライベート クラウドはその通信に設定されたプロキシを使用**しません**。

ステップ 9　[Register] をクリックします。

ダイアログ ボックスが表示され、プライベート クラウド設定を作成すると設定済みのすべてのパブリック クラウド接続が無効になることが通知されます。

ステップ 10　[Yes] をクリックします。

FireAMP ポータルに移動してもよいことを確認し、ポータルにログインします。

ステップ 11　プライベート クラウド情報がシステムによって処理され、設定を完了するために FireAMP サイトにリダイレクトされます。詳細な手順については、『*FireAMP Private Cloud Administration Portal User Guide*』を参照してください。

ネットワーク トラフィックの接続のロギング

管理対象デバイスがネットワーク上でホストによって生成されたトラフィックをモニタするとき、デバイスは検出した接続のログを生成できます。アクセス コントロールおよび SSL ポリシーでさまざまな設定を行うことで、ログする接続の種類、接続をログする時期、およびデータを保存する場所のきめ細かい制御を行うことができます。また、アクセス コントロール ルールの特定のロギング設定では、接続に関連するファイル イベントとマルウェア イベントをログに記録するかどうかも決定します。

ほとんどの場合、接続の開始または終了、またはその両方で接続をロギングできます。接続をログに記録すると、システムによって*接続イベント*が生成されます。接続がレピュテーション ベースのセキュリティ インテリジェンス機能によってブラックリスト登録（ブロック）される場合は、*セキュリティ インテリジェンス イベント*と呼ばれる特別な種類の接続イベントをログに記録することもできます。

接続イベントには、検出されたセッションに関するデータも含まれています。個々の接続イベントで入手可能な情報はいくつかの要因によって決まりますが、一般的には次のものがあります。

- タイムスタンプ、送信元と宛先の IP アドレス、入出力ゾーン、接続を処理したデバイスなど、基本的な接続特性
- アプリケーション、要求される URL、または接続に関連付けられているユーザなど、システムによって検出または推測される追加の接続特性
- ポリシーがトラフィックを処理したアクセス コントロール ルール（または他の設定）、接続が許可またはブロックされているかどうか、暗号化された接続および復号化された接続に関する詳細など、接続がログに記録された理由に関するメタデータ

組織のセキュリティ上およびコンプライアンス上の要件に従って接続をロギングしてください。アクセス コントロールに到達する前にデバイス レベルで高速パス処理される接続を除く**すべての**接続をログに記録できます。

接続イベントを Defense Center データベースに保存すると、FireSIGHT システム のレポート、分析、およびデータ相関関係の多くの機能を活用できます。接続およびセキュリティ インテリジェンス のデータの使用（39-1 ページ）を参照してください。または、外部システム ログ（syslog）または SNMP トラップ サーバに接続データを送信できます。

管理対象デバイスで収集された接続データを補うために、NetFlow 対応デバイスによって生成されたレコードを使用して接続イベントを生成できます。FireSIGHT システム の管理対象デバイスによって監視できない NetFlow 対応デバイスがネットワークに配置されている場合は特に有効です。

注　NetFlow のデータ収集はアクセス コントロールにリンクされていないため、ロギングする NetFlow 接続については、きめ細かい制御ができません。FireSIGHT システム の管理対象デバイスは NetFlow 対応デバイスによってエクスポートされるレコードを検出し、それらのレコードのデータに基づいて単一方向の接続終了イベントを生成し、最終的にそのイベントをデータベースに記録するために Defense Center へ送信します。NetFlow レコードはセキュリティ インテリジェンス イベントを生成できず、外部サーバにも記録できません。詳細については、NetFlow について（45-18 ページ）を参照してください。

接続データのロギングの詳細については、以下を参照してください。

- どの接続をログに記録するかの決定（38-2 ページ）
- セキュリティ インテリジェンス（ブラックリスト登録）の決定のロギング（38-12 ページ）
- 暗号化された接続のロギング（38-14 ページ）
- アクセス コントロールの処理に基づく接続のロギング（38-17 ページ）
- 接続で検出された URL のロギング（38-21 ページ）

どの接続をログに記録するかの決定

ライセンス： すべて

アクセス コントロール ポリシーと SSL ポリシーのさまざまな設定を使用して、デバイスがモニタする非高速パス接続をログに記録できます。ほとんどの場合、接続の開始または終了、またはその両方で接続をロギングできます。しかし、ブロックされたトラフィックは追加のインスペクションなしですぐに拒否されるため、多くの場合、ユーザがログに記録できるのはブロックまたはブラックリスト登録されたトラフィックの接続開始イベントのみです。ログに記録できる固有の接続終了イベントはありません。

接続イベントをログに記録するときに、Defense Center データベースにそれを保存し、FireSIGHT システム を使用してさらなる分析を行うことができます。または、外部 syslog または SNMP トラップ サーバに接続データを送信できます。

ヒント　FireSIGHT システム を使用して接続データの詳細な分析を実行するためには、Cisco はクリティカルな接続の終了を Defense Center データベースに記録することを推奨します。

詳細については、以下を参照してください。

- クリティカルな接続のロギング（38-3 ページ）
- 接続の開始または終了のロギング（38-4 ページ）
- Defense Center または外部サーバへの接続のロギング（38-5 ページ）
- アクセス コントロールおよび SSL ルール アクションがどのようにロギングに影響を及ぼすかについて（38-6 ページ）
- 接続ロギングのライセンスおよびモデル要件（38-10 ページ）

クリティカルな接続のロギング

ライセンス：すべて

組織のセキュリティ上およびコンプライアンス上の要件に従って接続をロギングしてください。目標が生成するイベントの数を抑えパフォーマンスを向上させることである場合は、分析のために重要な接続のロギングのみを有効にします。しかし、プロファイリングの目的でネットワーク トラフィックの広範な表示が必要な場合は、追加の接続のロギングを有効にできます。アクセス コントロールおよび SSL ポリシーでさまざまな設定を行うことで、ログする接続の種類、接続をログする時期、およびデータを保存する場所のきめ細かい制御を行うことができます。

注意　サービス妨害（DoS）攻撃の間にブロックされた TCP 接続をロギングすると、システム パフォーマンスに影響し、複数の同様のイベントによってデータベースが過負荷になる可能性があります。ブロック ルールのロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたは DoS 攻撃を受けやすい他のインターフェイス上のトラフィックをモニタするかどうかを検討します。

設定するロギングに加えて、システムは禁止されたファイル、マルウェア、または侵入の試みを検出した場合に、ほとんどの接続を自動的にログに記録します。他のロギング設定に関係なく、システム ポリシーを使用して接続イベント ストレージを完全に無効にしない限り、システムはこれらの接続終了イベントを Defense Center データベースに保存し、さらなる分析に使用します。すべての接続イベントは、自動的にログ記録された理由を [Action] および [Reason] フィールドを使用して反映します。処理（39-5 ページ）および Reason（39-8 ページ）を参照してください。

セキュリティ インテリジェンス ブラックリスト登録の決定（オプション）

接続がレピュテーション ベースのセキュリティ インテリジェンス機能によってブラックリスト登録（ブロック）される場合は、その接続をログに記録できます。オプションで、セキュリティ インテリジェンス フィルタリングには「モニタ専用」設定を使用できます。パッシブ展開環境では、この設定が推奨されます。この設定では、ブラックリスト登録されるはずの接続をシステムがさらに分析できるだけでなく、ブラックリストと一致する接続をログに記録することもできます。セキュリティ インテリジェンス モニタリングによって、セキュリティ インテリジェンス情報を使用してトラフィック プロファイルを作成することもできます。

セキュリティ インテリジェンス ロギングを有効にすると、ブラックリストの一致によってセキュリティ インテリジェンス イベントおよび接続イベントが生成されます。セキュリティ インテリジェンス イベントは特殊なタイプの接続イベントで、個別に表示および分析できるだけでなく、個別に保存およびプルーニングできます。詳細については、セキュリティ インテリジェンス（ブラックリスト登録）の決定のロギング（38-12 ページ）を参照してください。

暗号化された接続（任意）

SSL ポリシーの設定に従ってシステムが暗号化されたセッションをブロックしたときの接続をログに記録できます。また、トラフィックを復号化するかどうかにかかわらず、またシステムがトラフィックを後でどのように処理または検査するかにかかわらず、アクセス コントロール ルールによるさらなる評価のためにシステムが渡す接続をログに記録するように強制することもできます。クリティカルな接続のみをログに記録するように、このロギングは SSL ルールごとに設定します。詳細については、暗号化された接続のロギング（38-14 ページ）を参照してください。

アクセス コントロールの処理（オプション）

接続がアクセス コントロール ルールまたはアクセス コントロールのデフォルト アクションによって処理される場合は、その接続をログに記録できます。クリティカルな接続のみをログに記録できるように、このロギングはアクセス コントロール ルールごとに設定します。詳細については、アクセス コントロールの処理に基づく接続のロギング（38-17 ページ）を参照してください。

侵入に関連付けられる接続（自動）

アクセス コントロール ルールによって呼び出された侵入ポリシー（アクセス コントロール ルールを使用したトラフィック フローの調整（14-1 ページ）を参照）が侵入を検出して侵入イベントを生成すると、システムはルールのロギング設定に関係なく、侵入が発生した接続の終了を Defense Center データベースに自動的にロギングします。

しかし、アクセス コントロールのデフォルト アクションに関連付けられた侵入ポリシー（デフォルトの処理の設定およびネットワーク トラフィックのインスペクション（12-7 ページ）を参照）によって侵入イベントが生成された場合、システムは関連する接続の終了を自動的にログに記録**しません**。代わりに、デフォルトのアクション接続のロギングを明示的に有効にする必要があります。これは、接続データをログに記録する必要がない、侵入防御専用の展開環境に役立ちます。

侵入がブロックされた接続では、接続ログ内の接続のアクションは `Block`、理由は `Intrusion Block` ですが、侵入インスペクションを実行するには、許可ルールを使用する必要があります。

ヒント　シリーズ 3 または仮想デバイスでこの接続ロギングを無効にするには、CLI を使用します。log-ips-connections（D-32 ページ）を参照してください。

ファイル イベントとマルウェア イベントに関連付けられた接続（自動）

アクセス コントロール ルールによって呼び出されたファイル ポリシーが禁止されたファイル（マルウェアを含む）を検出してファイル イベントまたはマルウェア イベントを生成すると、システムはアクセス コントロール ルールのロギング設定に関係なく、ファイルが検出された接続の終了を Defense Center データベースに自動的にロギングします。このロギングを無効にすることは**できません**。

注　NetBIOS-ssn（SMB）トラフィックのインスペクションによって生成されるファイル イベントは、即座には接続イベントを生成しません。これは、クライアントとサーバが持続的接続を確立するためです。システムはクライアントまたはサーバがセッションを終了した後に接続イベントを生成します。

ファイルがブロックされた接続では、接続ログ内の接続のアクションは `Block` ですが、ファイルおよびマルウェアのインスペクションを実行するには、許可ルールを使用する必要があります。接続の原因は、`File Monitor`（ファイル タイプまたはマルウェアが検出された）、あるいは `Malware Block` または `File Block`（ファイルがブロックされた）です。

接続の開始または終了のロギング

ライセンス： すべて

システムが接続を検出すると、ほとんどの場合、その開始または終了をログに記録できます。

しかし、ブロックされたトラフィックは追加のインスペクションなしですぐに拒否されるため、多くの場合、ユーザがログに記録できるのはブロックまたはブラックリスト登録されたトラフィックの接続開始イベントのみです。ログに記録できる固有の接続終了イベントはありません。暗号化されたトラフィックをブロックする場合は例外です。SSL ポリシーで接続のロギングを有効にすると、システムは接続開始イベントではなく接続終了イベントをログに記録します。これは、システムが接続がセッション内で最初のパケットを使用して暗号化されているかどうかを判定できず、暗号化されたセッションを即座にブロックできないためです。

注　単一のブロックされていない接続の場合、接続終了イベントには、接続開始イベントに含まれるすべての情報に加えて、セッション期間中に収集された情報も含まれます。

パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。接続の開始イベントまたは終了イベントのどちらかに基づいて相関ルールをトリガーできます。何らかの理由で接続をモニタすると、接続終了ロギングが強制されることに注意してください。モニタされた接続のロギングについて（38-7 ページ）を参照してください。

次の表では、接続開始イベントと接続終了イベントの違い（それぞれをロギングする利点を含む）を詳細に説明します。

表 38-1　接続開始イベントと接続終了イベントの比較

	接続開始イベント	接続終了イベント
次の場合に生成可能です	システムが接続の開始を検出した場合（または、イベントの生成がアプリケーションまたは URL の識別に依存する場合は最初の数パケットの後）	システムが以下の場合 • 接続のクローズを検出した場合 • 一定期間後に接続の終了を検出しない場合 • メモリ制約によりセッションを追跡できなくなった場合
次のものについてロギングが可能です	セキュリティ インテリジェンスまたはアクセス コントロール ルールによって評価されたすべての接続。しかし、すべての場所で接続終了ロギングを設定できない場合があります。	すべての接続。しかし、すべての場所で接続終了ロギングを設定できない場合があります。
次を含みます	最初のパケット（または、イベントの生成がアプリケーションまたは URL の識別に依存する場合は最初の数パケット）で判定できる情報のみ	接続開始イベント内のすべての情報と、セッション期間を通してトラフィックを検査して判別された情報（たとえば伝送されたデータ総量、接続の最後のパケットのタイムスタンプなど）
次の場合に有用です	次のものをロギングする場合 • セキュリティ インテリジェンス ブラックリスト登録の決定を含む、ブロックされた接続 • 接続終了情報はユーザにとって重要ではないので、接続の開始のみ	次を実行する場合 • SSL ポリシーによって処理される暗号化接続をロギングする場合 • セッションの期間にわたって収集された情報であらゆる種類の詳細な分析を実行する場合、またはその情報を使用して相関ルールをトリガーする場合 • カスタム ワークフローで接続の概要（集約接続データ）を表示する場合、グラフ形式で接続データを表示する場合、またはトラフィック プロファイルを作成して使用する場合

Defense Center または外部サーバへの接続のロギング

ライセンス：すべて

接続イベントのログは、Defense Center データベースの他に、外部の syslog または SNMP トラップ サーバに記録できます。外部サーバに接続データを記録する前に、そのサーバに *アラート応答* という接続を設定する必要があります。アラート応答の使用（43-2 ページ）を参照してください。

Defense Center データベースにロギングすると、FireSIGHT システム のレポート、分析、およびデータ相関関係の多くの機能を活用できます。次に例を示します。

- ダッシュボードおよび Context Explorer では、システムによってロギングされた接続をグラフ形式によって一目で確認できます。ダッシュボードの使用（55-1 ページ）および Context Explorer の使用法（56-1 ページ）を参照してください。
- イベント ビューには、システムによってロギングされた接続の詳細情報が提示され、グラフ形式や表形式で表示したり、レポートに要約することもできます。接続およびセキュリティ インテリジェンス のデータの使用（39-1 ページ）を参照してください。
- トラフィック プロファイリングは、接続データを使用して正常なネットワーク トラフィックのプロファイルを作成します。ユーザはそのプロファイルを基準として使用して、異常な動作を検出および追跡できます。トラフィック プロファイルの作成（53-1 ページ）を参照してください。
- 相関ポリシーを使用して、イベントを生成し、特定のタイプの接続またはトラフィック プロファイルの変更に対する応答（アラートや外部修復など）をトリガーできます。相関ポリシーのルールの作成（51-3 ページ）を参照してください。

注　これらの機能を使用するには、接続（ほとんどの場合、接続の開始ではなく接続の終了）を Defense Center データベースにロギングする**必要があります**。システムがクリティカルな接続（ログに記録された侵入、禁止されたファイルおよびマルウェアに関連付けられているもの）を自動的にロギングするのはこのためです。

Defense Center が保存できる接続イベントおよびセキュリティ インテリジェンス イベントの数は、そのモデルによって異なります。それらの制限のリストおよび接続イベント ストレージの無効化については、データベース イベント制限の設定（63-16 ページ）を参照してください。

アクセス コントロールおよび SSL ルール アクションがどのようにロギングに影響を及ぼすかについて

ライセンス： 機能によって異なる

すべてのアクセス コントロールおよび SSL ルールには*アクション*があり、それによってシステムがルールに一致するトラフィックを検査および処理する方法だけでなく、一致するトラフィックに関する詳細をユーザがロギングできる時期と方法が決まります。

注　アクセス コントロールと SSL ポリシーのデフォルト アクションによって許可された接続のロギングは、若干処理が異なります。アクセス コントロールのデフォルト アクションによって処理された接続のロギング（38-19 ページ）および 暗号化された接続および復号化できない接続のデフォルトのロギング設定（38-16 ページ）を参照してください。

詳細については、以下を参照してください。

- ルール アクションを使用したトラフィックの処理とインスペクションの決定（14-8 ページ）
- ルール アクションを使用した暗号化トラフィックの処理と検査の決定（21-9 ページ）
- モニタされた接続のロギングについて（38-7 ページ）
- 信頼されている接続のロギングについて（38-7 ページ）

モニタされた接続のロギングについて

ライセンス： 機能によって異なる

システムは、ルールのロギング設定や、後で接続を処理するデフォルト アクションとは関係なく、次の接続の終了を Defense Center データベースに常にロギングします。

- モニタに設定されたセキュリティ インテリジェンスのブラックリストに一致する接続
- SSL モニタ ルールに一致する接続
- アクセス コントロールのモニタ ルールに一致する接続

言い換えると、パケットが他のルールに一致せず、デフォルト アクションでロギングが有効になっていない場合でも、パケットがモニタ ルールまたはセキュリティ インテリジェンスのモニタ対象ブラックリストに一致すれば、必ず接続がロギングされます。セキュリティ インテリジェンスのフィルタリングの結果、システムが接続イベントをロギングすると、一致するセキュリティ インテリジェンス イベントもロギングされます。そのイベントは特殊なタイプの接続イベントで、個別に表示および分析できます。セキュリティ インテリジェンス（ブラックリスト登録）の決定のロギング（38-12 ページ）を参照してください。

モニタ対象のトラフィックは、必ず後で別のルールまたはデフォルト アクションによって処理されるため、モニタ ルールが原因でロギングされる接続に関連するアクションは、決して `Monitor` にはなりません。代わりに、後で接続を処理するルールまたはデフォルト アクションの操作が反映されます。処理（39-5 ページ）を参照してください。

システムは、1 つの接続が 1 つの SSL またはアクセス コントロールのモニタ ルールに一致するたびに 1 つの別個のイベントを生成する**わけではありません**。1 つの接続が複数のモニタ ルールに一致する可能性があるため、Defense Center データベースにロギングされる各接続イベントには、接続が一致する最初の 8 つのモニタ アクセス コントロール ルールに関する情報だけでなく、最初の一致するモニタ SSL ルールに関する情報を含めて表示することができます。

同様に、外部 syslog または SNMP トラップ サーバに接続イベントを送る場合、システムは 1 つの接続が 1 つのモニタ ルールに一致するたびに 1 つの別個のアラートを送信するわけではありません。代わりに、接続の終了時にシステムから送られるアラートに、接続が一致したモニタ ルールの情報が含まれます。

ヒント　接続ログ内のルール アクションは決して `Monitor` になりませんが、モニタ ルールに一致する接続に対する相関ポリシー違反をトリガーすることはできます。詳細については、相関ルール トリガー条件の指定（51-5 ページ）を参照してください。

信頼されている接続のロギングについて

ライセンス： 機能によって異なる

信頼されている接続は、信頼アクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションによって処理される接続です。これらの接続の開始と終了をロギングできますが、暗号化されているかどうかにかかわらず、信頼されている接続は検出データ、侵入、または禁止されているファイルおよびマルウェアの有無について検査されないことに注意してください。したがって、信頼されている接続の接続イベントには、限られた情報が含まれます。

システムは、接続を検出したデバイスに応じて異なる方法で、信頼アクセス コントロール ルールによって処理された TCP 接続をロギングすることに注意してください。

- シリーズ 3 デバイスでは、信頼ルールによって最初のパケットで検出された TCP 接続は、すでに有効になっているモニタ ルールの有無に応じて異なるイベントを生成します。モニタ ルールがアクティブな場合、システムはパケットを評価し、接続の開始および終了イベントを生成します。アクティブなモニタ ルールがない場合、システムは接続終了イベントだけを生成します。
- 他のすべてのモデルでは、信頼ルールによって最初のパケットで検出された TCP 接続は、接続終了イベントだけを生成します。システムは、最後のセッション パケットの 1 時間後にイベントを生成します。

ブロックされた接続およびインタラクティブにブロックされた接続のロギングについて

ライセンス: 機能によって異なる

ブロックされた接続をロギングするときは、システムがその接続をどのようにロギングするかは接続がブロックされた理由によって異なります。これは、接続ログに基づいて相関ルールを設定する際に留意しておくことが重要です。

- 暗号化されたトラフィックをブロックする SSL ルールおよび SSL ポリシーのデフォルト アクションの場合、システムは接続**終了**イベントをロギングします。これは、システムが接続がセッション内で最初のパケットを使用して暗号化されているかどうかを決定できないためです。
- 復号化されたトラフィックまたは暗号化されていないトラフィックをブロックするアクセス コントロール ルールおよびアクセス コントロール ポリシーのデフォルト アクション（インタラクティブなブロッキング ルールを含む）の場合、システムは接続**開始**イベントをロギングします。一致するトラフィックは、追加のインスペクションなしで拒否されます。

アクセス コントロールまたは SSL ルールでブロックされたセッションの接続イベントには、アクション `Block` または `Block with reset` があります。ブロックされた暗号化接続には 理由 `SSL Block` があります。

インタラクティブ ブロッキング アクセス コントロール ルール（このルールではユーザが禁止されている Web サイトを参照するとシステムによって警告ページが表示されます）を使用すると、接続終了ロギングを設定できます。その理由は、警告ページをユーザがクリック スルーすると、その接続は新規の、許可された接続と見なされ、システムによってモニタとロギングができるためです。許可された接続のロギングについて（38-9 ページ）を参照してください。

したがって、インタラクティブ ブロック ルールまたはリセット付きインタラクティブ ブロック ルールにパケットが一致する場合、システムは以下の接続イベントを生成できます。

- ユーザの要求が最初にブロックされ警告ページが表示されたときの接続開始イベント。このイベントにはアクション `Interactive Block` または `Interactive Block with reset` が関連付けられます。
- 複数の接続開始または終了イベント（ユーザが警告ページをクリック スルーし、要求した最初のページをロードした場合。これらのイベントには `Allow` アクションおよび理由 `User Bypass` が関連付けられます）

インラインで展開されたデバイスのみがトラフィックをブロックできることに注意してください。ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

注意　サービス妨害(DoS)攻撃の間にブロックされた TCP 接続をロギングすると、システム パフォーマンスに影響し、複数の同様のイベントによってデータベースが過負荷になる可能性があります。ブロック ルールに対してロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたは DoS 攻撃を受けやすい他のインターフェイス上のトラフィックをモニタするかどうかを検討します。

許可された接続のロギングについて

ライセンス: 機能によって異なる

Decrypt SSL ルール、Do not decrypt SSL ルール、および Allow access control ルールは、一致するトラフィックがインスペクションおよびトラフィックの処理の次のフェーズへと通過することを許可します。

SSL ルールを使用して暗号化されたトラフィックを復号化するかどうかにかかわらず、トラフィックはアクセス コントロール ルールによって引き続き評価されます。この SSL ルールにロギングを有効にすると、アクセス コントロール ルールまたはそれらを後で処理するデフォルト アクションのロギング設定に関係なく、システムは一致する接続の終了をロギングします。

アクセス コントロール ルールでトラフィックを許可すると、関連付けられた侵入ポリシーまたはファイル ポリシー(またはその両方)を使用して、トラフィックをさらに検査し、トラフィックが最終宛先に到達する前に、侵入、禁止されたファイル、およびマルウェアをブロックすることができます。ただし、デフォルトでは、ファイルおよび侵入のインスペクションは暗号化されたペイロードでは無効になっていることに注意してください。

許可アクセス コントロール ルールに一致するトラフィックの接続は次のようにロギングされます。

- アクセス コントロール ルールによって呼び出された侵入ポリシーが侵入を検出して侵入イベントを生成すると、システムはルールのロギング設定に関係なく、侵入が発生した接続の終了を Defense Center データベースに自動的にロギングします。
- アクセス コントロール ルールによって呼び出されたファイル ポリシーが禁止されたファイル(マルウェアを含む)を検出してファイル イベントまたはマルウェア イベントを生成すると、システムはアクセス コントロール ルールのロギング設定に関係なく、ファイルが検出された接続の終了を Defense Center データベースに自動的にロギングします。
- 任意で、システムが安全と見なすトラフィックや、侵入ポリシーまたはファイル ポリシーで検査をしないトラフィックなど、許可されたトラフィックに対して接続の開始および終了のロギングを有効にできます。

結果として生じるすべての接続イベントで、[Action] および [Reason] フィールドにイベントがロギングされた理由が反映されます。処理(39-5 ページ) および Reason(39-8 ページ)を参照してください。次の点に注意してください。

- アクション `Allow` は、最終宛先に到達した明示的に許可されインタラクティブにユーザがバイパスしたブロックされた接続を表します。
- アクション `Block` は、アクセス コントロール ルールによって初めは許可されたが、侵入、禁止されたファイル、またはマルウェアが検出された接続を表します。

許可された接続のファイルおよびマルウェア イベント ロギングの無効化

ライセンス： ProtectionまたはMalware

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

アクセス コントロール ルールで暗号化されていないまたは復号化されたトラフィックを許可すると、関連付けられたファイル ポリシーを使用して、送信されたファイルを検査し、そのトラフィックが宛先に到達する前に禁止されたファイルおよびマルウェアをブロックできます。侵入防御パフォーマンスの調整（18-10 ページ）を参照してください。DC500 で Malware ライセンスを使用したり、シリーズ 2 デバイスまたは Cisco NGIPS for Blue Coat X-Series で Malware ライセンスを有効にすることはできないので、それらのアプライアンスをマルウェア防御に使用することはできないことに注意してください。

システムが禁止されたファイルを検出すると、次のタイプのイベントの 1 つを Defense Center データベースに自動的にロギングします。

- *ファイル イベント*：検出またはブロックされたファイル（マルウェア ファイルを含む）を表します
- *マルウェア イベント*：検出されたまたはブロックされたマルウェア ファイルのみを表します
- *レトロスペクティブ マルウェア イベント*：以前に検出されたファイルでのマルウェア処理が変化した場合に生成されます

ファイル イベントまたはマルウェア イベントをロギングしない場合は、アクセス コントロール ルール エディタの [Logging] タブの [Log Files] チェックボックスをオフにすることで、アクセス コントロール ルールごとにこのロギングを無効にできます。ファイルおよびマルウェアのイベント ストレージを完全に無効にする詳細については、データベース イベント制限の設定（63-16 ページ）を参照してください。

注 Cisco では、ファイル イベントおよびマルウェア イベントのロギングを有効のままにすることを推奨しています。

ファイル イベントおよびマルウェア イベントを保存するかどうかにかかわらず、ネットワーク トラフィックがファイル ポリシーに違反すると、呼び出し元のアクセス コントロール ルールのロギング設定に関係なく、システムは関連付けられた接続の終了を Defense Center データベースに自動的にロギングします。ファイル イベントとマルウェア イベントに関連付けられた接続（自動）（38-4 ページ）を参照してください。

接続ロギングのライセンスおよびモデル要件

ライセンス： 機能によって異なる

アクセス コントロール ポリシーおよび SSL ポリシーで接続ロギングを設定する前に、これらのポリシーが正常に処理できる任意の接続をロギングできます。

アクセス コントロール ポリシーおよび SSL ポリシーは、Defense Center でのライセンスに関係なく作成できます。ただし、アクセス コントロールのある側面では、ポリシーを適用する前にターゲット デバイスで特定のライセンス交付対象の機能を有効にする必要があります。また、一部の機能は、特定のモデルでのみ使用できます。

Defense Center に含まれている FireSIGHT ライセンスを使用して、ホスト、ユーザおよびアプリケーションのデータを接続ログの情報に基づいてネットワーク マップに追加できます。また、接続イベントに関連付けられている侵害の兆候（IOC）情報を表示できます。DC500 以外では、接続に関連付けられている位置情報データ（送信元または宛先の国または大陸）を表示することもできます。

次の表では、アクセス コントロールを正常に設定し、アクセス コントロール ポリシーによって処理される接続をロギングするのに必要なライセンスについて説明します。

表 38-2　アクセス コントロール ポリシーにおける接続ロギングのライセンスおよびモデルの要件

次の接続をロギングするには	ライセンス	サポートされる Defense Center	サポートされるデバイス数
ネットワーク、VLAN、ポートまたはリテラル URL 基準を使用して処理されるトラフィック用	いずれか	いずれか	以下を除くすべて: • シリーズ 2 デバイスは、URL フィルタリングを実行できません • ASA FirePOWER デバイスは、VLAN フィルタリングを実行できません
位置情報データを使用して処理されるトラフィック用	FireSIGHT	すべて（DC500 を除く）	すべて（シリーズ 2 または X-Series を除く）
関連付ける対象 • レピュテーションが低い IP アドレス（セキュリティ インテリジェンスのフィルタリング） • 暗号化されていないまたは復号化されたトラフィックの侵入または禁止されたファイル	Protection	いずれか	任意：例外として、シリーズ 2 デバイスではセキュリティ インテリジェンス フィルタリングを実行できません。
暗号化されていないまたは復号化されたトラフィックで検出されたマルウェアに関連付けられる	Malware	すべて（DC500 を除く）	すべて（シリーズ 2 または X-Series を除く）
ユーザ制御またはアプリケーション制御によって処理されるトラフィック用	Control	任意：例外として、DC500 ではユーザ制御を実行できません。	すべて（シリーズ 2 または X-Series を除く）
URL カテゴリおよびレピュテーション データを使用してシステムがフィルタリングするトラフィック用、およびモニタ対象ホストによって要求される URL の URL カテゴリおよび URL レピュテーション情報を表示するため	URL Filtering	すべて（DC500 を除く）	すべて（シリーズ 2 を除く）

次の表では、SSL インスペクションを正常に設定し、SSL ポリシーによって処理される接続をロギングするために必要なライセンスについて説明します。暗号化された接続が SSL ポリシーによってロギングされない（または検査さえされない）場合でも、他の理由で引き続きロギングされる場合があることに留意してください。

表 38-3　SSL ポリシーにおける接続ロギングのライセンスおよびモデルの要件

次の接続をロギングするには	ライセンス	サポートされる Defense Center	サポートされるデバイス数
ゾーン、ネットワーク、VLAN、ポート、または SSL 関連の基準を使用して処理される暗号化トラフィック用	いずれか	いずれか	シリーズ 3
位置情報データを使用して処理される暗号化トラフィック用	FireSIGHT	すべて(DC500 を除く)	シリーズ 3
アプリケーションまたはユーザの基準を使用して処理される暗号化トラフィック用	Control	任意:例外として、DC500 ではユーザ制御を実行できません。	シリーズ 3
URL カテゴリおよびレピュテーション データを使用してシステムがフィルタリングする暗号化トラフィック用	URL Filtering	すべて(DC500 を除く)	シリーズ 3

セキュリティ インテリジェンス(ブラックリスト登録)の決定のロギング

ライセンス: Protection

サポートされるデバイス: すべて(シリーズ 2 を除く)

サポートされる防御センター: DC500 を除くいずれか

悪意のあるインターネット コンテンツに対する第一の防衛ラインとして、FireSIGHT システムにはセキュリティ インテリジェンス機能があり、それを使用することで、最新のレピュテーション インテリジェンスに基づいて接続を即座にブラックリスト登録(ブロック)することができ、リソースを集中的に使用する詳細な分析の必要がなくなります。このトラフィック フィルタリングは、他のどのポリシー ベースのインスペクション、分析、またはトラフィック処理よりも**前**に行われますが、高速パスなどのハードウェア レベルの処理の後に発生します。

オプションで、セキュリティ インテリジェンス フィルタリングには「モニタ専用」設定を使用できます。パッシブ展開環境では、この設定が推奨されます。この設定では、ブラックリスト登録されるはずの接続をシステムがさらに分析できるだけでなく、ブラックリストと一致する接続をログに記録することもできます。

注　セキュリティ インテリジェンス情報に基づいてトラフィック プロファイルを作成する場合、または接続終了イベントのセキュリティ インテリジェンス情報を使用して相関ルールをトリガーする場合は、この情報を Defense Center データベースにロギングする**必要があります**。最初に、セキュリティ インテリジェンスのロギングを有効にします。次に、モニタ専用のセキュリティ インテリジェンス オブジェクトを使用して、ブラックリストを作成します。詳細については、セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録 (13-1 ページ)を参照してください。

セキュリティ インテリジェンスのロギングを有効にすると、アクセス コントロール ポリシーのターゲット デバイスによって処理されるすべてのブロックされた接続およびモニタされた接続がロギングされます。ただし、システムはホワイトリストの一致はロギングしません。ホワイトリストに登録された接続のロギングは、その接続の最終的な傾向によって異なります。

セキュリティ インテリジェンスのフィルタリングの結果、システムが接続イベントをロギングすると、一致するセキュリティ インテリジェンス イベントもロギングされます。そのイベントは特殊なタイプの接続イベントで、個別に表示および分析できます。どちらのタイプのイベントも、[Action] および [Reason] フィールドを使用して、ブラックリストの一致を反映します。さらに、接続でブラックリスト登録された IP アドレスを特定できるように、IP アドレスの横にあるホスト アイコンは、ブラックリスト登録された IP アドレスとモニタされた IP アドレスではイベント ビューアで少々異なる表示になっています。

ブロックされたブラックリスト登録された接続のロギング

ブロックされた接続の場合、システムは接続開始セキュリティ インテリジェンス イベントと接続イベントをロギングします。ブラックリスト登録されたトラフィックは追加のインスペクションなしですぐに拒否されるため、ログに記録できる固有の接続の終了イベントはありません。これらのイベントの場合、アクションは `Block` で、理由は `IP Block` です。

`IP Block` 接続イベントのしきい値は、開始側と応答側の固有のペアあたり 15 秒です。つまり、システムは接続をブロックしてイベントを生成した時点から 15 秒の間、この 2 つのホスト間で接続がブロックされたとしても、ポートやプロトコルの違いに関わらず、別の接続イベントを生成しません。

モニタされブラックリスト登録された接続のロギング

セキュリティ インテリジェンスによってモニタされた（ブロックではなく）接続の場合、システムは接続終了セキュリティ インテリジェンス イベントと接続イベントを Defense Center データベースにロギングします。このロギングは、接続が後で SSL ポリシー、アクセス コントロール ルール、またはアクセス コントロールのデフォルト アクションによってどのように処理されるかにかかわらず発生します。

これらの接続イベントの場合、アクションは接続の最終的な傾向によって異なります。[Reason] フィールドには、`IP Monitor` と、接続がロギングされている可能性がある他の理由が含まれています。

ただし、モニタされる接続の場合、以降に接続を処理するアクセス コントロール ルールやデフォルト アクションでのロギング設定によっては、接続開始イベントが生成されることもあります。

ブラックリスト登録された接続をログに記録する方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　設定するアクセス コントロール ポリシーの横にある編集アイコン（  ）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3　[Security Intelligence] タブを選択します。

アクセス コントロール ポリシーのセキュリティ インテリジェンス設定が表示されます。

ステップ 4　ロギング アイコン（  ）をクリックします。

[Blacklist Options] ポップアップ ウィンドウが表示されます。

ステップ 5　[Log Connections] チェックボックスをオンにします。

ステップ 6　接続イベントとセキュリティ インテリジェンス イベントの送信先を指定します。次の選択肢があります。

- イベントを Defense Center に送信する場合は、**[Defense Center]** を選択します。

- イベントを外部 syslog サーバに送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。オプションで、syslog アラート応答を追加するには、追加アイコン（ ）をクリックします。Syslog アラート応答の作成（43-5 ページ）を参照してください。
- 接続イベントを SNMP トラップ サーバに送信する場合は、[SNMP Trap] を選択し、ドロップダウンリストから SNMP アラート応答を選択します。オプションで、追加アイコン（ ）をクリックして SNMP アラート応答を追加することもできます（SNMP アラート応答の作成（43-4 ページ）を参照）。

ブラックリスト登録されたオブジェクトをモニタ専用に設定する場合、またはセキュリティ インテリジェンス フィルタリングによって生成された接続イベントで他の Defense Center ベースの分析を行う場合は、イベントを Defense Center に送信することが**必須**となります。詳細については、Defense Center または外部サーバへの接続のロギング（38-5 ページ）を参照してください。

ステップ 7　[OK] をクリックしてロギング オプションを設定します。

[Security Intelligence] タブが再表示されます。

ステップ 8　[Save] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

暗号化された接続のロギング

ライセンス： SSL

サポートされるデバイス： シリーズ 3

アクセス コントロールの一部として、*SSL インスペクション*機能を使用することで、SSL ポリシーを使用してアクセス コントロール ルールによるさらなる評価のために暗号化されたトラフィックを復号化できます。システムがトラフィックを後でどのように処理または検査するかにかかわらず、これらの復号化された接続のログを記録するようにシステムに強制できます。また、暗号化されたトラフィックをブロックするとき、または復号化せずにトラフィックがアクセス コントロール ルールに渡されることを許可するときに、接続をロギングすることもできます。

暗号化セッションの接続ログには、セッションの暗号化に使用される証明書など、暗号化の詳細が含まれます。クリティカルな接続のみをログに記録するように、SSL ポリシーの暗号化されたセッションの接続ロギングは SSL ルールごとに設定します。

詳細については、次の項を参照してください。

- SSL ルールによる復号可能接続のロギング（38-14 ページ）
- 暗号化された接続および復号化できない接続のデフォルトのロギング設定（38-16 ページ）

SSL ルールによる復号可能接続のロギング

ライセンス： SSL

サポートされるデバイス： シリーズ 3

SSL ポリシー内では、*SSL ルール*は複数の管理対象デバイス間で暗号化されたトラフィックを処理する詳細な方法を提供します。クリティカルな接続のみをロギングできるように、SSL ルールごとに接続ロギングを有効にします。あるルールに対して接続ロギングを有効にすると、システムはそのルールによって処理されるすべての接続をロギングします。

SSL ポリシーによって検査される暗号化された接続の場合、接続イベントのログは、Defense Center データベース、または外部の syslog や SNMP トラップ サーバに記録できます。ただし次の場合は、接続の終了（end-of-connection）イベントだけをログに記録できます。

- ブロックされた接続（[Block]、[Block with reset]）の場合、システムは即座にセッションを終了し、イベントを生成します。
- モニタ対象の接続（[Monitor]）およびアクセス コントロール ルールに渡す接続（[Decrypt]、[Do not decrypt]）の場合、アクセス コントロール ルールまたはそのセッションを後で処理するデフォルト アクションのロギング設定に関係なく、システムはセッション終了時にイベントを生成します。

詳細については、アクセス コントロールおよび SSL ルール アクションがどのようにロギングに影響を及ぼすかについて（38-6 ページ）を参照してください。

復号化できる接続をログに記録するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin/Security Approver

ステップ 1　[Policies] > [SSL] を選択します。

[SSL Policy] ページが表示されます。

ステップ 2　編集する SSL ポリシーの横にある編集アイコン（）をクリックします。

SSL ポリシー エディタが表示され、[Rules] タブにフォーカスが移動します。

ステップ 3　ロギングを設定するルールの横にある編集アイコン（）をクリックします。

SSL ルール エディタが表示されます。

ステップ 4　[Logging] タブを選択します。

[Logging] タブが表示されます。

ステップ 5　[Log at End of Connection] を選択します。

ステップ 6　接続イベントの送信先を指定します。次の選択肢があります。

- 接続イベントを Defense Center に送信する場合は、**[Defense Center]** を選択します。ルール アクションが [Monitor] である場合は、接続をDefense Centerにロギングする必要があります。
- イベントを外部の syslog に送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。オプションで、syslog アラート応答を追加するには、追加アイコン（）をクリックします。Syslog アラート応答の作成（43-5 ページ）を参照してください。
- イベントを SNMP トラップ サーバに送信する場合は、[SNMP Trap] を選択し、ドロップダウンリストから SNMP アラート応答を選択します。オプションで、追加アイコン（）をクリックして SNMP アラート応答を追加することもできます（SNMP アラート応答の作成（43-4 ページ）を参照）。

これらの接続イベントで Defense Center ベースの分析を実行するには、Defense Center にイベントを送信する**必要があります**。詳細については、Defense Center または外部サーバへの接続のロギング（38-5 ページ）を参照してください。

ステップ 7　[Add] をクリックして変更を保存します。

変更を反映させるには、SSL ポリシーが関連付けられているアクセス コントロール ポリシーを適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

暗号化された接続および復号化できない接続のデフォルトのロギング設定

ライセンス： SSL

サポートされるデバイス： シリーズ 3

SSL ポリシーのデフォルト アクションによって処理されるトラフィックの接続をログに記録できます。これらのロギング設定では、システムが復号化できないセッションをどのようにログに記録するかも管理されます。

SSL ポリシーのデフォルト アクションは、ポリシー内のどの SSL ルール（トラフィックの照合とロギングは行うが、処理または検査はしないモニタ ルールを除く）にも一致しない暗号化されたトラフィックをシステムがどのように処理するかを決定します。SSL ポリシーに SSL ルールが含まれていない場合、デフォルト アクションは、ネットワーク上のすべての暗号化セッションがどのようにログに記録されるかを決定します。詳細については、暗号化トラフィックのデフォルトの処理と検査の設定（20-4 ページ）を参照してください。

接続イベントを Defense Center データベース、または外部の syslog や SNMP トラップ サーバにロギングするように SSL ポリシーのデフォルト アクションを設定できます。ただし次の場合は、接続の終了（end-of-connection）イベントだけをログに記録できます。

- ブロックされた接続（Block、Block with reset）の場合、システムは即座にセッションを終了してイベントを生成します。
- 暗号化されていない接続をアクセス コントロールに渡すことを許可する接続の場合（[Do not decrypt]）、システムはセッションの終了時にイベントを生成します。

SSL ポリシーのデフォルト アクションのロギングを無効にしても、接続が以前に少なくとも 1 つの SSL モニタ ルールに一致していた場合、または後でアクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに一致する場合は、接続終了イベントが引き続き Defense Center データベースにロギングされる可能性があることに注意してください。

暗号化されたトラフィックおよび復号化できないトラフィックのデフォルトの処理を設定するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin/Security Approver

ステップ 1　[Policies] > [SSL] を選択します。

[SSL Policy] ページが表示されます。

ステップ 2　編集する SSL ポリシーの横にある編集アイコン（  ）をクリックします。

SSL ポリシー エディタが表示され、[Rules] タブにフォーカスが移動します。

ステップ 3　[Default Action] ドロップダウンリストの横にあるロギング アイコン（  ）をクリックします。

[Logging] ポップアップ ウィンドウが表示されます。

ステップ 4　[Log at End of Connection] を選択して、接続イベントのロギングを有効にします。

ステップ 5　接続イベントの送信先を指定します。次の選択肢があります。

- 接続イベントを Defense Center に送信する場合は、[Defense Center] を選択します。
- イベントを外部 syslog サーバに送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。オプションで、追加アイコン（  ）をクリックすることで、syslog アラート応答を設定できます。Syslog アラート応答の作成（43-5 ページ）を参照してください。

- イベントを SNMP トラップ サーバに送信する場合は、[SNMP Trap] を選択し、ドロップダウンリストから SNMP アラート応答を選択します。オプションで、追加アイコン（  ）をクリックすることで、SNMP アラート応答を設定できます。SNMP アラート応答の作成（43-4 ページ）を参照してください。

これらの接続イベントで Defense Center ベースの分析を実行するには、Defense Center にイベントを送信する**必要があります**。しかし、SSL ポリシーのデフォルト アクションによって処理されるトラフィックは、侵入、マルウェア、または検出データの有無についてさらなる検査が行われないことに注意してください。詳細については、Defense Center または外部サーバへの接続のロギング（38-5 ページ）を参照してください。

ステップ 6　[OK] をクリックして変更を保存します。

変更を反映させるには、SSL ポリシーが関連付けられているアクセス コントロール ポリシーを適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

アクセス コントロールの処理に基づく接続のロギング

ライセンス： すべて

アクセス コントロール ポリシー内で、アクセス コントロール ルールは複数の管理対象デバイスでネットワーク トラフィックを処理する詳細な方法を提供しています。クリティカルな接続のみをロギングできるように、アクセス コントロール ルールごとに接続ロギングを有効にします。あるルールに対して接続ロギングを有効にすると、システムはそのルールによって処理されるすべての接続をロギングします。

また、アクセス コントロール ポリシーのデフォルト アクションによって処理されたトラフィックの接続もロギングできます。デフォルト アクションによって、システムがポリシー内のアクセス コントロール ルールのいずれにも一致しないトラフィックを処理する方法が決まります（トラフィックに一致しロギングするが、処理または検査はしないモニタ ルールを除く）。

すべてのアクセス コントロール ルールおよびデフォルト アクションのロギングを無効にしても、接続がアクセス コントロール ルールに一致し、侵入の試み、禁止されたファイル、またはマルウェアが含まれている場合、またはシステムによって復号化され、SSL ポリシーで接続のロギングを有効にした場合は、接続終了イベントは引き続き Defense Center データベースにロギングされる場合があることに注意してください。

ルールまたはデフォルトのポリシー アクション、および設定した関連するインスペクション オプションによって、ロギング オプションは異なります。詳細については、以下を参照してください。

- アクセス コントロール ルールに一致する接続のロギング（38-17 ページ）
- アクセス コントロールのデフォルト アクションによって処理された接続のロギング（38-19 ページ）

アクセス コントロール ルールに一致する接続のロギング

ライセンス： すべて

クリティカルな接続のみをロギングするには、アクセス コントロール ルールごとに接続ロギングを有効にします。あるルールに対しロギングを有効にすると、システムはそのルールによって処理されたすべての接続をロギングします。

ルール アクションおよびそのルールの侵入およびファイルのインスペクション設定によって、ロギング オプションは異なります。アクセス コントロールおよび SSL ルール アクションがどのようにロギングに影響を及ぼすかについて（38-6 ページ）を参照してください。また、アクセス コントロール ルールに対してロギングを無効にしても、接続が以下の場合は、そのルールに一致する接続の接続終了イベントは引き続き Defense Center データベースにロギングされる場合があることに注意してください。

- 侵入の試み、禁止されたファイル、またはマルウェアが含まれている場合
- SSL ポリシーによって検査され、ログに記録された場合
- 以前に少なくとも 1 つのアクセス コントロールのモニタ ルールに一致した場合

接続、ファイル、およびマルウェア情報をログに記録するアクセス コントロール ルールを設定する方法：

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　変更するアクセス コントロール ポリシーの横にある編集アイコン（  ）をクリックします。

アクセス コントロール ポリシー エディタが表示され、[Rules] タブに焦点が置かれています。

ステップ 3　ロギングを設定するルールの横にある編集アイコン（  ）をクリックします。

アクセス コントロール ルール エディタが表示されます。

ステップ 4　[Logging] タブを選択します。

[Logging] タブが表示されます。

ステップ 5　接続の開始/終了時点でのロギングを示す [Log at Beginning of Connection] または [Log at End of Connection] を選択します。

パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。

単一のブロックされていない接続の場合、接続終了イベントには、接続開始イベントに含まれるすべての情報に加えて、セッション期間中に収集された情報も含まれます。ブロックされたトラフィックは追加のインスペクションなしで即座に拒否されるので、ブロック ルールの接続開始イベントのみをログに記録できます。

また、モニタ ルールの目的は一致するトラフィックをロギングすることなので、Defense Center データベースへの接続終了ロギングは自動的に有効になっており、無効にできないことに注意してください。詳細については、接続の開始または終了のロギング（38-4 ページ）を参照してください。

ステップ 6　接続に関連しているファイル イベントとマルウェア イベントをすべてログに記録するかどうか指定するには、[Log Files] チェック ボックスを使用します。

ユーザがファイル ポリシーをルールに関連付けてファイル制御または AMP を実行すると、システムはこのオプションを自動的に有効にします。Cisco は、このオプションを有効のままにすることを推奨します。許可された接続のファイルおよびマルウェア イベント ロギングの無効化（38-10 ページ）を参照してください。

ステップ 7　接続イベントの送信先を指定します。次の選択肢があります。

- 接続イベントを Defense Center に送信する場合は、[Defense Center] を選択します。このオプションは、モニタ ルールに対して無効にできません。

- イベントを外部 syslog サーバに送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。オプションで、syslog アラート応答を追加するには、追加アイコン（  ）をクリックします。Syslog アラート応答の作成（43-5 ページ）を参照してください。
- イベントを SNMP トラップ サーバに送信する場合は、[SNMP Trap] を選択し、ドロップダウンリストから SNMP アラート応答を選択します。オプションで、追加アイコン（  ）をクリックして SNMP アラート応答を追加することもできます（SNMP アラート応答の作成（43-4 ページ）を参照）。

接続イベントで Defense Center ベースの分析を実行するには、データベースにイベントを送信する**必要があります**。詳細については、Defense Center または外部サーバへの接続のロギング（38-5 ページ）を参照してください。

ステップ 8　[Save] をクリックしてルールを保存します。

ルールが保存されます。変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

アクセス コントロールのデフォルト アクション によって処理された接続のロギング

ライセンス： すべて

アクセス コントロール ポリシーのデフォルト アクションによって処理されたトラフィックの接続をロギングできます。デフォルト アクションによって、システムがポリシー内のアクセス コントロール ルールのいずれにも一致しないトラフィックを処理する方法が決まります（トラフィックに一致しロギングするが、処理または検査はしないモニタ ルールを除く）。デフォルトの処理の設定およびネットワーク トラフィックのインスペクション（12-7 ページ）を参照してください。

ポリシーのデフォルト アクションによって処理された接続のメカニズムとオプションは、次の表で示すように、個々のアクセス コントロール ルールによって処理された接続のロギング オプションとほとんど同じです。つまり、ブロックされたトラフィックを除き、接続の開始と終了をログに記録でき、接続イベントを Defense Center データベース、または外部の syslog や SNMP トラップ サーバに送信できます。

表 38-4　　アクセス コントロールのデフォルト アクションのロギング オプション

デフォルト アクション	比較対象	参照先
Access Control: Block All Traffic	ブロック ルール	ブロックされた接続およびインタラクティブにブロックされた接続のロギングについて（38-8 ページ）
Access Control: Trust All Traffic	信頼ルール	信頼されている接続のロギングについて（38-7 ページ）
Intrusion Prevention	関連付けられた侵入ポリシーを持つ許可ルール	許可された接続のロギングについて（38-9 ページ）
Network Discovery Only	関連付けられた侵入ポリシーを持たない許可ルール	

しかし、アクセス コントロール ルールによって処理された接続のロギングとデフォルト アクションによって処理された接続のロギングにはいくつかの違いがあります。

- デフォルト アクションにはファイル ロギング オプションはありません。デフォルト アクションを使用して、ファイル制御または AMP を実行できません。
- アクセス コントロールのデフォルト アクションに関連付けられた侵入ポリシーによって侵入イベントが生成された場合、システムは、そのイベントに関連する接続の終了を自動的にログに記録**しません**。これは、接続データをログに記録する必要のない、侵入検知および防御のみを行う展開で役立ちます。

  ただし例外として、デフォルト アクションの接続開始ロギングを有効にした場合はその限りではありません。この場合、関連付けられた侵入ポリシーがトリガーされると、システムは接続の開始だけでなく、接続の終了もログに記録**します**。

デフォルト アクションに対してロギングを無効にしても、接続が以前に少なくとも 1 つのアクセス コントロールのモニタ ルールに一致した場合、または SSL ポリシーによって検査およびロギングされた場合は、そのルールに一致する接続の接続終了イベントは引き続き Defense Center データベースにロギングされる場合があることに注意してください。

アクセス コントロールのデフォルト アクションによって処理されたトラフィックの接続をログに記録するには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　変更するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示され、[Rules] タブに焦点が置かれています。

ステップ 3　[Default Action] ドロップダウンリストの横にあるロギング アイコン（）をクリックします。

[Logging] ポップアップ ウィンドウが表示されます。

ステップ 4　接続の開始/終了時点でのロギングを示す [Log at Beginning of Connection] または [Log at End of Connection] を選択します。

パフォーマンスを最適化するためには、これらの接続の開始と終了の両方ではなく、どちらか一方をロギングします。単一のブロックされていない接続の場合、接続終了イベントには、接続開始イベントに含まれるすべての情報に加えて、セッション期間中に収集された情報も含まれます。ブロックされたトラフィックは追加のインスペクションなしで即座に拒否されるので、[Block All Traffic] デフォルト アクションの接続開始イベントのみをログに記録できます。

ステップ 5　接続イベントの送信先を指定します。次の選択肢があります。

- 接続イベントを Defense Center に送信する場合は、[Defense Center] を選択します。このオプションは、モニタ ルールに対して無効にできません。
- イベントを外部 syslog サーバに送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。オプションで、syslog アラート応答を追加するには、追加アイコン（）をクリックします。Syslog アラート応答の作成（43-5 ページ）を参照してください。
- イベントを SNMP トラップ サーバに送信する場合は、[SNMP Trap] を選択し、ドロップダウンリストから SNMP アラート応答を選択します。オプションで、追加アイコン（）をクリックして SNMP アラート応答を追加することもできます（SNMP アラート応答の作成（43-4 ページ）を参照）。

接続イベントで Defense Center ベースの分析を実行するには、データベースにイベントを送信する**必要があります**。詳細については、Defense Center または外部サーバへの接続のロギング（38-5 ページ）を参照してください。

ステップ 6　[Save] をクリックしてポリシーを保存します。

ポリシーが保存されます。変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

接続で検出された URL のロギング

ライセンス： FireSIGHT

HTTP トラフィックで、接続終了イベントのログを Defense Center データベースに記録する場合、システムはセッション中にモニタ対象のホストが要求した URL を記録します。

デフォルトでは、システムは URL の最初の 1024 文字を接続ログに保管します。ただし、URL ごとに最大 4096 文字を保管するようにシステムを設定して、モニタ対象のホストが要求する完全な URL が取り込まれるようにすることができます。または、アクセスされた個々の URL を知る必要がない場合は、保管する文字数をゼロに設定して、URL の保管を無効にすることもできます。ネットワーク トラフィックによっては、URL の保管を無効にするか、あるいは保管する URL の文字数を制限すると、システム パフォーマンスが向上する可能性があります。

URL のロギングを無効にしても、URL フィルタリングには影響しません。アクセス コントロール ルールにより、要求された URL、そのカテゴリ、およびレピュテーションに基づいて、トラフィックが適切にフィルタリングされます。システムが、これらのルールによって処理されたトラフィックで要求された個々の URL を記録しないだけです。詳細については、URL のブロッキング（16-9 ページ）を参照してください。

保存する URL の文字数をカスタマイズするには、次の手順を実行します。

アクセス： Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　設定するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3　[Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ 4　[General Settings] の横にある編集アイコン（  ）をクリックします。

[General Settings] ポップアップ ウィンドウが表示されます。

ステップ 5　**接続イベントで保存する URL の最大文字数**を入力します。

0 ～ 4096 の値を指定できます。保管する文字数をゼロにすると、URL フィルタリングを無効にすることなく URL の保管が無効になります。

ステップ 6　[OK] をクリックします。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ 7　[Save] をクリックしてポリシーを保存します。

ポリシーが保存されます。変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

接続およびセキュリティ インテリジェンスのデータの使用

管理対象デバイスがネットワーク上でホストによって生成されたトラフィックをモニタするとき、デバイスは検出した接続のログを生成できます。アクセス コントロールおよび SSL ポリシーでさまざまな設定を行うことで、ログする接続の種類、接続をログする時期、およびデータを保存する場所のきめ細かい制御を行うことができます。ほとんどの場合、接続の開始または終了、またはその両方で接続をロギングできます。

接続をログに記録すると、システムによって*接続イベント*が生成されます。接続がレピュテーション ベースのセキュリティ インテリジェンス機能によってブラックリスト登録(ブロック)またはモニタされる場合は、*セキュリティ インテリジェンス イベント*と呼ばれる特別な種類の接続イベントをログに記録することもできます。

*接続イベント*と呼ばれる接続ログには、検出されたセッションに関するデータが含まれています。組織のセキュリティ上およびコンプライアンス上の要件に従って接続をロギングしてください。アクセス コントロールに到達する前にデバイス レベルで高速パス処理される接続を除く**すべての**接続をログに記録できます。

設定するロギングに加えて、システムは禁止されたファイル、マルウェア、または侵入の試みを検出した場合に、ほとんどの接続を自動的にログに記録します。接続イベント ストレージを完全に無効にしない限り、システムはこれらの接続終了イベントを Defense Center データベースに保存し、さらなる分析に使用します。接続ロギングの設定の詳細については、ネットワーク トラフィックの接続のロギング(38-1 ページ)を参照してください。

注 アプライアンスとライセンスを使用して接続をロギングすることができます個々の接続またはセキュリティ インテリジェンス イベントに使用可能な情報は、ライセンスなどのさまざまな要因によって異なります。詳細については、接続ロギングのライセンスおよびモデル要件(38-10 ページ)を参照してください。

管理対象デバイスで収集された接続データを補うために、NetFlow 対応デバイスによって生成されたレコードを使用して接続イベントを生成できます。FireSIGHT システム の管理対象デバイスによって監視できない NetFlow 対応デバイスがネットワークに配置されている場合は特に有効です。

注　NetFlow のデータ収集はアクセス コントロールにリンクされていないため、ロギングする NetFlow 接続については、きめ細かい制御ができません。FireSIGHT システム の管理対象デバイスは NetFlow 対応デバイスによってエクスポートされるレコードを検出し、それらのレコードのデータに基づいて単一方向の接続終了イベントを生成し、最終的にそのイベントをデータベースに記録するために Defense Center へ送信します。NetFlow レコードはセキュリティ インテリジェンス イベントを生成できず、外部サーバにも記録できません。詳細については、NetFlow について（45-18 ページ）を参照してください。

接続イベントおよびセキュリティ インテリジェンス イベントの動作の詳細については、以下を参照してください。

- 接続およびセキュリティ インテリジェンスのデータについて（39-2 ページ）
- 接続およびセキュリティ インテリジェンスのデータの表示（39-15 ページ）
- 接続グラフの使用（39-17 ページ）
- 接続およびセキュリティ インテリジェンスのデータ テーブルの使用（39-29 ページ）
- 接続およびセキュリティ インテリジェンスのデータの検索（39-34 ページ）
- 接続サマリー ページの表示（39-41 ページ）

接続およびセキュリティ インテリジェンスのデータについて

ライセンス： すべて

*接続イベント*と呼ばれる接続ログには、検出されたセッションに関するデータが含まれています。個々の接続イベントで入手可能な情報はいくつかの要因によって決まりますが、一般的には次のものがあります。

- タイムスタンプ、送信元と宛先の IP アドレス、入出力ゾーン、接続を処理したデバイスなど、基本的な接続特性
- アプリケーション、要求される URL、または接続に関連付けられているユーザなど、システムによって検出または推測される追加の接続特性
- ポリシーがトラフィックを処理したアクセス コントロール ルール（または他の設定）、接続が許可またはブロックされているかどうか、暗号化された接続および復号化された接続に関する詳細など、接続がログに記録された理由に関するメタデータ

アクセス コントロールおよび SSL ポリシーでさまざまな設定を行うことで、ログする接続の種類、接続をログする時期、およびデータを保存する場所のきめ細かい制御を行うことができます。アクセス コントロール ポリシーおよび SSL ポリシーが正常に処理できる任意の接続をログに記録できます。それには、特定のアプライアンス モデルまたはライセンス付与対象の機能が必要な場合があります。接続のロギングは、次の状況で有効にできます。

- 接続がレピュテーション ベースのセキュリティ インテリジェンス機能によってブラックリスト登録（ブロック）またはモニタされた場合
- 暗号化セッションが SSL ポリシーによって処理される場合
- 接続がアクセス コントロール ルールまたはアクセス コントロールのデフォルト アクションによって処理された場合

設定するロギングに加えて、システムは禁止されたファイル、マルウェア、または侵入の試みを検出した場合に、ほとんどの接続を自動的にログに記録します。他のロギング設定に関係なく、システム ポリシーを使用して接続イベント ストレージを完全に無効にしない限り、システムはこれらの接続終了イベントを Defense Center データベースに保存し、さらなる分析に使用します。

また、セキュリティ インテリジェンス ロギングを有効にすると、ブラックリストの一致によって *セキュリティ インテリジェンス イベント*および接続イベントが自動的に生成されます。セキュリティ インテリジェンス イベントは特殊なタイプの接続イベントで、個別に表示および分析できるだけでなく、個別に保存およびプルーニングできます。セキュリティ インテリジェンス ブラックリスト登録の決定を含む、接続ロギングの設定の詳細については、ネットワーク トラフィックの接続のロギング（38-1 ページ）を参照してください。

ヒント　特に明記されていない限り、接続イベントに関する一般情報もまたセキュリティ インテリジェンス イベントに関連します。セキュリティ インテリジェンスの詳細については、セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録（13-1 ページ）を参照してください。

以降のセクションでは、検出された接続に関して使用できる情報の種類の詳細について説明します。

接続サマリーについて

ライセンス： すべて

FireSIGHT システム は 5 分間隔で収集された接続データを接続サマリーに集約します。システムはこれを使用して接続グラフとトラフィック プロファイルを生成します。必要に応じて、接続サマリーのデータに基づいてカスタム ワークフローを作成できます。これは、個々の接続イベントに基づいたワークフローと同じように使用できます。

セキュリティ インテリジェンス イベント専用の接続サマリーはないことに注意してください。ただし、対応する接続終了イベントは接続サマリーのデータに集約できます。

集約するには、複数の接続が次のとおりでなければなりません。

- 接続終了を表している
- 送信元と宛先の IP アドレスが同じで、応答側（宛先）のホストで同じポートを使用している
- 同じプロトコルを使用している（TCP または UDP）
- 同じアプリケーション プロトコルを使用している
- 同じ Cisco 管理対象デバイスで検出されているか、同じ NetFlow 対応デバイスによってエクスポートされている

各接続サマリーには、総合的なトラフィック統計情報のほか、サマリーの接続数も含まれています。NetFlow 対応デバイスは単一方向接続を生成するので、NetFlow データに基づいて接続ごとにサマリーの接続数が 2 ずつ増えます。

接続サマリーには、サマリーに集約された接続に関連付けられたすべての情報が含まれているのではないことに注意してください。たとえば、接続サマリーに接続を集約する際にクライアント情報は使用されないため、サマリーにクライアント情報は含まれません。

詳細については、次の項を参照してください。

- 長時間接続（39-4 ページ）
- 外部応答側からの結合された接続サマリー（39-4 ページ）
- 接続およびセキュリティ インテリジェンスのイベントで利用可能な情報（39-12 ページ）

長時間接続

ライセンス： すべて

接続データを集約する 5 分間隔の 2 回以上に監視対象のセッションがまたがる場合、その接続は *長時間接続* と見なされます。接続サマリーで接続数を計算する際には、システムは長時間接続が開始された 5 分間隔の回のみカウントします。

また、長時間接続において発信側と応答側が送信したパケット数とバイト数を計算する際は、システムは 5 分間隔の各回で実際に送信されたパケット数とバイト数を報告しません。代わりにシステムは、送信された合計パケット数と合計バイト数、接続の長さ、5 分間隔の各回で接続のどの部分が行われたかに基づいて、一定の送信速度を仮定し、値を推定します。

外部応答側からの結合された接続サマリー

ライセンス： すべて

接続データの保存に必要なスペースを減らし、接続グラフのレンダリングを高速化するために、システムは次の場合に接続サマリーを結合します。

- 接続に関連するホストの 1 つが監視対象のネットワーク上にない場合
- 外部ホストの IP アドレスを除き、サマリーに含まれる接続が接続サマリーについて（39-3 ページ）に記載された集約の要件を満たしている場合（プロトコル、アプリケーション プロトコル、検出デバイスなど）

イベント ビューアで接続サマリーを表示する場合や、接続グラフを使用する場合、システムは非監視対象ホストの IP アドレスの代わりに `external` と表示します。

この集約の結果として、外部応答側を含む接続サマリーまたはグラフから接続データのテーブル ビューにドリルダウンしようとすると（つまり、個別の接続データへのアクセス）、テーブル ビューには情報が何も表示されません。

接続およびセキュリティ インテリジェンスのデータ フィールドについて

ライセンス： 機能によって異なる

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

各接続のテーブル ビューまたは接続グラフには、表示している接続または接続サマリーのタイムスタンプ、IP アドレス、地理情報、アプリケーションなどの情報が含まれています。セキュリティ インテリジェンス イベントのビューには接続イベントのビューと同じ一般情報が含まれていますが、[Security Intelligence Category] の値が割り当てられている接続のみ表示します。

注　個々の接続またはセキュリティ インテリジェンス イベントで利用可能な情報は、ライセンスやアプライアンス モデルなど、いくつかの要因によって異なります。詳細については、接続ロギングのライセンスおよびモデル要件（38-10 ページ）を参照してください。

次のリストでは、FireSIGHT システムによってロギングされた接続データを詳しく説明します。個々の接続またはセキュリティ インテリジェンス イベントでロギングされる情報を決定する要素についての説明は、接続およびセキュリティ インテリジェンスのイベントで利用可能な情報（39-12 ページ）のセクションを参照してください。

Access Control Policy

接続をモニタしたアクセス コントロール ポリシー。

Access Control Rule

接続を処理したアクセス コントロール ルールまたはデフォルト アクションと、その接続に一致した最大 8 つの Monitor ルール。

接続が 1 つの Monitor ルールに一致した場合、Defense Centerは接続を処理したルールの名前を表示し、その後に Monitor ルール名を表示します。接続が複数の Monitor ルールに一致したときは、イベント ビューアは一致した Monitor ルールの数を `Default Action + 2 Monitor Rules` などと表示します。

接続に一致した最初の 8 つの Monitor ルールのリストをポップアップ ウィンドウに表示するには、[*N* Monitor Rules] をクリックします。

処理

次の接続をロギングしたアクセス コントロール ルールまたはデフォルト アクションに関連付けられたアクション。

- [Allow] は、明示的に許可され、インタラクティブにユーザがバイパスした、ブロックされた接続を表します。
- [Trust] は、信頼できる接続を表します。システムは、信頼ルールによって検出された TCP 接続をアプライアンスに応じて別にロギングすることに注意してください。

  シリーズ 2、仮想アデバイス、および Cisco NGIPS for Blue Coat X-Series では、信頼ルールによって最初のパケットで検出された TCP 接続だけが接続終了イベントを生成します。システムは、最後のセッション パケットの 1 時間後にイベントを生成します。

  シリーズ 3 アプライアンスでは、信頼ルールによって最初のパケットで検出された TCP 接続は、モニタ ルールの有無に応じて異なるイベントを発生させます。モニタ ルールがアクティブな場合、システムはパケットを評価し、接続の開始および終了イベントを生成します。アクティブなモニタ ルールがない場合、システムは接続終了イベントだけを生成します。
- [Block] と [Block with reset] は、ブロックされた接続を表します。さらにシステムは、[Block] アクションを、セキュリティ インテリジェンスによってブラックリストに記載された接続、SSL ポリシーによってブロックされた接続、侵入ポリシーによってエクスプロイトが検出された接続、ファイル ポリシーによってファイルがブロックされた接続と関連付けます。
- [Interactive Block] と [Interactive Block with reset] は、システムが Interactive Block ルールを使用して最初にユーザの HTTP 要求をブロックしたときにロギングできる接続開始イベントをマークします。システムが表示する警告ページでユーザがクリック操作をすると、そのセッションについてロギングするその他の接続イベントは、アクションが [Allow] になります。

– [Default Action] は、接続がデフォルト アクションによって処理されたことを示します。
– セキュリティ インテリジェンスによって監視されている接続の場合、そのアクションは、接続によってトリガーされる最初の監視以外のアクセス コントロール ルールのアクションか、またはデフォルト アクションです。同様に、Monitor ルールに一致するトラフィックは常に後続のルールまたはデフォルト アクションによって処理されるため、Monitor ルールによってロギングされた接続に関連付けられたアクションが [Monitor] になることはありません。

アプリケーション プロトコル

接続で検出された、ホスト間の通信を表すアプリケーション プロトコル。

Application Risk

接続で検出されたアプリケーション トラフィックに関連するリスク：`Very High`、`High`、`Medium`、`Low`、または `Very Low`。接続で検出されたアプリケーションのタイプごとに、関連するリスクがあります。このフィールドでは、それらのうち最も高いものが表示されます。詳細については、表 45-2（45-12 ページ）を参照してください。

Business Relevance

接続で検出されたアプリケーション トラフィックに関連するビジネス関連性：`Very High`、`High`、`Medium`、`Low`、または `Very Low`。接続で検出されたアプリケーションのタイプごとに、関連するビジネス関連性があります。このフィールドでは、それらのうち最も低いもの（関連が最も低い）が表示されます。詳細については、表 45-2（45-12 ページ）を参照してください。

Category, Tag (Application Protocol, Client, Web Application)

アプリケーションの機能を理解するのに役立つ、アプリケーションを特徴付ける条件。詳細については、表 45-2（45-12 ページ）を参照してください。

Client and Client Version

接続で検出されたクライアントのクライアント アプリケーションとバージョン。

接続に使用されている特定のクライアントをシステムが特定できなかった場合、このフィールドは汎用的な名称としてアプリケーション プロトコル名の後に `client` を付加して `FTP client` などと表示します。

Connections

接続サマリーに含まれる接続数。長時間接続（複数回の接続サマリー間隔にまたがる接続）の場合、最初の接続サマリー間隔の分だけ増加します。

Count

各行に表示される情報に一致する接続数。同一の行が複数作成される制約を適用した後にのみ、[Count] フィールドが表示されることに注意してください。

注　カスタム ワークフローを作成し、ドリルダウン ページに [Count] カラムを追加しない場合、各接続は個別に表示され、パケット数とバイト数は合計されません。

Device

接続を検出した管理対象デバイス。または、NetFlow 対応デバイスからエクスポートされた接続の場合は、NetFlow データを処理した管理対象デバイス。

ファイル

接続に関連付けられたファイル イベント（ある場合）。ファイル リストの代わりに、Defense Centerはファイル表示アイコン（  ）をこのフィールドに表示します。アイコンの数字は、その接続で検出またはブロックされたファイル数（マルウェア ファイルを含む）を示します。

アイコンをクリックするとポップアップ ウィンドウが表示され、接続で検出されたファイルのリストとともに、そのタイプと、該当する場合はマルウェアのルックアップ処理が示されます。

DC500 Defense Center および シリーズ 2 デバイスはどちらもネットワークベースのマルウェア ファイル検出をサポートしていないことに注意してください。

詳細については、接続で検出されたファイルの表示（39-32 ページ）を参照してください。

First Packet or Last Packet

セッションの最初または最後のパケットが検出された日時。

HTTP Referrer

接続で検出された HTTP トラフィックの要求 URL の参照元を示す HTTP 参照元（他の URL へのリンクを提供した Web サイト、他の URL からリンクをインポートした Web サイトなど）。

Ingress Interface or Egress Interface

接続に関連付けられた入力または出力のインターフェイス。展開環境に非同期のルーティング設定が含まれている場合は、入力と出力のインターフェイスが同じインターフェイス セットに属する場合があることに注意してください。

Ingress Security Zone or Egress Security Zone

接続に関連付けられた入力または出力のセキュリティ ゾーン。

Initiator Bytes or Responder Bytes

セッションの開始側またはセッションの応答側が送信した合計バイト数。

Initiator Country or Responder Country

ルーティング可能な IP が検出された場合に、セッションを開始したホスト IP アドレスまたはセッションの応答側に関連付けられた国。その国の国旗のアイコンとともに、その国の ISO 31661 alpha- 3 の国番号が表示されます。国旗アイコンの上にポインタを移動すると、国の完全な名称が表示されます。

DC500 Defense Centerはこの機能をサポートしていないことに注意してください。

Initiator IP or Responder IP

セッションを開始したか、またはセッション応答側として応答したホスト IP アドレス（DNS 解決が有効化されている場合はホスト名も）。ブラックリストに記載された接続でブラックリストに記載された IP アドレスを識別できるように、ブラックリストに記載された IP アドレスの横のアイコンは見た目が少し異なります。

Initiator Packets or Responder Packets

セッションの開始側またはセッションの応答側が送信した合計パケット数。

Initiator User

セッションの開始側にログインしていたユーザ。

Intrusion Events

接続に関連付けられた侵入イベント（ある場合）。イベント リストの代わりに、Defense Center は侵入イベント表示アイコン（  ）をこのフィールドに表示します。

アイコンをクリックするとポップアップ ウィンドウが表示され、接続に関連付けられた侵入イベントのリストとともに、優先度と影響度が示されます。詳細については、接続に関連付けられた侵入イベントの表示（39-33 ページ）を参照してください。

IOC

接続にかかわったホストに対する侵害の痕跡（IOC）をこのイベントがトリガーとして使用するかどうか。IOC の詳細については、侵害の兆候について（45-22 ページ）を参照してください。

NetBIOS Domain

セッションで使用された NetBIOS ドメイン。

NetFlow Destination/Source Autonomous System

NetFlow 対応デバイスによってエクスポートされた接続の場合、接続のトラフィックの送信元または宛先に対する、Border Gateway Protocol の自律システム番号。

NetFlow Destination/Source Prefix

NetFlow 対応デバイスによってエクスポートされた接続の場合、送信元または宛先の IP アドレスに、送信元と宛先のプレフィクス マスクが追加されたもの。

NetFlow Destination/Source TOS

NetFlow 対応デバイスによってエクスポートされた接続の場合、接続トラフィックが NetFlow 対応デバイスに入ったか、NetFlow 対応デバイスから出たときの Type of Service（TOS）バイトの設定。

NetFlow SNMP Input/Output

NetFlow 対応デバイスによってエクスポートされた接続の場合、接続トラフィックが NetFlow 対応デバイスに入ったか、NetFlow 対応デバイスから出た際のインターフェイスのインターフェイス インデックス。

Network Analysis Policy

イベントの生成に関連付けられているネットワーク分析ポリシー（NAP）（ある場合）。

Reason

次の場合に接続がロギングされた 1 つまたは複数の原因。

- [User Bypass] は、システムが最初はユーザの HTTP 要求をブロックしたが、ユーザが警告ページでクリック操作をして、最初に要求していたサイトへ進むことを選択したことを示します。[User Bypass] の原因は必ず [Allow] のアクションとペアになります。
- [IP Block] は、システムがセキュリティ インテリジェンス データに基づいて、インスペクションなしで接続を拒否したことを示します。[IP Block] の原因は必ず [Block] のアクションとペアになります。
- [IP Monitor] は、システムがセキュリティ インテリジェンス データに基づいて接続を拒否するはずでしたが、ユーザが接続を拒否せず監視するように設定したことを示します。
- [File Monitor] は、システムが接続において特定のファイルの種類を検出したことを示します。

- [File Block] は、ファイルまたはマルウェア ファイルが接続に含まれており、システムがその送信を防いだことを示します。[File Block] の理由は必ず [Block] のアクションとペアになります。
- [File Custom Detection] は、カスタム検出リストにあるファイルが接続に含まれており、システムがその送信を防いだことを示します。
- [File Resume Allow] は、ファイル送信がはじめにファイル ブロックまたはマルウェア ブロック ファイル ルールによってブロックされたことを示します。そのファイルを許可する新しいアクセス コントロール ポリシーが適用された後で、HTTP セッションは自動的に再開しました。この原因は、インライン構成のみで表示されることに注意してください。
- [File Resume Block] は、ファイル送信がはじめにファイル検出または マルウェア クラウド ルックアップ ファイル ルールによって許可されたことを示します。そのファイルをブロックする新しいアクセス コントロール ポリシーが適用された後で、HTTP セッションは自動的に停止しました。この原因は、インライン構成のみで表示されることに注意してください。
- [SSL Block] は、システムが SSL インスペクション設定に基づいて、暗号化接続をブロックしたことを示します。[SSL Block] の原因は必ず [Block] のアクションとペアになります。
- [Intrusion Block] は、接続で検出されたエクスプロイト（侵入ポリシー違反）をシステムがブロックしたか、ブロックするはずだったことを示します。[Intrusion Block] の原因は、ブロックされたエクスプロイトの場合は [Block]、ブロックされるはずだったエクスプロイトの場合は [Allow] のアクションとペアになります。
- [Intrusion Monitor] は、接続で検出されたエクスプロイトをシステムが検出したものの、ブロックしなかったことを示します。これは、トリガーされた侵入ルールの状態が [Generate Events] に設定されている場合に発生します。

Referenced Host

接続のプロトコルが DNS、HTTP、または HTTPS の場合、このフィールドにはそれぞれのプロトコルが使用していたホスト名が表示されます。

セキュリティ コンテキスト

トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。システムがこのフィールドにデータを設定するのは、マルチコンテキスト モードの ASA FirePOWER デバイスだけです。

Security Intelligence Category

接続でブラックリストに記載された IP アドレスを表すか、もしくはそれを含む、ブラックリストに記載されたオブジェクトの名前。セキュリティ インテリジェンスのカテゴリは、ネットワーク オブジェクトまたはグループ、グローバル ブラックリスト、カスタム セキュリティ インテリジェンスのリストまたはフィード、またはインテリジェンス フィードのカテゴリのいずれかの名前にすることができます。[Reason] が [IP Block] または [IP Monitor] の場合にのみ、このフィールドに値が入力されることに注意してください。セキュリティ インテリジェンス イベントのビューでは、エントリに必ず原因が表示されます。詳細については、セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録（13-1 ページ）を参照してください。

また、DC500 Defense Centerおよび シリーズ 2 デバイスはどちらもこの機能をサポートしていないことに注意してください。

Source Device

接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。管理対象デバイスによって接続が検出された場合、このフィールドには `FireSIGHT` の値が入ります。

Source Port/ICMP Type or Destination Port/ICMP Code

セッションの開始側またはセッションの応答側で使用されるポート、ICMP タイプ、または ICMP コード。

SSL Status

暗号化された接続を記録した、SSL ルールに関連したアクション、デフォルト アクション、または復号化不能トラフィック アクション:

- 「Block」および [Block with reset] は、ブロックされた暗号化接続を表します。
- [Decrypt (Resign)] は、再署名サーバ証明書を使用して復号化された発信接続を表します。
- [Decrypt (Replace Key)] は、置き換えられた公開キーと自己署名サーバ証明書を使用して復号化された発信接続を表します。
- [Decrypt (Known Key)] は、既知の秘密キーを使用して復号化された着信接続を表します。
- [Do not Decrypt] は、システムが復号化していない接続を表します。

システムが暗号化接続を復号化できなかった場合は、実行された復号化不能のトラフィック アクションと失敗の原因が表示されます。たとえば、不明な暗号スイートによって暗号化されたトラフィックをシステムが検出し、それ以上のインスペクションをせずにこれを許可した場合、このフィールドには [Do Not Decrypt (Unknown Cipher Suite)] が表示されます。

証明書の詳細を表示するには、ロック アイコン( )をクリックします。詳細については、暗号化接続に関連付けられた証明書の表示（39-33 ページ）を参照してください。

SSL Certificate Status

暗号化されたトラフィックが SSL ルールと一致する場合、このフィールドにはサーバ証明書のステータスが表示されます。復号化できないトラフィックが SSL ルールと一致する場合、このフィールドには [Not Checked] と表示されます。詳細については、証明書ステータスによる暗号化トラフィックの制御（22-25 ページ）を参照してください。

SSL Flow Error

エラーが SSL セッション中に発生した場合はエラー名および 16 進数コード。エラーが発生しない場合は [Success]。

SSL Version

接続の暗号化に使用された SSL または TLS プロトコル バージョン。

SSL Cipher Suite

接続の暗号化に使用された暗号スイート。

SSL Policy

接続を処理した SSL ポリシー。

SSL Rule

接続を処理した SSL ルールまたはデフォルト アクションと、その接続に一致した最初の Monitor ルール。接続が Monitor ルールに一致した場合、Defense Centerは接続を処理したルールの名前を表示し、その後に Monitor ルール名を表示します。

SSL セッション ID

SSL ハンドシェイク時にクライアントとサーバ間でネゴシエートされた16 進数セッション ID。

SSL Ticket ID

SSL ハンドシェイク時に送信されたセッション チケット情報の 16 進数のハッシュ値。

SSL Flow Flags

暗号化された接続の最初の 10 個のデバッグ レベル フラグ。すべてのフラグを表示するには、省略記号をクリックします(...)。

SSL Flow Messages

SSL ハンドシェイク時にクライアントとサーバ間で交換されたメッセージ。詳細については、http://tools.ietf.org/html/rfc5246 を参照してください。

TCP Flags

接続で検出された TCP フラグ。

Time

システムが接続を接続サマリーに集約するために使用した 5 分間隔の終了時刻。

URL, URL Category, and URL Reputation

セッション中に監視対象のホストによって要求された URLと、関連付けられたカテゴリおよびレピュテーション(利用できる場合)。

システムが SSL アプリケーションを識別またはブロックする場合、要求された URL は暗号化トラフィック内にあるため、システムは、SSL 証明書に基づいてトラフィックを識別します。したがって SSL アプリケーションの場合、このフィールドは証明書に含まれる一般名を表示します。

DC500 Defense Centerおよび シリーズ 2 デバイスはどちらも、URL カテゴリとレピュテーション データをサポートしていないことに注意してください。

ユーザ エージェント

接続で検出された HTTP トラフィックから取得したユーザ エージェント アプリケーションの情報。

Web アプリケーション

接続で検出された HTTP トラフィックの内容または要求された URL を表す Web アプリケーション。

Web アプリケーションがイベントの URL に一致しない場合、そのトラフィックは通常、参照先のトラフィックです(アドバタイズメントのトラフィックなど)。システムは、参照先のトラフィックを検出すると、参照元のアプリケーションを保存し(可能な場合)、そのアプリケーションを Web アプリケーションとして表示します。

HTTP トラフィックに含まれる特定の Web アプリケーションをシステムが特定できなかった場合、このフィールドには [Web Browsing] と表示されます。

接続およびセキュリティ インテリジェンスのイベントで利用可能な情報

ライセンス: 機能によって異なる

サポートされるデバイス: 機能によって異なる

サポートされる防御センター: 機能によって異なる

個別の接続、接続サマリー、セキュリティ インテリジェンス イベントについての利用可能な情報は、複数の要因によって異なります。

アプライアンス モデルおよびライセンス

アクセス コントロール ポリシーおよび SSL ポリシーが正常に処理できる任意の接続をログに記録できます。ただし、多くの機能では、ターゲット デバイスで特定のライセンス付与対象の機能を有効化する必要があり、多くの機能は一部のモデルでのみ使用可能です。

たとえば、SSL インスペクションには シリーズ 3 デバイスが必要です。他のアプライアンス モデルは暗号化されたトラフィックを検査できません。記録された接続イベントには暗号化された接続に関する情報は含まれていません。別の例として、DC500 を使用して接続イベントの位置情報データを表示できます。詳細については、接続ロギングのライセンスおよびモデル要件（38-10 ページ）を参照してください。

トラフィックの特性

システムは、ネットワーク トラフィック内に存在する（および検出可能な）情報だけを報告します。たとえば、イニシエータ ホストに関連付けられているユーザがいない、またはプロトコルが DNS、HTTP、または HTTPS ではない接続で検出される参照先ホストがいない可能性があります。

検出方法：FireSIGHT システム または NetFlow

TCP フラグ、NetFlow 自律システム、プレフィクス、および TOS データを除いて、NetFlow レコードで利用可能な情報は、管理対象デバイスを使用したネットワーク トラフィックの監視によって生成される情報よりも限定的です。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

ロギング方法：接続の開始または終了

システムが接続を検出するとき、その接続の開始または終了（またはその両方）をログに記録できるかどうかは、システムがその接続をどのように検出して処理するように設定されているかによって異なります。接続の開始または終了のロギング（38-4 ページ）を参照してください。

接続開始イベントは、セッション期間にわたってトラフィックを調査して判別する必要がある情報を持っていません（送信されたデータの合計量や、接続の最終パケットのタイムスタンプなど）。また、接続開始イベントがセッションのアプリケーションや URL トラフィックに関する情報を持っている保証はなく、セッションの暗号化に関する詳細も含まれていません。

インスペクション方法：関連付けられている SSL ポリシー、ファイル ポリシーおよび侵入ポリシー

SSL ポリシーによって処理された暗号化接続のみが、接続ログで SSL 関連の情報を持っています。ファイル ポリシーに関連付けられたアクセス コントロール ルールによってロギングされた接続にのみ、ファイル情報が含まれます。同様に、接続ログで侵入情報を参照するには、侵入ポリシーをアクセス コントロール ルールもしくはデフォルト アクションと関連付ける必要があります。

接続イベント タイプ:個々またはサマリー

接続サマリーには、集約された接続に関連付けられたすべての情報が含まれているのではありません。たとえば、接続サマリーに接続を集約する際にクライアント情報は使用されないため、サマリーにクライアント情報は含まれません。

接続グラフは、接続終了ログのみを使用する接続サマリーのデータに基づいていることに注意してください。接続開始データだけをロギングした場合、接続グラフと接続サマリーのイベント ビューにはデータが含まれていません。

その他の設定

アクセス コントロール ポリシーの詳細設定では、HTTP セッションの監視対象ホストによって要求された URL ごとにシステムが接続ログに保存する文字数を制御できます。この設定を使用して URL のロギングを無効化する場合、システムは接続ログで個々の URL を表示しませんが、カテゴリとレピュテーション データは参照できます(存在する場合)。

また、すべての接続イベントに [Reason] があるわけではありません。これは、Interactive Block の設定をユーザがバイパスした場合など、特定の状況でのみ値が入力されるフィールドです。Reason(39-8 ページ)を参照してください。

次の表は、接続イベントおよびセキュリティ インテリジェンス イベントの各フィールドとともに、検出方法、ロギング方法、接続イベント タイプによってシステムがそのフィールドに情報を表示するかどうかを示します。セキュリティ インテリジェンス イベントは集約されないため、[Summary] カラムは接続イベントのサマリーについてのみ示されることに注意してください。

ヒント　接続イベントとセキュリティ インテリジェンス イベントの両方のテーブル ビューでは、各アプリケーション タイプの [Category] および [Tag] フィールド、NetFlow 関連のフィールド、SSL 関連のフィールドなど、いくつかのフィールドがデフォルトで非表示になっています。イベント ビューに非表示フィールドを表示するには、検索条件を拡大し、[Disabled Columns] の下のフィールド名をクリックします。

表 39-1　ロギングおよび検出方法に基づいた接続およびセキュリティ インテリジェンスのデータ

	検出方法:		ロギング方法:		接続イベント:	
フィールド	FireSIGHT	NetFlow	開始	終了	シングル	概要
時刻	yes	yes	no	yes	no	yes
First Packet	yes	yes	yes	yes	yes	no
Last Packet	yes	yes	no	yes	yes	no
Action	yes	no	yes	yes	yes	no
理由	yes	no	yes	yes	yes	no
Initiator IP	yes	yes	yes	yes	yes	yes
Initiator Country	yes	no	yes	yes	yes	yes
Initiator User	yes	yes	yes	yes	yes	yes
Responder IP	yes	yes	yes	yes	yes	yes
Responder Country	yes	no	yes	yes	yes	yes
Security Intelligence Category	yes	no	yes	yes	yes	no
Ingress Security Zone	yes	no	yes	yes	yes	yes
Egress Security Zone	yes	no	yes	yes	yes	yes

表 39-1　ロギングおよび検出方法に基づいた接続およびセキュリティ インテリジェンスのデータ(続き)

	検出方法:		ロギング方法:		接続イベント:	
フィールド	FireSIGHT	NetFlow	開始	終了	シングル	概要
Source Port/ICMP Code	yes	yes	yes	yes	yes	no
Destination Port/ICMP Type	yes	yes	yes	yes	yes	yes
SSL Status	yes	no	no	yes	yes	no
SSL Certificate Status	yes	no	no	yes	yes	no
SSL Version	yes	no	no	yes	yes	no
SSL Policy	yes	no	no	yes	yes	no
SSL Rule	yes	no	no	yes	yes	no
SSL Cipher Suite	yes	no	no	yes	yes	no
SSL Flow Flags	yes	no	no	yes	yes	no
SSL Flow Messages	yes	no	no	yes	yes	no
アプリケーション プロトコル	yes	yes	利用可能な場合	yes	yes	yes
クライアント	yes	no	利用可能な場合	yes	yes	no
Client Version	yes	no	利用可能な場合	yes	yes	no
Web アプリケーション	yes	no	利用可能な場合	yes	yes	no
Category, Tag (Application Protocol, Client, Web Application)	yes	no	利用可能な場合	yes	yes	no
Application Risk	yes	no	利用可能な場合	yes	yes	no
Business Relevance	yes	no	利用可能な場合	yes	yes	no
URL	yes	no	利用可能な場合	yes	yes	no
URL カテゴリ	yes	no	利用可能な場合	yes	yes	no
URL Reputation	yes	no	利用可能な場合	yes	yes	no
VLAN ID	yes	no	yes	yes	yes	no
Referenced Host	yes	no	no	yes	yes	no
ユーザ エージェント	yes	no	no	yes	yes	no
HTTP Referrer	yes	no	no	yes	yes	no
IOC	yes	no	yes	yes	yes	no
Intrusion Events	yes	no	no	yes	yes	no
ファイル	yes	no	no	yes	yes	no
侵入ポリシー	yes	no	yes	yes	yes	no

表 39-1　ロギングおよび検出方法に基づいた接続およびセキュリティ インテリジェンスのデータ（続き）

	検出方法:		ロギング方法:		接続イベント:	
フィールド	FireSIGHT	NetFlow	開始	終了	シングル	概要
Access Control Policy	yes	no	yes	yes	yes	no
Access Control Rule	yes	no	yes	yes	yes	no
Network Analysis Policy	yes	no	yes	yes	yes	no
デバイス	yes	yes	yes	yes	yes	yes
Ingress Interface	yes	no	yes	yes	yes	yes
Egress Interface	yes	no	yes	yes	yes	yes
Security Context（ASA のみ）	yes	no	yes	yes	yes	yes
TCP Flags	no	yes	no	yes	yes	no
NetFlow Destination/Source Autonomous System	no	yes	no	yes	yes	no
NetFlow Destination/Source Prefix	no	yes	no	yes	yes	no
NetFlow Destination/Source TOS	no	yes	no	yes	yes	no
NetFlow SNMP Input/Output	no	yes	no	yes	yes	no
Source Device	yes	yes	FireSIGHT	yes	yes	yes
NetBIOS Domain	yes	no	yes	yes	yes	no
Initiator Packets	yes	yes	有用でない	yes	yes	yes
Responder Packets	yes	yes	有用でない	yes	yes	yes
Initiator Bytes	yes	yes	有用でない	yes	yes	yes
Responder Bytes	yes	yes	有用でない	yes	yes	yes
Connections	yes	yes	no	yes	no	yes
Count	yes	yes	yes	yes	yes	no

接続およびセキュリティ インテリジェンスのデータの表示

ライセンス: 機能によって異なる

サポートされるデバイス: 機能によって異なる

サポートされる防御センター: 機能によって異なる

接続データの詳細な情報を取得するために、システムは接続データをグラフおよび表形式で表示できます。接続データにアクセスしたときに表示されるページは、使用するワークフローによって異なります。定義済みのワークフローのいずれかを使用するか、特定の要件に合致した情報のみを表示するカスタム ワークフローを作成することができます。

セキュリティ インテリジェンス イベントは Protectionライセンスを必要とし、表形式でのみ表示されます。セキュリティ インテリジェンスのデータは シリーズ 2 管理対象デバイスまたは DC500 Defense Center ではサポートされません。セキュリティ インテリジェンス イベントからデータ グラフは作成できません。ただし、対応する接続イベントはグラフ形式で表示できます。

セキュリティ インテリジェンス データのインタラクティブなグラフ表示を行うには、コンテキスト エクスプローラの [Security Intelligence] セクションを参照します。詳細については、「[Security Intelligence] セクションについて（56-17 ページ）」を参照してください。

注　個々の接続またはセキュリティ インテリジェンス イベントで利用可能な情報は、ライセンスやアプライアンス モデルなど、いくつかの要因によって異なります。詳細については、接続ロギングのライセンスおよびモデル要件（38-10 ページ）を参照してください。

各テーブル ビューまたはグラフには、表示している接続または接続サマリーについて、タイムスタンプ、IP アドレス、アプリケーションなどの情報が含まれています。FireSIGHT システムによって検出された個別の接続について利用可能な情報は、検出方法やロギング オプションなどの複数の要因によって異なります。詳細については、接続およびセキュリティ インテリジェンスのデータ フィールドについて（39-4 ページ）および接続およびセキュリティ インテリジェンスのイベントで利用可能な情報（39-12 ページ）を参照してください。

ヒント　[Connection Summary] ダッシュボードは、システムによってロギングされた接続の概要ビューを表示します。[Summary Dashboard] は、セキュリティ インテリジェンス イベントのデータを表示します。詳細については、ダッシュボードの使用（55-1 ページ）を参照してください。

接続またはセキュリティ インテリジェンスのデータを表示するには、次の手順を実行します。

アクセス： Admin/Any Security Analyst

ステップ 1　次の 2 つのオプションから選択できます。

- 接続イベントを表示するには、[Analysis] > [Connections] > [Events] を選択します。
- セキュリティ インテリジェンス イベントを表示するには、[Analysis] > [Connections] > [Security Intelligence Events] を選択します。

デフォルトの接続またはセキュリティ インテリジェンスのワークフローの最初のページが表示されます。接続イベントの場合は 2 通りの可能性があります。

- ワークフローのページに**グラフ**が表示される。実行できるアクションについては、接続グラフの使用（39-17 ページ）を参照してください。
- ワークフローのページに**表**が表示される。実行できるアクションについては、接続およびセキュリティ インテリジェンスのデータ テーブルの使用（39-29 ページ）を参照してください。

セキュリティ インテリジェンス イベントの場合、ワークフローのページには**表**が表示されます。

カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。イベントが表示されない場合、時間範囲を調整する必要がある場合があります。イベント時間の制約の設定（58-26 ページ）を参照してください。

接続グラフの使用

ライセンス： すべて

システムが接続データを表示する方法の 1 つがグラフです。折れ線グラフ、棒グラフ、円グラフという、3 つの接続グラフがあります。棒グラフおよび折れ線グラフは複数のデータセットを表示できます。つまり、各 X 軸データ ポイントに対し、Y 軸に複数の値を表示できます。

次のようにさまざまな方法で接続グラフを操作できます。

- グラフに表示するデータのタイプを変更する
- グラフ タイプを切り替える
- グラフを制約して、特定の時間範囲、ホスト、アプリケーション、ポート、デバイスのデータを表示します

トラフィック プロファイルは接続データに基づいているため（トラフィック プロファイルの作成（53-1 ページ）を参照）、トラフィック プロファイルは折れ線グラフとして表示できます。その他の接続グラフと同様にこれらのグラフを操作できますが、いくつかの制限があります。

セキュリティ インテリジェンス イベントからデータ グラフは作成できません。ただし、対応する接続イベントはグラフ形式で表示できます。セキュリティ インテリジェンス データのインタラクティブなグラフ表示を行うには、コンテキスト エクスプローラの [Security Intelligence] セクションを参照します。詳細については、「[Security Intelligence] セクションについて（56-17 ページ）」を参照してください。

注　トラフィック プロファイルを表示するには、Administrator アクセス権が必須です。任意の Security Analyst または Administrator アクセス権で表示できるその他の接続グラフと比較してみてください。

接続およびセキュリティ インテリジェンスのデータの表示（39-15 ページ）で説明したように接続グラフを表示する場合、次の表で説明する基本的な操作を実行できます。

アクセス： Admin/Any Security Analyst

表 39-2　基本的な接続グラフ機能

目的	操作
表示されたデータについて調べる	詳細については、接続およびセキュリティ インテリジェンスのデータ フィールドについて（39-4 ページ）を参照してください。
日付と時刻の範囲を変更する	詳細については、イベント時間の制約の設定（58-26 ページ）を参照してください。
ホストのプロファイルを表示する	発信側または応答側別に接続データを表示するグラフで、棒グラフの棒か円グラフの扇形をクリックし、[View Host Profile] を選択します。
カスタム ワークフローなどの別のワークフローを使用する	ワークフローのタイトルの横の [(switch workflow)] をクリックします。
現在のワークフローのページ間を移動する	詳細については、ワークフローのページの使用（58-21 ページ）を参照してください。
関連付けられたイベントを表示するために、ほかのイベント ビューに移動する	ワークフロー間のナビゲート（58-40 ページ）で詳細を参照してください。

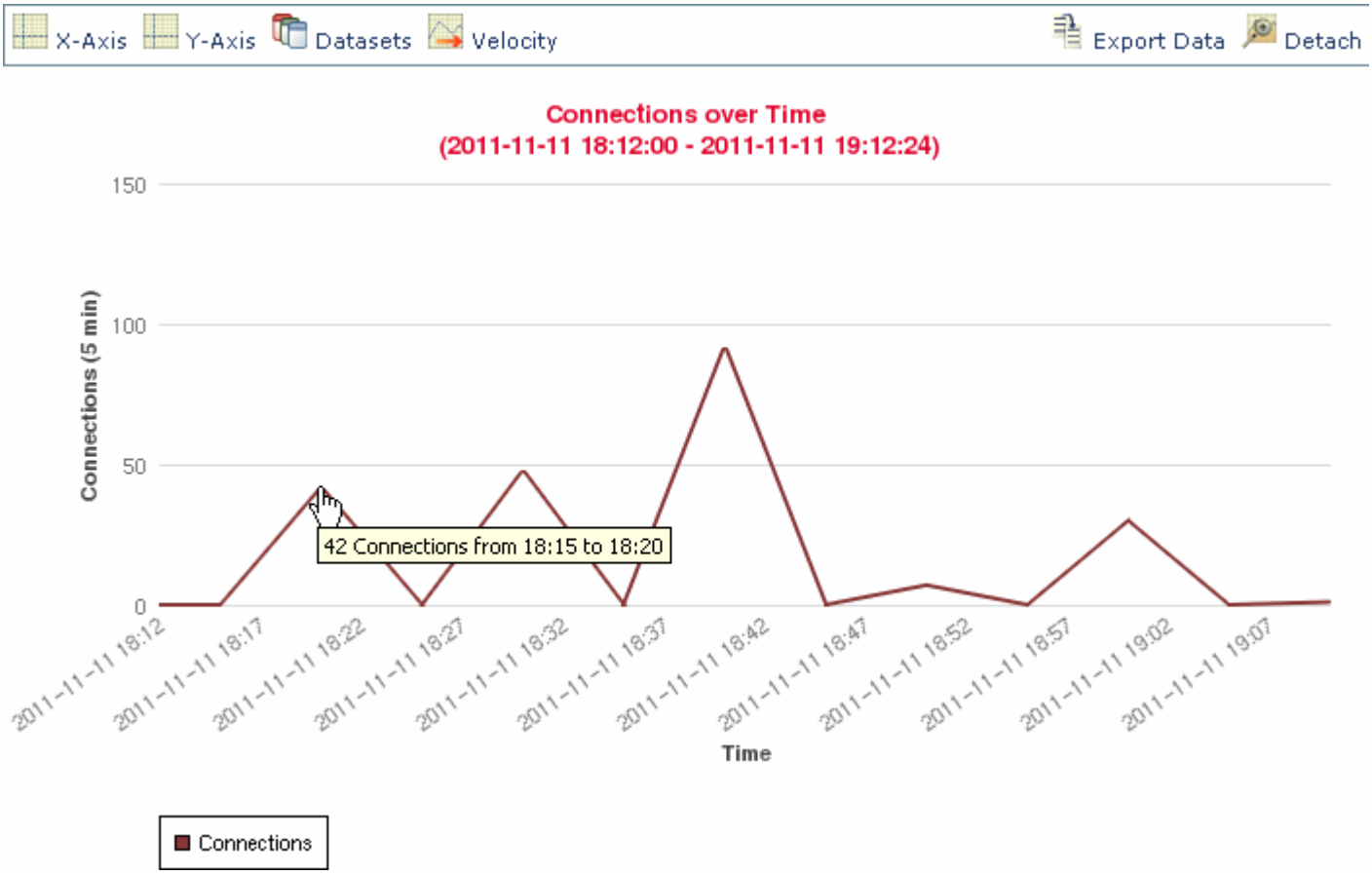
接続データの詳細な分析をする際に接続グラフを操作する方法は、ほかにも多数あります。詳細については、以下を参照してください。

- グラフ タイプの変更（39-18 ページ）では、棒グラフと円グラフ、標準折れ線グラフと速度グラフの切り替え方法について説明しています。
- データシートの選択（39-22 ページ）では、折れ線グラフおよび棒グラフの各 X 軸データ ポイントに対し、Y 軸に複数の値を表示する方法について説明しています。
- 集約された接続データに関する情報の表示（39-24 ページ）では、グラフ上のデータ ポイントに関する詳細情報を得る方法や、統計情報がグラフ化されているホストのプロファイルを表示する方法を説明しています。
- ワークロー ページでの接続グラフの操作（39-25 ページ）では、ワークフローを次のページへ進めずに、接続グラフに表示されるデータを制約する方法について説明しています。
- 接続データ グラフのドリルダウン（39-25 ページ）では、ワークフローを次のページへ進めて、接続グラフに表示されるデータを制約する方法について説明しています。
- 折れ線グラフのズームと再センタリング（39-26 ページ）では、折れ線グラフを任意の時点を中心に再センタリングする方法について説明します。
- グラフのデータを選択する（39-27 ページ）では、X 軸または Y 軸を変更することによって、接続グラフに表示されるデータを変更する方法について説明しています。
- 接続グラフの分離（39-28 ページ）では、接続グラフを新しいブラウザ ウィンドウに分離し、Defense Centerのデフォルトの時間範囲に影響を与えることなく詳細な分析を実行する方法について説明します。
- 接続データのエクスポート（39-29 ページ）では、グラフの作成に使用された接続データをコンマ区切り値（CSV）ファイルとしてエクスポートする方法について説明しています。

グラフ タイプの変更

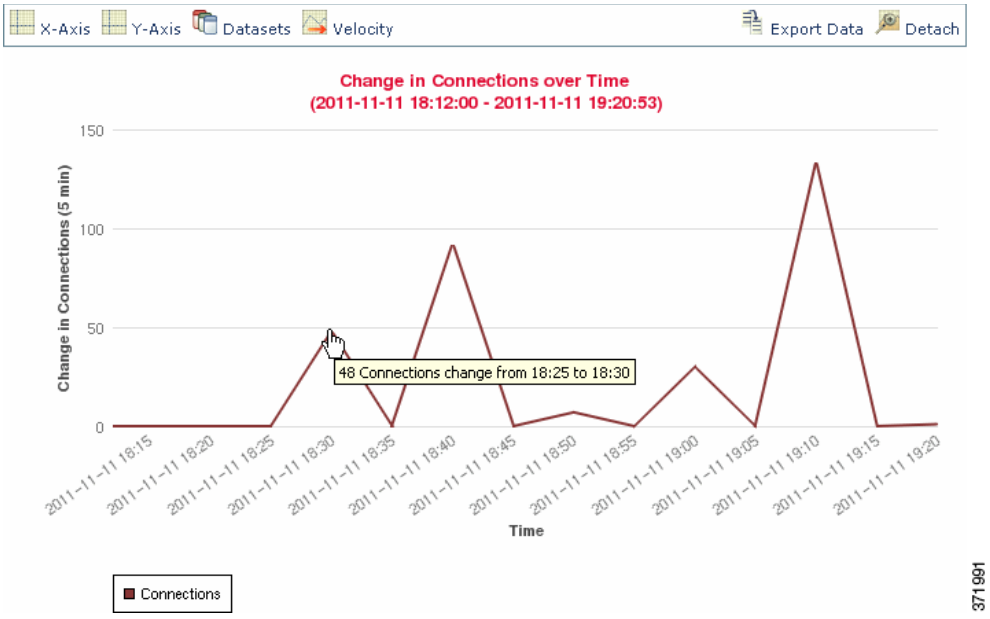
ライセンス： すべて

折れ線グラフ、棒グラフ、円グラフという、3 つのタイプの接続グラフがあります。*折れ線グラフ*はある期間のデータをプロットします。たとえば次の折れ線グラフには、1 時間の時間枠において監視対象ネットワークで検出された合計接続数が表示されます。トラフィック プロファイルは常に折れ線グラフとして表示されます。

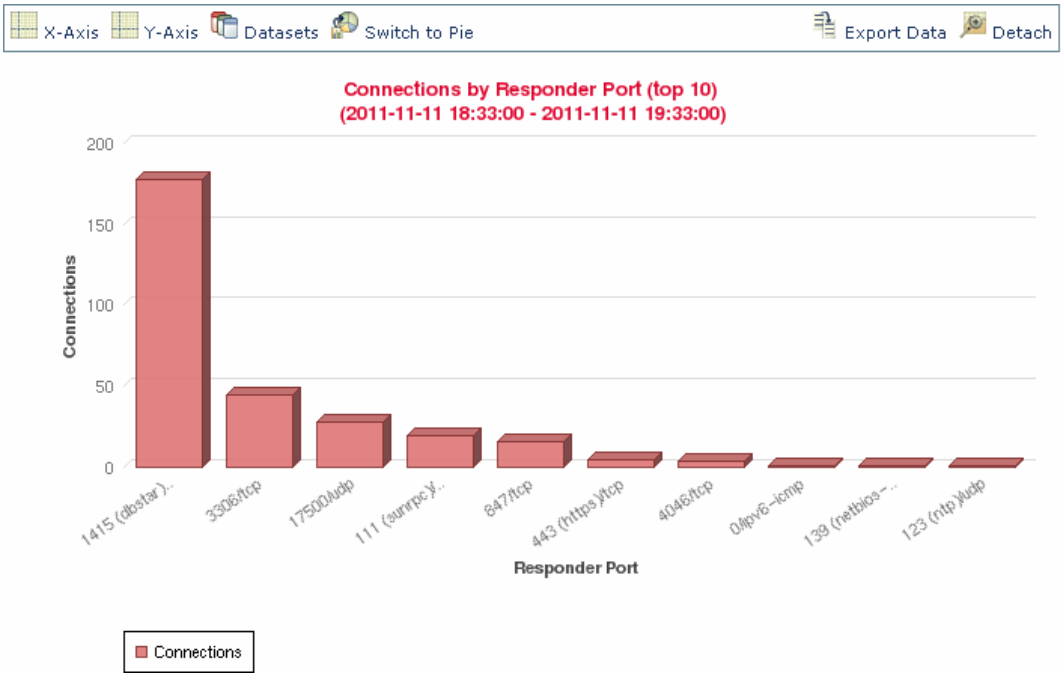


デフォルトでは、折れ線グラフは*標準ビュー*で表示されます。標準の折れ線グラフでは、5 分間隔でデータを集約し、集約したデータ ポイントをプロットし、そのポイントを接続します。

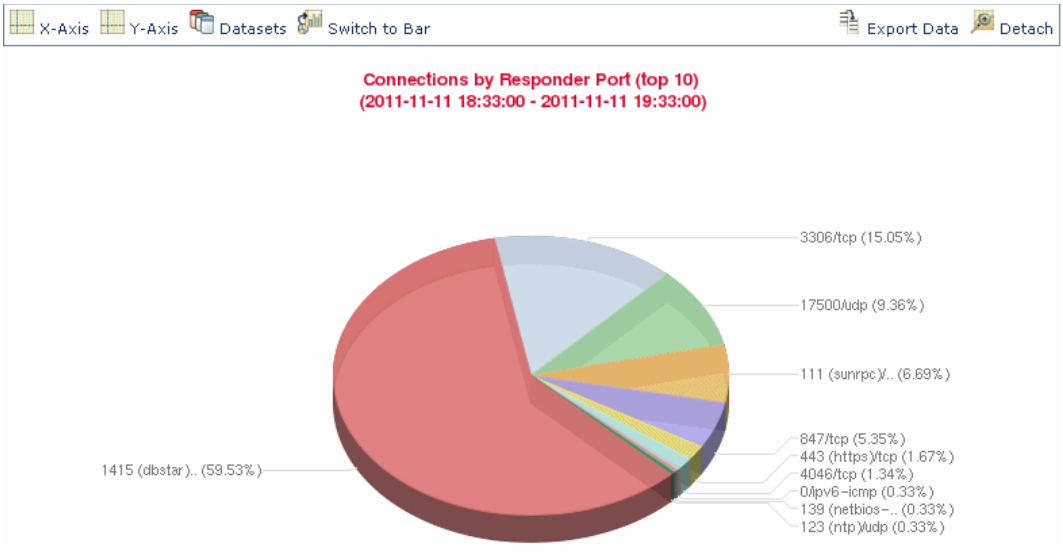
一方で、折れ線グラフは標準ビューから*速度ビュー*に変更できます。速度折れ線グラフでは、これらのデータ ポイント間の変化率を示します。上のグラフを速度グラフに変更すると、Y 軸は接続数の表示から、ある期間の接続数の変化の表示へと変わります。



*棒グラフ*は個別のカテゴリにグループ化されたデータを表示します。たとえば棒グラフは、1 時間の時間枠において最もアクティブだった 10 のポートについて、監視対象ネットワークで検出された接続数を表示できます。



*円グラフ*も棒グラフと同様に、個別のカテゴリにグループ化されたデータを表示します。次の円グラフは、前述の棒グラフと同じ情報を表示しています。



標準と速度の折れ線グラフの切り替え、棒グラフと円グラフの切り替えをするには、次の表の手順に従います。

アクセス: Admin/Any Security Analyst

表 39-3　　グラフ タイプの変更

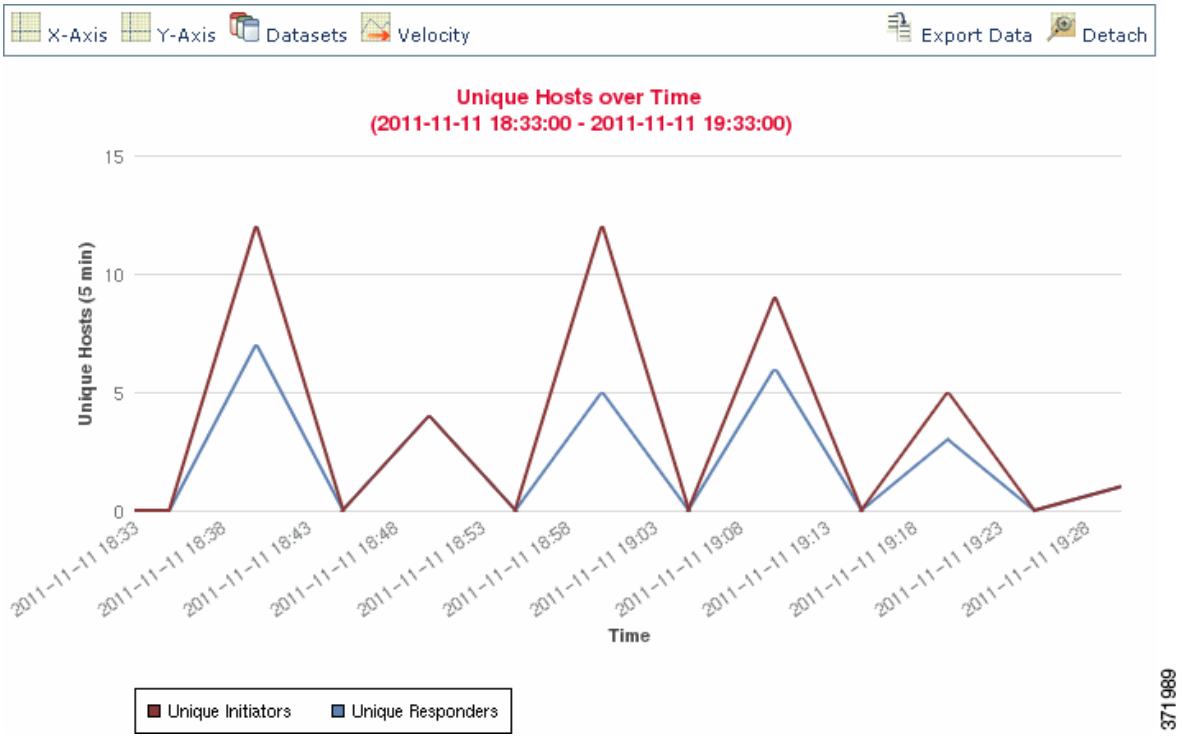
変更内容	操作
棒グラフから円グラフへ	[Switch to Pie] をクリックします。 円グラフには複数のデータセットを表示できないことに注意してください。データシートの選択 (39-22 ページ)を参照してください。
円グラフから棒グラフへ	[Switch to Bar] をクリックします。
折れ線グラフを標準グラフから速度グラフへ	[Velocity] をクリックし、[Velocity] を選択します。
折れ線グラフを速度グラフから標準グラフへ	[Velocity] をクリックし、[Standard] を選択します。

データシートの選択

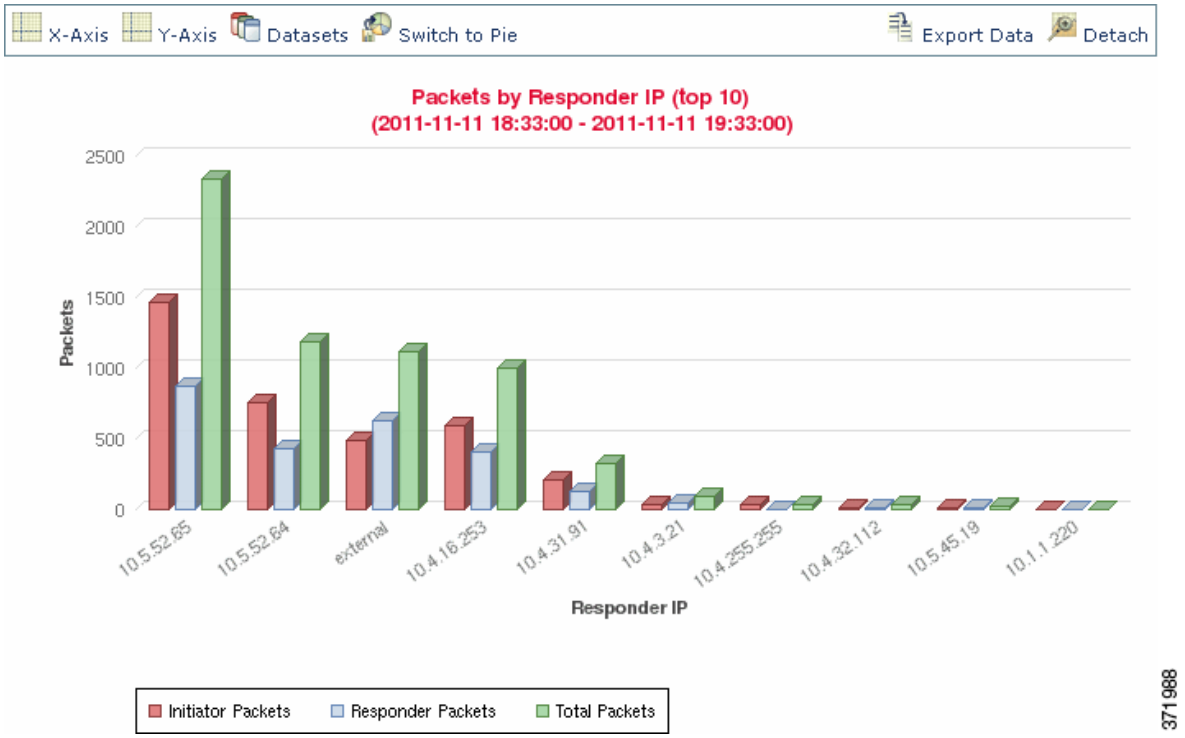
ライセンス：すべて

棒グラフおよび折れ線グラフはどちらも複数のデータセットを表示できます。つまり、各 X 軸データ ポイントに対し、Y 軸に複数の値を表示できます。たとえば、一意な発信側の合計数を表示し、一意な円グラフの合計数にはデータセットを 1 つだけ表示できます。

折れ線グラフでは、複数のデータセットは複数の線として、それぞれ異なる色で表示されます。たとえば次のグラフは、監視対象ネットワークにおいて 1 時間間隔の 1 回で検出された一意な発信側の合計数と一意な応答側の合計数を表示しています。



棒グラフでは、複数のデータセットが X 軸データ ポイントごとに色分けされた棒として表示されます。たとえば次の棒グラフは、監視対象ネットワーク上で送信されたパケットの合計数と、発信側によって送信されたパケット数、応答側によって送信されたパケット数を表示しています。



円グラフには複数のデータセットを表示**できません**。複数のデータセットを持つ棒グラフから円グラフに切り替えた場合、円グラフは自動的に選択された 1 つのデータセットだけを表示します。表示するデータセットを選択する際、Defense Centerは、発信側と応答側の統計情報よりも全体の統計情報を優先し、応答側の統計情報よりも発信側の統計情報を優先します。次の表では、接続グラフの X 軸に表示できるデータセットについて説明します。

表 39-4　　データセットのオプション

Y 軸の表示内容	選択可能なデータセット
Connections	デフォルトの、監視対象ネットワークで検出された接続数のみ（[Connections]） これは、トラフィック プロファイル グラフの唯一のオプションです。
KBytes	以下の組み合わせ • 監視対象ネットワーク上で送信された合計キロバイト数（[Total KBytes]） • 監視対象ネットワーク上でホスト IP アドレスから送信されたキロバイト数（[Initiator KBytes]） • 監視対象ネットワーク上でホスト IP アドレスによって受信されたキロバイト数（[Responder KBytes]）
KBytes Per Second	デフォルトの、監視対象ネットワークで 1 秒あたりに送信された合計キロバイト数のみ（[Total KBytes Per Second]）

表 39-4　データセットのオプション（続き）

Y 軸の表示内容	選択可能なデータセット
Packets	以下の組み合わせ • 監視対象ネットワーク上で送信された合計パケット数（[Total Packets]） • 監視対象ネットワーク上でホスト IP アドレスから送信されたパケット数（[Initiator Packets]） • 監視対象ネットワーク上でホスト IP アドレスによって受信されたパケット数（[Responder Packets]）
Unique Hosts	以下の組み合わせ • 監視対象ネットワーク上の一意なセッション開始側の数（[Unique Initiators]） • 監視対象ネットワーク上の一意なセッション応答側の数（[Unique Responders]）
Unique Application Protocols	デフォルトの、監視対象ネットワーク上の一意なアプリケーション プロトコル数のみ（[Unique Application Protocols]）
Unique Users	デフォルトの、監視対象ネットワーク上のセッション開始側にログインした一意なユーザ数のみ（[Unique Initiator Users]）

接続グラフに表示するデータセットを選択するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

ステップ 1　[Datasets] をクリックし、グラフに表示するデータセットを選択します。

選択できるデータセットについては、データセットのオプションの表で説明しています。

集約された接続データに関する情報の表示

ライセンス：すべて

接続グラフは 5 分間隔で集約したデータに基づいており、*接続サマリー*とも呼ばれます。接続グラフの作成に使用された特定の接続サマリーについて、詳細情報を入手することができます。たとえば、ある期間の接続のグラフで、ある間隔に検出された正確な接続数を把握したい場合があります。

集約された接続データの詳細を取得するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

ステップ 1　折れ線グラフの点、棒グラフの棒、もしくは円グラフの扇形の上にカーソルを置きます。グラフのその部分の作成に使用されたデータの詳細がツールチップに表示されます。

ワークロー ページでの接続グラフの操作

ライセンス: すべて

接続データのワークフローを開くと、データは最初は時間範囲のみによって制約されます。ワークフローを次のページへ進めることなく、追加条件で接続グラフを制約できます。

ヒント このように接続データを制約すると、グラフの X 軸（円グラフの表示時には独立変数とも呼びます）が変わります。接続データを制約せずに独立変数を変更するには、[X-Axis] および [Y-Axis] メニューを使用します。詳細については、グラフのデータを選択する（39-27 ページ）を参照してください。

接続データを制約するには、次の手順を実行します。

アクセス: Admin/Any Security Analyst

ステップ 1 折れ線グラフの点、棒グラフの棒、または円グラフの扇形をクリックします。

ステップ 2 [View by...] オプションを選択します。

X 軸の機能の表に表示された条件のいずれかに基づいて接続データを制約できます。

たとえば、ある期間の接続のグラフについて考えてみましょう。グラフ上の点をポートによって制約すると、検出された接続イベント数に基づいて、最もアクティブだった 10 のポートを示す棒グラフが表示されますが、クリックした点を中心とする 10 分間の時間枠によって制約されます。

棒の 1 つをクリックし、[View by Initiator IP] を選択してグラフをさらに制約すると、それまでと同じ 10 分間の時間枠だけでなく、クリックした棒が表すポートでも制約された新しい棒グラフが表示されます。

注 分離したグラフを使用している場合を除いて、このように接続データを制約すると、時間範囲が変わります。分離したグラフの詳細については、接続グラフの分離（39-28 ページ）を参照してください。

接続データ グラフのドリルダウン

ライセンス: すべて

接続データのワークフローを開くと、データは最初は時間範囲のみによって制約されます。ワークフローを次のページへ進めて接続グラフを制約できます。

接続データのワークフローでドリルダウンするには、次の手順を実行します。

アクセス: Admin/Any Security Analyst

ステップ 1 折れ線グラフの点、棒グラフの棒、または円グラフの扇形をクリックします。

ステップ 2 [Drill-down] を選択します。

次のワークフロー ページにドリルダウンし、クリックした項目を使用して制約します。

- 折れ線グラフで点をクリックすることで、次のページの時間枠は、クリックした点を中心とする 10 分間に制約されます。
- 棒グラフの棒または円グラフの扇形をクリックすると、その棒または扇形が表す条件に基づいて次のページが制約されます。たとえば、ポート使用を表す棒をクリックすると、ワークフローの次のページへドリルダウンします。これは、クリックした棒が表すポートによって制約されています。

折れ線グラフのズームと再センタリング

ライセンス： すべて

折れ線グラフを任意の時点を中心に再センタリングできます。デフォルトの時間範囲を使用して再センタリングするか、別の時間範囲を選択することができます。

注　分離したグラフを使用している場合を除いて、再センタリングするとデフォルトの時間範囲が変わります。分離したグラフの詳細については、接続グラフの分離（39-28 ページ）を参照してください。

デフォルトの時間範囲を使用して再センタリングするには、次の手順を実行します。

アクセス： Admin/Any Security Analyst

ステップ 1　折れ線グラフ上で、グラフの再センタリングの中心にしたい点をクリックし、[recenter] をクリックします。

クリックした点を中心とする、デフォルトの時間範囲と同じ長さの時間枠のグラフが再描画されます。

別の時間範囲を使用して再センタリングするには、次の手順を実行します。

アクセス： Admin/Any Security Analyst

ステップ 1　グラフの再センタリングの中心にしたい点をクリックし、[Zoom] をクリックします。

ステップ 2　新しいグラフに時間範囲を選択します。最短は 1 時間、最長は 1 週間です。

クリックした点を中心とする、選択した時間枠のグラフが再描画されます。

グラフのデータを選択する

ライセンス: すべて

X 軸または Y 軸、もしくは両方を変更することによって、接続グラフにさまざまなデータを表示できます。

円グラフでは、X 軸を変更すると独立変数が変わり、Y 軸を変更すると従属変数を変わることに注意してください。たとえば、ポートごとのキロバイト数を表示する円グラフについて考えてみましょう。この場合、X 軸は **Responder Port**、Y 軸は **KBytes** です。この円グラフは、ある間隔に監視対象ネットワークで送信されたデータの合計キロバイト数を表します。円の中の扇形は、各ポートで検出されたデータの比率を表します。グラフの X 軸を **Application Protocol** に変更すると、引き続き円グラフは送信データの合計キロバイト数を表しますが、円の中の扇形は検出された各アプリケーション プロトコルの送信データの比率を表します。

しかし、はじめの円グラフの Y 軸を **Packets** に変更すると、円グラフはある間隔に監視対象ネットワークで送信された合計パケット数を表し、円の中の扇形は各ポートで検出された合計パケット数を表します。

接続グラフの X 軸を変更するには、次の表の手順に従います。

表 39-5　　X 軸の機能

接続データのグラフ化方法	操作
監視対象ネットワークで最もアクティブだった 10 のアプリケーション プロトコル別に、検出済みの接続イベント数に基づいてグラフ化	[X-Axis] をクリックし、[Application Protocol] を選択します。
監視対象ネットワークで最もアクティブだった 10 の管理対象デバイス別に、検出済みの接続イベント数に基づいてグラフ化	[X-Axis] をクリックし、[Device] を選択します。
監視対象ネットワークで最もアクティブだった 10 のホスト IP アドレス別に、そのホスト IP アドレスが接続トランザクションを開始した接続イベント数に基づいてグラフ化	[X-Axis] をクリックし、[Initiator IP] を選択します。
監視対象ネットワークで最もアクティブだった 10 のユーザ別に、ユーザがログインしたホストが接続トランザクションを開始した接続イベント数に基づいてグラフ化	[X-Axis] をクリックし、[Initiator User] を選択します。
監視対象ネットワークで最もアクティブだった 10 のホスト IP アドレス別に、そのアドレスが接続トランザクションの応答側となっていた接続イベント数に基づいてグラフ化	[X-Axis] をクリックし、[Responder IP] を選択します。
監視対象ネットワークで最もアクティブだった 10 のポート別に、ホストが接続トランザクションの応答側となっていた検出済みの接続イベント数に基づいてグラフ化	[X-Axis] をクリックし、[Responder Port] を選択します。
最もアクティブだった 10 の送信元デバイス（接続の接続データをエクスポートした NetFlow 対応デバイスを含む）と、FireSIGHT という名前の送信元デバイス別に、Cisco の管理対象デバイスによって検出されたすべての接続についてグラフ化	[X-Axis] をクリックし、[Source Device] を選択します。
時間経過	[X-Axis] をクリックし、[Time] を選択します。

接続グラフの Y 軸を変更するには、次の表の手順に従います。

表 39-6　　Y 軸の機能

目的	操作
X 軸に選択した条件によって、監視対象ネットワークの接続数をグラフ化	[Y-Axis] をクリックし、[Connections] を選択します。
X 軸に選択した条件によって、監視対象ネットワークで送信された合計キロバイト数をグラフ化	[Y-Axis] をクリックし、[KBytes] を選択します。
X 軸に選択した条件によって、監視対象ネットワークで 1 秒あたりに送信された合計キロバイト数をグラフ化	[Y-Axis] をクリックし、[KBytes Per Second] を選択します。
X 軸に選択した条件によって、監視対象ネットワークで送信された合計パケット数をグラフ化	[Y-Axis] をクリックし、[Packets] を選択します。
X 軸に選択した条件によって、監視対象ネットワークで検出された一意なホスト数の合計をグラフ化	[Y-Axis] をクリックし、[Unique Hosts] を選択します。
X 軸に選択した条件によって、監視対象ネットワークで検出された一意なアプリケーション プロトコル数の合計をグラフ化	[Y-Axis] をクリックし、[Unique Application Protocols] を選択します。
X 軸に選択した条件によって、監視対象ネットワークで検出された一意なユーザ数の合計をグラフ化	[Y-Axis] をクリックし、[Unique Users] を選択します。

接続グラフの分離

ライセンス： すべて

デフォルトの時間範囲に影響を与えることなく接続グラフの詳細な分析をしたい場合、グラフを新しいブラウザ ウィンドウに分離することができます。組み込みの接続グラフでできる操作と同じことが、分離した接続グラフでも、すべてできます。[Print] をクリックすれば、分離したグラフを印刷することもできます。トラフィック プロファイル グラフはデフォルトで分離したグラフであることに注意してください。

ヒント　分離したグラフを表示している場合、[New Window] をクリックすると、分離したグラフの別のコピーを新しいブラウザ ウィンドウで作成できます。分離した各グラフ上で、別々の分析ができるようになります。

グラフを分離するには、次に手順を実行します。

アクセス： Admin/Any Security Analyst

ステップ 1　[Detach] をクリックします。

接続データのエクスポート

ライセンス： すべて

接続データをコンマ区切り値（CSV）ファイルとしてエクスポートすることで、ほかの人と容易に共有できます。

ヒント　また、グラフを右クリックし、ブラウザのプロンプトに従うことで、接続グラフの画像を保存できます。

接続データをエクスポートするには、次の手順を実行します。

アクセス： Admin/Any Security Analyst

ステップ 1　[Export Data] をクリックします。

ポップアップ ウィンドウが表示され、グラフのデータのテーブル ビューが示されます。

ステップ 2　[Download CSV File] をクリックし、ファイルを保存します。

接続およびセキュリティ インテリジェンスのデータ テーブルの使用

ライセンス： 機能によって異なる

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

FireSIGHT システムのイベント ビューアでは、接続データを表に表示できます。また、分析に関連する情報に応じてイベント ビューを操作できます。セキュリティ インテリジェンス イベントを表示すると、特定のセキュリティ インテリジェンスのレピュテーションがある接続に注目できます。（セキュリティ インテリジェンスは Protection ライセンスを必要とし、シリーズ 2 の管理対象デバイスおよび DC 500 Defense Centerではサポートされていません。）接続データにアクセスしたときに表示されるページはワークフローによって異なります。ワークフローとは、広範なビューから集中的なビューに移動することでイベントを評価するために使用できる一連のページです。

注　個々の接続またはセキュリティ インテリジェンス イベントで利用可能な情報は、ライセンスやアプライアンス モデルなど、いくつかの要因によって異なります。詳細については、接続ロギングのライセンスおよびモデル要件（38-10 ページ）を参照してください。

システムによって提供される*接続イベント*および*セキュリティ インテリジェンス イベント*のワークフローは、接続と検出されたアプリケーションの基本情報の概要を表示します。これを使用して、イベントのテーブル ビューにドリルダウンできます。また、特定の要件に合致した情報だけを表示するカスタム ワークフローを作成できます。

イベント ビューアを使用して、次のことができます。

- イベントを検索、ソート、制約、また表示するイベントの時間範囲を変更する
- 表示されるカラムを指定する（テーブル ビューのみ）
- IP アドレスに関連付けられたホスト プロファイル、またはユーザ ID に関連付けられたユーザの詳細とホスト履歴を表示する
- 接続で検出されたファイル（マルウェア ファイルを含む）と侵入を表示する
- IP アドレスに関連付けられた地理情報を表示する
- 接続イベントの URL のフル テキストを表示する
- セッションの暗号化に使用された証明書に関する情報を表示する
- 暗号化セッションの詳細を表示する
- 同じワークフロー内の異なるワークフローのページを使用してイベントを表示する
- 別のワークフローを一緒に使用してイベントを表示する
- 特定の値に制約して、ワークフロー内のページからページへドリルダウンする
- 現在のページと制約をブックマークして、後で同じデータに戻れるようにする（データがまだ存在している前提）
- 現在の制約を使用してレポート テンプレートを作成する
- データベースからイベントを削除する
- IP アドレスのコンテキスト メニューを使用して、ホワイトリストまたはブラックリストに記載、もしくは接続に関連付けられたホストまたは IP アドレスに関するその他の情報を取得する

ドリルダウン ページで接続イベントを制約する場合、同一のイベントからのパケット数とバイト数が合計されることに注意してください。ただし、カスタム ワークフローを使用しており、ドリルダウン ページに [Count] カラムを追加していない場合、イベントは個別に表示され、パケット数とバイト数は合計されません。

システムが生成した接続イベントが 25 個を超えると、[Connection Events] テーブル ビューに、使用可能なイベントのページ数ではなく、「1 of Many」と表示されます。

次の項には、接続およびセキュリティ インテリジェンスのイベント テーブルの表示および分析についての情報が含まれています。

- ワークフローの概要と使用（58-1 ページ）では、イベント ビューアの使用手順を詳しく説明しています。
- 地理情報の使用（58-23 ページ）では、接続およびセキュリティ インテリジェンスのイベントに関連付けられた地理情報を表示および解釈する方法について説明しています。
- イベント ビュー設定の設定（71-3 ページ）では、接続およびセキュリティ インテリジェンスのイベントのデータを表示するデフォルトのワークフローを変更する方法について説明しています。
- 接続およびセキュリティ インテリジェンスのデータ フィールドについて（39-4 ページ）および接続およびセキュリティ インテリジェンスのイベントで利用可能な情報（39-12 ページ）では、接続およびセキュリティ インテリジェンスのイベントのデータに関する詳細を提供しています。
- Monitor ルールに関連付けられたイベントの使用（39-31 ページ）では、Monitor ルールの条件を使用して接続イベントを制約する方法について説明しています。
- 接続で検出されたファイルの表示（39-32 ページ）では、接続で検出またはブロックされたファイル（マルウェア ファイルを含む）を表示する方法について説明しています。

- 接続に関連付けられた侵入イベントの表示（39-33 ページ）では、接続に関連付けられた侵入イベントを表示する方法について説明しています。
- 暗号化接続に関連付けられた証明書の表示（39-33 ページ）では、接続の暗号化に使用された証明書に関する詳細を表示する方法について説明しています。

Monitor ルールに関連付けられたイベントの使用

ライセンス： すべて

ロギングされた接続をイベント ビューアを使用して表示する場合、Defense Centerは各接続を処理したアクセス コントロール ルールまたはデフォルト アクションとともに、各接続に一致する Monitor ルールを 8 つまで表示します。

接続が 1 つの Monitor ルールに一致した場合、Defense Centerは接続を処理したルールの名前を表示し、その後に Monitor ルール名を表示します。接続が複数の Monitor ルールに一致したときは、イベント ビューアは一致した Monitor ルールの数を `Default Action + 2 Monitor Rules` などと表示します。

一致した Monitor ルールを使用し、以下のいずれかを使用して接続イベント ビューを制約できます。

- 接続を処理したアクセス コントロール ルールまたはデフォルト アクション
- 接続に一致した個々の Monitor ルール

接続イベントを Monitor ルールの一致を使用して制約するには、次の手順を実行します。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Connections] > [Events] を選択します。

デフォルトの接続データのワークフローの最初のページが表示されます。

ステップ 2　分析に使用するワークフローを表示します。使用しているドリルダウン ページまたはテーブル ビューに、[Access Control Rule] フィールドが表示されていることを確認します。

ステップ 3　イベントをどのように制約しますか。

- 接続を処理したアクセス コントロールまたはデフォルト アクションに制約するには、ルール名または [Default Action] をクリックします。
- ロギングされた接続に一致した Monitor ルールのみに制約するには、Monitor ルール名をクリックします。
- ロギングされた接続に一致した複数の Monitor ルールのうち 1 つに制約するには、[*N* Monitor Rules] の値をクリックします。たとえば、[2 Monitor Rules] をクリックします。

  その接続イベントの [Monitor Rules] ポップアップ ウィンドウが表示され、接続に一致した最初の 8 つの Monitor ルールが示されます。接続イベントの制約に使用する Monitor ルール名をクリックします。

イベントが制約されます。ドリルダウン ページを使用している場合、イベント ビューがワークフローの次のページに進みます。

接続で検出されたファイルの表示

ライセンス： ProtectionまたはMalware

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

1 つまたは複数のアクセス コントロール ルールにファイル ポリシーを関連付けると、システムは一致するトラフィックのファイル(マルウェアを含む)を検出できます。これらのルールによってロギングされた接続に関連付けられたファイル イベントがある場合は、イベント ビューアを使用して確認できます。

ファイル リストの代わりに、Defense Centerはファイル表示アイコン( )を [Files] カラムに表示します。アイコンの数字は、その接続で検出またはブロックされたファイル数(マルウェア ファイルを含む)を示します。アイコンをクリックしても、次のワークフロー ページにドリルダウンされたり、接続イベントが制約されたりすることはありません。代わりにポップアップ ウィンドウが表示され、接続で検出されたファイルのリストとともに、そのタイプと、該当する場合はマルウェア処理が示されます。

ポップアップ ウィンドウで、クリック操作によって次のことができます。

- ファイル表示アイコン( )をクリックして、ファイル イベントのテーブル ビューで詳細を表示
- マルウェア ファイル表示アイコン( )をクリックして、マルウェア イベントのテーブル ビューで詳細を表示
- ファイル軌跡アイコン( )をクリックして、ネットワークを介したファイル送信をトレース
- [View File Events] または [View Malware Events] で、接続で検出されたファイルまたはネットワークベースのマルウェア イベントのすべての詳細を表示

ヒント 1 つまたは複数の接続に関連付けられたファイルまたはマルウェア イベントをすばやく表示するには、イベント ビューアでチェック ボックスを使用して接続を選択し、[Jump to] ドロップダウン リストから [Malware Events] または [File Events] を選択します。同様に、ファイルの送信に使用された接続も表示できます。詳細については、ワークフロー間のナビゲート (58-40 ページ)を参照してください。

関連付けられたイベントを表示する際、Defense Centerはそのイベント タイプのデフォルトのワークフローを使用します。ファイルおよびマルウェア イベントの詳細については、ファイル イベントの操作(40-8 ページ)およびマルウェア イベントの操作(40-17 ページ)を参照してください。ネットワーク ファイル トラジェクトリ機能の使用の詳細については、ネットワーク ファイル トラジェクトリの操作(40-37 ページ)を参照してください。

次のように、すべてのファイルおよびマルウェア イベントが接続に関連付けられてはいないことに注意してください。

- エンドポイントベースのマルウェア イベントは、接続に関連付けられていません。これらのイベントは、ネットワーク トラフィックをインスペクションするシステムではなく、FireAMP コネクタによって生成されます。
- IMAP に対応した電子メール クライアントの多くは単一 IMAP セッションを使用し、それはユーザがアプリケーションを終了したときに終了します。長時間接続はシステムによってロギングされますが(長時間接続(39-4 ページ)を参照)、セッションでダウンロードされたファイルは、そのセッションが終了するまで接続に関連付けられません。

また、シリーズ 2 および Cisco NGIPS for Blue Coat X-Series デバイスと DC500 Defense Center はどちらもネットワークベースの高度なマルウェア防御をサポートしていないことに注意してください。

接続に関連付けられた侵入イベントの表示

ライセンス：Protection

アクセス コントロール ルールまたはデフォルト アクションに侵入ポリシーを関連付けると、システムは一致するトラフィックのエクスプロイトを検出できます。ロギングされた接続に関連付けられた侵入イベントがある場合は、イベント ビューアを使用して確認できます。

イベント リストの代わりに、Defense Centerは 侵入イベント表示アイコン（）を [Intrusion Events] カラムに表示します。アイコンをクリックしても、次のワークフロー ページにドリルダウンされたり、接続イベントが制約されたりすることはありません。代わりにポップアップ ウィンドウが表示され、接続に関連付けられた侵入イベントのリストとともに、優先度と影響度が示されます。

ポップアップ ウィンドウで、一覧表示されたイベントの表示アイコン（）をクリックして、パケットのビューで詳細を表示できます。また、[View Intrusion Events] をクリックして、接続に関連付けられた侵入イベントすべての詳細を表示できます。

ヒント　1 つまたは複数の接続に関連付けられた侵入イベントをすばやく表示するには、イベント ビューアでチェック ボックスを使用して接続を選択し、[Jump to] ドロップダウン リストから [Intrusion Events] を選択します。同様に、侵入イベントに関連付けられた接続も表示できます。詳細については、ワークフロー間のナビゲート（58-40 ページ）を参照してください。

関連付けられたイベントを表示する際、Defense Centerはデフォルトの侵入イベント ワークフローを使用します。侵入イベントの詳細については、侵入イベントの操作（41-1 ページ）を参照してください。

暗号化接続に関連付けられた証明書の表示

ライセンス：すべて

SSL インスペクションを設定すると、暗号化接続をロギングできます。トラフィックでシステムが機能し、かつ証明書が利用可能な場合は、イベント ビューアを使用して、接続の暗号化に使用された公開キー証明書の詳細を表示できます。

証明書自体の代わりに、Defense Center ロック アイコン（）を [SSL Status] カラムに表示します。アイコンをクリックすると、ポップアップ ウィンドウが表示され、次の表で説明されている証明書の詳細が示されます。

表 39-7　暗号化接続の証明書の詳細

属性	説明
Subject/Issuer Common Name	証明書のサブジェクトまたは証明書発行元のホストおよびドメイン名。
Subject/Issuer Organization	証明書のサブジェクトまたは証明書発行元の組織。
Subject/Issuer Organization Unit	証明書のサブジェクトまたは証明書発行元の組織ユニット。

表 39-7　暗号化接続の証明書の詳細（続き）

属性	説明
Not Valid Before/After	証明書の有効期間。
Serial Number	発行元 CA によって割り当てられたシリアル番号。
Certificate Fingerprint	証明書の認証に使用する SHA ハッシュ値。
Public Key Fingerprint	証明書に含まれる公開キーの認証に使用する SHA ハッシュ値。

見出しをダブル クリックして、ポップアップ ウィンドウ内のセクションの展開または折りたたみができます。

暗号化トラフィックでシステムが機能していたけれども証明書が利用できない場合は、ロック アイコンがグレー表示されることに注意してください。たとえば、SSL ハンドシェイク エラーが含まれていてシステムが復号化できなかった接続をシステムがブロックした場合、システムには暗号化証明書の詳細がなく、その接続のロック アイコンはグレー表示されます。

接続およびセキュリティ インテリジェンスのデータの検索

ライセンス： すべて

Defense Center の [Search] ページを使用して、特定の接続イベント、セキュリティ インテリジェンス イベント、または接続サマリーを検索し、その結果をイベント ビューアーで表示できます。また、後で再利用するために検索条件を保存できます。[Custom Analysis] ダッシュボード ウィジェット、レポート テンプレート、カスタム ユーザ ロールも、保存した検索を使用できます。

サンプルとしてシステムに付属している検索には、[Saved Searches] リストで（`Cisco`）というラベルが付いています。

接続グラフは接続サマリーに基づいているため、接続サマリーを制約しているのと同じ条件が接続グラフを制約します。アスタリスク（*）が付いているフィールドが、接続グラフと接続サマリーに加えて、個々の接続またはセキュリティ インテリジェンス イベントを制約しています。

無効な検索条件を使用して接続サマリーを検索し、カスタム ワークフローの接続サマリー ページを使用して結果を見る場合、無効な条件には適用不可（N/A）としてラベルが付けられ、次の図に示すように取り消し線が引かれます。

検索結果は検索対象イベントで使用可能なデータに依存することにも注意してください。つまり、使用可能なデータによっては、検索条件が適用されないことがあります。各接続データ フィールドでデータを使用できる状況については接続およびセキュリティ インテリジェンスのイベントで利用可能な情報（39-12 ページ）を参照してください。

一般的な検索構文

それぞれの検索フィールドの隣には、使用できる構文の例が表示されます。検索条件を入力する場合、次の点に注意してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「`A`」または「`B`」または「`C, D, E`」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク（*）を使用できます。
- そのフィールドで情報を利用できないイベントを特定するには、フィールドに `n/a` を指定します。そのフィールドに値が入力されているイベントを特定するには、`!n/a` を使用します。
- 特定のデバイス、およびグループ、スタック、またはクラスタ内のデバイスを検索するには、デバイス フィールドを使用します。検索での FireSIGHT システムによるデバイス フィールドの処理方法については、検索でのデバイスの指定（60-7 ページ）を参照してください。
- オブジェクトを検索条件として使用するには、検索フィールドの隣にあるオブジェクトの追加アイコン（ ＋ ）をクリックします。

検索でのオブジェクトの使用など、検索構文の詳細については、イベントの検索（60-1 ページ）を参照してください。

接続およびセキュリティ インテリジェンスのデータ用の特別な検索構文

上記の一般的な検索構文に加えて、次のリストでは接続およびセキュリティ インテリジェンスのデータ用の特別な検索構文について説明しています。

接続に一致する Monitor ルール

個々の Monitor ルールに一致する接続を検索するには、[Access Control Rule] 条件を使用します。

Monitor ルールに一致するトラフィックは後で必ず別のルールかデフォルト アクションによって処理されるため、アクションが [Monitor] の接続は検索できません。Monitor ルールの名前を検索すると、後で接続を処理したルールやデフォルト アクションに関係なく、その Monitor ルールに一致したすべての接続が返されます。

数値を使用した条件（[Bytes]、[Packets]、[Connections]）

数字の前に、大なり（>）、以上（>=）、小なり（<）、以下（<=）、等しい（=）を付けられます。

ヒント [Connections] 条件を使用した検索で意味のある結果を表示するには、接続サマリー ページを持つカスタム ワークフローを使用する必要があります。

接続に関連付けられたファイルまたは侵入イベント

接続に関連付けられたファイル、マルウェア、侵入イベントの検索に、接続やセキュリティ インテリジェンスのイベントの検索ページは使用できません。これらの関連付けられたイベントの表示の詳細については、接続で検出されたファイルの表示（39-32 ページ）および接続に関連付けられた侵入イベントの表示（39-33 ページ）を参照してください。

接続の開始ユーザまたは URL

システムは部分一致を実行します。つまり、アスタリスクを使用せずに、フィールドの内容の全部または一部を検索できます。

[The total Traffic (in bytes)] または [transport Protocol used in the connection]

接続テーブル ビューにプロトコルまたはトラフィックの制約があるかどうかを確認するには、検索条件を展開します。

特定のプロトコルを検索するには、名前を使用するか、http://www.iana.org/assignments/protocol-numbers に記載されたプロトコルの番号を指定します。

これらのカラムは、テーブル ビューには表示されません。

TCP Flags in a NetFlow connection

これらのフラグの、すべてではなく、*少なくとも* 1 つがある接続をすべて表示するには、コンマ区切り TCP フラグのリストを入力します。また、[Only] チェック ボックスを選択して、指定するフラグのいずれかを唯一の TCP フラグとして持つ接続を検索できます。

SSL Encryption applied to the connection

SSL 暗号化された接続または暗号化されていない接続を表示するには、`yes` または `no` を入力します。

このカラムは、セキュリティ インテリジェンス イベントまたは接続イベントのテーブル ビューには表示されません。

The SSL Status

システムがアクションを適用した、またはシステムが条件を検出した暗号化トラフィックを表示するには、[SSL Actual Action] および [SSL Failure Reason] にリストされた 1 つ以上キーワードを入力します。このフィールドには、[SSL Actual Action] の値 1 つと [SSL Failure Reason] の値 1 つを同時に含めることができます。

復号化が成功すると、セキュリティ インテリジェンスおよび接続イベントのテーブル ビューには、[SSL Status] カラムに [SSL Actual Action] の値が表示されます。システムがトラフィックの復号化に失敗すると、セキュリティ インテリジェンスおよび接続イベントのテーブル ビューには、[SSL Status] カラムに [SSL Actual Action] および [SSL Failure Reason] の両方の値が表示されます。

The SSL Actual Action taken

システムが指定したアクションを適用した暗号化されたトラフィックを表示するには、次のキーワードのいずれかを入力します。

- [Do not Decrypt] は、システムが復号化しなかった接続を表します。
- [Block] および [Block with reset] は、ブロックされた暗号化接続を表します。
- [Decrypt (Known Key)] は、既知の秘密キーを使用して復号化された着信接続を表します。
- [Decrypt (Replace Key)] は、置き換えられた公開キーと自己署名サーバ証明書を使用して復号化された発信接続を表します。
- [Decrypt (Resign)] は、再署名サーバ証明書を使用して復号化された発信接続を表します。

復号化が成功すると、セキュリティ インテリジェンスおよび接続イベントのテーブル ビューには、[SSL Status] カラムにこの値が表示されます。システムがトラフィックの復号化に失敗すると、セキュリティ インテリジェンスおよび接続イベントのテーブル ビューには、[SSL Status] カラムに [SSL Failure Reason] としてこの値が表示されます。

The SSL Expected Action

システムが指定された SSL ルールの通りに実際にプロセスを処理するように期待された暗号化されたトラフィックを表示するには、次のキーワードのいずれかを入力します。

- [Do not Decrypt] は、システムが復号化しなかった接続を表します。
- [Block] および [Block with reset] は、ブロックされた暗号化接続を表します。
- [Decrypt (Known Key)] は、既知の秘密キーを使用して復号化された着信接続を表します。
- [Decrypt (Replace Key)] は、置き換えられた公開キーと自己署名サーバ証明書を使用して復号化された発信接続を表します。
- [Decrypt (Resign)] は、再署名サーバ証明書を使用して復号化された発信接続を表します。

このカラムは、セキュリティ インテリジェンス イベントまたは接続イベントのテーブル ビューには表示されません。

The SSL Failure Reason

システムが指定された理由で復号化に失敗した暗号化トラフィックを表示するには、次のキーワードのいずれかを入力します。

- Unknown
- No Match
- Success
- Uncached Session
- Unknown Cipher Suite
- Unsupported Cipher Suite
- Unsupported SSL Version
- SSL Compression Used
- Session Undecryptable in Passive Mode
- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup
- Internal Error
- Network Parameters Unavailable

- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- Invalid Action

システムがトラフィックの復号化に失敗すると、セキュリティ インテリジェンスおよび接続イベントのテーブル ビューには、[SSL Status] カラムに [SSL Actual Action] としてこの値が表示されます。

The SSL Cipher Suite used

接続を暗号化するのに使用される暗号スイートを表すマクロ値を入力します。暗号スイート値の指定については、www.iana.org/assignments/tls-parameters/tls-parameters.xhtml を参照してください。

The SSL Subject Country

暗号化証明書のサブジェクト国に関連付けられている暗号化されたトラフィックを表示するには、2 文字の ISO 3166-1 アルファ 2 国番号を入力します。

このカラムは、セキュリティ インテリジェンス イベントまたは接続イベントのテーブル ビューには表示されません。

The SSL Issuer Country

暗号化証明書のサブジェクト国に関連付けられている暗号化されたトラフィックを表示するには、2 文字の ISO 3166-1 アルファ 2 国番号を入力します。

このカラムは、セキュリティ インテリジェンス イベントまたは接続イベントのテーブル ビューには表示されません。

SSL Certificate Fingerprint

証明書に関連付けられているトラフィックを表示するには、その証明書の認証に使用される SHA ハッシュ値を入力するか、または貼り付けます。

このカラムは、セキュリティ インテリジェンス イベントまたは接続イベントのテーブル ビューには表示されません。

SSL Public Key Fingerprint

証明書に関連付けられているトラフィックを表示するには、その証明書に含まれている公開キーの認証に使用される SHA ハッシュ値を入力するか、または貼り付けます。

このカラムは、セキュリティ インテリジェンス イベントまたは接続イベントのテーブル ビューには表示されません。

SSL Certificate Status

これは、認証ステータスのルール条件が設定されている場合にのみ適用されます。サーバ証明書のステータスに関連付けられている暗号化されたトラフィックを表示するには、以下に示す 1 つ以上のキーワードを入力します。暗号化されたトラフィックは、複数のサーバ証明書ステータス値に同時に一致する場合があります。

- Not Checked
- Self Signed
- Valid
- Invalid Signature
- Invalid Issuer
- Expired
- 不明(Unknown)
- Not Valid Yet
- Revoked

SSL Flow Messages

SSL ハンドシェイク時にクライアントとサーバ間で交換される次のメッセージに関連付けられている暗号化されたトラフィックを表示するには、次のキーワードのいずれかを入力します。

- HELLO_REQUEST
- CLIENT_ALERT
- SERVER_ALERT
- CLIENT_HELLO
- SERVER_HELLO
- SERVER_CERTIFICATE
- SERVER_KEY_EXCHANGE
- CERTIFICATE_REQUEST
- SERVER_HELLO_DONE
- CLIENT_CERTIFICATE
- CLIENT_KEY_EXCHANGE
- CERTIFICATE_VERIFY
- CLIENT_CHANGE_CIPHER_SPEC
- CLIENT_FINISHED
- SERVER_CHANGE_CIPHER_SPEC
- SERVER_FINISHED
- NEW_SESSION_TICKET
- HANDSHAKE_OTHER
- APP_DATA_FROM_CLIENT
- APP_DATA_FROM_SERVER

SSL Version

指定された SSL または TLS プロトコル バージョンに関連付けられている暗号化されたトラフィックを表示するには、次のキーワードのいずれかを入力します。

- 不明(Unknown)
- SSLv2.0
- SSLv3.0
- TLSv1.0

- TLSv1.1
- TSLv1.2

SSL Serial Number

発行元の CA によって公開キー証明書に割り当てられたシリアル番号を入力するか、または貼り付けます。

このカラムは、セキュリティ インテリジェンス イベントまたは接続イベントのテーブル ビューには表示されません。

接続またはセキュリティ インテリジェンスのデータを検索するには、次の手順を実行します。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　次の選択肢があります。

- 接続データを検索するには、テーブルのドロップダウンリストから [Connection Events] を選択します。
- セキュリティ インテリジェンスのデータを検索するには、テーブルのドロップダウンリストから [Security Intelligence Events] を選択します。

ページが適切な制約によって更新されます。

ステップ 3　該当するフィールドに検索条件を入力します。

- 接続およびセキュリティ インテリジェンスのイベント テーブルのフィールドの詳細については、接続およびセキュリティ インテリジェンスのデータ フィールドについて（39-4 ページ）を参照してください。
- 公開キー証明書に関連するフィールドの詳細については、暗号化接続に関連付けられた証明書の表示（39-33 ページ）を参照してください。
- 接続イベントおよびセキュリティ インテリジェンス イベントの特別な検索構文については、接続およびセキュリティ インテリジェンスのデータ用の特別な検索構文（39-35 ページ）を参照してください。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　カスタム ユーザ ロールに対するデータの制約として検索を使用する場合は、検索を非公開として保存する**必要があります**。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save as New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

検索結果は、現在の時刻範囲によって制限されるデフォルトの接続またはセキュリティ インテリジェンスのワークフローに表示されます。

接続サマリー ページの表示

ライセンス： すべて

[Connection Summary] ページは、監視対象ネットワーク上のアクティビティをさまざまな条件で整理したグラフを表示します。たとえば [Connections over Time] グラフでは、選択した間隔における監視対象ネットワーク上の接続の合計数が表示されます。

注　[Connection Summary] ページは、接続イベントの検索によって制限されたカスタム ロールを持ち、[Connection Summary] ページへの明示的なアクセスを許可されたユーザにのみ表示されます。詳細については、制限付きユーザ アクセス プロパティについて（61-59 ページ）およびカスタム ユーザ ロールの管理（61-55 ページ）を参照してください。

次の表では、[Connection Summary] ページで行うことができるさまざまな操作について説明します。

表 39-8　[Connection Summary] ページでの操作

目的	操作
[Connection Summary] ページの時刻と日付の範囲を変更	詳細については、イベント時間の制約の設定（58-26 ページ）を参照してください。
接続グラフを操作	詳細については、接続グラフの使用（39-17 ページ）を参照してください。
接続グラフをページから分離	分離したいグラフの [View] をクリックします。分離したグラフの詳細については、接続グラフの分離（39-28 ページ）を参照してください。

接続グラフでできる操作と同じことが、接続サマリーのグラフでも、ほぼすべてできます。ただし、[Connection Summary] ページのグラフは集約データに基づいているため、グラフの基になっている個々の接続イベントを調べることはできません。つまり、接続サマリーのグラフから接続データのテーブル ビューにドリルダウンすることはできません。

[Connection Summary] ページを表示するには、次の手順を実行します。

アクセス: Custom

ステップ 1　[Overview] > [Summary] > [Connection Summary] を選択します。

現在の時間範囲の [Connection Summary] ページがDefense Centerに表示されます。

ステップ 2　[Select Device] リストから、サマリーを表示したいデバイスを選択するか、もしくはすべてのデバイスのサマリーを表示するために [All] を選択します。

CHAPTER 40

マルウェアとファイル アクティビティの分析

Defense Centerは、システムのファイル インスペクション レコードを、キャプチャされたファイル、ファイル イベント、マルウェア イベントとしてログ記録します。

- *キャプチャされたファイル*は、システムでキャプチャされたファイルを表します。
- *ファイル イベント*は、システムがネットワーク トラフィック内で検出した(さらにオプションでブロックした)ファイルを表します。
- *マルウェア イベント*は、システムがネットワーク トラフィック内で検出した(さらにオプションでブロックした)マルウェア ファイルを表します。
- *遡及的マルウェア イベント*は、マルウェア ファイルの性質が変更されたファイルを表します。

システムがネットワーク トラフィックでのマルウェアの検出またはブロックに基づいてマルウェア イベントを生成する場合、ファイル イベントも生成します。ファイル内のマルウェアを検出するために、システムはまずファイル自体を検出する必要があるからです。FireAMP コネクタによって生成されたエンドポイント ベースのマルウェア イベント(FireAMP と FireSIGHT システムの統合(37-8 ページ) を参照)には、対応するファイル イベントがないことに注意してください。同様に、システムがネットワーク トラフィック内でファイルをキャプチャするとき、システムはまずファイルを検出するため、ファイル イベントも生成されます。

Defense Centerを使用すると、キャプチャされたファイル、ファイル イベント、およびマルウェア イベントを表示、操作、分析して、分析内容を他のユーザに送信できます。Context Explorer、ダッシュボード、イベント ビューアー、コンテキスト メニュー、ネットワーク ファイル トラジェクトリー マップ、およびレポート機能を使用することにより、検出、キャプチャ、ブロックされたファイルおよびマルウェアに関してより深く理解できるようになります。また、イベントを使用して相関ポリシー違反をトリガーしたり、電子メール、SMTP、または syslog によるアラートを発行したりすることもできます。

DC500 では Malware ライセンスを使用できず、シリーズ 2 デバイスまたは Cisco NGIPS for Blue Coat X-Series では Malware ライセンスを有効にすることもできません。このため、これらのアプライアンスを使用して、マルウェア クラウド ルックアップまたはアーカイブ ファイルの内容に関連するキャプチャされたファイル、ファイル イベント、およびマルウェア イベントを生成/分析することはできません。

詳細については、以下を参照してください。

- ファイル ストレージの操作(40-2 ページ)
- 動的分析の操作(40-5 ページ)
- ファイル イベントの操作(40-8 ページ)

- マルウェア イベントの操作（40-17 ページ）
- キャプチャ ファイルの操作（40-32 ページ）
- ネットワーク ファイル トラジェクトリの操作（40-37 ページ）

この章で説明するデータを生成する、マルウェア保護およびファイル制御アクションを実行するためのシステムの設定の詳細については、マルウェアと禁止されたファイルのブロッキング（37-1 ページ）を参照してください。

ファイル ストレージの操作

ライセンス： Malware

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

サポートされる防御センター： すべて（DC500 を除く）

ファイル ポリシーの設定に基づき、ファイル制御機能を使用して、ファイルの検出およびブロックを行えます。ただし、疑わしいホストまたはネットワークからのファイルや、ネットワーク上の監視対象ホストに送信された大量のファイルについては、さらに分析が必要になる場合があります。ファイル ストレージ機能を使用することにより、選択したファイル（トラフィックで検出された）をキャプチャして、それらをデバイスのハード ドライブかマルウェア ストレージ パック（インストールされている場合）に自動的に保存できます。

デバイスがトラフィックでファイルを検出すると、そのファイルをキャプチャできます。このようにして作成されたコピーは、動的分析のために、システムが保存したり送信したりできます。デバイスがファイルをキャプチャした後に、以下の選択肢があります。

- 後で分析するために、キャプチャしたファイルをデバイスのハード ドライブに保存する。詳細については、「キャプチャ ファイル ストレージについて（40-3 ページ）」を参照してください。
- さらに手動で分析したりアーカイブしたりするために、保存したファイルをローカル コンピュータにダウンロードする。詳細については、「保存されているファイルの別の場所へのダウンロード（40-4 ページ）」を参照してください。
- 動的分析のために、キャプチャしたファイルを Collective Security Intelligence クラウドに送信する。詳細については、「動的分析の操作（40-5 ページ）」を参照してください。

注意すべき点として、デバイスがファイルを保存した後は、以後それを検出しても、デバイスが引き続きそれを保存していれば、そのファイルを再度キャプチャすることはありません。

注　初めて検出されたファイルは、Defense Center によるクラウド ルックアップの完了後に性質が割り当てられます。システムはファイル イベントを生成しますが、ファイルに性質が即座に割り当てられなければ、ファイルを保存できません。

前に検出されていないファイルがブロック マルウェア アクション付きのファイル ルールと一致する場合、後続のクラウド ルックアップによって即座に性質が返されるので、システムはファイルを保存しイベントを生成できるようになります。

前に検出されていないファイルがマルウェア クラウド ルックアップ アクション付きのファイル ルールと一致する場合、システムはファイル イベントを生成しますが、クラウド ルックアップを実行し性質を返すのに追加の時間を要します。この遅延のため、システムはマルウェア クラウド ルックアップ アクション付きのファイル ルールに一致するファイルがネットワーク上に 2 回目に現れるまで保存することはできません。

システムがファイルをキャプチャするか保存するかに関わらず、以下が可能です。

- イベント ビューアーからのキャプチャされたファイルに関する情報（動的分析のためにファイルが保存されたのか送信されたかどうか、ファイルの性質、脅威スコアなど）を確認することにより、ネットワーク上で検出されたマルウェアの潜在的な脅威について迅速に検討する。詳細については、「キャプチャ ファイルの操作（40-32 ページ）」を参照してください。
- ファイルのトラジェクトリーを表示して、ネットワークのトラバースの仕方およびコピーを保持しているホストを判別する。詳細については、「ネットワーク ファイル トラジェクトリの分析（40-40 ページ）」を参照してください。
- 以後の検出時に、ファイルをクリーンまたはマルウェアな性質を持つものとして常に扱うように、ファイルをクリーン リストまたはカスタム検出リストに追加する。詳細については、「ファイル リストの操作（3-36 ページ）」を参照してください。

ファイル ポリシーでファイル ルールを設定して、特定のタイプまたは特定のファイル性質（使用できる場合）のファイルをキャプチャして保存します。ファイル ポリシーをアクセス コントロール ポリシーと関連付けて、それをデバイスに適用した後、トラフィック内の一致ファイルが検出され、保存されます。また、保存する最小ファイル サイズと最大ファイル サイズを制限できます。詳細については、ファイルおよびマルウェアのインスペクション パフォーマンスおよびストレージの調整（18-22 ページ）およびファイル ルールの操作（37-19 ページ）を参照してください。

ファイル ストレージには、デバイスに十分なディスク領域が必要です。デバイスのプライマリ ハード ドライブに十分な領域がなく、マルウェア ストレージ パックもインストールされていない場合、デバイスにファイルを保存できません。

注意　Ciscoから提供されたものではないハード ドライブをデバイスに取り付けないでください。サポートされていないハード ドライブを取り付けると、デバイスが破損する可能性があります。マルウェア ストレージ パック キットは、Ciscoから**のみ**購入でき、8000 シリーズ デバイスで**のみ**使用できます。マルウェア ストレージ パック のサポートが必要な場合は、サポートにお問い合わせください。詳細については、『*FireSIGHT System Malware Storage Pack Guide*』を参照してください。

DC500 で Malware ライセンスを使用したり、シリーズ 2 デバイスまたは Cisco NGIPS for Blue Coat X-Series で Malware ライセンスを有効にすることはできないので、それらのアプライアンスをファイルのキャプチャまたは保存に使用することはできないことに注意してください。

詳細については、以下を参照してください。

- キャプチャ ファイル ストレージについて（40-3 ページ）
- 保存されているファイルの別の場所へのダウンロード（40-4 ページ）

キャプチャ ファイル ストレージについて

ライセンス： Malware

サポートされるデバイス： 8000 シリーズ

ファイル ポリシー構成に基づいて、デバイスはハード ドライブにかなりの量のファイル データを保存することがあります。デバイスにマルウェア ストレージ パックを設置できます。システムがファイルをマルウェア ストレージ パックに保存することにより、イベントおよび設定ファイルを保存するために、プライマリ ハード ドライブにより多くスペースを確保できます。システムは定期的に古いファイルを削除します。

注意 Ciscoから提供されたものではないハード ドライブをデバイスに取り付けないでください。サポートされていないハード ドライブを取り付けると、デバイスが破損する可能性があります。マルウェア ストレージ パック キットは、Ciscoから**のみ**購入でき、8000 シリーズ デバイスで**のみ**使用できます。マルウェア ストレージ パック のサポートが必要な場合は、サポートにお問い合わせください。詳細については、『*FireSIGHT System Malware Storage Pack Guide*』を参照してください。

マルウェア ストレージ パックが設置されていない場合、ファイルを保存するようにデバイスを構成する際に、設定された量のプライマリ ハード ドライブのスペースだけがキャプチャ ファイル ストレージに割り当てられます。デバイスにマルウェア ストレージ パックを設置して、ファイルを保存するようにデバイスを構成すると、デバイスは代わりに、マルウェア ストレージ パック全体をキャプチャ ファイルを保存するために割り当てます。デバイスは、マルウェア ストレージ パックに他の情報を保存することはできません。

キャプチャ ファイル ストレージに割り当てられたスペースがいっぱいになると、システムは割り当てられたスペースがシステム定義しきい値に達するまで、保管されている古いファイルを削除します。保存されていたファイルの数によっては、システムがファイルを削除した後、ディスク使用率がかなり減る場合があります。

マルウェア ストレージ パックを設置する時点で、デバイスがすでにファイルを保存している場合、次にデバイスを再起動したときに、プライマリ ハード ドライブに保存されていたキャプチャ ファイルがすべて、マルウェア ストレージ パックに移動されます。それ以降デバイスが保存するファイルはすべて、マルウェア ストレージ パックに保存されます。デバイスのプライマリ ハード ドライブに使用可能な領域が十分でなく、マルウェア ストレージ パックも設置されていない場合、ファイルを保存することはできません。

保存したファイルは、システム バックアップ ファイルに含められないことに注意してください。詳細については、バックアップ ファイルの作成（70-2 ページ）を参照してください。

保存されているファイルの別の場所へのダウンロード

ライセンス： Malware

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

サポートされる防御センター： すべて（DC500 を除く）

デバイスがファイルを保存すると、Defense Centerがそのデバイスと通信でき、ファイルが削除されていない限り、そのファイルをダウンロードできます。手動でファイルを分析したり、長期保存や分析のためにローカル ホストにダウンロードしたりできます。関連ファイル イベント、マルウェア イベント、キャプチャ ファイル ビュー、またはファイルのトラジェクトリからファイルをダウンロードできます。詳細については、コンテキスト メニューの使用（2-5 ページ）およびサマリー情報（40-40 ページ）を参照してください。

マルウェアによる被害を防ぐため、デフォルトでは、ファイルのダウンロードのたびに確認を行う必要があります。ただし、ファイルのダウンロードのプロンプトで確認を無効にできます。確認を再度有効にするには、ファイルのプリファレンス（71-5 ページ）を参照してください。

注意 Ciscoは、有害な結果が発生することがあるため、マルウェアをダウンロード**しない**ように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先をセキュアにするために必要な予防措置を行っていることを確認します。

性質が使用不可のファイルにはマルウェアが含まれている可能性があるため、ファイルをダウンロードすると、システムはまずそのファイルを .zip パッケージにアーカイブします。.zip ファイル名には、ファイルの性質とファイル タイプ（存在する場合）さらに SHA-256 値が含まれます。誤って解凍してしまわないように、.zip ファイルをパスワードで保護できます。デフォルトの .zip ファイル パスワードを編集または削除するには、ファイルのプリファレンス（71-5 ページ）を参照してください。

動的分析の操作

ライセンス： Malware

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

サポートされる防御センター： すべて（DC500 を除く）

クラウドの精度を向上させ、追加のマルウェア分析および脅威識別を提供するために、適格なキャプチャ ファイルを Cisco クラウドに送信して、動的分析を行うことができます。クラウドはテスト環境でそのファイルを実行し、その結果に基づいて、脅威スコアおよび動的分析のサマリ レポートをDefense Centerに返します。適格なファイルをクラウドに送信して、Spero 分析を行うこともできます。これは、マルウェア識別を補うために、ファイルの構造を調べます。

動的分析のためのクラウドへのファイルの送信は、キャプチャされたファイルのタイプと、アクセス制御ポリシーで設定された可能な最小および最大のファイル サイズによって異なります。以下を行うことができます。

- ファイル ルールによって実行可能ファイルにマルウェア クラウド ルックアップが行われ、ファイル性質が不明の場合、動的分析のために自動的にファイルを送信できます。
- 保存済みで、サポートされているファイル タイプ（PDF や Microsoft Office ドキュメントなど）の場合、最大で 25 個のファイルを手動で一度に送信できます。

ファイルを送信すると、クラウドでの分析のためにキューに入れられます。キャプチャ ファイルおよびファイルのトラジェクトリを表示して、ファイルが動的分析のために送信されているかどうかを判別できます。注意すべき点として、動的分析のためにファイルを送信するたびに、最初の分析で結果が生成されていても、クラウドはそのファイルを分析します。

詳細については、ファイル ルールの操作（37-19 ページ）および動的分析のためのファイルの送信（40-6 ページ）を参照してください。

注　動的分析に適格なファイル タイプのリストと送信可能な最小および最大のファイル サイズに関して更新がないか、システムはクラウドを検査します（一日に 2 回以上行われることはありません）。

クラウドは、サンドボックス環境でファイルを実行して、動的分析を実行します。以下が返されます。

- 脅威スコア：ファイルにマルウェアが含まれている可能性について詳しく示します。
- 動的分析のサマリー レポート：クラウドがその脅威スコアを割り当てた理由について詳しく示します。

ファイル ポリシーの設定に基づき、定義されているしきい値を脅威スコアが超えているファイルを自動的にブロックできます。また、動的分析のサマリー レポートを確認して、マルウェアの識別を向上させたり、検出機能を調整したりできます。

動的分析を補うために、ファイル ルールによって実行可能ファイルにマルウェア クラウド ルックアップが行われる場合に、自動的にファイルを送信して Spero 分析を行うことができます。クラウドは実行可能ファイルの構造（メタデータや見出しの情報を含む）を調べて、ファイルがマルウェアかどうかを識別できます。詳細については、「マルウェア対策とファイル制御について（37-2 ページ）」を参照してください。

注意すべき点として、DC500 で Malware ライセンスは使用できず、シリーズ 2 デバイスまたは Cisco NGIPS for Blue Coat X-Series で Malware ライセンスを有効にすることもできないため、それらのアプライアンスを使用して、動的分析または Spero 分析のためにファイルを送信することはできません。

注　HTTP プロキシ経由で Cisco クラウドにファイルを送信するように、管理対象デバイスを設定できます。物理アプライアンスを設定する場合、管理インターフェイスの構成（64-9 ページ）を参照してください。仮想アプライアンスを設定する場合、http-proxy（D-34 ページ）を参照してください。Cisco NGIPS for Blue Coat X-Series では、プロキシ設定はサポートされていません。

詳細については、以下を参照してください。

- Spero 分析について（40-6 ページ）
- 動的分析のためのファイルの送信（40-6 ページ）
- 脅威スコアおよび動的解析のサマリーの確認（40-7 ページ）

Spero 分析について

ライセンス： Malware

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

サポートされる防御センター： すべて（DC500 を除く）

Spero 分析は SHA256 ハッシュの分析を補うもので、実行可能ファイル内のマルウェアをより正確に識別できます。Spero 分析では、デバイスがファイル構造の特性（メタデータや見出し情報など）を調べます。この情報に基づいて Spero シグニチャを生成した後、デバイスはそれを Cisco クラウド内の Spero ヒューリスティック エンジンに送信します。Spero シグニチャに基づいて、そのファイルがマルウェアかどうかを Spero エンジンが返します。マルウェアの場合、現時点の性質が不明であれば、システムはマルウェアの性質をファイルに割り当てます。ファイル性質の詳細については、マルウェア対策とファイル制御について（37-2 ページ）を参照してください。

Spero 分析のために実行可能ファイルを送信できるのは、検出時だけなので注意してください。後から手動で送信することはできません。動的分析のためにファイルを送信しなくても、Spero 解析のためにファイルを送信できます。詳細については、ファイル ルールの操作（37-19 ページ）を参照してください。

動的分析のためのファイルの送信

ライセンス： Malware

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

サポートされる防御センター： すべて（DC500 を除く）

イベント ビューアーのコンテキスト メニューまたはネットワーク ファイルのトラジェクトリから、動的分析のためにファイルを手動で送信できます。実行可能ファイルの他に、自動送信に適格ではないファイル タイプ（たとえば、PDF や Microsoft Office ドキュメントなど）も送信できます。詳細については、コンテキスト メニューの使用（2-5 ページ）およびサマリー情報（40-40 ページ）を参照してください。

問題が生じた後で複数のファイルを分析するために、キャプチャ ファイル ビューから一度に最大で 25 個の（特定のタイプの）ファイルをファイル性質に関係なく手動で送信できます。これにより、さまざまなファイルをより迅速に分析し、問題の正確な原因を突き止めることができます。詳細については、キャプチャ ファイルの操作（40-32 ページ）およびワークフロー ページの行の選択（58-39 ページ）を参照してください。

脅威スコアおよび動的解析のサマリーの確認

ライセンス： Malware

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

サポートされる防御センター： すべて（DC500 を除く）

動的分析のためにファイルを送信すると、Cisco クラウドはファイルのシグニチャを分析し、脅威スコアと動的分析のサマリーの両方を返します。これらは、潜在的なマルウェア脅威をより詳しく分析し、検出戦略を調整するのに役立ちます。

脅威スコア

ファイルは、マルウェアである可能性に応じて、脅威スコア レーティングのいずれかに分類されます。

表 40-1　　脅威スコア レーティング

脅威スコア	アイコン	定格
Low	●○○○	1 ～ 25
Medium	●●○○	26 ～ 50
High	●●●○	51 ～ 75
Very High	●●●●	76 ～ 100

Defense Centerは、ファイルの性質と同じ期間、ファイルの脅威スコアをローカルのキャッシュに入れます。以後これらのファイルを検出すると、システムは Cisco クラウドに再度クエリーを行う代わりに、キャッシュに入れられた脅威スコアを表示します。ファイル ポリシーの設定に基づき、ファイルの脅威スコアが、定義済みのマルウェアしきい値の脅威スコアを超える場合、そのファイルにマルウェアの性質を自動的に割り当てることができます。詳細については、ファイル ポリシーの作成（37-18 ページ）を参照してください。

動的分析のサマリー

動的分析のサマリーを使用できる場合、脅威スコアのアイコンをクリックすると、それが表示されます。動的分析のサマリーでは、脆弱性調査チーム（VRT）のファイル分析による全体的な脅威スコアの構成するレーティングと、クラウドがそのファイルを実行しようとしたときに開始された他のプロセスについて説明されています。

複数のレポートが存在する場合、このサマリーは、脅威スコアと完全に一致する最新のレポートに基づきます。完全に一致する脅威スコアがない場合、脅威スコアが最も高いレポートが表示されます。複数のレポートがある場合は、脅威スコアを選択して、それぞれのレポートを表示できます。

サマリーには、脅威スコアを構成する各コンポーネントの脅威がリストされています。各コンポーネントの脅威は、そのコンポーネントの脅威に関連するプロセスだけでなく、VRT の調査結果のリストまで展開できます。

プロセス ツリーには、クラウドがファイルを実行しようとしたときに開始されたプロセスが示されています。これは、マルウェアを含むファイルが、想定外のプロセスやシステム リソースへアクセスしようとしているかどうか（たとえば、Word ドキュメントを実行すると、Microsoft Word が開き、次にエクスプローラが起動し、さらに Java が起動するなど）を識別するのに役立ちます。

リストされている各プロセスには、実際のプロセスを検査するのに使用できるプロセス ID と md5 チェックサムが含まれています。プロセス ツリーには、親プロセスの結果として開始されたプロセスが子ノードとして表示されます。

動的分析のサマリーから [View Full Report] をクリックすることにより、VRT の完全な分析を詳述する VRT の分析レポートを表示できます。これには、ファイルの一般情報、検出されたすべてのプロセスのより綿密な説明、ファイル分析の概要、および他の関連情報が含まれています。

ファイル イベントの操作

ライセンス： Protection

システムは、現在適用されているファイル ポリシーのルールに従って、管理対象デバイスがネットワーク トラフィック内のファイルを検出またはブロックしたときに生成されたファイル イベントを記録します。注意すべき点として、システムがファイル イベントを生成する際に、呼び出しを行うアクセス制御ルールのログ設定に関係なく、システムはDefense Centerデータベースへの関連する接続の終わりも記録します。詳細については、ファイル ポリシーの概要と作成（37-10 ページ）を参照してください。

注　ネットワーク トラフィックで検出され、FireSIGHT システムによってマルウェアとして識別されたファイルは、ファイル イベントとマルウェア イベントの両方を生成します。これは、ファイル内のマルウェアを検出するために、システムはまずそのファイル自体を検出する必要があるためです。エンドポイントベースのマルウェア イベントには、対応するファイル イベントはありません。詳細については、マルウェア イベントの操作（40-17 ページ）およびキャプチャ ファイルの操作（40-32 ページ）を参照してください。

Defense Centerのイベント ビューアを使用して、ファイル イベントの表示、検索、削除を行えます。さらに、Files Dashboard では、ネットワークで検出されたファイル（マルウェア ファイルを含む）に関する詳細情報を、図やグラフを使って一目で知ることができます。ネットワーク ファイル トラジェクトリでは、個々のファイルの情報とそれらが時間の経過に伴ってネットワークでどのように推移してきたかに関する情報のサマリーが提供されるので、それらのファイルに関してより綿密に知ることができます。ファイルの識別データを使用して、相関ルールをトリガーしたり、レポートを作成したりできます。後者では、定義済みの Files Report テンプレートかカスタム レポート テンプレートを使用します。

詳細については、以下を参照してください。

- ファイル イベントの表示（40-9 ページ）
- ファイル イベント テーブルについて（40-10 ページ）

- 地理情報の使用（58-23 ページ）
- ファイル イベントの検索（40-13 ページ）

ファイル イベントの表示

ライセンス：Protection

FireSIGHT システムのイベント ビューアーでは、分析に関連した情報に応じてイベント ビューを操作するほかに、ファイル イベントをテーブルの形で表示できます。また、個々のファイル イベントに使用可能な情報は、ライセンスなどのさまざまな要因によって異なることに注意してください。詳細については、サービス サブスクリプション（65-8 ページ）を参照してください。

ファイル イベントにアクセスしたときに表示されるページは、ワークフローによって異なります。ワークフローは、大まかなビューから詳細なビューに移動してイベントを評価するために使用できる、一連のページです。システムには、ファイル イベント用の以下の定義済みのワークフローが付属しています。

- [File Summary]（デフォルト）：さまざまなファイル イベントのカテゴリーとタイプ、および関連するマルウェア ファイル性質の概要を提供します。
- [Hosts Receiving Files] および [Hosts Sending Files]：ファイルを送受信したホストのリストを、それらのファイルの関連するマルウェア性質でグループ化した形で提供します。

注 ファイル性質は、システムがマルウェア クラウド ルックアップを実行したファイルに関してのみ表示されます。ファイル ルール アクションと評価順序（37-13 ページ）を参照してください。

特有の必要にかなった情報だけを表示するカスタム ワークフローを作成することもできます。カスタム ワークフローを含む、さまざまなデフォルト ワークフローの指定の詳細については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

FireSIGHT システム は、Unicode（UTF8）文字を使用するファイル名の表示および入力を Web インターフェイスのすべてのエリア（イベント ビューアー、イベント検索、ダッシュボード、Context Explorer など）でサポートしています。ただし、PDF 形式で生成したレポートでは Unicode がサポートされないので注意してください。PDF レポートでは、Unicode ファイル名は翻字形式で表示されます。詳細については、レポートの生成と表示（57-28 ページ）を参照してください。また、SMB プロトコルは Unicode ファイル名を印刷可能な文字に変換することにも注意してください。SMB を通して検出した Unicode ファイル名を持つファイルは、印刷不可能な文字の代わりにピリオド（.）とともに表示されます。

イベント ビューアを使用して、以下を行うことができます。

- イベントの検索、ソート、および制限と、表示されるイベントの時間範囲の変更
- 表示される列の指定（テーブル ビューのみ）
- IP アドレスに関連付けられたホスト プロファイル、またはユーザ ID に関連付けられたユーザの詳細およびホスト履歴の表示
- 特定のファイルが検出された接続の表示
- 同じワークフロー内のさまざまなワークフロー ページを使用したイベントの表示
- 別のワークフローを使用したイベントの表示
- 特定の値で制限されるワークフロー内のページからページへのドリルダウン
- 後で同じデータに戻る（存在している場合）ための、現在のページおよび制限のブックマーク
- ファイルに関連付けられたルーティング可能な IP アドレスの送受信の国および大陸の表示

- ファイルのトラジェクトリの表示
- ファイル リストへのファイルの追加、ファイルのダウンロード、動的分析のためのファイルの送信、ファイルの SHA-256 値のフルテキストの表示
- ファイルの動的分析のサマリー レポート（使用可能な場合）の表示
- アーカイブ ファイル内のネストされたファイルの表示
- 現在の制限を使用したレポート テンプレートの作成
- データベースからのイベントの削除
- IP アドレスのコンテキスト メニューを使用した、ホワイトリストまたはブラックリストへの追加、あるいはファイル イベントに関連付けられたホストまたは IP アドレスに関する他の使用可能な情報の取得

カスタム ワークフローの作成など、イベント ビューアの使用の詳細については、ワークフローの概要と使用（58-1 ページ）を参照してください。

特定のファイルが検出された接続をすぐに表示するには、イベント ビューアーでチェック ボックスを使用してファイルを選択してから、[Jump to] ドロップダウン リストで [Connections Events] を選択します。詳細については、ワークフロー間のナビゲート（58-40 ページ）を参照してください。

ファイル イベントを表示するには、以下を行います。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Files] > [Files Events] を選択します。

デフォルトのファイル イベントのワークフローの最初のページが表示されます。表示される列の詳細については、ファイル イベント テーブルについて（40-10 ページ）を参照してください。

ファイル イベント テーブルについて

ライセンス： Protection

Defense Centerは、適用されているファイル ポリシーの設定に従って、監視されているネットワーク トラフィックで送信されるファイルを管理対象デバイスが検出またはブロックしたときに、ファイル イベントを記録します。

ファイル イベントのテーブル ビューは、定義済みファイル イベントのワークフローの最後のページであり、カスタム ワークフローに追加できます。このテーブル ビューには、ファイル テーブルの各フィールドの列が含まれます。デフォルトでは、ファイル イベントのテーブル ビューにいくつかのフィールドが表示されます。セッションの期間中にフィールドを有効にするには、展開矢印（  ）をクリックして検索の制限を展開してから、[Disabled Columns] の下の列名をクリックします。

個々のファイル イベントに使用可能な情報は、ライセンスなどのさまざまな要因によって異なることに留意してください。たとえば、ファイル制御を行えるのは Protection ライセンスだけですが、Malware ライセンスを使用して、特定のファイル タイプの高度なマルウェア対策を実行したり、ネットワークで転送されたファイルを追跡したりできます。

以下の表は、ファイル イベント フィールドについて説明しています。

表 40-2　ファイル イベント フィールド

フィールド	説明
時刻	イベントが生成された日時。
Action	ファイルを検出したファイル ポリシー ルールに関連したアクション、および関連するファイル アクション オプション。
Sending IP	検出されたファイルを送信するホストの IP アドレス。
Sending Country	検出されたファイルを送信するホストの国。 DC500 Defense Centerはこの機能をサポートしていないことに注意してください。
Receiving IP	検出されたファイルを受信するホストの IP アドレス。
Receiving Country	検出されたファイルを受信するホストの国。 DC500 Defense Centerはこの機能をサポートしていないことに注意してください。
Sending Port	ファイルが検出されたトラフィックによって使用される送信元ポート。
Receiving Port	ファイルが検出されたトラフィックによって使用される宛先ポート。
SSL Status	暗号化された接続を記録した、SSL ルールに関連したアクション、デフォルト アクション、または復号化不能トラフィック アクション: • [Block] および [Block with reset] は、ブロックされた暗号化接続を表します。 • [Decrypt (Resign)] は、再署名サーバ証明書を使用して復号化された発信接続を表します。 • [Decrypt (Replace Key)] は、置き換えられた公開キーと自己署名サーバ証明書を使用して復号化された発信接続を表します。 • [Decrypt（Known Key）] は、既知の秘密キーを使用して復号化された着信接続を表します。 • [Default Action] は、デフォルト アクションによって接続が処理されたことを示します。 • [Do not Decrypt] は、システムが復号化しなかった接続を表します。 システムが暗号化接続を復号化できなかった場合は、実行された復号化不能のトラフィック アクションと失敗の原因が表示されます。たとえば、システムが不明な暗号スイートで暗号化されたトラフィックを検出し、さらにインスペクションを行わずにそのトラフィックを許可した場合、このフィールドには [Do Not Decrypt (Unknown Cipher Suite)] が表示されます。 証明書の詳細を表示するには、ロック アイコン（  ）をクリックします。詳細については、暗号化接続に関連付けられた証明書の表示（39-33 ページ）を参照してください。
User	ファイルの宛先のホスト（[Receiving IP]）にログインしたユーザ。 ユーザが宛先ホストに関連付けられているため、ユーザがファイルをアップロードしたファイル イベントに、ユーザが関連付けられないことに注意してください。
File Name	ファイルの名前です。

表 40-2　ファイル イベント フィールド（続き）

フィールド	説明
処理	以下のファイル性質のいずれかです。 • Malware：クラウドでそのファイルがマルウェアとして分類されていること、またはファイルの脅威スコアが、ファイル ポリシーで定義されたマルウェアしきい値を超えていることを示します。 • Clean：クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。 • Unknown ：クラウドが性質を割り当てる前にマルウェア クラウド ルックアップが行われたことを示します。ファイルは分類されていません。 • Custom Detection：ユーザがカスタム検出リストにファイルを追加したことを示します。 • Unavailable：Defense Centerがマルウェア クラウド ルックアップを実行できなかったことを示します。この性質で見られるイベントはごくわずかである可能性があります。これは予期された動作です。 • N/A：ファイル検出またはファイル ブロック ルールがファイルを処理し、Defense Centerがマルウェア クラウド ルックアップを行わなかったことを示します。
SHA256	ファイルの SHA-256 ハッシュ値と、最後に検出されたファイル イベントおよびファイル性質を表すネットワーク ファイル トラジェクトリ アイコン（このファイルが以下の結果として検出された場合）。 • **Store Files** が有効になっているファイル検出ファイル ルール。 • **Store Files** が有効になっているファイル ブロック ファイル ルール。 • マルウェア クラウド ルックアップ ファイル ルール • マルウェア ブロック ファイル ルール ネットワーク ファイル トラジェクトリを表示するには、トラジェクトリ アイコンをクリックします。詳細については、ネットワーク ファイル トラジェクトリの分析（40-40 ページ）を参照してください。
Threat Score	そのファイルに関連する最新の脅威スコア： • Low（●○○○） • Medium（●●○○） • High（●●●○） • Very High（●●●●） 動的分析のサマリー レポートを表示するには、脅威スコア アイコンをクリックします。
タイプ	ファイルのタイプ（HTML や MSEXE など）。
カテゴリ	ファイル タイプの一般的なカテゴリ（Office Documents、Archive、Multimedia、Executables、PDF files、Encoded、Graphics、System Files など）。
Size (KB)	ファイルのサイズ（KB 単位）。ファイルが完全に受信される前にシステムがファイルのタイプを判別すると、ファイル サイズが計算されずに、このフィールドがブランクになる場合があるので注意してください。
URI	ファイルの送信元の URI（ファイルをダウンロードした URL など）。

表 40-2　ファイル イベント フィールド（続き）

フィールド	説明
Archive Name	ファイルが関連付けられているアーカイブ ファイル（存在する場合）の名前（archive.zip など）。アーカイブ ファイルの内容を表示するには、アーカイブ ファイルのイベント ビューア行を右クリックしてコンテキスト メニューを開いてから、[View Archive Contents] をクリックします。詳細については、アーカイブ ファイルの内容の表示（37-24 ページ）を参照してください。
Archive SHA256	ファイルが関連付けられているアーカイブ ファイル（存在する場合）の SHA256 ハッシュ値。
Archive Depth	アーカイブ ファイル内でファイルがネストされたレベル（存在する場合）。たとえば、1 や 3 など。
アプリケーション プロトコル	管理対象デバイスがファイルを検出したトラフィックで使用されるアプリケーション プロトコル。
Application Protocol、Client、Web Application Category、Tag	アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。表 45-2（45-12 ページ）を参照してください。
クライアント	ファイルを送信する接続で使用されるクライアント アプリケーション。
Web アプリケーション	HTTP を使用してファイルが送信された場合、接続で検出され、ファイルの送信に使用された Web アプリケーション（コンテンツまたは要求された URL）。
Application Risk	接続で検出されたアプリケーション トラフィックに関連するリスク：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するリスクがあります。このフィールドでは、それらのうち最も高いものが表示されます。詳細については、表 45-2（45-12 ページ）を参照してください。
Business Relevance	接続で検出されたアプリケーション トラフィックに関連するビジネス関連性：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するビジネス関連性があります。このフィールドでは、それらのうち最も低いもの（関連が最も低い）が表示されます。詳細については、表 45-2（45-12 ページ）を参照してください。
メッセージ	マルウェア性質が変更されたファイル（つまり、遡及的マルウェア イベントに関連したファイル）で、性質がいつ、どのように変更されたかに関する情報。
File Policy	ファイルを検出したファイル ポリシー。
デバイス	ファイルを検出したデバイスの名前。
セキュリティ コンテキスト	トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。システムがこのフィールドにデータを設定するのは、マルチコンテキスト モードの ASA FirePOWER デバイスだけです。
Count	各行の情報に一致するイベントの数。このフィールドが表示されるのは、2 つ以上の同一の行を作成する制限を適用した後です。

ファイル イベントの検索

ライセンス：Protection

Defense Centerの [Search] ページを使用して、特定のファイル イベントを検索し、その結果をイベント ビューアーで表示できます。また、後で再利用するために検索条件を保存できます。[Custom Analysis] ダッシュボード ウィジェット、レポート テンプレート、カスタム ユーザ ロールも、保存した検索を使用できます。

覚えておくべき点として、検索結果は、検索するイベントの使用可能なデータに依存します。つまり、使用可能なデータによっては、検索の制限が適用されないことがあります。たとえば、[Disposition] および [SHA256] フィールドにデータが入れられるのは、Defense Centerがマルウェア クラウド ルックアップを実行したファイルに限られます。

一般的な検索の構文

それぞれの検索フィールドの隣には、使用できる構文の例が表示されます。検索条件を入力する場合、次の点に注意してください。

- すべてのフィールドで否定(!)を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「`A`」または「`B`」または「`C, D, E`」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク(*)を使用できます。
- フィールドで情報を使用できないイベントを示すには、そのフィールドに `n/a` を指定します。フィールドにデータが入れられるイベントを示すには、`!n/a` を使用します。
- 特定のデバイス、およびグループ、スタック、またはクラスタ内のデバイスを検索するには、デバイス フィールドを使用します。検索での FireSIGHT システムによるデバイス フィールドの処理方法については、検索でのデバイスの指定(60-7 ページ)を参照してください。
- オブジェクトを検索条件として使用するには、検索フィールドの隣にあるオブジェクトの追加アイコン(+)をクリックします。

検索でのオブジェクトの使用など、検索構文の詳細については、イベントの検索(60-1 ページ)を参照してください。

ファイル イベントの特別な検索構文

前述の一般的な検索構文を補うために、以下のリストでは、ファイル イベントの特別な検索構文について説明しています。

Sending/Receiving Continent

システムは [Sending Continent] または [Receiving Continent] が指定した大陸と一致するすべてのイベントを返します。

Sending/Receiving Country

システムは [Sending Country] または [Receiving Country] が指定した国と一致するすべてのイベントを返します。

Sending/Receiving IP

システムは [Sending IP] または [Receiving IP] が指定した IP アドレスと一致するすべてのイベントを返します。

URI または Message

システムは部分一致を実行します。つまり、アスタリスクを使用せずに、フィールドの内容の全部または一部を検索できます。

File Storage

以下の 1 つ以上を入力します。

- [Stored] は、関連するファイルが現在保存されているすべてのイベントを返します。
- [Stored in connection] は、関連するファイルが現在保存されているかどうかに関係なく、関連するファイルをシステムがキャプチャおよび保存したすべてのイベントを返します。
- [Failed] は、関連するファイルをシステムが保存できなかったすべてのイベントを返します。

The SSL Actual Action taken

システムが指定したアクションを適用した暗号化されたトラフィックのファイル イベントを表示するには、次のキーワードのいずれかを入力します。

- [Do not Decrypt] は、システムが復号化しなかった接続を表します。
- [Block] および [Block with reset] は、ブロックされた暗号化接続を表します。
- [Decrypt (Known Key)] は、既知の秘密キーを使用して復号化された着信接続を表します。
- [Decrypt (Replace Key)] は、置き換えられた公開キーと自己署名サーバ証明書を使用して復号化された発信接続を表します。
- [Decrypt (Resign)] は、再署名サーバ証明書を使用して復号化された発信接続を表します。

このカラムは、ファイル イベントのテーブル ビューに表示されません。

The SSL Failure Reason

システムが指定された理由で復号化に失敗した暗号化されたトラフィックのファイル イベントを表示するには、次のキーワードのいずれかを入力します。

- `Unknown`
- `No Match`
- `Success`
- `Uncached Session`
- `Unknown Cipher Suite`
- `Unsupported Cipher Suite`
- `Unsupported SSL Version`
- `SSL Compression Used`
- `Session Undecryptable in Passive Mode`
- `Handshake Error`
- `Decryption Error`

- Pending Server Name Category Lookup
- Pending Common Name Category Lookup
- Internal Error
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- Invalid Action

このカラムは、ファイル イベントのテーブル ビューに表示されません。

The SSL Subject Country

証明書サブジェクトの国に関連付けられている暗号化されたトラフィックのファイル イベントを表示するには、2 文字の ISO 3166-1 アルファ 2 国番号を入力します。

このカラムは、ファイル イベントのテーブル ビューに表示されません。

The SSL Issuer Country

証明書発行者の国に関連付けられている暗号化されたトラフィックのファイル イベントを表示するには、2 文字の ISO 3166-1 アルファ 2 国番号を入力します。

このカラムは、ファイル イベントのテーブル ビューに表示されません。

SSL Certificate Fingerprint

その証明書に関連付けられているトラフィックのファイル イベントを表示するには、その証明書の認証に使用される SHA ハッシュ値を入力するか、または貼り付けます。

このカラムは、ファイル イベントのテーブル ビューに表示されません。

SSL Public Key Fingerprint

その証明書に関連付けられているトラフィックのファイル イベントを表示するには、その証明書に含まれている公開キーの認証に使用される SHA ハッシュ値を入力するか、または貼り付けます。

このカラムは、ファイル イベントのテーブル ビューに表示されません。

ファイル イベントを検索するには、以下を行います。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　テーブル ドロップダウン リストから [File Events] を選択します。

ページが適切な制約によって更新されます。

ステップ 3　次の項に記載されているように、該当するフィールドに検索基準を入力します。

- ファイル イベント テーブルのフィールドの詳細については、ファイル イベント フィールドの表を参照してください。
- ファイル イベントの特別な検索構文については、ファイル イベントの特別な検索構文（40-14 ページ）を参照してください。
- 公開キー証明書に関連するフィールドについては、暗号化接続に関連付けられた証明書の表示（39-33 ページ）を参照してください。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　検索をカスタム ユーザ ロールのデータ制限として使用する場合は、**必ず**プライベート検索として保存してください。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。
- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save as New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

検索結果は、現在の時刻範囲によって制限されるデフォルトのファイル イベントのワークフローに表示されます。

マルウェア イベントの操作

ライセンス： Malware または任意

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

システムは以下のタイミングでマルウェア イベントをDefense Center データベースに記録します。

- 管理対象デバイスがネットワーク トラフィックでファイルを検出し、そのファイルがマルウェア クラウド ルックアップでマルウェアとして識別された。
- 管理対象デバイスがネットワーク トラフィックでカスタム検出リストに含まれているファイルを検出した。

- ファイルのマルウェア性質が変更されたことをシステムが認識した。これらは、遡及的マルウェア イベントと呼ばれます。
- 組織のエンドポイントにインストールされた FireAMP コネクタが脅威を検出し、その脅威を Cisco クラウドに伝えた。

FireAMP マルウェア検出がダウンロード時または実行時にエンドポイントで行われるのに対し、管理対象デバイスはネットワーク トラフィックでファイルを検出するため、これらのマルウェア イベントの情報は異なります。遡及的マルウェア イベントには、他のネットワークベースのマルウェア イベントとも、エンドポイントベースのマルウェア イベントとも若干異なるデータが含まれます。

以降の項では、さまざまな種類のマルウェア イベントについて簡単に説明します。マルウェア検出の全体的なプロセスの詳細については、マルウェア対策とファイル制御について（37-2 ページ）を参照してください。

エンドポイントベース（FireAMP）のマルウェア イベント

お客様の組織で FireAMP サブスクリプションをご利用の場合、個々のユーザは自分のコンピュータやモバイル デバイスに FireAMP コネクタをインストールします。これらの軽量のエージェントは Cisco クラウドと通信し、それはDefense Centerと通信します。FireAMP 用のクラウド接続の操作（37-27 ページ）を参照してください。クラウドは脅威の通知や他の種類の情報（スキャン、隔離、ブロックされた実行、クラウドのリコールのデータなど）を送信できます。Defense Centerはこの情報をマルウェア イベントとしてデータベースに記録します。

注　エンドポイントベースのマルウェア イベントで報告される IP アドレスは、ネットワーク マップに（そして、監視対象ネットワークにも）含まれない場合もあります。展開、コンプライアンスのレベル、およびその他の要因によっては、FireAMP コネクタがインストールされている組織内のエンドポイントが、管理対象デバイスによって監視されているものと同じホストではない可能性があります。

ネットワーク トラフィックに基づくマルウェア イベント

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

サポートされる防御センター： すべて（DC500 を除く）

Malware ライセンスを使用すると、管理対象デバイスは全体的なアクセス制御設定の一部として、ネットワーク トラフィック内のマルウェアを検出できます。ファイル ポリシーの概要と作成（37-10 ページ）を参照してください。

以下のシナリオでは、マルウェア イベントが生成される可能性があります。

- 管理対象デバイスが一連の特定のファイル タイプのいずれかを検出すると、Defense Center はマルウェア クラウド ルックアップを実行します。これにより、ファイル性質として `Malware`、`Clean`、または `Unknown` がDefense Centerに返されます。
- Defense Centerがクラウドとの接続を確立できない場合や、それ以外でクラウドが使用できない場合、ファイル性質は `Unavailable` になります。この性質で見られるイベントはごくわずかである可能性があります。これは予期された動作です。
- ファイルに関連付けられている脅威スコアが、ファイルを検出したファイル ポリシーで定義されたマルウェアしきい値の脅威スコアを超えた場合、Defense Centerはファイル性質として `Malware` をそのファイルに割り当てます。
- SHA-256 値がカスタム検出リストに保存されているファイルを管理対象デバイスが検出した場合、Defense Centerはファイル性質として `Custom Detection` をそのファイルに割り当てます。

- クリーン リストに含まれているファイルを管理対象デバイスが検出した場合、Defense Centerはファイル性質として Clean をそのファイルに割り当てます。

Defense Centerは他のコンテキスト データとともに、ファイルの検出と性質のレコードをマルウェア イベントとして記録します。

注 ネットワーク トラフィックで検出され、FireSIGHT システムによってマルウェアとして識別されたファイルは、ファイル イベントとマルウェア イベントの両方を生成します。これは、ファイル内のマルウェアを検出するために、システムはまずそのファイル自体を検出する必要があるためです。詳細については、ファイル イベントの操作（40-8 ページ）およびキャプチャ ファイルの操作（40-32 ページ）を参照してください。

遡及的マルウェア イベント

サポートされるデバイス： シリーズ 3、仮想

サポートされる防御センター： すべて（DC500 を除く）

ネットワーク トラフィックで検出されたマルウェア ファイルの場合、ファイル性質が変わることがあります。たとえば、Cisco クラウドがあるファイルを以前はクリーンであると識別したものの、今はマルウェアとして判断したり、その逆にマルウェアとして識別したファイルが実際にはクリーンだったと判断する場合があります。

前の週にマルウェア ルックアップを実行したファイルのファイル性質が変更された場合、クラウドはDefense Centerに通知します。その場合、以下の 2 つが行われます。

- Defense Centerが新しい遡及的マルウェア イベントを生成します。

  この新しい遡及的マルウェア イベントは、前の週に検出され、同じ SHA-256 ハッシュ値を持つ同じすべてのファイルの性質変更を表します。そのため、これらのイベントには限られた情報（Defense Centerに性質変更が通知された日時、新しい性質、ファイルの SHA-256 ハッシュ値、および脅威名）が含まれます。IP アドレスや他のコンテキスト情報は含まれません。

- Defense Centerは遡及的イベントの関連する SHA-256 ハッシュ値を持つ既に検出済みのファイルのファイル性質を変更します。

  ファイルの性質が Malware に変更されると、Defense Centerは新しいマルウェア イベントをデータベースに記録します。新しい性質を除いて、この新しいマルウェア イベントの情報は、ファイルが最初に検出されたときに生成されたファイル イベントのものと同じです。

  ファイルの性質が Clean に変更された場合に、Defense Centerがそのマルウェア イベントをマルウェア テーブルから削除することはありません。そうする代わりに、イベントは単に性質の変更を反映します。つまり、性質が Clean のファイルがマルウェア テーブルに含められる場合があり、それはそのファイルが最初マルウェアと識別されていた場合だけです。マルウェアとして識別されたことのないファイルは、ファイルのテーブルにのみ含められます。

  いずれの場合でも、マルウェア イベントの [Message] に、性質がいつ、どのように変更されたかが示されます。以下に例を示します。

  ```
  Retrospective Event, Mon Oct 1 20:44:00 2012 (UTC), Old Disp: Unknown, New Disp:
  Malware
  ```

マルウェア イベントの使用

Defense Centerのイベント ビューアを使用して、マルウェア イベントの表示、検索、削除を行えます。さらに、Files Dashboard および Context Explorer では、ネットワークで検出されたファイル（マルウェア ファイルを含む）に関する詳細情報を、図やグラフを使って一目で知ることができます。ネットワーク ファイル トラジェクトリでは、個々のマルウェア ファイルの情報とそれらが時間の経過に伴ってネットワーク内をどのように移動してきたかに関する情報のサマリーが提

供されるので、それらのファイルに関してより綿密に知ることができます。マルウェア検出データを使用して、相関ルールをトリガーしたり、レポートを作成したりできます。後者では、定義済みのマルウェア レポート テンプレートかカスタム レポート テンプレートを使用します。

詳細については、以下を参照してください。

- マルウェア イベントの表示（40-20 ページ）
- マルウェア イベント テーブルについて（40-21 ページ）
- マルウェア イベントの検索（40-28 ページ）

マルウェア イベントの表示

ライセンス： Malware または任意

FireSIGHT システムのイベント ビューアーでは、マルウェア イベントをテーブルの形で表示でき、分析に関連した情報に応じてイベント ビューを操作することもできます。また、個々のマルウェア イベントに使用可能な情報は、ライセンスなどのさまざまな要因によって異なることに注意してください。詳細については、サービス サブスクリプション（65-8 ページ）を参照してください。

マルウェア イベントにアクセスしたときに表示されるページは、ワークフローによって異なります。ワークフローは、大まかなビューから詳細なビューに移動してイベントを評価するために使用できる、一連のページです。システムには、マルウェア イベント用の以下の定義済みのワークフローが付属しています。

- [Malware Summary]（デフォルト）：個々の脅威でグループ化された、検出マルウェアのリストを提供します。
- [Malware Event Summary]：さまざまなマルウェア イベントのタイプとサブタイプの概要を提供します。
- [Hosts Receiving Malware] および [Hosts Sending Malware]：マルウェアを送受信したホストのリストを、それらのファイルの関連するマルウェア性質でグループ化した形で提供します。性質はマルウェア クラウド ルックアップまたはマルウェア ブロック ファイル ルールの結果として検出されたファイルに関してのみ表示されるので注意してください。
- [Applications Introducing Malware]：組織のエンドポイントで検出されたマルウェアにアクセスしたか、そのマルウェアを実行したクライアント アプリケーションのリストを提供します。このリストから、それぞれの親クライアントによってアクセスされる個々のマルウェア ファイルにドリルダウンできます。

特有の必要にかなった情報だけを表示するカスタム ワークフローを作成することもできます。カスタム ワークフローを含む、さまざまなデフォルト ワークフローの指定の詳細については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

FireSIGHT システム は、Unicode（UTF8）ファイル名の表示および入力を Web インターフェイスのすべてのエリア（イベント ビューアー、イベント検索、ダッシュボード、Context Explorer など）でサポートしています。ただし、PDF 形式で生成したレポートでは Unicode がサポートされないので注意してください。PDF レポートでは、Unicode ファイル名は翻字形式で表示されます。詳細については、レポートの生成と表示（57-28 ページ）を参照してください。

イベント ビューアを使用して、以下を行うことができます。

- イベントの検索、ソート、および制限と、表示されるイベントの時間範囲の変更
- 表示される列の指定（テーブル ビューのみ）
- IP アドレスに関連付けられたホスト プロファイル、またはユーザ ID に関連付けられたユーザの詳細およびホスト履歴の表示

- 特定のマルウェアが検出された接続の表示（ネットワークベースのマルウェア イベントのみ）
- 同じワークフロー内のさまざまなワークフロー ページを使用したイベントの表示
- 別のワークフローを使用したイベントの表示
- 特定の値で制限されるワークフロー内のページからページへのドリルダウン
- 後で同じデータに戻る（存在している場合）ための、現在のページおよび制限のブックマーク
- ファイルに関連付けられたルーティング可能 IP アドレスの位置情報の表示
- ファイルのトラジェクトリの表示
- アーカイブ ファイル内のネストされたファイルの表示
- 現在の制限を使用したレポート テンプレートの作成
- データベースからのイベントの削除
- ファイル リストへのファイルの追加、ファイルのダウンロード、動的分析のためのファイルの送信、ファイルの SHA-256 値のフルテキストの表示
- ファイルの動的分析のサマリー レポート（使用可能な場合）の表示
- IP アドレスのコンテキスト メニューを使用した、ホワイトリストまたはブラックリストへの追加、あるいはマルウェア イベントに関連付けられたホストまたは IP アドレスに関する他の使用可能な情報の取得

シリーズ 2 デバイス、Cisco NGIPS for Blue Coat X-Series、および DC500 Defense Center は、ネットワークベースのマルウェア保護およびアーカイブ ファイル インスペクションをサポートしていません。これは、表示されるデータに影響を及ぼす場合があるので注意してください。たとえば、シリーズ 2 デバイスだけを管理するシリーズ 3 Defense Centerは、エンドポイントベースのマルウェア イベントだけを表示できます。

カスタム ワークフローの作成など、イベント ビューアの使用の詳細については、ワークフローの概要と使用（58-1 ページ）を参照してください。

マルウェア イベントを表示するには、以下を行います。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Files] > [Malware Events] を選択します。

デフォルトのマルウェア イベントのワークフローの最初のページが表示されます。表示される列の詳細については、マルウェア イベント テーブルについて（40-21 ページ）を参照してください。

マルウェア イベント テーブルについて

ライセンス： Malware または任意

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

組織内のエンドポイントにインストールされた FireAMP コネクタが脅威を検出した場合、または管理対象デバイスがネットワーク トラフィックでファイルを検出し、そのファイルがマルウェア クラウド ルックアップでマルウェアとして識別された場合、システムはマルウェア イベントを Defense Center データベースに記録します。また、ファイルのマルウェア性質が変更されたことをシステムが認識した場合、システムは遡及的マルウェア イベントを記録します。シリーズ 2 デバイス、Cisco NGIPS for Blue Coat X-Series、および DC500 Defense Center は、ネットワーク

ベースのマルウェア保護をサポートしていません。これは、表示されるデータに影響を及ぼす場合があるので注意してください。たとえば、シリーズ 2 デバイスだけを管理するシリーズ 3 Defense Centerは、エンドポイントベースのマルウェア イベントだけを表示できます。詳細については、マルウェア対策とファイル制御について（37-2 ページ）およびマルウェア イベントの操作（40-17 ページ）を参照してください。

マルウェア イベントのテーブル ビューは、定義済みファイル イベントのワークフローの最後のページであり、カスタム ワークフローに追加できます。このテーブル ビューには、ファイル テーブルの各フィールドの列が含まれます。マルウェア イベントのテーブル ビューのいくつかのフィールドは、デフォルトで表示されます。セッションの期間中にフィールドを有効にするには、展開矢印（  ）をクリックして検索の制限を展開してから、[Disabled Columns] の下の列名をクリックします。

すべてのイベントで、すべてのフィールドにデータが入っている訳ではないことに留意してください。マルウェア イベントのタイプが異なれば、含まれる情報も異なる可能性があります。たとえば、FireAMP マルウェア検出はダウンロード時または実行時にエンドポイントで行われるため、エンドポイントベースのマルウェア イベントには、ファイル パスや呼び出し元のクライアント アプリケーションに関する情報などが含まれます。対照的に、管理対象デバイスはネットワーク トラフィックでマルウェア ファイルを検出するため、それらに関連したマルウェア イベントには、ファイルを送信するのに使用される接続に関する、ポート、アプリケーション プロトコル、および送信元 IP アドレスの情報が含まれます。

次の表では各マルウェア イベント フィールドがリストされており、マルウェア イベントのタイプに応じて、システムがそのフィールドに情報を表示するかどうかを示しています。DC500 Defense Centerは、送受信の大陸または国の位置情報をサポートしていないので注意してください。

表 40-3　　マルウェア イベント フィールド

フィールド	説明	ネットワーク	エンドポイント	クラウドからのレトロスペクティブ
時刻	イベントが生成された日時。	yes	yes	yes
Action	ファイルが一致したルールのルール アクションに関連付けられているファイル ルール アクションと、関連するファイル ルール アクションのオプション。	yes	no	yes
Sending IP	検出されたマルウェアを送信しているホストの IP アドレス。	yes	no	no
Sending Continent	検出されたマルウェアを送信しているホストがある大陸。	yes	no	yes
Sending Country	検出されたマルウェアを送信しているホストがある国。	yes	no	no
Receiving IP	ネットワークベースのマルウェア イベントの場合、検出されたマルウェアを受信するホストの IP アドレス。 エンドポイントベースのマルウェア イベントの場合、FireAMP コネクタがインストールされていて、マルウェア イベントが発生したエンドポイントの IP アドレス。	yes	yes	no
Receiving Continent	検出されたマルウェアを受信しているホストがある大陸。	yes	no	yes
Receiving Country	検出されたマルウェアを受信しているホストがある国。	yes	no	no
Sending Port	管理対象デバイスがマルウェアを検出したトラフィックによって使用されている送信元ポート。	yes	no	no

表 40-3　マルウェア イベント フィールド（続き）

フィールド	説明	ネットワーク	エンドポイント	クラウドからのレトロスペクティブ
Receiving Port	管理対象デバイスがマルウェアを検出したトラフィックによって使用されている宛先ポート。	yes	no	no
SSL Status	暗号化された接続を記録した、SSL ルールに関連したアクション、デフォルト アクション、または復号化不能トラフィック アクション: • [Block] および [Block with reset] は、ブロックされた暗号化接続を表します。 • [Decrypt (Resign)] は、再署名サーバ証明書を使用して復号化された発信接続を表します。 • [Decrypt (Replace Key)] は、置き換えられた公開キーと自己署名サーバ証明書を使用して復号化された発信接続を表します。 • [Decrypt（Known Key）] は、既知の秘密キーを使用して復号化された着信接続を表します。 • [Do not Decrypt] は、システムが復号化しなかった接続を表します。 システムが暗号化接続を復号化できなかった場合は、実行された復号化不能のトラフィック アクションと失敗の原因が表示されます。たとえば、システムが不明な暗号スイートで暗号化されたトラフィックを検出し、さらにインスペクションを行わずにそのトラフィックを許可した場合、このフィールドには [Do Not Decrypt (Unknown Cipher Suite)] が表示されます。 証明書の詳細を表示するには、ロック アイコン（  ）をクリックします。詳細については、暗号化接続に関連付けられた証明書の表示（39-33 ページ）を参照してください。	yes	no	no
User	マルウェア イベントが発生したホスト（**Receiving IP**）のユーザ ネットワークベースのマルウェア イベントの場合、このユーザはネットワーク検出によって判別されます。ユーザが宛先ホストに関連付けられているため、ユーザがマルウェア ファイルをアップロードしたマルウェア イベントに、ユーザは関連付けられていません。 エンドポイントベースのマルウェア イベントの場合、FireAMP コネクタがユーザ名を判別します。FireAMPユーザをユーザ検出または制御に関連付けることは**できません**。それらは [Users] テーブルに含まれず、それらのユーザの詳細を表示することもできません。	yes	yes	no
Event Type	マルウェア イベントのタイプ。イベント タイプの完全なリストについては、マルウェア イベントのタイプ（40-27 ページ）を参照してください。	yes	yes	yes

表 40-3　マルウェア イベント フィールド（続き）

フィールド	説明	ネットワーク	エンドポイント	クラウドからのレトロスペクティブ
Event Subtype	マルウェア検出につながった FireAMP アクション（`Create`、`Execute`、`Move`、または `Scan` など）。	no	yes	no
Threat Name	検出されたマルウェアの名前。	yes	yes	yes
File Name	マルウェア ファイルの名前。	yes	yes	no
File Disposition	以下のファイル性質のいずれかです。 • **マルウェア**は、クラウドでそのファイルがマルウェアとして分類されていること、またはファイルの脅威スコアが、ファイル ポリシーで定義されたマルウェアしきい値を超えていることを示します。 • **クリーン**は、クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。 • **不明**は、クラウドが性質を割り当てる前にマルウェア クラウド ルックアップが行われたことを示します。ファイルは分類されていません。 • **カスタム検出**は、ユーザがカスタム検出リストにファイルを追加したことを示します。 • **使用不可**は、Defense Centerがマルウェア クラウド ルックアップを実行できなかったことを示します。この性質で見られるイベントはごくわずかである可能性があります。これは予期された動作です。 Clean のファイルがマルウェア テーブルに含められるのは、そのファイルが Clean に変更された場合だけです。遡及的マルウェア イベント（40-19 ページ）を参照してください。	yes	no	yes
File SHA256	ファイルの SHA-256 ハッシュ値と、最後に検出されたファイル イベントおよびファイル性質を表すネットワーク ファイル トラジェクトリ アイコン。 ネットワーク ファイル トラジェクトリを表示するには、トラジェクトリ アイコンをクリックします。詳細については、ネットワーク ファイル トラジェクトリの分析（40-40 ページ）を参照してください。	yes	yes	yes
Threat Score	そのファイルに関連する最新の脅威スコア： • `Low`（●○○○） • `Medium`（●●○○） • `High`（●●●○） • `Very High`（●●●●） 動的分析のサマリー レポートを表示するには、脅威スコア アイコンをクリックします。	yes	no	no

表 40-3　マルウェア イベント フィールド（続き）

フィールド	説明	ネットワーク	エンドポイント	クラウドからのレトロスペクティブ
File Path	マルウェア ファイルのファイル パス（ファイル名を含まない）。	no	yes	no
File Type	マルウェア ファイルのファイル タイプ（HTML や MSEXE など）。	yes	yes	no
File Type Category	ファイル タイプの一般的なカテゴリ（Office Documents、Archive、Multimedia、Executables、PDF files、Encoded、Graphics、System Files など）。	yes	yes	no
File Timestamp	マルウェア ファイルが作成された日時。	no	yes	no
File Size (KB)	マルウェア ファイルのサイズ（KB 単位）。	yes	yes	no
File URI	マルウェア ファイルの送信元の URI（ファイルをダウンロードした URL など）。	yes	no	no
Archive Name	マルウェア ファイルが関連付けられているアーカイブ ファイル（存在する場合）の名前（archive.zip など）。	yes	yes	no
Archive SHA256	マルウェア ファイルが関連付けられているアーカイブ ファイル（存在する場合）の SHA256 ハッシュ値。アーカイブ ファイルの内容を表示するには、アーカイブ ファイルのイベント ビューア行を右クリックしてコンテキスト メニューを開いてから、[View Archive Contents] をクリックします。詳細については、アーカイブ ファイルの内容の表示（37-24 ページ）を参照してください。	yes	yes	no
Archive Depth	アーカイブ ファイル内でファイルがネストされたレベル（存在する場合）。たとえば、1 や 3 など。	yes	yes	no
Application File Name	検出が行われたときに、マルウェア ファイルにアクセスしていたクライアント アプリケーション。これらのアプリケーションはネットワーク検出またはアプリケーション制御とは関係**ありません**。	no	yes	no
Application File SHA256	検出が行われたときに、FireAMP で検出された、または隔離されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。	no	yes	no
アプリケーション プロトコル	管理対象デバイスがマルウェア ファイルを検出したトラフィックで使用されるアプリケーション プロトコル。	yes	no	no
Application Protocol、Client、Web Application Category、Tag	アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。表 45-2（45-12 ページ）を参照してください。	yes	no	yes
クライアント	1 つのホストで実行され、ファイルを送信するためにサーバに依存するクライアント アプリケーション。	yes	no	yes
Web アプリケーション	接続で検出された HTTP トラフィックについて、内容を表すまたは URL を要求したアプリケーション。	yes	no	yes

表 40-3　マルウェア イベント フィールド（続き）

フィールド	説明	ネットワーク	エンドポイント	クラウドからのレトロスペクティブ
IOC	マルウェア イベントが、接続に関与したホストに対する侵害の痕跡 (IOC) をトリガーしたかどうか。エンドポイントベースのマルウェア検出が IOC ルールをトリガーした場合、タイプ `FireAMP IOC` で、完全なマルウェア イベントが生成されます。IOC の詳細については、侵害の兆候について（45-22 ページ）を参照してください。	yes	yes	yes
Application Risk	接続で検出されたアプリケーション トラフィックに関連するリスク：`Very High`、`High`、`Medium`、`Low`、または `Very Low`。接続で検出されたアプリケーションのタイプごとに、関連するリスクがあります。このフィールドでは、それらのうち最も高いものが表示されます。詳細については、表 45-2（45-12 ページ）を参照してください。	yes	no	yes
Business Relevance	接続で検出されたアプリケーション トラフィックに関連するビジネス関連性：`Very High`、`High`、`Medium`、`Low`、または `Very Low`。接続で検出されたアプリケーションのタイプごとに、関連するビジネス関連性があります。このフィールドでは、それらのうち最も低いもの（関連が最も低い）が表示されます。詳細については、表 45-2（45-12 ページ）を参照してください。	yes	no	yes
Detector	マルウェアを識別した FireAMP ディテクタ（ClamAV、Spero、SHA など）。	no	yes	no
メッセージ	マルウェア イベントに関連する追加情報。 ネットワークベースのマルウェア イベントの場合、このフィールドにデータが入れられるのは、性質が変更されたファイルだけです。遡及的マルウェア イベント（40-19 ページ）を参照してください。	yes	yes	no
FireAMP クラウド	イベントが発信された FireAMP クラウドの名前。	no	yes	no
デバイス	ネットワークベースのマルウェア イベントの場合、マルウェア ファイルを検出したデバイスの名前。 エンドポイントベースのマルウェア イベントおよびクラウドによって生成される遡及的マルウェア イベントの場合、Defense Centerの名前。	yes	yes	yes
セキュリティ コンテキスト	トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。システムがこのフィールドにデータを設定するのは、マルチコンテキスト モードの ASA FirePOWER デバイスだけです。	yes	yes	yes
Count	各行の情報に一致するイベントの数。このフィールドが表示されるのは、2 つ以上の同一の行を作成する制限を適用した後です。	n/a	n/a	n/a

マルウェア イベントのタイプ

ライセンス： Malware または任意

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

ネットワークベースのマルウェア イベントの場合、イベントのタイプは以下のいずれかになります。

- Threat Detected in Network File Transfer
- Threat Detected in Network File Transfer (retrospective)

エンドポイントベースのマルウェア イベントは、以下のタイプのいずれかになります。

- Blocked Execution
- Cloud Recall Quarantine
- Cloud Recall Quarantine Attempt Failed
- Cloud Recall Quarantine Started
- Cloud Recall Restore from Quarantine
- Cloud Recall Restore from Quarantine Failed
- Cloud Recall Restore from Quarantine Started
- FireAMP IOC
- Quarantine Failure
- Quarantined Item Restored
- Quarantine Restore Failed
- Quarantine Restore Started
- Scan Completed, No Detections
- Scan Completed With Detections
- Scan Failed
- Scan Started
- Threat Detected
- Threat Detected in Exclusion
- Threat Quarantined

ファイルのトラジェクトリ マップにマルウェア イベントが含まれている場合、イベントのタイプは、Threat Detected in Network File Transfer、Threat Detected in Network File Transfer (retrospective)、Threat Detected、Threat Detected in Exclusion、Threat Quarantined のいずれかになります。詳細については、「ネットワーク ファイル トラジェクトリの操作（40-37 ページ）」を参照してください。

シリーズ 2 デバイス、Cisco NGIPS for Blue Coat X-Series、および DC500 Defense Center は、ネットワークベースのマルウェア保護をサポートしていません。これは、表示されるデータに影響を及ぼす場合があるので注意してください。たとえば、シリーズ 2 デバイスだけを管理するシリーズ 3 Defense Centerは、エンドポイントベースのマルウェア イベントだけを表示できます。

マルウェア イベントの検索

ライセンス：Malware または任意

Defense Centerの [Search] ページを使用して、特定のマルウェア イベントを検索し、その結果をイベント ビューアーで表示できます。また、後で再利用するために検索条件を保存できます。[Custom Analysis] ダッシュボード ウィジェット、レポート テンプレート、カスタム ユーザ ロールも、保存した検索を使用できます。

サンプルとしてシステムに付属している検索には、[Saved Searches] リストで（`Cisco`）というラベルが付いています。

覚えておくべき点として、検索結果は、検索するイベントの使用可能なデータに依存します。つまり、使用可能なデータによっては、検索の制限が適用されないことがあります。たとえば、エンドポイントベースのマルウェア イベントは、ネットワーク トラフィックを検査する管理対象デバイスの結果として生成されないため、接続情報（ポート、アプリケーション プロトコルなど）は含まれません。

一般的な検索の構文

それぞれの検索フィールドの隣には、使用できる構文の例が表示されます。検索条件を入力する場合、次の点に注意してください。

- すべてのフィールドで否定（`!`）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「`A`」または「`B`」または「`C, D, E`」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク（`*`）を受け入れます。
- フィールドでその情報を利用できないイベントを示すには、そのフィールドで `n/a` を指定します。フィールドに情報が入力されているイベントを示すには `!n/a` を使用します。
- 特定のデバイス、およびグループ、スタック、またはクラスタ内のデバイスを検索するには、デバイス フィールドを使用します。検索での FireSIGHT システムによるデバイス フィールドの処理方法については、検索でのデバイスの指定（60-7 ページ）を参照してください。
- オブジェクトを検索条件として使用するには、検索フィールドの隣にあるオブジェクトの追加アイコン（ ＋ ）をクリックします。

検索でのオブジェクトの使用など、検索構文の詳細については、イベントの検索（60-1 ページ）を参照してください。

マルウェア イベントの特別な検索構文

前述の一般的な検索構文を補うために、以下のリストでは、マルウェア イベントの特別な検索構文について説明しています。

Sending/Receiving IP

システムは [Sending IP] または [Receiving IP] が指定した IP アドレスと一致するすべてのイベントを返します。

イベント タイプ

特定のマルウェア イベント タイプのイベントを検索する場合（マルウェア イベントのタイプ（40-27 ページ）を参照）、イベント タイプを引用符で囲みます（`"Scan Completed With Detection"`など）。そうしないと、システムは部分一致を実行します。つまり、同じストリングで引用符を使用しない場合、システムは次のタイプのイベントを返します。

- `Scan Completed, No Detections`
- `Scan Completed With Detection`

Initiator/Responder Continent

システムは [Initiator Continent] または [Responder Continent] が指定した大陸と一致するすべてのイベントを返します。

Initiator/Responder Country

システムは、[Initiator Country] または [Responder Country] が、指定した国に一致するすべてのイベントを返します。

URI または Message

システムは部分一致を実行します。つまり、アスタリスクを使用せずに、フィールドの内容の全部または一部を検索できます。

The SSL Actual Action taken

システムが指定したアクションを適用した暗号化されたトラフィックのマルウェア イベントを表示するには、次のキーワードのいずれかを入力します。

- [Do not Decrypt] は、システムが復号化しなかった接続を表します。
- [Block] および [Block with reset] は、ブロックされた暗号化接続を表します。
- [Decrypt (Known Key)] は、既知の秘密キーを使用して復号化された着信接続を表します。
- [Decrypt (Replace Key)] は、置き換えられた公開キーと自己署名サーバ証明書を使用して復号化された発信接続を表します。
- [Decrypt (Resign)] は、再署名サーバ証明書を使用して復号化された発信接続を表します。

このカラムは、マルウェア イベントのテーブル ビューに表示されません。

The SSL Failure Reason

システムが指定された理由で復号化に失敗した暗号化トラフィックのマルウェア イベントを表示するには、次のキーワードのいずれかを入力します。

- `Unknown`
- `No Match`

- Success
- Uncached Session
- Unknown Cipher Suite
- Unsupported Cipher Suite
- Unsupported SSL Version
- SSL Compression Used
- Session Undecryptable in Passive Mode
- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup
- Internal Error
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- Invalid Action

このカラムは、マルウェア イベントのテーブル ビューに表示されません。

The SSL Subject Country

証明書サブジェクトの国に関連付けられている暗号化されたトラフィックのマルウェア イベントを表示するには、2 文字の ISO 3166-1 アルファ 2 国番号を入力します。

このカラムは、マルウェア イベントのテーブル ビューに表示されません。

The SSL Issuer Country

証明書発行者の国に関連付けられている暗号化されたトラフィックを表示するには、2 文字の ISO 3166-1 アルファ 2 国番号を入力します。

このカラムは、マルウェア イベントのテーブル ビューに表示されません。

SSL Certificate Fingerprint

証明書に関連付けられているトラフィックを表示するには、その証明書の認証に使用される SHA ハッシュ値を入力するか、または貼り付けます。

このカラムは、マルウェア イベントのテーブル ビューに表示されません。

SSL Public Key Fingerprint

証明書に関連付けられているトラフィックを表示するには、その証明書に含まれている公開キーの認証に使用される SHA ハッシュ値を入力するか、または貼り付けます。

このカラムは、マルウェア イベントのテーブル ビューに表示されません。

マルウェア イベントを検索するには、以下を行います。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　テーブル ドロップダウン リストから [Malware Events] を選択します。

ページが適切な制約によって更新されます。

ステップ 3　次の項に記載されているように、該当するフィールドに検索基準を入力します。

- マルウェア イベント テーブルのフィールドの詳細については、マルウェア イベント フィールドの表を参照してください。
- マルウェア イベントの特別な検索構文については、マルウェア イベントの特別な検索構文（40-29 ページ）を参照してください。
- 公開キー証明書に関連するフィールドについては、暗号化接続に関連付けられた証明書の表示（39-33 ページ）を参照してください。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。または、すべてのユーザに対し検索を保存するにはこのチェックボックスをオフのままにします。

ヒント　カスタム ユーザ ロールに対するデータ制限として検索を使用する場合は、プライベート検索として保存する**必要があります**。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。
- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save as New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

検索結果は現在の時刻範囲によって制約されて、デフォルトのマルウェア イベントのワークフローに表示されます。

キャプチャ ファイルの操作

ライセンス： Malware

サポートされるデバイス： すべて（シリーズ 2 または X-Series を除く）

サポートされる防御センター： すべて（DC500 を除く）

システムは、現在適用されているファイル ポリシーのルールに従って、管理対象デバイスがネットワーク トラフィック内のファイルをキャプチャしたときに記録を行います。イベント ビューアから、キャプチャ ファイルに関連した情報（SHA-256 値に関連した最新のファイル名、ファイルの性質および脅威スコア、ファイル ストレージのステータス、アーカイブ インスペクションのステータス、ファイルが動的分析のために手動で送信されたかなど）を表示できます。

注 マルウェアはキャプチャされる前に検出される必要があるため、マルウェアを含むデバイスでキャプチャされたファイルは、ファイル イベントとマルウェア イベントの両方を生成します。詳細については、ファイル イベントの操作（40-8 ページ）およびマルウェア イベントの操作（40-17 ページ）を参照してください。

Defense Centerのイベント ビューアーを使用して、キャプチャされたファイルの表示および検索を行ったり、キャプチャされたファイルを動的分析のために送信したりできます。さらに、Files Dashboard では、ネットワークで検出されたファイル（マルウェア ファイルを含む）に関する詳細情報を、図やグラフを使って一目で知ることができます。

詳細については、以下を参照してください。

- キャプチャ ファイルの表示（40-32 ページ）
- キャプチャ ファイル テーブルについて（40-33 ページ）
- キャプチャ ファイルの検索（40-35 ページ）

キャプチャ ファイルの表示

ライセンス： Malware

FireSIGHT システムのイベント ビューアーでは、キャプチャ イベントをテーブルの形で表示したり、分析に関連した情報に応じてイベント ビューを操作したりすることができます。

キャプチャ ファイルにアクセスしたときに表示されるページは、ワークフローによって異なります。ワークフローは、大まかなビューから詳細なビューに移動してイベントを評価するために使用できる、一連のページです。システムには、キャプチャ ファイル用の以下の定義済みのワークフローが付属しています。

- [Captured File Summary]（デフォルト）：タイプ、カテゴリー、および脅威スコアに基づく、キャプチャ ファイルの概要を提供します。
- [Dynamic Analysis Status]：動的分析のために送信したかどうかに基づいて、キャプチャ ファイルのカウントを提供します。

特有の必要にかなった情報だけを表示するカスタム ワークフローを作成することもできます。カスタム ワークフローを含む、さまざまなデフォルト ワークフローの指定の詳細については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

FireSIGHT システム は、Unicode（UTF8）ファイル名の表示および入力を Web インターフェイスのすべてのエリア（イベント ビューアー、イベント検索、ダッシュボード、Context Explorer など）でサポートしています。ただし、PDF 形式で生成したレポートでは Unicode がサポートされないので注意してください。PDF レポートでは、Unicode ファイル名は翻字形式で表示されます。詳細については、レポートの生成と表示（57-28 ページ）を参照してください。

イベント ビューアを使用して、以下を行うことができます。

- イベントを検索、ソート、制約、また表示するイベントの時間範囲を変更する
- 表示される列の指定（テーブル ビューのみ）
- 同じワークフロー内のさまざまなワークフロー ページを使用したイベントの表示
- 別のワークフローを一緒に使用してイベントを表示する
- 特定の値に制約して、ワークフロー内のページからページへドリルダウンする
- 後で同じデータに戻る（存在している場合）ための、現在のページおよび制限のブックマーク
- ファイルのトラジェクトリの表示
- アーカイブ ファイルの内容とインスペクションのステータスの表示
- ファイル リストへのファイルの追加、ファイルのダウンロード、動的分析のためのファイルの送信、ファイルの SHA-256 値のフルテキストの表示
- ファイルの動的分析のサマリー レポート（使用可能な場合）の表示
- 動的分析のための最大 25 個のファイルの送信
- 現在の制限を使用したレポート テンプレートの作成

シリーズ 2 デバイス、Cisco NGIPS for Blue Coat X-Series、および DC500 Defense Center は、ネットワークベースのマルウェア保護およびアーカイブ ファイル インスペクションをサポートしていません。これは、表示されるデータに影響を及ぼす場合があるので注意してください。たとえば、シリーズ 2 デバイスだけを管理するシリーズ 3 Defense Centerは、キャプチャ ファイルを表示できません。

カスタム ワークフローの作成など、イベント ビューアの使用の詳細については、ワークフローの概要と使用（58-1 ページ）を参照してください。

ファイル イベントを表示するには、以下を行います。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Files] > [Captured Files] を選択します。

デフォルトのファイル イベントのワークフローの最初のページが表示されます。表示される列の詳細については、キャプチャ ファイル テーブルについて（40-33 ページ）を参照してください。

キャプチャ ファイル テーブルについて

ライセンス： Malware

Defense Centerは、適用されているファイル ポリシーの設定に従って、監視されているネットワーク トラフィックで送信されるファイルを管理対象デバイスがキャプチャしたときに記録を行います。

キャプチャされたファイルのテーブル ビューは、定義済みファイル イベントのワークフローの最後のページであり、カスタム ワークフローに追加できます。このテーブル ビューには、ファイル テーブルの各フィールドの列が含まれます。キャプチャ ファイルのテーブル ビューのいくつかのフィールドは、デフォルトで表示されます。セッションの期間中にフィールドを有効にするには、展開矢印( )をクリックして検索の制限を展開してから、[Disabled Columns] の下の列名をクリックします。以下の表は、キャプチャ ファイル フィールドについて説明しています。

表 40-4　キャプチャ ファイル フィールド

フィールド	説明
Last Changed	このファイルに関連した情報が最後に更新された時刻。
File Name	ファイルの SHA-256 ハッシュ値に関連した、最後に検出されたファイル名。
処理	以下のファイル性質のいずれかです。 • **マルウェア**は、クラウドでそのファイルがマルウェアとして分類されていること、またはファイルの脅威スコアが、ファイル ポリシーで定義されたマルウェアしきい値を超えていることを示します。 • **クリーン**は、クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。 • **不明**は、クラウドが性質を割り当てる前にマルウェア クラウド ルックアップが行われたことを示します。ファイルは分類されていません。 • **カスタム検出**は、ユーザがカスタム検出リストにファイルを追加したことを示します。 • **使用不可**は、Defense Centerがマルウェア クラウド ルックアップを実行できなかったことを示します。この性質で見られるイベントはごくわずかである可能性があります。これは予期された動作です。 • N/A は、ファイル検出またはファイル ブロック ルールがファイルを処理し、Defense Centerがマルウェア クラウド ルックアップを行わなかったことを示します。
SHA256	ファイルの SHA-256 ハッシュ値と、最後に検出されたファイル イベントおよびファイル性質を表すネットワーク ファイル トラジェクトリ アイコン。 ネットワーク ファイル トラジェクトリを表示するには、トラジェクトリ アイコンをクリックします。詳細については、ネットワーク ファイル トラジェクトリの分析(40-40 ページ)を参照してください。
Threat Score	そのファイルに関連する最新の脅威スコア: • Low( ) • Medium( ) • High( ) • Very High( ) 動的分析のサマリー レポートを表示するには、脅威スコア アイコンをクリックします。
タイプ	ファイルのタイプ(HTML や MSEXE など)。
カテゴリ	ファイル タイプの一般的なカテゴリ(Office Documents、Archive、Multimedia、Executables、PDF files、Encoded、Graphics、System Files など)。
Storage Status	ファイルが管理対象デバイスに保存されているかどうか。

表 40-4　キャプチャ ファイル フィールド（続き）

フィールド	説明
Archive Inspection Status	アーカイブ ファイルでの、アーカイブ インスペクションのステータス： • [Pending] は、システムがアーカイブ ファイルとその内容をまだ検査していることを示しています。ファイルが再びシステムを通過する場合、完全な情報が使用可能になります。 • [Extracted] は、システムがアーカイブの内容を抽出し、検査できたことを示しています。 • [Failed] は、まれなケースですが、システムが抽出を処理できない場合に発生します。 • [Depth Exceeded] は、許可された最大深さを超えるネストされたアーカイブ ファイルがアーカイブに含まれていることを示しています。 • [Encrypted] は、アーカイブ ファイルの内容が暗号化されていて、検査できなかったことを示しています。 • [Not Inspectable] は、システムがアーカイブの内容を抽出して検査しなかったことを示しています。このステータスの主な理由としては、ポリシー ルール アクション、ポリシー設定、破損ファイルの 3 つがあります。 アーカイブ ファイルの内容を表示するには、そのイベント ビューア行を右クリックしてコンテキスト メニューを開いてから、[View Archive Contents] を選択します。詳細については、アーカイブ ファイルのインスペクション オプションの設定（37-22 ページ）を参照してください。
Analysis Status	ファイルが動的分析のために送信されているかどうか。
Last Sent	ファイルが動的分析のためにクラウドに最後に送信された時刻。

キャプチャ ファイルの検索

ライセンス：Malware

Defense Centerの [Search] ページを使用して、特定のキャプチャ ファイルを検索し、その結果をイベント ビューアーで表示できます。また、後で再利用するために検索条件を保存できます。[Custom Analysis] ダッシュボード ウィジェット、レポート テンプレート、カスタム ユーザ ロールも、保存した検索を使用できます。

覚えておくべき点として、検索結果は、検索するイベントの使用可能なデータに依存します。つまり、使用可能なデータによっては、検索の制限が適用されないことがあります。たとえば、ファイルが動的分析のために送信されていない場合は、関連する脅威スコアがない場合があります。

一般的な検索の構文

それぞれの検索フィールドの隣には、使用できる構文の例が表示されます。検索条件を入力する場合、次の点に注意してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「`A`」または「`B`」または「`C, D, E`」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。

  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク(*)を使用できます。
- そのフィールドで情報を利用できないイベントを特定するには、フィールドに `n/a` を指定します。そのフィールドに値が入力されているイベントを特定するには、`!n/a` を使用します。
- 検索条件としてオブジェクトを使用するには、検索フィールドの横にあるオブジェクト追加アイコン(+)をクリックします。

検索でのオブジェクトの使用など、検索構文の詳細については、イベントの検索(60-1 ページ)を参照してください。

キャプチャ ファイルの特別な検索構文

前述の一般的な検索構文を補うために、以下の表では、キャプチャ ファイルの特別な検索構文について説明しています。

表 40-5　キャプチャ ファイルの特別な検索構文

検索条件	特別な構文
Storage Status	以下の 1 つ以上を指定してください。 • `File Stored`:デバイスに保存されたすべてのキャプチャ ファイルを返します • `Unable to Store File`:デバイスに保存されなかったすべてのキャプチャ ファイルを返します
Dynamic Analysis Status	以下の 1 つ以上を指定してください。 • `Sent for Analysis`:動的分析のためにキューに入れられたすべてのキャプチャ ファイルを返します • `Not Sent for Analysis`:動的分析のために送信されなかったすべてのキャプチャ ファイルを返します • `Analysis Complete`:動的分析のために送信されず、脅威スコアおよび動的分析のサマリー レポートを受け取った、すべてのキャプチャ ファイルを返します • `Previously Analyzed` :再度動的分析のために送信しようとした、キャッシュに入れられた脅威スコアを持つすべてのファイルを返します • `Failure (Analysis Timeout)`:クラウドがまだ結果を返していない動的分析のために送信されたすべてのキャプチャ ファイルを返します • `Failure (Network Issue)`:ネットワーク接続の障害のために動的分析に送信できなかったすべてのファイルを返します • `Failure (Cannot Run File)`:クラウドがテスト環境で実行できなかった動的分析のために送信されたすべてのファイルを返します

キャプチャ ファイルを検索するには、以下を行います。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　テーブル ドロップダウン リストから [Captured Files] を選択します。

ページが適切な制約によって更新されます。

ステップ 3　該当するフィールドに検索基準を入力します。

キャプチャ ファイル テーブルのフィールドの詳細については、キャプチャ ファイル フィールドの表を参照してください。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　カスタム ユーザ ロールに対するデータの制約として検索を使用する場合は、検索を非公開として保存する**必要があります**。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save as New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

検索結果は、現在の時刻範囲によって制限されるデフォルトのキャプチャ イベントのワークフローに表示されます。

ネットワーク ファイル トラジェクトリの操作

ライセンス： Malware または任意

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

ネットワーク ファイルのトラジェクトリ機能は、ネットワーク全体でホストがどのようにファイル（マルウェア ファイルを含む）を転送したかをマッピングします。このマップを使用して、どのホストがマルウェアを転送した可能性があるか、またどのホストにリスクがあるかを判別したり、ファイル転送の傾向を観察したりできます。

トラジェクトリ マップは、ファイルの転送データ、ファイルの性質、ファイル転送がブロックされたかどうか、ファイルが隔離されたかどうかをグラフにします。マップの作成に使用されるデータは、ネットワークベースのマルウェア イベント（システムがマルウェア クラウド ルックアップを実行してマルウェア性質を返したファイル イベント）から取得される場合も、マルウェアの検出およびブロックに関連した特定のエンドポイントベースのマルウェア イベント（Threat Detected または Threat Quarantined イベント タイプ）から取得される場合もあります。データ ポイント間の縦線は、ホスト間でのファイル転送を表します。データ ポイントをつなぐ横棒は、時間の経過に伴うホストのファイル アクティビティを示します。

システムがマルウェア クラウド ルックアップを実行できるファイル タイプの伝送を追跡できます。ファイルのトラジェクトリに直接アクセスするには、[Network File Trajectory List] ページ（[Analysis] > [Files] > [Network File Trajectory]）を使用して、特定のファイルを見つけることができます。さらに、侵入を分析して、関連するファイルのトラジェクトリを確認する場合、接続、ファイル、マルウェア イベントの Context Explorer、ダッシュボード、イベント ビューからファイルのトラジェクトリにアクセスできます。

単一のトランジェクトリ マップが表示するデータは、アプライアンスに適用されるライセンスによって異なります。次の表は、さまざまな種類のファイル トランジェクトリを追跡するのに必要なライセンスをリストしています。

表 40-6　　ネットワーク ファイル トランジェクトリのライセンス要件

表示対象	必要なライセンス
ネットワークベースのファイルおよびマルウェア トラジェクトリ	Malware
エンドポイントベースの脅威および隔離の追跡	任意（FireAMP サブスクリプションが必要）

詳細については、「マルウェア対策とファイル制御について（37-2 ページ）」を参照してください。

注意すべき点として、DC500 で Malware ライセンスは使用できず、シリーズ 2 デバイスまたは Cisco NGIPS for Blue Coat X-Series で Malware ライセンスを有効にすることもできないため、それらのアプライアンスを使用して、個々のファイルのキャプチャ/保存/ブロック、動的分析のためのファイルの送信、アーカイブ ファイルの内容の表示、マルウェア クラウド ルックアップを行うファイルのファイル トラジェクトリの表示を行うことはできません。ただし、エンドポイントベースの脅威および隔離の追跡のためにファイル トラジェクトリを表示することは可能です。

詳細については、次の項を参照してください。

- ネットワーク ファイル トラジェクトリの確認（40-38 ページ）
- ネットワーク ファイル トラジェクトリの分析（40-40 ページ）

ネットワーク ファイル トラジェクトリの確認

ライセンス： Malware または任意

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

キャプチャされたファイル、イベント イベント、およびマルウェア イベントを確認する際に、Context Explorer、適切に設定されたダッシュボード ウィジェット、さまざまなイベント ビューからファイルのトラジェクトリ マップを表示できます。また、最後に表示されたネットワーク ファイル トラジェクトリおよび最後に検出されたマルウェアを [Network File Trajectory List] ページから確認することもできます。

詳細については、次の項を参照してください。

- [Top File Names] グラフの表示（56-27 ページ）
- Context Explorer データのドリルダウン（56-40 ページ）
- Custom Analysis ウィジェットについて（55-12 ページ）
- アーカイブ ファイルのインスペクション オプションの設定（37-22 ページ）
- ファイル イベント テーブルについて（40-10 ページ）
- マルウェア イベント テーブルについて（40-21 ページ）
- キャプチャ ファイル テーブルについて（40-33 ページ）
- 接続およびセキュリティ インテリジェンスのイベントで利用可能な情報（39-12 ページ）
- ネットワーク ファイル トラジェクトリへのアクセス（40-39 ページ）

ネットワーク ファイル トラジェクトリへのアクセス

ライセンス： Malware または任意

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

[Network File Trajectory List] ページを使用して、最新の検出されたマルウェアを分析するため、または特定の脅威を追跡するために、ある SHA256 ハッシュ値を持つファイルを見つけることができます。

このページには、ネットワークで最後に検出されたマルウェアと最後に表示したトラジェクトリ マップのファイルが表示されます。これらのリストから、ネットワークでファイルが最後に発見されたのはいつか、ファイルの SHA-256 のハッシュ値、名前、タイプ、現在のファイル性質、内容（アーカイブ ファイルの場合）、ファイルに関連付けられたイベント数を表示できます。フィールドの詳細については、ファイル イベント テーブルについて（40-10 ページ）を参照してください。

また、このページに含まれる検索ボックスを使用して、SHA256 ハッシュ値またはファイル名に基づくか、ファイルを送信または受信するホストの IP アドレスで、ファイルを見つけることができます。ファイルを見つけたら、[File SHA256] 値をクリックして詳細なトラジェクトリ マップを表示できます。詳細については、「ネットワーク ファイル トラジェクトリの分析（40-40 ページ）」を参照してください。

FireSIGHT システム は、Unicode（UTF8）ファイル名の表示および入力を Web インターフェイスのすべてのエリア（イベント ビューアー、イベント検索、ダッシュボード、Context Explorer など）でサポートしています。ただし、PDF 形式で生成したレポートでは Unicode がサポートされないので注意してください。PDF レポートでは、Unicode ファイル名は翻字形式で表示されます。詳細については、レポートの生成と表示（57-28 ページ）を参照してください。

注意すべき点として、DC500 で Malware ライセンスは使用できず、シリーズ 2 デバイスまたは Cisco NGIPS for Blue Coat X-Series で Malware ライセンスを有効にすることもできないため、それらのアプライアンスを使用して、マルウェア クラウド ルックアップを行うファイルのファイル トラジェクトリを表示することはできません。

[Network File Trajectory List] ページからファイルを見つけるには、以下を行います。

アクセス： すべて

ステップ 1　[Analysis] > [Files] > [Network File Trajectory] を選択します。

[Network File Trajectory List] ページが表示され、最近表示したファイルと最近のマルウェアのリストが示されます。

ステップ 2　オプションで、追跡するファイルの完全な SHA256 ハッシュ値、ホスト IP アドレス、ファイル名を検索フィールドに入力して、Enter を押すこともできます。

[Query Results] ページが表示され、検索に一致するすべてのファイルがリストされます。1 つの結果だけが一致する場合、そのファイルの [Network File Trajectory] ページが表示されます。

ネットワーク ファイル トラジェクトリの分析

ライセンス： Malware または任意

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

詳細なネットワーク ファイル トラジェクトリを表示して、ネットワークを介してファイルを追跡できます。ファイルのトラジェクトリは、ファイルに関するサマリー情報を提供し、時間の経過に伴うデータ ポイントをグラフにしたマップを表示します。また、データ ポイントに関係したイベント データをテーブルにリストします。テーブルおよびマップを使用して、特定のファイル イベント、このファイルを転送または受信したネットワーク上のホスト、マップ内の関連するイベント、選択した値で制限されたテーブル内の他の関連するイベントを特定することができます。

注意すべき点として、DC500 で Malware ライセンスは使用できず、シリーズ 2 デバイスまたは Cisco NGIPS for Blue Coat X-Series で Malware ライセンスを有効にすることもできないため、それらのアプライアンスを使用して、マルウェア クラウド ルックアップを行うファイルのファイル トラジェクトリを表示することはできません。

詳細については、次の項を参照してください。

- サマリー情報（40-40 ページ）
- トラジェクトリ マップ（40-43 ページ）
- [Events] テーブル（40-46 ページ）

サマリー情報

ライセンス： Malware または任意

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

ファイルのトラジェクトリ ページには、ファイルに関する基本的な情報（ファイル識別情報、ネットワーク上でファイルが最初に発見された時間および最後に発見された時間、ファイルに関連したイベントおよびホストの数、ファイルの現在の性質など）が表示されます。このセクションから、管理対象デバイスがファイルを保存した場合に、そのファイルをローカルにダウンロードしたり、ファイルを動的分析用に送信したり、ファイルをファイル リストに追加したりできます。

ヒント　関連するファイル イベントを表示するには、フィールド値のリンクをクリックします。ファイル イベントのデフォルトのワークフローの最初のページが新しいウィンドウで開き、選択した値を含むすべてのファイル イベントも表示されます。

次の表では、サマリー情報フィールドについて説明されています。

表 40-7　ネットワーク ファイル トラジェクトリのサマリー情報フィールド

名前	説明
File SHA256	ファイルの SHA-256 ハッシュ値。 デフォルトで、ハッシュは簡略化された形式で表示されます。完全なハッシュ値を表示するには、その上にポインタを移動させます。複数の SHA256 ハッシュ値がファイル名に関連付けられている場合、リンクの上にポインタを移動されると、すべてのハッシュ値が表示されます。 ファイルのダウンロード アイコン ( ) をクリックすると、ファイルがローカル コンピュータにダウンロードされます。プロンプトが出力されたら、ファイルをダウンロードすることを確認します。ファイルを保存するには、ブラウザのプロンプトに従います。ファイルをダウンロードできない場合、このアイコンはグレー表示されます。 **注意**　Ciscoは、有害な結果が発生することがあるため、マルウェアをダウンロード**しない**ように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先をセキュアにするために必要な予防措置を行っていることを確認します。
File Names	ネットワーク上で発見された、イベントに関連したファイルの名前。 複数のファイル名が SHA256 ハッシュ値に関連付けられている場合、最後に検出されたファイル名がリストされます。[more] をクリックすると、これが展開されて、残りのファイル名が表示されます。
File Type	ファイルのタイプ（`HTML` や `MSEXE` など）。
File Category	ファイル タイプの一般的なカテゴリ（`Office Documents` や `System Files` など）。
Parent Application	検出が行われたときに、マルウェア ファイルにアクセスしていたクライアント アプリケーション。これらのアプリケーションはネットワーク検出またはアプリケーション制御とは関係**ありません**。 このフィールドは、エンドポイントベースのマルウェア イベントにだけ表示されます。
First Seen	管理対象デバイスまたは FireAMP コネクタがファイルを最初に検出した時刻と、そのファイルを最初にアップロードしたホストの IP アドレス。
Last Seen	管理対象デバイスまたは FireAMP コネクタがファイルを最後に検出した時刻と、そのファイルを最後にアップロードしたホストの IP アドレス。
Event Count	ファイルに関連付けられたネットワークで発見されたイベントの数、検出されたイベントの数が 250 を超える場合は、マップに表示されるイベントの数。
Seen On	ファイルを送信または受信したホストの数。1 つのホストが 1 つのファイルのアップロードおよびダウンロードを時を異にして行う場合があるため、ホストの合計数が、[Seen On Breakdown] フィールドの送信側の総数と受信側の総数の合計と一致しないことがあります。

表 40-7　ネットワーク ファイル トラジェクトリのサマリー情報フィールド（続き）

名前	説明
Seen On Breakdown	ファイルを送信したホストの数とファイルを受信したホストの数。
Current Disposition	以下のファイル性質のいずれかです。 • **マルウェア**は、クラウドでそのファイルがマルウェアとして分類されていること、またはファイルの脅威スコアが、ファイル ポリシーで定義されたマルウェアしきい値を超えていることを示します。 • **クリーン**は、クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。 • **不明**は、クラウドが性質を割り当てる前にマルウェア クラウド ルックアップが行われたことを示します。ファイルは分類されていません。 • **カスタム検出**は、ユーザがカスタム検出リストにファイルを追加したことを示します。 • **使用不可**は、Defense Centerがマルウェア クラウド ルックアップを実行できなかったことを示します。この性質で見られるイベントはごくわずかである可能性があります。これは予期された動作です。 • N/A は、ファイル検出またはファイル ブロック ルールがファイルを処理し、Defense Centerがマルウェア クラウド ルックアップを行わなかったことを示します。 クリーン リストまたはカスタム検出リストに対してファイルの追加や削除を行うには、編集アイコン（）をクリックします。 このフィールドは、ネットワークベースのマルウェア イベントにだけ表示されます。
Archive Contents	検査されたアーカイブ ファイルで、アーカイブに含まれているファイルの数。[Archive Contents] ウィンドウでコンテンツ ファイルの情報を表示するには、表示アイコン（）をクリックします。 アーカイブ ファイルのインスペクションの詳細については、アーカイブ ファイルのインスペクション オプションの設定（37-22 ページ）を参照してください。
Threat Name	ファイルに関連付けられたマルウェア脅威の名前。 このフィールドは、エンドポイントベースのマルウェア イベントにだけ表示されます。
Threat Score	ファイルの脅威スコア： • Low（） • Medium（） • High（） • Very High（） 動的分析のサマリー レポートを表示するには、脅威スコア アイコンをクリックします。 その脅威スコアのすべてのキャプチャ ファイルを表示するには、脅威スコア リンクをクリックします。 動的分析のためにクラウドにファイルを送信するには、クラウド アイコン（）をクリックします。ファイルを送信できない場合、またはクラウドに接続できない場合は、このアイコンはグレーで表示されます。

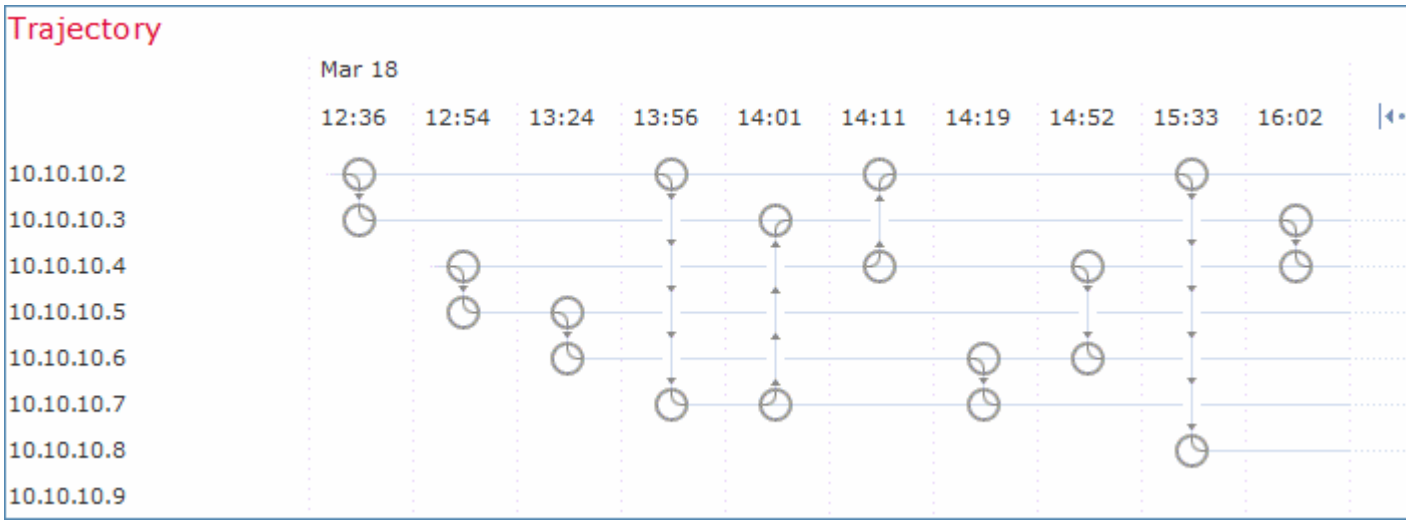
トラジェクトリ マップ

ライセンス： Malware または任意

サポートされるデバイス： 機能によって異なる

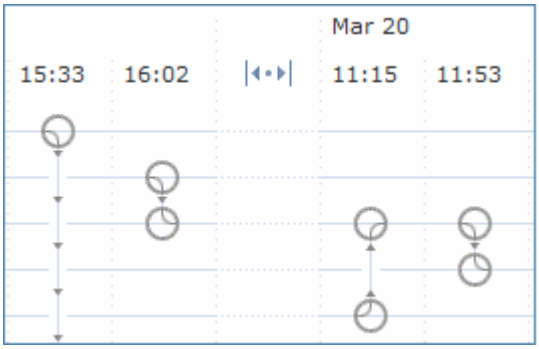
サポートされる防御センター： 機能によって異なる

ファイルのトラジェクトリ マップは、ネットワークで最初に検出された時点から直近までファイルを視覚的に追跡します。このマップは、ホストがファイルを転送または受信した時点、ファイルを転送した頻度、ファイルがブロックまたは隔離された時点を示します。また、そのファイルでファイル イベントが発生した頻度や、システムがファイルに性質または遡及的性質を割り当てた時点についても示します。マップでデータ ポイントを選択し、ホストがそのファイルを転送した最初のインスタンスに遡るパスを強調表示できます。また、このパスは、ファイルの送信側または受信側としてホストが関与する各オカレンスと交差します。次の図は、トラジェクトリ マップの例を示しています。



マップの Y 軸には、ファイルと対話したすべてのホストの IP アドレスがリストされます。IP アドレスは、システムがそのホストでファイルを最初に検出した時点に基づいて降順でリストされます。各行には、その IP アドレスに関連付けられたすべてのイベント（単一のファイル イベント、ファイル転送、遡及的イベント）が含まれます。X 軸には、システムが各イベントを検出した日時が含まれます。タイムスタンプは時間順にリストされます。複数のイベントが 1 分以内に発生する場合、すべてが同じ列内にリストされます。マップを左右および上下にスクロールして、イベントおよび IP アドレスをさらに表示できます。

マップには、ファイルの SHA256 ハッシュに関連した最大 250 のイベントが表示されます。イベントが 250 を超える場合、マップには最初の 10 個が表示され、余分のイベントは省略されて矢印アイコン（|◂▸|）が示されます。その後ろに、マップは残りの 240 個のイベントを表示します。次の図では、イベントが省略され、矢印アイコンが示されています。

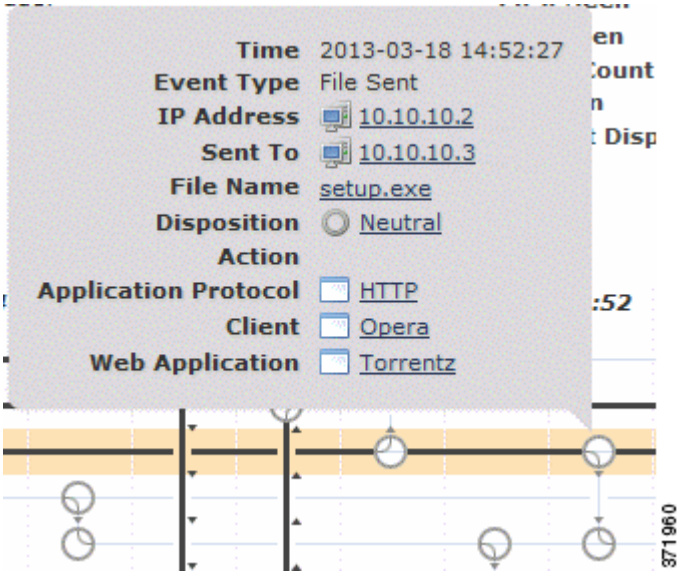


矢印アイコン(|◂•▸|)をクリックすると、[File Summary] イベント ビューで示されているすべてのイベントが表示されます。デフォルトの [File Events(ファイル イベント)] ワークフローの最初のページが新しいウィンドウで開き、ファイル タイプに基づいて制限されて、すべての余分のイベントが表示されます。エンドポイントベースのマルウェア イベントが表示されない場合、[Malware Events] テーブルに切り替えて、それらを表示する必要があります。

各データ ポイントは、イベントの他にファイル性質を表しています。マップの下の凡例を参照してください。たとえば、[Malware Block] イベント アイコンは、[Malicious Disposition] アイコンと [Block Event] アイコンを結合したものです。

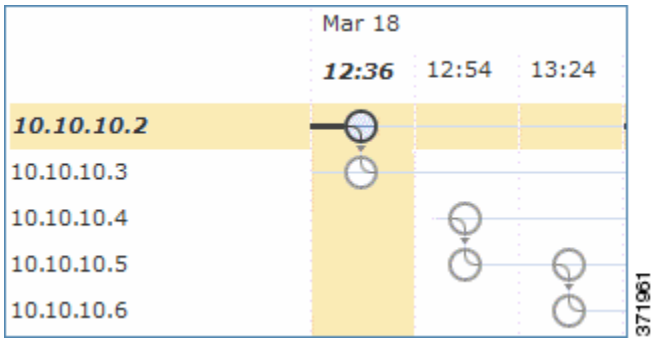
エンドポイントベースのマルウェア イベントには 1 つアイコンが含まれます。遡及的イベントでは、ファイルで検出された各ホストのコラムにアイコンが表示されます。ファイル転送イベントでは、縦線でつながれた 2 つのアイコン(ファイル送信アイコンとファイル受信アイコン)が常に含まれます。矢印は、送信側から受信側へのファイル転送方向を示します。

イベント アイコン( )上にポインタを移動させると、イベント アイコンのサマリー情報を表示できます。表示されるサマリー情報は、[Events] テーブルに表示される情報と一致しています。次の図は、イベント アイコンのサマリー情報を示しています。



イベントのサマリー情報のリンクをクリックすると、ファイル イベントのデフォルトのワークフローの最初のページが新しいウィンドウで開き、ファイル タイプに基づいて制限されて、すべての余分のイベントが表示されます。[File Summary] イベント ビューが新しいウィンドウで開きクリックした基準値と一致するすべてのファイル イベントが表示されます。

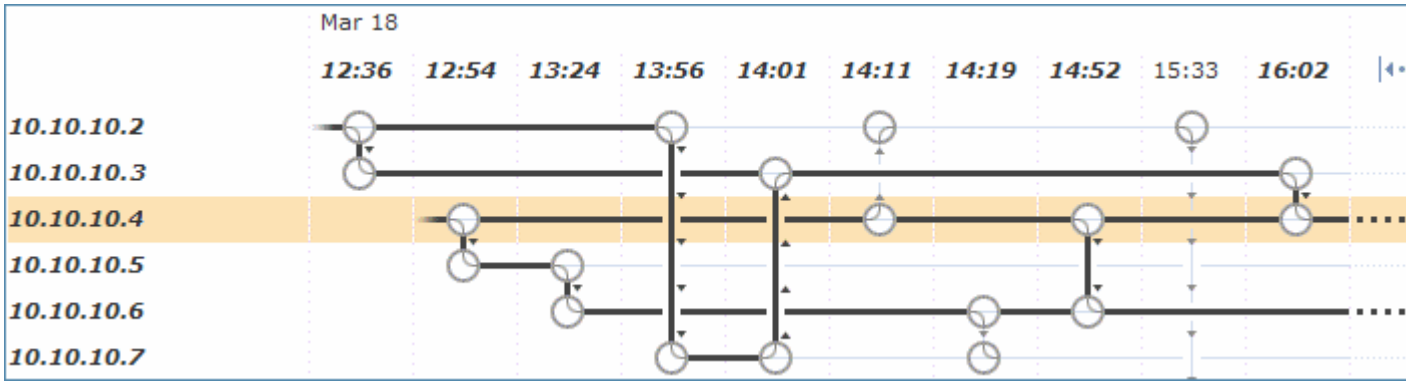
IP アドレスが関係するファイル イベントが最初に発生した時点を見つけるには、そのアドレスをクリックします。これにより、そのデータ ポイントへのパスが強調表示され、その最初のファイル イベントに関連した仲介ファイル イベントと IP アドレスがあればそれも強調表示されます。[Events] テーブルの対応するイベントも強調表示されます。そのデータ ポイントが現在表示されていない場合、表示されるまでマップがスクロールされます。次の図は、IP アドレスをクリックした後にパスが強調表示されている様子を示しています。



ネットワークを介したファイルの進行状況を追跡するために、データ ポイントをクリックして、選択したデータ ポイントに関連するすべてのデータ ポイントを含むパスを強調表示できます。これには、次のタイプのイベントに関連付けられたデータ ポイントが含まれます。

- 関連付けられている IP アドレスが送信側または受信側だったファイル転送
- 関連付けられている IP アドレスが関係するエンドポイントベースのマルウェア イベント
- 別の IP アドレスが関係する場合、その関連する IP アドレスが送信側または受信側であったすべてのファイル転送
- 別の IP アドレスが関係する場合、その他方の IP アドレスが関係するエンドポイントベースのマルウェア イベント

次の図は、イベント アイコンをクリックした後でパスが強調表示されている様子を示しています。



強調表示されたデータ ポイントに関連付けられたすべての IP アドレスとタイムスタンプも強調表示されます。[Events] テーブルの対応するイベントも強調表示されます。省略されたイベントがパスに含まれている場合、そのパス自体が点線で強調表示されます。省略されたイベントがパスを交差している場合がありますが、マップに表示されません。

[Events] テーブル

ライセンス： Malware または任意

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

[Events] テーブルには、マップ内の各データ ポイントに関するイベント情報がリストされます。列見出しをクリックすると、イベントを昇順または降順でソートできます。テーブル行を選択して、マップ内のデータ ポイントを強調表示できます。選択したファイル イベントが現在表示されていない場合、表示されるまでマップがスクロールされます。フィールドの詳細については、ファイル イベント テーブルについて (40-10 ページ) を参照してください。

侵入イベントの操作

FireSIGHT システムは、ホストとそのデータの可用性、整合性、および機密性に影響する可能性のあるトラフィックがないかどうか、ネットワークをモニタするのに役立ちます。主要なネットワーク セグメントに管理対象デバイスを配置すると、悪意のあるアクティビティを目的としてネットワークを通過するパケットを検査できます。このシステムには、攻撃者が開発したさまざまなエクスプロイトを検索するのに使用できるいくつかのメカニズムがあります。

システムは、潜在的な侵入を特定すると*侵入イベント*を生成します。これは、エクスプロイトの日付、時間、タイプ、および攻撃元とそのターゲットに関するコンテキスト情報のデータです。パケットベースのイベントの場合、イベントをトリガーしたパケットのコピーも記録されます。管理対象デバイスは、Defense Centerにイベントを送信します。ここで、集約データを確認し、ネットワーク アセットに対する攻撃を的確に把握できます。

管理対象デバイスをインライン型、スイッチ型、またはルート型の侵入システムとして展開することもできます。これにより、危険だと認識したパケットをドロップまたは置換するようデバイスを設定できます。

FireSIGHT システムは、ユーザが侵入イベントを確認し、ネットワーク環境とセキュリティ ポリシーのコンテキストでそのイベントが重要であるかどうかを評価するために必要なツールを提供します。これらのツールは次のとおりです。

- 管理対象デバイスでの現在のアクティビティの概要について説明するイベント要約ページ
- 選択した任意の期間に対して生成できるテキストベースおよびグラフィカルなレポート。独自のレポートを設計し、スケジュールされた間隔で実行されるよう設定することもできます
- 攻撃に関連したイベント データの収集に使用できるインシデント処理ツール。調査や応答のトラッキングに役立つ注記を追加することもできます
- SNMP、電子メール、および Syslog で設定できる自動アラート
- 特定の侵入イベントに対する応答や修復に使用できる自動化された相関ポリシー
- データをドリルダウンして、さらに調査したいイベントを特定するのに使用できる定義済みカスタム ワークフロー

詳細については、次の項を参照してください。

- 侵入イベントの統計の表示（41-2 ページ）は [Intrusion Event Statistics] ページについて説明しています。このページでは、アプライアンスのヘルスの概要とネットワークに対する上位の脅威の要約について説明します。
- 侵入イベントのパフォーマンスの表示（41-4 ページ）は、侵入イベントのパフォーマンス統計情報のグラフを生成する方法について説明します。
- 侵入イベント グラフの表示（41-9 ページ）は、経時的にイベントのトレンドを示すグラフを生成する方法について説明します。

- 侵入イベントの表示（41-9 ページ）は、Web インターフェイスを使用して侵入イベントを表示および調査する方法について説明します。
- 侵入イベントのワークフロー ページについて（41-18 ページ）は、侵入イベント ワークフローで使用可能なさまざまなページと、それらを使用して侵入イベントを分析する方法について説明します。
- ドリルダウン ページとテーブル ビュー ページの使用（41-20 ページ）は、侵入イベント ワークフローでの 2 つのタイプのページの機能について説明します。
- パケット ビューの使用（41-23 ページ）は、侵入イベントのパケット ビューの使用方法について説明します。
- 影響レベルを使用してイベントを評価する（41-39 ページ）は、影響レベルを使用して侵入イベントを評価する方法について説明します。
- プリプロセッサ イベントの読み取り（41-41 ページ）は、プリプロセッサ ルールによって生成されるイベントを読み取る方法について説明します。
- 侵入イベントの検索（41-44 ページ）は、検索機能を使用して侵入イベントのリストを特定の条件に制限する方法について説明します。
- クリップボードの使用（41-52 ページ）は、後でイベントをインシデントに追加できるように、クリップボードと呼ばれる保存エリアに侵入イベントを追加する方法について説明します。このセクションでは、クリップボードの内容に基づいてイベント レポートを生成する方法についても説明します。

次のセクションも参照してください。

- インシデント対応（42-1 ページ）は、インシデントの処理についての詳細と、インシデントを使用してイベント分析の進行状況をトラックする方法について説明します。
- 侵入ルールの外部アラートの設定（44-1 ページ）は、自動アラートの詳細について説明します。
- レポートの操作（57-1 ページ）は、侵入イベントのレポートの詳細について説明します。
- 地理情報の使用（58-23 ページ）は、侵入イベントの位置情報の詳細について説明します。

侵入イベントの統計の表示

ライセンス： Protection

[Intrusion Event Statistics] ページは、アプライアンスの現在の状態の概要と、ネットワークで生成されたすべての侵入イベントを表示します。

[Intrusion Event Statistics] ページには、次の 3 つのメイン エリアがあります。

- ホスト統計情報（41-3 ページ）は、[Host Statistics] セクションについて説明します。このセクションは、アプライアンスに関する情報、および、Defense Centerの場合はその管理対象デバイスに関する情報を表示します。
- イベントの概要（41-4 ページ）は、イベント データベース情報の概要を表示する [Event Overview] について説明します。
- イベント統計情報（41-4 ページ）は、上位 10 件のイベントなど、イベント データベースの情報の詳細を具体的に表示する [Event Statistics] について説明します。

このページの IP アドレス、ポート、プロトコル、イベント メッセージなどはそれぞれリンクになっています。関連イベントの情報を表示するには、任意のリンクをクリックします。たとえば、上位 10 個の宛先ポートのいずれかが `80(http)/tcp` である場合、そのリンクをクリックすると、デフォルトの侵入イベント ワークフローの最初のページが表示され、そのポートをターゲットとするイベントがリストされます。現在の時刻範囲で表示されるのはイベント（およびイベント

を生成する管理対象デバイス）のみであることに注意してください。さらに、確認済みマークを付けた侵入イベントも統計に引き続き表示されます。たとえば、現在の時刻範囲が過去 1 時間であり、最初のイベントが 5 時間前に生成された場合、[First Event] リンクをクリックすると、そのイベントは時刻範囲を変更するまでイベント ページには表示されません。

侵入イベントの統計情報を表示する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Overview] > [Summary] > [Intrusion Event Statistics] を選択します。

[Intrusion Event Statistics] ページが表示されます。

ステップ 2　ページの上部にある 2 つの選択ボックスから、統計を表示するゾーンおよびデバイスを選択するか、[All Security Zones] および [All Devices] を選択して、侵入イベントを収集するすべてのデバイスの統計を表示します。

ステップ 3　[Get Statistics] をクリックします。

[Intrusion Event Statistics] ページは、選択したデバイスのデータに表示が更新されます。

ヒント　カスタム時刻範囲からデータを表示するには、右上のページ エリアのリンクをクリックし、イベント時間の制約の設定（58-26 ページ）にある指示に従います。

ステップ 4　[Intrusion Event Statistics] ページで表示される統計の詳細については、次のセクションを参照してください。

- ホスト統計情報（41-3 ページ）
- イベントの概要（41-4 ページ）
- イベント統計情報（41-4 ページ）

ホスト統計情報

ライセンス：Protection

[Intrusion Event Statistics] ページの [Host Statistics] セクションは、アプライアンス自体に関する情報を提供します。Defense Centerでは、このセクションはすべての管理対象デバイスに関する情報も提供します。

この情報には、次の内容が含まれます。

- [Time] は、アプライアンス上の現在の時刻を表示します。
- [Uptime] は、アプライアンス自体が再起動してから経過した日数、時間、および分数を示します。Defense Centerでは、[Uptime] に各管理対象デバイスの最終起動時刻、ログインしたユーザの数、および負荷平均も示されます。
- [Disk Usage] は使用中のディスクの割合を示します。
- [Memory Usage] は使用中のシステム メモリの割合を示します。
- [Load Average] は、過去 1 分間、5 分間、15 分間の CPU キュー内の平均プロセス数を示します。

イベントの概要

ライセンス： Protection

[Intrusion Event Statistics] ページの [Event Overview] セクションは、侵入イベント データベースにある情報の概要を示します。

これらの統計には、次が含まれています。

- [Events] は、侵入イベント データベース内のイベント数を示します。
- [Events in Time Range] は、現在選択されている時間範囲と、時間範囲内に収まるデータベースのイベントの割合を示します。
- [First Event] は、イベント データベース内の最初のイベントのイベント メッセージを示します。
- [Last Event] は、イベント データベース内の最後のイベントのイベント メッセージを示します。

注　Defense Centerでは、管理対象デバイスを選択した場合、そのデバイスの [Event Overview] セクションが代わりに表示されることに注意してください。

イベント統計情報

ライセンス： Protection

[Intrusion Event Statistics] ページの [Event Statistics] セクションでは、侵入イベント データベース内の情報に関する具体的な情報が表示されます。

この情報には、次に関する詳細が含まれます。

- 上位 10 個のイベント タイプ
- 上位 10 個のソース IP アドレス
- 上位 10 個の宛先 IP アドレス
- 上位 10 個の宛先ポート
- イベント数が最大であるプロトコル、イングレスとイーグレスのセキュリティ ゾーン、およびデバイス

侵入イベントのパフォーマンスの表示

ライセンス： Protection

[Intrusion Event Performance] ページでは、指定された期間の侵入イベントのパフォーマンス統計情報を示すグラフを生成できます。グラフを生成することにより、1 秒あたりの侵入イベントの数、1 秒あたりのメガビット数、1 パケットあたりの平均バイト数、Snort によって検査されていないパケットの割合、および TCP 正規化の結果としてブロックされたパケットの数を反映できます。これらのグラフは、過去 1 時間、前日、先週、または先月の操作の統計を表示できます。

詳細については、「侵入イベントのパフォーマンス統計グラフの生成（41-5 ページ）」を参照してください。

侵入イベントのパフォーマンス統計情報を表示する方法：

アクセス：Admin/Maint

ステップ 1　[Overview] > [Summary] > [Intrusion Event Performance] を選択します。

[Intrusion Event Performance] ページが表示されます。

侵入イベントのパフォーマンス統計グラフの生成

ライセンス：Protection

1 秒あたりの侵入イベントの数、1 秒あたりのメガビット数、1 パケットあたりの平均バイト数、Snort によって検査されていないパケットの割合、および TCP 正規化の結果としてブロックされたパケットの数に基づいて、Defense Centerまたは管理対象デバイスのパフォーマンス統計を示すグラフを生成できます。

注　新しいデータは 5 分ごとに統計グラフに蓄積されます。したがって、グラフをすぐにリロードしても、次の 5 分の差分更新が実行されるまでデータは変更されていない場合があります。

次の表に、表示可能なグラフの種類を示します。ネットワーク分析ポリシーの [Inline Mode] 設定の影響を受けるデータを含むグラフ タイプでは、表示が異なるので注意してください。[Inline Mode] が無効になっている場合、Web インターフェイスでアスタリスク（*）が付いているグラフ タイプ（下記の表では列に `yes` と記載）には、[Inline Mode] が有効になっている場合に変更またはドロップされるトラフィックに関するデータが含まれています。[Inline Mode] 設定の詳細については、インライン展開でプリプロセッサがトラフィックに影響を与えることを許可する（26-6 ページ）を参照してください。

必要なオプションと設定の詳細については、インライン トラフィックの正規化（29-7 ページ）、インライン展開でプリプロセッサがトラフィックに影響を与えることを許可する（26-6 ページ）、およびインライン展開でのドロップ動作の設定（31-6 ページ）を参照してください。

表 41-1　侵入イベントのパフォーマンス グラフの種類

データの生成対象となるグラフ	実行する操作	説明	インライン モードによる影響
Avg Bytes/Packet	n/a	各パケットに含まれる平均バイト数。	no
ECN Flags Normalized in TCP Traffic/Packet	[Explicit Congestion Notification] を有効にして、[Packet] を選択します。	ネゴシエーションに関係なく、パケット単位で ECN フラグがクリアされたパケットの数	yes
ECN Flags Normalized in TCP Traffic/Session	[Explicit Congestion Notification] を有効にして、[Stream] を選択します。	ECN の使用がネゴシエートされなかった場合にストリーム単位で ECN フラグがクリアされた回数。	yes
Events/Sec	n/a	デバイスで生成された 1 秒あたりのイベント数。	no
ICMPv4 Echo Normalizations	[Normalize ICMPv4] を有効にします。	エコー（要求）またはエコー応答メッセージの 8 ビット コード フィールドがクリアされた ICMPv4 パケットの数	yes

表 41-1　侵入イベントのパフォーマンス グラフの種類（続き）

データの生成対象となるグラフ	実行する操作	説明	インライン モードによる影響
ICMPv6 Echo Normalizations	[Normalize ICMPv6] を有効にします。	エコー（要求）またはエコー応答メッセージの 8 ビット コード フィールドがクリアされた ICMPv6 パケットの数	yes
IPv4 DF Flag Normalizations	[Normalize IPv4] と [Normalize Don't Fragment Bit] を有効にします。	IPv4 Flags ヘッダー フィールドのシングル ビット DF（Don't Fragment）サブフィールドがクリアされた IPv4 パケットの数	yes
IPv4 Options Normalizations	[Normalize IPv4] を有効にします。	オプション オクテットが「1」（No Operation）に設定された IPv4 パケットの数	yes
IPv4 Reserved Flag Normalizations	[Normalize IPv4] と [Normalize Reserved Bit] を有効にします。	IPv4 フラグ ヘッダー フィールドのシングル ビット予約サブフィールドがクリアされた IPv4 パケットの数。	yes
IPv4 Resize Normalizations	[Normalize IPv4] を有効にします。	超過ペイロードが IP ヘッダーで指定されたデータグラム長に切り詰められた IPv4 パケットの数	yes
IPv4 TOS Normalizations	[Normalize IPv4] と [Normalize TOS Bit] を有効にします。	1 バイト 差別化サービス（DS）フィールド（旧「タイプ オブ サービス（ToS）フィールド」）がクリアされた IPv4 パケットの数。	yes
IPv4 TTL Normalizations	[Normalize IPv4]、[Maximum TTL]、および [Reset TTL] を有効にします。	IPv4 存続時間（TTL）正規化の数。	yes
IPv6 Options Normalizations	[Normalize IPv6] を有効にします。	ホップバイホップ オプションまたは宛先オプション拡張ヘッダーのすべてのオプション タイプ フィールドが、00（スキップして処理を続行）に設定された IPv6 パケットの数。	yes
IPv6 TTL Normalizations	[Normalize IPv6]、[Minimum TTL]、および [Reset TTL] を有効にします。	IPv6 ホップ リミット（TTL）正規化の数。	yes
Mbits/Sec	n/a	デバイスをパススルーするトラフィックの 1 秒あたりのメガビット数。	no
Packet Resized to Fit MSS Normalizations	[Trim Data to MSS] を有効にします。	ペイロードが TCP データ フィールドよりも長かったため、ペイロードが最大セグメント サイズに切り詰められたパケットの数。	yes
Packet Resized to Fit TCP Window Normalizations	[Trim Data to Window] を有効にします。	受信側ホストの TCP ウィンドウに合わせて TCP データ フィールドが切り詰められたパケットの数。	yes

表 41-1　侵入イベントのパフォーマンス グラフの種類（続き）

データの生成対象となるグラフ	実行する操作	説明	インライン モードによる影響
Percent Packets Dropped	n/a	選択されたすべてのデバイスにおける未検査のパケットの平均割合。たとえば、2 つのデバイスを選択した場合、平均が 50 % であるというのは、1 つのデバイスのドロップ率が 90 % であり、もう 1 つのデバイスのドロップ率が 10 % であることを示している可能性があります。また、両方のデバイスのドロップ率が 50% である可能性もあります。グラフは、1 つのデバイスを選択した場合にのみ合計ドロップ率を表します。	no
RST Packets With Data Stripped Normalizations	[Remove Data on RST] を有効にします。	TCP リセット（RST）パケットからデータが削除されたパケットの数。	yes
SYN Packets With Data Stripped Normalizations	[Remove Data on SYN] を有効にします。	TCP オペレーティング システムが Mac OS でない場合に、SYN パケットからデータが削除されたパケットの数。	yes
TCP Header Padding Normalizations	[Normalize/Clear Option Padding Bytes] を有効にします。	オプションの埋め込みバイトが 0 に設定された TCP パケットの数。	yes
TCP No Option Normalizations	[Allow These TCP Options] を有効にして、any 以外のオプションに設定します。	タイムスタンプ オプションがストリップされたパケットの数。	yes
TCP NS Flag Normalizations	[Explicit Congestion Notification] を有効にして、[Packet] を選択します。	ECN Nonce Sum（NS）オプション正規化の数。	yes
TCP Options Normalizations	[Allow These TCP Options] を有効にして、any 以外のオプションに設定します。	オプション フィールドが「No Operation」（TCP オプション 1）に設定されているオプションの数（MSS、ウィンドウ スケール、タイムスタンプ、および明示的に許可されたオプションを除く）。	yes
TCP Packets Blocked By Normalizations	[Normalize TCP Payload] を有効にします（セグメントのリアセンブリは失敗します）。	TCP セグメントを正常にリアセンブルできなかったためにドロップされたパケットの数。	yes
TCP Reserved Flags Normalizations	[Normalize/Clear Reserved Bits] を有効にします。	予約ビットがクリアされた TCPパケットの数。	yes
TCP Segment Reassembly Normalizations	[Normalize TCP Payload] を有効にします（セグメントのリアセンブリは成功します）。	再送信データの一貫性を確保するために TCP データ フィールドが正規化されたパケットの数。（正しくリアセンブルできないセグメントはすべてドロップされます）。	yes

表 41-1　侵入イベントのパフォーマンス グラフの種類（続き）

データの生成対象となるグラフ	実行する操作	説明	インライン モードによる影響
TCP SYN Option Normalizations	[Allow These TCP Options] を有効にして、any 以外のオプションに設定します。	SYN 制御ビットが設定されていないため、最大セグメント サイズまたはウィンドウ スケール オプションが「No Operation」（TCP オプション 1）に設定されたオプションの数。	yes
TCP Timestamp ECR Normalizations	[Allow These TCP Options] を有効にして、any 以外のオプションに設定します。	確認応答（ACK）制御ビットが設定されていないため、タイムスタンプ エコー応答（TSecr）オプション フィールドがクリアされたパケットの数。	yes
TCP Urgent Pointer Normalizations	[Normalize Urgent Pointer] を有効にします。	TCP ヘッダーの緊急ポインタ フィールド（2 バイト）がペイロード長を超えていたため、ペイロード長に合わせてセットされたパケットの数。	yes
Total Blocked Packets	[Inline Mode] または [Drop when Inline] を設定します。	ルール、デコーダ、およびプリプロセッサのドロップを含めて、ドロップされたパケットの総数。	no
Total Injected Packets	[Inline Mode] を設定します。	再送信前にサイズ変更されたパケットの数。	no
Total TCP Filtered Packets	TCP ストリームの前処理を設定します。	TCP ポート フィルタリングのためにストリームによってスキップされたパケットの数。	no
Total UDP Filtered Packets	UDP ストリームの前処理を設定します。	UDP ポート フィルタリングのためにストリームによってスキップされたパケットの数。	no
Urgent Flag Cleared Normalizations	[Clear URG if Urgent Pointer is Not Set] を有効にします。	緊急ポインタが設定されていなかったため、TCP ヘッダーの URG 制御ビットがクリアされたパケットの数。	yes
Urgent Pointer and Urgent Flag Cleared Normalizations	[Clear Urgent Pointer/URG on Empty Payload] を有効にします。	ペイロードがなかったため、TCP ヘッダーの緊急ポインタ フィールドと URG 制御ビットがクリアされたパケットの数。	yes
Urgent Pointer Cleared Normalizations	[Clear Urgent Pointer if URG=0] を有効にします。	緊急（UGR）ポインタが設定されていなかったため、TCP ヘッダーの緊急ポインタ フィールド（16 ビット）がクリアされたパケットの数。	yes

侵入イベントのパフォーマンス グラフを生成する方法：

アクセス：Admin/Maint

ステップ 1　[Overview] > [Summary] > [Intrusion Event Performance] を選択します。

[Intrusion Event Performance] ページが表示されます。

ステップ 2　[Select Device] リストから、データを表示するデバイスを選択します。

ステップ 3　[Select Graph(s)] リストから、作成するグラフの種類を選択します。

ステップ 4　[Select Time Range] リストから、グラフに使用する時間範囲を選択します。

過去 1 時間、前日、先週、または先月から選択できます。

ステップ 5　[Graph] をクリックします。

グラフが表示され、ユーザが指定した情報が表示されます。

ステップ 6　グラフを保存するには、グラフを右クリックし、ブラウザでイメージを保存する手順に従います。

侵入イベント グラフの表示

ライセンス： Protection

FireSIGHT システムは、経時的な侵入イベントの傾向を示すグラフを表示します。以下に関する侵入イベントについて、過去 1 時間から先月までの範囲の経時的なグラフを生成できます。

- 1 つまたはすべての管理対象デバイス
- 上位 10 個の宛先ポート
- 上位 10 個の送信元 IP アドレス
- 上位 10 個のイベント メッセージ

イベント グラフを生成する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Overview] > [Summary] > [Intrusion Event Graphs] を選択します。

[Intrusion Event Graphs] ページが表示されます。ページの上部にある 3 つの選択ボックスは、どのグラフを生成するかを制御します。

ステップ 2　[Select Device] で、[all] を選択してすべてのデバイスを含めるか、グラフに含める特定のデバイスを選択します。

ステップ 3　[Select Graph(s)] で、生成するグラフの種類を選択します。

ステップ 4　[Select Time Range] で、グラフの時間範囲を選択します。

ステップ 5　[Graph] をクリックします。

グラフが生成されます。

侵入イベントの表示

ライセンス： Protection

システムは、悪意のある可能性があるパケットを認識すると、侵入イベントを生成し、イベントをデータベースに追加します。

初期の侵入イベント ビューは、ページにアクセスするために使用するワークフローによって異なります。1 つ以上のドリルダウン ページ、侵入イベントのテーブル ビュー、および終了パケット ビューを含む、定義済みワークフローの 1 つを使用するか、独自のワークフローを作成できます。カスタム テーブルに基づいてワークフローを表示することもできます。これには、侵入イベ

ントを含めることができます。大量の IP アドレスが含まれている状態で、[Resolve IP Addresses] イベント ビュー設定が有効になっている場合、イベント ビューの表示が遅くなる場合があることに注意してください。詳細については、「イベント ビュー設定の設定（71-3 ページ）」を参照してください。

侵入イベントは、ネットワーク セキュリティに対する脅威があるかどうかを判断するために表示します。侵入イベントが悪意のあるものではないことがわかったら、そのイベントを確認済みとしてマークできます。ユーザの名前がレビューアとして表示され、確認されたイベントはデフォルトの侵入イベント ビューには表示されなくなります。イベントに未確認のマークを付けることによって、確認済みイベントをデフォルトの侵入イベント ビューに戻すことができます。

確認済みとしてマークした侵入イベントを表示できます。確認済みのイベントはイベント データベースに保存され、イベント要約統計に含まれますが、デフォルトのイベント ページには表示されなくなります。詳細については、「侵入イベントについて（41-17 ページ）」を参照してください。

バックアップを実行してから確認済みの侵入イベントビューを削除した場合、バックアップを復元すると、削除された侵入イベント ビューは復元されますが、確認済みのステータスは復元されません。これらの復元された侵入イベントは、[Reviewed Events] ではなく [Intrusion Events] で表示されます。

1 つ以上の侵入イベントと関連付けられた接続イベントをすばやく表示するには、イベント ビューアのチェック ボックスを使用して侵入イベントを選択してから、[Jump to] ドロップダウン リストから [Connections] を選択します。これは、イベントのテーブル ビュー間を移動する場合に非常に役立ちます。同じ方法で、特定の接続に関連した侵入を表示することもできます。

詳細については、次の項を参照してください。

- 侵入イベントについて（41-11 ページ）
- カスタム ワークフローの作成（58-43 ページ）
- ドリルダウン ページとテーブル ビュー ページの使用（41-20 ページ）
- パケット ビューの使用（41-23 ページ）
- 侵入イベントと関連付けられた接続データの表示（41-16 ページ）
- 侵入イベントについて（41-17 ページ）
- カスタム テーブルに基づいたワークフローの表示（59-8 ページ）

侵入イベントを表示する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Analysis] > [Intrusions] > [Events] を選択します。

デフォルトの侵入イベントのワークフローの最初のページが表示されます。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。イベントが表示されない場合は、時間範囲の調整が必要になることがあります。イベント時間の制約の設定（58-26 ページ）を参照してください。

ヒント　侵入イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合、ワークフローのタイトルの横にある [(switch workflow)] をクリックして、アプライアンスに付属の定義済みワークフローのいずれかを選択します。

侵入イベント ビューに表示されるイベントの詳細については、侵入イベントについて（41-11 ページ）を参照してください。分析にとって重要な侵入イベントにビューを絞り込む方法の詳細については、侵入イベントのワークフロー ページについて（41-18 ページ）を参照してください。

侵入イベントについて

ライセンス：Protection

システムは、ホストとそのデータの可用性、整合性、および機密性に影響する可能性のある悪意のあるアクティビティについて、ネットワークを通過するパケットを検査します。システムは、潜在的な侵入を特定すると*侵入イベント*を生成します。これは、エクスプロイトの日付、時間、タイプ、および攻撃元とそのターゲットに関するコンテキスト情報のデータです。パケットベースのイベントの場合、イベントをトリガーしたパケットのコピーも記録されます。個々の侵入イベントで利用可能な情報は、ライセンスなどいくつかの要因に応じて決まります。詳細については、サービス サブスクリプション（65-8 ページ）を参照してください。

次のリストで、侵入イベントに含まれる情報について説明します。侵入イベントのテーブル ビューの一部のフィールドはデフォルトで無効になっていることに注意してください。セッション中にフィールドを有効にするには、展開矢印（  ）をクリックして、検索制限を拡張してから、[Disabled Columns] の下の列名をクリックします。

時刻

イベントの日付と時刻。

プライオリティ

Cisco VRT で指定されたイベントの優先度。

Impact

このフィールドの影響レベルは、侵入データ、ネットワーク検出 データ、脆弱性情報との関係を示します。詳細については、影響レベルを使用してイベントを評価する（41-39 ページ）を参照してください。

NetFlow データに基づいてネットワーク マップに追加されたホストで使用可能なオペレーティング システム情報が存在しない場合、ホスト入力機能を使用してホストのオペレーティング システム ID を手動で設定しない限り、Defense Centerはこれらのホストに関係した侵入イベントに対して影響レベル [Vulnerable]（影響レベル 1：赤）を割り当てることができないことに注意してください。

Inline Result

次のいずれかが必要です。

- 黒い下矢印。ルールをトリガーとして使用したパケットをシステムがドロップしたことを示します
- 灰色の下矢印。[Drop when Inline] ポリシー オプション（インライン展開環境）を有効にした場合、またはシステムがプルーニングしている間に [Drop and Generate] ルールがイベントを生成した場合、IPS がパケットをドロップしたことを示します
- ブランク。トリガーとして使用されたルールが [Drop and Generate Events] に設定されてないことを示します

  侵入ポリシーのルールの状態またはインライン ドロップ動作にかかわらず、インライン インターフェイスがタップ モードになっている場合を含め、パッシブ展開環境ではシステムはパケットをドロップしないことに注意してください。

Source IP

送信元ホストが使用する IP アドレス。

Source Country

送信元ホストの国。

Destination IP

受信ホストが使用する IP アドレス。

Destination Country

受信ホストの国。

Original Client IP

X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義の HTTP ヘッダーから取得された、元のクライアント IP アドレス。このフィールドの値を表示するには、ネットワーク解析ポリシーの HTTP プリプロセッサ [Extract Original Client IP Address] オプションを有効にする必要があります。オプションで、ネットワーク解析ポリシーの同じエリアで、最大 6 つのカスタム クライアント IP 見出しを指定し、システムが [Original Client IP] イベント フィールドの値を選択する優先順位を設定します。詳細については、「サーバレベル HTTP 正規化オプションの選択（27-36 ページ）」を参照してください。

このフィールドは、デフォルトでイネーブルにされています。

Source Port / ICMP Type

送信元ホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、システムは ICMP タイプを表示します。

Destination Port / ICMP Code

トラフィックを受信するホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、システムは ICMP コードを表示します。

SSL Status

暗号化された接続を記録した、SSL ルールに関連したアクション、デフォルト アクション、または復号化不能トラフィック アクション：

- [Block] および [Block with reset] は、ブロックされた暗号化接続を表します。
- [Decrypt (Resign)] は、再署名サーバ証明書を使用して復号化された発信接続を表します。
- [Decrypt (Replace Key)] は、置き換えられた公開キーと自己署名サーバ証明書を使用して復号化された発信接続を表します。
- [Decrypt（Known Key）] は、既知の秘密キーを使用して復号化された着信接続を表します。
- [Do not Decrypt] は、システムが復号化しなかった接続を表します。

システムが暗号化接続を復号化できなかった場合は、実行された復号化不能のトラフィック アクションと失敗の原因が表示されます。たとえば、システムが不明な暗号スイートで暗号化されたトラフィックを検出し、さらにインスペクションを行わずにそのトラフィックを許可した場合、このフィールドには [Do Not Decrypt (Unknown Cipher Suite)] が表示されます。

証明書の詳細を表示するには、ロック アイコン（  ）をクリックします。詳細については、暗号化接続に関連付けられた証明書の表示（39-33 ページ）を参照してください。

VLAN ID

侵入イベントをトリガーとして使用したパケットと関連付けられた内部 VLAN ID。

MPLS Label

この侵入イベントをトリガーとして使用したパケットと関連付けられたマルチプロトコル ラベル スイッチング ラベル。

このフィールドは、デフォルトでは無効です。

メッセージ

イベントを説明するテキスト。ルールベースの侵入イベントの場合、イベント メッセージはルールから取得されます。デコーダベースおよびプリプロセッサベースのイベントの場合は、イベント メッセージはハード コーディングされています。

分類

イベントを生成したルールが属する分類。ルールの分類名と番号のリストについては、ルール分類の表を参照してください。

Generator

イベントを生成したコンポーネント。侵入イベント ジェネレータ ID のリストについては、表 41-7（41-42 ページ）の表を参照してください。

Source User

送信元ホストにログインしている既知のユーザのユーザ ID。

Destination User

宛先ホストにログインしている既知のユーザのユーザ ID。

アプリケーション プロトコル

（使用可能な場合）侵入イベントをトリガーとして使用したトラフィックで検出されたホスト間の通信を表す、アプリケーション プロトコル。Defense Center Web インターフェイスで検出されたアプリケーション プロトコルをシステムが特定するしくみについては、表 45-3（45-14 ページ）を参照してください。

クライアント

（使用可能な場合）侵入イベントをトリガーとして使用したトラフィックで検出されたモニタ対象のホストで実行されているソフトウェアを表す、クライアント アプリケーション。

Web アプリケーション

侵入イベントをトリガーとして使用したトラフィックで検出された HTTP トラフィックの内容または要求された URL を表す、Web アプリケーション。

システムが HTTP のアプリケーション プロトコルを検出し、特定の Web アプリケーションを検出できなかった場合、システムはここで一般的な Web ブラウジング指定を提供することに注意してください。

IOC

侵入イベントをトリガーとして使用したトラフィックが、接続に関係するホストに対する侵入の痕跡（IOC）もトリガーとして使用したかどうか。IOC の詳細については、侵害の兆候について（45-22 ページ）を参照してください。

Category、Tag（Application Protocol、Client、Web Application）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準（表 45-2（45-12 ページ）を参照）。

Application Risk

侵入イベントをトリガーとして使用したトラフィックで、検出されたアプリケーションと関連付けられたリスク。接続で検出されるアプリケーションのタイプごとに関連するリスクがあります。このフィールドは、それらのうち最も高いリスクを表示します。詳細については、表 45-2（45-12 ページ）を参照してください。

Business Relevance

侵入イベントをトリガーとして使用したトラフィックで、検出されたアプリケーションと関連付けられたビジネスとの関連性。接続で検出されるアプリケーションのタイプごとに関連するビジネスとの関連性があります。このフィールドは、それらのうち最も低い（関連性が最も低い）ものを表示します。詳細については、表 45-2（45-12 ページ）を参照してください。

Ingress Security Zone

イベントをトリガーとして使用したパケットの入力セキュリティ ゾーン。パッシブ展開環境では、このセキュリティ ゾーン フィールドだけに入力されます。セキュリティ ゾーンの操作（3-42 ページ）を参照してください。

Egress Security Zone

インライン展開環境の場合、イベントをトリガーとして使用したパケットの出力セキュリティ ゾーン。パッシブ展開環境では、このセキュリティ ゾーンのフィールドには入力されません。セキュリティ ゾーンの操作（3-42 ページ）を参照してください。

デバイス

アクセス コントロール ポリシーが適用された管理対象デバイス。デバイスの管理（4-1 ページ）を参照してください。

セキュリティ コンテキスト

トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。システムがこのフィールドにデータを設定するのは、マルチコンテキスト モードの ASA FirePOWER デバイスだけです。

Ingress Interface

イベントをトリガーとして使用したパケットの入力インターフェイス。パッシブ インターフェイスの場合、このインターフェイスの列だけに入力されます。センシング インターフェイスの設定（4-64 ページ）を参照してください。

Egress Interface

インライン セットの場合、イベントをトリガーとして使用したパケットの出力インターフェイス。パッシブ インターフェイスの場合、このインターフェイスの列には入力されません。センシング インターフェイスの設定（4-64 ページ）を参照してください。

Intrusion Policy

イベントを生成した侵入ルール、プリプロセッサ ルール、またはデコーダ ルールが有効にされた侵入ポリシー。アクセス コントロール ポリシーのデフォルト アクションとして侵入ポリシーを選択するか、アクセス コントロール ルールと侵入ポリシーを関連付けることができます。デフォルトの処理の設定およびネットワーク トラフィックのインスペクション（12-7 ページ）および侵入防御を実行するアクセス コントロール ルールの設定（18-8 ページ）を参照してください。

Access Control Policy

イベントを生成した侵入ルール、プリプロセッサ ルール、またはデコーダ ルールが有効になっている侵入ポリシーを含んでいるアクセス コントロール ポリシー（アクセス コントロール ポリシーの管理（12-12 ページ）を参照）。

Access Control Rule

イベントを生成した侵入ルールを呼び出したアクセス コントロール ルール（侵入防御を実行するアクセス コントロール ルールの設定（18-8 ページ）を参照）。[Default Action] は、ルールが有効化されている侵入ポリシーが特定のアクセス コントロール ルールに関連付けられておらず、代わりに、アクセス コントロール ポリシーのデフォルト アクションとして設定されていることを示しています（デフォルトの処理の設定およびネットワーク トラフィックのインスペクション（12-7 ページ）を参照）。

侵入インスペクションがアクセス コントロール ルールにもデフォルト アクションにも関連付けられていない場合、このフィールドは空欄になります。たとえば、パケットがデフォルトの侵入ポリシーによって検査された場合などです。詳細については、アクセス コントロールのデフォルト侵入ポリシーの設定（25-1 ページ）を参照してください。

Network Analysis Policy

（存在する場合）イベントの生成に関連付けられているネットワーク分析ポリシー（NAP）（ネットワーク分析ポリシーの開始（26-1 ページ）を参照）。

HTTP Hostname

HTTP 要求のホスト 見出しから取得されたホスト名（存在する場合）。要求パケットにホスト名が常に含まれているわけではないことに注意してください。

ホスト名を表示するには、HTTP 検査プリプロセッサ [Log Hostname] オプションを有効にする必要があります。詳細については、「サーバレベル HTTP 正規化オプションの選択（27-36 ページ）」を参照してください。

この列には、取得されたホスト名の最初の 50 文字が表示されます。ホストの省略名の表示部分にポインタを合わせると、最大 256 バイトまでの完全な名前を表示することができます。また、最大 256 バイトまでの完全なホスト名をパケット ビューに表示することもできます。詳細については、「イベント情報の表示（41-25 ページ）」を参照してください。

このフィールドは、デフォルトでは無効です。

HTTP URI

（存在する場合）侵入イベントをトリガーとして使用した HTTP 要求パケットに関連付けられた raw URI。要求パケットに URI が常に含まれているわけではないことに注意してください。

取得された URI を表示するには、HTTP 検査プリプロセッサ [Log URI] オプションを有効にする必要があります。詳細については、「サーバレベル HTTP 正規化オプションの選択（27-36 ページ）」を参照してください。

HTTP 応答によってトリガーとして使用された侵入イベントの関連 HTTP URI を参照するには、[Perform Stream Reassembly on Both Ports] オプションに HTTP サーバのポートを設定する必要があります。ただし、これにより、トラフィックのリアセンブル用のリソース要求が増加することに注意してください。ストリームの再アセンブリのオプションの選択（29-29 ページ）を参照してください。

この列には、取得された URI の最初の 50 文字が表示されます。省略 URI の表示部分にポインタを合わせると、最大 2048 バイトまでの完全な URI を表示することができます。また、最大 2048 バイトまでの完全な URI をパケット ビューに表示することもできます。詳細については、「イベント情報の表示（41-25 ページ）」を参照してください。

このフィールドは、デフォルトでは無効です。

Email Sender

SMTP MAIL FROM コマンドから取得された電子メール送信者のアドレス。このフィールドの値を表示するには、SMTP プリプロセッサの [Log From Address] オプションを有効にする必要があります。複数の送信者アドレスがサポートされます。詳細については、「SMTP デコードについて（27-64 ページ）」を参照してください。

このフィールドは、デフォルトでは無効です。

Email Recipient

SMTP RCPT TO コマンドから取得された電子メール受信者のアドレス。このフィールドの値を表示するには、SMTP プリプロセッサの [Log To Addresses] オプションを有効にする必要があります。複数の受信者アドレスがサポートされます。詳細については、「SMTP デコードについて（27-64 ページ）」を参照してください。

このフィールドは、デフォルトでは無効です。

Email Attachments

MIME Content-Disposition ヘッダーから取得された MIME 添付ファイル名。添付ファイルの名前を表示するには、SMTP プリプロセッサの [Log MIME Attachment Names] オプションを有効にする必要があります。複数の添付ファイル名がサポートされます。詳細については、「SMTP デコードについて（27-64 ページ）」を参照してください。

このフィールドは、デフォルトでは無効です。

Reviewed By

イベントを確認したユーザの名前。侵入イベントについて（41-17 ページ）を参照してください。

Count

各ローに表示される情報に一致するイベントの数。[Count] フィールドは 2 つ以上の同一の行を作成する制約を適用した後にのみ表示されることに注意してください。

侵入イベントと関連付けられた接続データの表示

ライセンス：Protection

システムは、侵入イベントが検出された接続を記録できます。このロギングは、アクセス コントロール ルールに関連付けられている侵入ポリシーに対して自動的に行われますが、デフォルト アクションに関連する接続データを参照するには、接続ロギングを手動で有効にする必要があります（アクセス コントロールの処理に基づく接続のロギング（38-17 ページ）を参照）。

注　個々の接続またはセキュリティ インテリジェンス イベントで利用可能な情報は、ライセンスやアプライアンス モデルなど、いくつかの要因によって異なります。詳細については、接続ロギングのライセンスおよびモデル要件（38-10 ページ）を参照してください。

1 つ以上の侵入イベントに関連付けられた接続データを表示する方法：

アクセス：Admin

ステップ 1　[Analysis] > [Intrusions] > [Events] を選択します。

デフォルトの侵入イベントのワークフローの最初のページが表示されます。

関連データの表示は、イベントのテーブル ビュー間を移動する場合に非常に役立ちます。分析にとって重要な侵入イベントにビューを絞り込む方法の詳細については、侵入イベントのワークフロー ページについて（41-18 ページ）を参照してください。

ステップ 2　イベント ビューアのチェック ボックスを使用して侵入イベントを選択してから、[Jump to] ドロップダウン リストから [Connections] を選択します。

同じ方法で、特定の接続に関連した侵入イベントを表示できます。詳細については、ワークフロー間のナビゲート（58-40 ページ）を参照してください。

関連イベントを確認するとき、Defense Centerはデフォルトの接続データのワークフローを使用します。接続データの詳細については、接続およびセキュリティ インテリジェンス のデータの使用（39-1 ページ）を参照してください。

ヒント　侵入イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合、ワークフローのタイトルの横にある [(switch workflow)] をクリックして、アプライアンスに付属の定義済みワークフローのいずれかを選択します。

侵入イベントについて

ライセンス： Protection

侵入イベントを調べて、そのイベントがネットワーク セキュリティに対して脅威ではないことがわかったら（おそらく、ネットワーク上のどのホストも検出されたエクスプロイトに対して脆弱でないことがわかったため）、そのイベントを確認済みとしてマークできます。ユーザの名前がレビューアとして表示され、確認されたイベントはデフォルトの侵入イベント ビューには表示されなくなります。確認済みとしてマークしたイベントはイベント データベースに残りますが、侵入イベントのビューには表示されなくなります。

侵入イベントに確認済みのマークを付けるには：

アクセス： Admin/Intrusion Admin

ステップ 1　侵入イベントが表示されるページで、次の 2 つの方法を選択できます。

- イベントのリストから 1 つまたは複数の侵入イベントにマークを付けるには、イベントの横にあるチェック ボックスを選択し、[Review] をクリックします。
- イベントのリストからすべての侵入イベントにマークを付けるには、[Review All] をクリックします。

成功メッセージが表示され、確認済みイベント リストが更新されます。

侵入イベント ビューに表示されるイベントの詳細については、侵入イベントについて（41-11 ページ）を参照してください。分析にとって重要な侵入イベントにビューを絞り込む方法の詳細については、侵入イベントのワークフロー ページについて（41-18 ページ）を参照してください。

注　確認されたイベントは、侵入イベントに関連したワークフローのページに表示されませんが、イベント要約の統計情報には含まれます。

以前に確認済みとマークされたイベントを表示する方法:

アクセス: Admin/Intrusion Admin

ステップ 1　[Analysis] > [Intrusions] > [Reviewed Events] を選択します。

デフォルトの確認済み侵入イベントのワークフローの最初のページが表示されます。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。イベントが表示されない場合は、時間範囲の調整が必要になることがあります。イベント時間の制約の設定（58-26 ページ）を参照してください。

ヒント　侵入イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合、ワークフローのタイトルの横にある [(switch workflow)] をクリックして、アプライアンスに付属の定義済みワークフローのいずれかを選択します。

確認済み侵入イベント ビューに表示されるイベントの詳細については、侵入イベントについて（41-11 ページ）を参照してください。分析にとって重要な侵入イベントにビューを絞り込む方法の詳細については、侵入イベントのワークフロー ページについて（41-18 ページ）を参照してください。

確認済みイベントに未確認のマークを付けるには:

アクセス: Admin/Intrusion Admin

ステップ 1　確認済みイベントが表示されるページで、次の 2 つの方法を選択できます。

- 確認済みイベント リストから個別の侵入イベントを削除するには、イベントの横にあるチェック ボックスを選択し、[Unreview] をクリックします。
- 確認済みイベント リストからすべての侵入イベントを削除するには、[Unreview All] をクリックします。

成功メッセージが表示され、確認済みイベント リストが更新されます。

侵入イベントのワークフロー ページについて

ライセンス: Protection

現在の侵入ポリシーで有効になっているプリプロセッサ、デコーダ、および侵入ルールは、モニタしているトラフィックがポリシーに違反するたびに、侵入イベントを生成します。

FireSIGHT システムは、侵入イベントの表示および分析に使用できる、イベント データが入力された定義済みワークフローのセットを提供します。これらのワークフローは、評価する侵入イベントの特定に役立つ一連のページを表示して手順を示します。

定義済みの侵入イベントのワークフローには、次の 3 種類のページまたはイベント ビューがあります。

- 1 つ以上のドリルダウン ページ
- 侵入イベントのテーブル ビュー
- パケット ビュー

*ドリルダウン ページ*には通常、1 つの特定の種類の情報を表示できるように、1 つのテーブル（一部のドリルダウン ビューでは複数のテーブル）に複数の列が含まれています。

「ドリルダウン」して 1 つ以上の宛先ポートの詳細情報を検索すると、これらのイベントは自動的に選択され、ワークフローの次のページが表示されます。このように、ドリルダウン テーブルを使用すると、一度に分析するイベントの数を減らすことができます。

侵入イベントの最初の*テーブル ビュー*では、各侵入イベントが独自の行にリストされます。テーブルの列には、時間、発信元 IP アドレスおよびポート、宛先 IP アドレスおよびポート、イベントの優先度、イベント メッセージなどの情報が示されます。

イベントを選択してワークフローの次のページを表示する代わりに、テーブル ビューでイベントを選択した場合、イベントはいわゆる*制約*に追加されます。制約とは、分析するイベントの種類に加える制限のことです。

たとえば、任意の列で列のクローズ アイコン（ ）をクリックして、ドロップダウン リストから [Time] をクリアすると、[Time] を列の 1 つとして削除できます。分析内でイベントのリストを絞り込むには、テーブル ビューの行のいずれかの値のリンクをクリックします。たとえば、分析を送信元 IP アドレスの 1 つ（おそらく、潜在的な攻撃者）から生成されたイベントに制限するには、[Source IP Address] 列の IP アドレスをクリックします。

テーブル ビューの 1 つまたは複数の行を選択し、[View] をクリックすると、パケット ビューが表示されます。*パケット ビュー*は、ルールをトリガーとして使用したパケットまたはイベントを生成したプリプロセッサに関する情報を提供します。パケット ビューの各セクションには、パケット内の特定の層についての情報が含まれます。折りたたまれたセクションを展開すると、より多くの情報を参照できます。

注　それぞれのポート スキャン イベントは複数のパケットによってトリガーとして使用されるため、ポート スキャン イベントは特別なバージョンのパケット ビューを使用します。詳細については、「ポート スキャンの検出（34-3 ページ）」を参照してください。

事前定義済みのワークフローが特定のニーズに合致しない場合は、必要な情報だけを表示するカスタム ワークフローを作成できます。カスタム侵入イベントのワークフローには、ドリルダウン ページ、イベントのテーブル ビュー、またはその両方を含めることができます。システムはパケット ビューを最後のページとして自動的に組み込みます。イベントを調査する方法に応じて、定義済みワークフローと独自のカスタム ワークフローを簡単に切り替えることができます。

ヒント　ワークフローの概要と使用（58-1 ページ）は、すべてのワークフロー ページに共通のワークフローおよび機能の使用方法について説明します。この章では、カスタム侵入イベントのワークフローを作成および使用する方法についても説明します。

詳細については、以下を参照してください。

- ドリルダウン ページとテーブル ビュー ページの使用（41-20 ページ）には、多くの共通機能を共有している、ドリルダウン ページとイベントのテーブル ビューの使用方法が記載されています。
- パケット ビューの使用（41-23 ページ）は、パケット ビューで機能を使用する方法について説明します。
- 侵入イベントの検索（41-44 ページ）は、イベント データベースで特定の侵入イベントを検索する方法について説明します。

ドリルダウン ページとテーブル ビュー ページの使用

ライセンス： Protection

侵入イベントを調査するために使用できるワークフローでは、次の 3 種類のページが利用されます。

- ドリルダウン ページ
- 侵入イベントのテーブル ビュー
- パケット ビュー

これらの各ページについては、侵入イベントのワークフロー ページについて（41-18 ページ）で説明されています。

イベントのドリルダウン ビューとテーブル ビューはいくつかの共通機能を共有しています。これらの機能を使用して、イベントのリストを絞り込み、関連する一連のイベントを集中的に分析できます。次の表に、これらの機能について説明します。

表 41-2　侵入イベントの共通機能

目的	操作
表示された列の詳細を表示する	詳細については、侵入イベントについて（41-11 ページ）を参照してください。
ホスト プロファイルの表示	ホスト IP アドレスの横に表示されるホスト プロファイル アイコン（  ）をクリックします。
位置情報の詳細の表示	[Source Country] または [Destination Country] 列に表示されるフラグ アイコンをクリックします。
表示されたイベントの日付と時刻の範囲の変更	詳細については、イベント時間の制約の設定（58-26 ページ）を参照してください。 イベント ビューを時間によって制約している場合は、（グローバルかイベント固有かに関係なく）アプライアンスに設定されている時間枠の外で生成されたイベントが、イベント ビューに表示されることがあるので注意してください。これは、アプライアンスのスライド時間ウィンドウを設定している場合でも発生する可能性があります。
現在のワークフロー ページでイベントをソートおよび制約する	以下で詳細を参照できます。 • ドリルダウン ワークフロー ページのソート（58-38 ページ） • ドリルダウン ページでのイベントの制約の表 • イベントのテーブル ビューのイベントの制約の表
現在のワークフロー ページ内の移動	詳細については、ワークフロー内の他のページへのナビゲート（58-39 ページ）を参照してください。 **ヒント**　別のワークフロー ページで同じ侵入イベントを表示しないようにするため、ページの下部にあるリンクをクリックして別のページのイベントを表示すると時間範囲は一時停止し、クリックして後続のページでその他のアクションを実行すると再開します。詳細については、イベント時間の制約の設定（58-26 ページ）を参照してください。
現在の制約を保持しながら、現在のワークフローのページ間を移動する	ワークフロー ページの左上で、該当するページ リンクをクリックします。詳細については、ワークフローのページの使用（58-21 ページ）を参照してください。

表 41-2　侵入イベントの共通機能（続き）

目的	操作
後でインシデントに転送できるようにイベントをクリップボードに追加する	次のいずれかの方法を使用します。 • ワークフロー ページの複数の侵入イベントをクリップボードにコピーするには、コピーするイベントの横にあるチェック ボックスを選択して、[Copy] をクリックします。 • 現在制約されているビューにあるすべての侵入イベントをクリップボードにコピーするには、[Copy All] をクリックします。 クリップボードはユーザごとに最大 25,000 個のイベントを保存します。詳細については、クリップボードの使用（41-52 ページ）を参照してください。
イベント データベースからのイベントの削除	次のいずれかの方法を使用します。 • 選択した侵入イベントを削除するには、削除するイベントの横にあるチェック ボックスを選択し、[Delete] をクリックします。 • 現在の制約ビューにあるすべての侵入イベントを削除するには、[Delete All] をクリックし、すべてのイベントを削除してよいかどうかを確認します。
イベントに確認済みのマークを付けて、侵入イベントのページからそれらを削除し、イベント データベースからは削除しない	次のいずれかの方法を使用します。 • 選択した侵入イベントを確認するには、確認するイベントの横にあるチェック ボックスを選択し、[Review] をクリックします。 • 現在制約されているビューにあるすべての侵入イベントを確認するには、[Review All] をクリックします。 詳細については、侵入イベントについて（41-17 ページ）を参照してください。
選択した各イベントをトリガーとして使用したパケット（libpcap 形式のパケット キャプチャ ファイル）のローカル コピーをダウンロードする	次のいずれかの方法を使用します。 • 選択した侵入イベントをトリガーとして使用したパケットをダウンロードするには、ダウンロードするパケットによってトリガーとして使用されたイベントの横にあるチェック ボックスを選択し、[Download Packets] をクリックします。 • 現在制約されているビューにある侵入イベントをトリガーとして使用したすべてのパケットをダウンロードするには、[Download All Packets] をクリックします。 キャプチャされたパケットは libpcap 形式で保存されます。この形式は、複数の一般的なプロトコル アナライザで使用されます。
他のイベント ビューに移動して、関連イベントを確認する	詳細については、ワークフロー間のナビゲート（58-40 ページ）を参照してください。
一時的に別のワークフローを使用する	[(switch workflow)] をクリックします。詳細については、ワークフローの選択（58-18 ページ）を参照してください。
すぐに再表示できるように、現在のページをブックマークする	[Bookmark This Page] をクリックします。詳細については、ブックマークの使用（58-41 ページ）を参照してください。
[Summary Dashboard] の [Intrusion Events] セクションを表示する	[Dashboards] をクリックします。詳細については、ダッシュボードの操作（55-40 ページ）を参照してください。
ブックマークの管理ページへ移動する	[View Bookmarks] をクリックします。詳細については、ブックマークの使用（58-41 ページ）を参照してください。
現在のビューのデータに基づいてレポートを生成する	[Report Designer] をクリックします。詳細については、イベント ビューからのレポート テンプレートの作成（57-10 ページ）を参照してください。

イベント ビューに表示される侵入イベントの数は、次の内容によっては非常に多くなることがあります。

- ユーザが選択する時間範囲
- ネットワークのトラフィック量
- 適用する侵入ポリシー

侵入イベントをさらに分析しやすくするために、イベント ページを制約できます。制約プロセスは、侵入イベントのドリルダウン ビューとテーブル ビューとでは若干異なります。

ヒント　時間範囲は、侵入イベントのワークフロー ページの下部にあるリンクの 1 つをクリックして別のページに移動したときに一時停止し、クリックして後続のページでワークフローの終了を含む別のアクションを実行した時に再開します。これにより、ワークフロー内の他のページに移動してより多くのイベントを参照した場合に同じイベントが表示される可能性が減ります。詳細については、イベント時間の制約の設定（58-26 ページ）およびワークフロー内の他のページへのナビゲート（58-39 ページ）を参照してください。

次の表では、ドリルダウン ページの使用方法を示しています。

表 41-3　ドリルダウン ページでのイベントの制約

目的	操作
次のワークフロー ページのドリルダウンを特定の値に制約する	値をクリックします。 たとえば、[Destination Port（宛先ポート）] ワークフローで、イベントを宛先がポート 80 であるものに制約するには、[DST Port/ICMP Code] 列で [80/tcp] をクリックします。ワークフローの次のページ [Events] が表示され、ポート 80/tcp のイベントだけが含まれます。
次のワークフロー ページのドリルダウンを選択したイベントに制約する	次のワークフロー ページで表示するイベントの横にあるチェック ボックスを選択し、[View] をクリックします。 たとえば、[Destination Port（宛先ポート）] ワークフローで、イベントを宛先がポート 20/tcp および 21/tcp であるものに制約するには、それらのポートの行の横にあるチェック ボックスを選択し、[View] をクリックします。ワークフローの次のページ [Events] が表示され、ポート 20/tcp および 21/tcp のイベントだけが含まれます。 **注**　複数の行を制約し、テーブルに複数の列が存在する場合（[Count] 列を含まない）、いわゆる複合制約が作成されます。複合制約により、必要以上のイベントを制約に含めないようにすることができます。たとえば、[Event and Destination] ワークフローを使用する場合は、最初のドリルダウン ページで選択した各行により、複合制約が作成されます。宛先 IP アドレス 10.10.10.100 のイベント 1:100 を選択し、宛先 IP アドレス 192.168.10.100 のイベント 1:200 も選択した場合、複合制約により、イベント タイプとして 1:100 を含むイベントや宛先 IP アドレスとして 192.168.10.100 を含むイベント、またはイベント タイプとして 1:200 を含むイベントや宛先 IP アドレスとして 10.10.10.100 を含むイベントが選択されないようになります。
現在の制約を保持しながら、次のワークフロー ページをドリルダウンする	[View All] をクリックします。

次の表では、テーブル ビューの使用方法について説明します。

表 41-4　イベントのテーブル ビューのイベントの制約

目的	操作
1 つの属性を持つイベントにビューを制約する	属性をクリックします。 たとえば、宛先がポート 80 であるイベントにビューを制約するには、[DST Port/ICMP Code] 列で [80/tcp] をクリックします。
テーブルから列を削除する	非表示にする列見出しのクローズ アイコン( )をクリックします。表示されるポップアップ ウィンドウで、[Apply] をクリックします。 **ヒント**　その他の列を表示するには該当するチェック ボックスを選択し、非表示にするにはクリアしてから、[Apply] をクリックします。無効になった列をビューに再追加するには、展開矢印( )をクリックして検索制約を拡張し、[Disabled Columns] の下の列名をクリックします。
1 つ以上のイベントに関連付けられたパケットを表示する	次のいずれかを行います。 • パケットを表示するイベントの横にある下矢印アイコン( )をクリックします。 • パケットを表示する 1 つ以上のイベントを選択し、ページの下部にある [View] をクリックします。 • ページの下部で、[View All] をクリックして、現在の制約に一致するすべてのイベントのパケットを表示します。

ヒント　プロセスの任意の時点で、制約を検索条件のセットとして保存できます。たとえば、ネットワークが数日にわたり単一の IP アドレスから攻撃者によって探られていることに気付いた場合、調査中に制約をいったん保存し、後で使用することができます。ただし、複合制約を検索条件のセットとして保存することはできません。詳細については、検索設定の実行と保存（60-1 ページ）を参照してください。

ヒント　侵入イベントがイベント ビューに表示されない場合、選択した時間範囲を調整すると、結果が返される場合があります。古い時間範囲を選択した場合、その時間範囲内のイベントが削除されることがあります。ルールのしきい値の設定を調整すると、イベントが生成される場合があります。

パケット ビューの使用

ライセンス： Protection

パケット ビューは、侵入イベントを生成したルールをトリガーとして使用したパケットに関する情報を表示します。

ヒント　イベントを検出するデバイスで [Transfer Packet] オプションが無効になっている場合、Defense Centerでのパケット ビューにはパケット情報は含まれません。

パケット ビューは、パケットがトリガーとして使用した侵入イベントに関する情報を提供することによって、イベントのタイム スタンプ、メッセージ、分類、優先度、およびイベントを生成したルール（標準テキスト ルールでイベントが生成された場合）など、特定のパケットがキャプチャされた理由を示します。パケット ビューは、パケットのサイズなど、パケットに関する一般情報も表示します。

さらに、パケット ビューにはパケット内の各層（データ リンク、ネットワーク、およびトランスポート）について説明したセクションと、パケットを構成するバイトについて説明したセクションがあります。システムがパケットを復号化した場合は、復号化されたバイトを表示できます。折りたたまれたセクションを展開すると、詳細情報を参照できます。

注　それぞれのポートスキャン イベントは複数のパケットによってトリガーとして使用されるため、ポートスキャン イベントは特別なバージョンのパケット ビューを使用します。詳細については、「ポートスキャンの検出（34-3 ページ）」を参照してください。

次の表に、パケット ビューで実行できる操作を示します。

表 41-5　パケット ビューの操作

目的	操作
パケット ビューで日時範囲を変更する	詳細については、イベント時間の制約の設定（58-26 ページ）を参照してください。
パケットのビューに表示される情報について理解する	以下で詳細を参照できます。 • イベント情報の表示（41-25 ページ） • フレーム情報の表示（41-32 ページ） • データリンク層情報の表示（41-33 ページ） • ネットワーク層情報の表示（41-34 ページ） • トランスポート層情報の表示（41-36 ページ） • パケット バイト情報の表示（41-39 ページ）
後でインシデントに転送できるようにイベントをクリップボードに追加する	次のいずれかを行います。 • [Copy] をクリックして、パケットを表示するイベントをコピーします • [Copy All] をクリックして、以前にパケットを選択したすべてのイベントをコピーします クリップボードはユーザごとに最大 25,000 個のイベントを保存します。クリップボードの詳細については、クリップボードの使用（41-52 ページ）を参照してください。
イベント データベースからイベントを削除する	次のいずれかを行います。 • [Delete] をクリックして、パケットを表示するイベントを削除します • [Delete All] をクリックして、以前にパケットを選択したすべてのイベントを削除します

表 41-5　パケット ビューの操作（続き）

目的	操作
イベントに確認済みのマークを付けて、イベント ビューから削除し、イベント データベースからは削除しない	次のいずれかを行います。 • [Review] をクリックして、パケットを確認するイベントを確認します • [Review All] をクリックして、以前にパケットを選択したすべてのイベントを確認します 詳細については、侵入イベントについて（41-17 ページ）を参照してください。確認されたイベントは、[Intrusion Event Statistics] ページのイベント統計情報には引き続き含まれることに注意してください。
イベントをトリガーとして使用したパケット（libpcap 形式のパケット キャプチャ ファイル）のローカル コピーをダウンロードする	次のいずれかを行います。 • [Download Packet] をクリックして、表示中のイベントのキャプチャされたパケットのコピーを保存します • [Download All Packets] をクリックして、以前にパケットを選択したすべてのイベントのキャプチャされたパケットのコピーを保存します キャプチャされたパケットは libpcap 形式で保存されます。この形式は、複数の一般的なプロトコル アナライザで使用されます。 単一のポート スキャン イベントは複数のパケットに基づいているため、ポート スキャン パケットをダウンロードできないことに注意してください。ただし、ポート スキャン ビューは使用可能なすべてのパケット情報を提供します。詳細については、「ポート スキャン イベントについて（34-7 ページ）」を参照してください。 ダウンロードするには少なくとも 15 % の使用可能なディスク領域が必要であることに注意してください。
ページ セクションを展開または縮小する	セクションの隣にある矢印をクリックします。

パケット ビューを表示する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　侵入イベントのテーブル ビューで、表示するパケットを選択します。詳細については、イベントのテーブル ビューのイベントの制約の表を参照してください。

パケット ビューが表示されます。複数のイベントを選択した場合は、ページの下部にあるページ番号を使用してパケットのページ切り替えができます。

イベント情報の表示

ライセンス：Protection

パケット ビューで、[Event Information] セクションのパケットに関する情報を表示できます。

Event

イベントのメッセージ。ルールベースのイベントの場合、これはルール メッセージに対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

イベントの ID は、*(GID:SID:Rev)* の形式でメッセージに付加されます。*GID* は、ルール エンジン、デコーダ、またはイベントを生成したプリプロセッサのジェネレータ ID です。*SID* は、ルール、デコーダ メッセージ、またはプリプロセッサ メッセージの ID です。*Rev* はルールのリビジョン番号です。詳細については、プリプロセッサ ジェネレータ ID の読み取り (41-42 ページ)を参照してください。

Timestamp

パケットが検出された時間。

分類

イベントの分類。ルールベースのイベントの場合、これはルールの分類に対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

プライオリティ

イベントの優先度。ルールベースのイベントの場合、これは `priority` キーワードの値または `classtype` キーワードの値に対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

Ingress Security Zone

イベントをトリガーとして使用したパケットの入力セキュリティ ゾーン。パッシブ展開環境では、このセキュリティ ゾーン フィールドだけに入力されます。セキュリティ ゾーンの操作 (3-42 ページ)を参照してください。

Egress Security Zone

インライン展開環境の場合、イベントをトリガーとして使用したパケットの出力セキュリティ ゾーン。セキュリティ ゾーンの操作 (3-42 ページ)を参照してください。

デバイス

アクセス コントロール ポリシーが適用された管理対象デバイス。デバイスの管理 (4-1 ページ)を参照してください。

セキュリティ コンテキスト

トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。システムがこのフィールドにデータを設定するのは、マルチコンテキスト モードの ASA FirePOWER デバイスだけです。

Ingress Interface

イベントをトリガーとして使用したパケットの入力インターフェイス。パッシブ インターフェイスの場合、このインターフェイスの列だけに入力されます。センシング インターフェイスの設定 (4-64 ページ)を参照してください。

Egress Interface

インライン セットの場合、イベントをトリガーとして使用したパケットの出力インターフェイス。センシング インターフェイスの設定 (4-64 ページ)を参照してください。

Source/Destination IP

イベント (ソース) をトリガーとして使用したパケットの発生元であるホスト IP アドレスまたはドメイン名、またはイベントをトリガーとして使用したトラフィックのターゲット (宛先) ホスト。

ドメイン名を表示するには、IP アドレス解決を有効にする必要があることに注意してください。詳細については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

アドレスまたはドメイン名をクリックしてコンテキスト メニューを表示してから、whois 検索を実行する場合は [Whois] を、ホスト情報を表示する場合は [View Host Profile] を、アドレスをグローバル ブラックリストまたはホワイトリストに追加する場合は [Blacklist Now] または [Whitelist Now] を選択します。ホスト プロファイルの使用（49-1 ページ）およびグローバル ホワイトリストおよびブラックリストの操作（3-7 ページ）を参照してください。

Source Port/ICMP Type

イベントをトリガーとして使用したパケットの送信元ポート。ICMP トラフィックの場合は、ポート番号がないため、システムは ICMP タイプを表示します。

Destination Port/ICMP Code

トラフィックを受信するホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、システムは ICMP コードを表示します。

Email Headers

電子メール 見出しから取得したデータ。電子メール 見出しは侵入イベントのテーブル ビューには表示されませんが、電子メール 見出し データは検索条件として使用できることに注意してください。

電子メール 見出しを SMTP トラフィックの侵入イベントと関連付けるには、SMTP プリプロセッサの [Log Headers] オプションを有効にする必要があります。詳細については、「SMTP デコードについて（27-64 ページ）」を参照してください。ルールベースのイベントの場合、この行は電子メール データが取得されたときに表示されます。

HTTP Hostname

（存在する場合）HTTP 要求のホスト 見出しから取得されたホスト名。この行には、最大 256 バイトの完全なホスト名が表示されます。ホスト名が単一行よりも長い場合、展開矢印（  ）をクリックすると完全なホスト名が表示されます。

ホスト名を表示するには、HTTP 検査プリプロセッサ [Log Hostname] オプションを有効にする必要があります。詳細については、「サーバレベル HTTP 正規化オプションの選択（27-36 ページ）」を参照してください。

HTTP 要求パケットにホスト名が常に含まれているわけではないことに注意してください。ルールベースのイベントの場合、この行はパケットに HTTP ホスト名または HTTP URI が含まれている場合に表示されます。

HTTP URI

（存在する場合）侵入イベントをトリガーとして使用した HTTP 要求パケットに関連付けられた raw URI。この行には、最大 2048 バイトの完全な URI が表示されます。URI が単一行よりも長い場合、展開矢印（）をクリックすると完全な URI が表示されます。

URI を表示するには、HTTP 検査プリプロセッサ [Log URI] オプションを有効にする必要があります。詳細については、「サーバレベル HTTP 正規化オプションの選択（27-36 ページ）」を参照してください。

HTTP 要求パケットに URI が常に含まれているわけではないことに注意してください。ルールベースのイベントの場合、この行はパケットに HTTP ホスト名または HTTP URI が含まれている場合に表示されます。

HTTP 応答によってトリガーとして使用された侵入イベントの関連 HTTP URI を参照するには、[Perform Stream Reassembly on Both Ports] オプションに HTTP サーバのポートを設定する必要があります。ただし、これにより、トラフィックのリアセンブル用のリソース要求が増

加することに注意してください。ストリームの再アセンブリのオプションの選択（29-29 ページ）を参照してください。

Intrusion Policy

（存在する場合）侵入イベントを生成した侵入、プリプロセッサ、デコーダのルールが有効にされた侵入ポリシー。アクセス コントロール ポリシーのデフォルト アクションとして侵入ポリシーを選択するか、アクセス コントロール ルールと侵入ポリシーを関連付けることができます。デフォルトの処理の設定およびネットワーク トラフィックのインスペクション（12-7 ページ）および侵入防御を実行するアクセス コントロール ルールの設定（18-8 ページ）を参照してください。

Access Control Policy

イベントを生成した侵入ルール、プリプロセッサ ルール、またはデコーダ ルールが有効にされた侵入ポリシーが含まれるアクセス コントロール ポリシー。アクセス コントロール ポリシーの管理（12-12 ページ）を参照してください。

Access Control Rule

イベントを生成した侵入ルールと関連付けられたアクセス コントロール ルール。侵入防御を実行するアクセス コントロール ルールの設定（18-8 ページ）を参照してください。[Default Action] は、ルールが有効にされた侵入ポリシーがアクセス コントロール ルールに関連付けられていないことと、代わりにアクセス コントロール ポリシーのデフォルト アクションとして設定されていることを示します。デフォルトの処理の設定およびネットワーク トラフィックのインスペクション（12-7 ページ）を参照してください。

ルール

標準テキスト ルール イベントの場合、イベントを生成したルール。

イベントが、shared object rule、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

ルール データにはネットワークに関する機密情報が含まれるため、管理者はユーザが View Local Rules 権限を使用してパケット ビューでルール情報を表示できる機能を、ユーザ ロール エディタで切り替えることができます。詳細については、ユーザ特権とオプションの変更（61-58 ページ）を参照してください。

Actions

標準テキスト ルール イベントの場合は、[Actions] を展開して、イベントをトリガーとして使用したルールに対して次の操作のいずれかを実行します。

- ルールを編集する
- ルールのリビジョンのドキュメントを表示する
- ルールにコメントを追加する
- ルールの状態を変更する
- ルールのしきい値を設定する
- ルールを抑制する

詳細については、パケット ビュー アクションの使用（41-29 ページ）、パケット ビュー内でのしきい値オプションの設定（41-31 ページ）、およびパケット ビュー内での抑制オプションの設定（41-32 ページ）を参照してください。

イベントが、shared object rule、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

パケット ビュー アクションの使用

ライセンス：Protection

パケット ビューで、イベントを生成したルールの [Event Information] セクションにあるいくつかのアクションを実行できます。イベントが、shared object rule、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。ルールのアクションを表示するには、[Actions] を展開する必要があります。

編集

標準テキスト ルール イベントの場合、[Edit] をクリックして、イベントを生成したルールを変更します。

イベントが、shared object rule、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

注 Ciscoによって提供された（カスタム 標準テキスト ルール ではない）ルールを編集する場合、実際には新規のローカル ルールを作成していることになります。ローカル ルールを設定して、イベントを生成し、現在の侵入ポリシーで元のルールを無効にしていることを確認してください。ただし、デフォルトのポリシーのローカル ルールは有効に**できない**ことに注意してください。詳細については、既存のルールの変更（36-111 ページ）を参照してください。

マニュアルの表示

標準テキスト ルール イベントの場合、[View Documentation] をクリックして、イベントを生成したルール リビジョンの説明を確認します。

ルールのコメント

標準テキスト ルール イベントの場合、[Rule Comment] をクリックして、イベントを生成したルールにテキスト コメントを追加します。

これにより、ルールや、特定されたエクスプロイトまたはポリシー違反に関するコンテキストおよび情報を提供できます。さらに、ルール エディタでルールのコメントの追加および表示を行うこともできます。詳細については、ルールにコメントを追加する（36-112 ページ）を参照してください。

このルールを無効にする

このイベントが標準テキスト ルールによって生成された場合は、必要に応じてルールを無効にできます。ローカルで編集できるすべてのポリシーにルールを設定できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみにルールを設定することもできます。

詳細については、ルール状態の設定（32-22 ページ）を参照してください。

現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーを編集できますが、Ciscoが提供するデフォルト ポリシーは編集できません。

注 パケット ビューから shared object rule を無効にしたり、デフォルトのポリシーでルールを無効にしたりすることは**できません**。

イベントを生成するようにこのルールを設定する

このイベントが標準テキスト ルールによって生成された場合は、ルールを設定して、ローカルで編集できるすべてのポリシーでイベントを生成できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみにルールを設定することもできます。

詳細については、ルール状態の設定（32-22 ページ）を参照してください。

現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーを編集できますが、Ciscoが提供するデフォルト ポリシーは編集できません。

注　shared object ruleでパケット ビューからイベントを生成するようにを設定したり、デフォルト ポリシーのルールを無効にしたりすることは**できません**。

ドロップするようにこのルールを設定する

管理対象デバイスがネットワーク上でインライン展開されている場合、イベントをトリガーとして使用したルールを設定して、ローカルで編集できるすべてのポリシーでルールをトリガーするパケットをドロップできます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみにルールを設定することもできます。

現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーを編集できますが、Ciscoが提供するデフォルト ポリシーは編集できません。このオプションは [Drop when Inline] が現在のポリシーで有効になっている場合のみ表示されることに注意してください。詳細については、「インライン展開でのドロップ動作の設定（31-6 ページ）」を参照してください。

しきい値オプションを設定する

このオプションを使用して、ローカルで編集できるすべてのポリシーでも、これをトリガーとして使用したルールのしきい値を作成できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）でのみしきい値を作成することもできます。

しきい値オプションについては、パケット ビュー内でのしきい値オプションの設定（41-31 ページ）で説明します。

現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーは編集できますが、Ciscoが提供するデフォルトの侵入ポリシーは編集できません。

抑制オプションを設定する

このオブジェクトを使用して、ローカルで編集できるすべてのポリシーで、このイベントをトリガーとして使用したルールを抑制できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみでルールを制約することもできます。

抑制オプションについては、パケット ビュー内での抑制オプションの設定（41-32 ページ）で説明します。

現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーを編集できますが、Ciscoが提供するデフォルト ポリシーは編集できません。

パケット ビュー内でのしきい値オプションの設定

ライセンス：Protection

侵入イベントのパケット ビューでしきい値オプションを設定することによって、ルールごとに時間の経過とともに生成されるイベントの数を制御できます。ローカルで編集できるすべてのポリシーに、またはローカルで編集できる場合は現在のポリシー（つまり、イベントを生成したポリシー）のみに、しきい値オプションを設定できます。

パケット ビュー内でしきい値オプションを設定する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　侵入ルールによって生成された侵入イベントのパケット ビュー内で、[Event Information] セクションの [Actions] を展開し、[Set Thresholding Options] を展開し、次の 2 つのオプションのいずれかを選択します。

- **in the current policy**
- **in all locally created policies**

現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーを編集できますが、Ciscoが提供するデフォルト ポリシーは編集できません。

しきい値オプションが表示されます。

ステップ 2　設定するしきい値の種類を選択します。

- [limit] を選択して、通知を期間ごとに指定したイベント インスタンスの数に制限します。
- [threshold] を選択して、期間ごとに指定したイベント インスタンス数に達するたびに通知します。
- [both] を選択して、指定したイベント インスタンス数に達したら、期間ごとに 1 度通知します。

ステップ 3　イベント インスタンスを [Source] または [Destination] IP アドレスでトラックするかどうかを示すため、該当するオプション ボタンを選択します。

ステップ 4　[Count] フィールドに、しきい値として使用するイベント インスタンスの数を入力します。

ステップ 5　[Seconds] フィールドで、イベント インスタンスをトラックする期間を指定する 1 から 86400 までの数を入力します。

ステップ 6　既存の侵入ポリシーでこのルールの現在のしきい値をオーバーライドする場合、[Override any existing settings for this rule] を選択します。

ステップ 7　[Save Thresholding] をクリックします。

システムはしきい値を追加し、成功を示すメッセージを表示します。既存の設定をオーバーライドしない選択をした場合に競合が発生すると、競合を通知するメッセージが表示されます。

パケット ビュー内での抑制オプションの設定

ライセンス：Protection

抑制オプションを使用して、侵入イベントをまとめて、または発信元 IP アドレスまたは宛先 IP アドレスに基づいて抑制できます。ローカルで編集できるすべてのポリシーで抑制オプションを設定できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみに抑制オプションを設定することもできます。

パケット ビュー内で侵入イベントを抑制する方法:

アクセス: Admin/Intrusion Admin

ステップ 1　侵入ルールによって生成された侵入イベントのパケット ビュー内で、[Event Information] セクションの [Actions] を展開し、[Set Suppression Options] を展開し、次の 2 つのオプションのいずれかをクリックします。

- **in the current policy**
- **in all locally created policies**

現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーを編集できますが、Ciscoが提供するデフォルト ポリシーは編集できません。

抑制オプションが表示されます。

ステップ 2　次のいずれかの [Track By] オプションを選択します。

- このイベントをトリガーとして使用したルールのイベントを完全に抑制するには、[Rule] を選択します。
- 指定した送信元 IP アドレスから発信されたパケットによって生成されるイベントを抑制するには、[Source] を選択します。
- 指定した宛先 IP アドレスに入るパケットによって生成されるイベントを抑制するには、[Destination] を選択します。

ステップ 3　[IP address] または [CIDR block] フィールドで、発信元または宛先 IP アドレスとして指定する IP アドレスまたは CIDR ブロック/プレフィクス長を入力します。

FireSIGHT システムで CIDR 表記およびプレフィクス長を使用する方法の詳細については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ステップ 4　[Save Suppression] をクリックします。

侵入ポリシー内の抑制オプションは、ユーザの仕様に従って変更されます。既存の設定をオーバーライドしない選択をした場合に競合が発生すると、競合を通知するメッセージが表示されます。

フレーム情報の表示

ライセンス: Protection

パケット ビューで、[Frame] の横にある矢印をクリックして、キャプチャされたフレームに関する情報を表示します。パケット ビューには単一フレームまたは複数フレームを表示できます。各フレームには、個々のネットワークのパケットに関する情報が表示されます。たとえば、タグ付きパケットまたはリアセンブルされたTCP ストリーム内のパケットの場合、複数のフレームが表示されます。タグ付きパケットの詳細については、攻撃後トラフィックの評価（36-95 ページ）を参照してください。リアセンブルされた TCP ストリームの詳細については、TCP ストリームの再アセンブリ（29-29 ページ）を参照してください。

Frame n

キャプチャされたフレーム。*n* は単一フレーム パケットの場合は 1、複数フレーム パケットの場合は差分フレーム番号です。フレーム内のキャプチャされたバイト数はフレーム番号に追加されます。

Arrival Time

フレームがキャプチャされた日時。

Time delta from previous captured frame

複数フレーム パケットの場合、前のフレームがキャプチャされてからの経過時間。

Time delta from previous displayed frame

複数フレーム パケットの場合、前のフレームが表示されてからの経過時間。

Time since reference or first frame

複数フレーム パケットの場合、最初のフレームがキャプチャされてからの経過時間。

Frame Number

差分フレーム番号。

Frame Length

フレームの長さ（バイト単位）。

Capture Length

キャプチャされたフレームの長さ（バイト単位）。

Frame is marked

フレームがマークされているかどうか（true または false）。

Protocols in frame

フレームに含まれるプロトコル。

データリンク層情報の表示

ライセンス：Protection

パケット ビューで、データリンク層プロトコル（**イーサネット II** など）の横にある矢印をクリックして、パケットに関するデータリンク層情報を表示します。この情報には、送信元ホストと宛先ホストの 48 ビットの Media Access Control（MAC）アドレスが含まれています。ハードウェア プロトコルに応じて、パケットに関する他の情報も表示されることがあります。

注　この例では、イーサネット リンク層情報について説明していることに注意してください。他のプロトコルも表示されることがあります。

パケット ビューはデータリンク層で使用されるプロトコルを反映します。次のリストでは、パケット ビューでイーサネット II または IEEE 802.3 イーサネット パケットについて参照できる情報について説明します。

Destination

宛先ホストの MAC アドレス。

注　イーサネットは、宛先アドレスとしてマルチキャストおよびブロードキャスト アドレスを使用することもできます。

Source

送信元ホストの MAC アドレス。

タイプ

イーサネット II パケットの場合、イーサネット フレームでカプセル化されるパケットの種類。たとえば、IPv6 または ARP データグラム。この項目はイーサネット II パケットの場合にのみ表示されることに注意してください。

長さ

IEEE 802.3 イーサネット パケットの場合、チェックサムを含まないパケットのトータル長（バイト単位）。この項目はIEEE 802.3 イーサネット パケットの場合にのみ表示されることに注意してください。

ネットワーク層情報の表示

ライセンス： Protection

パケット ビューで、パケットにネットワーク層プロトコル（たとえば、[Internet Protocol]）の横にある矢印をクリックして、パケットに関連したネットワーク層の情報の詳細情報を表示します。

注　この例では、IP パケットについて説明していることに注意してください。他のプロトコルも表示されることがあります。

詳細については、次の項を参照してください。

- IPv4 ネットワーク層情報の表示（41-34 ページ）
- IPv6 ネットワーク層情報の表示（41-36 ページ）

IPv4 ネットワーク層情報の表示

ライセンス： Protection

以下のリストは、IPv4 パケットで表示される可能性があるプロトコル固有の情報の説明です。

Version

インターネット プロトコルのバージョン番号。

Header Length

すべての IP オプションを含む、見出しのバイト数。オプションのない IP 見出しの長さは 20 バイトです。

Differentiated Services Field

送信元ホストが明示的輻輳通知（ECN）サポートする方法を示す次の差別化サービスの値。

– `0x0`：ECN-Capable Transport（ECT）をサポートしません。

- 0x1 および 0x2：ECT をサポートします
- 0x3：Congestion Experienced（CE）

合計長

IP 見出しを差し引いた IP パケットの長さ（バイト単位）。

ID

送信元ホストから送信される IP データグラムを一意的に識別する値。この値は同じデータグラム フラグメントをトレースするために使用されます。

Flags

IP フラグメンテーションを制御する値。

[Last Fragment] の値は、データグラムに関連付けられた追加のフラグメントが存在するかどうかを次のように示します。

- 0：データグラムに関連付けられた追加のフラグメントは存在しない
- 1：データグラムに関連付けられた追加のフラグメントが存在する

[Don't Fragment] フラグの値は、データグラムをフラグメント化できるかどうかを次のように制御します。

- 0：データグラムをフラグメント化できる
- 1：データグラムをフラグメント化**してはならない**

フラグメント オフセット

データグラムの先頭からのフラグメント オフセットの値。

Time to Live (ttl)

データグラムが期限切れになる前にデータグラムがルータ間で作成できるホップの数。

Protocol

IP データグラムにカプセル化されるトランスポート プロトコル。たとえば、ICMP、IGMP、TCP、または UDP。

Header Checksum

IP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損したか、侵入回避の試行において使用中である可能性があります。

Source/Destination

送信元（または宛先）ホストの IP アドレスまたはドメイン名。

ドメイン名を表示するには、IP アドレス解決を有効にする必要があることに注意してください。詳細については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

アドレスまたはドメイン名をクリックしてコンテキスト メニューを表示してから、whois 検索を実行する場合は [Whois] を、ホスト情報を表示する場合は [View Host Profile] を、アドレスをグローバル ブラックリストまたはホワイトリストに追加する場合は [Blacklist Now] または [Whitelist Now] を選択します。ホスト プロファイルの使用（49-1 ページ） およびグローバル ホワイトリストおよびブラックリストの操作（3-7 ページ）を参照してください。

IPv6 ネットワーク層情報の表示

ライセンス：Protection

以下のリストは、IPv6 パケットで表示される可能性があるプロトコル固有の情報の説明です。

トラフィック クラス

IPv6 パケットのクラスまたは優先度を識別するための IPv6 ヘッダーの試験的な 8 ビット フィールド。IPv4 で提供される差別化サービス機能に類似しています。未使用の場合、このフィールドはゼロに設定されます。

フロー ラベル

非デフォルトの QoS やリアルタイム サービスなど、特別なフローを識別するオプションの 20 ビット IPv6 16 進数値（1 ～ FFFF）。未使用の場合、このフィールドはゼロに設定されます。

ペイロード長

IPv6 ペイロードのオクテットの数を特定する 16 ビット フィールド。このフィールドは、拡張ヘッダーなど、IPv6 ヘッダーに続くすべてのパケットから構成されます。

次ヘッダー

IPv6 ヘッダーのすぐ後に続く、ヘッダーの種類を特定する 8 ビットのフィールド。IPv4 プロトコル フィールドと同じ値が使用されます。

ホップ リミット

パケットを転送するノードごとに 1 つずつデクリメントする 8 ビットの 10 進整数。デクリメントした値がゼロになると、パケットは破棄されます。

Source

送信元ホストの 128 ビットの IPv6 アドレス。

Destination

宛先ホストの 128 ビットの IPv6 アドレス。

トランスポート層情報の表示

ライセンス：Protection

パケット ビューで、トランスポート層プロトコル（たとえば [TCP]、[UDP]、または [ICMP]）の横にある矢印をクリックして、パケットに関連した詳細情報を表示します。

ヒント　（存在する場合）[Data] をクリックして、パケット ビューの [Packet Information] セクションで、プロトコルのすぐ上にあるペイロードの最初の 24 バイトを表示します。

次の各プロトコルのトランスポート層の内容は、以下で説明されています。

- TCP パケット ビュー（41-37 ページ）
- UDP パケット ビュー（41-38 ページ）
- ICMP パケット ビュー（41-38 ページ）

注　これらの例では、TCP、UDP、および ICMP パケットについて説明していることに注意してください。他のプロトコルも表示されることがあります。

TCP パケット ビュー

ライセンス: Protection

ここでは、TCP パケットのプロトコル固有の情報について説明します。

送信元ポート

発信元のアプリケーション プロトコルを識別する番号。

宛先ポート

受信側のアプリケーション プロトコルを識別する番号。

シーケンス番号

TCP ストリームの初期シーケンス番号と連動する、現在の TCP セグメントの最初のバイトの値。

Next sequence number

応答パケットにおける、送信する次のパケットのシーケンス番号。

Acknowledgement number

以前に受信されたデータのシーケンス番号に連動したTCP 確認応答。

Header Length

見出しのバイト数。

Flags

TCP セグメントの転送状態を示す 6 ビット。

- U:緊急ポインタが有効
- A:確認応答番号が有効
- P:受信者はデータをプッシュする必要がある
- R:接続をリセットする
- S:シーケンス番号を同期して新しい接続を開始する
- F:送信者はデータ送信を終了した

ウィンドウ サイズ

受信ホストが受け入れる、確認応答されていないデータの量(バイト単位)。

チェックサム

TCP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損したか、回避の試行において使用中である可能性があります。

Urgent Pointer

緊急データが終了する TCP セグメントの位置(存在する場合)。U フラグとともに使用します。

Options

TCP オプションの値(存在する場合)。

UDP パケット ビュー

ライセンス: Protection

ここでは、UDP パケットのプロトコル固有の情報について説明します。

送信元ポート

発信元のアプリケーション プロトコルを識別する番号。

宛先ポート

受信側のアプリケーション プロトコルを識別する番号。

長さ

UDP 見出しとデータを組み合わせた長さ。

チェックサム

UDP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損した可能性があります。

ICMP パケット ビュー

ライセンス: Protection

ここでは、ICMP パケットのプロトコル固有の情報について説明します。

タイプ

ICMP メッセージのタイプ。

- 0:エコー応答
- 3:宛先到達不能
- 4:ソース クエンチ(始点抑制要求)
- 5:リダイレクト
- 8:エコー要求
- 9:ルータ アドバタイズメント
- 10:ルータ送信要求
- 11:時間超過
- 12:パラメータの問題
- 13:タイムスタンプ要求
- 14:タイムスタンプ応答
- 15:情報要求(廃止)
- 16:情報応答(廃止)
- 17:アドレス マスク要求
- 18:アドレス マスク応答

コード

ICMP メッセージ タイプに付随するコード。ICMP メッセージ タイプ 3、5、11、および 12 には、RFC 792 で説明されている対応コードがあります。

チェックサム

ICMP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損した可能性があります。

パケット バイト情報の表示

ライセンス：Protection

パケット ビューで、[Packet Bytes] の横にある矢印をクリックして、パケットを構成するバイトの 16 進数および ASCII バージョンを表示します。システムがトラフィックを復号化した場合は、復号化されたパケット バイトを表示できます。

影響レベルを使用してイベントを評価する

ライセンス：Protection

イベントがネットワークに与える影響を評価するために、Defense Centerは侵入イベントのテーブル ビューに影響レベルを表示します。イベントごとに、Defense Centerは影響レベル アイコンを追加し、侵入データ、ネットワーク検出 データ、脆弱性情報との関係を色で示します。

注 NetFlow データに基づいてネットワーク マップに追加されたホストで使用可能なオペレーティング システム情報が存在しない場合、ホスト入力機能を使用してホストのオペレーティング システム ID を手動で設定しない限り、Defense Centerはこれらのホストに関係した侵入イベントに対して影響レベル [Vulnerable]（影響レベル 1：赤）を割り当てることはできません。

次の表に、影響レベルで使用可能な値を示します。

表 41-6　影響レベル

影響レベル	脆弱性	色	説明
0	不明（Unknown）	グレー	送信元ホストと宛先ホストは両方ともネットワーク検出によってモニタされているネットワーク上に存在しません。
1	脆弱	レッド	次のいずれかを行います。 • 送信元ホストまたは宛先ホストはネットワーク マップ内にあり、脆弱性はホストにマッピングされます • 送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵害される可能性があります。詳細については、影響レベル 1 の設定（36-49 ページ）を参照してください。

表 41-6　影響レベル（続き）

影響レベル	脆弱性	色	説明
2	潜在的に脆弱	オレンジ	送信元ホストまたは宛先ホストはネットワーク マップ内にあり、次のいずれかに当てはまります。 • ポート指向のトラフィックの場合、ポートはサーバ アプリケーション プロトコルを実行しています • ポート指向ではないトラフィックの場合、ホストはプロトコルを使用します
3	現在は脆弱ではない	黄色	送信元ホストまたは宛先ホストはネットワーク マップ内にあり、次のいずれかに当てはまります。 • ポート指向のトラフィック（TCP や UDP など）の場合、ポートは開いていません • ポート指向ではないトラフィック（ICMP など）の場合、ホストはプロトコルを使用しません
4	不明なターゲット	ブルー	送信元ホストまたは宛先ホストがモニタ対象のネットワークにありますが、ネットワーク マップ内にそのホストのエントリがありません。

テーブル ビューの影響レベルを使用してイベントを評価する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Analysis] > [Intrusions] > [Events] を選択します。

デフォルトの侵入イベントのワークフローの最初のページが表示されます。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。イベントが表示されない場合は、時間範囲の調整が必要になることがあります。イベント時間の制約の設定（58-26 ページ）を参照してください。

ステップ 2　評価するイベントのみを表示するには、イベント ビューを制約します。

詳細については、ドリルダウン ページとテーブル ビュー ページの使用（41-20 ページ）を参照してください。

ステップ 3　ページの上部にある [Table View of Events] をクリックします。

イベントのテーブル ビューが表示されます。[Impact] には、影響レベルの表に記載されているいずれかの値が入ります。

ステップ 4　影響レベルでテーブルをソートするには、[Impact] をクリックします。

イベントは影響レベルでソートされます。

ヒント　ソート順序を反転させるには、もう一度 [Impact] をクリックします。

プリプロセッサ イベントの読み取り

ライセンス：Protection

プリプロセッサは 2 つの機能を備えています。指定されたアクション（HTTP トラフィックのデコード化や正規化など）をパケットに対して実行する機能と、指定されたプリプロセッサ オプションの実行をレポートする機能です。これは、関連するプリプロセッサ ルールが有効になっている場合に、パケットによって指定のプリプロセッサ オプションがトリガーされたときに、常にイベントを生成することによって実現されます（たとえば、HTTP Inspect ジェネレータ（GID）119 と Snort ID（SID）2 に関連するプリプロセッサ ルールと、[Double Encoding] HTTP Inspect オプションを有効にすると、プリプロセッサが IIS 二重エンコード トラフィックを検出したときにイベントを生成できます）。プリプロセッサの実行を報告するイベントを生成すると、異常なプロトコル エクスプロイトを検出するのに役立ちます。たとえば、攻撃者は、ホスト上で DoS 攻撃を引き起こす重複 IP フラグメントを細工することがあります。IP 最適化のプリプロセッサはこのタイプの攻撃を検出し、それに関する侵入イベントを生成できます。

詳細については、次の項を参照してください。

- プリプロセッサ イベントのパケットの表示について（41-41 ページ）では、プリプロセッサで生成されたイベントに含まれる情報ついて説明しています。
- プリプロセッサ ジェネレータ ID の読み取り（41-42 ページ）は、プリプロセッサ ジェネレータ ID によって提供される情報について詳述します。

プリプロセッサ イベントのパケットの表示について

ライセンス：Protection

プリプロセッサ イベントは、イベントに関するルールの詳細な説明がパケットの表示に含まれないという点がルール イベントと異なります。代わりに、パケット ディスプレイには、イベント メッセージ、ジェネレータ ID、Snort ID、パケット 見出し データおよびパケット ペイロードが表示されます。これにより、パケットの見出し情報を解析し、その見出し オプションが使用中かどうか判断し、それがシステムをエクスプロイトする可能性がある場合は、パケット ペイロードを検査できます。プリプロセッサによる各パケットの解析が完了すると、ルール エンジンは、パケットに対して適切なルールを実行し（プリプロセッサが各パケットを最適化し、有効なセッションの一部として確立できた場合）、潜在的なコンテンツ レベルの脅威についてさらに解析を行い、それらのパケットについてレポートします。

プリプロセッサ ジェネレータ ID の読み取り

ライセンス：Protection

各プリプロセッサには、パケットによってトリガーとして使用されたプリプロセッサを示す独自のジェネレータ ID 番号、つまり GID があります。一部のプリプロセッサには関連した SID もあります。これは、潜在的な攻撃を分類する ID 番号です。これにより、ルールの Snort ID（SID）がルールをトリガーするパケットのコンテキストを提供するのとほぼ同じ方法で、イベントのタイプを分類することによって、より効率的にイベントを解析できます。侵入ポリシーの [Rules] ページでは、[Preprocessors] フィルタ グループでプリプロセッサ別にルールを一覧表示できます。また、プリプロセッサのプリプロセッサ ルールや [Category] フィルタ グループのパケット デコーダ サブグループを一覧表示することもできます。詳細については、ルールを使用した侵入ポリシーの調整（32-1 ページ）および表 32-1（32-2 ページ）を参照してください。

注　標準テキスト ルールによって生成されたイベントのジェネレータ ID は 1 です。イベントの SID は、トリガーとして使用された特定のルールを示します。shared object ruleの場合、イベントにはジェネネレータ ID 3 と、トリガーとして使用された特定のルールを示す SID が含まれます。

次の表に、各 GID を生成するイベントの種類を示します。

表 41-7　ジェネレータ ID

ID	コンポーネント	説明	詳細情報の参照先
1	標準テキスト ルール	イベントは、パケットが標準テキスト ルールをトリガーとして使用したときに生成されました。	表 32-1（32-2 ページ）
2	タグ付きパケット	イベントは、タグ付きセッションからパケットを生成するタグ ジェネレータによって生成されました。これは、[tag] ルール オプションが使用された場合に発生します。	攻撃後トラフィックの評価（36-95 ページ）
3	共有オブジェクト ルール	イベントは、パケットがshared object ruleをトリガーとして使用したときに生成されました。	表 32-1（32-2 ページ）
102	HTTP デコーダ	デコーダ エンジンがパケット内の HTTP データを復号化しました。	HTTP トラフィックのデコード（27-33 ページ）
105	Back Orifice ディテクタ	Back Orifice ディテクタが、パケットに関連付けられた Back Orifice 攻撃を特定しました。	バック オリフィスの検出（34-2 ページ）
106	RPC デコーダ	RPC デコーダがパケットを復号化しました。	Sun RPC プリプロセッサの使用（27-49 ページ）
116	パケット デコーダ	イベントはパケット デコーダによって作成されました。	パケットのデコードについて（29-18 ページ）
119、120	HTTP 検査プリプロセッサ	イベントは HTTP 検査プリプロセッサによって生成されました。GID 120 ルールは、サーバ固有の HTTP トラフィックに関連しています。	HTTP トラフィックのデコード（27-33 ページ）
122	ポートスキャン ディテクタ	イベントはポートスキャン フロー ディテクタによって生成されました。詳細を参照してください。	ポートスキャンの検出（34-3 ページ）
123	IP デフラグメンタ	イベントは、フラグメント化された IP データグラムを正しくリアセンブルできなかったときに生成されました。	IP パケットのデフラグ（29-12 ページ）
124	SMTP デコーダ	イベントは、SMTP プリプロセッサが SMTP verb に対するエクスプロイトを検出したときに生成されました。	SMTP デコードについて（27-64 ページ）
125	FTP デコーダ	イベントは、FTP/Telnet デコーダが FTP トラフィック内でエクスプロイトを検出したときに生成されました。	サーバレベルの FTP オプションについて（27-24 ページ） クライアントレベルの FTP オプションについて（27-30 ページ）
126	Telnet デコーダ	イベントは、FTP/Telnet デコーダが telnet トラフィック内でエクスプロイトを検出したときに生成されました。	FTP および Telnet トラフィックのデコード（27-20 ページ）

表 41-7　ジェネレータ ID（続き）

ID	コンポーネント	説明	詳細情報の参照先
128	SSH プリプロセッサ	イベントは、SSH プリプロセッサが SSH トラフィック内でエクスプロイトを検出したときに生成されました。	SSH プロプロセッサによるエクスプロイトの検出（27-71 ページ）
129	ストリーム プリプロセッサ	イベントはストリームの前処理時にストリーム プリプロセッサによって生成されました。	TCP ストリームの前処理の使用（29-22 ページ）
131	DNS プリプロセッサ	イベントは DNS プリプロセッサによって生成されました。	DNS ネーム サーバ応答におけるエクスプロイトの検出（27-16 ページ）
133	DCE/RPC プリプロセッサ	イベントは DCE/RPC プリプロセッサによって生成されました。	DCE/RPC トラフィックのデコード（27-2 ページ）
134	ルール遅延 パケット遅延	ルールの遅延によって侵入ルールのグループが中断（134:1）または再有効化（134:2）されたとき、またはパケットの遅延しきい値に達したためにシステムがパケットの検査を停止（134:3）したときに、イベントが生成されました。	パケットおよび侵入ルール遅延しきい値の設定（18-14 ページ）
135	レートベースの攻撃ディテクタ	イベントは、レートベースの攻撃ディテクタがネットワーク上のホストに対する過剰な接続数を識別したときに生成されました。	レート ベース攻撃の防止（34-10 ページ）
138、139	センシティブ データ プリプロセッサ	イベントは、センシティブ データ プリプロセッサによって生成されました。	センシティブ データの検出（34-20 ページ）
140	SIP プリプロセッサ	イベントは SIP プリプロセッサによって生成されました。	Session Initiation Protocol のデコード（27-51 ページ）
141	IMAP プリプロセッサ	イベントは IMAP プリプロセッサによって生成されました。	IMAP トラフィックのデコード（27-57 ページ）
142	POP プリプロセッサ	イベントは POP プリプロセッサによって生成されました。	POP トラフィックのデコード（27-60 ページ）
143	GTP プリプロセッサ	イベントは GTP プリプロセッサによって生成されました。	GTP コマンド チャネルの設定（27-55 ページ）
144	Modbus プリプロセッサ	イベントは Modbus SCADA プリプロセッサによって生成されました。	Modbus プリプロセッサの設定（28-1 ページ）
145	DNP3 プリプロセッサ	イベントは DNP3 SCADA プリプロセッサによって生成されました。	DNP3 プリプロセッサの設定（28-3 ページ）

侵入イベントの検索

ライセンス：Protection

FireSIGHT システムで配信された定義済み検索を使用するか、または独自の検索基準を作成することによって特定の侵入イベントを検索できます。

定義済み検索は例として使用でき、これによりネットワークに関する重要な情報に素早くアクセスできます。デフォルトの検索内の特定のフィールドを変更して、使用するネットワーク環境に合わせてカスタマイズし、後で再利用できるようにそれらを保存することもできます。覚えて

おくべき点として、検索結果は、検索するイベントの使用可能なデータに依存します。つまり、使用可能なデータによっては、検索の制限が適用されないことがあります。たとえば、復号化されたトラフィックでトリガーされた侵入イベントだけが SSL 情報を含んでいます。

ヒント　侵入イベント検索で IP アドレスとポートを指定するための構文の詳細については、検索での IP アドレスの指定（60-6 ページ）および検索でのポートの指定（60-8 ページ）を参照してください。

保存済み検索のロードおよび削除方法を含む、検索の詳細については、イベントの検索（60-1 ページ）を参照してください。

使用できる検索条件を以下に示します。

プライオリティ

表示するイベントの優先度を指定します。優先度は、`priority` キーワードの値または `classtype` キーワードの値に対応します。その他の侵入イベントの場合、プライオリティはデコーダまたはプリプロセッサによって決定されます。有効な値は、`high`、`medium`、および `low` です。

Impact

侵入データとネットワーク検出 データの相互関係に基づいて、侵入イベントに割り当てる影響レベルを指定します。大文字と小文字を区別しない有効な値は、`Impact 0`、`Impact Level 0`、`Impact 1`、`Impact Level 1`、`Impact 2`、`Impact Level 2`、`Impact 3`、`Impact Level 3`、`Impact 4`、および `Impact Level 4` です。

影響アイコンの色や部分文字列（たとえば `blue`、`level 1`、`0` など）を使用しないでください。

詳細については、影響レベルを使用してイベントを評価する（41-39 ページ）を参照してください。

Inline Result

次のいずれかを入力してください。

- `dropped`。パケットがインライン展開環境でパケットをドロップするかどうかを指定します
- `would have dropped`。インライン展開環境でパケットをドロップするように侵入ポリシーが設定されている場合に、パケットをドロップするかどうかを指定します

侵入ポリシーのルールの状態またはインライン ドロップ動作にかかわらず、インライン インターフェイスがタップ モードになっている場合を含め、パッシブ展開環境ではシステムはパケットをドロップしないことに注意してください。

Source IP

侵入イベントに関連する送信元ホストが使用する IP アドレスを指定します。

Destination IP

侵入イベントに関連する宛先ホストが使用する IP アドレスを指定します。

Source/Destination IP

侵入イベントを表示するホストによって使用される送信元または宛先 IP アドレスを指定します。

Source Country

侵入イベントに関連する送信元ホストの国を指定します。

Destination Country

侵入イベントに関連する宛先ホストの国を指定します。

Source/Destination Country

表示する侵入イベントに関連する送信元または宛先ホストの国を指定します。

Source Continent

侵入イベントに関連する送信元ホストの大陸を指定します。

Destination Continent

侵入イベントに関連する宛先ホストの大陸を指定します。

Source/Destination Continent

表示する侵入イベントに関連する送信元または宛先ホストの大陸を指定します。

Original Client IP

X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義の HTTP ヘッダーから取得された、元のクライアント IP アドレスを指定します。侵入イベントのこのフィールドの値を取得するには、HTTP プリプロセッサ [Extract Original Client IP Address] オプションを有効にする必要があります。オプションで、ネットワーク解析ポリシーの同じエリアで、最大 6 つのカスタム クライアント IP 見出しを指定し、システムが [Original Client IP] イベント フィールドの値を選択する優先順位を設定します。詳細については、「サーバレベル HTTP 正規化オプションの選択（27-36 ページ）」を参照してください。

プロトコル

http://www.iana.org/assignments/protocol-numbers に一覧表示されている、接続で使用するトランスポート プロトコルの名前または番号を入力します。

侵入イベントのテーブル ビューには [Protocol] 列がないことに注意してください。これは、送信元および宛先ポート/ICMP の列と関連付けられたプロトコルです。

Source Port / ICMP Type

侵入イベントに関連する送信元ポートを指定します。

ヒント　ICMP トラフィックの場合、ポートをターゲットとしないため、このフィールドを使用して特定の ICMP タイプのイベントを検索することができます。

Destination Port / ICMP Code

侵入イベントに関連する宛先ポートを指定します。

ヒント　ICMP トラフィックの場合、ポートをターゲットとしないため、このフィールドを使用して特定の ICMP コードのイベントを検索することができます。

VLAN ID

侵入イベントをトリガーとして使用したパケットと関連付けられた内部 VLAN ID を指定します。

MPLS Label

侵入イベントをトリガーとして使用したパケットと関連付けられたマルチプロトコル ラベル スイッチング ラベルを指定します。

メッセージ

表示するイベントのイベント メッセージのすべてまたは一部を指定します。

分類

表示するイベントを生成したルールの分類番号を入力するか、分類名または説明のすべてまたは一部を入力します。また、番号、名前、または説明をカンマで区切ったリストを入力することもできます。最後に、カスタム分類を追加した場合、その名前または説明のすべてまたは一部を使用して検索することもできます。分類の番号、名前、および説明のリストについては、ルール分類の表を参照してください。

Generator

表 41-7（41-42 ページ）に示されている、表示するイベントを生成したコンポーネントを指定します。

Snort ID

イベントを生成したルールの Snort ID（SID）を指定するか、オプションで、ルールの複合ジェネレータ ID（GID）および SID を指定します。ここで、GID および SID は、コロン（:）で区切られ、GID:SID の形式になります。次の表の任意の値を指定できます。

表 41-8　Snort ID の検索値

値	例
単一の SID	10000
SID の範囲	10000-11000
SID より大きい	>10000
SID 以上	>=10000
SID 未満	<10000
SID 以下	<=10000
SID のコンマ区切りリスト	10000,11000,12000
単一の GID:SID の組み合わせ	1:10000
GID:SID の組み合わせのコンマ区切りリスト	1:10000,1:11000,1:12000
SID および GID:SID の組み合わせのコンマ区切りリスト	10000,1:11000,12000

詳細については、プリプロセッサ ジェネレータ ID の読み取り（41-42 ページ）を参照してください。

Snort ID 列は検索結果に表示されないことに注意してください。ユーザが表示するイベントの SID は [Message] 列にリストされます。

Source User

送信元ホストにログインしているユーザのユーザ ID を指定します。

Destination User

宛先ホストにログインしているユーザのユーザ ID を指定します。

Source/Destination User

送信元または宛先ホストにログインしているユーザのユーザ ID を指定します。

アプリケーション プロトコル

侵入イベントをトリガーとして使用したトラフィックで検出された、ホスト間の通信を表すアプリケーション プロトコルの名前を入力します。

クライアント

侵入イベントをトリガーとして使用したトラフィックで検出されたモニタ対象のホストで実行されているソフトウェアを表す、クライアント アプリケーションの名前を入力します。

Web アプリケーション

侵入イベントをトリガーとして使用したトラフィックで検出された HTTP トラフィックの内容または要求された URL を表す、Web アプリケーションの名前を入力します。

Category、Tag（Application Protocol、Client、Web Application）

セッションで検出されたアプリケーションに関連するカテゴリまたはタグを入力します。複数のカテゴリまたはタグを指定する場合はカンマで区切ります。これらのフィールドでは、大文字と小文字は区別されません。

Application Risk

セッションで検出されたアプリケーションに関連する最も高いリスクを入力します。有効な条件は次のとおりです。`Very High`、`High`、`Medium`、`Low`、および `Very Low`。これらのフィールドでは、大文字と小文字は区別されません。

Business Relevance

セッションで検出されたアプリケーションに関連する最も低いビジネスとの関連性を入力します。有効な条件は次のとおりです。`Very High`、`High`、`Medium`、`Low`、および `Very Low`。これらのフィールドでは、大文字と小文字は区別されません。

Security Zone (Ingress、Egress、Ingress/Egress)

イベントをトリガーとして使用したパケットと関連付けられたセキュリティ ゾーンの名前を指定します。これらのフィールドでは、大文字と小文字は区別されません。セキュリティ ゾーンの操作（3-42 ページ）を参照してください。

デバイス

アクセス コントロール ポリシーが適用された特定のデバイスに限定して検索するには、デバイスの名前または IP アドレス、デバイス グループ、スタック、またはクラスタ名を入力します。FireSIGHT システム が検索でデバイス フィールドを処理する方法については、検索でのデバイスの指定（60-7 ページ）を参照してください。

スタック構成設定では、プライマリ デバイスとセカンダリ デバイスは、侵入イベントを別々にレポートすることに注意してください。詳細については、「スタックに含まれるデバイスの管理（4-46 ページ）」を参照してください。

セキュリティ コンテキスト

トラフィックが通過した仮想ファイアウォール グループを特定するセキュリティ コンテキストの名前を入力します。システムがこのフィールドにデータを設定するのは、マルチコンテキスト モードの ASA FirePOWER デバイスだけです。

Interface（Ingress、Egress）

イベントをトリガーとして使用したパケットと関連付けられたインターフェイスの名前を入力します。センシング インターフェイスの設定（4-64 ページ）を参照してください。

Intrusion Policy

イベントと関連付けられた侵入ポリシー名を入力します。侵入ポリシーの管理（31-3 ページ）を参照してください。

Access Control Policy

イベントと関連付けられたアクセス コントロール ポリシー名を入力します。アクセス コントロール ポリシーの管理（12-12 ページ）を参照してください。

Access Control Rule

イベントに関連付けられているアクセス コントロール ポリシーの名前を入力します（アクセス コントロール ルールを使用したトラフィック フローの調整（14-1 ページ）を参照）。

HTTP Hostname

HTTP 要求のホスト 見出しから取得された単一のホスト名を指定します。

ホスト名を HTTP クライアント トラフィックの侵入イベントと関連付けるには、HTTP 検査プリプロセッサの [Log Headers] オプションを有効にする必要があります。詳細については、「サーバレベル HTTP 正規化オプションの選択（27-36 ページ）」を参照してください。

HTTP URI

侵入イベントをトリガーとして使用した HTTP 要求パケットと関連付けられた単一 URI を指定します。

URI を HTTP クライアント トラフィックの侵入イベントと関連付けるには、HTTP 検査プリプロセッサの [Log URI] オプションを有効にする必要があります。詳細については、「サーバレベル HTTP 正規化オプションの選択（27-36 ページ）」を参照してください。

Email Sender

SMTP MAIL FROM コマンドから取得された電子メール送信者のアドレスを指定します。また、コンマ区切りリストを入力して、すべての指定アドレスに関連付けられているイベントを検索することもできます。詳細については、「侵入イベントについて（41-11 ページ）」を参照してください。

Email Recipient

SMTP RCPT TO コマンドから取得された電子メール受信者のアドレスを指定します。また、コンマ区切りリストを入力して、すべての指定アドレスに関連付けられているイベントを検索することもできます。詳細については、「侵入イベントについて（41-11 ページ）」を参照してください。

Email Attachments

MIME Content-Disposition ヘッダーから取得された MIME 添付ファイル名を指定します。リスト内のすべての添付ファイル名に関連付けられているイベントを検索するには、コンマ区切りリストを入力します。詳細については、「侵入イベントについて（41-11 ページ）」を参照してください。

Email Headers

電子メール 見出しから取得したデータを指定します。電子メール 見出しは侵入イベントのテーブル ビューには表示されませんが、電子メール 見出し データは検索条件として使用できることに注意してください。

電子メール 見出しを SMTP トラフィックの侵入イベントと関連付けるには、SMTP プリプロセッサの [Log Headers] オプションを有効にする必要があります。詳細については、「SMTP デコードについて（27-64 ページ）」を参照してください。

Reviewed By

イベントを確認したユーザの名前を指定します。侵入イベントについて（41-17 ページ）を参照してください。

ヒント　`unreviewed` と入力すると、まだ確認されていないイベントを検索できます。

侵入イベントの特別な検索構文

前述の一般的な検索構文の補足として、以下でマルウェア イベントの特別な検索構文について説明します。

The SSL Actual Action taken

アクションを指定して、そのアクションが適用された暗号化トラフィックに対する侵入イベントを表示するには、次のいずれかのキーワードを入力します。

- [Do not Decrypt] は、システムが復号化しなかった接続を表します。
- [Block] および [Block with reset] は、ブロックされた暗号化接続を表します。
- [Decrypt (Known Key)] は、既知の秘密キーを使用して復号化された着信接続を表します。
- [Decrypt (Replace Key)] は、置き換えられた公開キーと自己署名サーバ証明書を使用して復号化された発信接続を表します。
- [Decrypt (Resign)] は、再署名サーバ証明書を使用して復号化された発信接続を表します。

この列は、侵入イベント テーブル ビューには表示されません。

The SSL Failure Reason

指定した理由で、復号化に失敗した暗号化トラフィックに対する侵入イベントを表示するには、次のいずれかのキーワードを入力します。

- `Unknown`
- `No Match`
- `Success`
- `Uncached Session`
- `Unknown Cipher Suite`
- `Unsupported Cipher Suite`
- `Unsupported SSL Version`
- `SSL Compression Used`

- Session Undecryptable in Passive Mode
- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup
- Internal Error
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- Invalid Action

この列は、侵入イベント テーブル ビューには表示されません。

The SSL Subject Country

証明書の対象国に関連付けられている暗号化トラフィックに対する侵入イベントを表示するには、2 文字の ISO 3166-1 alpha-2 国番号を入力します。

この列は、侵入イベント テーブル ビューには表示されません。

The SSL Issuer Country

証明書の発行国に関連付けられている暗号化トラフィックに対する侵入イベントを表示するには、2 文字の ISO 3166-1 alpha-2 国番号を入力します。

この列は、侵入イベント テーブル ビューには表示されません。

SSL Certificate Fingerprint

証明書に関連付けられているトラフィックに対する侵入イベントを表示するには、証明書の認証に使用された SHA ハッシュ値を入力するか、貼り付けます。

この列は、侵入イベント テーブル ビューには表示されません。

SSL Public Key Fingerprint

証明書に関連付けられているトラフィックに対する侵入イベントを表示するには、証明書に含まれている公開キーの認証に使用された SHA ハッシュ値を入力するか、貼り付けます。

この列は、侵入イベント テーブル ビューには表示されません。

侵入イベントを検索する方法:

アクセス: Admin/Intrusion Admin

ステップ 1　[Analysis] > [Search] を選択します。

[Intrusion Events] 検索ページが表示されます。

侵入イベントのリストを表示しているときに（[Analysis] > [Intrusions] > [Events]）、[Search] をクリックすることもできます。

ステップ 2　手順の上の表に示されているように、該当するフィールドに検索条件を入力します。

- 検索でのオブジェクトの使用を含む、検索の構文の詳細については、イベントの検索（60-1 ページ）を参照してください。
- 公開キー証明書に関連するフィールドについては、暗号化接続に関連付けられた証明書の表示（39-33 ページ）を参照してください。
- 侵入イベントの特別な検索構文の詳細については、侵入イベントの特別な検索構文（41-49 ページ）を参照してください。

ステップ 3　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　カスタム ユーザ ロールに関するデータ制約として検索を使用する予定の場合は、それをプライベート検索として保存する**必要があります**。

ステップ 4　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。
- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save as New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 5　検索を開始するには、[Search] ボタンをクリックします。

検索結果は、現在の時刻範囲によって制約される、デフォルトの侵入イベント ワークフローに表示されます。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

クリップボードの使用

ライセンス：Protection

クリップボードは、任意の侵入イベント ビューから侵入イベントをコピーできる保存エリアです。クリップボードにイベントを追加する方法については、ドリルダウン ページとテーブル ビュー ページの使用（41-20 ページ）およびパケット ビューの使用（41-23 ページ）を参照してください。

クリップボードの内容は、イベントが生成された日時別にソートされます。クリップボードに侵入イベントを追加した後、クリップボードからそれらを削除することも、クリップボードの内容のレポートを生成することもできます。

クリップボードの侵入イベントをインシデントに追加することもできます。インシデントとは、セキュリティ ポリシーの違反の可能性に関係していると思われるイベントのコンパイルです。クリップボードからインシデントにイベントを追加する方法の詳細については、インシデントの作成（42-5 ページ）を参照してください。

詳細については、次の項を参照してください。

- クリップボードのレポートの生成（41-52 ページ）
- クリップボードからのイベントの削除（41-53 ページ）

クリップボードのレポートの生成

ライセンス： Protection

任意のイベント ビューで行うのと同じように、クリップボードのイベントに関するレポートを生成できます。

クリップボードの侵入イベントのレポートを生成する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　次のように、クリップボードに 1 つ以上のイベントを追加します。

- ドリルダウン ページまたはイベントのテーブル ビューからクリップボードにイベントを追加する方法については、ドリルダウン ページとテーブル ビュー ページの使用（41-20 ページ）を参照してください。
- パケット ビューからクリップボードにイベントを追加する方法については、パケット ビューの使用（41-23 ページ）を参照してください。

ステップ 2　[Analysis] > [Intrusions] > [Clipboard] を選択します。

クリップボードが表示されます。

ステップ 3　次の選択肢があります。

- クリップボード上のページの特定のイベントを含めるには、そのページに移動し、イベントの横にあるチェック ボックスを選択し、[Generate Report] をクリックします。
- クリップボードのすべてのイベントを含めるには、[Generate Report] をクリックします。

いずれの場合も、[Report Templates] ページが表示されます。

ステップ 4　レポートの表示方法を指定してから、[Generate] をクリックします。

[Generate Report] ポップアップ ダイアログが表示されます。

ステップ 5　1 つ以上の出力形式（HTML、PDF、CSV）を選択し、オプションで、他の設定を変更します。

ヒント　レポート デザイナの使用方法の詳細については、レポートの操作（57-1 ページ）を参照してください。

ステップ 6　[Generate] をクリックし、[Yes] をクリックします。

[Report Generation Complete] ポップアップ ウィンドウと、レポートを表示するためのリンクが表示されます。

ステップ 7　次のいずれかをクリックします。

- レポートのリンク。新しいウィンドウが開き、選択したレポートが表示されます。
- [OK]。レポートのデザインを変更できる [Report Templates] ページに戻ります。

クリップボードからのイベントの削除

ライセンス： Protection

インシデントに追加したくない侵入イベントがクリップボード上に存在する場合は、そのイベントを削除できます。

注　クリップボードからイベントを削除しても、イベント データベースからイベントは削除**されません**。ただし、イベント データベースからイベントを削除すると、イベントはクリップボードから削除されます。

イベントをクリップボードから削除する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Analysis] > [Intrusions] > [Clipboard] を選択します。

クリップボードが表示されます。

ステップ 2　次の選択肢があります。

- クリップボード上のページの特定の侵入イベントを削除するには、そのページに移動し、イベントの横にあるチェック ボックスを選択し、[Delete] をクリックします。

  イベントが削除されます。
- クリップボードのすべてのイベントを削除するには、[Delete All] をクリックします。

  すべてのイベントがクリップボードから削除されます。[Event Preferences] で [Confirm 'All' Actions] オプションを選択した場合、最初にすべてのイベントを削除するかどうか確認するプロンプトが出されることに注意してください。

インシデント対応

インシデント対応とは、セキュリティ ポリシーの違反が疑われる場合に組織が取る対応を指します。FireSIGHT システムには、インシデントの調査に関連する情報の収集および処理をサポートする機能が含まれます。これらの機能を使用して、インシデントに関連する可能性のある侵入イベントおよびパケット データを収集することができます。攻撃の影響を軽減するために FireSIGHT システムの外部で実行するアクティビティに関する記録のためのリポジトリとしてインシデントを使用できます。たとえば、セキュリティ ポリシーによって、ネットワークの安全性に問題のあるホストの検疫が要求される場合は、インシデントにそのことを記録できます。

FireSIGHT システムはインシデントのライフ サイクルもサポートします。これにより、攻撃への対応を進めるごとに、インシデントのステータスを変更できます。インシデントを閉じるときに、学んだ教訓の結果としてセキュリティ ポリシーに加えた変更を記録できます。

FireSIGHT システムでのインシデントの対応に関する詳細については、以下のセクションを参照してください。

インシデント対応の基本

ライセンス： Protection

各組織には、セキュリティ ポリシーの違反を検出し、定義し、対応するための独自のプロセスがある場合があります。続くセクションでは、インシデント対応の基本、および FireSIGHT システムをインシデント対応計画にどのように組み込むことができるかについて説明します。

インシデントの定義

ライセンス：Protection

一般的に、*インシデント*とは、セキュリティ ポリシー違反の可能性があることが疑われる、1 つ以上の侵入イベントと定義されます。Ciscoではまた、インシデントへの対応を追跡するのに FireSIGHT システムで使用される機能を説明するためにこの用語を使用しています。

侵入イベントの操作（41-1 ページ）で説明されているように、一部の侵入イベントは、ネットワーク資産の可用性、機密性、および整合性の点で他のイベントよりも重要になります。たとえば、FireSIGHT システムによって提供されるポート スキャン検出機能は、ネットワークでのポート スキャン アクティビティについて通知することができます。しかし、セキュリティ ポリシーでは、ポート スキャンが明確に禁止されていなかったり、優先度の高い脅威とは見なされていなかったりすることがあります。それで、直接的なアクションの実行はしないで、代わりにすべてのポート スキャンのログを後の調査のために保持しておくことができます。

一方、ネットワーク内のホストが侵害されていることを示す、分散型サービス拒否（DDoS）攻撃に関係したイベントをシステムが生成する場合、そのアクティビティはセキュリティ ポリシーの明確な違反であると考えられます。それで、これらのイベントを調査して追跡できるように、FireSIGHT システムでインシデントを作成する必要があります。

共通のインシデント対応プロセス

ライセンス：Protection

各組織では、セキュリティ インシデントを処理するための独自のプロセスを定義していることがあります。ほとんどのメソッドは、次のフェーズの一部またはすべてを含みます。

- 準備（42-2 ページ）
- 検出と通知（42-3 ページ）
- 調査と認定（42-3 ページ）
- 通信（42-3 ページ）
- 封じ込めとリカバリ（42-4 ページ）
- 学んだ教訓（42-4 ページ）

これらの各フェーズについては、続くセクションで説明します。各フェーズで FireSIGHT システムがどのように役立つかについても説明します。

準備

インシデントの準備には次の 2 通りの方法があります。

- 明確で包括的なセキュリティ ポリシーと、それらを施行するためのハードウェアおよびソフトウェア リソースを配置する
- インシデントに対応するための明確に定義された計画と、その計画を実行できる適切なトレーニングを受けたチームを配置する

インシデント対応において重要なのは、ネットワークのどの部分が最も大きなリスクとなるかを理解することです。これらのネットワーク セグメントに FireSIGHT システム コンポーネントを展開することで、インシデントがいつどのように発生するかについて理解を深めることができます。また、時間をかけて各管理対象デバイスに対する侵入ポリシーを慎重に調整することによって、生成されるイベントの品質を最大限に高めることができます。

検出と通知

インシデントを検出できなければ、インシデントに対応できません。インシデント対応プロセスは、検出できるセキュリティ関連イベントの種類と、それらを検出するために使用するメカニズム（ソフトウェアとハードウェアの両方）を識別する必要があります。また、セキュリティ ポリシーの違反を検出できるケースにも注意する必要があります。積極的あるいは受動的にモニタされないセグメントがネットワークに含まれている場合、それらのセグメントにも注意する必要があります。

ユーザがネットワークに展開する管理対象デバイスは、それらがインストールされているセグメントのトラフィックの分析、侵入の検知、およびそれらを説明するイベントの生成を行う必要があります。各管理対象デバイスに適用するアクセス コントロール ポリシーが、検出するアクティビティの種類、および優先順位に影響を与えることに注意してください。インシデント チームが数百のイベントを取捨選択しなくてもよいように、特定のタイプの侵入イベントに対して通知オプションを設定することもできます。特定の優先順位の高い、重大度の高いイベントが検出されたときに自動的に通知するように指定できます。

調査と認定

インシデント対応プロセスでは、セキュリティ インシデントの検出後に、どのように調査を実施するかを指定する必要があります。ある組織では、チームの新人メンバーが、すべてのインシデントのトリアージを行い、重大度や優先度の低いケースは自分で処理します。重大度や優先度の高いインシデントは、チームの上級メンバーが対応します。各チーム メンバーがインシデントの重要度を繰り上げる基準について理解するように、エスカレーション プロセスの概要を慎重にまとめる必要があります。

エスカレーション プロセスでは、検出されたイベントがネットワーク資産のセキュリティにどのような影響を与えるかについての理解が不可欠です。たとえば、Microsoft SQL Server を実行するホストに対する攻撃は、それとは異なるデータベース サーバを使用する組織にとって優先度は高くありません。同様に、ネットワークで SQL Server を使用しているものの、すべてのサーバにパッチを適用済みで、その攻撃に対する脆弱性がないことを確信している場合には、その攻撃の重要度は低くなります。しかし、最近誰かが脆弱性のあるバージョンのソフトウェア コピーを（テスト目的などで）インストールしていたりすれば、簡易調査で指摘されるよりも大きな問題が発生するおそれがあります。

FireSIGHT システムは、調査および認定のプロセスをサポートするのに特に適しています。独自のイベント分類を作成し、ネットワークの脆弱性を最も適切に示す方法で、それらを適用することができます。ネットワークのトラフィックがイベントを発生させると、自動的にそのイベントの優先順位付けと見極めが行われ、脆弱であることが分かっているホストに対して行われたのがどの攻撃かを示す特別なインジケータが付されます。

FireSIGHT システムのインシデント トラッキング機能には、エスカレーション済みのインシデントを示すための、ユーザが変更できるステータス インジケータも含まれます。

通信

すべてのインシデント対応プロセスでは、インシデント対応チームと内部および外部の対象者の間でのインシデントについての連絡の方法が指定されている必要があります。たとえば、どの種類のインシデントが管理介入を必要とし、どのレベルでの介入が必要かを考慮する必要があります。また、プロセスでは、組織の外部との連絡の方法とタイミングが説明されている必要があります。あるインシデントについて、法執行機関に通知する必要がありますか。ホストがリモート サイトに対する分散サービス拒否（DDoS）に関与している場合、そのことを通知しますか。CERT 調整センター（CERT/CC）や FIRST などの組織と情報を共有する必要があるでしょうか。

FireSIGHT システムには、HTML、PDF、CSV（カンマ区切り値）などの標準形式で侵入データを収集するために使用できる機能があり、侵入データを他のユーザと簡単に共有できます。

たとえば、CERT/CC は Web サイトのセキュリティ インシデントに関する標準情報を収集します。CERT/CC は、以下のような FireSIGHT システムから簡単に抽出できる情報を探しています。

- 影響を受けるマシンに関する情報。これには、以下が含まれます。
- ホスト名および IP
- 時間帯
- ホストの目的や機能
- 攻撃元に関する次のような情報:
- ホスト名および IP
- 時間帯
- 攻撃者と接触したことがあるかどうか
- インシデントを扱う概算コスト
- 次のようなインシデントの説明:
- 日付
- 侵入方法
- 使用された侵入者のツール
- ソフトウェア バージョンとパッチ レベル
- 侵入者のツールの出力
- 悪用された脆弱性の詳細
- 攻撃元
- その他の関連情報

また、インシデントのコメント セクションを使用して、問題を伝えた時と相手を記録することができます。

封じ込めとリカバリ

インシデント対応プロセスでは、ホストまたは他のネットワーク コンポーネントが侵害された場合に、どのような手順を実行するかを明確に示す必要があります。封じ込めとリカバリの方法には、脆弱なホストへのパッチの適用から、ターゲットのシャット ダウンとネットワークからの削除まで、さまざまなオプションがあります。攻撃の性質と重大度によっては、刑事責任を追求する場合に備えて証拠を保存しておくことの重要性を考慮する必要もあります。

FireSIGHT システムのインシデント機能を使用して、インシデントの封じ込めとリカバリのフェーズ中に実行するアクションを記録しておくことができます。

学んだ教訓

それぞれのセキュリティ インシデントは、攻撃が成功したかどうかに関わりなく、セキュリティ ポリシーを見直す機会となります。ファイアウォール ルールを更新する必要はありますか。パッチ管理へのより構造化されたアプローチが必要ですか。不正なワイヤレス アクセス ポイントは新しいセキュリティ問題となりますか。それぞれの学んだ教訓は、セキュリティ ポリシーにフィードバックし、次のインシデントへのより良い対処のために役立てる必要があります。

FireSIGHT システムのインシデント タイプ

ライセンス： Protection

作成する各インシデントにインシデント タイプを割り当てることができます。FireSIGHT システムでは、以下のタイプがデフォルトでサポートされます。

- 侵入
- DoS
- 不正な管理者アクセス
- Web サイトの改変
- システム整合性の侵害
- デマ ウイルス
- 盗難
- ダメージ
- 不明（Unknown）

カスタム インシデント タイプの作成（42-8 ページ）で説明されているように、独自のインシデント タイプを作成することもできます。

インシデントの作成

ライセンス： Protection

このセクションでは、インシデントを作成する方法について説明します。

インシデントの作成方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Analysis] > [Intrusions] > [Incidents] を選択します。

[Incidents] ページが表示されます。

ステップ 2　[Create Incident] をクリックします。

[Create Incident] ページが表示されます。

クリップボードに侵入イベントをコピーした場合は、ページの下部に表示されます。クリップボードの使用についてはクリップボードの使用（41-52 ページ）を参照してください。

ステップ 3　[Type] ドロップダウン メニューから、インシデントを最も適切に説明するオプションを選択します。

ステップ 4　[Time Spent] フィールドに、インシデントで費やした時間の合計を #d #h #m #s の形式で入力します。ここで、# は日数、時間数、分数、秒数を表します。

ステップ 5　[Summary] テキスト ボックスに、インシデントの簡単な説明（最大 255 文字の英数字、スペース、および記号）を入力します。

ステップ 6　[Add Comment] テキスト ボックスに、インシデントのより詳細な説明（最大 8191 文字の英数字、スペース、および記号）を入力します。

ステップ 7　インシデントにイベントを追加しますか。

- **追加する**場合、クリップボードのイベントを選択して、[Add to Incident] をクリックします。

[Add All to Incident] をクリックして、クリップボードからすべてのイベントを追加することもできます。

- **追加しない**場合、[Save] をクリックします。

いずれの場合も、インシデントは入力した情報とともに保存されます。

注　クリップボードの複数のページにある個々のイベントを追加する場合は、1 つのページのイベントを追加してから、他のページのイベントを追加します（ページごとに追加します）。

インシデントの編集

ライセンス： Protection

追加の情報を収集しながらインシデントを更新できます。調査の進展に伴って、インシデントにイベントを追加したり、削除したりすることもできます。

インシデントの編集方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Analysis] > [Intrusions] > [Incidents] を選択します。

[Incidents] ページが表示されます。

ステップ 2　編集するインシデントの横にある [Edit] アイコン（ ）をクリックします。

ステップ 3　インシデントの以下の側面を編集できます。

- ステータスの変更
- タイプの変更
- クリップボードからのイベントの追加
- イベントの削除

ステップ 4　[Time Spent] フィールドに、インシデントに費やした追加の時間の合計を入力します。

ステップ 5　[Add Comment] テキスト ボックスで、インシデントに対する変更点（最大 8191 文字の英数字、スペース、および記号）を示します。

ステップ 6　オプションで、インシデントにイベントを追加したり、削除したりすることができます。

- クリップボードからイベントを追加するには、クリップボードのイベントを選択して、[Add to Incident] をクリックします。
- クリップボードからすべてのイベントを追加するには、[Add All to Incident] をクリックします。
- インシデントから特定のイベントを削除するには、イベントを選択し、[Delete] をクリックします。
- インシデントからすべてのイベントを削除するには、[Delete All] をクリックします。
- イベントを追加または削除せずにインシデントを更新するには、[Save] をクリックします。

インシデントへの変更内容が保存されます。

インシデント レポートの生成

ライセンス： Protection

FireSIGHT システムを使用して、インシデント レポートを生成できます。インシデント レポートには、インシデントの概要、インシデントのステータス、およびコメントに加えて、インシデントに追加するイベントの情報を含めることができます。また、レポートにイベントの概要情報を含めるかどうかも指定できます。

インシデント レポートの生成方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Analysis] > [Intrusions] > [Incidents] を選択します。

[Incidents] ページが表示されます。

ステップ 2　レポートに含めるインシデントの横にある [Edit] アイコン（  ）をクリックします。

ステップ 3　次の 2 つのオプションから選択できます。

- レポートにインシデントのすべてのイベントを含めるには、[Generate Report All] をクリックします。
- レポートにインシデントの特定のイベントを含めるには、含めるイベントの横にあるチェック ボックスを選択してから、[Generate Report] をクリックします。

いずれの場合も、インシデント レポートのオプションを含む [Generate Report] ページが表示されます。

ステップ 4　レポートの名前を入力します。英数字、ピリオド、およびスペースを使用できます。

ステップ 5　[Incident Report Sections] で、レポートに含めるインシデントの部分（**ステータス**、**概要**、および**コメント**）のチェック ボックスを選択します。

ステップ 6　レポートにイベント情報を含める場合は、使用するワークフローを選択し、[Report Sections] で、イベントの概要情報を含めるかどうかを指定します。

ステップ 7　レポートに含めるワークフロー ページの横にあるチェック ボックスを選択します。

ステップ 8　レポートに使用する出力形式（**PDF**、**HTML**、および**CSV**）の横にあるチェック ボックスを選択します。

注　CSV ベースのインシデント レポートには、イベント情報のみが含まれます。また、インシデントのステータス、概要、コメントは含まれ**ません**。

ステップ 9　[Generate Report] をクリックして、レポート プロファイルを更新することを確認します。

レポートが生成されます。

カスタム インシデント タイプの作成

ライセンス： Protection

FireSIGHT システムでは、インシデントを分類するために使用できる以下のインシデント タイプが用意されています。

- システム整合性の侵害
- ダメージ
- DoS
- デマ ウイルス
- 侵入
- 盗難
- 不正な管理者アクセス
- 不明（Unknown）
- Web サイトの改変

これらのインシデント タイプがニーズを満たしていない場合、独自のタイプを追加できます。カスタム インシデント タイプは削除できないことに注意してください。

新しいインシデント タイプの作成方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Analysis] > [Intrusions] > [Incidents] を選択します。

[Incident] ページが表示されます。

ステップ 2　[Create Incident] をクリックします。

[Create Incident] ページが表示されます。

ステップ 3　[Type] 領域で、[Types] をクリックします。

インシデント管理の [Types] ページが表示されます。デフォルトのインシデント タイプがページの下部に表示されます。

ステップ 4　[Incident Type Name] フィールドに、新しいインシデント タイプの名前を入力します。

英数字とスペースを使用します。

ステップ 5　[Add] をクリックします。

新しいインシデント タイプが追加されます。

ステップ 6　[Done] をクリックしてポップアップ ウィンドウを閉じ、[Incidents] ページに戻ります。

次にインシデントを作成または編集するときに、新しいインシデント タイプを使用できます。

外部アラートの設定

FireSIGHT システムではイベントのさまざまなビューを Web インターフェイス内で提供しますが、重要なシステムの継続的なモニタリングを容易にするために外部イベント通知を設定することもできます。次のいずれかが発生したときに、電子メール、SNMP トラップ、または syslog で通知するアラートを生成するように FireSIGHT システムを設定できます。

- 特定の影響フラグを持つ侵入イベント
- 特定のタイプの検出イベント
- ネットワークベースのマルウェア イベントまたはレトロスペクティブ マルウェア イベント
- 特定の相関ポリシー違反によってトリガーとして使用される相関イベント
- 特定のアクセス コントロール ルールによってトリガーとして使用される接続イベント
- 正常性ポリシー内のモジュールに対する特定のステータス変更

システムでこれらのアラートが送信されるようにするには、まず *アラート応答*を作成する必要があります。アラート応答は、アラート送信を計画している外部システムと FireSIGHT システムが連携できるようにする一連の設定です。それらの設定では、たとえば、電子メール リレー ホスト、SNMP アラート パラメータ、または syslog ファシリティおよびプライオリティを指定する場合があります。

アラート応答を作成した後、アラートをトリガーとして使用するために使用するイベントに関連付けます。アラート応答とイベントを関連付けるための処理は、次のように、イベントのタイプによって異なることに注意してください。

- アラート応答を影響フラグ、検出イベント、およびマルウェア イベントと関連付ける場合は、独自の設定ページを使用します。
- 相関イベントを相関ポリシー内でアラート応答（および修復応答）と関連付けます（修復応答については、修復の作成（54-1 ページ）を参照してください）。
- SNMP および syslog アラート応答を接続のログ記録と関連付ける場合は、アクセス コントロール ルールとポリシーを使用します。電子メール アラートは接続のログ記録ではサポートされません。
- アラート応答をヘルス モジュールのステータス変更と関連付ける場合は、ヘルス モニタを使用します。

FireSIGHT システムには、実行可能なもう 1 つのタイプのアラートがあります。この場合は、影響フラグに関係なく個々の侵入イベントに対して、電子メール、SNMP、および syslog による侵入イベント通知を設定します。これらの通知は侵入ポリシーで設定します。侵入ルールの外部アラートの設定（44-1 ページ）およびSNMP アラートの追加（32-36 ページ）を参照してください。次の表では、アラート生成に必要なライセンスについて説明します。

表 43-1　アラートを生成するためのライセンス要件

アラートを生成する条件	必要なライセンス
特定の影響フラグを持つ侵入イベント	FireSIGHT + Protection
特定のタイプの検出イベント	FireSIGHT
ネットワークベースのマルウェア イベント	Malware
相関ポリシー違反	ポリシー違反をトリガーとして使用するために必要なライセンス
接続イベント	接続をログに記録するために必要なライセンス
ヘルス モジュール ステータス変更	いずれか

詳細については、以下を参照してください。

- アラート応答の使用（43-2 ページ）
- 影響フラグ アラートの設定（43-8 ページ）
- 検出イベント アラートの設定（43-9 ページ）
- 高度なマルウェア対策アラートの設定（43-9 ページ）
- ルールとホワイトリストに応答を追加する（51-52 ページ）
- ネットワーク トラフィックの接続のロギング（38-1 ページ）
- ヘルス モニタ アラートの設定（68-42 ページ）

アラート応答の使用

ライセンス： すべて

外部アラートを設定する際の最初の手順はまずアラート応答を作成することです。アラート応答は、アラート送信を計画している外部システムと FireSIGHT システム が連携できるようにする一連の設定です。アラート応答を作成して、電子メール、Simple Network Management Protocol（SNMP）トラップ、またはシステム ログ（syslog）によりアラートを送信できます。

アラートで受け取る情報は、アラートをトリガーしたイベントのタイプによって異なります。たとえば、影響フラグのアラートには、タイムスタンプ、侵入ルール、影響フラグ、およびイベントの説明情報が含まれます。別の例として、検出イベントのアラートも、タイムスタンプと説明情報のほか、検出イベント タイプの情報が含まれます。

相関ポリシーでアラート応答を使用する場合、アラート情報は、相関ポリシー違反をトリガーしたイベントのタイプによって異なります。

注　接続トラッカーを含む相関ルールに対する応答としてアラートを設定した場合、相関ルール自体が異なる種類のイベントに基づいていても、受け取るアラート情報はトラフィック プロファイル変更のアラートの場合と同じです。

作成したアラート応答は自動的に有効になります。有効なアラート応答のみがアラートを生成できます。アラートの生成を停止するには、設定を削除する代わりに、一時的にアラート応答を無効にすることができます。

アラート応答は [Alerts] ページ（[Policies] > [Actions] > [Alerts]）で管理します。各アラート応答の横のスライダは有効かどうかを示します。有効なアラート応答のみがアラートを生成できます。このページは、たとえば、アクセス コントロール ルールの接続をログに記録するための設定でアラート応答が使用されているかどうかも示します。該当する列見出しをクリックして、名前、タイプ、使用中ステータス、および有効または無効のステータスでアラート応答をソートできます。列見出しを再度クリックすると、順序が反転します。

詳細については、以下を参照してください。

- 電子メール アラート応答の作成（43-3 ページ）
- SNMP アラート応答の作成（43-4 ページ）
- Syslog アラート応答の作成（43-5 ページ）
- アラート応答の変更（43-7 ページ）
- アラート応答の削除（43-7 ページ）
- アラート応答の有効化と無効化（43-8 ページ）

電子メール アラート応答の作成

ライセンス： すべて

電子メール アラートはアクセス コントロール ポリシーの接続のログ記録に対して実行**できない**ことに注意してください。

電子メール アラート応答を作成する前に、Defense Center が自身の IP アドレスを逆引き解決できることを確認する必要があります。また、メール リレー ホストおよび通知アドレスの設定（63-19 ページ）で説明しているように、メール リレー ホストを設定する必要があります。

電子メール アラート応答を作成する方法：

アクセス： Admin

ステップ 1　[Policies] > [Actions] > [Alerts] の順に選択します。

[Alerts] ページが表示されます。

ステップ 2　[Create Alert] ドロップダウン メニューから、[Create Email Alert] を選択します。

[Create Email Alert Configuration] ポップアップ ウィンドウが表示されます。

ステップ 3　[Name] フィールドに、アラート応答を識別するために使用する名前を入力します。

ステップ 4　[To] フィールドに、アラートを送信する電子メール アドレスを入力します。

電子メール アドレスが複数ある場合はカンマで区切ります。

ステップ 5　[From] フィールドに、アラートの送信者として表示する電子メール アドレスを入力します。

ステップ 6　[Relay Host] の横に表示されるメール サーバが、アラートの送信に使用するサーバであることを確認します。

サーバを変更する場合、またはリレー ホストをまだ設定していない場合は、編集アイコン（  ）をクリックしてポップアップ ウィンドウに [System Policy] ページを表示し、メール リレー ホストおよび通知アドレスの設定（63-19 ページ）の指示に従います。変更内容を有効にするために、編集後にシステム ポリシーを適用する必要があります。

ステップ 7　[Save] をクリックします。

アラート応答が保存され、自動的に有効になります。

SNMP アラート応答の作成

ライセンス：すべて

SNMPv1、SNMPv2、または SNMPv3 を使用して SNMP アラート応答を作成できます。

注　SNMP で 64 ビット値を監視する場合は、SNMPv2 または SNMPv3 を使用する必要があります。SNMPv1 は 64 ビットのモニタリングをサポートしていません。

ネットワーク管理システムでDefense Centerの管理情報ベース（MIB）ファイルが必要な場合は、`/etc/sf/DC EALERT.MIB` で取得できます。

SNMP アラート応答を作成する方法：

アクセス：Admin

ステップ 1　[Policies] > [Actions] > [Alerts] の順に選択します。

[Alerts] ページが表示されます。

ステップ 2　[Create Alert] ドロップダウン メニューから、[Create SNMP Alert] を選択します。

[Create SNMP Alert Configuration] ポップアップ ウィンドウが表示されます。

ステップ 3　[Name] フィールドに、SNMP 応答を識別するために使用する名前を入力します。

ステップ 4　[Trap Server] フィールドに、英数字を使用して SNMP トラップ サーバのホスト名または IP アドレスを入力します。

このフィールドに無効な IPv4 アドレス（192.169.1.456 など）を入力した場合でも、システムからの警告が**ない**ことに注意してください。無効なアドレスはホスト名として扱われます。

ステップ 5　[Version] ドロップダウンリストから、使用する SNMP バージョンを選択します。

SNMP v3 がデフォルトです。SNMP v1 または SNMP v2 を選択すると、異なるオプションが表示されます。

ステップ 6　どのバージョンの SNMP を選択したかに応じて、以下のようにします。

- SNMP v1 または SNMP v2 の場合、英数字または特殊文字（`*` または `$`）を使用して、[Community String] フィールドに SNMP コミュニティの名前を入力し、ステップ 12 に進みます。
- SNMP v3 の場合、[User Name] フィールドに SNMP サーバで認証するユーザの名前を入力し、次のステップに進みます。

ステップ 7　[Authentication Protocol] ドロップダウンリストから、認証に使用するプロトコルを選択します。

ステップ 8　[Authentication Password] フィールドに、SNMP サーバの認証に必要なパスワードを入力します。

ステップ 9　[Privacy Protocol] リストから、[None] を選択してプライバシー プロトコルを使用しないか、または [DES] を選択してプライバシー プロトコルにデータ暗号規格を使用します。

ステップ 10　[Privacy Password] フィールドに、SNMP サーバに必要なプライバシー パスワードを入力します。

ステップ 11　[Engine ID] フィールドに、SNMP エンジンの識別子を偶数桁の 16 進表記で入力します。

SNMPv3 を使用する場合、メッセージの符号化には Engine ID 値が使用されます。SNMP サーバでは、メッセージを復号化するためにこの値が必要です。

Ciscoは、Defense Centerの IP アドレスの 16 進数バージョンを使用することを推奨します。たとえば、Defense Centerの IP アドレスが `10.1.1.77` である場合、`0a01014D0` を使用します。

ステップ 12　[Save] をクリックします。

アラート応答が保存され、自動的に有効になります。

Syslog アラート応答の作成

ライセンス： すべて

syslog アラート応答を設定する際、syslog サーバで確実に正しく処理されるようにするために、syslog メッセージに関連付けられる重大度とファシリティを指定できます。ファシリティはメッセージを作成するサブシステムを示し、重大度はメッセージの重大度を定義します。ファシリティと重大度は syslog に示される実際のメッセージには表示されませんが、syslog メッセージを受信するシステムに対して、メッセージの分類方法を指示するために使用されます。

ヒント　syslog の機能とその設定方法の詳細については、ご使用のシステムのマニュアルを参照してください。UNIX システムでは、`syslog` および `syslog.conf` の `man` ページで概念情報および設定手順が説明されています。

syslog アラート応答の作成時に任意のタイプのファシリティを選択できますが、syslog サーバに基づいて意味のあるものを選択する必要があります。すべての syslog サーバがすべてのファシリティをサポートしているわけではありません。UNIX syslog サーバの場合、`syslog.conf` ファイルで、どのファシリティがサーバ上のどのログ ファイルに保存されるかを示す必要があります。

次の表に、選択可能な syslog ファシリティを示します。

表 43-2　使用可能な syslog ファシリティ

ファシリティ	説明
ALERT	アラート メッセージ。
AUDIT	監査サブシステムによって生成されるメッセージ。
AUTH	セキュリティと承認に関連するメッセージ。
AUTHPRIV	セキュリティと承認に関連する制限付きアクセス メッセージ。多くのシステムで、これらのメッセージはセキュア ファイルに転送されます。
CLOCK	クロック デーモンによって生成されるメッセージ。 Windows オペレーティング システムを実行している syslog サーバは `CLOCK` ファシリティを使用することに注意してください。
CRON	クロック デーモンによって生成されるメッセージ。 Linux オペレーティング システムを実行している syslog サーバは `CRON` ファシリティを使用することに注意してください。
DAEMON	システム デーモンによって生成されるメッセージ。
FTP	FTP デーモンによって生成されるメッセージ。
KERN	カーネルによって生成されるメッセージ。多くのシステムでは、これらのメッセージが発生する場合コンソールに出力されます。
LOCAL0-LOCAL7	内部プロセスによって生成されるメッセージ。
LPR	印刷サブシステムによって生成されるメッセージ。
MAIL	メール システムで生成されるメッセージ。

表 43-2　使用可能な syslog ファシリティ（続き）

ファシリティ	説明
NEWS	ネットワーク ニュース サブシステムによって生成されるメッセージ。
NTP	NTP デーモンによって生成されるメッセージ。
SYSLOG	syslog デーモンによって生成されるメッセージ。
USER	ユーザ レベルのプロセスによって生成されるメッセージ。
UUCP	UUCP サブシステムによって生成されるメッセージ。

次の表に、選択可能な標準の syslog 重大度レベルを示します。

表 43-3　syslog 重大度レベル

レベル	説明
ALERT	ただちに修正する必要がある状態。
CRIT	クリティカルな状態。
DEBUG	デバッグ情報を含むメッセージ。
EMERG	すべてのユーザに配信されるパニック状態。
ERR	エラー状態。
INFO	情報メッセージ。
NOTICE	エラー状態ではないが、注意が必要な状態。
WARNING	警告メッセージ。

syslog アラートの送信を開始する前に、syslog サーバがリモート メッセージを受信できることを確認してください。

syslog アラートを作成する方法：

アクセス： Admin

ステップ 1　[Policies] > [Actions] > [Alerts] の順に選択します。

[Alerts] ページが表示されます。[Create Alert] ドロップダウン メニューから、[Create Syslog Alert] を選択します。

[Create Syslog Alert Configuration] ポップアップ ウィンドウが表示されます。

ステップ 2　[Name] フィールドに、保存される応答を識別するために使用する名前を入力します。

ステップ 3　[Host] フィールドに、syslogサーバのホスト名またはIPアドレスを入力します。

このフィールドに無効な IPv4 アドレス（192.168.1.456 など）を入力した場合でも、システムからの警告が**ない**ことに注意してください。無効なアドレスはホスト名として扱われます。

ステップ 4　[Port] フィールドに、サーバが syslog メッセージに使用するポートを入力します。

この値はデフォルトで 514 です。

ステップ 5　[Facility] リストから、ファシリティを選択します。

使用可能なファシリティの一覧については、使用可能な syslog ファシリティの表を参照してください。

ステップ 6　[Severity] リストから、重大度を選択します。

使用可能な重大度の一覧については、syslog 重大度レベルの表を参照してください。

ステップ 7　[Tag] フィールドに、syslog メッセージとともに表示するタグ名を入力します。

タグ名には英数字のみを使用します。スペースまたは下線は使用**できません**。

例として、syslog に送信されるすべてのメッセージの前に `FromDC` を付ける場合、フィールドに `FromDC` と入力します。

ステップ 8　[Save] をクリックします。

アラート応答が保存され、自動的に有効になります。

アラート応答の変更

ライセンス： すべて

ほとんどのタイプのアラートについて、アラート応答が有効で使用中の場合、アラート応答への変更はすぐに反映されます。ただし、接続イベントをログに記録するアクセス コントロール ルールで使用されるアラート応答の場合、アクセス コントロール ポリシーを再適用するまで変更は有効になりません。

アラート応答を編集する方法：

アクセス： Admin

ステップ 1　[Policies] > [Actions] > [Alerts] の順に選択します。

[Alerts] ページが表示されます。

ステップ 2　編集するアラート応答の横にある編集アイコン（  ）をクリックします。

そのアラート応答の設定ポップアップ ウィンドウが表示されます。

ステップ 3　必要に応じて変更を加えます。

ステップ 4　[Save] をクリックします。

アラート応答が保存されます。

アラート応答の削除

ライセンス： すべて

使用中でない任意のアラート応答を削除できます。

アラート応答を削除する方法：

アクセス： Admin

ステップ 1　[Policies] > [Actions] > [Alerts] の順に選択します。

[Alerts] ページが表示されます。

ステップ 2　削除するアラート応答の横にある削除アイコン（  ）をクリックします。

ステップ 3　アラート応答を削除することを確認します。

アラート応答が削除されます。

アラート応答の有効化と無効化

ライセンス： すべて

有効なアラート応答のみがアラートを生成できます。アラートの生成を停止するには、設定を削除する代わりに、一時的にアラート応答を無効にすることができます。無効化するときにアラートが使用中の場合は、無効にしても使用中とみなされることに注意してください。

アラート応答を有効または無効にする方法：

アクセス： Admin

ステップ 1　[Policies] > [Actions] > [Alerts] の順に選択します。

[Alerts] ページが表示されます。

ステップ 2　有効または無効にするアラート応答の横の有効または無効のスライダをクリックします。

アラート応答が有効だった場合は、無効になります。無効だった場合は、有効になります。

影響フラグ アラートの設定

ライセンス： Protection

特定の影響フラグを持つ侵入イベントが発生するたびにアラートが生成されるようにシステムを設定できます。影響フラグは、侵入データ、ネットワーク検出データ、および脆弱性情報を関連付けることにより、侵入がネットワークに与える影響を評価するのに役立ちます。詳細については、影響レベルを使用してイベントを評価する (41-39 ページ) を参照してください。

影響フラグ アラートを設定する方法：

アクセス： Admin

ステップ 1　[Policies] > [Actions] > [Alerts] を選択した後、[Impact Flag Alerts] タブを選択します。

[Impact Flag Alerts] ページが表示されます。

ステップ 2　[Alerts] セクションで、各アラート タイプで使用するアラート応答を選択します。

新しいアラート応答を作成するには、任意のドロップダウンリストから [New] を選択します。詳細については、アラート応答の使用 (43-2 ページ) を参照してください。

ステップ 3　[Impact Configuration] セクションで、各影響フラグに対して、受信するアラートに対応するチェック ボックスを選択します。

ステップ 4　[Save] をクリックします。

影響フラグ アラート設定が保存されます。

検出イベント アラートの設定

ライセンス： FireSIGHT

特定のタイプの検出イベントが発生するたびにアラートが生成されるようにシステムを設定できます。さまざまなイベント タイプについては、ディスカバリ イベントのタイプについて（50-10 ページ）およびホスト入力イベントのタイプについて（50-14 ページ）を参照してください。

検出イベント タイプに基づいてアラートを生成するには、そのイベント タイプをログに記録するようにネットワーク検出ポリシーを設定する必要があることに注意してください（検出イベント ロギングの設定（45-40 ページ）を参照してください）。デフォルトでは、すべてのイベント タイプに対してロギングは有効です。

検出イベント アラートを設定する方法：

アクセス： Admin

ステップ 1　[Policies] > [Actions] > [Alerts] を選択した後、[Discovery Event Alerts] タブを選択します。

[Discovery Event Alerts] ページが表示されます。

ステップ 2　[Alerts] セクションで、各アラート タイプで使用するアラート応答を選択します。

新しいアラート応答を作成するには、任意のドロップダウンリストから [New] を選択します。詳細については、アラート応答の使用（43-2 ページ）を参照してください。

ステップ 3　[Events Configuration] セクションで、各検出イベント タイプに対して、受信するアラートに対応するチェック ボックスを選択します。

ステップ 4　[Save] をクリックします。

検出イベント アラート設定が保存されます。

高度なマルウェア対策アラートの設定

ライセンス： Malware

サポートされるデバイス： シリーズ 3 または仮想

サポートされる防御センター： DC500 を除くいずれか

ネットワークベースのマルウェア イベント（レトロスペクティブ イベントを含む）が発生するたびにアラートが生成されるようにシステムを設定できます。ただし、エンドポイント ベースの（FireAMP）マルウェア イベントではアラートを生成できません。マルウェア イベントの詳細については、マルウェア イベントの操作（40-17 ページ）を参照してください。

マルウェア イベントに基づいてアラートを生成するには、マルウェア クラウド検索を実行するファイル ポリシーを作成した後、そのポリシーをアクセス コントロール ルールに関連付ける必要があります。詳細については、侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（18-1 ページ）を参照してください。

マルウェア イベント アラートを設定する方法:

アクセス: Admin

ステップ 1　[Policies] > [Actions] > [Alerts] を選択した後、[Advanced Malware Protections Alerts] タブを選択します。

[Advanced Malware Protection Alerts] ページが表示されます。

ステップ 2　[Alerts] セクションで、各アラート タイプで使用するアラート応答を選択します。

新しいアラート応答を作成するには、任意のドロップダウンリストから [New] を選択します。詳細については、アラート応答の使用（43-2 ページ）を参照してください。

ステップ 3　[Event Configuration] セクションで、各マルウェア イベント タイプに対して、受信するアラートに対応するチェック ボックスを選択します。

[All network-based malware events] には [Retrospective Events] が含まれることに注意してください。

ステップ 4　[Save] をクリックします。

マルウェア イベント アラート設定が保存されます。

侵入ルールの外部アラートの設定

FireSIGHT システムは、Web インターフェイスで侵入イベントのさまざまなビューを提供しますが、企業によっては、重要なシステムの継続的なモニタリングを容易にするために、外部侵入のイベント通知を定義したいという要望があります。特定のユーザに重大イベントについてすぐに通知したい場合は、電子メール アラートを設定できます。さらに、syslog ファシリティへのロギングを有効にしたり、SNMP トラップ サーバにイベント データを送信したりできます。

各侵入ポリシー内では、侵入イベントの通知制限を指定し、外部ロギング ファシリティへの侵入イベント通知をセットアップし、侵入イベントへの外部応答を設定できます。

ヒント アナリストによっては、同じ侵入イベントに対して複数のアラートを受信することは望まないものの、特定の侵入イベントの発生については、頻度を制限したうえで通知を受信したいと考えています。詳細については、「ポリシー単位の侵入イベント通知のフィルタ処理（32-25 ページ）」を参照してください。

侵入ポリシー以外にも、FireSIGHT システムで実行可能な別のタイプのアラートがあります。特定の影響フラグが設定された侵入イベントや特定のアクセス コントロール規則によって記録された接続イベントなど、他のタイプのイベントに対して電子メール、SNMP、syslog アラートによる応答を設定できます。詳細については、外部アラートの設定（43-1 ページ）を参照してください。

外部侵入イベント通知の詳細情報については、次の項を参照してください。

- SNMP 応答の使用（44-1 ページ）では、指定された SNMP トラップ サーバにイベント データを送信する場合に設定可能なオプションや、SNMP アラート オプションを指定する手順について説明します。
- Syslog 応答の使用（44-4 ページ）では、外部 syslog にイベント データを送信する場合に設定可能なオプションや、syslog アラート オプションを指定する手順について説明します。
- 電子メール アラートについて（44-7 ページ）では、電子メールで侵入イベントの通知を送信する場合に設定可能なオプションについて説明します。

SNMP 応答の使用

ライセンス：Protection

*SNMP トラップ*は、ネットワーク管理に関する通知です。侵入イベントに関する通知を SNMP トラップ（*SNMP アラート*とも呼ばれる）として送信するようにデバイスを設定できます。各 SNMP アラートには次のものが含まれます。

- トラップを生成するサーバの名前

- アラートを検出したデバイスの IP アドレス
- アラートを検出したデバイスの名前
- イベント データ

さまざまな SNMP アラート パラメータを設定できます。使用可能なパラメータは、使用する SNMP のバージョンによって異なります。SNMP アラートを有効化および無効化する方法の詳細については、侵入ポリシーの詳細設定の設定（31-7 ページ）を参照してください。

ヒント　ネットワーク管理システムで Management Information Base（MIB）ファイルが必要な場合は、Defense Center の `/etc/sf/DCEALERT.MIB` から取得できます。

SNMP v2 オプション

SNMP v2 の場合、次の表で説明されているオプションを指定できます。

表 44-1　SNMP v2 オプション

オプション	説明
トラップ タイプ	アラートに表示される IP アドレスに使用するトラップ タイプ。 ネットワーク管理システムによって INET_IPV4 アドレス タイプが正常にレンダリングされた場合は、[as Binary] を選択できます。そうでない場合は、[as String] を選択します。たとえば、HP Openview では文字列タイプが必要になります。
Trap Server	SNMP トラップ通知を受信するサーバ。 単一の IP アドレスまたはホスト名を指定できます。
Community String	コミュニティ名。

SNMP v3 オプション

SNMP v3 の場合、次の表で説明されているオプションを指定できます。

注　SNMP v3 を使用する場合、アプライアンスは Engine ID 値を使用してメッセージをエンコードします。SNMP サーバでは、メッセージを復号化するためにこの値が必要です。現在、この Engine ID 値は常に、文字列の末尾に `01` が付く、アプライアンスの IP アドレスの 16 進数バージョンになります。たとえば、SNMP アラートを送信するアプライアンスの IP アドレスが `172.16.1.50` である場合、Engine ID は `0xAC10013201` になります。また、アプライアンスの IP アドレスが `10.1.1.77` である場合、Engine ID `0x0a01014D01` が使用されます。

表 44-2　SNMP v3 オプション

オプション	説明
トラップ タイプ	アラートに表示される IP アドレスに使用するトラップ タイプ。 ネットワーク管理システムによって INET_IPV4 アドレス タイプが正常にレンダリングされた場合は、[as Binary] を選択できます。そうでない場合は、[as String] を選択します。たとえば、HP Openview では文字列タイプが必要になります。
Trap Server	SNMP トラップ通知を受信するサーバ。 単一の IP アドレスまたはホスト名を指定できます。

表 44-2　SNMP v3 オプション（続き）

オプション	説明
Authentication Password	認証に必要なパスワード。SNMP v3 は、設定に応じて Message Digest 5（MD5）ハッシュ関数または Secure Hash Algorithm（SHA）ハッシュ関数のいずれかを使用し、このパスワードを暗号化します。 認証パスワードを指定すると、認証が有効になります。
Private Password	プライバシー用の SNMP キー。SNMP v3 は Data Encryption Standard（DES）ブロック暗号を使用して、このパスワードを暗号化します。 プライベート パスワードを指定すると、プライバシーが有効になります。プライベート パスワードを指定する場合は、認証パスワードも指定する必要があります。
ユーザ名	SNMP ユーザ名。

SNMP アラートの設定の詳細については、SNMP 応答の設定（44-3 ページ）を参照してください。

SNMP 応答の設定

ライセンス：Protection

侵入ポリシーで SNMP アラートを設定できます。アクセス コントロール ポリシーの一部としてポリシーを適用すると、システムは SNMP トラップで検出した侵入イベントをすべて通知するようになります。SNMP アラートの詳細については、SNMP 応答の使用（44-1 ページ）を参照してください。

SNMP アラート オプションを設定するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Advanced Settings] をクリックします。

[Advanced Settings] ページが表示されます。

ステップ 4　外部応答の [SNMP Alerting] が有効かどうかに応じて、次の 2 つの選択肢があります。

- 設定が有効な場合、[Edit] をクリックします。
- 設定が無効である場合、[Enabled] をクリックし、[Edit] をクリックします。

[SNMP Alerting] ページが表示されます。

ページ下部のメッセージは、設定を含む侵入ポリシー層を示します。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　IP アドレスに使用するトラップ タイプの形式を [as Binary] または [as String] のいずれかに指定します。

注　ネットワーク管理システムによって INET_IPV4 アドレス タイプが正常にレンダリングされた場合は、[as Binary] オプションを使用できます。正常にレンダリングされなかった場合は、[as String] オプションを使用します。たとえば、HP OpenView では [as String] オプションが必要になります。

ステップ 6　SNMP v2 または SNMP v3 を選択します。

- SNMP v2 を設定するには、使用するトラップ サーバの IP アドレスとコミュニティ名を対応するフィールドに入力します。SNMP v2 オプション（44-2 ページ）を参照してください。
- SNMP v3 を設定するには、使用するトラップ サーバの IP アドレス、認証パスワード、プライベート パスワード、およびユーザ名を対応するフィールドに入力します。詳細については、「SNMP v3 オプション（44-2 ページ）」を参照してください。

注　SNMP v2 **または** SNMP v3 を選択する必要があります。

注　SNMP v3 パスワードを入力すると、パスワードは初期設定時にはプレーン テキストで表示されますが、暗号化形式で保存されます。

ステップ 7　ポリシーを保存するか、編集を続けるか、変更を破棄するか、基本ポリシーのデフォルト構成設定に戻すか、あるいはシステム キャッシュに変更を残して終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

Syslog 応答の使用

ライセンス： Protection

システム ログ、つまり *syslog* は、ネットワーク イベント ロギングの標準ロギング メカニズムです。侵入イベントの通知である *syslog* アラートをアプライアンスの syslog に送信できます。syslog では、syslog 内の情報を優先順位別およびファシリティ別に分類することができます。*優先順位*はアラートの重大度を反映し、*ファシリティ*はアラートを生成したサブシステムを示します。ファシリティおよび優先順位は syslog の実際のメッセージに表示されませんが、その代わりに、syslog メッセージを受信するシステムにそれを分類する方法を指示するために使用されます。

syslog アラートには次の情報が含まれます。

- アラート生成の日時
- イベント メッセージ
- イベント データ
- トリガー イベントのジェネレータ ID
- トリガー イベントの Snort ID
- リビジョン

侵入ポリシーでは、syslog アラートを有効にして、syslog の侵入イベントの通知に関連付けられている syslog の優先順位およびファシリティを指定できます。アクセス コントロール ポリシーの一部として侵入ポリシーを適用した場合、システムは、検出した侵入イベントの syslog アラートをローカル ホストまたはポリシーで指定されたロギング ホストの syslog ファシリティに送信します。アラートを受信したホストは、syslog アラートの設定時に設定されたファシリティおよび優先順位に関する情報を使用して、アラートを分類します。

次の表には、syslog アラートを設定する場合に選択できるファシリティを示します。使用するリモート syslog サーバの設定に基づいて、効果のあるファシリティの設定を行ってください。リモート システムにある `syslog.conf` ファイル（UNIX または Linux ベースのシステムに syslog メッセージをロギングしている場合）は、サーバのどのログ ファイルにどのファシリティが保存されるかを示します。

表 44-3　使用可能な syslog ファシリティ

ファシリティ	説明
AUTH	セキュリティと承認に関連するメッセージ。
AUTHPRIV	セキュリティと承認に関連する制限付きアクセス メッセージ。多くのシステムで、これらのメッセージはセキュア ファイルに転送されます。
CRON	クロック デーモンによって生成されるメッセージ。
DAEMON	システム デーモンによって生成されるメッセージ。
FTP	FTP デーモンによって生成されるメッセージ。
KERN	カーネルによって生成されるメッセージ。多くのシステムでは、これらのメッセージが発生する場合コンソールに出力されます。
LOCAL0-LOCAL7	内部プロセスによって生成されるメッセージ。
LPR	印刷サブシステムによって生成されるメッセージ。
MAIL	メール システムで生成されるメッセージ。
NEWS	ネットワーク ニュース サブシステムによって生成されるメッセージ。
SYSLOG	syslog デーモンによって生成されるメッセージ。
USER	ユーザ レベルのプロセスによって生成されるメッセージ。
UUCP	UUCP サブシステムによって生成されるメッセージ。

このアラートで生成されるすべての通知を表示するには、次の標準的な syslog の優先順位レベルのいずれかを選択します。

表 44-4　syslog の優先順位レベル

レベル	説明
EMERG	すべてのユーザにブロードキャストするパニック状態
ALERT	すぐに修正する必要がある状態
CRIT	重大な状態
ERR	エラー状態
WARNING	警告メッセージ
NOTICE	エラー状態ではないが、注意が必要な状態
INFO	通知メッセージ
DEBUG	デバッグ情報を含むメッセージ

syslog の動作とその設定方法の詳細については、システムに付属の資料を参照してください。UNIX または Linux ベースのシステムの syslog にログインしている場合、`syslog.conf` man ファイル（コマンドラインで `man syslog.conf` と入力）および syslog man ファイル（コマンドラインで `man syslog` と入力）に、syslog の動作とその設定方法に関する情報が示されます。

syslog 応答の設定

ライセンス：Protection

侵入ポリシーで syslog アラートを設定できます。アクセス コントロール ポリシーの一部としてポリシーを適用すると、システムは syslog で検出した侵入イベントをすべて通知するようになります。syslog アラートの詳細については、Syslog 応答の使用（44-4 ページ）を参照してください。

syslog アラート オプションを設定するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Advanced Settings] をクリックします。

[Advanced Settings] ページが表示されます。

ステップ 4　外部応答の [Syslog Alerting] が有効かどうかに応じて、次の 2 つの選択肢があります。

- 設定が有効な場合、[Edit] をクリックします。
- 設定が無効である場合、[Enabled] をクリックし、[Edit] をクリックします。

[Syslog Alerting] ページが表示されます。

ページ下部のメッセージは、設定を含む侵入ポリシー層を示します。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）」を参照してください。

ステップ 5　オプションで、[Logging Hosts] フィールドに、ロギング ホストとして指定するリモート アクセス IP アドレスを入力します。複数のホストを指定する場合は、カンマで区切ります。

ステップ 6　ドロップダウンリストからファシリティおよび優先順位のレベルを選択します。

ファシリティおよび優先順位オプションの詳細については、Syslog 応答の使用（44-4 ページ）を参照してください。

ステップ 7　ポリシーを保存するか、編集を続けるか、変更を破棄するか、基本ポリシーのデフォルト構成設定に戻すか、あるいはシステム キャッシュに変更を残して終了します。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

電子メール アラートについて

ライセンス：Protection

*電子*メール アラートは、電子メールによる侵入イベントの通知です。電子メール アラートには次の情報が含まれます。

- データベース内のアラートの合計数
- 最後の電子メールの時刻（システムが最後の電子メール レポートを生成した時刻）
- 現在の時刻（システムが現在の電子メール レポートを生成した時刻）
- 新しいアラートの合計数
- 指定した電子メール フィルタに一致したイベントの数（特定のルールに対してイベントが設定されている場合）
- 各イベントのタイムスタンプ、プロトコル、イベント メッセージ、およびセッション情報（トラフィック方向が指定された送信元および宛先の IP およびポート）（[Summary Output] がオフの場合）

注　複数の侵入イベントが同じ送信元 IP から発生した場合、追加イベントの数を示すメモがイベントの下に表示されます。

- 宛先ポートあたりのイベント数
- 送信元 IP あたりのイベント数

ルールまたはルール グループごとに、侵入イベントの電子メール アラートを有効化または無効化できます。アクセス コントロール ポリシーの一部としてデバイスに適用する侵入ポリシーにかかわらず、電子メール アラート設定が使用されます。

次のリストには、電子メール アラートに設定できるパラメータを示します。

On/Off

電子メールによる通知を有効または無効にします。

From Address

システムによる侵入イベントの送信元となる電子メール アドレスを指定します。

To Address

システムによる侵入イベントの送信先となる電子メール アドレスを指定します。電子メールを複数の受信者に送信するには、電子メール アドレスをコンマで区切ります。次に例を示します。

```
user1@example.com, user2@example.com
```

Max Alerts

システムが電子メールで送信する侵入イベントの最大数を、[Frequency（seconds）] で指定された時間枠で指定します。

Frequency（seconds）

システムが侵入イベントをメール送信する頻度を指定します。この設定では、電子メール設定が保存される頻度も指定します。

最小頻度：300 秒
最大頻度：40 億秒

Coalesce Alerts

送信元 IP およびイベントによる侵入イベントのグループ化を有効または無効にし、同じ送信元 IP に対して生成された複数の同一侵入イベントが 1 つだけのイベントとしてページに表示されるようにします。

アラートの結合（グループ化）はイベントのフィルタリング後に行われることに注意してください。したがって、特定のルールで電子メール アラートを設定した場合、Mail Alerting Configuration で指定した規則に一致するイベントのリストのみを受信します。

Summary Output

短い電子メール アラートを有効または無効にします。これは、ポケットベルなどのテキスト制限があるデバイスに適しています。短い電子メール アラートには、以下の情報が含まれています。

- イベントのタイムスタンプ
- イベントを生成したデバイスの IP アドレス（Defense Centerの場合）
- イベントのプロトコル
- 送信元 IP およびポート
- 宛先 IP およびポート
- イベント メッセージ
- 同じ送信元 IP に対して生成された侵入イベントの数

次に例を示します。

```
2011-05-18 10:35:10 10.1.1.100 icmp 10.10.10.1:8 -> 10.2.1.3:0
snort_decoder: Unknown Datagram decoding problem!(116:108)
```

Email Alerting on Specific Rules Configuration

指定した電子メール アドレスにイベントを送信するルールまたはルール グループを指定します。

電子メール アラートの設定の詳細については、電子メール アラートの設定（44-8 ページ）を参照してください。

電子メール アラートの設定

ライセンス： Protection

電子メール アラートを設定して、侵入イベントが特定のルールまたはルール グループに対して発生するたびにアプライアンスが通知するように設定できます。

電子メール アラートを受信できるようにするには、以下のことを**行う必要があります。**

- 電子メール アラートを受信するようにメール ホストを設定する（メール リレー ホストおよび通知アドレスの設定（63-19 ページ）を参照）
- 管理対象デバイスと Defense Centerの両方が独自の IP アドレスを互いに解決できることを確認する

電子メール アラート オプションを設定するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Email] を選択します。

[Email Alerting] ページが表示されます。

ステップ 2　[State] の横にある [on] を選択して電子メール アラートを有効にします。

ステップ 3　[From Address] フィールドに、電子メール アラートの [From] フィールドに表示するアドレスを入力します。

ステップ 4　[To Address] フィールドに、電子メール アラートを受信するアドレスを入力します。

ステップ 5　[Max Alerts] フィールドに、単一の電子メールに含めるイベントの最大数を入力します。

ステップ 6　[Min Frequency] フィールドに、電子メール アラートを受信する最小間隔の秒数を入力します。

ステップ 7　IP アドレス別にイベントをグループ化するには、[Coalesce Alerts] の横にある [on] を選択します。

ステップ 8　短い電子メール アラートを送信するには、[Summary Output] の横にある [on] を選択します。

ヒント　[Summary Output] を有効にする場合は、[Coalesce Alerts] を有効にして、生成されるアラートの数を減らすことを検討してください。また、デバイスのテキスト メッセージ バッファがオーバーフローしないように [Max Alerts] を 1 に設定することも検討してください。

ステップ 9　[Time Zone] フィールドで、ドロップダウン リストからタイム ゾーンを選択します。

ステップ 10　ルールごとに電子メール アラートを有効にするには、[Email Alerting per Rule Configuration] をクリックします。

ルール グループが表示されます。

ヒント　すべてのカテゴリのすべてのルールについて電子メール アラートを受信するには、[Select All] を選択します。

ステップ 11　次のいずれかまたは両方を実行します。

- カテゴリに属するすべてのルールで、電子メール アラートを受信するルール カテゴリの横にある [All] をクリックします。
- そのカテゴリの個々のルールで電子メール アラートを指定するカテゴリ フォルダをクリックし、電子メール アラートを受信するルールを有効にします。

ステップ 12　[Save] をクリックします。

システムは電子メール アラート設定を保存します。該当する侵入イベントが発生すると、電子メール アラートが送信されます。

ネットワーク検出の概要

FireSIGHT システムは、*ネットワーク検出*と呼ばれる機能を使用して、ネットワーク上のトラフィックを監視し、ネットワーク アセットの包括的な地図を作成します。

管理対象デバイスは指定されたネットワーク セグメント上のトラフィックを受動的に監視するため、システムはネットワーク トラフィックからの特定のパケット 見出し値とその他の一意のデータ(*フィンガープリント*と呼ばれる)を設定された定義と比較し、ネットワーク上のホストの台数と種類(ネットワーク デバイスを含む)だけでなく、それらのホスト上のオペレーティング システム、アクティブ アプリケーション、およびオープン ポートも判断します。

また、ネットワーク上のユーザ活動を監視するようにFireSIGHT システムの管理対象デバイスを設定することもできます。これにより、ポリシー違反、攻撃、またはネットワークの脆弱性の発生源を特定できます。

システムによって収集されたデータを補完するために、NetFlow 対応デバイス、Nmap アクティブ スキャン、ホスト入力機能、および Microsoft Active Directory サーバ上に存在し LDAP 認証を報告するユーザ エージェントによって生成されたレコードをインポートできます。FireSIGHT システムは、管理対象デバイスによる直接ネットワーク トラフィック監視を介して、これらのレコードと自ら収集した情報を統合します。

システムは、ネットワーク上のホストで発生した特定タイプの侵入、マルウェア、およびその他のイベントを関連付け、ホストが侵害された可能性がある時点を特定して、そのようなホストに*侵害の兆候*(IOC)タグを付けます。IOC データを使用すれば、監視対象ネットワークのホストに関連する脅威の現状を明確かつ直接的に把握できます。

システムは、この情報のすべてを使用して、科学捜査的分析、行動プロファイリング、アクセス コントロール、および組織が被りやすい脆弱性や悪用に対する対策と対応を支援します。

詳細については、以下を参照してください。

- 検出データ収集について(45-1 ページ)
- NetFlow について(45-18 ページ)
- 侵害の兆候について(45-22 ページ)
- ネットワーク検出ポリシーの作成(45-25 ページ)

検出データ収集について

ライセンス: FireSIGHT

検出データには、ネットワークのホスト、それらのホスト上のオペレーティング システム、アクティブ アプリケーション、およびユーザ活動に関する情報が含まれます。

検出データの収集を開始するには、まず、アクセス コントロール ポリシーを適用する必要があります。アクセス コントロール ポリシーは、許可するトラフィック、つまり、ネットワーク検出で監視可能なトラフィックを定義します。これは、アクセス コントロールを使用して特定のトラフィックをブロックすると、システムでホスト、ユーザ、またはアプリケーションの活動に関するトラフィックを検査できなくなることを意味することに注意してください。たとえば、ソーシャル ネットワーキング アプリケーションへのアクセスをブロックすると、システムからソーシャル ネットワーキング アプリケーションに関する検出データが提供されなくなります。

アクセス コントロール ポリシーの適用後は、管理対象デバイスで監視するネットワーク セグメントとポートと、収集するデータの種類を指定するようにネットワーク検出ポリシーを設定して適用する必要があります。ネットワーク検出ポリシーを適用すると、Defense Center Web インターフェイスを使用して表示または分析が可能な検出データの生成が開始されます。

ネットワーク検出データは Defense Center データベースに保存されます。保存制限の詳細については、データベース イベント制限の設定（63-16 ページ）を参照してください。データベース制限に加えて、Defense Centerで保存可能な検出対象のホストとユーザの総数は FireSIGHT ライセンスによって異なります。

ライセンス ユーザ制限に達すると、ほとんどの場合、データベースへの新しいユーザの追加が停止されます。新しいユーザを追加するには、古いユーザまたは非アクティブなユーザをデータベースから手動で削除するか、データベースからすべてのユーザを消去する必要があります。一方、ライセンス ホスト制限に達した場合は、データベースへの新しいホストの追加を停止するか、最も長い時間非アクティブのままだったホストを交換するようにシステムを設定できます。

システムによって収集されたデータを補完するために、NetFlow 対応デバイス、Nmap アクティブ スキャン、ホスト入力機能、および Microsoft Active Directory サーバ上に存在し LDAP 認証を報告するユーザ エージェントによって生成されたレコードをインポートできます。FireSIGHT システムは、管理対象デバイスによる直接ネットワーク トラフィック監視を介して、これらのレコードと自ら収集した情報を統合します。

詳細については、以下を参照してください。

- ホスト データ収集について（45-2 ページ）
- ユーザ データ収集について（45-3 ページ）
- アプリケーション検出について（45-11 ページ）
- 侵害の兆候について（45-22 ページ）
- サードパーティ検出データのインポート（45-17 ページ）
- 検出データの用途（45-17 ページ）

ホスト データ収集について

ライセンス： FireSIGHT

システムはネットワークを通過するトラフィックを受動的に監視するため、ネットワーク トラフィックからの特定のパケット ヘッダー値とその他の一意のデータを設定された定義と比較して（*フィンガープリント*と呼ばれる）、ネットワーク上のホストに関する次の情報を判断します。

- ホストの台数と種類（ブリッジ、ルータ、ロード バランサ、NAT デバイスなどのネットワーク デバイスを含む）
- ネットワーク上の検出ポイントからホストまでのホップ数を含む、基本的なネットワーク トポロジ データ
- ホスト上で動作しているオペレーティング システム
- これらのアプリケーションに関連付けられているホストとユーザのアプリケーション

システムでホストのオペレーティング システムを特定できない場合は、カスタム フィンガープリント機能を使用して、カスタム クライアント フィンガープリントまたはカスタム サーバ フィンガープリントを作成できます。システムはこれらのフィンガープリントを使用して新しいホストを特定します。フィンガープリントを脆弱性データベース（VDB）内のシステムにマップすることにより、カスタム フィンガープリントを使用してホストが特定されるたびに適切な脆弱性情報を表示できます。詳細については、カスタム フィンガープリントの使用（46-7 ページ）を参照してください。

また、ホスト入力機能を介してホスト データとオペレーティング システム データを追加または更新することもできます。加えて、ホスト検出が有効な NetFlow 対応検出ルールを作成すれば、NetFlow データからネットワーク マップにホストを追加できます。

システムで検出されたホストを Defense Center Web インターフェイスを使用して表示できます。

- イベント ビューアを使用したホストの表示および検索方法については、ホストの使用（50-21 ページ）を参照してください。
- ネットワーク アセットとトポロジが詳しく記載されたネットワーク マップの表示方法については、ネットワーク マップの使用（48-1 ページ）を参照してください。
- 検出されたホストで利用可能なすべての情報の完全なビューであるホスト プロファイルの表示方法については、ホスト プロファイルの使用（49-1 ページ）を参照してください。

ユーザ データ収集について

ライセンス： FireSIGHT

FireSIGHT システムを使用してネットワーク上のユーザ活動を監視できます。これにより、脅威、エンドポイント、およびネットワーク インテリジェンスをユーザ ID 情報に関連付けることができます。ネットワーク動作、トラフィック、およびイベントを個別のユーザに直接リンクすることによって、ポリシー違反、攻撃、またはネットワークの脆弱性の発生源の特定に役立てることができます。つまり、システムが「現象」の背後に存在する「人物」を教えてくれます。たとえば、以下について決定できます。

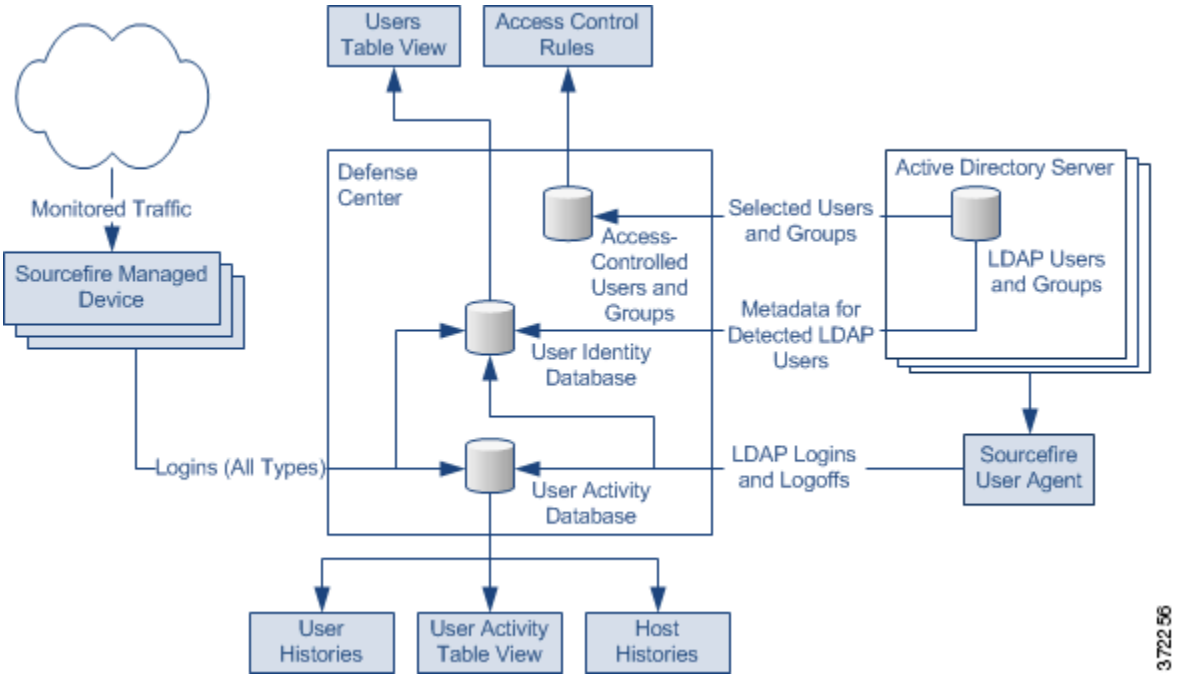
- 脆弱（レベル 1：赤）影響レベルの侵入イベントの対象になっているホストの所有者
- 内部攻撃またはポート スキャンを開始した人物
- ホスト重要度の高いサーバの不正アクセスを試みている人物
- 不合理な容量の帯域幅を使用している人物
- 重要なオペレーティング システム更新を適用しなかった人物
- 会社の IT ポリシーに違反してインスタント メッセージング ソフトウェアまたはピアツーピア ファイル共有アプリケーションを使用している人物

この情報を入手すれば、リスクを軽減したり、ユーザまたはユーザ活動をブロックしたり、その他の人を混乱させない措置を講じたりするための的を絞ったアプローチを使用できます。これらの機能により、監査制御が大幅に改善され、規制の順守が促進されます。

システムが LDAP 接続内のユーザ認識設定に基づいて Microsoft Active Directory LDAP サーバからアクセス コントロール ポリシー内で使用されているユーザをダウンロードします。その後で、ユーザ エージェントがこれらのユーザに関するログイン データを提供し、ユーザがユーザ データベースに追加されます。これらのユーザは*アクセス制御対象ユーザ*と呼ばれます。ユーザ条件を含むアクセス コントロール ポリシーを作成するときに、アクセス制御対象ユーザに対する条件を書き込みます。詳細については、アクセス コントロール ルールへのユーザ条件の追加（17-3 ページ）を参照してください。

システムがユーザ ログイン、ユーザ エージェント、トラフィックで検出されたアプリケーション データ、あるいは POP3、SMTP、または IMAP 経由の電子メール ログインからユーザ データを検出すると、ユーザのリストに照らしてログインからのユーザがチェックされます。ログイン ユーザがエージェントから報告された既存のユーザと一致した場合は、ログインからのデータがそのユーザに割り当てられます。ログインが SMTP トラフィック内に存在しない場合は、既存のユーザと一致しないログインによって新しいユーザが作成されます。SMTP トラフィック内の一致しないログインは破棄されます。

次の図は、FireSIGHT システムがユーザ データをどのように収集して保存するかを示しています。



図に示すように、ユーザ データの 3 つの発生源と、そのデータが保存される 3 つの場所があります。ユーザ データ収集の詳細については、以下を参照してください。

- 管理対象デバイス (45-5 ページ)
- ユーザ エージェント (45-5 ページ)
- Defense Center と LDAP サーバ間の接続 (45-7 ページ)
- ユーザ データベース (45-8 ページ)
- ユーザ活動データベース (45-8 ページ)
- アクセス制御対象ユーザ データベース (45-9 ページ)
- ユーザ データ収集の制限 (45-9 ページ)

管理対象デバイス

ライセンス：FireSIGHT

ネットワーク検出ポリシーを使用して、指定されたネットワーク上で LDAP、AIM、POP3、IMAP、Oracle、SIP（VoIP）、FTP、HTTP、MDNS および SMTP ログインを受動的に検出するように管理対象デバイスを設定します。ネットワーク検出ルールでユーザの検出を有効にすると、ホスト検出が自動的に有効になることに注意してください。

注　管理対象デバイスは、LDAP 接続に対する Kerberos ログインのみを LDAP 認証として解釈します。また、管理対象デバイスは、SSL や TLS などのプロトコルを使用して暗号化された LDAP 認証を検出できません。

デバイスがログインを検出すると、次の情報をユーザ活動として記録するためにDefense Centerに送信します。

- ログインで識別されたユーザ名
- ログインの時刻
- ログインに関係する IP アドレス。このアドレスは、ユーザのホスト（LDAP、POP3、IMAP、および AIM ログインの場合）、サーバ（HTTP、MDNS、FTP、SMTP および Oracle ログインの場合）、またはセッション発信元（SIP ログインの場合）の IP アドレスになります。
- ユーザの電子メール アドレス（POP3、IMAP、および SMTP ログインの場合）
- ログインを検出したデバイスの名前

ユーザがすでに検出されている場合、Defense Centerはそのユーザのログイン履歴を更新します。Defense Centerは POP3 および IMAP ログイン内の電子メール アドレスを使用して LDAP ユーザに関連付けることができることに注意してください。これは、Defense Centerが新しい IMAP ログインを検出して、その IMAP ログイン内の電子メール アドレスが既存の LDAP ユーザのアドレスと一致した場合は、IMAP ログインで新しいユーザが作成されるのではなく、LDAP ユーザの履歴が更新されることを意味します。

そのユーザがこれまで検出されたことがなければ、Defense Centerがそのユーザをデータベースに追加します。AIM、SIP、および Oracle ログインでは一意のにそれぞれ、新しいユーザ レコードが作成されます。これは、それらのログイン イベントにはDefense Centerが他のログイン タイプに関連付けることができるデータが含まれていないためです。

Defense Centerは、次の場合に、ユーザ活動またはユーザ ID を記録**しません**。

- ユーザ ロギングの制限（45-33 ページ）の説明に従って、そのログイン タイプを無視するようにネットワーク検出ポリシーを設定した場合
- 管理対象デバイスが SMTP ログインを検出したものの、ユーザ データベースに電子メール アドレスが一致する、検出済みの LDAP、POP3、または IMAP ユーザが含まれていない場合

ユーザ エージェント

ライセンス：FireSIGHT

組織で Microsoft Active Directory LDAP サーバを使用している場合は、Ciscoでは、Active Directory サーバ経由でユーザ活動を監視するためにユーザ エージェントをインストールすることを推奨しています。ユーザ制御を実行する場合は、ユーザ エージェントをインストールして使用する**必要があります**。エージェントがユーザと IP アドレスを関連付けるため、ユーザ条件を含むアクセス コントロール ルールでトリガーできます。1 つのエージェントを使用して最大 5 つの Active Directory サーバ上のユーザ活動を監視できます。

エージェントを使用するには、エージェントに接続された各Defense Centerと監視対象 LDAP サーバ間の接続を設定する必要があります。この接続は、ログインとログオフがユーザ エージェントによって検出されたユーザのメタデータを取得可能にするだけでなく、アクセス コントロール ルール内で使用するユーザとグループを指定するためにも使用されます。ユーザ検出用の LDAP サーバの設定方法については、アクセス制御されたユーザおよび LDAP ユーザのメタデータの取得（17-5 ページ）を参照してください。

各エージェントは、定期的にスケジュールされたポーリングまたはリアルタイム モニタリングを通して、暗号化されたトラフィックを使用したログインを監視できます。ログインは、ユーザがワークステーションで、または、リモート デスクトップ ログイン経由でコンピュータにログインしたときに Active Directory サーバによって生成されます。

エージェントは、ユーザ ログオフを監視して報告することもできます。ログオフは、ホスト IP アドレスからログアウトしたユーザをエージェントが検出したときに、エージェント自体によって生成されます。また、ログオフは、ホストにログインしたユーザが変わったことをエージェントが検出したときにも生成され、その後で Active Directory サーバがユーザが変わったことを報告します。ログオフ データとログイン データを組み合わせれば、ネットワークにログインしたユーザのより完全なビューが形成されます。

Active Directory サーバのポーリングによって、エージェントは定義されたポーリング時間間隔でユーザ アクティビティ データをまとめて取得できます。リアルタイム モニタリングは、Active Directory サーバがデータを受信するとすぐに、ユーザ アクティビティ データをエージェントに送信します。

特定のユーザ名または IP アドレスに関連付けられたログインまたはログオフの報告を除外するようにエージェントを設定できます。これは、ファイル共有やプリント サーバなどの共有サーバに対する反復ログインを除外したり、トラブルシューティングのためにマシンにログインしているユーザを除外したりする場合に役立ちます。

エージェントは除外するユーザ名または IP アドレスが含まれていない検出されたすべてのログインとログオフのレコードを Defense Centerに送信し、レコードはそこでユーザ活動として記録および報告されます。エージェントは、Defense Centerのバージョンを検出し、ログイン レコードを適切なデータ形式で送信します。これにより、管理対象デバイスで直接検出されたユーザ活動が補完されます。ユーザ エージェントから報告されたログインによって、ユーザと IP アドレスが関連付けられるため、ユーザ条件を含むアクセス コントロール ルールをトリガーできます。

ユーザ エージェントは、ネットワークにログインしたとき、または、他の理由でアカウントが Active Directory 資格情報に照らして認証されたときにユーザを監視します。ユーザ エージェントのバージョン 2.1 は、ホストに対する対話型ユーザ ログイン、リモート デスクトップ ログイン、ファイル共有認証、およびコンピュータ アカウント ログインだけでなく、ユーザ ログオフとユーザがログオフしたリモート デスクトップ セッションも検出します。

検出されたログインのタイプによって、エージェントがログインをどのように報告するかと、ログインがホスト プロファイルでどのように表示されるかが決まります。ホストに対する*権限のあるユーザ ログイン*によって、ホスト IP アドレスにマップされた現在のユーザが新しいログインからのユーザに変更されます。他のログインでは、現在のユーザが変更されないか、ホスト上の既存のユーザにホストに対する権限のあるユーザ ログインが付与されていない場合にホストの現在のユーザだけが変更されるかのどちらかです。このようなケースでは、想定していたユーザがすでにログインしていなければ、エージェントがそのユーザのログオフを生成します。ネットワーク検出によって検出されたユーザ ログインでは、ホスト上の既存のユーザにホストに対する権限のあるユーザ ログインが付与されていない場合にホストの現在のユーザだけが変更されます。エージェント検出ログインはネットワーク マップに次のような影響を与えます。

- エージェントがユーザまたはリモート デスクトップ ログインによるホストに対する対話型ログインを検出した場合は、ホストに対する権限のあるユーザ ログインを報告して、ホストの現在のユーザを新しいユーザに変更します。

- ファイル共有認証のログインを検出した場合、エージェントはホストに対するユーザ ログインを報告しますが、ホストの現在のユーザは変更しません。
- エージェントがホストに対するコンピュータ アカウント ログインを検出した場合は、NetBIOS Name Change 検出イベントを生成し、ホスト プロファイルに NetBIOS 名の変更が反映されます。
- エージェントが除外されたユーザ名からのログインを検出した場合は、Defense Centerにログインを報告しません。

ログインまたはその他の認証が実行されると、エージェントは次の情報をDefense Centerに送信します。

- ユーザの LDAP ユーザ名
- ログインまたはその他の認証の時刻
- ユーザのホストの IP アドレスと、エージェントがコンピュータ アカウント ログインの IPv6 アドレスを報告した場合のリンクローカル アドレス

Defense Centerは、ログイン情報とログオフ情報をユーザ活動として記録します。ユーザ エージェントがユーザ ログインまたはログオフからのユーザ データを報告すると、報告されたユーザがユーザのリストに照らしてチェックされます。報告されたユーザがエージェントから報告された既存のユーザと一致した場合は、報告されたデータがそのユーザに割り当てられます。報告されたユーザが既存のユーザと一致しなかった場合は、新しいユーザが作成されます。

除外されたユーザ名に関連付けられたユーザ活動は報告されませんが、関連するユーザ活動が報告される場合があります。エージェントがマシンに対するユーザ ログインを検出してから、2 人目のユーザ ログインを検出し、その 2 人目のユーザ ログインに関連付けられたユーザ名が報告から除外されていた場合は、1 人目のユーザのログオフを報告します。ただし、2 人目のユーザのログインは報告されません。その結果、除外されたユーザがホストにログインしていた場合でも、ユーザが IP アドレスにマップされません。

エージェントによって検出されるユーザ名の次の制限に注意してください。

- Defense Center に報告されるドル記号($)で終わるユーザ名は、ネットワーク マップを更新しますが、ユーザ ログインとして表示されません。
- Unicode 文字を含むユーザ名のDefense Centerの表示は制限されることがあります。

Defense Centerで保存できる検出済みユーザの総数は、FireSIGHT ライセンスによって異なります。ライセンス ユーザ制限に達すると、ほとんどの場合、データベースへの新しいユーザの追加が停止されます。新しいユーザを追加するには、古いユーザまたは非アクティブなユーザをデータベースから手動で削除するか、データベースからすべてのユーザを消去する必要があります。

Defense Center と LDAP サーバ間の接続

ライセンス: FireSIGHT

Defense Center と LDAP サーバ間の接続を使用すれば、検出された特定のユーザのメタデータを取得できます。LDAP ユーザのメタデータとして、ログインが管理対象デバイスによって検出されたのか、ユーザ エージェントによって検出されたのかを取得できます。また、POP3 ユーザと IMAP ユーザのメタデータとして、それらのユーザーが LDAP ユーザと同じ電子メール アドレスを持っているかどうかを取得できます。

組織で Microsoft Active Directory サーバを使用している場合は、接続を通して、アクセス コントロール ルールで使用する LDAP ユーザとグループを指定できます。ユーザ制御を実行する場合は、Defense Centerと Active Directory サーバの接続を設定する**必要があります**。組織で Active Directory を使用していない場合でも、管理対象デバイスを使用してユーザ ログインを検出し、Oracle または OpenLDAP サーバから一部のユーザのメタデータを取得できます。ただし、これらのユーザまたはその活動に基づいてユーザ制御を実行することはできません。

Defense Centerは LDAP サーバから、それぞれのユーザに関する次の情報とメタデータを取得します。

- LDAP ユーザ名
- 姓と名
- 電子メール アドレス
- 部門
- 電話番号

ユーザ データベース

ライセンス：FireSIGHT

ユーザ データベースには、管理対象デバイスまたはユーザ エージェントで検出された各ユーザのレコードが格納されます。Defense Centerで保存できる検出済みユーザの総数は、FireSIGHT ライセンスによって異なります。ライセンスされた制限に達すると、ほとんどの場合、このシステムはデータベースへの新しいユーザの追加を停止します。新しいユーザを追加するには、古いユーザまたは非アクティブなユーザをデータベースから手動で削除するか、データベースからすべてのユーザを消去する必要があります。

ただし、システムは権限のあるユーザ ログインを特別扱いします。制限に達してから、システムが未検出だったユーザの権限のあるユーザ ログインを検出した場合は、最も長い時間非アクティブのままだった権限のないユーザを削除して新しいユーザに置き換えます。

Defense Center Web インターフェイスを使用してユーザ データベースの内容を表示できます。検出されたユーザの表示、検索、および削除の方法については、ユーザの使用（50-64 ページ）を参照してください。

ユーザ活動データベース

ライセンス：FireSIGHT

ユーザ アクティビティ データベースには、ネットワーク上のユーザ アクティビティのレコードが格納されます。これらのアクティビティは、ユーザ エージェントが監視している Active Directory LDAP サーバとの接続から取得されるか、またはネットワーク ディスカバリによって取得されます。システムは次の状況でイベントを記録します。

- 個別のログインまたはログオフを検出したとき
- 新しいユーザを検出したとき
- 手動でユーザが削除されたとき
- データベース内に存在しないユーザをシステムが検出したものの、FireSIGHT のライセンス制限に達したためにそのユーザを追加できなかったとき

システムで検出されたユーザ活動をDefense Center Web インターフェイスを使用して表示できます。ユーザ活動の表示、検索、および削除の方法については、ユーザ アクティビティ の使用（50-70 ページ）を参照してください。ユーザ エージェントのバージョン 2.1 を使用して LDAP ログイン データを Defense Center に送信する場合は、エージェントを接続する各 Defense Center 上でそれぞれのエージェント用の接続を設定する必要があります。エージェントはこの接続を使用して、ログイン データを送信可能なDefense Centerとのセキュアな接続を確立することができます。エージェントが特定のユーザ名を除外するように設定されている場合は、そのようなユーザ名のログイン データはDefense Centerに報告されません。

加えて、ユーザ アクセス コントロールを実装する場合は、データを収集する各 Microsoft Active Directory サーバへの接続を、ユーザ認識パラメータを設定してセットアップする必要があります。

可能な場合はいつでも、FireSIGHT システムがユーザ活動とその他のタイプのイベントを関連付けます。たとえば、侵入イベントは、イベント発生時に送信元ホストおよび宛先ホストにログインしていたユーザを通知することができます。

システムは、ユーザ活動を使用して、各ユーザがログインしていたホストを追跡する*ホスト履歴*と個別のホストにログインしていたユーザを追跡する*ユーザ履歴*も生成します。また、過去 24 時間の各ユーザの活動と過去 24 時間の各ホストへのログインがグラフで表示されます。詳細については、ユーザの詳細とホストの履歴について（50-68 ページ）およびホスト プロファイルでのユーザ履歴の使用（49-24 ページ）を参照してください。

アクセス制御対象ユーザ データベース

ライセンス： Control

アクセス制御対象ユーザ データベースには、FireSIGHT システム でユーザ制御を実行するためのアクセス コントロール ルールで使用できるユーザとグループが格納されます。これらのユーザは次の 2 つのタイプに分けられます。

- *アクセス制御対象ユーザ*は、アクセス コントロール ルールに追加してユーザ制御を実行可能なユーザです。Defense Center と LDAP サーバ間の接続を設定するときに、アクセス制御対象ユーザを追加する必要があるグループを指定します。
- *非アクセス制御対象ユーザ*は、検出されたその他のユーザです。

アクセス制御されたユーザおよび LDAP ユーザのメタデータの取得（17-5 ページ） の説明に従って、Defense Center と LDAP サーバ間の接続を設定するときに、アクセス制御対象ユーザを追加する必要があるグループを指定します。

ユーザ エージェントのバージョン 2.1 を使用して LDAP ログインおよびログオフ データをバージョン 5.x Defense Center に送信する場合は、エージェントを接続する各 Defense Center 上でそれぞれのエージェント用の接続を設定する必要があります。エージェントはこの接続を使用して、ユーザ アクティビティ データを送信可能なDefense Centerとのセキュアな接続を確立することができます。

エージェントが特定のユーザ名を除外するように設定されている場合は、そのようなユーザ名のユーザ アクティビティ データはDefense Centerに報告されません。これらの除外されたユーザ名はデータベースに残りますが、IP アドレスに関連付けられません。

加えて、ユーザ アクセス コントロールを実装する場合は、データを収集する各 Microsoft Active Directory サーバへの接続を、ユーザ認識パラメータを設定してセットアップする必要があります。

アクセス コントロールで使用可能なユーザの最大数は FireSIGHT ライセンスによって異なります。Defense Center と LDAP サーバ間の接続を設定するときに、含まれているユーザの総数が FireSIGHT ユーザ ライセンスの数より少ないことを確認してください。詳細については、「FireSIGHTホストおよびユーザ ライセンスの制限について（65-9 ページ）」を参照してください。

ユーザ データ収集の制限

ライセンス： FireSIGHT

次の表に、ユーザ データ収集の制限事項を示します。

表 45-1　ユーザ認識の制限

制限事項	説明
ユーザ制御	ユーザ制御を実行するには、組織で Microsoft Active Directory LDAP サーバを使用している**必要があります**。システムは、Active Directory からアクセス コントロール ルールで使用可能なユーザとグループを取得し、Active Directory サーバにインストールされたユーザ エージェントから報告されたログインとログオフを使用してユーザを IP アドレスに関連付けます。
Kerberos 以外による LDAP 接続のログイン	管理対象デバイスは、LDAP 接続に対する Kerberos ログインのみを LDAP 認証として解釈します。管理対象デバイスは、SSL や TLS などの他のプロトコルが使用されている場合に、暗号化された LDAP 認証を検出できません。 一方、ユーザ エージェントは Active Directory サーバ上のセキュリティ ログを使用してユーザ ログイン データを収集するため、このような制限がありません。
ログイン検出	Active Directory サーバへのログインを検出する場合は、サーバ IP アドレスを使用して Active Directory サーバ接続を設定します。詳細については、『*User Agent Configuration Guide*』を参照してください。 複数のユーザがリモート セッションを使用してホストにログインしている場合は、エージェントがそのホストからのログインを正確に検出しない場合があります。これを回避する方法については、『*User Agent Configuration Guide*』を参照してください。
ログオフ検出	ログオフはすぐに検出されない場合があります。ログオフに関連付けられたタイムスタンプは、ユーザがホスト IP アドレスにマップされなくなったことをエージェントが検出した時点を反映しているため、ユーザがホストからログオフした実際の時間と対応しない可能性があります。 ログオフは、ホスト IP アドレスからログアウトしたユーザをエージェントが検出したときに、エージェント自体によって生成されます。また、ログオフは、ホストにログインしたユーザが変わったことをエージェントが検出したときにも生成され、その後で Active Directory サーバがユーザが変わったことを報告します。
リアルタイム データ検索	Active Directory サーバは、Windows Server 2008 または Windows Server 2012 を実行している必要があります。
複数のユーザによる同じホストへの複数のログイン	システムは、特定のホストにログインするユーザは一度に 1 人だけであり、ホストの現在のユーザが最後の権限のあるユーザ ログインであると見なします。権限のないログインだけがホストにログインしている場合は、最後にログインしたものが現在のユーザと見なされます。複数のユーザがリモート セッション経由でログインしている場合は、Active Directory サーバによって報告された最後のユーザがDefense Centerに報告されるユーザです。
同じユーザによる同じホストへの複数のログイン	システムは、ユーザが初めて特定のホストにログインした時点を記録し、それ以降のログインを無視します。あるユーザが特定のホストにログインしている唯一の人物の場合は、システムが記録する唯一のログインがオリジナルのログインです。 ただし、そのホストに別のユーザがログインした時点で、システムは新しいログインを記録します。その後で、オリジナルのユーザが再度ログインすると、その人物の新しいログインが記録されます。
Unicode 文字	ユーザ インターフェイスは Unicode 文字を含むユーザ名を正しく表示しない場合があります。

表 45-1　ユーザ認識の制限（続き）

制限事項	説明
ユーザ データベース内の LDAP ユーザ アカウント	LDAP サーバで LDAP ユーザを削除または無効化するか、あるいは Defense Center に報告する対象からユーザ名を除外した場合、Defense Center はユーザ データベースからそのユーザを削除せず、そのユーザは引き続きデータベースに登録されるユーザのライセンス制限に照らしてカウントされます。データベースからユーザを手動で消去する必要があります。 ユーザ ライセンス制限がアクセス制御対象ユーザにも同時に適用されることに注意してください。アクセス制御対象ユーザのユーザ カウントは LDAP 設定で取得されたユーザ数によって異なります。
AOL Instant Messenger（AIM）ログイン検出	管理対象デバイスは OSCAR プロトコルを使用した AIM ログインだけを検出できます。ほとんどの AIM クライアントが OSCAR を使用するのに対して、一部のクライアントは TOC2 を使用します。

アプリケーション検出について

ライセンス：FireSIGHT

FireSIGHT システムは IP トラフィックを分析するときに、ネットワーク上でよく使用されているアプリケーションを特定しようとします。アプリケーション認識は、アプリケーション ベースのアクセス コントロールを行うために不可欠です。

システムで検出されるアプリケーションには次の 3 種類があります。

- HTTP や SSH などのホスト間の通信を表す*アプリケーション プロトコル*
- Web ブラウザや電子メール クライアントなどのホスト上で動作しているソフトウェアを表す*クライアント*
- HTTP トラフィックの内容または要求された URL を表す MPEG ビデオや Facebook などの *Web アプリケーション*

システムは、パケット 見出し内の ASCII または 16 進パターン、あるいは、トラフィックで使用されたポートを使用して、ネットワーク トラフィック内のアプリケーションを特定します。特定のアプリケーションのトラフィックを識別する精度を上げるために、ポート検出とパターン検出の両方を使用するアプリケーション ディテクタもあります。加えて、Secure Socket Layer（SSL）プロトコル ディテクタは、セキュアなセッションからの情報を使用して、セッションからアプリケーションを識別します。FireSIGHT システム内のアプリケーション ディテクタの供給元には次の 2 つがあります。

- *Cisco 提供ディテクタ*。Web アプリケーション、クライアント、およびアプリケーション プロトコルを検出します

  アプリケーション（およびオペレーティング システム、ホスト データ収集について（45-2 ページ）を参照）に対する Cisco 提供ディテクタの可用性は、インストールされている FireSIGHT システム のバージョンと VDB のバージョンによって異なります。リリース ノートとアドバイザリに、新しいディテクタと更新されたディテクタに関する情報が記載されています。また、プロフェッショナル サービスが作成した個別のディテクタをインポートすることもできます。検出されるアプリケーションの完全なリストについては、サポート サイトを参照してください。

- *ユーザ定義アプリケーション プロトコル ディテクタ*。システムのアプリケーション プロトコル検出機能を強化するために作成できます

また、*暗黙的アプリケーション プロトコル検出*を通してアプリケーション プロトコルを検出することもできます。これは、クライアントの検出に基づいてアプリケーション プロトコルの存在を暗示するものです。

システムは、次の表に示す基準を使用して、検出したアプリケーションのそれぞれを特徴付けます。また、これらの特徴を利用して、アプリケーション フィルタまたはアプリケーション グループを作成します。これらのフィルタと独自に作成したフィルタを使用して、アクセス コントロールを実行したり、検索、レポート、およびダッシュボード ウィジェットを制限したりできます。詳細については、アプリケーション フィルタの操作（3-16 ページ）を参照してください。

:

表 45-2　　アプリケーションの特徴

特性	説明	例
タイプ	アプリケーションのタイプ： • **アプリケーション プロトコル**は、ホスト間の通信手段を意味します。 • **クライアント**は、ホスト上で動作しているソフトウェアを意味します。 • **Web アプリケーション**は、HTTP トラフィックの内容または要求された URL を意味します。	HTTP と SSH はアプリケーション プロトコルです。 Web ブラウザと電子メール クライアントはクライアントです。 MPEG ビデオと Facebook は Web アプリケーションです。
リスク	このアプリケーションが、組織のセキュリティ ポリシーに違反するかもしれない目的で使用される可能性がどの程度であるか。アプリケーションのリスクは、**Very Low** から **Very High** までの範囲です。	ピアツーピア アプリケーションはリスクが極めて高いと見なされます。
ビジネスとの関連性	アプリケーションが、娯楽としてではなく、組織のビジネス活動の範囲内で使用される可能性。アプリケーションのビジネスとの関連性は、**Very Low** から **Very High** までの範囲です。	ゲーム アプリケーションはビジネス関連性が非常に低いと見なされます。
カテゴリ	アプリケーションの最も不可欠な機能を表す一般的な分類。各アプリケーションは、少なくとも 1 つのカテゴリに属します。	Facebook は**ソーシャル ネットワーキング**のカテゴリに入ります。
タグ	アプリケーションに関する追加情報。アプリケーションには任意の数（0 を含む）のタグを付けることができます。	ビデオ ストリーミング Web アプリケーションには、大抵、**high bandwidth** と **displays ads** というタグが付けられます。

システムによって収集されたアプリケーション データを補完するために、NetFlow 対応デバイス、Nmap アクティブ スキャン、およびホスト入力機能によって生成されたレコードを使用できます。

詳細については、以下を参照してください。

- アプリケーション プロトコル検出プロセスについて（45-13 ページ）
- クライアント検出からの暗黙的アプリケーション プロトコル検出（45-14 ページ）
- アプリケーション プロトコル検出に関する特記事項：Squid（45-15 ページ）
- 特記事項：SSL アプリケーション検出（45-15 ページ）
- 特記事項：照会先 Web アプリケーション（45-16 ページ）

- アプリケーション ディテクタの使用（46-18 ページ）
- サードパーティ検出データのインポート（45-17 ページ）
- NetFlow について（45-18 ページ）

アプリケーション プロトコル検出プロセスについて

ライセンス：FireSIGHT

システムがアプリケーション トラフィックを検出すると、まず、その特定のポートを唯一の検出基準として使用するディテクタによって特定されたポート上でアプリケーション プロトコルが動作しているかどうかを判断します。アプリケーション プロトコルがそのようなポートの 1 つで動作している場合、システムは既知のポート ディテクタを使用してアプリケーション プロトコルを肯定的に識別します。

注　Cisco 提供ディテクタによって使用されるポート上でユーザ定義のポート ベース アプリケーション プロトコル ディテクタを作成してアクティブにすることができるため、Cisco の検知機能がオーバーライドされる可能性があります。たとえば、ユーザ定義のディテクタがポート 22 上のすべてのアプリケーション プロトコル トラフィックを `myapplication` アプリケーション プロトコルとして識別する場合は、ポート 22 上の SSH トラフィックが `myapplication` トラフィックとして誤って識別されます。

アプリケーション プロトコルがそのようなポートの 1 つで動作していない場合は、システムがポート照合とパターン照合に基づいて識別するより確実な方法を採用します。2 つのディテクタが両方ともトラフィックを肯定的に識別する場合は、より長いパターン照合を採用しているディテクタが優先されます。同様に、複数のパターン照合を使用したディテクタは単一のパターン照合より優先されます。

ネットワーク検出ポリシーで定義されているように、システムは監視対象ネットワーク内のホスト上で動作しているアプリケーション プロトコルだけを識別することに注意してください。たとえば、監視されていないリモート サイト上の FTP サーバに内部ホストがアクセスする場合、システムはアプリケーション プロトコルを FTP として識別しません。一方、監視されているホスト上の FTP サーバにリモートまたは内部ホストがアクセスする場合、システムはアプリケーション プロトコルを肯定的に識別できます。

例外は、監視対象ホストがアクセスしている非監視対象サーバとの間の接続に使用しているクライアントをシステムが識別できる場合です。この場合、システムは、接続内のクライアントに対応する適切なアプリケーション プロトコルを肯定的に識別しますが、そのアプリケーション プロトコルをネットワーク マップに追加しません。詳細については、クライアント検出からの暗黙的アプリケーション プロトコル検出（45-14 ページ）を参照してください。アプリケーション検出が発生するためには、クライアント セッションにサーバからの応答が含まれている必要があることに注意してください。

次の表に、FireSIGHT システムがDefense Center Web インターフェイスで検出されたアプリケーション プロトコルを識別する方法（ネットワーク マップ、ホスト プロファイル、イベント ビューなど）の概要を示します。

表 45-3　FireSIGHT システム のアプリケーション プロトコルの識別

アプリケーション	説明
アプリケーション プロトコル名	Defense Centerは、次のアプリケーション プロトコルの場合に、名前でアプリケーション プロトコルを識別します。 • システムによって肯定的に識別された • NetFlow データを使用して識別され、/etc/sf/services にポートとアプリケーション プロトコルの関連付けが存在する • ホスト入力機能を使用して手動で識別された • Nmap または別のアクティブな発生源によって識別された
pending	Defense Centerは、システムが肯定的と否定的のどちらでもアプリケーションを識別できない場合に、アプリケーション プロトコルを pending として識別します。 大抵の場合、システムはより多くの接続データ(アプリケーションが識別される)を収集して分析しないと、pending アプリケーションを識別できません。 [Application Details and Servers] テーブルやホスト プロファイルで pending ステータスが表示されるのは、特定のアプリケーション プロトコル トラフィック(クライアントまたは Web アプリケーション トラフィック以外の)が検出されたアプリケーション プロトコルだけです。
unknown	Defense Centerは、アプリケーションが以下の場合にアプリケーション プロトコルを unknown として識別します。 • システムのディテクタのどれとも一致しない • アプリケーション プロトコルが NetFlow データを使用して識別されたものの、/etc/sf/services にポートとアプリケーション プロトコルの関連付けが存在しない
blank	使用可能なすべての検出データが検証されましたが、アプリケーション プロトコルが識別されませんでした。[Application Details and Servers] テーブルとホスト プロファイルでは、アプリケーション プロトコルが検出されなかった非 HTTP 汎用クライアント トラフィックに対して、アプリケーション プロトコルが空白として表示されます。

クライアント検出からの暗黙的アプリケーション プロトコル検出

ライセンス: FireSIGHT

監視対象ホストがアクセスしている非監視対象サーバとの間の接続に使用しているクライアントをシステムが識別できる場合、Defense Center はその接続でクライアントに対応するアプリケーション プロトコルが使用されていると推測します。(システムは監視対象ネットワーク上のアプリケーションだけを追跡するため、通常、接続ログには監視対象ホストが非監視対象サーバにアクセスしている接続に関するアプリケーション プロトコル情報が含まれていません。)

クライアントの検出からのアプリケーション プロトコルの暗黙的検出の結果は複数存在します。

- システムはこれらのサーバの New TCP Port イベントまたは New UDP Port イベントを生成しないため、サーバが [Servers] テーブルに表示されません。加えて、これらのアプリケーション プロトコルの検出を基準にして、検出イベント アラートまたは相関ルールをトリガーすることはできません。
- アプリケーション プロトコルはホストに関連付けられないため、ホスト プロファイルの詳細を表示したり、サーバ ID を設定したり、トラフィック プロファイルまたは相関ルールに関するホスト プロファイル資格内の情報を使用したりできません。加えて、システムはこの種の検出に基づいて脆弱性とホストを関連付けません。

ただし、接続内のアプリケーション プロトコル情報に対する相関イベントをトリガーできます。また、接続ログ内のアプリケーション プロトコル情報を使用して、接続トラッカーとトラフィック プロファイルを作成できます。

ホスト制限と検出イベント ロギング

ライセンス： FireSIGHT

システムがクライアント、サーバ、または Web アプリケーションを検出すると、関連するホストがすでにクライアント、サーバ、または Web アプリケーションの最大数に達していなければ、検出イベントが生成されます。

ホスト プロファイルには、ホストごとに最大 16 のクライアント、100 のサーバ、および 100 の Web アプリケーションが表示されます。詳細については、ホスト プロファイルでのサーバの使用 (49-16 ページ)およびホスト プロファイルでのアプリケーションの表示 (49-22 ページ)を参照してください。

クライアント、サーバ、または Web アプリケーションの検出によって異なるアクションはこの制限の影響を受けないことに注意してください。たとえば、サーバ上でトリガーするように設定されたアクセス コントロール ルールでは、引き続き、接続イベントが記録されます。

アプリケーション プロトコル検出に関する特記事項：Squid

ライセンス： FireSIGHT

システムは、次のいずれかの場合に Squid サーバ トラフィックを肯定的に識別します。

- 監視対象ネットワーク上のホストからプロキシ認証が有効になっている Squid サーバへの接続をシステムが検出した場合
- 監視対象ネットワーク上の Squid プロキシ サーバからターゲット システム（つまり、クライアントが情報または別のリソースを要求する宛先サーバ）への接続をシステムが検出した場合

ただし、システムは次の場合に Squid サービス トラフィックを識別できません。

- 監視対象ネットワーク上のホストが、プロキシ認証が無効になっている Squid サーバに接続している場合
- Squid プロキシ サーバが HTTP 応答から Via: 見出し フィールドを除去するように設定されている場合

特記事項：SSL アプリケーション検出

ライセンス： FireSIGHT

FireSIGHT システム は、Secure Socket Layer（SSL）セッションからのセッション情報を使用してセッション内のアプリケーション プロトコル、クライアント アプリケーション、または Web アプリケーションを識別するディテクタを備えています。

システムは暗号化された接続を検出すると、その接続を汎用 HTTPS 接続として、または、該当する場合に、SMTPS などのより特殊なセキュア プロトコルとしてマークします。システムは SSL セッションを検出すると、そのセッションに対する接続イベント内の **Client** フィールドに `SSL client` を追加します。システムはセッションで Web アプリケーションを識別すると、そのトラフィックに対する検出イベントを生成します。

SSL アプリケーション トラフィックの場合は、管理対象デバイスも、サーバ証明書から一般名を検出して SSL ホスト パターンからのクライアントまたは Web アプリケーションと照合できます。システムが特定のクライアントを識別すると、SSL client をそのクライアントの名前に置き換えます。

SSL アプリケーション トラフィックは暗号化されるため、システムは暗号化されたストリーム内のアプリケーション データではなく、証明書内の情報しか識別に使用できません。そのため、SSL ホスト パターンではアプリケーションを制作した会社しか識別できない場合があり、同じ会社が作成した SSL アプリケーションは識別情報が同じ可能性があります。

HTTPS セッションが HTTP セッション内から起動される場合などは、管理対象デバイスがクライアント側のパケット内のクライアント証明書からサーバ名を検出します。

SSL アプリケーション識別を有効にするには、応答側のトラフィックを監視するアクセス コントロール ルールを作成する必要があります。このようなルールには、SSL アプリケーションに関するアプリケーション条件または SSL 証明書からの URL を使用した URL 条件を含める必要があります。ネットワーク検出では、応答側の IP アドレスがネットワーク上に存在しなくても、ネットワーク検出ポリシーで監視できます。アクセス コントロール ポリシーの設定によって、トラフィックが識別されるかどうかが決まります。アプリケーション ディテクタ リストで、または、アプリケーション条件をアクセス コントロール ルールに追加するときに、SSL protocol タグでフィルタ処理して SSL アプリケーションのディテクタを識別できます。

特記事項：照会先 Web アプリケーション

Web サーバがトラフィックを他の Web サイト（アドバタイズメント サーバであることが多い）に照会する場合があります。ネットワーク上で発生するトラフィック照会のコンテキストをわかりやすくするために、システムは、照会セッションに対するイベント内の Web Application フィールドにトラフィックを照会した Web アプリケーションを列挙します。VDB に既知の照会先サイトのリストが含まれています。システムがこのようなサイトのいずれかからのトラフィックを検出すると、照会元サイトがそのトラフィックに対するイベントと一緒に保存されます。たとえば、Facebook 経由でアクセスされるアドバタイズメントが実際は Advertising.com 上でホストされている場合は、検出された Advertising.com トラフィックが Facebook Web アプリケーションに関連付けられます。また、システムは、Web サイトで他のサイトへの単リンクが提供されている場合などは、HTTP トラフィック内の参照元 URL を検出することもできます。この場合、参照元 URL は [HTTP Referrer] イベント フィールドに表示されます。

イベントでは、照会元アプリケーションが存在する場合に、それがトラフィックの Web アプリケーションとして列挙されますが、URL は照会先サイトの URL です。上の例では、トラフィックに対する接続イベントの Web アプリケーションは Facebook ですが、URL は Advertising.com です。照会元 Web アプリケーションが検出されない、ホストがそれ自体に照会する、または、照会のチェーンが存在する場合は、照会先アプリケーションがイベント内の Web アプリケーションとして表示されます。ダッシュボードでは、Web アプリケーションの接続カウントとバイト カウントに、Web アプリケーションが照会先のトラフィックに関連付けられたセッションが含まれます。

照会先トラフィックに対して明示的に機能するルールを作成する場合は、照会元アプリケーションではなく、照会先アプリケーションに関する条件を追加する必要があることに注意してください。Facebook から照会される Advertising.com トラフィックをブロックするには、Advertising.com アプリケーションのアクセス コントロール ルールにアプリケーション条件を追加します。

サードパーティ検出データのインポート

ライセンス： FireSIGHT

Nmap アクティブ スキャンを使用してオペレーティング システム、アプリケーション、および脆弱性に関する情報を追加することにより、システムによって収集されたデータを補完できます。Nmap スキャンとスキャン結果の詳細については、Nmap スキャンの概要（47-1 ページ）を参照してください。

ホスト入力機能を使用して API 経由で FireSIGHT システム と対話するようにサードパーティ アプリケーションを設定するか、手動でデータを追加することにより、システムがモニタリング ネットワーク トラフィックから収集した情報を補完することもできます。製品、脆弱性、および修正のマッピングを作成して、サードパーティ データを Cisco 定義にマップすることにより、オペレーティング システムとサーバの影響相関を明確にすることができます。ホスト入力機能とサードパーティ データのマップ方法の詳細については、『*FireSIGHT System Host Input API Guide*』と ホスト入力データのインポート（46-32 ページ）を参照してください。

システムは、オペレーティング システム ID とサーバ ID に関して収集されたデータを照合し、フィンガープリント ソース プライオリティ値、ID 競合解決設定、および収集の時刻に基づいて各 ID を決定します。

NetFlow 対応デバイスからのデータを使用してネットワーク マップ テーブルとイベント テーブルを拡張するようにネットワーク マップを設定することもできます。詳細については、NetFlow について（45-18 ページ）を参照してください。

検出データの用途

ライセンス： FireSIGHT

検出データを記録することにより、次のような FireSIGHT システム内のさまざまな機能を活用できます。

- ホストとネットワーク デバイス、ホスト属性、アプリケーション プロトコル、または脆弱性をグループ化して表示することが可能なネットワーク アセットとトポロジの詳細表現であるネットワーク マップの表示（ネットワーク マップの使用（48-1 ページ）を参照）
- 検出されたホストで利用可能なすべての情報の完全なビューであるホスト プロファイルの表示（ホスト プロファイルの使用（49-1 ページ）を参照）
- （他の機能のいずれかで）ネットワーク アセットとユーザ活動の概要を提供可能なダッシュボードの表示（ダッシュボードの使用（55-1 ページ） を参照）
- システムによって記録された検出イベントとユーザ活動に関する詳細情報の表示（ディスカバリ イベントの使用（50-1 ページ）を参照）
- 検出データに基づくレポートの作成（レポートの操作（57-1 ページ）を参照）
- アプリケーションおよびユーザ制御の実行、つまり、アプリケーション条件とユーザ条件を使用したアクセス コントロール ルールの作成（アプリケーション トラフィックの制御（16-2 ページ） と アクセス コントロール ルールへのユーザ条件の追加（17-3 ページ） を参照）
- ホストおよびそれが実行しているサーバまたはクライアントとそれらが影響を受ける悪用との関連付け。これにより、脆弱性を特定して軽減したり、ネットワークに対する侵入イベントの影響を評価したり、ネットワーク アセットの最大限の保護が提供できるように侵入ルール状態を調整したりできます（ホスト プロファイルでの脆弱性の使用（49-29 ページ）、影響レベルを使用してイベントを評価する（41-39 ページ）、侵害の兆候について（45-22 ページ）、およびネットワーク資産に応じた侵入防御の調整（33-1 ページ）を参照）

- システムが特定の影響フラグ付きの侵入イベントまたは特定のタイプの検出イベントを生成した場合の電子メール、SNMP トラップ、または Syslog 経由の警告（外部アラートの設定（43-1 ページ）を参照）
- 許可されたオペレーティング システム、クライアント、アプリケーション プロトコル、およびプロトコルのホワイト リストを使用した組織の準拠の監視（FireSIGHT システムのコンプライアンス ツールとしての使用（52-1 ページ）を参照）
- システムが検出イベントを生成するかユーザ活動を検出したときにトリガーして相関イベントを生成するルールを使用した相関ポリシーの作成（相関ポリシーおよび相関ルールの設定（51-1 ページ）を参照）
- NetFlow 接続を記録している場合のその接続データの使用（Defense Center または外部サーバへの接続のロギング（38-5 ページ）を参照）

NetFlow について

ライセンス： FireSIGHT

NetFlow は、ネットワーク運用を特徴づける Cisco IOS ソフトウェアに組み込まれた機能です。RFC プロセスを通して標準化された NetFlow は、Cisco のネットワーキング デバイス上で使用できるだけでなく、Juniper、FreeBSD、および OpenBSD デバイスにも組み込むことができます。

NetFlow 対応デバイスは、デバイスを通過するトラフィックに関するデータを収集してエクスポートするために広く使用されています。NetFlow 対応デバイスには、デバイスを通過するフローのレコードを保存する NetFlow キャッシュと呼ばれるデータベースが付属しています。FireSIGHT システムで*接続*と呼ばれるフローは、特定のポート、プロトコル、およびアプリケーション プロトコルを使用する送信元ホストと宛先ホスト間のセッションを表すパケットのシーケンスです。

指定されたネットワークで、FireSIGHT システム の管理対象デバイスが NetFlow 対応デバイスからエクスポートされたレコードを検出して、それらのレコード内のデータに基づいて接続イベントを生成し、最後にそれらのイベントを Defense Center に送信して、データベースに記録します。NetFlow 接続内の情報に基づいて、ホストとアプリケーション プロトコルに関する情報をデータベースに追加するようにシステムを設定することもできます。

この検出データと接続データを使用して、管理対象デバイスによって直接収集されたデータを補完できます。これは、管理対象デバイスで監視できないネットワーク上に NetFlow 対応デバイスを配置した場合に特に有効です。

接続ロギングを含む NetFlow データ収集は、ネットワーク検出ポリシー内のルールを使用して設定します。これを、アクセス コントロールの処理に基づく接続のロギング（38-17 ページ）の説明に従ってアクセス コントロール ルールごとに設定したFireSIGHT システム管理対象デバイスによって検出された接続の接続ロギングと比較してください。NetFlow データ収集は、アクセス コントロール ルールではなく、ネットワークにリンクされるため、記録する接続を細かく制御することはできません。また、システムは自動的にすべての NetFlow ベースの接続イベントを Defense Center 接続イベント データベースに保存するため、それらをシステム ログまたは SNMP トラップ サーバに送信できません。

詳細については、以下を参照してください。

- NetFlow と FireSIGHT データの違い（45-19 ページ）
- NetFlow データの分析準備（45-21 ページ）
- 検出データの用途（45-17 ページ）
- Defense Center または外部サーバへの接続のロギング（38-5 ページ）

NetFlow と FireSIGHT データの違い

ライセンス：FireSIGHT

1 つの例外（TCP フラグ）を除いて、NetFlow レコードで入手可能な情報は、管理対象デバイスを使用したネットワーク トラフィックの監視によって生成される情報より限られています。システムは NetFlow データによって表されるトラフィックを直接分析できないため、NetFlow レコードを処理するときに、さまざまな手段を使用して、そのデータを接続ログだけでなく、ホスト レコードやアプリケーション プロトコル レコードに変換します。

変換されたNetFlow データと、管理対象デバイスによって直接収集された検出および接続データにはいくつかの違いがあります。以下のことを必要とする分析を実行する場合に、この違いを意識しなければなりません。

- 検出された接続数に基づく統計情報
- オペレーティング システムとその他のホスト関連情報（脆弱性を含む）
- クライアント情報、Web アプリケーション情報、ベンダーおよびバージョン サーバ情報を含むアプリケーション データ
- 接続内の発信側のホストと応答側のホストの認識

ヒント　接続イベント内の各フィールドに関して、表 39-1（39-13 ページ）に、接続が FireSIGHT システムの管理対象デバイスによって直接検出されたかどうかによって、または、接続イベントが NetFlow データに基づいている場合に、使用可能なデータを示します。

監視対象セッションごとに生成される接続イベントの数

管理対象デバイスによって直接検出された接続の場合は、アクセス コントロール ルール アクションに応じて、接続の最初か最後またはその両方で双方向接続イベントを記録できます。

ただし、NetFlow 対応デバイスは一方向接続データをエクスポートするため、システムは、常に、デバイスの設定状態に応じて、NetFlow 対応デバイスによって検出された接続ごとに 2 つ以上の接続イベントを生成します。これは、概要の接続カウントが NetFlow データに基づいた接続ごとに 2 ずつ増加することも意味しており、ネットワーク上で実際に発生している接続数が急増することになります。

接続が終了したときにのみレコードを出力するように NetFlow 対応デバイスを設定した場合は、システムがそのセッションに対して 2 つの接続イベントを生成することに注意してください。一方、接続が継続中でも一定間隔でレコードを出力するように NetFlow 対応デバイスを設定した場合、システムはデバイスによってエクスポートされたレコードごとに 1 つずつの接続イベントを生成します。たとえば、長期間接続に関するレコードを 5 分ごとに出力するように NetFlow 対応デバイスを設定し、特定の接続が 12 分間続いた場合、そのセッションに対してシステムは次の 6 つの接続イベントを生成します。

- 最初の 5 分間の 1 つのイベント ペア
- 次の 5 分間の 1 つのペア
- 接続が終了した時点の最後のペア

そのため、Cisco では、監視対象セッションが閉じるときにのみレコードを出力するように NetFlow 対応デバイスを設定することを**強く**推奨しています。

ホスト データとオペレーティング システム データ

NetFlow レコードに基づいてネットワーク マップにホストを追加するようにネットワーク検出ポリシーを設定できますが、ホスト プロファイルには接続に関係するホストのオペレーティング システムや NetBIOS のデータが含まれていないため、システムはホストがネットワーク デバイス(ブリッジ、ルータ、NAT デバイス、またはロード バランサ)なのかどうかを識別できません。ただし、ホスト入力機能を使用してホストのオペレーティング システム ID を手動で設定できます。

アプリケーション データ

管理対象デバイスによって直接検出された接続の場合は、接続内のパケットを検査することによって、システムはアプリケーション プロトコル、クライアント、および Web アプリケーションを識別できます。

システムは NetFlow レコードを処理するときに、`/etc/sf/services` 内のポート関連付けを使用して、アプリケーション プロトコル ID を推測します。ただし、これらのアプリケーション プロトコルに関するベンダーまたはバージョン情報が存在しないため、接続ログにはセッションで使用されるクライアントまたは Web アプリケーションに関する情報が含まれません。しかし、ホスト入力機能を使用してこの情報を手動で提供できます。

単純なポート関連付けでは、非標準ポート上で動作しているアプリケーション プロトコルが特定されないまたは誤認される可能性があることに注意してください。加えて、関連付けが存在しない場合は、システムがそのアプリケーション プロトコルを接続ログで `unknown` としてマークします。

脆弱性マッピング

ホスト入力機能を使用してホストのオペレーティング システム ID またはアプリケーション プロトコル ID が手動で設定されていなければ、FireSIGHT システムはネットワーク マップに追加されたホストに影響する脆弱性を NetFlow レコードに基づいて識別することはできません。NetFlow 接続内にクライアント情報が存在しないため、クライアントの脆弱性と NetFlow ホストを関連付けることができないことに注意してください。

接続内の発信側情報と応答側情報

管理対象デバイスによって直接検出された接続の場合、システムは発信側または送信元のホストと応答側または宛先のホストを識別できます。ただし、NetFlow データには発信側または応答側の情報が含まれていません。

システムが NetFlow レコードを処理するときには、各ホストが使用しているポート、およびそれらのポートが既知であるかどうかに基づき、アルゴリズムに従ってその情報が判別されます。

- 使用されているポートの両方が既知のポートの場合、または、どちらも既知のポートでない場合、システムは番号の若い方のポートを使用しているホストを応答側と見なします。
- どちらかのホストだけが既知のポートを使用している場合は、システムはそのホストを応答側と見なします。

したがって、既知のポートは、1 ～ 1023 の番号が割り当てられたポートまたは管理対象デバイス上の `/etc/sf/services` にアプリケーション プロトコル情報が保存されているポートです。

NetFlow データの分析準備

ライセンス：FireSIGHT

NetFlow データを分析するように FireSIGHT システム を設定する前に、使用するルータまたはその他の NetFlow 対応デバイス上の NetFlow 機能を有効にして、管理対象デバイスのセンシング インターフェイスが接続されている宛先ネットワークに NetFlow バージョン 5 のデータをエクスポートするようにデバイスを設定する必要があります。

システムは NetFlow バージョン 5 と NetFlow バージョン 9 のレコードを解釈できることに注意してください。NetFlow 対応デバイスは、FireSIGHT システム 導入と一緒に使用する場合に、これらのバージョンのどちらかを使用する**必要があります**。加えて、システムは、NetFlow 対応デバイスが送信するテンプレートとレコード内に特定のフィールドが存在することを必要とします。NetFlow 対応デバイスがカスタマイズ可能なバージョン 9 を使用している場合は、デバイスが送信するテンプレートとレコードに次のフィールドが任意の順序で含まれていることを確認する**必要があります**。

- IN_BYTES (1)
- IN_PKTS (2)
- PROTOCOL (4)
- TCP_FLAGS (6)
- L4_SRC_PORT (7)
- IPV4_SRC_ADDR (8)
- L4_DST_PORT (11)
- IPV4_DST_ADDR (12)
- LAST_SWITCHED (21)
- FIRST_SWITCHED (22)
- IPV6_SRC_ADDR (27)
- IPV6_DST_ADDR (28)

FireSIGHT システム は管理対象デバイスを使用して NetFlow データを分析するため、NetFlow 対応デバイスを監視可能な 1 つ以上の管理対象デバイスを導入に含める必要があります。この管理対象デバイス上の 1 つ以上のセンシング インターフェイスを、NetFlow 対応デバイスがエクスポートするデータを収集可能なネットワークに接続する必要があります。通常、管理対象デバイス上のセンシング インターフェイスには IP アドレスが割り当てられないため、システムは NetFlow レコードの直接収集をサポートしません。

加えて、Cisco では、監視対象セッションが閉じるときにのみレコードを出力するように NetFlow 対応デバイスを設定することを**強く**推奨しています。一定間隔でレコードを出力するように NetFlow 対応デバイスを設定した場合は、NetFlow レコードから抽出された接続データの分析がより複雑になる可能性があります。監視対象セッションごとに生成される接続イベントの数 (45-19 ページ) を参照してください。

最後に、一部の NetFlow 対応デバイス上で使用可能な Sampled NetFlow 機能は、デバイスを通過するパケットのサブセットだけに基づく NetFlow 統計情報を収集することに注意してください。この機能を有効にすると、NetFlow 対応デバイス上の CPU 使用率が改善される可能性がありますが、システムで分析するために収集されているデータに影響する場合があります。

侵害の兆候について

ライセンス：FireSIGHT

ネットワーク検出の一部として、FireSIGHT システムの Data Correlator は、ホストに関連するさまざまなタイプのデータ（侵入イベント、セキュリティ インテリジェンス、接続イベント、およびマルウェア イベント）を関連付けることにより、監視対象ネットワーク上のホストが悪意のある手段で侵害される可能性があるかどうかを特定できます。この関連付けは侵害の兆候（IOC）と呼ばれています。この機能をアクティブにするには、検出ポリシー エディタでこの機能と Cisco によるさまざまな事前定義の *IOC ルール*のうちのいずれかを有効にします。この機能が有効になっている場合は、そのホストのホスト プロファイルからの個別のホストのルール状態を編集することもできます。IOC ルールのそれぞれがホストに関連付けられた 1 つの特定の *IOC タグ*に対応します。

Data Correlator に加えて、Cisco のエンドポイント ベースの Collective Security Intelligence クラウド データも IOC ルールから IOC タグを生成できます。このデータがホスト自体の活動（個別のプログラムによってまたはプログラム上で実行されるアクションなど）を検査するため、ネットワーク専用データでは理解するのが難しい可能性がある脅威に対する理解が促されます。エンドポイントからの FireAMP IOC データは Cisco クラウド接続経由で送信されます。

アクティブ IOC タグ付きのホストは、通常のホスト アイコン（  ）ではなく、侵害されたホスト アイコン（  ）を伴ってイベント ビューの [IP Address] 列に表示されます。IOC タグをトリガー可能なイベントのイベント ビューで、イベントが IOC をトリガーしたかどうかが示されます。

侵害の兆候タイプについて

ライセンス：FireSIGHT

多くの侵害の兆候（IOC）ルールとタグ タイプがあります。すべてが Cisco により事前定義済みで、1 つの IOC ルールが 1 つの IOC タグに対応します。IOC ルールは FireSIGHT システムのその他の機能（および一部のイベントは Cisco クラウド）から提供されるデータに基づいてトリガーされるため、これらの機能を使用可能にして、IOC タグをセットする IOC ルールに対してアクティブにする必要があります。Cisco が新しいエンドポイント ベースのマルウェア イベントの IOC タイプを作成すると、システムはクラウド経由で自動的にそれらをダウンロードし、使用します。下のリストに、IOC ルール タイプ、それらが関連付けられた機能、および追加のライセンス要件（ネットワーク検出に必要な FireSIGHT ライセンス以外）の詳細を示します。

- エンドポイント ベースのマルウェア イベント IOC タイプ（45-22 ページ）
- 侵入イベント IOC タイプ（45-23 ページ）
- セキュリティ インテリジェンス イベント IOC タイプ（45-24 ページ）

エンドポイント ベースのマルウェア イベント IOC タイプ

ライセンス：FireSIGHT

次のリストには、Cisco クラウドへのサブスクリプションが必要な、エンドポイント ベースのマルウェア イベントに関連付けられている IOC タイプの例が含まれています。次に示す IOC タイプに加えて、Cisco では定期的に新しいタイプを作成しており、システムはクラウドへの接続を介してそれらを自動的にダウンロードして実装しています。

エンドポイント ベースのマルウェア防御の設定方法については、FireAMP 用のクラウド接続の操作（37-27 ページ）と ネットワークベースの AMP とエンドポイント ベースの FireAMP の比較（37-9 ページ）を参照してください。

- Adobe Reader 侵害:Adobe Reader がシェルを起動
- Adobe Reader 侵害:FireAMP によって検出された PDF 侵害
- CnC の接続:FireAMP によって検出された疑わしいボットネット
- ドロッパ感染:FireAMP によって検出されたドロッパ感染
- Excel 侵害:FireAMP によって検出された Excel 侵害
- Excel 侵害:Excel がシェルを起動
- FireAMP によって検出された汎用 IOC
- Java 侵害:FireAMP によって検出された Java 侵害
- Java 侵害:Java がシェルを起動
- マルウェアの検出:FireAMP によって検出された脅威:未実行
- マルウェアの検出:ファイル転送中に検出された脅威
- マルウェアの実行:FireAMP によって検出された脅威:実行
- Microsoft Calculator 侵害:FireAMP によって検出された Microsoft Calculator 侵害
- Microsoft Notepad 侵害:FireAMP によって検出された Microsoft Calculator 侵害
- PowerPoint 侵害:FireAMP によって検出された PowerPoint 侵害
- PowerPoint 侵害:PowerPoint がシェルを起動
- QuickTime 侵害:FireAMP によって検出された QuickTime 侵害
- QuickTime 侵害:QuickTime がシェルを起動
- Word 侵害:FireAMP によって検出された Word 侵害
- Word 侵害:Word がシェルを起動

侵入イベント IOC タイプ

ライセンス: FireSIGHT+Protection

次の IOC タイプは、Protection ライセンスが必要な侵入イベントに関連付けられます。侵入イベントの表示方法と侵入検知および防御の設定方法については、侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（18-1 ページ）と侵入イベントの表示（41-9 ページ）を参照してください。

- CnC の接続:侵入イベント - malware-backdoor
- CnC の接続:侵入イベント - malware-cnc
- エクスプロイト キット:侵入イベント - exploit-kit
- 影響 1 攻撃:影響 1 侵入イベント - attempted-admin
- 影響 1 攻撃:影響 1 侵入イベント - attempted-user
- 影響 1 攻撃:影響 1 侵入イベント - successful-admin
- 影響 1 攻撃:影響 1 侵入イベント - successful-user
- 影響 1 攻撃:影響 1 侵入イベント - web-application-attack
- 影響 2 攻撃:影響 2 侵入イベント - attempted-admin
- 影響 2 攻撃:影響 2 侵入イベント - attempted-user

- 影響 2 攻撃:影響 2 侵入イベント - successful-admin
- 影響 2 攻撃:影響 2 侵入イベント - successful-user
- 影響 2 攻撃:影響 2 侵入イベント - web-application-attack

セキュリティ インテリジェンス イベント IOC タイプ

ライセンス: FireSIGHT+Protection

サポートされるデバイス: すべて(シリーズ 2 を除く)

サポートされる防御センター: すべて(DC500 を除く)

CnC の接続:セキュリティ インテリジェンス イベント - CnC タイプは、接続イベントのタイプであるセキュリティ インテリジェンス イベントに関連付けられています。セキュリティ インテリジェンス機能には、Protection ライセンスが必要です。セキュリティ インテリジェンスの設定方法とセキュリティ インテリジェンス イベントの表示方法については、セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録(13-1 ページ)と接続およびセキュリティ インテリジェンスのデータの表示(39-15 ページ)を参照してください。

侵害の兆候データの表示と編集

ライセンス: FireSIGHT

ネットワーク検出ポリシーそのものを除いて、FireSIGHT システム Web インターフェイスの他の部分で侵害の兆候(IOC)データを表示して編集できます。

- ダッシュボードでは、デフォルトで、サマリー ダッシュボードの [Threats] タブに、ホスト別の IOC タグと一定期間にトリガーされた新しい IOC ルールが表示されます。カスタム分析ウィジェットは IOC データに基づくプリセットを提供します。詳細については、ダッシュボードの使用(55-1 ページ)およびCustom Analysis ウィジェットの設定(55-15 ページ)を参照してください。
- Context Explorer の [Indications of Compromise] セクションに、IOC カテゴリ別のホストとホスト別の IOC カテゴリのグラフが表示されます。詳細については、[Indications of Compromise] セクションについて(56-4 ページ)を参照してください。
- 検出(IOC)イベント、接続イベント、セキュリティ インテリジェンス イベント、侵入イベント、およびマルウェア イベントのイベント ビューには、イベントが IOC ルールをトリガーしたかどうかが表示されます(IOC 列)。IOC ルールをトリガーするエンドポイント ベースのマルウェア イベントは、イベント タイプが FireAMP IOC であり、侵害を指定するイベント サブタイプと一緒に表示されます。イベント ビューアに表示されるすべての IOC データに対して準拠ルールを作成できます。詳細については、次の項を参照してください。
- 接続およびセキュリティ インテリジェンスのデータの表示(39-15 ページ)
- 侵入イベントの表示(41-9 ページ)
- マルウェア イベントの操作(40-17 ページ)
- 侵害の痕跡の使用(50-35 ページ)
- 相関ポリシーおよび相関ルールの設定(51-1 ページ)
- ネットワーク マップの [Indications of Compromise] タブに、監視対象ネットワーク上のホストが、IOC タグでグループ化されて一覧表示されます。詳細については、セキュリティ侵害の痕跡のネットワークのマップの使用(48-5 ページ)を参照してください。

- 侵害された可能性のあるホストのホスト プロファイル ビューでは、そのホストに関連付けられたすべての IOC タグを表示したり、IOC タグの一部または全部を解決したり、IOC ルール状態を設定したりできます。詳細については、ホスト プロファイルでの侵害の痕跡の使用（49-9 ページ）を参照してください。

ネットワーク検出ポリシーの作成

ライセンス： FireSIGHT

Defense Center上のネットワーク検出ポリシーは、システムが組織のネットワーク アセットに関するデータを収集する方法と、どのネットワーク セグメントとポートを監視対象とするかを制御します。

ポリシー内の検出ルールは、FireSIGHT システムが監視してトラフィック内のネットワーク データに基づいて検出データを生成するネットワークおよびポートと、ポリシーを適用するゾーンを指定します。ルール内では、ホスト、アプリケーション、およびユーザを検出するかどうかを設定できます。検出からネットワークとゾーンを除外するルールを作成できます。NetFlow デバイスから検出するためのルールを作成するときに、接続を記録するだけにすることもできます。

ネットワーク検出ポリシーには、0.0.0.0/0 ネットワーク上の IPv4 トラフィックでアプリケーションを検出するように設定された、単一のデフォルト ルールが組み込まれています。アクセス コントロール ポリシーを対象のデバイスに適用しておかなければ、ネットワーク検出ポリシーを適用できないことに注意してください。このルールでは、どのネットワーク、ゾーン、またはポートも除外されず、ホストとユーザの検出が設定されず、NetFlow デバイスが設定されません。ポリシーは Defense Centerに登録されたときに、デフォルトで、すべての管理対象デバイスに適用されることに注意してください。ホストまたはデータの収集を開始するには、検出ルールを追加または変更して、ポリシーをデバイスに再適用する必要があります。

アクセス コントロール ポリシーは許可されたトラフィック、つまり、ネットワーク検出を使用して監視可能なトラフィックを定義することに注意してください。これは、アクセス コントロールを使用して特定のトラフィックをブロックすると、システムでホスト、ユーザ、またはアプリケーションの活動に関するトラフィックを検査できなくなることを意味することに注意してください。たとえば、アクセス コントロール ポリシーでソーシャル ネットワーキング アプリケーションへのアクセスをブロックすると、システムはそのようなアプリケーションに関する検出データを提供しなくなります。

ネットワーク検出の範囲を調整する場合は、追加の検出ルールを作成して、デフォルト ルールを変更または削除できます。NetFlow デバイスからのデータの検出を設定して、ネットワーク上でユーザ データが検出されるトラフィックのプロトコルを制限できます。

FireSIGHT システムを使用して侵入検知および防御を実行するものの検出データを利用する必要がない場合は、新しい検出を無効にしてパフォーマンスを最適化できます。まず、適用されるアクセス コントロール ポリシーに、ユーザ、アプリケーション、または URL の条件を扱うルールが含まれないことを確認してください。その後、ネットワーク検出ポリシーからすべてのルールを削除し、それを管理対象デバイスに適用します。アクセス コントロール ルールの設定方法については、アクセス コントロール ルールを使用したトラフィック フローの調整（14-1 ページ）を参照してください。

検出ルールでユーザ検出を有効にすると、一連のアプリケーション プロトコル全体のトラフィック内のユーザ ログイン活動を通してユーザを検出できます。必要に応じて、すべてのルールにわたって特定のプロトコル内の検出を無効にできます。一部のプロトコルを無効にすると、FireSIGHT ライセンスに関連付けられたユーザ制限に達するのを防ぐのに役立ち、他のプロトコルからのユーザに使用可能なユーザ カウントを確保できます。

詳細ネットワーク検出設定を使用すれば、記録するデータの種類、検出データの保存方法、アクティブにする侵害の兆候（IOC）ルール、影響評価に使用する脆弱性マッピング、送信元からの検出データが競合していた場合の対処を管理できます。また、ホスト入力として NetFlow デバイスと送信元を追加できます。

詳細については、以下を参照してください。

- 検出ルールの操作（45-26 ページ）
- ユーザ ロギングの制限（45-33 ページ）
- 高度なネットワーク検出オプションの設定（45-34 ページ）
- ネットワーク検出ポリシーの適用（45-41 ページ）

検出ルールの操作

ライセンス： FireSIGHT

検出ルールを使用すれば、ネットワーク マップに対して検出される情報を調整し、必要な特定のデータだけを含めるようにすることができます。ネットワーク検出ポリシー内のルールは順番に評価されます。モニタリング基準が重複したルールを作成できますが、その場合はシステム パフォーマンスに影響する可能性があることに注意してください。

モニタリングからホストまたはネットワークを除外すると、そのホストまたはネットワークがネットワーク マップに表示されず、それに対するイベントが報告されません。Ciscoでは、モニタリングからロード バランサ（またはロード バランサ上の特定のポート）と NAT デバイスを除外することを推奨しています。これらのデバイスは紛らわしいイベントを過剰に生成するため、データベースがいっぱいになったり、Defense Centerが過負荷になったりする可能性があります。たとえば、監視対象 NAT デバイスが短期間にオペレーティング システムの複数の更新を表示する場合があります。ロード バランサと NAT デバイスの IP アドレスがわかっている場合は、モニタリングからそれらを除外できます。

ヒント システムは、ネットワーク トラフィックを検査することにより、複数のロード バランサと NAT デバイスを識別できます。ネットワーク上のどのホストがロード バランサでどのホストが NAT デバイスかを特定するには、ネットワーク検出ポリシーを適用して、システムがネットワーク マップを生成するまで待機してから、ホスト タイプで絞り込んだホストの検索を実行します。

加えて、カスタム サーバ フィンガープリントを作成する必要がある場合は、フィンガープリントを行っているホストとの通信に使用されている IP アドレスをモニタリングから一時的に除外する必要があります。そうしないと、ネットワーク マップおよびディスカバリ イベント ビューに、その IP アドレスによって表されるホストに関する不正確な情報が混在することになります。フィンガープリントを作成したら、その IP アドレスを監視するようにポリシーを設定し直すことができます。詳細については、サーバのフィンガープリントの作成（46-11 ページ）を参照してください。

Cisco では、NetFlow 対応デバイスと FireSIGHT システム 管理対象デバイスを使用して、同じネットワーク セグメントを監視**しない**ことも推奨しています。重複しないルールを使用してネットワーク検出ポリシーを設定するのが理想ですが、管理対象デバイスによって生成された重複接続ログはシステムによって破棄されます。管理対象デバイスと NetFlow 対応デバイスの両方で検出された接続に関する重複接続ログは破棄**できない**ことに注意してください。

詳細については、次の項を参照してください。

- デバイス選択について（45-27 ページ）
- アクションと検出されるアセットについて（45-27 ページ）

デバイス選択について

ライセンス：FireSIGHT

検出ルール内で NetFlow デバイスを選択する場合、ルールは指定されたネットワークの NetFlow データの検出に制限されます。NetFlow デバイスを選択すると使用可能なルール アクションが変更されるため、NetFlow デバイスを選択してからルール動作の他の側面を設定します。加えて、NetFlow トラフィックのポート除外は設定できません。

ネットワーク検出ルール内で NetFlow デバイスを選択する場合は、ネットワーク検出の詳細設定で NetFlow デバイスへの接続を設定しておく必要があります。詳細については、NetFlow 対応デバイスの追加（45-38 ページ）を参照してください。

アクションと検出されるアセットについて

ライセンス：FireSIGHT

検出ルールを設定するときに、ルールのアクションを選択する必要があります。このアクションによって、システムがルールを処理するときに、どのアセットが検出され、どのアセットが除外されるかが決まります。ただし、ルール アクションの影響は、管理対象デバイスからのデータを検出するルールを使用しているかまたは NetFlow 対応デバイスからのデータを検出するルールを使用しているかによって異なることに注意してください。

ホストまたはユーザを検出するルールを使用せずにネットワーク検出ポリシーを作成して適用すると、アプライアンスの新しい検出が無効になることに注意してください。管理対象デバイスを侵入防御のためだけに使用する場合にパフォーマンスを最適化するには、ポリシーからすべての検出ルールを削除し、アクティブ デバイスに適用します。

次の表に、これら 2 つのシナリオで指定されたアクション設定を使用したルールで検出されるアセットの説明を示します。

表 45-4　検出ルールのアクション

アクション	管理対象デバイス	NetFlow
除外	モニタリングから指定されたネットワークを除外します。接続の発信元ホストまたは宛先ホストを検出から除外すると、接続は記録されますが、除外したホストの検出イベントは作成されません。	
検出：ホスト	検出イベントに基づいてネットワーク マップにホストを追加します（任意、ユーザ検出が有効になっていない場合は必須）。	NetFlow レコードに基づいてネットワーク マップにホストを追加します。（必須）

表 45-4　検出ルールのアクション（続き）

アクション	管理対象デバイス	NetFlow
検出:アプリケーション	アプリケーション ディテクタに基づいてネットワーク マップにアプリケーションを追加します。アプリケーションも検出しないルールでは、ホストまたはユーザを検出できないことに注意してください。（必須）	NetFlow レコードと /etc/sf/services 内のポートとアプリケーション プロトコルの関連付けに基づいてネットワーク マップにアプリケーション プロトコルを追加します。/etc/sf/services。（任意）
検出:ユーザ	ネットワーク検出ポリシーで設定されたユーザ プロトコルと一致するトラフィックで検出された活動に基づいてユーザをユーザ テーブルに追加し、ユーザ活動を記録します。（任意）	n/a
NetFlow 接続の記録	n/a	NetFlow 接続のみを記録します。ホストまたはアプリケーションを検出しません。

監視対象ネットワークについて

ライセンス: FireSIGHT

検出ルールは、監視対象アセットの検出を、指定されたネットワーク上のホストとの間のトラフィックだけを対象にして行います。検出ルールでは、指定されたネットワーク内の 1 つ以上の IP アドレスが割り当てられた接続に対して検出が行われ、監視対象ネットワーク内の IP アドレスに対してのみイベントが生成されます。デフォルトの検出ルールは、0.0.0.0/0 ネットワークと ::/0 ネットワーク上でのみアプリケーションを検出します。

ルールで NetFlow デバイスが指定され、Log Network Connectionsオプションが有効になっている場合は、指定されたネットワーク内の IP アドレスとの間の接続も記録されます。ネットワーク検出ルールが NetFlow ネットワーク接続を記録する唯一の方法を提供することに注意してください。

また、ネットワーク オブジェクトまたはオブジェクト グループを使用して監視対象ネットワークを指定することもできます。ネットワーク検出ポリシーで使用されているネットワーク オブジェクトを変更した場合は、その変更を検出に反映させるためにポリシーを再適用する必要があります。

ネットワーク検出ポリシー内のゾーンについて

ライセンス: FireSIGHT

パフォーマンス上の理由で、ルール内の監視対象ネットワークに物理的に接続されている管理対象デバイス上のセンシング インターフェイスがルール内のゾーンに含まれるように各検出ルールを設定する必要があります。

残念ながら、ネットワーク設定の変更が常に通知されるわけではありません。ネットワーク管理者が通知せずにルーティングやホストの変更によりネットワーク設定を変更した場合、正しいネットワーク検出ポリシー設定を完全に把握するのが難しくなります。管理対象デバイス上のセンシング インターフェイスが物理的にネットワークに接続されている方法がわからない場合は、導入内のすべてのゾーンに検出ルールが適用されるデフォルトのゾーン設定のまま変更しないでください（ゾーンが除外されていなければ、検出ポリシーがすべてのゾーンに適用されます）。

ポート除外について

ライセンス：FireSIGHT

モニタリングからホストを除外できる（アクションと検出されるアセットについて（45-27 ページ）を参照）のと同様に、モニタリングから特定のポートを除外できます。

たとえば、ロード バランサは短期間に同じポート上の複数のアプリケーションを報告する可能性があります。モニタリングからそのポートを除外する（Web ファームを処理するロード バランサ上のポート 80 を除外するなど）ようにネットワーク検出ポリシーを設定できます。

別のシナリオとして、組織で特定の範囲のポートを使用するカスタム クライアントを使用しているとします。このクライアントからのトラフィックが紛らわしいイベントを過剰に生成する場合は、モニタリングからそれらのポートを除外できます。同様に、DNS トラフィックを監視しないように設定することもできます。この場合は、ポート 53 を監視しないように、ポリシーを設定します。

除外するポートを追加するときには、[Available Ports] リストから再利用可能なポート オブジェクトを選択するのか、送信元または宛先除外リストにポートを直接追加するのか、新しい再利用可能なポートを作成してからそれを除外リストに移動するのかを決定できます。

NetFlow 対応デバイスは、モニタリングからポートを除外するように設定できないことに注意してください。

検出ルールの追加

ライセンス：FireSIGHT

検出ルールを設定し、ニーズに合わせてホスト データとアプリケーション データの検出を調整できます。ルールで参照されているオブジェクトを変更した場合は、その変更を反映させるためにネットワーク検出ポリシーを再適用する必要があることに注意してください。

検出ルールを追加する方法：

アクセス：Admin/Discovery Admin

ステップ 1　アクセス コントロール ポリシーをチェックして、ネットワーク データを検出するトラフィックの必要な接続が記録されていることを確認します。

詳細については、アクセス コントロールの処理に基づく接続のロギング（38-17 ページ）を参照してください。ほとんどのデータを検出するには、検出するトラフィックの接続の最後で記録します。

ステップ 2　[Policies] > [Network Discovery] の順に選択します。

[Network Discovery Policy] ページが表示されます。

ステップ 3　[Add Rule] をクリックします。

[Add Rule] ポップアップ ウィンドウが表示されます。

ステップ 4　次の 2 つのオプションから選択できます。

- NetFlow トラフィックを監視するルールを使用する場合は、[Add Rule] ポップアップ ウィンドウで、[NetFlow Device] をクリックします。

  [NetFlow Device] ページが表示されます。

  NetFlow ページは、NetFlow デバイスを検出ポリシーに追加した場合にのみ使用できることに注意してください。詳細については、NetFlow 対応デバイスの追加（45-38 ページ）を参照してください。

- 管理対象デバイスを監視するルールを使用する場合は、ステップ 6 を省略します。

詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）およびデバイス選択について（45-27 ページ）を参照してください。

ステップ 5　ドロップダウンリストから、使用する NetFlow デバイスの IP アドレスを選択します。

ステップ 6　ルールのアクションの設定：

- ネットワーク検出からルールと一致するすべてのトラフィックを除外するには、[Exclude] を選択します。このルール アクションを選択すると、[Port Exclusions] タブが無効になることに注意してください。
- ルールと一致するトラフィックの選択したデータのタイプを検出するには、[Discovery] を選択して、該当するデータ タイプのチェック ボックスをオンまたはオフにします。

  管理対象デバイス上のトラフィックを監視している場合は、アプリケーション ロギングが必須です。ユーザを監視している場合は、ホスト ロギングが必須です。NetFlow トラフィックを監視している場合は、ユーザを記録できないことと、アプリケーションのロギングが任意であることに注意してください。
- NetFlow トラフィックを監視している場合は、NetFlow トラフィック内の接続を記録するルールを使用するために、[Log NetFlow Connections] を選択します。このオプションは、ルール内で NetFlow デバイスを選択した後でしか表示されないことに注意してください。

注　システムは、ネットワーク検出ポリシー設定に基づいて NetFlow トラフィック内の接続を検出します。管理対象デバイス トラフィックでの接続ロギングはアクセス コントロール ポリシーで設定します。詳細については、ネットワーク トラフィックの接続のロギング（38-1 ページ）を参照してください。

ルール アクションとアセットの検出の詳細については、アクションと検出されるアセットについて（45-27 ページ）を参照してください。

ステップ 7　すべての検出ルールに 1 つ以上のネットワークを含める必要があります。オプションで、ルール アクションを特定のネットワークに制限するには、[Networks] タブをクリックして、[Available Networks] リストからネットワークを選択し、[Add] をクリックするか、[Networks] リストの下でネットワークを入力して [Add] をクリックします。

ネットワーク モニタリングの詳細については、監視対象ネットワークについて（45-28 ページ）を参照してください。[Available Networks] リストにネットワーク オブジェクトを追加する方法については、ネットワーク オブジェクトの作成（45-31 ページ）を参照してください。ネットワーク検出ポリシーで使用されているネットワーク オブジェクトを変更した場合は、その変更を検出に反映させるためにポリシーを再適用する必要があることに注意してください。

ステップ 8　オプションで、ルール アクションを特定のゾーン内のトラフィックに制限するには、[Zones] をクリックして、[Available Zones] リストから 1 つまたは複数のゾーンを選択し、[Add] をクリックします。

モニタリング用のゾーンの選択方法については、ネットワーク検出ポリシー内のゾーンについて（45-28 ページ）を参照してください。

ステップ 9　モニタリングからポートを除外するには、[Port Exclusions] をクリックします。

[Port Exclusions] ページが表示されます。

ステップ 10　モニタリングから特定の送信元ポートを除外するには、次の 2 つの選択肢があります。

- [Available Ports] リストから 1 つまたは複数のポートを選択して、[Add to Source] をクリックします。

- ポート オブジェクトを追加せずに特定の送信元ポートからのトラフィックを除外するには、[Selected Source Ports] リストの下にある [Protocol] ドロップダウンリストから該当するプロトコルを選択して、[Port] フィールドに 1 ～ 65535 のポート番号を入力し、[Add] をクリックします。

  モニタリングからポートを除外する方法については、ポート除外について（45-29 ページ）を参照してください。[Available Networks] リストにポート オブジェクトを追加する方法については、ポート オブジェクトの作成（45-32 ページ）を参照してください。ネットワーク検出ポリシーで使用されているポート オブジェクトを変更した場合は、その変更を検出に反映させるためにポリシーを再適用する必要があることに注意してください。

ステップ 11　モニタリングから特定の宛先ポートを除外するには、次の 2 つの選択肢があります。

- [Available Ports] リストから 1 つまたは複数のポートを選択して、[Add to Destination] をクリックします。
- ポート オブジェクトを追加せずに特定の宛先ポートからのトラフィックを除外するには、[Selected Destination Ports] リストの下にある [Protocol] ドロップダウンリストから該当するプロトコルを選択して、[Port] フィールドに 1 ～ 65535 のポート番号を入力し、[Add] をクリックします。

ステップ 12　ルールの編集が終了したら、[Save] をクリックして、検出ポリシー ルールのリストに戻ります。

変更を反映させるためにネットワーク検出ポリシーを適用する必要があります。詳細については、ネットワーク検出ポリシーの適用（45-41 ページ）を参照してください。

ネットワーク オブジェクトの作成

ライセンス： FireSIGHT

検出ルールに表示される利用可能なネットワークのリストには、FireSIGHT システムのあらゆる場所で使用できる再利用可能なネットワーク オブジェクトとグループが含まれています。このリストに新しいネットワーク オブジェクトを追加することができます。ルールで参照されているオブジェクトを変更した場合は、その変更を反映させるためにネットワーク検出ポリシーを再適用する必要があることに注意してください。

新しいネットワーク オブジェクトを作成する方法：

Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] の順に選択します。

[Network Discovery Policy] ページが表示されます。

ステップ 2　[Add Rule] をクリックします。

[Add Rule] ポップアップ ウィンドウが表示されます。

ステップ 3　[Networks] ページで、追加アイコン（  ）をクリックします。

[Network Objects] ポップアップ ウィンドウが表示されます。

ステップ 4　[Name] にネットワーク オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　ネットワーク オブジェクトに追加する IP アドレス、CIDR ブロック、およびプレフィクス長ごとに、その値を入力して [Add] をクリックします。

ステップ 6　[Save] をクリックして、[Available Networks] リストにネットワーク オブジェクトを追加します。

ヒント　ネットワークがすぐにリストに表示されない場合は、更新アイコン( )をクリックします。

ポート オブジェクトの作成

ライセンス: FireSIGHT

検出ルールに表示される利用可能なポートのリストには、FireSIGHT システムのあらゆる場所で使用できる再利用可能なポート オブジェクトとグループが含まれています。このリストに新しいポート オブジェクトを追加することができます。ルールで参照されているオブジェクトを変更した場合は、その変更を反映させるためにネットワーク検出ポリシーを再適用する必要があることに注意してください。

新しいポート オブジェクトを作成する方法:

Admin/Discovery Admin

ステップ 1　[Port Exclusions] をクリックします。

[Port Exclusions] ページが表示されます。

ステップ 2　[Available Ports] リストにポートを追加するには、追加アイコン( )をクリックします。

[Port Objects] ポップアップ ウィンドウが表示されます。

ステップ 3　ポート オブジェクトの [Name] を入力します。縦線(|)と中カッコ({})を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 4　[Protocol] フィールドで、除外するトラフィックのプロトコルを指定します。

[TCP]、[UDP]、または [Other] を選択して、ドロップダウンリストからオプションを選択し、プロトコルまたは [All] を選択します。

ステップ 5　[Port(s)] フィールドに、モニタリングから除外するポートを入力します。

単一のポート、ダッシュ(-)を使用したポートの範囲、またはポートとポート範囲のカンマ区切りのリストを指定できます。許容されるポート値は 1 ～ 65535 です。

ステップ 6　[Save] をクリックして、[Available Ports] リストにポートを追加します。

ヒント　ポートがすぐにリストに表示されない場合は、更新アイコン( )をクリックします。

ユーザ ロギングの制限

ライセンス: FireSIGHT

ユーザを検出するルールを使用したネットワーク検出ポリシーを適用すると、AIM、IMAP、LDAP、Oracle、POP3、SMTP、FTP、HTTP、MDNS および SIP プロトコルを使用するトラフィック内でユーザが検出されます。これらのユーザは、[Analysis] メニューからアクセス可能な [users] テーブルに追加されます。ユーザ 活動を検出するプロトコルを制限して、検出するユーザの総数を削減することにより、ほぼ完全なユーザ情報を提供していると思われるユーザに焦点を絞ることができます。

Defense Centerで保存できる検出済みユーザの総数は、FireSIGHT ライセンスによって異なります。ライセンス制限に達すると、ほとんどの場合、システムはデータベースへの新しいユーザの追加を停止します。新しいユーザを追加するには、古いユーザまたは非アクティブなユーザをデータベースから手動で削除するか、データベースからすべてのユーザを消去する必要があります。プロトコル検出を制限すれば、ユーザ名の氾濫を最小限に抑え、FireSIGHT ユーザ ライセンスを節約できます。

たとえば、AIM、POP3、IMAP などのプロトコル経由でユーザ名を取得すると、契約業者、訪問者、およびその他のゲストからのネットワーク アクセスによって組織に無関係なユーザ名が収集される可能性があります。

別の例として、AIM、Oracle、および SIP ログインは、無関係なユーザ レコードを作成する可能性があります。この現象は、このようなログイン タイプが、システムが LDAP サーバから取得するユーザ メタデータのいずれにも関連付けられていないうえ、管理対象デバイスが検出するその他のログイン タイプに含まれている情報のいずれにも関連付けられていないために発生します。そのため、Defense Centerは、これらのユーザとその他のユーザ タイプを関連付けることができません。

管理対象デバイスだけは非 LDAP ユーザ ログインを検出できることに注意してください。Microsoft Active Directory サーバにインストールされたユーザ エージェントのみを使用してユーザ活動を検出している場合は、非 LDAP ログインを制限しても効果はありません。また、SMTP ロギングを制限することはできません。これは、ユーザが SMTP ログインに基づいてデータベースに追加されていないためです。システムが SMTP ログインを検出しても、一致する電子メール アドレスのユーザがデータベース内に存在しなければ、そのログインは記録されません。

LDAP、POP3、FTP または IMAP トラフィック内でユーザ ログインの失敗が検出された場合にそのログイン試行の失敗を記録するように選択できます。失敗ログイン試行で新しいユーザがデータベース内のユーザのリストに追加されることはありません。ユーザ エージェントは失敗ログイン活動を報告しないことに注意してください。検出された失敗ログイン活動のユーザ活動タイプは Failed User Login です。

システムは失敗した HTTP ログインと成功した HTTP ログインを区別できないことに注意してください。HTTP ユーザ情報を表示するには、[Capture Failed Login Attempts] を有効にする必要があります。

ユーザ ログインを検出するプロトコルを制限する方法:

Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] の順に選択します。

[Network Discovery Policy] ページが表示されます。

ステップ 2　[User] をクリックします。

[User] ページが表示されます。

ステップ 3　ログインを検出するプロトコルのチェック ボックスをオンにするか、ログインを検出しないプロトコルのチェック ボックスをオフにします。

ステップ 4　オプションで、LDAP、POP3、FTP、または IMAP トラフィックで検出されたログイン試行の失敗を記録したり、HTTP ログインのユーザ情報を取得するには、[Capture Failed Login Attempts] を有効にします。

ステップ 5　[Save] をクリックして、ネットワーク ポリシーを保存します。

変更を反映させるためにネットワーク検出ポリシーを適用する必要があります。詳細については、ネットワーク検出ポリシーの適用（45-41 ページ）を参照してください。

高度なネットワーク検出オプションの設定

ライセンス： FireSIGHT

ネットワーク検出ポリシーの [Advanced] タブを使用すれば、検出するイベント、検出データの保存期間と更新頻度、影響相関に使用する脆弱性マッピング、およびオペレーティング システム ID とサーバ ID の競合の解決方法に関するポリシー全体の設定を構成できます。加えて、ホスト入力ソースと NetFlow 対応デバイスを追加して、他のソースからのデータのインポートを許可できます。

検出イベントとユーザ活動イベントのデータベース イベント制限はシステム ポリシーで設定されることに注意してください。詳細については、データベース イベント制限の設定（63-16 ページ）を参照してください。

高度な設定を設定するには、次の手順を実行します。

Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] の順に選択します。

[Network Discovery Policy] ページが表示されます。

ステップ 2　[Advanced] をクリックします。

[Advanced] ページが表示されます。

ステップ 3　必要に応じて詳細設定を編集します。

- 一般設定の構成（45-35 ページ）
- ID 競合解決の設定（45-35 ページ）
- 脆弱性影響評価マッピングの有効化（45-36 ページ）
- 侵害の兆候ルールの設定（45-37 ページ）
- NetFlow 対応デバイスの追加（45-38 ページ）
- データ保存の設定（45-39 ページ）
- 検出イベント ロギングの設定（45-40 ページ）
- ID ソースの追加（45-40 ページ）

ステップ 4　設定の編集が終了したら、[Save] をクリックしてポリシーを保存します。

ステップ 5　ポリシーを編集して保存したら、それを適用して更新した設定を反映させます。詳細については、ネットワーク検出ポリシーの適用（45-41 ページ）を参照してください。

一般設定の構成

ライセンス：FireSIGHT

一般設定は、システムがネットワーク マップ内の情報を更新する頻度と、検出中にサーバ バナーをキャプチャするかどうかを制御します。

Capture Banners

サーバ ベンダーとバージョン（「バナー」）をアドバタイズするネットワーク トラフィックからの見出し情報をシステムで保存させる場合、このチェック ボックスをオンにします。この情報は、収集された情報に追加のコンテキストを提供できます。サーバ詳細にアクセスすることによって、ホストに関して収集されたサーバ バナーにアクセスできます。

Update Interval

システムが情報を更新する時間間隔（ホストの IP アドレスのいずれかが最後に検出された時点、アプリケーションが使用された時点、アプリケーションのヒット数など）。デフォルト設定は 3600 秒（1 時間）です。

更新タイムアウトの時間間隔を短く設定すると、より正確な情報がホスト画面に表示されますが、より多くのネットワーク イベントが生成されることに注意してください。

一般設定を更新する方法：

Admin/Discovery Admin

ステップ 1　[General Settings] の横にある編集アイコン（）をクリックします。

[General Settings] ポップアップ ウィンドウが表示されます。

ステップ 2　必要に応じて設定を更新します。

ステップ 3　[Save] をクリックして一般設定を保存し、ネットワーク検出ポリシーの [Advanced] タブに戻ります。

変更を反映させるためにネットワーク検出ポリシーを適用する必要があります。詳細については、ネットワーク検出ポリシーの適用（45-41 ページ）を参照してください。

ID 競合解決の設定

ライセンス：FireSIGHT

システムは、オペレーティング システムとサーバのフィンガープリントとトラフィック内のパターンを照合することによって、特定のホスト上で実行しているオペレーティング システムとアプリケーションを判断します。最も信頼できるオペレーティング システムとサーバの ID 情報を提供するために、システムは複数のソースからのフィンガープリント情報を照合します。

システムは、すべてのパッシブ データを使用して、オペレーティング システム ID を抽出し、信頼値を割り当てます。最新の ID とシステムが最新の ID を選択する方法の詳細については、ネットワーク マップの強化（46-4 ページ）を参照してください。

デフォルトでは、ID 競合が存在しなければ、スキャナまたはサード パーティ アプリケーションによって追加された ID データで、FireSIGHT システム によって検出された ID データが上書きされます。[Identity Sources] 設定を使用して、スキャナとサードパーティ アプリケーションのフィンガープリント ソースをプライオリティでランク付けできます。システムはソースごとに 1 つずつの ID を保持しますが、プライオリティが最も高いサードパーティ アプリケーションま

たはスキャナ ソースからのデータのみが最新の ID として使用されます。ただし、プライオリティに関係なく、ユーザ入力データによって、スキャナとサードパーティ アプリケーションのデータが上書きされることに注意してください。

ID 競合は、[Identity Sources] 設定に列挙されたアクティブなスキャナ ソースまたはサードパーティ アプリケーション ソースと FireSIGHT システム ユーザのどちらかから取得された既存の ID と競合する ID をシステムが検出した場合に発生します。デフォルトでは、ID 競合は自動的に解決されないため、ホスト プロファイルを通して、または、ホストをスキャンし直すか新しい ID データを追加し直してパッシブ ID を上書きすることにより、解決する必要があります。ただし、パッシブ ID を維持しつつ常に自動的に競合を解決するようにシステムを設定することも、アクティブ ID を維持しつつ常に競合を解決するようにシステムを設定することもできます。

Generate Identity Conflict Event

ネットワーク マップ内のホストで ID 競合が発生したときにイベントを生成する場合に、このオプションを有効にします。

Automatically Resolve Conflicts

次の選択肢があります。

- ID 競合の手動競合解決を強制するには、[Automatically Resolve Conflicts] ドロップダウンリストから [Disabled] を選択します。
- ID 競合が発生したときにパッシブ フィンガープリントを使用するには、[Automatically Resolve Conflicts] ドロップダウンリストから [Identity] を選択します。
- ID 競合が発生したときにプライオリティが最も高いアクティブ ソースからの最新の ID を使用するには、[Automatically Resolve Conflicts] ドロップダウンリストから [Keep Active] を選択します。

ID 競合解決設定を更新する方法:

Admin/Discovery Admin

ステップ 1　[Identity Conflict Settings] の横にある編集アイコン( )をクリックします。

[Edit Identity Conflict Settings] ポップアップ ウィンドウが表示されます。

ステップ 2　必要に応じて設定を更新します。

ステップ 3　[Save] をクリックして ID 競合設定を保存し、ネットワーク検出ポリシーの [Advanced] タブに戻ります。

変更を反映させるためにネットワーク検出ポリシーを適用する必要があります。詳細については、ネットワーク検出ポリシーの適用(45-41 ページ)を参照してください。

脆弱性影響評価マッピングの有効化

ライセンス: FireSIGHT

FireSIGHT システムで侵入イベントとの影響相関を実行する方法を設定できます。オプションは次のとおりです。

- システム ベースの脆弱性情報を使用して影響相関を実行する場合は、[Use Network Discovery Vulnerability Mappings] をオンにします。

- サードパーティの脆弱性参照を使用して影響相関を実行する場合は、[Use Third-Party Vulnerability Mappings] をオンにします。詳細については、サードパーティの脆弱性のマッピング（46-36 ページ）または『*FireSIGHT System Host Input API Guide*』を参照してください。

チェック ボックスのどちらかまたは両方を選択できます。システムが侵入イベントを生成し、選択された脆弱性マッピング セット内の脆弱性のあるサーバまたはオペレーティング システムがそのイベントに関係するホストに含まれている場合、侵入イベントは脆弱（レベル 1：赤）影響アイコンでマークされます。ベンダーまたはバージョン情報のないサーバの場合は、システム ポリシーで脆弱性マッピングを設定する必要があることに注意してください。詳細については、サーバの脆弱性のマッピング（63-32 ページ）を参照してください。

両方のチェック ボックスをオフにした場合は、侵入イベントが脆弱（レベル 1：赤）影響アイコンでマーク**されません**。詳細については、影響レベルを使用してイベントを評価する（41-39 ページ）を参照してください。

脆弱性設定を更新する方法：

Admin/Discovery Admin

ステップ 1　[Vulnerabilities to use for Impact Assessment] の横にある編集アイコン（  ）をクリックします。

[Edit Vulnerability Settings] ポップアップ ウィンドウが表示されます。

ステップ 2　必要に応じて設定を更新します。

ステップ 3　[Save] をクリックして脆弱性設定を保存し、ネットワーク検出ポリシーの [Advanced] タブに戻ります。

変更を反映させるためにネットワーク検出ポリシーを適用する必要があります。詳細については、ネットワーク検出ポリシーの適用（45-41 ページ）を参照してください。

侵害の兆候ルールの設定

ライセンス： FireSIGHT

システムで侵害の兆候（IOC）を検出してタグを付けるには、まず、検出ポリシーで 1 つ以上の IOC ルールをアクティブにする必要があります。IOC ルールのそれぞれが IOC タグの 1 つのタイプに対応します。すべての IOC ルールはCiscoが事前定義しています。オリジナル ルールを作成することはできません。ネットワークや組織のニーズに合わせて、一部またはすべてのルールを有効にすることができます。たとえば、Microsoft Excel などのソフトウェアを使用しているホストが絶対に監視対象ネットワーク上に出現しない場合は、Excel ベースの脅威に関係する IOC タグを有効にしないようにできます。IOC 機能の詳細については、侵害の兆候について（45-22 ページ）を参照してください。

また、有効にした侵入防御やマルウェア防御などの IOC ルールに関連付けられた FireSIGHT システム機能を有効にする必要もあります。ルールに関連した機能が有効になっていない場合は、関連データが収集されず、ルールをトリガーできません。IOC ルールのタイプと関連機能の詳細については、侵害の兆候タイプについて（45-22 ページ）を参照してください。

検出ポリシーで侵害の兆候ルールを設定する方法：

Admin/Discovery Admin

ステップ 1　[Indications of Compromise Settings] の横にある編集アイコン（  ）をクリックします。

[Edit Indications of Compromise Settings] ポップアップ ウィンドウが表示されます。

ステップ 2　IOC 機能全体のオンとオフを切り替えるには、[Enable IOC] の横にあるスライダをクリックします。

ステップ 3　個別の IOC ルールを有効または無効にするには、ルールの [Enabled] 列のスライダをクリックします。

ステップ 4　[Save] をクリックして、IOC ルール設定を保存し、検出ポリシーの [Advanced] タブに戻ります。

変更が保存されます。

変更を反映させるためにネットワーク検出ポリシーを適用する必要があります。詳細については、ネットワーク検出ポリシーの適用（45-41 ページ）を参照してください。

NetFlow 対応デバイスの追加

ライセンス：FireSIGHT

NetFlow 対応デバイス上で NetFlow 機能を有効にした場合は、そのデバイスからエクスポートされた接続データを使用して、Cisco デバイスによって収集された接続データを補完することができます。

NetFlow 対応デバイスを検出ルールで使用するには、そのデバイスを設定（NetFlow データの分析準備（45-21 ページ）を参照）してから、ネットワーク検出ポリシーに追加する必要があります。

FireSIGHT システムで NetFlow データを使用する方法については、その他の前提条件に関する情報も含め、NetFlow について（45-18 ページ）を参照してください。

接続データ収集用の NetFlow 対応デバイスを追加するには、次の手順を実行します。

Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] の順に選択します。

[Network Discovery Policy] ページが表示されます。

ステップ 2　[Advanced] をクリックします。

[Advanced] ページが表示されます。

ステップ 3　NetFlow デバイスの横にある追加アイコン（  ）をクリックします。

[Add NetFlow Device] ポップアップ ウィンドウが表示されます。

ステップ 4　[IP Address] フィールドに、接続データを収集するために使用する NetFlow 対応デバイスの IP アドレスを入力します。

ステップ 5　さらに NetFlow 対応デバイスを追加するには、ステップ 3 と 4 を繰り返します。

ヒント　NetFlow 対応デバイスを削除するには、削除するデバイスの横にある削除アイコン（  ）をクリックします。検出ルールで NetFlow 対応デバイスを使用する場合は、先にルールを削除しないと、[Advanced] ページからデバイスを削除できないことに注意してください。詳細については、検出ルールの操作（45-26 ページ）を参照してください。

ステップ 6　[Save] をクリックします。

デバイスが NetFlow 対応デバイスのリストに表示されます。

変更を反映させるためにネットワーク検出ポリシーを適用する必要があります。詳細については、ネットワーク検出ポリシーの適用（45-41 ページ）を参照してください。

データ保存の設定

ライセンス：FireSIGHT

データ保存設定によってデータベースに保存されるデータの種類が制御されるため、FireSIGHT システムで使用可能なデータが決まります。この設定は、データがネットワーク マップに保存される期間も制御します。

次のオプションがネットワーク検出データ保存設定を構成しています。

When Host Limit Reached

Defense Centerがホスト制限（FireSIGHT ライセンスによって決定される）に達して、ネットワーク マップがいっぱいになったときのホストの処理方法を制御できます。このオプションは、特に、スプーフィングされたホストがネットワーク マップ内の有効なホストに取って代わるのを防ぐ場合に重要です。古いホストを除外するには、[When Host Limit Reached] ドロップダウンリストから [Drop hosts] を選択します。新しいホストを除外するには、[When Host Limit Reached] ドロップダウンリストから [Don't insert new hosts] を選択します。詳細については、FireSIGHTホストおよびユーザ ライセンスの制限について（65-9 ページ）を参照してください。

Host Timeout

システムが、非アクティブであるという理由でネットワーク マップからホストを除外するまでの分単位の時間。デフォルト設定は 10080 分（7 日）です。ホスト IP アドレスと MAC アドレスは個別にタイムアウトすることができますが、関連するアドレスのすべてがタイムアウトするまで、ホストはネットワーク マップから削除されません。

ホストの早期タイムアウトを避けるために、ホストのタイムアウト値がネットワーク検出ポリシー内の更新間隔より長いことを確認します。更新間隔の詳細については、一般設定の構成（45-35 ページ）を参照してください。

Server Timeout

システムが、非アクティブであるという理由でネットワーク マップからサーバを除外するまでの分単位の時間。デフォルト設定は 10080 分（7 日）です。

サーバの早期タイムアウトを避けるために、サーバのタイムアウト値がネットワーク検出ポリシー内の更新間隔より長いことを確認します。詳細については、一般設定の構成（45-35 ページ）を参照してください。

Client Application Timeout

システムが、非アクティブであるという理由でネットワーク マップからクライアントを除外するまでの分単位の時間。デフォルト設定は 10080 分（7 日）です。

クライアントのタイムアウト値がネットワーク検出ポリシー内の更新間隔より長いことを確認する必要があります。詳細については、一般設定の構成（45-35 ページ）を参照してください。

データ保存設定を更新する方法：

Admin/Discovery Admin

ステップ 1　[Data Storage Settings] の横にある編集アイコン（  ）をクリックします。

[Data Storage Settings] ポップアップ ウィンドウが表示されます。

ステップ 2　必要に応じて設定を更新します。

ステップ 3　[Save] をクリックしてデータ保存設定を保存し、ネットワーク検出ポリシーの [Advanced] タブに戻ります。

変更を反映させるためにネットワーク検出ポリシーを適用する必要があります。詳細については、ネットワーク検出ポリシーの適用（45-41 ページ）を参照してください。

検出イベント ロギングの設定

ライセンス： FireSIGHT

イベント ロギング設定は、検出イベントとホスト入力イベントを記録するかどうかを制御します。イベントを記録しない場合は、イベント ビューで検索することも、相関ルールをトリガーするために使用することもできません。

イベント ロギング設定を構成する方法：

Admin/Discovery Admin

ステップ 1　[Event Logging Settings] の横にある編集アイコン（  ）をクリックします。

[Event Logging Settings] ポップアップ ウィンドウが表示されます。

ステップ 2　データベースに記録する検出イベント タイプとホスト入力イベント タイプの横にあるチェック ボックスをオンまたはオフにします。各イベント タイプに関する情報については、ディスカバリ イベントのタイプについて（50-10 ページ）とホスト入力イベントのタイプについて（50-14 ページ）を参照してください。

ステップ 3　[Save] をクリックしてイベント ロギング設定を保存し、ネットワーク検出ポリシーの [Advanced] タブに戻ります。

変更を反映させるためにネットワーク検出ポリシーを適用する必要があります。詳細については、ネットワーク検出ポリシーの適用（45-41 ページ）を参照してください。

ID ソースの追加

ライセンス： FireSIGHT

このページで新しいアクティブ ソースを追加することも、既存のソースのプライオリティまたはタイムアウト設定を変更することもできます。このページにスキャナを追加しても、Nmap スキャナ用の完全統合機能は追加されませんが、インポートされたサードパーティ アプリケーションまたはスキャン結果の統合が可能になることに注意してください。サードパーティ アプリケーションまたはスキャナからデータをインポートする場合は、ソースからの脆弱性とネットワーク マップ内の脆弱性がマップされているかどうかを確認するのを忘れないでください。詳細については、サードパーティの脆弱性のマッピング（46-36 ページ）を参照してください。

ID ソースを追加する方法：

Admin/Discovery Admin

ステップ 1　[OS and Server Identity Sources] の横にある編集アイコン（  ）をクリックします。

[Edit OS and Server Identity Sources] ポップアップ ウィンドウが表示されます。

ステップ 2　新しいソースを追加するには、[Add Sources] をクリックします。

[Add Identity Source] ポップアップ ウィンドウが表示されます。

ステップ 3　ソースの [Name] を入力します。

ステップ 4　[Type] ドロップダウンリストから入力ソース タイプを選択します。

- AddScanResult 機能を使用してスキャン結果をインポートする場合は、[Scanner] を選択します。
- スキャン結果をインポートしない場合は、[Application] を選択します。

ステップ 5　このソースによるネットワーク マップへの ID の追加からその ID の削除までの期間を指定するには、[Timeout] ドロップダウンリストから、[Hours]、[Days]、または [Weeks] を選択し、該当する期間を入力します。

ヒント　追加したソースを削除するには、そのソースの横にある削除アイコン（ ）をクリックします。

ステップ 6　オプションで、ソースを昇格させて、オペレーティング システム ID とアプリケーション ID よりもリストでは下にあるソースを優先的に使用するには、そのソースを選択して上矢印をクリックします。

ステップ 7　また、オプションで、ソースを降格させて、リストで上にあるソースから提供される ID が存在しない場合にのみオペレーティング システム ID とアプリケーション ID を使用するには、そのソースを選択して下矢印をクリックします。

ステップ 8　[Save] をクリックして ID ソース設定を保存し、ネットワーク検出ポリシーの [Advanced] タブに戻ります。

変更を反映させるためにネットワーク検出ポリシーを適用する必要があります。詳細については、ネットワーク検出ポリシーの適用（45-41 ページ）を参照してください。

ネットワーク検出ポリシーの適用

ライセンス： FireSIGHT

デフォルトでは、ネットワーク検出ポリシーは、Defense Centerに登録されている管理対象デバイス上のすべてのターゲット ゾーンに適用されます。ネットワーク検出ポリシーを適用すると、システムが指定内容に従ってネットワークの監視を開始します。ネットワーク検出ポリシーを変更した場合は、その変更を反映させるためにポリシーを再適用する必要があります。

ネットワーク検出ポリシーを再適用した場合：

- システムは、監視対象ネットワーク内のホストのネットワーク マップから MAC アドレス、TTL、およびホップ情報を削除してから、再検出を行います
- 影響を受ける管理対象デバイスは、まだDefense Centerに送信されていない検出データを破棄します。

ネットワーク検出ポリシーを適用するときは、Defense Center によって管理されるすべてのデバイスにアクセス コントロール ポリシーがすでに適用されていることを確認します。アクセス コントロール ポリシーが各デバイスに適用されていない場合は、ネットワーク検出ポリシーの適用が失敗します。FireSIGHT ライセンスがインストールされていないDefense Centerにはネットワーク検出ポリシーを適用できないことに注意してください。

ネットワーク検出ポリシーで使用されているネットワークまたはポート オブジェクトを変更した場合は、その変更を検出に反映させるためにポリシーを再適用する必要があります。

FireSIGHT システムの別のバージョンを実行しているスタックされたデバイス(デバイスのいずれかのアップグレードが失敗した場合など)にはネットワーク検出ポリシーを適用できないことに注意してください。

ネットワーク検出ポリシーを適用する方法:

Admin/Security Approver

ステップ 1　[Policies] > [Network Discovery] の順に選択します。

[Network Discovery Policy] ページが表示されます。

ステップ 2　[Apply] をクリックします。

Defense Center上のアクセス コントロール ポリシーの対象となるすべてのゾーンにポリシーを適用するかどうかを確認するメッセージが表示されます。

ステップ 3　[Yes] をクリックしてポリシーを適用します。

ネットワーク検出の拡張

FireSIGHT システムによって収集されるネットワーク トラフィックに関する情報は、この情報を関連付けて最も脆弱で最も重要なネットワークのホストを識別することができる場合に、最もその価値を発揮します。

たとえば、ネットワーク上に SuSE Linux のカスタマイズ バージョンを実行している複数のデバイスがある場合、システムはそのオペレーティング システムを識別することができません。そのため、脆弱性をそれらのホストにマッピングすることはできません。しかし、システムに SuSE Linux に関する脆弱性のリストがあるならば、同じオペレーティング システムを実行する他のホストを識別するために使用できるカスタム フィンガープリントを、ホストのいずれか 1 台に対して作成することができます。フィンガープリントに SuSE Linux の脆弱性リストのマッピングを含め、フィンガープリントに一致する各ホストとそのリストを関連付けることができます。

また、ホスト入力機能を使用して、ホスト データをサードパーティ システムからネットワーク マップに直接入力することもできます。ただし、サードパーティのオペレーティング システムやアプリケーション データは、脆弱性情報に自動的にマッピングされません。脆弱性を確認し、サードパーティのオペレーティング システム、サーバ、アプリケーション プロトコル データを使用してホストの影響の関連付けを実行する場合、サードパーティ システムからのベンダーとバージョンの情報を、脆弱性データベース（VDB）にリストされているベンダーとバージョンにマッピングする必要があります。また、ホストの入力データを継続的に維持する必要がある場合もあります。アプリケーション データを FireSIGHT システム ベンダーおよびバージョン定義にマッピングしたとしても、インポートされたサードパーティの脆弱性はクライアントまたは Web アプリケーションの影響評価に使用されないことに注意してください。

システムがネットワーク上のホストで実行されているアプリケーション プロトコルを識別できない場合は、システムがポートまたはパターンに基づいてアプリケーションを識別できるようにする、ユーザ定義のアプリケーション プロトコル ディテクタを作成できます。また、特定のアプリケーション ディテクタをインポートしたり、アクティブ/非アクティブにしたりすることによって、FireSIGHT システムのアプリケーション検出機能をカスタマイズすることができます。

さらに、Nmap アクティブ スキャナのスキャン結果を使用してオペレーティング システムやアプリケーション データの検出を置き換えたり、サードパーティの脆弱性で脆弱性リストを拡張したりすることもできます。システムは複数のソースからのデータを照合して、アプリケーションの ID を判別できます。この実行方法の詳細については、現在の ID について（46-5 ページ）を参照してください。アクティブ スキャンの詳細については、アクティブ スキャンの設定（47-1 ページ）を参照してください。

詳細については、次の項を参照してください。

- 検出戦略の評価（46-2 ページ）
- ネットワーク マップの強化（46-4 ページ）
- カスタム フィンガープリントの使用（46-7 ページ）

検出戦略の評価

ライセンス： FireSIGHT

システムのデフォルト検出機能に変更を加える前に、実装すべきソリューションを決定できるように、どのホストが正しく識別されないか、またその原因を分析する必要があります。以下を参考にして、ソリューションを決定します。

管理対象デバイスは正しく配置されていますか

ライセンス： FireSIGHT

ロード バランサ、プロキシ サーバ、NAT デバイスなどのネットワーク デバイスが、識別されていないホストまたは誤って識別されたホストと管理対象デバイスの間に存在する場合は、カスタム フィンガープリントを使用せずに、誤って識別されたホストの近くに管理対象デバイスを配置します。Ciscoでは、このシナリオでカスタム フィンガープリントを使用することを推奨しません。

未確認のオペレーティング システムに一意の TCP スタックがありますか

ライセンス： FireSIGHT

システムがホストを誤って識別した場合、カスタム フィンガープリントを作成してアクティブにするか、ディスカバリ データの代わりに Nmap またはホストの入力データを使用するかを決定するために、ホストが誤って識別された理由を調べる必要があります。

注意　ホストの誤認が発生した場合は、カスタム フィンガープリントを作成する前にサポート担当者にお問い合わせください。

ホストがデフォルトではシステムに検出されないオペレーティング システムを実行していて、識別している TCP スタックの特性を既存の検出されているオペレーティング システムと共有していない場合、カスタム フィンガープリントを作成する必要があります。

たとえば、システムが識別できない一意の TCP スタックを実装した Linux のカスタマイズ バージョンが存在する場合、継続的に自分でデータを更新する必要のあるスキャン結果またはサードパーティのデータを使用するのではなく、システムがホストを識別して監視を続行できるようにカスタム フィンガープリントを作成すると便利です。

オープン ソースの Linux ディストリビューションの多くは同じカーネルを使用し、システムは Linux カーネル名を使用してそれらを識別します。Red Hat Linux システム用のカスタム フィンガープリントを作成する場合、同じフィンガープリントが複数の Linux ディストリビューションに一致するために、その他のオペレーティング システム（Debian Linux、Mandrake Linux、Knoppix など）が Red Hat Linux として識別されることがあります。

フィンガープリントはすべての状況で使用できるわけではありません。たとえば、ホストの TCP スタックが別のオペレーティング システムと似るように、または同一になるように、変更が加えられる事例がありました。たとえば、Apple Mac OS X ホストが Linux 2.4 ホストと同じフィンガープリントになるように変更されると、システムはホストを Mac OS X ではなく Linux 2.4 として識別します。Mac OS X ホストのカスタム フィンガープリントを作成すると、すべての正規の Linux 2.4 ホストが誤って Mac OS X ホストとして識別される場合があります。この場合、Nmap が正しくホストを特定するならば、そのホストに対して定期的な Nmap スキャンをスケジュールできます。

ホスト入力を使用して、サードパーティ システムからデータをインポートする場合、サーバおよびアプリケーション プロトコルを説明するためにサードパーティが使用するベンダー、製品、およびバージョンの文字列を、それらの製品のCisco定義にマッピングする必要があります。詳細については、サードパーティ製品マッピングの管理（46-33 ページ）を参照してください。アプリケーション データを FireSIGHT システム ベンダーおよびバージョン定義にマッピングしたとしても、インポートされたサードパーティの脆弱性はクライアントまたは Web アプリケーションの影響評価に使用されないことに注意してください。

システムは複数のソースからのデータを照合して、オペレーティング システムまたはアプリケーションの現行 ID を判別できます。この実行方法の詳細については、現在の ID について（46-5 ページ）を参照してください。

Nmap データの場合、定期的な Nmap スキャンをスケジュールできます。ホスト入力データの場合、インポート用の Perl スクリプトまたはコマンド ライン ユーティリティを定期的に実行できます。ただし、アクティブ スキャン データおよびホスト入力データは、データ ディスカバリの頻度で更新されないことがあるので注意してください。

FireSIGHT システムはすべてのアプリケーションを識別できますか

ライセンス： FireSIGHT

ホストがシステムによって正しく識別されるものの、未確認のアプリケーションがある場合、ユーザ定義ディテクタを作成して、アプリケーションを識別するのに役立つポートおよびパターン マッチング情報をシステムに提供することができます。詳細については、ユーザ定義のアプリケーション プロトコル ディテクタの作成（46-20 ページ）を参照してください。

脆弱性を修正するパッチを適用しましたか

ライセンス： FireSIGHT

システムがホストを正しく識別するものの、適用した修正が反映されない場合、ホスト入力機能を使用してパッチ情報をインポートすることができます。パッチ情報をインポートする場合、修正名をデータベースの修正にマッピングする必要があります。詳細については、サード パーティ製品の修正のマッピング（46-35 ページ）を参照してください。

サードパーティの脆弱性を追跡しますか

ライセンス：FireSIGHT

影響の関連付けに使用するサードパーティ システムからの脆弱性情報がある場合、サーバおよびアプリケーション プロトコル用のサードパーティ脆弱性 ID をCisco データベースの脆弱性 ID にマッピングし、ホスト入力機能を使用して脆弱性をインポートすることができます。ホスト入力機能の使用方法の詳細については、『*FireSIGHT System Host Input API Guide*』を参照してください。サードパーティの脆弱性マッピングの詳細については、サードパーティの脆弱性のマッピング（46-36 ページ）を参照してください。アプリケーション データを FireSIGHT システム ベンダーおよびバージョン定義にマッピングしたとしても、インポートされたサードパーティの脆弱性はクライアントまたは Web アプリケーションの影響評価に使用されないことに注意してください。

ネットワーク マップの強化

ライセンス：FireSIGHT

FireSIGHT システムは、パッシブにトラフィックを分析することによって検出されたデータを使用してネットワーク マップを作成します。また、ホスト入力機能や Nmap スキャナなどのアクティブ ソースを介して追加されたデータも使用します。アプリケーションまたはオペレーティング システムの ID に使用するデータをシステムがどのように決定するかを理解することは、アクティブ入力ソースでシステムのパッシブ検出機能を強化する最善の方法を決定するうえで役立ちます。

詳細については、次のトピックを参照してください。

- パッシブ検出について（46-4 ページ）
- アクティブ検出について（46-5 ページ）
- 現在の ID について（46-5 ページ）
- ID の競合について（46-7 ページ）

パッシブ検出について

ライセンス：FireSIGHT

*パッシブ検出*とは、システムによってパッシブに収集されたトラフィックを分析することによって、ホストのオペレーティング システム、クライアント、およびアプリケーション情報を検出することです。システムは、ネットワーク資産を識別するのに役立つ VDB の情報を使用します。

システムがあるホストのオペレーティング システムを識別できない場合に、類似したオペレーティング システムの特性を持つ他のホストでそのオペレーティング システムを認識できるようにするため、手動でオペレーティング システムを判別し、サーバまたはクライアントのカスタム フィンガープリントを作成できます。

システムは、ホスト オペレーティング システムに関する収集されたすべてのパッシブ フィンガープリントを使用して、*派生フィンガープリント*を作成します。システムは、収集された各フィンガープリントの信頼値と ID 間の裏付けとなるフィンガープリント データの量を使用して、最も可能性の高い ID を計算する式を適用することによって、派生フィンガープリントを作成します。一般的な要素は ID 間で識別されます。

ネットワークでユーザ定義アプリケーション ディテクタを使用する場合、それらのアプリケーションを識別するために必要な情報をシステムに提供するカスタム ディテクタを作成することによって、システムのアプリケーション検出機能を強化できます。また NetFlow は、ネットワーク マップにパッシブに検出されたアプリケーション情報を追加することもできます。

システムは、データを解釈できないため、*不明*として分類されたアプリケーション プロトコルおよびオペレーティング システムのデータを使用しないことに注意してください。管理対象デバイスは ID をDefense Centerに**不明**として報告し、その ID データはフィンガープリントを取得するためには使用されません。

アクティブ検出について

ライセンス： FireSIGHT

*アクティブ検出*では、ホストのオペレーティング システムやアプリケーションの情報などアクティブ ソースによって収集されるデータをネットワーク マップに追加します。たとえば、Nmap スキャナを使用して、ネットワーク上の対象ホストをアクティブにスキャンできます。Nmap は、ホストでオペレーティング システムおよびアプリケーションを検出します。

さらに、ホスト入力機能によって、ネットワーク マップに*ホスト入力データ*をアクティブに追加することができます。ホスト入力データには 2 種類のカテゴリがあります。

- FireSIGHT システムのユーザ インターフェイスを使用して、ホストのオペレーティング システムやアプリケーションの ID を変更できます。このインターフェイスを使用して追加したデータは、*ユーザ入力データ*になります。
- コマンド ライン ユーティリティを使用してデータをインポートすることもできます。インポートしたデータは、*ホスト インポート入力データ*になります。

システムは、それぞれのアクティブ ソースに対して 1 個の ID を保持します。たとえば、Nmap スキャン インスタンスを実行すると、以前のスキャンの結果は新しいスキャン結果に置き換えられます。ただし、Nmap スキャンを実行し、それらの結果をクライアントからのデータ（コマンド ラインを使用してインポートした結果）と交換する場合、システムは Nmap の結果の ID とインポート クライアントの ID の両方を保持します。システムは、システム ポリシーで設定された優先順位を使用して、現在の ID として使用するアクティブ ID を判別します。

複数のユーザが入力したとしても、ユーザ入力は 1 ソースと見なされることに注意してください。たとえば、UserA がホスト プロファイルを使用してオペレーティング システムを設定し、UserB がホスト プロファイルを使用してその定義を変更した場合、UserB によって設定された定義が保持され、UserA によって設定された定義は破棄されます。また、ユーザ入力によって、他のアクティブ ソースすべてが上書きされ、存在する場合、現在の ID として使用されることに注意してください。

現在の ID について

ライセンス： FireSIGHT

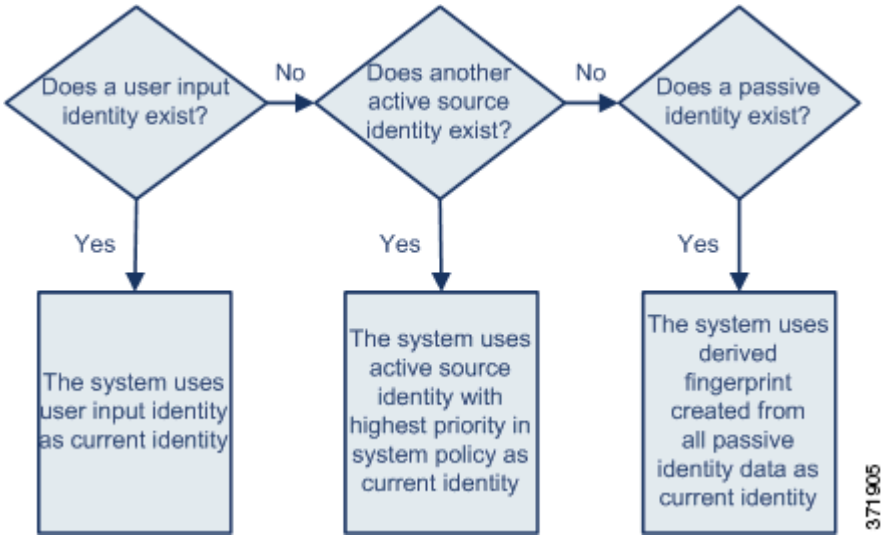
ホストのアプリケーションまたはオペレーティング システムの*現在の ID* は、ホストが最も正しい可能性が高いと認識する ID です。

システムは、以下の目的で、オペレーティング システムまたはアプリケーションの現在の ID を使用します。

- 脆弱性のホストへの割り当て
- 影響評価

- オペレーティング システムの識別、ホスト プロファイルの認定、およびコンプライアンスのホワイトリストに対して記述された相関ルールの評価
- ワークフローのホストおよびサーバのテーブル ビューでの表示
- ホスト プロファイルでの表示
- [Discovery Statistics] ページでのオペレーティング システムとアプリケーションの統計の計算

システムは、ソースの優先順位を使用して、アプリケーションまたはオペレーティング システムの現在の ID として使用するアクティブ ID を判別します。



たとえば、ユーザがホストでオペレーティング システムを Windows 2003 Server に設定した場合、Windows 2003 Server が現在の ID になります。そのホストの Windows 2003 Server の脆弱性を狙った攻撃により大きな影響力があると見なされ、ホスト プロファイルのそのホストについてリストされた脆弱性に、Windows 2003 Server の脆弱性が含められます。

データベースは、ホストのオペレーティング システムや特定のアプリケーションに関する複数のソースからの情報を保持する場合があります。

データのソースに最も高いソースの優先順位が付けられている場合に、システムはオペレーティング システムまたはアプリケーションの ID を現在の ID として扱います。使用される可能性のあるソースには、次の優先順位があります。

1. ユーザ
2. スキャナとアプリケーション（ネットワーク検出ポリシーで設定）
3. 管理対象デバイス
4. NetFlow

新しい優先度の高いアプリケーション ID は、現在のアプリケーション ID ほど詳細でない場合は、現在の ID を上書きしないことに注意してください。

また、ID の競合が発生した場合、ID の競合について（46-7 ページ）で説明されているように、競合の解決はネットワーク検出ポリシーの設定または手動解決に依存することに注意してください。

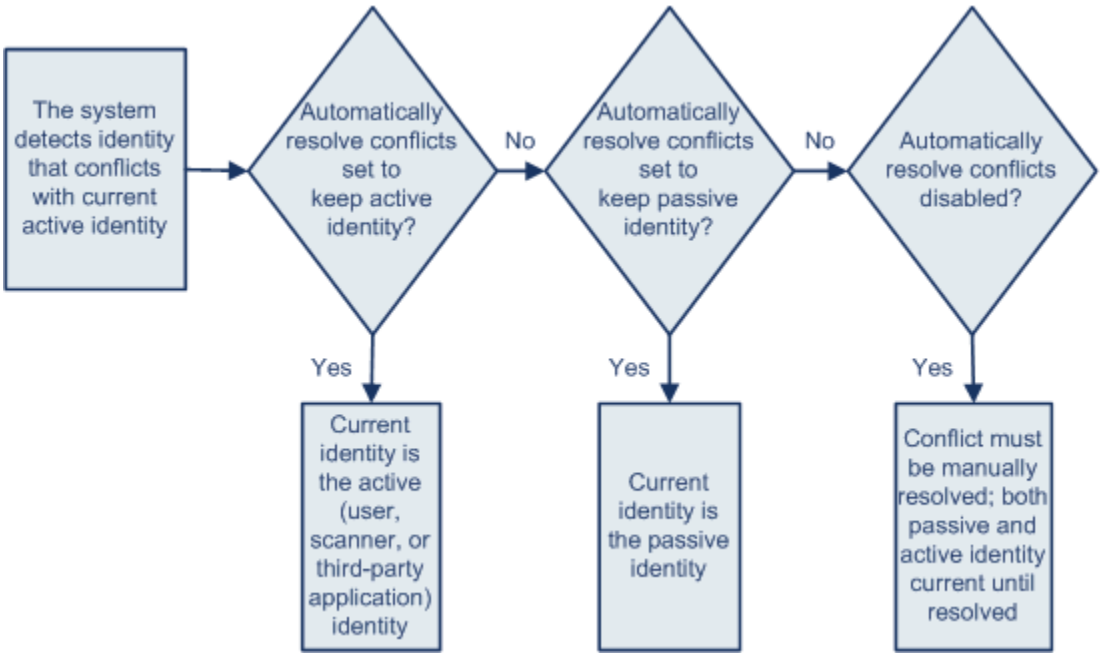
ID の競合について

ライセンス：FireSIGHT

現在のアクティブ ID および以前に報告されたパッシブ ID と競合する新しいパッシブ ID が報告されると、*ID の競合*が発生します。たとえば、オペレーティング システムの以前のパッシブ ID は Windows 2000 と報告され、Windows XP のアクティブ ID が現在の ID になります。次に、システムが Ubuntu Linux 8.04.1 の新しいパッシブ ID を検出します。Windows XP と Ubuntu Linux の ID が競合状態になります。

ホストのオペレーティング システムまたはホスト上のいずれかのアプリケーションの ID に対して ID の競合が存在する場合、システムは現在の ID として競合する両方の ID をリストし、競合が解決されるまで影響評価に両方の ID を使用します。

管理者特権を持つユーザは、パッシブ ID を常に使用するか、またはアクティブ ID を常に使用するかを選択することによって、自動的に ID の競合を解決できます。ID の競合の自動解決を無効にしない限り、ID の競合は常に自動的に解決されます。



管理者特権を持つユーザは、ID の競合が発生した場合に、イベントを生成するようにシステムを設定することもできます。そのユーザは、相関応答として Nmap スキャンを使用する相関ルールで相関ポリシーを設定できます。イベントが発生すると、Nmap はホストをスキャンして、更新されたホストのオペレーティング システムとアプリケーション データを取得します。

カスタム フィンガープリントの使用

ライセンス：FireSIGHT

FireSIGHT システムには、検出された各ホストのオペレーティング システムを識別するためにシステムが使用するオペレーティング システムの*フィンガープリント*が含まれます。しかし、オペレーティング システムに一致するフィンガープリントがないため、システムがホストのオペレーティング システムを識別できない、または誤って識別することがあります。この問題を解決

するために、不明または誤認されたオペレーティング システムに固有のオペレーティング システム特性のパターンを提供するカスタム フィンガープリントを作成し、識別用のオペレーティング システムの名前を提供することができます。

システムはオペレーティング システムのフィンガープリントから各ホストの脆弱性リストを取得するため、システムがホストのオペレーティング システムを照合できない場合、ホストの脆弱性を識別することはできません。たとえば、システムが Microsoft Windows を実行するホストを検出した場合、そのシステムには保存された Microsoft Windows の脆弱性リストが存在します。このリストは、検出した Windows オペレーティング システムに基づいて、そのホストのホスト プロファイルに追加されます。

たとえば、ネットワーク上に Microsoft Windows の新しいベータ バージョンを実行する複数のデバイスがある場合、システムはそのオペレーティング システムを識別することができません。そのため、脆弱性をそれらのホストにマッピングすることはできません。しかし、システムに Microsoft Windows に関する脆弱性のリストがあるならば、同じオペレーティング システムを実行する他のホストを識別するために使用できるカスタム フィンガープリントをいずれか 1 台のホストに対して作成できます。フィンガープリントに Microsoft Windows の脆弱性リストのマッピングを含め、フィンガープリントに一致する各ホストとそのリストを関連付けることができます。

カスタム フィンガープリントを作成するときは、オペレーティング システム情報のカスタマイズした表示を追加できます。また、システムがフィンガープリントの脆弱性リストのモデルとして使用する必要のあるオペレーティング システムのベンダー、製品名、製品バージョンを選択できます。Defense Centerは、同じオペレーティング システムを実行するすべてのホストに関するそのフィンガープリントに関連付けられた脆弱性のセットをリストします。ユーザが作成したカスタム フィンガープリントに脆弱性マッピングが 1 つも存在しない場合、システムはフィンガープリントを使用して、フィンガープリントで提供するカスタム オペレーティング システムの情報を割り当てます。すでに検出され、ネットワーク マップに現在存在しているホストからの新しいトラフィックが確認されると、システムはそのホストを新しいフィンガープリント情報で更新します。さらに、そのオペレーティング システムを実行する新しいホストの最初の検出時に、新しいフィンガープリントを使用して識別します。

ホストのフィンガープリントを作成する前に、ホストが正しく識別されない理由を特定して、カスタム フィンガープリントが実行可能なソリューションであるかどうかを判断する必要があります。詳細については、検出戦略の評価（46-2 ページ）を参照してください。

以下の 2 種類のフィンガープリントを作成できます。

- クライアントのフィンガープリント。ネットワーク上の別のホストで実行する TCP アプリケーションに接続されている場合、ホストが送信する SYN パケットに基づいてオペレーティング システムを識別します。

  ホストのクライアント フィンガープリントを取得する方法については、クライアントのフィンガープリントの作成（46-9 ページ）を参照してください。

- サーバのフィンガープリント。実行されている TCP アプリケーションへの着信接続に応答するためにホストが使用する SYN-ACK パケットに基づいてオペレーティング システムを識別します。

  ホストのサーバ フィンガープリントを取得する方法については、サーバのフィンガープリントの作成（46-11 ページ）を参照してください。

フィンガープリントを作成した後、システムがそれらをホストに関連付けるには、その前に、それらのフィンガープリントをアクティブにする必要があります。詳細については、「フィンガープリントの管理（46-14 ページ）」を参照してください。

注　クライアントとサーバの両方のフィンガープリントが同じホストに一致する場合、クライアントのフィンガープリントが使用されます。

クライアントのフィンガープリントの作成

ライセンス：FireSIGHT

クライアントのフィンガープリントは、ネットワーク上の別のホストで実行する TCP アプリケーションに接続されている場合、ホストが送信する SYN パケットに基づいてオペレーティング システムを識別します。

Defense Centerが監視対象ホストと直接通信することがない場合は、クライアントのフィンガープリントのプロパティを指定するときに、Defense Centerによって管理され、フィンガープリントを作成するホストに最も近いデバイスを指定することができます。

フィンガープリント作成プロセスを開始する前に、フィンガープリントを作成するホストに関する次の情報を取得します。

- ホストとフィンガープリントを取得するために使用するDefense Centerまたはデバイスの間のネットワーク ホップの数。（Ciscoでは、ホストが接続されている同じサブネットにDefense Centerまたはデバイスを直接接続することを強く推奨します。）
- ホストが存在するネットワークに接続されているネットワーク インターフェイス（Defense Centerまたはデバイス上）。
- ホストの実際のオペレーティング システム ベンダー、製品、バージョン。
- クライアント トラフィックを生成するためのホストへのアクセス。

ホストのクライアント フィンガープリントを取得する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] を選択し、[Custom Operating Systems] をクリックします。

[Custom Fingerprint] ページが表示されます。

ステップ 2　[Create Custom Fingerprint] をクリックします。

[Create Custom Fingerprint] ページが表示されます。

ステップ 3　[Device] ドロップダウン リストから、フィンガープリントを収集するために使用するDefense Centerまたはデバイスを選択します。

ステップ 4　[Fingerprint Name] フィールドに、フィンガープリントの識別名を入力します。

ステップ 5　[Fingerprint Description] フィールドに、フィンガープリントの説明を入力します。

ステップ 6　[Fingerprint Type] リストから、[Client] を選択します。

ステップ 7　[Target IP Address] フィールドで、フィンガープリントを作成するホストの IP アドレスを入力します。フィンガープリントは、ホストに他の IP アドレスが存在していても、ユーザが指定したホスト IP アドレスから送受信されるトラフィックのみに基づくことに注意してください。

注意　管理対象デバイスおよびDefense Centerでの IPv6 の有効化の詳細については、管理インターフェイスの構成（64-9 ページ）を参照してください。

ステップ 8　[Target Distance] フィールドで、ホストとステップ 3 で選択したデバイスの間のネットワーク ホップ数を入力します。

注意　これは、ホストへの実際の物理ネットワーク ホップ数である必要があります。システムによって検出されるホップ数と同じになる場合も、同じにならない場合もあります。

ステップ 9　[Interface] リストから、ホストが存在するネットワーク セグメントに接続されているネットワーク インターフェイスを選択します。

注意　Ciscoでは、いくつかの理由でフィンガープリントの作成に管理対象デバイスのセンシング インターフェイスを使用**しない**ことを推奨します。まず、フィンガープリントは、センシング インターフェイスが SPAN ポート上にあると機能しません。また、デバイスでセンシング インターフェイスを使用する場合、デバイスはフィンガープリントを収集している間、ネットワークの監視を停止します。ただし、フィンガープリントの収集を実行するために、管理インターフェイスまたはその他の使用可能なネットワーク インターフェイスを使用できます。どのインターフェイスがデバイスのセンシング インターフェイスであるかがわからない場合は、フィンガープリントの作成に使用している特定のモデルの *インストレーション ガイド* を参照してください。

ステップ 10　フィンガープリントを作成したホストのホスト プロファイルのカスタム情報を表示する場合（またはフィンガープリントを作成するホストが [OS Vulnerability Mappings] セクションに存在しない場合）、[Custom OS Display] セクションの [Use Custom OS Display] を選択し、以下のホスト プロファイルに表示する値を指定します。

- [Vendor String] フィールドに、オペレーティング システムのベンダー名を入力します。たとえば、Microsoft Windows のベンダーは「Microsoft」になります。
- [Product String] フィールドに、オペレーティング システムの製品名を入力します。たとえば、Microsoft Windows 2000 の製品名は「Windows」になります。
- [Version String] フィールドに、オペレーティング システムのバージョン番号を入力します。たとえば、Microsoft Windows 2000 のバージョン番号は「2000」になります。

ステップ 11　[OS Vulnerability Mappings] セクションで、脆弱性マッピングに使用するオペレーティング システム、製品、およびバージョンを選択します。

たとえば、カスタム フィンガープリントで Redhat Linux 9 の脆弱性リストを一致するホストに割り当てる場合、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、メジャー バージョンとして [9] を選択します。

ヒント　フィンガープリントを作成するとき、フィンガープリントに単一の脆弱性マッピングを割り当てます。フィンガープリントを作成してアクティブにした後、オペレーティング システムのその他のバージョンに関する別個の脆弱性マッピングを追加できます。詳細については、「アクティブなフィンガープリントの編集（46-17 ページ）」を参照してください。

フィンガープリントを使用して一致するホストの脆弱性を識別する場合、またはオペレーティング システムのカスタム表示情報を割り当てない場合、このセクションでベンダーと製品名を指定する必要があります。オペレーティング システムのすべてのバージョンの脆弱性をマッピングするには、ベンダーおよび製品名のみを指定します。たとえば、Palm OS のすべてのバージョンを追加するには、[Vendor] リストから [PalmSource, Inc.]、[Product] リストから [Palm OS] を選択し、その他のすべてのリストはデフォルトの設定のままにします。

注　[Major Version]、[Minor Version]、[Revision Version]、[Build]、[Patch]、および [Extension] ドロップダウン リストのオプションの中には、選択したオペレーティング システムに該当しないものもあります。また、フィンガープリントを作成するオペレーティング システムに一致するリストに表示される定義がない場合は、それらの値を空のままにすることができます。フィンガープリントで OS の脆弱性マッピングを作成しない場合、システムはそのフィンガープリントを使用して、脆弱性リストをフィンガープリントによって識別されるホストに割り当てることはできないことに注意してください。

ステップ 12　[Create] をクリックします。

[Custom Fingerprint] ステータス ページが再表示されます。当該のホストからデータを受信するまで、ステータス ページは 10 秒ごとに更新されます。

ヒント　[Create] をクリックすると、ステータスには [New] が一時的に表示され、すぐに [Pending] に切り替わります。このステータスは、トラフィックがフィンガープリントで確認されるまで継続します。確認されたら、ステータスは [Ready] に切り替わります。

ステップ 13　ターゲット IP アドレスとして指定した IP アドレスを使用して、フィンガープリントを作成しようとしているホストにアクセスし、アプライアンスへの TCP 接続を開始します。

たとえば、フィンガープリントを作成しようとしているホストからDefense Centerの Web インターフェイスに、または SSH でホストからDefense Centerにアクセスします。SSH を使用する場合、次のコマンドを使用します。

```
ssh -b localIPv6address DCmanagementIPv6address
```

ここで、*localIPv6address* は、現在ホストに割り当てられているステップ 7 で指定した IPv6 アドレスです。*DCmanagementIPv6address* は、Defense Centerの管理 IPv6 アドレスです。

これで、[Custom Fingerprint] ページが [Ready] ステータスでリロードされるはずです。

注　正確なフィンガープリントを作成するためには、トラフィックがフィンガープリントを収集するアプライアンスで認識される**必要**があります。スイッチを介して接続している場合は、アプライアンス以外のシステムへのトラフィックはシステムによって認識されない場合があります。

ステップ 14　フィンガープリントが作成された後、Defense Centerがそのフィンガープリントを使用してホストを識別するには、それをアクティブにする必要があります。詳細については、「フィンガープリントの管理（46-14 ページ）」を参照してください。

サーバのフィンガープリントの作成

ライセンス： FireSIGHT

サーバのフィンガープリントは、実行されている TCP アプリケーションへの着信接続に応答するためにホストが使用する SYN-ACK パケットに基づいてオペレーティング システムを識別します。開始する前に、フィンガープリントを作成するホストに関する次の情報を取得します。

- ホストとフィンガープリントを取得するために使用するアプライアンスの間のネットワーク ホップの数。Ciscoでは、ホストが接続されている同じサブネットにアプライアンスの使用されていないインターフェイスを直接接続することを強く推奨します。
- ホストが存在するネットワークに接続されているネットワーク インターフェイス（アプライアンス上）。
- ホストの実際のオペレーティング システム ベンダー、製品、バージョン。
- 現在使用されておらず、ホストが存在するネットワーク上で許可されている IP アドレス。

ヒント　Defense Centerが監視対象ホストと直接通信することがない場合は、サーバのフィンガープリントのプロパティを指定するときに、フィンガープリントを作成するホストに最も近い管理対象デバイスを指定することができます。

ホストのサーバ フィンガープリントを取得する方法:

アクセス: Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] を選択し、[Custom Operating Systems] をクリックします。

[Custom Fingerprint] ページが表示されます。

ステップ 2　[Create Custom Fingerprint] をクリックします。

[Create Custom Fingerprint] ページが表示されます。

ステップ 3　[Device] リストから、フィンガープリントを収集するために使用するDefense Centerまたは管理対象デバイスを選択します。

ステップ 4　[Fingerprint Name] フィールドに、フィンガープリントの識別名を入力します。

ステップ 5　[Fingerprint Description] フィールドに、フィンガープリントの説明を入力します。

ステップ 6　[Fingerprint Type] リストから、[Server] を選択します。

サーバのフィンガープリントのオプションが表示されます。

ステップ 7　[Target IP Address] フィールドで、フィンガープリントを作成するホストの IP アドレスを入力します。フィンガープリントは、ホストに他の IP アドレスが存在していても、ユーザが指定したホスト IP アドレスから送受信されるトラフィックのみに基づくことに注意してください。

注意　FireSIGHT システムのバージョン 5.2 以降を実行するアプライアンスでのみ IPv6 フィンガープリントをキャプチャできます。

ステップ 8　[Target Distance] フィールドで、ホストとステップ 3 で選択したデバイスの間のネットワーク ホップ数を入力します。

注意　これは、ホストへの実際の物理ネットワーク ホップ数である必要があります。システムによって検出されるホップ数と同じになる場合も、同じにならない場合もあります。

ステップ 9　[Interface] リストから、ホストが存在するネットワーク セグメントに接続されているネットワーク インターフェイスを選択します。

注意　Ciscoでは、いくつかの理由でフィンガープリントの作成に管理対象デバイスのセンシング インターフェイスを使用**しない**ことを推奨します。まず、フィンガープリントは、センシング インターフェイスが SPAN ポート上にあると機能しません。また、デバイスでセンシング インターフェイスを使用する場合、デバイスはフィンガープリントを収集している間、ネットワークの監視を停止します。ただし、フィンガープリントの収集を実行するために、管理インターフェイスまたはその他の使用可能なネットワーク インターフェイスを使用できます。どのインターフェイスがデバイスのセンシング インターフェイスであるかがわからない場合は、フィンガープリントの作成に使用している特定のモデルの *インストレーション ガイド*を参照してください。

ステップ 10　[Get Active Ports] をクリックします。

システムがホストでオープン ポートを検出した場合は、ドロップダウン リストに表示されます。

ステップ 11　[Server Port] フィールドに、フィンガープリントを収集するように選択したデバイスが通信を開始するポートを入力します。または、[Get Active Ports] ドロップダウン リストからポートを選択します。

ホストでオープンしていると判明しているすべてのサーバ ポートを使用できます（たとえば、ホストで Web サーバを実行している場合、80）。

ステップ 12　[Target IP Address] フィールドで、ホストとの通信を試行するために使用する IP アドレスを入力します。

ネットワークでの使用が許可されているものの、現在使用されていない送信元 IP アドレス（たとえば、現在使用されていない DHCP プール アドレス）を使用する必要があります。これにより、フィンガープリントを作成している間に、別のホストをオフラインで一時的にノックすることを防ぎます。

また、フィンガープリントを作成している間、ネットワーク検出ポリシーでのモニタリングからその IP アドレスを除外する必要があります。そうしないと、ネットワーク マップおよびディスカバリ イベント ビューに、その IP アドレスによって表されるホストに関する不正確な情報が混在することになります。詳細については、検出データ収集について（45-1 ページ）を参照してください。

ステップ 13　[Source Subnet Mask] フィールドでは、ユーザが使用している IP アドレスのサブネット マスクを入力します。

ステップ 14　[Source Gateway] フィールドが表示されたら、ホストへのルートを確立するために使用するデフォルトのゲートウェイ IP アドレスを入力します。

ターゲットの距離（ホップ数）が 1 以上であり、管理インターフェイス以外のインターフェイスを使用してホストが存在するネットワークに接続している場合に、[Source Gateway] フィールドが表示されます。

ステップ 15　フィンガープリントを作成したホストのホスト プロファイルのカスタム情報を表示する場合、または使用するフィンガープリントの名前が [OS Definition] セクションに存在しない場合、[Custom OS Display] セクションの [Use Custom OS Display] を選択します。

以下のように、ホスト プロファイルで表示する値を入力します。

- [Vendor String] フィールドに、オペレーティング システムのベンダー名を入力します。たとえば、Microsoft Windows のベンダーは「Microsoft」になります。
- [Product String] フィールドに、オペレーティング システムの製品名を入力します。たとえば、Microsoft Windows 2000 の製品名は「Windows」になります。
- [Version String] フィールドに、オペレーティング システムのバージョン番号を入力します。たとえば、Microsoft Windows 2000 のバージョン番号は「2000」になります。

ステップ 16　[OS Vulnerability Mappings] セクションで、脆弱性マッピングに使用するオペレーティング システム、製品、およびバージョンを選択します。たとえば、カスタム フィンガープリントで Redhat Linux 9 の脆弱性リストを一致するホストに割り当てる場合、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、バージョンとして [9] を選択します。

ヒント　フィンガープリントを作成するとき、フィンガープリントに単一の脆弱性マッピングを割り当てます。フィンガープリントを作成してアクティブにした後、オペレーティング システムのその他のバージョンに関する別個の脆弱性マッピングを追加できます。詳細については、「アクティブなフィンガープリントの編集（46-17 ページ）」を参照してください。

フィンガープリントを使用して一致するホストの脆弱性を識別する場合、またはオペレーティング システムのカスタム表示情報を割り当てない場合、このセクションでベンダーと製品名を指定する必要があります。オペレーティング システムのすべてのバージョンの脆弱性をマッピ

ングするには、ベンダーおよび製品名のみを指定します。たとえば、Palm OS のすべてのバージョンを追加するには、[Vendor] リストから [PalmSource, Inc.]、[Product] リストから [Palm OS] を選択し、その他のすべてのリストはデフォルトの設定のままにします。

注　[Major Version]、[Minor Version]、[Revision Version]、[Build]、[Patch]、および [Extension] ドロップダウン リストのオプションの中には、選択したオペレーティング システムに該当しないものもあります。また、フィンガープリントを作成するオペレーティング システムに一致するリストに表示される定義がない場合は、それらの値を空のままにすることができます。フィンガープリントで OS の脆弱性マッピングを作成しない場合、システムはそのフィンガープリントを使用して、脆弱性リストをフィンガープリントによって識別されるホストに割り当てることはできないことに注意してください。

ステップ 17　[Create] をクリックします。

ステップ 18　[Custom Fingerprint] ステータス ページが表示されます。このページは 10 秒ごとにリロードされ、[Ready] ステータスでリロードされる必要があります。

注　ターゲット システムがフィンガープリント プロセス時に応答を停止した場合、ステータスにはメッセージ「`ERROR: No Response`」が示されます。このメッセージが表示された場合は、フィンガープリントを再度送信します。3 ～ 5 分間（時間はターゲット システムによって異なる場合があります）待機して、編集アイコン（  ）をクリックし、[Custom Fingerprint] ページにアクセスしてから [Create] をクリックします。

ステップ 19　フィンガープリントが作成されたら、それをアクティブにし、オプションで脆弱性マッピングを追加します。詳細については、「フィンガープリントの管理（46-14 ページ）」を参照してください。

フィンガープリントの管理

ライセンス：FireSIGHT

カスタム フィンガープリントのアクティブ化、非アクティブ化、削除、表示、および編集を実行できます。フィンガープリントを作成するとき、フィンガープリントに単一の脆弱性マッピングを割り当てます。フィンガープリントの作成の詳細については、クライアントのフィンガープリントの作成（46-9 ページ）およびサーバのフィンガープリントの作成（46-11 ページ）を参照してください。フィンガープリントを作成してアクティブにした後、フィンガープリントを編集して変更を加えたり、脆弱性マッピングを追加したりできます。

[Custom Fingerprints] ページにアクセスする方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] を選択し、[Custom Operating Systems] をクリックします。

[Custom Fingerprint] ページが表示されます。

システムがフィンガープリントを作成するデータを待機している場合、フィンガープリントが作成されるまで 10 秒ごとに自動的に更新されます。

詳細については、次の項を参照してください。

- フィンガープリントのアクティブ化（46-15 ページ）
- フィンガープリントの非アクティブ化（46-15 ページ）
- フィンガープリントの削除（46-16 ページ）
- フィンガープリントの編集（46-16 ページ）

フィンガープリントのアクティブ化

ライセンス： FireSIGHT

カスタム フィンガープリントを作成した後、システムがそのフィンガープリントを使用してホストを識別するには、その前に、それをアクティブにする必要があります。アクティブ化された新しいフィンガープリントは、以前に検出したホストの再識別および新しいホストの検出に使用されます。

フィンガープリントをアクティブにする方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] を選択し、[Custom Operating Systems] をクリックします。

[Custom Fingerprint] ページが表示されます。

ステップ 2　アクティブにするフィンガープリントの横にあるスライダをクリックします。

注　アクティブ化オプションは、作成したフィンガープリントが有効である場合に限り使用できます。スライダが使用できない場合、フィンガープリントを再作成してください。

Defense Centerは、フィンガープリントをアクティブにし、すべての管理対象デバイスに伝播します。フィンガープリントの名前の横にあるアイコンは変更され、そのフィンガープリントがアクティブであることが示されます。

フィンガープリントの非アクティブ化

ライセンス： FireSIGHT

フィンガープリントの使用を停止する場合は、それを非アクティブにすることができます。フィンガープリントを非アクティブにすると、フィンガープリントは使用できなくなりますが、システム上で維持できます。フィンガープリントを非アクティブにすると、オペレーティング システムは、フィンガープリントを使用しているホストに対して不明としてマークされます。ホストが再度検出され、別のアクティブなフィンガープリントに一致すると、ホストはそのアクティブなフィンガープリントによって識別されます。

フィンガープリントを削除すると、システムから完全に削除されます。フィンガープリントを非アクティブにした後に削除できます。

アクティブなフィンガープリントを非アクティブにする方法:

アクセス: Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] を選択し、[Custom Operating Systems] をクリックします。

[Custom Fingerprint] ページが表示されます。

ステップ 2　非アクティブにするアクティブなフィンガープリントの横にあるスライダをクリックします。

Defense Centerは、フィンガープリントを非アクティブにし、すべての管理対象デバイスにその非アクティブ化を伝播します。

フィンガープリントの削除

ライセンス: FireSIGHT

フィンガープリントを使用しなくなった場合、システムから削除できます。フィンガープリントを削除する前に、そのフィンガープリントを非アクティブにする必要があることに注意してください。

フィンガープリントを削除する方法:

アクセス: Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] を選択し、[Custom Operating Systems] をクリックします。

[Custom Fingerprint] ページが表示されます。

ステップ 2　削除するフィンガープリントがアクティブである場合、それぞれの横にあるスライダ アイコンをクリックして、そのフィンガープリントを非アクティブにします。

ステップ 3　削除するフィンガープリントの横にある削除アイコン( )をクリックします。

ステップ 4　[OK] をクリックして、フィンガープリントを削除することを確認します。

フィンガープリントが削除されます。

フィンガープリントの編集

ライセンス: FireSIGHT

フィンガープリントを作成したら、それを表示または編集できます。フィンガープリントを変更して再送信したり、その他の脆弱性マッピングを追加したりすることができます。アクティブまたは非アクティブであるかに関わらずフィンガープリントを変更できますが、フィンガープリントの状態に応じて、変更できる事柄は異なります。

フィンガープリントが*非アクティブ*である場合は、フィンガープリントのすべての要素を変更し、それらをDefense Centerに再送信できます。これには、フィンガープリントのタイプ、ターゲットの IP アドレスとポート、脆弱性マッピングなど、フィンガープリントの作成時に指定したすべてのプロパティが含まれます。非アクティブのフィンガープリントを編集および送信すると、システムに再送信されます。また、それがクライアントのフィンガープリントである場合、アクティブにする前に、アプライアンスにトラフィックを再送信する必要があります。非アクティブ

のフィンガープリントに対して選択できる脆弱性マッピングは 1 つだけであることに注意してください。フィンガープリントをアクティブにした後、追加のオペレーティング システムおよびバージョンを脆弱性リストにマッピングすることができます。

フィンガープリントがアクティブである場合、フィンガープリントの名前、説明、オペレーティング システムのカスタム表示の変更、および追加の脆弱性のフィンガープリントへのマッピングを行えます。

詳細については、次の項を参照してください。

- 非アクティブなフィンガープリントの編集（46-17 ページ）
- アクティブなフィンガープリントの編集（46-17 ページ）

非アクティブなフィンガープリントの編集

ライセンス：FireSIGHT

フィンガープリントが非アクティブである場合は、フィンガープリントのプロパティを変更し、それらをシステムに再送信できます。これには、使用するフィンガープリントのタイプ、フィンガープリントのターゲット システムなどの変更が含まれます。

非アクティブなフィンガープリントを編集する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] を選択し、[Custom Operating Systems] をクリックします。

[Custom Fingerprint] ページが表示されます。

ステップ 2　編集するフィンガープリントの横にある編集アイコン（ ）をクリックします。

[Edit Custom Fingerprint] ページが表示されます。

ステップ 3　必要に応じてフィンガープリントを変更します。

- クライアントのフィンガープリントを変更する場合、設定できるオプションの詳細については、クライアントのフィンガープリントの作成（46-9 ページ）を参照してください。
- サーバのフィンガープリントを変更する場合、設定できるオプションの詳細については、サーバのフィンガープリントの作成（46-11 ページ）を参照してください。

ステップ 4　[Save] をクリックして、フィンガープリントを再送信します。

注　クライアントのフィンガープリントを変更した場合は、ホストからフィンガープリントを収集しているアプライアンスにトラフィックを必ず送信してください。

アクティブなフィンガープリントの編集

ライセンス：FireSIGHT

フィンガープリントがアクティブな場合、その名前、説明、および表示ラベルを変更できます。また、脆弱性マッピングの追加や削除など、脆弱性マッピングを管理することができます。

アクティブなフィンガープリントを編集する方法:

アクセス: Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] を選択し、[Custom Operating Systems] をクリックします。

[Custom Fingerprint] ページが表示されます。

ステップ 2　編集するフィンガープリントの横にある編集アイコン( )をクリックします。

[Edit Custom Fingerprint Product Mappings] ページが表示されます。

ステップ 3　必要に応じて、フィンガープリントの名前、説明、およびカスタム OS 表示を変更します。

ステップ 4　脆弱性マッピングを削除する場合は、ページの [Pre-Defined OS Product Maps] セクションのマッピングの横にある [Delete] をクリックします。

ステップ 5　脆弱性マッピングにその他のオペレーティング システムを追加する場合は、[Product] を選択し(該当する場合は [Major Version]、[Minor Version]、[Revision Version]、[Build]、[Patch]、および [Extension] も選択します)、[Add OS Definition] をクリックします。

脆弱性マッピングが、[Pre-Defined OS Product Maps] リストに追加されます。

ステップ 6　[Save] をクリックして変更を保存します。

アプリケーション ディテクタの使用

ライセンス: FireSIGHT

FireSIGHT システムが IP トラフィックを分析する場合、ネットワークで一般的に使用されるアプリケーションを識別するためにディテクタを使用します。[Detectors] ページ([Policies] > [Application Detectors])を使用して、FireSIGHT システムの検出機能をカスタマイズします。

このページには、各ディテクタに関する次のような情報が表示されます。

- ディテクタの名前
- ディテクタが検査するトラフィックのプロトコル(TCP、UDP、またはその両方)
- ディテクタのタイプがアプリケーション プロトコル、クライアント、Web アプリケーション、または内部ディテクタのいずれであるか
- ポートベースのアプリケーション ディテクタの場合、アプリケーション トラフィックによって使用されるポート
- 検出されたアプリケーションに関する詳細(ディテクタによって検出されたアプリケーションに関連付けられた名前、説明、リスク、ビジネスとの関連性、タグ、およびカテゴリ)
- ディテクタの状態(アクティブまたは非アクティブ)

システムは、アプリケーション トラフィックを分析するために、アクティブなディテクタのみを使用します。

リストされたディテクタに異なるプロパティが存在することがあります。たとえば、一部のディテクタの設定を表示できますが、その他のディテクタの設定は表示できません。同様に、一部のディテクタを削除できますが、その他のディテクタは削除できません。これは、次のセクションで説明しているように、Ciscoが提供するディテクタに複数の異なるタイプが存在するためです。

Ciscoが提供する内部ディテクタ

*内部ディテクタ*は、FireSIGHT システムへの更新によってのみ提供されるアプリケーション ディテクタです。内部ディテクタは、そのディテクタに応じて、クライアント、Web アプリケーション、またはアプリケーション プロトコルのトラフィックを検出します。しかし、それらが組み込みディテクタであり、非アクティブにすることができないという理由で、他のタイプのいずれでもなく、内部ディテクタとして分類されます。

内部ディテクタは常にアクティブです。それらを非アクティブにすることも、削除することも、または別の方法で設定することもできません。内部ディテクタの例には、組み込み Amazon ディテクタや組み込み AppleTalk ディテクタがあります。

Ciscoが提供するクライアント ディテクタ

Ciscoが提供する *クライアント ディテクタ*は、クライアント トラフィックを検出し、VDB アップデートを介して提供されますが、FireSIGHT システムへの更新によっても提供されることがあります。これらのディテクタは、インポート可能なディテクタとしてCisco プロフェッショナル サービスによって提供されることもあります。

組織の必要に応じてクライアント ディテクタをアクティブまたは非アクティブにできます。VDB アップデートも、クライアント ディテクタをアクティブまたは非アクティブにすることがあります。インポートする場合のみ、クライアント ディテクタをエクスポートできます。

クライアント ディテクタの例には、Google Earth ディテクタや Immunet ディテクタがあります。

Ciscoが提供する Web アプリケーション ディテクタ

Ciscoが提供する *Web アプリケーション ディテクタ*は、HTTP トラフィックのペイロードで Web アプリケーションを検出し、VDB アップデートを介して提供されますが、FireSIGHT システムへの更新によっても提供されることがあります。

組織の必要に応じて Web アプリケーション ディテクタをアクティブまたは非アクティブにできます。VDB アップデートは、Web アプリケーション ディテクタをアクティブまたは非アクティブにすることがあります。Web アプリケーション ディテクタの例には、Blackboard ディテクタや LiveJournal ディテクタがあります。

Ciscoが提供するアプリケーション プロトコル(ポート)ディテクタ

*ポートベースの アプリケーション プロトコル ディテクタ*は、Ciscoによって提供され、既知のポートのネットワーク トラフィックの検出に基づきます。これらのディテクタは、VDB アップデートを介して提供されますが、FireSIGHT システムへの更新、またはインポート可能なディテクタとしてCisco プロフェッショナル サービスによっても提供されることがあります。

組織の必要に応じてアプリケーション プロトコル ディテクタをアクティブまたは非アクティブにできます。カスタム ディテクタの基礎として使用するためにディテクタ定義を表示することもできます。VDB アップデートによって、アプリケーション プロトコル ディテクタがアクティブまたは非アクティブにされることがあります。

ポート ディテクタの例には、chargen ディテクタや finger ディテクタがあります。

Ciscoが提供するアプリケーション プロトコル(FireSIGHT)ディテクタ

Ciscoが提供する FireSIGHT ベースのアプリケーション プロトコル ディテクタは、FireSIGHT アプリケーション フィンガープリントを使用したネットワーク トラフィックの検出に基づきます。これらのディテクタは、VDB アップデートを介して提供されますが、FireSIGHT システムへの更新によっても提供されることがあります。

組織の必要に応じてアプリケーション プロトコル ディテクタをアクティブまたは非アクティブにできます。VDB アップデートによって、Ciscoが提供するアプリケーション プロトコル ディテクタがアクティブまたは非アクティブにされることがあります。FireSIGHT ベースのアプリケーション プロトコル ディテクタの例には、Jabber ディテクタや Steam ディテクタがあります。

アプリケーション プロトコル(パターン)ディテクタ

*パターンベースのアプリケーション ディテクタ*は、ネットワーク トラフィックからのパケットのパターンの検出に基づきます。これらのディテクタは、インポート可能なディテクタとしてCisco プロフェッショナル サービスによって提供されることも、ユーザが作成することもできます。これにより、FireSIGHT システム全体を更新せずに、新しいパターンベースのディテクタを用いてシステムの検出機能を強化することができます。

組織の必要に応じてアプリケーション プロトコル ディテクタをアクティブまたは非アクティブにできます。

インポートしたディテクタやユーザ定義のディテクタを完全に制御できます。つまり、これらのディテクタのアクティブ化、非アクティブ化、編集、インポート、エクスポート、および削除を実行できます。パターンベースのディテクタの例には、カスタム アプリケーションのトラフィックを検出するためにパケット見出しのパターンを使用するユーザ定義のディテクタがあります。

ディテクタ リストは、FireSIGHT システムのバージョン、インストールした VDB、およびインポートまたは作成した個々のディテクタに応じて異なる可能性があることに注意してください。各 FireSIGHT システムの更新プログラムのリリース ノートや更新されたディテクタの情報に関する各 VDB アップデートのアドバイザリを注意深く読んでください。

詳細については、以下を参照してください。

- アプリケーション検出について(45-11 ページ)
- ユーザ定義のアプリケーション プロトコル ディテクタの作成(46-20 ページ)
- ディテクタの管理(46-26 ページ)

ユーザ定義のアプリケーション プロトコル ディテクタの作成

ライセンス: FireSIGHT

ネットワークのカスタム アプリケーションを使用する場合、これらのアプリケーションを識別するために必要な情報をシステムに提供するユーザ定義のアプリケーション プロトコル ディテクタを作成できます。アプリケーション トラフィックによって使用されるポート、トラフィック内のパターン、またはポートとパターンの両方に基づいて、アプリケーション プロトコルの検出を実行できます。

たとえば、ポート 1180 を使用するカスタム アプリケーション プロトコルのトラフィックが予想される場合は、そのポートのトラフィックを検出するアプリケーション プロトコル ディテクタを作成できます。別の例として、アプリケーション プロトコルのトラフィックを格納するすべてのパケットの見出しに `ApplicationName` の文字列が含まれることを把握している場合、照合するパターンとして `ApplicationName` の ASCII 文字列を登録するディテクタを作成できます。

クライアントまたは Web アプリケーションでは**なく**、アプリケーション プロトコルに対して**のみ**ユーザ定義アプリケーション ディテクタを作成できます。それぞれの説明については、アプリケーション検出について(45-11 ページ)を参照してください。システムがサーバ トラフィックでアプリケーション プロトコルの検出および識別を開始するように、クライアント セッションにサーバからの応答パケットを含める必要があります。UDP トラフィックの場合、応答パケットの送信元がサーバとして指定されることに注意してください。

注意 新しいアプリケーション ディテクタを作成してアクティブにすると、管理対象デバイス上のトラフィック フローと処理で、短時間の一時停止が発生する場合があります。これは、いくつかのパケットが検査されずに通過する原因となる可能性があります。

ユーザ定義のアプリケーション プロトコル ディテクタでは、ポートまたはパターンのいずれかのマッチングを使用する必要があります。つまり、既存のディテクタに基づくディテクタを作成する場合であっても、いずれも使用しないディテクタは作成できません。これら両方の基準を使用するディテクタを作成することもできます。この場合、そのアプリケーション プロトコルのトラフィックを正しく識別する可能性が高くなります。

ヒント すでに別のDefense Centerにディテクタを作成している場合、そのディテクタをエクスポートして、このDefense Centerにインポートすることができます。その後、必要に応じてインポートしたディテクタを編集できます。ユーザ定義のディテクタおよびCisco プロフェッショナル サービスが提供するディテクタをエクスポートおよびインポートすることができます。ただし、Ciscoが提供するその他の種類のディテクタをエクスポートおよびインポートすることは**できません**。詳細については、設定のインポートおよびエクスポート（A-1 ページ）を参照してください。

ユーザ定義のアプリケーション プロトコル ディテクタを作成する方法：

アクセス：Admin/Discovery Admin

ステップ 1 [Policies] > [Application Detectors] を選択します。

[Detectors] ページが表示されます。

ステップ 2 [Create Detector] をクリックします。

[Create Detector] ページが表示されます。

ステップ 3 ディテクタの名前や説明など、基本的なディテクタの情報を指定します。

基本的なアプリケーション プロトコル ディテクタ情報の提供（46-22 ページ）を参照してください。

ステップ 4 オプションで、ディテクタのユーザ定義のアプリケーションを作成します。

ユーザ定義のアプリケーションの作成（46-22 ページ）を参照してください。

ステップ 5 ディテクタが検査する必要のあるトラフィックのプロトコルやトラフィックが使用するポートなど検出基準を指定します。

アプリケーション プロトコル ディテクタの検出基準の指定（46-23 ページ）を参照してください。

ステップ 6 オプションで、そのアプリケーション プロトコルのトラフィックで発生する 1 つ以上のパターンに一致するかどうかトラフィックを検査するようにディテクタを設定します。

アプリケーション プロトコル ディテクタへの検出パターンの追加（46-24 ページ）を参照してください。

ステップ 7 オプションで、1 つ以上の PCAP ファイルの内容に対して新しいディテクタをテストします。

パケット キャプチャに対するアプリケーション プロトコル ディテクタのテスト（46-25 ページ）を参照してください。

ステップ 8 [Save] をクリックします。

アプリケーション プロトコル ディテクタが保存されます。

注　アプリケーション プロトコルのトラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタをアクティブにする必要があります。詳細については、ディテクタのアクティブ化と非アクティブ化（46-30 ページ）を参照してください。アクセス コントロール ルールにアプリケーションを含めると、ディテクタは自動的にアクティブにされ、使用中は非アクティブにできないことに注意してください。

基本的なアプリケーション プロトコル ディテクタ情報の提供

ライセンス： FireSIGHT

それぞれのユーザ定義のアプリケーション プロトコル ディテクタに名前を付け、検出するアプリケーション プロトコルを識別する必要があります。オプションで、ディテクタの簡単な説明を提供できます。

ユーザが提供する情報に加えて、Defense Centerは、ディテクタがアクティブまたは非アクティブのいずれであるか、ディテクタがポート ディテクタまたはパターン ディテクタのいずれであるかを示します。ディテクタがポートとパターンによってアプリケーション プロトコルのトラフィックを識別する場合、FireSIGHT システムはそれをパターン ディテクタと見なします。

既存のディテクタを編集する場合、Defense Centerはディテクタの作成者も表示します。ユーザ定義のアプリケーション プロトコル ディテクタを作成したら、そのユーザが作成者になります。また、ディテクタをインポートまたは編集および保存した場合も作成者になります。

基本的なアプリケーション プロトコル ディテクタ情報を提供する方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Create Detector] ページの [Please enter a name] フィールドに、ディテクタの名前を入力します。

ディテクタの名前は、検査するトラフィックのプロトコル内で一意である必要があります。つまり、同じ名前で TCP ディテクタと UDP ディテクタを作成できますが、同じ名前で 2 つの TCP ディテクタを作成することはできません。

ステップ 2　検出するアプリケーション プロトコルを識別します。次の選択肢があります。

- 既存のアプリケーション プロトコルのディテクタを作成する場合（たとえば、非標準ポートで特定のアプリケーション プロトコルを検出する場合）、[Application Protocol] ドロップダウン リストからアプリケーション プロトコルを選択します。アプリケーション プロトコル ディテクタの検出基準の指定（46-23 ページ）の手順に進みます。
- カスタム アプリケーションのディテクタを作成する場合は、次の項ユーザ定義のアプリケーションの作成の手順に進みます。

ユーザ定義のアプリケーションの作成

ライセンス： FireSIGHT

ネットワークのカスタム アプリケーションを識別するユーザ定義のアプリケーションを作成することができます。そのアプリケーションを記述するカスタム カテゴリとカスタム タグを作成することもできます。ここで作成するアプリケーション、カテゴリ、およびタグは、アクセス コントロール ルールやアプリケーション フィルタ オブジェクト マネージャで使用できます。

アプリケーション プロトコル、およびそれらを説明するために使用されるカテゴリ、タグ、リスク レベル、ビジネスとの関連性など、アプリケーション検出の詳細については、アプリケーション検出について（45-11 ページ）を参照してください。

ユーザ定義のアプリケーションを作成する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Create Detector] ページで、[Add] をクリックします。

[Application Editor] ポップアップ ウィンドウが表示されます。

ステップ 2　カスタム アプリケーションの [Name] に名前を入力します。

ステップ 3　カスタム アプリケーションの [Description] に説明を入力します。

ステップ 4　[Business Relevance] を選択します。

ステップ 5　[Risk] を選択します。

ステップ 6　[Categories] の横にある [Add] をクリックしてカテゴリを追加し、新しいカテゴリの名前を入力するか、または [Categories] ドロップダウン リストから既存のカテゴリを選択します。

ステップ 7　オプションで、[Tags] の横にある [Add] をクリックしてタグを追加し、新しいタグの名前を入力するか、または [Tags] ドロップダウン リストから既存のタグを選択します。

[OK] をクリックして、[Create Detector] ページに戻ります。

ステップ 8　次のセクションアプリケーション プロトコル ディテクタの検出基準の指定の手順に進みます。

アプリケーション プロトコル ディテクタの検出基準の指定

ライセンス：FireSIGHT

ユーザ定義のアプリケーション プロトコル ディテクタを作成する場合、ディテクタが検査するトラフィックのプロトコル（TCP、UDP、またはその両方）を指定する必要があります。オプションで、トラフィックが使用するポートを指定できます。

アプリケーション プロトコル ディテクタへの検出パターンの追加（46-24 ページ）で説明されているように、ポートを指定しなかった場合は、1 つ以上のパターンに一致するかどうかトラフィックを検査するようにディテクタを設定する必要があることに注意してください。

アプリケーション プロトコル ディテクタの検出基準を指定する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Create Detector] ページで、[Protocol] ドロップダウン リストから、ディテクタが検査する必要があるトラフィックのプロトコルを選択します。

ディテクタは、TCP、UDP、または TCP と UDP のトラフィックを検査できます。

ステップ 2　オプションで、使用するポートに基づいてアプリケーション プロトコルのトラフィックを指定するには、1 から 65535 までのポートを [Port(s)] フィールドに入力します。複数のポートを使用する場合は、カンマで区切ります。

ステップ 3　次の選択肢があります。

- そのアプリケーション プロトコルのトラフィックで発生する 1 つ以上のパターンに一致するかどうかトラフィックを検査するようにアプリケーション プロトコル ディテクタを設定する場合は、次のセクションアプリケーション プロトコル ディテクタへの検出パターンの追加の手順に進みます。
- 1 つ以上の PCAP ファイルの内容に対して新しいディテクタをテストする場合は、パケット キャプチャに対するアプリケーション プロトコル ディテクタのテスト（46-25 ページ）をスキップします。
- ディテクタの作成が完了したら、[Save] をクリックします。

  アプリケーション プロトコル ディテクタが保存されます。

アプリケーション プロトコルのトラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタをアクティブにする必要があることに注意してください。詳細については、ディテクタのアクティブ化と非アクティブ化（46-30 ページ）を参照してください。

アプリケーション プロトコル ディテクタへの検出パターンの追加

ライセンス： FireSIGHT

アプリケーション プロトコルのトラフィックを格納するパケットの見出しに特定のパターン文字列が含まれていることが判明している場合、そのパターンを検索するように、ユーザ定義のアプリケーション プロトコル ディテクタを設定できます。

アプリケーション プロトコル ディテクタは、オフセットを使用して ASCII または 16 進数のパターンを検索できます。また、複数のパターンを検索するようにディテクタを設定することもできます。この場合は、アプリケーション プロトコルのトラフィックは、アプリケーション プロトコルを確実に識別するため、ディテクタのすべてのパターンとマッチングさせる必要があります。

アプリケーション プロトコル ディテクタの検出基準の指定（46-23 ページ）で説明されているように、パターンを指定しなかった場合は、1 つ以上のポートを使用するトラフィックを検査するようにディテクタを設定する必要があることに注意してください。

検出パターンをアプリケーション プロトコル ディテクタに追加する方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Create Detector] ページの [Detection Patterns] セクションで、[Add] をクリックします。

[Add Pattern] ポップアップ ウィンドウが表示されます。

ステップ 2　検出するパターンのタイプ（[Ascii] または [Hex]）を指定します。

ステップ 3　[Pattern String] フィールドに指定したタイプの文字列を入力します。

ステップ 4　オプションで、システムがパターンの検索を開始するパケットの場所（オフセットと呼ばれます）を指定します。

[Offset] フィールドにオフセット（パケット ペイロードの先頭からのバイト数）を入力します。

パケット ペイロードは 0 バイトから始まるため、パケット ペイロードの先頭から数えたバイト数から 1 を減算することでオフセットを計算します。たとえば、パケットの 5 桁目のビット パターンを検索するには、[Offset] フィールドに「4」と入力します。

ステップ 5　オプションで、さらにパターンを追加するには、手順 1 ～ 4 を繰り返します。

ヒント　パターンを削除するには、削除するパターンの横の削除アイコン（）をクリックします。

ステップ 6　次の選択肢があります。

- 1 つ以上の PCAP ファイルの内容に対して新しいディテクタをテストする場合は、次のセクションパケット キャプチャに対するアプリケーション プロトコル ディテクタのテストの手順に進みます。
- ディテクタの作成が完了したら、[Save] をクリックします。

  アプリケーション プロトコル ディテクタが保存されます。

注　アプリケーション プロトコルのトラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタをアクティブにする必要があります。詳細については、ディテクタのアクティブ化と非アクティブ化（46-30 ページ）を参照してください。

パケット キャプチャに対するアプリケーション プロトコル ディテクタのテスト

ライセンス： FireSIGHT

検出するアプリケーション プロトコルからのトラフィックを持つパケットが格納されたパケット キャプチャ（PCAP）ファイルが存在する場合、その PCAP ファイルに対してユーザ定義のアプリケーション プロトコル ディテクタをテストできます。PCAP ファイルは 32KB 以下である必要があることに注意してください。それより大きい PCAP ファイルに対してディテクタのテストを試行すると、Defense Centerは自動的にファイルを切り捨てます。

PCAP ファイルに対してアプリケーション プロトコル ディテクタをテストする方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Create Detector] ページの [Packet Captures] セクションで、[Add] をクリックします。

ポップアップ ウィンドウが表示されます。

ステップ 2　PCAP ファイルを参照し、[OK] をクリックします。

PCAP ファイルがパケット キャプチャのファイル リストに表示されます。

ステップ 3　PCAP ファイルの内容に対してディテクタをテストするには、PCAP ファイルの横にある評価アイコンをクリックします。

テストが成功したかどうかを示すメッセージが表示されます。

ステップ 4　必要に応じて手順 1 ～ 3 を繰り返し、その他の PCAP ファイルに対してディテクタをテストします。

ヒント　PCAP ファイルを削除するには、削除するファイルの横の削除アイコン（）をクリックします。

ステップ 5　ディテクタを保存するには、[Save] をクリックします。

注　アプリケーション プロトコルのトラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタをアクティブにする必要があります。詳細については、ディテクタのアクティブ化と非アクティブ化（46-30 ページ）を参照してください。

ディテクタの管理

ライセンス： FireSIGHT

[Detectors] ページでディテクタを表示および管理します。

[Detectors] ページから以下を実行できます。

- ディテクタが識別するアプリケーションの詳細の表示
- ディテクタ リストの並べ替え、フィルタリング、および参照
- Ciscoが提供する内部ディテクタのリストの表示
- Ciscoが提供するアプリケーション プロトコル ポート ディテクタのプロパティの表示、およびオプションで、変更可能なユーザ定義の新規ディテクタとしてのコピーの保存
- ユーザ定義のアプリケーション プロトコル ディテクタの作成、変更、削除、およびエクスポート
- 個別にインポートしたアプリケーション プロトコル ディテクタの削除とエクスポート
- ユーザ定義、インポート済み、またはCiscoが提供する Web アプリケーション、クライアント、およびアプリケーション プロトコルのディテクタのアクティブ化と非アクティブ化

内部またはCiscoが提供するアプリケーション プロトコル、クライアント、または Web アプリケーションのディテクタは変更および削除できないこと、また内部ディテクタを非アクティブ化できないことに注意してください。

詳細については、以下を参照してください。

- ディテクタの詳細の表示（46-26 ページ）
- ディテクタ リストの並べ替え（46-27 ページ）
- ディテクタ リストのフィルタリング（46-27 ページ）
- 他のディテクタのページへの移動（46-29 ページ）
- ディテクタのアクティブ化と非アクティブ化（46-30 ページ）
- アプリケーション ディテクタの変更（46-31 ページ）
- ディテクタの削除（46-31 ページ）

ディテクタの詳細の表示

ライセンス： FireSIGHT

アプリケーション ディテクタのリストからディテクタの詳細を表示できます。

アプリケーション ディテクタの詳細を表示する方法:

アクセス: Admin/Discovery Admin

ステップ 1　[Details] 列の情報アイコン( )をクリックします。

ディテクタに関する情報ポップアップ ウィンドウが表示されます。

リスク、ビジネスとの関連性、タグ、およびカテゴリの詳細については、アプリケーション検出について(45-11 ページ)を参照してください。

ディテクタ リストの並べ替え

ライセンス: FireSIGHT

[Detectors] ページには、デフォルトで名前のアルファベット順にディテクタがリストされます。列見出しの横にある上矢印(▲)または下矢印は、その列のその方向でページが並べ替えられていることを示します。

ディテクタを並べ替えるには:

アクセス: Admin/Discovery Admin

ステップ 1　[Detectors] ページで、該当する列見出しをクリックします。

ディテクタは、列見出しに表示される矢印によって示される方向で並べ替えられます。反対方向でソートするには、見出しを再度クリックします。

ディテクタ リストのフィルタリング

ライセンス: FireSIGHT

単一の基準または複数の基準の組み合わせによって、[Detectors] ページに表示するディテクタをフィルタリングできます。構築したフィルタは、ページの上部に表示されます。複数のフィルタグループを別個にまたは組み合わせて使用し、ディテクタのリストをフィルタリングすることができます。

名前

ユーザが入力した文字列を含む名前または説明でディテクタを検索します。文字列には任意の英数字または特殊文字を含めることができます。

Custom Filter

オブジェクト管理ページで作成したカスタム アプリケーション フィルタに一致するディテクタを検索します。詳細については、アプリケーション フィルタの操作(3-16 ページ)を参照してください。

作成者

ディテクタを作成したユーザに照らしてディテクタを検索します。次によってディテクタをフィルタリングできます。

– ディテクタを作成またはインポートした個々のユーザ

- **Cisco**。これは、個別にインポートされたアドオン ディテクタを*除く*Ciscoが提供するすべてのディテクタを表します。ディテクタをインポートした場合、そのユーザはそのディテクタの作成者になります。
- **Any User**。これは、Ciscoによって提供されたのではないすべてのディテクタを表します。

状態

状態（つまり、アクティブまたは 非アクティブ）に照らしてディテクタを検索します。詳細については、ディテクタのアクティブ化と非アクティブ化（46-30 ページ）を参照してください。

タイプ

ディテクタのタイプ（アプリケーション プロトコル、Web アプリケーション、クライアント、または 内部ディテクタ）に照らして検索します。

アプリケーション プロトコル ディテクタには、ディテクタをさらにフィルタリングするために使用できる 3 つのサブタイプがあります。

- **ポート** アプリケーション プロトコル ディテクタには、Ciscoが提供するよく知られているポート ディテクタやポートベースのユーザ定義アプリケーション ディテクタが含まれます。
- **パターン** アプリケーション プロトコル ディテクタには、パターンベースまたはポートベースとパターンベースのユーザ定義アプリケーション ディテクタが含まれます。
- **FireSIGHT** アプリケーション プロトコル ディテクタは、アクティブにしたり、非アクティブにしたりできるCiscoが提供するアプリケーション プロトコル フィンガープリント ディテクタです。

ディテクタ タイプの詳細については、アプリケーション ディテクタの使用（46-18 ページ）を参照してください。

Protocol

ディテクタが検査するトラフィック プロトコルに照らしてディテクタを検索します。ディテクタは、TCP、UDP、または TCP と UDP のトラフィックを検査できます。

カテゴリ

検出するアプリケーションに割り当てられたカテゴリに照らしてディテクタを検索します。

タグ

検出するアプリケーションに割り当てられたタグに照らしてディテクタを検索します。

リスク

検出するアプリケーションに割り当てられたリスク（Very High、High、Medium、Low、Very Low）に照らしてディテクタを検索します。

ビジネスとの関連性

検出するアプリケーションに割り当てられたビジネスとの関連性（**Very High**、**High**、**Medium**、**Low**、**Very Low**）に照らしてディテクタを検索します。

フィルタを適用する方法:

Admin/Discovery Admin

ステップ 1　[Detectors] ページで、ディテクタをフィルタリングするために使用するフィルタ グループを展開します。

ステップ 2　名前を入力するか、使用する特定のフィルタを選択します。グループ内のすべてのフィルタを選択するには、グループ名を右クリックし、[Check All] を選択します。

ステップ 3　オプションで、使用するフィルタにサブフィルタが存在する場合、さらにディテクタをフィルタリングするサブフィルタを選択します。

フィルタを削除する方法:

アクセス: Admin/Discovery Admin

ステップ 1　[Filters] フィールドにあるフィルタの名前の削除アイコン( )をクリックするか、フィルタ リストでフィルタを無効にします。グループ内のすべてのフィルタを削除するには、グループ名を右クリックし、[Uncheck All] を選択します。

フィルタが削除され、結果が更新されます。

すべてのフィルタを削除する方法:

アクセス: Admin/Discovery Admin

ステップ 1　ディテクタに適用されているフィルタ リストの横にある [Clear all] をクリックします。

他のディテクタのページへの移動

ライセンス: FireSIGHT

[Detectors] ページには、一度に 25 個のディテクタが表示されます。次の表では、ページ下部のナビゲーション リンクを使用してディテクタの追加ページの表示方法について説明します。

アクセス: Admin/Discovery Admin

表 46-1　ディテクタ ページの移動

目的	操作
次のページを表示する	右矢印アイコン( )をクリックします。
前のページを表示する	左矢印アイコン( )をクリックします。
別のページを表示する	ページ番号を入力して、Enter キーを押します。
最後のページに移動する	右端矢印アイコン( )をクリックします。
最初のページに移動する	左端矢印アイコン( )をクリックします。

ディテクタのアクティブ化と非アクティブ化

ライセンス：FireSIGHT

ネットワーク トラフィックを分析するためにディテクタを使用できるようにするには、その前に、ディテクタをアクティブにする必要があります。デフォルトでは、Ciscoが提供するすべてのディテクタはアクティブになっています。

システムの検出機能を補完するために、ポートごとに複数のアプリケーション ディテクタをアクティブにすることができます。

ポリシーのアクセス コントロール ルールにアプリケーションを含め、そのポリシーを適用するときに、そのアプリケーションに対してアクティブなディテクタがない場合、1 つ以上のディテクタが自動的にアクティブになります。同様に、適用されているポリシーのアプリケーションが使用されているときに、そのアプリケーションのアクティブなディテクタをすべて非アクティブにしようとしても、ディテクタを非アクティブにすることはできません。

注意　既存のディテクタをアクティブまたは非アクティブにすると、管理対象デバイス上のトラフィック フローと処理で、短時間の一時停止が発生する場合があります。これは、いくつかのパケットが検査されずに通過する原因となる可能性があります。

ヒント　パフォーマンスを向上させるために、使用する予定のないアプリケーション プロトコル、クライアント、または Web アプリケーションのディテクタはすべて非アクティブにします。

ディテクタをアクティブまたは非アクティブにする方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Application Detectors] を選択します。

[Detectors] ページが表示されます。

ステップ 2　アクティブまたは非アクティブにするディテクタを見つけます。

アクティブまたは非アクティブにするディテクタが最初のページにない場合、ディテクタ リストのページを移動するか、1 つ以上のフィルタを適用することによって、そのディテクタを見つけることができます。詳細については、ディテクタの管理（46-26 ページ）を参照してください。

ステップ 3　次の選択肢があります。

- ディテクタを**アクティブ**にして、システムがネットワーク トラフィックを分析するときにそのディテクタを使用するようにするには、ディテクタの横にある非アクティブにされたスライダ（）をクリックします。
- ディテクタを**非アクティブ**にして、システムがネットワーク トラフィックを分析するときにそのディテクタを使用しないようにするには、ディテクタの横にあるアクティブにされたスライダ（  ）をクリックします。

一部のアプリケーション ディテクタはその他のディテクタによって必要とされることに注意してください。そのようなディテクタのいずれかを非アクティブにすると、それに依存するディテクタも無効にされることを示す警告が表示されます。

アプリケーション ディテクタの変更

ライセンス：FireSIGHT

ユーザ定義のアプリケーション ディテクタを変更するには、次の手順を使用します。

アプリケーション ディテクタを変更する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Applications] を選択します。

[Detectors] ページが表示されます。

ステップ 2　変更するディテクタを見つけます。

変更するディテクタが最初のページにない場合、ディテクタ リストのページを移動するか、1 つ以上のフィルタを適用することによって、そのディテクタを見つけることができます。詳細については、ディテクタの管理（46-26 ページ）を参照してください。

ステップ 3　ユーザ定義のディテクタを変更するには、変更するディテクタの横にある [Edit] をクリックします。

[Edit Application Detector] ページが表示されます。

ステップ 4　ディテクタを変更します。

変更可能なさまざまな設定の詳細については、ユーザ定義のアプリケーション プロトコル ディテクタの作成（46-20 ページ）を参照してください。

ステップ 5　次の選択肢があります。

- 非アクティブなユーザ定義ディテクタを変更する場合は、[Save] をクリックして変更を保存するか、[Save as New] をクリックしてディテクタを新規の非アクティブなユーザ定義ディテクタとして保存します。
- アクティブなユーザ定義ディテクタを変更する場合は、[Save and Reactivate] をクリックして変更を保存し、すぐに変更したディテクタの使用を開始するか、[Save as New] をクリックしてディテクタを新規の非アクティブなユーザ定義ディテクタとして保存します。

注　システムは、アプリケーション トラフィックを分析するために、ディテクタがアクティブなアプリケーションのみを使用します。詳細については、ディテクタのアクティブ化と非アクティブ化（46-30 ページ）を参照してください。

ディテクタの削除

ライセンス：FireSIGHT

ディテクタを削除するには、次の手順を使用します。ユーザ定義のディテクタおよびCisco プロフェッショナル サービスが提供する個別にインポートされたアドオン ディテクタを削除することができます。その他のCiscoが提供するディテクタを削除することはできませんが、その多くを非アクティブにすることはできます。

注　ディテクタが適用されたポリシーで使用されている間は、そのディテクタを非アクティブにしたり、削除したりすることはできません。

ディテクタを削除する方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Policies] > [Application Detectors] を選択します。

[Detectors] ページが表示されます。

ステップ 2　削除するディテクタの横にあるチェック ボックスを選択し、[Delete] をクリックします。

削除するディテクタが最初のページにない場合、ディテクタ リストのページを移動するか、1 つ以上のフィルタを適用することによって、そのディテクタを見つけることができます。詳細については、ディテクタの管理（46-26 ページ）を参照してください。

ステップ 3　[OK] をクリックして、ディテクタを削除することを確認します。

ディテクタが削除されます。

ホスト入力データのインポート

ライセンス： FireSIGHT

サードパーティからネットワーク マップ データをインポートするために、組織にスクリプトを作成する機能、またはコマンドライン インポート ファイルを作成する機能がある場合、データをインポートしてネットワーク マップの情報を強化することができます。また、Web インターフェイスを使用して、オペレーティング システムまたはアプリケーションの ID を変更するか、アプリケーション プロトコル、プロトコル、ホスト属性、クライアントを削除することによって、ホスト入力機能を使用することができます。

システムは複数のソースからのデータを照合して、オペレーティング システムまたはアプリケーションの現行 ID を判別できます。この実行方法の詳細については、現在の ID について（46-5 ページ）を参照してください。

ネットワーク マップから影響を受けるホストを削除すると、サードパーティの脆弱性を除くすべてのデータは破棄されることに注意してください。スクリプトまたはインポート ファイルの設定方法の詳細については、『*FireSIGHT System Host Input API Guide*』を参照してください。

影響の関連付けにインポートしたデータを含めるには、データベースのオペレーティング システムおよびアプリケーション定義にデータをマッピングする必要があります。詳細については、次の項を参照してください。

- サードパーティ データの使用の有効化（46-33 ページ）
- サードパーティ製品マッピングの管理（46-33 ページ）
- サードパーティの脆弱性のマッピング（46-36 ページ）
- カスタム製品マッピングの管理（46-37 ページ）

サードパーティ データの使用の有効化

ライセンス：FireSIGHT

ネットワークのサードパーティ システムからネットワーク マップ データをインポートできます。ただし、FireSIGHTの推奨事項、適応型プロファイル、影響評価など、侵入データやディスカバリ データを一緒に使用する機能を有効にするには、可能な限り多くの要素を対応する定義にマッピングする必要があります。サードパーティ データを使用する場合は、以下の要件を考慮してください。

- ネットワーク資産に特定のデータを持つサードパーティ システムがある場合、ホスト入力機能を使用してそのデータをインポートできます。ただし、製品にはサードパーティによって異なる名前が付けられていることがあるため、対応するCisco製品定義にサードパーティのベンダー、製品、バージョンをマッピングする必要があります。製品をマッピングした後、システム ポリシーでの影響評価のために脆弱性マッピングを有効にして、影響の関連付けを可能にする必要があります。バージョンレスまたはベンダーレスのアプリケーション プロトコルの場合、システム ポリシーでアプリケーション プロトコルの脆弱性をマッピングする必要があります。詳細については、サードパーティ製品のマッピング（46-34 ページ）を参照してください。
- サード パーティからパッチ情報をインポートし、そのパッチによって解決されたすべての脆弱性を無効としてマークする場合、データベースの修正定義にサードパーティの修正名をマッピングする必要があります。その修正によって解決されたすべての脆弱性は、その修正を追加したホストから除去されます。詳細については、サード パーティ製品の修正のマッピング（46-35 ページ）を参照してください。
- サードパーティからオペレーティング システムおよびアプリケーション プロトコルの脆弱性をインポートし、影響の関連付けに使用する場合、サードパーティの脆弱性の識別文字列をデータベースの脆弱性にマッピングする必要があります。多くのクライアントには関連付けられた脆弱性があり、クライアントが影響評価に使用されますが、サードパーティのクライアントの脆弱性をインポートしてマッピングすることはできないことに注意してください。脆弱性をマッピングした後、システム ポリシーでの影響評価のためにサードパーティの脆弱性マッピングを有効にする必要があります。詳細については、サードパーティの脆弱性のマッピング（46-36 ページ）を参照してください。アプリケーション プロトコルにベンダー情報またはバージョン情報がない場合に、脆弱性にマッピングするには、管理ユーザがシステム ポリシーでアプリケーションの脆弱性もマッピングする必要があります。詳細については、サーバの脆弱性のマッピング（63-32 ページ）を参照してください。
- アプリケーション データをインポートし、影響の関連付けにそのデータを使用する場合は、対応するCisco アプリケーション プロトコル定義に各アプリケーション プロトコルのベンダー文字列をマッピングする必要があります。詳細については、カスタム製品マッピングの管理（46-37 ページ）を参照してください。

サードパーティ製品マッピングの管理

ライセンス：FireSIGHT

ユーザ入力機能を使用してサードパーティからネットワーク マップにデータを追加する場合、Cisco製品定義にサードパーティが使用するベンダー、製品、バージョンの名前をマッピングする必要があります。製品をCiscoの定義にマッピングすると、これらの定義に基づいて脆弱性が割り当てられます。

同様に、パッチ管理製品などサードパーティからパッチ情報をインポートする場合、修正の名前を適切なベンダーおよび製品およびデータベースの対応する修正にマッピングする必要があります。

詳細については、次の項を参照してください。

- サードパーティ製品のマッピング（46-34 ページ）
- サード パーティ製品の修正のマッピング（46-35 ページ）

サードパーティ製品のマッピング

ライセンス：FireSIGHT

サードパーティからデータをインポートする場合、そのデータを使用して脆弱性を割り当てたり、影響の関連付けを行ったりするために、Cisco製品をサードパーティの名前にマッピングする必要があります。製品をマッピングすることにより、Ciscoの脆弱性の情報をサードパーティ製品の名前に関連付けます。これにより、システムはそのデータを使用して、影響の関連付けを実行できます。

ホスト入力のインポート機能を使用してデータをインポートする場合、AddScanResult 機能を使用して、インポート中にサードパーティ製品をオペレーティング システムおよびアプリケーションの脆弱性にマッピングすることもできます。

例として、Apache Tomcat をアプリケーションとしてリストするサードパーティからデータをインポートするときに、それがバージョン 6 の製品であると分かっている場合、[Vendor Name] が `Apache`、[Product Name] が `Tomcat` に設定され、[Vendor] ドロップダウン リストから [Apache]、[Product] ドロップダウン リストから [Tomcat]、[Version] ドロップダウン リストから [6] が選択されているサードパーティ マップを追加できます。このマッピングによって、Apache Tomcat 6 のすべての脆弱性が、アプリケーションとして Apache Tomcat をリストするホストに割り当てられます。

バージョンレスまたはベンダーレスのアプリケーションの場合、システム ポリシーでアプリケーション タイプの脆弱性をマッピングする必要があります。詳細については、サーバの脆弱性のマッピング（63-32 ページ）を参照してください。多くのクライアントには関連付けられた脆弱性があり、クライアントが影響評価に使用されますが、サードパーティのクライアントの脆弱性をインポートしてマッピングすることはできないことに注意してください。

ヒント　すでに別のDefense Centerにサードパーティのマッピングを作成している場合、そのマッピングをエクスポートして、このDefense Centerにインポートすることができます。その後、必要に応じてインポートしたマッピングを編集できます。詳細については、設定のインポートおよびエクスポート（A-1 ページ）を参照してください。

サードパーティ製品をCisco製品定義にマッピングする方法：

アクセス：Admin

ステップ 1　[Policies] > [Application Detectors] を選択し、[User Third-Party Mappings] をクリックします。

[User Third-Party Mappings] ページが表示されます。

ステップ 2　次の 2 つの選択肢があります。

- 既存のマップ セットを編集するには、マップ セットの横にある [Edit] をクリックします。
- 新しいマップ セットを作成するには、[Create Product Map Set] をクリックします。

[Edit Third-Party Product Mappings] ページが表示されます。

ステップ 3　[Mapping Set Name] フィールドにマッピング セットの名前を入力します。

ステップ 4　[Description] フィールドに説明を入力します。

ステップ 5　次の 2 つの選択肢があります。

- サードパーティ製品をマッピングするには、[Add Product Map] をクリックします。
- 既存のサードパーティ製品マップを編集するには、マップ セットの横にある [Edit] をクリックします。

[Add Product Map] ページが表示されます。

ステップ 6　[Vendor String] フィールドにサードパーティ製品によって使用されるベンダー文字列を入力します。

ステップ 7　[Product String] フィールドにサードパーティ製品によって使用される製品文字列を入力します。

ステップ 8　[Version String] フィールドにサードパーティ製品によって使用されるバージョン文字列を入力します。

ステップ 9　[Product Mappings] セクションで、以下のリストから脆弱性マッピングに使用するオペレーティング システム、製品、およびバージョンを選択します(該当する場合)。

- **ベンダー**
- **製品**
- **Major Version**
- **Minor Version**
- **Revision Version**
- **ビルド**
- **Patch**
- **Extension**

たとえば、名前がサードパーティ文字列で構成される製品を実行するホストで Red Hat Linux 9 の脆弱性を使用する場合、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、バージョンとして [9] を選択します。

ステップ 10　[Save] をクリックします。

サード パーティ製品の修正のマッピング

ライセンス: FireSIGHT

修正名をデータベースの特定の修正セットにマッピングする場合、サードパーティのパッチ管理アプリケーションからデータをインポートし、修正を一連のホストに適用することができます。修正名がホストにインポートされると、システムはその修正によって解決されるすべての脆弱性をそのホストに対して無効としてマークします。

サードパーティの修正をCiscoの修正定義にマッピングする方法:

アクセス: Admin/

ステップ 1　[Policies] > [Application Detectors] を選択し、[User Third-Party Mappings] をクリックします。

[User Third-Party Mappings] ページが表示されます。

ステップ 2　次の 2 つの選択肢があります。

- 既存のマップ セットを編集するには、マップ セットの横にある [Edit] をクリックします。
- 新しいマップ セットを作成するには、[Create Product Map Set] をクリックします。

[Edit Third-Party Product Mappings] ページが表示されます。

ステップ 3　[Mapping Set Name] フィールドにマッピング セットの名前を入力します。

ステップ 4　[Description] フィールドに説明を入力します。

ステップ 5　次の 2 つの選択肢があります。

- サードパーティ製品をマッピングするには、[Add Fix Map] をクリックします。
- 既存のサードパーティ製品マップを編集するには、その横にある [Edit] をクリックします。

[Add Fix Map] ページが表示されます。

ステップ 6　[Third-Party Fix Name] フィールドにマッピングする修正の名前を入力します。

ステップ 7　[Product Mappings] セクションで、以下のリストから修正マッピングに使用するオペレーティング システム、製品、およびバージョンを選択します（該当する場合）。

- **ベンダー**
- **製品**
- **Major Version**
- **Minor Version**
- **Revision Version**
- **ビルド**
- **Patch**
- **Extension**

たとえば、マッピングで Red Hat Linux 9 から選択した修正をパッチが適用されるホストに割り当てる場合、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、バージョンとして [9] を選択します。

ステップ 8　[Save] をクリックして、修正マップを保存します。

サードパーティの脆弱性のマッピング

ライセンス：FireSIGHT

サードパーティから VDB に脆弱性情報を追加するには、インポートしたそれぞれの脆弱性のサードパーティ識別文字列を、既存のCisco、Bugtraq、または Snort の ID にマッピングする必要があります。脆弱性のマッピングを作成したら、マッピングはネットワーク マップのホストにインポートされたすべての脆弱性に対して機能し、それらの脆弱性に対する影響の関連付けを可能にします。

サードパーティの脆弱性に対する影響の関連付けを有効にし、関連付けの実行を可能にする必要があることに注意してください。詳細については、脆弱性影響評価マッピングの有効化（45-36 ページ）を参照してください。バージョンレスまたはベンダーレスのアプリケーションの場合、システム ポリシーでアプリケーション タイプの脆弱性をマッピングする必要もあります。詳細については、サーバの脆弱性のマッピング（63-32 ページ）を参照してください。

また、多くのクライアントには関連付けられた脆弱性があり、クライアントが影響評価に使用されますが、サードパーティのクライアントの脆弱性は影響評価に使用できません。

ヒント　すでに別のDefense Centerにサードパーティのマッピングを作成している場合、そのマッピングをエクスポートして、このDefense Centerにインポートすることができます。その後、必要に応じてインポートしたマッピングを編集できます。詳細については、設定のインポートおよびエクスポート（A-1 ページ）を参照してください。

サードパーティの脆弱性を既存の脆弱性にマッピングする方法:

アクセス: Admin

ステップ 1　[Policies] > [Application Detectors] を選択し、[User Third-Party Mappings] をクリックします。

[User Third-Party Mappings] ページが表示されます。

ステップ 2　次の 2 つの選択肢があります。

- 既存の脆弱性セットを編集するには、脆弱性セットの横にある [Edit] をクリックします。
- 新しい脆弱性セットを作成するには、[Create Vulnerability Map Set] をクリックします。

[Edit Third-Party Vulnerability Mappings] ページが表示されます。

ステップ 3　[Add Vulnerability Map] をクリックします。

[Add Vulnerability Map] ポップアップ ウィンドウが表示されます。

ステップ 4　[Vulnerability ID] フィールドに脆弱性のサード パーティ ID を入力します。

ステップ 5　[Vulnerability Description] フィールドに説明を入力します。

ステップ 6　オプションで、[Snort Vulnerability ID Mappings] フィールドにシグニチャ ID を入力します。

ステップ 7　オプションで、[Cisco Vulnerability ID Mappings] フィールドにCiscoの脆弱性 ID を入力します。

ステップ 8　オプションで、[Bugtraq Vulnerability ID Mappings] フィールドに Bugtraq ID 番号を入力します。

ステップ 9　[Add] をクリックします。

カスタム製品マッピングの管理

ライセンス: FireSIGHT

製品マッピングを使用して、サードパーティによるサーバ入力が適切なCisco定義に関連付けられていることを確認できます。製品マッピングを定義してアクティブにした後、マッピングされたベンダー文字列が存在するネットワーク マップのホスト上のすべてのサーバまたはクライアントは、カスタム製品マッピングを使用します。したがって、サーバのベンダー、製品、バージョンを明示的に設定する代わりに、特定のベンダー文字列でネットワーク マップのすべてのサーバの脆弱性をマップすることをお勧めします。

詳細については、次の説明を参照してください。

- カスタム製品マッピングの作成（46-37 ページ）
- カスタム製品マッピング リストの編集（46-39 ページ）
- カスタム製品マッピングのアクティベーション状態の管理（46-39 ページ）

カスタム製品マッピングの作成

ライセンス: FireSIGHT

システムがネットワーク マップのサーバを VDB 内のベンダーおよび製品にマッピングできない場合、サーバを識別するときに使用するシステムのマッピングを手動で作成できます。カスタム製品マッピングをアクティブにすると、システムは選択されたベンダーおよび製品の脆弱性を、そのベンダー文字列が発生するネットワーク マップのすべてのサーバにマッピングします。

注　カスタム製品マッピングは、アプリケーション データのソース（Nmap、ホスト入力機能、または FireSIGHT システム自体など）に関係なく、アプリケーション プロトコルのすべての発生に適用されます。ただし、ホスト入力機能を使用してインポートしたデータのサードパーティの脆弱性マッピングが、カスタム製品マッピングを介して設定したマッピングと競合する場合、サードパーティの脆弱性マッピングはカスタム製品マッピングをオーバーライドし、入力が発生したときにサードパーティの脆弱性マッピング設定を使用します。詳細については、サードパーティの脆弱性のマッピング（46-36 ページ）を参照してください。

製品マッピング リストを作成し、各リストをアクティブ化/非アクティブ化することによって、複数のマッピングの同時使用を有効にするか、無効にします。マッピングするベンダーを選択すると、そのベンダーによって作成された製品のみを含むように製品リストが更新されます。

カスタム製品マッピングを作成した後で、カスタム製品マッピング リストをアクティブにする必要があります。カスタム製品マッピング リストをアクティブにすると、指定されたベンダー文字列が発生するすべてのサーバが更新されます。ホスト入力機能を介してインポートされるデータでは、このサーバの製品マッピングをすでに明示的に設定していない限り、脆弱性が更新されます。

たとえば、組織が `Internal Web Server` を読み取るように Apache Tomcat Web サーバのバナーを変更した場合、ベンダー文字列 `Internal Web Server` をベンダー **Apache** および製品 **Tomcat** にマッピングできます。その後、そのマッピングを含むリストをアクティブにすると、`Internal Web Server` とラベル付けされたサーバが発生するすべてのホストで、Apache Tomcat の脆弱性がデータベースに保存されます。

ヒント　この機能を使用して、もう 1つの脆弱性にルールの SID をマッピングすることによって、ローカルの侵入ルールに脆弱性をマッピングすることができます。

カスタム製品マッピングを作成する方法：

アクセス： Admin

ステップ 1　[Policies] > [Application Detectors] を選択し、[Custom Product Mappings] をクリックします。

[Custom Product Mappings] ページが表示されます。

ステップ 2　[Create Custom Product Mapping List] をクリックします。

[Edit Custom Product Mappings List] ページが表示されます。

ステップ 3　名前を [Custom Product Mapping List Name] フィールドに入力します。

ステップ 4　[Add Vendor String] をクリックします。

[Add Vendor String] ポップアップ ウィンドウが表示されます。

ステップ 5　[Vendor String] フィールドに、選択したベンダーおよび製品値にマッピングする必要があるアプリケーションを識別するベンダー文字列を入力します。

ステップ 6　[Vendor] ドロップダウン リストから、マッピングするベンダーを選択します。

ステップ 7　[Product] ドロップダウン リストから、マッピングする製品を選択します。

ステップ 8　[Add] をクリックして、マッピングしたベンダー文字列をリストに追加します。

ステップ 9　オプションで、さらにベンダー文字列のマッピングをリストに追加するには、必要に応じて手順 4 ～ 8 を繰り返します。

ステップ 10　終了したら、[Save] をクリックします。

[Custom Product Mappings] ページが、追加したリストとともに再度表示されます。

カスタム製品マッピング リストの編集

ライセンス：FireSIGHT

ベンダー文字列を追加または削除したり、リスト名を変更したりして、既存のカスタム製品マッピング リストを変更できます。

カスタム製品マッピングを編集する方法：

アクセス：Admin

ステップ 1　[Policies] > [Application Detectors] を選択し、[Custom Product Mappings] をクリックします。

[Custom Product Mappings] ページが表示されます。

ステップ 2　編集する製品マッピング リストの横にある編集アイコン（  ）をクリックします。

[Edit Custom Product Mappings List] ページが表示されます。

ステップ 3　必要に応じてリストを変更します。詳細については、カスタム製品マッピングの作成（46-37 ページ）を参照してください。

ステップ 4　終了したら、[Save] をクリックします。

[Custom Product Mappings] ページが、変更したリストとともに表示されます。

カスタム製品マッピングのアクティベーション状態の管理

ライセンス：FireSIGHT

カスタム製品マッピング リスト全体の使用を一度に有効または無効にすることができます。カスタム製品マッピング リストをアクティブにすると、そのリストの各マッピングが、管理対象デバイスによって検出されたか、またはホスト入力機能を介してインポートされたかに関わらず、指定したベンダー文字列を持つネットワーク マップのホスト上のすべてのアプリケーションに適用されます。

カスタム製品マッピング リストをアクティブまたは非アクティブにする方法：

アクセス：Admin

ステップ 1　[Policies] > [Application Detectors] を選択し、[Custom Product Mappings] をクリックします。

[Custom Product Mappings] ページが表示されます。

ステップ 2　以下のように、カスタム製品マッピング リストの状態を変更します。

- カスタム製品マッピング リストの使用を有効にするには、[Activate] をクリックします。
- カスタム製品マッピング リストの使用を無効にするには、[Deactivate] をクリックします。

アクティブ スキャンの設定

FireSIGHT システムは、ネットワークのトラフィックをパッシブ分析してネットワーク マップを構築します。しかし、ホストをアクティブにスキャンして、そのホストに関する情報を判別する必要が生じることがあります。たとえば、オープン ポート上で実行中のサーバがホストにあり、システムによるネットワークのモニタリング中にそのサーバがトラフィックを送受信しなかった場合、システムではそのサーバに関する情報をネットワーク マップに追加しません。しかし、アクティブ スキャナを使用して直接そのホストをスキャンすると、サーバの存在を検出できます。

ホストをアクティブにスキャンする場合、ホストに関する情報を取得しようとする際にパケットを送信します。FireSIGHT システムは Nmap™ 6.01 と統合されています。これはネットワークの調査やセキュリティの監査用のオープン ソースのアクティブ スキャナで、ホスト上で実行されているオペレーティング システムやサーバを検出するのに使用できます。Nmap スキャンを使用すると、その結果に基づいて、ホスト上で実行されているオペレーティング システムやサーバに関する詳細情報を調べ、システムの脆弱性に関する報告内容を改善できます。

注 スキャン オプションによっては（ポート スキャンなど）低帯域幅のネットワークに非常に負荷をかけることがあります。この種のスキャンは、必ずネットワーク利用率が低い時間にスケジュールする必要があります。

詳細については、次の項を参照してください。

- Nmap スキャンの概要（47-1 ページ）
- Nmap スキャンのセットアップ（47-10 ページ）
- Nmap スキャンの管理（47-16 ページ）
- スキャン ターゲットの管理（47-20 ページ）
- アクティブ スキャンの結果での作業（47-21 ページ）

Nmap スキャンの概要

ライセンス： FireSIGHT

Nmap を使用すると、ネットワーク内のホスト上のポートをアクティブにスキャンして、そのホストのオペレーティング システムやサーバのデータを判別することにより、ネットワーク マップの質を高めたり、スキャン対象のホストにマップされている脆弱性の精度を微調整したりできます。Nmap がホスト プロファイルに結果を追加できるようにするには、その前にホストがネットワーク マップ内になければならないことに注意してください。結果ファイル内でスキャン結果を参照することもできます。

Nmap を使用してホストをスキャンすると、以前に検出されなかったオープン ポート上のサーバが、そのホストに関するホスト プロファイル内の Servers リストに追加されます。ホスト プロファイルの Scan Results セクションには、フィルタ処理されていたり閉じていたりしている TCP ポートや UDP ポート上で検出されたサーバがリストされます。デフォルトでは、Nmap は 1660 を超える TCP ポートをスキャンします。

Nmap はスキャン結果と 1500 を超える既知のオペレーティング システムのフィンガープリントを比較して、オペレーティング システムを判別し、それぞれにスコアを割り当てます。最高スコアのオペレーティング システムのフィンガープリントが、ホストに割り当てられるオペレーティング システムになります。

Nmap スキャンで識別されたサーバがシステムで認識され、対応するサーバ定義がシステムにある場合、システムはそのサーバの脆弱性をホストにマップします。システムは、Nmap で使用されているサーバの名前を対応するCiscoのサーバ定義にマップし、システム内で各サーバにマップされた脆弱性を使用します。同様に、システムは Nmap のオペレーティング システム名をCiscoのオペレーティング システム定義にマップします。Nmap がホストのオペレーティング システムを検出すると、システムは対応するCiscoのオペレーティング システム定義からホストに脆弱性を割り当てます。

スキャンに使用される基礎的な Nmap テクノロジーの詳細については、http://insecure.org にある Nmap のマニュアルを参照してください。

Ciscoアプライアンス上の Nmap の詳細については、次のトピックを参照してください。

- Nmap 修復の概要（47-2 ページ）
- Nmap スキャン戦略の作成（47-6 ページ）
- サンプルの Nmap スキャン プロファイル（47-7 ページ）

Nmap 修復の概要

ライセンス： FireSIGHT

Nmap 修復を作成して、Nmap スキャンの設定を定義できます。Nmap 修復は、相関ポリシー内で応答として使用したり、オン デマンドで実行したり、特定の時間に実行するようにスケジュールしたりできます。Nmap スキャンの結果をネットワーク マップ内に表示するには、スキャン対象のホストがネットワーク マップ内にすでに存在していなければなりません。

Nmap により提供されるサーバやオペレーティング システムのデータは、もう一度 Nmap スキャンを実行するまで静的な状態のままであることに注意してください。Nmap を使用してホスト内でオペレーティング システムやサーバのデータをスキャンすることを計画している場合は、定期的なスキャンのスケジュールをセットアップして、Nmap によって提供されるオペレーティング システムやサーバのデータを最新に保つこともできます。詳細については、Nmap スキャンの自動化（62-5 ページ）を参照してください。ホストがネットワーク マップから削除されると、そのホストに関する Nmap スキャン結果は破棄されることにも注意してください。

Nmap の機能に関する詳細情報については、http://insecure.org のマニュアルを参照してください。次の表に、FireSIGHT システム システム上で設定できる Nmap 修復オプションを示します。

表 47-1　Nmap 修復オプション

オプション	説明	対応する Nmap オプション
Scan Which Address(es) From Event?	Nmap スキャンを相関ルールに対する応答として使用する場合、イベント内の送信元ホスト、宛先ホスト、またはその両方のどのアドレスをスキャンするのか制御するオプションを選択します。	該当なし
Scan Types	Nmap がポートをスキャンする方法を選択します。 • [TCP Syn] スキャンは、完全な TCP ハンドシェイクを使用せずに数千のポートにただちに接続します。このオプションを使用すると、TCP 接続が開始されますが完了はしていない状態で、`admin` アカウントが raw パケット アクセス権を持つホストや IPv6 が実行されていないホスト上でステルス モードでクイック スキャンできます。ホストが TCP Syn スキャンで送信される SYN パケットを確認応答すると、Nmap は接続をリセットします。 • [TCP Connect] スキャンは、`connect()` システム コールを使用して、ホスト上のオペレーティング システムを介して接続を開きます。TCP Connect スキャンは、Defense Center上の `admin` ユーザや管理対象デバイスがホストに対する raw パケット特権を持っていない場合や、IPv6 ネットワークをスキャンしている場合に使用できます。つまり、このオプションは TCP Syn スキャンを使用できない状況で使用します。 • [TCP ACK] スキャンは、ACK パケットを送信して、ポートがフィルタ処理されているかいないかを検査します。 • [TCP Window] スキャンは、TCP ACK スキャンと同じ機能に加えて、ポートが開いているか閉じているかも判別します。 • [TCP Maimon] スキャンは、FIN/ACK プローブを使用して BSD 派生システムを識別します。	**TCP Syn**: `-sS` **TCP Connect**: `-sT` **TCP ACK**: `-sA` **TCP Window**: `-sW` **TCP Maimon**: `-sM`
Scan for UDP ports	TCP ポートに加えて UDP ポートのスキャンも有効にします。UDP ポートのスキャンには時間がかかることがあるので、クイック スキャンする場合はこのオプションを使用しないように注意してください。	`-sU`
Use Port From Event	相関ポリシー内で応答として修復を使用する計画の場合に、修復によるスキャンの対象として、相関応答をトリガーするイベントで指定されたポートのみを有効にします。 **ヒント**　Nmap がオペレーティング システムやサーバに関する情報を収集するかどうかも制御できます。新しいサーバに関連付けられたポートをスキャンするには、[Use Port From Event] オプションを有効にします。	該当なし
Scan from reporting detection engine	ホストを報告した検出エンジンがあるアプライアンスからホストへのスキャンを有効にします。	該当なし
Fast Port Scan	スキャン元デバイス上の `/var/sf/nmap/share/nmap/nmap-services` ディレクトリ内にある `nmap-services` ファイルにリストされている TCP ポートのみに対するスキャンを有効にし、その他のポート設定を無視できるようにします。このオプションと [Port Ranges and Scan Order] オプションを併用できないことに注意してください。	`-F`

表 47-1　Nmap 修復オプション(続き)

オプション	説明	対応する Nmap オプション
Port Ranges and Scan Order	Nmap ポート仕様シンタックスを使用して、スキャンする特定のポートを設定し、スキャンする順序も設定します。このオプションと [Fast Port Scan] オプションを併用できないことに注意してください。	`-p`
Probe open ports for vendor and version information	サーバ ベンダーとバージョン情報の検出を有効にします。オープン ポートでサーバ ベンダーとバージョン情報を調査する場合、Nmap はサーバの識別に使用するサーバ データを取得します。次に、Ciscoのサーバ データをそのサーバに置き換えます。	`-sV`
Service Version Intensity	サービス バージョンに対する Nmap プローブの強度を選択します。サービスの強度の数値が大きいほど、使用されるプローブが多くなり、精度は高くなります。強度の数値が小さいほど、プローブは高速になりますが、取得する情報は少なくなります。	`--version-intensity <intensity>`
Detect Operating System	ホストのオペレーティング システム情報の検出を有効にします。 ホストでのオペレーティング システムの検出を設定した場合、Nmap はホストをスキャンし、その結果を使用してオペレーティング システムごとに評価を作成します。この評価は、ホスト上でそのオペレーティング システムが実行されている可能性を反映します。Nmap で識別されるアイデンティティ データがネットワーク マップに表示される時点とその方法の詳細については、現在の ID について(46-5 ページ)を参照してください。	`-o`
Treat All Hosts As Online	ホスト ディスカバリ プロセスを省略し、ターゲット範囲内のすべてのホスト上でのポート スキャンを有効にします。このオプションを有効にすると、Nmap は [Host Discovery Method] と [Host Discovery Port List] の設定を無視するので注意してください。	`-PN`

表 47-1　Nmap 修復オプション（続き）

オプション	説明	対応する Nmap オプション
Host Discovery Method	ホスト ディスカバリを、ターゲット範囲内のすべてのホストに対して実行するか、[Host Discovery Port List] にリストされているポートを経由して実行するか、または、ポートがリストされていない場合にそのホスト ディスカバリ方式のデフォルト ポートを経由するかを選択します。 ここで、[Treat All Hosts As Online] も有効にすると、[Host Discovery Method] オプションは無効になり、ホスト ディスカバリが実行されないことに注意してください。 ホストが存在していて利用可能であるかどうかを Nmap がテストする際に使用する方式を以下から選択します。 • [TCP SYN] オプションは、SYN フラグが設定された空の TCP パケットを送信し、応答を受信するとホストが利用可能であると認識します。デフォルトでは TCP SYN はポート 80 をスキャンします。TCP SYN スキャンは、ステートフル ファイアウォール ルールが指定されたファイアウォールでブロックされる可能性が低いことに注意してください。 • [TCP ACK] オプションは、ACK フラグが設定された空の TCP パケットを送信し、応答を受信するとホストが利用可能であると認識します。デフォルトでは TCP ACK もポート 80 をスキャンします。TCP ACK スキャンは、ステートレス ファイアウォール ルールが指定されたファイアウォールでブロックされる可能性が低いことに注意してください。 • [UDP] オプションは、UDP パケットを送信し、クローズ ポートからポート到達不能応答が戻されるとホストが利用可能であると想定します。デフォルトでは UDP はポート 40125 をスキャンします。	**TCP SYN**：`-PS` **TCP ACK**：`-PA` **UDP**：`-PU`
Host Discovery Port List	ホスト ディスカバリの実行時にスキャンするポートを、カスタマイズしたカンマ区切りリストで指定します。	ホスト ディスカバリ方式に応じたポート リスト
Default NSE Scripts	ホスト ディスカバリを行い、サーバ、オペレーティング システム、脆弱性を検出する Nmap スクリプトのデフォルト セットを実行できるようにします。デフォルト スクリプトのリストについては、http://nmap.org/nsedoc/categories/default.html を参照してください。	`-sC`
Timing Template	スキャン プロセスのタイミングを選択します。選択する数値が大きいほど、スキャンは高速になり包括的ではなくなります。	**0**：`T0`（paranoid） **1**：`T1`（sneaky） **2**：`T2`（polite） **3**：`T3`（normal） **4**：`T4`（aggressive） **5**：`T5`（insane）

Nmap スキャン戦略の作成

ライセンス：FireSIGHT

アクティブ スキャンにより重要な情報が得られることがありますが、Nmap などのツールを多用すると、ネットワーク リソースに負荷がかかり、重要なホストがクラッシュすることさえあります。アクティブ スキャナを使用する際には、スキャン戦略を作成して、スキャンする必要があるホストとポートのみスキャンするようにしてください。

詳細については、次の項を参照してください。

- 適切なスキャン ターゲットの選択（47-6 ページ）
- スキャン対象にする適切なポートの選択（47-7 ページ）
- ホスト ディスカバリ オプションの設定（47-7 ページ）

適切なスキャン ターゲットの選択

ライセンス：FireSIGHT

Nmap を設定する際に、スキャン対象のホストを識別するスキャン ターゲットを作成できます。スキャン ターゲットには 1 つの IP アドレス、IP アドレスの CIDR ブロックまたはオクテット範囲、IP アドレス範囲、スキャンする IP アドレスまたは範囲のリスト、および 1 つ以上のホスト上のポートが含まれます。

次の方法でターゲットを指定できます。

- IPv6 ホストの場合：
  - 厳密な IP アドレス（`192.168.1.101` など）
- IPv4 ホストの場合：
  - 厳密な IP アドレス（`192.168.1.101` など）またはカンマかスペースで区切った IP アドレスのリスト
  - CIDR 表記を使用した IP アドレス ブロック（たとえば、`192.168.1.0/24` は、両端を含めて 192.168.1.1 から 192.168.1.254 の間の 254 個のホストをスキャンします）

    FireSIGHT システムでの CIDR 表記の使用法の詳細については、IP アドレスの表記規則（1-23 ページ）を参照してください。
  - オクテットの範囲アドレッシングを使用した IP アドレス範囲（たとえば、`192.168.0-255.1-254` は、192.168.x.x の範囲内の末尾が .0 と .255 以外のすべてのアドレスをスキャンします）
  - ハイフンを使用した IP アドレス範囲（たとえば、`192.168.1.1 - 192.168.1.5` は、両端を含めて 192.168.1.1 から 192.168.1.5 の間の 6 つのホストをスキャンします）
  - カンマかスペースで区切ったアドレスか範囲のリスト（たとえば、`192.168.1.0/24, 194.168.1.0/24` は、両端を含めて 192.168.1.1 から 192.168.1.254 の間の 254 個のホストと、両端を含めて 194.168.1.1 から 194.168.1.254 の間の 254 個のホストをスキャンします）

理想的な Nmap スキャンのスキャン ターゲットには、システムで識別できないオペレーティング システムがあるホスト、識別されていないサーバがあるホスト、最近ネットワーク上で検出されたホストが含まれます。ネットワーク マップ内にないホストに関する Nmap 結果は、ネットワーク マップに追加できないことに注意してください。

注意　Nmap によって提供されるサーバやオペレーティング システムのデータは、もう一度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap を使用したホストのスキャンを計画している場合は、Nmap で提供されるオペレーティング システムやサーバのデータを最新に保つため、定期的なスキャンのスケジュールをセットアップすることもできます。詳細については、Nmap スキャンの自動化（62-5 ページ）を参照してください。ホストがネットワーク マップから削除されると、Nmap スキャン結果は破棄されることにも注意してください。また、ターゲットをスキャンする権限を持っていることを確認してください。Nmap を使用して自分や自社に属さないホストをスキャンすると違法になる場合があります。

スキャン対象にする適切なポートの選択

ライセンス：FireSIGHT

設定するスキャン ターゲットごとに、スキャン対象のポートを選択できます。各ターゲット上でスキャンする必要があるポートのセットを正確に識別するため、個々のポート番号、ポート範囲、または一連のポート番号やポート範囲を指定できます。

デフォルトでは、Nmap は 1 から 1024 までの TCP ポートをスキャンします。相関ポリシー内で応答として修復を使用する計画の場合は、相関応答をトリガーするイベントで指定されたポートのみを修復でスキャンできます。オン デマンドまたはスケジュール済みタスクとして修復を実行する場合、または Use Port From Event を使用しない場合は、その他のポート オプションを使用して、スキャンするポートを決定できます。`nmap-services` ファイルにリストされている TCP ポートのみスキャンし、その他のポート設定を無視するよう選択できます。TCP ポートの他に UDP ポートもスキャンできます。UDP ポートに対するスキャンには時間がかかることがあるので、すばやくスキャンする場合はこのオプションを使用しないように注意してください。スキャン対象として特定のポートかポート範囲を選択するには、Nmap ポート仕様シンタックスを使用してポートを識別します。

ホスト ディスカバリ オプションの設定

ライセンス：FireSIGHT

ホストに対してポート スキャンを始める前にホスト ディスカバリを実行するかどうかを決めるか、またはスキャンを計画しているすべてのホストがオンラインであると想定できます。すべてのホストをオンラインとして扱わないことを選択した場合、使用するホスト ディスカバリ方式を選択でき、必要に応じて、ホスト ディスカバリ時のスキャン対象ポートのリストをカスタマイズできます。ホスト ディスカバリ時には、リストされているポートでオペレーティング システムやサーバの情報は調査されません。特定のポートを経由する応答を使用して、ホストがアクティブで使用可能かどうかのみを判別します。ホスト ディスカバリを実行して、ホストが利用可能でなかった場合には、そのホスト上のポートは Nmap でスキャンされません。

サンプルの Nmap スキャン プロファイル

ライセンス：FireSIGHT

次のシナリオには、ご使用のネットワーク上で Nmap を使用する方法の例が示されています。

- 例：不明なオペレーティング システムの解決（47-8 ページ）
- 例：新しいホストに対する応答（47-9 ページ）

例：不明なオペレーティング システムの解決

ライセンス：FireSIGHT

システムでネットワーク上のホストのオペレーティング システムを判別できない場合、Nmap を使用してホストをアクティブ スキャンできます。Nmap は、スキャンから得られた情報を利用して、使用されている可能性のあるオペレーティング システムを評価します。次に、最高の評価のオペレーティング システムを、ホストのオペレーティング システムを識別したものとして使用します。

Nmap を使用して新しいホストにオペレーティング システムやサーバの情報を要求すると、スキャン対象のホストに対するシステムによるそのデータのモニタリングは非アクティブになります。Nmap を使用してホスト検出を実行し、システムにより不明なオペレーティング システムがあるとマークが付けられたホストのサーバ オペレーティング システムを検出すると、同種のホストのグループを識別できる場合があります。その場合、それらのホストのうちの 1 つに基づいたカスタム フィンガープリントを作成し、システムでそのフィンガープリントを、Nmap スキャンに基づいてそのホスト上で実行されていると判明したオペレーティング システムと関連付けるようにすることができます。可能な限り、Nmap などのサードパーティ製の静的データを入力するよりも、カスタム フィンガープリントを作成してください。カスタム フィンガープリントを使用すると、システムはホストのオペレーティング システムを継続してモニタし、必要に応じて更新できるからです。

Nmap を使用してオペレーティング システムを検出する方法：

アクセス：Admin/Discovery Admin

ステップ 1　Nmap モジュールのスキャン インスタンスを設定します。

詳細については、Nmap スキャン インスタンスの作成（47-10 ページ）を参照してください。

ステップ 2　次の設定を使用して Nmap 修復を作成します。

- [Use Port From Event] を有効にして、新しいサーバに関連付けられたポートをスキャンします。
- [Detect Operating System] を有効にして、ホストのオペレーティング システムの情報を検出します。
- [Probe open ports for vendor and version information] を有効にして、サーバ ベンダーとバージョン情報を検出します。
- ホストが既存であることが判明しているので、[Treat All Hosts as Online] を有効にします。

Nmap 修復の作成の詳細については、Nmap 修復の作成（47-13 ページ）を参照してください。

ステップ 3　システムで不明なオペレーティング システムがあるホストが検出されたときにトリガーされる相関ルールを作成します。

このルールは、**ディスカバリ イベントが発生**し、**ホストの OS 情報が変更**されており、**OS 名が不明**という条件が満たされている場合にトリガーされる必要があります。

相関ルールの作成の詳細については、相関ポリシーのルールの作成（51-3 ページ）を参照してください。

ステップ 4　相関ルールを組み込む相関ポリシーを作成します。

相関ポリシーの作成の詳細については、相関ポリシーの作成（51-49 ページ）を参照してください。

ステップ 5　相関ポリシー内で、ステップ 2 で応答として作成した Nmap 修復をステップ 3 で作成したルールに追加します。

ステップ 6　相関ポリシーをアクティブにします。

ステップ 7　ネットワーク マップ上のホストを消去し、強制的にネットワーク検出が再起動されてネットワーク マップが再構築されるようにします。

ステップ 8　1 日後か 2 日後に、相関ポリシーによって生成されたイベントを検索します。Nmap 結果から、ホスト上で検出されたオペレーティング システムを分析し、システムで認識されない特定のホスト設定がネットワーク上にあるかどうか調べます。

Nmap 結果の分析の詳細については、スキャン結果の分析（47-24 ページ）を参照してください。

ステップ 9　不明なオペレーティング システムがあるホストが複数検出され、Nmap 結果が同一の場合は、それらのホストの 1 つに対してカスタム フィンガープリントを作成し、将来類似のホストを識別する際に使用します。

詳細については、クライアントのフィンガープリントの作成（46-9 ページ）を参照してください。

例：新しいホストに対する応答

ライセンス：FireSIGHT

システムにより、侵入の可能性があるサブネット内で新しいホストが検出された場合、そのホストをスキャンして、そのホストの脆弱性に関する正確な情報を入手できます。

そのためには、このサブネット内に新しいホストが出現した時点で検出し、そのホスト上で Nmap スキャンを実行する修復を起動する相関ポリシーを作成してアクティブにします。

このポリシーをアクティブにした後で、修復状態の表示（[Policy & Response] > [Responses] > [Remediations] > [Status]）を定期的に検査して、修復が起動された時点を調べることができます。修復の動的なスキャン ターゲットには、サーバ検出の結果としてスキャンされたホストの IP アドレスを含める必要があります。これらのホストのホスト プロファイルを調べて、Nmap によって検出されたオペレーティング システムとサーバに基づいて、対処する必要がある脆弱性がホストにあるかどうか確認します。

注意　大規模なネットワークや動的なネットワークがある場合、新しいホストの検出は頻繁に発生するので、スキャンを使用して応答するには不向きな場合があります。リソースの過負荷を避けるために、頻繁に発生するイベントへの応答として Nmap スキャンを使用しないでください。また、Nmap を使用して新しいホストのオペレーティング システムやサーバの情報を要求すると、スキャン対象のホストに対するCiscoによるそのデータのモニタリングが非アクティブになることに注意してください。

新しいホストの出現に対する応答としてスキャンする方法：

アクセス：Admin/Discovery Admin

ステップ 1　Nmap モジュールのスキャン インスタンスを設定します。

詳細については、Nmap スキャン インスタンスの作成（47-10 ページ）を参照してください。

ステップ 2　次の設定を使用して Nmap 修復を作成します。

- [Use Port From Event] を有効にして、新しいサーバに関連付けられたポートをスキャンします。
- [Detect Operating System] を有効にして、ホストのオペレーティング システムの情報を検出します。
- [Probe open ports for vendor and version information] を有効にして、サーバ ベンダーとバージョン情報を検出します。

- ホストが既存であることが判明しているので、[Treat All Hosts as Online] を有効にします。

Nmap 修復の作成の詳細については、Nmap 修復の作成（47-13 ページ）を参照してください。

ステップ 3　システムが特定のサブネット上で新しいホストを検出したときにトリガーされる相関ルールを作成します。

このルールは、**ディスカバリ イベントが発生**し、**新しいホストが検出**されたときにトリガーされる必要があります。

相関ルールの作成の詳細については、相関ポリシーのルールの作成（51-3 ページ）を参照してください。

ステップ 4　相関ルールを組み込む相関ポリシーを作成します。

相関ポリシーの作成の詳細については、相関ポリシーの作成（51-49 ページ）を参照してください。

ステップ 5　相関ポリシー内で、ステップ 2 で応答として作成した Nmap 修復をステップ 3 で作成したルールに追加します。

ステップ 6　相関ポリシーをアクティブにします。

ステップ 7　新しいホストが通知されたら、ホスト プロファイルを調べて Nmap スキャンの結果を確認し、ホストに適用されている脆弱性に対処します。

Nmap スキャンのセットアップ

ライセンス： FireSIGHT

Nmap を使用してスキャンするには、最初にスキャン インスタンスとスキャン修復を設定します。Nmap スキャンをスケジュールする計画の場合は、スキャン ターゲットも定義します。

詳細については、次の項を参照してください。

- Nmap スキャン インスタンスの作成（47-10 ページ）
- Nmap スキャン ターゲットの作成（47-11 ページ）
- Nmap 修復の作成（47-13 ページ）

Nmap スキャン インスタンスの作成

ライセンス： FireSIGHT

脆弱性についてネットワークをスキャンするのに使用する Nmap モジュールごとに別々のスキャン インスタンスをセットアップできます。Defense Center上のローカル Nmap モジュールか、リモートでスキャンを実行するために使用するデバイスに対してスキャン インスタンスをセットアップできます。各スキャンの結果は常にDefense Centerに保存されます。リモート デバイスからスキャンを実行する場合でも、この場所でスキャンを設定できます。ミッション クリティカルなホストへの不慮のスキャンや悪意のあるスキャンを防ぐには、インスタンスのブラックリストを作成し、そのインスタンスで決してスキャンしてはならないホストを指示できます。

既存のスキャン インスタンスと同じ名前のスキャン インスタンスを追加できないことに注意してください。

スキャン インスタンスを作成する方法:

アクセス: Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scanners] ページが表示されます。

ステップ 2　[Add Nmap Instance] をクリックします。

[Instance Detail] ページが表示されます。

ステップ 3　[Instance Name] フィールドに、1 文字から 63 文字の英数字の名前を入力します。アンダースコア (_) とハイフン (-) 以外の特殊文字およびスペースは使用できません。

ステップ 4　[Description] フィールドに 0 文字から 255 文字の英数字の説明を指定します。スペースや特殊文字を使用できます。

ステップ 5　オプションで、[Black Listed Scan hosts] フィールドで、このスキャン インスタンスがスキャン*しない*ホストまたはネットワークを指定します。

- IPv6 ホストの場合は厳密な IP アドレス (たとえば、`2001:DB8::fedd:eeff`)
- IPv4 ホストの場合、厳密な IP アドレス (`192.168.1.101` など) または CIDR 表記を使用した IP アドレス ブロック (たとえば、`192.168.1.0/24` は、両端を含めて `192.168.1.1` から `192.168.1.254` の間の 254 個のホストをスキャンします)
- 感嘆符 (!) を使用してアドレス値の否定はできないことに注意してください。

ブラックリストに含まれるネットワーク内のホストをスキャン対象として特定すると、スキャンは実行されません。

ステップ 6　オプションで、Defense Centerの代わりにリモート デバイスからスキャンを実行するには、そのデバイスの IP アドレスか名前を指定します。この情報は、Defense Center Web インターフェイス内のそのデバイスに関する [Information] ページの [Remote Device Name] フィールドに表示されます。

ステップ 7　[Create] をクリックします。

スキャン インスタンスが作成されます。

Nmap スキャン ターゲットの作成

ライセンス: FireSIGHT

特定のホストとポートを識別するスキャン ターゲットを作成して保存できます。その後、オンデマンド スキャンを実行するかスキャンをスケジュールする際に、保存済みのスキャン ターゲットの 1 つを使用できます。

IPv4 アドレスのターゲットをスキャンする場合、1 つの IP アドレス、IP アドレスのリスト、CIDR 表記、または Nmap スキャンのオクテットを使用して、スキャンするホストを選択できます。ハイフンを使用して、アドレスの範囲を指定することもできます。カンマかスペースを使用して、リスト内のアドレスや範囲を区切ります。

IPv6 アドレスのスキャンの場合、1 つの IP アドレスを使用します。インターフェイスの範囲は入力できません。

Nmap により提供されるサーバやオペレーティング システムのデータは、もう一度 Nmap スキャンを実行するまで静的な状態のままであることに注意してください。Nmap を使用したホストのスキャンを計画している場合は、Nmap で提供されるオペレーティング システムやサーバの

データを最新に保つため、定期的なスキャンのスケジュールをセットアップすることもできます。詳細については、Nmap スキャンの自動化（62-5 ページ）を参照してください。ホストがネットワーク マップから削除されると、そのホストに関する Nmap スキャン結果は破棄されることにも注意してください。

スキャン ターゲットを作成する方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scanners] ページが表示されます。

ステップ 2　ツールバーで、[Targets] をクリックします。

[Scan Target List] ページが表示されます。

ステップ 3　[Create Scan Target] をクリックします。

[Scan Target] ページが表示されます。

ステップ 4　[Name] フィールドに、このスキャン ターゲットに使用する名前を入力します。

ステップ 5　[IP Range] テキスト ボックスで、次のシンタックスを使用して、スキャンする 1 つ以上のホストを指定します。

- IPv6 ホストの場合、厳密な IP アドレス（`2001:DB8::fedd:eeff` など）
- IPv4 ホストの場合、厳密な IP アドレス（`192.168.1.101` など）または IP アドレスのカンマ区切りリスト
- IPv4 ホストの場合、CIDR 表記を使用した IP アドレス ブロック（たとえば、`192.168.1.0/24` は、両端を含めて 192.168.1.1 から 192.168.1.254 の間の 254 個のホストをスキャンします）

  FireSIGHT システムでの CIDR 表記の使用法の詳細については、IP アドレスの表記規則（1-23 ページ）を参照してください。
- IPv4 ホストの場合、オクテットの範囲アドレッシングを使用した IP アドレス範囲（たとえば、`192.168.0-255.1-254` は、`192.168.x.x` の範囲内の末尾が .0 と .255 以外のすべてのアドレスをスキャンします）
- IPv4 ホストの場合、ハイフンを使用した IP アドレス範囲（たとえば、`192.168.1.1 - 192.168.1.5` は、両端を含めて 192.168.1.1 から 192.168.1.5 の間の 6 つのホストをスキャンします）
- IPv4 ホストの場合、カンマかスペースで区切ったアドレスまたは範囲のリスト（たとえば、`192.168.1.0/24, 194.168.1.0/24` は、両端を含めて 192.168.1.1 から 192.168.1.254 の間の 254 個のホストと、両端を含めて 194.168.1.1 から 194.168.1.254 の間の 254 個のホストをスキャンします）

注　[IP Range] テキスト ボックスには最大 255 文字まで入力できます。また、スキャン ターゲット内の IP アドレスか範囲のリストでカンマを使用した場合、ターゲットを保存する際にカンマはスペースに変換されるので注意してください。

ステップ 6　[Ports] フィールドで、スキャンするポートを指定します。

1 から 65535 までの値を使用して、次のいずれかを入力できます。

- 1 つのポート番号
- カンマで区切ったポートのリスト

- ハイフンで区切ったポート番号の範囲
- ハイフンで区切ったポート番号の複数の範囲をカンマで区切ったもの

ステップ 7　[Save] をクリックします。

スキャン ターゲットが作成されます。

Nmap 修復の作成

ライセンス：FireSIGHT

Nmap 修復を作成することにより、Nmap スキャンの設定を定義できます。Nmap 修復は、相関ポリシーの応答として、オンデマンドで実行するために使用することも、指定時刻に実行するようにスケジュール設定することもできます。Nmap スキャンの結果をネットワーク マップ内に表示するには、スキャン対象のホストがネットワーク マップ内にすでに存在していなければなりません。

Nmap 修復の具体的な設定について詳しくは、Nmap 修復の概要（47-2 ページ）を参照してください。

Nmap により提供されるサーバやオペレーティング システムのデータは、もう一度 Nmap スキャンを実行するまで静的な状態のままであることに注意してください。Nmap を使用してホスト内でオペレーティング システムやサーバのデータをスキャンすることを計画している場合は、定期的なスキャンのスケジュールをセットアップして、Nmap によって提供されるオペレーティング システムやサーバのデータを最新に保つこともできます。詳細については、Nmap スキャンの自動化（62-5 ページ）を参照してください。また、ホストがネットワーク マップから削除されると、そのホストのすべての Nmap スキャン結果が廃棄されることにも注意してください。

Nmap の機能に関する一般情報については、http://insecure.org にある Nmap のマニュアルを参照してください。

Nmap 修復を作成する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scanners] ページが表示されます。

ステップ 2　修復を追加するスキャン インスタンスの横の [Add Remediation] をクリックします。

[Edit Remediation] ページが表示されます。

ステップ 3　[Remediation Name] フィールドに、1 ～ 63 文字の英数字を使用して修復の名前を入力します。スペースと下線（_）およびハイフン（-）以外の特殊文字を使用することはできません。

ステップ 4　[Description] フィールドに、スペースと特殊文字を含む、0 ～ 255 文字の英数字を使用して修復の説明を入力します。

ステップ 5　侵入イベント、接続イベント、またはユーザ イベントでトリガーとして使用する相関ルールに応じてこの修復を使用する場合は、[Scan Which Address(es) From Event?] オプションを設定します。

- [Scan Source and Destination Addresses] を選択して、イベントの送信元 IP アドレスと宛先 IP アドレスによって表されるホストをスキャンします。
- [Scan Source Address Only] を選択して、イベントの送信元 IP アドレスで表されるホストをスキャンします。

- [Scan Destination Address Only] を選択して、イベントの宛先 IP アドレスで表されるホストをスキャンします。

ディスカバリ イベントまたはホスト入力イベントに対してトリガーする相関ルールへの応答としてこの修復を使用する計画の場合は、デフォルトでそのイベントに関連するホストの IP アドレスが修復によってスキャンされます。このオプションを設定する必要はありません。

注　トラフィック プロファイルの変更に対してトリガーする相関ルールへの応答として Nmap 修復を割り当て**ないでください**。

ステップ 6　以下のように [Scan Type] オプションを設定します。

- TCP 接続を開始して完了していない状態で、`admin` アカウントが raw パケット アクセス権を持つホストや IPv6 が実行されていないホスト上でステルス モードですばやくスキャンするには、[TCP Syn Scan] を選択します。
- Defense Centerの `admin` アカウントがロー パケット アクセスを持つホスト、または IPv6 が動作しているホストで使用可能な、システムの `connect()` コールを使用してスキャンするには、[TCP Connect Scan] を選択します。
- ACK パケット送信して、ポートがフィルタ処理されているかどうか検査するには、[TCP ACK Scan] を選択します。
- ACK パケットを送信して、ポートがフィルタ処理されているかどうか検査し、ポートが開いているか閉じているかも判別するには、[TCP Window Scan] を選択します。
- FIN/ACK プローブを使用して BSD 派生システムを識別するには、[TCP Maimon Scan] を選択します。

ステップ 7　オプションで、TCP ポートに加えて UDP ポートをスキャンするには、[Scan for UDP ports] オプションで [On] を選択します。

ヒント　UDP ポート スキャンは TCP ポート スキャンよりも時間がかかります。スキャンの速度を上げるには、このオプションを無効のままにします。

ステップ 8　相関ポリシー違反への応答としてこの修復を使用する場合は、[Use Port From Event] オプションを設定します。

- [On] を選択して、ステップ 11 で指定したポートではなく、相関イベントのポートをスキャンします。

  相関イベントのポートをスキャンする場合、修復はステップ 5 で指定する IP アドレスのポートをスキャンすることに注意してください。これらのポートは、修復のダイナミックなスキャン ターゲットにも追加されます。
- [Off] を選択して、ステップ 11 で指定するポートのみをスキャンします。

ステップ 9　相関ポリシー違反への応答としてこの修復を使用し、イベントが検出された検出エンジンを実行するアプライアンスを使用してスキャンする場合、[Scan from reporting detection engine] オプションを設定します。

- レポート検出エンジンを実行するアプライアンスからスキャンするには、[On] を選択します。
- 修復に設定されたアプライアンスからスキャンするには、[Off] を選択します。

ステップ 10　[Fast Port Scan] オプションを以下のように設定します。

- スキャン元デバイス上の `/var/sf/nmap/share/nmap/nmap-services` ディレクトリ内の `nmap-services` ファイルにリストされているポートのみスキャンし、その他のポート設定を無視するには、[On] を選択します。
- すべての TCP ポートをスキャンするには、[Off] を選択します。

ステップ 11　[Port Ranges and Scan Order] フィールドで、Nmap のシンタックスを使用して、デフォルトでスキャンするポートを、スキャンする順序で入力します。

1 から 65535 までの値を指定します。複数のポートを、カンマまたはスペースを使用して区切ります。ハイフンを使用してポートの範囲を示すこともできます。TCP ポートと UDP ポートの両方ともスキャンする場合は、スキャン対象の TCP ポートのリストの先頭に T を挿入し、UDP ポートのリストの先頭に U を挿入します。たとえば UDP トラフィックのポート 53 と 111 をスキャンしてから TCP トラフィックのポート 21 ～ 25 をスキャンするのであれば `U:53,111,T:21-25` と入力します。

ステップ 8 で説明されているように、相関ポリシー違反への応答として修復が起動する場合には、[Use Port From Event] オプションによりこの設定が上書きされることに注意してください。

ステップ 12　オープン ポートでサーバ ベンダーとバージョン情報を調査するには、[Probe open ports for vendor and version information] を以下のように設定します。

- ホスト上のオープン ポートでサーバ情報をスキャンして、サーバ ベンダーとバージョンを識別するには、[On] を選択します。
- ホストに関するCiscoのサーバ情報を使い続ける場合は、[Off] を選択します。

ステップ 13　オープン ポートの調査を選択する場合は、[Service Version Intensity] ドロップダウン リストから数値を選択して、使用するプローブの数を設定します。

- 使用するプローブを多くして、長いスキャンで高い精度を得るには、大きな数値を選択します。
- 使用するプローブを少なくして、低い精度で高速なスキャンを行うには、小さな数値を選択します。

ステップ 14　オペレーティング システム情報をスキャンするには、[Detect Operating System] 設定を構成します。

- ホストに対してオペレーティング システムを識別する情報をスキャンするには、[On] を選択します。
- ホストに関するCiscoのオペレーティング システム情報を使い続ける場合は、[Off] を選択します。

ステップ 15　ホスト ディスカバリが行われるかどうか、およびポートのスキャンが使用可能なホストのみに対して実行されるかどうかを決めるには、[Treat All Hosts As Online] を以下のように設定します。

- ホスト ディスカバリ プロセスを省略し、ターゲット範囲内のすべてのホスト上でのポート スキャンを実行するには、[On] を選択します。
- [Host Discovery Method] と [Host Discovery Port List] の設定を使用してホスト ディスカバリを実行し、使用不能なホスト上でのポート スキャンを省略するには、[Off] を選択します。

ステップ 16　Nmap でホストの可用性をテストする場合に使用する方式を以下のように選択します。

- SYN フラグが設定された空の TCP パケットを送信し、使用可能なホスト上のクローズ ポート上の RST 応答かオープン ポート上の SYN/ACK 応答を引き起こすには、[TCP SYN] を選択します。

  このオプションは、デフォルトでポート 80 をスキャンし、TCP SYN スキャンはステートフル ファイアウォール ルールが設定されたファイアウォールによりブロックされる可能性が低いことに注意してください。

- ACK フラグが設定された空の TCP パケットを送信し、使用可能なホストで RST 応答を得るために、[TCP ACK] を選択します。

  このオプションは、デフォルトでポート 80 をスキャンし、TCP ACK スキャンはステートレス ファイアウォール ルールが設定されたファイアウォールによりブロックされる可能性が低いことに注意してください。

- UDP パケットを送信し、使用可能なホストで閉じているポートのポート到達不能応答を得るには、[UDP] を選択します。このオプションは、デフォルトでポート 40125 をスキャンします。

ステップ 17　ホスト ディスカバリ時にポートのカスタム リストをスキャンする場合は、選択したホスト ディスカバリ方式に該当するポートのリストを、[Host Discovery Port List] フィールドにカンマで区切って入力します

ステップ 18　ホスト ディスカバリを行い、サーバ、オペレーティング システム、脆弱性 のディスカバリを行う Nmap スクリプトのデフォルト セットを使用するかどうかを制御するには、[Default NSE Scripts] オプションを以下のように設定します。

- Nmap スクリプトのデフォルト セットを実行するには、[On] を選択します。
- Nmap スクリプトのデフォルト セットを省略するには、[Off] を選択します。

デフォルト スクリプトのリストについては、http://nmap.org/nsedoc/categories/default.html を参照してください。

ステップ 19　スキャン プロセスのタイミングを設定するには、タイミング テンプレート番号を選択します。番号が大きいほど高速で包括度が低いスキャンになり、番号が小さいほど低速で包括度が高いスキャンになります。

ステップ 20　[Save] をクリックし、次に [Done] をクリックします。

修復が作成されます。

Nmap スキャンの管理

ライセンス： FireSIGHT

必要に応じて、Nmap スキャン インスタンスや修復を変更したり削除したりできます。オンデマンドの Nmap スキャンを実行することもできます。以前のスキャンに関する Nmap 結果を表示したりダウンロードしたりすることもできます。詳細については、次の項を参照してください。

- Nmap スキャン インスタンスの管理（47-16 ページ）
- Nmap 修復の管理（47-18 ページ）
- オンデマンド Nmap スキャンの実行（47-19 ページ）

Nmap スキャン インスタンスの管理

ライセンス： FireSIGHT

Nmap スキャン インスタンスを編集したり削除したりできます。詳細については、次の項を参照してください。

- Nmap スキャン インスタンスの編集（47-17 ページ）
- Nmap スキャン インスタンスの削除（47-17 ページ）

Nmap スキャン インスタンスの編集

ライセンス：FireSIGHT

スキャン インスタンスを変更するには、次の手順を使用します。インスタンスを変更する際に、そのインスタンスに関連付けられた修復を表示、追加、削除できることに注意してください。

スキャン インスタンスを編集する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scanners] ページが表示されます。

ステップ 2　編集するインスタンスの横にある [View] をクリックします。

[Instance Detail] ページが表示されます。

ステップ 3　オプションで、表示または編集する修復の横にある [View] をクリックします。

修復の編集の詳細については、Nmap 修復の編集（47-18 ページ）を参照してください。

ステップ 4　オプションで、削除する修復の横にある [Delete] をクリックします。

修復の削除の詳細については、Nmap 修復の削除（47-18 ページ）を参照してください。

ステップ 5　オプションで、[Add] をクリックして、このスキャン インスタンスに新しい修復を追加します。

新しい修復の作成の詳細については、Nmap 修復の管理（47-18 ページ）を参照してください。

ステップ 6　オプションで、スキャン インスタンスの設定に変更を加えてから、[Save] をクリックします。

ステップ 7　[Done] をクリックします。

スキャン インスタンスが変更されます。

Nmap スキャン インスタンスの削除

ライセンス：FireSIGHT

インスタンス内でプロファイルが作成された Nmap モジュールを使用しなくなった場合には、Nmap スキャン インスタンスを削除します。スキャン インスタンスを削除すると、そのインスタンスを使用する修復も削除されることに注意してください。

スキャン インスタンスを削除する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] をクリックします。

[Scanners] ページが表示されます。

ステップ 2　削除するスキャン インスタンスの横にある [Delete] をクリックします。

インスタンスが削除されます。

Nmap 修復の管理

ライセンス：FireSIGHT

Nmap 修復を編集したり削除したりできます。詳細については、次の項を参照してください。

- Nmap 修復の編集（47-18 ページ）
- Nmap 修復の削除（47-18 ページ）

Nmap 修復の編集

ライセンス：FireSIGHT

Nmap 修復に加えた変更は、進行中のスキャンには影響しません。新しい設定は、次回スキャンが開始されたときに有効になります。

Nmap 修復を編集する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scanners] ページが表示されます。

ステップ 2　編集する修復の横にある [View] をクリックします。

[Remediation Edit] ページが表示されます。

ステップ 3　必要に応じて変更を加えます。

変更できる設定については、Nmap 修復の作成（47-13 ページ）を参照してください。

ステップ 4　[Save] をクリックし、[Done] をクリックします。

修復が変更されます。

Nmap 修復の削除

ライセンス：FireSIGHT

Nmap 修復が不要になったら削除します。

Nmap 修復を削除する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scanners] ページが表示されます。

ステップ 2　削除する修復の横にある [Delete] をクリックします。

ステップ 3　修復を削除することを確認します。

修復が削除されます。

オンデマンド Nmap スキャンの実行

ライセンス：FireSIGHT

必要なときにいつでもオンデマンド Nmap スキャンを起動できます。スキャンする IP アドレスとポートを入力するか、既存のスキャン ターゲットを選択して、オンデマンド スキャンのターゲットを指定できます。

Nmap により提供されるサーバやオペレーティング システムのデータは、もう一度 Nmap スキャンを実行するまで静的な状態のままであることに注意してください。Nmap を使用したホストのスキャンを計画している場合は、Nmap で提供されるオペレーティング システムやサーバのデータを最新に保つため、定期的なスキャンのスケジュールをセットアップすることもできます。詳細については、Nmap スキャンの自動化（62-5 ページ）を参照してください。また、ホストがネットワーク マップから削除されると、Nmap スキャン結果は破棄されることにも注意してください。

オンデマンド Nmap スキャンを実行する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scanners] ページが表示されます。

ステップ 2　スキャンの実行時に使用する Nmap 修復の横にある [Scan] をクリックします。

[Nmap Scan Target] ダイアログ ボックスが表示されます。

ステップ 3　オプションで、保存済みのスキャン ターゲットを使用してスキャンするには、[Saved Targets] ドロップダウン リストからターゲットを選択して、[Load] をクリックします。

スキャン ターゲットに関連付けられた IP アドレスおよびポートが、[IP Range(s)] フィールドと [Ports] フィールドに入力されます。

ヒント　スキャン ターゲットを作成するには、[Edit/Add Targets] をクリックします。詳細については、Nmap スキャン ターゲットの作成（47-11 ページ）を参照してください。

ステップ 4　[IP Range(s)] フィールドで、最大 255 文字までで、スキャンするホストの IP アドレスを指定するかロードされたリストを変更します。

IPv4 アドレスのホストの場合、複数の IP アドレスをカンマで区切って指定するか、CIDR 表記を使用できます。感嘆符（!）を前に挿入して IP アドレスを否定することもできます。FireSIGHT システムでの CIDR 表記の使用の詳細については、IP アドレスの表記規則（1-23 ページ）を参照してください。

IPv6 アドレスのホストの場合、厳密な IP アドレスを使用します。インターフェイスの範囲は入力できません。

ステップ 5　[Ports] フィールドで、スキャンするポートを指定するか、ロードされたリストを変更します。

ポート番号、カンマで区切ったポートのリスト、ハイフンで区切ったポート番号の範囲を入力できます。ポートの入力の詳細については、検索でのポートの指定（60-8 ページ）を参照してください。

ステップ 6　[Scan Now] をクリックします。

Nmap サーバがスキャンを実行します。

Nmap は IP アドレスの範囲を検証し、範囲が無効な場合はエラー メッセージを表示することに注意してください。表示された場合は、[IP Range(s)] フィールドの内容を訂正し、有効な IP アドレス範囲を指定してください。

スキャン ターゲットの管理

ライセンス： FireSIGHT

Nmap モジュールを設定する際にスキャン ターゲットを作成して保存できます。スキャン ターゲットは、オンデマンドまたはスケジュール済みのスキャンの実行時にターゲットにするホストとポートを識別します。これにより、毎回新しいスキャン ターゲットを作成する必要がなくなります。スキャン ターゲットには、スキャンする 1 つの IP アドレスか IP アドレスのブロック、および 1 つ以上のホスト上のポートが含まれます。Nmap ターゲットの場合、Nmap オクテット範囲のアドレッシングや IP アドレスの範囲も使用できます。Nmap オクテットの範囲アドレッシングの詳細については、http://insecure.org にある Nmap のマニュアルを参照してください。

スキャン ターゲットに多数のホストが含まれている場合、スキャンに要する時間が延びる場合があることに注意してください。回避策として、一度にスキャンするホストを減らしてください。

スキャン ターゲットの作成後に変更または削除できます。

詳細については、次の項を参照してください。

- Nmap スキャン ターゲットの作成（47-11 ページ）
- スキャン ターゲットの編集（47-20 ページ）
- スキャン ターゲットの削除（47-21 ページ）

スキャン ターゲットの編集

ライセンス： FireSIGHT

作成したスキャン ターゲットを変更できます。

ヒント　修復を使用して特定の IP アドレスをスキャンするつもりがないのに、修復を起動した相関ポリシー違反にホストが関係していたためにその IP アドレスがターゲットに追加された場合は、修復の動的スキャン ターゲットを編集できます。

既存のスキャン ターゲットを編集する方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scanners] ページが表示されます。

ステップ 2　ツールバーで、[Targets] をクリックします。

[Scan Target List] ページが表示されます。

ステップ 3　編集するスキャン ターゲットの横にある [Edit] をクリックします。

[Scan Target] ページが表示されます。

ステップ 4　必要に応じて変更を加え、[Save] をクリックします。

スキャン ターゲットが更新されます。

スキャン ターゲットの削除

ライセンス：FireSIGHT

スキャン ターゲットにリストされているホストをスキャンする必要がなくなった場合は、そのスキャン ターゲットを削除します。

スキャン ターゲットを削除する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scanners] ページが表示されます。

ステップ 2　ツールバーで、[Targets] をクリックします。

[Scan Target List] ページが表示されます。

ステップ 3　削除するスキャン ターゲットの横にある [Delete] をクリックします。

スキャン ターゲットが削除されます。

アクティブ スキャンの結果での作業

ライセンス：FireSIGHT

進行中の Nmap スキャンをモニタする方法、FireSIGHT システムで以前に実行したスキャンからの結果か FireSIGHT システム以外で実行した結果をインポートする方法、およびスキャン結果を表示して分析する方法については、次の項を参照してください。

スキャン結果の表示

ライセンス：FireSIGHT

スキャン結果のテーブルを表示してから、探している情報に応じてイベント表示を操作できます。

スキャン結果にアクセスすると表示されるページは、使用するワークフローに応じて異なります。定義済みのワークフローを使用できます。このワークフローにはスキャン結果のテーブル ビューが含まれます。

特定の必要に合致する情報だけが表示されるカスタム ワークフローを作成することもできます。カスタム ワークフローの作成の詳細については、カスタム ワークフローの作成（58-43 ページ）を参照してください。

次の表で、スキャン結果ワークフローのページで実行できる特定のアクションの一部について説明します。

表 47-2　スキャン結果テーブルの機能

目的	操作
テーブルのカラムの内容について詳しく調べる	詳細については、スキャン結果テーブルについて（47-23 ページ）を参照してください。
スキャン結果の日時範囲の変更	時間範囲のリンクをクリックします。詳細については、イベント時間の制約の設定（58-26 ページ）を参照してください。
スキャン結果のソート	列のタイトルをクリックします。列のタイトルを再度クリックすると、ソート順序が逆になります。
表示される列の制約	非表示にする列見出しのクローズ アイコン（ ✖ ）をクリックします。表示されるポップアップ ウィンドウで、[Apply] をクリックします。 **ヒント**　その他の列を表示するには該当するチェック ボックスを選択し、非表示にするにはクリアしてから、[Apply] をクリックします。無効にした列を再度表示するには、 展開矢印（ ▶ ）をクリックして検索制約を展開してから、[Disabled Columns] の下の列名をクリックします。
特定の値を制約しながらのワークフロー内の次のページへのドリルダウン	次のいずれかの方法を使用します。 • カスタム ワークフローで作成したドリルダウン ページで、行内の値をクリックします。テーブル ビューの行内の値をクリックすると、テーブル ビューが制限され、次のページに**ドリルダウンされない**ことに注意してください。 • 一部のユーザに制限して次のワークフロー ページにドリルダウンするには、次のワークフロー ページに表示するユーザの横にあるチェック ボックスをオンにしてから、[View] をクリックします。 • 現在の制限を維持して次のワークフロー ページにドリルダウンするには、[View All] をクリックします。 **ヒント**　テーブル ビューでは、必ずページ名に「Table View」が含まれます。 詳細については、イベントの制約（58-35 ページ）を参照してください。

表 47-2　スキャン結果テーブルの機能（続き）

目的	操作
スキャン インスタンスと修復の設定	ツールバーの [Scanners] をクリックします。 詳細については、Nmap スキャンのセットアップ（47-10 ページ）を参照してください。
ワークフローのページ内やページ間の移動	詳細については、ワークフローのページの使用（58-21 ページ）を参照してください。
他のイベント ビューに移動して、関連イベントを確認する	表示するイベント ビューの名前を [Jump to] ドロップダウン リストから選択します。詳細については、ワークフロー間のナビゲート（58-40 ページ）を参照してください。
スキャン結果の検索	[Search] をクリックします。詳細については、スキャン結果の検索（47-25 ページ）を参照してください。

スキャン結果を表示する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

ステップ 2　[Scan Results] をクリックします。

デフォルトのスキャン結果ワークフローの先頭ページが表示されます。カスタム ワークフローなどの別のワークフローを使用するには、ワークフローのタイトルの付近の [(switch workflows)] をクリックします。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

スキャン結果テーブルについて

ライセンス：FireSIGHT

Nmap スキャンを実行すると、Defense Centerでデータベース内のスキャン結果が収集されます。スキャン結果テーブルのフィールドについて、以下の表で説明します。

表 47-3　スキャン結果のフィールド

フィールド	説明
Start Time	この結果を作成したスキャンの開始日時。
End Time	この結果を作成したスキャンの終了日時。
Scan Target	この結果を作成したスキャンのスキャン ターゲットの IP アドレス（DNS 解決が有効になっている場合はホスト名）。
Scan Type	この結果を作成したスキャンのタイプを示す、Nmap またはサードパーティのスキャナ名。

表 47-3　スキャン結果のフィールド（続き）

フィールド	説明
Scan Mode	この結果を作成したスキャンのモード： • `On Demand`：オン デマンドで実行されたスキャンからの結果。 • `Imported`：別のシステムでスキャンされてDefense Centerにインポートされた結果 • `Scheduled`：スケジュール済みタスクとして実行されたスキャンからの結果。

スキャン結果の分析

ライセンス：FireSIGHT

ローカル Nmap モジュールを使用して作成したスキャン結果を、レンダリングされたページとしてポップアップ ウィンドウで表示できます。Nmap 結果ファイルを raw XML 形式でダウンロードすることもできます。

Nmap によって検出されたオペレーティング システムやサーバの情報を、ホスト プロファイルやネットワーク マップ内で参照することもできます。ホストのスキャンが生成するサーバ情報がフィルタ除去されているかクローズ状態のポートのサーバに関する情報の場合、または、スキャンが収集した情報がオペレーティング システム情報やサーバのセクションに含めることができない情報の場合、それらの結果は、ホスト プロファイルの Nmap Scan Results セクションに含められます。詳細については、ホスト プロファイルの表示（49-5 ページ）を参照してください。

スキャンのモニタリング

ライセンス：FireSIGHT

Nmap スキャンの進行状況を検査し、現在進行中のスキャン ジョブをキャンセルできます。スキャン結果には各スキャンの開始時刻と終了時刻が示されます。またスキャンの完了後に、スキャン結果をレンダリングされたページとしてポップアップ ウィンドウで表示することもできます。Nmap は、http://insecure.org で入手できる Nmap バージョン 1.01 DTD を使用して、ダウンロードして表示できる結果を生成します。スキャン結果をクリアすることもできます。

スキャンをモニタする方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

ステップ 2　[Scan Results] をクリックします。

デフォルトのスキャン結果ワークフローの先頭ページが表示されます。カスタム ワークフローなどの別のワークフローを使用するには、ワークフローのタイトルの付近の [(switch workflows)] をクリックします。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

ヒント　スキャン結果のテーブル ビューが含まれていないカスタム ワークフローを使用している場合、ワークフローのタイトル付近の [(switch workflows)] をクリックしてから、[Scan Results] を選択します。

ステップ 3　次の操作を実行できます。

- スキャン結果をレンダリングされたページとしてポップアップ ウィンドウで表示するには、スキャン ジョブの横にある [View] をクリックします。
- テキスト エディタで raw XML コードを表示できるようにスキャン結果ファイルのコピーを保存するには、スキャン ジョブの横の [Download] をクリックします。

スキャン結果のインポート

ライセンス： FireSIGHT

FireSIGHT システムの外部で実行された Nmap スキャンによって作成された XML 結果ファイルをインポートできます。以前に FireSIGHT システムからダウンロードした XML 結果ファイルもインポートできます。Nmap スキャン結果をインポートするには、結果ファイルは XML 形式で、Nmap バージョン 1.01 DTD に準拠している必要があります。Nmap 結果の作成と Nmap DTD の詳細については、http://insecure.org にある Nmap のマニュアルを参照してください。FireSIGHT システムからの XML 結果のダウンロードの詳細については、スキャンのモニタリング（47-24 ページ）を参照してください。

Nmap がホスト プロファイルに結果を追加できるようにするには、その前にホストがネットワーク マップ内になければならないことに注意してください。

結果をインポートする方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scan Instances] ページが表示されます。

ステップ 2　ツールバーで、[Import Results] をクリックします。

[Import Results] ページが表示されます。

ステップ 3　[Browse] をクリックし、結果ファイルに移動します。

ステップ 4　[Import Results] ページに戻ったら、[Import] をクリックして結果をインポートします。

結果ファイルがインポートされます。

スキャン結果の検索

ライセンス： FireSIGHT

FireSIGHT システム内のアプライアンスや管理対象アプライアンスで実行した Nmap またはサードパーティのスキャン結果を検索できます。

表 47-4　スキャン結果の検索条件

フィールド	検索条件ルール
Start Time	この結果を作成したスキャンの開始日時を入力します。 時間入力の構文については、検索での時間制約の指定（60-5 ページ）を参照してください。
End Time	この結果を作成したスキャンの終了日時を入力します。 時間入力の構文については、検索での時間制約の指定（60-5 ページ）を参照してください。
Scan Target	この結果を作成したスキャンのスキャン ターゲットの IP アドレス（DNS 解決が有効になっている場合はホスト名）を入力します。 IP アドレスの範囲を指定するには、特定の IP アドレスか CIDR 表記を使用します。IP アドレスに使用できるシンタックスの完全な説明については、検索での IP アドレスの指定（60-6 ページ）を参照してください。
Scan Type	この結果を作成したスキャンのタイプを示す、`Nmap` またはサードパーティのスキャナ ID を入力します。
Scan Mode	この結果を作成したスキャンのモードを以下のように入力します。 • オン デマンドで実行されたスキャンからの結果を取得するには、`On Demand` と入力します。 • 別のシステムでスキャンされてDefense Centerにインポートされた結果を取得するには、`Imported` と入力します。 • スケジュール済みタスクとして実行されたスキャンからの結果を取得するには、`Scheduled` と入力します。

保存済み検索のロードおよび削除方法を含む、検索の詳細については、イベントの検索（60-1 ページ）を参照してください。

スキャン結果を検索する方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Analysis] > [Search] を選択してから、テーブルのドロップダウン リストから [Scan Results] を選択します。

[Scan Results] 検索ページが表示されます。

ヒント　データベース内で別の種類のイベントを検索するには、テーブルのドロップダウン リストから選択します。

ステップ 2　表スキャン結果の検索条件に記載されているように、該当するフィールドに検索基準を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。

ステップ 3　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　制約された権限を持つカスタム ユーザ ロールの制約として検索を保存する場合は、検索を非公開として保存する**必要があります**。

ステップ 4　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save As New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 5　検索を開始するには、[Search] ボタンをクリックします。

検索結果が表示されます。

ネットワーク マップの使用

FireSIGHT システムは、ネットワーク上を移動するトラフィックをパッシブに収集し、データを解釈し、設定されたオペレーティング システムおよびフィンガープリントと比較します。この情報から、システムはネットワークの詳細な表現である *ネットワーク マップ*を作成します。

ネットワーク マップではDefense Centerを使用して、ホストとネットワーク デバイス(ブリッジ、ルータ、NAT デバイス、ロード バランサ)に関するネットワーク トポロジを調べることができます。迅速にネットワークの全体を見るために便利なツールです。ネットワーク マップでは、関連付けられたホスト属性、アプリケーション、クライアント、セキュリティ侵害を受けたホストの痕跡、脆弱性をドリルダウンできます。つまり、実行する分析に合わせて、ネットワーク マップのビューを選択できます。

ホスト入力機能を使用して、サードパーティ製アプリケーションから、オペレーティング システム、アプリケーション、クライアント、プロトコル、またはホスト属性情報を追加して、システムが収集する情報を増やすことができます。また、Nmap を使用してアクティブにネットワーク マップのホストをスキャンして、ネットワーク マップにスキャン結果を追加できます。

ネットワーク マップのビューでサブネットを整理および識別するために、カスタム トポロジ機能を使用できます。たとえば、組織の各部署が異なるサブネットを使用している場合、カスタム トポロジ機能を使用して、そのサブネットに分かりやすいラベルを割り当てることができます。

詳細については、次の項を参照してください。

ネットワーク マップの概要

ライセンス：FireSIGHT

ネットワーク マップの各ビューは、展開可能なカテゴリおよびサブカテゴリの階層ツリーからなる、同一の形式です。カテゴリをクリックすると、展開されて、その下のサブカテゴリが表示されます。実行する分析の種類に応じて、ネットワーク マップの異なるビューを選択できます。

Defense Centerは、ディスカバリ ポリシーが適用されているすべてのセキュリティ ゾーン（NetFlow 対応デバイスからのデータを処理するゾーンを含む）からデータを収集します。複数のデバイスが同じネットワーク資産を検出した場合、Defense Centerは情報をまとめて資産を複合表示します。

NetFlow 対応デバイスによってエクスポートされるデータを追加するようネットワーク検出ポリシーを設定できますが、これらのホストに関して利用可能な情報は限られています。たとえば、これらのホストのオペレーティング システム データは得られません（ただしホスト入力機能を使って指定する場合を除く）。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

任意のネットワーク マップで任意のホストの*ホスト プロファイル*を参照できます。システムによって収集されたホストのすべての情報の完全なビューを提供します。ホスト プロファイルには、ホスト名、オペレーティング システム、およびすべての関連付けられた IP アドレスといった一般情報と、検出されたプロトコル、アプリケーション、セキュリティ侵害の痕跡、およびホスト上で実行しているクライアントといった固有情報が含まれます。ホスト プロファイルには、ホストと検出された資産に関連付けられた脆弱性に関する情報も含まれます。ホスト プロファイルの詳細については、ホスト プロファイルの使用（49-1 ページ）を参照してください。

調査する必要がなくなった項目はネットワーク マップから削除できます。ネットワーク マップからホストとアプリケーションを削除できます。また、脆弱性を削除または非アクティブ化できます。システムは、削除されたホストに関連付けられたアクティビティを検出した場合は、ネットワーク マップにホストを再追加します。同様に、削除したアプリケーションは、システムがアプリケーションの変更（たとえば Apache Web サーバが新しいバージョンにアップグレードされた）を検出すると、アプリケーションのネットワーク マップに再追加されます。システムがホストを脆弱にする変更を検出すると、そのホストの脆弱性は再アクティブ化されます。

また、ネットワーク マップを使用して、ネットワーク全体の脆弱性を非アクティブにできます。これにより、システムが脆弱と判断したホストについて、その特定の攻撃や悪用の心配がないとみなすことになります。

ヒント　ネットワーク マップからホストまたはサブネットを永続的に除外するには、ネットワーク検出ポリシーを変更します。モニタリング対象からロード バランサおよび NAT デバイスを除外する必要がある場合があります。これらは、多数のイベントおよび誤った結果をもたらすイベントを生成して、データベースを一杯にしたり、Defense Centerをオーバーロードさせたりする可能性があります。詳細については、「ホスト データ収集について（45-2 ページ）」を参照してください。

ホストのネットワーク マップの使用

ライセンス：FireSIGHT

ホストのネットワーク マップを使用して、サブネットによって階層ツリーに整理されたネットワークのホストを参照でき、特定のホストのホスト プロファイルにドリルダウンできます。このネットワーク マップ ビューは、ホストに 1 つの IP アドレスまたは複数の IP アドレスがあるかを問わず、システムによって検出されたすべての一意のホスト数を表示します。

NetFlow 対応デバイスによってエクスポートされるデータに基づいてホストをネットワーク マップに追加するようネットワーク検出ポリシーを設定できますが、これらのホストについて利用可能な情報は限られています。たとえば、ホスト入力機能を使用してデータが提供されていない限り、NetFlow データを使用してネットワーク マップに追加されたホストに関して利用可能なオペレーティング システム データはありません。

ネットワークのカスタム トポロジを作成して、サブネットに意味のあるラベル（部門名など）を割り当てることができます。これはホストのネットワーク マップで表示されます。

また、カスタム トポロジで指定した組織に基づいてホストのネットワーク マップを表示できます。カスタム ネットワーク トポロジの使用（48-11 ページ）を参照してください。

ホストのネットワーク マップからネットワーク全体、サブネット、または個々のホストを削除できます。ホストがネットワークに接続されていないことがわかっている場合など、分析を効率化するためにネットワーク マップから削除できます。システムは削除されたホストに関連付けられたアクティビティを後で検出すると、ネットワーク マップにホストを再追加します。ネットワーク マップからホストまたはサブネットを永続的に除外するには、ネットワーク検出ポリシーを変更します。詳細については、「ネットワーク検出ポリシーの作成（45-25 ページ）」を参照してください。

注　Ciscoは、ネットワーク マップからネットワーク デバイスを削除**しない**ことを**強く**推奨します。システムはその場所を使用してネットワーク トポロジを特定するからです（モニタリング対象ホスト用のネットワーク ホップと TTL 値の生成を含む）。ネットワーク デバイスのネットワーク マップからはネットワーク デバイスを削除できませんが、ホストのネットワーク マップからネットワーク デバイスを削除しないようにしてください。

ホストのネットワーク マップを表示するには、次の手順を実行します。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Hosts] > [Network Map] を選択し、[Hosts] タブを選択します。

ホストのネットワーク マップが開き、ホスト数と、ホストの IP アドレスと MAC アドレスのリストが表示されます。各アドレスまたはアドレスの一部は、次のレベルへのリンクです。

ステップ 2　調査するホストの IP アドレスまたは MAC アドレスにドリルダウンします。

たとえば、IP アドレス 192.168.40.11 のホストを表示するには、**192**、**192.168**、**192.168.40**、**192.168.40.11** の順にクリックします。**192.168.40.11** をクリックすると、ホスト プロファイルが表示されます。ホスト プロファイルの詳細については、ホスト プロファイルの使用（49-1 ページ）を参照してください。

IP または MAC アドレスでフィルタリングするには、検索フィールドにアドレスを入力します。検索をクリアするには、クリア アイコン（ ）をクリックします。

ステップ 3　オプションで、サブネット、IP アドレス、または MAC アドレスを削除するには、削除する要素の隣にある削除アイコン（ ）をクリックし、ホストまたはサブネットを削除することを確認します。

ホストが削除されます。システムはホストを再検出すると、ネットワーク マップにホストを再追加します。

ステップ 4　オプションで、ホストのネットワーク マップのホスト ビューとトポロジー ビューを切替えます。

- カスタム トポロジで整理されたホストのネットワーク マップのビューに切替えるには、ホスト ビュー（デフォルト）で、ネットワーク マップの一番上にある [(topology)] をクリックします。

- サブネットで整理されたホストのネットワーク マップのビューに切替えるには、トポロジ ビューで、ネットワーク マップの一番上にある [(hosts)] をクリックします。

カスタム トポロジの設定については、カスタム ネットワーク トポロジの使用（48-11 ページ）を参照してください。

ネットワーク デバイスのネットワーク マップの使用

ライセンス： FireSIGHT

ネットワークのセグメント同士を接続するネットワーク デバイス（ブリッジ、ルータ、NAT デバイス、ロード バランサ）を表示するため、またそのネットワーク デバイスのホスト プロファイルにドリルダウンするために、ネットワーク デバイスのネットワーク マップを使用します。ネットワーク デバイスのネットワーク マップは、IP および MAC という 2 つの部分に分けられます。IP セクションは IP アドレスで識別されたネットワーク デバイスのリストを表示します。MAC の部分は MAC アドレスで識別されるネットワーク デバイスを示します。また、このネットワーク マップ ビューは、デバイスに 1つの IP アドレスまたは複数の IP アドレスがあるかを問わず、システムによって検出されたすべての一意のネットワーク デバイスの数を表示します。

ネットワークのカスタム トポロジを作成した場合、サブネットに割り当てたラベルはネットワーク デバイスのネットワーク マップに表示されます。

ネットワーク デバイスを区別するためにシステムでは次の方法を使用します。

- Cisco Discovery Protocol（CDP）メッセージの分析。ネットワーク デバイスと種類を特定します（シスコ デバイスのみ）。
- スパニング ツリー プロトコル（STP）の検出。デバイスをスイッチまたはブリッジとして識別します。
- 同じ MAC アドレスを使用している複数のホストの検出。MAC アドレスを、ルータに属しているものとして識別します。
- クライアント側からの TTL 値の変更、または通常のブート時間よりも頻繁に変更されている TTL 値の検出。この検出では、NAT デバイスとロード バランサを識別します。

ネットワーク デバイスが CDP を使用して通信している場合、1 つ以上の IP アドレスを持っている可能性があります。STP を使用して通信している場合は、1 つの MAC アドレスのみを持っている可能性があります。

ネットワーク マップからネットワーク デバイスを削除することはできません。システムはその場所を使用してネットワーク トポロジを特定するからです（モニタリング対象ホスト用のネットワーク ホップと TTL 値の生成を含む）。

ネットワーク デバイスのホスト プロファイルには、[Operating Systems] セクションではなく、ネットワーク デバイスの背後で検出されたモバイル デバイスのハードウェア プラットフォームを反映する [Hardware] カラムを含む [Systems] セクションがあります。[Systems] の下にハードウェア プラットフォームの値が表示され場合、システムは、ネットワーク デバイスの背後で 1 つ以上のモバイル デバイスが検出されたことを示しています。モバイル デバイスはハードウェア プラットフォームの情報を持っていることも、持っていないこともありますが、モバイル デバイスではないシステムではハードウェア プラットフォーム情報は検出されないことに注意してください。

ネットワーク デバイスのネットワーク マップを表示するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Hosts] > [Network Map] > [Network Devices] を選択します。

ネットワーク デバイスのネットワーク マップが開き、一意のネットワーク デバイスの数と、ネットワーク デバイスの IP アドレスと MAC アドレスのリストを表示します。各アドレスまたはアドレスの一部は、アドレスの次のレベルか、各ホストのホスト プロファイルへのリンクです。

ステップ 2　調査するネットワーク デバイスの IP アドレスまたは MAC アドレスにドリルダウンします。

ネットワーク デバイスのホスト プロファイルが表示されます。ホスト プロファイルの詳細については、ホスト プロファイルの使用（49-1 ページ）を参照してください。

ステップ 3　オプションで、IP または MAC アドレスでフィルタリングをするには、検索フィールドにアドレスを入力します。検索をクリアするには、クリア アイコン（ ）をクリックします。

セキュリティ侵害の痕跡のネットワークのマップの使用

ライセンス：FireSIGHT

セキュリティ侵害の痕跡（IOC）のネットワーク マップを使用して、ネットワーク上の侵害されたホストを IOC のカテゴリで整理して表示します。影響を受けているホストは各カテゴリの下に表示されます。

システムは、ホストのセキュリティ侵害のステータスを判断するために、侵入イベント、Security Intelligence、FireAMP を含む複数のソースからのデータを使用します。

セキュリティ侵害の痕跡のネットワーク マップから、何らかのセキュリティ侵害を受けたと判断される各ホストのホスト プロファイルを表示できます。さらに、IOC カテゴリまたは特定のホストを削除でき（解決済みにする）、これによって当該ホストから IOC タグが削除されます。たとえば、問題が対応済みで、繰り返し発生する可能性が低いと判断した場合に、IOC カテゴリをネットワーク マップから削除できます。

ネットワーク マップのホストや IOC カテゴリを解決済みにしても、ネットワークからは削除されません。システムがその IOC をトリガーする情報を新たに検出すると、解決済みのホストまたは IOC カテゴリはネットワーク マップに再表示されます。

セキュリティ侵害の痕跡のネットワーク マップを表示するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Hosts] > [Network Map] > [Indications of Compromise] を選択します。

セキュリティ侵害の痕跡のネットワーク マップが表示されます。

ステップ 2　調査する IOC カテゴリをクリックします。

たとえば、マルウェアが検出されたホストを表示するには、[Malware Detected] をクリックします。

IP または MAC アドレスでフィルタリングするには、検索フィールドにアドレスを入力します。検索をクリアするには、クリア アイコン（ ）をクリックします。

ステップ 3　選択した IOC カテゴリで、特定の IP アドレスへドリルダウンします。各アドレスまたはアドレスの一部は、次のレベルへのリンクです。

セキュリティ侵害を受けたホストのホスト プロファイルが表示され、セキュリティ侵害の痕跡のセクションが展開されます。ホスト プロファイルの IOC セクションの詳細については、ホスト プロファイルでの侵害の痕跡の使用（49-9 ページ）を参照してください。

ステップ 4　オプションで、IOC カテゴリ、セキュリティ侵害を受けたホスト、またはセキュリティ侵害を受けたホストのグループを解決済みにするには、解決する要素の隣にある削除アイコン（ ）をクリックし、それを解決することを確認します。

カテゴリまたはホストが解決されます（IOC タグが削除されます）。その IOC が再度トリガーされると、ネットワーク マップに再追加されます。

モバイル デバイスのネットワーク マップの使用

ライセンス： FireSIGHT

ネットワークに接続されたモバイル デバイスを表示するため、またそのデバイスのホスト プロファイルにドリルダウンするために、モバイル デバイスのネットワーク マップを使用します。また、このネットワーク マップ ビューは、デバイスに 1 つの IP アドレスまたは複数の IP アドレスがあるかを問わず、システムによって検出されたすべての一意のモバイル デバイスの数を表示します。

モバイル デバイスを区別するためにシステムでは次の方法を使用します。

- モバイル デバイスのモバイル ブラウザからの HTTP トラフィックのユーザ エージェント ストリングの分析
- 特定のモバイル アプリケーションの HTTP トラフィックのモニタリング

ネットワークのカスタム トポロジを作成した場合、サブネットに割り当てたラベルはモバイル デバイスのネットワーク マップに表示されます。

モバイル デバイスのネットワーク マップを表示するには、次の手順を実行します。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Hosts] > [Network Map] を選択し、[Mobile Devices] タブを選択します。

モバイル デバイスのネットワーク マップが開き、一意のモバイル デバイスの数と、モバイル デバイスの IP アドレスと MAC アドレスのリストを表示します。各アドレスまたはアドレスの一部は、次のレベルへのリンクです。

ステップ 2　調査するモバイル デバイスの特定の IP アドレスにドリルダウンします。

たとえば、IP アドレス 10.11.40.11 のデバイスを表示するには、**10**、**10.11**、**10.11.40**、**10.11.40.11** の順にクリックします。**10.11.40.11** をクリックすると、ホスト プロファイルが表示されます。ホスト プロファイルの詳細については、ホスト プロファイルの使用（49-1 ページ）を参照してください。

IP または MAC アドレスでフィルタリングするには、検索フィールドにアドレスを入力します。検索をクリアするには、クリア アイコン（ ）をクリックします。

ステップ 3　オプションで、サブネットまたは IP アドレスを削除するには、削除する要素の隣にある削除アイコン（ ）をクリックし、デバイスまたはサブネットを削除することを確認します。

デバイスが削除されます。システムはデバイスを再検出すると、ネットワーク マップにデバイスを再追加します。

アプリケーションのネットワーク マップの使用

ライセンス： FireSIGHT

アプリケーションのネットワーク マップを使用して、アプリケーション名、ベンダー、バージョン、さらには各アプリケーションを実行するホストによって階層ツリーに整理された、ネットワークのアプリケーションを参照できます。

システムが検出するアプリケーションは、システム ソフトウェアおよび VDB アップデートによって、およびアドオン ディテクタをインポートした場合に変わることがあります。各システムまたは VDB アップデートのリリース ノートまたはアドバイザリ テキストには、新規および更新されたディテクタの情報が含まれています。ディテクタの全般的な情報を含む最新のリストについては、次のサポート サイトのいずれかを参照してください。

- **シスコ：**（http://www.cisco.com/cisco/web/support/index.html）

アプリケーションのネットワーク マップから、特定のアプリケーションを実行する各ホストのホスト プロファイルを表示できます。また、アプリケーション カテゴリ、すべてのホストで実行されているアプリケーション、特定のホストで実行されているアプリケーションを削除することもできます。たとえば、あるアプリケーションがホスト上で無効化されているとわかっており、システムによる影響レベルの認定で使用されないようにする場合は、そのアプリケーションをネットワーク マップから削除できます。

ネットワーク マップからアプリケーションを削除しても、ネットワークからは削除されません。削除したアプリケーションは、システムがアプリケーションの変更（たとえば Apache Web サーバが新しいバージョンにアップグレードされた）を検出するか、ユーザがシステムの検出機能を再起動すると、ネットワーク マップに再表示されます。

何を削除するかによって、動作は次のように異なります。

- アプリケーション カテゴリを削除すると、そのアプリケーション カテゴリはネットワーク マップから削除されます。カテゴリの下にあるすべてのアプリケーションは、そのアプリケーションを含むすべてのホスト プロファイルから削除されます。

  たとえば、[http] を削除した場合、[http] として示されるすべてのアプリケーションがすべてのホスト プロファイルから削除され、[http] はネットワーク マップのアプリケーション ビューに表示されなくなります。

- 特定のアプリケーション、ベンダー、またはバージョンを削除すると、影響を受けるアプリケーションは、ネットワーク マップと、それを含むホスト プロファイルから削除されます。

  たとえば、[http] カテゴリを展開し、[Apache] を削除すると、[Apache] としてリストされているすべてのアプリケーションは、[Apache] の下にリストされているバージョンを問わず、それらを含むホスト プロファイルから削除されます。同様に、[Apache] を削除する代わりに、特定のバージョン（[1.3.17] など）を削除すると、影響を受けるホスト プロファイルから、選択されたバージョンだけが削除されます。

- 特定の IP アドレスを削除する場合、IP アドレスはアプリケーション リストから削除され、アプリケーション自体は、選択した IP アドレスのホスト プロファイルから削除されます。

  たとえば、[http]、[Apache]、[1.3.17 (Win32)] の順に展開し、**[172.16.1.50:80/tcp]** を削除すると、Apache 1.3.17（Win32）アプリケーションは IP アドレス 172.16.1.50 のホスト プロファイルから削除されます。

アプリケーションのネットワーク マップを表示するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Hosts] > [Network Map] > [Applications] を選択します。

アプリケーションのネットワーク マップが表示されます。

ステップ 2　調査する特定のアプリケーションにドリルダウンします。

たとえば、Apache など特定のタイプの Web サーバを表示する場合は、[http] をクリックし、[Apache] をクリックして、表示する Apache Web サーバのバージョンをクリックします。

IP または MAC アドレスでフィルタリングするには、検索フィールドにアドレスを入力します。検索をクリアするには、クリア アイコン（ ）をクリックします。

ステップ 3　選択したアプリケーションの特定の IP アドレスをクリックします。

アプリケーションを実行しているホストのホスト プロファイルが表示され、アプリケーション セクションが展開されます。ホスト プロファイルのアプリケーション セクションの詳細については、ホスト プロファイルでのサーバの使用（49-16 ページ）を参照してください。

ステップ 4　オプションで、アプリケーション カテゴリ、すべてのホストで実行されているアプリケーション、または特定のホストで実行されているアプリケーションを削除するには、削除する要素の隣にある削除アイコン（ ）をクリックし、削除することを確認します。

アプリケーションが削除されます。システムはアプリケーションを再検出すると、ネットワーク マップに再追加します。

脆弱性のネットワーク マップの使用

ライセンス：FireSIGHT

脆弱性のネットワーク マップを使用して、システムがネットワーク上で検出した脆弱性を従来の脆弱性 ID（SVID）、Bugtraq ID、CVE ID、または Snort ID 別に表示します。脆弱性は ID 番号によって並べられ、影響を受けるホストが各脆弱性の下にリストされます。

脆弱性のネットワーク マップから、特定の脆弱性の詳細を表示できます。また、特定の脆弱性の影響を受けるホストのホスト プロファイルを表示できます。これは、影響を受ける特定のホストの脆弱性によって生じる脅威を評価するために役立ちます。

特定の脆弱性がネットワーク上のホストに該当しないと見なす場合（パッチを適用済みの場合など）、その脆弱性を非アクティブ化できます。非アクティブ化された脆弱性はネットワーク マップに表示されますが、これまで影響を受けていたホストの IP アドレスはグレーのイタリック体で表示されます。これらのホストのホスト プロファイルでは、非アクティブ化した脆弱性は無効として表示されますが、個々のホストについて手動で有効にすることができます。詳細については、個々のホストに対する脆弱性の設定（49-33 ページ）を参照してください。

ホスト上のアプリケーションまたはオペレーティング システムのアイデンティティの競合がある場合、システムは候補となるアイデンティティの両方について脆弱性を表示します。アイデンティティの競合が解決した場合、脆弱性は現在のアイデンティティに関連付けされたままになります。詳細については、現在の ID について（46-5 ページ）およびID の競合について（46-7 ページ）を参照してください。

デフォルトでは、パケットにアプリケーションのベンダーおよびバージョンが含まれていた場合にのみ、検出されたアプリケーションの脆弱性が脆弱性のネットワーク マップに表示されます。ただし、システム ポリシーでアプリケーションの脆弱性マッピングの設定を有効化すること

で、ベンダーおよびバージョンのデータがないアプリケーションの脆弱性をリストするようにシステムを設定できます。アプリケーションの脆弱性マッピングの設定の詳細については、サーバの脆弱性のマッピング（63-32 ページ）を参照してください。

脆弱性 ID（または脆弱性 ID の範囲）の隣の数字は、次の 2 つの数を示します。

- 最初の数字は、1 つまたは複数の脆弱性の影響を受ける、一意でないホストの数です。ホストが複数の脆弱性の影響を受ける場合、複数回カウントされます。したがって、この数字がネットワーク上のホスト数を上回ることもあります。脆弱性を非アクティブ化すると、その脆弱性の影響を受ける可能性のあるホスト数の分、この数が減ります。1 つまたは複数の脆弱性の影響を受ける可能性のあるホストについて、脆弱性を 1 つも非アクティブ化していない場合、この数は表示されません。
- 2 番目の数字は、1 つまたは複数の脆弱性の影響を受ける *可能性がある* とシステムが判断した、一意でないホストの総数とほぼ同じ数です。

脆弱性を非アクティブ化すると、ユーザが指定したホストについてのみ非アクティブになります。脆弱と判断されたすべてのホストか、指定した個々の脆弱なホストの脆弱性を非アクティブ化することができます。その後でシステムが非アクティブ化されていないホストに脆弱性を検出すると（たとえば、ネットワーク マップの新しいホスト）、システムはそのホストの脆弱性をアクティブ化します。新たに検出された脆弱性は明示的に非アクティブ化する必要があります。また、システムはホストのオペレーティング システムまたはアプリケーションの変更を検出すると、非アクティブ化されている関連付けられた脆弱性を再アクティブ化することがあります。

脆弱性のネットワーク マップを表示するには、次の手順を実行します。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Hosts] > [Network Map] > [Vulnerabilities] を選択します。

脆弱性のネットワーク マップが表示されます。

ステップ 2　[Type] ドロップダウン リストから、表示する脆弱性のクラスを選択します。デフォルトでは、脆弱性は従来の脆弱性 ID（SVID）ごとに表示されます。

ステップ 3　調査する特定の脆弱性にドリルダウンします。

IP または MAC アドレスでフィルタリングするには、検索フィールドにアドレスを入力します。検索をクリアするには、クリア アイコン（ ）をクリックします。

脆弱性の詳細が表示されます。表示される情報の詳細については、脆弱性の詳細の表示（49-30 ページ）を参照してください。

さらにネットワーク マップでは、影響を受けるホストの IP アドレスがDefense Centerによって表示されます。任意の IP アドレスをクリックして、そのホストのホスト プロファイルを表示できます。

ステップ 4　オプションで、脆弱性を非アクティブ化します。

- 脆弱性の影響を受けるすべてのホストの脆弱性を非アクティブ化するには、脆弱性番号の隣にある削除アイコン（ ）をクリックします。
- 個々のホストの脆弱性を非アクティブ化するには、ホストの IP アドレスの隣にある削除アイコン（ ）をクリックします。

脆弱性が非アクティブになります。該当するホストの IP アドレスは、ネットワーク マップにグレーの斜体で表示されます。さらに、これらのホストのホスト プロファイルでは、非アクティブ化された脆弱性を無効として表示します。

ヒント　脆弱性の再アクティブ化の詳細については、個々のホストに対する脆弱性の設定（49-33 ページ）を参照してください。

ホスト属性のネットワーク マップの使用

ライセンス： FireSIGHT

ホスト属性のネットワーク マップを使用して、ネットワーク上のホストをホスト属性で整理して表示します。ホストを整理するために使用するホスト属性を選択すると、Defense Centerはネットワーク マップで使用可能なその属性の値をリストし、割り当てられた値に基づいてホストをグループ化します。また、特定のホスト属性値が割り当てられた任意のホストのホスト プロファイルを表示することもできます。

ホスト属性のネットワーク マップでは、ユーザ定義のホスト属性に基づいてホストを整理できます。これらの属性について、ネットワーク マップは値が Unassigned として割り当てられていないホストを表示します。

詳細については、ユーザ定義のホスト属性の使用（49-35 ページ）を参照してください。

さらに、ホスト属性のネットワーク マップは、ユーザが作成したコンプライアンス ホワイト リストに対応するホスト属性に基づいてホストを整理できます。ユーザが作成するコンプライアンス ホワイト リストごとに、各ホワイト リストと同じ名前でホスト属性が自動的に作成されます。

ホワイト リストのホスト属性がとり得る値は次の通りです。

- `Compliant`は、ホワイト リストに準拠しているホスト
- `Non-Compliant` は、ホワイト リストに違反しているホスト
- `Not Evaluated` は、ホワイトリストの有効な対象でないか、または何らかの理由で評価されていないホスト

コンプライアンス ホワイト リストの詳細については、FireSIGHT システムのコンプライアンス ツールとしての使用（52-1 ページ）を参照してください。

注　ホスト属性のネットワーク マップでは、事前定義されたホスト属性（ホストの重要度など）を使用して、ホストを整理することはできません。

ホスト属性のネットワーク マップを表示するには、次の手順を実行します。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Hosts] > [Network Map] > [Host Attributes] を選択します。

ホスト属性のネットワーク マップが表示されます。

ステップ 2　[Attribute] ドロップダウン リストから、ホスト属性を選択します。

Defense Centerはホスト属性の値をリストし、その値が割り当てられたホストの数を括弧内に表示します。

IP または MAC アドレスでフィルタリングするには、検索フィールドにアドレスを入力します。検索をクリアするには、クリア アイコン（ ✖ ）をクリックします。

ステップ 3　ホスト属性値をクリックすると、その値が割り当てられたホストが表示されます。

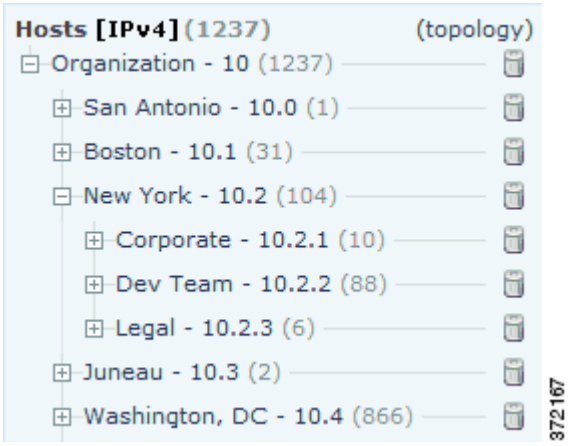
ステップ 4　ホストの IP アドレスをクリックすると、そのホストのホスト プロファイルが表示されます。

カスタム ネットワーク トポロジの使用

ライセンス：FireSIGHT

ホストおよびネットワーク デバイスのネットワーク マップでサブネットを整理および識別するために、カスタム トポロジ機能を使用します。

たとえば、組織内の各部署が異なるサブネットを使用している場合、カスタム トポロジ機能を使用して、これらのサブネットにラベルを付けられます。こうすることで、ホストまたはネットワーク デバイスのネットワーク マップを参照する際に、サブネットに割り当てたラベルが次の図のように表示されます。



また、カスタム トポロジで指定した組織に基づいてホストのネットワーク マップを表示することもできます。

ホストおよびネットワーク デバイスのネットワーク マップの詳細については、ホストのネットワーク マップの使用 (48-2 ページ)およびネットワーク デバイスのネットワーク マップの使用 (48-4 ページ)を参照してください。

詳細については、次の項を参照してください。

- カスタム トポロジの作成（48-12 ページ）
- カスタム トポロジの管理（48-15 ページ）

カスタム トポロジの作成

ライセンス：FireSIGHT

カスタム トポロジを作成するには、ネットワークを指定する必要があります。これには、次の 3 つの方法のいずれかまたはすべてを使用します。

- Ciscoが検出したトポロジのインポート。システムによって検出されたホストとネットワーク デバイスに基づいて推測した、最も正確と考えられるネットワークの展開を使用して、ネットワークを追加します。
- ネットワーク検出ポリシーからのネットワークのインポート。ネットワーク検出ポリシーで、FireSIGHT システムのモニタリング対象として設定したネットワークを追加します。
- ネットワークのトポロジへの手動追加。他の 2 つの方法で作成される展開の表現が不正確または不完全な場合に使用します。

トポロジをネットワーク マップで使用するには、トポロジを保存してアクティブ化する必要があります。

カスタム トポロジを作成するには、次の手順を実行します。

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] を選択し、[Custom Topology] を選択します。

[Custom Topology] ページが表示されます。

ステップ 2　[Create Topology] をクリックします。

[Create Topology] ページが表示されます。

ステップ 3　トポロジ名や説明など、基本的なトポロジ情報を入力します。

基本的なトポロジ情報の入力（48-13 ページ）を参照してください。

ステップ 4　トポロジにネットワークを追加します。次の方法のいずれかまたはすべてを使用できます。

- Ciscoが検出したトポロジをインポートしてネットワークをトポロジに追加する場合は、検出されたトポロジのインポート（48-13 ページ）の手順に従います。
- ネットワーク検出ポリシーからインポートすることによってトポロジにネットワークを追加するには、ネットワーク検出ポリシーからのネットワークのインポート（48-14 ページ）の手順を参照してください。
- トポロジにネットワークを手動で追加するには、手動によるカスタム トポロジへのネットワークの追加（48-15 ページ）の手順に従います。

ステップ 5　トポロジを修正するには、次の手順を実行します。

- カスタム トポロジからネットワークを削除するには、削除するネットワークの隣にある [Delete] をクリックします。
- ネットワークの名前を変更するには、ネットワークの隣にある [Rename] をクリックします。表示されるポップアップ ウィンドウで、[Name] フィールドに新しい名前を入力し、[Rename] をクリックします。この名前のラベルが、ネットワーク マップのネットワークに付けられます。

ステップ 6　[Save] をクリックします。

トポロジが保存されます。

注　ネットワーク マップでこのトポロジを使用するには、アクティブ化する必要があります。詳細については、カスタム トポロジの管理（48-15 ページ）を参照してください。

基本的なトポロジ情報の入力

ライセンス：FireSIGHT

各カスタム トポロジに、名前と必要に応じて簡単な説明を入力します。

基本的なトポロジ情報を入力するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[Edit Topology] ページで、[Name] フィールドにトポロジの名前を入力します。

ステップ 2　オプションで、[Description] フィールドにトポロジの説明を入力します。

ステップ 3　オプションで、カスタム トポロジをどのように構築するかに応じて、以降のセクションの手順に進みます。

- 検出されたトポロジのインポート（48-13 ページ）
- ネットワーク検出ポリシーからのネットワークのインポート（48-14 ページ）
- 手動によるカスタム トポロジへのネットワークの追加（48-15 ページ）

検出されたトポロジのインポート

ライセンス：FireSIGHT

カスタム トポロジにネットワークを追加する方法の 1 つは、FireSIGHT システムによって検出されたトポロジをインポートすることです。この検出されたトポロジは、検出されたホストとネットワーク デバイスに基づいてシステムが推測した、最も正確と考えられるネットワークの展開です。

検出されたトポロジをインポートするには、次の手順を実行します。

アクセス：Admin

ステップ 1　[Edit Topology] ページで、[Import Discovered Topology] をクリックします。

ステップ 2　検出されたネットワークがページに示されます。

ステップ 3　オプションで、カスタム トポロジをどのように構築するかに応じて、以降のセクションの手順に進みます。

- 検出されたトポロジのインポート（48-13 ページ）
- ネットワーク検出ポリシーからのネットワークのインポート（48-14 ページ）
- 手動によるカスタム トポロジへのネットワークの追加（48-15 ページ）

ネットワーク検出ポリシーからのネットワークのインポート

ライセンス：FireSIGHT

カスタム トポロジにネットワークを追加する方法の 1 つは、ネットワーク検出ポリシーで FireSIGHT システムのモニタリング対象として設定したネットワークをインポートすることです。ネットワーク検出ポリシーの作成（45-25 ページ）を参照してください。

ネットワーク検出ポリシーからネットワークをインポートするには、次の手順を実行します。

アクセス：Admin

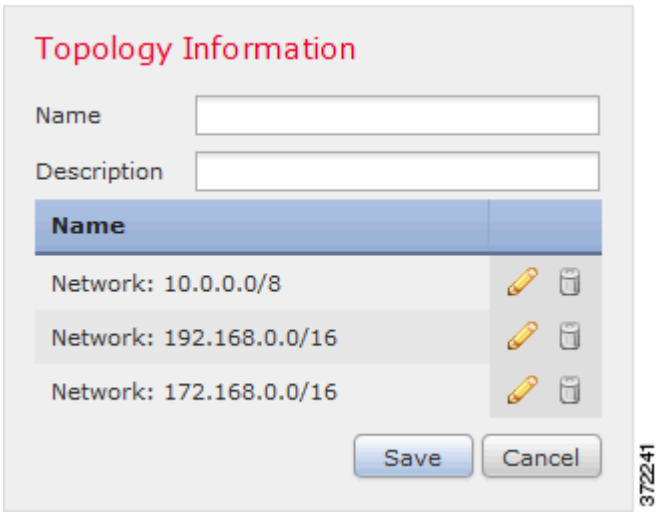
ステップ 1　[Edit Topology] ページで、[Import Policy Networks] をクリックします。

ポップアップ ウィンドウが表示されます。

ステップ 2　ドロップダウン リストから、使用するネットワーク検出ポリシーを選択し、[Load] をクリックします。

ステップ 3　ネットワーク検出ポリシーのモニタリング対象ネットワークがページに示されます。

たとえば、10.0.0.0/8、192.168.0.0/16、172.12.0.0/16 のネットワークをモニタするようにネットワーク検出ポリシーを設定すると、そのネットワークがページに表示されます。



ステップ 4　別のネットワーク検出ポリシーからネットワークを追加するには、手順 1 と 2 を繰り返します。

ステップ 5　オプションで、カスタム トポロジをどのように構築するかに応じて、以降のセクションの手順を実行します。

- 検出されたトポロジのインポート（48-13 ページ）
- 手動によるカスタム トポロジへのネットワークの追加（48-15 ページ）

手動によるカスタム トポロジへのネットワークの追加

ライセンス：FireSIGHT

Ciscoが検出したトポロジのインポートや、ネットワーク検出ポリシーからのネットワークのインポートによって、ネットワーク配置が不正確または不完全に表示される場合は、カスタム トポロジにネットワークを手動で追加できます。

ネットワークをカスタム トポロジに手動で追加するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[Edit Topology] ページで、[Add Network] をクリックします。

ポップアップ ウィンドウが表示されます。

ステップ 2　オプションで、[Name] フィールドに名前を入力してネットワークに名前を付けます。

この名前のラベルが、トポロジをアクティブ化した後で、ホストおよびネットワーク デバイスのネットワーク マップのネットワークに付けられます。

詳細については、ホストのネットワーク マップの使用（48-2 ページ）およびネットワーク デバイスのネットワーク マップの使用（48-4 ページ）を参照してください。

ステップ 3　[IP Address] フィールドと [Netmask] フィールドに、トポロジに追加するネットワークを表す IP アドレスとネットワーク マスク（CIDR 表記）を入力します。

FireSIGHT システムでの CIDR 表記の使用法の詳細については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ステップ 4　[Add] をクリックします。

ネットワークがトポロジに追加されます。

ステップ 5　トポロジにさらにネットワークを追加するには、手順 1 ～ 4 を繰り返します。

ヒント　トポロジからネットワークを削除するには、削除するネットワークの隣にある [Delete] をクリックし、ネットワークと、ネットワークへのすべてのリンクを削除することを確認します。

ステップ 6　オプションで、カスタム トポロジをどのように構築するかに応じて、以降のセクションの手順を実行します。

- 検出されたトポロジのインポート（48-13 ページ）
- ネットワーク検出ポリシーからのネットワークのインポート（48-14 ページ）

カスタム トポロジの管理

ライセンス：FireSIGHT

カスタム トポロジの管理には [Custom Topology] ページを使用します。トポロジを作成、変更、削除できます。

トポロジの状態が名前とともに表示されます。ポリシー名の隣の電球アイコンが点灯している場合、そのトポロジはアクティブで、ネットワーク マップに影響します。消灯している場合、トポロジは非アクティブです。常に 1 つのカスタム トポロジのみアクティブにできます。複数のトポロジを作成した場合、1 つをアクティブ化すると、自動的に現在アクティブなトポロジが非アクティブになります。

次の手順を使用して、カスタム トポロジのアクティブ化または非アクティブ化、トポロジの変更、またはトポロジの削除を行います。

アクティブなトポロジを削除すると、その変更はただちに有効になります。つまり、ネットワーク マップにはカスタム トポロジが表示されなくなります。

カスタム トポロジをアクティブ化または非アクティブ化するには、次の手順を実行します。

アクセス： Admin

ステップ 1　[Policies] > [Network Discovery] > [Custom Topology] を選択します。

[Custom Topology] ページが表示されます。

ステップ 2　次の 2 つのオプションから選択できます。

- トポロジを**アクティブ化する**には、ポリシーの隣にある [Activate] をクリックします。
- トポロジを**非アクティブ化する**には、ポリシーの隣にある [Deactivate] をクリックします。

カスタム トポロジを変更するには、次の手順を実行します。

アクセス： Admin

ステップ 1　[Policies] > [Network Discovery] > [Custom Topology] を選択します。

[Custom Topology] ページが表示されます。

ステップ 2　編集するトポロジの隣にある編集アイコン（  ）をクリックします。

[Edit Topology] ページが表示されます。変更可能な設定については、カスタム トポロジの作成（48-12 ページ）を参照してください。

ステップ 3　必要な変更を行い、[Save] をクリックします。

トポロジが変更されます。トポロジがアクティブな場合は、ネットワーク マップに行った変更は即時に有効になります。

カスタム トポロジを削除するには、次の手順を実行します。

アクセス： Admin

ステップ 1　[Policies] > [Network Discovery] > [Custom Topology] を選択します。

[Custom Topology] ページが表示されます。

ステップ 2　削除するトポロジの隣にある [Delete] をクリックします。トポロジがアクティブな場合は、削除することを確認します。

トポロジが削除されます。

CHAPTER 49

ホスト プロファイルの使用

ホスト プロファイルは、システムが 1 つのホストについて収集したすべての情報の完全なビューを提供します。ユーザは、プロファイルを通じてホスト名やオペレーティング システムなど、ホストの全般的な情報にアクセスできます。たとえば、ホストの MAC アドレスをすぐに見つける必要がある場合は、ホスト プロファイルを見ればわかります。

プロファイルには、*ホストの属性*も示されています。ホストの属性は、ホストに適用することができる、ユーザ定義の説明です。たとえば、ホストが存在するビルディングを示すようなホストの属性を割り当てることがあります。ホスト プロファイルから、そのホストに適用された既存のホスト属性を表示し、そのホスト属性の値を変更することができます。別の例として、*ホストの重要度*の属性を使用して、特定のホストのビジネス重要度を特定し、ホストの重要度に基づいて相関ポリシーとアラートを調整できます。

またホスト プロファイルは、特定のホスト上で稼動しているサーバ、クライアント、およびホスト プロトコルに関する情報を、コンプライアンスのホワイト リストに準拠しているかどうかも含めて提供します。サーバ リストからサーバを削除することも、サーバの詳細を表示することも可能です。サーバの*接続イベント*、サーバのトラフィックが検出されたセッションのログ情報も表示できます。また、クライアントの詳細および接続イベントを表示したり、ホスト プロファイルからサーバ、クライアント、またはホスト プロトコルを削除したりできます。

FireSIGHT システムの展開に FireSIGHT のライセンスが含まれている場合は、ホスト プロファイルにおける*侵害の痕跡*(IOC)を表示できます。これらの痕跡は、モニタリング対象のネットワーク上でホストが悪意のある手段によって侵害される可能性があるどうかを判断するために、ホストに関連付けられているさまざまなタイプのデータ(侵入イベント、Security Intelligence、接続イベント、ファイルまたはマルウェア イベント)との関連性を示しています。ホスト プロファイルから、ホストの IOC タグの概要を確認する、IOC に関連付けられているイベントを表示する、IOC タグに解決済みのマークを付ける、ディスカバリ ポリシーで IOC ルール ステートを編集する、といったことができます。

展開に Protection のライセンスが含まれている場合は、ホスト上のオペレーティング システム、およびホストが実行しているサーバとクライアントのタイプに最も適合するように、システムがトラフィックを処理する方法を調整することができます。詳細については、パッシブ展開における前処理の調整(30-1 ページ)を参照してください。

履歴情報を追跡するようシステムを設定している場合は、ホスト上のユーザの履歴情報を表示することもできます。過去 24 時間のユーザ アクティビティをグラフィック表示できます。

ホスト プロファイルから、ホストの脆弱性のリストを変更できます。この機能を使用して、ホストに対してどの脆弱性が対処されたかを追跡できます。脆弱性に対して修正ファイルを適用することもできます。このようにすると、修正ファイルで対処されたすべての脆弱性が自動的に無効とマークされることになります。

Ciscoで生成された脆弱性の情報を使用できます。また、サードパーティのスキャナで検出された脆弱性の情報を、ホスト入力機能によってDefense Centerにインポートして使用することもできます。

オプションで、ホスト プロファイルから Nmap スキャンを実行し、ホスト プロファイルのサーバ情報とオペレーティング システムの情報を増やすことができます。Nmap スキャナはホストをアクティブに調査し、ホストを実行しているオペレーティング システムおよびサーバの情報を取得します。スキャンの結果は、ホストのオペレーティング システムおよびサーバ アイデンティティのリストに追加されます。

ホスト プロファイルは、ネットワーク上のすべてのホストでは使用できない可能性があることに注意してください。考えられる原因は次のとおりです。

- タイムアウトしたため、ネットワーク マップからホストが削除された
- FireSIGHT ホストのライセンス制限に達した
- ネットワーク検出ポリシーでモニタリングされないネットワーク セグメントに、ホストが存在している

ホスト プロファイルに表示される情報は、ホストのタイプ、および利用可能なホストの情報によって異なる可能性があることに注意してください。たとえば、非 IP ベースのプロトコル（STP、SNAP、IPX など）を使用するホストを検出した場合、そのホストは MAC ホストとしてネットワーク マップに追加され、IP ホストに比べて使用できる情報はかなり少なくなります。

別の例として、NetFlow 対応のデバイスによってエクスポートされたデータに基づいて、ホスト、サーバ、およびクライアントをネットワーク マップに追加するようネットワーク検出ポリシーを設定することができますが、これらのホスト、サーバ、およびクライアントについて利用できる情報は制限されます。たとえば、スキャナやホストの入力機能を使用してオペレーティング システムのデータを提供していない場合、ホストではこれらのデータを使用できません。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

次の図は、ホスト プロファイルの例を示しています。

Host Profile

Scan Host | Generate White List Profile

IP Addresses	**192.168.1.4**
NetBIOS Name	
Device (Hops)	sampledevice (9)
MAC Addresses (TTL)	00:00:00:00:00:00 (Dell Inc.) (64)
Host Type	Host
Last Seen	2013-11-22 23:18:55
Current User	
View	Context Explorer | Connection Events | Intrusion Events | File Events | Malware Events

Indications of Compromise (3)

Edit Rule States | Mark All Resolved

Category	Event Type	Description	First Seen	Last Seen
Malware Executed	Threat Detected by FireAMP - Executed	The host has executed malware	2013-11-20 14:23:30	2013-12-03 10:35:07
Malware Detected	Threat Detected by FireAMP - Not Executed	The host has encountered malware	2013-11-20 15:26:50	2013-12-03 09:40:20
Dropper Infection	Dropper Infection Detected by FireAMP	The host may be infected with Dropper	2013-11-21 02:43:56	2013-12-02 03:44:29

Operating System (pending)

Edit Operating System

Users (no user history available)

Attributes

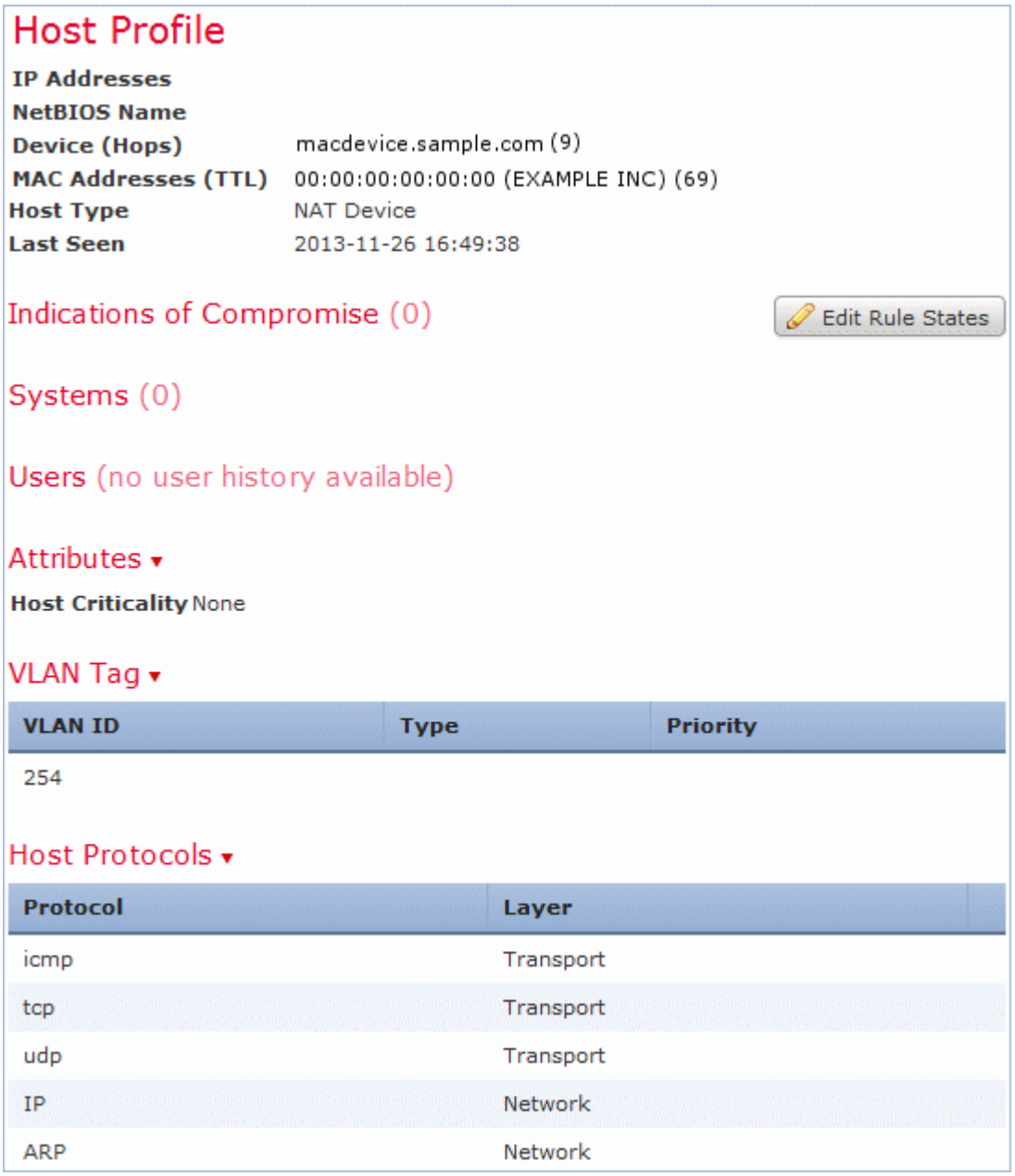
Edit Attributes

Host Criticality None

Host Protocols

Protocol	Layer
icmp	Transport
tcp	Transport
udp	Transport
IP	Network
ARP	Network

次の図は、MAC のホストのホスト プロファイルの例を示しています。



ホスト プロファイルの各セクションの詳細については、以下を参照してください。

- ホスト プロファイルの表示（49-5 ページ）では、ホスト プロファイルへのアクセス方法について説明します。
- ホスト プロファイルの基本的なホスト情報の使用（49-6 ページ）では、ホスト プロファイルの [Host] セクションで提供される情報について説明します。
- ホスト プロファイルの IP アドレスの使用（49-8 ページ）では、ホスト プロファイルの [IP Addresses] セクションで提供される情報について説明します。

- ホスト プロファイルでの侵害の痕跡の使用（49-9 ページ）では、ホスト プロファイルの [Indications of Compromise] セクションで提供される情報について説明します。
- ホスト プロファイルでのオペレーティング システムの使用（49-12 ページ）では、ホスト プロファイルの [Operating System] セクションまたは [Operating System Conflicts] セクションで提供される情報について、およびオペレーティング システムの編集方法、オペレーティング システムの競合の解決方法について説明します。
- ホスト プロファイルでのサーバの使用（49-16 ページ）では、ホスト プロファイルの [Servers] セクション、[Server Detail] セクション、および [Server Banner] セクションで提供される情報について説明します。
- ホスト プロファイルでのアプリケーションの使用（49-22 ページ）では、ホスト プロファイルの [Clients] セクションで提供される情報について説明します。
- ホスト プロファイルでの VLAN タグの使用（49-24 ページ）では、ホスト プロファイルの [VLAN Tag] セクションで提供される情報について説明します。
- ホスト プロファイルでのユーザ履歴の使用（49-24 ページ）では、ホスト プロファイルの [User History] セクションで提供される情報について説明します。
- ホスト プロファイルでのホスト属性の使用（49-25 ページ）では、ホスト プロファイルの [Attributes] セクションで提供される情報について説明します。
- 事前定義のホスト属性の使用（49-34 ページ）では、ホストの重要度の属性を設定する方法、およびホスト プロファイルにメモを追加する方法について説明します。
- ユーザ定義のホスト属性の使用（49-35 ページ）では、ユーザ定義のホスト属性の作成および使用に関する情報を示します。
- ホスト プロファイルでのホスト プロトコルの使用（49-26 ページ）では、ホスト プロファイルの [Host Protocols] セクションで提供される情報について説明します。
- ホスト プロファイルにおけるホワイト リスト違反の使用（49-26 ページ）では、ホスト プロファイルの [White List Violations] セクションで提供される情報について説明します。
- ホスト プロファイルでのマルウェア検出の使用（49-28 ページ）では、ホスト プロファイルの [Most Recent Malware Detections] セクションで提供される情報について説明します。
- ホスト プロファイルでの脆弱性の使用（49-29 ページ）では、ホスト プロファイルの [Vulnerabilities] セクション、および [Vulnerability Detail] セクションで提供される情報について説明します。

ホスト プロファイルの表示

ライセンス： FireSIGHT

モニタリング対象のネットワーク上のホストの IP アドレスを含む任意のネットワーク マップまたはイベント ビューから、ホスト プロファイルにアクセスできます。たとえば、検出イベントのテーブル ビューには、[IP Address] カラムのすべてのエントリの隣に、ホスト プロファイルへのリンクが含まれています。侵害の痕跡（IOC）ルールで有効になっているものがある場合は、侵害される可能性のあるホストが、異なるホスト プロファイル アイコンで示されます。

イベント ビューからホスト プロファイルを表示する方法

アクセス：Admin/Any Security Analyst

ステップ 1　任意のイベント ビューで、ホスト プロファイル アイコン（  ）をクリックするか、またはプロファイルを表示するホストの IP アドレスの隣にある、侵害されたホスト アイコン（  ）をクリックします。

ポップアップ ウィンドウにホスト プロファイルが表示されます。

ネットワーク マップからホスト プロファイルを表示する方法

アクセス：Admin/Any Security Analyst

ステップ 1　ネットワーク マップで、プロファイルを表示するホストの IP アドレスをドリルダウンします。

ホスト プロファイルが表示されます。ネットワーク マップからホスト プロファイルにアクセスする方法の例については、ホストのネットワーク マップの使用（48-2 ページ）を参照してください。

ホスト プロファイルの基本的なホスト情報の使用

ライセンス：FireSIGHT

各ホスト プロファイルは、検出されたホストまたは他のデバイスに関する基本情報を提供します。

次に、基本的なホスト プロファイルのフィールドについて説明します。

IP Addresses

ホストに関連付けられているすべての IP アドレス（IPv4 と IPv6 の両方）。多くの場合 IPv6 ホストでは、少なくとも 2 つの IPv6 アドレス（ローカルのみでルーティング可能なものと、グローバルにルーティング可能なもの）の他に、IPv4 アドレスを持っていることがあります。IPv4 専用ホストは、複数の IPv4 アドレスを持っていることがあります。可能な場合は、ルーティング可能なホスト IP アドレスに、フラグ アイコン、およびアドレスに関連付けられている地理情報データを表す国コードも含まれています。この機能、および他の地理情報機能の詳細については、地理情報の使用（58-23 ページ）を参照してください。

ホスト名

ホストの完全修飾されたドメイン名（わかる場合）。

NetBIOS Name

ホストの NetBIOS 名（使用できる場合）。Microsoft Windows ホストだけでなく Macintosh、Linux、または NetBIOS を使用するように設定されたその他のプラットフォームに NetBIOS 名を指定できます。たとえば、Samba サーバとして設定された Linux ホストに NetBIOS 名を指定します。

Device（Hops）

次のいずれかを行います。

- ホストが存在しているネットワークに関するレポート作成のデバイス（ネットワーク検出ポリシーで定義されている）、または
- ホストをネットワーク マップへ追加する NetFlow データを処理したデバイス
- デバイス名の後に、デバイス、およびホストを検出したデバイスとホスト自身の間のネットワーク ホップの数が丸括弧で囲まれて示されます。複数のデバイスで対象のホストを参照できる場合は、レポート作成のデバイスが太字で示されます。
- このフィールドが空白の場合は、次のいずれかになります。
- ホストがデバイスによってネットワーク マップに追加されたが、このデバイスは、ホストが存在しているネットワークに対してネットワーク検出ポリシーに定義されているとおりに明示的にモニタリングしていない。または、
- ホストの入力機能を使用してホストが追加されたが、FireSIGHT システムによって検出されていない

MAC Addresses（TTL）

ホストの検出された 1 つ以上の MAC アドレスおよび関連付けられている NIC ベンダー。NIC のハードウェア ベンダーおよび現在の存続可能時間（TTL）値が括弧内に示されます。MAC アドレスが太字で示されている場合、この MAC アドレスは、ARP および DHCP トラフィックでシステムによって検出されたホストの実際の MAC アドレスです。複数のデバイスが同じホストを検出した場合、Defense Centerにはどのデバイスがホストをレポートしたかに関係なく、ホストに関連付けられているすべての MAC アドレスおよび TTL 値が表示されます。

MAC アドレスをクリックして、同じ MAC アドレスを持つホストのリストを表示できます。ルータのホスト プロファイルは通常、このリスト内でルーティングしているネットワーク セグメント内のホスト（IP アドレス）を示します。モニタリング対象のルータの IP アドレスは多くの場合、モニタリングされるワークステーションとサーバのリストに表示されます。MAC アドレスの実際の IP アドレスは太字で表示されます。

Host Type

システムが検出したデバイスのタイプ（ホスト、モバイル デバイス、ジェイルブレイクされたモバイル デバイス、ルータ、ブリッジ、NAT デバイス、またはロード バランサ）。

ネットワーク デバイスを区別するためにシステムでは次の方法を使用します。

- Cisco Discovery Protocol（CDP）メッセージの分析。ネットワークのデバイスおよびそれらのタイプ（Cisco デバイスのみ）を特定できます。
- スパニング ツリー プロトコル（STP）の検出。デバイスをスイッチまたはブリッジとして識別します。
- 同じ MAC アドレスを使用している複数のホストの検出。MAC アドレスを、ルータに属しているものとして識別します。
- クライアント側からの TTL 値の変更、または通常のブート時間よりも頻繁に変更されている TTL 値の検出。この検出では、NAT デバイスとロード バランサを識別します。
- モバイル デバイスを区別するためにシステムでは次の方法を使用します。
- モバイル デバイスのモバイル ブラウザからの HTTP トラフィックのユーザ エージェント ストリングの分析
- 特定のモバイル アプリケーションの HTTP トラフィックのモニタリング

デバイスがネットワーク デバイスまたはモバイル デバイスとして識別されない場合は、ホストとして分類されます。

Last Seen

ホストのいずれかの IP アドレスが最後に検出された日時。

Current User

このホストに最後にログインしたユーザ。

既存の現行ユーザが権限のあるユーザでない場合、ホストにログインしている権限を持たないユーザは、現行ユーザとして登録されるだけであることに注意してください。詳細については、ユーザ データベース（45-8 ページ）を参照してください。

ビュー

イベント データのビューへのリンク。このリンクは、そのイベント タイプのデフォルト ワークフローを使用し、ホストに関連するイベントを表示するように制限されています。可能な場合は、これらのイベントには、ホストに関連付けられているすべての IP アドレスが含まれます。詳細については、次の項を参照してください。

- Content Explorer：詳細については、Context Explorer の使用法（56-1 ページ）を参照してください。
- Connection Events：詳細については、接続およびセキュリティ インテリジェンスのデータについて（39-2 ページ）を参照してください。
- Discovery Events：詳細については、ディスカバリ イベントの使用（50-1 ページ）を参照してください。
- Malware Events：詳細については、マルウェア イベントの操作（40-17 ページ）を参照してください。
- Intrusion Events by Source：詳細については、侵入イベントの操作（41-1 ページ）を参照してください。
- Intrusion Events by Destination：詳細については、侵入イベントの操作（41-1 ページ）を参照してください。

ホスト プロファイルの IP アドレスの使用

ライセンス： FireSIGHT

システムは、ホストに関連付けられている IP アドレスを検出し、サポートされている場合は、同じホストで使用される複数の IP アドレスをグループ化します。IPv6 ホストには通常、少なくとも 2 つの IPv6 アドレス（ローカルのみのものと、グローバルにルーティング可能なもの）があります。また、割り当てられた 1 つ以上の IPv4 アドレスを持っていることがあります。IPv4 専用ホストは、複数の IPv4 アドレスを持っていることがあります。

ホスト プロファイルは、そのホストに関連付けられている、検出されたすべての IP アドレスを一覧で示します。可能な場合、IP アドレスには小さいフラグ アイコン、および関連付けられている国を示す ISO の国コードも示されます。フラグ アイコンまたは国コードをクリックすると、地理情報の詳細を表示できます。詳細については、地理情報の使用（58-23 ページ）を参照してください。

デフォルトでは、最初の 3 つのアドレスだけが示されることに注意してください。ホストのすべてのアドレスを表示するには、[Show All] をクリックします。

ホスト プロファイルでの侵害の痕跡の使用

ライセンス：FireSIGHT

FireSIGHT システムは、モニタリング対象のネットワーク上でホストが悪意のある手段によって侵害される可能性があるかどうかを判断するために、ホストに関連付けられているさまざまなタイプのデータ（侵入イベント、Security Intelligence、接続イベント、ファイルまたはマルウェア イベント）との関連性を示すことができます。イベント データの特定の組み合わせと頻度は、影響を受けたホストの侵害の痕跡（IOC）タグをトリガーとして使用します。ホスト プロファイルの [Indications of Compromise] セクションには、ホストのすべての IOC タグが表示されます。このセクションでは、対象ではなくなった IOC タグを解決済みにするだけでなく、ホストが直面している脅威の詳細を表示する、IOC タグをトリガーとして使用したイベントに移動する、IOC ルールの状態を編集する、といったことが可能です。

IOC の機能を使用するには、機能、およびディスカバリ ポリシー内の少なくとも 1 つの IOC ルールを有効にする必要があります。対象ホストのホスト プロファイル ページから、個々のホストの IOC ルール状態を編集することもできます。各 IOC ルールは、IOC タグの 1 つのタイプに対応しています。組織のニーズに応じていずれかのルールまたはすべてのルールを有効にできます。ディスカバリ ポリシーおよび全般的な IOC に関する詳細は、侵害の兆候について（45-22 ページ）を参照してください。

IOC はホスト プロファイル内に存在しているだけではなく、イベント ビューアで IOC データを分析することもできます。詳細については、侵害の痕跡の使用（50-35 ページ）を参照してください。

次に、ホスト プロファイルで表示される IOC 情報のフィールドについて説明します。

IP Address

IOC をトリガーとして使用したホストに関連付けられている IP アドレス。

カテゴリ

`Malware Executed` や `Impact 1 Attack` など、示された侵害のタイプの簡単な説明。

イベント タイプ

特定の侵害の痕跡（IOC）に関連付けられている識別子で、トリガーとして使用したイベントを参照します。

説明

侵害される可能性のあるホストの脅威の原因についての説明（`This host may be under remote control` や `Malware has been executed on this host` など）。

First/Last Seen

ホストの IOC をトリガーとして使用したイベントが発生した最初（または最新）の日付と時刻。

ホスト プロファイルにおける IOC データの使用の詳細については、次の項を参照してください。

- 単一ホストにおける侵害の痕跡のルール状態の編集（49-10 ページ）
- 侵害の痕跡に対するソース イベントの表示（49-10 ページ）
- 侵害の痕跡を解決済みにする（49-11 ページ）

単一ホストにおける侵害の痕跡のルール状態の編集

ライセンス：FireSIGHT

システムで侵害の痕跡（IOC）を検出してタグを付けるには、最初にディスカバリ ポリシーの IOC 機能を有効にして、少なくとも 1 つの IOC ルールを（ポリシー全体または個別のホストに対して）有効にする必要があります。ホスト プロファイルから、個別のホストに適用される IOC ルールの状態を設定することができます。ディスカバリ ポリシーでの IOC の設定、およびポリシー全体での IOC ルール状態の設定の詳細については、侵害の兆候ルールの設定（45-37 ページ）を参照してください。

ホスト プロファイルから [Indications of Compromise] セクションの [Edit Rule States] リンクを使用して IOC ルールのリストにアクセスし、編集することができます。ネットワークや組織のニーズに合わせて、一部またはすべてのルールを有効にすることができます。たとえば、Microsoft Excel などのソフトウェアを使用しているホストが絶対に監視対象ネットワーク上に出現しない場合は、Excel ベースの脅威に関係する IOC タグを有効にしないようにできます。

すべての IOC ルールはCiscoで事前に定義されています。ユーザはオリジナルのルールを作成することはできませんが、トリガーされた IOC タグについてコンプライアンス ルールを作成できます。詳細については、相関ポリシーおよび相関ルールの設定（51-1 ページ）を参照してください。各 IOC ルールはイベントの 1 つのタイプのみ（マルウェアや侵害など）でトリガーされ、特定の IOC タグに対応します。ルールとタグは簡単に対応できるよう、同じ Category、Event Type、および Description のデータを持っています。IOC ルール状態の [Edit] ページには、ルールをトリガーとして使用するために必要なシステム機能を明確にするために、各ルールの Source イベント データも表示されます。

ホストについて侵害の痕跡のルール状態を編集する方法

アクセス：Admin/Any Security Analyst

ステップ 1　ホスト プロファイルの [Indications of Compromise] セクションで [Edit Rule States] をクリックします。

新しいウィンドウに [Edit Indication of Compromise Rule States] ページが表示されます。

ステップ 2　ルールの [Enabled] カラムで、スライダーをクリックして有効と無効を切り替えます。

ステップ 3　[Save] をクリックします。

変更が保存されます。

侵害の痕跡に対するソース イベントの表示

ライセンス：FireSIGHT

[Indications of Compromise] セクションを使用して、ホスト上で IOC タグをトリガーとして使用したイベントへすばやくナビゲートすることができます。これらのイベントを分析すると、侵害される可能性があるホストへの脅威に対処するのに必要なアクション、およびアクションが必要かどうかを判断するための情報が提供されます。

IOC タグのタイムスタンプの隣の表示アイコン（  ）をクリックすると、関連するイベント タイプのイベントのテーブル ビューにナビゲートします。ここでは、IOC タグをトリガーとして使用したイベントのみが表示されます。

IOC タグをトリガーとして使用するイベントのタイプと機能の詳細については、以下を参照してください。

- 接続およびセキュリティ インテリジェンス のデータの使用（39-1 ページ）
- 侵入イベントの操作（41-1 ページ）
- マルウェア対策とファイル制御について（37-2 ページ）

[Indications of Compromise] タグのソース イベントを表示する方法

アクセス： Admin/Any Security Analyst

ステップ 1　ホスト プロファイルの [Indications of Compromise] セクションで、調べる IOC タグの [First Seen] または [Last Seen] カラムの表示アイコン（  ）をクリックします。

IOC をトリガーとして使用した対象のイベントについて、イベントのテーブル ビューが表示されます。ここでは、トリガーとして使用したイベントのみが表示されます。ホスト プロファイル ページを別のウィンドウで表示している場合は、メイン ウィンドウにイベント ビューが表示されます。

侵害の痕跡を解決済みにする

ライセンス： FireSIGHT

IOC タグで示された脅威が分析および対処された後、または IOC タグが誤検出を示していると判断した場合、このタグを解決済みとしてマークすることができます。IOC タグを解決済みとしてマークすると、このタグがホスト プロファイルから削除されます。ホスト上でアクティブなすべての IOC タグが解決済みになると、ホストでは、侵害されたホスト アイコン（  ）が表示されなくなります。解決済みの IOC についても、IOC のトリガー元イベントは引き続き表示できます。

イベントがホストの IOC タグを再度トリガーとして使用すると、タグがもう一度設定されます。ホスト上の個別の IOC タグを解決することも、ホスト上のすべてのタグに解決済みとマークすることもできます。

Indications of Compromise タグを解決済みにする方法

アクセス： Admin/Any Security Analyst

ステップ 1　ホスト プロファイルの [Indications of Compromise] セクションで、次の 2 つの方法のいずれかを実行します。

- 個別の IOC タグに解決済みとマークするには、解決するタグの右にある解決のアイコン（  ）をクリックします。
- ホスト上のすべての IOC タグを解決済みとマークするには、[Mark All Resolved] をクリックします。

変更が保存され、選択した IOC タグが削除されます。

ホスト プロファイルでのオペレーティング システムの使用

ライセンス：FireSIGHT

システムは、ホストで生成されたトラフィック内のネットワークおよびアプリケーション スタックを分析したり、User Agent でレポートされたホスト データを分析することによって、ホスト上で稼動しているオペレーティング システムのアイデンティティをパッシブに検出します。システムでは、他のソース（Nmap スキャナ、ホストの入力機能によりインポートされたアプリケーション データ）のオペレーティング システムの情報も照合します。どのアイデンティティを使用するかを判断する場合、システムは、各アイデンティティのソース（発生源）に割り当てられている優先度を考慮します。デフォルトでは、ユーザ入力が最も高い優先度を持ち、以降は高い順にアプリケーションまたはスキャナ ソース、Ciscoにより検出されたアイデンティティ、となります。

システムでは、オペレーティング システムの具体的な定義ではなく、全般的な定義を提供することがあります。これは、トラフィックおよび他のアイデンティティ ソースで、対象のアイデンティティを詳しく調べるための十分な情報が提供されないためです。システムは、できるだけ詳しい定義を使用するために、ソースの情報を照合します。

次に、ホスト プロファイルで表示されるオペレーティング システムの情報フィールドについて説明します。

Hardware

モバイル デバイスのハードウェア プラットフォーム。

OS Vendor/Vendor

オペレーティング システムのベンダー。

OS Product/Product

すべてのソースから収集されたアイデンティティ データに基づいて、実行されている可能性が最も高いと判断されたオペレーティング システム。

オペレーティング システムが [Pending] の場合、システムはオペレーティング システムをまだ識別しておらず、他に使用可能なアイデンティティ データはありません。オペレーティング システムが [unknown] の場合、システムはオペレーティング システムを識別できず、オペレーティング システムに関して他に使用可能なアイデンティティ データはありません。

ホストのオペレーティング システムがシステムで検出可能なものでなかった場合、以下の方針のいずれかを使用できます。

- カスタム フィンガープリントの使用（46-7 ページ）に記載されているとおりに、ホストのカスタム フィンガープリントを作成する
- ホスト プロファイルからのホストのスキャン（49-39 ページ）に記載されているとおりに、ホストに対して Nmap スキャンを実行する
- 『*FireSIGHT System Host Input API Guide*』に記載されているホスト入力機能を使用して、データをネットワーク マップにインポートする
- ホスト プロファイルでのオペレーティング システムの使用（49-12 ページ）に記載されているとおりに、オペレーティング システムの情報を手動で入力する

OS Version/Version

オペレーティング システムのバージョン。ホストがジェイルブレイクされたモバイル デバイスの場合、バージョンの後に括弧で囲まれて `Jailbroken` と示されます。

Source

次の値のいずれかを指定します。

- ユーザ: *user_name*
- アプリケーション: *app_name*
- スキャナ: *scanner_type*（Nmap、またはシステム ポリシーによって追加されたスキャナ）
- FireSIGHT

システムでは、オペレーティング システムのアイデンティティを判断するために、複数のソースのデータを統合することができます。現在の ID について（46-5 ページ）を参照してください。

ホストの脆弱性リスト、およびホストを対象とするイベントの影響の相関関係はオペレーティング システムによって異なるため、オペレーティング システムの特定の情報を手動で入力することもできます。また、オペレーティング システムに対して、サービス パックやアップデートなどの修正ファイルが適用されたことを示すことも、修正ファイルによって対処された脆弱性を無効にすることもできます。

たとえば、システムでホストのオペレーティング システムが Microsoft Windows 2003 であると特定されたが、実際にはホストが Microsoft Windows XP Professional および Service Pack 2 を実行していることがわかっている場合、オペレーティング システムのアイデンティティを実際のとおりに設定することができます。より具体的なオペレーティング システムのアイデンティティを設定すると、ホストの脆弱性のリストの精度が向上するため、対象のホストに対する影響の相関関係が、より限定的かつ正確になります。

システムでホストに対するオペレーティング システム情報が検出され、その情報が、アクティブなソースによって提供されている現行のオペレーティング システムのアイデンティティと競合している場合、アイデンティティの競合が発生します。実際にアイデンティティの競合が発生している場合、システムは脆弱性と影響の相関関係の両方のアイデンティティを使用します。

NetFlow 対応デバイスによってエクスポートされたデータに基づきネットワーク マップにホストを追加するようネットワーク検出ポリシーを設定することはできますが、オペレーティング システムのアイデンティティを設定していない場合は、これらのホストで使用できるオペレーティング システムのデータはありません。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

オペレーティング システムを実行しているホストが、有効なネットワーク検出ポリシーのコンプライアンスのホワイト リストに違反している場合、Defense Centerはオペレーティング システムの情報にホワイト リストの違反アイコン（）のマークを付けます。また、ジェイルブレイクされたモバイル デバイスが有効なホワイト リストに違反している場合、そのデバイスのオペレーティング システムの隣にアイコンが表示されます。

ホストのオペレーティング システムのアイデンティティに対して、カスタム表示文字列を設定できます。この表示文字列は、ホスト プロファイルで使用されます。

注　あるホストについてオペレーティング システムの情報を変更すると、ホストのコンプライアンス、およびコンプライアンスのホワイト リストが変わる可能性があることに注意してください。

ネットワーク デバイスに対するホスト プロファイルでは、[Operating Systems] セクションのラベルが [Systems] に変わり、[Hardware] カラムが新しく表示されます。[Systems] の下にハードウェア プラットフォームの値が表示され場合、システムは、ネットワーク デバイスの背後で 1 つ以上のモバイル デバイスが検出されたことを示しています。モバイル デバイスはハードウェア プラットフォームの情報を持っていることも、持っていないこともありますが、モバイル デバイスではないシステムではハードウェア プラットフォーム情報は検出されないことに注意してください。

オペレーティング システムのアイデンティティの表示

ライセンス：FireSIGHT

検出された、またはホストに追加された特定のオペレーティング システムのアイデンティティを表示することができます。システムはソースの優先度を使用して、ホストに対する現行のアイデンティティを判断します。アイデンティティのリストでは、現行のアイデンティティが太字で強調されます。

各オペレーティング システムのアイデンティティでは、ホスト プロファイルに、ホスト プロファイルでのオペレーティング システムの使用（49-12 ページ）に記載されている情報が含まれていることがあります。

1 つのホストに対して複数のオペレーティング システムのアイデンティティが存在している場合のみ、[View] ボタンが有効になっていることに注意してください。

ホストに対するオペレーティング システムのアイデンティティ リストを表示する方法

アクセス：Admin/Any Security Analyst

ステップ 1　ホスト プロファイルの [Operating System] または [Operating System Conflicts] セクションで [View] をクリックします。

[Operating System Identity Information] ポップアップ ウィンドウが表示されます。

ヒント　いずれかのオペレーティング システムのアイデンティティの隣にある削除アイコン（）をクリックして、[Operating System Identity Information] ポップアップ ウィンドウからアイデンティティを削除し、可能な場合は、ホスト プロファイルでオペレーティング システムの現行のアイデンティティを更新します。Ciscoが検出したオペレーティング システムのアイデンティティは、削除できないことに注意してください。

オペレーティング システムの編集

ライセンス：FireSIGHT

FireSIGHT システム Web インターフェイスを使用して、ホストに対する現行のオペレーティング システムのアイデンティティを設定できます。Web インターフェイスを介してアイデンティティを設定すると、他のすべてのアイデンティティ ソースが上書きされるため、このアイデンティティが、脆弱性の評価および影響の相関関係で使用されます。ただし、オペレーティング システムを編集した後で、ホストに対するオペレーティング システムのアイデンティティの競合がシステムで検出された場合、オペレーティング システムの競合が発生することに注意してください。

競合が解決されるまで、両方のオペレーティング システムが現行のものであるとみなされます。詳細については、オペレーティング システムのアイデンティティの競合を解決する（49-15 ページ）を参照してください。

オペレーティング システムのアイデンティティを変更する方法

アクセス：Admin/Any Security Analyst

ステップ 1　ホスト プロファイルの [Operating System] セクションで [Edit] をクリックします。

ポップアップ ウィンドウが表示され、ここでオペレーティング システムのアイデンティティを設定することができます。

ステップ 2　ここでは次のオプションがあります。

- [OS Definition] ドロップダウン リストから [Current Definition] を選択し、ホスト入力によって現行のオペレーティング システムのアイデンティティを確認して、6 の手順に進みます。
- [OS Definition] ドロップダウン リストから現行のオペレーティング システムのアイデンティティのバリエーションを選択し、6 の手順に進みます。
- [OS Definition] ドロップダウン リストから [User-Defined] を選択し、3 の手順に進みます。

ステップ 3　オプションとして、[Use Custom Display String] を選択し、[Vendor String]、[Product String]、および [Version String] フィールドで表示するカスタム文字列を修正します。

ステップ 4　オプションで別のベンダーからオペレーティング システムを変更するには、[Vendor] および [Product] ドロップダウン リストから、ベンダーおよび他のオペレーティング システムの詳細を選択します。

ステップ 5　オプションでオペレーティング システムの製品リリース レベルを設定するには、[Major]、[Minor]、[Revision]、[Build]、[Patch] および [Extension] ドロップダウン リストから対象のアイテムを選択します。

ステップ 6　オプションで、オペレーティング システムに対して修正ファイルが適用されたことを示す場合は、[Configure Fixes] をクリックします。

パッケージの有効な修正リストが表示されます。

ステップ 7　ドロップダウン リストから適用可能な修正を選択し、[Add] をクリックします。

ステップ 8　オプションで、[Patch] および [Extension] ドロップダウン リストを使用して、対象のパッチおよび拡張機能を追加します。

ステップ 9　[Finish] をクリックして、オペレーティング システムのアイデンティティの設定を完了します。

オペレーティング システムのアイデンティティの競合を解決する

ライセンス：FireSIGHT

システムで検出された新しいアイデンティティと現行のアイデンティティが競合しており、そのアイデンティティが、スキャナやアプリケーション、ユーザなどのアクティブなソースによって提供されていた場合、オペレーティング システムのアイデンティティで競合が発生します。

ホスト プロファイルでは、競合状態のオペレーティング システムのアイデンティティのリストは太字で表示されます。

システムの Web インターフェイスを介して、アイデンティティの競合を解決し、ホストに対する現行のオペレーティング システムのアイデンティティを設定することができます。Web インターフェイスを介してアイデンティティを設定すると、他のすべてのアイデンティティ ソースが上書きされるため、このアイデンティティが、脆弱性の評価および影響の相関関係で使用されます。

競合しているアイデンティティのいずれかを現行のアイデンティティにする方法

アクセス：Admin/Any Security Analyst

ステップ 1　次の 2 つのオプションから選択できます。

- ホストのオペレーティング システムとして設定するオペレーティング システムのアイデンティティの隣にある、[Make Current] をクリックします。
- アクティブなソースで、現行のアイデンティティとして使用*しない*アイデンティティが表示された場合は、使用しないアイデンティティを削除します。

オペレーティング システムのアイデンティティの競合を解決する方法

アクセス：Admin/Any Security Analyst

ステップ 1　ホスト プロファイルの [Operating System Conflicts] セクションで [Resolve] をクリックします。

ポップアップ ウィンドウが表示され、ここで現行のオペレーティング システムのアイデンティティを設定することができます。

ステップ 2　ここでは次のオプションがあります。

- [OS Definition] ドロップダウン リストから [Current Definition] を選択し、ホスト入力によって現行のオペレーティング システムのアイデンティティを確認して、6 の手順に進みます。
- [OS Definition] ドロップダウン リストから、競合しているオペレーティング システムのアイデンティティのいずれかのバリエーションを選択し、6 の手順に進みます。
- [OS Definition] ドロップダウン リストから [User-Defined] を選択し、3 の手順に進みます。

ステップ 3　オプションとして、[Use Custom Display String] を選択し、[Vendor String]、[Product String]、および [Version String] フィールドで表示するカスタム文字列を入力します。

ステップ 4　オプションで別のベンダーからオペレーティング システムを変更するには、ベンダーおよび他のオペレーティング システムの詳細を選択します。

ステップ 5　オプションでオペレーティング システムの製品リリース レベルを設定するには、[Major]、[Minor]、[Revision]、[Build]、[Patch] および [Extension] ドロップダウン リストから対象のアイテムを選択します。

ステップ 6　オプションで、オペレーティング システムに対して修正ファイルが適用されたことを示す場合は、[Configure Fixes] をクリックします。

ステップ 7　適用した修正ファイルを、修正ファイル リストに追加します。

ステップ 8　[Finish] をクリックして、オペレーティング システムのアイデンティティの設定を終了し、ホスト プロファイルに戻ります。

ホスト プロファイルでのサーバの使用

ライセンス：FireSIGHT

システムが、モニタリング対象のネットワーク上のホストで稼動しているサーバを検出した場合、またはホストの入力機能、スキャナ、他の有効なソースを介してサーバが追加された場合は、Defense Centerは、ホスト プロファイルの [Servers] セクションにこれらのサーバを表示します。

Defense Centerは 1 つのホストにつき最大 100 台のサーバを表示します。100 個の制限に達すると、ホストからサーバを削除するか、またはサーバがタイム アウトになるまで、いずれかのソースの新しいサーバ情報は、アクティブであってもパッシブであっても廃棄されます。詳細については、ホスト制限と検出イベント ロギング（45-15 ページ）を参照してください。

Nmap を使用してホストをスキャンすると、オープンな TCP ポート上で稼動している、検出されなかったサーバの結果が Nmap によって Servers リストに追加されます。ホストで Nmap スキャンを実行した場合、または Nmap の結果をインポートした場合、ホスト プロファイルに拡張可能な [Scan Results] セクションも表示され、Nmap スキャンによってホスト上で検出されたサーバ情報が示されます。詳細については、ホスト プロファイルでのスキャン結果の使用（49-39 ページ）およびNmap スキャンのセットアップ（47-10 ページ）を参照してください。ネットワーク マップからホストが削除されると、ホストのそのサーバに対する Nmap スキャンの結果は廃棄されることに注意してください。

注　NetFlow 対応のデバイスによってエクスポートされたデータに基づいて、サーバとクライアントをネットワーク マップに追加するようネットワーク検出ポリシーを設定することができますが、これらのアプリケーションについて利用できる情報は限定的です。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

ホスト プロファイルでサーバを使用するためのプロセスは、ユーザがプロファイルにアクセスした方法によって異なります。

- Servers ネットワーク マップを介したドリル ダウンによりホスト プロファイルにアクセスした場合は、サーバの名前が太字で強調されて、サーバの詳細が表示されます。ホストの他のサーバについて詳細を表示する場合は、対象のサーバ名の隣にある表示アイコン（  ）をクリックします。
- 他の方法でホスト プロファイルにアクセスした場合は、[Servers] セクションを展開し、詳細を表示するサーバの隣にある表示アイコン（  ）をクリックします。

また、次の操作も実行できます。

- ホスト上の特定のサーバに関連付けられている接続イベントを分析するには、サーバの隣にあるイベント アイコンをクリックします。

  接続イベントに対する優先ワークフロー最初のページが表示され、ホストの IP アドレスの他、サーバのポートおよびプロトコルで制約されて接続イベントが示されます。接続イベントに対する優先ワークフローがない場合、ワークフローを選択する必要があります。接続データの詳細については、接続およびセキュリティ インテリジェンス のデータの使用（39-1 ページ）を参照してください。
- ホスト プロファイルからサーバを削除するには、サーバの隣にある削除アイコン（  ）をクリックします。

  サーバはホスト プロファイルから削除されますが、システムがサーバからトラフィックを再度検出すると、そのサーバがもう一度表示されます。ホストからサーバを削除すると、そのホストにホワイト リストのコンプライアンスが適用されることがあります。
- サーバのアイデンティティの競合を解決するには、サーバの隣にある解決のアイコンをクリックします。

  競合しているアイデンティティのいずれかを選択して、これらのアイデンティティのいずれか 1 つのバリエーションを選択するか、またはユーザ定義の新しいアイデンティティを設定することができます。
- サーバのアイデンティティを編集するには、サーバの隣にある編集アイコン（  ）をクリックします。

  現行のアイデンティティの選択、そのアイデンティティのバリエーションの選択、またはユーザ定義の新しいアイデンティティの設定を実行できます。

次に、[Servers list] の列について説明します。

[Protocol]

サーバが使用するプロトコルの名前。

Port

サーバが実行されているポート。

Application Protocol

次のいずれかになります。

- アプリケーション プロトコルの名前
- [pending]：システムで、いずれかの理由のでアプリケーション プロトコルをポジティブまたはネガティブに識別できない場合
- [unknown]：既知のアプリケーション プロトコルのフィンガープリントに基づいてシステムでアプリケーション プロトコルを識別できない場合、または（対応するサーバは追加せずに、ポート情報での脆弱性を追加することにより）ホストの入力を介してサーバが追加された場合

アプリケーション プロトコルの名前にマウスを重ねると、タグが表示されます。タグの詳細については、アプリケーション検出について（45-11 ページ）を参照してください。

Vendor and Version

FireSIGHT システム、Nmap、または他のアクティブなソースで識別されたベンダーとバージョン、またはホストの入力機能を介して取得したベンダーとバージョン。有効なソースで識別が行われなかった場合、フィールドは空白になります。

ホストが、有効な相関ポリシーのコンプライアンス ホワイト リストに違反するサーバを実行している場合、Defense Centerは非準拠サーバに、ホワイト リストの違反アイコン（）のマークを付けます。

詳細については、次の項を参照してください。

- サーバの詳細（49-18 ページ）
- サーバのアイデンティティの編集（49-20 ページ）
- サーバ アイデンティティの競合の解決（49-21 ページ）

サーバの詳細

ライセンス： FireSIGHT

Defense Centerは、1 つのサーバについてパッシブに検出される（Ciscoまたは NetFlow で検出される）アイデンティティを最大 16 個表示します。システムで、このサーバの複数のベンダーまたはバージョンを検出した場合、サーバは複数のパッシブなアイデンティティを持つことができます。たとえば、Web サーバが、サーバ ソフトウェアと同じバージョンを実行していない場合、管理対象デバイスと Web サーバ ファーム間にロード バランサがあると、HTTP に対してシステムが複数のパッシブ アイデンティティを識別することがあります。Defense Centerは、ユーザ入力、スキャナ、その他のアプリケーションなど、アクティブなソースからのサーバ アイデンティティの数を制限することはありません。

Defense Centerは現行のアイデンティティを太字で表示します。システムでは、1 つのホストに対する脆弱性の割り当て、影響の評価、ホスト プロファイルの証明書およびコンプライアンス ホワイト リストに対して記載された相関ルールの評価など、いくつかの目的のためにサーバの現行のアイデンティティを使用します。

ヒント サーバの詳細からのサーバ アイデンティティの変更、およびアイデンティティの競合の解決については、サーバのアイデンティティの編集（49-20 ページ）およびサーバ アイデンティティの競合の解決（49-21 ページ）を参照してください。

サーバの詳細には、選択されたサーバについて知られている、更新済みのサブサーバ情報が表示されることがあります。最後に、サーバの詳細にサーバのバナーが表示されることがあります。これは、ホスト プロファイルからサーバを表示したときに、サーバの詳細の下に表示されます。

サーバのバナーは、サーバを識別するのに役立つサーバに関する追加情報を提供します。攻撃者がサーバのバナー文字列を意図的に変更した場合、システムは誤ったアイデンティティが示されたサーバを識別または検出できません。サーバのバナーには、そのサーバについて検出された最初のパケットの最初の 256 文字が表示されます。この情報は、サーバがシステムによって最初に検出されたときに一度だけ収集されます。バナーの内容は 2 列で表示されます。左側の列は 16 進表記で示され、右側の列は対応する ASCII 表記で示されます。

注 サーバのバナーを表示するには、ネットワーク検出ポリシーで [Capture Banners] チェック ボックスを有効にする必要があります。このオプションは、デフォルトで無効です。

次に、サーバの詳細情報について説明します。

Protocol

サーバが使用するプロトコルの名前。

Port

サーバが実行されているポート。

Hits

Ciscoの管理対象デバイスまたは Nmap によってサーバが検出された回数。ホストの入力によってインポートされたサーバについては、システムがそのサーバについてトラフィックを検出しない場合、検出回数は 0 になることに注意してください。

Last Used

サーバが最後に検出された日時。システムで対象のサーバについて新しいトラフィックを検出しない場合、ホスト入力のデータが最後に使用された時間は、データの最初のインポート時間を反映していることに注意してください。また、ホストの入力機能を介してインポートされたスキャナおよびアプリケーションのデータは、システム ポリシーの設定に従ってタイムアウトになりますが、Defense Centerの Web インターフェイスを介したユーザ入力はタイムアウトにならないことに注意してください。

アプリケーション プロトコル

サーバによって使用されるアプリケーション プロトコルの名前（既知の場合）。

ベンダー

サーバのベンダー。ベンダーがわからない場合、このフィールドは表示されません。

Version

サーバのバージョン。バージョンがわからない場合、このフィールドは表示されません。

Source

次の値のいずれかを指定します。

- User: *user_name*
- Application: *app_name*
- Scanner: *scanner_type*（Nmap、またはシステム ポリシーによって追加されたスキャナ）
- FireSIGHT、FireSIGHT Port Match、または FireSIGHT Pattern Match（Ciscoが検出したアプリケーションの場合）
- NetFlow（NetFlow データに基づいてネットワーク マップに追加されたサーバの場合）

システムでは、サーバのアイデンティティを判断するために、複数のソースのデータを統合することができます。現在の ID について（46-5 ページ）を参照してください。

サーバの詳細を表示する方法

アクセス： Admin/Any Security Analyst

ステップ 1　ホスト プロファイルの [Servers] セクションで、サーバの隣にある表示アイコン（  ）をクリックします。

[Server Detail] ポップアップ ウィンドウが表示されます。

サーバのアイデンティティの編集

ライセンス： FireSIGHT

ホスト上のサーバのアイデンティティ設定を手動で更新し、修正ファイルによって対処された脆弱性を削除するために、ホストに適用した何らかの修正ファイルを設定することができます。サーバのアイデンティティを削除することもできます。

アイデンティティを削除しても、（アイデンティティが 1 つしかない場合でも）サーバは削除されないことに注意してください。アイデンティティを削除すると、[Server Detail] ポップアップ ウィンドウからアイデンティティが削除されます。可能な場合は、ホスト プロファイルでそのサーバの現行のアイデンティティを更新します。

Ciscoの管理対象デバイスによって追加されたサーバのアイデンティティは、編集または削除できません。

サーバのアイデンティティの編集方法

アクセス： Admin/Any Security Analyst

ステップ 1　ホスト プロファイルの [Servers] セクションで、[View] をクリックして [Server Detail] ポップアップ ウィンドウを表示します。

ステップ 2　次の 2 つのオプションから選択できます。

- サーバのアイデンティティを削除するには、削除するサーバ アイデンティティの隣にある削除アイコン（  ）をクリックします。

- サーバのアイデンティティを変更するには、サーバ リストでサーバの隣にある編集アイコン( )をクリックします。

  [Server Identity] ポップアップ ウィンドウが表示されます。

ステップ 3　次の 2 つのオプションから選択できます。

- [Select Server Type] ドロップダウン リストから現行の定義を選択します。
- [Select Server Type] ドロップダウン リストからサーバのタイプを選択します。

ステップ 4　オプションで対象のサーバ タイプのベンダーと製品のみを表示するには、[Restrict by Server Type] チェック ボックスをオンにします。

ステップ 5　オプションでサーバの名前とバージョンをカスタマイズするには、[Use Custom Display String] を選択し、[Vendor String] と [Version String] に入力します。

ステップ 6　[Product Mappings] セクションで、使用するオペレーティング システム、製品、およびバージョンを選択します。

たとえば、サーバを Red Hat Linux 9 へマップする場合は、ベンダーとして [Redhat, Inc.] を、製品として [Redhat Linux] を選択し、バージョンとして [9] を選択します。

ステップ 7　サーバに対して修正ファイルが適用されていることを示す場合は、[Configure Fixes] をクリックします。それ以外の場合は、9の手順に進みます。

[Available Package Fixes] ページが表示されます。

ステップ 8　サーバに適用するパッチを、修正ファイル リストに追加します。

ステップ 9　[Finish] をクリックしてサーバ アイデンティティの設定を完了します。

サーバ アイデンティティの競合の解決

ライセンス： FireSIGHT

アプリケーションやスキャナなどのアクティブなソースが、サーバのアイデンティティ データをホストへ追加したときに、サーバ アイデンティティの競合が発生した場合、システムは競合しているサーバ アイデンティティを示しているポートのトラフィックを検出します。

サーバ アイデンティティの競合を解決する方法

アクセス： Admin/Any Security Analyst

ステップ 1　[Server] リストで、サーバの隣にある解決のアイコンをクリックします。

[Server Identity] ポップアップ ウィンドウが表示されます。

ステップ 2　[Select Server Type] ドロップダウン リストからサーバのタイプを選択します。

ステップ 3　オプションで対象のサーバ タイプのベンダーと製品のみを表示するには、[Restrict by Server Type] チェック ボックスをオンにします。

ステップ 4　オプションでサーバの名前とバージョンをカスタマイズするには、[Use Custom Display String] を選択し、[Vendor String] と [Version String] に入力します。

ステップ 5　[Product Mappings] セクションで、使用するオペレーティング システム、製品、およびバージョンを選択します。

たとえば、サーバを Red Hat Linux 9 へマップする場合は、ベンダーとして [Redhat, Inc.] を、製品として [Redhat Linux] を選択し、バージョンとして [9] を選択します。

ステップ 6　サーバに対して修正ファイルが適用されていることを示す場合は、[Configure Fixes] をクリックします。それ以外の場合は、9の手順に進みます。

[Available Package Fixes] ページが表示されます。

ステップ 7　サーバに適用するパッチを、修正ファイル リストに追加します。

ステップ 8　[Finish] をクリックしてサーバ アイデンティティの設定を完了し、ホスト プロファイルへ戻ります。

ホスト プロファイルでのアプリケーションの使用

ライセンス： FireSIGHT

ホスト プロファイルで、ホスト上で稼動しているアプリケーションを表示することができます。ホスト プロファイルからアプリケーションを削除する場合は、そのアプリケーションを削除します。

ホスト プロファイルでのアプリケーションの管理については、以下を参照してください。

- ホスト プロファイルでのアプリケーションの表示（49-22 ページ）
- ホスト プロファイルからのアプリケーションの削除（49-23 ページ）

ホスト プロファイルでのアプリケーションの表示

ライセンス： FireSIGHT

システムは、ネットワーク上のホストで稼動しているさまざまなクライアントと Web アプリケーションを検出できます。

注　モニタリング対象のネットワーク内のホストでアプリケーションを検出するには、システムのネットワーク検出ポリシー内の NetFlow デバイスに対するディスカバリ ルールで、[Applications] チェック ボックスをオンにする必要があります。このオプションは、NetFlow ルールではデフォルトで有効になっており、管理対象デバイスを介した検出で使用されるルールに対しては無効にすることはできません。

ホスト プロファイルは、ホスト上で検出されたアプリケーションの製品とバージョン、使用できるクライアントまたは Web アプリケーションの情報、およびアプリケーションが最後に使用中であると検出された時間を表示します。

Defense Centerは、ホスト上で稼動している最大 16 個のクライアントを表示します。16 個の制限に達すると、ユーザがホストからクライアント アプリケーションを削除するか、または非アクティブである（クライアントがタイムアウトしている）ためにシステムによってホスト プロファイルからクライアントが削除されるまで、新しいクライアント情報は、どのソースのものであるか、アクティブかパッシブかにかかわらず、廃棄されます。

また、検出されたそれぞれの Web ブラウザについてホスト プロファイルは、アクセスされた最初の 100 個の Web アプリケーションを表示します。この制限に達すると、ブラウザに関連付けられている新しい Web アプリケーションは、どのソースのものであるか、アクティブかパッシブかにかかわらず、次の条件を満たすまで廃棄されます。

- Web ブラウザのクライアント アプリケーションがタイムアウトになる、または

- ユーザが、Web アプリケーションに関連付けられているアプリケーション情報をホスト プロファイルから削除する

次に、ホスト プロファイルに表示されるアプリケーション情報について説明します。

アプリケーション プロトコル

アプリケーション（HTTP ブラウザ、DNS クライアントなど）で使用されるアプリケーション プロトコルを表示します。

クライアント

FireSIGHT システムで識別された場合、Nmap または他のアクティブなソースで取得された場合、あるいはホストの入力機能を介して取得された場合に、ペイロードから派生したクライアント情報。有効なソースで識別が行われなかった場合、フィールドは空白になります。

Version

クライアントのバージョンを表示します。

Web アプリケーション

Web ブラウザ の場合は、http トラフィックでシステムによって検出されたコンテンツ。Web アプリケーションの情報は、FireSIGHT システムによって識別された、Nmap によって取得された、他のアクティブなソースによって取得された、またはホストの入力機能を介して取得された特定のタイプのコンテンツ（WMV や QuickTime など）を表します。有効なソースで識別が行われなかった場合、フィールドは空白になります。

ホストが、有効な相関ポリシーのコンプライアンス ホワイト リストに違反するアプリケーションを実行している場合、Defense Centerは非準拠アプリケーションに、ホワイト リストの違反アイコン（ ）のマークを付けます。

ホスト上の特定のアプリケーションに関連付けられている接続イベントを分析するには、アプリケーションの隣にあるイベント アイコン（ ）をクリックします。接続イベントに対する優先ワークフロー最初のページが表示され、ホストの IP アドレスの他、アプリケーションのタイプ、プロトコル、およびバージョンで制約されて接続イベントが示されます。接続イベントに対する優先ワークフローがない場合、ワークフローを選択する必要があります。接続データの詳細については、接続およびセキュリティ インテリジェンス のデータの使用（39-1 ページ）を参照してください。

ホスト プロファイルからのアプリケーションの削除

ライセンス：FireSIGHT

ホスト プロファイルからアプリケーションを削除して、ホスト上で稼動していないことがわかっているアプリケーションを削除することができます。ホストからアプリケーションを削除すると、そのホストにホワイト リストのコンプライアンスが適用されることがあります。

注　システムでアプリケーションが再検出されると、アプリケーションはネットワーク マップおよびホスト プロファイルに再度追加されます。

ホスト プロファイルからアプリケーションを削除する方法

アクセス：Admin/Any Security Analyst

ステップ 1　ホスト プロファイルの [Applications] セクションで、削除するアプリケーションの隣にある削除アイコン（ ）をクリックします。

アプリケーションは、そのホストに対して削除されます。

ホスト プロファイルでの VLAN タグの使用

ライセンス：FireSIGHT

ホストが仮想 LAN（VLAN）のメンバである場合、ホスト プロファイルの [VLAN Tag] セクションが表示されます。

物理ネットワーク機器は、多くの場合に VLAN を使用して、さまざまなネットワーク ブロックから論理ネットワーク セグメントを作成します。システムは 802.1q VLAN タグを検出し、それぞれに対して以下の情報を表示します。

- [VLAN ID] は、ホストがメンバである VLAN を表します。これは、802.1q VLAN の場合、0～4095 の任意の整数となります。
- [Type] は、VLAN タグが含まれている、カプセル化されたパケットを表します。値は Ethernet または Token Ring となります。
- [Priority] は、VLAN タグの優先度を表します。これは 0～7 の任意の整数で、7 は最も高い優先度です。

VLAN タグがパケット内でネスト構造になっている場合、システムは最も内側の VLAN タグを処理し、Defense Centerは最も内側の VLAN タグを表示します。システムは、ARP および DHCP トラフィックを通じて識別される MAC アドレスのみの VLAN タグ情報を収集し、Defense Center はこれらのタグを表示します。

たとえば全体がプリンタで構成されている VLAN があり、システムがこの VLAN で Microsoft Windows 2000 のオペレーティング システムを検出した場合などは、VLAN タグ情報が有用です。VLAN 情報により、システムはより正確なネットワーク マップを生成できるようになります。

ホスト プロファイルでのユーザ履歴の使用

ライセンス：FireSIGHT

ホスト プロファイルのユーザ履歴の部分には、過去 24 時間のユーザ アクティビティがグラフィック表示されます。一般的なユーザは夜間にログオフし、他のユーザとホストのリソースを共有します。電子メールのチェックなどの目的で行われる定期的なログインの要求は、短い標準の棒で示されます。ユーザのアイデンティティ リストは棒グラフで提示され、ユーザのログインが検出されたタイミングを示します。権限のないログインの場合は、棒グラフがグレーになっていることに注意してください。

システムは、ホストに対する権限を持たないユーザのログインを、そのホストの IP アドレスに関連付けて、ホストのユーザ履歴にユーザが表示されるようにします。ただし、同じホストに対して権限を持つユーザのログインが検出されると、権限を持つユーザのログインに関連付けられているユーザは、ホスト IP アドレスとの関連を引き継ぎます。権限を持たない別のユーザがログインしても、ホスト IP アドレスとユーザとの関係付けは解消されません。ユーザのタイプの詳細

については、ユーザ データベース (45-8 ページ) を参照してください。ネットワーク検出ポリシーで、失敗したログインのキャプチャを設定した場合、リストには、ホストへのログインに失敗したユーザが含まれます。

ホスト プロファイルでのホスト属性の使用

ライセンス：FireSIGHT

*ホスト属性*を使用して、ネットワーク環境にとって重要な方法でホストを分類することができます。ホスト属性の値として、正の整数、文字列、または URL を使用できます。また、文字列の値のリストを作成し、ホスト IP アドレスに基づいて、それらを自動的に割り当てることができます。ユーザ定義のホスト属性の作成および管理の詳細については、ユーザ定義のホスト属性の使用 (49-35 ページ) を参照してください。

FireSIGHT システムには、Host Criticality と Notes の 2 つの定義済みのホスト属性が含まれています。これらの定義済みホスト属性の使用については、事前定義のホスト属性の使用 (49-34 ページ) を参照してください。

また、ユーザがコンプライアンス ホワイト リストを作成すると、ホワイト リストと同じ名前のホスト属性が自動的に作成されます。使用される値は、Compliant (ホワイト リストに準拠しているホストの場合)、Non-Compliant (ホワイト リストに違反しているホストの場合)、または Not Evaluated (ホワイト リストの正当な対象ではないホスト、または何らかの理由で評価されないホストの場合) です。ホワイト リストのホスト属性の値は、手動で変更**できません**。ホワイト リストの詳細については、FireSIGHT システムのコンプライアンス ツールとしての使用 (52-1 ページ) を参照してください。

ホスト属性の値の割り当て

ライセンス：FireSIGHT

既存のホスト属性の値として、正の整数、文字列、または URL を指定できます。

ヒント　ホスト プロファイルのページの [Attributes] セクションの [Edit] リンクをクリックして、ホストのホスト属性を簡単に割り当てることができます。これにより、すべてのホスト属性のフィールドが含まれているポップアップ ウィンドウが起動されます。

ホスト属性の値を割り当てる方法

アクセス：Admin/Any Security Analyst

ステップ 1　ホスト プロファイルを開きます。

ステップ 2　[Attributes] の下で、値を割り当てるホスト属性の名前をクリックします。

ポップアップ ウィンドウが表示されます。

ステップ 3　属性の値を入力するか、またはドロップダウン リストから値を選択します。

ステップ 4　[Save] をクリックします。

ホスト属性の値が保存されます。

ホスト プロファイルでのホスト プロトコルの使用

ライセンス： FireSIGHT

ホスト プロファイルで、ホスト上で稼動しているプロトコルを表示することができます。必要に応じて、特定のホストに対するホスト プロトコルをプロファイルから削除することもできます。

各ホスト プロファイルには、ホストに関連付けられているネットワーク トラフィックで検出されたプロトコルに関する情報が含まれています。

次に、プロトコルとネットワークのレイヤ情報について説明します。

Protocol

ホストが使用するプロトコルの名前。

Layer

プロトコルを実行しているネットワーク層（**ネットワーク**または**トランスポート**）。

ホストが、有効な相関ポリシーのコンプライアンス ホワイト リストに違反するプロトコルを実行している場合、Defense Centerは非準拠プロトコルに、ホワイト リストの違反アイコン（）のマークを付けます。

ホスト プロファイルからプロトコルを削除して、ホスト上で稼動していないことがわかっているプロトコルを削除することができます。ホストからプロトコルを削除すると、そのホストにホワイト リストのコンプライアンスが適用されることがあります。

注　システムでプロトコルが再検出されると、プロトコルはネットワーク マップおよびホスト プロファイルに再度追加されます。

ホスト プロファイルからプロトコルを削除する方法

アクセス： Admin/Any Security Analyst

ステップ 1　ホスト プロファイルの [Protocols] セクションで、削除するプロトコルの隣にある削除アイコン（）をクリックします。

プロトコルは、そのホストに対して削除されます。

ホスト プロファイルにおけるホワイト リスト違反の使用

ライセンス： FireSIGHT

コンプライアンス ホワイト リスト（または*ホワイト リスト*）は一連の基準で、ユーザはこれを使用して、特定のサブネット上での実行が許可されるオペレーティング システム、アプリケーション プロトコル、クライアント、Web アプリケーション、およびプロトコルを指定することができます。

アクティブな相関ポリシーにホワイト リストを追加した場合に、システムでホワイト リストに違反しているホストが検出されると、Defense Centerはホワイト リストのイベント（相関イベントの特別な種類）をデータベースに記録します。これらのホワイト リスト イベントはそれぞれ

*ホワイト リスト違反*に関連付けられます。これには、特定のホストがどのようにホワイト リストに違反しているか、および違反している理由が含まれています。あるホストが 1 つ以上のホワイト リストに違反している場合、ホスト プロファイルにおいて、2 つの方法でこれらの違反を参照することができます。

最初に、ホスト プロファイルに、ホストに関連付けられている個々のホワイト リストの違反がすべて一覧表示されます。

次に、ホスト プロファイルにおけるホワイト リスト違反の情報について説明します。

タイプ

違反のタイプ（つまり、非準拠のオペレーティング システム、アプリケーション、サーバ、またはプロトコルのいずれが原因で違反が生じたか）。

理由

違反についての特別な理由。たとえば、Microsoft Windows のホストのみを許可するホワイト リストがある場合、ホスト プロファイルには、ホストで稼動している現行のオペレーティング システム（`Linux Linux 2.4`、`2.6` など）が表示されます。

ホワイトリスト

違反に関連付けられているホワイト リストの名前。

さらに、オペレーティング システム、アプリケーション、プロトコル、およびサーバに関連付けられたセクションでは、Defense Centerによって非準拠の要素にホワイト リスト違反のアイコン（）が付けられます。たとえば、Microsoft Windows ホストのみを許可するようなホワイト リストでは、ホスト プロファイルは、ホストのオペレーティング システム情報の隣にホワイト リスト違反のアイコンを表示します。

ホストのプロファイルを使用して、コンプライアンス ホワイト リストに対して共有のホスト プロファイルを作成できることに注意してください。詳細は、次の項、ホスト プロファイルからのホワイト リスト ホスト プロファイルの作成を参照してください。

ホスト プロファイルからのホワイト リスト ホスト プロファイルの作成

ライセンス： FireSIGHT

コンプライアンス ホワイト リストに対する共有ホスト プロファイルは、複数のホワイト リストをまたがるターゲット ホスト上で実行を許可されるオペレーティング システム、アプリケーション プロトコル、クライアント、Web アプリケーション、およびプロトコルを指定します。つまり、複数のホワイト リストを作成するが、同じホスト プロファイルを使用して複数のホワイト リストで特定のオペレーティング システムを実行するホストを評価する場合は、共有のホスト プロファイルを使用します。

既知の IP アドレスを持つ任意のホストのホスト プロファイルを使用して、コンプライアンス ホワイト リストで使用できる共有ホスト プロファイルを作成することができます。ただし、システムでホストのオペレーティング システムをまだ特定していない場合は、個々のホストのホスト プロファイルに基づいて共有ホスト プロファイルを作成することはできないことに注意してください。

ホスト プロファイルに基づいてコンプライアンス ホワイト リストに対する共有ホスト プロファイルを作成する方法

アクセス：Admin

ステップ 1　任意のネットワーク マップまたはイベント ビューからホスト プロファイルにアクセスします。

詳細については、ホスト プロファイルの表示（49-5 ページ）を参照してください。

ステップ 2　[Generate White List Profile] をクリックします。

[Edit Shared Profiles] ページが表示されます。ページのフィールドには、アクセスしたホスト プロファイルの情報に基づいて値が挿入されています。

ステップ 3　特別なニーズに応じて、共有ホスト プロファイルを変更し、保存します。

コンプライアンス ホワイト リストに対する共有ホスト プロファイルの作成については、共有ホスト プロファイルの操作（52-27 ページ）を参照してください。

ホスト プロファイルでのマルウェア検出の使用

ライセンス：FireSIGHT およびMalware

[Most Recent Malware Detections] セクションには、ホストがマルウェア ファイルを送信または受信した、最近のマルウェア イベントが最大 100 個表示されます。ホスト プロファイルは、ネットワークベースのマルウェア イベントとエンドポイントベースのマルウェア イベントの両方を表示します。

ファイルが遡ってマルウェアと識別されたファイル イベントにホストが関係している場合、ファイルが送信された元のイベントは、マルウェアの特定が行われた後で、マルウェアの検出リストに表示されます。マルウェアとして識別されたファイルが、マルウェアではないと遡って判断された場合、そのファイルに関連するマルウェア イベントはリストには表示されなくなります。たとえば、ファイルに `Malware` の処理が含まれており、その処理が `Clean` に変わった場合、そのファイルのイベントは、ホスト プロファイル上のマルウェア検出リストから削除されます。マルウェア イベントの詳細については、マルウェア イベントの操作（40-17 ページ）を参照してください。

次に、ホスト プロファイルの [Most Recent Malware Detections] セクションのカラムについて説明します。

時刻

イベントが生成された日時。

ファイルがマルウェアであると遡って特定されたイベントでは、これはマルウェアが特定された時刻ではなく、元のイベントの時刻であることに注意してください。

Host Role

検出されたマルウェアの伝送におけるホストの役割（送信者または受信者）。エンドポイントベースのマルウェア イベントの場合は、ホストは常に受信者であることに注意してください。

Threat Name

検出されたマルウェアの名前。

File Name

マルウェア ファイルの名前。

File Type

ファイルのタイプ（PDF や MSEXE など）。

ホスト プロファイルでマルウェアの検出を表示する場合は、イベント ビューアで、そのホストのマルウェア イベントを表示できます。イベントを表示するには、マルウェアのアイコン（  ）をクリックします。

ホスト プロファイルでの脆弱性の使用

ライセンス： FireSIGHT

ホスト プロファイルの [Vulnerabilities] セクションには、ホストに影響を与える脆弱性が示されます。

[Sourcefire Vulnerabilities] セクションには、システムがホスト上で検出したオペレーティング システム、サーバ、およびアプリケーションに基づいた脆弱性が示されます。

ホストのオペレーティング システムのアイデンティティ、またはホスト上のアプリケーション プロトコルのアイデンティティのいずれかで、アイデンティティの競合が発生している場合、システムは、競合が解決するまで両方のアイデンティティに対して脆弱性を表示します。

NetFlow データに基づいてネットワーク マップに追加されたホストで使用できるオペレーティング システムの情報がないため、ホストの入力機能を使用してホストのオペレーティング システムのアイデンティティを手動で設定しない限り、Defense Centerはどの脆弱性がホストに影響を与えるかを判断できません。

サーバのベンダーおよびバージョンの情報は、ほとんどの場合はトラフィックに含まれていません。デフォルトでは、システムはこのようなトラフィックの送信側および受信側に対して、関連付けられている脆弱性をマップしません。ただし、システム ポリシーを使用して、ベンダーまたはバージョンの情報を持たない特定のアプリケーション プロトコルに対して脆弱性をマップするよう、システムを設定することができます。詳細については、サーバの脆弱性のマッピング（63-32 ページ）を参照してください。

ホスト入力機能を使用して、ネットワーク上のホストに関するサードパーティの脆弱性情報を追加すると、追加の [Vulnerabilities] セクションが表示されます。たとえば QualysGuard Scanner から脆弱性をインポートすると、ホスト プロファイルには [QualysGuard Vulnerabilities] セクションが含まれます。

サードパーティの脆弱性をオペレーティング システムおよびアプリケーション プロトコルと関連付けることはできますが、クライアントに関連付けることはできません。サードパーティの脆弱性のインポートについては、『*FireSIGHT System Host Input API Guide*』を参照してください。

次に、ホスト プロファイルの [Vulnerabilities] セクションのカラムについて説明します。

名前

脆弱性の名前。

Remote

脆弱性がリモートで不正利用される可能性があるかどうかを示します。この列が空白の場合、脆弱性の定義にはこの情報は含まれていません。

コンポーネント

脆弱性に関連付けられているオペレーティング システム、アプリケーション プロトコル、またはクライアントの名前。

ポート

ポート番号（脆弱性が、特定のポート上で実行されているアプリケーション プロトコルに関連付けられている場合）。

サードパーティの脆弱性の場合は、ホスト プロファイルの対応する [Vulnerabilities] セクションの情報は、ホストの入力機能を使用して脆弱性データをインポートしたときに提供した情報に制限されます。

ホスト プロファイルで脆弱性を表示する場合には、次のことが可能です。

- 列見出しをクリックして、[Vulnerabilities] セクションの列をソートする。ソートを元に戻すには、もう一度クリックします。
- 脆弱性の名前をクリックして、脆弱性に関する技術的な詳細（既知の解決方法など）を表示する。詳細については、「脆弱性の詳細の表示（49-30 ページ）」を参照してください。脆弱性のイベント ビュー、または Vulnerabilities ネットワーク マップから、脆弱性の詳細にアクセスできることに注意してください。
- 脆弱性が、影響の相関関係を評価するために使用されないようにする。詳細については、「脆弱性の Impact Qualification の設定（49-32 ページ）」を参照してください。
- ネットワーク上のホストで検出された脆弱性を軽減するためのパッチをダウンロードする。詳細については、「脆弱性に対するパッチのダウンロード（49-33 ページ）」を参照してください。
- ホストにパッチが適用されたことがわかっている場合は、個々の脆弱性について脆弱ではないとホストをマークする。詳細については、「個々のホストに対する脆弱性の設定（49-33 ページ）」を参照してください。

脆弱性の詳細の表示

ライセンス： FireSIGHT

脆弱性の詳細には、脆弱性および既知の解決方法に関する技術的な説明が含まれています。

特定の脆弱性について脆弱性の詳細にアクセスするには、[Analysis] > [Vulnerabilities]、または [Analysis] > [Third-Party Vulnerabilities] を選択し、SVID の隣の表示アイコン（  ）をクリックします。ネットワーク マップおよびホスト プロファイルから脆弱性の詳細にアクセスすることもできます。

次に、[Vulnerability Detail] ページのフィールドについて説明します。

Cisco Vulnerability ID

脆弱性を追跡するためにシステムで使用する識別番号（SVID）。

Snort ID

Snort ID（SID）データベースにおいて脆弱性に関連付けられている識別番号。つまり、侵入ルールで特定の脆弱性を悪用するネットワーク トラフィックを検出できる場合、その脆弱性は侵入ルールの SID に関連付けられます。

脆弱性は複数の SID に関連付けることが可能（または SID に関連付けないことも可能）であることに注意してください。脆弱性に関連付けられている SID がない場合は、このフィールドは表示されません。

BugTraq ID

Bugtraq データベースで脆弱性に関連付けられている識別番号（http://www.securityfocus.com/bid）。

CVE ID

MITRE の Common Vulnerabilities and Exposures（CVE）データベースで、脆弱性に関連付けられている識別番号（http://www.cve.mitre.org/）。

Title

脆弱性のタイトル。

Impact Qualification

ドロップダウン リストを使用して、脆弱性を有効または無効にします。Defense Centerは、影響の相関関係において、無効な脆弱性を無視します。

ここで指定する設定によって、システム全体で脆弱性がどのように処理されるか、およびユーザが値を選択するホスト プロファイルに脆弱性が限定されるかどうかが決まります。この機能を使用して脆弱性を有効および無効にするための情報については、脆弱性の Impact Qualification の設定（49-32 ページ）を参照してください。

Date Published

脆弱性が公開された日付。

Vulnerability Impact

Bugtraq データベースにおいて脆弱性に割り当てられている重大度。1～10の値で、10 は最も重大であることを示します。脆弱性の影響は、Bugtraq エントリの作成者によって決定されます。この作成者は、SANS Critical Vulnerability Analysis（CVA）の基準に従い、自身の判断に基づいて脆弱性の影響レベルを決定します。

Remote

脆弱性がリモートで不正利用されるかどうかを示します。

Available Exploits

脆弱性に対して既知の不正利用があるかどうかを示します。

説明

脆弱性に関する概要的な説明。

Technical Description

脆弱性に関する詳細な技術的説明。

ソリューション

脆弱性の修復に関する情報。

その他の情報

既知の不正利用や可用性、不正利用のシナリオ、脆弱性を軽減する方針など、脆弱性に関する追加情報を（利用可能な場合に）表示するには、矢印をクリックします。

Fixes

選択した脆弱性に対して、ダウンロード可能なパッチへのリンクを提供します。

ヒント　修正またはパッチのダウンロードへの直接リンクが表示されている場合は、リンクを右クリックして、自分のローカル コンピュータに保存します。

脆弱性の Impact Qualification の設定

ライセンス：FireSIGHT

システムが、ネットワークに対して適用されない脆弱性を報告した場合は、影響フラグの相関を評価するのに脆弱性が使用されないようにすることができます。ホスト プロファイルで脆弱性を非アクティブにした場合、ネットワーク上のすべてのホストに対して脆弱性が非アクティブになることに注意してください。ただし、脆弱性は随時に再アクティブ化できます。

ホストのオペレーティング システム、またはホスト上のいずれかのアプリケーションのアイデンティティについて競合が存在する場合、システムは、競合が解決されるまで、競合している両方のアイデンティティに対して脆弱性を示します。詳細については、ID の競合について（46-7 ページ）およびオペレーティング システムのアイデンティティの競合を解決する（49-15 ページ）を参照してください。

システムは、Impact Qualification 機能を使用して無効にする脆弱性に基づいて、侵入ルールのルール状態を推奨しないことにも注意してください。詳細については、ネットワーク資産に応じた侵入防御の調整（33-1 ページ）を参照してください。

ヒント　ネットワーク マップおよび脆弱性のイベント ビューから脆弱性を非アクティブにすることもできます。詳細については、脆弱性のネットワーク マップの使用（48-8 ページ）および脆弱性の非アクティブ化（50-57 ページ）を参照してください。

システム全体で脆弱性の使用を変更する方法

アクセス：Admin/Any Security Analyst

ステップ 1　非アクティブにする脆弱性によって影響されるホストのホスト プロファイルにアクセスします。

ステップ 2　[Vulnerabilities] セクションを展開します。

ステップ 3　有効または無効にする脆弱性の名前をクリックします。

ポップアップ ウィンドウが表示され、脆弱性の詳細が示されます。詳細については、脆弱性の詳細の表示（49-30 ページ）を参照してください。

ステップ 4　[Impact Qualification] ドロップダウン リストから [Disabled] または [Enabled] を選択して、脆弱性がどのように使用されるかを指定します。

ステップ 5　ネットワーク マップ上のすべてのホストに対して、Impact Qualification を変更することを確認します。

脆弱性が有効または無効になります。

ステップ 6　[Done] をクリックして、脆弱性の詳細のポップアップ ウィンドウを閉じます。

脆弱性に対するパッチのダウンロード

ライセンス：FireSIGHT

利用可能な場合、ネットワーク上のホストで検出された脆弱性を軽減するためのパッチをダウンロードすることができます。

脆弱性に対するパッチをダウンロードする方法

アクセス：Admin/Any Security Analyst

ステップ 1　パッチをダウンロードするホストのホスト プロファイルにアクセスします。

ステップ 2　[Vulnerabilities] セクションを展開します。

ステップ 3　パッチを適用する脆弱性の名前をクリックします。

[Vulnerability Detail] ページが表示されます。

ステップ 4　[Fixes] セクションを展開します。

脆弱性に対してダウンロード可能なパッチの一覧が表示されます。

ステップ 5　ダウンロードするパッチの隣の [Download] をクリックします。

パッチ ベンダーのダウンロード ページが表示されます。

ステップ 6　パッチをダウンロードして、影響を受けるシステムに適用します。

個々のホストに対する脆弱性の設定

ライセンス：FireSIGHT

ホストの脆弱性エディタを使用して、ホストごとに脆弱性をアクティブまたは非アクティブにすることができます。ホストの脆弱性を非アクティブにしても、そのホストの影響の相関に対して脆弱性は使用されますが、影響レベルは自動的に 1 レベル減少します。

1 つのホストに対して脆弱性をアクティブまたは非アクティブにする方法

アクセス：Admin/Security Analyst

ステップ 1　ホスト プロファイルを開きます。

ステップ 2　[Vulnerabilities] の隣で [Edit] をクリックします。

[Host Vulnerabilities editor] ページが表示されます。

ヒント　脆弱性に関する詳細を表示するには、[View] をクリックします。詳細については、脆弱性の詳細の表示（49-30 ページ）を参照してください。

ステップ 3　次の 2 つのオプションから選択できます。

- 脆弱性を非アクティブにするには、[Valid Vulnerabilities] リストから脆弱性を選択し、下向きの矢印をクリックします。
- 脆弱性をアクティブにするには、[Invalid Vulnerabilities] リストから脆弱性を選択し、上向きの矢印をクリックします。

ヒント　複数の脆弱性を選択するには、Ctrl キーまたは Shift キーを押しながらクリックします。隣接している複数の脆弱性を選択するには、クリックおよびドラッグを使用します。脆弱性をダブルクリックして、リスト間を移動することもできます。

ステップ 4　[Save] をクリックします。

変更が保存されます。

事前定義のホスト属性の使用

ライセンス: FireSIGHT

各ホストに割り当てることができる事前定義のホスト属性として、ホストの重要度とホスト特有のメモの 2 つの属性があります。ホストの重要度の属性を使用して、特定のホストのビジネス重要度を指定し、ホストの重要度に基づいて相関ポリシーとアラートを作成できます。たとえば業務にとって、組織のメール サーバは一般的なユーザ ワークステーションよりも重要であるとみなしている場合は、メール サーバ、および業務にとって重要なその他のデバイスに High の値を割り当てて、他のホストに Medium または Low の値を割り当てることができます。次に相関ポリシーを作成できます。これは、影響を受けるホストの重要度に基づいてさまざまなアラートを起動します。

メモ機能を使用して、他の分析を表示するホストの情報を記録します。たとえば、ネットワーク上のコンピュータに、パッチが適用されていない古いバージョンの、テスト用オペレーティング システムが搭載されている場合、メモ機能を使用して、システムは意図的にパッチが適用されていないと示すことができます。

ホスト プロファイルで事前定義のホスト属性を設定する方法

アクセス: Admin/Security Analyst

ステップ 1　ビジネスの重要度を設定するホストのホスト プロファイルを開きます。

ステップ 2　[Attributes] の隣の鉛筆型のアイコン( )をクリックします。

[Host Attributes] ポップアップ ウィンドウが表示されます。

ステップ 3　[Host Criticality] ドロップダウン リストから、適用する値として [None]、[Low]、[Medium]、または [High] を選択します。

ステップ 4　[Save] をクリックします。

選択した内容が保存されます。

ユーザ定義のホスト属性の使用

ライセンス：FireSIGHT

FireSIGHT システムには、ホストの重要度とホスト メモの 2 つの事前定義のホスト属性があります。これらの属性を使用して、ネットワーク上のホストのビジネスでの重要度を示すことができます。ホストを識別するための他の基準がある場合は、ユーザ定義のホスト属性を作成できます。

ユーザ定義のホスト属性は、ホスト プロファイルのページに表示されます。ここでホストごとに値を割り当てることができます。相関ポリシーまたは検索でこれらの属性を使用することができます。また、イベントのホスト属性テーブル ビューで属性を表示して、それに基づいてレポートを生成することもできます。

注　ホスト属性は、ポリシーごとではなくグローバルに定義されます。作成したホスト属性は、適用されるポリシーに関係なく使用できます。

ユーザ定義のホスト属性の例として、次のものがあります。

- ホストに対する、ファシリティ コード、市町村、部屋番号などの物理的なロケーション ID の割り当て。
- 特定のホストに対して、どのシステム管理者が責任を持っているのかを示すための Responsible Party Identifier の割り当て。ホストに関連する問題が検出された場合、相関ルールとポリシーを作成して、適切なシステム管理者にアラートを送信することができます。

ホスト属性として、テキスト文字列、テキストの事前定義されたリストから選択した値、または数字の範囲を使用できます。ホストの IP アドレスに基づいて、事前定義されたリストからホストへ自動的に値を割り当てることもできます。この機能を使用すると、ネットワーク上にホストが初めて表示されたときに、新しいホストへ値を自動的に割り当てることができます。

ホスト属性として、次のタイプのいずれか 1 つを使用できます。

テキスト

ホストに対して最大 255 文字のテキスト文字列を手動で割り当てることができます。

Integer

正の整数の番号範囲の最初の数と最後の数を指定し、ホストに対してこれらの番号を手動で割り当てることができます。

List

文字列値のリストを作成し、ホストに対してこの値のいずれかを割り当てることができます。また、ホストの IP アドレスに基づいて、ホストに対して値を自動的に割り当てることもできます。

注　複数の IP アドレスを持つホストの 1 つの IP アドレスに基づいて値を自動的に割り当てると、これらの値は、ホストに関連付けられているすべてのアドレスに適用されます。Host Attributes テーブルを参照する場合は、このことに注意してください。

URL

ホストに対して手動で URL の値を割り当てることができます。

ユーザがコンプライアンス ホワイト リストを作成すると、ホワイト リストと同じ名前のホスト属性が自動的に作成されることに注意してください。使用される値は、Compliant（ホワイト リストに準拠しているホストの場合）、Non-Compliant（ホワイト リストに違反しているホストの場合）、および Not Evaluated（ホワイト リストの正当な対象ではないホスト、または何らかの理由で評価されないホストの場合）です。ホワイト リストのホスト属性の値は、手動で変更**できません**。ホワイト リストの詳細については、FireSIGHT システムのコンプライアンス ツールとしての使用（52-1 ページ）を参照してください。

詳細については、次の項を参照してください。

- ユーザ定義のホスト属性の作成（49-36 ページ）
- ユーザ定義ホスト属性の編集（49-38 ページ）
- ユーザ定義ホスト属性の削除（49-38 ページ）

ユーザ定義のホスト属性の作成

ライセンス： FireSIGHT

次の手順では、ユーザ定義のホスト属性の作成方法について説明します。

注　ホスト属性は、ポリシーごとではなくグローバルに定義されます。作成したホスト属性は、適用されるポリシーに関係なく使用できます。

新しいホスト属性を作成する方法

アクセス： Admin/Discovery Admin

ステップ 1　[Analysis] > [Hosts] > [Host Attributes] を選択します。

[Host Attributes] ページが表示されます。

ステップ 2　[Host Attribute Management] をクリックします。

[Host Attribute Management] ページが表示されます。

ステップ 3　[Create Attribute] をクリックします。

[Create Attribute] ページが表示されます。

ステップ 4　[Name] フィールドに、英数字および空白を使用してホスト属性の名前を入力します。

ステップ 5　ホスト プロファイルでのホスト属性の使用（49-25 ページ）の説明に従って、[Type] ドロップダウン リストから、作成する属性のタイプを選択します。

- [Text] または [URL] ホスト属性を作成する場合は、続いて6の手順を実行します。
- [Integer] ホスト属性を作成する場合は、整数ホスト属性の作成（49-37 ページ）を参照してください。
- [List] ホスト属性を作成する場合は、リスト ホスト属性の作成（49-37 ページ）を参照してください。

ステップ 6　[Save] をクリックします。

新しいユーザ定義のホスト属性が保存されます。

整数ホスト属性の作成

ライセンス：FireSIGHT

整数ベースのホスト属性を定義する場合は、その属性に使用できる数字の範囲を指定する必要があります。

整数ベースのホスト属性を作成する方法

アクセス：Admin/Discovery Admin

ステップ 1　[Min] フィールドに、ホストに対して割り当てることができる範囲の最小の整数値を入力します。

ステップ 2　[Max] フィールドに、ホストに対して割り当てることができる範囲の最大の整数値を入力します。

ステップ 3　[Save] をクリックします。

新しい整数ベースのホスト属性が保存されます。

リスト ホスト属性の作成

ライセンス：FireSIGHT

リストベースのホスト属性を定義する場合は、リストに対してそれぞれの値を指定する必要があります。これらの値には、英数字、スペース、および記号を含めることができます。

ホスト属性の値を作成する場合は、IP アドレスのブロックに値を自動的に割り当てて、新しいホストが検出されたときに、ホスト属性の値が自動的に割り当てられるようにすることもできます。

リストベースのホスト属性を作成する方法

アクセス：Admin/Discovery Admin

ステップ 1　リストに値を追加するには、[Add Value] をクリックします。

[List Values] セクションが展開されます。

ステップ 2　[Name] フィールドに、英数字、記号、およびスペースを使用して、追加する最初の値を入力します。

ステップ 3　オプションで、ホストに追加した属性値を自動で割り当てるには、[Add Networks] をクリックします。

[Auto-Assign Networks] セクションが展開されます。

ステップ 4　[Value] ドロップダウン リストから、追加した値を選択します。

ステップ 5　[IP Address] および [Netmask] フィールドに、IP アドレス、およびこの値を自動割り当てする IP アドレスのブロックを表すネットワーク マスクを（CIDR 表記で）入力します。

FireSIGHT システムでの CIDR 表記の使用の詳細については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ステップ 6　リストにさらに値を追加して、IP アドレス ブロックの範囲内の新しいホストにこれらの値を自動的に割り当てるには、手順 1 ～ 5 を繰り返します。

ヒント　特定の IP ブロック内のホストに対してリストの値を自動割り当てしない場合は、事前定義のホスト属性の使用（49-34 ページ）の説明に従って手動で割り当てることができます。

ユーザ定義ホスト属性の編集

ライセンス：FireSIGHT

ユーザ定義の既存のホスト属性を変更する場合、値の定義は変更できますが、属性のタイプ（テキスト、リスト、整数、URL）は変更できません。また、コンプライアンス ホワイト リストのホスト属性を変更することは**できません**。

ユーザ定義の既存のホスト属性を編集する方法

アクセス：Admin/Discovery Admin

ステップ 1　[Analysis] > [Hosts] > [Host Attributes] を選択します。

[Host Attributes] ページが表示されます。

ステップ 2　[Host Attribute Management] をクリックします。

[Host Attribute Management] ページが表示されます。

ステップ 3　編集するホストの属性の隣にある編集アイコン（  ）をクリックします。

ホスト属性のページは、選択した属性の設定とともに表示されます。

ステップ 4　必要に応じて設定を変更し、[Save] をクリックします。

編集可能な属性タイプについて、およびそれらの属性に含まれる値については、ユーザ定義のホスト属性の作成（49-36 ページ）を参照してください。

ユーザ定義ホスト属性の削除

ライセンス：FireSIGHT

ユーザ定義のホスト属性を削除して、その属性が使用されたすべてのホスト プロファイルから削除します。コンプライアンス ホワイト リストのホスト属性を削除することは**できません**。

ホスト属性を削除する方法

アクセス：Admin/Discovery Admin

ステップ 1　[Analysis] > [Hosts] > [Host Attributes] を選択します。

[Host Attributes] ページが表示されます。

ステップ 2　[Host Attribute Management] をクリックします。

[Host Attribute Management] ページが表示されます。

ステップ 3　削除するホスト属性の隣にある削除アイコン（  ）をクリックします。

選択したホスト属性がシステムから削除されます。

ホスト プロファイルでのスキャン結果の使用

ライセンス：FireSIGHT

Nmap を使用してホストをスキャンする場合、または Nmap のスキャンから結果をインポートする場合、これらの結果は、スキャンに含まれているすべてのホストのホスト プロファイルに表示されます。

Nmap が、ホストのオペレーティング システムについて、およびオープンでフィルタリングされていないポート上で稼動している任意のサーバについて収集した情報が、ホスト プロファイルの [Operating System] と [Servers] セクションにそれぞれ追加されます。また、Nmap は、そのホストのスキャン結果のリストを [Scan Results] セクションに追加します。

各結果には、情報のソース、スキャンしたポートの番号とタイプ、ポート上で稼動しているサーバの名前、Nmap で検出された任意の追加情報（ポートの状態やサーバのベンダー名など）が示されます。UDP ポートをスキャンする場合、そのポートで検出されたサーバは [Scan Results] セクションにのみ表示されます。

ホスト プロファイルから Nmap スキャンを実行できることに注意してください。詳細は、次の項、ホスト プロファイルからのホストのスキャンを参照してください。

ホスト プロファイルからのホストのスキャン

ライセンス：FireSIGHT

ホスト プロファイルから、ホストに対して Nmap スキャンを実行できます。スキャンが完了すると、そのホストのサーバおよびオペレーティング システムの情報は、ホスト プロファイルで更新されます。追加のスキャン結果は、すべてホスト プロファイルの [Scan Results] セクションに追加されます。

注意　Nmap 提供のサーバおよびオペレーティング システムのデータは、別の Nmap スキャンを実行するか、より優先度の高いホスト入力で上書きするまでスタティックなままになります。Nmap を使用してホストをスキャンする場合は、定期的にスケジュールされたスキャンをセットアップして、Nmap 提供のオペレーティング システムとサーバのデータを最新の状態に保つことができます。詳細については、Nmap スキャンの自動化（62-5 ページ）を参照してください。

ホスト プロファイルからホストをスキャンする方法

アクセス：Admin

ステップ 1　ホスト プロファイルで [Scan Host] をクリックします。

[Scan Host] ポップアップ ウィンドウが表示されます。

ステップ 2　ホストのスキャンで使用するスキャン修復の隣にある [Scan] をクリックします。

ホストがスキャンされ、結果がホスト プロファイルに追加されます。

CHAPTER 50

ディスカバリ イベントの使用

ディスカバリ イベントは、ユーザにネットワーク上のアクティビティを警戒するよう警告し、適切に対応する必要がある情報を提供します。これらのイベントは、管理対象デバイスが監視しているネットワーク セグメント内で、管理対象デバイスが検出する変更によってトリガーされます。*ネットワーク検出ポリシー*は、システムが収集するデータの種類、監視対象ネットワーク セグメント、およびシステムがトラフィックの監視で使用する特定のハードウェア インターフェイスについて明記しています。ネットワーク検出 の詳細については、検出データ収集について (45-1 ページ)を参照してください。

ディスカバリ イベントの簡単な例として、会議室または予備の作業空間があり、そこへ来た従業員がネットワークにアクセスする場合があります。ユーザはこれらのセグメントで生成される New Host イベントを定期的に見ることが予想されますが、悪意のある行為だとは疑わないでしょう。ただし、ロック ダウンしたネットワーク セグメントで New Host イベントが見つかった場合は、それに応じて、応答のエスカレーションを行うことができます。

ユーザ ディスカバリ イベントは、ネットワーク上のホストにログインしているユーザに関する情報を提供します。ユーザは、ネットワーク上のユーザ アクティビティをカタログしているイベントを表示してドリル ダウンし、特定のユーザの情報を表示することができます。たとえば、新しいホストに関連付けられているユーザを表示する場合は、ホスト プロファイルを確認し、対象のホストとやりとりしているトラフィックで検出されたのがどのユーザかを特定することができます。

ディスカバリ イベントは、このような簡単な例に比べて、ネットワーク上のアクティビティを知るうえではるかに詳しく、精度の高い情報を提供します。監視されている各ホストについて、関連するアプリケーション プロトコル、ネットワーク プロトコル、クライアント、ユーザ、および潜在的な脆弱性を検出するようシステムを設定することができます。システムは、ユーザがホスト入力機能を使用してDefense Centerにインポートしたサードパーティのスキャナで検出された脆弱性についても情報を提供することができます。侵害の痕跡(IOC)は侵入、マルウェア、および他のデータを使用して、セキュリティが侵害される可能性があるホストを特定します。またユーザは、ユーザ インターフェイスを介して入力するホストの重要度、ホスト属性、脆弱性の設定における何らかの変更を追跡できます。

システムには事前定義のワークフロー セットが用意されており、これを使用して、システムで生成されるディスカバリ イベントを分析することができます。また、特定のニーズにあった情報のみを表示するカスタム ワークフローを作成することもできます。

分析用にネットワーク検出データを収集および格納するには、Ciscoの管理対象デバイスおよびNetFlow 対応デバイスがトラフィックを監視するネットワークおよびゾーンで適切なデータを検出するように、ネットワーク検出ポリシーを設定する必要があります。監視対象領域をディスカバリの範囲から除外するには、ネットワーク検出ポリシーで設定します。ネットワーク検出ポリシーを適用する前に、アクセス コントロール ポリシーを管理対象デバイスに適用する必要があります。詳細については、ネットワーク検出ポリシーの作成 (45-25 ページ)を参照してください。

詳細については、以下を参照してください。

ディスカバリ イベントの統計情報の表示

ライセンス： FireSIGHT

[Discovery Statistics] ページには、システムで検出されたホスト、イベント、プロトコル、アプリケーション プロトコル、およびオペレーティング システムの概要が表示されます。

- 統計情報の概要は、イベントの合計、アプリケーション プロトコル、ホスト、ネットワーク デバイス、およびホストの使用制限に関する全般的な情報を提供します。統計情報のサマリ（50-3 ページ）を参照してください。
- イベントの明細には、システムで発生しているイベントのタイプに関する統計情報が示されます。Event Breakdown（50-4 ページ）を参照してください。
- プロトコルの明細には、検出されたホストで使用しているプロトコルに関する統計情報が示されます。Protocol Breakdown（50-5 ページ）を参照してください。
- アプリケーション プロトコルの明細には、ネットワーク上で稼動しているアプリケーション プロトコルの統計情報が示されます。Application Protocol Breakdown（50-5 ページ）を参照してください。
- オペレーティング システムの明細には、ネットワーク上で稼動しているオペレーティング システムについて、およびそれぞれのオペレーティング システムを何台のホストが使用しているかが示されます。OS Breakdown（50-5 ページ）を参照してください。

ページには、最後の 1 時間の統計情報、および累計の統計情報が示されます。特定のデバイス、またはすべてのデバイスについての統計情報を選択することができます。サマリに示されているイベント、サーバー、オペレーティング システム、またはオペレーティング システムのベンダーをクリックして、ページ上のエントリに一致するイベントを表示することもできます。

ディスカバリ統計情報サマリを表示するには、以下を行います。

アクセス: Admin/Any Security Analyst

ステップ 1　[Overview] > [Summary] > [Discovery Statistics] を選択します。

統計情報のサマリ ページが表示されます。

ステップ 2　[Select Device] リストから、統計情報を表示するデバイスを選択します。Defense Centerで管理されるすべてのデバイスの統計情報を表示するには、[All] を選択します。

統計情報のサマリ

ライセンス: FireSIGHT

統計情報のサマリは、イベントの合計、アプリケーション プロトコル、ホスト、ネットワーク デバイス、およびホストの使用制限に関する全般的な統計情報を提供します。

[Statistics Summary] セクションの行の説明は次のとおりです。

Total Events

Defense Centerに格納されているディスカバリ イベントの合計数。

Total Events Last Hour

最後の 1 時間に生成されたディスカバリ イベントの合計数。

Total Events Last Day

最後の 1 日に生成されたディスカバリ イベントの合計数。

Total Application Protocols

検出されたホストで実行されているサーバのアプリケーション プロトコルの合計数。

Total IP Hosts

一意の IP アドレスによって特定された検出済みホストの合計数。

Total MAC Hosts

IP アドレスで特定されない検出済みホストの合計数。

すべてのデバイス、または特定のデバイスのどちらについてのディスカバリ統計情報を参照している場合でも、[Total MAC Hosts] の統計情報は同じになることに注意してください。これは、管理対象デバイスが IP アドレスに基づいてホストを検出するためです。この統計情報は、他の方法によって識別され、特定の管理対象デバイスに依存しないすべてのホストの合計を表します。

Total Routers

ルータとして識別された検出ノードの合計数

Total Bridges

ブリッジとして識別された検出ノードの合計数

Host Limit Usage

使用中のホスト制限のパーセンテージ合計。ホストの制限は、FireSIGHT のライセンスによって定義されます。すべての管理対象デバイスについての統計情報を表示している場合は、ホストの使用制限のみが表示されることに注意してください。モニタリングしているホストの使用についての詳細は、FireSIGHT ホスト使用量モニタリングの設定（68-18 ページ）を参照してください。

注　ホストの制限に達して、あるホストが削除された場合、ディスカバリを実行するよう設定されたすべての管理対象デバイスでネットワーク検出を再開するまで、ホストはネットワーク マップに表示されません。

Last Event Received

最後のディスカバリ イベントが行われた日付と時間。

Last Connection Received

最後の接続が完了した日付と時間。

Event Breakdown

ライセンス： FireSIGHT

[Event Breakdown] セクションには、データベースに格納されている各イベント タイプの合計数のカウントの他に、ネットワーク検出の各タイプのカウント、および最後の 1 時間で発生したホスト入力イベントが示されます。各イベント タイプの詳細な説明については、ディスカバリ イベントのタイプについて（50-10 ページ）およびホスト入力イベントのタイプについて（50-14 ページ）を参照してください。

[Event Breakdown] セクションを使用して、ディスカバリ イベントおよびホスト入力イベントの詳細を表示することもできます。

ネットワーク検出 イベントおよびホスト入力イベントをタイプごとに表示するには、以下を行います。

アクセス： Admin/Any Security Analyst

ステップ 1　表示するイベントのタイプをクリックします。

デフォルトのディスカバリ イベント ワークフローの最初のページが、選択したイベント タイプによって制約されて表示されます。カスタム ワークフローなどの別のワークフローを使用するには、ワークフロー タイトルの近くの [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。イベントが表示されない場合は、時間範囲の調整が必要なことがあります。イベント時間の制約の設定（58-26 ページ）を参照してください。

ディスカバリ イベントの使用については、ディスカバリ イベントとホスト入力イベントの使用（50-9 ページ）を参照してください。

Protocol Breakdown

ライセンス：FireSIGHT

[Protocol Breakdown] セクションには、検出されたホストで使用されているプロトコルが示されます。このセクションでは、検出されたそれぞれのプロトコル名、プロトコル スタックの「レイヤ」、およびプロトコルを使用して通信しているホストの合計数を表示します。

Application Protocol Breakdown

ライセンス：FireSIGHT

[Application Protocol Breakdown] セクションには、検出されたホストで使用されているアプリケーション プロトコルが示されます。このセクションでは、プロトコル名、最後の 1 時間にアプリケーション プロトコルを実行したホストの合計数、いずれかのポイントでプロトコルの実行が検出されたホストの合計数を表示します。

[Application Protocol Breakdown] セクションにより、検出されたプロトコルを使用しているサーバの詳細を表示することもできます。

リストされたアプリケーション プロトコルを使用しているサーバを表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

ステップ 1　表示するアプリケーション プロトコルの名前をクリックします。

デフォルトのサーバ ワークフローの最初のページが、選択したアプリケーション プロトコルによって制約されて表示されます。カスタム ワークフローなどの別のワークフローを使用するには、ワークフロー タイトルの近くの [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

サーバの使用については、サーバの使用（50-39 ページ）を参照してください。

OS Breakdown

ライセンス：FireSIGHT

[OS Breakdown] セクションには、監視対象ネットワーク上で稼動しているオペレーティング システム、およびオペレーティング システムのベンダー、各オペレーティング システムを実行しているホストの合計数が示されます。

オペレーティング システムの名前またはバージョンの値が `unknown` の場合は、オペレーティング システムまたはそのバージョンが、システムのフィンガープリントの内容と一致しないことを意味します。値が `pending` の場合は、オペレーティング システムまたはそのバージョンを識別するための十分な情報がシステムで収集されていないことを意味します。

[OS Breakdown] セクションを使用して、検出されたオペレーティング システムの詳細を表示することができます。

オペレーティング システムまたはベンダーによってホストを表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

ステップ 1　次の 2 つのオプションから選択できます。

- 特定のオペレーティング システムを実行しているすべてのホストを表示するには、[OS Name] の下でオペレーティング システムの名前をクリックします。
- 特定のベンダーからいずれかのオペレーティング システムを実行しているすべてのホストを表示するには、[OS Vendor] の下でベンダーの名前をクリックします。

デフォルトのホスト ワークフローの最初のページが、選択したオペレーティング システムまたはベンダーによって制約されて表示されます。カスタム ワークフローなどの別のワークフローを使用するには、ワークフロー タイトルの近くの [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

ホストの使用については、ホストの使用（50-21 ページ）を参照してください。

ディスカバリのパフォーマンス グラフの表示

ライセンス：FireSIGHT

ディスカバリ イベントを使用して、管理対象デバイスのパフォーマンス統計情報を示すグラフを生成することができます。

注　新しいデータは、統計情報のグラフに 5 分ごとに累積されます。したがって、グラフをすぐにリロードしても、次の 5 分の差分更新が実行されるまでデータは変更されていない場合があります。

次に、使用できるグラフのタイプについて説明します。

Processed Events/Sec

Data Correlator が 1 秒間に処理するイベントの数を表します。

Processed Connections/Sec

Data Correlator が 1 秒間に処理する接続の数を表します。

Generated Events/Sec

システムが 1 秒間に生成するイベントの数を表します。

Mbits/Sec

ディスカバリ プロセスによって 1 秒間に分析されたトラフィック数（メガビット）を表します。

Avg Bytes/Packet

ディスカバリ プロセスによって分析された各パケットに含まれるバイト数の平均を表します。

K Packets/Sec

ディスカバリ プロセスで 1 秒間に分析されるパケット数を 1000 単位で表します。

ディスカバリのパフォーマンス グラフを生成するには、以下を行います。

アクセス：Admin/Maint

ステップ 1　[Overview] > [Summary] > [Discovery Performance] を選択します。

[Discovery Performance] ページが表示されます。

ステップ 2　[Select Device] リストから、Defense Centerまたは対象とする管理対象デバイスを選択します。

[Select Graph(s)] リストでは、選択するアプライアンスによって、使用できるグラフの表示が変わります。

ステップ 3　[Select Graph(s)] リストから、作成するグラフのタイプを選択します。

ヒント　Ctrl キーまたは Shift キーを押しながらグラフのタイプをクリックすると、複数のグラフを選択できます。

ステップ 4　[Select Time Range] リストから、グラフで使用する時間範囲を選択します。直近の 1 時間、1 日、1 週間、または 1 月を選択できます。

ステップ 5　[Graph] をクリックして、選択した統計情報をグラフ化します。

選択したグラフが表示されます。

ディスカバリ イベントのワークフローについて

ライセンス：FireSIGHT

Defense Centerは、ネットワークで生成されるディスカバリ イベントの分析で使用できるワークフロー セットを提供します。ワークフローはネットワーク マップとともに、ネットワーク資産に関する主要な情報源になります。これらのワークフローには、システムによって生成されたディスカバリ データが挿入されたテーブルが含まれています。

[Analysis] > [Hosts] メニューから、ネットワークのディスカバリ ワークフローにアクセスします。Defense Centerには、検出されたホストとそのホストの属性、サーバ、アプリケーション、アプリケーションの詳細、脆弱性、ユーザ アクティビティ、およびユーザのワークフローだけでなく、ディスカバリ イベントの事前定義のワークフローが用意されています。ユーザはカスタム ワークフローを作成することもできます。ワークフローの詳細については、ワークフローの概要と使用 (58-1 ページ) を参照してください。

ヒント　[Analysis] > [Custom] > [Custom Tables] を選択して、カスタム テーブルに基づいたワークフローにアクセスします。

ネットワークのディスカバリ ワークフローを使用している場合は、イベントのタイプに関係なく、多数の一般的なアクションを実行できます。これらの一般的な機能については、一般的なディスカバリ イベントのアクションの表で説明します。

表 50-1　一般的なディスカバリ イベントのアクション

目的	操作
IP アドレスのホスト プロファイルを表示する	プロファイル アイコン( )をクリックするか、または侵害の痕跡(IOC)タグがアクティブになっているホストで、IP アドレスの隣に示されている侵害されているホストのアイコン( )をクリックします。IOC については、侵害の痕跡の使用(50-35 ページ)を参照してください。
ユーザ プロファイルの情報を表示する	ユーザ ID の隣に表示されているユーザ アイコン( )をクリックします。詳細については、ユーザの詳細とホストの履歴について(50-68 ページ)を参照してください。
データをソートする	カラム タイトルをクリックします。ソート順を反対にするには、カラムのタイトルをもう一度クリックします。
ワークフローの次のページにドリルダウンする	次のいずれかの方法を使用します。 • 特定の値に制約している次のワークフロー ページにドリルダウンするには、対象のロー内の値をクリックします。この操作はドリルダウン ページでのみ可能です。テーブルのロー内の値をクリックしても、テーブル ビューが制約されるだけで、次のページにはドリル ダウンしません。 • いくつかのイベントについて制約している次のワークフロー ページへドリルダウンするには、次のワークフロー ページで表示するイベントの隣にあるチェック ボックスをオンにして、[View] をクリックします。 • 現行の制約を保持したまま次のワークフロー ページへドリルダウンするには、[View All] をクリックします。 **ヒント**　テーブル ビューには必ず、ページ名に「Table View」が含まれます。 詳細については、イベントの制約(58-35 ページ)を参照してください。
表示するカラムを制約する	非表示にするカラムの見出しで、クローズ アイコン( )をクリックします。表示されるポップアップ ウィンドウで、[Apply] をクリックします。 **ヒント**　他のカラムを表示または非表示にするには、[Apply] をクリックする前に、対象のチェック ボックスをオンまたはオフにします。無効にしたカラムをビューに戻すには、展開の矢印をクリックして検索の制約を展開し、[Disabled Columns] の下のカラム名をクリックします。
現行のワークフロー ページ内で移動する	詳細については、ワークフロー内の他のページへのナビゲート(58-39 ページ)で確認できます。
現在の制約を保持したまま、現行のワークフローのページ間を移動する	ワークフロー ページの左上にある、対象のページ リンクをクリックします。詳細については、ワークフローのページの使用(58-21 ページ)を参照してください。

表 50-1　一般的なディスカバリ イベントのアクション（続き）

目的	操作
以下のアイテムをシステムから削除する • ディスカバリ イベント ワークフローからディスカバリ イベントおよびホスト入力イベントを削除する • ホスト ワークフローからホスト デバイスおよびネットワーク デバイスを削除する • ホスト属性のワークフローからホスト属性を削除する • サーバ ワークフローからサーバを削除する • アプリケーション ワークフローからアプリケーションを削除する • サードパーティ脆弱性ワークフローからサードパーティの脆弱性を削除する • ユーザ ワークフローからユーザを削除する	次のいずれかの方法を使用します。 • いくつかのアイテムを削除するには、削除するアイテムの隣にあるチェック ボックスをオンにして [Delete] をクリックします。 • 現行の制約されているビューのすべてのアイテムを削除するには、[Delete All] をクリックして、すべてのアイテムを削除することを確認します。 これらのアイテムが再検出されても、システムのディスカバリ機能が再開されるまで、これらのアイテムは削除されたままになります。 **ヒント**　データベースからすべてのディスカバリ イベントを削除する方法、およびディスカバリを再開する方法については、データベースからの検出データの消去（B-1 ページ）を参照してください。 サードパーティの場合とは異なり、Ciscoの脆弱性は削除**できない**ことに注意してください。ただし、確認済みとしてマークすることはできます。詳細については、脆弱性の処理（50-54 ページ）を参照してください。
他のイベント ビューに移動して、関連するイベントを表示する	詳細については、ワークフロー間のナビゲート（58-40 ページ）で確認できます。

ディスカバリ イベントとホスト入力イベントの使用

ライセンス： FireSIGHT

システムはディスカバリ イベントを生成します。このイベントは、監視対象ネットワーク セグメントにおける変更の詳細をやりとりします。新しく検出されたネットワーク機能に対しては、*新しい*イベントが生成され、以前に認識されたネットワーク資産における何らかの変更に対しては、変更のイベントが生成されます。

最初のネットワーク検出のフェーズ中に、システムは各ホスト、および各ホスト上での稼動が検出された TCP または UDP サーバについて、新しいイベントを生成します。必要に応じて、NetFlow 対応のデバイスでエクスポートされたデータを使用してこれらの新しいホストおよびサーバのイベントを生成するよう、システムを設定することができます。

またシステムは、検出された各ホスト上で稼動しているネットワーク、トランスポート、およびアプリケーション プロトコルのそれぞれに対して新しいイベントを生成します。NetFlow 対応のデバイスが含まれるように設定したディスカバリ ルールを作成する場合は、アプリケーション プロトコルの検出を無効にすることができます。ただし、設定された NetFlow 対応のデバイスを使用しないディスカバリ ルールでは、アプリケーションの検出を無効にすることはできません。NetFlow 以外のディスカバリ ルールでホストまたはユーザの検出を有効にすると、アプリケーションが自動的に検出されます。

最初のネットワーク マッピングが完了すると、続けてシステムは、変更イベントを生成し、ネットワークの変更を記録します。変更イベントは、以前に検出された資産の設定が変更されるたびに生成されます。

ディスカバリ イベントが生成されると、データベースに記録されます。Defense Centerの Web インターフェイスを使用して、ディスカバリ イベントを表示、検索、および削除することができます。また、相関ルールでディスカバリ イベントを使用することもできます。ユーザが指定する他の基準だけでなく、生成されるディスカバリ イベントのタイプに基づいて、相関ルールを作成することができます。相関ルールは相関ポリシーで使用され、ネットワーク トラフィックが基準を満たしたときに、修復、syslog、SNMP、および電子メール アラートの応答を起動します。

ホスト入力機能を使用して、ネットワーク マップにデータを追加することができます。オペレーティング システムの情報を追加、修正、または削除することができますが、この場合、システムは対象のホストに対する情報の更新を停止します。アプリケーション プロトコル、クライアント、サーバ、およびホストの属性を手動で追加、変更、または削除することも、脆弱性の情報を変更することもできます。この処理を行う場合、システムはホスト入力機能を生成します。

詳細については、次の項を参照してください。

- ディスカバリ イベントのタイプについて（50-10 ページ）
- ホスト入力イベントのタイプについて（50-14 ページ）
- ディスカバリ イベントおよびホスト入力イベントの表示（50-16 ページ）
- ディスカバリ イベント テーブルについて（50-17 ページ）
- ディスカバリ イベントの検索（50-18 ページ）

ディスカバリ イベントのタイプについて

ライセンス： FireSIGHT

ディスカバリ イベントには多数のタイプがあります。たとえば、監視対象ネットワーク セグメントで新しいホストが検出された場合、システムは New Host イベントを生成し、記録します。ディスカバリ イベントのテーブルを表示すると、[Event] カラムにイベント タイプが表示されます。詳細については、ディスカバリ イベントおよびホスト入力イベントの表示（50-16 ページ）を参照してください。

監視対象ネットワークでシステムが変更を検出した（以前に検出されなかったホストからトラフィックが検出されたなど）ときに生成されるディスカバリ イベントとは異なり、ホスト入力イベントは、ユーザが特別なアクションを実行した（手動でホストを追加するなど）ときに生成されます。ホスト入力イベントの詳細については、ホスト入力イベントのタイプについて（50-14 ページ）を参照してください。

ネットワーク検出ポリシーを変更して、システムが記録するディスカバリ イベントのタイプを設定できます。デフォルトでは、システムですべてのタイプのディスカバリ イベントが記録されます。詳細については、データベース イベント制限の設定（63-16 ページ）を参照してください。

さまざまなタイプのディスカバリ イベントが提示する情報を理解すると、どのイベントを記録およびアラートの対象にするか、相関ポリシーでこれらのアラートをどのように使用するかを効率よく判断できるようになります。また、イベント タイプの名前がわかると、より効率のよいイベント検索を作成するうえで役に立ちます。次に、ディスカバリ イベントのさまざまなタイプについて説明します。

Additional MAC Detected for Host

このイベントは、以前に検出したホストに対してシステムが新しい MAC アドレスを検出したときに生成されます。

このイベントは多くの場合、ルータを通じてトラフィックを渡すホストをシステムが検出したときに生成されます。それぞれのホストには 1 つの IP アドレスがありますが、これらの IP アドレスはすべて、ルータに関連付けられている MAC アドレスを持っているように見えま

す。システムは IP アドレスに関連付けられている実際の MAC アドレスを検出すると、ホスト プロファイル内でその MAC アドレスを太字で表示し、イベント ビューのイベント説明に「ARP/DHCP detected」のメッセージを表示します。

Client Timeout

このイベントは、非アクティブであるという理由で、システムがデータベースからクライアントをドロップしたときに生成されます。

Client Update

このイベントは、HTTP トラフィック内でシステムがペイロード（つまり音声やビデオ、Web メールなどの特別なタイプのコンテンツ）を検出したときに生成されます。

DHCP: IP Address Changed

このイベントは、DHCP アドレスの割り当てによってホスト IP アドレスが変わったことがシステムで検出された場合に生成されます。

DHCP: IP Address Reassigned

このイベントは、ホストが IP アドレスを再利用するとき、つまり他の物理ホストが以前に使用した IP アドレスを、別のホストが DHCP の IP アドレス割り当てによって取得した場合に生成されます。

Hops Change

このイベントは、ホストと、そのホストを検出するデバイス間でシステムがネットワーク ホップ数の変更を検出した場合に生成されます。

デバイスがさまざまなルータを介してホストのトラフィックを監視しており、ホストの場所についてより適切な決定ができる場合に、このような状況が発生することがあります。また、デバイスがホストから ARP 送信を検出し、ホストがローカル セグメント上にあることを示している場合に、このような状況が発生することもあります。

Host Deleted: Host Limit Reached

このイベントは、Defense Center上でホストの制限を超えて、Defense Centerのネットワーク マップから監視対象のホストが削除されたときに生成されます。

Host Dropped: Host Limit Reached

このイベントは、Defense Center上でホストの制限に達して新しいホストがドロップされたときに生成されます。このイベントとの相違点として、前述のイベントでは、ホストの制限に達したときに古いホストがネットワーク マップから削除されます。

ホストの制限に達したときに新しいホストをドロップするには、[Policies] > [Network Discovery] > [Advanced] を選択し、[When Host Limit Reached] を [Drop hosts] に設定します。詳細については、「データ保存の設定（45-39 ページ）」を参照してください。

Host IOC Set

このイベントは、ホストに対して IOC（侵害の痕跡）が設定され、アラートが生成されたときに生成されます。

Host Timeout

このイベントは、ネットワーク検出ポリシーで定義された間隔内でホストがトラフィックを生成しなかったために、ネットワーク マップからホストがドロップされたときに生成されます。個々のホストの IP アドレスと MAC アドレスはそれぞれタイムアウトになることに注

意してください。関連付けられているアドレスがすべてタイムアウトになるまで、ホストはネットワーク マップから消えません。ホストのタイムアウト値の設定については、データ保存の設定（45-39 ページ）を参照してください。

ネットワーク検出ポリシーで監視するネットワークを変更する場合は、ネットワーク マップから古いホストを手動で削除して、それらのホストがFireSIGHT のライセンスに不利に作用しないようにします。詳細については、ホストのネットワーク マップの使用（48-2 ページ）を参照してください。

Host Type Changed to Network Device

このイベントは、システムが、検出されたホストが実際はネットワーク デバイスであったことを認識したときに生成されます。

Identity Conflict

このイベントは、システムが、新しいサーバまたはオペレーティング システムに対する現行のアクティブなアイデンティティと競合する、そのサーバまたはオペレーティング システムのアイデンティティを検出したときに生成されます。

より新しいアクティブなアイデンティティ データを取得するためにホストを再スキャンして、アイデンティティの競合を解決する場合は、Identity Conflict イベントを使用して Nmap の修復をトリガーできます。詳細については、Nmap 修復の設定（54-12 ページ）を参照してください。

詳細については、ID の競合について（46-7 ページ）およびID 競合解決の設定（45-35 ページ）を参照してください。手動による競合の解決については、オペレーティング システムのアイデンティティの競合を解決する（49-15 ページ）およびサーバ アイデンティティの競合の解決（49-21 ページ）を参照してください。

Identity Timeout

このイベントは、アクティブなソースを介してネットワーク マップに追加されたアイデンティティ データがタイムアウトになったときに生成されます。

より新しいアクティブなアイデンティティ データを取得するために、ホストを再スキャンしてアイデンティティ データをリフレッシュする場合は、Identity Conflict イベントを使用して Nmap の修復をトリガーできます。詳細については、Nmap 修復の設定（54-12 ページ）を参照してください。

詳細については、サーバ アイデンティティの競合の解決（49-21 ページ）を参照してください。

MAC Information Change

このイベントは、特定の MAC アドレスまたは TTL 値に関連付けられている情報で、システムが変更を検出したときに生成されます。

このイベントは多くの場合、ルータを通じてトラフィックを渡すホストをシステムが検出したときに発生します。それぞれのホストには 1 つの IP アドレスがありますが、これらの IP アドレスはすべて、ルータに関連付けられている MAC アドレスを持っているように見えます。システムは IP アドレスに関連付けられている実際の MAC アドレスを検出すると、ホスト プロファイル内でその MAC アドレスを太字で表示し、イベント ビューのイベント説明に「ARP/DHCP detected」のメッセージを表示します。TTL は変わる可能性がありますが、これはトラフィックが複数のルータを通じて渡される可能性があるためです。また、システムがホストの実際の MAC アドレスを検出した場合も TTL が変わる可能性があります。

NETBIOS Name Change

このイベントは、システムがホストの NetBIOS 名に対する変更を検出したときに生成されます。このイベントは、NetBIOS プロトコルを使用するホストに対してのみ生成されます。

New Client

このイベントは、システムが新しいクライアントを検出したときに生成されます。

注 分析用にクライアント データを収集および格納するには、ネットワーク検出ポリシーのディスカバリ ルールでアプリケーションの検出が有効になっていることを確認します。詳細については、アプリケーション検出について（45-11 ページ）を参照してください。

New Host

このイベントは、システムがネットワーク上で稼動している新しいホストを検出したときに生成されます。

NetFlow デバイスが選択されているネットワーク検出 ルールで [Discover] オプションを選択して [Hosts] を選択した場合、新しいホストに関係する NetFlow データをデバイスが処理したときにも、このイベントが生成されます。

New Network Protocol

このイベントは、ホストが新しいネットワーク プロトコル（IP、ARP など）と通信していることをシステムが検出したときに生成されます。

New OS

このイベントは、システムがホストの新しいオペレーティング システムを検出した、またはホストのオペレーティング システムで変更を検出したときに生成されます。

New TCP Port

このイベントは、新しい TCP サーバ ポート（SMTP または Web サービスで使用されているポートなど）をシステムが検出したときに生成されます。このイベントは、アプリケーション プロトコル、またはアプリケーション プロトコルに関連付けられているサーバの識別には使用されないことに注意してください。情報は、TCP Server Information Update イベントで伝送されます。

NetFlow データについて、ネットワーク検出 ルールで [Discover] オプションを選択して [Applications] を選択した場合、監視対象ネットワーク上のサーバに関連する NetFlow データで、ネットワーク マップにまだ存在しないデータをデバイスが処理したときにも、このイベントが生成されます。

New Transport Protocol

このイベントは、ホストが新しいトランスポート プロトコル（TCP、UDP など）と通信していることをシステムが検出したときに生成されます。

New UDP Port

このイベントは、システムが、ホスト上で稼動している新しい UDP サーバ ポートを検出したときに生成されます。

NetFlow データについて、ネットワーク検出 ルールで [Discover] オプションを選択して [Applications] を選択した場合、監視対象ネットワーク上のサーバに関連する NetFlow データで、ネットワーク マップにまだ存在しないデータをデバイスが処理したときにも、このイベントが生成されます。

TCP Port Closed

このイベントは、システムが、ホスト上で TCP ポートがクローズしたことを検出したときに生成されます。

TCP Port Timeout

このイベントは、システムのネットワーク検出ポリシーに定義された間隔内で、システムが TCP ポートからアクティビティを検出しなかったときに生成されます。サーバのタイムアウト値の設定については、データ保存の設定（45-39 ページ）を参照してください。

TCP Server Information Update

このイベントは、ホスト上で稼動しており、すでに検出されている TCP サーバでシステムが変更を検出したときに生成されます。

このイベントは、TCP サーバが更新されたときに生成される場合があります。

UDP Port Closed

このイベントは、システムが、ホスト上で UDP ポートがクローズしていることを検出したときに生成されます。

UDP Port Timeout

このイベントは、ネットワーク検出ポリシーに定義された間隔内で、システムが UDP ポートからアクティビティを検出しなかったときに生成されます。サーバのタイムアウト値の設定については、データ保存の設定（45-39 ページ）を参照してください。

UDP Server Information Update

このイベントは、ホスト上で稼動しており、すでに検出されている UDP サーバで、システムが変更を検出したときに生成されます。

このイベントは、UDP サーバが更新されたときに生成される場合があります。

VLAN Tag Information Update

このイベントは、システムが、VLAN タグ内でホストに起因する変更を検出したときに生成されます。VLAN タグの詳細については、ホスト プロファイルでの VLAN タグの使用（49-24 ページ）を参照してください。

ホスト入力イベントのタイプについて

ライセンス：FireSIGHT

ホスト入力イベントには多数のタイプがあります。たとえば、ユーザがホスト インポート機能を使用してホストを追加すると、システムは Add Host イベントを生成および記録します。ディスカバリ イベントのテーブルを表示すると、[Event] カラムにイベント タイプが表示されます。詳細については、ディスカバリ イベントおよびホスト入力イベントの表示（50-16 ページ）を参照してください。

ユーザが（手動でホストを追加するなどの）特定のアクションを実行したときに生成されるホスト入力イベントとは異なり、ディスカバリ イベントは、システムが、監視対象ネットワークで変更を検出したとき（以前は検出されなかったホストでトラフィックを検出した場合など）に生成されます。ホスト入力イベントの詳細については、ディスカバリ イベントのタイプについて（50-10 ページ）を参照してください。

ネットワーク検出ポリシーを変更して、システムが記録するホスト入力イベントのタイプを設定できます。デフォルトでは、システムですべてのタイプのホスト入力イベントが記録されます。詳細については、データベース イベント制限の設定（63-16 ページ）を参照してください。

さまざまなタイプのホスト入力イベントが提示する情報を理解すると、どのイベントを記録およびアラートの対象にするか、相関ポリシーでこれらのアラートをどのように使用するかを効率よく判断できるようになります。また、イベント タイプの名前がわかると、より効率のよいイベント検索を作成するうえで役に立ちます。次に、ホスト入力イベントのさまざまなタイプについて説明します。

Add Client

このイベントは、ユーザがクライアントを追加したときに生成されます。

Add Host

このイベントは、ユーザがホストを追加したときに生成されます。

Add Protocol

このイベントは、ユーザがプロトコルを追加したときに生成されます。

Add Scan Result

このイベントは、システムが Nmap スキャンの結果をホストに追加したときに生成されます。

Add Port

このイベントは、ユーザがサーバ ポートを追加したときに生成されます。

Delete Client

このイベントは、ユーザがシステムからクライアントを削除したときに生成されます。

Delete Host/Network

このイベントは、ユーザがシステムから IP アドレスまたはサブネットを削除したときに生成されます。

Delete Protocol

このイベントは、ユーザがシステムからプロトコルを削除したときに生成されます。

Delete Port

このイベントは、ユーザがシステムからサーバ ポートまたはサーバ ポートのグループを削除したときに生成されます。

Host Attribute Add

このイベントは、ユーザが新しいホスト属性を作成したときに生成されます。

Host Attribute Delete

このイベントは、ユーザが、ユーザ定義のホスト属性を削除したときに生成されます。

Host Attribute Delete Value

このイベントは、ユーザが、ホスト属性に割り当てられている値を削除したときに生成されます。

Host Attribute Set Value

このイベントは、ユーザがホストに対してホスト属性値を設定したときに生成されます。

Host Attribute Update

このイベントは、ユーザが、ユーザ定義のホスト属性の定義を変更したときに生成されます。

Set Host Criticality

このイベントは、ユーザがホストに対してホストの重要度の値を設定した、または変更したときに生成されます。

Set Operating System Definition

このイベントは、ユーザがホストに対してオペレーティング システムを設定したときに生成されます。

Set Server Definition

このイベントは、ユーザがサーバに対してベンダーおよびバージョンの定義を設定したときに生成されます。

Set Vulnerability Impact Qualification

このイベントは、脆弱性の影響の認定が設定されたときに生成されます。

脆弱性が、影響の認定に対する使用でグローバル レベルで無効になったとき、または脆弱性がグローバル レベルで有効になったときに、このイベントが生成されます。

Vulnerability Set Invalid

このイベントは、ユーザが 1 つ以上の脆弱性を無効にした（または確認した）ときに生成されます。

Vulnerability Set Valid

このイベントは、ユーザが、以前に無効であるとマークされた脆弱性を有効にしたときに生成されます。

ディスカバリ イベントおよびホスト入力イベントの表示

ライセンス： FireSIGHT

ディスカバリ イベントとホスト入力イベントは、[Discovery Events（ディスカバリ イベント）] ワークフローを使用して表示できます。ディスカバリ イベントは、アプライアンスに対して設定されているネットワーク検出ポリシーに基づいてネットワーク検出 データの検出を記録します。ホスト入力イベントは、ホスト入力機能を介してホスト データの入力をネットワーク マップへ記録します。詳細については、ディスカバリ イベントのタイプについて（50-10 ページ）およびホスト入力イベントのタイプについて（50-14 ページ）を参照してください。

Defense Centerを使用して、ディスカバリ イベントまたはホスト入力イベントのテーブルを表示することができます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

ユーザがイベントにアクセスするときに表示されるページは、使用するワークフローによって異なります。ユーザは事前定義のワークフローを使用できますが、これにはディスカバリ イベントのテーブル ビューと、ホスト ビューの最終ページが含まれています。また、特定のニーズにあった情報のみを表示するカスタム ワークフローを作成することもできます。カスタム ワークフローの作成の詳細については、カスタム ワークフローの作成（58-43 ページ）を参照してください。

ディスカバリ イベントのアクションの表で、ディスカバリ イベントのワークフロー ページで実行できる特定の操作について説明します。一般的なディスカバリ イベントのアクションの表に記載されているタスクも実行できます。

表 50-2　ディスカバリ イベントのアクション

目的	操作
表示されたイベントの時間と日付の範囲を変更する	詳細については、イベント時間の制約の設定（58-26 ページ）を参照してください。 イベント ビューを時間によって制約している場合は、（グローバルかイベントに特有かに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあることに注意してください。これは、アプライアンスに対してスライディングの時間枠を設定した場合でも発生することがあります。
テーブルのカラムの内容について詳細を参照する	詳細については、ディスカバリ イベント テーブルについて（50-17 ページ）で確認できます。

ディスカバリ イベントを表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Hosts] > [Discovery Events] を選択します。

デフォルトのディスカバリ イベント ワークフローの最初のページが表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。イベントが表示されない場合は、時間範囲の調整が必要なことがあります。イベント時間の制約の設定（58-26 ページ）を参照してください。

ディスカバリ イベント テーブルについて

ライセンス：FireSIGHT

システムはディスカバリ イベントを生成します。このイベントは、監視対象ネットワーク セグメントにおける変更の詳細をやりとりします。新しく検出されたネットワーク機能に対しては、*新しい*イベントが生成され、以前に認識されたネットワーク資産における何らかの変更に対しては、変更のイベントが生成されます。

最初のネットワーク検出のフェーズ中に、システムは各ホスト、および各ホストで検出する TCP または UDP サーバについて新しいイベントを生成します。またシステムは、検出された各ホスト上で稼動しているネットワーク、トランスポート、およびアプリケーション プロトコルのそれぞれに対して新しいイベントを生成します。NetFlow 関連のトラフィックについては、ホストで稼動しているアプリケーション プロトコルをシステムが検出したときに、システムが新しいイベントを作成するかどうかを制御できます。最初のネットワーク マッピングが完了すると、続けてシステムは、変更イベントを生成し、ネットワークの変更を記録します。以前に検出されたホスト、サーバ、またはクライアントの設定が変更されるたびに、変更イベントが生成されます。

次に、ディスカバリ イベント テーブルのフィールドについて説明します。

時刻

システムがイベントを生成した時間。

Event

イベントのタイプ。使用可能な各イベントの説明については、ディスカバリ イベントのタイプについて（50-10 ページ）およびホスト入力イベントのタイプについて（50-14 ページ）を参照してください。

IP Address

イベントに関連するホストに関連付けられている IP アドレス。

User

イベントが生成される前に、イベントに関係するホストに最後にログインしたユーザ。権限のあるユーザの後に、権限のないユーザのみがログインした場合、権限のあるユーザが次にログインするまで、権限のあるユーザが現行のユーザとして保持されます。

MAC アドレス

ディスカバリ イベントをトリガーとして使用したネットワーク トラフィックが使用する NIC の MAC アドレス。この MAC アドレスは、イベントに関連するホストの実際の MAC アドレスであるか、またはトラフィックが通過したネットワーク デバイスの MAC アドレスになります。

MAC Vendor

ディスカバリ イベントをトリガーとして使用したネットワーク トラフィックが使用する NIC の MAC ハードウェア ベンダー。

ポート

イベントをトリガーとして使用したトラフィックが使用するポート（該当する場合）。

説明

テキストによるイベントの説明。

デバイス

イベントを生成したデバイス名。NetFlow データに基づいた新しいホストおよび新しいサーバ イベントの場合、これは NetFlow データを処理したデバイスになります。

ディスカバリ イベントの検索

ライセンス： FireSIGHT

ユーザは特定のディスカバリ イベントを検索することができます。ネットワーク環境に合わせてカスタマイズした検索を作成し、後で再使用するために保存することもできます。

一般的な検索の構文

それぞれの検索フィールドの隣には、使用できる構文の例が表示されます。検索条件を入力する場合、次の点に注意してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。

  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「`A`」または「`B`」または「`C, D, E`」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク(*)を使用できます。
- いくつかのフィールドでは、フィールドに `n/a` または `blank` を指定して、そのフィールドで情報を使用できないイベントを特定することができます。`!n/a` または `!blank` を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。
- 特定のデバイス、およびグループ、スタック、またはクラスタ内のデバイスを検索するには、デバイス フィールドを使用します。検索での FireSIGHT システムによるデバイス フィールドの処理方法については、検索でのデバイスの指定(60-7 ページ)を参照してください。
- オブジェクトを検索条件として使用するには、検索フィールドの隣にあるオブジェクトの追加アイコン(+)をクリックします。

検索でのオブジェクトの使用など、検索構文の詳細については、イベントの検索(60-1 ページ)を参照してください。

ディスカバリ イベントの特別な検索構文

次の表に、特定のディスカバリ イベント フィールドに固有の検索情報について示します。ディスカバリ イベントのフィールドの詳細は、ホスト テーブルについて(50-22 ページ)を参照してください。

表 50-3　ディスカバリ イベントの検索条件のメモ

フィールド	検索条件のメモ
Event	イベント名の対象は、ディスカバリ イベントのタイプについて(50-10 ページ)およびホスト入力イベントのタイプについて(50-14 ページ)に記載されています。
MAC Vendor	仮想 MAC ベンダー(つまり、仮想マシンが含まれているイベント)を検索するには、`virtual_mac_vendor` と入力します。 名前にカンマが含まれているベンダーを検索するには、検索語全体を引用符で囲みます。このようにしないと、Defense Centerは検索語を 2 つの検索として扱い、それぞれの検索語に一致するイベントを返します。

表 50-3　ディスカバリ イベントの検索条件のメモ（続き）

フィールド	検索条件のメモ
ポート	注意すべき点として、次の処理は行うことはできません。 • 他の種類のイベントを検索するときと同じように、ポート/プロトコルの組み合わせを入力する • ポート番号または範囲を指定するときにスペースを使用する

ディスカバリ イベントを検索するには、以下を行います。

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　テーブルのドロップダウン リストから [Discovery Events] を選択します。

ページが適切な制約によって更新されます。

ステップ 3　一般的な検索の構文（50-18 ページ）およびディスカバリ イベントの特別な検索構文（50-19 ページ）に記載されているように、該当するフィールドに検索条件を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。オブジェクトを検索条件として使用するには、検索フィールドの隣にある追加アイコン（ ＋ ）をクリックします。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　検索をカスタム ユーザ ロールのデータ制限として使用する場合は、**必ず**プライベート検索として保存してください。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save As New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

検索結果は、現行の時間範囲によって制約され、デフォルトのディスカバリ イベント ワークフローに表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

ホストの使用

ライセンス：FireSIGHT

システムがホストを検出し、ホスト プロファイルを作成するためにホストに関する情報を収集したときに、イベントが生成されます。Defense Center Web インターフェイスを使用して、ホストを表示、検索、および削除できます。

ホストの表示中に、選択したホストに基づいてトラフィックのプロファイル、およびコンプライアンスのホワイト リストを作成できます。また、(ビジネスの重要度を設定する)ホストの重要度の値などのホスト属性をホスト グループに割り当てることもできます。そのあとで、相関ルールおよびポリシーの中でこれらの重要度の値、ホワイト リスト、およびトラフィック プロファイルを使用できます。

NetFlow 対応デバイスによってエクスポートされたデータに基づきネットワーク マップにホストを追加するようネットワーク検出ポリシーを設定することはできますが、これらのホストに関して使用可能な情報は限られています。たとえば、これらのホストのオペレーティング システム データは得られません(ただしホスト入力機能を使って指定する場合を除く)。詳細については、NetFlow と FireSIGHT データの違い(45-19 ページ)を参照してください。

詳細については、次の項を参照してください。

- ホストの表示(50-21 ページ)
- ホスト テーブルについて(50-22 ページ)
- 選択したホストのトラフィック プロファイルの作成(50-26 ページ)
- 選択したホストに基づいたコンプライアンスのホワイト リストの作成(50-26 ページ)
- ホストの検索(50-27 ページ)
- 選択したホストのホスト属性の設定(50-32 ページ)

ホストの表示

ライセンス：FireSIGHT

Defense Centerを使用して、システムが検出したホストのテーブルを表示することができます。ここでユーザは、検索する情報に応じてビューを操作できます。

ユーザがホストにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローは両方とも、ホスト ビューで終了しますが、これにはユーザの制約を満たすすべてのホストのホスト プロファイルが含まれています。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。詳細については、カスタム ワークフローの作成(58-43 ページ)を参照してください。

ホスト アクションの表で、ホストのワークフロー ページで実行できる特定の操作について説明します。一般的なディスカバリ イベントのアクションの表に記載されているタスクも実行できます。

表 50-4　ホスト アクション

目的	操作
テーブルのカラムの内容について詳細を参照する	詳細については、ホスト テーブルについて(50-22 ページ)で確認できます。
選択したホストにホスト属性を割り当てる	詳細については、選択したホストのホスト属性の設定(50-32 ページ)で確認できます。

表 50-4　ホスト アクション（続き）

目的	操作
選択したホストのトラフィック プロファイルを作成する	詳細については、選択したホストのトラフィック プロファイルの作成（50-26 ページ）で確認できます。
選択したホストに基づいて、コンプライアンスのホワイト リストを作成する	詳細については、選択したホストに基づいたコンプライアンスのホワイト リストの作成（50-26 ページ）で確認できます。

ホストを表示するには、以下を行います。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Hosts] > [Hosts] を選択します。

デフォルトのホスト ワークフローの最初のページが表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

ヒント　ホストのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(switch workflow)] をクリックして [Hosts] を選択します。

ホスト テーブルについて

ライセンス： FireSIGHT

システムはホストを検出したときに、そのホストに関するデータを収集します。そのデータには、ホストの IP アドレス、ホストが実行しているオペレーティング システムなどが含めることが可能です。ユーザは、ホストのテーブル ビューでこれらの情報の一部を表示することができます。システムが、検出したホストに関して収集するデータの詳細は、ホスト プロファイルの使用（49-1 ページ）を参照してください。

次に、ホスト テーブルのフィールドについて説明します。

NetFlow 対応デバイスによってエクスポートされたデータに基づきネットワーク マップにホストを追加するようネットワーク検出ポリシーを設定することはできますが、これらのホストに関して使用可能な情報は限られています。たとえば、これらのホストのオペレーティング システム データは得られません（ただしホスト入力機能を使って指定する場合を除く）。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

Last Seen

システムによっていずれかのホストの IP アドレスが最後に検出された日付と時間。Last Seen の値は、ホストの IP アドレスに対してシステムが新しいホスト イベントを生成したときだけでなく、少なくともユーザがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。

ホスト入力機能を使用して、オペレーティング システムのデータを更新しているホストでは、Last Seen の値は、そのデータが最初に追加された日付と時間を表します。

IP アドレス

ホストに関連付けられている IP アドレス。

MAC アドレス

ホストが検出した NIC の MAC アドレス。

[MAC Address] フィールドは、[Hosts] ワークフローの [Table View of Hosts] に表示されます。以下のものに対して [MAC Address] フィールドを追加できます。

- Hosts テーブルのフィールドが含まれているカスタム テーブル
- [Hosts] テーブルに基づいたカスタム ワークフローのドリルダウン ページ

MAC Vendor

ホストが検出した NIC の MAC ハードウェア ベンダー。

[MAC Vendor] フィールドは、[Hosts] ワークフローの [Table View of Hosts] に表示されます。以下のものに対して [MAC Vendor] フィールドを追加できます。

- Hosts テーブルのフィールドが含まれているカスタム テーブル
- [Hosts] テーブルに基づいたカスタム ワークフローのドリルダウン ページ

Current User

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることが可能です。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

Host Criticality

ホストに割り当てられている、ユーザ指定の重要度の値。このフィールドの詳細については、ホスト属性のテーブルについて（50-31 ページ）の [Host Criticality] カラムの説明を参照してください。

NetBIOS Name

ホストの NetBIOS 名。NetBIOS プロトコルを実行しているホストにのみ、NetBIOS 名があります。

VLAN ID

ホストが使用する VLAN ID。VLAN ID の詳細については、ホスト プロファイルでの VLAN タグの使用（49-24 ページ）を参照してください。

Hops

ホストを検出したデバイスからホストへのネットワークのホップ数。

Host Type

ホストのタイプ（ホスト、モバイル デバイス、jailbroken モバイル デバイス、ルータ、ブリッジ、NAT デバイス、またはロード バランサ）。ネットワーク デバイスを区別するためにシステムでは次の方法を使用します。

– Cisco Discovery Protocol（CDP）メッセージの分析。ネットワークのデバイスおよびそれらのタイプ（Cisco デバイスのみ）を特定できます。
– スパニング ツリー プロトコル（STP）の検出。デバイスをスイッチまたはブリッジとして識別します。
– 同じ MAC アドレスを使用している複数のホストの検出。MAC アドレスを、ルータに属しているものとして識別します。
– クライアント側からの TTL 値の変更、または通常のブート時間よりも頻繁に変更されている TTL 値の検出。この検出では、NAT デバイスとロード バランサを識別します。

デバイスがネットワーク デバイスとして識別されない場合は、ホストとして分類されます。

ハードウェア

モバイル デバイスのハードウェア プラットフォーム。

OS

ホスト上で稼動中の、検出されたオペレーティング システム（名前、ベンダー、およびバージョン）、または Nmap かホスト入力機能を使用して更新されたオペレーティング システム。このフィールドは、ダッシュボード上で [Custom Analysis] ウィジェットからホスト イベント ビューを起動したときに表示されます。また、これは [Hosts] テーブルに基づいたカスタム テーブルのフィールド オプションです。

システムが複数のアイデンティティを検出した場合は、これらのアイデンティティはカンマ区切りで列挙されて表示されます。

このフィールドでは、`unknown` の値は、オペレーティング システムが既知のフィンガープリントのいずれにも一致しないことを意味します。値が `pending` の場合は、オペレーティング システムを識別するための十分な情報がシステムで収集されていないことを意味します。

OS Vendor

ホストで検出されたオペレーティング システムのベンダー、または Nmap かホスト入力機能を使用して更新されたオペレーティング システムのベンダー。

システムが複数のベンダーを検出した場合は、これらのベンダーはカンマ区切りで列挙されて表示されます。

このフィールドでは、`unknown` の値は、オペレーティング システムが既知のフィンガープリントのいずれにも一致しないことを意味します。値が `pending` の場合は、オペレーティング システムを識別するための十分な情報がシステムで収集されていないことを意味します。

OS Name

ホスト上で稼動中の、検出されたオペレーティング システム、または Nmap かホスト入力機能を使用して更新されたオペレーティング システム。

システムが複数の名前を検出した場合は、これらの名前はカンマ区切りで列挙されて表示されます。

このフィールドでは、`unknown` の値は、オペレーティング システムが既知のフィンガープリントのいずれにも一致しないことを意味します。値が `pending` の場合は、オペレーティング システムを識別するための十分な情報がシステムで収集されていないことを意味します。

OS Version

ホストで検出されたオペレーティング システムのバージョン、または Nmap かホスト入力機能を使用して更新されたオペレーティング システムのバージョン。

システムが複数のバージョンを検出した場合は、これらのバージョンはカンマ区切りで列挙されて表示されます。

このフィールドでは、unknown の値は、オペレーティング システムが既知のフィンガープリントのいずれにも一致しないことを意味します。値が pending の場合は、オペレーティング システムを識別するための十分な情報がシステムで収集されていないことを意味します。

Source Type

ホストのオペレーティング システムのアイデンティティ ソースに対する次のいずれかの値

- User: *user_name*
- Application: *app_name*
- Scanner: *scanner_type*（ネットワーク検出の設定を介して追加された Nmap またはスキャナ）
- FireSIGHT（システムによって検出されたオペレーティング システムの場合）

システムでは、オペレーティング システムのアイデンティティを判断するために、複数のソースのデータを統合することができます。現在の ID について（46-5 ページ）を参照してください。

Confidence

次のいずれかになります。

- システムで検出されたホストについて、ホスト上で稼動しているオペレーティング システムのアイデンティティ内にシステムが保持している信頼度（パーセンテージ）。
- 100%（ホスト入力機能や Nmap スキャナなどのアクティブなソースによって識別されたオペレーティング システムの場合）。
- unknown（システムがオペレーティング システムのアイデンティティを特定できないホスト、および NetFlow データに基づいてネットワーク マップに追加されたホストの場合）。

注意

Notes ホスト属性の、ユーザ定義のコンテンツ。

デバイス

トラフィックを検出した管理対象デバイス、またはネットワーク マップへホストを追加した NetFlow またはホスト入力データを処理したデバイス。

このフィールドが空白の場合、ホストが存在しているネットワークをネットワーク検出ポリシーの定義どおりに、明示的にモニタリングしていないデバイスによってホストがネットワーク マップに追加されたか、ホスト入力機能を使用してホストが追加され、システムでまだ検出されていません。

Count

各行に表示された情報と一致するイベントの数。[Count] フィールドは、2 つ以上の同じローを作成する制約を適用した場合のみ表示されることに注意してください。

選択したホストのトラフィック プロファイルの作成

ライセンス：FireSIGHT

トラフィック プロファイルは、指定した期間に収集された接続データに基づいた、ネットワーク上のトラフィックのプロファイルです。トラフィック プロファイルを作成した後で、正常なネットワーク トラフィックを表すと思われる新しいトラフィックをプロファイルに対して評価することにより、異常なネットワーク トラフィックを検出することができます。

[Hosts] ページを使用して、指定するホスト グループのトラフィック プロファイルを作成できます。トラフィック プロファイルは、指定したホストのいずれかが発信元ホストである、検出された接続に基づいています。ソートおよび検索機能を使用して、プロファイルを作成するホストを分離することができます。

選択したホストのトラフィック プロファイルを作成するには、以下を行います。

アクセス：Admin

ステップ 1　ホスト ワークフローのテーブル ビューで、トラフィック プロファイルを作成するホストの隣にあるチェック ボックスをオンにします。

ステップ 2　ページの下部で [Create Traffic Profile] をクリックします。

[Create Profile] ページが表示され、監視対象のホストとして指定されたホストの IP アドレスが示されます。

ステップ 3　特別なニーズに応じて、トラフィック プロファイルを変更し、保存します。

トラフィック プロファイルの作成の詳細については、トラフィック プロファイルの作成（53-1 ページ）を参照してください。

選択したホストに基づいたコンプライアンスのホワイト リストの作成

ライセンス：FireSIGHT

コンプライアンスのホワイト リストでは、ネットワーク上で許可されるオペレーティング システム、クライアント、ネットワーク、トランスポート、またはアプリケーション プロトコルを指定することができます。

[Hosts] ページを使用して、ユーザが指定するホスト グループのホスト プロファイルに基づいて、コンプライアンスのホワイト リストを作成することができます。ソートおよび検索機能を使用して、ホワイト リストの作成に使用するホストを分離することができます。

選択したホストに基づいてコンプライアンスのホワイト リストを作成するには、以下を行います。

アクセス：Admin

ステップ 1　ホスト ワークフローのテーブル ビューで、ホワイト リストを作成するホストの隣にあるチェック ボックスをオンにします。

ステップ 2　ページの下部で [Create White List] をクリックします。

[Create White List] ページが表示され、指定したホストのホスト プロファイルの情報が示されます。

ステップ 3　特別なニーズに応じて、ホワイト リストを変更し、保存します。

コンプライアンスのホワイト リストの作成の詳細は、コンプライアンス ホワイト リストの作成 (52-9 ページ)を参照してください。

ホストの検索

ライセンス：FireSIGHT

事前定義のいずれかの検索、または独自の検索条件を使用して、特定のホストについて検索することができます。

ホストを検索する場合には、NetFlow 対応のデバイスによってエクスポートされたデータに基づいてネットワーク マップにホストを追加するように、ネットワーク検出ポリシーを設定できますが、これらのホストについて利用できる情報は制限されることに注意してください。たとえば、これらのホストのオペレーティング システム データは得られません（ただしホスト入力機能を使って指定する場合を除く）。詳細については、NetFlow と FireSIGHT データの違い (45-19 ページ)を参照してください。

ユーザは特定のディスカバリ イベントを検索することができます。ネットワーク環境に合わせてカスタマイズした検索を作成し、後で再使用するために保存することもできます。

一般的な検索の構文

それぞれの検索フィールドの隣には、使用できる構文の例が表示されます。検索条件を入力する場合、次の点に注意してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「A」または「B」または「C, D, E」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク（*）を使用できます。
- いくつかのフィールドでは、フィールドに `n/a` または `blank` を指定して、そのフィールドで情報を使用できないイベントを特定することができます。`!n/a` または `!blank` を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。

- IP アドレスは CIDR 表記を使用して指定できます。FireSIGHT システムへの IP アドレスの入力については、IP アドレスの表記規則（1-23 ページ）を参照してください。

注 IP アドレスを使用してホストを検索した場合、結果には、少なくとも 1 つの IP アドレスが検索条件と一致するホストがすべて含まれます（つまり、IPv6 のアドレスの検索では、プライマリ アドレスが IPv4 であるホストが返されることがあります）。

- 特定のデバイス、およびグループ、スタック、またはクラスタ内のデバイスを検索するには、デバイス フィールドを使用します。検索での FireSIGHT システムによるデバイス フィールドの処理方法については、検索でのデバイスの指定（60-7 ページ）を参照してください。
- 検索条件としてオブジェクトを使用するには、検索フィールドの横に表示されるオブジェクトの追加アイコン (+) をクリックします。

検索でのオブジェクトの使用など、検索構文の詳細については、イベントの検索（60-1 ページ）を参照してください。

ホストの特別な検索構文

次の表に、特定のホスト フィールドに固有の検索情報について示します。ホストのフィールドに関する詳細は、ホスト テーブルについて（50-22 ページ）を参照してください。

表 50-5　ホストの検索条件

フィールド	検索条件のメモ
Host Type	すべてのネットワーク デバイスを検索するには、`!host` と入力します。
MAC Vendor	仮想 MAC ベンダー（つまり、仮想マシンが含まれているイベント）を検索するには、`virtual_mac_vendor` と入力します。 名前にカンマが含まれているベンダーを検索するには、検索語全体を引用符で囲みます。このようにしないと、Defense Centerは検索語を 2 つの検索として扱い、それぞれの検索語に一致するイベントを返します。
OS Vendor/Name/Version	オペレーティング システムが不明であるホストを検索するには、`unknown` と入力します。オペレーティング システムがまだ識別されていないホストを検索するには、`n/a` と入力します。
Confidence	信頼度の前に、より大きい（`>`）、以上（`>=`）、より小さい（`<`）、以下（`<=`）、等しい（`=`）の演算子を付けることができます。 `n/a` の検索で一致するものには、NetFlow データに基づいてネットワーク マップに追加されたホストも含まれます。
OS Conflict	検索結果には、[OS Conflict] カラムは表示されないことに注意してください。表示しているホストにオペレーティング システムの競合が発生しているかどうかを判断するには、ワークフロー ページで検索の制約を展開します。オペレーティング システムにおける競合の解決の詳細については、オペレーティング システムのアイデンティティの競合を解決する（49-15 ページ）を参照してください。

保存された検索のロードおよび削除方法など、検索の詳細については、イベントの検索（60-1 ページ）を参照してください。

ホストを検索するには、以下を行います。

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　テーブルのドロップダウン メニューから [Hosts] を選択します。

ページが適切な制約によって更新されます。

ヒント　データベース内で別の種類のイベントを検索するには、テーブルのドロップダウン リストから選択します。

ステップ 3　表ホストの検索条件に記載されているように、該当するフィールドに検索基準を入力します。

複数のフィールドに条件を入力すると、Defense Centerはすべてのフィールドに対して指定された検索条件に一致するレコードのみを返します。オブジェクトを検索条件として使用するには、検索フィールドの隣にある追加アイコン（ ＋ ）をクリックします。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　制約された権限を持つカスタム ユーザ ロールの制約として検索を保存する場合は、検索を非公開として保存する**必要があります**。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save As New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

検索結果は、デフォルトのホスト ワークフローに表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

ホスト属性の使用

ライセンス：FireSIGHT

FireSIGHT システムは、検出したホストに関する情報を収集し、その情報を使用してホスト プロファイルを作成します。ただし、ネットワーク上のホストについて、アナリストに提供する追加情報が存在する場合があります。ユーザは、ホスト プロファイルにメモを追加する、ホストのビジネス重要度を設定する、選択する他の情報を提供する、といったことが可能です。それぞれの情報は、ホスト属性と呼ばれます。

ホスト プロファイルの認定でホスト属性を使用することができます。これにより、トラフィック プロファイルの作成中に収集するデータを制約し、相関ルールをトリガーする条件を制限することができます。相関ルールに応じて属性値を設定することもできます。

詳細については、以下を参照してください。

- ホスト属性の表示（50-30 ページ）
- ホスト属性のテーブルについて（50-31 ページ）
- 選択したホストのホスト属性の設定（50-32 ページ）
- ホスト属性の検索（50-33 ページ）
- セット属性修復の構成（54-16 ページ）

ホスト属性の表示

ライセンス：FireSIGHT

Defense Centerを使用して、システムで検出されたホストのテーブル、およびそのホスト属性を表示することができます。ここでユーザは、検索する情報に応じてビューを操作できます。

ユーザがホスト属性にアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフロー（検出されたすべてのホスト、およびそのホストの属性が記載されているホスト属性のテーブル ビューが含まれており、ホスト ビュー ページで終了するワークフロー）を使用することができます。このワークフローには、制約を満たすすべてのホストについて 1 つのホスト プロファイルが含まれています。

また、特定のニーズにあった情報のみを表示するカスタム ワークフローを作成することもできます。カスタム ワークフローの作成方法については、カスタム ワークフローの作成（58-43 ページ）を参照してください。

ホスト属性のアクションの表で、ホスト属性のワークフロー ページで実行できる特定の操作について説明します。一般的なディスカバリ イベントのアクションの表に記載されているタスクも実行できます。

表 50-6　　ホスト属性のアクション

目的	操作
テーブルのカラムの内容について詳細を参照する	詳細については、ホスト属性のテーブルについて（50-31 ページ）で確認できます。
選択したホストにホスト属性を割り当てる	詳細については、選択したホストのホスト属性の設定（50-32 ページ）で確認できます。

ホストの属性を表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Hosts] > [Host Attributes] を選択します。

デフォルトのホスト属性ワークフローの最初のページが表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

ヒント　ホスト属性のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(switch workflow)] をクリックして [Attributes] を選択します。

ホスト属性のテーブルについて

ライセンス：FireSIGHT

FireSIGHT システムは、検出したホストに関する情報を収集し、その情報を使用してホスト プロファイルを作成します。ただし、ネットワーク上のホストについて、アナリストに提供する追加情報が存在する場合があります。ユーザは、ホスト プロファイルにメモを追加する、ビジネスの重要度を設定する、選択する他の情報を提供する、といったことが可能です。それぞれの情報は、ホスト属性と呼ばれます。

ホスト プロファイルの認定でホスト属性を使用することができます。これにより、トラフィック プロファイルの作成中に収集するデータを制約し、相関ルールをトリガーする条件を制限することができます。

ホスト属性テーブルには、MAC アドレスでのみ識別されるホストは表示されないことに注意してください。

ホスト属性の詳細については、事前定義のホスト属性の使用（49-34 ページ）およびユーザ定義のホスト属性の使用（49-35 ページ）を参照してください。

次に、ホスト属性テーブルのフィールドについて説明します。

IP Address

ホストに関連付けられている IP アドレス。

Current User

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることが可能です。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

Host Criticality

ユーザが割り当てた、企業にとってのホストの重要度。ホストの重要度を相関ルールおよびポリシーで使用して、イベントに関するホストの重要度に対して、ポリシー違反および違反の応答を作成することができます。ホストの重要度に Low、Medium、High、または None を割り当てることができます。

ホストの重要度の設定については、事前定義のホスト属性の使用（49-34 ページ）および選択したホストのホスト属性の設定（50-32 ページ）を参照してください。

注意

他のアナリストに提示する、ホストに関する情報。メモを追加する方法については、事前定義のホスト属性の使用（49-34 ページ）を参照してください。

Any user-defined host attribute, including those for compliance white lists

ユーザ定義のホスト属性の値。

ホスト属性テーブルには、ユーザ定義のそれぞれのホスト属性のフィールドが含まれています。詳細については、ユーザ定義のホスト属性の使用（49-35 ページ）を参照してください。

Count

各ローに表示される情報に一致するイベントの数。[Count] フィールドは、2 つ以上の同じローを作成する制約を適用した場合のみ表示されることに注意してください。

選択したホストのホスト属性の設定

ライセンス：FireSIGHT

各ホストに割り当てることができる事前定義のホスト属性として、ホストの重要度とホスト特有のメモの 2 つの属性があります。

ホストの重要度を使用して、特定のホストのビジネス重要度を特定します。ホストの重要度に基づいて、相関ポリシーとアラートを作成することができます。たとえば、ユーザの業務にとって、組織のメール サーバは一般のユーザ ワークステーションよりも重要です。メール サーバや、他のビジネスに不可欠なサーバに対しては高いホスト重要度を割り当てて、その他のホストには中程度、または低い重要度を割り当てることができます。次に相関ポリシーを作成できます。これは、影響を受けるホストの重要度に基づいてさまざまなアラートを起動します。

メモを使用して、他のアナリストに提示するホストの情報を記録します。たとえば、ネットワーク上のコンピュータに、パッチが適用されていない古いバージョンの、テスト用オペレーティング システムが搭載されている場合、メモ機能を使用して、システムは意図的にパッチが適用されていないと示すことができます。

ユーザ定義のホスト属性を作成することもできます。たとえば、ファシリティ コード、市、または部屋番号など、ホストに対して物理的な場所の識別子を割り当てるホスト属性を作成することもできます。作成したユーザ定義のホスト属性の詳細については、ユーザ定義のホスト属性の作成（49-36 ページ）を参照してください。

選択したホストのホスト重要度は、ホスト ワークフローで設定することも、ホスト プロファイル、または修復によって設定することもできます。詳細については、事前定義のホスト属性の使用（49-34 ページ）またはセット属性修復の構成（54-16 ページ）を参照してください。

選択したホストのホスト属性を設定するには、以下を行います。

アクセス：Admin/Any Security Analyst

ステップ 1　ホスト属性に追加するホストの隣にあるチェック ボックスをオンにします。

ヒント　ソートおよび検索機能を使用して、特別な属性を割り当てるホストを分離することができます。

ステップ 2　ページの下部にある [Set Attributes] をクリックします。

[Host Attributes] ポップアップ ウィンドウが表示されます。

ステップ 3　必要に応じて、選択したホストに対してホストの重要度を設定します。

[None]、[low]、[Medium]、または [High] を選択できます。

ステップ 4　必要に応じて、選択したホストのホスト プロファイルにメモを追加することができます。メモは、最大 255 文字の英数字、特殊文字、およびスペースを使用してテキスト ボックスに入力します。

ステップ 5　必要に応じて、自身で設定したユーザ定義のホスト属性を設定します。

ステップ 6　[Save] をクリックします。

指定したホスト属性は、選択されたホストに割り当てられます。

ホスト属性の検索

ライセンス：FireSIGHT

特定のホストの属性を持つホストを検索できます。たとえば企業に複数の支社がある場合、いずれかのホストが存在する都市を示すホスト属性を設定することができます。これで、特定の地域のホストを検索できるようになります。ホスト属性の詳細については、ユーザ定義のホスト属性の使用（49-35 ページ）を参照してください。

ネットワーク環境に合わせてカスタマイズした検索を作成し、後で再使用するために保存することもできます。ホスト属性のフィールドの詳細については、ホスト属性のテーブルについて（50-31 ページ）を参照してください。

一般的な検索の構文

システムは、各検索フィールドの横に有効な構文の例を示します。検索条件を入力する場合、次の点に注意してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「A」または「B」または「C, D, E」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。

  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。

- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク(*)を使用できます。
- いくつかのフィールドでは、フィールドに `n/a` または `blank` を指定して、そのフィールドで情報を使用できないイベントを特定することができます。`!n/a` または `!blank` を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。FireSIGHT システムへの IPv4 および IPv6 のアドレスの入力については、IP アドレスの表記規則(1-23 ページ)を参照してください。
- オブジェクトを検索条件として使用するには、検索フィールドの隣にあるオブジェクトの追加アイコン(+)をクリックします。

検索でのオブジェクトの使用など、検索構文の詳細については、イベントの検索(60-1 ページ)を参照してください。

ホスト属性を検索するには、以下を行います。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　テーブルのドロップダウン リストから [Host Attributes] を選択します。

ページが適切な制約によって更新されます。

ヒント　データベース内で別の種類のイベントを検索するには、テーブルのドロップダウン リストから選択します。

ステップ 3　ホスト属性のテーブルについてに記載されているように、該当するフィールドに検索条件を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。オブジェクトを検索条件として使用するには、検索フィールドの隣にある追加アイコン(+)をクリックします。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　制約された権限を持つカスタム ユーザ ロールの制約として検索を保存する場合は、検索を非公開として保存する**必要があります**。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save As New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

検索結果は、デフォルトのホスト属性ワークフローに表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

侵害の痕跡の使用

ライセンス：FireSIGHT

FireSIGHT システムは、監視対象ネットワーク上でホストが悪意のある手段によって侵害されそうかどうかを判断するために、ホストに関連付けられているさまざまなタイプのデータ（侵入イベント、Security Intelligence、接続イベント、ファイルまたはマルウェア イベント）との関連性を示します。イベント データの特定の組み合わせと頻度は、影響を受けたホストの侵害の痕跡（IOC）タグをトリガーとして使用します。IOC のタグが付けられたホスト IP アドレスは、侵害されたホストの特別なアイコン（  ）付きでイベント ビューに表示されます。ユーザはコンプライアンス ルールを記述して、IOC のタグが付けられているホストについて説明することができます。

この機能を使用するには、ネットワーク検出ポリシーで IOC ルールを有効にしておく必要があります。侵害されたホストの IOC タグをトリガーするために、事前定義のいずれか、またはすべてのルールを有効にすることができます。詳細については、侵害の兆候ルールの設定（45-37 ページ）を参照してください。

侵害の痕跡に関する詳細は、以降の項を参照してください。

侵害の痕跡の表示

ライセンス：FireSIGHT

Defense Centerを使用して、トリガーされた侵害の痕跡（IOC）のテーブルを表示することができます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

ユーザが IOC にアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義の IOC ワークフローは両方とも、ホスト ビューで終了しますが、これにはユーザの制約を満たすすべてのホストのホスト プロファイルが含まれています。また、特定のニーズにあった情報のみを表示するカスタム ワークフローを作成することもできます。詳細については、カスタム ワークフローの作成（58-43 ページ）を参照してください。

次の表では、IOC のワークフロー ページでユーザが実行できる特定のアクションについて説明します。一般的なディスカバリ イベントのアクションの表に記載されているタスクも実行できます。

表 50-7　侵害の痕跡のアクション

目的	操作
テーブルのカラムの内容について詳細を参照する	詳細については、侵害の痕跡テーブルについて（50-36 ページ）で確認できます。
侵害されたホストのホスト プロファイルを表示する	[IP Address] カラムで侵害されたホストのアイコン（  ）をクリックします。
選択した IOC イベントに解決済みとマークして、リストに表示されないようにする	編集する IOC イベントの隣にあるチェック ボックスをオンにして、[Mark Resolved] をクリックします。詳細については、侵害の痕跡を解決済みにする（49-11 ページ）を参照してください。
IOC をトリガーとして使用したイベントの詳細を表示する	[First Seen] または [Last Seen] カラムで表示アイコン（  ）をクリックします。

侵害の痕跡を表示するには、以下を行います。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Hosts] > [Indications of Compromise] を選択します。

デフォルトの侵害の痕跡（IOC）ワークフローの最初のページが表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

ヒント　IOC のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(switch workflow)] をクリックして [Indications of Compromise] を選択します。

侵害の痕跡テーブルについて

ライセンス： FireSIGHT

FireSIGHT システムは、監視対象ネットワーク上でホストが悪意のある手段によって侵害されそうかどうかを判断するために、ホストに関連付けられているさまざまなタイプのイベント データとの関連性を示します。これらの相関は、ホストに関連付けられている侵害の痕跡（IOC）として表示されます。ホストの IOC を解決済みにマークして、ホストから IOC タグを削除することが

できます。1 つのホストで複数の IOC タグをトリガーできます。ユーザは、ホスト プロファイルの [Indications of Compromise] セクションで、ホストに関連付けられているすべての IOC タグを表示できます。ホスト プロファイルにおける IOC データの詳細については、ホスト プロファイルでの侵害の痕跡の使用（49-9 ページ）を参照してください。

次に、IOC テーブルのフィールドについて説明します。

IP Address

IOC をトリガーとして使用したホストに関連付けられている IP アドレス。

カテゴリ

`Malware Executed` や `Impact 1 Attack` など、示された侵害のタイプの簡単な説明。

イベント タイプ

特定の侵害の痕跡（IOC）に関連付けられている識別子で、トリガーとして使用したイベントを参照します。

説明

侵害される可能性のあるホストについて、IOC が表している内容の説明（`This host may be under remote control` や `Malware has been executed on this host` など）。

First/Last Seen

ホストの IOC をトリガーとして使用したイベントが発生した最初（または最新）の日付と時刻。

侵害の痕跡の検索

ライセンス：FireSIGHT

事前定義のいずれかの検索を使用するか、または独自の検索条件を使用して、監視対象のホスト上でトリガーされた特定の侵害の痕跡（IOC）タグを検索することができます。事前定義の検索は例として機能し、これを使用してネットワークに関する重要な情報へすばやくアクセスできます。

デフォルトの検索で特定のフィールドを変更し、ネットワーク環境に合わせてカスタマイズして、後で再使用するために保存することもできます。データを取得するために使用できるフィールドは、侵害の痕跡テーブルについて（50-36 ページ）に記載されています。

一般的な検索の構文

それぞれの検索フィールドの隣には、使用できる構文の例が表示されます。検索条件を入力する場合、次の点に注意してください。

- すべてのフィールドで否定（`!`）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「`A`」または「`B`」または「`C, D, E`」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。

  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク(*)を使用できます。
- いくつかのフィールドでは、フィールドに `n/a` または `blank` を指定して、そのフィールドで情報を使用できないイベントを特定することができます。`!n/a` または `!blank` を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。FireSIGHT システムへの IPv4 および IPv6 のアドレスの入力については、IP アドレスの表記規則(1-23 ページ)を参照してください。
- オブジェクトを検索条件として使用するには、検索フィールドの隣にあるオブジェクトの追加アイコン(+)をクリックします。

検索でのオブジェクトの使用など、検索構文の詳細については、イベントの検索(60-1 ページ)を参照してください。

侵害の痕跡を検索するには、以下を行います。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　テーブルのドロップダウン リストから、[Indications of Compromise] を選択します。

ページが適切な制約によって更新されます。

ヒント　データベース内で別の種類のイベントを検索するには、テーブルのドロップダウン リストから選択します。

ステップ 3　侵害の痕跡テーブルについて(50-36 ページ)に記載されているように、該当するフィールドに検索条件を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。オブジェクトを検索条件として使用するには、検索フィールドの隣にある追加アイコン(+)をクリックします。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　制約された権限を持つカスタム ユーザ ロールの制約として検索を保存する場合は、検索を非公開として保存する**必要があります**。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save As New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

検索結果は、デフォルトの IOC ワークフローに表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

サーバの使用

ライセンス：FireSIGHT

FireSIGHT システムは、監視対象ネットワーク セグメント上のホストで稼動しているすべてのサーバに関する情報を収集します。システムが収集する情報には、サーバ名、サーバが使用するアプリケーションおよびネットワークのプロトコル、サーバのベンダーとバージョン、サーバを実行しているホストに関連付けられている IP アドレス、およびサーバが通信しているポートが含まれています。

システムはサーバを検出すると、関連するホストがまだサーバの最大数に達していない場合は、ディスカバリ イベントを生成します。詳細については、ホスト制限と検出イベント ロギング（45-15 ページ）を参照してください。Defense Centerの Web インターフェイスを使用して、サーバイベントを表示、検索、および削除できます。

また、サーバ イベントを相関ルールのベースにすることもできます。たとえばシステムが、いずれかのホスト上で稼動している ircd などのチャット サーバを検出したときに相関ルールをトリガーできます。

NetFlow 対応のデバイスによってエクスポートされたアプリケーション データに基づいてサーバをネットワーク マップに追加するよう、ネットワーク検出ポリシーを設定できますが、これらのサーバについて使用できる情報は制限されます。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

詳細については、次の項を参照してください。

- サーバの表示（50-40 ページ）
- サーバのテーブルについて（50-40 ページ）
- サーバの検索（50-43 ページ）
- サーバのアイデンティティの編集（49-20 ページ）

サーバの表示

ライセンス：FireSIGHT

Defense Centerを使用して、検出されたサーバのテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

ユーザがサーバにアクセスしたときに表示されるページは、使用するワークフローによって異なります。事前定義のすべてのワークフローはホスト ビューで終了しますが、このホスト ビューには、制約を満たすすべてのホストに対して 1 つずつホスト プロファイルが含まれています。また、特定のニーズにあった情報のみを表示するカスタム ワークフローを作成することもできます。詳細については、カスタム ワークフローの作成（58-43 ページ）を参照してください。

サーバの操作の表で、サーバ ワークフロー ページで実行できる特定の操作について説明します。一般的なディスカバリ イベントのアクションの表に記載されているタスクも実行できます。

表 50-8　　サーバの操作

目的	操作
テーブルのカラムの内容について詳細を参照する	詳細については、サーバのテーブルについて（50-40 ページ）で確認できます。
サーバ アイデンティティを編集する	編集するサーバのイベントの隣にあるチェック ボックスをオンにして、[Set Server Identity] をクリックします。詳細については、サーバのアイデンティティの編集（49-20 ページ）を参照してください。

サーバを表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Hosts] > [Servers] を選択します。

デフォルトのサーバ ワークフローの最初のページが表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

ヒント　サーバのテーブル ビューが含まれていないカスタム ワークフローを使用している場合は、[(switch workflow)] をクリックして [Servers] を選択します。

サーバのテーブルについて

ライセンス：FireSIGHT

FireSIGHT システムは、監視対象ネットワーク セグメント上のホストで稼動しているサーバに関する情報を収集します。

次に、サーバのテーブルのフィールドについて説明します。

NetFlow 対応のデバイスによってエクスポートされたデータに基づいてサーバをネットワーク マップに追加するよう、ネットワーク検出ポリシーを設定できますが、これらのサーバについて使用できる情報は制限されます。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

Last Used

ネットワーク上でサーバが最後に使用された日付と時間、またはホスト入力機能を使用してサーバが最初に更新された日付と時間。[Last Used] の値は、システムがサーバ情報の更新を検出したときだけでなく、少なくともユーザがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。更新間隔の設定については、データ保存の設定（45-39 ページ）を参照してください。

IP Address

サーバを実行しているホストに関連付けられている IP アドレス。

Port

サーバが稼動しているポート。

プロトコル

サーバが使用するネットワークまたはトランスポート プロトコル。

アプリケーション プロトコル

以下のいずれかによって示されるアプリケーション プロトコル

- サーバのアプリケーション プロトコルの名前
- `pending`：システムで、いずれかの理由のでサーバをポジティブまたはネガティブに識別できない場合
- `unknown`：既知のサーバ フィンガープリントに基づいてシステムでサーバを識別できない場合、またはホストの入力を介してサーバが追加され、アプリケーション プロトコルが含まれていなかった場合

Category, Tags, Risk, or Business Relevance for Application Protocols

アプリケーション プロトコルに割り当てられているカテゴリ、タグ、リスク レベル、およびビジネス関連性。これらのフィルタを使用して、特定のデータ セットを対象にすることができます。詳細については、表 45-2（45-12 ページ）を参照してください。

ベンダー

次のいずれかになります。

- サーバのベンダー：システム、Nmap、その他のアクティブなソースで識別された、またはホスト入力機能を使用して指定されたサーバのベンダー
- 空白：システムが既知のサーバ フィンガープリントに基づいてベンダーを識別できなかった場合、または NetFlow データを使用してサーバがネットワーク マップに追加された場合

Version

次のいずれかになります。

- サーバのバージョン：システム、Nmap、その他のアクティブなソースで識別された、またはホスト入力機能を使用して指定されたサーバのバージョン

– 空白：システムが既知のサーバ フィンガープリントに基づいてバージョンを識別できない場合、または NetFlow データを使用してサーバがネットワーク マップに追加された場合

Web Application

http トラフィックでシステムが検出したペイロード コンテンツに基づいた Web アプリケーション。システムが HTTP のアプリケーション プロトコルを検出したものの、特定の Web アプリケーションを検出できない場合は、一般的な Web ブラウジングの指定が提示されるので注意してください。

Category, Tags, Risk, or Business Relevance for Web Applications

Web アプリケーションに割り当てられているカテゴリ、タグ、リスク レベル、およびビジネス関連性。これらのフィルタを使用して、特定のデータ セットを対象にすることができます。詳細については、表 45-2（45-12 ページ）を参照してください。

Hits

サーバがアクセスされた回数。ホスト入力機能を使用して追加されたサーバの場合、この値は必ず 0 になります。

Source Type

次の値のいずれかを指定します。

– User: *user_name*

– Application: *app_name*

– Scanner: *scanner_type*（ネットワーク検出の設定を介して追加された Nmap またはスキャナ）

– FireSIGHT、FireSIGHT Port Match、または FireSIGHT Pattern Match（FireSIGHT システムで検出されたサーバの場合）

– NetFlow（NetFlow データに基づいてネットワーク マップに追加されたサーバの場合）

システムでは、サーバのアイデンティティを判断するために、複数のソースのデータを統合することができます。現在の ID について（46-5 ページ）を参照してください。

デバイス

サーバを検出したデバイスの名前、またはネットワーク マップにサーバを追加した NetFlow あるいはホスト入力データを処理したデバイスの名前。

Current User

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることが可能です。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

Count

各ローに表示される情報に一致するイベントの数。[Count] フィールドは、2 つ以上の同じローを作成する制約を適用した場合のみ表示されることに注意してください。

サーバの検索

ライセンス：FireSIGHT

事前定義のいずれかの検索、または独自の検索条件を使用して、監視対象のホストで稼動中の特定のサーバを検索することができます。事前定義の検索は例として機能し、これを使用してネットワークに関する重要な情報へすばやくアクセスできます。

デフォルトの検索で特定のフィールドを変更し、ネットワーク環境に合わせてカスタマイズして、後で再使用するために保存することもできます。データを取得するために使用できるフィールドは、サーバのテーブルについて（50-40 ページ）に記載されています。

サーバを検索する場合には、NetFlow 対応のデバイスによってエクスポートされたデータに基づいてアプリケーションやサーバをネットワーク マップに追加するよう、ネットワーク検出ポリシーを設定できますが、これらのサーバについて使用できる情報は制限されることに注意してください。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

一般的な検索の構文

それぞれの検索フィールドの隣には、使用できる構文の例が表示されます。検索条件を入力する場合、次の点に注意してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「`A`」または「`B`」または「`C, D, E`」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク（*）を使用できます。
- いくつかのフィールドでは、フィールドに `n/a` または `blank` を指定して、そのフィールドで情報を使用できないイベントを特定することができます。`!n/a` または `!blank` を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。FireSIGHT システムへの IPv4 および IPv6 のアドレスの入力については、IP アドレスの表記規則（1-23 ページ）を参照してください。
- 特定のデバイス、およびグループ、スタック、またはクラスタ内のデバイスを検索するには、デバイス フィールドを使用します。検索での FireSIGHT システムによるデバイス フィールドの処理方法については、検索でのデバイスの指定（60-7 ページ）を参照してください。

- オブジェクトを検索条件として使用するには、検索フィールドの隣にあるオブジェクトの追加アイコン(+)をクリックします。

検索でのオブジェクトの使用など、検索構文の詳細については、イベントの検索（60-1 ページ）を参照してください。

サーバを検索するには、以下を行います。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　テーブルのドロップダウン リストから [Servers] を選択します。

ページが適切な制約によって更新されます。

ヒント　データベース内で別の種類のイベントを検索するには、テーブルのドロップダウン リストから選択します。

ステップ 3　該当するフィールドに検索基準を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。オブジェクトを検索条件として使用するには、検索フィールドの隣にある追加アイコン(+)をクリックします。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　制約された権限を持つカスタム ユーザ ロールの制約として検索を保存する場合は、検索を非公開として保存する**必要があります**。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save As New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

検索結果は、デフォルトのサーバ ワークフローに表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

アプリケーションの使用

ライセンス：FireSIGHT

監視対象ホストが別のホストに接続すると、システムは多くの場合、どのアプリケーションが使用されたかを判断することができます。FireSIGHT システムは多くの電子メールの使用、インスタント メッセージ、ピア ツー ピア、Web アプリケーション、およびその他のタイプのアプリケーションの使用を検出します。

検出されたそれぞれのアプリケーションに対してシステムは、アプリケーションを使用した IP アドレス、製品、バージョン、および使用が検出された回数を記録します。Web インターフェイスを使用して、アプリケーション イベントを表示、検索、および削除できます。ホスト入力機能を使用して、1 つ以上のホスト上のアプリケーション データを更新することもできます。

どのアプリケーションがどのホストで稼動しているかがわかっている場合は、そのことを使用してホスト プロファイルの認定を作成し、この認定によって、トラフィック プロファイルの作成中に収集するデータを制約することができます。また、相関ルールをトリガーする条件を制約することもできます。また、アプリケーションの検出を相関ルールのベースにすることもできます。たとえば、従業員に特定のメール クライアントを使用させたい場合は、システムが、いずれかの対象ホストで別のメール クライアントが稼動していることを検出したときに相関ルールをトリガーすることができます。

更新されたディテクタの情報については、各 VDB 更新のアドバイザリの他に、FireSIGHT システムの各更新に関するリリース ノートをよく読んでください。

分析用にアプリケーション データを収集および格納するには、ネットワーク検出ポリシーでアプリケーションの検出が有効になっていることを確認します。詳細については、検出データ収集について（45-1 ページ）を参照してください。

詳細については、次の項を参照してください。

- アプリケーションの詳細の表示（50-50 ページ）
- アプリケーションの詳細テーブルについて（50-51 ページ）
- アプリケーションの詳細の検索（50-52 ページ）

アプリケーションの表示

ライセンス：FireSIGHT

Defense Centerを使用して、検出されたアプリケーションのテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

ユーザがアプリケーションにアクセスするときに表示されるページは、使用するワークフローによって異なります。また、特定のニーズにあった情報のみを表示するカスタム ワークフローを作成することもできます。詳細については、カスタム ワークフローの作成（58-43 ページ）を参照してください。

アプリケーションの操作の表で、アプリケーション ワークフロー ページで実行できる特定の操作について説明します。一般的なディスカバリ イベントのアクションの表に記載されているタスクも実行できます。

表 50-9　アプリケーションの操作

目的	操作
テーブルのカラムの内容について詳細を参照する	詳細については、アプリケーション テーブルについて（50-46 ページ）で確認できます。
特定のアプリケーションに対する [Application Detail View] を開く	クライアント、アプリケーション プロトコル、または Web アプリケーションの隣にあるアプリケーション詳細ビューのアイコン（）をクリックします。

アプリケーションを表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Hosts] > [Applications Details] を選択します。

デフォルトのアプリケーション詳細ワークフローの最初のページが表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

ヒント　アプリケーションの詳細のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(switch workflow)] をクリックして [Clients] を選択します。

アプリケーション テーブルについて

ライセンス：FireSIGHT

監視対象ホストが別のホストに接続すると、FireSIGHT システムは多くの場合、どのアプリケーションが使用されたかを判断することができます。システムはさまざまな Web ブラウザまたはサーバ、電子メール クライアントまたはサーバ、インスタント メッセンジャー、ピアツーピア アプリケーションなどを検出します。システムは既知のクライアント、アプリケーション プロトコル、または Web アプリケーションに対してトラフィックを検出すると、アプリケーション、およびそのアプリケーションを実行しているホストに関する情報を記録します。

FireSIGHT システムはアプリケーション データを 3 つのタイプ（クライアント、Web アプリケーション、アプリケーション プロトコル）に分類します。アプリケーション テーブルは、アプライアンスで検出された 3 つのすべてのタイプのアプリケーションの組み合わせのリストを提供します。

次に、アプリケーション テーブルのフィールドについて説明します。

アプリケーション

検出されたアプリケーションの名前。

IP Address

アプリケーションを使用しているホストに関連付けられている IP アドレス。

Category

アプリケーションの最も不可欠な機能を表す一般的な分類。各アプリケーションは、少なくとも 1 つのカテゴリに属します。

Tag

アプリケーションに関する追加情報。アプリケーションには任意の数(0 を含む)のタグを付けることができます。

Risk

このアプリケーションが、組織のセキュリティ ポリシーに違反するかもしれない目的で使用される可能性がどの程度であるか。アプリケーションのリスクは、Very Low から Very High までの範囲です。

侵入イベントをトリガーとして使用したトラフィックで検出された 3 つの Application Protocol Risk、Client Risk、および Web Application Risk の中で最も高いものとなります(有効な場合)。

Business Relevance

アプリケーションが、娯楽としてではなく、組織のビジネス活動の範囲内で使用される可能性。アプリケーションのビジネスとの関連性は、Very Low から Very High までの範囲です。

侵入イベントをトリガーとして使用したトラフィックで検出された 3 つの Application Protocol Business Relevance、Client Business Relevance、および Web Application Business Relevance の中で、最も低いものとなります(有効な場合)。

Current User

ホストに現在ログインしているユーザの ID(ユーザ名)。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることが可能です。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

タイプ

アプリケーションのタイプ:

- **Application Protocols** はホスト間の通信を表します。
- **Client Applications** は、ホスト上で稼動しているソフトウェアを表します。
- **Web Applications** は、HTTP トラフィックのコンテンツまたは要求された URL を表します。

Count

各ローに表示される情報に一致するイベントの数。[Count] フィールドは、2 つ以上の同じローを作成する制約を適用した場合のみ表示されることに注意してください。

アプリケーションの検索

ライセンス：FireSIGHT

特定のクライアント、アプリケーション プロトコル、または Web アプリケーションを実行しているホストを検索することができます。ネットワーク環境に合わせてカスタマイズした検索を作成し、後で再使用するために保存することもできます。

一般的な検索の構文

それぞれの検索フィールドの隣には、使用できる構文の例が表示されます。検索条件を入力する場合、次の点に注意してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「`A`」または「`B`」または「`C, D, E`」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク（*）を使用できます。
- いくつかのフィールドでは、フィールドに `n/a` または `blank` を指定して、そのフィールドで情報を使用できないイベントを特定することができます。`!n/a` または `!blank` を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。FireSIGHT システムへの IPv4 および IPv6 のアドレスの入力については、IP アドレスの表記規則（1-23 ページ）を参照してください。
- オブジェクトを検索条件として使用するには、検索フィールドの隣にあるオブジェクトの追加アイコン（ ＋ ）をクリックします。

検索でのオブジェクトの使用など、検索構文の詳細については、イベントの検索（60-1 ページ）を参照してください。

アプリケーションを検索するには、以下を行います。

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　テーブルのドロップダウン リストから [Applications] を選択します。

ページが適切な制約によって更新されます。

ステップ 3　該当するフィールドに検索基準を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。オブジェクトを検索条件として使用するには、検索フィールドの隣にある追加アイコン（ ＋ ）をクリックします。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　制約された権限を持つカスタム ユーザ ロールの制約として検索を保存する場合は、検索を非公開として保存する**必要があります**。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save As New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

検索結果は、デフォルトのクライアント ワークフローに表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

アプリケーションの詳細の使用

ライセンス：FireSIGHT

監視対象ホストが別のホストに接続すると、システムは多くの場合、どのアプリケーションが使用されたかを判断することができます。FireSIGHT システムは多くの電子メールの使用、インスタント メッセージ、ピア ツー ピア、Web アプリケーション、およびその他のタイプのアプリケーションの使用を検出します。

検出されたそれぞれのアプリケーションに対してシステムは、アプリケーションを使用した IP アドレス、製品、バージョン、および使用が検出された回数を記録します。Web インターフェイスを使用して、アプリケーション イベントを表示、検索、および削除できます。ホスト入力機能を使用して、1 つ以上のホスト上のアプリケーション データを更新することもできます。

どのアプリケーションがどのホストで稼動しているかがわかっている場合は、そのことを使用してホスト プロファイルの認定を作成し、この認定によって、トラフィック プロファイルの作成中に収集するデータを制約することができます。また、相関ルールをトリガーする条件を制約

することもできます。また、アプリケーションの検出を相関ルールのベースにすることもできます。たとえば、従業員に特定のメール クライアントを使用させたい場合は、システムが、いずれかの対象ホストで別のメール クライアントが稼動していることを検出したときに相関ルールをトリガーすることができます。

更新されたディテクタの情報については、各 VDB 更新のアドバイザリの他に、FireSIGHT システムの各更新に関するリリース ノートをよく読んでください。

分析用にアプリケーション データを収集および格納するには、ネットワーク検出ポリシーでアプリケーションの検出が有効になっていることを確認します。詳細については、アプリケーション検出について（45-11 ページ）を参照してください。

詳細については、次の項を参照してください。

- アプリケーションの詳細の表示（50-50 ページ）
- アプリケーションの詳細テーブルについて（50-51 ページ）
- アプリケーションの詳細の検索（50-52 ページ）

アプリケーションの詳細の表示

ライセンス：FireSIGHT

Defense Centerを使用して、検出されたアプリケーションの詳細テーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

ユーザがアプリケーションの詳細にアクセスするときに表示されるページは、使用するワークフローによって異なります。2 つの事前定義されたワークフローがあります。また、特定のニーズにあった情報のみを表示するカスタム ワークフローを作成することもできます。詳細については、カスタム ワークフローの作成（58-43 ページ）を参照してください。

アプリケーションの詳細の操作の表で、アプリケーション詳細ワークフロー ページで実行できる特定の操作について説明します。一般的なディスカバリ イベントのアクションの表に記載されているタスクも実行できます。

表 50-10　アプリケーションの詳細の操作

目的	操作
テーブルのカラムの内容について詳細を参照する	詳細については、アプリケーションの詳細テーブルについて（50-51 ページ）で確認できます。
特定のアプリケーションに対する [Application Detail View] を開く	クライアントの隣にあるアプリケーション詳細ビューのアイコン（  ）をクリックします。

アプリケーションの詳細を表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Hosts] > [Applications Details] を選択します。

デフォルトのアプリケーション詳細ワークフローの最初のページが表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

ヒント　アプリケーションの詳細のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(switch workflow)] をクリックして [Clients] を選択します。

アプリケーションの詳細テーブルについて

ライセンス：FireSIGHT

監視対象ホストが別のホストに接続すると、FireSIGHT システムは多くの場合、どのアプリケーションが使用されたかを判断することができます。システムはさまざまな Web ブラウザ、電子メール クライアント、インスタント メッセンジャー、ピアツーピア アプリケーションなどを検出します。.

システムは既知のクライアント、アプリケーション プロトコル、または Web アプリケーションに対してトラフィックを検出すると、アプリケーション、およびそのアプリケーションを実行しているホストに関する情報を記録します。次に、アプリケーションの詳細テーブルのフィールドについて説明します。

Last Used

アプリケーションが最後に使用された時間、またはホスト入力機能を使用してアプリケーション データが更新された時間。[Last Used] の値は、システムがアプリケーション情報の更新を検出したときだけでなく、少なくともユーザがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。更新間隔の設定については、データ保存の設定（45-39 ページ）を参照してください。

IP Address

アプリケーションを使用しているホストに関連付けられている IP アドレス。

Client

アプリケーションの名前。システムがアプリケーション プロトコルを検出したものの、特定のクライアントを検出できなかった場合は、一般的な名前を提示するために、アプリケーション プロトコル名に `client` が付加されます。

Version

アプリケーションのバージョン。

クライアント、アプリケーション プロトコル、および Web アプリケーションの Category、Tags、Risk、または Business Relevance

アプリケーションに割り当てられているカテゴリ、タグ、リスク レベル、およびビジネス関連性。これらのフィルタを使用して、特定のデータ セットを対象にすることができます。詳細については、表 45-2（45-12 ページ）を参照してください。

Application Protocol

アプリケーションによって使用されるアプリケーション プロトコル。システムがアプリケーション プロトコルを検出したものの、特定のクライアントを検出できなかった場合は、一般的な名前を提示するために、アプリケーション プロトコル名に `client` が付加されます。

Web Application

http トラフィックでシステムが検出したペイロード コンテンツまたは URL に基づいた Web アプリケーション。システムが HTTP のアプリケーション プロトコルを検出したものの、特定の Web アプリケーションを検出できない場合は、一般的な Web ブラウジングの指定がここで提示されるので注意してください。

Hits

システムが使用中のアプリケーションを検出した回数。ホスト入力機能を使用して追加されたアプリケーションの場合、この値は必ず 0 になります。

デバイス

アプリケーションの詳細が含まれているディスカバリ イベントを生成したデバイス。

Current User

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることが可能です。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

Count

各ローに表示される情報に一致するイベントの数。[Count] フィールドは、2 つ以上の同じローを作成する制約を適用した場合のみ表示されることに注意してください。

アプリケーションの詳細の検索

ライセンス：FireSIGHT

特定のクライアント、アプリケーション プロトコル、または Web アプリケーションを実行しているホストを検索することができます。ネットワーク環境に合わせてカスタマイズした検索を作成し、後で再使用するために保存することもできます。

一般的な検索の構文

それぞれの検索フィールドの隣には、使用できる構文の例が表示されます。検索条件を入力する場合、次の点に注意してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、A, B, "C, D, E" を検索すると、指定したフィールドに「A」または「B」または「C, D, E」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。

  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。

- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク(*)を使用できます。
- いくつかのフィールドでは、フィールドに `n/a` または `blank` を指定して、そのフィールドで情報を使用できないイベントを特定することができます。`!n/a` または `!blank` を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。FireSIGHT システムへの IPv4 および IPv6 のアドレスの入力については、IP アドレスの表記規則(1-23 ページ)を参照してください。
- 特定のデバイス、およびグループ、スタック、またはクラスタ内のデバイスを検索するには、デバイス フィールドを使用します。検索での FireSIGHT システムによるデバイス フィールドの処理方法については、検索でのデバイスの指定(60-7 ページ)を参照してください。
- オブジェクトを検索条件として使用するには、検索フィールドの隣にあるオブジェクトの追加アイコン(+)をクリックします。

検索でのオブジェクトの使用など、検索構文の詳細については、イベントの検索(60-1 ページ)を参照してください。

アプリケーションの詳細を検索するには、以下を行います。

アクセス: Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　テーブルのドロップダウン リストから [Application Details] を選択します。

ページが適切な制約によって更新されます。

ヒント　データベース内で別の種類のイベントを検索するには、テーブルのドロップダウン リストから選択します。

ステップ 3　該当するフィールドに検索基準を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。オブジェクトを検索条件として使用するには、検索フィールドの隣にある追加アイコン(+)をクリックします。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　制約された権限を持つカスタム ユーザ ロールの制約として検索を保存する場合は、検索を非公開として保存する**必要があります**。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save As New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

検索結果は、デフォルトのアプリケーション詳細ワークフローに表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

脆弱性の処理

ライセンス： FireSIGHT

FireSIGHT システムには、独自の脆弱性追跡データベースが含まれています。これはシステムのフィンガープリンティング機能と組み合わせて使用して、ネットワーク上のホストに関連付けられている脆弱性を特定します。

ホストで稼動しているオペレーティング システム、サーバ、およびクライアントには、関連付けられている一連の脆弱性があります。ホストにパッチを適用した後、またはホストが脆弱性に関して問題ないと判断された場合は、そのホストの脆弱性を非アクティブにすることができます。Defense Centerを使用して、各ホストに対する脆弱性を追跡および確認できます。

サーバで使用されるアプリケーション プロトコルがシステム ポリシー内でマップされない限り、ベンダーレスおよびバージョンレスのサーバに対する脆弱性はマップされないことに注意してください。ベンダーレスおよびバージョンレスのクライアントに対する脆弱性はマップできません。詳細については、サーバの脆弱性のマッピング（63-32 ページ）を参照してください。

詳細については、以下を参照してください。

- 脆弱性の表示（50-54 ページ）
- 脆弱性テーブルについて（50-56 ページ）
- 脆弱性の非アクティブ化（50-57 ページ）
- 脆弱性の検索（50-58 ページ）

脆弱性の表示

ライセンス： FireSIGHT

Defense Centerを使用して、脆弱性のテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

脆弱性にアクセスするときに表示されるページは、使用するワークフローによって異なります。ユーザは事前定義のワークフローを使用できますが、これには脆弱性のテーブル ビューが含まれています。検出されたいずれかのホストが脆弱性を示しているかどうかに関係なく、テーブル ビューにはデータベース内の各脆弱性に対して 1 つのローが含まれています。事前定義のワークフローの 2 ページ目には、ネットワーク上で検出されたホストに適用されるそれぞれの脆弱性（まだユーザが非アクティブにしていないもの）に対して 1 つのローが含まれています。事前定義のワークフローは脆弱性の詳細ビューで終了しますが、このビューには、制約を満たすすべての脆弱性について詳細な説明が含まれています。

ヒント　単一のホストまたはホストのセットに適用される脆弱性を表示する場合は、ホストの IP アドレスまたは IP アドレスの範囲を指定して、脆弱性の検索を実行します。脆弱性の検索の詳細については、脆弱性の検索（50-58 ページ）を参照してください。

また、特定のニーズにあった情報のみを表示するカスタム ワークフローを作成することもできます。カスタム ワークフローの作成については、カスタム ワークフローの作成（58-43 ページ）を参照してください。

次の表では、脆弱性のワークフロー ページでユーザが実行できる特定の操作について説明します。一般的なディスカバリ イベントのアクションの表に記載されているタスクも実行できます。

表 50-11　脆弱性の操作

目的	操作
テーブルのカラムの内容について詳細を参照する	詳細については、脆弱性テーブルについて（50-56 ページ）で確認できます。
脆弱性の詳細を表示する	[SVID] カラムの表示アイコン（🔍）をクリックします。または、脆弱性 ID を制約して脆弱性の詳細ページへドリルダウンします。詳細については、脆弱性の詳細の表示（49-30 ページ）を参照してください。
選択した脆弱性を非アクティブにして、現在脆弱な状態にあるホストについて、侵入の影響の相関に使用しないようにする	詳細については、脆弱性の非アクティブ化（50-57 ページ）で確認できます。
脆弱性のタイトルの全テキストを表示する	タイトルを右クリックして [Show Full Text] を選択します。

脆弱性を表示するには、以下を行います。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Vulnerabilities] > [Vulnerabilities] を選択します。

デフォルトの脆弱性ワークフローの最初のページが表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

ヒント　脆弱性テーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(switch workflow)] をクリックして [Vulnerabilities] を選択します。

脆弱性テーブルについて

ライセンス：FireSIGHT

FireSIGHT システムには、独自の脆弱性追跡データベースが含まれています。これはシステムのフィンガープリンティング機能と組み合わせて使用して、ネットワーク上のホストに関連付けられている脆弱性を特定します。

ホストで稼動しているオペレーティング システム、サーバ、およびクライアントには、関連付けられている一連の脆弱性があります。ホストにパッチを適用した後、またはホストが脆弱性に関して問題ないと判断された場合は、そのホストの脆弱性を非アクティブにすることができます。Defense Centerを使用して、各ホストに対する脆弱性を追跡および確認できます。

脆弱性の詳細については、脆弱性のネットワーク マップの使用（48-8 ページ）およびホスト プロファイルでの脆弱性の使用（49-29 ページ）を参照してください。

次に、脆弱性テーブルのフィールドについて説明します。

SVID

脆弱性を追跡するためにシステムで使用するCiscoの脆弱性の識別番号。

SVID について脆弱性の詳細にアクセスするには、表示アイコン（  ）をクリックします。詳細については、「脆弱性の詳細の表示（49-30 ページ）」を参照してください。

Bugtraq ID

Bugtraq データベースにおいて脆弱性に関連付けられている識別番号。（http://www.securityfocus.com/bid/）

Snort ID

Snort ID（SID）データベースにおいて脆弱性に関連付けられている識別番号。つまり、侵入ルールで特定の脆弱性を悪用するネットワーク トラフィックを検出できると、その脆弱性は、侵入ルールの SID に関連付けられます。

脆弱性は複数の SID に関連付けることが可能（または SID に関連付けないことも可能）であることに注意してください。脆弱性が複数の SID に関連付けられている場合、脆弱性テーブルには、各 SID に対して 1 つのローが含まれています。

Title

脆弱性のタイトル。

IP Address

脆弱性の影響を受けるホストに関連付けられている IP アドレス。

Date Published

脆弱性が公開された日付。

Vulnerability Impact

Bugtraq データベースにおいて脆弱性に割り当てられている重大度を示します。0～10の値で、10 は最も重大であることを示します。脆弱性の影響は、Bugtraq エントリの作成者によって決定されます。この作成者は、自身の判断および SANS Critical Vulnerability Analysis（CVA）の基準に従って脆弱性の影響を決定します。

Remote

脆弱性がリモートで不正利用されるかどうかを示します。

Available Exploits

脆弱性に対して既知の不正利用があるかどうかを示します。

説明

脆弱性についての簡単な説明。

Technical Description

脆弱性に関する詳細な技術的説明。

ソリューション

脆弱性の修復に関する情報。

Count

各ローに表示される情報に一致するイベントの数。[Count] フィールドは、2 つ以上の同じローを作成する制約を適用した場合のみ表示されることに注意してください。

脆弱性の非アクティブ化

ライセンス：FireSIGHT

ネットワーク上のホストにパッチを適用した後、またはホストが脆弱性に関して問題ないと判断された後に、脆弱性を非アクティブにします。非アクティブにした脆弱性は、侵入の影響の相関には使用されなくなります。システムが、この脆弱性によって影響を受けている新しいホストを検出すると、脆弱性はこのホストに対して有効であると見なされます（自動的には非アクティブになりません）。

ユーザは、ネットワーク上の特定のホストに対して脆弱性を示すワークフローのページ（以下を参照）で**のみ**、脆弱性ワークフロー内で脆弱性を非アクティブにすることができます。

- デフォルトの脆弱性ワークフローの 2 ページ目の [Vulnerabilities on the Network]。これは、ネットワーク上のホストに適用される脆弱性のみを示します。
- 脆弱性の（カスタムまたは事前定義の）ワークフローの任意のページ。このワークフローは、検索を使用して IP アドレスに基づいて制約されます。

IP アドレスで制約されていない脆弱性ワークフロー内で脆弱性を非アクティブにすると、ネットワーク上で検出された**すべて**のホストに対する脆弱性が非アクティブ化されます。1 つのホストに対して脆弱性を非アクティブにするには、次の 3 つの方法があります。

- ネットワーク マップを使用する。

  詳細については、脆弱性のネットワーク マップの使用（48-8 ページ）を参照してください。
- ホストのホスト プロファイルを使用する。

  詳細については、個々のホストに対する脆弱性の設定（49-33 ページ）を参照してください。
- 脆弱性を非アクティブにする 1 つ以上のホストの IP アドレスに基づいて、脆弱性ワークフローを制約する。関連する複数の IP アドレスを持つホストの場合、この機能は 1 つのアドレス（そのホストで選択された IP アドレス）のみに適用されます。

IP アドレスに基づいてビューを制約するには、脆弱性を非アクティブにするホストに対して 1 つの IP アドレス、または IP アドレスの範囲を指定して、脆弱性の検索を実行します。脆弱性の検索の詳細については、脆弱性の検索（50-58 ページ）を参照してください。

脆弱性を非アクティブにするには、以下を行います。

アクセス：Admin/Any Security Analyst

ステップ 1　[Vulnerabilities on the Network] ページで、非アクティブにする脆弱性の隣にあるチェック ボックスをオンにして [Review] をクリックします。

脆弱性の検索

ライセンス：FireSIGHT

ネットワーク上のホストに影響を及ぼす脆弱性を検索できます。ネットワーク環境に合わせてカスタマイズした検索を作成し、後で再使用するために保存することもできます。

一般的な検索の構文

それぞれの検索フィールドの隣には、使用できる構文の例が表示されます。検索条件を入力する場合、次の点に注意してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「`A`」または「`B`」または「`C, D, E`」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク（*）を使用できます。
- いくつかのフィールドでは、フィールドに `n/a` または `blank` を指定して、そのフィールドで情報を使用できないイベントを特定することができます。`!n/a` または `!blank` を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。FireSIGHT システムへの IPv4 および IPv6 のアドレスの入力については、IP アドレスの表記規則（1-23 ページ）を参照してください。
- オブジェクトを検索条件として使用するには、検索フィールドの隣にあるオブジェクトの追加アイコン（ ＋ ）をクリックします。

検索でのオブジェクトの使用など、検索構文の詳細については、イベントの検索（60-1 ページ）を参照してください。

脆弱性に対する特定の検索条件

以下の、脆弱性の検索に特有な情報に注意してください。

- Bugtraq ID 番号の検索は http://www.securityfocus.com/bid で行います。
- エクスプロイトされる脆弱性を検索する場合は TRUE を入力し、そのような脆弱性を除外する場合は FALSE を入力します。

脆弱性を検索するには、以下を行います。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　テーブルのドロップダウン リストから [Vulnerabilities] を選択します。

ページが適切な制約によって更新されます。

ステップ 3　該当するフィールドに検索基準を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。オブジェクトを検索条件として使用するには、検索フィールドの隣にある追加アイコン（ ＋ ）をクリックします。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　カスタム ユーザ ロールに関するデータ制約として検索を使用する予定の場合は、それをプライベート検索として保存する**必要があります**。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save As New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

検索結果は、デフォルトの脆弱性ワークフローに表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

サードパーティの脆弱性の処理

ライセンス：FireSIGHT

FireSIGHT システムには、独自の脆弱性追跡データベースが含まれています。これはシステムのフィンガープリンティング機能と組み合わせて使用して、ネットワーク上のホストに関連付けられている脆弱性を特定します。

組織でスクリプトを記述するか、またはコマンドライン インポート ファイルを作成して、サードパーティのアプリケーションからネットワーク マップ データをインポートすることが可能な場合は、サードパーティの脆弱性データをインポートして、システムの脆弱性データを増やすことができます。詳細については、『*FireSIGHT System Host Input API Guide*』を参照してください。

インポートしたデータを影響の相関に含めるには、サードパーティの脆弱性情報を、データベース内のオペレーティング システムおよびアプリケーションの定義にマップする必要があります。サードパーティの脆弱性情報はクライアント定義にマップできません。

詳細については、以下を参照してください。

- サードパーティの脆弱性の表示（50-60 ページ）
- サードパーティの脆弱性テーブルについて（50-61 ページ）
- サードパーティの脆弱性の検索（50-62 ページ）

サードパーティの脆弱性の表示

ライセンス：FireSIGHT

ホスト入力機能を使用してサードパーティの脆弱性データをインポートした後で、Defense Centerを使用してサードパーティの脆弱性のテーブルを表示することができます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

サードパーティの脆弱性にアクセスするときに表示されるページは、使用するワークフローによって異なります。2 つの事前定義されたワークフローがあります。また、特定のニーズにあった情報のみを表示するカスタム ワークフローを作成することもできます。詳細については、カスタム ワークフローの作成（58-43 ページ）を参照してください。

次の表では、サードパーティ脆弱性のワークフロー ページでユーザが実行できる特定の操作について説明します。一般的なディスカバリ イベントのアクションの表に記載されているタスクも実行できます。

表 50-12　サードパーティの脆弱性の操作

目的	操作
テーブルのカラムの内容について詳細を参照する	詳細については、サードパーティの脆弱性テーブルについて（50-61 ページ）で確認できます。
サードパーティの脆弱性の詳細を表示する	[SVID] カラムの表示アイコン（🔍）をクリックします。または、脆弱性 ID を制約して脆弱性の詳細ページへドリルダウンします。詳細については、脆弱性の詳細の表示（49-30 ページ）を参照してください。

サードパーティの脆弱性を表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Vulnerabilities] > [Third-Party Vulnerabilities] を選択します。

デフォルトのサードパーティの脆弱性ワークフローの最初のページが表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

ヒント　サードパーティの脆弱性のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(switch workflow)] をクリックして [Vulnerabilities by Source] または [Vulnerabilities by IP Address] を選択します。

サードパーティの脆弱性テーブルについて

ライセンス：FireSIGHT

ホスト入力機能を使用して、サードパーティの脆弱性情報をインポートすると、システムはその情報をデータベースに格納します。サードパーティの脆弱性テーブルのフィールドについては、次の表で説明します。

Vulnerability Source

サードパーティの脆弱性のソース（QualysGuard、NeXpose など）。

Vulnerability ID

ソースで脆弱性に関連付けられている ID 番号。

IP Address

脆弱性の影響を受けるホストに関連付けられている IP アドレス。

Port

ポート番号（脆弱性が、特定のポート上で実行されているサーバに関連付けられている場合）。

Bugtraq ID

Bugtraq データベースにおいて脆弱性に関連付けられている識別番号。（http://www.securityfocus.com/bid/）

CVE ID

MITRE の Common Vulnerabilities and Exposures（CVE）データベースで、脆弱性に関連付けられている識別番号（http://www.cve.mitre.org/）。

SVID

脆弱性を追跡するためにシステムで使用する従来の脆弱性識別番号。

SVID について脆弱性の詳細にアクセスするには、表示アイコン（🔍）をクリックします。詳細については、「脆弱性の詳細の表示（49-30 ページ）」を参照してください。

Snort ID

Snort ID（SID）データベースにおいて脆弱性に関連付けられている識別番号。つまり、侵入ルールで特定の脆弱性を悪用するネットワーク トラフィックを検出できると、その脆弱性は、侵入ルールの SID に関連付けられます。

脆弱性は複数の SID に関連付けることが可能（または SID に関連付けないことも可能）であることに注意してください。脆弱性が複数の SID に関連付けられている場合、脆弱性テーブルには、各 SID に対して 1 つのローが含まれています。

Title

脆弱性のタイトル。

説明

脆弱性についての簡単な説明。

Count

各ローに表示される情報に一致するイベントの数。[Count] フィールドは、2 つ以上の同じローを作成する制約を適用した場合のみ表示されることに注意してください。

サードパーティの脆弱性の検索

ライセンス：FireSIGHT

ネットワーク上のホストに影響を及ぼすサードパーティの脆弱性を検索できます。ネットワーク環境に合わせてカスタマイズした検索を作成し、後で再使用するために保存することもできます。

一般的な検索の構文

それぞれの検索フィールドの隣には、使用できる構文の例が表示されます。検索条件を入力する場合、次の点に注意してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「A」または「B」または「C, D, E」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに A または B、または C、D、E のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。

- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク(*)を使用できます。
- いくつかのフィールドでは、フィールドに n/a または blank を指定して、そのフィールドで情報を使用できないイベントを特定することができます。!n/a または !blank を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。FireSIGHT システムへの IPv4 および IPv6 のアドレスの入力については、IP アドレスの表記規則(1-23 ページ)を参照してください。
- オブジェクトを検索条件として使用するには、検索フィールドの隣にあるオブジェクトの追加アイコン(+)をクリックします。

検索でのオブジェクトの使用など、検索構文の詳細については、イベントの検索(60-1 ページ)を参照してください。

脆弱性に対する特定の検索条件

以下の、脆弱性の検索に特有な情報に注意してください。

- Bugtraq ID 番号の検索は http://www.securityfocus.com/bid で行います。
- エクスプロイトされる脆弱性を検索する場合は TRUE を入力し、そのような脆弱性を除外する場合は FALSE を入力します。

サードパーティの脆弱性を検索するには、以下を行います。

アクセス: Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　テーブルのドロップダウン リストから [Third-Party Vulnerabilities] を選択します。

ページが適切な制約によって更新されます。

ステップ 3　該当するフィールドに検索基準を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。オブジェクトを検索条件として使用するには、検索フィールドの隣にある追加アイコン(+)をクリックします。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　カスタム ユーザ ロールに関するデータ制約として検索を使用する予定の場合は、それをプライベート検索として保存する**必要があります**。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され([Private] を選択した場合は本人のアカウントでのみ閲覧可能)、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save As New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

検索結果は、デフォルトのサードパーティ脆弱性ワークフローに表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

ユーザの使用

ライセンス：FireSIGHT

Active Directory Agent または管理対象デバイスがデータベースにないユーザのユーザ ログインを検出した場合、そのログイン タイプが特に制限されていない限り、そのユーザはデータベースに追加されます（ユーザ ロギングの制限（45-33 ページ）を参照してください）。

注　システムは SMTP ログインを検出しますが、電子メール アドレスが一致するユーザがデータベースにない場合、それらのログインは記録されず、ユーザは、SMTP ログインに基づいたデータベースに追加**されません**。

新しいユーザについてどの情報を格納するかは、次の表に記載されている、システムが検出したログインのタイプによって判断されます。

表 50-13　ログインのタイプと格納されるユーザ データ

ログイン タイプ	格納されるユーザ データ
LDAP AIM Oracle SIP HTTP FTP MDNS	• ユーザ名 • 現行の IP アドレス • ログイン タイプ（`aim`、`ldap`、`oracle`、`sip`、`http`、`ftp`、または `mdns`）
POP3 IMAP	• ユーザ名 • 現行の IP アドレス • 電子メール アドレス • ログイン タイプ（`pop3` または `imap`）

Defense Centerと LDAP サーバとの接続を設定すると、Defense Centerは LDAP サーバに 5 分ごとに問い合わせして、ユーザ データベースの新しいユーザに関するメタデータを取得します。それと同時にDefense Centerは、レコードがDefense Centerデータベースに格納されており、12 時間以上経過しているユーザの更新情報を LDAP サーバに問い合わせします。システムが新しいユーザのログインを検出してから、Defense Centerデータベースがユーザのメタデータを更新するまでに、5～10 分かかることがあります。Defense Centerは LDAP サーバから、各ユーザについて次の情報とメタデータを取得します。

- LDAP ユーザ名
- 姓と名
- 電子メール アドレス
- 部門
- 電話番号

Defense Centerがデータベースに格納できるユーザの数は、FireSIGHT のライセンスによって異なります。AIM、Oracle、および SIP のログインは、システムが LDAP サーバから取得したどのユーザ メタデータにも関連付けられないため、これらのログインにより重複したユーザ レコードが作成されることに注意してください。これらのプロトコルでのユーザ レコードの重複により、ユーザ カウントが過剰に使用されないようにするために、ネットワーク検出ポリシーではプロトコルのロギングを無効にします。詳細については、ユーザ ロギングの制限（45-33 ページ）を参照してください。

データベースからユーザを検索、表示、削除することができます。また、データベースからすべてのユーザを消去することもできます。詳細については、次の項を参照してください。

- ユーザの表示（50-65 ページ）
- ユーザ テーブルについて（50-66 ページ）
- ユーザの詳細とホストの履歴について（50-68 ページ）
- ユーザの検索（50-68 ページ）

ユーザの表示

ライセンス： FireSIGHT

ユーザのテーブルを表示して、検索する情報に応じてイベント ビューを操作することができます。

ユーザにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローを使用することができますが、これには、検出されたすべてのユーザが記載されているユーザのテーブル ビューが含まれています。このワークフローは、ユーザの詳細ページで終了します。ユーザの詳細ページは、制約を満たす各ユーザについての情報を提供します。

また、特定のニーズにあった情報のみを表示するカスタム ワークフローを作成することもできます。カスタム ワークフローの作成については、カスタム ワークフローの作成（58-43 ページ）を参照してください。

テーブルのカラムの内容については、ユーザ テーブルについて（50-66 ページ）に詳しく記載されています。次の表は、ユーザ ワークフロー ページで実行できる特定の操作について説明します。一般的なディスカバリ イベントのアクションの表に記載されている操作も実行できます。

ユーザを表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Users] > [Users] を選択します。

デフォルトのユーザ ワークフローの最初のページが表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

ヒント　ユーザのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(switch workflow)] をクリックして [Users] を選択します。

ユーザ テーブルについて

ライセンス：FireSIGHT

システムはユーザを検出したときに、そのユーザに関するデータを収集してデータベースに格納します。次に、ユーザ テーブルのフィールドについて説明します。

User

次のいずれかになります。

- ユーザの姓、名、およびユーザ名（Defense Centerと LDAP サーバの接続を設定した場合に収集されます）
- ユーザ名のみ（Defense Centerと LDAP サーバの接続を設定していない場合、または Defense Centerが LDAP レコードと相関できなかったユーザの場合）

Defense Centerは、ユーザの検出に使用したプロトコルも表示します。

成功しなかった AIM ログインの試行も記録されるため、Defense Centerには、（ユーザが入力するユーザ名のスペルを間違っていた場合など）無効な AIM ユーザが格納されている可能性があることに注意してください。

Current IP

ユーザがログインしたホストに関連付けられている IP アドレス。（あるユーザが権限を持っており、新しいユーザが権限を持っていない場合を除いて）、ユーザがログインした後で、権限を持っている他のユーザが同じ IP アドレスでホストにログインすると、このフィールドは空白になります（システムは、IP アドレスと、最後にホストにログインした権限のあるユーザを関連付けます）。権限のあるユーザと権限のないユーザの詳細については、ユーザ データベース（45-8 ページ）を参照してください。

First Name

ユーザの名（オプションのDefense Centerと LDAP サーバとの接続で取得されたもの）。以下の場合、このフィールドは空白になります。

- Defense Centerと LDAP サーバの接続を設定していない
- Defense Centerが、Defense Center データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）
- LDAP サーバに、対象のユーザと関連付けられている名前がない

Last Name

ユーザの姓（Defense Centerと LDAP サーバの接続を設定した場合に収集されます）。以下の場合、このフィールドは空白になります。

- Defense Centerと LDAP サーバの接続を設定していない
- Defense Centerが、Defense Center データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）
- LDAP サーバに、対象のユーザと関連付けられている姓がない

E-Mail

ユーザの電子メール アドレス。以下の場合、このフィールドは空白になります。

- AIM ログインによってユーザがデータベースに追加された
- LDAP ログインによってユーザがデータベースに追加されており、LDAP サーバ上にユーザと関連付けられている電子メール アドレスがない

部門

ユーザの部門（Defense Centerと LDAP サーバの接続を設定した場合に収集されます）。LDAP サーバ上のユーザに明示的に関連付けられている部門がない場合、この部門は、サーバが割り当てるいずれかのデフォルト グループとして示されます。たとえば、Active Directory では、これは `Users (ad)` となります。以下の場合、このフィールドは空白になります。

- Defense Centerと LDAP サーバの接続を設定していない
- Defense Centerが、Defense Center データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）

Phone

ユーザの電話番号（Defense Centerと LDAP サーバの接続を設定した場合に収集されます）。以下の場合、このフィールドは空白になります。

- Defense Centerと LDAP サーバの接続を設定していない
- Defense Centerが、Defense Center データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）
- LDAP サーバに、対象のユーザと関連付けられている電話番号がない

User Type

ユーザの検出に使用されるプロトコル。たとえば、POP3 ログインを検出したときにデータベースに追加されるユーザの場合、ユーザ タイプは `pop3` になります。

Count

各ローに示される情報と一致するユーザの数。[Count] フィールドは、2 つ以上の同じローを作成する制約を適用した場合のみ表示されることに注意してください。

ユーザの詳細とホストの履歴について

ライセンス：FireSIGHT

特定のユーザについて詳細を示すために、ユーザのテーブル ビューだけでなく、ユーザ ID データを他の種類のイベントに関連付けているイベント ビューを利用して [User Identity] ポップアップ ウィンドウを表示することができます。ユーザ ワークフローの最終ページには、ユーザの情報も表示されます。

このユーザ データは、ユーザのテーブル ビューで表示されるものと同じです。詳細については、ユーザ テーブルについて（50-66 ページ）を参照してください。

ホストの履歴には、過去 24 時間のユーザ アクティビティがグラフィック表示されます。ユーザがログインおよびログオフしたホストの IP アドレスのリストは、ログインとログアウトの回数の概数を棒グラフで示します。一般的なユーザは、1 日の間に複数のホストに対してログオンおよびログオフする可能性があります。たとえば、メール サーバに対する定期的な自動ログインは複数回の短いセッションとして示されますが、（勤務時間中などの）長時間のログインは、長いセッションとして示されます。

ホストに対して権限のないユーザがログインしていることが検出された場合、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることが可能です。ただし、ホストに対して権限のあるユーザのログインが検出された後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。ネットワーク検出ポリシーで、失敗したログインのキャプチャを設定した場合、ホストの履歴には、ユーザがログインに失敗したホストも示されます。

ホストの履歴を生成するのに使用されるデータは、ユーザの履歴データベースに格納されています。このデータベースは、デフォルトで 1000 万のユーザ ログイン イベントが格納されます。ホストの履歴で特定のユーザに関するデータが表示されない場合、そのユーザが非アクティブであるか、またはデータベースの制限を増やさなければならないことが考えられます。詳細については、データベース イベント制限の設定（63-16 ページ）を参照してください。

ユーザの詳細およびホストの履歴を表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

ステップ 1　次の 2 つのオプションから選択できます。

- ユーザが示されているいずれかのイベント ビューで、ユーザ ID の隣に示されているユーザ アイコン（）をクリックします。
- いずれかのユーザ ワークフローで、[Users] の最終ページをクリックします。

ユーザの詳細が表示されます。

ユーザの検索

ライセンス：FireSIGHT

特定のユーザを検索することができます。ネットワーク環境に合わせてカスタマイズした検索を作成し、後で再使用するために保存することもできます。

一般的な検索の構文

それぞれの検索フィールドの隣には、使用できる構文の例が表示されます。検索条件を入力する場合、次の点に注意してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「`A`」または「`B`」または「`C, D, E`」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク（*）を使用できます。
- いくつかのフィールドでは、フィールドに `n/a` または `blank` を指定して、そのフィールドで情報を使用できないイベントを特定することができます。`!n/a` または `!blank` を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。FireSIGHT システムへの IPv4 および IPv6 のアドレスの入力については、IP アドレスの表記規則（1-23 ページ）を参照してください。
- オブジェクトを検索条件として使用するには、検索フィールドの隣にあるオブジェクトの追加アイコン（ ＋ ）をクリックします。

検索でのオブジェクトの使用など、検索構文の詳細については、イベントの検索（60-1 ページ）を参照してください。

特定のユーザの検索条件

[User Type] の有効な検索条件は `ldap`、`pop3`、`imap`、`oracle`、`sip`、`http`、`ftp`、`mdns`、および `aim` です。ユーザは SMTP ログインに基づいてデータベースに追加されることがないため、`smtp` と入力しても結果は返されません。

ユーザを検索するには、以下を行います。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　テーブルのドロップダウン リストから [Users] を選択します。

[Users search] ページが表示されます。

ヒント　データベース内で別の種類のイベントを検索するには、テーブルのドロップダウン リストから選択します。

ステップ 3　該当するフィールドに検索基準を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　制約された権限を持つカスタム ユーザ ロールの制約として検索を保存する場合は、検索を非公開として保存する**必要があります**。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save As New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

検索結果は、デフォルトのユーザ ワークフローに表示されます。別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

ユーザ アクティビティ の使用

ライセンス： FireSIGHT

FireSIGHT システムは、ネットワーク上のユーザ アクティビティの詳細についてやりとりするイベントを生成します。次に、ユーザ アクティビティの 4 つのタイプについて説明します。

New User Identity

このイベントは、システムが、データベースに存在しないユーザのユーザ ログインを検出したときに生成されます。

User Login

このイベントは、以下の後に生成されます。

- Active Directory サーバにインストールした Active Directory Agent が LDAP ログインを検出した
- 管理対象デバイスが LDAP、POP3、IMAP、SMTP、AIM、Oracle、FTP、HTTP、MDNS、または SIP のログインを検出した
- ユーザ ログイン イベントについては、以下の点について留意しておく必要があります。
- 一致する電子メール アドレスを持つユーザがすでにデータベースに存在する場合を除いて、SMTP ログインは記録されません。
- 失敗したログインは、トラフィック内で検出された LDAP、IMAP、FTP、および POP3 に限定されます。ログインに失敗すると、検出されたユーザ データベースにユーザは追加されません。ただし、ネットワーク検出ポリシーのユーザ ログインの設定に基づいて、ユーザ アクティビティ データベースにオプションとしてアクティビティが記録されます。
- 特別にログイン タイプを制限している場合は、ユーザ ログインは記録されません。ユーザ ロギングの制限(45-33 ページ)を参照してください。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることが可能です。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

Delete User Identity

このイベントは、データベースからユーザを手動で削除したときに生成されます。

User Identity Dropped: User Limit Reached

このイベントは、システムがデータベースに存在しないユーザを検出したものの、FireSIGHT ライセンスで設定されているデータベースの最大ユーザ数に達したためにユーザを追加できなかったときに生成されます。

Defense Centerで保存できる検出済みユーザの総数は、FireSIGHT ライセンスによって異なります。ライセンス制限に達すると、ほとんどの場合、システムはデータベースへの新しいユーザの追加を停止します。新しいユーザを追加するには、古いユーザまたは非アクティブなユーザをデータベースから手動で削除するか、データベースからすべてのユーザを消去する必要があります。

ただし、システムでは権限のあるユーザが優先されます。すでに制限に達しており、これまでに検出されていない権限のあるユーザのログインが検出された場合、システムは長期間非アクティブな状態が続いている権限のないユーザを削除して、権限のある新しいユーザに置き換えます。

システムがユーザ アクティビティを検出すると、そのアクティビティはデータベースに記録されます。ユーザ アクティビティを表示、検索、および削除することも、データベースからすべてのユーザ アクティビティを消去することもできます。

可能な場合はいつでも、FireSIGHT システムがユーザ活動とその他のタイプのイベントを関連付けます。たとえば、侵入イベントは、イベント発生時に送信元ホストおよび宛先ホストにログインしていたユーザを通知することができます。これにより、攻撃の対象になっていたホストの所有者、または内部攻撃やポート スキャンを開始したユーザがわかります。

また、相関ルールでユーザ アクティビティを使用することもできます。ユーザ アクティビティのタイプだけでなく、自分で指定する他の条件に基づいて、相関ルールを作成することができます。相関ルールは相関ポリシーで使用され、ネットワーク トラフィックが条件を満たしたときに、修復およびアラートの応答を起動します。ユーザ アクティビティの詳細については、ユーザ データ収集について（45-3 ページ）を参照してください。

詳細については、次の項を参照してください。

- ユーザ アクティビティ イベントの表示（50-72 ページ）
- ユーザ アクティビティ テーブルについて（50-73 ページ）
- ユーザ アクティビティの検索（50-74 ページ）

ユーザ アクティビティ イベントの表示

ライセンス：FireSIGHT

ユーザ アクティビティのテーブルを表示して、検索する情報に応じてイベント ビューを操作することができます。

ユーザ アクティビティにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローを使用することができます。このワークフローにはユーザ アクティビティのテーブル ビューが含まれており、制約を満たすすべてのユーザの詳細が含まれている、ユーザの詳細ページで終了します。また、特定のニーズにあった情報のみを表示するカスタム ワークフローを作成することもできます。カスタム ワークフローの作成については、カスタム ワークフローの作成（58-43 ページ）を参照してください。

テーブルのカラムの内容については、ユーザ アクティビティ テーブルについて（50-73 ページ）に詳しく記載されています。次の表は、ユーザ アクティビティのワークフロー ページで実行できる特定の操作について説明しています。一般的なディスカバリ イベントのアクションの表に記載されている操作も実行できます。

ユーザ アクティビティを表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Users] > [User Activity] を選択します。

デフォルトのユーザ アクティビティ ワークフローの最初のページが表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。イベントが表示されない場合は、時間範囲の調整が必要なことがあります。イベント時間の制約の設定（58-26 ページ）を参照してください。

ヒント　ユーザ アクティビティのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(switch workflow)] をクリックして [User Activity] を選択します。

ユーザ アクティビティ テーブルについて

ライセンス：FireSIGHT

システムがユーザ アクティビティを検出すると、そのアクティビティはデータベースに記録されます。次に、ユーザ テーブルのフィールドについて説明します。

時刻

システムがユーザ アクティビティを検出した時間。

Event

ユーザ アクティビティのタイプ。詳細については、ユーザ アクティビティ の使用（50-70 ページ）を参照してください。

User

アクティビティに関連付けられているユーザ。このフィールドには少なくとも、ユーザの検出に使用されたユーザ名とプロトコルが含まれています。ユーザの LDAP メタデータがある場合は、このフィールドには、ユーザの名前と姓も含まれることがあります。

User Type

ユーザの検出に使用されるプロトコル。たとえば、システムが POP3 ログインを検出したときにデータベースに追加されるユーザの場合、ユーザ タイプは `pop3` になります。

IP Address

User Login アクティビティの場合はログインに関連する IP アドレスです。ユーザのホストの IP アドレス（LDAP、POP3、IMAP、FTP、HTTP、MDNS、および AIM ログインの場合）、サーバの IP アドレス（SMTP および Oracle ログインの場合）、またはセッションの開始者の IP アドレス（SIP ログインの場合）のいずれかになります。

関連付けられている IP アドレスは、そのユーザが IP アドレスの現行のユーザであることを意味するわけではないので注意してください。権限を持たないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されます。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることが可能です。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。

他のタイプのユーザ アクティビティの場合、このフィールドは空白です。

説明

Delete User Identity and User Identity Dropped アクティビティの場合、データベースから削除されたユーザの名前、またはデータベースへの追加に失敗したユーザの名前になります。ネットワーク リソースへのログインの場合、`network login` が表示されます。他のタイプのユーザ アクティビティの場合、このフィールドは空白です。

デバイス

管理対象デバイスで検出したユーザ アクティビティの場合は、そのデバイスの名前。他のタイプのユーザ アクティビティの場合は、管理しているDefense Centerになります。

Count

各ローに表示される情報に一致するイベントの数。[Count] フィールドは、2 つ以上の同じローを作成する制約を適用した場合のみ表示されることに注意してください。

ユーザ アクティビティの検索

ライセンス：FireSIGHT

特定のユーザ アクティビティを検索することができます。ネットワーク環境に合わせてカスタマイズした検索を作成し、後で再使用するために保存することもできます。

一般的な検索の構文

それぞれの検索フィールドの隣には、使用できる構文の例が表示されます。検索条件を入力する場合、次の点に注意してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「`A`」または「`B`」または「`C, D, E`」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク（*）を使用できます。
- いくつかのフィールドでは、フィールドに `n/a` または `blank` を指定して、そのフィールドで情報を使用できないイベントを特定することができます。`!n/a` または `!blank` を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。FireSIGHT システムへの IPv4 および IPv6 のアドレスの入力については、IP アドレスの表記規則（1-23 ページ）を参照してください。
- 特定のデバイス、およびグループ、スタック、またはクラスタ内のデバイスを検索するには、デバイス フィールドを使用します。検索での FireSIGHT システムによるデバイス フィールドの処理方法については、検索でのデバイスの指定（60-7 ページ）を参照してください。
- オブジェクトを検索条件として使用するには、検索フィールドの隣にあるオブジェクトの追加アイコン（ ＋ ）をクリックします。

検索でのオブジェクトの使用など、検索構文の詳細については、イベントの検索（60-1 ページ）を参照してください。

ユーザ アクティビティを検索するには、以下を行います。

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　テーブルのドロップダウン メニューから [User Activity] を選択します。

[User Activity search] ページが表示されます。

ヒント　データベース内で別の種類のイベントを検索するには、テーブルのドロップダウン リストから選択します。

ステップ 3　該当するフィールドに検索基準を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。オブジェクトを検索条件として使用するには、検索フィールドの隣にある追加アイコン（ ＋ ）をクリックします。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　制約された権限を持つカスタム ユーザ ロールの制約として検索を保存する場合は、検索を非公開として保存する**必要があります**。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save As New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

検索結果は、現行の時間範囲によって制約され、デフォルトのユーザ アクティビティ ワークフローに表示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

CHAPTER 51

相関ポリシーおよび相関ルールの設定

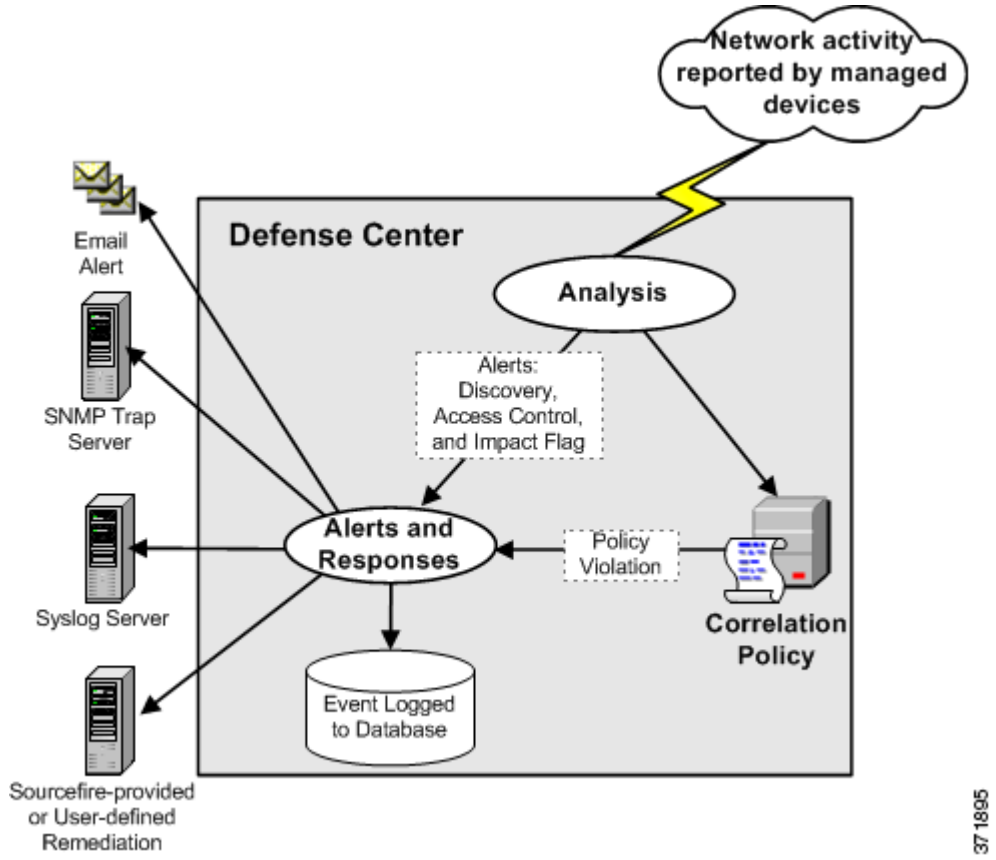
FireSIGHT システムの *相関* 機能を使用すると、*相関ポリシー* を作成し、そこに *相関ルール* と *コンプライアンス ホワイトリスト* を含めることで、ネットワークに対する脅威にリアルタイムで対処できます。ネットワーク上のアクティビティによって相関ルールまたはホワイトリストのいずれかがトリガーとして使用されると、相関 *ポリシー違反* が発生します。

相関ルールがトリガーとして使用されるのは、FireSIGHT システムによって生成された特定のイベントがユーザ指定の基準に一致した場合、あるいは既存のトラフィック プロファイルで特徴付けられる通常のネットワーク トラフィック パターンからネットワーク トラフィックが逸脱した場合です。

一方、コンプライアンス ホワイトリストがトリガーとして使用されるのは、ネットワーク上のホストが、禁止されているオペレーティング システム、クライアント アプリケーション（またはクライアント）、アプリケーション プロトコル、またはプロトコルを実行しているとシステムが判断した場合です。

ポリシー違反への応答を開始するよう、FireSIGHT システムを設定できます。応答には、単純なアラートやさまざまな修正（ホストのスキャンなど）が含まれます。応答をグループ化すると、1 つのポリシー違反に対してシステムに複数の応答を開始させることができます。

以下の図に、イベント通知と相関のプロセスを示します。



この章では、相関ルールの作成方法、相関ルールをポリシーで使用する方法、応答や応答グループを相関ルールに関連付ける方法、および相関イベントを分析する方法について主に説明します。詳細については、以下を参照してください。

- 相関ポリシーのルールの作成（51-3 ページ）
- 相関ポリシーのルールの管理（51-45 ページ）
- 相関応答のグループ化（51-47 ページ）
- 相関ポリシーの作成（51-49 ページ）
- 相関ポリシーの管理（51-54 ページ）
- 相関イベントの操作（51-56 ページ）

コンプライアンス ホワイトリストおよび相関応答（アラートと修正）を作成する方法の詳細については、以下の項を参照してください。

- FireSIGHT システムのコンプライアンス ツールとしての使用（52-1 ページ）
- アラート応答の使用（43-2 ページ）。
- 相関ポリシーおよび相関ルールの設定（51-1 ページ）。

相関ポリシーのルールの作成

ライセンス： FireSIGHT、Protection、URL Filtering、またはMalware

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

相関ポリシーを作成する前に、それに含める相関ルールまたはコンプライアンス ホワイトリスト（あるいはその両方）を作成する必要があります。

注 この項では、相関ルールの作成方法を説明します。コンプライアンス ホワイトリストを作成する方法については、コンプライアンス ホワイト リストの作成（52-9 ページ）を参照してください。

ユーザ指定の基準にネットワーク トラフィックが一致すると相関ルールがトリガーとして使用され、相関イベントが生成されます。相関ルールを作成するときには、単純な条件を使用することも、条件と制約の組み合わせやネストによって複雑な構造を作成することもできます。

さらに、以下の要素を相関ルールに追加することができます。

- *ホスト プロファイル限定* を追加すると、トリガー イベントに関連するホストのプロファイルからの情報に基づいてルールを制約できます。
- *接続トラッカー* を相関ルールに追加すると、ルールの初期基準に一致した場合、システムは特定の接続を追跡し始めます。その後、追跡対象の接続がさらに追加の基準を満たす場合にのみ、相関イベントが生成されます。
- *ユーザ限定* を相関ルールに追加すると、特定のユーザまたはユーザ グループを追跡します。たとえば、送信元または宛先ユーザのアイデンティティが特定のユーザである場合、または特定の部門（マーケティング部門など）のユーザである場合にのみトリガーとして使用するよう、相関ルールを制約できます。
- *スヌーズ期間* および *非アクティブ期間* を追加できます。スヌーズ期間で時間間隔を指定すると、相関ルールが一度トリガーとして使用された後、その時間間隔内にルール違反が再び発生しても、ルールが再びトリガーとして使用されることはありません。スヌーズ期間が経過すると、ルールは再びトリガー可能になります（そして新しいスヌーズ期間が始まります）。非アクティブ期間中は、相関ルールはトリガーとして使用されません。

注意 頻繁に発生するイベントによってトリガーとして使用される複雑な相関ルールを評価することにより、Defense Centerのパフォーマンスが低下する可能性があります。たとえば、システムで記録されるすべての接続に対して、複数の条件からなるルールを Defense Center が評価しなければならない場合、リソースが過負荷になる可能性があります。

次の表は、効果的な相関ルールを作成するために必要となるライセンスを示しています。該当するライセンスがない場合、ライセンス供与されていない FireSIGHT システム機能を使用する相関ルールはトリガーとして使用されません。特定のライセンスの詳細については、サービス サブスクリプション（65-8 ページ）を参照してください。

表 51-1　相関ルールを作成するためのライセンス要件

目的	必要なライセンス
侵入イベントまたはセキュリティ インテリジェンス イベントによって相関ルールをトリガーとして使用する	Protection
ディスカバリ イベント、ホスト入力イベント、位置情報データ、またはユーザ アクティビティによって相関イベントをトリガーとして使用する、またはホスト プロファイルやユーザ限定を相関ルールに追加する	FireSIGHT
接続イベントまたはエンドポイント ベースのマルウェア イベントによって相関イベントをトリガーとして使用する、または接続トラッカーをルールに追加する	いずれか
URL データを使用して接続イベントによって相関ルールをトリガーとして使用する、または URL データを使用して接続トラッカーを作成する シリーズ 2 デバイスと DC500 Defense Centerはどちらも、カテゴリまたはレピュテーションによる URL フィルタリングをサポートしていません。また、シリーズ 2 デバイスはリテラル URL または URL グループによる URL フィルタリングをサポートしていません。	URL Filtering
ネットワークベースのマルウェア データまたはレトロスペクティブなネットワークベースのマルウェア データに基づいて相関ルールをトリガーとして使用する シリーズ 2 および Cisco NGIPS for Blue Coat X-Series デバイスと DC500 Defense Center は、ネットワークベースのマルウェア防御をサポートしていないことに注意してください。	Malware

相関ルール トリガー基準、ホスト プロファイル限定、ユーザ限定、または接続トラッカーを作成するときの構文はそれぞれに異なりますが、メカニズムはすべて同じです。詳細については、ルールの作成メカニズムについて（51-37 ページ）を参照してください。

相関ルールを作成する方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Policies] > [Correlation] を選択し、[Rule Management] タブを選択します。

[Rule Management] ページが表示されます。

ステップ 2　[Create Rule] をクリックします。

[Create Rule] ページが表示されます。

ステップ 3　ルールの基本情報（ルールの名前、説明、グループなど）を指定します。

ルールの基本情報の指定（51-5 ページ）を参照してください。

ステップ 4　ルールをトリガーとして使用させる基本的な基準を指定します。

相関ルール トリガー条件の指定（51-5 ページ）を参照してください。

ステップ 5　オプションで、ホスト プロファイル限定をルールに追加します。

ホスト プロファイル限定の追加（51-20 ページ）を参照してください。

ステップ 6　オプションで、接続トラッカーをルールに追加します。

経時的な接続データを使用した相関ルールの制約（51-24 ページ）を参照してください。

ステップ 7　オプションで、ユーザ限定をルールに追加します。

ユーザ限定の追加（51-34 ページ）を参照してください。

ステップ 8　オプションで、非アクティブ期間またはスヌーズ期間（あるいはその両方）をルールに追加します。

スヌーズ期間および非アクティブ期間の追加（51-36 ページ）を参照してください。

ステップ 9　[Save Rule] をクリックします。

ルールが保存されます。こうして作成したルールを相関ポリシーの中で使用することも、同じイベント タイプによってトリガーとして使用される他の相関ルールの中で使用することもできます。

ルールの基本情報の指定

ライセンス： すべて

それぞれの相関ルールの名前を入力する必要があり、オプションで簡単な説明を入力できます。また、ルールをルール グループに含めることもできます。

ルールの基本情報を指定する方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Policies] > [Correlation] を選択し、[Rule Management] タブを選択します。

[Rule Management] ページが表示されます。

ステップ 2　[Create Rule] をクリックします。

[Create Rule] ページが表示されます。

ステップ 3　[Create Rule] ページの [Rule Name] フィールドに、ルールの名前を入力します。

ステップ 4　[Rule Description] フィールドに、ルールの説明を入力します。

ステップ 5　オプションで、[Rule Group] ドロップダウンリストからルールのグループを選択します。

ルール グループの詳細については、相関ポリシーのルールの管理（51-45 ページ）を参照してください。

ステップ 6　次の項（相関ルール トリガー条件の指定）の手順に進みます。

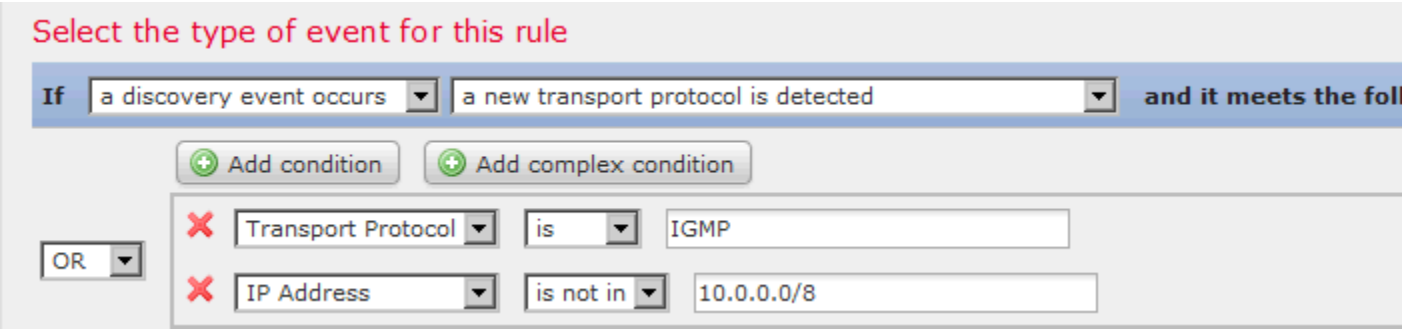
相関ルール トリガー条件の指定

ライセンス： 機能によって異なる

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

単純な相関ルールでは、特定のタイプのイベントが発生することだけを指定します。より具体的な条件を指定する必要はありません。たとえば、トラフィック プロファイル変化に基づく相関ルールでは、条件を指定する必要はまったくありません。一方、複数の条件がネストされた複雑な相関ルールにすることもできます。たとえば、以下の図に示すルールは、10.x.x.x サブネットに含まれない IP アドレスから IGMP メッセージが送信された場合にルールをトリガーとして使用するという基準で構成されています。



注　イベントに基づく条件を作成するときに、相関ルール トリガー基準を追加できるのは、デバイスがその条件に必要な情報を収集でき、しかも Defense Center でその情報を管理できる場合に限られます。たとえば、シリーズ 2 デバイスと DC500 Defense Center はいずれも SSL インスペクション、カテゴリまたはレピュテーション別の URL フィルタリング、またはセキュリティ インテリジェンスをサポートしないので、それらの機能に基づいてそれらのアプライアンスでイベント条件を設定することはできません。詳細については、相関ポリシーのルールの作成（51-3 ページ）を参照してください。

相関ルール トリガー基準を指定する方法：

アクセス： Admin/Discovery Admin

ステップ 1　ルールの基礎となるイベントのタイプを選択します。

相関ルールを作成するときは、まず始めに、ルールの基礎となるイベントのタイプを選択する必要があります。[Select the type of event for this rule] の下には、次のオプションがあります。

- 特定の侵入イベントが発生したときにルールをトリガーとして使用する場合は、[an intrusion event occurs] を選択します。
- 特定のマルウェア イベントが発生したときにルールをトリガーとして使用する場合は、[a Malware event occurs] を選択します。
- 特定のディスカバリ イベントが発生したときにルールをトリガーとして使用する場合は、[a discovery event occurs] を選択します。また、ディスカバリ イベントによって相関ルールをトリガーとして使用する場合は、使用するイベントのタイプを選択する必要もあります。ディスカバリ イベントのタイプについて（50-10 ページ）で説明されているディスカバリ イベントのサブセットから選択可能です（たとえばホップ変更によって相関ルールをトリガーとして使用することはできません）。ただし、[there is any type of event] を選択すると、あらゆるタイプのディスカバリ イベントの発生時にルールをトリガーできます。
- 新しいユーザが検出されたとき、またはユーザがホストにログインしたときにルールをトリガーとして使用する場合は、[user activity is detected] を選択します。
- 特定のホスト入力イベントが発生したときにルールをトリガーとして使用する場合は、[a host input event occurs] を選択します。また、ホスト入力イベントによって相関ルールをトリガーとして使用する場合は、使用するイベントのタイプを選択する必要もあります。ホスト入力イベントのタイプについて（50-14 ページ）で説明されているイベントのサブセットから選択可能です。
- 接続データが特定の基準を満たすときにルールをトリガーとして使用する場合は、[a connection event occurs] を選択します。また、接続イベントによって相関ルールをトリガーとして使用する場合には、接続の開始または終了だけを表す接続イベントを使用するのか、それとも両者のいずれも表す接続イベントを使用するのかを選択する必要もあります。

- 既存のトラフィック プロファイルで特徴付けられた通常のネットワーク トラフィック パターンからネットワーク トラフィックが逸脱したときに相関ルールをトリガーとして使用する場合は、[a traffic profile changes] を選択します。

ステップ 2　ルールの条件を指定します。

相関ルール トリガー基準の条件で使用できる構文は、ステップ 1 で選択した基本イベントにより異なりますが、メカニズムは同じです。詳細については、ルールの作成メカニズムについて（51-37 ページ）を参照してください。

条件を作成するために使用できる構文については、以下の項で説明します。

- 侵入イベントの構文（51-7 ページ）
- マルウェア イベントの構文（51-10 ページ）
- ディスカバリ イベントの構文（51-11 ページ）
- ユーザ アクティビティ イベントの構文（51-14 ページ）
- ホスト入力イベントの構文（51-14 ページ）
- 接続イベントの構文（51-16 ページ）
- トラフィック プロファイル変化の構文（51-18 ページ）

ヒント　ステップ 1 で指定した同じ基本イベント タイプを共有する複数のルールをネストさせることができます。たとえば、オープン TCP ポートの検出に基づく新しいルールを作成する場合、その新規ルールのトリガー基準に [rule “MyDoom Worm” is true] および [rule “Kazaa (TCP) P2P” is true] を含めることができます。

ステップ 3　オプションで、以下の項の手順に進みます。

- ホスト プロファイル限定の追加（51-20 ページ）
- 経時的な接続データを使用した相関ルールの制約（51-24 ページ）
- ユーザ限定の追加（51-34 ページ）
- スヌーズ期間および非アクティブ期間の追加（51-36 ページ）

相関ルールの作成が終了した場合は、相関ポリシーのルールの作成（51-3 ページ）で説明している手順のステップ 9 に進んでルールを保存します。

侵入イベントの構文

ライセンス： Protection

侵入イベントを基本イベントとして選択した場合、次の表で説明する方法に従って相関ルールの条件を作成します。

ルール条件を作成するときには、ネットワーク トラフィックによってルールをトリガーできることを確認してください。個々の侵入イベントで使用可能な情報は、検出方法やロギング方法など、いくつかの要因によって異なります。詳細については、侵入イベントについて（41-11 ページ）を参照してください。

表 51-2　侵入イベントの構文

指定する項目	演算子を指定した後に行う操作
Access Control Policy	侵入イベントを生成した侵入ポリシーを使用するアクセス コントロール ポリシーを 1 つ以上選択します。
Access Control Rule Name	侵入イベントを生成した侵入ポリシーを使用するアクセス コントロール ルールの名前全体またはその一部を入力します。
アプリケーション プロトコル	侵入イベントに関連付けられたアプリケーション プロトコルを 1 つ以上選択します。
Application Protocol Category	アプリケーション プロトコルのカテゴリを 1 つ以上選択します。
分類	1 つ以上の分類を選択します。
クライアント	侵入イベントに関連付けられたクライアントを 1 つ以上選択します。
Client Category	クライアントのカテゴリを 1 つ以上選択します。
Destination Country または Source Country	侵入イベントの送信元または宛先 IP アドレスに関連付けられた国を 1 つ以上選択します。
Destination IP、Source IP、または Source/Destination IP	単一の IP アドレスまたはアドレス ブロックを指定します。FireSIGHT システムで使用する IP アドレス表記およびプレフィクス長については、IP アドレスの表記規則（1-23 ページ）を参照してください。
Destination Port/ICMP Code または Source Port/ICMP Type	送信元トラフィックのポート番号または ICMP タイプ、あるいは宛先トラフィックのポート番号または ICMP タイプを入力します。
デバイス	イベントを生成した可能性があるデバイスを 1 つ以上選択します。
Egress Interface または Ingress Interface	インターフェイスを 1 つ以上選択します。
Egress Security Zone または Ingress Security Zone	セキュリティ ゾーンを 1 つ以上選択します。
Generator ID	プリプロセッサを 1 つ以上選択します。使用可能なプリプロセッサの詳細については、ネットワーク分析ポリシーでのプリプロセッサの設定（26-7 ページ）を参照してください。
Impact Flag	侵入イベントに割り当てられる影響レベルを選択します。`is`、`is not`、`is greater than` などを指定する演算子と一緒に、以下のいずれかを選択します。 • 0：グレー（不明） • 1：レッド（脆弱） • 2：オレンジ（脆弱の可能性あり） • 3：イエロー（現在は脆弱でない） • 4：ブルー（不明なターゲット） **注**　NetFlow データに基づいてネットワーク マップに追加されたホストに関して使用可能なオペレーティング システム情報はありません。そのため、ホスト入力機能を使って手動でホスト オペレーティング システム アイデンティティを設定しない限り、Defense Centerは、これらのホストが関与する侵入イベントに「脆弱」（レベル 1：レッド）影響レベルを割り当てることができません。 詳細については、影響レベルを使用してイベントを評価する（41-39 ページ）を参照してください。

表 51-2　侵入イベントの構文（続き）

指定する項目	演算子を指定した後に行う操作
Inline Result	次のいずれかを選択します。 • dropped は、インライン型、スイッチ型、またはルーティング型展開でパケットがドロップされたかどうかを示します。 • would have dropped は仮定を表します。インライン型、スイッチ型、またはルーティング型展開でパケットをドロップするよう侵入ポリシーが設定されていると仮定した場合、パケットがドロップされるかどうかを示します。 侵入ポリシーのドロップ動作やルール状態とは無関係に、パッシブ展開（インライン セットがタップ モードである場合を含む）ではシステムがパケットをドロップしないことに注意してください。
Intrusion Policy	侵入イベントを生成した侵入ポリシーを 1 つ以上選択します。
IOC Tag	侵入イベントの結果として IOC タグが設定されているか（`is`）、または設定されていないか（`is not`）を選択します。
プライオリティ	ルールのプライオリティとして、**low**、**medium** または **high** のいずれかを選択します。 ルール ベースの侵入イベントの場合、プライオリティは `priority` キーワードまたは `classtype` キーワードのいずれかの値に対応します。その他の侵入イベントの場合、プライオリティはデコーダまたはプリプロセッサによって決定されます。
Protocol	トランスポート プロトコルの名前または番号を入力します。プロトコル番号は、http://www.iana.org/assignments/protocol-numbers.
Rule Message	ルール メッセージ全体またはその一部を入力します。
Rule SID	単一の Snort ID 番号（SID）またはカンマで区切った複数の SID を入力します。 **注**　演算子として [is in] または [is not in] を選択する場合、複数選択ポップアップ ウィンドウを使用することはできません。複数 SID のカンマ区切りリストを入力する必要があります。
ルール タイプ	ルールがローカルか、ローカルでないかを指定します。ローカル ルールには、カスタマイズされた標準テキスト侵入ルール、ユーザが変更した標準テキスト ルール、見出し情報を変更してルールを保存するときに作成されるshared object ruleの新規インスタンスが含まれます。詳細については、既存のルールの変更（36-111 ページ）を参照してください。
SSL Actual Action	システムが暗号化された接続をどのように処理したかを示す SSL ルール アクションを選択します。
SSL Certificate Fingerprint	トラフィックの暗号化に使用された証明書のフィンガープリントを入力するか、フィンガープリントに関連付けられたサブジェクトの共通名を選択します。
SSL Certificate Subject Common Name (CN)	セッションの暗号化に使用された証明書のサブジェクト共通名またはその一部を入力します。
SSL Certificate Subject Country (C)	セッションの暗号化に使用された証明書のサブジェクト国別コードを 1 つ以上選択します。
SSL Certificate Subject Organization (O)	セッションの暗号化に使用された証明書のサブジェクト組織名またはその一部を入力します。
SSL Certificate Subject Organizational Unit (OU)	セッションの暗号化に使用された証明書のサブジェクト組織単位名またはその一部を入力します。
SSL Flow Status	システムによるトラフィック復号化試行の結果に基づく 1 つ以上のステータスを選択します。

表 51-2　侵入イベントの構文（続き）

指定する項目	演算子を指定した後に行う操作
[Username]	侵入イベントで送信元ホストにログインしたユーザを示すユーザ名を入力します。
VLAN ID	侵入イベントをトリガーとして使用したパケットに関連付けられた最も内側の VLAN ID を入力します。
Web アプリケーション	侵入イベントに関連付けられた Web アプリケーションを 1 つ以上選択します。
Web Application Category	Web アプリケーションのカテゴリを 1 つ以上選択します。

マルウェア イベントの構文

ライセンス： すべてまたは Malware

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

マルウェア イベントに基づく相関ルール条件の構文は、イベントがエンドポイント ベースのマルウェア エージェントによって報告されるのか、管理対象デバイスによって検出されるのか、または管理対象デバイスによって検出されレトロスペクティブにマルウェアとして識別されるのかによって異なります。

シリーズ 2 および Cisco NGIPS for Blue Coat X-Series デバイスと DC500 Defense Center はネットワークベースのマルウェア防御をサポートしていないので、これらのアプライアンスは、ネットワークベースのマルウェア データまたはレトロスペクティブなネットワークベースのマルウェア データに基づくマルウェア イベントによる相関ルール トリガーをサポートしないことに注意してください。

ルール条件を作成するときには、ネットワーク トラフィックによってルールをトリガーできることを確認してください。個々の接続イベントまたは接続サマリー イベントで使用可能な情報は、検出方法、ロギング方法、イベント タイプなど、いくつかの要因により異なります。詳細については、マルウェア イベント テーブルについて（40-21 ページ）を参照してください。

マルウェアを基本イベントとして選択した場合、次の表で説明する方法に従って相関ルールの条件を作成します。

表 51-3　マルウェア イベントの構文

指定する項目	演算子を指定した後に行う操作
アプリケーション プロトコル	マルウェア イベントに関連付けられたアプリケーション プロトコルを 1 つ以上選択します。
Application Protocol Category	アプリケーション プロトコルのカテゴリを 1 つ以上選択します。
クライアント	マルウェア イベントに関連付けられたクライアントを 1 つ以上選択します。
Client Category	クライアントのカテゴリを 1 つ以上選択します。
Destination Country または Source Country	マルウェア イベントの送信元または宛先 IP アドレスに関連付けられた国を 1 つ以上選択します。
Destination IP、Host IP、または Source IP	単一の IP アドレスまたはアドレス ブロックを指定します。FireSIGHT システムで使用する IP アドレス表記については、IP アドレスの表記規則（1-23 ページ）を参照してください。
Destination Port/ICMP Code	宛先トラフィックのポート番号または ICMP コードを入力します。

表 51-3　マルウェア イベントの構文（続き）

指定する項目	演算子を指定した後に行う操作
処理	Malware または Custom Detection、あるいはその両方を選択します。
イベント タイプ	マルウェア イベントに関連付けられたエンドポイント ベースのイベント タイプを 1 つ以上選択します。詳細については、マルウェア イベントのタイプ（40-27 ページ）を参照してください。
File Name	ファイルの名前を入力します。
File Type	ファイルのタイプを選択します（たとえば PDF、MSEXE など）。
File Type Category	ファイル タイプのカテゴリを 1 つ以上選択します（たとえば Office Documents、Executables など）。
IOC Tag	マルウェア イベントの結果として IOC タブが設定されているか（is）、または設定されていないか（is not）を選択します。
SHA-256	ファイルの SHA-256 ハッシュ値を入力するか、貼り付けます。
SSL Actual Action	システムが暗号化された接続をどのように処理したかを示す SSL ルール アクションを選択します。
SSL Certificate Fingerprint	トラフィックの暗号化に使用された証明書のフィンガープリントを入力するか、フィンガープリントに関連付けられたサブジェクトの共通名を選択します。
SSL Certificate Subject Common Name (CN)	セッションの暗号化に使用された証明書のサブジェクト共通名またはその一部を入力します。
SSL Certificate Subject Country (C)	セッションの暗号化に使用された証明書のサブジェクト国別コードを 1 つ以上選択します。
SSL Certificate Subject Organization (O)	セッションの暗号化に使用された証明書のサブジェクト組織名またはその一部を入力します。
SSL Certificate Subject Organizational Unit (OU)	セッションの暗号化に使用された証明書のサブジェクト組織単位名またはその一部を入力します。
SSL Flow Status	システムによるトラフィック復号化試行の結果に基づく 1 つ以上のステータスを選択します。
Source Port/ICMP Type	送信元トラフィックのポート番号または ICMP タイプを入力します。
Web アプリケーション	マルウェア イベントに関連付けられた Web アプリケーションを 1 つ以上選択します。
Web Application Category	Web アプリケーションのカテゴリを 1 つ以上選択します。

ディスカバリ イベントの構文

ライセンス： FireSIGHT

ディスカバリ イベントに基づく相関ルールにする場合は、まず、使用するイベントのタイプをドロップダウンリストから選択する必要があります。次の表に、トリガー基準としてドロップダウンリストから選択できるイベントをリストし、対応するイベント タイプを示します。ディスカバリ イベント タイプの詳細については、ディスカバリ イベントのタイプについて（50-10 ページ）を参照してください。

表 51-4　相関ルールのトリガー条件とディスカバリ イベント タイプ

選択するオプション	ルールをトリガーとして使用するイベント タイプ
a client has changed	クライアント更新
a client timed out	クライアント タイムアウト
a host IP address is reused	DHCP:IP アドレスの再割り当て
a host is deleted because the host limit was reached	ホスト削除:ホスト制限に到達
a host is identified as a network device	ネットワーク デバイスへのホスト タイプの変更
a host timed out	ホスト タイムアウト
a host's IP address has changed	DHCP:IP アドレスの変更
a NETBIOS name change is detected	NetBIOS 名の変更
a new client is detected	新しいクライアント
a new IP host is detected	新しいホスト
a new MAC address is detected	ホストの追加 MAC の検出
a new MAC host is detected	新しいホスト
a new network protocol is detected	新しいネットワーク プロトコル
a new transport protocol is detected	新しいトランスポート プロトコル
a TCP port closed	TCP ポート クローズ
a TCP port timed out	TCP ポート タイムアウト
a UDP port closed	UDP ポート クローズ
a UDP port timed out	UDP ポート タイムアウト
a VLAN tag was updated	VLAN タグ情報の更新
an IOC was set	侵害の兆候
an open TCP port is detected	新しい TCP ポート
an open UDP port is detected	新しい UDP ポート
the OS information for a host has changed	新しい OS
the OS or server identity for a host has a conflict	アイデンティティ競合
the OS or server identity for a host has timed out	アイデンティティ タイムアウト
there is any kind of event	(任意のイベント タイプ)
there is new information about a MAC address	MAC 情報の変更
there is new information about a TCP server	TCP サーバ情報の更新
there is new information about a UDP server	UDP サーバ情報の更新

ホップ変更によって相関ルールをトリガーとして使用したり、ライセンス ホスト制限到達のためにシステムが新しいホストをドロップした時点で相関ルールをトリガーとして使用したりすることはできません。ただし、[there is any type of event] を選択することで、任意のタイプのディスカバリ イベントの発生時にルールをトリガーできます。

ディスカバリ イベントのタイプを選択した後、以下の表で説明されているように相関ルールの条件を作成できます。選択したイベント タイプに応じて、以下の表に示す基準のサブセットを使用して条件を作成できます。たとえば、新しいクライアントの検出時に相関ルールをトリガーとして使用する場合、ホストの IP または MAC アドレス、クライアントの名前、タイプ、バージョン、およびイベントを検出したデバイスに基づいて条件を作成できます。

表 51-5　ディスカバリ イベントの構文

指定する項目	演算子を指定した後に行う操作
Application Protocol	アプリケーション プロトコルを 1 つ以上選択します。
Application Protocol Category	アプリケーション プロトコルのカテゴリを 1 つ以上選択します。
Application Port	アプリケーション プロトコルのポート番号を入力します。
Client	クライアントを 1 つ以上選択します。
Client Category	クライアントのカテゴリを 1 つ以上選択します。
Client Version	クライアントのバージョン番号を入力します。
デバイス	ディスカバリ イベントを生成した可能性があるデバイスを 1 つ以上選択します。
ハードウェア	モバイル デバイスのハードウェア モデルを入力します。たとえば、すべての Apple iPhone に一致させるには `iPhone` と入力します。
Host Type	ドロップダウン リストから 1 つ以上のホスト タイプを選択します。ホスト、またはいずれかのタイプのネットワーク デバイスを選択できます。
IP Address または New IP Address	単一の IP アドレスまたはアドレス ブロックを入力します。FireSIGHT システムで使用する IP アドレス表記については、IP アドレスの表記規則（1-23 ページ）を参照してください。
Jailbroken	イベントのホストがジェイルブレイクされたモバイル デバイスであることを示すには [Yes] を、そうでない場合は [No] を選択します。
MAC アドレス	ホストの MAC アドレス全体またはその一部を入力します。 たとえば、特定のハードウェア製造元のデバイスの MAC アドレスが 0A:12:34 で始まることがわかっている場合、演算子として [begins with] を選択し、値として `0A:12:34` を入力できます。
MAC Type	MAC アドレスが ARP/DHCP で検出されたかどうかを選択します。 つまり、MAC アドレスがホストに属していることをシステムが識別したのか（**is ARP/DHCP Detected**）、または、管理対象デバイスとホストの間にルータがあるなどの理由で、その MAC アドレスを持つ多数のホストをシステムが認識しているのか（**is not ARP/DHCP Detected**）を選択します。
MAC Vendor	ディスカバリ イベントをトリガーとして使用したネットワーク トラフィックで使われている NIC の MAC ハードウェア ベンダーの名前またはその一部を入力します。
Mobile	イベントのホストがモバイル デバイスであることを示すには [Yes] を、そうでない場合は [No] を選択します。
NETBIOS Name	ホストの NetBIOS 名を入力します。
Network Protocol	http://www.iana.org/assignments/ethernet-numbers にリストされているネットワーク プロトコル番号を入力します。
OS Name	オペレーティング システムの名前を 1 つ以上選択します。
OS Vendor	オペレーティング システムのベンダーを 1 つ以上選択します。
OS Version	オペレーティング システムのバージョンを 1 つ以上選択します。

表 51-5　ディスカバリ イベントの構文（続き）

指定する項目	演算子を指定した後に行う操作
Protocol または トランスポート プロトコル	トランスポート プロトコルの名前または番号を入力します。プロトコル番号は、http://www.iana.org/assignments/protocol-numbers.
Source	ホスト入力データのソースを選択します（オペレーティング システムとサーバのアイデンティティ変更およびタイムアウトの場合）。
Source Type	ホスト入力データのソースのタイプを選択します（オペレーティング システムとサーバのアイデンティティ変更およびタイムアウトの場合）。
VLAN ID	イベントに関連しているホストの VLAN ID を入力します。
Web Application	Web アプリケーションを選択します。

ユーザ アクティビティ イベントの構文

ライセンス：FireSIGHT

ユーザ アクティビティに基づく相関ルールにする場合は、まず、使用するユーザ アクティビティのタイプをドロップダウンリストから選択する必要があります。

- a user logged into a host（ホストへのユーザ ログイン）または
- a new user identity was detected（新しいユーザ ID の検出）

ユーザ アクティビティのタイプを選択した後、以下の表で説明されているように相関ルールの条件を作成できます。選択したユーザ アクティビティのタイプに応じて、以下の表に示す基準のサブセットを使って条件を作成できます。新しいユーザ ID によってトリガーとして使用される相関ルールでは、IP アドレスを指定できません。

表 51-6　ユーザ アクティビティの構文

指定する項目	演算子を指定した後に行う操作
デバイス	ユーザ アクティビティを検出した可能性のあるデバイスを 1 つ以上選択します。
IP Address	単一の IP アドレスまたはアドレス ブロックを入力します。FireSIGHT システムで使用する IP アドレス表記については、IP アドレスの表記規則（1-23 ページ）を参照してください。
[Username]	ユーザ名を入力します。

ホスト入力イベントの構文

ライセンス：FireSIGHT

ホスト入力イベントに基づく相関ルールにする場合は、まず、使用するホスト入力イベントのタイプをドロップダウンリストから選択する必要があります。次の表に、トリガー基準としてドロップダウンリストから選択できるイベントをリストし、対応するホスト入力イベント タイプを示します。ホスト入力イベント タイプの詳細については、ホスト入力イベントのタイプについて（50-14 ページ）を参照してください。

表 51-7　相関ルールのトリガー条件とホストの入力イベント タイプ

選択するオプション	ルールをトリガーとして使用するイベント タイプ
a client is added	クライアントの追加
a client is deleted	クライアントの削除
a host is added	ホストの追加
a protocol is added	プロトコルの追加
a protocol is deleted	プロトコルの削除
a scan result is added	スキャン結果の追加
a server definition is set	サーバ定義の設定
a server is added	ポートの追加
a server is deleted	ポートの削除
a vulnerability is marked invalid	脆弱性を無効に設定
a vulnerability is marked valid	脆弱性を有効に設定
an address is deleted	ホスト/ネットワークの削除
an attribute value is deleted	ホスト属性値の削除
an attribute value is set	ホスト属性値の設定
an OS definition is set	オペレーティング システム定義の設定
host criticality is set	ホスト重要度の設定

ユーザ定義によるホスト属性定義を追加/削除/変更するとき、あるいは脆弱性の影響限定を設定するときに相関ルールをトリガーとして使用することはできません。

ホスト入力イベントのタイプを選択した後、以下の表で説明されているように相関ルールの条件を作成できます。選択したホスト入力イベント タイプに応じて、以下の表に示す基準のサブセットを使用して条件を作成できます。たとえば、クライアントの削除時に相関ルールをトリガーとして使用する場合、イベントに関連するホストの IP アドレス、削除のソース タイプ（手動、サードパーティ アプリケーション、またはスキャナ）、およびソース自体（特定のスキャナ タイプまたはユーザ）に基づいて条件を作成することができます。

表 51-8　ホスト入力イベントの構文

指定する項目	演算子を指定した後に行う操作
IP Address	単一の IP アドレスまたはアドレス ブロックを入力します。FireSIGHT システムで使用する IP アドレス表記については、IP アドレスの表記規則（1-23 ページ）を参照してください。
Source	ホスト入力データのソースを選択します。
Source Type	ホスト入力データのソースのタイプを選択します。

接続イベントの構文

ライセンス：すべて

接続イベントに基づく相関ルールにする場合には、まず、接続の開始または終了だけを表すイベントを評価するのか、それとも開始/終了のいずれも表すイベントを評価するのかを選択する必要があります。接続イベントのタイプを選択した後、接続イベントの構文 の表で説明されているように相関ルールの条件を作成できます。

ルール条件を作成するときには、ネットワーク トラフィックによってルールをトリガーできることを確認してください。個々の接続イベントまたは接続サマリー イベントで使用可能な情報は、検出方法、ロギング方法、イベント タイプなど、いくつかの要因により異なります。詳細については、接続およびセキュリティ インテリジェンスのイベントで利用可能な情報（39-12 ページ）を参照してください。

表 51-9　　接続イベントの構文

指定する項目	演算子を指定した後に行う操作
Access Control Policy	接続をログに記録したアクセス コントロール ポリシーを 1 つ以上選択します。
Access Control Rule Action	接続をログに記録したアクセス コントロール ルールに関連付けられたアクションを 1 つ以上選択します。 **注**　あとで接続を処理するルール/デフォルト アクションとは無関係に、ネットワーク トラフィックがいずれかのモニタ ルールの条件に一致した場合に相関イベントをトリガーとして使用するには、[Monitor] を選択します。
Access Control Rule Name	接続をログに記録したアクセス コントロール ルールの名前またはその一部を入力します。 **注**　あとで接続を処理したルール/デフォルト アクションとは無関係に、接続と一致した条件を持つモニタ ルールの名前を入力できます。
アプリケーション プロトコル	接続に関連付けられたアプリケーション プロトコルを 1 つ以上選択します。
Application Protocol Category	アプリケーション プロトコルのカテゴリを 1 つ以上選択します。
Client	クライアントを 1 つ以上選択します。
Client Category	クライアントのカテゴリを 1 つ以上選択します。
Client Version	クライアントのバージョン番号を入力します。
Connection Duration	接続イベントの期間（秒数）を入力します。
Connection Type	Cisco の管理対象デバイスによって接続が検出されたかどうか基づいて相関ルールをトリガーとして使用するのか（**FireSIGHT**）、それとも NetFlow 対応デバイスによって接続がエクスポートされたかどうかに基づいて相関ルールをトリガーとして使用するのか（**NetFlow**）を選択します。
Destination Country または Source Country	接続イベントの送信元または宛先 IP アドレスに関連付けられた国を 1 つ以上選択します。
デバイス	接続を検出したデバイスを 1 つ以上選択します。または（NetFlow 対応デバイスによってエクスポートされた接続データの場合）接続を処理したデバイスを 1 つ以上選択します。
Egress Interface または Ingress Interface	インターフェイスを 1 つ以上選択します。
Egress Security Zone または Ingress Security Zone	セキュリティ ゾーンを 1 つ以上選択します。

表 51-9　接続イベントの構文（続き）

指定する項目	演算子を指定した後に行う操作
Initiator Bytes、Responder Bytes、または Total Bytes	以下のいずれかを入力します。 • 送信されたバイト数（[Initiator Bytes]） • 受信されたバイト数（[Responder Bytes]） • 送受信されたバイト数（[Total Bytes]）
Initiator IP、Responder IP、または Initiator/Responder IP	単一の IP アドレスまたはアドレス ブロックを指定します。FireSIGHT システムで使用する IP アドレス表記およびプレフィクス長については、IP アドレスの表記規則（1-23 ページ）を参照してください。
Initiator Packets、Responder Packets、または合計パケット数	以下のいずれかを入力します。 • 送信されたパケット数（[Initiator Packets]） • 受信されたパケット数（[Initiator Packets]） • 送受信されたパケット数（[Total Packets]）
Initiator Port/ICMP Type または Responder Port/ICMP Code	イニシエータ トラフィックのポート番号または ICMP タイプ、あるいはレスポンダ トラフィックのポート番号または ICMP コードを入力します。
IOC Tag	接続イベントの結果として IOC タグが設定されているか（`is`）、または設定されていないか（`is not`）を選択します。
NETBIOS Name	接続におけるモニタ対象ホストの NetBIOS 名を入力します。
NetFlow Device	相関ルールをトリガーとして使用するために使用される接続データをエクスポートした NetFlow 対応デバイスの IP アドレスを選択します。展開環境に NetFlow 対応デバイスをまだ追加していない場合、[NetFlow Device] ドロップダウンリストは空白になります。
理由	接続イベントに関連付けられた理由を 1 つ以上選択します。
Security Intelligence Category	接続イベントに関連付けられたセキュリティ インテリジェンスのカテゴリを 1 つ以上選択します。 **注**　接続終了イベントの条件としてセキュリティ インテリジェンス カテゴリを使用するには、アクセス コントロール ポリシーの [Security Intelligence] セクションで、その条件を [Block] ではなく [Monitor] に設定する必要があります。詳細については、セキュリティ インテリジェンスのホワイトリストおよびブラックリストの作成（13-4 ページ）を参照してください。
SSL Actual Action	システムが暗号化された接続をどのように処理したかを示す SSL ルール アクションを選択します。
SSL Certificate Fingerprint	トラフィックの暗号化に使用された証明書のフィンガープリントを入力するか、フィンガープリントに関連付けられたサブジェクトの共通名を選択します。
SSL Certificate Status	セッションの暗号化に使用された証明書に関連付けられたステータスを 1 つ以上選択します。
SSL Certificate Subject Common Name (CN)	セッションの暗号化に使用された証明書のサブジェクト共通名またはその一部を入力します。
SSL Certificate Subject Country (C)	セッションの暗号化に使用された証明書のサブジェクト国別コードを 1 つ以上選択します。
SSL Certificate Subject Organization (O)	セッションの暗号化に使用された証明書のサブジェクト組織名またはその一部を入力します。

表 51-9　接続イベントの構文(続き)

指定する項目	演算子を指定した後に行う操作
SSL Certificate Subject Organizational Unit (OU)	セッションの暗号化に使用された証明書のサブジェクト組織単位名またはその一部を入力します。
SSL Cipher Suite	セッションの暗号化に使用された暗号スイートを 1 つ以上選択します。
SSL Encrypted Session	[Successfully Decrypted] を選択します。
SSL Flow Status	システムによるトラフィック復号化試行の結果に基づく 1 つ以上のステータスを選択します。
SSL Policy	暗号化接続をログに記録した SSL ポリシーを 1 つ以上選択します。
SSL Rule Name	暗号化接続をログに記録した SSL ルールの名前またはその一部を入力します。
SSL Server Name	クライアントが暗号化接続を確立した相手のサーバーの名前、またはその一部を入力します。
SSL URL Category	暗号化接続でアクセスされた URL のカテゴリを 1 つ以上選択します。
SSL Version	セッションの暗号化に使用された SSL または TLS のバージョンを 1 つ以上選択します。
TCP Flags	相関ルールをトリガーとして使用するために接続イベントに含まれていなければならない TCP フラグを選択します。 **注**　TCP フラグが含まれるのは、NetFlow 対応デバイスによってエクスポートされた接続データのみです。
トランスポート プロトコル	接続で使用されたトランスポート プロトコル(TCP または UDP)を入力します。
URL	接続でアクセスされた URL 全体、またはその一部を入力します。
URL カテゴリ	接続でアクセスされた URL のカテゴリを 1 つ以上選択します。
URL Reputation	接続でアクセスされた URL のレピュテーション値を 1 つ以上選択します。
[Username]	この接続でいずれかのホストにログインしたユーザを示すユーザ名を入力します。
Web Application	接続に関連付けられた Web アプリケーションを 1 つ以上選択します。
Web Application Category	Web アプリケーションのカテゴリを 1 つ以上選択します。

トラフィック プロファイル変化の構文

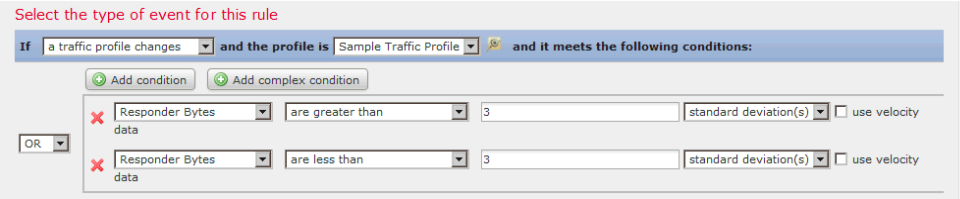
ライセンス: すべて

トラフィック プロファイル変化に基づく相関ルールの場合、既存のトラフィック プロファイルで特徴付けられた通常のネットワーク トラフィック パターンからネットワーク トラフィックが逸脱したときに、ルールがトリガーとして使用されます。トラフィック プロファイルを作成する方法については、トラフィック プロファイルの作成(53-1 ページ)を参照してください。

raw データ、またはデータから計算された統計情報のいずれかに基づいてルールをトリガーできます。たとえば、ネットワーク内を移動するデータ量(バイト数で測定)が急激に変化した場合、攻撃または他のセキュリティー ポリシー違反が発生した可能性がありますが、そのような変動時にトリガーとして使用されるルールを作成できます。以下のいずかの場合にトリガーとして使用されるよう、ルールを指定できます。

- ネットワーク内を移動するバイト数が、平均トラフィック量より上または下の特定数の標準偏差を超えて急激に変化した場合

ネットワーク内を移動するバイト数が、特定数の標準偏差からなる範囲を（上または下に）超えたときにトリガーとして使用されるルールを作成するには、次の図に示すように、上限と下限を指定する必要があります。



移動するバイト数が、平均を基準とした特定数の標準偏差の**上側**を超えた場合にトリガーとして使用されるルールを作成するには、以下の図に示されている最初の条件だけを使用します。

移動するバイト数が、平均を基準とした特定数の標準偏差の**上側**を超えた場合にトリガーとして使用されるルールを作成するには、以下の図に示されている最初の条件だけを使用します。

- ネットワーク内を移動するバイト数が特定のバイト数を上回る場合

[use velocity data] チェック ボックスを選択すると（グラフ タイプの変更（39-18 ページ）を参照）、データ ポイント間の速度変化に基づいて相関ルールをトリガーできます。上記の例で仮に速度データを使用する場合は、次のいずれかの時点でルールがトリガーとして使用されるように指定できます。

- ネットワーク内を移動するバイト数の変化が、平均変化率より上または下の特定数の標準偏差を超えた場合
- ネットワーク内を移動するバイト数の変化が、特定のバイト数を上回った場合

トラフィック プロファイル変化を基準イベントとして選択した場合、以下の表で説明する方法に従って相関ルールの条件を作成します。NetFlow 対応デバイスによってエクスポートされる接続データをトラフィック プロファイルで使用する場合は、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照して、トラフィック プロファイルの作成に使われるデータが、検出方法に応じてどのように異なるかを確認してください。

表 51-10　　トラフィック プロファイル変化の構文

指定する項目	演算子を指定した後に入力する内容	その後、さらに次のいずれかを選択
Number of Connections	検出された接続の合計数 **または** 平均より上または下の標準偏差の数（検出された接続数がこれを超えるとルールがトリガーとして使用されます）	接続 standard deviation(s)：標準偏差の数
Total Bytes、Initiator Bytes、または Responder Bytes	次のいずれかを入力します。 • 送信された合計バイト数（[Total Bytes]） • イニシエータから送信されたバイト数（[Initiator Bytes]） • レスポンダで受信されたバイト数（[Responder Bytes]） **または** 平均より上または下の標準偏差の数（検出された接続数がこれを超えるとルールがトリガーとして使用されます）	bytes standard deviation(s)：標準偏差の数

表 51-10　トラフィック プロファイル変化の構文（続き）

指定する項目	演算子を指定した後に入力する内容	その後、さらに次のいずれかを選択
Total Packets、Initiator Packets、または Responder Packets	次のいずれかを入力します。 • 送信された合計パケット数（[Total Packets]） • イニシエータから送信されたパケット数（[Initiator Packets]） • レスポンダで受信されたパケット数（[Responder Packets]） **または** 平均より上または下の標準偏差の数（上記のいずれかの基準がこれを超えると、ルールがトリガーとして使用されます）	パケット standard deviation(s): 標準偏差の数
Unique Initiators	セッションを開始した個別のホストの数 **または** 平均より上または下の標準偏差の数（検出された接続数がこれを超えるとルールがトリガーとして使用されます）	initiators: イニシエータ数 standard deviation(s): 標準偏差の数
Unique Responders	セッションに応答した個別のホストの数 **または** 平均より上または下の標準偏差の数（検出された接続数がこれを超えるとルールがトリガーとして使用されます）	responders: レスポンダ数 standard deviation(s): 標準偏差の数

ホスト プロファイル限定の追加

ライセンス: FireSIGHT

接続、侵入、ディスカバリ、ユーザ アクティビティ、またはホスト入力のいずれかのイベントを使用して相関ルールをトリガーとして使用する場合、イベントに関連するホストのプロファイルに基づいてルールを制約することができます。この制約は、*ホスト プロファイル限定* と呼ばれます。

注　マルウェア イベント、トラフィック プロファイル変化、または新しい IP ホスト検出によってトリガーとして使用される相関ルールに、ホスト プロファイル限定を追加することは**できません**。

たとえば、ルールの作成対象となる脆弱性がMicrosoft Windows コンピュータにのみ存在するため、Microsoft Windows ホストが有害トラフィックのターゲットとなっている場合にのみ相関ルールをトリガーとして使用するよう、制約することができます。別の例として、ホストがホワイトリストに準拠していない場合にのみ相関ルールがトリガーとして使用されるよう、制約することもできます。

暗黙的（または汎用の）クライアントを照合するには、クライアントに応答するサーバーで使われるアプリケーション プロトコルに基づいてホスト プロファイル限定を作成します。接続のイニシエータ（または送信元）として機能するホスト上のクライアント リストに含まれるアプリケーション プロトコル名の後に**クライアント**が続いている場合、そのクライアントは実際には暗黙的クライアントである可能性があります。つまり、検出されたクライアント トラフィックに基づいてではなく、そのクライアントのアプリケーション プロトコルを使用するサーバー応答トラフィックに基づいて、システムがそのクライアントを報告します。

たとえば、ホストのクライアントとして **HTTPS クライアント**がシステムにより報告される場合、[Application Protocol] を [HTTPS] に設定した**レスポンダ ホスト**または**宛先ホスト**のホスト プロファイル限定を作成します。これは、レスポンダまたは宛先ホストから送られる HTTPS サーバ応答トラフィックに基づいて **HTTPS クライアント**が汎用クライアントとして報告されるためです。

ホスト プロファイル限定を使用するには、そのホストがネットワーク マップに存在すること、および限定として使用するホスト プロファイル プロパティがホスト プロファイルにすでに含まれていることが必要です。たとえば、Windows を実行するホストでの侵入イベントが生成されると相関ルールがトリガーとして使用されるよう設定した場合、そのルールがトリガーとして使用されるのは、侵入イベント生成時にホストがすでに Windows として識別されている場合だけです。

ホスト プロファイル限定を追加する方法:

アクセス: Admin/Discovery Admin

ステップ 1　[Policies] > [Correlation] を選択し、[Rule Management] タブを選択します。

[Rule Management] ページが表示されます。

ステップ 2　[Create Rule] をクリックします。

[Create Rule] ページが表示されます。

ステップ 3　[Create Rule] ページで、[Add Host Profile Qualification] をクリックします。

[Host Profile Qualification] セクションが表示されます。

ヒント　ホスト プロファイル限定を削除するには、[Remove Host Profile Qualification] をクリックします。

ステップ 4　ホスト プロファイル限定の条件を作成します。

1 つの単純な条件を作成することも、複数の条件の組み合わせやネストを使って複雑な構造を作成することもできます。Web インターフェイスを使用して条件を作成する方法については、ルールの作成メカニズムについて（51-37 ページ）を参照してください。

条件を作成するために使用できる構文については、ホスト プロファイル限定の構文（51-21 ページ）で説明しています。

ステップ 5　オプションで、以下の項の手順に進みます。

- 経時的な接続データを使用した相関ルールの制約（51-24 ページ）
- ユーザ限定の追加（51-34 ページ）
- スヌーズ期間および非アクティブ期間の追加（51-36 ページ）

相関ルールの作成が終了した場合は、相関ポリシーのルールの作成（51-3 ページ）で説明している手順のステップ 9 に進んでルールを保存します。

ホスト プロファイル限定の構文

ライセンス: FireSIGHT

ホスト プロファイル限定の条件を作成するときには、まず、相関ルールを制約するために使用するホストを選択する必要があります。選択できるホストは、ルールをトリガーとして使用するために使われるイベントのタイプに応じて次のように異なります。

- 接続イベントを使用する場合は、応答側を示す [Responder Host] または開始側を示す [Initiator Host] を選択します。
- 侵入イベントを使用する場合は、宛先を示す [Destination Host] または送信元を示す [Source Host] を選択します。
- ディスカバリ イベント、ホスト入力イベント、またはユーザ アクティビティを使用する場合は、[Host] を選択します。

ホスト タイプを選択した後、以下の表の説明に従ってホスト プロファイル限定条件の作成を続けます。

NetFlow 対応デバイスによってエクスポートされたデータに基づき、ネットワーク マップにホストを追加するようネットワーク検出ポリシーを設定することはできますが、これらのホストに関して使用可能な情報は限られています。たとえば、これらのホストのオペレーティング システム データは得られません（ただしホスト入力機能を使って指定する場合を除く）。さらに、NetFlow 対応デバイスによってエクスポートされた接続データを使用する場合、NetFlow レコードには、どのホストがイニシエータで、どのホストがレスポンダであるかを示す情報が含まれないことに注意してください。システムが NetFlow レコードを処理するときには、各ホストが使用しているポート、およびそれらのポートがウェルノウンであるかどうかに基づき、アルゴリズムに従ってその情報が判別されます。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

表 51-11　ホスト プロファイル限定の構文

指定する項目	演算子を指定した後に行う操作
Host Type	ホスト タイプを 1 つ以上選択します。ホスト、またはいずれかのタイプのネットワーク デバイスを選択できます。
NETBIOS Name	ホストの NetBIOS 名を入力します。
Operating System > OS Name	オペレーティング システムの名前を 1 つ以上選択します。
Operating System > OS Vendor	オペレーティング システムのベンダー名を 1 つ以上選択します。
Operating System > OS Version	オペレーティング システムのバージョンを 1 つ以上選択します。
ハードウェア	モバイル デバイスのハードウェア モデルを入力します。たとえば、すべての Apple iPhone に一致させるには `iPhone` と入力します。
IOC Tag	IOC タグを 1 つ以上選択します。IOC タグ タイプの詳細については、侵害の兆候タイプについて（45-22 ページ）を参照してください。
Jailbroken	イベントのホストがジェイルブレイクされたモバイル デバイスであることを示すには [Yes] を、そうでない場合は [No] を選択します。
Mobile	イベントのホストがモバイル デバイスであることを示すには [Yes] を、そうでない場合は [No] を選択します。
Network Protocol	http://www.iana.org/assignments/ethernet-numbers にリストされているネットワーク プロトコル番号を入力します。
トランスポート プロトコル	トランスポート プロトコルの名前、または http://www.iana.org/assignments/protocol-numbers にリストされている番号を入力します。
Host Criticality	ホストの重要度（**None**、**Low**、**Medium**、または **High**）を選択します。ホストの重要度の詳細については、事前定義のホスト属性の使用（49-34 ページ）を参照してください。
VLAN ID	ホストに関連付けられた VLAN ID を入力します。

表 51-11　ホスト プロファイル限定の構文（続き）

指定する項目	演算子を指定した後に行う操作
Application Protocol > アプリケーション プロトコル	アプリケーション プロトコルを 1 つ以上選択します。
Application Protocol > Application Port	アプリケーション プロトコルのポート番号を入力します。 侵入イベントを使って相関ルールをトリガーとして使用する場合、ホスト プロファイル限定で選択したホストに応じて、イベントのポートがこのフィールドに事前入力されます（[Destination Host] の場合は `dst_port`、[Source Host] の場合は `src_port`）。
Application Protocol > Protocol	プロトコルを 1 つ以上選択します。
Application Protocol Category	カテゴリを 1 つ選択します。
[Client] > [Client]	クライアントを 1 つ以上選択します。
Client > Client Version	クライアントのバージョンを入力します。
Client Category	カテゴリを 1 つ選択します。
Web アプリケーション	Web アプリケーションを選択します。
Web Application Category	カテゴリを 1 つ選択します。
MAC Address > MAC Address	ホストの MAC アドレス全体またはその一部を入力します。 たとえば、特定のハードウェア デバイスの MAC アドレスが 0A:12:34 で始まることがわかっている場合、演算子として [begins with] を選択し、値として `0A:12:34` を入力できます。
MAC Address > MAC Type	MAC タイプが ARP/DHCP で検出されたかどうかを選択します。 つまり、MAC アドレスがホストに属していることをシステムが識別したのか（**is ARP/DHCP Detected**）、管理対象デバイスとホストの間にルータがあるなどの理由で、その MAC アドレスを持つ多数のホストをシステムが認識しているのか（**is not ARP/DHCP Detected**）、または MAC タイプが無関係であるのか（**is any**）を選択します。
MAC Vendor > MAC Vendor	ホストの MAC ハードウェア ベンダーの名前またはその一部を入力します。
使用可能な任意のホスト属性（デフォルト コンプライアンス ホワイトリスト ホスト属性を含む）	選択するホスト属性のタイプに応じて、適切な値を次のように指定します。 • ホスト属性タイプが `Integer` の場合、その属性で定義されている範囲内の整数値を入力します。 • ホスト属性タイプが `Text` の場合、テキスト値を入力します。 • ホスト属性タイプが `List` の場合、有効なリスト文字列を選択します。 • ホスト属性タイプが `URL` の場合、URL 値を入力します。 ホスト属性の詳細については、ユーザ定義のホスト属性の使用（49-35 ページ）を参照してください。

ホスト プロファイル限定を作成する際に、イベント データを使用できる場合がよくあります。たとえば、モニタ対象のいずれかのホストで Internet Explorer が使用されていることをシステムが検出した場合に相関ルールがトリガーとして使用されるとします。さらに、使用が検出された場合、ブラウザのバージョンが最新でなければイベントを生成するとします（この例では最新バージョンが 9.0 であると想定します）。

この場合、**クライアント**が**イベント クライアント**（つまり Internet Explorer）であり、しかも**クライアント バージョン**が 9.0 でない場合にのみルールがトリガーとして使用されるよう、ホスト プロファイル限定をこの相関ルールに追加することができます。

経時的な接続データを使用した相関ルールの制約

ライセンス：FireSIGHT

*接続トラッカー*は、（ホスト プロファイル限定およびユーザ限定を含む）ルールの初期基準に一致した後にシステムが特定の接続を追跡し始めるよう、相関ルールを制約します。追跡される接続が、指定した期間にわたって収集された追加の基準を満たす場合には、Defense Centerがルールの相関イベントを生成します。

接続、侵入、ディスカバリ、ユーザ アクティビティ、またはホスト入力のいずれかのイベントを使用して相関ルールをトリガーとして使用する場合は、接続トラッカーをルールに追加できます。マルウェア イベントやトラフィック プロファイル変化によってトリガーとして使用されるルールに、接続トラッカーを追加することはできません。

ヒント　通常、接続トラッカーは特定のトラフィックだけをモニタし、トリガーとして使用された場合には指定された一定期間だけ実行されます。接続トラッカーは、広範なネットワーク トラフィックをモニタして持続的に実行されるトラフィック プロファイルとは対照的です（トラフィック プロファイルの作成（53-1 ページ）を参照）。

次に示すように、接続トラッカーをどのように作成するかに応じて、接続トラッカーは 2 つの方法でイベントを生成できます。

条件に一致するとただちに起動する接続トラッカー

ネットワーク トラフィックが接続トラッカーの条件に一致すると即座に相関ルールが起動するよう、接続トラッカーを設定できます。この場合、タイムアウト期間が満了していなくても、システムはその接続トラッカー インスタンスでの接続追跡を停止します。相関ルールをトリガーとして使用したのと同じタイプのポリシー違反が再び発生した場合、システムは新しい接続トラッカーを作成します。

一方、ネットワーク トラフィックが接続トラッカーの条件に一致する前にタイムアウト期間が満了した場合、Defense Centerは相関イベントを生成せず、そのルール インスタンスの接続追跡を停止します。

たとえば、特定のタイプの接続が特定の期間中に特定回数を超えて発生した場合にのみ相関イベントを生成させることで、接続トラッカーをある種のイベントしきい値として機能させることができます。あるいは、初期接続後に過剰なデータ転送量をシステムが検出した場合にのみ、相関イベントを生成させることもできます。

タイムアウト期間の満了時に起動する接続トラッカー

タイムアウト期間全体にわたって収集されるデータに依存するよう、接続トラッカーを設定できます。この場合、タイムアウト期間が満了するまでは起動しません。

たとえば、特定の期間内に検出された転送量が特定のバイト数を下回った場合に接続トラッカーを起動するよう設定すると、システムはその期間が経過するまで待って、ネットワーク トラフィックがその条件に一致した場合はイベントを生成します。

詳細については、次の項を参照してください。

- 接続トラッカーの追加（51-25 ページ）
- 接続トラッカーの構文（51-26 ページ）

接続トラッカーの追加

ライセンス：FireSIGHT

接続トラッカー は、（ホスト プロファイル限定およびユーザ限定を含む）初期基準が満たされた後にシステムが特定の接続を追跡し始めるよう、相関ルールを制約します。追跡される接続が、指定した期間にわたって収集された追加の基準を満たす場合には、Defense Centerがルールの相関イベントを生成します。

接続トラッカーを設定するときには、次の項目を指定する必要があります。

- どの接続を追跡するか
- Defense Centerに相関イベントを生成させるために、追跡対象の接続が満たす必要のある条件
- 接続トラッカーの最大有効期間（相関イベントが生成されるためには、この期間内に指定の条件が満たされる必要があります）

ヒント　接続、侵入、ディスカバリ、ユーザ アイデンティティ、またはホスト入力のいずれかのイベントが発生することだけを必要とする単純な相関ルールに、接続トラッカーを追加することができます。

接続トラッカーを追加する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Create Rule]ページで、[Add Connection Tracker] をクリックします。

[Connection Tracker] セクションが表示されます。

ヒント　接続トラッカーを削除するには、[Remove Connection Tracker] をクリックします。

ステップ 2　接続トラッカーの基準を設定することにより、追跡対象の接続を指定します。

接続トラッカーの基準を設定するときには、1 つの単純な条件を作成することも、複数の条件の組み合わせやネストを使って複雑な構造を作成することもできます。

Web インターフェイスを使用して条件を作成する方法については、ルールの作成メカニズムについて（51-37 ページ）を参照してください。接続トラッカーの条件を作成するために使用できる構文については、接続トラッカーの構文（51-26 ページ）で説明しています。

ステップ 3　ステップ 2 で追跡対象として指定した接続に応じて、どのようなときに相関イベントを生成するかを記述します。

イベント生成時を記述する 1 つの単純な条件を作成することも、複数の条件の組み合わせやネストを使って複雑な構造を作成することもできます。

また、期間を秒数、分数、または時間数で指定する必要があります（相関イベントが生成されるためには、この期間内に指定の条件が満たされる必要があります）。

Web インターフェイスを使用して条件を作成する方法については、ルールの作成メカニズムについて（51-37 ページ）を参照してください。接続トラッカーの条件を作成するために使用できる構文については、接続トラッカー イベントの構文（51-28 ページ）で説明しています。

ステップ 4　オプションで、以下の項の手順に進みます。

- ユーザ限定の追加（51-34 ページ）
- スヌーズ期間および非アクティブ期間の追加（51-36 ページ）

相関ルールの作成が終了した場合は、相関ポリシーのルールの作成（51-3 ページ）で説明している手順のステップ 9 に進んでルールを保存します。

接続トラッカーの構文

ライセンス： すべて

次の表は、どのような接続を追跡するかを指定する接続トラッカー条件の作成方法を説明しています。

Cisco の管理対象デバイスによって検出された接続と、NetFlow 対応デバイスによってエクスポートされた接続データには、異なる情報が含まれていることに注意してください。たとえば、管理対象デバイスによって検出された接続には、TCP フラグ情報が含まれません。したがって、相関ルールをトリガーとして使用するために特定の TCP フラグが接続イベントに含まれる必要があると指定した場合、管理対象デバイスによって検出された接続がルールをトリガーとして使用させることは決してありません。

別の例として、NetFlow レコードには、接続の中でどのホストがイニシエータ/レスポンダであるかを示す情報が含まれません。システムが NetFlow レコードを処理するときには、各ホストが使用しているポート、およびそれらのポートがウェルノウンであるかどうかに基づき、アルゴリズムに従ってその情報が判別されます。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

表 51-12　接続トラッカーの構文

指定する項目	演算子を指定した後に行う操作
Access Control Policy	追跡対象の接続をログに記録したアクセス コントロール ポリシーを 1 つ以上選択します。
Access Control Rule Action	追跡対象の接続をログに記録したアクセス コントロール ルールに関連付けられたアクセス コントロール ルール アクションを 1 つ以上選択します。 **注**　あとで接続を処理するルール/デフォルト アクションとは無関係に、任意のモニタ ルールの条件に一致する接続を追跡するには、[Monitor] を選択します。
Access Control Rule Name	追跡対象の接続をログに記録したアクセス コントロール ルールの名前またはその一部を入力します。 **注**　モニタ ルールに一致する接続を追跡するには、モニタ ルールの名前を入力します。あとで接続を処理するルール/デフォルト アクションとは無関係に、システムは該当する接続を追跡します。
Application Protocol	アプリケーション プロトコルを 1 つ以上選択します。
Application Protocol Category	アプリケーション プロトコルのカテゴリを 1 つ以上選択します。
クライアント	クライアントを 1 つ以上選択します。
Client Category	クライアントのカテゴリを 1 つ以上選択します。

表 51-12　接続トラッカーの構文（続き）

指定する項目	演算子を指定した後に行う操作
Client Version	クライアントのバージョンを入力します。
Connection Duration	接続期間（秒数）を入力します。
Connection Type	Cisco の管理対象デバイスによって検出された接続を追跡するのか（**FireSIGHT**）、または NetFlow 対応デバイスによってエクスポートされた接続を追跡するのか（**NetFlow**）を選択します。
Destination Country または Source Country	1 つ以上の国を選択します。
デバイス	追跡対象の接続が検出されるデバイスを 1 つ以上選択します。NetFlow 接続を追跡する場合は、NetFlow 対応デバイスによってエクスポートされた接続データを処理するデバイスを選択します。
Ingress Interface または Egress Interface	インターフェイスを 1 つ以上選択します。
Ingress Security Zone または Egress Security Zone	セキュリティ ゾーンを 1 つ以上選択します。
Initiator IP、Responder IP、または Initiator/Responder IP	単一の IP アドレスまたはアドレス ブロックを入力します。FireSIGHT システムで使用する IP アドレス表記については、IP アドレスの表記規則（1-23 ページ）を参照してください。
Initiator Bytes、Responder Bytes、または Total Bytes	以下のいずれかを入力します。 • イニシエータから送信されたバイト数（[Initiator Bytes]） • レスポンダで受信されたバイト数（[Responder Bytes]） • 送受信されたバイト数（[Total Bytes]）
Initiator Packets、Responder Packets、または合計パケット数	以下のいずれかを入力します。 • イニシエータから送信されたパケット数（[Initiator Packets]） • レスポンダで受信されたパケット数（[Responder Packets]） • 送受信されたパケット数（[Total Packets]）
Initiator Port/ICMP Type または Responder Port/ICMP Code	イニシエータ トラフィックのポート番号または ICMP タイプ、あるいはレスポンダ トラフィックのポート番号または ICMP コードを入力します。
IOC Tag	IOC タグが設定されているか（`is`）、設定されていないか（`is not`）を選択します。
NETBIOS Name	接続におけるモニタ対象ホストの NetBIOS 名を入力します。
NetFlow Device	追跡対象の接続をエクスポートした NetFlow 対応デバイスの IP アドレスを選択します。展開環境に NetFlow 対応デバイスをまだ追加していない場合、[NetFlow Device] ドロップダウンリストは空白になります。
理由	追跡対象の接続に関連付けられた理由を 1 つ以上選択します。
Security Intelligence Category	追跡対象の接続に関連付けられたセキュリティ インテリジェンスのカテゴリを 1 つ以上選択します。
TCP Flags	接続を追跡するために接続に含まれている必要のある TCP フラグを選択します。 **注**　NetFlow 対応デバイスによってエクスポートされた接続にのみ、TCP フラグ データが含まれます。
トランスポート プロトコル	接続で使用されたトランスポート プロトコル（`TCP` または `UDP`）を入力します。
URL	追跡対象の接続でアクセスされた URL 全体、またはその一部を入力します。

表 51-12　接続トラッカーの構文（続き）

指定する項目	演算子を指定した後に行う操作
URL カテゴリ	追跡対象の接続でアクセスされた URL のカテゴリを 1 つ以上選択します。
URL Reputation	追跡対象の接続でアクセスされた URL のレピュテーション値を 1 つ以上選択します。
[Username]	追跡対象の接続でいずれかのホストにログインしたユーザを示すユーザ名を入力します。
Web Application	Web アプリケーションを 1 つ以上選択します。
Web Application Category	Web アプリケーションのカテゴリを 1 つ以上選択します。

接続トラッカーを作成する際に、イベント データを使用できる場合がよくあります。たとえば、いずれかのモニタ対象ホストで新しいクライアントをシステムが検出したときに相関ルールがトリガーとして使用されるとします。つまり、基本イベント タイプ [a new client is detected] であるシステム イベントが生成されたときにこのルールがトリガーとして使用します。

さらに、この新しいクライアントが検出されたとき、検出場所のホストでそのクライアントに関連する接続を追跡するとします。システムはホストの IP アドレスとクライアントの名前を認識しているため、これらの接続を追跡する単純な接続トラッカーを作成できます。

実際、このような相関ルールに接続トラッカーを追加すると、接続トラッカーにはデフォルト制約が設定されます。つまり [Initiator/Responder IP] が [Event IP Address] に設定され、[Client] が [Event Client] に設定されます。

ヒント　特定の IP アドレスまたは IP アドレス ブロックに関連する接続を接続トラッカーで追跡するよう指定するには、[switch to manual entry] をクリックして、手動で IP を指定します。[switch to event fields] をクリックすると、イベントの IP アドレスを使用する設定に戻ります。

接続トラッカー イベントの構文

ライセンス：すべて

追跡対象の接続に基づいてどのようなときに相関イベントを生成するかを指定する接続トラッカー条件を作成するには、次の表の説明に従います。

表 51-13　接続トラッカー イベントの構文

指定する項目	演算子を指定した後に行う操作
Number of Connections	検出された接続の合計数を入力します。
Number of SSL Encrypted Sessions	検出された SSL または TLS 暗号化セッションの合計数を入力します。
Total Bytes、Initiator Bytes、または Responder Bytes	以下のいずれかを入力します。 • 送信された合計バイト数（[Total Bytes]） • イニシエータから送信されたバイト数（[Initiator Bytes]） • レスポンダで受信されたバイト数（[Responder Bytes]）

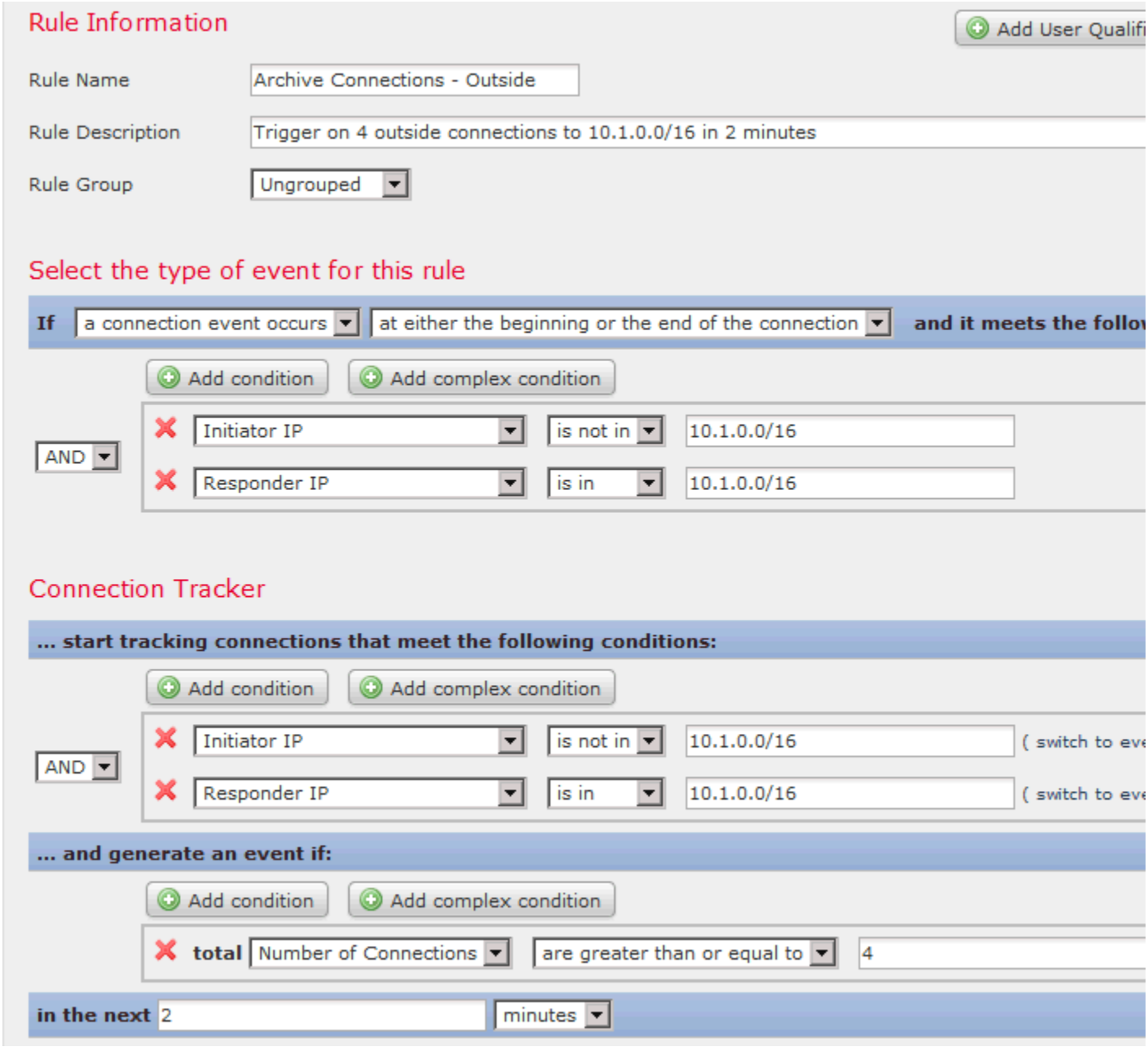
表 51-13　接続トラッカー イベントの構文(続き)

指定する項目	演算子を指定した後に行う操作
Total Packets、Initiator Packets、または Responder Packets	以下のいずれかを入力します。 • 送信された合計パケット数([Total Packets]) • イニシエータから送信されたパケット数([Initiator Packets]) • レスポンダで受信されたパケット数([Responder Packets])
Unique Initiators または Unique Responders	以下のいずれかを入力します。 • 検出されたセッションを開始した個別のホストの数([Unique Initiators]) • 検出された接続に応答した個別のホストの数([Unique Responders])

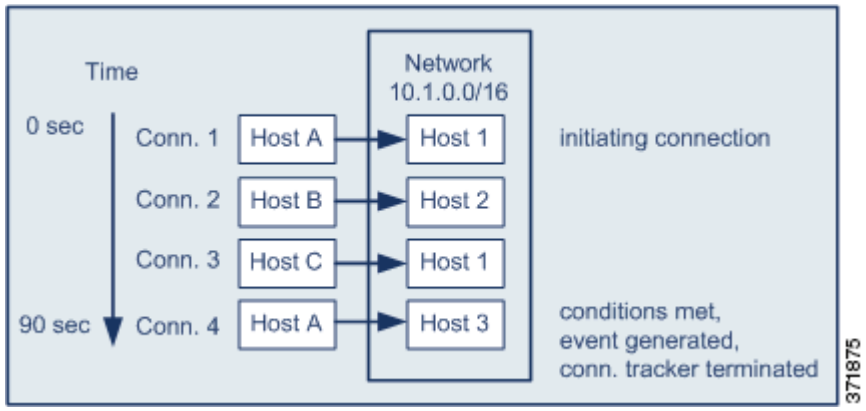
例:外部ホストからの過剰な接続数

たとえば、ネットワーク 10.1.0.0/16 で機密ファイルをアーカイブしていて、このネットワーク外部のホストは通常、ネットワーク内部のホストとの接続を開始しないとします。時にはネットワーク外部から接続が開始されることもありますが、2 分以内に 4 つ以上の接続が開始された場合には注意が必要だと判断するとします。

以下の図に示されているルールは、ネットワーク 10.1.0.0/16 の外部からネットワーク内部への接続が発生した場合、その基準に一致する接続をシステムが追跡し始めることを指定します。システムが、そのシグニチャに一致する 4 つの接続(元の接続を含む)を 2 分以内に検出した場合、Defense Centerは相関イベントを生成します。


Rule Information
Add User Qualifi
Rule Name
Archive Connections - Outside
Rule Description
Trigger on 4 outside connections to 10.1.0.0/16 in 2 minutes
Rule Group
Ungrouped
Select the type of event for this rule
If
a connection event occurs
at either the beginning or the end of the connection
and it meets the follo
Add condition
Add complex condition
AND
Initiator IP
is not in
10.1.0.0/16
Responder IP
is in
10.1.0.0/16
Connection Tracker
... start tracking connections that meet the following conditions:
Add condition
Add complex condition
AND
Initiator IP
is not in
10.1.0.0/16
(switch to eve
Responder IP
is in
10.1.0.0/16
(switch to eve
... and generate an event if:
Add condition
Add complex condition
total
Number of Connections
are greater than or equal to
4
in the next
2
minutes

ネットワーク トラフィックがこの相関ルールをどのようにトリガーとして使用するか、以下の図に示します。



この例では、相関ルールの基本条件に一致する接続をシステムが検出しました。つまり、ネットワーク 10.1.0.0/16 の外部にあるホストからネットワーク内部のホストへの接続をシステムが検出しました。これにより、接続トラッカーが作成されました。

接続トラッカーは以下の手順で処理されます。

ステップ 1　システムがネットワーク外部のホスト A からネットワーク内部のホスト 1 への接続を検出すると、その接続の追跡を開始します。

ステップ 2　システムは接続トラッカーのシグニチャに一致する接続をさらに 2 つ検出します（ホスト B からホスト 2、ホスト C からホスト 1）。

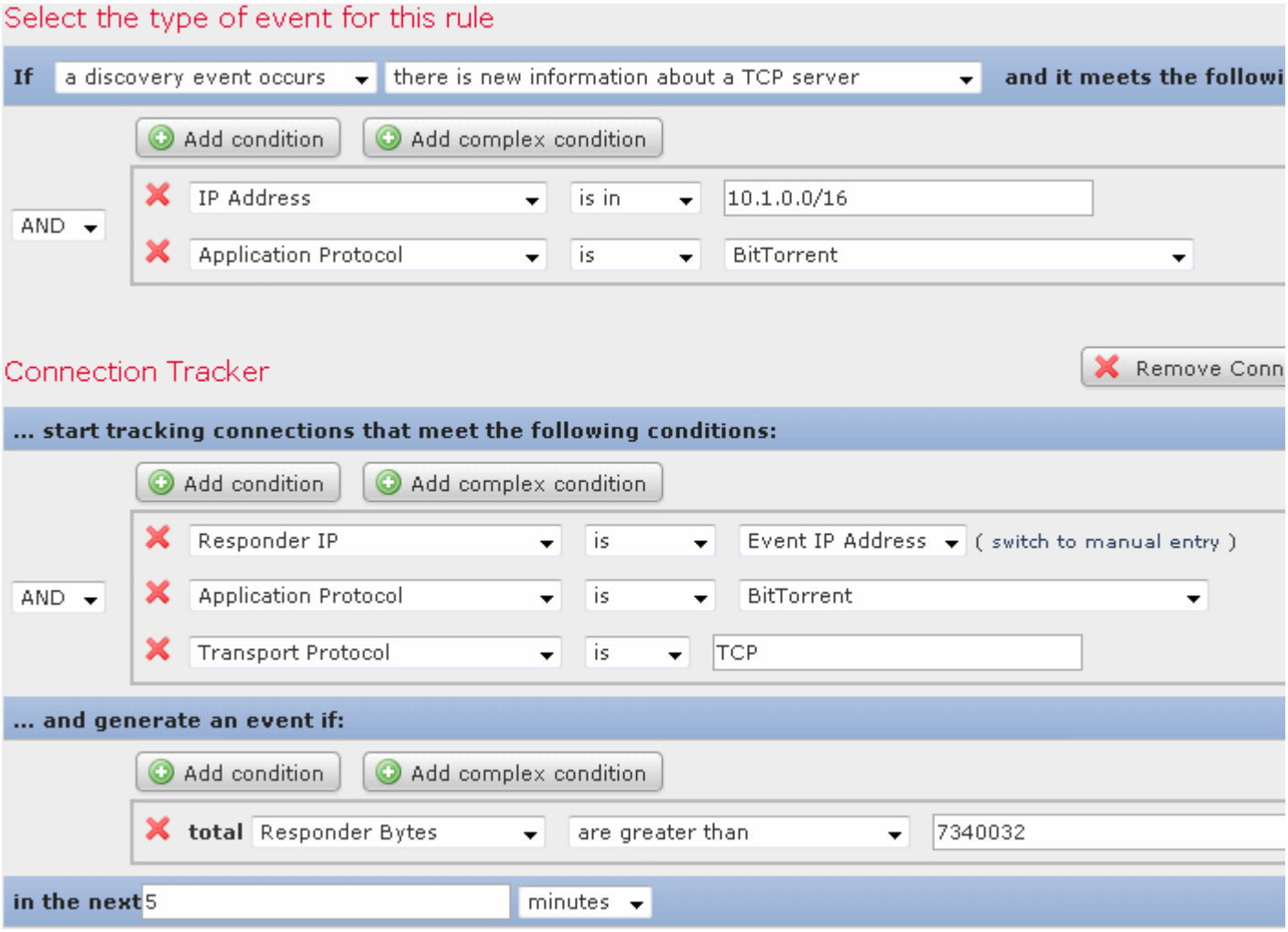
ステップ 3　2 分の制限時間内にホスト A がホスト 3 に接続すると、システムは 4 番目の適格性確認の接続を検出します。これで、ルールの条件が満たされました。

ステップ 4　Defense Centerが相関イベントを生成し、システムは接続の追跡を停止します。

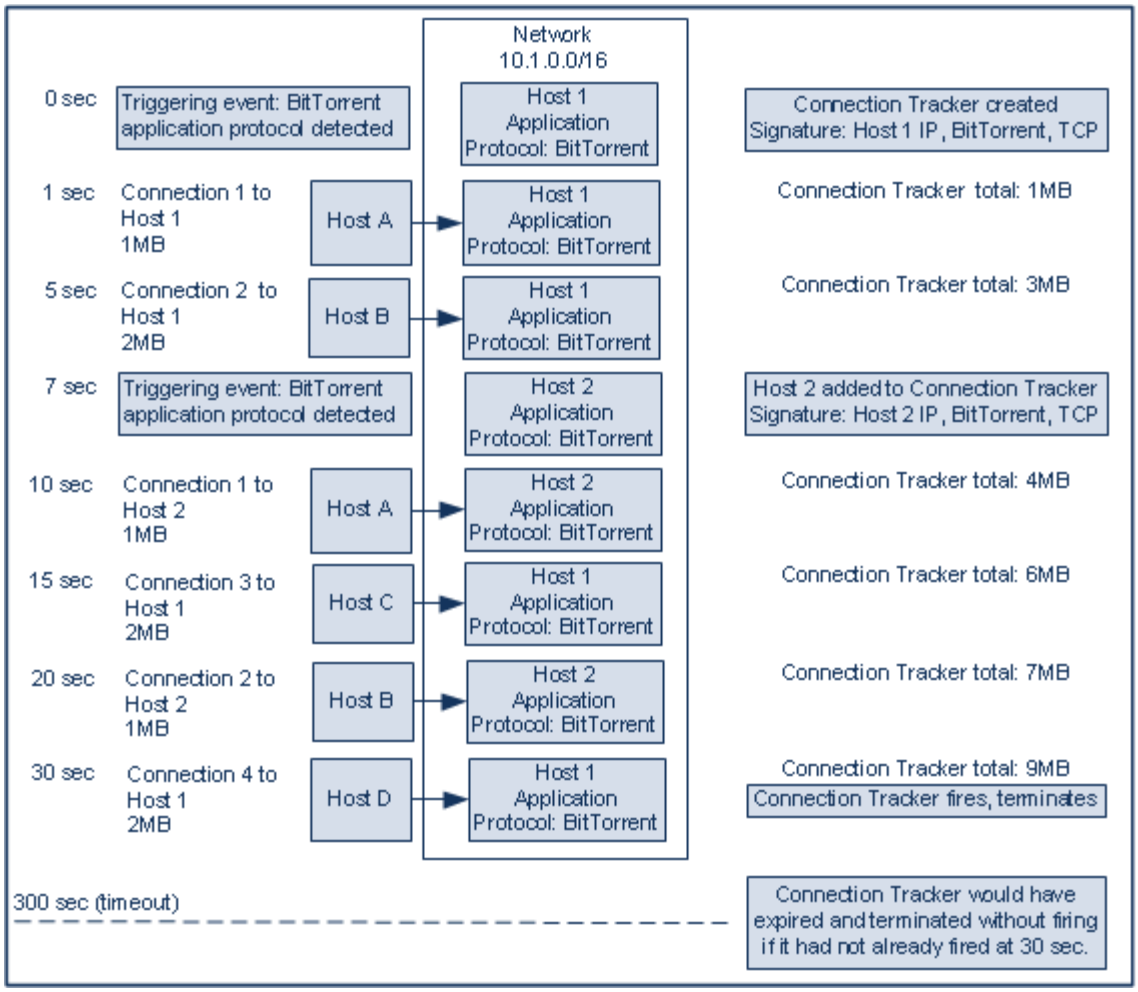
例：過剰な BitTorrent データの転送

このシナリオでは、モニタ対象ネットワーク上のいずれかのホストへの初期接続が発生した後、過剰な BitTorrent データ転送をシステムが検出すると、相関イベントを生成します。

モニタ対象ネットワークでシステムが BitTorrent アプリケーション プロトコルを検出したときにトリガーとして使用される相関ルールを以下の図に示します。このルールの接続トラッカーは、モニタ対象ネットワーク（この例では 10.1.0.0/16）上のホストが、最初のポリシー違反から 5 分間に BitTorrent を介して合計 7MB（7340032 バイト）のデータを転送した場合にのみルールがトリガーとして使用されるように制約します。


Select the type of event for this rule
If
a discovery event occurs
there is new information about a TCP server
and it meets the followi
Add condition
Add complex condition
AND
IP Address
is in
10.1.0.0/16
Application Protocol
is
BitTorrent
Connection Tracker
Remove Conn
... start tracking connections that meet the following conditions:
Add condition
Add complex condition
AND
Responder IP
is
Event IP Address
(switch to manual entry)
Application Protocol
is
BitTorrent
Transport Protocol
is
TCP
... and generate an event if:
Add condition
Add complex condition
total
Responder Bytes
are greater than
7340032
in the next
5
minutes

ネットワーク トラフィックがこの相関ルールをどのようにトリガーとして使用するか、以下の図に示します。



この例で、システムは 2 つの異なるホスト（ホスト 1 とホスト 2）で BitTorrent TCP アプリケーション プロトコルを検出しました。この 2 つのホストは、他の 4 つのホスト（ホスト A、ホスト B、ホスト C、ホスト D）に BitTorrent を介してデータを転送しました。

この接続トラッカーは以下の手順で処理されます。

ステップ 1　システムがホスト 1 で BitTorrent アプリケーション プロトコルを検出すると、システムは 0 秒マーカーで接続を追跡し始めます。

これに続く（300 秒マーカーによる）5 分間で、7MB の BitTorrent TCP データ転送をシステムが検出しなければ、接続トラッカーは期限切れになります。

ステップ 2　5 秒経過した時点で、ホスト 1 はシグニチャに一致する 3MB のデータを次のように送信しました。

- 1 秒マーカーの時点で、ホスト 1 からホスト A に 1MB を転送（接続トラッカーの条件適合に向けて合計 1MB の BitTorrent トラフィックをカウント）
- 5 秒マーカーの時点で、ホスト 1 からホスト B に 2MB（合計 3MB）

ステップ 3　7 秒経過した時点で、システムはホスト 2 での BitTorrent アプリケーション プロトコルを検出し、そのホストでも BitTorrent 接続を追跡し始めます。

ステップ 4　20 秒経過した時点で、システムは、シグニチャに一致するさらに他のデータがホスト 1 およびホスト 2 から転送されていることを検出しました。

- 10 秒マーカーの時点で、ホスト 2 からホスト A に 1MB（合計 4MB）
- 15 秒マーカーの時点で、ホスト 1 からホスト C に 2MB（合計 6MB）
- 20 秒マーカーの時点で、ホスト 2 からホスト B に 1MB（合計 7MB）

ホスト 1 とホスト 2 が転送した BitTorrent データは合計で 7MB になりましたが、転送された合計バイト数が 7MB を**超過**していることが条件となっているため（**Responder Bytes are greater than 7340032**）、ルールはトリガーとして使用されません。

この時点で、仮にトラッカー タイムアウト期間の残り 280 秒間にシステムが他の BitTorrent 転送を検出しない場合は、トラッカーが期限切れになり、Defense Centerは相関イベントを生成しません。

ステップ 5　しかし、30 秒経過した時点でシステムは別の BitTorrent 転送を次のように検出しました。

- 30 秒マーカーの時点で、ホスト 1 からホスト D に 2MB（合計 9MB）

これで、ルールの条件が満たされました。

ステップ 6　Defense Centerが相関イベントを生成します。

さらに、まだ 5 分の期間が経過していませんが、Defense Center はこの接続トラッカー インスタンスの接続の追跡を停止します。この時点で、BitTorrent TCP アプリケーション プロトコルを使用した新しい接続を検出した場合は、システムは新しい接続トラッカーを作成します。

Defense Centerはセッション終了まで接続データを集計しないため、相関イベントが生成されるのは、ホスト 1 がホスト D に 2MB を全部転送し終わった*後*であることに注意してください。

ユーザ限定の追加

ライセンス： FireSIGHT

接続、侵入、ディスカバリ、またはホスト入力のいずれかのイベントを使用して相関ルールをトリガーとして使用する場合、イベントに関連するユーザのアイデンティティに基づいてルールを制約することができます。この制約は、*ユーザ限定*と呼ばれます。トラフィック プロファイル変化やユーザ アクティビティ検出によってトリガーとして使用される相関ルールに、ユーザ限定を追加することは**できません**。

たとえば、送信元または宛先ユーザのアイデンティティが販売部門所属である場合にのみトリガーとして使用するよう、相関ルールを制約できます。

ユーザ アイデンティティ限定を追加する方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Create Rule] ページで、ユーザ限定の追加を示す [Add User Qualification] をクリックします。

[User Identity Qualification] セクションが表示されます。

ヒント　ユーザ限定を削除するには、[Remove User Qualification] をクリックします。

ステップ 2　ユーザ限定の条件を作成します。

1 つの単純な条件を作成することも、複数の条件の組み合わせやネストを使って複雑な構造を作成することもできます。Web インターフェイスを使用して条件を作成する方法については、ルールの作成メカニズムについて（51-37 ページ）を参照してください。

条件を作成するために使用できる構文については、ユーザ限定の構文（51-35 ページ）で説明しています。

ステップ 3　オプションで、スヌーズ期間および非アクティブ期間の追加（51-36 ページ）に進みます。

相関ルールの作成が終了した場合は、相関ポリシーのルールの作成（51-3 ページ）で説明している手順のステップ 9 に進んでルールを保存します。

ユーザ限定の構文

ライセンス：FireSIGHT

ユーザ限定の条件を作成するときには、まず、相関ルールを制約するために使用するアイデンティティを選択する必要があります。選択できるアイデンティティは、ルールをトリガーとして使用するために使われるイベントのタイプに応じて次のように異なります。

- 接続イベントを使用している場合は、[Identity on Initiator] または [Identity on Responder] を選択します。
- 侵入イベントを使用している場合は、宛先を示す [Identity on Destination] または送信元を示す [Identity on Source] を選択します。
- ディスカバリ イベントを使用している場合は、[Identity on Host] を選択します。
- ホスト入力イベントを使用している場合は、[Identity on Host] を選択します。

ユーザ タイプを選択した後、以下の表の説明に従ってユーザ限定条件の作成を続けます。

Defense Center は、オプションの Defense Center /LDAP サーバ間接続から、ユーザに関する特定の情報（姓名、部門、電話番号、電子メール アドレスなど）を取得します（Active Directory のログインを報告するためのユーザ エージェントの使用（17-11 ページ） を参照）。データベース内のすべてのユーザに関して、この情報が入手可能とは限りません。

表 51-14　ユーザ限定の構文

指定する項目	演算子を指定した後に行う操作
[Username]	相関ルールを制約するために使用するユーザを示すユーザ名を入力します。
Authentication Protocol	認証プロトコル（またはユーザ タイプ プロトコル）を選択します。これは、ユーザの検出に使用されたプロトコルです。
First Name	相関ルールを制約するために使用するユーザの名前（ファースト ネーム）を入力します。
Last Name	相関ルールを制約するために使用するユーザの姓を入力します。
部門	相関ルールを制約するために使用するユーザの部門/部署を入力します。
Phone	相関ルールを制約するために使用するユーザの電話番号を入力します。
電子メール	相関ルールを制約するために使用するユーザの電子メール アドレスを入力します。

スヌーズ期間および非アクティブ期間の追加

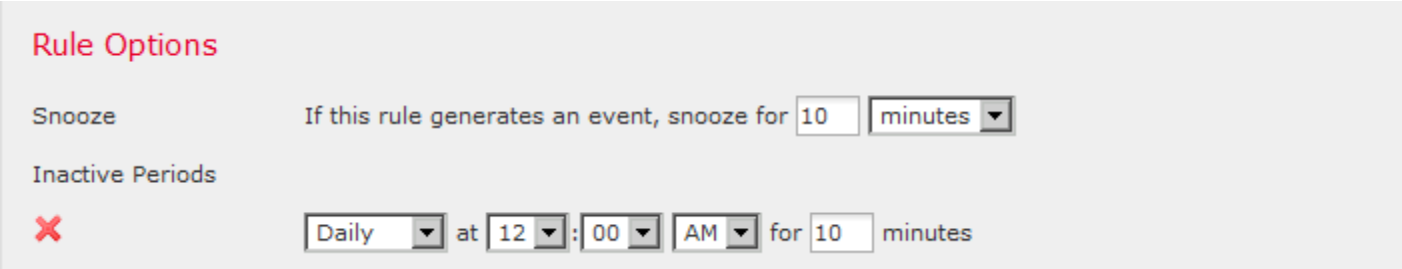
ライセンス：すべて

相関ルールで*スヌーズ期間*を設定することができます。スヌーズ期間を設定すると、相関ルールがトリガーとして使用されたとき、指定した時間間隔内にルール違反が再び発生しても、Defense Centerはその期間中はルールのトリガーを停止します。スヌーズ期間が経過すると、ルールは再びトリガー可能になります（新しいスヌーズ期間が始まります）。

たとえば、通常はトラフィックを全く生成しないはずのホストがネットワーク上にあるとします。このホストが関与する接続がシステムで検出されるたびにトリガーとして使用される単純な相関ルールの場合、このホストで送受信されるネットワーク トラフィックによっては、短時間に多数の相関イベントが生成される可能性があります。ポリシー違反を示す相関イベントの数を制限するために、スヌーズ期間を追加できます。これにより、（指定した期間内に）システムで検出されたそのホストに関連する最初の接続に対してのみ、Defense Centerは相関イベントを生成します。

また、相関ルールで非アクティブ期間を設定することもできます。非アクティブ期間中は、相関ルールはトリガーとして使用されません。非アクティブ期間を毎日、毎週、または毎月繰り返すように設定できます。たとえば、ホスト オペレーティング システム変更を探すために内部ネットワークで夜間に Nmap スキャンを実行するとします。この場合、相関ルールが誤ってトリガーとして使用されないよう、毎日のスキャン時間帯に、該当する相関ルールで非アクティブ期間を設定することができます。

以下の図は、相関ルールの中でスヌーズ期間と非アクティブ期間を設定する部分を示しています。



スヌーズ期間を追加する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Create Profile]ページの [Rule Options] で、ルールのトリガー後に再びルールをトリガーとして使用させるまでDefense Centerに待機させる間隔を指定します。

ヒント　スムーズ期間を削除するには、間隔を 0（秒、分、または時間）に指定します。

非アクティブ期間を追加する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Create Profile]ページの [Rule Options] で、[Add Inactive Period] をクリックします。

ステップ 2　ドロップダウンリストとテキスト フィールドを使用して、相関ルールに基づくネットワーク トラフィック評価を Defense Center に停止させる時点および頻度を指定します。

ヒント　非アクティブ期間を削除するには、削除対象の非アクティブ期間の横にある削除アイコン（✖）をクリックします。

スヌーズ期間と非アクティブ期間を追加し終わったら、相関ポリシーのルールの作成（51-3 ページ）で説明している手順のステップ 9 に進んでルールを保存します。

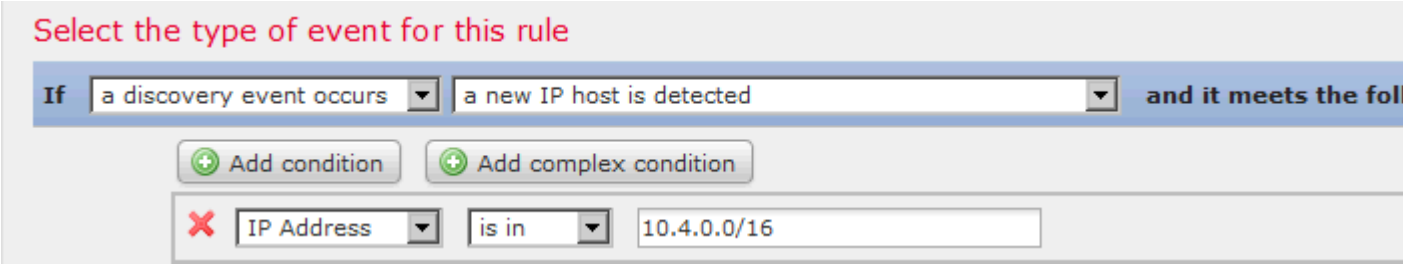
ルールの作成メカニズムについて

ライセンス：すべて

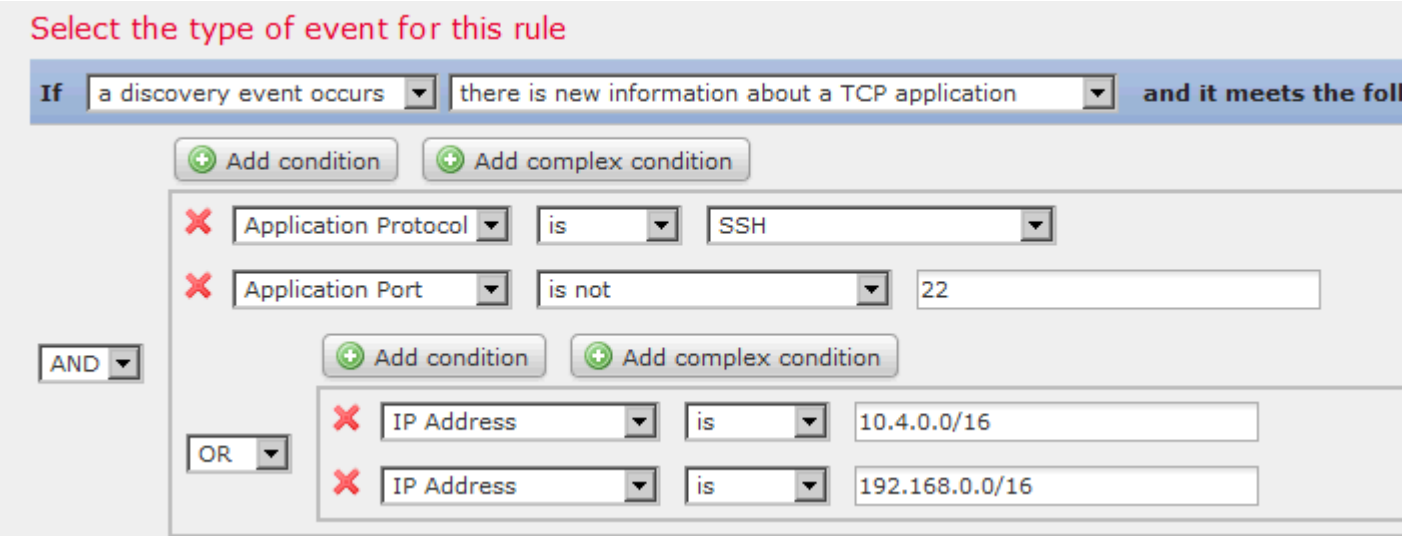
相関ルール、接続トラッカー、ユーザ限定、およびホスト プロファイル限定を作成するときには、それぞれをトリガーとして使用する条件を指定します。単純な条件を作成することも、複数の条件の組み合わせやネストを使って複雑な構造を作成することもできます。

たとえば、新しいホストが検出されるたびに相関イベントを生成するには、以下の図に示すように、条件をまったく含まない非常に単純なルールを作成できます。

ルールをさらに制約して、新しいホストが 10.4.x.x ネットワークで検出された場合にのみイベントを生成するには、以下の図に示すような 1 つの条件を追加できます。



一方、10.4.x.x ネットワークおよび 192.168.x.x ネットワーク上の非標準ポートで SSH アクティビティを検出する以下のルールには、4 つの条件が設定されており、下の 2 つは複合条件を形成しています。



条件で使用できる構文は、作成しようとしている要素により異なりますが、メカニズムはすべて同じです。

注意　頻繁に発生するイベントによってトリガーとして使用される複雑な相関ルールを評価することにより、Defense Centerのパフォーマンスが低下する可能性があります。たとえば、システムで記録されるすべての接続に対して、複数の条件からなるルールを Defense Center が評価しなければならない場合、リソースが過負荷になる可能性があります。

条件の作成の詳細については、以下の項を参照してください。

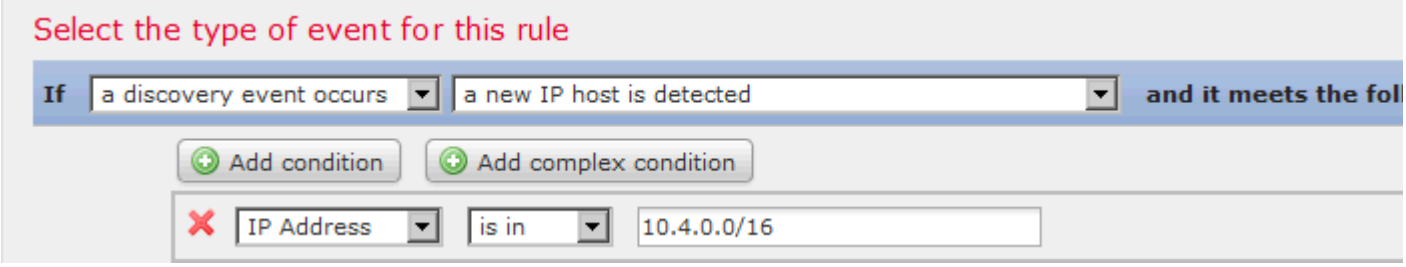
- 単一の条件の作成（51-38 ページ）
- 条件の追加と結合（51-41 ページ）
- 複数の値を条件で使用する（51-44 ページ）

単一の条件の作成

ライセンス： すべて

ほとんどの条件は*カテゴリ*、*演算子*、*値* の 3 つの要素で構成されます。より複雑な、複数のカテゴリを含む条件もあり、各カテゴリに固有の演算子と値が含まれることがあります。

たとえば、以下の相関ルールは、新しいホストが 10.4.x.x ネットワークで検出された場合にトリガーとして使用されます。条件のカテゴリは [IP Address]、演算子は [is in]、値は `10.4.0.0/16` です。



上記の例の相関ルール トリガー基準を作成する方法:

アクセス: Admin/Discovery Admin

ステップ 1　相関ルールの作成を開始します。

詳細については、相関ポリシーのルールの作成（51-3 ページ）を参照してください。

ステップ 2　[Create Rule] ページの [Select the type of event for this rule] で [a discovery event occurs] を選択した後、ドロップダウンリストから [a new IP host is detected] を選択します。

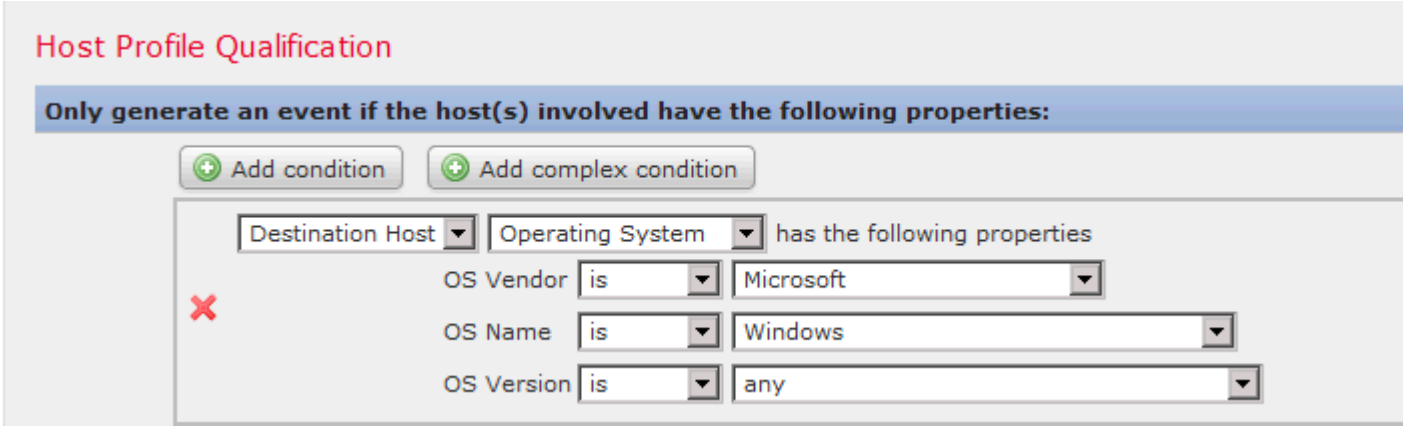
ステップ 3　ルールの単一の条件を作成するには、まず、最初の（つまり *カテゴリ*）ドロップダウンリストから [IP Address] を選択します。

ステップ 4　表示される演算子のドロップダウンリストから、[is in] を選択します。

ヒント　カテゴリが IP アドレスを表す場合、演算子として [is in] または [is not in] を選択すると、CIDR などの特殊な表記で表される IP アドレス ブロックにその IP アドレスが *含まれる* のか、*含まれない* のかを指定できます。FireSIGHT システムで使用する IP アドレス表記については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ステップ 5　テキスト フィールドに `10.4.0.0/16` と入力します。

一方、以下のホスト プロファイル限定はより複雑です。これにより相関ルールが制約され、ルールの基礎となるディスカバリ イベントに関連するホストが Microsoft Windows のバージョンを実行している場合にのみ、ルールがトリガーとして使用されます。



上記の例のホスト プロファイル限定を作成する方法:

アクセス: Admin/Discovery Admin

ステップ 1　ディスカバリ イベントによってトリガーとして使用される相関ルールを作成します。

詳細については、相関ポリシーのルールの作成（51-3 ページ）を参照してください。

ステップ 2　[Create Rule] ページで、[Add Host Profile Qualification] をクリックします。

[Host Profile Qualification] セクションが表示されます。

ステップ 3　[Host Profile Qualification] の最初の条件で、相関ルールを制約するために使用するホスト プロファイルを持つホストを指定します。

このホスト プロファイル限定は、ディスカバリ イベントに基づく相関ルールの一部であるため、使用可能なカテゴリは [Host] のみです。

ステップ 4　ホストのオペレーティング システムの詳細を指定するために、まず [Operating System] カテゴリを選択します。

[OS Vendor]、[OS Name]、[OS Version] の 3 つのサブカテゴリが表示されます。

ステップ 5　ホストが Microsoft Windows のどのバージョンを実行していても差し支えないことを指定するには、3 つのサブカテゴリすべてに同じ演算子 [is] を使用します。

ステップ 6　最後に、サブカテゴリの値を指定します。

[OS Vendor] の値には [Microsoft]、[OS Name] の値には [Windows] を選択し、[OS Version] の値は [any] のままにします。

相関ルール トリガー、ホスト プロファイル限定、接続トラッカー、またはユーザ限定のどれを作成しているのかに応じて、選択できるカテゴリが異なります。相関ルール トリガーの中でも、相関ルールの基礎となるイベントの種類に応じてカテゴリがさらに異なります。

また、選択するカテゴリに応じて、条件で使用できる演算子が異なります。さらに、条件の値を指定するために使用できる構文は、カテゴリと演算子に応じて異なります。場合によっては、テキスト フィールドに値を入力する必要があります。それ以外の場合、ドロップダウン リストから値を選択できます。

注　条件の構文でドロップダウン リストから値を選択できる場合、通常はリストから複数の値を選択できます。詳細については、複数の値を条件で使用する（51-44 ページ）を参照してください。

相関ルール トリガー基準を作成するための構文の詳細については、以下の項を参照してください。

- 侵入イベントの構文（51-7 ページ）
- マルウェア イベントの構文（51-10 ページ）
- ディスカバリ イベントの構文（51-11 ページ）
- ユーザ アクティビティ イベントの構文（51-14 ページ）
- ホスト入力イベントの構文（51-14 ページ）
- 接続イベントの構文（51-16 ページ）
- トラフィック プロファイル変化の構文（51-18 ページ）

ホスト プロファイル限定、ユーザ限定、および接続トラッカーを作成するための構文の詳細については、以下の項を参照してください。

- ホスト プロファイル限定の構文（51-21 ページ）
- 接続トラッカーの構文（51-26 ページ）
- 接続トラッカー イベントの構文（51-28 ページ）
- ユーザ限定の構文（51-35 ページ）

条件の追加と結合

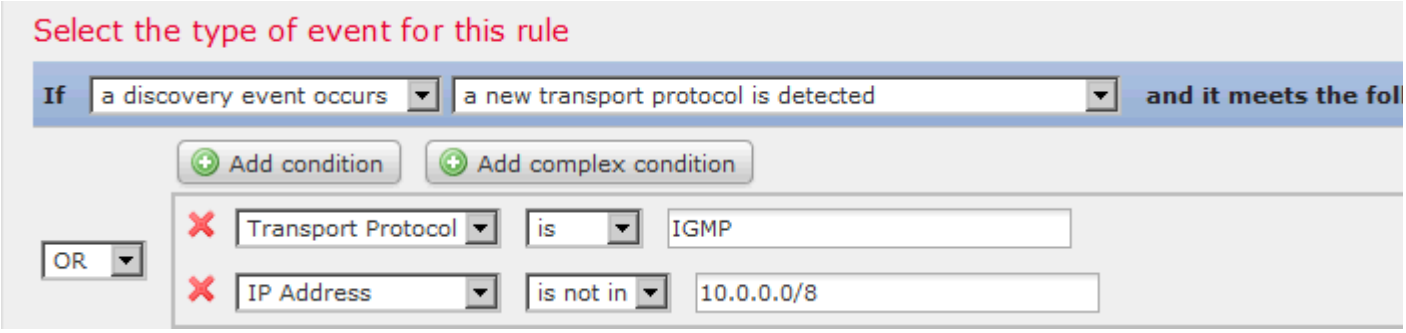
ライセンス： すべて

単純な相関ルール トリガー、接続トラッカー、ホスト プロファイル限定、ユーザ限定を作成することも、複数の条件の組み合わせやネストを使って複雑な構造を作成することもできます。

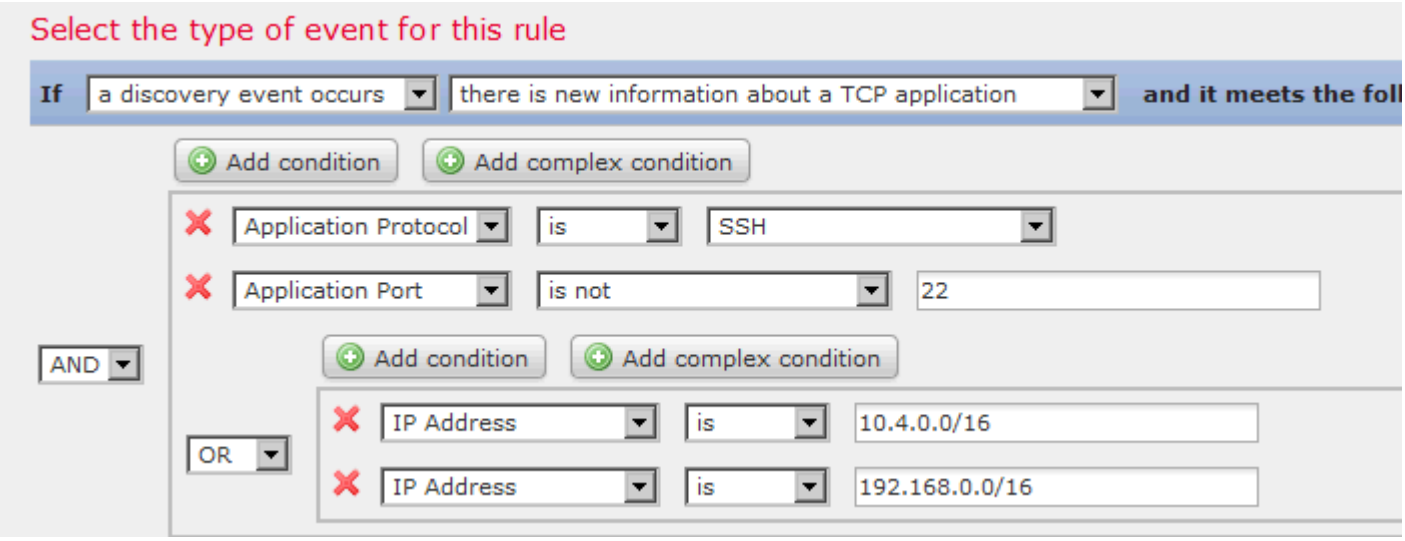
構造に複数の条件を含める場合は、それらの条件を **AND** または **OR** 演算子で結合する必要があります。同じレベルにある複数の条件は、一緒に評価されます。

- **AND** 演算子は、制御対象のレベルにあるすべての条件が満たされなければならないことを示します。
- **OR** 演算子は、制御対象のレベルにある少なくとも 1 つの条件が満たされなければならないことを示します。

たとえば、以下の相関ルール トリガー基準には、**OR** で結合された 2 つの条件が含まれます。これは、いずれかの条件が真であれば、ルールがトリガーとして使用されることを意味します。つまり、ホストの IP アドレスが 10.x.x.x サブネットに含まれない場合、またはホストが IGMP メッセージを送信する場合です。



一方、10.4.x.x ネットワークおよび 192.168.x.x ネットワーク上の非標準ポートで SSH アクティビティを検出する以下のルールには 4 つの条件が設定されており、下の 2 つは複合条件を形成しています。



このルールは、非標準ポートで SSH が検出された場合にトリガーとして使用されます。最初 2 つの条件は、アプリケーション プロトコルの名前が SSH であること、およびポートが 22 でないことを指定します。このルールはさらに、イベントに関連するホストの IP アドレスが 10.4.x.x ネットワークまたは 192.168.x.x ネットワークのいずれかに含まれていなければならないことを指定します。

論理的には、ルールは次のように評価されます。

```
(A and B and (C or D))
```

表 51-15　ルールの評価

項目	条件で指定する内容
A	アプリケーション プロトコルが SSH である
B	アプリケーション ポートが 22 ではない
C	IP アドレスが 10.4.0.0/8 に含まれる
D	IP アドレスが 196.168.0.0/16 に含まれる

単一の条件を追加する方法：

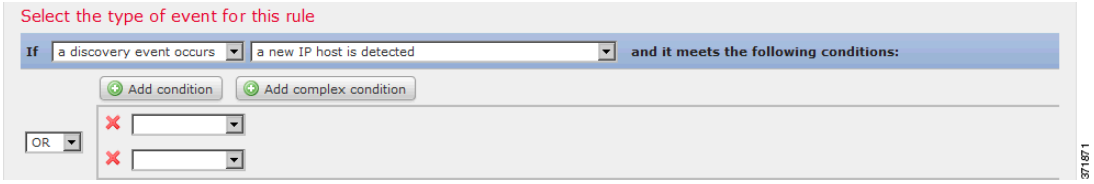
アクセス： Admin/Discovery Admin

ステップ 1　単一の条件を追加するには、現在の条件の上にある [Add condition] をクリックします。

現在の条件セットの下に、現在の条件セットと同じレベルで新しい条件が追加されます。デフォルトでは、同じレベルの条件に **OR** 演算子で結合されますが、演算子を **AND** に変更することもできます。

たとえば、以下のルールに単純な条件を追加すると、

結果は以下のとおりです。



複合条件を追加する方法:

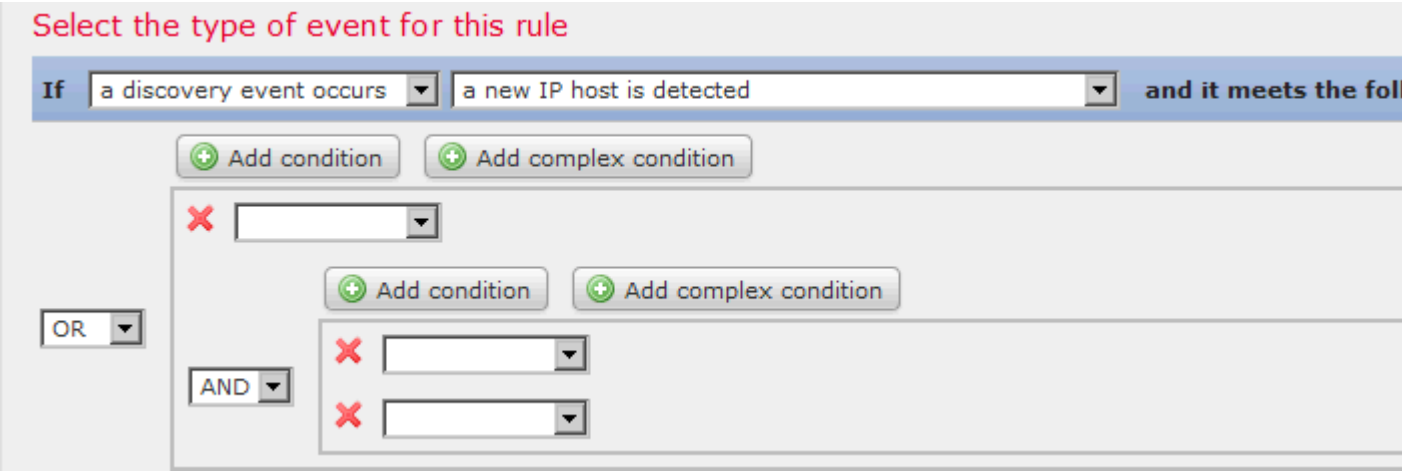
アクセス: Admin/Discovery Admin

ステップ 1　現在の条件の上にある [Add complex condition] をクリックします。

現在の条件セットの下に複合条件が追加されます。1 つの複合条件は 2 つの副条件からなり、演算子(その上のレベルにある条件を結合するために使われているものとは逆の演算子)を使って副条件が互いに結合されます。

たとえば、以下のルールに複合条件を追加すると、

結果は以下のとおりです。



条件を結合する方法:

アクセス: Admin/Discovery Admin

ステップ 1　条件セットの左側にあるドロップダウンリストを次のように使用します。次のどちらかを選択します。

- **AND** 演算子:制御対象のレベルにあるすべての条件が満たされなければならないことを示します
- **OR** 演算子:制御対象のレベルにある 1 つの条件だけが満たされればよいことを示します

複数の値を条件で使用する

ライセンス: すべて

条件を作成するときに、条件の構文でドロップダウン リストから値を選択できる場合、通常はリストから複数の値を選択できます。たとえば、ホストで何らかの UNIX フレーバを実行している必要があることを示すホスト プロファイル限定をルールに追加するには、多数の条件を OR 演算子で結合する代わりに、以下の手順を使用できます。

複数の値を 1 つの条件に含めるには:

アクセス: Admin/Discovery Admin

ステップ 1　演算子として [is in] または [is not in] を選択して 1 つの条件を作成します。

ドロップダウン リストがテキスト フィールドに変わります。

ステップ 2　テキスト フィールド内の任意の場所または [Edit] リンクをクリックします。

ポップアップ ウィンドウが表示されます。

ステップ 3　[Available] の下で、Ctrl キーまたは Shift キーを押しながら複数の値をクリックして選択します。また、クリックしてドラッグすることで、隣接する複数の値を選択できます。

ステップ 4　右矢印(**>**)をクリックして、選択した項目を [Selected] に移動します。

ステップ 5　[OK] をクリックします。

[Create Rule] ページが再び表示されます。選択した内容が、条件の値フィールドに表示されます。

相関ポリシーのルールの管理

ライセンス： すべて

相関ポリシー内で使われている相関ルールを管理するには、[Rule Management] ページを使用します。ルールを作成、変更、および削除することができます。また、ルール グループを作成すると相関ルールを簡単に編成できます。ルールを変更/削除する方法、およびルール グループを作成する方法の詳細については、以下の項を参照してください。

- ルールの変更（51-45 ページ）
- ルールの削除（51-45 ページ）
- ルール グループの作成（51-46 ページ）

ルールの作成の詳細については、相関ポリシーのルールの作成（51-3 ページ）を参照してください。

ルールの変更

ライセンス： すべて

既存の相関ルールを変更するには、以下の手順に従います。

既存のルールを変更する方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Policies] > [Correlation] を選択し、[Rule Management] タブを選択します。

[Rule Management] ページが表示されます。

ステップ 2　ルールがルール グループに含まれている場合は、グループ名をクリックしてグループを展開します。

ステップ 3　変更するルールの横にある編集アイコン（ ）をクリックします。

[Create Rule] ページが表示されます。

ステップ 4　必要に応じて変更した後、[Save] をクリックします。

ルールが更新されます。

ルールの削除

ライセンス： すべて

1 つ以上の相関ポリシーで使用している相関ルールを削除することはできません。そのようなルールを削除する前に、それを含んでいるすべてのポリシーからそのルールを削除する必要があります。ポリシーからルールを削除する方法については、相関ポリシーの編集（51-55 ページ）を参照してください。

既存のルールを削除する方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Policies] > [Correlation] を選択し、[Rule Management] タブを選択します。

[Rule Management] ページが表示されます。

ステップ 2　ルールがルール グループに含まれている場合は、グループ名をクリックしてグループを展開します。

ステップ 3　削除するルールの横にある削除アイコン（）をクリックします。

ステップ 4　ルールを削除することを確認します。

ルールが削除されます。

ルール グループの作成

ライセンス： すべて

ルール グループを作成すると、相関ルールを簡単に編成できます。FireSIGHT システムには多数のデフォルト ルールが備わっており、これらのルールは機能に応じてグループ化されています。たとえば、Worms ルール グループには、一般的なワームのアクティビティを検出するルールが含まれます。ルール グループの目的は、単に相関ルールを編成しやすくするためです。1 つのルール グループを相関ポリシーに割り当てることはできません。そうする代わりに、各ルールを個別に追加する必要があります。

ルールを作成するときに、そのルールを既存のグループに追加できます。また、既存のルールを変更して、グループに追加することもできます。詳細については、次の項を参照してください。

- 相関ポリシーのルールの作成（51-3 ページ）
- ルールの変更（51-45 ページ）

ヒント　ルール グループを削除するには、削除するグループの横にある削除アイコン（）をクリックします。ルール グループを削除しても、そのグループに含まれていたルールは**削除されません**。単にグループ化が解除されるだけです。

ルール グループを作成する方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Policies] > [Correlation] を選択し、[Rule Management] タブを選択します。

[Rule Management] ページが表示されます。

ステップ 2　[Create Group] をクリックします。

[Create Group] ページが表示されます。

ステップ 3　[Group Name] フィールドにグループの名前を入力します。

ステップ 4　[Add Group] をクリックします。

グループが追加されます。

相関応答のグループ化

ライセンス： すべて

アラート応答および修正を作成した後（アラート応答の使用（43-2 ページ）および修復の作成（54-1 ページ）を参照）、それらをグループ化すると、グループに含まれるすべての応答がポリシー違反によってトリガーとして使用されます。応答グループを相関ルールに割り当てるには、その前に、[Groups] ページでグループを作成する必要があります。

グループの横にあるスライダは、グループがアクティブであるかどうかを示します。相関ポリシー内のルールに応答グループを割り当てるには、それをアクティブにする必要があります。[Sort by] ドロップダウンリストを使用すると、応答グループを状態別（アクティブ/非アクティブ）または名前のアルファベット順でソートできます。

詳細については、次の項を参照してください。

- 応答グループの作成（51-47 ページ）
- 応答グループの変更（51-48 ページ）
- 応答グループの削除（51-48 ページ）
- 応答グループのアクティブ化と非アクティブ化（51-49 ページ）

応答グループの作成

ライセンス： すべて

個々のアラートと修正を応答グループに含めた後、それを相関ポリシー内のルールに割り当てると、ポリシー違反が発生したときにアラートや修正のグループを起動させることができます。アクティブ ポリシー内のルールにグループが割り当てられた後、グループまたはグループ内のアラートや修正を変更すると、それが自動的にアクティブ ポリシーに適用されます。

応答グループを作成する方法：

アクセス： Admin

ステップ 1　[Policies] > [Correlation] を選択し、[Groups] をクリックします。

[Groups] ページが表示されます。

ステップ 2　[Create Group] をクリックします。

[Response Group] ページが表示されます。

ステップ 3　[Name] フィールドに、新しいグループの名前を入力します。

ステップ 4　[Active] を選択するとグループがアクティブになり、相関ポリシー違反に対する応答としてこれを使用できるようになります。

ステップ 5　[Available Responses] リストから、グループに含めるアラートと修正を選択します。

ヒント　複数の応答を選択するには、Ctrl キーを押したままクリックします。

ステップ 6　右矢印（>）をクリックして、アラートと修正をグループに移動します。

反対に、[Responses in Group] リストからアラートと修正を選択して左矢印（<）をクリックすると、応答グループの外にアラートを移動することができます。

ステップ 7　[Save] をクリックします。

グループが作成されます。

応答グループの変更

ライセンス： すべて

応答グループを変更するには、以下の手順に従います。

応答グループを変更する方法：

アクセス： Admin

ステップ 1　[Policies] > [Correlation] を選択し、[Groups] をクリックします。

[Groups] ページが表示されます。

ステップ 2　変更するグループの横にある編集アイコン（ ）をクリックします。

[Response Group] ページが表示されます。

ステップ 3　必要に応じて変更を行い、[Save] をクリックします。

グループがアクティブで、使用中の場合は、変更内容がすぐに適用されます。

応答グループの削除

ライセンス： すべて

相関ポリシーで使用されていない応答グループを削除することができます。応答グループを削除しても、そのグループに含まれている応答は**削除されません**。相互の関連付けが解除されるだけです。

応答グループを削除する方法：

アクセス： Admin

ステップ 1　[Policies] > [Correlation] を選択し、[Groups] をクリックします。

[Groups] ページが表示されます。

ステップ 2　削除するグループの横にある削除アイコン（ ）をクリックします。

ステップ 3　グループを削除することを確認します。

グループが削除されます。

応答グループのアクティブ化と非アクティブ化

ライセンス：すべて

応答グループを削除せずに、一時的に非アクティブにすることができます。これにより、グループはシステムに残りますが、そのグループが割り当てられているポリシーに対する違反が発生しても、グループは起動されません。なお、相関ポリシーで使用されている応答グループを非アクティブにした場合、その応答グループは非アクティブであっても使用中とみなされます。使用中の応答グループを削除することはできません。

応答グループをアクティブまたは非アクティブにする方法：

アクセス：Admin

ステップ 1　[Policies] > [Correlation] を選択し、[Groups] をクリックします。

[Groups] ページが表示されます。

ステップ 2　アクティブまたは非アクティブにする応答グループの横にあるスライダをクリックします。

グループがアクティブ化されていた場合は、非アクティブになります。非アクティブ化されていた場合は、アクティブになります。

相関ポリシーの作成

ライセンス：すべて

相関ルールまたはコンプライアンス ホワイトリスト（あるいはその両方）、およびオプションでアラート応答と修正を作成した後、それらを使用して相関ポリシーを作成できます。

アクティブ ポリシー内の相関ルールまたはホワイトリストで指定されている基準をネットワーク トラフィックが満たす場合、Defense Centerは相関イベントまたはホワイトリスト イベントを生成します。また、ルールあるいはホワイト リストに割り当てられた応答も起動します。それぞれのルールまたはホワイトリストを、単一の応答または応答グループにマッピングできます。ネットワーク トラフィックが複数のルールまたはホワイト リストをトリガーとして使用した場合、Defense Centerはそれぞれのルールとホワイトリストに関連付けられているすべての応答を起動します。

相関ポリシーを作成するために使用できる相関ルール、コンプライアンス ホワイトリスト、および応答を作成する方法の詳細については、以下の項を参照してください。

- 相関ポリシーのルールの作成（51-3 ページ）
- コンプライアンス ホワイト リストの作成（52-9 ページ）
- 外部アラートの設定（43-1 ページ）
- 修復の設定（54-1 ページ）

ヒント　オプションで、スケルトン ポリシーを作成し、あとでそれを変更してルールと応答を追加できます。

相関ポリシーを作成する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Correlation] を選択します。

[Policy Management] ページが表示されます。

ステップ 2　[Create Policy] をクリックします。

[Create Policy] ページが表示されます。

ステップ 3　ポリシーの基本情報（名前や説明など）を指定します。

ポリシーの基本情報の指定（51-50 ページ）を参照してください。

ステップ 4　相関ポリシーに 1 つ以上のルールまたはホワイトリストを追加します。

ルールとホワイトリストを相関ポリシーに追加する（51-51 ページ）を参照してください。

ステップ 5　オプションで、ルールおよびホワイトリストのプライオリティを設定します。

ルールおよびホワイトリストのプライオリティの設定（51-52 ページ）を参照してください。

ステップ 6　オプションで、追加したルールまたはホワイトリストに、応答を追加します。

ルールとホワイトリストに応答を追加する（51-52 ページ）を参照してください。

ステップ 7　[Save] をクリックします。

ポリシーが保存されます。

注　ポリシーで相関イベントやホワイトリスト イベントを生成したり、ポリシー違反に対する応答を起動したりするには、その前にポリシーをアクティブにする必要があります。詳細については、相関ポリシーの管理（51-54 ページ）を参照してください。

ポリシーの基本情報の指定

ライセンス：すべて

各ポリシーを識別する名前を指定する必要があります。オプションで、簡単な説明をポリシーに追加できます。

また、ユーザ定義のプライオリティをポリシーに割り当てることもできます。相関ポリシーに対する違反の結果として生成される相関イベントには、そのポリシーに割り当てたプライオリティが表示されます（ただし、トリガーとして使用されたルールに独自のプライオリティが設定されている場合を除く）。

注　ルールとホワイトリストのプラオリティは、ポリシーのプライオリティをオーバーライドします。詳細については、ルールとホワイトリストを相関ポリシーに追加する（51-51 ページ）を参照してください。

ポリシーの基本情報を指定する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Create Policy] ページで、[Policy Name] フィールドにポリシーの名前を入力します。

ステップ 2　[Policy Description] フィールドに、ポリシーの説明を入力します。

ステップ 3　[Default Priority] ドロップダウンリストから、ポリシーのプライオリティを選択します。

1 から 5 までのプライオリティ値を選択できます。1 が最高、5 が最低です。または、[None] を選択すると、特定のルールに割り当てられたプライオリティだけが使用されます。

ステップ 4　次の項（ルールとホワイトリストを相関ポリシーに追加する（51-51 ページ））の手順に進みます。

ルールとホワイトリストを相関ポリシーに追加する

ライセンス：すべて

1 つの相関ポリシーには、1 つ以上の相関ルールまたはホワイトリストが含まれます。ポリシー内のいずれかのルールまたはホワイト リストに対する違反が発生すると、システムはイベントをデータベースに記録します。ルールまたはホワイトリストに 1 つ以上の応答がすでに割り当てられている場合、それらの応答が起動されます。

以下の図は、コンプライアンス ホワイトリストと一連の相関ルールからなる、さまざまな応答が設定された相関ポリシーを示しています。

z

Policy Rules

Rule	Responses
Bugbear Worm Detects the Bugbear HTTP server backdoor	Sample Email Alert Response (Email
Default White List	Sample SNMP Alert Response (SNMP
Lovgate Worm Detects activity by the Lovgate worm backdoor component	Sample Syslog Alert Response (Sysl
MyDoom Worm Detects activity by the backdoor component of MyDoom	Sample Syslog Alert Response (Sysl Sample SNMP Alert Response (SNMP Sample Email Alert Response (Email
NetSky.S Detects the backdoor component of the NetSky.S worm.	This rule does not have any respons

ルールまたはホワイトリストを相関ポリシーに追加する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Create Policy] ページで、[Add Rules] をクリックします。

[Available Rules] ポップアップが表示されます。

ステップ 2　該当するフォルダ名をクリックしてフォルダを展開します。

ステップ 3　ポリシーで使用するルールとホワイトリストを選択して、[Add] をクリックします。

[Create Policy] ページが再び表示されます。選択したルールとホワイトリストがポリシーに含まれます。

ステップ 4　次の項（ルールおよびホワイトリストのプライオリティの設定（51-52 ページ））の手順に進みます。

ルールおよびホワイトリストのプライオリティの設定

ライセンス： すべて

相関ポリシーに含まれる個々の相関ルールやコンプライアンス ホワイトリストに、ユーザ定義のプライオリティを割り当てることができます。ルールまたはホワイトリストがトリガーとして使用された結果として生成されるイベントには、そのルールまたはホワイトリストに割り当てたプライオリティが表示されます。一方、プライオリティ値を割り当てない状態でルールまたはホワイトリストがトリガーとして使用されると、結果として生成されるイベントには、ポリシーのプライオリティ値が表示されます。

たとえば、あるポリシー自体のプライオリティが 1 に設定され、そのポリシー内の 1 つのルールにプライオリティ 3 が設定され、他のルールまたはホワイトリストにはデフォルト プライオリティが設定されているとします。プライオリティ 3 のルールがトリガーとして使用された場合、結果としてできる相関イベントのプライオリティ値は 3 と表示されます。ポリシー内の他のルールまたはホワイトリストがトリガーとして使用された場合、結果としてできるイベントには、ポリシーのプライオリティから得られたプライオリティ値 1 が表示されます。

ルールまたはホワイトリストのプライオリティを設定する方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Create Policy] ページで、ルールまたはホワイトリストごとの [Priority] リストから、デフォルト プライオリティを選択します。次のオプションを選択できます。

- 1 から 5 までのプライオリティ値（1 が最高、5 が最低）
- **なし**
- **Default**（ポリシーのデフォルト プライオリティを使用）

ステップ 2　次の項（ルールとホワイトリストに応答を追加する（51-52 ページ））の手順に進みます。

ルールとホワイトリストに応答を追加する

ライセンス： すべて

相関ポリシー内で、個々のルールまたはホワイトリストを 1 つの応答または応答のグループにマッピングできます。ポリシー内のいずれかのルールまたはホワイトリストに対する違反が発生した場合、システムは関連するイベントをデータベースに記録し、そのルールまたはホワイトリストに割り当てられている応答を起動します。ポリシー内の複数のルールまたはホワイトリストがトリガーとして使用された場合、Defense Centerはそれぞれのルールまたはホワイトリストに関連付けられている応答を起動します。

応答と応答グループを作成する方法の詳細については、以下の項を参照してください。

- 外部アラートの設定（43-1 ページ）
- 修復の設定（54-1 ページ）
- 相関応答のグループ化（51-47 ページ）

注　トラフィック プロファイル変化によってトリガーとして使用される相関ルールへの応答として、Nmap 修正を**割り当てないでください**。修正は起動されません。

以下の図は、コンプライアンス ホワイトリストと一連の相関ルールからなる、さまざまな応答が設定された相関ポリシーを示しています。

z

Policy Rules

Rule	Responses
Bugbear Worm Detects the Bugbear HTTP server backdoor	Sample Email Alert Response (Email
Default White List	Sample SNMP Alert Response (SNMP
Lovgate Worm Detects activity by the Lovgate worm backdoor component	Sample Syslog Alert Response (Sysl
MyDoom Worm Detects activity by the backdoor component of MyDoom	Sample Syslog Alert Response (Sysl Sample SNMP Alert Response (SNMP Sample Email Alert Response (Email
NetSky.S Detects the backdoor component of the NetSky.S worm.	This rule does not have any respons

ルールとホワイト リストに応答を追加する方法:

アクセス: Admin/Discovery Admin

ステップ 1　[Create Policy] ページで、応答を追加するルールまたはホワイト リストの横にある応答アイコン（）をクリックします。

ポップアップ ウィンドウが表示されます。

ステップ 2　[Unassigned Responses] の下で、ルールまたはホワイトリストがトリガーとして使用された場合に起動する 1 つ以上の応答または応答グループを選択して、上矢印をクリックします。

ヒント　複数の応答を選択するには、Ctrl キーを押したままクリックします。

ステップ 3　[Update] をクリックします。

[Create Policy] ページが再び表示されます。指定した応答がルールまたはホワイト リストに追加されます。

相関ポリシーの管理

ライセンス： すべて

相関ポリシーの管理は、[Policy Management] ページで行います。ポリシーを作成、変更、ソート、アクティブ化、非アクティブ化、および削除できます。

ポリシーの横にあるスライダは、ポリシーがアクティブであるかどうかを示します。ポリシーで相関イベントやホワイトリスト イベントを生成するためには、ポリシーをアクティブにする必要があります。[Sort by] ドロップダウンリストを使用すると、ポリシーを状態別（アクティブ/非アクティブ）または名前のアルファベット順でソートできます。

アクティブな相関ポリシーにコンプライアンス ホワイトリストが含まれている場合、以下のアクションによって、そのホワイトリストに関連付けられているホスト属性が削除されることも、ホスト属性の値が変更されることも**ありません**。

- ポリシーの非アクティブ化
- ポリシーの変更（ホワイトリストを削除）
- ポリシーの削除

つまり、たとえばアクションを実行した時点で準拠していたホストは、ホスト属性ネットワークマップで引き続き準拠ホストとして表示されます。ホスト属性を削除するには、対応するホワイト リストを削除する必要があります。

ネットワーク上のホストのホワイトリスト コンプライアンスを更新するには、相関ポリシー再びアクティブ化するか（以前に非アクティブ化した場合）、またはホワイトリストを別のアクティブな相関ポリシーに追加する必要があります（相関ポリシーからホワイト リストを削除した場合、またはポリシー自体を削除した場合）。この操作を実行すると発生するホワイトリストの再評価によって、ホワイトリスト イベントが生成されることは**ありません**。したがって、ホワイトリストに関連付けられた応答がトリガーとして使用されることもありません。コンプライアンス ホワイトリストの詳細については、FireSIGHT システムのコンプライアンス ツールとしての使用（52-1 ページ）を参照してください。

相関ポリシーを管理する方法の詳細については、以下の項を参照してください。

- 相関ポリシーのアクティブ化と非アクティブ化（51-54 ページ）
- 相関ポリシーの編集（51-55 ページ）
- 相関ポリシーの削除（51-55 ページ）

新しいポリシーを作成する方法については、相関ポリシーの作成（51-49 ページ）を参照してください。

相関ポリシーのアクティブ化と非アクティブ化

ライセンス： すべて

相関ポリシーをアクティブまたは非アクティブにするには、以下の手順に従います。

ポリシーをアクティブ化または非アクティブ化する方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Policies] > [Correlation] を選択します。

[Policy Management] ページが表示されます。

ステップ 2　アクティブまたは非アクティブにするポリシーの横にあるスライダをクリックします。

ポリシーがアクティブであった場合は、非アクティブになります。非アクティブ化されていた場合は、アクティブになります。

相関ポリシーの編集

ライセンス： すべて

相関ポリシーを変更するには、以下の手順に従います。

ポリシーを編集するには、次の手順を実行します。

アクセス： Admin/Discovery Admin

ステップ 1　[Policies] > [Correlation] を選択します。

[Policy Management] ページが表示されます。

ステップ 2　ポリシーの横にある編集アイコン（  ）をクリックします。

[Create Policy] ページが表示されます。変更可能なさまざまな設定の詳細については、相関ポリシーの作成（51-49 ページ）を参照してください。相関ポリシーからルールまたはホワイトリストを削除するには、[Create Policy] ページで、削除するルールまたはホワイトリストの横にある削除アイコン（  ）をクリックします。

ステップ 3　必要に応じて変更を行い、[Save] をクリックします。

ポリシーが変更されます。ポリシーがアクティブな場合は、変更内容がすぐに適用されます。

相関ポリシーの削除

ライセンス： すべて

相関ポリシーを削除するには、以下の手順に従います。

ポリシーを削除する方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Policies] > [Correlation] を選択します。

[Policy Management] ページが表示されます。

ステップ 2　削除するポリシーの横にある削除アイコン（  ）をクリックします。

ポリシーが削除されます。

相関イベントの操作

ライセンス： すべて

アクティブな相関ポリシーに含まれる相関ルールがトリガーとして使用されると、Defense Centerが相関イベントを生成してデータベースにそれを記録します。データベースに保存される相関イベントの数を設定する方法については、データベース イベント制限の設定（63-16 ページ）を参照してください。

注　アクティブな相関ポリシーに含まれるコンプライアンス ホワイトリストがトリガーとして使用されると、Defense Centerがホワイトリスト イベントを生成します。詳細については、ホワイト リスト イベントの操作（52-33 ページ）を参照してください。

詳細については、次の項を参照してください。

- 相関イベントの表示（51-56 ページ）
- 相関イベント テーブルについて（51-58 ページ）
- 相関イベントの検索（51-59 ページ）

相関イベントの表示

ライセンス： すべて

相関イベントのテーブルを表示し、検索対象の情報に応じてイベント ビューを操作できます。

相関イベントにアクセスしたときに表示されるページは、使用するワークフローによって異なります。相関イベントのテーブル ビューが含まれる定義済みワークフローを使用できます。また、特定の要件に一致する情報のみを表示するカスタム ワークフローを作成することもできます。カスタム ワークフローの作成については、カスタム ワークフローの作成（58-43 ページ）を参照してください。

次の表では、相関イベント ワークフローのページで実行できる操作をいくつか説明します。

表 51-16　相関イベントの操作

目的	操作
IP アドレスのホスト プロファイルを表示する	IP アドレスの横に表示されるホスト プロファイル アイコンをクリックします。
ユーザ プロファイル情報を表示する	ユーザ アイデンティティの横に表示されるユーザ アイコン（  ）をクリックします。詳細については、ユーザの詳細とホストの履歴について（50-68 ページ）を参照してください。
現在のワークフロー ページでイベントをソートおよび制約する	ドリルダウン ワークフロー ページのソート（58-38 ページ）にある詳細情報を参照してください。
現在のワークフロー ページ内を移動する	ワークフロー内の他のページへのナビゲート（58-39 ページ）にある詳細情報を参照してください。
現在の制約を保持しながら、現在のワークフローのページ間を移動する	ワークフロー ページの左上にある、該当するページのリンクをクリックします。詳細については、ワークフローのページの使用（58-21 ページ）を参照してください。
表示されるカラムの詳細を調べる	相関イベント テーブルについて（51-58 ページ）にある詳細情報を参照してください。

表 51-16　相関イベントの操作（続き）

目的	操作
表示するイベントの日時範囲を変更する	イベント時間の制約の設定（58-26 ページ）にある詳細情報を参照してください。 イベント ビューを時間によって制約している場合は、（グローバルかイベントに特有かに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあることに注意してください。アプライアンスでスライド時間枠を設定した場合でも、これが発生する可能性があります。
特定の値に制約して、ワークフロー内の次のページにドリルダウンする	次のいずれかの方法を使用します。 • カスタム ワークフローで作成したドリルダウン ページで、行内の値をクリックします。テーブル ビューの行内の値をクリックすると、テーブル ビューが制約されることに注意してください（次のページにはドリルダウン**されません**）。 • 一部のユーザに制約して次のワークフロー ページにドリルダウンするには、次のワークフロー ページに表示させるユーザの横のチェック ボックスを選択し、[View] をクリックします。 • 現在の制約を保持しながら、次のワークフロー ページにドリルダウンするには、[View All] をクリックします。 **ヒント**　テーブル ビューのページ名には必ず「Table View」が含まれます。 詳細については、イベントの制約（58-35 ページ）を参照してください。
システムから相関イベントを削除する	次のいずれかの方法を使用します。 • いくつかのイベントを削除するには、削除するイベントの横にあるチェック ボックスを選択し、[Delete] をクリックします。 • 現在の制約付きビューにあるすべてのイベントを削除するには、[Delete All] をクリックした後、すべてのイベントを削除することを確認します。
他のイベント ビューに移動して関連するイベント表示する	ワークフロー間のナビゲート（58-40 ページ）にある詳細情報を参照してください。

相関イベントを表示する方法：

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Correlation] > [Correlation Events] を選択します。

デフォルト相関イベント ワークフローの最初のページが表示されます。カスタム ワークフローなど別のワークフローを使用するには、ワークフロー タイトルの近くの [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください（イベント時間の制約の設定（58-26 ページ）を参照）。

ヒント　相関イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(switch workflow)] をクリックし、[Correlation Events] を選択します。

相関イベント テーブルについて

ライセンス：すべて

相関ルールがトリガーとして使用されると、Defense Centerは相関イベントを生成します。相関イベント テーブルのフィールドについて、以下の表で説明します。

表 51-17　相関イベントのフィールド

フィールド	説明
時刻	相関イベントが生成された日時。
Impact	侵入データ、ディスカバリ データ、および脆弱性情報の間の相関に基づいて相関イベントに割り当てられた影響レベル詳細については、影響レベルを使用してイベントを評価する (41-39 ページ)を参照してください。
Inline Result	次のいずれか： • 黒の下矢印：侵入ルールをトリガーとして使用したパケットがシステムによってドロップされたことを示します • グレーの下矢印：侵入ポリシー オプション [Drop when Inline] を有効にした場合、インライン型、スイッチ型、またはルーティング型展開でパケットがシステムによってドロップされたと想定されることを示します • 空白：トリガーとして使用された侵入ルールが [Drop and Generate Events] に設定されていなかったことを示すます 侵入ポリシーのドロップ動作やルール状態とは無関係に、パッシブ展開（インライン セットがタップ モードである場合を含む）ではシステムがパケットをドロップしないことに注意してください。
Source IP または Destination IP	ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホストの IP アドレス。
Source Country または Destination Country	ポリシー違反をトリガーとして使用したイベントの送信元または宛先 IP アドレスに関連付けられた国。
Security Intelligence Category	ブラックリスト化されたオブジェクトの名前。これは、ポリシー違反をトリガーとして使用したイベントでブラックリスト化された IP アドレスを示す（またはその IP アドレスを含む）オブジェクトです。
Source User または Destination User	ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホストにログインしたユーザの名前。
Source Port/ICMP Type または Destination Port/ICMP Code	ポリシー違反をトリガーとして使用したイベントに関連付けられた、送信元トラフィックの送信元ポート/ICMP タイプまたは宛先トラフィックの宛先ポート/ICMP コード。
説明	相関イベントについての説明。説明に示される情報は、ルールがどのようにトリガーとして使用されたかによって異なります。 たとえば、オペレーティング システム情報の更新イベントによってルールがトリガーとして使用された場合、新しいオペレーティング システムの名前と信頼度レベルが表示されます。
ポリシー（Policy）	違反が発生したポリシーの名前。
ルール	ポリシー違反をトリガーとして使用したルールの名前。
プライオリティ	ポリシー違反をトリガーとして使用したポリシーまたはルールで指定されたプライオリティ。

表 51-17　相関イベントのフィールド（続き）

フィールド	説明
Source Host Criticality または Destination Host Criticality	相関イベントに関連する送信元または宛先ホストにユーザが割り当てたホスト重要度。None、Low、Medium、または High のいずれかです。 ディスカバリ イベント、ホスト入力イベント、または接続イベントに基づくルールによって生成された相関イベントにのみ、送信元ホスト重要度が含まれることに注意してください。ホストの重要度の詳細については、事前定義のホスト属性の使用（49-34 ページ）を参照してください。
Ingress Security Zone または Egress Security Zone	ポリシー違反をトリガーとして使用した侵入イベントまたは接続イベントの入力または出力セキュリティ ゾーン。
デバイス	ポリシー違反をトリガーとして使用したイベントを生成したデバイスの名前。
Ingress Interface または Egress Interface	ポリシー違反をトリガーとして使用した侵入イベントまたは接続イベントの入力または出力インターフェイス。
Count	各行に表示された情報に一致するイベントの数。[Count] フィールドは、制約を適用した後に 2 つ以上の同一行が生じた場合にのみ表示されることに注意してください。

相関イベント テーブルの表示の詳細については、以下の項を参照してください。

- 相関イベントの表示（51-56 ページ）
- 相関イベントの検索（51-59 ページ）

相関イベントの検索

ライセンス：すべて

特定の相関イベントを検索できます。実際のネットワーク環境に合わせてカスタマイズされた検索を作成して保存すると、あとで再利用できます。以下の表に、使用できる検索基準を示します。

表 51-18　相関イベントの検索基準

フィールド	検索基準の規則
ポリシー（Policy）	検索する相関ポリシーの名前を入力します。
ルール	検索する相関ルールの名前を入力します。
説明	相関イベントの説明またはその一部を入力します。説明に含まれる情報は、ルールをトリガーとして使用させたイベントによって異なります。
プライオリティ	相関イベントのプライオリティを指定します（これは、トリガーとして使用されたルールのプライオリティまたは違反が発生した相関ポリシーのプライオリティによって決まります）。プライオリティなしを指定するには、none と入力します。相関ルールとポリシーのプライオリティを設定する方法については、ポリシーの基本情報の指定（51-50 ページ）およびルールおよびホワイトリストのプライオリティの設定（51-52 ページ）を参照してください。
Source Country、Destination Country、または Source/Destination Country	ポリシー違反をトリガーとして使用したイベントの送信元 IP アドレス、宛先 IP アドレス、または送信元/宛先 IP アドレスに関連付けられた国を指定します。
Source Continent、Destination Continent、または Source/Destination Continent	ポリシー違反をトリガーとして使用したイベントの送信元 IP アドレス、宛先 IP アドレス、または送信元/宛先 IP アドレスに関連付けられた大陸を指定します。

表 51-18　相関イベントの検索基準（続き）

フィールド	検索基準の規則
Security Intelligence Category	ポリシー違反をトリガーとして使用した相関イベントに関連付けられたセキュリティ インテリジェンスのカテゴリを指定します。セキュリティ インテリジェンスのカテゴリとして、セキュリティ インテリジェンス オブジェクト、グローバル ブラックリスト、カスタム セキュリティー インテリジェンス リストまたはフィード、あるいはインテリジェンス フィードに含まれるいずれかのカテゴリを指定できます。詳細については、セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録（13-1 ページ）を参照してください。
Source IP、Destination IP、または Source/Destination IP	ポリシー違反をトリガーとして使用したイベントの送信元ホスト、宛先ホスト、または送信元/宛先ホストの IP アドレスを指定します。単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をコンマで区切ったリストを指定できます。また、否定を使用することもできます。詳細については、「検索での IP アドレスの指定（60-6 ページ）」を参照してください。
Source User または Destination User	ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホストにログインしたユーザを指定します。
Source Port/ICMP Type または Destination Port/ICMP Code	ポリシー違反をトリガーとして使用したイベントに関連付けられた、送信元トラフィックの送信元ポート/ICMP タイプまたは宛先トラフィックの宛先ポート/ICMP コードを指定します。
Impact	相関イベントに割り当てられた影響を指定します。大文字と小文字を区別しない有効な値は、`Impact 0`、`Impact Level 0`、`Impact 1`、`Impact Level 1`、`Impact 2`、`Impact Level 2`、`Impact 3`、`Impact Level 3`、`Impact 4`、および `Impact Level 4` です。影響アイコンの色や部分文字列（たとえば `blue`、`level 1`、`0` など）を使用しないでください。詳細については、影響レベルを使用してイベントを評価する（41-39 ページ）を参照してください。
Inline Result	侵入イベントによってトリガーとして使用されたポリシー違反の場合、以下のいずれかを入力します。 • dropped は、インライン型、スイッチ型、またはルーティング型展開でパケットがドロップされたかどうかを示します。 • would have dropped は仮定を表します。インライン型、スイッチ型、またはルーティング型展開でパケットをドロップするよう侵入ポリシーが設定されていると仮定した場合、パケットがドロップされるかどうかを示します。 侵入ポリシーのドロップ動作やルール状態とは無関係に、パッシブ展開（インライン セットがタップ モードである場合を含む）ではシステムがパケットをドロップしないことに注意してください。
Source Host Criticality または Destination Host Criticality	ポリシー違反に関連する送信元または宛先ホストの重要度として、`None`、`Low`、`Medium`、または `High` のいずれかを指定します。ディスカバリ イベント、ホスト入力イベント、または接続イベントに基づくルールによって生成された相関イベントにのみ、送信元ホスト重要度が含まれることに注意してください。ホストの重要度の詳細については、事前定義のホスト属性の使用（49-34 ページ）を参照してください。
Ingress Security Zone、Egress Security Zone、または Ingress/Egress Security Zone	ポリシー違反をトリガーとして使用した侵入イベントまたは接続イベントの入力、出力、または入力/出力セキュリティ ゾーンを指定します。

表 51-18　相関イベントの検索基準（続き）

フィールド	検索基準の規則
デバイス	ポリシー違反をトリガーしたイベントを生成した特定のデバイスに検索を制限するには、デバイス名または IP アドレス、またはデバイス グループ、スタック、またはクラスタ名を入力します。検索での FireSIGHT システムによるデバイス フィールドの処理方法については、検索でのデバイスの指定（60-7 ページ）を参照してください。
Ingress Interface または Egress Interface	ポリシー違反をトリガーとして使用した侵入イベントまたは接続イベントの入力または出力インターフェイスを指定します。

相関イベントを検索する方法：

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　テーブル ドロップダウン リストから [Correlation Events] を選択します。

ページが適切な制約によって更新されます。

ステップ 3　相関イベントの検索基準の表に示すように、該当するフィールドに検索基準を入力します。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「`A`」または「`B`」または「`C, D, E`」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク（*）を使用できます。
- 任意のフィールドで `n/a` を指定すると、そのフィールドの情報がないイベントを識別できます。一方、フィールドに情報があるイベントを識別すには `!n/a` を使用します。
- 検索条件としてオブジェクトを使用するには、検索フィールドの横にあるオブジェクト追加アイコン（ ✚ ）をクリックします。

検索でのオブジェクトの使用を含む、検索の構文の詳細については、イベントの検索（60-1 ページ）を参照してください。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　カスタム ユーザ ロールに関するデータ制約として検索を使用する予定の場合は、それをプライベート検索として保存する**必要があります**。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save As New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

現在の時間範囲によって制約されたデフォルト相関イベント ワークフローに、検索結果が表示されます。カスタム ワークフローなど別のワークフローを使用するには、ワークフロー タイトルの近くの [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

CHAPTER 52

FireSIGHT システムのコンプライアンス ツールとしての使用

コンプライアンス ホワイト リスト（または*ホワイト リスト*）は、一連の基準で、ユーザはこれを使用して、特定のサブネット上での実行を許可するオペレーティング システム、アプリケーション、およびプロトコルを指定できます。また、サブネット上のホストがホワイト リストに違反した場合、自動的にイベントが生成されます。たとえば、セキュリティ ポリシーで、Web サーバには HTTP の実行を許可するが、ネットワーク上の他のホストには許可しないように指定したとします。HTTP を実行しているホストを特定するために Web ファーム以外のネットワーク全体を評価するホワイト リストを作成できます。

次の条件でトリガーされるようにルールを設定することによって、この機能を実現する相関ルールを作成できます。

- システムがアプリケーション プロトコルに関する新しい情報を検出する
- アプリケーション プロトコルの名前は http である
- イベントに関係するホストの IP アドレスが Web ファーム内に存在しない

ただし、ネットワーク上のポリシー違反を警告して対処するためのより柔軟な方法を提供する相関ルールは、ホワイト リストよりも設定や保守が複雑です。また、相関ルールの方が対象範囲が広いうえ、複数のイベント タイプのいずれかが指定された条件を満たした段階で相関イベントを生成することができます。一方、ホワイト リストは、ネットワーク上で実行しているオペレーティング システム、アプリケーション プロトコル、クライアント、Web アプリケーション、およびプロトコルが組織のポリシーに違反していないかどうかの評価を支援するためのものです。

特定のニーズを満たすカスタム ホワイト リストを作成することも、オペレーティング システム、アプリケーション プロトコル、クライアント、Web アプリケーション、およびプロトコルを許可する場合の推奨設定を含む、Ciscoの脆弱性調査チーム（VRT）が作成したデフォルト ホワイト リストを使用することもできます。デフォルト ホワイト リストはネットワーク環境に合わせてカスタマイズすることもできます。

ホワイト リストをアクティブな相関ポリシーに追加すると、ホストがホワイト リストに違反していることをシステムが検出したときに、特別な種類の相関イベントであるホワイト リスト イベントがデータベースに記録されます。また、ホワイト リスト違反の検出時に自動的に応答（修復とアラート）をトリガーするようにシステムを設定できます。

注 NetFlow 対応デバイスによってエクスポートされたデータに基づいてホストとアプリケーション プロトコルをネットワーク マップに追加するようにネットワーク検出ポリシーを設定できますが、これらのホストとアプリケーション プロトコルに関して利用可能な情報が制限されます。たとえば、これらのホストのオペレーティング システム データは得られません（ただしホスト入力機能を使って指定する場合を除く）。これは、コンプライアンス ホワイト リストの作成方法に影響する場合があります。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

作成されたホワイト リストに準拠しているかどうかを示すホスト属性がホストごとに作成されるため、ネットワークの準拠の概要を把握できます。数秒で、ポリシーに違反して HTTP を実行している組織内のホストを正確に特定して適切に対処できます。

その後で、相関機能を使用して、Web ファーム内に存在しないホストが HTTP の実行を開始するたびに警告するようにシステムを設定できます。

加えて、ホスト プロファイルを使用して、個別のホストが設定されたホワイト リストに違反しているどうかと、ホストがどのようにホワイト リストに違反しているかを特定できます。FireSIGHT システムには、個別のホワイト リスト違反のそれぞれとホストあたりの違反数を表示可能なワークフローも含まれています。

最後に、ダッシュボードを使用して、ホワイト リスト イベントやネットワーク全体のホワイト リスト準拠の概要ビューを含む、最新のシステム規模の準拠活動を監視できます。

コンプライアンス ホワイト リストの作成および管理とホワイト リスト イベントおよび違反の解釈に関する詳細については、以下の項を参照してください。

- コンプライアンス ホワイト リストについて（52-3 ページ）
- コンプライアンス ホワイト リストの作成（52-9 ページ）
- コンプライアンス ホワイト リストの管理（52-26 ページ）
- 共有ホスト プロファイルの操作（52-27 ページ）
- ホワイト リスト イベントの操作（52-33 ページ）
- ホワイト リスト違反の処理（52-38 ページ）

加えて、以下の章と項で追加情報を参照してください。

- 相関ポリシーの作成（51-49 ページ）では、コンプライアンス ホワイト リストを含む相関ポリシーの作成方法と設定方法およびホワイト リストへの応答とプライオリティの割り当て方法について説明します。
- ホスト プロファイルの使用（49-1 ページ）では、ホストのプロファイルを使用してホワイト リストに違反しているかどうかを判断する方法について説明します。
- ダッシュボードの使用（55-1 ページ）では、ホワイト リスト準拠活動を含む、現在のシステム ステータスの概要を取得する方法について説明します。

コンプライアンス ホワイト リストについて

ライセンス：FireSIGHT

*コンプライアンス ホワイト リスト*は、ネットワーク上での実行を許可するオペレーティング システム、クライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルを指定する基準のセットです。特定のニーズを満たすカスタム ホワイト リストを作成することも、推奨設定を含む VRT によって作成されたデフォルト ホワイト リストを使用することもできます。

カスタム ホワイト リストの基準は単純にすることができます。特定のオペレーティング システムを実行しているホストのみを許可するように指定できます。基準は複雑にすることもできます。すべてのオペレーティング システムを許可するが、特定のオペレーティング システムを実行しているホストのみに特定のポート上での特定のアプリケーション プロトコルの実行を許可するように指定できます。

ホワイト リストは*ターゲット*と*ホスト プロファイル*という 2 つの主要部分で構成されます。ターゲットはホワイト リストによって評価される特定のホストであるのに対して、ホスト プロファイルはターゲット上での実行を許可するオペレーティング システム、クライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルを指定します。

ホワイト リストを作成してアクティブな相関ポリシーに追加すると、システムがホスト プロファイルに照らしてホワイト リストのターゲットを評価し、ホワイト リストに準拠しているかどうかを判断します。この初期評価後に、システムは有効なターゲットがホワイト リストに違反していることを検出した時点で*ホワイト リスト イベント*を生成します。

詳細については、次の項を参照してください。

- ホワイト リスト ターゲットについて（52-3 ページ）では、ホワイト リストがどのようにして指定されたホストのみを対象とするかを説明します。
- ホワイト リスト ホスト プロファイルについて（52-4 ページ）では、ネットワーク上での実行を許可するクライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルを記述したさまざまなプロファイルについて説明します。
- ホワイト リストの評価について（52-6 ページ）では、システムがどのようにネットワーク上のホストをホワイト リストに照らして評価するかと、準拠しているホストと準拠していないホストの区別方法について説明しています。
- ホワイト リスト違反について（52-7 ページ）では、システムがどのようにホワイト リスト違反を検出し、通知するかについて説明します。

ホワイト リスト ターゲットについて

ライセンス：FireSIGHT

ホワイト リストを作成する場合は、最初にそれを適用するネットワークの部分を指定します。ホワイト リストを使用してモニタリング対象ネットワーク上のすべてのホストを評価することも、特定のネットワーク セグメントまたは個別のホストのみを評価するようにホワイト リストを制限することもできます。特定のホスト属性を持っている、または、特定の VLAN に属しているホストのみを評価するようにさらにホワイト リストを制限できます。ホワイト リストの評価対象となるホストは、*有効なターゲット*（または*ターゲット*）と呼ばれます。有効なターゲットは次のようなものです。

- 指定された IP アドレス ブロックのいずれかに含まれている必要があります。IP アドレスのブロックを除外することもできます。

- 指定されたホスト属性を 1 つ以上持っている必要があります。

  たとえば、ホスト重要度の高いホストのみを評価するようにホワイト リストを設定できます。ホスト重要度を含むホスト属性の詳細については、ユーザ定義のホスト属性の使用（49-35 ページ）と事前定義のホスト属性の使用（49-34 ページ）を参照してください。

- 指定された VLAN のいずれかに属している必要があります。

ホストがこれらの基準のすべてを満たしていない場合は、そのホスト プロファイルがホワイト リストに違反しているかどうかに関係なく、ホワイト リストに照らして評価されません。

ホワイト リストに複数のターゲットが含まれている場合、その中のいずれか 1 つのみで指定された条件を満たしていれば、ホストは有効と見なされます。たとえば、10.10.x.x ネットワークを含むターゲットと 10.10.x.x ネットワークを除外するターゲットを作成した場合、そのネットワークのホストは有効なターゲットと見なされます。ホワイト リストにターゲットが含まれていない場合は、ネットワーク上のどのホストもホワイト リストに照らして評価されないことに注意してください。

ホワイト リストのターゲット ネットワークは、[Create White List] ページの左側に一覧表示されます。デフォルト ホワイト リストではモニタリング対象ネットワークの全体を表す 0.0.0.0/0 と ::/0 のターゲットが使用されることに注意してください。このホワイト リストを使用する場合は、ターゲット ネットワークを現状のままにすることも、使用しているネットワーク環境を反映するように変更することもできます。

ホワイト リスト ターゲットの作成方法については、コンプライアンス ホワイト リスト ターゲットの設定（52-12 ページ）を参照してください。

ホワイト リスト ホスト プロファイルについて

ライセンス：FireSIGHT

ホワイト リストで評価するターゲットを指定したら、次のステップは*ホスト プロファイル*の設定です。ホワイト リスト内のホスト プロファイルは、ターゲット ホスト上での実行を許可するオペレーティング システム、クライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルを指定します。

ホワイト リストで設定可能なホスト プロファイルには 3 つの種類（グローバル ホスト プロファイル、特定のオペレーティング システム用のホスト プロファイル、および共有ホスト プロファイル）があります。ホワイト リストの作成中、それぞれのタイプのホスト プロファイルは異なって表示されます。

次の表に、異なる種類のホスト プロファイルの識別方法とアクセス方法の説明を示します。

表 52-1　コンプライアンス ホワイト リスト ホスト プロファイルへのアクセス

表示対象	[Allowed Host Profiles] でのクリック対象
ホワイト リストのグローバル ホスト プロファイル	**任意のオペレーティング システム**
特定のオペレーティング システム用のホスト プロファイル	斜体ではなく、プレーン テキストで表記されたホスト プロファイル名
ホワイト リストで使用される共有ホスト プロファイル	斜体で表記されたホスト プロファイル名

詳細については、次の項を参照してください。

- グローバル ホスト プロファイルについて（52-5 ページ）
- 特定のオペレーティング システム用のホスト プロファイルについて（52-5 ページ）
- 共有ホスト プロファイルについて（52-6 ページ）

グローバル ホスト プロファイルについて

ライセンス：FireSIGHT

すべてのホワイト リストに、ホストのオペレーティング システムに関係なく、ターゲット ホスト上での実行を許可されたアプリケーション プロトコル、クライアント、Web アプリケーション、およびプロトコルを指定するグローバル ホスト プロファイルが含まれています。

たとえば、Internet Explorer を許可するように複数の Microsoft Windows ホスト プロファイルと Linux ホスト プロファイルを編集する代わりに、検出されたオペレーティング システムに関係なく、Internet Explorer を許可するようにグローバル ホスト プロファイルを設定できます。ARP、IP、TCP、および UDP の各プロトコルは、常に、すべてのホスト上での実行が許可されることに注意してください。これらを禁止することはできません。詳細については、グローバル ホスト プロファイルの設定（52-15 ページ）を参照してください。

特定のオペレーティング システム用のホスト プロファイルについて

ライセンス：FireSIGHT

ネットワーク上での実行を許可するオペレーティング システムごとに 1 つのホスト プロファイルを作成する必要があります。ネットワーク上でオペレーティング システムを禁止する場合は、そのオペレーティング システム用のホスト プロファイルを作成しません。たとえば、ネットワーク上のすべてのホストで Microsoft Windows が実行されるようにするには、そのオペレーティング システム用のホスト プロファイルのみを含めるようにホワイト リストを設定します。

特定のオペレーティング システム用のホスト プロファイルを作成するときに、特定のバージョンに限定することもできます。たとえば、準拠ホストが Windows 7 または Windows Server 2008 R2 を実行する必要があると指定できます。

特定のオペレーティング システム用のホスト プロファイルを作成したら、そのオペレーティング システムを実行しているターゲット ホスト上での実行を許可するアプリケーション プロトコル、クライアント、Web アプリケーション、およびプロトコルを指定できます。たとえば、Linux ホストのポート 22 での SSH の実行を許可することができます。また、特定のベンダーとバージョンを OpenSSH 4.2 に限定することもできます。

未確認ホストは、確認されるまで、すべてのホワイト リストに準拠していると見なされることに注意してください。ただし、不明ホストのホワイト リスト ホスト プロファイルを作成することはできます。

注　未確認ホストと不明ホストは違います。*未確認*ホストは、オペレーティング システムを識別するために十分な情報が収集されていないホストです。*不明*ホストは、トラフィックがシステムによって分析されているが、オペレーティング システムが既知のフィンガープリントのいずれとも一致しないホストです。

詳細については、特定のオペレーティング システム用のホスト プロファイルの作成（52-16 ページ）を参照してください。

共有ホスト プロファイルについて

ライセンス：FireSIGHT

共有ホスト プロファイルは特定のオペレーティング システムに関連付けられますが、それぞれの共有ホスト プロファイルを複数のホワイト リスト内で使用できます。つまり、複数のホワイト リストを作成するが、同じホスト プロファイルを使用して複数のホワイト リストで特定のオペレーティング システムを実行するホストを評価する場合は、共有のホスト プロファイルを使用します。

たとえば、世界中にオフィスがあり、拠点ごとに別々のホワイト リストを作成したうえで、Apple Mac OS X を実行しているすべてのホストに対しては常に同じプロファイルを使用する場合に、そのオペレーティング システム用の共有プロファイルを作成して、それをすべてのホワイト リストで使用します。

デフォルト ホワイト リストは、オペレーティング システム、クライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルを許可する場合に推奨される「ベスト プラクティス」設定を意味します。このホワイト リストでは、*組み込みホスト プロファイル*と呼ばれる特殊なカテゴリの共有ホスト プロファイルが使用されます。組み込みホスト プロファイルには組み込みホスト プロファイル アイコン（）が付けられることに注意してください。

組み込みホスト プロファイルでは、組み込みアプリケーション プロトコル、プロトコル、およびクライアントが使用されます。これらの要素は、デフォルト ホワイト リストと作成されたカスタム ホワイト リストの両方でそのまま使用することも、必要に応じて変更することもできます。また、これらの要素は、組み込みホスト プロファイルおよびそれらの要素を使用するその他すべてのホスト プロファイル内で斜体で表示されます。

共有ホスト プロファイルと同様に、組み込みホスト プロファイルを変更した場合は、それが使用されているすべてのホワイト リストに影響することに注意してください。同様に、組み込みアプリケーション プロトコル、プロトコル、またはクライアントを変更した場合は、それが使用されているすべてのホワイト リストに影響します。

共有ホスト プロファイルの詳細については、共有ホスト プロファイルの操作（52-27 ページ）を参照してください。

ホワイト リストの評価について

ライセンス：FireSIGHT

ホワイト リスト ホスト プロファイルを作成してホワイト リストを保存したら、相関ルールと同様に、ホワイト リストを相関ポリシーに追加できます。詳細については、相関ポリシーおよび相関ルールの設定（51-1 ページ）を参照してください。

相関ポリシーをアクティブにすると、システムがホワイト リストの条件に照らしてホワイト リストのターゲットを評価します。その後で、ホスト属性ネットワーク マップを使用して、ネットワーク上のホストのホワイト リスト準拠の全体像を把握できます。

ネットワーク上のすべてのホストに、ホワイト リストと同じ名前のホスト属性が割り当てられます。このホスト属性に次のいずれかの値が付与されます。

- [Compliant] ホワイト リストに準拠する有効なターゲットの場合
- [Non-Compliant] ホワイト リストに違反する有効なターゲットの場合
- [Not Evaluated] 何らかの理由で評価されていない無効なターゲットとホストの場合

ネットワークが大規模で、システムがネットワーク マップ内のすべての有効なターゲットをホワイト リストに照らして評価している途中の場合は、まだ評価されていないターゲットが [Not Evaluated] としてマークされることに注意してください。システムが処理を完了すると、さらに多くのホストが [Not Evaluated] から [Compliant] または [Non-Compliant] のいずれかに移行します。システムは 1 秒あたり約 100 ホストを評価できます。

加えて、ホストが準拠しているかどうかを判断するのに十分な情報が収集されていない場合は、ホストが [Not Evaluated] としてマークされます。たとえば、この状態は、新しいホストが検出されたが、そのホスト上で実行されているオペレーティング システム、クライアント、アプリケーション プロトコル、Web アプリケーション、またはプロトコルに関連した情報が収集されていない場合に発生します。

注　ホストでホスト属性が変更または削除され、その変更または削除がホストが有効なターゲットでなくなったことを意味する場合、そのホストは [Compliant] または [Non-Compliant] から [Not Evaluated] に移行されます。

ホスト属性の詳細については、ホスト属性のネットワーク マップの使用（48-10 ページ）を参照してください。

ホワイト リスト違反について

ライセンス： FireSIGHT

ホワイト リストの初期評価後に、システムは有効なターゲットがホワイト リストに違反していることを検出した時点で*ホワイト リスト イベント*を生成します。ホワイト リスト イベントは、相関イベントの特殊な形態で、Defense Center相関イベント データベースに記録されます。ワークフロー内のホワイト リスト イベントを表示したり、特定のホワイト リスト イベントを検索したりできます。詳細については、ホワイト リスト イベントの操作（52-33 ページ）を参照してください。

ホワイト リスト違反は、ホストが準拠していないことを示すイベントが生成されたときに発生します。同様に、検出イベントによって非準拠だったホストが準拠に移行したことが示される場合がありますが、この場合システムではホワイト リスト イベントを生成**しません**。

次のイベントはホストの準拠に影響を与える可能性があります。

- システムがホストのオペレーティング システムの変更を検出
- システムがホストのオペレーティング システムまたはホスト上のアプリケーション プロトコルのアイデンティティ競合を検出
- システムがホスト上でアクティブになっている新しい TCP サーバ ポート（SMTP または Web サーバによって使用されるポートなど）、または、ホスト上で実行中の新しい UDP サーバを検出
- システムが、ホスト上で実行中の検出された TCP または UDP サーバで、アップグレードのためのバージョン変更などの変更を検出
- システムがホスト上で実行中の新しいクライアントを検出
- システムが非アクティブという理由でデータベースからクライアントをドロップ
- システムがホスト上で実行中の新しい Web アプリケーションを検出
- システムが非アクティブという理由でホスト プロファイルから Web アプリケーションをドロップ

- システムが、ホストが Novell NetWare や IPv6 などの新しいネットワーク プロトコルまたは ICMP や EGP などの新しい転送プロトコルで通信中であることを検出
- システムがジェイルブレイクされた新しいモバイル デバイスを検出
- システムが TCP または UDP ポートがホスト上で閉じられたか、タイムアウトしたことを検出

加えて、ホスト入力機能またはホスト プロファイルを使用して次の操作を実行することによって、ホストの準拠の変化をトリガーできます。

- ホストにクライアント、プロトコル、またはサーバを追加する
- ホストからクライアント、プロトコル、またはサーバを削除する
- ホストのオペレーティング システム定義を設定する
- ホストが有効なターゲットでなくなるようにホストのホスト属性を変更する

たとえば、ホワイト リストで Microsoft Windows ホストのみをネットワーク上で許可するように指定されている場合は、ホストが現在 Mac OS X を実行していることをシステムが検出したときに、ホワイト リスト イベントが生成されます。加えて、ホワイト リストに関連付けられたホスト属性の値が [Compliant] から [Non-Compliant] に変更されます。

この例のホストが準拠に復帰するには、次のいずれかが行われる必要があります。

- Mac OS X オペレーティング システムを許可するようにホワイト リストを編集する
- ホストのオペレーティング システム定義を手動で Microsoft Windows に変更する
- オペレーティング システムが Microsoft Windows に戻ったことをシステムが検出する

いずれの場合も、ホワイト リストに関連付けられたホスト属性の値が [Non-Compliant] から [Compliant] に変更されます。

別の例として、コンプライアンス ホワイト リストで FTP の使用が禁止されている状態で、アプリケーション プロトコル ネットワーク マップまたはイベント ビューから FTP が削除された場合は、FTP を実行中のホストが準拠になります。ただし、システムがアプリケーション プロトコルをもう一度検出すると、ホワイト リスト イベントが生成され、ホストは非準拠になります。

システムがホワイト リストに関する情報が不十分なイベントを生成した場合は、ホワイト リストがトリガーされないことに注意してください。たとえば、ホワイト リストでポート 21 上の TCP FTP トラフィックのみを許可するように指定されているシナリオについて考えてみます。この場合、システムは、TCP プロトコルを使用しているポート 21 がホワイト リスト ターゲットのいずれかでアクティブになっていることを検出しますが、トラフィックが FTP かどうかを判断することはできません。このシナリオでは、システムがトラフィックを FTP 以外のトラフィックとして識別するか、またはユーザがホスト入力機能を使用してトラフィックを非 FTP トラフィックとして指定するまで、ホワイト リストがトリガーされません。

注　ホワイト リストの初期評価中は、システムは非準拠ホストに関するホワイト リスト イベントを生成**しません**。すべての非準拠ターゲットに対してホワイト リスト イベントを生成する場合は、Defense Center データベースを消去する必要があります。これにより、ネットワークと関連クライアント上のホスト、アプリケーション プロトコル、Web アプリケーション、およびプロトコルが再検出され、ホワイト リスト イベントがトリガーされます。詳細については、データベースからの検出データの消去（B-1 ページ）を参照してください。

最後に、ホワイト リスト違反を検出したときに自動的に応答をトリガーとして使用するようにシステムを設定できます。応答には、修復（Nmap スキャンの実行など）、アラート（電子メール、SNMP、および syslog アラート）、またはアラートと修復の組み合わせが含まれます。詳細については、ルールとホワイトリストに応答を追加する（51-52 ページ）を参照してください。

コンプライアンス ホワイト リストの作成

ライセンス：FireSIGHT

ホワイト リストを作成するときに、ネットワーク全体または特定のネットワーク セグメントを調査できます。ネットワークを調査すると、システムがネットワーク セグメント上で検出したオペレーティング システムごとに 1 つずつのホスト プロファイルでホワイト リストが生成されます。デフォルトで、これらのホスト プロファイルは、システムが該当するオペレーティング システム上で検出したクライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルのすべてを許可します。

次に、ホワイト リストのターゲットを指定する必要があります。モニタリング対象のネットワーク上のすべてのホストを評価するようにホワイト リストを設定することも、特定のネットワーク セグメントまたは個別のホストのみを評価するようにホワイト リストを制限することもできます。特定のホスト属性を持っている、または、特定の VLAN に属しているホストのみを評価するようにさらにホワイト リストを制限できます。ネットワークを調査すると、デフォルトで、調査したネットワーク セグメントがホワイト リスト ターゲットになります。調査したネットワークを編集または削除したり、新しいターゲットを追加したりできます。

その後で、準拠ホストを示すホスト プロファイルを作成します。ホワイト リスト内のホスト プロファイルは、ターゲット ホスト上での実行を許可するオペレーティング システム、クライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルを指定します。グローバル ホスト プロファイルの設定、実施したネットワーク調査によって作成されたホスト プロファイルの編集、新しいホスト プロファイルの追加、および共有ホスト プロファイルの追加と編集を行うことができます。

最後に、ホワイト リストを保存して、それをアクティブな相関ポリシーに追加します。システムは、ターゲット ホストの準拠の評価、ホストがホワイト リストに違反した場合のホワイト リスト イベントの生成、およびホワイト リスト違反に対して設定された応答のトリガーを開始します。コンプライアンス ホワイト リストの詳細については、コンプライアンス ホワイト リストについて（52-3 ページ）を参照してください。

ヒント　ホストのテーブル ビューからホワイト リストを作成することもできます。詳細については、選択したホストに基づいたコンプライアンスのホワイト リストの作成（50-26 ページ）を参照してください。

コンプライアンス ホワイト リストを作成する方法：

アクセス：Admin

ステップ 1　[Policies] > [Correlation] の順に選択してから、[White List] をクリックします。

[White List] ページが表示されます。

ステップ 2　[New White List] をクリックします。

[Survey Network] ページが表示されます。

ステップ 3　オプションで、ネットワークを調査します。

- ネットワークを調査するには、ネットワークの調査（52-10 ページ）を参照してください。
- ネットワークを調査せずにホワイト リストを作成するには、[Skip] をクリックして次のステップに進みます。

[Create White List] ページが表示されます。

ステップ 4　[Name] フィールドに、新しいホワイト リストの名前を入力します。

ステップ 5　[Description] フィールドに、ホワイト リストの簡単な説明を入力します。

ステップ 6　ネットワーク上でジェイルブレイクされたモバイル デバイスを許可するには、[Allow Jailbroken Mobile Devices] をオンにします。ジェイルブレイクされたデバイスをホワイト リストで評価することによってホワイト リスト違反を発生させる場合は、このオプションをオフにします。

ステップ 7　ホワイト リストのターゲットを指定します。ネットワーク調査により作成されたターゲットを編集または削除するだけでなく、新しいターゲットを追加することもできます。オプションで、ホスト属性または VLAN ID に基づいてさらにターゲットを制限します。詳細については、コンプライアンス ホワイト リスト ターゲットの設定（52-12 ページ）を参照してください。

ステップ 8　準拠ホストを示すホスト プロファイルを作成します。グローバル ホスト プロファイルの設定、ネットワーク調査によって作成されたホスト プロファイルの編集、新しいホスト プロファイルの追加、および共有ホスト プロファイルの追加と編集を行うことができます。詳細については、コンプライアンス ホワイト リスト ホスト プロファイルの設定（52-14 ページ）を参照してください。

ステップ 9　ホワイト リストを保存するには、[Save White List] をクリックします。

ホワイト リストが保存されます。これで、ホワイト リストをアクティブな相関ポリシーに追加して、ターゲット ホストの準拠の評価、ホストがホワイト リストに違反した場合のホワイト リスト イベントの生成、およびオプションのホワイト リスト違反に対する応答のトリガーを開始できます。詳細については、相関ポリシーの作成（51-49 ページ）を参照してください。

ネットワークの調査

ライセンス： FireSIGHT

コンプライアンス ホワイト リストの作成を開始するときに、ネットワーク全体または特定のネットワーク セグメントを調査できます。

ネットワークの調査で、検出されたさまざまなオペレーティング システム上で実行中のアプリケーション プロトコル、クライアント、Web アプリケーション、およびプロトコルに関するデータがデータベースから収集されます。その後で、システムがホワイト リストに検出したオペレーティング システムごとに 1 つずつのホスト プロファイルを作成します。デフォルトで、これらのホスト プロファイルは、システムが該当するオペレーティング システム上で検出したクライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルのすべてを許可します。

これにより、ベースライン ホワイト リストが作成されるため、手動で複数のホスト プロファイルを作成して設定する必要がありません。ネットワークを調査したら、調査によりニーズに合わせて作成されたホスト プロファイルを編集または削除できます。必要なその他のホスト プロファイルを追加することもできます。

ホワイト リストの作成プロセス中はいつでもネットワークを調査できることに注意してください。これにより、新しく許可したクライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルを既存のホスト プロファイルに追加したり、初期調査で検出されなかったオペレーティング システムを実行中のホストが今回の調査で検出された場合に追加のホスト プロファイルを作成したりできます。アクティブな相関ポリシーで使用されているホワイト リスト内のネットワークを再調査して、ターゲットとホスト プロファイルのどちらかが変更された場合は、ホワイト リストの保存時にターゲット ホストが再評価されます。この再評価で一部のホストが準拠に移行したとしても、ホワイト リスト イベントは生成されません。

ネットワークを調査することによって、コンプライアンス ホワイト リストの作成を開始する方法:

アクセス: Admin

ステップ 1　[Policies] > [Correlation] の順に選択してから、[White List] をクリックします。

[White List] ページが表示されます。

ステップ 2　[New White List] をクリックします。

[Survey Network] ページが表示されます。

ステップ 3　ネットワークを調査しますか。

- **はい**の場合は、次のステップに進みます。
- **いいえ**の場合は、[Skip] をクリックします。

  [Create White List] ページが開いて、空白のホワイト リストが表示されます。次の項（基本的なホワイト リスト情報の提供）の手順に進みます。

ステップ 4　[IP Address] フィールドと [Netmask] フィールドに、調査するホストを表す IP アドレスとネットワーク マスクを（CIDR などの特殊な表記で）入力します。

ネットワーク検出ポリシーで監視するようにシステムを設定したネットワークを指定したことを確認します。FireSIGHT システムで使用する IP アドレス表記については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ヒント　モニタリング対象のネットワーク全体を調査するには、デフォルト値の `0.0.0.0/0` と `::/0` を使用します。

ステップ 5　[OK] をクリックします。

[Create White List] ページが表示されます。

ホワイト リストは事前設定されています。そのターゲットは調査したネットワーク上のホストであり、許可されるホスト プロファイルはターゲットのプロファイルです。

ステップ 6　追加のネットワークを調査するには、[Target Network] をクリックし、調査する追加のネットワークごとにステップ 4 と 5 を繰り返します。

追加のネットワークの調査で、新しく許可したクライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルを既存のホスト プロファイルに追加したり、初期調査で検出されなかったオペレーティング システムを実行中のホストが今回の調査で検出された場合に追加のホスト プロファイルを作成したりできます。また、調査したネットワーク セグメント内のホストを表すホワイト リストにターゲットを追加することもできます。このターゲットは、後で、編集または削除することができます。

ステップ 7　次の項基本的なホワイト リスト情報の提供に進みます。

基本的なホワイト リスト情報の提供

ライセンス: FireSIGHT

ホワイト リストごとに名前と簡単な説明（オプション）を入力する必要があります。加えて、ジェイルブレイクされたモバイル デバイスによってホワイト リスト違反が発生するかどうかを選択できます。

基本的なホワイト リスト情報を提供する方法：

アクセス：Admin

ステップ 1　[Name] フィールドに、新しいホワイト リストの名前を入力します。

ステップ 2　[Description] フィールドに、ホワイト リストの簡単な説明を入力します。

ステップ 3　ネットワーク上でジェイルブレイクされたモバイル デバイスを許可するには、[Allow Jailbroken Mobile Devices] をオンにします。ジェイルブレイクされたデバイスをホワイト リストで評価することによってホワイト リスト違反を発生させる場合は、このオプションをオフにします。

ステップ 4　次の項コンプライアンス ホワイト リスト ターゲットの設定に進みます。

コンプライアンス ホワイト リスト ターゲットの設定

ライセンス：FireSIGHT

コンプライアンス ホワイト リストを作成するときに、それを適用するネットワークの部分を指定する必要があります。ホワイト リストを使用してモニタリング対象ネットワーク上のすべてのホストを評価することも、特定のネットワーク セグメントまたは個別のホストのみを評価するようにホワイト リストを制限することもできます。特定のホスト属性を持っている、または、特定の VLAN に属しているホストのみを評価するようにさらにホワイト リストを制限できます。ホワイト リストの評価対象になるホストは、ターゲットと呼ばれます。ホワイト リスト ターゲットの詳細については、ホワイト リスト ターゲットについて（52-3 ページ）を参照してください。

コンプライアンス ホワイト リスト ターゲットの作成が完了したら、コンプライアンス ホワイト リスト ホスト プロファイルの設定（52-14 ページ）に進みます。

注　ホストのホスト属性を変更または削除した結果、ホストが有効なターゲットではなくなった場合、そのホストはホワイト リストに照らして評価されなくなり、準拠でも非準拠でもないと見なされます。

ターゲットの変更方法と削除方法については、以下を参照してください。

- 既存のターゲットの変更（52-14 ページ）
- 既存のターゲットの削除（52-14 ページ）

コンプライアンス ホワイト リストのターゲットを作成するときに、ホストがホワイト リストに照らして評価されるための基準を指定します。有効なターゲットは次のようなものです。

- 指定された IP アドレス ブロックのいずれかに含まれている必要があります。IP アドレスのブロックを除外することもできます。
- 指定されたホスト属性を 1 つ以上持っている必要があります。
- 指定された VLAN のいずれかに属している必要があります。

アクティブな相関ポリシーで使用されているホワイト リストにターゲットを追加した場合は、ホワイト リストの保存後に新しいターゲット ホストの準拠が評価されることに注意してください。ただし、この評価でホワイト リスト イベントは生成されません。

コンプライアンス ホワイト リスト ターゲットを作成する方法:

アクセス: Admin

ステップ 1　[Create White List] ページで、[Target Networks] の横にある追加アイコン( )をクリックします。

新しいターゲットの設定が表示されます。

ヒント　ネットワーク セグメントを調査することによって新しいターゲットを作成することもできます。[Create White List] ページで、[Target Network] をクリックしてから、ネットワークの調査（52-10 ページ）のステップ 4 と 5 を実行します。新しいターゲットが作成され、指定された IP アドレスに基づいて名前が付けられます。作成したターゲットをクリックし、残りの手順に進んでターゲットの名前を変更したり、新しいネットワークを追加または除外したり、ホスト属性または VLAN 制限を追加したりします。

ステップ 2　[Name] フィールドに、新しいターゲットの名前を入力します。

ステップ 3　[Targeted Networks] の横にある追加アイコン( )をクリックして、特定の IP アドレスのセットをターゲットにします。

ステップ 4　[IP Address] フィールドと [Netmask] フィールドに、ターゲットにするまたはターゲットから除外するホストを表す IP アドレスとネットワーク マスクを（CIDR などの特殊な表記で）入力します。

ネットワーク検出ポリシーで監視するようにシステムを設定したネットワークを指定したことを確認する必要があります。FireSIGHT システムで使用する IP アドレス表記については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ヒント　モニタリング対象のネットワーク全体をターゲットにするには、`0.0.0.0/0` と `::/0` を使用します。

ステップ 5　ネットワークをモニタリング対象から除外する場合は、[Exclude] を選択します。

ステップ 6　追加のネットワークを追加するには、ステップ 4 と 5 を繰り返します。

ステップ 7　[Targeted Host Attributes] の横にある [Add] をクリックして、特定のホスト属性を持つホストをターゲットにします。

ステップ 8　[Attribute] と [Value] の各ドロップダウンリストから、ホスト属性を指定します。

ステップ 9　追加のホスト属性を追加するには、ステップ 7 と 8 を繰り返します。

ホストには、ホワイト リストに照らして評価される 1 つ以上のホスト属性を指定する必要があります。

ステップ 10　[Targeted VLANs] の横にある [Add] をクリックして、特定の VLAN に属しているホストをターゲットにします。

ステップ 11　[VLAN ID] フィールドで、ホワイト リストに照らして評価するホストの VLAN ID を指定します。これは、802.1q VLAN 用の 0 ～ 4095 の任意の整数にすることができます。

ステップ 12　追加の VLAN ID を追加するには、ステップ 10 と 11 を繰り返します。

ホストは、ホワイト リストに照らして評価するように指定された VLAN のいずれかのメンバーである必要があります。

ヒント　ネットワーク、ホスト属性制限、または VLAN 制限を削除するには、削除する要素の横にある削除アイコン( )をクリックします。

既存のターゲットの変更

ライセンス：FireSIGHT

ターゲットを変更したら、その変更を反映させるためにホワイト リストを保存する必要があります。アクティブな相関ポリシーで使用されているホワイト リスト内のターゲットを変更した場合は、ホワイト リストの保存後に新しいターゲット ホストの準拠が評価されることに注意してください。ただし、この評価でホワイト リスト イベントは生成されません。加えて、システムが有効だったターゲットのホワイト リスト ホスト属性を [Not Evaluated] に変更します。

既存のターゲットを変更する方法：

アクセス：Admin

ステップ 1　[Create White List] ページの [Targets] で、変更するターゲットをクリックします。

ターゲットの設定が表示されます。

ステップ 2　必要に応じて変更を加えます。

ターゲットの名前を変更したり、新しいネットワークを追加または除外したり、ホスト属性または VLAN 制限を追加したりできます。詳細については、コンプライアンス ホワイト リスト ターゲットの設定（52-12 ページ）を参照してください。

既存のターゲットの削除

ライセンス：FireSIGHT

ターゲットを削除したら、その変更を反映させるためにホワイト リストを保存する必要があります。アクティブな相関ポリシーで使用されているホワイト リストからターゲットを削除した場合は、システムが有効だったターゲットのホワイト リスト ホスト属性を [Not Evaluated] に変更することに注意してください。

ホワイト リスト ターゲットを削除する方法：

アクセス：Admin

ステップ 1　削除するターゲットの横にある削除アイコン（ ）をクリックします。

ステップ 2　プロンプトが表示されたら、ターゲットの削除を確認します。

ターゲットが削除されます。

コンプライアンス ホワイト リスト ホスト プロファイルの設定

ライセンス：FireSIGHT

コンプライアンス ホワイト リスト内のホスト プロファイルは、ターゲット ホスト上での実行を許可するオペレーティング システム、クライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルを指定します。ホワイト リストで設定可能なホスト プロファイルには次の 3 つの種類があります。

- ホストのオペレーティング システムに関係なく、ターゲット ホスト上での実行を許可するアプリケーション プロトコル、クライアント、Web アプリケーション、およびプロトコルを指定するグローバル ホスト プロファイル
- ネットワーク上での実行を許可するオペレーティング システムだけでなく、それらのオペレーティング システム上での実行を許可するアプリケーション プロトコル、クライアント、Web アプリケーション、およびプロトコルも指定する特定のオペレーティング システム用のホスト プロファイル
- 単一のホワイト リストに関連付けられないことを除いて、特定のオペレーティング システム用のホスト プロファイルとまったく同様に機能する共有ホスト プロファイル。これは、複数のホワイト リストで使用できます。

ホワイト リスト ホスト プロファイルの詳細については、ホワイト リスト ホスト プロファイルについて（52-4 ページ）を参照してください。

コンプライアンス ホワイト リスト ホスト プロファイルの作成が完了したら、ホワイト リストをアクティブな相関ポリシーに追加して、ターゲット ホストの準拠の評価、ホストがホワイト リストに違反した場合のホワイト リスト イベントの生成、およびオプションでホワイト リスト違反に基づく応答のトリガーを開始できます。

コンプライアンス ホワイト リスト ホスト プロファイルの作成方法、変更方法、および削除方法については、以下を参照してください。

- グローバル ホスト プロファイルの設定（52-15 ページ）
- 特定のオペレーティング システム用のホスト プロファイルの作成（52-16 ページ）
- コンプライアンス ホワイト リストへの共有ホスト プロファイルの追加（52-21 ページ）
- 既存のホスト プロファイルの変更（52-22 ページ）
- 既存のホスト プロファイルの削除（52-25 ページ）

グローバル ホスト プロファイルの設定

ライセンス： FireSIGHT

すべてのホワイト リストに、ホストのオペレーティング システムに関係なく、ターゲット ホスト上での実行を許可されたアプリケーション プロトコル、クライアント、Web アプリケーション、およびプロトコルを指定するグローバル ホスト プロファイルが含まれています。グローバル ホスト プロファイルの詳細については、グローバル ホスト プロファイルについて（52-5 ページ）を参照してください。

グローバル ホスト プロファイルを設定する方法：

アクセス： Admin

ステップ 1　[Create White List] ページの [Allowed Host Profiles] で、[Any Operating System] をクリック します。

グローバル ホスト プロファイルの設定が表示されます。

ステップ 2　許可するアプリケーション プロトコルを指定するには、ホスト プロファイルへのアプリケーション プロトコルの追加（52-17 ページ）の指示に従ってください。

ステップ 3　許可するクライアントを指定するには、ホスト プロファイルへのクライアントの追加（52-18 ページ）の指示に従ってください。

ステップ 4　許可する Web アプリケーションを指定するには、ホスト プロファイルへの Web アプリケーションの追加（52-20 ページ）の指示に従ってください。

ステップ 5　許可するプロトコルを指定するには、ホスト プロファイルへのプロトコルの追加（52-20 ページ）の指示に従ってください。

ARP、IP、TCP、および UDP は常に許可されることに注意してください。

特定のオペレーティング システム用のホスト プロファイルの作成

ライセンス： FireSIGHT

特定のオペレーティング システム用のホスト プロファイルは、ネットワーク上での実行を許可するオペレーティング システムだけでなく、それらのオペレーティング システム上での実行を許可するアプリケーション プロトコル、クライアント、Web アプリケーション、およびプロトコルも指定します。詳細については、特定のオペレーティング システム用のホスト プロファイルについて（52-5 ページ）を参照してください。

特定のオペレーティング システム用の新しいコンプライアンス ホワイト リスト ホスト プロファイルを作成する方法：

アクセス： Admin

ステップ 1　[Allowed Host Profiles] の横にある追加アイコン（  ）をクリックします。

新しいホスト プロファイルの設定が表示されます。

ステップ 2　[Name] フィールドに、ホスト プロファイルの分かりやすい名前を入力します。

ステップ 3　[OS Vendor]、[OS Name]、および [Version] の各ドロップダウンリストから、ホスト プロファイルを作成するオペレーティング システムとバージョンを選択します。

ステップ 4　許可するアプリケーション プロトコルを指定します。次の 3 つのオプションがあります。

- すべてのアプリケーション プロトコルを許可するには、[Allow all Application Protocols] チェック ボックスをオンのままにします。
- どのアプリケーション プロトコルも許可しない場合は、[Allow all Application Protocols] チェック ボックスをオフにします。
- 特定のアプリケーション プロトコルを許可するには、ホスト プロファイルへのアプリケーション プロトコルの追加（52-17 ページ）の指示に従ってください。

ステップ 5　許可するクライアントを指定します。次の 3 つのオプションがあります。

- すべてのクライアントを許可するには、[Allow all Clients] チェック ボックスをオンのままにします。
- どのクライアントも許可しない場合は、[Allow all Clients] チェック ボックスをオフにします。
- 特定のクライアントを許可するには、ホスト プロファイルへのクライアントの追加（52-18 ページ）の指示に従ってください。

ステップ 6　許可する Web アプリケーションを指定します。次の 3 つのオプションがあります。

- すべての Web アプリケーションを許可するには、[Allow all Web Applications] チェック ボックスをオンのままにします。
- どの Web アプリケーションも許可しない場合は、[Allow all Web Applications] チェック ボックスをオフにします。
- 特定の Web アプリケーションを許可するには、ホスト プロファイルへの Web アプリケーションの追加（52-20 ページ）の指示に従ってください。

ステップ 7　許可するプロトコルを指定します。

プロトコルを追加するには、[Allowed Protocols] の横で、ホスト プロファイルへのプロトコルの追加（52-20 ページ）の手順に従ってください。ARP、IP、TCP、および UDP は常に許可されることに注意してください。

ホスト プロファイルへのアプリケーション プロトコルの追加

ライセンス： FireSIGHT

コンプライアンス ホワイト リストは、共有ホスト プロファイル、または単一のホワイト リストに属しているホスト プロファイルのいずれかを使用して、特定のオペレーティング システム上での特定のアプリケーション プロトコルの実行を許可するように設定できます。また、ホワイト リストは、有効な任意のターゲット上での特定のアプリケーション プロトコルの実行を許可するように設定できます。これは、グローバルに許可されたアプリケーション プロトコルと呼ばれます。

許可するアプリケーション プロトコルに関して、許可するアプリケーション プロトコルのタイプ（FTP と SSH がアプリケーション プロトコル タイプの例）を指定することも、アプリケーション プロトコル タイプに [any] を指定してカスタム アプリケーション プロトコルを許可することもできます。許可するアプリケーション プロトコルで使用されるプロトコル（TCP または UDP）を指定する必要もあります。任意のポートでアプリケーション プロトコルを許可することも、特定のポートに限定することもできます。

オプションで、アプリケーション プロトコル サーバのベンダーまたはバージョンを限定することができます。たとえば、Linux ホストのポート 22 での SSH の実行を許可することができます。また、特定のベンダーとバージョンを OpenSSH 4.2 に限定することもできます。

アプリケーション プロトコルをコンプライアンス ホワイト リスト ホスト プロファイルに追加する方法：

アクセス： Admin

ステップ 1　ホワイト リスト ホスト プロファイルを作成または変更しているときに、[Allowed Application Protocols]（または [Any Operating System] ホスト プロファイルを変更している場合は [Globally Allowed Application Protocols]）の横にある追加アイコン（  ）をクリックします。

ポップアップ ウィンドウが表示されます。一覧表示されるアプリケーション プロトコルは次のとおりです。

- ホワイト リスト内で作成したアプリケーション プロトコル
- ネットワークの調査（52-10 ページ）の説明に従ってネットワークを調査したときにネットワーク マップ内に存在したアプリケーション プロトコル
- ホワイト リスト内の他のホスト プロファイルによって使用されるアプリケーション プロトコル。これには、デフォルト ホワイト リストで使用するために VRT によって作成された組み込みアプリケーション プロトコルが含まれる場合があります。

ステップ 2　次の 2 つのオプションから選択できます。

- リスト内にすでに存在するアプリケーション プロトコルを追加するには、それを選択して、[OK] をクリックします。複数のアプリケーション プロトコルを選択する場合は、Ctrl または Shift キーを押しながらクリックします。また、クリックしてドラッグすることによって、隣接する複数のアプリケーション プロトコルを選択することもできます。

アプリケーション プロトコルが追加されます。組み込みアプリケーション プロトコルを追加した場合は、その名前が斜体で表示されることに注意してください。残りの手順を省略することも、オプションで、アプリケーション プロトコルの値（ポートやプロトコルなど）を変更するために、追加したアプリケーション プロトコルをクリックしてアプリケーション プロトコル エディタを表示することもできます。

- 新しいアプリケーション プロトコルを追加するには、[<New Application Protocol>] を選択して、[OK] をクリックします。

  アプリケーション プロトコル エディタが表示されます。

ステップ 3　[Type] ドロップダウンリストから、アプリケーション プロトコル タイプを選択します。カスタム アプリケーション プロトコルの場合は、[any] を選択します。

ステップ 4　アプリケーション プロトコル ポートを指定します。次の 2 つのオプションから選択できます。

- 任意のポート上でのアプリケーション プロトコルの実行を許可するには、[Any port] チェック ボックスをオンにします。
- 特定のポート上でのアプリケーション プロトコルの実行を許可するには、[port] フィールドにポート番号を入力します。

ステップ 5　[Protocol] ドロップダウンリストから、プロトコル（[TCP] または [UDP]）を選択します。

ステップ 6　オプションで、[Vendor] フィールドと [Version] フィールドで、アプリケーション プロトコルのベンダーとバージョンを指定します。

ベンダーまたはバージョンを指定しなかった場合は、タイプとプロトコルが一致している限り、ホワイト リストではすべてのベンダーとバージョンが許可されます。ベンダーとバージョンを制限する場合は、イベント ビューまたはアプリケーション プロトコル ネットワーク マップに表示されるとおりに正確に指定する必要があります。

ステップ 7　[OK] をクリックします。

アプリケーション プロトコルが追加されます。変更を反映するためにはホワイト リストを保存する必要があることに注意してください。

アプリケーション プロトコルをアクティブな相関ポリシーで使用されているホワイト リストに追加した場合は、ホワイト リストの保存後に、ターゲット ホストが再評価されます。この再評価で一部のホストが準拠に移行したとしても、ホワイト リスト イベントは生成されません。

ホスト プロファイルへのクライアントの追加

ライセンス： FireSIGHT

コンプライアンス ホワイト リストは、共有ホスト プロファイル、または単一のホワイト リストに属しているホスト プロファイルのいずれかを使用して、特定のオペレーティング システム上での特定のクライアント アプリケーションの実行を許可するように設定できます。また、ホワイト リストは、有効な任意のターゲット上での特定のクライアントの実行を許可するように設定できます。これは、グローバルに許可されたクライアントと呼ばれます。

オプションで、クライアントを特定のバージョンに限定することができます。たとえば、Microsoft Windows ホスト上での実行を Microsoft Internet Explorer 8.0 のみに許可することができます。

クライアントをコンプライアンス ホワイト リスト ホスト プロファイルに追加する方法:

アクセス: Admin

ステップ 1　ホワイト リスト ホスト プロファイルを作成または変更しているときに、[Allowed Clients]（または [Any Operating System] ホスト プロファイルを変更している場合は [Globally Allowed Clients]）の横にある追加アイコン（  ）をクリックします。

ポップアップ ウィンドウが表示されます。一覧表示されるクライアントは次のとおりです。

- ホワイト リスト内で作成したクライアント
- ネットワークの調査（52-10 ページ）の説明に従ってネットワークを調査したときにネットワーク マップ内のホスト上で実行されていたクライアント
- ホワイト リスト内の他のホスト プロファイルによって使用されるクライアント。これには、デフォルト ホワイト リストで使用するために VRT によって作成された組み込みクライアントが含まれる場合があります。

ステップ 2　次の 2 つのオプションから選択できます。

- リスト内にすでに存在するクライアントを追加するには、それを選択して、[OK] をクリックします。複数のクライアントを選択する場合は、Ctrl または Shift キーを押しながらクリックします。また、クリックしてドラッグすることによって、隣接する複数のクライアントを選択することもできます。

  クライアントが追加されます。組み込みクライアントを追加した場合は、その名前が斜体で表示されることに注意してください。残りの手順を省略することも、オプションで、クライアントの値（バージョンなど）を変更するために、追加したクライアントをクリックしてクライアント エディタを表示することもできます。
- 新しいクライアントを追加するには、[<New Client>] を選択して、[OK] をクリックします。

  クライアント エディタが表示されます。

ステップ 3　[Client] ドロップダウンリストから、クライアントを選択します。

ステップ 4　オプションで、[Version] フィールドで、クライアントのバージョンを指定します。

バージョンを指定しなかった場合は、名前が一致している限り、ホワイト リストではすべてのバージョンが許可されます。バージョンを制限する場合は、クライアントのテーブル ビューに表示されているとおりに正確に指定する必要があることに注意してください。

ステップ 5　[OK] をクリックします。

クライアントが追加されます。変更を反映するためにはホワイト リストを保存する必要があることに注意してください。

クライアントをアクティブな相関ポリシーで使用されているホワイト リストに追加した場合は、ホワイト リストの保存後に、ターゲット ホストが再評価されます。この再評価で一部のホストが準拠に移行したとしても、ホワイト リスト イベントは生成されません。

ホスト プロファイルへの Web アプリケーションの追加

ライセンス：FireSIGHT

コンプライアンス ホワイト リストは、共有ホスト プロファイル、または、単一のホワイト リストに属しているホスト プロファイルのいずれかを使用して、特定のオペレーティング システム上での特定の Web アプリケーションの実行を許可するように設定できます。また、ホワイト リストは、有効な任意のターゲット上での特定の Web アプリケーションの実行を許可するように設定できます。これは、グローバルに許可された Web アプリケーションと呼ばれます。

Web アプリケーションをコンプライアンス ホワイト リスト ホスト プロファイルに追加する方法：

アクセス：Admin

ステップ 1　ホワイト リスト ホスト プロファイルを作成または変更しているときに、[Allowed Web Applications]（または [Any Operating System] ホスト プロファイルを変更している場合は [Globally Allowed Web Applications]）の横にある追加アイコン（  ）をクリックします。

ポップアップ ウィンドウが表示され、システムで検出されたすべての Web アプリケーションが一覧表示されます。

ステップ 2　Web アプリケーションを選択して、[OK] をクリックします。複数の Web アプリケーションを選択する場合は、Ctrl または Shift キーを押しながらクリックします。また、クリックしてドラッグすることによって、隣接する複数の Web アプリケーションを選択することもできます。

Web アプリケーションが追加されます。変更を反映するためにはホワイト リストを保存する必要があることに注意してください。

Web アプリケーションをアクティブな相関ポリシーで使用されているホワイト リストに追加した場合は、ホワイト リストの保存後に、ターゲット ホストが再評価されます。この再評価で一部のホストが準拠に移行したとしても、ホワイト リスト イベントは生成されません。

ホスト プロファイルへのプロトコルの追加

ライセンス：FireSIGHT

コンプライアンス ホワイト リストは、共有ホスト プロファイル、または単一のホワイト リストに属しているホスト プロファイルのいずれかを使用して、特定のオペレーティング システム上での特定のプロトコルの実行を許可するように設定できます。また、ホワイト リストは、有効な任意のターゲット上での特定のプロトコルの実行を許可するように設定できます。これは、グローバルに許可されたプロトコルと呼ばれます。ARP、IP、TCP、および UDP は、常にすべてのホスト上での実行が許可されることに注意してください。これらを禁止することはできません。

許可するプロトコルに関して、そのタイプ（ネットワークまたはトランスポート）と番号を指定する必要があります。

プロトコルをコンプライアンス ホワイト リスト ホスト プロファイルに追加する方法：

アクセス：Admin

ステップ 1　ホワイト リスト ホスト プロファイルを作成または変更しているときに、[Allowed Protocols]（または [Any Operating System] ホスト プロファイルを変更している場合は [Globally Allowed Protocols]）の横にある追加アイコン（  ）をクリックします。

ポップアップ ウィンドウが表示されます。一覧表示されるプロトコルは次のとおりです。

- ホワイト リスト内で作成したプロトコル
- ネットワークの調査（52-10 ページ）の説明に従ってネットワークを調査したときにネットワーク マップ内のホスト上で実行されていたプロトコル
- ホワイト リスト内の他のホスト プロファイルによって使用されるプロトコル。これには、デフォルト ホワイト リストで使用するために VRT によって作成された組み込みプロトコルが含まれる場合があります。

ステップ 2　次の 2 つのオプションから選択できます。

- リスト内にすでに存在するプロトコルを追加するには、それを選択して、[OK] をクリックします。複数のプロトコルを選択する場合は、Ctrl または Shift キーを押しながらクリックします。また、クリックしてドラッグすることによって、隣接する複数のプロトコルを選択することもできます。

  プロトコルが追加されます。組み込みプロトコルを追加した場合は、その名前が斜体で表示されることに注意してください。残りの手順を省略することも、オプションで、プロトコルの値（タイプや番号など）を変更するために、追加したプロトコルをクリックしてプロトコル エディタを表示することもできます。
- 新しいプロトコルを追加するには、[<New Protocol>] を選択して、[OK] をクリックします。

  プロトコル エディタが表示されます。

ステップ 3　[Type] ドロップダウンリストから、プロトコル タイプ（[Network] または [Transport]）を選択します。

ステップ 4　プロトコルを指定します。次の 2 つのオプションから選択できます。

- ドロップダウンリストからプロトコルを選択します。
- リスト内に存在しないプロトコルを指定するには、[Other (manual entry)] を選択します。ネットワーク プロトコルの場合は、http://www.iana.org/assignments/ethernet-numbers/ に記載されている適切な番号を入力します。トランスポート プロトコルの場合は、http://www.iana.org/assignments/protocol-numbers/ に記載されている適切な番号を入力します。

ステップ 5　[OK] をクリックします。

プロトコルが追加されます。変更を反映するためにはホワイト リストを保存する必要があることに注意してください。

プロトコルをアクティブな相関ポリシーで使用されているホワイト リストに追加した場合は、ホワイト リストの保存後に、ターゲット ホストが再評価されます。この再評価で一部のホストが準拠に移行したとしても、ホワイト リスト イベントは生成されません。

コンプライアンス ホワイト リストへの共有ホスト プロファイルの追加

ライセンス：FireSIGHT

共有ホスト プロファイルは、特定のオペレーティング システムに関連付けられますが、ホワイト リスト全体で使用できます。つまり、複数のホワイト リストを作成するが、同じホスト プロファイルを使用して複数のホワイト リストで特定のオペレーティング システムを実行するホストを評価する場合は、共有のホスト プロファイルを使用します。

組み込み共有ホスト プロファイルをコンプライアンス ホワイト リストに追加することも、作成した共有ホスト プロファイルを追加することもできます。詳細については、共有ホスト プロファイルについて（52-6 ページ）および共有ホスト プロファイルの作成（52-27 ページ）を参照してください。

共有ホスト プロファイルをコンプライアンス ホワイト リストに追加する方法：

アクセス：Admin

ステップ 1　[Create White List] ページで、[Add Shared Host Profile] をクリックします。

[Add Shared Host Profile] ページが表示されます。

ステップ 2　[Name] ドロップダウンリストから、ホワイト リストに追加する共有ホスト プロファイルを選択して、[OK] をクリックします。

共有ホスト プロファイルがホワイト リストに追加され、[Create White List] ページが再び表示されます。共有ホスト プロファイルの名前が [Allowed Host Profiles] の下に斜体で表示されます。

ヒント　[Allowed Host Profiles] でプロファイル名をクリックすることによって、それを使用するホワイト リストから共有ホスト プロファイルを編集できます。詳細については、既存のホスト プロファイルの変更（52-22 ページ）を参照してください。

既存のホスト プロファイルの変更

ライセンス：FireSIGHT

コンプライアンス ホワイト リスト内のホスト プロファイルを変更したら、その変更を反映させるためにホワイト リストを保存する必要があります。

変更するホスト プロファイルがアクティブな相関ポリシーで使用されているホワイト リストに属している場合は、プロファイルを変更すると、ホストが準拠または非準拠に移行する場合がありますが、ホワイト リスト イベントは**生成されません**。また、共有ホスト プロファイルを変更すると、それを使用しているすべてのホワイト リストに影響します。これにより、操作しているホワイト リストだけでなく、その他のホワイト リストでもホストが準拠または非準拠に移行する場合があります。

ヒント　他の共有ホスト プロファイルと同様に、デフォルト ホワイト リストで使用されている組み込みホスト プロファイルを編集できます。それらを出荷時の初期状態にリセットすることもできます。詳細については、組み込みホスト プロファイルの出荷時の初期状態へのリセット（52-32 ページ）を参照してください。

既存のホスト プロファイルを変更する方法：

アクセス：Admin

ステップ 1　[Create White List] ページで、変更するホスト プロファイルの名前をクリックします。

ホスト プロファイルの設定が表示されます。共有ホスト プロファイルを編集している場合は、[Edit] リンクがホスト プロファイルの名前の横に表示されることに注意してください。組み込みホスト プロファイルを編集している場合は、組み込みホスト プロファイル アイコン（）も表示されます。

ステップ 2　次の 2 つのオプションから選択できます。

- 共有ホスト プロファイルを変更している場合は、[Edit] をクリックします。

ポップアップ ウィンドウが表示されます。次の表に従って、必要に応じて変更を加えます。[Save All Profiles] をクリックしてプロファイルを保存してから、[Done] をクリックしてポップアップ ウィンドウを閉じます。

共有ホスト プロファイルの編集方法については、共有ホスト プロファイルの変更（52-29 ページ）を参照してください。

- ホワイト リストのグローバル ホスト プロファイルまたは特定のオペレーティング システム用のホスト プロファイルを変更している場合は、次の手順に記載されているいずれかの操作を実行します。

ホスト プロファイルの名前を変更する方法：

アクセス： Admin

ステップ 1　[Name] フィールドに新しい名前を記入します。

ホスト プロファイルのオペレーティング システムを変更する方法：

アクセス： Admin

ステップ 1　[OS Vendor]、[OS Name]、[Version] の各ドロップダウンリストから、新しいオペレーティング システムとバージョンを選択します。

これらの値を変更するときに、ホスト プロファイルの名前を変更することもできます。ホワイト リストのグローバル ホスト プロファイルにはオペレーティング システムが関連付けられていないため、変更できないことに注意してください。

アプリケーション プロトコルを追加する方法：

アクセス： Admin

ステップ 1　ホスト プロファイルへのアプリケーション プロトコルの追加（52-17 ページ）の指示に従ってください。

クライアントを追加する方法：

アクセス： Admin

ステップ 1　ホスト プロファイルへのクライアントの追加（52-18 ページ）の指示に従ってください。

Web アプリケーションを追加する方法：

アクセス： Admin

ステップ 1　ホスト プロファイルへの Web アプリケーションの追加（52-20 ページ）の指示に従ってください。

プロトコルを追加する方法：

アクセス：Admin

ステップ 1　ホスト プロファイルへのプロトコルの追加（52-20 ページ）の指示に従ってください。

すべてのアプリケーション プロトコルを許可する方法：

アクセス：Admin

ステップ 1　[Allowed Application Protocols] で、[Allow all Application Protocols] チェック ボックスをオンにします。

過去に許可したアプリケーション プロトコルを削除するまで、チェック ボックスが表示されないことに注意してください。

すべてのクライアントを許可する方法：

アクセス：Admin

ステップ 1　[Allowed Clients] で、[Allow all Clients] チェック ボックスをオンにします。

過去に許可したクライアントを削除するまで、チェック ボックスが表示されないことに注意してください。

すべての Web アプリケーションを許可する方法：

アクセス：Admin

ステップ 1　[Allowed Web Applications] で、[Allow all Web Applications] チェック ボックスをオンにします。

過去に許可した Web アプリケーションを削除するまで、チェック ボックスが表示されないことに注意してください。

アプリケーション プロトコル、クライアント、Web アプリケーション、またはプロトコルを変更する方法：

アクセス：Admin

ステップ 1　変更する要素をクリックします。

変更可能なプロパティの詳細については、以下を参照してください。

- ホスト プロファイルへのアプリケーション プロトコルの追加（52-17 ページ）
- ホスト プロファイルへのクライアントの追加（52-18 ページ）
- ホスト プロファイルへのプロトコルの追加（52-20 ページ）

注　アプリケーション プロトコル、クライアント、Web アプリケーション、またはプロトコルに加えた変更は、その要素を使用しているすべてのホスト プロファイルに反映されます。

アプリケーション プロトコル、クライアント、Web アプリケーション、またはプロトコルを削除する方法：

アクセス：Admin

ステップ 1　削除する要素の横にある削除アイコン（ ）をクリックします。

ネットワークを調査する方法：

アクセス：Admin

ステップ 1　[Survey Network] をクリックします。ネットワークを調査することで、新しく許可したクライアント、アプリケーション プロトコル、およびプロトコルを既存のホスト プロファイルに追加したり、初期調査で検出されなかったオペレーティング システムを実行中のホストが今回の調査で検出された場合に追加のホスト プロファイルを作成したりできます。詳細については、ネットワークの調査（52-10 ページ）を参照してください。

既存のホスト プロファイルの削除

ライセンス：FireSIGHT

コンプライアンス ホワイト リストからホスト プロファイルを削除したら、その変更を反映させるためにホワイト リストを保存する必要があります。共有ホスト プロファイルを削除すると、それがホワイト リストから除外されますが、プロファイルは削除されず、それを使用する他のホワイト リストからも除外されないことに注意してください。ホワイト リストのグローバル ホスト プロファイルは削除できません。

削除するホスト プロファイルがアクティブな相関ポリシーで使用されている 1 つ以上のホワイト リストに属している場合は、プロファイルを削除すると、ホストが非準拠に移行する場合がありますが、ホワイト リスト イベントは**生成されません**。

コンプライアンス ホワイト リスト ホスト プロファイルを削除する方法：

アクセス：Admin

ステップ 1　[Create White List] ページで、削除するホスト プロファイルの横にある削除アイコン（ ）をクリックします。

ステップ 2　プロンプトが表示されたら、ホスト プロファイルの削除を確認します。

ホスト プロファイルが削除されます。

コンプライアンス ホワイト リストの管理

ライセンス：FireSIGHT

コンプライアンス ホワイト リストは [White List] ページを使用して管理します。デフォルト ホワイト リストを含め、ホワイト リストを作成、変更、および削除することができます。作成した共有ホスト プロファイルだけでなく、組み込み共有ホスト プロファイルを編集したり、新しい共有ホスト プロファイルを追加したりすることもできます。詳細については、以下を参照してください。

- コンプライアンス ホワイト リストの作成（52-9 ページ）
- コンプライアンス ホワイト リストの変更（52-26 ページ）
- コンプライアンス ホワイト リストの削除（52-26 ページ）
- 共有ホスト プロファイルの操作（52-27 ページ）

コンプライアンス ホワイト リストの変更

ライセンス：FireSIGHT

アクティブな相関ポリシーに含まれているコンプライアンス ホワイト リストを変更すると、システムがターゲット ホストを再評価します。この再評価中は、ホワイト リストがアクティブな相関ポリシーに含まれており、以前に準拠していたホストが更新されたホワイト リストによって非準拠になった場合でも、システムはホワイト リスト イベントを生成**せず**、したがってホワイト リストに関連付けられた応答もトリガーされないことに注意してください。

既存のコンプライアンス ホワイト リストを変更する方法：

アクセス：Admin

ステップ 1　[Policies] > [Correlation] の順に選択してから、[White List] をクリックします。

[White List] ページが表示されます。

ステップ 2　変更するホワイト リストの横にある編集アイコン（  ）をクリックします。

[Create White List] ページが表示されます。

ステップ 3　必要に応じて変更を加えて、[Save White List] をクリックします。

ホワイト リストが更新されます。

コンプライアンス ホワイト リストの削除

ライセンス：FireSIGHT

1 つ以上の相関ポリシーで使用しているコンプライアンス ホワイト リストは削除できません。その前に、それが使用されているすべてのポリシーからホワイト リストを削除する必要があります。ポリシーからホワイト リストを削除する方法については、相関ポリシーの編集（51-55 ページ）を参照してください。

ホワイト リストを削除すると、ネットワーク上のすべてのホストからそのホワイト リストに関連付けられたホスト属性も削除されます。

既存のコンプライアンス ホワイト リストを削除する方法：

アクセス：Admin

ステップ 1　[Policies] > [Correlation] の順に選択してから、[White List] をクリックします。

[White List] ページが表示されます。

ステップ 2　削除するホワイト リストの横にある削除アイコン（ ）をクリックします。

ホワイト リストが削除されます。

共有ホスト プロファイルの操作

ライセンス：FireSIGHT

共有ホスト プロファイルは、複数のホワイト リストに渡りターゲット ホスト上での実行を許可するオペレーティング システム、クライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルを指定します。つまり、複数のホワイト リストを作成するが、同じホスト プロファイルを使用して複数のホワイト リストで特定のオペレーティング システムを実行するホストを評価する場合は、共有のホスト プロファイルを使用します。デフォルト ホワイト リストでは、*組み込みホスト プロファイル*と呼ばれる特殊なカテゴリの共有ホスト プロファイルが使用されることに注意してください。

共有ホスト プロファイルの詳細については、共有ホスト プロファイルについて（52-6 ページ）を参照してください。

共有ホスト プロファイルは作成、変更、および削除できます。加えて、組み込み共有ホスト プロファイルを変更または削除した場合、あるいは、組み込みアプリケーション プロトコル、プロトコル、またはクライアントを変更または削除した場合は、それらを出荷時の初期状態にリセットできます。詳細については、以下を参照してください。

- 共有ホスト プロファイルの作成（52-27 ページ）
- 共有ホスト プロファイルの変更（52-29 ページ）
- 共有ホスト プロファイルの削除（52-31 ページ）
- 組み込みホスト プロファイルの出荷時の初期状態へのリセット（52-32 ページ）

共有ホスト プロファイルを作成したら、それを複数のホワイト リストに追加できます。詳細については、コンプライアンス ホワイト リストへの共有ホスト プロファイルの追加（52-21 ページ）を参照してください。

共有ホスト プロファイルの作成

ライセンス：FireSIGHT

1 つのホスト プロファイルを使用して、複数のホワイト リストに渡り特定のオペレーティング システムを実行しているホストを評価する場合は、共有ホスト プロファイルを作成します。

ヒント　特定のホストのホスト プロファイルを使用して、コンプライアンス ホワイト リストの共有ホスト プロファイルを作成することもできます。詳細については、ホスト プロファイルからのホワイト リスト ホスト プロファイルの作成（49-27 ページ）を参照してください。

共有ホスト プロファイルを作成する方法:

アクセス: Admin

ステップ 1　[Policies] > [Correlation] の順に選択してから、[White List] をクリックします。

[White List] ページが表示されます。

ステップ 2　[Edit Shared Profiles] をクリックします。

[Edit Shared Profiles] ページが表示されます。

ステップ 3　オプションで、ネットワークを調査します。

ネットワークを調査すると、システムがネットワークについて収集したデータに基づいていくつかのベースライン共有ホワイト リストが作成されます。これにより、複数の共有ホスト プロファイルを手動で作成して設定する手間が省けます。次の 2 つのオプションから選択できます。

- ネットワークを調査するには、[Survey Network] をクリックします。詳細については、ネットワークの調査（52-10 ページ）を参照してください。

  システムは 1 つ以上のベースライン共有ホスト プロファイルを作成します。これらの共有ホスト プロファイルは、共有ホスト プロファイルの変更（52-29 ページ）と共有ホスト プロファイルの削除（52-31 ページ）の説明に従って編集または削除できます。他に必要な共有ホスト プロファイルを追加するには、次のステップに進みます。
- ネットワークの調査を省略するには、次のステップに進みます。

ステップ 4　[Shared Host Profiles] の横にある追加アイコン（  ）をクリックします。

新しい共有ホスト プロファイルの設定が表示されます。

ステップ 5　[Name] フィールドに、共有ホスト プロファイルの分かりやすい名前を入力します。

ステップ 6　[OS Vendor]、[OS Name]、および [Version] の各ドロップダウンリストから、共有ホスト プロファイルを作成するオペレーティング システムとバージョンを選択します。

ステップ 7　許可するアプリケーション プロトコルを指定します。次の 3 つのオプションがあります。

- すべてのアプリケーション プロトコルを許可するには、[Allow all Application Protocols] チェック ボックスをオンにします。
- どのアプリケーション プロトコルも許可しない場合は、[Allow all Application Protocols] チェック ボックスをオフのままにします。
- 特定のアプリケーション プロトコルを許可するには、[Allowed Application Protocols] の横で、ホスト プロファイルへのアプリケーション プロトコルの追加（52-17 ページ）の手順に従ってください。

ステップ 8　許可するクライアントを指定します。次の 3 つのオプションがあります。

- すべてのクライアントを許可するには、[Allow all Clients] チェック ボックスをオンにします。
- どのクライアントも許可しない場合は、[Allow all Clients] チェック ボックスをオフのままにします。
- 特定のクライアントを許可するには、ホスト プロファイルへのクライアントの追加（52-18 ページ）の指示に従ってください。

ステップ 9　許可する Web アプリケーションを指定します。次の 3 つのオプションがあります。

- すべての Web アプリケーションを許可するには、[Allow all Web Applications] チェック ボックスをオンにします。
- どの Web アプリケーションも許可しない場合は、[Allow all Web Applications] チェック ボックスをオフのままにします。

- 特定の Web アプリケーションを許可するには、ホスト プロファイルへの Web アプリケーションの追加（52-20 ページ）の指示に従ってください。

ステップ 10　許可するプロトコルを指定します。

プロトコルを追加するには、[Allowed Protocols] の横で、ホスト プロファイルへのプロトコルの追加（52-20 ページ）の手順に従ってください。ARP、IP、TCP、および UDP は常に許可されることに注意してください。

ステップ 11　[Save all Profiles] をクリックして変更を保存します。

共有ホスト プロファイルが作成されます。これで、共有ホスト プロファイルを任意のコンプライアンス ホワイト リストに追加できるようになりました。

共有ホスト プロファイルの変更

ライセンス：FireSIGHT

共有ホスト プロファイル変更すると、それが属しているすべてのホワイト リストのプロファイルが変更されます。共有ホスト プロファイルを使用し、アクティブな相関ポリシーでも使用されているホワイト リストの場合は、共有ホスト プロファイルを変更すると、ホストが非準拠に移行する場合がありますが、ホワイト リスト イベントは**生成されません**。

次の表に、共有ホスト プロファイルを変更するための操作の説明を示します。

表 52-2　共有ホスト プロファイルの操作

目的	操作
ホスト プロファイルの名前を変更する	[Name] フィールドに新しい名前を記入します。
オペレーティング システムを変更する	[OS Vendor]、[OS Name]、[Version] の各ドロップダウン リストから、新しいオペレーティング システムとバージョンを選択します。これらの値を変更するときに、ホスト プロファイルの名前を変更することもできます。
アプリケーション プロトコルを追加する	ホスト プロファイルへのアプリケーション プロトコルの追加（52-17 ページ）の指示に従ってください。
クライアントを追加する	ホスト プロファイルへのクライアントの追加（52-18 ページ）の指示に従ってください。
Web アプリケーションを追加する	ホスト プロファイルへの Web アプリケーションの追加（52-20 ページ）の指示に従ってください。
プロトコルを追加する	ホスト プロファイルへのプロトコルの追加（52-20 ページ）の指示に従ってください。
すべてのアプリケーション プロトコルを許可する	[Allowed Application Protocols] で、[Allow all Application Protocols] チェック ボックスをオンにします。過去に許可したアプリケーション プロトコルを削除するまで、チェック ボックスが表示されないことに注意してください。
すべてのクライアントを許可する	[Allowed Clients] で、[Allow all Clients] チェック ボックスをオンにします。過去に許可したクライアントを削除するまで、チェック ボックスが表示されないことに注意してください。

表 52-2　共有ホスト プロファイルの操作（続き）

目的	操作
すべての Web アプリケーションを許可する	[Allowed Web Applications] で、[Allow all Web Applications] チェック ボックスをオンにします。過去に許可したクライアントを削除するまで、チェック ボックスが表示されないことに注意してください。
アプリケーション プロトコル、クライアント、Web アプリケーション、またはプロトコルを変更する	変更する要素をクリックします。変更可能なプロパティの詳細については、以下を参照してください。 • ホスト プロファイルへのアプリケーション プロトコルの追加（52-17 ページ） • ホスト プロファイルへのクライアントの追加（52-18 ページ） • ホスト プロファイルへの Web アプリケーションの追加（52-20 ページ） • ホスト プロファイルへのプロトコルの追加（52-20 ページ） **注**　アプリケーション プロトコル、クライアント、またはプロトコルに加えた変更は、その要素を使用しているすべてのホスト プロファイルに反映されます。
アプリケーション プロトコル、クライアント、Web アプリケーション、またはプロトコルを削除する	削除する要素の横にある削除アイコン（ ）をクリックします。
ネットワークを調査する	[Survey Network] をクリックします。ネットワークを調査すると、新しく許可したクライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルを既存のホスト プロファイルに追加したり、初期調査で検出されなかったオペレーティング システムを実行中のホストが今回の調査で検出された場合に追加のホスト プロファイルを作成したりできます。詳細については、ネットワークの調査（52-10 ページ）を参照してください。

共有ホスト プロファイルを変更する方法：

アクセス： Admin

ステップ 1　[Policies] > [Correlation] の順に選択してから、[White List] をクリックします。

[White List] ページが表示されます。

ステップ 2　[Edit Shared Profiles] をクリックします。

[Edit Shared Profiles] ページが表示されます。

ステップ 3　組み込み共有ホスト プロファイルのいずれかを編集しますか。

- はいの場合は、[Built-in Host Profiles] を展開してそれらのホスト プロファイルを表示します。
- いいえの場合は、次のステップに進みます。

ステップ 4　変更する共有ホスト プロファイルの名前をクリックします。

ホスト プロファイルが表示されます。

ステップ 5　表 52-2（52-29 ページ）に記載されている操作のいずれかを実行します。

ステップ 6　[Save all Profiles] をクリックして変更を保存します。

共有ホスト プロファイルが保存されます。

共有ホスト プロファイルの削除

ライセンス：FireSIGHT

削除する共有ホスト プロファイルがアクティブな相関ポリシーで使用されている 1 つ以上のホワイト リストに属している場合は、プロファイルを削除すると、ホストが非準拠に移行する場合がありますが、ホワイト リスト イベントは**生成されません**。

ヒント　デフォルト ホワイト リストで使用されている組み込み共有ホスト プロファイルを削除した場合は、組み込みプロファイルを出荷時の初期状態にリセットすることによって、それを復元できます。詳細については、組み込みホスト プロファイルの出荷時の初期状態へのリセット（52-32 ページ）を参照してください。

共有ホスト プロファイルを削除する方法：

アクセス：Admin

ステップ 1　[Policies] > [Correlation] の順に選択してから、[White List] をクリックします。

[White List] ページが表示されます。

ステップ 2　[Edit Shared Profiles] をクリックします。

[Edit Shared Profiles] ページが表示されます。

ステップ 3　組み込み共有ホスト プロファイルのいずれかを削除しますか。

- はいの場合は、[Built-in Host Profiles] を展開してそれらのホスト プロファイルを表示します。
- いいえの場合は、次のステップに進みます。

ステップ 4　削除する共有ホスト プロファイルの横にある削除アイコン（ ）をクリックします。

共有ホスト プロファイルの削除を確認します。

ステップ 5　[Save all Profiles] をクリックして変更を保存します。

共有ホスト プロファイルが削除され、それを使用しているすべてのコンプライアンス ホワイト リストから除外されます。

組み込みホスト プロファイルの出荷時の初期状態へのリセット

ライセンス：FireSIGHT

デフォルト ホワイト リストでは、*組み込みホスト プロファイル*と呼ばれる特殊なカテゴリの共有ホスト プロファイルが使用されます。組み込みホスト プロファイルでは、組み込みアプリケーション プロトコル、プロトコル、およびクライアントが使用されます。これらの要素は、デフォルト ホワイト リストおよびユーザが作成したカスタム ホワイト リストの両方でそのまま使用することも、ニーズに合わせて変更することもできます。詳細については、共有ホスト プロファイルについてを参照してください。

組み込みプロファイル、アプリケーション プロトコル、プロトコル、Web アプリケーション、またはクライアントに加えた変更を元に戻す必要がある場合は、出荷時の初期状態にリセットすることができます。出荷時の初期状態にリセットすると、次の現象が発生します。

- 変更した組み込みホスト プロファイル、アプリケーション プロトコル、プロトコル、およびクライアントの**すべて**が出荷時の初期状態にリセットされます。
- 削除した組み込みホスト プロファイル、アプリケーション プロトコル、プロトコル、およびクライアントの**すべて**が復元されます。
- アクティブな相関ポリシーで使用されているホワイト リスト（デフォルト ホワイト リストを含む）と、リセットした組み込みホスト プロファイル、アプリケーション プロトコル、プロトコル、またはクライアントのいずれかを使用していたホワイト リストの**すべて**が再評価されます。この再評価で一部のホストが準拠に移行される場合がありますが、ホワイト リスト イベントは生成されません。

組み込みホスト プロファイル、アプリケーション プロトコル、プロトコル、およびクライアントをリセットするには、次の手順を実行します。

アクセス：Admin

ステップ 1　[Policies] > [Correlation] の順に選択してから、[White List] をクリックします。

[White List] ページが表示されます。

ステップ 2　[Edit Shared Profiles] をクリックします。

[Edit Shared Profiles] ページが表示されます。

ステップ 3　[Built-in Host Profiles] をクリックします。

[Built-in Host Profiles] ページが表示されます。

ステップ 4　[Reset to Factory Defaults] をクリックします。

ステップ 5　[OK] をクリックすることによって、出荷時の初期状態へのリセットを確認します。

組み込みホスト プロファイル、アプリケーション プロトコル、プロトコル、およびクライアントのすべてが出荷時の初期状態にリセットされます。アクティブな相関ポリシーで使用されているホワイト リストと、リセットした組み込みホスト プロファイル、アプリケーション プロトコル、プロトコル、またはクライアントを使用していたホワイト リストがすべて再評価されます。

ホワイト リスト イベントの操作

ライセンス：FireSIGHT

ホストがアクティブな相関ポリシーに含まれているホワイト リストに準拠していないことを示す検出イベントをシステムが生成すると、ホワイト リスト イベントが生成されます。ホワイト リスト イベントは、相関イベントの特殊な形態で、相関イベント データベースに記録されます。ホワイト リスト イベントは検索、表示、および削除することができます。

ヒント　データベースに保存されるイベント数の設定方法については、データベース イベント制限の設定（63-16 ページ）を参照してください。ホワイト リスト イベントは相関イベント データベースに保存されることに注意してください。

詳細については、次の項を参照してください。

- ホワイト リスト イベントの表示（52-33 ページ）
- ホワイト リスト イベント テーブルについて（52-35 ページ）
- コンプライアンス ホワイト リスト イベントの検索（52-36 ページ）

ホワイト リスト イベントの表示

ライセンス：FireSIGHT

Defense Centerを使用して、コンプライアンス ホワイト リスト イベントのテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

ホワイト リスト イベントにアクセスしたときに表示されるページは使用しているワークフローによって異なります。ホワイト リスト イベントのテーブル ビューを含む事前定義のワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。カスタム ワークフローの作成方法については、カスタム ワークフローの作成（58-43 ページ）を参照してください。

次の表に、ホワイト リスト イベント ワークフロー ページで実行可能な特定の操作の説明を示します。

表 52-3　コンプライアンス ホワイト リスト イベントの操作

目的	操作
ホストのホスト プロファイルを表示する	IP アドレスの横に表示されたホスト プロファイル アイコン（）をクリックします。
ユーザ プロファイル情報を表示する	ユーザ ID の横に表示されたユーザ アイコン（）をクリックします。詳細については、ユーザの詳細とホストの履歴について（50-68 ページ）を参照してください。
現在のワークフロー ページでイベントをソートしたり、制限したりする	ドリルダウン ワークフロー ページのソート（58-38 ページ）で詳細を参照してください。
現在のワークフロー ページ内で移動する	ワークフロー内の他のページへのナビゲート（58-39 ページ）で詳細を参照してください。

表 52-3　コンプライアンス ホワイト リスト イベントの操作（続き）

目的	操作
現在の制限を維持して、現在のワークフロー内のページ間を移動する	ワークフロー ページの左上で、該当するページ リンクをクリックします。詳細については、ワークフローのページの使用（58-21 ページ）を参照してください。
表示された列の詳細を表示する	ホワイト リスト イベント テーブルについて（52-35 ページ）で詳細を参照してください。
表示されたイベントの時刻と日付の範囲を変更する	イベント時間の制約の設定（58-26 ページ）で詳細を参照してください。
特定の値に制限して、ワークフロー内の次のページにドリルダウンする	次のいずれかの方法を使用します。 • カスタム ワークフローで作成したドリルダウン ページで、行内の値をクリックします。テーブル ビューの行内の値をクリックすると、テーブル ビューが制限され、次のページに**ドリルダウンされない**ことに注意してください。 • 一部のユーザに制限して次のワークフロー ページにドリルダウンするには、次のワークフロー ページに表示するユーザの横にあるチェック ボックスをオンにしてから、[View] をクリックします。 • 現在の制限を維持して次のワークフロー ページにドリルダウンするには、[View All] をクリックします。 **ヒント**　テーブル ビューでは、必ずページ名に「Table View」が含まれます。 詳細については、イベントの制約（58-35 ページ）を参照してください。
システムからホワイト リスト イベントを削除する	次のいずれかの方法を使用します。 • 特定のイベントを削除するには、削除するイベントの横にあるチェック ボックスをオンにしてから、[Delete] をクリックします。 • 現在の制限ビュー内のすべてのイベントを削除するには、[Delete All] をクリックしてから、すべてのイベントを削除することを確認します。
他のイベント ビューに移動して関連イベントを表示する	ワークフロー間のナビゲート（58-40 ページ）で詳細を参照してください。

コンプライアンス ホワイト リスト イベントを表示する方法：

アクセス： Admin/Any Security Analyst/Discovery Admin

ステップ 1　[Analysis] > [Correlation] > [White List Events] の順に選択します。

デフォルト ホワイト リスト イベント ワークフローの最初のページが表示されます。カスタム ワークフローを含む別のワークフローを使用するには、ワークフロー タイトルのそばにある [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。イベントが表示されない場合は、時間範囲の調整が必要な可能性があります。イベント時間の制約の設定（58-26 ページ）を参照してください。

ホワイト リスト イベント テーブルについて

ライセンス：FireSIGHT

相関ポリシー機能を使用して*相関ポリシー*を作成し、システムがネットワーク上の脅威にリアルタイムに対処するように設定できます。相関ポリシーには、コンプライアンス ホワイト リスト違反を含む、ポリシー違反を構成する活動の種類が記載されます。相関ポリシーの詳細については、相関ポリシーおよび相関ルールの設定（51-1 ページ）を参照してください。

コンプライアンス ホワイト リストの違反があると、ホワイト リスト イベントが生成されます。ホワイト リスト イベント テーブル内のフィールドの説明を次の表に示します。

表 52-4　コンプライアンス ホワイト リスト イベントのフィールド

フィールド	説明
時刻	ホワイト リスト イベントが生成された日時。
IP Address	非準拠ホストの IP アドレス。
User	非準拠ホストにログインしている既知のユーザの ID。
ポート	アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーしたイベントに関連付けられたポート（存在する場合）他のタイプのホワイト リスト違反の場合、このフィールドは空白です。

説明	ホワイト リスト違反の説明。次に例を示します。
	`Client "AOL Instant Messenger" is not allowed.`
	アプリケーション プロトコルに関係する違反は、アプリケーション プロトコルの名前とバージョンだけでなく、それが使用しているポートとプロトコル（TCP または UDP）も示します。禁止を特定のオペレーティング システムに限定する場合は、説明にオペレーティング システム名が含まれます。次に例を示します。
	`Server "ssh / 22 TCP ( OpenSSH 3.6.1p2 )" is not allowed on Operating System "Linux Linux 2.4 or 2.6".`

ポリシー（Policy）	違反した相関ポリシー、つまりホワイト リストを含む相関ポリシーの名前。
ホワイトリスト	ホワイト リストの名前。
プライオリティ	ポリシーまたはポリシー違反をトリガーしたホワイト リストで指定された優先度。相関ルールとポリシーの優先度の設定方法については、ポリシーの基本情報の指定（51-50 ページ）とルールおよびホワイトリストのプライオリティの設定（51-52 ページ）を参照してください。
Host Criticality	ホワイト リストに準拠していないホストに対してユーザが割り当てたホスト重要度（[None]、[Low]、[Medium]、または [High]）。 ホスト重要度の詳細については、事前定義のホスト属性の使用（49-34 ページ）を参照してください。
デバイス	ホワイト リスト違反を検出した管理対象デバイスの名前。
Count	各ローに表示される情報に一致するイベントの数。[Count] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

コンプライアンス ホワイト リスト イベントの検索

ライセンス：FireSIGHT

特定のコンプライアンス ホワイト リスト イベントを検索できます。ネットワーク環境に合わせてカスタマイズした検索を作成して保存しておけば、後で再利用することができます。次の表に、使用可能な検索基準の説明を示します。

表 52-5　コンプライアンス ホワイト リスト イベントの検索基準

フィールド	検索基準ルール
ポリシー（Policy）	相関ポリシーに含まれるホワイト リストの違反によって引き起こされたすべてのイベントを返す相関ポリシーの名前を入力します。
ホワイトリスト	ホワイト リストの違反によって引き起こされたすべてのイベントを返すホワイト リストの名前を入力します。
説明	ホワイト リスト イベントの説明を入力します。
プライオリティ	相関ポリシー内のホワイト リストの優先度または相関ポリシー自体の優先度によって決定されるホワイト リスト イベントの優先度を指定します。ホワイト リストの優先度のほうがそのポリシーの優先度より優先されることに注意してください。優先度がない場合は、「none」と入力します。 相関ルールとポリシーの優先度の設定方法については、ポリシーの基本情報の指定（51-50 ページ）とルールおよびホワイトリストのプライオリティの設定（51-52 ページ）を参照してください。
IP Address	ホワイト リストに非準拠になったホストの IP アドレスを指定します。
User	ホワイト リストに非準拠になったホストにログインしていたユーザの ID を指定します。
Port	アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーした検出イベントに関連付けられたポート（存在する場合）を指定します。
Host Criticality	ホワイト リスト イベントに関係するソース ホストのホスト重要度（[None]、[Low]、[Medium]、または [High]）を指定します。ホスト重要度の詳細については、事前定義のホスト属性の使用（49-34 ページ）を参照してください。
デバイス	ホワイト リスト違反を検出した特定のデバイスに検索を制限するには、デバイス名か IP アドレス、デバイス グループ、スタック、またはクラスタ名を入力します。FireSIGHT システム が検索でデバイス フィールドを処理する方法については、検索でのデバイスの指定（60-7 ページ）を参照してください。

コンプライアンス ホワイト リスト イベントを検索する方法：

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　テーブル ドロップダウンリストから [White List Events] を選択します。

ページが適切な制約によって更新されます。

ステップ 3　表 52-5（52-36 ページ）の説明に従って、該当するフィールドに検索基準を入力します。このとき、次の点に留意してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「`A`」または「`B`」または「`C, D, E`」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク（*）を受け入れます。
- フィールドでその情報を利用できないイベントを示すには、そのフィールドで `n/a` を指定します。フィールドに情報が入力されているイベントを示すには `!n/a` を使用します。
- 検索基準としてオブジェクトを使用する場合は、検索フィールドの横に表示されたオブジェクト追加アイコン（ ＋ ）をクリックします。

検索でのオブジェクトの使用を含む検索構文の詳細については、イベントの検索（60-1 ページ）を参照してください。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　検索をカスタム ユーザ ロールのデータ制限として使用する場合は、**必ず**プライベート検索として保存してください。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。
- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save As New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

デフォルト ホワイト リスト イベント ワークフローに、現在の時刻範囲に制限された検索結果が表示されます。カスタム ワークフローを含む別のワークフローを使用するには、ワークフロー タイトルのそばにある [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

ホワイト リスト違反の処理

ライセンス： FireSIGHT

システムは、ネットワーク上のホストがアクティブな相関ポリシー内のコンプライアンス ホワイト リストにどのように違反しているかを追跡します。これらのレコードを検索して表示することができます。

詳細については、次の項を参照してください。

- ホワイト リスト違反の表示（52-38 ページ）
- ホワイト リスト違反テーブルについて（52-40 ページ）
- ホワイト リスト違反の検索（52-41 ページ）

ホワイト リスト違反の表示

ライセンス： FireSIGHT

Defense Centerを使用して、ホワイト リスト違反のテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。ホワイト リスト違反にアクセスしたときに表示されるページは使用しているワークフローによって異なります。次の 2 つの事前定義ワークフローが用意されています。

- ホスト違反カウント ワークフローには、1 つ以上のホワイト リストに違反したすべてのホストが一覧表示された一連のページが示されます。最初のページでは、ホストがホストあたりの違反数に基づいてソートされ、違反数が最大のホストがリストの先頭に表示されます。ホストが複数のホワイト リストに違反している場合は、違反しているホワイト リストごとに別の行が表示されます。ワークフローには、最近検出された違反を先頭に、すべての違反を一覧表示するホワイト リスト違反のテーブル ビューも含まれています。テーブル内の各行に 1 つずつ検出された違反が示されます。
- ホワイト リスト違反ワークフローには、最近検出された違反を先頭に、すべての違反を一覧表示するホワイト リスト違反のテーブル ビューが含まれています。テーブル内の各行に 1 つずつ検出された違反が示されます。

両方の事前定義ワークフローが、制限を満たすすべてのホストのホスト プロファイルを含むホスト ビューで終わります。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。詳細については、カスタム ワークフローの作成（58-43 ページ）を参照してください。

次の表に、ホワイト リスト違反ワークフロー ページで実行可能な特定の操作の説明を示します。

表 52-6　コンプライアンス ホワイト リスト違反の操作

目的	操作
ホストのホスト プロファイルを表示する	IP アドレスの横に表示されたホスト プロファイル アイコン（  ）をクリックします。
現在のワークフロー ページでイベントをソートしたり、制限したりする	ドリルダウン ワークフロー ページのソート（58-38 ページ）で詳細を参照してください。
現在のワークフロー ページ内で移動する	ワークフロー内の他のページへのナビゲート（58-39 ページ）で詳細を参照してください。
現在の制限を維持して、現在のワークフロー内のページ間を移動する	ワークフロー ページの左上で、該当するページ リンクをクリックします。詳細については、ワークフローのページの使用（58-21 ページ）を参照してください。
表示された列の詳細を表示する	ホワイト リスト違反テーブルについて（52-40 ページ）で詳細を参照してください。
ワークフロー内の次のページにドリルダウンする	次のいずれかの方法を使用します。 • 特定の値に制限して、次のワークフロー ページにドリルダウンするには、行内の値をクリックします。この操作はドリルダウン ページでのみ可能です。テーブル ビューの行内の値をクリックすると、テーブル ビューが制約されます（次のページにはドリルダウンされません）。ドリルダウン**されません**。 • いくつかのイベントによって制約したまま次のワークフロー ページにドリルダウンするには、次のワークフロー ページに表示させるイベントの横のチェック ボックスを選択し、[View] をクリックします。 • 現在の制限を維持して次のワークフロー ページにドリルダウンするには、[View All] をクリックします。 **ヒント**　テーブル ビューでは、必ずページ名に「Table View」が含まれます。 詳細については、イベントの制約（58-35 ページ）を参照してください。
他のイベント ビューに移動して関連イベントを表示する	ワークフロー間のナビゲート（58-40 ページ）で詳細を参照してください。

コンプライアンス ホワイト リスト違反を表示する方法：

アクセス： Admin/Any Security Analyst/Discovery Admin

ステップ 1　[Analysis] > [Correlation] > [White List Violations] の順に選択します。

デフォルト ホワイト リスト違反ワークフローの最初のページが表示されます。カスタム ワークフローを含む別のワークフローを使用するには、ワークフロー タイトルのそばにある [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

ホワイト リスト違反テーブルについて

ライセンス：FireSIGHT

相関ポリシー機能を使用して*相関ポリシー*を作成し、システムがネットワーク上の脅威にリアルタイムに対処するように設定できます。相関ポリシーには、コンプライアンス ホワイト リスト違反を含む、ポリシー違反を構成する活動の種類が記載されます。相関ポリシーの詳細については、相関ポリシーおよび相関ルールの設定（51-1 ページ）を参照してください。

コンプライアンス ホワイト リストに違反すると、その違反が記録されます。テーブル ビューにはネットワーク上の現在のホスト違反しか表示されないため、イベント時間制限をテーブル ビューに設定できないことに注意してください。ホワイト リスト違反テーブル内のフィールドの説明を次の表に示します。

表 52-7　コンプライアンス ホワイト リスト違反のフィールド

フィールド	説明
時刻	ホワイト リスト違反が検出された日時。
IP Address	非準拠ホストの関連 IP アドレス。
タイプ	ホワイト リスト違反のタイプ、つまり、非準拠の結果として違反が発生したかどうか。 • オペレーティング システム（os） • アプリケーション プロトコル（server） • クライアント（client） • プロトコル（protocol） • Web アプリケーション（web）
Information	ホワイト リスト違反に関連付けられたすべての利用可能なベンダー、製品、またはバージョン情報。 たとえば、Microsoft Windows ホストのみを許可するホワイト リストを使用している場合は、[Information] フィールドに、Microsoft Windows を実行していないホストのオペレーティング システムが示されます。 ホワイト リストに違反するプロトコルの場合は、[Information] フィールドに、違反の原因がネットワーク プロトコルとトランスポート プロトコルのどちらなのかも示されます。
ポート	アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーしたイベントに関連付けられたポート（存在する場合）他のタイプのホワイト リスト違反の場合、このフィールドは空白です。
Protocol	アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーしたイベントに関連付けられたプロトコル（存在する場合）他のタイプのホワイト リスト違反の場合、このフィールドは空白です。
ホワイトリスト	違反されたホワイト リストの名前。
Count	各ローに表示される情報に一致するイベントの数。[Count] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

ホワイト リスト違反の検索

ライセンス：FireSIGHT

特定のコンプライアンス ホワイト リスト違反を検索できます。ネットワーク環境に合わせてカスタマイズした検索を作成して保存しておけば、後で再利用することができます。次の表に、使用可能な検索基準の説明を示します。

表 52-8　コンプライアンス ホワイト リスト違反の検索基準

フィールド	検索基準ルール
時刻	ホワイト リストが違反された日時を指定します。
IP Address	ホワイト リストに非準拠になったホストの IP アドレスを指定します。
ホワイトリスト	そのホワイト リストのすべての違反を返すホワイト リストの名前を入力します。
タイプ	ホワイト リスト違反のタイプを入力します。 • オペレーティング システムに基づいて違反を検索する場合は、「os」（または「operating system」）と入力します。 • アプリケーション プロトコルに基づいて違反を検索する場合は、「server」と入力します。 • クライアントに基づいて違反を検索する場合は、「client」と入力します。 • プロトコルに基づいて違反を検索する場合は、「protocol」と入力します。 • Web アプリケーションに基づいて違反を検索する場合は、「web application」と入力します。
Information	ホワイト リスト違反情報を入力します。
Port	アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーした検出イベントに関連付けられたポート（存在する場合）を指定します。
Protocol	アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーした検出イベントに関連付けられたプロトコル（存在する場合）を指定します。

コンプライアンス ホワイト リスト違反を検索する方法：

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　テーブル ドロップダウン リストから [White List Violations] を選択します。

ページが適切な制約によって更新されます。

ステップ 3　コンプライアンス ホワイト リスト イベントの検索基準の表の説明に従って、該当するフィールドに検索基準を入力します。このとき、次の点に留意してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。

  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、A, B, "C, D, E" を検索すると、指定したフィールドに「A」または「B」または「C, D, E」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、A, B, "C, D, E" をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに A または B、または C、D、E のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク(*)を使用できます。
- そのフィールドで情報を利用できないイベントを特定するには、フィールドに n/a を指定します。そのフィールドに値が入力されているイベントを特定するには、!n/a を使用します。
- 検索基準としてオブジェクトを使用する場合は、検索フィールドの横に表示されたオブジェクト追加アイコン(+)をクリックします。

検索でのオブジェクトの使用を含む検索構文の詳細については、イベントの検索(60-1 ページ)を参照してください。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　検索をカスタム ユーザ ロールのデータ制限として使用する場合は、**必ず**プライベート検索として保存してください。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され([Private] を選択した場合は本人のアカウントでのみ閲覧可能)、後で実行できます。
- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save As New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され([Private] を選択した場合は本人のアカウントでのみ閲覧可能)、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

検索結果がデフォルト ホワイト リスト違反ワークフローに表示されます。カスタム ワークフローを含む別のワークフローを使用するには、ワークフロー タイトルのそばにある [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定(71-3 ページ)を参照してください。

CHAPTER 53

トラフィック プロファイルの作成

トラフィック プロファイルは、指定した期間にわたって収集された接続データに基づく、ネットワーク上のトラフィックに関する単なるプロファイルです。デバイスによって収集された接続データ、いずれか（またはすべて）の NetFlow 対応デバイスによってエクスポートされた接続データ、またはその両方を使用できます。

トラフィック プロファイルを作成した後、正常なネットワーク トラフィックを表すと想定されるプロファイルに照らして新しいトラフィックを評価することにより、異常なネットワーク トラフィックを検出できます。

FireSIGHT システムは接続データを使用して、トラフィック プロファイルを作成したり、トラフィック プロファイルの変化に基づいて相関ルールをトリガーしたりすることに注意してください。Defense Center データベースにログとして記録されない接続をトラフィック プロファイルに含めることはできません。接続の要約（接続サマリーについて（39-3 ページ）を参照）の生成には、接続終了時のデータだけが使用されます。システムはその後、この要約を使って接続グラフやトラフィック プロファイルを作成します。したがって、トラフィック プロファイルを作成/使用するには、必ず接続終了時における接続イベントをログに記録してください。

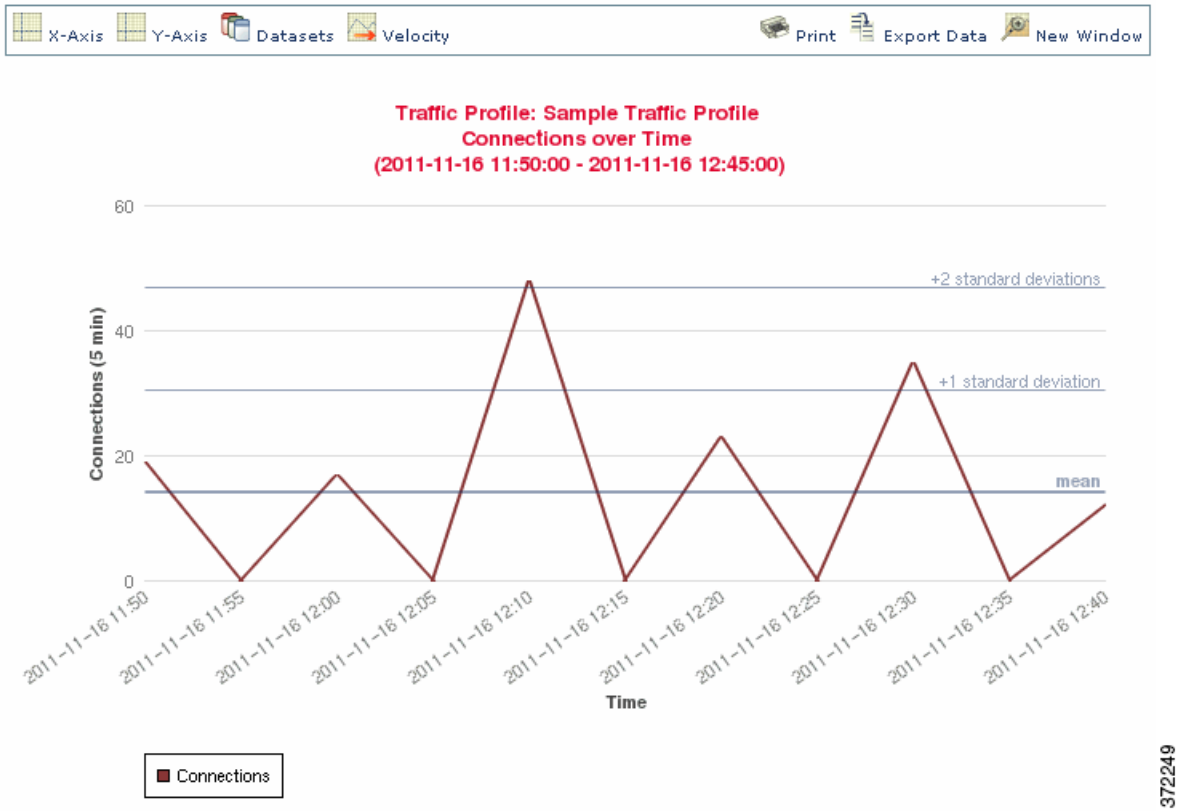
トラフィック プロファイルを構築するためのデータ収集期間を、プロファイル作成時間枠（PTW）と呼びます。PTW はスライディング時間枠です。つまり、PTW が 1 週間（デフォルト）の場合、先週の間に収集された接続データがトラフィック プロファイルに含まれます。PTW を最短で 1 時間、最長で数週間に変更できます。

初めてトラフィック プロファイルをアクティブにすると、学習期間（PTW と等しい時間）にわたる接続データが、設定した基準に従って収集され、評価されます。トラフィック プロファイルに関して作成したルールは、学習期間が完了するまではDefense Centerで評価されません。

モニタ対象のネットワーク セグメント上のすべてのトラフィックを使ってプロファイルを作成することも、接続イベント内のデータに基づく基準を使用して、さらにターゲットを絞ったプロファイルを作成することもできます。たとえば、検出されたセッションで特定のポート、プロトコル、アプリケーションが使われている場合にのみトラフィック プロファイルでデータを収集するよう、プロファイル条件を設定できます。あるいは、ホスト重要度が **High** であるホストのデータだけを収集するよう、トラフィック プロファイルにホスト プロファイル限定を追加することもできます。

最後に、トラフィック プロファイルを作成する際には、非アクティブ期間を指定できます。この期間内は、接続データがプロファイル統計情報に影響を及ぼさず、プロファイルに関して作成されたルールはトリガーしません。また、収集済みの接続データをどれほどの頻度でトラフィック プロファイルで集約し、統計情報を計算するかを変更することもできます。

次の図は、PTW 1 日、およびサンプリング レート 5 分のトラフィック プロファイルを示しています。



トラフィック プロファイルを作成してアクティブにした後、その学習期間が完了したら、異常なトラフィックの検出時にトリガーされる相関ルールを作成することができます。たとえば、ネットワークを通過するデータ量（パケット数、KB 数、または接続数で測定）が、平均トラフィック量に比べて標準偏差の 3 倍も急激に上昇した場合、攻撃または他のセキュリティ ポリシー違反を示す可能性があると判断してトリガーするルールを作成できます。その後、このルールを相関ポリシーに組み込んで、トラフィックの急増に関するアラートを出したり、応答として修復を実行したりできます。トラフィック プロファイルを使用して異常なネットワーク トラフィックを検出する方法については、相関ポリシーのルールの作成（51-3 ページ）を参照してください。

[Traffic Profiles] ページでトラフィック プロファイルを作成します。各プロファイルの隣にあるスライダ アイコンは、プロファイルがアクティブであるかどうかを示します。トラフィック プロファイルの変化に基づく相関ルールを使用するには、プロファイルをアクティブにする必要があります。スライダ アイコンが青色でチェック マークが付いている場合は、そのプロファイルがアクティブです。灰色で x が表示されている場合は、プロファイルが非アクティブです。詳細については、トラフィック プロファイルのアクティブ化と非アクティブ化（53-9 ページ）を参照してください。

経過表示バーは、トラフィック プロファイルの学習期間の状態を示します。経過表示バーが 100% に達すると、プロファイルに関して作成された相関ルールがトリガーとして使用されます。

ヒント　[Sort by] ドロップダウン リストを使用すると、状態別（アクティブ/非アクティブ）または名前のアルファベット順でトラフィック プロファイルをソートできます。

詳細については、以下を参照してください。

基本的なプロファイル情報の指定

ライセンス： FireSIGHT

トラフィック プロファイルを作成するときには、名前を付ける必要があり、オプションで短い説明を入力します。

トラフィック プロファイルの作成を開始する方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Policies] > [CorrelationSelect] を選択してから、[Traffic Profiles] をクリックします。

[Traffic Profiles] ページが表示されます。

ステップ 2　[New Profile] をクリックします。

[Create Profile] ページが表示されます。

ステップ 3　[Profile Name] フィールドに、新しいトラフィック プロファイルの名前を最大 255 文字で入力します。

ステップ 4　[Profile Description] フィールドに、新しいトラフィック プロファイルの短い説明を最大 255 文字で入力します。

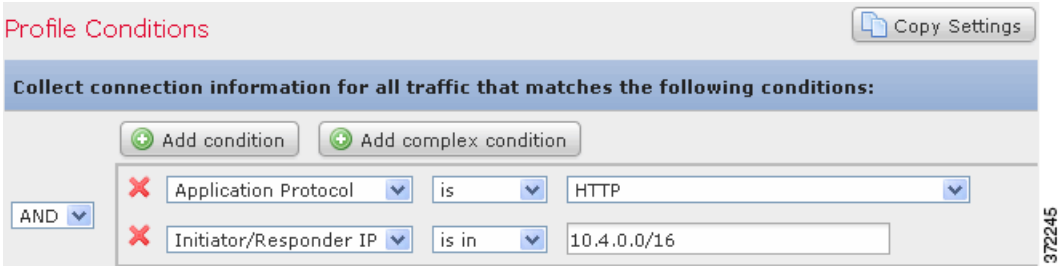
ステップ 5　トラフィック プロファイル条件の指定に進みます。

トラフィック プロファイル条件の指定

ライセンス： FireSIGHT

プロファイル条件は、トラフィック プロファイルで追跡する接続データの種類を制約します。単純なトラフィック プロファイルは、モニタ対象のネットワーク セグメント上のすべてのトラフィックに関するプロファイルを無条件で作成します。これに対し、複数の条件がネストされた、複雑なトラフィック プロファイルもあります。

たとえば、次の図のトラフィック プロファイル条件は、10.4.x.x サブネットでの HTTP 接続を収集します。



[Create Profile] ページの [Profile Conditions] セクションで、トラフィック プロファイル条件を作成します。条件の作成の詳細については、条件の作成手順について（53-10 ページ）を参照してください。また、条件を作成するために使用できる構文については、トラフィック プロファイル条件の構文（53-4 ページ）で詳しく説明しています。

ヒント　既存のトラフィック プロファイルの設定を使用するには、[Copy Settings] をクリックし、ポップアップ ウィンドウで、使用するトラフィック プロファイルを選択して [Load] をクリックします。

トラフィック プロファイル条件の構文

ライセンス：FireSIGHT

次の表で、トラフィック プロファイル条件を作成する方法について説明します。

NetFlow レコードには、接続の中でどのホストがイニシエータ/レスポンダであるかを示す情報が含まれないことに注意してください。システムが NetFlow レコードを処理するときには、各ホストが使用しているポート、およびそれらのポートがウェルノウンであるかどうかに基づき、アルゴリズムに従ってその情報が判別されます。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

トラフィック プロファイルで使用可能な情報は、検出方法、ロギング方法、イベント タイプなど、いくつかの要因により異なります。詳細については、接続およびセキュリティ インテリジェンスのイベントで利用可能な情報（39-12 ページ）を参照してください。

表 53-1　プロファイル条件の構文

指定する項目	演算子を指定した後に行う操作
Application Protocol	使用可能なプロトコルを示すドロップダウン リストから、アプリケーション プロトコルの名前を選択します。
Application Protocol Category	使用可能なカテゴリを示すドロップダウン リストから、アプリケーション プロトコルのカテゴリ名を選択します。
Client	使用可能なクライアントを示すドロップダウン リストから、クライアント名を選択します。
Client Category	使用可能なカテゴリを示すドロップダウン リストから、クライアントのカテゴリ名を選択します。
Connection Type	トラフィック プロファイル内で、Ciscoデバイスによって収集された接続データと NetFlow 対応デバイスによって収集された接続データのどちらを使用するかを指定します。接続タイプを指定しない場合、トラフィック プロファイルには両方が含まれます。

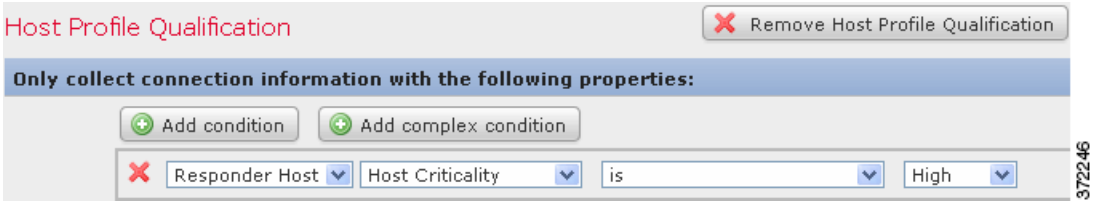
表 53-1　プロファイル条件の構文（続き）

指定する項目	演算子を指定した後に行う操作
Destination Country または Source Country	選択可能な国を示すドロップダウン リストから、国を選択します。これは、ネットワーク トラフィック内で識別される送信元 IP アドレスや宛先 IP アドレスに関連付けられる国を表します。
Initiator IP、Responder IP、または Initiator/Responder IP	IP アドレスの範囲を指定するには、特定の IP アドレスか CIDR 表記を使用します。 IP アドレスに使用できる構文の説明については、検索での IP アドレスの指定（60-6 ページ）を参照してください。なお、モニタ対象のネットワーク内またはネットワーク外の IP アドレスを指定するためにキーワード `local` および `remote` を使用**できない**ことに注意してください。
NetFlow Device	トラフィック プロファイルの作成に使われるデータのエクスポート元となる NetFlow 対応デバイスを選択します。（ローカル設定を使用して）展開環境に NetFlow 対応デバイスをまだ追加していない場合、[NetFlow Device] ドロップダウン リストは空白になります。
Responder Port/ICMP Code	ポート番号または ICMP コードを入力します。
Security Intelligence Category	使用可能なカテゴリを示すドロップダウン リストから、セキュリティ インテリジェンスのカテゴリ名を選択します。トラフィック プロファイル条件でセキュリティ インテリジェンス カテゴリを使用するには、アクセス制御ポリシーの [Security Intelligence] セクションで、そのカテゴリを [Block] ではなく [Monitor] に設定する必要があります。詳細については、セキュリティ インテリジェンスのホワイトリストおよびブラックリストの作成（13-4 ページ）を参照してください。
SSL Encrypted Session	[Successfully Decrypted] を選択します。
トランスポート プロトコル	トランスポート プロトコルとして `TCP` または `UDP` と入力します。
Web Application	使用可能な Web アプリケーションを示すドロップダウン リストから、Web アプリケーションの名前を選択します。
Web Application Category	使用可能なカテゴリを示すドロップダウン リストから、Web アプリケーションのカテゴリ名を選択します。

ホスト プロファイル限定の追加

ライセンス：FireSIGHT

追跡対象のホストのプロファイル情報を使用して、トラフィック プロファイルを制約できます。この制約は、*ホスト プロファイル限定*と呼ばれます。たとえば、次の図に示すように、ホスト重要度 **High** が割り当てられたホストの接続データだけを収集することができます。



ホスト プロファイル限定を使用するには、そのホストがデータベース内に存在すること、および限定として使用するホスト プロファイル プロパティがホスト プロファイルにすでに含まれていることが必要です。たとえば、Windows を実行するホストで侵入イベントが生成されると相関ルールがトリガーされるよう設定した場合、そのルールがトリガーされるのは、侵入イベント生成時にホストがすでに Windows として識別されている場合だけです。

ホスト プロファイル限定を追加する方法:

アクセス: Admin/Discovery Admin

ステップ 1　[Create Profile] ページで、[Add Host Profile Qualification] をクリックします。

[Host Profile Qualification] セクションが表示されます。

ステップ 2　ホスト プロファイル限定の条件を作成します。

1 つの単純な条件を作成することも、複数の条件の組み合わせやネストを使って複雑な構造を作成することもできます。条件の作成の詳細については、条件の作成手順について（53-10 ページ）を参照してください。

条件を作成するために使用できる構文については、ホスト プロファイル限定の構文（53-6 ページ）で説明しています。

ヒント　ホスト プロファイル限定を削除するには、[Remove Host Profile Qualification] をクリックします。

ホスト プロファイル限定の構文

ライセンス: FireSIGHT

ホスト プロファイル限定の条件を作成するときには、まず、トラフィック プロファイルを制約するために使用するホストを選択する必要があります。[Responder Host] または [Initiator Host] を選択できます。ホストの役割を選択した後、ホスト プロファイル限定の構文の表の説明に従ってホスト プロファイル限定条件の作成を続けます。

NetFlow 対応デバイスによってエクスポートされたデータに基づきネットワーク マップにホストを追加するようネットワーク検出ポリシーを設定することはできますが、これらのホストに関して使用可能な情報は限られています。たとえば、これらのホストのオペレーティング システム データは得られません（ただしホスト入力機能を使って指定する場合を除く）。さらに、NetFlow 対応デバイスによってエクスポートされた接続データをトラフィック プロファイルで使用する場合、NetFlow レコードには、どのホストが接続のイニシエータで、どのホストがレスポンダであるかを示す情報が含まれないことに注意してください。システムが NetFlow レコードを処理するときには、各ホストが使用しているポート、およびそれらのポートがウェルノウンであるかどうかに基づき、アルゴリズムに従ってその情報が判別されます。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

暗黙的（または汎用の）クライアントを照合するには、クライアントに応答するサーバーで使われるアプリケーション プロトコルに基づいてホスト プロファイル限定を作成します。接続のイニシエータ（または送信元）として機能するホスト上のクライアント リストに含まれるアプリケーション プロトコル名の後に**クライアント**が続いている場合、そのクライアントは実際には暗黙的クライアントである可能性があります。つまり、検出されたクライアント トラフィックに基づいてではなく、そのクライアントのアプリケーション プロトコルを使用するサーバー応答トラフィックに基づいて、システムがそのクライアントを報告します。

たとえば、ホスト上のクライアントとして **HTTPS クライアント**がシステムにより報告される場合、[Application Protocol] を [HTTPS] に設定した [Responder Host] のホスト プロファイル限定を作成します。これは、レスポンダまたは宛先ホストから送られる HTTPS サーバ応答トラフィックに基づいて HTTPS クライアントが汎用クライアントとして報告されるためです。

表 53-2　ホスト プロファイル限定の構文

指定する項目	演算子を指定した後に行う操作
Host Type	ドロップダウン リストから 1 つ以上のホスト タイプを選択します。通常のホスト、またはいずれかのタイプのネットワーク デバイスを選択できます。
NETBIOS Name	ホストの NetBIOS 名を入力します。
Operating System > OS Vendor	ドロップダウン リストから、1 つ以上のオペレーティング システム ベンダー名を選択します。
Operating System > OS Name	ドロップダウン リストから、1 つ以上のオペレーティング システムの名前を選択します。
Operating System > OS Version	ドロップダウン リストから、1 つ以上のオペレーティング システムのバージョンを選択します。
Network Protocol	http://www.iana.org/assignments/ethernet-numbers にリストされているネットワーク プロトコル番号を入力します。
トランスポート プロトコル	トランスポート プロトコルの名前、または http://www.iana.org/assignments/protocol-numbers にリストされている番号を入力します。
Host Criticality	表示されるリストから、ホストの重要度を選択します。[None] 、[Low] 、[Medium] 、または [High] を選択できます。ホストの重要度の詳細については、事前定義のホスト属性の使用（49-34 ページ）を参照してください。
VLAN ID	ホストの VLAN ID 番号を入力します。
Application Protocol > アプリケーション プロトコル	ドロップダウン リストから、アプリケーション プロトコルを選択します。
Application Protocol > Application Port	アプリケーション プロトコルのポート番号を入力します。
Application Protocol > プロトコル	ドロップダウン リストからプロトコルを選択します。
Client > Client	ドロップダウン リストからクライアントを選択します。
Client > Client Version	クライアントのバージョンを入力します。
Web アプリケーション	ドロップダウン リストからクライアントを選択します。
MAC Address > MAC Address	ホストの MAC アドレス全体またはその一部を入力します。
MAC Address > MAC Type	MAC タイプが ARP/DHCP で検出されたかどうかを選択します。 つまり、MAC アドレスがホストに属していることをシステムが識別したのか（**is ARP/DHCP Detected**）、デバイスとホストの間にルータがあるなどの理由で、その MAC アドレスを持つ多数のホストをシステムが認識しているのか（**is not ARP/DHCP Detected**）、または MAC タイプが無関係であるのか（**is any**）を選択します。
MAC Vendor	ホストで使用されているハードウェアの MAC ベンダー全体またはその一部を入力します。

表 53-2　ホスト プロファイル限定の構文（続き）

指定する項目	演算子を指定した後に行う操作
使用可能な任意のホスト属性（デフォルト コンプライアンス ホワイトリスト ホスト属性を含む）	選択するホスト属性のタイプに応じて、適切な値を次のように指定します。 • ホスト属性タイプが Integer の場合、その属性で定義されている範囲内の整数値を入力します。 • ホスト属性タイプが Text の場合、テキスト値を入力します。 • ホスト属性タイプが List の場合は、ドロップダウン リストから有効なリスト文字列を選択します。 • ホスト属性タイプが URL の場合、URL 値を入力します。 ホスト属性の詳細については、ユーザ定義のホスト属性の使用（49-35 ページ）を参照してください。

プロファイル オプションの設定

ライセンス：FireSIGHT

プロファイル作成時間枠（PTW）はスライド時間枠です。これは、FireSIGHT システムでトラフィック プロファイルの統計情報の計算に使用される、学習期間と同じ長さの時間です。デフォルト PTW は 1 週間ですが、最短で 1 時間、最長で数週間に変更できます。

また、トラフィック プロファイルは集約された接続データに基づきます。デフォルトで、トラフィック プロファイルは 5 分間隔でシステム生成の接続イベントに関する統計情報を生成します。ただし、デフォルトの 5 分から 1 時間までの範囲で、このサンプリング レートを設定できます。

統計的に意味のある十分なデータがトラフィック プロファイルに含まれるように、PTW とサンプリング レートを設定する必要があることに注意してください。たとえば PTW が 1 日、サンプリング レートが 1 時間の場合、それに含まれるデータ ポイントは 24 個だけであるため、ネットワーク トラフィックのパターンを正確に分析するには不十分な可能性があります。

ヒント　PTW には少なくとも 100 個のデータ ポイントを含めてください。

また、トラフィック プロファイル内で非アクティブ期間をセットアップすることもできます。たとえば、すべてのワークステーションが毎日深夜 0:00 にバックアップされるネットワーク インフラストラクチャがあるとします。バックアップには約 30 分かかり、ネットワーク トラフィックが急増します。この場合、スケジュール済みバックアップと同じ時間帯にトラフィック プロファイルの非アクティブ期間を繰り返すようセットアップできます。非アクティブ期間中は、トラフィック プロファイルがデータを収集します（したがってトラフィック プロファイルのグラフにトラフィックが表示されます）が、プロファイル統計情報の計算時にはこのデータが使用されません。非アクティブ期間を毎日、毎週、または毎月繰り返すように設定できます。非アクティブ期間は最短で 5 分、最長で 1 時間にすることができます。トラフィック プロファイルの時系列グラフでは、非アクティブ期間が網掛け領域として示されます。

プロファイル オプションを設定するには、次の操作を実行します。

アクセス：Admin/Discovery Admin

表 53-3　プロファイル オプション

実行する操作	操作
プロファイル作成時間枠の変更	[Profiling Time Window] フィールドで、時間、日、または週の数値を入力します。次に、ドロップダウン リストから [hour(s)]、[day(s)]、または [week(s)] を選択します。
サンプリング レートの変更	[Sampling Rate] ドロップダウン リストからレートを選択します。
非アクティブ期間の追加	[Add Inactive Period] をクリックします。次に、ドロップダウン リストを使用して、トラフィック プロファイルでのデータ収集を中断する時点と頻度を指定します。
非アクティブ期間の削除	削除する非アクティブ期間の横の [Delete] をクリックします。

トラフィック プロファイルの保存

ライセンス：FireSIGHT

トラフィック プロファイルを保存するには、次の手順に従います。

トラフィック プロファイルを保存する方法：

アクセス：Admin/Discovery Admin

ステップ 1　次の 2 つのオプションから選択できます。

- アクティブ化せずにプロファイルを保存するには、[Save] をクリックします。
- プロファイルを保存し、ただちにデータを収集し始めるには、[Save & Activate] をクリックします。

トラフィック プロファイルのアクティブ化と非アクティブ化

ライセンス：FireSIGHT

モニタ対象ネットワーク セグメント上のトラフィックのプロファイル作成を開始するには、トラフィック プロファイルをアクティブにする必要があります。

接続データの収集と評価を停止するには、プロファイルを非アクティブにします。非アクティブ化されトラフィック プロファイルに関して作成されたルールは、トリガーされません。さらに、トラフィック プロファイルを非アクティブにすると、そのプロファイルによってすでに収集/集約されたデータがすべて削除されます。非アクティブにしたトラフィック プロファイルを後で再度アクティブにした場合、そのプロファイルに関して作成されたルールがトリガーするようになるまで、PTW の長さだけ待つ必要があります。

トラフィック プロファイルをアクティブまたは非アクティブにする方法:

アクセス: Admin/Discovery Admin

ステップ 1 [Policies] > [CorrelationSelect] を選択してから、[Traffic Profiles] をクリックします。

[Traffic Profiles] ページが表示されます。

ステップ 2 次の 2 つのオプションから選択できます。

- 非アクティブなトラフィック プロファイルをアクティブにするには、プロファイルの隣の [Activate] をクリックします。
- アクティブなトラフィック プロファイルを非アクティブにするには、プロファイルの隣の [Deactivate] をクリックします。[OK] をクリックして、プロファイルを非アクティブにすることを確認します。

トラフィック プロファイルの編集

ライセンス: FireSIGHT

アクティブなトラフィック プロファイルを実質的に編集することはできません。トラフィック プロファイルがアクティブな場合には、名前と説明のみを変更できます。トラフィック プロファイルの条件オプションを編集するには、まず非アクティブにする必要があります。なお、トラフィック プロファイルを非アクティブにすると、すでに収集されたデータがすべて削除されることに注意してください。

トラフィック プロファイルのアクティブ化と非アクティブ化の詳細については、トラフィック プロファイルのアクティブ化と非アクティブ化（53-9 ページ）を参照してください。

トラフィック プロファイルを編集する方法:

アクセス: Admin/Discovery Admin

ステップ 1 [Policies] > [CorrelationSelect] を選択してから、[Traffic Profiles] をクリックします。

[Traffic Profiles] ページが表示されます。

ステップ 2 編集するトラフィック プロファイルの横にある [Edit] をクリックします。

[Create Profile] ページが表示されます。

ステップ 3 プロファイルを変更して、[Save] をクリックします。

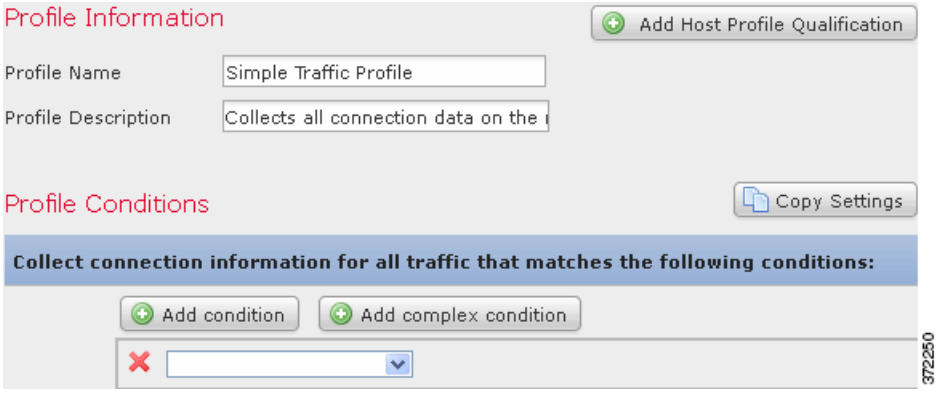
プロファイルが更新されます。

条件の作成手順について

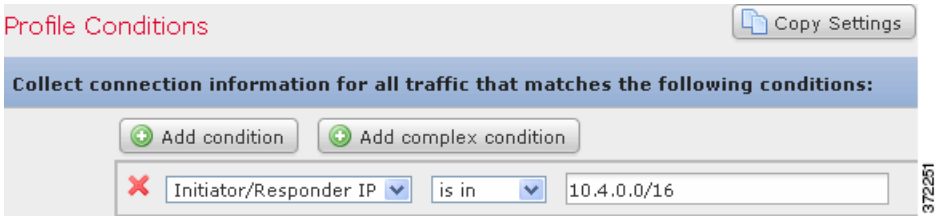
ライセンス: FireSIGHT

トラフィック プロファイルを作成する際には、データの収集に使われる条件を指定します。単純な条件を作成することも、条件をネストさせた複雑な構造を作成することもできます。

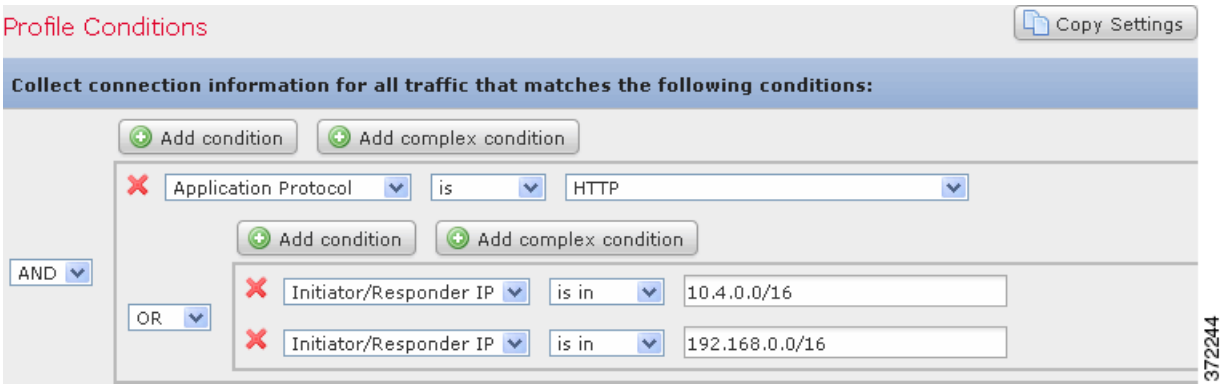
たとえば、モニタ対象ネットワーク セグメント全体のデータを収集するトラフィック プロファイルを作成するには、次の図のように、条件を含まない非常に単純なプロファイルを作成できます。



プロファイルを制約して、10.4.x.x ネットワークのデータのみを収集するにはは、次の図のように 1 つの条件を追加できます。



一方、次のトラフィック プロファイルは 10.4.x.x ネットワークと 192.168.x.x ネットワーク上の HTTP アクティビティを収集しますが、3 つの条件のうち最後は複合条件を形成しています。



条件で使用できる構文は、作成しようとしている要素により異なりますが、メカニズムはすべて同じです。詳細については、以下を参照してください。

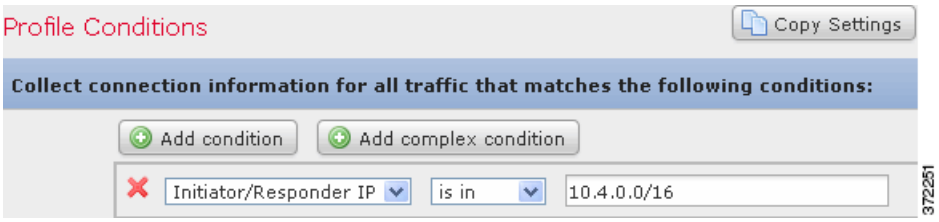
- 単一の条件の作成（53-12 ページ）
- 条件の追加と結合（53-14 ページ）
- 複数の値を条件で使用する（53-16 ページ）

単一の条件の作成

ライセンス：FireSIGHT

ほとんどの条件は、カテゴリ、演算子、値の 3 つの部分からなります。もっと複雑な条件もあり、それぞれ独自の演算子と値を持つ複数のカテゴリが含まれることがあります。

たとえば、次のトラフィック プロファイルは 10.4.x.x ネットワーク上の情報を収集します。条件のカテゴリは [Initiator/Responder IP]、演算子は [is in]、値は `10.4.0.0/16` です。



次の手順では、このトラフィック プロファイル条件を作成する方法について説明します。

1 つの条件を構築する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [CorrelationSelect] を選択してから、[Traffic Profiles] をクリックします。

[Traffic Profiles] ページが表示されます。

ステップ 2　[New Profile] をクリックします。

[Create Profile] ページが表示されます。

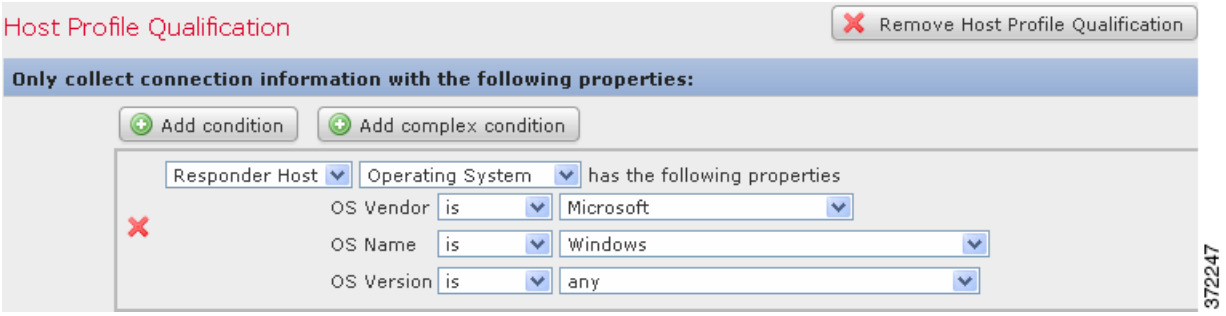
ステップ 3　[Profile Conditions] の下で、最初の（カテゴリ）ドロップダウン リストから [Initiator/Responder IP] を選択して、プロファイルの単一条件を作成し始めます。

ステップ 4　2 番目の（演算子）ドロップダウン リストから [is in] を選択します。

ヒント　カテゴリが IP アドレスを表している場合、演算子として [is in] または [is not in] を選択すると、CIDR 表記で表される IP アドレス範囲内にその IP アドレスが*含まれる*のか、*含まれない*のかを指定できます。FireSIGHT システムでの CIDR 表記の使用法の詳細については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ステップ 5　テキスト フィールドに `10.4.0.0/16` と入力します。

一方、次のホスト プロファイル限定はもっと複雑です。これによりトラフィック プロファイルが制約され、検出された接続内の応答側ホストで任意のバージョンの Microsoft Windows が実行されている場合にのみ、接続データが収集されます。



次の手順では、このホスト プロファイル限定の作成方法について説明します。

このホスト プロファイル限定を作成する方法:

アクセス: Admin/Discovery Admin

ステップ 1　[Policies] > [CorrelationSelect] を選択してから、[Traffic Profiles] をクリックします。

[Traffic Profiles] ページが表示されます。

ステップ 2　[New Profile] をクリックします。

[Create Profile] ページが表示されます。

ステップ 3　[Add Host Profile Qualification] をクリックします。

ステップ 4　[Host Profile Qualification] の下の最初の条件で、情報を収集する対象となるホストを指定します。

この例では、接続内の応答側ホストに関する情報だけが必要なので、[Responder Host] を選択します。

ステップ 5　ホストのオペレーティング システムの詳細を指定するために、まず [Operating System] カテゴリを選択します。

[OS Vendor]、[OS Name]、[OS Version] の 3 つのサブカテゴリが表示されます。

ステップ 6　ホストが Microsoft Windows のどのバージョンを実行していても差し支えないことを指定するには、3 つのサブカテゴリすべてに同じ演算子 [is] を使用します。

ステップ 7　最後に、サブカテゴリの値を指定します。

[OS Vendor] の値には [Microsoft]、[OS Name] の値には [Windows] を選択し、[OS Version] の値は [any] のままにします。

トラフィック プロファイル条件を作成しているか、それともホスト プロファイル限定を作成しているかに応じて、選択できるカテゴリが異なることに注意してください。また、選択するカテゴリに応じて、条件で使用できる演算子が異なります。さらに、条件の値を指定するために使用できる構文は、カテゴリと演算子に応じて異なります。場合によっては、テキスト フィールドに値を入力する必要があります。それ以外の場合、ドロップダウン リストから値を選択できます。

注　条件の構文でドロップダウン リストから値を選択できる場合、通常はリストから複数の値を選択できます。詳細については、複数の値を条件で使用する (53-16 ページ) を参照してください。

トラフィック プロファイルの条件とホスト プロファイル限定を作成するための構文については、以下の項を参照してください。

- トラフィック プロファイル条件の構文（53-4 ページ）
- ホスト プロファイル限定の構文（53-6 ページ）

条件の追加と結合

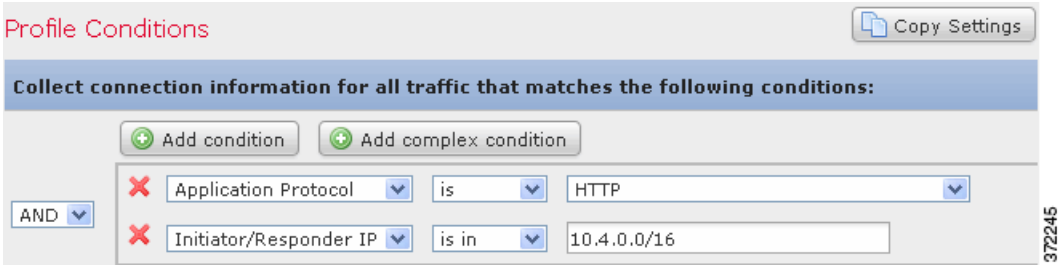
ライセンス：FireSIGHT

単純なトラフィック プロファイル条件やホスト プロファイル限定を作成することも、複数の条件の組み合わせやネストを使って複雑な構造を作成することもできます。

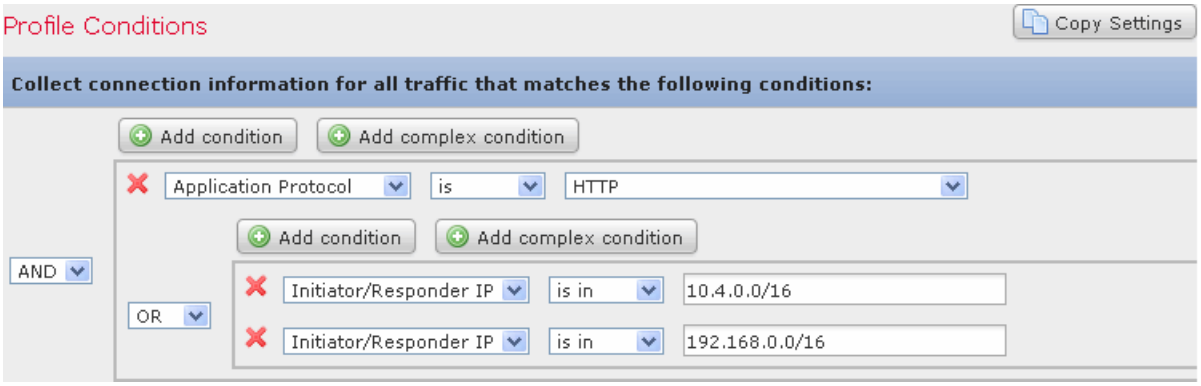
構造に複数の条件を含める場合は、それらの条件を **AND** または **OR** 演算子で結合する必要があります。同じレベルにある複数の条件は、一緒に評価されます。

- **AND** 演算子は、制御対象のレベルにあるすべての条件が満たされなければならないことを示します。
- **OR** 演算子は、制御対象のレベルにある少なくとも 1 つの条件が満たされなければならないことを示します。

たとえば、次のトラフィック プロファイルには、**AND** で結合された 2 つの条件が含まれます。つまり、両方の条件とも満たされる場合に限り、このトラフィック プロファイルが接続データを収集します。この例では、10.4.x.x サブネット内の IP アドレスを持つすべてのホストに関する HTTP 接続を収集します。



一方、次のトラフィック プロファイルは、10.4.x.x ネットワークまたは 192.168.x.x ネットワーク内の HTTP アクティビティに関する接続データを収集しますが、3 つの条件のうち最後は複合条件を形成しています。



論理的には、上記のトラフィック プロファイルは次のように評価されます。

(A および(B または C))

項目	条件で指定する内容
A	アプリケーション プロトコル名が HTTP である
B	IP アドレスが 10.4.0.0/16 内にある
C	IP アドレスが 192.168.0.0/16 内にある

単一の条件を追加する方法:

アクセス: Admin/Discovery Admin

ステップ 1　単一の条件を追加するには、現在の条件の上にある [Add condition] をクリックします。

新しい条件が、現在の条件セットと同じ論理レベルに追加されます。デフォルトでは、そのレベルの条件に **OR** 演算子で結合されますが、演算子を **AND** に変更することもできます。

たとえば、次のホスト プロファイル限定に単純な条件を追加すると、

結果は以下のとおりです。

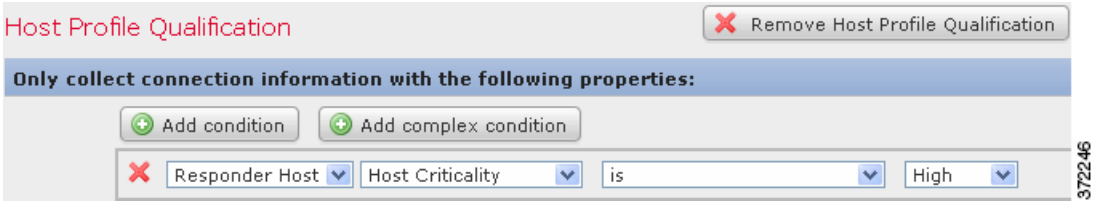
複合条件を追加する方法:

アクセス: Admin/Discovery Admin

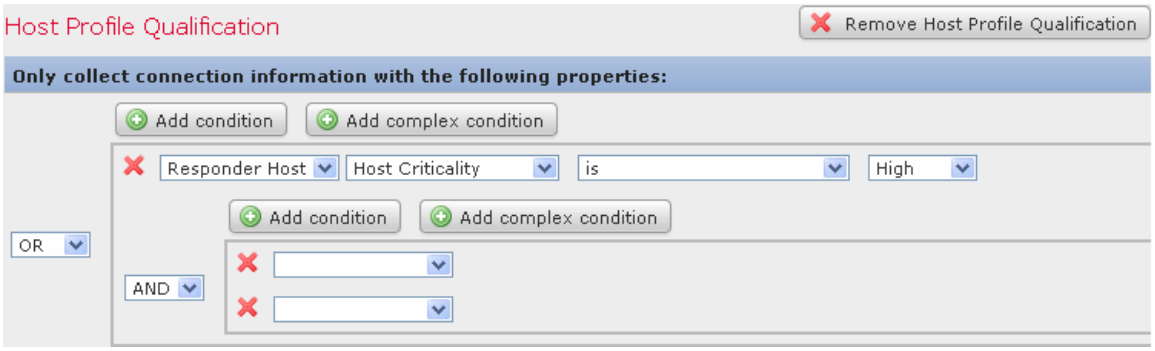
ステップ 1　現在の条件の上にある [Add complex condition] をクリックします。

現在の条件セットの下に複合条件が追加されます。1 つの複合条件は 2 つの副条件からなり、演算子(その上のレベルにある条件を結合するために使われているものとは逆の演算子)を使って副条件が互いに結合されます。

たとえば、次のホスト プロファイル限定に複合条件を追加すると、



結果は以下のとおりです。



条件を結合する方法:

アクセス: Admin/Discovery Admin

ステップ 1　条件セットの左側にあるドロップダウン リストを次のように使用します。

- 演算子で制御されるレベルのすべての条件が満たされるべきことを指定するには、[AND] を選択します。
- 演算子で制御されるレベルの 1 つの条件だけが満たされるべきことを指定するには、[OR] を選択します。

複数の値を条件で使用する

ライセンス: FireSIGHT

条件を作成するときに、条件の構文でドロップダウン リストから値を選択できる場合、通常はリストから複数の値を選択できます。たとえば、ホストで何らかの UNIX フレーバを実行している必要があることを示すホスト プロファイル限定をトラフィック プロファイルに追加するには、多数の条件を OR 演算子で結合する代わりに、以下の手順を使用できます。

複数の値を 1 つの条件に含めるには:

アクセス: Admin/Discovery Admin

ステップ 1　演算子として [is in] または [is not in] を選択して 1 つの条件を作成します。

ドロップダウン リストがテキスト フィールドに変わります。

ステップ 2　テキスト フィールド内の任意の場所または [Edit] リンクをクリックします。

ポップアップ ウィンドウが表示されます。

ステップ 3　[Available] の下で、Ctrl キーまたは Shift キーを押しながら複数の値をクリックして選択します。また、クリックしてドラッグすることで、隣接する複数の値を選択できます。

ステップ 4　右矢印（>）をクリックして、選択した項目を [Selected] に移動します。

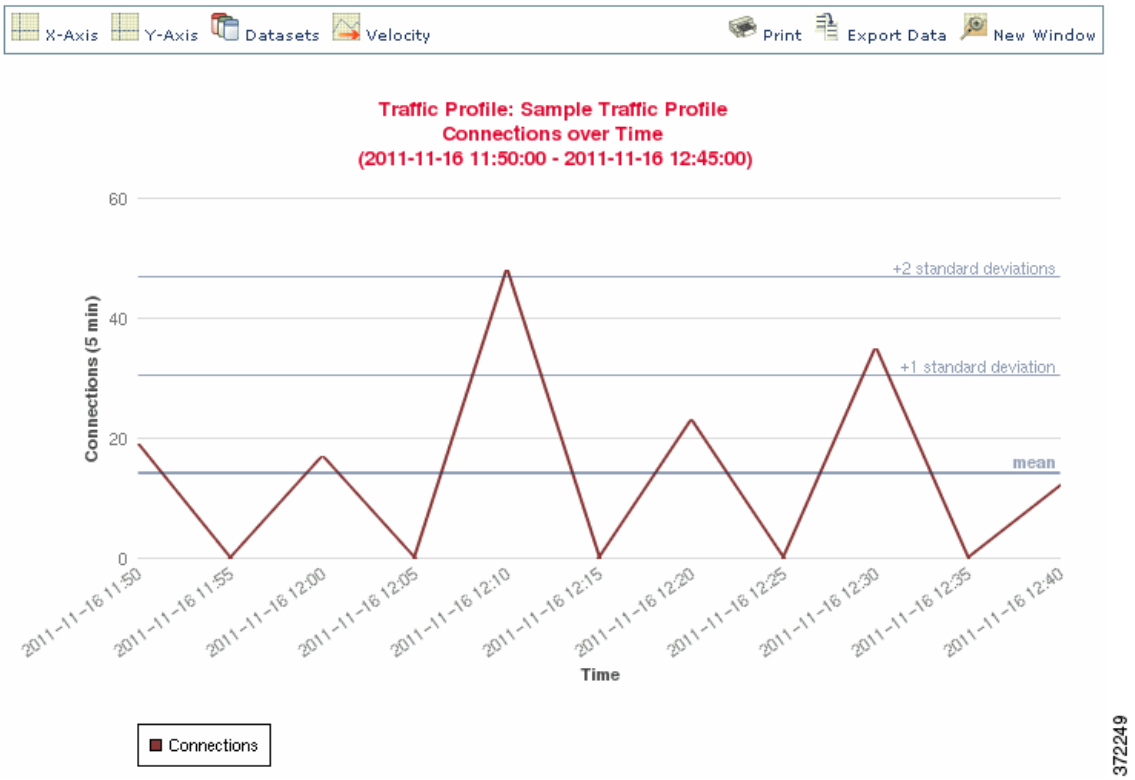
ステップ 5　[OK] をクリックします。

選択した内容が [Create Profile] ページの条件の値フィールドに表示されます。

トラフィック プロファイルの表示

ライセンス：FireSIGHT

トラフィック プロファイルは接続データに基づいているため、トラフィック プロファイルのグラフを表示できます。次の図は、PTW 1 週間、サンプリング レート 5 分、非アクティブ期間として毎日深夜 12:00 から 12:30 までの 30 分間が設定されているトラフィック プロファイルを示します。



接続データ グラフで実行できるほとんどすべてのアクションを、トラフィック プロファイル グラフでも実行できます。ただし、トラフィック プロファイルは集約データ（接続の要約）に基づいているため、グラフの基礎となる個々の接続イベントを調べることはできません。つまり、トラフィック プロファイル グラフから接続データ テーブル ビューにドリル ダウンすることはできません。詳細については、「接続およびセキュリティ インテリジェンスのデータの表示（39-15

ページ）」を参照してください。また、トラフィック プロファイルは分離グラフとして表示されます。詳細については、接続グラフの分離（39-28 ページ）を参照してください。

さらに、トラフィック プロファイルの時系列グラフでは、Y 軸の中間（平均）値が太い横棒で示されます。また、時系列グラフでは、ネットワーク トラフィックが正規分布することを前提に、最初の 4 つの標準偏差値が平均の上下に示されます。デフォルトではこれらの統計情報が PTW 期間にわたって計算されますが、グラフの時間設定を変更すると、Defense Centerにより統計情報が再計算されます。ただし、トラフィック プロファイル統計情報に関して作成されたルールは、常に PTW 期間の統計情報に照らして評価されます。

トラフィック プロファイルに関するグラフを表示する方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Policies] > [CorrelationSelect] を選択してから、[Traffic Profiles] をクリックします。

[Traffic Profiles] ページが表示されます。

ステップ 2　グラフを表示する対象のトラフィック プロファイルの隣にあるグラフ アイコン（  ）をクリックします。

トラフィック プロファイルのグラフが、別のブラウザ ウィンドウで表示されます。

修復の設定

相関ポリシー違反の発生時に、FireSIGHT システムを設定して、1 つまたは複数の応答を開始できます。この中には、修復（Nmap スキャンの実行など）とさまざまなタイプのアラートが含まれます。

起動可能な最も基本的なタイプの応答はアラートです。アラートは電子メール、SNMP トラップ サーバ、または syslog によってポリシー違反をユーザに通知します。アラートの作成については、外部アラートの設定（43-1 ページ）を参照してください。

起動可能なもう 1 つの応答は修復です。修復はネットワーク トラフィックが相関ポリシーに違反したときにDefense Centerが実行するプログラムです。FireSIGHT システムには出荷時に定義済みの修復が含まれています。この修復は、ポリシーの違反時にファイアウォールまたはルータでホストをブロックしたりホストをスキャンしたりするアクションを実行します。

Defense Centerが修復を起動すると、修復ステータス イベントが生成されます。他のイベントと同様に修復ステータス イベントを検索、表示、および削除できます。

FireSIGHT システムはまた、相関ポリシー違反に応答するためのカスタム修復モジュールを作成できる柔軟な API を提供します。たとえば、Linux ベースのファイアウォールを実行している場合、相関ポリシーに違反するトラフィックをブロックするように、Linux サーバ上の `iptables` ファイルを動的に更新する修復モジュールを作成し、アップロードすることができます。独自の修復モジュールの作成に関する詳細については、『Cisco *Remediation API Guide*』を参照してください。

注 修復を設定および使用するには、Defense Centerを使用する必要があります。

詳細については、以下を参照してください。

- 修復の作成（54-1 ページ）
- 修復ステータス イベントの使用（54-18 ページ）

修復の作成

ライセンス： FireSIGHT

相関ポリシー違反を簡単に通知できるアラートに加えて、*修復*という応答を設定することもできます。修復は、相関ポリシー違反が発生したときにDefense Centerが実行するプログラムです。これらのプログラムは、違反の原因となったイベントで提供される情報を使用して、特定のアクションを実行します。

FireSIGHT システムには出荷時に次のような複数の定義済み修復モジュールが含まれています。

- Cisco IOS ヌル ルート モジュール。Cisco IOS® バージョン 12.0 以降を使用する Cisco ルータが実行中の場合、相関ポリシーに違反する IP アドレスまたはネットワークに送信されるトラフィックを動的にブロックできます。

  詳細については、「Cisco IOS ルータ用修復の設定（54-3 ページ）」を参照してください。

- Cisco PIX Shun モジュール。Cisco PIX® ファイアウォール バージョン 6.0 以降を実行中の場合、相関ポリシーに違反する IP アドレスから送信されたトラフィックを動的にブロックできます。

  詳細については、「Cisco PIX ファイアウォール用修復の設定（54-8 ページ）」を参照してください。

- Nmap スキャン モジュール。特定のターゲットを能動的にスキャンし、そうしたホスト上で稼動中のオペレーティング システムおよびサーバを判別できます。

  詳細については、「Nmap 修復の設定（54-12 ページ）」を参照してください。

- セット属性値モジュール。相関イベントが発生するホストのホスト属性を設定できます。

  セット属性修復の構成（54-16 ページ）を参照してください。

各修復モジュールについて複数のインスタンスを作成できます。各インスタンスは特定のアプライアンスへの接続を表します。たとえば、修復を送信する Cisco IOS ルータが 4 台ある場合、Cisco IOS 修復モジュールのインスタンスを 4 つ設定する必要があります。

インスタンスを作成する際、Defense Centerがアプライアンスとの接続を確立するために必要な設定情報を指定します。次に、設定済みの各インスタンスで、ポリシーに違反した場合にアプライアンスが実行するアクションを説明する修復を追加します。

修復を設定した後で、応答グループと呼ばれるものに追加するか、または相関ポリシー内のルールに個別に割り当てることができます。システムがこれらの修復を実行すると、修復ステータス イベントが生成されます。この中には、修復の名前、その原因となったポリシーとルール、および終了ステータス メッセージといった詳細が含まれます。これらのイベントの詳細については、修復ステータス イベントの使用（54-18 ページ）を参照してください。

Ciscoが提供するデフォルトのモジュールに加えて、ポリシー違反がトリガーとして使用したときに他の特定のタスクを実行する、カスタム修復モジュールを作成できます。独自の修復モジュールを作成し、Defense Centerにインストールする方法の詳細については、『*Remediation API Guide*』を参照してください。カスタム モジュールをインストールする場合、[Modules] ページを使用して、新しいモジュールのインストール、表示、および削除を行うことができます。

新しいモジュールをDefense Centerにインストールする方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Modules] を選択します。

[Modules] ページが表示されます。

ステップ 2　[Browse] をクリックして、カスタム修復モジュールを含むファイルを保存した場所に移動します（詳細については『*Remediation API Guide*』を参照）。

ステップ 3　[Install] をクリックします。

カスタム修復モジュールがインストールされます。

モジュールをDefense Centerで表示または削除する方法:

アクセス: Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Modules] を選択します。

[Modules] ページが表示されます。

ステップ 2　次のいずれかの操作を実行します。

- [View] をクリックして、モジュールを表示します。

  [Module Detail] ページが表示されます。
- 削除するファイルの横の [Delete] をクリックします。Ciscoで提供されるデフォルトのモジュールは削除**できません**。

  修復モジュールが削除されます。

Cisco IOS ルータ用修復の設定

ライセンス: FireSIGHT

Ciscoでは、相関ポリシーに違反した場合に、シスコの「null route」コマンドを使用して単一の IP アドレスまたはアドレスのブロック全体をブロックできる、Cisco IOS ヌル ルート修復モジュールを提供します。このモジュールは、相関ポリシーに違反したイベントに送信元または宛先ホストとして示された、ホストまたはネットワークに送信されるすべてのトラフィックをルータのヌル インターフェイスに転送し、ドロップします(違反ホストまたはネットワーク**から**送信されたトラフィックはブロックされないことに注意してください)。

Cisco IOS ヌル ルート修復モジュールは Cisco IOS 12.0 以上を実行している Cisco ルータをサポートします。Cisco IOS 修復を実行するには、ルータに対してレベル 15 の管理アクセスを持っている必要があります。

注　宛先ベースの修復が機能するのは、接続イベントまたは侵入イベントに基づく相関ルールによってトリガーされたときに起動するように設定されている場合だけです。ディスカバリ イベントは送信元ホストのみを送信します。

注意　Cisco IOS 修復がアクティブになる際、タイムアウト期間はありません。ブロックされた IP アドレスまたはネットワークをルータから削除するには、ルータ自体から手動でルーティング変更をクリアする必要があります。

Cisco IOS を実行しているルータの修復を作成する方法:

アクセス: Admin/Discovery Admin

ステップ 1　Cisco ルータで Telnet を有効にします。

Telnet を有効にする方法の詳細については Cisco ルータまたは Cisco IOS ソフトウェアのマニュアルを参照してください。

ステップ 2　Defense Centerで、Defense Centerと共に使用する予定の各 Cisco IOS ルータに対する Cisco IOS ヌル ルート インスタンスを追加します。

手順については、Cisco IOS インスタンスの追加（54-4 ページ）を参照してください。

ステップ 3　相関ポリシーに違反した場合にルータで実現する応答のタイプに基づき、インスタンスごとに特定の修復を作成します。

使用可能な修復の各タイプについて、次の項で説明しています。

- Cisco IOS ブロック宛先修復（54-5 ページ）
- Cisco IOS ブロック宛先ネットワーク修復（54-6 ページ）
- Cisco IOS ブロック送信元修復（54-7 ページ）
- Cisco IOS ブロック送信元ネットワーク修復（54-7 ページ）

ステップ 4　特定の相関ポリシー ルールに対する Cisco IOS 修復の割り当てを開始します。

Cisco IOS インスタンスの追加

ライセンス：FireSIGHT

Cisco IOS ルータで Telnet アクセスを設定した後で（Telnet アクセスを有効にする方法の詳細については Cisco ルータまたは Cisco IOS ソフトウェアのマニュアルを参照）、Defense Centerにインスタンスを追加できます。修復を送信するルータが複数ある場合は、各ルータに対して別々のインスタンスを作成する必要があります。

Cisco IOS インスタンスを追加する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

ステップ 2　[Add a New Instance] リストから[Cisco IOS Null Route (v1.0)] を選択し、[Add] をクリックします。

[Edit Instance] ページが表示されます。

ステップ 3　[Instance Name] フィールドに、インスタンスの名前を入力します。

選択する名前には、スペースや特殊文字を含めず、説明的である必要があります。たとえば、複数の Cisco IOS ルータを接続する場合、複数のインスタンスがあるため、`IOS_01` および `IOS_02` などの名前を選択することをお勧めします。

ステップ 4　[Router IP] フィールドに、修復のために使用する Cisco IOS ルータの IP アドレスを入力します。

ステップ 5　[Username] フィールドに、ルータの Telnet ユーザ名を入力します。このユーザは、ルータでレベル 15 管理アクセスを持っている必要があります。

ステップ 6　[Connection Password] フィールドに、Telnet ユーザのパスワードを入力します。両方のフィールドに入力したパスワードが一致している必要があります。

ステップ 7　[Enable Password] フィールドに、Telnet ユーザのイネーブル パスワードを入力します。これは、ルータの特権モードに入るために使用するパスワードです。両方のフィールドに入力したパスワードが一致している必要があります。

ステップ 8　[White List] フィールドに、修復から除外する IP アドレスを 1 行につき 1 つ入力します。CIDR 表記または特定の IP アドレスを使用できます。たとえば、次のホワイトリストはシステムによって受け入れられます。

```
10.1.1.152
172.16.1.0/24
```

このホワイトリストは作成したコンプライアンスのホワイトリストに関連付けられていないことに注意してください。FireSIGHT システムでの CIDR 表記の使用法の詳細については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ステップ 9　[Create] をクリックします。

インスタンスが作成され、ページの [Configured Remediations] セクションに修復が表示されます。相関ポリシーで使用するために特定の修復を追加する必要があります。詳細については、次の項を参照してください。

- Cisco IOS ブロック宛先修復（54-5 ページ）
- Cisco IOS ブロック宛先ネットワーク修復（54-6 ページ）
- Cisco IOS ブロック送信元修復（54-7 ページ）
- Cisco IOS ブロック送信元ネットワーク修復（54-7 ページ）

Cisco IOS ブロック宛先修復

ライセンス：FireSIGHT

Cisco IOS ブロック宛先修復により、ルータから相関イベントの宛先ホストに送信されるトラフィックをブロックできます。

注　ディスカバリ イベントに基づいた相関ルールに対する応答としてこの修復を使用**しない**でください。ディスカバリ イベントは送信元ホストのみを送信し、宛先ホストを送信しません。接続イベントまたは侵入イベントに基づいた相関ルールに応じてこの修復を使用できます。

修復を追加する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

ステップ 2　修復を追加するインスタンスの横にある表示アイコン（🔍）をクリックします。

インスタンスを追加したことがない場合は、Cisco IOS インスタンスの追加（54-4 ページ）を参照してください。

[Edit Instance] ページが表示されます。

ステップ 3　[Configured Remediations] セクションで、[Block Destination] を選択し、[Add] をクリックします。

[Edit Remediation] ページが表示されます。

ステップ 4　[Remediation Name] フィールドに修復の名前を入力します。

選択する名前には、スペースや特殊文字を含めず、説明的である必要があります。たとえば、Cisco IOS ルータが複数台あり、各インスタンスに複数の修復がある場合、`IOS_01_BlockDest` などの名前を指定することお勧めします。

ステップ 5　必要に応じて、[Description] フィールドに、修復の説明を入力します。

ステップ 6　[Create] をクリックし、次に [Done] をクリックします。

修復が追加されます。

Cisco IOS ブロック宛先ネットワーク修復

ライセンス：FireSIGHT

Cisco IOS ブロック宛先ネットワーク修復により、ルータから相関イベントの宛先ホストのネットワークに送信されるすべてのトラフィックをブロックできます。

注　ディスカバリ イベントに基づいた相関ルールに対する応答としてこの修復を使用**しない**でください。ディスカバリ イベントは送信元ホストのみを送信し、宛先ホストを送信しません。接続イベントまたは侵入イベントに基づいた相関ルールに応じてこの修復を使用できます。

修復を追加する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

ステップ 2　修復を追加するインスタンスの横で、[View] をクリックします。

インスタンスを追加したことがない場合は、Cisco IOS インスタンスの追加（54-4 ページ）を参照してください。

[Edit Instance] ページが表示されます。

ステップ 3　[Configured Remediations] セクションで、[Block Destination Network] を選択し、[Add] をクリックします。

[Edit Remediation] ページが表示されます。

ステップ 4　[Remediation Name] フィールドに修復の名前を入力します。

選択する名前には、スペースや特殊文字を含めず、説明的である必要があります。たとえば、Cisco IOS ルータが複数台あり、各インスタンスに複数の修復がある場合、`IOS_01_BlockDestNet` などの名前を指定することお勧めします。

ステップ 5　必要に応じて、[Description] フィールドに、修復の説明を入力します。

ステップ 6　[Netmask] フィールドに、サブネット マスクを入力するか、または CIDR 表記を使用して、トラフィックをブロックするネットワークを記述します。

たとえば、1 つのホストがルールをトリガーとして使用したときにクラス C ネットワーク全体へのトラフィックをブロックするには、ネットマスクとして `255.255.255.0` または `24` を使用します。

別の例として、トリガーの IP アドレスを含む 30 個のアドレスへのトラフィックをブロックするには、ネットマスクとして `255.255.255.224` または `27` を指定します。この場合、IP アドレス `10.1.1.15` が修復をトリガーとして使用し、`10.1.1.1` と `10.1.1.30` の間のすべての IP アドレスがブロックされます。トリガーの IP アドレスのみをブロックするには、このフィールドは空のままにして、`32` を入力するか、または `255.255.255.255` を入力します。

ステップ 7　[Create] をクリックし、次に [Done] をクリックします。

修復が追加されます。

Cisco IOS ブロック送信元修復

ライセンス：FireSIGHT

Cisco IOS ブロック送信元修復により、ルータから、相関ポリシーに違反する相関イベントに含まれている送信元ホストに送信される、すべてのトラフィックをブロックできます。送信元ホストは、相関ルールに基づいた接続イベントまたは侵入イベントの送信元 IP アドレス、またはディスカバリ イベントのホスト IP アドレスです。

修復を追加する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

ステップ 2　修復を追加するインスタンスの横で、[View] をクリックします。

インスタンスを追加したことがない場合は、Cisco IOS インスタンスの追加（54-4 ページ）を参照してください。

[Edit Instance] ページが表示されます。

ステップ 3　[Configured Remediations] セクションで、[Block Source] を選択し、[Add] をクリックします。

[Edit Remediation] ページが表示されます。

ステップ 4　[Remediation Name] フィールドに修復の名前を入力します。

選択する名前には、スペースや特殊文字を含めず、説明的である必要があります。たとえば、Cisco IOS ルータが複数台あり、各インスタンスに複数の修復がある場合、`IOS_01_BlockSrc` などの名前を指定することお勧めします。

ステップ 5　必要に応じて、[Description] フィールドに、修復の説明を入力します。

ステップ 6　[Create] をクリックし、次に [Done] をクリックします。

修復が追加されます。

Cisco IOS ブロック送信元ネットワーク修復

ライセンス：FireSIGHT

Cisco IOS ブロック送信元ネットワーク修復により、ルータから相関イベントの送信元ホストのネットワークに送信されるすべてのトラフィックをブロックできます。送信元ホストは、相関ルールに基づいた接続イベントまたは侵入イベントの送信元 IP アドレス、またはディスカバリ イベントのホスト IP アドレスです。

修復を追加する方法:

アクセス: Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

ステップ 2　修復を追加するインスタンスの横で、[View] をクリックします。

インスタンスを追加したことがない場合は、Cisco IOS インスタンスの追加（54-4 ページ）を参照してください。

[Edit Instance] ページが表示されます。

ステップ 3　[Configured Remediations] セクションで、[Block Source Network] を選択し、[Add] をクリックします。

[Edit Remediation] ページが表示されます。

ステップ 4　[Remediation Name] フィールドに修復の名前を入力します。

選択する名前には、スペースや特殊文字を含めず、説明的である必要があります。たとえば、Cisco IOS ルータが複数台あり、各インスタンスに複数の修復がある場合、`IOS_01_BlockSourceNet` などの名前を指定することお勧めします。

ステップ 5　必要に応じて、[Description] フィールドに、修復の説明を入力します。

ステップ 6　[Netmask] フィールドに、トラフィックをブロックするネットワークの説明となるサブネット マスクまたは CIDR 表記を入力します。

たとえば、1 つのホストがルールをトリガーとして使用したときにクラス C ネットワーク全体へのトラフィックをブロックするには、ネットマスクとして `255.255.255.0` または `24` を使用します。

別の例として、トリガーの IP アドレスを含む 30 個のアドレスへのトラフィックをブロックするには、ネットマスクとして `255.255.255.224` または `27` を指定します。この場合、IP アドレス `10.1.1.15` が修復をトリガーとして使用し、`10.1.1.1` と `10.1.1.30` の間のすべての IP アドレスがブロックされます。トリガーの IP アドレスのみをブロックするには、このフィールドは空のままにして、`32` を入力するか、または `255.255.255.255` を入力します。

ステップ 7　[Create] をクリックし、次に [Done] をクリックします。

修復が追加されます。

Cisco PIX ファイアウォール用修復の設定

ライセンス: FireSIGHT

Ciscoは、シスコの「shun」コマンドを使用して IP アドレスまたはネットワークをブロックできる、Cisco PIX Shun 修復モジュールを提供します。これは、相関ポリシーに違反した送信元ホストまたは宛先ホストのいずれかから送信されるすべてのトラフィックをブロックし、現行の接続をすべて閉じます（ファイアウォールを介してホストに送信されるトラフィックはブロックされないことに注意してください）。

Cisco PIX Shun 修復モジュールは Cisco PIX ファイアウォール 6.0 以上をサポートします。Cisco PIX 修復を起動するにはレベル 15 以上の管理アクセスが必要です。

注　宛先ベースの修復が機能するのは、接続イベントまたは侵入イベントに基づく相関ルールによってトリガーされたときに起動するように設定されている場合だけです。ディスカバリ イベントは送信元ホストのみを送信します。

注意　Cisco PIX 修復がアクティブになる際、タイムアウト期間は使用されません。IP アドレスまたはネットワークのブロックを解除するには、手動でファイアウォールのルールを削除する必要があります。

Cisco PIX ファイアウォール用の修復を作成する方法：

アクセス：Admin/Discovery Admin

ステップ 1　ファイアウォール上で Telnet または SSH を有効にします（Ciscoは SSH を推奨します）。

SSH または Telnet を有効にする方法の詳細については Cisco PIX ファイアウォールのマニュアルを参照してください。

ステップ 2　Defense Centerで、Defense Centerと共に使用する予定の各 Cisco PIX ファイアウォールに対する Cisco PIX Shun インスタンスを追加します。

手順については、Cisco PIX インスタンスの追加（54-9 ページ）を参照してください。

ステップ 3　相関ポリシーに違反した場合にファイアウォールで実現する応答のタイプに基づき、インスタンスごとに特定の修復を作成します。

使用可能な修復タイプは次の項で説明されています。

- Cisco PIX ブロック宛先修復（54-10 ページ）
- Cisco PIX ブロック送信元修復（54-11 ページ）

ステップ 4　特定の相関ポリシー ルールに対する Cisco PIX 修復の割り当てを開始します。

Cisco PIX インスタンスの追加

ライセンス：FireSIGHT

Cisco PIX ファイアウォールで SSH または Telnet を設定した後で、Defense Centerにインスタンスを追加できます。修復を送信するファイアウォールが複数ある場合は、各ファイアウォールに対して別々のインスタンスを作成する必要があります。

注　Ciscoは、Telnet 接続の代わりに SSH 接続を使用することを推奨します。SSH を使用して送信されるデータは暗号化されるので、Telnet よりもはるかに安全です。

Cisco PIX インスタンスを追加する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

ステップ 2　[Add a New Instance] リストから、[Cisco PIX Shun] を選択し、[Add] をクリックします。

[Edit Instance] ページが表示されます。

ステップ 3　[Instance Name] フィールドに、インスタンスの名前を入力します。

選択する名前には、スペースや特殊文字を含めず、説明的である必要があります。たとえば、複数の Cisco ファイアウォールを接続する場合、複数のインスタンスがあるため、`PIX_01`、`PIX_02` などの名前を選択することをお勧めします。

ステップ 4　オプションで、[Description] フィールドに、インスタンスの説明を入力します。

ステップ 5　[PIX IP] フィールドに、修復のために使用する Cisco PIX ファイアウォールの IP アドレスを入力します。

ステップ 6　デフォルト（`pix`）以外の特定のユーザ名が必要な場合は、[Username] フィールドに入力します。

ステップ 7　[Connection Password] フィールドに、SSH または Telnet を使用してファイアウォールに接続するためのパスワードを入力します。両方のフィールドに入力したパスワードが一致している必要があります。

ステップ 8　[Enable Password] フィールドに、SSH または Telnet のイネーブル パスワードを入力します。これは、ファイアウォールの特権モードに入るために使用するパスワードです。両方のフィールドに入力したパスワードが一致している必要があります。

ステップ 9　[White List] フィールドに、修復から除外する IP アドレスを 1 行につき 1 つ入力します。CIDR 表記または特定の IP アドレスを使用できます。たとえば、次のホワイトリストはシステムによって受け入れられます。

```
10.1.1.152
172.16.1.0/24
```

このホワイトリストは作成したコンプライアンスのホワイトリストに関連付けられていないことに注意してください。FireSIGHT システムでの CIDR 表記の使用法の詳細については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ステップ 10　[Protocol] リストから、ファイアウォールに接続するために使用する方式を選択します。

ステップ 11　[Create] をクリックします。

インスタンスが作成され、ページの [Configured Remediations] セクションに修復が表示されます。相関ポリシーで使用するために特定の修復を追加する必要があります。詳細については、次の項を参照してください。

- Cisco PIX ブロック宛先修復（54-10 ページ）
- Cisco PIX ブロック送信元修復（54-11 ページ）

Cisco PIX ブロック宛先修復

ライセンス： FireSIGHT

Cisco PIX ブロック宛先修復により、相関イベントの宛先ホストから送信されるトラフィックをブロックできます。

注　ディスカバリ イベントに基づいた相関ルールに対する応答としてこの修復を使用**しない**でください。ディスカバリ イベントは送信元ホストのみを送信し、宛先ホストを送信しません。接続イベントまたは侵入イベントに基づいた相関ルールに応じてこの修復を使用できます。

修復を追加する方法:

アクセス: Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

ステップ 2　修復を追加するインスタンスの横で、[View] をクリックします。

インスタンスを追加したことがない場合は、Cisco PIX インスタンスの追加（54-9 ページ）を参照してください。

[Edit Instance] ページが表示されます。

ステップ 3　[Configured Remediations] セクションで、[Block Destination] を選択し、[Add] をクリックします。

[Edit Remediation] ページが表示されます。

ステップ 4　[Remediation Name] フィールドに修復の名前を入力します。

選択する名前には、スペースや特殊文字を含めず、説明的である必要があります。たとえば、Cisco PIX ファイアウォールが複数台あり、各インスタンスに複数の修復がある場合、`PIX_01_BlockDest` などの名前を指定することお勧めします。

ステップ 5　必要に応じて、[Description] フィールドに、修復の説明を入力します。

ステップ 6　[Create] をクリックし、次に [Done] をクリックします。

修復が追加されます。

Cisco PIX ブロック送信元修復

ライセンス: FireSIGHT

Cisco PIX ブロック送信元修復により、相関ポリシーに違反するイベントに含まれる送信元ホストから送信されるすべてのトラフィックをブロックできます。送信元ホストは、相関ルールに基づいた接続イベントまたは侵入イベントの送信元 IP アドレス、またはディスカバリ イベントのホスト IP アドレスです。

修復を追加する方法:

アクセス: Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

ステップ 2　修復を追加するインスタンスの横で、[View] をクリックします。

インスタンスを追加したことがない場合は、Cisco PIX インスタンスの追加（54-9 ページ）を参照してください。

[Edit Instance] ページが表示されます。

ステップ 3　[Configured Remediations] セクションで、[Block Source] を選択し、[Add] をクリックします。

[Edit Remediation] ページが表示されます。

ステップ 4　[Remediation Name] フィールドに修復の名前を入力します。

選択する名前には、スペースや特殊文字を含めず、説明的である必要があります。たとえば、Cisco PIX ファイアウォールが複数台あり、各インスタンスに複数の修復がある場合、`PIX_01_BlockSrc` などの名前を指定することお勧めします。

ステップ 5　必要に応じて、[Description] フィールドに、修復の説明を入力します。

修復が追加されます。

Nmap 修復の設定

ライセンス： FireSIGHT

トリガー イベントが発生したホストをスキャンすることにより、相関イベントに応答できます。相関イベントをトリガーとして使用したイベントからポートのみをスキャンすることができます。

相関イベントに応じて Nmap スキャンをセットアップするには、最初に Nmap スキャン インスタンスを作成してから Nmap スキャン修復を追加する必要があります。その後、ポリシー内のルールの違反に対する応答として Nmap スキャンを設定できます。

次の項を参照してください。

- Nmap スキャン インスタンスの追加（54-12 ページ）
- Nmap スキャン修復（54-13 ページ）

Nmap スキャン インスタンスの追加

ライセンス： FireSIGHT

ネットワーク上のホストのオペレーティング システムおよびサーバの情報をスキャンするために使用する、Nmap の各モジュールに対して個別のスキャン インスタンスをセットアップできます。スキャン インスタンスのセットアップは、Defense Centerのローカルの Nmap モジュールおよびスキャンをリモートから実行するために使用する任意の管理対象デバイスに対して行うことができます。各スキャンの結果は、リモートの管理対象デバイスからスキャンを実行した場合であっても、スキャンを設定するDefense Centerに常に保存されます。ミッション クリティカルなホストへの不慮のスキャンや悪意のあるスキャンを防ぐには、インスタンスのブラックリストを作成し、そのインスタンスで決してスキャンしてはならないホストを指示できます。

既存のスキャン インスタンスと同じ名前のスキャン インスタンスを追加できないことに注意してください。

スキャン インスタンスを作成する方法：

アクセス： Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

ステップ 2　[Add a module type] ドロップダウン リストから、[Nmap Remediation (v1.0)] を選択し、[Add] をクリックします。

[Edit Instance] ページが表示されます。

ステップ 3　[Instance Name] フィールドに、1 文字から 63 文字の英数字の名前を入力します。アンダースコア（_）とハイフン（-）以外の特殊文字およびスペースは使用できません。

ステップ 4　[Description] フィールドに、スペースと特殊文字を含む、0 ～ 255 文字の英数字を使用して説明を指定します。

ステップ 5　オプションで、[Black Listed Scan hosts] フィールドで、このスキャン インスタンスがスキャンしないホストまたはネットワークを指定します。次の構文を使用します。

- IPv6 ホストの場合は厳密な IP アドレス（たとえば、`2001:DB8::fedd:eeff`）
- IPv4 ホストの場合は厳密な IP アドレス（たとえば、`192.168.1.101`）または CIDR 表記を使用した IP アドレス ブロック（たとえば、`192.168.1.0/24` は `192.168.1.1` から `192.168.1.254` までの 254 ホスト（両端を含む）をスキャンします）

ブラックリスト化されたネットワーク上にあるホストを特にスキャン対象とした場合、スキャンは実行されません。FireSIGHT システムでの CIDR 表記の使用法の詳細については、IP アドレスの表記規則（1-23 ページ）を参照してください。

ステップ 6　オプションで、Defense Centerの代わりに、リモートの管理対象デバイスからスキャンするには、[Remote Device Name] フィールドで管理対象デバイスの名前または IP アドレスを指定します。

ステップ 7　[Create] をクリックします。

スキャン インスタンスが作成されます。

Nmap スキャン修復

ライセンス：FireSIGHT

Nmap 修復を作成することにより、Nmap スキャンの設定を定義できます。Nmap 修復は、相関ポリシーの応答として、オンデマンドで実行するために使用することも、指定時刻に実行するようにスケジュール設定することもできます。Nmap スキャンの結果をネットワーク マップに表示するには、スキャンされるホストがネットワーク マップに存在している必要があります。ホスト入力機能である NetFlow とシステム自体がホストをネットワーク マップに追加できることに注意してください。

Nmap 修復の具体的な設定の詳細については、Nmap 修復の概要（47-2 ページ）を参照してください。

Nmap により提供されるサーバやオペレーティング システムのデータは、もう一度 Nmap スキャンを実行するまで静的な状態のままであることに注意してください。Nmap を使用してホスト内でオペレーティング システムやサーバのデータをスキャンすることを計画している場合は、定期的なスキャンのスケジュールをセットアップして、Nmap によって提供されるオペレーティング システムやサーバのデータを最新に保つこともできます。詳細については、Nmap スキャンの自動化（62-5 ページ）を参照してください。また、ホストがネットワーク マップから削除されると、そのホストのすべての Nmap スキャン結果が廃棄されることにも注意してください。

Nmap の機能に関する一般情報については、http://insecure.org にある Nmap のマニュアルを参照してください。

Nmap 修復を作成する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scanners] ページが表示されます。

ステップ 2　修復を追加するスキャン インスタンスの横の [Add Remediation] をクリックします。

[Edit Remediation] ページが表示されます。

ステップ 3　[Remediation Name] フィールドに、1 ～ 63 文字の英数字を使用して修復の名前を入力します。スペースと下線(_)およびハイフン(-)以外の特殊文字を使用することはできません。

ステップ 4　[Description] フィールドに、スペースと特殊文字を含む、0 ～ 255 文字の英数字を使用して修復の説明を入力します。

ステップ 5　侵入イベント、接続イベント、またはユーザ イベントでトリガーとして使用する相関ルールに応じてこの修復を使用する場合は、[Scan Which Address(es) From Event?] オプションを設定します。

- [Scan Source and Destination Addresses] を選択して、イベントの送信元 IP アドレスと宛先 IP アドレスによって表されるホストをスキャンします。
- [Scan Source Address Only] を選択して、イベントの送信元 IP アドレスで表されるホストをスキャンします。
- [Scan Destination Address Only] を選択して、イベントの宛先 IP アドレスで表されるホストをスキャンします。

ディスカバリ イベントまたはホスト入力イベントでトリガーとして使用する相関ルールに応じてこの修復を使用する場合、デフォルトで、修復はイベントに含まれるホストの IP アドレスをスキャンします。このオプションを設定する必要はありません。

注　トラフィック プロファイルの変更でトリガーとして使用する相関ルールへの応答として Nmap 修復を割り当て**ない**でください。

ステップ 6　次のように、[Scan type] オプションを設定します。

- TCP 接続を開始し、完了しないことにより、`admin` アカウントがロー パケット アクセスを持つホスト、または IPv6 が動作していないホストで、ステルス モードですばやくスキャンするには、[TCP Syn Scan] を選択します。
- Defense Centerの `admin` アカウントがロー パケット アクセスを持つホスト、または IPv6 が動作しているホストで使用可能な、システムの `connect()` コールを使用してスキャンするには、[TCP Connect Scan] を選択します。
- ポートがフィルタリングされているかどうかを確認するために ACK パケットを送信するには、[TCP ACK Scan] を選択します。
- ポートがフィルタリングされているかどうかを確認し、ポートが開いているか閉じているかも判別するために ACK パケットを送信するには、[TCP Window Scan] を選択します。
- FIN/ACK プローブを使用して BSD 派生システムを識別するには、[TCP Maimon Scan] を選択します。

ステップ 7　オプションで、TCP ポートに加えて UDP ポートをスキャンするには、[Scan for UDP ports] オプションで [On] を選択します。

ヒント　UDP ポート スキャンは TCP ポート スキャンよりも時間がかかります。スキャンの速度を上げるには、このオプションを無効のままにします。

ステップ 8　相関ポリシー違反への応答としてこの修復を使用する場合は、[Use Port From Event] オプションを設定します。

- [On] を選択して、ステップ 12 で指定したポートではなく、相関イベントのポートをスキャンします。

相関イベントのポートをスキャンする場合、修復はステップ 8 で指定する IP アドレスのポートをスキャンすることに注意してください。これらのポートは、修復のダイナミックなスキャン ターゲットにも追加されます。

- [Off] を選択して、ステップ 12 で指定するポートのみをスキャンします。

ステップ 9　相関ポリシー違反への応答としてこの修復を使用し、イベントが検出された検出エンジンを実行するアプライアンスを使用してスキャンする場合、[Scan from reporting detection engine] オプションを設定します。

- レポート検出エンジンを実行するアプライアンスからスキャンするには、[On] を選択します。
- 修復に設定されたアプライアンスからスキャンするには、[Off] を選択します。

ステップ 10　[Fast Port Scan] オプションを設定します。

- スキャンを実行する管理対象デバイスの `/var/sf/nmap/share/nmap/nmap-services` ディレクトリにある `nmap-services` ファイルに記述されたポートのみをスキャンし、他のポート設定を無視するには、[On] を選択します。
- すべての TCP ポートをスキャンするには、[Off] を選択します。

ステップ 11　[Port Ranges and Scan Order] フィールドに、デフォルトでスキャンするポートを入力します。Nmap 構文を使用し、ポートをスキャンする順序で入力します。

1 ～ 65535 の値を指定します。複数のポートを、カンマまたはスペースを使用して区切ります。ハイフンを使用してポートの範囲を示すこともできます。TCP ポートと UDP ポートの両方ともスキャンする場合は、スキャン対象の TCP ポートのリストの先頭に T を挿入し、UDP ポートのリストの先頭に U を挿入します。たとえば UDP トラフィックのポート 53 と 111 をスキャンしてから TCP トラフィックのポート 21 ～ 25 をスキャンするのであれば `U:53,111,T:21-25` と入力します。

ステップ 8 で説明しているように、修復が相関ポリシー違反への応答として起動されると、[Use Port From Event] オプションがこの設定をオーバーライドすることに注意してください。

ステップ 12　サーバ ベンダーおよびバージョン情報に関して開いているポートをプローブするには、[Probe open ports for vendor and version information] を設定します。

- サーバ情報に関してホストの開いているポートをスキャンし、サーバ ベンダーおよびバージョンを識別するには、[On] を選択します。
- ホストのサーバ情報を使用して続行するには、[Off] を選択します。

ステップ 13　オープン ポートの調査を選択する場合は、[Service Version Intensity] ドロップダウン リストから数値を選択して、使用するプローブの数を設定します。

- 使用するプローブを多くして、長いスキャンで高い精度を得るには、大きな数値を選択します。
- 使用するプローブを少なくして、低い精度で高速なスキャンを行うには、小さな数値を選択します。

ステップ 14　オペレーティング システム情報をスキャンするには、[Detect Operating System] 設定を構成します。

- オペレーティング システムを識別する情報に関してホストをスキャンするには、[On] を選択します。
- ホストのオペレーティング システム情報を使用して続行するには、[Off] を選択します。

ステップ 15　ホスト ディスカバリが発生するかどうか、および使用可能なホストに対してのみポート スキャンが実行されるかどうかを判別するには、[Treat All Hosts As Online] を設定します。

- ホスト ディスカバリ プロセスを省略し、ターゲット範囲内のすべてのホストでポート スキャンを実行するには、[On] を選択します。

- [Host Discovery Method] および [Host Discovery Port List] の設定を使用してホスト ディスカバリを実行し、使用不可能なすべてのホストでポート スキャンを省略するには、[Off] を選択します。

ステップ 16　ホストが存在して使用可能かどうかを Nmap がテストする場合に使用する方式を選択します。

- SYN フラグが設定された空の TCP パケットを送信し、使用可能なホストで閉じているポートの RST 応答または開いているポートの SYN/ACK 応答を得るには、[TCP SYN] を選択します。

  このオプションは、デフォルトでポート 80 をスキャンし、TCP SYN スキャンはステートフル ファイアウォール ルールが設定されたファイアウォールによりブロックされる可能性が低いことに注意してください。

- ACK フラグが設定された空の TCP パケットを送信し、使用可能なホストで RST 応答を得るために、[TCP ACK] を選択します。

  このオプションは、デフォルトでポート 80 をスキャンし、TCP ACK スキャンはステートレス ファイアウォール ルールが設定されたファイアウォールによりブロックされる可能性が低いことに注意してください。

- UDP パケットを送信し、使用可能なホストで閉じているポートのポート到達不能応答を得るには、[UDP] を選択します。このオプションは、デフォルトでポート 40125 をスキャンします。

ステップ 17　ホスト ディスカバリ時にポートのカスタム リストをスキャンする場合は、[Host Discovery Port List] に、選択したホストのディスカバリ方法に適したポートのリストをカンマで区切って入力します。

ステップ 18　[Default NSE Scripts] オプションを設定して、ホスト ディスカバリおよび、サーバ、オペレーティング システム、脆弱性のディスカバリに Nmap スクリプトのデフォルト セットを使用するかどうかを制御します。

- Nmap スクリプトのデフォルト セットを実行するには、[On] を選択します。
- Nmap スクリプトのデフォルト セットを省略するには、[Off] を選択します。

デフォルト スクリプトのリストについては、http://nmap.org/nsedoc/categories/default.html を参照してください。

ステップ 19　スキャン プロセスのタイミングを設定するには、タイミング テンプレート番号を選択します。番号が大きいほど高速で包括度が低いスキャンになり、番号が小さいほど低速で包括度が高いスキャンになります。

ステップ 20　[Save] をクリックし、次に [Done] をクリックします。

修復が作成されます。

セット属性修復の構成

ライセンス： FireSIGHT

トリガー イベントが発生したホストでホスト属性値を設定することにより、相関イベントに応答できます。テキストのホスト属性の場合、イベントの説明を属性値として使用することを選択できます。ホスト属性の詳細については、事前定義のホスト属性の使用（49-34 ページ）および ユーザ定義のホスト属性の使用（49-35 ページ）を参照してください。

相関イベントへの応答として属性値を設定するには、まず属性設定インスタンスを作成してからセット属性の修復を追加します。その後、ポリシー内のルールの違反に対する応答として属性値更新を設定できます。

詳細については、次の項を参照してください。

- セット属性値インスタンスの追加（54-17 ページ）
- セット属性値修復（54-17 ページ）

セット属性値インスタンスの追加

ライセンス：FireSIGHT

相関ルール違反への応答として、属性値を設定するインスタンスを設定できます。

セット属性インスタンスを作成する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

ステップ 2　[Add a module type] ドロップダウン リストから、[Set Attribute Value (v1.0)] を選択し、[Add] をクリックします。

[Edit Instance] ページが表示されます。

ステップ 3　[Instance Name] フィールドに、1 文字から 63 文字の英数字の名前を入力します。アンダースコア（_）とハイフン（-）以外の特殊文字およびスペースは使用できません。

ステップ 4　[Description] フィールドに、スペースと特殊文字を含む、0 ～ 255 文字の英数字を使用して説明を指定します。

ステップ 5　[Create] をクリックします。

インスタンスが作成されます。

セット属性値修復

ライセンス：FireSIGHT

相関ルール違反への応答として設定する各属性値のセット属性値修復を作成できます。設定する属性がテキスト属性の場合、イベントの説明を属性値として使用する修復を設定できます。

セット属性値修復を作成する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

ステップ 2　修復を追加するスキャン インスタンスの横の [View] をクリックします。

[Edit Instance] ページが表示されます。

ステップ 3　[Add a new remediation of type] ドロップダウン リストから [Set Attribute Value] を選択します。

[Edit Remediation] ページが表示されます。

ステップ 4　[Remediation Name] フィールドに、1 ～ 63 文字の英数字を使用して修復の名前を入力します。スペースと下線（_）およびハイフン（-）以外の特殊文字を使用することはできません。

ステップ 5　[Description] フィールドに、スペースと特殊文字を含む、0 ～ 255 文字の英数字を使用して修復の説明を入力します。

ステップ 6　侵入イベント、ユーザ イベント、または接続イベントで発生する相関ルールへの応答としてこの修正を使用する場合は、[Update Which Host(s) From Event] オプションを設定します。

- [Update Source and Destination Hosts] を選択して、イベントの送信元 IP アドレスと宛先 IP アドレスによって表されるホストの属性値を更新します。
- [Update Source Host Only] を選択して、イベントの送信元 IP アドレスで表されるホストの属性値を更新します。
- [Update Destination Host Only] を選択して、イベントの宛先 IP アドレスで表されるホストの属性値を更新します。

ディスカバリ イベントまたはホスト入力イベントでトリガーとして使用する相関ルールへの応答としてこの修復を使用する場合、デフォルトで、修復はイベントに含まれるホストの IP アドレスをスキャンします。このオプションを設定する必要はありません。

ステップ 7　[Use Description From Event For Attribute Value (text attributes only)] オプションを設定します。

- イベントの説明を属性値として使用するには、[On] を選択します。
- 修復の [Attribute Value] 設定を属性値として使用するには、[Off] を選択します。

ステップ 8　イベントの説明を使用しない場合は、[Attribute Value] フィールドに、設定する属性値を入力します。

ステップ 9　[Save] をクリックし、次に [Done] をクリックします。

修復が作成されます。

修復ステータス イベントの使用

ライセンス： FireSIGHT

修復がトリガーとして使用すると、修復ステータス イベントが生成されます。これらのイベントはデータベースに記録され、[Remediation Status] ページで確認できます。修復ステータス イベントの検索、表示、および削除を行うことができます。

詳細については、以下を参照してください。

- イベント時間の制約の設定（58-26 ページ）
- 修復ステータス イベントの検索（54-22 ページ）

修復ステータス イベントの表示

ライセンス： FireSIGHT

修復ステータス イベントにアクセスするときに表示されるページは、使用するワークフローにより異なります。修復のテーブル ビューを含む定義済みワークフローを使用できます。テーブル ビューには、各修復ステータス イベントの行が含まれます。また、特定の要件に一致する情報のみを表示するカスタム ワークフローを作成することもできます。カスタム ワークフローの作成の詳細については、カスタム ワークフローの作成（58-43 ページ）を参照してください。

次の表では、修復ステータス イベント ワークフローのページで実行できる具体的なアクションの一部を説明します。

表 54-1　修復ステータス イベントの表示オプション

目的	操作
表示された列の詳細を表示する	修復ステータス テーブルについて（54-20 ページ）で詳細を参照してください。
表示されたイベントの時刻と日付の範囲を変更する	イベント時間の制約の設定（58-26 ページ）を参照してください。 イベント ビューを時間によって制約している場合は、（グローバルかイベントに特有かに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあることに注意してください。これは、アプライアンスのスライドの時間範囲を設定しても発生する可能性があります。
イベントをソートして制限する	イベントの制約（58-35 ページ）およびドリルダウン ワークフロー ページのソート（58-38 ページ）を参照してください。
一時的に他のワークフローを使用する	ワークフローのタイトルの横の [(switch workflow)] をクリックします。詳細については、ワークフローの選択（58-18 ページ）を参照してください。
相関イベントのビューへ移動して、関連するイベントを表示する	[Correlation Events] をクリックします。詳細については、ワークフロー間のナビゲート（58-40 ページ）を参照してください。
すぐに再表示できるように、現在のページをブックマークする	[Bookmark This Page] をクリックします。詳細については、ブックマークの使用（58-41 ページ）を参照してください。
ブックマークの管理ページへ移動する	[View Bookmarks] をクリックします。詳細については、ブックマークの使用（58-41 ページ）を参照してください。
テーブル ビューのデータに基づいてレポートを生成する	[Report Designer] をクリックします。詳細については、イベント ビューからのレポート テンプレートの作成（57-10 ページ）を参照してください。
特定の値に制限して、ワークフロー内の次のページにドリルダウンする	次のいずれかの方法を使用します。 • カスタム ワークフローで作成したドリルダウン ページで、行内の値をクリックします。テーブル ビューの行内の値をクリックすると、テーブル ビューが制限され、次のページに**ドリルダウンされない**ことに注意してください。 • 一部のユーザに制限して次のワークフロー ページにドリルダウンするには、次のワークフロー ページに表示するユーザの横にあるチェックボックスをオンにしてから、[View] をクリックします。 • 現在の制限を維持して次のワークフロー ページにドリルダウンするには、[View All] をクリックします。 **ヒント**　テーブル ビューでは、必ずページ名に「Table View」が含まれます。 詳細については、イベントの制約（58-35 ページ）を参照してください。
システムから修復ステータス イベントを削除する	次のいずれかの方法を使用します。 • 特定のイベントを削除するには、削除するイベントの横にあるチェック ボックスをオンにしてから、[Delete] をクリックします。 • 現在の制限ビュー内のすべてのイベントを削除するには、[Delete All] をクリックしてから、すべてのイベントを削除することを確認します。
修復ステータス イベントを検索する	[Search] をクリックします。詳細については、修復ステータス イベントの検索（54-22 ページ）を参照してください。

修復ステータス イベントを表示する方法:

アクセス: Admin

ステップ 1　[Analysis] > [Correlation] > [Status] を選択します。

デフォルトの修復ワークフローの最初のページが表示されます。カスタム・ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。イベントが表示されない場合、時間範囲を調整する必要がある場合があります。イベント時間の制約の設定（58-26 ページ）を参照してください。

ヒント　修復のテーブル ビューが含まれないカスタム ワークフローを使用する場合、ワークフローのタイトルの横の [(switch workflow)] メニューをクリックし、[Remediation Status] を選択します。

修復ステータス イベントの使用

ライセンス: FireSIGHT

イベント ビューのレイアウトを変更したり、ビュー内のイベントをフィールド値によって制限したりすることができます。

列を無効にすると、現在のセッションの間無効になります（その後再度追加しない場合）。最初の列を無効にすると、[Count] 列が追加されることに注意してください。

テーブル ビューの行内の値をクリックすると、テーブル ビューが制約されます（次のページにはドリルダウンされません）。

ヒント　テーブル ビューでは、必ずページ名に「Table View」が含まれます。

詳細については、次のトピックを参照してください。

- イベントの制約（58-35 ページ）。
- 複合的な制約の使用（58-37 ページ）。
- ドリルダウン ワークフロー ページのソート（58-38 ページ）。
- 修復ステータス テーブルについて（54-20 ページ）

修復ステータス テーブルについて

ライセンス: FireSIGHT

Defense Centerを設定して、ポリシー違反およびディスカバリ イベントへのさまざまな応答を起動できます。こうした応答には、ポリシー違反時のファイアウォールまたはルータにおけるホストのブロックなどの修復が含まれます。修復がトリガーとして使用すると、修復ステータス イベント生成され、データベースに記録されます。修復の詳細については、修復の設定（54-1 ページ）を参照してください。

修復ステータス テーブルのフィールドについて、次の表で説明します。

表 54-2　修復ステータス フィールド

フィールド	説明
ポリシー(Policy)	違反し、修復をトリガーとして使用した相関ポリシーの名前。
Remediation Name	起動された修復の名前。
Result Message	修復の起動時に発生した事象を説明するメッセージ。ステータス メッセージには以下が含まれます。 • Successful completion of remediation • Error in the input provided to the remediation module • Error in the remediation module configuration • Error logging into the remote device or server • Unable to gain required privileges on remote device or server • Timeout logging into remote device or server • Timeout executing remote commands or servers • The remote device or server was unreachable • The remediation was attempted but failed • Failed to execute remediation program • Unknown/unexpected error **注**　カスタム修復モジュールがインストールされている場合、カスタム モジュールによって実装される追加のステータス メッセージが表示される場合があります。
ルール	修復をトリガーとして使用したルールの名前。
時刻	Defense Centerが修復を起動した日付と時刻。
Count	各ローに表示される情報に一致するイベントの数。同一の行が複数作成される制約を適用した後にのみ、[Count] フィールドが表示されることに注意してください。

修復ステータス イベントのテーブル ビューを表示する方法:

アクセス: Admin

ステップ 1　[Analysis] > [Correlation] > [Status] を選択します。

テーブル ビューが表示されます。修復ステータス イベントを使用の詳細については、修復ステータス イベントの使用 (54-18 ページ)を参照してください。

ヒント　修復ステータス イベントのテーブル ビューが含まれないカスタム ワークフローを使用する場合、ワークフローのタイトルの横の [(switch workflow)] をクリックし、[Remediation Status] をクリックします。

修復ステータス イベントの検索

ライセンス：FireSIGHT

特定の修復が起動されたかどうか、およびいつ起動されたかを判別するために修復ステータス イベントを検索できます。使用するネットワーク環境に合わせてカスタマイズされた検索を作成し、保存して再利用することをお勧めします。次の表で、ユーザが使用できる検索条件について説明します。

表 54-3　修復ステータスの検索条件

検索フィールド	説明
Result Message	照合する結果メッセージ（修復が起動されたときに発生した事象を説明するメッセージ）の**正確な**名前を入力します有効なステータス メッセージは次のとおりです。 • Successful completion of remediation • Error in the input provided to the remediation module • Error in the remediation module configuration • Error logging into the remote device or server • Unable to gain required privileges on remote device or server • Timeout logging into remote device or server • Timeout executing remote commands or servers • The remote device or server was unreachable • The remediation was attempted but failed • Failed to execute remediation program • Unknown/unexpected error **注**　カスタム修復モジュールをインストールした場合、カスタム モジュールによって実装される追加のステータス メッセージを入力できる場合があります。
時刻	Defense Centerが修復を起動した日付と時刻を指定します。時間入力の構文については、検索での時間制約の指定（60-5 ページ）を参照してください。
Remediation Name	起動された修復の正確な名前を入力します。これは修復を作成したときに指定した名前です。
ポリシー（Policy）	修復をトリガーとして使用した相関ポリシーの名前を入力します。
ルール	修復をトリガーとして使用した相関ポリシーの名前を入力します。

保存されている検索をロードおよび削除する方法など、検索の詳細については、イベントの検索（60-1 ページ）を参照してください。

修復ステータス イベントを検索する方法：

アクセス：Admin

ステップ 1　[Analysis] > [Search] を選択します。

検索ページが表示されます。

ステップ 2　テーブルのドロップダウン メニューから、[Remediation Status] を選択します。

ヒント　データベース内で別の種類のイベントを検索するには、テーブルのドロップダウン リストから選択します。

ステップ 3　表 修復ステータスの検索条件 に記載されているように、該当するフィールドに検索基準を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　制限されたイベント アナリスト ユーザ向けに検索を制限として保存する場合は、**必ず**プライベート検索として保存します。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save As New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

検索結果は、現在の時刻範囲によって制限され、デフォルトの修復ステータス ワークフローに表示されます。カスタム・ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

ダッシュボードの使用

FireSIGHT システム ダッシュボードは、システムによって収集および生成されたイベントに関するデータを含む、現在のシステムのステータスを概要的なビューとして提供します。またダッシュボードを使用して、展開のアプライアンスのステータスと全体の正常性に関する情報を表示することもできます。ダッシュボードへアクセスできるのは、特定のユーザ ロール（Administrator、Maintenance User、Security Analyst、Security Analyst（読み取り専用）、およびダッシュボードの権限のカスタム ロール）だけです。他のロールでは、デフォルトの起動ページとして、ロールに関連するページが表示されます。たとえば、Discovery Admin には、[Network Discovery] ページが表示されます。

ダッシュボードには 1 つ以上のタブがあり、それぞれのタブには、3 列のレイアウトで 1 つ以上のウィジェットを表示できます。ウィジェットは、FireSIGHT システム のさまざまな側面を理解するための、自己完結型の小さなコンポーネントです。FireSIGHT システムには、事前定義された複数のウィジェットが付属しています。たとえば、Appliance Information ウィジェットは、アプライアンスの名前、モデル、リモート マネージャ、および FireSIGHT システム ソフトウェアの実行中のバージョンを通知します。

ダッシュボードには、ウィジェットを制約する時間範囲があります。最短で 1 時間前から、最長では 1 年前からの期間を反映するように時間範囲を変更できます。

ダッシュボードは、複雑で高度にカスタマイズ可能なモニタリング機能です。多くのタイプのシステム データを表示するためのもうひとつの方法は、Context Explorer の使用です。これはプリセットの視覚的なコンテキスト セットで侵入、接続、および検出データを使用して情報を提供するものです。このコンテキストは、精度を向上させるためのフィルタを使用して、一時的にのみ変更することができます。FireSIGHT システム ダッシュボードで使用できる包括的なデータとは異なり、Context Explorer はモニタリングの対象のネットワークがどのように見えて、どのように動作しているかを簡単にカラフルな図で示します。Context Explorer の詳細については、Context Explorer の使用法（56-1 ページ）を参照してください。

各タイプのアプライアンスには、Summary Dashboard というデフォルトのダッシュボードが付属しています。このダッシュボードは、一般ユーザに対して、ご利用の FireSIGHT システムの展開についての汎用的な FireSIGHT、侵入、脅威の検出、地理情報、システム ステータスの情報を提供します。ウィジェットには特定のアプライアンス タイプでのみ有用なものもあるため、ユーザが Defense Center仮想 Defense Center、または管理対象デバイスを使用しているかどうかによって、Summary Dashboard は異なります。

注 仮想管理対象デバイスには Web インターフェイスがないため、ダッシュボードをサポートしていません。

デフォルトでは、自身のアプライアンスのホーム ページに Summary Dashboard が表示されますが、別のデフォルト ホーム ページが表示されるようアプライアンスを設定することができます。

ヒント　ホーム ページを変更する場合は、[Overview] > [Dashboards] を選択してダッシュボードにアクセスできます。詳細については、ダッシュボードの表示（55-42 ページ）を参照してください。

表示されるデータは、管理対象デバイスのライセンスと導入方法、データを提供する機能を設定するかどうか、および シリーズ 2 アプライアンスと Cisco NGIPS for Blue Coat X-Series の場合はデータを提供する機能をサポートしているかどうかなどの要因に応じて異なることに注意してください。たとえば、DC500 Defense Center および シリーズ 2 のデバイスは、いずれもカテゴリおよびレピュテーションによる URL フィルタリングをサポートしていないため、DC500 Defense Centerでは、この機能のデータが表示されず、シリーズ 2 デバイスではこのデータを検出しません。

Defense Centerには、Summary Dashboard の他に、事前定義された次のダッシュボードが付属しています。

- Application Statistics ダッシュボードは、モニタリング対象のネットワークについて、アプリケーションのアクティビティおよび侵入イベントの詳しい情報を提供します。このダッシュボードを使用して、多くのトラフィックが生じているアプリケーション、許可および拒否された接続、侵入イベント、および使用中の一意のアプリケーションの数と、それらのアプリケーションの推定リスクとビジネスの関連性を追跡することができます。
- Connection Summary ダッシュボードは、接続データを使用して、モニタリング対象のネットワークのアクティビティについて表およびチャートを作成します。このダッシュボードを使用して、ポート、アプリケーション、ネットワークの接続とトラフィックに関連するイニシエータおよびレスポンダの IP、接続とトラフィックの全体量、位置情報を追跡することができます。データを生成するには、このダッシュボードの接続を記録する必要があります。接続およびセキュリティ インテリジェンスのデータについて（39-2 ページ）を参照してください。このウィジェットの出力は、接続のロギング設定によって異なることに注意してください。

ヒント　このダッシュボードのウィジェットは、トラフィックの合計をキロバイト（KB）単位で示します。トラフィックの合計（KB）は、1 秒あたりのトラフィック（KB/s）に、選択された期間に対象となった合計の秒数を掛けた値と同じです。

- Detailed Dashboard は、アドバンスト ユーザに対して、自身の FireSIGHT システムの展開について詳細な情報を提供します。この中には、収集された侵入イベント、ネットワーク検出、コンプライアンス、相関、トラフィック、システム ステータス データを要約した複数のウィジェットが含まれているだけでなく、Ciscoのニュースおよび製品のアップデートに関する情報を提供します。このダッシュボードを使用して、さまざまなネットワーク情報を一度にモニタリングすることができます。
- Files Dashboard は、管理対象のデバイスによってネットワークで検出されたファイル（マルウェア ファイルも含む）、取得されたファイル（デバイスに格納されており動的な分析のために送信されたファイル）、サブスクリプションベースの FireAMP 方式を使用して検出されたマルウェアについての詳細な情報を提供します。ネットワークベースのマルウェア データを含めるには、Malware のライセンスを所有しており、このダッシュボードに対してマルウェアの検出を有効にしておくことが必要です。また、DC500 および シリーズ 2 デバイスまたは Cisco NGIPS for Blue Coat X-Series はいずれも高度なマルウェア防御をサポートしていないため、DC500 はこのデータを表示できず、シリーズ 2 デバイスと Cisco NGIPS for Blue Coat X-Series はこのデータを検出しません。詳細については、マルウェア対策とファイル制御について（37-2 ページ）を参照してください。
- URL Statistics ダッシュボードは、モニタリング対象のネットワークから外部 URL へ許可および拒否されたトラフィックについての詳細情報を、URL のカテゴリおよびレピュテーションでソートして提供します。URL カテゴリおよびレピュテーション データを含めるに

は、URL Filtering のライセンスを所有しており、このダッシュボードに対して URL Filtering を有効にしておくことが必要です。DC500 および シリーズ 2 のデバイスはいずれもレピュテーションおよびカテゴリによる URL のフィルタリングをサポートしていないため、DC500 はこのデータを表示できず、シリーズ 2 デバイスではこれを検出しないことに注意してください。レピュテーション ベースの URL ブロックの実行（16-11 ページ）を参照してください。

- [Access Controlled User Statistics] ダッシュボードは、モニタリング対象のネットワークについて、ユーザのアクティビティおよび侵入イベントの詳しい情報を提供します。このダッシュボードを使用して、許可および拒否された接続、トラフィック、およびネットワーク上のユーザに関連付けられている侵入イベント、ネットワーク上の一意のユーザ数を追跡できます。このダッシュボードはユーザによって認識されるデータを利用しているため、このダッシュボードで意味のある統計を表示するためには、少なくとも 1 つの User Agent および Defense Center-Active Directory LDAP サーバ接続を設定している必要があります。Active Directory のログインを報告するためのユーザ エージェントの使用（17-11 ページ）を参照してください。

事前定義されたダッシュボードを使用し、それらのダッシュボードを修正することも、自身のニーズに合わせてカスタム ダッシュボードを作成することも可能です。アプライアンスのすべてのユーザでカスタム ダッシュボードを共有することも、自分専用に使用するカスタム ダッシュボードを作成することもできます。また、カスタム ダッシュボードを自分のデフォルトのダッシュボードに設定することもできます。

イベントのドリルダウン ページとテーブル ビューには、[Dashboard] ツールバーのリンクが含まれているものがあります。このリンクをクリックして、関連する事前定義されたダッシュボードを表示することができます。次の表は、イベント ビューと、対応する事前定義されたダッシュボードの対応を示しています。事前定義されたダッシュボード またはタブを削除すると、関連付けられているダッシュボードのリンクが機能しなくなることに注意してください。

表 55-1　　イベント テーブルのダッシュボード リンク

テーブル	ダッシュボード リンク
Connection Events （[Analysis] > [Connections] > [Events]）	Connection Summary
Security Intelligence Events （[Analysis] > [Connections] > [Security Intelligence]）	Connection Summary
Intrusion Events （[Analysis] > [Intrusions] > [Events]）	Summary（[Intrusion Events] タブ）
Malware Events （[Analysis] > [Files] > [Malware Events]）	Files（[Malware] タブ）
File Events （[Analysis] > [Files] > [File Events]）	Files（[Files] タブ）
Captured Files （[Analysis] > [Files] > [Captured Files]）	Files（[File Storage] タブ）
アプリケーション （[Analysis] > [Hosts] > [Applications]）	Application Statistics
Application Details （[Analysis] > [Hosts] > [Applications Details]）	Application Statistics

表 55-1　イベント テーブルのダッシュボード リンク（続き）

テーブル	ダッシュボード リンク
Indications of Compromise（侵害の痕跡） （[Analysis] > [Hosts] > [Indications of Compromise]）	Summary（[Threats] タブ）
ユーザ （[Analysis] > [Users] > [Users]）	Access Controlled User Statistics
User Activity （[Analysis] > [Users] > [User Activity]）	Access Controlled User Statistics
Correlation Events （[Analysis] > [Correlation] > [Correlation Events]）	Detailed（[Correlation] タブ）
White List Events （[Analysis] > [Correlation] > [White List Events]）	Detailed（[Correlation] タブ）

ダッシュボードおよび内容の詳細については、次の項を参照してください。

- ダッシュボード ウィジェットについて（55-4 ページ）
- 事前定義されたウィジェットについて（55-7 ページ）
- ダッシュボードの操作（55-40 ページ）

ダッシュボード ウィジェットについて

ライセンス： すべて

ダッシュボードには 1 つ以上のタブがあり、それぞれのタブには、3 列のレイアウトで 1 つ以上のウィジェットを表示できます。FireSIGHT システムには、事前定義された多数のダッシュボード ウィジェットが付属しています。それぞれのウィジェットは、FireSIGHT システムのさまざまな側面を理解するうえで役に立ちます。ウィジェットは、次の 3 つのカテゴリに分類されます。

- *Analysis & Reporting* ウィジェットは、FireSIGHT システム で収集および生成されたイベントに関するデータを表示します。
- *Miscellaneous* ウィジェットは、イベント データもオペレーション データも表示しません。現時点では、このカテゴリのウィジェットのみが RSS フィードを表示します。
- *Operations* ウィジェットは、FireSIGHT システムのステータスおよび全体の正常性に関する情報を表示します。

表示できるダッシュボード ウィジェットは、使用しているアプライアンスのタイプと、自分のユーザ ロールによって異なります。また、各ダッシュボードには、動作を決定する一連のプリファレンスがあります。ユーザは、ウィジェットを最小化および最大化する、タブに対してウィジェットを追加および削除する、タブ上でウィジェットを再配置する、といったことができます。

注　所定の時間範囲でのイベント数を表示するウィジェットでは、イベント ビューアで利用できる詳細なデータのイベント数が、イベントの総数に反映されないことがあります。これは、システムがディスク領域の使用率を管理するために、古いイベントの詳細をプルーニングすることがあるために発生します。イベント詳細のプルーニングを最小限にするために、対象の展開にとって最も重要なイベントだけを記録するようにイベント ロギングを調整できます。詳細については、ネットワーク トラフィックの接続のロギング（38-1 ページ）を参照してください。

詳細については、以下を参照してください。

- ウィジェットの可用性について（55-5 ページ）
- ウィジェットのプリファレンスについて（55-7 ページ）
- 事前定義されたウィジェットについて（55-7 ページ）
- ダッシュボードの操作（55-40 ページ）

ウィジェットの可用性について

ライセンス： すべて

FireSIGHT システムには、事前定義された複数のダッシュボード ウィジェットが付属しています。表示できるダッシュボード ウィジェットは、使用しているアプライアンスのタイプと、自分のユーザ ロールによって異なります。

- *無効な*ウィジェットは、ユーザが間違ったタイプのアプライアンスを使用しているため、表示することができないものです。
- *不正な*ウィジェットは、ユーザが必要なアカウントの権限を持っていないため、表示することができないものです。

たとえば、Current Sessions ウィジェットはすべてのアプライアンスで使用できますが、Administrator アカウント権限を持っているユーザしか使用できません。また、Appliance Status ウィジェットは、Defense Center上で、Administrator、Maintenance User、Security Analyst、または Security Analyst（読み取り専用）アカウント権限を持っているユーザのみが使用できます。

不正なウィジェットまたは無効なウィジェットはダッシュボードに追加できませんが、他の種類のアプライアンスで作成された、または他のアクセス権限を持つユーザによって作成されたダッシュボードをインポートした場合、それらのダッシュボードには、不正または無効なウィジェットが含まれていることがあります。これらのウィジェットは使用できなくなり、ユーザが表示できない理由を示すエラー メッセージが表示されます。

ウィジェットは、アプライアンスがアクセス権を持っていないデータを表示できないことにも注意してください。たとえば、管理対象デバイスは、相関イベント、侵入イベント、検出イベントなどにアクセスできません。これらのデータ タイプのいずれかを表示するために設定された Custom Analysis ウィジェットが含まれている管理対象デバイスにダッシュボードをインポートすると、ウィジェットでエラー メッセージが表示されます。これらのウィジェットがタイムアウトした場合、またはそれ以外で問題が発生した場合には、個々のウィジェットでもエラー メッセージが表示されます。

ウィジェットの内容は、使用しているアプライアンスのタイプによって異なる場合があります。たとえば、Defense Center上の Custom Analysis ウィジェットはディスカバリ情報を表示できますが、管理対象デバイスで Custom Analysis が設定されている場合は、この機能は使用できません。テーブルの列見出しをクリックすると、表形式で生成されている任意の内容をソートできます。

不正なウィジェットと無効なウィジェット、および表示するデータがないウィジェットを削除または最小化できます。共有しているダッシュボード上でウィジェットを変更すると、アプライアンスのすべてのユーザに変更が反映されることに注意してください。詳細については、ウィジェットの最小化および最大化（55-48 ページ）およびウィジェットの削除（55-48 ページ）を参照してください。

次の表に、各アプライアンスが表示できる有効なウィジェットを示します。

表 55-2　FirePOWER アプライアンスとダッシュボード ウィジェットの可用性

ウィジェット	Defense Center	任意の管理対象デバイス
Appliance Information	はい	はい
Appliance Status	はい	いいえ
Correlation Events	はい	いいえ
Current Interface Status	はい	はい
Current Sessions	はい	はい
Custom Analysis	はい	いいえ
Disk Usage	はい	はい
Interface Traffic	はい	はい
Intrusion Events	はい	いいえ
Network Compliance	はい	いいえ
Product Licensing	はい	いいえ
Product Updates	はい	はい
RSS Feed	はい	はい
System Load	はい	はい
System Time	はい	はい
White List Events	はい	いいえ

次の表に、各ウィジェットを表示するために必要なユーザ アカウントの権限を示します。Administrator、Maintenance User、Security Analyst、または Security Analyst（読み取り専用）のアクセス権を持つユーザ アカウントのみがダッシュボードを使用できます。

カスタム ロールを持つユーザは、自身のユーザ ロールの許可によって、ウィジェットのいずれかの組み合わせにアクセスできる場合もあれば、どのウィジェットにもアクセスできない場合もあります。

表 55-3　ユーザ ロールとダッシュボード ウィジェットの可用性

ウィジェット	Administrator	Maintenance User	Security Analyst	Security Analyst（RO）
Appliance Information	はい	はい	はい	はい
Appliance Status	はい	はい	はい	いいえ
Correlation Events	はい	いいえ	はい	はい
Current Interface Status	はい	はい	はい	はい
Current Sessions	はい	いいえ	いいえ	いいえ
Custom Analysis	はい	いいえ	はい	はい
Disk Usage	はい	はい	はい	はい
Interface Traffic	はい	はい	はい	はい
Intrusion Events	はい	いいえ	はい	はい
Network Compliance	はい	いいえ	はい	はい
Product Licensing	はい	はい	いいえ	いいえ

表 55-3　ユーザ ロールとダッシュボード ウィジェットの可用性（続き）

ウィジェット	Administrator	Maintenance User	Security Analyst	Security Analyst（RO）
Product Updates	はい	はい	いいえ	いいえ
RSS Feed	はい	はい	はい	はい
System Load	はい	はい	はい	はい
System Time	はい	はい	はい	はい
White List Events	はい	いいえ	はい	はい

ウィジェットのプリファレンスについて

ライセンス： すべて

各ウィジェットには、動作を決定する一連のプリファレンスがあります。

ウィジェットのプリファレンスは単純なものにすることもできます。たとえば、次の図は Current Interface Status ウィジェットのプリファレンスを示しています。これは、内部ネットワークで有効になっているすべてのインターフェイスについて現在のステータスを表示します。このウィジェットでは、アップデートの頻度のみを設定します。

ウィジェットのプリファレンスは、もっと複雑にすることもできます。たとえば、次の図は Custom Analysis ウィジェットのプリファレンスを示しています。これは高度にカスタマイズ可能なウィジェットで、これを使用すると、FireSIGHT システムで収集および生成されたイベントの詳細情報を表示できます。

ウィジェットのプリファレンスを変更する方法：

アクセス： Admin/Any Security Analyst/Maint

ステップ 1　プリファレンスを変更するウィジェットのタイトル バーで、プリファレンスの表示アイコン（ ）をクリックします。

そのウィジェットのプリファレンス セクションが表示されます。

ステップ 2　必要に応じて変更を加えます。

変更はすぐに反映されます。ユーザが個々のウィジェットに指定できるプリファレンスについては、事前定義されたウィジェットについて（55-7 ページ）を参照してください。

ステップ 3　プリファレンスのセクションを非表示にするには、ウィジェットのタイトル バーで、プリファレンスの非表示アイコン（ ）をクリックします。

事前定義されたウィジェットについて

ライセンス： すべて

FireSIGHT システム にはいくつかの事前定義されたウィジェットが付属しています。ダッシュボード上でこれらのウィジェットを使用すると、展開におけるアプライアンスのステータスと全体の正常性に関する情報だけでなく、システムで収集および生成されたイベントに関するデータも含めて、現在のシステムのステータスを概要的なビューとして提供します。

FireSIGHT システムに付属するウィジェットの詳細については、以降の項を参照してください。

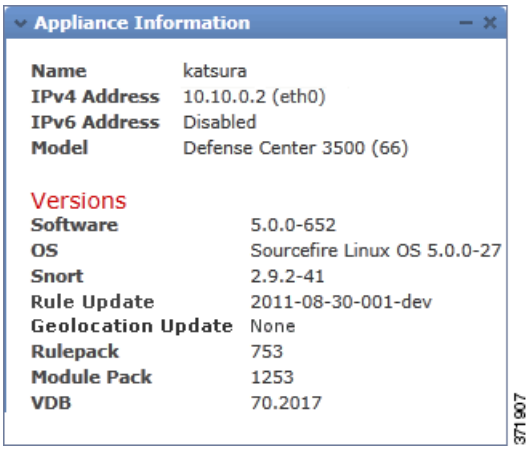
- Appliance Information ウィジェットについて（55-8 ページ）
- Appliance Status ウィジェットについて（55-9 ページ）
- Correlation Events ウィジェットについて（55-10 ページ）
- Current Interface Status ウィジェットについて（55-10 ページ）
- Current Sessions ウィジェットについて（55-11 ページ）
- Custom Analysis ウィジェットについて（55-12 ページ）
- Disk Usage ウィジェットについて（55-29 ページ）
- インターフェイス トラフィック ウィジェットについて（55-30 ページ）
- Intrusion Events ウィジェットについて（55-31 ページ）
- Network Compliance ウィジェットについて（55-33 ページ）
- Product Licensing ウィジェットについて（55-35 ページ）
- Product Updates ウィジェットについて（55-36 ページ）
- RSS Feed ウィジェットについて（55-37 ページ）
- System Load ウィジェットについて（55-38 ページ）
- System Time ウィジェットについて（55-38 ページ）
- White List Events ウィジェットについて（55-39 ページ）

注　表示できるダッシュボード ウィジェットは、使用しているアプライアンスのタイプと、自分のユーザ ロールによって異なります。詳細については、ウィジェットの可用性について（55-5 ページ）を参照してください。

Appliance Information ウィジェットについて

ライセンス： すべて

Appliance Information ウィジェットは、アプライアンスのスナップショットを提供します。このウィジェットは、Detailed Dashboard および Summary Dashboard の [Status] タブにデフォルトで表示されます。



このウィジェットは以下の情報を提供します。

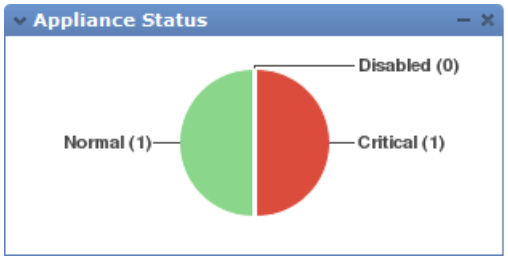
- アプライアンスの名前、IPv4 アドレス、IPv6 アドレス、およびモデル
- ダッシュボードでアプライアンスにインストールされている、FireSIGHT システム ソフトウェア、オペレーティング システム、Snort、ルール アップデート、ルール パック、モジュール パック、脆弱性データベース（VDB）、および地理情報のアップデートのバージョン（仮想 Defense Centerは除く）
- 管理対象アプライアンスの場合は、管理アプライアンスとの通信リンクの名前とステータス
- ハイアベイラビリティ ペアのDefense Centerの場合は、Defense Centerによって最近行われた通信、およびピアDefense Centerの名前、モデル、および FireSIGHT システム ソフトウェアとオペレーティング システムのバージョン

単純なビューまたは高度なビューを表示するようにウィジェットのプリファレンスを変更することで、ウィジェットで表示する情報量を調整できます。プリファレンスでは、ウィジェットをアップデートする頻度を調整することもできます。詳細については、ウィジェットのプリファレンスについて（55-7 ページ）を参照してください。

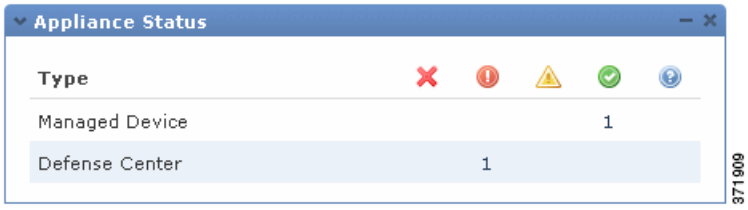
Appliance Status ウィジェットについて

ライセンス：すべて

Appliance Status ウィジェットは、アプライアンスの正常性、およびそのアプライアンスが管理しているアプライアンスの正常性を示します。Defense Centerは、管理対象のデバイスに対して自動的に正常性ポリシーを適用しないため、ユーザは正常性ポリシーをデバイスへ手動で適用する必要があります。このようにしないと、デバイスのステータスは `Disabled` として示されます。このウィジェットは、Detailed Dashboard および Summary Dashboard の [Status] タブにデフォルトで表示されます。



ウィジェットのプリファレンスを変更して、アプライアンスのステータスを円グラフまたは表で表示するように設定できます。



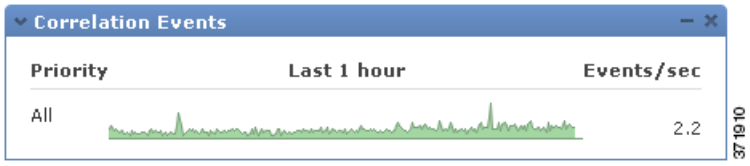
プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。詳細については、ウィジェットのプリファレンスについて（55-7 ページ）を参照してください。

円グラフの一部、またはアプライアンス ステータス表のいずれかの数字をクリックすると、[Health Monitor] ページが表示され、対象のアプライアンス、およびそのアプライアンスが管理しているすべてのアプライアンスのコンパイル済みの正常性ステータスを参照することができます。詳細については、ヘルス モニタの使用（68-45 ページ）を参照してください。

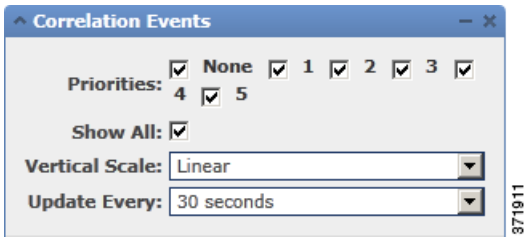
Correlation Events ウィジェットについて

ライセンス：FireSIGHT

Correlation Events ウィジェットは、ダッシュボードの時間範囲における 1 秒あたりの相関イベントの平均数を、優先度ごとに示します。このウィジェットは、Detailed Dashboard の [Correlation] タブにデフォルトで表示されます。



ウィジェットを設定して、線形（増分）や対数（10 の倍数）のスケールを選択するだけでなく、ウィジェットのプリファレンスを変更してさまざまな優先度の相関イベントを表示することができます。



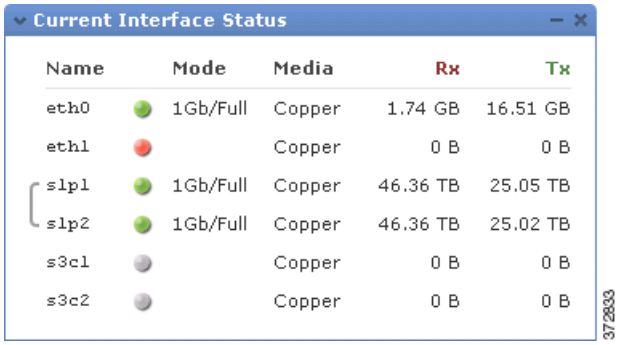
優先度を持たないイベントも含めて、特定の優先度のイベントに対して別のグラフを表示するには、1 つ以上の [Priorities] チェック ボックスをオンにします。優先度に関係なくすべての相関イベントに対して追加のグラフを表示するには、[Show All] を選択します。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。詳細については、ウィジェットのプリファレンスについて（55-7 ページ）を参照してください。

グラフをクリックして特定の優先度の相関イベントを表示することも、[All] グラフをクリックしてすべての相関イベントを表示することもできます。いずれの場合も、イベントはダッシュボードの時間範囲に制限されます。ダッシュボードを介して相関イベントにアクセスすると、そのアプライアンスに対するイベント（またはグローバル）の期間が変わります。相関イベントの詳細については、相関イベントの表示（51-56 ページ）を参照してください。

Current Interface Status ウィジェットについて

ライセンス：すべて

Current Interface Status ウィジェットは、有効になっているか未使用のアプライアンスのすべてのインターフェイスのステータスを示します。Defense Center では、管理（`eth0`、`eth1` など）インターフェイスを表示できます。管理対象デバイスでは、センシング（`s1p1` など）インターフェイスのみを表示するか、または管理インターフェイスとセンシング インターフェイスの両方を表示するかを選択できます。インターフェイスは、タイプ（管理、インライン、パッシブ、スイッチド、ルーテッド、スタック、未使用）別にグループ化されます。



ウィジェットは、各インターフェイスに対して次の情報を提供します。

- インターフェイスの名前
- インターフェイスのリンク状態
- インターフェイスのリンク モード（100Mb 全二重、または 10Mb 半二重など）
- インターフェイスのタイプ（銅線または光ファイバ）
- インターフェイスで受け取ったデータ量（Rx）および送信したデータ量（Tx）

リンク状態を表すボールの色は、次のように現在のステータスを示します。

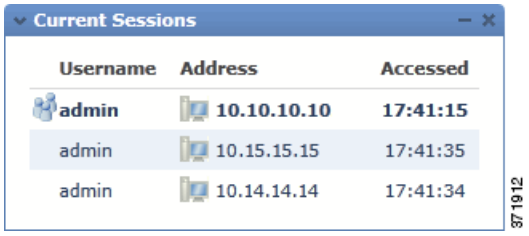
- 緑色：リンクがフル スピードでアップ状態になっています
- 黄色：リンクはアップ状態ですがフル スピードではありません
- 赤色：リンクはアップ状態ではありません
- 灰色：リンクは管理上無効になっています
- 青色：リンク ステート情報は使用できません（たとえば ASA）

ウィジェットのプリファレンスでは、ウィジェットをアップデートする頻度を調整します。詳細については、ウィジェットのプリファレンスについて（55-7 ページ）を参照してください。

Current Sessions ウィジェットについて

ライセンス： すべて

Current Sessions ウィジェットは、アプライアンスに現在ログインしているユーザ、セッションが生じたマシンに関連付けられている IP アドレス、各ユーザがアプライアンス上のページにアクセスした最後の（アプライアンスのローカル時間に基づいた）時間を示します。自分を表すユーザ（現在ウィジェットを表示しているユーザ）には、ユーザ アイコン（ ）のマークが付けられ、太字で示されます。ログオフするか非アクティブになってから 1 時間以内に、セッションはこのウィジェットのデータからプルーニングされます。このウィジェットは、Detailed Dashboard および Summary Dashboard の [Status] タブにデフォルトで表示されます。



Current Sessions ウィジェットで、次のことができます。

- いずれかのユーザ名をクリックして、[User Management] ページでユーザ アカウントを管理します。ユーザ アカウントの管理（61-46 ページ）を参照してください。
- ホスト アイコン（）、または IP アドレスの隣の侵害されたホスト アイコン（）をクリックして、関連付けられているマシンのホスト プロファイルを表示します。ホスト プロファイルの使用（49-1 ページ）を参照してください（ネットワーク検出でのDefense Centerのみ）。
- いずれかの IP アドレスまたはアクセス時間をクリックして、その IP アドレスおよびその IP アドレスに関連付けられているユーザが Web インターフェイスにログオンした時間によって制約される監査ログを表示します。監査レコードの表示（69-2 ページ）を参照してください。

ウィジェットのプリファレンスでは、ウィジェットをアップデートする頻度を調整します。詳細については、ウィジェットのプリファレンスについて（55-7 ページ）を参照してください。

Custom Analysis ウィジェットについて

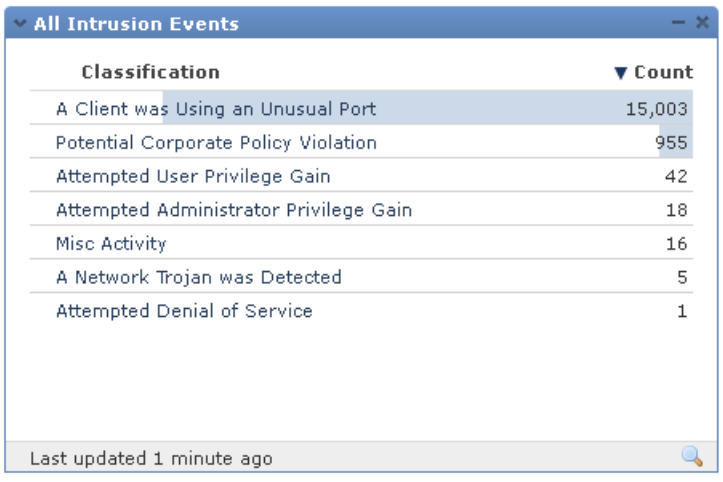
ライセンス： すべて

Custom Analysis ウィジェットは高度にカスタマイズ可能なウィジェットで、これを使用すると、FireSIGHT システムで収集および生成されたイベントの詳細情報を表示できます。

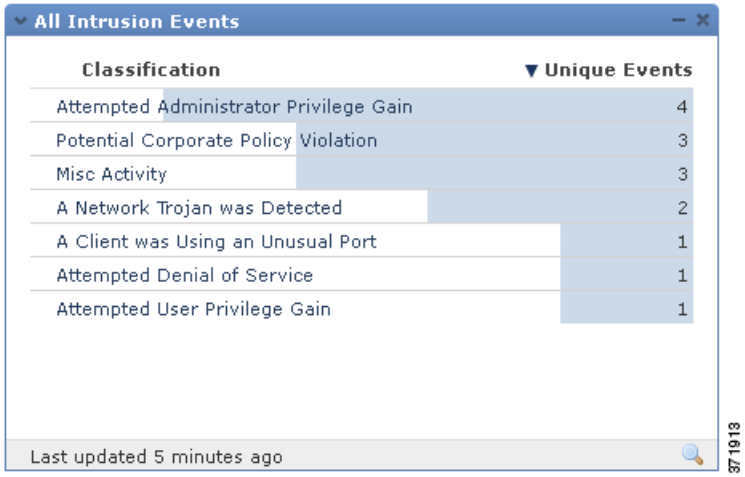
Custom Analysis ウィジェットには、ウィジェットの多数のプリセットが付属しています。これらのプリセットは、Ciscoで事前定義された設定のグループです。プリセットは例として機能し、これを使用して展開に関する情報へすばやくアクセスできます。これらのプリセットを使用することも、カスタム設定を作成することもできます。

ウィジェットのプリファレンスを設定する場合、ウィジェットで表示するデータをどのようにグループ化するかを設定する集約方法の他に、どのテーブルおよび個々のフィールドを表示するかを選択する必要があります。

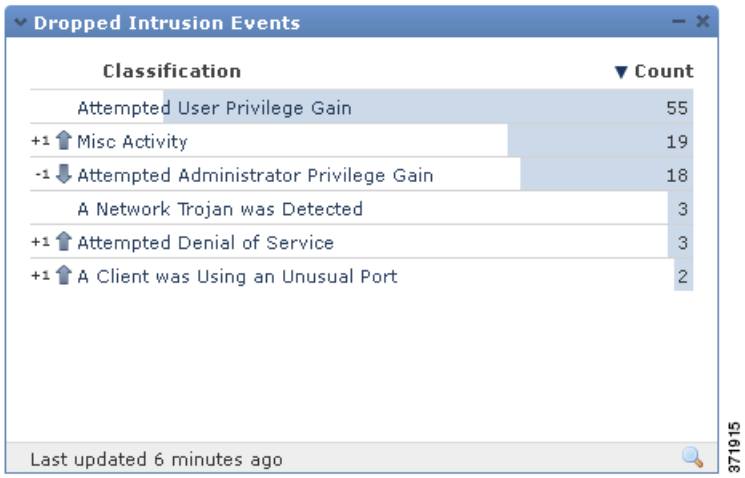
たとえば、[Intrusion Events] テーブルのデータを表示するようにウィジェットを設定して、最近の侵入イベントのリストを表示するよう Custom Analysis ウィジェットを設定することができます。[Classification] フィールドを選択し、このデータを [Count] によって集約すると、各タイプのイベントがいくつ生成されたかが通知されます。この数には、侵入イベントについてレビューされたイベントが含まれていることに注意してください。イベント数をイベント ビューアで表示する場合は、レビューされたイベントは含まれません。



一方、[Unique Events] によって集約すると、各タイプで一意の侵入イベントがいくつ発生したかが通知されます（たとえばネットワークの Trojan、企業ポリシーの潜在的な違反、行われたサービス妨害攻撃の検出個数など）。



オプションとして、保存されている検索（アプライアンスに付属している事前定義の検索、またはユーザが作成したカスタム検索のいずれか）を使用して、ウィジェットをさらに制約することができます。たとえば、最初の例（[Classification] フィールドを使用して [Count] で集約する）を、[Dropped Events] の検索を使用して制約すると、各タイプの侵入イベントがいくつドロップされたかが通知されます。



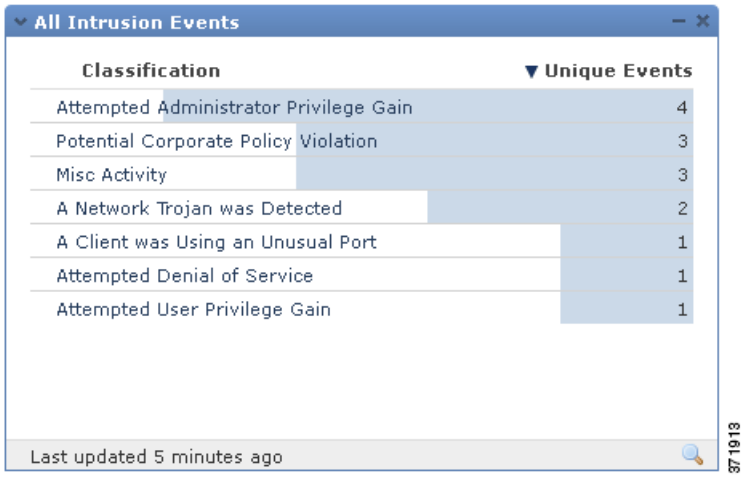
ウィジェットの背景の色付きバーは、各イベントの発生の相対数を示しています。このバーは右から左へ読みます。バーの色およびウィジェットに表示される行数を変更できます。また、発生頻度が最も多いイベントや、発生頻度が最も少ないイベントを表示するようウィジェットを設定することもできます。

矢印のアイコン（▼）は、表示のソート順を示して、制御しています。下向きのアイコンは降順を表し、上向きのアイコンは昇順を表します。ソート順を変更するには、アイコンをクリックします。

最新の結果以降何らかの変更点があることを示すために、ウィジェットでは、各イベントの横に次の 3 つのアイコンのうちの 1 つを表示します。

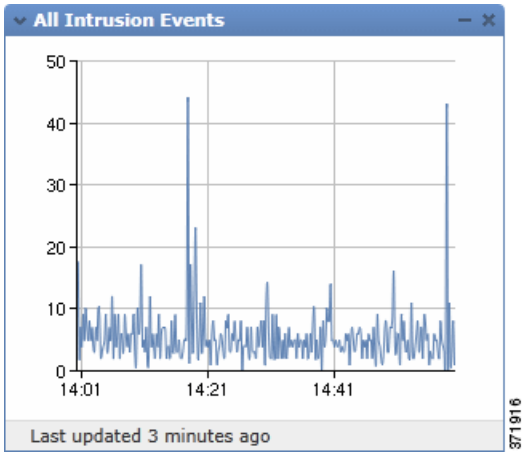
- 新しいイベント アイコン( )は、イベントが、最新の結果以降のものであることを示します。
- 上向き矢印のアイコン( )は、ウィジェットが最後にアップデートされた後で、イベントがこの場所に上がってきたことを示します。イベントが何段階上がってきたかを表す数字が、アイコンの横に示されます。
- 下向き矢印のアイコン( )は、ウィジェットが最後にアップデートされた後で、イベントがこの場所に下がってきたことを示します。イベントが何段階下がってきたかを表す数字が、アイコンの横に示されます。

ウィジェットは、アプライアンスのローカル時間に基づいて、最後にアップデートされた時間を表示します。ウィジェットは、ダッシュボードの時間範囲に基づいた頻度でアップデートされます。たとえば、ダッシュボードの時間範囲を 1 時間に設定すると、ウィジェットは 5 分ごとにアップデートされます。また、ダッシュボードの時間範囲を 1 年に設定すると、ウィジェットは 1 週間ごとにアップデートされます。ダッシュボードが次にアップデートされるタイミングを設定するには、ウィジェットの左下にある [Last updated] の通知にポインタを移動します。



注　保存されている検索を使用して Custom Analysis ウィジェットを制約し、その後で検索を編集すると、次にアップデートされるまでウィジェットには変更が反映されません。

一定期間のイベントまたは収集されたその他のデータに関する情報が必要な場合は、対象の展開で、一定期間に発生した侵入イベントの合計数を表示するような線グラフを表示するように Custom Analysis ウィジェットを設定することができます。一定期間のグラフでは、ウィジェットで使用するタイム ゾーンおよび線の色を選択できます。



最後に、ウィジェットのカスタム タイトルを選択できます。

Custom Analysis ウィジェットから、イベント ビュー（つまりワークフロー）を起動することができます。イベント ビューは、ウィジェットに表示されるイベントに関する詳細情報を提供します。これには、詳細情報を表示するイベントをクリックします。

または、Custom Analysis ウィジェットのいずれかの IP アドレスを右クリックしてコンテキスト メニューを表示します。コンテキスト メニューから、関連するホストの詳細な情報を取得したり、Security Intelligence フィルタリングに対するグローバルなブラックリストまたはホワイトリストに情報を追加したりすることができます。

注　Custom Analysis ウィジェットをどのように設定するかによって、アプライアンス リソースの消費量が増えることがあります。赤い影の付いた Custom Analysis ウィジェットは、そのウィジェットの使用によりシステムのパフォーマンスが低下していることを示しています。ウィジェットが長時間赤い状態のままになっている場合は、そのウィジェットを削除する必要があります。

詳細については、次の項を参照してください。

- Custom Analysis ウィジェットの設定（55-15 ページ）
- Custom Analysis ウィジェットから関連付けられているイベントを表示する（55-27 ページ）
- Custom Analysis ウィジェットの制限（55-28 ページ）
- コンテキスト メニューの使用（2-5 ページ）

Custom Analysis ウィジェットの設定

ライセンス： すべて

他のウィジェットと同様に、Custom Analysis ウィジェットには動作を決定するためのプリファレンスがあります。Custom Analysis ウィジェットを設定するには、ウィジェットのプリファレンスについて（55-7 ページ）に記載されているようにプリファレンスを表示します。

イベントの相対的な発生数を示す（棒グラフ）ようにウィジェットを設定するか、一定期間のグラフを示す（線グラフ）ようにウィジェットを設定するかによって、表示されるプリファレンスのセットが異なります。

棒グラフを表示するようにウィジェットを設定するには、[Field] ドロップダウンリストから [Time] を除く任意の値を選択します。

線グラフを表示するようにウィジェットを設定するには、[Field] ドロップダウンリストから [Time] を選択します。

次の表に、Custom Analysis ウィジェットで設定できるさまざまな設定について示します。

表 55-4　Custom Analysis ウィジェットのプリファレンス

使用するプリファレンス	制御する内容
Title	ウィジェットのタイトル。 タイトルを指定しない場合、アプライアンスは、設定済みのイベント タイプをウィジェットのタイトルとして使用します。
プリセット	ウィジェットのプリセット。 Custom Analysis ウィジェットには多数のプリセットが付属しています。これらのプリセットは、Ciscoによって事前定義されたウィジェットの設定です。プリセットは例として機能し、これを使用して展開に関する情報へすばやくアクセスできます。これらのプリセットを使用することも、カスタム設定を作成することもできます。 プリセットの詳細については、Custom Analysis ウィジェットのプリセットの表を参照してください。
Table	ウィジェットが表示するイベント データが含まれているイベントのテーブル。
フィールド	表示するイベントタイプの特定のフィールド。 **ヒント**　一定期間のグラフを表示するには、[Time] を選択します。
Aggregate	ウィジェットの集約方法。 集約方法は、表示するデータをウィジェットがどのようにグループ化するかを設定します。ほとんどのイベント タイプで、デフォルトの集約基準は [Count] です。
フィルタ	ウィジェットが表示するデータをさらに制限するための、ユーザ定義のアプリケーション フィルタ。 [Application Statistics] または [Intrusion Event Statistics by Application] テーブルのデータを表示している場合は、アプリケーション フィルタのみ使用できます。アプリケーション フィルタの詳細については、アプリケーション フィルタの操作（3-16 ページ）を参照してください。
検索	ウィジェットが表示するデータをさらに制限するために使用する、保存済みの検索。 検索を指定する必要はありませんが、プリセットの中には事前定義された検索が使用されるものがあります。 アスタリスク（*）なしでフィールド内のデータを使用する保存済みの接続イベント検索を作成すると、ウィジェットに誤ったデータが表示されます。接続イベントに基づいてカスタム分析ダッシュボードのウィジェットを制約できるのは、接続サマリーを制限しているフィールドだけです。無効な検索はグレー表示され、選択できません。
表示	発生頻度が最も多いイベントを表示する（[Top]）か、発生頻度が最も少ないイベントを表示する（[Bottom]）か。

表 55-4　Custom Analysis ウィジェットのプリファレンス（続き）

使用するプリファレンス	制御する内容
結果	表示する結果の行数。 結果は 10 から 25 行で表示できます。行数は 5 行ずつ増やすことができます。
Show Movers	最新の結果以降の変更を示すアイコンを表示するかどうか。
Time Zone	結果の表示に使用するタイム ゾーン。 タイム ゾーンは、時間ベースのフィールドを選択したときに常に表示されます。
色	各結果の相対的な発生数を示す、ウィジェット背景のバーの色。

以下の表で、Custom Analysis ウィジェットで使用できるプリセットについて説明します。また、各プリセットがDefense Center事前定義されたどのダッシュボードに使用されるかについても示します（事前定義されたダッシュボードがある場合）。次の点に注意してください。

- NO MDC THIS TIME管理対象デバイス上の事前定義されたダッシュボードには、Custom Analysis ウィジェットが含まれていません。
- DC500 Defense Center はサポートしていない機能のデータを表示しません。また、シリーズ 2 デバイスおよび Cisco NGIPS for Blue Coat X-Series はサポートしていない機能のデータを検出しません。

特定のライセンス タイプの詳細については、サービス サブスクリプション（65-8 ページ）を参照してください。

表 55-5　Custom Analysis ウィジェットのプリセット

プリセット	説明	事前定義されたダッシュボード	ライセンス
All Intrusion Events	ダッシュボードの時間範囲で、モニタリング対象のネットワーク上の侵入イベントの合計数のグラフを表示します。	Detailed Dashboard サマリー ダッシュボード	Protection
All Intrusion Events（Not Dropped）	発生頻度が最も多いタイプの侵入イベントを分類して表示します。ここでは、イベントの一部としてパケットはドロップしていません。	Detailed Dashboard	Protection
Allowed Connections by Application	モニタリング対象のネットワーク上で許可されたアプリケーションの接続を、アプリケーションごとにグループ化して表示します。	Application Statistics	FireSIGHT
Allowed Connections by Application Risk	モニタリング対象のネットワーク上で許可されたアプリケーションの接続を、アプリケーションのリスク レベルによってグループ化して表示します。	Application Statistics	FireSIGHT
Allowed Connections by Business Relevance	モニタリング対象のネットワーク上で許可されたアプリケーションの接続を、事業活動の推定される関連性によってグループ化して表示します。	Application Statistics	FireSIGHT

表 55-5　Custom Analysis ウィジェットのプリセット（続き）

プリセット	説明	事前定義されたダッシュボード	ライセンス
Allowed Connections by URL Category	モニタリング対象のネットワーク上で許可されたアプリケーションの接続を、URL カテゴリごとにグループ化して表示します。	URL Statistics	URL Filtering
Allowed Connections by URL Reputation	モニタリング対象のネットワーク上で許可されたアプリケーションの接続を、URL レピュテーションごとにグループ化して表示します。	URL Statistics	URL Filtering
Allowed Connections by User	モニタリング対象のネットワーク上で許可されたアプリケーションの接続を、接続しているユーザごとにグループ化して表示します。	Access Controlled User Statistics	FireSIGHT
Application Protocols Introducing Malware	ネットワークを介して送信されたマルウェア ファイルの数を、ファイルの送信に使用されたアプリケーション プロトコルごとにグループ化して表示します。	Files Dashboard	Malware
Application Protocols Transferring Files	ネットワークを介して送信されたファイルの数を、ファイルの送信に使用されたアプリケーション プロトコルごとにグループ化して表示します。	Files Dashboard	Protection
Client Applications Introducing Malware	FireAMP コネクタで検出されたマルウェアにアクセスした、または作成したアプリケーション、または親ファイルを表示します。	Files Dashboard	FireAMPサブスクリプション
Client Applications Transferring Files	ネットワークを介してファイルを送信したアプリケーション、または親ファイルを表示します。	Files Dashboard	Protection
クライアント	モニタリング対象のネットワーク上のクライアントを、タイプごとに表示します。	Detailed Dashboard	FireSIGHT
Connections by Application	モニタリング対象のネットワーク上のアプリケーションを、検出された接続数に基づいて表示します。	Connection Summary	FireSIGHT
Connections by Destination Continent	モニタリング対象のネットワークから送信された接続の宛先の大陸を、接続数に基づいて表示します。	Connection Summary	FireSIGHT
Connections by Destination Country	モニタリング対象のネットワークから送信された接続の宛先の国を、接続数に基づいて表示します。	Connection Summary	FireSIGHT
Connections by Initiator IP	モニタリング対象のネットワーク上のホスト IP アドレスを、接続（ホスト上の IP アドレスがセッションを開始した接続）の数に基づいて表示します。	Connection Summary	FireSIGHT
Connections by Port	モニタリング対象のネットワーク上のポートを、検出された接続数に基づいて表示します。	Connection Summary	FireSIGHT

表 55-5　Custom Analysis ウィジェットのプリセット（続き）

プリセット	説明	事前定義されたダッシュボード	ライセンス
Connections by Responder IP	モニタリング対象のネットワーク上のホスト IP アドレスを、セッションのレスポンダがホスト上の IP アドレスであった接続の数に基づいて表示します。このウィジェットの出力は、接続のロギング設定によって異なります。	Connection Summary	FireSIGHT
Connections by Security Intelligence Category	モニタリング対象のネットワーク上の Security Intelligence によってモニタリングまたはブロックされたすべての接続を、Security Intelligence のカテゴリごとにグループ化して表示します。	サマリー ダッシュボード	Protection
Connections by Source Continent	モニタリング対象のネットワークと通信する大陸を、各大陸から開始された接続数に基づいて表示します。	Connection Summary	FireSIGHT
Connections by Source Country	モニタリング対象のネットワークと通信する国を、各国から開始された接続数に基づいて表示します。	Connection Summary	FireSIGHT
Connections by URL Category	モニタリング対象のネットワーク上のすべてのアプリケーションの接続を、URL カテゴリごとにグループ化して表示します。	サマリー ダッシュボード	URL Filtering
Connections by URL Reputation	モニタリング対象のネットワーク上のすべてのアプリケーションの接続を、URL レピュテーションごとにグループ化して表示します。	サマリー ダッシュボード	URL Filtering
Connections over Time	ダッシュボードの時間範囲で、モニタリング対象のネットワーク上の接続の合計数のグラフを表示します。	Connection Summary	FireSIGHT
Denied Connections by Application	モニタリング対象のネットワーク上で拒否された接続を、アプリケーションごとにグループ化して表示します。	Application Statistics	FireSIGHT
Denied Connections by URL Category	モニタリング対象のネットワーク上で拒否された接続を、URL カテゴリごとにグループ化して表示します。	URL Statistics	URL Filtering
Denied Connections by URL Reputation	モニタリング対象のネットワーク上で拒否された接続を、URL レピュテーションごとにグループ化して表示します。	URL Statistics	URL Filtering
Denied Connections by User	モニタリング対象のネットワーク上で拒否された接続を、接続しているユーザごとにグループ化して表示します。	Access Controlled User Statistics	FireSIGHT
Dropped Events by Application	ドロップされた侵入イベントを、アプリケーションごとにグループ化して表示します。	Application Statistics	Protection + FireSIGHT
Dropped Events by User	ドロップされた侵入イベントを、ユーザごとにグループ化して表示します。	Access Controlled User Statistics	Protection + FireSIGHT

表 55-5　Custom Analysis ウィジェットのプリセット（続き）

プリセット	説明	事前定義されたダッシュボード	ライセンス
Dropped Intrusion Events	侵入イベントの数を分類して表示します。ここでは、パケットがドロップされています。	Detailed Dashboard サマリー ダッシュボード	Protection
Dynamic Analysis Traffic by Device	分析用に Collective Security Intelligence クラウド に送信されたファイル データのサイズに基づいて、最もアクティブなデバイスを表示します。	Files Dashboard	Malware
Dynamic Analysis Traffic over Time	ダッシュボードの時間範囲で、取得され、分析用にクラウドに送信されたファイル データのサイズを表示します。	Files Dashboard	Malware
File Actions	ネットワークを介して送信されたファイルの数を、ファイルの処理に使用したファイル ルール アクションごとにグループ化して表示します。	Files Dashboard	Protection または Malware
File Categories	ネットワークを介して送信されたファイルの数を、ファイルのカテゴリごとにグループ化して表示します。	Files Dashboard	Protection
File Dispositions	マルウェア クラウド ルックアップ ファイル ルールの結果としてネットワーク トラフィック内で検出されたファイル数を、マルウェアの性質ごとにグループ化して表示します。	Files Dashboard	Malware
File Names	ネットワークを介して送信されたファイルの数を、ファイル名ごとにグループ化して表示します。	Files Dashboard	Protection
File Storage by Device	最も多くのファイル データを格納したデバイスを表示します。	Files Dashboard	Malware
File Storage by Disposition	デバイス上に格納されたファイル データのサイズ（KB）を、ファイルの性質に基づいて表示します。	Files Dashboard	Malware
File Storage by Type	デバイス上に格納されたファイル データのサイズ（KB）を、ファイルのタイプに基づいて表示します。	Files Dashboard	Malware
File Storage over Time	ダッシュボードの時間範囲で管理対象のデバイス上に格納されているファイル データのキロバイト数のグラフを表示します。	Files Dashboard	Malware
File Transfers over Time	ダッシュボードの時間範囲で、ネットワーク トラフィック内でシステムによって検出されたファイル転送の合計数のグラフを表示します。	Files Dashboard	Protection
File Types	ネットワークを介して送信されたファイルの数を、ファイルのタイプごとにグループ化して表示します。	Files Dashboard	Protection

表 55-5　Custom Analysis ウィジェットのプリセット（続き）

プリセット	説明	事前定義されたダッシュボード	ライセンス
File Types Infected with Malware	システム、または FireAMP コネクタによってネットワーク トラフィック内で検出されたマルウェアの数を、ファイルのタイプごとにグループ化して表示します。	Files Dashboard	Malware
Files Sent for Dynamic Analysis over Time	ダッシュボードの時間範囲で、動的分析のために送信されたファイルの合計数のグラフを表示します。	Files Dashboard	Malware
Files Stored over Time	ダッシュボードの時間範囲で、管理対象のデバイス上に格納されたファイルの合計数のグラフを表示します。	Files Dashboard	Malware
Hosts Receiving Files	ネットワーク上のホスト IP アドレスで受信した（ダウンロードした）ファイル数を、IP アドレスごとにグループ化して表示します。	Files Dashboard	Protection
Hosts Receiving Malware	ネットワーク上のホスト IP アドレスで受信したマルウェア ファイル数を、IP アドレスごとにグループ化して表示します。	Files Dashboard	Malware ライセンスまたは FireAMP サブスクリプション
Hosts Sending Files	ネットワーク上のホスト IP アドレスから送信した（アップロードした）ファイル数を、IP アドレスごとにグループ化して表示します。	Files Dashboard	Protection
Hosts Sending Malware	ネットワーク上のホスト IP アドレスから送信したマルウェア ファイル数を、IP アドレスごとにグループ化して表示します。	Files Dashboard	Malware
Impact x Events by Application	予想される影響レベルが x（x は数字の 0 ～ 4）のイベントの数を、アプリケーションごとにグループ化して表示します。	Application Statistics	Protection + FireSIGHT
Impact Level x Events by Application Protocol	予想される影響レベルが x（x は数字の 1 ～ 2）のイベントの数を、アプリケーション プロトコルごとにグループ化して表示します。	サマリー ダッシュボード	Protection + FireSIGHT
Impact Level x Events by User	予想される影響レベルが x（x は数字の 0 ～ 4）のイベントの数を、ユーザごとにグループ化して表示します。	Access Controlled User Statistics	Protection + FireSIGHT
Indications of Compromise by Host	トリガーされた侵害の兆候の数を、関連付けられているホスト IP アドレスごとにグループ化して表示します。	サマリー ダッシュボード	FireSIGHT
Intrusion Events Requiring Analysis	分析が必要な侵入イベントの数を、イベントの分類に基づいて表示します。	Detailed Dashboard	Protection + FireSIGHT
Intrusion Events by Destination Continent	侵入イベントの対象となった大陸を、各大陸に関連付けられているイベントの数に基づいて表示します。	サマリー ダッシュボード	FireSIGHT
Intrusion Events by Destination Country	侵入イベントの対象となった国を、各国に関連付けられているイベントの数に基づいて表示します。	サマリー ダッシュボード	FireSIGHT

表 55-5　Custom Analysis ウィジェットのプリセット（続き）

プリセット	説明	事前定義されたダッシュボード	ライセンス
Intrusion Events by Source Continent	侵入イベントが生じた大陸を、各大陸から生じたイベントの数に基づいて表示します。	サマリー ダッシュボード	FireSIGHT
Intrusion Events by Source Country	侵入イベントが生じた国を、各国から生じたイベントの数に基づいて表示します。	サマリー ダッシュボード	FireSIGHT
Intrusion Events to High Criticality Hosts	侵入イベントを、重要度の高いホストで発生している侵入イベントの数に基づいて表示します。	Detailed Dashboard	Protection + FireSIGHT
Malware Intrusions	侵入イベントを、マルウェアを送信している接続で発生している侵入イベントの数に基づいて表示します。	Files Dashboard	Malware
Malware Threats	システム、または FireAMP コネクタによってネットワーク トラフィック内で検出されたマルウェアの脅威の数を、脅威の名前ごとにグループ化して表示します。	Files Dashboard	Malware ライセンスまたは FireAMP サブスクリプション
New Indications of Compromise over Time	ダッシュボードの時間範囲で検出された、侵害の新しい兆候のグラフを表示します。	サマリー ダッシュボード	FireSIGHT
オペレーティング システム	オペレーティング システムを、ネットワーク内の各オペレーティング システムを実行しているホストの数に基づいて表示します。	Detailed Dashboard	FireSIGHT
Possible Zero-Day Malware	ファイルの性質が不明で、脅威スコアが High または Very High のいずれかであり、ゼロディ マルウェアである可能性が高い検出されたファイルを、ファイルが検出された回数に基づいて表示します。	Files Dashboard	Malware
Processes Introducing Malware	FireAMP コネクタによって検出されたマルウェアにアクセスしたシステム プロセス、またはそれらのマルウェアを作成したシステム プロセスを表示します。	Files Dashboard	Malware ライセンスまたは FireAMP サブスクリプション
Risky Applications with Low Business Relevance	アプリケーション リスクのレベルが高く、予想されるビジネス関連性が低い、モニタリング対象のネットワーク上のすべてのアプリケーション接続を表示します。	サマリー ダッシュボード	FireSIGHT
サーバ	サーバを、ホストの数ごとに表示します。	Detailed Dashboard	FireSIGHT
SSL Actions	暗号化されたトラフィックで行われた SSL ルール アクションの数を、頻度に基づいて表示します。	Connection Summary	いずれか
SSL Certificate Status	SSL 暗号化セッションでシステムが検出した証明書ステータスの数を、頻度に基づいて表示します。	Connection Summary	いずれか
SSL Decryption Failure Reasons	システムが SSL 暗号化セッションを正しく復号化できなかった理由の数を、頻度に基づいて表示します。	Connection Summary	いずれか

表 55-5　Custom Analysis ウィジェットのプリセット（続き）

プリセット	説明	事前定義されたダッシュボード	ライセンス
SSL Sessions Decrypted over Time	ダッシュボードの時間範囲で、システムが復号化した SSL 暗号化セッションの数のグラフを表示します。	Connection Summary	いずれか
SSL Sessions Not Decrypted over Time	ダッシュボードの時間範囲で、システムが復号化しなかった SSL 暗号化セッションの数のグラフを表示します。	Connection Summary	いずれか
SSL Sessions with Errors over Time	ダッシュボードの時間範囲で、内部エラーが含まれていることをシステムが検出した SSL 暗号化セッションの数のグラフを表示します。	Connection Summary	いずれか
Threat Detections over Time	ダッシュボードの時間範囲で、ネットワークトラフィックにおいてシステム、または FireAMP コネクタのいずれかによって検出されたマルウェア脅威の合計数のグラフを表示します。	Files Dashboard	Malware ライセンスまたは FireAMP サブスクリプション
Top Attackers	モニタリング対象のネットワーク上の攻撃元のホスト IP アドレスを、リストされた IP アドレスが、イベントの発生元の接続での攻撃者である侵入イベントの数に基づいて表示します。	サマリー ダッシュボード	Protection
Top Client Applications Seen	モニタリング対象のネットワーク上のクライアント アプリケーションを、クライアント アプリケーションによって伝送されたデータの合計（キロバイト）に基づいて表示します。	サマリー ダッシュボード	FireSIGHT
Top Operating Systems Seen	モニタリング対象のネットワーク上のオペレーティング システムを、そのオペレーティング システムを持つネットワーク ホストの数に基づいて表示します。	サマリー ダッシュボード	FireSIGHT
Top Server Applications Seen	モニタリング対象のネットワーク上のサーバ アプリケーションを、サービスを実行しているホストの数に基づいて表示します。	サマリー ダッシュボード	FireSIGHT
Top Targets	モニタリング対象のネットワーク上のホスト IP アドレスを、アドレスがイベントの発生元の接続の対象であった侵入イベントの数に基づいて表示します。	サマリー ダッシュボード	Protection
Top Threats	脅威スコアの分布を、その脅威スコアを持つ格納ファイルの数に基づいて表示します。	Files Dashboard	Malware
Top Web Applications Seen	モニタリング対象のネットワーク上の Web アプリケーションを、クライアント アプリケーションによって伝送されたデータの合計キロバイト数に基づいて表示します。	サマリー ダッシュボード	FireSIGHT

表 55-5　Custom Analysis ウィジェットのプリセット（続き）

プリセット	説明	事前定義されたダッシュボード	ライセンス
Total Events by Application	モニタリング対象のネットワーク上のアプリケーションを、アプリケーションによって生成された侵入イベントの数に基づいて表示します。	Application Statistics	Protection + FireSIGHT
Total Events by Application Protocol	モニタリング対象のネットワーク上のアプリケーション プロトコルを、アプリケーション プロトコルに関連付けられている侵入イベントの数に基づいて表示します。	サマリー ダッシュボード	Protection + FireSIGHT
Total Events by User	モニタリング対象のネットワーク上のユーザを、各ユーザのアクティビティによって生成された侵入イベントの数に基づいて表示します。	サマリー ダッシュボード Access Controlled User Statistics	Protection + FireSIGHT
Traffic by Application	モニタリング対象のネットワーク上のアプリケーションを、ダッシュボードの時間範囲で、モニタリング対象のネットワークにおいてアプリケーションによって伝送されたデータの合計キロバイト数に基づいて表示します。	Application Statistics Connection Summary Detailed Dashboard	FireSIGHT
Traffic by Application Category	モニタリング対象のネットワーク上のアプリケーション カテゴリを、ダッシュボードの時間範囲で、モニタリング対象のネットワークにおいて各カテゴリのアプリケーションによって伝送されたデータの合計キロバイト数に基づいて表示します。	Application Statistics サマリー ダッシュボード	FireSIGHT
Traffic by Application Risk	モニタリング対象のネットワーク上のアプリケーションの予想されるリスク レベルを、ダッシュボードの時間範囲で、モニタリング対象のネットワークにおいて各レベルでアプリケーションによって伝送されたデータの合計キロバイト数に基づいて表示します。	サマリー ダッシュボード	FireSIGHT
Traffic by Business Relevance	モニタリング対象のネットワーク上のアプリケーションの予想されるビジネス関連性レベルを、ダッシュボードの時間範囲で、モニタリング対象のネットワークにおいて各レベルでアプリケーションによって伝送されたデータの合計キロバイト数に基づいて表示します。	サマリー ダッシュボード	FireSIGHT
Traffic by Destination Continent	モニタリング対象のネットワークからアクセスされた大陸を、ダッシュボードの時間範囲で、モニタリング対象のネットワークにおいて各大陸へ伝送されたデータの合計キロバイト数に基づいて表示します。	Connection Summary	FireSIGHT

表 55-5　Custom Analysis ウィジェットのプリセット（続き）

プリセット	説明	事前定義されたダッシュボード	ライセンス
Traffic by Destination Country	モニタリング対象のネットワークからアクセスされた国を、ダッシュボードの時間範囲で、モニタリング対象のネットワークにおいて各国へ伝送されたデータの合計キロバイト数に基づいて表示します。	Connection Summary	FireSIGHT
Traffic by Initiator IP	モニタリング対象のネットワーク上のホスト IP アドレスを、ダッシュボードの時間範囲で、モニタリング対象のネットワークにおいて IP アドレスから伝送されたデータの合計キロバイト数に基づいて表示します。	Connection Summary Detailed Dashboard	FireSIGHT
Traffic by Initiator User	モニタリング対象のネットワーク上のユーザを、ユーザがログインしたホストで受信したデータの合計（キロバイト）に基づいて表示します。	Detailed Dashboard サマリー ダッシュボード	FireSIGHT
Traffic by Port	モニタリング対象のネットワーク上のレスポンダ ポートを、ダッシュボードの時間範囲で、モニタリング対象のネットワークにおいて各ポートを介して伝送されたデータの合計キロバイト数に基づいて表示します。このウィジェットの出力は、接続のロギング設定によって異なります。	Connection Summary	FireSIGHT
Traffic by Responder IP	モニタリング対象のネットワーク上の IP アドレスを、ダッシュボードの時間範囲で、（ホスト上の）IP アドレスによって受信したデータの合計キロバイト数に基づいて表示します。このウィジェットの出力は、接続のロギング設定によって異なります。	Connection Summary Detailed Dashboard	FireSIGHT
Traffic by Security Intelligence Category	モニタリング対象のネットワーク上の Security Intelligence カテゴリを、ダッシュボードの時間範囲で、各カテゴリの接続を介して伝送されたデータの合計キロバイト数に基づいて表示します。	サマリー ダッシュボード	Protection
Traffic by Source Continent	モニタリング対象のネットワークへデータを伝送している大陸を、ダッシュボードの時間範囲で、モニタリング対象のネットワークにおいて各大陸から伝送されたデータの合計キロバイト数に基づいて表示します。	Connection Summary	FireSIGHT
Traffic by Source Country	モニタリング対象のネットワークへデータを伝送している国を、ダッシュボードの時間範囲で、モニタリング対象のネットワークにおいて各国から伝送されたデータの合計キロバイト数に基づいて表示します。	Connection Summary	FireSIGHT

表 55-5　Custom Analysis ウィジェットのプリセット（続き）

プリセット	説明	事前定義されたダッシュボード	ライセンス
Traffic by URL Category	モニタリング対象のネットワーク上のアプリケーション URL カテゴリを、ダッシュボードの時間範囲で、各カテゴリの URL と通信されたデータの合計キロバイト数に基づいて表示します。	URL Statistics	URL Filtering
Traffic by URL Reputation	モニタリング対象のネットワーク上のアプリケーション URL レピュテーション タイプを、ダッシュボードの時間範囲で、各レピュテーションの URL と通信されたデータの合計キロバイト数に基づいて表示します。	URL Statistics	URL Filtering
Traffic by User	モニタリング対象のネットワーク上のユーザを、ダッシュボードの時間範囲で、各ユーザと通信されたデータの合計キロバイト数に基づいて表示します。	なし	FireSIGHT
Traffic over Time	ダッシュボードの時間範囲で、モニタリング対象のネットワークで伝送されたデータの合計キロバイト数のグラフを表示します。	Connection Summary Detailed Dashboard	FireSIGHT
Unique Applications over Time	ダッシュボードの時間範囲で、モニタリング対象のネットワークで検出された一意のアプリケーションの合計のグラフを表示します。	Application Statistics サマリー ダッシュボード	FireSIGHT
Unique Users over Time	ダッシュボードの時間範囲で、モニタリング対象のネットワークで検出された一意のユーザの合計のグラフを表示します。	Access Controlled User Statistics	FireSIGHT
Users Affected by Malware	システム、または FireAMP コネクタによってネットワーク トラフィック内で検出された脅威の数を、ユーザごとにグループ化して表示します。	Files Dashboard	Malware + FireSIGHT、または FireAMP サブスクリプション
Users Transferring Files	ネットワークを介して伝送されているファイルの数を、送信者ごとにグループ化して表示します。	Files Dashboard	Malware + FireSIGHT
Web Applications Introducing Malware	モニタリング対象のネットワーク上の Web アプリケーション（FireAMP コネクタで検出されたマルウェアにアクセスしたアプリケーション、またはこのようなマルウェアを作成したアプリケーション）を表示します。	Files Dashboard	Malware ライセンスまたは FireAMP サブスクリプション
Web Applications Transferring Files	ネットワークを介して送信されたファイルの数を、ファイルの送信に使用された Web アプリケーションごとにグループ化して表示します。	Files Dashboard	Malware ライセンスまたは FireAMP サブスクリプション
White List Violations	ホワイト リスト違反のホストを、違反件数ごとに表示します。	Detailed Dashboard	FireSIGHT

Custom Analysis ウィジェットから関連付けられているイベントを表示する

ライセンス：すべて

Custom Analysis ウィジェットで表示されるように設定しているデータの種類によっては、イベント ビュー（つまりワークフロー）を起動することができます。イベント ビューは、ウィジェットに表示されるイベントの詳細情報を提供します。

ダッシュボードからイベント ビューを起動すると、対象のイベント タイプについてのデフォルト ワークフローにイベントが表示されますが、これはダッシュボードの時間範囲による制約を受けます。また、設定した期間の数、および表示するイベントのタイプによっても、アプライアンスに対する適切な期間が変更されます。

たとえば、Defense Centerに複数の期間が設定されており、Custom Analysis ウィジェットから正常性イベントにアクセスすると、デフォルトの正常性イベント ワークフローにイベントが表示され、正常性のモニタリング期間はダッシュボードの時間範囲に変更されます。

もうひとつの例として、1 つの期間を設定していて Custom Analysis ウィジェットから任意のタイプのイベントにアクセスすると、イベントはそのイベント タイプのデフォルト ワークフローに表示され、グローバル期間がダッシュボードの時間範囲に変更されます。

期間の詳細については、デフォルトの時間枠（71-6 ページ）および検索での時間制約の指定（60-5 ページ）を参照してください。

Custom Analysis ウィジェットから関連付けられているイベントを表示する方法：

アクセス：Admin/Any Security Analyst/Maint

ステップ 1　ウィジェットをどのように設定したかによって、次の 2 つのオプションがあります。

- イベントの相対的な発生数を表示するように設定されたウィジェット（つまり棒グラフ）で、任意のイベントをクリックして、そのイベント、およびウィジェットのプリファレンスによる制約を受ける関連イベントを表示します。また、ウィジェットの右下にあるすべて表示のアイコン（  ）をクリックして、ウィジェットのプリファレンスによる制約を受けるすべての関連イベントを表示することもできます。
- 一定期間の接続データを表示するよう設定されているウィジェットで、ウィジェットの右下にあるすべて表示のアイコンをクリックして、ウィジェットのプリファレンスによる制約を受けるすべての関連イベントを表示します。

特定のイベント タイプの操作については、以下の項を参照してください。

- セキュリティ インテリジェンス リストとフィードの操作（3-5 ページ）
- 監査レコードの表示（69-2 ページ）
- 侵入イベントの表示（41-9 ページ）
- ディスカバリ イベントおよびホスト入力イベントの表示（50-16 ページ）
- ファイル イベントの表示（40-9 ページ）
- マルウェア イベントの表示（40-20 ページ）
- キャプチャ ファイルの表示（40-32 ページ）
- ホストの表示（50-21 ページ）
- ホスト属性の表示（50-30 ページ）
- 侵害の痕跡の表示（50-35 ページ）
- サーバの表示（50-40 ページ）
- アプリケーションの詳細の表示（50-50 ページ）

- 脆弱性の表示（50-54 ページ）
- サードパーティの脆弱性の表示（50-60 ページ）
- 接続およびセキュリティ インテリジェンスのデータの表示（39-15 ページ）
- ユーザの表示（50-65 ページ）
- ユーザ アクティビティ イベントの表示（50-72 ページ）
- 相関イベントの表示（51-56 ページ）
- ホワイト リスト イベントの表示（52-33 ページ）
- ホワイト リスト違反の表示（52-38 ページ）
- ヘルス イベントの表示（68-53 ページ）
- ルール更新ログの表示（66-24 ページ）
- アクティブ スキャンの結果での作業（47-21 ページ）
- 地理情報の使用（58-23 ページ）
- カスタム テーブルについて（59-1 ページ）

Custom Analysis ウィジェットの制限

ライセンス： すべて

Custom Analysis ウィジェットを使用する場合に、留意すべきいくつかの重要な点があります。

共有ダッシュボード上でウィジェットを設定する場合は、ユーザのアカウント権限によって、すべてのユーザがすべてのイベント タイプのデータを表示できるわけではないことに注意してください。たとえば、Maintenance Users は検出イベントを表示できません。

同様に、別のアプライアンスからインポートされたダッシュボードを使用している場合は、すべてのアプライアンスがすべてのイベント タイプのデータにアクセスできるわけではないことに注意してください。たとえば、管理対象のデバイスに相関データは格納されません。ダッシュボードに、ユーザが表示できないデータを表示する Custom Analysis ウィジェットが含まれている場合、ウィジェットに、そのユーザにデータの表示権限がないことが示されます。ただし、そのユーザ（およびダッシュボードを共有している他のユーザ）は、ウィジェットのプリファレンスを変更して、自分が表示できるデータを表示することも、ウィジェットを削除することもできることに注意してください。これを防ぐには、ダッシュボードをプライベート（非公開）で保存します。

ユーザがアクセスできる検索は、プライベートで保存した検索だけです。共有ダッシュボード上にウィジェットを設定し、プライベートの検索を使用してイベントを制約すると、ウィジェットは、他のユーザがログインしたときにその検索を使用しないようにリセットされます。ウィジェットのビューにも影響します。これを防ぐには、ダッシュボードをプライベート（非公開）で保存します。

Custom Analysis ウィジェットは、システム ポリシーの [Dashboard] 設定から有効または無効にします。詳細については、ダッシュボードの設定（63-15 ページ）を参照してください。

Disk Usage ウィジェットについて

ライセンス：すべて

Disk Usage ウィジェットは、ディスク使用率のカテゴリに基づいて、ハード ドライブで使用される領域のパーセンテージを表示します。また、アプライアンスのハード ドライブの各パーティションで使用される領域のパーセンテージおよび容量も示します。Disk Usage ウィジェットがデバイスにインストールされている場合、またはDefense Centerが、マルウェア ストレージ パックが含まれているデバイスを管理している場合は、Disk Usage ウィジェットはマルウェア ストレージ パックについて同じ情報を表示します。このウィジェットは、Default Dashboard および Summary Dashboard の [Status] タブにデフォルトで表示されます。

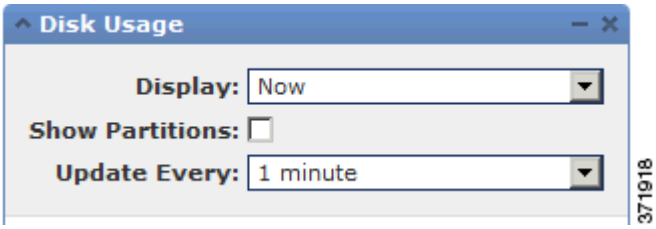
By Category スタック バーは、各ディスク使用率のカテゴリを、使用可能な合計ディスク領域に対する使用量の割合として表示します。次の表で、使用可能なカテゴリについて説明します。

表 55-6　Disk Usage のカテゴリ

Disk Usage のカテゴリ	説明
Event	システムで記録されたすべてのイベント
ファイル	システムに格納されたすべてのファイル
バックアップ	すべてのバックアップ ファイル
Updates	ルールのアップデートやシステムのアップデートなど、アップデートに関連するすべてのファイル
Other	システムのトラブルシューティング ファイルおよびその他のファイル
Free	アプライアンス上の残りの空き領域

By Category スタック バーのディスク使用率カテゴリにポインタを合わせると、使用可能なディスク領域のうち、そのカテゴリで使用された領域の割合、ディスク上の実際のストレージ領域、およびそのカテゴリで使用可能なディスク領域の合計を表示することができます。マルウェア ストレージ パックがインストールされている場合は、Files カテゴリで使用できるディスク領域の合計は、マルウェア ストレージ パックで使用できるディスク領域になることに注意してください。詳細については、キャプチャ ファイル ストレージについて（40-3 ページ）を参照してください。

マルウェア ストレージ パックがインストールされている場合は、ウィジェットのプリファレンスを変更して、By Category スタック バーのみを表示したり、スタック バーと admin（/）、`/Volume`、および `/boot` パーティションの使用率、および `/var/storage` パーティションを表示したりするようにウィジェットを設定できます。



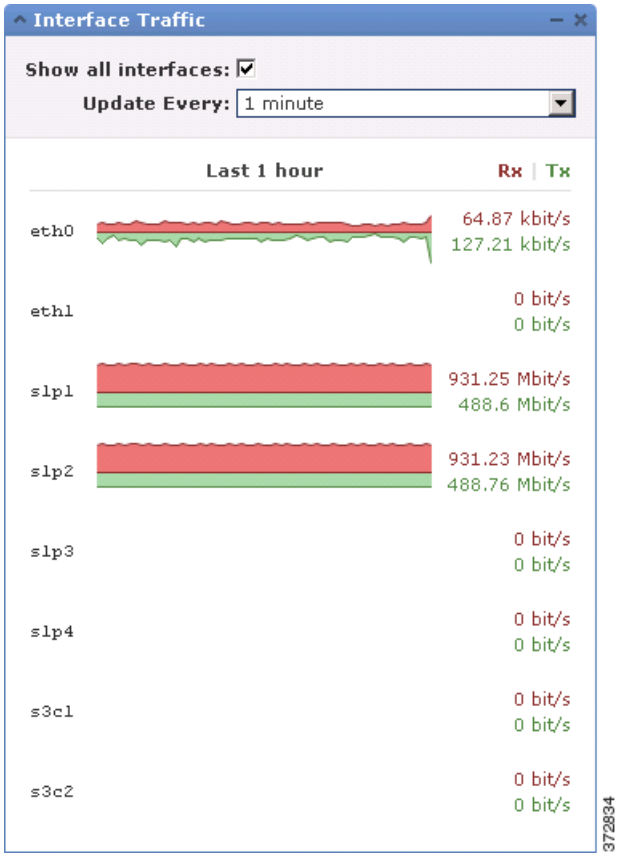
ウィジェットのプリファレンスは、ウィジェットのアップデート頻度、およびダッシュボードの時間範囲で現在のディスク使用率または収集したディスク使用率の統計のいずれかを表示するかも制御します。詳細については、ウィジェットのプリファレンスについて（55-7 ページ）を参照してください。

インターフェイス トラフィック ウィジェットについて

ライセンス： すべて

Interface Traffic ウィジェットは、ダッシュボードの時間範囲において、アプライアンスの管理（`eth0` など）インターフェイスおよびセンシング（`s1p1` など）インターフェイス上で受信した（Rx）トラフィックおよび送信した（Tx）トラフィックの割合を示します。これは、事前定義されたどのダッシュボードにおいてもデフォルトでは表示されません。

アウトバウンド（送信）トラフィックには、フロー制御パケットが含まれます。このため、アプライアンス上のパッシブ インターフェイスは送信トラフィックを示し、イベントを生成する場合があります。これは予期された動作です。動的解析を設定していない場合でも、Malware ライセンスが有効になっているデバイスは Cisco クラウドへの接続を定期的に試行することにも注意してください。このため、これらのデバイスは送信トラフィックを示します。これもまた予期された動作です。

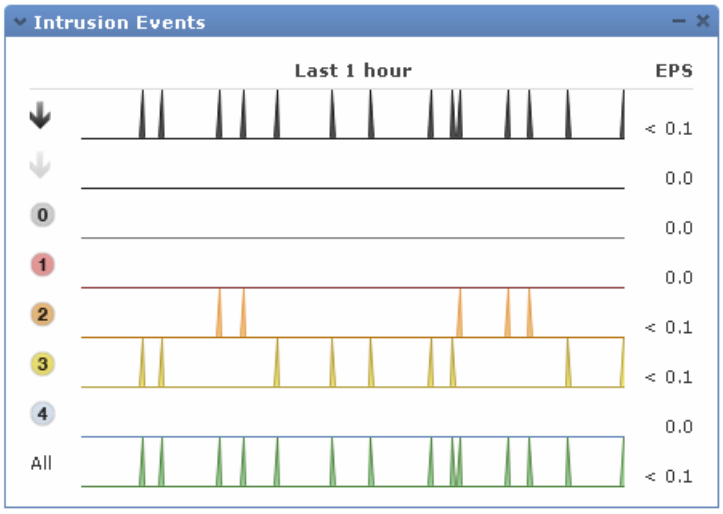


ウィジェットのプリファレンスでは、ウィジェットをアップデートする頻度を調整します。管理対象デバイスでは、プリファレンスは、使用されていないインターフェイスのトラフィック レートをウィジェットに表示するかどうかも制御します(デフォルトでは、ウィジェットにはアクティブなインターフェイスのトラフィック レートのみが表示されます)。詳細については、ウィジェットのプリファレンスについて(55-7 ページ)を参照してください。

Intrusion Events ウィジェットについて

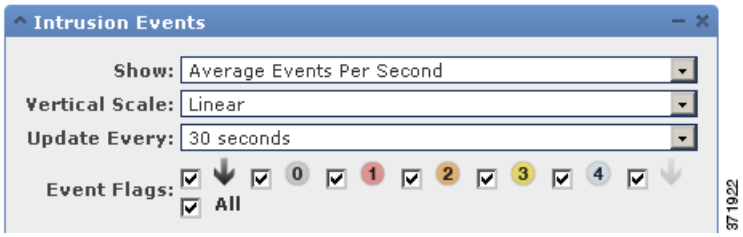
ライセンス: Protection

Intrusion Events ウィジェットは、ダッシュボードの時間範囲で発生した侵入イベントを、優先度ごとに表示します。これには、ドロップされたパケットおよびさまざまな影響を含む、侵入イベントの統計が含まれています。このウィジェットは、Summary Dashboard の [Intrusion Events] タブにデフォルトで表示されます。



管理対象デバイスで、このウィジェットは、ドロップされた（つまり、パッシブに配置されたデバイスではドロップされたと考えられる）侵入イベント、すべての侵入イベント、またはその両方の統計を表示できます。ローカル イベント ストレージを有効にしなければならないことに注意してください。有効にしないと、ウィジェットには表示するデータがありません。[All] で示される合計の割合には、ドロップされたイベントの割合は含まれないことにも注意してください。

管理対象のデバイスではなく、Defense Center では、ウィジェットのプリファレンスを変更して、ドロップされた（またはドロップされたと考えられる）パケットを持つ侵入イベント、およびさまざまな影響を表示するようにウィジェットを設定することができます。Defense Center、NO MDC THIS TIMEおよびデバイス上でドロップされたイベント、およびドロップされたと考えられるイベントを表示することができます。次の図は、ウィジェットのプリファレンスの Defense Center バージョンを示しています。



ウィジェットのプリファレンスでは、次のことができます。

- Defense Center で、1 つ以上の [Event Flags] チェック ボックスをオンにして、ドロップされたパケット、ドロップされたと考えられるパケット、または特定の影響を持つイベントを別のグラフで表示することができます。影響やルールの状態に関係なくすべての侵入イベントについて別のグラフを表示する場合は、[All] を選択します。詳細については、影響レベルを使用してイベントを評価する（41-39 ページ）を参照してください。
- [Show] を選択して、[Average Events Per Second] または [Total Events] を選択します。
- [Vertical Scale] を選択して、[Linear]（増分）または [Logarithmic]（10 の倍数）のスケールを選択できます。

プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。詳細については、ウィジェットのプリファレンスについて（55-7 ページ）を参照してください。

Intrusion Events ウィジェットでは、次のことができます。

- Defense Center で、ドロップされたパケット、ドロップされたと考えられるパケット、または特定の影響に対応するグラフをクリックして、そのタイプの侵入イベントを表示します
- ドロップされたイベントに対応するグラフをクリックして、ドロップされたイベントを表示します
- ドロップされたと考えられるイベントに対応するグラフをクリックして、ドロップされたと考えられるイベントを表示します
- [All] グラフをクリックして、すべての侵入イベントを表示します。

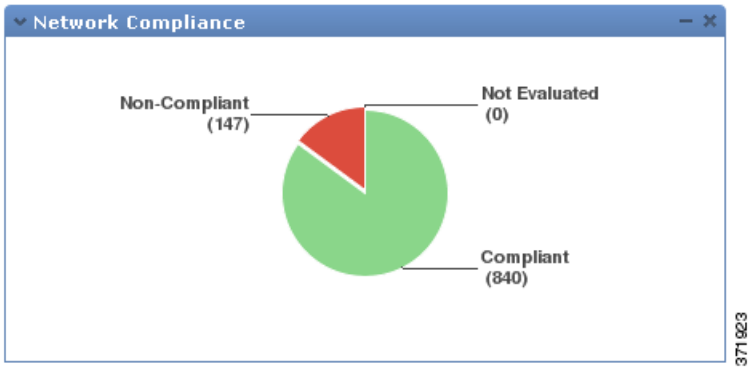
結果のイベント ビューは、ダッシュボードの時間範囲に制約されることに注意してください。ダッシュボードを介して侵入イベントにアクセスすると、そのアプライアンスに対するイベント（またはグローバル）の期間が変わります。侵入イベントの詳細については、侵入イベントの表示（41-9 ページ）を参照してください。

ルールの状態、または侵入ポリシーのインライン ドロップ動作に関係なく、パッシブな配置のパケットはドロップされないことに注意してください。

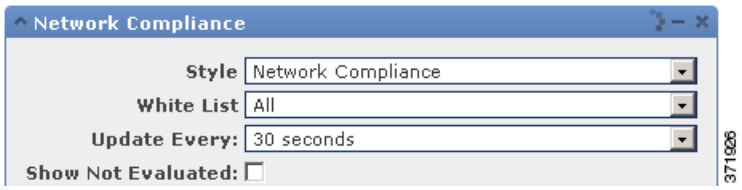
Network Compliance ウィジェットについて

ライセンス：FireSIGHT

Network Compliance ウィジェットは、ユーザが設定したホワイト リストに対するホストのコンプライアンスを要約します（FireSIGHT システムのコンプライアンス ツールとしての使用（52-1 ページ）を参照してください）。デフォルトでは、このウィジェットにアクティブな相関ポリシーにおけるすべてのコンプライアンス ホワイト リストに対して準拠しているホスト、準拠していないホスト、および評価されなかったホストの数を示す円グラフが表示されます。このウィジェットは、Detailed Dashboard の [Correlation] タブにデフォルトで表示されます。



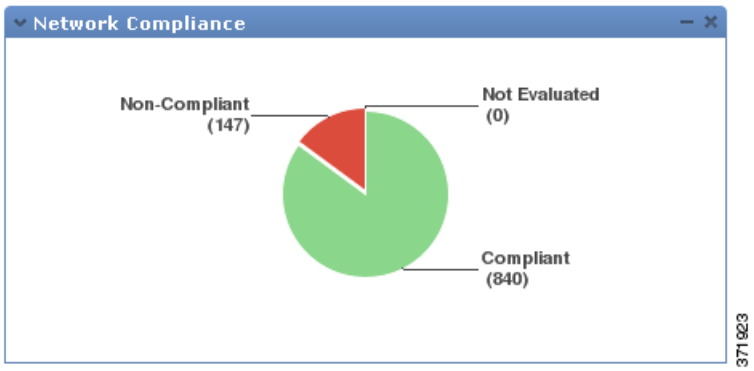
ウィジェットのプリファレンスを変更して、すべてのホワイト リスト、または特定のホワイト リストのいずれかについてネットワーク コンプライアンスを表示するようにウィジェットを設定できます。



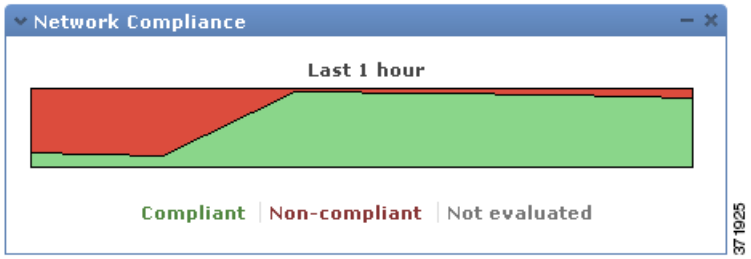
すべてのホワイト リストに対してネットワーク コンプライアンスを表示するよう選択すると、あるホストが、アクティブな相関ポリシーのいずれのホワイト リストにも準拠していない場合、ウィジェットはそのホストが非準拠であるとみなします。

また、このウィジェットのプリファレンスを使用すると、ネットワーク コンプライアンスの表示で次の 3 つのスタイルのうちどれを使用するかを指定することができます。

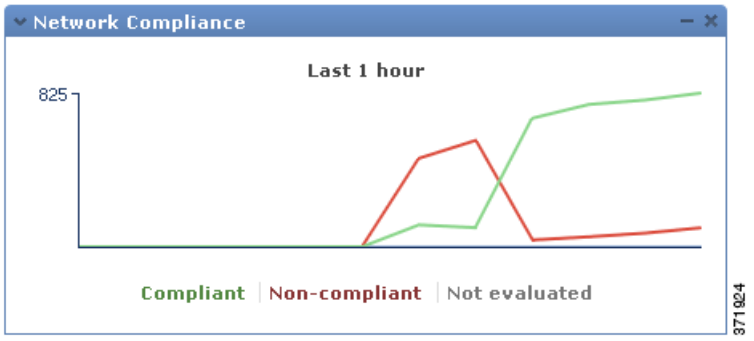
[Network Compliance] スタイル（デフォルト）は、準拠しているホスト、準拠していないホスト、および評価されなかったホストの数を示す円グラフを表示します。ホストの違反の件数を表示するには、円グラフをクリックします。このようにすると、少なくとも 1 つのホワイト リストに違反しているホストが表示されます。詳細については、ホワイト リスト違反の表示（52-38 ページ）を参照してください。



[Network Compliance over Time (%)] スタイルは、ダッシュボードの時間範囲において準拠しているホスト、準拠していないホスト、およびまだ評価されていないホストの相対的な割合を示す積み重ね面積グラフを表示します。



[Network Compliance over Time] スタイルは、ダッシュボードの時間範囲において準拠しているホスト、準拠していないホスト、およびまだ評価されていないホストの数を示す折れ線グラフを表示します。

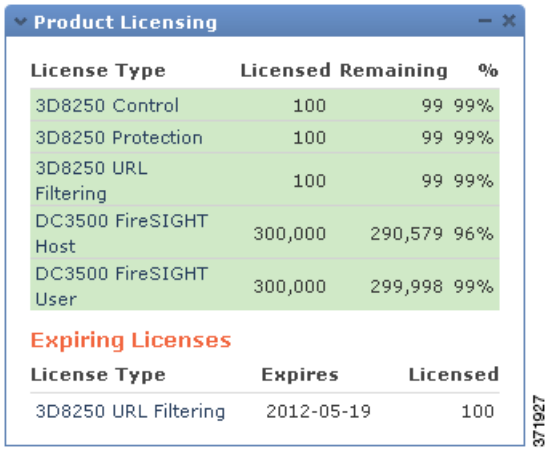


プリファレンスは、ウィジェットをアップデートする頻度を調整します。まだ評価されていないイベントを非表示にするには、[Show Not Evaluated] ボックスを選択します。詳細については、ウィジェットのプリファレンスについて（55-7 ページ）を参照してください。

Product Licensing ウィジェットについて

ライセンス：すべて

Product Licensing ウィジェットは、Defense Centerに現在インストールされているデバイスおよび機能のライセンスを示します。また、ライセンス契約されているアイテム（ホストやユーザ）の数、許可される残りのライセンス契約アイテム数も示します。これは、事前定義されたどのダッシュボードにおいてもデフォルトでは表示されません。



このウィジェットの上部のセクションには、一時的なライセンスも含めて、Defense Centerにインストールされているすべてのデバイスおよび機能のライセンスが表示されますが、[Expiring Licenses] セクションには、一時的なライセンスおよび期限の切れたライセンスのみが表示されます。たとえば FireSIGHT Host に対して 2 つの機能ライセンスを持っており、1 つは永久ライセンスで 750 台のホストが使用可能で、もうひとつは一時ライセンスで追加の 750 台のホストが使用可能であるとします。この場合、ウィジェットの上部のセクションには、ライセンス契約された 1500 台のホストの FireSIGHT Host 機能ライセンスが表示されますが、[Expiring Licenses] セクションには、750 台のホストの FireSIGHT Host 機能ライセンスが表示されます。

ウィジェットの背景のバーは、使用中のライセンスのそれぞれのタイプの割合を示しています。このバーは右から左へ読みます。期限の切れたライセンスには、取り消し線が付けられています。

ウィジェットのプリファレンスを変更して、現在ライセンス契約されている機能を表示するか、またはライセンス契約が可能なすべての機能を表示するようにウィジェットを設定することができます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。詳細については、ウィジェットのプリファレンスについて（55-7 ページ）を参照してください。

任意のライセンス タイプをクリックすると、ローカル設定の [License] ページに移動して、機能ライセンスを追加または削除することができます。詳細については、FireSIGHT システムのライセンス（65-1 ページ）を参照してください。

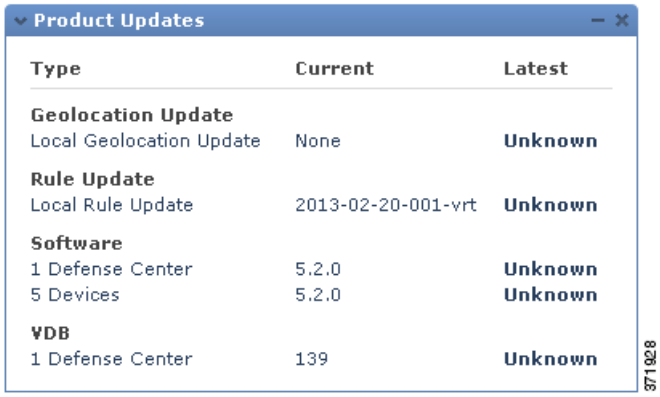
Product Updates ウィジェットについて

ライセンス：すべて

Product Updates ウィジェットは、アプライアンスに現在インストールされているソフトウェア（FireSIGHT システム ソフトウェアおよびルール アップデート）の概要、およびそのソフトウェアについてダウンロードしたが、まだインストールしていないアップデートの情報を提供します。このウィジェットは、Detailed Dashboard および Summary Dashboard の [Status] タブにデフォルトで表示されます。

このウィジェットは、ユーザがソフトウェアのアップデートをダウンロード、プッシュ、またはインストールするスケジュールされたタスクを設定していない場合、ソフトウェアの最新バージョンを [Unknown] と表示します。ウィジェットではスケジュールされたタスクを使用して、最新のバージョンを決定するためです。詳細については、タスクのスケジュール（62-1 ページ）を参照してください。

ウィジェットは、ソフトウェアをアップデートできるページへのリンクも提供します。ウィジェットの Defense Center バージョンには類似のリンクがあり、このリンクを使用して管理対象のデバイスでソフトウェアをアップデートすることができます。



ウィジェットのプリファレンスを変更して、最新のバージョンを非表示にするようウィジェットを設定できます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。詳細については、ウィジェットのプリファレンスについて（55-7 ページ）を参照してください。

Product Updates ウィジェットでは、次のことができます。

- FireSIGHT システム ソフトウェア、ルール アップデート、地理情報のアップデート、または VDB の最新バージョンをクリックして、アプライアンスを手動でアップデートします。
- システム ソフトウェア、地理情報データベース、または VDB をアップデートするには、システムソフトウェアの更新（66-1 ページ）を参照してください。
- 最新のルール アップデートをインポートするには、ルールの更新とローカル ルール ファイルのインポート（66-16 ページ）を参照してください。
- 最新バージョンをクリックするか、または [Latest] カラムの [Unknown] リンクをクリックして、FireSIGHT システム ソフトウェア、ルール アップデート、または VDB の最新バージョンをダウンロードするためのスケジュールされたタスクを作成します。タスクのスケジュール（62-1 ページ）を参照してください。

RSS Feed ウィジェットについて

ライセンス：すべて

RSS Feed ウィジェットは、ダッシュボードに RSS フィードを追加します。デフォルトでは、ウィジェットは Cisco セキュリティ ニュースのフィードを示します。このウィジェットは、Detailed Dashboard および Summary Dashboard の [Status] タブにデフォルトで表示されます。

また、企業ニュース、Snort.org ブログ、または脆弱性調査チーム（VRT）ブログの事前設定済みのフィードを表示するようウィジェットを設定することができます。ウィジェットのプリファレンス内に URL を指定して、他の RSS フィードに対するカスタム接続を作成することもできます。

フィードは 24 時間ごとにアップデートされます（ただしユーザはフィードを手動でアップデートできます）。また、ウィジェットはアプライアンスのローカル時間に基づいて、フィードが最後にアップデートされた時間を表示します。アプライアンスは、（事前設定された 2 つのフィードについて）Web サイトに対するアクセス権を持っている、または設定したいずれかのカスタムフィードに対するアクセス権を持っている必要があります。

ウィジェットを設定する場合には、フィードからいくつのストーリーをウィジェットに表示するか、およびヘッドラインとともにストーリーの説明を表示するかどうかを選択することができます。ただしすべての RSS フィードで説明が使用できるわけではないことに注意してください。

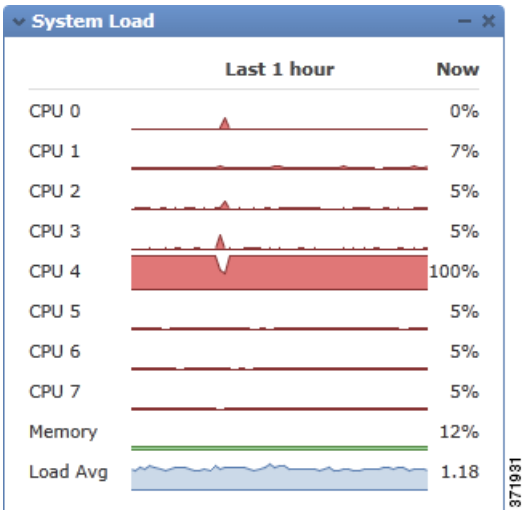
RSS Feed ウィジェットでは、次のことができます。

- フィード内のストーリーのいずれかをクリックして、ストーリーを表示します
- [more] リンクをクリックして、フィードの Web サイトへ移動します
- アップデート アイコン（）をクリックして、フィードを手動でアップデートします

System Load ウィジェットについて

ライセンス：すべて

System Load ウィジェットは、アプライアンス上の（各 CPU についての）CPU の使用率、メモリ（RAM）の使用率、およびシステムの負荷（実行を待機しているプロセスの数によって測定され、負荷平均とも呼ばれる）を現在、およびダッシュボードの時間範囲について表示します。このウィジェットは、Detailed Dashboard および Summary Dashboard の [Status] タブにデフォルトで表示されます。



ウィジェットのプリファレンスを変更して、負荷平均を表示または非表示にするようウィジェットを設定できます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。詳細については、ウィジェットのプリファレンスについて（55-7 ページ）を参照してください。

System Time ウィジェットについて

ライセンス：すべて

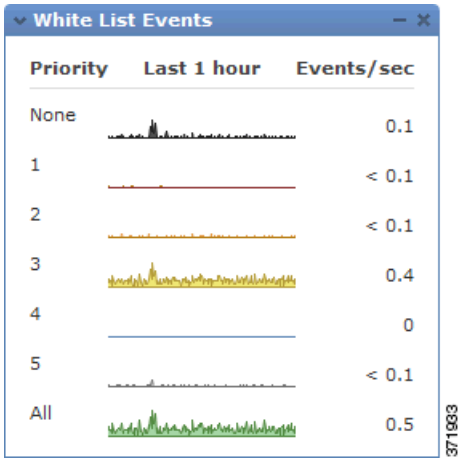
System Time ウィジェットは、アプライアンスのローカル システム時間、稼動時間、およびブート時間を表示します。このウィジェットは、Detailed Dashboard および Summary Dashboard の [Status] タブにデフォルトで表示されます。

ウィジェットのプリファレンスを変更して、ブート時間を非表示にするようウィジェットを設定できます。プリファレンスは、ウィジェットがアプライアンスの時計と同期する頻度も調整します。詳細については、ウィジェットのプリファレンスについて（55-7 ページ）を参照してください。

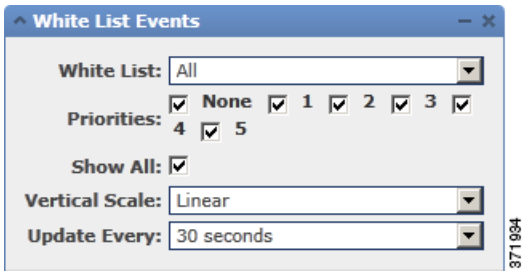
White List Events ウィジェットについて

ライセンス：FireSIGHT

White List Events ウィジェットは、ダッシュボードの時間範囲における 1 秒あたりの平均イベント数を、優先度ごとに表示します。このウィジェットは、Default Dashboard の [Correlation] タブにデフォルトで表示されます。



ウィジェットのプリファレンスを変更して、さまざまな優先度のホワイト リスト イベントを表示するようウィジェットを設定できます。



ウィジェットのプリファレンスでは、次のことができます。

- 優先度を持たないイベントも含めて、特定の優先度のイベントに対して別のグラフを表示するには、1 つ以上の [Priorities] チェック ボックスをオンにします。
- 優先度に関係なくすべてのホワイト リスト イベントに対して追加のグラフを表示するには、[Show All] を選択します。
- [Vertical Scale] を選択して、[Linear]（増分）または [Logarithmic]（10 の倍数）のスケールを選択できます。

プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。詳細については、ウィジェットのプリファレンスについて（55-7 ページ）を参照してください。

グラフをクリックして特定の優先度のホワイト リスト イベントを表示することも、[All] グラフをクリックしてすべてのホワイト リスト イベントを表示することもできます。いずれの場合も、イベントは、ダッシュボードの時間範囲に制約されます。ダッシュボードを介してホワイト リスト イベントにアクセスすると、Defense Centerに対するイベント（またはグローバル）の期間が変わります。ホワイト リスト イベントの詳細については、ホワイト リスト イベントの表示（52-33 ページ）を参照してください。

ダッシュボードの操作

ライセンス： すべて

ダッシュボードに示されるウィジェットを表示および変更できます。

[Dashboard Management] ページでダッシュボードを管理します（ダッシュボードの表示（55-42 ページ）を参照してください）。ダッシュボードを作成、表示、変更、エクスポート、および削除できます。

各ダッシュボードでは、ページに所有者（ダッシュボードを作成したユーザ）が表示され、ダッシュボードがプライベートかどうかも示されます。Administrator 権限を持っていない場合は、自分のプライベート ダッシュボードのみを表示できます。他のユーザが作成したプライベート ダッシュボードを表示または変更することはできません。

最後に、ページには、どのダッシュボードがデフォルトかが示されます。ユーザのプリファレンスでデフォルトのダッシュボードを指定します。詳細については、デフォルトのダッシュボードの指定（71-9 ページ）を参照してください。

ダッシュボードの詳細については、以下を参照してください。

- カスタム ダッシュボードの作成（55-40 ページ）
- ダッシュボードの表示（55-42 ページ）
- ダッシュボードの変更（55-44 ページ）
- ダッシュボードの削除（55-48 ページ）
- 設定のエクスポート（A-1 ページ）

カスタム ダッシュボードの作成

ライセンス： すべて

新しいダッシュボードを作成する場合は、ユーザが作成した、または Cisco で事前定義されている既存のダッシュボードをベースとして使用するよう選択できます。この場合は、既存のダッシュボードのコピーが作成されます。ユーザは自身のニーズに合わせてコピーを変更できます。また、既存のダッシュボードをベースとして使用せずに、新しい空のダッシュボードを作成することもできます。

また、タブの変更間隔およびページの更新間隔を指定する（または無効にする）必要があります。これらの設定は、ダッシュボードがタブを自動変更する頻度、およびダッシュボード全体のページを更新する頻度を定義します。

ダッシュボード全体を更新すると、共有のダッシュボードに対して他のユーザが行ったプリファレンスまたはレイアウトの変更や、他のコンピュータ上のプライベート ダッシュボードに対して、ダッシュボードが最後に更新された後で自分が行った変更を確認できます。これは、ダッシュボードが常に表示されているネットワーク オペレーション センター（NOC）などで有用です。ダッシュボードを変更する場合には、ローカル コンピュータで変更を行うことができます。この場合、NOC のダッシュボードは、ユーザが指定した間隔で自動的に更新され、NOC のダッシュボードを手動で更新しなくても変更が表示されます。データのアップデートを確認するためにダッシュボード全体を更新する必要はありません。個々のウィジェットはプリファレンスに従ってアップデートされます。

最後に、新しいダッシュボードをプライベート ダッシュボードとして保存して、そのダッシュボードをユーザ アカウントに関連付けることができます。ダッシュボードをプライベートとして保存しない場合、アプライアンスの他のすべてのユーザがダッシュボードを表示できるようになります。

すべてのユーザ ロールがすべてのダッシュボード ウィジェットに対してアクセス権を持っているわけではないため、多くの権限を持つユーザが作成したダッシュボードを、それよりも少ない権限を持つユーザが参照する場合、ダッシュボードのすべてのウィジェットを使用できないことがあることに注意してください。ダッシュボード上に、許可されていないウィジェットが表示されることがありますが、これらのウィジェットは無効です。

また、ロールに関係なく、ダッシュボードへアクセスできるすべてのユーザが共有ダッシュボードを変更できることにも注意してください。特定のダッシュボードを自分のみが変更できるようにするには、そのダッシュボードをプライベートとして保存します。

ヒント　新しいダッシュボードを作成する代わりに、別のアプライアンスからダッシュボードをエクスポートし、それを自分のアプライアンスへインポートすることができます。その後でニーズに合わせて、インポートしたダッシュボードを編集することができます。自分が表示できるダッシュボードは、使用しているアプライアンスのタイプ、および自分のユーザ ロールによって異なることに注意してください。たとえば、Defense Center で作成され、管理対象のデバイスにインポートされたダッシュボードには、無効なウィジェットが表示されることがあります。詳細については、設定のインポートおよびエクスポート (A-1 ページ)を参照してください。

新しいダッシュボードを作成するには、次のようにします。

アクセス: Admin/Any Security Analyst/Maint

ステップ 1　[Overview] > [Dashboards] > [Management] を選択します。

[Dashboard Management] ページが表示されます。

ステップ 2　[Create Dashboard] をクリックします。

[Create Dashboard] ページが表示されます。

ステップ 3　[Copy Dashboard] ドロップダウンリストを使用して、新しいダッシュボードのベースとして使用するダッシュボードを選択します。

事前定義のダッシュボードまたはユーザ定義のダッシュボードを選択できます。オプションとして、[None] (デフォルト) を選択して、空のダッシュボードを作成することもできます。

ステップ 4　ダッシュボードの名前と説明 (オプション) を入力します。

ステップ 5　[Change Tabs Every] フィールドで、ダッシュボードでタブを変更する頻度 (分単位) を指定します。

ダッシュボードを一時停止した場合や、ダッシュボードのタブが 1 つのみの場合を除き、この設定により、指定した間隔で次のタブが表示されます。タブの自動変更を無効にするには、[Change Tabs Every] フィールドに 0 を入力します。

ステップ 6　[Refresh Page Every] フィールドで、現在のダッシュボード タブを新しいデータで更新する頻度を (分単位で) 指定します。この値は、[Change Tabs Every] の設定より大きい値にする必要があります。

ダッシュボードを一時停止しない限り、この設定より、指定した間隔でダッシュボード全体が更新されます。定期的なページ更新を無効にするには、[Refresh Page Every] フィールドに 0 を入力します。

この設定は、個々のウィジェットの多くで使用可能なアップデート間隔とは異なることに注意してください。ダッシュボードのページを更新すると個々のウィジェットのアップデート間隔はリセットされますが、[Refresh Page Every] 設定を無効にしていても、ウィジェットはそれ自身のプリファレンスに従ってアップデートされます。

ステップ 7　オプションで、ダッシュボードを自分のユーザ アカウントと関連付けて、他のユーザがダッシュボードを表示および変更できないようにするために、[Save As Private] チェック ボックスをオンにします。

ステップ 8　[Save] をクリックします。

ダッシュボードが作成され、Web インターフェイスに表示されます。これで、タブやウィジェットを追加して（既存のダッシュボードをベースにしている場合は、ウィジェットを再配置および削除して）、ニーズに合わせてダッシュボードを調整できるようになりました。詳細については、ダッシュボードの変更（55-44 ページ）を参照してください。

ダッシュボードの表示

ライセンス： すべて

デフォルトでは、アプライアンスのホーム ページにデフォルトのダッシュボードが表示されます。デフォルトのダッシュボードを定義していない場合は、ホーム ページに [Dashboard Management] ページが示され、ここで表示するダッシュボードを選択できます。いつでも、[Overview] > [Dashboards] を選択して、アプライアンスに対して設定したデフォルトのダッシュボードを表示できます。使用可能なすべてのダッシュボードの詳細を表示する場合は、[Overview] > [Dashboards] > [Management] を選択します。

ヒント　ダッシュボード ページではないページを含む、別のデフォルト ホーム ページを表示するようにアプライアンスを設定できます。デフォルトのダッシュボードを変更することもできます。詳細については、ホーム ページの指定（71-3 ページ）およびデフォルトのダッシュボードの指定（71-9 ページ）を参照してください。

各ダッシュボードには、ウィジェットを制約する時間範囲があります。最短で 1 時間前（デフォルト）から、最長では 1 年前からの期間を反映するように時間範囲を変更できます。時間範囲を変更する場合は、時間によって制約される可能性のあるウィジェットが自動でアップデートされ、新しい時間範囲が反映されます。

すべてのウィジェットを時間で制約できるわけではないことに注意してください。たとえば、ダッシュボードの時間範囲は Appliance Information ウィジェットには影響を与えません。このウィジェットは、アプライアンスの名前、モデル、および FireSIGHT システム ソフトウェアの現在のバージョンが含まれている情報を提供します。

企業による FireSIGHT システムの展開では、新しいイベントが古いイベントを置き換える頻度によっては、時間範囲を長期に変更しても、Custom Analysis ウィジェットなどのウィジェットでは役立たない場合があることに注意してください。

ダッシュボードを一時停止することもできます。これにより変更を表示したり、分析を中断したりせずに、ウィジェットで提供されたデータを調べることができます。ダッシュボードを一時停止すると、次のような影響があります。

- Update Every ウィジェットのプリファレンスに関係なく、個々のウィジェットでアップデートが停止します。
- ダッシュボードのプロパティの [Cycle Tabs Every] 設定に関係なく、ダッシュボードのタブの自動変更が停止します。
- ダッシュボードのプロパティの [Refresh Page Every] 設定に関係なく、ダッシュボードのページの更新が停止します。
- 時間範囲を変更しても影響はありません。

分析が完了したら、ダッシュボードの一時停止を解除できます。ダッシュボードの一時停止を解除すると、ページ上で該当するすべてのウィジェットがアップデートされ、最新の時間範囲が反映されます。また、ダッシュボードのプロパティで指定した設定に従って、ダッシュボード タブの自動変更が再開され、ダッシュボード ページの更新が再開されます。

ダッシュボードに対するシステム情報のフローを中断するような接続の問題、または他の問題が発生した場合、ダッシュボードは自動的に一時停止し、問題が解決するまでエラー通知を表示します。

注　ダッシュボードが一時停止しているかどうかに関係なく、セッションは通常、非アクティブな状態が 1 時間（または設定した他の時間）続いた場合、ユーザをログアウトします。ダッシュボードを長期間パッシブにモニタリングする場合は、一部のユーザをセッション タイムアウトしないよう設定したり、システムのタイムアウト設定を変更することを検討してください。詳細については、ユーザ ログイン設定の管理（61-51 ページ）およびユーザ インターフェイスの設定（63-30 ページ）を参照してください。

ダッシュボードを表示するには、次のようにします。

アクセス： Admin/Any Security Analyst/Maint

ステップ 1　[Overview] > [Dashboards] を選択します。デフォルトのダッシュボードが定義されているかどうかによって、次の 2 つのオプションがあります。

- デフォルトのダッシュボードを定義している場合は、それが表示されます。別のダッシュボードを表示するには、[Overview] > [Dashboards] メニューを使用します。
- デフォルトのダッシュボードを定義していない場合は、[Dashboard Management] ページが表示されます。表示するダッシュボードの隣の [View] をクリックします。

選択したダッシュボードが表示されます。

ダッシュボードの時間範囲を変更するには、次のようにします。

アクセス： Admin/Any Security Analyst/Maint

ステップ 1　[Show the Last] ドロップダウンリストから、ダッシュボードの時間範囲を選択します。

ダッシュボードを一時停止しない限り、ページ上で該当するすべてのウィジェットがアップデートされ、最新の時間範囲が反映されます。

ダッシュボードを一時停止するには、次のようにします。

アクセス： Admin/Any Security Analyst/Maint

ステップ 1　時間範囲のコントロールで、一時停止のアイコン（ ）をクリックします。

一時停止を解除するまで、ダッシュボードは一時停止します。

ダッシュボードの一時停止を解除するには、次のようにします。

アクセス： Admin/Any Security Analyst/Maint

ステップ 1　一時停止しているダッシュボードの時間範囲のコントロールで、再生のアイコン（▶）をクリックします。

ダッシュボードの一時停止が解除されます。

ダッシュボードの変更

ライセンス： すべて

ダッシュボードには 1 つ以上のタブがあります。タブは追加、削除、および名前変更できます。ダッシュボードのタブの順序は変更できないことに注意してください。

各タブには、3 列のレイアウトで 1 つ以上のウィジェットを表示できます。ユーザは、ウィジェットを最小化および最大化する、タブに対してウィジェットを追加および削除する、タブ上でウィジェットを再配置する、といったことができます。

ダッシュボードの基本的なプロパティを変更することもできます。このプロパティには、名前と説明、タブの自動変更とページ更新の間隔、およびダッシュボードを他のユーザと共有するかどうかが含まれています。

ロールに関係なく、ダッシュボードへアクセスできるすべてのユーザは、共有ダッシュボードを変更できることに注意してください。特定のダッシュボードを自分だけが変更できるようにするには、ダッシュボードのプロパティでプライベート ダッシュボードとして設定します。

Ciscoの事前定義のダッシュボード内の Custom Analysis ウィジェットのすべての設定が、ウィジェットのプリセットに対応しています。これらのウィジェットの 1 つを変更または削除した場合は、適切なプリセットをベースにして新しい Custom Analysis ウィジェットを作成して復元することができます。詳細については、次のサイトを参照してください。

ヒント　Ciscoの事前定義のダッシュボード内の Custom Analysis ウィジェットのすべての設定が、ウィジェットのシステム プリセットに対応しています。これらのウィジェットの 1 つを変更または削除した場合は、適切なプリセットをベースにして新しい Custom Analysis ウィジェットを作成して復元することができます。詳細については、Custom Analysis ウィジェットの設定（55-15 ページ）を参照してください。

詳細については、次の項を参照してください。

- ダッシュボードのプロパティの変更（55-45 ページ）
- タブの追加（55-45 ページ）
- タブの削除（55-46 ページ）
- タブの名前変更（55-46 ページ）
- ウィジェットの追加（55-46 ページ）
- ウィジェットの再配置（55-47 ページ）
- ウィジェットの最小化および最大化（55-48 ページ）
- ウィジェットの削除（55-48 ページ）

ダッシュボードのプロパティの変更

ライセンス：すべて

次の手順を使用してダッシュボードの基本的なプロパティを変更します。このプロパティには、名前と説明、タブの自動変更とページ更新の間隔、およびダッシュボードを他のユーザと共有するかどうかが含まれています。

ダッシュボードのプロパティを変更するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

ステップ 1　[Overview] > [Dashboards] > [Management] を選択します。

[Dashboard Management] ページが表示されます。

ステップ 2　プロパティを変更するダッシュボードの隣の編集アイコン（ ）をクリックします。

[Edit Dashboard] ページが表示されます。変更可能なさまざまな設定の詳細については、カスタムダッシュボードの作成（55-40 ページ）を参照してください。

ステップ 3　必要に応じて変更を行い、[Save] をクリックします。

ダッシュボードが変更されます。

タブの追加

ライセンス：すべて

ダッシュボードへタブを追加するには、次の手順を使用します。

ダッシュボードにタブを追加するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

ステップ 1　タブを追加するダッシュボードを表示します。

詳細については、ダッシュボードの表示（55-42 ページ）を参照してください。

ステップ 2　既存のタブの右側で、タブの追加アイコン（ ＋ ）をクリックします。

ポップアップ ウィンドウが表示され、タブに名前を指定するよう要求されます。

ステップ 3　（25 文字までの）タブの名前を入力し、[OK] をクリックするか、または単純に [OK] をクリックしてデフォルトの名前を受け入れます。タブの名前はいつでも変更できます。タブの名前変更（55-46 ページ）を参照してください。

新しいタブが追加されます。これで、新しいタブにウィジェットを追加できるようになりました。詳細については、ウィジェットの追加（55-46 ページ）を参照してください。

タブの削除

ライセンス：すべて

次の手順を使用して、ダッシュボードのタブ、およびそのすべてのウィジェットを削除します。ダッシュボードから最後のタブを削除することはできません。各ダッシュボードには少なくとも 1 つのタブが必要です。

ダッシュボードからタブを削除するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

ステップ 1　タブを削除するダッシュボードを表示します。

詳細については、ダッシュボードの表示（55-42 ページ）を参照してください。

ステップ 2　削除するタブで、削除のアイコン（ ✖ ）をクリックします。

ステップ 3　タブを削除することを確認します。

タブが削除されます。

タブの名前変更

ライセンス：すべて

ダッシュボード タブの名前を変更するには、次の手順を使用します。

タブの名前を変更するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

ステップ 1　タブの名前を変更するダッシュボードを表示します。

詳細については、ダッシュボードの表示（55-42 ページ）を参照してください。

ステップ 2　名前変更するタブをクリックします。

ステップ 3　タブのタイトルをクリックします。

ポップアップ ウィンドウが表示され、タブの名前を変更するよう要求されます。

ステップ 4　タブの名前（最大 25 文字）を入力し、[OK] をクリックします。

タブの名前が変更されます。

ウィジェットの追加

ライセンス：すべて

ダッシュボードにウィジェットを追加するには、最初に、ウィジェットを追加するタブを決定する必要があります。タブにウィジェットを追加すると、アプライアンスによって自動的に、含まれているウィジェットが最も少ないカラムに追加されます。すべてのカラムに同じ数のウィジェットがある場合、新しいウィジェットは最も左のカラムに追加されます。ダッシュボード タブには最大 15 個のウィジェットを追加できます。

ヒント　追加したウィジェットは、タブの任意の場所に移動できます。ただし、別のタブにはウィジェットを移動できません。詳細については、ウィジェットの再配置（55-47 ページ）を参照してください。

ダッシュボードにウィジェットを追加するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

ステップ 1　ウィジェットを追加するダッシュボードを表示します。

詳細については、ダッシュボードの表示（55-42 ページ）を参照してください。

ステップ 2　ウィジェットを追加するタブを選択します。

ステップ 3　[Add Widgets] をクリックします。

[Add Widgets] ページが表示されます。

ユーザが追加できるウィジェットは、使用しているアプライアンスのタイプと、自分のユーザロールによって異なります。ウィジェットは、Analysis & Reporting、Miscellaneous、および Operations の機能に従って整理されます。カテゴリ名をクリックして各カテゴリのウィジェットを表示することも、[All Categories] をクリックしてすべてのウィジェットを表示することもできます。

ステップ 4　追加するウィジェットの隣の [Add] をクリックします。

ヒント　（複数の RSS Feed ウィジェット、または複数の Custom Analysis ウィジェットを追加する場合など）同じタイプの複数のウィジェットを追加するには、[Add] をもう一度クリックします。

ウィジェットはすぐにダッシュボードに追加されます。[Add Widgets] ページには、新しく追加したウィジェットも含めて、各タイプのウィジェットがタブ上にいくつあるかが示されます。

ステップ 5　オプションで、ウィジェットの追加が終了したときに、[Done] をクリックしてダッシュボードに戻ることもできます。

ウィジェットを追加したタブがもう一度表示され、変更が反映されます。

ウィジェットの再配置

ライセンス：すべて

タブ上で、任意のウィジェットの場所を変更できます。ただし、別のタブにはウィジェットを移動できないことに注意してください。ウィジェットを別のタブに表示する場合は、現在のタブからいったん削除してから新しいタブに追加する必要があります。

ウィジェットを移動するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

ステップ 1　移動するウィジェットのタイトル バーをクリックし、新しい場所へドラッグします。

ウィジェットの最小化および最大化

ライセンス：すべて

ウィジェットを最小化してビューを単純化したり、その後で最大化してもう一度表示したりできます。

ウィジェットを最小化するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

ステップ 1　ウィジェットのタイトル バーで、最小化のアイコン（ − ）をクリックします。

ウィジェットを最大化するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

ステップ 1　ウィジェットのタイトル バーで、最大化のアイコン（ □ ）をクリックします。

ウィジェットの削除

ライセンス：すべて

タブに表示する必要がなくなったウィジェットを削除します。

ウィジェットを削除するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

ステップ 1　ウィジェットのタイトル バーで、閉じるアイコン（ ✖ ）をクリックします。

ステップ 2　ウィジェットを削除することを確認します。

タブからウィジェットが削除されます。

ダッシュボードの削除

ライセンス：すべて

使用する必要がなくなった場合は、ダッシュボードを削除します。

デフォルトのダッシュボードを削除する場合は、新しいデフォルトを定義する必要があります。そうしない場合、ダッシュボードを表示しようとするたびに、アプライアンスからダッシュボードを選択するよう要求されます。詳細については、デフォルトのダッシュボードの指定（71-9 ページ）を参照してください。

ダッシュボードを削除するには、次のようにします。

アクセス: Admin/Any Security Analyst/Maint

ステップ 1　[Overview] > [Dashboards] > [Management] を選択します。

[Dashboard Management] ページが表示されます。

ステップ 2　削除するダッシュボードの隣の削除アイコン( )をクリックします。

ステップ 3　ダッシュボードを削除することを確認します。

ダッシュボードが削除されます。

Context Explorer の使用法

FireSIGHT システムContext Explorer には、モニタ対象ネットワークのステータスに関するコンテキストでの詳細でインタラクティブなグラフィカル情報が表示されます。これには、アプリケーション、アプリケーション統計、接続、位置情報、侵害の兆候、侵入イベント、ホスト、サーバ、Security Intelligence、ユーザ、ファイル（マルウェア ファイルを含む）、および関連 URL に関するデータが含まれます。各セクションには、このデータが鮮やかな色の折れ線グラフ、棒グラフ、円グラフ、ドーナツ グラフの形式で表示され、グラフとともに詳しいリストが示されます。

分析を細かく調整するためのカスタム フィルタを容易に作成および適用できます。またグラフ エリアをクリックするか、カーソルをグラフ エリアに置くことでデータ セクションを詳しく調べることができます。過去 1 時間から過去 1 年までの期間を反映するように Explorer の時間範囲を設定することもできます。Context Explorer にアクセスできるユーザは、Administrator、Security Analyst、または Security Analyst (Read Only) のユーザ ロールが割り当てられているユーザだけです。

FireSIGHT システム ダッシュボードは細かくカスタマイズ可能であり、区分化されており、リアルタイムで更新されます。一方、Context Explorer は手動で更新され、より幅広いデータのコンテキストを提供することを目的としており、アクティブなユーザ操作のために単一で一貫性のあるレイアウトを備えています。

特定のニーズに基づいてネットワークとアプライアンスのリアルタイムのアクティビティをモニタするには、ダッシュボードを使用します。逆に、詳細かつ明確なコンテキストで事前に定義されている最新の FireSIGHT データ セットを調査するには、Context Explorer を使用します。たとえば、ネットワークのホストのうち Linux を使用しているホストは 15% であるが、ほぼすべての YouTube トラフィックはこれらのホストによるものであることが判明した場合、Linux ホストのデータのみを表示するフィルタ、YouTube 関連のアプリケーション データのみを表示するフィルタ、あるいはこの両方のフィルタを簡単に適用できます。コンパクトで対象が絞り込まれているダッシュボード ウィジェットとは異なり、Context Explorer の各セクションは、FireSIGHT システムの専門知識を持つユーザと一般的なユーザの両方に役立つ形式で、システム アクティビティを鮮明なビジュアル表現で提供します。

表示されるデータは、管理対象デバイスのライセンスと導入方法、データを提供する機能を設定するかどうか、および シリーズ 2 アプライアンスと Cisco NGIPS for Blue Coat X-Series の場合はデータを提供する機能をサポートしているかどうかなどの要因に応じて異なることに注意してください。たとえば、DC500 Defense Center と シリーズ 2 デバイスまたは Cisco NGIPS for Blue Coat X-Series はいずれも高度なマルウェア防御をサポートしていないため、DC500 Defense Center はこのデータを表示できず、シリーズ 2 デバイスと Cisco NGIPS for Blue Coat X-Series はこのデータを検出しません。

次の表に、ダッシュボード と Context Explorer の主な相違点の要約を示します。

表 56-1　比較：ダッシュボードおよび Context Explorer

機能	ダッシュボード	Context Explorer
表示可能なデータ	FireSIGHT システムによって監視されるすべてのデータ	アプリケーション、アプリケーション統計、位置情報、侵害の兆候、侵入イベント、ファイル（マルウェア ファイルを含む）、ホスト、Security Intelligence イベント、サーバ、ユーザ、および URL
カスタマイズ可能かどうか	• ダッシュボードで選択されているウィジェットはカスタマイズ可能です • 個々のウィジェットはさまざまなレベルでカスタマイズ可能です	• 基本レイアウトは変更できません • 適用されたフィルタは Explorer URL に示され、後で使用するためにブックマークできます
データの更新頻度	自動（デフォルト）、ユーザ設定	手動
データのフィルタリング	一部のウィジェットで可能です（ウィジェット設定を編集する必要があります）	Explorer のすべての部分で可能であり、複数フィルタに対応しています
グラフィカル コンテキスト	一部のウィジェット（特に Custom Analysis）では、データをグラフ形式で表示できます。	すべてのデータの豊富なグラフィカル コンテキスト（独自の詳細なドーナツ グラフを含む）
関連 Web インターフェイス ページへのリンク	一部のウィジェット	すべてのセクション
表示データの時間範囲	ユーザ設定された	ユーザ設定された

関連する FireSIGHT システム ダッシュボードの詳細については、ダッシュボードの使用（55-1 ページ）を参照してください。

Context Explorer について

ライセンス： FireSIGHT

Context Explorer を構成するさまざまな個別のセクションの情報から、モニタ対象ネットワークの FireSIGHT データの全体的な概要を把握できます。1 番目のセクションに表示される時間の経過に伴うトラフィックとイベント数の変化を示した折れ線グラフは、ネットワークのアクティビティにおける最近の傾向の概要を示します。

他のセクションは、侵害の兆候、ネットワーク、アプリケーション、Security Intelligence、侵入、ファイル、位置情報および URL のデータをより詳細に示す一連のインタラクティブ グラフとリストからなります。トラフィックとイベントの時間グラフ以外のすべてのセクションは、表示または非表示にできます。また、すべてのセクションに表示するデータを制限するフィルタを適用できます。詳細については、Context Explorer でのフィルタ操作（56-42 ページ）参照してください。

Context Explorer のセクションの内容と機能の詳細については、次のトピックを参照してください。

- [Traffic and Intrusion Event Counts] グラフについて（56-3 ページ）
- [Indications of Compromise] セクションについて（56-4 ページ）
- [Network Information] セクションについて（56-6 ページ）
- [Application Information] セクションについて（56-12 ページ）
- [Security Intelligence] セクションについて（56-17 ページ）

- [Intrusion Information] セクションについて（56-19 ページ）
- [Files Information] セクションについて（56-26 ページ）
- [Geolocation Information] セクションについて（56-32 ページ）
- [URL Information] セクションについて（56-35 ページ）

Context Explorer の全体的な設定方法については、次のトピックを参照してください。

- Context Explorer の更新（56-39 ページ）
- Context Explorer の時間範囲の設定（56-39 ページ）
- Context Explorer のセクションの最小化および最大化（56-40 ページ）
- Context Explorer データのドリルダウン（56-40 ページ）

Context Explorer フィルタの設定および使用方法の詳細については、次の項を参照してください。

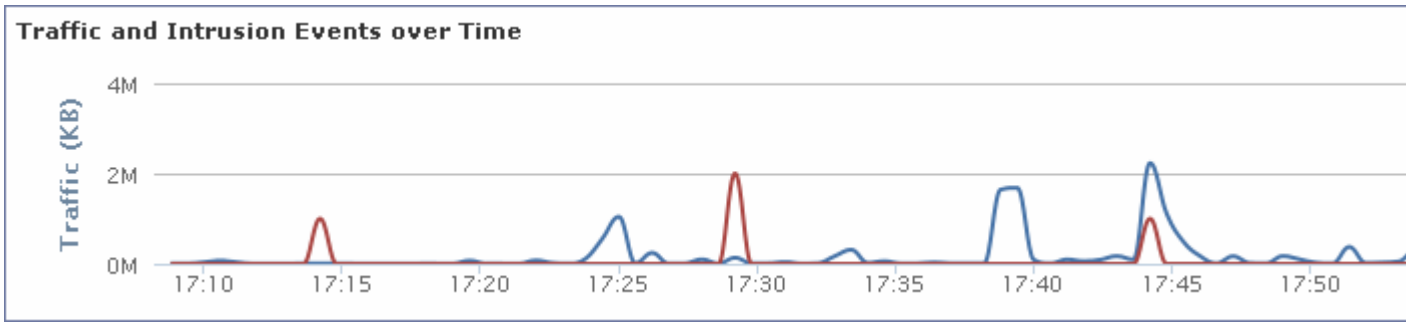
- Context Explorer でのフィルタ操作（56-42 ページ）
- フィルタの追加および適用（56-42 ページ）
- コンテキスト メニューを使用したフィルタの作成（56-46 ページ）
- フィルタのブックマーク（56-47 ページ）

[Traffic and Intrusion Event Counts] グラフについて

ライセンス：FireSIGHT

Context Explorer の上部には、時間の経過に伴うトラフィックおよび侵入イベント数の変化を示す折れ線グラフが表示されます。X 軸は時間間隔を示します（選択されている時間枠に応じて、5 分～ 1 か月）。Y 軸は、KB 単位のトラフィック（青色の線）と侵入イベント数（赤色の線）を示します。

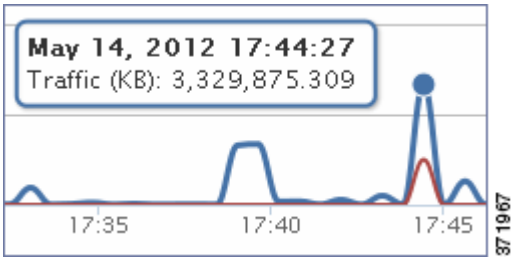
X 軸の最小間隔が 5 分であることに注意してください。これに対応するため、選択された時間範囲の開始点と終了点が、システムにより、最も近い 5 分間間隔に調整されます。



デフォルトでは、このセクションには選択された時間範囲のすべてのネットワーク トラフィックおよび生成されたすべての侵入イベントが示されます。フィルタを適用すると、フィルタに指定されている条件に関連するトラフィックおよび侵入イベントだけがグラフに表示されます。たとえば、[OS Name] に `Windows` を指定してフィルタリングすると、時間グラフには Windows オペレーティング システムを使用するホストに関連するトラフィックとイベントだけが表示されます。

侵入イベント データ（[Priority] が High に設定されたものなど）に基づいて Context Explorer をフィルタリングすると、青色のトラフィックを示す線が非表示になり、侵入イベントだけに集中することができます。

トラフィックおよびイベント数に関する正確な情報を確認するには、グラフ線上の任意のポイントにポインタを置きます。色付きの線の 1 つにポインタを置くと、その線がグラフの前面に移動し、コンテキストがより明確になります。



このセクションに取り込まれるデータは主に [Intrusion Events] 表と [Connection Events] 表のデータです。

[Indications of Compromise] セクションについて

ライセンス：FireSIGHT

Context Explorer の [Indications of Compromise (IOC)] セクションには、モニタ対象ネットワークでセキュリティが侵害されている可能性があるホストの概要を示す 2 つのインタラクティブ セクション（トリガーとして使用された主な IOC 種類の割合のビューと、トリガーとして使用された兆候の数をホストごとに表したビュー）が表示されます。

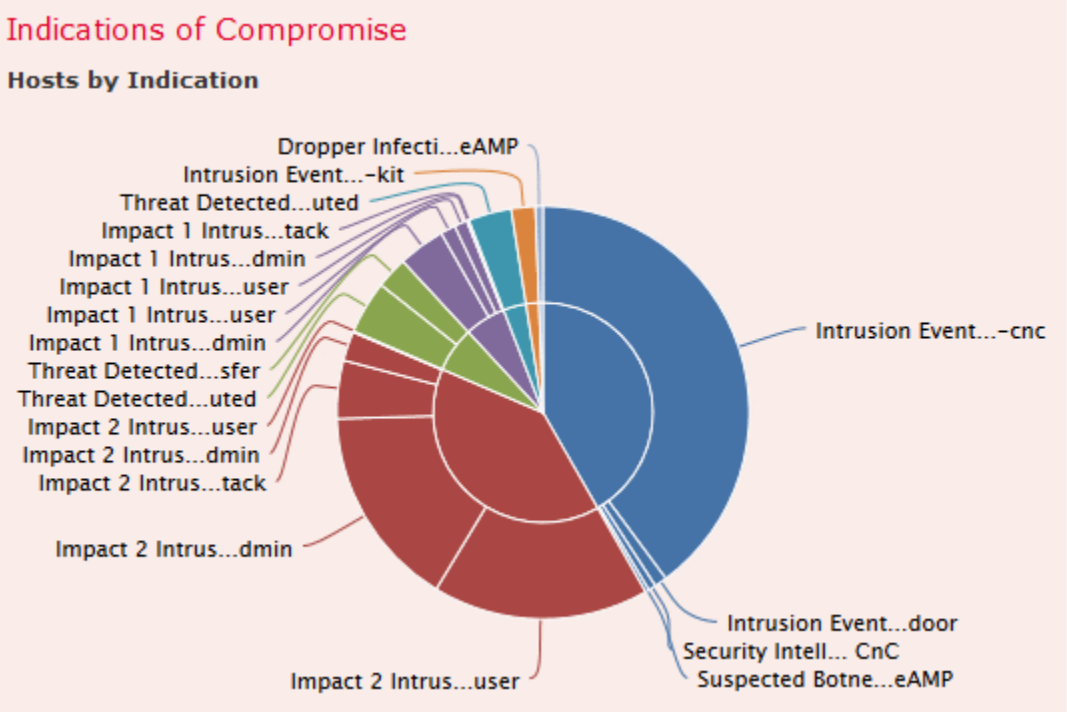
[Indications of Compromise] セクションのグラフの詳細については、次のトピックを参照してください。

- [Hosts by Indication] グラフの表示（56-4 ページ）
- [Indications by Host] グラフの表示（56-5 ページ）

[Hosts by Indication] グラフの表示

ライセンス：FireSIGHT

[Hosts by Indication] グラフはドーナツ形式であり、モニタ対象ネットワーク上のホストでトリガーとして使用された侵害の兆候（IOC）の割合のビューを表示します。内側のリングは IOC カテゴリ（CnC Connected や Malware Detected など）ごとに分割されており、外側のリングではそれがさらに具体的なイベントの種類（Impact 2 Intrusion Event - attempted-admin や Threat Detected in File Transfer など）ごとに分割されています。



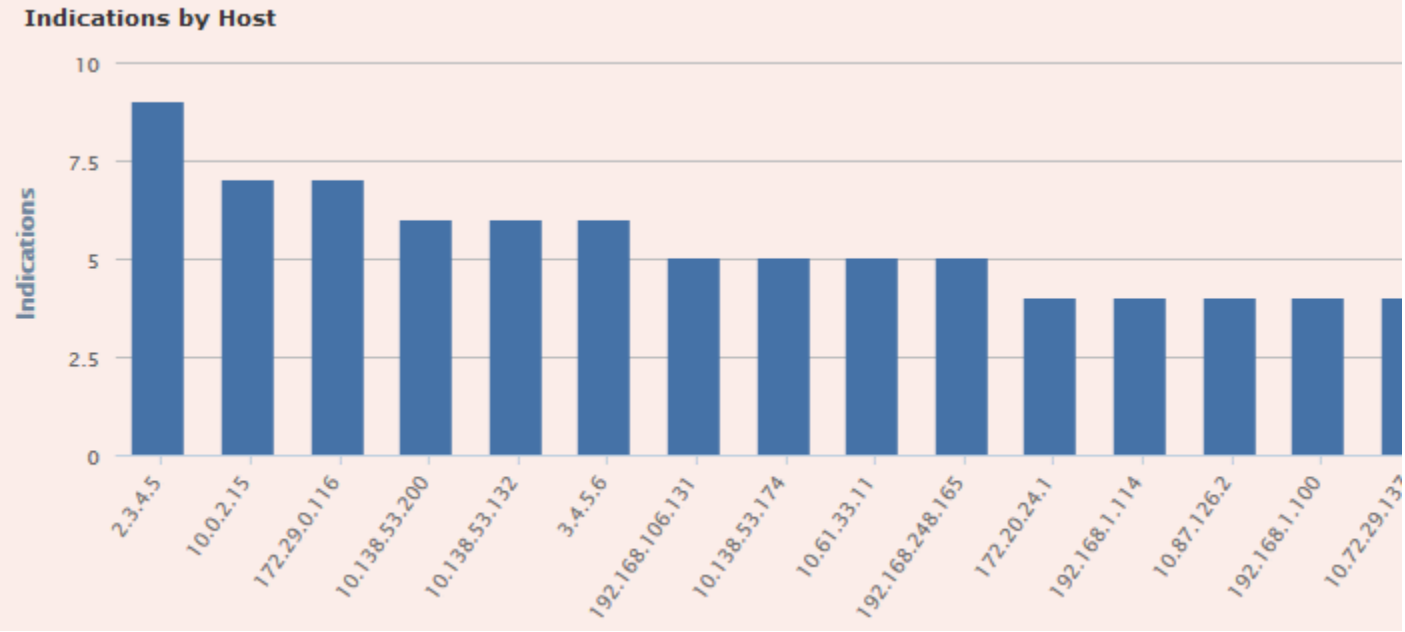
グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [Hosts] 表と [Indications of Compromise] 表から取得されます。

[Indications by Host] グラフの表示

ライセンス：FireSIGHT

[Indications by Host] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最も IOC が激しい 15 のホストによりトリガーとして使用された固有の侵害の兆候（IOC）の数を表示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [Hosts] 表と [Indications of Compromise] 表から取得されます。

[Network Information] セクションについて

ライセンス：FireSIGHT

Context Explorer の [Network Information] セクションには、モニタ対象ネットワーク上の接続トラフィックの概要（トラフィックに関連する送信元、宛先、ユーザ、およびセキュリティ ゾーン、ネットワーク上のホストで使用されているオペレーティング システムの内訳、FireSIGHT システムがネットワーク トラフィックに対して実行したアクセス制御アクションの割合のビュー）を示す 6 つのインタラクティブ グラフが含まれます。

[Network Information] セクションのグラフの詳細については、次のトピックを参照してください。

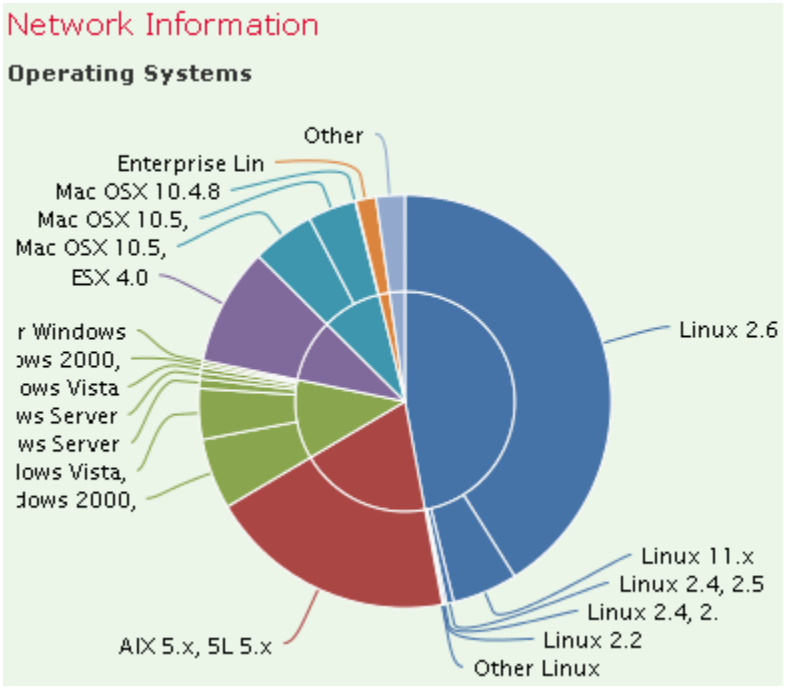
- [Operating Systems] グラフの表示（56-7 ページ）
- [Traffic by Source IP] グラフの表示（56-8 ページ）
- [Traffic by Source User] グラフの表示（56-9 ページ）
- [Connections by Access Control Action] グラフの表示（56-10 ページ）
- [Traffic by Destination IP] グラフの表示（56-11 ページ）
- [Traffic by Ingress/Egress Security Zone] グラフの表示（56-11 ページ）

[Operating Systems] グラフの表示

ライセンス：FireSIGHT

[Operating Systems] グラフはドーナツ グラフ形式であり、モニタ対象ネットワークのホストで検出されたオペレーティング システムを割合で表示します。内側のリングは OS 名（`Windows` や `Linux` など）ごとに分割され、外側のリングではそのデータがさらにオペレーティング システムのバージョン（`Windows Server 2008` や `Linux 11.x` など）ごとに分割されています。密接に関連するいくつかのオペレーティング システム（Windows 2000、Windows XP、Windows Server 2003 など）は 1 つにまとめられます。ごく少数の認識されないオペレーティング システムは [Other] にまとめられます。

このグラフは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Explorer の時間範囲を変更しても、グラフは変化しません。



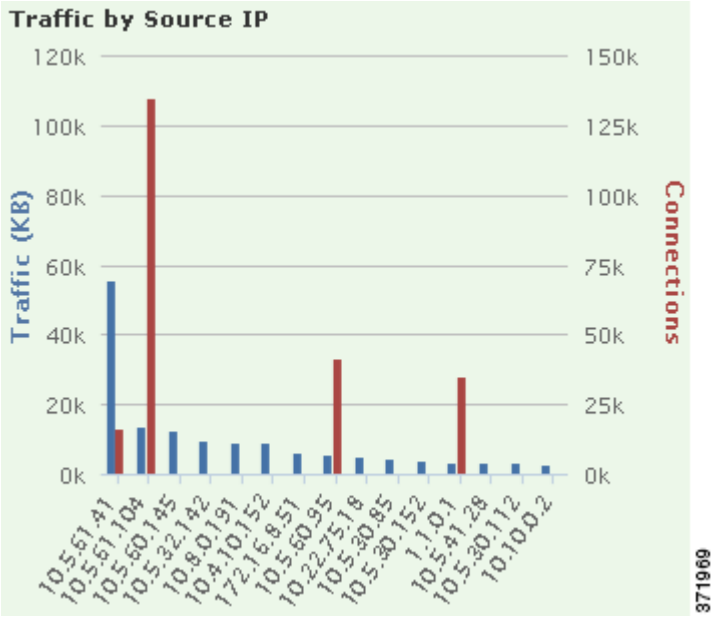
グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [Hosts] 表から取得されます。

[Traffic by Source IP] グラフの表示

ライセンス：FireSIGHT

[Traffic by Source IP] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最もアクティブな上位 15 の送信元 IP アドレスのネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。リストされた送信元 IP アドレスごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

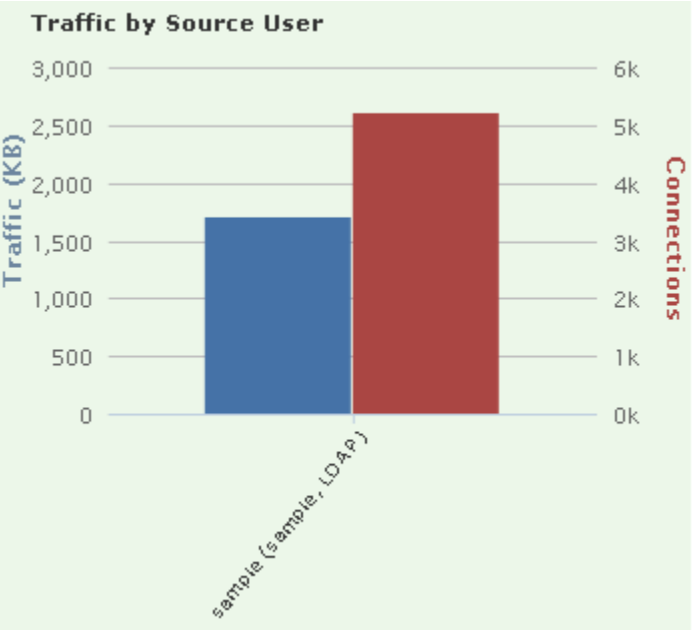
注　侵入イベントの情報でフィルタリングすると、[Traffic by Source IP] グラフは非表示になります。

このグラフのデータは主に [Connection Events] 表から取得されます。

[Traffic by Source User] グラフの表示

ライセンス：FireSIGHT

[Traffic by Source User] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最もアクティブな上位 15 の送信元ユーザのネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。リストされた送信元 IP アドレスごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

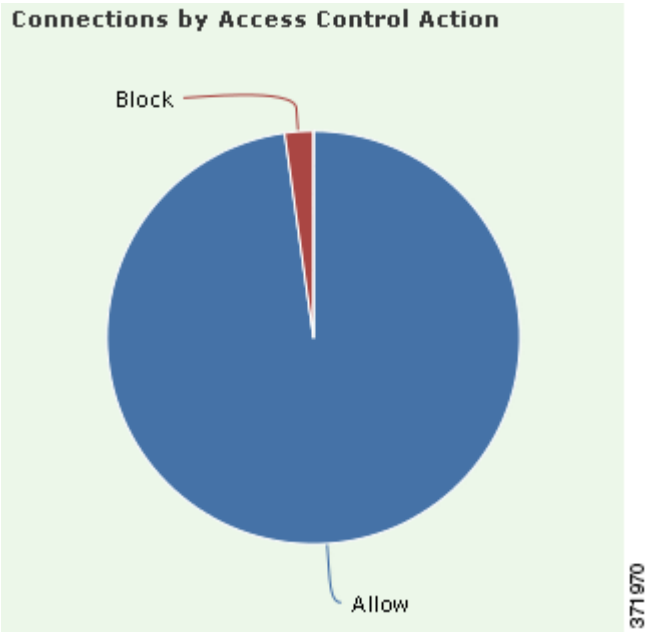
注　侵入イベントの情報でフィルタリングすると、[Traffic by Source User] グラフは非表示になります。

このグラフのデータは主に [Connection Events] 表から取得されます。User Agent によって報告されるユーザだけが表示されることに注意してください。

[Connections by Access Control Action] グラフの表示

ライセンス：FireSIGHT

[Connections by Access Control Action] グラフは円グラフ形式であり、導入されている FireSIGHT システムでモニタ対象トラフィックに対して実行されたアクセス制御アクション（[Block] や [Allow] など）の割合のビューを表示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

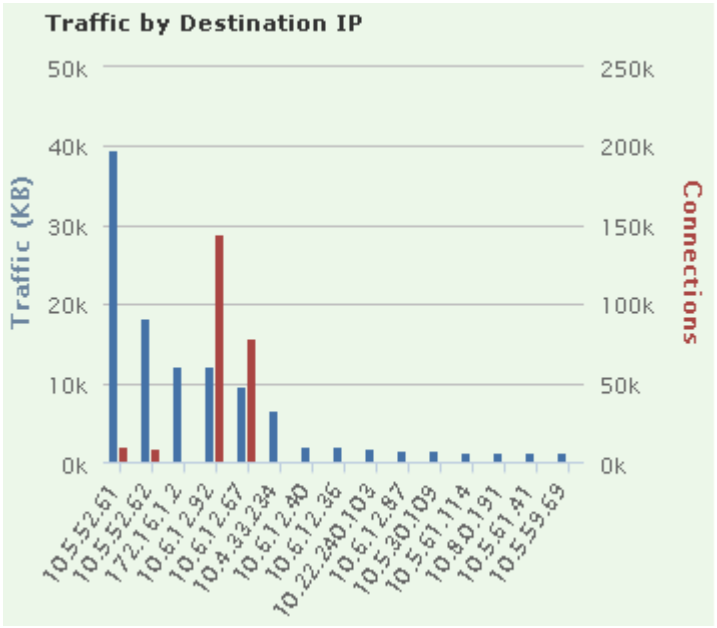
注　侵入イベントの情報でフィルタリングすると、[Traffic by Source User] グラフは非表示になります。

このグラフのデータは主に [Connection Events] 表から取得されます。

[Traffic by Destination IP] グラフの表示

ライセンス：FireSIGHT

[Traffic by Destination IP] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最もアクティブな上位 15 の宛先 IP アドレスのネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。リストされた宛先 IP アドレスごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

注　侵入イベントの情報でフィルタリングすると、[Traffic by Destination IP] グラフは非表示になります。

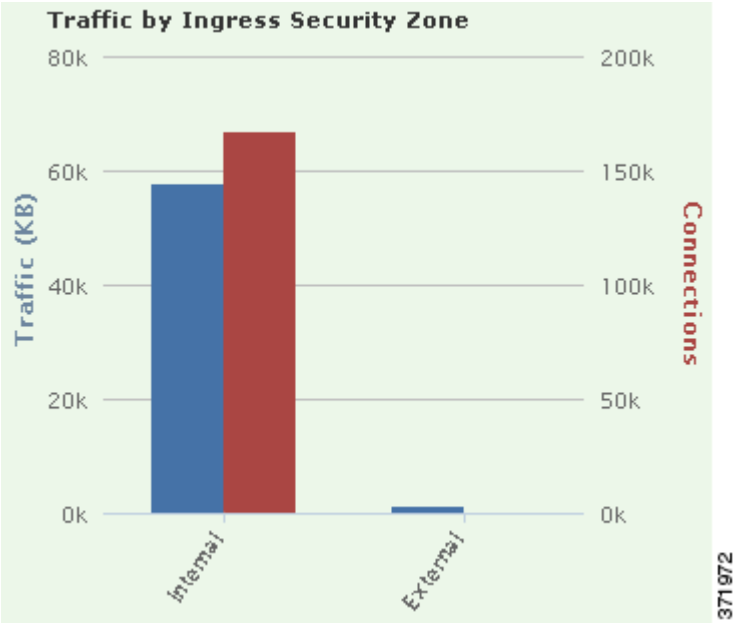
このグラフのデータは主に [Connection Events] 表から取得されます。

[Traffic by Ingress/Egress Security Zone] グラフの表示

ライセンス：FireSIGHT

[Traffic by Ingress/Egress Security Zone] グラフは棒グラフ形式であり、モニタ対象ネットワークで設定されている各セキュリティ ゾーンごとに、その着信/発信ネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。必要に応じて、このグラフに入力（デフォルト）セキュリティ ゾーン情報または出力セキュリティ ゾーン情報のいずれかを表示するように設定できます。

リストされたセキュリティ ゾーンごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。セキュリティ ゾーンの詳細については、セキュリティ ゾーンの操作（3-42 ページ）を参照してください。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント グラフに制約を適用して、出力セキュリティ ゾーンのトラフィックだけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Egress] をクリックします。デフォルト ビューに戻すには [Ingress] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [Ingress] ビューに戻ることに注意してください。

注 侵入イベントの情報でフィルタリングすると、[Traffic by Ingress/Egress Security Zone] グラフは非表示になります。

このグラフのデータは主に [Connection Events] 表から取得されます。

[Application Information] セクションについて

ライセンス： FireSIGHT

Context Explorer の [Application Information] セクションには、3 つのインタラクティブ グラフと 1 つの表形式リストが表示されます。これらのグラフとリストは、モニタ対象ネットワーク上でのアプリケーション アクティビティの概要（アプリケーションに関連するトラフィック、侵入イベント、およびホストを、各アプリケーションに割り当てられている推定リスクまたは推定ビジネス関連度ごとに編成したもの）を示します。[Application Details List] は、各アプリケーションとそのリスク、ビジネス関連度、カテゴリ、およびホスト数を示すインタラクティブなリストです。

このセクションのすべての「アプリケーション」インスタンスについて、[Application Information] のグラフのセットは、デフォルトでは特にアプリケーション プロトコル（DNS、SSH など）を検査します。クライアント アプリケーション（PuTTY や Firefox など）や Web アプリケーション（Facebook や Pandora など）を特に検査するように [Application Information] セクションを設定することもできます。

[Application Information] セクションのグラフとリストの詳細については、次のトピックを参照してください。

- [Traffic by Risk/Business Relevance and Application] グラフの表示（56-13 ページ）
- [Intrusion Events by Risk/Business Relevance and Application] グラフの表示（56-14 ページ）
- [Hosts by Risk/Business Relevance and Application] グラフの表示（56-15 ページ）
- [Application Details List] の表示（56-16 ページ）

[Application Information] セクションのフォーカスを設定するには、次の手順を実行します。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Context Explorer] を選択します。

Context Explorer が表示されます。

ステップ 2　[Application Protocol Information] セクションにポインタを置きます。（同じ Context Explorer セッションで以前にこの設定を変更している場合は、セクション タイトルが[Client Application Information] または [Web Application Information] と表示されることがある点に注意してください。）

セクションのオプション ボタンが右上に表示されます。

ステップ 3　[Application Protocol]、[Client Application]、または [Web Application] をクリックします。

[Application Information] セクションは、選択したオプションに従って更新されます。

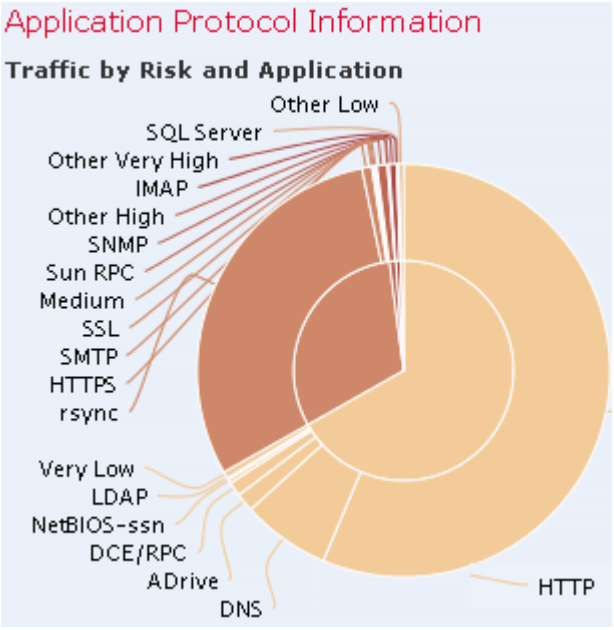
注　Context Explorer の外部に移動すると、このセクションはデフォルトの状態（Application Protocol）に戻ります。

[Traffic by Risk/Business Relevance and Application] グラフの表示

ライセンス： FireSIGHT

[Traffic by Risk/Business Relevance and Application] グラフはドーナツ形式であり、モニタ対象ネットワークで検出されたアプリケーション トラフィックを、アプリケーションの推定リスク（デフォルト）または推定ビジネス関連度ごとの割合で表示します。内側のリングは推定リスク/ビジネス関連度レベル（`Medium` または `High` など）ごとに分割され、外側のリングではそのデータがさらに具体的なアプリケーション（`SSH` または `NetBIOS` など）ごとに分割されます。稀に検出されるアプリケーションは [Other] にまとめられます。

このグラフは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Explorer の時間範囲を変更しても、グラフは変化しません。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント グラフに制約を適用して、ビジネス関連度とアプリケーションごとにトラフィックが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Business Relevance] をクリックします。デフォルト ビューに戻すには [Risk] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [Risk] ビューに戻ることに注意してください。

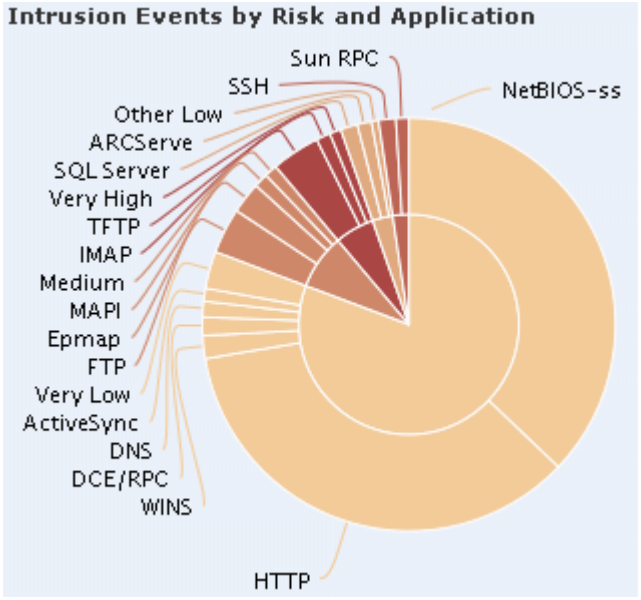
注 侵入イベントの情報でフィルタリングすると、[Traffic by Risk/Business and Application] グラフは非表示になります。

このグラフのデータは主に [Connection Events] 表と [Application Statistics] 表から取得されます。

[Intrusion Events by Risk/Business Relevance and Application] グラフの表示

ライセンス： FireSIGHT

[Intrusion Events by Risk/Business Relevance and Application] グラフはドーナツ形式であり、モニタ対象ネットワークで検出された侵入イベントと、これらのイベントに関連するアプリケーションを、アプリケーションの推定リスク（デフォルト）または推定ビジネス関連度ごとの割合で表示します。内側のリングは推定リスク/ビジネス関連度レベル（`Medium` または `High` など）ごとに分割され、外側のリングではそのデータがさらに具体的なアプリケーション（`SSH` または `NetBIOS` など）ごとに分割されます。稀に検出されるアプリケーションは [Other] にまとめられます。



ドーナツ グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされるか、または（該当する場合には）アプリケーション情報が表示されます。

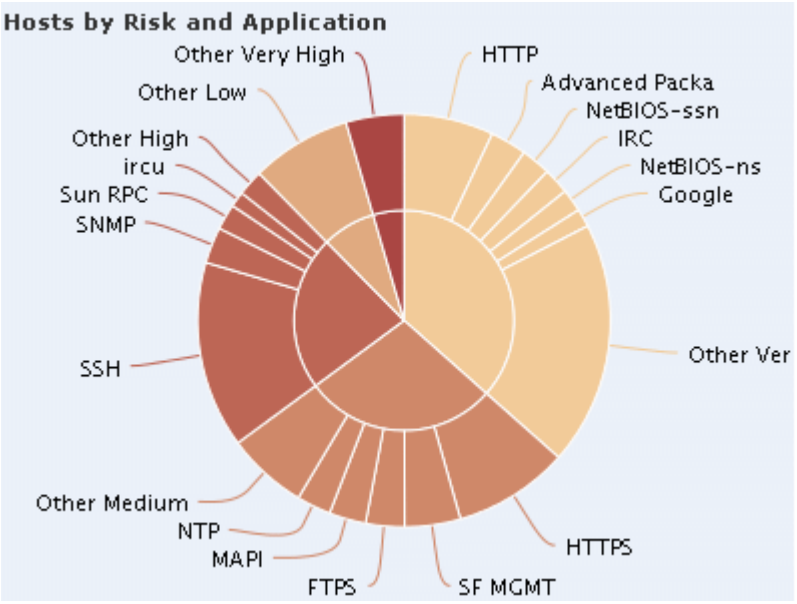
ヒント　グラフに制約を適用して、ビジネス関連度とアプリケーションごとに侵入イベントが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Business Relevance] をクリックします。デフォルト ビューに戻すには [Risk] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [Risk] ビューに戻ることに注意してください。

このグラフのデータは主に [Intrusion Events] 表と [Application Statistics] 表から取得されます。

[Hosts by Risk/Business Relevance and Application] グラフの表示

ライセンス：FireSIGHT

[Hosts by Risk/Business Relevance and Application] グラフはドーナツ形式であり、モニタ対象ネットワークで検出されたホストと、これらのホストに関連するアプリケーションを、アプリケーションの推定リスク（デフォルト）または推定ビジネス関連度ごとの割合で表示します。内側のリングは推定リスク/ビジネス関連度レベル（`Medium` または `High` など）ごとに分割され、外側のリングではそのデータがさらに具体的なアプリケーション（`SSH` または `NetBIOS` など）ごとに分割されます。非常に少数のアプリケーションは [Other] にまとめられます。



ドーナツ グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、ビジネス関連度とアプリケーションに基づいてホストが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Business Relevance] をクリックします。デフォルト ビューに戻すには [Risk] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [Risk] ビューに戻ることに注意してください。

このグラフのデータは主に [Applications] 表から取得されます。

[Application Details List] の表示

ライセンス：FireSIGHT

[Application Information] セクション下部に表示される [Application Details List] は、モニタ対象ネットワークで検出される各アプリケーションの推定リスク、推定ビジネス関連度、カテゴリ、およびホスト数の情報を示す表です。アプリケーションは、関連ホスト数の降順でリストされます。

[Application Details List] 表はソートできませんが、表の項目をクリックして、その情報でフィルタリングまたはドリルダウンしたり、(該当する場合に) アプリケーション情報を表示したりすることができます。この表のデータは主に [Applications] 表から取得されます。

このリストは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Explorer の時間範囲を変更しても、リストは変化しません。

[Security Intelligence] セクションについて

ライセンス： Protection

サポートされるデバイス： すべて（シリーズ 2 を除く）

サポートされる防御センター： DC500 を除くいずれか

Context Explorer の [Security Intelligence] セクションには、3 つのインタラクティブな棒グラフが表示されます。これらのグラフは、モニタ対象ネットワーク上でブラックリストに登録されているトラフィックまたは Security Intelligence によってモニタされるトラフィックの概要を示します。これらのグラフでは、カテゴリ、送信元 IP アドレス、カテゴリ、および宛先 IP アドレスに基づいてトラフィックがソートされ、トラフィックの容量（KB/秒）と該当する接続の数の両方が表示されます。

[Security Intelligence] セクションのグラフの詳細については、次のトピックを参照してください。

- [Security Intelligence Traffic by Category] グラフの表示（56-17 ページ）
- [Security Intelligence Traffic by Source IP] グラフの表示（56-18 ページ）
- [Security Intelligence Traffic by Destination IP] グラフの表示（56-19 ページ）

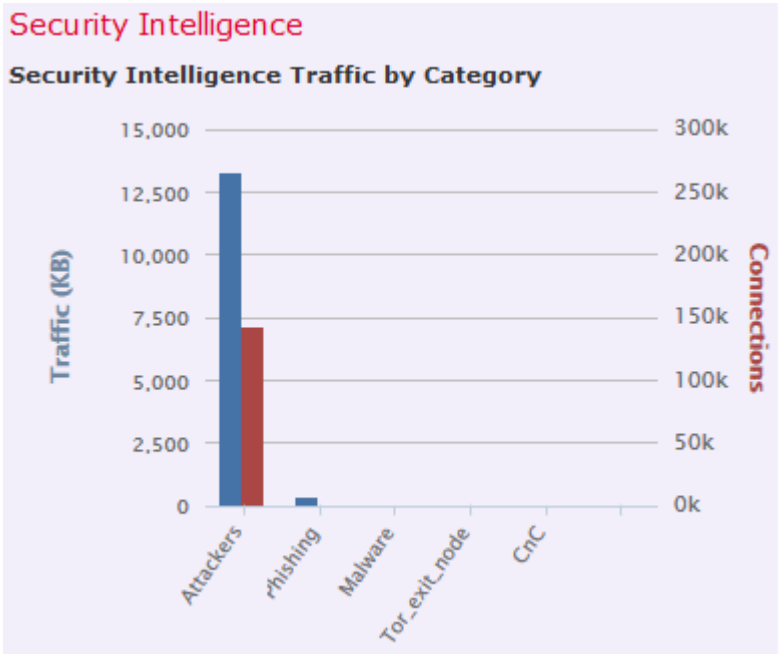
[Security Intelligence Traffic by Category] グラフの表示

ライセンス： Protection

サポートされるデバイス： すべて（シリーズ 2 を除く）

サポートされる防御センター： DC500 を除くいずれか

[Security Intelligence Traffic by Category] グラフは棒グラフ形式であり、モニタ対象ネットワーク上のトラフィックの上位 Security Intelligence カテゴリのネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンされます。

注　侵入イベントの情報でフィルタリングすると、[Security Intelligence Traffic by Category] グラフは非表示になります。

このグラフのデータは主に [Security Intelligence] 表から取得されます。

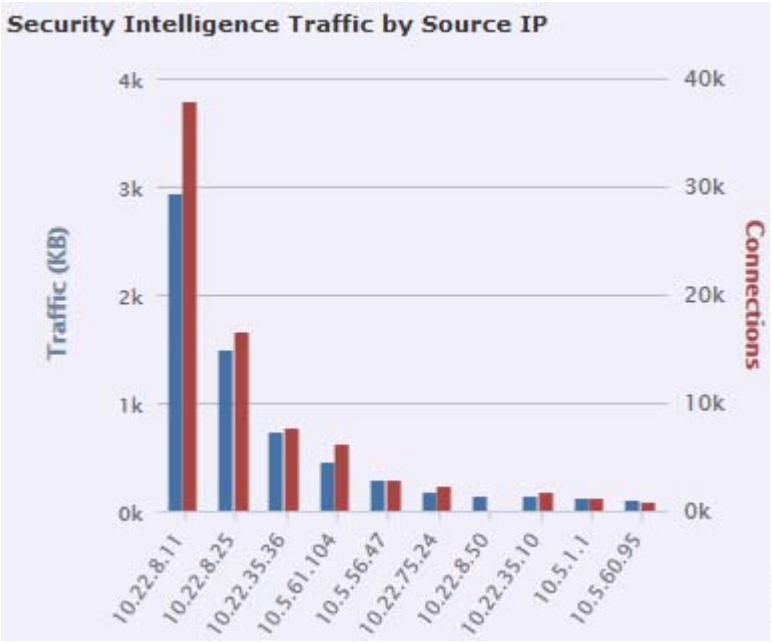
[Security Intelligence Traffic by Source IP] グラフの表示

ライセンス： Protection

サポートされるデバイス： すべて（シリーズ 2 を除く）

サポートされる防御センター： DC500 を除くいずれか

[Security Intelligence Traffic by Source IP] グラフは棒グラフ形式であり、モニタ対象ネットワーク上のセキュリティ インテリジェンスによってモニタされるトラフィックの上位の送信元 IP アドレスのネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンされます。

注　侵入イベントの情報でフィルタリングすると、[Security Intelligence Traffic by Source IP] グラフは非表示になります。

このグラフのデータは主に [Security Intelligence] 表から取得されます。

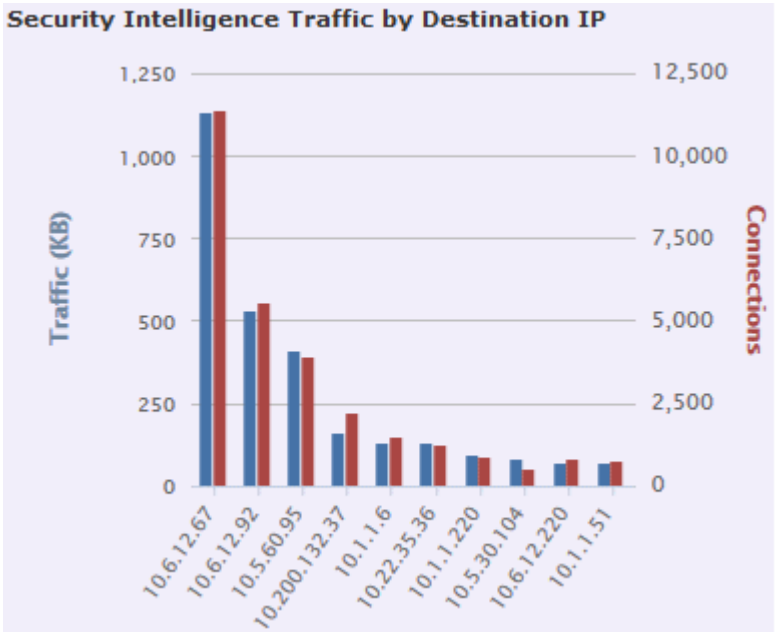
[Security Intelligence Traffic by Destination IP] グラフの表示

ライセンス： Protection

サポートされるデバイス： すべて（シリーズ 2 を除く）

サポートされる防御センター： DC500 を除くいずれか

[Security Intelligence Traffic by Destination IP] グラフは棒グラフ形式であり、モニタ対象ネットワーク上のセキュリティ インテリジェンスによってモニタされるトラフィックの上位の宛先 IP アドレスごとに、そのネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンされます。

注　侵入イベントの情報でフィルタリングすると、[Security Intelligence Traffic by Destination IP] グラフは非表示になります。

このグラフのデータは主に [Security Intelligence] 表から取得されます。

[Intrusion Information] セクションについて

ライセンス： Protection

Context Explorer の [Intrusion Information] セクションには 6 つのインタラクティブ グラフと 1 つの表形式リストが表示されます。これらのグラフとリストは、モニタ対象ネットワークの侵入イベントの概要（侵入イベントに関連付けられている影響レベル、攻撃元、攻撃対象先、ユーザ、優先レベル、およびセキュリティ ゾーンと、侵入イベントの分類、優先度、カウントを示す詳細なリスト）を示します。

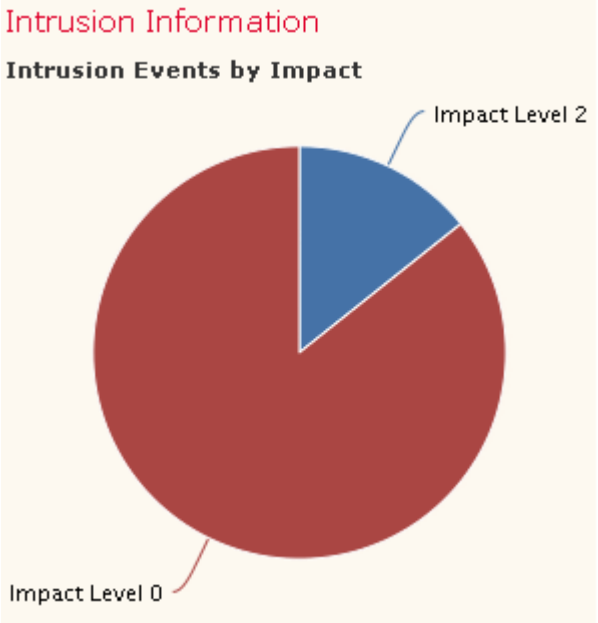
[Network Information] セクションのグラフとリストの詳細については、次のトピックを参照してください。

- [Intrusion Events by Impact] グラフの表示（56-20 ページ）
- [Top Attackers] グラフの表示（56-21 ページ）
- [Top Users] グラフの表示（56-22 ページ）
- [Intrusion Events by Priority] グラフの表示（56-23 ページ）
- [Top Targets] グラフの表示（56-24 ページ）
- [Top Ingress/Egress Security Zones] グラフの表示（56-24 ページ）
- [Intrusion Event Details List] の表示（56-25 ページ）

[Intrusion Events by Impact] グラフの表示

ライセンス：Protection

[Intrusion Events by Impact] グラフは円グラフ形式であり、モニタ対象ネットワークの侵入イベントを、推定影響レベル（0 ～ 4）のグループごとの割合のビューで表示します。



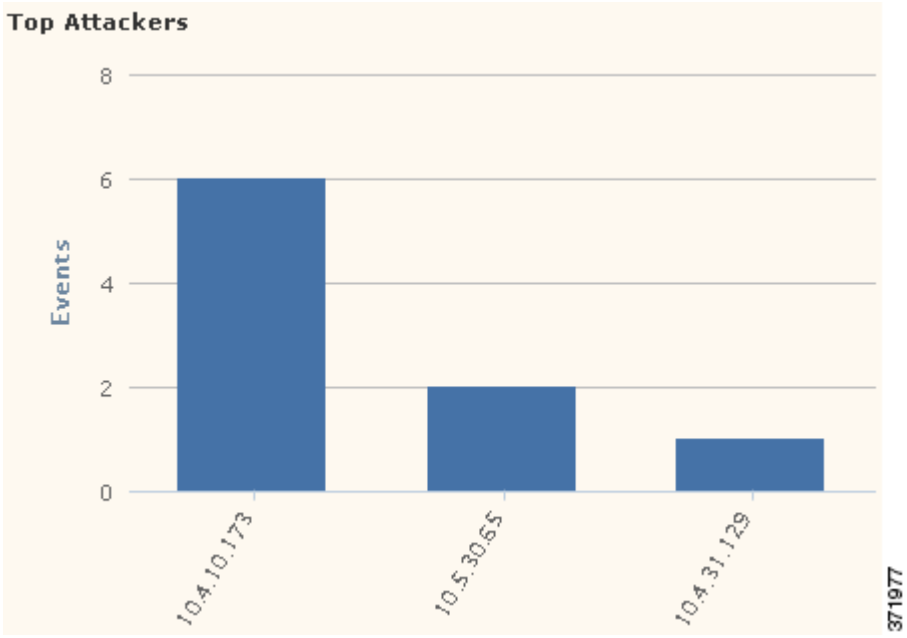
グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [Intrusion Events] 表と [IDS Statistics] 表から取得されます。

[Top Attackers] グラフの表示

ライセンス：Protection

[Top Attackers] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の（侵入イベントを発生させた）上位の攻撃元ホスト IP アドレスの侵入イベント数を表示します。



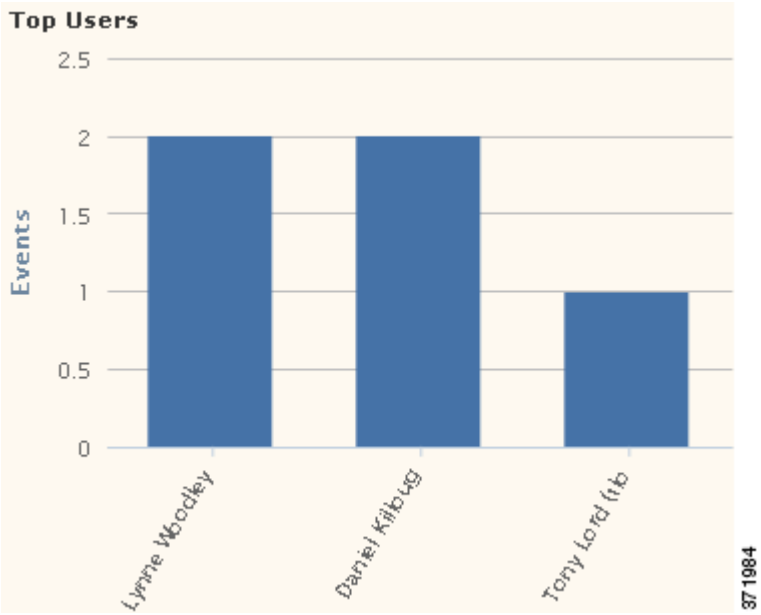
グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [Intrusion Events] 表から取得されます。

[Top Users] グラフの表示

ライセンス：Protection

[Top Users] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最大侵入イベント数に関連するユーザと、イベント数を表示します。



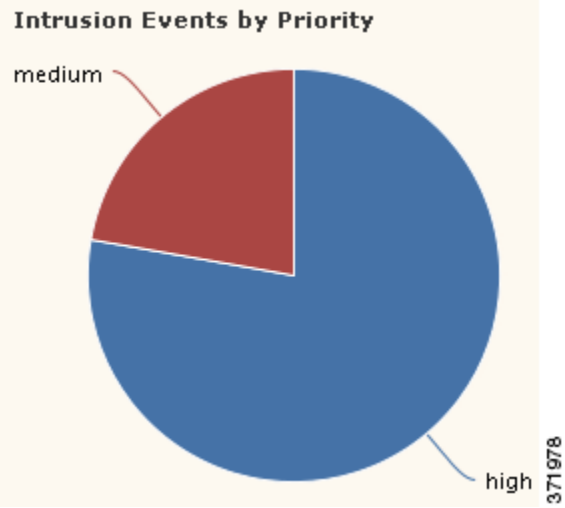
グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [Intrusion Events] 表と [IDS User Statistics] 表から取得されます。User Agent によって報告されるユーザだけが表示されることに注意してください。

[Intrusion Events by Priority] グラフの表示

ライセンス：Protection

[Intrusion Events by Priority] グラフは円グラフ形式であり、モニタ対象ネットワークの侵入イベントを、推定優先度レベル（`High`、`Medium`、`Low` など）のグループごとの割合のビューで表示します。



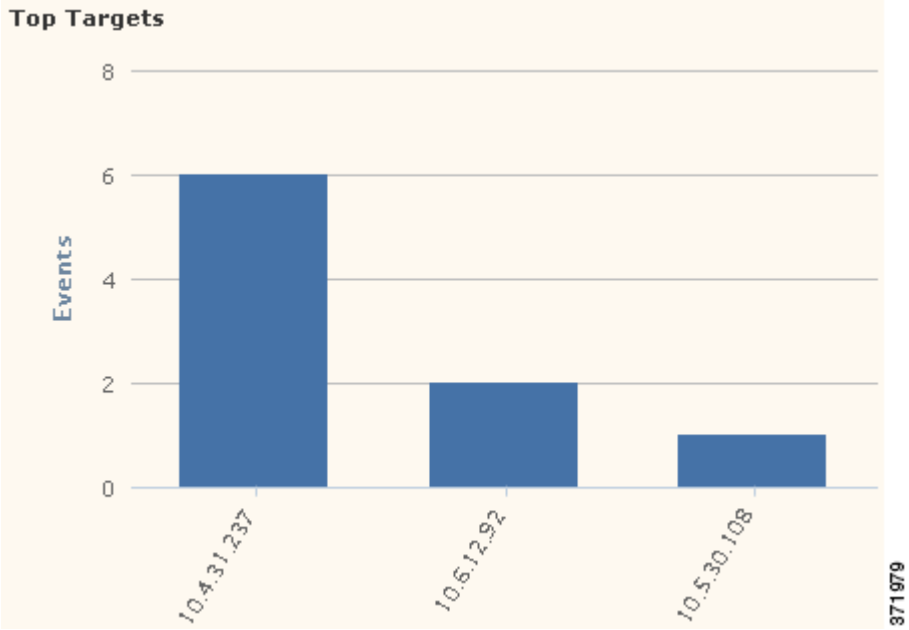
グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [Intrusion Events] 表から取得されます。

[Top Targets] グラフの表示

ライセンス：Protection

[Top Targets] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の（侵入イベントを発生させた接続で攻撃対象となった）上位の攻撃対象ホスト IP アドレスの侵入イベント数を表示します。



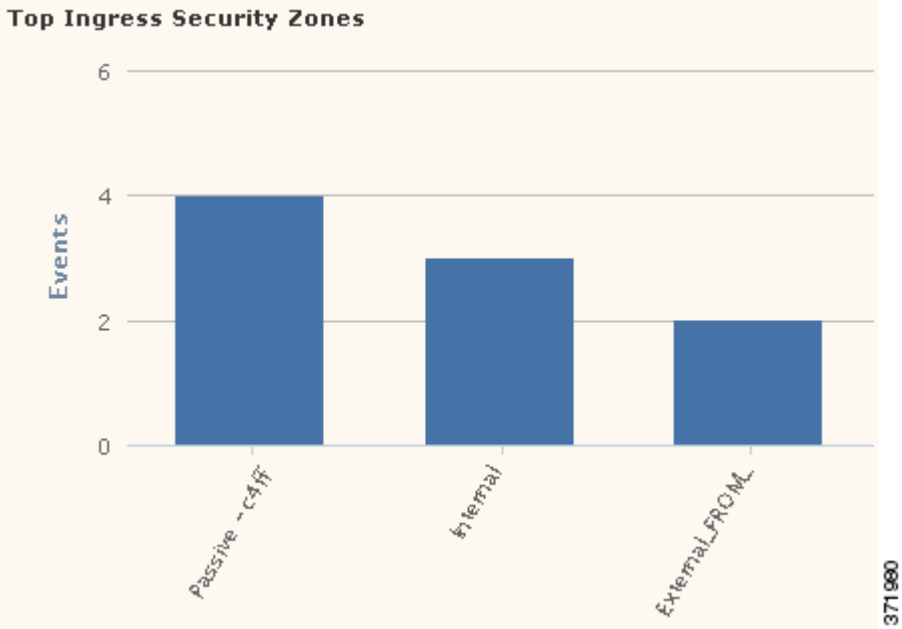
グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [Intrusion Events] 表から取得されます。

[Top Ingress/Egress Security Zones] グラフの表示

ライセンス：Protection

[Top Ingress/Egress Security Zones] グラフは棒グラフ形式であり、モニタ対象ネットワーク上で設定されている各セキュリティ ゾーン（グラフ設定に応じて入力または出力）に関連する侵入イベントの数を表示します。セキュリティ ゾーンの詳細については、セキュリティ ゾーンの操作（3-42 ページ）を参照してください。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、出力セキュリティ ゾーンのトラフィックだけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Egress] をクリックします。デフォルト ビューに戻すには [Ingress] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [Ingress] ビューに戻ることに注意してください。

このグラフのデータは主に [Intrusion Events] 表から取得されます。

必要に応じて、このグラフに入力(デフォルト)セキュリティ ゾーン情報または出力セキュリティ ゾーン情報のいずれかを表示するように設定できます。

[Intrusion Event Details List] の表示

ライセンス： Protection

[Intrusion Information] セクション下部に表示される [Event Details List] は、モニタ対象ネットワークで検出される各侵入イベントの分類、推定優先度、およびイベント数の情報を示す表です。イベントは、イベント数の降順でリストされます。

[Event Details List] 表はソートできませんが、表の項目をクリックして、その情報でフィルタリングまたはドリルダウンすることができます。この表のデータは主に [Intrusion Events] 表から取得されます。

[Files Information] セクションについて

ライセンス： ProtectionまたはMalware

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

Context Explorer の [Files Information] セクションには、6 つのインタラクティブ グラフが表示されます。これらのグラフは、モニタ対象ネットワーク上のファイルとマルウェア イベントの概要を示します。このうち 5 つのグラフには、ネットワーク トラフィックで検出されたファイルのファイル タイプ、ファイル名、マルウェアの性質、およびこれらのファイルを送信（アップロード）および受信（ダウンロード）するホストが表示されます。最後のグラフは、ネットワークで検出されたマルウェア脅威を表示し、FireAMPサブスクリプションがある場合はユーザが FireAMP コネクタをインストールしているエンドポイントで検出されたマルウェア脅威も表示します。

注　侵入情報でフィルタリングすると、[File Information] セクション全体が非表示になります。

[File Information] のグラフにネットワークベースのマルウェア データを組み込むには、Malware ライセンスを所有しており、マルウェア検出を有効にしている必要があることに注意してください。また、DC500 Defense Center および シリーズ 2 デバイスと Cisco NGIPS for Blue Coat X-Series は高度なマルウェア防御をサポートしていないため、DC500 Defense Center はこのデータを表示できず、シリーズ 2 デバイスと Cisco NGIPS for Blue Coat X-Series はこのデータを検出しないことに注意してください。マルウェア対策とファイル制御について（37-2 ページ）を参照してください。

[Files Information] セクションのグラフの詳細については、次のトピックを参照してください。

- [Top File Types] グラフの表示（56-26 ページ）
- [Top File Names] グラフの表示（56-27 ページ）
- [Files by Disposition] グラフの表示（56-28 ページ）
- [Top Hosts Sending Files] グラフ（56-29 ページ）
- [Top Hosts Receiving Files] グラフ（56-30 ページ）
- [Top Malware Detections] グラフの表示（56-31 ページ）

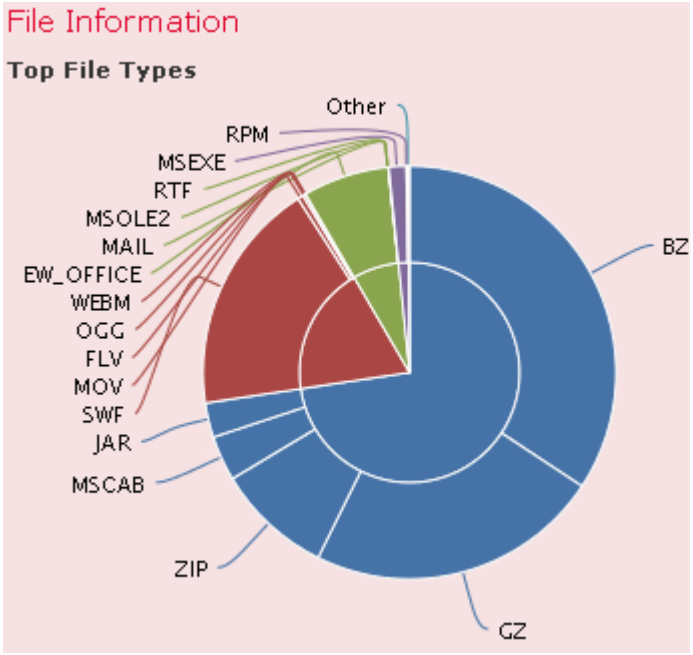
[Top File Types] グラフの表示

ライセンス： ProtectionまたはMalware

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

[Top File Types] グラフはドーナツ グラフ形式であり、ネットワーク トラフィックで検出されたファイル タイプ（外部リング）を、ファイル カテゴリ（内部リング）のグループごとの割合のビューで表示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフにネットワークベースのマルウェア データを組み込むには、Malware ライセンスを所有しており、マルウェア検出を有効にしている必要があることに注意してください。また、DC500 Defense Center および シリーズ 2 デバイスと Cisco NGIPS for Blue Coat X-Series は高度なマルウェア防御をサポートしていないため、DC500 Defense Center はこのデータを表示できず、シリーズ 2 デバイスと Cisco NGIPS for Blue Coat X-Series はこのデータを検出しないことに注意してください。マルウェア対策とファイル制御について（37-2 ページ）を参照してください。

このグラフのデータは主に [File Events] 表から取得されます。

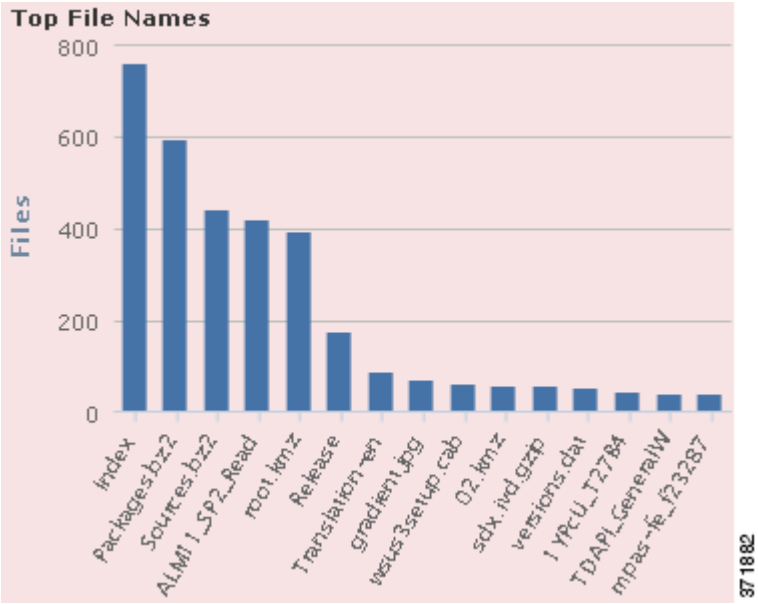
[Top File Names] グラフの表示

ライセンス： ProtectionまたはMalware

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

[Top File Names] グラフは棒グラフ形式であり、ネットワーク トラフィックで検出された上位の固有ファイル名の数を表示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフにネットワークベースのマルウェア データを組み込むには、Malware ライセンスを所有しており、マルウェア検出を有効にしている必要があることに注意してください。また、DC500 Defense Center および シリーズ 2 デバイスと Cisco NGIPS for Blue Coat X-Series は高度なマルウェア防御をサポートしていないため、DC500 Defense Center はこのデータを表示できず、シリーズ 2 デバイスと Cisco NGIPS for Blue Coat X-Series はこのデータを検出しないことに注意してください。マルウェア対策とファイル制御について (37-2 ページ) を参照してください。

このグラフのデータは主に [File Events] 表から取得されます。

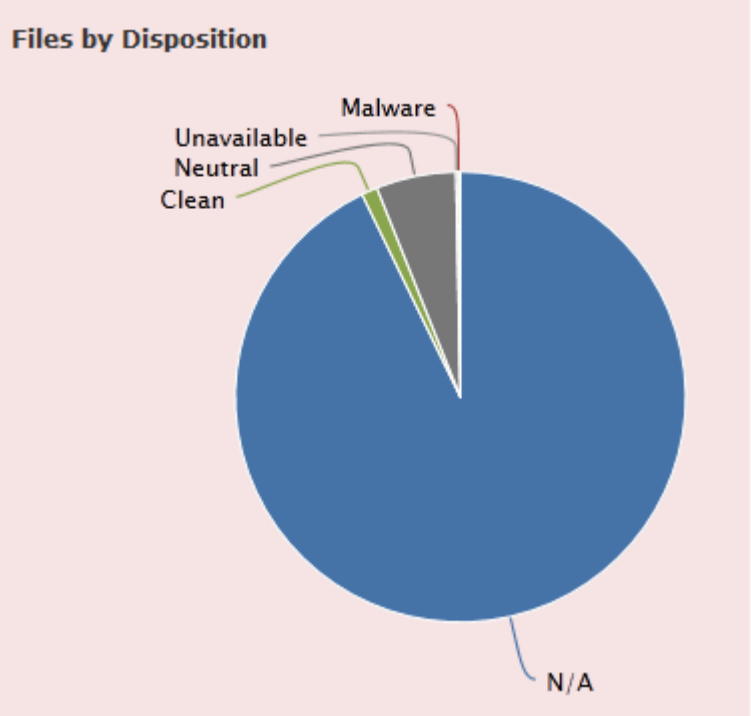
[Files by Disposition] グラフの表示

ライセンス： ProtectionまたはMalware

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

[Files by Disposition] グラフは円グラフ形式であり、ネットワーク トラフィックで検出されたファイルのマルウェアの性質の割合のビューを表示します。Defense Centerが Collective Security Intelligence クラウド 検索 (Malware ライセンスが必要) を実行したファイルのみが性質を持つことに注意してください。クラウド検索をトリガーしなかったファイルには、`N/A` という性質が設定されます。`Unavailable` という性質は、Defense Centerがマルウェア クラウド検索を実行できなかったことを示します。他の性質の説明についてはマルウェア対策とファイル制御について (37-2 ページ) を参照してください。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフにネットワークベースのマルウェア データを組み込むには、Malware ライセンスを所有しており、マルウェア検出を有効にしている必要があることに注意してください。また、DC500 Defense Center および シリーズ 2 デバイスと Cisco NGIPS for Blue Coat X-Series は高度なマルウェア防御をサポートしていないため、DC500 Defense Center はこのデータを表示できず、シリーズ 2 デバイスと Cisco NGIPS for Blue Coat X-Series はこのデータを検出しないことに注意してください。マルウェア対策とファイル制御について（37-2 ページ）を参照してください。

このグラフのデータは主に [File Events] 表から取得されます。

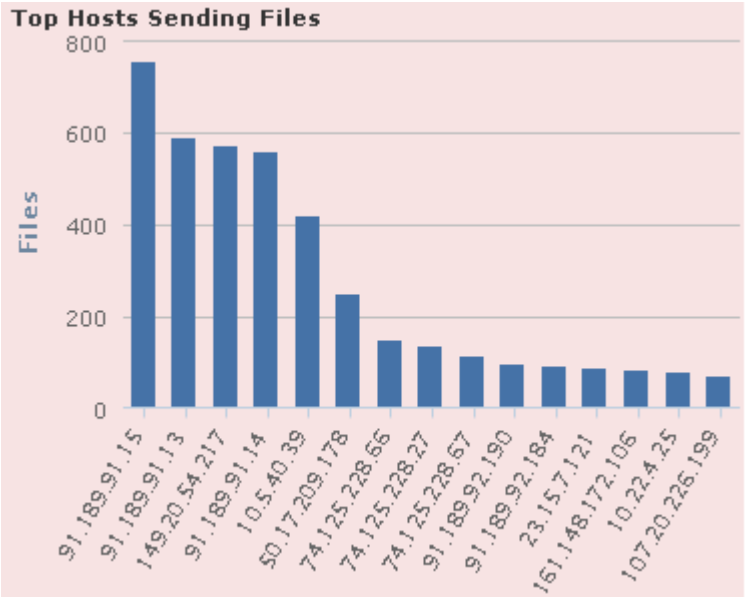
[Top Hosts Sending Files] グラフ

ライセンス： ProtectionまたはMalware

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

[Top Hosts Sending Files] グラフは棒グラフ形式であり、ネットワーク トラフィックで検出された、上位のファイル送信ホスト IP アドレスに対するファイルの数を表示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、マルウェアを送信するホストだけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Malware] をクリックします。デフォルトのファイルのビューに戻すには [Files] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトのファイルのビューに戻ることに注意してください。

このグラフにネットワークベースのマルウェア データを組み込むには、Malware ライセンスを所有しており、マルウェア検出を有効にしている必要があることに注意してください。また、DC500 Defense Center および シリーズ 2 デバイスと Cisco NGIPS for Blue Coat X-Series は高度なマルウェア防御をサポートしていないため、DC500 Defense Center はこのデータを表示できず、シリーズ 2 デバイスと Cisco NGIPS for Blue Coat X-Series はこのデータを検出しないことに注意してください。マルウェア対策とファイル制御について（37-2 ページ）を参照してください。

このグラフのデータは主に [File Events] 表から取得されます。

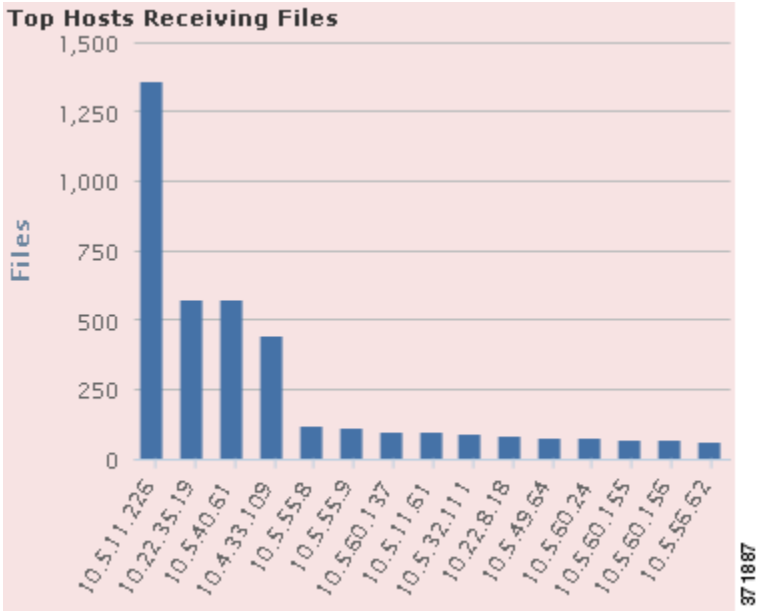
[Top Hosts Receiving Files] グラフ

ライセンス： ProtectionまたはMalware

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

[Top Hosts Receiving Files] グラフは棒グラフ形式であり、ネットワーク トラフィックで検出された、上位のファイル受信ホスト IP アドレスに対するファイルの数を表示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント

グラフに制約を適用して、マルウェアを受信するホストだけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Malware] をクリックします。デフォルトのファイルのビューに戻すには [Files] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトのファイルのビューに戻ることに注意してください。

このグラフにネットワークベースのマルウェア データを組み込むには、Malware ライセンスを所有しており、マルウェア検出を有効にしている必要があることに注意してください。また、DC500 Defense Center および シリーズ 2 デバイスと Cisco NGIPS for Blue Coat X-Series は高度なマルウェア防御をサポートしていないため、DC500 Defense Center はこのデータを表示できず、シリーズ 2 デバイスと Cisco NGIPS for Blue Coat X-Series はこのデータを検出しないことに注意してください。マルウェア対策とファイル制御について（37-2 ページ）を参照してください。

このグラフのデータは主に [File Events] 表から取得されます。

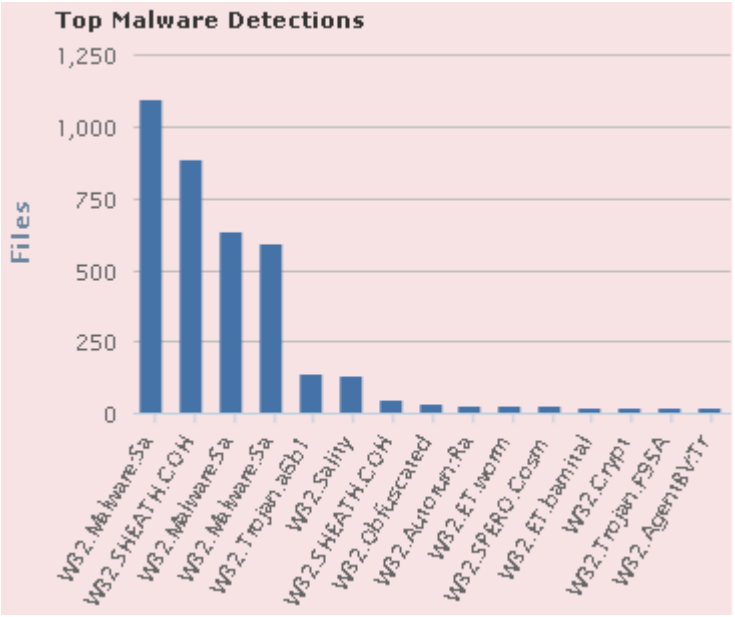
[Top Malware Detections] グラフの表示

ライセンス： ProtectionまたはMalware

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

[Top Malware Detections] グラフは棒グラフ形式であり、ネットワークで検出された上位のマルウェア脅威の数を表示します。また、FireAMPサブスクリプションがある場合は、ユーザが FireAMP コネクタをインストールしているエンドポイントで検出された上位のマルウェア脅威の数も表示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフにネットワークベースのマルウェア データを組み込むには、Malware ライセンスを所有しており、マルウェア検出を有効にしている必要があることに注意してください。また、DC500 Defense Center および シリーズ 2 デバイスと Cisco NGIPS for Blue Coat X-Series は高度なマルウェア防御をサポートしていないため、DC500 Defense Center はこのデータを表示できず、シリーズ 2 デバイスと Cisco NGIPS for Blue Coat X-Series はこのデータを検出しないことに注意してください。マルウェア対策とファイル制御について（37-2 ページ）を参照してください。

このグラフのデータは主に [File Events] 表と [Malware Events] 表から取得されます。

[Geolocation Information] セクションについて

ライセンス： FireSIGHT

サポートされる防御センター： DC500 を除くいずれか

Context Explorer の [Geolocation Information] セクションには、3 つのインタラクティブなドーナツ グラフが表示されます。これらのグラフは、モニタ対象ネットワークのホストがデータを交換している国の概要（イニシエータ国またはレスポンダ国ごとの固有接続数、送信元または宛先の国ごとの侵入イベント数、および送信側または受信側の国ごとのファイル イベント数）を示します。

[Geolocation Information] セクションのグラフの詳細については、次のトピックを参照してください。

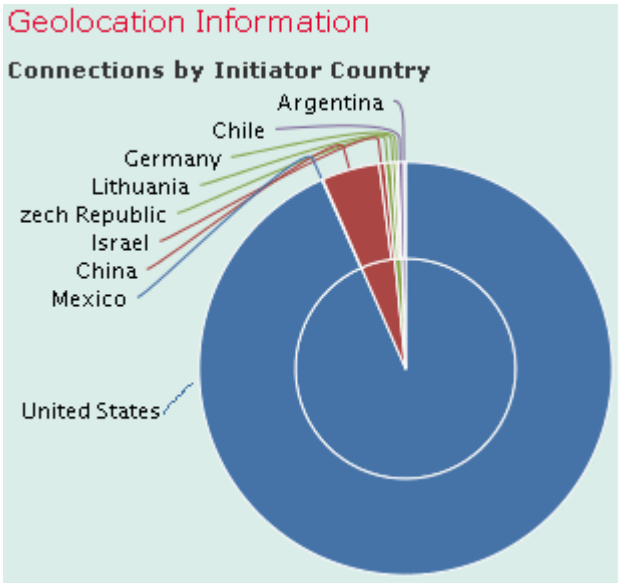
- [Connections by Initiator/Responder Country] グラフの表示（56-33 ページ）
- [Intrusion Events by Source/Destination Country] グラフの表示（56-33 ページ）
- [File Events by Sending/Receiving Country] グラフの表示（56-34 ページ）

[Connections by Initiator/Responder Country] グラフの表示

ライセンス： FireSIGHT

サポートされる防御センター： DC500 を除くいずれか

[Connections by Initiator/Responder Country] グラフはドーナツ グラフ形式であり、ネットワーク上での接続にイニシエータ（デフォルト）またはレスポンダとして関わる国の割合のビューを表示します。内側のリングでは、これらの国が大陸別にグループ化されています。位置情報については、地理情報の使用（58-23 ページ）を参照してください。接続データについては、接続およびセキュリティ インテリジェンス のデータの使用（39-1 ページ）を参照してください。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、接続でレスポンダとなっている国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Responder] をクリックします。デフォルト ビューに戻すには [Initiator] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの[Initiator] ビューに戻ることに注意してください。

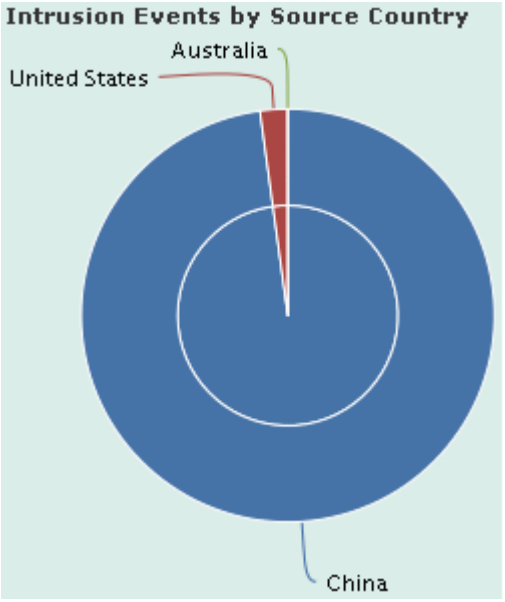
このグラフのデータは主に [Connection Summary Data] 表から取得されます。

[Intrusion Events by Source/Destination Country] グラフの表示

ライセンス： FireSIGHT

サポートされる防御センター： DC500 を除くいずれか

[Intrusion Events by Source/Destination Country] グラフはドーナツ グラフ形式であり、ネットワーク上の侵入イベントにイベントの送信元（デフォルト）または宛先として関わる国の割合のビューを表示します。内側のリングでは、これらの国が大陸別にグループ化されています。位置情報については、地理情報の使用（58-23 ページ）を参照してください。侵入イベント データについては、侵入イベントの操作（41-1 ページ）を参照してください。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、侵入イベントの宛先となっている国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Destination] をクリックします。デフォルト ビューに戻すには [Source] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [Source] ビューに戻ることに注意してください。

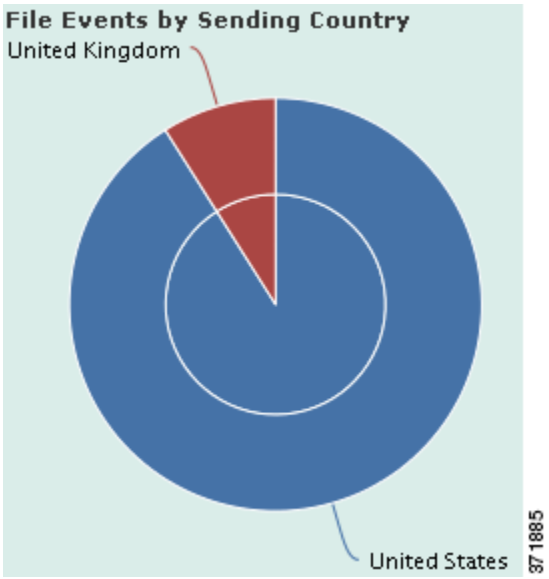
このグラフのデータは主に [Intrusion Events] 表から取得されます。

[File Events by Sending/Receiving Country] グラフの表示

ライセンス： FireSIGHT

サポートされる防御センター： DC500 を除くいずれか

[File Events by Sending/Receiving Country] グラフはドーナツ グラフ形式であり、ネットワーク上のファイル イベントでファイルの送信側（デフォルト）または受信側として検出された国の割合のビューを表示します。内側のリングでは、これらの国が大陸別にグループ化されています。位置情報については、地理情報の使用（58-23 ページ）を参照してください。ファイル イベント データについては、ファイル イベントの操作（40-8 ページ）を参照してください。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、ファイルを受信する国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Receiver] をクリックします。デフォルト ビューに戻すには [Sender] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [Sender] ビューに戻ることに注意してください。

このグラフのデータは主に [File Events] 表から取得されます。

[URL Information] セクションについて

ライセンス： FireSIGHTまたはURL Filtering

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

Context Explorer の [URL Information] セクションには、3 つのインタラクティブ グラフが表示されます。これらのグラフは、モニタ対象ネットワーク上のホストがデータを交換する URL の概要（URL に関連付けられているトラフィックおよび固有接続数を個々の URL、URL カテゴリ、および URL レピュテーションごとにソートしたもの）を示します。URL 情報でフィルタリングすることはできません。

注　侵入イベント情報でフィルタリングすると、[URL Information] セクション全体が非表示になります。

URL フィルタリング グラフに URL カテゴリとレピュテーション のデータを組み込むには、URL Filtering ライセンスを所有しており、URL Filtering を有効にしている必要があることに注意してください。また、DC500のDefense Centerと シリーズ 2 デバイスはいずれもレピュテーションとカテゴリによる URL フィルタリングをサポートしていないため、DC500のDefense Centerはこのデータを表示できず、シリーズ 2 デバイスはこのデータを検出しないことにも注意してください。URL のブロッキング（16-9 ページ）を参照してください。

[URL Information] セクションのグラフの詳細については、次のトピックを参照してください。

- [Traffic by URL] グラフの表示（56-36 ページ）
- [Traffic by URL Category] グラフの表示（56-37 ページ）
- [Traffic by URL Reputation] グラフの表示（56-38 ページ）

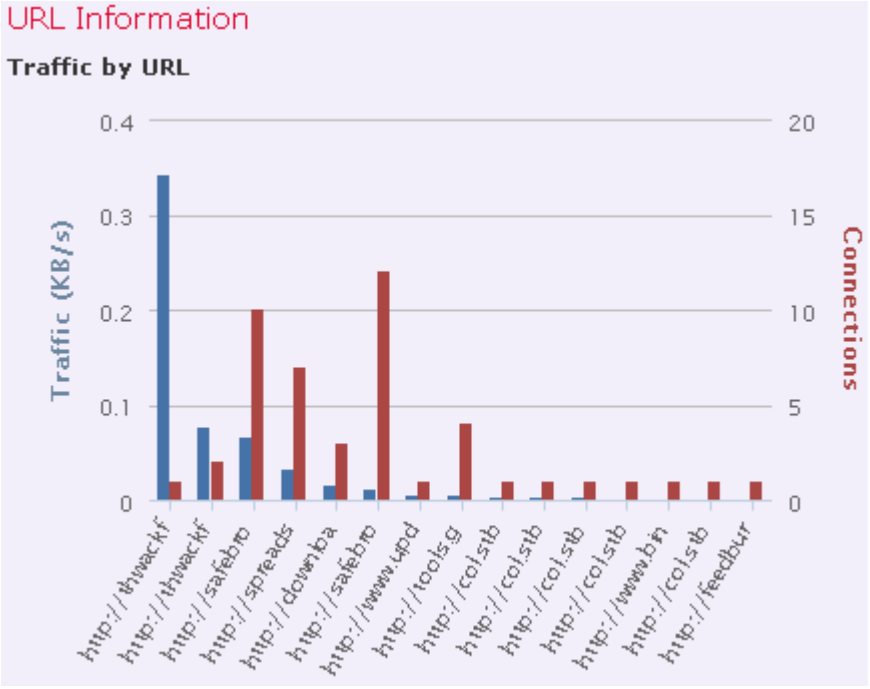
[Traffic by URL] グラフの表示

ライセンス： FireSIGHTまたはURL Filtering

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

[Traffic by URL] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最も要求される上位 15 の URL のネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。リストされた URL ごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンされます。

注　侵入イベントの情報でフィルタリングすると、[Traffic by URL] グラフは非表示になります。

URL フィルタリング グラフに URL カテゴリとレピュテーション のデータを組み込むには、URL Filtering ライセンスを所有しており、URL Filtering を有効にしている必要があることに注意してください。また、DC500のDefense Centerと シリーズ 2 デバイスはいずれもレピュテーションとカテゴリによる URL フィルタリングをサポートしていないため、DC500のDefense Centerはこのデータを表示できず、シリーズ 2 デバイスはこのデータを検出しないことにも注意してください。クラウド通信の有効化（64-30 ページ）を参照してください。

このグラフのデータは主に [Connection Events] 表から取得されます。

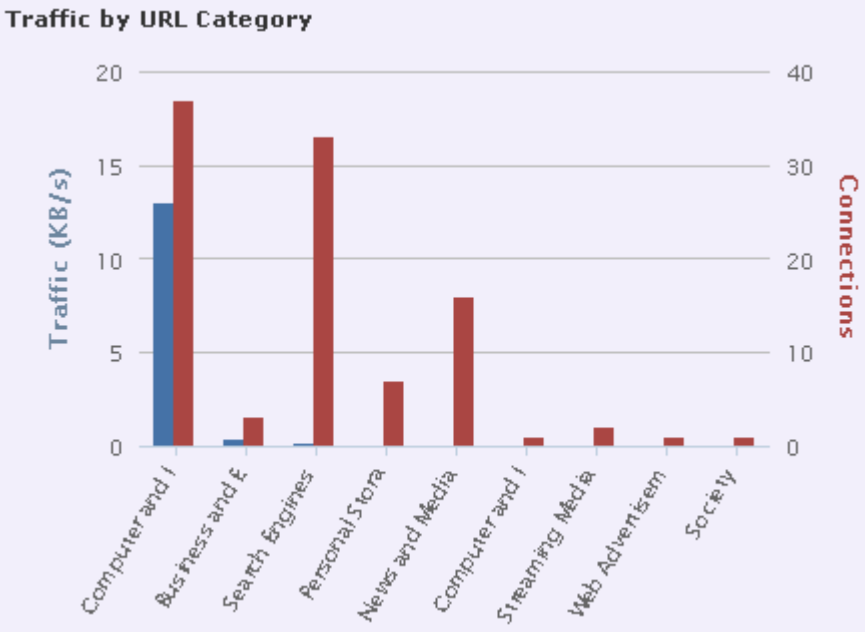
[Traffic by URL Category] グラフの表示

ライセンス： URL Filtering

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

[Traffic by URL Category] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最も要求される URL カテゴリ（`Search Engines`、`Streaming Media` など）のネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。リストされた URL カテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンされます。

注　侵入イベントの情報でフィルタリングすると、[Traffic by URL Category] グラフは非表示になります。

URL フィルタリング グラフに URL カテゴリとレピュテーション のデータを組み込むには、URL Filtering ライセンスを所有しており、URL Filtering を有効にしている必要があることに注意してください。また、DC500のDefense Centerと シリーズ 2 デバイスはいずれもレピュテーションとカテゴリによる URL フィルタリングをサポートしていないため、DC500のDefense Centerはこのデータを表示できず、シリーズ 2 デバイスはこのデータを検出しないことにも注意してください。レピュテーション ベースの URL ブロックの実行（16-11 ページ）を参照してください。

このグラフのデータは主に [URL Statistics] 表と [Connection Events] 表から取得されます。

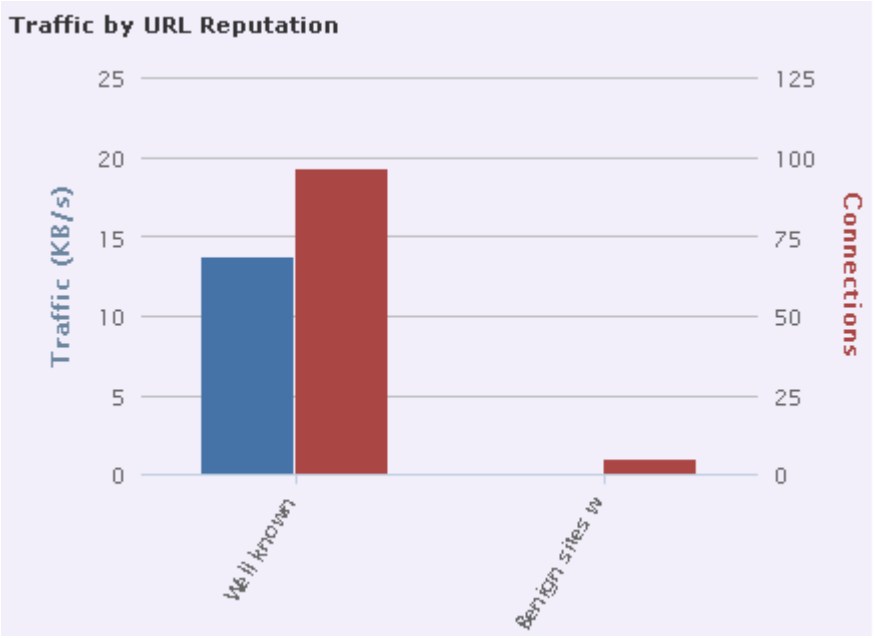
[Traffic by URL Reputation] グラフの表示

ライセンス： URL Filtering

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

[Traffic by URL Reputation] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最も要求される URL レピュテーション グループ（`Well known`、`Benign sites with security risks` など）のネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。リストされた URL レピュテーションごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンされます。

注　侵入イベントの情報でフィルタリングすると、[Traffic by URL Reputation] グラフは非表示になります。

URL フィルタリング グラフに URL カテゴリとレピュテーション のデータを組み込むには、URL Filtering ライセンスを所有しており、URL Filtering を有効にしている必要があることに注意してください。また、DC500のDefense Centerと シリーズ 2 デバイスはいずれもレピュテーションとカテゴリによる URL フィルタリングをサポートしていないため、DC500のDefense Centerはこのデータを表示できず、シリーズ 2 デバイスはこのデータを検出しないことにも注意してください。レピュテーション ベースの URL ブロックの実行（16-11 ページ）を参照してください。

このグラフのデータは主に [URL Statistics] 表と [Connection Events] 表から取得されます。

Context Explorer の更新

ライセンス：FireSIGHT

Context Explorer は、表示情報を自動的に更新しません。新しいデータを組み込むには、Explorer を手動で更新する必要があります。

（ブラウザ プログラムの更新または Context Explorer から外部へ移動した後に戻る操作などにより）Context Explorer 自体をリロードすると、すべての表示情報が更新されますが、セクション設定（Ingress/Egress グラフや [Application Information] セクションなど）に対して行った変更は保持されず、また、読み込みに時間がかかることがある点に注意してください。

Context Explorer の更新方法：

アクセス：Admin/Any Security Analyst

ステップ 1　Context Explorer の右上にある [Reload] をクリックします。

Explorer が更新され、選択した時間範囲内の最新情報が表示されます。更新が完了するまでは [Reload] ボタンがグレー表示になることに注意してください。

Context Explorer の時間範囲の設定

ライセンス：FireSIGHT

過去 1 時間（デフォルト）から過去 1 年までの期間を反映するように、Context Explorer の時間範囲を設定できます。時間範囲を変更しても、Context Explorer は変更を反映するために自動的に更新されないことに注意してください。新しい時間範囲を適用するには、Explorer を手動で更新する必要があります。

時間範囲の変更は、Context Explorer から外部に移動したり、ログイン セッションを終了したりしても維持されます。

Context Explorer の時間範囲を変更するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

ステップ 1　[Show the last] ドロップダウンリストから時間範囲を選択します。

ステップ 2　オプションで、新しい時間範囲のデータを表示するには、[Reload] をクリックします。

Context Explorer のすべてのセクションが更新され、新しい時間範囲が反映されます。

ヒント　[Apply Filters] をクリックすると、時間範囲の更新が適用されます。

Context Explorer のセクションの最小化および最大化

ライセンス：FireSIGHT

Context Explorer では 1 つ以上のセクションを最小化して非表示にできます。これは、特定のセクションだけを強調する場合や、ビューをシンプルにしたい場合に便利です。[Traffic and Intrusion Event Counts Time] グラフは最小化できません。

Context Explorer のセクションでは、ページを更新したり、アプライアンスからログアウトしたりしても、設定した最小化または最大化の状態が維持されることに注意してください。

Context Explorer のセクションを最小化する方法：

アクセス：Admin/Any Security Analyst

ステップ 1　セクションのタイトル バーの最小化アイコン（ − ）をクリックします。

Context Explorer のセクションを最大化する方法：

アクセス：Admin/Any Security Analyst

ステップ 1　最小化されているセクションのタイトル バーの最大化アイコン（ □ ）をクリックします。

Context Explorer データのドリルダウン

ライセンス：機能によって異なる

Context Explorer で許容されている詳細レベルよりもさらに詳細にグラフを調べたりデータをリストしたりするには、当該データのテーブル ビューにドリルダウンします。（[Traffic and Intrusion Events over Time] グラフではドリル ダウンできないことに注意してください。）たとえば、[Traffic by Source IP] グラフの IP アドレスでドリルダウンすると、[Connection Events] 表の [Connections with Application Details] ビューが表示されます。このビューには、選択した送信元 IP アドレスに関連するデータのみが表示されます。

調べるデータのタイプに応じて、コンテキスト メニューに追加のオプションが表示されることがあります。特定の IP アドレスに関連付けられているデータ ポイントの場合、選択した IP アドレスのホストまたは whois 情報を表示するためのオプションが表示されます。特定のアプリケーションに関連付けられているデータ ポイントの場合、選択したアプリケーションに関するアプリケーション情報を表示するためのオプションが表示されます。特定のユーザに関連付けられているデータ ポイントの場合、ユーザのユーザ プロファイル ページを表示するためのオプションが表示されます。侵入イベントのメッセージに関連付けられているデータ ポイントの場合、そのイベントに関連する侵入ルールに関するルール ドキュメントを表示するオプションが表示されます。特定の IP アドレスに関連付けられているデータ ポイントの場合、そのアドレスをブラックリストまたはホワイトリストに追加するためのオプションが表示されます。

データのドリルダウンに使用するコンテキスト メニューには、そのデータをフィルタリングするためのオプションも含まれています。フィルタリングの詳細については、Context Explorer でのフィルタ操作（56-42 ページ）を参照してください。

Context Explorer でデータをドリルダウンする方法：

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Context Explorer] を選択します。

Context Explorer が表示されます。

ステップ 2　[Traffic and Intrusion Events over Time] 以外の任意のセクションで、調査するデータ ポイントをクリックします。

コンテキスト メニュー ポップアップ ウィンドウが表示されます。

ステップ 3　選択するデータ ポイントに応じて、表示されるオプションが異なります。

- テーブル ビューでこのデータの詳細を表示するには、[Drill into Analysis] を選択します。

  新しいウィンドウが開き、選択したデータの詳細なテーブル ビューが表示されます。

- 特定の IP アドレスに関連付けられているデータ ポイントを選択している場合に、関連するホストに関する詳細情報を参照するには、[View Host Information] を選択します。

  新しいウィンドウが開き、選択した IP アドレスのホスト プロファイル ページが表示されます。ホスト属性とホスト プロファイルの詳細については、ホスト プロファイルの使用（49-1 ページ）を参照してください。

- 特定の IP アドレスのデータ ポイントを選択している場合に、そのアドレスで whois 検索を行うには、[Whois] を選択します。

  新しいウィンドウが開き、選択した IP アドレスの whois クエリの結果が表示されます。

- 特定のアプリケーションに関連付けられているデータ ポイントを選択している場合に、そのアプリケーションに関する詳細情報を参照するには、[View Application Information] を選択します。

  新しいウィンドウが開き、選択したアプリケーションの情報が表示されます。アプリケーション属性の詳細については、アプリケーション検出について（45-11 ページ）を参照してください。

- 特定のユーザに関連付けられているデータ ポイントを選択している場合に、そのユーザに関する詳細情報を参照するには、[View User Information] を選択します。

  新しいウィンドウが開き、選択したユーザのユーザ プロファイル ページが表示されます。ユーザ詳細について詳しくは、ユーザの詳細とホストの履歴について（50-68 ページ）を参照してください。

- 特定の侵入イベント メッセージに関連付けらているデータ ポイントを選択している場合に、関連する侵入ルールに関する詳細情報を参照するには、[View Rule Documentation] を選択します。

  新しいウィンドウが開き、選択したイベントに関連するルール詳細ページが表示されます。侵入ルール詳細について詳しくは、ルール詳細の表示（32-5 ページ）を参照してください。

- 特定の IP アドレスに関連付けられているデータ ポイントを選択している場合に、Security Intelligence グローバル ブラックリストまたはホワイトリストにその IP アドレスを追加するには、[Blacklist Now] または [Whitelist Now] のいずれか該当するオプションを選択してください。表示されるポップアップ ウィンドウで選択内容を確認します。

IP アドレスがブラックリストまたはホワイトリストに登録されます。詳細については、グローバル ホワイトリストおよびブラックリストの操作（3-7 ページ）を参照してください。

Security Intelligence データをサポートしていない DC500 Defense Centerでは、これらのオプションは表示されません。

Context Explorer でのフィルタ操作

ライセンス： FireSIGHT

Context Explorer に最初に表示される基本的で広範なデータをフィルタリングして、ネットワーク上のアクティビティのより詳細な状況を把握することができます。フィルタは URL 情報以外のすべての種類のFireSIGHT データに対応し、除外と包含がサポートされており、Context Explorer のグラフ データ ポイントをクリックするだけですぐに適用でき、Explorer 全体に反映されます。ネットワークおよび組織のニーズに合った独自の設定にするために、一度に最大 20 個のフィルタを適用できます。適用するフィルタは Context Explorer URL に反映されるため、有用なフィルタ セットはブラウザ プログラムで後で使用できるようにブックマークしておくことができます。

Context Explorer でのフィルタの使用法については、次のトピックを参照してください。

- フィルタの追加および適用（56-42 ページ）
- コンテキスト メニューを使用したフィルタの作成（56-46 ページ）
- フィルタのブックマーク（56-47 ページ）

フィルタの追加および適用

ライセンス： 機能によって異なる

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

Context Explorer データにフィルタを追加する方法はいくつかあります。

- [Add Filter] ウィンドウを使用する
- コンテキスト メニュー ポップアップ ウィンドウを使用する（Explorer のデータ ポイントを選択する場合）
- Context Explorer アイコン（ ）または特定の詳細ビュー ページ（[Application Detail]、[Host Profile]、[Rule Detail]、[User Profile]）に表示されるテキスト リンクを使用する。これらのリンクをクリックすると、Context Explorer が自動的に開き、詳細ビュー ページの当該データに基づいて Context Explorer がフィルタリングされます。たとえば、ユーザ `jenkins` のユーザ詳細ページで [Context Explorer] リンクをクリックすると、Explorer にはそのユーザに関連するデータだけが表示されます。

ここでは、[Add Filter] ウィンドウでフィルタを新規に作成する方法について説明します。コンテキスト メニューを使用して Context Explorer のグラフとリスト データからクイック フィルタを作成する方法については、コンテキスト メニューを使用したフィルタの作成（56-46 ページ）を参照してください。

Context Explorer の左上にある [Filters] の下のプラス アイコン（ ）をクリックすると表示される [Add Filter] ウィンドウには、[Data Type] と [Filter] の 2 つのフィールドだけが表示されます。

[Data Type] ドロップダウンリストには、Context Explorer に制約を適用するために使用できる多数の FireSIGHT システム データ タイプが含まれています。データ タイプの選択後に、そのタイプの固有の値を [Filter] フィールドに入力します（たとえば、[Continent] タイプの場合は値 Asia など）。ユーザ支援のため、[Filter] フィールドでは、選択したデータ タイプのさまざまな値の例がグレー表示で示されます。（フィールドにデータを入力すると、これらは消去されます。）

次の表に、フィルタとして使用できるデータ タイプと、各データ タイプの例と説明を示します。DC500 Defense Center では、サポートされていない機能のデータは表示されず、シリーズ 2 デバイスおよび Cisco NGIPS for Blue Coat X-Series ではサポートされていない機能のデータは検出されないことに注意してください。シリーズ 2 デバイスおよび Cisco NGIPS for Blue Coat X-Series の機能の要約については、各デバイス モデルでサポートされるアクセス制御機能 の表を参照してください。

表 56-2　フィルタ データ タイプ

タイプ	値の例	定義
Access Control Action	Allow、Block	トラフィックを許可またはブロックするためにアクセス制御ポリシーにより実行されるアクション
Application Category	web browser、email	アプリケーションの主要機能の一般的な分類
Application Name	Facebook、HTTP	アプリケーションの名前
Application Risk	Very High、Medium	アプリケーションの推定セキュリティ リスク
Application Tag	encrypts communications、sends mail	アプリケーションに関する追加情報。アプリケーションには任意の数のタグを使用できます（タグを使用しないことも可能です）。
Application Type	Client、Web Application	アプリケーション タイプ（アプリケーション プロトコル、クライアント、または Web アプリケーション）
Business Relevance	Very Low、High	（娯楽ではない）ビジネス アクティビティに対するアプリケーションの推定関連度
Continent	North America、Asia	モニタ対象ネットワークで検出されたルーティング可能な IP アドレスに関連付けられている大陸
Country	Canada、Japan	モニタ対象ネットワークで検出されたルーティング可能な IP アドレスに関連付けられている国
デバイス	device1.example.com、192.168.1.3	モニタ対象ネットワーク上のデバイスの名前または IP アドレス
Event Classification	Potential Corporate Policy Violation、Attempted Denial of Service	侵入イベントの簡単な説明。侵入イベントをトリガーしたルール、デコーダ、またはプリプロセッサにより決定されます。
イベント メッセージ	dns response、P2P	イベントによって生成されるメッセージ。イベントをトリガーしたルール、デコーダ、またはプリプロセッサにより決定されます。
File Disposition	Malware、Clean	Defense Center によるマルウェア クラウド検索の実行対象ファイルの性質。この性質は、クラウドにより決定されます。
File Name	Packages.bz2	ネットワーク トラフィックで検出されたファイルの名前
File SHA256	任意の 32 ビット文字列	Defense Centerによるマルウェア クラウド検索の実行対象ファイルの SHA-256 ハッシュ値

表 56-2　フィルタ データ タイプ(続き)

タイプ	値の例	定義
File Type	GZ、SWF、MOV	ネットワーク トラフィックで検出されたファイルのタイプ
File Type Category	Archive、Multimedia、Executables	ネットワーク トラフィックで検出されたファイルのタイプの一般カテゴリ
IP Address	192.168.1.3、2001:0db8:85a3::0000/24	IPv4 または IPv6 のアドレス、アドレス範囲、またはアドレス ブロック IP アドレスを検索すると、そのアドレスが送信元または宛先のいずれかになっているイベントが返されることに注意してください。
Impact Level	Impact Level 1、Impact Level 2	モニタ対象ネットワークでのイベントの推定影響レベル
Inline Result	dropped、would have dropped	トラフィックがドロップされたか、ドロップされた可能性があるか、またはシステムによりトラフィックが処理されていないかのいずれかです。
IOC Category	High Impact Attack、Malware Detected	トリガーとして使用された侵害の兆候(IOC)イベントのカテゴリ
IOC Event Type	exploit-kit、malware-backdoor	特定の侵害の兆候(IOC)に関連付けられている ID。その兆候をトリガーしたイベントを示します。
Malware Threat Name	W32.Trojan.a6b1	マルウェア脅威の名前
OS Name	Windows、Linux	オペレーティング システム名
OS Version	XP、2.6	オペレーティング システムの特定のバージョン
プライオリティ	high、low	イベントの推定緊急度
Security Intelligence Category	Malware、Spam	Security Intelligence により判別される危険なトラフィックのカテゴリ
Security Zone	My Security Zone、Security Zone X	トラフィックが分析されたインターフェイスのセット。インライン展開の場合は、トラフィックが通過するインターフェイスのセット。
SSL	yes、no	SSL 暗号化トラフィック または TLS 暗号化トラフィック
User	wsmith、mtwain	モニタ対象ネットワーク上のホストにログインしたユーザの ID

[Filter] フィールドには、イベント検索と同様に、* や ! などの特殊検索パラメータを入力できます。フィルタ パラメータの前に ! 記号を付けることで排他的なフィルタを作成できます。FireSIGHT システムで一般にサポートされている検索制約の詳細については、検索でのワイルドカードと記号の使用(60-5 ページ)を参照してください。

複数のフィルタがアクティブな場合、同じデータ タイプの値は OR 検索条件として扱われます。つまり、いずれか 1 つの値と一致するデータがすべて表示されます。異なるデータ タイプの値は AND 検索条件として扱われます。つまり、データは各フィルタ データ タイプの 1 つ以上の値と一致する必要があります。たとえば、Application: 2channel、Application: Reddit、および User: edickinson というフィルタ セットで表示されるデータは、ユーザ edickinson に関連付けられており、**かつ(AND)**アプリケーション 2channel **または(OR)**アプリケーション Reddit に関連付けられている必要があります。

フィルタのデータ タイプと値を確認した後で、新しいフィルタのデータ タイプと値を示すフィルタ ウィジェットがページの左上に表示されます。

複数のフィルタを設定してから適用したい場合もあるため、また Context Explorer ではすべてのセクションが完全にリロードされるまでに時間がかかることがあるため、追加したフィルタは自動的には適用されません。フィルタを適用するには、[Apply Filters] をクリックする必要があります。設定されたがまだ適用されていないフィルタはぼかし表示されます。一度に最大 20 個のフィルタを適用できます。また、フィルタのウィジェットで削除アイコン(✖)をクリックして、個々のフィルタを削除することもできます。すべてのフィルタを一括削除するには、[Clear] ボタンをクリックします。

ファイル タイプの中には、相互に互換性がないタイプがあることに注意してください。たとえば、侵入イベント関連のフィルタ（**Device** や **Inline Result** など）を、接続イベント関連フィルタ（**Access Control Action** など）と同時に適用することはできません。これは、システムでは接続イベント データを侵入イベント データによってソートできないためです。互換性のないフィルタの同時適用はシステムによって自動的に防止されます。互換性の問題が存在する場合、より後に適用されたほうのフィルタ タイプと互換性のないタイプのフィルタは非表示になります。

表示されるデータは、管理対象デバイスのライセンスと導入方法、データを提供する機能を設定するかどうか、および シリーズ 2 アプライアンスの場合はデータを提供する機能をサポートしているかどうかなどの要因に応じて異なることに注意してください。たとえば DC500 のDefense Centerと シリーズ 2 デバイスはいずれもカテゴリまたはレピュテーションによる URL フィルタリングをサポートしていないため、DC500 のDefense Centerではこの機能のデータは表示されず、シリーズ 2 デバイスではこのデータが検出されません。

[Add Filter] ウィンドウで新しいフィルタを作成するには、次の手順を実行します。

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Context Explorer] を選択します。

Context Explorer が表示されます。

ステップ 2　右上にある [Filter] の下で、プラス アイコン(✚)をクリックします。

[Add Filter] ポップアップ ウィンドウが表示されます。

ステップ 3　[Data Type] ドロップダウンリストから、フィルタリングの条件として使用するデータ タイプを選択します。

[Filter] フィールドに、そのデータ タイプの値の例が取り込まれます。

ステップ 4　[Filter] フィールドに、フィルタリングの条件として使用するデータ タイプ値を入力します。

ステップ 5　[OK] をクリックします。

フィルタが追加されます。Context Explorer が再び表示され、対応するフィルタ ウィジェットが表示されます。

ステップ 6　オプションで、前述の手順を繰り返し、必要なフィルタ セットが設定されるまで、フィルタを追加します。Context Explorer は自動的に更新されないため、フィルタを追加してもフィルタは適用されないことに注意してください。

ステップ 7　[Apply Filters] をクリックします。

フィルタが適用され、Context Explorer が更新され、フィルタリングされたデータが反映されます。

フィルタを削除する方法:

アクセス: Admin/Any Security Analyst

ステップ 1　任意のフィルタ ウィジェットの削除アイコン(✖)をクリックします。

フィルタが削除されます。

すべてのフィルタをクリアする方法:

アクセス: Admin/Any Security Analyst

ステップ 1　フィルタ ウィジェットの右に表示される [Clear] ボタンをクリックします。

すべてのフィルタがクリアされます。

フィルタが作成されていない場合、このボタンが表示されないことに注意してください。

コンテキスト メニューを使用したフィルタの作成

ライセンス: FireSIGHT

Context Explorerのグラフとリスト データを詳しく調べるときに、データ ポイントをクリックし、コンテキスト メニューを使用してそのデータに基づいてフィルタ(包含または除外)を簡単に作成できます。コンテキスト メニューを使用して、Application、User、または Intrusion Event Message データ タイプの情報、あるいは任意の個別ホストでフィルタリングする場合、フィルタ ウィジェットには、そのデータ タイプの該当する詳細ページ(アプリケーション データの場合は [Application Detail] など)にリンクするウィジェット情報アイコンが表示されます。URL データではフィルタリングできないことに注意してください。

特定のグラフまたはリストのデータを詳しく調査する場合にもコンテキスト メニューを使用できます。詳細については、Context Explorer データのドリルダウン(56-40 ページ)を参照してください。

コンテキスト メニューからフィルタを作成する方法:

アクセス: Admin/Any Security Analyst

ステップ 1　[Analysis] > [Context Explorer] を選択します。

Context Explorer が表示されます。

ステップ 2　[Traffic and Intrusion Events over Time] セクションと URL データを含むセクション以外の Explorer セクションで、フィルタリングするデータ ポイントをクリックします。

コンテキスト メニュー ポップアップ ウィンドウが表示されます。

ステップ 3　次の 2 つのオプションから選択できます。

- このデータにフィルタを追加するには、[Add Filter] をクリックします。

  フィルタが追加され、そのウィジェットが左上に表示されます。
- このデータに除外フィルタを追加するには、[Add Exclude Filter] をクリックします。このフィルタが適用されると、除外された値に関連付けられて**いない**すべてのデータが表示されます。

フィルタが追加され、そのウィジェットが左上に表示されます。除外フィルタでは、フィルタ値の前に感嘆符が表示されます。

フィルタの詳細を表示する方法：

アクセス：Admin/Any Security Analyst

ステップ 1　該当するフィルタ ウィジェットの情報アイコン( )をクリックします。

新しいウィンドウが開き、フィルタのデータ タイプに関連する詳細ページが表示されます。

フィルタのブックマーク

ライセンス：FireSIGHT

フィルタは、必要とする正確な FireSIGHT データ コンテキストをいつでも取得できるシンプルかつ俊敏性に優れたツールとして機能します。永続的に設定するものではなく、Context Explorer から外部に移動するか、セッションを終了すると消去されます。ただし、組織では特定のフィルタの組み合わせを頻繁に使用することがあります。フィルタ設定を後で使用できるように維持するには、そのフィルタを適用した Context Explorer のブラウザ ブックマークを作成できます。適用されるフィルタは Context Explorer ページ URL に組み込まれているので、そのページのブックマークを読み込むと、対応するフィルタも読み込まれます。

レポートの操作

FireSIGHT システムは柔軟なレポート作成システムを提供しており、Defense Centerで表示されるイベント ビューやダッシュボードを使用して、複数のセクションがあるレポートを短時間で簡単に生成できます。独自のカスタム レポートを最初から設計することもできます。レポート作成は、Defense Centerでのみ使用可能です。

レポートは、通信しようとしている内容が含まれるドキュメント ファイルで、PDF、HTML、または CSV 形式になります。レポート テンプレートは、データの検索設定とレポートおよびそのセクションの形式を指定します。FireSIGHT システムには強力なレポート デザイナが含まれていて、レポート テンプレートの設計を自動的に行います。Web インターフェイスに表示されるイベント ビュー テーブルやダッシュボードのグラフィックの内容を複製できます。

レポート テンプレートは必要な数だけ作成できます。各レポート テンプレートは、レポートの個々のセクションを定義し、レポートの内容を作成するデータベース検索設定を指定し、表示形式（表、グラフ、詳細表示など）とタイム フレームも指定します。さらに、テンプレートでは、表紙や目次の情報、ドキュメント ページに見出しとフッターを付けるかどうかなどのドキュメント属性も指定します（PDF 形式のレポートでのみ指定可能）。レポート テンプレートを 1 つの設定パッケージ ファイルとしてエクスポートし、別のDefense Centerにインポートして再使用できます。

テンプレートに入力パラメータを組み込んで実用性を向上させることができます。入力パラメータを使用すると、同じレポートを用途に合わせて異なる様々なレポートに変えることができます。入力パラメータのあるレポートを生成するときには、生成プロセスで各入力パラメータの値を入力するよう求められます。ユーザが入力する値は、レポートの内容をその 1 回だけ制約します。たとえば、侵入イベントのレポートを作成する検索の宛先 IP フィールドに入力パラメータを使用できます。この場合、レポートの生成時に、宛先 IP アドレスの入力を求められたときに特定の部門のネットワーク セグメントを指定できます。その結果、この特定の部門に関する情報だけが含まれるレポートが生成されます。

レポートやレポート テンプレートの詳細については、次の項を参照してください。

- レポート テンプレートについて（57-2 ページ）
- レポート テンプレートの作成と編集（57-4 ページ）
- レポートの生成と表示（57-28 ページ）
- レポート生成オプションの使用法（57-30 ページ）
- レポート テンプレートとレポート ファイルの管理（57-33 ページ）

レポート テンプレートについて

ライセンス： すべて

FireSIGHT システムのレポート作成機能によって、Defense Centerからイベント ビュー、ダッシュボード、またはワークフローの内容をすばやくキャプチャして、レポート形式で表示できます。レポート テンプレートを使用して、レポートの各セクション内のデータの内容と形式や、レポート ファイルのドキュメント属性（表紙、目次、ページ 見出し、ページ フッター）を定義します。レポートの生成後、削除しない限りテンプレートは再利用可能な状態になります。

レポートには、1 つ以上の情報セクションが含まれます。個々のセクションごとに形式（テキスト、表、またはグラフ）を選択します。セクションの形式の選択内容によっては、組み込めるデータが制約される場合があります。たとえば、円グラフの形式を使用すると、特定の表に時間ベースの情報を表示できません。いつでもセクションのデータの基準や形式を変更して、表示を最適にすることができます。

定義済みイベント ビューのレポートの初期設計をベースにするか、定義済みのダッシュボード、ワークフロー、または要約から内容をインポートして設計を開始できます。空のテンプレート シェルから始めて、1 つずつセクションを追加したり属性を定義したりすることもできます。

レポート テンプレートのすべてのセクションには、タイトル バーと、セクションの内容や外観を制御する各種の属性フィールドがあります。詳細については、次の説明を参照してください。

- レポート セクションのタイトル バーの要素表
- レポート セクションのフィールド表

次の表に、テンプレート セクションごとのタイトル バー上のコントロールについて説明します。

表 57-1　　レポート セクションのタイトル バーの要素

属性	定義
セクション タイトル	レポートに表示されるセクションの名前が含まれます。名前を変更するには、この名前をクリックして新しい名前を入力します。表示の問題を回避するため、長いセクション タイトル名は [Report Sections] ページで表示するときに切り詰められます。
セクション タイトルの アイコン	レポート テンプレートにセクションの複製を追加するには、複製アイコン（ ＋ ）をクリックします。 セクションを最小化するには、最小化アイコン（ － ）をクリックします。 セクションを削除するには、削除アイコン（ ✖ ）をクリックして、その後確定します。

次の表は、レポート テンプレートの各セクション内のフィールドを定義します。

表 57-2　　レポート セクションのフィールド

フィールド名	定義
Table	セクション データの取り出し元のテーブルを選択できるドロップダウン メニューを表示します。
プリセット	定義済み検索設定のドロップダウン メニューを表示します。新しい検索設定を定義する際に、該当する事前設定を選択して、検索条件を初期化できます。

表 57-2　レポート セクションのフィールド（続き）

フィールド名	定義
書式	セクション データの形式を選択できるアイコンを表示します。次のオプションがあります。 棒グラフ：選択した変数の数量を比較します。 折れ線グラフ：選択した変数の、時間の経過に伴う傾向/変化を示します。時間ベースのテーブルにのみ使用できます。 円グラフ：選択した各変数を全体の割合として示します。数量がゼロの変数はグラフからドロップされます。ごくわずかな数量は、[Other] というラベルのカテゴリに集められます。 表形式の表示：レコードごとの属性の値を示します。要約や統計のデータには使用できません。 詳細表示：パケット（侵入イベントの場合）やホスト プロファイル（ホスト イベントの場合）など、特定のイベントに関連付けられた複合オブジェクトのデータを示します。Format は、この種のオブジェクトが関係する特定のイベント タイプだけに使用できます。出力が多数要求されている場合には、パフォーマンスが低下することがあります。
Search または Filter	検索設定またはアプリケーション フィルタのドロップダウン メニューを表示します。 ほとんどのテーブルの場合、定義済みまたは保存済みの**検索設定**を使用してレポートを制約できます。編集アイコン（）をクリックして、新しい検索設定を作成することもできます。レポート テンプレート セクションの検索設定の操作（57-18 ページ）を参照してください。 Application Statistics テーブルの場合、ユーザ定義のアプリケーション **フィルタ**を使用してレポートを制約できます。フィルタの作成については、アプリケーション フィルタの操作（3-16 ページ）を参照してください。
X-Axis	選択したグラフの X 軸に関する使用可能なデータ列のドロップダウン メニューを表示します。グラフの形式を選択する場合にのみ表示されます。折れ線グラフの場合、X 軸の値は常に**時刻**です。棒グラフと円グラフの場合、X 軸の値として**時刻**を選択できません。
Y-Axis	選択したグラフの Y 軸に関する使用可能なデータ カラムのドロップダウン メニューを表示します。
Section Description	セクション内で検索データの前にある説明テキストを定義します。テキストと入力パラメータの組み合わせを入力します。新しいセクションのデフォルトは、`$<Time Window>` と `$<Constraints>` の 2 つの入力パラメータのセットです。 入力パラメータの詳細については、入力パラメータの使用法（57-19 ページ）を参照してください。
Time Window	セクションに表示されるデータの時間枠を定義します。セクションで時間ベースのテーブルが検索される場合、このチェック ボックスを選択して、レポートのグローバル時間枠を継承できます。または、セクションの特定の時間枠を設定することもできます。時間枠の設定については、レポート テンプレートのセクションの編集（57-13 ページ）を参照してください。

表 57-2　レポート セクションのフィールド（続き）

フィールド名	定義
結果	[Top] か [Bottom] を選択し、セクションに含めるレコードの最大数を入力します。
色	セクション内でグラフ化されるデータの色を定義します。必要に応じて、1 つ以上の色を選択します。

レポート テンプレートの作成と編集

ライセンス： すべて

次のいずれかの方法で新しいレポート テンプレートを構築できます。

- 新しいレポート テンプレートの作成（57-4 ページ）
- 既存のテンプレートからのレポート テンプレートの作成（57-6 ページ）
- イベント ビューからのレポート テンプレートの作成（57-10 ページ）
- ダッシュボードまたはワークフローのインポートによるレポート テンプレートの作成（57-11 ページ）

レポート テンプレートの変更とカスタマイズについては、次の項を参照してください。

- レポート テンプレートのセクションの編集（57-13 ページ）
- レポート テンプレート セクションの検索設定の操作（57-18 ページ）
- 入力パラメータの使用法（57-19 ページ）
- レポート テンプレート内のドキュメント属性の編集（57-24 ページ）
- 表紙のカスタマイズ（57-25 ページ）
- ロゴの管理（57-26 ページ）

新しいレポート テンプレートの作成

ライセンス： すべて

既存のレポート テンプレートをコピーしない場合は、まったく新しいテンプレートを作成できます。最初に、デフォルト テンプレートのシェルを作成します。次に、ご希望の順序で、個々のテンプレート セクションを設計し、レポート ドキュメントの属性を設定します。これらの手順の詳細については、次の項を参照してください。

- テンプレートのシェルの作成（57-4 ページ）
- テンプレート セクションの内容の設定（57-5 ページ）
- PDF および HTML レポート ドキュメントの属性の設定（57-6 ページ）

テンプレートのシェルの作成

ライセンス： すべて

レポート テンプレートは、独自のデータベース クエリから個別に構築されたセクションのフレームワークです。テンプレート作成の最初の手順として、セクションを追加したり形式設定したりできるフレームワーク シェルを生成します。

テンプレートのシェルを作成する方法:

アクセス: Admin/Any Security Analyst

ステップ 1　[Overview] > [Reporting] を選択します。

ステップ 2　[Report Templates] タブをクリックします。

[Report Templates] ページが表示されます。

ステップ 3　[Create Report Template] をクリックします。

[Report Sections] ページが表示され、デフォルトのテンプレート名 `New Report` が [Report Title] フィールドに表示されます。

ステップ 4　オプションで、[Report Title] フィールドに新しいテンプレートの名前を入力し、[Save] をクリックします。レポート タイトルには英数字とスペースの組み合わせを使用できます。

新しいテンプレート名のエントリが [Report Templates] ページのリストに表示されます。

ステップ 5　入力パラメータもレポート タイトルに使用できます。入力パラメータを追加するには、タイトル内で、パラメータの値を表示させるスポットにカーソルを置いてから、入力パラメータ挿入アイコン（  ）をクリックします。

追加した入力パラメータが [Report Title] フィールドに表示されます。入力パラメータの詳細については、入力パラメータの使用法（57-19 ページ）を参照してください。

ステップ 6　必要に応じて、[Report Sections] タイトル バーの下にある追加アイコンのセットを使用し、セクション シェルを挿入します。セクションの形式設定の詳細については、レポート セクションのフィールド表を参照してください。

追加した各セクションは、テンプレートの下部に表示されます。セクションを正しい場所にドラッグします。

ステップ 7　セクションのタイトル バーに表示されているセクションのタイトルをクリックし、セクションの名前を入力します（最大 120 文字を使用）。

ステップ 8　[Save] をクリックして、テンプレートを保存します。

テンプレートが保存されます。

テンプレート セクションの内容の設定

ライセンス: すべて

各テンプレート セクションは、検索設定やフィルタによって生成されたデータセットで構成され、表示モードを確定する形式の仕様（表や円グラフなど）があります。出力に含めるデータ レコードのフィールドを選択し、タイム フレームと表示するレコード数も選択して、さらにセクションの内容を確定します。

レポート テンプレート セクションを設定する方法:

アクセス: Admin/Any Security Analyst

ステップ 1　レポート テンプレートのセクションの編集（57-13 ページ）で説明されているように、セクションの属性を編集します。

ステップ 2　オプションで、セクションのウィンドウの下部にある [Preview] をクリックして、選択したカラムのレイアウトやグラフィックの形式を表示します。

注　セクション プレビュー ユーティリティを使用して、カラムの選択内容や、円グラフの色などの出力の特性を検査します。このインジケータは、設定済みの検索設定を必ずしも正確に反映するとは限りません。

PDF および HTML レポート ドキュメントの属性の設定

ライセンス： すべて

テンプレートから生成したレポートには、表紙、見出しとフッター、ページ番号など、すべてのセクションにまたがって機能を制御する複数のドキュメント属性があります。

レポート ドキュメントの属性を設定する方法：

アクセス： Admin/Any Security Analyst

ステップ 1　[Overview] > [Reporting] を選択します。

ステップ 2　[Report Templates] タブをクリックします。

[Report Templates] ページが表示されます。

ステップ 3　レポートの生成に使用するレポート テンプレートの [Edit] をクリックします。

このテンプレートの [Report Sections] ページが表示されます。

ステップ 4　[Advanced] をクリックします。

[Advanced Settings] ポップアップ ウィンドウが表示されます。

ステップ 5　PDF 形式か HTML 形式のキュメントの場合は、レポート テンプレート内のドキュメント属性の編集（57-24 ページ）で説明されている作業を実行します。

CSV をドキュメントの形式として選択した場合は、ドキュメントの属性を設定できません。

既存のテンプレートからのレポート テンプレートの作成

ライセンス： すべて

既存のテンプレートの中に適切なモデルがあれば、そのテンプレートをコピーして属性を編集することで、新しいレポート テンプレートを作成できます。また、Ciscoからは一連の定義済みレポート テンプレートが提供され、[Reports] タブのテンプレートの一覧で確認できます。これらの属性の説明については、定義済みレポート テンプレートの使用法（57-7 ページ）を参照してください。

既存のテンプレートからレポート テンプレートを作成する方法：

アクセス： Admin/Any Security Analyst

ステップ 1　[Overview] > [Reporting] を選択します。

ステップ 2　[Report Templates] タブをクリックします。

[Report Templates] ページが表示されます。Ciscoが用意しているレポート テンプレートについては、定義済みレポート テンプレートの使用法（57-7 ページ）を参照してください。

ステップ 3　モデルとしてコピーするレポート テンプレートの横のコピー アイコン（  ）をクリックします。

コピーしたテンプレートが、新しいレポート テンプレートとして表示されます。

ステップ 4　[Report Title] フィールドに、新しいレポート テンプレートの名前を入力します。

ステップ 5　[Save] をクリックします。

レポート テンプレートが保存され、新しいレポート テンプレートのエントリが [Report Templates] ページに表示されます。

ステップ 6　必要に応じてテンプレートを変更します。

テンプレートのセクションやドキュメントの属性の定義の詳細については、以下を参照してください。

- レポート テンプレートのセクションの編集（57-13 ページ）
- レポート テンプレート内のドキュメント属性の編集（57-24 ページ）

定義済みレポート テンプレートの使用法

ライセンス： すべて

次の定義済みレポート テンプレートは、現状のまま使用したり、編集を加えたり、独自のテンプレートのベースとして使用したりできます。

- Host Report: $<Host>
- User Report: $<User>
- Attack Report: Attack $<Attack SID>
- Malware Report
- FireSIGHT Report: $<Customer Name>
- Files Report

Host Report: $<Host>

Host Report: $<Host> レポート テンプレートは、ネットワーク上の特定のホストについての情報を提供します。このレポート テンプレートには、次のセクションがあります。

- Server Applications
- Client Applications
- Intrusion Events Originating from This Host
- Intrusion Events Destined to This Host
- Connections Originating from This Host
- Connections Destined to This Host
- Users of This Host
- White List Violations by This Host

User Report: $<User>

User Report: $<User> レポート テンプレートは、ネットワーク上の特定のユーザに関する情報を提供します。このレポート テンプレートには、次のセクションがあります。

- Client Applications Used by This User
- Web Applications Used by This User
- Application Protocols Used by This User
- Comprehensive List of Applications Used by This User
- Intrusion Events Originated By This User's Machines
- Intrusion Events Destined to This User's Machines
- Connections Originating from This User's Machines
- Connections Destined to This User's Machines
- Hosts for This User

Attack Report: Attack $<Attack SID>

Attack Report: Attack $<Attack SID> レポート テンプレートは、ネットワーク上の特定の攻撃に関する情報を提供します。このレポート テンプレートには、次のセクションがあります。

- General Information About This Attack
- Number of Attacks
- Number of Machines Initiating Attack
- Number of Machines Being Attacked
- Sources of This Attack
- Destinations of This Attack
- Traffic Patterns of This Attack

Malware Report

Malware Report レポート テンプレートは、ネットワークベースとエンドポイントベースのマルウェア イベントに関する情報を提供します。このレポート テンプレートには、次のセクションがあります。

- Malware Threats
- Threat Detections over Time
- Application Protocols Transferring Malware
- Hosts Receiving Malware
- Hosts Sending Malware
- Users Affected by Malware
- Malware Intrusions
- File Types Infected with Malware
- Applications Introducing Malware
- Table View of Malware Events

シリーズ 2デバイスと DC500 Defense Centerのどちらもネットワークベースのマルウェア対策をサポートしておらず、検出されて表示されるデータに影響を与える可能性があることに注意してください。たとえば、シリーズ 2 デバイスだけを管理するシリーズ 3 Defense Centerは、エンドポイントベースのマルウェア イベントだけを表示できます。

FireSIGHT Report: $<Customer Name>

FireSIGHT Report: $<Customer Name> レポート テンプレートは、組織のネットワークに関する全体的な情報を提供します。このレポート テンプレートには、次のセクションがあります。

- Summary of Application Traffic by Risk
- Risky Applications with Low Business Relevance
- Users of Risky Applications
- Anonymizers and Proxies
- Typically High Bandwidth Applications
- Applications by Total Bandwidth
- Hosts Accessing Sensitive Network
- Users Accessing Sensitive Network
- Applications on Sensitive Network
- Ports and Protocols Related to Sensitive Network
- Hosts Visiting Malicious URLs
- Users Visiting Malicious URLs
- Granular Application Usage
- Web Applications
- Client Applications
- Application Protocols
- Web Browser Versions
- Operating System Versions
- Overall User Activity
- Intrusion Events by Impact
- Intrusion Events by Impact (After Blocking)
- Intrusion Events by Application
- Top Intrusion Events
- Comprehensive Application List

Files Report

Files Report レポート テンプレートは、管理対象デバイスによってネットワーク トラフィックで検出されたファイルに関する情報を提供します。このレポート テンプレートには、次のセクションがあります。

- File Transfers over Time
- Application Protocols Used by File Transfers
- File Dispositions
- File Actions

- Hosts Receiving Files
- Hosts Sending Files
- Users Transferring Files
- File Categories
- File Types
- File Names
- Table View of File Events

イベント ビューからのレポート テンプレートの作成

ライセンス： すべて

レポートを生成する前に、レポート作成システムにより作成されるレポート テンプレートに、必要に合わせて変更を加えることができます。セクションを追加したり、自動的に組み込まれるセクションを変更したり、セクションを削除したりできます。

イベント ビューからレポート テンプレートを作成する方法：

アクセス： Admin/Any Security Analyst

ステップ 1　レポートに含めるイベントをイベント ビューに入力します。さまざまな方法で入力できます。

- イベント検索設定を使用して、表示するイベントを定義します。イベント検索設定の使用法の詳細については、イベントの検索（60-1 ページ）を参照してください。
- イベント ビューに該当するイベントが表示されるまでワークフローをドリルダウンします。ワークフローと、ワークフロー内のイベントを制約する方法の詳細については、ワークフローの概要と使用（58-1 ページ）を参照してください。

ステップ 2　イベント ビューのページから、[Report Designer] をクリックします。

[Report Sections] ページが表示され、キャプチャされるワークフロー内のビューごとにセクションが示されます。

ステップ 3　オプションで、[Report Title] フィールドに新しい名前を入力し、[Save] をクリックします。

ステップ 4　オプションで、セクションのタイトル バーの削除アイコン（ ✖ ）をクリックし、削除を確認して、レポートから除外するテンプレート セクションを削除します。

削除されたセクションは非表示になります。

注　一部のワークフロー内の最後のレポート セクションには詳細ビューが含まれ、ワークフローに応じてパケット、ホスト プロファイル、または脆弱性が示されます。レポートの生成時に、これらの詳細ビューがあるイベントを多数取得すると、Defense Centerのパフォーマンスに影響を与えることがあります。

ステップ 5　オプションで、レポート セクション内のフィールドの設定を調整します。

レポート セクション内のフィールドの設定の詳細については、レポート テンプレートのセクションの編集（57-13 ページ）を参照してください。

ヒント　セクションの現在のカラムのレイアウトやグラフの形式を表示する場合は、そのセクションの [Preview] リンクをクリックします。

ステップ 6　オプションで、タイトル バーでセクションのタイトルをクリックして、そのセクションのタイトルを変更します。

[Set Section Title] ポップアップ ウィンドウが表示されます。セクションのタイトルを入力し、[OK] をクリックします。

ステップ 7　オプションで、改ページを追加します。改ページ追加アイコン（  ）をクリックします。

新しい改ページ オブジェクトがテンプレートの下部に表示されます。そのオブジェクトを、新しいページの先頭にするセクションの前にドラッグします。改ページの使用法の詳細については、レポート テンプレートのセクションの編集（57-13 ページ）を参照してください。

ステップ 8　オプションで、テキスト セクションを追加します。テキスト セクション追加アイコン（  ）をクリックします。

新しいテキスト セクションがテンプレートの下部に表示されます。そのセクションを、レポート テンプレート内の表示位置にドラッグします。テキスト セクションの編集については、レポート テンプレートのセクションの編集（57-13 ページ）を参照してください。

ヒント　テキスト セクションはリッチ テキスト（太字、斜体、可変フォント サイズなど）やインポート済みイメージをサポートしており、レポートやレポート セクションの概要として活用できます。

ステップ 9　オプションで、[Advanced Settings] をクリックして、表紙、目次、開始ページ番号、または見出しとフッターのテキストを追加します。詳細については、レポート テンプレート内のドキュメント属性の編集（57-24 ページ）を参照してください。

ステップ 10　レポート テンプレートが適切な場合は、[Save] をクリックします。

レポート テンプレートが保存され、レポート テンプレートのエントリが [Report Templates] ページに表示されます。

ダッシュボードまたはワークフローのインポートによるレポート テンプレートの作成

ライセンス： すべて

ダッシュボード、ワークフロー、統計の要約をインポートして、新しいレポートをすばやく作成できます。インポートすると、ダッシュボードのウィジェット グラフィックごと、およびワークフローのイベント ビューごとにセクションが作成されます。最も重要な情報に焦点が当たるように不要なセクションを削除できます。次の表で、インポート オプションについて説明します。

表 57-3　[Import Report Sections] ウィンドウのデータ ソース オプション

選択オプション	インポート対象
Import Dashboard	選択したダッシュボード上のカスタム分析ウィジェット。
Import Workflow	定義済みのワークフローまたはカスタム ワークフロー。 **ヒント**　選択項目の形式は次のようになっています。 `Table - Workflow name` たとえば、`Connection Events - Traffic by Port` は、Connection Events テーブルから生成された Traffic by Port ワークフロー内のビューをインポートします。
Import Summary Sections	次の一般的な要約: • Intrusion Detailed Summary • Intrusion Short Summary • Discovery Detailed Summary • Discovery Short Summary

ダッシュボード、ワークフロー、または統計情報の要約からレポート テンプレートを作成する方法:

アクセス: Admin/Any Security Analyst

ステップ 1　レポート内で複製するダッシュボード、ワークフロー、または要約を識別します。

ステップ 2　[Overview] > [Reporting] を選択します。

ステップ 3　[Report Templates] タブをクリックします。

[Report Templates] ページが表示されます。

ステップ 4　[Create Report Template] をクリックします。

[Report Sections] ページが表示されます。

ステップ 5　[Report Title] フィールドに新しいレポート テンプレートの名前を入力します。

ステップ 6　新しい名前でレポート テンプレートを保存する場合は、[Save] をクリックします。

レポート テンプレートが保存され、レポート テンプレートのエントリが [Report Templates] ページに表示されます。

ステップ 7　ダッシュボード、要約、ワークフローのアイコン( )からインポート セクションをクリックします。

[Import Report Sections] ポップアップ ウィンドウが表示されます。[Import Report Sections] ウィンドウのデータ ソース オプション表で説明されているデータ ソースのいずれかを選択できます。

ステップ 8　ドロップダウンメニューからダッシュボード、ワークフロー、または要約を選択します。

ステップ 9　追加しようとしているデータ ソースの、[Import] をクリックします。

テンプレートの [Report Sections] ページが再び表示され、選択したデータ ソースの要素ごとのセクションが示されます。ダッシュボードの場合、ウィジェット グラフィックごとに独自のセクションがあります。ワークフローの場合、イベント ビューごとに独自のセクションがあります。

ステップ 10　必要に応じてセクションの内容を変更します。

レポート テンプレートの編集については、レポート テンプレートのセクションの編集(57-13 ページ)を参照してください。

注　一部のワークフロー内の最後のレポート セクションには詳細ビューが含まれ、ワークフローに応じてパケット、ホスト プロファイル、または脆弱性が示されます。レポートの生成時に、これらの詳細ビューがあるイベントを多数取得すると、Defense Centerのパフォーマンスに影響を与えることがあります。

ステップ 11　レポート テンプレートが適切な場合は、[Save] をクリックします。

レポート テンプレートが保存され、レポート テンプレートのエントリが [Report Templates] ページに表示されます。

レポート テンプレートのセクションの編集

ライセンス： すべて

さまざまなレポート セクションの属性を変更して、セクションとそのデータ表示の内容を調整できます。詳細については、次の項を参照してください。

- テンプレート セクションのテーブルとデータ形式の設定（57-13 ページ）
- テンプレート セクションの検索設定またはフィルタの指定（57-14 ページ）
- 表形式のセクションに表示される検索フィールドの設定（57-15 ページ）
- レポート テンプレートへのテキスト セクションの追加（57-15 ページ）
- レポート テンプレートへの改ページの追加（57-16 ページ）
- テンプレートとそのセクションの時間枠の設定（57-16 ページ）
- テンプレート セクションの名前変更（57-18 ページ）
- テンプレート セクションのプレビュー（57-18 ページ）

注　セキュリティ アナリストは、自分が作成したレポート テンプレートだけを編集できます。

テンプレート セクションのテーブルとデータ形式の設定

ライセンス： すべて

レポート テンプレート内の各セクションでは、データベース テーブルを照会して、そのセクションの内容を生成します。セクションのデータ形式を変更する際にも同じデータ クエリーが使用されますが、形式のタイプごとの分析の目的に従って、セクションに表示されるフィールドが変わります。たとえば、侵入イベントの表形式の表示では、イベント レコードごとに多数のデータ フィールドがセクションに入力され、円グラフのセクションでは、選択した各属性が表すすべての一致レコードの割合が示され、個々のイベントに関する詳細情報は表示されません。棒グラフのセクションでは、特定の属性を持つ一致レコードの合計数が比較されます。折れ線グラフでは、1 つの属性に関係する一致レコード数の変化が時系列で要約されます。折れ線グラフは時間ベースのデータの場合のみ使用でき、ホスト、ユーザ、サードパーティの脆弱性などに関する情報の場合は使用できません。

使用できるさまざまな形式の詳細については、レポート セクションのフィールド表を参照してください。

テンプレート セクションのテーブルと出力形式を選択する方法：

アクセス： Admin/Any Security Analyst

ステップ 1　[Table] ドロップダウン メニューを使用して、このセクションで照会するテーブルを選択します。

選択したテーブルで使用できる出力形式ごとに、アイコンが [Format] フィールドに表示されます。

ステップ 2　セクションに該当する出力形式のアイコンを選択します。これらの形式については、レポート セクションのタイトル バーの要素表を参照してください。

出力に含められるフィールドが表示されます。

ステップ 3　検索設定の制約を変更するには、[Search] フィールドか [Filter] フィールドの横にある編集アイコン（  ）クリックします。

[Search Editor] ポップアップ ウィンドウが表示され、検索設定の制約に関するオプションが示されます。このウィンドウの使用方法の詳細については、レポート テンプレート セクションの検索設定の操作（57-18 ページ）を参照してください。

ステップ 4　グラフ出力形式（円グラフや棒グラフなど）の場合、ドロップダウン メニューを使用して、[X-Axis] と [Y-Axis] のパラメータを調整します。

X 軸の値を選択すると、互換性のある値だけが Y 軸のドロップダウン メニューに表示されます。その逆も同様です。

ステップ 5　表出力の場合、出力内の列、表示順序、ソート順序を選択します。詳細については、表形式のセクションに表示される検索フィールドの設定（57-15 ページ）を参照してください。

ステップ 6　[Save] をクリックして、テンプレートを保存します。

テンプレートが保存されます。

テンプレート セクションの検索設定またはフィルタの指定

ライセンス： すべて

レポート セクションの検索設定やフィルタは、セクションの内容のベースになるデータベース クエリーを指定します。ほとんどのテーブルの場合、定義済み検索設定か保存済み検索設定を使用してレポートを制約するか、新しい検索設定を即座に作成することができます。

- 定義済み検索設定は特定のイベント テーブルの検索サンプルの役割を果たし、レポートに含めようとしている、ネットワークに関する重要情報にクイック アクセスできます。
- 保存済みイベント検索設定には、自分や他のユーザが作成したすべてのパブリック イベント検索設定と、自分で保存したすべてのプライベート イベント検索設定が含まれます。保存済みイベント検索設定の定義、命名、使用法の詳細については、イベントの検索（60-1 ページ）を参照してください。
- 現在のレポート テンプレートの保存済み検索設定は、そのレポート テンプレート自体に限りアクセスできます。保存済みレポート テンプレートの検索設定の名前は、末尾が文字列「Custom Search」になります。ユーザは、レポートの設計時にこれらの検索設定を作成します。

Application Statistics テーブルの場合、ユーザ定義のアプリケーション フィルタを使用してレポートを制約できます。フィルタの作成については、アプリケーション フィルタの操作（3-16 ページ）を参照してください。

テンプレート セクションの検索設定やフィルタを指定する方法:

アクセス: Admin/Any Security Analyst

ステップ 1 [Table] ドロップダウンメニューから、照会するデータベース テーブルを選択します。

- ほとんどのテーブルの場合、[Search] ドロップダウン リストが表示されます。
- Application Statistics テーブルの場合、[Filter] ドロップダウン リストが表示されます。

ステップ 2 レポートの制約に使用する検索設定かフィルタを選択します。

編集アイコン( )をクリックして、検索条件を表示したり、新しい検索設定を作成したりできます。詳細については、レポート テンプレート セクションの検索設定の操作(57-18 ページ)を参照してください。

表形式のセクションに表示される検索フィールドの設定

ライセンス: すべて

セクションに表データを組み込む場合に、データ レコード内のどのフィールドを表示するか選択できます。表形式のすべてのフィールドを組み込みに対象にも除外対象にもすることができます。レポートの目的を達成するのに必要なフィールドを選択し、それに従って配列したりソートしたりします。

表形式のセクションでフィールドを追加したり削除したりする方法:

アクセス: Admin/Any Security Analyst

ステップ 1 表形式のセクションで、[Fields] パラメータの横にある編集アイコン( )をクリックします。

[Table Field Selector] ウィンドウが表示されます。

ステップ 2 オプションで、フィールドを追加したり削除したりしてから、フィールドのアイコンをドラッグし、ご希望のカラム順にします。

ステップ 3 オプションで、カラムのソート順序を変更します。各フィールド アイコン上のドロップダウン リストを使用して、ソート順序と優先度を設定します。

ステップ 4 フィールドの順序が正しく、必要なソート特性がある場合は、[OK] をクリックします。

[Report Sections] ページが表示されます。

レポート テンプレートへのテキスト セクションの追加

ライセンス: すべて

テンプレートにテキスト セクションを追加して、レポート全体や個々のセクションに概要などのカスタム テキストを用意することができます。テキスト セクションには、複数のフォント サイズやフォント スタイル(太字や斜体など)を使用できるリッチ テキスト、入力パラメータ、インポート済みイメージを使用できます。入力パラメータの詳細については、入力パラメータの使用法(57-19 ページ)を参照してください。

テキスト セクションをレポート テンプレートに追加する方法：

アクセス： Admin/Any Security Analyst

ステップ 1　テキスト セクション追加アイコン（  ）をクリックします。

テキスト セクションがテンプレートの下部に表示されます。

ステップ 2　新しいテキスト セクションを、レポート テンプレート内のご希望の位置にドラッグします。

ステップ 3　オプションで、テキスト セクションの前後に改ページを追加します。改ページの詳細については、レポート テンプレートへの改ページの追加（57-16 ページ）を参照してください。

ステップ 4　オプションで、タイトル バー内のテキスト セクションの総称名をクリックして、新しい名前を入力します。

ステップ 5　テキスト セクションの本文に形式設定済みのテキストやイメージを追加します。レポートの生成時に動的に更新する入力パラメータを組み込むことができます。

ステップ 6　設定が終わったら [Save] をクリックします。

テンプレートが保存されます。

レポート テンプレートへの改ページの追加

ライセンス： すべて

テンプレート内のどのセクションの前後にも改ページを追加できます。この機能は、複数のセクションから成るレポートで、各種セクションの概要を示すテキスト ページがある場合に特に便利です。

改ページを追加する方法：

アクセス： Admin/Any Security Analyst

ステップ 1　改ページ追加アイコン（  ）をクリックします。

改ページがテンプレートの下部に表示されます。

ステップ 2　改ページを、セクションの前後のご希望の場所にドラッグします。

ステップ 3　テンプレートに追加するすべての改ページに対してこのプロセスを繰り返します。

テンプレートとそのセクションの時間枠の設定

ライセンス： すべて

レポート テンプレートの時間枠は、テンプレートのレポート作成期間を定義します。時間ベースのデータ（侵入イベントや検出イベントなど）があるレポート テンプレートにはグローバル時間枠があります。この時間枠は、テンプレート内の時間ベースのセクションでデフォルトで作成時に継承されます。グローバル時間枠を変更すると、グローバル時間枠を継承するように設定されているセクションのローカル時間枠が変更されます。[Inherit Time Window] チェック ボックスをクリアすると、個々のセクションの時間枠の継承を無効にできます。それから、ローカル時間枠を編集できます。

注　グローバル時間枠の継承は、侵入イベントや検出イベントなど、時間ベースのテーブルからのデータがあるレポート セクションだけに適用されます。ネットワーク アセット（ホストやデバイス）と関連情報（脆弱性など）を報告するセクションの場合、各時間枠を個別に設定する必要があります。

レポート テンプレートのグローバル時間枠を変更する方法：

アクセス： Admin/Any Security Analyst

ステップ 1　[Report Templates] ページで、編集するレポート テンプレートの横にある編集アイコン（）をクリックします。

[Report Sections] ページが表示されます。

ステップ 2　[Generate] をクリックします。

[Generate Report] ポップアップ ウィンドウが表示されます。

ステップ 3　グローバル時間枠を変更するには、時間枠のアイコン（）をクリックします。

新しいウィンドウに [Events Time Window] ページが表示されます。このページの使用法に関する詳細については、イベント時間の制約の設定（58-26 ページ）を参照してください。

ステップ 4　終了したら、[Events Time Window] ウィンドウで [Apply] をクリックします。

[Generate Report] ポップアップ ウィンドウに新しい時間枠が再表示されます。

ステップ 5　[Cancel] をクリックして [Report Sections] ページに戻るか、[OK] をクリックしてレポートを生成します。

レポート内のセクションごとに別の時間枠を使用できます。たとえば、最初のセクションを月の要約にして、残りのセクションで週レベルの詳細情報へドリルダウンするようにできます。この場合、セクション レベルの時間枠を個別に設定します。

セクションのローカル時間枠を設定する方法：

アクセス： Admin/Any Security Analyst

ステップ 1　テンプレートの [Report Sections] ページで、セクションの [Inherit Time Window] チェック ボックスが存在する場合はクリアします。

ローカル セクション時間枠のアイコンが表示されます。

ステップ 2　セクションのローカル時間枠を変更するには、時間枠のアイコン（）をクリックします。

[Events Time Window] ページが表示されます。このページの使用法に関する詳細については、イベント時間の制約の設定（58-26 ページ）を参照してください。

注　統計テーブルからのデータがあるセクションでは、スライド式の時間枠のみ使用できます。

ステップ 3　新しいローカル時間枠を設定し終えたら、[Events Time Window] で [Apply] をクリックします。

ステップ 4　[Save] をクリックします。

さらに編集できるように [Report Sections] ページが表示されます。

テンプレート セクションの名前変更

ライセンス：すべて

新しいテンプレートの作成時に追加したセクションには総称セクション名が付けられるので、内容を表す名前に変更する必要があります。

テンプレート セクションの名前を変更する方法：

アクセス：Admin/Any Security Analyst

ステップ 1　セクション 見出し内の現在のセクション名をクリックします。

[Set Section Title] ポップアップ ウィンドウが表示されます。

ステップ 2　セクションの新しい名前を入力し（最大 120 文字）、[OK] をクリックします。

セクションのタイトル バー内の名前が変わります。

テンプレート セクションのプレビュー

ライセンス：すべて

プレビュー機能は、表形式の表示のフィールドのレイアウトとソート順序や、円グラフの色などのグラフの読みやすさに関する重要な特性を表示します。

テンプレート セクションをプレビューする方法：

アクセス：Admin/Any Security Analyst

ステップ 1　セクションの編集中のいつでも、そのセクションの [Preview] をクリックします。

[Preview] ポップアップ ウィンドウが表示されます。

ステップ 2　ウィンドウの下部にある [OK] をクリックし、プレビューを閉じます。

[Report Sections] ページが表示されます。

レポート テンプレート セクションの検索設定の操作

ライセンス：すべて

レポートが正常に作成されるかどうかは、レポートのセクションへの入力内容を決める検索設定の定義が重要な要素になります。FireSIGHT システムには検索エディタが備えられており、レポート テンプレートで使用できる検索設定を表示したり、新しいカスタム検索設定を定義したりできます。

ヒント　レポート テンプレート内で作成したカスタム検索設定は、そのテンプレートに固有になります。イベント ビューアで、すべてのレポート テンプレートで再利用できる検索設定を作成できます。イベント ビューアでカスタム検索設定を保存すると、すべてのレポート テンプレートの [Search] ドロップダウン メニューに表示されます。イベント ビューアを使用してカスタム検索設定を作成して保存する方法の詳細については、イベントの検索（60-1 ページ）を参照してください。

カスタム検索設定を作成する方法:

アクセス: Admin/Any Security Analyst

ステップ 1　レポート テンプレート内の関連するセクションから、[Search] フィールドの横にある編集アイコン( )をクリックします。

[Search Editor] ページが表示され、選択した検索対象のテーブルが示されます。

ステップ 2　オプションで、[Saved Searches] ドロップダウン メニューから、定義済み検索設定を選択します。

ドロップダウンに、このテーブルに関する使用可能な定義済み検索設定がすべて表示されます。システム規模の定義済み検索設定とレポート固有の定義済み検索設定が含まれます。

ステップ 3　該当するフィールドで検索条件を編集します。特定のフィールドの場合、制約にイベント検索設定と同じ演算子(< や <> など)を含めることができます。検索条件の構文については、イベントの検索(60-1 ページ)を参照してください。

複数の条件を入力すると、検索時にはすべての条件を満たすレコードだけが返されます。

ステップ 4　オプションで、入力パラメータのアイコン( )が表示されている位置で、制約値を入力する代わりにドロップダウン メニューから入力パラメータを挿入できます。レポートの設計で入力パラメータを使用する方法の詳細については、入力パラメータの使用法(57-19 ページ)を参照してください。

一部の検索フィールドの場合、ドロップダウン メニューにユーザ定義の管理対象オブジェクトが、入力パラメータの代わりに示されるか、入力パラメータと共に示される場合があります。管理対象オブジェクトは、検索設定を制約する値として使用できるシステム設定変数で、タイプに応じて固有なアイコンがあります。ただしこれらは、入力パラメータで行われるユーザ入力に関する生成時クエリを作成しません。管理対象オブジェクトの詳細については、再利用可能なオブジェクトの管理(3-1 ページ)を参照してください。

注　レポートの検索設定の制約を編集すると、システムにより *section* `custom search` という名前で編集済みの検索設定が保存されます。*section* は、セクションのタイトル バーに示される文字列 `custom search` の前の名前の部分です。保存するカスタム検索設定の名前をわかりやすくするには、セクション名を変更した後に編集済みの検索設定を保存するようにしてください。保存したレポートの検索設定の名前を変更することはできません。

ステップ 5　検索エディタでフィールドを変更し終えたら、[OK] をクリックします。

[Report Sections] ページが再表示され、新しい定義済み検索設定がセクションの [Search] ドロップダウン メニューに表示されます。

入力パラメータの使用法

ライセンス: すべて

レポートの生成時に動的に更新できる入力パラメータをレポート テンプレート内で使用できます。入力パラメータのアイコン( )は、入力パラメータを処理できるフィールドを示します。次の 2 種類の入力パラメータがあります。

- 定義済み: 定義済みの入力パラメータ表を参照
- ユーザ定義: ユーザ定義の入力パラメータのタイプ表を参照

定義済みの入力パラメータ

ライセンス: すべて

定義済みの入力パラメータは、内部システム関数か設定情報によって解決されます。たとえば、レポートの生成時に、システムにより $<Time> パラメータは現在の日時に置き換えられます。次の表に、使用できるパラメータを定義します。たとえば、スケジューラの制御下で自動的に生成される月次要約レポートのタイトルに $<Month> を含めることもできます。その後、レポートのタイトルは正しい月で自動的に更新されます。

表 57-4　定義済みの入力パラメータ

挿入するパラメータ	テンプレートに含められる情報
$<Logo>	選択したアップロード済みのロゴ
$<Report Title>	レポートのタイトル
$<Time>	レポートが実行された日時、精度 1 秒
$<Month>	現在の月
$<Year>	現在の年
$<System Name>	Defense Centerの名前
$<Model Number>	Defense Centerのモデル番号
$<Time Window>	現在レポート セクションに適用されている時間枠
$<Constraints>	現在レポート セクションに適用されている検索制約

次の表に、[Report Templates] ページ内のさまざまな領域で使用できる有効な入力パラメータをリストします。

表 57-5　定義済みの入力パラメータの使用法

パラメータ	Report Template Cover Page	Report Template Report Title	Report Template Section Description	Report Template Text Section	Generate Report File Name	Generate Report Email Subject, Body
$<Logo>	はい	いいえ	いいえ	いいえ	いいえ	いいえ
$<Report Title>	はい	いいえ	はい	はい	はい	はい
$<Time>	はい	はい	はい	はい	はい	はい
$<Month>	はい	はい	はい	はい	はい	はい
$<Year>	はい	はい	はい	はい	はい	はい
$<System Name>	はい	はい	はい	はい	はい	はい
$<Model Number>	はい	はい	はい	はい	はい	はい
$<Time Window>	いいえ	いいえ	はい	いいえ	いいえ	いいえ
$<Constraints>	いいえ	いいえ	はい	いいえ	いいえ	いいえ

ユーザ定義の入力パラメータ

ライセンス：すべて

独自の入力パラメータを作成して、セクションの検索設定で制約として使用できます。入力パラメータを使用して検索設定を制約すると、レポートの生成時に要求者から値を収集するようにシステムに指示できます。この方法で、テンプレートを変更せずに、レポートを生成時に動的に調整して特定のデータのサブセットを表示できます。たとえば、レポート セクションの検索設定の [Destination IP] フィールドに入力パラメータを指定できます。指定後、レポートの生成時に、特定の部門の IP ネットワークのセグメントを入力して、その部門のデータだけを取得できます。

ヒント　また、入力パラメータ フィールドに * を入力すると、制約が無視される効果があります。

文字列タイプの入力パラメータを定義して、電子メール（件名または本文）、レポート ファイル名、テキスト セクションなどのレポートの特定のフィールドに動的テキストを追加することもできます。すべて同じテンプレートを利用し、カスタマイズしたレポート ファイル名、電子メール アドレス、電子メール メッセージを使用して、さまざまな部門用にレポートをパーソナル化できます。

定義する入力パラメータごとに名前とタイプがあります。次の表に、パラメータのタイプを示します。

表 57-6　ユーザ定義の入力パラメータのタイプ

パラメータのタイプ	使用先のフィールド内のデータ
ネットワーク/IP	CIDR 形式の IP アドレスまたはネットワーク セグメント
アプリケーション	アプリケーション プロトコル、クライアント アプリケーション、または Web アプリケーションの名前
イベント メッセージ	イベント ビュー メッセージ
デバイス	3D アプライアンス（Defense Centerまたは FireSIGHT システムの管理対象デバイス）
[Username]	イニシエータ ユーザやレスポンダ ユーザなどのユーザ ID
番号（VLAN ID、Snort ID、Vuln ID）	VLAN ID、Snort ID、または脆弱性 ID
文字列	アプリケーションや OS のバージョン、注記、説明などのテキスト フィールド

入力パラメータのタイプにより、そのパラメータを使用できる検索フィールドが決まります。指定したタイプは、ユーザ定義の入力パラメータのタイプ表に示されている当該フィールドのみで使用できます。たとえば、ユーザ パラメータを文字列タイプとして定義すると、テキスト フィールド内への挿入には使用できますが、IP アドレスを使用するフィールドでは使用できません。

レポート テンプレートに関するユーザ定義の入力パラメータを作成する方法：

アクセス：Admin/Any Security Analyst

ステップ 1　[Overview] > [Reporting] を選択します。

ステップ 2　[Report Templates] タブを選択します。

[Report Templates] ページが表示されます。

ステップ 3　編集するテンプレートの編集アイコン( )をクリックします。

[Report Sections] ページが表示されます。

ステップ 4　[Advanced] をクリックします。

[Advanced Settings] ポップアップ ウィンドウが表示されます。

ステップ 5　入力パラメータ追加アイコン( )をクリックします。

[Add Input Parameter] ポップアップ ウィンドウが表示されます。

ステップ 6　[Name] フィールドにパラメータ名を入力し、[Type] ドロップダウンメニューを使用してタイプを選択してから、[OK] をクリックします。

新しいパラメータが [Input Parameters] メニューに表示されます。

ステップ 7　必要なパラメータをすべて定義し終えるまで、上記の手順を繰り返します。

ステップ 8　[OK] をクリックします。

このテンプレートの新しい入力パラメータが保存され、[Report Sections] ページが再表示されます。

レポート テンプレートを再利用する場合、入力パラメータの名前とタイプを変更して、新しいレポートの目的をいっそう反映させることができます。

レポート テンプレートに関するユーザ定義の入力パラメータを編集する方法：

アクセス： Admin/Any Security Analyst

ステップ 1　[Overview] > [Reporting] を選択します。

ステップ 2　[Report Templates] タブを選択します。

[Report Templates] ページが表示されます。

ステップ 3　編集するテンプレートの編集アイコン( )をクリックします。

[Report Sections] ページが表示されます。

ステップ 4　[Advanced] をクリックします。

[Advanced Settings] ポップアップ ウィンドウが表示されます。[Input Parameters] セクションに、レポート テンプレートの使用可能なユーザ定義パラメータがすべてリストされます。

ステップ 5　編集アイコン( )をクリックします。

[Edit Input Parameter] ポップアップ ウィンドウが表示されます。

ステップ 6　[Name] フィールドでパラメータ名を変更し、[Type] ドロップダウンメニューを使用してパラメータ タイプを変更してから、[OK] をクリックします。

変更したパラメータが、[Input Parameters] セクションに表示されます。

ステップ 7　必要なパラメータをすべて定義し終えるまで、上記の手順を繰り返します。[OK] をクリックします。

変更が保存され、[Report Sections] ページが再表示されます。

レポート テンプレートに関するユーザ定義の入力パラメータを削除する方法:

アクセス: Admin/Any Security Analyst

ステップ 1 [Overview] > [Reporting] を選択します。

ステップ 2 [Report Templates] タブを選択します。

[Report Templates] ページが表示されます。

ステップ 3 編集するテンプレートの編集アイコン( )をクリックします。

[Report Sections] ページが表示されます。

ステップ 4 [Advanced] をクリックします。

[Advanced Settings] ポップアップ ウィンドウが表示されます。[Input Parameters] セクションに、レポート テンプレートの使用可能なユーザ定義パラメータがすべてリストされます。

ステップ 5 入力パラメータの横の削除アイコン( )をクリックして確認します。

ステップ 6 [OK] をクリックします。

入力パラメータが削除され、[Report Sections] ページが再表示されます。

入力パラメータを使用して、検索設定の実用性を向上させます。入力パラメータにより、レポートの生成時に要求者から値を収集するようにシステムに指示できます。この方法で、検索設定を変更せずに、レポートを生成時に動的に制約して特定のデータのサブセットを表示できます。たとえば、レポート セクションの [Destination IP] フィールドに入力パラメータを指定して、部門レベルでセキュリティ イベントをドリル ダウンできます。レポートの生成時に、特定の部門の IP ネットワークのセグメントを入力して、その部門のデータだけを取得できます。

ユーザ定義の入力パラメータを使用してレポート テンプレート内の検索設定を制約する方法:

アクセス: Admin/Any Security Analyst

ステップ 1 [Overview] > [Reporting] を選択します。

ステップ 2 [Report Templates] タブを選択します。

[Report Templates] ページが表示されます。

ステップ 3 編集するテンプレートの編集アイコン( )をクリックします。

[Report Sections] ページが表示されます。

ステップ 4 セクション内の [Search] フィールドの横にある編集アイコン( )をクリックします。

[Search Editor] ポップアップ ウィンドウが表示されます。入力パラメータを使用できるフィールドは、入力パラメータのアイコン( )のマークが付けられます。

ステップ 5 フィールドの横にある入力パラメータのアイコン( )をクリックして、ドロップダウン メニューから入力パラメータを選択します。ユーザ定義の入力パラメータはアイコン( )のマークが付けられます。

入力パラメータがフィールドに表示されます。

注 定義した入力パラメータは、そのパラメータのタイプと一致する検索フィールドでのみ使用できます。たとえば、**ネットワーク/IP** タイプのパラメータは、CIDR 形式の IP アドレスまたはネットワーク セグメントを受け入れるフィールドだけで使用できます。

ステップ 6　必要な入力パラメータをすべて追加し終えたら、[OK] をクリックします。

[Report Sections] ページと変更内容が表示されます。

レポート テンプレート内のドキュメント属性の編集

ライセンス： すべて

レポートを生成する前に、レポートの外観に影響を与えるドキュメント属性を設定できます。これらの属性には、オプションの表紙と目次が含まれます。一部の属性のサポートは、レポートの形式に PDF、HTML、CSV のいずれを選択したかによって異なります。次の表で、形式別の属性のサポートについて詳しく説明します。

表 57-7　　ドキュメント属性のサポート

属性	PDF のサポート	HTML のサポート	CSV のサポート
表紙	可能、オプションでロゴと外観のカスタマイズ	可能、オプションでロゴと外観のカスタマイズ	いいえ
目次	はい	はい	いいえ
ページの見出しとフッター	可能、オプションでフィールド内にテキストかロゴ	いいえ	いいえ
カスタムの開始ページ番号	はい	いいえ	いいえ
先頭ページに番号を付けないオプション	はい	いいえ	いいえ

PDF レポートや HTML レポートのドキュメント属性を設定する方法：

アクセス： Admin/Any Security Analyst

ステップ 1　[Overview] > [Reporting] を選択します。

ステップ 2　[Report Templates] タブを選択します。

[Report Templates] ページが表示されます。

ステップ 3　編集するレポート テンプレートの編集アイコン（  ）をクリックします。

[Report Sections] ページが表示されます。

ステップ 4　[Advanced] をクリックします。

[Advanced Settings] ポップアップ ウィンドウが表示されます。

ステップ 5　[Include Cover Page] を選択して表紙を追加します。

ステップ 6　[Cover Page Design] フィールドの横にある編集アイコン（  ）をクリックして、表紙のデザインを編集します。

詳細については、表紙のカスタマイズ（57-25 ページ）を参照してください。

ステップ 7　[Include Table of Contents] を選択して、目次を追加します。

ステップ 8　3 つの [Header] フィールドと [Footer] フィールドのドロップダウンを使用して、見出しとフッターを設定します。ドロップダウン メニューから見出しとフッターのコンテンツとしてロゴ、日付、ページ番号などを選択します。

[Logo] を選択すると、選択したフィールドにデフォルトのロゴ イメージが表示されます。デフォルトのロゴ イメージを変更する場合は、ロゴの管理（57-26 ページ）を参照してください。

ステップ 9　[Page Number Start] フィールドで、レポートの先頭ページのページ番号を選択します。

[Number First Page?] を選択すると、表紙の次の先頭ページにページ番号が表示されます。これを選択すると、表紙には番号が付けられません。

ステップ 10　[OK] をクリックします。

ドキュメント属性が保存され、[Report Sections] ページが再表示されます。

表紙のカスタマイズ

ライセンス： すべて

レポート テンプレートの表紙をカスタマイズできます。表紙には、複数のフォント サイズやフォント スタイル（太字や斜体など）を使用できるリッチ テキスト、入力パラメータ、インポート済みイメージを使用できます。入力パラメータの詳細については、入力パラメータの使用法（57-19 ページ）を参照してください。

レポート テンプレートの表紙をカスタマイズする方法：

アクセス： Admin/Any Security Analyst

ステップ 1　[Overview] > [Reporting] を選択します。

ステップ 2　[Report Templates] タブを選択します。

[Report Templates] ページが表示され、テンプレートのリストが示されます。

ステップ 3　レポート テンプレートの編集アイコン（  ）をクリックします。

[Report Sections] ページが表示されます。

ステップ 4　[Advanced] をクリックします。

[Advanced Settings] ポップアップ ウィンドウが表示されます。

ステップ 5　[Cover Page Design] の横にある編集アイコン（）をクリックします。

[Edit Cover Page] ウィンドウが表示され、デフォルトの表紙のデザインが示されます。

ステップ 6　リッチ テキスト エディタで表紙のデザインを編集します。

ステップ 7　[OK] をクリックします。

表紙のデザインが保存され、[Advanced Settings] ウィンドウが再表示されます。

ロゴの管理

ライセンス：すべて

Defense Centerで複数のロゴを保存し、さまざまなレポート テンプレートに関連付けることができます。テンプレートを設計する際に、ロゴの関連付けを設定します。テンプレートをエクスポートすると、エクスポート パッケージにロゴが含まれます。

レポート内のロゴを挿入できる位置については、レポート テンプレート内のドキュメント属性の編集（57-24 ページ）を参照してください。

詳細については、次の関連した手順を参照してください。

- 新しいロゴの追加（57-26 ページ）
- レポート テンプレートのロゴの変更（57-27 ページ）
- ロゴの削除（57-27 ページ）

新しいロゴの追加

ライセンス：すべて

Defense Centerにアップロードしたロゴは、そのDefense Center上のすべてのレポート テンプレートで利用できます。ロゴ イメージは JPG 形式にする必要があります。

ロゴをDefense Centerに追加する方法：

アクセス：Admin/Any Security Analyst

ステップ 1　[Overview] > [Reporting] を選択します。

ステップ 2　[Report Templates] タブを選択します。

[Report Templates] ページが表示されます。

ステップ 3　編集するレポート テンプレートの編集アイコン（）をクリックします。

[Report Sections] ページが表示されます。

ステップ 4　[Advanced] をクリックします。

[Advanced Settings] ポップアップ ウィンドウが表示されます。現在テンプレートと関連付けられているロゴが、[General Settings] の [Logo] の下に表示されます。

ステップ 5　ロゴの編集アイコン（  ）をクリックします。

[Select Logo] ポップアップ ウィンドウが表示され、現在アップロードされているロゴのイメージが示されます。

ステップ 6　[Upload Logo] をクリックします。

[Upload Logo] ポップアップ ウィンドウが表示されます。

ステップ 7　次のいずれかの手順で、アップロードするロゴ ファイルを選択します。

- ロゴ ファイルの場所を入力します。
- [Browse] ボタンをクリックし、ファイルの場所を参照します。

ステップ 8　[Upload] をクリックします。

イメージがDefense Centerにアップロードされ、[Select Logo] ポップアップ ウィンドウに表示されます。

ステップ 9　オプションで、新しいロゴを選択して [OK] をクリックし、現在のテンプレートに関連付けます。

[Advanced Settings] ウィンドウが再表示され、関連付けられたロゴ イメージが表示されます。

レポート テンプレートのロゴの変更

ライセンス： すべて

レポート内のロゴを、Defense Centerにアップロードされている JPG イメージのいずれかに変更できます。たとえば、テンプレートを再使用する場合に、別の組織のロゴをレポートに関連付けることができます。

レポート テンプレートのロゴを変更する方法：

アクセス： Admin/Any Security Analyst

ステップ 1　[Overview] > [Reporting] を選択します。

ステップ 2　[Report Templates] タブを選択します。

[Report Templates] ページが表示されます。

ステップ 3　編集するレポート テンプレートの編集アイコン（  ）をクリックします。

[Report Sections] ページが表示されます。

ステップ 4　[Advanced] をクリックします。

[Advanced Settings] ポップアップ ウィンドウが表示されます。現在テンプレートと関連付けられているロゴが、[General Settings] の [Logo] の下に表示されます。

ステップ 5　ロゴの編集アイコン（  ）をクリックします。

[Select Logo] ポップアップ ウィンドウが表示され、現在アップロードされているロゴのイメージが示されます。

ステップ 6　レポート テンプレートに関連付けるロゴを選択します。

選択したロゴが強調表示されます。

ステップ 7　[OK] をクリックします。

[Advanced Settings] ウィンドウが再表示され、関連付けられたロゴ イメージが表示されます。

ロゴの削除

ライセンス： すべて

ロゴをDefense Centerから削除できます。ロゴを削除すると、そのロゴが使用されているすべてのテンプレートから削除されます。削除を取り消すことはできません。

定義済みのCiscoのロゴを削除できないことに注意してください。

ロゴをDefense Centerから削除する方法：

アクセス： Admin/Any Security Analyst

ステップ 1　[Overview] > [Reporting] を選択します。

ステップ 2　[Report Templates] タブを選択します。

[Report Templates] ページが表示されます。

ステップ 3　編集するレポート テンプレートの編集アイコン（）をクリックします。

[Report Sections] ページが表示されます。

ステップ 4　[Advanced] をクリックします。

[Advanced Settings] ポップアップ ウィンドウが表示されます。現在テンプレートと関連付けられているロゴが、[General Settings] の [Logo] の下に表示されます。

ステップ 5　ロゴの編集アイコン（）をクリックします。

[Select Logo] ポップアップ ウィンドウが表示され、現在アップロードされているロゴのイメージが示されます。

ステップ 6　削除するロゴを選択します。

選択したロゴが強調表示されます。

ステップ 7　[Delete Logo] をクリックします。

削除したロゴが、[Select Logo] ポップアップ ウィンドウで表示されなくなります。

ステップ 8　[OK] をクリックします。

変更内容が保存され、[Advanced Settings] ウィンドウが再表示されます。

レポートの生成と表示

ライセンス： すべて

レポート テンプレートの作成とカスタマイズができたら、レポート生成の準備は終了です。生成プロセスで、レポートの形式（HTML、PDF、または CSV）を選択できます。レポートのグローバル時間枠を調整することもできます。この時間枠は、免除していないすべてのセクションに一貫したタイム フレームを適用します。レポートの時間枠の設定については、テンプレートとそのセクションの時間枠の設定（57-16 ページ）を参照してください。

レポート テンプレートの検索の指定にユーザ入力パラメータが含まれている場合、生成プロセスで値を入力するよう求められ、このレポートの実行内容がデータのサブセットに合わせて調整されます。入力パラメータの詳細については、入力パラメータの使用法（57-19 ページ）を参照してください。

[Reports] タブには、以前に生成されたすべてのレポートと、そのレポート名、生成日時、生成したユーザ、およびそのレポートがローカルに保存されたかリモートに保存されたかが一覧表示されます。ステータスのカラムには、レポートがすでに生成されているか、生成キュー内にある（スケジュール済みタスクの場合など）か、それとも生成できなかった（ディスク領域不足などの理由で）かが示されます。

[Reports] タブのページには、ローカルに保存されたレポートがすべて示されます。現在リモート ストレージが設定されている場合、リモートに保存されたレポートも示されます。ページの下部に、現在設定されているレポート ストレージの場所が表示され、ローカル、NFS、SMB ストレー

ジの場合はディスク使用率も表示されます。SSH を使用してリモート ストレージにアクセスする場合、ディスク使用率のデータは利用できません。リモート ストレージのセットアップの詳細については、レポート用のリモート ストレージの使用法（57-32 ページ）を参照してください。

注　リモートに保存してから、ローカル ストレージに切り替えた場合、リモート ストレージ内のレポートは [Reports] タブのリストに表示されません。同様に、あるリモート ストレージの場所から別の場所に切り替えた場合、以前の場所にあるレポートはリストに表示されません。

Unicode（UTF8）文字を使用したファイル名は PDF レポートではサポートされません。PDF 形式のレポートを生成すると、特殊な Unicode ファイル名が含まれるレポート セクション（ファイル イベントやマルウェア イベントで表示されるセクションなど）では、そのファイル名は書き直された形式で表示されます。

DNS サーバの設定および IP アドレス解決が有効化されている場合、正常に解決されたホスト名がレポートに取り込まれます。詳細については、管理インターフェイスの構成（64-9 ページ）およびイベントのプリファレンス（71-4 ページ）を参照してください。

レポートを生成して表示するには、次の手順を実行します。管理者アクセス権を持つユーザはすべてのレポートを表示でき、その他のユーザは自分が生成したレポートだけを表示できることに注意してください。レポート ファイルの管理については、レポートのダウンロード（57-35 ページ）およびレポートの削除（57-36 ページ）を参照してください。

レポート テンプレートからレポートを生成する方法：

アクセス： Admin/Any Security Analyst

ステップ 1　[Overview] > [Reporting] を選択します。

ステップ 2　[Report Templates] タブをクリックします。

[Report Templates] ページが表示されます。

ステップ 3　使用するテンプレートのレポート生成アイコン（  ）をクリックします。

[Generate Report] ポップアップ ダイアログが表示されます。

ステップ 4　オプションで、[File Name] フィールドに新しい名前を入力します。生成されるレポート ファイルの名前が設定されます。入力パラメータのアイコン（  ）を使用して、1 つ以上の入力パラメータをファイル名に追加することもできます。入力パラメータの詳細については、入力パラメータの使用法（57-19 ページ）を参照してください。

ステップ 5　対応するアイコン（HTML、PDF、または CSV）をクリックして、レポートの出力形式を選択します。

ステップ 6　オプションで、時間枠のアイコン（  ）をクリックして、グローバル時間枠を変更します。

[Events Time Window] ポップアップ ウィンドウが表示されます。イベントの時間枠の設定については、イベント時間の制約の設定（58-26 ページ）を参照してください。

注　グローバル時間枠を設定すると、個々のレポート セクションのうちグローバル設定を継承するように設定されているものの内容だけに影響します。レポート セクションのグローバル時間枠の継承については、テンプレートとそのセクションの時間枠の設定（57-16 ページ）を参照してください。

ステップ 7　[Input Parameters] セクションに表示されるフィールドの値を入力します。

ヒント　フィールドにワイルドカード文字 * を入力すると、ユーザ パラメータを無視できます。こうすると、検索設定がユーザ パラメータで制約されなくなります。

ステップ 8　オプションで、システム ポリシーで電子メール リレー ホストが設定されている場合、[Email] をクリックして、レポートの生成時電子メール配信を自動化します。電子メール配信機能について詳しくは、レポートの生成時の電子メール配布（57-31 ページ）を参照してください。

ステップ 9　求められたら、[OK] をクリックして確認します。

[Report Generation Complete] ポップアップ ウィンドウと、レポートを表示するためのリンクが表示されます。

ステップ 10　次のいずれかをクリックします。

- 新しいウィンドウを開いてレポートを表示する場合は、レポートのリンク。
- [Report Section] ページに戻る場合は、[OK]。このページでレポートの設計を変更できます。

初めて生成した後に、完成したレポートをレビューすることもできます。

ステップ 11　オプションで、レポート ファイルを管理します。詳細については、レポートのダウンロード（57-35 ページ）およびレポートの削除（57-36 ページ）を参照してください。

生成したレポートを表示する方法：

アクセス： Admin/Any Security Analyst

ステップ 1　[Overview] > [Reporting] を選択します。

ステップ 2　[Reports] タブをクリックします。

[Reports] ページが表示されます。

ステップ 3　レポート名をクリックします。

ローカル ホスト上のデフォルトのプログラムにより、新しいウィンドウでレポートが開かれます。

ステップ 4　ドキュメントの確認が終わったら、ブラウザを使用して [Reports] タブに戻ります。

レポート生成オプションの使用法

ライセンス： すべて

レポートを生成する際の追加のオプションが複数あります。レポートの生成を自動的にスケジュールしたり、レポートを電子メールで送信したり、生成したレポートをリモートに保存したりできます。詳細については、次の項を参照してください。

- スケジューラを使用したレポートの生成（57-31 ページ）
- レポートの生成時の電子メール配布（57-31 ページ）
- レポート用のリモート ストレージの使用法（57-32 ページ）

スケジューラを使用したレポートの生成

ライセンス：すべて

FireSIGHT システムのスケジューラを使用して、レポートの生成を自動化できます。毎日、毎週、毎月など、さまざまな範囲のタイム フレームに基づいたスケジュールでもカスタマイズできます。詳細については、レポートの生成を自動化する方法（62-9 ページ）を参照してください。

また、スケジューラを使用して電子メール レポートを配布する場合は、タスクをスケジュールする**前に**、レポート テンプレートとメール リレー ホストの設定が必要です。詳細については、レポートの生成時の電子メール配布（57-31 ページ）およびメール リレー ホストおよび通知アドレスの設定（63-19 ページ）を参照してください。

レポートの生成時の電子メール配布

ライセンス：すべて

レポートをテンプレートから生成するときには、レポートを電子メールの添付ファイルとして受信者のリストに自動的に送信するよう選択できます。

注　レポートを電子メールで配信するように、メール リレー ホストを適切に設定していなければなりません。以前にメール ホストをセットアップしていない場合は、メール リレー ホストおよび通知アドレスの設定（63-19 ページ）を参照してください。

レポートを生成時に電子メールで送信する方法：

アクセス：Admin/Any Security Analyst

ステップ 1　[Overview] > [Reporting] を選択します。

ステップ 2　[Report Templates] タブを選択します。

[Report Templates] ページが表示されます。

ステップ 3　生成元のテンプレートのレポート生成アイコン（  ）をクリックします。

[Generate Report] ポップアップ ウィンドウが表示されます。

ステップ 4　このウィンドウの [Email] セクションを展開します。

ステップ 5　[Email Options] フィールドで、[Send Email] を選択します。

ステップ 6　[Recipient List]、[CC] および [BCC] フィールドで、カンマ区切りリストの形式で受信者の電子メール アドレスを入力します。

ステップ 7　[Subject] フィールドに電子メールの件名を入力します。

ヒント　[Subject] フィールドやメッセージ本文に入力パラメータを使用して、電子メール内にタイムスタンプやDefense Centerの名前などの情報を動的に生成できます。詳細については、入力パラメータの使用法（57-19 ページ）を参照してください。

ステップ 8　必要に応じて、電子メールの本文にカバレターを入力します。さまざまなフォント、番号リスト、箇条書きリストなどのリッチ テキスト機能を使用できます。

ステップ 9　[Generate Report] ウィンドウのすべてのフィールドが正しい場合は、[OK] をクリックして確認します。

システムにより、生成されたレポートが電子メールで配布されます。システム ポリシーで、[Email Notification] を利用して電子メールの送信元アドレスを設定できます。詳細については、システム ポリシーの管理（63-1 ページ）を参照してください。

レポート用のリモート ストレージの使用法

ライセンス： すべて

新しく生成されたレポート ファイルを設定済みのリモート ストレージの場所に置くように、レポート作成システムを設定できます。ローカルに保存されたレポートを、リモート ストレージの場所に移動することもできます。

注　リモート ストレージ内のレポートを移動してローカル ストレージに戻すことはできません。

リモート ストレージを使用するには、まずリモート ストレージの場所を設定します。リモート ストレージの場所を設定すると、レポート リストの下部に表示されます。NFS および SMB がマウントされたストレージの場合、この場所には現在のディスク使用状況も示されますが、SSH の場合は示されません。設定情報については、リモート ストレージの管理（64-17 ページ）を参照してください。

生成したレポートをリモートに保存する方法：

アクセス： Admin/Any Security Analyst

ステップ 1　[Overview] > [Reporting] を選択します。

ステップ 2　[Reports] タブを選択します。

[Reports] ページが表示されます。

ステップ 3　ページ下部の [Enable Remote Storage of Reports] チェック ボックスを選択します。

Defense Centerにより、新しく生成されたレポートが、ページの下部に示されているリモートの場所に保存されます。これらのレポートの [Location] カラム データは、[Remote] になります。

バッチ モードまたは単独で、ローカル ストレージ内のレポートをリモート ストレージの場所に移動できます。

生成したレポートをローカル ストレージからリモート ストレージに移動する方法：

アクセス： Admin/Any Security Analyst

ステップ 1　[Overview] > [Reporting] を選択します。

ステップ 2　[Reports] タブを選択します。

[Reports] ページが表示されます。

ステップ 3　移動するレポートの横にあるチェック ボックスを選択して、[Move] をクリックします。

ヒント ページ上のすべてのレポートを移動するには、そのページの左上にあるチェック ボックスを選択します。複数のレポートが複数のページにある場合は、2 つ目のチェック ボックスが表示され、すべてのページ上のすべてのレポートを移動するよう選択できます。

ステップ 4 レポートを移動することを確認します。

レポートが移動されます。

レポート テンプレートとレポート ファイルの管理

ライセンス： すべて

テンプレートの作成と編集に加えて、次のテンプレートの管理タスクを実行できます。

- レポート テンプレートのエクスポートとインポート（57-33 ページ）
- レポート テンプレートの削除（57-34 ページ）

生成されたレポート ファイルに対して次の管理タスクも実行できます。

- レポートのダウンロード（57-35 ページ）
- レポートの削除（57-36 ページ）

レポート テンプレートのエクスポートとインポート

ライセンス： すべて

レポート テンプレートをエクスポートする際に生成するファイルには、別のDefense Centerで同じレポートを作成するのに必要なすべてのデータが含まれます。エクスポート ファイルは独自の SFO 形式で、次のものが含まれます。

- レポート テンプレート、およびすべてのセクションの設計要素とドキュメント属性
- レポートで使用されるすべての保存済みの検索設定
- レポートで使用されるすべてのイメージ
- レポートで使用されるすべてのカスタム テーブル

自動レポート生成スケジュールの設定だけは、別のDefense Centerにテンプレートをインポートした後に必要になることがあります。

注 レポート テンプレートをインポートしたりエクスポートしたりするには、両方のDefense Centerのソフトウェア バージョン レベルが同じである必要があります。

レポート テンプレートをエクスポートする方法：

アクセス： Admin

ステップ 1 [Overview] > [Reporting] を選択します。

ステップ 2 [Report Templates] タブを選択します。

[Report Templates] ページが表示されます。

ステップ 3　エクスポートするテンプレートのエクスポート アイコン( )をクリックします。

システムにより、拡張子が .sfo の設定パッケージ ファイルが作成され、[Opening Object] ポップアップ ウィンドウが開かれてパッケージのファイル名が表示されます。

ステップ 4　[Save file] と [OK] を選択して、ローカル コンピュータにファイルを保存します。

ステップ 5　.sfo パッケージの名前を変更し、後で参考になるように説明的な名前にすることができます。パッケージ名にかかわらず、パッケージをインポートすると、インポート先のDefense Centerでは元のDefense Centerと同じ名前がテンプレートに付けられます。

Defense Centerからエクスポートされる SFO ファイルには、別のDefense Centerにレポート テンプレートを追加するのに必要なすべての要素が含まれています。したがって、インポート プロセスで必要なのは、2 つ目のDefense Centerにパッケージをアップロードすることと、インポート プロセスを実行することだけです。

レポート テンプレートをインポートする方法:

アクセス: Admin

ステップ 1　[System] > [Tools] > [Import/Export] を選択します。

[Import/Export] ページが表示され、Defense Center上のレポート テンプレートのリストが示されます。

ステップ 2　[Upload Package] をクリックします。

[Package Name] ページが表示されます。

ステップ 3　次の 2 つのオプションから選択できます。

- アップロードするパッケージへのパスを入力します。
- [Browse] をクリックして、パッケージを見つけます。

ステップ 4　[Upload] をクリックします。

設定リストの [Report Template] セクションが表示され、インポートするテンプレートが示されます。

ステップ 5　テンプレートの横にあるチェック ボックスを選択し、[Import] をクリックします。

このテンプレートが、インポート先のDefense Centerの設定のリストに表示されます。

レポート テンプレートの削除

ライセンス: すべて

レポート テンプレートは、削除しない限り、再利用できるように [Report Templates] タブにリストされたままになります。Ciscoから提供されているレポート テンプレートは削除できないことに注意してください。

注　セキュリティ アナリストは、自分が作成したレポート テンプレートだけを削除できます。

レポート テンプレートを削除する方法:

アクセス: Admin/Any Security Analyst

ステップ 1　[Overview] > [Reporting] を選択します。

ステップ 2　[Report Templates] タブを選択します。

[Report Templates] ページが表示されます。

ステップ 3　削除するテンプレートの隣にある削除アイコン( )をクリックして確認します。

テンプレート名がリストから削除されます。

レポートのダウンロード

ライセンス: すべて

ローカル コンピュータにレポート ファイルをダウンロードできます。そのコンピュータから、電子メールや他の使用可能な方法で電子的に配布できます。レポートを生成時に電子メールで自動的に配布することについて詳しくは、レポートの生成時の電子メール配布 (57-31 ページ)を参照してください。

レポートをダウンロードする方法:

アクセス: Admin/Any Security Analyst

ステップ 1　[Overview] > [Reporting] を選択します。

ステップ 2　[Reports] タブを選択します。

[Reports] ページが表示されます。

ステップ 3　ダウンロードするレポートの横にあるチェック ボックスを選択し、[Download] をクリックします。

ヒント　ページ上のすべてのレポートをダウンロードするには、そのページの左上にあるチェック ボックスを選択します。複数のレポートが複数のページにある場合は、2 つ目のチェック ボックスが表示され、すべてのページ上のすべてのレポートをダウンロードするよう選択できます。

ステップ 4　ブラウザのプロンプトに従って、レポートをダウンロードします。

複数のレポートを選択すると、1 つの `.zip` ファイルでダウンロードされます。

レポートの削除

ライセンス：すべて

レポート ファイルはいつでも削除できます。この手順ではファイルが完全に削除され、リカバリは不可能になります。レポートの生成に使用したレポート テンプレートがまだ残っていますが、時間枠を拡大したりスライドしたりした場合は、特定のレポート ファイルを再生成するのは難しくなることがあります。時間枠の詳細については、レポート テンプレートのセクションの編集（57-13 ページ）を参照してください。テンプレートで入力パラメータを使用した場合も、再生成するのが難しくなることがあります。入力パラメータの使用法の詳細については、入力パラメータの使用法（57-19 ページ）を参照してください。

レポートを削除する方法：

アクセス：Admin/Any Security Analyst

ステップ 1　[Overview] > [Reporting] を選択します。

ステップ 2　[Reports] タブを選択します。

[Reports] ページが表示されます。

ステップ 3　削除するレポートの隣のチェック ボックスを選択し、[Delete] をクリックします。

ヒント　ページ上のすべてのレポートを削除するには、そのページの左上にあるチェック ボックスを選択します。複数のレポートが複数のページにある場合は、2 つ目のチェック ボックスが表示され、すべてのページ上のすべてのレポートを削除するよう選択できます。

ステップ 4　削除を確認します。

レポートが削除されます。

ワークフローの概要と使用

ワークフローはDefense Centerの Web インターフェイス上でユーザに合わせて作成された一連のデータ ページで、アナリストはワークフローを使用して、システムで生成されたイベントを評価することができます。Defense Centerには、次の 3 つのタイプのワークフローがあります。

- *事前定義ワークフロー*: システムにインストールされているプリセット ワークフローで、ユーザは変更または削除できません。
- *保存済みのカスタム ワークフロー*: 事前に定義されているカスタム ワークフローで、ユーザは変更または削除できます。
- *カスタム ワークフロー*: ユーザが作成し、自身のニーズに合わせてカスタマイズするワークフローです。

たとえば、侵入イベントを分析する場合は、このタスク用に作成されたいくつかの事前定義ワークフローから選択することができます。

ワークフローに表示されるデータは、ほとんどの場合、管理対象デバイスのライセンスおよび導入方法、データを提供する機能を設定しているかどうか(シリーズ 2 アプライアンスおよびCisco NGIPS for Blue Coat X-Seriesの場合は、アプライアンスがデータを提供する機能をサポートしているかどうか)によって異なります。たとえば、DC500 Defense Centerおよび シリーズ 2 のデバイスは、カテゴリおよびレピュテーションによる URL フィルタリングをサポートしていないため、DC500 Defense Centerではこの機能のデータが表示されず、シリーズ 2 デバイスはこのデータを検出しません。

事前定義ワークフローおよびカスタム ワークフローの使用に関する詳細は、次の項を参照してください。

- ワークフローのコンポーネント(58-1 ページ)
- ワークフローの使用(58-17 ページ)
- カスタムワークフローの使用(58-43 ページ)

ヒント カスタム ワークフローを、イベント レポートのベースとして使用することもできます。詳細については、「レポートの操作(57-1 ページ)」を参照してください。

ワークフローのコンポーネント

ライセンス: すべて

ワークフローには、以下の項に記載されているように、複数のタイプのページを含めることができます。

テーブル ビュー

テーブル ビューには、ワークフローのベースとなるデータベースの各フィールドに対するカラムが含まれています。

たとえば、検出イベントのテーブル ビューには、[Time]、[Event]、[IP Address]、[User]、[MAC Address]、[MAC Vendor]、[Port]、[Description]、および [Device] カラムが含まれています。

また、サーバのテーブル ビューには、[Last Used]、[IP Address]、[Port]、[Protocol]、[Application Protocol]、[Vendor]、[Version]、[Web Application]、[Application Risk]、[Business Relevance]、[Hits]、[Source Type]、[Device]、および [Current User] カラムが含まれています。

ドリルダウン ページ

ドリルダウン ページには、データベースで使用できるカラムのサブセットが含まれています。

たとえば、検出イベントのドリルダウン ページには、[IP Address]、[MAC Address]、および [Time] カラムのみが含まれています。また、侵入イベントのドリルダウン ページには、[Priority]、[Impact Flag]、[Inline Result]、および [Message] カラムが含まれています。

一般的にドリルダウン ページは、テーブル ビューのページに移動する前にユーザが使用して調査対象を絞り込むための中間ページです。

グラフ

接続データに基づくワークフローには、グラフ ページ（*接続グラフ*とも呼ばれる）を含めることができます。

たとえば接続グラフには、一定期間にシステムで検出された接続の数を示す線グラフを表示することができます。一般的に接続グラフは、ドリルダウン ページと同様に、ユーザが調査対象を絞り込むために使用する中間ページです。詳細については、接続グラフの使用（39-17 ページ）を参照してください。

最終ページ

ワークフローの最終ページは、ワークフローがベースとするイベントのタイプによって異なります。

- ホスト ビューは、アプリケーション、アプリケーションの詳細、検出イベント、ホスト、侵害の痕跡（IOC）、サーバ、または任意のタイプの脆弱性に基づいたワークフローの最終ページです。このページからホスト プロファイルを表示することにより、ユーザは、複数のアドレスを持つホストに関連付けられているすべての IP アドレス上のデータを簡単に表示することができます。詳細については、ホスト プロファイルの使用（49-1 ページ）を参照してください。
- ユーザの詳細ビューは、ユーザ、およびユーザ アクティビティに基づいたワークフローの最終ページです。詳細については、ユーザの詳細とホストの履歴について（50-68 ページ）を参照してください。
- 脆弱性の詳細ビューは、Ciscoの脆弱性に基づいたワークフローの最終ページです。詳細については、脆弱性の詳細の表示（49-30 ページ）を参照してください。
- パケット ビューは、侵入イベントに基づいたワークフローの最終ページです。詳細については、パケット ビューの使用（41-23 ページ）を参照してください。

他の種類のイベント（監査ログ イベントやマルウェア イベントなど）に基づいたワークフローには、最終ページがありません。

ワークフローの詳細については、以下の項を参照してください。

- 事前定義ワークフローとカスタム ワークフローの比較（58-3 ページ）
- 事前定義テーブルとカスタム テーブルのワークフローの比較（58-4 ページ）

事前定義ワークフローとカスタム ワークフローの比較

ライセンス: すべて

FireSIGHT システムには、(これ以降の項で説明されている) *事前定義*ワークフローのセットが付随しており、ユーザはこれを使用して、イベントや収集した他のデータを分析することができます。

カスタム ワークフローは、組織に特有のニーズに合わせて作成するワークフローです。カスタム ワークフローを作成する場合は、ワークフローのベースとなるイベント(またはデータベース テーブル)の種類を選択します。Defense Centerでは、カスタム ワークフローをカスタム テーブルのベースにすることができます。また、カスタム ワークフローに含まれるページを選択することもできます。カスタム ワークフローには、ドリルダウン、テーブル ビュー、ホストまたはパケット ビューのページを含めることができます。

Defense Centerには、いくつかの*保存済みのカスタム ワークフロー*が付属しています。このワークフローは、Defense Centerに付属している保存済みのカスタム テーブルに基づいています。事前定義のテーブルとカスタム テーブルに基づいたワークフローの違いについては、次の項事前定義テーブルとカスタム テーブルのワークフローの比較で説明します。

事前定義テーブルとカスタム テーブルのワークフローの比較

ライセンス：FireSIGHT

カスタム テーブルの機能を使用して、複数のイベント タイプのデータを使用するテーブルを作成することができます。これにより、たとえば、ユーザが侵入イベントのデータと検出データを関連付けるテーブルおよびワークフローを作成して、重要なシステムに影響を及ぼすイベントを簡単に検索できるようになるため、役立ちます。カスタム テーブルの作成については、カスタム テーブルの使用（59-1 ページ）を参照してください。

それぞれのカスタム テーブルにはデフォルトでワークフローが含まれており、これを使用して、テーブルに関連付けられているイベントを表示することができます。ワークフローの機能は、使用するテーブルのタイプによって異なります。たとえば、侵入イベント テーブルに基づいたカスタム テーブルのワークフローは、必ずパケット ビューで終了します。ただし、検出イベントに基づいたカスタム テーブルのワークフローは、必ずホスト ビューで終了します。

事前定義のイベント テーブルに基づいたワークフローとは異なり、カスタム テーブルに基づいたワークフローには、他のタイプのワークフローへのリンクがありません。

事前定義の侵入イベント ワークフロー

ライセンス：Protection

次の表で、FireSIGHT システムに含まれている事前定義の侵入イベント ワークフローについて説明します。これらのワークフローへのアクセスについては、侵入イベントの表示（41-9 ページ）および侵入イベントについて（41-17 ページ）を参照してください。

表 58-1　事前定義の侵入イベント ワークフロー

ワークフロー名	説明
宛先ポート	宛先ポートは通常、アプリケーションに関連付けられているため、このワークフローは、通常以上に大量のアラートが発生しているアプリケーションを検出するのに役に立ちます。[Destination Port] カラムは、ネットワークに存在してはいけないアプリケーションを識別するうえでも役に立ちます。 このワークフローは、侵入イベントに関連付けられている宛先ポートを表示するページから始まり、その後に、生成されたイベント タイプを表示するページが続きます。ここで、（イベントのテーブル ビューと呼ばれる）イベント情報の表形式のビューを表示し、次に、各イベントに関連付けられているパケットの復号化されたコンテンツを表示するパケット ビューを表示することができます。
Event-Specific（イベントに特有）	このワークフローには、2 つの便利な機能があります。頻繁に発生するイベントには、以下のことを示している可能性があります。 • 誤検出 • ワーム • 設定が大幅に間違っているネットワーク 頻繁に発生するイベントはほとんどの場合、攻撃の対象にされており、特別な注意が必要であることを意味しています。 このワークフローは、生成されたイベントのタイプを示すページから始まります。ここで、2 つのテーブル（イベントに関連付けられている送信元 IP アドレスを示すテーブルと、イベントに関連付けられている宛先 IP アドレスを示すテーブル）を持つページを表示できます。ワークフローの最終ページは、イベントのテーブル ビューとパケット ビューです。

表 58-1　事前定義の侵入イベント ワークフロー(続き)

ワークフロー名	説明
Events by Priority and Classification(優先度および分類に基づいたイベント)	このワークフローは、イベントおよびイベントのタイプを、イベントの優先度の順に表示し、各イベントが発生した回数も示します。 このワークフローは、優先度のレベル、分類、および表示されている各イベントのカウントが含まれているドリルダウン ページから始まります。ワークフローの最終ページは、イベントのテーブル ビューとパケット ビューです。
Events to Destinations(イベントと宛先)	このワークフローは、どのホスト IP アドレスが攻撃されているか、また攻撃の性質について概要レベルのビューを提供します。可能な場合には、攻撃に関与している国の情報も表示することができます。 このワークフローは、イベント タイプと宛先 IP アドレスのペアが示されているページから始まります。これによりユーザは、特定の IP アドレスに対してどのタイプのイベントが発生しているかを調べることができます。ワークフローの最終ページは、イベントのテーブル ビューとパケット ビューです。
IP-Specific(IP に特有)	このワークフローは、最も多くのアラートを生成しているホスト IP アドレスを示します。最も多くのイベントが生じているホストは、公開されていて、ワーム タイプのトラフィックを受け取っている(チューニングに適した場所であることを示している)か、あるいはアラートの原因を決定するためにさらに調査が必要です。カウントが最も少ないホストも攻撃の対象となる可能性があるため、調査が必要です。カウントが少ないことは、ホストがネットワークに属していない可能性があることも示しています。 このワークフローは、2 つのテーブル(イベントに関連付けられている送信元 IP アドレスのテーブルと、イベントに関連付けられている宛先 IP アドレスのテーブル)を表示するページから始まります。次のページで、生成されたイベント タイプを示します。ワークフローの最終ページは、イベントのテーブル ビューとパケット ビューです。
Impact and Priority(影響および優先度)	このワークフローを使用して、影響が大きく、繰り返し発生するイベントをすばやく見つけることができます。報告される影響レベルは、イベントが発生した回数と合わせて表示されます。この情報を使用して、最も頻繁に再発する、影響の大きいイベントを特定することができます。このようなイベントは、ネットワーク上の広範囲に攻撃が存在していることを示している可能性もあります。 このワークフローは、各イベントに関連付けられている影響のレベル、優先度、およびカウントを示すページから始まります。次に、各イベントの送信元および宛先の IP アドレスを示したドリルダウン ページが表示されます。2 ページ目のイベントは、カウントでソートされています。ワークフローの最終ページは、イベントのテーブル ビューとパケット ビューです。
Impact and Source(影響および送信元)	このワークフローは、進行中の攻撃の発生源を特定する場合に役立ちます。報告される影響レベルは、イベントに関連付けられている送信元 IP アドレスと合わせて表示されますたとえば、特定の IP アドレスからレベル 1 の影響度のイベントが繰り返し発生している場合は、脆弱なシステムを特定し、それらのシステムをターゲットにしている攻撃者が存在していることを示している可能性があります。 このワークフローは、各イベントに関連付けられている影響のレベル、送信元 IP アドレス、優先度、およびカウントを示すページから始まります。各イベントのレベル内で、イベントはカウントでソートされ、次に優先度でソートされます。次に、各イベントの送信元および宛先の IP アドレスを示したドリルダウン ページが表示されます。2 ページ目のイベントは、カウントでソートされています。ワークフローの最終ページは、イベントのテーブル ビューとパケット ビューです。

表 58-1　事前定義の侵入イベント ワークフロー（続き）

ワークフロー名	説明
Impact to Destination（影響と宛先）	このワークフローを使用して、脆弱なコンピュータで繰り返し発生しているイベントを特定することができます。これにより、システム上の脆弱性に対処し、進行中の攻撃を停止することが可能になります。 このワークフローは、各イベントに関連付けられている影響のレベル、インラインの結果（パケットがドロップしたか、またはドロップする可能性があったかどうか）、宛先 IP アドレス、優先度、およびカウントを示すページから始まります。各イベントのレベル内で、イベントはカウントでソートされ、次に優先度でソートされます。次に、各イベントの送信元および宛先の IP アドレスを示したドリルダウン ページが表示されます。2 ページ目のイベントは、カウントでソートされています。ワークフローの最終ページは、イベントのテーブル ビューとパケット ビューです。
送信元ポート	このワークフローは、最も多くのアラートを生成しているサーバを示します。この情報を使用して、調整が必要なエリアを特定し、注意が必要なサーバを決定することができます。 このワークフローは、侵入イベントに関連付けられている送信元ポートを表示するページから始まり、その後に、生成されたイベント タイプを表示するページが続きます。ワークフローの最終ページは、イベントのテーブル ビューとパケット ビューです。
送信元と宛先	このワークフローは、高レベルのアラートを共有しているホスト IP アドレスを特定します。リストの先頭のペアは誤検出である可能性がありますが、調整が必要なエリアを特定している場合があります。リストの下部に示されているペアをチェックして、対象となる攻撃、アクセスが禁止されているリソースにアクセスしているユーザ、ネットワークに属さないホストを調べることができます。 このワークフローは、各イベントの送信元および宛先 IP アドレスを表示するページから始まり、その後に、生成されたイベント タイプを表示するページが続きます。ワークフローの最終ページは、イベントのテーブル ビューとパケット ビューです。

事前定義のマルウェア ワークフロー

ライセンス： すべて

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

次の表で、Defense Centerに含まれている事前定義のマルウェア ワークフローについて説明します。すべての事前定義のマルウェア ワークフローは、マルウェア イベントのテーブル ビューを使用します。

DC500 シリーズ 2 Defense Center、シリーズ 2 のデバイス、およびCisco NGIPS for Blue Coat X-Seriesは、高度なマルウェア防御をサポートしていないため、DC500 Defense Centerではこの機能のデータが表示されないことと、シリーズ 2 デバイスおよびCisco NGIPS for Blue Coat X-Seriesはこのデータを検出しないことに注意してください。

マルウェア イベントへのアクセスについては、マルウェア イベントの操作（40-17 ページ）を参照してください。

表 58-2　事前定義のマルウェア ワークフロー

ワークフロー名	説明
Malware Summary（マルウェアの概要）	このワークフローは、ネットワーク トラフィックで検出されたマルウェア、またはエンドポイントベースの FireAMP コネクタで検出されたマルウェアを、脅威ごとにグループ化して表示します。
Malware Event Summary（マルウェア イベントの概要）	このワークフローは、さまざまなマルウェア イベントのタイプおよびサブタイプについて詳細な情報を迅速に提供します。
Hosts Receiving Malware（マルウェアを受信したホスト）	このワークフローは、マルウェアを受信したホスト IP アドレスのリストを、マルウェア ファイルに関連付けられている処理ごとにグループ化して提供します。
Hosts Sending Malware（マルウェアを送信したホスト）	このワークフローは、マルウェアを送信したホスト IP アドレスのリストを、マルウェア ファイルに関連付けられている処理ごとにグループ化して提供します。
Applications Introducing Malware（マルウェアを取り込んだアプリケーション）	このワークフローは、ファイルを受信したホスト IP アドレスのリストを、これらのファイルに関連付けられているマルウェアの処理ごとにグループ化して提供します。

事前定義のファイル ワークフロー

ライセンス： Protection

次の表で、Defense Centerに含まれている事前定義のファイル イベント ワークフローについて説明します。すべての事前定義のファイル イベント ワークフローは、ファイル イベントのテーブル ビューを使用します。ファイル イベントへのアクセスについては、ファイル イベントの操作（40-8 ページ）を参照してください。

表 58-3　事前定義のファイル ワークフロー

ワークフロー名	説明
File Summary（ファイルの概要）	このワークフローは、さまざまなファイル イベントのカテゴリとタイプ、および関連するすべてのマルウェアの処理について詳細な情報を迅速に提供します。
Hosts Receiving Files（ファイルを受信したホスト）	このワークフローは、ファイルを受信したホスト IP アドレスのリストを、これらのファイルに関連付けられているマルウェアの処理ごとにグループ化して提供します。
Hosts Sending Files（ファイルを送信したホスト）	このワークフローは、ファイルを送信したホスト IP アドレスのリストを、これらのファイルに関連付けられているマルウェアの処理ごとにグループ化して提供します。

事前定義されたキャプチャ ファイル ワークフロー

ライセンス： Malware

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能に応じて異なる

次の表で、Defense Centerに含まれている事前定義のキャプチャ ファイルワークフローについて説明します。すべての事前定義のキャプチャ ファイル ワークフローは、キャプチャ ファイルのテーブル ビューを使用します。

DC500 シリーズ 2 Defense Center、シリーズ 2 のデバイス、およびCisco NGIPS for Blue Coat X-Seriesは、高度なマルウェア防御をサポートしていないため、DC500 Defense Centerではこの機能のデータが表示されないことと、シリーズ 2 デバイスおよびCisco NGIPS for Blue Coat X-Seriesはこのデータを検出しないことに注意してください。

キャプチャ ファイルへのアクセスについては、キャプチャ ファイルの操作（40-32 ページ）を参照してください。

表 58-4　事前定義されたキャプチャ ファイル ワークフロー

ワークフロー名	説明
Captured File Summary（キャプチャ ファイルの概要）	このワークフローは、タイプ、カテゴリ、および脅威のスコアに基づいてキャプチャ ファイルについての詳細な情報を提供します。
Dynamic Analysis Status（動的解析のステータス）	このワークフローは、キャプチャ ファイルが動的解析用に送信されたかどうかに基づいて、キャプチャ ファイルのカウントを提供します。

事前定義の接続データ ワークフロー

ライセンス：FireSIGHT

次の表で、Defense Centerに含まれている事前定義の接続データ ワークフローについて説明します。すべての事前定義の接続データ ワークフローは、接続データのテーブル ビューを使用します。接続データへのアクセスについては、接続およびセキュリティ インテリジェンスのデータの表示（39-15 ページ）を参照してください。

表 58-5　事前定義の接続データ ワークフロー

ワークフロー名	説明
Connection Events	このワークフローは、基本的な接続および検出されたアプリケーションの情報についての概要ビューを提供します。ユーザはこれを使用して、イベントのテーブル ビューへドリル ダウンすることができます。
Connections by Application（接続に基づいたアプリケーション）	このワークフローには、検出された接続の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のアプリケーションのグラフが含まれています。
Connections by Initiator（接続に基づいた発信側）	このワークフローには、ホストが接続トランザクションを開始した接続の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のホスト IP アドレスのグラフが含まれています。
Connections by Port（接続に基づいたポート）	このワークフローには、検出された接続の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のポートのグラフが含まれています。
Connections by Responder（接続に基づいた応答側）	このワークフローには、ホスト IP が接続トランザクションの応答側であった接続の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のホスト IP アドレスのグラフが含まれています。
Connections over Time（一定期間の接続）	このワークフローには、モニタリング対象のネットワーク セグメントにおける、一定期間の接続の合計数のグラフが含まれています。

表 58-5　事前定義の接続データ ワークフロー（続き）

ワークフロー名	説明
Traffic by Application（トラフィックに基づいたアプリケーション）	このワークフローには、送信されたキロバイト数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のアプリケーションのグラフが含まれています。
Traffic by Initiator（トラフィックに基づいた発信側）	このワークフローには、各アドレスから送信されたキロバイト数の合計に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のホスト IP アドレスのグラフが含まれています。
Traffic by Port（トラフィックに基づいたポート）	このワークフローには、送信されたキロバイト数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のポートのグラフが含まれています。
Traffic by Responder（トラフィックに基づいた応答側）	このワークフローには、各アドレスが受信したキロバイト数の合計に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のホスト IP アドレスのグラフが含まれています。
Traffic over Time	このワークフローには、モニタリング対象のネットワーク セグメントにおける、一定期間に送信されたキロバイト数の合計のグラフが含まれています。
Unique Initiators by Responder（一意の発信側に基づいた応答側）	このワークフローには、各アドレスに接続した一意の発信側の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな応答側の 10 個のホスト IP アドレスのグラフが含まれています。
Unique Responders by Initiator（一意の応答側に基づいた発信側）	このワークフローには、アドレスが接続した一意の応答側の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな送信側の 10 個のホスト IP アドレスのグラフが含まれています。

事前定義のセキュリティ インテリジェンス ワークフロー

ライセンス： Protection

サポートされるデバイス： すべて（シリーズ 2 を除く）

サポートされる防御センター： DC500 を除くいずれか

次の表で、Defense Centerに含まれている事前定義のセキュリティ インテリジェンス ワークフローについて説明します。すべての事前定義のセキュリティ インテリジェンス ワークフローは、セキュリティ インテリジェンス イベントのテーブル ビューを使用します。セキュリティ インテリジェンス イベント データへのアクセスについては、接続およびセキュリティ インテリジェンスのデータの表示（39-15 ページ）を参照してください。

表 58-6　事前定義のセキュリティ インテリジェンス ワークフロー

ワークフロー名	説明
Security Intelligence Events	このワークフローは、基本的なセキュリティ インテリジェンスおよび検出されたアプリケーションの情報についての概要ビューを提供します。ユーザはこれを使用して、イベントのテーブル ビューへドリル ダウンすることができます。
Security Intelligence Summary（セキュリティ インテリジェンスの概要）	このワークフローは [Security Intelligence Events（セキュリティ インテリジェンス イベント）] ワークフローと同じですが、[Security Intelligence Summary] ページで始まります。このページには、カテゴリおよびカウントのみによってセキュリティ インテリジェンス イベントが表示されます。

事前定義のホスト ワークフロー

ライセンス：FireSIGHT

次の表で、ホスト データで使用できる事前定義のワークフローについて説明します。

表 58-7　事前定義のホスト ワークフロー

ワークフロー名	説明
ホスト	このワークフローには、ホストのテーブル ビューが含まれており、その後にホスト ビューが続きます。ホスト テーブルに基づいたワークフロー ビューにより、ホストに関連付けられているすべての IP アドレスに関するデータを簡単に表示することができます。詳細については、「ホストの表示（50-21 ページ）」を参照してください。
Operating System Summary（オペレーティング システムの概要）	このワークフローを使用して、ネットワークで使用されているオペレーティング システムを分析することができます。このワークフローには一連のページがあり、ネットワーク上のオペレーティング システム、およびオペレーティング システムのベンダーのリストを示すページから始まり、オペレーティング システムの各バージョンを実行しているホスト数を示すページが続きます。次のページには、重要度、IP アドレス、および NetBIOS 名別にホストがリストされ、関連するオペレーティング システムおよびオペレーティング システムのベンダーも示されます。このワークフローは、ホストのテーブル ビュー、およびその後に続くホスト ビューで終了します。詳細については、「ホストの表示（50-21 ページ）」を参照してください。

事前定義の侵害の痕跡ワークフロー

ライセンス：FireSIGHT

次の表は、IOC（侵害の痕跡）データで使用できる事前定義のワークフローについて説明します。

表 58-8　事前定義の侵害の痕跡ワークフロー

ワークフロー名	説明
Indications of Compromise（侵害の痕跡）	このワークフローは、カウントおよびカテゴリによってグループ化された IOC データの概要ビューで始まり、その後で、イベント タイプによってサマリー データを細分化した詳細ビューが示されます。次に、IOC データの完全なテーブル ビューが示されます。このワークフローは、ホスト ビューで終了します。IOC データの表示と解釈の詳細については、侵害の痕跡の使用（50-35 ページ）を参照してください。
Indications of Compromise by Host（ホストごとの侵害の痕跡）	このワークフローを使用して、ネットワーク上のどのホストが最も侵害されそうかを（IOC データに基づいて）判断できます。このワークフローには、IOC データ カウント別のホスト IP アドレスのビューが含まれており、その後に IOC データのテーブル ビューがあり、ホスト ビューで終了します。IOC データの表示と解釈の詳細については、侵害の痕跡の使用（50-35 ページ）を参照してください。

事前定義のアプリケーション ワークフロー

ライセンス：FireSIGHT

次の表で、アプリケーション データで使用できる事前定義のワークフローについて説明します。

表 58-9　事前定義のアプリケーション ワークフロー

ワークフロー名	説明
Application Business Relevance（アプリケーションのビジネスの関連性）	このワークフローを使用して、ネットワーク上で推定されるそれぞれのビジネスの関連性レベルの実行中アプリケーションを分析できます。これにより、ネットワーク リソースの適切な使用を監視することができます。このワークフローは、それぞれの関連性レベルのアプリケーションを実行しているホストのカウントで始まり、その後に対象のビジネスの関連性レベルおよびホスト カウントを持つ個々のアプリケーションのテーブルが続き、アプリケーションのテーブル ビュー、ホスト ビューと続きます。詳細については、「アプリケーションの表示（50-45 ページ）」を参照してください。
Application Category	このワークフローを使用して、ネットワーク上の各カテゴリ（電子メール、検索エンジン、ソーシャル ネットワークなど）の実行中アプリケーションを分析できます。これにより、ネットワーク リソースの適切な使用を監視することができます。このワークフローは、各カテゴリのアプリケーションを実行しているホストのカウントで始まり、その後に個々のアプリケーションを実行しているホストのカウント、アプリケーションのテーブル ビュー、ホスト ビューと続きます。詳細については、「アプリケーションの表示（50-45 ページ）」を参照してください。
Application Risk（アプリケーションのリスク）	このワークフローを使用して、ネットワーク上で推定されるそれぞれのセキュリティ リスク レベルの実行中アプリケーションを分析できます。これにより、ユーザ アクティビティの潜在的なリスクを推定し、適切なアクションを実行することができます。このワークフローは、それぞれのリスク レベルのアプリケーションを実行しているホストのカウントで始まり、その後に対象のビジネスの関連性レベルおよびホスト カウントを持つ個々のアプリケーションのテーブルが続き、アプリケーションのテーブル ビュー、ホスト ビューと続きます。詳細については、「アプリケーションの表示（50-45 ページ）」を参照してください。
Application Summary（アプリケーションの概要）	このワークフローを使用して、ネットワーク上のアプリケーションおよび関連するホストの詳細情報を取得できます。これにより、ホスト アプリケーションのアクティビティについて詳しく調べることができます。このワークフローは、アプリケーションを実行する個々のホストの IP アドレスのリストで始まり、アプリケーションのテーブル ビュー、およびホスト ビューと続きます。
アプリケーション	このワークフローを使用して、ネットワーク上で実行中のアプリケーションを分析できます。これにより、ネットワークがどのように使用されているか、概要を理解することができます。このワークフローは、個々のアプリケーションを実行しているホストのカウントで始まり、アプリケーションのテーブル ビュー、およびホスト ビューと続きます。詳細については、「アプリケーションの表示（50-45 ページ）」を参照してください。

事前定義のアプリケーション詳細ワークフロー

ライセンス：FireSIGHT

次の表で、アプリケーションの詳細およびクライアント データで使用できる事前定義のワークフローについて説明します。

表 58-10　事前定義のアプリケーション詳細ワークフロー

ワークフロー名	説明
Application Details（アプリケーションの詳細）	このワークフローを使用して、ネットワーク上のクライアント アプリケーションを詳しく分析することができます。このワークフローには、ネットワーク上のクライアント アプリケーションとアプリケーション製品のリスト、および各アプリケーションを実行しているホスト数のカウントを示す一連のページが含まれています。対象のアプリケーションの各バージョンを実行しているホストの数を表示できます。次のページでは、特定のホストに対して最も頻繁にアクセスしたアプリケーションを特定することができます。次にワークフローはクライアント アプリケーションのテーブル ビューを提供し、続いてホスト ビューを提供します。詳細については、「アプリケーションの詳細の表示（50-50 ページ）」を参照してください。
クライアント	このワークフローには、クライアント アプリケーションのテーブル ビューが含まれており、その後にホスト ビューが続きます。詳細については、「アプリケーションの詳細の表示（50-50 ページ）」を参照してください。

事前定義のサーバ ワークフロー

ライセンス：FireSIGHT

次の表で、サーバ データで使用できる事前定義のワークフローについて説明します。

表 58-11　事前定義のサーバ ワークフロー

ワークフロー名	説明
Network Applications by Count（カウントに基づいたネットワーク アプリケーション）	このワークフローを使用して、ネットワークで最も頻繁に使用されるアプリケーションを分析することができます。このワークフローには、アプリケーション、および各アプリケーションが存在するホストのカウントを示す一連のページが含まれています。さらに、各アプリケーションのベンダーとバージョンも示されます。ワークフローは、ホストごとのアプリケーションを示すテーブル ビュー、およびその後に続くホスト ビューで終了します。詳細については、「サーバの表示（50-40 ページ）」を参照してください。
Network Applications by Hit（ヒットに基づいたネットワーク アプリケーション）	このワークフローを使用して、ネットワークで最もアクティブなアプリケーションを分析することができます。このワークフローには、アプリケーション、および各アプリケーションがアクセスされた頻度のカウントを示す一連のページが含まれています。さらに、各アプリケーションのベンダーとバージョンの情報も示されます。ワークフローは、ホストごとのアプリケーションを示すテーブル ビュー、およびその後に続くホスト ビューが含まれているページで終了します。詳細については、「サーバの表示（50-40 ページ）」を参照してください。

表 58-11　事前定義のサーバ ワークフロー（続き）

ワークフロー名	説明
Server Details（サーバの詳細）	このワークフローを使用して、検出されたサーバ アプリケーション プロトコルのベンダーおよびバージョンを詳しく分析することができます。ワークフローには、ベンダーに関連付けられているサーバのリストが含まれています。その後に、ベンダーとバージョンの両方に関連するサーバのリストが続き、サーバのテーブル ビューとホスト ビューで終了します。
サーバ	このワークフローには、アプリケーションのテーブル ビューが含まれており、その後にホスト ビューが続きます。詳細については、「サーバの表示（50-40 ページ）」を参照してください。

事前定義のホスト属性ワークフロー

ライセンス：FireSIGHT

次の表で、ホスト属性のデータで使用できる事前定義のワークフローについて説明します。

表 58-12　事前定義のホスト属性ワークフロー

ワークフロー名	説明
Attributes	このワークフローを使用して、ネットワーク上のホストの IP アドレスおよびホストのステータスを監視することができます。このワークフローは、個々の IP アドレス、および現行のユーザ、ホストの重要度、注記、およびホワイトリストのコンプライアンスを示したホスト属性のテーブル ビューで始まります。そして、ホスト ビューで終了します。詳細については、ホスト属性の表示（50-30 ページ）を参照してください。

事前定義のディスカバリ イベント ワークフロー

ライセンス：FireSIGHT

次の表で、ディスカバリ イベントのデータで使用できる事前定義のワークフローについて説明します。

表 58-13　事前定義のディスカバリ イベント ワークフロー

ワークフロー名	説明
Discovery Events（ディスカバリ イベント）	このワークフローは、ディスカバリ イベントについてテーブル ビューの形式で詳細なリストを提供し、その後にホスト ビューが続きます。詳細については、ディスカバリ イベント テーブルについて（50-17 ページ）を参照してください。

事前定義のユーザ ワークフロー

ライセンス：FireSIGHT

次の表で、Defense Centerに含まれている事前定義のユーザ ワークフローについて説明します。

表 58-14　事前定義のユーザ ワークフロー

ワークフロー名	説明
ユーザ	このワークフローは、ユーザ イベントまたは LDAP サーバの接続から収集したユーザ情報のリストを提供します。ユーザ アイデンティティ ワークフローの詳細については、ユーザの表示（50-65 ページ）を参照してください。

事前定義の脆弱性ワークフロー

ライセンス：FireSIGHT

次の表で、Defense Centerに含まれている事前定義の脆弱性ワークフローについて説明します。

表 58-15　事前定義の脆弱性ワークフロー

ワークフロー名	説明
Vulnerabilities	このワークフローを使用して、データベース内のすべての脆弱性を示す脆弱性のテーブル ビューを確認することができます。その後に、ネットワーク上で検出されたホストに適合するアクティブな脆弱性のみのテーブル ビューが続きます。ワークフローは、脆弱性の詳細ビューで終了します。この詳細ビューには、ユーザの制約に一致するすべての脆弱性について詳しい説明が含まれています。詳細については、脆弱性の表示（50-54 ページ）を参照してください。

事前定義のサードパーティの脆弱性ワークフロー

ライセンス：FireSIGHT

次の表で、Defense Centerに含まれている事前定義のサードパーティの脆弱性ワークフローについて説明します。

表 58-16　事前定義のサードパーティの脆弱性ワークフロー

ワークフロー名	説明
Vulnerabilities by IP Address（IP アドレスごとの脆弱性）	このワークフローを使用して、サードパーティの脆弱性が何個検出されたかを、モニタリング対象のネットワーク上のホスト IP アドレスごとにすぐに確認することができます。このワークフローは、サードパーティの脆弱性のテーブル ビュー、およびその後に続くホスト ビューで終了します。詳細については、サードパーティの脆弱性の表示（50-60 ページ）を参照してください。
Vulnerabilities by Source（ソースごとの脆弱性）	このワークフローを使用して、サードパーティの脆弱性が何個検出されたかを、サードパーティの脆弱性ソース（QualysGuard Scanner など）ごとにすぐに確認することができます。このワークフローは、中間のドリルダウン ページ上にこれらの脆弱性に関する詳細な情報を提供し、サードパーティの脆弱性のテーブル ビュー、およびその後に続くホスト ビューで終了します。詳細については、サードパーティの脆弱性の表示（50-60 ページ）を参照してください。

事前定義の相関およびホワイトリスト ワークフロー

ライセンス：FireSIGHT

相関データ、ホワイトリスト イベント、ホワイトリスト違反、および修正ステータス イベントの各タイプについて、1 つの事前定義ワークフローが用意されています。

表 58-17　事前定義の相関ワークフロー

ワークフロー名	説明
Correlation Events（相関イベント）	このワークフローには、相関イベントのテーブル ビューが含まれています。詳細については、「相関イベントの操作（51-56 ページ）」を参照してください。
White List Events（ホワイトリスト イベント）	このワークフローには、ホワイトリスト イベントのテーブル ビューが含まれています。詳細については、「ホワイト リスト イベントの操作（52-33 ページ）」を参照してください。
Host Violation Count（ホストの違反カウント）	このワークフローは、1 つ以上のホワイトリストに違反しているすべてのホスト IP アドレスを示す一連のページを提供します。最初のページはアドレスごとの違反の数に基づいてアドレスをソートし、違反数が最も多い IP アドレスがリストの最上部に示されます。あるホスト IP アドレスが複数のホワイトリストに違反している場合、違反したそれぞれのホワイトリストに対して別の行が示されます。ワークフローには、すべての違反を示すホワイトリスト違反のテーブル ビューも含まれ、最後に検出された違反がリストの最上部に示されます。テーブルの各行には、検出された 1 つの違反が含まれます。詳細については、「ホワイト リスト違反の処理（52-38 ページ）」を参照してください。
White List Violations（ホワイトリスト違反）	ワークフローには、すべての違反を示すホワイトリスト違反のテーブル ビューも含まれ、最後に検出された違反がリストの最上部に示されます。テーブルの各行には、検出された 1 つの違反が含まれます。詳細については、「ホワイト リスト違反の処理（52-38 ページ）」を参照してください。
Status（ステータス）	このワークフローには、修正ステータスのテーブル ビューが含まれています。このテーブル ビューには、違反したポリシーの名前、適用された修正の名前とステータスが含まれています。詳細については、「修復ステータス イベントの使用（54-18 ページ）」を参照してください。

事前定義のシステム ワークフロー

ライセンス：すべて

FireSIGHT システムには、ルール更新のインポートやアクティブ スキャンの結果を表示するワークフロー、およびシステム イベント（監査イベントやヘルス イベント）などのいくつかの追加ワークフローが用意されています。

表 58-18　その他の事前定義ワークフロー

ワークフロー名	説明
監査ログ	このワークフローには、監査イベントを示す監査ログのテーブル ビューが含まれています。詳細については、「監査レコードの表示（69-2 ページ）」を参照してください。
Health Events（ヘルス イベント）	このワークフローは、ヘルス モニタリング ポリシーによってトリガーされたイベントを表示します。詳細については、「ヘルス イベント テーブル ビューの操作（68-55 ページ）」を参照してください。

表 58-18　その他の事前定義ワークフロー（続き）

ワークフロー名	説明
Rule Update Import Log（ルール更新のインポート ログ）	このワークフローには、正常終了および失敗したルール更新のインポート両方の情報を示すテーブル ビューが含まれています。詳細については、ルールの更新とローカル ルール ファイルのインポート（66-16 ページ）を参照してください。
Scan Results（スキャン結果）	このワークフローには、完了したそれぞれのスキャンを示すテーブル ビューが含まれています。詳細については、アクティブ スキャンの結果での作業（47-21 ページ）を参照してください。

保存済みのカスタム ワークフロー

ライセンス：Protection + FireSIGHT

修正できない事前定義のワークフローだけでなく、Defense Centerには、保存済みのカスタム ワークフローがいくつか含まれています。これらのワークフローはそれぞれ 1 つのカスタム テーブルに基づいており、修正することができます。これらのワークフローへのアクセスについては、カスタム テーブルに基づいたワークフローの表示（59-8 ページ）を参照してください。

表 58-19　保存済みのカスタム ワークフロー

ワークフロー名	説明
Events by Impact, Priority, and Host Criticality（影響、優先度、およびホストの重大度に基づいたイベント）	このワークフローを使用して、ネットワークにとって重要で、現在は脆弱な状態にあり、攻撃を受ける可能性があるようなホストをすばやく見つけて表示することができます。 デフォルトでは、このワークフローは、影響レベルでソートされ、次にホストの重要度、さらにイベントの発生数でソートされたイベントの概要で始まります。ワークフローの 2 ページ目を使用して、特定のイベントが発生した送信元および宛先のアドレスに対してドリルダウンし、表示することができます。ワークフローは、[Intrusion Events with Destination Criticality] のテーブル ビュー、およびパケット ビューで終了します。このワークフローは、[Intrusion Events with Destination Criticality] カスタム テーブルに基づいています。詳細については、カスタム テーブルについて（59-1 ページ）を参照してください。
Events by Priority and Classification（優先度および分類に基づいたイベント）	このワークフローは、イベントおよびイベントのタイプを、イベントの優先度の順に表示し、各イベントが発生した回数も示します。 このワークフローは、優先度のレベル、分類、および表示されている各イベントのカウントが含まれているドリルダウン ページから始まります。ワークフローの最終ページは、イベントのテーブル ビューとパケット ビューです。このワークフローは、[Intrusion Events] カスタム テーブルに基づいています。詳細については、カスタム テーブルについて（59-1 ページ）を参照してください。
Events with Destination, Impact, and Host Criticality（宛先、影響、およびホストの重大度に基づいたイベント）	このワークフローを使用して、ネットワークにとって重要で、現在脆弱な状態にあるホスト上の最近の攻撃を見つけることができます。 デフォルトでは、このワークフローは、影響レベルでソートされた最近のイベントのリストで始まります。ワークフローの次のページは、[Intrusion Events with Destination Criticality] のテーブル ビューを提供し、その後にパケット ビューが続きます。このワークフローは、[Intrusion Events with Destination Criticality] カスタム テーブルに基づいています。詳細については、カスタム テーブルについて（59-1 ページ）を参照してください。

表 58-19　保存済みのカスタム ワークフロー（続き）

ワークフロー名	説明
Hosts with Servers Default Workflow（サーバに接続しているホストのデフォルト ワークフロー）	このワークフローを使用して、[Hosts with Servers] カスタム テーブルの基本情報をすばやく表示することができます。 デフォルトでは、このワークフローはサーバに接続しているホストのテーブル ビューで始まり、その後にホスト ビューが続きます。このワークフローは、[Hosts with Servers] カスタム テーブルに基づいています。詳細については、カスタム テーブルについて（59-1 ページ）を参照してください。
Intrusion Events with Destination Criticality Default Workflow（宛先の重大度に基づく侵入イベントのデフォルト ワークフロー）	このワークフローを使用して、Intrusion Events with Destination Criticality カスタム テーブルの基本情報をすばやく表示することができます。 デフォルトでは、このワークフローは Intrusion Events with Destination Criticality のテーブル ビューで始まり、その後にパケット ビューが続きます。このワークフローは、[Intrusion Events with Destination Criticality] カスタム テーブルに基づいています。詳細については、カスタム テーブルについて（59-1 ページ）を参照してください。
Intrusion Events with Source Criticality Default Workflow（送信元の重大度に基づく侵入イベントのデフォルト ワークフロー）	このワークフローを使用して、[Intrusion Events with Source Criticality] カスタム テーブルの基本情報をすばやく表示することができます。 デフォルトでは、このワークフローは [Intrusion Events with Source Criticality] のテーブル ビューで始まり、その後にパケット ビューが続きます。このワークフローは、[Intrusion Events with Source Criticality] カスタム テーブルに基づいています。詳細については、カスタム テーブルについて（59-1 ページ）を参照してください。
Server and Host Details（サーバとホストの詳細）	このワークフローを使用して、ネットワーク上で最も頻繁に使用されているサーバ、およびそれらのサーバを実行しているホストを決定できます。 デフォルトでは、このワークフローは、各サービスにアクセスする頻度が示されたサーバの概要で始まります。次のページには、オペレーティング システムのベンダーとバージョンごとにサーバが示されます。このワークフローは、サーバを実行しているホストのテーブル ビュー、およびその後に続くホスト ビューで終了します。このワークフローは、[Hosts with Servers] カスタム テーブルに基づいています。詳細については、カスタム テーブルについて（59-1 ページ）を参照してください。

ワークフローの使用

ライセンス： すべて

ワークフローのドリル ダウンおよびテーブル ビューのページを使用して、データのビューをすばやく絞り込むことができます。これにより、分析にとって重要なイベントに集中することが可能です。ワークフローのタイプによってデータは異なりますが、すべてのワークフローが共通の機能セットを共有しています。以降の項では、これらの機能について、およびこれらの機能の使用方法について説明します。

- ワークフローの選択（58-18 ページ）では、ワークフローの選択ページについて、および使用するワークフローを選択する方法について説明します。
- ワークフローのツールバーについて（58-20 ページ）では、ワークフローで使用できるツールバー オプションについて説明します。
- ワークフローのページの使用（58-21 ページ）では、すべてのワークフロー ページに表示される機能について、およびそれらの機能の使用方法について説明します。

- イベント時間の制約の設定（58-26 ページ）では、イベントベースのワークフローに対して時間範囲を設定する方法について説明します。ワークフローには、指定された時間範囲に生成されたイベントが含まれます。
- イベントの制約（58-35 ページ）では、ワークフローでデータのビューを制約して（絞り込んで）、次のワークフロー ページに進むために使用する機能について説明します。
- 複合的な制約の使用（58-37 ページ）では、複合的な制約の使用方法を説明し、その例を示します。
- ドリルダウン ワークフロー ページのソート（58-38 ページ）では、ワークフローで表示されるデータをソートする機能について、および表示するテーブル カラムを削除および復元する機能について説明します。
- ワークフロー ページの行の選択（58-39 ページ）では、表示されるテーブル内で、分析の対象とする、または他のアクションを実行するデータ行を選択する方法について説明します。
- ワークフロー内の他のページへのナビゲート（58-39 ページ）では、選択されたすべてのイベントを含め、制約を使用して現行のワークフローから他のワークフローをオープンする方法について説明します。
- ワークフロー間のナビゲート（58-40 ページ）では、[Jump to] ドロップダウン リストについて、およびこのリストを使用して現行の制約を他のワークフローに適用する方法について説明します。
- イベントの検索（60-1 ページ）では、イベント データの検索に使用する機能について説明します。
- ブックマークの使用（58-41 ページ）では、ブックマークの作成、管理、および使用方法について説明します。

ワークフローの選択

ライセンス： すべて

FireSIGHT システムは、次の表に記載されているデータのタイプに対して、事前定義のワークフローを提供しています。

表 58-20　　ワークフローを使用する機能

機能	Menu Path	オプション
侵入イベント	[Analysis] > [Intrusions]	Event Reviewed Events Clipboard インシデント
マルウェア イベント	[Analysis] > [Files]	Malware Events
ファイル イベント	[Analysis] > [Files]	File Events
キャプチャ ファイル	[Analysis] > [Files]	Captured Files
接続イベント	[Analysis] > [Connections]	Event
セキュリティ インテリジェンス イベント	[Analysis] > [Connections]	Security Intelligence Events

表 58-20　ワークフローを使用する機能（続き）

機能	Menu Path	オプション
ホスト イベント	[Analysis] > [Hosts]	Network Map ホスト Indications of Compromise（侵害の痕跡） アプリケーション Application Details サーバ Host Attributes Discovery Events
ユーザ イベント	[Analysis] > [Users]	User Activity ユーザ
脆弱性イベント	[Analysis] > [Vulnerabilities]	Vulnerabilities Third-Party Vulnerabilities
相関イベント	[Analysis] > [Correlation]	Correlation Events White List Events White List Violations Status（ステータス）
監査イベント	[System] > [Monitoring]	Audit
ヘルス イベント	[Health] > [Health Events]	n/a
ルール更新のインポート ログ	[System] > [Updates]	n/a
スキャン結果	[Policies] > [Actions] > [Scanners]	n/a

上記の表に記載されているいずれかの種類のデータを表示する場合、そのデータのデフォルトのワークフローの最初のページにイベントが表示されます。

また、ワークフローのアクセスは、以下のとおりに、自身のユーザ ロールによって異なります（ユーザ ロールの設定（61-52 ページ）を参照してください）。

- Administrator ユーザはすべてのワークフローにアクセスできます。また、Administrator は監査ログ、スキャン結果、およびルール更新のインポート ログにアクセスできる唯一のユーザです。
- Maintenance ユーザは、ヘルス イベントにアクセスできます。
- Security Analyst および Security Analyst（読み取り専用）ユーザは、侵入、マルウェア、ファイル、接続、ディスカバリ、脆弱性、相関、およびヘルスのワークフローにアクセスできます。

デフォルト以外のワークフローを使用してデータを表示する方法：

アクセス：Admin/Any Security Analyst

ステップ 1　ワークフローを使用する機能の表に記載されているように、適切なメニュー パスとオプションを選択します。

対象のデータ タイプに対するデフォルト ワークフローの最初のページが表示されます。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

ステップ 2　必要に応じて、別のワークフローを使用します。ワークフローのタイトルの隣にある [(switch workflow)] をクリックして、使用するワークフローを選択します。

ステップ 3　選択したワークフローの最初のページが表示されます。

ワークフローのツールバーについて

ライセンス：すべて

ワークフローの各ページには、関連する機能へすばやくアクセスするためのツールバーが含まれています。次の表に、ツールバー上の各リンクについて説明します。

表 58-21　ワークフローのツールバー リンク

機能	説明
Bookmark This Page	後でそのページに戻れるように、現在のページをブックマークします。ブックマークすると、表示中のページに適用されている制約が取得され、（データがまだ存在していれば）後で同じデータに戻ることができます。ブックマークの作成については、ブックマークの使用（58-41 ページ）を参照してください。
Report Designer	現在制約されているワークフローを選択基準として使用して、Report Designer を開きます。レポートの作成については、イベント ビューからのレポート テンプレートの作成（57-10 ページ）を参照してください。
ダッシュボード	現行のワークフローに関連するダッシュボードを開きます。たとえば、[Connection Events（接続イベント）] ワークフローは [Connection Summary] ダッシュボードと関連付けられています。ダッシュボードの使用については、ダッシュボードの使用（55-1 ページ）を参照してください。
View Bookmarks	ユーザが選択できる、保存したブックマークのリストを表示します。ブックマークの作成および管理については、ブックマークの使用（58-41 ページ）を参照してください。
検索	[Search] ページが表示され、ここでワークフローのデータについて高度な検索を実行することができます。下向きの矢印アイコンをクリックし、保存済みの検索を選択して使用することもできます。ワークフローの検索については、イベントの検索（60-1 ページ）を参照してください。

ワークフローのページの使用

ライセンス：すべて

ユーザがワークフローのページ上で実行できるアクションは、ページのタイプによって異なります。テーブル ビュー ページおよびドリルダウン ページには、ユーザが表示するイベント セットの制約、またはワークフローへのナビゲートに使用できる多数の機能が含まれています。各タイプのページで使用できる機能の詳細については、以降の項を参照してください。

- 共通のテーブル ビューまたはドリルダウン ページ機能の使用（58-21 ページ）
- 地理情報の使用（58-23 ページ）
- テーブル ビュー ページの使用（58-25 ページ）
- ドリルダウン ページの使用（58-25 ページ）
- ホスト ビュー、パケット ビュー、または脆弱性の詳細ページの使用（58-26 ページ）

共通のテーブル ビューまたはドリルダウン ページ機能の使用

ライセンス：すべて

テーブル ビューおよびドリルダウン ワークフローのページでは、テーブル見出しおよびテーブル行に一連のアイコンおよび他の機能が用意されています。これを使用して、表示されたデータについてアクションを実行できます。

次の表で機能について説明します。

表 58-22　テーブル ビューおよびドリルダウン ページの機能

機能	説明
	青色の下向き矢印のアイコンをクリックして、ワークフローの次ページの該当する行を表示します。
 （正常）  （マルウェア）  （カスタム検出）  （不明）  （利用不可）	ファイル名および SHA-256 ハッシュ値のカラムに表示されるネットワーク ファイルのトラジェクトリ アイコンをクリックして、ファイルのトラジェクトリ マップを新しいウィンドウに表示します。詳細については、ネットワーク ファイル トラジェクトリの分析（40-40 ページ）を参照してください。 DC500 Defense Center、シリーズ 2 デバイス、およびCisco NGIPS for Blue Coat X-Series は高度なマルウェア防御をサポートしていないため、これらのアプライアンスでは、ネットワークベースのマルウェアおよびファイル イベントに対するネットワーク ファイルのトラジェクトリは表示できないことに注意してください。

表 58-22　テーブル ビューおよびドリルダウン ページの機能（続き）

機能	説明
  （侵害の可能性がある）  （ブラックリスト登録済み）  （ブラックリスト登録済み、監視対象に設定）	[IP address] カラムに表示されるホスト プロファイル アイコンをクリックして、IP アドレスに関連付けられているホスト プロファイルをポップアップ ウィンドウに表示します。詳細については、ホスト プロファイルの使用（49-1 ページ）を参照してください。 侵害の痕跡（IOC）ルールによってトリガーされた侵害の可能性が存在するとタグ付けされたホストには、通常のアイコンではなく、侵害されたホストのアイコンが表示されます。IOC の詳細については、侵害の兆候について（45-22 ページ）を参照してください。 ホスト プロファイルのアイコンがグレー表示になっている場合は、ネットワーク マップ内にそのホストが存在することができないため、ホスト プロファイルを表示できません（0.0.0.0 など）。 セキュリティ インテリジェンス データに基づいてトラフィックのフィルタリングを実行する場合は、接続イベントで、ブラックリストに記載されている監視対象の IP アドレスの隣にあるホスト アイコンが少し異なります。これは、接続においてどのホストがブラックリストに記載されているかを識別するのに役に立ちます。DC500 Defense Center およびシリーズ 2 のデバイスはセキュリティ インテリジェンスのデータをサポートしていないことに注意してください。
 （低脅威スコア）  （中脅威スコア）  （高脅威スコア）  （非常に高い脅威スコア）	脅威スコアのカラムに表示される脅威スコアのアイコンをクリックし、Dynamic Analysis Summary レポートで、ファイルに関連付けられている最高の脅威スコアを表示します。 DC500 Defense Center、シリーズ 2 デバイス、および Cisco NGIPS for Blue Coat X-Series は高度なマルウェア防御をサポートしているため、これらのアプライアンスでは Dynamic Analysis Summary レポートを表示することはできません。
	ユーザ アイデンティティのカラムに表示されるユーザ アイコンをクリックして、ユーザのプロファイル情報を表示します。詳細については、ユーザの詳細とホストの履歴について（50-68 ページ）を参照してください。 ユーザ アイコンがグレー表示になっている場合は、そのユーザがデータベース内に存在することができないため、ユーザ プロファイルは表示できません（FireAMP コネクタ ユーザなどの場合）。
	サードパーティの脆弱性 ID のカラムに表示される脆弱性アイコンをクリックし、サードパーティの脆弱性について詳細を表示します。詳細については、脆弱性の詳細の表示（49-30 ページ）を参照してください。
チェック ボックス	ページ上で複数の行のチェック ボックスを選択して、処理を反映させる行を表示し、ページの下部にあるいずれかのボタン（[View] ボタンなど）をクリックします。行の先頭にあるチェック ボックスを選択して、ページ上のすべての行を選択することもできます。
国旗およびコード	接続イベント、侵入イベント、ファイル イベント、マルウェア イベントなどのワークフローのページの中には、ルート可能な IP アドレスに、関連する国の情報が含まれているものがあります。このような*地理情報*が使用可能な場合は、その国の国旗および ISO コードが該当するカラム（[Source Country] など）に表示されます。国名を表示するには、ポインタを国旗の上に移動します。（集約されたデータではなく）個別のデータ ポイントを表示する場合は、国旗のアイコンをクリックして、詳細な地理情報を表示することができます。詳細については、「地理情報の使用（58-23 ページ）」を参照してください。 DC500 Defense Centerは地理情報データをサポートしていないことに注意してください。

表 58-22　テーブル ビューおよびドリルダウン ページの機能（続き）

機能	説明
検索の制約	データ ビューを制約する値が存在する場合に、その値を表示します。展開の矢印（▲）をクリックすると、アクティブな制約および無効なカラムのリストが表示され、縮小の矢印（▶）をクリックすると、ビューからリストが非表示になります。デフォルトでは、このリストは縮小されています。これは制約のリストが長く、画面には収まらない場合に便利です。 1 つの制約を解除するには、その制約をクリックします。複合的な制約を解除するには、[Compound Constraints] をクリックします。 現行の 1 つの制約により値が事前に挿入された検索ページを開くには、[Edit Search] または [Save Search] をクリックします。詳細については、「イベントの制約（58-35 ページ）」を参照してください。 **注**　複合的な制約では、複数の不可算値を持つ行に基づいて制約が作成されます。複合的な制約について、検索および検索の保存を実行することはできません。
時間範囲	ページの右上隅に表示される日付範囲は、ワークフローに含めるイベントの時間範囲を設定します。詳細については、「イベント時間の制約の設定（58-26 ページ）」を参照してください。 イベント ビューを時間によって制約している場合は、（グローバルかイベントに特有かに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあることに注意してください。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。
ワークフロー ページのリンク	ワークフロー ページのリンクは、事前定義されたワークフロー テーブル ビュー、およびドリルダウン ページの左上隅の、イベントの上で、ワークフロー名の下に示されます。ワークフロー ページのリンクをクリックして、アクティブな制約を使用しているページを表示します。
ワークフロー名	ページの上部にワークフロー名が表示されます。該当する場合は、ワークフロー名の隣に（[switch workflows]）リンクがあります。これを使用して、同じタイプの他のワークフローを選択することができます。

地理情報の使用

ライセンス： FireSIGHT

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： すべて（DC500 を除く）

ネットワークの監視中、*地理情報*機能によって、ルート可能な IP アドレスの地理的な送信元について、追加のデータ（国や大陸など）が提供されます。たとえば、このデータを使用して、自身の組織と未接続の国が接続の発信元または宛先であるかどうかを判断することができます。

地理情報は、侵入イベント、接続イベント、ファイル イベント、マルウェア イベント、ホスト プロファイル、およびユーザ プロファイルで使用することができます。地理情報は、Context Explorer およびダッシュボードでも使用できます。

この目的でカスタムな地理情報オブジェクトを作成するだけでなく、アクセス コントロール ルールの条件として地理情報データ（送信元および宛先の国/大陸）を使用することもできます。また、相関ルールおよびトラフィック プロファイルの条件として、送信元/宛先の国データを使用することもできます。詳細については、位置情報オブジェクトの操作（3-56 ページ）、ネットワークまたは地理的位置によるトラフィックの制御（15-4 ページ）、相関ポリシーのルールの作成（51-3 ページ）、およびトラフィック プロファイル条件の指定（53-3 ページ）を参照してください。

地理情報データベース(GeoDB)の更新をインストールすると [Geolocation Details] ページが表示され、IP アドレスに関して使用可能な詳細情報(郵便番号、緯度/経度の座標、タイム ゾーン、自律システム番号(ASN)、インターネット サービス プロバイダ(ISP)、使用タイプ(個人または会社)、組織、ドメイン名、接続タイプ、プロキシ情報など)が示されます。また、サードパーティの 4 つのマップ ツールのいずれかを使用して、検出された場所を特定することもできます。GeoDB が更新されていない場合は、国旗アイコンおよび国名のみが表示され、[Geolocation Details] ページを参照することはできません。GeoDB のインストールと更新については、地理情報データベースについて(66-30 ページ)を参照してください。[Help] > [About] をクリックして GeoDB 更新の最新バージョンを表示することができます。

使用可能なデータに応じて、[Geolocation Details] ページに多数のフィールドが表示されることがあります。情報が含まれないフィールドは表示されません。次の表で、これらのフィールドの情報について示します。

表 58-23　地理情報の詳細フィールド

フィールド	目次
Country	ホスト IP アドレスに関連付けられている国が国旗とともに示されます。大陸はカッコ内に表示されます。例:`United States (North America)`、`Equatorial Guinea (Africa)`
領域	ホストが存在する国の州、県、またはその他の小区域。例:`VA`、`35`
市町村	ホストが存在する市。例:`Seattle`、`Fukuoka`
Postal Code	ホストが存在する地域の郵便番号。例:`361000`、`90210`
Latitude/Longitude	ホストの場所の正確な座標。例:`40.0375, -76.1053`、`53.4050, -0.5484`
マップ	外部のマッピング サイト(Google Maps、Yahoo Maps、Bing Maps、OpenStreetMap など)へのリンク。ホストのおよその位置のコンテキスト マップを表示するには、リンクをクリックします。
Timezone	ホストの場所のタイム ゾーン(該当する場合には夏時間が示されます)。例:`GMT+8:00`、`GMT-4:00 (In DST)`
ASN	ホスト IP アドレスに関連付けられている自律システム番号(ASN)、およびその ASN に関する追加情報。例:`14618 (Amazon.com Inc.)`、`4837 (Cncgroup China169 Backbone)`
ISP	ホストの IP アドレスに関連付けられているインターネット サービス プロバイダ(ISP)。例:`Atlantic Broadband`、`China Unicom Ip Network`
Home/Business	ホストの接続が**個人**または**会社**のどちらの目的であるかを示します。
マニュアルの構成	ホストの IP アドレスに関連付けられている組織。例:`Amazon.com`、`Bank of America`
Domain Name	ホストの IP アドレスに関連付けられているドメイン名。例:`amazonaws.com`、`xmcnc.net`
Connection Type	ホストの IP アドレスに関連付けられている接続タイプ。例:`Broadband`、`DSL`
Proxy Type	使用するプロキシのタイプ。例:`Anonymous`、`Corporate`

地理情報の詳細を表示する方法:

アクセス: すべて

ステップ 1　イベント ビュー、ホスト プロファイル、またはその他の地理情報をサポートしているページで、個々のデータ ポイントのそばに表示される小さい国旗のアイコンまたは ISO 国コードをクリックします(国旗のアイコンが存在しても、[Connection Summary] ダッシュボードなどで、集約的な地理情報から詳細を表示することはできません)。

ヒント　イベント ビューで国旗のアイコンの上にポインタを移動すると、ツールチップとして国名が示されます。

[Geolocation Details] ページが新しいウィンドウに表示されます。

テーブル ビュー ページの使用

ライセンス： すべて

デフォルトでカラムが有効になっている場合、テーブル ビューには、データベースの各フィールドに対するカラムが含まれています。テーブル ビューでカラムを無効にし、そのカラムを無効にすることによって同じ行が複数生成される場合には、FireSIGHT システムはイベント ビューに [Count] カラムを追加します。テーブル ビュー ページで 1 つの値をクリックすると、その値によって制約することができます。カスタム ワークフローを作成する場合は、[Add Table View] をクリックしてテーブル ビューを追加します。

テーブル ビュー ページには、ドリルダウン、ホスト ビュー、パケット ビュー、または脆弱性の詳細ページでは利用できない追加機能が用意されています。次の表で、これらの機能の詳細な情報について説明します。

表 58-24　テーブル ビュー ページの追加機能

機能	説明
✖	非表示にするカラムの見出しで、このアイコンをクリックします。表示されるポップアップ ウィンドウで、[Apply] をクリックします。 **ヒント**　他のカラムを表示または非表示にするには、[Apply] をクリックする前に、該当するチェック ボックスをオンまたはオフにします。
[Disabled Columns] リスト	ページからカラムを削除した場合、またはデフォルトでカラムを無効になっている場合、[Disabled Columns] リストにカラム名が表示されます。このリストは、テーブルの上にありますが、デフォルトでは非表示になっています。 無効になったカラムをイベント ビューに戻すには、[Search Constraints] の展開アイコン（▲ ）をクリックして検索の制約を展開し、[Disabled Columns] の下にあるカラム名をクリックします。 詳細については、「ドリルダウン ワークフロー ページのソート (58-38 ページ)」を参照してください。

ドリルダウン ページの使用

ライセンス： すべて

ドリルダウン ページには、データベースで使用できるカラムのサブセットが含まれています。事前定義のワークフローに対するドリルダウン ページには、必ず [Count] カラムがあることに注意してください。ドリルダウン ページでは、表示するイベントの範囲を絞り込んで、ワークフローの先へ進むことができます。ドリルダウン ページで 1 つの値をクリックすると（たとえば、その値によって制約を行い、ワークフローの次のページへ進むと）、選択した値に一致するイベントに絞り込むことができます。ドリルダウン ページで値をクリックした場合は、次のページがテーブル ビューであっても、値が存在するカラムは無効になりません。カスタム ワークフローを作成する場合は、[Add Page] をクリックして、ドリルダウン ページを追加します。

ドリルダウン ページの機能を使用して、ワークフローを移動するときにイベント セットを制約する方法の詳細については、共通のテーブル ビューまたはドリルダウン ページ機能の使用（58-21 ページ）を参照してください。

ホスト ビュー、パケット ビュー、または脆弱性の詳細ページの使用

ライセンス： すべて

検出イベント、ホスト、ホスト属性、侵害の痕跡、サーバ、クライアント アプリケーション、または接続データのワークフローの最終ページはホスト ビューです。脆弱性のワークフローの最終ページは、脆弱性の詳細ページです。侵入イベントのワークフローは必ず、パケット ビューで終了します。ワークフローの最終ページで詳細セクションを展開して、ワークフローの進行中に絞り込んだセットの各オブジェクトについて、具体的な情報を表示することができます。Web インターフェイスは、ワークフローの最終ページに制約を表示しませんが、以前に設定した制約は保持されており、データのセットに適用されます。

イベント時間の制約の設定

ライセンス： すべて

各イベントには、そのイベントがいつ発生したかを示すタイム スタンプがあります。時間枠（時間範囲とも呼ばれる）を設定することによって、いくつかのワークフローに表示される情報を制約することができます。

時間によって制約できるイベントに基づいたワークフローには、ページの上部に次の図に示すような時間範囲を表す行が含まれています。

デフォルトでは、Cisco アプライアンス上のワークフローは、1 時間前が開始時間として設定された時間枠を使用します。たとえば、午前 11:30 にログインした場合、午前 10:30～11:30 の間に発生したイベントが表示されます。時間が経過するにしたがって、時間枠が拡張されます。午後 12:30 には、午前 10:30～午後 12:30 の間に発生したイベントが表示されます。

デフォルトで独自の時間枠を設定することによって、この動作を変更することができます。これにより、次の 3 つのプロパティが影響を受けます。

- 時間枠のタイプ（静的、拡張、またはスライディング）
- 時間枠の長さ
- 時間枠の数（複数の時間枠、または単一のグローバル時間枠）

デフォルトの時間枠の一般的な情報については、デフォルトの時間枠（71-6 ページ）を参照してください。

ページの上部にある時間範囲をクリックして [Date/Time] ポップアップ ウィンドウを表示し、デフォルトの時間枠の設定に関係なく、イベントの分析中に時間枠を手動で変更することができます。設定した時間枠の数、および使用しているアプライアンスのタイプに応じて [Date/Time] ウィンドウを使用して、表示しているイベントのタイプに対するデフォルトの時間枠を変更することもできます。

最後に、時間枠は一時停止することができるため、時間枠の変更と削除、または必要のないイベントを追加することなく、ワークフローで提供されたデータを調べることができます。ページの下部にあるリンクをクリックしてイベントの他のページを表示する場合は、異なるワークフロー ページで同じイベントを表示しないように、時間枠が自動的に一時停止することに注意してください。準備ができたら時間枠の一時停止を解除できます。

詳細については、次の項を参照してください。

- 時間枠の変更（58-27 ページ）
- イベント タイプのデフォルトの時間枠の変更（58-31 ページ）
- 時間枠の一時停止（58-34 ページ）

時間枠の変更

ライセンス： すべて

デフォルトの時間枠に関係なく、イベントの分析中に時間枠を手動で変更することができます。

注　手動による時間枠の設定は、現行のセッションに対してのみ有効です。いったんログアウトしてからもう一度ログインすると、時間枠はデフォルトにリセットされます。

ユーザが設定した時間枠の数によっては、1 つのワークフローの時間枠の変更が、アプライアンス上の他のワークフローに影響を与えることがあります。たとえば、単一のグローバルな時間枠がある場合、1 つのワークフローの時間枠を変更すると、アプライアンス上の他のすべてのワークフローの時間枠が変更されます。一方、複数の時間枠を使用している場合は、監査ログまたはヘルス イベント ワークフローの時間枠を変更しても、他の時間枠には影響がありませんが、他の種類のイベントで時間枠を変更すると、時間によって制約されるすべてのイベント（監査イベントとヘルス イベントは除く）が影響を受けます。

すべてのワークフローを時間によって制約できるわけではないため、時間枠の設定は、ホスト、ホスト属性、アプリケーション、アプリケーションの詳細、脆弱性、ユーザ、またはホワイトリスト違反に基づいたワークフローには影響を与えないことに注意してください。

[Date/Time] ウィンドウの [Time Window] タブを使用して、時間枠を手動で設定します。デフォルトの時間枠設定で設定した時間枠の数によって、タブのタイトルは以下のいずれかになります。

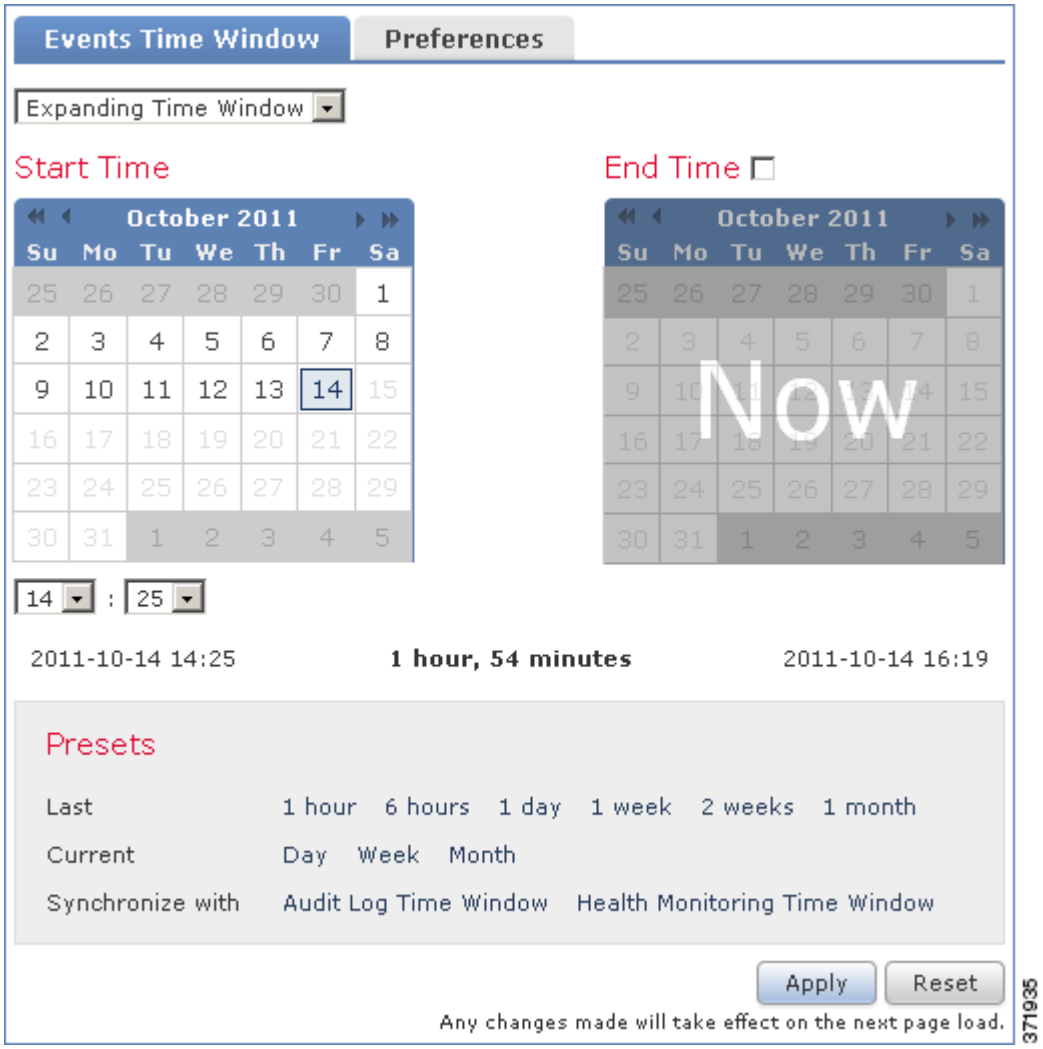
- [Events Time Window]：複数の時間枠を設定し、監査ログまたはヘルス イベント ワークフロー以外のワークフローに対して時間枠を設定している場合
- [Health Monitoring Time Window]：複数の時間枠を設定し、ヘルス イベント ワークフローに対して時間枠を設定している場合
- [Audit Log Time Window]：複数の時間枠を設定し、監査ログに対して時間枠を設定している場合
- [Global Time Window]：単一の時間枠を設定している場合

時間枠を設定する場合には、最初に、使用する時間枠のタイプを決定する必要があります。

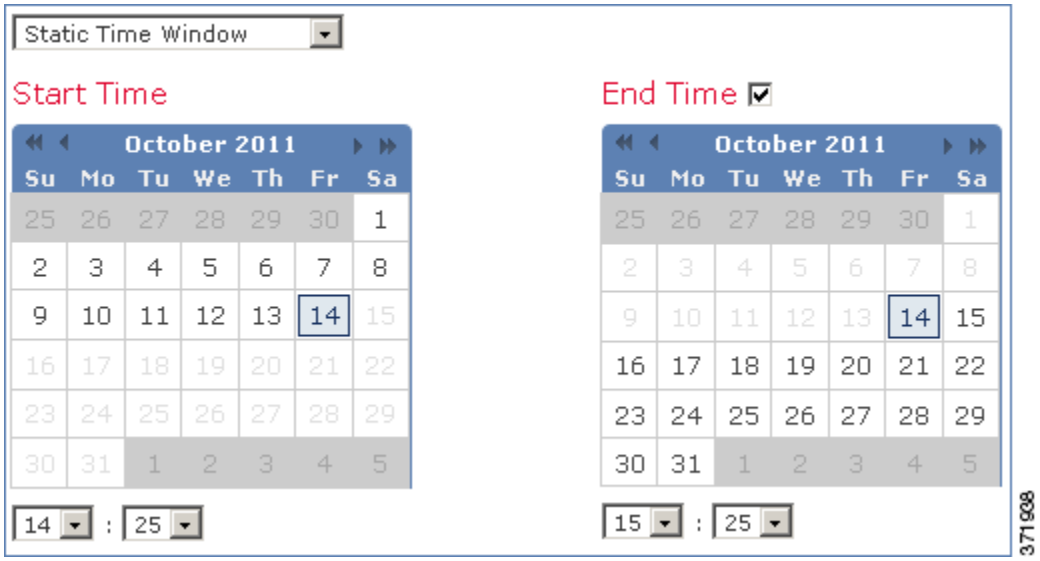
- *静的な*時間枠は、特定の開始時間から特定の終了時間の間に生成されたすべてのイベントを表示します。
- *拡張*時間枠は、特定の開始時間から現在までの間に生成されたすべてのイベントを表示します。時間の経過とともに時間枠が拡張され、イベント ビューに新しいイベントが追加されます。

- *スライディング*時間枠は、特定の開始時間（1 週間前など）から現在までの間に生成されたすべてのイベントを表示します。時間の経過とともに時間枠が「スライド」し、自身が設定した範囲（この例では、過去 1 週間）のイベントのみが表示されます。

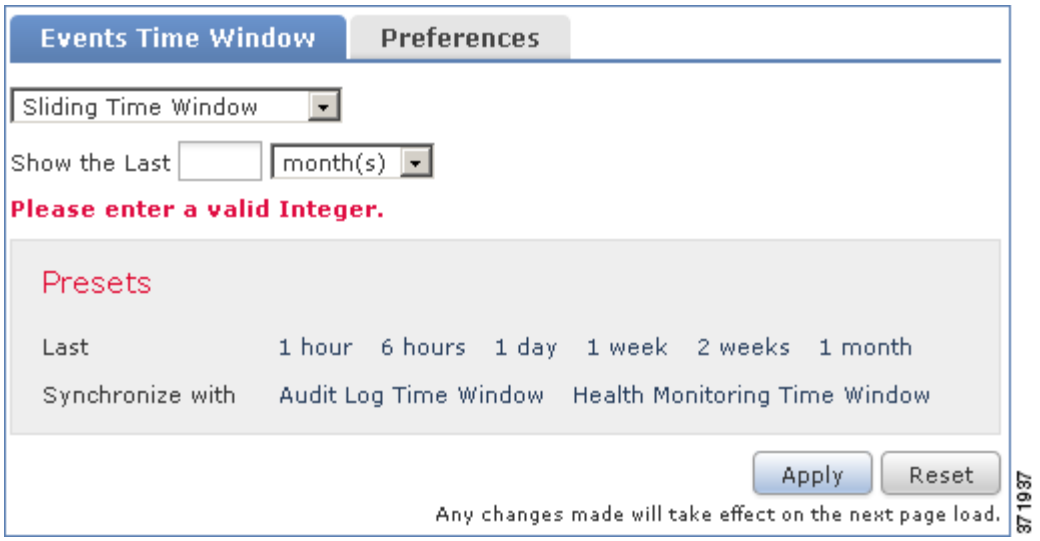
選択するタイプによっては、[Date/Time] ウィンドウが変化し、さまざまな設定オプションを提供します。次の図は、拡張の時間枠を使用するよう指定した [Date/Time] ウィンドウを示しています。拡張の時間枠では、[End Time] カレンダーがグレー表示され、終了時間は「Now」と示されます。



静的な時間枠を使用する場合は、終了時間を設定できます。



スライディング時間枠を使用するよう選択すると、オプションがさらに変わります。



注　FireSIGHT システムは、タイム ゾーンのプリファレンスに指定された時間に基づいて、24 時間の時計を使用します。タイム ゾーンの設定の詳細については、デフォルトのタイム ゾーンの設定 (71-8 ページ) を参照してください。

次の表で、[Time Window] タブで設定できるさまざまな設定について説明します。

表 58-25　時間枠の設定

設定	時間枠のタイプ	説明
時間枠タイプのドロップダウン リスト	n/a	使用する時間枠のタイプを、静的、拡張、またはスライディングのいずれかから選択します。 イベント ビューを時間によって制約している場合は、(グローバルかイベントに特有かに関係なく)アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあることに注意してください。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。
[Start Time] カレンダー	静的および拡張	時間枠の開始日と時間を指定します。すべての時間枠の最大時間範囲は、1970 年 1 月 1 日午前 0 時(UTC)～ 2038 年 1 月 19 日午前 3 時 14 分 7 秒です。 **ヒント**　カレンダーを使用する代わりに、下記で説明するプリセット オプションを使用できます。
[End Time] カレンダー	静的	時間枠の終了日付と時間を指定します。すべての時間枠の最大時間範囲は、1970 年 1 月 1 日午前 0 時(UTC)～ 2038 年 1 月 19 日午前 3 時 14 分 7 秒です。 拡張時間枠を使用している場合は、[End Time] カレンダーがグレー表示になり、終了時間が「Now」と示されることに注意してください。 **ヒント**　カレンダーを使用する代わりに、下記で説明するプリセット オプションを使用できます。
[Show the Last] フィールドおよびドロップダウン リスト	スライディング	スライディング時間枠の長さを設定します。
プリセット:[Last]	all	リスト内のいずれかの時間範囲をクリックし、アプライアンスのローカル時刻に基づいて時間枠を変更します。たとえば、[1 week] をクリックすると、最後の 1 週間を反映するように時間枠が変わります。プリセットをクリックすると、選択したプリセットを反映するようにカレンダーが変わります。

表 58-25　時間枠の設定（続き）

設定	時間枠のタイプ	説明
プリセット：[Current]	静的および拡張	リスト内のいずれかの時間範囲をクリックし、アプライアンスのローカル時間と日付に基づいて時間枠を変更します。プリセットをクリックすると、選択したプリセットを反映するようにカレンダーが変わります。 次の点に注意してください。 • 現在日付は午前 0 時から始まる • 現在の週は日曜日の午前 0 時から始まる • 現在の月は、月の最初の日の午前 0 時から始まる
プリセット：[Synchronize with]	すべて（グローバルな時間枠を使用している場合は使用不可）	以下のいずれかをクリックします • [Events Time Window]：現在の時間枠とイベントの時間枠を同期する場合 • [Health Monitoring Time Window]：現在の時間枠とヘルス モニタリングの時間枠を同期する場合 • [Audit Log Time Window]：現在の時間枠と監査ログの時間枠を同期する場合

イベントの分析中に時間枠を変更する方法：

アクセス： Admin/Maint/Any Security Analyst

ステップ 1　時間に制約されるワークフローで、時間範囲のアイコン（）をクリックします。

[Date/Time] ウィンドウが表示されます。

ステップ 2　[Time Window] タブで、時間枠の設定の表に記載されているように時間枠を設定します。

ヒント　時間枠をデフォルトの設定に戻すには、[Reset] をクリックします。

ステップ 3　[Apply] をクリックします。

ウィンドウが閉じて、イベント ビュー ページに新しい時間枠のイベントが表示されます。

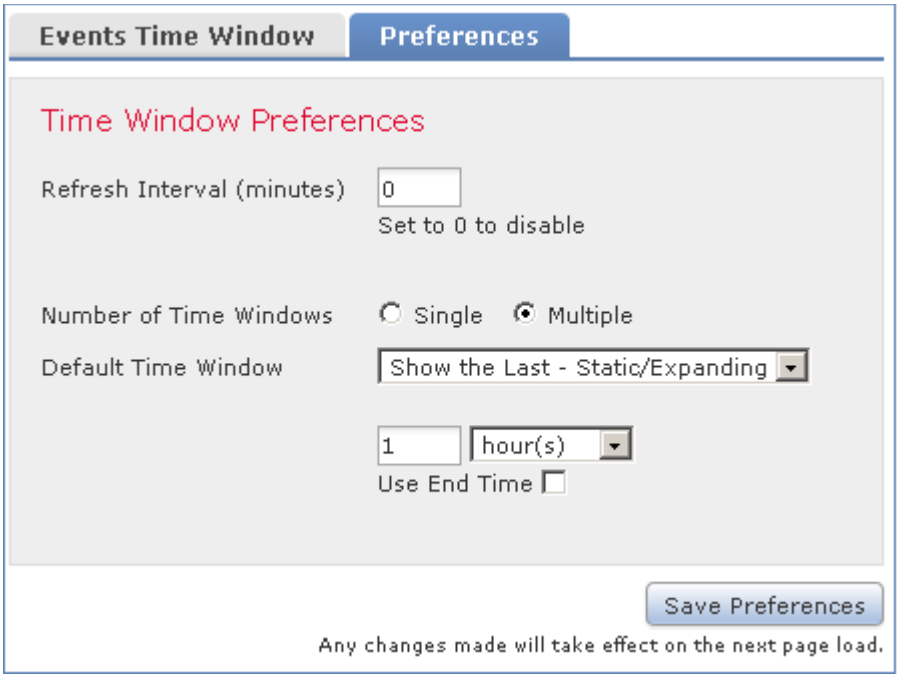
イベント タイプのデフォルトの時間枠の変更

ライセンス： すべて

イベントの分析中に、[Date/Time] ウィンドウの [Preferences] タブを使用し、表示しているイベントのタイプに対するデフォルトの時間枠を（イベント ビューの設定を使用せずに）変更することができます（デフォルトの時間枠（71-6 ページ）を参照してください）。

この方法でデフォルトの時間枠を変更すると、表示しているイベントのタイプのデフォルト時間枠のみが変わります。たとえば、複数の時間枠を設定しており、[Preferences] タブでデフォルトの時間枠を変更すると、イベント、ヘルス モニタリング、または監査ログ ウィンドウのいずれかの設定が変更されます。つまり、最初のタブで示されている時間枠が変更されます。1 つの時間枠を設定している場合に、[Preferences] タブでデフォルトの時間枠を変更すると、イベントのすべてのタイプのデフォルト時間枠が変わります。

次の図は、複数の時間枠が設定されているアプライアンスにおける、[Preferences] タブのDefense Center バージョンを示しています。



次の表で、[Preferences] タブで設定できるさまざまな設定について説明します。

表 58-26　時間枠のプリファレンス

優先順位	説明
Refresh Interval	イベント ビューのリフレッシュ間隔を分単位で設定します。ゼロを入力すると、リフレッシュ オプションは無効になります。
Number of Time Windows	使用する時間枠の数を指定します。 • 監査ログ、ヘルス イベント、および時間によって制約可能なイベントに基づいたワークフローに対してそれぞれ別のデフォルト時間枠を設定する場合は、[Multiple] を選択します。 • すべてのイベントに適用されるグローバルな時間枠を使用する場合は、[Single] を選択します。
Default Time Window: Show the Last - Sliding	この設定を選択すると、指定する長さのスライディングのデフォルト時間枠を設定できます。 アプライアンスは、特定の開始時刻（たとえば 1 時間前）から現在までに生成されたすべてのイベントを表示します。イベント ビューの変更と共に、時間枠は「スライド」して、常に最後の 1 時間内のイベントが表示されます。

表 58-26　時間枠のプリファレンス（続き）

優先順位	説明
Default Time Window: Show the Last - Static/Expanding	この設定を選択すると、指定する長さの、静的または拡張のデフォルト時間枠を設定できます。 **静的な**時間枠の場合（[Use End Time] チェック ボックスをオンにした場合）、アプライアンスは特定の開始時間（1 時間前などの）から、最初にユーザがイベントを参照した時間までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。 **拡張**時間枠の場合（[Use End Time] チェック ボックスをオフにしたの場合）、アプライアンスは特定の開始時間（1 時間前などの）から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。
Default Time Window: Current Day - Static/Expanding	この設定を選択すると、現在の日付に対して静的または拡張のデフォルト時間枠を設定できます。現在の日付は、現行セッションのタイム ゾーン設定に基づいて午前 0 時に始まります。 **静的な**時間枠の場合（[Use End Time] チェック ボックスをオンにした場合）、アプライアンスは午前 0 時から、最初にユーザがイベントを参照した時間までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。 **拡張**時間枠の場合（[Use End Time] チェック ボックスをオフにした場合）、アプライアンスは午前 0 時から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に 24 時間を超えて分析を続けた場合、この時間枠は 24 時間よりも長くなる可能性があることに注意してください。
Default Time Window: Current Week - Static/Expanding	この設定を選択すると、現在の週に対して静的または拡張のデフォルト時間枠を設定できます。現在の週は、現行セッションのタイム ゾーン設定に基づいて直前の日曜日の午前 0 時に始まります。 **静的な**時間枠の場合（[Use End Time] チェック ボックスをオンにした場合）、アプライアンスは午前 0 時から、最初にユーザがイベントを参照した時間までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。 **拡張**時間枠の場合（[Use End Time] チェック ボックスをオフにした場合）、アプライアンスは日曜日の午前 0 時から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に 1 週間を超えて分析を続けた場合、この時間枠は 1 週間よりも長くなる可能性があることに注意してください。

イベントの分析中に時間枠のプリファレンスを変更する方法：

アクセス： Admin/Maint/Any Security Analyst

ステップ 1　時間に制約されるワークフローで、時間範囲のアイコン（）をクリックします。

[Date/Time] ウィンドウが表示されます。

ステップ 2　[Preferences] タブを選択し、時間枠のプリファレンスの表に記載されているようにプリファレンスを変更します。

ステップ 3　[Save Preferences] をクリックします。

プリファレンスが保存されます。

ステップ 4　次の 2 つのオプションから選択できます。

- 使用しているイベント ビューに新しいデフォルト時間枠の設定を適用するには、[Apply] をクリックして [Date/Time] ウィンドウを閉じてイベント ビューをリフレッシュします。
- デフォルトの時間枠設定を適用せずに分析を続けるには、[Apply] をクリックせずに [Date/Time] ウィンドウを閉じます。

時間枠の一時停止

ライセンス： すべて

時間枠を一時停止することができます。これにより、ワークフローで提供されたデータのスナップショットを調べることができます。一時停止されないワークフローが更新されると、調査するイベントが削除されたり、調査対象外のイベントが追加されたりすることがあるため、この機能は有用です。

静的な時間枠は一時停止できないので注意してください。また、イベント時間枠の一時停止はダッシュボードには影響を与えず、ダッシュボードの一時停止も時間枠の一時停止に影響しません。

分析が完了したら、時間枠の一時停止を解除できます。時間枠の一時停止を解除すると、プリファレンスに従って時間枠が更新されます。また、一時停止を解除した時間枠を反映するようにイベント ビューが更新されます。

1 つのワークフロー ページで表示できるイベントよりも多くのイベントがデータベースに含まれている場合は、ページの下部にあるリンクをクリックして、他のイベントを表示できます（ワークフロー内の他のページへのナビゲート (58-39 ページ)を参照してください）。この際、同じイベントが 2 回表示されないように時間枠が自動的に一時停止します。準備ができたら、時間枠の一時停止を解除できます。

時間枠を一時停止する方法：

アクセス： Admin/Maint/Any Security Analyst

ステップ 1　時間枠のコントロールで、一時停止のアイコン（  ）をクリックします。

一時停止を解除するまで、時間枠は一時停止します。

時間枠の一時停止を解除する方法：

アクセス： Admin/Maint/Any Security Analyst

ステップ 1　時間範囲のコントロールで、再生のアイコン（）をクリックします。

時間枠の一時停止が解除され、プリファレンスに従って更新されます。現行の時間枠を反映するようにイベント ビューが更新されます。

イベントの制約

ライセンス：すべて

ワークフロー ページに表示される情報は、ユーザが設定した制約によって異なります。たとえばイベント ワークフローを最初に開いた場合、情報は、最後の 1 時間に生成されたイベントに制約されています。

ワークフローの次のページに進んで、表示されるデータを特定の値で制約する場合は、ページでこれらの値を持つ行を選択し、[View] をクリックします。現在の制約を保持し、すべてのイベントを含めた状態でワークフローの次のページに進むには、[View All] を選択します。

注　複数の不可算値を持つ行を選択し、[View] を選択すると、複合的な制約が作成されます。複合的な制約の詳細については、複合的な制約の使用（58-37 ページ）を参照してください。

ワークフローのデータを制約するための 3 番目の方法があります自身が選択した値を持つ行のみが表示されるようページを制約し、ページの上部に示される制約リストに選択した値を追加するには、ページの行で値をクリックします。

たとえば、次のイベントでページ上の [Initiator IP] カラムの [10.10.60.119] をクリックすると、

	First Packet	Action	Initiator IP	Responder IP	Source Port / ICMP Type
	2013-03-10 23:27:34	Block	10.10.60.119	10.1.1.57	820 / tcp
	2013-03-10 23:27:34	Block	10.10.60.119	10.1.1.57	820 / tcp
	2013-03-10 22:19:28	Block	10.10.60.119	10.1.1.57	753 (rrh) / tcp
	2013-03-10 16:13:39	Block	10.10.32.124	10.10.60.165	856 / tcp

372156

制約されたページには、この IP アドレスを持つイベントのみが示されます。

Search Constraints (Edit Search Save Search)

Initiator IP　10.10.60.119

Connections | Intrusion | Malware | Files | Hosts | Applications | Application Details | Server

	First Packet	Action	Initiator IP	Responder IP	Source Port / ICMP Ty
	2013-03-10 23:27:34	Block	10.10.60.119	10.1.1.57	820 / tcp
	2013-03-10 23:27:34	Block	10.10.60.119	10.1.1.57	820 / tcp
	2013-03-10 22:19:28	Block	10.10.60.119	10.1.1.57	753 (rrh) / tcp
	2013-03-09 23:21:59	Block	10.10.60.119	10.1.1.57	822 / tcp

ヒント　監視ルールの条件に基づいて接続イベントを制約するための手順は少し異なり、いくつかの追加手順が必要になる場合があります。また、関連付けられているファイルや侵入情報によって接続イベントを制約することはできません。詳細については、接続およびセキュリティ インテリジェンスのデータ テーブルの使用（39-29 ページ）を参照してください。

検索を使用して、ワークフローの情報を制約することもできます。検索ページで入力した検索条件はページの上部に制約として表示され、これに従って制約されたイベントが合わせて表示されます。Defense Centerでは、複合的な制約でない限り、他のワークフローにナビゲートしたときにも現在の制約が適用されます（ワークフロー間のナビゲート（58-40 ページ）を参照してください）。

検索する場合は、検索対象のテーブルに検索の制約を適用するかどうかに注意する必要があります。たとえば、クライアント データは接続サマリーでは使用できません。接続で検出されたクライアントに基づいて接続イベントを検索し、結果を接続サマリー イベント ビューで表示すると、Defense Centerでは、制約が設定されていない場合と同じように接続データが表示されます。無効な制約は、非適用（N/A）とラベルが付けられ、取り消し線が付けられます。

次の表では、制約を適用する場合に実行できるそれぞれのアクションについて説明します。

表 58-27　検索の制約機能

目的	クリックする対象
ビューを、1 つの値に一致するイベントに制約する	テーブルの値。 たとえば、記録された接続のリストを表示する場合に、アクセス制御を使用して、自身が許可したものだけがリストに示されるよう制約する場合は、[Action] カラムで [Allow] をクリックします。他の例では、侵入イベントを表示する場合に、宛先ポートが 80 のイベントのみがリストに示されるよう制約する場合は、[DST Port/ICMP Code] カラムで [80 (http)/tcp] をクリックします。
ビューを、複数の値に一致するイベントに制約する	これらの値を持つイベントのチェック ボックスをオンにし、[View] をクリックします。 行に複数の不可算値が含まれている場合は、複合的な制約が追加されることに注意してください。複合的な制約の詳細については、複合的な制約の使用（58-37 ページ）を参照してください。
制約を削除する	[Search Constraints] ボックスで制約の名前をクリックします。
検索ページを使用して制約を編集する	[Search Constraints] ボックスで [Edit Search] をクリックします。 1 つのカラム内の複数の値について制約する場合は、この機能を使用します。たとえば、2 つの IP アドレスに関連しているイベントを表示する場合は、[Edit Search] をクリックし、[Search] ページで対象の [IP address] フィールドを変更して両方のアドレスが含まれるようにして、[Search] をクリックします。
保存済みの検索として制約を保存する	[Search Constraints] ボックスで [Save Search] をクリックし、クエリに名前を指定します。 複合的な制約が含まれているクエリは保存できないことに注意してください。複合的な制約の詳細については、複合的な制約の使用（58-37 ページ）を参照してください。

表 58-27　検索の制約機能（続き）

目的	クリックする対象
別のイベント ビューで同じ制約を使用する	[Jump to] をクリックしてイベント ビューを選択します。詳細については、「ワークフロー間のナビゲート (58-40 ページ)」を参照してください。 別のワークフローに切り替えると、複合的な制約は保持されないことに注意してください。複合的な制約の詳細については、複合的な制約の使用 (58-37 ページ) を参照してください。
制約の表示を切り替える	展開の矢印（▲）をクリックします。制約のリストが長く、画面の大半を占有する場合に、この機能は役立ちます。

複合的な制約の使用

ライセンス： すべて

複合的な制約は、特定のイベントに対するすべての不可算値に基づいています。複数の不可算値を持つ行を選択する場合は、ページ上の対象行におけるすべての不可算値と一致するイベントのみを取得する複合的な制約を設定します。たとえば、送信元 IP アドレスが `10.10.31.17` で、宛先 IP アドレスが `10.10.31.15` である行と、送信元 IP アドレスが `172.10.10.17` で宛先 IP アドレスが `172.10.10.15` である行を選択すると、次のすべての結果が取得されます。

- 送信元 IP アドレスが 10.10.31.17 で、かつ宛先 IP アドレスが 10.10.31.15 のイベント

  または

- 送信元 IP アドレスが 172.10.31.17 で、かつ宛先 IP アドレスが 172.10.31.15 のイベント

複合的な制約と単純な制約を組み合わせると、複合的な制約の各セットに単純な制約が追加されます。たとえば、上記に記載されている複合的な制約に対して、プロトコル値 `tcp` の単純な制約を追加すると、次のすべての結果が取得されます。

- 送信元 IP アドレスが 10.10.31.17 で、かつ宛先 IP アドレスが 10.10.31.15 で、かつプロトコルが tcp であるイベント

  または

- 送信元 IP アドレスが 172.10.31.17 で、かつ宛先 IP アドレスが 172.10.31.15 で、かつプロトコルが tcp であるイベント

複合的な制約について、検索および検索の保存を実行することはできません。また、別のワークフローに切り替えるのに、イベント ビューのリンクを使用した場合、または [(switch workflow)] をクリックした場合は、複合的な制約は保持できません。複合的な制約が適用されているイベント ビューをブックマークしても、制約はブックマークに保存されません。

複合的な制約をすべて消去するには、[Compound Constraints] をクリックします。

テーブル ビュー ページのソートおよびレイアウトの変更

ライセンス： すべて

ワークフローのデータを表示する場合に、使用可能なカラムに基づいてデータをソートすることも、表示するカラムを削除して復元することもできます。カラムによってデータを昇順または降順でソートできます。

ヒント　カスタム ワークフローを作成すると、ページ上のカラムの配置を完全にカスタマイズしたり、ページのソート順を事前定義したりできます。詳細については、「カスタム ワークフローの作成（58-43 ページ）」を参照してください。

表 58-28　ソートおよびレイアウトの機能

目的	クリックする対象
カラムをソートする	カラムのタイトル。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。 **ヒント**　矢印のアイコン（▼）は、データのソート基準になっているカラム、およびソートが昇順である（上向き矢印のアイコン）か、または降順である（下向き矢印のアイコン）かを表します。
テーブル ビューからカラムを削除する	非表示にするカラムの見出しの閉じるアイコン（✖）。表示されるポップアップ ウィンドウで、[Apply] をクリックします。 カラムを無効にすると、そのカラムは（後で元に戻さない限り）そのセッションの期間中は無効になります。最初のカラムを無効にすると、[Count] カラムが追加されることに注意してください。[Count] カラムは無効にすることができません。 **ヒント**　他のカラムを表示または非表示にするには、[Apply] をクリックする前に、該当するチェック ボックスをオンまたはオフにします。無効になったカラムをビューに戻すには、展開アイコン（▲）をクリックして検索の制約を展開し、[Disabled Columns] の下にあるカラム名をクリックします。
無効にしたカラムをビューに戻す	[Disabled Columns] の下のカラム名。 デフォルトで無効になっているカラムを有効にすると、そのカラムは（後で無効にしない限り）セッションの期間中は有効になります。カラムを有効にしても同一行が複数作成されない場合、[Count] カラムは削除されることに注意してください。

ドリルダウン ワークフロー ページのソート

ライセンス： すべて

ワークフローまたはイベント ビューのデータを表示する場合に、使用可能なカラムに基づいてデータをソートしたり、表示するカラムを削除して復元したりすることができます。カラムによってデータを昇順または降順でソートできます。矢印のアイコン（▼）は、データのソート基準になっているカラム、およびソートが昇順である（上向き矢印のアイコン）か、または降順である（下向き矢印のアイコン）かを表します。

ヒント　カスタム ワークフローを作成すると、ページ上のカラムの配置を完全にカスタマイズしたり、ページのソート順を事前定義したりできます。詳細については、「カスタム ワークフローの作成（58-43 ページ）」を参照してください。

カラムをソートする方法：

アクセス： Admin/Maint/Any Security Analyst

ステップ 1　カラムのタイトルをクリックします。

ソートの順序を逆にする方法:

アクセス: Admin/Maint/Any Security Analyst

ステップ 1　カラムのタイトルをもう一度クリックします。

ワークフロー ページの行の選択

ライセンス: すべて

ワークフロー ページで行を選択し、処理を行うにはいくつかの方法があります。

- ページ上のすべての行を選択するには、ページの上部にあるチェック ボックスをオンにします。

  ページの下部にあるいずれかのボタン（[View] や [Delete] など）をクリックすると、そのページ上のすべてのイベントにそのアクションを実行することができます。
- 1 行を選択するには、それぞれの行の隣にあるチェック ボックスをオンにします。

  ページの下部にあるいずれかのボタンをクリックすると、その行に関連付けられているイベントでのみ、そのアクションを実行することができます。
- 1 行を選択し、ワークフローの次のページでその行に関連するイベントを表示するには、矢印のアイコン（  ）をクリックします。

注　複数のページから一度に行を選択することはできません。

ワークフロー内の他のページへのナビゲート

ライセンス: すべて

1 つのワークフロー ページで表示できるイベントよりも多くのイベントがデータベースに含まれている場合は、ページの下部にあるリンクをクリックして、さらにイベントを表示できます。

これらのリンクの 1 つをクリックすると時間枠が自動的に一時停止されるため、同じイベントが 2 回表示されません。準備ができたら時間枠の一時停止を解除できます。詳細については、イベント時間の制約の設定（58-26 ページ）を参照してください。

次の表で、ナビゲート リンクの使用方法について説明します。

表 58-29　ページのナビゲート

目的	クリックする対象
別のページを表示する	ページ番号をクリックし、表示するページを入力して Enter キーを押します
次のページを表示する	>
前のページを表示する	<
最後のページに移動する	>|
最初のページに移動する	|<

ワークフロー間のナビゲート

ライセンス： すべて

ワークフロー ページの [Jump to...] ドロップダウン リストのリンクを使用して、他のワークフローへナビゲートできます。ドロップダウン リストを選択し、追加のワークフローを表示および選択します。

新しいワークフローを選択すると、(適切な場合は)、選択する行で共有されているプロパティおよび設定する制約が、新しいワークフローで使用されます。設定した制約またはイベントのプロパティが、新しいワークフローのフィールドにマップされない場合は、これらはドロップされます。また、ワークフローを切り替えた場合には、複合的な制約は保持されません。キャプチャ ファイルのワークフローの制約は、ファイルおよびマルウェアのイベント ワークフローのみに転送されます。

注 所定の時間範囲のイベント数を表示する場合、詳細なデータを利用できるイベントの数が、イベントの総数に反映されないことがあります。これは、ディスク領域の使用率を管理するために、古いイベントの詳細がシステムによってプルーニングされることがあるために発生します。イベント詳細のプルーニングを最小限にするために、対象の展開にとって最も重要なイベントだけを記録するようにイベント ロギングを調整できます。詳細については、ネットワーク トラフィックの接続のロギング (38-1 ページ) を参照してください。

時間枠を一時停止するか、または静的な時間枠を設定していない場合、ワークフローを変更したときに時間枠も変更されることに注意してください。詳細については、イベント時間の制約の設定 (58-26 ページ) を参照してください。

[Jump to] ドロップダウン リストを使用すると、次のテーブルのワークフローにすばやくアクセスできます。

- 接続イベント
- セキュリティ インテリジェンス イベント
- 侵入イベント
- マルウェア イベント
- ファイル イベント
- ホスト
- 侵害の痕跡
- アプリケーション
- アプリケーションの詳細
- サーバ
- ホスト属性
- 検出イベント
- users
- 脆弱性
- サードパーティの脆弱性
- 相関イベント
- ホワイトリスト イベント

この機能により、疑わしいアクティビティの調査が強化されます。たとえば、接続データを表示していて、内部ホストが異常に大量のデータを外部サイトに転送していることに気付いた場合は、応答側の IP アドレスとポートを制約として選択し、[Applications] ワークフローへ移動することができます。[Applications] ワークフローは応答側の IP アドレスとポートを IP アドレスとポートの制約として使用し、アプリケーションの種類などの追加情報を表示することができます。ページの上部にある [Hosts] をクリックして、リモート ホストのホスト プロファイルを表示することもできます。

アプリケーションに関する詳細を検索した後で、[Correlation Events] を選択して接続データ ワークフローに戻る、制約から応答側の IP アドレスを削除する、制約にイニシエータの IP アドレスを追加する、[Application Details] を選択して、データをリモート ホストに転送するときに開始側のホストでユーザがどのクライアントを使用しているかを確認する、といったことができます。ポートの制約は、[Application Details] ページには転送されないことに注意してください。ローカル ホストを制約として保持したまま、追加情報を検索するために他のナビゲート ボタンを使用することもできます。

- ローカル ホストがいずれかのポリシーに違反しているかどうかを検出するには、IP アドレスを制約として保持したままで [Jump to] ドロップダウン リストから [Correlation Events] を選択します。
- ホストに対して侵入ルールがトリガーされた（侵害を表している）かどうかを確認するには、[Jump to] ドロップダウン リストから [Intrusion Events] を選択します。
- ローカル ホストのホスト プロファイルを表示し、ホストが、悪用された可能性のある脆弱性の影響を受けやすくなっているかどうかを判断するには、[Jump to] ドロップダウン リストから [Hosts] を選択します。

ブックマークの使用

ライセンス： すべて

イベントの分析中に所定の場所および時間にすばやく戻りたい場合には、ブックマークを作成します。ブックマークは、次の情報を保持します。

- 使用中のワークフロー
- 表示中のワークフローの部分
- ワークフローのページ番号
- 検索の制約
- 無効になっているカラム
- 使用している時間範囲

あるユーザが作成したブックマークは、ブックマーク アクセスを持っているすべてのユーザ アカウントで利用できます。これは、より詳細な分析を必要とするイベント セットを見つけた場合、簡単にブックマークを作成し、適切な権限を持った他のユーザに調査を引き継ぐことが可能であることを意味します。

注　ブックマークに表示されているイベントが（ユーザによって直接、またはデータベースの自動クリーンアップによって）削除されると、そのブックマークにはイベントの元のセットは表示されません。

ブックマークの使用の詳細については、以下の項を参照してください。

- ブックマークの作成（58-42 ページ）では、新しいブックマークを作成する方法について説明します。
- ブックマークの表示（58-42 ページ）では、既存のブックマークを表示および使用する方法について説明します。
- ブックマークの削除（58-43 ページ）では、ブックマークを削除する方法について説明します。

ブックマークの作成

ライセンス： すべて

新しいブックマークを作成するには、次の手順を使用します。

ブックマークを作成する方法：

アクセス： Admin/Maint/Any Security Analyst

ステップ 1　イベントの分析中に、表示されている対象のイベントで [Bookmark This Page] をクリックします。

[Create a Bookmark] ページが表示されます。

ステップ 2　[Bookmark Name] フィールドで、ブックマークの名前を（最大 80 文字の英数字とスペースで）入力し、[Save Bookmark] をクリックします。

ブックマークが保存され、ブックマークしたイベントのページがもう一度表示されます。

ブックマークの表示

ライセンス： すべて

既存のブックマークを表示して使用するには、次の手順を使用します。

ブックマークを表示する方法：

アクセス： Admin/Maint/Any Security Analyst

ステップ 1　イベント ビューから [View Bookmarks] をクリックします。

[Bookmarks] ページが表示されます。

ステップ 2　使用するブックマークの隣にある [View] をクリックします。

ブックマークしたページが表示されます。

注　最初にブックマークに表示されていたイベントが（ユーザによって直接、またはデータベースの自動クリーンアップによって）削除されると、そのブックマークにはイベントの元のセットは表示されません。

ブックマークの削除

ライセンス：すべて

ブックマークを削除するには、次の手順を使用します。ブックマークを削除しても、そのブックマークによって取得されるイベントは影響を受けないことに注意してください。

ブックマークを削除する方法：

アクセス：Admin/Maint/Any Security Analyst

ステップ 1　イベント ビューから [View Bookmarks] をクリックします。

[Bookmarks] ページが表示されます。

ステップ 2　削除するブックマークの隣にある [削除] をクリックします。

ブックマークが削除されます。

カスタムワークフローの使用

ライセンス：すべて

Ciscoが提供する事前定義のカスタム ワークフローがニーズに合わない場合は、カスタム ワークフローを作成することができます。

詳細については、以下を参照してください。

- カスタム ワークフローの作成（58-43 ページ）（カスタム ワークフローを作成する手順）
- カスタム接続データ ワークフローの作成（58-45 ページ）（接続データに基づいてカスタム ワークフローを作成する手順）
- カスタム ワークフローの表示（58-47 ページ）（イベントおよびカスタム テーブルに基づいてカスタム ワークフローを表示する手順）
- カスタム ワークフローの編集（58-48 ページ）（カスタム ワークフローを編集する手順）
- カスタム ワークフローの削除（58-49 ページ）（カスタム ワークフローを削除する手順）

カスタム ワークフローの作成

ライセンス：すべて

Ciscoが提供する事前定義のカスタム ワークフローがニーズに合わない場合は、カスタム ワークフローを作成することができます。

ヒント　新しいカスタム ワークフローを作成する代わりに、別のアプライアンスからカスタム ワークフローをエクスポートし、それを自身のアプライアンスへインポートすることができます。その後でニーズに合わせて、インポートしたワークフローを編集することができます。詳細については、設定のインポートおよびエクスポート（A-1 ページ）を参照してください。

カスタム ワークフローを作成する場合は、次の操作を行います。

- ワークフローのソースとなるテーブルを選択する
- ワークフローの名前を指定する
- ワークフローにドリル ダウン ページおよびテーブル ビュー ページを追加する

ワークフローの各ドリル ダウン ページでは、次のことができます。

- Web インターフェイスのページの上部に表示される名前を指定する
- 1 ページにつき最大 5 個のカラムを含める
- デフォルトのソート順（昇順または降順）を指定する

ワークフロー ページの順序において、任意の場所にテーブル ビュー ページを追加することができます。これらのページには編集可能なプロパティ（ページ名、ソート順、ユーザ定義可能なカラム位置など）がありません。

カスタム ワークフローの最終ページは、次の表に記載されているように、ワークフローのベースにしているテーブルによって異なります。これらの最終ページは、ワークフローを作成したときにデフォルトで追加されます。

表 58-30　　カスタム ワークフローの最終ページ

ワークフローのベース	最終ページ
検出イベント	ホスト
脆弱性	脆弱性の詳細
サードパーティの脆弱性	ホスト
users	users
侵害の痕跡	ホスト
侵入イベント	パケット

アプライアンスは、他の種類のイベント（監査ログやマルウェア イベントなど）に基づいたカスタム ワークフローには最終ページを追加しません。

注　接続データに基づいてカスタム ワークフローを作成するための手順は少し異なります。詳細は、次の項カスタム接続データ ワークフローの作成を参照してください。

カスタム ワークフローを作成する方法：

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Custom] > [Custom Workflows] を選択します。

[Custom Workflows] ページが表示されます。

ステップ 2　[Create Custom Workflow] をクリックします。

[Edit Custom Workflow] ページが表示されます。

ステップ 3　[Name] フィールドにワークフローの名前を入力します。

名前には最大 60 文字の英数字およびスペースを使用できます。

ステップ 4　オプションで、[Description] フィールドに、ワークフローの説明を入力します。

最大 80 文字の英数字およびスペースを使用できます。

ステップ 5　[Table] ドロップダウン リストから、対象とするテーブルを選択します。

ステップ 6　オプションで、[Add Page] をクリックして、ワークフローに 1 つ以上のドリルダウン ページを追加します。

ドリルダウン ページのセクションが表示されます。

最大 80 文字の英数字（スペースは不可）を使用して、[Page Name] フィールドにページの名前を入力します。

[Column 1] で、ソートの優先度およびテーブルのカラムを選択します。このカラムは、ページの最も左のカラムとして表示されます。たとえば、対象とする宛先ポートを示すページを作成し、カウントでページをソートするには、[Sort Priority] ドロップダウン リストから [2] を選択し、[Field] ドロップダウン リストから [DST Port/ICMP Code] を選択します。

ページに表示するすべてのフィールドの指定が完了するまで、フィールドを選択してソートの優先度の設定を続けます。1 ページにつき最大 5 個のフィールドを指定できます。

注　ステップ 5 で [Table Type] として [Vulnerabilities] を選択し、テーブル カラムとして [IP Address] を追加しても、検索機能を使用して特定の IP アドレスまたはアドレスのブロックを表示するようワークフローを制約しない限り、カスタム ワークフローを使用して脆弱性を表示する場合に [IP Address] カラムは表示されません。脆弱性の検索の詳細については、脆弱性の検索（50-58 ページ）を参照してください。

ステップ 7　オプションで、[Add Table View] をクリックして、ワークフローにテーブル ビュー ページを追加します。

注　カスタム ワークフローには、イベントのドリルダウン ページまたはテーブル ビューを少なくとも 1 つ追加する必要があります。

ステップ 8　[Save] をクリックします。

新しいワークフローが保存され、カスタム ワークフローのリストに追加されます。

カスタム接続データ ワークフローの作成

ライセンス：FireSIGHT

接続データに基づいたカスタム ワークフローは他のカスタム ワークフローと似ていますが、ドリルダウン ページとテーブル ビュー ページだけでなく、接続データ グラフのページも含めることができます。必要に応じて、ワークフローにそれぞれのタイプのページを任意の数だけ、任意の順序で含めることができます。それぞれの接続データ グラフのページには 1 つのグラフ（線グラフ、棒グラフ、または円グラフ）が含まれます。線グラフと棒グラフには、複数のデータセットを含めることができます。接続のサマリー、接続グラフ、データセットなどの接続データの詳細については、接続およびセキュリティ インテリジェンスのデータについて（39-2 ページ）を参照してください。

ヒント　新しいカスタム ワークフローを作成する代わりに、別のアプライアンスからカスタム ワークフローをエクスポートし、それを自身のアプライアンスへインポートすることができます。その後でニーズに合わせて、インポートしたワークフローを編集することができます。詳細については、設定のインポートおよびエクスポート（A-1 ページ）を参照してください。

接続データに基づいてカスタム ワークフローを作成する方法:

アクセス: Admin

ステップ 1　[Analysis] > [Custom] > [Custom Workflow] を選択します。

ステップ 2　[Create Custom Workflow] をクリックします。

[Edit Custom Workflow] ページが表示されます。

ステップ 3　[Name] フィールドにワークフローの名前を入力します。

最大 60 文字の英数字およびスペースを使用できます。

ステップ 4　オプションで、[Description] フィールドに、ワークフローの説明を入力します。

最大 80 文字の英数字およびスペースを使用できます。

ステップ 5　[Table] ドロップダウン リストから、[Connection Events] を選択します。

ステップ 6　オプションで、ワークフローに 1 つ以上のドリルダウン ページを追加します。

- 個々の接続に関するデータが含まれているドリルダウン ページを追加するには、[Add Page] をクリックします。
- 接続のサマリー データが含まれているドリルダウン ページを追加するには、[Add Summary Page] をクリックします。

いずれの場合も、ドリルダウン ページのセクションが表示されます。

最大 80 文字の英数字（スペースは不可）を使用して、[Page Name] フィールドにページの名前を入力します。

[Column 1] で、ソートの優先度およびテーブルのカラムを選択します。このカラムは、ページの最も左のカラムとして表示されます。

ページに表示するすべてのフィールドの指定が完了するまで、フィールドを選択してソートの優先度の設定を続けます。1 ページにつき最大 5 個のフィールドを指定できます。

たとえば、監視対象ネットワーク経由で転送されるトラフィックの量を表示するページを作成し、トラフィックの転送量が最も多い応答側によってページをソートするには、[Sort Priority] ドロップダウン リストで [1] を選択し、[Field] ドロップダウン リストで [Responder Bytes] を選択します。

ステップ 7　オプションで、[Add Graph] をクリックして、ワークフローに 1 つ以上のグラフ ページを追加します。

グラフ セクションが表示されます。

最大 80 文字の英数字（スペースは不可）を使用して、[Graph Name] フィールドにページの名前を入力します。

次に、ページに含めるグラフの種類（線グラフ、棒グラフ、または円グラフ）を選択します。

グラフの X 軸と Y 軸を選択し、どのようなデータをグラフ化するのかを指定します。円グラフでは、X 軸は独立変数を表し、Y 軸は従属変数を表します。

最後に、グラフに含めるデータセットを選択します。円グラフには 1 つのデータセットしか含めることができないことに注意してください。

ステップ 8　オプションで、[Add Table View] をクリックして、接続データのテーブル ビューを追加します。

ステップ 9　[Save] をクリックします。

新しいワークフローが保存され、カスタム ワークフローのリストに追加されます。

カスタム ワークフローの表示

ライセンス：すべて

ワークフローが、事前定義のイベント テーブルまたはカスタム テーブルのいずれに基づいているかによって、ワークフローの表示に使用する方法が異なります。

カスタム ワークフローが事前定義のイベント テーブルに基づいている場合は、アプライアンスに付属しているワークフローにアクセスするのと同じ方法でアクセスします。たとえば、ホスト テーブルに基づいているカスタム ワークフローにアクセスするには、[Analysis Hosts] を選択します。また、カスタム ワークフローがカスタム テーブルに基づいている場合は、[Custom Tables] ページからアクセスする必要があります。

ヒント　任意のイベント タイプについて、デフォルト ワークフローとしてカスタム ワークフローを設定することができます。イベント ビュー設定の設定（71-3 ページ）を参照してください。

詳細については、以下を参照してください。

- 事前定義のテーブルのカスタム ワークフローの表示（58-47 ページ）
- カスタム テーブルのカスタム ワークフローの表示（58-48 ページ）

事前定義のテーブルのカスタム ワークフローの表示

ライセンス：すべて

カスタム テーブルに基づいて**いない**カスタム ワークフローを表示するには、次の手順を使用します。ワークフローの選択（58-18 ページ）に記載されているように、ワークフローのアクセスは使用しているプラットフォームとユーザ ロールによって異なることに注意してください。

事前定義のテーブルに基づいたカスタム ワークフローを表示する方法：

アクセス：Admin/Any Security Analyst

ステップ 1　ワークフローを使用する機能の表に記載されているように、カスタム ワークフローのベースとなるテーブルについて、適切なメニュー パスとオプションを選択します。

そのテーブルのデフォルト ワークフローの最初のページが表示されます。カスタム ワークフローも含め、別のワークフローを使用するには、現行のワークフロー タイトルの隣にある [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。イベントが表示されず、ワークフローを時間によって制約できる場合は、時間範囲の調整が必要なことがあります。イベント時間の制約の設定（58-26 ページ）を参照してください。

カスタム テーブルのカスタム ワークフローの表示

ライセンス：FireSIGHT

カスタム テーブルに基づいているカスタム ワークフローを表示するには、次の手順を使用します。

カスタム テーブルに基づいたカスタム ワークフローを表示する方法：

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Custom] > [Custom Tables] を選択します。

[Custom Tables] ページが表示され、使用できるカスタム テーブルが示されます。

ステップ 2　表示するカスタム テーブルの隣にある表示アイコンをクリックするか、またはカスタム テーブルの名前をクリックします。

そのテーブルのデフォルト ワークフローの最初のページが表示されます。カスタム ワークフローも含め、別のワークフローを使用するには、現行のワークフロー タイトルの隣にある [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。イベントが表示されず、ワークフローを時間によって制約できる場合は、時間範囲の調整が必要なことがあります。イベント時間の制約の設定（58-26 ページ）を参照してください。

カスタム ワークフローの編集

ライセンス：すべて

イベント評価プロセスが変わった場合には、新しいニーズを満たすようにカスタム ワークフローを編集することができます。事前定義のワークフローは編集できないことに注意してください。

カスタム ワークフローを編集する方法：

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Custom] > [Custom Workflows] を選択します。

[Custom Workflows] ページが表示され、既存のカスタム ワークフローが示されます。

ステップ 2　編集するワークフロー名の隣にある編集アイコン（  ）をクリックします。

[Edit Workflow] ページが表示されます。

ステップ 3　ワークフローに必要な変更を加え、[Save] をクリックします。

ワークフローに対する変更が保存されます。

カスタム ワークフローの削除

ライセンス: すべて

次の手順は、不要になったカスタム ワークフローを削除する方法について説明します。

カスタム ワークフローを削除する方法:

アクセス: Admin/Any Security Analyst

ステップ 1　[Analysis] > [Custom] > [Custom Workflows] を選択します。

[Custom Workflows] ページが表示され、使用できるカスタム ワークフローが示されます。

ステップ 2　削除するワークフロー名の隣にある削除アイコン( )をクリックします。

ワークフローが削除されます。

カスタム テーブルの使用

FireSIGHT システムがネットワークに関する情報を収集し、Defense Centerがその情報を一連のデータベース テーブルに保存します。結果として生成される情報を表示するためにワークフローを使用する場合、Defense Centerはそれらのテーブルのいずれかからデータを取り出します。たとえば、[Network Applications by Count（カウントに基づいたネットワーク アプリケーション）] ワークフローの各ページのカラムは、[Applications] テーブルのフィールドから取得されます。

さまざまなテーブルのフィールドを結合することにより、ネットワークのアクティビティの分析が向上する場合、カスタム テーブルを作成できます。たとえば、定義済みの [Host Attributes] テーブルのホスト重大度情報と、定義済みの [Connection Data] テーブルのフィールドを結合してから、新しいコンテキストで接続データを検証できます。

定義済みのテーブルまたはカスタム テーブルのどちらについても、カスタム ワークフローを作成できます。カスタム ワークフローの作成の詳細については、カスタム ワークフローの作成（58-43 ページ）を参照してください。

以下のセクションでは、独自のカスタム テーブルを作成して使用する方法について説明します。

カスタム テーブルについて

ライセンス： FireSIGHT

カスタム テーブルには、2 つ以上の定義済みのテーブルのフィールドが含まれます。FireSIGHT システム では、システム定義のカスタム テーブルが多数提供されていますが、自分のニーズに合った情報だけを含むカスタム テーブルをさらに作成できます。

たとえば、FireSIGHT システム では、侵入イベント データをホスト データと相関させるシステム定義のカスタム テーブルが提供されているので、重要なシステムに影響を与えるイベントを検索して、その検索の結果を 1 つのワークフローで表示できます。次の表は、システムに付属しているカスタム テーブルについて説明します。

表 59-1　システム定義のカスタム テーブル

テーブル	説明
Hosts with Servers	ネットワーク上で実行されている検出されたアプリケーションに関する情報と、それらのアプリケーションを実行しているホストに関する基本的なオペレーティング システム情報を提供する、[Hosts] および [Servers] テーブルのフィールドが含まれます。
Intrusion Events with Destination Criticality	侵入イベントに関する情報と、各侵入イベントに関係する宛先ホストのホスト重大度に関する情報を提供する、[Intrusion Events] および [Hosts] テーブルのフィールドが含まれます。 **ヒント**　このテーブルは、ホスト重大度が高い宛先ホストが関係する侵入イベントを検索するために使用します。
Intrusion Events with Source Criticality	侵入イベントに関する情報と、各侵入イベントに関係する送信元ホストのホスト重大度に関する情報を提供する、[Intrusion Events] および [Hosts] テーブルのフィールドが含まれます。 **ヒント**　このテーブルは、ホスト重大度が高い送信元ホストが関係する侵入イベントを検索するために使用します。

可能なテーブルの結合について

ライセンス: FireSIGHT + Protection

カスタム テーブルを作成する場合、関連データを含む定義済みのテーブルのフィールドを結合できます。次の表は、新しいカスタム テーブルを作成するために結合できる定義済みのテーブルをリストしています。3 つ以上の定義済みのカスタム テーブルのフィールドを結合してカスタム テーブルを作成できることに留意してください。

表 59-2　カスタム テーブルの結合

以下のテーブルのフィールドを	以下のテーブルのフィールドと結合可能
アプリケーション	• Correlation Events • Intrusion Events • Connection Summary Data • Host Attributes • Application Details • Discovery Events • Connection Events • ホスト • サーバ • White List Events
Correlation Events	• アプリケーション • Host Attributes • ホスト

表 59-2　カスタム テーブルの結合（続き）

以下のテーブルのフィールドを	以下のテーブルのフィールドと結合可能
Intrusion Events	• アプリケーション • Host Attributes • ホスト • サーバ
Connection Summary Data	• アプリケーション • Host Attributes • ホスト • サーバ
Indications of Compromise	• アプリケーション • Application Details • Captured Files • Connection Events • Connection Summary Data • Correlation Events • Discovery Events • Host Attributes • ホスト • Intrusion Events • Security Intelligence Events • サーバ • White List Events
Host Attributes	• アプリケーション • Correlation Events • Intrusion Events • Connection Summary Data • Application Details • Discovery Events • Connection Events • ホスト • サーバ • White List Events
Application Details	• アプリケーション • Host Attributes • ホスト

表 59-2　カスタム テーブルの結合（続き）

以下のテーブルのフィールドを	以下のテーブルのフィールドと結合可能
Discovery Events	• アプリケーション • Host Attributes • ホスト
Connection Events	• アプリケーション • Host Attributes • ホスト • サーバ
セキュリティ インテリジェンス イベント	• アプリケーション • Host Attributes • ホスト • サーバ
ホスト	• アプリケーション • Correlation Events • Intrusion Events • Connection Summary Data • Host Attributes • Application Details • Discovery Events • Connection Events • サーバ • White List Events
サーバ	• アプリケーション • Intrusion Events • Connection Summary Data • Host Attributes • Connection Events • ホスト
White List Events	• アプリケーション • Host Attributes • ホスト

あるテーブルのフィールドが、別のテーブルの複数のフィールドにマップされる場合があります。たとえば、定義済みの [Intrusion Events with Destination Criticality] カスタム テーブルは、[Intrusion Events] テーブルと [Hosts] テーブルのフィールドを結合します。[Intrusion Events] テーブルの各イベントは、2 つの IP アドレス（送信元 IP アドレスと宛先 IP アドレス）と関連付けられています。しかし、[Hosts] テーブルの「イベント」はそれぞれ、単一のホスト IP アドレスを表します（ホストに複数の IP アドレスが存在する場合があります）。したがって、[Intrusion Events] テー

ブルと [Hosts] テーブルに基づいてカスタム テーブルを作成する場合は、[Hosts] テーブルから表示するデータが [Intrusion Events] テーブルのホストの送信元 IP アドレスまたはホストの宛先 IP アドレスのどちらに適用されるかを選択する必要があります。

新しいカスタム テーブルを作成すると、テーブルのすべてのカラムを表示するデフォルトのワークフローが自動的に作成されます。定義済みのテーブルと同じように、ネットワーク分析で使用するデータをカスタム テーブルで検索することもできます。また、定義済みのテーブルで行うのと同じように、カスタム テーブルに基づいてレポートを生成することもできます。

カスタム テーブルの作成の詳細については、以下を参照してください。

カスタム テーブルの作成

ライセンス： FireSIGHT

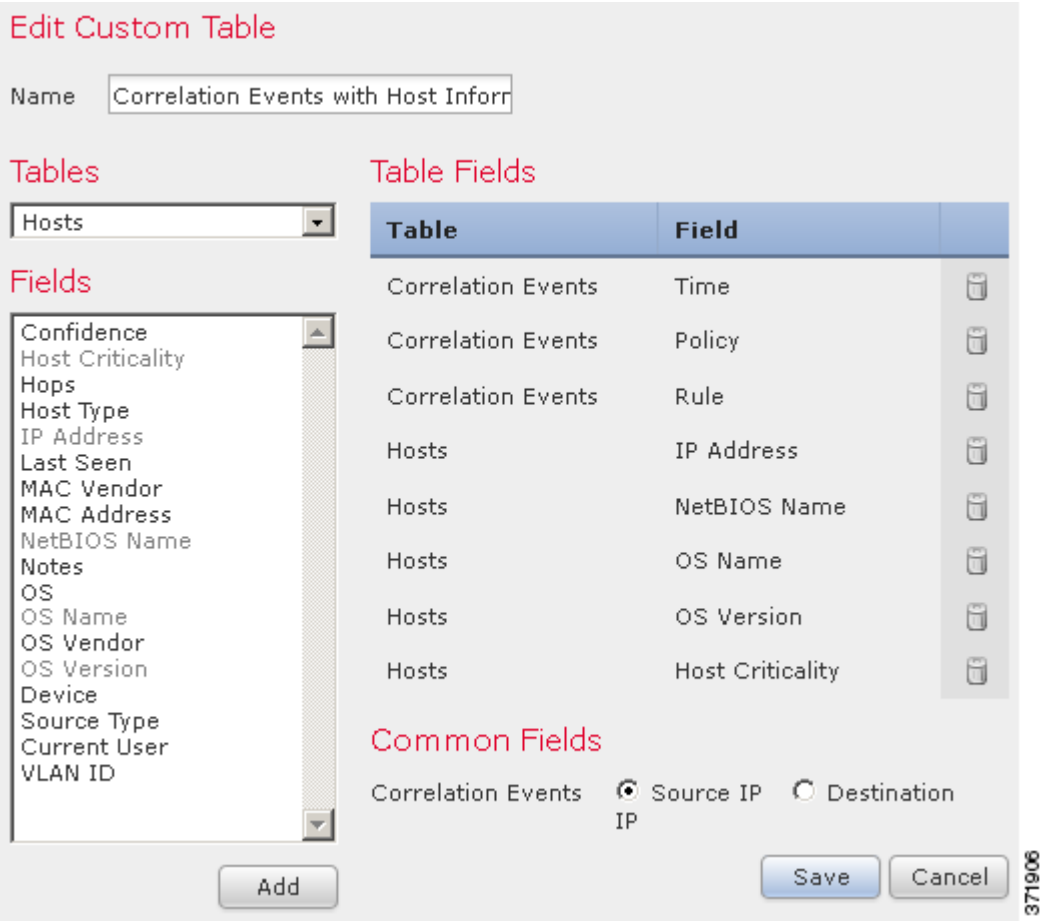
さまざまなテーブルのフィールドを結合することにより、ネットワークのアクティビティの分析が向上する場合、カスタム テーブルを作成できます。

ヒント 新しいカスタム テーブルを作成する代わりに、別のDefense Centerからカスタム テーブルをエクスポートし、Defense Centerにインポートできます。その後、必要に合わせて、インポートしたカスタム テーブルを編集できます。詳細については、設定のインポートおよびエクスポート（A-1 ページ）を参照してください。

カスタム テーブルを作成するには、FireSIGHT システムに付属しているどの定義済みテーブルに、カスタム テーブルに組み込むフィールドが含まれているかを判断します。その後、組み込むフィールドを選択できます。さらに、必要に応じて、共通フィールドのフィールド マッピングを設定することもできます。

ヒント [Hosts] テーブルを含むデータでは、1 つの IP アドレスではなく、1 つのホストのすべての IP アドレスに関連したデータを表示できます。

例として、[Correlation Events] テーブルと [Hosts] テーブルのフィールドを結合するカスタム テーブルについて考慮します。このカスタム テーブルを使用して、相関ポリシーの違反に関係するホストの詳細情報を取得できます。注意すべき点として、[Correlation Events] テーブルの送信元 IP アドレスと宛先 IP アドレスのどちらと一致する [Hosts] テーブルのデータを表示するかを決定する必要があります。



このカスタム テーブルのイベントのテーブル ビューを表示する場合、相関イベントが 1 行に 1 つずつ表示されます。次の情報が表示されます。

- イベントが生成された日時
- 違反された相関ポリシーの名前
- 違反をトリガーとして使用した規則の名前
- 相関イベントに関係する送信元ホスト（開始ホスト）に関連付けられた IP アドレス
- 送信元ホストの NetBIOS 名
- 送信元ホストが実行しているオペレーティング システムおよびバージョン
- 送信元ホストの重大度

ヒント　宛先ホスト（応答ホスト）の同じ情報を表示する同じようなカスタム テーブルを作成することもできます。

上述の例のカスタム テーブルを作成する方法:

アクセス: Admin

ステップ 1　[Analysis] > [Custom] > [Custom Tables] を選択します。

[Custom Tables] ページが表示されます。

ステップ 2　[Create Custom Table] をクリックします。

[Create Custom Table] ページが表示されます。

ステップ 3　[Name] フィールドに、[Correlation Events with Host Information (Src IP)] などのカスタム テーブルの名前を入力します。

ステップ 4　[Tables] ドロップダウンリストから、[Correlation Events] を選択します。

[Correlation Events] テーブルのフィールドが [Fields] リストに表示されます。

ステップ 5　[Fields] で [Time] を選択し、[Add] をクリックして、相関イベントが生成された日時を追加します。

ステップ 6　ステップ 5 を繰り返して、[Policy] および [Rule] フィールドを追加します。

ヒント　Ctrl または Shift を押しながらクリックすることにより、複数のフィールドを選択できます。また、クリックしてドラッグすることで、隣接する複数の値を選択できます。しかし、テーブルに関連したイベントのテーブル ビューでフィールドが表示される順序を指定する場合、フィールドを一度に 1 つずつ追加します。

ステップ 7　[Table] ドロップダウンリストから [Hosts] を選択します。

[Hosts] テーブルのフィールドが [Fields] リストに表示されます。これらのフィールドの詳細については、ホスト テーブルについて (50-22 ページ) を参照してください。

ステップ 8　[IP Address]、[NetBIOS Name]、[OS Name]、[OS Version]、および [Host Criticality] フィールドをカスタム テーブルに追加します。

ステップ 9　[Correlation Events] の隣にある [Common Fields] で、[Source IP] を選択します。

相関イベントに関係する送信元ホスト (開始ホスト) 用にステップ 8 で選択したホスト情報を表示するように、カスタム テーブルが設定されます。

ヒント　相関イベントに関係する宛先ホスト (応答ホスト) に関する詳細なホスト情報を表示するカスタム テーブルを作成する場合、この手順に従うものの、[Source IP] ではなく、[Destination IP] を選択します。

ステップ 10　[Save] をクリックします。

カスタム テーブルが保存されます。

カスタム テーブルの変更

ライセンス: FireSIGHT

ニーズの変化に応じて、カスタム テーブルのフィールドを追加したり削除したりできます。

カスタム テーブルを変更する方法:

アクセス: Any/Admin

ステップ 1　[Analysis] > [Custom] > [Custom Tables] を選択します。

[Custom Tables] ページが表示されます。

ステップ 2　編集するテーブルの横にある編集アイコン( )をクリックします。

[Edit Custom Table] ページが表示されます。変更可能なさまざまな設定の詳細については、カスタム テーブルの作成（59-5 ページ）を参照してください。

ステップ 3　除外するフィールドの横にある削除アイコン( )をクリックして、テーブルからフィールドを除外することもできます。

注　レポートで現在使用中のフィールドを削除すると、それらのフィールドを使用しているセクションをそれらのレポートから除外するか確認するプロンプトが出されます。

ステップ 4　必要に応じて他の変更を行い、[Save] をクリックします。

カスタム テーブルが更新されます。

カスタム テーブルの削除

ライセンス: FireSIGHT

必要なくなったカスタム テーブルを削除できます。カスタム テーブルを削除すると、そのカスタム テーブルを使用する保存済み検索も削除されます。

カスタム テーブルを削除する方法:

アクセス: Any/Admin

ステップ 1　[Analysis] > [Custom] > [Custom Tables] を選択します。

[Custom Tables] ページが表示されます。

ステップ 2　削除するカスタム テーブルの隣にある削除アイコン( )をクリックします。

テーブルが削除されます。

カスタム テーブルに基づいたワークフローの表示

ライセンス: FireSIGHT

カスタム テーブルを作成すると、そのデフォルトのワークフローがシステムによって自動的に作成されます。このワークフローの最初のページには、イベントのテーブル ビューが表示されます。カスタム テーブルに侵入イベントを含める場合、ワークフローの 2 番目のページはパケット ビューになります。それ以外の場合、ワークフローの 2 番目のページはホスト ページになります。カスタム テーブルに基づいて、独自のカスタム ワークフローを作成することもできます。

ヒント　カスタム テーブルに基づいてカスタム ワークフローを作成する場合、それをそのテーブルのデフォルトのワークフローとして指定できます。詳細については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

同じ手法を使用して、定義済みのテーブルに基づいたイベント ビューに使用するカスタム テーブルでイベントを表示できます。詳細については、「ワークフローのページの使用（58-21 ページ）」を参照してください。

カスタム テーブルに基づいたワークフローを表示する方法：

アクセス： Any/Admin

ステップ 1　[Analysis] > [Custom] > [Custom Tables] を選択します。

[Custom Tables] ページが表示されます。

ステップ 2　表示するワークフローが基づくカスタム テーブルの隣にある表示アイコン（  ）をクリックします。

カスタム テーブルのデフォルトのワークフローの最初のページが表示されます。別のワークフローを使用するには、ワークフローのタイトルの横にある [(switch workflow)] をクリックします。別のデフォルトのワークフローを指定する方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。イベントが表示されず、ワークフローを時間によって制約できる場合は、時間範囲の調整が必要なことがあります。イベント時間の制約の設定（58-26 ページ）を参照してください。

カスタム テーブルの検索

ライセンス： FireSIGHT

カスタム テーブルの検索を作成して保存できます。ネットワーク環境に合わせてカスタマイズされた検索を作成してから、後で再利用できるように保存することができます。カスタム テーブルを削除すると、そのカスタム テーブル用に保存したすべての検索も削除されるので注意してください。

使用できる検索基準は、カスタム テーブルを作成するために使用した定義済みのテーブルの基準と同じです。使用できる検索基準の詳細については、以下の表に示されているセクションを参照してください。

表 59-3　テーブルの検索基準

検索基準	参照先
Audit Events	監査レコードの検索（69-8 ページ）
Application Details	アプリケーションの詳細の検索（50-52 ページ）
Correlation Events	相関イベントの検索（51-59 ページ）
Connection Data	接続およびセキュリティ インテリジェンスのデータの検索（39-34 ページ）
ホスト	ホストの検索（50-27 ページ）
Host Attributes	ホスト属性の検索（50-33 ページ）

表 59-3　テーブルの検索基準（続き）

検索基準	参照先
Hosts with Applications	ホストの検索（50-27 ページ）およびサーバの検索（50-43 ページ）
Intrusion Events	侵入イベントの検索（41-44 ページ）
Intrusion Events with Destination Criticality	侵入イベントの検索（41-44 ページ）およびホストの検索（50-27 ページ）
Intrusion Events with Source Criticality	侵入イベントの検索（41-44 ページ）およびホストの検索（50-27 ページ）
Status Events	修復ステータス イベントの検索（54-22 ページ）
Discovery Events	ディスカバリ イベントの検索（50-18 ページ）
User Events	ユーザ アクティビティの検索（50-74 ページ）
Rule Update Import Log	[Rule Update Import Log] の検索（66-28 ページ）
アプリケーション	アプリケーションの検索（50-48 ページ）
Security Intelligence Events	接続およびセキュリティ インテリジェンスのデータの検索（39-34 ページ）
ユーザ	ユーザの検索（50-68 ページ）
Vulnerabilities	脆弱性の検索（50-58 ページ）
White List Events	コンプライアンス ホワイト リスト イベントの検索（52-36 ページ）
White List Violations	ホワイト リスト違反の検索（52-41 ページ）

テーブル検索にそれらの基準を実装するには、次の手順を参照してください。

カスタム テーブルで検索を実行する方法：

アクセス： Any/Admin

ステップ 1　[Analysis] > [Custom] > [Custom Tables] を選択します。

[Custom Tables] ページが表示されます。

ステップ 2　検索するカスタム テーブルの隣にある表示アイコン（🔍）をクリックします。

カスタム テーブルのデフォルトのワークフローの最初のページが表示されます。別のワークフロー（カスタム ワークフローを含む）を使用するには、ワークフローのタイトルの横にある [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。イベントが表示されず、ワークフローを時間によって制約できる場合は、時間範囲の調整が必要なことがあります。イベント時間の制約の設定（58-26 ページ）を参照してください。

ステップ 3　[Search] をクリックします。

カスタム テーブルの検索ページが表示されます。

ヒント　さまざまな種類のイベントまたはデータをデータベースで検索するには、[Table] ドロップダウンリストから選択します。

ステップ 4　該当するフィールドに検索基準を入力します。検索基準を選択する方法の詳細については、テーブルの検索基準を参照してください。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。

ヒント　検索基準としてオブジェクトを使用する場合は、検索フィールドの横にあるオブジェクト アイコン（ ＋ ）をクリックします。特別な検索構文、検索でのオブジェクトの使用、検索の保存およびロードなど、検索の詳細については、検索設定の実行と保存（60-1 ページ）を参照してください。

ステップ 5　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　カスタム ユーザ ロールのデータの制限として検索を使用する場合は、**必ず**プライベート検索として保存する必要があります。

ステップ 6　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save As New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 7　検索を開始するには、[Search] ボタンをクリックします。

検索結果は、現在の時間範囲によって制限されている、カスタム テーブルのデフォルトのワークフローに表示されます（該当する場合）。別のワークフロー（カスタム ワークフローを含む）を使用するには、ワークフローのタイトルの横にある [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

イベントの検索

Ciscoのアプライアンスは、データベース テーブルにイベントとして保存される情報を生成します。イベントには、アプライアンスがイベントを生成する原因となったアクティビティを示すいくつかのフィールドが含まれます。

FireSIGHT システムに備わっている定義済みの検索設定をサンプルとして使用すると、ネットワークに関する重要な情報にすばやくアクセスできます。ネットワーク環境に合わせて定義済み検索設定のフィールドを変更し、検索設定を保存して、あとで再利用することができます。また、独自の検索条件を使用することもできます。

検索の種類に応じて、使用できる検索条件は異なりますが、メカニズムは同じです。検索の実行方法と、検索フィールドで使用する正しい構文の詳細ついては、以下の項を参照してください。

検索設定の実行と保存

ライセンス： すべて

任意のイベント タイプに関する検索設定を作成し、保存することができます。検索設定を作成するときには、その検索設定の名前を付け、それを自分だけで使用するか、それともアプライアンスの全ユーザが使用できるようにするかを指定します。カスタム ユーザ ロールに関するデータ制約として検索を使用する予定の場合は、それをプライベート検索として保存する**必要があります**。

詳細については、次の項を参照してください。

注　カスタム テーブルを検索する場合には、少し異なる手順に従います（カスタム テーブルの検索（59-9 ページ）を参照）。

検索の実行

ライセンス： すべて

いくつかのイベント タイプに関しては、FireSIGHT システムに備わっている定義済みの検索設定をサンプルとして使用すると、ネットワークについての重要な情報にすばやくアクセスできます。ネットワーク環境に合わせて定義済み検索設定のフィールドを変更し、検索設定を保存して、あとで再利用することができます。また、独自の検索条件を使用することもできます。

検索を実行する方法：

アクセス： Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　テーブルのドロップダウン リストから、検索するイベント タイプまたはデータを選択します。

適切な検索制約に従ってページが更新されます。

ステップ 3　該当するフィールドに検索条件を入力します。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「`A`」または「`B`」または「`C, D, E`」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク（*）を使用できます。
- 任意のフィールドで `n/a` を指定すると、そのフィールドの情報がないイベントを識別できます。一方、フィールドに情報があるイベントを識別すには `!n/a` を使用します。
- 検索条件としてオブジェクトを使用するには、検索フィールドの横にあるオブジェクト追加アイコン（ ＋ ）をクリックします。

ステップ 4　使用可能な検索条件の詳細については、次の項を参照してください。

- 監査レコードの検索（69-8 ページ）
- アプリケーションの検索（50-48 ページ）
- アプリケーションの詳細の検索（50-52 ページ）
- キャプチャ ファイルの検索（40-35 ページ）
- コンプライアンス ホワイト リスト イベントの検索（52-36 ページ）
- 接続およびセキュリティ インテリジェンスのデータの検索（39-34 ページ）
- 相関イベントの検索（51-59 ページ）
- ディスカバリ イベントの検索（50-18 ページ）
- ファイル イベントの検索（40-13 ページ）
- ヘルス イベントの検索（68-60 ページ）
- ホスト属性の検索（50-33 ページ）
- ホストの検索（50-27 ページ）
- 侵入イベントの検索（41-44 ページ）
- マルウェア イベントの検索（40-28 ページ）
- [Rule Update Import Log] の検索（66-28 ページ）
- 修復ステータス イベントの検索（54-22 ページ）
- スキャン結果の検索（47-25 ページ）
- サーバの検索（50-43 ページ）
- サードパーティの脆弱性の検索（50-62 ページ）
- ユーザの検索（50-68 ページ）
- ユーザ アクティビティの検索（50-74 ページ）
- 脆弱性の検索（50-58 ページ）
- ホワイト リスト違反の検索（52-41 ページ）

ステップ 5　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　カスタム ユーザ ロールに関するデータ制約として検索を使用する予定の場合は、それをプライベート検索として保存する**必要があります**。

ステップ 6　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。
- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save As New] をクリックします。

ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 7　検索を開始するには、[Search] ボタンをクリックします。

検索結果は、検索されるテーブルのデフォルト ワークフローで表示され、該当する場合には時間で制約されます。カスタム ワークフローなど別のワークフローを使用するには、ワークフロータイトルの近くの [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。スキャン結果には別のワークフローを使用**できない**ことに注意してください。

保存済み検索設定のロード

ライセンス： すべて

以前に検索設定を保存した場合、それをロードし、必要に応じて修正して、検索を開始することができます。

保存済みの検索設定をロードする方法：

アクセス： Admin/Any Security Analyst

ステップ 1　次の選択肢があります。

- ワークフローの任意のページから [Search] をクリックします。
- [Analysis] > [Search] を選択し、検索するイベント タイプを選択します。

[Search] ページが表示されます。

ステップ 2　[Custom Searches] リストまたは [Predefined Searches] リストから、ロードする検索を選択します。

保存済み検索の設定値が検索制約に入力されます。

ステップ 3　オプションで、検索制約を変更します。

ステップ 4　[Search] をクリックします。

検索制約に一致するイベントが表示されます。

保存済み検索設定の削除

ライセンス： すべて

保存済みの検索設定がある場合、[Search] ページからそれらを削除できます。

保存済み検索設定を削除する方法：

アクセス： Admin/Any Security Analyst

ステップ 1　次の選択肢があります。

- ワークフローの任意のページから [Search] をクリックします。
- [Analysis] > [Search] を選択し、削除する検索設定のイベント タイプを選択します。

[Search] ページが表示されます。

ステップ 2　[Custom Searches] リストから削除する検索を選択して、検索名の横に表示される削除アイコン（ ✖ ）をクリックします。

検索設定が削除されます。

検索でのワイルドカードと記号の使用

ライセンス： すべて

検索ページの多くのテキスト フィールドでは、文字列内の文字に一致させるためのアスタリスク（*）を使用できます。たとえば `net*` と指定すると、`network`、`netware`、`netscape` などに一致します。

英数字以外の文字（アスタリスク文字を含む）を検索するには、検索文字列を引用符で囲みます。たとえば、次の文字列を検索するには、

```
Find an asterisk (*)
```

次の行を入力します。

```
"Find an asterisk (*)"
```

ワイルドカードを使用できるテキスト フィールドで、部分的な文字列に一致させるには、ワイルドカードを使用する**必要**があることに注意してください。たとえば、ページ ビューを含む（つまりメッセージが「Page View」である）すべての監査レコードを監査ログ内で検索する場合、「`Page`」を検索しても結果は返されません。代わりに、「`Page*`」と指定してください。

検索でのオブジェクトとアプリケーション フィルタの使用

ライセンス： すべて

FireSIGHT システムでは、ネットワーク構成の一部として使用可能な名前付きオブジェクト、オブジェクト グループ、およびアプリケーション フィルタを作成できます。検索を実行または保存するときには、検索条件としてこれらのオブジェクト、グループ、およびフィルタを使用できます。

検索を実行するときに、オブジェクト、オブジェクト グループ、およびアプリケーション フィルタは `${object_name}` という形式で表示されます。たとえば、オブジェクト名 `ten_ten_network` であるネットワーク オブジェクトは、検索では `${ten_ten_network}` と表されます。

検索基準としてオブジェクトを使用できる検索フィールドの横にはオブジェクト追加アイコン（ ✚ ）が表示され、これをクリックすることができます。

検索での時間制約の指定

ライセンス： すべて

時間による検索制約を指定するには、いくつかの形式を使用できます。一致させる時間を入力し、オプションで、その時間の前後に一致させるために「より小さい」（`<`）または「より大きい」（`>`）演算子を入力できます。

時間値を持つ検索条件フィールドで使用可能な形式を、次の表に示します。

表 60-1　検索フィールドにおける時間指定

時間の形式	例
today [at HH:MMam|pm]	today today at 12:45pm
YYYY-MM-DD HH:MM:SS	2006-03-22 14:22:59

時間値の前に、以下のいずれか 1 つの演算子/キーワードを指定できます。

表 60-2　時間指定の演算子

Operator	例	説明
<	< 2006-03-22 14:22:59	2006 年 3 月 22 日午後 2:23 より前のタイムスタンプを持つイベントを返します。
>	> today at 2:45pm	今日の午後 2:45 より後のタイムスタンプを持つイベントを返します。

検索での IP アドレスの指定

ライセンス： すべて

検索で IP アドレスを指定するときには、個別の IP アドレス、複数アドレスのカンマ区切りリスト、アドレス ブロック、またはハイフン(-)で区切った IP アドレス範囲を入力することができます。また、否定を使用することもできます。

IPv6 をサポートする検索(侵入イベント、接続データ、相関イベントの検索など)では、IPv4 アドレス、IPv6 アドレス、および CIDR/プレフィクス長アドレス ブロックを任意に組み合わせて入力できます。

CIDR またはプレフィクス長の表記を使って IP アドレスのブロックを指定すると、FireSIGHT システムは、マスクまたはプレフィクス長で指定されたネットワーク IP アドレス部分**のみ**を使用します。たとえば 10.1.2.3/8 と入力すると、FireSIGHT システムは 10.0.0.0/8 を使用します。

次の表に、IP アドレスを入力する適切な方法を例示します。IP アドレスをネットワーク オブジェクトによって表すことができるため、IP アドレス検索フィールドの横にあるネットワーク オブジェクト追加アイコン(✚)をクリックして、ネットワーク オブジェクトを IP アドレス検索基準として使用することもできます。詳細については、検索でのオブジェクトとアプリケーション フィルタの使用(60-5 ページ)を参照してください。

表 60-3　使用可能な IP アドレス構文

指定する項目	入力内容	例
単一の IP アドレス	その IP アドレス	192.168.1.1 2001:db8::abcd
リストを使用した複数の IP アドレス	IP アドレスのカンマ区切りリスト。カンマの前後にスペースを追加**しない**でください。	192.168.1.1,192.168.1.2 2001:db8::b3ff,2001:db8::0202

表 60-3　使用可能な IP アドレス構文（続き）

指定する項目	入力内容	例
CIDR ブロックまたはプレフィクス長で指定できる IP アドレスの範囲	IPv4 CIDR または IPv6 プレフィクス長表記の IP アドレス ブロック。	`192.168.1.0/24` これは、サブネット マスク 255.255.255.0 である 192.168.1.0 ネットワーク内の任意の IP を指定します（つまり 192.168.1.0 から 192.168.1.255 まで）。詳細については、IP アドレスの表記規則（1-23 ページ）を参照してください。
CIDR ブロックやプレフィクスで指定できない IP アドレスの範囲	ハイフンを使用した IP アドレス範囲。ハイフンの前後にスペースを入力**しない**でください。	`192.168.1.1-192.168.1.5` `2001:db8::0202-2001:db8::8329`

他の方法で否定を使用して IP アドレスまたは IP アドレス範囲を指定	IP アドレス、ブロック、または範囲の先頭に感嘆符を付ける。	`192.168.0.0/32,!192.168.1.10`
		`!2001:db8::/32`
		`!192.168.1.10,!2001:db8::/32`

検索でのデバイスの指定

ライセンス： すべて

管理対象デバイスを制約として使用して検索を作成する場合、[Device] 検索条件フィールドに次のいずれかを指定できます。

- 管理対象デバイス名、IP アドレス、またはホスト名
- デバイス グループ名
- デバイス スタック名
- デバイス クラスタ名

システムでグループ、クラスタ、またはスタックの一致が検出されると、検索を実行するために、そのグループ名、クラスタ名、またはスタック名が適切なメンバー デバイス名に置き換えられます。デバイス フィールドのデバイス グループ、クラスタ、またはスタックを使用する検索を保存すると、デバイス フィールドで指定した名前がシステムによって保存され、検索が実行されるたびにデバイス名の置換が再度実行されます。

詳細については、次の項を参照してください。

- デバイスの操作（4-19 ページ）
- デバイス グループの管理（4-29 ページ）
- スタックに含まれるデバイスの管理（4-46 ページ）
- デバイスのクラスタリング（4-31 ページ）

検索でのポートの指定

ライセンス: すべて

FireSIGHT システムでは、ポート番号を表す特定の構文を検索で指定できます。次の入力が可能です。

- 単一のポート番号
- 複数のポート番号を含むカンマ区切りリスト
- 2 つのポート番号をハイフンで区切ることにより、ポート番号の範囲を表す
- 1 つのポート番号の後に、スラッシュで区切られたプロトコル省略形（侵入イベントを検索する場合のみ）
- 1 つのポート番号またはポート番号範囲の前に 1 つの感嘆符（指定されたポートの否定を表す）

注 ポート番号や範囲を指定するときには、スペースを使用**しない**でください。

次の表に、検索制約としてポートを入力する適切な方法を例示します。

\

表 60-4　ポートの構文例

例	説明
`21`	ポート 21 でのすべてのイベントを返します（TCP および UDP イベントを含む）。
`!23`	ポート 23 上のイベントを除くすべてのイベントを返します。
`25/tcp`	ポート 25 でのすべての TCP 関連の侵入イベントを返します。
`21/tcp,25/tcp`	ポート 21 および 25 でのすべての TCP 関連の侵入イベントを返します。
`21 ～ 25`	ポート 21 から 25 までのすべてのイベントを返します。

実行時間が長いクエリの停止

ライセンス: すべて

サポートされるデバイス: すべてDefense Center

システム管理者は、シェル ベースのクエリ管理ツールを使用して、実行時間の長いクエリを検出および停止することができます。

注 Web インターフェイス内の検索ページを終了しても、クエリは停止しません。長い時間をかけて結果を返すクエリは、クエリ実行中にシステム全体のパフォーマンスに影響を与えます。

クエリ管理ツールでは、指定した分数より長く実行されているクエリを検出し、それらのクエリを停止することができます。クエリを停止すると、このツールによって監査ログと syslog にイベントが記録されます。

Defense Centerでのシェル アクセスを持つローカル作成されたユーザだけが、admin ユーザであることに注意してください。シェル アクセスを与える外部認証オブジェクトを使用する場合、シェル アクセス フィルタに一致するユーザもまたシェルにログインできます。

使用方法:

```
query_manager [-v] [-l [minutes]] [-k query_id [...]]
[--kill-all minutes]
```

オプション:

`-h, --help`
短いヘルプ メッセージを出力します。

`-l, --list [minutes]`
指定された時間(分単位)を超えるすべてのクエリをリストします。デフォルトでは、1 分より長くかかっているすべてのクエリーを表示します。

`-k, --kill query_id [...]`
指定した ID でクエリを強制終了します。オプションには、複数の ID を指定できます。

`--kill-all minutes`
指定された時間(分単位)より長くかかっているすべてのクエリを強制終了します。

`-v, --verbose`
完全な SQL クエリを含む詳細な出力。

注意　シェル アクセスを、システム管理者のみに制限する必要があります。

Defense Centerでクエリを停止する方法:

アクセス: admin またはシェル アクセスが付与されたユーザ

ステップ 1　ssh を使用してDefense Centerに接続します。

ステップ 2　前述の構文を使用して、sudo で query_manager を実行します。

ユーザの管理

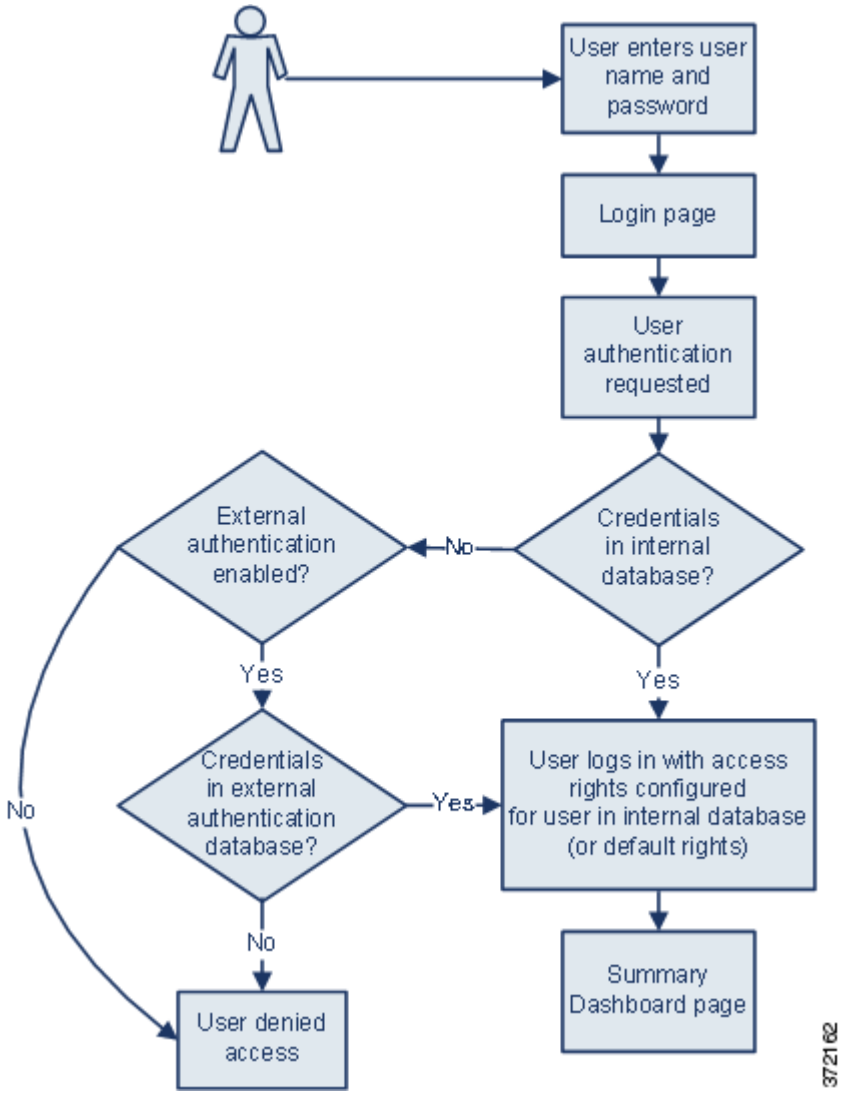
ユーザ アカウントに Administrator アクセスが付与されている場合、Defense Centerまたは管理対象デバイスの Web インターフェイスにアクセス可能なユーザ アカウントを管理できます。Defense Centerでは、内部データベースではなく、外部認証サーバを使用したユーザ認証をセットアップすることもできます。

詳細については、次の項を参照してください。

Ciscoユーザ認証について

ライセンス：すべて

ユーザが Web インターフェイスにログインすると、アプライアンスがローカルのユーザ リストでユーザ名とパスワードに一致するものを検索します。このプロセスは*認証*と呼ばれます。認証には、内部認証と外部認証の 2 種類があります。ユーザ アカウントで内部*認証*が使用される場合、認証プロセスはローカル データベースでこのリストを確認します。アカウントで*外部認証*が使用される場合、プロセスはローカル データベースにユーザが存在するかどうかを調べ、ユーザがローカル データベースに存在しない場合は外部サーバ（Lightweight Directory Access Protocol（LDAP）ディレクトリ サーバ、Remote Authentication Dial In User Service（RADIUS）認証サーバなど）に対してユーザ リストを照会します。



内部認証または外部認証を使用するユーザの場合、ユーザのアクセス許可を制御できます。外部認証を使用するユーザには、ユーザのアクセス許可を手動で変更していない限り、ユーザが属するグループまたはアクセス リストの権限、またはサーバ認証オブジェクトあるいは管理元の Defense Centerのシステム ポリシーで設定したデフォルト ユーザ アクセス ロールに基づくアクセス許可が付与されます。

詳細については、次の項を参照してください。

- 内部認証について（61-3 ページ）
- 外部認証について（61-3 ページ）
- ユーザ特権について（61-4 ページ）

内部認証について

ライセンス: すべて

デフォルトでは、FireSIGHT システム が内部認証を使用してユーザのログイン時のユーザ資格情報を確認します。内部認証は、ユーザ名とパスワードが内部 FireSIGHT システム データベースのレコードと照合されるときに発生します。ユーザの作成時に外部認証を有効にしないと、ユーザ資格情報は内部データベースで管理されます。

各内部認証ユーザは手動で作成されるため、ユーザを作成するときにアクセス権を設定します。デフォルト設定は必要ありません。

注 外部認証を有効にした場合に、内部認証ユーザと同一のユーザ名が外部サーバに存在し、外部サーバでそのユーザに対して保存されているパスワードを使用してユーザがログインすると、内部認証ユーザが外部認証に変換されることに注意してください。内部認証ユーザを外部認証ユーザに変換した後で、内部認証に戻すことはできません。

外部認証について

ライセンス: すべて

外部認証は、Defense Centerまたは管理対象デバイスが LDAP ディレクトリ サーバまたは RADIUS 認証サーバなどの外部リポジトリからユーザ資格情報を取得するときに発生します。外部認証のタイプには、LDAP 認証と RADIUS 認証があります。アプライアンスに対して使用できる外部認証形式は 1 つだけであることに注意してください。

外部認証を使用する場合、ユーザ情報を要求する外部認証サーバごとに、*認証オブジェクト*を設定する必要があります。認証オブジェクトには、そのサーバに接続してユーザ データを取得するための設定が含まれています。管理元のDefense Centerのシステム ポリシーでそのオブジェクトを有効にし、そのポリシーをアプライアンスに適用して認証を有効にすることができます。外部認証ユーザがログインすると、Web インターフェイスは、システム ポリシーにリストされている順序で各認証サーバを調べ、そのユーザがリストされているかどうかを確認します。

ユーザの作成時に、そのユーザに対し内部認証または外部認証のいずれが実行されるかを指定できます。

注 シリーズ 3 管理対象デバイスで外部認証を有効にする前に、シェル アクセス フィルタに含まれている外部認証ユーザと同じユーザ名を持つ内部認証シェル ユーザをすべて削除してください。

管理対象デバイスで外部認証を有効にするために、そのデバイスにシステム ポリシーをプッシュできますが、デバイスの Web インターフェイスから認証オブジェクトを制御することはできません。新規ユーザに対して外部認証を選択すると、デバイスでは外部認証の設定だけが行われます。管理対象デバイスで外部認証を無効にする場合は、管理元のDefense Centerのシステム ポリシーで外部認証を無効にし、デバイスにポリシーを再適用します。また、デバイス自体に(管理対象デバイスで作成された)ローカル システム ポリシーを適用すると、外部認証も無効になります。

ヒント システム ポリシーをエクスポートするには、インポート/エクスポート機能を使用できます。外部認証が有効になっているポリシーをエクスポートすると、認証オブジェクトがそのポリシーとともにエクスポートされます。その後、別のDefense Centerにそのポリシーとオブジェクトをインポートできます。ポリシーと認証オブジェクトを管理対象デバイスにインポート**しないでください**。

各種外部認証の詳細については、次の項を参照してください。

- LDAP 認証（61-5 ページ）
- RADIUS 認証（61-34 ページ）

ユーザ特権について

ライセンス： すべて

FireSIGHT システムでは、ユーザのロールに基づいてユーザ特権を割り当てることができます。たとえばアナリストは通常、監視対象ネットワークのセキュリティを分析するためイベント データへのアクセスが必要ですが、FireSIGHT システム自体の管理機能へのアクセス権は必要としません。アナリストに対し、Security Analyst や Discovery Admin などの事前定義ロールを付与し、FireSIGHT システムを管理するネットワーク管理者に対し Administrator ロールを予約することができます。また、組織のニーズに合わせて調整されたアクセス権限を含むカスタム ユーザ ロールを作成できます。

Defense Centerのシステム ポリシーでは、外部認証されるすべてのユーザのデフォルト アクセス ロールを設定します。外部認証ユーザの初回ログイン後に、[User Management] ページで、そのユーザのアクセス権を追加または削除できます。ユーザの権限を変更しない場合、そのユーザにはデフォルトで付与される権限のみが設定されます。内部認証ユーザは手動で作成されるため、内部認証ユーザの作成時にアクセス権を設定します。

LDAP グループを使用したアクセス権の管理を設定した場合、ユーザのアクセス権は LDAP グループ メンバーシップに基づいています。属しているグループの中で最も高いレベルのアクセスを持つグループのデフォルト アクセス権が付与されます。ユーザがどのグループにも属していない場合にグループ アクセスを設定した場合、ユーザには、LDAP サーバの認証オブジェクトで設定されているデフォルト ユーザ アクセス権が付与されます。グループ アクセスを設定すると、それらの設定によってシステム ポリシーのデフォルト アクセス設定がオーバーライドされます。

同様に、RADIUS 認証オブジェクトの特定のユーザ ロール リストにユーザを割り当てると、1 つ以上のロールが相互に矛盾しない限り、割り当てられたすべてのロールがそのユーザに付与されます。2 つの相互に矛盾するロールのリストにユーザが含まれている場合、最も高いレベルのアクセスを持つロールが付与されます。ユーザがどのリストにも属しておらず、認証オブジェクトでデフォルト アクセス ロールを設定している場合、ユーザにはそのデフォルト アクセス ロールが付与されます。認証オブジェクトでデフォルト アクセスを設定すると、それらの設定によってシステム ポリシーのデフォルト アクセス設定がオーバーライドされます。

FireSIGHT システムでは、ライセンスされている機能に応じて、次に示す事前定義ユーザ ロールがサポートされています。これらのロールは、優先度順にリストされています。

- *Access Admin* はアクセス制御ポリシーとファイル ポリシーを表示、変更できますが、ポリシーの変更を適用することはできません。
- *Administrator* は、アプライアンスのネットワーク設定をセットアップし、ユーザ アカウントおよびCollective Security Intelligence クラウド接続を管理し、システム ポリシーとシステム設定を設定できます。Administrator ロールが割り当てられているユーザは、その他のすべてのロールのすべての権限と特権を持ちます（ただしこれらの特権の制限付きの低いバージョンは除きます）。
- *Discovery Admin* は、ネットワーク検出ポリシーを確認、変更、削除できますが、ポリシー変更を適用することはできません。
- *External Database* ユーザは、JDBC SSL 接続をサポートする外部アプリケーションを使用して FireSIGHT システム データベースに対してクエリを実行できます。Web インターフェイスでは、オンライン ヘルプとユーザ設定にアクセスできます。

- *Intrusion Admins* は、すべての侵入ポリシー、侵入ルール、およびネットワーク解析ポリシーの機能にアクセスできます。Intrusion Admin は、[Policies] メニューの侵入関連オプションにアクセスできます。Intrusion Admin は、侵入またはネットワーク解析ポリシーをアクセス制御ポリシーの一部として適用できないことに注意してください。
- *Maintenance User* は、監視機能（ヘルス モニタ、ホスト統計、パフォーマンス データ、システム ログなど）と保守機能（タスク スケジューリング、システムのバックアップなど）にアクセスできます。

  Maintenance User は、[Policies] メニューの機能にはアクセスできず、[Analysis] メニューからダッシュボードへのアクセスだけが可能であることに注意してください。
- *Network Admin* は、デバイス設定を確認、変更、適用し、アクセス制御ポリシーを確認、変更できます。
- *Security Approver* は、設定およびポリシーの変更を確認、適用できますが、作成することはできません。
- *Security Analyst* は、侵入、ディスカバリ、ユーザ アクティビティ、接続、相関、およびネットワーク変更の各イベントを確認、分析、削除できます。ホスト、ホスト属性、サービス、脆弱性、およびクライアント アプリケーションの確認、分析、および（該当する場合は）削除を行うことができます。Security Analyst は、レポートを生成し、ヘルス イベントを確認することもできます（ただしヘルス イベントの削除と変更はできません）。
- *Security Analysts (読み取り専用)* には、Security Analyst と同じ権限が含まれていますが、イベントの削除はできません。

前述の事前定義ロールの他に、特別なアクセス権限を含むカスタム ユーザ ロールを設定できます。どのロールでも、外部認証ユーザのデフォルト アクセス ロールとして設定できます。

外部認証ユーザ アカウントにユーザ ロール エスカレーション特権を付与できます。また、外部認証ユーザのパスワードをエスカレーション パスワードとして使用できます。詳細については、ユーザ ロール エスカレーションの管理（61-69 ページ）を参照してください。

認証オブジェクトの管理

ライセンス： すべて

認証オブジェクトは、外部認証サーバのサーバ プロファイルであり、これらのサーバの接続設定と認証フィルタ設定が含まれています。Defense Centerで認証オブジェクトを作成、設定、削除し、また認証オブジェクトを使用して LDAP または RADIUS サーバへの外部認証を管理することができます。詳細については、次の各項を参照してください。

- LDAP 認証（61-5 ページ）
- RADIUS 認証（61-34 ページ）
- 認証オブジェクトの削除（61-45 ページ）

LDAP 認証

ライセンス： すべて

LDAP（Lightweight Directory Access Protocol）により、ユーザ資格情報などのオブジェクトをまとめるためのディレクトリをネットワーク上の一元化されたロケーションにセットアップできます。その後複数のアプリケーションが、これらの資格情報と、資格情報の記述に使用される情報にアクセスできます。ユーザの資格情報を変更する必要がある場合は、1 か所で変更でき、FireSIGHT システム アプライアンスごとに資格情報を変更する必要はありません。

詳細については、次の項を参照してください。

- LDAP 認証について（61-6 ページ）
- CAC を使用した LDAP 認証について（61-10 ページ）
- LDAP 認証オブジェクトの作成の準備（61-12 ページ）
- 基本 LDAP 認証オブジェクトの作成（61-13 ページ）
- 拡張 LDAP 認証オブジェクトの作成（61-17 ページ）
- LDAP 認証オブジェクトの例（61-28 ページ）
- LDAP 認証オブジェクトの編集（61-33 ページ）

LDAP 認証について

ライセンス： すべて

LDAP 認証オブジェクトはDefense Centerで作成できますが、ほかの FireSIGHT システム アプライアンスでは作成できません。ただし、オブジェクトが有効に設定されているシステム ポリシーをアプライアンスに適用することで、アプライアンスで外部認証オブジェクトを使用できます（仮想デバイスまたは Cisco NGIPS for Blue Coat X-Series を除く）。ポリシーを適用すると、オブジェクトがアプライアンスにコピーされます。

注　シリーズ 3 管理対象デバイスで外部認証を有効にする前に、シェル アクセス フィルタに含まれている外部認証ユーザと同じユーザ名を持つ内部認証シェル ユーザをすべて削除してください。

LDAP 命名標準は、アドレスの指定と、認証オブジェクトのフィルタおよび属性の構文に使用できることに注意してください。詳細については、『Lightweight Directory Access Protocol (v3): Technical Specification』（RFC 3377）に記載されている RFC を参照してください。この手順では構文の例が示されています。Microsoft Active Directory Server へ接続するための認証オブジェクトをセットアップするときに、ドメインを含むユーザ名を参照する場合には、Internet RFC 822（Standard for the Format of ARPA Internet Text Messages）仕様に記載されているアドレス指定構文を使用できることに注意してください。たとえばユーザ オブジェクトを参照する場合は、`JoeSmith@security.example.com` と入力し、Microsoft Active Directory Sever を使用する場合の同等のユーザ識別名 `cn=JoeSmith,ou=security, dc=example,dc=com` は使用しません。

注　現在 FireSIGHT システムでは、Microsoft Active Directory on Windows Server 2003 および Windows Server 2008、Windows Server 2003 および Windows Server 2008 上の Oracle Directory Server Enterprise Edition 7.0、または OpenLDAP on Linux が稼働する LDAP サーバでの LDAP 外部認証がサポートされています。ただし、FireSIGHT システムは、仮想デバイスまたは Cisco NGIPS for Blue Coat X-Series の外部認証はサポートしていません。

詳細については、次の項を参照してください。

- デフォルトについて（61-7 ページ）
- ベース DN について（61-7 ページ）
- 基本フィルタについて（61-7 ページ）
- 偽装アカウントについて（61-7 ページ）
- LDAP 接続について（61-7 ページ）
- ユーザ名テンプレートについて（61-8 ページ）

デフォルトについて

ライセンス： すべて

ユーザが接続する予定のサーバのタイプに基づいて、各種フィールドにデフォルト値を移入できます。サーバのタイプを選択してデフォルトを設定すると、[User Name Template]、[UI Access Attribute]、[Shell Access Attribute]、[Group Member Attribute]、[Group Member URL Attribute] の各フィールドにデフォルト値が取り込まれます。

ベース DN について

ライセンス： すべて

ローカル アプライアンスが認証サーバのユーザ情報を取得するため LDAP サーバを検索するときには、検索起点が必要となります。ローカル アプライアンスにより検索されるツリーを指定するには、ベース識別名（*ベース DN*）を指定します。

通常、ベース DN には、企業ドメインおよび部門を示す基本構造があります。たとえば、Example 社のセキュリティ（Security）部門のベース DN は、`ou=security,dc=example,dc=com` となります。

プライマリ サーバの指定後に、使用可能なベース DN のリストをプライマリ サーバから自動的に取得し、適切なベース DN を選択できます。

基本フィルタについて

ライセンス： すべて

特定の属性に特定の値を設定する*基本フィルタ*を追加できます（囲み用のカッコを含めて最大 450 文字）。基本フィルタでは、ベース DN でフィルタに設定されている属性値を含むオブジェクトだけを取得することで、検索を絞り込みます。基本フィルタはカッコで囲みます。たとえば、F で始まる一般名を持つユーザのみをフィルタで検出するには、フィルタ `(cn=F*)` を使用します。

テスト ユーザ名とパスワードを入力して基本フィルタをより具体的にテストするにはユーザ認証のテスト（61-40 ページ）を参照してください。

偽装アカウントについて

ライセンス： すべて

ローカル アプライアンスがユーザ オブジェクトにアクセスできるようにするには、偽装アカウントのユーザ資格情報を指定する必要があります。*偽装アカウント*とは、ベース DN によって指定されるディレクトリを参照し、必要なユーザ オブジェクトを取得するための適切な権限が付与されているユーザ アカウントです。指定するユーザの識別名は、サーバのツリーで一意である必要があることに注意してください。

LDAP 接続について

ライセンス： すべて

LDAP 接続の暗号化方式を管理できます。暗号化なし、Transport Layer Security（TLS）、または Secure Sockets Layer（SSL）暗号化を選択できます。

TLS または SSL 経由での接続時に認証に証明書を使用する場合、証明書の LDAP サーバ名が、[Host Name/IP Address] フィールドで使用する名前と一致している**必要がある**ことに注意してください。たとえば、外部認証設定に `10.10.10.250` と入力し、証明書に `computer1.example.com` と入力すると、接続は失敗します。外部認証設定のサーバ名を `computer1.example.com` に変更すると、接続が正常に行われます。

ユーザ名テンプレートについて

ライセンス： すべて

ユーザ名テンプレートを選択する場合、文字列変換文字（`%s`）をユーザの UI アクセス属性またはシェル アクセス属性の値にマッピングすることで、ログイン時に入力されるユーザ名の形式を指定できます。ユーザ名テンプレートは、認証に使用する識別名の形式です。ユーザがログイン ページにユーザ名を入力すると、文字列変換文字が名前に置き換えられ、その結果生成される識別名がユーザ資格情報の検索に使用されます。

たとえば、Example 社のセキュリティ（Security）部門のユーザ名テンプレートを設定するには、`%s@security.example.com` と入力します。CAC 認証および認可にオブジェクトを使用するには、UI アクセス属性値に対応するユーザ名テンプレートの値を入力する**必要があります**。詳細については、CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。

接続タイムアウトについて

ライセンス： すべて

バックアップ認証サーバを指定する場合は、プライマリ サーバへの接続試行操作のタイムアウトを設定できます。プライマリ認証サーバから応答がない状態でタイムアウト期間が経過すると、アプライアンスはバックアップ サーバに対してクエリを実行します。たとえば、プライマリ サーバで LDAP が無効な場合、アプライアンスはバックアップ サーバに対してクエリを実行します。

ただし LDAP がプライマリ LDAP サーバのポートで実行されており、何らかの理由（誤った設定またはその他の問題など）で要求の処理を拒否する場合は、バックアップ サーバへのフェールオーバーは行われません。

属性を使用したアクセスの管理

ライセンス： すべて

LDAP サーバのタイプによって、ユーザ データの保管に使用される属性が異なります。UI およびシェル アクセス属性の詳細については、次の項を参照してください。

UI アクセス属性

LDAP サーバが UI アクセス属性 `uid` を使用する場合、ローカル アプライアンスは、設定されたベース DN が示すツリー内の各オブジェクトで `uid` 属性値を調べます。特定の UI アクセス属性を設定しない場合、ローカル アプライアンスは、LDAP サーバの各ユーザ レコードの識別名を調べ、ユーザ名に一致しているかどうかを確認します。いずれかのオブジェクトに一致するユーザ名とパスワードがある場合は、ユーザ ログイン要求が認証されます。

異なる LDAP 属性を使用して、ローカル アプライアンスが、識別名の値ではなく LDAP 属性に対してユーザ名を照合するようにできます。サーバ タイプを選択し、デフォルトを設定すると、そのサーバ タイプに適した UI アクセス属性に値が取り込まれます。いずれかのオブジェクトに、指定した属性の値として一致するユーザ名と、（CAC 以外のオブジェクトの場合に）パスワードあると、ユーザ ログイン要求が認証されます。FireSIGHT システム Web インターフェイスの有効なユーザ名が値として設定されている属性であれば、どの属性でも使用できます。有効なユーザ名は一意のユーザ名であり、アンダースコア（_）、ピリオド（.）、ハイフン（-）、英数字を使用でき

ます。CAC 認証および認可にオブジェクトを使用するには、ユーザ名テンプレートの値に対応する UI アクセス属性の値を入力する**必要があります**。詳細については、CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。

シェル アクセス属性

シェル アクセス属性として LDAP サーバが `uid` を使用する場合、ローカル アプライアンスはログイン時に入力されたユーザ名を、`uid` の属性値と照合して調べます。また、`uid` 以外のカスタム シェル アクセス属性も設定できます。

サーバ タイプを選択し、デフォルトを設定すると、そのサーバ タイプに適したシェル アクセス属性に値が取り込まれることに注意してください。シェル アクセスの有効なユーザ名が値として設定されている属性であれば、どの属性でも使用できます。有効なユーザ名は一意のユーザ名であり、アンダースコア（_）、ピリオド（.）、ハイフン（-）、英数字を使用できます。

グループ メンバーシップを使用したアクセスの管理

ライセンス： すべて

LDAP グループのユーザのメンバーシップに基づいてデフォルト アクセス権を設定する場合は、FireSIGHT システムにより使用される各アクセス ロールに、LDAP サーバの既存のグループの識別名を指定できます。これを行うと、LDAP によって検出された、指定のどのグループにも属さないユーザのデフォルト アクセス設定を設定できます。ユーザがログインすると、FireSIGHT システムは LDAP サーバを動的に検査し、ユーザの現在のグループ メンバーシップに基づいてアクセス権を割り当てます。

LDAP サーバによって認証されたユーザは、ローカル FireSIGHT システム アプライアンスに初めてログインすると、ユーザが属するグループのアクセス権を受け取ります。グループが設定されていない場合は、システム ポリシーで選択されているデフォルト アクセス設定を受け取ります。

その後、これらの設定がグループ メンバーシップを介して付与されていない場合には、設定を変更できます。

シェル アクセスについて

ライセンス： すべて

LDAP サーバを使用して、管理対象デバイスまたはDefense Centerでシェル アクセス用のアカウントを認証できます。シェル アクセスを付与するユーザの項目を取得する検索フィルタを指定します。シェル アクセスは、システム ポリシーの最初の認証オブジェクトでのみ設定できることに注意してください。認証オブジェクトの順序の管理については、外部認証の有効化（63-12 ページ）を参照してください。

admin アカウントを除き、シェル アクセスは設定したシェル アクセス属性によって完全に制御されます。シェル ユーザはアプライアンスのローカル ユーザとして設定されます。ここで設定するフィルタにより、シェルにログインできる LDAP サーバのユーザが決定されます。

ログイン時に各シェル ユーザのホーム ディレクトリが作成されること、および(LDAP 接続を無効にすることで)LDAP シェル アクセス ユーザ アカウントが無効になっている場合はディレクトリが維持されますが、ユーザ シェルは `/etc/password` 内の `/bin/false` に設定され、シェルが無効になることに注意してください。ユーザが再度有効になると、同じホーム ディレクトリを使用してシェルがリセットされます。

ベース DN で限定されるすべてのユーザがシェル アクセス権限でも限定される場合は、[Same as Base Filter] を選択してシェル アクセス フィルタを設定することで、より効率的に検索できます。通常、ユーザを取得する LDAP クエリは、基本フィルタとシェル アクセス フィルタを組み合わせます。同じシェル アクセス フィルタを基本フィルタとして入力すると、同じクエリが 2 回実行されることになり、不必要に時間を消費することになります。

シェル ユーザは、小文字で構成されたユーザ名を使用してログインすることができます。シェルのログイン認証では、大文字と小文字が区別されます。

注意　シリーズ 3 Defense Centerでは、すべてのシェル ユーザに `sudoers` 特権が付与されます。シェル アクセスが付与されるユーザのリストを適切に制限してください。シリーズ 3 と仮想デバイスでは、外部認証ユーザに付与されるシェル アクセスのデフォルトは、**Configuration** レベルのコマンド ライン アクセスになります。このアクセスでも `sudoers` 特権が付与されます。

CAC を使用した LDAP 認証について

ライセンス： すべて

組織で Common Access Card（CAC）が使用される場合は、Web インターフェイスにログインするユーザを認証し、グループ メンバーシップまたはデフォルト アクセス権に基づいて特定機能へのアクセスを許可するように、LDAP 認証を設定できます。CAC 認証および認可が設定されている場合、ユーザは、アプライアンスに個別のユーザ名とパスワードを指定せずに直接ログインすることができます。

注　CAC 設定プロセスの一部としてユーザ証明書を有効にするには、ブラウザに有効なユーザ証明書（この場合は CAC を介してユーザのブラウザに渡されるサーバ証明書）が存在している**必要があります**。CAC 認証および認可の設定後に、ネットワーク上のユーザはブラウズ セッション期間にわたって CAC 接続を維持する**必要があります**。セッション中に CAC を削除または交換すると、Web ブラウザでセッションが終了し、システムにより Web インターフェイスから強制的にログアウトされます。

CAC 認証および認可を設定および管理する方法の詳細については、次の項を参照してください。

- CAC 認証および許可の設定（61-10 ページ）
- CAC 認証および認可の管理（61-12 ページ）

CAC 認証および許可の設定

ライセンス： すべて

サポートされるデバイス： 仮想または X-Series を除くすべて

サポートされる防御センター： 仮想または X-Series を除くすべて

ネットワークのユーザが各自の CAC 資格情報を使用してログインする前に、適切なアクセス許可を持つユーザが、CAC 認証および認可のマルチステップ設定プロセスを完了しておく必要があります。

CAC 認証および認可を設定して有効にするには、次の手順を実行します。

アクセス： Admin/Network Admin

ステップ 1　組織の指示に従い CAC を挿入します。

ステップ 2　ブラウザで `https://hostname/` を開きます（*hostname* はご使用のDefense Centerのホスト名に対応しています）。

ステップ 3　プロンプトが表示されたら、ステップ 1 で挿入した CAC に関連付けられている PIN を入力します。

PIN が受け入れられます。

ステップ 4　プロンプトが表示されたら、ドロップダウン リストから該当する証明書を選択します。

ブラウザが選択内容を受け入れ、[Login] ページが表示されます。

ステップ 5　[Username] フィールドと [Password] フィールドに、Administrator 特権を持つユーザとしてログインします。ユーザ名では、大文字と小文字が区別されます。

ヒント　CAC 認証および認可の設定が完了するまで、CAC 証明書を使用したログインは**できません**。

デフォルトの開始ページが表示されます。

ステップ 6　[System] > [Local] > [User Management] に移動し、[External Authentication] タブをクリックします。LDAP 認証オブジェクトの作成の準備（61-12 ページ）および拡張 LDAP 認証オブジェクトの作成（61-17 ページ）で説明する手順に従い、CAC 認証および認可専用の LDAP 認証オブジェクトを作成します。次の設定を行う必要があります。

- [LDAP-Specific Parameters] セクションの詳細設定オプションの [User Name Template]。詳細については、ユーザ名テンプレートについて（61-8 ページ）を参照してください。
- [Attribute Mapping] セクションの [UI Access Attribute]。詳細については、属性を使用したアクセスの管理（61-8 ページ）を参照してください。
- [Group Controlled Access Roles] セクションの既存の LDAP グループの識別名（LDP グループ メンバーシップによってアクセス権を事前に設定する場合）。詳細については、グループ メンバーシップを使用したアクセスの管理（61-9 ページ）を参照してください。

ヒント　同一認証オブジェクトで CAC 認証とシェル アクセスの両方を設定**できない**ことに注意してください。シェル アクセスのユーザを認証する場合は、別の認証オブジェクトを作成し、システム ポリシーで個別に有効にします。

ステップ 7　[Save] をクリックします。

[External Authentication] ページが表示され、このページに新しいオブジェクトが示されます。

ステップ 8　[System] > [Local] > [System Policy] に移動します。外部認証の有効化（63-12 ページ）の手順に従って外部認証を有効にし、続いてシステム ポリシーで CAC 認証を有効にします。

注意　変更は、システム ポリシーをDefense Centerとその管理対象デバイスに適用するまでは反映**されません**。詳細については、「システム ポリシーの適用（63-4 ページ）」を参照してください。

ステップ 9　[System] > [Local] > [Configuration] に移動し、[HTTPS Certificate] をクリックします。HTTPS サーバ証明書をインポートし、必要に応じてサーバ証明書のアップロード（64-5 ページ）で説明する手順に従います。

注　認証および認可に使用する予定の CAC で、HTTPS サーバ証明書とユーザ証明書が同じ認証局（CA）により発行される**必要があります**。

[Current HTTPS Certificate Page] が更新され、新しい証明書が反映されます。

ステップ 10　[HTTPS User Certificate Settings] の [Enable User Certificates] を選択します。詳細については、ユーザ証明書の要求（64-6 ページ）を参照してください。

ステップ 11　オプションで、ユーザが初めてログインした後で [System] > [Local] > [User Management] に移動し、そのユーザのアクセス権を手動で追加または削除します。ユーザの権限を変更しない場合、そのユーザにはデフォルトで付与される権限のみが設定されます。詳細については、ユーザ特権について（61-4 ページ）およびユーザ特権とオプションの変更（61-58 ページ）を参照してください。

CAC ユーザの初回ログイン後の CAC ユーザのロールの変更の詳細については、CAC 認証および認可の管理（61-12 ページ）を参照してください。

CAC 認証および認可の管理

CAC 認証および認可を設定して有効にすると、ネットワークのユーザは各自の CAC 資格情報を使用してアプライアンスの Web インターフェイスにログインできます。詳細については、アプライアンスへのログイン（2-1 ページ）を参照してください。

システムでは、CAC 認証ユーザは Electronic Data Interchange Personal Identifier（EDIPI）番号により識別されます。ユーザが CAC 資格情報を使用して初めてログインした後で、[User Management] ページでのこれらのユーザのアクセス権限を手動で追加または削除できます。グループ制御アクセス ロールを使用してユーザの権限を事前に設定していない場合、ユーザには、システム ポリシーでデフォルトで付与される権限だけが与えられています。詳細については、ユーザ特権について（61-4 ページ）、グループ メンバーシップを使用したアクセスの管理（61-9 ページ）、ユーザ特権とオプションの変更（61-58 ページ）を参照してください。

操作が行われない状態で 24 時間が経過すると、システムによって [User Management] ページから CAC 認証ユーザを消去されるときに、手動で設定されたアクセス権限が削除されることに注意してください。その後ユーザがログインするたびに、ユーザがページに復元されますが、ユーザのアクセス権限に対する手動での変更はすべて再設定する必要があります。

LDAP 認証オブジェクトの作成の準備

ライセンス： すべて

LDAP サーバへの接続を設定する前に、LDAP 認証オブジェクトの作成に必要な情報を収集する必要があります。設定の特定の側面については、LDAP 認証について（61-6 ページ）を参照してください。

すべての認証オブジェクトに必要な情報は次のとおりです。

- 接続するサーバのサーバ名または IP アドレス
- 接続するサーバのサーバ タイプ
- LDAP ツリーを参照するための十分な権限が付与されているユーザ アカウントのユーザ名とパスワード
- アプライアンスと LDAP サーバの間にファイアウォールがある場合、発信接続を許可するファイアウォールの項目
- ユーザ名が存在するサーバ ディレクトリのベース識別名（可能な場合）

サードパーティの LDAP クライアントを使用して、LDAP ツリーを参照し、ベース DN と属性の説明を確認できることに注意してください。またそのクライアントを使用して、選択したユーザが、選択した DN を参照できることを確認することもできます。LDAP 管理者に連絡し、ご使用の LDAP サーバ向けの推奨される認定 LDAP クライアントを確認してください。

LDAP 認証オブジェクト設定をどのようにカスタマイズするかによって、次の表に示す情報が必要となることがあります。

表 61-1　追加の LDAP 設定情報

目的	必要な情報
389 以外のポートを介した接続	ポート番号
暗号化接続を使用した接続	接続の証明書
属性値に基づいてアプライアンスにアクセスできるユーザをフィルタにより絞り込む	フィルタの条件となる属性と値のペア
ユーザ識別名を検査するのではなく、特定の属性を UI アクセス属性として使用する	属性の名前
ユーザ識別名を検査するのではなく、特定の属性をシェル ログイン属性として使用する	属性の名前
属性値に基づいてシェルを介してアプライアンスにアクセスできるユーザをフィルタにより絞り込む	フィルタの条件となる属性と値のペア
特定のユーザ ロールへのグループの関連付け	各グループの識別名、およびグループがスタティック グループの場合はグループ メンバー属性、グループがダイナミック グループの場合はグループ メンバーの URL 属性
認証および認可での CAC の使用	CAC、CAC を発行した CA により署名されたサーバ証明書、および両方の証明書の証明書チェーン

基本 LDAP 認証オブジェクトの作成

ライセンス: すべて

LDAP 認証オブジェクトをセットアップできます。LDAP 認証オブジェクトでは多くの値をカスタマイズします。ただし、特定ディレクトリ内のすべてのユーザを認証するだけの場合は、そのディレクトリのベース DN を使用して基本認証オブジェクトを作成できます。ご使用のサーバ タイプでベース DN のデフォルトを設定し、サーバからユーザ データを取得するために使用するアカウントの認証資格情報を指定すれば、認証オブジェクトを簡単に作成できます。このためには、次の手順に従います。

注　(CAC 認証および認可の設定などのために)認証オブジェクトを作成するときに、各認証設定を検討してカスタマイズする場合は、拡張 LDAP 認証オブジェクトの作成(61-17 ページ)の手順に従ってオブジェクトを作成します。サーバへの接続の暗号化、ユーザ タイムアウトの設定、ユーザ名テンプレートのカスタマイズ、または LDAP グループ メンバーシップに基づく FireSIGHT システム ユーザ ロールの割り当てを行う場合にも、この高度な手順を使用してください。

LDAP サーバへの接続を設定する前に、LDAP 認証オブジェクトの作成に必要な情報を収集する必要があります。設定の特定の側面については、LDAP 認証について(61-6 ページ)を参照してください。

基本認証オブジェクトを作成するには、次の情報が必要です。

- 接続するサーバのサーバ名または IP アドレス
- 接続するサーバのサーバ タイプ

- LDAP ツリーを参照できる十分な権限が付与されているユーザ アカウントのユーザ名とパスワード。Ciscoはこの目的でドメイン管理ユーザのアカウントを使用することを推奨します。

オプションで、ユーザ検索をさらに絞り込む場合には、特定の属性に特定の値を設定する基本フィルタを追加できます。基本フィルタでは、ベース DN でフィルタに設定されている属性値を含むオブジェクトだけを取得することで、検索を絞り込みます。基本フィルタはカッコで囲みます。たとえば、F で始まる一般名を持つユーザのみをフィルタで検出するには、フィルタ `(cn=F*)` を使用します。認証オブジェクトを保存すると、ローカル アプライアンスは、基本フィルタを使用してクエリを実行し、基本フィルタをテストして、このフィルタが正しいかどうかを示します。

LDAP 認証オブジェクトを作成するには、次の手順を実行します。

アクセス： Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 2　[External Authentication] タブをクリックします。

[External Authentication] ページが表示されます。

ステップ 3　[Create External Authentication Object] をクリックします。

ステップ 4　[Authentication Method] ドロップダウン リストから [LDAP] を選択します。

LDAP 設定オプションが表示されます。

ステップ 5　[Name] フィールドと [Description] フィールドに、認証サーバの名前と説明を入力します。

ステップ 6　[Server Type] ドロップダウン リストからサーバ タイプを選択し、[Set Defaults] ボタンをクリックして、そのタイプのデフォルト設定を設定します。次の選択肢があります。

- Microsoft Active Directory Server に接続する場合は、[MS Active Directory] を選択し、次に [Set Defaults] をクリックします。
- Sun Java System Directory Server または Oracle Directory Server に接続する場合は、[Oracle Directory] を選択し、次に [Set Defaults] をクリックします。
- OpenLDAP サーバに接続する場合は、[OpenLDAP] を選択し、次に [Set Defaults] をクリックします。
- 上記のサーバ以外のサーバに接続し、デフォルト設定をクリアする場合は、[Other] を選択し、次に [Set Defaults] をクリックします。

ステップ 7　認証データを取得するプライマリ サーバの IP アドレスまたはホスト名を [Primary Server Host Name/IP Address] フィールドに入力します。

注　証明書を使用し、TLS または SSL 経由で接続する場合は、証明書のホスト名が、このフィールドに入力するホスト名と一致している必要がりあります。また、暗号化接続では IPv6 アドレスはサポートされていません。

ステップ 8　すべてのベース DN のリストを取得するには、[Fetch DNs] をクリックして、ドロップダウン リストから適切なベース DN を選択します。

たとえば、Example 社のセキュリティ（Security）部門の名前を認証するには、`ou=security,dc=example,dc=com` を選択します。

ステップ 9　オプションで、ベース DN として指定したディレクトリ内の特定のオブジェクトだけを取得するフィルタを設定するには、[Base Filter] フィールドに、属性タイプ、比較演算子、フィルタとして使用する属性値をカッコで囲んで入力します（囲み用のカッコを含めて最大 450 文字）。

たとえば、ツリー内のユーザ オブジェクトに physicalDeliveryOfficeName 属性が設定されており、New York 支店のユーザに対しこの属性に値 `NewYork` が設定されている場合、New York 支店のユーザだけを取得するには、`(physicalDeliveryOfficeName=NewYork)` と入力します。

ステップ 10　[User Name] フィールドと [Password] フィールドに、LDAP サーバを参照できる十分な資格情報を持つユーザの識別名とパスワードを入力します。

たとえば、ユーザ オブジェクトに `uid` 属性が含まれている OpenLDAP サーバに接続し、Example 社のセキュリティ（Security）部門の管理者のオブジェクトの `uid` に値 `NetworkAdmin` が設定されている場合は、`uid=NetworkAdmin,ou=security,dc=example,dc=com` と入力します。

注意　Microsoft Active Directory Server に接続する場合は、末尾の文字が `$` のサーバ ユーザ名は指定できません。

ステップ 11　[Confirm Password] フィールドに、パスワードを再入力します。

ステップ 12　オプションで、シェル アクセスのユーザを取得するには、フィルタ条件とする属性タイプを [Shell Access Attribute] フィールドに入力します。

たとえば、Microsoft Active Directory Server で `sAMAccountName` シェル アクセス属性を使用してシェル アクセス ユーザを取得するには、[Shell Access Attribute] フィールドに `sAMAccountName` と入力します。

注　シェル認証では IPv6 アドレスはサポートされていません。

ステップ 13　[User Name] フィールドと [Password] フィールドに、LDAP サーバへのアクセスの検証に資格情報が使用されるユーザの `uid` 値またはシェル アクセス属性値と、パスワードを入力します。この場合も、Microsoft Active Directory Server に関連付けられたサーバ ユーザ名の末尾の文字が `$` であってはならないことに注意してください。

たとえば、Example 社のユーザ `JSmith` の資格情報を取得できるかどうかをテストするには、`JSmith` と入力します。

ステップ 14　[Test] をクリックして接続をテストします。

テストの成功を示すメッセージ、または欠落しているか訂正する必要がある設定を詳しく示すメッセージが表示されます。テストが成功した場合、テストの出力はページ下部に表示されます。この出力には、接続によって取得されたユーザのリストが含まれています。テストの出力に示されるユーザ数が、LDAP サーバから返されるユーザ レコードの数により制限される場合、テスト出力にこの制限が示されます。

ステップ 15　次の 2 つのオプションから選択できます。

- テストが成功した場合は [Save] をクリックします。

  [External Authentication] ページが表示され、このページに新しいオブジェクトが示されます。

  アプライアンスでオブジェクトを使用して LDAP 認証を有効にするには、そのオブジェクトが有効になっているシステム ポリシーをアプライアンスに適用する必要があります。詳細については、外部認証の有効化（63-12 ページ）およびシステム ポリシーの適用（63-4 ページ）を参照してください。

- テストが失敗した場合、または取得したユーザのリストをさらに絞り込む場合は、次の項の基本 LDAP 認証接続の調整（61-16 ページ）に進みます。

基本 LDAP 認証接続の調整

ライセンス: すべて

LDAP 認証オブジェクトを作成したが、選択したサーバへの接続が失敗したか、または必要なユーザのリストが取得されなかった場合は、そのオブジェクトの設定を調整できます。

接続のテストで接続が失敗する場合は、設定のトラブルシューティングに関する次の推奨手順を試してください。

- 画面上部とテスト出力に示されるメッセージから、問題の原因となっているオブジェクトの部分を確認します。
- オブジェクトに使用したユーザ名とパスワードが有効であることを確認します。
- サードパーティの LDAP ブラウザを使用して LDAP サーバに接続し、ベース識別名に示されているディレクトリを参照する権限がユーザにあることを確認します。
- ユーザ名が、LDAP サーバのディレクトリ情報ツリーで一意であることを確認します。
- ユーザ名に、アンダースコア、ピリオド、ハイフン、英数字だけが使用されていることを確認します。
- テスト出力に LDAP バインド エラー 49 が示される場合は、ユーザのユーザ バインディングが失敗しています。サードパーティ アプリケーションを使用してサーバ認証を試行し、その接続でも同様にバインディングが失敗するかどうかを確認します。
- サーバを正しく指定していることを確認します。
- サーバの IP アドレスまたはホスト名が正しいことを確認します。
- ローカル アプライアンスから、接続する認証サーバに TCP/IP でアクセスできることを確認します。
- サーバへのアクセスがファイアウォールによって妨げられないこと、およびオブジェクトで設定されているポートがオープンしていることを確認します。
- 証明書を使用して TLS または SSL 経由で接続する場合は、証明書のホスト名が、サーバに使用されているホスト名と一致している必要があります。
- シェル アクセスを認証する場合は、サーバ接続に IPv6 アドレスを使用していないことを確認します。
- サーバ タイプのデフォルトを使用している場合は、正しいサーバ タイプであることを確認し、[Set Default] をもう一度クリックしてデフォルト値をリセットします。

  詳細については、LDAP 認証サーバの指定（61-18 ページ）を参照してください。
- ベース識別名を入力した場合は、[Fetch DNs] をクリックし、サーバで使用可能なすべてのベース識別名を取得し、リストから名前を選択します。
- フィルタ、アクセス属性、または詳細設定を使用している場合は、それぞれが有効であり正しく入力されていることを確認します。
- フィルタ、アクセス属性、または詳細設定を使用している場合は、各設定を削除し、設定なしでオブジェクトをテストしてみます。
- 基本フィルタまたはシェル アクセス フィルタを使用している場合は、フィルタがカッコで囲まれており、有効な比較演算子を使用していることを確認します。詳細については、基本フィルタについて（61-7 ページ）およびシェル アクセスについて（61-9 ページ）を参照してください。
- より制限された基本フィルタをテストするには、特定のユーザだけを取得するため、フィルタにそのユーザのベース識別名を設定します。

- 暗号化接続を使用する場合:
- 証明書の LDAP サーバの名前が、接続に使用するホスト名と一致していることを確認します。
- 暗号化されたサーバ接続で IPv6 アドレスを使用していないことを確認します。
- テスト ユーザを使用する場合、ユーザ名とパスワードが正しく入力されていることを確認します。
- テスト ユーザを使用する場合、ユーザ資格情報を削除してオブジェクトをテストします。
- 次の構文を使用して、接続するアプライアンスでコマンド ラインから LDAP サーバに接続し、使用するクエリをテストします。

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

たとえば、domainadmin@myrtle.example.com ユーザと基本フィルタ (cn=*) を使用して myrtle.example.com のセキュリティ ドメインに接続する場合は、次のステートメントを使用して接続をテストできます。

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

接続のテストが正常に完了したが、システム ポリシーの適用後に認証が機能しない場合は、使用する認証とオブジェクトの両方が、アプライアンスに適用されるシステム ポリシーで有効になっていることを確認します。

正常に接続したが、接続で取得されたユーザ リストを調整する必要がある場合は、基本フィルタまたはシェル アクセス フィルタを追加または変更するか、ベース DN をさらに制限するかまたは制限を緩めて使用することができます。詳細については、次のトピックを参照してください。

- ベース DN について（61-7 ページ）
- 基本フィルタについて（61-7 ページ）
- LDAP 固有パラメータの設定（61-20 ページ）

拡張 LDAP 認証オブジェクトの作成

ライセンス: すべて

アプライアンスにユーザ認証サービスを提供するため、LDAP 認証オブジェクトを作成できます。

認証オブジェクトの作成時に、認証サーバに接続できるようにするための設定を定義します。また、サーバからユーザ データを取得するために使用するディレクトリ コンテキストと検索条件も選択します。オプションで、シェル アクセス認証を設定できます。

ローカル アプライアンスから、接続する認証サーバに TCP/IP でアクセスできることを確認します。

ご使用のサーバ タイプのデフォルト設定を使用して基本 LDAP 設定を迅速にセットアップできますが、詳細設定をカスタマイズして、アプライアンスから LDAP サーバに暗号化接続するかどうか、接続のタイムアウト、およびサーバがユーザ情報を検査する属性を制御することもできます。

LDAP 固有のパラメータの場合、LDAP 命名基準とフィルタおよび属性の構文を使用できます。詳細については、『Lightweight Directory Access Protocol (v3): Technical Specification』(RFC 3377) に記載されている RFC を参照してください。この手順では構文の例が示されています。Microsoft Active Directory Server へ接続するための認証オブジェクトをセットアップするときに、ドメインを含むユーザ名を参照する場合には、Internet RFC 822 (Standard for the Format of ARPA Internet Text Messages) 仕様に記載されているアドレス指定構文を使用できることに注意してください。

たとえばユーザ オブジェクトを参照する場合は、`JoeSmith@security.example.com` と入力し、Microsoft Active Directory Sever を使用する場合の同等のユーザ識別名 `cn=JoeSmith,ou=security, dc=example,dc=com` は使用しません。

注　CAC 認証に使用する LDAP 認証オブジェクトを設定する場合は、コンピュータに挿入されている CAC を**取り外さないでください**。ユーザ証明書を有効にした後では、CAC が常に挿入された状態にしておく**必要があります**。詳細については、ユーザ証明書の要求（64-6 ページ）およびCAC を使用した LDAP 認証について（61-10 ページ）を参照してください。

拡張認証オブジェクトを作成するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 2　[External Authentication] タブをクリックします。

[External Authentication] ページが表示されます。

ステップ 3　[Create External Authentication Object] をクリックします。

[Create External Authentication Object] ページが表示されます。

ステップ 4　外部認証のためのユーザ データを取得する認証サーバを指定します。詳細については、LDAP 認証サーバの指定（61-18 ページ）を参照してください。

ステップ 5　認証対象ユーザを取得する検索要求を作成するための認証設定を設定します。ユーザがログイン時に入力するユーザ名の形式を規定するユーザ名テンプレートを指定します。詳細については、LDAP 固有パラメータの設定（61-20 ページ）を参照してください。

ステップ 6　オプションで、デフォルト アクセス ロール割り当ての基準として使用する LDAP グループを設定します。詳細については、グループによるアクセス権の設定（61-24 ページ）を参照してください。

ヒント　CAC 認証および認可にこのオブジェクトを使用する予定の場合、Ciscoは、アクセス ロール割り当ての管理のために LDAP グループを設定することを推奨します。詳細については、CAC 認証および認可の管理（61-12 ページ）を参照してください。

ステップ 7　オプションで、シェル アクセスの認証設定を設定します。詳細については、シェル アクセスの設定（61-26 ページ）を参照してください。

ステップ 8　正常に認証を実行できるユーザの名前とパスワードを入力して、設定をテストします。詳細については、ユーザ認証のテスト（61-27 ページ）を参照してください。

変更が保存されます。認証の変更がアプライアンスで行われる前に、オブジェクトが有効に設定されているシステム ポリシーをそのアプライアンスに適用する必要があることに注意してください。詳細については、外部認証の有効化（63-12 ページ）およびシステム ポリシーの適用（63-4 ページ）を参照してください。

LDAP 認証サーバの指定

ライセンス：すべて

認証オブジェクトの作成時には、管理対象デバイスまたはDefense Centerが認証のために接続する、プライマリおよびバックアップ サーバとサーバ ポートを最初に指定します。

LDAP 認証サーバを指定するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 2　[External Authentication] タブをクリックします。

[External Authentication] ページが表示されます。

ステップ 3　[Create External Authentication Object] をクリックします。

[Create External Authentication Object] ページが表示されます。

ステップ 4　[Authentication Method] ドロップダウン リストから [LDAP] を選択します。

LDAP 設定オプションが表示されます。

ステップ 5　オプションで、CAC 認証および認可にこの認証オブジェクトを使用する予定の場合は、[CAC] チェック ボックスをオンにします。

CAC 認証および認可の設定の概要については、CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。

ステップ 6　[Name] フィールドと [Description] フィールドに、認証サーバの名前と説明を入力します。

ステップ 7　オプションで、[Server Type] フィールドで接続先 LDAP サーバのタイプを選択し、[Set Defaults] をクリックして、[User Name Template]、[UI Access Attribute]、[Shell Access Attribute]、[Group Member Attribute]、および [Group Member URL Attribute] の各フィールドにデフォルト値を取り込みます。次の選択肢があります。

- Microsoft Active Directory Server に接続する場合は、[MS Active Directory] を選択し、[Set Defaults] をクリックします。
- Sun Java System Directory Server または Oracle Directory Server に接続する場合は、[Oracle Directory] を選択し、[Set Defaults] をクリックします。
- OpenLDAP サーバに接続する場合は、[OpenLDAP] を選択し、[Set Defaults] をクリックします。
- 上記のサーバ以外の LDAP サーバに接続し、デフォルト設定をクリアする場合は、[Other] を選択し、[Set Defaults] をクリックします。

ステップ 8　認証データを取得するプライマリ サーバの IP アドレスまたはホスト名を [Primary Server Host Name/IP Address] フィールドに入力します。

注　証明書を使用し、TLS または SSL 経由で接続する場合は、証明書のホスト名が、このフィールドに入力するホスト名と一致している必要があります。また、暗号化接続では IPv6 アドレスはサポートされていません。

ステップ 9　オプションで、[Primary Server Port] フィールドでプライマリ認証サーバが使用するポートを変更します。

ステップ 10　オプションで、認証データを取得するバックアップ サーバの IP アドレスまたはホスト名を [Backup Server Host Name/IP Address] フィールドに入力します。

ステップ 11　オプションで、[Backup Server Port] フィールドでプライマリ認証サーバが使用するポートを変更します。

LDAP 固有パラメータの設定（61-20 ページ）に進みます。

LDAP 固有パラメータの設定

ライセンス: すべて

LDAP 固有パラメータ セクションの設定により、アプライアンスがユーザ名を検索する LDAP ディレクトリの領域が決定され、アプライアンスから LDAP サーバへの接続の詳細が制御されます。

これらの設定を行う場合、有効なユーザ名は一意のユーザ名であり、アンダースコア(_)、ピリオド(.)、ハイフン(-)、英数字を使用できることに注意してください。

ほとんどの LDAP 固有設定の他に、LDAP 命名基準とフィルタおよび属性の構文を使用できます。詳細については、『Lightweight Directory Access Protocol (v3): Technical Specification』(RFC 3377)に記載されている RFC を参照してください。この手順では構文の例が示されています。Microsoft Active Directory Server へ接続するための認証オブジェクトをセットアップするときに、ドメインを含むユーザ名を参照する場合には、Internet RFC 822(Standard for the Format of ARPA Internet Text Messages)仕様に記載されているアドレス指定構文を使用できることに注意してください。たとえばユーザ オブジェクトを参照する場合は、`JoeSmith@security.example.com` と入力し、Microsoft Active Directory Sever を使用する場合の同等のユーザ識別名 `cn=JoeSmith,ou=security, dc=example,dc=com` は使用しません。

次の表で、各 LDAP 固有パラメータについて説明します。

表 61-2　LDAP 固有のパラメータ

設定	説明	例
Base DN	アプライアンスがユーザ情報を検索する LDAP サーバのディレクトリのベース識別名を指定します。 通常、ベース DN には、企業ドメインおよび部門を示す基本構造があります。 プライマリ サーバを特定したら、そのサーバから使用可能なベース DN のリストが自動的に取得され、該当するベース DN を選択できることに注意してください。	Example 社のセキュリティ(Security)部門のベース DN は、`ou=security,dc=example,dc=com` となります。
Base Filter	ベース DN でフィルタに設定されている特定の属性と値のペアを含むオブジェクトだけを取得することで、検索を絞り込みます。基本フィルタはカッコで囲む必要があることに注意してください。 テスト ユーザ名とパスワードを入力して基本フィルタをより具体的にテストするにはユーザ認証のテスト (61-27 ページ)を参照してください。	F で始まる一般名を持つユーザのみをフィルタで検出するには、フィルタ `(cn=F*)` を使用します。
User Name/ Password	ローカル アプライアンスがユーザ オブジェクトにアクセスできるようにします。取得する認証オブジェクトに対する適切な権限を持つユーザのユーザ資格情報を指定します。指定するユーザの識別名は、LDAP サーバのディレクトリ情報ツリーで一意である必要があります。Microsoft Active Directory Server に関連付けられたサーバ ユーザ名の末尾の文字が `$` であってはならないことに注意してください。	Example 社のセキュリティ(Security)部門の `admin` ユーザのユーザ名は、`cn=admin, ou=security, dc=example,dc=com`

表 61-2　LDAP 固有のパラメータ（続き）

設定	説明	例
Encryption	通信が暗号化されるかどうかと、暗号化方法を示します。暗号化なし、Transport Layer Security（TLS）、または Secure Sockets Layer（SSL）暗号化を選択できます。TLS または SSL 経由で接続するときに認証に証明書を使用する場合、証明書の LDAP サーバ名が、接続時に使用する名前と一致している**必要がある**ことに注意してください。 ポートを指定した後で暗号化方式を変更すると、ポートが、選択されているサーバ タイプのデフォルト値にリセットされます。	外部認証設定に `10.10.10.250` と入力し、証明書に `computer1.example.com` と入力すると、`computer1.example.com` の IP アドレスが `10.10.10.250` の場合でも、接続は失敗します。外部認証設定のサーバ名を `computer1.example.com` に変更することで、接続が正常に行われます。
SSL Certificate Upload Path	ローカル コンピュータで、暗号化に使用する証明書のパスを指定します。	`c:/server.crt`
User Name Template	文字列変換文字（`%s`）をユーザのシェル アクセス属性の値にマッピングすることで、ログイン時に入力されるユーザ名の形式を指定します。ユーザ名テンプレートは、認証に使用する識別名の形式です。ユーザがログイン ページにユーザ名を入力すると、アプライアンスにより文字列変換文字が名前に置き換えられ、その結果生成される識別名がユーザ資格情報の検索に使用されます。 CAC 認証および許可にこのオブジェクトを使用するには、[UI Access Attribute] の値に対応する値を入力する**必要があります**。詳細については、CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。	`%s@security.example.com`, `%s@mail.com`, `%s@mil`, `%s@smil.mil`,
Timeout	プライマリ サーバへの接続試行のタイムアウトを設定します。これにより、接続がバックアップ サーバにロールオーバーされます。プライマリ認証サーバからの応答がない状態でこのフィールドに示されている秒数（または LDAP サーバのタイムアウト）が経過すると、アプライアンスはバックアップ サーバに対してクエリを実行します。 ただし LDAP がプライマリ LDAP サーバのポートで実行されており、何らかの理由で要求の処理を拒否する場合は、バックアップ サーバへのフェールオーバーは行われません。	プライマリ サーバで LDAP が無効な場合、アプライアンスはバックアップ サーバに対してクエリを実行します。

表 61-2　LDAP 固有のパラメータ（続き）

設定	説明	例
UI Access Attribute	ローカル アプライアンスに対し、ユーザ識別名の値ではなく、特定の属性の値の照合を行うように指示します。FireSIGHT システム Web インターフェイスの有効なユーザ名が値として設定されている属性であれば、どの属性でも使用できます。いずれかのオブジェクトに一致するユーザ名とパスワードがある場合は、ユーザ ログイン要求が認証されます。 サーバ タイプを選択し、デフォルトを設定すると、[UI Access Attribute] に、そのサーバ タイプに適した値が取り込まれます。 このフィールドを空白のままにすると、ローカル アプライアンスは、LDAP サーバの各ユーザ レコードのユーザ識別名値を調べ、ユーザ名に一致しているかどうかを確認します。 CAC 認証および許可にこのオブジェクトを使用するには、[User Name Template] の値に対応する値を入力する**必要があります**。詳細については、CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。	`sAMAccountName`, `userPrincipalName`, `mail`
Shell Access Attribute	シェル アクセス資格情報の特定の属性を調べる場合は、その属性に一致するようにこのフィールドを明示的に設定する必要があります。シェル アクセスの有効なユーザ名が値として設定されている属性であれば、どの属性でも使用できます。 このフィールドを空白のままにした場合、シェル アクセス認証にはユーザ識別名が使用されます。 サーバ タイプを選択し、デフォルトを設定すると、そのサーバ タイプに適した属性がこのフィールドに事前に取り込まれることに注意してください。	`sAMAccountName`

サーバに LDAP 固有のパラメータを設定するには、次の手順を実行します。

アクセス： Admin

ステップ 1　[Create External Authentication Object] ページの [LDAP-Specific Parameters] セクションには、ベース DN を設定する 2 つのオプションがあります。

- 使用可能なすべてのドメインのリストを取得するには、[Fetch DNs] をクリックして、ドロップダウン リストから適切なベース ドメイン名を選択します。
- アクセスする LDAP ディレクトリのベース識別名を [Base DN] フィールドに入力します。

たとえば、Example 社のセキュリティ（Security）部門の名前を認証するには、`ou=security,dc=example,dc=com` を入力または選択します。

ステップ 2　オプションで、ベース DN として指定したディレクトリ内の特定のオブジェクトだけを取得するフィルタを設定するには、[Base Filter] フィールドに、属性タイプ、比較演算子、フィルタとして使用する属性値をカッコで囲んで入力します。

たとえば、ディレクトリ ツリー内のユーザ オブジェクトに physicalDeliveryOfficeName 属性が設定されており、New York 支店のユーザに対しこの属性に値 `NewYork` が設定されている場合、New York 支店のユーザだけを取得するには、`(physicalDeliveryOfficeName=NewYork)` と入力します。

ステップ 3　[User Name] および [Password] フィールドに、LDAP ディレクトリへのアクセスの検証に資格情報が使用されるユーザの識別名とパスワードを入力します。

たとえば、ユーザ オブジェクトに uid 属性が含まれている OpenLDAP サーバに接続し、Example 社のセキュリティ（Security）部門の管理者のオブジェクトの uid に値 NetworkAdmin が設定されている場合は、uid=NetworkAdmin,ou=security,dc=example,dc=com と入力します。

注意　Microsoft Active Directory Server に接続する場合は、末尾の文字が $ のサーバ ユーザ名は指定できません。

ステップ 4　[Confirm Password] フィールドに、パスワードを再入力します。

ステップ 5　基本的な LDAP 固有パラメータの設定後に行う手順には、いくつかの選択肢があります。

- 詳細オプションにアクセスするには、[Show Advanced Options] の横の矢印をクリックし、次のステップに進みます。
- LDAP グループ メンバーシップに基づいてユーザ デフォルト ロールを設定する場合は、グループによるアクセス権の設定（61-24 ページ）に進みます。
- 認証に LDAP グループを使用しない場合は、シェル アクセスの設定（61-26 ページ）に進みます。

ステップ 6　オプションで、次のいずれかの暗号化モードを選択できます。

- Secure Sockets Layer（SSL）を使用して接続するには、[SSL] を選択します。
- Transport Layer Security（TLS）を使用して接続するには、[TLS] を選択します。
- 暗号化なしで接続するには、[None] を選択します。

注　ポートを指定した後で暗号化方式を変更すると、ポートがその方式のデフォルト値にリセットされることに注意してください。[None] または [TLS] の場合、ポートはデフォルト値 389 を使用します。SSL 暗号化を選択した場合は、ポートはデフォルト値 636 を使用します。

ステップ 7　TLS または SSL 暗号化を選択しており、認証に証明書を使用する場合は、[Browse] をクリックして有効な TLS または SSL 証明書のロケーションを参照するか、または [SSL Certificate Upload Path] フィールドに証明書のパスを入力します。

証明書のアップロードが正常に完了したことを示すメッセージが表示されます。

注　以前にアップロードした証明書を置き換えるには、新しい証明書をアップロードし、システム ポリシーをアプライアンスに再適用して、新しい証明書を上書きコピーします。

ステップ 8　オプションで、[User Name Template] フィールドに、[UI Access Attribute] の値からユーザ名を判別するときに使用する文字列変換文字（%s）を入力します。

たとえば、シェル アクセス属性が uid である OpenLDAP サーバに接続し、Example 社のセキュリティ（Security）部門で働くすべてのユーザを認証するには、[User Name Template] フィールドに uid=%s,ou=security,dc=example,dc=com と入力します。Microsoft Active Directory Server の場合は %s@security.example.com と入力します。

認証および認可に CAC 資格情報を使用するには、[User Name Template] フィールドに値を入力する**必要があります**。詳細については、CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。

ステップ 9　オプションで、バックアップ接続にロールオーバーするまでの経過秒数を [Timeout] フィールドに入力します。

ステップ 10　オプションで、ベース DN および基本フィルタの代わりに属性に基づいてユーザを取得する場合、2 つのオプションがあります。

- [Fetch Attrs] をクリックして使用可能な属性のリストを取得し、適切な属性を選択します。
- 属性を [UI Access Attribute] フィールドに入力します。

たとえば Microsoft Active Directory Server では、Active Directory Server ユーザ オブジェクトに `uid` 属性がないため、[UI Access Attribute] を使用してユーザを取得することがあります。代わりに [UI Access Attribute] フィールドに `userPrincipalName` と入力して、`userPrincipalName` 属性を検索できます。

認証および認可に CAC 資格情報を使用するには、[UI Access Attribute] フィールドに値を入力する**必要があります**。詳細については、CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。

ステップ 11　オプションで、シェル アクセスのユーザを取得するには、フィルタ条件とする属性を [Shell Access Attribute] フィールドに入力します。

たとえば、Microsoft Active Directory Server で `sAMAccountName` シェル アクセス属性を使用してシェル アクセス ユーザを取得するには、[Shell Access Attribute] フィールドに `sAMAccountName` と入力します。

注　同一認証オブジェクトで CAC 認証および認可とシェル アクセスの両方を設定することは**できません**。[CAC] チェック ボックスをオンにすると、そのページのシェル アクセス設定のオプションが無効になります。代わりに、別の認証オブジェクトを作成し、システム ポリシーで個別に有効にします。詳細については、外部認証の有効化（63-12 ページ）を参照してください。

ステップ 12　次のステップでは、3 つの選択肢があります。

- LDAP グループ メンバーシップに基づいてユーザ デフォルト ロールを設定する場合は、グループによるアクセス権の設定（61-24 ページ）に進みます。
- 認証に LDAP グループを使用**しない**が、シェル アクセスを設定する場合は、シェル アクセスの設定（61-26 ページ）に進みます。
- 認証に LDAP グループを使用**せず**、シェル アクセスを設定**しない**場合は、ユーザ認証のテスト（61-27 ページ）に進みます。

グループによるアクセス権の設定

ライセンス： すべて

LDAP グループのユーザのメンバーシップに基づいてデフォルト アクセス権を設定する場合は、FireSIGHT システムにより使用される各アクセス ロールに、LDAP サーバの既存のグループの識別名を指定できます。これを行うと、LDAP によって検出された、指定のどのグループにも属さないユーザのデフォルト アクセス設定を設定できます。ユーザがログインすると、FireSIGHT システムは LDAP サーバを動的に検査し、ユーザの現在のグループ メンバーシップに基づいてデフォルト アクセス権を割り当てます。

CAC 認証および認可にオブジェクトを使用する予定の場合、Ciscoは、CAC 認証ユーザへのアクセス ロール割り当ての管理のために LDAP グループを設定することを推奨します。詳細については、CAC 認証および認可の管理（61-12 ページ）を参照してください。

参照するグループはすべて LDAP サーバに存在している必要があります。スタティック LDAP グループまたはダイナミック LDAP グループを参照できます。スタティック LDAP グループとは、特定のユーザを指し示すグループ オブジェクト属性によってメンバーシップが決定される

グループであり、ダイナミック LDAP グループとは、ユーザ オブジェクト属性に基づいてグループ ユーザを取得する LDAP 検索を作成することでメンバーシップが決定されるグループです。ロールのグループ アクセス権は、グループのメンバーであるユーザにのみ影響します。

ユーザが FireSIGHT システムにログインするときに付与されるアクセス権は、LDAP 構成によって異なります。

- LDAP サーバでグループ アクセス権が設定されていない場合、新しいユーザがログインすると、FireSIGHT システムはそのユーザを LDAP サーバに対して認証し、システム ポリシーに設定されているデフォルトの最小アクセス ロールに基づいてユーザ権限を付与します。
- グループ設定を設定すると、指定されたグループに属している新しいユーザは、メンバーとなっているグループの最小アクセス設定を継承します。
- 新しいユーザが指定のどのグループにも属していない場合は、認証オブジェクトの [Group Controlled Access Roles] セクションに指定されているデフォルトの最小アクセス ロールが割り当てられます。
- 設定されている複数のグループにユーザが属している場合、ユーザは最も高いアクセスを持つグループのアクセス ロールを最小アクセス ロールとして受け取ります。

FireSIGHT システム ユーザ管理ページでは、LDAP グループ メンバーシップによってアクセス ロールが割り当てられているユーザの最小アクセス権を削除することはできません。ただし、追加の権限を割り当てることはできます。外部認証ユーザのアクセス権を変更すると、[User Management] ページの [Authentication Method] カラムに、[External - Locally Modified] というステータスが表示されます。

注　ダイナミック グループを使用する場合、LDAP クエリは、LDAP サーバで設定されている通りに使用されます。この理由から、検索構文エラーが原因で無限ループが発生することを防ぐため、FireSIGHT システムでは検索の再帰回数が 4 回に制限されています。この再帰回数内でユーザのグループ メンバーシップが確立されない場合、[Group Controlled Access Roles] セクションで定義されているデフォルト アクセス ロールがユーザに付与されます。

グループ メンバーシップに基づいてデフォルトのロールを設定するには、次の手順を実行します。

アクセス： Admin

ステップ 1　[Create External Authentication Object] ページで、[Group Controlled Access Roles] の横の下矢印をクリックします。

セクションが展開されます。

ステップ 2　オプションで、グループ メンバーシップ別のアクセス デフォルトを設定します。

FireSIGHT システム ユーザ ロールに対応する [DN] フィールドに、これらのロールに割り当てる必要があるユーザを含む LDAP グループの識別名を入力します。

たとえば、`Example` 社の情報テクノロジー（Information Technology）部門の名前を認証するには、[Administrator] フィールドに次のように入力します。

```
cn=itgroup,ou=groups, dc=example,dc=com
```

ユーザ アクセス ロールの詳細については、新しいユーザ アカウントの追加（61-47 ページ）を参照してください。

ステップ 3　[Default User Role] から、指定のどのグループにも属さないユーザのデフォルト最小アクセス ロールを選択します。

ヒント　複数のロールを選択するには、Ctrl キーを押しながらロール名をクリックします。

ステップ 4　スタティック グループを使用していた場合は、スタティック グループのメンバーシップを指定する LDAP 属性を [Group Member Attribute] フィールドに入力します。

たとえば、デフォルトの Security Analyst アクセスのために参照するスタティック グループのメンバーシップを示すために `member`属性を使用する場合は、`member` と入力します。

ステップ 5　ダイナミック グループを使用していた場合は、ダイナミック グループのメンバーシップの決定に使用される LDAP 検索文字列を含む LDAP 属性を [Group Member URL Attribute] フィールドに入力します。

たとえば、デフォルトの Admin アクセスに対して指定したダイナミック グループのメンバーを取得する LDAP 検索が `memberURL` 属性に含まれている場合は、`memberURL` と入力します。

ステップ 6　シェル アクセスの設定（61-26 ページ）に進みます。

シェル アクセスの設定

ライセンス： すべて

LDAP サーバを使用して、管理対象デバイスまたはDefense Centerでシェル アクセス用アカウントを認証することもできます。シェル アクセスを付与するユーザの項目を取得する検索フィルタを指定します。

同一認証オブジェクトで CAC 認証および認可とシェル アクセスの両方を設定することは**できません**。代わりに、別の認証オブジェクトを作成し、システム ポリシーで個別に有効にします。シェル アクセスの認証オブジェクトは、システム ポリシーの最初の認証オブジェクトである必要があります。認証オブジェクトの順序の管理については、外部認証の有効化（63-12 ページ）を参照してください。

注　Ciscoは、仮想デバイスまたは Cisco NGIPS for Blue Coat X-Series の外部認証をサポートしていません。さらに、シェル アクセス認証では IPv6 がサポートされていません。

admin アカウントを除き、シェル アクセスは設定したシェル アクセス属性によって完全に制御されます。設定するシェル アクセス フィルタにより、シェルにログインできる LDAP サーバのユーザが決定します。

ログイン時に各シェル ユーザのホーム ディレクトリが作成されること、および（LDAP 接続を無効にすることで）LDAP シェル アクセス ユーザ アカウントが無効になっている場合はディレクトリが維持されますが、ユーザ シェルは `/etc/password` 内の `/bin/false` に設定され、シェルが無効になることに注意してください。ユーザが再度有効になると、同じホーム ディレクトリを使用してシェルがリセットされます。

[Same as Base Filter] チェック ボックスを使用すると、ベース DN で限定されるすべてのユーザが、シェル アクセス権限でも限定される場合に、より効率的に検索できます。通常、ユーザを取得する LDAP クエリは、基本フィルタとシェル アクセス フィルタを組み合わせます。シェル アクセス フィルタが基本フィルタと同一である場合は、同じクエリが 2 回実行されることになり、不必要に時間を消費することになります。[Same as Base Filter] オプションを使用すると、この両方の目的でクエリを 1 回だけ実行することができます。

シェル ユーザは、小文字で構成されたユーザ名を使用してログインすることができます。シェルのログイン認証では大文字と小文字が区別されます。

注意　シリーズ 3 Defense Centerでは、すべてのシェル ユーザに sudoers 特権が付与されます。シェル アクセスが付与されるユーザのリストを適切に制限してください。シリーズ 3 と仮想デバイスでは、外部認証ユーザに付与されるシェル アクセスのデフォルトは、**Configuration** レベルのコマンド ライン アクセスになります。このアクセスでも sudoers 特権が付与されます。

シェル アカウント認証を設定するには、次の手順を実行します。

アクセス： Admin

ステップ 1　オプションで、[Create External Authentication Object] ページでシェル アクセス アカウント フィルタを設定します。次の複数のオプションがあります。

- 属性値に基づいて管理ユーザ項目を取得するには、属性名、比較演算子、およびフィルタとして使用する属性値を、カッコで囲んで [Shell Access Filter] フィールドに入力します。
- 認証設定の設定時に指定したものと同じフィルタを使用するには、[Same as Base Filter] を選択します。
- シェル アクセスの LDAP 認証を防止するには、このフィールドを空白にします。シェル アクセス フィルタを指定しないことを選択すると、認証オブジェクトの保存時に、フィルタを空白のままにすることを確認する警告が表示されます。

たとえば、すべてのネットワーク管理者の manager 属性に属性値 shell が設定されている場合は、基本フィルタ (manager=shell) を設定できます。

ステップ 2　ユーザ認証のテスト (61-27 ページ) に進みます。

ユーザ認証のテスト

ライセンス： すべて

LDAP サーバを設定し、認証設定を行ったら、これらの設定をテストするため、認証できる必要があるユーザのユーザ資格情報を指定できます。

ユーザ名として、テストに使用するユーザの uid 属性の値を入力できます。Microsoft Active Directory Server に接続して uid の代わりにシェル アクセス属性を指定する場合は、ユーザ名としてこの属性の値を使用します。ユーザの完全修飾識別名も指定できます。

テスト出力には、有効なユーザ名と無効なユーザ名が示されます。有効なユーザ名は一意のユーザ名であり、英数字と、アンダースコア (_)、ピリオド (.)、ハイフン (-) のみを使用できます。無効なユーザ名は、その他の英数字以外の文字 (スペースなど) が含まれているユーザ名です。

Web インターフェイスのページ サイズ制限のため、ユーザ数が 1000 を超えているサーバへの接続をテストする場合、返されるユーザの数は 1000 であることに注意してください。

ヒント　テスト ユーザの名前とパスワードを誤って入力すると、サーバ設定が正しい場合でもテストが失敗します。最初に、追加のテスト パラメータを使用せずにサーバ設定をテストします。正常に完了した場合は、テストする特定ユーザのユーザ名とパスワードを指定します。

ユーザ認証をテストするには、次の手順を実行します。

アクセス：Admin

ステップ 1　[User Name] フィールドと [Password] フィールドに、LDAP サーバへのアクセスの検証に資格情報が使用されるユーザの `uid` 値またはシェル アクセス属性値と、パスワードを入力します。

たとえば、Example 社のユーザ `JSmith` の資格情報を取得できるかどうかをテストするには、`JSmith` と入力します。

ステップ 2　[Test] をクリックします。

テストの成功を示すメッセージ、または欠落しているか訂正する必要がある設定を詳しく示すメッセージが表示されます。次の 2 つのオプションから選択できます。

- テストが成功した場合、テストの出力がページ下部に表示されます。[Save] をクリックします。[External Authentication] ページが表示され、このページに新しいオブジェクトが示されます。

  アプライアンスでオブジェクトを使用して LDAP 認証を有効にするには、そのオブジェクトが有効になっているシステム ポリシーをアプライアンスに適用する必要があります。詳細については、外部認証の有効化（63-12 ページ）およびシステム ポリシーの適用（63-4 ページ）を参照してください。

- テストが失敗した場合は、接続のトラブルシューティングの提案事項につて基本 LDAP 認証接続の調整（61-16 ページ）を参照してください。表示されるエラー メッセージに、接続失敗の原因が示されていることに注意してください。

LDAP 認証オブジェクトの例

ライセンス：すべて

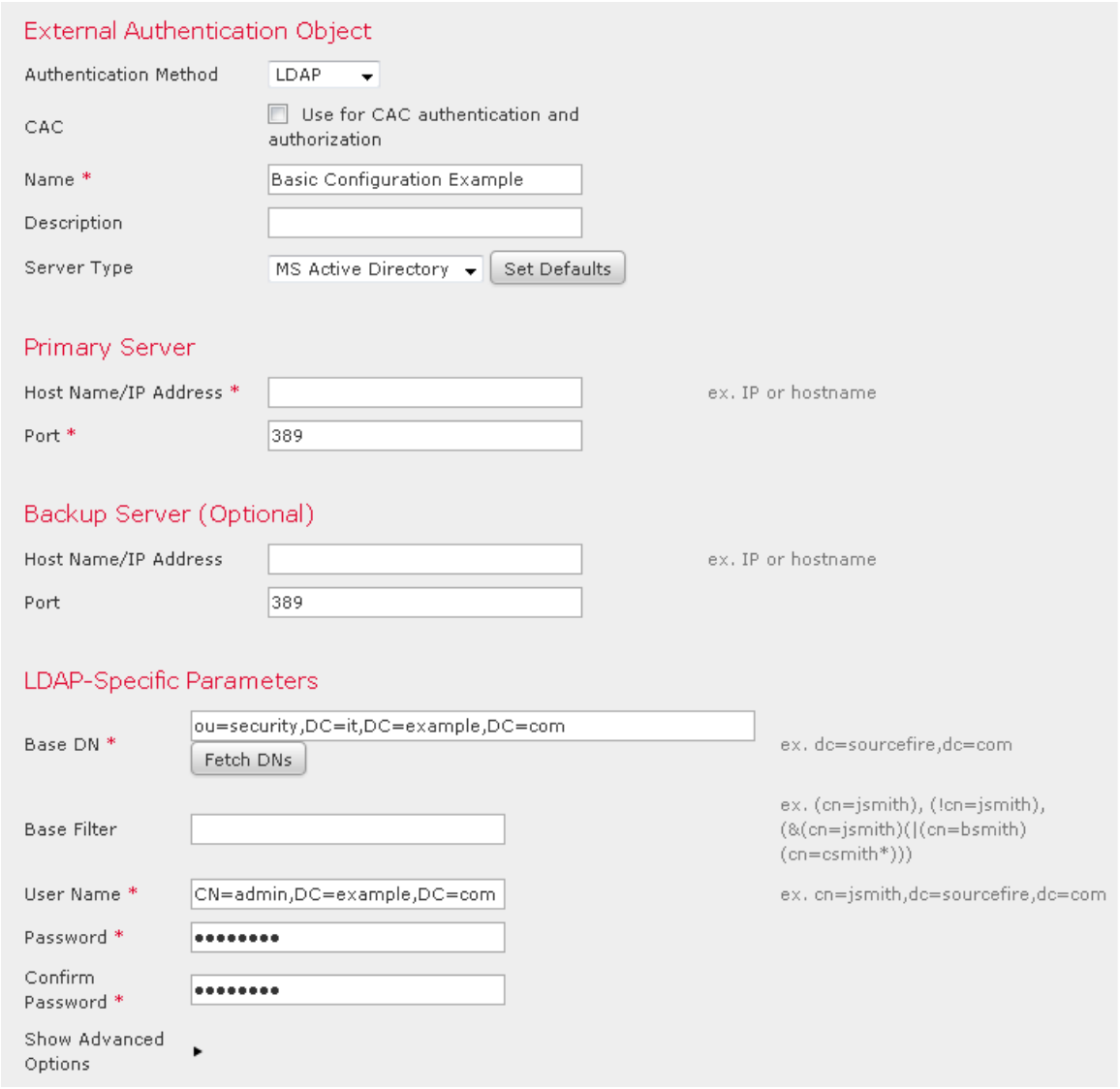
ここでは、基本設定を使用する LDAP 設定の例と、詳細な設定オプションを使用する例を示します。

- 例：LDAP の基本設定（61-28 ページ）
- 例：詳細な LDAP 設定（61-30 ページ）

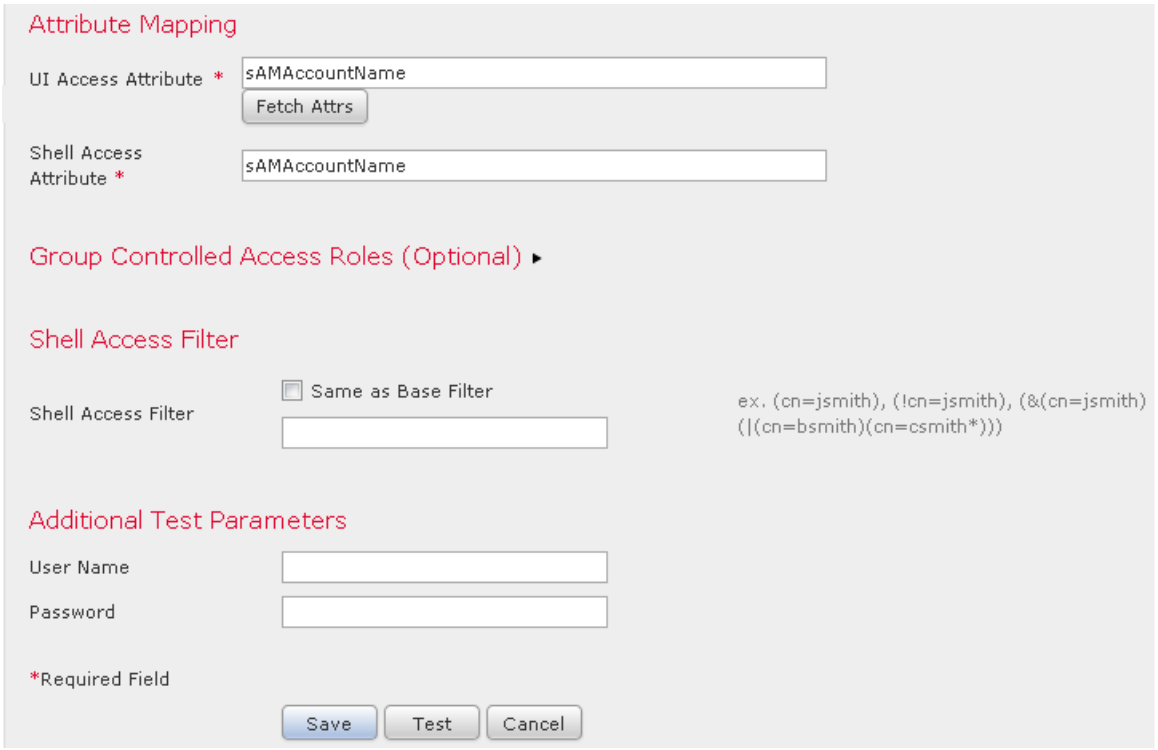
例：LDAP の基本設定

ライセンス：すべて

次の図は、Microsoft Active Directory Server の LDAP ログイン認証オブジェクトの基本設定を示します。この例の LDAP サーバの IP アドレスは 10.11.3.4 です。接続ではアクセスのためにポート 389 が使用されます。



この例では、Example 社の情報テクノロジー ドメインのセキュリティ（Security）部門のベース識別名として `OU=security,DC=it,DC=example,DC=com` が使用されています。



ただし、このサーバが Microsoft Active Directory Server であるため、ユーザ名の保存に `uid` 属性ではなく `sAMAccountName` 属性が使用されます。サーバのタイプとして MS Active Directory を選択し、[Set Defaults] をクリックすると、[UI Access Attribute] が `sAMAccountName` に設定されます。その結果、ユーザが FireSIGHT システムへのログインを試行すると、FireSIGHT システムは各オブジェクトの `sAMAccountName` 属性を検査し、一致するユーザ名を検索します。

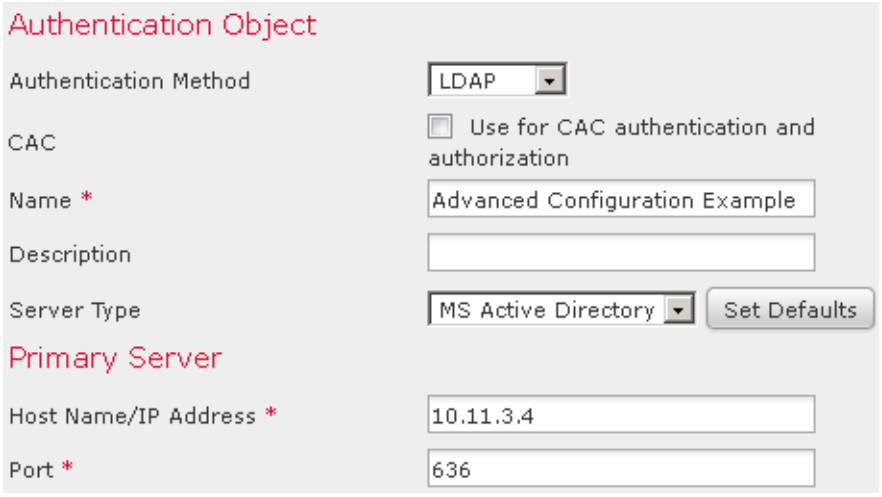
また、[Shell Access Attribute] が `sAMAccountName` の場合、ユーザがアプライアンスでシェル アカウントにログインすると、ディレクトリ内のすべてのオブジェクトの各 `sAMAccountName` 属性が検査され、一致が検索されます。

基本フィルタはこのサーバに適用されないため、FireSIGHT システムはベース識別名により示されるディレクトリ内のすべてのオブジェクトの属性を検査することに注意してください。サーバへの接続は、デフォルトの期間（または LDAP サーバで設定されたタイムアウト期間）の経過後にタイムアウトします。

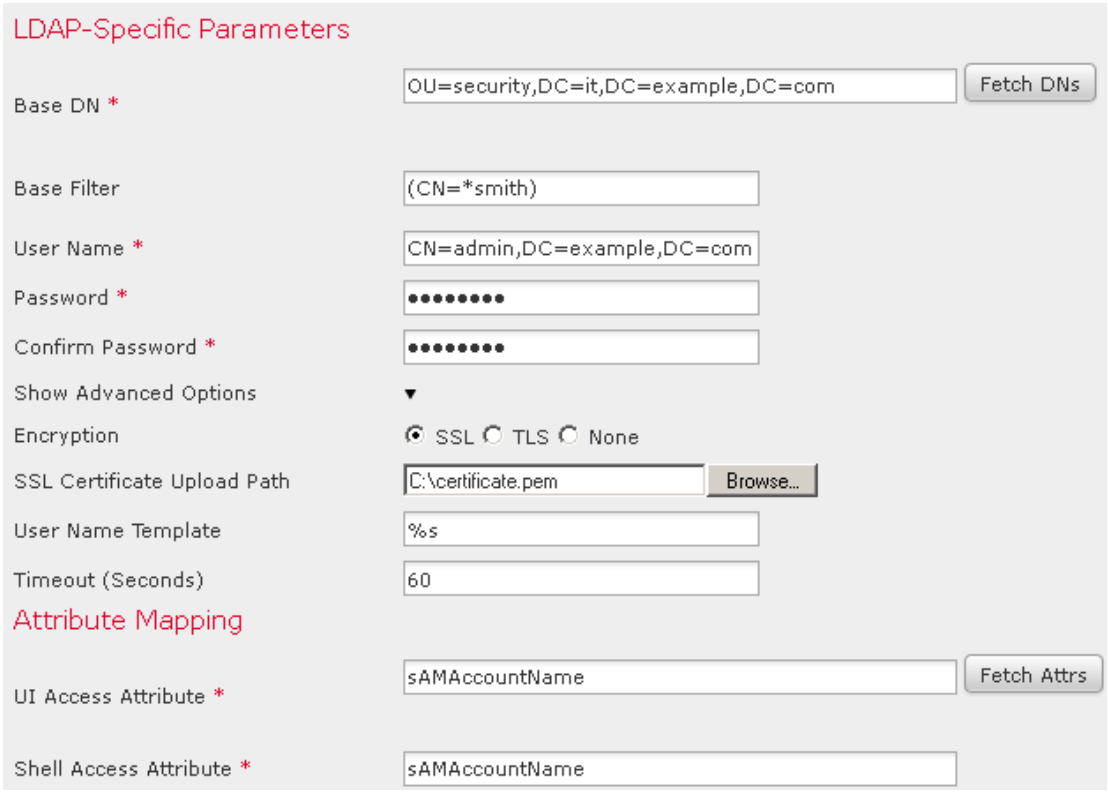
例：詳細な LDAP 設定

ライセンス： すべて

次の例は、Microsoft Active Directory Server の LDAP ログイン認証オブジェクトの詳細設定を示します。この例の LDAP サーバの IP アドレスは 10.11.3.4 です。接続ではアクセスのためにポート 636 が使用されます。



この例では、Example 社の情報テクノロジー ドメインのセキュリティ(Security)部門のベース識別名として `OU=security,DC=it,DC=example,DC=com` が使用されています。ただし、このサーバに基本フィルタ `(cn=*smith)` が設定されていることに注意してください。このフィルタは、サーバから取得するユーザを、一般名が `smith` で終わるユーザに限定します。

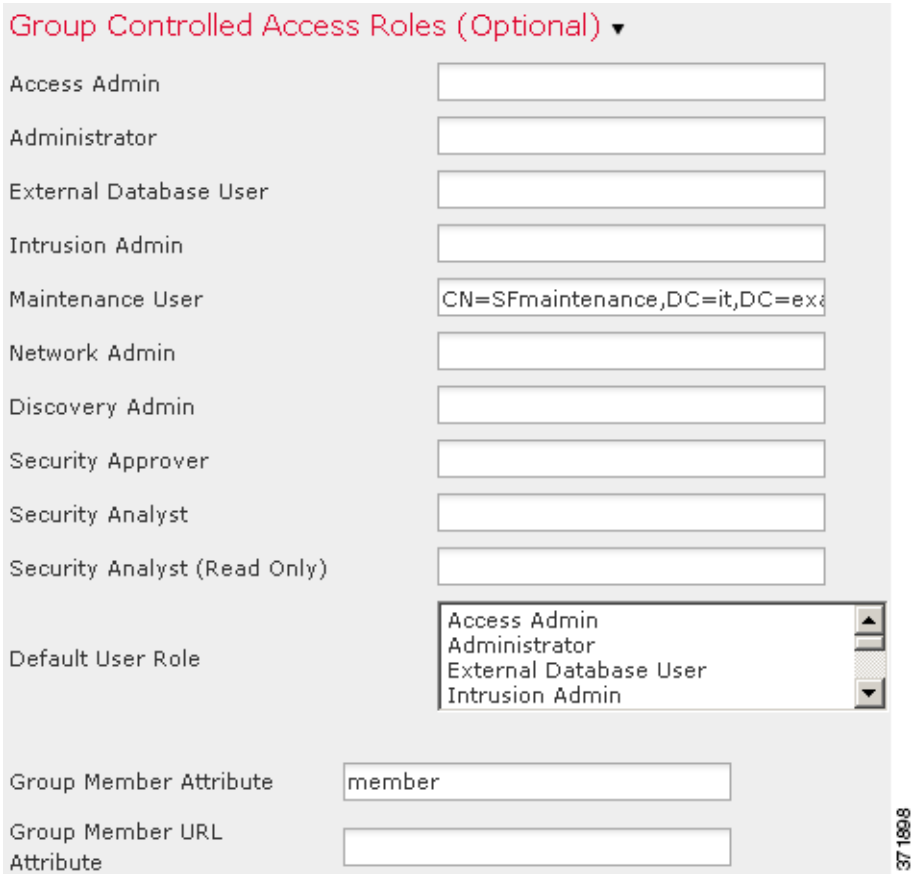


サーバへの接続が SSL を使用して暗号化され、`certificate.pem` という名前の証明書が接続に使用されます。また、[Timeout] の設定により、60 秒経過後にサーバへの接続がタイムアウトします。

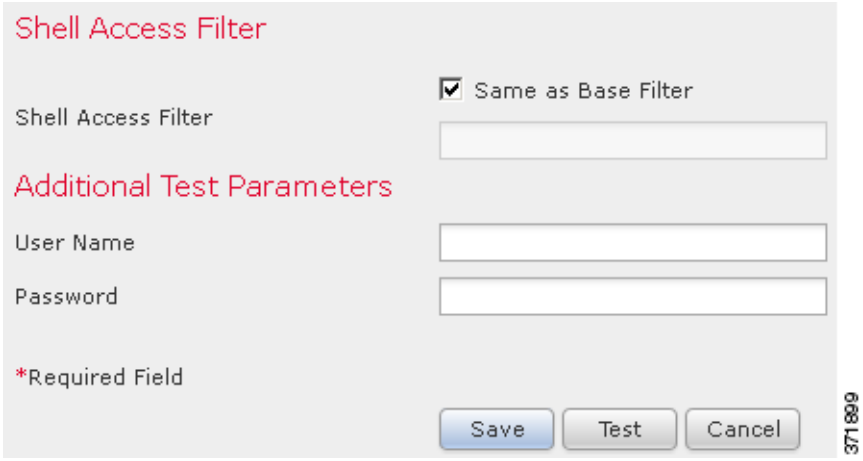
このサーバが Microsoft Active Directory Server であるため、ユーザ名の保存に uid 属性ではなく sAMAccountName 属性が使用されます。設定では、[UI Access Attribute] が sAMAccountName であることに注意してください。その結果、ユーザが FireSIGHT システムへのログインを試行すると、FireSIGHT システムは各オブジェクトの sAMAccountName 属性を検査し、一致するユーザ名を検索します。

また、[Shell Access Attribute] が sAMAccountName の場合、ユーザがアプライアンスでシェル アカウントにログインすると、ディレクトリ内のすべてのオブジェクトの各 sAMAccountName 属性が検査され、一致が検索されます。

この例では、グループ設定も行われます。Maintenance User ロールが、member グループ属性を持ち、ベース ドメイン名が CN=SFmaintenance,DC=it,DC=example,DC=com であるグループのすべてのメンバーに自動的に割り当てられます。



シェル アクセス フィルタは、基本フィルタと同一に設定されます。このため、同じユーザが Web インターフェイスを使用する場合と同様に、シェルを介してアプライアンスにアクセスできます。



LDAP 認証オブジェクトの編集

ライセンス：すべて

既存の認証オブジェクトを編集できます。ポリシーを再適用するまでは、変更内容は反映されません。

認証オブジェクトを編集するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 2　[External Authentication] タブをクリックします。

[External Authentication] ページが表示されます。

ステップ 3　編集するオブジェクトの横にある編集アイコン（ ）をクリックします。

[Create External Authentication Object] ページが表示されます。

ステップ 4　必要に応じてオブジェクト設定を変更します。

ステップ 5　[Test] をクリックします。

テストの成功を示すメッセージ、または欠落しているか訂正する必要がある設定を詳しく示すメッセージが表示されます。テストが成功した場合、テストの出力がページ下部に表示されます。

テストが失敗した場合は、接続のトラブルシューティングの提案事項につて基本 LDAP 認証接続の調整（61-16 ページ）を参照してください。表示されるエラー メッセージに、接続失敗の原因が示されていることに注意してください。

ステップ 6　[Save] をクリックします。

変更が保存され、[External Authentication] ページが表示されます。認証の変更がアプライアンスで行われる前に、オブジェクトが有効に設定されているシステム ポリシーをそのアプライアンスに適用する必要があることに注意してください。詳細については、外部認証の有効化（63-12 ページ）およびシステム ポリシーの適用（63-4 ページ）を参照してください。

RADIUS 認証

Remote Authentication Dial In User Service（RADIUS）は、ネットワーク リソースへのユーザ アクセスの認証、認可、およびアカウンティングに使用される認証プロトコルです。RFC 2865 に準拠するすべての RADIUS サーバで、認証オブジェクトを作成できます。

詳細については、次の項を参照してください。

RADIUS 認証について

ライセンス： すべて

RADIUS サーバで認証されたユーザが初めてログインすると、認証オブジェクトでそのユーザに指定されているロールがユーザに付与されます。どのユーザ ロールにもリストされていないユーザには、認証オブジェクトで選択されているデフォルト アクセス ロールが付与されます。認証オブジェクトでデフォルト アクセス ロールが選択されていない場合は、システム ポリシーのデフォルト アクセス ロールが付与されます。設定が認証オブジェクトのユーザ リストを介して付与されていない場合は、必要に応じてユーザのロールを変更できます。属性照合を使用して RADIUS サーバで認証されたユーザが初めてログインしようとすると、ユーザ アカウントが作成されているためログインが拒否されることに注意してください。ユーザはもう一度ログインする必要があります。

注　シリーズ 3 管理対象デバイスで外部認証を有効にする前に、シェル アクセス フィルタに含まれている外部認証ユーザと同じユーザ名を持つ内部認証シェル ユーザをすべて削除してください。

FireSIGHT システムの RADIUS 実装では、SecurID® トークンの使用がサポートされています。SecurID を使用したサーバによる認証を設定すると、そのサーバに対して認証されているユーザが、SecurID PIN の末尾に SecurID トークンを付加し、Cisco アプライアンスへのログイン時にそれをパスワードとして使用します。SecurID が FireSIGHT システム外部のユーザを認証するように適切に設定されている限り、これらのユーザは PIN と SecurID を使用して FireSIGHT システムにログインでき、アプライアンスでの追加の設定は不要です。

RADIUS 認証オブジェクトの作成

ライセンス： すべて

RADIUS 認証オブジェクトの作成時に、認証サーバに接続できるようにする設定を定義します。また、特定のユーザおよびデフォルト ユーザにユーザ ロールを付与します。RADIUS サーバから、認証予定のユーザのカスタム属性が返される場合は、これらのカスタム属性を定義する必要があります。オプションで、シェル アクセス認証も設定できます。

認証オブジェクトを作成するには、ローカル アプライアンスから、接続する認証サーバに TCP/IP でアクセスできる必要があることに注意してください。

認証オブジェクトを作成するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 2　[External Authentication] タブをクリックします。

[External Authentication] ページが表示されます。

ステップ 3　[Create External Authentication Object] をクリックします。

[Create External Authentication Object] ページが表示されます。

ステップ 4　外部認証のためのユーザ データを取得するプライマリ認証サーバとバックアップ認証サーバを指定し、タイムアウト値と再試行値を設定します。詳細については、RADIUS 接続の設定（61-35 ページ）を参照してください。

ステップ 5　デフォルトのユーザ ロールを設定します。オプションで、ユーザを指定するか、または特定の FireSIGHT システム アクセス ロールを付与するユーザのユーザ属性値を指定します。詳細については、RADIUS ユーザ ロールの設定（61-37 ページ）を参照してください。

ステップ 6　オプションで、管理シェル アクセスを設定します。詳細については、管理シェル アクセスの設定（61-38 ページ）を参照してください。

ステップ 7　認証対象ユーザのプロファイルからカスタム RADIUS 属性が返される場合は、これらの属性を定義します。詳細については、カスタム RADIUS 属性の定義（61-39 ページ）を参照してください。

ステップ 8　認証が成功する必要があるユーザの名前とパスワードを入力して、設定をテストします。詳細については、ユーザ認証のテスト（61-40 ページ）を参照してください。

変更が保存されます。認証の変更がアプライアンスで行われる前に、オブジェクトが有効に設定されているシステム ポリシーをそのアプライアンスに適用する必要があることに注意してください。詳細については、外部認証の有効化（63-12 ページ）およびシステム ポリシーの適用（63-4 ページ）を参照してください。

RADIUS 接続の設定

ライセンス：すべて

RADIUS 認証オブジェクトの作成時には、ローカル アプライアンス（管理対象デバイスまたは Defense Center）が認証のために接続するプライマリおよびバックアップ サーバとサーバ ポートを最初に指定します。

注　RADIUS が正しく機能するためは、ファイアウォールで認証ポートとアカウンティング ポート（デフォルトでは 1812 および 1813）を開く必要があります。

バックアップ認証サーバを指定する場合は、プライマリ サーバへの接続試行操作のタイムアウトを設定できます。プライマリ認証サーバからの応答がない状態で [Timeout] フィールド（または LDAP サーバのタイムアウト）に指定された秒数が経過すると、アプライアンスはプライマリ サーバに対してクエリを再実行します。

アプライアンスがプライマリ認証サーバに対して再クエリを実行した後に、プライマリ認証サーバからの応答がない状態で [Retries] フィールドに指定された回数を超え、[Timeout] フィールドに指定された秒数が再び経過すると、プライアンスはバックアップ サーバにロールオーバーします。

たとえば、プライマリ サーバで RADIUS が無効な場合、アプライアンスはバックアップ サーバに対してクエリを実行します。ただし RADIUS がプライマリ RADIUS サーバのポートで実行されており、何らかの理由（誤った設定またはその他の問題など）で要求の処理を拒否する場合は、バックアップ サーバへのフェールオーバーは行われません。

RADIUS 認証サーバを指定するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 2　[External Authentication] タブをクリックします。

[External Authentication] ページが表示されます。

ステップ 3　[Create External Authentication Object] をクリックします。

[Create External Authentication Object] ページが表示されます。

ステップ 4　[Authentication Method] ドロップダウン リストから [RADIUS] を選択します。

RADIUS 設定オプションが表示されます。

ステップ 5　[Name] フィールドと [Description] フィールドに、認証サーバの名前と説明を入力します。

ステップ 6　認証データを取得するプライマリ RADIUS サーバの IP アドレスまたはホスト名を [Primary Server Host Name/IP Address] フィールドに入力します。

注　シェル認証では IPv6 アドレスはサポートされていません。プライマリ RADIUS サーバに IPv6 アドレスを使用するときにシェル認証を許可するには、サーバの IPv4 アドレスを使用して認証オブジェクトをセットアップし、システム ポリシーの最初の認証オブジェクトとしてその IPv4 オブジェクトを使用します。

ステップ 7　オプションで、[Primary Server Port] フィールドでプライマリ RADIUS 認証サーバが使用するポートを変更します。

注　認証ポート番号とアカウンティング ポート番号が連続番号ではない場合は、このフィールドを空白にします。システムは、アプライアンスの `/etc/services` ファイルの `radius` データと `radacct` データから RADIUS ポート番号を判断します。

ステップ 8　プライマリ RADIUS 認証サーバの秘密キーを [RADIUS Secret Key] フィールドに入力します。

ステップ 9　認証データを取得するバックアップ RADIUS 認証サーバの IP アドレスまたはホスト名を [Backup Server Host Name/IP Address] フィールドに入力します。

ステップ 10　オプションで、[Backup Server Port] フィールドで、バックアップ RADIUS 認証サーバが使用するポートを変更します。

注　認証ポート番号とアカウンティング ポート番号が連続番号ではない場合は、このフィールドを空白にします。システムは、アプライアンスの `/etc/services` ファイルの `radius` データと `radacct` データから RADIUS ポート番号を判断します。

ステップ 11　バックアップ RADIUS 認証サーバの秘密キーを [RADIUS Secret Key] フィールドに入力します。

ステップ 12　[Timeout] フィールドに、接続を再試行するまでの経過秒数を入力します。

ステップ 13　[Retries] フィールドに、バックアップ接続にロールオーバーする前に、プライマリ サーバ接続を試行する回数を入力します。

ステップ 14　RADIUS ユーザ ロールの設定（61-37 ページ）に進みます。

RADIUS ユーザ ロールの設定

ライセンス： すべて

RADIUS サーバで既存のユーザに対してアクセス ロールを指定するには、FireSIGHT システムで使用される各アクセス ロールに対してユーザ名をリストします。これを行うと、RADIUS によって検出された、特定のロールに対して指定されていないユーザのデフォルト アクセス設定を設定できます。

ユーザがログインすると、FireSIGHT システムは RADIUS サーバを検査し、RADIUS 設定に基づいてアクセス権を付与します。

- ユーザに対して特定のアクセス権が設定されておらず、デフォルト アクセス ロールが選択されていない場合、新しいユーザがログインすると、FireSIGHT システムは RADIUS サーバに対してそのユーザを認証してから、システム ポリシーで設定されているデフォルト アクセス ロールに基づいてユーザ権限を付与します。
- 新しいユーザがどのリストにも指定されておらず、認証オブジェクトの [Default User Role] リストでデフォルト アクセス ロールが選択されている場合、ユーザにはこのデフォルト アクセス ロールが割り当てられます。
- 1 つ以上の特定のロールのリストにユーザを追加すると、割り当てられているすべてのアクセス ロールがそのユーザに付与されます。

また、ユーザ名の代わりに属性と値のペアを使用して、特定のユーザ ロールが付与される必要があるユーザを示すこともできます。たとえば、Security Analyst とする必要があるすべてのユーザの [User-Category] 属性の値が [Analyst] である場合、これらのユーザにそのロールを付与するには、[Security Analyst List] フィールドに `User-Category=Analyst` と入力します。カスタム属性を使用してユーザ ロール メンバーシップを設定するには、その前に、カスタム属性を定義する必要があることに注意してください。詳細については、カスタム RADIUS 属性の定義（61-39 ページ）を参照してください。

外部認証されるが、特定のロールにリストされないすべてのユーザに、デフォルトのユーザ ロールを割り当てることができます。[Default User Role] リストでは、複数のロールを選択できます。

FireSIGHT システムでサポートされているユーザ ロールの詳細については、RADIUS ユーザ ロールの設定（61-37 ページ）を参照してください。

FireSIGHT システム ユーザ管理ページで RADIUS ユーザ リスト メンバーシップが設定されているため、アクセス ロールが割り当てられているユーザの最小アクセス権を削除することはできません。ただし、追加の権限を割り当てることはできます。

注意　ユーザの最小アクセス設定を変更するには、[ADIUS Specific Parameters] セクションのリスト間でユーザを移動するかまたは RADIUS サーバでユーザの属性を変更する他に、システム ポリシーを再適用し、ユーザ管理ページで割り当てられているユーザ権限を削除する必要があります。

ユーザ リストに基づいてアクセスを設定するには、次の手順を実行します。

アクセス：Admin

ステップ 1　FireSIGHT システム ユーザ ロールに対応するフィールドに、各ユーザの名前を入力するか、またはこれらのロールに割り当てる必要がある属性と値のペアを指定します。ユーザ名と属性値のペアは、カンマで区切ります。

たとえば、ユーザ `jsmith` と `jdoe` に Administrator ロールを付与する場合は、[Administrator] フィールドに `jsmith, jdoe` と入力します。

もう 1 つの例として、[User-Category] の値が [Maintenance] であるすべてのユーザに Maintenance User ロールを付与するには、[Maintenance User] フィールドに `User-Category=Maintenance` と入力します。

ユーザ アクセス ロールの詳細については、ユーザ ロールの設定（61-52 ページ）を参照してください。

ステップ 2　[Default User Role] リストから、指定のどのグループにも属していないユーザのデフォルト最小アクセス ロールを選択します。

ヒント　複数のロールを選択するには、Ctrl キーを押しながらロール名をクリックします。

ステップ 3　管理シェル アクセスの設定（61-38 ページ）に進みます。

管理シェル アクセスの設定

ライセンス：すべて

RADIUS サーバを使用して、ローカル アプライアンス（管理対象デバイスまたはDefense Center）で、シェル アクセスについてアカウントを認証することもできます。シェル アクセスを付与するユーザのユーザ名を指定します。シェル アクセスは、システム ポリシーの最初の認証オブジェクトでのみ設定できることに注意してください。認証オブジェクトの順序の管理については、外部認証の有効化（63-12 ページ）を参照してください。

注　シェル認証では IPv6 アドレスはサポートされていません。IPv6 アドレスを使用してプライマリ RADIUS サーバを設定し、管理シェル アクセスも設定すると、シェル アクセスの設定は無視されます。プライマリ RADIUS サーバに IPv6 アドレスを使用するときにシェル認証を許可するには、サーバの IPv4 アドレスを使用して別の認証オブジェクトをセットアップし、システム ポリシーの最初の認証オブジェクトとしてそのオブジェクトを使用します。

Admin アカウント以外は、RADIUS 認証オブジェクトで設定したシェル アクセス リストにより、アプライアンスでのシェル アクセスが完全に制御されます。システム ポリシーの適用時に、シェル ユーザはアプライアンスのローカル ユーザとして設定されます。属性照合を使用して RADIUS サーバで認証されたユーザが初めてログインしようとすると、ユーザ アカウントが作成されているためログインが拒否されることに注意してください。ユーザはもう一度ログインする必要があります。

ログイン時に各シェル ユーザのホーム ディレクトリが作成されること、および(RADIUS 接続を無効にすることで)RADIUS シェル アクセス ユーザ アカウントが無効になっている場合はディレクトリが維持されますが、ユーザ シェルは /etc/password 内の /bin/false に設定され、シェルが無効になることに注意してください。ユーザが再度有効になると、同じホーム ディレクトリを使用してシェルがリセットされます。

シェル ユーザは、小文字で構成されたユーザ名を使用してログインすることができます。シェルのログイン認証では大文字と小文字が区別されます。

注意　シリーズ 3 Defense Centerでは、すべてのシェル ユーザに sudoers 特権が付与されます。シェル アクセスが付与されるユーザのリストを適切に制限してください。シリーズ 3 と仮想デバイスでは、外部認証ユーザに付与されるシェル アクセスのデフォルトは、**Configuration** レベルのコマンド ライン アクセスになります。このアクセスでも sudoers 特権が付与されます。

シェル アカウント認証を設定するには、次の手順を実行します。

アクセス: Admin

ステップ 1　[Administrator Shell Access User List] フィールドに、ユーザ名をカンマで区切って入力します。

注　シェル アクセス フィルタを指定しないことを選択すると、認証オブジェクトの保存時に、フィルタを空白のままにすることを確認する警告が表示されます。

ステップ 2　カスタム RADIUS 属性の定義(61-39 ページ)に進みます。

カスタム RADIUS 属性の定義

ライセンス: すべて

RADIUS サーバが、/etc/radiusclient/ 内の dictionary ファイル に含まれていない属性の値を返し、これらの属性を使用してユーザにユーザ ロールを設定する予定の場合は、ログイン認証オブジェクトでこれらの属性を定義する必要があります。

RADIUS サーバでユーザ プロファイルを調べると、ユーザについて返される属性を見つけることができます。

属性を定義する場合は、英数字からなる属性名を指定します。属性名の中の単語を区切るには、スペースではなくダッシュを使用することに注意してください。また、指定する属性 ID は整数であり、etc/radiusclient/dictionary ファイルの既存の属性 ID と競合していてはなりません。属性のタイプ(文字列、IP アドレス、整数、または日付)も指定します。

たとえば、Cisco ルータが接続しているネットワーク上で RADIUS サーバが使用される場合、Ascend-Assign-IP-Pool 属性を使用して、特定の IP アドレス プールからログインするすべてのユーザに特定のロールを付与できます。Ascend-Assign-IP-Pool は、ユーザがログインできるアドレス プールを定義する整数属性であり、割り当てられる IP アドレス プールの番号を示す整数が指定されます。そのカスタム属性を宣言するには、属性名が Ascend-IP-Pool-Definition、属性 ID が 218、属性タイプが integer のカスタム属性を作成します。次に、Ascend-IP-Pool-Definition 属性値が 2 のすべてのユーザに対し、読み取り専用の Security Analyst 権限を付与するには、Ascend-Assign-IP-Pool=2 を [Security Analyst (Read Only)] フィールドに入力します。

RADIUS 認証オブジェクトの作成時に、そのオブジェクトの新しいディクショナリ ファイルが FireSIGHT システム アプライアンスの `/var/sf/userauth` ディレクトリに作成されます。認証オブジェクトに追加するカスタム属性はすべて、そのディクショナリ ファイルに追加されます。

カスタム属性を定義するには、次の手順を実行します。

アクセス： Admin

ステップ 1　矢印をクリックして、[Define Custom RADIUS Attributes] セクションを展開します。

属性フィールドが表示されます。

ステップ 2　[Attribute Name] フィールドに、英数字とダッシュからなる属性名をスペースなしで入力します。

ステップ 3　[Attribute ID] フィールドに、属性 ID を整数形式で入力します。

ステップ 4　[Attribute Type] ドロップダウン リストから、属性のタイプを選択します。

ステップ 5　認証オブジェクトにカスタム属性を追加するには、[Add] をクリックします。

ヒント　認証オブジェクトからカスタム属性を削除するには、その属性の横にある [Delete] をクリックします。

ステップ 6　ユーザ認証のテスト（61-40 ページ）に進みます。

ユーザ認証のテスト

ライセンス： すべて

RADIUS 接続、ユーザ ロール、およびカスタム属性を設定したら、これらの設定をテストするため、認証できる必要があるユーザのユーザ資格情報を指定できます。

ユーザ名として、テストするユーザのユーザ名を入力できます。

UI のページ サイズ制限により、ユーザ数が 1000 を超えているサーバへの接続をテストする場合、返されるユーザの数は 1000 であることに注意してください。

ヒント　テスト ユーザの名前とパスワードを誤って入力すると、サーバ設定が正しい場合でもテストが失敗します。サーバ設定が正しいことを確認するには、最初に [Additional Test Parameters] フィールドにユーザ情報を入力せずに [Test] をクリックします。正常に完了した場合は、テストする特定ユーザのユーザ名とパスワードを指定します。

ユーザ認証をテストするには、次の手順を実行します。

アクセス： Admin

ステップ 1　[User Name] フィールドと [Password] フィールドに、RADIUS サーバへのアクセスの検証に資格情報が使用されるユーザのユーザ名とパスワードを入力します。

たとえば、Example 社の `jsmith` のユーザ資格情報を取得できるかどうかをテストするには、`jsmith` と入力します。

ステップ 2　[Show Details] を選択し、[Test] をクリックします。

テストの成功を示すメッセージ、または欠落しているか訂正する必要がある設定を詳しく示すメッセージが表示されます。

ステップ 3　テストが成功した場合は [Save] をクリックします。

[External Authentication] ページが表示され、このページに新しいオブジェクトが示されます。

アプライアンスでオブジェクトを使用して RADIUS 認証を有効にするには、そのオブジェクトが有効に設定されているシステム ポリシーをアプライアンスに適用する必要があります。詳細については、外部認証の有効化（63-12 ページ）およびシステム ポリシーの適用（63-4 ページ）を参照してください。

RADIUS 認証オブジェクトの例

ライセンス： すべて

ここでは、RADIUS サーバ認証オブジェクトの例を示し、FireSIGHT システム RADIUS 認証機能をどのように使用できるかを示します。詳細については、次の項を参照してください。

- 例：RADIUS を使用したユーザの認証（61-41 ページ）
- 例：カスタム属性を使用したユーザの認証（61-43 ページ）

例：RADIUS を使用したユーザの認証

ライセンス： すべて

次の図は、IP アドレスが 10.10.10.98 で FreeRADIUS が稼働しているサーバのサンプル RADIUS ログイン認証オブジェクトを示します。接続ではアクセスのためにポート 1812 が使用されること、および不使用期間が 30 秒を経過するとサーバ接続がタイムアウトになり、バックアップ認証サーバへの接続試行前に、サーバ接続が 3 回再試行されることに注意してください。

次の例は、RADIUS ユーザ ロール設定の重要な特徴を示します。

- ユーザ `ewharton` と `gsand` には、この認証オブジェクトが有効になっている FireSIGHT システム アプライアンスへの管理アクセスが付与されます。
- ユーザ `cbronte` には、この認証オブジェクトが有効になっている FireSIGHT システム アプライアンスへの Maintenance User アクセスが付与されます。
- ユーザ `cbronte` には、この認証オブジェクトが有効になっている FireSIGHT システム アプライアンスへの Security Analyst アクセスが付与されます。
- ユーザ `ewharton` は、シェル アカウントを使用してアプライアンスにログインできます。

次の図に、この例のロール設定を示します。

RADIUS-Specific Parameters

Timeout (Seconds)	30
Retries	3
Access Admin	
Administrator	ewharton, gsand
External Database User	
Intrusion Admin	
Maintenance User	
Network Admin	
Discovery Admin	
Security Approver	
Security Analyst	
Security Analyst (Read Only)	MS-RAS-Version=MSRASV5.00
Default User Role	Access Admin Administrator External Database User Intrusion Admin

Shell Access Filter

Administrator Shell Access User List	ewharton

Define Custom RADIUS Attributes

Attribute Name	Attribute ID	Attribute Type		
		string	Add	
MS-Ras-Version	18	string	Delete	

371901

例：カスタム属性を使用したユーザの認証

ライセンス：すべて

属性と値のペアを使用して、特定のユーザ ロールが付与される必要があるユーザを示すこともできます。使用する属性がカスタム属性の場合、そのカスタム属性を定義する必要があります。

次の図は、前述の例と同じ FreeRADIUS サーバのサンプル RADIUS ログイン認証オブジェクトでのロール設定とカスタム属性の定義を示します。

ただしこの例では、Microsoft リモート アクセス サーバが使用されているため、1 つ以上のユーザの `MS-RAS-Version` カスタム属性が返されます。`MS-RAS-Version` カスタム属性は文字列であることに注意してください。この例では、Microsoft v. 5.00 リモート アクセス サーバ経由で RADIUS にログインするすべてのユーザに対し、Security Analyst（読み取り専用）ロールが付与される必要があります。このため、属性と値のペア `MS-RAS-Version=MSRASV5.00` を [Security Analyst (Read Only)] フィールドに入力します。

RADIUS-Specific Parameters

Timeout (Seconds)	30
Retries	3
Access Admin	
Administrator	ewharton, gsand
External Database User	
Intrusion Admin	
Maintenance User	
Network Admin	
Discovery Admin	
Security Approver	
Security Analyst	
Security Analyst (Read Only)	MS-RAS-Version=MSRASV5.00
Default User Role	Access Admin Administrator External Database User Intrusion Admin

Shell Access Filter

Administrator Shell Access User List	ewharton

▾ Define Custom RADIUS Attributes

Attribute Name	Attribute ID	Attribute Type	
		string	Add
MS-Ras-Version	18	string	Delete

371901

RADIUS 認証オブジェクトの編集

ライセンス：すべて

既存の認証オブジェクトを編集できます。オブジェクトがシステム ポリシーで使用されている場合、ポリシーが適用された時点での設定が、ポリシーを再適用するまで有効になります。

認証オブジェクトを編集するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 2　[External Authentication] タブをクリックします。

[External Authentication] ページが表示されます。

ステップ 3　編集するオブジェクトの横にある編集アイコン（  ）をクリックします。

[Create External Authentication Object] ページが表示されます。

ステップ 4　必要に応じてオブジェクト設定を変更します。

ステップ 5　[Save] をクリックします。

変更が保存され、[External Authentication] ページが再び表示されます。認証の変更がアプライアンスで行われる前に、オブジェクトが有効に設定されているシステム ポリシーをそのアプライアンスに適用する必要があることに注意してください。詳細については、外部認証の有効化（63-12 ページ）およびシステム ポリシーの適用（63-4 ページ）を参照してください。

認証オブジェクトの削除

ライセンス：すべて

削除できる認証オブジェクトは、システム ポリシーで現在有効ではない認証オブジェクトです。

認証オブジェクトを削除するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 2　[External Authentication] タブをクリックします。

[External Authentication] ページが表示されます。

ステップ 3　削除するオブジェクトの横にある削除アイコン（  ）をクリックします。

オブジェクトが削除され、[External Authentication] ページが表示されます。

ユーザ アカウントの管理

ライセンス： すべて

Administration アクセスが付与されている場合は、Web インターフェイスを使用してDefense Centerまたは管理対象デバイスでユーザ アカウントを表示および管理（アカウントの追加、変更、削除など）できます。また、カスタム ユーザ ロールを作成および変更し、ユーザ ロール エスカレーションを設定できます。Administrator アクセスのないユーザ アカウントでは、管理機能へのアクセスが制限されています。表示されるナビゲーション メニューは、ユーザのタイプによって異なります。

ユーザ アカウントの管理の詳細については、次の項を参照してください。

- ユーザ アカウントの表示（61-46 ページ）では、[User Management] ページへのアクセス方法を説明します。このページでは、ユーザ アカウントを追加、アクティブ化、非アクティブ化、編集、削除できます。
- 新しいユーザ アカウントの追加（61-47 ページ）では、新しいユーザ アカウントを追加するときに使用できるさまざまなオプションについて説明します。
- コマンド ライン アクセスの管理（61-48 ページ）では、仮想デバイスまたは シリーズ 3 のローカル デバイス ユーザにコマンド ライン インターフェイス アクセス権を割り当てる方法について説明します。
- 外部認証ユーザ アカウントの管理（61-50 ページ）では、外部認証ユーザの追加方法と、FireSIGHT システム内で管理できるユーザ設定の内容を説明します。
- ユーザ特権とオプションの変更（61-58 ページ）では、既存のユーザ アカウントにアクセスして変更する方法を説明します。
- 制限付きユーザ アクセス プロパティについて（61-59 ページ）では、制限付きデータ アクセスを使用して、ユーザ アカウントに対して使用可能なデータを制限する方法を説明します。
- ユーザ アカウントの削除（61-60 ページ）では、ユーザ アカウントを削除する方法について説明します。
- アカウント特権について（61-60 ページ）には、各種ユーザ アカウントでアクセスできるメニューとオプションをまとめた表が収録されています。

ユーザ アカウントの表示

ライセンス： すべて

[User Management] ページでは、既存のアカウントを表示、編集、削除できます。[Authentication Method] カラムでユーザの認証タイプを確認できます。[Password Lifetime] カラムには、ユーザ パスワードの残りの有効日数が示されます。[Action] カラムのアイコンを使用して、ユーザの詳細を編集したり、ユーザをアクティブまたは非アクティブにしたりできます。外部認証ユーザの場合、サーバの認証オブジェクトが無効であると、[Authentication Method] カラムに [External (Disabled)] が表示されます。

[User Management] ページにアクセスするには、次の手順を実行します。

アクセス： Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページに、各ユーザと、ユーザ アカウントのアクティブ化、非アクティブ化、編集、または削除のオプションが表示されます。

[User Management] ページで実行できるアクションについては、次の項を参照してください。

- 新しいユーザ アカウントの追加（61-47 ページ）
- ユーザ ロールの設定（61-52 ページ）
- ユーザ特権とオプションの変更（61-58 ページ）
- 制限付きユーザ アクセス プロパティについて（61-59 ページ）
- ユーザ パスワードの変更（61-59 ページ）
- ユーザ アカウントの削除（61-60 ページ）

新しいユーザ アカウントの追加

ライセンス： すべて

サポートされるデバイス： 機能によって異なる

新しいユーザ アカウントをセットアップするときに、そのアカウントでアクセスできるシステムの部分を制御できます。ユーザ アカウントの作成時に、ユーザ アカウントのパスワードの有効期限と強度を設定できます。シリーズ 3 デバイスのローカル アカウントの場合、ユーザに付与するコマンド ライン アクセスのレベルも設定できます。

新規のユーザを追加するには、次の手順を実行します。

アクセス： Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 2　[Create User] をクリックします。

[Create User] ページが表示されます。

ステップ 3　[User Name] フィールドに、新しいユーザの名前を入力します。

新しいユーザ名は、英数字とハイフン文字のみからなり、スペースを使用せず、32 文字以下の長さにする必要があります。ユーザ名では、大文字と小文字が区別されます。

ステップ 4　このユーザがログイン時に外部ディレクトリ サーバに対して認証されるようにするには、[Use External Authentication Method] を選択します。

このオプション有効にすると、パスワード管理オプションが非表示になります。ユーザのアクセス ロールの設定を続行するには、ステップ 8 に移動してください。

外部ディレクトリ サーバに対してユーザを認証する場合は、Defense Centerを使用して、使用するサーバの認証オブジェクトを作成し、次に認証が有効な状態でシステム ポリシーを適用します。また、これらのユーザが FireSIGHT システム アプライアンスにログインするには、外部認証サーバが使用可能である必要があります。詳細については、認証オブジェクトの管理（61-5 ページ）および外部認証の有効化（63-12 ページ）を参照してください。

ステップ 5　[Password] および [Confirm Password] フィールドに、パスワード（最大 32 文字の英数字）を入力します。

パスワード強度の検査を有効にする場合は、パスワードは 8 文字以上の英数字からなり、大文字と小文字を使用し、1 つ以上の数字と 1 つ以上の特殊文字を使用する必要があります。辞書に記載されている単語や、同じ文字を連続して繰り返し使用することはできません。

注　アプライアンスで STIG 準拠を有効にするには、シェル アクセス ユーザのパスワード設定の詳細について『*FireSIGHT システムSTIG Release Notes*』を参照してください。

ステップ 6　その他のユーザ アカウント ログイン オプションを設定します。

詳細については、ユーザ アカウント ログイン オプションの表を参照してください。

ステップ 7　シリーズ 3 デバイスの Web インターフェイスでローカル ユーザを作成する場合は、[Command-Line Interface Access] でユーザのコマンド ライン インターフェイス アクセス レベルを割り当てることができます。

- ユーザに対しコマンド ラインへのアクセスを無効にするには、[None] を選択します。
- ユーザがシェルにログインし、特定のコマンド サブセットにアクセスできるようにするには、[Basic] を選択します。
- ユーザがシェルにログインし、すべてのコマンド ライン オプション（アプライアンスでエキスパート モードが有効な場合はエキスパート モードも含む）を使用できるようにするには、[Configuration] を選択します。

  コマンド ライン アクセスの詳細については、コマンド ライン アクセスの管理（61-48 ページ）を参照してください。

ステップ 8　ユーザに付与するアクセス ロールを選択します。

注　すべての物理管理対象デバイスでは、Ciscoから提供される事前定義のユーザ ロールは、Administrator、Maintenance User、および Security Analyst に限定されています。

詳細については、ユーザ ロールの設定（61-52 ページ）を参照してください。

ステップ 9　[Save] をクリックします。

ユーザが作成され、[User Management] ページが再度表示されます。

ヒント　[User Management] ページの内部認証ユーザの名前の横にあるスライダをクリックして、非アクティブなユーザを再度アクティブにするか、またはアクティブ ユーザ アカウントを削除せずに無効にします。

コマンド ライン アクセスの管理

ライセンス： すべて

サポートされるデバイス： シリーズ 3、仮想

シリーズ 3 または仮想デバイスでは、コマンド ライン インターフェイス アクセスをローカル デバイス ユーザに割り当てることができます。

仮想デバイスのユーザにコマンド ライン アクセスを割り当てることができますが、コマンドはコマンド ライン インターフェイスから使用することに注意してください。詳細については、コマンドライン リファレンス（D-1 ページ）を参照してください。

ユーザが実行できるコマンドは、ユーザに割り当てられているアクセスのレベルによって決まります。[Command-Line Interface Access] を [None] に設定すると、ユーザはコマンド ラインでアプライアンスにログインできなくなります。ユーザが資格情報を指定すると、ユーザが開始したセッションはすべて閉じます。ユーザ作成時に、アクセス レベルはデフォルトで [None] に設定されます。[Command-Line Interface Access] を [Basic] に設定すると、ユーザは特定のコマンド セットだけを実行できます。

表 61-3　基本のコマンド ライン コマンド

configure password	**インターフェイス**
end	lcd
exit	link-state
help	log-ips-connection
history	managers
logout	**メモリ**
?	model
??	mpls-depth
access-control-config	NAT
アラーム	network
arp-tables	network-modules
audit-log	ntp
bypass	perfstats
clustering	portstats
cpu	power-supply-status
database	process-tree
device-settings	**プロセス**
disk	routing-table
disk-manager	serial-number
dns	stacking
expert	summary
fan-status	time
fastpath-rules	traffic-statistics
GUI	version
hostname	virtual-routers
hyperthreading	virtual-switches
inline-sets	

[Command-Line Interface Access] を [Configuration] に設定すると、ユーザはすべてのコマンド ライン オプションにアクセスできます。このアクセス レベルをユーザに割り当てるときには注意してください。

注意　外部認証ユーザに付与されるシェル アクセスは、デフォルトで [Configuration] レベルのコマンド ライン アクセスになります。これにより、すべてのコマンド ライン ユーティリティの権限が付与されます。外部認証ユーザのシェル アクセスの詳細については、シェル アクセスについて（61-9 ページ）およびシェル アクセスの設定（61-26 ページ）を参照してください。

外部認証ユーザ アカウントの管理

ライセンス： すべて

外部認証が有効になっているアプライアンスに外部認証ユーザがログインすると、認証オブジェクトでグループ メンバーシップを指定して設定したデフォルト アクセス ロールが、アプライアンスによりユーザに付与されます。アクセス グループ設定を設定していない場合、アプライアンスは、システム ポリシーで設定されているデフォルト ユーザ ロールを付与します。ただし、ユーザがアプライアンスにログインする前に、ユーザをローカルで追加すると、[User Management] ページで設定するユーザ特権によってデフォルト設定がオーバーライドされます。

デフォルト ユーザ ロールの選択の詳細については、外部認証の有効化（63-12 ページ）およびユーザ特権について（61-4 ページ）を参照してください。外部認証ユーザのデフォルト ユーザ ロールとして、事前定義のユーザ ロールとカスタム ユーザ ロールの両方を設定できることに注意してください。詳細については、ユーザ ロールの設定（61-52 ページ）を参照してください。

次のすべての条件が満たされている場合には、内部認証ユーザが外部認証に変換されます。

- LDAP（CAC を使用する場合および使用しない場合）または RADIUS 認証を有効にしている。
- LDAP サーバまたは RADIUS サーバでユーザに対して同一ユーザ名が存在する。
- ユーザが、LDAP または RADIUS サーバに保存されているそのユーザのパスワードを使用してログインする。

Defense Centerではシステム ポリシーの外部認証だけを有効にできることに注意してください。管理対象デバイスで外部認証を使用するには、Defense Centerを使用して管理対象デバイスにポリシーを適用する必要があります。

外部認証ユーザがアプライアンスに初めてログインすると、アプライアンスは、ローカル ユーザ レコードを作成して、これらの資格情報を一連のアクセス許可に関連付けます。ユーザ ログインの詳細については、アプライアンスへのログイン（2-1 ページ）を参照してください。初回ログイン後、そのローカル ユーザ レコードのアクセス許可がグループ メンバーシップまたはリスト メンバーシップを介して付与されていない場合は、そのアクセス許可を以下のように変更できます。

- 外部認証ユーザ アカウントのデフォルト ロールとして特定のアクセス ロールが設定されている場合、ユーザは外部アカウント資格情報を使用してアプライアンスにログインでき、この際にシステム管理者による追加の設定は必要ありません。
- アカウントが外部で認証され、デフォルトではアクセス権限が付与されない場合、ユーザはログインできますが、どの機能にもアクセスできません。その後で、ユーザ（またはシステム管理者）は、アクセス許可を変更して、ユーザ機能への適切なアクセスを付与できます。

ヒント システムでは、シェル アクセス ユーザのローカル ユーザ アカウントは作成されません。シェル アクセスは、LDAP サーバに対して設定されている PAM ログイン属性またはシェル アクセス フィルタ、または RADIUS サーバのシェル アクセス リストのいずれかを使用して完全に制御されます。

ユーザ アクセスの変更の詳細については、ユーザ特権とオプションの変更（61-58 ページ）を参照してください。FireSIGHT システム インターフェイスでは、外部認証ユーザのパスワード管理および外部認証ユーザの非アクティブ化は実行できないことに注意してください。外部認証ユーザの場合、LDAP グループ メンバーシップ、RADIUS リスト メンバーシップ、または属性値によってアクセス ロールが割り当てられているユーザの FireSIGHT システム ユーザ管理ページでは、最小アクセス権を削除することができません。外部認証ユーザの [Edit User] ページでは、外部認証サーバの設定により付与された権限は、[Externally Modified] ステータスでマークされます。

ただし、追加の権限を割り当てることはできます。外部認証ユーザのアクセス権を変更すると、[User Management] ページの [Authentication Method] カラムに、[External - Locally Modified] というステータスが表示されます。

シェル ユーザは、小文字で構成されたユーザ名を使用してログインすることができます。シェルのログイン認証では大文字と小文字が区別されます。

注意　シリーズ 3 Defense Centerでは、すべてのシェル ユーザに `sudoers` 特権が付与されます。シェル アクセスが付与されるユーザのリストを適切に制限してください。シリーズ 3 と仮想デバイスでは、外部認証ユーザに付与されるシェル アクセスのデフォルトは、**Configuration** レベルのコマンド ライン アクセスになります。このアクセスでも `sudoers` 特権が付与されます。シェル アクセスのセットアップの詳細については、シェル アクセスについて（61-9 ページ）およびシェル アクセスの設定（61-26 ページ）を参照してください。

ユーザ ログイン設定の管理

ライセンス： すべて

各ユーザ アカウントのパスワードの変更方法と変更する条件、およびユーザ アカウントが無効になる条件を制御できます。Web インターフェイス ログイン セッションのタイムアウトを設定している場合は、このタイムアウトからユーザを除外できます。次の表に、パスワードおよびアカウント アクセスの調整に使用できるオプションの一部について説明します。

シリーズ 3 管理対象デバイス上のローカル認証ユーザの場合、Web インターフェイスのユーザ パスワードを変更すると、コマンド ライン インターフェイスのパスワードも変更されることに注意してください。

[Check Password Strength] オプションを有効にすると、最小パスワード長が自動的に 8 文字に設定されます。また、[Minimum Password Length] に 8 文字を超える値を設定すると、いずれか大きい方の値が適用されます。

注　[Use External Authentication Method] を有効にした後は、ログイン オプションが表示されなくなります。ログイン設定の管理に外部認証サーバを使用します。

表 61-4　ユーザ アカウント ログイン オプション

オプション	説明
Use External Authentication Method	このユーザの資格情報を外部で認証する場合に、このチェック ボックスをオンにします。 **注**　ユーザに対してこのオプションを選択した場合に外部認証サーバが使用できないと、そのユーザは Web インターフェイスにログインできますが、どの機能にもアクセスできません。
Maximum Number of Failed Logins	各ユーザが、ログイン試行の失敗後に、アカウントがロックされるまでに試行できるログインの最大回数を示す整数を、スペースなしで入力します。デフォルト設定は 5 回です。ログイン失敗回数を無制限にするには、0 を使用します。
Minimum Password Length	ユーザのパスワードの必須最小長（文字数）を示す整数を、スペースなしで入力します。デフォルト設定は `8` です。値 `0` は、最小長が必須ではないことを示します。

表 61-4　ユーザ アカウント ログイン オプション（続き）

オプション	説明
Days Until Password Expiration	ユーザのパスワードの有効期限までの日数を入力します。デフォルト設定は 0 で、パスワードは期限切れにならないことを示します。
Days Before Password Expiration Warning	パスワードが実際に期限切れになる何日前に、ユーザがパスワードを変更する必要があるという警告が表示されるかを入力します。デフォルト設定は 0 日間です。 **注意**　警告日数は、パスワードの残りの有効期間の日数**未満**である必要があります。
Force Password Reset on Login	初回ログイン時に、ユーザが強制的に各自のパスワードを変更するようにするには、このオプションを選択します。
Check Password Strength	強力なパスワードを必須にするには、このオプションを選択します。強力なパスワードは 8 文字以上の英数字からなり、大文字と小文字を使用し、1 つ以上の数字と 1 つ以上の特殊文字を使用する必要があります。辞書に記載されている単語や、同じ文字を連続して繰り返し使用することはできません。
Exempt from Browser Session Timeout	操作が行われなかったことが原因でユーザのログイン セッションが終了しないようにするには、このオプションを選択します。Administrator ロールが割り当てられているユーザを除外することはできません。セッション タイムアウトの詳細については、ユーザ インターフェイスの設定（63-30 ページ）を参照してください。

ユーザ ロールの設定

ライセンス：すべて

各 FireSIGHT システム ユーザには、1 つ以上のユーザ アクセス ロールが関連付けられています。たとえばアナリストは、ネットワークのセキュリティを分析するためイベント データへのアクセスが必要ですが、FireSIGHT システム自体の管理機能へのアクセスが必要となることはありません。たとえばユーザ ロールを使用して、アナリストには Security Analyst アクセスを付与し、FireSIGHT システムを管理する 1 人以上のユーザに対して Administrator ロールを予約しておくことができます。FireSIGHT システムには、さまざまな管理者とアナリスト向けに設計された 10 の事前定義ユーザ ロールがあります。また、特殊なアクセス権限を含むカスタム ユーザ ロールを作成できます。

ユーザがアクセスできる Web インターフェイスのメニューとその他のオプションは、ロールによって異なります。事前定義のユーザ ロールには、一連の事前定義のアクセス権限が含まれており、カスタム ユーザ ロールには、作成者が指定する詳細なアクセス権限が含まれています。

[User Roles] ページでユーザ ロールを設定します。

[User Roles] ページにアクセスするには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 2　[User Roles] タブをクリックします。

[User Roles] ページが表示され、すべての事前定義ユーザ ロールとカスタム ユーザ ロール、およびロールのアクティブ化、非アクティブ化、編集、コピー、削除、エクスポートのためのオプションが表示されます。

この 2 種類のユーザ ロールの設定の詳細については、次の項を参照してください。

- 事前定義ユーザ ロールの管理（61-53 ページ）
- カスタム ユーザ ロールの管理（61-55 ページ）
- 事前定義ユーザ ロールのカスタム コピーの作成（61-57 ページ）
- カスタム ユーザ ロールの削除（61-58 ページ）

事前定義ユーザ ロールの管理

ライセンス： すべて

FireSIGHT システムには、組織のニーズに対応するためのさまざまなアクセス権限セットを提供する 10 の事前定義ユーザ ロールがあります。[User Roles] ページでは、事前定義ユーザ ロールに「Cisco Provided」というラベルが付いています。管理対象デバイスは、10 の事前定義ユーザ ロールのうち 3 つのユーザ ロール（Administrator、Maintenance User、および Security Analyst）にだけアクセスできることに注意してください。

事前定義ユーザ ロールは編集できませんが、そのアクセス権限セットをカスタム ユーザ ロールのベースとして使用できます。カスタム ユーザ ロールの作成と編集については、カスタム ユーザ ロールの管理（61-55 ページ）を参照してください。また、事前定義ユーザ ロールを編集できないため、事前定義ユーザ ロールが別のユーザ ロールにエスカレーションするように設定することができません。詳細については、ユーザ ロール エスカレーションの管理（61-69 ページ）を参照してください。

次の表に、使用可能な事前定義ロールの簡単な説明を示します。各ロールで使用可能なメニューおよびオプションのリストについては、アカウント特権について（61-60 ページ）を参照してください。

表 61-5　事前定義ユーザ ロール

ユーザ ロール	権限
Access Admin	アクセス制御、SSL インスペクション、およびファイル ポリシー機能にアクセスするためのアクセス権を提供します。ただし、Access Admin はアクセス制御ポリシーを適用することはできません。Access Admin は、[Policies] メニューでアクセス制御、SSL インスペクション、およびファイル関連オプションにアクセスできます。
Administrator	分析およびレポート機能、ルールおよびポリシーの設定、システム管理、およびすべての保守機能へのアクセスを提供します。Administrator はすべてのメニュー オプションにアクセスできるため、セッションでセキュリティが侵害されると、高いセキュリティ リスクが生じます。このため、ログイン セッション タイムアウトから Administrator を除外することはできません。 セキュリティ上の理由から、Administrator ロールの使用を制限する必要があることに注意してください。 このロールは、管理対象デバイスでも使用可能です。
Discovery Admin	ネットワーク検出、相関、およびユーザ アクティビティ機能へのアクセスを提供します。Discovery Admin は、[Policies] メニューの関連オプションにアクセスできます。

表 61-5　事前定義ユーザ（続き）ロール

ユーザ ロール	権限
External Database User	JDBC SSL 接続をサポートするアプリケーションを使用した FireSIGHT システム データベースへの読み取り専用アクセスを提供します。サードパーティ アプリケーションを FireSIGHT システム アプライアンスに対して認証するには、データベースへのアクセスの有効化（64-7 ページ）の説明に従い、システム設定でデータベース アクセスを有効にする必要があることに注意してください。Web インターフェイスでは、External Database User は [Help] メニューのオンライン ヘルプ関連オプションだけにアクセスできます。このロールの機能には Web インターフェイスが含まれていないため、容易なサポートとパスワード変更の目的でのみアクセスが提供されます。
Intrusion Admin	すべての侵入ポリシー、侵入ルール、およびネットワーク解析ポリシーの機能にアクセスするためのアクセス権を提供します。Intrusion Admin は、[Policies] メニューの侵入関連オプションにアクセスできます。Intrusion Admin は、侵入またはネットワーク解析ポリシーをアクセス制御ポリシーの一部として適用できないことに注意してください。
Maintenance User	監視機能と保守機能へのアクセスを提供します。Maintenance User は、[Health] メニューと [System] メニューの保守関連オプションにアクセスできます。 このロールは、管理対象デバイスでも使用可能です。
ネットワーク管理者	アクセス制御、SSL インスペクション、およびデバイス設定機能にアクセスするためのアクセス権を提供します。Network Admin は、アクセス制御、SSL インスペクション、および [Policies] メニューと [Devices] メニューのデバイス関連オプションにアクセスできます。
Security Analyst	セキュリティ イベント分析機能（イベント ビュー、レポート、ホスト、ホスト属性、サービス、脆弱性、クライアント アプリケーション、ヘルス イベントへの読み取り専用アクセスなど）へのアクセスを提供します。Security Analyst は、[Overview]、[Analysis]、[Health]、および [System] メニューの分析関連オプションにアクセスできます。 このロールは、管理対象デバイスでも使用可能です。
Security Analyst (Read Only)	セキュリティ イベント分析機能（イベント ビュー、レポート、ホスト、ホスト属性、サービス、脆弱性、クライアント アプリケーション、ヘルス イベントなど）への読み取り専用アクセスを提供します。Security Analyst は、[Overview]、[Analysis]、[Health]、および [System] メニューの分析関連オプションにアクセスできます。
Security Approver	アクセス制御、侵入、ファイル、SSL、およびネットワーク検出ポリシーへの制限付きアクセスを提供します。Security Approver は、これらのポリシーを表示し、ネットワーク検出、侵入、およびアクセス制御ポリシーを適用できますが、ポリシーを変更することはできません。[Policies] メニューのポリシー関連オプションにアクセスできます。

ユーザに Event Analyst ロールを割り当てるときに、そのユーザの削除権限を、そのユーザにより作成されるレポート プロファイル、検索、ブックマーク、カスタム テーブル、およびカスタム ワークフローの削除だけに制限できます。詳細については、新しいユーザ アカウントの追加（61-47 ページ）を参照してください。

その他のロールが割り当てられていない外部認証ユーザには、LDAP または RADIUS 認証オブジェクトとシステム ポリシーでの設定に基づいて最小アクセス権が付与されることに注意してください。追加の権限をこれらのユーザに割り当てることができますが、最小アクセス権を削除または変更するには、次の操作を行う必要があります。

- 認証オブジェクト内のリスト間でユーザを移動するか、または外部認証サーバのユーザの属性値またはグループ メンバーシップを変更します。
- システム ポリシーを再度適用します。
- [User Management] ページでそのユーザ アカウントからアクセスを削除します。

事前定義ユーザ ロールは削除できませんが、非アクティブにすることができます。ロールを非アクティブにすると、そのロールが割り当てられているすべてのユーザから、そのロールと関連するアクセス許可が削除されます。

注意　非アクティブにされたロールが、特定のユーザに割り当てられていた唯一のロールである場合、そのユーザはログインして [User Preferences] メニューにアクセスできますが、FireSIGHT システムにはアクセスできません。

ユーザ ロールをアクティブ化または非アクティブ化するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 2　[User Roles] タブをクリックします。

[User Roles] ページが表示されます。

ステップ 3　アクティブまたは非アクティブにするユーザ ロールの横にあるスライダをクリックします。

注　Lights-Out Management を含むロールが割り当てられているユーザがログインしているときに、このロールを非アクティブにしてから再度アクティブにする場合、またはユーザのログイン セッション中にバックアップからユーザまたはユーザ ロールを復元する場合、そのユーザは Web インターフェイスに再度ログインして、IPMItool コマンドへのアクセスを再度取得する必要があります。詳細については、Lights-Out 管理の使用（64-28 ページ）を参照してください。

カスタム ユーザ ロールの管理

ライセンス：すべて

事前定義ユーザ ロールの他に、特別なアクセス権限を含むカスタム ユーザ ロールを作成できます。カスタム ユーザ ロールには、メニューベースのアクセス許可およびシステム アクセス許可の任意のセットを割り当てることができます。また、最初から独自に作成したり、事前定義されたユーザ ロールを基に作成したりできます。事前定義ユーザ ロールと同様に、カスタム ロールは外部認証ユーザのデフォルト ロールとして使用できます。事前定義ロールとは異なり、カスタム ロールは変更、削除できます。

選択可能なアクセス許可は階層構造になっており、FireSIGHT システム メニュー レイアウトに基づいています。アクセス許可にサブページが含まれているか、または単純なページ アクセスよりも詳細なアクセス許可が含まれている場合、このアクセス許可は拡張可能です。その場合、上位アクセス許可によって、ページ ビュー アクセス、およびそのページの関連機能への詳細な下位アクセス権が付与されます。たとえば [Correlation Events] アクセス許可は [Correlation Events] ページへのアクセスを付与し、[Modify Correlation Events] チェック ボックスは、ユーザがそのページで使用可能な情報を編集、削除できるようにします。「Manage」という単語が含まれているアクセス許可は、他のユーザが作成する情報を編集および削除できる権限を付与します。

ヒント　メニュー構造に含まれていないページまたは機能の権限は、上位または関連ページにより付与されます。たとえば、Modify Intrusion Policy 特権があれば、ネットワーク解析ポリシーの変更もできます。

カスタム ユーザ ロールに制限付き検索を適用できます。これにより、イベント ビューアでユーザに対して表示されるデータが制限されます。制限付き検索を設定するには、最初に、プライベートの保存済み検索を作成し、該当するメニュー ベースのアクセス許可の下で、[Restricted Search] ドロップダウン メニューからその検索を選択します。詳細については、検索の実行（60-2 ページ）を参照してください。

Defense Centerでカスタム ユーザ ロールを設定するときには、すべてのメニュー ベースのアクセス許可を付与できます。管理対象デバイスでカスタム ユーザ ロールを設定するときには、デバイス機能に関連する一部のアクセス許可だけを使用できます。設定できるメニュー ベースのアクセス許可と、事前定義ユーザ ロールとの関係については、次の項を参照してください。

- [Analysis] メニュー（61-62 ページ）
- [Policies] メニュー（61-64 ページ）
- [Devices] メニュー（61-66 ページ）
- Object Manager（61-67 ページ）
- [Health] メニュー（61-67 ページ）
- [System] メニュー（61-67 ページ）
- [Help] メニュー（61-68 ページ）

[System Permissions] で選択できるオプションでは、外部データベースに対してクエリを実行したり、ターゲット ユーザ ロールのアクセス許可にエスカレーションしたりすることができるユーザ ロールを作成できます。詳細については、データベースへのアクセスの有効化（64-7 ページ）およびユーザ ロール エスカレーションの管理（61-69 ページ）を参照してください。

オプションで、新しいカスタム ユーザ ロールを作成する代わりに、別のアプライアンスからカスタム ユーザ ロールをエクスポートし、ご使用のアプライアンスにインポートできます。インポートしたロールは、適用する前に、ニーズに合わせて編集できます。詳細については、設定のエクスポート（A-1 ページ）および設定のインポート（A-5 ページ）を参照してください。

カスタム ユーザ ロールを作成するには、次の手順を実行します。

アクセス： Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 2　[User Roles] タブをクリックします。

[User Roles] ページが表示されます。

ステップ 3　[Create User Role] をクリックします。

[User Role Editor] ページが表示されます。

ステップ 4　[Name] フィールドに、新しいユーザ ロールの名前を入力します。

英数字またはハイフン文字を使用できます。スペースは使用しないでください。ロール名は 75 文字以下でなければなりません。ユーザ ロール名では、大文字と小文字が区別されます。

ステップ 5　オプションで、[Description] フィールドに新しいロールの説明を入力します。

ロールの説明は 255 文字以下でなければなりません。

ステップ 6　新しいロールのアクセス許可を選択します。

選択されていないアクセス許可を選択すると、その権限の下位のアクセス許可もすべて選択され、複数値を持つアクセス許可では最初の値が選択されます。上位のアクセス許可をクリアすると、下位のアクセス許可もすべてクリアされます。選択されたアクセス許可の下位のアクセス許可がすべて選択されていない場合、イタリック テキストで表示されます。

カスタム ロールのベースとして使用する事前定義ユーザ ロールをコピーすることを選択すると、その事前定義ロールに関連付けられているアクセス許可が事前に選択されることに注意してください。事前定義ユーザ ロールのコピーの詳細については、事前定義ユーザ ロールのカスタム コピーの作成（61-57 ページ）を参照してください。

現在のエスカレーション ターゲット ロールは、ロール エスカレーション チェック ボックスの横に表示されます。このチェック ボックスをオンにすると、割り当てられているユーザのパスワードまたは指定されている別のユーザ ロールのパスワードのいずれかを使用してエスカレーションを認証することを選択できます。詳細については、ユーザ ロール エスカレーションの管理（61-69 ページ）を参照してください。

ステップ 7　[Save] をクリックします。

カスタム ユーザ ロールが作成され、[User Roles] ページが再度表示されます。

事前定義ユーザ ロールのカスタム コピーの作成

ライセンス：すべて

新しいカスタム ロールのベースとして使用する既存のロールをコピーできます。これにより、[User Role Editor] で既存のロールのアクセス許可が事前に選択されるので、あるロールをモデルとして別のロールを作成できます。

事前定義ユーザ ロールのカスタム コピーを作成するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 2　[User Roles] タブをクリックします。

[User Roles] ページが表示されます。

ステップ 3　コピーするユーザ ロールの横にあるコピー アイコン（  ）をクリックします。

[User Role Editor] ページが表示され、コピーされたロールのアクセス許可が事前に選択されます。

カスタム ユーザ ロールと事前定義ユーザ ロールの両方をこの方法でコピーできることに注意してください。

カスタム ユーザ ロールの削除

ライセンス：すべて

事前定義ユーザ ロールとは異なり、不要になったカスタム ロールは削除できます。カスタム ロールを完全に削除せずに無効にするには、カスタム ロールを非アクティブ化します。詳細については、事前定義ユーザ ロールの管理（61-53 ページ）を参照してください。各自のユーザ ロール、またはシステム ポリシーでデフォルト ユーザ ロールとして設定されているロールは削除できないことに注意してください。詳細については、外部認証の有効化（63-12 ページ）を参照してください。

カスタム ユーザ ロールを削除するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 2　[User Roles] タブをクリックします。

[User Roles] ページが表示されます。

ステップ 3　削除するカスタム ロールの横にある削除アイコン（ ）をクリックします。

カスタム ロールが削除されます。

削除されたロールが、特定のユーザに割り当てられていた唯一のロールである場合、そのユーザはログインして [User Preferences] メニューにアクセスできますが、FireSIGHT システムにはアクセスできません。

ユーザ特権とオプションの変更

ライセンス：すべて

システムにユーザ アカウントを追加したら、アクセス権限、アカウント オプション、パスワードをいつでも変更できます。パスワード管理オプションは、外部ディレクトリ サーバに対して認証されるユーザには適用されないことに注意してください。これらの設定は外部サーバで管理します。ただし、外部認証されるアカウントを含め、すべてのアカウントのアクセス権を設定する必要があります。

外部認証ユーザの場合、LDAP グループ メンバーシップ、RADIUS リスト メンバーシップ、または属性値によってアクセス ロールが割り当てられているユーザの FireSIGHT システム ユーザ管理ページでは、最小アクセス権を削除することができません。ただし、追加の権限を割り当てることはできます。外部認証ユーザのアクセス権を変更すると、[User Management] ページの [Authentication Method] カラムに、[External - Locally Modified] というステータスが表示されます。

ユーザの認証を外部認証から内部認証に変更した場合は、ユーザの新しいパスワードを指定する必要があることに注意してください。

ユーザ アカウント特権を変更するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 2　変更するユーザの横にある編集アイコン（ ）をクリックします。

[Edit User] ページが表示されます。

ステップ 3　必要に応じて 1 つ以上のアカウントを変更します。

- 外部サーバでユーザを認証する方法の説明については、外部認証ユーザ アカウントの管理（61-50 ページ）を参照してください。
- 内部認証ユーザのパスワード設定の変更については、ユーザ ログイン設定の管理（61-51 ページ）を参照してください。
- FireSIGHT システム機能のアクセスを付与するロールの設定の詳細については、ユーザ ロールの設定（61-52 ページ）を参照してください。

制限付きユーザ アクセス プロパティについて

ライセンス： すべて

イベント ビューアであるユーザ ロールが表示できるデータを制限するには、そのロールに制限付き検索を適用します。ユーザに割り当てられたロールを作成または編集するときに、この情報を指定できます。制限付きアクセスを使用してカスタム ロールを作成するには、[Menu Based Permissions] リストから制限するテーブルを選択し、次に [Restrictive Search] ドロップダウン リストからプライベート保存検索を選択します。詳細については、カスタム ユーザ ロールの管理（61-55 ページ）を参照してください。

ユーザ パスワードの変更

ライセンス： すべて

内部認証ユーザの [User Management] ページで、ユーザ パスワードを変更できます。LDAP または RADIUS サーバで外部認証ユーザのパスワードを管理する必要があることに注意してください。

注　アプライアンスで STIG 準拠または Lights-Out Management（LOM）を有効にすると、異なるパスワード制限が適用されます。STIG 準拠を有効にしたシステムでのシェル アクセス ユーザのパスワード設定の詳細については、『*FireSIGHT システムSTIG Release Notes*』を参照してください。LOM ユーザ用システム パスワードのパスワード設定の詳細については、Lights-Out 管理ユーザ アクセスの有効化（64-25 ページ）を参照してください。

ユーザ パスワードを変更するには、次の手順を実行します。

アクセス： Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 2　ユーザ名の横にある編集アイコン（ ）をクリックします。

[Edit User] ページが表示されます。

ステップ 3　[Password] フィールドに、新しいパスワード（最大 32 文字の英数字）を入力します。

ステップ 4　[Confirm Password] フィールドに、新しいパスワードをもう一度入力します。

ユーザ アカウントのパスワード強度検査が有効な場合は、パスワードは 8 文字以上の英数字からなり、大文字と小文字を使用し、1 つ以上の数字と 1 つ以上の特殊文字を使用する必要があります。辞書に記載されている単語や、同じ文字を連続して繰り返し使用することはできません。

ステップ 5　ユーザ設定に、必要なその他のすべての変更を行います。

- パスワード オプションの詳細については、ユーザ ログイン設定の管理（61-51 ページ）を参照してください。
- ユーザ ロールの詳細については、ユーザ ロールの設定（61-52 ページ）を参照してください。

ステップ 6　[Save] をクリックします。

パスワードが変更され、その他のすべての変更が保存されます。

ユーザ アカウントの削除

ライセンス： すべて

admin アカウント以外のユーザ アカウントはシステムからいつでも削除できます。admin アカウントは削除できません。

ユーザ アカウントを削除するには、次の手順を実行します。

アクセス： Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 2　アカウントを削除するユーザの横の削除アイコン（）をクリックします。アカウントが削除されます。

アカウント特権について

ライセンス： すべて

ここでは、FireSIGHT システムの設定可能なユーザ アクセス許可と、これらのアクセス許可にアクセスできるユーザ ロールのリストを示します。ここに記載されているアクセス許可は、カスタム ユーザ ロールの作成時に表示される [Menu Based Permissions] リストの順序に従っています。管理対象デバイスでは使用できないアクセス許可があります。Defense Centerでのみ使用可能なアクセス許可には、そのことが記されています。詳細については、カスタム ユーザ ロールの管理（61-55 ページ）を参照してください。

DC500 Defense Centerと シリーズ 2 デバイスでは制限付き機能セットがサポートされているため、これらのアプライアンスに適用されないアクセス許可があることに注意してください。シリーズ 2 アプライアンス機能の要約については、各デバイス モデルでサポートされるアクセス制御機能の表を参照してください。

このマニュアルで、これ以降のすべての表で使用されるアクセスの表記の詳細については、アクセスの表記規則（1-22 ページ）を参照してください。ここでは、Web ベース インターフェイスの各メイン メニューに関連付けられているユーザ ロール特権を示します。

[Overview] メニュー

ライセンス：すべて

次の表は、[Overview] メニューの各オプションにアクセスするために必要なユーザ ロール特権と、ユーザ ロールがオプション内のサブ権限にアクセスできるかどうかを順に示しています。Security Approver、Discovery Admin、Intrusion Admin、Access Admin、Network Admin、および External Database User の各ロールには、[Overview] メニューのアクセス許可がありません。

表 61-6　[Overview] メニュー

権限	Admin	Maint User	Security Analyst	Security Analyst（RO）
Dashboards	yes	yes	yes	yes
Manage Dashboards	yes	no	no	no
Appliance Information Widget	yes	yes	yes	yes
Appliance Status Widget *(Defense Center のみ)*	yes	yes	yes	yes
Correlation Events Widget	yes	no	yes	yes
Current Interface Status Widget	yes	yes	yes	yes
Current Sessions Widget	yes	no	no	no
Custom Analysis Widget *(Defense Center のみ)*	yes	no	yes	yes
Disk Usage Widget	yes	yes	yes	yes
Interface Traffic Widget	yes	yes	yes	yes
Intrusion Events Widget *(Defense Center のみ)*	yes	no	yes	yes
Network Correlation Widget *(Defense Center のみ)*	yes	no	yes	yes
Product Licensing Widget *(Defense Center のみ)*	yes	yes	no	no
Product Updates Widget	yes	yes	no	no
RSS Feed Widget	yes	yes	yes	yes
System Load Widget	yes	yes	yes	yes
System Time Widget	yes	yes	yes	yes
White List Events Widget *(Defense Center のみ)*	yes	no	yes	yes
Reporting（*Defense Center のみ*）	yes	no	yes	yes

表 61-6　[Overview] メニュー（続き）

権限	Admin	Maint User	Security Analyst	Security Analyst（RO）
Manage Report Templates *(Defense Center のみ)*	yes	no	yes	yes
概要	yes	no	yes	yes
Intrusion Event Statistics *(Defense Center のみ)*	yes	no	yes	yes
Intrusion Event Performance	yes	no	no	no
Intrusion Event Graphs *(Defense Center のみ)*	yes	no	yes	yes
Discovery Statistics *(Defense Center のみ)*	yes	no	yes	yes
Discovery Performance *(Defense Center のみ)*	yes	no	no	no
Connection Summary *(Defense Center のみ)*	yes	no	yes	yes

[Analysis] メニュー

ライセンス：すべて

次の表は、[Analysis] メニューの各オプションにアクセスするために必要なユーザ ロール特権と、ユーザ ロールがオプション内のサブ権限にアクセスできるかどうかを順に示しています。異なる見出しの下に複数回出現する権限は、最初に出現する表にのみ示されています。ただし、サブメニューの見出しを示す場合を除きます。Security Approver、Intrusion Admin、Access Admin、Network Admin、および External Database User の各ロールには、[Analysis] メニューのアクセス許可がありません。[Analysis] メニューはDefense Centerでのみ使用可能です。

表 61-7　[Analysis] メニュー

メニュー	Admin	Discovery Admin	Maint User	Security Analyst	Security Analyst（RO）
Application Statistics	yes	no	no	yes	yes
Geolocation Statistics	yes	no	no	yes	yes
User Statistics	yes	no	no	yes	yes
URL Category Statistics	yes	no	no	yes	yes
URL Reputation Statistics	yes	no	no	yes	yes
SSL Statistics	yes	no	no	yes	yes
Intrusion Event Statistics by Application	yes	no	no	yes	yes
Intrusion Event Statistics by User	yes	no	no	yes	yes
Security Intelligence Category Statistics	yes	no	no	yes	yes
File Storage Statistics by Disposition	yes	no	no	yes	yes
File Storage Statistics by Type	yes	no	no	yes	yes
Dynamic File Analysis Statistics	yes	no	no	yes	yes
Context Explorer	yes	no	no	yes	yes
Connection Events	yes	no	no	yes	yes
Modify Connection Events	yes	no	no	yes	no
Connection Summary Events	yes	no	no	yes	yes

表 61-7　[Analysis] メニュー（続き）

メニュー	Admin	Discovery Admin	Maint User	Security Analyst	Security Analyst（RO）
Modify Connection Summary Events	yes	no	no	yes	no
Security Intelligence Events	yes	no	no	yes	yes
Modify Security Intelligence Events	yes	no	no	yes	no
侵入	yes	no	no	yes	yes
Intrusion Events	yes	no	no	yes	yes
Modify Intrusion Events	yes	no	no	yes	no
View Local Rules	yes	no	no	yes	yes
Reviewed Events	yes	no	no	yes	yes
Clipboard	yes	no	no	yes	yes
インシデント	yes	no	no	yes	yes
ファイル	yes	no	no	yes	yes
Malware Events	yes	no	no	yes	yes
Modify Malware Events	yes	no	no	yes	no
File Events	yes	no	no	yes	yes
Modify File Events	yes	no	no	yes	no
Captured Files	yes	no	no	yes	yes
Modify Captured Files	yes	no	no	yes	no
ファイル トラジェクトリ	yes	no	no	yes	yes
File Download	yes	no	no	yes	yes
Dynamic File Analysis	yes	no	no	yes	no
ホスト	yes	no	no	yes	yes
Network Map	yes	no	no	yes	yes
ホスト	yes	no	no	yes	yes
Modify Hosts	yes	no	no	yes	no
Indications of Compromise（侵害の痕跡）	yes	no	no	yes	yes
Modify Indications of Compromise	yes	no	no	yes	no
サーバ	yes	no	no	yes	yes
Modify Servers	yes	no	no	yes	no
Vulnerabilities	yes	no	no	yes	yes
Modify Vulnerabilities	yes	no	no	yes	no
Host Attributes	yes	no	no	yes	yes
Modify Host Attributes	yes	no	no	yes	no
アプリケーション	yes	no	no	yes	yes
Application Details	yes	no	no	yes	yes
Modify Application Details	yes	no	no	yes	no

表 61-7　[Analysis] メニュー（続き）

メニュー	Admin	Discovery Admin	Maint User	Security Analyst	Security Analyst（RO）
Host Attribute Management	yes	no	no	no	no
Discovery Events	yes	no	no	yes	yes
Modify Discovery Events	yes	no	no	yes	no
ユーザ	yes	yes	no	yes	yes
User Activity	yes	yes	no	yes	yes
Modify User Activity Events	yes	yes	no	yes	no
ユーザ	yes	yes	no	yes	yes
ユーザの変更	yes	yes	no	yes	no
Vulnerabilities	yes	no	no	yes	yes
Third-party Vulnerabilities	yes	no	no	yes	yes
Modify Third-party Vulnerabilities	yes	no	no	yes	no
Correlation（相関）	yes	yes	no	yes	yes
Correlation Events	yes	yes	no	yes	yes
Modify Correlation Events	yes	yes	no	yes	no
White List Events	yes	yes	no	yes	yes
Modify White List Events	yes	yes	no	yes	no
White List Violations	yes	yes	no	yes	yes
Remediation Status	yes	yes	no	no	no
Modify Remediation Status	yes	yes	no	no	no
Custom	yes	no	no	yes	yes
Custom Workflows	yes	no	no	yes	yes
Manage Custom Workflows	yes	no	no	yes	yes
Custom Tables	yes	no	no	yes	yes
Manage Custom Tables	yes	no	no	yes	yes
検索	yes	no	yes	yes	yes
Manage Search	yes	no	no	no	no
Bookmarks	yes	no	no	yes	yes
Manage Bookmarks	yes	no	no	yes	yes

[Policies]メニュー

ライセンス: すべて

次の表は、[Policies] メニューの各オプションにアクセスするために必要なユーザ ロール特権と、ユーザ ロールがオプション内のサブ権限にアクセスできるかどうかを順に示しています。External Database User、Maintenance User、Security Analyst、および Security Analyst（Read Only）の各ロールには、[Policy] メニューでのアクセス許可がありません。[Policies] メニューはDefense Centerでのみ使用可能です。

Intrusion Policy および Modify Intrusion Policy 特権があれば、ネットワーク解析ポリシーの作成および修正もできることに注意してください。

表 61-8　[Policies]メニュー

メニュー	Access Admin	Admin	Discovery Admin	Intrusion Admin	ネットワーク管理者	Security Approver
アクセス コントロール	yes	yes	no	no	yes	yes
アクセス コントロール リスト	yes	yes	no	no	yes	yes
アクセス コントロール ポリシーの変更	yes	yes	no	no	yes	no
Modify Administrator Rules	yes	yes	no	no	yes	no
Modify Root Rules	yes	yes	no	no	yes	no
Apply Intrusion Policies	no	yes	no	no	no	yes
アクセス コントロール ポリシーの適用	no	yes	no	no	no	yes
侵入	yes	yes	no	yes	no	yes
Intrusion Policy	no	yes	no	yes	no	yes
Rule Editor	no	yes	no	yes	no	no
電子メール	no	yes	no	yes	no	no
Modify Intrusion Policy	no	yes	no	yes	no	no
File Policy	yes	yes	no	no	no	no
Modify File Policy	yes	yes	no	no	no	no
Network Discovery	no	yes	yes	no	no	yes
Custom Fingerprinting	no	yes	yes	no	no	no
Custom Topology	no	yes	yes	no	no	no
Modify Network Discovery	no	yes	yes	no	no	no
Apply Network Discovery	no	yes	no	no	no	yes
SSL	yes	yes	no	no	yes	yes
Modify SSL Policy	yes	yes	no	no	yes	no
Modify Administrator Rules	yes	yes	no	no	yes	no
Modify Root Rules	yes	yes	no	no	yes	no
Apply SSL Policy	no	yes	no	no	no	yes
Application Detectors	no	yes	yes	no	no	no
User 3rd Party Mappings	no	yes	yes	no	no	no
Custom Product Mappings	no	yes	yes	no	no	no
ユーザ	no	yes	no	no	no	no
Correlation（相関）	no	yes	no	no	no	no
Policy Management	no	yes	no	no	no	no
Rule Management	no	yes	no	no	no	no
ホワイトリスト	no	yes	no	no	no	no

表 61-8　[Policies]メニュー（続き）

メニュー	Access Admin	Admin	Discovery Admin	Intrusion Admin	ネットワーク管理者	Security Approver
Traffic Profiles	no	yes	no	no	no	no
Actions	no	yes	yes	no	no	no
Alerts	no	yes	yes	no	no	no
Impact Flag Alerts	no	yes	yes	no	no	no
Discovery Event Alerts	no	yes	yes	no	no	no
Scanners	no	yes	yes	no	no	no
Scan Results	no	yes	yes	no	no	no
Modify Scan Results	no	yes	yes	no	no	no
グループ	no	yes	no	no	no	no
Modules	no	yes	no	no	no	no
Instances	no	yes	no	no	no	no

[Devices] メニュー

ライセンス: すべて

[Devices] メニューの表には、[Devices] メニューの各オプションとそのサブ権限にアクセスするために必要なユーザ ロール特権を順に示します。X はユーザ ロールにアクセス権があることを示します。Access Admin、Discovery Admin、External Database User、Maintenance User、Security Approver、Security Analyst、および Security Analyst（Read Only）の各ロールには、[Devices] メニューでのアクセス許可がありません。[Devices] メニューはDefense Centerでのみ使用可能です。

表 61-9　[Devices] メニュー

メニュー	Admin	ネットワーク管理者
Device Management	yes	yes
デバイスの変更	yes	yes
Apply Device Changes	yes	yes
NAT	yes	yes
NAT List	yes	yes
Modify NAT Policy	yes	yes
Apply NAT Rules	yes	no
VPN	yes	yes
Modify VPN	yes	yes
Apply VPN Changes	yes	yes

Object Manager

ライセンス: すべて

[Object Manager] アクセス許可は、Access Admin、Administrator、Network Admin の各ユーザ ロールに対して使用可能です。[Object Manager] アクセス許可はDefense Centerでのみ使用可能です。

FireAMP

ライセンス: すべて

FireAMP アクセス許可は、Administrator ユーザ ロールのみに対して使用可能です。このアクセス許可は、Defense Centerでのみ使用可能です。

[Health] メニュー

ライセンス: すべて

次の表は、[Health] メニューの各オプションにアクセスするために必要なユーザ ロール特権と、ユーザ ロールがオプション内のサブ権限にアクセスできるかどうかを順に示します。Access Admin、Discovery Admin、Intrusion Admin、External Database User、Network Admin、および Security Approver の各ロールには、[Health] メニューでのアクセス許可がありません。[Health] メニューはDefense Centerでのみ使用可能です。

表 61-10　[Health] メニュー

メニュー	Admin	Maint User	Security Analyst	Security Analyst（RO）
Health Policy	yes	yes	no	no
Modify Health Policy	yes	yes	no	no
Apply Health Policy	yes	yes	no	no
Health Events	yes	yes	yes	yes
Modify Health Events	yes	yes	no	no

[System] メニュー

ライセンス: すべて

次の表は、[System] メニューの各オプションにアクセスするために必要なユーザ ロール特権と、ユーザ ロールがオプション内のサブ権限にアクセスできるかどうかを順に示します。Access Admin、Discovery Admin、Intrusion Admin、External Database User、および Security Approver の各ロールには、[System] メニューでのアクセス許可はありません。

表 61-11　[System] メニュー

メニュー	Admin	Maint User	Network Admin	Security Approver	Security Analyst
ローカル	yes	no	no	no	no
設定（Configuration）	yes	no	no	no	no
登録	yes	no	no	no	no

表 61-11　[System] メニュー（続き）

メニュー	Admin	Maint User	Network Admin	Security Approver	Security Analyst
High Availability *(DC1000、DC1500、DC2000、DC3000、DC3500、DC4000 のみ)*	yes	no	no	no	no
eStreamer	yes	no	no	no	no
Host Input Client *(Defense Center のみ)*	yes	no	no	no	no
User Management	yes	no	no	no	no
ユーザ	yes	no	no	no	no
ユーザ ロール	yes	no	no	no	no
Login Authentication *(Defense Center のみ)*	yes	no	no	no	no
System Policy *(Defense Center のみ)*	yes	no	no	no	no
Apply System Policy *(Defense Center のみ)*	yes	no	no	no	no
Modify System Policy *(Defense Center のみ)*	yes	no	no	no	no
Updates	yes	no	no	no	no
Rule Updates *(Defense Center のみ)*	yes	no	no	no	no
Rule Update Import Log *(Defense Center のみ)*	yes	no	no	no	no
ライセンス	yes	no	no	no	no
モニタリング	yes	yes	yes	yes	yes
Audit	yes	no	no	no	no
Modify Audit Log	yes	no	no	no	no
Syslog	yes	yes	no	no	no
Task Status	yes	yes	yes	yes	yes
View Other Users' Tasks	yes	no	no	no	no
統計情報	yes	yes	no	no	no
Tools	yes	yes	no	no	yes
Backup Management	yes	yes	no	no	no
Restore Backup	yes	yes	no	no	no
スケジューリング	yes	yes	no	no	no
Delete Other Users' Scheduled Tasks	yes	no	no	no	no
Import/Export	yes	no	no	no	no
Discovery Data Purge *(Defense Center のみ)*	yes	no	no	no	yes
Whois	yes	yes	no	no	yes

[Help] メニュー

ライセンス: すべて

[Help] メニューとその権限には、すべてのユーザ ロールがアクセスできます。[Help] メニュー オプションを制限することはできません。

ユーザ ロール エスカレーションの管理

ライセンス：すべて

カスタム ユーザ ロールにアクセス許可を付与し、パスワードを設定することで、ベース ロールの特権に加え、他のターゲット ユーザ ロールの特権を一時的に取得できます。これにより、あるユーザが不在であるときにそのユーザを別のユーザに容易に置き換えることや、拡張ユーザ特権の使用状況を緊密に追跡することができます。

たとえば、ユーザのベース ロールに含まれている特権が非常に限られている場合、そのユーザは管理アクションを実行するために Administrator ロールにエスカレーションします。ユーザが各自のパスワードを使用するか、または指定された別のユーザのパスワードを使用することができるように、この機能を設定できます。2 番目のオプションでは、該当するすべてのユーザのための 1 つのエスカレーション パスワードを容易に管理できます。詳細については、エスカレーションに使用するカスタム ユーザ ロールの設定（61-70 ページ）を参照してください。

エスカレーション ターゲット ロールにすることができるユーザ ロールは一度に 1 つだけであることに注意してください。カスタム ユーザ ロールまたは事前定義ユーザ ロールを使用できます。各エスカレーションはログイン セッション期間中保持され、監査ログに記録されます。

この機能の構成および使用方法の詳細については、次の項を参照してください。

- エスカレーション ターゲット ロールの設定（61-69 ページ）
- エスカレーションに使用するカスタム ユーザ ロールの設定（61-70 ページ）
- ユーザ ロールのエスカレーション（61-71 ページ）

エスカレーション ターゲット ロールの設定

ライセンス：すべて

各自のユーザ ロール（事前定義またはカスタム）をシステム全体でのエスカレーション ターゲット ロールとして機能するように割り当てることができます。これは、他のロールからのエスカレーション先となるロールです（エスカレーションが可能な場合）。

エスカレーション ターゲット ロールを設定するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 2　[User Roles] をクリックします。

[User Roles] ページが表示されます。

ステップ 3　[Configure Permission Escalation] をクリックします。

[Configure Permission Escalation] ダイアログ ボックスが表示されます。

ステップ 4　ドロップダウン リストからユーザ ロールを選択します。

ステップ 5　[OK] をクリックして変更を保存します。

変更が保存され、[User Roles] ページが表示されます。

注　エスカレーション ターゲット ロールの変更は即時に反映されます。エスカレーションされたセッションのユーザには、新しいエスカレーション ターゲットのアクセス許可が付与されます。

エスカレーションに使用するカスタム ユーザ ロールの設定

ライセンス： すべて

ユーザ ロール エスカレーション機能を使用するには、最初にエスカレーション権限を持つカスタム ユーザ ロールを設定し、そのエスカレーション パスワードを選択して、そのロールをユーザに割り当てる必要があります。詳細については、新しいユーザ アカウントの追加（61-47 ページ）およびユーザ ロールの設定（61-52 ページ）を参照してください。

カスタム ロールのエスカレーション パスワードを設定するときには、部門のニーズを考慮してください。多数のエスカレーション ユーザを容易に管理するには、別のユーザを選択し、そのユーザのパスワードをエスカレーション パスワードとして使用することができます。そのユーザのパスワードを変更するか、またはそのユーザを非アクティブにすると、そのパスワードを必要とするすべてのエスカレーション ユーザが影響を受けます。このことにより、特に一元管理できる外部認証ユーザを選択した場合に、ユーザ ロール エスカレーションをより効率的に管理できます。

エスカレーションに使用するカスタム ユーザ ロールを設定するには、次の手順を実行します。

アクセス： Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 2　[User Roles] をクリックします。

[User Roles] ページが表示されます。

ステップ 3　[Create User Role] をクリックして新しいカスタム ユーザ ロールを作成するか、既存のカスタム ユーザ ロールの横の編集アイコン（）をクリックします。

[User Role Editor] ページが表示されます。

ステップ 4　カスタム ユーザ ロールの名前、説明、およびメニュー ベースのアクセス許可を選択します。

詳細については、カスタム ユーザ ロールの管理（61-55 ページ）の手順を参照してください。

ステップ 5　[System Permissions] で、[Set this role to escalate to:] チェック ボックスをオンにします。

エスカレーション パスワード オプションが表示されます。

ステップ 6　このロールがエスカレーションするときに使用するパスワードを選択します。次の 2 つのオプションから選択できます。

- このロールが割り当てられているユーザがエスカレーション時に各自のパスワードを使用できるようにするには、[Authenticate with the assigned user's password] を選択します。
- このロールが割り当てられているユーザが、別のユーザのパスワードを使用するようにするには、[Authenticate with the specified user's password] を選択し、そのユーザ名を入力します。

注　別のユーザのパスワードで認証するときには、任意のユーザ名（非アクティブなユーザまたは存在しないユーザを含む）を入力できます。エスカレーションにパスワードが使用されるユーザを非アクティブにすると、そのパスワードを必要とするロールが割り当てられているユーザのエスカレーションが不可能になります。この機能を使用して、必要に応じてエスカレーション機能をただちに削除できます。

ステップ 7　[Save] をクリックします。

変更が保存され、[User Roles] ページが再度表示されます。これで、このロールが割り当てられているユーザはターゲット ユーザ ロールにエスカレーションできます。ユーザへのユーザ ロールの割り当ての詳細については、新しいユーザ アカウントの追加（61-47 ページ）を参照してください。

ユーザ ロールのエスカレーション

ライセンス：すべて

エスカレーション対象のアクセス許可が含まれているカスタム ユーザ ロールが割り当てられているユーザは、いつでもターゲット ロールのアクセス許可にエスカレーションできます。エスカレーションはユーザ設定に影響しないことに注意してください。割り当てられているユーザ ロールがユーザ ロール エスカレーション向けに設定されていない場合、[User] メニューの [Escalate Permissions] オプションは表示されません。

ユーザ アクセス許可をエスカレーションするには、次の手順を実行します。

アクセス：すべて

ステップ 1　[Local] > [User] > [Escalate Permissions] を選択します。

[Escalate User Permissions] ダイアログ ボックスが表示されます。

ステップ 2　認証パスワードを入力します。

ステップ 3　[Escalate] をクリックします。

これで、現行ロールに加え、エスカレーション ターゲット ロールのすべてのアクセス許可が付与されました。

エスカレーションはログイン セッションの残り期間にわたって保持されることに注意してください。ベース ロールの特権だけに戻すには、ログアウトしてから新しいセッションを開始する必要があります。

Cisco Security Manager からのシングル サインオンの設定

ライセンス： すべて

サポートされるデバイス： ASA FirePOWER

シングル サインオン（SSO）により、Cisco Security Manager（CSM）バージョン 4.7 以上とDefense Centerを統合できます。これにより、ログインのために追加認証なしで CSM からDefense Centerにアクセスできます。ASA FirePOWER デバイスの ASA モジュールの管理では、デバイスの FirePOWER モジュールに適用されるポリシーの変更が必要となる場合もあります。CSM で Defense Centerを管理することを選択し、Web ブラウザで起動します。管理元のDefense Centerが高可用性ペアのメンバーの場合、SSO を使用すると、プライマリ ピアに移動します。

ユーザ ロールに基づくアクセスがある場合、CSM でクロス起動したデバイスの [Device Management] ページの [Device] タブに移動します。それ以外の場合は、[Summary Dashboard] ページ（[Overview] > [Dashboards]）に移動します。ただしダッシュボードにアクセスできないユーザ アカウントの場合は、[Welcome] ページが使用されます。

Defense Centerに SSO を行うには、その前に、CSM からDefense Centerへの一方向暗号化認証パスをセットアップする必要があります。NAT 環境では、Defense Centerと CSM は NAT 境界の同じ側に存在している必要があります。通信を有効にするには、CSM とDefense Centerが相互を認識できるように、次の基準を指定する必要があります。

- CSM から、接続を識別する SSO 共有暗号キーを生成する必要があります。Defense Centerでこの鍵を入力する必要があります。
- Defense Centerで、CSM サーバのホスト名または IP アドレスとサーバ ポートを指定します。高可用性を使用する場合は、プライマリ ピアで SSO を設定します。
- 暗号化認証パラメータを検証するため、SSO アクセスを持たせるすべてのユーザに対し、CSM とDefense Centerで同じユーザ名（大文字小文字を区別）をセットアップする必要があります。

Defense Centerで STIG 準拠が有効な場合、システムにより SSO が無効化されます。詳細については、「STIG コンプライアンスの有効化（63-26 ページ）」を参照してください。

注　組織で認証に CAC が使用されている場合は、シングル サインオンでログインできません。詳細については、CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。

シングル サインオンをセットアップするには、次の手順を実行します。

アクセス： Admin

ステップ 1　CSM から SSO 共有暗号キーを生成します。

詳細については、CSM のマニュアルを参照してください。

ステップ 2　Defense Centerで [System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 3　[CSM Single Sign-on] を選択します。

[CSM Single Sign-on] ページが表示されます。

ステップ 4　**CSM ホスト名**または **IP** アドレスとサーバの**ポート**を入力します。

ステップ 5　CSM から生成した**共有キー**を入力します。

ステップ 6　オプションで、Defense Centerのプロキシ サーバを使用して CSM と通信する場合は、[Use Proxy For Connection] チェックボックスを選択します。詳細については、管理インターフェイスのオプションについて（64-10 ページ）を参照してください。

ステップ 7　[Submit] をクリックします。`

CSM 証明書が表示されます。

ステップ 8　[Confirm Certificate] をクリックして証明書を保存します。

これで CSM からDefense Centerにログインできるようになります。追加のログインを実行する必要はありません。

タスクのスケジュール

さまざまな種類の管理タスクを、指定した回数（1 度または繰り返し）実行するようにスケジュールを設定できます。

注 タスクによっては低帯域幅のネットワークに非常に負荷をかけることがあります（ソフトウェアの自動更新が含まれるタスクや、管理対象デバイスに更新をプッシュする必要があるタスクなど）。ネットワーク使用率が低い時間帯にこのようなタスクを実行するよう、スケジュールしてください。

詳細については、次の項を参照してください。

- 定期タスクの設定（62-2 ページ）：スケジュール済みタスクが定期的に実行されるようセットアップする方法について説明します。
- バックアップ ジョブの自動化（62-3 ページ）：バックアップ ジョブをスケジュールする手順を示します。
- 証明書失効リストのダウンロードの自動化（62-4 ページ）：アプライアンスの証明書失効リスト（CRL）を自動的に更新する手順を示します。
- Nmap スキャンの自動化（62-5 ページ）：Nmap スキャンをスケジュールする手順を示します。
- 侵入ポリシーの適用の自動化（62-7 ページ）：管理対象デバイスに対する侵入ポリシーの適用をキューイングする手順を示します。
- レポートの生成を自動化する方法（62-9 ページ）：レポートをスケジュールする手順を示します。
- 位置情報データベースの更新の自動化（62-10 ページ）：位置情報データベース（GeoDB）の自動更新をスケジュールする手順を示します。
- FireSIGHT 推奨の自動化（62-11 ページ）：侵入ルール状態の推奨の自動更新をスケジュールする手順について示します。
- ソフトウェア更新の自動化（62-12 ページ）：ソフトウェア更新のダウンロード、プッシュ、インストールをスケジュールする手順について示します。
- 脆弱性データベースの更新の自動化（62-17 ページ）：VDB 更新のダウンロードとインストールをスケジュールする手順を示します。
- URL フィルタリング更新の自動化（62-20 ページ）：URL フィルタリング データの更新を自動化する手順を示します。
- タスクの表示（62-21 ページ）：すでにスケジュールした後のタスクを表示したり管理したりする方法について説明します。

- スケジュール済みタスクの編集（62-22 ページ）：既存のタスクを編集する方法について説明します。
- スケジュール済みタスクの削除（62-23 ページ）：ワンタイム タスクや、定期タスクのすべてのインスタンスを削除する方法について説明します。

定期タスクの設定

ライセンス： すべて

定期タスクの頻度を設定する際には、すべてのタイプのタスクで同じ手順に従います。

Web インターフェイスのほとんどのページに表示される時間はローカル時刻であり、ローカル設定で指定したタイム ゾーンに従ってそれが決定されます。さらに、Defense Centerは、該当する場合にはローカル時刻の表示を夏時間（DST）に合わせて自動的に調整します。ただし、DST から標準時への移行日および元に戻る移行日をまたがる定期タスクは、移行を考慮して調整されません。つまり、標準時の午前 2:00 にタスク スケジュールを作成すると、DST 期間中は午前 3:00 に実行されます。同様に、DST の午前 2:00 にタスク スケジュールを作成すると、標準時には午前 1:00 に実行されます。

定期タスクを設定する方法：

アクセス： Admin/Maint

ステップ 1　[System] > [Tools] > [Scheduling] を選択します。

[Scheduling] ページが表示されます。

ステップ 2　[Add Task] をクリックします。

[New Task] ページが表示されます。

ステップ 3　[Job Type] リストから、スケジュールするタスクのタイプを選択します。

スケジュールできるタスク タイプについては、それぞれ該当するセクションで説明します。

ステップ 4　[Schedule task to run] オプションで、定期タスクを指定するために [Recurring] を選択します。

ページがリロードされ、定期タスクのオプションが示されます。

ステップ 5　[Start On] フィールドに、定期タスクを開始する日付を指定します。ドロップダウンリストを使用して月、日、年を選択できます。

ステップ 6　[Repeat Every] フィールドに、タスクを繰り返す頻度を指定します。時間、日、週、または月の数値を指定できます。

ヒント　数値を入力するか、上矢印（▲）および下矢印（▼）アイコンをクリックして、間隔を指定できます。たとえば、2 日おきにタスクを実行するには、2 を入力して [Days] を選択します。

ステップ 7　[Run At] フィールドで、定期タスクを開始する時刻を指定します。

ステップ 8　[Repeat Every] で [Weeks] を選択した場合は、[Repeat On] フィールドが表示されます。タスクを実行する曜日の横にあるチェック ボックスを選択してください。

ステップ 9　[Repeat Every] に [Months] を選択した場合は、[Repeat On] フィールドが表示されます。ドロップダウンリストを使用して、タスクを実行する各月の日を選択します。

[New Task] ページ上のその他のオプションは、作成中のタスクに応じて異なります。詳細については、次の項を参照してください。

- バックアップ ジョブの自動化（62-3 ページ）
- 証明書失効リストのダウンロードの自動化（62-4 ページ）
- Nmap スキャンの自動化（62-5 ページ）
- レポートの生成を自動化する方法（62-9 ページ）
- FireSIGHT 推奨の自動化（62-11 ページ）
- ソフトウェア更新の自動化（62-12 ページ）
- 脆弱性データベースの更新の自動化（62-17 ページ）
- URL フィルタリング更新の自動化（62-20 ページ）

バックアップ ジョブの自動化

ライセンス： すべて

サポートされるデバイス： シリーズ 2 およびシリーズ 3

サポートされる防御センター： すべて

スケジューラを使用して、Defense Centerや物理管理対象デバイスのバックアップを自動化できます。バックアップをスケジュール済みタスクとして設定するには、その前にバックアップ プロファイルを設計する必要があります。詳細については、バックアップ プロファイルの作成（70-6 ページ）を参照してください。

仮想管理対象デバイス、Cisco NGIPS for Blue Coat X-Series、またはCisco ASA with FirePOWER Servicesのスケジュール バックアップは実行**できません**。物理管理対象デバイスの設定データのスケジュール バックアップを実行するには、デバイス自体の Web インターフェイスからタスクをスケジュールします。イベント データのスケジュール バックアップを実行するには、管理を行うDefense Centerのスケジュール バックアップを実行します。

バックアップ タスクを自動化する方法：

アクセス： Admin/Maint

ステップ 1　[System] > [Tools] > [Scheduling] を選択します。

[Scheduling] ページが表示されます。

ステップ 2　[Add Task] をクリックします。

[New Task] ページが表示されます。

ステップ 3　[Job Type] リストから、[Backup] を選択します。

ページがリロードされ、バックアップのオプションが表示されます。

ステップ 4　バックアップをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。[Current Time] フィールドには、アプライアンスの現在時刻が示されます。

- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定（62-2 ページ）を参照してください。

ステップ 5　[Job Name] フィールドに、255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 6　[Backup Profile] リストから、適切なバックアップ プロファイルを選択します。

新しいバックアップ プロファイルの作成の詳細については、バックアップ プロファイルの作成（70-6 ページ）を参照してください。

ステップ 7　オプションで、[Comment] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント　コメント フィールドはページの [View Tasks] セクションに表示されるので、ある程度短くしてください。

ステップ 8　オプションで、[Email Status To:] フィールドに、ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、Defense Centerで有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定（63-19 ページ）を参照してください。

ステップ 9　[Save] をクリックします。

タスクが追加されます。[Task Status] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示（C-1 ページ）を参照）。

証明書失効リストのダウンロードの自動化

ライセンス： すべて

スケジューラを使用すると、アプライアンスのユーザ証明書を有効にするための、アプライアンス上のアプライアンス Web サーバの証明書失効リスト（CRL）を自動的に更新できます。ローカル アプライアンス設定で CRL の取得を有効にすると Download CRL タスクが自動的に作成されるため、以下の手順では、スケジュール済みタスクを開いて頻度を設定する方法について説明します。

ヒント　このタスクをスケジュールする前に、ユーザ証明書を有効化して設定し、CRL ダウンロード URL を設定する必要があります。ユーザ証明書の設定については、ユーザ証明書の要求（64-6 ページ）を参照してください。

証明書失効リストのダウンロードを自動化する方法：

アクセス： Admin/Maint

ステップ 1　[System] > [Tools] > [Scheduling] を選択します。

[Scheduling] ページが表示されます。

ステップ 2　[Task Details] で **Download CRL** タスクを見つけ、編集アイコン（  ）をクリックします。

[Edit Task] ページが表示され、ダウンロード オプションが示されます。

ステップ 3　CRL ダウンロードをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。[Current Time] フィールドには、アプライアンスの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定（62-2 ページ）を参照してください。

ステップ 4　オプションで、[Comment] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント　コメント フィールドはページの [View Tasks] セクションに表示されるので、ある程度短くしてください。

ステップ 5　オプションで、[Email Status To:] フィールドに、ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、Defense Centerで有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定（63-19 ページ）を参照してください。

ステップ 6　[Save] をクリックします。

タスクが追加されます。[Task Status] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示（C-1 ページ）を参照）。

Nmap スキャンの自動化

ライセンス：FireSIGHT

ネットワーク上のターゲットに対する定期的な Nmap スキャンをスケジュールできます。スキャンを自動化すると、Nmap スキャンによって以前に提供された情報を更新できます。FireSIGHT システムは Nmap 提供データを更新できないため、このデータを最新に保つには定期的に再スキャンする必要があります。また、ネットワーク上のホストに識別不能なアプリケーションやサーバがあるかどうか自動的に検査するよう、スキャンをスケジュールすることもできます。詳細については、次の項を参照してください。

- Nmap スキャン用にシステムを準備する
- Nmap スキャンのスケジュール

さらに、Discovery Administrator が修正用に Nmap スキャンを使用する場合があることにも注意してください。たとえば、ホストでオペレーティング システム競合が発生したために、Nmap スキャンがトリガーされることがあります。スキャンが実行されると、そのホストでのオペレーティング システムの更新済み情報が取得され、こうして競合が解決されます。詳細については、Nmap スキャン修復（54-13 ページ）を参照してください。

Nmap スキャン用にシステムを準備する

ライセンス：FireSIGHT

以前に Nmap スキャン機能を使用したことがない場合は、スキャンのスケジュールを定義する前に、いくつかの Nmap 設定手順を完了する必要があります。詳細については、次の項を参照してください。

- Nmap スキャン インスタンスの作成（47-10 ページ）では、Nmap サーバ接続プロファイルのセットアップについて説明します。
- Nmap スキャン ターゲットの作成（47-11 ページ）では、スキャン対象のセットアップについて説明します。
- Nmap 修復の作成（47-13 ページ）では、修正定義のセットアップについて説明します。

Nmap スキャンのスケジュール

ライセンス：FireSIGHT

Nmap ユーティリティを使用してネットワーク上の 1 つ以上のホストをスキャンする操作をスケジュールできます。

システムで検出されたホストのオペレーティング システム、アプリケーション、またはサーバが Nmap スキャン結果で置き換えられた後、システムは、Nmap によって置換されたホストに関する情報をもはや更新しません。Nmap で提供されたサービスおよびオペレーティング システムのデータは、もう一度 Nmap スキャンを実行するまで静的な状態になります。Nmap を使ってホストをスキャンする予定の場合は、Nmap 提供のオペレーティング システム、アプリケーション、またはサーバを最新の状態に保つために、定期的なスキャン スケジュールをセットアップできます。ネットワーク マップからホストが削除されて再び追加されると、Nmap スキャン結果はすべて破棄され、システムはホストに関するすべてのオペレーティング システムとサービスのデータのモニタリングを再開します。

Nmap スキャンを自動化する方法：

アクセス：Admin/Maint

ステップ 1　[System] > [Tools] > [Scheduling] を選択します。

[Scheduling] ページが表示されます。

ステップ 2　[Add Task] をクリックします。

[New Task] ページが表示されます。

ステップ 3　[Job Type] リストから、[Nmap Scan] を選択します。

ページがリロードされ、Nmap スキャンを自動化するオプションが表示されます。

ステップ 4　タスクをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。[Current Time] フィールドには、アプライアンスの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定（62-2 ページ）を参照してください。

ステップ 5　[Job Name] フィールドに、255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 6　[Nmap Remediation] フィールドでは、スキャン実行時に使用する Nmap 修正を選択します。

ステップ 7　[Nmap Target] フィールドで、スキャンされるホストを定義するスキャン対象を選択します。

ステップ 8　オプションで、[Comment] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント　コメント フィールドはページの [View Tasks] セクションに表示されるので、ある程度短くしてください。

ステップ 9　オプションで、[Email Status To:] フィールドに、ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定（63-19 ページ）を参照してください。

ステップ 10　[Save] をクリックします。

タスクが追加されます。[Task Status] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示（C-1 ページ）を参照）。

侵入ポリシーの適用の自動化

ライセンス：Protection

管理対象デバイスに侵入ポリシーを適用する操作をキューイングすることができます。このタスクの実行時点で、侵入ポリシーを参照するアクセス コントロール ポリシーが、選択されたデバイスに対して適用されている場合に限り、このタスクは侵入ポリシーを適用します。それ以外の場合、このタスクは完了せずに終了します。

このタスクをスケジュールする前に、侵入ポリシーをアクセス コントロール ポリシーに関連付けて、アクセス コントロール ポリシーをデバイスに適用する必要があります。侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（18-1 ページ）を参照してください。

管理対象デバイスへのポリシー適用をキューイングする方法：

アクセス：Admin/Maint

ステップ 1　[System] > [Tools] > [Scheduling] を選択します。

現在の月のスケジュール カレンダー ページが表示されます。

ステップ 2　[Add Task] をクリックします。

[New Task] ページが表示されます。

ステップ 3　[Job Type] リストから、[Queue Intrusion Policy Apply] を選択します。

ページがリロードされ、ポリシー適用のキューイングに関するオプションが表示されます。

ステップ 4　タスクをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。[Current Time] フィールドには、Defense Centerの現在時刻が示されます。

- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定（62-2 ページ）を参照してください。

ステップ 5　[Job Name] フィールドに、255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 6　[Intrusion Policy] フィールドで、次の操作を実行できます。

- 選択したターゲット デバイスに適用する侵入ポリシーを 1 つ選択します。
- [All intrusion policies] を選択すると、[Device] フィールドで選択したデバイスにすでに適用されているすべての侵入ポリシーが適用されます。

ステップ 7　[Device] フィールドで、次のオプションのいずれかを行います。

- [Intrusion Policy] フィールドで選択した侵入ポリシーの適用対象となるデバイスを 1 つ選択します。
- [All targeted devices] を選択すると、選択した侵入ポリシーがすでに適用されているすべてのモニタ対象デバイスに、その侵入ポリシーが適用されます。

ヒント　このフィールドには、[Intrusion Policy] フィールドで選択した侵入ポリシーがすでに適用されているデバイスのみが表示されます。

ステップ 8　オプションで、[Comment] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント　スケジュール カレンダー ページの下部、[Task Details] セクションにコメント フィールドが表示されるため、コメントの長さを制限してください。

ステップ 9　オプションで、[Email Status To:] フィールドに、ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定（63-19 ページ）を参照してください。

ステップ 10　[Save] をクリックします。

タスクが追加されます。カレンダー ページの [Task Details] セクションで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示（C-1 ページ）を参照）。

ステップ 11　保存済みのタスクを編集するには、スケジュール カレンダー ページに表示されているタスクをクリックします。

[Task Details] セクションがページの下部に表示されます。変更を行うには、編集アイコン（  ）をクリックします。

レポートの生成を自動化する方法

ライセンス： すべて

サポートされるデバイス： すべて（X-Seriesを除く）

一定期間ごとにレポートを実行するよう自動化できます。ただし、レポートをスケジュール済みタスクとして設定するには、その前にレポートのテンプレートを設計する必要があります。レポート デザイナを使用してレポート テンプレートを作成する方法の詳細については、レポート テンプレートについて（57-2 ページ）を参照してください。

また、スケジューラを使用して電子メール レポートを配布する場合は、タスクをスケジュールする**前に**、レポート テンプレートとメール リレー ホストの設定が必要です。詳細については、レポートの生成時の電子メール配布（57-31 ページ）およびメール リレー ホストおよび通知アドレスの設定（63-19 ページ）を参照してください。

レポートの生成を自動化する方法：

アクセス： Admin/Maint

ステップ 1　[System] > [Tools] > [Scheduling] を選択します。

現在の月のスケジュール カレンダー ページが表示されます。

ステップ 2　[Add Task] をクリックします。

[New Task] ページが表示されます。

ステップ 3　[Job Type] リストから、[Report] を選択します。

ページがリロードされ、レポートの自動実行をセットアップするためのオプションが表示されます。

ステップ 4　タスクをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウン リストを使用して開始日時を指定します。[Current Time] フィールドには、Defense Centerの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定（62-2 ページ）を参照してください。

ステップ 5　[Job Name] フィールドに、255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 6　[Report Template] フィールドで、ドロップダウン リストから、使用するレポート テンプレートを選択します。詳細については、レポート テンプレートの作成と編集（57-4 ページ）を参照してください。

ステップ 7　オプションで、[Comment] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント　スケジュール カレンダー ページの下部、[Task Details] セクションにコメント フィールドが表示されるため、コメントの長さを制限してください。

ステップ 8　オプションで、[Email Status To:] フィールドに、ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定（63-19 ページ）を参照してください。

注　このオプションを設定しても、レポートは配布**されません**。詳細については、レポートの生成時の電子メール配布（57-31 ページ）を参照してください。

ステップ 9　レポートのデータがない場合（たとえばレポート期間中に特定のタイプのイベントが発生しなかった場合）にレポート電子メール添付ファイルを受信しないようにするには、[If report is empty, still attach to email] チェック ボックスを選択します。

ステップ 10　[Save] をクリックします。

タスクが追加されます。カレンダー ページの [Task Details] セクションで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示（C-1 ページ）を参照）。

ステップ 11　保存済みのタスクを編集するには、スケジュール カレンダー ページに表示されているタスクをクリックします。

[Task Details] セクションがページの下部に表示されます。変更を行うには、編集アイコン（  ）をクリックします。

位置情報データベースの更新の自動化

ライセンス： FireSIGHT

サポートされる防御センター： すべて（DC500 を除く）

スケジューラを使用して、位置情報データベース（GeoDB）の定期更新を自動化できます。GeoDB の定期更新は 7 日ごとに 1 度（週 1 回）実行されます。週ごとに更新が繰り返される時刻を設定できます。GeoDB 更新の詳細については、地理情報データベースについて（66-30 ページ）を参照してください。

位置情報データベースの更新を自動化する方法：

アクセス： Admin

ステップ 1　[System] > [Updates] を選択します。

[Product Updates] ページが表示されます。

ステップ 2　[Geolocation Updates] タブをクリックします。

[Geolocation Updates] ページが表示されます。

ステップ 3　[Recurring Geolocation Updates] の下で、[Enable Recurring Weekly Updates] チェック ボックスを選択します。

[Update Start Time] フィールドが表示されます。

ステップ 4　[Update Start Time] フィールドで、週ごとに GeoDB 更新を行う曜日と時刻を指定します。

ステップ 5　[Save] をクリックします。

タスクが追加されます。[Task Status] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示（C-1 ページ）を参照）。

FireSIGHT 推奨の自動化

ライセンス： Protection

カスタム侵入ポリシーで保存済みの最新の設定を使用し、ネットワークのディスカバリ データに基づいてルール状態の推奨を自動的に生成することができます。

注　変更が未保存のまま、侵入ポリシーに関するスケジュール済み推奨がシステムによって自動生成される場合、自動生成された推奨をポリシーに反映させるには、そのポリシー内の変更を破棄してポリシーをコミットする必要があります。詳細については、「競合の解決とポリシー変更の確定（23-17 ページ）」を参照してください。

タスクの実行時に、推奨されるルール状態がシステムによって自動的に生成されます。また、ポリシーの設定によっては、ネットワーク資産に応じた侵入防御の調整（33-1 ページ）で説明されている基準に基づいて侵入ルールの状態が変更されることもあります。変更されたルール状態は、侵入ポリシーを次回に適用するときに有効になります。

ルール状態の推奨の生成を自動化する方法：

アクセス： Admin/Maint

ステップ 1　[System] > [Tools] > [Scheduling] を選択します。

[Scheduling] ページが表示されます。

ステップ 2　[Add Task] をクリックします。

[New Task] ページが表示されます。

ステップ 3　[Job Type] リストから、[FireSIGHT Recommended Rules] を選択します。

ページがリロードされ、FireSIGHT 推奨を生成するためのオプションが表示されます。

ステップ 4　オプションで、[Job Type] フィールドの横にあるポリシー リンクをクリックして、[Detection & Prevention] ページを表示します。このページでは侵入ポリシー内の FireSIGHT 推奨ルールを設定できます。

ステップ 5　タスクをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。[Current Time] フィールドには、アプライアンスの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定（62-2 ページ）を参照してください。

ステップ 6　[Job Name] フィールドに、255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 7　[Policies] の横で、推奨を生成する 1 つ以上のポリシーを選択します。次の選択肢があります。

- [Policies] フィールドで、1 つ以上のポリシーを選択します。複数のポリシーを選択するには Shift キーと Ctrl キーを使用します。
- [All Policies] チェック ボックスをクリックして、すべてのポリシーを選択します。

ステップ 8　オプションで、[Comment] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント　コメント フィールドはページの [View Tasks] セクションに表示されるので、ある程度短くしてください。

ステップ 9　オプションで、[Email Status To:] フィールドに、ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定（63-19 ページ）を参照してください。

ステップ 10　[Save] をクリックします。

タスクが追加されます。[Task Status] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示（C-1 ページ）を参照）。

ソフトウェア更新の自動化

ライセンス： すべて

ほとんどのパッチや機能リリースを自動的にダウンロードして FireSIGHT システムに適用することができます。

注　手動で更新をアップロードしてインストールする必要が生じる状況が 2 つあります。まず、FireSIGHT システムのメジャー アップデート（主要な更新）をスケジュールすることはできません。次に、サポート サイトにアクセスできないアプライアンスの更新や、そのアプライアンスからのプッシュをスケジュールすることはできません。アプライアンスがインターネットに直接接続しない場合、管理インターフェイスの構成（64-9 ページ）の説明に従って、サポート サイトから更新をダウンロードできるようプロキシをセットアップする必要があります。FireSIGHT システムの手動更新について詳しくは、システム ソフトウェアの更新（66-1 ページ）を参照してください。

ソフトウェア更新をインストールするためにどんなタスクをスケジュールする必要があるかは、Defense Centerを更新する場合と、Defense Centerを使って管理対象デバイスを更新する場合とで異なります。Ciscoでは、Defense Centerを使用して管理対象デバイスを更新することを**強く**お勧めしています。

Defense Centerを更新するには、Install Latest Update タスクを使用してソフトウェア インストールをスケジュールします。Defense Centerを使用して管理対象デバイスのソフトウェア更新を自動化するには、次の 2 つのタスクをスケジュールする必要があります。

ステップ 1　Push Latest Update タスクを使用して、管理対象デバイスに更新をプッシュ（コピー）します。

ステップ 2　Install Latest Update タスクを使用して、管理対象デバイス上に更新をインストールします。

更新をスケジュールする際には、プッシュ タスクとインストール タスクが連続して行われるようにスケジュールしてください。つまり、管理対象デバイスでのソフトウェア更新を自動化するには、まず更新をデバイスにプッシュする必要があり、その後でインストールできます。デバイス グループでのソフトウェア更新を自動化するには、グループ内のすべてのデバイスを選択する必要があります。（手動による更新プロセスでは、インストールする前に、更新を管理対象デバイスにプッシュする必要がないことに注意してください。詳細については、管理対象デバイスの更新（66-9 ページ）を参照してください。）

注　クラスタ設定やスタック設定では、管理対象デバイスに対する個別の更新タスクを作成できません。

プロセスを完了させるには、タスクとタスクの間に必ず十分な時間を確保してください。タスク間を 30 分以上空けてスケジュールする必要があります。たとえば、更新のインストール タスクをスケジュールする場合、Defense Centerからデバイスへの更新のコピーがまだ終了していないと、インストール タスクは正しく実行されません。ただし、スケジュール済みインストール タスクが毎日繰り返される場合は、翌日の実行時に、すでにプッシュされた更新がインストールされます。

デバイス グループに更新プログラムをインストールするようにスケジュールされたタスクによって、デバイス グループ内の各デバイスに同時に更新プログラムがインストールされることに注意してください。デバイス グループ内のすべてのデバイスについてスケジュールされたタスクが完了するだけの十分な時間を確保してください。

このプロセスをより確実に制御するには、更新がリリースされたことがわかった後、[Once] オプションを使用してオフピーク時間帯に更新をダウンロード/インストールできます。

詳細については、次の項を参照してください。

- ソフトウェア ダウンロードの自動化（62-13 ページ）
- ソフトウェア プッシュの自動化（62-14 ページ）
- ソフトウェア インストールの自動化（62-15 ページ）

ソフトウェア ダウンロードの自動化

ライセンス： すべて

Ciscoから最新のソフトウェア更新を自動的にダウンロードするスケジュール済みタスクを作成することができます。このタスクを使用すると、手動でインストールする予定の更新をダウンロードするスケジュールを設定できます。

ソフトウェア更新のダウンロードを自動化する方法：

アクセス： Admin/Maint

ステップ 1　[System] > [Tools] > [Scheduling] を選択します。

[Scheduling] ページが表示されます。

ステップ 2　[Add Task] をクリックします。

[New Task] ページが表示されます。

ステップ 3　[Job Type] リストから、[Download Latest Update] を選択します。

[New Task] ページがリロードされ、更新オプションが示されます。

ステップ 4　タスクをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。[Current Time] フィールドには、アプライアンスの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定（62-2 ページ）を参照してください。

ステップ 5　[Job Name] フィールドに、255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 6　[Update Items] セクションで、[Software] を選択します。

ステップ 7　オプションで、[Comment] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント　コメント フィールドはページの [View Tasks] セクションに表示されるので、ある程度短くしてください。

ステップ 8　オプションで、[Email Status To:] フィールドに、ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定（63-19 ページ）を参照してください。

ステップ 9　[Save] をクリックします。

タスクが追加されます。[Task Status] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示（C-1 ページ）を参照）。

ソフトウェア プッシュの自動化

ライセンス： すべて

管理対象デバイスでのソフトウェア更新のインストールを自動化するには、インストールの前に、更新をデバイスにプッシュする必要があります。

更新を管理対象デバイスにプッシュするとき、プッシュ プロセスの状態に関する情報が [Tasks] ページに報告されます。詳細については、「実行時間が長いタスクのステータスの表示（C-1 ページ）」を参照してください。

ソフトウェア更新を管理対象デバイスにプッシュするタスクを作成する際には、更新がデバイスに確実にコピーされるよう、プッシュ タスクとスケジュール済みインストール タスクの間に十分な時間を確保してください。

ソフトウェア更新を管理対象デバイスにプッシュする方法：

アクセス：Admin/Maint

ステップ 1　[System] > [Tools] > [Scheduling] を選択します。

[Scheduling] ページが表示されます。

ステップ 2　[Add Task] をクリックします。

[New Task] ページが表示されます。

ステップ 3　[Job Type] リストから、[Push Latest Update] を選択します。

ページがリロードされ、更新をプッシュするためのオプションが表示されます。

ステップ 4　タスクをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。[Current Time] フィールドには、アプライアンスの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定（62-2 ページ）を参照してください。

ステップ 5　[Job Name] フィールドに、255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 6　[Device] リストから、更新を受け取るデバイスを選択します。

ステップ 7　オプションで、[Comment] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント　コメント フィールドはページの [View Tasks] セクションに表示されるので、ある程度短くしてください。

ステップ 8　オプションで、[Email Status To:] フィールドに、ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定（63-19 ページ）を参照してください。

ステップ 9　[Save] をクリックします。

タスクが追加されます。[Task Status] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示（C-1 ページ）を参照）。

ソフトウェア インストールの自動化

ライセンス：すべて

Defense Centerを使用して、管理対象デバイスにソフトウェア更新をインストールするタスクを作成する場合は、更新をデバイスにプッシュするタスクと、更新をインストールするタスクの間に十分な時間を確保してください。管理対象デバイスに更新をプッシュする方法の詳細については、ソフトウェア プッシュの自動化（62-14 ページ）を参照してください。

注意　インストールする更新によっては、ソフトウェアのインストール後にアプライアンスがリブートする場合があります。

ソフトウェア インストール タスクをスケジュールする方法:

アクセス: Admin/Maint

ステップ 1　[System] > [Tools] > [Scheduling] を選択します。

[Scheduling] ページが表示されます。

ステップ 2　[Add Task] をクリックします。

[New Task] ページが表示されます。

ステップ 3　[Job Type] リストから、[Install Latest Update] を選択します。

ページがリロードされ、更新をインストールするためのオプションが表示されます。

ステップ 4　タスクをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。[Current Time] フィールドには、アプライアンスの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定（62-2 ページ）を参照してください。

ステップ 5　[Job Name] フィールドに、255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 6　[Device] リストで、次の操作を行うことができます。

- 更新のインストール場所となるデバイスを選択します。
- Defense Centerの名前を選択して、更新をそこにインストールします。

ステップ 7　[Update Items] セクションで、[Software] を選択します。

ステップ 8　オプションで、[Comment] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント　コメント フィールドはページの [View Tasks] セクションに表示されるので、ある程度短くしてください。

ステップ 9　オプションで、[Email Status To:] フィールドに、ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定（63-19 ページ）を参照してください。

ステップ 10　[Save] をクリックします。

タスクが追加されます。[Task Status] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示（C-1 ページ）を参照）。

脆弱性データベースの更新の自動化

ライセンス：FireSIGHT

FireSIGHT システムで認識されるネットワーク アセット、トラフィック、および脆弱性のリストを拡張するために、Ciscoでは脆弱性データベース (VDB) 更新を使用しています。スケジュール機能を使用して最新の VDB 更新をDefense Centerにダウンロード/インストールすることにより、常に最新の情報を使ってネットワーク上のホストを評価できます。

注　サポート サイトにアクセスできないアプライアンスの更新をスケジュールすることはできません。アプライアンスがインターネットに直接接続しない場合、管理インターフェイスの構成 (64-9 ページ) の説明に従って、サポート サイトから更新をダウンロードできるようプロキシをセットアップする必要があります。FireSIGHT システムの手動更新について詳しくは、システム ソフトウェアの更新 (66-1 ページ) を参照してください。

VDB 更新を自動化するには、次に示す 2 つの別個の手順を自動化する必要があります。

ステップ 1　VDB 更新をダウンロードします。

ステップ 2　VDB 更新をインストールします。

プロセスを完了させるには、タスクとタスクの間に必ず十分な時間を確保してください。たとえば、更新のインストール タスクをスケジュールする場合、更新がまだ完全にダウンロードされていないと、インストール タスクは正しく実行されません。ただし、スケジュール済みインストール タスクが毎日繰り返される場合は、翌日のタスク実行時に、すでにダウンロードされた VDB 更新がインストールされます。

このプロセスをより確実に制御するには、更新がリリースされたことがわかった後、[Once] オプションを使用してオフピーク時間帯に VDB 更新をダウンロード/インストールできます。

注　VDB の更新をインストールすると、トラフィック フローと処理が一時的に停止することがあります。また、いくつかのパケットが検査されない場合があります。

詳細については、次の項を参照してください。

- VDB 更新のダウンロードの自動化 (62-17 ページ)
- VDB 更新のインストールの自動化 (62-18 ページ)

VDB 更新のダウンロードの自動化

ライセンス：FireSIGHT

Defense Center上で、Ciscoから最新の VDB 更新を自動的にダウンロードするスケジュール済みタスクを作成できます。

VDB 更新のダウンロードを自動化する方法：

アクセス：Admin/Maint

ステップ 1　[System] > [Tools] > [Scheduling] を選択します。

[Scheduling] ページが表示されます。

ステップ 2　[Add Task] をクリックします。

[New Task] ページが表示されます。

ステップ 3　[Job Type] リストから、[Download Latest Update] を選択します。

[New Task] ページがリロードされ、更新オプションが示されます。

ステップ 4　タスクをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。[Current Time] フィールドには、アプライアンスの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定（62-2 ページ）を参照してください。

ステップ 5　[Job Name] フィールドに、255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 6　[Update Items] セクションで、脆弱性データベースを示す [Vulnerability Database] を選択します。

ステップ 7　オプションで、[Comment] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント　コメント フィールドはページの [View Tasks] セクションに表示されるので、ある程度短くしてください。

ステップ 8　オプションで、[Email Status To:] フィールドに、ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定（63-19 ページ）を参照してください。

ステップ 9　[Save] をクリックします。

タスクが追加されます。[Task Status] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示（C-1 ページ）を参照）。

VDB 更新のインストールの自動化

ライセンス：FireSIGHT

VDB 更新をダウンロードするタスクと、その更新をインストールするタスクの間に十分な時間を確保する必要があります。詳細については、VDB 更新のダウンロードの自動化（62-17 ページ）を参照してください。

注　VDB の更新をインストールすると、トラフィック フローと処理が一時的に停止することがあります。また、いくつかのパケットが検査されない場合があります。

VDB 更新をスケジュールする方法：

アクセス：Admin/Maint

ステップ 1　[System] > [Tools] > [Scheduling] を選択します。

[Scheduling] ページが表示されます。

ステップ 2　[Add Task] をクリックします。

[New Task] ページが表示されます。

ステップ 3　[Job Type] リストから、[Install Latest Update] を選択します。

ページがリロードされ、更新をインストールするためのオプションが表示されます。

ステップ 4　タスクをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。[Current Time] フィールドには、アプライアンスの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定（62-2 ページ）を参照してください。

ステップ 5　[Job Name] フィールドに、255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 6　[Device] ドロップダウン リストから、Defense Centerの名前を選択します。

ステップ 7　[Update Items] セクションで、脆弱性データベースを示す [Vulnerability Database] を選択します。

ステップ 8　オプションで、[Comment] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント　コメント フィールドはページの [View Tasks] セクションに表示されるので、ある程度短くしてください。

ステップ 9　オプションで、[Email Status To:] フィールドに、ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定（63-19 ページ）を参照してください。

ステップ 10　[Save] をクリックします。

タスクが追加されます。[Task Status] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示（C-1 ページ）を参照）。

URL フィルタリング更新の自動化

ライセンス： URL Filtering

サポートされる防御センター： すべて（DC500 を除く）

スケジューラを使用して、Collective Security Intelligence クラウドからの URL フィルタリング データの更新を自動化できます。URL フィルタリングを更新するタスクが正しく実行されるには:

- Defense Centerがインターネットにアクセスできる必要があります。アクセスできない場合は、クラウドと通信できません。
- クラウド通信の有効化（64-30 ページ）の説明に従って、URL フィルタリングを有効にする必要があります。

また、URL フィルタリングを有効にする際に、自動更新を有効にできることに注意してください。その場合、URL フィルタリング データの更新を確認するためにDefense Centerは必ず 30 分ごとにクラウドと通信します。自動更新がすでに有効になっている場合は、URL フィルタリング データを更新するスケジュール済みタスクを作成**しないでください**。

通常、毎日の更新は小規模ですが、最終更新日から 5 日を超えると、帯域幅によっては新しい URL フィルタリング データのダウンロードに最長 20 分かかる場合があります。その後、更新自体を実行するのに最長で 30 分かかることがあります。

URL フィルタリング データのタスクを自動化する方法:

アクセス： Admin/Maint

ステップ 1　[System] > [Tools] > [Scheduling] を選択します。

[Scheduling] ページが表示されます。

ステップ 2　[Add Task] をクリックします。

[New Task] ページが表示されます。

ステップ 3　[Job Type] リストから、[Update URL Filtering Database] を選択します。

ページがリロードされ、URL フィルタリング更新のオプションが示されます。

ステップ 4　更新をスケジュールする頻度として、ワンタイム更新を示す [Once] または定期更新を示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。[Current Time] フィールドには、アプライアンスの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定（62-2 ページ）を参照してください。

ステップ 5　[Job Name] フィールドに、255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 6　オプションで、[Comment] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント　コメント フィールドはページの [View Tasks] セクションに表示されるので、ある程度短くしてください。

ステップ 7　オプションで、[Email Status To:] フィールドに、ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定（63-19 ページ）を参照してください。

ステップ 8　[Save] をクリックします。

タスクが追加されます。[Task Status] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示（C-1 ページ）を参照）。

タスクの表示

ライセンス： すべて

スケジュール済みタスクを追加した後、それらのタスクを表示したり、状態を評価したりできます。ページの [View Options] セクションで、カレンダーやスケジュール済みタスク リストを使用してスケジュール済みタスクを表示できます。

詳細については、次の項を参照してください。

- カレンダーの使用法（62-21 ページ）
- タスク リストの使用法（62-22 ページ）

カレンダーの使用法

ライセンス： すべて

カレンダー表示オプションを使用すると、どの日にどのスケジュール済みタスクが行われるかを表示できます。

カレンダーを使用してスケジュール済みタスクを表示する方法：

アクセス： Admin/Maint

ステップ 1　[System] > [Tools] > [Scheduling] を選択します。

[Scheduling] ページが表示されます。

ステップ 2　カレンダー ビューを使用して、次のタスクを実行できます。

- 二重左矢印アイコン（  ）をクリックすると、1 年戻ります。
- 単一の左矢印アイコン（）をクリックすると、1 ヵ月戻ります。
- 単一の右矢印アイコン（）をクリックすると、1 ヵ月進みます。
- 二重右矢印アイコン（  ）をクリックすると、1 年進みます。
- [Today] をクリックすると、現在の年月に戻ります。
- [Add Task] をクリックすると、新しいタスクをスケジュールできます。
- 1 つの日付をクリックすると、カレンダーの下にあるタスク リスト表に、特定の日付のスケジュール済みタスクがすべて表示されます。

- ある日付の特定のタスクをクリックすると、カレンダーの下にあるタスク リスト表にそのタスクが表示されます。

注　タスク リストの使用方法の詳細については、タスク リストの使用法を参照してください。

タスク リストの使用法

ライセンス： すべて

タスク リストには、タスクのリストとその状態が表示されます。タスク リストき、カレンダーを開いたときにカレンダーの下にが表示されます。また、カレンダーで 1 つの日付またはタスクを選択してアクセスすることもできます。詳細については、「カレンダーの使用法（62-21 ページ）」を参照してください。

表 62-1　タスク リストのカラム

カラム	説明
名前	スケジュール済みタスクの名前と、関連付けられているコメントを表示します。
タイプ	スケジュール済みタスクのタイプを表示します。
Start Time	スケジュールされている開始日時を表示します。
Frequency	タスクの実行頻度を表示します。
Status（ステータス）	スケジュール済みタスクの現在の状態を次のように示します。 • チェック マーク アイコン（）は、タスクが正常に実行されたことを示します。 • 疑問符アイコン（  ）は、タスクの状態が不明であることを示します。 • 感嘆符アイコン（  ）は、タスクが失敗したことを示します。
Creator	スケジュール済みタスクを作成したユーザの名前を表示します。
編集	スケジュール済みタスクを編集します。
削除	スケジュール済みタスクを削除します。

スケジュール済みタスクの編集

ライセンス： すべて

以前に作成したスケジュール済みタスクを編集できます。この機能は、パラメータが正しいことを確認するために、スケジュール済みタスクを 1 度テストする場合に特に役立ちます。タスクが正常に完了したら、あとで定期タスクに変更できます。

既存のスケジュール済みタスクを編集する方法：

アクセス： Admin/Maint

ステップ 1　[System] > [Tools] > [Scheduling] を選択します。

[Scheduling] ページが表示されます。

ステップ 2　編集するタスク、またはタスクが表示されている日付をクリックします。

[Task Details] 表に、選択した 1 つ以上のタスクが示されます。

ステップ 3　この表で、編集するタスクを見つけて編集アイコン（  ）をクリックします。

[Edit Task] ページが表示され、選択したタスクの詳細が示されます。

ステップ 4　必要に応じて、タスクの開始時間、ジョブ名、コメント、実行頻度（1 度または繰り返し）などを編集します。ジョブのタイプを変更することはできません。

残りのオプションは、編集中のタスクに応じて異なります。詳細については、次の項を参照してください。

- バックアップ ジョブの自動化（62-3 ページ）
- 証明書失効リストのダウンロードの自動化（62-4 ページ）
- Nmap スキャンの自動化（62-5 ページ）
- レポートの生成を自動化する方法（62-9 ページ）
- FireSIGHT 推奨の自動化（62-11 ページ）
- ソフトウェア更新の自動化（62-12 ページ）
- 脆弱性データベースの更新の自動化（62-17 ページ）
- URL フィルタリング更新の自動化（62-20 ページ）

ステップ 5　[Save] をクリックして編集内容を保存します。

変更が保存され、[Scheduling] ページが再び表示されます。

スケジュール済みタスクの削除

ライセンス： すべて

[Schedule View] ページから 2 種類の削除操作を実行できます。まだ実行されていない特定のワンタイム タスク、または定期タスクのすべてのインスタンスを削除できます。定期タスクの 1 つのインスタンスを削除すると、そのタスクのすべてのインスタンスが削除されます。1 度だけ実行するようスケジュールされているタスクを削除すると、そのタスクだけが削除されます。

以下の項では、タスクを削除する方法について説明します。

- タスクのすべてのインスタンスを削除するには、定期タスクの削除（62-23 ページ）を参照してください。
- タスクの 1 つのインスタンスを削除するには、ワンタイム タスクの削除（62-24 ページ）を参照してください。

定期タスクの削除

ライセンス： すべて

定期タスクの 1 つのインスタンスを削除すると、そのタスクのすべてのインスタンスが自動的に削除されます。

定期タスクを削除する方法:

アクセス: Admin/Maint

ステップ 1　[System] > [Tools] > [Scheduling] を選択します。

[Scheduling] ページが表示されます。

ステップ 2　カレンダーで、削除する定期タスクのインスタンスを 1 つ選択します。

ページがリロードされ、カレンダーの下にタスクの表が表示されます。

ステップ 3　この表で、削除する定期タスクのインスタンスを見つけて、削除アイコン( )をクリックします。

その定期タスクのすべてのインスタンスが削除されます。

ワンタイム タスクの削除

ライセンス: すべて

タスク リストを使用して、スケジュール済みのワンタイム タスクを削除したり、以前に実行されたスケジュール済みタスクのレコードを削除したりできます。

1 つのタスク(そのタスクがすでに実行済みの場合はタスク レコード)を削除する方法:

アクセス: Admin/Maint

ステップ 1　[System] > [Tools] > [Scheduling] を選択します。

[Scheduling] ページが表示されます。

ステップ 2　削除するするタスク、またはタスクが表示されている日付をクリックします。

選択した 1 つ以上のタスクを含む表が表示されます。

ステップ 3　この表で、削除するタスクを見つけて削除アイコン( )をクリックします。

選択したタスクのインスタンスが削除されます。

CHAPTER 63

システム ポリシーの管理

システム ポリシーを使用して、FireSIGHT システム アプライアンスで次のものを管理できます。

- アクセス コントロールの設定
- アプライアンスのアクセス リスト
- 監査ログ設定
- 外部認証
- ダッシュボードの設定
- データベース イベント制限
- DNS キャッシュのプロパティ
- メール リレー ホストおよび通知アドレス
- 侵入ポリシーおよびネットワーク解析ポリシーの変更のトラッキング
- 別の言語の指定
- カスタム ログイン バナー
- SNMP ポーリング設定
- 時間の同期
- STIG コンプライアンス
- Defense Centerからの時間の提供
- ユーザ インターフェイスとコマンド ライン インターフェイスのタイムアウト設定
- サーバのマッピングの脆弱性

システム ポリシーを使用して、展開内の他のアプライアンスで同じ可能性が高いDefense Centerの側面を制御できます。たとえば、組織のセキュリティ ポリシーによっては、ユーザのログイン時に表示するアプライアンスの「No Unauthorized Use」メッセージを必要とする場合があります。システム ポリシーを使用すると、Defense Centerのシステム ポリシーでログイン バナーを一度設定すれば、管理するすべてのデバイスにそのポリシーを適用できます。

また、Defense Centerで複数のシステム ポリシーを活用することもできます。たとえば、さまざまな状況で別々のメール リレー ホストを使用する場合や、さまざまなデータベース制限をテストする場合は、単一のポリシーを編集するのではなく、いくつかのシステム ポリシーを作成し、それらを切り替えることができます。

システム ポリシー（展開内で同じ可能性が高いアプライアンスの側面を制御する）をシステム設定（単一のアプライアンスに固有である可能性が高い）と比較します。詳細については、「アプライアンス設定の構成（64-1 ページ）」を参照してください。

詳細については、次の項を参照してください。

- システム ポリシーの作成（63-2 ページ）
- システム ポリシーの編集（63-3 ページ）
- システム ポリシーの適用（63-4 ページ）
- システム ポリシーの比較（63-5 ページ）
- システム ポリシーの削除（63-7 ページ）

システム ポリシーの作成

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

システム ポリシーを作成したら、それに名前と説明を割り当てます。次に、ポリシーのさまざまな側面（それぞれの項の説明を参照）を設定します。

新しいポリシーを作成する代わりに、別のアプライアンスからシステム ポリシーをエクスポートし、アプライアンスにインポートすることができます。必要に合わせて、インポートされたポリシーを編集してから、それを適用することができます。詳細については、設定のインポートおよびエクスポート（A-1 ページ）を参照してください。

システム ポリシーを作成する方法：

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

[Policy Name] 列には、システム ポリシーの説明が含まれます。[Applied to] 列は、そのポリシーが適用されているアプライアンスの数と、以前に適用されたポリシーが変更されており、再適用が必要な **out-of-date** アプライアンスの数を示します。

ステップ 2　[Create Policy] をクリックします。

[Create Policy] ページが表示されます。

ステップ 3　ドロップダウン リストから、新しいシステム ポリシーのテンプレートとして使用する既存のポリシーを選択します。

ステップ 4　新規ポリシーの名前を [New Policy Name] フィールドに入力します。

ステップ 5　新規ポリシーの説明を [New Policy Description] フィールドに入力します。

ステップ 6　[Create] をクリックします。

システム ポリシーが保存され、[Edit System Policy] ページが表示されます。システム ポリシーのそれぞれの側面の設定については、次の項のいずれかを参照してください。

- アプライアンスのアクセス リストの設定（63-9 ページ）
- 監査ログの設定（63-11 ページ）
- 外部認証の有効化（63-12 ページ）
- ダッシュボードの設定（63-15 ページ）
- データベース イベント制限の設定（63-16 ページ）
- DNS キャッシュ プロパティの設定（63-18 ページ）

システム ポリシーの編集

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

既存のシステム ポリシーを編集できます。アプライアンスに現在適用されているシステム ポリシーを編集する場合、変更を保存した後にポリシーを再適用してください。詳細については、システム ポリシーの適用（63-4 ページ）を参照してください。

既存のシステム ポリシーを編集する方法：

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

既存のシステム ポリシーのリストを含む、[System Policy] ページが表示されます。

ステップ 2　編集するシステム ポリシーの横にある編集アイコン（  ）をクリックします。

[Edit Policy] ページが表示されます。ポリシー名とポリシーの説明を変更できます。システム ポリシーのそれぞれの側面の設定については、次の項のいずれかを参照してください。

- アクセス コントロール ポリシー設定の構成（63-8 ページ）
- アプライアンスのアクセス リストの設定（63-9 ページ）
- 監査ログの設定（63-11 ページ）
- 外部認証の有効化（63-12 ページ）
- ダッシュボードの設定（63-15 ページ）
- データベース イベント制限の設定（63-16 ページ）
- DNS キャッシュ プロパティの設定（63-18 ページ）
- メール リレー ホストおよび通知アドレスの設定（63-19 ページ）
- ネットワーク解析ポリシーの設定の構成（63-21 ページ）

- 侵入ポリシー設定の構成（63-22 ページ）
- 別の言語の指定（63-23 ページ）
- カスタム ログイン バナーの追加（63-24 ページ）
- SNMP ポーリングの設定（63-24 ページ）
- 時刻の同期（63-27 ページ）
- Defense Centerからの時刻の提供（63-29 ページ）
- ユーザ インターフェイスの設定（63-30 ページ）
- サーバの脆弱性のマッピング（63-32 ページ）

注　アプライアンスに適用されているシステム ポリシーを編集する場合、編集が完了したら、更新されたポリシーを再適用してください。システム ポリシーの適用（63-4 ページ）を参照してください。

ステップ 3　[Save Policy and Exit] をクリックして変更を保存します。変更が保存され、[System Policy] ページが表示されます。

システム ポリシーの適用

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

アプライアンスにシステム ポリシーを適用できます。システム ポリシーがすでに適用されている場合、再適用するまで、ポリシーに加えた変更は有効になりません。

注　システム ポリシーは Cisco NGIPS for Blue Coat X-Series には適用**できません**。

システム ポリシーを適用する方法：

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　適用するシステム ポリシーの横にある適用アイコン（ ）をクリックします。

[Apply] ページが表示されます。

ステップ 3　システム ポリシーを適用するアプライアンスを選択します。

ヒント　グループ、モデル、ヘルス ポリシー、または適用済みのシステム ポリシーごとにアプライアンスをソートできます。個々のアプライアンスまたはグループ全体を選択できます。

ステップ 4　[Apply] をクリックします。

[System Policy] ページが表示されます。メッセージはシステム ポリシーの適用のステータスを示します。

システム ポリシーの比較

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

ユーザがアクセスできるシステム ポリシーに応じて、2 つのシステム ポリシーまたは同じシステム ポリシーの 2 つのリビジョンを比較できます。これにより、組織の規格のコンプライアンスや、システム パフォーマンスの最適化を目的として、ポリシー変更を確認することができます。アクティブなシステム ポリシーを別のポリシーと素早く比較する場合は、[Running Configuration] オプションを選択できます。比較後に PDF レポートを生成して、システム ポリシー間またはシステム ポリシーのリビジョン間の相違点を記録することもできます。

システム ポリシーまたはシステム ポリシーのリビジョンを比較するために使用できる 2 つのツールがあります。

- 比較ビューには、2 つのシステム ポリシー間またはシステム ポリシーのリビジョン間の相違点がサイドバイサイド形式で表示されます。各ポリシーまたはポリシー リビジョンの名前は、比較ビューの左右のタイトル バーに表示されます。

  これを使用して、Web インターフェイスで相違点を強調表示したまま、両方のポリシーのリビジョンを表示し移動することができます。

- 比較レポートでは、2 つのシステム ポリシー間またはシステム ポリシーのリビジョン間の相違点のレコードがシステム ポリシーと同様の形式（ただし、PDF 形式）で作成されます。

  これを使用して、ポリシーの比較の保存、コピー、出力、共有を行って、さらに検証することができます。

システム ポリシーの比較ビューの使用

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

比較ビューには、両方のシステム ポリシーまたはポリシー リビジョンがサイドバイサイド形式で表示され、各ポリシーまたはポリシー リビジョンは、比較ビューの左右のタイトル バーにある名前で識別されます。すべてのリビジョンについては、システム ポリシーの比較ビューのポリシー名の右側に、最後に修正が行われた時間と最後のユーザが表示されます。

2 つのシステム ポリシーまたはシステム ポリシーのリビジョンの相違点は次のように強調表示されます。

- 青色は強調表示された設定が 2 つのポリシーまたはポリシー リビジョンで違うことを意味します。違いは赤色のテキストで表示されます。
- 緑は、強調表示されている設定が一方のポリシーまたはポリシー リビジョンにあるものの、もう一方の設定にはないことを示します。

次の表に、実行できる操作を記載します。

表 63-1　システム ポリシーの比較ビューの操作

目的	操作
変更に個別にナビゲートする	タイトル バーの上の [Previous] または [Next] を選択します。 左側と右側の間にある二重矢印アイコン（◂▸）が移動し、表示している違いを示す [Difference] 番号が変わります。
新しいシステム ポリシーの比較ビューを生成する	[New Comparison] を選択します。 [Select Comparison] ウィンドウが表示されます。詳細については、「システム ポリシーの比較レポートの使用」を参照してください。
システム ポリシーの比較レポートを生成する	[Comparison Report] を選択します。 システム ポリシーの比較レポートは、システム ポリシーの比較ビューと同じ情報を含む PDF です。

システム ポリシーの比較レポートの使用

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

システム ポリシーの比較レポートは、システム ポリシーの比較ビューで特定された、2 つのシステム ポリシー間または同じシステム ポリシーの 2 つのリビジョン間の相違点をすべて記録したものであり、PDF 形式で提供されます。このレポートを使用して、2 つのシステム ポリシーの設定の間の相違点をさらに調べ、その結果を保存して配信することができます。

システム ポリシーの比較レポートは、ユーザがアクセスできる任意のシステム ポリシーの比較ビューから生成できます。ユーザがシステム ポリシーに加えた変更は、変更を保存するまではシステム ポリシーの比較レポートに表示されません。

設定によっては、システム ポリシーの比較レポートに 1 つ以上のセクションを含めることができます。それぞれのセクションで、同じ形式が使用され、同じレベルの詳細が提供されます。[Value A] 列と [Value B] 列は、比較ビューで設定されたポリシーまたはポリシー リビジョンを表していることに注意してください。

ヒント　同様の手順を使用して、SSL ポリシー、ネットワーク解析ポリシー、侵入ポリシー、ファイル ポリシー、アクセス コントロール ポリシー、またはヘルス ポリシーを比較できます。

2 つのシステム ポリシーまたは同じポリシーの 2 つのリビジョンを比較する方法：

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　[Compare Policies] をクリックします。

[Select Comparison] ポップアップ ウィンドウが表示されます。

ステップ 3　[Compare Against] ドロップダウンリストから、比較するタイプを次のように選択します。

- 異なる 2 つのポリシーを比較するには、[Other Policy] を選択します。
- 同じポリシーの 2 つのリビジョンを比較するには、[Other Revision] を選択します。

- 別のポリシーと現在アクティブなポリシーを比較するには、[Running Configuration] を選択します。

ステップ 4　選択した比較タイプに応じて、次のような選択肢があります。

- 2 つの異なるポリシーを比較する場合は、[Policy A] および [Policy B] ドロップダウンリストのそれぞれから、比較するポリシーを選択します。
- 同じポリシーの 2 つのリビジョンを比較する場合は、[Policy] ドロップダウンリストからポリシーを選択し、次に [Revision A] および [Revision B] ドロップダウンリストから比較するリビジョンを選択します。
- 実行中の設定を別のポリシーと比較する場合は、[Target/Running Configuration A] ドロップダウン リストから実行中の設定を選択し、[Policy B] ドロップダウン リストから他のポリシーを選択します。

ステップ 5　システム ポリシーの比較ビューを表示するには、[OK] をクリックします。

比較ビューが表示されます。

ステップ 6　システム ポリシーの比較レポートを生成するには、[Comparison Report] をクリックします。

システム ポリシーの比較レポートが表示されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。

システム ポリシーの削除

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

システム ポリシーは、使用中でも削除できます。使用中の場合、新しいポリシーが適用されるまで現在のポリシーが使用されます。デフォルトのシステム ポリシーは削除できません。

システム ポリシーを削除する方法：

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　削除するシステム ポリシーの横にある削除アイコン（ ）をクリックします。ポリシーを削除するには、[OK] をクリックします。

[System Policy] ページが表示されます。ポリシーを削除するかどうか確認するポップアップ メッセージが表示されます。

システム ポリシーの設定

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

さまざまなシステム ポリシーの設定を行うことができます。システム ポリシーのそれぞれの側面の設定については、次の項のいずれかを参照してください。

アクセス コントロール ポリシー設定の構成

ライセンス： Protection

サポートされるデバイス： すべて（X-Series を除く）

ユーザがアクセス コントロール ポリシーでルールを追加または変更する場合、ルールのコメントの入力を要求するようにシステムを設定できます。これを使用して、ユーザのポリシーの変更の理由を追跡できます。アクセス コントロール ルールの変更に関するコメントを有効にした場合、ルールのコメントをオプションまたは必須に設定できます。システムは、ルールに対する新しい変更が保存されるたびに、ユーザにコメントを入力するようプロンプトを出します。

ユーザがルールを保存したときに、システムはルールのコメントの履歴にコメントを追加します。詳細については、ルールへのコメントの追加（14-14 ページ）を参照してください。

アクセス コントロール ポリシーのルール コメントの設定を構成する方法：

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーのアクセス コントロール ポリシーの設定を変更するには、システム ポリシーの横にある編集アイコン（  ）をクリックします。
- 新しいシステム ポリシーの一部としてアクセス コントロール ポリシーの設定を行うには、[Create Policy] をクリックします。

  システム ポリシーの作成（63-2 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[Save] をクリックします。

いずれの場合も、[Access List] ページが表示されます。

ステップ 3　[Access Control Preferences] をクリックします。

[Access Control Preferences] ページが表示されます。

ステップ 4　次の選択肢があります。

- ドロップダウン リストから [Disabled] を選択すると、ユーザはコメントを入力せずにアクセス コントロール ポリシーのルールを追加または変更できます。
- ドロップダウン リストから [Optional] を選択すると、アクセス コントロール ポリシーのルールに対する変更を保存するときに [Description of Changes (Optional)] ウィンドウが表示されます。これにより、ユーザはコメントの変更について記述することができます。
- ドロップダウン リストから [Required] を選択すると、アクセス コントロール ポリシーのルールに対する変更を保存するときに [Description of Changes (Required)] ウィンドウが表示されます。この場合、ユーザは変更を保存する前にコメントの変更について記述する必要があります。

ステップ 5　[Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、「システム ポリシーの適用（63-4 ページ）」を参照してください。

アプライアンスのアクセス リストの設定

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

[Access List] ページを使用して、特定のポートのアプライアンスにコンピュータがアクセスできるかを制御できます。デフォルトでは、Web インターフェイスへのアクセスに使用するポート 443（Hypertext Transfer Protocol Secure（HTTPS））、コマンドラインへのアクセスに使用するポート 22（Secure Shell（SSH））が任意の IP アドレスに対して有効です。ポート 161 を介した SNMP アクセスを追加することもできます。SNMP 情報をポーリングするには、使用する任意のコンピュータで SNMP アクセスを追加する必要があることに注意してください。

注意　デフォルトでは、アプライアンスへのアクセスは制限**されません**。よりセキュアな環境でアプライアンスを稼動させるために、特定の IP アドレスに対してアプライアンスへのアクセスを追加してから、デフォルトのオプション**すべて**を削除することを検討してください。

アクセス リストは、システム ポリシーの一部です。新しいシステム ポリシーを作成するか、既存のシステム ポリシーを編集することによって、アクセス リストを指定できます。いずれの場合も、システム ポリシーを適用するまでアクセス リストは有効になりません。

このアクセス リストは、外部データベース アクセスを制御しないことに注意してください。外部データベースのアクセス リストの詳細については、データベースへのアクセスの有効化（64-7 ページ）を参照してください。

アクセス リストを設定するには、次の手順を実行します。

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーのアクセス リストを変更するには、システム ポリシーの横にある編集アイコン（  ）をクリックします。
- 新しいシステム ポリシーの一部としてアクセス リストを設定するには、[Create Policy] をクリックします。

  システム ポリシーの作成（63-2 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[Save] をクリックします。

いずれの場合も、[Access List] ページが表示されます。

ステップ 3　現在の設定の 1 つを削除するために、削除アイコン（  ）をクリックすることもできます。

設定が削除されます。

注意　アプライアンスのインターフェイスへの接続に現在使用されている IP アドレスへのアクセスを削除し、`IP=any port=443` のエントリが存在しない場合、ポリシーを適用した時点でシステムへのアクセスは失われます。

ステップ 4　1 つ以上の IP アドレスへのアクセスを追加するために、[Add Rules] をクリックすることもできます。

[Add IP Address] ページが表示されます。

ステップ 5　[IP Address] フィールドでは、追加する IP アドレスに応じて以下の選択肢があります。

- 厳密な IP アドレス（`192.168.1.101` など）
- CIDR 表記を使用した IP アドレス ブロック（`192.168.1.1/24` など）

  FireSIGHT システムでの CIDR の使用方法については、IP アドレスの表記規則（1-23 ページ）を参照してください。
- `any`（任意の IP アドレスを指定）

ステップ 6　[SSH]、[HTTPS]、[SNMP]、またはこれらのオプションの組み合わせを選択して、これらの IP アドレスで有効にするポートを指定します。

ステップ 7　[Add] をクリックします。

[Access List] ページが再度表示され、ユーザが行った変更が反映されます。

ステップ 8　[Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、「システム ポリシーの適用（63-4 ページ）」を参照してください。

監査ログの設定

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

アプライアンスが外部ホストに監査ログをストリーミングするように、システム ポリシーを設定できます。

注　外部ホストが機能しており、監査ログを送信するアプライアンスからアクセス可能であることを確認する必要があります。

送信元ホスト名は送信される情報の一部です。ファシリティ、重大度、およびオプションのタグを使用して監査ログ ストリームをより詳細に識別できます。アプライアンスは、システム ポリシーが適用されるまで監査ログを送信しません。

この機能が有効になっている状態でポリシーが適用され、宛先ホストが監査ログを受け入れるように設定された後で、syslog メッセージが送信されます。次に、出力構造の例を示します。

```
Date Time Host [Tag] Sender: [User_Name]@[User_IP], [Subsystem], [Action]
```

現地の日付、時刻、およびホスト名の後に、角括弧で囲まれたオプション タグが続き、送信側デバイス名の後に監査ログ メッセージが続きます。

次に例を示します。

```
Mar 01 14:45:24 localhost [TAG] Dev-DC3000: admin@10.1.1.2, Operations > Monitoring, Page View
```

監査ログの設定を行うには、次の手順を実行します。

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーの監査ログの設定を変更するには、システム ポリシーの横にある編集アイコン（）をクリックします。
- 新しいシステム ポリシーの一部として監査ログ設定を設定するには、[Create Policy] をクリックします。

  システム ポリシーの作成（63-2 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[Save] をクリックします。

いずれの場合も、[Access List] ページが表示されます。

ステップ 3　[Audit Log Settings] をクリックします。

[Audit Log Settings] ページが表示されます。

ステップ 4　[Send Audit Log to Syslog] ドロップダウン メニューから、[Enabled] を選択します。（デフォルト設定では [Disabled] になっています。）

ステップ 5　[Host] フィールドにあるホストの IP アドレスまたは完全修飾名を使用して、監査情報の宛先ホストを指定します。デフォルト ポート（514）が使用されます。

注意　監査ログを受け入れるように設定しているコンピュータが、リモート メッセージを受け入れるようにセットアップされていない場合、ホストは監査ログを受け入れません。

ステップ 6　[Facility] フィールドから syslog ファシリティを選択します。

ステップ 7　[Severity] フィールドから重大度を選択します。

ステップ 8　必要に応じて、[Tag (optional)] フィールドで参照タグを挿入します。

ステップ 9　外部 HTTP サーバに定期的な監査ログの更新を送信するには、[Send Audit Log to HTTP Server] ドロップダウン リストから [Enabled] を選択します。デフォルト設定では [Disabled] になっています。

ステップ 10　[URL to Post Audit] フィールドに、監査情報を送信する URL を指定します。次にリストされている HTTP POST 変数を要求するリスナー プログラムに対応する URL を入力する必要があります。

- `subsystem`
- `actor`
- `event_type`
- `message`
- `action_source_ip`
- `action_destination_ip`
- `result`
- `time`
- `tag`（上記のように定義されている場合）

注意　暗号化されたポストを許可するには、HTTPS URL を使用する必要があります。外部 URL に監査情報を送信すると、システム パフォーマンスに影響を与える場合があるので注意してください。

ステップ 11　[Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーをDefense Centerと管理対象デバイスに適用するまで、変更は有効になりません。詳細については、「システム ポリシーの適用（63-4 ページ）」を参照してください。

外部認証の有効化

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

通常、ユーザがアプライアンスにログインする際に、アプライアンスは、アプライアンスのローカル データベースに保存されているユーザ アカウントとユーザの資格情報を比較することによって、資格情報を検証します。ただし、外部認証サーバを参照する認証オブジェクトを作成する場合、システム ポリシーで外部認証を有効化することにより、ローカル データベースを使用せずに、Defense Centerまたは管理対象デバイスにログインしているユーザをそのサーバに認証させることができます。

外部認証が有効になっているシステム ポリシーをアプライアンスに適用した場合、アプライアンスはユーザ資格情報を LDAP または RADIUS サーバ上のユーザに対して検証します。さらに、ユーザがローカルの内部認証を有効にしており、ユーザ資格情報が内部データベースにない場合、アプライアンスは一致する資格情報のセットがないか外部サーバを検査します。ユーザが複数のシステムで同じユーザ名を持っている場合、すべてのサーバですべてのパスワードが動作します。ただし、使用可能な外部認証サーバで認証が失敗した場合、アプライアンスはローカル データベースの検査に戻らないので注意してください。

外部認証を有効にすると、アカウントが外部で認証されている任意のユーザのデフォルトのユーザ ロールを設定できます。これらのロールを組み合わせることができる場合は、複数のロールを選択できます。たとえば、自社の [Network Security] グループのユーザのみを取得する外部認証を有効化した場合、デフォルトのユーザ ロールを設定して [Security Analyst] ロールを組み込み、ユーザが自分で追加のユーザ設定を行わなくても収集されたイベント データにアクセスできるようにすることが可能です。ただし、外部認証がセキュリティ グループに加えて他のユーザのレコードを取得する場合、デフォルトのロールを未選択のままにしておきたい場合もあります。使用可能なユーザ ロールの詳細については、ユーザ特権について（61-4 ページ）を参照してください。

アクセス ロールが選択されていない場合、ユーザはログインできますが、どの機能にもアクセスできません。ユーザがログインを試行すると、アカウントが [User Management] ページに表示されます。ここで、追加の権限を付与するアカウント設定を編集できます。ユーザ アカウントの変更の詳細については、ユーザ特権とオプションの変更（61-58 ページ）を参照してください。

ヒント　1 つのユーザ ロールを使用するようにシステム ポリシーを設定してそのポリシーを適用し、後でポリシーを変更して別のデフォルトのユーザ ロールを使用し再適用する場合、アカウントを変更するか、削除して再作成するまで、変更前に作成されたユーザ アカウントはすべて、最初のユーザ ロールを保持します。

シェル アクセス用に LDAP サーバに対して正常に認証できるユーザのセットを指定する場合、システム ポリシーで外部認証を有効にする前に、LDAP 認証オブジェクト内でシェル アクセス属性および他の設定を行う必要があります。詳細については、LDAP 固有パラメータの設定（61-20 ページ）およびシェル アクセスについて（61-9 ページ）を参照してください。

CAC 認証および認可用に LDAP サーバに対して正常に認証できるユーザのセットを指定する場合、システム ポリシーで外部認証を有効にする前に、LDAP 認証オブジェクト内で UI アクセス属性、ユーザ名テンプレート、および他の設定を行う必要があります。詳細については、LDAP 固有パラメータの設定（61-20 ページ）およびCAC を使用した LDAP 認証について（61-10 ページ）を参照してください。

注　シェル アクセスと CAC 認証の両方をアプライアンスで有効にする場合は、個別の認証オブジェクトを作成し、それらをシステム ポリシーで別々に有効にする**必要があります**。

認証オブジェクトのカスタマイズが完了したら、ユーザは外部認証をDefense Centerのシステム ポリシーで有効にしてから、そのポリシーを管理対象デバイスにプッシュする必要があります。デバイスにポリシーを適用した後、外部で認証された対象ユーザはそのデバイスにログインできます。外部認証の設定を変更するには、Defense Centerでシステム ポリシーを変更してから、そのポリシーをデバイスに再度適用する必要があります。管理対象デバイスでの認証を無効にするには、Defense Centerのシステム ポリシーでそれを無効にし、デバイスにプッシュすることができます。

外部認証を有効にできるのは、物理および外部Defense Centerおよび管理対象デバイスのみであることに注意してください。システム ポリシーの適用による外部認証の有効化は、Cisco NGIPS for Blue Coat X-Seriesではサポートされません。

内部認証によってユーザがログインしようとすると、アプライアンスは最初にそのユーザがローカル ユーザ データベースに存在するかどうか検査します。ユーザが存在する場合、アプライアンスは次にユーザ名とパスワードをローカル データベースに対して検査します。一致が検出されると、ユーザは正常にログインします。ただし、ログインが失敗し、外部認証が有効になっている場合、アプライアンスはそれぞれの外部認証サーバに対して、ユーザをシステム ポリシーに表示される認証順序で検査します。ユーザ名およびパスワードが外部サーバからの結果と一致した場合、アプライアンスはユーザを、その認証オブジェクトに対してデフォルトの権限を持つ外部ユーザに変更します。

外部ユーザがログインしようとすると、アプライアンスは外部認証サーバに対してユーザ名およびパスワードを検査します。一致が検出されると、ユーザは正常にログインします。ログインが失敗した場合、ユーザのログイン試行は拒否されます。外部ユーザは、ローカル データベース内のユーザ リストに対して認証できません。ユーザが新しい外部ユーザの場合、外部認証オブジェクトのデフォルト権限を持つ外部ユーザ アカウントがローカル データベースに作成されます。

外部サーバでのユーザ認証を有効にする方法:

アクセス: Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーの外部認証の設定を変更するには、システム ポリシーの横にある編集アイコン( )をクリックします。
- 新しいシステム ポリシーの一部として外部認証の設定を行うには、[Create Policy] をクリックします。

  システム ポリシーの作成（63-2 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[Save] をクリックします。

いずれの場合も、[Access List] ページが表示されます。

ステップ 3　[External Authentication] をクリックします。

[External Authentication] ページが表示されます。

ステップ 4　[Status] ドロップダウン リストから [Enabled] を選択します。

ステップ 5　[Default User Role] ドロップダウン リストから、ユーザ ロールを選択して、外部認証済みユーザに付与するデフォルト権限を定義します。

ヒント　ロールを選択する前に Ctrl キーを押すと、複数のデフォルト ユーザ ロールを選択できます。[Security Analyst] ロールと対応する [Security Analyst（Read Only）] ロールの両方を選択した場合でも、適用されるのは [Security Analyst] ロールだけであることに注意してください。

ステップ 6　外部サーバを使用してシェル アクセス アカウントも認証する場合、[Shell Authentication] ドロップダウン リストから [Enabled] を選択します。

ステップ 7　CAC 認証および認可を有効にする場合は、[CAC Authentication] ドロップダウン リストから使用可能な CAC 認証オブジェクトを選択します。

CAC 認証および認可を設定するための完全な手順については、CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。

ステップ 8　事前設定された認証オブジェクトの使用を有効にするには、オブジェクトの横にあるチェックボックスを選択します。外部認証を有効にするには、少なくとも 1 つの認証オブジェクトを選択する**必要があります**。

ヒント　手順6でシェル認証を有効にした場合、シェル アクセスを許可するよう設定された認証オブジェクトを選択する**必要があります**。同じシステム ポリシーでシェル アクセスと CAC 認証を管理するには、別の認証オブジェクトを使用する**必要がある**ことに注意してください。詳細については、シェル アクセスについて（61-9 ページ）およびCAC を使用した LDAP 認証について（61-10 ページ）を参照してください。

ステップ 9　必要に応じて、上矢印および下矢印を使用して、認証要求が行われたときに認証サーバがアクセスされる順序を変更できます。

注　シェル アクセスのユーザは、認証オブジェクトがプロファイルの順序で最も高いサーバに対して**のみ**認証できることに注意してください。

ステップ 10　[Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーをDefense Centerと管理対象デバイスに適用するまで、変更は有効になりません。詳細については、「システム ポリシーの適用（63-4 ページ）」を参照してください。

ダッシュボードの設定

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

[Custom Analysis] ウィジェットがダッシュボードで有効になるように、システム ポリシーを設定できます。ダッシュボードでは、ウィジェットを使用することにより、現在のシステム ステータスが一目でわかります。ウィジェットは小さな自己完結型コンポーネントであり、FireSIGHT システムのさまざまな側面に関するインサイトを提供します。

[Custom Analysis] ウィジェットを使用して、柔軟でユーザが設定可能なイベントのクエリに基づいて、アプライアンスのデータベースにイベントを視覚的に作成することができます。カスタム ウィジェットの使用方法の詳細については、Custom Analysis ウィジェットについて（55-12 ページ）を参照してください。

[Custom Analysis] ウィジェットを有効にする方法：

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーのダッシュボードの設定を変更するには、システム ポリシーの横にある編集アイコン（ ）をクリックします。

- 新しいシステム ポリシーの一部としてダッシュボードの設定を行うには、[Create Policy] をクリックします。システム ポリシーの作成（63-2 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[Save] をクリックします。

いずれの場合も、[Access List] ページが表示されます。

ステップ 3　[Dashboard] をクリックします。

[Dashboard Settings] ページが表示されます。

ステップ 4　ユーザが [Custom Analysis] ウィジェットをダッシュボードに追加できるようにするには、[Enable Custom Analysis Widgets] チェック ボックスを選択します。ユーザがこれらのウィジェットを使用できないようにする場合は、このチェック ボックスをオフにします。

ステップ 5　[Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、「システム ポリシーの適用（63-4 ページ）」を参照してください。

データベース イベント制限の設定

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

[Database] ページを使用して、Defense Centerが保存できる各イベント タイプの最大数を指定します。監査レコードの設定は、管理対象デバイスにも適用されることに注意してください。パフォーマンスを向上させるには、定期的に処理するイベント数に合わせてイベント制限を調整する必要があります。一部のイベント タイプでは、ストレージを無効にすることができます。次の表は、各イベント タイプを保存できる最小および最大レコード数を示しています。

表 63-2　　データベース イベントの制限

イベント タイプ	イベントの上限	イベントの下限
侵入イベント	250 万（DC500） 1,000 万（DC1000、仮想 Defense Center） 2,000 万（DC750） 3,000 万（DC1500） 6,000 万（DC2000） 1 億（DC3000） 1 億 5,000 万（DC3500） 3 億（DC4000）	10,000
検出イベント	1,000 万 2,000 万（DC2000、DC4000）	ゼロ（ストレージを無効にする）
接続イベント セキュリティ インテリジェンス イベント	1,000 万（DC500、DC1000、仮想Defense Center） 5,000 万（DC750） 1 億（DC1500、DC3000） 3 億（DC2000） 5 億（DC3500） 10 億（DC4000） イベントの上限は、接続イベントとセキュリティ インテリジェンス イベントとの間で共有されます。2 つのイベントの設定済み最大数の合計はイベントの上限数を超えてはなりません。	ゼロ（ストレージを無効にする）

表 63-2　データベース イベントの制限（続き）

イベント タイプ	イベントの上限	イベントの下限
接続の要約（集約された接続イベント）	1,000 万（DC500、DC1000、仮想Defense Center） 5,000 万（DC750） 1 億（DC1500、DC3000） 3 億（DC2000） 5 億（DC3500） 10 億（DC4000）	ゼロ（ストレージを無効にする）
相関およびコンプライアンスのホワイト リスト イベント	100 万 200 万（DC2000、DC4000）	1
マルウェア イベント	1,000 万 2,000 万（DC2000、DC4000）	10,000
ファイル イベント	1,000 万 2,000 万（DC2000、DC4000）	ゼロ（ストレージを無効にする）
ヘルス イベント	100 万	ゼロ（ストレージを無効にする）
監査レコード	100,000	1
修復ステータス イベント	1,000 万	1
ネットワーク上のホストのホワイト リスト違反履歴	30 日間の違反履歴	1 日の履歴
ユーザ アクティビティ（ユーザ イベント）	1,000 万	1
ユーザ ログイン（ユーザ履歴）	1,000 万	1
ルール更新のインポート ログ レコード	100 万	1

侵入イベント データベース内のイベント数が最大数を超えると、データベースがイベントの制限内に戻るまで、最も古いイベントおよびパケット ファイルがプルーニングされます。イベントが自動的にプルーニングされたときに自動電子メール通知を生成する方法については、メール リレー ホストおよび通知アドレスの設定（63-19 ページ）を参照してください。

検出およびユーザ データベースを手動でプルーニングする方法の詳細については、データベースからの検出データの消去（B-1 ページ）を参照してください。

さらに、侵入イベントおよび監査レコードがデータベースからプルーニングされたときに通知を受け取る電子メール アドレスを設定できます。

データベース内のレコードの最大数を設定する方法：

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーのデータベースの設定を変更するには、システム ポリシーの横にある編集アイコン( )をクリックします。
- 新しいシステム ポリシーの一部としてデータベースの設定を行うには、[Create Policy] をクリックします。

  システム ポリシーの作成(63-2 ページ)で説明されているように、システム ポリシーの名前および説明を入力し、[Save] をクリックします。

いずれの場合も、[Access Control Preferences] ページが表示されます。

ステップ 3　[Database] をクリックします。

[Database] ページが表示されます。

ステップ 4　各データベースについて、保存するレコードの数を入力します。

各データベースが保持できるレコード数の詳細については、データベース イベントの制限を参照してください。

ステップ 5　必要に応じて、[Data Pruning Notification Address] フィールドで、侵入イベント、検出イベント、監査レコード、セキュリティ インテリジェンス データ、または URL フィルタリング データがアプライアンスのデータベースからプルーニングされたときに通知を受け取る電子メール アドレスを入力します。

また、電子メール サーバを設定する必要があることにも注意してください。詳細については、「メール リレー ホストおよび通知アドレスの設定(63-19 ページ)」を参照してください。

ステップ 6　[Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、「システム ポリシーの適用(63-4 ページ)」を参照してください。

DNS キャッシュ プロパティの設定

ライセンス: すべて

サポートされるデバイス: すべて(X-Series を除く)

DNS サーバが [Network] ページで設定されている場合、イベント ビュー ページで IP アドレスを自動的に解決するようにアプライアンスを設定できます。[Administrator] ロールが割り当てられたユーザは、アプライアンスによって実行される DNS キャッシングの基本プロパティも設定できます。DNS キャッシングを設定すると、追加のルックアップを実行せずに、以前に解決した IP アドレスを識別できます。これにより、IP アドレスの解決が有効になっている場合に、ネットワーク上のトラフィックの量を減らし、イベント ページの表示速度を早めることができます。

DNS キャッシュ プロパティを構成するには、次の手順を実行します。

アクセス: Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーの DNS キャッシュの設定を変更するには、システム ポリシーの横にある編集アイコン( )をクリックします。

- 新しいシステム ポリシーの一部として DNS キャッシュの設定を設定するには、[Create Policy] をクリックします。

  システム ポリシーの作成（63-2 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[Save] をクリックします。

いずれの場合も、[Access List] ページが表示されます。

ステップ 3　[DNS Cache] をクリックします。

[DNS Cache] ページが表示されます。

ステップ 4　キャッシングを有効にするには、[DNS Resolution Caching] ドロップダウン リストから [Enabled] を選択します。これを無効にするには、[Disabled] を選択します。

注　DNS 解決のキャッシングは、以前に解決された DNS ルックアップのキャッシングを許可するシステム全体の設定です。ユーザ アカウントごとに IP アドレス解決を設定するには、ユーザは [User Preferences] メニューから [Event View Settings] も選択し、[Resolve IP Addresses] を有効にしてから [Save] をクリックする必要があります。DNS サーバの設定の詳細については、管理インターフェイスの構成（64-9 ページ）を参照してください。イベント ビューの設定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

ステップ 5　[DNS Cache Timeout（in minutes）] フィールドで、非アクティブのために削除されるまで DNS エントリがメモリ内にキャッシュされる時間（分単位）を入力します。

デフォルトは 300 分（5 時間）です。

ステップ 6　[Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、「システム ポリシーの適用（63-4 ページ）」を参照してください。

注意　DNS キャッシングがアプライアンスで有効になっている場合でも、[User Preferences] メニューからアクセスできる [Events] ページで設定されていなければ、ユーザごとの IP アドレス解決は有効になりません。

メール リレー ホストおよび通知アドレスの設定

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

次の処理を行う場合、メール ホストを設定する必要があります。

- イベント ベースのレポートの電子メール送信
- スケジュールされたタスクのステータス レポートの電子メール送信
- 変更調整レポートの電子メール送信
- データ切り捨て通知の電子メール送信
- ディスカバリ イベント、影響フラグ、および相関イベント アラートについての電子メールの使用

- 侵入イベント アラートについての電子メールの使用
- ヘルス イベント アラートについての電子メールの使用

アプライアンスとメール リレー ホストとの間の通信に使用する暗号化方式を選択し、メール サーバの認証資格情報を指定できます（必要な場合）。設定を行った後、指定された設定を使用してアプライアンスとメール サーバとの間の接続をテストできます。

メール リレー ホストを設定するには、次の手順を実行します。

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーの電子メールの設定を変更するには、システム ポリシーの横にある編集アイコン（  ）をクリックします。
- 新しいシステム ポリシーの一部として電子メールの設定を行うには、[Create Policy] をクリックします。

  システム ポリシーの作成（63-2 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[Save] をクリックします。

いずれの場合も、[Access List] ページが表示されます。

ステップ 3　[Email Notification] をクリックします。

[Configure Email Notification] ページが表示されます。

ステップ 4　[Mail Relay Host] フィールドで、使用するメール サーバのホスト名または IP アドレスを入力します。

注　入力したメール ホストはアプライアンスからのアクセスを許可している必要があります。

ステップ 5　[Port Number] フィールドに、電子メール サーバで使用するポート番号を入力します。ポートは通常、暗号化を使用しない場合は 25、SSLv3 を使用する場合は 465、TLS を使用する場合は 587 です。

ステップ 6　暗号化方式を選択するには、次のオプションがあります。

- Transport Layer Security を使用してアプライアンスとメール サーバとの間の通信を暗号化するには、[Encryption Method] ドロップダウン リストから [TLS] を選択します。
- セキュア ソケット レイヤを使用してアプライアンスとメール サーバとの間の通信を暗号化するには、[Encryption Method] ドロップダウン リストから [SSLv3] を選択します。
- アプライアンスとメール サーバとの間の非暗号化通信を許可するには、[Encryption Method] ドロップダウン リストから [None] を選択します。

アプライアンスとメール サーバとの間の暗号化された通信では、証明書の検証は不要であることに注意してください。

ステップ 7　アプライアンスによって送信されるメッセージの送信元の電子メール アドレスとして使用する有効な電子メール アドレスを、[From Address] フィールドに入力します。

ステップ 8　必要に応じて、メール サーバに接続する際にユーザ名とパスワードを指定するために、[Use Authentication] を選択します。[Username] フィールドにユーザ名を入力します。パスワードを [Password] フィールドに入力します。

ステップ 9　設定したメール サーバを使用してテスト メールを送信するには、[Test Mail Server Settings] をクリックします。

テストの成功または失敗を示すメッセージがボタンの横に表示されます。

ステップ 10　[Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、「システム ポリシーの適用（63-4 ページ）」を参照してください。

ネットワーク解析ポリシーの設定の構成

ライセンス： Protection

サポートされるデバイス： すべて（X-Series を除く）

ネットワーク解析ポリシーを変更する場合に、コメントの入力を要求するようシステムを設定できます。これを使用して、ユーザのポリシーの変更の理由を追跡できます。ネットワーク解析ポリシーの変更に関するコメントを有効にした場合、コメントをオプションまたは必須に設定できます。変更に関する説明が監査ログに書き込まれます。

ネットワーク解析ポリシーのすべての変更を監査ログに書き込むこともできます。監査ログの詳細については、監査レコードの管理（69-1 ページ）を参照してください。

ネットワーク解析ポリシーのコメントの設定を行うには、次の手順を実行します。

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーのネットワーク解析ポリシーの設定を変更するには、システム ポリシーの横にある編集アイコン（）をクリックします。
- 新しいシステム ポリシーの一部としてネットワーク解析ポリシーの設定を行うには、[Create Policy] をクリックします。

  システム ポリシーの作成（63-2 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[Save] をクリックします。

いずれの場合も、[Access List] ページが表示されます。

ステップ 3　[Network Analysis Policy Preferences] をクリックします。

[Network Analysis Policy Preferences] ページが表示されます。

ステップ 4　[Comments on policy change] ドロップダウン リストには、次のオプションがあります。

- [Disabled] を選択すると、変更に関する説明を入力せずにネットワーク解析ポリシーを変更できます。
- [Optional] を選択すると、ネットワーク解析ポリシーに対する変更を保存するときに [Description of Changes] ウィンドウが表示されます。これにより、ユーザはコメントの変更について記述することができます。
- [Required] を選択すると、ネットワーク解析ポリシーに対する変更を保存するときに [Description of Changes] ウィンドウが表示されます。この場合、ユーザは変更を保存する前にコメントの変更について記述する必要があります。

ステップ 5　必要に応じて、ネットワーク解析ポリシーのすべての変更を監査ログに書き込むには、[Write changes in Network Analysis Policy to audit log] を選択します。

ステップ 6　[Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、「システム ポリシーの適用（63-4 ページ）」を参照してください。

侵入ポリシー設定の構成

ライセンス： Protection

サポートされるデバイス： すべて（X-Series を除く）

侵入ポリシーを変更する場合に、コメントの入力を要求するようシステムを設定できます。これを使用して、ユーザのポリシーの変更の理由を追跡できます。侵入ポリシーの変更に関するコメントを有効にした場合、コメントをオプションまたは必須に設定できます。変更に関する説明が監査ログに書き込まれます。

侵入ポリシーのすべての変更を監査ログに書き込むこともできます。監査ログの詳細については、監査レコードの管理（69-1 ページ）を参照してください。

侵入ポリシーのコメントの設定を行うには、次の手順を実行します。

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーの侵入ポリシーの設定を変更するには、システム ポリシーの横にある編集アイコン（  ）をクリックします。
- 新しいシステム ポリシーの一部として侵入ポリシーの設定を行うには、[Create Policy] をクリックします。

  システム ポリシーの作成（63-2 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[Save] をクリックします。

いずれの場合も、[Access List] ページが表示されます。

ステップ 3　[Intrusion Policy Preferences] をクリックします。

[Intrusion Policy Preferences] ページが表示されます。

ステップ 4　[Comments on policy change] ドロップダウン リストには、次のオプションがあります。

- [Disabled] を選択すると、変更に関する説明を入力せずに侵入ポリシーを変更できます。
- [Optional] を選択すると、侵入ポリシーに対する変更を保存するときに [Description of Changes] ウィンドウが表示されます。これにより、ユーザはコメントの変更について記述することができます。
- [Required] を選択すると、侵入ポリシーに対する変更を保存するときに [Description of Changes] ウィンドウが表示されます。この場合、ユーザは変更を保存する前にコメントの変更について記述する必要があります。

ステップ 5　必要に応じて、侵入ポリシーのすべての変更を監査ログに書き込むには、[Write changes in Intrusion Policy to audit log] を選択します。

ステップ 6　[Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、「システム ポリシーの適用（63-4 ページ）」を参照してください。

別の言語の指定

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

[Language] ページを使用して、Web インターフェイス用に異なる言語を指定できます。

注意　ここで選択した言語は、アプライアンスにログインしたすべてのユーザの Web インターフェイスに使用されます。

ユーザ インターフェイスに異なる言語を選択する方法：

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーの言語の設定を変更するには、システム ポリシーの横にある編集アイコン（  ）をクリックします。
- 新しいシステム ポリシーの一部として言語の設定を行うには、[Create Policy] をクリックします。

  システム ポリシーの作成（63-2 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[Save] をクリックします。

いずれの場合も、[Access List] ページが表示されます。

ステップ 3　[Language] をクリックします。

[Language] ページが表示されます。

ステップ 4　使用する言語を選択します。

ステップ 5　[Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、「システム ポリシーの適用（63-4 ページ）」を参照してください。

カスタム ログイン バナーの追加

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

SSH を使用してアプライアンスにログインしたときに、Web インターフェイスのログイン ページに表示されるカスタム ログイン バナーを作成できます。バナーには、小なり記号（<）および大なり記号（>）以外の出力可能な文字を含めることができます。

カスタム バナーを追加するには、次の手順に従ってください。

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーのログイン バナーを変更するには、システム ポリシーの横にある編集アイコン（）をクリックします。
- 新しいシステム ポリシーの一部としてログイン バナーの設定を行うには、[Create Policy] をクリックします。

  システム ポリシーの作成（63-2 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[Save] をクリックします。

いずれの場合も、[Access List] ページが表示されます。

ステップ 3　[Login Banner] をクリックします。

[Login Banner] ページが表示されます。

ステップ 4　[Custom Login Banner] フィールドに、このシステム ポリシーで使用するログイン バナーを入力します。

ステップ 5　[Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、「システム ポリシーの適用（63-4 ページ）」を参照してください。

SNMP ポーリングの設定

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

システム ポリシーを使用してアプライアンスの Simple Network Management Protocol（SNMP）ポーリングを有効にできます。SNMP 機能では、SNMP プロトコルのバージョン 1、2、および 3 の使用がサポートされます。

この機能を使用して、次のものにアクセスできます。

- アプライアンスの標準 Management Information Base（MIB）。これには、連絡先、管理、場所、サービス情報、IP アドレッシングやルーティングの情報、およびトランスミッション プロトコルの使用状況の統計などのシステムの詳細が含まれます。

- 管理対象デバイスの追加の MIB。これには、物理インターフェイス、論理インターフェイス、仮想インターフェイス、ARP、NDP、仮想ブリッジ、および仮想ルータを通して渡されるトラフィックの統計が含まれます。

システム ポリシー SNMP 機能を有効にすると、アプライアンスで SNMP トラップを送信できなくなり、MIB の情報はネットワーク管理システムによるポーリングでのみ使用可能になることに注意してください。

注　アプライアンスをポーリングするには、使用する任意のコンピュータで SNMP アクセスを追加する必要があります。詳細については、アプライアンスのアクセス リストの設定（63-9 ページ）を参照してください。SNMP MIB にはアプライアンスの攻撃に使用される可能性のある情報も含まれることに注意してください。Ciscoでは、SNMP アクセスのアクセス リストを MIB のポーリングに使用される特定のホストに制限することを推奨しています。Ciscoでは、SNMPv3 を使用し、ネットワーク管理アクセスには強力なパスワードを使用することも推奨しています。

SNMP ポーリングを設定するには、次の手順を実行します。

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーの SNMP ポーリングの設定を変更するには、システム ポリシーの横にある編集アイコン（ ）をクリックします。
- 新しいシステム ポリシーの一部として SNMP ポーリングの設定を行うには、[Create Policy] をクリックします。

  システム ポリシーの作成（63-2 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[Create] をクリックします。

いずれの場合も、[Access List] ページが表示されます。

ステップ 3　アプライアンスをポーリングするために使用するコンピュータごとに SNMP アクセスをまだ追加していない場合は、ここで追加してください。詳細については、アプライアンスのアクセス リストの設定（63-9 ページ）を参照してください。

ステップ 4　[SNMP] をクリックします。

[SNMP] ページが表示されます。

ステップ 5　[SNMP Version] ドロップダウン リストから、使用する SNMP バージョンを選択します。

ドロップダウン リストに選択したバージョンが表示されます。

ステップ 6　次の選択肢があります。

- [Version 1] または [Version 2] を選択した場合、[Community String] フィールドに SNMP コミュニティ名を入力します。15 に進みます。
- [Version 3] を選択した場合、[Add User] をクリックするとユーザ定義ページが表示されます。

ステップ 7　[Username] フィールドにユーザ名を入力します。

ステップ 8　[Authentication Protocol] ドロップダウン リストから、認証に使用するプロトコルを選択します。

ステップ 9　[Authentication Password] フィールドに SNMP サーバの認証に必要なパスワードを入力します。

ステップ 10　[Authentication Password] フィールドのすぐ下にある [Verify Password] フィールドに認証パスワードを再入力します。

ステップ 11　使用するプライバシー プロトコルを [Privacy Protocol] リストから選択するか、プライバシー プロトコルを使用しない場合は [None] を選択します。

ステップ 12　[Privacy Password] フィールドに SNMP サーバで必要な SNMP プライバシー キーを入力します。

ステップ 13　[Privacy Password] フィールドのすぐ下にある [Verify Password] フィールドにプライバシー パスワードを再入力します。

ステップ 14　[Add] をクリックします。

ユーザが追加されます。手順 6 から 13 までを繰り返して、さらにユーザを追加することができます。ユーザを削除するには、削除アイコン（ ）をクリックします。

ステップ 15　[Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、「システム ポリシーの適用（63-4 ページ）」を参照してください。

STIG コンプライアンスの有効化

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

米国連邦政府内の組織は、Security Technical Implementation Guides（STIG）に示されている一連のセキュリティ チェックリストに準拠しなければならない場合があります。STIG コンプライアンス オプションは、米国国防総省によって定められた特定の要件に準拠することを目的とした設定を有効にします。

展開内の任意のアプライアンスで STIG コンプライアンスを有効にする場合は、それをすべてのアプライアンスで有効にする必要があります。非準拠の管理対象デバイスを STIG 準拠の Defense Centerに登録したり、STIG 準拠デバイスを非準拠のDefense Centerに登録したりすることはできません。

STIG コンプライアンスを有効にした場合、適用可能なすべての STIG に対する厳格なコンプライアンスは保証されません。製品のこのバージョンでこのモードを使用する場合、FireSIGHT システム STIG コンプライアンスの詳細については、サポートに問い合わせて、バージョン 5.4.1 用の FireSIGHT システム STIG リリース ノートのコピーを入手してください。

STIG コンプライアンスを有効にすると、ローカル シェル アクセス アカウントのパスワードの複雑さや維持に関するルールが変わります。これらの設定の詳細については、バージョン 5.4.1 用の FireSIGHT システム STIG リリース ノートを参照してください。さらに、STIG コンプライアンス モードでは、`ssh` のリモート ストレージを使用できません。

STIG コンプライアンスが有効なシステム ポリシーを適用すると、アプライアンスは強制的にリブートされることに注意してください。STIG が有効なシステム ポリシーをすでに STIG が有効になっているアプライアンスに適用した場合、アプライアンスはリブートしません。STIG が無効なシステム ポリシーを STIG が有効になっているアプライアンスに適用した場合、STIG は引き続き有効であり、アプライアンスはリブートしません。

バージョン 5.2.0 よりも前のバージョンからアップグレードしたアプライアンスの場合、コンプライアンスを有効にしたままポリシーを適用してもアプライアンス証明書が再生成されるため、すでに登録されている管理対象デバイスまたはピアを再登録する必要があります。

注意　サポートからの支援なしでこの設定を無効にすることはできません。また、この設定は、システムのパフォーマンスに大きく影響する可能性があります。Ciscoでは、米国国防総省のセキュリティ要件に準拠する以外の目的で、STIG コンプライアンスを有効化することを推奨しません。

STIG コンプライアンスを有効にするには、次の手順を実行します。

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーの時間の設定を変更するには、システム ポリシーの横にある編集アイコン（）をクリックします。
- 新しいシステム ポリシーの一部として時間の設定を行うには、[Create Policy] をクリックします。

  システム ポリシーの作成（63-2 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[Save] をクリックします。

いずれの場合も、[Access List] ページが表示されます。

ステップ 3　[STIG Compliance] をクリックします。

[STIG Compliance] ページが表示されます。

ステップ 4　STIG コンプライアンスをアプライアンスで*永続的に*有効にする場合は、[Enable STIG Compliance] を選択します。

注意　STIG コンプライアンスが有効なポリシーを適用した後に、STIG コンプライアンスをアプライアンスで無効にすることはできません。コンプライアンスを無効にする必要がある場合は、サポートに連絡してください。

ステップ 5　[Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、「システム ポリシーの適用（63-4 ページ）」を参照してください。

アプライアンスに対して STIG コンプライアンスを有効にするシステム ポリシーを適用した場合、アプライアンスがリブートすることに注意してください。STIG が有効なシステム ポリシーをすでに STIG が有効になっているアプライアンスに適用した場合は、アプライアンスはリブートしないことに注意してください。

また、デバイスがバージョン 5.2.0 よりも前のバージョンからアップグレードされた場合、STIG コンプライアンスを有効にした後でデバイスを再登録する必要があります。

時刻の同期

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

[Time Synchronization] ページを使用して、アプライアンスで時刻の同期を管理できます。時刻を同期する場合、以下の方法を選択できます。

- 手動
- 1 つまたは複数の NTP サーバを使用（そのうちの 1 つはDefense Centerに指定できる）

時刻の設定は、システム ポリシーの一部です。新しいシステム ポリシーを作成するか、既存のポリシーを編集することによって、時刻の設定を指定できます。いずれの場合も、システム ポリシーを適用するまで時刻の設定は使用されません。

アプライアンスの大半のページでは、時刻の設定は [Time Zone] ページ（デフォルトでは米国/ニューヨーク）で設定したタイム ゾーンを使用してローカル時刻で表示されますが、アプライアンス自体には UTC 時間を使用して保存されることに注意してください。さらに、現在の時刻は [Time Synchronization] ページの上部に UTC で表示されます（ローカル時刻は手動時計設定オプションで表示されます（有効になっている場合））。

Cisco NGIPS for Blue Coat X-Series の時刻設定を管理するには、コマンドライン インターフェイスまたはオペレーティング システム インターフェイスなどのネイティブ アプリケーションを使用する必要があります。Cisco NGIPS for Blue Coat X-Series とそれが管理するDefense Centerの時刻は、同じ物理アプライアンスまたは NTP サーバから同期します。詳細については、*Cisco Software for X-Series Installation Guide* を参照してください。

アプライアンスの時刻は、外部タイム サーバと同期できます。リモート NTP サーバを指定した場合、アプライアンスはそれに対するネットワーク アクセス権限を持っている必要があります。信頼できない NTP サーバを指定しないでください。NTP サーバへの接続では、構成されたプロキシ設定は使用されません。NTP サーバとしてDefense Centerを使用するには、Defense Centerからの時刻の提供（63-29 ページ）を参照してください。

Ciscoでは、仮想アプライアンスを物理 NTP サーバと同期することを推奨します。管理対象デバイス（仮想または物理）と仮想Defense Centerを同期しないでください。

注　時刻の同期後に、Defense Centerと管理対象デバイスの時刻が一致していることを確認します。そうしないと、管理対象デバイスがDefense Centerと通信する場合に意図しない結果が発生することがあります。

時刻を同期する手順は、Defense Centerか管理対象デバイスのどちらの Web インターフェイスを使用するかによって若干異なります。各手順については後で個別に説明します。

時刻を同期するには、次の手順を実行します。

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーの時間の設定を変更するには、システム ポリシーの横にある編集アイコン（  ）をクリックします。
- 新しいシステム ポリシーの一部として時間の設定を行うには、[Create Policy] をクリックします。

  システム ポリシーの作成（63-2 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[Save] をクリックします。

いずれの場合も、[Access List] ページが表示されます。

ステップ 3　[Time Synchronization] をクリックします。

[Time Synchronization] ページが表示されます。

ステップ 4　Defense Centerから管理対象デバイスに時刻を提供する場合は、[Serve time via NTP] ドロップダウン リストで [Enabled] を選択します。

ステップ 5　Defense Centerで時刻を同期する方法を指定するには、次のオプションがあります。

- 時刻を手動で設定するには、[Manually in Local Configuration] を選択します。システム ポリシーを適用した後の時刻の設定については、手動による時刻の設定（64-15 ページ）を参照してください。
- NTP を介して別のサーバから時刻を受信するには、[Via NTP from] を選択し、使用する NTP サーバの IP アドレスのコンマ区切りリストをテキスト ボックスに入力するか、DNS が有効になっている場合は、完全修飾ホストおよびドメインの名前を入力します。

注意　アプライアンスがリブートされ、ここで指定したものとは異なる NTP サーバ レコードを DHCP サーバが設定した場合、DHCP 提供の NTP サーバが代わりに使用されます。この状況を回避するには、同じ NTP サーバを設定するように DHCP サーバを設定します。

ステップ 6　任意の管理対象デバイスで時刻を同期する方法を指定するには、次のオプションがあります。

- 時刻を手動で設定するには、[Manually in Local Configuration] を選択します。システム ポリシーを適用した後の時刻の設定については、手動による時刻の設定（64-15 ページ）を参照してください。
- NTP を介してDefense Centerから時刻を受信するには、[Via NTP from Defense Center] を選択します。詳細については、「Defense Centerからの時刻の提供（63-29 ページ）」を参照してください。
- NTP を介して別のサーバから時刻を受信するには、[Via NTP from] を選択します。テキスト ボックスで、NTP サーバの IP アドレスのコンマ区切りリストを入力するか、DNS が有効になっている場合は、完全修飾ホストおよびドメインの名前を入力します。

注　管理対象デバイスを設定された NTP サーバと同期するには、数分かかる場合があります。さらに、管理対象デバイスを NTP サーバとして設定されているDefense Centerと同期する場合、Defense Center自体が NTP サーバを使用するように設定されていると、時刻を同期するのにいくらか時間がかかることがあります。これは、管理対象デバイスに時刻を提供するために、Defense Centerは設定された NTP サーバとまず同期する必要があるためです。

ステップ 7　[Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、「システム ポリシーの適用（63-4 ページ）」を参照してください。

Defense Centerからの時刻の提供

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

NTP を使用してDefense Centerをタイム サーバとして設定してから、それを使用してDefense Centerと管理対象デバイスの間で時刻を同期することができます。

NTP を使用して時刻を提供するようにDefense Centerを設定した後は、時刻を手動で設定できないことに注意してください。時刻を手動で変更する必要がある場合は、NTP を使用して時刻を提供するようDefense Centerを設定する**前に**、その変更を行う必要があります。Defense CenterをNTP サーバとして設定した**後に**、時刻を手動で変更する必要がある場合は、[Via NTP] オプションを無効にして [Save] をクリックし、時刻を手動で変更して [Save] をクリックしてから、[Via NTP] を有効にして [Save] をクリックします。

注　NTP を使用して時刻を提供するようDefense Centerを設定してから、後でそれを無効にした場合、管理対象デバイスの NTP サービスは引き続きDefense Centerと時刻を同期しようとします。同期の試行を停止するには、NTP を管理対象デバイスの Web インターフェイスから無効にする必要があります。

NTP サーバとしてDefense Centerを設定するには、次の手順を実行します。

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーの NTP サーバの設定を変更するには、システム ポリシーの横にある編集アイコン（）をクリックします。
- 新しいシステム ポリシーの一部として NTP サーバの設定を行うには、[Create Policy] をクリックします。

  システム ポリシーの作成（63-2 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[Save] をクリックします。

いずれの場合も、[Access List] ページが表示されます。

ステップ 3　[Time Synchronization] をクリックします。

[Time Synchronization] ページが表示されます。

ステップ 4　[Serve Time via NTP] ドロップダウン リストから [Enabled] を選択します。

ステップ 5　管理対象デバイスの [Set My Clock] オプションで、[Via NTP from Defense Center] を選択します。

ステップ 6　[Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーをDefense Centerと管理対象デバイスに適用するまで、変更は有効になりません。詳細については、「システム ポリシーの適用（63-4 ページ）」を参照してください。

注　Defense Centerを管理対象デバイスと同期するには、数分かかる場合があります。

ユーザ インターフェイスの設定

ライセンス： すべて

サポートされるデバイス： すべて（X-Series を除く）

FireSIGHT システムの Web インターフェイスまたはコマンド ライン インターフェイスの無人ログイン セッションは、セキュリティ上のリスクを生じさせる場合があります。非アクティブが原因でユーザのログイン セッションがタイムアウトになるまでのアイドル時間を分単位で設定できます。シェル（コマンドライン）セッションでも同様のタイムアウトを設定できます。

長期にわたり Web インターフェイスに対してセキュアにパッシブな監視を行う予定のユーザが、展開内に存在する可能性があります。ユーザ設定オプションで Web インターフェイスのセッション タイムアウトからユーザを除外することができます。（メニュー オプションへの完全な

アクセス権がある [Administrator] ロールのユーザは、侵害が生じる場合、余分のリスクを生じさせますが、セッション タイムアウトから除外することはできません）。詳細については、ユーザ ログイン設定の管理（61-51 ページ）を参照してください。

システムへのシェル アクセスを制限する必要がある場合、3 番目のオプションによってコマンドラインの expert コマンドを永続的に無効にすることができます。アプライアンスでエキスパート モードを無効にすると、設定シェル アクセスを持つユーザーでも、シェルのエキスパート モードに入ることができなくなります。ユーザがコマンドラインのエキスパート モードに入ると、ユーザはシェルに応じた任意の Linux コマンドを実行できます。エキスパート モードに入っていない場合は、コマンド ライン ユーザはコマンドライン インターフェイスが提供するコマンドだけを実行できます。コマンドライン インターフェイスは、シリーズ 2 アプライアンスではサポートされていないことに注意してください。

コマンドライン インターフェイス コマンドの詳細については、コマンドライン リファレンス（D-1 ページ）を参照してください。コマンドライン アクセス用にユーザを設定する方法の詳細については、コマンド ライン アクセスの管理（61-48 ページ）および コマンドライン リファレンス（D-1 ページ）（仮想デバイスの CLI ユーザ管理用）を参照してください。

ユーザ インターフェイスの設定を行うには、次の手順を実行します。

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーのユーザ インターフェイスの設定を変更するには、システム ポリシーの横にある編集アイコン（  ）をクリックします。
- 新しいシステム ポリシーの一部としてユーザ インターフェイスの設定を行うには、[Create Policy] をクリックします。

  システム ポリシーの作成（63-2 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[Save] をクリックします。

いずれの場合も、[Access List] ページが表示されます。

ステップ 3　[User Interface] をクリックします。

[User Interface] ページが表示されます。

ステップ 4　次の選択肢があります。

- Web インターフェイスのセッション タイムアウトを設定するには、[Browser Session Timeout（Minutes）] フィールドに数値（分数）を入力します。デフォルトの値は `60` で、最大値は `1440`（24 時間）です。

  このセッション タイムアウトからユーザを除外する方法については、ユーザ ログイン設定の管理（61-51 ページ）を参照してください。
- コマンドライン インターフェイスのセッション タイムアウトを設定するには、[Shell Timeout（Minutes）] フィールドに数値（分数）を入力します。デフォルトの値は `0` で、最大値は `1440`（24 時間）です。
- コマンドライン インターフェイスで `expert` コマンドを永続的に無効にするには、[Permanently Disable Expert Access] チェック ボックスを選択します。

注意　エキスパート モードが無効になった状態でシステム ポリシーをアプライアンスに適用した場合、Web インターフェイスまたはコマンドラインを介してエキスパート モードにアクセスする機能を復元することはできません。エキスパート モード機能を復元するには、サポートに問い合わせる必要があります。

ステップ 5　[Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーをDefense Centerと管理対象デバイスに適用するまで、変更は有効になりません。セッション タイムアウト間隔の変更は、次回のログイン セッションまでは有効になりません。

サーバの脆弱性のマッピング

ライセンス： Protection

サポートされるデバイス： すべて（X-Series を除く）

サーバのディスカバリ イベント データベースにアプリケーション ID が含まれており、トラフィックのパケット ヘッダにベンダーおよびバージョンが含まれる場合、FireSIGHT システムは、そのアドレスから送受信されるすべてのアプリケーション プロトコル トラフィックについて、脆弱性をホスト IP アドレスに自動的にマップします。

ただし、多くのサーバには、ベンダーとバージョンの情報が含まれていません。システム ポリシーにリストされているサーバの場合、システムが脆弱性をベンダーとバージョンがないサーバのサーバ トラフィックに関連付けるかどうかを設定できます。

たとえば、ホストが見出しにベンダーまたはバージョンが含まれていない SMTP トラフィックを提供するとします。システム ポリシーの [Vulnerability Mapping] ページで SMTP サーバを有効にしてから、トラフィックを検出するデバイスを管理するDefense Centerにそのポリシーを適用した場合、SMTP サーバと関連付けられたすべての脆弱性がホストのホスト プロファイルに追加されます。

ディテクタがサーバ情報を収集し、それをホスト プロファイルに追加した場合、アプリケーション プロトコル ディテクタは脆弱性のマッピングに使用されません。これは、カスタム アプリケーション プロトコル ディテクタのベンダーまたはバージョンを指定できず、システム ポリシーで脆弱性のマッピングのためにサーバを選択できないためです。

サーバの脆弱性のマッピングを設定するには、次の手順を実行します。

アクセス： Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーの脆弱性マッピングの設定を変更するには、システム ポリシーの横にある編集アイコン（ ）をクリックします。
- 新しいシステム ポリシーの一部として脆弱性マッピングの設定を行うには、[Create Policy] をクリックします。

  システム ポリシーの作成（63-2 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[Save] をクリックします。

いずれの場合も、[Access List] ページが表示されます。

ステップ 3　[Vulnerability Mapping] をクリックします。

[Vulnerability Mapping] ページが表示されます。

ステップ 4　次の選択肢があります。

- ベンダーまたはバージョンの情報が含まれていないアプリケーション プロトコル トラフィックを受信するホストに、サーバの脆弱性がマップされないようにするには、そのサーバのチェック ボックスをオフにします。
- ベンダーまたはバージョンの情報が含まれていないアプリケーション プロトコル トラフィックを受信するホストに、サーバの脆弱性がマップされるようにするには、そのサーバのチェック ボックスをオンにします。

ヒント　[Enabled] の横にあるチェック ボックスを使用して、一度にすべてのチェック ボックスをオンまたはオフにすることができます。

ステップ 5　[Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーをDefense Centerと管理対象デバイスに適用するまで、変更は有効になりません。詳細については、「システム ポリシーの適用（63-4 ページ）」を参照してください。

アプライアンス設定の構成

FireSIGHT システム アプライアンスの *ローカル構成*（[System] > [Local] > [Configuration]）は、単一のアプライアンスに特有なものと想定される設定グループです。ローカル構成は、導入全体でほぼ同じになると想定されるアプライアンス設定を制御するシステム ポリシー（システム ポリシーの管理（63-1 ページ））とは対照的です。

次の表は、アプライアンスのローカル構成をまとめたものです。

表 64-1　　ローカル構成のオプション

オプション	説明	詳細情報の参照先
Information	アプライアンスに関する現在の情報が表示されます。アプライアンスの名前を変更することもできます。	アプライアンス情報の表示と変更（64-2 ページ）
HTTPS Certificate	信頼できる機関の HTTPS サーバ証明書を要求し（必要な場合）、証明書をアプライアンスにアップロードできます。	カスタム HTTPS 証明書の使用（64-3 ページ）
データベース	外部からアプライアンス データベースへの読み取り専用アクセスを有効化し、ダウンロードするクライアント ドライバを提供します。	データベースへのアクセスの有効化（64-7 ページ）
管理インターフェイス	インストールの一部として最初に設定されたアプライアンスの IP アドレス、ホスト名、プロキシ設定などのオプションを変更できます。アプライアンスの管理インターフェイスの設定を表示および変更することもできます。	管理インターフェイスの構成（64-9 ページ）
プロセス	アプライアンスのシャット ダウンやリブート、および FireSIGHT システムに関連するプロセスの再起動を実行できます。	システムのシャット ダウンと再起動（64-14 ページ）
時刻	現在の時間が表示されます。アプライアンスの現在のシステム ポリシー内の時間同期設定が [Manually in Local Configuration] に設定されている場合は、このページを使用して時間を変更できます。	手動による時刻の設定（64-15 ページ）
Remote Storage Device	Defense Centerで、バックアップとレポート用のリモート ストレージを構成できます。	リモート ストレージの管理（64-17 ページ）
Change Reconciliation	過去 24 時間に発生したシステム変更の詳細レポートを電子メールで受信できます。	変更調整について（64-21 ページ）
コンソール コンフィギュレーション	VGA またはシリアル ポート、または物理的にアプライアンスの近くにいなくても限られた監視および管理タスクなら実行できる Lights-Out 管理（LOM）を使用して、FireSIGHT システム アプライアンスへのコンソール アクセスを構成できます。	リモート コンソール アクセスの管理（64-23 ページ）

表 64-1　ローカル構成のオプション（続き）

オプション	説明	詳細情報の参照先
Cloud Services	Defense Centerで、Collective Security Intelligence クラウド から URL フィルタリング データをダウンロードしたり、未分類の URL を検索したり、検出されたファイルの診断情報をCiscoに送信したりできます。	クラウド通信の有効化（64-30 ページ）
VMware Tools	仮想Defense Centerで、VMware Tools を有効にして使用できます。	VMware ツールの有効化（64-33 ページ）

アプライアンス情報の表示と変更

ライセンス： すべて

[Information] ページには、アプライアンスに関する情報が表示されます。これには、製品名とモデル番号、オペレーティング システムとバージョン、現在のアプライアンスレベルのポリシーなどの読み取り専用情報が含まれます。このページには、アプライアンスの名前を変更するオプションも用意されています。

次の表で、各フィールドについて説明します。

表 64-2　アプライアンスの情報

フィールド	説明
名前	アプライアンスに割り当てられた名前。この名前は FireSIGHT システムのコンテキスト内でのみ使用されることに注意してください。ホスト名をアプライアンスの名前として使用できますが、このフィールドに別の名前を入力しても、ホスト名は変更されません。
製品モデル	アプライアンスのモデル名。
Software Version	現在インストールされているソフトウェアのバージョン。
Serial Number	アプライアンスのシャーシのシリアル番号。
Store Events Only on Defense Center	管理対象デバイスでこのチェック ボックスをオンにすると、イベント データはDefense Centerには格納されますが、その管理対象デバイスに格納されなくなります。このチェック ボックスをオフにすると、両方のアプライアンスにイベント データが格納されます。
Prohibit Packet Transfer to the Defense Center	管理対象デバイスでこのチェック ボックスをオンにすると、その管理対象デバイスはイベントのパケット データを送信しなくなります。このチェック ボックスをオフにすると、イベントでパケット データがDefense Centerに格納されます。
オペレーティング システム	アプライアンス上で現在実行されているオペレーティング システム。
オペレーティング システムのバージョン	アプライアンス上で現在実行されているオペレーティング システムのバージョン。
IPv4 Address	アプライアンスのデフォルトの管理インターフェイス（`eth0`）の IPv4 アドレス。アプライアンスで IPv4 の管理が無効になっている場合は、このフィールドにそのことが示されます。

表 64-2　アプライアンスの情報（続き）

フィールド	説明
IPv6 Address	アプライアンスのデフォルトの管理インターフェイス（eth0）の IPv6 アドレス。アプライアンスで IPv6 の管理が無効になっている場合は、このフィールドにそのことが示されます。
Current Policies	現在適用されているアプライアンスレベルのポリシー。ポリシーが最後に適用された後で更新されていると、ポリシーの名前がイタリック体で表示されます。
モデル番号	アプライアンスのモデル番号。この番号は、トラブルシューティングで重要になる場合があります。

アプライアンスの情報を変更する方法：

アクセス：Admin

ステップ 1　[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 2　アプライアンス名を変更するには、[Name] フィールドに新しい名前を入力します。

名前は、英数字である**必要があり**、数字だけで構成することはできません。

ステップ 3　変更を保存するには、[Save] をクリックします。

ページが更新され、変更が保存されます。

カスタム HTTPS 証明書の使用

ライセンス：すべて

Cisco Defense Center、および Web ベースのユーザ インターフェイスをサポートしている管理対象デバイスには、デフォルトの SSL（Secure Socket Layer）証明書が含まれています。この証明書を使用して、Web ブラウザとアプライアンス間に暗号化した通信チャネルを確立できます。ただし、アプライアンスのデフォルト証明書は世界的に知られている認証局（CA）に信頼されている CA によって生成されていないため、世界的に知られている CA または内部的に信頼できる CA によって署名されたカスタム証明書に置き換えることができます。

証明書は、アプライアンスのローカル構成で管理できます。詳細については、次の説明を参照してください。

- 現在の HTTPS サーバ証明書の表示（64-4 ページ）
- サーバ証明書要求の生成（64-4 ページ）
- サーバ証明書のアップロード（64-5 ページ）
- ユーザ証明書の要求（64-6 ページ）

現在の HTTPS サーバ証明書の表示

ライセンス：すべて

アプライアンスに現在適用されているサーバ証明書の詳細を表示できます。証明書には次の情報が含まれています。

表 64-3　HTTPS サーバ証明書の情報

フィールド	説明
Subject	証明書がインストールされているアプライアンスの commonName、countryName、organizationName、および organizationalUnitName を示します。
発行者	証明書を発行したアプライアンスの commonName、countryName、organizationName、および organizationalUnitName を示します。
Validity	証明書の有効期間を示します。
Version	証明書のバージョンを示します。
Serial Number	証明書のシリアル番号を示します。
Signature Algorithm	証明書の署名に使用されるアルゴリズムを示します。

証明書の詳細を表示する方法：

アクセス：Admin

ステップ 1　[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 2　[HTTPS Certificate] をクリックします。

[HTTPS Certificate] ページが表示され、アプライアンスの現在の証明書の詳細が示されます。

サーバ証明書要求の生成

ライセンス：すべて

アプライアンスの情報と指定した ID 情報に基づいて、証明書要求を生成できます。生成された要求を認証局に送信して、サーバ証明書を要求できます。内部認証局（CA）がインストールされ、ブラウザによって信頼されている場合は、生成された要求を使用して証明書に自己署名することもできます。生成されるキーは、Base 64 符号化（PEM）形式です。

ローカル構成の [HTTPS Certificate] ページで証明書要求を生成する場合は、1 つのサーバの証明書しか生成できないことに注意してください。[Common Name] フィールドに、サーバの完全修飾ドメイン名を、証明書に表示されるとおりに正確に入力する必要があります。一般名と DNS ホスト名が一致しない場合は、アプライアンスに接続するときに警告が表示されます。同様に、世界的に知られている CA または内部的に信頼できる CA によって署名されていない証明書をインストールした場合は、アプライアンスに接続するときにセキュリティ警告が表示されます。

証明書要求を生成する方法:

アクセス: Admin

ステップ 1　[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 2　[HTTPS Certificate] をクリックします。

[HTTPS Certificate] ページが表示されます。

ステップ 3　[Generate New CSR] をクリックします。

[Generate Certificate Signing Request] ポップアップ ウィンドウが表示されます。

ステップ 4　[Country Name (two-letter code)] フィールドに、国を表す 2 文字の国コードを入力します。

ステップ 5　[State or Province] フィールドに、都道府県の名前を入力します。

ステップ 6　[Locality or City] フィールドに、市区町村の名前を入力します。

ステップ 7　[Organization] フィールドに、組織の名前を入力します。

ステップ 8　[Organizational Unit (Department)] フィールドに、組織単位（部門）の名前を入力します。

ステップ 9　[Common Name] フィールドに、証明書の要求先となるサーバの完全修飾ドメイン名を、証明書に表示されるとおりに正確に入力します。

ステップ 10　[Generate] をクリックします。

[Certificate Signing Request] ポップアップ ウィンドウが表示されます。

ステップ 11　テキスト エディタを開きます。

ステップ 12　証明書要求のテキスト ブロック全体（`BEGIN CERTIFICATE REQUEST` 行と `END CERTIFICATE REQUEST` 行を含む）をコピーして、空のテキスト ファイルに貼り付けます。

ステップ 13　このファイルを *servername*`.csr` として保存します。*servername* は証明書を使用するサーバの名前です。

ステップ 14　この CSR ファイルを証明書の要求先となる認証局にアップロードするか、またはこの CSR を使用して自己署名証明書を作成します。

サーバ証明書のアップロード

ライセンス: すべて

認証局（CA）から署名付き証明書を取得した後は、その証明書をアップロードできます。証明書を生成した署名認証局から中間 CA を信頼するように要求された場合は、証明書チェーン（証明書パスとも呼ばれる）も提供する必要があります。ユーザ証明書が必要な場合は、証明書チェーンに中間認証局が含まれる認証局によってユーザ証明書が生成されている必要があります。

証明書をアップロードする方法:

アクセス: Admin

ステップ 1　[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 2　[HTTPS Certificate] をクリックします。

[HTTPS Certificate] ページが表示されます。

ステップ 3　[Import HTTPS Certificate] をクリックします。

[Import HTTPS Certificate] ポップアップ ウィンドウが表示されます。

ステップ 4　テキスト エディタでサーバ証明書を開き、テキスト ブロック全体（BEGIN CERTIFICATE 行と END CERTIFICATE 行を含む）をコピーして、[Server Certificate] フィールドに貼り付けます。

ステップ 5　必要に応じて、秘密キー ファイルを開き、テキスト ブロック全体（BEGIN RSA PRIVATE KEY 行と END RSA PRIVATE KEY 行を含む）をコピーして、[Private Key] フィールドに貼り付けます。

ステップ 6　提供する必要がある中間証明書を開き、各証明書のテキスト ブロック全体をコピーして、[Certificate Chain] フィールドに貼り付けます。

ステップ 7　[Save] をクリックして証明書をアップロードします。

証明書がアップロードされ、新しい証明書を反映するために [HTTPS Certificate] ページが更新されます。

ユーザ証明書の要求

ライセンス： すべて

クライアント ブラウザの証明書チェック機能を使用して FireSIGHT システムの Web サーバへのアクセスを制限できます。ユーザ証明書を有効にすると、Web サーバはユーザのブラウザ クライアントで有効なユーザの証明書が選択されていることを確認します。そのユーザ証明書は、サーバ証明書で使用されているのと同じ信頼できる認証局によって生成されている必要があります。ブラウザ内でユーザが有効でない証明書、またはデバイス上の証明書チェーンに含まれる認証局によって生成されていない証明書を選択した場合、ブラウザは Web インターフェイスをロードできません。

サーバに証明書失効リスト（CRL）をロードすることもできます。CRL には認証局によって取り消されたすべての証明書の一覧があるため、Web サーバはクライアント ブラウザの証明書が取り消されていないことを確認できます。ユーザが CRL にある失効した証明書の一覧に含まれる証明書を選択した場合、ブラウザは Web インターフェイスをロードできません。アプライアンスは識別符号化規則（DER）形式での CRL のアップロードをサポートします。1 つのサーバにロードできる CRL は 1 つだけです。

失効した証明書のリストを最新の状態に保つため、CRL を更新するスケジュール タスクを作成できます。直近に更新された CRL がインターフェイスに表示されます。

サーバ証明書で使用されるのと同じ認証局を使用していること、および証明書の中間証明書をアップロードしたことを確認してください。詳細については、サーバ証明書のアップロード（64-5 ページ）を参照してください。

注　ユーザ証明書を有効にし、その後で Web インターフェイスにアクセスするには、ブラウザに有効なユーザ証明書が存在する（またはリーダーに CAC が挿入されている）**必要があります**。

有効なユーザ証明書を要求する方法：

アクセス：Admin

ステップ 1　[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 2　[HTTPS Certificate] をクリックします。

[HTTPS Certificate] ページが表示されます。

ステップ 3　[Enable User Certificates] を選択します。プロンプトが表示されたら、ドロップダウン リストから該当する証明書を選択します。

[Enable Fetching of CRL] オプションが表示されます。

ステップ 4　必要に応じて、[Enable Fetching of CRL] を選択します。

残りの CRL 構成オプションが表示されます。

ステップ 5　既存の CRL ファイルの有効な URL を入力し、[Refresh CRL] をクリックします。

指定した URL にある最新の CRL がサーバにロードされます。

注　CRL のフェッチを有効にすると、CRL を定期的に更新するスケジュール タスクが作成されます。このタスクを編集して、更新の頻度を設定します。詳細については、証明書失効リストのダウンロードの自動化（62-4 ページ）を参照してください。

ステップ 6　サーバ証明書を作成したのと同じ認証局によって生成された有効なユーザ証明書があることを確認します。

注意　ユーザ証明書を有効にした構成を保存すると、ブラウザの証明書ストアに有効なユーザ証明書が存在しない場合に、アプライアンスへのすべての Web サーバ アクセスが無効になります。設定を保存する前に、有効な証明書がインストールされていることを確認してください。

ステップ 7　ユーザ証明書の構成を Web サーバに適用するため、[Save] をクリックします。

証明書を有効にしても、ユーザ証明書へのアクセスが有効になっていない場合は、コマンドラインでユーザ証明書の適用を無効にすることができます。詳細については、disable-http-user-cert（D-45 ページ）を参照してください。

データベースへのアクセスの有効化

ライセンス：すべて

サードパーティ製クライアントによるデータベースへの読み取り専用アクセスを許可するように、Defense Centerを設定できます。これによって、次のいずれかを使用して SQL でデータベースを照会できるようになります。

- 業界標準のレポート作成ツール（Actuate BIRT、JasperSoft iReport、Crystal Reports など）
- JDBC SSL 接続をサポートするその他のレポート作成アプリケーション（カスタム アプリケーションを含む）

- Ciscoが提供する RunQuery と呼ばれるコマンドライン型 Java アプリケーション（インタラクティブに実行することも、1 つのクエリーの結果をカンマ区切り形式で取得することもできる）

ローカル構成の [Database Settings] ページで、データベース アクセスを有効にして、選択したホストにデータベースの照会を許可するアクセス リストを作成できます。このアクセス リストは、アプライアンスのアクセスは制御しません。アプライアンスのアクセス リストの詳細については、アプライアンスのアクセス リストの設定（63-9 ページ）を参照してください。

次のツールを含むパッケージをダウンロードすることもできます。

- RunQuery（Ciscoが提供するデータベース クエリ ツール）
- InstallCert（アクセスしたいDefense Centerから SSL 証明書を取得して受け入れるために使用できるツール）
- データベースへの接続時に使用する必要がある JDBC ドライバ

外部クライアントからデータベースに接続するときは、Defense Centerの Administrator または External Database ユーザと一致するユーザ名とパスワードを入力する必要があることに注意してください。詳細については、新しいユーザ アカウントの追加（61-47 ページ）を参照してください。

データベース スキーマとサポートされるクエリーに関する情報を含め、FireSIGHT システム データベースへの外部アクセスの構成の詳細については、『*FireSIGHT System Database Access Guide*』を参照してください。

データベース アクセスを有効にする方法：

アクセス： Admin

ステップ 1　[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 2　[Database] をクリックします。

[Database Settings] ページが表示されます。

ステップ 3　[Allow External Database Access] チェック ボックスをオンにします。

[Access List] フィールドが表示されます。詳細については、ステップ 6 を参照してください。

ステップ 4　サードパーティ製アプリケーションの要件に応じて、[Server Hostname] フィールドにDefense Centerの完全修飾ドメイン名（FQDN）、IPv4 アドレス、または IPv6 アドレスを入力します。

FQDN を入力する場合は、クライアントがDefense Centerの FQDN を解決できることを確認する必要があります。IP アドレスを入力する場合は、クライアントがその IP アドレスを使用して Defense Centerに接続できることを確認する必要があります。

ステップ 5　[Client JDBC Driver] の横にある [Download] をクリックし、ブラウザのプロンプトに従って `client.zip` パッケージをダウンロードします。

データベース アクセスを設定するためにダウンロードしたパッケージ内のツールの使用方法については、『*FireSIGHT System Database Access Guide*』を参照してください。

ステップ 6　1 つ以上の IP アドレスからのデータベース アクセスを追加するため、[Add Hosts] をクリックします。

[Access List] フィールドに [IP Address] フィールドが表示されます。

ステップ 7　[IP Address] フィールドでは、追加する IP アドレスに応じて次のいずれかを入力できます。

- 正確な IP アドレス（192.168.1.101 など）

- CIDR 表記を使用した IP アドレス ブロック（192.168.1.1/24 など）

  FireSIGHT システムでの CIDR の使用方法については、IP アドレスの表記規則（1-23 ページ）を参照してください。
- 任意の IP アドレスを示す `any`

ステップ 8　[Add] をクリックします。

IP アドレスがデータベース アクセス リストに追加されます。

ステップ 9　必要に応じてデータベース アクセス リストのエントリを削除するには、削除アイコン（ ）をクリックします。

ステップ 10　[Save] をクリックします。

データベース アクセス設定が保存されます。

ヒント　最後に保存されたデータベース設定に戻すには、[Refresh] をクリックします。

管理インターフェイスの構成

ライセンス： すべて

アプライアンスを最初に設定するときは、内部の保護された管理ネットワーク上で通信できるようにアプライアンスのネットワーク設定を構成します。アプライアンスを最初に設定したときに作成したネットワーク設定を変更して、プロキシなどの追加のネットワーク設定を構成できます。シリーズ 3 アプライアンスおよび仮想Defense Centerでは、パフォーマンスを向上させるために、トラフィック チャネルを有効にして追加の管理インターフェイスを設定できます。また、異なるネットワーク上のDefense Centerとデバイス間のトラフィックを管理および分離するためのルートを作成できます。シリーズ 3 デバイスでは、デバイスの LCD パネル アクセスを有効または無効にすることもできます。これらの設定を変更したり、追加のネットワーク設定（プロキシなど）を構成したりするには、[Management Interfaces] ページ（[System] > [Local] > [Configuration] を選択して [Management Interfaces] をクリック）を使用します。

注　仮想デバイスのネットワークおよびプロキシ設定を変更する場合と、Cisco NGIPS for Blue Coat X-Series のネットワーク設定を変更する場合は、コマンドライン ツールを使用する必要があります。Cisco NGIPS for Blue Coat X-Series はプロキシをサポート**しない**ことに注意してください。詳細については、『*FireSIGHT System Virtual Installation Guide*』および『*Cisco NGIPS for Blue Coat X-Series Installation and Configuration Guide*』を参照してください。

構成のオプションと手順については、次の節を参照してください。

- 管理インターフェイスのオプションについて（64-10 ページ）
- 管理インターフェイスの編集（64-13 ページ）

管理インターフェイスのオプションについて

設定を変更することで、パフォーマンスを向上させたり、さまざまな機能を有効にしたり、導入内のネットワーク構成を変更したりできます。シリーズ 3 アプライアンスでは、トラフィック チャネルを設定したり、追加の管理インターフェイスを有効にしたり、異なるネットワーク上のデバイスからのトラフィックを分離するためのルートを作成することができます。詳細については、管理インターフェイスについて（4-4 ページ）を参照してください。

インターフェイス

FireSIGHT システムは、IPv4 と IPv6 の両方の管理環境に対応するデュアル スタック実装を提供します。一方または両方のプロトコルを選択できます。使用しないプロトコルは（あれば）無効にしてください。

管理プロトコルごとに、デフォルト管理インターフェイス（`eth0`）の IP アドレス、ネットマスクまたはプレフィクス長、およびデフォルト ゲートウェイを指定する必要があります。これらを手動で設定することも、ローカル DHCP サーバまたは IPv6 ルータからこれらを取得するようにアプライアンスを構成することもできます。ただし、有効にする追加の管理インターフェイス（`eth1` など）はそれぞれ手動で設定する必要があります。

管理インターフェイスに対して、次のオプションを構成できます。

- [Enabled]：管理インターフェイスを有効にします。別の管理インターフェイスを有効にして保存するまでは、デフォルトの管理インターフェイスを無効にしないでください。
- [Channels]：インターフェイス上の [Management Traffic] チャネルと [Event Traffic] チャネルを有効にします。

  トラフィック チャネル（管理トラフィック、イベント トラフィック、またはその両方）を有効にして、各管理インターフェイスの通信チャネル内に異なる接続を作成できます。また、複数の管理インターフェイスにまたがってトラフィック チャネルを分割し、両方のインターフェイスのスループットを統合してパフォーマンスをさらに向上させることもできます。詳細については、管理インターフェイスについて（4-4 ページ）を参照してください。
- [Mode]：デフォルトの自動ネゴシエーションを変更したり、リンク モードを指定したりできます。ギガビット インターフェイスでは、[Auto Negotiate] の値を変更しても無視されることに注意してください。

  Defense Centerに 8000 シリーズ の管理対象デバイスを登録するときは、接続の両側で自動ネゴシエーションするか、または両側を同じ固定速度に設定して安定したネットワーク リンクを確保する必要があります。8000 シリーズ の管理対象デバイスは、半二重のネットワーク リンクをサポートしません。また、接続の反対側の速度構成やデュプレックス構成の違いもサポートしません。
- [MTU]：デフォルト設定を変更できます。

（注） 他のインターフェイスとは異なり、管理インターフェイスの最大伝送単位（MTU）を変更しても、トラフィックは中断されません。

次の表に、管理インターフェイスの MTU の構成範囲を示します。

表 64-4　デバイスごとの管理インターフェイスの MTU の範囲

デバイスのモデル	MTU の範囲
シリーズ 2（3D6500 および 3D9900 を除く）	576-1518
3D6500、3D9900、仮想	576-9018
シリーズ 3 のデフォルト（eth0）	576-9234
シリーズ 3非デフォルト（eth1 など）	1518-9018

MTU の構成値から 18 バイトが自動的に削減されるため、1298 未満の値は IPv6 の最小 MTU 設定値である 1280 を満たしません。また、594 未満の値は IPv4 の最小 MTU 設定値である 576 を満たしません。たとえば、構成値 576 は自動的に 558 に削減されます。

- [MDI/MDIX]：[Auto-MDIX] のデフォルト設定を変更できます。
- [IPv4 Configuration]：[Static]、[DHCP]、または [Disabled] を設定（選択）できます。
  - IPv4 の管理 IP アドレスとネットマスクを入力するには、[Static] を選択します。
  - DHCP サーバからネットワーク設定を取得するには、[DHCP] を選択します。（eth0 のみ）
  - このプロトコルを無効にするには、[Disabled] を選択します。IPv4 と IPv6 の両方を無効にしないでください。
- [IPv6 Configuration]：[Static]、[DHCP]、[Router Assigned]、または [Disabled] を設定できます。
  - IPv4 の管理 IP アドレスとネットマスクを入力するには、[Static] を選択します。
  - DHCP サーバからネットワーク設定を取得するには、[DHCP] を選択します。（eth0 のみ）
  - ローカル IPv6 ルータからネットワーク設定を取得するには、[Router Assigned] を選択します。
  - このプロトコルを無効にするには、[Disabled] を選択します。IPv4 と IPv6 の両方を無効にしないでください。

ルート

[Edit] アイコンをクリックすると、デフォルトの管理インターフェイスへのルートを表示または編集できます。[View] アイコンをクリックすると、ルートの統計情報を表示できます。

追加のネットワークへの新しいルートを作成できます。[Add] アイコンをクリックすると、ポップアップ ウィンドウが表示され、宛先ネットワークの IP アドレス、ネットマスクまたはプレフィクス長、インターフェイスのドロップダウン（eth0 など）、およびゲートウェイを入力できます。次の例に、別のネットワークへのルートを使用する方法をいくつか示します。

- Defense Centerでは、別のネットワーク上のデバイスへのルートを作成することで、異なるネットワーク上のデバイスからのトラフィックを 1 つのDefense Centerで管理および分離できるようになります。
- デバイスでは、ルートを作成して 2 つの異なるネットワーク上のDefense Centerにデバイスを登録することで、より広範な展開においてDefense Centerのハイ アベイラビリティを設定できます。

特定の管理インターフェイスで次の設定を行うことで、ネットワークへのルートを作成できます。

- [Destination]：ルートを作成する宛先ネットワークのアドレス。
- [Netmask] または [Prefix Length]：ネットワークのネットマスク（IPv4）またはプレフィクス長（IPv6）

- [Interface]：新しいルートに割り当てるアプライアンス上の管理インターフェイス。
- [Gateway]：新しいネットワークのゲートウェイ。

共有設定

管理環境に関係なく、デバイスのホスト名とドメインと、最大 3 つの DNS サーバを指定できます。

管理ポートを変更できます。FireSIGHT システム アプライアンスは、双方向の SSL 暗号化通信チャネル（デフォルトではポート 8305）を使用して通信します。Ciscoでは、デフォルト設定のままにしておくことを**強く**推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。

注意　管理ポートを変更する場合は、導入内の相互に通信する必要があるすべてのアプライアンスの管理ポートを変更する必要があります。

LCD パネル

シリーズ 3 デバイスでは、デバイス前面の LCD パネルを使用してデバイス情報を表示できます。シリーズ 3 の [Management Interfaces] ページでは、他のユーザが LCD パネルを使用してネットワーク設定を変更できるように設定できます。

LCD パネルを使用して管理対象デバイスの IP アドレスを編集する場合、管理Defense Centerに変更が反映されることを確認してください。場合によっては、デバイス管理設定を手動で編集する必要があります。詳細については、デバイス管理設定の編集（4-57 ページ）を参照してください。

注意　LCD パネルを使用した再構成を許可すると、セキュリティ リスクが発生する可能性があります。LCD パネルを使用してネットワーク設定を構成する場合は、物理的にアクセスするだけでよく、認証は必要ありません。

プロキシ

FireSIGHT システムのすべてのアプライアンスは、ポート 443/tcp（HTTPS）および 80/tcp（HTTP）を使用してインターネットに直接接続するように構成されています。セキュリティ、インターネット アクセス、および通信ポート（E-1 ページ）を参照してください。Cisco NGIPS for Blue Coat X-Series を除き、FireSIGHT システムのアプライアンスは HTTP ダイジェストで認証できるプロキシ サーバの使用をサポートしています。

注意　NT LAN Manager（NTLM）認証を使用するプロキシは、Collective Security Intelligence クラウド と通信して情報を受信できません。クラウドベースの機能を使用する場合は、必ずプロキシに別の認証を設定してください。詳細については、クラウド通信の有効化（64-30 ページ）を参照してください。

管理インターフェイスの編集

ライセンス: すべて

[Management Interface] ページを使用して、Defense Centerのデフォルトの管理インターフェイスのデフォルト設定を変更できます。シリーズ 3 アプライアンスおよび仮想Defense Centerでは、トラフィック チャネルや追加の管理インターフェイスを有効にしたり設定することができます。ギガビット インターフェイスでは、[Auto Negotiate] の値を変更しても無視されます。

注意　アプライアンスに物理的にアクセスできない場合は、管理インターフェイスの設定を変更しないでください。Web インターフェイスへのアクセスが困難になる設定を選択する可能性があります。

管理インターフェイスを編集する方法:

アクセス: Admin

ステップ 1　[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 2　[Management Interfaces] をクリックします。

[Management Interfaces] ページが表示され、Defense Centerの各インターフェイスの現在の設定が一覧表示されます。

ステップ 3　(任意) [Interfaces] で、設定するインターフェイスの横にある [Edit] をクリックします。

デフォルトの管理インターフェイス(`eth0`)を変更したり、追加の管理インターフェイス(`eth1` など)を有効にして構成したりできます。追加の管理インターフェイスごとに、一意のスタティック IP アドレス(IPv4 または IPv6)またはホスト名を割り当てる必要があります。モード、リンク、MTU、および IP 構成の設定に加えて、伝送するトラフィック チャネルを選択できます。

ステップ 4　必要に応じて、[Routes] で、宛先ネットワークの IP アドレス、ネットマスクまたはプレフィクス長、およびゲートウェイを入力し、このネットワーク ルートに使用する管理インターフェイスを指定します。

虫眼鏡アイコンをクリックして、ルートの統計情報を表示することもできます。

ステップ 5　必要に応じて、[Shared Settings] で、管理ネットワーク プロトコルに依存しないネットワーク設定を指定します。

アプライアンスのホスト名とドメインと、最大 3 つの DNS サーバを指定できます。前の手順で [DHCP] を選択した場合は、これらの共有設定を手動で指定できないことに注意してください。

注意　Ciscoでは、デフォルト設定のままにしておくことを**強く**推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、導入内の相互に通信する必要がある**すべての**アプライアンスの管理ポートを変更する必要があります。

ステップ 6　必要に応じて、シリーズ 3 デバイスで [LCD Panel] の [Allow reconfiguration of network settings] チェック ボックスをオンにして、デバイスの LCD パネルを使用したネットワーク設定の変更を有効にします。

注意　LCD パネルを使用した再構成を許可すると、セキュリティ リスクが発生する可能性があります。LCD パネルを使用してネットワーク設定を構成する場合は、物理的にアクセスするだけでよく、認証は必要ありません。このオプションを有効にするとセキュリティ上の問題が発生する可能性があることを示す警告が Web インターフェイスに表示されます。

ステップ 7　必要に応じて、[Proxy] で、プロキシを有効にするチェック ボックスをオンにしてから、次の手順を実行します。

- [HTTP Proxy] フィールドに、プロキシ サーバの IP アドレスまたは完全修飾ドメイン名を入力します。[Port] フィールドにポートを入力します。
- 必要に応じて、[Use Proxy Authentication] を選択してから [User Name] と [Password] を入力して、認証資格情報を設定します。

ステップ 8　アプライアンスのネットワーク設定の構成が完了したら、[Save] をクリックします。

ネットワーク設定が変更されます。アプライアンスのホスト名を変更した場合は、アプライアンスをリブートした後で新しい名前が syslog に反映されます。

システムのシャット ダウンと再起動

ライセンス: すべて

アプライアンス上のプロセスを制御するために、いくつかのオプションが用意されています。次の作業を実行できます。

- アプライアンスのシャット ダウン
- アプライアンスのリブート
- アプライアンス上の通信、データベース、および HTTP サーバ プロセスの再起動（通常はトラブルシューティング時に使用される）
- Snort プロセスの再起動

注意　電源ボタンを使用してアプライアンスを停止**しないでください**。データが失われる可能性があります。アプライアンスを完全にシャット ダウンするには、[Appliance Process] ページを使用します。

アプライアンスをシャット ダウンまたは再起動する方法:

アクセス: Admin

ステップ 1　[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 2　[Process] をクリックします。

[Appliance Process] ページが表示されます。

ステップ 3　実行するコマンドを指定します。

Defense Center で:

- アプライアンスをシャット ダウンするには、[Shutdown Defense Center] の横にある [Run Command] をクリックします。
- アプライアンスをリブートするには、[Reboot Defense Center] の横にある [Run Command] をクリックします。これによってユーザがDefense Centerからログアウトすることに注意してください。
- アプライアンスを再起動するには、[Restart Defense Center Console] の横にある [Run Command] をクリックします。Defense Centerを再起動すると、ネットワーク マップ内に削除されたホストが再表示されることがあります。

注 Defense Centerをリブートすると、データベースのチェックが実行されます。このチェックが完了するまでに最大 1 時間かかることがあります。

管理対象デバイスで:

- アプライアンスをシャット ダウンするには、[Shutdown Appliance] の横にある [Run Command] をクリックします。
- アプライアンスをリブートするには、[Reboot Appliance] の横にある [Run Command] をクリックします。これによってユーザがそのデバイスからログアウトすることに注意してください。
- アプライアンスを再起動するには、[Restart Appliance Console] の横にある [Run Command] をクリックします。
- Snort プロセスを再起動するには、[Restart Snort] の横にある [Run Command] をクリックします。

注 管理対象デバイスをリブートすると、データベースのチェックが実行されます。このチェックが完了するまでに最大 1 時間かかることがあります。

手動による時刻の設定

ライセンス: すべて

現在適用されているシステム ポリシー内の時間同期設定が [Manually in Local Configuration] に設定されている場合は、ローカル構成の [Time] ページを使用して手動でアプライアンスの時間を設定できます。

Cisco NGIPS for Blue Coat X-Series の時間設定を管理するには、コマンドライン インターフェイスやオペレーティング システム インターフェイスなどのネイティブ アプリケーションを使用する必要があります。詳細については、『*Cisco NGIPS for Blue Coat X-Series Installation Guide*』を参照してください。

アプライアンスが NTP に基づいて時間を同期している場合は、時間を手動で変更できません。代わりに、[Time] ページの [NTP Status] セクションに次の情報が表示されます。

表 64-5　NTP のステータス

カラム	説明
NTP Server	構成済みの NTP サーバの IP アドレスと名前。
Status（ステータス）	NTP サーバの時間同期のステータス。次の状態が表示されます。 • [Being Used] は、アプライアンスが NTP サーバと同期していることを示します。 • [Available] は、NTP サーバが使用可能であるものの、時間がまだ同期していないことを示します。 • [Not Available] は、NTP サーバが構成に含まれているものの、NTP デーモンがその NTP サーバを使用できないことを示します。 • [Pending] は、NTP サーバが新しいか、または NTP デーモンが最近再起動されたことを示します。この値は、時間の経過とともに [Being Used]、[Available]、または [Not Available] に変わるはずです。 • [Unknown] は、NTP サーバのステータスが不明であることを示します。
Offset	アプライアンスと構成済みの NTP サーバ間の時間の差（ミリ秒）。負の値はアプライアンスの時間が NTP サーバより遅れていることを示し、正の値は進んでいることを示します。
Last Update	NTP サーバと最後に時間を同期してから経過した時間（秒数）。NTP デーモンは、いくつかの条件に基づいて自動的に同期時間を調整します。たとえば、更新時間が大きい（300 秒など）場合、それは時間が比較的安定しており、NTP デーモンが小さい更新増分値を使用する必要がないと判断したことを示します。

システム ポリシー内の時間設定の詳細については、時刻の同期（63-27 ページ）を参照してください。

時間を手動で構成する方法：

アクセス：Admin

ステップ 1　[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 2　[Time] をクリックします。

[Time] ページが表示されます。

ステップ 3　[Set Time] ドロップダウン リストから、以下を選択します。

- year
- month
- day
- hour
- minute

ステップ 4　[Apply] をクリックします。

時間が更新されます。タイム ゾーンの変更については、デフォルトのタイム ゾーンの設定（71-8 ページ）を参照してください。

リモート ストレージの管理

ライセンス： すべて

Defense Center では、バックアップとレポート用にローカルまたはリモート ストレージを使用できます。バックアップとレポートのリモート ストレージでは、ネットワーク ファイル システム（NFS）、セキュア シェル（SSH）、またはサーバ メッセージ ブロック（SMB）/Common Internet File System（CIFS）を使用できます。1 つのリモート システムにバックアップを送信し、別のリモート システムにレポートを送信することはできませんが、どちらかをリモート システムに送信し、もう一方をローカルのDefense Centerに格納することは可能です。バックアップと復元については、バックアップと復元の使用（70-1 ページ）を参照してください。

ヒント リモート ストレージを構成して選択した後は、接続データベースの制限を**増やさなかった**場合に**のみ**、ローカル ストレージに戻すことができます。

外部リモート ストレージ システムが機能しており、Defense Center からアクセスできることを確認してください。

バックアップとレポートのストレージ オプションとして、次のいずれかを選択してください。

- 外部リモート ストレージを無効にして、バックアップとレポートのストレージとしてローカルのDefense Center を使用するには、ローカルストレージの使用（64-17 ページ）を参照してください。
- バックアップとレポートのストレージ用に NFS を使用するには、リモート ストレージでの NFS の使用（64-18 ページ）を参照してください。
- バックアップとレポートのストレージ用に SSH 経由のセキュア シェル（SCP）を使用するには、リモート ストレージでの SSH の使用（64-19 ページ）を参照してください。
- バックアップとレポートのストレージ用に SMB を使用するには、リモート ストレージでの SMB の使用（64-20 ページ）を参照してください。

注 リモート バックアップおよび復元を使用して Cisco NGIPS for Blue Coat X-Series 上のデータを管理することはできません。

ローカルストレージの使用

ライセンス： すべて

ローカルのDefense Center にバックアップとレポートを格納できます。

バックアップとレポートをローカルで格納する方法：

アクセス： Admin

ステップ 1　[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 2　[Remote Storage Device] をクリックします。

[Remote Storage Device] ページが表示されます。

ステップ 3　[Storage Type] ドロップダウン リストから [Local (No Remote Storage)] を選択します。

ステップ 4　[Save] をクリックします。

選択したストレージの場所が保存されます。

ヒント　ローカル ストレージでは [Test] ボタンを使用しません。

リモート ストレージでの NFS の使用

ライセンス： すべて

ネットワーク ファイル システム（NFS）プロトコルを選択して、レポートとバックアップを格納できます。必要に応じて、NFS マウントのマニュアル ページに記載されているいずれかのマウント バイナリ オプションを使用するには、[Use Advanced Options] チェック ボックスをオンにします。

NFS を使用してバックアップとレポートを格納する方法：

アクセス： Admin

ステップ 1　[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 2　[Remote Storage Device] をクリックします。

[Remote Storage Device] ページが表示されます。

ステップ 3　[Storage Type] ドロップダウン リストから [NFS] を選択します。

ページが更新され、NFS ストレージ構成オプションが表示されます。

ステップ 4　接続情報を追加します。

- [Host] フィールドに、ストレージ システムの IPv4 アドレスまたはホスト名を入力します。
- [Directory] フィールドに、ストレージ領域へのパスを入力します。

ステップ 5　必要なコマンドライン オプションがある場合は、[Use Advanced Options] を選択します。

[Command Line Options] フィールドが表示され、マウント バイナリ オプションを入力できます。

ステップ 6　[System Usage] で、次のいずれかまたは両方を選択します。

- 指定したホストにバックアップを格納するには、[Use for Backups] を選択します。
- 指定したホストにレポートを格納するには、[Use for Reports] を選択します。
- リモート ストレージへのバックアップに関する [Disk Space Threshold] を入力します。デフォルトは 90% です。

ステップ 7　必要に応じて、[Test] をクリックします。

このテストは、Defense Centerが指定されたホストおよびディレクトリにアクセスできることを確認します。

ステップ 8　[Save] をクリックします。

リモート ストレージの構成が保存されます。

リモート ストレージでの SSH の使用

ライセンス：すべて

セキュア コピー(SCP)を使用してレポートとバックアップを格納するには、[SSH] を選択します。必要に応じて、SSH マウントのマニュアル ページに記載されているいずれかのマウント バイナリ オプションを使用するには、[Use Advanced Options] チェック ボックスをオンにします。

注意　アプライアンスの STIG 準拠を有効にすると、そのアプライアンスのリモート ストレージでは SSH を使用できません。詳細については、STIG コンプライアンスの有効化(63-26 ページ)を参照してください。

SSH を使用してバックアップとレポートを格納する方法：

アクセス：Admin

ステップ 1　[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 2　[Remote Storage Device] をクリックします。

[Remote Storage Device] ページが表示されます。

ステップ 3　[Storage Type] で [SSH] を選択します。

ページが更新され、SSH 経由の SCP ストレージ構成オプションが表示されます。

ステップ 4　接続情報を追加します。

- [Host] フィールドに、ストレージ システムの IP アドレスまたはホスト名を入力します。
- [Directory] フィールドに、ストレージ領域へのパスを入力します。
- [Username] フィールドにストレージ システムのユーザ名を入力し、[Password] フィールドにそのユーザのパスワードを入力します。ドメインを指定するには、ユーザ名の前にドメインとスラッシュ(/)を付けます。
- SSH キーを使用するには、[SSH Public Key] フィールドの内容をコピーして authorized_keys ファイルに貼り付けます。

ステップ 5　必要なコマンドライン オプションがある場合は、[Use Advanced Options] を選択します。

[Command Line Options] フィールドが表示され、マウント バイナリ オプションを入力できます。

ステップ 6　[System Usage] で、次のいずれかまたは両方を選択します。

- 指定したホストにバックアップを格納するには、[Use for Backups] を選択します。
- 指定したホストにレポートを格納するには、[Use for Reports] を選択します。

ステップ 7　必要に応じて、[Test] をクリックします。

このテストは、Defense Centerが指定されたホストおよびディレクトリにアクセスできることを確認します。

ステップ 8　[Save] をクリックします。

リモート ストレージの構成が保存されます。

リモート ストレージでの SMB の使用

ライセンス：すべて

サーバ メッセージ ブロック（SMB）プロトコルを選択して、レポートとバックアップを格納できます。必要に応じて、SMB マウントのマニュアル ページに記載されているいずれかのマウント バイナリ オプションを使用するには、[Use Advanced Options] チェック ボックスをオンにします。たとえば、SMB を使用するときは、[Command Line Options] フィールドに次の形式でセキュリティ モードを入力できます。

```
sec=mode
```

mode は、リモート ストレージで使用するセキュリティ モードです。設定オプションについては、セキュリティ モードの設定の表を参照してください。

表 64-6　セキュリティ モードの設定

モード	説明
（なし）	NULL ユーザ（名前なし）として接続します。
krb5	Kerberos バージョン 5 認証を使用します。
krb5i	Kerberos 認証とパケット署名を使用します。
ntlm	NTLM パスワード ハッシュを使用します。（デフォルト）
ntlmi	署名付きの NTLM パスワード ハッシュを使用します（/proc/fs/cifs/PacketSigningEnabled がオンになっている場合またはサーバが署名を要求する場合はデフォルト）。
ntlmv2	NTLMv2 パスワード ハッシュを使用します。
ntlmv2i	パケット署名付きの NTLMv2 パスワード ハッシュを使用します。

SMB を使用してバックアップとレポートを格納する方法：

アクセス：Admin

ステップ 1　[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 2　[Remote Storage Device] をクリックします。

[Remote Storage Device] ページが表示されます。

ステップ 3　[Storage Type] で [SMB] を選択します。

ページが更新され、SMB ストレージ構成オプションが表示されます。

ステップ 4　接続情報を追加します。

- [Host] フィールドに、ストレージ システムの IPv4 アドレスまたはホスト名を入力します。
- [Share] フィールドに、ストレージ領域の共有を入力します。システムに認識されるのは、ファイルのフル パスではなく、最上位の共有だけであることに注意してください。指定した共有ディレクトリをリモート バックアップ先として使用するには、それを Windows システムで共有する必要があります。
- 必要に応じて、[Domain] フィールドにリモート ストレージ システムのドメイン名を入力します。
- [Username] フィールドにストレージ システムのユーザ名を入力し、[Password] フィールドにそのユーザのパスワードを入力します。

ステップ 5　必要なコマンドライン オプションがある場合は、[Use Advanced Options] を選択します。

[Command Line Options] フィールドが表示され、セキュリティ モードなどのマウント バイナリ コマンドを入力できます。詳細については、「表 64-6セキュリティ モードの設定（64-20 ページ）」を参照してください。

ステップ 6　[System Usage] で、次のいずれかまたは両方を選択します。

- 指定したホストにバックアップを格納するには、[Use for Backups] を選択します。
- 指定したホストにレポートを格納するには、[Use for Reports] を選択します。

ステップ 7　必要に応じて、[Test] をクリックします。

このテストは、Defense Centerが指定されたホストおよびディレクトリにアクセスできることを確認します。

ステップ 8　[Save] をクリックします。

リモート ストレージの構成が保存されます。

変更調整について

ライセンス： すべて

ユーザが行う変更を監視し、それらが組織の推奨する標準に従っていることを確認するため、過去 24 時間に行われたシステム変更の詳細なレポートを電子メールで送信するようにシステムを構成できます。ユーザが変更をシステム構成に保存するたびに、変更のスナップショットが取得されます。変更調整レポートは、これらのスナップショットを組み合せて、最近のシステム変更の概要を提供します。

次の図は、変更調整レポートの [User] セクションの例を示しています。ここには、各構成の変更前の値と変更後の値の両方が一覧表示されています。ユーザが同じ構成に対して複数の変更を行った場合は、個々の変更の概要が最新のものから順に時系列でレポートに一覧表示されます。

6 User - SampleUser

6.1 User (2011-03-29 12:42:17 by admin from 10.4.4.4)

Field	Previous Value	Current Value
Name	SampleUser	
Active	Enabled	
Authentication	SHA512	
Password	********	
Maximum Number of Failed Logins	5	
Days Until Password Expiration	Unlimited	
Days Until Expiration Warning	0	
Check Password Strength	No	
Roles		
	Administrator	

6.2 User (2011-03-29 12:42:12 by admin from 10.4.4.4)

Field	Previous Value	Current Value
Name		SampleUser
Active		Enabled

371868

過去 24 時間に行われた変更を参照できます。しかし、それ以前の変更を確認するには、監査ログを参照する必要があります。詳細については、「監査ログを使って変更を調査する（69-8 ページ）」を参照してください。

変更調整機能を使用する方法：

アクセス：Admin

ステップ 1　[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 2　[Change Reconciliation] をクリックします。

[Change Reconciliation] ページが表示されます。

ステップ 3　[Enable] チェック ボックスをオンにします。

ステップ 4　[Time to Run] ドロップダウン リストから、システムが変更調整レポートを送信する時刻を選択します。

ステップ 5　[Email to] フィールドに、レポートの受信者の電子メール アドレスを入力します。いつでも [Resend Last Report] をクリックして、最新の変更調整レポートのコピーを受信者に再送信できます。

注　変更調整レポートを受信するには、最初にメール リレー ホストと通知アドレスを構成する必要があります。詳細については、メール リレー ホストおよび通知アドレスの設定（63-19 ページ）を参照してください。

ステップ 6　必要に応じて、変更調整レポートにポリシー変更の記録を含めるには、[Include Policy Configuration] を選択します。これには、アクセス制御、侵入、システム、ヘルス、およびネットワーク検出の各ポリシーの変更が含まれます。このオプションを選択しなかった場合は、ポリシーの変更はどれもレポートに表示されません。

注　このオプションは管理対象デバイスでは使用できません。

ステップ 7　必要に応じて、過去 24 時間に行われたすべての変更の記録を変更調整レポートに含めるには、[Show Full Change History] を選択します。このオプションを選択しなかった場合は、変更がカテゴリごとに統合された形でレポートに表示されます。

ステップ 8　[Save] をクリックします。

変更が保存されます。このレポートは、毎日、ユーザが選択した時刻に実行されます。

リモート コンソール アクセスの管理

ライセンス: すべて

サポートされるデバイス: 機能によって異なる

サポートされる防御センター: 機能によって異なる

アプライアンス上でリモート アクセスを行うため、VGA ポート（デフォルト）または物理アプライアンス上のシリアル ポートを介して Linux システムのコンソールを使用できます。組織の Cisco導入の物理レイアウトに最も適したオプションを選択してください。

Serial Over LAN（SOL）接続のデフォルトの管理インターフェイス（`eth0`）で Lights-Out 管理（LOM）を使用すると、アプライアンスの管理インターフェイスにログインすることなく、リモートで シリーズ 3 アプライアンスを監視または管理できます。アウト オブ バンド管理接続のコマンドライン インターフェイスを使用すると、シャーシのシリアル番号の表示や状態（ファン速度や温度など）の監視など、限定的なタスクを実行できます。シリーズ 2、仮想アプライアンス、ASA FirePOWER モジュール、Cisco NGIPS for Blue Coat X-Series は LOM をサポートしていません。

LOM は、アプライアンスとアプライアンスを管理するユーザの両方で有効にする必要があります。アプライアンスとユーザを有効にした後、サードパーティ製の Intelligent Platform Management Interface（IPMI）ユーティリティを使用し、アプライアンスにアクセスして管理します。

注　3D71xx、3D82xx、または 3D83xx デバイスのベースボード管理コントローラ（BMC）は、ホストの電源がオンのときにのみ 1Gbps のリンク速度でアクセスできます。デバイスの電源がオフの場合、BMC は 10/100 Mbps でのみイーサネット リンクを確立できます。したがって、デバイスにリモートから電源供給するために LOM を使用している場合は、10/100 Mbps のリンク速度だけを使用してデバイスをネットワークに接続してください。

詳細については、次のトピックを参照してください。

- アプライアンス上のリモート コンソール設定の構成（64-24 ページ）
- Lights-Out 管理ユーザ アクセスの有効化（64-25 ページ）
- Serial over LAN 接続の使用（64-26 ページ）
- Lights-Out 管理の使用（64-28 ページ）

アプライアンス上のリモート コンソール設定の構成

ライセンス： すべて

サポートされるデバイス： 機能によって異なる

サポートされる防御センター： 機能によって異なる

リモートで管理するアプライアンスの Web インターフェイスを使用して、使用するリモート コンソール アクセスのオプションを選択し構成します。

シリーズ 2、仮想アプライアンス、ASA FirePOWER モジュール、Cisco NGIPS for Blue Coat X-Series は LOM をサポートしていないので注意してください。

注　LOM/SOL を使用してシリーズ 3 デバイスに接続する前に、デバイスの管理インターフェイスに接続されたサードパーティ製のスイッチング機器のスパニング ツリー プロトコル（STP）を無効にする必要があります。

リモート コンソール設定を構成する方法：

アクセス： Admin

ステップ 1　[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 2　[Console Configuration] を選択します。

[Console Configuration] ページが表示されます。

ステップ 3　リモート コンソール アクセスのオプションを選択します。

- アプライアンスの VGA ポートを使用するには、[VGA] を選択します。これがデフォルトのオプションです。
- アプライアンスのシリアル ポートを使用する場合や、シリーズ 3 Defense Center、3D7050、8000 シリーズ デバイスで LOM/SOL を使用する場合は、[Physical Serial Port] を選択します。

  3D2100、3D2500、3D3500、および 3D4500 管理対象デバイスにはシリアル ポートはありません。
- 7000 シリーズ デバイス（3D7050 以外）で LOM/SOL を使用する場合は、[Lights-Out Management] を選択します。これらのデバイスでは、SOL と通常のシリアル接続を同時に使用することはできません。

[Physical Serial Port] または [Lights-Out Management] を選択した場合は、LOM の設定が表示されます。

注　リモート コンソールを [Physical Serial Port] から [Lights-Out Management] に変更した場合や、70xx ファミリ デバイス（3D7050 以外）で [Lights-Out Management] から [Physical Serial Port] に変更した場合は、アプライアンスを 2 回リブートしないと、期待どおりのブート プロンプトが表示されないことがあります。

ステップ 4　SOL 経由で LOM を設定するには、次の該当する設定値を入力します。

- アプライアンスの DHCP 設定（[DHCP] または [Static]）
- LOM に使用する [IP Address]

注　LOM の IP アドレスは、アプライアンスの管理インターフェイスの IP アドレスと異なっている必要があります。

- アプライアンスの [Netmask]
- アプライアンスの [Default Gateway]

ステップ 5　[Save] をクリックします。

アプライアンスのリモート コンソール構成が保存されます。Lights-Out 管理を構成した場合は、少なくとも 1 人のユーザに対してそれを有効にする必要があります。Lights-Out 管理ユーザ アクセスの有効化（64-25 ページ）を参照してください。

Lights-Out 管理ユーザ アクセスの有効化

ライセンス： すべて

サポートされるデバイス： シリーズ 3

サポートされる防御センター： シリーズ 3

Lights-Out 管理機能を使用するユーザに対して、この機能の権限を明示的に付与する必要があります。アプライアンスのローカル Web インターフェイスを使用して、アプライアンスごとに LOM と LOM ユーザを設定します。つまり、Defense Centerを使用して管理対象デバイスに LOM を設定することはできません。同様に、ユーザはアプライアンスごとに個別に管理されるため、Defense Centerで LOM 対応ユーザを有効化または作成しても、管理対象デバイスのユーザにはその機能が伝達されません。

LOM ユーザには、さらに次の制約事項があります。

- ユーザに Administrator ロールを割り当てる必要があります。
- ユーザ名に使用できるのは最大 16 個の英数字です。LOM ユーザについては、ハイフンとこれより長いユーザ名はサポートされません。
- 3D7100 ファミリ デバイスを除き、パスワードには最大 20 文字の英数字を使用できます。3D7110、3D7115、3D7120、または 3D7125 デバイスで LOM が有効になっている場合、パスワードには最大 16 文字の英数字を使用できます。20 または 16 文字よりも長いパスワードは、LOM ユーザに対してサポートされません。ユーザの LOM パスワードは、そのユーザのシステム パスワードと同じです。辞書に載っていない複雑な最大長のパスワードをアプライアンスに対して使用し、それを 3 か月ごとに変更することを推奨します。
- シリーズ 3 Defense Centerおよび 8000 シリーズ デバイスでは、最大 13 人の LOM ユーザを作成できます。7000 シリーズ デバイスでは、最大 8 人の LOM ユーザを作成できます。

あるロールを持つユーザのログイン中に LOM でそのロールを非アクティブ化してから再アクティブ化した場合や、ユーザのログイン セッション中にそのユーザまたはユーザ ロールをバックアップから復元した場合、そのユーザは IPMItool コマンドへのアクセスを回復するために Web インターフェイスにログインし直す必要があります。詳細については、事前定義ユーザ ロールの管理（61-53 ページ）を参照してください。

Lights-Out 管理ユーザ アクセスを有効化または表示する方法:

アクセス: Admin

ステップ 1　[System] > [Local] > [User Management] を選択します。

[User Management] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のユーザに LOM ユーザ アクセスを許可するには、リスト内のユーザ名の横にある編集アイコン( )をクリックします。
- 新しいユーザに LOM ユーザ アクセスを許可するには、[Create User] をクリックします。

ステップ 3　[User Configuration] で、Administrator ロールを有効にします。

[Administrator Options] が表示されます。

ステップ 4　[Allow Lights-Out Management Access] チェック ボックスをオンにします。

ステップ 5　[Save] をクリックします。

このアプライアンスの LOM アクセスがユーザに付与されます。

Serial over LAN 接続の使用

ライセンス: すべて

サポートされるデバイス: シリーズ 3

サポートされる防御センター: シリーズ 3

コンピュータ上でサードパーティ製の IPMI ユーティリティを使用して、アプライアンスへの Serial over LAN 接続を確立できます。コンピュータで Linux 系環境または Mac 環境を使用している場合は IPMItool を使用し、Windows 環境の場合は IPMIutil を使用します。

注　Ciscoでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

Linux

多くのディストリビューションで IPMItool が標準となっており、使用可能です。

Mac

Mac では、IPMItool をインストールする必要があります。最初に、Mac に Apple の XCode Apple Developer Tools がインストールされていることを確認します。これにより、コマンドライン開発用のオプション コンポーネント（新しいバージョンでは UNIX Development and System Tools、古いバージョンでは Command Line Support）がインストールされていることを確認できます。次に、MacPorts と IPMItool をインストールします。詳細については、好みの検索エンジンを使用するか、次のサイトを参照してください。

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
```

Windows

Windows では、IPMIutil をコンパイルする必要があります。コンパイラにアクセスできない場合は、IPMIutil 自体を使用してコンパイルできます。詳細については、好みの検索エンジンを使用するか、次のサイトを参照してください。

```
http://ipmiutil.sourceforge.net/
```

IPMI ユーティリティのコマンドについて

IPMI ユーティリティで使用するコマンドは、次の IPMItool の例に示したセグメントで構成されます。

```
ipmitool -I lanplus -H IP_address -U user_name command
```

値は次のとおりです。

- `ipmitool` はユーティリティを起動します
- `-I lanplus` はセッションの暗号化を有効にします
- `-H IP_address` はアクセスするアプライアンスの IP アドレスを示します
- `-U user_name` は権限を持つユーザの名前です
- `-command` は指定するコマンドの名前です

注　Ciscoでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

Windows 用の同等のコマンドは次のとおりです。

```
ipmiutil command -V 4 -J 3 -N IP_address -U user_name
```

このコマンドは、アプライアンスのコマンドラインにユーザを接続します。これによって、ユーザは物理的にそのアプライアンスの近くにいるときと同じようにログインできます。場合によっては、パスワードの入力を求められます。

Serial over LAN 接続を作成する方法:

アクセス: LOM アクセス権限がある Admin

ステップ 1　次のコマンドを入力します。

IPMItool の場合:

```
ipmitool -I lanplus -H IP_address -U user_name sol activate
```

注　Ciscoでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

IPMIutil の場合:

```
ipmiutil -J 3 -H IP_address -U username sol -a
```

アプライアンスのコマンドライン ログインが表示されます。場合によっては、パスワードの入力を求められます。

Lights-Out 管理の使用

ライセンス: すべて

サポートされるデバイス: シリーズ 3

サポートされる防御センター: シリーズ 3

Lights-Out 管理では、アプライアンスにログインすることなく、デフォルトの管理インターフェイス（eth0）から SOL 接続を介して一連の限定操作を実行できます。SOL 接続を作成するコマンドに続いて、次の表に示すいずれかのコマンドを使用します。コマンドが完了すると、接続は終了します。電源制御コマンドの中には、70xx ファミリ デバイスに対して有効でないものもあります。

注　3D71xx、3D82xx、または 3D83xx デバイスのベースボード管理コントローラ（BMC）は、ホストの電源がオンのときにのみ 1Gbps のリンク速度でアクセスできます。デバイスの電源がオフの場合、BMC は 10/100 Mbps でのみイーサネット リンクを確立できます。したがって、デバイスにリモートから電源供給するために LOM を使用している場合は、10/100 Mbps のリンク速度だけを使用してデバイスをネットワークに接続してください。

注意　まれに、コンピュータがアプライアンスの管理インターフェイスとは異なるサブネットにあり、そのアプライアンスに DHCP が構成されている場合は、シリーズ 3 アプライアンスの LOM 機能にアクセスしようとすると失敗することがあります。この場合は、アプライアンスの LOM を無効にして再び有効にするか、または同じサブネット上のコンピュータをアプライアンスとして使用して、その管理インターフェイスを ping することができます。その後、LOM を使用できるようになるはずです。

注意　Ciscoでは、Intelligent Platform Management Interface（IPMI）標準（CVE20134786）に内在する脆弱性を認識しています。アプライアンスで Lights-Out 管理（LOM）を有効にすると、この脆弱性が顕在化します。この脆弱性を軽減するために、信頼済みユーザだけがアクセス可能なセキュアな管理ネットワークにアプライアンスを展開し、辞書に載っていない複雑な最大長のパスワードをアプライアンスに対して使用し、それを 3 か月ごとに変更してください。この脆弱性のリスクを回避するには、LOM を有効にしないでください。

アプライアンスへのアクセス試行がすべて失敗した場合は、LOM を使用してリモートでアプライアンスを再起動できます。SOL 接続がアクティブなときにシステムが再起動すると、LOM セッションが切断されるか、またはタイムアウトする可能性があります。

注意　アプライアンスが別の再起動の試行に応答している間は、アプライアンスを再起動**しないでください**。リモートでアプライアンスを再起動すると、通常の方法でシステムがリブートしないため、データが失われる可能性があります。

表 64-7　Lights-Out 管理のコマンド

IPMItool	IPMIutil	説明
（非該当）	`-V 4`	IPMI セッションの管理者権限を有効にします
`-I lanplus`	`-J 3`	IPMI セッションの暗号化を有効にします
`-H`	`-N`	リモート アプライアンスの IP アドレスを指定します
`-U`	`-U`	認可された LOM アカウントのユーザ名を指定します
`sol activate`	`sol -a`	SOL セッションを開始します
`sol deactivate`	`sol -d`	SOL セッションを終了します
`chassis power cycle`	`power -c`	アプライアンスを再起動します（70xx ファミリ デバイスでは無効）
`chassis power on`	`power -u`	アプライアンスの電源を投入します
`chassis power off`	`power -d`	アプライアンスの電源を切断します（70xx ファミリ デバイスでは無効）
`sdr`	**センサー**	アプライアンスの情報（ファン速度や温度など）を表示します

たとえば、アプライアンスの情報のリストを表示する IPMItool のコマンドは、次のとおりです。

```
ipmitool -I lanplus -H IP_address -U user_name sdr
```

注　Ciscoでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

IPMIutil ユーティリティの同等のコマンドは次のとおりです。

```
ipmiutil sensor -V 4 -J 3 -N IP_address -U user_name
```

Lights-Out 管理を使用する方法：

アクセス： LOM アクセス権限がある Admin

ステップ 1　次のコマンドを入力します。

IPMItool の場合：

```
ipmitool -I lanplus -H IP_address -U user_name command
```

注　Ciscoでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

IPMIutil の場合：

```
ipmiutil -J 3 -H IP_address -U username command
```

command は、Lights-Out 管理のコマンドの表に示されたいずれかのコマンドです。

この表に示された対応するアクションが実行されます。場合によっては、パスワードの入力を求められます。

クラウド通信の有効化

ライセンス： URL FilteringまたはMalware

サポートされる防御センター： すべて（DC500 を除く）

FireSIGHT システム は、Ciscoの Collective Security Intelligence クラウド に接続してさまざまなタイプの情報を取得します。

- 組織に FireAMP サブスクリプションがある場合は、エンドポイントベースのマルウェア イベントを受信できます（FireAMP 用のクラウド接続の操作（37-27 ページ）を参照）。
- アクセス コントロール ルールに関連付けられたファイル ポリシーにより、管理対象デバイスは、ネットワーク トラフィックで送信されるファイルを検出できます。Defense Centerは、Cisco クラウドからのデータを使用して、ファイルがマルウェアに相当するかどうかを判定します。ファイル ポリシーの概要と作成（37-10 ページ）を参照してください。
- URL フィルタリングを有効にすると、Defense Centerはよくアクセスされる多くの URL のカテゴリおよびレピュテーション データを取得し、未分類の URL を検索します。その後、アクセス コントロール ルールの URL 条件をすばやく作成できます。レピュテーション ベースの URL ブロックの実行（16-11 ページ）を参照してください。

ファイルおよびマルウェアに関するクラウドベースの機能については、組織が追加のセキュリティを必要とする場合や外部接続を制限したい場合に、標準のクラウド接続の代わりに FireAMP プライベート クラウドを使用できます。すべてのファイルおよびマルウェアのクラウド検索、および FireAMP エンドポイントからのイベント データの収集とリレーは、プライベート クラウドを介して処理されます。プライベート クラウドは、Ciscoのパブリック クラウドに接続したときに、匿名化されたプロキシ接続を介してこれらの処理を行います。プライベート クラウドは、動的分析や FireAMP 以外のクラウド機能（セキュリティ インテリジェンスや URL フィルタリングなど）をサポートしていませんが、ユーザの観点からは標準のクラウド接続とほぼ同じように機能します。プライベート クラウドの構成方法の詳細については、FireAMP プライベート クラウドの操作（37-30 ページ）を参照してください。

Defense Centerのローカル構成を使用して、次のオプションを指定します。

Enable URL Filtering

カテゴリおよびレピュテーションベースの URL フィルタリングを実行するには、このオプションを有効にする必要があります。

Query Cloud for Unknown URL

監視対象ネットワーク上で誰かがローカル データ セットに存在しない URL を参照しようとしたときに、システムがクラウドを照会できるようにします。

クラウドが URL のカテゴリまたはレピュテーションを識別できない場合や、Defense Centerがクラウドに接続できない場合、その URL は、カテゴリまたはレピュテーション ベースの URL 条件を含むアクセス コントロール ルールと一致**しません**。URL にカテゴリやレピュテーションを手動で割り当てることはできません。

プライバシー上の理由などで、未分類の URL をCisco クラウドでカタログ化したくない場合は、このオプションを無効にします。

Enable Automatic Updates

システムが定期的にクラウドに接続して、アプライアンスのローカル データ セットに含まれる URL データの更新を取得できるようにします。クラウドはそのデータを通常 1 日に 1 回更新しますが、自動更新を有効にすると、Defense Centerによるチェックが 30 分ごとに強制的に行われ、常に最新の情報が保持されるようになります。

毎日の更新はたいてい小規模ですが、最終更新から 6 日以上経過すると、帯域幅によっては新しい URL フィルタリング データをダウンロードにするのに最大 20 分かかることがあります。その場合、アップデート自体の実行にも最大 30 分かかることがあります。

システムがクラウドに接続するタイミングを厳密に制御する必要がある場合は、URL フィルタリング更新の自動化（62-20 ページ）で説明しているように、自動更新を無効にして、代わりにスケジューラを使用できます。

注　Ciscoでは、自動更新を有効にするか、またはスケジューラを使用して更新をスケジュールすることを推奨しています。手動でオンデマンド更新を実行することもできますが、システムによるクラウドへの定期的な接続を自動化することで、最も関連性の高い最新の URL データを取得できます。

Share URI Information of malware events with Cisco

必要に応じて、ネットワーク トラフィックで検出されたファイルに関する情報をDefense Centerからクラウドに送信できます。この情報には、検出されたファイルに関連する URI 情報と、ファイルの SHA-256 ハッシュ値が含まれています。共有はオプト インですが、この情報をCiscoに送信すると、マルウェアを識別して追跡する今後の取り組みに役立ちます。

Use legacy port 32137 for network AMP lookups

このチェック ボックスをオンにすると、システムがネットワーク クラウド検索でポート 443/tcp の代わりにポート 32137/tcp（以前のデフォルト ポート）を使用できるようになります。アプライアンスを FireSIGHT システムの以前のバージョンから更新した場合は、デフォルトでこのチェック ボックスがオンになっています。

Licensing

カテゴリおよびレピュテーションベースの URL フィルタリングとデバイスベースのマルウェア検出を実行するには、管理対象デバイスで適切なライセンスを有効にする必要があります（FireSIGHT システムのライセンス（65-1 ページ）を参照）。

Defense Centerに URL Filtering または Malware ライセンスがない場合は、クラウド接続オプションを構成**できません**。どちらかのライセンスがあってもう一方がない場合は、[Cloud Services] ローカル構成ページに、ライセンスされているオプションのみが表示されます。ライセンスが期限切れになっているDefense Centerでは、クラウドに接続できません。

Defense Centerに URL Filtering ライセンスを追加すると、URL フィルタリングの構成オプションが表示されるのに加えて、[Enable URL Filtering] と [Enable Automatic Updates] が自動的に有効になります。必要な場合は、手動でこれらのオプションを無効にすることができます。

FireAMP サブスクリプションを使用してエンドポイントベースのマルウェア イベントを受信する場合は、ライセンスが不要であり、許可またはブロックする個々の URL や URL のグループを指定する必要もありません。詳細については、マルウェア対策とファイル制御について（37-2 ページ）および手動による URL ブロッキングの実行（16-14 ページ）を参照してください。

Internet Access and High Availability

システムは、Cisco クラウドへの接続にポート 80/HTTP および 443/HTTPS を使用し、プロキシの使用もサポートします。管理インターフェイスの構成（64-9 ページ）を参照してください。

ハイ アベイラビリティの導入では、Defense Center間ですべての URL フィルタリング構成と情報が同期されますが、URL フィルタリング データをダウンロードするのはプライマリ Defense Centerだけです。プライマリ Defense Centerに障害が発生した場合は、セカンダリ Defense Centerがインターネットに直接アクセスできることを確認し、セカンダリDefense Centerの Web インターフェイスを使用して [Active] に昇格させる必要があります。詳細については、ハイ アベイラビリティ ステータスのモニタリングおよび変更（4-16 ページ）を参照してください。

一方、ハイ アベイラビリティ ペアのDefense Centerは、ファイル ポリシーと関連する構成を共有しますが、クラウド接続やマルウェア処理は共有しません。運用の継続性を確保し、検出されたファイルのマルウェアの処理が両方のDefense Centerで同じになるようにするには、プライマリとセカンダリの両方のDefense Centerがクラウドにアクセスできる必要があります。

ヘルス モニタリング

デフォルトのヘルス ポリシーには、Defense Centerのクラウド接続の状態と安定性を追跡する次のモジュールが含まれています。

- URL フィルタリング モニタ。これは、Defense Centerがその管理対象デバイスにカテゴリとレピュテーションの更新をプッシュできない場合にも、ユーザに対して警告を表示します。
- 高度なマルウェア対策

ヒント もう一方のモジュールである FireAMP ステータス モニタは、FireAMP サブスクリプションの保有者のために、Defense CenterからCisco クラウドへの接続を追跡します。ヘルス モニタリングの詳細については、ヘルス モニタの使用（68-45 ページ）を参照してください。

次の手順では、Cisco クラウドとの通信を有効にする方法と、URL データのオンデマンド更新を実行する方法について説明します。更新がすでに進行中である場合は、オンデマンド更新を開始できません。

クラウドとの通信を有効にする方法：

アクセス： Admin

ステップ 1　[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 2　[Cloud Services] をクリックします。

[Cloud Services] ページが表示されます。URL Filtering ライセンスがある場合は、このページに URL データの最終更新時間が表示されます。

ステップ 3　上記の説明に従って、クラウド接続のオプションを構成します。

[Enable Automatic Updates] または [Query Cloud for Unknown URLs] を有効にするには、あらかじめ [Enable URL Filtering] を有効にする必要があります。

ステップ 4　[Save] をクリックします。

設定が保存されます。URL フィルタリングを有効にした場合は、URL フィルタリングが最後に有効になってから経過した時間に応じて、または URL フィルタリングを今回初めて有効にしたかどうかによって、Defense Centerがクラウドから URL フィルタリング データを取得します。

システムの URL データのオンデマンド更新を実行する方法：

アクセス：Admin

ステップ 1　[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 2　[URL Filtering] をクリックします。

[URL Filtering] ページが表示されます。

ステップ 3　[Update Now] をクリックします。

Defense Centerがクラウドに接続し、更新が使用可能な場合はその URL フィルタリング データを更新します。

VMware ツールの有効化

ライセンス：すべて

サポートされる防御センター：仮想

VMware ツールは、仮想マシンのパフォーマンスを向上させるためのユーティリティ スイートです。これらのユーティリティを使用すると、VMware 製品の便利な機能をすべて活用できます。システムは、すべての仮想アプライアンスについて以下のプラグインをサポートしています。

- guestInfo
- powerOps
- snapshot
- timeSync
- vmbackup

サポート対象のすべての ESXi バージョンで VMware Tools を有効化できます。サポートされているバージョンのリストについては、『*FireSIGHT System Virtual Installation Guide*』を参照してください。VMware ツールのすべての機能については、VMware の Web サイト（http://www.vmware.com/）を参照してください。

次の手順では、仮想Defense Center上で Web インターフェイスの構成メニューを使用して VMware Tools を有効にする方法について説明します。仮想デバイスには Web インターフェイスがないため、仮想デバイスではコマンド ライン インターフェイスを使用して VMware ツールを有効にする必要があります。『*FireSIGHT System Virtual Installation Guide*』を参照してください。

仮想Defense Centerで VMware ツールを有効にする方法：

アクセス：Admin

ステップ 1　[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 2　[VMware Tools] をクリックします。

[VMware Tools] ページが表示されます。

ステップ 3　[Enable VMware Tools] をクリックしてから、[Save] をクリックします

変更が保存されます。

FireSIGHT システムのライセンス

組織に合わせて最適な FireSIGHT システム導入環境を作成するため、さまざまな機能のライセンスを取得できます。Defense Centerを使用して、防御センター自体および防御センターが管理するデバイスを管理できます。

詳細については、以下を参照してください。

ライセンスについて

ライセンス： すべて

組織に合わせて最適な FireSIGHT システム導入環境を作成するため、さまざまな機能のライセンスを取得できます。FireSIGHT ライセンスはDefense Centerに含まれており、ホスト、アプリケーション、およびユーザのディスカバリを実行するために必要です。

追加のモデル固有ライセンスにより、管理対象デバイスは次のようなさまざまな機能を実行できます。

- 侵入検知および防御
- Security Intelligence フィルタリング
- ファイル制御および拡張マルウェア対策
- アプリケーション、ユーザ、および URL 制御
- スイッチングおよびルーティング
- デバイス クラスタリング
- ネットワーク アドレス変換（NAT）
- バーチャル プライベート ネットワーク（VPN）導入環境

FireSIGHT システムのライセンス付き機能にアクセスできなくなる状況がいくつかあります。Defense Centerからライセンスを削除できますが、これはこの防御センターにより管理されているすべてのデバイスに影響します。特定の管理対象デバイスでライセンス付き機能を無効にす

ることもできます。最後に、一部のライセンスには有効期限が設定されています。いくつかの例外がありますが、期限切れライセンスまたは削除済みライセンスに関連付けられている機能は使用できません。

FireSIGHT ライセンスのような特定のライセンスは永続的です。他のライセンスの場合は、ライセンスを有効にするためにサービス サブスクリプションを購入する必要があります。

詳細については、以下を参照してください。

- ライセンスのタイプと制約事項（65-2 ページ）
- サービス サブスクリプション（65-8 ページ）
- ハイ アベイラビリティ ペアのライセンス（65-8 ページ）
- スタック構成デバイスおよびクラスタ構成デバイスのライセンス（65-8 ページ）
- シリーズ 2 アプライアンスのライセンス付与（65-9 ページ）
- FireSIGHTホストおよびユーザ ライセンスの制限について（65-9 ページ）

ライセンスのタイプと制約事項

ライセンス： すべて

ここでは、FireSIGHT システム導入環境で使用可能なライセンスのタイプについて説明します。アプライアンスで有効にできるライセンスは、アプライアンスのモデル、バージョン、および（一部の管理対象デバイスの場合）他の有効なライセンスに応じて異なります。

仮想デバイスおよび シリーズ 3 デバイスの場合、ライセンスはモデルによって異なります。管理対象デバイスのライセンスは、ライセンスがデバイスのモデルと正確に一致しない場合は有効にできません。たとえば、3D8140 デバイスで Protection 機能を有効にする場合に 3D8250 Protection ライセンスは使用できません。組織と導入環境の拡大に伴い、管理対象デバイスを追加し、その追加ライセンスを購入できます。

シリーズ 2 デバイスには Protection 機能（Security Intelligence フィルタリングを除く）が自動的に組み込まれます。デバイスで Protectionシリーズ 2 を明示的に有効化する必要はありませんが、その他のライセンスを有効にすることもできません。

また、ユーザ制御とアプリケーション制御を実行するために、仮想デバイスまたは ASA FirePOWER デバイスで Control を有効にできますが、これらのデバイスではスイッチング、ルーティング、スタック構成、クラスタリングがサポートされないので注意してください。

次の表に、FireSIGHT システム ライセンスの要約を示します。

表 65-1　FireSIGHT システム ライセンス

FireSIGHT システムで割り当てるライセンス	購入するサービス サブスクリプション	プラットフォーム	付与される機能	要件	有効期限設定可/不可
FireSIGHT	none	Defense Center	ディスカバリ	none	no
Protection（ライセンス済み）	TA（デバイスに付属）	シリーズ 3、仮想、X-Series、ASA FirePOWER	侵入検知および防御 ファイル制御 Security Intelligence フィルタリング	none	no
Protection（自動）	なし（デバイスに付属）	シリーズ 2	侵入検知および防御 ファイル制御	none	no

表 65-1　FireSIGHT システム ライセンス（続き）

FireSIGHT システムで割り当てるライセンス	購入するサービス サブスクリプション	プラットフォーム	付与される機能	要件	有効期限設定可/不可
Control	なし（デバイスに付属）	仮想、ASA FirePOWER	ユーザおよびアプリケーション制御	Protection	no
Control	なし（デバイスに付属）	シリーズ 3	ユーザおよびアプリケーション制御 スイッチングおよびルーティング クラスタ構成	Protection	no
Malware	TAM、TAMC、または AMP	シリーズ 3、仮想、ASA FirePOWER	高度なマルウェア防御（ネットワークベースのマルウェアの検出とブロッキング）	Protection	yes
URL Filtering	TAC、TAMC、または URL	シリーズ 3、仮想、X-Series、ASA FirePOWER	カテゴリとレピュテーションに基づく URL フィルタリング	Protection	yes
VPN	なし（詳細は販売担当者までお問い合わせください）	シリーズ 3	仮想プライベート ネットワークの導入	Control	yes

ただし、DC500 Defense Center は URL Filtering または Malware のライセンスよって提供される機能をサポートしていません。

詳細については、以下を参照してください。

- FireSIGHT（65-3 ページ）
- Protection（65-4 ページ）
- Control（65-5 ページ）
- Malware（65-6 ページ）
- URL Filtering（65-6 ページ）
- VPN（65-7 ページ）

FireSIGHT

ライセンス： FireSIGHT

FireSIGHT ライセンスはDefense Centerに含まれており、このライセンスによりホスト、アプリケーション、およびユーザのディスカバリを実行できます。ディスカバリ データにより、システムは完全かつ最新のネットワーク プロファイルを作成し、脅威、エンドポイント、およびネットワーク インテリジェンスをユーザ識別情報に関連付けることができます。ディスカバリ データを使用して、トラフィック プロファイリングを実行し、ネットワーク コンプライアンスを評価し、および相関ポリシーを実装することができます。

FireSIGHT ライセンスは、Defense Centerとその管理対象デバイスで監視できる個々のホストおよびユーザの数も決定します。ユーザ制限が次の項目に*単独*で適用されることに注意してください。

- Users データベース（FireSIGHT システムで検出された各ユーザのレコードを格納）
- ユーザ制御を実行するためアクセス制御ルールで使用できるユーザ（別名「*アクセス制御ユーザ*」）の数

ライセンス制限に達した場合の結果の詳細については、FireSIGHTホストおよびユーザ ライセンスの制限について（65-9 ページ）を参照してください。

FireSIGHT のライセンスがない状態でも、基本的なシステム設定、監視、ネットワークベースのアクセス制御（ゾーン、ネットワーク、VLAN、およびポート ルールの条件）、接続のロギング、レポートを実行できます。また、FireSIGHT ライセンスがない状態でも Collective Security Intelligence クラウド からエンドポイントに基づくマルウェア イベントを受信できますが、組織に FireAMP サブスクリプションが必要です。

ヒント　このマニュアルのライセンスに関する説明では、Defense Centerに FireSIGHT ライセンスがあることを前提としています。ただし、Defense Center バージョン 4.10.x が以前稼働していた場合は、FireSIGHT ライセンスの代わりに RNA Host および RUA User ライセンス（レガシー）を使用できる場合があります。詳細については、Protection（65-4 ページ）を参照してください。

Protection

ライセンス： Protection

サポートされるデバイス： シリーズ 3、仮想、X-Series、ASA FirePOWER

Protection ライセンスでは、侵入検知および防御、ファイル制御、およびセキュリティ インテリジェンスのフィルタリングを実行できます。

- *侵入検知および防御*により、侵入とエクスプロイトを検出するためネットワーク トラフィックを分析できます。またオプションで違反パケットをドロップできます。
- *ファイル制御*により、特定のアプリケーション プロトコルを介した特定タイプのファイルを検出し、オプションでこれらのファイルのアップロード（送信）またはダウンロード（受信）をブロックできます。Malware ライセンス（Malware（65-6 ページ）を参照）では、マルウェアの性質に基づいて限られたファイル タイプを検査およびブロックすることもできます。
- *Security Intelligence フィルタリング*により、トラフィックをアクセス制御ルールによる分析対象にする前に、特定の IP アドレスをブラックリストに追加（その IP アドレスとの間のトラフィックを拒否）できます。ダイナミック フィードにより、最新の情報に基づいて接続を直ちにブラックリストに追加できます。オプションで、セキュリティ インテリジェンス フィルタリングに「監視のみ」設定を使用できます。

保護ライセンスは（制御ライセンスとともに）、管理対象デバイスの購入時に自動的に付属します。このライセンスは無期限ですが、システムの更新を有効にするには、TA サブスクリプションを購入する必要があります。

ライセンスがない状態でも Protection 関連の検査を実行するようにアクセス制御ポリシーを設定できますが、最初に Protection ライセンスをDefense Centerに追加してから、ポリシー適用対象デバイスでこのライセンスを有効にするまではポリシーを適用できません。

Protection ライセンスを Defense Centerから削除するか、または管理対象デバイスで Protection を無効にすると、Defense Centerは対象デバイスからの侵入イベントとファイル イベントを認識しなくなります。結果として、トリガー条件としてこれらのイベントを使用する相関ルールがトリガーしなくなります。また、Defense CenterはCisco提供またはサードパーティの Security Intelligence 情報を取得するためにインターネットに接続しません。Protection を再度有効にするまでは、既存のポリシーを再適用できません。

Protection ライセンスは URL Filtering、Malware、およびControl ライセンスに必要であるため、Protection ライセンスを削除または無効にすると、URL Filtering、Malware、または Control ライセンスを削除または無効にすることと同じ効果があります。

注 シリーズ 2 デバイスにはほとんどの Protection 機能が自動的に組み込まれるため、これらのデバイスの Protection ライセンスを購入または有効にする必要はありません。ただし シリーズ 2 デバイスは Security Intelligence フィルタリングを実行できません。

Control

ライセンス： Control

サポートされるデバイス： シリーズ 3、仮想、ASA FirePOWER

サポートされる防御センター： 機能によって異なる

Control ライセンスでは、アクセス制御ルールにユーザとアプリケーションの条件を追加することで、ユーザとアプリケーションの制御を実装できます。また、スイッチングおよびルーティング（DHCP リレーおよび NAT を含む）を実行するように シリーズ 3 管理対象デバイスを設定し、クラスタ管理対象デバイスを設定することができます。管理対象デバイス上で Control 有効にするには、Protection も有効にする必要があります。

注 仮想デバイスまたは ASA FirePOWER デバイスで Control ライセンスを有効にできますが、これらのデバイスではスイッチング、ルーティング、スタック構成、またはクラスタ構成がサポート**されません**。

制御ライセンスは（保護ライセンスとともに）、管理対象デバイスの購入時に自動的に付属します。このライセンスは無期限ですが、システムの更新を有効にするには、TA サブスクリプションを購入する必要があります。

Control ライセンスがない状態でアクセス制御ルールにユーザ条件とアプリケーション条件を追加できますが、ポリシーを適用するには、最初に Control ライセンスをDefense Centerに追加し、ポリシー適用対象デバイスで有効にする必要があります。

DC500 Defense Centerではアクセス制御ルールへのユーザ条件の追加がサポートされていないことに注意してください。

Control ライセンスがない場合、管理対象デバイスでのスイッチド インターフェイス、ルーテッド インターフェイス、ハイブリッド インターフェイスの作成、NAT 項目の作成、および仮想ルータの DHCP リレーの設定はできません。仮想スイッチおよびルータを作成できますが、データを取り込むスイッチド インターフェイスおよびルーテッド インターフェイスがない状態ではこれらのスイッチとルータは有用ではありません。さらに、Control を有効にしていない管理対象デバイスにスイッチングまたはルーティングを組み込むデバイス設定を適用することはできません。また、管理対象デバイス間でクラスタ構成を確立するには、デバイスが Control に対して有効になっている必要があります。

Control ライセンスをDefense Centerから削除するか、または個別のデバイスで Control を無効にしても、対象デバイスでのスイッチングとルーティングの実行しなくなったり、デバイス クラスタが破損したりは**しません**。既存の設定を編集または削除できますが、対象デバイスに変更を適用することはできません。新しいスイッチド インターフェイス、ルーテッド インターフェイス、またはハイブリッド インターフェイスを追加することも、新しい NAT 項目の追加、DHCP リレーの設定、デバイスのクラスタ構成の確立もできません。既存のアクセス制御ポリシーに、ユーザ条件またはアプリケーション条件を含むルールが含まれている場合は、それらのポリシーを再適用することができません。

URL Filtering

ライセンス： URL Filtering

サポートされるデバイス： シリーズ 3、仮想、X-Series、ASA FirePOWER

サポートされる防御センター： すべて（DC500 を除く）

URL フィルタリングにより、監視対象ホストにより要求される URL に基づいてネットワークを移動可能なトラフィックを判別するアクセス制御ルールを作成し、Defense Centerが Cisco クラウドから取得する URL に関する情報に関連付けることができます。URL Filtering を有効にするには、Protection ライセンスも有効にする必要があります。

ヒント URL Filtering ライセンスがない状態で、許可またはブロックする個別 URL または URL グループを指定できます。これにより、Web トラフィックをカスタムできめ細かく制御できますが、URL カテゴリおよびレピュテーション データをネットワーク トラフィックのフィルタリングに使用することはできません。

URL フィルタリング ライセンスは、脅威 & アプリ（TAC）または脅威 & アプリおよびマルウェア（TAMC）と組み合わせてサービス サブスクリプションとして購入できます。また、脅威 & アプリ（TA）が既に有効になっているシステムの場合は、アドオン サブスクリプションとして購入できます。

URL Filtering ライセンスがない状態でも、アクセス制御ルールにカテゴリ ベース URL 条件およびレピュテーション ベース URL 条件を追加できますが、Defense Centerは URL 情報を取得するためにクラウドに接続しません。最初に URL Filtering ライセンスをDefense Centerに追加し、ポリシー適用対象デバイスで有効にするまでは、アクセス制御ポリシーを適用できません。

Defense Centerからライセンスを削除するか、または管理対象デバイスで URL Filtering を無効にすると、URL フィルタリングにアクセスできなくなることがあります。また、URL Filtering ライセンスが期限切れになることがあります。ライセンスが期限切れになるか、ライセンスを削除または無効にすると、URL 条件が含まれているアクセス制御ルールは URL フィルタリングを直ちに停止し、Defense Centerはクラウドにアクセスできなくなります。既存のアクセス制御ポリシーに、カテゴリ ベースまたはレピュテーション ベースの URL 条件を含むルールが含まれている場合は、それらのポリシーを再適用することができません。

Malware

ライセンス： Malware

サポートされるデバイス： シリーズ 3、仮想、ASA FirePOWER

サポートされる防御センター： すべて（DC500 を除く）

Malware ライセンスでは、拡張マルウェア防御を実行できます。つまり、管理対象デバイスを使用して、ネットワーク上で送信されるファイルからマルウェアを検出してブロックできます。管理対象デバイス上で Malware 有効にするには、Protection も有効にする必要があります。

注 Malware ライセンスが有効になっている管理対象デバイスは、動的分析を設定していない場合でも、定期的に Cisco クラウドへの接続を試行します。このため、デバイスの [Interface Traffic] ダッシュボード ウィジェットには、送信済みトラフィックが表示されます。これは正常な動作です。

ファイル ポリシーの一部としてマルウェア検出を設定し、その後 1 つ以上のアクセス制御ルールを関連付けます。ファイル ポリシーは、特定のアプリケーション プロトコルを使用して特定のファイルをアップロードまたはダウンロードするユーザを検出できます。Malware ライセンス

では、限られたファイル タイプ を調べてマルウェアが存在するかどうかを確認し、特定のファイル タイプをダウンロードし、Cisco クラウドに送信し、ダイナミック分析および Spero 分析を実行してこれらのファイルにマルウェアが含まれているかを判断することができます。Malware ライセンスでは、ファイル リストに特定のファイルを追加し、そのファイル リストをファイル ポリシー内で有効にすることもできます。これにより、検出時にこれらのファイルを自動的に許可またはブロックできます。

マルウェア ライセンスは、脅威 & アプリ（TAM）または脅威 & アプリおよび URL フィルタリング（TAMC）と組み合わせてサブスクリプションとして購入できます。また、脅威 & アプリ（TA）が既に有効になっているシステムの場合は、アドオン サブスクリプションとして購入できます。

Malware ライセンスがなくてもアクセス制御ルールにマルウェア検出ファイル ポリシーを追加できますが、アクセス制御ルール エディタでこのファイル ポリシーに警告アイコン（⚠）が付きます。ファイル ポリシー内でも、マルウェア クラウド検索ルールに警告アイコンが付きます。マルウェア検出ファイル ポリシーを含むアクセス制御ポリシーを適用する前に、Malware ライセンスを追加してから、そのポリシー適用対象デバイスで有効にする**必要があります**。後でデバイス上でライセンスを無効にすると、マルウェア検出を実行するファイル ポリシーが含まれている既存のアクセス制御ポリシーをこれらのデバイスに対して再適用することはできません。

Malware ライセンスをすべて削除するか、それらがすべて期限切れになると、Defense Centerはマルウェア クラウド検索の実行と、Cisco クラウドから送信される遡及的イベントの認識を停止します。既存のアクセス制御ポリシーにマルウェア検出を実行するファイル ポリシーが含まれている場合、このアクセス制御ポリシーを再適用することはできません。Malware ライセンスの期限切れまたは削除後のごく短い時間内は、マルウェア クラウド検索ファイル ルールで検出されたファイルのキャッシュされた性質を、システムが使用できることに注意してください。この時間枠の経過後は、システムは検索を実行せず `Unavailable` という性質をこれらのファイルに割り当てます。

Malware ライセンスが必要であるのは、システムでネットワーク トラフィックのマルウェアを検出する必要がある場合だけであることに注意してください。Malware ライセンスがない状態でも、組織に FireAMP サブスクリプションがある場合は、Defense CenterはCisco クラウドからエンドポイント ベースのマルウェア イベントを受信できます。詳細については、マルウェア対策とファイル制御について（37-2 ページ）を参照してください。

VPN

ライセンス： VPN

サポートされるデバイス： シリーズ 3

VPN を使用すると、インターネットやその他のネットワークなどの公共ソースを経由してエンドポイント間にセキュア トンネルを確立できます。Cisco管理対象デバイスの仮想ルータ間にセキュア VPN トンネルを確立するように FireSIGHT システムを設定できます。VPN を有効にするには、Protection および Control ライセンスも有効にする必要があります。VPN ライセンスを購入するには、販売担当者までお問い合わせください。

VPN ライセンスがないと、管理対象デバイスで VPN 導入環境を設定できません。導入環境の作成はできますが、データを取り込むための 1 つ以上の VPN 対応スイッチド インターフェイスおよびルーテッド インターフェイスがない状態では、導入環境は有用ではありません。

VPN ライセンスをDefense Centerから削除するか、または個別のデバイスで VPN を無効にすると、対象デバイスは現在の VPN 導入環境をブレイク**しません**。既存の導入環境を編集または削除できますが、対象デバイスに変更を適用することはできません。

サービス サブスクリプション

ライセンス： すべて

サービス サブスクリプションは、所定の時間内限定で、管理対象デバイス上の特定の機能を有効にします。サービス サブスクリプションは、1 年、3 年、または 5 年単位で購入できます。サブスクリプションの期限が切れると、サブスクリプションを更新する必要があることが通知されます。サブスクリプションの期限が切れた場合、機能のタイプによっては、関連機能を使用できなくなることがあります。

管理対象デバイスを購入すると、制御および保護のライセンスが自動的に付属します。これらのライセンスは無期限ですが、システムの更新を有効にするには、TA サービス サブスクリプションを購入する必要があります。その他のサービス サブスクリプションはオプションです。

サービス サブスクリプションは、FireSIGHT システムで管理対象デバイスに割り当てるライセンスと、次のように対応しています。

表 65-2　FireSIGHT サービス サブスクリプション

購入するサブスクリプション	FireSIGHT システムで割り当てるライセンス
TA	制御 + 保護（別名「脅威 & アプリ」、システム更新に必要）
TAC	制御 + 保護 + URL フィルタリング
TAM	制御 + 保護 +マルウェア
TAMC	制御 + 保護 + URL フィルタリング + マルウェア
AMP	マルウェア（TA が既に存在する場合はアドオン）
URL	URL フィルタリング（TA が既に存在する場合はアドオン）

ハイ アベイラビリティ ペアのライセンス

ライセンス： すべて

サポートされる防御センター： DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

高可用性ペアのDefense Centerは、ライセンスを共有**しません**。ペアの各メンバに同等のライセンスを適用する必要があります。Ciscoは各Defense Centerの固有ライセンス キーに基づいてライセンスが生成するため、異なるDefense Centerで同じキーを使用することはできません。

スタック構成デバイスおよびクラスタ構成デバイスのライセンス

ライセンス： すべて

サポートされるデバイス： 機能によって異なる

個々のデバイスをスタック構成またはクラスタ構成する前に、これらの各デバイスに同等のライセンスがインストールされている必要があります。デバイスのスタック構成後に、スタック全体のライセンスを変更できます。ただし、デバイス クラスタでは有効なライセンスを変更することはできません。

スタックに含まれるデバイスの管理（4-46 ページ）で説明する要件に準拠する同一モデルの 3D8140、3D8200 ファミリ、3D8300 ファミリ、および 3D9900 デバイスをスタック構成にできます。デバイスのクラスタリング（4-31 ページ）で説明する要件に準拠する同一 シリーズ 3 モデルの 2 つのデバイスをクラスタ構成にできます。

シリーズ 2 アプライアンスのライセンス付与

ライセンス：Protection

サポートされるデバイス：シリーズ 2

DC500 を除き、シリーズ 2、および シリーズ 3Defense Centerのライセンス付与方法は同一です。DC500 は URL フィルタリングおよびネットワークベースのマルウェア検出をサポートしていないため、URL Filtering や Malware のライセンスのメリットを活用できません。

シリーズ 2 デバイスには、Protection ライセンスにより有効になる Security Intelligence 以外の機能を自動的に組み込まれています。シリーズ 2 デバイスでは Protection ライセンスを無効にできません。また、その他のライセンスを有効にできません。

詳細については、次の項を参照してください。

- サービス サブスクリプション（65-8 ページ）では、FireSIGHT システム導入環境で使用可能なライセンスのタイプについて説明します。
- 管理対象デバイスの各モデルでサポートされる機能の概要（1-6 ページ）では、シリーズ 2 アプライアンスでサポートされている機能とサポートされていない機能の要約を示します。

FireSIGHTホストおよびユーザ ライセンスの制限について

ライセンス：FireSIGHT

Defense Centerの FireSIGHT ライセンスにより、Defense Centerとその管理対象デバイスで監視できる個々のホストとユーザの数、およびユーザ制御を実行するときに使用できるユーザの数が決定します。FireSIGHT ホストおよびユーザのライセンス制限は、次の表に示すようにモデルに応じて異なります。

表 65-3　Defense Center モデル別の FireSIGHT の制限

Defense Center モデル	FireSIGHT のホストとユーザの制限
DC500	1000
DC750	2000
DC1000	20,000
DC1500	50,000
DC2000	100,000
DC3000	100,000
DC3500	300,000
DC4000	600,000
virtual	50,000

たとえば、DC500 では 1000 ホストおよび 1000 ユーザを監視できます。

以前に Defense Centerで FireSIGHT システム バージョン 4.10.x が稼働しており、ISO ファイルを使用してアプライアンスをバージョン 5.x の出荷時デフォルトに「復元」した場合、FireSIGHT ライセンスの代わりにレガシー RNA Host および RUA User ライセンスを使用できる場合があります。

詳細については、次の項を参照してください。

- FireSIGHTホスト制限について（65-10 ページ）
- FireSIGHTユーザ制限について（65-10 ページ）
- アクセス制御ユーザ制限について（65-11 ページ）
- Protection（65-4 ページ）

FireSIGHTホスト制限について

ライセンス：FireSIGHT

Defense Centerの FireSIGHT ライセンスにより、Defense Centerおよびその管理対象デバイスで監視できる個々のホストの数、およびネットワーク マップに保管できるホストの数が決定します。

システムでは、IP アドレスと MAC アドレスの両方によって識別されるホストとは別に、MAC 専用ホストがカウントされるので注意してください。1 つのホストに関連付けられているすべての IP アドレスは、まとめて 1 つのホストとしてカウントされます。

システムが（ネットワーク検出ポリシーで定義されている）監視対象ネットワークの IP アドレスを持つホストに関連するアクティビティを検出すると、そのホストがネットワーク マップに追加されます。

ホスト制限に達した後でシステムにより新しいホストが検出される場合、新しいホストがネットワーク マップに追加されるかどうかは、ネットワーク検出ポリシーの [When Host Limit Reached] 設定に基づきます。データベースへの新しいホストの追加を停止するか、または最も長い期間にわたり非アクティブなホストを置き換えるようにシステムを設定できます。

注　ネットワーク マップに新しいホストを追加できない場合でも、システムはそのホストのネットワーク トラフィックに対してアクセス 制御を実行します。ライセンス制限に達した後でも、FireSIGHT ホストの制限に達したために検出されたホストに対してアクセス制御を実行できなくなることはありませんが、ホスト プロファイル データを使用してこれらのホストの分析を実行または表示することはできません。たとえば、コンプライアンス ホワイトリストを使用してこれらのホストのネットワーク コンプライアンスを監視したり、ホスト プロファイル認定にこれらのホストを使用したりすることはできません。

ホスト、サブネット全体、またはすべてのホストをネットワーク マップから手動で削除することもできます。ただし、システムは削除されたホストに関連するアクティビティを検出すると、そのホストをネットワーク マップに再度追加します。

ネットワーク検出ポリシーで指定された最後の [Host Timeout] 期間内に、ホストからのネットワーク トラフィックが検出されない場合、ホストはネットワーク マップから削除されることにも注意してください。デフォルト設定は 10080 分（7 日）です。

ホスト ライセンスの使用状況を追跡できるようにするため、残りの設定可能なホスト ライセンスの数よりも少ない場合には、FireSIGHT Host License Limit ヘルス モジュールにより警告が出されます。

FireSIGHTユーザ制限について

ライセンス：FireSIGHT

Defense Centerの FireSIGHT ライセンスにより、監視できる個々のユーザの数が決定します。システムが新しいユーザのアクティビティを検出すると、そのユーザは Users データベースに追加されます。ユーザは次の方法で検出できます。

- ネットワーク検出ポリシーを使用して、LDAP、AIM、POP3、IMAP、Oracle、SIP (VoIP)、FTP、HTTP、MDNS、および SMTP ユーザのログインを受動的に検出するように管理対象デバイスを設定することができます。
- Active Directory 資格情報に対する認証を検出するため、Microsoft Active Directory LDAP サーバに User Agent をインストールできます。

ライセンス制限に達すると、ほとんどの場合、システムはデータベースへの新しいユーザの追加を停止します。新しいユーザを追加するには、データベースからユーザを手動で削除するか、またはデータベースからすべてのユーザを消去する必要があります。

ただしシステムは、信頼できるユーザのログインを優先します。ライセンス制限に達した後、システムが以前は検出されなかった信頼できるユーザのログインを検出した場合、システムは、最も長い期間にわたって非アクティブな信頼できないユーザを削除し、このユーザを新しい信頼できるユーザに置き換えます。

ヒント　管理対象デバイスを使用してユーザ アクティビティを検出する場合、ユーザ名が複雑になることを最小限に抑え、FireSIGHT ユーザ ライセンスを保持するため、ユーザ ロギングをプロトコルにより制限できることに注意してください。たとえば、AIM、POP3、および IMAP で検出されるユーザを監視すると、契約業者、訪問者、およびその他のゲストからのネットワーク アクセスが原因で、組織に関係のないユーザが追加されることがあります。詳細については、ユーザ ロギングの制限（45-33 ページ）を参照してください。

アクセス制御ユーザ制限について

ライセンス： Control

サポートされるデバイス： シリーズ 3、仮想、ASA FirePOWER

Defense Centerの FireSIGHT ライセンスにより、監視できる個々のユーザの数ばかりでなく、ユーザ制御を実行するためにアクセス制御ルールで使用できるユーザの数も決まります。これらのユーザは*アクセス制御ユーザ*と呼ばれます。

注　ユーザ制御を実行するには、組織で Microsoft Active Directory が使用されている**必要があります**。システムは Active Directory サーバで稼働している User Agent を使用してアクセス制御ユーザに IP アドレスを関連付けます。これにより、アクセス制御ルールがトリガー可能になります。

Defense Center と Active Directory サーバ間に接続（*ユーザ認証オブジェクト*）を設定して、アクセス制御ユーザが属すべきグループを指定します。次に、Defense Centerは定期的にサーバに対してクエリを実行し、認証オブジェクトで指定したグループのユーザのリストを取得します。これらのユーザを使用してアクセス制御を実行できます。

認証オブジェクトに指定したグループのユーザの総数が、FireSIGHT ユーザ ライセンスよりも少ないことを確認する**必要があります**。パラメータが一般的でありすぎると、Defense Centerは可能な限り多くのユーザを取得し、タスク キューで取得できなかったユーザの数を報告します。パフォーマンスとライセンスの理由から、Ciscoはアクセス制御に使用するユーザを表すグループだけを指定することを推奨します。

ライセンスの表示

ライセンス： すべて

[Licenses] ページで、Defense Centerとその管理対象デバイスのライセンスを表示します。導入環境内のアプライアンスのタイプごとに、所有しているライセンスの総数と、使用中のライセンスの割合がこのページにリストされます。

このページでは、使用中の FireSIGHT User ライセンスの数は、FireSIGHT システムにより検出されるユーザの数、つまり Users データベース内のユーザの数を表すことに注意してください。これは、アクセス制御に使用するアクセス制御ユーザの数ではありません。詳細については、FireSIGHTホストおよびユーザ ライセンスの制限について（65-9 ページ）を参照してください。

[Licenses] ページには、各ライセンスの詳細も表示されます。モデルごとに、各タイプの所有ライセンス数、各タイプのライセンスでライセンス付与できる管理対象デバイスの数が表示されます。有効期限のあるライセンスの場合、このページに有効期限が表示されます。

[Licenses] ページ以外にも、ライセンスとライセンス制限を確認できる方法がいくつかあります。

- [Product Licensing] ダッシュボード ウィジェットはライセンスの概要を示します。
- [Device Management] ページ（[Devices] > [Device Management]）は、各管理対象デバイスに適用されているライセンスをリストします。
- 2 つの ヘルス モジュール（License Monitor および FireSIGHT Host License Limit）をヘルス ポリシーで使用すると、ライセンス ステータスが通知されます。

ライセンスを確認するには、次の手順を実行します。

アクセス： Admin

ステップ 1　[System] > [Licenses] を選択します。

[Licenses] ページが表示されます。

Defense Centerへのライセンスの追加

ライセンス： すべて

Defense Centerにライセンスを追加する前に、ライセンスの購入時にCiscoから提供されたアクティベーション キーがあることを確認してください。

FireSIGHT を除き、ライセンス付き機能を使用する前に、管理対象デバイスでライセンスを有効にする**必要があります**。デバイスをDefense Centerに追加するとき、またはデバイスの追加後にデバイスの一般プロパティを編集することで、ライセンスを有効にできます。シリーズ 2 デバイスには Protection の機能（Security Intelligence フィルタリングを除く）が自動的に組み込まれるため、これらの機能を無効にできず、また他のライセンスを シリーズ 2 デバイスに適用できないことに注意してください。デバイスのライセンス付き機能の変更（65-14 ページ）を参照してください。

注　バックアップの完了後に追加したライセンスは、このバックアップを復元しても削除または上書きされません。復元時の競合を防ぐため、バックアップの復元前にこれらのライセンスを削除し、ライセンスの使用先を書きとめます。バックアップの復元後にこれらのライセンスを追加して再設定できます。競合が発生した場合は、サポートに連絡してください。

ライセンスを追加するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Licenses] を選択します。

[Licenses] ページが表示されます。

ステップ 2　[Add New License] をクリックします。

[Add License] ページが表示されます。

ステップ 3　ライセンスを電子メールで受信しましたか?

- 電子メールで受信した場合は電子メールからライセンスをコピーし、[License] フィールドに貼り付け、[Submit License] をクリックします。

  ライセンスが正しい場合、ライセンスが追加されます。残りの手順は省略します。

- 電子メールで受信していない場合は、[Get License] をクリックします。

  Licensing Center Web サイトが表示されます。インターネットにアクセスできない場合は、インターネットにアクセスできるコンピュータに切り替えてください。ページ下部に表示されるライセンス キーを書きとめ、https://tools.cisco.com/SWIFT/LicensingUI/Home を参照します。

ステップ 4　画面の指示に従ってライセンスを取得します。ライセンスは電子メールで送信されます。

ヒント　サポート サイトにログインした後で、[Licenses] タブでライセンスを要求することもできます。

ステップ 5　電子メールからライセンスをコピーし、Defense Centerの Web インターフェイスの [License] フィールドに貼り付け、[Submit License] をクリックします。

ライセンスが有効な場合、ライセンスが追加されます。これで、デバイスのライセンス付き機能の変更（65-14 ページ）の説明に従って管理対象デバイスでライセンスの機能を有効にできます。

ライセンスの削除

ライセンス：すべて

何らかの理由でライセンスを削除する必要がある場合は、次の手順を使用します。Ciscoは各Defense Centerの固有ライセンス キーに基づいてライセンスを生成するため、あるDefense Centerからライセンスを削除し、削除したライセンスを別のDefense Centerで再利用する場合は、新しいDefense Centerのライセンス キーに基づいた新しいライセンスをリクエストする必要があります。

ほとんどの場合、ライセンスを削除すると、そのライセンスによって有効になる機能を使用することができなくなります。詳細については、サービス サブスクリプション（65-8 ページ）を参照してください。

ライセンスを削除するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Licenses] を選択します。

[Licenses] ページが表示されます。

ステップ 2　削除するライセンスの横にある削除アイコン( )をクリックします。

ライセンスを削除すると、そのライセンスを使用するすべてのデバイスからライセンス付き機能が削除されます。たとえば、Protection ライセンスが 100 台の管理対象デバイスで有効である場合、このライセンスを削除すると、100 台のデバイスすべてから Protection の機能が削除されます。

ステップ 3　ライセンスを削除することを確認します。

ライセンスが削除されます。

デバイスのライセンス付き機能の変更

ライセンス： すべて

サポートされるデバイス： シリーズ 3、仮想、X-Series、ASA FirePOWER

シリーズ 3 デバイス、仮想デバイス、Cisco NGIPS for Blue Coat X-Series、またはASA FirePOWER のライセンス付き機能を変更するには、[Device Management] ページでデバイスの全般プロパティを編集します。一部の例外はありますが、管理対象デバイスでライセンスを無効にすると、そのライセンスに関連づけられている機能は使用できなくなります。

シリーズ 2 デバイスには Protection 機能（Security Intelligence フィルタリングを除く）が自動的に組み込まれています。これらの機能を無効にすること、およびシリーズ 2 デバイスに他のライセンスを適用することはできません。DC500 Defense Centerでは Malware または URL Filtering ライセンスを使用できませんが、DC500 を使用して、シリーズ 3 デバイス、仮想デバイス、Cisco NGIPS for Blue Coat X-Series、または ASA FirePOWER デバイスのこれらのライセンス付き機能およびその他のライセンス付き機能を有効にしたり変更したりすることはできます。

有効にできるライセンスの詳細（バージョン、モデル、およびその他の要件を含む）については、サービス サブスクリプション（65-8 ページ）を参照してください。

デバイスのライセンス付き機能を有効または無効にするには、次の手順を実行します。

アクセス： Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　ライセンスを有効または無効にするデバイスの横にある編集アイコン( )をクリックします。

デバイスの [Interfaces] タブが表示されます。

ステップ 3　[Device] をクリックします。

[Device] タブが表示されます。

ステップ 4　[License] セクションの横にある編集アイコン( )をクリックします。

[License] ポップアップ ウィンドウが表示されます。

ステップ 5　該当するチェック ボックスをオンまたはオフにして、デバイスのライセンス機能を有効または無効にします。

ステップ 6　[Save] をクリックします。

変更は保存されますが、デバイス設定を適用するまでは反映されません。デバイスへの変更の適用（4-27 ページ）を参照してください。

システムソフトウェアの更新

Ciscoは、ルールの更新や地理情報データベース（GeoDB）の更新、脆弱性データベース（VDB）の更新だけでなく、システム ソフトウェア本体のメジャーおよびマイナーの更新など、さまざまなタイプの更新を電子的に配布しています。

注意 この章では、FireSIGHT システムの更新に関する全般的な情報について説明します。VDB、GeoDB、侵入ルールなどを含めて、FireSIGHT システムのいずれかの部分を更新する前に、更新に付随しているリリース ノートまたはアドバイザリ テキストを読んでおく**必要があります**。リリース ノートには、サポートされるプラットフォーム、互換性、前提条件、警告、および特定のインストールとアンインストールの手順などの重要な情報が記載されています。

リリース ノートまたはアドバイザリ テキストに特に記載されていない限り、アプライアンスを更新しても設定は変更されず、アプライアンスの設定はそのまま保持されます。

詳細については、次の項を参照してください。

更新のタイプについて

ライセンス： すべて

Ciscoは、侵入ルールの更新や VDB の更新だけでなく、システム ソフトウェア本体のメジャーおよびマイナーの更新など、さまざまなタイプの更新を電子的に配布しています。

次の表で、Ciscoが提供している更新のタイプについて説明します。ほとんどのタイプの更新では、ダウンロードとインストールをスケジュールすることができます。タスクのスケジュール（62-1 ページ）および再帰的なルール更新の使用（66-20 ページ）を参照してください。

表 66-1　FireSIGHT システム更新のタイプ

更新のタイプ	説明	スケジュール	アンインストール
FireSIGHT システムへのパッチ適用	パッチには、限定された範囲の修正が含まれています(また通常は、5.4.0.1 のようにバージョン番号の 4 桁目が変更されます)。	yes	yes
FireSIGHT システムに対する機能の更新	機能の更新はパッチよりも包括的であり、通常は新しい機能が含まれています(また通常は、5.4.1 のようにバージョン番号の 3 桁目が変更されます)。	yes	yes
FireSIGHT システムに対するメジャーな更新(メジャーおよびマイナーバージョンのリリース)	メジャーな更新はアップグレードと呼ばれることもあります。この更新には新しい機能が含まれており、製品に対する大規模な変更が含まれることがあります(通常は、5.3 または 5.4 のようにバージョン番号の最初の桁または 2 桁目が変更されます)。	no	no
VDB	VDB の更新は、オペレーティング システム、アプリケーション、およびクライアントによって検出された脆弱性、および FireSIGHT システムによって報告された脆弱性に影響を与えます。	yes	no
侵入ルール	侵入ルールを更新すると、更新された新しい侵入ルールおよびプリプロセサ ルール、既存のルールに対して変更された状態、および変更されたデフォルトの侵入ポリシーの設定が提供されます。ルールの更新では、ルールが削除されたり、新しいルール カテゴリとデフォルトの変数が提供されたり、デフォルトの変数値が変更されたりすることもあります。	yes	no
地理情報データベース(GeoDB)	GeoDB の更新により、物理的な場所や接続タイプなど、検出されたルート可能な IP アドレスにシステムが関連付けることができるものに関する情報が提供されます。地理情報データを、アクセス コントロール ルールとして使用することができます。地理情報の詳細を表示するには、GeoDB をインストールする必要があります。 DC500 Defense Centerはこの機能をサポートしません。	yes	no

FireSIGHT システムに対するパッチおよび他のマイナーな更新はアンインストールできますが、VDB、GeoDB、または侵入ルールに対するメジャーな更新をアンインストールしたり、前のバージョンに戻したりすることはできないことに注意してください。自分のアプライアンスを、FireSIGHT システムの新しいメジャー バージョンに更新した場合、および古いバージョンに戻す必要がある場合は、サポートに連絡してください。

ソフトウェア更新の実行

ライセンス: すべて

FireSIGHT システムの展開を更新するには、いくつかの基本的な手順があります。最初に、更新の準備として、リリース ノートを参照し、必要な更新前のタスクをすべて完了しておく**必要があります**。これで更新を開始することができます。まずDefense Centerを更新し、次にこれらが管理するデバイスを更新します。更新が完了し、更新が正常に終了したことを確認するまで、更新の進捗状況を監視する必要があります。最後に、更新後の必要な手順を完了させます。

詳細については、次の項を参照してください。

更新の計画

ライセンス： すべて

更新を開始する前に、リリース ノートをよく読んで理解する必要があります。リリース ノートはサポート サイトからダウンロードすることができます。リリース ノートには、サポートされているプラットフォーム、新しい機能、既知および解決済みの問題、製品の互換性について記載されています。また、リリース ノートには前提条件、警告、および特別なのインストールおよびアンインストールの手順についての重要な情報が含まれています。

以降の項では、更新の計画で検討しなければならない要素の概要を提供します。

FireSIGHT システムのバージョンの要件

アプライアンス（ソフトウェアベースのデバイスを含む）が、FireSIGHT システムの正しいバージョンを実行していることを確認する必要があります。リリース ノートには必要なバージョンが示されています。古いバージョンを実行している場合は、サポート サイトから更新を取得することができます。

オペレーティング システム要件

ソフトウェアベースのデバイスをインストールしたコンピュータが、オペレーティング システムの正しいバージョンを実行していることを確認します。リリース ノートには必要なバージョンが示されています。仮想デバイスでサポートされるオペレーティング システムの詳細については、『*FireSIGHT SystemVirtual Installation Guide*』を参照してください。Cisco NGIPS for Blue Coat X-Series でサポートされるオペレーティング システムの詳細については、『*Cisco NGIPS for Blue Coat X-Series Installation Guide*』を参照してください。

時間とディスク領域の要件

十分な空きディスク領域があることを確認し、更新のために十分な時間を確保しておく必要があります。管理対象デバイスを更新する場合には、Defense Centerで追加のディスク領域が必要になります。リリース ノートには、領域と時間の要件が示されています。

設定およびイベント バックアップのガイドライン

Ciscoでは、メジャーの更新を開始する前に、外部の場所へコピーした後にアプライアンス上に残っているバックアップをすべて削除することを推奨しています。更新のタイプに関係なく、現行のイベントおよび設定データを外部の場所にバックアップしておく必要もあります。イベント データは、更新プロセスの一部としてバックアップされ**ません**。

Defense Centerを使用して、それ自身、および管理対象のイベントと設定データをバックアップすることができます。バックアップと復元の使用（70-1 ページ）を参照してください。

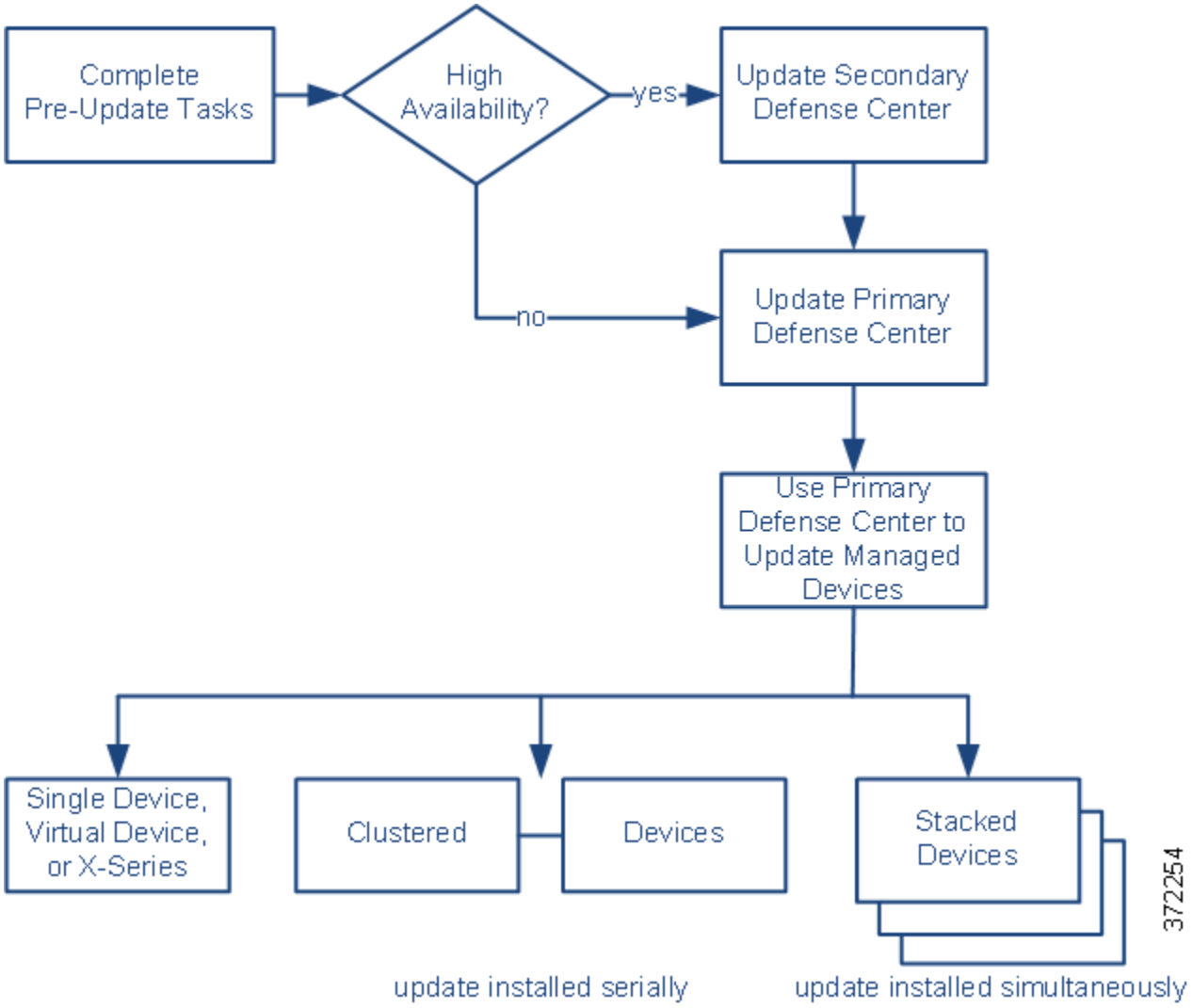
更新を実行するタイミング

更新プロセスはトラフィックの調査、トラフィック フロー、およびリンク ステートに影響を与えることがあること、および更新を行っている間は Data Correlator が無効になっていることにより、Ciscoでは、保守を行っている間、または中断が展開に及ぼす影響が最も少ない時間に更新を行うことを推奨しています。

更新プロセスについて

ライセンス： すべて

次の図は、更新プロセスの概要を示しています。



更新の順序

管理対象のデバイスを更新するには、その前に、Defense Centerを更新**する必要があります**。

Defense Centerを使用した更新の実行

Ciscoは、Defense Centerの Web インターフェイスを使用して、それ自身だけでなく、管理対象のデバイスも更新することを推奨しています。仮想デバイスや Cisco NGIPS for Blue Coat X-Series など、Web インターフェイスを持たない管理対象デバイスを更新するには、Defense Center を使用する**必要があります**。Cisco NGIPS for Blue Coat X-Series に対するメジャーな更新では、前のバージョンをアンインストールして新しいバージョンをインストールしなければならないことがあります。詳細については、『*Cisco NGIPS for Blue Coat X-SeriesInstallation Guide*』を参照してください。

[Product Updates] ページ（[System] > [Updates]）には、それぞれの更新のバージョン、およびその更新が生成された日時が表示されます。また、更新の一環としてリブートが必要かどうかも示されます。

サポートから取得した更新をアプライアンスへアップロードすると、更新がページに示されます。パッチ機能および機能の更新のアンインストーラも表示されます。ソフトウェア更新のアンインストール（66-12 ページ）を参照してください。Defense Centerで、ページに VDB 更新を表示できます。

ヒント　パッチおよび機能の更新では、自動更新機能を利用することができます。ソフトウェア更新の自動化（62-12 ページ）を参照してください。

ペアのDefense Centerの更新

高可用性ペアの 1 つのDefense Centerの更新を開始すると、Defense Centerのペアの一方が（まだプライマリになっていない場合は）プライマリになります。また、ペアのDefense Centerが設定情報の共有を停止すると、ペアのDefense Centerは、通常の同期プロセスの一環としてのソフトウェア更新は受信しません。

操作の継続性を保証するには、ペアのDefense Centerを同時に更新**しないでください**。まず、セカンダリDefense Centerの更新手順を完了してからプライマリを更新してください。

クラスタ デバイスの更新

クラスタ デバイスまたはクラスタ スタック上で更新をインストールすると、システムは、複数のデバイスまたはスタック上で同時に更新を実行します。更新を開始すると、システムは最初にバックアップ デバイスまたはスタックに更新を適用し、必要なプロセスが再開され、デバイスまたはスタックがトラフィックを再処理するまでメンテナンス モードになります。システムは、アクティブなデバイスまたはスタックに更新を適用し、同じプロセスを行います。

クラスタ スタックのデバイスを更新するには、クラスタのすべてのメンバ上で同時に、管理しているDefense Centerから更新を実行する必要があります。デバイスから直接更新を実行することはできません。

スタック デバイスの更新

スタック デバイスに更新をインストールすると、システムは更新を同時に実行します。各デバイスは、更新が完了すると通常の動作を再開します。次の点に注意してください。

- すべてのセカンダリ デバイスの更新が完了する*前に*プライマリ デバイスが更新を完了した場合、すべてのデバイスが更新を完了するまでスタックは、バージョンが混在した制限付きの状態で作動します。
- すべてのセカンダリ デバイスの更新が完了した*後で*プライマリ デバイスの更新が完了した場合は、プライマリ デバイスで更新が完了したときに、スタックは通常の動作を再開します。

トラフィック フローとインスペクション

管理対象デバイスから更新をインストールまたはアンインストールすると、次の機能に影響を及ぼすことがあります。

- トラフィックのインスペクション（アプリケーションおよびユーザの認識とコントロール、URL フィルタリング、セキュリティ インテリジェンス フィルタリング、侵入検出と防御、接続のロギングなど）
- トラフィック フロー（スイッチング、ルーティング、関連する機能など）
- リンク ステート

Data Correlator は、システムの更新中は動作しません。更新が完了すると再開します。

ネットワーク トラフィックの中断の方法と期間は、更新が影響を及ぼす FireSIGHT システムのコンポーネント、デバイスがどのように設定および展開されているか、更新によりデバイスがリブートされるかどうか、によって異なります。特定の更新に対してネットワーク トラフィックがいつ、どのように影響を受けるかについての情報は、リリース ノートを参照してください。

ヒント　クラスタ デバイスを更新する場合、システムは、トラフィックの中断を回避するために、一度に 1 つずつ更新を実行します。

更新中の Web インターフェイスの使用

更新のタイプに関係なく、更新中のアプライアンスの Web インターフェイスを使用して、更新の監視以外のタスクを実行**しないで**ください。

メジャーな更新中にユーザがアプライアンスを使用しないようにし、メジャーな更新の進捗をユーザが簡単に監視できるようにするために、アプライアンスの Web インターフェイスが合理化されています。タスク キュー（[System] > [Monitoring] > [Task Status]）でマイナーな更新の進捗を監視することができます。マイナーな更新中に Web インターフェイスを使用することは禁止されていませんが、Ciscoでは推奨していません。

ヒント　管理対象デバイスの更新を監視するには、Defense Centerでタスク キューを使用します。

マイナーな更新であっても、更新プロセス中は、更新しているアプライアンスの Web インターフェイスは使用できないか、またはアプライアンスでユーザがログアウトされることがあります。これは想定されている動作です。この場合は、もう一度ログインしタスク キューを表示します。まだ更新が実行中の場合は、更新が完了するまで Web インターフェイスを使用**しないで**ください。更新中は、管理対象デバイスが 2 回リブートされることがありますが、これは予想される動作です。

注意　（Web インターフェイスに更新が失敗したことが示されている、タスク キューの手動更新または [Update Status] ページに進捗が表示されないなど）更新で問題が発生した場合には、更新を再開**しない**でください。代わりに、サポートへ連絡してください。

更新後

リリース ノートに記載されている更新後のすべてのタスクを完了し、展開が正常に実行されていることを確認する**必要があります**。

更新後のタスクで最も重要なことは、Defense Centerを更新した後と、管理対象デバイスを更新した後の両方で、アクセス コントロール ポリシーを再適用することです。

注意　アクセス コントロール ポリシーを適用した場合、リソースを要求すると、いくつかのパケットが検査なしでドロップされることがあります。さらに、構成の一部を適用するときに、Snort プロセスの再開が要求され、これにより一時的にトラフィック検査が中断されます。この検査中にトラフィックがドロップされるか、それ以上検査が行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。アクセス コントロール ポリシーの適用（12-17 ページ）とSnort プロセスを再開する構成（1-8 ページ）を参照してください。

また、次の作業を実行する必要があります。

- 更新が正常に終了したことを確認する
- 展開のすべてのアプライアンスが正常に通信していることを確認する
- 必要に応じて侵入ルール、VDB、および GeoDB を更新する
- リリース ノートの情報に基づいて、必要な設定変更を行う
- リリース ノートに記載されている、更新後の追加タスクを実行する

Defense Center の更新

ライセンス： すべて

更新のタイプ、およびDefense Centerがインターネットへアクセスできるかどうかによって、Defense Centerを次のいずれかの方法で更新します。

- Defense Centerがインターネットにアクセスできる場合は、Defense Centerを使用して、サポート サイトから直接更新を取得します。このオプションは、メジャーな更新ではサポート**されていません**。
- サポート サイトから更新を手動でダウンロードして、Defense Centerへアップロードすることもできます。Defense Centerがインターネットへアクセスできない場合、またはメジャーな更新を実行している場合は、このオプションを選択します。

注意　操作の継続性を保証するために、ペアのDefense Centerを同時に更新**しないでください**。ペアのDefense Centerの更新（66-5 ページ）を参照してください。

メジャーな更新の場合は、Defense Centerを更新すると、以前の更新のアンインストーラが削除されます。

Defense Centerを更新する方法：

アクセス： Admin

ステップ 1　リリース ノートを読んで、更新前の必要なタスクを完了します。

更新前のタスクには、Defense CenterがCiscoソフトウェアの正しいバージョンを実行している、更新を実行するための十分な空きディスク領域がある、更新を実行するために十分な時間を確保している、イベントおよび設定データをバックアップした、などの確認が含まれています。

ステップ 2　更新をDefense Centerへアップロードします。ここで、更新のタイプによって、およびDefense Centerがインターネットにアクセスできるかどうかによって、2 つのオプションがあります。

- メジャーな更新を除くすべての更新で、Defense Centerがインターネットにアクセスできる場合は、[System] > [Updates] を選択し、[Download Updates] をクリックして、最新の更新をチェックします。メジャーな更新の場合、またはDefense Centerがインターネットにアクセスできない場合は、最初に更新を手動でダウンロードする必要があります。次のサポート サイトのいずれかから更新をダウンロードします。
  - **すべての Sourcefire の更新**: (https://support.sourcefire.com/)
  - **シスコの更新**:

    物理防御センター
    (http://software.cisco.com/download/navigator.html?mdfid=278875421)
    仮想防御センター
    (http://software.cisco.com/download/type.html?mdfid=286259687&catid=null)
- [System] > [Updates] を選択して [Upload Update] をクリックします。更新を参照して、[Upload] をクリックします。

注　サポート サイトから、手動でまたは [Product Updates] タブで [Download Updates] をクリックして、更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、ファイルが破損することがあります。

更新がDefense Centerへアップロードされます。

ステップ 3　展開内でアプライアンスが正常に通信していること、およびヘルス モニタによって問題が報告されていないことを確認します。

ステップ 4　[System] > [Monitoring] > [Task Status] を選択してタスク キューを表示し、進行中のジョブがないことを確認します。

更新を開始したときに実行されているタスクは停止され、再開できません。更新が完了した後で、タスク キューから手動で削除する必要があります。タスク キューは 10 秒ごとに自動的にリフレッシュされます。更新を始める前に、長時間実行しているタスクが完了するまで待機する必要があります。

ステップ 5　[System] > [Updates] を選択します。

[Product Updates] ページが表示されます。

ステップ 6　ユーザがアップロードする更新の隣にあるインストール アイコンをクリックします。

[Install Update] ページが表示されます。

ステップ 7　Defense Centerを選択し、[Install] をクリックします。プロンプトが表示されたら、更新をインストールすることを確認してDefense Centerをリブートします。

更新プロセスが開始されます。更新を監視する方法は、更新がメジャーかマイナーかによって異なります。更新のタイプを判断するには、FireSIGHT システム更新のタイプの表およびリリース ノートを参照してください。

- マイナーな更新については、タスク キュー ([System] > [Monitoring] > [Task Status]) で更新の進捗を監視することができます。
- メジャーな更新については、タスク キューで更新の進捗の監視を開始できます。ただし、Defense Centerによる更新前のチェックが完了すると、ユーザはログアウトされます。もう一度ログインすると、[Upgrade Status] ページが表示されます。詳細については、メジャーな更新のステータスの監視 (66-11 ページ)を参照してください。

注意　更新のタイプに関係なく、更新が完了するまで、更新の監視以外のタスクを実行するために Web インターフェイスを使用**しないで**ください。必要な場合は、Defense Centerをリブートします。詳細については、更新中の Web インターフェイスの使用（66-6 ページ）を参照してください。

ステップ 8　更新が完了したら、必要に応じてDefense Centerにログインします。

メジャーな更新の後に最初にログインするユーザには、エンド ユーザ ライセンス契約（EULA）が表示されることがあります。EULA を確認して承認し、処理を続行します。

ステップ 9　ブラウザのキャッシュを消去し、ブラウザを強制的にリロードします。このようにしない場合は、ユーザ インターフェイスが予期せぬ動作をすることがあります。

ステップ 10　[Help] > [About] を選択し、ソフトウェアのバージョンが正しく示されていることを確認します。また、Defense Centerでルール更新および VDB のバージョンをメモしておいてください。この情報は後で必要になります。

ステップ 11　すべての管理対象デバイスが、Defense Centerと正常に通信していることを確認します。

ステップ 12　サポート サイトで利用できるルール更新が、自身のDefense Center上のルールよりも新しい場合は、新しいルールをインポートします。

詳細については、ルールの更新とローカル ルール ファイルのインポート（66-16 ページ）を参照してください。

ステップ 13　アクセス コントロール ポリシーを再適用します。

アクセス コントロール ポリシーを適用した場合、リソースを要求すると、いくつかのパケットが検査なしでドロップされることがあります。さらに、構成の一部を適用するときに、Snort プロセスの再開が要求され、これにより一時的にトラフィック検査が中断されます。この検査中にトラフィックがドロップされるか、それ以上検査が行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。アクセス コントロール ポリシーの適用（12-17 ページ） およびSnort プロセスを再開する構成（1-8 ページ）を参照してください。

ステップ 14　サポート サイトで利用可能な VDB が、ご使用のDefense Centerの VDB より新しい場合は、最新の VDB をインストールします。

VDB の更新をインストールすると、トラフィック フローと処理が一時的に停止することがあります。また、いくつかのパケットが検査されない場合があります。詳細については、脆弱性データベースの更新（66-14 ページ）を参照してください。

ステップ 15　次の項、管理対象デバイスの更新へ進んで、Defense Centerが管理するデバイス上でCisco ソフトウェアを更新します。

管理対象デバイスの更新

ライセンス： すべて

Ciscoでは、Defense Centerの更新が終わったあとでこれを使用して、管理対象のデバイスを更新することを推奨しています。仮想デバイスや Cisco NGIPS for Blue Coat X-Series など、Web インターフェイスを持たない管理対象デバイスを更新するには、Defense Centerを使用する**必要があります**。Cisco NGIPS for Blue Coat X-Series に対するメジャーな更新では、前のバージョンをアンインストールして新しいバージョンをインストールしなければならないことがあります。

管理対象デバイスの更新は、2 段階のプロセスです。最初に、以下のいずれかのサポート サイトから更新をダウンロードし、それを管理元の Defense Center へアップロードします。

- **Sourcefire:**（https://support.sourcefire.com/）
- **シスコ：**（http://www.cisco.com/cisco/web/support/index.html）

次に、ソフトウェアをインストールします。

注 トラフィックのインスペクション、トラフィック フロー、およびリンク状態は、デバイスがどのように設定および展開されているか、更新がどのコンポーネントに影響を及ぼすか、更新によってデバイスがリブートされるかどうかよって、更新中に影響を受けることがあります。特定の更新に対してネットワーク トラフィックがいつ、どのように影響を受けるかについての具体的な情報は、対象の更新のリリース ノートを参照してください。

管理対象デバイスを更新する方法：

アクセス： Admin

ステップ 1 リリース ノートを読んで、更新前の必要なタスクを完了します。

更新前のタスクには、管理元のDefense Centerを更新する、イベントおよび設定データをバックアップする、およびデバイスがCiscoソフトウェアの正しいバージョンを実行していること、ソフトウェアベースのデバイスをインストールしたコンピュータがオペレーティング システムの正しいバージョンを実行していること、更新を実行するのに十分な空きディスク領域があること、更新を実行するのに十分な時間を確保していることを確認する、といったことが含まれています。

ステップ 2 デバイスを管理しているDefense Center上で FireSIGHT システム ソフトウェアを更新します。Defense Center の更新（66-7 ページ）を参照してください。

ステップ 3 次のサポート サイトのいずれかから更新をダウンロードします。

- **すべての Sourcefire の更新：**（https://support.sourcefire.com/）
- **シスコの更新：**

物理管理対象デバイス：（http://software.cisco.com/download/navigator.html?mdfid=278875421）
仮想管理対象デバイス：
（http://software.cisco.com/download/type.html?mdfid=286259690&flowid=70802）
デバイス モデルごとに異なる更新を使用できます。ダウンロードできる更新については、リリース ノートを参照してください。

注 サポート サイトから更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、ファイルが破損することがあります。

ステップ 4 展開内でアプライアンスが正常に通信していること、およびヘルス モニタによって問題が報告されていないことを確認します。

ステップ 5 管理元のDefense Centerで、[System] > [Update] を選択します。

[Product Updates] ページが表示されます。

ステップ 6 [Upload Update] をクリックして、ダウンロードした更新を参照し、[Upload] をクリックします。

更新が Defense Center へアップロードされます。[Product Updates] タブに、アップロードした更新のタイプ、バージョン番号、および生成された日付と時刻が示されます。このページには、更新の一環としてリブートが必要かどうかも示されます。

ステップ 7 ユーザがインストールする更新の隣にあるインストール アイコンをクリックします。

[Install Update] ページが表示されます。

ステップ 8　更新をインストールするデバイスを選択して [Install] をクリックします。同じ更新を使用する場合は、複数のデバイスを一度に更新できます。プロンプトが表示されたら、更新をインストールすることを確認してデバイスをリブートします。

更新プロセスが開始されます。ファイルのサイズによっては、すべてのデバイスで更新をインストールするのに時間がかかることがあります。Defense Centerのタスク キュー（[System] > [Monitoring] > [Task Status]）で更新の進捗を監視することができます。更新中に、管理対象デバイスが 2 回リブートされることがありますが、これは正常な動作です。

注意　（タスク キューに更新が失敗したことが示されている、またはタスク キューの手動更新で進捗が表示されないなど）更新で問題が発生した場合には、更新を再開**しない**でください。代わりに、サポートへ連絡してください。

ステップ 9　オプションとして、メジャーな更新の後でデバイスのローカル Web インターフェイスにログインします。

メジャーな更新の後に最初にログインするユーザには、エンド ユーザ ライセンス契約（EULA）が表示されることがあります。EULA を確認して承認し、処理を続行します。Web インターフェイスではなくコマンドライン インターフェイスを介して最初にログインした場合も EULA が表示されるので、必ず承認してください。

ステップ 10　Defense Centerで、[Devices] > [Device Management] を選択し、更新したデバイスのバージョンが記載されている正しいものであることを確認します。

ステップ 11　更新したデバイスが、Defense Centerと正常に通信していることを確認します。

ステップ 12　アクセス コントロール ポリシーを再適用します。

アクセス コントロール ポリシーを適用した場合、リソースを要求すると、いくつかのパケットが検査なしでドロップされることがあります。さらに、構成の一部を適用するときに、Snort プロセスの再開が要求され、これにより一時的にトラフィック検査が中断されます。この検査中にトラフィックがドロップされるか、それ以上検査が行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。アクセス コントロール ポリシーの適用（12-17 ページ）およびSnort プロセスを再開する構成（1-8 ページ）を参照してください。

メジャーな更新のステータスの監視

ライセンス： すべて

メジャーな更新では、FireSIGHT システムは、更新プロセスを簡単に監視できるような、簡潔な Web インターフェイスを提供します。インターフェイスが簡潔であるため、更新の監視以外のタスクを実行するために Web インターフェイスが使用されることもなくなります。

タスク キュー（[System] > [Monitoring] > [Task Queue]）で更新の進捗の監視を開始できます。ただし、アプライアンスが更新前の必要なチェックを完了したら、自分を含めたすべてのユーザが Web インターフェイスからログアウトされます。Administrator または Maintenance User 以外の場合は、更新が完了するまでログインし直すことはできません。

Administrator の場合は、ログインし直すと、簡潔な更新ページが表示されます。

Defense Centerを使用して管理対象デバイスを更新する場合、Ciscoでは、Defense Centerのタスク キューから更新の進捗を監視することを推奨しています。ただし、アプライアンスが更新前のチェックを終了した後で、ユーザがデバイスのローカル Web インターフェイスにログインしようとすると、簡潔な更新ページが表示され、これを使用して更新の進捗を監視することができます。

このページには、更新前の FireSIGHT システムのバージョン、更新後のバージョン、および更新を開始してからの経過時間が表示されます。また進捗バーが表示され、実行中のスクリプトに関する詳細が示されます。

ヒント 更新ログを表示するには、[show log for current script] をクリックします。ログをもう一度非表示にするには、[hide log for current script] をクリックします。

何らかの理由で更新が失敗すると、ページにはエラー メッセージが表示され、失敗した日時、更新が失敗したときに実行していたスクリプト、およびサポートへ連絡するための方法が示されます。更新を再開**しないで**ください。

注意 更新で他の問題（ページの手動更新で長時間経過しても進捗が表示されない、など）が生じた場合も、更新を再開**しないで**ください。代わりに、サポートへ連絡してください。

更新が完了すると、アプライアンスで正常終了のメッセージが表示され、リブートが行われます。アプライアンスのリブートが完了した後で、ページを更新してログインし、更新後の必要な手順を完了します。

ソフトウェア更新のアンインストール

ライセンス： すべて

Cisco アプライアンスへパッチまたは機能の更新を適用すると、更新プロセスによってアンインストーラが作成されます。これにより、Web インターフェイスを使用してアプライアンスから更新を削除することができます。

更新をアンインストールした場合、結果として保持されるCisco ソフトウェアのバージョンは、アプライアンスをどのような経路で更新したかによって異なります。たとえば、アプライアンスをバージョン 5.0 からバージョン 5.0.0.2 へ直接更新した場合のシナリオについて考えてみます。バージョン 5.0.0.2 のパッチをアンインストールすると、バージョン 5.0.0.1 の更新をインストールしたことがなくても、バージョン 5.0.0.1 を実行するアプライアンスが結果として生成されます。更新をアンインストールしたときに結果として生成されるCisco ソフトウェアのバージョンの詳細については、リリース ノートを参照してください。

注 メジャーな更新では、Web インターフェイスからのアンインストールはサポートされていません。アプライアンスを FireSIGHT システムの新しいメジャー バージョンに更新して、古いバージョンに戻す必要がある場合は、サポートに連絡してください。

アンインストールの順序

更新は、インストールの逆の順序でアンインストールします。つまり、最初に管理対象デバイスから更新をアンインストールし、次にDefense Centerからアンインストールします。

ローカル Web インターフェイスを使用した更新のアンインストール

更新をアンインストールするにはローカル Web インターフェイスを使用する必要があります。Defense Centerを使用して、管理対象デバイスから更新をアンインストールすることはできません。ローカル Web インターフェイスを持たないデバイス（仮想デバイスや Cisco NGIPS for Blue Coat X-Series など）からパッチをアンインストールする場合の詳細については、リリース ノートを参照してください。

このプロセスを使用して、Cisco NGIPS for Blue Coat X-Series のマイナーな更新をアンインストールできますが、このプロセスを使用して、X-Series プラットフォームから Cisco NGIPS for Blue Coat X-Series アプリケーションをアンインストールすることはできないことに注意してください。詳細については、『*Cisco NGIPS for Blue Coat X-Series インストレーション ガイド*』を参照してください。

クラスタまたはペア アプリケーションからの更新のアンインストール

高可用性ペアのクラスタ デバイスおよびDefense Centerは、同じバージョンの FireSIGHT システム を実行する必要があります。アンインストール プロセスは自動フェールオーバーをトリガーしますが、不一致のペアまたはクラスタのアプライアンスは、設定情報を共有せず、同期の一部として更新をインストールまたはアンインストールすることもありません。冗長なアプライアンスから更新をアンインストールしなければならない場合は、アンインストールを連続して実行するよう計画します。

アンインストールによって、これらのデバイスが、クラスタ スタックがサポートされないバージョンに戻される場合は、クラスタ スタックのデバイスから更新をアンインストールできません。

運用の継続性を保証するために、クラスタ デバイスおよびペアのDefense Centerから一度に 1 つずつ更新をアンインストールします。まず、セカンダリ アプライアンスから更新をアンインストールします。アンインストール プロセスが完了するまで待ってから、すぐにプライマリ アプライアンスから更新をアンインストールします。

注意　クラスタ デバイスまたはペアDefense Centerからのアンインストール プロセスが失敗した場合は、アンインストールを再開したり、ピアの設定を変更したり**しないでください**。代わりに、サポートへ連絡してください。

スタック デバイスからの更新のアンインストール

スタック内のすべてのデバイスが、同じバージョンの FireSIGHT システム を実行する必要があります。スタック デバイスのいずれかから更新をアンインストールすると、そのスタックではデバイスが限定的な、バージョンが混在する状態になります。

展開における影響を最小限にするために、Ciscoでは、スタック デバイスから更新を同時にアンインストールすることを推奨しています。スタック内のすべてのデバイスで更新が完了すると、スタックは通常の動作を再開します。

アンインストールによって、これらのデバイスが、クラスタ スタックがサポートされないバージョンに戻される場合は、クラスタ スタックのデバイスから更新をアンインストールできません。

トラフィック フローとインスペクション

管理対象デバイスから更新をアンインストールすると、トラフィックのインスペクション、トラフィック フロー、およびリンク ステートに影響を及ぼすことがあります。特定の更新に対してネットワーク トラフィックがいつ、どのように影響を受けるかについての情報は、リリース ノートを参照してください。

アンインストール後

更新をアンインストールした後、展開環境が正しく動作していることを保証するために、いくつかの手順を実行する必要があります。これらの手順には、アンインストールが正常に終了したことの確認、および展開内のすべてのアプライアンスが正常に通信していることの確認が含まれます。それぞれの更新に特定の情報については、リリース ノートを参照してください。

ローカル Web インターフェイスを使用してパッチまたは機能の更新をアンインストールする方法：

アクセス：Admin

ステップ 1　[System] > [Updates] を選択します。

[Product Updates] ページが表示されます。

ステップ 2　削除する更新のアンインストーラの隣にあるインストール アイコンをクリックします。

- Defense Centerで、[Install Update] ページが表示されます。Defense Centerを選択し、[Install] をクリックします。
- 管理対象デバイスには、操作のページがありません。

いずれの場合も、プロンプトが表示されたら、更新をアンインストールすることを確認してアプライアンスをリブートします。

アンインストール プロセスが開始されます。タスク キュー（[System] > [Monitoring] > [Task Status]）で進捗を監視することができます。

注意　アンインストールが完了するまで、更新の監視以外のタスクを実行するために Web インターフェイスを使用**しないで**ください。必要に応じて、アプライアンスをリブートします。詳細については、更新中の Web インターフェイスの使用（66-6 ページ）を参照してください。

ステップ 3　アンインストールが完了したら、必要に応じてアプライアンスにログインします。

ステップ 4　ブラウザのキャッシュを消去し、ブラウザを強制的にリロードします。このようにしない場合は、ユーザ インターフェイスが予期せぬ動作をすることがあります。

ステップ 5　[Help] > [About] を選択し、ソフトウェアのバージョンが正しく示されていることを確認します。

ステップ 6　パッチをアンインストールしたアプライアンスが正常に管理対象デバイスと通信していること（Defense Centerの場合）、または管理元のDefense Centerと通信していること（管理対象デバイスの場合）を確認します。

脆弱性データベースの更新

ライセンス：すべて

Cisco脆弱性データベース（VDB）は、オペレーティング システム、クライアント、およびアプリケーションのフィンガープリントだけでなく、ホストが影響を受ける可能性のある既知の脆弱性のデータベースです。FireSIGHT システムはフィンガープリントと脆弱性を関連付けて、特定のホストがネットワークの侵害のリスクを増大させているかどうかを判断するのをサポートします。Cisco脆弱性調査チーム（VRT）は、VDB を定期的に更新します。

VDB を更新するには、Defense Centerで [Product Updates] ページを使用します。サポートから取得した VDB の更新をアプライアンスへアップロードすると、このページに、アップロードした更新と FireSIGHT システムの更新およびそのアンインストーラの更新が示されます。

脆弱性のマッピングを更新するのにかかる時間は、ネットワーク マップ内のホストの数によって異なります。システムのダウンタイムの影響を最小にするために、システムの使用率が低い時間帯に更新をスケジュールすることをお勧めします。一般的に、更新の実行にかかるおおよその時間（分）を判断するには、ネットワーク上のホストの数を 1000 で割ります。

注 更新されたアプリケーションのディテクタおよび VDB 内のオペレーティング システムのフィンガープリントについては、有効にする前にアクセス コントロール ポリシーの再適用が必要です。VDB の更新完了後に、古くなったすべてのアクセス コントロール ポリシーを管理対象デバイスに再適用します。VDB のインストールまたはアクセス コントロール ポリシーの再適用を行うと、管理対象デバイス上でトラフィック フローと処理が一時的に停止することがあり、また、いくつかのパケットが検査されずに通過する場合があるので注意してください。詳細については、アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

この項では、手動による VDB 更新を計画および実行する方法について説明します。自動更新機能を利用して VDB の更新をスケジュールすることもできます。脆弱性データベースの更新の自動化（62-17 ページ）を参照してください。

脆弱性データベースを更新する方法:

アクセス: Admin

ステップ 1 更新用の VDB 更新アドバイザリ テキストを読みます。

このアドバイザリ テキストには、更新で作成された VDB に対する変更、および製品の互換性情報が含まれています。

ステップ 2 [System] > [Updates] を選択します。

[Product Updates] ページが表示されます。

ステップ 3 Defense Centerへ更新をアップロードします。

- Defense Centerがインターネットにアクセスできる場合は、[Download Updates] をクリックして、次のいずれかのサポート サイトで最新の更新を確認します。
  - **Sourcefire:**（https://support.sourcefire.com/）
  - **シスコ**:（http://www.cisco.com/cisco/web/support/index.html）
- Defense Centerがインターネットにアクセスできない場合は、次のいずれかのサポート サイトから更新を手動でダウンロードして [Upload Update] をクリックします。更新を参照して、[Upload] をクリックします。
  - **Sourcefire:**（https://support.sourcefire.com/）
  - **シスコ**:（http://www.cisco.com/cisco/web/support/index.html）

注 サポート サイトから、手動でまたは [Download Updates] をクリックして、更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、ファイルが破損することがあります。

更新がDefense Centerへアップロードされます。

ステップ 4 VDB 更新の隣にあるインストール アイコンをクリックします。

[Install Update] ページが表示されます。

ステップ 5 Defense Centerを選択し、[Install] をクリックします。

更新プロセスが開始されます。ネットワーク マップ内のホストの数によっては、更新のインストールに時間がかかることがあります。タスク キュー（[System] > [Monitoring] > [Task Status]）で更新の進捗を監視することができます。

注意 更新が完了するまで、マップされた脆弱性に関連するタスクを実行するために Web インターフェイスを使用**しないで**ください。(タスク キューに更新が失敗したことが示されている、またはタスク キューの手動更新で進捗が表示されないなど) 更新で問題が発生した場合には、更新を再開**しない**でください。代わりに、サポートへ連絡してください。

ステップ 6 更新が終了したら、[Help] > [About] を選択して、VDB のビルド番号が、インストールした更新と一致していることを確認します。

VDB 更新を有効にするには、古くなったすべてのアクセス コントロール ポリシーを再適用する必要があります。「アクセス コントロール ポリシーの適用 (12-17 ページ)」を参照してください。

ルールの更新とローカル ルール ファイルのインポート

ライセンス: すべて

新しい脆弱性に関する情報が判明すると、Cisco脆弱性調査チーム (VRT) からルール更新がリリースされるので、これを最初にDefense Centerにインポートしてから、影響を受けるアクセス コントロール、ネットワーク解析、および侵入ポリシーを管理対象デバイスに適用することで、その実装ができます。

ルール更新は累積的なので、Ciscoは常に最新の更新をインポートすることを推奨しています。現在インストールされているルールのバージョンに一致するルール更新、またはそれより前のバージョンのルール更新をインポートすることはできません。展開に高可用性ペアのDefense Centerが含まれる場合は、プライマリ側だけに更新をインポートします。セカンダリのDefense Centerは、通常の同期プロセスの一環としてルールの更新を受け取ります。

注 ルール更新には新しいバイナリが含まれている場合があるので、これらのダウンロードおよびインストールのプロセスが、自身のセキュリティ ポリシーに適合していることを確認してください。また、ルールの更新は量が多くなることがあるため、ルールのインポートはネットワークの使用量が少ないときに行うようにしてください。

ルール更新では、次のものを提供します。

- **新規または変更されたルールおよびルールの状態**: ルール更新は、新規または更新された侵入およびプリプロセッサのルールを提供します。新しいルールについては、ルールの状態がそれぞれのシステム提供の侵入ポリシーで異なる場合があります。たとえば、Security over Connectivity の侵入ポリシーでは新しいルールが有効になっており、Connectivity over Security の侵入ポリシーでは無効になっていることがあります。ルールの更新では、既存のルールのデフォルト状態が変更されたり、既存のルールそのものが削除されることもあります。
- **新しいルール カテゴリ**: ルール更新には、常に追加される新しいルール カテゴリが含まれている場合があります。
- **変更されたプリプロセッサおよび詳細設定**: ルール更新は、システム提供の侵入ポリシーの詳細設定および、システム提供のネットワーク解析ポリシーのプリプロセッサ設定を変更することがあります。また、アクセス コントロール ポリシーにおける高度な前処理やパフォーマンス オプションに関するデフォルト値を更新することもあります。

- **新規の変数および変数の変更**：ルール更新は、既存のデフォルト変数のデフォルト値を変更することがありますが、ユーザによる変更は上書きされません。新しい変数は常に追加されています。

ルール更新でポリシーが変更されるタイミングの概要

ルール更新は、すべてのアクセス コントロール ポリシーと同様に、システム提供およびカスタムのネットワーク解析ポリシーの両方に影響を与えます。

- **システム提供**：システムが提供するネットワーク解析および侵入ポリシーへの変更は、その他のアクセス コントロールの詳細設定と同様に、更新後にポリシーを再適用すると自動的に有効になります。
- **カスタム**：カスタムのネットワーク解析および侵入ポリシーは、いずれもシステム提供のポリシーをベースとして使用するか、ポリシー チェーン中でのイベント ベースとして使用しているので、ルール更新がカスタムのネットワーク解析および侵入ポリシーにも影響を与えることがあります。ただし、ルール更新によるこれらの自動的な変更が行われないようにすることができます。これにより、ルール更新のインポートとは関係ないスケジュールで、システムによって提供される基本ポリシーを手動で更新できます。ユーザによる選択とは関係なく（カスタム ポリシーごとに実装）システム提供のポリシーに対する更新では、ユーザがカスタマイズした設定は上書き**されません**。詳細については、ルール更新がシステムによって提供される基本ポリシーを変更することを許可する（24-4 ページ）を参照してください。

ルールの更新をインポートすると、ネットワーク解析および侵入ポリシーのキャッシュされていた変更は、すべて廃棄されることに注意してください。確認用に [Rule Updates] ページには、ポリシーとキャッシュされた変更、および変更を行ったユーザが表示されます。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

ポリシーの再適用

ルール更新による変更を反映させるには、変更されたすべてのポリシーを再適用する必要があります。ルール更新をインポートする際には、侵入またはアクセス コントロール ポリシーを自動的にターゲット デバイスに再適用するように、システムを設定できます。この機能が特に役立つのは、ルール更新によるシステム提供の基本ポリシーの変更を許可する場合です。

- アクセス コントロール ポリシーを再適用すると、関連付けられた SSL、ネットワーク解析、ファイルのポリシーも再適用されますが、侵入ポリシーは再適用**されません**。また、変更された詳細設定のデフォルト値もすべて更新されます。ネットワーク解析のポリシーは個別に適用できないので、ネットワーク解析ポリシーのプリプロセッサ設定を更新するには、アクセス コントロール ポリシーの再適用が**必要です**。
- 侵入ポリシーを再適用すると、ルールおよびその他の変更された侵入ポリシーの設定も更新することができます。侵入ポリシーの再適用はアクセス コントロール ポリシーとあわせて行うこともできますが、その他のアクセス コントロールの設定は更新せずに、侵入ポリシーの適用で侵入ルールだけを更新することもできます。

ルールの更新にshared object ruleが含まれている場合に、インポートの後で初めてアクセス コントロールまたは侵入ポリシーを適用すると、トラフィック フローと処理が一時的に停止し、いくつかのパケットが検査されずに通過する場合があります。アクセス コントロールおよび侵入ポリシーの適用における、要件、その他の影響、および推奨事項などを含めた詳細については「アクセス コントロール ポリシーの適用（12-17 ページ）」を参照してください。

ルール更新のインポートの詳細については、次の解説を参照してください。

- ワンタイム ルール更新の使用（66-18 ページ）では、サポート サイトから 1 つのルール更新をインポートする方法について説明しています。
- 再帰的なルール更新の使用（66-20 ページ）では、Web インターフェイスで自動機能を使用して、サポート サイトからルールの更新をダウンロードおよびインストールする方法について説明しています。

- ローカル ルール ファイルのインポート（66-22 ページ）では、ローカル マシンで作成した標準テキスト ルール ファイルのコピーをインポートする方法について説明しています。
- ルール更新ログの表示（66-24 ページ）では、ルール更新のログについて説明しています。

ワンタイム ルール更新の使用

ライセンス： すべて

ワンタイム ルール更新では次の 2 つの方法を使用することができます。

- 手動によるワンタイム ルール更新の使用（66-18 ページ）では、サポート サイトからローカル マシンへ手動でルール更新をダウンロードし、それを手動でインストールする方法について説明しています。
- 自動によるワンタイム ルール更新の使用（66-19 ページ）では、Web インターフェイスで自動機能を使用し、サポート サイトで新しいルール更新を検索し、それをアップロードする方法について説明しています。

手動によるワンタイム ルール更新の使用

ライセンス： すべて

次の手順では、新しいルール更新を手動でインポートする方法について説明します。この手順は、Defense Centerがインターネットにアクセスできない場合に特に有用です。

手動でルール更新をインポートする方法：

アクセス： Admin

ステップ 1　インターネットにアクセスできるコンピュータから、次のサイトのいずれかへアクセスします。

- **Sourcefire:**（https://support.sourcefire.com/）
- **シスコ：**（http://www.cisco.com/cisco/web/support/index.html）

ステップ 2　[Download] をクリックし、[Rules] をクリックします。

ステップ 3　最新のルール更新へ移動します。

ルール更新は累積的です。現在インストールされているルールのバージョンに一致するルール更新、またはそれより前のバージョンのルール更新をインポートすることはできません。

ステップ 4　ダウンロードするルール更新ファイルをクリックし、そのファイルをコンピュータに保存します。

ステップ 5　アプライアンスの Web インターフェイスにログインします。

ステップ 6　[System] > [Updates] を選択し、[Rule Updates] タブを選択します。

[Rule Updates] ページが表示されます。

ヒント　または [Rule Editor] ページで [Import Rules] をクリックします（[Policies] > [Intrusion] > [Rule Editor] ）。

ステップ 7　オプションで [Delete All Local Rules] をクリックし、[OK] をクリックして、作成した、または削除されたフォルダにインポートしたすべてのユーザ定義ルールを移動します。詳細については、「カスタム ルールの削除（36-113 ページ）」を参照してください。

ステップ 8　[Rule Update or text rule file to upload and install] を選択し、[Choose File] をクリックしてナビゲートし、ルール更新ファイルを選択します。

ステップ 9　オプションで、更新の完了後にポリシーを管理対象デバイスに再適用します。

- [Reapply intrusion policies after the rule update import completes] を選択すると、侵入ポリシーが自動的に再適用されます。このオプションを選択するのは、その他のアクセス コントロールのユーザ設定は更新せずに、ルールおよびその他の変更された侵入ポリシーの設定を更新する場合だけです。このオプションの選択が**必要となる**のはアクセス コントロール ポリシーとあわせて侵入ポリシーを再適用する場合であり、そうしたケースではアクセス コントロール ポリシーを再適用しても完全には適用されません。
- [Reapply access control policies after the rule update import completes] を選択すると、アクセス コントロール ポリシーとその関連の SSL、ネットワーク解析、ファイルのポリシーも自動的に再適用されますが、侵入ポリシーは再適用されません。このオプションを選択すると、変更されたアクセス コントロールの詳細設定のデフォルト値もすべて更新されます。ネットワーク解析のポリシーは親となるアクセス コントロール ポリシーと個別には適用できないので、ネットワーク解析ポリシーのプリプロセッサ設定を更新するには、アクセス コントロール ポリシーの再適用が**必要です**。

ステップ 10　[Import] をクリックします。

システムはルール更新をインストールし、[Rule Update Log] 詳細ビューを表示します。「[Rule Update Import Log] 詳細ビューについて（66-27 ページ）」を参照してください。システムは、前のステップで指定したポリシーも適用します。「アクセス コントロール ポリシーの適用（12-17 ページ）」および「侵入ポリシーの適用（31-9 ページ）」を参照してください。

注　ルール更新のインストール中にエラー メッセージが表示された場合は、サポートに連絡してください。

自動によるワンタイム ルール更新の使用

ライセンス： すべて

次の手順では、サポート サイトに自動で接続して、新しいルール更新をインポートする方法について説明します。この手順は、アプライアンスがインターネットにアクセスできる場合のみ使用できます。

自動でルール更新をインポートする方法：

アクセス： Admin

ステップ 1　[System] > [Updates] を選択し、[Rule Updates] タブを選択します。

[Rule Updates] ページが表示されます。

ヒント　または [Rule Editor] ページで [Import Rules] をクリックします（[Policies] > [Intrusion] > [Rule Editor] ）。

ステップ 2　オプションで [Delete All Local Rules] をクリックし、[OK] をクリックして、作成した、または削除されたフォルダにインポートしたすべてのユーザ定義ルールを移動します。詳細については、「カスタム ルールの削除（36-113 ページ）」を参照してください。

ステップ 3　[Download new Rule Update from the Support Site] を選択します。

ステップ 4　オプションで、更新の完了後にポリシーを管理対象デバイスに再適用します。

- [Reapply intrusion policies after the rule update import completes] を選択すると、侵入ポリシーが自動的に再適用されます。このオプションを選択するのは、その他のアクセス コントロールのユーザ設定は更新せずに、ルールおよびその他の変更された侵入ポリシーの設定を更新する場合だけです。このオプションの選択が**必要となる**のはアクセス コントロール ポリシーとあわせて侵入ポリシーを再適用する場合であり、そうしたケースではアクセス コントロール ポリシーを再適用しても完全には適用されません。
- [Reapply access control policies after the rule update import completes] を選択すると、アクセス コントロール ポリシーとその関連の SSL、ネットワーク解析、ファイルのポリシーも自動的に再適用されますが、侵入ポリシーは再適用されません。このオプションを選択すると、変更されたアクセス コントロールの詳細設定のデフォルト値もすべて更新されます。ネットワーク解析のポリシーは親となるアクセス コントロール ポリシーと個別には適用できないので、ネットワーク解析ポリシーのプリプロセッサ設定を更新するには、アクセス コントロール ポリシーの再適用が**必要です**。

ステップ 5　[Import] をクリックします。

システムはルール更新をインストールし、[Rule Update Log] 詳細ビューを表示します。「[Rule Update Import Log] 詳細ビューについて（66-27 ページ）」を参照してください。システムは、前のステップで指定したポリシーも適用します。「アクセス コントロール ポリシーの適用（12-17 ページ）」および「侵入ポリシーの適用（31-9 ページ）」を参照してください。

注　ルール更新のインストール中にエラー メッセージが表示された場合は、サポートに連絡してください。

再帰的なルール更新の使用

ライセンス： すべて

[Rule Updates] ページを使用して、ルール更新を日次、週次、または月次ベースでインポートすることができます。展開に高可用性ペアのDefense Centerが含まれる場合は、プライマリ側だけに更新をインポートします。セカンダリのDefense Centerは、通常の同期プロセスの一環としてルールの更新を受け取ります。

ルール更新のインポートにおける適用可能なサブタスクは、ダウンロード、インストール、ベース ポリシーの更新、およびポリシーの再適用の順序で生じます。1 つのサブタスクが完了すると、次のサブタスクが開始されます。適用できるのは、再帰的なインポートが設定されているアプライアンスで以前に適用されたポリシーのみであることに注意してください。

再帰的なルール更新をスケジュールする方法：

アクセス： Admin

ステップ 1　[System] > [Updates] を選択し、[Rule Updates] タブを選択します。

[Rule Updates] ページが表示されます。

ヒント　または [Rule Editor] ページで [Import Rules] をクリックします（[Policies] > [Intrusion] > [Rule Editor] ）。

ステップ 2　オプションで [Delete All Local Rules] をクリックし、[OK] をクリックして、作成した、または削除されたフォルダにインポートしたすべてのユーザ定義ルールを移動します。詳細については、「カスタム ルールの削除（36-113 ページ）」を参照してください。

ステップ 3　[Enable Recurring Rule Update Imports] を選択します。

ページが拡張され、再帰的なインポートを設定するためのオプションが表示されます。[Recurring Rule Update Imports] セクション見出しの下に、インポート ステータスのメッセージが表示されます。設定を保存すると、再帰的なインポートが有効になります。

ヒント　再帰的なインポートを無効にするには、[Enable Recurring Rule Update Imports] チェック ボックスをオフにして [Save] をクリックします。

ステップ 4　[Import Frequency] フィールドで、ドロップダウン リストから [Daily]、[Weekly]、または [Monthly] を選択します。

週次または月次インポート間隔を選択した場合は、表示されるドロップダウン リストを使用して、ルールの更新をインポートする曜日または月の日を選択します。選択する内容をクリックするか、または最初の文字または数字を 1 回以上入力して、Enter を押すことで、再帰タスクのドロップダウン リストから選択できます。

ステップ 5　[Import Frequency] フィールドで、再帰的なルール更新のインポートを開始するタイミングを指定します。

ステップ 6　オプションで、更新の完了後にポリシーを管理対象デバイスに再適用します。

- [Reapply intrusion policies after the rule update import completes] を選択すると、侵入ポリシーが自動的に再適用されます。このオプションを選択するのは、その他のアクセス コントロールのユーザ設定は更新せずに、ルールおよびその他の変更された侵入ポリシーの設定を更新する場合だけです。このオプションの選択が**必要となる**のはアクセス コントロール ポリシーとあわせて侵入ポリシーを再適用する場合であり、そうしたケースではアクセス コントロール ポリシーを再適用しても完全には適用されません。
- [Reapply access control policies after the rule update import completes] を選択すると、アクセス コントロール ポリシーとその関連の SSL、ネットワーク解析、ファイルのポリシーも自動的に再適用されますが、侵入ポリシーは再適用されません。このオプションを選択すると、変更されたアクセス コントロールの詳細設定のデフォルト値もすべて更新されます。ネットワーク解析のポリシーは親となるアクセス コントロール ポリシーと個別には適用できないので、ネットワーク解析ポリシーのプリプロセッサ設定を更新するには、アクセス コントロール ポリシーの再適用が**必要です**。

ステップ 7　[Save] をクリックし、設定を使用した再帰的なルール更新のインポートを有効にします。

[Recurring Rule Update Imports] セクションの見出しの下のステータス メッセージが変わり、ルールの更新がまだ実行されていないことが示されます。スケジュールされた時間になるとシステムは、前のステップで指定したルール更新をインストールしてポリシーを適用します。「アクセス コントロール ポリシーの適用（12-17 ページ）」および「侵入ポリシーの適用（31-9 ページ）」を参照してください。

インポートの前、またはインポート中にログオフすることも、Web インターフェイスを使用して他のタスクを実行することもできます。インポート中にアクセスした場合は、[Rule Update Log] に赤いステータスのアイコン（ ）が表示され、[Rule Update Log] 詳細ビューでは表示された

メッセージを確認できます。ルールの更新のサイズと内容によっては、ステータス メッセージが表示されるまでに数分かかることがあります。詳細については、ルール更新ログの表示（66-24 ページ）を参照してください。

注　ルール更新のインストール中にエラー メッセージが表示された場合は、サポートに連絡してください。

ローカル ルール ファイルのインポート

ライセンス： すべて

ローカル ルールはカスタム標準テキスト ルールで、ユーザがローカル マシンから ASCII または UTF-8 エンコードのプレーン テキスト ファイルとしてインポートします。Snort ユーザ マニュアル（http://www.snort.org で入手可能）の指示に従って、ローカル ルールを作成することができます。

ローカル ルールのインポートについて、次の点に注意してください。

- テキスト ファイル名には英数字とスペースを使用できますが、下線（_）、ピリオド（.）、ダッシュ（-）以外の特殊記号は使用できません。
- ジェネレータ ID（GID）を指定する必要はありません。GID を指定する場合は、標準テキスト ルールに対しては GID 1、機密データ ルールに対しては 138 のみ指定できます。
- 初めてルールをインポートするときには、Snort ID（SID）またはリビジョン番号を指定**しないで**ください。これにより、削除されたルールを含む、他のルールの SID との競合が回避されます。

  システムはルールに対して、1000000 以上の次に使用できるカスタム ルール SID 、およびリビジョン番号 の 1 を自動的に割り当てます。
- 以前にインポートしたローカル ルールの更新バージョンをインポートする場合には、システムによって割り当てられた SID、および現在のリビジョン番号よりも大きいリビジョン番号を**含める必要があります**。

  現行のローカル ルールのリビジョン番号を表示するには、[Rule Editor] ページ（[Policies] > [Intrusion] > [Rule Editor]）を表示し、ローカル ルールのカテゴリをクリックしてフォルダを展開し、ルールの隣にある [Edit] をクリックします。
- システムによって割り当てられた SID、および現行のリビジョン番号よりも大きいリビジョン番号を使用してルールをインポートして削除したローカル ルールは、元に戻すことができます。ローカル ルールを削除すると、システムは自動的にリビジョン番号を増やすことに注意してください。これは、ローカル ルールを元に戻すための方法です。

  削除されたローカル ルールのリビジョン番号を表示するには、[Rule Editor] ページ（[Policies] > [Intrusion] > [Rule Editor]）を表示し、削除されたルール カテゴリをクリックしてフォルダを展開し、ルールの隣にある [Edit] をクリックします。
- 2147483647 よりも大きい SID を持つルールが含まれているルール ファイルはインポートできません。この場合、インポートが失敗します。
- 64 文字を超える送信元または宛先のポートのリストが含まれているルールをインポートすると、そのインポートは失敗します。

- システムは常に、ユーザがインポートするローカル ルールを無効なルール状態に設定します。これらを侵入ポリシーで使用するには、その前に手動でローカル ルールの状態を設定する必要があります。詳細については、「ルール状態の設定（32-22 ページ）」を参照してください。
- ファイル内のルールに、エスケープ文字が含まれていないことを確認する必要があります。
- ルール インポータでは、すべてのカスタム ルールを ASCII または UTF-8 エンコードでインポートする必要があります。
- インポートされたすべてのローカル ルールは、ローカル ルール カテゴリに自動的に保存されます。
- 削除されたすべてのローカル ルールは、ローカル ルール カテゴリから、削除されたルール カテゴリへ移動されます。
- システムは、単一のポンド文字（#）で始まるローカル ルールをインポートしますが、これらには削除のフラグが立てられます。
- また、二重のポンド文字（##）で始まるローカル ルールは無視し、インポートしません。
- Ciscoでは、SID の番号付けの問題を回避するために、高可用性ペアのプライマリ Defense Centerにローカル ルールをインポートすることを強くお勧めしています。
- 侵入ポリシーで、侵入イベントのしきい値機能と組み合わせて非推奨の `threshold` キーワードを使用しているローカル ルールをインポートして有効にすると、ポリシーの検証は失敗します。詳細については、「イベントしきい値の設定（32-25 ページ）」を参照してください。

ローカル ルール ファイルをインポートする方法：

アクセス： Admin

ステップ 1　[Policies] > [Intrusion] > [Rule Editor] の順に選択します。

[Rule Editor] ページが表示されます。

ステップ 2　[Import Rules] をクリックします。

[Import Rules] ページが表示されます。

ヒント　[System] > [Updates] を選択して、[Rule Updates] タブを選択することもできます。

ステップ 3　[Rule Update or text rule file to upload and install] を選択して [Browse] をクリックすると、ルール ファイルにナビゲートできます。この方法でアップロードされたすべてのルールは、ローカル ルール カテゴリに保存されることに注意してください。

ヒント　インポートできるのは、ASCII または UTF-8 エンコードのプレーン テキスト ファイル**だけ**です。

ステップ 4　[Import] をクリックします。

ルール ファイルがインポートされます。侵入ポリシーで、適切なルールが有効になっていることを確認してください。影響を受けるポリシーが次に適用されるまで、ルールはアクティブにはなりません。

注　管理対象デバイスは、侵入ポリシーを適用するまで、インスペクションに対して新しいルール セットを使用**しません**。手順については、アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

ルール更新ログの表示

ライセンス：すべて

Defense Centerは、ユーザがインポートする各ルール更新およびローカル ルール ファイルごとに 1 つのレコードを生成します。

各レコードにはタイム スタンプ、ファイルをインポートしたユーザ名、およびインポートが正常に終了したか失敗したかを示すステータス アイコンが含まれています。ユーザは、自分がインポートするすべてのルール更新およびローカル ルール ファイルのリストを管理する、リストからレコードを削除する、インポートしたすべてのルールおよびルール更新のコンポーネントについての詳細レコードにアクセスする、といったことができます。以下の表で、[Rule Update Log] のフィールドについて説明します。

表 66-2　[Rule Update Log] のアクション

目的	操作
テーブルのカラムの内容について詳細を参照する	詳細については、[Rule Update Log] 表について（66-25 ページ）を参照してください。
インポート ログからインポート ファイル レコード（ファイルに含まれているすべてのオブジェクトについて削除されたレコードも含めて）を削除する	インポート ファイルでファイル名の隣にある削除アイコン（ ）をクリックします。 **注**　ログからファイルを削除しても、インポート ファイルにインポートされているオブジェクトはいずれも削除されませんが、インポート ログ レコードのみは削除されます。
ルール更新またはローカル ルール ファイルにインポートされている各オブジェクトの詳細を表示する	インポート ファイルでファイル名の隣にある表示アイコン（ ）をクリックします。

詳細については、次の項を参照してください。

- [Rule Update Log] 表について（66-25 ページ）では、インポートするルール更新およびローカル ルール ファイルのリスト内のフィールドについて説明します。
- [Rule Update Import Log] の詳細の表示（66-25 ページ）では、ルール更新またはローカル ルール ファイルにインポートされた各オブジェクトの詳細レコードについて説明します。
- [Rule Update Import Log] 詳細ビューについて（66-27 ページ）では、[Rule Update Log] 詳細ビューの各フィールドについて説明します。
- [Rule Update Import Log] の検索（66-28 ページ）では、インポート ログで検索基準と一致する特定のレコード、またはすべてのレコードを検索する方法について説明します。

[Rule Update Log] を表示する方法：

アクセス：Admin

ステップ 1　[System] > [Updates] を選択し、[Rule Updates] タブを選択します。

[Rule Updates] ページが表示されます。

ヒント　または [Rule Editor] ページで [Import Rules] をクリックします。ここには、[Policies] > [Intrusion] > [Rule Editor] を選択してアクセスすることができます。

ステップ 2　[Rule Update Log] をクリックします。

[Rule Update Log] ページが表示されます。このページには、インポートされた各ルール更新とローカル ルール ファイルが示されています。

[Rule Update Log] 表について

ライセンス： すべて

次の表で、ユーザがインポートするルール更新およびローカル ルール ファイルのリストのフィールドについて説明します。

表 66-3　[Rule Update Log] のフィールド

フィールド	説明
概要	インポート ファイルの名前。インポートが失敗した場合は、ファイル名の下に、失敗した理由の簡単な説明が表示されます。
時刻	インポートが開始された日時。
ユーザ ID	インポートをトリガーとして使用したユーザ名。
Status（ステータス）	インポートの状態を表します • 正常終了（） • 失敗した、または実行中（  ） **ヒント**　インポート中には [Rule Update Log] ページで、正常終了しなかった、または完了していないことを示す赤いステータス アイコンが表示され、インポートが正常終了した場合のみこれが緑色のアイコンに変わります。

ルール更新またはファイル名の隣にある表示アイコン（  ）をクリックして、ルール更新またはローカル ルール ファイルの [Rule Update Log] 詳細ページを表示するか、または削除アイコン（  ）をクリックして、ファイル レコード、およびファイルと一緒にインポートされたすべての詳細オブジェクト レコードを削除します。

ヒント　ルール更新のインポートの進行中に示される、インポートの詳細を表示することができます。

[Rule Update Import Log] の詳細の表示

ライセンス： すべて

[Rule Update Import Log] 詳細ビューには、ルール更新またはローカル ルール ファイルにインポートされた各オブジェクトの詳細レコードが表示されます。表示されるレコードのうち、自分のニーズに合う情報のみを含むカスタム ワークフローまたはレポートを作成することもできます。

次の表は、[Rule Update Import Log] 詳細ビューのワークフロー ページで実行できる特定のアクションについて説明します。

表 66-4　[Rule Update Import Log] 詳細ビューのアクション

目的	操作
テーブルのカラムの内容について詳細を参照する	詳細については、[Rule Update Import Log] 詳細ビューについて (66-27 ページ) を参照してください。
現行のワークフロー ページ上でレコードをソートおよび制限する	詳細については、ドリルダウン ワークフロー ページのソート (58-38 ページ) を参照してください。
一時的に他のワークフローを使用する	[(switch workflows)] をクリックします。ワークフローの選択については、ワークフローの選択 (58-18 ページ) を参照してください。カスタム ワークフローの作成については、カスタム ワークフローの作成 (58-43 ページ) を参照してください。
すぐに再表示できるように、現在のページをブックマークする	[Bookmark This Page] をクリックします。詳細については、ブックマークの使用 (58-41 ページ) を参照してください。
ブックマークの管理ページへ移動する	[View Bookmarks] をクリックします。詳細については、ブックマークの使用 (58-41 ページ) を参照してください。
現在のビューのデータに基づいてレポートを生成する	[Report Designer] をクリックします。詳細については、イベント ビューからのレポート テンプレートの作成 (57-10 ページ) を参照してください。
[Rule Update Import Log] データベース全体で、ルール更新のインポート レコードを検索する	[Search] をクリックします。詳細については、[Rule Update Import Log] の検索 (66-28 ページ) を参照してください。
現行の制約が設定されている検索ページを開く	[Search Constraints] の隣にある [Edit Search] または [Save Search] を選択します。詳細については、テーブル ビューおよびドリルダウン ページの機能の表を参照してください。

[Rule Update Import Log] 詳細ビューを表示する方法:

アクセス: Admin

ステップ 1　[System] > [Updates] を選択し、[Rule Updates] タブを選択します。

[Rule Updates] ページが表示されます。

ヒント　または [Rule Editor] ページで [Import Rules] をクリックします。ここには、[Policies] > [Intrusion] > [Rule Editor] を選択してアクセスすることができます。

ステップ 2　[Rule Update Log] をクリックします。

[Rule Update Log] ページが表示されます。

ステップ 3　表示する詳細レコードが含まれているファイルの隣にある表示アイコン ( ) をクリックします。

詳細レコードのテーブル ビューが表示されます。

[Rule Update Import Log] 詳細ビューについて

ライセンス：すべて

ルール更新またはローカル ルール ファイルにインポートされた各オブジェクトの詳細レコードを表示することができます。以下の表で、[Rule Update Log] 詳細ビューのフィールドについて説明します。

表 66-5　[Rule Update Import Log] 詳細ビューのフィールド

フィールド	説明
時刻	インポートが開始された日時。
名前	インポートされたオブジェクトの名前。ルールの場合はルールの [Message] フィールドに対応した名前で、ルール更新コンポーネントの場合はコンポーネント名です。
タイプ	インポートされたオブジェクトのタイプで、有効な値は次のいずれかです。 • [rule update component]（ルール パックまたはポリシー パックなどの、インポートされたコンポーネント） • [rule]（新しいルールまたは更新されたルールの場合。バージョン 5.0.1 では、廃止された [update] 値の代わりにこの値が使用されます）。 • [policy apply]（インポートで [Reapply intrusion policies after the Rule Update import completes] オプションが有効だった場合）
Action	オブジェクト タイプについて、次のいずれかが発生していることを示します。 • [new]（ルールで、このアプライアンスにルールが最初に格納された場合） • [changed]（ルール更新コンポーネントまたはルールで、ルール更新コンポーネントが変更された場合、ルールのリビジョン番号が大きく、GID と SID が同じだった場合） • [collision]（ルール更新コンポーネントまたはルールで、アプライアンス上の既存のコンポーネントまたはルールとリビジョンの競合によりインポートがスキップされた場合） • [deleted]（ルールで、ルール更新からルールが削除された場合） • [enabled]（ルール更新の編集で、プリプロセッサ、ルール、または他の機能が、Cisco によって提供されるデフォルト ポリシーで有効になっていた場合） • [disabled]（ルールで、Ciscoによって提供されるデフォルト ポリシーでルールが無効になっていた場合） • [drop]（ルールで、Ciscoによって提供されるデフォルト ポリシーで、ルールが [Drop] または [Generate Events] に設定されていた場合） • [error]（ルール更新またはローカル ルール ファイルで、インポートが失敗した場合） • [apply]（インポートで [Reapply intrusion policies after the Rule Update import completes] オプションが有効だった場合）
Default Action	ルールの更新によって定義されているデフォルトのアクション。インポートされたオブジェクトのタイプが [rule] の場合、デフォルトのアクションは [Pass]、[Alert]、または [Drop] になります。インポートされた他のすべてのオブジェクト タイプには、デフォルトのアクションはありません。
GID	ルールのジェネレータ ID。例：1（標準テキスト ルール）や 3（shared object ruleなど）。詳細については、「表 41-7（41-42 ページ）」を参照してください。
SID	ルールの SID。
Rev	ルールのリビジョン番号。

表 66-5　[Rule Update Import Log] 詳細ビューのフィールド（続き）

フィールド	説明
ポリシー（Policy）	インポートされたルールの場合、このフィールドには [All] が表示されます。これは、インポートされたルールがデフォルトのすべての侵入ポリシーに含まれていたことを意味します。インポートされた他のタイプのオブジェクトについては、このフィールドは空白です。
Details	コンポーネントまたはルールに対する一意の文字列。ルール、GID、SID、および変更されたルールの以前のリビジョン番号については、`previously (GID:SID:Rev)` のように表示されます。変更されていないルールについては、このフィールドは空白です。
Count	各レコードのカウント（1）。テーブルが制限されており、[Rule Update Log] 詳細ビューがデフォルトでルール更新レコードに制限されている場合は、テーブル ビューに [Count] フィールドが表示されます。

[Rule Update Import Log] の検索

ライセンス：すべて

注　ベータ ユーザ：この機能については、ドキュメントの最終版で完全に説明します。

インポート ログで検索基準と一致する特定のレコード、またはすべてのレコードを検索することができます。カスタマイズされた検索を作成し、後で再利用できるように保存しておくこともできます。

ヒント　1 つのインポート ファイルのレコードのみが表示されている [Rule Update Import Log] 詳細ビューからツールバーの [Search] をクリックして検索を開始した場合でも、[Rule Update Import Log] データベースの全体が検索されます。検索の対象とするすべてのオブジェクトが含まれるように、時間制限が設定されていることを確認します。詳細については、「検索での時間制約の指定（60-5 ページ）」を参照してください。

次の表で、ユーザが使用できる検索条件について説明します。レコード検索では大文字/小文字が区別されないことに注意してください。たとえば、`RULE` または `rule` の検索では同じ結果が得られます。

表 66-6　[Rule Update Import Log] の検索基準

検索フィールド	説明	例
時刻	レコードが生成された日時を指定します。時間入力の構文については、検索での時間制約の指定（60-5 ページ）を参照してください。	`> 2006-01-15 13:30:00` のように指定すると、2006 年 1 月 15 日午後 1:30 より後にインポートされたすべてのルール レコードが返されます。
名前	ルールの [Message] フィールドのすべてまたは一部の内容を指定します。このフィールドでは、ワイルドカード文字としてアスタリスク（*）を使用できます。	`*dhcp*` のように指定すると、[Message] フィールドで DHCP という文字列が含まれるすべてのルール レコードが返されます。

表 66-6　[Rule Update Import Log] の検索基準（続き）

検索フィールド	説明	例
タイプ	レコードのタイプを指定します。[rule update component]、[rule]、または [policy apply] を使用できます。 バージョン 5.0.1 より前にインポートされたルールの検索では、検索で [update] 検索値を使用できることに注意してください。	[update] を指定すると、ルール パックやポリシー パックなど、インポートされたルール更新コンポーネントが返されます。[rule] を指定すると、新しいルールも含めてルールの更新が返されます。[policy apply] を指定すると、更新の後に侵入ポリシーが自動的に再適用されたルール更新の情報が、表形式の行で返されます。
Action	表示するオブジェクトに対するアクションを指定します。指定できるアクションについては、[Rule Update Import Log] 詳細ビューのフィールドの表を参照してください。	タイプが [rule]、[new] の場合は、アプライアンスに最初にインポートされたすべてのルールが返されます。
GID	ルールのジェネレータ ID を指定します。	3 を指定すると、すべてのshared object ruleが返されます。
SID	ルールのシグネチャ ID または SID の範囲を指定します。	923 と指定すると、SID 923 を持つルールのレコードが返されます。
Rev	ルールのリビジョン番号を指定します。	3 を指定すると、リビジョン番号 3 のルールが返されます。
ポリシー（Policy）	ルールがインポートされたデフォルト ポリシーを指定します。	[All] を指定すると、すべてのデフォルト ポリシーにインポートされたルールが返されます。
Rule Update	Rule Update ファイルの名前を指定します。	[filename] と指定すると、指定されたインポート ファイルのすべてのレコードが返されます。
Details	インポートされたオブジェクトの詳細を指定します。	previously* と指定すると、変更されたすべてのルールのレコードが返されます。

保存されている検索をロードおよび削除する方法など、検索の詳細については、イベントの検索（60-1 ページ）を参照してください。

[Rule Update Import Log] を検索する方法：

アクセス： Admin/Intrusion Admin

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　[Table] ドロップダウン リストから、[Rule Update Import Log] を選択します。

ページが適切な制約を使用してリロードされます。

ヒント　[Rule Update Log] 詳細ビューで [Search] をクリックすることもできます。[Rule Update Import Log] の詳細の表示（66-25 ページ）を参照してください。

ステップ 3　オプションで、検索を保存するには、[Name] フィールドに検索の名前を入力します。

名前を入力しない場合は、検索が保存されるときに Web インターフェイスで自動的に名前が生成されます。

ステップ 4　表 [Rule Update Import Log] の検索基準 に記載されているように、該当するフィールドに検索基準を入力します。複数の条件を入力すると、検索によって、すべての基準に一致するレコードが返されます。

ステップ 5　他のユーザがアクセスできるように検索を保存する場合、[Save As Private] チェック ボックスをクリアします。それ以外の場合は、このチェック ボックスを選択したままにし、検索をプライベートとして保存します。

カスタム ユーザ ロールのデータの制限として検索を使用する場合は、**必ず**プライベート検索として保存する必要があります。

ステップ 6　次の選択肢があります。

- 検索を開始するには、[Search] ボタンをクリックします。

  デフォルトの [Rule Update Import Log] 詳細ビューのワークフローに検索結果が示されます。カスタム ワークフローなどの別のワークフローを使用するには、[(switch workflows)] をクリックします。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。
- 既存の検索を変更しており、その変更を保存する場合は、[Save] をクリックします。
- 検索基準を保存する場合は、[Save as New Search] をクリックします。検索が保存され（[Save As Private] を選択した場合はユーザ アカウントに関連付けられ）、後で実行できます。

地理情報データベースについて

ライセンス： FireSIGHT

サポートされる防御センター： すべて（DC500 を除く）

Cisco地理情報データベース（GeoDB）は、ルート可能な IP アドレスに関連する地理情報データ（国、都市、緯度と経度の座標など）、および接続関係のデータ（インターネット サービス プロバイダー、ドメイン名、接続タイプなど）のデータベースです。システムで、検出された IP アドレスと一致する GeoDB 情報が検出された場合は、その IP アドレスに関連付けられている地理情報を表示することができます。国や大陸以外の地理情報の詳細を表示するには、システムに GeoDB をインストールする必要があります。Ciscoでは、GeoDB の定期的な更新を提供しています。

GeoDB を更新するには、Defense Centerで [Geolocation Updates] ページ（[System] > [Updates] > [Geolocation Updates]）を使用します。サポートまたは自身のアプライアンスから取得した GeoDB の更新をアップロードすると、このページに表示されます。

GeoDB の更新にかかる時間はアプライアンスによって異なります。インストールには通常、30～40 分かかります。GeoDB の更新は他のシステムの機能（実行中の地理情報の収集など）を中断することはありませんが、更新が完了するまでシステムのリソースを消費します。更新を計画する場合には、この点について考慮してください。

この項では、手動による GeoDB 更新を計画および実行する方法について説明します。自動更新機能を利用して GeoDB の更新をスケジュールすることもできます。詳細については、位置情報データベースの更新の自動化（62-10 ページ）を参照してください。地理情報の詳細については、地理情報の使用（58-23 ページ）を参照してください。

地理情報データベースを更新する方法:

アクセス: Admin

ステップ 1　[System] > [Updates] を選択します。

[Product Updates] ページが表示されます。

ステップ 2　[Geolocation Updates] タブをクリックします。

[Geolocation Updates] ページが表示されます。

ステップ 3　更新をDefense Centerへアップロードします。

- Defense Centerがインターネットにアクセスできる場合は、[Download and install geolocation update from the Support Site] をクリックして、以下のサポート サイトのいずれかで最新の更新を確認します。
  - **Sourcefire:**（https://support.sourcefire.com/）
  - **シスコ:**（http://www.cisco.com/cisco/web/support/index.html）
- Defense Centerがインターネットにアクセスできない場合は、以下のサポート サイトのいずれかから更新を手動でダウンロードして、[Upload and install geolocation update] をクリックします。更新を参照して、[Import] をクリックします。
  - **Sourcefire:**（https://support.sourcefire.com/）
  - **シスコ:**（http://www.cisco.com/cisco/web/support/index.html）

注　手動で、または [Geolocation Updates] ページで [Download and install geolocation update from the Support Site] をクリックして、サポート サイトから更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、ファイルが破損することがあります。

更新プロセスが開始されます。更新のインストールには、平均で 30～40 分かかります。これは、アプライアンスのハードウェアによって異なります。タスク キュー（[System] > [Monitoring] > [Task Status]）で更新の進捗を監視することができます。

ステップ 4　更新が終了したら、[Geolocation Updates] ページに戻るか、[Help] > [About] を選択して、GeoDB のビルド番号が、インストールした更新と一致していることを確認します。

GeoDB を更新すると、GeoDB の以前のバージョンが上書きされ、すぐに有効になります。GeoDB を更新すると、Defense Centerにより、管理対象デバイスが自動的に更新されます。展開全体で GeoDB の更新が有効になるには数分かかることがありますが、更新した後にアクセス コントロール ポリシーを再適用する必要はありません。

CHAPTER 67

システムのモニタリング

FireSIGHT システムは、日常のシステム管理をサポートする多くの便利なモニタリング機能を、単一のページ上で提供します。たとえば、[Host Statistics] ページでは、基本的なホスト統計情報および侵入イベント情報に加え、当日の [Data Correlator] やネットワーク検出プロセスを監視できます。また、Defense Centerまたは管理対象デバイスで現在実行されているすべてのプロセスの概要と詳細情報を監視できます。以下の項では、システムに備わっているモニタリング機能について詳しく説明します。

- ホスト統計情報の表示（67-2 ページ）では、次のようなホスト情報の表示方法について説明します。
- システム稼働時間
- ディスクおよびメモリの使用状況
- Data Correlator 統計
- システム プロセス
- 侵入イベント情報
- Defense Centerで、ヘルス モニタを使用して、ディスク使用状況を監視し、ディスク容量不足の状態をアラートすることもできます。詳細については、ヘルス モニタリングについて（68-2 ページ）を参照してください。
- システム ステータスとディスク領域使用率の監視（67-4 ページ）では、基本的なイベントおよびディスク パーティションの情報を表示する方法について説明します。
- システム プロセス ステータスの表示（67-5 ページ）では、基本プロセスの状態を表示する方法について説明します。
- 実行中のプロセスについて（67-6 ページ）では、アプライアンスで実行する基本システム プロセスについて説明します。

[Overview] > [Summary] にあるオプションを使用して、侵入イベントおよび検出イベントの統計情報を表示およびグラフ化することができます。詳細については、以下を参照してください。

- 侵入イベントの統計の表示（41-2 ページ）
- 侵入イベント グラフの表示（41-9 ページ）
- ディスカバリ イベントの統計情報の表示（50-2 ページ）
- ディスカバリのパフォーマンス グラフの表示（50-6 ページ）

ホスト統計情報の表示

ライセンス： すべて

[Statistics] ページには、次の内容の現在のステータスが表示されます。

- 一般的なホスト統計情報。詳細については、ホスト統計情報の表を参照してください
- Data Correlator の統計情報（Defense Centerのみ、FireSIGHT が必要）。詳細については、Data Correlator プロセスの統計情報の表を参照してください
- 侵入イベント情報（Protection が必要）。詳細については、侵入イベントの情報の表を参照してください

次の表に、[Statistics] ページにリストされているホスト統計情報を示します。

表 67-1　ホスト統計情報

カテゴリ	説明
時刻	システムの現在の時刻。
Uptime	システムが前回起動されてから経過した日数（該当する場合）、時間数、および分数。
Memory Usage	使用中のシステム メモリの割合。
Load Average	直前の 1 分間、5 分間、15 分間の CPU キュー内の平均プロセス数。
Disk Usage	使用中のディスクの割合。詳細なホスト統計情報を表示するには、矢印をクリックします。詳細については、「システム ステータスとディスク領域使用率の監視（67-4 ページ）」を参照してください。
プロセス	システムで実行されているプロセスの概要。詳細については、「システム プロセス ステータスの表示（67-5 ページ）」を参照してください。

FireSIGHT システムの展開に FireSIGHT のライセンスを使用したDefense Centerが含まれる場合、当日の [Data Correlator] やネットワーク検出プロセスも表示できます。管理対象デバイスがデータの取得、復号化、および分析を実行する際に、ネットワーク検出プロセスはデータをフィンガープリントおよび脆弱性データベースと関連付けてから、Defense Centerで実行中の Data Correlator で処理されるバイナリ ファイルを生成します。Data Correlator はバイナリ ファイルの情報を分析し、イベントを生成し、検出ネットワーク マップを作成します。

ネットワーク検出と Data Correlator に表示される統計情報は、デバイスごとに 0:00 から 23:59 までの間に収集された統計情報を使用した、当日の平均です。

次の表に、Data Correlator プロセスに表示される統計情報を示します。

表 67-2　Data Correlator プロセスの統計情報

カテゴリ	説明
Events/Sec	Data Correlator が受信し処理する検出イベントの 1 秒当たりの数
Connections/Sec	Data Correlator が受信し処理する接続の 1 秒当たりの数
CPU Usage — User (%)	当日のユーザ プロセスで使用される CPU 時間の平均割合
CPU Usage — System (%)	当日のシステム プロセスで使用される CPU 時間の平均割合

表 67-2　Data Correlator プロセスの統計情報（続き）

カテゴリ	説明
VmSize（KB）	当日の Data Correlator に割り当てられたメモリの平均サイズ（キロバイト単位）
VmRSS（KB）	当日の Data Correlator で使用されるメモリの平均量（キロバイト単位）

管理対象デバイスおよびデバイスを管理するDefense Centerでは、前回の侵入イベントの日時、過去 1 時間および過去 1 日に発生したイベントの合計数、およびデータベース内のイベントの合計数を表示することもできます。

注　[Statistics] ページの [Intrusion Event Information] セクションにある情報は、Defense Centerに送信された侵入イベントではなく、管理対象デバイスに保存されている侵入イベントに基づいています。侵入イベントがローカルで保存されないようにデバイスを管理する場合、このページには侵入イベントの情報は表示されません。これは、イベントをローカルで保存できない管理対象デバイスについても同様です。

次の表に、[Statistics] ページの [Intrusion Event Information] セクションに表示される統計情報を示します。

表 67-3　侵入イベントの情報

統計	説明
Last Alert Was	前回のイベントが発生した日時
Total Events Last Hour	過去 1 時間に発生したイベントの合計数
Total Events Last Day	過去 24 時間に発生したイベントの合計数
Total Events in Database	イベント データベース内のイベントの合計数

[Statistics] ページを表示する方法：

アクセス：Admin/Maint

ステップ 1　[System] > [Monitoring] > [Statistics] を選択します。

[Statistics] ページが表示されます。

ステップ 2　Defense Centerで、管理対象デバイスの統計情報をリストすることもできます。[Select Device(s)] ボックスから、[Select Devices] をクリックします。Shift キーまたは Ctrl キーを使用して、複数のデバイスを同時に選択することができます。

[Statistics] ページは、選択したデバイスの統計情報で更新されます。

システム ステータスとディスク領域使用率の監視

ライセンス： すべて

[Statistics] ページの [Disk Usage] セクションは、カテゴリ別およびパーティション ステータス別に、ディスク使用率のクイック概要を示します。マルウェア ストレージ パックがデバイスにインストールされている場合、そのパーティション ステータスも確認できます。このページを定期的に監視して、システム プロセスおよびデータベースで十分なディスク領域が使用可能であることを確認できます。

ヒント Defense Centerで、ヘルス モニタを使用して、ディスク使用状況を監視し、ディスク容量不足の状態をアラートすることもできます。詳細については、ヘルス モニタリングについて（68-2 ページ）を参照してください。

ディスク使用量情報にアクセスする方法：

アクセス： Admin/Maint

ステップ 1 [System] > [Monitoring] > [Statistics] を選択します。

[Statistics] ページが表示されます。

ステップ 2 [By Category] 積み上げ横棒で、ディスク使用率カテゴリの上にポインタを移動すると、以下が（順番に）表示されます。

- そのカテゴリが使用する使用可能なディスク領域の割合
- ディスク上の実際のストレージ領域
- そのカテゴリで使用可能なディスク容量の合計

ディスク使用量カテゴリの詳細については、Disk Usage ウィジェットについて（55-29 ページ）を参照してください。

ステップ 3 展開するには、[Total] の横にある下矢印をクリックします。

[Disk Usage] セクションが展開され、パーティションの使用状況が表示されます。マルウェア ストレージ・パックがインストールされている場合は、`/var/storage` パーティションの使用状況も表示されます。

複数の管理対象デバイスが展開に含まれる場合、特定のデバイスによってディスク使用状況のデータを制約することもできます。

Defense Centerで、特定のデバイスのディスク使用状況の情報を表示するには、次の手順に従います。

アクセス： Admin/Maint

ステップ 1 [Select Device(s)] ボックスからデバイス名を選択し、[Select Devices] をクリックします。

ページがリロードされ、選択した各デバイスのホスト統計情報が表示されます。

ステップ 2 展開するには、[Disk Usage] の横にある下矢印をクリックします。

[Disk Usage] セクションが展開されます。

システム プロセス ステータスの表示

ライセンス: すべて

[Host Statistics] ページの [Processes] セクションで、アプライアンスで現在実行中のプロセスを表示できます。これは、一般的なプロセス情報と、実行中の各プロセスに固有の情報を提供します。Defense Centerでデバイスを管理している場合、Defense Centerの Web インターフェイスを使用して、管理対象デバイスのプロセス ステータスを表示することができます。

次の表に、プロセス リストに表示される各列を示します。

表 67-4　プロセス ステータス

カラム	説明
Pid	プロセス ID 番号
[Username]	プロセスを実行しているユーザまたはグループの名前
Pri	プロセスの優先度
Nice	*nice* 値。プロセスのスケジューリング優先度を示す値です。値は 20（最も高い優先度）から 19（最も低い優先度）までの範囲になります
サイズ	プロセスで使用されるメモリ サイズ（値の後ろにメガバイトを表す m がない場合はキロバイト単位）
Res	メモリ内の常駐ページング ファイルの量（値の後ろにメガバイトを表す m がない場合はキロバイト単位）
状態	プロセスの状態: • D - プロセスが中断不能スリープ状態（通常は入出力）にある • N - プロセスの nice 値が正の値 • R - プロセスが実行可能である（実行するキュー上で） • S - プロセスがスリープ モードにある • T - プロセスがトレースまたは停止されている • W - プロセスがページングしている • X - プロセスがデッド状態である • Z - プロセスが機能していない • < - プロセスの nice 値が負の値
時刻	プロセスが実行されている時間（時間 : 分 : 秒）
Cpu	プロセスが使用している CPU の割合
コマンド	プロセスの実行可能ファイル名

プロセス リストを展開する方法:

アクセス: Admin/Maint

ステップ 1　[System] > [Monitoring] > [Statistics] を選択します。

[Statistics] ページが表示されます。

ステップ 2　Defense Centerで、プロセス統計を表示するデバイスを [Select Device(s)] ボックスから選択し、[Select Devices] をクリックします。

ステップ 3　[Processes] の横にある下矢印をクリックします。

プロセス リストが展開され、実行中のタスクの数やタイプ、現在の時刻、現在のシステム稼働時間、システムの負荷平均、CPU、メモリ、およびスワップ情報などの、一般的なプロセス ステータス情報と、実行中の各プロセスに関する固有の情報がリストされます。

[Cpu(s)] は、以下の CPU 使用状況情報をリストします。

- ユーザ プロセスの使用状況の割合
- システム プロセスの使用状況の割合
- nice 使用状況の割合（高い優先度を示す、負の nice 値を持つプロセスの CPU 使用状況）

  nice 値は、システム プロセスのスケジュールされた優先度を示しており、20（最も高い優先度）から 19（最も低い優先度）の範囲の値になります。
- アイドル状態の使用状況の割合

[Mem] は、以下のメモリ使用状況情報をリストします。

- メモリ内の合計キロバイト数
- メモリ内の使用キロバイト数の合計
- メモリ内の空きキロバイト数の合計
- メモリ内のバッファに書き出されたキロバイト数の合計

[Swap] は、以下のスワップ使用状況情報をリストします。

- スワップ内の合計キロバイト数
- スワップ内の使用キロバイト数の合計
- スワップ内の空きキロバイト数の合計
- スワップ内のキャッシュされたキロバイト数の合計

注　アプライアンスで実行されるプロセスのタイプの詳細については、実行中のプロセスについて（67-6 ページ）を参照してください。

プロセス リストを折りたたむには、次の手順に従います。

アクセス： Admin/Maint

ステップ 1　[Processes] の横にある上矢印をクリックします。

プロセス リストが折りたたまれます。

実行中のプロセスについて

ライセンス： すべて

アプライアンスで実行されるプロセスには、デーモンと実行可能ファイルの 2 種類があります。デーモンは常に実行され、実行可能ファイルは必要に応じて実行されます。

詳細については、次の項を参照してください。

- システム デーモンについて（67-7 ページ）
- 実行可能ファイルおよびシステム ユーティリティについて（67-8 ページ）

システム デーモンについて

ライセンス： すべて

デーモンは、アプライアンスで継続的に実行されます。これにより、サービスが使用可能になり、必要に応じてプロセスが生成されるようになります。次の表では、[Process Status] ページに表示されるデーモンをリストし、その機能について簡単に説明します。

注　次の表は、アプライアンスで実行される可能性があるすべてのプロセスの包括的なリストではありません。

表 67-5　システム デーモン

デーモン	説明
crond	スケジュールされたコマンド（cron ジョブ）の実行を管理します
dhclient	ダイナミック ホスト IP アドレッシングを管理します
fpcollect	クライアントとサーバのフィンガープリントの収集を管理します
httpd	HTTP（Apache Web サーバ）プロセスを管理します
httpsd	HTTPS（SSL を使用した Apache Web サーバ）サービスを管理し、SSL および有効な証明書の認証が機能しているかチェックし、アプライアンスへの安全な Web アクセスを提供するためにバックグラウンドで実行します。
keventd	Linux カーネルのイベント通知メッセージを管理します
klogd	Linux カーネル メッセージのインターセプションおよびロギングを管理します
kswapd	Linux カーネルのスワップ メモリを管理します
kupdated	ディスクの同期を実行する、Linux カーネルの更新プロセスを管理します
mysqld	FireSIGHT システム データベース プロセスを管理します
ntpd	Network Time Protocol（NTP）プロセスを管理します
pm	すべての Cisco プロセスを管理し、必要なプロセスを始動し、予期せずに失敗したプロセスをすべて再始動します
reportd	レポートを管理します
safe_mysqld	データベースのセーフ モード運用を管理し、エラーが発生した場合にはデータベース デーモンを再始動し、ランタイム情報をファイルに記録します
SFDataCorrelator	データ転送を管理します
sfestreamer（Defense Centerのみ）	Event Streamer を使用するサード パーティ製クライアント アプリケーションへの接続を管理します。
sfmgr	アプライアンスへの sftunnel 接続を使用して、リモートでアプライアンスを管理および設定するための RPC サービスを提供します

表 67-5　システム デーモン（続き）

デーモン	説明
SFRemediateD（Defense Centerのみ、FireSIGHT が必要）	修復応答を管理します
sftimeserviced（Defense Centerのみ）	時間同期メッセージを管理対象デバイスに転送します
sfmbservice（Protection が必要）	アプライアンスへの sftunnel 接続を使用して、リモート アプライアンスで実行されている sfmb メッセージ ブローカ プロセスへのアクセスを提供します。現在ヘルス モニタリングによってのみ使用されており、管理対象デバイスからDefense Centerに、または高可用性環境ではDefense Center間でヘルス イベントおよびアラートを送信します
sftroughd	着信ソケットで接続をリッスンしてから、正しい実行可能ファイル（通常は、Cisco メッセージ ブローカ sfmb）を呼び出して要求を処理します
sftunnel	リモート アプライアンスとの通信を必要とするすべてのプロセスに対し、安全な通信チャネルを提供します。
sshd	Secure Shell (SSH) プロセスを管理し、アプライアンスへの SSH アクセスを提供するためにバックグラウンドで実行します
syslogd	システム ロギング（syslog）プロセスを管理します

実行可能ファイルおよびシステム ユーティリティについて

ライセンス: すべて

システム上には、他のプロセスまたはユーザ操作によって実行される実行可能ファイルが数多く存在します。次の表に、[Process Status] ページで表示される実行可能ファイルについて説明します。

表 67-6　システムの実行可能ファイルおよびユーティリティ

実行可能	説明
awk	awk プログラミング言語で作成されたプログラムを実行するユーティリティ
bash	GNU Bourne-Again シェル
cat	ファイルを読み取り、コンテンツを標準出力に書き込むユーティリティ
chown	ユーザーおよびグループのファイル権限を変更するユーティリティ
chsh	デフォルトのログイン シェルを変更するユーティリティ
SFDataCorrelator（Defense Centerのみ、FireSIGHT が必要）	FireSIGHT で作成されるバイナリ ファイルを分析し、イベント、接続データ、およびネットワーク マップを生成します。
cp	ファイルをコピーするユーティリティ
df	アプライアンスの空き領域の量をリストするユーティリティ
echo	コンテンツを標準出力に書き込むユーティリティ

表 67-6　システムの実行可能ファイルおよびユーティリティ（続き）

実行可能	説明
egrep	指定された入力を、ファイルおよびフォルダで検索するユーティリティ。標準 grep でサポートされていない正規表現の拡張セットをサポートします
find	指定された入力のディレクトリを再帰的に検索するユーティリティ
grep	指定された入力をファイルとディレクトリで検索するユーティリティ
halt	サーバを停止するユーティリティ
httpsdctl	セキュアな Apache Web プロセスを処理する
hwclock	ハードウェア クロックへのアクセスを許可するユーティリティ
ifconfig	ネットワーク構成実行可能ファイルを示します。MAC アドレスが常に一定になるようにします
iptables	[Access Configuration] ページに加えられた変更に基づいてアクセス制限を処理します。アクセス権の設定の詳細については、アプライアンスのアクセス リストの設定（63-9 ページ）を参照してください。
iptables-restore	iptables ファイルの復元を処理します
iptables-save	iptables に対する保存済みの変更を処理します
kill	セッションおよびプロセスを終了するために使用できるユーティリティ
killall	すべてのセッションおよびプロセスを終了するために使用できるユーティリティ
ksh	Korn シェルのパブリック ドメイン バージョン
logger	コマンドラインから syslog デーモンにアクセスする方法を提供するユーティリティ
md5sum	指定したファイルのチェックサムとブロック数を印刷するユーティリティ
mv	ファイルを移動（名前変更）するユーティリティ
myisamchk	データベース テーブルの検査および修復を示します
mysql	データベース プロセスを示します。複数のインスタンスが表示されることがあります
openssl	認証証明書の作成を示します。
perl	perl プロセスを示します。
ps	標準出力にプロセス情報を作成するユーティリティ
sed	1 つ以上のテキスト ファイルの編集に使用されるユーティリティ
sfheartbeat	アプライアンスがアクティブであることを示す、ハートビート ブロードキャストを識別します。ハートビートはデバイスとDefense Centerの間の接続を維持するのに使用されます
sfmb	メッセージ ブローカ プロセスを示します。Defense Centerとデバイスとの間の通信を処理します。
sh	Korn シェルのパブリック ドメイン バージョン
shutdown	アプライアンスをシャットダウンするユーティリティ
sleep	指定された秒数のあいだプロセスを中断するユーティリティ

表 67-6　システムの実行可能ファイルおよびユーティリティ（続き）

実行可能	説明
smtpclient	電子メール イベント通知機能が有効な場合に、電子メール送信を処理するメール クライアント
snmptrap	SNMP 通知機能が有効な場合に、指定された SNMP トラップ サーバに SNMP トラップ データを転送します
snort （Protection が必要）	Snort が動作していることを示します
ssh	アプライアンスへの Secure Shell (SSH) 接続を示します
sudo	sudo プロセスを示します。これにより、admin 以外のユーザが実行可能ファイルを実行できるようになります
top	上位の CPU プロセスに関する情報を表示するユーティリティ
touch	指定したファイルへのアクセス時刻や変更時刻を変更するために使用できるユーティリティ
vim	テキスト ファイルの編集に使用されるユーティリティ
wc	指定したファイルの行、ワード、バイトのカウントを実行するユーティリティ

ヘルス モニタリングの使用

ヘルス モニタは、防御センター からアプライアンスの正常性を確認するためのさまざまなテストを提供します。ヘルス モニタを使用すれば、*正常性ポリシー*とも呼ばれるテストのコレクションを作成し、正常性ポリシーを 1 つ以上のアプライアンスに適用できます。システム内のすべてのアプライアンスに共通の正常性ポリシーを作成することも、適用を予定している特定のアプライアンス用に正常性ポリシーをカスタマイズすることも、デフォルトの正常性ポリシーを使用することもできます。別の防御センター からエクスポートした正常性ポリシーをインポートすることもできます。

*ヘルス モジュール*とも呼ばれるテストは、指定された基準に照らしてテストするスクリプトです。テストを有効または無効にするか、テスト設定を変更することによって、正常性ポリシーを変更したり、不要になった正常性ポリシーを削除したりできます。アプライアンスをブラックリストに登録することによって、選択したアプライアンスからのメッセージを抑制することもできます。

正常性ポリシー内のテストは設定された時間間隔で自動的に実行されます。すべてのテストを実行することも、オンデマンドで特定のテストを実行することもできます。ヘルス モニタは設定されたテスト条件に基づいてヘルス イベントを収集します。オプションで、ヘルス イベントに対応して警告する電子メール、SNMP、または syslog を設定することもできます。

防御センター では、システム全体または特定のアプライアンスに関するヘルス ステータス情報を表示できます。完全にカスタマイズ可能なイベント ビューを使用すれば、ヘルス モニタによって収集されたヘルス ステータス イベントを迅速かつ容易に分析できます。このイベント ビューでは、イベント データを検索して表示したり、調査中のイベントに関係する他の情報にアクセスしたりできます。

サポートから依頼された場合に、アプライアンスのトラブルシューティング ファイルを作成することもできます。

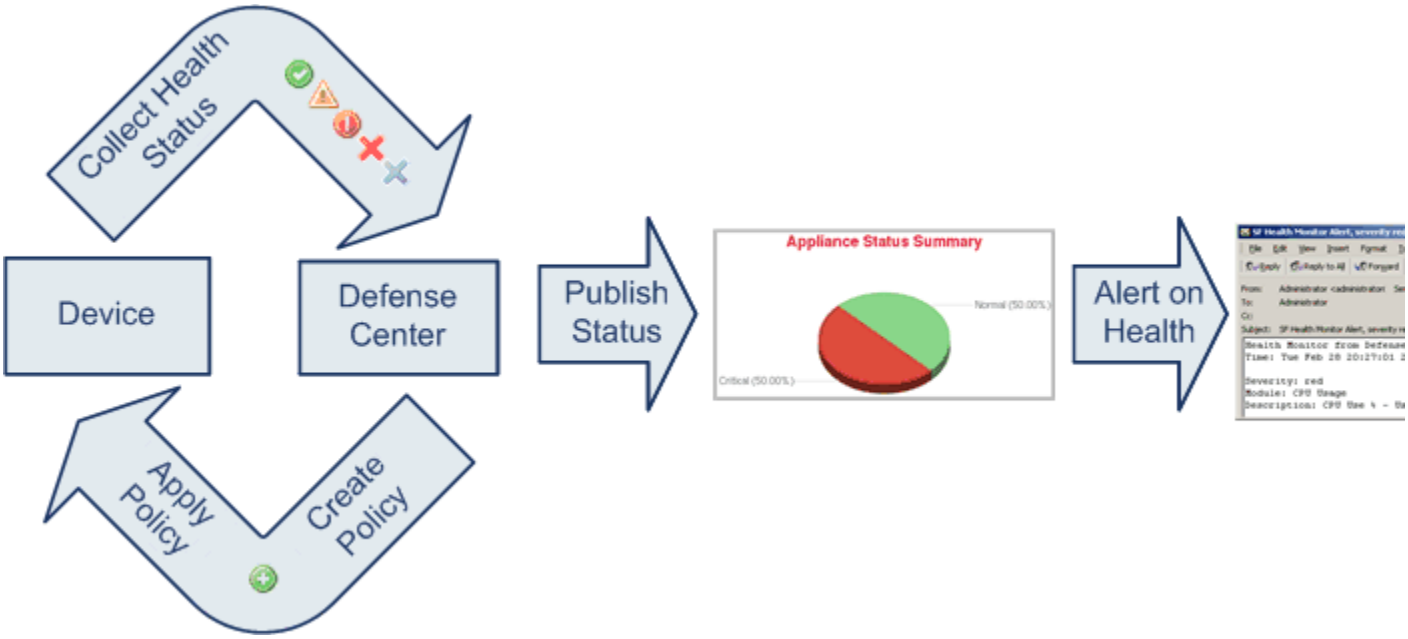
詳細については、次の項を参照してください。

- ヘルス モニタリングについて(68-2 ページ)
- 正常性ポリシーの設定(68-7 ページ)
- ヘルス モニタ ブラックリストの使用(68-38 ページ)
- ヘルス モニタ アラートの設定(68-42 ページ)
- ヘルス モニタの使用(68-45 ページ)
- アプライアンス ヘルス モニタの使用(68-46 ページ)
- ヘルス イベントの操作(68-52 ページ)

ヘルス モニタリングについて

ライセンス： すべて

ヘルス モニタを使用して、FireSIGHT システム展開全体の重要な機能のステータスを確認できます。防御センターを通して管理対象デバイスのそれぞれに正常性ポリシーを適用し、防御センターで結果のヘルス データを収集することによって、FireSIGHT システム全体の正常性を監視します。[Health Monitor] ページ上の円グラフとステータス テーブルは、監視対象のアプライアンスのヘルス ステータスを視覚的に表しているため、一目でステータスをチェックでき、必要に応じてステータス詳細にドリルダウンできます。



ヘルス モニタを使用して、システム全体または特定のアプライアンスのヘルス ステータス情報にアクセスできます。[Health Monitor] ページには、システム上のすべてのアプライアンスのステータスの概要が表示されます。個々のアプライアンスのヘルス モニタを使用すれば、特定のアプライアンスのヘルス詳細にドリルダウンできます。

標準の FireSIGHT システム テーブル ビューでヘルス イベントを表示することもできます。個々のアプライアンスのヘルス モニタから、特定のイベント発生のテーブル ビューを開いたり、そのアプライアンスのすべてのステータス イベントを取得したりできます。特定のヘルス イベントを検索することもできます。たとえば、特定のパーセンテージの CPU 使用率の全記録を表示する場合は、CPU 使用率モジュールを検索して、パーセンテージ値を入力できます。

ヘルス イベントに対応した電子メール、SNMP、または syslog アラートを設定することもできます。ヘルス アラートは、標準アラートとヘルス ステータス レベルを関連付けたものです。たとえば、アプライアンスでハードウェアの過負荷が原因で障害が発生することは絶対ないことを確認する必要がある場合は、電子メール アラートをセットアップできます。その後で、CPU、ディスク、またはメモリの使用率がそのアプライアンスに適用される正常性ポリシーで設定された警告レベルに達するたびにその電子メール アラートをトリガーとして使用するヘルス アラートを作成できます。アラートしきい値を、受け取る反復アラートの数が最小になるように設定できます。

ヘルス モニタリングは管理活動であるため、管理者ユーザー ロール特権を持っているユーザーのみがシステム ヘルス データにアクセスできます。ユーザ特権の割り当て方法については、ユーザ特権とオプションの変更（61-58 ページ）を参照してください。

注　防御センター を除いて、FireSIGHT システム デバイスにはデフォルトでヘルス モニタリング ポリシーが適用されません。管理対象デバイスはハードウェア アラーム ヘルス モジュール経由で自動的にハードウェア ステータスを報告します。他のモジュールを使用して管理対象デバイスを監視する場合は、正常性ポリシーをそのデバイスに適用する必要があります。Ciscoが提供するアプライアンス用のデフォルト正常性ポリシーの詳細については、デフォルト正常性ポリシーについて（68-8 ページ）を参照してください。カスタマイズした正常性ポリシーの作成方法については、正常性ポリシーの作成（68-9 ページ）を参照してください。ポリシーの適用について詳しくは、正常性ポリシーの適用（68-32 ページ）を参照してください。

正常性ポリシーと、システム ヘルスをテストするために実行可能なヘルス モジュールの詳細については、次のトピックを参照してください。

- 正常性ポリシーについて（68-3 ページ）
- ヘルス モジュールについて（68-3 ページ）
- ヘルス モニタリング設定について（68-6 ページ）

正常性ポリシーについて

ライセンス： すべて

*正常性ポリシー*は、防御センター がアプライアンスの正常性をチェックするときに使用する基準を定義するためにアプライアンスに適用するヘルス モジュール設定のコレクションです。ヘルス モニタは、FireSIGHT システムのハードウェアとソフトウェアが正しく機能していることを確認するためのさまざまなヘルス インジケータを追跡します。

正常性ポリシーを作成するときに、アプライアンスの正常性を確認するために実行するテストを選択します。また、デフォルト正常性ポリシーをアプライアンスに適用することもできます。

ヘルス モジュールについて

ライセンス： すべて

*ヘルス テスト*とも呼ばれる*ヘルス モジュール*は、正常性ポリシー内で指定された基準に照らしてテストするスクリプトです。使用可能なヘルス モジュールの説明を次の表に示します。

表 68-1　　ヘルス モジュール

モジュール	説明
高度なマルウェア対策	このモジュールは、ファイル ポリシー設定に基づいて、ネットワーク トラフィックで検出されたファイルに関するファイル性質情報を取得するため、または動的分析用にファイルを送信するために防御センター が Collective Security Intelligence クラウド に接続できなかった場合、または、ネットワーク トラフィックで過剰なファイル数が検出された場合に警告します。FireAMP プライベート クラウド経由の接続でも、プライベート クラウドがCiscoのパブリック クラウドに接続できなかった場合にアラートが生成されます。 このモジュールは、高度なマルウェア対策をサポートしていない DC500 を除くすべての防御センター 上で動作します。

表 68-1　ヘルス モジュール（続き）

モジュール	説明
アプライアンス ハートビート	このモジュールは、アプライアンス ハートビートがアプライアンスから届いているかどうかを確認し、アプライアンスのハートビート ステータスに基づいてアラートを出します。
自動アプリケーション バイパス ステータス	このモジュールは、アプライアンスがバイパスしきい値で設定された秒数以内に応答しなかったためにバイパスされたかどうかを確認し、バイパスが発生した場合にアラートを出します。
CPU 使用率	このモジュールは、アプライアンス上の CPU が過負荷になっていないことを確認し、CPU 使用率がモジュールに設定されたパーセンテージを超えた場合にアラートを出します。 このモジュールは、3D9900 デバイスに適用される正常性ポリシーでは使用できません。
カード リセット	このモジュールは、リセット時に、ハードウェア障害原因で再起動されたネットワーク カードをチェックし、アラートを出します。
ディスク ステータス	このモジュールは、ハード ディスクと、アプライアンス上のマルウェア ストレージ パック（設置されている場合）のパフォーマンスを調査します。また、ハード ディスクと RAID コントローラ（設置されている場合）に障害が発生する恐れがある場合、あるいは、マルウェア ストレージ パックが設置後に検出されないまたは正規品でない場合にアラートを出します。
ディスク使用率	このモジュールは、アプライアンスのハード ドライブとマルウェア ストレージ パック上のディスク使用率をモジュールに設定された制限と比較し、その使用率がモジュールに設定されたパーセンテージを超えた時点でアラートを出します。また、モジュールしきい値に基づいて、システムが監視対象のディスク使用カテゴリ内のファイルを過剰に削除する場合、または、これらのカテゴリを除くディスク使用率が過剰なレベルに達した場合にもアラートを出します。
FireAMP ステータス モニタ	このモジュールは、防御センター が初期接続の成功後にCisco クラウドに接続できない場合、または FireAMP ポータルを使用してクラウド接続を登録解除した場合、またはプライベート クラウドがシスコのパブリック クラウドと通信できない場合にアラートを出します。 このモジュールは、防御センター上でのみ動作します。
FireSIGHTホスト ライセンス制限	このモジュールは、十分な FireSIGHT ホスト ライセンスが残っているかどうかを確認し、モジュールに設定された警告レベルに基づいてアラートを出します。 このモジュールは、防御センター上でのみ動作します。
ハードウェア アラーム	このモジュールは、シリーズ 3 または 3D9900 デバイス上のハードウェアを交換する必要があるかどうかを確認し、ハードウェア ステータスに基づいてアラートを出します。また、ハードウェア関連デーモンのステータスとクラスタ化されたアプライアンスのステータスについて報告します。 これらのデバイスについて報告される詳細については、3D9900 デバイスのハードウェア アラート詳細の解釈（68-56 ページ）とシリーズ 3 デバイスのハードウェア アラート詳細の解釈（68-57 ページ）を参照してください。
ヘルス モニタ プロセス	このモジュールは、ヘルス モニタ自体のステータスを監視し、防御センター で受信された最後のステータス イベント以降の分数が警告制限または重大制限を超えた場合にアラートを出します。 このモジュールは、防御センター上でのみ動作します。
インライン リンク不一致アラーム	このモジュールは、インライン セットに関連付けられたポートを監視し、インライン ペアの 2 つのインターフェイスが別々の速度をネゴシエートした場合にアラートを出します。

表 68-1　ヘルス モジュール（続き）

モジュール	説明
侵入イベント レート	このモジュールは、1 秒あたりの侵入イベント数をこのモジュールに設定された制限と比較し、制限を超えた場合にアラートを出します。侵入イベント レートが 0 の場合は、侵入プロセスがダウンしているか、管理対象デバイスがイベントを送信していない可能性があります。イベントがデバイスから送られているかどうかをチェックするには、[Analysis] > [Intrusions] > [Events] の順に選択します。
インターフェイス ステータス	このモジュールは、デバイスが現在トラフィックを収集しているかどうかを確認して、物理インターフェイスおよび集約インターフェイスのトラフィック ステータスに基づいてアラートを出します。物理インターフェイスの情報には、インターフェイス名、リンク ステート、および帯域幅が含まれます。集約インターフェイスの情報には、インターフェイス名、アクティブ リンクの数、および総集約帯域幅が含まれます。
ライセンス モニタ	このモジュールは、Control、Protection、URL Filtering、Malware、および VPN 用の十分なライセンスが残っているかどうかを確認します。また、スタック内のデバイスに適合しないライセンス セットが含まれている場合にアラートを出します。モジュールに自動的に設定された警告レベルに基づいてアラートを出します。このモジュールの設定は変更できません。 このモジュールは、防御センター上でのみ動作します。
リンク ステート伝達	このモジュールは、ペア化されたインライン セット内のリンクで障害が発生した時点を特定して、リンクステート伝達モードをトリガーとして使用します。
メモリ使用率	このモジュールは、アプライアンス上のメモリ使用率をモジュールに設定された制限と比較し、使用率がモジュールに設定されたレベルを超えるとアラートを出します。
電源	このモジュールは、デバイスの電源が交換が必要かどうかを確認し、電源ステータスに基づいてアラートを出します。 このモジュールは、防御センター DC1500、DC2000、DC3500、DC4000 上で動作します。 このモジュールは、デバイス 3D3500、3D4500、3D6500、3D9900、およびシリーズ 3 上で動作します。
プロセス ステータス	このモジュールは、アプライアンス上のプロセスがプロセス マネージャの外部で停止または終了したかを確認します。プロセスが故意にプロセス マネージャの外部で停止された場合は、モジュールが再開してプロセスが再起動するまで、モジュール ステータスが Warning に変更され、ヘルス イベント メッセージが停止されたプロセスを示します。プロセスがプロセス マネージャの外部で異常終了またはクラッシュした場合は、モジュールが再開してプロセスが再起動するまで、モジュール ステータスが Critical に変更され、ヘルス イベント メッセージが終了したプロセスを示します。
検出の再設定	このモジュールは、登録された管理対象デバイスでポリシーの適用に失敗した後も検出機能が保持されるかどうかを確認します。ポリシーの適用に失敗して検出機能が動作不能になった場合、モジュールは検出機能が再確立されるまでヘルス アラートを生成します。
RRD サーバ プロセス	このモジュールは、時系列データを保存するラウンド ロビン データ サーバが正常に動作しているかどうかを確認し、最近の RRD サーバの再起動回数に基づいてアラートを出します。 このモジュールは、防御センター上でのみ動作します。
セキュリティ インテリジェンス	このモジュールは、フィード更新、フィード破損、メモリ問題などのセキュリティ インテリジェンス フィルタリングに関するさまざまな状況でアラートを出します。 このモジュールは、セキュリティ インテリジェンス フィルタリングをサポートしていない DC500 以外のすべての防御センター上で動作します。

表 68-1　ヘルス モジュール（続き）

モジュール	説明
時系列データ モニタ	このモジュールは、時系列データ（コンプライアンス イベント カウントなど）が保存されるディレクトリ内の破損ファイルの存在を追跡して、ファイルが破損としてフラグが付けられ、削除された段階でアラートを出します。 このモジュールは、防御センター上でのみ動作します。
時刻同期ステータス	このモジュールは、NTP を使用して時刻を取得するデバイス クロックと NTP サーバ上のクロックの同期を追跡して、クロックの差が 10 秒を超えた場合にアラートを出します。
URL フィルタリング モニタ	このモジュールは、通常訪問される URL に関する URL フィルタリング（カテゴリとレピュテーション）データをシステムが取得する防御センターと Cisco クラウド間の通信を追跡します。防御センターがクラウドとの通信またはクラウドからの更新の取得に失敗した場合にアラートを出します。 このモジュールは、防御センターと、URL フィルタリングが有効になっている管理対象デバイス間の通信も追跡します。防御センターが URL フィルタリング データをそのようなデバイスにプッシュできない場合にアラートを出します。 このモジュールは、URL フィルタリングをサポートしていない DC500 以外のすべての防御センター上でのみ動作します。
ユーザ エージェント ステータス モニタ	このモジュールは、防御センターに接続されたユーザ エージェントでハートビートが検出されない場合にアラートを出します。 このモジュールは、防御センター上でのみ動作します。
VPN ステータス	このモジュールは、VPN 機能が動作していないことをシステムが検出するとアラートを出します。 このモジュールは、防御センター上でのみ動作します。

ヘルス モニタリング設定について

ライセンス： すべて

次の手順に示すように、FireSIGHT システム上でヘルス モニタリングをセットアップするためのいくつかのステップがあります。

ステップ 1　アプライアンス用の正常性ポリシーを作成します。

FireSIGHT システムで使用しているアプライアンスの種類ごとに固有のポリシーをセットアップして、そのアプライアンスに適切なテストだけを有効にすることができます。

ヒント　モニタリング動作をカスタマイズすることなくすぐにヘルス モニタリングを有効にするには、そのために用意されたデフォルト ポリシーを適用できます。

正常性ポリシーのセットアップについては、正常性ポリシーの設定（68-7 ページ）を参照してください。

ステップ 2　ヘルス ステータスを追跡するアプライアンスごとに正常性ポリシーを適用します。すぐに適用できるデフォルト正常性ポリシーについては、デフォルト正常性ポリシーについて（68-8 ページ）を参照してください。

ステップ 3　オプションで、ヘルス モニタ アラートを設定します。

ヘルス ステータス レベルが特定のヘルス モジュールの特定の重大度レベルに達した段階でトリガーされる電子メール、Syslog、または SNMP アラートをセットアップできます。

ヘルス モニタ アラートのセットアップについては、ヘルス モニタ アラートの設定（68-42 ページ）を参照してください。

システム上でヘルス モニタリングをセットアップしたら、[Health Monitor] ページまたは [Health Events] テーブル ビューでいつでもヘルス ステータスを確認できます。システム正常性データの表示方法については、次のトピックを参照してください。

- ヘルス モニタの使用（68-45 ページ）
- アプライアンス ヘルス モニタの使用（68-46 ページ）
- ヘルス イベントの操作（68-52 ページ）

正常性ポリシーの設定

ライセンス： すべて

正常性ポリシーには、複数のモジュールに対して設定されたヘルス テスト基準が含まれます。アプライアンスごとにどのヘルス モジュールを実行するかを制御したり、モジュールごとに実行するテストで使用される特定の制限を設定したりできます。正常性ポリシーで設定可能なヘルス モジュールの詳細については、ヘルス モニタリングについて（68-2 ページ）を参照してください。

システム内のすべてのアプライアンスに適用可能な 1 つの正常性ポリシーを作成することも、適用を計画している特定のアプライアンス用に正常性ポリシーをカスタマイズすることも、付属のデフォルト正常性ポリシーを使用することもできます。別の防御センター からエクスポートした正常性ポリシーをインポートすることもできます。

正常性ポリシーを設定するときに、そのポリシーに対して各ヘルス モジュールを有効にするかどうかを決定します。また、有効にした各モジュールが、プロセスの正常性を評価するたびに報告するヘルス ステータスを制御するための基準を選択することもできます。

防御センター に自動的に適用されるデフォルト正常性ポリシーの詳細については、デフォルト正常性ポリシーについて（68-8 ページ）を参照してください。

詳細については、次のトピックを参照してください。

- デフォルト正常性ポリシーについて（68-8 ページ）
- 正常性ポリシーの作成（68-9 ページ）
- 正常性ポリシーの適用（68-32 ページ）
- 正常性ポリシーの編集（68-33 ページ）
- 正常性ポリシーの比較（68-35 ページ）
- 正常性ポリシーの削除（68-38 ページ）

デフォルト正常性ポリシーについて

ライセンス： すべて

防御センター ヘルス モニタには、アプライアンスのヘルス モニタリングの迅速な実装を容易にするデフォルト正常性ポリシーが付属しています。デフォルト正常性ポリシーは、自動的に防御センターに適用されます。デフォルト正常性ポリシーを編集することはできませんが、コピーしてその設定に基づくカスタム ポリシーを作成することができます。詳細については、正常性ポリシーの作成（68-9 ページ）を参照してください。

また、デバイスの正常性を監視するために、正常性ポリシーを管理対象デバイスにプッシュすることもできます。

注　正常性ポリシーを Cisco NGIPS for Blue Coat X-Series に適用することはできません。

デフォルト正常性ポリシーでは、実行中のプラットフォーム上で使用可能なヘルス モジュールのほとんどが自動的に有効になります。次の表に、防御センターと管理対象デバイスのデフォルト ポリシーでアクティブにされているモジュールの詳細を示します。

表 68-2　デフォルト アクティブ ヘルス モジュール

モジュール	防御センター	管理対象デバイス
高度なマルウェア対策	yes	no
アプライアンス ハートビート	yes	no
自動アプリケーション バイパス	no	yes
CPU Usage	no	no
カード リセット	no	no
ディスク ステータス	yes	yes
Disk Usage	yes	yes
FireAMP ステータス モニタ	yes	no
FireSIGHT ホスト ライセンス制限	yes	no
ハードウェア アラーム	no	yes
ヘルス モニタ プロセス	no	no
インライン リンク不一致アラーム	no	yes
Interface Status	no	yes
侵入イベント レート	no	yes
ライセンス モニタ	yes	no
リンクステート伝達	no	yes
Memory Usage	yes	yes
電源モジュール	no	yes
プロセス ステータス	yes	yes
検出の再設定	no	yes
RRD サーバ プロセス	yes	no
セキュリティ インテリジェンス	yes	no

表 68-2　デフォルト アクティブ ヘルス モジュール（続き）

モジュール	防御センター	管理対象デバイス
時系列データ モニタ	yes	no
時刻同期ステータス	yes	yes
URL フィルタリング モニタ	yes	no
ユーザ エージェント ステータス モニタ	yes	no
VPN ステータス	yes	no

正常性ポリシーの作成

ライセンス： すべて

アプライアンスで使用する正常性ポリシーをカスタマイズすることによって、新しいポリシーを作成できます。ポリシー内の設定は、最初に、新しいポリシーの基準として選択した正常性ポリシー内の設定を使用して生成されます。必要に応じて、ポリシー内のモジュールを有効または無効にし、各モジュールのアラート基準を変更できます。

ヒント　新しいポリシーを作成する代わりに、別の防御センターから正常性ポリシーをエクスポートして、それを対象の防御センターにインポートできます。その後で、インポートしたポリシーをニーズに合わせて編集してから、適用できます。詳細については、設定のインポートおよびエクスポート（A-1 ページ）を参照してください。

正常性ポリシーを作成する方法：

アクセス： Admin/Maint

ステップ 1　[Health] > [Health Policy] の順に選択します。

[Health Policy] ページが表示されます。

ステップ 2　[Create Policy] をクリックします。

[Create Health Policy] ページが表示されます。

ステップ 3　[Copy Policy] ドロップダウン リストから、新しいポリシーの基準として使用する既存のポリシーを選択します。

ステップ 4　ポリシーの名前を入力します。

ステップ 5　ポリシーの説明を入力します。

ステップ 6　[Save] を選択して、ポリシー情報を保存します。

[Health Policy Configuration] ページが開いて、モジュールのリストが表示されます。

ステップ 7　次の項の説明に従って、アプライアンスのヘルス ステータスをテストするために使用する各モジュールの設定を構成します。

- ポリシー実行時間間隔の設定（68-11 ページ）
- 高度なマルウェア対策モニタリングの設定（68-11 ページ）
- アプライアンス ハートビート モニタリングの設定（68-12 ページ）

- 自動アプリケーション バイパス モニタリングの設定(68-13 ページ)
- CPU 使用率モニタリングの設定(68-13 ページ)
- カード リセット モニタリングの設定(68-14 ページ)
- ディスク ステータス モニタリングの設定(68-15 ページ)
- ディスク使用率モニタリングの設定(68-16 ページ)
- ステータス モニタリングFireAMPの設定(68-17 ページ)
- FireSIGHT ホスト使用量モニタリングの設定(68-18 ページ)
- ハードウェア アラーム モニタリングの設定(68-18 ページ)
- ヘルス ステータス モニタリングの設定(68-19 ページ)
- インライン リンク不一致アラーム モニタリングの設定(68-20 ページ)
- インターフェイス ステータス モニタリングの設定(68-21 ページ)
- 侵入イベント レート モニタリングの設定(68-22 ページ)
- ライセンス モニタリングについて(68-23 ページ)
- リンクステート伝達モニタリングの設定(68-23 ページ)
- メモリ使用率モニタリングの設定(68-24 ページ)
- 電源モニタリングの設定(68-25 ページ)
- プロセス ステータス モニタリングの設定(68-25 ページ)
- 検出のモニタリングの再設定の構成(68-26 ページ)
- RRD サーバ プロセス モニタリングの設定(68-27 ページ)
- セキュリティ インテリジェンス モニタリングの設定(68-28 ページ)
- 時系列データ モニタリングの設定(68-29 ページ)
- 時刻同期モニタリングの設定(68-29 ページ)
- URL フィルタリング モニタリングの設定(68-30 ページ)
- ユーザ エージェント ステータス モニタリングの設定(68-31 ページ)
- VPN ステータス モニタリングの設定(68-31 ページ)

注　設定を構成するときに、それぞれの [Health Policy Configuration] ページでヘルス ステータスをテストするために実行するモジュールが有効になっていることを確認します。無効になっているモジュールは、そのモジュールを含むポリシーがアプライアンスに適用されていても、ヘルス ステータス フィードバックを生成しません。

ステップ 8　[Save Policy and Exit] をクリックしてポリシーを保存します。

有効にするには、それぞれのアプライアンスにポリシーを適用する必要があります。正常性ポリシーの適用方法については、正常性ポリシーの適用(68-32 ページ)を参照してください。

ポリシー実行時間間隔の設定

ライセンス：すべて

正常性ポリシーのポリシー実行時間間隔を変更することによって、正常性テストの実行頻度を制御できます。設定可能な最大実行時間間隔は 99999 分です。

注意　5 分未満の実行時間間隔を設定しないでください。

ポリシー実行時間間隔を設定する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Policy Run Time Interval] を選択します。

[Health Policy Configuration — Policy Run Time Interval] ページが表示されます。

ステップ 2　[Run Interval (mins)] フィールドに、テストの自動反復の時間間隔を分単位で入力します。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

高度なマルウェア対策モニタリングの設定

ライセンス：Malware

このモジュールは、Cisco クラウドに問い合わせてネットワーク トラフィックでファイルを検出する防御センターの機能の状態と安定性を追跡します。システムで、クラウドとの接続が中断された、接続に使用されている暗号キーが無効である、または一定のタイム フレームで検出されたファイル数が多すぎることが検出された場合は、このモジュールのステータス分類が Warning に変更され、モジュールが正常性アラートを生成します。使用している FireAMP プライベート クラウドがシスコのパブリック クラウドと通信できない場合は、プライベート クラウド自体でアラートが生成されます。詳細については、『*FireAMP Private Cloud Administration Portal User Guide*』を参照してください。

注　防御センターのインターネット接続が切断された場合、高度なマルウェア対策ヘルス アラートの生成に最大 30 分かかることがあります。

高度なマルウェア対策ヘルス モジュールの設定を構成する方法:

アクセス: Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Advanced Malware Protection] を選択します。

[Health Policy Configuration — Advanced Malware Protection] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

アプライアンス ハートビート モニタリングの設定

ライセンス: すべて

防御センター は、デバイスが実行しており防御センター と正常に通信していることを示すものとして、その管理対象デバイスから、2 分ごとと 200 イベントごとのどちらか早い方でハートビートを受け取ります。アプライアンス ハートビート ヘルス ステータス モジュールは、防御センター が管理対象アプライアンスからハートビートを受信しているかどうかを追跡するために使用します。防御センター がデバイスからのハートビートを検出しない場合、このモジュールのステータス分類が Critical に変わります。このステータス データがヘルス モニタに反映されます。

アプライアンス ハートビート ヘルス モジュールの設定を構成する方法:

アクセス: Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Appliance Heartbeat] を選択します。

[Health Policy Configuration — Appliance Heartbeat] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。

- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

自動アプリケーション バイパス モニタリングの設定

ライセンス： すべて

このモジュールは、管理対象デバイスがバイパスしきい値として設定された秒数以内に応答しなかったためにバイパスされた時点を検出するために使用します。バイパスが発生すると、このモジュールがアラートを生成します。このステータス データがヘルス モニタに反映されます。

自動アプリケーション バイパスの詳細については、Automatic Application Bypass（4-59 ページ）を参照してください。

自動アプリケーション バイパス モニタリング ステータスを設定する方法：

アクセス： Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Automatic Application Bypass Status] を選択します。

[Health Policy Configuration — Automatic Application Bypass Status] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当する管理対象デバイスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

CPU 使用率モニタリングの設定

ライセンス： すべて

サポートされるデバイス： すべて（3D9900 を除く）

サポートされる防御センター： すべて

CPU 使用率が高すぎる場合、ハードウェアをアップグレードする必要がある、または、正しく機能していないプロセスが存在することを示している可能性があります。CPU 使用率ヘルス ステータス モジュールは、CPU 使用率の制限を設定するために使用します。

監視対象アプライアンスの CPU 使用率が警告制限を超えた場合、そのモジュールのステータス分類が Warning に変更されます。監視対象アプライアンスの CPU 使用率が重大制限を超えた場合、そのモジュールのステータス分類が Critical に変更されます。このステータス データがヘルス モニタに反映されます。

両方の制限に設定可能な最大パーセンテージは 100% であり、重大制限は警告制限より高くする必要があります。

CPU 使用率の制限を設定する方法：

アクセス： Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[CPU Usage] を選択します。

[Health Policy Configuration — CPU Usage] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　[Critical Threshold %] フィールドに、重大ヘルス ステータスをトリガーとして使用する CPU 使用率のパーセンテージを入力します。

ステップ 4　[Warning Threshold %] フィールドに、警告ヘルス ステータスをトリガーとして使用する CPU 使用率のパーセンテージを入力します。

ステップ 5　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

カード リセット モニタリングの設定

ライセンス： すべて

カード リセット モニタリング ヘルス ステータス モジュールは、ハードウェア障害が原因でネットワーク カードが再起動された時点を追跡するために使用します。リセットが発生すると、このモジュールがアラートを生成します。このステータス データがヘルス モニタに反映されます。

カード リセット モニタリングを設定する方法:

アクセス: Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Card Reset] を選択します。

[Health Policy Configuration — Card Reset Monitoring] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、該当する防御セ ン タ ーに正常性ポリシーを適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

ディスク ステータス モニタリングの設定

ライセンス: すべて

ディスク ステータス ヘルス モジュールは、アプライアンスのハード ディスクとマルウェア ストレージ パック（設置されている場合）の現在のステータスを監視するために使用します。このモジュールは、ハード ディスクと RAID コントローラ（設置されている場合）で障害が発生する恐れがある場合、または、マルウェア ストレージ パックではない追加のハード ドライブが設置されている場合に、警告（黄色）ヘルス アラートを生成します。また、設置されているマルウェア ストレージ パックを検出できなかった場合はアラート（赤色）ヘルス アラートを生成します。

ディスク ステータス ヘルス モジュールの設定を構成する方法:

アクセス: Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Disk Status] をクリックします。

[Health Policy Configuration — Disk Status] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。

- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

ディスク使用率モニタリングの設定

ライセンス： すべて

十分なディスク スペースがないと、アプライアンスは動作できません。ヘルス モニタは、スペースが使い果たされる前に、アプライアンスのハード ドライブとマルウェア ストレージ パック上のディスク スペースが少ない状態を特定できます。また、ヘルス モニタは、ハード ドライブのファイル ドレインが頻繁に発生する場合にアラートを出せます。ディスク使用率ヘルス ステータス モジュールは、アプライアンス上の `/` パーティションと `/volume` パーティションのディスク使用率を監視して、ドレイン頻度を追跡するために使用します。

注　ディスク使用率モジュールは `/boot` パーティションを監視対象パーティションとして列挙しますが、そのパーティションのサイズが固定のため、このモジュールはブート パーティションに基づいてアラートを出すことはしません。

監視対象アプライアンスのディスク使用率が警告制限を超えた場合、そのモジュールのステータス分類が Warning に変更されます。監視対象アプライアンスのディスク使用率が重大制限を超えた場合、そのモジュールのステータス分類が Critical に変更されます。両方の制限に設定可能な最大パーセンテージは 100% であり、重大制限は警告制限より高くする必要があります。

システムが未処理のイベントを削除すると、そのモジュールのステータス分類が Warning に変更されます。システムがモジュールしきい値に基づいて、頻繁に、ディスク使用率カテゴリ内のファイルをドレインしている場合、または、監視対象ディスク使用率カテゴリに含まれないファイルのディスク使用率がモジュールしきい値に基づいて大きくなる場合、そのモジュールのステータス分類が Critical に変更されます。ディスク使用率カテゴリの詳細については、Disk Usage ウィジェットについて（55-29 ページ）を参照してください。

ディスク使用率ヘルス モジュールの設定を構成する方法：

アクセス： Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Disk Usage] を選択します。

[Health Policy Configuration — Disk Usage] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　[Critical Threshold %] フィールドに、重大ヘルス ステータスをトリガーとして使用するディスク使用率のパーセンテージを入力します。

ステップ 4　[Warning Threshold %] フィールドに、警告ヘルス ステータスをトリガーとして使用するディスク使用率のパーセンテージを入力します。

ステップ 5　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

ステータス モニタリングFireAMPの設定

ライセンス： すべて

FireAMP ステータス モニタ モジュールは、次の状況でアラートを出すために使用します。

- 防御センターが Cisco クラウドに最初は正しく接続できたのに、その後接続できない
- FireAMP ポータルを使用してクラウド接続を登録解除した
- FireAMP プライベート クラウドがシスコのパブリック クラウドと通信できない

このようなケースでは、モジュール ステータスが Critical に変更され、失敗した接続に関連付けられたクラウド名が表示されます。クラウド接続の設定方法については、FireAMP 用のクラウド接続の操作（37-27 ページ）を参照してください。

FireAMP ステータス モニタ モジュールの設定を構成する方法：

アクセス： Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[FireAMP Status Monitor] を選択します。

[Health Policy Configuration — FireAMP Status Monitor] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、FireAMP ステータス モニタリングに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを防御センターに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

FireSIGHT ホスト使用量モニタリングの設定

ライセンス：FireSIGHT

FireSIGHT ホスト ライセンス制限ヘルス ステータス モジュールは、FireSIGHT ホスト使用量警告制限を設定するために使用します。監視対象デバイス上の残りの FireSIGHT ホスト数が警告ホスト数制限を下回った場合は、そのモジュールのステータス分類が Warning に変更されます。監視対象デバイス上の残りの FireSIGHT ホスト数が重大ホスト数制限を下回った場合は、そのモジュールのステータス分類が Critical に変更されます。このステータス データがヘルス モニタに反映されます。

両方の制限に設定可能な最大ホスト数は 1000 で、重大ホスト制限数は警告制限より小さくする必要があります。

FireSIGHT ホスト ライセンス制限ヘルス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[FireSIGHT Host License Limit] を選択します。

[Health Policy Configuration — FireSIGHT Host License Limit] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　[Critical number Hosts] フィールドに、重大ヘルス ステータスをトリガーとして使用する使用可能なホストの残数を入力します。

ステップ 4　[Warning number Hosts] フィールドに、警告ヘルス ステータスをトリガーとして使用する使用可能なホストの残数を入力します。

ステップ 5　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

ハードウェア アラーム モニタリングの設定

ライセンス：すべて

サポートされるデバイス：シリーズ 3、3D9900

ハードウェア アラーム ヘルス ステータス モジュールは、シリーズ 3 または 3D9900 デバイス上でハードウェア障害を検出するために使用します。ハードウェア アラーム モジュールが、障害が発生したハードウェア コンポーネントまたは相互に通信していないクラスタ化されたデバイスを検出すると、そのモジュールのステータス分類が Critical に変更されます。このステータス データがヘルス モニタに反映されます。

3D9900 デバイス上のハードウェア アラートの原因となるハードウェア ステータス状態の詳細については、3D9900 デバイスのハードウェア アラート詳細の解釈（68-56 ページ）を参照してください。

ハードウェア アラーム ヘルス モジュールの設定を構成する方法：

アクセス： Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Hardware Alarms] を選択します。

[Health Policy Configuration — Hardware Alarm Monitor] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

ヘルス ステータス モニタリングの設定

ライセンス： すべて

ヘルス モニタ プロセス モジュールは、監視対象アプライアンスから受け取るヘルス イベントの時間間隔が長すぎる場合にアラートを生成することによって、防御センター上でのヘルス モニタの正常性を監視するために使用します。

たとえば、防御センター（`myrtle.example.com`）がデバイス（`dogwood.example.com`）を監視する場合は、ヘルス モニタ プロセス モジュールが有効になっている正常性ポリシーを `myrtle.example.com` に適用します。その後で、ヘルス モニタ プロセス モジュールが、`dogwood.example.com` から最後のイベントが受信されてから経過した分数を示すイベントを報告します。

アラートの生成を引き起こすイベントの時間間隔を分単位で設定できます。最後のイベント制限以降の待ち時間が [Warning Minutes] に設定された分数を超えると、そのモジュールのステータス分類が Warning に変更されます。最後のイベント制限以降の待ち時間が [Critical Minutes] を超えると、そのモジュールのステータス分類が Critical に変更されます。このステータス データがヘルス モニタに反映されます。

両方の制限に設定可能な最大分数は 144 であり、重大制限は警告制限より高くする必要があります。最小分数は 5 です。

ヘルス モニタ プロセス モジュールの設定を構成する方法:

アクセス: Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Health Monitor Process] を選択します。

[Health Policy Configuration — Health Monitor Process] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　[Critical Minutes since last event] に、重大ヘルス ステータスをトリガーとして使用する前にイベント間で待機する最大分数を入力します。

ステップ 4　[Warning Minutes since last event] に、警告ヘルス ステータスをトリガーとして使用する前にイベント間で待機する最大分数を入力します。

ステップ 5　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするためには、正常性ポリシーを防御セ ン タ ーに適用する必要があります。詳細については、「正常性ポリシーの適用 (68-32 ページ)」を参照してください。

インライン リンク不一致アラーム モニタリングの設定

ライセンス: すべて

インライン リンク不一致アラーム ヘルス ステータス モジュールは、インライン セットの両側のインターフェイスが別々の接続速度をネゴシエートした時点を追跡するために使用します。別々にネゴシエートされた速度が検出された場合は、このモジュールがアラートを生成します。

インライン リンク不一致モニタリングを設定する方法:

アクセス: Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Inline Link Mismatch Alarms] を選択します。

[Health Policy Configuration — Inline Link Mismatch Alarms] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。

- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、該当する防御センターに正常性ポリシーを適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

インターフェイス ステータス モニタリングの設定

ライセンス：FireSIGHT

インターフェイス ステータス ヘルス ステータス モジュールは、デバイスがトラフィックを受信しているかどうかを検出するために使用します。インターフェイス ステータス モジュールで、デバイスがトラフィックを受信していないことが確認されると、そのモジュールのステータス分類が Critical に変わります。このステータス データがヘルス モニタに反映されます。

注　`DataPlaneInterfacex` というラベルの付いたインターフェイス（ここで、`x` は数値）は、内部 ASA インターフェイス（ユーザ定義ではない）で、システム内部のパケット フローに関与します。

インターフェイス ステータス ヘルス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Interface Status] を選択します。

[Health Policy Configuration — Interface Status] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

侵入イベント レート モニタリングの設定

ライセンス：Protection

侵入イベント レート ヘルス ステータス モジュールは、ヘルス ステータスの変化をトリガーとして使用する 1 秒あたりのパケット数の制限を設定するために使用します。監視対象デバイス上のイベント レートが [Events per second (Warning)] 制限で設定された 1 秒あたりのイベント数を超えると、そのモジュールのステータス分類が Warning に変更されます。監視対象デバイス上のイベント レートが [Events per second (Critical)] 制限で設定された 1 秒あたりのイベント数を超えると、そのモジュールのステータス分類が Critical に変更されます。このステータス データがヘルス モニタに反映されます。

一般に、ネットワーク セグメントのイベント レートは平均で 1 秒あたり 20 イベントです。この平均レートのネットワーク セグメントでは、[Events per second (Critical)] を 50 に設定し、[Events per second (Warning)] を 30 に設定する必要があります。システムの制限を決定するには、デバイスの [Statistics] ページ（[System] > [Monitoring] > [Statistics]）で [Events/Sec] 値を探してから、次の式を使用して制限を計算します。

- Events per second (Critical) = Events/Sec * 2.5
- Events per second (Warning) = Events/Sec * 1.5

両方の制限に設定可能な最大イベント数は 999 であり、重大制限は警告制限より大きくする必要があります。

侵入イベント レート モニタ ヘルス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Intrusion Event Rate] を選択します。

[Health Policy Configuration — Intrusion Event Rate] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　[Events per second (Critical)] フィールドに、重大ヘルス ステータスをトリガーとして使用する 1 秒あたりのイベント数を入力します。

ステップ 4　[Events per second (Warning)] フィールドに、警告ヘルス ステータスをトリガーとして使用する 1 秒あたりのイベント数を入力します。

ステップ 5　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

ライセンス モニタリングについて

ライセンス： すべて

ライセンス モニタリング ヘルス ステータス モジュールは、Control、Protection、URL Filtering、Malware、および VPN の十分なライセンスが残っているかどうかを確認するために使用します。このモジュールは、残りのライセンスの数が少ないまたは不十分な場合にアラートを出します。

また、スタック設定内のデバイスのライセンス セットが一致しないことをシステムが検出した場合にもアラートを出します（スタックされたデバイスのライセンス セットは同じでなければなりません）。

ライセンス モニタリング モジュールは自動的に設定されます。このモジュールは変更または無効にすることができないため、[Health Policy Configuration] ページに表示されません。

リンクステート伝達モニタリングの設定

ライセンス： すべて

リンクステート伝達ヘルス ステータス モジュールは、インライン ペア上のリンク ステートの伝達を検出するために使用します。リンクステートがペアに伝達した場合は、そのモジュールのステータス分類が Critical に変更され、状態が次のように表示されます。

```
Module Link State Propagation: ethx_ethy is Triggered
```

ここで、*x* と *y* はペア化されたインターフェイス番号です。

リンクステート伝達ヘルス モジュールの設定を構成する方法：

アクセス： Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Link State Propagation] を選択します。

[Health Policy Configuration — Link State Propagation monitor] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

メモリ使用率モニタリングの設定

ライセンス: すべて

メモリ使用率ヘルス ステータス モジュールは、メモリ使用率の制限を設定するために使用します。このモジュールは、空きメモリ、キャッシュされたメモリ、およびスワップ メモリを考慮して空きメモリを計算します。監視対象アプライアンスのメモリ使用率が警告制限を超えた場合は、そのモジュールのステータス分類が Warning に変更されます。監視対象アプライアンスのメモリ使用率が重大制限を超えた場合は、そのモジュールのステータス分類が Critical に変更されます。このステータス データがヘルス モニタに反映されます。

メモリが 4 GB を超えるアプライアンスの場合、プリセットされたアラートしきい値は、システム問題を引き起こす可能性のあるメモリ空き容量の割合を求める式に基づいています。

注　4 GB 未満のアプライアンスでは、警告しきい値と重大しきい値の時間間隔が非常に狭いため、Ciscoは、[Warning Threshold %] の値を手動で 50 に設定することを推奨します。これにより、時間内にアプライアンスのメモリ アラートを受け取って問題を解決できる可能性がさらに高まります。

両方の制限に設定可能な最大パーセンテージは 100% であり、重大制限は警告制限より高くする必要があります。

注　多数の FireSIGHT 機能（セキュリティ インテリジェンス、ファイル キャプチャ、複数のルールを使用した侵入ポリシー、URL フィルタリングなど）を有効にして、アクセス コントロール ポリシーを適用した場合、よりローエンドの ASA FirePOWER デバイスによっては、メモリ割り当てを最大限拡張して使用するために、断続的なメモリ使用率警告が生成される可能性があります。

メモリ使用率ヘルス モジュールの設定を構成する方法:

アクセス: Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Memory Usage] を選択します。

[Health Policy Configuration — Memory Usage] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　[Critical Threshold %] フィールドに、重大ヘルス ステータスをトリガーとして使用するメモリ使用率のパーセンテージを入力します。

ステップ 4　[Warning Threshold %] フィールドに、警告ヘルス ステータスをトリガーとして使用するメモリ使用率のパーセンテージを入力します。

ステップ 5　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

電源モニタリングの設定

ライセンス： すべて

サポートされるデバイス： 3D3500、3D4500、3D6500、3D9900、シリーズ 3

サポートされる防御センター： DC1500、DC2000、DC3500、DC4000

電源ヘルス ステータス モジュールは、サポートされているプラットフォームのいずれかで電源障害を検出するために使用します。モジュールが電力を消失した電源を検出すると、そのモジュールのステータス分類は No Power に変わります。モジュールが電源の存在を検出できない場合、ステータスは Critical Error に変わります。このステータス データがヘルス モニタに反映されます。ヘルス モニタの [Alert Detail] リストで [Power Supply] 項目を展開して、電源ごとの特定のステータス項目を表示できます。

電源ヘルス モジュールの設定を構成する方法：

アクセス： Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Power Supply] を選択します。

[Health Policy Configuration — Power Supply] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

プロセス ステータス モニタリングの設定

ライセンス： すべて

プロセス ステータス ヘルス モジュールは、プロセス マネージャの外部で停止または終了したアプライアンス上で実行中のプロセスを監視するために使用します。プロセス ステータス モジュールのプロセス終了に対する応答はプロセスの終了方法によって異なります。

- プロセスがマネージャ プロセスの内部で終了した場合、モジュールはヘルス イベントを報告しません。

- プロセスが故意にプロセス マネージャの外部で停止された場合は、モジュールが再開してプロセスが再起動するまで、モジュール ステータスが Warning に変更され、ヘルス イベント メッセージが停止されたプロセスを示します。
- プロセスがプロセス マネージャの外部で異常終了またはクラッシュした場合は、モジュールが再開してプロセスが再起動するまで、モジュール ステータスが Critical に変わり、ヘルス イベント メッセージが終了したプロセスを示します。

プロセス ステータス ヘルス モジュールの設定を構成する方法:

アクセス: Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Process Status] を選択します。

[Health Policy Configuration — Process Status] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

検出のモニタリングの再設定の構成

ライセンス: すべて

検出モニタの再設定モジュールは、管理対象デバイスへのポリシー適用後に検出機能のステータスを確認するために使用します。ポリシーの適用に失敗して検出の機能が停止すると、モジュールはヘルス イベントでアラートを生成します。

時系列データ モニタリングの設定を構成する方法:

アクセス: Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Reconfiguring Detection] を選択します。

[Health Policy Configuration — Reconfiguring Detection] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス アラートに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。

- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

RRD サーバ プロセス モニタリングの設定

ライセンス： すべて

RRD サーバ プロセス モジュールは、時系列データを保存する RRD サーバが正常に動作しているかどうかを確認するために使用します。このモジュールは、RRD サーバが前回の更新以降に再起動した場合にアラートを出します。また、RRD サーバの再起動を伴う連続更新回数がモジュール設定で指定された数値に達した場合に Critical または Warning ステータスに遷移します。

RRD サーバ プロセス モニタリングの設定を構成する方法：

アクセス： Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[RRD Server Process] を選択します。

[Health Policy Configuration — RRD Server Process] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　[Critical Number of restarts] フィールドに、重大ヘルス ステータスをトリガーとして使用する連続検出される RRD サーバ リセットの回数を入力します。

ステップ 4　[Warning Number of restarts] フィールドに、警告ヘルス ステータスをトリガーとして使用する連続検出される RRD サーバ リセットの回数を入力します。

ステップ 5　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

セキュリティ インテリジェンス モニタリングの設定

ライセンス： Protection

サポートされる防御センター： すべて（DC500 を除く）

セキュリティ インテリジェンス モジュールは、セキュリティ インテリジェンス フィルタリングを伴うさまざまな状況で警告するために使用します。このモジュールは、セキュリティ インテリジェンスが使用中で次の場合にアラートを出します。

- 防御センターがフィードを更新できないか、フィード データが破損している、または認識可能な IP アドレスが含まれていない
- 管理対象デバイスが防御センターから更新されたセキュリティ インテリジェンス データを受信できない
- 管理対象デバイスが、メモリ問題のために、防御センターから提供されたすべてのセキュリティ インテリジェンス データをロードできない

ヒント セキュリティ インテリジェンス メモリ警告がヘルス モニタに表示された場合は、影響を受けるデバイスのアクセス コントロール ポリシーを再適用して、セキュリティ インテリジェンスに割り当てるメモリを増やすことができます。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

セキュリティ インテリジェンス フィルタリングの詳細については、セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録（13-1 ページ）とセキュリティ インテリジェンス リストとフィードの操作（3-5 ページ）を参照してください。

セキュリティ インテリジェンス モジュールの設定を構成する方法：

アクセス： Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Security Intelligence] を選択します。

[Health Policy Configuration — Security Intelligence] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、セキュリティ インテリジェンス モニタリングに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

時系列データ モニタリングの設定

ライセンス：すべて

時系列データ モニタ モジュールは、システムが保存した時系列データ（コンプライアンス イベントのリストなど）のステータスを監視するために使用します。このモジュールは、時系列データ ストレージ ディレクトリで破損ファイルをスキャンします。モジュールが破損したデータを検出すると、Warning ステータスに遷移し、影響を受けるすべてのファイルの名前を報告します。

時系列データ モニタリングの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Time Series Data Monitor] を選択します。

[Health Policy Configuration — Time Series Data Monitor] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

時刻同期モニタリングの設定

ライセンス：すべて

時刻同期ステータス モジュールは、NTP を使用して NTP サーバから時刻を取得する管理対象デバイス上の時刻がサーバ上の時刻と 10 秒以上異なる時点を検出するために使用します。

時刻同期モニタリングの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Time Synchronization Status] を選択します。

[Health Policy Configuration — Time Synchronization Status] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。

- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

URL フィルタリング モニタリングの設定

ライセンス： URL Filtering

サポートされる防御センター： すべて（DC500 を除く）

URL フィルタリング モニタ モジュールは、防御センター と Cisco クラウド間の通信を追跡するために使用します。システムは、頻繁に訪問される URL に関する URL フィルタリング（カテゴリとレピュテーション）データを取得します。防御センター がクラウドと正常に通信できない、または、クラウドから更新を取得できない場合、そのモジュールのステータス分類は Critical に変わります。

ハイ アベイラビリティ設定では、プライマリ防御センター だけが URL フィルタリング クラウドと通信します。このモジュールからのすべてのデータはそのプライマリ アプライアンスのみを参照します。

URL フィルタリング モニタ モジュールは、防御センター と URL フィルタリングが有効になっている管理対象デバイス間の通信も追跡します。防御センター がクラウドと正常に通信している状態で、防御センター が新しい URL フィルタリング データをその管理対象デバイスにプッシュできない場合、モジュール ステータスは Warning に変わります。

URL フィルタリング モニタ ヘルス モジュールの設定を構成する方法：

アクセス： Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[URL Filtering Monitor] を選択します。

[Health Policy Configuration — URL Filtering Monitor] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを防御センター に適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

ユーザ エージェント ステータス モニタリングの設定

ライセンス：FireSIGHT

ユーザ エージェント ステータス モニタ ヘルス モジュールは、防御センターに接続されているエージェントのハートビートを監視するために使用できます。適用した正常性ポリシー内のモジュールを有効にすると、防御センターが防御センター上で設定されているエージェントのハートビートを検出しない場合に、モジュールはヘルス アラートを生成します。

ユーザ エージェント ステータス モニタ ヘルス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[User Agent Status Monitor] を選択します。

[Health Policy Configuration — User Agent Status Monitor] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを防御センターに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

VPN ステータス モニタリングの設定

ライセンス：VPN

サポートされる防御センター： すべて（シリーズ 2 を除く）

VPN ステータス ヘルス モジュールは、設定したゲートウェイ VPN トンネルの現在のステータスを監視するために使用します。個別のトンネルに関する情報が表示されます。このモジュールは、VPN トンネルのいずれかが動作していないときに、重大（赤色）ヘルス アラートを生成します。

VPN ステータス ヘルス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[VPN Status] をクリックします。

[Health Policy Configuration — VPN Status] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用（68-32 ページ）」を参照してください。

正常性ポリシーの適用

ライセンス： すべて

正常性ポリシーをアプライアンスに適用すると、ポリシー内で有効にしたすべてのモジュールのヘルス テストが、アプライアンス上のプロセスとハードウェアの正常性を自動的に監視します。その後、ヘルス テストは、ポリシー内で設定された時間間隔で実行を続け、アプライアンスのヘルス データを収集し、そのデータを防御センター に転送します。

正常性ポリシーでモジュールを有効にしてから、ヘルス テストが必要ないアプライアンスにポリシーを適用した場合、ヘルス モニタはそのヘルス モジュールのステータスを無効として報告します。

すべてのモジュールが無効になっているポリシーをアプライアンスに適用すると、適用されたすべての正常性ポリシーがアプライアンスから削除されるため、どの正常性ポリシーも適用されません。

すでにポリシーが適用されているアプライアンスに別のポリシーを適用した場合は、新しく適用されたテストに基づく新しいデータの表示が少し遅れる可能性があります。

注　ハイ アベイラビリティ ペア内の防御センター 上で作成されたカスタム 正常性ポリシーは両方のアプライアンス間で複製されます。ただし、デフォルト正常性ポリシーに対する変更は複製されません。各アプライアンスは、それ用に設定されたローカルのデフォルト正常性ポリシーを使用します。

正常性ポリシーを適用する方法：

アクセス： Admin/Maint

ステップ 1　[Health] > [Health Policy] の順に選択します。

[Health Policy] ページが表示されます。

ステップ 2　適用するポリシーの横にある適用アイコン（ ）をクリックします。

[Health Policy Apply] ページが表示されます。

ヒント　[Health Policy] 列の横にあるステータス アイコン( )は、アプライアンスの現在のヘルス ステータスを示します。[System Policy] 列の横にあるステータス アイコン( )は、防御センター とデバイス間の通信ステータスを示します。削除アイコン( )をクリックすることによって、現在適用されているポリシーを削除できることに注意してください。

ステップ 3　正常性ポリシーを適用するアプライアンスを選択します。

ステップ 4　[Apply] をクリックして、選択したアプライアンスにポリシーを適用します。

[Health Policy] ページが開いて、ポリシーの適用が成功したかどうかを示すメッセージが表示されます。アプライアンスのモニタリングは、ポリシーが正常に適用された直後に開始されます。

正常性ポリシーの編集

ライセンス: すべて

モジュールを有効または無効にするか、モジュール設定を変更することによって、正常性ポリシーを変更できます。すでにアプライアンスに適用されているポリシーを変更すると、その変更はポリシーを再適用するまで有効になりません。

さまざまなアプライアンスに適用可能なヘルス モデルを次の表に列挙します。

表 68-3　アプライアンスに適用可能なヘルス モジュール

モジュール	適用可能なアプライアンス
高度なマルウェア対策	防御センター、DC500 以外
アプライアンス ハートビート	防御センター
自動アプリケーション バイパス ステータス	すべての管理対象デバイス
CPU Usage	任意（3D9900 は除く）
カード リセット	すべての管理対象デバイス
ディスク ステータス	いずれか
Disk Usage	いずれか
FireAMP ステータス モニタ	防御センター
FireSIGHT ホスト ライセンス制限	防御センター
ハードウェア アラーム	シリーズ 3、3D9900
ヘルス モニタ プロセス	防御センター
インライン リンク不一致アラーム	すべての管理対象デバイス
Interface Status	すべての管理対象デバイス
侵入イベント レート	Protection 付きの管理対象デバイス
ライセンス モニタ	防御センター
リンクステート伝達	Protection 付きの管理対象デバイス
Memory Usage	いずれか

表 68-3　アプライアンスに適用可能なヘルス モジュール（続き）

モジュール	適用可能なアプライアンス
電源モジュール	防御センター：DC1500、DC2000、DC3500、DC4000 デバイス：3D3500、3D4500、3D6500、3D9900、シリーズ 3
プロセス ステータス	いずれか
検出の再設定	いずれか
RRD サーバ プロセス	防御センター
セキュリティ インテリジェンス	防御センター、DC500 以外
時系列データ モニタ	防御センター
時刻同期ステータス	いずれか
URL フィルタリング モニタ	防御センター、DC500 以外
ユーザ エージェント ステータス モニタ	防御センター
VPN ステータス	防御センター

正常性ポリシーを編集する方法：

アクセス： Admin/Maint

ステップ 1　[Health] > [Health Policy] の順に選択します。

[Health Policy] ページが表示されます。

ステップ 2　変更するポリシーの横にある編集アイコン（  ）をクリックします。

[Policy Run Time Interval] 設定が選択された状態で [Health Policy Configuration] ページが表示されます。

ステップ 3　必要に応じて、次の項の説明に従って、設定を変更します。

- ポリシー実行時間間隔の設定（68-11 ページ）
- 高度なマルウェア対策モニタリングの設定（68-11 ページ）
- アプライアンス ハートビート モニタリングの設定（68-12 ページ）
- 自動アプリケーション バイパス モニタリングの設定（68-13 ページ）
- CPU 使用率モニタリングの設定（68-13 ページ）
- カード リセット モニタリングの設定（68-14 ページ）
- ディスク ステータス モニタリングの設定（68-15 ページ）
- ディスク使用率モニタリングの設定（68-16 ページ）
- ステータス モニタリングFireAMPの設定（68-17 ページ）
- FireSIGHT ホスト使用量モニタリングの設定（68-18 ページ）
- ハードウェア アラーム モニタリングの設定（68-18 ページ）
- ヘルス ステータス モニタリングの設定（68-19 ページ）
- インライン リンク不一致アラーム モニタリングの設定（68-20 ページ）
- インターフェイス ステータス モニタリングの設定

- 侵入イベント レート モニタリングの設定（68-22 ページ）
- ライセンス モニタリングについて（68-23 ページ）
- リンクステート伝達モニタリングの設定（68-23 ページ）
- メモリ使用率モニタリングの設定（68-24 ページ）
- 電源モニタリングの設定（68-25 ページ）
- プロセス ステータス モニタリングの設定（68-25 ページ）
- 検出のモニタリングの再設定の構成（68-26 ページ）
- RRD サーバ プロセス モニタリングの設定（68-27 ページ）
- セキュリティ インテリジェンス モニタリングの設定（68-28 ページ）
- 時系列データ モニタリングの設定（68-29 ページ）
- 時刻同期モニタリングの設定（68-29 ページ）
- URL フィルタリング モニタリングの設定（68-30 ページ）
- ユーザ エージェント ステータス モニタリングの設定（68-31 ページ）
- VPN ステータス モニタリングの設定（68-31 ページ）

ステップ 4　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

ステップ 5　正常性ポリシーの適用（68-32 ページ）の説明に従って、該当するアプライアンスにポリシーを再適用します。

正常性ポリシーの比較

ライセンス： すべて

ポリシーの変更が組織の標準に準拠していることを確認する、または、ヘルス モニタリングのパフォーマンスを最適化するため、2 つの正常性ポリシー間の違いを調査することができます。アクセス可能な正常性ポリシーの場合、2 つの正常性ポリシーまたは同じ正常性ポリシーの 2 つのリビジョンを比較できます。アクティブな正常性ポリシーを他の正常性ポリシーとすばやく比較するには、[Running Configuration] オプションを選択できます。比較した後に、必要に応じて、2 つのポリシーまたはポリシー リビジョン間の違いを記録した PDF レポートを生成できます。

正常性ポリシーまたは正常性ポリシー リビジョンを比較するための 2 つのツールが用意されています。

- 比較ビューには、2 つの正常性ポリシーまたは正常性ポリシー リビジョン間の相違点のみが並べて表示されます。各ポリシーまたはポリシー リビジョンの名前が比較ビューの左右のタイトル バーに表示されます。

これを使用して、Web インターフェイスで相違点を強調表示したまま、両方のポリシーのリビジョンを表示し移動することができます。

- 比較レポートは、正常性ポリシー レポートに類似した PDF 形式で 2 つの正常性ポリシーまたは正常性ポリシー リビジョン間の違いのみのレコードを作成します。

  これは、ポリシー比較を保存、コピー、出力、および共有して、詳しく調査するために使用できます。

正常性ポリシー比較ツールの知識と使い方の詳細については、以下を参照してください。

- 正常性ポリシー比較ビューの使用（68-36 ページ）
- 正常性ポリシー比較レポートの使用（68-37 ページ）

正常性ポリシー比較ビューの使用

ライセンス： すべて

比較ビューには、両方の正常性ポリシーまたはポリシー リビジョンが並べて表示されます。それぞれのポリシーまたはポリシー リビジョンは、比較ビューの左右のタイトル バーに表示された名前で識別されます。最終変更時刻と最終変更ユーザがポリシー名の右側に表示されます。[Health Policy] ページにはポリシーが最後に変更された時刻が現地時間で表示されますが、正常性ポリシー レポートでは変更時刻が UTC で表示されることに注意してください。

2 つの正常性ポリシーまたはポリシー リビジョン間の違いが強調表示されます。

- 青色は強調表示された設定が 2 つのポリシーまたはポリシー リビジョンで違うことを意味します。違いは赤色のテキストで表示されます。
- 緑色は強調表示された設定が一方のポリシーまたはポリシー リビジョンだけにあるが、他方にないことを意味します。

次の表に、実行できる操作を記載します。

表 68-4　　正常性ポリシー比較ビューの操作

目的	操作
個々の変更の間を移動する	またはタイトル バーの上にある [Previous] または [Nex] をクリックします。 左側と右側の間にある二重矢印アイコン（）が移動し、表示している違いを示す [Difference] 番号が変わります。
新しい正常性ポリシー比較ビューを生成する	[New Comparison] をクリックします。 [Select Comparison] ウィンドウが表示されます。詳細については、「正常性ポリシー比較レポートの使用」を参照してください。
正常性ポリシー比較レポートを生成する	[Comparison Report] をクリックします。 正常性ポリシー比較レポートは比較ビューと同じ情報を含む PDF を作成します。

正常性ポリシー比較レポートの使用

ライセンス: すべて

正常性ポリシー比較レポートは、正常性ポリシー比較ビューで特定された 2 つ正常性ポリシー間または同じ正常性ポリシーの 2 つのリビジョン間のすべての違いの記録を、PDF として提供するものです。このレポートは、2 つの正常性ポリシー設定間の違いをさらに調査し、その結果を保存して共有するために使用できます。

正常性ポリシー比較レポートは、アクセス可能な任意の正常性ポリシーの比較ビューから生成できます。正常性ポリシー レポートを生成する前に、未確定の変更をコミットするのを忘れないでください。コミットされた変更だけがレポートに表示されます。

設定に応じて、正常性ポリシー比較レポートに 1 つ以上のセクションを含めることができます。それぞれのセクションで、同じ形式が使用され、同じレベルの詳細が提供されます。[Value A] 列と [Value B] 列は、比較ビューで設定されたポリシーまたはポリシー リビジョンを表していることに注意してください。

ヒント 同様の手順を使用して、SSL ポリシー、ネットワーク分析ポリシー、侵入ポリシー、ファイル ポリシー、システム ポリシー、またはアクセス コントロール ポリシーを比較できます。

2 つの正常性ポリシーまたは同じポリシーの 2 つのリビジョンを比較する方法:

アクセス: Admin/Maint

ステップ 1 [Health] > [Health Policy] の順に選択します。

[Health Policy] ページが表示されます。

ステップ 2 [Compare Policies] をクリックします。

[Select Comparison] ウィンドウが表示されます。

ステップ 3 [Compare Against] ドロップダウンリストから、比較するタイプを次のように選択します。

- 異なる 2 つのポリシーを比較するには、[Other Policy] を選択します。
- 同じポリシーの 2 つのリビジョンを比較するには、[Other Revision] を選択します。
- 現在のアクティブ ポリシーを他のポリシーに対して比較するには、[Running Configuration] を選択します。

正常性ポリシー レポートを生成する前に、変更をコミットするのを忘れないでください。コミットされた変更だけがレポートに表示されます。

ステップ 4 選択した比較タイプに応じて、次のような選択肢があります。

- 2 つの異なるポリシーを比較する場合は、[Policy A] および [Policy B] ドロップダウンリストのそれぞれから、比較するポリシーを選択します。
- 同じポリシーの 2 つのリビジョンを比較する場合は、[Policy] ドロップダウンリストからポリシーを選択し、次に [Revision A] および [Revision B] ドロップダウンリストから比較するリビジョンを選択します。
- 実行中の設定を他のポリシーと比較する場合は、[Policy B] ドロップダウン リストから 2 つ目のポリシーを選択します。

ステップ 5 正常性ポリシー比較ビューを表示するには、[OK] をクリックします。

比較ビューが表示されます。

ステップ 6　正常性ポリシー比較レポートを生成するには、[Comparison Report] をクリックします。

正常性ポリシー レポートが表示されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。

正常性ポリシーの削除

ライセンス： すべて

不要になった正常性ポリシーを削除できます。アプライアンスに適用されているポリシーを削除した場合は、別のポリシーを適用するまでそのポリシー設定が有効のままになります。加えて、デバイスに適用されている正常性ポリシーを削除した場合、元となる関連アラート応答を無効にするまでは、そのデバイスに対して有効になっているヘルス モニタリング アラートがアクティブなままになります。アラート応答の有効化と無効化（43-8 ページ）を参照してください。

ヒント　アプライアンスのヘルス モニタリングを停止するには、すべてのモジュールが無効になっている正常性ポリシーを作成し、それをアプライアンスに適用します。正常性ポリシーの作成方法については、正常性ポリシーの作成（68-9 ページ）を参照してください。正常性ポリシーの適用方法については、正常性ポリシーの適用（68-32 ページ）を参照してください。

正常性ポリシーを削除する方法：

アクセス： Admin/Maint

ステップ 1　[Health] > [Health Policy] の順に選択します。

[Health Policy] ページが表示されます。

ステップ 2　削除するポリシーの横にある削除アイコン（ ）をクリックします。

削除が成功したかどうかを示すメッセージが表示されます。

ヘルス モニタ ブラックリストの使用

ライセンス： すべて

通常のネットワーク メンテナンスの一環として、アプライアンスを無効にしたり、一時的に使用不能にしたりすることがあります。このような機能停止は意図したものであり、アプライアンスからのヘルス ステータスに 防御セ ン タ ー 上のサマリー ヘルス ステータスを反映させる必要がありません。

ヘルス モニタ ブラックリスト機能を使用して、アプライアンスまたはモジュールに関するヘルス モニタリング ステータス レポートを無効にすることができます。たとえば、ネットワークのあるセグメントが使用できなくなることがわかっている場合は、そのセグメント上の管理対象デバイスのヘルス モニタリングを一時的に無効にして、防御セ ン タ ー上のヘルス ステータスにデバイスへの接続がダウンしたことによる警告状態または重大状態が表示されないようにできます。

ヘルス モニタリング ステータスを無効にしても、ヘルス イベントは生成されますが、そのステータスが無効になっているため、ヘルス モニタのヘルス ステータスには影響しません。ブラックリストからアプライアンスまたはモジュールを削除しても、ブラックリストに登録中に生成されたイベントのステータスは Disabled のままです。

アプライアンスからのヘルス イベントを一時的に無効にするには、ブラックリスト設定ページに移動して、アプライアンスをブラックリストに追加します。設定が有効になると、システムは全体のヘルス ステータスを計算するときにブラックリストに登録されているアプライアンスを含めません。[Health Monitor Appliance Status Summary] にはこのアプライアンスが Disabled としてリストされます。

アプライアンス上の個別のヘルス モニタリング モジュールをブラックリストに登録する方が実用的な場合があります。たとえば、アプライアンス上の FireSIGHT ホスト ライセンスを使い果たした場合は、FireSIGHT ホスト ライセンス制限ステータス メッセージをブラックリストに登録できます。

メインの [Health Monitor] ページで、ステータス行内の矢印をクリックして特定のステータスを持つアプライアンスのリストを展開表示すれば、ブラックリストに登録されたアプライアンスを区別できることに注意してください。このビューの展開方法については、ヘルス モニタの使用（68-45 ページ）を参照してください。

ブラックリストに登録されたアプライアンスまたは部分的にブラックリストに登録されたアプライアンスのビューを展開すると、ブラックリスト アイコン（ ）と注記が表示されます。

注　防御センターでは、ヘルス モニタのブラックリスト設定はローカル コンフィギュレーション設定です。そのため、防御センター上でデバイスをブラックリストに登録してから削除しても、後で再登録すれば、ブラックリスト設定は元どおりになります。新たに再登録したデバイスはブラックリストに登録されたままです。

詳細については、以下を参照してください。

- 正常性ポリシーまたはアプライアンスのブラックリストへの登録（68-39 ページ）
- 個別のアプライアンスのブラックリストへの登録（68-40 ページ）
- 個別の正常性ポリシー モジュールのブラックリストへの登録（68-41 ページ）

正常性ポリシーまたはアプライアンスのブラックリストへの登録

ライセンス： すべて

特定の正常性ポリシーが適用されたすべてのアプライアンスに対するヘルス イベントを無効に設定する場合、そのポリシーをブラックリストに登録できます。アプライアンス グループのヘルス モニタリングの結果を無効にする必要がある場合、そのアプライアンス グループをブラックリストに登録できます。ブラックリスト設定が有効になると、[Health Monitor Appliance Module Summary] と [Device Management] ページでアプライアンスが Disabled として表示されます。アプライアンスのヘルス イベントのステータスは Disabled です。

防御センターがハイ アベイラビリティ設定の場合は、一方のハイ アベイラビリティ ピア上の管理対象デバイスだけをブラックリストに登録できることに注意してください。ハイ アベイラビリティ ピアをブラックリストに登録することによって、それが生成したイベントとそれがヘルス イベントを受け取ったデバイスを Disabled としてマークすることもできます。ハイ アベイラビリティ ペア内の防御センターには、ピアを完全にまたは部分的にブラックリストに登録するためのオプションがあります。

正常性ポリシー全体またはアプライアンスのグループをブラックリストに登録する方法:

アクセス: Admin/Maint

ステップ 1　[Health] > [Blacklist] の順に選択します。

[Blacklist] ページが表示されます。

ステップ 2　右側にあるドロップダウン リストを使用して、リストをグループ、ポリシー、またはモデルでソートします(防御セ ン タ ー上のグループは管理対象デバイスです。)。

全部ではなく一部のヘルス モジュールがブラックリストに登録されたアプライアンスは [(Partially Blacklisted)] として表示されることに注意してください。メインのブラックリスト ページでブラックリスト ステータスを編集する場合、アプライアンス上のすべてのモジュールをブラックリストに登録するか、すべてのブラックリスト登録を削除するかのいずれかを行えます。アプライアンス上の個別のヘルス モジュールをブラックリストに登録する方法については、個別の正常性ポリシー モジュールのブラックリストへの登録(68-41 ページ)を参照してください。

ヒント　[Health Policy] 列の横にあるステータス アイコン( )は、アプライアンスの現在のヘルス ステータスを示します。[System Policy] 列の横にあるステータス アイコン( )は、防御セ ン タ ーとデバイス間の通信ステータスを示します。

ステップ 3　次の 2 つのオプションから選択できます。

- グループ、モデル、またはポリシー カテゴリ内のすべてのアプライアンスをブラックリストに登録するには、カテゴリを選択してから、[Blacklist Selected Devices] をクリックします。
- グループ、モデル、またはポリシー カテゴリ内のすべてのアプライアンスからブラックリスト登録を消去するには、カテゴリを選択してから、[Clear Blacklist on Selected Devices] をクリックします。

ページが更新して、アプライアンスの新しいブラックリスト状態が表示されます。

個別のアプライアンスのブラックリストへの登録

ライセンス: すべて

個別のアプライアンスのイベントとヘルス ステータスを Disabled に設定する必要がある場合、アプライアンスをブラックリストに登録できます。ブラックリスト設定が有効になると、アプライアンスが [Health Monitor Appliance Module Summary] に Disabled として表示され、アプライアンスのヘルス イベントのステータスが Disabled になります。

個別のアプライアンスをブラックリストに登録する方法:

アクセス: Admin/Maint

ステップ 1　[Health] > [Blacklist] の順に選択します。

[Blacklist] ページが表示されます。

ステップ 2　アプライアンス グループ、モデル、またはポリシーでリストをソートするには、右側にあるドロップダウン リストを使用します

ステップ 3　次の 2 つのオプションから選択できます。

- グループ、モデル、またはポリシー カテゴリ内のすべてのアプライアンスをブラックリストに登録するには、カテゴリを選択してから、[Blacklist Selected Devices] をクリックします。
- グループ、モデル、またはポリシー カテゴリ内のすべてのアプライアンスからブラックリスト登録を消去するには、カテゴリを選択してから、[Clear Blacklist on Selected Devices] をクリックします。

ページが更新されて、アプライアンスの新しいブラックリスト状態が表示されます。個別の正常性ポリシー モジュールをブラックリストに登録するには、[Edit] をクリックして、個別の正常性ポリシー モジュールのブラックリストへの登録（68-41 ページ）を参照してください。

個別の正常性ポリシー モジュールのブラックリストへの登録

ライセンス： すべて

アプライアンス上の個別の正常性ポリシー モジュールをブラックリストに登録できます。この操作により、モジュールからのイベントによってアプライアンスのステータスが Warning または Critical に変更されないようにすることができます。

モジュールの一部がブラックリストに登録されている場合、そのモジュールの行は 防御センター Web インターフェイスにボールド体で表示されます。

ヒント　ブラックリスト設定が有効になると、アプライアンスが [Blacklist] ページと [Appliance Health Monitor Module Status Summary] で [Partially Blacklisted] または [All Modules Blacklisted] として表示されますが、メインの [Appliance Status Summary] ページでは展開されたビューにだけ表示されます。個別にブラックリストに登録したモジュールを追跡して、必要に応じてそれらを再アクティブ化できるようにしてください。誤ってモジュールを無効にすると、必要な警告または重大メッセージを見逃す可能性があります。

個別の正常性ポリシー モジュールをブラックリストに登録する方法：

アクセス： Admin/Maint

ステップ 1　[Health] > [Blacklist] の順に選択します。

[Blacklist] ページが表示されます。

ステップ 2　グループ、ポリシー、またはモデルでソートしてから、[Edit] をクリックして、アプライアンスの正常性ポリシー モジュールのリストを表示します。

正常性ポリシー モジュールが表示されます。

ステップ 3　ブラックリストに登録するモジュールを選択します。

ステップ 4　[Save] をクリックします。

ヘルス モニタ アラートの設定

ライセンス： すべて

正常性ポリシー内のモジュールのステータスが変更された場合に電子メール、SNMP、またはシステム ログ経由で通知するアラートをセットアップできます。特定のレベルのヘルス イベントが発生したときにトリガーとして使用して警告するヘルス イベント レベルと既存のアラート応答を関連付けることができます。

たとえば、アプライアンスがハード ディスク スペースを使い果たす可能性を懸念している場合は、残りのディスク スペースが警告レベルに達したときに自動的に電子メールをシステム管理者に送信できます。ハード ドライブがさらにいっぱいになる場合、ハード ドライブが重大レベルに達したときに 2 つ目の電子メールを送信できます。

詳細については、次のトピックを参照してください。

- ヘルス モニタ アラートの作成（68-42 ページ）
- ヘルス モニタ アラートの解釈（68-43 ページ）
- ヘルス モニタ アラートの編集（68-44 ページ）
- ヘルス モニタ アラートの削除（68-44 ページ）

ヘルス モニタ アラートの作成

ライセンス： すべて

ヘルス モニタ アラートを作成するときに、重大度レベル、ヘルス モジュール、およびアラート応答の関連付けを作成します。既存のアラートを使用することも、新しいアラートをシステム ヘルスの報告専用に設定することもできます。選択したモジュールが重大度レベルに達すると、アラートがトリガーされます。

既存のしきい値と重複するようにしきい値を作成または更新すると、競合が通知されることに注意してください。重複したしきい値が存在する場合、ヘルス モニタは最も少ないアラートを生成するしきい値を使用し、その他のしきい値を無視します。しきい値のタイムアウト値は、5 ～ 4,294,967,295 分の間にする必要があります。

ヘルス モニタ アラートを作成する方法：

アクセス： Admin

ステップ 1　[Health] > [Health Monitor Alerts] の順に選択します。

[Health Monitor Alerts] ページが表示されます。

ステップ 2　[Health Alert Name] フィールドに、ヘルス アラートの名前を入力します。

ステップ 3　[Severity] リストから、アラートをトリガーとして使用する重大度レベルを選択します。

ステップ 4　[Module] リストから、アラートを適用するモジュールを選択します。

ヒント　複数のモジュールを選択するには、Ctrl + Shift キーを押しながら、モジュール名をクリックします。

ステップ 5　[Alert] リストから、選択した重大度レベルに達したときにトリガーとして使用するアラート応答を選択します。

ヒント　[Alerts] をクリックして、[Alerts] ページを開きます。アラートの作成方法については、アラート応答の使用（43-2 ページ）を参照してください。

ステップ 6　オプションで、[Threshold Timeout] フィールドに、それぞれのしきい値期間が終了してしきい値がリセットされるまでの分数を入力します。デフォルト値は 5 分です。

ポリシー実行時間間隔の値がしきい値タイムアウトの値より小さい場合でも、特定のモジュールから報告される 2 つのヘルス イベントの時間間隔の方が常に大きくなります。したがって、しきい値タイムアウトが 8 分で、ポリシー実行時間間隔が 5 分の場合、報告されるイベントの時間間隔は 10 分（5 X 2）です。

ステップ 7　[Save] をクリックして、ヘルス アラートを保存します。

アラート設定が正常に保存されたかどうかを示すメッセージが表示されます。これで、[Active Health Alerts] リストに作成したアラートが表示されます。

ヘルス モニタ アラートの解釈

ライセンス： すべて

ヘルス モニタによって生成されるアラートには次の情報が含まれます。

- アラートの重大度レベルを示す Severity。
- テスト結果がアラートをトリガーとして使用したヘルス モジュールを示す Module。
- アラートをトリガーとして使用したヘルス テスト結果を含む Description。

ヘルス アラートの重大度レベルの詳細については、次の表を参照してください。

表 68-5　アラートの重大度

重大度	説明
Critical	ヘルス テスト結果が Critical アラート ステータスをトリガーとして使用する基準を満たしました。
Warning	ヘルス テスト結果が Warning アラート ステータスをトリガーとして使用する基準を満たしました。
Normal	ヘルス テスト結果が Normal アラート ステータスをトリガーとして使用する基準を満たしました。
Error	ヘルス テストが実行されませんでした。
Recovered	ヘルス テスト結果が Critical または Warning アラート ステータスから Normal アラート ステータスに戻るための基準を満たしました。

ヘルス モジュールの詳細については、ヘルス モジュールについて（68-3 ページ）を参照してください。

ヘルス モニタ アラートの編集

ライセンス：すべて

既存のヘルス モニタ アラートを編集して、ヘルス モニタ アラートに関連付けられた重大度レベル、ヘルス モジュール、またはアラート応答を変更できます。

ヘルス モニタ アラートを編集する方法：

アクセス：Admin

ステップ 1　[Health] > [Health Monitor Alerts] の順に選択します。

[Health Monitor Alerts] ページが表示されます。

ステップ 2　[Active Health Alerts] リストで、変更するアラートを選択します。

ステップ 3　[Load] をクリックして、選択したアラートの構成済みの設定をロードします。

ステップ 4　必要に応じて設定を変更します。詳細については、ヘルス モニタ アラートの作成（68-42 ページ）を参照してください。

ステップ 5　[Save] をクリックして、変更したヘルス アラートを保存します。

アラート設定が正常に保存されたかどうかを示すメッセージが表示されます。

ヘルス モニタ アラートの削除

ライセンス：すべて

既存のヘルス モニタ アラートを削除できます。

注　ヘルス モニタ アラートを削除しても、関連するアラート応答は削除されません。アラートが継続しないようにするには、元になるアラート応答を無効にするまたは削除する必要があります。詳細については、アラート応答の有効化と無効化（43-8 ページ）およびアラート応答の削除（43-7 ページ）を参照してください。

ヘルス モニタ アラートを削除する方法：

アクセス：Admin

ステップ 1　[Health] > [Health Monitor Alerts] の順に選択します。

[Health Monitor Alerts] ページが表示されます。

ステップ 2　[Active Health Alerts] リストで、削除するアラートを選択します。

ステップ 3　[Delete] をクリックします。

アラート設定が正常に削除されたかどうかを示すメッセージが表示されます。

ヘルス モニタの使用

ライセンス： すべて

[Health Monitor] ページには、防御センターによって管理されているすべてのデバイスに加えて、防御センターに関して収集されたヘルス ステータスが表示されます。[Status] テーブルには、この防御センターの管理対象アプライアンスの台数が全体のヘルス ステータス別に表示されます。円グラフは、各ヘルス ステータス カテゴリに含まれているアプライアンスのパーセンテージを示すヘルス ステータス内訳の別のビューを提供します。

ヘルス モニタを使用する方法：

アクセス： Admin/Maint/Any Security Analyst

ステップ 1　[Health] > [Health Monitor] の順にクリックします。

[Health Monitor] ページが表示されます。

ステップ 2　テーブルの [Status] 列内の該当するステータスまたは円グラフの該当する部分を選択して、そのステータスを持つアプライアンスをリストします。

ヒント　ステータス レベルに関する行内の矢印が下を向いている場合は、そのステータスのアプライアンス リストが下側のテーブルに表示されます。矢印が右を向いている場合、アプライアンス リストは非表示です。

次のトピックで、[Health Monitor] ページから実行可能な作業について詳しく説明します。

- ヘルス モニタ ステータスの解釈（68-45 ページ）
- アプライアンス ヘルス モニタの使用（68-46 ページ）
- 正常性ポリシーの設定（68-7 ページ）
- ヘルス モニタ アラートの設定（68-42 ページ）

ヘルス モニタ ステータスの解釈

ライセンス： すべて

次の表に示すように、重大度別に使用可能なステータス カテゴリには、Error、Critical、Warning、Normal、Recovered、および Disabled が含まれます。

表 68-6　　ヘルス ステータス インジケータ

ステータス レベル	ステータス アイコン	ステータス色	説明
Error		白色	アプライアンス上の 1 つ以上のヘルス モニタリング モジュールで障害が発生し、それ以降、正常に再実行されていないことを示します。テクニカル サポート担当者に連絡して、ヘルス モニタリング モジュールの更新プログラムを入手してください。
Critical		赤	アプライアンス上の 1 つ以上のヘルス モジュールが重大制限を超え、問題が解決されていないことを示します。

表 68-6　ヘルス ステータス インジケータ（続き）

ステータス レベル	ステータス アイコン	ステータス色	説明
警告		黄色	アプライアンス上の 1 つ以上のヘルス モジュールが警告制限を超え、問題が解決されていないことを示します。
標準		グリーン	アプライアンス上のすべてのヘルス モジュールがアプライアンスに適用された正常性ポリシーで設定された制限内で動作していることを示します。
Recovered		グリーン	アプライアンス上のすべてのヘルス モジュールがアプライアンスに適用された正常性ポリシーで設定された制限内で動作していることを示します。これには、前に Critical または Warning 状態だったモジュールも含まれます。
ディセーブル		青色	アプライアンスが無効またはブラックリストに登録されている、アプライアンスに正常性ポリシーが適用されていない、またはアプライアンスが現在到達不能になっていることを示します。

アプライアンス ヘルス モニタの使用

ライセンス： すべて

アプライアンス ヘルス モニタは、アプライアンスのヘルス ステータスの詳細ビューを提供します。

注　通常は、非活動状態が 1 時間（または設定された他の時間間隔）続くと、ユーザはセッションからログアウトされます。ヘルス モニタを長期間受動的に監視する予定の場合は、一部のユーザのセッション タイムアウトの免除、またはシステム タイムアウト設定の変更を検討してください。詳細については、ユーザ ログイン設定の管理（61-51 ページ）およびユーザ インターフェイスの設定（63-30 ページ）を参照してください。

特定のアプライアンスのステータス サマリーを表示する方法：

アクセス： Admin/Maint/Any Security Analyst

ステップ 1　[Health] > [Health Monitor] の順に選択します。

[Health Monitor] ページが表示されます。

ステップ 2　特定のステータスを持つアプライアンスのリストを表示するには、そのステータス行内の矢印をクリックします。

ヒント　ステータス レベルに関する行内の矢印が下を向いている場合は、そのステータスのアプライアンス リストが下側のテーブルに表示されます。矢印が右を向いている場合、アプライアンス リストは非表示です。

ステップ 3　アプライアンス リストの [Appliance] 列で、ヘルス モニタ ツールバーで詳細を表示するアプライアンスの名前をクリックします。

[Health Monitor Appliance] ページが表示されます。

ステップ 4　オプションで、[Module Status Summary] グラフで、表示するイベント ステータス カテゴリの色をクリックします。[Alert Detail] リストは表示を切り替えてイベントを表示または非表示にします。

詳細については、次の項を参照してください。

- ヘルス モジュールについて（68-3 ページ）
- ヘルス モニタ ステータスの解釈（68-45 ページ）
- ステータス別のアラートの表示（68-47 ページ）
- アプライアンスのすべてのモジュールの実行（68-47 ページ）
- 特定のヘルス モジュールの実行（68-48 ページ）
- ヘルス モジュール アラート グラフの生成（68-49 ページ）
- ヘルス モニタを使用したトラブルシューティング（68-50 ページ）

ステータス別のアラートの表示

ライセンス： すべて

ステータス別にアラートのカテゴリを表示または非表示にできます。

ステータス別にアラートを表示する方法：

アクセス： Admin/Maint/Any Security Analyst

ステップ 1　表示するアラートのヘルス ステータスに対応するステータス アイコンまたは円グラフの色セグメントをクリックします。そのカテゴリのアラートが [Alert Detail] リストに表示されます。

ステータス別にアラートを非表示にする方法：

アクセス： Admin/Maint/Any Security Analyst

ステップ 1　表示するアラートのヘルス ステータスに対応するステータス アイコンまたは円グラフの色セグメントをクリックします。そのカテゴリの [Alert Detail] リスト内のアラートが非表示になります。

アプライアンスのすべてのモジュールの実行

ライセンス： すべて

ヘルス モジュール テストは、正常性ポリシー作成時に設定されたポリシー実行時間間隔で自動的に実行されます。ただし、アプライアンスの最新のヘルス情報を収集するためにすべてのヘルス モジュール テストをオンデマンドで実行することもできます。

アプライアンスのすべてのヘルス モジュールを実行する方法:

アクセス: Admin/Maint/Any Security Analyst

ステップ 1　[Health] > [Health Monitor] の順に選択します。

[Health Monitor] ページが表示されます。

ステップ 2　アプライアンス リストを展開して特定のステータスを持つアプライアンスを表示するには、そのステータス行内の矢印をクリックします。

ヒント　ステータス レベルに関する行内の矢印が下を向いている場合は、そのステータスのアプライアンス リストが下側のテーブルに表示されます。矢印が右を向いている場合、アプライアンス リストは非表示です。

ステップ 3　アプライアンス リストの [Appliance] 列で、詳細を表示するアプライアンスの名前をクリックします。

[Health Monitor Appliance] ページが表示されます。

ステップ 4　[Run All Modules] をクリックします。

ステータス バーにテストの進捗状況が表示されてから、[Health Monitor Appliance] ページが更新されます。

注　ヘルス モジュールを手動で実行した場合は、自動的に発生する最初の更新に、手動で実行されたテストの結果が反映されない可能性があります。手動で実行したばかりのモジュールの値が変更されていない場合は、数秒待ってから、デバイス名をクリックしてページを更新します。ページが再び自動的に更新するのを待つこともできます。

特定のヘルス モジュールの実行

ライセンス: すべて

ヘルス モジュール テストは、正常性ポリシー作成時に設定されたポリシー実行時間間隔で自動的に実行されます。ただし、そのモジュールの最新のヘルス情報を収集するためにヘルス モジュール テストをオンデマンドで実行することもできます。

特定のヘルス モジュールを実行する方法:

アクセス: Admin/Maint/Any Security Analyst

ステップ 1　[Health] > [Health Monitor] の順に選択します。

[Health Monitor] ページが表示されます。

ステップ 2　アプライアンス リストを展開して特定のステータスを持つアプライアンスを表示するには、そのステータス行内の矢印をクリックします。

ヒント　ステータス レベルに関する行内の矢印が下を向いている場合は、そのステータスのアプライアンス リストが下側のテーブルに表示されます。矢印が右を向いている場合、アプライアンス リストは非表示です。

ステップ 3　アプライアンス リストの [Appliance] 列で、詳細を表示するアプライアンスの名前をクリックします。

[Health Monitor Appliance] ページが表示されます。

ステップ 4　[Health Monitor Appliance] ページの [Module Status Summary] グラフで、表示するヘルス アラート ステータス カテゴリの色をクリックします。

[Alert Detail] リストが展開して、そのステータス カテゴリの選択されたアプライアンスのヘルス アラートがリストされます。

ステップ 5　イベントのリストを表示するアラートの [Alert Detail] 行で、[Run] をクリックします。

ステータス バーにテストの進捗状況が表示されてから、[Health Monitor Appliance] ページが更新されます。

注　ヘルス モジュールを手動で実行した場合は、自動的に発生する最初の更新に、手動で実行されたテストの結果が反映されない可能性があります。手動で実行したばかりのモジュールの値が変更されていない場合は、数秒待ってから、デバイス名をクリックしてページを更新します。ページが再び自動的に更新するのを待つこともできます。

ヘルス モジュール アラート グラフの生成

ライセンス: すべて

特定のアプライアンスの特定のヘルス テストの一定期間に及ぶ結果をグラフ化できます。

ヘルス アラート モジュール グラフを生成する方法:

アクセス: Admin/Maint/Any Security Analyst

ステップ 1　[Health] > [Health Monitor] の順に選択します。

[Health Monitor] ページが表示されます。

ステップ 2　アプライアンス リストを展開して特定のステータスを持つアプライアンスを表示するには、そのステータス行内の矢印をクリックします。

ヒント　ステータス レベルに関する行内の矢印が下を向いている場合は、そのステータスのアプライアンス リストが下側のテーブルに表示されます。矢印が右を向いている場合、アプライアンス リストは非表示です。

ステップ 3　アプライアンス リストの [Appliance] 列で、詳細を表示するアプライアンスの名前をクリックします。

[Health Monitor Appliance] ページが表示されます。

ステップ 4　[Health Monitor Appliance] ページの [Module Status Summary] グラフで、表示するヘルス アラート ステータス カテゴリの色をクリックします。

[Alert Detail] リストが展開して、そのステータス カテゴリの選択されたアプライアンスのヘルス アラートがリストされます。

ステップ 5　イベントのリストを表示するアラートの [Alert Detail] 行で、[Graph] をクリックします。

一定期間のイベントのステータスを示すグラフが表示されます。グラフの下の [Alert Detail] セクションに、選択したアプライアンスのすべてのヘルス アラートがリストされます。

ヒント　イベントが表示されない場合は、時間範囲を調整する必要があります。詳細については、「イベント時間の制約の設定（58-26 ページ）」を参照してください。

ヘルス モニタを使用したトラブルシューティング

ライセンス： すべて

アプリケーションで問題が発生したときに、サポートから問題の診断を容易にするためにトラブルシューティング ファイルの作成を依頼されることがあります。次の表に示すオプションのいずれかを選択して、ヘルス モニタから報告されるトラブルシューティング データをカスタマイズすることができます。

表 68-7　選択可能なトラブルシュート オプション

オプション	報告内容
Snort Performance and Configuration	アプライアンス上の Snort に関連するデータとコンフィギュレーション設定
Hardware Performance and Logs	アプライアンス ハードウェアのパフォーマンスに関連するデータとログ
System Configuration, Policy, and Logs	アプライアンスの現在のシステム設定に関連するコンフィギュレーション設定、データ、およびログ
Detection Configuration, Policy, and Logs	アプライアンス上の検出に関連するコンフィギュレーション設定、データ、およびログ
Interface and Network Related Data	アプライアンスのインライン セットとネットワーク設定に関連するコンフィギュレーション設定、データ、およびログ
Discovery, Awareness, VDB Data, and Logs	アプライアンス上の現在の検出設定と認識設定に関連するコンフィギュレーション設定、データ、およびログ
Upgrade Data and Logs	アプライアンスの以前のアップグレードに関連するデータとログ
All Database Data	トラブルシュート レポートに含まれるすべてのデータベース関連データ
All Log Data	アプライアンス データベースによって収集されたすべてのログ
Network Map Information	現在のネットワーク トポロジ データ

一部のオプションは報告するデータの観点で重複していますが、どのオプションが選択されたかに関係なく、トラブルシューティング ファイルには冗長なコピーは含まれません。

詳細については、次の項を参照してください。

- アプライアンス トラブルシューティング ファイルの生成（68-51 ページ）
- トラブルシューティング ファイルのダウンロード（68-51 ページ）

アプライアンス トラブルシューティング ファイルの生成

ライセンス: すべて

次の手順を使用して、サポートに送信可能なカスタマイズされたトラブルシューティング ファイルを生成できます。

注　ハイ アベイラビリティ設定で、セカンダリ 防御セ ン タ ー のトラブルシューティング ファイルを生成するためにプライマリ 防御セ ン タ ー を使用することは**できず**、その逆も同様です。独自の Web インターフェイスから 防御セ ン タ ー のトラブルシューティング ファイルを生成する必要があります。

トラブルシューティング ファイルを生成する方法:

アクセス: Admin/Maint/Any Security Analyst

ステップ 1　[Health] > [Health Monitor] の順に選択します。

[Health Monitor] ページが表示されます。

ステップ 2　アプライアンス リストを展開して特定のステータスを持つアプライアンスを表示するには、そのステータス行内の矢印をクリックします。

ヒント　ステータス レベルに関する行内の矢印が下を向いている場合は、そのステータスのアプライアンス リストが下側のテーブルに表示されます。矢印が右を向いている場合、アプライアンス リストは非表示です。

ステップ 3　アプライアンス リストの [Appliance] 列で、詳細を表示するアプライアンスの名前をクリックします。

[Health Monitor Appliance] ページが表示されます。

ステップ 4　[Generate Troubleshooting Files] をクリックします。

[Troubleshooting Options] ポップアップ ウィンドウが表示されます。

ステップ 5　[All Data] を選択して可能性のあるすべてのトラブルシューティング データを生成することも、個別のチェック ボックスをオンにしてレポートをカスタマイズすることもできます。詳細については、選択可能なトラブルシュート オプションの表を参照してください。

ステップ 6　[OK] をクリックします。

防御セ ン タ ーがトラブルシューティング ファイルを生成します。タスク キュー（[System] > [Monitoring] > [Task Status]）でファイル生成プロセスを監視できます。

ステップ 7　次の項（トラブルシューティング ファイルのダウンロード）の手順に進みます。

トラブルシューティング ファイルのダウンロード

ライセンス: すべて

次の手順を使用して、生成されたトラブルシューティング ファイルのコピーをダウンロードします。

トラブルシューティング ファイルをダウンロードする方法:

アクセス: Admin/Maint/Any Security Analyst

ステップ 1 [System] > [Monitoring] > [Task Status] の順にクリックします。

[Task Status] ページが表示されます。

ステップ 2 生成されたトラブルシューティング ファイルに対応するタスクを探します。

ステップ 3 アプライアンスがトラブルシューティング ファイルを生成し、タスク ステータスが [Completed] に変ったら、[Click to retrieve generated files] をクリックします。

ステップ 4 ブラウザのプロンプトに従ってファイルをダウンロードします。

ファイルは単一の `.tar.gz` ファイルとしてダウンロードされます。

ステップ 5 サポートの指示に従って、トラブルシューティング ファイルをCiscoに送信してください。

ヘルス イベントの操作

ライセンス: すべて

防御センター には、ヘルス モニタによって収集されたヘルス ステータス イベントを迅速かつ容易に分析するための完全にカスタマイズ可能なイベント ビューがあります。このイベント ビューでは、イベント データを検索して表示したり、調査中のイベントに関係する他の情報に簡単にアクセスしたりできます。

ヘルス イベント ビュー ページで実行可能なさまざまな機能がすべてのイベント ビュー ページで一貫しています。これらの一般的な手順の詳細については、ヘルス イベント ビューについて (68-52 ページ)を参照してください。

[Health] > [Health Events] メニュー オプションで、ヘルス イベントを表示したり、特定のイベントを検索したりできます。

イベントの表示について詳しくは、次の項を参照してください。

- ヘルス イベント ビューについて (68-52 ページ)では、FireSIGHT が生成するイベントの種類について説明します。
- ヘルス イベントの表示 (68-53 ページ)では、[Event View] ページへのアクセス方法と使用方法について説明します。
- ヘルス イベントの検索 (68-60 ページ)では、[Event Search] ページを使用して特定のイベントを検索する方法について説明します。

ヘルス イベント ビューについて

ライセンス: すべて

防御センター ヘルス モニタはヘルス イベントを記録し、記録されたヘルス イベントは [Health Event View] ページで表示できます。ヘルス モジュールごとにテストされる条件を理解していれば、ヘルス イベントに対するアラートをより効率的に設定できます。ヘルス イベントを生成するヘルス モジュールのタイプの詳細については、ヘルス モジュールについて (68-3 ページ)を参照してください。

ヘルス イベントの表示方法と検索方法については、次の項を参照してください。

- ヘルス イベントの表示（68-53 ページ）
- ヘルス イベント テーブルについて（68-59 ページ）
- ヘルス イベントの検索（68-60 ページ）

ヘルス イベントの表示

ライセンス： すべて

ヘルス モニタによって収集されたアプライアンス ヘルス データはさまざまな方法で表示できます。

詳細については、次のトピックを参照してください。

- すべてのステータス イベントの表示（68-53 ページ）
- モジュールとアプライアンス別のヘルス イベントの表示（68-54 ページ）
- ヘルス イベント テーブル ビューの操作（68-55 ページ）
- 3D9900 デバイスのハードウェア アラート詳細の解釈（68-56 ページ）
- シリーズ 3 デバイスのハードウェア アラート詳細の解釈（68-57 ページ）

すべてのステータス イベントの表示

ライセンス： すべて

[Table View of Health Events] ページには、選択したアプライアンス上のすべてのヘルス イベントのリストが表示されます。このページに表示されるイベントを生成したヘルス モジュールについては、ヘルス モジュールについて（68-3 ページ）を参照してください。

防御センター上の [Health Monitor] ページからヘルス イベントにアクセスした場合は、すべての管理対象アプライアンスのすべてのヘルス イベントが表示されます。

すべての管理対象アプライアンス上のすべてのステータス イベントを表示する方法：

アクセス： Admin/Maint/Any Security Analyst

ステップ 1　[Health] > [Health Events] の順に選択します。

[Events] ページが開いて、すべてのヘルス イベントが表示されます。

注　イベントが表示されない場合は、時間範囲を調整する必要があります。詳細については、イベント時間の制約の設定（58-26 ページ）を参照してください。

ヒント　このビューをブックマークすれば、イベントの [Health Events] テーブルを含むヘルス イベント ワークフロー内のページに戻ることができます。ブックマークしたビューには、現在見ている時間範囲内のイベントが表示されますが、必要に応じて時間範囲を変更してテーブルを最新情報で更新することができます。詳細については、イベント時間の制約の設定（58-26 ページ）を参照してください。

モジュールとアプライアンス別のヘルス イベントの表示

ライセンス：すべて

特定のアプライアンス上の特定のヘルス モジュールによって生成されたイベントを問い合わせることができます。

特定のモジュールのヘルス イベントを表示する方法：

アクセス：Admin/Maint/Any Security Analyst

ステップ 1　[Health] > [Health Monitor] の順に選択します。

[Health Monitor] ページが表示されます。

ステップ 2　アプライアンス リストを展開して特定のステータスを持つアプライアンスを表示するには、そのステータス行内の矢印をクリックします。

ヒント　ステータス レベルに関する行内の矢印が下を向いている場合は、そのステータスのアプライアンス リストが下側のテーブルに表示されます。矢印が右を向いている場合、アプライアンス リストは非表示です。

ステップ 3　アプライアンス リストの [Appliance] 列で、詳細を表示するアプライアンスの名前をクリックします。

[Health Monitor Appliance] ページが表示されます。

ステップ 4　[Health Monitor Appliance] ページの [Module Status Summary] グラフで、表示するヘルス アラート ステータス カテゴリの色をクリックします。

[Alert Detail] リストが展開して、そのステータス カテゴリの選択されたアプライアンスのヘルス アラートがリストされます。

ステップ 5　イベントのリストを表示するアラートの [Alert Detail] 行で、[Events] をクリックします。

[Health Events] ページが開いて、制限としてアプライアンスの名前と選択したヘルス アラート モジュールの名前を含むクエリーのクエリー結果が表示されます。

イベントが表示されない場合は、時間範囲を調整する必要があります。詳細については、イベント時間の制約の設定（58-26 ページ）を参照してください。

ステップ 6　選択したアプライアンスのすべてのステータス イベントを表示する場合は、[Search Constraints] を展開し、[Module Name] 制限をクリックして削除します。

ヘルス イベント テーブル ビューの操作

ライセンス：すべて

次の表に、[Event View] ページから実行可能な各操作の説明を示します。

表 68-8　　ヘルス イベント ビューの機能

目的	操作
ヘルス イベント ビューに表示される列の内容を確認する	ヘルス イベント テーブルについて（68-59 ページ）で詳細を確認してください。
ヘルス テーブル ビューに表示されるイベントの時刻と日付範囲を変更する	イベント時間の制約の設定（58-26 ページ）で詳細を確認してください。 イベント ビューを時間によって制約している場合は、（グローバルかイベントに特有かに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあることに注意してください。この現象は、アプライアンスの変動時間範囲を設定している場合でも発生する可能性があります。
表示されたイベントをソートする、イベント テーブルに表示する列を変更する、または表示するイベントを制限する	ドリルダウン ワークフロー ページのソート（58-38 ページ）で詳細を確認してください。
ヘルス イベントを削除する	削除するイベントの横にあるチェック ボックスをオンにして、[Delete] をクリックします。現在制限されているビューですべてのイベントを削除するには、[Delete All] をクリックしてから、すべてのイベントを削除することを確認します。
イベント ビュー ページ間を移動する	ワークフロー内の他のページへのナビゲート（58-39 ページ）で詳細を確認してください。
他のイベント テーブルに移動して関連イベントを表示する	ワークフロー間のナビゲート（58-40 ページ）で詳細を確認してください。
現在のページをブックマークしてすばやくそこに戻れるようにする	[Bookmark This Page] をクリックして、ブックマークの名前を指定し、[Save] をクリックします。詳細については、「ブックマークの使用（58-41 ページ）」を参照してください。
ブックマーク管理ページに移動する	イベント ビューで [View Bookmarks] をクリックします。詳細については、「ブックマークの使用（58-41 ページ）」を参照してください。
テーブル ビュー内のデータに基づいてレポートを生成する	[Report Designer] をクリックします。詳細については、「イベント ビューからのレポート テンプレートの作成（57-10 ページ）」を参照してください。
別のヘルス イベント ワークフローを選択する	[(switch workflow)] をクリックします。詳細については、「ワークフローの選択（58-18 ページ）」を参照してください。
1 つのヘルス イベントに関連付けられた詳細を表示する	イベントの左側にある下矢印リンクをクリックします。
複数のヘルス イベントのイベント詳細を表示する	詳細を表示するイベントに対応する行の横にあるチェック ボックスをオンにしてから、[View] をクリックします。

表 68-8　ヘルス イベント ビューの機能（続き）

目的	操作
ビュー内のすべてのイベントのイベント詳細を表示する	[View All] をクリックします。
特定のステータスのすべてのイベントを表示する	そのステータスを持つイベントの [Status] 列内のステータス アイコンをクリックします。

3D9900 デバイスのハードウェア アラート詳細の解釈

ライセンス: すべて

3D9900 デバイス モデルでは、次の表に示すイベントに応答してハードウェア アラームが生成されます。トリガー条件はアラートのメッセージ詳細で見つけることができます。

表 68-9　3D9900 デバイスの監視対象条件

監視対象条件	黄色または赤色エラー状態の原因
NFE カードの存在	アプライアンスに対して無効な NFE ハードウェアが検出されると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細に NFE カードの存在への参照が追加されます。
NFE 温度	NFE 温度が 95 ℃を超えると、ハードウェア アラーム モジュールのヘルス ステータスが黄色に変化し、メッセージ詳細に NFE 温度への参照が追加されます。 NFE 温度が 99 ℃を超えると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細に NFE 温度への参照が追加されます。
NFE プラットフォーム デーモン	NFE プラットフォーム デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
NFE メッセージ デーモン	NFE メッセージ デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
NFE `TCAM` デーモン	NFE `TCAM` デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
LBIM の存在	ロード バランシング インターフェイス モジュール（LBIM）スイッチ アセンブリが存在しないか、通信していない場合は、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細に LBIM の存在への参照が追加されます。
`Scmd` デーモン	`Scmd` デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
`Psls` デーモン	`Psls` デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。

表 68-9　3D9900 デバイスの監視対象条件（続き）

監視対象条件	黄色または赤色エラー状態の原因
Ftwo デーモン	Ftwo デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
Rulesd（ホスト ルール）デーモン	Rulesd デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが黄色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
nfm_ipfragd（ホスト フラグ）デーモン	nfm_ipfragd デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。

シリーズ 3 デバイスのハードウェア アラート詳細の解釈

シリーズ 3 デバイスでは、次の表に示すイベントに応答してハードウェア アラームが生成されます。トリガー条件がアラートのメッセージ詳細に表示されます。

表 68-10　シリーズ 3 デバイスの監視対象条件

監視対象条件	黄色または赤色エラー状態の原因
クラスタ ステータス	クラスタ化されたデバイスが相互に通信していない（ケーブル配線の問題などで）場合は、ハードウェア アラーム モジュールが赤色に変化します。
ftwo デーモン ステータス	ftwo デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
検出された NFE カード	システム上で検出された NFE カードの枚数を示します。この値がアプライアンスの予想 NFE カウントと一致しない場合は、ハードウェア アラーム モジュールが赤色に変化します。
NFE ハードウェア ステータス	1 つ以上の NFE カードが通信していない場合は、ハードウェア アラーム モジュールが赤色に変化し、該当するカードがメッセージ詳細に表示されます。
NFE ハートビート	システムが NFE ハートビートを検出しなかった場合は、ハードウェア アラーム モジュールが赤色に変化し、メッセージ詳細に関連カードへの参照が追加されます。
NFE 内部リンク ステータス	NMSB カードと NFE カード間のリンクがダウンした場合は、ハードウェア アラーム モジュールが赤色に変化し、メッセージ詳細に関連ポートへの参照が追加されます。
NFE メッセージ デーモン	NFE メッセージ デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。

表 68-10　シリーズ 3 デバイスの監視対象条件（続き）

監視対象条件	黄色または赤色エラー状態の原因
NFE 温度	NFE 温度が 97 ℃を超えると、ハードウェア アラーム モジュールのヘルス ステータスが黄色に変化し、メッセージ詳細に NFE 温度への参照（および該当する場合は NFE カード番号）が追加されます。 NFE 温度が 102 ℃を超えると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細に NFE 温度への参照（および該当する場合は NFE カード番号）が追加されます。
NFE 温度ステータス	特定の NFE カードの現在の温度ステータスを示します。OK の場合ハードウェア アラーム モジュールは緑色を、Warning の場合は黄色を、Critical の場合は赤色（および該当する場合は NFE カード番号）を示します。
NFE TCAM デーモン	NFE TCAM デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。
nfm_ipfragd（ホスト フラグ）デーモン	nfm_ipfragd デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。
NFE プラットフォーム デーモン	NFE プラットフォーム デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。
NMSB コミュニケーション	メディア アセンブリが存在しないか、通信していない場合は、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細に NFE 温度への参照（および該当する場合は NFE カード番号）が追加されます。
psls デーモン ステータス	psls デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
Rulesd（ホスト ルール）デーモン	Rulesd デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが黄色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。
scmd デーモン ステータス	scmd デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。

ヘルス イベント テーブルについて

ライセンス： すべて

防御センターのヘルス モニタを使用して、FireSIGHT システム内の重要な機能のステータスを確認できます。ハードウェア ステータスやソフトウェア ステータスなどのさまざまな側面を監視するため正常性ポリシーを作成してアプライアンスに適用します。正常性ポリシー内で有効にされたヘルス モニタ モジュールが、さまざまなテストを実行してアプライアンスのヘルス ステータスを特定します。ヘルス ステータスが指定された基準を満たしている場合は、ヘルス イベントが生成されます。ヘルス モニタリングの詳細については、システムのモニタリング（67-1 ページ）を参照してください。

ヘルス イベント テーブル内のフィールドについて、次の表で説明します。

表 68-11　　ヘルス イベント フィールド

フィールド	説明
Test Name	イベントを生成したヘルス モジュールの名前。ヘルス モジュールのリストについては、ヘルス モジュールを参照してください。
時刻	ヘルス イベントのタイムスタンプ。
説明	イベントを生成したヘルス モジュールの説明。たとえば、プロセスが実行できない場合に生成されるヘルス イベントには [Unable to Execute] というラベルが付けられます。
値	イベントが生成されたヘルス テストから得られた結果の値（単位数）。 たとえば、監視対象デバイスが 80% 以上の CPU リソースを使用しているときに生成されるヘルス イベントを防御センターが生成した場合の値は 80 ～ 100 です。
単位	結果の単位記述子。アスタリスク（*）を使用してワイルドカード検索を作成できます。 たとえば、監視対象デバイスが 80% 以上の CPU リソースを使用しているときに生成されるヘルス イベントを防御センターが生成した場合の単位記述子はパーセント記号（%）です。
Status（ステータス）	アプライアンスに報告されるステータス（Critical、Yellow、Green、または Disabled）。
デバイス	ヘルス イベントが報告されたアプライアンス。

ヘルス イベントのテーブル ビューを表示する方法：

アクセス： Admin/Maint/Any Security Analyst

ステップ 1　[Health] > [Health Events] の順に選択します。

テーブル ビューが表示されます。ヘルス イベントの操作方法については、ヘルス イベントの操作（68-52 ページ）を参照してください。

ヒント　ヘルス イベントのテーブル ビューが含まれていないカスタム ワークフローを使用している場合は、[(switch workflow)] をクリックします。[Select Workflow] ページで、[Health Events] をクリックします。

ヘルス イベントの検索

ライセンス：すべて

特定のヘルス イベントを検索できます。ネットワーク環境に合わせてカスタマイズされた検索を作成して保存すれば、後で再利用できます。次の表に、使用可能な検索基準の説明を示します。

表 68-12　ヘルス イベントの検索基準

検索フィールド	説明
モジュール名	表示するヘルス イベントを生成したモジュールの名前を指定します。たとえば、CPU パフォーマンスを測定するイベントを表示するには、「CPU」と入力します。検索によって、該当する CPU 使用率イベントと CPU 温度イベントが取得されるはずです。
値	表示するイベントのヘルス テストから得られた結果の値（単位数）を指定します。 たとえば、値として 15 を指定し、[Units] フィールドに「CPU」と入力した場合は、テストの実行時点でアプライアンス CPU が 15% の使用率で動作していたイベントが取得されます。
説明	表示するイベントの説明を指定します。たとえば、プロセスが実行できなかったヘルス イベントを表示するには、「Unable to Execute」と入力します。このフィールドでアスタリスク（*）を使用してワイルドカード検索を作成できます。
単位	表示するイベントのヘルス テストから得られた結果の単位記述子を指定します。このフィールドでアスタリスク（*）を使用してワイルドカード検索を作成できます。 たとえば、[Units] フィールドに「%」と入力した場合は、ディスク使用率モジュールの [Units] フィールドに「%」というラベルが付けられる（そして追加のテキストがない）ため、ディスク使用率モジュールに関するすべてのイベントが取得されます。ただし、[Units] フィールドに「*%」と入力した場合は、[Units] フィールド内のテキストの最後に「%」記号が付いているモジュールに関するすべてのイベントが取得されます。
Status（ステータス）	表示するヘルス イベントのステータスを指定します。有効なステータス レベルは、Critical、Warning、Normal、Error、および Disabled です。 たとえば、Critical ステータスを示すすべてのヘルス イベントを取得するには、「Critical」と入力します。
デバイス	検索を 1 つ以上の特定のデバイスによって生成されたヘルス イベントに制限するには、デバイス名か IP アドレス、またはデバイス グループ名、スタック名、またはクラスタ名を入力します。FireSIGHT システム が検索でデバイス フィールドを処理する方法については、検索でのデバイスの指定（60-7 ページ）を参照してください。

特殊な検索構文や検索の保存とロードに関する情報を含む検索の詳細については、検索設定の実行と保存（60-1 ページ）を参照してください。

ヘルス イベントを検索する方法：

アクセス：Admin/Maint/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　テーブルのドロップダウン リストから [Health Events] を選択します。

ページが適切な制約によって更新されます。

ステップ 3　表ヘルス イベントの検索基準に記載されているように、該当するフィールドに検索基準を入力します。

複数の基準を入力した場合は、すべての基準を満たすレコードだけが検索で返されます。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　カスタム ユーザ ロールに関するデータ制約として検索を使用する予定の場合は、それをプライベート検索として保存する**必要があります**。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存されて（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

- 新しい検索を保存するか、以前保存した検索の変更によって作成した検索に名前を割り当てるには、[Save As New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

現在の時刻範囲に制限された検索結果がデフォルト ヘルス イベント ワークフローに表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

システムの監査

システム上のアクティビティを 2 つの方法で監査できます。FireSIGHT システムに含まれるアプライアンスは、Web インターフェイスとのユーザ インタラクションごとに監査レコードを生成し、システム ログ内にシステム ステータス メッセージも記録します。

以下の項では、システムに備わっているモニタリング機能について詳しく説明します。

- 監査レコードの管理（69-1 ページ）では、システムの監査情報を表示および管理する方法について説明します。
- システム ログの表示（69-10 ページ）では、システム ステータス メッセージを含むシステム ログの表示方法について説明します。

ヒント また、Protectionライセンスを持つ管理対象デバイスおよびDefense Centerに備わっているフル レポート機能を使用すると、監査データを含む、イベント ビューからアクセス可能なほぼすべての種類のデータのレポートを作成できます。詳細については、レポートの操作（57-1 ページ）を参照してください。

監査レコードの管理

ライセンス： すべて

Defense Centerおよび管理対象デバイスは、ユーザ アクティビティに関する読み取り専用の監査情報をログに記録します。監査ログは標準のイベント ビューに表示され、監査ビュー内の任意の項目に基づいて監査ログ メッセージを表示、ソート、およびフィルタリングできます。監査情報を簡単に削除したり、それに関するレポートを作成したりすることができ、ユーザが行った変更に関する詳細なレポートを表示することもできます。

監査ログには最大 100,000 個のエントリが保存されます。監査ログ エントリの数が 100,000 を超えると、アプライアンスはデータベースから最も古いデータをプルーニングし、その数を 100,000 まで減らします。

注 シリーズ 3 アプライアンスをリブートした直後にすばやく CLI にログインした場合、そこで実行するコマンドは、Web インターフェイスが使用可能になるまでは監査ログに記録されません。

詳細については、次の項を参照してください。

- 監査レコードの表示（69-2 ページ）
- 監査レコードの抑制（69-4 ページ）

監査レコードの表示

ライセンス： すべて

アプライアンスを使用して監査レコードのテーブルを表示できます。その後、探している情報に応じて表示方法を操作できます。事前定義された監査ワークフローには、イベントを示す単一のテーブル ビューが含まれます。このほか、特定の要件に一致する情報のみを表示するカスタム ワークフローを作成することもできます。カスタム ワークフローの作成については、カスタム ワークフローの作成（58-43 ページ）を参照してください。

次の表では、監査ログ ワークフローのページで実行できる操作をいくつか説明します。

表 69-1　監査ログの操作

目的	操作
テーブル内のカラムの内容について理解する	監査ログ テーブルについて（69-7 ページ）にある詳細情報を参照してください。
監査レコードを表示する際に使われる時間範囲を変更する	詳細については、イベント時間の制約の設定（58-26 ページ）を参照してください。 イベント ビューを時間によって制約している場合は、（グローバルかイベントに特有かに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあることに注意してください。アプライアンスでスライド時間枠を設定した場合でも、これが発生する可能性があります。
現在のワークフロー ページでイベントをソートおよび制約する	テーブル ビュー ページのソートおよびレイアウトの変更（58-37 ページ）にある詳細情報を参照してください。
現在のワークフロー ページ内を移動する	詳細については、ワークフロー内の他のページへのナビゲート（58-39 ページ）で確認できます。
現在の制約を保持したまま、現行のワークフローのページ間を移動する	ワークフロー ページの左上にある、該当するページのリンクをクリックします。詳細については、ワークフローのページの使用（58-21 ページ）を参照してください。
ワークフロー内の次のページにドリルダウンする	次のいずれかの方法を使用します。 • 特定の値に制約している次のワークフロー ページにドリルダウンするには、対象のロー内の値をクリックします。この操作はドリルダウン ページでのみ可能です。テーブル ビューの行内の値をクリックすると、テーブル ビューが制約されます（次のページにはドリルダウン**されません**）。 • いくつかのイベントによって制約したまま次のワークフロー ページにドリルダウンするには、次のワークフロー ページに表示させるイベントの横のチェック ボックスを選択し、[View] をクリックします。 • 現行の制約を保持したまま次のワークフロー ページへドリルダウンするには、[View All] をクリックします。 **ヒント**　テーブル ビューには必ず、ページ名に「Table View」が含まれます。 詳細については、イベントの制約（58-35 ページ）を参照してください。

表 69-1　監査ログの操作（続き）

目的	操作
特定の 1 つの値で制約する	行内の値をクリックします。 ドリルダウン ページで値をクリックすると、次のページに移動し、その値だけに制約されます。 テーブル ビューの行内の値をクリックすると、テーブル ビューが制約されることに注意してください（次のページにはドリルダウン**されません**）。 **ヒント**　テーブル ビューのページ名には、必ず「Table View」が含まれます。 詳細については、イベントの制約（58-35 ページ）を参照してください。
監査レコードの削除	次のいずれかの方法を使用します。 • いくつかの項目を削除するには、削除するイベントの横にあるチェックボックスを選択し、[Delete] をクリックします。 • 現在の制限付きビューにあるすべての項目を削除するには、[Delete All] をクリックした後、すべてのイベントを削除することを確認します。
一時的に別のワークフローを使用する	[(switch workflow)] をクリックします。詳細については、ワークフローの選択（58-18 ページ）を参照してください。
すぐに戻ることができるように現在のページをブックマークする	[Bookmark This Page] をクリックします。詳細については、ブックマークの使用（58-41 ページ）を参照してください。
ブックマークの管理ページに移動する	[View Bookmarks] をクリックします。詳細については、ブックマークの使用（58-41 ページ）を参照してください。
現在のビューのデータに基づいてレポートを生成する	[Report Designer] をクリックします。詳細については、イベント ビューからのレポート テンプレートの作成（57-10 ページ）を参照してください。
監査ログに記録されている変更の概要を表示する	[Message] カラムの該当するイベントの横にある比較アイコン（  ）をクリックします。詳細については、監査ログを使って変更を調査する（69-8 ページ）を参照してください。

監査レコードを表示するには、次のようにします。

アクセス： Admin

ステップ 1　[System] > [Monitoring] > [Audit] を選択します。

デフォルト監査ログ ワークフローの最初のページ（唯一のページ）が表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください。詳細については、イベント時間の制約の設定（58-26 ページ）を参照してください。

ヒント　監査イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(switch workflow)] をクリックし、[Audit Log] を選択します。

監査イベントの操作

ライセンス： すべて

イベント ビューのレイアウトを変更したり、ビュー内のイベントをフィールド値で制限したりできます。カラムを無効にする場合は、非表示にするカラム見出しのクローズ アイコン（ ✖ ）をクリックした後、表示されるポップアップ ウィンドウで [Apply] をクリックします。カラムを無効にすると、あとで再び追加した場合を除き、そのカラムはセッション有効期間にわたって無効になります。最初のカラムを無効にした場合、[Count] カラムが追加されることに注意してください。

他のカラムを表示/非表示にしたり、無効になったカラムをビューに再び追加したりするには、該当するチェック ボックスを選択またはクリアしてから [Apply] をクリックします。

テーブル ビューの行内の値をクリックすると、テーブル ビューが制約されます（次のページにはドリルダウンされません）。

ヒント　テーブル ビューのページ名には必ず「Table View」が含まれます。

詳細については、次のトピックを参照してください。

- イベントの制約（58-35 ページ）。
- 複合的な制約の使用（58-37 ページ）
- ドリルダウン ワークフロー ページのソート（58-38 ページ）
- 監査ログ テーブルについて（69-7 ページ）

監査レコードの抑制

ライセンス： すべて

監査ポリシーで、FireSIGHT システム/ユーザ間の特定のタイプのインタラクションを監査する必要がない場合は、それらのインタラクションによって監査レコードが生成されないように設定できます。たとえば、デフォルトでは、ユーザーがオンライン ヘルプを表示するたびに、FireSIGHT システムは監査レコードを生成します。このようなインタラクションのレコードを保持する必要がない場合は、これらを自動的に抑制できます。

監査イベントの抑制を設定するには、アプライアンスの `admin` ユーザー アカウントにアクセスできる必要があり、アプライアンスのコンソールにアクセスできる（またはセキュア シェルを開くことができる）必要があります。

注意　許可された担当者だけが、アプライアンスとその `admin` アカウントにアクセスできることを確認してください。

監査レコードを抑制するには、次の形式の 1 つ以上のファイルを `/etc/sf` ディレクトリに作成する必要があります。

```
AuditBlock.type
```

ここで、*`type`* は `address`、`message`、`subsystem`、または `user` です。

注　特定のタイプの監査メッセージに関する AuditBlock.*type* ファイルを作成した後、もはやそれらを抑制しないことを決定した場合、AuditBlock.*type* ファイルの内容を削除する必要がありますが、ファイル自体は FireSIGHT システムに残してください。

それぞれの監査ブロック タイプの内容は、次の表に示すような特定の形式でなければなりません。ファイル名の大文字/小文字を必ず正しく表記してください。また、ファイルの内容でも大文字と小文字が区別されることに注意してください。

表 69-2　監査ブロック タイプ

タイプ	説明
住所	AuditBlock.address という名前のファイルを作成し、監査ログから抑制する IP アドレスを 1 行に 1 つずつ含めます。部分的な IP アドレスを使用できます（ただしアドレスの先頭から照合されます）。たとえば、部分的なアドレス 10.1.1 は、10.1.1.0 から 10.1.1.255 までのアドレスと一致します。
メッセージ	AuditBlock.message という名前のファイルを作成し、抑制するメッセージ部分文字列を 1 行に 1 つずつ含めます。 たとえば backup をこのファイルに含めた場合、部分文字列の照合により backup という語を含むすべてのメッセージが抑制されることに注意してください。
サブシステム	AuditBlock.subsystem という名前のファイルを作成し、抑制するサブシステムを 1 行に 1 つずつ含めます。 部分文字列は照合**されない**ことに注意してください。正確な文字列を使用する必要があります。監査されるサブシステムのリストについては、サブシステム名の表を参照してください。
User	AuditBlock.user という名前のファイルを作成し、抑制するユーザ アカウントを 1 行に 1 つずつ含めます。部分的な文字列の照合を使用できます（ただしユーザ名の先頭から照合されます）。たとえば、部分的なユーザ名 IPSAnalyst はユーザ名 IPSAnalyst1 および IPSAnalyst2 と一致します。

AuditBlock ファイルを追加した場合、サブシステム Audit およびメッセージ Audit Filter *type* Changed を含む監査レコードが監査イベントに追加されることに注意してください。セキュリティ上の理由から、この監査レコードを抑制することは**できません**。

次の表に、監査されるサブシステムを示します。

表 69-3　サブシステム名

名前	どの機能のユーザ インタラクションを含んでいるか
Admin	管理機能：システムとアクセス権の設定、時刻の同期、バックアップと復元、デバイス管理、ユーザ アカウントの管理、スケジュール設定など
アラート	アラート機能：電子メール、SNMP、syslog アラートなど
監査ログ	監査イベントの表示
Audit Log Search	監査イベントの検索
Command Line	コマンドライン インターフェイス
設定（Configuration）	電子メール アラート機能

表 69-3　サブシステム名（続き）

名前	どの機能のユーザ インタラクションを含んでいるか
COOP	継続的な運用機能
日付	イベント ビューの日時範囲
Default Subsystem	サブシステムが割り当てられていないオプション
Detection & Prevention Policy	侵入ポリシーのメニュー オプション
Error	システム レベルのエラー
eStreamer	eStreamer の設定
EULA	エンド ユーザ ライセンス契約書の確認
Event	侵入およびディスカバリ イベント ビュー
Events Clipboard	侵入イベント クリップボード
Events Reviewed	レビューされた侵入イベント
Events Search	イベント検索
Failed to install rule update *rule_update_id*	ルール更新のインストール
Header	ユーザ ログイン後のユーザ インターフェイスの最初の表示
状態	ヘルス モニタリング
Health Events	ヘルス モニタリング イベントの表示
Help	オンライン ヘルプ
High Availability（高可用性）	高可用性（ハイ アベイラビリティ）機能
IDS Impact Flag	影響フラグの設定
IDS Policy	侵入ポリシー
IDSPolicy > *policy_name* > Appliance > *det_engine_name*	侵入ポリシーの適用
IDSRule sid:*sig_id* rev:*rev_num*	SID による侵入ルール
インシデント	侵入インシデント
Insert Policy Apply Job	ポリシーの適用
インストールするもの	更新のインストール
Intrusion Events	侵入イベント
ログイン	Web インターフェイスのログイン/ログアウト機能
メニュー	メニュー オプション
Configuration export > *config_type* > *config_name*	特定のタイプ/名前の設定のインポート
Permission Escalation	ユーザ ロールのエスカレーション
プリファレンス	ユーザ アカウントのタイム ゾーンや個々のイベント設定などのユーザ設定
ポリシー（Policy）	侵入ポリシーを含むポリシー
Register	Defense Centerでのデバイスの登録
RemoteStorageDevice	リモート ストレージ デバイスの設定

表 69-3　サブシステム名（続き）

名前	どの機能のユーザ インタラクションを含んでいるか
レポート	レポート リスト機能およびレポート デザイナ機能。
ルール	侵入ルール（ルール エディタとルールのインポート プロセスを含む）
Rule Update Import Log	ルール更新のインポート ログの表示
Rule Update Install	ルール更新のインストール
Status（ステータス）	syslog およびホストやパフォーマンスの統計情報
システム	システム全体のさまざまな設定
System Policy > *policy_name* Appliance > *appliance_name*	システム ポリシーの適用
Task Queue	タスク キューの表示
ユーザ	ユーザ アカウントとロールの作成および変更

監査ログ テーブルについて

ライセンス： すべて

各アプライアンスは、Web インターフェイスとのユーザ インタラクションごとに 1 つの監査イベントを生成します。各イベントには、タイムスタンプ、イベントを発生させたアクションを行ったユーザ名、発信元 IP、およびイベントの説明テキストが含まれます。監査ログ テーブルのフィールドについて、以下の表で説明します。

表 69-4　監査ログのフィールド

フィールド	説明
時刻	アプライアンスが監査レコードを生成した日時。
User	監査イベントをトリガーとして使用したユーザのユーザ名。
Subsystem	監査レコードが生成されたときにユーザがたどったメニュー パス。たとえば、[System] > [Monitoring] > [Audit] は、監査ログを表示するためのメニュー パスです。 メニュー パスが該当しない数少ないケースでは、[Subsystem] フィールドにイベント タイプのみが表示されます。たとえば、**Login** はユーザのログイン試行を分類します。
メッセージ	ユーザが実行した操作。 たとえば、`Page View` は [Subsystem] で示されたページをユーザが単に表示したことを意味します。`Save` は、ユーザがページの [Save] ボタンをクリックしたことを意味します。 FireSIGHT システムで行われた変更は比較アイコン（）付きで表示され、これをクリックすると変更の概要を表示できます。詳細については、監査ログを使って変更を調査する（69-8 ページ）を参照してください。
Source IP	ユーザが使用したホストに関連付けられている IP アドレス。
Count	各行に表示される情報と一致するイベントの数。[Count] フィールドは、制約を適用した後に 2 つ以上の同一行が生じた場合にのみ表示されることに注意してください。

監査ログを使って変更を調査する

ライセンス： すべて

監査ログを使用して、システムの変更に関する詳細レポートを表示できます。これらのレポートは、現在のシステム設定を、特定の変更が行われる直前の設定と比較します。

システムの変更を表す監査ログ イベントの横には比較アイコン（）が表示されます。比較アイコンをクリックすると、[Compare Configurations] ページにアクセスし、変更についての詳細レポートを表示できます。

[Compare Configurations] ページには、変更前のシステム設定と、現在実行中の設定との違いが横並び形式で表示されます。監査イベント タイプ、最終変更時間、および変更を行ったユーザ名が、各設定の上のタイトル バーに表示されます。

2 つの設定の違いは次のように強調表示されます。

- 青は、強調表示されている設定項目が 2 つの設定間で異なっていることを示し、異なっている部分は赤のテキストで表示されます。
- グリーンは、強調表示されている設定項目が一方の設定に含まれ、もう一方の設定には含まれないことを示します。

監査ログで変更を調査するには、次のようにします。

アクセス： Admin

ステップ 1　[System] > [Monitoring] > [Audit] を選択します。

デフォルト監査ログ ワークフローの最初のページが表示されます。

監査イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(switch workflow)] をクリックし、[Audit Log] を選択します。

ステップ 2　[Message] カラムの該当する監査ログ イベントの横にある比較アイコン（）をクリックします。

[Compare Configurations] ページが表示されます。タイトル バーの上の [Previous] または [Next] をクリックすると、個々の変更の間を移動できます。また、変更の概要が複数のページにまたがる場合は、右側のスクロール バーを使って追加の変更を表示できます。

監査レコードの検索

ライセンス： すべて

監査レコードを検索して、特定のユーザ、サブシステム、または監査レコード メッセージに固有の情報を見つけることができます。

実際のネットワーク環境に合わせてカスタマイズされた検索を作成して保存すると、あとで再利用できます。使用できる検索条件を次の表に示します。監査の検索では、大文字と小文字が区別されないことに注意してください。たとえば、`Analyst01` と `analyst01` を検索すると同じ結果になります。

表 69-5　監査レコードの検索条件

検索フィールド	説明	例
User	対象となる監査イベントをトリガーとして使用したユーザを示すユーザ名を入力します。このフィールドでは、アスタリスク（*）をワイルドカード文字として使用できます。	`jsmith` を指定すると、jsmith というユーザに関連したすべての監査レコードが返されます。
Subsystem	対象となる監査レコードが生成されたときにユーザがたどった完全メニュー パスを入力します。このフィールドでは、アスタリスク（*）をワイルドカード文字として使用できます。	たとえば、[System] > [Monitoring] > [Audit] および `*Audit` のどちらを指定した場合も、監査ログの使用に関連した監査レコードが返されます。 `*Audit*` の場合、上記のレコードに加えて、監査レコードの検索に関連したレコードも返されます。
メッセージ	ユーザが実行したアクション、またはユーザーがページでクリックしたボタン。このフィールドでは、アスタリスク（*）をワイルドカード文字として使用できます。	`Apply` を指定すると、ユーザが侵入ポリシーを適用した監査レコードが返されます。 `Save Rule` を指定すると、ユーザが相関ルールを保存した監査レコードが返されます。 `Page View` を指定すると、ユーザがページを表示した監査レコードが返されます。
時刻	監査レコードが生成された日時を指定します。時間入力の構文については、検索での時間制約の指定（60-5 ページ）を参照してください。	`> 2006-01-15 13:30:00` を指定すると、2006 年 1 月 15 日午後 1 時 30 分以降に生成されたすべての監査レコードが返されます。
Source IP	対象となる監査レコードに関連するホストの IP アドレスを入力します。 **注**　具体的な IP アドレスを入力する**必要があります**。監査ログを検索するときには IP 範囲を使用できません。	`172.16.1.37` を指定すると、IP アドレス 172.16.1.37 からユーザによって生成されたすべての監査レコードが返されます。
構成の変更内容	構成の変更に関する監査レコードを表示するかどうかを指定します。	`yes` を指定すると、構成変更の監査レコードが返されます。

保存済みの検索をロードしたり削除したりする方法など、検索の詳細については、イベントの検索（60-1 ページ）を参照してください。

監査レコードを検索するには、次のようにします。

アクセス： Admin

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　テーブルのドロップダウン リストから、[Audit Log Events] を選択します。

監査ログ（Audit Log）の検索ページが表示されます。

ヒント　データベース内で別の種類のイベントを検索するには、テーブルのドロップダウン リストから選択します。

ステップ 3　監査レコードの検索条件の表に示すように、該当するフィールドに検索条件を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。

ステップ 4　必要に応じて検索を保存する場合は、[Private] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　カスタム ユーザ ロールに対するデータの制約として検索を使用する場合は、検索を非公開として保存する**必要があります**。

ステップ 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [Save] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[Save As New] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [Save] をクリックします。検索が保存され（[Private] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

ステップ 6　検索を開始するには、[Search] ボタンをクリックします。

現在の時刻範囲によって制約されたデフォルト監査ログ ワークフローに、検索結果が表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

システム ログの表示

ライセンス： すべて

システム ログ（syslog）ページは、アプライアンスのシステム ログ情報を示します。システム ログには、システムによって生成された各メッセージが表示されます。次の項目が順にリストされます。

- メッセージが生成された日付
- メッセージが生成された時刻
- メッセージを生成したホスト
- メッセージ本体

注　システム ログ情報はローカルです。たとえば、Defense Centerを使用して、管理対象デバイスのシステム ログ内のシステム ステータス メッセージを見ることは**できません**。

フィルタリング機能を使用すると、特定のコンポーネントのシステム ログ メッセージを表示できます。詳細については、システム ログ メッセージのフィルタリング (69-11 ページ) を参照してください。

syslog を表示するには、次のようにします。

アクセス: Admin/Maint

ステップ 1　[System] > [Monitoring] > [Syslog] を選択します。

[System Log] ページが表示されます。

ヒント　3D9900 の場合、ロード バランシング インターフェイス モジュール (LBIM) がメッセージをデバイスの syslog に転送します。`lbim` でフィルタリングすることで、これらのメッセージを見つけることができます。

システム ログ メッセージのフィルタリング

ライセンス: すべて

フィルタリング機能を使用すると、特定のコンポーネントのシステム ログ メッセージを表示できます。フィルタリングにより、メッセージ内容に基づいて特定のメッセージを検索できます。

フィルタリング機能は、UNIX ファイル検索ユーティリティ Grep を使用するため、Grep で使用可能なほとんどの構文を使用できます。つまり、たとえばパターン マッチング用に Grep 互換の正規表現を使用できます。単一の語をフィルタとして使用したり、Grep でサポートされる正規表現を使用したりして内容を検索できます。

次の表に、システム ログ フィルタで使用できる正規表現構文を示します。

表 69-6　システム ログ フィルタ構文

構文のコンポーネント	説明	例
.	任意の文字またはスペースと一致します	`Admi.` は、`Admin`、`AdmiN`、`Admi1`、および `Admi ` と一致します。
`[[:alpha:]]`	任意の英文字と一致します	`[[:alpha:]]dmin` は、`Admin`、`bdmin`、および `Cdmin` と一致します
`[[:upper:]]`	任意の大文字の英文字と一致します	`[[:upper:]]dmin` は、`Admin`、`Bdmin`、および `Cdmin` と一致します
`[[:lower:]]`	任意の小文字の英文字と一致します	`[[:lower:]]dmin` は、`admin`、`bdmin`、および `cdmin` と一致します
`[[:digit:]]`	任意の数字と一致します	`[[:digit:]]dmin` は、`0dmin`、`1dmin`、および `2dmin` と一致します
`[[:alnum:]]`	任意の英数字と一致します	`[[:alnum:]]dmin` は、`1dmin`、`admin`、`2dmin`、および `bdmin` と一致します
`[[:space:]]`	タブを含む、任意のスペースと一致します	`Feb[[:space:]]29` は 2 月 29 日のログと一致します。

表 69-6　システム ログ フィルタ構文(続き)

構文のコンポーネント	説明	例
*	その前にある文字または式のゼロ個以上のインスタンスと一致します	ab* は、a、ab、abb、ca、cab、および cabb と一致します [ab]* はすべてのものと一致します
?	ゼロ個または 1 つのインスタンスと一致します	ab? は、a または ab と一致します。
\	これを使用すると、通常は正規表現構文と解釈される文字を検索できます	alert\? は、alert? と一致します。

次の表では、[System Log] ページで使用できるフィルタの例をいくつか示します。

表 69-7　システム ログ フィルタの例

次の条件を満たすすべてのログ エントリを検索する場合	使用するフィルタ
11 月 5 日に生成された	Nov[[:space:]]*5
ユーザ名「Admin」が含まれる	Admin
11 月 5 日の認証デバッグ情報が含まれる	Nov[[:space:]]*5.*AUTH.*DEBUG

システム ログ内で特定のメッセージ内容を検索するには、次のようにします。

アクセス: Admin/Maint

ステップ 1　[System] > [Monitoring] > [Syslog] を選択します。

[System Log] ページが表示されます。

ステップ 2　フィルタのフィールドに単語またはクエリを入力します。

使用できるフィルタ構文の詳細については、上記の表を参照してください。

注　Grep 互換の検索構文のみがサポートされます。たとえば、フィルタとして ntp を使ってすべての NTP 関連システム ログ メッセージを検索したり、Nov をフィルタとして使って 11 月に生成されたすべてのメッセージを検索したりできます。Nov[[:space:]]*27 または Nov.*27 を使用すると 11 月 27 日のメッセージを表示できますが、Nov 27 または Nov*27 を使ってこれらのメッセージを表示することはできません。

ステップ 3　オプションで、大文字と小文字が区別されるようにするには、[Case-sensitive] をチェックします。(デフォルトでは、フィルタで大文字/小文字は区別されません)。

ステップ 4　オプションで、[Exclusion] をチェックすると、入力した条件に一致**しない**すべてのシステム ログ メッセージが検索されます。

ステップ 5　[Go] をクリックします。

フィルタに一致するメッセージが表示されます。

バックアップと復元の使用

バックアップ/復元は、システム保守プランの重要な部分です。各組織のバックアップ計画は高度に個別化されていますが、FireSIGHT システム には、障害発生時に Defense Center や管理対象デバイスからのデータを復元できるようにデータをアーカイブするためのメカニズムが備わっています。

バックアップと復元に関する次の制限事項に注意してください。

- バックアップは、バックアップを作成した製品バージョンに対してのみ有効です。
- バックアップには、キャプチャされたファイル データは含まれません。
- 管理対象デバイス、Cisco NGIPS for Blue Coat X-Series または Cisco ASA with FirePOWER Services のバックアップ ファイルは作成または復元できません。すべてのイベント データをバックアップするには、管理 Defense Center のバックアップを実行します。
- 代替のアプライアンスにバックアップを復元できるのは、2 台のアプライアンスが同じモデルで、同じバージョンの FireSIGHT システム ソフトウェアを実行している場合のみです。

注意 管理対象デバイス間でコンフィギュレーション ファイルをコピーする目的で、バックアップと復元のプロセスを使用しないでください。コンフィギュレーション ファイルはデバイスを固有に識別する情報を含むため、共有できません。

注意 侵入ルールのアップデートを適用した場合、それらのアップデートはバックアップされません。復元**後に**、最新のルールのアップデートを適用する必要があります。

アプライアンスまたはローカル コンピュータにバックアップ ファイルを保存できます。さらに、Defense Centerを使用している場合は、リモート ストレージの管理（64-17 ページ）で詳述されているように、リモート ストレージを使用できます。

注意 3D9900 上の USB ポートに USB ドライブを挿入しないでください。また、デバイスをアップグレードまたは復元する前に、外部ストレージのあるデバイス（外部ストレージがある KVM スイッチなど）を 3D9900 から削除します。

詳細については、次の項を参照してください。

- Defense Center および物理管理対象デバイスのバックアップ ファイルの作成については、バックアップ ファイルの作成（70-2 ページ）を参照してください。

- バックアップ作成のテンプレートとして後で使用できるバックアップ プロファイルを作成する方法について詳しくは、バックアップ プロファイルの作成（70-6 ページ）を参照してください。
- ローカル ホストからバックアップ ファイルをアップロードする方法について詳しくは、ローカル ホストからのバックアップのアップロード（70-7 ページ）を参照してください。
- アプライアンスにバックアップ ファイルを復元する方法について詳しくは、バックアップ ファイルからのアプライアンスの復元（70-8 ページ）を参照してください。

バックアップ ファイルの作成

ライセンス： すべて

サポートされるデバイス： すべて（仮想、X-Series、および ASA FirePOWER を除く）

サポートされる防御センター： すべて

デバイス自体からの物理管理対象デバイスのバックアップ、管理する Defense Center からの物理管理対象デバイスのバックアップ、および Defense Center のバックアップを実行できます。システムは、実行するバックアップのタイプに応じて異なるデータをバックアップします。システムはキャプチャされたファイル データをバックアップ**しない**ことに注意してください。どのような種類のバックアップを実行するかを決定するには、次の表を使用します。

表 70-1　　バックアップのタイプによって保存されるデータ

バックアップ タイプ	構成データが含まれるか	イベント データが含まれるか	統合ファイルが含まれるか
Defense Center	Yes	Yes	No
デバイス自体から実行される、物理管理対象デバイス	Yes	No	No
管理する Defense Center から実行される、物理管理対象デバイス	Yes	No	Yes

注　仮想管理対象デバイス、Cisco NGIPS for Blue Coat X-Series、Cisco ASA with FirePOWER Services 用にバックアップ ファイルを作成したり復元することは**できません**。イベント データをバックアップするには、管理用のDefense Centerのバックアップを実行します。

既存のシステム バックアップを表示して使用するには、[Backup Management] ページに移動します。イベント データに加えて、アプライアンスの復元に必要なすべてのコンフィギュレーション ファイルを含むバックアップ ファイルを定期的に保存する必要があります。設定の変更をテストする際にも、システムをバックアップして、必要に応じて保存されている設定に戻せるようにすることができます。バックアップ ファイルを、アプライアンスに保存するか、ローカル コンピュータに保存するかを選択できます。

アプライアンスに十分なディスク スペースがない場合は、バックアップ ファイルを作成できません。バックアップ プロセスが使用可能なディスク スペースの 90% 以上を使用する場合、バックアップは失敗することがあります。必要に応じて、古いバックアップ ファイルを削除するか、古いバックアップ ファイルをアプライアンスの外部に転送するか、リモート ストレージを使用してください。

あるいは、バックアップ ファイルが 4GB を超える場合は、SCP 経由でリモート ホストにコピーします。4 GB よりも大きなファイルのアップロードは、Web ブラウザでサポートされていないため、バックアップ ファイルがそのように大きい場合には、ローカル コンピュータからのバックアップのアップロードはできません。Defense Centerでは、バックアップ ファイルをリモート ロケーションに保存できます。詳しくは、リモート ストレージの管理（64-17 ページ）を参照してください。

注　バックアップ タスクがディスカバリ イベントを収集してるとき、データの関連付けは一時的に停止されます。

次の点に注意してください。

- PKI オブジェクトに関連付けられた秘密キーは、アプライアンスに保存されるときに、ランダムに生成されたキーで暗号化されます。PKI オブジェクトに関連付けられた秘密キーを含むバックアップを実行する場合、秘密キーは、暗号化されないバックアップ ファイルに組み込まれる前に復号化されます。バックアップ ファイルを安全な場所に保存します。
- PKI オブジェクトに関連付けられている秘密キーを含むバックアップを復元すると、システムはアプライアンスに保存する前にランダムに生成されたキーでキーを暗号化します。
- バックアップを実行してから確認済みの侵入イベントを削除した場合、そのバックアップによって、削除された侵入イベントは復元されますが確認済みのステータスは復元されません。復元されたそれらの侵入イベントは、[Reviewed Events] の下ではなく [Intrusion Events] の下に表示されます。侵入イベントについて（41-17 ページ）を参照してください。
- 侵入イベントのデータを含むバックアップを、そのデータがすでに含まれているアプライアンスに復元すると、重複したイベントが作成されることになります。これを回避するため、以前の侵入イベント データが含まれていないアプライアンスにのみ、侵入イベント バックアップを復元します。

注意　セキュリティ ゾーンとのインターフェイスのアソシエーションを設定してある場合、それらのアソシエーションはバックアップされません。それらは、復元後に再設定する必要があります。詳細については、セキュリティ ゾーンの操作（3-42 ページ）を参照してください。

Defense Center のバックアップ ファイルの作成するには、次の手順を実行します。

アクセス： Admin/Maint

ステップ 1　[System] > [Tools] > [Backup]/[Restore] を選択します。

[Backup Management] ページが表示されます。

ステップ 2　[Defense Center Backup] をクリックします。

[Create Backup] ページが表示されます。

ステップ 3　[Name] フィールドに、バックアップ ファイルの名前を入力します。英数字、句読記号、およびスペースを使用できます。

ステップ 4　Defense Centerには、さらに以下の 2 つのオプションがあります。

- 設定をアーカイブするには、[Back Up Configuration] を選択します。
- イベント データベース全体をアーカイブするには、[Back Up Events] を選択します。

ステップ 5　オプションで、バックアップの完了時に通知を受けるためには、[Email] チェック ボックスをオンにして、用意されているテキスト ボックスに電子メール アドレスを入力します。

注　電子メール通知を受信するには、メール リレー ホストおよび通知アドレスの設定（63-19 ページ）で説明されているように、リレー ホストを設定する必要があります。

ステップ 6　オプションで、Defense Centerで、セキュアなコピー（SCP）を使用してバックアップ アーカイブを異なるマシンにコピーするには、[Copy when complete] チェック ボックスをオンにしてから、用意されているテキスト ボックスに以下の情報を入力します。

- [Host] フィールドに、バックアップのコピー先となるマシンのホスト名または IP アドレス
- [Path] フィールドに、バックアップのコピー先となるディレクトリへのパス
- [User] フィールドに、リモート マシンへのログインに使用するユーザ名
- [Password] フィールドに、そのユーザ名のパスワード
  パスワードの代わりに SSH 公開キーを使用してリモート マシンにアクセスする場合は、[SSH Public Key] フィールドの内容を、そのマシンの指定ユーザの `authorized_keys` ファイルにコピーします。

このオプションをオフにする場合、バックアップ中に使用された一時ファイルがシステムによってリモート サーバに保存されます。このオプションをオンにする場合は、一時ファイルはリモート サーバに保存**されません**。

ヒント　Ciscoは、システム障害が発生した場合にアプライアンスを復元できるように、バックアップをリモート ロケーションに定期的に保存することを推奨します。

ステップ 7　次の選択肢があります。

- バックアップ ファイルをアプライアンスに保存するには、[Start Backup] をクリックします。

  バックアップ ファイルは `/var/sf/backup` ディレクトリに保存されます。リモート ロケーションをバックアップ ファイルの場所として指定できます。リモート ストレージの管理（64-17 ページ）を参照してください。

  バックアップ プロセスが完了すると、[Restoration Database] ページでファイルを参照できます。バックアップ ファイルを復元する方法について詳しくは、バックアップ ファイルからのアプライアンスの復元（70-8 ページ）を参照してください。
- この設定を後で使用できるバックアップ プロファイルとして保存するには、[Save as New] をクリックします。

  [System] > [Tools] > [Backup]/[Restore] を選択してから [Backup Profiles] をクリックすることにより、バックアップ プロファイルを変更または削除できます。詳細については、「バックアップ プロファイルの作成（70-6 ページ）」を参照してください。

物理管理対象デバイスのバックアップ ファイルをそのデバイス自体から作成するには、次の手順を実行します。

アクセス： Admin/Maint

ステップ 1　[System] > [Tools] > [Backup]/[Restore] を選択します。

[Device Backups] ページが表示されます。

ステップ 2　[Device Backup] をクリックします。

[Create Backup] ページが表示されます。

ステップ 3　[Name] フィールドに、バックアップ ファイルの名前を入力します。英数字、句読記号、およびスペースを使用できます。

ステップ 4　オプションで、バックアップの完了時に通知を受けるためには、[Email] チェック ボックスをオンにして、用意されているテキスト ボックスに電子メール アドレスを入力します。

注　電子メール通知を受信するには、メール リレー ホストおよび通知アドレスの設定（63-19 ページ）で説明されているように、リレー ホストを設定する必要があります。

ステップ 5　オプションで、セキュアなコピー（SCP）を使用してバックアップ アーカイブを異なるマシンにコピーするには、[Copy when complete] チェック ボックスをオンにしてから、用意されているテキスト ボックスに以下の情報を入力します。

- [Host] フィールドに、バックアップのコピー先となるマシンのホスト名または IP アドレス
- [Path] フィールドに、バックアップのコピー先となるディレクトリへのパス
- [User] フィールドに、リモート マシンへのログインに使用するユーザ名
- [Password] フィールドに、そのユーザ名のパスワード
  パスワードの代わりに SSH 公開キーを使用してリモート マシンにアクセスする場合は、[SSH Public Key] フィールドの内容を、そのマシンの指定ユーザの `authorized_keys` ファイルにコピーします。

このオプションをオフにする場合、バックアップ中に使用された一時ファイルがシステムによってリモート サーバに保存されます。このオプションをオンにする場合は、一時ファイルはリモート サーバに保存**されません**。

ヒント　Ciscoは、システム障害が発生した場合にアプライアンスを復元できるように、バックアップをリモート ロケーションに定期的に保存することを推奨します。

ステップ 6　次の選択肢があります。

- バックアップ ファイルをアプライアンスに保存するには、[Start Backup] をクリックします。

  バックアップ ファイルは `/var/sf/backup` ディレクトリに保存されます。Defense Centerでは、リモート ロケーションをバックアップ ファイルの場所として指定できます。リモート ストレージの管理（64-17 ページ）を参照してください。

  バックアップ プロセスが完了すると、[Restoration Database] ページでファイルを参照できます。バックアップ ファイルを復元する方法について詳しくは、バックアップ ファイルからのアプライアンスの復元（70-8 ページ）を参照してください。
- この設定を後で使用できるバックアップ プロファイルとして保存するには、[Save as New] をクリックします。

  [System] > [Tools] > [Backup]/[Restore] を選択してから [Backup Profiles] をクリックすることにより、バックアップ プロファイルを変更または削除できます。詳細については、「バックアップ プロファイルの作成（70-6 ページ）」を参照してください。

物理管理対象デバイスのバックアップ ファイルをその管理 Defense Center から作成するには、次の手順を実行します。

アクセス: Admin/Maint

ステップ 1　[System] > [Tools] > [Backup]/[Restore] を選択します。

[Backup Management] ページが表示されます。

ステップ 2　[Managed Device Backup] をクリックします。

[Create Backup] ページが表示されます。

ステップ 3　[Managed Devices] フィールドで、1 つ以上の管理対象デバイスを選択します。複数の管理対象デバイスを選択するには、Shift キーと Ctrl キーを使用します。

ステップ 4　構成データと共に統合ファイルも含めるには、[Include All Unified Files] チェック ボックスをオンにします。

ステップ 5　バックアップ ファイルを Defense Center に保存するには、[Retrieve to Defense Center] チェック ボックスをオンにします。各デバイスのバックアップ ファイルをそのデバイス自体に保存するには、このチェック ボックスをオフにしておいてください。

注　[Retrieve to Defense Center] を選択した場合、Defense Center がバックアップのリモート ストレージ用に設定されていれば、デバイスのバックアップ ファイルは Defense Center 自体ではなく設定されたリモート ロケーションに保存されます。

ステップ 6　[Start Backup] をクリックします。

成功を示すメッセージが表示されて、バックアップ タスクが作成されます。

バックアップ ファイルは `/var/sf/backup` ディレクトリに保存されます。Defense Center を使用して、リモート ロケーションをバックアップ ファイルの場所として指定できます。リモート ストレージの管理（64-17 ページ）を参照してください。

バックアップ プロセスが完了すると、[Restoration Database] ページでファイルを参照できます。バックアップ ファイルを復元する方法について詳しくは、バックアップ ファイルからのアプライアンスの復元（70-8 ページ）を参照してください。

ステップ 7　オプションで、この設定を後で使用できるバックアップ プロファイルとして保存するには、[Save as New] をクリックします。

[System] > [Tools] > [Backup]/[Restore] を選択してから [Backup Profiles] をクリックすることにより、バックアップ プロファイルを変更または削除できます。詳細については、「バックアップ プロファイルの作成（70-6 ページ）」を参照してください。

バックアップ プロファイルの作成

ライセンス: すべて

サポートされるデバイス: すべて（仮想、X-Series、および ASA FirePOWER を除く）

サポートされる防御センター: すべて

[Backup Profiles] ページを使用して、さまざまな種類のバックアップに使用する設定値を含むバックアップ プロファイルを作成できます。後にアプライアンスのファイルをバックアップするときに、これらのプロファイルの 1 つを選択できます。

ヒント　バックアップ ファイルの作成（70-2 ページ）で説明されているようにバックアップ ファイルを作成すると、バックアップ プロファイルが自動的に作成されます。

バックアップ プロファイルの作成方法：

アクセス： Admin/Maint

ステップ 1　[System] > [Tools] > [Backup]/[Restore] を選択します。

[Backup Management] ページが表示されます。

ステップ 2　[Backup Profiles] タブをクリックします。

[Backup Profiles] ページが表示されて、既存のバックアップ プロファイルのリストが示されます。

ヒント　編集アイコン（）をクリックして既存のプロファイルを変更するか、または削除アイコン（）をクリックしてリストからプロファイルを削除することができます。

ステップ 3　[Create Profile] をクリックします。

[Create Backup] ページが表示されます。

ステップ 4　バックアップ プロファイルの名前を入力します。英数字、句読記号、およびスペースを使用できます。

ステップ 5　バックアップ プロファイルを必要に合わせて設定します。

このページのオプションについて詳しくは、バックアップ ファイルの作成（70-2 ページ）を参照してください。

ステップ 6　バックアップ プロファイルを保存するには、[Save as New] をクリックします。

[Backup Profiles] ページが表示されて、新しいプロファイルがリストに示されます。

ローカル ホストからのバックアップのアップロード

ライセンス： すべて

サポートされるデバイス： シリーズ 2 およびシリーズ 3

サポートされる防御センター： すべて

バックアップ管理の表で説明されているダウンロード機能を使用してローカル ホストにバックアップ ファイルをダウンロードした場合、それをDefense Centerにアップロードできます。

バックアップ ファイルに PKI オブジェクトが含まれている場合、内部 CA と内部証明書オブジェクトに関連付けられた秘密キーは、アップロードの際にランダムに生成されるキーによって再暗号化されます。

ヒント　4 GB よりも大きなファイルのアップロードは Web ブラウザでサポートされていないため、そのように大きなサイズのバックアップをローカル コンピュータからアップロードすることはできません。代わりに、バックアップを SCP 経由でリモート ホストにコピーし、そこから取得することができます。Defense Centerでは、バックアップ ファイルをリモート ロケーションに保存し、そこから取得できます。リモート ストレージの管理（64-17 ページ）を参照してください。

ローカル ホストからバックアップをアップロードする方法：

アクセス： Admin/Maint

ステップ 1　[System] > [Tools] > [Backup]/[Restore] を選択します。

[Backup Management] ページが表示されます。

ステップ 2　[Upload Backup] をクリックします。

[Upload Backup] ページが表示されます。

ステップ 3　[Browse] をクリックして、アップロードするバックアップ ファイルに移動します。

アップロードするファイルを選択した後に、[Upload Backup] をクリックします。

ステップ 4　[Backup Management] をクリックして、[Backup Management] ページに戻ります。

バックアップ ファイルがアップロードされ、バックアップ リストに表示されます。Defense Center アプライアンスによってファイルの整合性が検証された後に、[Backup Management] ページを更新して、詳細なファイル システム情報を確認します。

バックアップ ファイルからのアプライアンスの復元

ライセンス： すべて

サポートされるデバイス： シリーズ 2 およびシリーズ 3

サポートされる防御センター： すべて

[Backup Management] ページを使用して、バックアップ ファイルからアプライアンスを復元できます。バックアップを復元するには、バックアップ ファイル内の VDB のバージョンが、アプライアンスの現在の VDB のバージョンと一致している必要があります。復元プロセスが完了した後、最新の Sourcefire ルール アップデートを適用する**必要があります**。

注意　仮想 Defense Center で作成されたバックアップを物理 Defense Center に復元しないでください。これはシステム リソースに負荷をかける可能性があります。仮想バックアップを物理Defense Centerに復元する必要がある場合は、サポートに連絡してください。

バックアップ ファイルに PKI オブジェクトが含まれている場合、内部 CA と内部証明書オブジェクトに関連付けられた秘密キーは、アップロードの際にランダムに生成されるキーによって再暗号化されます。

ローカル ストレージを使用する場合、バックアップ ファイルは `/var/sf/backup` に保存されて、`/var` パーティションで使用されているディスク領域量と共に [Backup Management] ページの下部にリストされます。Defense Centerで、[Backup Management] ページの上部にある [Remote Storage] を選択して、リモート ストレージ オプションを設定します。その後、リモート ストレー

ジを有効にするために、[Backup Management] ページの [Enable Remote Storage for Backups] チェック ボックスをオンします。リモート ストレージを使用している場合は、プロトコル、バックアップ システム、およびバックアップ ディレクトリがページの下部に表示されます。

注 バックアップが完了した後にライセンスを追加した場合は、このバックアップを復元するときに、それらのライセンスが削除されたり上書きされたりすることはありません。復元時の競合を防ぐため、バックアップの復元前にこれらのライセンスを削除し、ライセンスの使用先を書きとめます。バックアップの復元後にこれらのライセンスを追加して再設定できます。競合が発生した場合は、サポートに連絡してください。

次の表では、[Backup Management] ページの各列とアイコンについて説明します。

表 70-2　　バックアップ管理

機能	説明
System Information	元のアプライアンスの名前、タイプ、バージョン。バックアップを復元できるのは、同一のアプライアンス タイプとバージョンに対してだけであることに注意してください。
Date Created	バックアップ ファイルが作成された日時
File Name	バックアップ ファイルのフルネーム
VDB Version	バックアップ時にアプライアンスで実行されている脆弱性データベース（VDB）のビルド。
場所	バックアップ ファイルの場所
Size (MB)	バックアップ ファイルのサイズ（メガバイト）
Event	[Yes] は、バックアップにイベント データが含まれていることを示します
ビュー	バックアップ ファイルの名前をクリックすると、圧縮されたバックアップ ファイルに含まれるファイルのリストが表示されます。
Restore（復元）	バックアップ ファイルが選択された状態でクリックすると、そのバックアップ ファイルがアプライアンスに復元されます。VDB バージョンがバックアップ ファイルの VDB のバージョンと一致しない場合、このオプションは無効になります。
Download	バックアップ ファイルが選択された状態でクリックすると、そのバックアップ ファイルがローカル コンピュータに保存されます。
削除	バックアップ ファイルが選択された状態でクリックすると、そのバックアップ ファイルが削除されます。
移動	Defense Centerで、以前に作成したローカル バックアップが選択された状態でクリックすると、そのバックアップが指定のリモート バックアップ ロケーションに送信されます。

バックアップ ファイルからのアプライアンスの復元方法：

アクセス：Admin

ステップ 1　[System] > [Tools] > [Backup]/[Restore] を選択します。

[Backup Management] ページが表示されます。

ステップ 2　バック アップ ファイルの内容を確認するには、ファイルの名前をクリックします。

マニフェストが表示され、各ファイルの名前、所有者と権限、およびファイル サイズと日付がリストされます。

ステップ 3　[Backup Management] をクリックして、[Backup Management] ページに戻ります。

ステップ 4　復元するバックアップ ファイルを選択して、[Restore] クリックします。

[Restore Backup]ページが表示されます。

バックアップの VDB バージョンがアプライアンスに現在インストールされている VDB のバージョンと一致しない場合、[Restore] ボタンはグレー表示されることに注意してください。

注意　この手順により、すべてのコンフィギュレーション ファイルが上書きされ、管理対象デバイスでは、すべてのイベント データが上書きされます。

ステップ 5　ファイルを復元するには、次のいずれかまたは両方を選択します。

- **Replace Configuration Data**
- **Restore Event Data**

注　管理対象デバイスの設定をバックアップ ファイルから復元すると、デバイスの管理用のDefense Centerから行われたデバイス設定の変更も復元されることに注意してください。復元される変更には、そのバックアップ ファイルを作成した後に行った変更も含まれます。

ステップ 6　[Restore] クリックして、復元を開始します。

アプライアンスが、指定したバックアップ ファイルを使用して復元されます。

ステップ 7　アプライアンスをリブートします。

ステップ 8　最新の Sourcefire ルール アップデートを適用して、ルールのアップデートを再適用します。

ステップ 9　復元されたシステムにアクセス コントロール ポリシー、侵入ポリシー、ネットワーク検出ポリシー、ヘルス ポリシー、システム ポリシーを再適用します。

ユーザ プリファレンスの指定

ホーム ページ、アカウント パスワード、タイム ゾーン、ダッシュボード、イベント ビューの各プリファレンスなど、単一のユーザ アカウントに関連付けられたプリファレンスを設定できます。

ユーザ ロールに応じて、パスワード、イベント ビューのプリファレンス、タイム ゾーンの設定、ホーム ページのプリファレンスなど、ユーザ アカウントに固有のプリファレンスを指定できます。詳細については、次の項を参照してください。

- パスワードの変更（71-1 ページ）では、ユーザ アカウントのパスワードを変更する方法を説明します。
- ホーム ページの指定（71-3 ページ）では、既存のページの 1 つをデフォルトのホーム ページとして使用する方法を説明します。この値を設定した後は、このページがアプライアンスにログインする際に最初に表示されるページになります。
- イベント ビュー設定の設定（71-3 ページ）では、イベント プリファレンスによって、イベントの表示内容がどのように変化するかを説明します。
- デフォルトのタイム ゾーンの設定（71-8 ページ）では、ユーザ アカウントのタイム ゾーンを設定する方法、およびその設定によって、表示されるイベントのタイムスタンプがどのように変化するかを説明します。
- デフォルトのダッシュボードの指定（71-9 ページ）では、どのダッシュボードをデフォルトのダッシュボードとして使用するかを選択する方法を説明します。

パスワードの変更

ライセンス： すべて

サポートされるデバイス： シリーズ 2、シリーズ 3

サポートされる防御センター： すべて

すべてのユーザ アカウントはパスワードで保護されています。パスワードはいつでも変更することができ、ユーザー アカウントの設定によっては定期的にパスワードを変更しなければならない場合もあります。期限切れのパスワードの変更（71-2 ページ）を参照してください。

パスワードの強度チェックが有効の場合、パスワードは大文字と小文字が混在する少なくとも 8 つの英数字で、少なくとも 1 つの数字が含まれている必要があることに注意してください。パスワードは、辞書に出現する単語であったり、連続する繰り返し文字を含んでいたりすることができません。

注　LDAP または RADIUS ユーザの場合、Web インターフェイスを介してパスワードを変更することはできません。

パスワードを変更するには、次の手順を実行します。

アクセス: すべて

ステップ 1　ユーザ名の下にあるドロップダウン リストから、[User Preferences] を選択します。

[Change Password] ページが表示されます。

ステップ 2　[Current Password] フィールドに、現在のパスワードを入力して、[Change] をクリックします。

ステップ 3　[New Password] および [Confirm] フィールドに、新しいパスワードを入力します。

ステップ 4　[Change] をクリックします。

新しいパスワードがシステムによって受け入れられると、成功を示すメッセージが表示されます。

期限切れのパスワードの変更

ライセンス: すべて

サポートされるデバイス: シリーズ 2、シリーズ 3

サポートされる防御センター: すべて

ユーザ アカウントの設定によっては、パスワードが期限切れになることがあります。パスワードの有効期間は、アカウントが作成されたときに設定され、変更できないことに注意してください。パスワードが期限切れになった場合、[Password Expiration Warning] ページが表示されます。

パスワードの期限切れ警告に応答するには、次のようにします。

アクセス: すべて

ステップ 1　次の 2 つの選択肢があります。

- すぐにパスワードを変更するには、[Change Password] をクリックします。

  残りの警告日数がゼロの場合は、パスワードを変更する**必要があります**。また、パスワードの強度チェックが有効の場合、パスワードは大文字と小文字が混在する少なくとも 8 つの英数字で、少なくとも 1 つの数字が含まれている必要があります。パスワードは、辞書に出現する単語であったり、連続する繰り返し文字を含んでいたりすることができません。
- 後でパスワードを変更するには、[Skip] をクリックします。

ホーム ページの指定

ライセンス： すべて

Web インターフェイス内のページをアプライアンスのホーム ページに指定できます。デフォルトのホーム ページはサマリー ダッシュボード（[Overview] > [Dashboards]）ですが、ダッシュボードにアクセスできないユーザ アカウントの場合は例外で、[Welcome] ページが使用されます。

ホーム ページを指定するには、次のようにします。

アクセス： External Database User を除くすべてのユーザ

ステップ 1　ユーザ名の下にあるドロップダウン リストから、[User Preferences] を選択します。

[Change Password] ページが表示されます。

ステップ 2　[Home Page] をクリックします。

[Home Page] ページが表示されます。

ステップ 3　ホーム ページとして使用するページをドロップダウン リストから選択します。

ドロップダウン リスト内のオプションは、ユーザ アカウントのアクセス権限に基づいて表示されます。詳細については、アカウント特権について（61-60 ページ）を参照してください。

ステップ 4　[Save] をクリックします。

ホーム ページのプリファレンスが保存されます。

イベント ビュー設定の設定

ライセンス： すべて

[Event View Settings] ページを使用して、FireSIGHT システムのイベント ビューの特性を設定します。イベント ビュー設定は、特定のユーザ ロールでのみ使用可能であることに注意してください。External Database User ロールを持つユーザは、イベント ビュー設定のユーザ インターフェイスの一部を表示できますが、それらの設定を変更しても意味のある結果は生じません。詳しくは、以下にリンクされている個々の項を参照してください。

イベントのプリファレンスを設定するには、次のようにします。

アクセス： 機能によって異なる

ステップ 1　ユーザ名の下にあるドロップダウン リストから、[User Preferences] を選択します。

[User Preferences] ページが表示されます。

ステップ 2　[Event View Settings] をクリックします。

[Event View Settings] ページが表示されます。

ステップ 3　イベント ビューの基本特性を設定します。

詳細については、イベントのプリファレンス（71-4 ページ）を参照してください。

ステップ 4　ファイルのダウンロードのプリファレンスを設定します。

詳細については、ファイルのプリファレンス（71-5 ページ）を参照してください。

ステップ 5　デフォルトの時間枠を設定します(複数可)。

詳細については、デフォルトの時間枠(71-6 ページ)を参照してください。

ステップ 6　デフォルトのワークフローを設定します。

詳細については、デフォルトのワークフロー(71-7 ページ)を参照してください。

ステップ 7　[Save] をクリックします。

変更が反映されます。

イベントのプリファレンス

ライセンス: すべて

[Event View Settings] ページの [Event Preferences] セクションを使用して、FireSIGHT システムのイベント ビューの基本特性を設定します。このセクションはすべてのユーザ ロールで使用可能ですが、イベントを表示できないユーザには、ほとんどまたはまったく意味がありません。

以下のフィールドが [Event Preferences] セクションに示されます。

- [Confirm “All” Actions] フィールドは、イベント ビューのすべてのイベントに影響を与える操作について、アプライアンスがユーザに確認を要求するかどうかを制御します。

  たとえば、この設定が有効である場合、イベント ビューで [Delete All] をクリックすると、アプライアンスがデータベースからの削除を実行する前に、現在の制約を満たすすべてのイベント(現在のページに表示されていないイベントを含む)を削除することをユーザが確認する必要があります。

- [Resolve IP Addresses] フィールドは、可能な場合には常に、アプライアンスがイベント ビューで IP アドレスの代わりにホスト名を表示するようにします。

  多数の IP アドレスが含まれている場合、このオプションを有効にすると、イベント ビューの表示に時間がかかる可能性があることに注意してください。この設定が有効になるためには、システム設定で DNS サーバを設定している必要があることにも注意してください。管理インターフェイスの構成(64-9 ページ)を参照してください。

- [Expand Packet View] フィールドでは、侵入イベントのパケット ビューをどのように表示するかを設定できます。デフォルトでは、アプライアンスによるパケット ビューの表示は折りたたまれた状態になっています。

  - [None] :パケット ビューの [Packet Information] セクションのサブセクションをすべて折りたたんだ状態にします。
  - [Packet Text] :[Packet Text] サブセクションだけを展開します。
  - [Packet Bytes] :[Packet Bytes] サブセクションだけを展開します。
  - [All] :すべてのセクションを展開します。

  デフォルト設定に関係なく、パケット ビューのセクションを手動で展開することで、検出されたパケットに関する詳細情報を常に表示することができます。パケット ビューに関する詳細については、パケット ビューの使用(41-23 ページ)を参照してください。

- [Rows Per Page] フィールドは、ドリル ダウン ページとテーブル ビューに表示する、ページごとのイベントの行数を制御します。

- [Refresh Interval] フィールドは、イベント ビューの更新間隔を分数で設定します。0 を入力すると、更新オプションが無効になります。この間隔はダッシュボードに適用されないことに注意してください。

- [Statistics Refresh Interval] は、[Intrusion Event Statistics] や [Discovery Statistics] ページなどのイベントのサマリー ページの更新間隔を制御します。0 を入力すると、更新オプションが無効になります。この間隔はダッシュボードに適用されないことに注意してください。
- [Deactivate Rules] フィールドは、標準テキスト ルールによって生成される侵入イベントのパケット ビューに、どのリンクを表示させるかを次のように制御します。
  - [All Policies] :すべてのローカルで定義されたカスタム侵入ポリシーで標準テキスト ルールを非アクティブにする単一リンク
  - [Current Policy] :現在適用中の侵入ポリシーだけで標準テキスト ルールを非アクティブにする単一リンク。デフォルトのポリシーのルールは非アクティブにできないことに注意してください。
  - [Ask] : これらの個々のオプションへのリンク

  パケット ビューでこれらのリンクを表示するには、Administrator または Intrusion Admin のアクセス権があるユーザ アカウントが必要です。

ファイルのプリファレンス

ライセンス: すべて

サポートされるデバイス: 機能によって異なる

サポートされる防御センター: 機能によって異なる

[Event View Settings] ページの [File Preferences] セクションを使用して、ローカル ファイル ダウンロードの基本特性を設定します。このセクションは、Administrator、Security Analyst、または Security Analyst（読み取り専用）ユーザ ロールを持つユーザのみが使用できます。

検出されたファイルのダウンロードをアプライアンスがサポートしていない場合、これらのオプションは無効になることに注意してください。DC500 ではMalware ライセンスを使用できないので、それらのアプライアンスを使用してファイルをダウンロードしたり、これらのオプションを変更したりすることはできません。

以下のフィールドが [File Preferences] セクションに示されます。

- [Confirm 'Download File' Actions] チェック ボックスは、ファイルをダウンロードするたびに [File Download] ポップアップ ウィンドウが表示され、警告が示されて続行するかキャンセルするかを選択するためのプロンプトが出されるようにするかどうかを制御します。

注意 Ciscoは、有害な結果が発生することがあるため、マルウェアをダウンロード**しない**ように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先をセキュアにするために必要な予防措置を行っていることを確認します。

ファイルをダウンロードする際には、いつでもこのオプションを無効にできることに注意してください。ファイルのダウンロード方法について詳しくは、保存されているファイルの別の場所へのダウンロード（40-4 ページ）を参照してください。

- 検出されたファイルをダウンロードすると、そのファイルを含むパスワード保護された .zip アーカイブがシステムによって作成されます。[Zip File Password] フィールドは、zip ファイルへのアクセスを制限するためにユーザが使用するパスワードを定義します。このフィールドを空欄にすると、パスワードなしのアーカイブ ファイルがシステムによって作成されます。
- [Show Zip File Password] チェック ボックスによって、[Zip File Password] フィールドにプレーン テキストを表示するかまたは不明瞭な文字を表示するかを切り替えます。このフィールドをオフにすると、[Zip File Password] には不明瞭な文字が表示されます。

デフォルトの時間枠

ライセンス： すべて

時間枠（時間範囲と呼ばれることもある）は、任意のイベント ビューでイベントに時間制約を課します。[Event View Settings] ページの [Default Time Windows] セクションを使用して、時間枠のデフォルトの動作を制御します。

このセクションへのユーザ ロール アクセスは以下のとおりです。

- Administrators と Maintenance Users は、セクション全体にアクセスできます。
- Security Analysts と Security Analysts（読み取り専用）は、[Audit Log Time Window] 以外のすべてのオプションにアクセスできます。
- Access Admins、Discovery Admins、External Database Users、Intrusion Admins、Network Admins、および Security Approvers は、[Events Time Window] オプションにのみアクセスできます。

デフォルトの時間枠設定に関係なく、イベントの分析中にいつでも手動で個別のイベント ビューの時間枠を変更できることに注意してください。また、時間枠の設定は、現在のセッションにだけ有効であることにも注意してください。ログアウトしてから再びログインすると、時間枠は、このページで設定したデフォルトにリセットされます。詳細については、イベント時間の制約の設定（58-26 ページ）を参照してください。

以下のように、デフォルトの時間枠を設定できる 3 つのタイプのイベントがあります。

- [Events Time Window] は、時間で制約できるほとんどイベントのために単一のデフォルトの時間枠を設定します。
- [Audit Log Time Window] は、監査ログのためにデフォルトの時間枠を設定します。
- [Health Monitoring Time Window] は、ヘルス イベントのためにデフォルトの時間枠を設定します。

時間枠は、ユーザ アカウントがアクセスできるイベント タイプにのみ設定できます。すべてのユーザ タイプは、イベントの時間枠を設定できます。Administrators、Maintenance Users、および Security Analysts は、ヘルス モニタリングの時間枠を設定できます。Administrators と Maintenance Users は、監査ログの時間枠を設定できます。

すべてのイベント ビューが時間で制約できるとは限らないので、時間枠の設定によって、ホスト、ホスト属性、アプリケーション、クライアント、脆弱性、ユーザの ID、ホワイトリスト違反を表示するイベント ビューは影響を受けないことに注意してください。

複数の時間枠を使用して、上記の各タイプのイベントに 1 つずつ適用するか、または**単一の**時間枠を使用して、それをすべてのイベントに適用することができます。単一の時間枠を使用すると、3 つのタイプの時間枠用の設定が非表示になり、新しく [Global Time Window] 設定が表示されます。

以下の 3 つのタイプの時間枠があります。

- *静的*は、特定の開始時刻から特定の終了時刻までに生成されたすべてのイベントを表示します
- *拡張*は、特定の開始時刻から現在までに生成されたすべてのイベントを表示します。時間の進行と共に時間枠が拡張され、新しいイベントがイベント ビューに追加されます。
- *スライディング*は、特定の開始時刻（たとえば 1 日前）から現在までに生成されたすべてのイベントを表示します。時間の進行と共に時間枠は「スライド」し、設定した範囲内（この例では直前の 1 日）のイベントだけが表示されます。

すべての時間枠の最大時間範囲は、1970 年 1 月 1 日午前 0 時（UTC）～ 2038 年 1 月 19 日午前 3 時 14 分 7 秒です。

次のオプションは、[Time Window Settings] ドロップダウン リストに表示されます。

- [Show the Last - Sliding] オプションにより、指定した長さのスライドするデフォルトの時間枠を設定できます。

  アプライアンスは、特定の開始時刻（たとえば 1 時間前）から現在までに生成されたすべてのイベントを表示します。イベント ビューの変更と共に、時間枠は「スライド」して、常に最後の 1 時間内のイベントが表示されます。

- [Show the Last - Static/Expanding] により、指定した長さのデフォルトの時間枠を静的または拡張のどちらかに設定できます。

  静的時間枠にするには、[Use End Time] チェック ボックスをオンにします。アプライアンスは、特定の開始時間（1 時間前など）から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

  拡張時間枠にするには、[Use End Time] チェック ボックスをオフにします。アプライアンスは、特定の開始時刻（たとえば 1 時間前）から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。

- [Current Day - Static/Expanding] オプションにより、現在の日付のデフォルトの時間枠を静的または拡張のどちらかに設定できます。現在の日付は、現行セッションのタイム ゾーン設定に基づいて午前 0 時に始まります。

  静的時間枠にするには、[Use End Time] チェック ボックスをオンにします。アプライアンスは、午前 0 時からユーザがイベントを初めて確認した時刻までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

  拡張時間枠にするには、[Use End Time] チェック ボックスをオフにします。アプライアンスは、午前 0 時から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に 24 時間を超えて分析を続けた場合、この時間枠は 24 時間よりも長くなる可能性があることに注意してください。

- [Current Week - Static/Expanding] オプションにより、現在の週のデフォルトの時間枠を静的または拡張のどちらかに設定できます。現在の週は、現行セッションのタイム ゾーン設定に基づいて直前の日曜日の午前 0 時に始まります。

  静的時間枠にするには、[Use End Time] チェック ボックスをオンにします。アプライアンスは、午前 0 時からユーザがイベントを初めて確認した時刻までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

  拡張時間枠にするには、[Use End Time] チェック ボックスをオフにします。アプライアンスは、日曜日の午前 0 時から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に 1 週間を超えて分析を続けた場合、この時間枠は 1 週間よりも長くなる可能性があることに注意してください。

デフォルトのワークフロー

ライセンス： すべて

ワークフローは、アナリストがイベントの評価に使用するデータが示された一連のページです。アプライアンスには、各イベント タイプに少なくとも 1 つの定義済みのワークフローが付属しています。たとえば、Security Analyst の場合、実行する分析のタイプに応じて、それぞれが侵入イベントのデータを別の形式で示している、10 の異なる侵入イベントのワークフローから選択できます。

アプライアンスは、イベント タイプごとのデフォルトのワークフローによって設定されます。たとえば、[Events by Priority and Classification（優先度および分類に基づいたイベント）] ワークフローが、侵入イベントのデフォルトになります。つまり、侵入イベント（確認済みの侵入イベントを含む）を表示するたびに、アプライアンスは [Events by Priority and Classification（優先度および分類に基づいたイベント）] ワークフローを表示します。

ただし、[Event View Settings] ページの [Default Workflows] セクションを使用して、各イベント タイプのデフォルトのワークフローを変更できます。

設定可能なデフォルトのワークフローは、ユーザ ロールによって異なることに注意してください。たとえば、侵入イベントのアナリストは、デフォルトのディスカバリ イベントのワークフローを設定できません。ワークフローの一般情報については、ワークフローの概要と使用（58-1 ページ）を参照してください。

デフォルトのタイム ゾーンの設定

ライセンス： すべて

イベントの表示に使用するタイム ゾーンを、アプライアンスが使用している標準 UTC 時間から変更できます。タイム ゾーンを設定すると、それは現在のユーザ アカウントにのみ適用され、タイム ゾーンをさらに変更するときまで有効となります。

注意　タイム ゾーン機能は、デフォルトのシステム クロックが UTC 時間に設定されていると想定しています。ローカル タイム ゾーンを使用するようにアプライアンスのシステム クロックを変更した場合は、アプライアンスで正確なローカル時刻が表示されるように、それを変更して UTC 時間に戻す必要があります。Defense Centerと管理対象デバイスの時間を同期させる方法について詳しくは、時刻の同期（63-27 ページ）を参照してください。

タイム ゾーンを変更するには、次のようにします。

アクセス： すべて

ステップ 1　ユーザ名の下にあるドロップダウン リストから、[User Preferences] を選択します。

[Change Password] ページが表示されます。

ステップ 2　[Time Zone Settings] をクリックします。

[Time Zone Preference] ページが表示されます。

ステップ 3　左側のリスト ボックスで、使用するタイム ゾーンを含む大陸または地域を選択します。

たとえば、北米、南米、カナダで標準のタイム ゾーンを使用する場合は、[America] を選択します。

ステップ 4　右側のリスト・ボックスで、使用するタイム ゾーンに対応するゾーン（都市名）を選択します。

たとえば、東部標準時を使用する場合は、最初のタイム ゾーン ボックスで [America] を選択した後に、[New York] を選択します。

ステップ 5　[Save] をクリックします。

タイム ゾーンが設定されます。

デフォルトのダッシュボードの指定

ライセンス： すべて

アプライアンスにあるダッシュボードの 1 つをデフォルトのダッシュボードとして指定できます。デフォルトのダッシュボードは、[Overview] > [Dashboards] を選択すると表示されます。デフォルトのダッシュボードが定義されていない場合は、[Dashboard List] ページが表示されます。ダッシュボードの一般情報については、ダッシュボードの使用（55-1 ページ）を参照してください。

デフォルトのダッシュボードを指定するには、次のようにします。

アクセス： Admin/Maint/Any Security Analyst

ステップ 1　ユーザ名の下にあるドロップダウン リストから、[User Preferences] を選択します。

[Change Password] ページが表示されます。

ステップ 2　[Dashboard Settings] をクリックします。

[Dashboard Settings] ページが表示されます。

ステップ 3　デフォルトとして使用するダッシュボードをドロップダウン リストから選択します。

[None] を選択した場合、[Overview] > [Dashboards] を選択すると [Dashboard List] ページが表示されます。その後、表示するダッシュボードを選択できます。

ステップ 4　[Save] をクリックします。

デフォルトのダッシュボードのプリファレンスが保存されます。

設定のインポートおよびエクスポート

インポート/エクスポート機能を使用して、ポリシーを含む複数のタイプの設定を、1 つのアプライアンスから同じタイプの別のアプライアンスにコピーにできます。設定のインポートおよびエクスポートは、バックアップ ツールとして設計されてはいませんが、FireSIGHT システムに新しいアプライアンスを追加するプロセスを効率化するために使用できます。

以下の設定をインポートおよびエクスポートできます。

- アクセス コントロール ポリシーとその関連するネットワーク分析ポリシー、SSL ポリシー、およびファイル ポリシー
- 侵入ポリシー
- 正常性ポリシーとシステム ポリシー
- アラート応答
- アプリケーション ディテクタ
- ダッシュボード、カスタム テーブル、カスタム ワークフロー、および保存した検索
- カスタム ユーザ ロール
- レポート テンプレート
- サードパーティ製品および脆弱性マッピング

エクスポートされた設定をインポートするには、両方のアプライアンスで同じバージョンの FireSIGHT システムが稼動していなければなりません。エクスポートされた侵入ポリシーまたはアクセス コントロール ポリシーをインポートするには、両方のアプライアンスでルール アップデート バージョンも一致している必要があります。

詳細については、次の項を参照してください。

- 設定のエクスポート（A-1 ページ）
- 設定のインポート（A-5 ページ）

設定のエクスポート

ライセンス： すべて

単一の設定をエクスポートすることや、（同じタイプまたは異なるタイプの）一連の設定を同時にエクスポートすることができます。後に別のアプライアンスにパッケージをインポートするとき、パッケージ内のどの設定をインポートするかを選択できます。

設定をエクスポートするとき、アプライアンスは、その設定のリビジョン情報もエクスポートします。FireSIGHT システムはその情報を使用して、別のアプライアンスにその設定をインポートできるかどうかを判別します。アプライアンスにすでに存在する設定リビジョンをインポートすることはできません。

また、設定をエクスポートするとき、その設定が依存する認証オブジェクトなどのシステム設定も、アプライアンスによってエクスポートされます。たとえば、LDAP サーバへの認証をDefense Centerにセットアップしてから、認証を有効にしてDefense Centerのシステム ポリシーをエクスポートする場合、認証オブジェクトも同様にエクスポートされます。

ヒント FireSIGHT システムの多くのリスト ページ には、リスト項目の横にエクスポート アイコン( )があります。このアイコンがある場合は、それを使用することにより、その後のエクスポート操作を簡単に代行させることができます。

以下の設定をエクスポートできます。

- *アラート応答*: アラート応答は、アラートの送信先とする予定の外部システムと FireSIGHT システムが対話できるようにするための一連の設定です。
- *カスタム テーブル*: カスタム テーブルは、FireSIGHT システムに付属している事前定義された複数のテーブルのフィールドを結合する、構築可能なテーブルです。
- *カスタム ユーザ ロール*: カスタム ユーザ ロールは、専用のアクセス権限セットを持つ、ユーザが作成するユーザ ロールです。保存済み検索を必要とするカスタム ユーザ ロールをエクスポートすると、必要なすべての保存済み検索もエクスポートされます。
- *カスタム ワークフロー*: カスタム ワークフローは、組織の固有のニーズを満たすためにユーザが作成するワークフローです。Defense Centerでは、作成したカスタム ワークフロー、およびアプライアンスに付属の事前定義されたカスタム ワークフローをエクスポートできます。

  エクスポートされたカスタム ワークフローの基礎となるテーブルをDefense Centerで表示できない場合、ワークフローをインポートすることはできますが、それを表示できないことに注意してください。
- *ダッシュボード*: ダッシュボードは、現在のシステム ステータスの概要を表示する、カスタマイズ可能なタブ付きのビューです。ダッシュボードは、さまざまなウィジェットを使用して、FireSIGHT システムで収集されたイベントや生成されたイベントに関するデータ、および展開に含まれるアプライアンスの状態と全体的な正常性に関する情報を表示します。

  自分が表示できるダッシュボードは、使用しているアプライアンスのタイプ、および自分のユーザ ロールによって異なることに注意してください。詳細については、ウィジェットの可用性について(55-5 ページ)を参照してください。
- *アクセス コントロール ポリシー*: アクセス コントロール ポリシーには、システムがネットワーク トラフィックをどのように管理するかを指定するために設定できる、さまざまなコンポーネントが含まれます。これらのコンポーネントには、アクセス コントロール ルール、関連する侵入ポリシー、ファイル ポリシー、ネットワーク分析ポリシー、SSL ポリシー、およびルールとポリシーが使用するオブジェクト(侵入の変数セットなど)が含まれます。アクセス コントロール ポリシーをエクスポートすると、そのポリシーのすべての設定とコンポーネントもエクスポートされます。ただし、複数のアプライアンスで同等であり、ユーザが変更できない URL レピュテーションとカテゴリは(それらが存在しても)エクスポートされません。アクセス コントロール ポリシーで参照されるカスタム URL オブジェクトまたはグループは、ポリシーのエクスポート時に組み込まれます。アクセス コントロール ポリシーをインポートするには、エクスポート元およびインポート先の防御センターに同じバージョンのルール アップデートが適用されている必要があります。アクセス コントロール ポリシーをインポートするには、エクスポート元およびインポート先のDefense Centerに同じバージョンのルール アップデートが適用されている必要があります。

エクスポートするアクセス コントロール ポリシー、またはこれにより呼び出される SSL ポリシーに位置情報データを参照するルールが含まれる場合、インポート先のDefense Centerの位置情報データベース（GeoDB）のアップデート バージョンが使用されます。

秘密キー情報を含む PKI オブジェクトは、アプライアンスに保存されるときに、ランダムに生成されたキーで暗号化されます。エクスポートするアクセス コントロール ポリシーが、秘密キーを含む PKI オブジェクトを使用する SSL ポリシーを参照している場合、エクスポート前に秘密キーが復号化されます。

エクスポートするアクセス コントロール ポリシーが、サポートされていない DC500 や、シリーズ 2 のデバイス ポリシー機能またはルール条件を参照している場合、DC 500 を使用してポリシーを適用することも、ポリシーをシリーズ 2 デバイスに適用することもできません。DC500 も シリーズ 2 デバイスも、マルウェア ブロック アクションやマルウェア クラウド ルックアップ アクションを使用するルールの含まれる、ユーザまたは URL のルール条件、セキュリティ インテリジェンス、ファイル ポリシーをサポートしません。さらに、シリーズ 2 デバイスはアプリケーション ルール条件をサポートしません。

- *ヘルス ポリシー*:ヘルス ポリシーは、展開内でのアプライアンスの正常性、つまりシスコのハードウェアとソフトウェアが正しく動作しているかどうかを検査する際に使用する基準で構成されます。
- *侵入ポリシー*:侵入ポリシーには、ネットワーク トラフィックを検査して侵入やポリシー違反を見つけるように設定できる、さまざまなコンポーネントが組み込まれています。これらのコンポーネントには、侵入ルール（プロトコル ヘッダー値、ペイロード コンテンツ、および特定のパケット サイズ特性を検査する）、FireSIGHTの推奨ルール設定、およびその他の詳細設定が含まれます。

  侵入ポリシーをエクスポートすると、そのポリシーのすべての設定もエクスポートされます。たとえば、イベントを生成するルールを設定するように選択した場合、ルールの SNMP アラートを設定した場合、またはポリシーでセンシティブ データ プリプロセッサをオンにした場合は、エクスポートされるポリシー内にそれらの設定値が保持されます。カスタム ルール、カスタム ルールの分類、およびユーザ定義変数も、ポリシーと共にエクスポートされます。

  レイヤを使用する侵入ポリシーをエクスポートする場合、そのレイヤが 2 番目の侵入ポリシーによって共有されているときは、エクスポートするポリシーにその共有レイヤがコピーされて、共有関係はなくなることに注意してください。侵入ポリシーを別のアプライアンスにインポートするときは、インポートするポリシーをニーズに合うように編集できます。レイヤの削除、追加、共有などができます。

  1 つのDefense Centerから別の防御センターに侵入ポリシーをエクスポートする場合、2 つ目のDefense Centerでデフォルト変数が別の設定になっている場合は、インポートされたポリシーの動作が異なる可能性があります。

注　インポート/エクスポート機能を使用して、シスコの脆弱性調査チーム（VRT）が作成したルールをアップデートすることはできません。代わりに、最新バージョンのルール アップデートをダウンロードして適用します。ルールの更新とローカル ルール ファイルのインポート（66-16 ページ）を参照してください。

- *レポート テンプレート*:レポートは、特定の FireSIGHT システムのデータを照合する、PDF、HTML、または CSV 形式のドキュメント ファイルです。レポート テンプレートは、レポートとそのセクション用にデータの検索と形式を指定します。レポート テンプレートをエクスポートすると、すべての保存済み検索、画像、オブジェクト マネージャで作成されたオブジェクト、およびレポートに必要なカスタム テーブルもエクスポートされます。

- *保存済み検索*: 保存済み検索は、アクセス許可の制限されたユーザが、事前定義された FireSIGHT システム データにアクセスできるようにします。保存済み検索を必要とするカスタム ユーザ ロールをエクスポートすると、必要な保存済み検索もエクスポートされます。また、個別のユーザ定義の保存済み検索もエクスポートできます。
- *SSL ポリシー*: SSL ポリシーには、ネットワークの暗号化されたトラフィックを管理する方法を指定するために設定できる、さまざまなコンポーネント（SSL ルールや再利用可能な参照オブジェクトなど）が含まれます。SSL ポリシーをエクスポートすると、そのポリシーのすべての設定とコンポーネントもエクスポートされます。ただし、複数のアプライアンスで同等であり、ユーザが変更できない URL レピュテーションとカテゴリは（それらが存在しても）エクスポートされません。SSL ポリシーをインポートするには、エクスポート元およびインポート先のDefense Centerに同じバージョンのルール アップデートが適用されている必要があります。

  秘密キー情報を含む PKI オブジェクトは、アプライアンスに保存されるときに、ランダムに生成されたキーで暗号化されます。エクスポートする SSL ポリシーで秘密キーを含む PKI オブジェクトを使用する場合、エクスポート前に秘密キーが復号化されます。

  エクスポートする SSL ポリシーに位置情報データを参照するルールが含まれる場合、インポート先のDefense Centerの位置情報データベース（GeoDB）のアップデート バージョンが使用されます。
- *システム ポリシー*: システム ポリシーは、データベース イベント制限、時間設定、ログイン バナーなど、展開内の他の FireSIGHT システム アプライアンスに類似する可能性のあるアプライアンスの局面を制御します。

  エクスポートするシステム ポリシーで外部認証が有効の場合、関連する認証オブジェクトもエクスポートされます。

  Defense Centerのシステム ポリシーには、管理対象デバイスに適用されないデータベース設定が含まれることに注意してください。システム ポリシーを管理対象デバイスからエクスポートした後にDefense Centerにインポートする場合、デバイスでは設定できなかったデータベース制限が、Defense Centerではデフォルト値に設定されます。
- *サードパーティ製品マッピング*: サードパーティ アプリケーションからデータをインポートする場合、そのデータを使用して脆弱性を割り当てたり、影響の関連付けを行ったりするために、製品をサードパーティの名前にマッピングする必要があります。製品をマッピングすることにより、シスコの脆弱性情報をサードパーティ製品の名前に関連付けます。これにより、FireSIGHT システムはそのデータを使用して、影響の関連付けを実行できます。サードパーティ製品マッピングを作成する方法について詳しくは、サードパーティ製品のマッピング（46-34 ページ）を参照してください。
- *サードパーティ脆弱性マッピング*: サードパーティ アプリケーションから脆弱性データベースに脆弱性情報を追加するには、インポートしたそれぞれの脆弱性のサードパーティ識別文字列を、既存のシスコ、Bugtraq、または Snort の ID にマッピングする必要があります。脆弱性のマッピングを作成したら、マッピングはネットワーク マップのホストにインポートされたすべての脆弱性に対して機能し、それらの脆弱性に対する影響の関連付けを可能にします。サードパーティ脆弱性マッピングを作成する方法について詳しくは、サードパーティの脆弱性のマッピング（46-36 ページ）を参照してください。
- *アプリケーション ディテクタ*: システムは IP トラフィックを分析するとき、ディテクタを使用して関連情報を収集してから、ネットワークのホストで一般的に使用されるアプリケーションを識別します。エクスポートできるディテクタは、ユーザ定義のディテクタとシスコ プロフェッショナル サービスが提供する個別のアドオン ディテクタの 2 種類です。ディテクタについて詳しくは、アプリケーション ディテクタの使用（46-18 ページ）を参照してください。

注　エクスポートされる設定の数や、それらのオブジェクトが参照する設定の数によっては、エクスポート プロセスに数分かかる場合があります。

一つ以上の設定をエクスポートする方法:

アクセス: Admin

ステップ 1　設定のエクスポート元のアプライアンスと設定のインポート先のアプライアンスで、同じバージョンの FireSIGHT システムが稼働していることを確認します。侵入ポリシーまたはアクセス コントロール ポリシーをエクスポートする場合は、ルールのアップデート バージョンが一致することを確認します。

FireSIGHT システムのバージョン（および該当する場合はルールのアップデート バージョン）が一致しない場合、インポートは失敗します。

ステップ 2　[Systems] > [Tools] > [Import/Export] を選択します。

[Import/Export] ページが表示され、アプライアンス上の設定のリストが示されます。エクスポートする設定がない設定カテゴリは、このリストに表示されないことに注意してください。

ヒント　設定のリストは、設定タイプの横にある折りたたみアイコン（）をクリックして折りたたむことができます。設定を確認するには、設定タイプの横にあるフォルダ展開アイコン（）をクリックします。

ステップ 3　エクスポートする設定の横にあるチェック ボックスを選択して、[Export] をクリックします。

ステップ 4　Web ブラウザのプロンプトに従って、エクスポートされたパッケージをコンピュータに保存します。

設定のインポート

ライセンス: すべて

アプライアンスから設定をエクスポートした後に、その設定が別のアプライアンスでもサポートされていれば、そのアプライアンスにインポートできます。ただし、使用するアプライアンスのタイプやユーザ ロールによっては、一部のインポートされた設定が役立たない場合があることに注意してください。

インポートしている設定のタイプに応じて、以下の点に注意する必要があります。

- 設定をインポートするアプライアンスが、設定のエクスポートに使用したアプライアンスと、同じバージョンの FireSIGHT システムを実行していることを確認します。侵入ポリシーまたはアクセス コントロール ポリシーをインポートする場合は、両方のアプライアンスでルールのアップデート バージョンも一致している必要があります。バージョンが一致しない場合、インポートは失敗します。
- 保存済み検索を必要とするカスタム ユーザ ロールをインポートすると、必要な保存済み検索もインポートされます。
- 表示できるダッシュボード ウィジェットは、使用しているアプライアンスのタイプと、自分のユーザ ロールによって異なります。たとえば、Defense Centerで作成され、管理対象デバイスにインポートされるダッシュボードは、無効なウィジェットを表示する場合があります。

- ゾーンに基づいてトラフィックを評価するアクセス コントロール ポリシーをインポートした場合、インポートされたポリシー内のゾーンを、インポート先のDefense Centerによって管理されるデバイスのゾーンにマッピングする必要があります。ゾーンをマッピングするときは、それらのタイプが一致している必要があります。したがって、インポートを開始する前に、インポート先のDefense Centerで必要となるゾーン タイプを作成する必要があります。セキュリティ ゾーンについて詳しくは、セキュリティ ゾーンの操作（3-42 ページ）を参照してください。
- 既存のオブジェクトやグループと同一の名前を持つオブジェクトやオブジェクト グループを含むアクセス コントロール ポリシーまたは保存済み検索をインポートする場合は、オブジェクトやグループの名前を変更する必要があります。
- アクセス コントロール ポリシーや侵入ポリシーをインポートする場合、インポート プロセスによって、デフォルト変数セットに含まれる既存のデフォルト変数が、インポートされたデフォルト変数に置換されます。既存のデフォルト変数セットに、インポートされたカスタム変数セットに存在しないカスタム変数が含まれる場合、一意的な変数が保持されます。
- 侵入ポリシーをインポートするとき、その侵入ポリシーが 2 番目の侵入ポリシーの共有レイヤを使用していた場合は、エクスポート プロセスによって共有関係が切断されて、それまで共有されていたレイヤがパッケージにコピーされます。つまり、インポートされた侵入ポリシーに共有レイヤは含まれません。

注　インポート/エクスポート機能を使用して、シスコの脆弱性調査チーム（VRT）が作成したルールをアップデートすることはできません。代わりに、最新バージョンのルール アップデートをダウンロードして適用します。ルールの更新とローカル ルール ファイルのインポート（66-16 ページ）を参照してください。

- 秘密キーを含む PKI オブジェクトを参照する SSL ポリシーをインポートする場合、システムはキーをアプライアンスに保存する前にランダムに生成されたキーでそのキーを暗号化します。
- 外部認証が有効になっているDefense Centerからエクスポートされたシステム ポリシーをインポートするときは、そのシステム ポリシーが依存する認証オブジェクトもインポートします。

1 つのパッケージで複数の設定をエクスポートできるため、パッケージのインポート時に、パッケージ内のどの設定をインポートするかを選択する必要があります。インポート先のアプライアンスでサポートされる設定だけがインポート可能です。

設定をインポートしようとすると、アプライアンスは、その設定がアプライアンスにすでに存在しているかどうかを判別します。競合がある場合は、以下の操作が可能です。

- 既存の設定を維持する、
- 既存の設定を新しい設定に置き換える、
- 最新の設定を維持する、または
- 設定を新しい設定としてインポートする。

設定をインポートした後に、宛先システムで設定を変更してその設定を再インポートすると、保持する設定のバージョンを選択する必要があります。

インポートされる設定の数や、それらのオブジェクトが参照する設定の数によっては、プロセスに数分かかる場合があります。

一つ以上の設定をインポートする方法:

アクセス: Admin

ステップ 1　設定のエクスポート元のアプライアンスと設定のインポート先のアプライアンスで、同じバージョンの FireSIGHT システムが稼働していることを確認します。侵入ポリシーまたはアクセス コントロール ポリシーをインポートする場合は、ルールのアップデート バージョンが一致することも確認する必要があります。

FireSIGHT システムのバージョン（および該当する場合はルールのアップデート バージョン）が一致しない場合、インポートは失敗します。

ステップ 2　インポートする設定をエクスポートします。設定のエクスポート（A-1 ページ）を参照してください。

ステップ 3　設定をインポートするアプライアンスで、[System] > [Tools] > [Import/Export] を選択します。

[Import/Export] ページが表示されます。

ヒント　設定のリストを折りたたむには、設定タイプの横にある折りたたみアイコン（  ）をクリックします。設定を確認するには、設定タイプの横にあるフォルダ展開アイコン（）をクリックします。

ステップ 4　[Upload Package] をクリックします。

[Upload Package] ページが表示されます。

ステップ 5　次の 2 つのオプションから選択できます。

- アップロードするパッケージのパスを入力します。
- [Browse] をクリックして参照し、パッケージを見つけます。

ステップ 6　[Upload] をクリックします。

アップロードの結果は、パッケージの内容によって異なります。

- パッケージ内の設定が、アプライアンスにすでに存在するバージョンと正確に一致する場合、そのバージョンが存在することを示すメッセージが表示されます。アプライアンスに最新の設定が存在するので、それらをインポートする必要はありません。
- 使用するアプライアンスとパッケージのエクスポート元のアプライアンスとの間に、FireSIGHT システムまたは（該当する場合）ルール アップデートのバージョンの不一致がある場合、パッケージをインポートできないことを示すメッセージが表示されます。FireSIGHT システムまたはルール アップデートのバージョンを更新して、プロセスを再試行します。
- アプライアンスに存在しない設定やルールのバージョンがパッケージに含まれている場合、[Package Import] ページが表示されます。次の手順に進んでください。

ステップ 7　インポートする設定を選択して、[Import] をクリックします。

インポート プロセスが解決されて、以下のような結果になります。

- アプライアンスに、インポートする設定の以前のリビジョンが存在しない場合でも、インポートは自動的に完了し、成功メッセージが表示されます。残りの手順は省略してください。
- セキュリティ ゾーンを含むアクセス コントロール ポリシーをインポートする場合、[Access Control Import Resolution] ページが表示されます。手順 8 に進みます。
- インポートする設定に対してアプライアンスに以前のリビジョンが存在する場合、[Import Resolution] ページが表示されます。手順 9 に進みます。

ステップ 8　取り込まれる各セキュリティ ゾーンの横で、同じタイプの既存のローカル セキュリティ ゾーンをマップ先として選択し、[Import] をクリックします。

手順 7 に戻ります。

ステップ 9　各設定を展開して、以下の該当するオプションを選択します。

- アプライアンスの設定を保持するには、[Keep existing] を選択します。
- アプライアンスの設定をインポートした設定に置き換えるには、[Replace existing] を選択します。
- 最新の設定を保持するには、[Keep newest] を選択します。
- インポートした設定を新しい設定として保存するには、[Import as new] を選択し、オプションとして設定名を編集します。

  クリーン リストまたはカスタム検出リストが有効になっているファイル ポリシーを含むアクセス コントロール ポリシーをインポートする場合、[Import as new] オプションは使用できません。
- 従属オブジェクトを含むアクセス コントロール ポリシーや保存済み検索をインポートする場合、提案された名前を受け入れるか、またはオブジェクトの名前を変更します。システムは常にこれらの従属オブジェクトを新規としてインポートします。既存のオブジェクトを保存したり置き換えたりするオプションはありません。システムではオブジェクトもオブジェクト グループも同様に処理されることに注意してください。

ステップ 10　[Import] をクリックします。

設定がインポートされます。

データベースからの検出データの消去

[Discovery Data Purge] ページは、ネットワーク検出イベント データベースとユーザ検出イベント データベースからファイルを消去するために使用できます。データベースを消去すると、該当するプロセスが再起動されることに注意してください。

注意 データベースを消去すると、Defense Centerから指定したデータが削除されます。削除されたデータは**復元できません**。

ネットワーク検出データベースとユーザ検出データベースを消去するには、以下を行います。

アクセス: Admin/Any Security Analyst

ステップ 1 [System] > [Tools] > [Data Purge] の順に選択します。

[Data Purge] ページが表示されます。

ステップ 2 [Network Discovery] で、次のいずれかまたはすべてを実行します。

- データベースからすべてのネットワーク検出イベントを削除するには、[Network Discovery Events] を選択します。
- データベースからすべてのホストと侵害の痕跡フラグを削除するには、[Hosts] を選択します。
- データベースからすべてのユーザ イベントを削除するには、[User Activity] を選択します。
- データベースからすべてのユーザ ログインとユーザ履歴データを削除するには、[User Identities] を選択します。

ステップ 3 [Connections] で、次のいずれかまたはすべてを実行します。

- データベースからすべての接続データを削除するには、[Connection Events] を選択します。
- データベースからすべての接続の概要データを削除するには、[Connection Summary Events] を選択します。
- データベースからすべてのセキュリティ インテリジェンス データを削除するには、[Security Intelligence Events] を選択します。

注 [Connection Events] を選択しても、セキュリティ インテリジェンス イベントは削除されません。セキュリティ インテリジェンス データを使用した接続がセキュリティ インテリジェンス イベント ビューアから消去されることはありません。同様に、[Security Intelligence Events] を選択しても、関連したセキュリティ インテリジェンス データを使用した接続イベントは削除されません。

ステップ 4　[Purge Selected Events] をクリックします。

項目が消去され、該当するプロセスが再起動されます。

実行時間が長いタスクのステータスの表示

FireSIGHT システムで実行できるタスクの中には、ポリシー適用やアップデート インストールのように、すぐに完了せず実行に時間がかかるものがあります。このように実行時間が長いタスクの進捗状況を、タスク キューで確認できます。また、これらのタスクが正常に終了したり、異常終了したりした場合にも、タスク キューで報告されます。

詳細については、次の項を参照してください。

- タスク キューの表示（C-1 ページ）
- タスク キューの管理（C-2 ページ）

タスク キューの表示

ライセンス： すべて

ポリシーの適用やアップデートのインストールなど、実行時間が長いタスクを実行すると、これらのタスクのステータスがタスク キューで報告されます。タスク キューは複雑なタスクに関する情報を示し、そのようなタスクが完了したときに報告します。

[Task Status] ページでタスク キューを表示します。これは 10 秒ごとに自動的に更新されます。ユーザは、自分が開始したタスクのステータスを常に表示できます。自身のユーザ アカウントが Administrator ユーザ ロールを持っているか、View Other Users' Tasks 権限付きユーザ ロールを持っている場合には、誰が開始したかに関係なく、すべてのタスクのステータスを表示できます。ユーザ ロールの設定の詳細については、ユーザ ロールの設定（61-52 ページ）を参照してください。

[Job Summary] セクションには、次の表に記載するように、ページに示されているタスクのステータスが表示されます。

表 C-1　　タスク キューのタスク タイプ

タスク タイプ	説明
Running	進行中のタスクの数。
Waiting	進行中のいずれかのタスクが完了するのを待機している、実行前のタスクの数。
Completed	正常に完了したタスクの数。
Retrying	自動的に再試行されるタスクの数。なお、すべてのタスクの再試行が許可されるわけではありません。

表 C-1　タスク キューのタスク タイプ（続き）

タスク タイプ	説明
Stopped	システムの更新のために中断されたタスクの数。停止したタスクは再開できません。タスク キューから手動で削除する必要があります。
Failed	正常に終了しなかったタスクの数。

[Jobs] セクションには、各タスクの情報（簡単な説明、タスクがいつ起動されたか、タスクの現在の状態、ステータスが最後に変更されたのはいつか、など）が示されます。「ネットワーク検出ポリシー適用」など、同じタイプの複数のタスクは 1 つのタスク グループにまとめて表示されます。

[Task Status] ページがすばやくロードされるように、FireSIGHT システムは 過去 1 ヶ月より前に完了/失敗/停止したすべてのタスクを 1 週間に一度、キューから削除します。さらに、1000 個を超えるタスクが含まれるタスク グループから古いタスクを同じ頻度で削除します。なお、手動でキューからタスクを削除することもできます（タスク キューの管理の説明を参照してください）。

タスク キューを表示する方法：

アクセス： Admin/Maint/Network Admin/Security Approver/Security Analyst

ステップ 1　次の 2 つのオプションから選択できます。

- 手動でタスクを起動した場合は、タスク起動時に表示された通知ボックスの [Task Status] リンクをクリックします。

  ポップアップ ウィンドウに [Task Status] ページが表示されます。

- タスクをスケジュールした場合、または表示されていないページからタスクが起動された場合は、[System] > [Monitoring] > [Task Status] を選択します。

  [Task Status] ページが表示されます。

[Task Status] ページで実行できる操作については、タスク キューの管理を参照してください。

タスク キューの管理

ライセンス： すべて

自身のユーザ アカウントに Administrator、Maintenance User、Network Admin、Security Approver、または Security Analyst ユーザ ロールが割り当てられている場合は、次の表に示すように、タスク キューを表示（タスク キューの表示（C-1 ページ）を参照）しているときにいくつかの操作を実行できます。

表 C-2　タスク キューの操作

目的	操作
完了したすべてのタスクをタスク キューから削除する	[Remove Completed Jobs] をクリックします。
失敗したすべてのタスクをタスク キューから削除する	[Remove Failed Jobs] をクリックします。

表 C-2　タスク キューの操作（続き）

目的	操作
タスク キューから 1 つのタスクを削除する	削除するタスクの横にある削除アイコン（ ）をクリックします。 実行中のタスクは削除できないことに注意してください。実行中のタスクを削除する必要がある場合（例えばタスクが何度も失敗する場合）は、サポート担当にお問い合わせください。
タスク グループを縮小し、タスクを非表示にする	展開されたタスク グループの横にあるオープン フォルダ アイコン（）をクリックします。
タスク グループの中を展開し、タスクを表示する	縮小されたタスク グループの横にあるクローズド フォルダ アイコン（）をクリックします。

コマンドライン リファレンス

このリファレンスでは、FirePOWER アプライアンス、仮想デバイス、および ASA FirePOWER デバイスの ASA FirePOWER モジュール のコマンドライン インターフェイス（CLI）について説明します。CLI を使用して、FireSIGHT システムを表示、設定、およびトラブルシューティングすることができます。

注 コマンドライン インターフェイスは、Defense Center、シリーズ 2 アプライアンス、Blue Coat X-Series 向け Cisco NGIPS、または ASA FirePOWER デバイスの ASA モジュールではサポートされていません。

CLI モードには `show` や `configure` など多数あり、これらのモードにはモード名で始まる一連のコマンドが含まれています。モードを開始して、そのモードで有効なコマンドを入力することも、任意のモードからフル コマンドを入力することもできます。たとえば、Analyst1 というユーザ アカウントの情報を表示するには、CLI プロンプトで次のように入力します。

```
show user Analyst1
```

すでに `show` モードを開始している場合は、CLI プロンプトで次のように入力します。

```
user Analyst1
```

各モードで、ユーザが使用できるコマンドは、ユーザの CLI アクセスによって異なります。ユーザ アカウントを作成する場合は、手動で次のいずれかの CLI アクセス レベル に割り当てることができます。

- Basic

  ユーザは読み取り専用のアクセス権を持ち、システムのパフォーマンスに影響を与えるコマンドを実行することはできません。

- Configuration

  ユーザは、読み取り/書き込みアクセス権があり、システムのパフォーマンスに影響を与えるコマンドを実行することができます。

- なし

  ユーザはシェルにログインできません。

シリーズ 3 デバイスでは、Web インターフェイスの [User Management] ページでコマンドラインの権限を割り当てることができます。詳細については、ユーザの管理（61-1 ページ）を参照してください。仮想デバイスと ASA FirePOWER デバイスでは、CLI 自身を通じてコマンドラインの権限を割り当てます。

注 シリーズ 3 デバイスをリブートし、できるだけ早く CLI にログインしても、Web インターフェイスが使用できるようになるまで、実行するすべてのコマンドは監査ログに記録されません。

CLI コマンドでは大文字と小文字が区別されません。ただし、ユーザ名や検索フィルタなど、テキストが CLI フレームワークの一部ではないパラメータでは区別されることに注意してください。

コマンドラインへのログインの詳細については、アプライアンスへのログイン（2-1 ページ）を参照してください。

以降の項で、CLI コマンドについて説明します。

基本的な CLI コマンド

基本的な CLI コマンドを使用して、CLI とやりとりすることができます。これらのコマンドはデバイスの処理に影響しません。基本的なコマンドは、すべての CLI ユーザが使用できます。

以降の項で、基本のコマンドについて説明します。

configure password

現行のユーザは、自身のパスワードを変更することができます。コマンドを発行すると、CLI は現在の（古い）パスワードを入力するようユーザに要求し、その後で新しいパスワードを 2 回入力するよう要求します。

アクセス

Basic

構文

```
configure password
```

例

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

end

ユーザをデフォルトのモードに戻します(ユーザを任意の下位レベルの CLI コンテキストから最大デフォルト モードまで移動します)。

アクセス
Basic

構文
```
end
```

例
```
configure network ipv4> end
>
```

exit

CLI コンテキストを、次に高い CLI コンテキスト レベルへ移動します。デフォルト モードからこのコマンドを発行すると、ユーザは現行の CLI セッションからログアウトします。これは、CLI コマンドの `logout` を発行するのと同じです。

アクセス
Basic

構文
```
exit
```

例
```
configure network ipv4> exit
configure network>
```

help

CLI 構文の概要を表示します。

アクセス
Basic

構文
```
help
```

例
```
> help
```

history

現行のセッションのコマンドラインの履歴を表示します。

アクセス
Basic

構文

```
history limit
```

ここで *limit* は履歴リストのサイズを設定します。サイズを無制限に設定するには、0 を入力します。

例

```
history 25
```

logout

現行の CLI コンソール セッションから現行のユーザをログアウトします。

アクセス
Basic

構文

```
logout
```

例

```
> logout
```

?（疑問符）

CLI コマンドおよびパラメータの状況依存ヘルプを表示します。次のように、疑問符（?）のコマンドを使用します。

- 現在の CLI コンテキスト内で使用できるコマンドのヘルプを表示するには、コマンド プロンプトで疑問符（?）を入力します。
- 特定文字セットから始まる使用可能なコマンドのリストを表示するには、疑問符（?）に続けて短縮されたコマンドを入力します。
- コマンドの正式な引数のヘルプを表示するには、コマンド プロンプトの引数の代わりに疑問符（?）を入力します。

疑問符（?）は、コンソールにエコーバックされないことに注意してください。

アクセス
Basic

構文

```
?
abbreviated_command ?
command [arguments] ?
```

例

```
> ?
```

??（二重の疑問符）

CLI コマンドおよびパラメータの詳細な状況依存ヘルプを表示します。

アクセス

Basic

構文

```
??
abbreviated_command end??
command [arguments] ??
```

例

```
> configure manager add ??
```

show コマンド

Show コマンドは、デバイスの状態に関する情報を提供します。これらのコマンドはデバイスの動作モードを変更しません。また、これらのコマンドを実行しても、システムの動作に対する影響は最小限になります。ほとんどの show コマンドはすべての CLI ユーザが利用できますが、`show user` コマンドを発行できるのは、configuration CLI アクセス権限を持つユーザのみです。

以降の項では、show コマンドについて説明します。

access-control-config

次のように現在適用されているアクセス コントロールの設定を表示します:セキュリティ インテリジェンス設定、参照された SSL ポリシー、ネットワーク分析ポリシー、侵入ポリシー、およびファイル ポリシーの名前、侵入変数セットのデータ、ロギング設定、およびポリシー レベルのパフォーマンス、前処理、一般設定などのその他の詳細設定。

また、送信元と宛先のポート データ（ICMP エントリのタイプとコードを含む）および各アクセス コントロール ルールに一致した接続数（ヒット数）などの、ポリシーに関連する接続情報も表示します。

アクセス
Basic

構文
```
show access-control-config
```

例
```
> show access-control-config
```

alarms

デバイス上で、現行のアクティブな（失敗した/停止している）ハードウェアのアラームを表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス
Basic

構文
```
show alarms
```

例
```
> show alarms
```

arp-tables

ネットワークに適用できる該当するアドレス解決プロトコル テーブルを表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス
Basic

構文

```
show arp-tables
```

例

```
> show arp-tables
```

audit-log

監査ログが時系列の逆順に表示され、最も新しい監査ログ イベントが最初に示されます。

アクセス
Basic

構文

```
show audit-log
```

例

```
> show audit-log
```

bypass

使用中のインライン セットを表示し、それらのセットのバイパス モードの状態（標準またはバイパス）を示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス
Basic

構文

```
show bypass
```

例

```
> show bypass
```

clustering

デバイスのクラスタリング設定、ステータス、およびメンバ スタックの情報を表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス
Basic

config

デバイスにおけるクラスタリング設定を表示します。

構文

```
show clustering config
```

例

```
> show clustering config
```

clustering ha-statistics

クラスタ内のデバイスについて、状態共有統計情報を表示します。

構文

```
show clustering ha-statistics
```

例

```
> show clustering ha-statistics
```

cpu

デバイス上のすべての CPU のプラットフォームに適合する現行の CPU の使用率の統計情報を表示します。管理対象デバイスでは、次の値が表示されます。

- CPU

  プロセッサの数。

- 負荷

  0～100 の数値で表される CPU の使用率。0 はロードされていない状態で、100 は完全にロードされたことを表します。

仮想デバイスおよび ASA FirePOWER デバイスについては、次の値が表示されます。

- CPU

  プロセッサの数。

- %user

  ユーザ レベル（アプリケーション）で実行中に生じた CPU 使用率のパーセンテージ。

- %nice

  高い優先度で実行中に生じた CPU 使用率のパーセンテージ。

- %sys

  システム レベル（カーネル）で実行中に生じた CPU 使用率のパーセンテージ。これには、サービスの割り込みや softirqs で経過する時間は含まれません。softirq（ソフトウェアの割り込み）は、複数の CPU で同時に実行できる最大 32 個の列挙されたソフトウェア割り込みの 1 つです。

- %iowait

  システムに未処理のディスク I/O 要求があったときに、CPU がアイドル状態だった時間の割合（パーセンテージ）。

- %irq

  割り込みを行うために CPU が費やした時間の割合（パーセンテージ）。
- %soft

  softirqs を行うために CPU が費やした時間の割合（パーセンテージ）。
- %steal

  ハイパーバイザが別の仮想プロセッサを実行しているときに、仮想 CPU が強制的な待機で費やした時間の割合（パーセンテージ）
- %guest

  仮想プロセッサを実行するために CPU が費やした時間の割合（パーセンテージ）。
- %idle

  CPU がアイドル状態で、システムに未処理のディスク I/O 要求がなかった時間の割合（パーセンテージ）。

アクセス
Basic

構文

```
show cpu [procnum]
```

ここで *procnum* は、使用率の情報を表示するプロセッサの数を表します。有効な値は、0からシステム上のプロセッサ数よりも少ない数です。*procnum* が管理対象デバイスで使用されている場合は無視されます。このプラットフォームについては、使用率の情報はすべてのプロセッサについてのみ表示されるためです。

例

```
> show cpu
```

database

`show database` コマンドは、デバイスの管理インターフェイスを設定します。

アクセス
Basic

processes

実行中のデータベース クエリを表示します。

アクセス
Basic

構文

```
show database processes
```

例

```
> show database processes
```

slow-query-log

データベースのスロー クエリを表示します。

アクセス
Basic

構文
```
show database slow-query-log
```

例
```
> show database slow-query-log
```

device-settings

現行のデバイスに特有のアプリケーションのバイパス設定に関する情報を表示します。

アクセス
Basic

構文
```
show device-settings
```

例
```
> show device-settings
```

disk

現行のディスクの使用率を表示します。

アクセス
Basic

構文
```
show disk
```

例
```
> show disk
```

disk-manager

システムの各パート（サイロ、低水位、高水位など）のディスク使用率の詳細情報を表示します。

アクセス
Basic

構文

```
show disk-manager
```

例

```
> show disk-manager
```

dns

現行の DNS サーバのアドレスと検索ドメインを表示します。

アクセス
Basic

構文

```
show dns
```

例

```
> show dns
```

expert

シェルを起動します。

アクセス
Basic

構文

```
expert
```

例

```
> expert
```

fan-status

ハードウェア ファンの現在のステータスを表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス
Basic

構文

```
show fan-status
```

例

```
> show fan-status
```

fastpath-rules

現在設定されている fastpath ルールを表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス
Basic

構文
```
show fastpath-rules
```

例
```
> show fastpath-rules
```

GUI

Web インターフェイスの現在の状態を表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス
Basic

構文
```
show gui
```

例
```
> show gui
```

hostname

デバイスのホスト名およびアプライアンス UUID を表示します。CLI を使用してデバイスのホスト名を編集する場合は、管理する Defense Center に変更が反映されることを確認します。場合によっては、デバイス管理設定を手動で編集する必要があります。詳細については、デバイス管理設定の編集（4-57 ページ）を参照してください。

アクセス
Basic

構文
```
show hostname
```

例
```
> show hostname
```

hosts

ASA FirePOWER モジュールの /etc/hosts ファイルの内容を表示します。

アクセス
Basic

構文

```
show hosts
```

例

```
> show hosts
```

hyperthreading

ハイパースレッディングが有効か無効かを表示します。このコマンドは ASA FirePOWER デバイスでは使用できません。

アクセス
Basic

構文

```
show hyperthreading
```

例

```
> show hyperthreading
```

inline-sets

すべてのインライン セキュリティ ゾーンと関連するインターフェイスの設定データを表示します。このコマンドは ASA FirePOWER デバイスでは使用できません。

アクセス
Basic

構文

```
show inline-sets
```

例

```
> show inline-sets
```

interfaces

パラメータが指定されていない場合は、設定されているすべてのインターフェイスのリストが表示されます。パラメータが指定されている場合は、指定されたインターフェイスの詳細情報が表示されます。

アクセス
Basic

構文

```
show interfaces [interface]
```

ここで *interface* は詳細情報を表示する特定のインターフェイスです。

例

```
> show interfaces
```

ifconfig

ASA FirePOWER モジュールに対するインターフェイスの設定を表示します。

アクセス
Basic

構文

```
show ifconfig
```

例

```
> show ifconfig
```

lcd

LCD のハードウェア ディスプレイが有効か無効かを表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス
Basic

構文

```
show lcd
```

例

```
> show lcd
```

link-aggregation

show link-aggregation コマンドは、リンク集約グループ（LAG）の設定および統計情報を表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス
Basic

configuration

LAG ID、インターフェイスの数、コンフィギュレーション モード、ロード バランシング モード、LACP 情報、および物理インターフェイスのタイプなど、設定された各 LAG の設定の詳細を表示します。

アクセス
Basic

構文

```
show link-aggregation configuration
```

例

```
> show link-aggregation configuration
```

statistics

ステータス、リンク ステートと速度、コンフィギュレーション モード、送受信されたパケットのカウンタ、および送受信されたバイトのカウンタなど、設定された各 LAG の統計情報をインターフェイスごとに表示します。

アクセス
Basic

構文

```
show link-aggregation statistics
```

例

```
> show link-aggregation statistics
```

link-state

デバイスのポートのタイプ、リンク、スピード、速度、デュプレックスの状態およびバイパス モードを表示します。このコマンドは ASA FirePOWER デバイスでは使用できません。

アクセス
Basic

構文

```
show link-state
```

例

```
> show link-state
```

log-ips-connection

記録された侵入イベントに関連付けられている接続イベントのロギングが有効か無効かを表示します。

アクセス

Basic

構文

```
show log-ips-connection
```

例

```
> show log-ips-connection
```

managers

Defense Centerの設定および通信のステータスを表示します。登録キーおよび NAT ID は、登録が保留中の場合のみ表示されます。デバイスが高可用性ペアに登録されている場合、管理している両方のDefense Centerの情報が表示されます。デバイスが、スタック設定のセカンダリ デバイスとして設定されている場合、管理している両方の Defense Center、およびプライマリ デバイスに関する情報が表示されます。

アクセス

Basic

構文

```
show managers
```

例

```
> show managers
```

memory

デバイスの合計メモリ、使用中のメモリ、使用可能なメモリを表示します。

アクセス

Basic

構文

```
show memory
```

例

```
> show memory
```

model

デバイスのモデル情報を表示します。

アクセス
Basic

構文
```
show model
```

例
```
> show model
```

mpls-depth

管理インターフェイスに設定されている MPLS レイヤ数を 0～6 で表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス
Basic

構文
```
show mpls-depth
```

例
```
> show mpls-depth
```

NAT

`show nat` コマンドは、管理インターフェイスの NAT データと設定情報を表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス
Basic

active-dynamic

ダイナミック ルールに従って変換されている NAT フローを表示します。これらのエントリは、フローがルールに一致している場合に、ルールがタイムアウトになるまで表示されます。したがって、リストは正確ではないことがあります。タイムアウトはプロトコルに依存します。ICMP は 5 秒、UDP は 120 秒、TCP は 3600 秒、他のすべてのプロトコルは 60 秒です。

構文
```
show nat active-dynamic
```

例
```
> show nat active-dynamic
```

active-static

スタティック ルールに従って変換されている NAT フローを表示します。これらのエントリは、デバイスにルールが適用されるとすぐに表示されます。リストは、スタティックな NAT ルールに一致しているアクティブな フローを示しているわけではありません。

構文

```
show nat active-static
```

例

```
> show nat active-static
```

allocators

すべての NAT アロケータの情報、ダイナミック ルールで使用されている変換済みアドレスのプールを表示します。

構文

```
show nat allocators
```

例

```
> show nat allocators
```

config

管理インターフェイスの現行の NAT ポリシーの設定を表示します。

構文

```
show nat config
```

例

```
> show nat config
```

dynamic-rules

指定されたアロケータ ID を使用しているダイナミックな NAT ルールを表示します。

構文

```
show nat dynamic-rules allocator_id
```

例

```
> show nat dynamic-rules 9
```

ここで *allocator_id* は有効なアロケータ ID 番号です。

flows

指定されたアロケータ ID を使用しているルールについてフローの数を表示します。

構文

```
show nat flows allocator-id
```

例

```
> show nat flows 81
```

ここで *allocator_id* は有効なアロケータ ID 番号です。

static-rules

すべてのスタティック NAT ルールを表示します。

構文

```
show nat static-rules
```

例

```
> show nat static-rules
```

netstat

ASA FirePOWER モジュールのアクティブなネットワーク接続を表示します。

アクセス

Basic

構文

```
show netstat
```

例

```
> show netstat
```

network

管理インターフェイスの IPv4 および IPv6 の設定、MAC アドレス、HTTP プロキシ アドレス、ポート、ユーザ名（設定されている場合）を表示します。

アクセス

Basic

構文

```
show network
```

例

```
> show network
```

network-modules

インストールされているすべてのモジュール、およびモジュールの情報（シリアル番号など）を表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス
Basic

構文

```
show network-modules
```

例

```
> show network-modules
```

network-static-routes

インターフェイス、宛先アドレス、ネットワーク マスク、およびゲートウェイ アドレスなど、設定済みのすべてのネットワーク スタティック ルートとその情報が表示されます。

アクセス
Basic

構文

```
show network-static-routes
```

例

```
> show network-static-routes
```

ntp

NTP コンフィギュレーションを表示します。

アクセス
Basic

構文

```
show ntp
```

例

```
> show ntp
```

perfstats

デバイスのパフォーマンスの統計情報を表示します。

アクセス
Basic

構文

```
show perfstats
```

例

```
> show perfstats
```

portstats

デバイスにインストールされているすべてのポートのポート統計情報を表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス

Basic

構文

```
show portstats [copper | fiber | internal | external | all]
```

ここで `copper` はすべての銅線ポートを表し、fiber はすべてのファイバ ポート、internal はすべての内部ポート、external はすべての外部（銅線およびファイバ）ポート、all はすべてのポート（外部および内部）を表します。

例

```
> show portstats fiber
```

power-supply-status

ハードウェアの電源の現在の状態を表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス

Basic

構文

```
show power-supply-status
```

例

```
> show power-supply-status
```

process-tree

デバイスで実行中のプロセスについて、タイプごとにツリー形式でソートして表示します。

アクセス

Basic

構文

```
show process-tree
```

例

```
> show process-tree
```

processes

デバイス上で実行中のプロセスについて、CPU 使用率の降順で表示します。

アクセス
Basic

構文

```
show processes [sort-flag] [filter]
```

ここで、メモリ（の降順）でソートする場合は、`sort-flag` に `-m` を指定し、プロセス名ではなくユーザ名でソートする場合は `-u` を指定します。また、コマンドのフルネームおよびパスを表示する場合は `verbose` を指定します。*`filter`* パラメータは、コマンドの検索語または結果をフィルタするために使用するユーザ名を指定します。見出し行は表示されたままです。

例

```
> show processes -u user1
```

route

ASA FirePOWER モジュールのルーティング情報を表示します。

アクセス
Basic

構文

```
show route
```

例

```
> show route
```

routing-table

パラメータが指定されていない場合は、すべての仮想ルータのルーティング情報を表示します。パラメータが指定されている場合は、指定されたルータのルーティング情報、および該当する場合は、指定されたルーティングのプロトコル タイプを表示します。パラメータはすべてオプションです。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス
Basic

構文

```
show routing-table [name] [ ospf | rip | static ]
```

ここで *`name`* は、情報を表示する特定のルータの名前で、`ospf`、`rip`、および `static` はルーティングプロトコルのタイプを表します。

例

```
> show routing-table Vrouter1 static
```

serial-number

シャーシのシリアル番号を表示します。このコマンドは仮想デバイスでは使用できません。

アクセス
Basic

構文

```
show serial-number
```

例

```
> show serial-number
```

ssl-policy-config

現在適用されている SSL ポリシーの設定（ポリシーの説明、デフォルトのロギング設定、有効なすべての SSL ルールとルールの設定など）、信頼できる CA 証明書、および復号化不可能なトラフィックのアクションを表示します。

アクセス
Basic

構文

```
show ssl-policy-config
```

例

```
> show ssl-policy-config
```

stacking

管理対象デバイスのスタッキングの設定とポジションを表示します。プライマリとして設定されているデバイスでは、すべてのセカンダリ デバイスのデータも示されます。クラスタ化されたスタックでは、このコマンドにより、スタックがクラスタのメンバであることも示します。スタッキングを有効または無効にする（大半の場合は無効にする）には、ユーザは Web インターフェイスを使用する必要があります。スタッキングが有効になっていない場合、コマンドは `Stacking not currently configured` というメッセージを返します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス
Basic

構文

```
show stacking
```

例

```
> show stacking
```

summary

デバイスに関して最もよく使用される情報（バージョン、タイプ、UUID など）のサマリーを表示します。詳細については、show コマンド：version（D-27 ページ）、interfaces（D-15 ページ）、device-settings（D-11 ページ）、および access-control-config（D-7 ページ）を参照してください。

アクセス
Basic

構文

```
show summary
```

例

```
> show summary
```

time

現在の日付と時刻を、UTC および現行のユーザに設定されているローカル タイム ゾーンで表示します。

アクセス
Basic

構文

```
show time
```

例

```
> show time
```

traffic-statistics

パラメータが指定されていない場合は、すべてのポートから送信された、および受信したバイトの詳細情報を表示します。ポートが指定されている場合は、指定されたポートの情報のみを表示します。ASA FirePOWER デバイスに対してポートを指定することはできません。システムはデータのプレーン インターフェイスのみを表示します。

アクセス
Basic

構文

```
show traffic-statistics [port]
```

ここで port は、情報を表示する特定のポートです。

例

```
> show traffic-statistics s1p1
```

user

仮想デバイスに対してのみ適用されます。指定されたユーザに関する設定の詳細情報を表示します。次の値が表示されます。

- Login：ログイン名
- UID：ユーザ ID（数値）
- Auth（`Local` または `Remote`）：ユーザがどのように認証されているか
- Access（`Basic` または `Config`）：ユーザの権限レベル
- Enabled（`Enabled` または `Disabled`）：ユーザがアクティブかどうか
- Reset（`Yes` または `No`）：次のログイン時にユーザがパスワードを変更する必要があるかどうか
- Exp（`Never` または数値）：ユーザのパスワード変更が必要になるまでの日数
- Warn（`N/A` または数値）：パスワードの有効期限が切れる前に、ユーザがパスワード変更のために与えられる日数
- Str（`Yes` または `No`）：ユーザのパスワードが強度チェックの基準を満たす必要があるかどうか
- Lock（`Yes` または `No`）：ログインの失敗が多すぎる場合に、ユーザのアカウントがロックされるかどうか
- Max（`N/A` または数値）：ユーザのアカウントがロックされる前に失敗するログインの最大回数

アクセス

設定（Configuration）

構文

```
show user username username username ...
```

ここで *username* はユーザの名前を表します。複数の username はスペースで区切って指定します。

例

```
> show user jdoe
```

users

仮想デバイスに対してのみ適用されます。すべてのローカル ユーザの設定の詳細情報を表示します。次の値が表示されます。

- Login：ログイン名
- UID：ユーザ ID（数値）
- Auth（`Local` または `Remote`）：ユーザがどのように認証されているか
- Access（`Basic` または `Config`）：ユーザの権限レベル
- Enabled（`Enabled` または `Disabled`）：ユーザがアクティブかどうか
- Reset（`Yes` または `No`）：次のログイン時にユーザがパスワードを変更する必要があるかどうか
- Exp（`Never` または数値）：ユーザのパスワード変更が必要になるまでの日数
- Warn（`N/A` または数値）：パスワードの有効期限が切れる前に、ユーザがパスワード変更のために与えられる日数
- Str（`Yes` または `No`）：ユーザのパスワードが強度チェックの基準を満たす必要があるかどうか

- Lock（Yes または No）：ログインの失敗が多すぎる場合に、ユーザのアカウントがロックされるかどうか
- Max（N/A または数値）：ユーザのアカウントがロックされる前に失敗するログインの最大回数

アクセス

設定（Configuration）

構文

```
show users
```

例

```
> show users
```

version

製品のバージョンとビルドを表示します。*detail* パラメータが指定されている場合は、追加のコンポーネントのバージョンが表示されます。

アクセス

Basic

構文

```
show version [detail]
```

例

```
> show version
```

virtual-routers

パラメータが指定されていない場合は、現在設定されているすべての仮想ルータのリスト、および DHCP リレー、OSPF、および RIP の情報が表示されます。パラメータが指定されている場合は、指定されたルータに関する情報が、指定されたルート タイプによって制限されて表示されます。パラメータはすべてオプションです。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス

Basic

構文

```
show virtual-routers [ dhcprelay | ospf | rip ] [name]
```

ここで dhcprelay、ospf、および rip はルート タイプを表します。*name* は、情報を表示する特定のルータの名前を表します。ospf を指定した場合は、ルート タイプ、および（存在する場合は）ルート名に対して neighbors、topology、または lsadb を指定することができます。

例

```
> show virtual-routers ospf VRouter2
```

virtual-switches

パラメータが指定されていない場合は、設定されているすべての仮想スイッチのリストが表示されます。パラメータが指定されている場合は、指定されたスイッチに関する情報が表示されます。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス
Basic

構文

```
show virtual-switches [name]
```

例

```
> show virtual-switches Vswitch1
```

vmware-tools

VMware Tools が、仮想デバイス上で現在有効になっているかどうかを示します。このコマンドは、仮想デバイスでのみ使用できます。

VMwareツールは、仮想マシンのパフォーマンスを向上させるためのユーティリティ スイートです。これらのユーティリティを使用すると、VMware 製品の便利な機能をすべて活用できます。このシステムは、すべての仮想アプライアンスで次のプラグインをサポートします。

- guestInfo
- powerOps
- snapshot
- timeSync
- vmbackup

VMware ツールおよびサポートされるプラグインの詳細については、VMware の Web サイト (http://www.vmware.com) を参照してください。

アクセス
Basic

構文

```
show vmware-tools
```

例

```
> show vmware-tools
```

VPN

`show VPN` コマンドは、VPN ステータス、および VPN 接続の設定情報を表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス
Basic

config

すべての VPN 接続の設定を表示します。

構文

```
show vpn config
```

例

```
> show vpn config
```

config by virtual router

仮想ルータについて、すべての VPN 接続の設定を表示します。

構文

```
show vpn config [virtual router]
```

例

```
> show vpn config VRouter1
```

status

VPN 接続すべてのステータスを表示します。

構文

```
show vpn status
```

例

```
> show vpn status
```

status by virtual router

仮想ルータについて、すべての VPN 接続のステータスを表示します。

構文

```
show vpn status [virtual router]
```

例

```
> show vpn status VRouter1
```

counters

すべての VPN 接続のカウンタを表示します。

構文

```
show vpn counters
```

例

```
> show vpn counters
```

counters by virtual router

仮想ルータについて、すべての VPN 接続のカウンタを表示します。

構文

```
show vpn counters [virtual router]
```

例

```
> show vpn counters VRouter1
```

コンフィギュレーション コマンド

コンフィギュレーション コマンドを使用して、システムを設定および管理することができます。これらのコマンドはシステムの動作に影響を与えます。そのため、Basic レベルの `configure password` を除いては、Configuration CLI アクセス権限を持つユーザのみがこれらのコマンドを発行できます。

以降の項で、コンフィギュレーション コマンドについて説明します。

clustering

デバイス上のクラスタリングに対してバイパスを無効にするか、または設定します。このコマンドは仮想デバイス、ASA FirePOWER デバイス、またはセカンダリ スタック メンバとして設定されているデバイスでは使用できません。

アクセス

設定（Configuration）

構文

```
configure clustering {disable | bypass}
```

例

```
> configure clustering disable
```

bypass

インライン ペアのバイパス モードを開いたり閉じたりします。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス

設定（Configuration）

構文

```
configure bypass {open | close} {interface}
```

ここで、*interface* はインライン ペアのいずれかのハードウェア ポートの名前です。

例

```
> configure bypass open s1p1
```

GUI

デバイスの Web インターフェイス（システムのメジャーな更新時に表示される、簡潔なアップグレード Web インターフェイスなど）を有効または無効にします。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス

設定（Configuration）

構文

```
configure gui {enable | disable}
```

例

```
> configure gui disable
```

lcd

デバイスの正面の LCD ディスプレイを有効または無効にします。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス

設定（Configuration）

構文

```
configure lcd {enable | disable}
```

例

```
> configure lcd disable
```

log-ips-connections

記録された侵入イベントに関連付けられている接続イベントのロギングを有効または無効にします。

アクセス

設定（Configuration）

構文

```
configure log-ips-connections {enable | disable}
```

例

```
> configure log-ips-connections disable
```

manager

`configure manager` コマンドは、管理元のDefense Centerへのデバイスの接続を設定します。

アクセス

設定（Configuration）

add

管理元のDefense Centerからの接続を承認するようデバイスを設定します。このコマンドは、デバイスがアクティブに管理されていない場合のみ機能します。

デバイスをDefense Centerに登録するには、一意の英数字による登録キーが必要です。ほとんどの場合は、登録キーと一緒にホスト名または IP アドレスを指定する必要があります。ただし、デバイスとDefense Centerが NAT デバイスによって分けられている場合は、登録キーと一緒に一意の NAT ID を入力し、ホスト名の代わりに `DONTRESOLVE` を指定します。

構文

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} regkey
[nat_id]
```

ここで {*hostname* | *IPv4_address* | *IPv6_address* | `DONTRESOLVE`} は、このデバイスを管理する Defense Center の DNS ホスト名、または IP アドレス（IPv4 または IPv6）を表します。Defense Centerが直接アドレス指定できない場合は、`DONTRESOLVE` を使用してください。`DONTRESOLVE` を使用する場合は、*nat_id* が必要です。*regkey* はデバイスをDefense Centerへ登録するのに必要な、英数字の一意の登録キーです。*nat_id* はオプションの英数字の文字列で、Defense Centerとデバイス間の登録プロセスで使用されます。hostname が `DONTRESOLVE` に設定されている場合に必要です。

例

```
> configure manager add DONTRESOLVE abc123 efg456
```

delete

Defense Centerの接続情報をデバイスから削除します。このコマンドは、デバイスがアクティブに管理されていない場合のみ機能します。

構文

```
configure manager delete
```

例

```
> configure manager delete
```

mpls-depth

管理インターフェイスで MPLS レイヤの数を設定します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス

設定（Configuration）

構文

```
configure mpls-depth {depth}
```

ここで *depth* は 0～6 の数値です。

例

```
> configure mpls-depth 3
```

network

`configure network` コマンドは、デバイスの管理インターフェイスを設定します。

アクセス

設定（Configuration）

dns searchdomains

DNS 検索ドメインの現行のリストを、コマンドで指定されたリストに置き換えます。

構文

```
configure network dns searchdomains {searchlist}
```

searchlist はカンマで区切られたドメインのリストです。

例

```
> configure network dns searchdomains foo.bar.com,bar.com
```

dns servers

DNS サーバの現行のリストを、コマンドで指定されたリストに置き換えます。

構文

```
configure nework dns servers {dnslist}
```

dnslist は、カンマで区切られた DNS サーバのリストです。

例

```
> configure network dns servers 10.123.1.10,10.124.1.10
```

hostname

デバイスのホスト名を設定します。

構文

```
configure network hostname {name}
```

name は新しいホスト名です。

例

```
> configure network hostname sfrocks
```

http-proxy

シリーズ 3 および仮想デバイスで、HTTP プロキシを設定します。コマンドを発行した後で、CLI はユーザに対して HTTP プロキシのアドレスとポート、プロキシの認証が必要かどうかを尋ねます。認証が必要な場合はプロキシのユーザ名、プロキシのパスワード、およびプロキシのパスワードの確認を入力するよう要求されます。

仮想デバイス上でこのコマンドを使用して、HTTP プロキシ サーバを設定し、仮想デバイスが動的解析のためにファイルを Collective Security Intelligence クラウド へ送信できるようにします。

構文

```
configure network http-proxy
```

例

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address:
Enter HTTP Proxy Port:
Use Proxy Authentication?(y/n) [n]:
Enter Proxy Username:
Enter Proxy Password:
Confirm Proxy Password:
```

http-proxy-disable

シリーズ 3 および仮想デバイスで、すべての HTTP プロキシの設定を削除します。

構文

```
configure network http-proxy-disable
```

例

```
> configure network http-proxy-disable
Are you sure that you wish to delete the current http-proxy configuration?(y/n):
```

ipv4 delete

デバイスの管理インターフェイスの IPv4 設定を無効にします。

構文

```
configure network ipv4 delete
```

例

```
> configure network ipv4 delete
```

ipv4 dhcp

デバイスの管理インターフェイスの IPv4 設定を DHCP に設定します。管理インターフェイスは DHCP サーバと通信して、設定情報を取得します。

構文

```
configure network ipv4 dhcp
```

例

```
> configure network ipv4 dhcp
```

ipv4 manual

デバイスの管理インターフェイスの IPv4 設定を手動で設定します。

構文

```
configure network ipv4 manual ipaddr netmask gw
```

ここで *ipaddr* は IP アドレスで、*netmask* はサブネットマスク、*gw* はデフォルト ゲートウェイの IPv4 アドレスです。

例

```
> configure network ipv4 manual 10.123.1.10 255.255.0.0 10.123.1.1
```

ipv6 delete

デバイスの管理インターフェイスの IPv6 設定を無効にします。

構文

```
configure network ipv6 delete
```

例

```
> configure network ipv6 delete
```

ipv6 dhcp

デバイスの管理インターフェイスの IPv6 設定を DHCP に設定します。管理インターフェイスは DHCP サーバと通信して、設定情報を取得します。

構文

```
configure network ipv6 dhcp
```

例

```
> configure network ipv6 dhcp
```

ipv6 router

デバイスの管理インターフェイスの IPv6 設定をルータに設定します。管理インターフェイスは IPv6 ルータと通信して、設定情報を取得します。

構文

```
configure network ipv6 router
```

例

```
> configure network ipv6 router
```

ipv6 manual

デバイスの管理インターフェイスの IPv6 設定を手動で設定します。

構文

```
configure network ipv6 manual ip6addr/ip6prefix [ip6gw]
```

ここで *ip6addr/ip6prefix* は IP アドレスと接頭辞の長さで、ip6*gw* はデフォルト ゲートウェイの IPv6 アドレスを表します。

例

```
> configure network ipv6 manual 2001:DB8:3ffe:1900:4545:3:200:f8ff:fe21:67cf 64
```

management-interface disable

指定した管理インターフェイスを無効にします。

構文

```
configure network management-interface disable ethn
```

n は、無効にする管理インターフェイスの数です。

例

```
> configure network management-interface disable eth1
```

management-interface disable-event-channel

指定した管理インターフェイスを介したイベント伝送を無効にします。

構文

```
configure network management-interface disable-event-channel ethn
```

n は、無効にする管理インターフェイスの数です。

例

```
> configure network management-interface disable-event-channel eth1
```

management-interface disable-management-channel

指定した管理インターフェイスを介した管理伝送を無効にします。

構文

```
configure network management-interface disable-management-channel ethn
```

n は、無効にする管理インターフェイスの数です。

例

```
> configure network management-interface disable-management-channel eth1
```

management-interface enable

指定した管理インターフェイスを有効にします。

構文

```
configure network management-interface enable ethn
```

n は、有効にする管理インターフェイスの数です。

例

```
> configure network management-interface enable eth1
```

management-interface enable-event-channel

指定した管理インターフェイスを介したイベント伝送を有効にします。

構文

```
configure network management-interface enable-event-channel ethn
```

n は、有効にする管理インターフェイスの数です。

例

```
> configure network management-interface enable-event-channel eth1
```

management-interface enable-management-channel

指定した管理インターフェイスを介した管理伝送を有効にします。

構文

```
configure network management-interface enable-management-channel ethn
```

n は、有効にする管理インターフェイスの数です。

例

```
> configure network management-interface enable-management-channel eth1
```

management-interface tcpport

管理用の TCP ポートの値を変更します。

構文

```
configure network management-interface tcpport port
```

port は設定する管理ポートの値です。

例

```
> configure network management-interface tcpport 8500
```

management-port

デバイスの TCP 管理ポートの値を設定します。

構文

```
configure network management-port number
```

number は設定する管理ポートの値を表します。

例

```
> configure network management-port 8500
```

static-routes ipv4 add

指定した管理インターフェイスの IPv4 スタティック ルートを追加します。

構文

```
configure network static-routes ipv4 add interface destination netmask gateway
```

interface は管理インターフェイス、*destination* は宛先 IP アドレス、*netmask* はネットワーク マスク アドレス、*gateway* は追加するゲートウェイ アドレスです。

例

```
> configure network static-routes ipv4 add eth1 10.115.24.0 255.255.255.0 10.115.9.2
```

static-routes ipv4 delete

指定した管理インターフェイスの IPv4 スタティック ルートを削除します。

構文

```
configure network static-routes ipv4 delete interface destination netmask gateway
```

interface は管理インターフェイス、*destination* は宛先 IP アドレス、*netmask* はネットワーク マスク アドレス、*gateway* は削除するゲートウェイ アドレスです。

例

```
> configure network static-routes ipv4 delete eth1 10.115.24.0 255.255.255.0
10.115.9.2
```

static-routes ipv6 add

指定した管理インターフェイスの IPv6 スタティック ルートを追加します。

構文

```
configure network static-routes ipv6 add interface destination prefix gateway
```

interface は管理インターフェイス、*destination* は宛先 IP アドレス、*prefix* は IPv6 プレフィックス長、*gateway* は追加するゲートウェイ アドレスです。

例

```
> configure network static-routes ipv6 add eth1 2001:DB8:3ffe:1900:4545:3:200:
f8ff:fe21:67cf 64
```

static-routes ipv6 delete

指定した管理インターフェイスの IPv6 スタティック ルートを削除します。

構文

```
configure network static-routes ipv6 delete interface destination prefix gateway
```

interface は管理インターフェイス、*destination* は宛先 IP アドレス、*prefix* は IPv6 プレフィックス長、*gateway* は削除するゲートウェイ アドレスです。

例

```
> configure network static-routes ipv6 delete eth1 2001:DB8:3ffe:1900:4545:3:200:f8ff:
fe21:67cf 64
```

password

現行のユーザは、自身のパスワードを変更することができます。コマンドを発行すると、CLI は現在の（古い）パスワードを入力するようユーザに要求し、その後で新しいパスワードを 2 回入力するよう要求します。

アクセス

Basic

構文

```
configure password
```

例

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

stacking disable

管理対象デバイスで、そのデバイスのスタッキング設定をすべて削除します。プライマリとして設定されているデバイスでは、スタックが完全に削除されます。セカンダリとして設定されているデバイスでは、デバイスはスタックから削除されます。このコマンドは、仮想デバイス、または ASA FirePOWER デバイスでは使用できません。また、このコマンドを使用して、クラスタ化されたスタックをクラスタ化解除することはできません。

スタッキング階層の上位アプライアンスとの通信を確立できない場合は、このコマンドを使用します。Defense Centerを通信で使用できる場合は、代わりにDefense CenterWeb インターフェイスを使用するよう伝えるメッセージが表示されます。同様に、プライマリ デバイスを使用できる場合に、セカンダリとして設定されているデバイス上で `stacking disable` を入力すると、プライマリ デバイスからコマンドを入力するよう伝えるメッセージが表示されます。

アクセス
設定（Configuration）

構文
```
configure stacking disable
```

例
```
> configure stacking disable
```

user

仮想デバイスでのみ使用できます。`configure user` コマンドは、デバイスのローカル ユーザ データベースを管理します。

アクセス
設定（Configuration）

アクセス
指定したユーザのアクセス レベルを変更します。このコマンドは、指定されたユーザが次にログインするときに有効になります。

構文
```
configure user access username [basic | config]
```

例
```
> configure user access jdoe basic
```
username は、アクセスを変更するユーザの名前を表します。`basic` は basic アクセスを、`config` は configuration アクセスを表します。

add

指定された名前とアクセス レベルで新しいユーザを作成します。このコマンドでは、ユーザのパスワードを入力するよう要求されます。

構文
```
configure user add username [basic | config]
```
ここで *username* は新しいユーザの名前を表します。`basic` は basic アクセス、`config`は configuration アクセスを表します。

例
```
> configure user add jdoe basic
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

aging

ユーザ パスワードに有効期限を設定します。

構文

```
configure user aging username max_days warn_days
```

ここで *username* はユーザの名前を表します。*max_days* はパスワードが有効な最大日数、*warn_days* は、有効期限が切れるまでにパスワードを変更するためにユーザが使用できる日数を表します。

例

```
> configure user aging jdoe 100 3
```

delete

ユーザとユーザのホーム ディレクトリを削除します。

構文

```
configure user delete username
```

username はユーザの名前を表します。

例

```
> configure user delete jdoe
```

disable

ユーザを無効にします。無効なユーザはログインできません。

構文

```
configure user disable username
```

username はユーザの名前を表します。

例

```
> configure user disable jdoe
```

enable

ユーザを有効にします。

構文

```
configure user enable username
```

username はユーザの名前を表します。

例

```
> configure user enable jdoe
```

forcereset

ユーザが次にログインするときに、パスワードの変更を要求します。ユーザがログインしてパスワードを変更すると、強度のチェックが自動的に有効になります。

構文

```
configure user forcereset username
```

username はユーザの名前を表します。

例

```
> configure user forcereset jdoe
```

maxfailedlogins

指定したユーザが、ログインで失敗できる最大回数を設定します。

構文

```
configure user maxfailedlogins username number
```

username はユーザの名前、*number* は、ログインで失敗できる最大回数を表します。

例

```
> configure user maxfailedlogins jdoe 3
```

password

ユーザのパスワードを設定します。このコマンドでは、ユーザのパスワードを入力するよう要求されます。

構文

```
configure user password username
```

username はユーザの名前を表します。

例

```
> configure user pasword jdoe
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

strengthcheck

ユーザのパスワードに対する強度の要件を有効または無効にします。ユーザ パスワードの有効期限が切れた場合、または configure user forcereset コマンドを使用している場合は、ユーザが次にログインしたときにこの要件が自動的に有効になります。

構文

```
configure user strengthcheck username {enable | disable}
```

username はユーザの名前を表します。`enable` は指定されたユーザのパスワードの要件を設定し、`disable` は、指定されたユーザのパスワードの要件を削除します。

例

```
> configure user strengthcheck jdoe enable
```

unlock

ログイン失敗の最大数を超過したユーザをロック解除します。

構文

```
configure user unlock username
```

username はユーザの名前を表します。

例

```
> configure user unlock jdoe
```

vmware-tools

仮想デバイス上で VMware Tools 機能を有効または無効にします。このコマンドは、仮想デバイスでのみ使用できます。

VMwareツールは、仮想マシンのパフォーマンスを向上させるためのユーティリティ スイートです。これらのユーティリティを使用すると、VMware 製品の便利な機能をすべて活用できます。システムは、すべての仮想アプライアンスについて以下のプラグインをサポートしています。

- guestInfo
- powerOps
- snapshot
- timeSync
- vmbackup

VMware ツールおよびサポートされるプラグインの詳細については、VMware の Web サイト (http://www.vmware.com) を参照してください。

アクセス

Basic

構文

```
configure vmware-tools (enable | disable)
```

例

```
> configure vmware-tools enable
```

system コマンド

system コマンドを使用して、システム全体のファイルおよびアクセス コントロールの設定を管理することができます。Configuration CLI アクセス権を持つユーザのみが、システム モードでコマンドを発行できます。

以降の項で、system コマンドについて説明します。

- access-control（D-44 ページ）
- disable-http-user-cert（D-45 ページ）
- file（D-45 ページ）

access-control

`system access-control` コマンドは、ユーザがデバイス上でアクセス コントロールの設定を管理できるようにします。

アクセス

設定（Configuration）

archive

現在適用されているアクセス コントロール ポリシーを、`/var/common` にテキスト ファイルとして保存します。

構文

```
system access-control archive
```

例

```
> system access-control archive
```

clear-rule-counts

アクセス コントロール ルールのヒット数を 0 にリセットします。

構文

```
system access-control clear-rule-counts
```

例

```
> system access-control clear-rule-counts
```

rollback

以前に適用していたアクセス コントロールの設定に、システムを戻します。クラスタ化されたデバイス、またはスタック デバイスではこのコマンドは使用できません。

構文

```
system access-control rollback
```

例

```
> system access-control rollback
```

disable-http-user-cert

システム上に存在するすべての HTTP ユーザ証明書を削除します。

アクセス
設定（Configuration）

構文
```
system disable-http-user-cert
```

例
```
> system disable-http-user-cert
```

file

`system file` コマンドを使用すると、ユーザは、デバイス上の common ディレクトリにあるファイルを管理することができます。

アクセス
設定（Configuration）

copy

FTP を使用して、ログイン ユーザ名を使用しているホスト上のリモート ロケーションへファイルを転送します。ローカル ファイルは common ディレクトリに配置する必要があります。

構文
```
system file copy hostname username path filenames filenames ...
```
hostname はターゲットのリモート ホストの名前または IP アドレスを表します。*username* はリモート ホスト上のユーザの名前、*path* はリモート ホスト上の宛先パス、*filenames* は転送するローカル ファイルを表します。複数のファイル名はスペースで区切って指定します。

例
```
> system file copy sfrocks jdoe /pub *
```

delete

common ディレクトリから、指定したファイルを削除します。

構文
```
system file delete filenames filenames ...
```
filenames は削除するファイルを指定します。複数のファイル名はスペースで区切って指定します。

例
```
> system file delete *
```

list

ファイル名が指定されていない場合は、common ディレクトリ内のすべてのファイルについて変更の時刻、サイズ、およびファイル名が表示されます。ファイル名が指定されている場合は、指定されたファイル名と一致したファイルで、変更の時刻、サイズ、およびファイル名が表示されます。

構文

```
system file list {filenames filenames ...}
```

`filenames` は表示するファイルを表します。複数のファイル名はスペースで区切って指定します。

例

```
> system file list
```

secure-copy

SCP を使用して、ログイン ユーザ名を使用しているホスト上のリモート ロケーションへファイルを転送します。ローカル ファイルは `/var/common` ディレクトリに配置する必要があります。

構文

```
system file secure-copy hostname username path filenames filenames ...
```

hostname はターゲットのリモート ホストの名前または IP アドレスを表します。*username* はリモート ホスト上のユーザの名前、*path* はリモート ホスト上の宛先パス、*filenames* は転送するローカル ファイルを表します。複数のファイル名はスペースで区切って指定します。

例

```
> system file secure-copy 10.123.31.1 jdoe /tmp *
```

generate-troubleshoot

シスコが解析に使用するトラブルシューティング データを生成します。

アクセス

設定（Configuration）

構文

```
system generate-troubleshoot
```

この構文は、どのトラブルシューティング データを表示するかを指定するための、オプションのパラメータのリストを表示します。

例

```
> system generate-troubleshoot
```

ldapsearch

ユーザが、指定された LDAP サーバのクエリを実行できるようにします。すべてのパラメータが必須であることに注意してください。

アクセス

設定（Configuration）

構文

```
system ldapsearch host port baseDN userDN basefilter
```

host は LDAP サーバのドメイン、*port* は LDAP サーバのポート、*baseDN* は検索する DN（識別名）、*userDN* は LDAP ディレクトリへバインドするユーザの DN、*basefilter* は検索するレコードを表します。

例

```
> system ldapsearch ldap.example.com 389 cn=users,
dc=example,dc=com cn=user1,cn=users,dc=example,dc=com, cn=user2
```

lockdown-sensor

`expert` コマンドを削除し、デバイス上の bash シェルへアクセスします。

注意 このコマンドは、サポートからのホットフィックスがない場合は取り消すことはできません。使用には注意が必要です。

アクセス

設定（Configuration）

構文

```
system lockdown-sensor
```

例

```
> system lockdown-sensor
```

nat rollback

以前に適用していた NAT の設定に、システムを戻します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。クラスタ化されたデバイス、またはスタック デバイスではこのコマンドは使用できません。

アクセス

設定（Configuration）

構文

```
system nat rollback
```

例

```
> system nat rollback
```

reboot

デバイスをリブートします。

アクセス

設定（Configuration）

構文

```
system reboot
```

例

```
> system reboot
```

restart

デバイス アプリケーションを再起動します。

アクセス

設定（Configuration）

構文

```
system restart
```

例

```
> system restart
```

shutdown

デバイスをシャット ダウンします。このコマンドは ASA FirePOWER モジュールでは使用できません。

アクセス

設定（Configuration）

構文

```
system shutdown
```

例

```
> system shutdown
```

セキュリティ、インターネット アクセス、および通信ポート

Defense Centerを保護するには、保護された内部ネットワークにそれをインストールしてください。Defense Centerは必要なサービスとポートだけを使用するよう設定されますが、ファイアウォール外部からの攻撃がそこまで（または管理対象デバイスまで）決して到達できないようにする必要があります。

Defense Centerとその管理対象デバイスが同じネットワーク上に存在する場合は、デバイス上の管理インターフェイスを、Defense Centerと同じ保護された内部ネットワークに接続できます。これにより、Defense Centerからデバイスを安全に制御することができます。また、他のネットワーク上のデバイスからのトラフィックをDefense Centerで管理および分離できるように、複数の管理インターフェイスを設定することもできます。

アプライアンスの展開方法とは無関係に、アプライアンス間通信は暗号化されます。それでも、分散型サービス拒否（DDoS）や中間者攻撃などの手段でFireSIGHT システム アプライアンス間の通信が中断、ブロック、または改ざんされないよう何らかの対策を講じる必要があります。

また、FireSIGHT システムの機能によってはインターネット接続が必要となることにも注意してください。デフォルトで、すべてのFireSIGHT システム アプライアンスはインターネットに直接接続するよう設定されます。加えて、システムで特定のポートを開いたままにしておく必要があります。その目的は基本的なアプライアンス間通信、セキュアなアプライアンス アクセス、および特定のシステム機能を正しく動作させるために必要なローカル/インターネット リソースへのアクセスを可能にすることです。

ヒント Blue Coat X-Series 向け Cisco NGIPS を除いて、FireSIGHT システム アプライアンスではプロキシ サーバを使用できます。詳細については、管理インターフェイスの構成（64-9 ページ）およびhttp-proxy（D-34 ページ）を参照してください。

詳細については、以下を参照してください。

インターネット アクセスの要件

デフォルトで、FireSIGHT システム アプライアンスはポート 443/tcp（HTTPS）および 80/tcp（HTTP）でインターネットに直接接続するよう設定されます。これらのポートは、すべての FireSIGHT システム アプライアンス上でデフォルトでオープンになっています（通信ポートの要件（E-3 ページ）を参照）。ほとんどのFireSIGHT システム アプライアンスではプロキシ サーバを使用できることに注意してください（管理インターフェイスの構成（64-9 ページ）を参照）。プロキシ サーバは whois アクセスに使用できない点にも注意が必要です。

運用継続性を確保するために、高可用性ペアの両方のDefense Centerがインターネットにアクセスできる必要があります。特定の機能では、プライマリDefense Centerがインターネットに接続した上で、同期プロセス中にセカンダリと情報を共有します。したがって、プライマリに障害が発生した場合は、ハイ アベイラビリティ ステータスのモニタリングおよび変更（4-16 ページ）の説明に従ってセカンダリをアクティブ ステータスにプロモートする必要があります。

次の表に、FireSIGHT システムの特定の機能におけるインターネット アクセス要件を示します。

表 E-1　FireSIGHT システム機能のインターネット アクセス要件

機能	インターネット アクセスの目的	アプライアンス	ハイ アベイラビリティの考慮事項
動的分析：照会	動的分析のために、送信済みファイルの脅威スコアをクラウドに照会します。	Defense Center	ペア化されたDefense Centerは、個別に脅威スコアをクラウドに照会します。
動的分析：送信	動的分析用にファイルをクラウドに送信します。	シリーズ 2 と X-Series を除く任意のデバイス	n/a
FireAMP 統合	シスコからエンドポイント ベースの（FireAMP）マルウェア イベントを受信します。	Defense Center	クラウド接続は同期されません。両方のDefense Centerで設定してください。
侵入ルール、VDB、および GeoDB の更新	侵入ルール、GeoDB、または VDB の更新をアプライアンスに直接ダウンロードするか、ダウンロードをスケジュールします。	Defense Center	侵入ルール、GeoDB、および VDB の更新は同期されます。
ネットワークベースの AMP	マルウェア クラウド検索を実行します。	Defense Center	ペア化されたDefense Centerは、個別にクラウド検索を実行します。
RSS フィード ダッシュボード ウィジェット	シスコを含む外部ソースから RSS フィード データをダウンロードします。	すべて（仮想デバイスと X-Series を除く）	フィード データは同期されません。
Security Intelligence フィルタリング	インテリジェンス フィードを含む、外部ソースからのセキュリティ インテリジェンス フィード データをダウンロードします。	Defense Center	プライマリDefense Centerがフィード データをダウンロードして、セカンダリと共有します。プライマリに障害が発生した場合は、セカンダリをアクティブに昇格させてください。
システム ソフトウェアの更新	システム更新をアプライアンスに直接ダウンロードするか、ダウンロードをスケジュールします。	すべて（仮想デバイスと X-Series を除く）	システム更新は同期されません。

表 E-1　FireSIGHT システム機能のインターネット アクセス要件（続き）

機能	インターネット アクセスの目的	アプライアンス	ハイ アベイラビリティの考慮事項
URL フィルタリング	アクセス コントロール用にクラウド ベースの URL カテゴリおよびレピュテーション データをダウンロードし、未分類 URL の検索を実行します。	Defense Center	プライマリ Defense Center は URL フィルタリング データをダウンロードして、セカンダリと共有します。プライマリに障害が発生した場合は、セカンダリをアクティブに昇格させてください。
whois	外部ホストの whois 情報を要求します。	すべて（仮想デバイスと X-Series を除く）	whois 情報を要求するアプライアンスは、インターネット アクセスを備えている必要があります。

通信ポートの要件

FireSIGHT システム アプライアンスは、（デフォルトでポート 8305/tcp を使用する）双方向 SSL 暗号化通信チャネルを使って通信します。基本的なアプライアンス間通信用にこのポートを開いたままにする**必要があります**。他のオープン ポートの役割は次のとおりです:

- アプライアンスの Web インターフェイスにアクセスする
- アプライアンスへのリモート接続を保護する
- 特定のシステム機能を正しく動作させるために必要なローカル/インターネット リソースへのアクセスを可能にする

一般に、機能関連のポートは、該当する機能を有効化または設定する時点まで、閉じたままになります。たとえば、Defense Center をユーザ エージェントに接続するまでは、エージェント通信ポート（3306/tcp）は閉じたままになります。別の例として、LOM を有効にするまでは、シリーズ 3 アプライアンス上のポート 623/udp が閉じたままになります。

注意　開いたポートを閉じると展開にどのような影響が及ぶか理解するまでは、開いたポートを**閉じないでください**。

たとえば、管理デバイス上のポート 25/tcp（SMTP）アウトバウンドを閉じた場合、個別の侵入イベントに関する電子メール通知をデバイスから送信できなくなります（『侵入ルールの外部アラートの設定（44-1 ページ）』を参照）。別の例として、ポート 443/tcp（HTTPS）を閉じることにより物理管理対象デバイスの Web インターフェイスへのアクセスを無効にできますが、それと同時に、動的分析のためにデバイスから疑わしいマルウェア ファイルをクラウドに送信できなくなります。

次のように、システムのいくつかの通信ポートを変更できることに注意してください。

- システムと認証サーバの間の接続を設定するときに、LDAP および RADIUS 認証用のカスタム ポートを指定できます（LDAP 認証サーバの指定（61-18 ページ）およびRADIUS 接続の設定（61-35 ページ）を参照）。
- 管理ポート（8305/tcp）を変更できます（管理インターフェイスの構成（64-9 ページ）を参照）。ただし、シスコ では、デフォルト設定を維持することを**強く**推奨しています。管理ポートを変更する場合は、相互に通信する必要のある展開内のすべてのアプライアンスでそれを変更する必要があります。

- ポート 32137/tcp を使用して、アップグレード対象のDefense Centerと シスコの通信を可能にすることができます。ただし、シスコでは、バージョン 5.3 以降の新規インストールのデフォルトであるポート 443 に切り替えることを推奨しています。詳細については、クラウド通信の有効化（64-30 ページ）を参照してください。

次の表は、FireSIGHT システムの機能を最大限に活用できるように、各アプライアンス タイプで必要なオープン ポートを示しています。

表 E-2　FireSIGHT システムの機能と運用のためのデフォルト通信ポート

ポート	説明	方向	開いているアプライアンス	目的
22/tcp	SSH/SSL	双方向	いずれか	アプライアンスへのセキュアなリモート接続を可能にします。
25/tcp	SMTP	発信	いずれか	アプライアンスから電子メール通知とアラートを送信します。
53/tcp	DNS	発信	いずれか	DNS を使用します。
67/udp 68/udp	DHCP	発信	すべて（X-Series を除く）	DHCP を使用します。 **注**　これらのポートはデフォルトで**閉じられています。**
80/tcp	HTTP	発信	すべて（仮想デバイスと X-Series を除く）	RSS フィード ダッシュボード ウィジェットからリモート Web サーバに接続できるようにします。
		双方向	Defense Center	HTTP 経由でカスタムおよびサードパーティのセキュリティ インテリジェンス フィードを更新します。 URL カテゴリおよびレピュテーション データをダウンロードします（さらにポート 443 も必要）。
161/udp	SNMP	双方向	すべて（X-Series を除く）	SNMP ポーリング経由でアプライアンスの MIB にアクセスできるようにします。
162/udp	SNMP	発信	いずれか	リモート トラップ サーバに SNMP アラートを送信します。
389/tcp 636/tcp	LDAP	発信	すべて（仮想デバイスと X-Series を除く）	外部認証用に LDAP サーバと通信します。
389/tcp 636/tcp	LDAP	発信	Defense Center	検出された LDAP ユーザに関するメタデータを取得します。
443/tcp	HTTPS	着信	すべて（仮想デバイスと X-Series を除く）	アプライアンスの Web インターフェイスにアクセスします。

表 E-2　FireSIGHT システムの機能と運用のためのデフォルト通信ポート（続き）

ポート	説明	方向	開いているアプライアンス	目的
443/tcp	HTTPS AMQP クラウド通信	双方向	Defense Center	次のものを取得します: • ソフトウェア、侵入ルール、VDB、および GeoDB の更新 • URL カテゴリおよびレピュテーション データ（さらにポート 80 も必要） • インテリジェンス フィードおよび他のセキュアなセキュリティ インテリジェンス フィード • エンドポイント ベースの（FireAMP）マルウェア イベント • ファイルに関してネットワーク トラフィックで検出されたマルウェアの性質 • 送信されたファイルに関する動的分析情報
			シリーズ 2 デバイスと シリーズ 3 デバイス	デバイスのローカル Web インターフェイスを使用してソフトウェア更新をダウンロードします。
			シリーズ 3 および仮想デバイス	動的分析のためにファイルを送信します。
514/udp	syslog	発信	いずれか	リモート syslog サーバにアラートを送信します。
623/udp	SOL/LOM	双方向	シリーズ 3	Serial Over LAN（SOL）接続を使用して Lights-Out Management を実行できるようにします。
1500/tcp 2000/tcp	データベース アクセス	着信	Defense Center	サードパーティ クライアントによるデータベースへの読み取り専用アクセスを可能にします。
1812/udp 1813/udp	RADIUS	双方向	すべて（仮想デバイスと X-Series を除く）	外部認証とアカウンティングのために RADIUS サーバと通信します。
3306/tcp	ユーザ エージェント	着信	Defense Center	ユーザ エージェントと通信します。
8302/tcp	eStreamer	双方向	すべて（仮想デバイスと X-Series を除く）	eStreamer クライアントと通信します。
8305/tcp	アプライアンス通信	双方向	いずれか	展開におけるアプライアンス間で安全に通信します。**必須です。**
8307/tcp	ホスト入力クライアント	双方向	Defense Center	ホスト入力クライアントと通信します。
32137/tcp	クラウド通信	双方向	Defense Center	アップグレード対象のDefense CenterとCollective Security Intelligence クラウド クラウドの通信を可能にします。

サードパーティ製品

FireSIGHT システム製品には、FireSIGHT システム製品と組み合わせて使用することを目的に配布されている、特定のサードパーティ製のオープン ソース コード製品が含まれます。これらの製品は無料であり、それぞれのライセンス契約書に記載されている一連の規定に基づいて「現状のまま」配布されています。次の表には、FireSIGHT システム製品と組み合わせて使用することを目的にシスコによって配布されている、主要なオープン ソース コード製品と、該当するライセンス契約書を記載しています。

表 F-1　　オープン ソース ソフトウェア ライセンス

オープン ソース ソフトウェア	ライセンス契約
Apache HTTPD Web サーバ 2.4.3	Apache License
Linux カーネル 2.6.32.24（シリーズ 2）	GNU 一般公的使用許諾バージョン 2（GPLv2）
Linux カーネル 2.6.35.14（シリーズ 3）	GNU 一般公的使用許諾バージョン 2（GPLv2）
Perl 5.10.1 および関連モジュール	Perl Artistic License
Snort 2.9.7	GNU 一般公的使用許諾バージョン 2（GPLv2）

FireSIGHT システム製品と共に配布されている、すべてのサードパーティ製オープン ソース コード製品の完全なリストと、すべての該当するライセンス契約書の全文は、製品のコマンド ラインにログインして次のファイルを表示すると取得できます。

```
/usr/share/license-files
```

FireSIGHT システム製品と組み合わせて使用されるサードパーティ製オープン ソース コード製品に対するソース コードが必要な場合は、サポート サイトに依頼を送信して入手できます。

VPN ライセンス

FireSIGHT システムのVPNの仮想ルータ間にセキュアな管理対象デバイストンネルを構築できるようにするライセンス。

7000 シリーズ

シリーズ 3 の管理対象デバイスグループ。このシリーズのデバイスには、70xx ファミリ（3D7010/7020/7030/7050 モデル）および 71xx ファミリ（3D7110/7120/3D7115/3D7125 および AMP7150 モデル）が含まれます。

8000 シリーズ

シリーズ 3 の管理対象デバイスグループ。このシリーズのデバイスには、81xx ファミリ（3D8120/8130/8140 および AMP8150 モデル）、82xx ファミリ（3D8250/8260/8270/8290 モデル）、83xx ファミリ（3D8350/8360/8370/8390 モデル）、および AMP83xx ファミリ（AMP8350/AMP8360/AMP8370/AMP8390 モデル）が含まれます。8000 シリーズ デバイスは、通常 7000 シリーズデバイスより高性能です。

access list

システム ポリシーにアクセス可能なホストを表す IP アドレスのリスト。アプライアンスで設定されます。デフォルトでは、だれでもポート 443（HTTPS）を使用してアプライアンスの Web インターフェイスに、またポート 22（SSH）を使用してコマンドラインにアクセスできます。さらに、ポート 161 を使用する SNMP アクセスも追加できます。

action

特定の基準を満たす（または満たさない）ネットワーク トラフィックを、システムが処理、検査、または記録する方法を決定する設定。アクションはポリシーのルールとして、特定のポリシーだけでなくさまざまなタイプのデフォルト アクションに関連付けられます。

ASA FirePOWER

Cisco ASA with FirePOWER Services の省略名。

Blue Coat X-Series 向け Cisco NGIPS

仮想デバイスのほとんどの機能を提供する、Blue Coat のスケーラブルなシャーシベースのシステム上に構築されたソフトウェアベースのアプリケーション。

CA

認証局を参照してください。

CAC 認証および許可

LDAP 認証によって提供されたクレデンシャルのみを使用してアプライアンスの Web インターフェイスにログインすることをユーザに許可する 共通アクセス カード（CAC）の種類。

category

アプリケーション カテゴリ、ファイル カテゴリ、またはURL カテゴリを参照してください。

Cisco ASA with FirePOWER Services

ASA FirePOWER モジュールがインストールされた Cisco Adaptive Security Appliance（ASA）管理対象デバイスのグループ。このシリーズのデバイスには、ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X、ASA5525-X、ASA5545-X、ASA5555-X、ASA5585-X-SSP-10、ASA5585-X-SSP-20、ASA5585-X-SSP-40、および ASA5585-X-SSP-60 モデルが含まれます。

CLI

コマンドライン インターフェイス（CLI）を参照してください。

Collective Security Intelligence クラウド

Defense Centerが最新の関連情報（マルウェア、セキュリティ インテリジェンス、および URL フィルタリング データなど）を取得できる、シスコがホストする外部サーバ。*クラウド サービス* または *シスコ クラウド* とも呼ばれます。「マルウェア クラウド ルックアップ」および「FireAMP プライベート クラウド」も参照してください。

Context Explorer

監視対象ネットワークに関する詳細でインタラクティブなグラフィカル情報を表示するページ。明確に区切られたセクションには、鮮明な線グラフ、棒グラフ、円グラフ、ドーナツ グラフの形式で情報が、詳細リストとともに表示されます。分析を調整するためにカスタム フィルタを容易に作成および適用できます。また、グラフ エリアをクリックするかまたはカーソルを置くと、データ セクションの詳細を確認できます。高度にカスタマイズ可能で、細分化され、リアルタイムで更新されるダッシュボードとは対照的に、Context Explorer は手動で更新され、より広範囲に及ぶデータのコンテキストを提供するように設計されています。また、ユーザが積極的に調査することができるようにレイアウトは 1 つの一貫した設計になっています。

Control ライセンス

ユーザ制御およびアプリケーション制御を実装できるようにするライセンス。スイッチングおよびルーティング（DHCP リレーと デバイス を含む）などのハードウェアベースのタスク、NAT、およびデバイス VPNを実行するように、サポートされている管理対象クラスタリングを設定することもできます。

CRL

証明書失効リスト（CRL）を参照してください。

eStreamer

イベント または管理対象Defense Centerから外部デバイスにクライアント アプリケーション データをストリーミングできるようにする FireSIGHT システムのコンポーネント。

failsafe

内部トラフィック バッファがいっぱいになった場合に、パケットが処理をバイパスして、そのインライン セットの終わりまで続行することを可能にするデバイスの特性。

file list

クリーン リスト およびカスタム検出リスト を参照してください。

FireAMP

シスコのエンタープライズクラスのエンドポイントをベースとした高度なマルウェア分析およびマルウェア対策ソリューション。マルウェアの発生、継続的な脅威、標的型攻撃を検出、認識、およびブロックします。組織に FireAMP サブスクリプションがある場合、個々のユーザがエンドポイント（コンピュータ、モバイル デバイス）にインストールした軽量のFireAMP コネクタが Collective Security Intelligence クラウドと通信します。これにより、マルウェアを瞬時に識別して検疫するだけでなく、マルウェアの発生を識別し、その伝搬経路を追跡し、その影響を把握して、正常にリカバリする方法を知ることができます。FireAMP ポータルを使用して、カスタム保護を作成したり、特定のアプリケーションの実行をブロックしたり、カスタム ホワイトリストを作成したりすることもできます。ネットワークベースの高度なマルウェア対策と比較してください。

FireAMP コネクタ

サブスクリプションベースのFireAMP 展開のユーザがコンピュータやモバイル デバイスなどのエンドポイントにインストールする軽量のエージェント。コネクタは、Collective Security Intelligence クラウドと通信し、情報を交換します。これにより、組織全体でマルウェアを識別し検疫できます。また、エンドポイントのホストで侵害の痕跡（IOC）も識別できます。

FireAMP サブスクリプション

組織がFireAMP（AMP）ソリューションとして 高度なマルウェア対策 を使用するために別個に購入するサブスクリプション。ネットワークベースの AMP を実行するために管理対象Malware ライセンスで有効にするデバイスと比較してください。

FireAMP プライベート クラウド

モニタ対象ネットワークと FireAMP ベース（ファイルおよびマルウェア）の機能の Collective Security Intelligence クラウドの間の安全なメディエータとして機能する FireAMP が提供する仮想マシン。クラウドへのすべての接続は、ネットワーク上の個々のエージェントやアプライアンスからではなく、プライベート クラウドの匿名化されたプロキシ接続上で発生します。

FireAMP ポータル

組織のサブスクリプションベースの FireAMP 展開を設定できる Web サイト（http://amp.sourcefire.com/）。

FireSIGHT 推奨ルール

侵入ポリシーの情報に基づいて、ネットワーク マップでどのルールを有効/無効にしたらよいかを推奨する機能。推奨に基づくルール状態の変更をシステムに許可することができます。この場合、システムは読み取り専用の FireSIGHT 推奨レイヤを追加します。

FireSIGHT 推奨レイヤ

組み込み レイヤ機能によって推奨される状態に侵入ポリシーを変更することをシステムに許可している場合に存在するルール状態のFireSIGHT 推奨ルール。

FireSIGHT ライセンス

Defense Center、ホスト、およびユーザ ディスカバリを実行するためのアプリケーションのデフォルト ライセンス。FireSIGHT ライセンスは、ホストとその管理対象Defense Centerを使用してモニタできるデバイスとユーザの数、およびアクセス制御ユーザを実行するためにアクセス制御ルールで使用できるユーザ制御の数を決定します。

GeoDB

位置情報データベース（GeoDB）を参照してください。

GID

ジェネレータ ID（GID）を参照してください。

HA リンク インターフェイス

ハイ アベイラビリティ リンク インターフェイスとも呼ばれ、デバイス間でヘルス情報を共有するため冗長通信チャネルとして機能する物理インターフェイスのクラスタ化されたペアの各メンバーに対して設定されるデバイス。

HTTP 応答ページ

ユーザの HTTP 要求がアクセス制御によってブロックされた場合に、システムに表示されるように設定できる Web ページ。シスコ提供の汎用応答ページを表示するか、カスタム HTML を提供できます。インタラクティブ ブロック ルールによって要求がブロックされる場合、ユーザが応答ページのボタンをクリックして、要求元のサイトに戻って続行できるようにすることができます。

ID の競合

現在のアクティブ ID および以前に報告されたパッシブ ID と競合する、新しいパッシブ オペレーティング システムまたはサーバの ID がシステムによって報告されると発生する競合。

LDAP 認証

ユーザ クレデンシャルを Lightweight Directory Access Protocol（LDAP）ディレクトリ サーバに保存されている LDAP ディレクトリと比較することによって、ユーザ クレデンシャルを確認する外部認証の形式。

Lights-Out Management（LOM）

アウトオブバンド Serial over LAN（SoL）管理接続を使用して、アプライアンスの Web インターフェイスにログインせずに、特定のシリーズ 3をリモートでモニタまたは管理できるアプライアンス の機能。シャーシのシリアル番号の表示や、ファンの速度や温度などの設定のモニタといった、限られたタスクを実行できます。

NAT

ネットワーク アドレス変換。プライベート ネットワーク上の複数のホストで単一のインターネット接続を共有するために最も一般的に使用される機能。ディスカバリを使用して、システムはネットワーク デバイスをロード バランサとして識別できます。また、FireSIGHT システムのレイヤ 3 展開では、NAT ポリシーを使用して NAT によるルーティングを設定できます。

NAT ポリシー

NAT ルールを使用してNATによるルーティングを実行するポリシー。

NAT ルール

ネットワーク トラフィックを評価し、条件に一致するトラフィックの変換方法を指定する一連の設定と条件。NAT ルールは、NAT ポリシー を使用してルーティングを実行するために既存のNATに追加されます。

NetFlow

Cisco IOS 対応機器で実行するためにシスコによって開発された、IP トラフィック情報を収集するための公開されている独自のネットワーク プロトコル。NetFlow 対応デバイスによって収集された情報は、FireSIGHT システムによって収集されたディスカバリ データと接続データを補足したり、管理対象デバイスがカバーしないネットワークをモニタしたりするために使用できます。

NetMod

管理対象デバイスのシャーシにインストールするモジュール。これには、そのデバイスのセンシング インターフェイスが含まれます。

Nmap

Network Mapper。ホストで実行しているオペレーティング システムとアプリケーション プロトコルを検出するために使用できるオープン ソースのアクティブ スキャナ。Nmap スキャンを実行すると、検出された情報がネットワーク マップに追加されます。

PKI

公開キー インフラストラクチャ（PKI）を参照してください。

PKI オブジェクト

オブジェクトおよびペアの公開キー証明書を表す再利用可能な秘密キー。

Protectionライセンス

侵入検知と防御、ファイル制御、およびセキュリティ インテリジェンス フィルタリングを実行できるライセンス。ライセンスがなくても、シリーズ 2 のデバイスでは、セキュリティ インテリジェンス以外のProtection機能を自動的に使用できます。

RADIUS 認証

Remote Authentication Dial In User Service。ネットワーク リソースへのユーザ アクセスを認証、許可、および説明するために使用されるサービス。外部認証オブジェクトを作成して、FireSIGHT システム ユーザが RADIUS サーバを介して認証できるようにすることができます。

RSA 暗号化

大きな数字の 2 つの素数への分解に基づく暗号化方式。楕円曲線（EC）暗号とは対照的な暗号です。

SFP モジュール

71xx ファミリ デバイスのネットワーク モジュールに挿入された Small Form-Factor Pluggable トランシーバ。SFP モジュールのセンシング インターフェイスは、設定可能なバイパスを許可しません。

SHA-256 ハッシュ値

マルウェア クラウド ルックアップを実行するファイルを表す 32 ビット文字列。SHA256 と略記されることもあります。ハッシュ値は、暗号ハッシュ関数を使用して計算されます。複数のファイルの SHA-256 値が同じであれば、コンテンツが同じである可能性が非常に高くなります。

SID

シグニチャ ID（Sid）を参照してください。

Snort

IP ネットワークでのリアルタイム トラフィック分析およびパケット ロギングを実行するオープン ソースの侵入検知システム。Snort は、プロトコル分析、コンテンツ検索、およびコンテンツ マッチングを実行できます。また、さまざまな攻撃やプローブを検出できます。Snort では、柔軟なルールの言語を使用して、収集または通過させるべきネットワーク トラフィックを示します。FireSIGHT システムは、Snot を使用して、デコーダ、プリプロセッサ、および侵入ルールに照らしてパケットをテストします。

Spero 分析

マルウェア分析のために、Collective Security Intelligence クラウドにファイル構造特性を送信する方法。結果は動的分析を補足します。

SSL

セキュア ソケット レイヤ（SSL）を参照してください。

SSL インスペクション

ネットワークを通過する暗号化されたトラフィックを検査し、復号化し、ログに記録することができる機能。復号化しないように選択したトラフィックと復号化されたトラフィックの両方を、アクセス制御でさらに検査できます。

SSL ポリシー

親アクセス制御ポリシーの一部として適用するポリシー、および SSL インスペクション デバイスでモニタする暗号化されたトラフィックに対してポリシー ターゲットを実行するポリシー。SSL ポリシーには、複数の SSL ルールを含めることができます。また、これらのルールの基準を満たさないトラフィックの処理とロギングを決定するデフォルト アクションも指定します。SSL ポリシーでは、CA の公開キー証明書に基づき、復号化できないトラフィックの処理方法、および信頼できる暗号化トラフィックを指定することもできます。

SSL ルール

システムが暗号化されたトラフィックを調査するために使用し、SSL インスペクションの実行を可能にする一連の条件。SSL ルールに組み込まれる SSL ポリシーは、簡単な IP アドレスのマッチングを実行したり、異なるユーザ、アプリケーション、ポート、URL、および暗号化されたセッション特性が関係する複雑な接続の特性を示したりすることがあります。SSL ルール アクションは、ルールの条件を満たすトラフィックをシステムがどのように処理するかを決定します。その他のルール設定によって、接続をログに記録する方法（および記録するかどうか）が決定されます。

SSL ルール アクション

システムがSSL ルールの条件を満たす暗号化されたネットワーク トラフィックをどのように処理するかを決定する設定。一致したトラフィックをブロックできます(接続の再設定はすることもしないこともできます)。また、暗号化されたトラフィックを復号化せず、アップロードされた秘密キーを使用して着信トラフィックを復号化したり、再署名された公開キー証明書を使用して発信トラフィックを復号化したり、追加の SSL ルールを使用してトラフィックのモニタを続行したりすることもできます。

SVID

脆弱性 IDを参照してください。

switch

マルチポート ブリッジとして機能するネットワーク デバイス。ネットワーク検出を使用することで、システムはスイッチをブリッジとして識別します。また、管理対象デバイスを、2 つ以上のネットワークの間でパケット スイッチングを実行する仮想スイッチとして設定できます。

TLS

Transport Layer Securityを参照してください。

Transport Layer Security

セキュア ソケット レイヤ(SSL) プロトコルの後を継ぐ暗号アプリケーション層プロトコル。SSL インスペクション機能を使用することにより、TLS プロトコルで暗号化されたトラフィックを復号化できます。

URL オブジェクト

個々の URL を表す再利用可能なオブジェクト。

URL カテゴリ

マルウェアやソーシャル ネットワーキングなど、URL の一般的な分類。

URL フィルタリング

モニタ対象ホストによって要求された URL に基づいて、ネットワークを通過できるトラフィックを決定するアクセス制御ルールを作成できる機能。URL カテゴリによって URL レピュテーションから取得される、それらの URL のCollective Security Intelligence クラウドおよび Defense Centerの情報に相関します。許可するまたはブロックする個々の URL または URL グループを指定することによって、Web トラフィックに関するよりきめの細かいカスタム コントロールを実現することもできます。

URL Filtering ライセンス

URL フィルタリングおよびURL カテゴリの情報に基づいて URL レピュテーションを実行することができるライセンス。URL Filtering ライセンスは期限切れになる可能性があります。

URL レピュテーション

組織のセキュリティ ポリシーに反する目的のために Web サイトが使用される可能性を表します。Collective Security Intelligence クラウドによって判定されます。

user

管理対象デバイスまたはユーザ エージェントによってネットワーク アクティビティが検出されたユーザ。

UTC 時間

協定世界時。グリニッジ標準時(GMT)とも呼ばれる、UTC は世界中のあらゆる場所で認識されている標準時間です。タイム ゾーン機能を使用して現地時間を設定することができますが、FireSIGHT システムは UTC を使用します。

VDB

脆弱性データベースを参照してください。

VLAN

仮想ローカル エリア ネットワーク(VLAN)を参照してください。

VLAN タグ オブジェクト

個々の オブジェクト タグを表す再利用可能な仮想ローカル エリア ネットワーク(VLAN)。

VPN

FireSIGHT システムの管理対象VPNの仮想ルータ間にセキュアな デバイス トンネルを構築できる機能。

VRT

シスコ VRTを参照してください。

VRT 分析レポート

シスコ VRTのために送信されたキャプチャされたファイルの 動的分析 分析のレコード。動的分析サマリ レポートで提供される情報および動的分析中に検出された追加の情報の詳細を示します。

Web アプリケーション

HTTP トラフィックの内容または要求された URL を表示する、アプリケーションの 1 つの種類。

X-Series

Blue Coat X-Series 向け Cisco NGIPS の省略名。

アクセス コントロール ルール アクション

システムがアクセス制御ルールの条件を満たすネットワーク トラフィックをどのように処理するかを決定する設定。該当トラフィックを*ブロック*することができます(接続の再設定はしてもしなくても構いません)。HTTP トラフィックでは、ブロックをバイパスするオプションを提供できます。また、トラフィックを*信頼*して、それ以上検査せずに通過させることも、該当トラフィック(必要に応じて侵入ポリシーとファイル ポリシーを使用して検査することが可能)を*許可*することも、または追加のアクセス コントロール ルールを使用してトラフィックを*モニタ*し続けることもできます。

アクセス制御

ネットワークを通過するトラフィックの指定、検査、記録を可能にする FireSIGHT システムの機能。アクセス制御は、セキュリティ インテリジェンス、SSL インスペクション、プリプロセッサ オプション、侵入検知と防御、ファイル制御、高度なマルウェア対策を呼び出します。また、ディスカバリで検査できるトラフィックを決定します。

アクセス制御ポリシー

管理対象ポリシーがモニタするネットワーク トラフィックに対して適用を実施するために、それらのデバイスにデバイスするアクセス制御。アクセス コントロール ポリシーには、複数のアクセス制御ルールが含まれる場合があります。これらのルールの基準を満たさないトラフィックの処理とロギングは、同じくアクセス コントロール ポリシーによって指定されるデフォルト アクションによって決定されます。アクセス コントロール ポリシーのその他の設定は、セキュリティ インテリジェンス、SSL インスペクション、パフォーマンス オプション、プリプロセッサ オプションなどの詳細設定を制御します。

アクセス制御ユーザ

アクセス制御によってネットワークの使用を制御されるユーザ。Microsoft Active Directory サーバとDefense Centerの間の接続を設定する場合は、アクセス制御ユーザが所属する必要のある LDAP グループを指定します。ユーザ エージェントがアクセス制御ユーザによるログインをレポートする場合、それらのユーザは IP アドレスと関連付けられます。これにより、ユーザ条件が指定されたアクセス制御ルールのトリガーが可能になります。非アクセス制御ユーザと比較

アクセス制御ルール

FireSIGHT システムが監視対象のネットワーク トラフィックを検査し、きめ細かなアクセス制御を実現するために使用する一連の条件。アクセス制御ポリシーに組み込まれるアクセス コントロール ルールで、簡単な IP アドレスのマッチングを実行したり、さまざまな基準が関係する複雑な接続の特性を示したりすることができます。アクセス コントロール ルール アクションは、ルールの条件を満たすトラフィックをシステムがどのように処理するかを決定します。その他のルール設定により、接続をログに記録する方法(およびログに記録するかどうか)と、ルールによって許可されたトラフィックを侵入ポリシーまたはファイル ポリシーのどちらで検査するかが決定します。

アクティブ検出

アクティブ ソースを使用したホスト、アプリケーション、およびuser情報の検出。アクティブ ソースには、Nmap のようなスキャナ、システムの Web インターフェイスへのユーザ入力、またはコマンドラインやサードパーティのアプリケーション API コールを使用したホスト入力へのネットワーク マップが含まれます。パッシブ検出と比較

アプライアンス

FireSIGHT システム、Defense Center、管理対象デバイス、Cisco ASA with FirePOWER Services、または Blue Coat X-Series 向け Cisco NGIPS。物理アプライアンスとソフトウェアベースのアプライアンスがあります。

アプライアンス統計情報

稼働時間、システム メモリの使用率、負荷平均、ディスク使用率、システム プロセスのサマリなど、アプライアンスに関する取得可能な情報。また、Defense Centerでは データ コリレータプロセスに関する情報。

アプリケーション

検出されたネットワーク資産、通信方法、または HTTP コンテンツ。システムは 3 種類のアプリケーション(アプリケーション プロトコル、クライアント アプリケーション、Web アプリケーション)を検出します。

アプリケーション カテゴリ

アプリケーションの最も本質的な機能を示す一般分類。各アプリケーションは、少なくとも 1 つのカテゴリに属します。

アプリケーション タイプ

アプリケーションが、アプリケーション プロトコル、クライアント アプリケーション、Web アプリケーションのいずれであるか。

アプリケーション タグ

アプリケーションでは説明されない、アプリケーション カテゴリに関する情報。たとえば、ビデオ ストリーミングの Web アプリケーションには、「高帯域幅」および「ディスプレイ広告」というタグが付けられることがよくありますアプリケーションには任意の数のタグを付けることができます(タグなしも可能)。

アプリケーション ディテクタ

ネットワーク上のアプリケーションを識別するためにシステムが使用するツール。アプリケーション ディテクタは、パケット 見出し内の ASCII または 16 進数のパターンか、トラフィックが使用するポート、あるいはその両方を使用して、アプリケーションを識別します。シスコでは、システムのアップデート、脆弱性データベースのアップデート、またはインポート/エクスポート機能を介して追加のディテクタを提供することがあります。独自のアプリケーション プロトコル ディテクタを作成することもできます。

アプリケーション フィルタ

アプリケーション アプリケーション、リスク、種類、カテゴリ、およびタグに関連した基準に従ってグループ化された 1 つ以上のビジネスとの関連性。アプリケーション フィルタはオブジェクト マネージャで作成します。

アプリケーション プロトコル

サーバとホスト上のアプリケーション アプリケーションの間の通信中に検出されるアプリケーション プロトコル トラフィックを表すクライアントの種類(たとえば、SSH や HTTP)。

アプリケーション リスク

アプリケーションの使用方法が組織のセキュリティ ポリシーに違反している可能性。アプリケーションのリスクは、Very Low から Very High までの範囲です。

アプリケーション制御

ネットワークを通過可能なアクセス制御 トラフィックを指定することのできる、アプリケーションの一環を成す機能。

アプリケーションのビジネスとの関連性

ビジネスとの関連性を参照してください。

アラート

システムが特定のイベントを生成したことを示す通知。侵入イベント（影響を含む）、ディスカバリ イベント、ネットワークベースのマルウェア イベント、相関ポリシー違反、ヘルス ステータスの変更、および記録された接続に基づいて警告できます。通常は電子メール、Syslog、または SNMP トラップで警告できます。

アラート応答

システムが電子メール、Syslog、または SNMP トラップでアラートを送信することを許可する一連の設定。単一のアラート応答を使用して複数のタイプのイベントについてのアラートを受けることができます。

暗号スイート リスト

トラフィックの暗号化に使用される複数の暗号スイートを表す再利用可能なオブジェクト。

位置情報

監視対象ネットワークのトラフィックで検出されたルーティング可能な IP アドレスの位置情報ソースに関するデータ（接続タイプ、インターネット サービス プロバイダなど）を提供する機能。イベントおよびホスト プロファイルで位置情報を表示し、アクセス制御ポリシーまたは SSL ポリシーのトラフィック フィルタリングに使用できます。

位置情報データベース（GeoDB）

ルーティング可能な IP アドレスに関連付けられた既知の位置情報データを格納し、定期的に更新されるデータベース。

イベント

イベント ビューアを使用して、ワークフローで表示できる特定のオカレンスに関する詳細の集合。イベントは、ネットワークに対する攻撃、検出されたネットワーク資産の変更、組織のセキュリティおよびネットワーク使用ポリシーの違反などを表します。システムは、アプライアンスのヘルス ステータスの変更、Web インターフェイスの使用状況、ルール更新、および起動された修復に関する情報を含むイベントも生成します。また、「イベント」が特定のオカレンスを表していない場合でも、システムはイベントとして他の特定の情報を表示します。たとえば、イベント ビューアを使用して、検出されたホスト、アプリケーション、およびそれらの脆弱性に関する詳細情報を表示することができます。

イベント ストリーマ

eStreamerを参照してください。

イベント トラフィック チャネル

トラフィック チャネルを参照してください。

イベント ビューア

イベントの表示および操作を可能にするシステムのコンポーネント。イベント ビューアは、ワークフローを使用して、広範なイベント ビューや、目的のイベントだけを含む絞り込まれたイベント ビューを表示します。イベント ビューのイベントを制約するには、ワークフローをドリル ダウンするか、検索を使用します。

イベントしきい値

指定した時間内にイベントが生成される回数に基づいて、システムがログを記録したり、侵入イベントを表示したりする回数を制限する機能。同一のイベントが大量に発生して悩まされている場合には、イベントしきい値を使用します。

イベント抑制

特定の IP アドレスまたは IP アドレスの範囲によって侵入イベントがトリガーとして使用された場合に、抑制侵入ルールを使用できるようにする機能。イベント抑制は、誤検出を低減するのに役立ちます。たとえば、特定のエクスプロイトのように見えるパケットを送信する電子メールサーバがある場合、そのサーバによってトリガーとして使用されるルールのイベントを抑止することにより、本物の攻撃に対するイベントのみが表示されるようにすることができます。

インシデント

予想される侵入イベントの違反に関与している疑いのある 1 つ以上のセキュリティ ポリシー。システムには、インシデントの調査に関連した情報の収集および処理に使用できるインシデント処理機能が備えられています。

インタラクティブ ブロック

ユーザが アクセス コントロール ルール アクションのボタンをクリックして、最初にブロックされた Web サイトを続行できるようにするHTTP 応答ページ。

インテリジェンス フィード

シスコ VRT によりレピュテーションが低いと判定される IP アドレスのリストの集合。リストは定期的に更新されます。インテリジェンス フィードの各リストは特定のカテゴリ（オープン リレー、既知の攻撃者、偽の IP アドレス（bogon）など）を表しています。アクセス制御ポリシーでは、ブラックリストを使用して、すべてまたはいずれかのカテゴリをセキュリティ インテリジェンスに登録できます。インテリジェンス フィードは定期的に更新されるため、インテリジェンス フィードを使用することで、システムがネットワーク トラフィックのフィルタリングに最新の情報を使用することが保証されます。

インポート

アプライアンスからアプライアンスにさまざまな設定を転送するために使用できる方法。同じ種類の別のアプライアンスから以前にエクスポート された設定をインポートできます。

インライン インターフェイス

センシング インターフェイスでトラフィックを処理するように設定されたインライン展開。インライン インターフェイスをインライン セットにペアで追加する必要があります。

インライン セット

インライン インターフェイスの 1 つ以上のペア。

インライン展開

管理対象デバイスがネットワーク上にインラインで配置される FireSIGHT システムの展開。この設定では、デバイスがネットワーク トラフィック フローに影響を与える可能性があります。トラフィック フローに影響を与えずに分析および応答できるパッシブ検出とは異なります。

ウィジェット

ダッシュボード ウィジェットを参照してください。

影響

侵入イベントに関する、侵入データ、ディスカバリ データ、および脆弱性の間の相関関係を示す番号付きインジケータ。たとえば、影響レベル 1（赤色の影響アイコン）は、ターゲット ホストが、侵入イベントによって表される攻撃に対して*脆弱*であることを意味します。影響レベル 2（オレンジ色の影響アイコン）は、*潜在的に脆弱*であることを意味します。ネットワーク検出ポリシーによってモニタされていないネットワーク上のホストに向けられた攻撃は、影響レベル 0（灰色の影響アイコン）になります。これは、Defense Centerがイベントの影響を判別できないことを示しています。

エクスポート

アプライアンスからアプライアンスへのさまざまな設定（ポリシーなど）を転送するために使用できる方法。1 つのアプライアンスから設定をエクスポートしたら、同じタイプの別のアプライアンスにその設定をインポートできます。

エンドポイント

組織のFireAMP コネクタ戦略の一部として 高度なマルウェア対策 をインストールするコンピュータまたはモバイル デバイス。

応答

相関ポリシー違反に対する反応（アラート または修復）。

オブジェクト

名前を値（IP アドレスまたは URL など）に関連付ける再利用可能な設定。Web インターフェイスでその値を使用するときは、その名前のオブジェクトを代わりに使用できます。オブジェクト マネージャを使用してオブジェクトを作成します。ネットワーク オブジェクト、セキュリティ インテリジェンス オブジェクト、ポート オブジェクト、VLAN タグ オブジェクト、URL オブジェクト、アプリケーション フィルタ、変数セット、file list、HA リンク インターフェイス、セキュリティ ゾーン、暗号スイート リスト、識別名オブジェクト、および PKI オブジェクトも参照してください。

オブジェクト マネージャ

オブジェクトおよびオブジェクト グループを管理する Web インターフェイスのページ。

オペレーティング システム ID

オペレーティング システム ベンダーと、ホスト上のオペレーティング システムのバージョンの詳細。

外部認証

ユーザが FireSIGHT システム LDAP 認証にログインする際、外部に保存されたユーザ クレデンシャルを使用してユーザ名とパスワードを認証する方法（RADIUS 認証や アプライアンスなど）。内部認証と比較してください。

カスタム テーブル

FireSIGHT システムによって提供される事前定義された 2 つ以上のテーブルからのフィールドを組み合わせた、ユーザが構築できるテーブル。たとえば、新しいコンテキストで接続データを調べるために、ホストの重要度テーブルのホスト属性情報と**接続**データ テーブルの情報を組み合わせることができます。

カスタム トポロジー

ホスト、モバイル デバイス、およびネットワーク デバイス ネットワーク マップのサブネットを意味ある仕方で編成および識別することを可能にする機能。

カスタム フィンガープリント

フィンガープリントを参照してください。

カスタム ユーザ ロール

特殊なアクセス権限を持つユーザ ロール。カスタム ユーザ ロールには一連のメニューベースのアクセス許可およびシステム アクセス許可を含めることができます。またカスタム ユーザ ロールは完全に独自に作成することも、事前定義ユーザ ロールを基にすることもできます。

カスタム ワークフロー

組織の固有のニーズを満たすために作成するワークフロー。

カスタム検出リスト

SHA-256 ハッシュ値で表されたファイルのリスト。システムはこのリストにあるファイルを検出した場合、マルウェア クラウド ルックアップでのそのファイルの処理が [Clean] であっても、そのファイルをマルウェアと見なしてCollective Security Intelligence クラウドを実行しません。

仮想スイッチ

ネットワークを通過するインバウンドおよびアウトバウンドのトラフィックを処理するスイッチド インターフェイスのグループ。レイヤ 2 展開では、論理セグメントにネットワークを分割しながら、スタンドアロン ブロードキャスト ドメインとして機能するように管理対象デバイスで仮想スイッチを設定できます。仮想switchは、ホストからの Media Access Control（MAC）アドレスを使用して、パケットの送信先を決定します。

仮想デバイス

仮想ホスティング環境の独自の機器に配置できる管理対象デバイス。仮想デバイスは、ハイ アベイラビリティ、クラスタリング、スタッキング、NAT、VPN、高速パス ルールなどのハードウェア ベースの機能をサポートしません。また、仮想デバイスを仮想スイッチまたは仮想ルータとして設定することはできません。

仮想Defense Center

仮想ホスティング環境の独自の機器に配置できるDefense Center。

仮想ルータ

レイヤ 3 トラフィックをルーティングするルーテッド インターフェイスのグループ。レイヤ 3 展開では、仮想ルータを設定し、宛先 IP アドレスに従ってパケット転送を決定することによって、パケットをルーティングできます。スタティック ルートを定義し、Routing Information Protocol（RIP）および Open Shortest Path First（OSPF）のダイナミック ルーティング プロトコルを設定して、ネットワーク アドレス変換（NAT）を実装できます。

仮想ローカル エリア ネットワーク（VLAN）

VLAN は、地理的な場所ではなく、その他の基準（部門や主な使用方法など）に従ってホストをマッピングします。モニタ対象ホストのホスト プロファイルには、そのホストに関連付けられた VLAN 情報が示されます。最も内側の VLAN タグの情報もさまざまなイベントに含まれます。システムでは、接続の VLAN タグに基づいて、アクセス制御を含む複数のタイプのトラフィック処理を実行できます。レイヤ 2 およびレイヤ 3 の展開では、VLAN タグが付けられたトラフィックを適切に処理するように、管理対象仮想スイッチで仮想ルータおよびデバイスを設定できます。

監査イベント

FireSIGHT システムの特定のユーザ インタラクションを示すイベント。各監査イベントには、タイム スタンプ、イベントを生成したアクションを実行したユーザのユーザ名、送信元 IP アドレス、イベントを説明するテキストが含まれます。監査イベントは、監査ログに記録されます。

監査ログ

システムとのユーザ インタラクションの記録。監査ログは、監査イベントで構成されます。

管理インターフェイス

FireSIGHT システムのアプライアンスを管理するために使用するネットワーク インターフェイス。ほとんどの展開では、管理インターフェイスは、内部保護されたネットワークに接続されます。センシング インターフェイスと比較仮想Defense Centerおよびすべてのシリーズ 3 アプライアンスで、パフォーマンスを向上させるためにトラフィックをチャネルに分割するか、Defense Centerが異なるネットワークにトラフィックを分離できるように追加ネットワークへのルートを作成するよう、複数の管理インターフェイスを設定できます。また、別個のネットワークにトラフィック チャネルをルーティングして、スループット容量を増やすこともできます。

管理対象デバイス

デバイスを参照してください。

管理トラフィック チャネル

トラフィック チャネルを参照してください。

基本ポリシー

カスタム ポリシーの侵入ポリシーとして機能するネットワーク分析ポリシーまたは基本ポリシー レイヤ。

基本ポリシー レイヤ

組み込み レイヤまたは侵入ポリシーの最下層であるネットワーク分析ポリシー。基本ポリシーによって基本ポリシー レイヤの設定が決まるため、ポリシーのデフォルト設定となります。

キャプチャされたファイル

ネットワーク トラフィックで検出され、Collective Security Intelligence クラウドまたは 動的分析用に Spero 分析へ送信するため、あるいはデバイスへのファイル ストレージのためにデバイスによってコピーされるファイル。

脅威スコア

ファイルをCollective Security Intelligence クラウドのために、動的分析に送信した結果としてファイルに割り当てられ、ファイルにマルウェアが含まれる可能性の尺度となる 1 ～ 100 の評価。

共通アクセス カード（CAC）

CAC 認証および許可に使用される米国国防総省発行の ID カード。

共有オブジェクトのルール

C ソース コードからコンパイルされたバイナリ モジュールとして提供される侵入ルール。共有オブジェクトのルールを使用すると、標準テキスト ルールでは検出できない方法で、攻撃を検出できます。共有オブジェクトのルールのルール キーワードおよび引数は変更できません。できるのは、ルールで使用される変数を変更したり、送信元と宛先のポートや IP アドレスなどの側面を変更したり、カスタム共有オブジェクトのルールとしてルールの新規インスタンスを保存したりすることに限られます共有オブジェクト ルールのジェネレータ ID（GID）は 3 です。

共有レイヤ

その他のポリシーによる使用が許可された侵入ポリシーまたはネットワーク分析ポリシーのレイヤ。共有レイヤを使用するポリシーは、共有レイヤでの変更がコミットされたときに更新されます。共有レイヤは、その共有を許可するポリシーでのみ変更できます。共有レイヤを使用するポリシーでは共有レイヤは読み取り専用になります。

組み込み レイヤ

レイヤまたは侵入ポリシーの読み取り専用ネットワーク分析ポリシー。これらのポリシーには、常に組み込み基本ポリシー レイヤが含まれます。侵入ポリシーには組み込み FireSIGHT 推奨レイヤを含めることもできます。

クライアント

クライアント アプリケーションとも呼ばれる、アプリケーションで実行され、一部の操作を別のホスト（ホスト）に頼って実行するサーバ。たとえば、電子メール クライアントは、電子メールの送受信を実行できます。あるホスト上のユーザが別のホストにアクセスするために特定のクライアントを使用していることをシステムが検出すると、クライアントの名前とバージョン（該当する場合）などを含めてその情報をホスト プロファイルとネットワーク マップでレポートします。

クライアント アプリケーション

クライアントを参照してください。

クラウド サービス

Collective Security Intelligence クラウドを参照してください。

クラスタリング

2 つのピア シリーズ 3 デバイス間またはピア スタック間でネットワーキング機能と設定データの冗長性を実現する機能。クラスタリングによって、ポリシー適用、システム更新、および登録のための単一の論理システムが作成されます。冗長ハイ アベイラビリティの設定を可能にする Defense Center と比較してください。

クリーン リスト

SHA-256 ハッシュ値で表されたファイルのリスト。システムはこのリストにあるファイルを検出した場合、マルウェア クラウド ルックアップでのそのファイルの処理が [Malware] であっても、そのファイルをクリーンとして見なして Collective Security Intelligence クラウドを実行しません。

クリップボード

後から侵入イベントに追加できるインシデントを最大 25,000 個までコピーできる保持領域。

グローバル ブラックリスト

すべてのセキュリティ インテリジェンス オブジェクトのアクセス制御ポリシーにデフォルトで含められるセキュリティ インテリジェンス ブラックリスト。グローバル ブラックリストはすべてのセキュリティ ゾーンに適用されます。コンテキスト メニュー、ダッシュボード、および多くの Context Explorer ページで、IP アドレスのイベント ビューアを使用して個々の IP アドレスをグローバル ブラックリストに追加できます。

グローバル ホワイトリスト

すべてのセキュリティ インテリジェンス オブジェクトのアクセス制御ポリシーにデフォルトで含められるセキュリティ インテリジェンス ホワイトリスト。グローバル ホワイトリストはすべてのセキュリティ ゾーンに適用されます。コンテキスト メニュー、ダッシュボード、および多くの Context Explorer ページで、IP アドレスのイベント ビューアを使用して個々の IP アドレスをグローバル ホワイトリストに追加できます。

現在の ID

特定のネットワーク資産に対して、システムが最も正しいと見なすオペレーティング システムまたはサーバの ID。システムは多くの方法でこのデータを使用します。たとえば、統計の計算、脆弱性情報の割り当て、攻撃の影響の評価、および相関ルールの評価のために使用します。

現在のユーザ

システムがホストと関連付けるユーザ。ユーザがアクセス制御ユーザである場合、システムはそのホストとの間のトラフィックに対してユーザ制御を実行できます。ホストに関連付けられたアクセス制御ユーザがいない場合は、非アクセス制御ユーザがホストの現在のユーザとなることができます。ただし、アクセス制御ユーザがホストにログインした後は、別のアクセス制御ユーザがログインした場合のみ、現在のユーザが変更されます。

公開キー

すべてのユーザが使用できる公開キー証明書に連付けられた暗号キー。公開キーおよびペアにされた秘密キーは、セキュア ソケット レイヤ（SSL）と Transport Layer Security の暗号化および復号化に使用されます。

公開キー インフラストラクチャ（PKI）

認証局が公開キー証明書およびペアにされた秘密キーを個々のユーザに対して発行する方法を管理するシステム。

公開キー証明書

証明書に保存された認証局がそのユーザに属していることを裏付ける、公開キーによって個々のユーザに対して発行されるデジタル文書。

高速パス ルール

分析する必要のないトラフィックが処理をバイパスできるようにするために、限定された基準セットを使用して、ルールのハードウェア レベルで設定するデバイス。

高度なマルウェア対策

略語は AMP。FireSIGHT システムのネットワークベースのマルウェア検出およびマルウェア ブロッキング機能です。FireAMPが必要なシスコのエンドポイントベースの AMP ツールである FireAMP サブスクリプション とこの機能を比較してください。

コマンドライン インターフェイス（CLI）

シリーズ 3 および仮想デバイスの制限付きテキストベース インターフェイス。CLI ユーザが実行できるコマンドは、ユーザに割り当てられているアクセス レベルによって異なります。

コンテキスト メニュー

FireSIGHT システムの他の機能にアクセスするためにショートカットとして使用できる、Web インターフェイスの多くのページで使用可能なポップアップ メニュー。メニューの内容は、表示しているページ、調べている特定のデータ、ユーザ ロールなどの複数の要因によって異なります。

コンプライアンス ホワイトリスト

相関ルールと同様、ネットワーク トラフィックが相関ポリシーに違反していると見なされる場合に満しているべき基準を指定する方法の 1 つ。どのオペレーティング システム、Defense Center、およびプロトコルが特定のサブネットのアプリケーション上で実行できるかを指定するコンプライアンス ホワイトリストは、ホストを使用して設定できます。ホワイトリストに違反した場合に、アラートや修復のような応答を起動するようにDefense Centerを設定することもできます。コンプライアンス ホワイトリストは他のタイプのホワイトリストとは関連付けられないことに注意してください。

コンプライアンス ホワイトリスト イベント

ホワイトリスト イベントを参照してください。

コンプライアンス ホワイトリスト違反

ホワイトリスト違反を参照してください。

サードパーティの脆弱性

サードパーティから取得された脆弱性データ。組織でスクリプトを作成するか、またはコマンドライン インポート ファイルを作成して、サードパーティ インポートからネットワーク マップ データをアプリケーションできる場合、システムの脆弱性データを補強するために、ホスト入力機能を使用してサードパーティの脆弱性データをインポートすることができます。

サーバ

アプリケーション トラフィックで識別されるクライアント アプリケーション上にインストールされたサーバ ホスト（アプリケーション プロトコルと比較してください）。

サーバ ID

アプリケーション プロトコル上のサーバのホストの種類、ベンダー、バージョンの詳細。

サーバ バナー

サーバを識別するうえで役立つ追加情報を提供するサーバに関して検出された最初のパケットの最初の 256 バイト。システムは、初めてサーバが検出されたときに、一度だけサーバ バナーを収集します。

サーバ証明書

認証局によって発行される暗号化された証明書。サーバ ID の変更できない証明書を提供します。任意の認証局に証明書を要求し、そのカスタム証明書をアプライアンスにアップロードできます。

最適化ポリシー

IP 最適化プリプロセッサ（ネットワーク分析ポリシーで設定）が、ターゲット ホストのオペレーティング システムに基づいて、フラグメント化された IP パケットを再構成する方法を示すサブポリシー。適応型プロファイルは適応型最適化ポリシーを使用することに注意してください。

サブサーバ

同じホスト上の別のサーバによって呼び出されるサーバ。

ジェネレータ ID（GID）

システムのどのコンポーネントが侵入イベントを生成したかを示す番号。GID は、ルールの シグニチャ ID（Sid）が、ルールをトリガーとして使用するパケットのコンテキストを提供するのと同じ方法でイベントの種類を分類することによって、より効率的にイベントを分析するのに役立ちます。

時間枠

任意のイベント ビューにおけるイベントの時間的制約。それぞれのイベント ビューには、ユーザ設定に応じた異なるデフォルトの時間枠がある場合があります。すべてのイベント ビューが時間で制約されるわけではないことに注意してください。

しきい値

イベントしきい値を参照してください。

識別名オブジェクト

公開キー証明書のサブジェクトまたは発行元の識別名を表す再利用可能なオブジェクト。

シグニチャ ID（Sid）

各侵入ルールに割り当てられた固有の識別番号（別名 Snort ID）。新しいルールを作成するか、既存の標準テキスト ルールを変更すると、1,000,000 かそれより大きな SID が割り当てられます。FireSIGHT システムで提供される共有オブジェクトのルールおよび標準テキスト ルールの SID は、1,000,000 より小さくなります。また、プリプロセッサおよびデコーダは、SID を使用して、検出するさまざまな種類のパケットを識別します。

シスコ VRT

シスコの脆弱性調査チーム。

シスコ クラウド

Collective Security Intelligence クラウドを参照してください。

システム ポリシー

メール中継ホスト設定や時刻同期設定のような、展開内の複数のアプライアンスで同じになる可能性のある設定。システム ポリシーは、Defense Centerを使用して、防御センター自体または管理対象適用にデバイスします。

自動アプリケーション バイパス（AAB）

インターフェイスを通過するパケットを処理する時間を制限し、時間が超過したときにパケットが処理をバイパスすることを可能にする高度なデバイス設定。

修復

システムに対する潜在的な攻撃を軽減するアクション。修復を設定し、相関ポリシー内でそれらを相関ルールおよびコンプライアンス ホワイトリストと関連付けることにより、それらがトリガーとして使用されるときに、Defense Centerによって修復が起動されるようにすることができます。これにより、ユーザが攻撃に即時に対処できない場合でも攻撃の影響を自動的に緩和でき、またシステムが組織のセキュリティ ポリシーに準拠し続けるようにすることができます。Defense Centerには事前定義された修復モジュールが付属しています。柔軟性のある API を使用して、カスタム修復を作成することもできます。

修復インスタンス

修復モジュールの一連の設定。モジュールごとに複数のインスタンスを設定できます。たとえば、異なる相関ポリシーの違反に対し、同一のモジュールの、設定の違う異なるインスタンスを使用して対応することができます。修復インスタンスがトリガーとして使用されると、その結果実行されるアクションを修復と呼びます。

修復ステータス イベント

イベントが起動すると、生成される修復。

修復モジュール

修復と呼ばれる一連の設定を使用して修復インスタンスを起動するプログラム。FireSIGHT システムには各種アクションを実行する複数の修復モジュールが付属しています。また、柔軟性のある API を使用して独自のモジュールを作成することもできます。

状態共有

デバイスまたはスタックのいずれかに障害が発生した場合に、ピアがトラフィック フローを中断することなく引き継ぐことができるようにするために、クラスタ化されたデバイスまたはスタックを同期できる機能。状態共有は、厳密な TCP の適用、単方向のアクセス制御ルール、ブロックの持続性、および動的 NAT が適切にフェールオーバーすることを保証します。

証明書

公開キー証明書を参照してください。

証明書失効リスト（CRL）

認証局のユーザ証明書を発行したアプライアンスによって取り消された証明書のリスト。これによって、クライアント ブラウザの証明書チェックを使用して FireSIGHT システム Web インターフェイスへのアクセスを制限することができます。失効した証明書として CRL にリストされている証明書をユーザが選択した場合、ブラウザは Web インターフェイスをロードできません。SSL インスペクション中、デバイスは CRL の公開キー証明書を検出できますが、暗号化されたトラフィックを信頼しません。

処理

マルウェア処理を参照してください。

シリーズ 2

FireSIGHT システム アプライアンス モデルの 2 番目のシリーズ。リソース、アーキテクチャ、ライセンス制限のため、シリーズ 2 アプライアンスでサポートされる機能セットは限定されています。シリーズ 2 デバイスには、3D500、3D1000、3D2000、3D2100、3D2500、3D3500、3D4500、3D6500 および 3D9900 が含まれます。シリーズ 2 Defense Centerには、DC500、DC 1000、および DC 3000 が含まれます。

シリーズ 3

FireSIGHT システム アプライアンス モデルの 3 番目の シリーズ。シリーズ 3 アプライアンスには、7000 シリーズおよび 8000 シリーズのデバイスと、DC750、DC1500、DC2000、DC3500 および DC4000 のDefense Centerが含まれます。

侵害の痕跡（IOC）

システムが ネットワーク検出ポリシー エンドポイント データをモニタ対象ネットワーク上のホストに関連付けるための機能。FireAMPで設定します。侵害を受けた可能性のあるホストには、そのステータスを示すタグが付けられます。このタグは、ホスト プロファイルや関連するイベント ビューで表示されます。

侵入

ネットワーク上で発生したセキュリティ違反、攻撃、またはエクスプロイト。

侵入イベント

イベント違反を記録する侵入ポリシー。侵入イベント データには、日付、時刻、エクスプロイトの種類、および攻撃とそのターゲットに関するその他のコンテキスト情報が含まれます。

侵入検知と防御

ネットワーク トラフィックのセキュリティ ポリシー違反のモニタリング、およびインライン展開で悪質なトラフィックをブロックまたは変更する機能。FireSIGHT システムでは、ネットワーク分析ポリシーでトラフィックを前処理してから、侵入ポリシーをアクセス制御ルールまたはデフォルト アクションに関連付けるときに侵入検知と防御を実行します。

侵入ポリシー

侵入およびセキュリティ ポリシー違反についてネットワーク トラフィックを検査するために設定できる各種のコンポーネント。ネットワーク トラフィックがアクセス制御ルールの条件を満たす場合、侵入ポリシーでそのトラフィックを検査できます。また、侵入ポリシーをアクセス制御ポリシーのデフォルト アクションに関連付けることもできます。侵入ポリシーの主要コンポーネントは、トラフィックを検査する侵入ルール、およびプリプロセッサ ルールで関連付けられたプリプロセッサ オプションのイベントを生成するネットワーク分析ポリシーです。機密データを検査したり、特別なFireSIGHT 推奨レイヤ処理を実行したりする詳細設定が可能なだけでなく、必要に応じて 侵入イベントを追加することもできます。侵入ポリシーは常に変数セットと組み合わせて使用します。

侵入ルール

モニタ対象のネットワーク トラフィックに適用される場合に、潜在的な侵入、セキュリティ ポリシー違反、およびセキュリティ違反を識別する一連のキーワードおよび引数。システムはルールの条件とパケットを比較します。パケット データが条件に一致した場合、ルールがトリガーとして使用され、侵入イベントが生成されます。侵入ルールには、廃棄ルールとパス ルールが含まれます。

スイッチド インターフェイス

レイヤ 2 展開でトラフィックをスイッチするために使用するインターフェイス。タグなし 仮想ローカル エリア ネットワーク（VLAN）トラフィックを処理するための物理スイッチド インターフェイスと、VLAN タグが指定されたトラフィックを処理するための論理スイッチド インターフェイスを設定できます。

スケジュール タスク

一度だけ、または定期的に実行するようにスケジュールできる管理タスク。

スタッキング

スタック構成で 2 ～ 4 台の物理デバイスを接続することによって、ネットワーク セグメントで検査されるトラフィックの量を増加させることができる機能。スタック構成を確立したら、スタックされた各デバイスのリソースを単一の共有設定に統合します。

スタック

検出リソースを共有する、2 ～ 4 台の接続されたデバイス。

スヌーズ期間

相関ルールがトリガーとして使用された後に、システムがそのルールのトリガーを停止する間隔（秒、分、時間単位で指定される）。そのルールが再度違反されても、この期間内はトリガーしません。スヌーズ期間が終了したら、ルールを再びトリガーできるようになります（そしてトリガーとして使用された時点から新しいスヌーズ期間が開始します）。非アクティブな期間も参照してください。

脆弱性

ホストに被害を及ぼす可能性がある、特定のセキュリティ侵害の説明。Defense Centerは、それぞれのホストが影響を受けやすい脆弱性に関する情報をホストのホスト プロファイルに示します。また、脆弱性ネットワーク マップを使用して、モニタ対象ネットワーク全体でシステムが検出した脆弱性の概要を把握できます。特定のセキュリティ侵害に対してホストが脆弱ではなくなったと判断した場合、特定の脆弱性を非アクティブにするか、無効としてマークすることができます。

脆弱性 ID

特定の脆弱性に関連付けられた ID 番号。シスコの脆弱性データベースおよびサードパーティの脆弱性データベース（Bugtraq や CVE など）では、異なる脆弱性 ID の番号付け方式が使用されています。

脆弱性データベース

ホストに被害を及ぼす可能性のある既知の脆弱性のデータベース。VDB とも呼ばれます。ユーザが特定のホストでネットワークのセキュリティ侵害のリスクが大きくなっているかどうかを判断できるように、システムは各ホストで検出されたオペレーティング システム、アプリケーション プロトコル、およびクライアントを VDB に関連付けます。VDB アップデートには、新規の脆弱性と更新された脆弱性、および新規アプリケーション ディテクタと更新されたアプリケーション ディテクタが含まれることがあります。

脆弱性の詳細

脆弱性ワークフローの最後のページ。脆弱性の詳細には、技術的な詳細と既知のソリューションを含む特定の脆弱性に関する情報が示されます。

脆弱性マッピング

脆弱性とのディスカバリ データ情報の関連付け。これにより、影響の相関を実行できます。

セキュア ソケット レイヤ（SSL）

Transport Layer Security プロトコルの基になった暗号アプリケーション層プロトコル。SSL インスペクション機能を使用することにより、SSL プロトコルで暗号化されたトラフィックを復号化できます。

セキュリティ インテリジェンス

送信元または宛先の IP アドレスに基づいて、アクセス制御ポリシーごとに、ネットワークを通過できるトラフィックを指定できる機能。特に、アクセス制御ルールによってトラフィックが分析される前に、特定の IP アドレスをブラックリストに登録する（アドレス間で送受信されるトラフィックを拒否する）必要がある場合に役立ちます。必要に応じて、セキュリティ インテリジェンス フィルタリングのモニタ設定を使用して、システムでブラックリストに追加された接続を分析し、さらにブラックリストとの一致を記録させることができます。

セキュリティ インテリジェンス イベント

接続イベントによってブロックまたはモニタされるトラフィックが生成するセキュリティ インテリジェンス ブラックリスト。通常の接続イベントとは別に、セキュリティ インテリジェンス イベントを表示および対話操作できます。

セキュリティ インテリジェンス オブジェクト

1 つ以上の IP アドレスを表す単一の設定。これは、アクセス制御ポリシーのセキュリティ インテリジェンス ブラックリストおよびセキュリティ インテリジェンス ホワイトリストに追加します。セキュリティ インテリジェンス オブジェクトには、セキュリティ インテリジェンス リスト、セキュリティ インテリジェンス フィード、およびネットワーク オブジェクトとグループが含まれます。グローバル ブラックリスト、グローバル ホワイトリスト、およびインテリジェンス フィードのカテゴリは、セキュリティ インテリジェンス オブジェクトと見なされます。

セキュリティ インテリジェンス フィード

セキュリティ インテリジェンス オブジェクトの種類の 1 つ。ユーザが設定する間隔で、システムが定期的にダウンロードする IP アドレスの動的なコレクション。フィードは定期的に更新されるため、フィードを使用することで、システムがセキュリティ インテリジェンス機能を使用したネットワーク トラフィックのフィルタリングに最新の情報を使用することが保証されます。インテリジェンス フィードも参照してください。

セキュリティ インテリジェンス ブラックリスト

アクセス制御ポリシーで、トラフィックをアクセス制御ルールによって分析する前に、対象のホストとの間のトラフィックを拒否できるようにする IP アドレスのリスト。ブラックリストはセキュリティ インテリジェンス オブジェクトで構成されます。これには、グローバル ブラックリストも含まれます。アクセス コントロール ポリシーのセキュリティ インテリジェンス ホワイトリストは、ブラックリストよりも優先されます。

セキュリティ インテリジェンス ホワイトリスト

アクセス制御ポリシーで、アクセス制御ルールを使用するホストとの間のトラフィックがポリシーによって検査されるように強制する（つまり、セキュリティ インテリジェンスを使用してトラフィックを拒否しないようにする）ための IP アドレスのリスト。ポリシーのホワイトリストはセキュリティ インテリジェンス ブラックリストよりも優先されるため、ブラックリストの微調整に使用できます。ホワイトリストは、セキュリティ インテリジェンス オブジェクトで構成されます。これには、グローバル ホワイトリストも含まれます。

セキュリティ インテリジェンス リスト

ユーザがDefense Centerとしてセキュリティ インテリジェンス オブジェクトに手動でアップロードする IP アドレスのシンプルで静的なコレクション。セキュリティ インテリジェンス フィード、グローバル ブラックリスト、およびグローバル ホワイトリストを補強および微調整するために、このリストを使用します。

セキュリティ ゾーン

さまざまなポリシーおよび設定でトラフィック フローを管理および分類するために使用できる 1 つ以上のインライン、パッシブ、スイッチド、またはルーテッド インターフェイスのグループ。単一ゾーンのインターフェイスは、複数デバイスのにまたがる場合があります。単一のデバイスに対して複数のセキュリティ ゾーンを設定することもできます。トラフィックをセキュリティ ゾーンと照合するには、少なくとも 1 つのインターフェイスをそのセキュリティ ゾーンに割り当てる必要があり、各インターフェイスは 1 つのゾーンのみに属することができます。

セキュリティ ポリシー

ネットワークを保護するための組織のガイドライン。たとえば、セキュリティ ポリシーではワイヤレス アクセス ポイントの使用が禁止されることがあります。セキュリティ ポリシーには、従業員に組織のシステムの使用方法に関するガイドラインを示す利用規定（AUP）が含まれる場合もあります。

セキュリティ ポリシー違反

セキュリティ違反、攻撃、エクスプロイト、またはその他のネットワークの誤用。

接続

2 台のホスト間のモニタ対象セッション。デバイス 対応デバイスからのインポート接続データだけでなく、FireSIGHT システム管理対象NetFlowによって検出された接続も記録できます。

接続イベント

システムがモニタ対象イベントとその他のホストの間で接続を検出したときに生成されるホスト。セキュリティ インテリジェンス イベントは、特殊な接続イベントです。接続イベントには、検出されたトラフィックに関する情報が含まれます。さまざまな設定を使用して、記録する接続とタイミング、およびそのデータの保存先に関するきめ細かい制御が可能です。管理対象デバイスによって接続が検出された場合、ブロック解除された接続は開始時および終了時に記録できますが、ブロックされた接続の多くは開始時にのみ記録できます。これらの接続は、Defense Center データベースに記録できます。ルールまたはデフォルト アクションに応じて、接続イベントを外部 Syslog または SNMP トラップ サーバに記録することもできます。NetFlow レコードには接続の終了が記録され、常にデータベースに保存されます。

接続グラフ

グラフ形式で接続イベントを表示する方法。

接続サマリ

5 分間隔で集約される接続データ。システムは接続サマリを使用して接続グラフとトラフィック プロファイルを作成します。データが集約されるためには、複数の接続が接続の終了を表し、送信元と宛先の IP アドレスが同じで、応答側（宛先）ホストで同じポートを使用している必要があります。それらは同じプロトコル（TCP または UDP）とアプリケーション プロトコルを使用している必要があります。また、同じ管理対象デバイスによって検出されるか、同じ NetFlow 対応デバイスによってエクスポートされている必要があります。

接続トラッカー

ルールの最初の基準が満たされた後、システムが特定の相関ルールの追跡を開始するように、接続を制約する 1 つ以上の条件。次にルールがトリガーされるのは、追跡された接続がさらに基準を満たした場合のみです。

接続ログ

接続イベントを参照してください。

設定（インポートまたはエクスポート用）

ポリシーやカスタム ワークフローなどの一連の設定。アプライアンス上に作成され、そのアプライアンスからエクスポートしたり、別のアプライアンスがインポートしたりできます。

設定可能なバイパス

インライン セットの設定を可能にするバイパス モードの特性。

センシング インターフェイス

ネットワーク セグメントをモニタするために使用するデバイス上のネットワーク インターフェイス。管理インターフェイスと比較

相関

ネットワークの脅威にリアルタイムで対応する相関ポリシーを構築するために使用できる機能。相関の修復コンポーネントは、**ポリシー**違反に対応する独自のカスタム修復モジュールを作成してアップロードすることを可能にする柔軟な API を提供します。

相関イベント

イベントがトリガーとして使用されると、Defense Centerよって生成される相関ルール。ホワイトリスト イベント（ホワイトリスト違反より生成される）は、特殊な相関イベントであることに注意してください。

相関ポリシー

セキュリティ ポリシーおよび相関ルールを使用して、コンプライアンス ホワイトリスト違反に相当するネットワーク アクティビティを示すポリシー。ポリシー内の各ルールまたはホワイトリストに対する応答を指定できます。

相関ルール

コンプライアンス ホワイトリストと同様、ネットワーク トラフィックが相関ポリシーに違反していると見なされる場合に満たしているべき基準を指定する方法の 1 つ。Defense Centerを使用して、特定のイベントが発生したとき、またはネットワーク トラフィックが相関イベントに示された通常のネットワーク トラフィック パターンから逸脱しているときにトリガーとして使用される（かつトラフィック プロファイルを生成する）相関ルールを設定できます。ホスト プロファイル条件、接続トラッカー、スヌーズ期間、および非アクティブな期間で相関ルールを制約できます。相関ルールのトリガー時にアラートや修復などの応答を起動するようにDefense Centerを設定することもできます。

ゾーン

セキュリティ ゾーンを参照してください。

ターゲット デバイス

ポリシー ターゲットを参照してください。

楕円曲線（EC）暗号

有限フィールドのランダムな楕円曲線上にある計算ポイントに基づく暗号化方式。RSA 暗号化とは対照的な暗号です。

タグ（アプリケーション）

アプリケーション タグを参照してください。

タスク キュー

アプライアンスが実行する必要のあるジョブのキュー。適用をポリシーし、ソフトウェア更新をインストールし、他の長時間かかるジョブを実行すると、ジョブがキューに入れられ、ジョブのステータスが [Task Status] ページに表示されます。[Task Status] ページには、ジョブの詳細リストが提供され、10 秒ごとに更新されて状態が更新されます。

ダッシュボード

現在のシステム ステータスを一目で理解できるビューを提供するディスプレイ。これには、システムによって収集され、生成されるイベントに関するデータが含まれます。システムによって提供されるダッシュボードを補強するために、選択したダッシュボード ウィジェットを組み込んだ複数のカスタム ダッシュボードを作成できます。モニタ対象のネットワークの状態と機能を、幅広の簡潔かつカラフルな図で示すContext Explorer と比較してください。

ダッシュボード ウィジェット

FireSIGHT システムの状況を把握するための小型の自己完結型ダッシュボード コンポーネント。

タップ モード

3D9900 および インライン セット のデバイスで使用可能な高度なシリーズ 3のオプション。これを使用する場合は、各パケットのコピーが分析され、ネットワーク トラフィック フローはデバイスを通過しないので、影響を受けません。パケット自体ではなくパケットのコピーを処理するため、トラフィックをドロップ、変更、またはブロックするように、アクセス制御および侵入ポリシーを設定した場合でも、デバイスはパケット ストリームに影響を与えることはありません。

ディスカバリ

管理対象デバイスを使用してネットワークをモニタし、ネットワークの完全で永続的なビューを提供する、FireSIGHT システムのコンポーネント。ネットワーク検出は、ネットワーク上のホスト (ネットワーク デバイスとモバイル デバイスを含む) の数と種類、およびそれらのホストのオペレーティング システム、アクティブなアプリケーション、オープン ポートを判別します。ネットワーク上のユーザ アクティビティをモニタするように管理対象デバイスを設定することもできます。これにより、ポリシー違反、攻撃、またはネットワークの脆弱性の源を識別できます。

ディスカバリ イベント

新しい資産または既存の資産に対する変更のイベントの詳細を示すディスカバリ。ホスト入力イベントは、特別な種類のディスカバリ イベントです。「ディスカバリ イベント」は、ディスカバリ データまたは脆弱性の情報を意味する場合があります。

ディスカバリ データ

アプリケーション機能を使用して収集されるネットワーク資産とトラフィック フローを絞り込むための、ホスト、ユーザ、およびディスカバリの情報。

ディスカバリ ポリシー

ネットワーク検出ポリシーを参照してください。

ディスカバリ ルール

ネットワーク検出ポリシー内で、モニタするネットワークとゾーン、それらをモニタするために使用するデバイス（NetFlow 対応デバイスを含む）、およびモニタ対象から除外するポートを指定します。各ルールは、モニタ対象ネットワークでホスト、user、またはアプリケーションを検出するかどうかも指定します。

データ コリレータ

システムによって収集されたデータを使用して、イベント上でネットワーク マップを生成し、Defense Centerを作成するプログラム。

データベース アクセス

サードパーティ クライアントによるDefense Center データベースへの読み取り専用アクセスを許可する機能。

テーブル ビュー

ワークフロー情報を表示するイベント ページの 1 つの種類。データベース テーブルの各フィールドに対して 1 列があります。イベント分析を実行する際は、目的のイベントに関する詳細を表示するテーブル ビューに移動する前に、ドリルダウン ページを使用して、調査するイベントを制約できます。多くの場合、テーブル ビューはシステム付属のワークフローの最後から 2 番目のページです。

適応型プロファイル

アクセス制御ポリシーを使用して、パケットのターゲット ディスカバリ データのオペレーティング システムを判別するホストの詳細設定（パッシブ展開に推奨）。ネットワーク分析ポリシー内の対象を絞ったプロファイルによって、ターゲット ホストのオペレーティング システムと同じ方法で IP パケットが最適化され、ストリームが再構成されます。次に、侵入ポリシーが宛先ホストで使用されるものと同じ形式でデータを分析します。

適用

ポリシーまたはそのポリシーに対する変更を有効にするアクション。ほとんどのポリシーは、Defense Centerから管理対象デバイスに適用します。ただし、相関ポリシーは管理対象デバイスの設定への変更に関与しないため、このポリシーはアクティブにしたり非アクティブにしたりします。

デコーダ

スニッフィングされたパケットを侵入検知と防御が認識できる形式に変換するネットワーク分析ポリシーのコンポーネント。プリプロセッサで設定されます。

デバイス

物理的にフォールトトレラントな専用アプライアンス（Cisco ASA with FirePOWER Services を含む）。スループットの範囲内、または同じ多くの機能があるソフトウェアベースの展開で使用できます。デバイスで有効にするライセンス機能に応じて、これらを使用してトラフィックを受動的にモニタし、ネットワーク資産、アプリケーション トラフィック、およびユーザ アクティビティの全体的なマップを作成したり、アクセス制御を実行したりすることができます。また、多くのデバイスでスイッチング、ルーティング（DHCP リレーと NAT を含む）、および VPN を実行できます。Defense Centerを使用してデバイスを管理する必要があります。

デバイス クラスタリング

クラスタリングを参照してください。

デバイス スタッキング

スタッキングを参照してください。

デフォルト アクション

アクセス制御ポリシーまたは SSL ポリシーの一部で、ポリシーのaction以外のルールの条件を満たさないトラフィックを処理、検査、および記録する方法を指定するモニタ。

動的分析

マルウェア分析のために、キャプチャされたファイルからデバイスにCollective Security Intelligence クラウドを送信する方法。クラウドはテスト環境でファイルを実行し、脅威スコアと動的分析サマリ レポートをDefense Centerに返します。動的分析サマリ レポートから、VRT 分析レポートも表示できます。

動的分析サマリ レポート

Collective Security Intelligence クラウドが脅威スコアをファイルに割り当てた理由（動的分析時に発見されたすべての脅威、およびファイルをテスト環境で実行したときに検出された追加のプロセスを含む）のサマリ。ここから、VRT 分析レポートを表示することもできます。

動的ルール状態

ルールに一致するトラフィックで検出されたレートの異常に応答して一定期間設定される侵入ルール状態。

トラフィック チャネル

管理トラフィックまたはイベント トラフィックのいずれかを伝送するため、シリーズ 3 のアプライアンスまたは仮想Defense Centerの管理インターフェイスで設定できる接続。イベント トラフィック チャネルは、管理対象デバイスのネットワーク セグメントで生成されたイベント データだけを伝送し、管理トラフィック チャネルは内部で生成されたトラフィック（つまり、Defense Centerとデバイス間の管理トラフィック）だけを伝送します。管理インターフェイスを参照してください。

トラフィック プロファイル

指定した期間にログに記録される**接続イベント**に基づいた、ネットワーク上のトラフィックのプロファイル。モニタ対象ネットワーク セグメントのすべてのトラフィックを使用してプロファイルを作成することも、より対象を絞ってプロファイルを作成することもできます。次に、相関機能を使用し、既存のプロファイルに照らして新しいトラフィックを評価することによって、異常なネットワーク トラフィックを検出することができます。

トランスペアレント インライン モード

インライン セットが「Bump In The Wire」として機能できるようにする、またデバイスが認識するすべてのネットワーク トラフィックを、その送信元および送信先に関係なく、転送できるようにする、高度なデバイスのオプション。

ドリルダウン ページ

ワークフロー ビューを制約するために使用される中間イベント ページ。通常、ドリルダウン ページは、ページまたはテーブル ビューをさらに詳細に絞り込むために選択できる制約を提供します。

ドロップ イベント

侵入イベントがトリガーとして使用されると生成される廃棄ルール。イベント ビューアでは、ドロップ イベントは黒色の下矢印でマークされます。

内部認証

アプライアンス上のローカル データベースにユーザ クレデンシャルを保存する認証方式。ユーザ がアプライアンスにログインする際に、ユーザ名およびパスワードが、データベース内の情報と照合されます。外部認証と比較

認証オブジェクト

FireSIGHT システムの Web インターフェイスに対する外部認証（RADIUS または LDAP）を有効にするため、外部認証サーバに接続できるようにする設定の集合。

認証局

サーバ証明書またはユーザの公開キー証明書の作成に使用される証明書発行元。サーバおよびユーザの証明書によって、サーバ ID またはユーザ ID の追加確認が行われます。

ネットワーク オブジェクト

1 つ以上の IP アドレス、CIDR ブロック、またはプレフィクス長を表す再利用可能なオブジェクト。

ネットワーク デバイス

FireSIGHT システムで、ブリッジ、ホスト、ルータ デバイス、またはNATとして識別されるロード バランサ。

ネットワーク ファイルの伝搬経路

ホストがネットワークでファイルを転送する際のファイル パスの視覚表現。SHA-256 ハッシュ値に関連付けられたファイルの場合、伝搬経路マップには、ファイルを転送したすべてのホストの IP アドレス、ファイルが検出された時間、ファイルのマルウェア処理、関連するファイル イベント、マルウェア イベントなどが表示されます。

ネットワーク マップ

ネットワークの詳細な表現。ネットワーク マップによって、ネットワークで実行するホスト、モバイル デバイス、およびネットワーク デバイス、またそれらに関連するホスト属性、アプリケーション プロトコル、および脆弱性の観点からネットワーク トポロジを表示することができます。

ネットワーク検出

ディスカバリを参照してください。

ネットワーク検出ポリシー

システムが特定のネットワーク セグメント(ポリシー 対応デバイスにより監視されるネットワークを含む)について収集する、ディスカバリ データの種類(ホスト、ユーザ、およびアプリケーション データを含む)を指定するNetFlow。ネットワーク検出ポリシーは、ID の競合の解決設定、アクティブ検出のソースの優先度、および侵害の痕跡(IOC)も管理します。

ネットワーク分析ポリシー

プリプロセッサによって後で分析できるように、ネットワーク トラフィックを復号化、標準化、および前処理するように設定できるさまざまな侵入ポリシー。デフォルトでは、システム付属の 1 つのネットワーク分析ポリシーが、アクセス制御ポリシーによって処理されたすべてのトラフィックを前処理します。ただし、この前処理を実行するカスタム ネットワーク分析ポリシーを選択することもできます。上級ユーザは、複数のカスタム ネットワーク分析ポリシーでセキュリティ ゾーン、ネットワーク、または VLAN タグに基づいてトラフィックを前処理できる、ネットワーク分析ルールを使用できます。

ネットワーク分析ルール

FireSIGHT システムの上級ユーザが複数のカスタム ネットワーク分析ポリシーを使用して対象を絞った前処理を実行するために使用できる一連の条件。ネットワーク分析ルールは、アクセス制御ポリシーの詳細オプションとして設定します。

ハイ アベイラビリティ

Defense Centerのグループを管理するように冗長物理デバイスを設定できる機能。イベント データは管理対象デバイスから両方のDefense Centerにストリームされ、ほとんどの設定要素が両方のDefense Centerに保持されます。プライマリDefense Centerに障害が発生した場合は、セカンダリDefense Centerを使用して、中断することなくネットワークをモニタできます。冗長デバイスを指定できるクラスタリングと比較してください。

廃棄ルール

侵入ルールが [Drop and Generate Events] に設定されたルール状態。悪質なパケットによってインライン展開のルールがトリガーとして使用された場合、ユーザが侵入ポリシーした適用が [Drop When Inline] に設定されていれば、システムはそのパケットをドロップし、侵入イベント(具体的には、ドロップ イベント)を生成します。

バイパス モード

インライン セットのセンシング インターフェイスが何らかの理由で失敗し場合に、トラフィックがフローを続行することを許可するインライン セットの特性。

ハイブリッド インターフェイス

論理インターフェイスとデバイスの間でのトラフィックのブリッジを可能にする管理対象仮想ルータ上の仮想スイッチ。

パケット ビュー

ワークフローをトリガーしたパケット、または侵入ルールを生成したプリプロセッサに関する詳細情報を提供する、侵入イベント ページの 1 つの種類。パケット ビューは、侵入イベントに基づくワークフローの最後のページです。

パス ルール

トリガーとして使用されたときに、侵入ルールを生成せず、またルールをトリガーしたパケットの詳細を記録しない侵入イベント。侵入ルールを無効にする代わりに、パス ルールを使用することによって、特定の状況で特定の基準を満たすパケットがイベントを生成しないようにできます。廃棄ルールと比較

派生フィンガープリント

システムにより、パッシブに収集されたフィンガープリントのフィンガープリントから作成されるオペレーティング システムのホスト。収集された各フィンガープリントの信頼値と ID 間の裏付けとなるフィンガープリント データの量を使用して最も可能性の高い ID を計算する式を適用することにより作成されます。

パッシブ インターフェイス

パッシブ展開でトラフィックを分析するように設定されたセンシング インターフェイス。

パッシブ検出

管理対象ディスカバリ データによってパッシブに収集されたトラフィックの分析によるデバイスのコレクション。アクティブ検出と比較してください。

バナー

サーバ バナーを参照してください。

非アクセス制御ユーザ

ユーザ エージェントまたは管理対象デバイスのいずれかによって検出された、アクセス制御には使用されないユーザ。非アクセス制御ユーザは、ホストにログインしている現在のユーザがいない場合のみ、そのホストのアクセス制御ユーザになることができます。

非アクティブな期間

相関ルールがトリガーとして使用されない間隔。非アクティブな期間の時間、頻度、および期間を設定できます。スヌーズ期間も参照してください。

ビジネスとの関連性

アプリケーションが、娯楽目的ではなく、組織の事業運営のコンテキスト内でが使用される可能性。アプリケーションのビジネスとの関連性は、Very Low から Very High までの範囲です。

非バイパス モード

インライン セットのセンシング インターフェイスが何らかの理由で失敗し場合に、トラフィックをブロックするインライン セットの特性。

秘密キー

ペアにされた公開キー証明書の所有者にのみ知らされる暗号キー。公開キーおよび秘密キーは、セキュア ソケット レイヤ（SSL）とTransport Layer Security の暗号化および復号化に使用されます。

標準テキスト ルール

ルール エディタで使用可能な ID、キーワード、および引数に基づいて作成された侵入ルール。独自のカスタム標準テキスト ルールを作成し、シスコが提供する標準テキスト ルールを変更できます。標準テキスト ルールのジェネレータ ID（GID）は 1 です。

ファイル イベント

管理対象イベントによってネットワーク トラフィックで検出されるファイルを表すデバイス。

ファイル カテゴリ

グラフィック、実行可能ファイル、アーカイブなど、ファイル タイプの一般的な分類。

ファイル キャプチャ

キャプチャされたファイルを参照してください。

ファイル ストレージ

保存済みファイルを参照してください。

ファイル タイプ

PDF、EXE、MP3 などのファイル形式の特定のタイプ。

ファイル ポリシー

システムがポリシーとネットワークベースのファイル制御を実行するために使用する高度なマルウェア対策。ファイル ルールが組み込まれたファイル ポリシーは、アクセス制御ルール内のアクセス制御ポリシーによって呼び出されます。

ファイル ルール

ネットワーク トラフィックを調べるために、FireSIGHT システムが使用するファイル ポリシー内の一連の基準。送信されたファイルがルールの基準と一致した場合、ルールがトリガーとして使用され、ファイル イベントが生成されます。ファイル ルール アクションによって、（ファイル タイプまたはマルウェア処理に基づいて）ファイルをブロックするか、単純にファイルを通過させて送信をログに記録するかが決まります。

ファイル ルール アクション

システムがファイル ルールの条件を満たすファイルをどのように処理するかを決定する設定。特定のファイル タイプを検出してそれについてのアラートを出すことや、それらのファイルの送信をブロックすることができます。これらのファイル タイプのサブセットでマルウェア クラウド ルックアップを実行することも、マルウェア処理に基づいてこれらのファイルの送信をブロックすることもできます。

ファイル処理

マルウェア処理を参照してください。

ファイル制御

ネットワークを通過できるファイル タイプを指定したり、ログに記録したりすることができる、アクセス制御の一環を成す機能。

ファイル伝搬経路

ネットワーク ファイルの伝搬経路を参照してください。

フィード

セキュリティ インテリジェンス フィードを参照してください。

フィンガープリント

ホストのオペレーティング システムを識別するために、システムが特定のパケット 見出し値やネットワーク トラフィックのその他の固有データと比較する確立された定義。システムがホストのオペレーティング システムを誤って識別したり、識別できなかったりする場合は、ホストを識別するカスタム フィンガープリントを作成できます。

複雑な制約

特定のイベントのすべての条件を使用してイベントのクエリを制約するイベント ビューまたはイベント検索の制約セット。

ブックマーク

イベント分析の特定の場所と時間への保存されたリンク。ブックマークは、使用しているワークフロー、表示しているワークフローの一部、表示しているワークフロー内のページ数、選択した時間枠、無効にした列、および課した制約に関する情報を保持します。

物理インターフェイス

NetMod の物理ポートを表すインターフェイス。

不明なホスト

システムによってトラフィックが分析されたが、既知のどのホストにもオペレーティング システムが一致しないフィンガープリント。未確認ホストと比較してください。

プライベート検索

ユーザ アカウントに関連付けられた特定のテーブルの検索基準の名前付きセット。ユーザ自身か管理者アクセス権を持つユーザのみがそのユーザのプライベート検索を使用できます。

ブラックリスト

ヘルス モニタ ブラックリストまたはセキュリティ インテリジェンス ブラックリストを参照してください。

プリプロセッサ

侵入およびエクスプロイトに関してさらに検査するようにトラフィックを準備するシステムのコンポーネント。プリプロセッサはトラフィックを正規化し、不適切なヘッダー オプションの特定、IP データグラムの最適化、TCP ステートフル インスペクションおよびストリーム再構成の提供、チェックサムの検証によって、ネットワーク層プロトコルおよびトランスポート層プロトコルの異常を特定するのに役立ちます。プリプロセッサは、特定の種類のパケット データを、システムが分析できる形式に変換することもできます。これらのプリプロセッサは、データ正規化のプリプロセッサ、またはアプリケーション層プロトコル プリプロセッサと呼ばれます。アプリケーション層プロトコル エンコードを正規化することで、システムは、データを表す方法が異なるパケットに同じコンテンツ関連侵入ルールを効果的に適用し、有意義な結果を得ることができます。プリプロセッサは、パケットがユーザが設定したプリプロセッサ オプションをトリガー

として使用するたびに、プリプロセッサ イベントを生成します。プリプロセッサの設定には特定の専門知識が必要で、通常はほとんどまたはまったく変更する必要がありません。さらに、すべての展開環境に共通するものではありません。

プリプロセッサ イベント

パケットが指定された侵入イベント オプションをトリガーとして使用すると生成されるプリプロセッサの 1 つの種類。プリプロセッサ イベントは、異常なプロトコルのエクスプロイトを検出するのに役立ちます。

プリプロセッサ ルール

侵入ルールまたはポートスキャン フロー ディテクタと関連付けられたプリプロセッサ。イベントが生成されるようにするには、プリプロセッサ ルールを有効にする必要があります。プリプロセッサ ルールにはプリプロセッサ固有のジェネレータ ID（GID）があります。

ヘルス イベント

展開内のいずれかのイベントがアプライアンスで指定されたパフォーマンス基準を満たす（または満たしていない）ときに生成されるヘルス モジュール。ヘルス イベントは、アラートを生成することもできます。

ヘルス ポリシー

展開内のアプライアンスのヘルスを検査するときに使用される基準。ヘルス ポリシーは、ヘルス モジュールを使用して、システムのハードウェアおよびソフトウェアが正しく動作しているかどうかを示します。デフォルトのヘルス ポリシーを使用するか、独自のヘルス ポリシーを作成できます。

ヘルス モジュール

展開内のアプライアンスの特定のパフォーマンスの側面（CPU 使用率や使用可能なディスク領域）のテスト。ヘルス ポリシーでユーザが有効にするヘルス モジュールは、ユーザがモニタするパフォーマンスの側面が特定のレベルに達した場合に、ヘルス イベントを生成します。

ヘルス モニタ

展開内のアプライアンスのパフォーマンスを継続的にモニタする機能。ヘルス モニタは、適用されたヘルス モジュール内のヘルス ポリシーを使用して、アプライアンスをテストします。

ヘルス モニタ ブラックリスト

不要なヘルス イベントの生成を防止するため、ヘルス モニタリングを部分的に一時無効にする設定。アプライアンスのグループ、単一のアプライアンス、または特定のヘルス モジュールのモニタリングを無効にすることができます。

変更調整レポート

過去 24 時間に行われたシステム変更すべての詳細レポート。新しい設定が保存されるたびに作成されるスナップショットに基づきます。毎日指定した時間に、それらのレポートを電子メールで送信するようにシステムを設定できます。

変数

侵入ルールで一般に使用される値の表現。FireSIGHT システムは、変数セットに編成された事前設定済みの変数を使用してネットワークおよびポート番号を定義します。複数のルールでこれらの値をハードコーディングするのではなく、ネットワーク環境を正確に反映するようにルールを調整するには、変数の値を変更できます。

変数セット

各侵入ポリシーで有効になっている変数をネットワーク トラフィックに厳密に一致させるために調整できるよう、侵入ポリシーにリンクさせる侵入ルール設定の集合。

Defense Center

デバイスを管理し、それらが生成したイベントを自動的に集約し、関連付けることができる一元管理ポイント。

ポート オブジェクト

トランスポート層プロトコル（TCP、UDP、ICMP など）を使用するオープン ポートを表す再利用可能なオブジェクト。

保護されたネットワーク

ファイアウォールなどのデバイスによって他のネットワーク ユーザから保護された組織の内部ネットワーク。システムによって提供される侵入ルールの多くは、変数を使用して保護されたネットワークと保護されていない（または外部）ネットワークを定義します。

ホスト

ネットワークに接続され、一意の IP アドレスを持つデバイス。FireSIGHT システムでは、ホストは、モバイル デバイス、ブリッジ、ルータ、NAT デバイス、またはロード バランサとしては分類されない、識別されたホストを指します。

ホスト ビュー

ワークフローまたはネットワーク資産を表示するディスカバリ イベントの最後のページ。ホスト ビューは、表示しているイベントや資産に関連するホスト プロファイルのホストを表示します。

ホスト プロファイル

特定の検出されたホストに関する収集された情報。これには、ホストの名前やオペレーティング システム、またホストで実行されているプロトコルやホストなどのアプリケーションに関する一般情報が含まれます。ホスト プロファイルには、そのホストに関するユーザ履歴、ホスト属性、仮想ローカル エリア ネットワーク（VLAN）情報、該当するホワイトリスト違反、検出された脆弱性、侵害の痕跡（IOC）、およびスキャン結果も含まれる場合があります。

ホスト プロファイル条件

トラフィック プロファイルまたは相関ルールで設定される制約。相関ルール内のホスト プロファイル条件は、Defense Centerが特定の基準を満たす場合のみ、相関イベントがホストを生成することを指定します。トラフィック プロファイル内のホスト プロファイル条件は、プロファイルが作成されるホストを制限します。

ホスト属性

システムで検出されるホストに関する情報を提供し、ネットワーク環境で重要になる方法でそれらのホストを分類するために使用できるツール。システムには、2 種類の事前定義されたホスト属性（ホストの重要度とメモ）と、それぞれのアクティブなコンプライアンス ホワイトリストとの各ホストのコンプライアンスを示すホスト属性があります。独自のホスト属性を作成することもできます。

ホスト入力

ネットワーク マップの情報を増やすために、スクリプトまたはコマンドライン ファイルを使用してサードパーティ ソースからデータをインポートできる機能。Web インターフェイスは、いくつかのホスト入力機能を提供します。オペレーティング システムやアプリケーション プロトコル ID の変更、脆弱性の有効化または無効化、ネットワーク マップからのさまざまな項目（クライアントとサーバのポートなど）の削除を実行できます。

ホスト入力イベント

ディスカバリ イベント機能を使用するときに生成される、ホスト入力の一種。ホスト入力イベントとパッシブ ディスカバリ イベントは相関ルールを作成するときには区別されますが、通常は、これらのイベントは同じように処理されます。

ホストの重要度

システムによって検出される特定のホスト属性のビジネス重要度（重要性）を示すホスト。

ホスト履歴

ユーザ アクティビティの過去 24 時間のグラフィカル表現。ユーザのユーザ詳細で表示できるホスト履歴には、棒グラフで表わされるおおよそのログインおよびログアウトの時間とともに、ユーザがログインしたホストの IP アドレスが表示されます。

保存済みファイル

キャプチャされたファイルのハード ドライブまたはデバイス（インストールされている場合）に保存されたマルウェアのストレージ パック。保存済みファイルは後でダウンロードし、分析することができます。

ポリシー

設定を（ほとんどの場合は、アプライアンスに）適用するためのメカニズム。アクセス制御ポリシー、相関ポリシー、ファイル ポリシー、ヘルス ポリシー、侵入ポリシー、ネットワーク分析ポリシー、ネットワーク検出ポリシー、SSL ポリシー、およびシステム ポリシーを参照してください。

ポリシー ターゲット

アプライアンスをゾーンする適用またはポリシー。ポリシーは、複数のターゲットを持つ場合があります。

保留中（アプリケーション プロトコル）

システムがアプリケーション プロトコルを肯定的にも否定的にも識別できないときにアプリケーション プロトコル ID に与えられる設定。多くの場合、システムが保留中のアプリケーション プロトコルを識別するには、より多くのデータを収集して分析する必要があります。

ホワイトリスト

コンプライアンス ホワイトリストで、ある種のアクションから IP アドレスを除外するために設定できるセキュリティ インテリジェンス ホワイトリスト、HA リンク インターフェイス、修復、または IP アドレスのリスト。

ホワイトリスト イベント

有効なターゲット ホストがイベントに準拠しなくなったことをシステムが検出したときに生成されるコンプライアンス ホワイトリスト。ホワイトリスト イベントは、特殊な相関イベントです。

ホワイトリスト違反

ホストがイベント ビューアにどのように準拠していないか詳細を示す、コンプライアンス ホワイトリストで確認できる情報。

マルウェア イベント

シスコのイベントソリューションのいずれかによって生成される高度なマルウェア対策。ネットワークベースのマルウェア イベントは、Collective Security Intelligence クラウドがネットワーク トラフィックで検出されたファイルに対してマルウェア処理を返すと、生成されます。レトロスペクティブ マルウェア イベントは、その処理が変更されたときに生成されます。展開されたエンドポイント が脅威を検出したとき、マルウェア の実行をブロックしたとき、マルウェアを検疫したまたは検疫に失敗したときに生成されるFireAMP コネクタベースのマルウェア イベントと比較してください。

マルウェア クラウド ルックアップ

ファイルの Defense Centerに基づいて、ネットワーク トラフィックで検出されたファイルの Collective Security Intelligence クラウドを決定するために、マルウェア処理が SHA-256 ハッシュ値と通信するプロセス。

マルウェア ブロッキング

シスコのネットワークベースの高度なマルウェア対策(AMP)ソリューションのコンポーネント。インライン展開で、マルウェア検出によって検出されたファイルのマルウェア処理が生成された場合、または検出されたファイルがカスタム検出リストにある場合は、ファイルをブロックしたり、ファイルのアップロードやダウンロードを許可したりすることができます。FireAMPが必要なシスコのエンドポイントベースの AMP ツールである FireAMP サブスクリプション とこの機能を比較してください。

Malware ライセンス

ネットワーク トラフィックで高度なマルウェア対策(AMP)を実行することができるライセンス。ファイル ポリシーを使用して、管理対象マルウェア クラウド ルックアップによって検出された特定のファイル タイプについてデバイスを実行するようにシステムを設定できます。FireAMP サブスクリプションと比較してください。

マルウェア検出

シスコのネットワークベースの高度なマルウェア対策(AMP)ソリューションのコンポーネント。全体的なデバイス設定の一環で管理対象アクセス制御に適用されたファイル ポリシーにより、ネットワーク トラフィックが検査されます。Defense Centerは、検出された特定のマルウェア クラウド ルックアップに対してファイル タイプを実行し、ファイルのマルウェア処理を警告するイベントを生成します。その後 AMP マルウェア ブロッキングが実行され、ファイルをブロッ

クするか、ファイルのアップロードまたはダウンロードを許可します。FireAMPが必要なシスコのエンドポイントベースの AMP ツールである FireAMP サブスクリプション とこの機能を比較してください。

マルウェア処理

ファイルにマルウェアが含まれているかどうかについての Collective Security Intelligence クラウド による判定。判定はファイルの SHA-256 ハッシュ値、脅威スコア、およびファイルがクリーンリストまたはカスタム検出リストのいずれにあるかに基づいて行われます。

マルウェア処理キャッシュ

ファイルのDefense Centerおよびマルウェア処理を保存する脅威スコアのキャッシュ。パフォーマンスの向上のために、システムがすでに SHA-256 ハッシュ値に基づいてファイルの処理または脅威スコアを認識している場合、Defense Centerはマルウェア クラウド ルックアップを実行する代わりにキャッシュ情報を使用します。特定の期間が経過したら、キャッシュの情報がタイムアウトすることにより、キャッシュ データが古くならないようになっています。

マルウェア対策

高度なマルウェア対策を参照してください。

マルウェアのストレージ パック

デバイスを保存するために特定のキャプチャされたファイルにインストールできるシスコが提供するセカンダリ ソリッド ステート ドライブ。これにより、イベントおよび設定ストレージのためにデバイスのプライマリ ハード ドライブに空き領域が確保されま

未確認ホスト

システムがホストに関する十分な情報をまだ収集していないため、オペレーティング システムを識別できないホスト。不明なホストと比較

モニタ

一致するトラフィックをログに記録する方法。接続をすぐに許可またはブロックせずに、システムが引き続き評価できるようにします。セキュリティ インテリジェンス ブラックリストに違反するトラフィックや、アクセス制御ルールまたは SSL ルールの基準の組み合わせに一致するトラフィックをモニタできます。

モバイル デバイス

FireSIGHT システムにおける、ホスト機能によってモバイルまたはハンドヘルド デバイスとして識別されるディスカバリ（携帯電話やタブレットなど）。多くの場合、システムは、モバイル デバイスがジェイルブレイクされているかどうかを検出できます。

ユーザ ID

userを参照してください。

ユーザ アクティビティ

システムがユーザ ログインまたはログオフ（失敗したログイン試行を含む場合があります）、またはイベント データベースでのユーザ レコードの追加または削除を検出すると生成される Defense Center。

ユーザ エージェント

ユーザがネットワークにログインする際、またはその他の理由で Active Directory 資格情報に対して認証する際に、ユーザをモニタするためにサーバにインストールするエージェント。アクセス制御ユーザによるアクティビティは、ユーザ エージェントによって報告される場合のみ、アクセス制御に使用されます。

ユーザ レイヤ

ポリシーの設定を変更できるレイヤの侵入ポリシー。

ユーザ ロール

FireSIGHT システムのユーザに付与されたアクセス レベル。たとえば、イベント アナリスト、FireSIGHT システムを管理する管理者、サードパーティ ツールを使用してDefense Center データベースにアクセスするユーザなどに対し、Web インターフェイスへの各種アクセス権限を付与できます。また、特殊なアクセス権限を持つカスタム ロールを作成することもできます。

ユーザ ロール エスカレーション

カスタム ユーザ ロールに付与すると、ログイン セッション中に、ユーザーがパスワードを入力して別のユーザ ロールの権限を取得することが可能になる特権。

ユーザ詳細

ユーザ ID およびユーザ アクティビティのワークフローの最後のページ。ユーザ詳細には、ユーザに関する一般情報とともに、ホスト履歴も表示されます。これは、過去 24 時間のユーザ アクティビティのグラフィック表示です。

ユーザ証明書

FireSIGHT システム Web サーバに対してユーザのブラウザを識別する暗号化された証明書。サーバでユーザ ID のセカンダリ検証を実行できるようにします。証明書は、認証局のサーバ証明書の発行元と同じアプライアンスによって発行される必要があります。

ユーザ制御

アクセス制御の一部であり、ネットワークを通過できるユーザ関連トラフィックの指定およびログ記録を可能にする機能。

ユーザ認識

組織が脅威、エンドポイント、ネットワーク インテリジェンスをユーザ ID 情報に関連付けることができる機能。また、この機能によってユーザ制御を実行することができます。

ユーザ認識オブジェクト

ネットワーク トラフィックまたはユーザ エージェントでアクティビティが検出されたユーザのメタデータを取得するために、LDAP サーバへの接続を可能にする設定の集合。組織が Microsoft Active Directory を使用している場合、ユーザ認識オブジェクトによってアクセス制御ユーザを指定することもできます。

ユーザ履歴

ユーザ アクティビティに関する過去 24 時間のホストのグラフィック表示。ホストのホスト プロファイルに表示されるユーザ履歴には、棒グラフで表されるおおよそのログインおよびログアウトの時間とともに、そのホストにログインしたことが検出されたユーザのユーザ名が表示されます。

ユニファイド ファイル

イベント データをログに記録するため FireSIGHT システムが使用するするバイナリ ファイル形式。

抑制

イベント抑制を参照してください。

リスク

アプリケーション リスクを参照してください。

リスト

セキュリティ インテリジェンス リストを参照してください。

リンク ステートの伝達

インライン セットのインターフェイスの 1 つが停止したときに、ペアの 2 番目のインターフェイスを自動的に停止させる、バイパス モードのインライン セットのオプション。停止したインターフェイスが再び起動すると、もう一方のインターフェイスも自動的に起動します。つまり、ペアにされたインターフェイスのリンク ステートが変更されると、その状態と一致するように他方のインターフェイスのリンク ステートが自動的に変更されます。

リンク集約グループ（LAG）

シリーズ 3の複数の物理イーサネット インターフェイスを単一の論理リンクにグループ化できる管理対象デバイス の機能。ネットワーク間のパケット スイッチングを提供するレイヤ 2 展開、またはインターフェイス間のトラフィックをルーティングするレイヤ 3 展開で設定します。このように 1 つに集約された論理リンクは、帯域幅と冗長性の向上および、2 つのエンドポイント間でのロードバランシングを実現します。

リンク集約制御プロトコル（LACP）

システムおよびポート情報の交換方法を提供する IEEE 802.3ad 仕様のコンポーネント。複数の物理ポートのバンドリングを制御して、リンク集約グループ（LAG）と呼ばれる単一の論理データを形成できます。LACP を有効にすると、チャネルの一方の端の各デバイスは、LACP を使用して集約でアクティブに使用されるリンクを特定します。

ルータ

ゲートウェイに配置され、ネットワーク間のパケットを転送するネットワーク デバイス。ネットワーク検出を使用することで、システムはルータを識別できます。また、管理対象デバイスを 2 つ以上のインターフェイス間のトラフィックをルーティングする仮想ルータとして設定できます。

ルーテッド インターフェイス

レイヤ 3 展開でトラフィックをルーティングするインターフェイス。タグなし 仮想ローカル エリア ネットワーク（VLAN）トラフィックを処理するための物理ルーテッド インターフェイスと、VLAN タグが指定されたトラフィックを処理するための論理ルーテッド インターフェイスを設定できます。また、静的なアドレス解決プロトコル（ARP）エントリをルーテッド インターフェイスに追加することもできます。

ルール

ネットワーク トラフィックの検査で照合する基準を提供する構成要素。通常、ポリシーに含まれています。アクセス制御ルール、相関ルール、ディスカバリ ルール、高速パス ルール、ファイル ルール、侵入ルール、ネットワーク分析ルール、プリプロセッサ ルール、および SSL ルールも参照してください。

ルール アクション

システムがルールの条件を満たすネットワーク トラフィックをどのように処理するかを決定する設定。アクセス コントロール ルール アクション、ファイル ルール アクション、および SSL ルール アクションも参照してください。

ルール更新

新規および更新された侵入ルール、標準テキスト ルール、および共有オブジェクトのルールを含む、必要に応じたプリプロセッサ ルールの更新。ルール更新では、ルールの削除、デフォルトの侵入ポリシー、ネットワーク分析ポリシー、および高度なアクセス制御ポリシーの設定の変更、デフォルト変数およびルール カテゴリの追加や削除が実行されることもあります。

ルール状態

侵入ルール内で侵入ポリシーが有効（[Generate Events] または [Drop and Generate Events] に設定されている）か、無効（[Disable] に設定されている）かを示します。ルールを有効にすると、そのルールはネットワーク トラフィックを評価するために使用されます。ルールを無効にすると、そのルールは使用されません。

レイヤ

侵入ポリシーまたはネットワーク分析ポリシー内の設定一式。ポリシー内のユーザ レイヤにカスタム 組み込み レイヤを追加できます。上位レイヤの設定により、下位レイヤの設定がオーバーライドされます。

レート フィルタリング

一致したトラフィック レートに基づいて、ルールの新しい侵入ルール状態を設定する異常検出の形式。

レトロスペクティブ マルウェア イベント

以前に検出されたファイルのマルウェア イベントが変更されると生成されるネットワークベースのマルウェア処理。このイベントが発生すると、システムは、そのレトロスペクティブ イベントの SHA-256 ハッシュ値を共有するファイルやマルウェアの処理も更新します。

レピュテーション（IP アドレス）

セキュリティ インテリジェンスを参照してください。

レピュテーション（URL）

URL レピュテーションを参照してください。

レポート テンプレート

レポートおよびそのセクションに対してデータの制約と形式を指定するテンプレート。

ロード バランサ

パフォーマンスとリソース使用を最適化するためにトラフィックを配信するネットワーク デバイス。ディスカバリを使用することで、システムはロード バランサを識別できます。

論理インターフェイス

タグ付きトラフィックが仮想ローカル エリア ネットワーク（VLAN）を通過する際に、特定の 物理インターフェイス タグを持つトラフィックを処理するために定義する仮想サブインターフェイス。

ワークフロー

イベント データの幅広いビューから、ユーザが関心のあるイベントだけが含まれた、より的が絞られたビューに移動することで、イベントを表示および評価するためにユーザが使用できる一連のページ。ワークフローには、それぞれが固有の機能を実行する 3 種類のページ（ドリルダウン ページ、テーブル ビュー、および最終ページ）を含めることができます。ワークフローの種類に応じて、最後のページは、テーブル ビュー、パケット ビュー、ホスト ビュー、脆弱性の詳細、ユーザ詳細のいずれかになることが考えられます。