Cisco Secure Firewall Management Center 7.4 管理ガイド

最終更新：2024 年 8 月 26 日

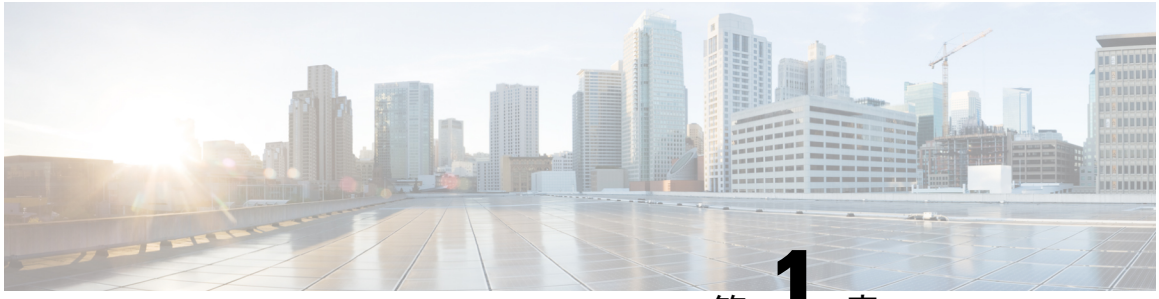
シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 部

スタートアップガイド



第 1 章

Management Center の概要

このガイドは、プライマリマネージャまたは分析専用マネージャとしてのオンプレミスの Secure Firewall Management Center に適用されます。Cisco Defense Orchestrator（CDO）クラウド提供型 Management Center をプライマリマネージャとして使用する場合、オンプレミスの Management Center は分析のみに使用できます。このガイドを CDO の管理には使用しないでください。Cisco Defense Orchestrator のクラウド提供型ファイアウォール管理センターを使用した Firewall Threat Defense の管理を参照してください。

Secure Firewall Management Center は強力な Web ベースのマルチデバイスマネージャです。独自のサーバーハードウェア上で、またはハイパーバイザ上の仮想デバイスとして稼働します。マルチデバイスマネージャを必要とし、Threat Defense のすべての機能が必要な場合は、Management Center を使用する必要があります。Management Center は、トラフィックとイベントの強力な分析とモニタリングも提供します。

（注） CDO 管理対象デバイスがあり、オンプレミス Management Center を分析のみに使用している場合、オンプレミス Management Center はポリシーの設定またはアップグレードをサポートしません。このガイドの一部の章と手順は、プライマリマネージャが CDO であるデバイスには適用されない可能性があります。

Management Center をプライマリマネージャとして使用する場合：Management Center は独自の Threat Defense 設定があり、Management Center をバイパスして Threat Defense を直接設定できないため、Management Center は他のマネージャと互換性がありません。

クイック スタート：基本設定

Cisco Secure Firewall の機能セットには、基本設定および詳細設定をサポートできるだけの強力さと柔軟性があります。以降に説明する手順に従って、Secure Firewall Management Center とその管理対象デバイスを迅速に設定し、トラフィックの制御と分析を開始することができます。

物理アプライアンスでの初期セットアップのインストールと実行

手順

目的のアプライアンスに対応するドキュメンテーションを使用して、すべての物理アプライアンスで初期セットアップをインストールおよび実行します。

- **Management Center**
  - ハードウェアモデルについては、『Cisco Secure Management Center Getting Started Guide』を参照してください。次のサイトから入手できます。

    『Cisco Secure Firewall Management Center Getting Started Guides』
- **Threat Defense 管理対象デバイス**
  - Cisco Firepower 1010 スタートアップガイド
  - Cisco Firepower 1100 Getting Started Guide
  - Cisco Firepower 2100 Getting Started Guide
  - Cisco Secure Firewall 3100 Getting Started Guide
  - Cisco Firepower 4100 Getting Started Guide
  - Cisco Secure Firewall 4200 スタートアップガイド
  - Cisco Firepower 9300 Getting Started Guide
  - 『Cisco Secure Firewall Threat Defense for the ISA 3000 Using Secure Firewall Management Center Quick Start Guide』 『』

仮想アプライアンスの展開

展開に仮想アプライアンスが含まれている場合は、以下の手順に従います。ドキュメンテーションロードマップを使用して、次のドキュメントを見つけてください：『Navigating the Cisco Secure Firewall Threat Defense Documentation』

手順

ステップ 1 Management Center とデバイスで使用する、サポートされている仮想プラットフォームを決定します（これらは同一とは限りません）。『*Cisco Secure Firewall Compatibility Guide*』『』を参照してください。

ステップ 2 ご使用の環境に応じたドキュメンテーションを使用して、仮想 Cisco Secure Firewall Management Center を展開します。

- VMware で実行されている Management Center Virtual：『*Cisco Secure Firewall Management Center Virtual Getting Started Guide*』
- AWS で実行されている Management Center Virtual：『*Cisco Secure Firewall Management Center Virtual Getting Started Guide*』
- KVM で実行されている Management Center Virtual：『*Cisco Secure Firewall Management Center Virtual Getting Started Guide*』

ステップ 3 ご使用のアプライアンスに応じたドキュメンテーションを使用して、仮想デバイスを展開します。

- VMware で実行されている Threat Defense Virtual：『*Cisco Secure Firewall Threat Defense Virtual for VMware Getting Started Guide*』
- AWS で実行されている Threat Defense Virtual：『*Cisco Secure Firewall Threat Defense Virtual for AWS Getting Started Guide*』
- KVM で実行されている Threat Defense Virtual：『*Cisco Secure Firewall Threat Defense Virtual for KVM Getting Started Guide*』
- Azure で実行されている Threat Defense Virtual：『*Cisco Secure Firewall Threat Defense Virtual for Azure Getting Started Guide*』

最初のログイン

新しいManagement Centerに初めてログインする前に、物理アプライアンスでの初期セットアップのインストールと実行 （2 ページ）または仮想アプライアンスの展開 （3 ページ）の説明に従ってアプライアンスを準備します。

新しい Management Center（または工場出荷時の初期状態に新しく復元された Management Center）に初めてログインするときは、CLI または Web インターフェイスの **admin** アカウントを使用して、お客様の Management Center モデル用の『*Cisco Cisco Secure Firewall Management Center Getting Started Guide*』の手順に従ってください。初期設定プロセスが完了したら、システムの次の側面を設定します。

- 2 つの **admin** アカウント（1 つは Web インターフェイスアクセス用、もう 1 つは CLI アクセス用）のパスワードは、Management Center のユーザーアカウントの注意事項と制約事項（145 ページ）で説明されている強力なパスワード要件に準拠した同じ値に設定されます。システムは、最初の設定プロセス中にのみ 2 つの **admin** アカウントのパスワードを同期します。その後、いずれかの **admin** アカウントのパスワードを変更すると、パスワードは同じではなくなり、Web インターフェイスの **admin** アカウントから強力なパスワード要件を削除できます。（内部ユーザーの追加または編集（147 ページ）を参照）。
- Management Center が管理インターフェイス（eth0）を介したネットワーク通信に使用する次のネットワーク設定は、デフォルト値または指定した値に設定されます。
  - 完全修飾ドメイン名（`<hostname>.<domain>`）
  - IPv4 設定用のブートプロトコル（DHCP またはスタティック/手動）
  - IPv4 アドレス
  - ネットワーク マスク
  - ゲートウェイ
  - DNS サーバー
  - NTP サーバー

  これらの設定値は、Management Center Web インターフェイスを使用して表示および変更できます。詳細については、Management Center 管理インターフェイスの変更（92 ページ）および時刻の同期（120 ページ）を参照してください。
- 初期構成の一環として、システムは週次 GeoDB 更新をスケジュールします。このタスクを確認し、必要に応じ、GeoDB 更新のスケジューリング（269 ページ）。
- 初期構成の一環として、システムは週ごとのダウンロードをスケジュールします。このタスクを確認し、必要に応じ、ソフトウェア ダウンロードの自動化（610 ページ）。

重要 このタスクは、更新のみをダウンロードします。ユーザは、このタスクがダウンロードした更新をインストールする必要があります。

- 初期構成の一環として、システムは（ローカルに保存された）設定のみの週次 Management Center バックアップをスケジュールします。このタスクを確認し、必要に応じ、Management Center のバックアップのスケジュール（600 ページ）。

- 初期構成の一環として、システムは最新のVDBをダウンロードしてインストールします。システムを最新の状態に保つために、「脆弱性データベースの更新の自動化 （613 ページ）。
- 初期構成の一環として、システムは日次の侵入ルール更新をスケジュールします。このタスクを確認し、必要に応じ、侵入ルールの更新のスケジュール （274 ページ）。

Management Centerの初期設定が完了すると、Webインターフェイスには、Cisco Secure Firewall Management Centerデバイス構成ガイドで説明されている[デバイス管理（Device Management）]ページが表示されます

（このページは、**admin**ユーザーが初めてログインしたときにのみ使用されるデフォルトのログイン ページです。**admin** またはユーザーによる以降のログインでは、ホームページの指定（241 ページ）の説明に従ってデフォルトのログイン ページが決定されます）。

初期設定を完了したら、基本ポリシーを設定することで、トラフィックの制御と分析を開始します。詳細については、基本ポリシーの設定 （5 ページ）を参照してください。

基本ポリシーの設定

ダッシュボード、コンテキストエクスプローラ、およびイベントテーブルにデータを表示するには、基本ポリシーを設定し、展開する必要があります。

（注） これはポリシーや機能に関する完全な説明ではありません。その他の機能とより高度な設定については、このガイドの他のセクションを参照してください。

始める前に

Web インターフェイスまたは CLI の **admin** アカウントを使用して Web インターフェイスにログインし、ご使用のハードウェアモデル用の『*Cisco Cisco Secure Firewall Management Center Getting Started Guide*』（[インストールおよびアップグレードガイド（Install and Upgrade Guides）]https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-guides-list.htmlから取得できます）の説明に従って初期設定を行います。

手順

ステップ 1 このアカウントのタイムゾーンを設定します。詳細については、「デフォルト タイム ゾーンの設定 （247 ページ）」を参照してください。

ステップ 2 必要に応じて、ライセンス （301 ページ）の説明に従ってライセンスを追加します。

ステップ 3 Cisco Secure Firewall Management Center デバイス構成ガイドの「*Add a Device to the Management Center*」の説明に従って、管理対象デバイスを展開に追加します。

ステップ 4 管理対象デバイスを設定します。手順については、次を参照してください。

- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Interface Overview*」：Threat Defense デバイスでトランスペアレントモードまたはルーテッドモードを設定する場合。
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Interface Overview*」：Threat Defense デバイスのインターフェイスを設定する場合。

ステップ 5 Cisco Secure Firewall Management Center デバイス構成ガイドの「*Creating a Basic Access Control Policy*」の説明に従って、アクセス コントロール ポリシーを設定します。

- ほとんどの場合、デフォルトのアクションとして、**セキュリティと接続のバランスの取れた**侵入ポリシーを設定することが提案されます。詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの「*Access Control Policy Default Action*」および「*System-Provided Network Analysis and Intrusion Policies*」を参照してください。
- ほとんどの場合、組織のセキュリティとコンプライアンスのニーズを満たすために接続のロギングを有効にすることが提案されます。表示を整理したり、システムに負担をかけないために、ログに記録する接続を決定する際はネットワークのトラフィックを考慮してください。詳細については、「接続ロギングについて （879ページ）」を参照してください。

ステップ 6 「正常性ポリシーの適用 （451ページ）」の説明に従って、システムが提供するデフォルトの正常性ポリシーを適用します。

ステップ 7 いくつかのシステム設定をカスタマイズします。

- サービス（SNMP や syslog など）の受信接続を許可する場合は、「アクセス リストの設定 （49 ページ）」の説明に従ってアクセス リストのポートを変更します。
- 「データベース イベント数の制限の設定 （66 ページ）」の説明に従って、データベースイベント制限の編集について理解し、検討します。
- 表示言語を変更する場合は、「Web インターフェイスの言語の設定 （83 ページ）」の説明に従って言語設定を編集します。
- 組織がプロキシサーバーを使用してネットワークアクセスを制限している場合は、Management Center 管理インターフェイスの変更 （92 ページ）の説明に従ってプロキシ設定を編集します。

ステップ 8 Cisco Secure Firewall Management Center デバイス構成ガイドの「*Configuring the Network Discovery Policy*」の説明に従って、ネットワーク検出ポリシーをカスタマイズします。デフォルトでは、ネットワーク検出ポリシーは、ネットワークのすべてのトラフィックを分析します。ほとんどの場合、RFC 1918 のアドレスに検出を制限することが提案されます。

ステップ 9 次の他の一般的な設定のカスタマイズを検討します。

- システム変数のデフォルト値をカスタマイズする場合は、Cisco Secure Firewall Management Center デバイス構成ガイドの「*Variable Sets*」の説明に従ってそれらの用途を理解します。
- Management Center にアクセスする追加のローカル認証ユーザーアカウントを作成する場合は、内部ユーザーの追加または編集 （147 ページ）を参照してください。

- LDAP または RADIUS 外部認証を使用して Management Center へのアクセスを許可する場合は、Management Center の外部認証の設定 （150 ページ）を参照してください。

ステップ 10 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

次のタスク

「機能 （8 ページ）」およびこのガイドの他のセクションに記載されているその他の機能の設定について確認し、検討してください。

最新バージョンのデバイスでサポートされていない画面

Management Center は、以前のバージョン（Cisco Secure Firewall Threat Defense 互換性ガイド で入手可能な互換性マトリックスで指定されています）を実行しているデバイスを管理できますが、このガイドには、最新バージョンのデバイスソフトウェアでサポートされている機能のみが含まれています。

古いバージョンのデバイスでのみサポートされている機能については、ご使用のバージョンに一致するガイドを参照してください。

Threat Defense デバイス

一般的な展開では、複数のトラフィック処理デバイスが、アドミニストレーション、管理、分析、および報告タスクの実行に使用される 1 つの Secure Firewall Management Center に報告します。

Threat Defense デバイスは、NGIPS 機能も備えた次世代ファイアウォール（NGFW）です。NGFW およびプラットフォーム機能には、サイト間およびリモートアクセス VPN、堅牢なルーティング、NAT、クラスタリング、およびアプリケーション インスペクションとアクセス制御におけるその他の最適化が含まれています。

Threat Defense は、幅広い物理プラットフォームおよび仮想プラットフォームで使用できます。

互換性

特定のデバイスモデル、仮想ホスティング環境、オペレーティングシステムなどと互換性のあるソフトウェアを含むマネージャとデバイスの互換性の詳細については、Cisco Secure Firewall Threat Defense リリースノート、Cisco Secure Firewall Management Center 互換性ガイド、および Cisco Secure Firewall Threat Defense 互換性ガイドを参照してください。

機能

次の表には、一般的に使用されるいくつかの機能が一覧表示されています。

アプライアンスおよびシステム管理の機能

ドキュメントを検索するには、Cisco Secure Firewall Threat Defense ドキュメントにアクセスを参照してください。

目的	設定	参照先
Cisco Secure Firewall デバイスへのログイン用のユーザーアカウントを管理する	デバイス認証	Management Centerユーザー（139 ページ）およびCisco Secure Firewall Management Center デバイス構成ガイドの「*Users for Devices*」
システム ハードウェアとシステム ソフトウェアの状況をモニターする	ヘルス モニタリング ポリシー	ヘルス モニタリングについて （431 ページ）
アプライアンスのデータをバックアップする	バックアップと復元	バックアップ/復元 （555 ページ）
新しいバージョンにアップグレードする	システムの更新プログラム	Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド Cisco Secure Firewall Threat Defense リリースノート
物理アプライアンスを基準に合わせる	工場出荷時の初期状態に復元（再イメージ化）する	Cisco FXOS トラブルシューティング ガイド（Threat Defense を実行している Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 向け）
VDB を更新する、侵入ルールを更新する、またはアプライアンスの GeoDB を更新する	脆弱性データベース（VDB）の更新、侵入ルールの更新、地理位置情報データベース（GeoDB）の更新	更新 （263 ページ）
ライセンス制御機能を利用するためにライセンスを適用する	スマートライセンシング	ライセンスについて （301 ページ）

目的	設定	参照先
アプライアンスの動作の継続性を確保する	管理対象デバイスの高可用性またはManagement Centerの高可用性（あるいはその両方）	Cisco Secure Firewall Management Centerデバイス構成ガイドの「*About Cisco Secure Firewall Threat Defense "High Availability chapter"*」 Management Centerのハイアベイラビリティについて（361ページ）
複数のインターフェイス間のトラフィックをルーティングするようにデバイスを設定する	ルーティング	Cisco Secure Firewall Management Centerデバイス構成ガイドの「*Reference for Routing*」
複数のネットワーク間のパケットスイッチングを設定する	デバイス スイッチング	Cisco Secure Firewall Management Centerデバイス構成ガイドの「*Configure Bridge Group Interfaces*」
インターネット接続のプライベートアドレスをパブリック アドレスに変換する	ネットワーク アドレス変換（NAT）	Cisco Secure Firewall Management Centerデバイス構成ガイドの「*Network Address Translation*」
管理対象のThreat Defenseデバイス間のセキュアなトンネルを確立する	サイト間バーチャル プライベート ネットワーク（VPN）	Cisco Secure Firewall Management Centerデバイス構成ガイドの「*VPN Overview*」
リモートユーザーと管理対象Threat Defenseデバイス間のセキュアなトンネルを確立する	リモート アクセス VPN	Cisco Secure Firewall Management Centerデバイス構成ガイドの「*VPN Overview*」
管理対象デバイス、設定、およびイベントへのユーザ アクセスをセグメント化する	ドメインを使用したマルチテナンシー	ドメインを使用したマルチテナンシーの概要（251ページ）
REST APIクライアントを使用してアプライアンスの設定を表示および管理する	REST APIおよびREST API エクスプローラ	REST API設定（103ページ） 『*Cisco Secure Firewall Mangement Center REST API Quick Start Guide*』
問題のトラブルシューティング	該当なし	トラブルシューティング（521ページ）

潜在的な脅威を検出、防御、および処理するための機能

ドキュメントを検索するには、Cisco Secure Firewall Threat Defense ドキュメントにアクセスを参照してください。

目的	設定	参照先
ネットワーク トラフィックのインスペクション、記録、およびアクションを実行する	アクセス コントロール ポリシー、他のいくつかのポリシーの親	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Introduction to Access Control*」
IP アドレス、URL、またはドメイン名との間の接続をブロックまたはモニターする	アクセス コントロール ポリシー内のセキュリティ インテリジェンス	Cisco Secure Firewall Management Center デバイス構成ガイドの「*About Security Intelligence*」
ネットワークのユーザがアクセスできる Web サイトを制御する	ポリシー ルール内の URL フィルタリング	Cisco Secure Firewall Management Center デバイス構成ガイドの「*URL Filtering*」
ネットワーク上の悪意のあるトラフィックと侵入をモニタする	侵入ポリシー	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Intrusion Policy Basics*」
インスペクションを実行せずに、暗号化されたトラフィックをブロックする 暗号化または複合されたトラフィックのインスペクション	SSL ポリシー	Cisco Secure Firewall Management Center デバイス構成ガイドの「*SSL Policies Overview*」
ディープ インスペクションをカプセル化トラフィックに合わせて調整し、高速パス処理でのパフォーマンスを向上させる	プレフィルタ ポリシー	Cisco Secure Firewall Management Center デバイス構成ガイドの「*About Prefiltering*」
アクセス コントロールによって許可または信頼されたネットワーク トラフィックのレート制限	サービス品質（QoS）ポリシー	Cisco Secure Firewall Management Center デバイス構成ガイドの「*About QoS Policies*」
ネットワーク上のファイル（マルウェアを含む）を許可またはブロックする	ファイル/マルウェア ポリシー	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Network Malware Protection and File Policies*」

目的	設定	参照先
脅威インテリジェンス ソースからデータを運用可能にします。	Cisco Threat Intelligence Director（TID）	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Secure Firewall Threat Intelligence Director Overview*」
ユーザーの認知およびユーザー制御を実行するためにパッシブまたはアクティブなユーザー認証を設定する	ユーザ認識、ユーザ アイデンティティ、アイデンティティ ポリシー	Cisco Secure Firewall Management Center デバイス構成ガイドの「*About User Identity Sources*」 Cisco Secure Firewall Management Center デバイス構成ガイドの「*About Identity Policies*」
ユーザー認識を実行するために、ネットワークのトラフィックからホスト、アプリケーション、およびユーザー データを収集する	ネットワーク検出ポリシー	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Network Discovery Policies*」
デバイス外のツールを使用してネットワークトラフィックと潜在的な脅威に関するデータを収集して分析する	外部ツールとの統合	外部ツールを使用したイベントの分析 （753 ページ）
アプリケーション検出およびコントロールを実行する	アプリケーション ディテクタ	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Application Detection*」
問題のトラブルシューティング	該当なし	トラブルシューティング （521 ページ）

外部ツールとの統合

ドキュメントを検索するには、Cisco Secure Firewall Threat Defense ドキュメントにアクセスを参照してください。

目的	設定	参照先
ネットワークの条件が、関連付けられたポリシーに違反した場合、自動的に修復を起動する	修復	修復の概要 （1249 ページ） 『*Firepower System Remediation API Guide*』

目的	設定	参照先
Management Center からカスタム開発されたクライアント アプリケーションにイベントデータをストリームする	eStreamer 統合	eStreamer サーバー ストリーミング （785 ページ） 『*Cisco Secure Firewall Mangement Center Event Streamer Integration Guide*』
サードパーティクライアントを使用して Management Center のデータベーステーブルを照会する	外部データベース アクセス	外部データベース アクセス （70 ページ） 『*Cisco Secure Firewall Mangement Center Database Access Guide*』
サードパーティ ソースからデータをインポートすることによって検出データを増やす	ホスト入力	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Host Input Data*」 『*Firepower System Host Input API Guide*』
外部イベント データ ストレージ ツールその他のデータ リソースを使用してイベントを調査します。	外部イベント分析ツールとの統合	外部ツールを使用したイベントの分析 （753 ページ）
問題のトラブルシューティング	該当なし	トラブルシューティング （521 ページ）

Management Center を検索します。

グローバル検索機能を使用して、Secure Firewall Management Center 設定の要素をすばやく見つけて移動することができます。

（注） この機能は、ライトテーマと Dusk テーマでのみサポートされています。テーマを変更するには、Web インターフェイス表示の変更 （240 ページ）を参照してください。

次のエンティティの Management Center 設定を検索できます。

- トップレベルメニューの Web インターフェイスページの名前。（Web インターフェイス メニューのオプションの検索 （16 ページ） を参照。）
- 特定のポリシータイプについて：
  - ポリシー名

- ポリシーの説明
- ルール名
- ルールのコメント

（ポリシーの検索 （17 ページ） を参照。）

- 特定のオブジェクトタイプについて：
  - オブジェクト名
  - オブジェクトの説明
  - 設定値

（オブジェクトの検索 （19 ページ）を参照）。

- How To ウォークスルー。

  検索すると、検索語を含むウォークスルーのリストと、各ウォークスルーへのリンクが返されます。（How To ウォークスルーの検索 （24 ページ） を参照。）

グローバル検索を使用するときは、次のことに注意してください。

- グローバル検索ツールを開くと、検索テキストボックスの下の履歴リストに、最近の 10 件の検索が表示されます。このリストから項目を選択して、検索を再実行できます。
- 検索式を入力すると、インターフェイスの検索履歴が検索結果に置き換わり、検索を入力するにつれて更新されます。検索を実行するために Enter キーを押す必要はありません。
- マウスまたはキーボードの矢印キーと Enter キーを使用して、履歴リストまたは検索結果を移動できます。Enter キーを押すと、検索結果で現在強調表示されている項目が選択されます。Web インターフェイスページの結果の場合は、強調表示されたページが Management Center インターフェイスに表示されます。オブジェクトとポリシーの場合は、見つかったエンティティに関する詳細が表示されます。
- 検索では大文字と小文字が区別されません。
- 検索では、次のワイルドカード文字を使用できます。
  - ? は、任意の単一文字と一致します。
  - * は、0 文字以上の任意の文字と一致します。
  - ^ は、前にある検索用語を一致するエンティティの先頭に固定します。
  - $ は、後ろにある検索用語を一致するエンティティの末尾に固定します

  ワイルドカードはエスケープできません。
- 効率を高めるために、グローバル検索では間接的な検索結果は返されません。つまり、検索用語が見つかったオブジェクトを参照するポリシーやオブジェクトは返されません。ただし、検索の詳細ペインで見つかったオブジェクトの [使用状況（Usages）] タブを表示す

ることで、多くの見つかったオブジェクトを参照しているポリシーまたはオブジェクトを判断することができます。

- グローバル検索では、Management Center で最も一般的に使用される設定エンティティとの関連性によって決定される、検索式の上位の結果が返されます。グローバル検索で期待していた結果が返されなかった場合は、検索を絞り込むか、多くの GUI ページの上部に表示される検索ツールまたはフィルタツールを使用するか、Web インターフェイスによって提供されている設定固有の検索機能を試してみてください。
  - Cisco Secure Firewall Management Center デバイス構成ガイド のルールの検索
  - Cisco Secure Firewall Management Center デバイス構成ガイド の *NAT* ルールテーブルの検索とフィルタリング
  - イベント検索
  - カスタム テーブルの検索

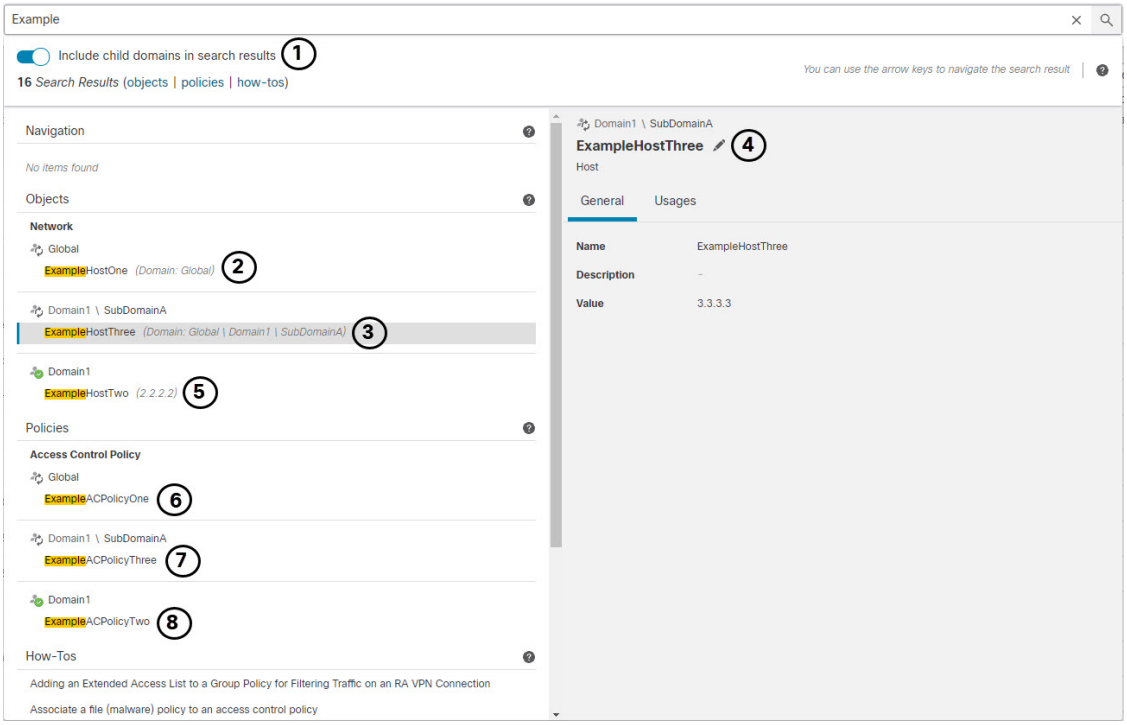
マルチドメイン展開でのグローバル検索

マルチドメイン展開の検索では、現在のドメインとその先祖ドメイン内で定義されているオブジェクトとポリシーのみがデフォルトで返されます。検索結果ダイアログのオプションを切り替えることで、子ドメインのオブジェクトとポリシーを表示できます。

オブジェクト検索では、現在のドメイン以外のドメインで定義されたオブジェクトで検索式が見つかった場合、検索結果には、それらのオブジェクトが存在するドメインの名前が表示されます。現在のドメイン内で定義されたオブジェクトで検索式が見つかった場合、検索結果にはオブジェクトの値が表示されます。

次のスクリーンショットの例では、展開は、Global、Domain1、および SubDomainA の 3 つのレベルのドメインで構成されています。現在のドメインが Domain1 であるユーザーが、先祖ドメインと子ドメインの両方で文字列「example」の検索を入力しました。

図 *1*:マルチドメイン環境でのグローバル検索の例



1	ユーザーは、子ドメイン（SubDomainA）、現在のドメイン（Domain1）、およびその先祖（Global）を検索することを選択しました。	2	親ドメイン Global で定義された一致するネットワークオブジェクト ExampleHostOne がドメイン名とともに表示されます。[外部ドメイン（External Domain）]（） アイコンは、詳細を編集するためにはドメインを切り替える必要があることを示しています。
3	子ドメイン SubDomainA で定義された一致するネットワークオブジェクト ExampleHostThree がドメイン名とともに表示されます。[外部ドメイン（External Domain）]（） アイコンは、詳細を編集するためにはドメインを切り替える必要があることを示しています。このオブジェクトは現在選択されています。	4	一致するネットワークオブジェクト ExampleHostThree が現在選択されており、右側のペインに情報が表示されています。[外部ドメイン（External Domain）]（） アイコンは、**[編集（Edit）]**（） をクリックしたときに、オブジェクトへの編集アクセスを許可する前にドメインの変更を確認するためのユーザープロンプトが表示されることを示しています。

5	現在のドメインで定義されている一致するネットワークオブジェクト ExampleHostTwo がオブジェクト値とともに表示されます。[現在のドメイン（Current Domain）]（）アイコンは、ドメインを切り替えずにこのオブジェクトを編集できることを示しています。	6	親ドメイン Global で定義された一致するアクセス コントロール ポリシー ExampleACPolicyOne がドメイン名とともに表示されます。[外部ドメイン（External Domain）]（）アイコンは、詳細を編集するためにドメインを切り替える必要があることを示しています。
7	子ドメイン SubDomainA で定義された一致するアクセス コントロール ポリシー ExampleACPolicyThree がドメイン名とともに表示されます。[外部ドメイン（External Domain）]（）アイコンは、詳細を編集するためにドメインを切り替える必要があることを示しています。	8	現在のドメインで定義されている一致するアクセス コントロール ポリシー ExampleACPolicyTwo が [現在のドメイン（Current Domain）]（）アイコンとともに表示されます。このアイコンは、ドメインを切り替えずに詳細を編集できることを示しています。

Web インターフェイスメニューのオプションの検索

Web インターフェイスのトップレベルメニューで、ページの場所を検索して見つけることができます。たとえば、Quality of Service の設定を表示または構成するには、**QoS** を検索します。

始める前に

この機能は、クラシックテーマでは使用できません。テーマを変更するには、Web インターフェイス表示の変更 （240 ページ）を参照してください。

手順

ステップ 1 検索を開始するには、次の 2 つの方法のいずれかを使用します。

- Management Center Web インターフェイスの上部にあるメニューバーで、 をクリックします。
- テキストボックスの外側にフォーカスを置いて、/（スラッシュ）を入力します。

ステップ 2 探しているメニューオプションの名前を 1 文字以上入力します。検索結果がテキストボックスの下に表示され、入力すると更新されます。検索を実行するために Enter キーを押す必要はありません。

ステップ 3 検索結果はカテゴリ別にグループ化されて表示されます。[ナビゲーション（Navigation）] の下に表示されたページに移動するには、検索結果リストのメニューパスをクリックします。

ポリシーの検索

次の表は、名前で検索できるポリシータイプを示しています。

範囲内	範囲外
アクセス コントロール ポリシー（Access Control Policy）	Threat Defense プラットフォーム設定
プレフィルタポリシー（Prefilter Policy）	Firepower 設定ポリシー
Threat Defense NAT ポリシー	Firepower NAT ポリシー
侵入カテゴリ • 侵入ポリシー（Intrusion Policy） • ネットワーク分析ポリシー（Network Analysis Policy）	QoS ポリシー（QoS Policy） FlexConfig ポリシー（FlexConfig Policy） DNS ポリシー マルウェア & ファイル ポリシー SSL ポリシー（SSL Policy） ID ポリシー ネットワーク検出（Network Discovery） アプリケーションディテクタ 相関ポリシー VPN カテゴリ • ダイナミック アクセス ポリシー • サイト間 • リモートアクセス

グローバル検索では、名前が検索語句に一致するポリシーと、名前またはコメントが検索語句に一致するルールが使用されているアクセス コントロール ポリシーが返されます。名前が検索内容に一致しないアクセス コントロール ポリシーが検索結果リストに表示された場合は、ポリシー内で設定されているルールの名前またはコメントが一致しています。

重要 グローバル検索では、Management Center で最も一般的に使用される設定エンティティとの関連性によって決定される、検索式の上位の結果が返されます。この検索機能の範囲外のポリシータイプに検索語句が含まれている可能性があります。グローバル検索機能と代替検索方法の詳細については、「Management Center を検索します。」を参照してください。

始める前に

この機能は、クラシックテーマでは使用できません。テーマを変更するには、Web インターフェイス表示の変更 （240 ページ）を参照してください。

手順

ステップ 1 検索を開始するには、次の 2 つの方法のいずれかを使用します。

- Management Center Web インターフェイスの上部にあるメニューバーで、 をクリックします。
- テキストボックスの外側にフォーカスを置いて、/（スラッシュ）を入力します。

ステップ 2 検索テキストボックスに検索式を入力します。検索結果がテキストボックスの下に表示され、入力すると更新されます。検索を実行するために Enter キーを押す必要はありません。

ステップ 3 （オプション）マルチドメイン展開では、現在のドメインに子孫ドメインがある場合、[検索結果に子ドメインを含める（Include child domains in search results）] を切り替えて、子孫ドメイン内のポリシーを表示できます。

ステップ 4 検索結果はカテゴリ別にグループ化されて表示されます。マルチドメイン展開では、[ポリシー（Policies）] カテゴリ内で、検出されたポリシーが定義されているドメインによって検索結果がグループ化されます。[ポリシー（Policies）] カテゴリでは、次のことができます。

方法：	操作手順
単一ポリシータイプの検索結果を表示します。	検索結果で、アクセスコントロールポリシーなどのポリシータイプをクリックします。
ポリシーに関する詳細を表示します。	検索結果リストのポリシー名をクリックして詳細ペインを表示し、[全般（General）] タブを表示します。
侵入ポリシーとネットワーク分析ポリシーを参照するアクセスコントロールポリシーを表示します。	検索結果の侵入ポリシーまたはネットワーク分析ポリシーの名前をクリックして詳細ペインを表示し、[使用状況（Usages）] タブを表示します。

方法：	操作手順
別のブラウザウィンドウでポリシーのポリシー設定ページを開きます。	検索結果でポリシー名をクリックし、詳細ペインで [編集（Edit）]（  ）をクリックします。 マルチドメイン展開では、現在のドメイン内で定義されていないポリシーを編集することを選択すると、現在のドメインの変更を求められます。

オブジェクトの検索

次の表は、[オブジェクト管理（Object Management）]ページ（**[オブジェクト（Objects）]**>**[オブジェクト管理（Object Management）]**）に一覧表示されるオブジェクトタイプのうち、グローバル検索機能の範囲内にあるものを示しています。

範囲内	範囲外
AAA サーバーカテゴリ • RADIUS サーバグループ • シングルサインオンサーバー アクセスリストカテゴリ • 拡張アクセス リスト • 標準アクセス リスト アドレスプールカテゴリ • IPv4 プール • IPv6 プール AS パス（AS Path） コミュニティリストカテゴリ • Extended Community DNS サーバ グループ 外部属性カテゴリ • ダイナミックオブジェクト • セキュリティ グループ タグ（Security Group Tag） 位置情報 インターフェイスカテゴリ • セキュリティ ゾーン • インターフェイス グループ	アプリケーション フィルタ 暗号スイート リスト コミュニティリストカテゴリ • コミュニティ（Community） 識別名カテゴリ • 個々の識別名オブジェクト • 識別名オブジェクトグループ ファイル リスト FlexConfig カテゴリ • FlexConfig オブジェクト • テキストオブジェクト PKI カテゴリ • 外部証明書グループ（External Cert Groups） • 外部証明書 • 内部 CA グループ（Internal CA Groups） • 内部 CA • 内部証明書グループ（Internal Cert Groups） • 内部証明書 • 信頼できる CA グループ（Trusted CA Groups） • 信頼できる CA

範囲内	範囲外
キーチェーン ネットワーク（ネットワーク、ホスト、範囲、FQDN、ネットワークグループを含む） PKI カテゴリ 証明書の登録 ポリシー リスト ポート（オブジェクトとグループ、TCP、UDP、ICMP、ICMP6、その他） プレフィックス リスト カテゴリ • IPv4 プレフィックス リスト • IPv6 プレフィックス リスト ルート マップ SLA モニタ 時間範囲 タイム ゾーン トンネル ゾーン URL（オブジェクト、グループ） VLAN タグ（オブジェクト、グループ） VPN カテゴリ • 証明書マップ • [グループ ポリシー（Group Policy）] • IKEv1 IPSec プロポーザル • IKEv1 ポリシー • IKEv2 IPSec プロポーザル • IKEv2 ポリシー	セキュリティ インテリジェンス カテゴリ • DNS リストとフィード • ネットワークリストとフィード • [URLのリストとフィード（URL Lists and Feeds）] シンクホール 変数セット VPN カテゴリ • Secure Client ファイル • カスタム属性

グローバル検索では、名前または説明が検索用語に一致するオブジェクトと、検索用語に一致する構成値を持つオブジェクトが返されます。名前が検索内容に一致しないオブジェクトが検索結果リストに表示された場合は、オブジェクト内の説明または構成値が一致しています。

重要 グローバル検索では、Management Center で最も一般的に使用される設定エンティティとの関連性によって決定される、検索式の上位の結果が返されます。この検索機能の範囲外のオブジェクトタイプに検索用語が含まれている可能性があります。グローバル検索機能と代替検索方法の詳細については、「Management Center を検索します。」を参照してください。

オブジェクト検索は、展開内のネットワーク情報を見つける必要がある場合に特に役立ちます。オブジェクト名、説明、または構成値で次のものを検索できます。

- 次の形式を含む、IPv4 および IPv6 アドレス情報。
  - 完全なアドレス（たとえば、`194.164.0.23`、`2001:0db8:85a3:0000:0000:8a2e:0370:7334`）。
  - 部分的なアドレス（たとえば、`194.164`、`2001:db8`）。
  - 範囲（たとえば、`192.164.1.1-192.168.1.5`、`2001:db8::0202-2001:db8::8329`。ハイフンの前後にスペースを入力しないでください。）グローバル検索は、指定された範囲内のいずれかに一致するネットワークアドレスを使用してオブジェクトを返します。
  - CIDR 表記。（たとえば、`192.168.1.0/24`、`2002::1234:abcd:ffff:101/64`。）グローバル検索は、指定された CIDR ブロック内のいずれかに一致するネットワークアドレスを使用してオブジェクトを返します。
- ポート情報：
  - ポート番号（たとえば、`22` または `80`）。
  - プロトコル。（たとえば、`https` または `ssh`。）
- 完全修飾ドメイン名。（たとえば、`www.cisco.com`）
- URL。（たとえば、`http://www.cisco.com`）
- 暗号化標準規格またはハッシュタイプ（たとえば、`AES-128` または `SHA`）。
- VLAN タグ番号（たとえば、`568`）。

始める前に

この機能は、クラシックテーマでは使用できません。テーマを変更するには、Web インターフェイス表示の変更 （240 ページ）を参照してください。

手順

ステップ 1 検索を開始するには、次の 2 つの方法のいずれかを使用します。

- Management Center Web インターフェイスの上部にあるメニューバーで、 をクリックします。
- テキストボックスの外側にフォーカスを置いて、/（スラッシュ）を入力します。

ステップ 2 検索テキストボックスに検索式を入力します。検索結果がテキストボックスの下に表示され、入力すると更新されます。検索を実行するために Enter キーを押す必要はありません。

現在のデフォルトドメイン以外のドメインで定義されたオブジェクトで検索式が見つかった場合、検索結果には、それらのオブジェクトが存在するドメインの名前が表示されます。現在のドメイン内で定義されたオブジェクトで検索式が見つかった場合、検索結果にはオブジェクトの値が表示されます。

ステップ 3 （オプション）マルチドメイン展開では、現在のドメインに子孫ドメインがある場合、[検索結果に子ドメインを含める（Include child domains in search results）] を切り替えて、子孫ドメイン内のオブジェクトを表示できます。

ステップ 4 検索結果はカテゴリ別に分けて表示されます。マルチドメイン展開では、[オブジェクト（Objects）] カテゴリ内で、検出されたオブジェクトが定義されているドメインによって検索結果がグループ化されます。[オブジェクト（Objects）] カテゴリでは、次のことができます。

方法：	操作手順
単一オブジェクトタイプの検索結果を表示します。	検索結果で、[ネットワーク（Network）] などのオブジェクトタイプをクリックします。
検索結果のオブジェクトに関する詳細を表示します。	検索結果のオブジェクト名をクリックして詳細ペインを表示し、[全般（General）] タブを表示します。
検索結果のオブジェクトを使用するポリシーまたはオブジェクトのリストを表示します。	検索結果のオブジェクト名をクリックして詳細ペインを表示し、[使用状況（Usages）] タブを表示します。 （注） グローバル検索では、すべてのオブジェクトタイプの使用情報を得られるわけではありません。

方法：	操作手順
オブジェクトのオブジェクト設定ページを別のブラウザウィンドウで開きます。	検索結果でオブジェクト名をクリックし、詳細ペインで[編集（Edit）]（✎）をクリックします。 マルチドメイン展開では、現在のドメイン内で定義されていないオブジェクトを編集することを選択すると、現在のドメインの変更を求められます。

How To ウォークスルーの検索

関心のあるタスクに対処する How To ウォークスルーを検索できます。たとえば、デバイスのセットアップ手順が説明されているウォークスルーを検索するには、「device」という用語を検索します。

始める前に

この機能は、クラシックテーマでは使用できません。テーマを変更するには、Web インターフェイス表示の変更 （240 ページ）を参照してください。

手順

ステップ 1 検索を開始するには、次の 2 つの方法のいずれかを使用します。

- Management Center Web インターフェイスの上部にあるメニューバーで、 をクリックします。
- テキストボックスの外側にフォーカスを置いて、/（スラッシュ）を入力します。

ステップ 2 ウォークスルーを表示するタスクに関連付けられた検索用語を入力します。検索結果がテキストボックスの下に表示され、入力すると更新されます。検索を実行するために Enter キーを押す必要はありません。

ステップ 3 検索結果はカテゴリ別にグループ化されて表示されます。[How-Tos]にリストされているウォークスルーを表示するには、検索結果リストでウォークスルーのタイトルをクリックします。How To ウォークスルーの詳細については、オンラインヘルプ、How To、およびドキュメント（28 ページ）を参照してください。

Secure Firewall Management Center のドメインの切り替え

マルチドメイン導入環境では、ユーザー ロール権限によって、ユーザーがアクセスできるドメインと、そのドメイン内でのユーザーの権限が決まります。単一のユーザアカウントを複数のドメインに関連付けて、各ドメインでそのユーザに異なる権限を割り当てることができます。たとえば、あるユーザにグローバル ドメインでは読み取り専用権限を割り当て、子孫ドメインでは管理者権限を割り当てることができます。

複数のドメインに関連付けられているユーザは、同じ Web インターフェイス セッション内でドメインを切り替えることができます。

ツールバーのユーザ名の下に、利用可能なドメインのツリーが表示されます。ツリーの表示は次のようになります。

- 先祖ドメインは表示されますが、使用しているユーザアカウントに割り当てられた権限に応じて、先祖ドメインへのアクセスが無効である場合があります。
- 兄弟ドメインや子孫ドメインを含め、使用しているユーザアカウントでアクセスできない他のドメインは非表示になります。

ドメインを切り替えると、以下の項目が表示されます。

- そのドメインのみに関連するデータ。
- そのドメインで割り当てられたユーザ ロールに応じて定められたメニュー オプション。

手順

アクセスするドメインは、ユーザー名の下にあるドロップダウン リストから選択します。

コンテキスト メニュー

Webインターフェイスの特定のページでは、右クリック（最も一般的）および左クリックでコンテキストメニューを表示できます。コンテキストメニューは、他の機能にアクセスするためのショートカットとして使用できます。コンテキストメニューの内容はどこでこのメニューにアクセスするか（どのページかだけでなく特定のデータにアクセスしているか）によって異なります。

次に例を示します。

- IPアドレスのホットスポットでは、そのアドレスに関連付けられているホストに関する情報（使用可能な whois とホスト プロファイル情報を含む）が表示されます。

- SHA-256 ハッシュ値のホットスポットでは、ファイルの SHA-256 ハッシュ値をクリーンリストまたはカスタム検出リストに追加したり、コピーするためにハッシュ値全体を表示したりできます。

コンテキストメニューをサポートしていないページや場所では、ブラウザの通常のコンテキストメニューが表示されます。

ポリシー エディタ

多くのポリシーエディタには、各ルールのホットスポットが含まれています。新しいルールとカテゴリの挿入、ルールの切り取り、コピー、貼り付け、ルール状態の設定、ルールの編集などを行うことができます。

侵入ルール エディタ

侵入ルールエディタには、各侵入ルールのホットスポットが含まれています。ルールの編集、ルール状態の設定、しきい値および抑止オプションの設定、ルールのドキュメンテーションの表示などを行うことができます。必要に応じて、コンテキストメニューで、**ルールのドキュメント**をクリックした後、具体的なルールの詳細を表示するドキュメントのポップアップ ウィンドウで、**ルールのドキュメント**をクリックすることができます。

イベント ビューア

イベントページ（[分析（Analysis）]ページにあるドリルダウンページとテーブル ビュー）には、各イベント、IP アドレス、URL、DNS クエリ、特定のファイルの SHA-256 ハッシュ値のホットスポットが含まれています。ほとんどのイベント タイプでは、表示中に以下の操作を行うことができます。

- Context Explorer で関連情報を表示する。
- 新しいウィンドウでイベント情報をドリルダウンする。
- イベント フィールドに含まれているテキスト（ファイルの SHA-256 ハッシュ値、脆弱性の説明、URL など）が長すぎてイベント ビューですべて表示できない場合、テキスト全体を表示する。
- コンテキストクロス起動機能を使用し、外部ソースからのエレメントに関する情報が表示されている Web ブラウザウィンドウを開きます。詳細については、「Web ベースのリソースを使用したイベントの調査 （763 ページ）」を参照してください。

接続イベントの表示中は、デフォルトのセキュリティインテリジェンスのブロックリストとブロックしないリストに以下の項目を追加できます。

- IP アドレスのホットスポットの場合、IP アドレス。
- URL のホットスポットの場合、URL またはドメイン名。
- DNS クエリのホットスポットの場合、DNS クエリ。

キャプチャ ファイル、ファイル イベント、マルウェア イベントの表示中は、以下の操作を行うことができます。

- クリーン リストまたはカスタム検出リストのファイルを追加または削除する。

- ファイルのコピーをダウンロードする。
- アーカイブ ファイル内のネストされたファイルを表示する。
- ネストされたファイルの親アーカイブ ファイルをダウンロードする。
- ファイルの構成を表示する。
- ローカル マルウェア分析およびダイナミック分析対象のファイルを送信する。

侵入イベントの表示中は、侵入ルールエディタまたは侵入ポリシーで実行できるようなタスクを行うことができます。

- トリガー ルールを編集する。
- ルールの無効化を含め、ルールの状態を設定する。
- しきい値および抑止オプションを設定する。
- ルールのドキュメンテーションを表示する。必要に応じて、コンテキスト メニューの [ルール ドキュメント（Rule documentation）] をクリックした後、ドキュメント ポップアップ ウィンドウの [ルール ドキュメント（Rule Documentation）] をクリックするとより具体的なルールの詳細情報を表示できます。

侵入イベントのパケット ビュー

侵入イベントのパケット ビューには、IP アドレスのホットスポットが含まれています。パケット ビューでは、左クリックによるコンテキスト メニューを使用します。

ダッシュボード

多くのダッシュボード ウィジェットには、関連する情報を Context Explorer で表示するためのホットスポットが含まれています。ダッシュボード ウィジェットには、IP アドレスと SHA-256 ハッシュ値のホットスポットが含まれる場合もあります。

Context Explorer

Context Explorer には、図、表、グラフのホットスポットが含まれています。Context Explorer よりも詳細なグラフまたはリストのデータを調べたい場合は、関連するデータのテーブル ビューにドリルダウンすることができます。また、関連するホスト、ユーザ、アプリケーション、ファイル、および侵入ルールの情報を表示できます。

Context Explorer でも左クリックのコンテキスト メニューを使用します。これには、Context Explorer に特有のフィルタリングおよび他のオプションも含まれています。

シスコとのデータの共有

次の機能を使用して、シスコとデータを共有することを選択できます。

- Cisco Success Network

Cisco Success Network の登録設定 （759 ページ）を参照してください

- Web 分析

「Web 分析 （131 ページ）」を参照してください

オンラインヘルプ、How To、 およびドキュメント

オンライン ヘルプには、Web インターフェイスからアクセスできます。

- 各ページで状況依存ヘルプのリンクをクリックする。
- **[ヘルプ（Help）]** > **[ページレベルのヘルプ（Page-level Help）]** を選択する。

How To は、Management Center 上でタスク間を移動するためのウォークスルーを提供するウィジェットです。ウォークスルーでは、タスクを実行するために移動する必要があるかもしれない各種 UI 画面かどうかを問わず、各ステップを順次体験することでタスクを完遂するために必要なステップを実行します。[How To] ウィジェットはデフォルトで有効になっています。ウィジェットを無効にするには、ユーザ名の下にあるドロップダウンリストから [User Preferences] を選択し、[How-To Settings] にある [Enable How-Tos] チェックボックスをオフにします。[How To] ウィジェットを開くには、**[ヘルプ（Help）]** > **[How-Tos]**を選択します。

（注） 通常、ウォークスルーはすべての UI ページで利用でき、ユーザ ロールは区別されていません。ただし、ユーザーの権限によっては Management Center インターフェイスに表示されないメニュー項目もあります。そのため、そのようなページではウォークスルーは実行されません。

Management Center では、次のウォークスルーを利用できます。

Management Center でサポートされている機能ウォークスルーのリストについては、「Feature Walkthroughs Supported in Secure Firewall Management Center」を参照してください。

ドキュメンテーション ロードマップを使用して、その他のドキュメントを検索できます。

Cisco Secure Firewall Threat Defense ドキュメントにアクセス。

cisco.com のユーザーガイド

Secure Firewall Management Center 展開のバージョン 6.0+ を設定するときは、次のドキュメントが役立つ可能性があります。

（注） リンクされたドキュメントの一部は、Secure Firewall Management Center 展開には適用できません。たとえば、Secure Firewall Threat Defense ページの一部のリンクは Secure Firewall Device Manager によって管理される展開に固有の内容で、ハードウェアページの一部のリンクは Management Center とは無関係です。混乱を避けるために、ドキュメントのタイトルには十分に注意してください。また、一部のドキュメントは複数の製品を対象としているため、複数の製品のページに記載されていることがあります。

Secure Firewall Management Center

- Secure Firewall Management Center ハードウェア アプライアンス：

  http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

- Secure Firewall Management Center Virtual アプライアンス：

  - http://www.cisco.com/c/en/us/support/security/defense-center-virtual-appliance/tsd-products-support-series-home.html
  - http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

NGFW（次世代ファイアウォール）デバイスとも呼ばれる Secure Firewall Threat Defense

- Secure Firewall Threat Defense ソフトウェア：

  http://www.cisco.com/c/en/us/support/security/firepower-ngfw/tsd-products-support-series-home.html

- Secure Firewall Threat Defense Virtual：

  http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/tsd-products-support-series-home.html

- FirePOWER 1000 シリーズ：

  https://www.cisco.com/c/en/us/support/security/firepower-1000-series/tsd-products-support-series-home.html

- FirePOWER 2100 シリーズ：

  https://www.cisco.com/c/en/us/support/security/firepower-2100-series/tsd-products-support-series-home.html

- Secure Firewall 3100：

  https://www.cisco.com/c/en/us/support/security/secure-firewall-3100-series/series.html

- FirePOWER 4100 シリーズ：

  https://www.cisco.com/c/en/us/support/security/firepower-4100-series/tsd-products-support-series-home.html

- Secure Firewall 4200：

https://www.cisco.com/c/en/us/support/security/secure-firewall-4200-series/series.html

- FirePOWER 9300：

  https://www.cisco.com/c/en/us/support/security/firepower-9000-series/tsd-products-support-series-home.html

- ISA 3000：

  https://www.cisco.com/c/en/us/support/security/industrial-security-appliance-isa/tsd-products-support-series-home.html

ドキュメンテーションのライセンス ステートメント

項の先頭に記載されているライセンスステートメントは、項で説明される機能を有効にするために管理対象デバイスに割り当てる必要があるのは従来のライセンスかスマートライセンスかを示します。

ライセンス付きの機能の多くは追加的であるため、ライセンス ステートメントでは、各機能で最も必要なライセンスについてのみ記載しています。

ライセンス文の「または」という語は、その項に記載されている機能を有効にするには特定のライセンスを管理対象デバイスに指定する必要があることを示していますが、追加のライセンスで機能を追加できます。たとえば、ファイルポリシー内では、一部のファイルルールアクションではデバイスに保護ライセンスを指定する必要がありますが、他方ではマルウェア防御ライセンスを指定する必要があります。

ライセンスの詳細については、「ライセンスについて （301 ページ）」を参照してください。

関連トピック

ライセンスについて （301 ページ）

ドキュメント内のサポート対象デバイスに関する記述

章または項目の先頭に記載されているサポート対象デバイスに関する記述は、ある機能が特定のデバイス シリーズ、ファミリ、またはモデルでのみサポートされていることを示しています。たとえば、多くの機能は Secure Firewall Threat Defense デバイスのみでサポートされています。

このリリースでサポートされているプラットフォームの詳細については、リリース ノートを参照してください。

ドキュメント内のアクセス ステートメント

このドキュメントの各手順の先頭に記載されているアクセス ステートメントは、手順の実行に必要な事前定義のユーザ ロールを示しています。記載されている任意のロールを使用して手順を実行することができます。

カスタム ロールを持っているユーザは、事前定義されたロールとは異なる権限セットを持つことができます。事前定義されたロールを使用して手順のアクセス要件が示されている場合は、同様の権限を持つカスタム ロールにもアクセス権があります。カスタム ロールを持っているユーザは、設定ページにアクセスするために使用するメニューパスが若干異なる場合があります。たとえば、侵入ポリシー権限のみが付与されているカスタム ロールを持つユーザは、アクセス コントロール ポリシーを使用する標準パスではなく侵入ポリシーを経由してネットワーク分析ポリシーにアクセスします。

IP アドレスの規則

IPv4 Classless Inter-Domain Routing（CIDR）の表記、および IPv6 と同様のプレフィックス長の表記を使用して、システムのさまざまな場所でアドレスブロックを定義することができます。

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

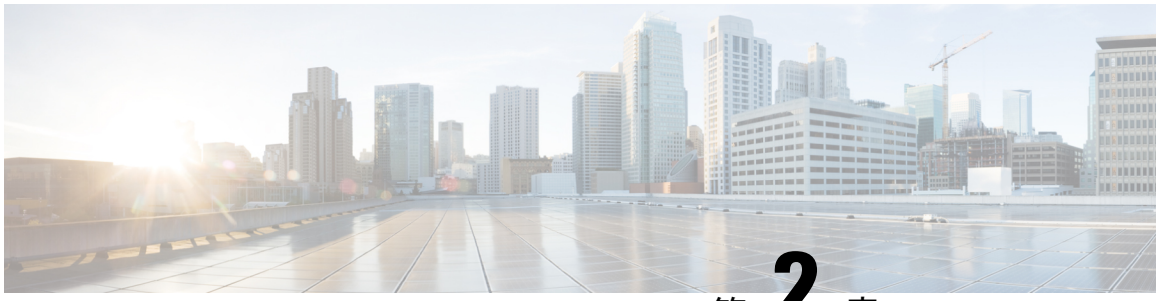
つまり、シスコでは CIDR またはプレフィックス長の表記を使用する場合に、ビット境界上でネットワーク IP アドレスを使用する標準の方法を推奨していますが、システムではこれは必要ありません。

関連リソース

ファイアウォール コミュニティは、参考資料の包括的リポジトリで、シスコの広範にわたるドキュメンテーションを補完します。これには、シスコのハードウェアの 3D モデル、ハードウェア構成セレクタ、製品販促アイテム、設定例、トラブルシューティングに関するテクニカル ノート、トレーニング ビデオ、ラボおよび Cisco Live セッション、ソーシャル メディア チャネル、Cisco ブログおよび技術文書チームによって公開されたすべてのドキュメンテーションへのリンクが含まれます。

管理人等、コミュニティ サイトや動画共有サイトに情報を掲載する個人が、シスコの社員であることがあります。それらのサイトおよび対応するコメントで表明される意見は、投稿者本人の個人的意見であり、シスコの意見ではありません。掲載内容は、情報の提供のみを目的としており、シスコや他の関係者による推奨または異議を目的としたものではありません。

（注） ファイアウォール コミュニティ の動画、テクニカルノート、および参考資料の中には、古いバージョンの Management Center に言及しているものがあります。ご使用のバージョンの Management Center と動画やテクニカルノートで参照されているバージョンとではユーザーインターフェイスに違いがあるために、手順も異なる場合があります。



第 2 章

Management Center へのログイン

以下のトピックでは、システムにログインする方法を示します。

ユーザ アカウント

ユーザー名とパスワードを入力して、Management Center または管理対象デバイスの Web インターフェイスまたはCLIへのローカルアクセスを取得する必要があります。管理対象デバイスでは、Config レベルのアクセス権を持つ CLI ユーザーは、`expert` コマンドを使用して Linux シェルにアクセスできます。Management Center では、すべての CLI ユーザーが `expert` コマンドを使用できます。Threat Defense と Management Center は、外部 LDAP や RADIUS サーバーでユーザーログイン情報を保存する外部認証を使用するように設定できる場合があります。その場合、外部ユーザーに対し、CLI へのアクセスを禁止または許可することができます。Management Center は、認証および承認のために、セキュリティ アサーション マークアップ言語（SAML）2.0 オープンスタンダードに準拠する任意の SSO プロバイダーを使用したシングルサインオン（SSO）をサポートするように設定できます。

Management Center CLI は、すべてのコマンドにアクセスできる単一の **admin** ユーザーを提供します。Management Center Web インターフェイスのユーザーがアクセスできる機能は、管理者がユーザーアカウントに付与する権限によって制御されます。管理対象デバイスでは、ユーザーがアクセスできる機能（CLI と Web インターフェイス用の）は、管理者がユーザー アカウントに付与する権限によって制御されます。

（注） システムはユーザーアカウントに基づいてユーザーアクティビティを監査します。ユーザーが正しいアカウントでシステムにログインすることを確認してください。

注意 すべての Management Center CLI ユーザー、および管理対象デバイスで Config レベルの CLI アクセス権を持つユーザーは、Linux シェルの root 権限を取得できます。このため、セキュリティ上のリスクが生じる可能性があります。システムセキュリティ上の理由から、次の点を強くお勧めします。

- 外部認証を確立した場合は、CLI へのアクセス権があるユーザーのリストを適切に制限してください。
- 管理対象デバイスで CLI アクセス権限を付与する場合は、Config レベルの CLI アクセス権を付与された内部ユーザのリストを制限します。
- Linux シェルユーザーは確立しないでください。事前定義された **admin** ユーザーおよび CLI 内で **admin** ユーザーが作成したユーザーのみを使用します。

注意 Cisco TAC または Cisco Secure Firewall のユーザーマニュアルの明示的な手順による指示がない限り、Linux シェルを使用しないことを強くお勧めします。

アプライアンスが異なれば、サポートするユーザーアカウントのタイプは異なり、搭載される機能もさまざまです。

Secure Firewall Management Centerについて

Secure Firewall Management Center では、次のユーザ アカウント タイプをサポートします。

- Web インターフェイス アクセス用に事前定義された **admin** アカウント。このアカウントは管理者ロールを保有し、Web インターフェイスから管理できます。
- カスタム ユーザー アカウント。このアカウントは Web インターフェイスへのアクセスが可能で、**admin** ユーザーおよび管理者権限を持つユーザーが作成および管理できます。
- CLI アクセスのために事前定義された **admin** アカウント。このアカウントでログインするユーザーは、`expert` コマンドを使用して Linux シェルにアクセスできます。

  CLI の **admin** アカウントと Web インターフェイスの **admin** アカウントのパスワードは初期設定時に同期されますが、それ以降、必要に応じて 2 つの **admin** アカウントに個別のパスワードを設定することができます。

注意 システム セキュリティ上の理由から、アプライアンスでは追加の Linux シェル ユーザーを確立しないことを強く推奨します。

Secure Firewall Threat Defense および Secure Firewall Threat Defense Virtual デバイス

Secure Firewall Threat Defense および Secure Firewall Threat Defense Virtual デバイスでは、次のユーザ アカウント タイプをサポートします。

- 事前定義された **admin** アカウント。このアカウントはデバイスにアクセスするすべての形態で使用できます。
- カスタム ユーザー アカウント。このアカウントは、**admin** ユーザーおよび Config アクセス権をもつユーザーが作成、管理できます。

Secure Firewall Threat Defense は、SSH ユーザの外部認証をサポートしています。

システム ユーザー インターフェイス

アプライアンスのタイプに応じて、Web ベースの GUI、補助的な CLI、または Linux シェルを使用してアプライアンスを操作できます。Secure Firewall Management Center 展開では、ほとんどの設定タスクを Management Center の GUI から実行します。CLI または Linux シェルを使用してアプライアンスに直接アクセスすることが必要なタスクは、ごく一部のタスクのみです。Cisco TAC またはユーザーマニュアルの明示的な手順による指示がない限り、Linux シェルを使用しないことを強くお勧めします。

ブラウザの要件については、『Cisco Secure Firewall Release Notes』を参照してください。

（注） すべてのアプライアンスでは、SSH を介した CLI へのログイン試行が 3 回連続して失敗すると、SSH 接続は終了します。

アプライアンス	Web ベースの GUI	補助的な CLI	Linux シェル
Secure Firewall Management Center	• 事前定義された **admin** ユーザーとカスタム ユーザー アカウントでサポートされます。 • アドミニストレーティブ タスク、管理タスク、分析タスクに使用することができます。	• 事前定義された **admin** ユーザーとカスタム外部ユーザー アカウントでサポートされます。 • SSH 接続、シリアル接続、またはキーボードおよびモニター接続を使用してアクセス可能です。 • Cisco TAC の指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください。	• 事前定義された **admin** ユーザーでサポートされます。 • Secure Firewall Management Center CLI から `expert` コマンドを使用してアクセスする必要があります。 • SSH 接続、シリアル接続、またはキーボードおよびモニター接続を使用してアクセス可能です。 • Cisco TAC または Management Center マニュアルの明示的な手順による指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください。
Secure Firewall Threat Defense Secure Firewall Threat Defense Virtual	—	• 事前定義された **admin** ユーザーとカスタム ユーザー アカウントでサポートされます。 • SSH、シリアル、またはキーボードとモニター接続を使用してアクセスできます。仮想デバイスでは、SSH または VM コンソール経由でアクセスできます。 • Cisco TAC の指示に従って設定およびトラブルシューティングを行う場合にのみ、使用できます	• 事前定義された **admin** ユーザーとカスタム ユーザー アカウントでサポートされます。 • Config アクセス権を持つ CLI ユーザーが `expert` コマンドを使用してアクセスできます。 • Cisco TAC または Management Center マニュアルの明示的な手順による指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください。

関連トピック

内部ユーザーの追加または編集 （147 ページ）

Web インターフェイスの考慮事項

- 組織が認証に共通アクセスカード（CAC）を使用している場合は、LDAP で認証されている外部ユーザーは CAC クレデンシャルを使用してアプライアンスの Web インターフェイスにアクセスすることができます。
- デフォルトのホーム ページの上部に表示されるメニューおよびメニュー オプションは、ユーザアカウントの権限に基づきます。ただし、デフォルト ホームページのリンクには、ユーザアカウントの権限の範囲に対応するオプションが含まれています。アカウントに付与されている権限とは異なる権限が必要なリンクをクリックすると、システムから警告メッセージが表示され、そのアクティビティがログに記録されます。
- プロセスの中には長時間かかるものがあります。このため、Web ブラウザで、スクリプトが応答しなくなっていることを示すメッセージが表示されることがあります。このメッセージが表示された場合は、スクリプトが完了するまでスクリプトの続行を許可してください。

関連トピック

ホームページの指定 （241 ページ）

セッション タイムアウト

セッションタイムアウトが適用されないように設定しない限り、デフォルトでは、非アクティブな状態が 1 時間続くと、システムが自動的にセッションからユーザーをログアウトします。

（注） SSO ユーザーの場合、Management Center セッションがタイムアウトすると、表示は IdP インターフェイスに一時的にリダイレクトされ、次に Management Center ログインページにリダイレクトされます。SSO セッションが他の場所から終了していない限り、ログインページの [シングルサインオン（Single Sign-On）] リンクをクリックするだけで、ログイン資格情報を提供しなくても、誰でも Management Center にアクセスできます。Management Center のセキュリティを確保し、他の人が SSO アカウントを使用して Management Center にアクセスするのを防ぐために、Management Center ログインセッションを無人のままにせず、Management Center からログアウトするときに IdP で SSO フェデレーションからログアウトすることをお勧めします。

管理者ロールを割り当てられたユーザーは、以下の設定を使用して、アプライアンスのセッション タイムアウト間隔を変更できます。

[システム（System）] > [設定（Configuration）] > [シェル タイムアウト（Shell Timeout）]

関連トピック

セッション タイムアウトの設定 （118 ページ）
SAML シングルサインオンの設定 （169 ページ）

Secure Firewall Management Center Web インターフェイスへのログイン

（注） このタスクは、LDAP または RADIUS サーバーによって認証された内部ユーザーと外部ユーザーに適用されます。SSO ログインについては、SSO を使用した Management Center Web インターフェイスへのログイン （39 ページ）を参照してください。

ユーザーは単一のアクティブなセッションに制限されます。すでにアクティブセッションがあるユーザーアカウントにログインしようとすると、もう一方のセッションを終了するか、または別のユーザーとしてログインするように求められます。

複数の Management Center が同じ IP アドレスを共有する NAT 環境の場合

- 各 Management Center が一度にサポートできるログイン セッションは 1 つだけです。
- 異なる Management Center にアクセスするには、ログインごとに別のブラウザ（Firefox や Chrome など）を使用するか、ブラウザをシークレット モードまたはプライベート モードに設定します。

始める前に

- Web インターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらうか、管理者アクセス権を持つユーザーとしてログインし、アカウントの特権を変更します。
- 「内部ユーザーの追加または編集 （147 ページ）」の説明に従って、ユーザアカウントを作成します。

手順

ステップ 1 ブラウザで **https://***ipaddress_or_hostname/* に移動します。ここで、*ipaddress* または *hostname* は使用している Management Center に対応します。

ステップ 2 [ユーザー名（Username）] および [パスワード（Password）] フィールドに、ユーザー名とパスワードを入力します。次の注意事項に注意を払ってください。

- ユーザ名は大文字/小文字を区別しません。
- マルチドメイン導入環境では、ユーザーアカウントが作成されたドメインをユーザー名の前に付加します。先祖ドメインを前に付加する必要はありません。たとえばユーザアカウントを SubdomainB で作成し、そのドメインの先祖ドメインが DomainA である場合、次の形式でユーザ名を入力します。

```
SubdomainB\username
```

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

ステップ 3 [ログイン（Login）] をクリックします。

関連トピック

セッション タイムアウト （37 ページ）

SSO を使用した Management Center Web インターフェイスへのログイン

Management Center は、セキュリティ アサーション マークアップ言語（SAML）2.0 オープンスタンダードに準拠する SSO プロバイダーで導入された、シングルサインオン（SSO）フェデレーションに参加するように設定できます。アイデンティティ プロバイダー（IdP）で SSO ユーザーアカウントを確立し、アカウント名に電子メールアドレスを使用する必要があります。ユーザー名が電子メールアドレスでない場合、または SSO ログインに失敗する場合は、システム管理者にお問い合わせください。

（注） Management Center は、SSO アカウントの CAC クレデンシャルを使用したログインをサポートしていません。

ユーザーは単一のアクティブなセッションに制限されます。すでにアクティブセッションがあるユーザーアカウントにログインしようとすると、もう一方のセッションを終了するか、または別のユーザーとしてログインするように求められます。

複数の Management Center が同じ IP アドレスを共有する NAT 環境の場合

- 各 Management Center が一度にサポートできるログイン セッションは 1 つだけです。
- 異なる Management Center にアクセスするには、ログインごとに別のブラウザ（Firefox や Chrome など）を使用するか、ブラウザをシークレット モードまたはプライベート モードに設定します。

始める前に

- Management Center を SSO アクセス用に設定します。SAML シングルサインオンの設定（169 ページ）を参照してください。
- Web インターフェイスにアクセスできない場合は、システム管理者に問い合わせて、SSO IdP でアカウントを設定してください。

手順

ステップ 1 ブラウザで **https://***ipaddress_or_hostname/* に移動します。ここで、*ipaddress* または *hostname* は使用している Management Center に対応します。

（注） SSO ユーザーは、常に SSO アクセス用に特別に設定されたログイン URL を使用して、Management Center にアクセスする必要があります。この情報については、管理者にお問い合わせください。

ステップ 2 [シングルサインオン（Single Sign-On）] リンクをクリックします。

ステップ 3 システムは、次の 2 つの方法のいずれかで応答します。

- SSO フェデレーションにすでにログインしている場合は、Management Center のデフォルトのホームページが表示されます。
- SSO フェデレーションにまだログインしていない場合は、Management Center によりブラウザが IdP のログインページにリダイレクトされます。IdP でログインプロセスを完了すると、Management Center のデフォルトのホームページが表示されます。

関連トピック

セッション タイムアウト （37 ページ）
SAML シングルサインオンの設定 （169 ページ）

CAC クレデンシャルを使用した Secure Firewall Management Center へのログイン

ユーザーは単一のアクティブなセッションに制限されます。すでにアクティブセッションがあるユーザーアカウントにログインしようとすると、もう一方のセッションを終了するか、または別のユーザーとしてログインするように求められます。

複数の Management Center が同じ IP アドレスを共有する NAT 環境の場合

- 各 Management Center が一度にサポートできるログイン セッションは 1 つだけです。
- 異なる Management Center にアクセスするには、ログインごとに別のブラウザ（Firefox や Chrome など）を使用するか、ブラウザをシークレット モードまたはプライベート モードに設定します。

⚠

注意 ブラウズ セッションがアクティブな間は、CAC を削除**しない**でください。セッション中に CAC を削除または交換すると、Web ブラウザでセッションが終了し、システムにより Web インターフェイスから強制的にログアウトされます。

始める前に

- Webインターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらうか、管理者アクセス権を持つユーザーとしてログインし、アカウントの特権を変更します。
- 「内部ユーザーの追加または編集 （147 ページ）」の説明に従ってユーザーアカウントを作成します。
- 「LDAP を使用した共通アクセス カード認証の設定 （167 ページ）」の説明に従って、CAC の認証と認可を設定します。

手順

ステップ 1 組織の指示に従って CAC を挿入します。

ステップ 2 ブラウザで **https://***ipaddress_or_hostname/* に移動します。ここで、*ipaddress* または *hostname* は使用している Management Center に対応します。

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

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

ステップ 5 [続行（Continue）] をクリックします。

関連トピック

LDAP を使用した共通アクセス カード認証の設定 （167 ページ）
セッション タイムアウト （37 ページ）
Management Center の SSO ガイドライン （170 ページ）

Management Center コマンドライン インターフェイスへのログイン

admin CLI ユーザーと特定のカスタム外部ユーザーは、Management Center CLI にログインできます。

注意 Cisco TAC または Management Center マニュアルの明示的な手順による指示がない限り、Linux シェルを使用しないことを強くお勧めします。

（注） すべてのアプライアンスでは、SSH を介した CLI へのログイン試行が 3 回連続して失敗すると、SSH 接続は終了します。

始める前に

admin ユーザーとして初期設定プロセスを完了します。「最初のログイン （3 ページ）」を参照してください。

手順

ステップ 1 **admin** ユーザー名とパスワードを使用して、SSH またはコンソールポート経由で Management Center に接続します。

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

ステップ 2 利用可能な CLI コマンドのいずれかを使用します。

最後のログインの表示

権限のないユーザがクレデンシャルを使用して Secure Firewall Management Center にサインインしていることが疑われる場合は、クレデンシャルが最後にログインに使用された日付、時刻、および IP アドレスを確認できます。

始める前に

この機能は、クラシックテーマを使用している場合は使用できません。ユーザー設定でUIテーマを選択できます。

手順

ステップ 1 Secure Firewall Management Center にサインインします。

ステップ 2 ブラウザ ウィンドウの右上隅で、サインインに使用したユーザー ID を探します。

ステップ 3 ユーザー名をクリックします。

ステップ 4 前回のログインに関する情報が、表示されるメニューの下部に表示されます。

Management Center の Web インターフェイスからのログアウト

Management Center の Web インターフェイスをアクティブに使用しなくなった場合、シスコでは、少しの間 Web ブラウザから離れるだけであっても、ログアウトすることを推奨しています。ログアウトすることで Web セッションを終了し、別のユーザーが自分の資格情報を使用してインターフェイスを使用できないようにします。

（注） Management Center で SSO セッションからログアウトしている場合は、ログアウトするときにブラウザで組織の SSO IdP にリダイレクトされます。Management Center のセキュリティを確保し、他の人が SSO アカウントを使用して Management Center にアクセスするのを防ぐために、IdP で SSO フェデレーションからログアウトすることをお勧めします。

手順

ステップ 1 ユーザー名の下にあるドロップダウンリストから、[ログアウト（Logout）] を選択します。

ステップ 2 Management Center で SSO セッションからログアウトしている場合は、組織の SSO IdP にリダイレクトされます。Management Center のセキュリティを確保するために、IdP でログアウトします。

関連トピック

セッション タイムアウト （37 ページ）

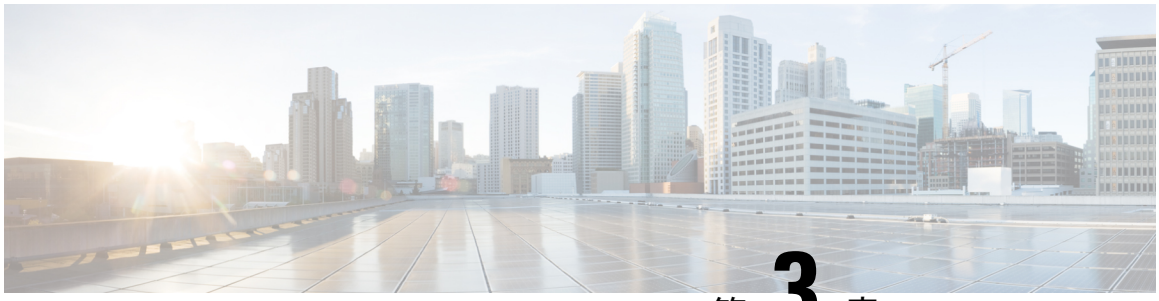
Management Center へのログイン履歴

機能	最小 Management Center	最小 Threat Defense	詳細
SAML 2.0 準拠の SSO プロバイダーを使用したシングルサインオン（SSO）のサポートが追加されました。	6.7	任意（Any）	サードパーティの SAML 2.0 準拠アイデンティティプロバイダー（IdP）で設定されたユーザーがログインページの新しい [シングルサインオン（Single Sign-On）] リンクを使用して Management Center にログインする機能が追加されました。 新規/変更された画面： ログイン画面

機能	最小 Management Center	最小 Threat Defense	詳細
Secure Firewall Management Center に最後にサインインした時刻に関する情報を表示します。	6.5	任意（Any）	最後にログインした日付、時刻、および IP アドレスを表示します。 新規/変更されたメニュー： ウィンドウの右上の、ログインに使用したユーザー名を表示するメニュー。 サポートされているプラットフォーム： Management Center
Management Center を対象とした自動 CLI アクセス	6.5	任意（Any）	SSH を使用して Management Center にログインすると、CLI に自動的にアクセスします。CLI `expert` コマンドを使用して Linux シェルにアクセスすることもできますが、このコマンドを使用しないことを強く推奨します。 （注） Management Center の CLI アクセスを有効または無効にするバージョン 6.3 の機能は廃止されます。このオプションが廃止された結果、仮想 Management Center は、**[システム（System）]** > **[設定（Configuration）]** > **[コンソールの設定（Console Configuration）]** ページを表示しなくなりました。このページは、物理 Management Center では引き続き表示されます。
SSH ログイン失敗の制限数	6.3	任意（Any）	ユーザーが SSH 経由でデバイスにアクセスし、ログイン試行を 3 回続けて失敗すると、デバイスは SSH セッションを終了します。
Management Center の CLI アクセスを有効化および無効化する機能	6.3	任意（Any）	新しい/変更された画面： Management Center の Web インターフェイスで管理者が使用可能な新しいチェックボックス：**システム**（⚙）> **[構成（Configuration）]** の [CLI アクセスの有効化（Enable CLI Access）] > [コンソール設定（Console Configuration）] ページ。 • オン： SSH を使用して Management Center にログインすると CLI にアクセスします。 • オフ：SSH を使用して Management Center にログインすると Linux シェルにアクセスします。これは、バージョン 6.3 の新規インストールと、以前のリリースからバージョン 6.3 にアップグレードした場合のデフォルトの状態です。 サポートされているプラットフォーム： Management Center

第 II 部

システム設定



第 3 章

システム設定

この章では、Secure Firewall Management Center でのシステム構成設定方法について説明します。

システム構成の要件と前提条件

モデルのサポート

Management Center

サポートされるドメイン

Global

ユーザの役割

管理者

Secure Firewall Management Center システム設定の管理

システム コンフィギュレーションは、Management Center の基本設定を識別します。

手順

ステップ 1 システム（⚙） > **[構成（Configuration）]**を選択します。

ステップ 2 ナビゲーションウィンドウを使用して、変更する設定を選択します。

アクセス リスト

IP アドレスとポートによって Management Center へのアクセスを制限できます。デフォルトでは、任意の IP アドレスに対して以下のポートが有効化されています。

- 443（HTTPS）：Web インターフェイス アクセスに使用されます。
- 22（SSH）：CLI アクセスに使用されます。

さらに、ポート 161 で SNMP 情報をポーリングするためのアクセスも追加できます。SNMP はデフォルトで無効になっているため、SNMP アクセスルールを追加する前に、まず SNMP を有効にする必要があります。詳細については、SNMP ポーリングの設定 （116 ページ）を参照してください。

注意 デフォルトでは、アクセスは制限されていません。よりセキュアな環境で運用するために、特定の IP アドレスに対するアクセスを追加してから、デフォルトの **any** オプションを削除することを検討してください。

アクセス リストの設定

このアクセス リストは、外部データベース アクセスを制御しません。データベースへの外部アクセスの有効化 （71 ページ）を参照してください。

注意 Management Center への接続に現在使用されている IP アドレスへのアクセスを削除し、「`IP=any port=443`」のエントリが存在しない場合、保存した時点でアクセスは失われます。

始める前に

デフォルトでは、アクセスリストには HTTPS と SSH のルールが含まれています。SNMP ルールをアクセスリストに追加するには、まず SNMP を有効にする必要があります。詳細については、SNMP ポーリングの設定 （116 ページ）を参照してください。

手順

ステップ 1 **システム**（⚙） > **[構成（Configuration）]** を選択します。

ステップ 2 （オプション）SNMP ルールをアクセスリストに追加する場合は、[SNMP] をクリックして SNMP を設定します。デフォルトでは、SNMP は無効になっています。SNMP ポーリングの設定 （116 ページ） を参照してください。

ステップ 3 [アクセス リスト（Access List）] をクリックします。

ステップ 4 1 つ以上の IP アドレスへのアクセスを追加するには、[ルールの追加（Add Rules）] をクリックします。

ステップ 5 [IP アドレス（IP Address）] フィールドに、IP アドレスまたはアドレスの範囲を入力するか、`any` を入力します。

ステップ 6 [SSH]、[HTTPS]、[SNMP]、またはこれらのオプションの組み合わせを選択して、これらの IP アドレスで有効にするポートを指定します。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

関連トピック

IP アドレスの規則 （31 ページ）

アクセス コントロールの設定

システム（⚙） > [設定（Configuration）] > [アクセスコントロールの設定（Access Control Preferences）] でアクセス制御の設定を指定します。

ルール変更に関するコメントの要求

ユーザーが保存時にコメントすることを許可（または要求）することで、アクセス制御ルールの変更を追跡できます。これにより、展開内の重要なポリシーが変更された理由をすばやく評価できます。デフォルトでは、この機能はディセーブルになっています。

オブジェクトの最適化

ルールポリシーをファイアウォールデバイスに展開すると、関連付けられたネットワーク オブジェクト グループをデバイス上に作成するときに、ルールで使用するネットワーク/ホストポリシーオブジェクトを評価して最適化するように Management Center を設定できます。最適化によって、隣接するネットワークがマージされ、冗長なネットワーク エントリが削除されます。これにより、実行時のアクセスリストデータ構造と設定のサイズが縮小されます。メモリ制約のある一部のファイアウォールデバイスでは、これによるメリットがあります。

たとえば、次のエントリを含みアクセスルール内で使用されるネットワーク/ホストオブジェクトについて考えてみます。

```
192.168.1.0/24
192.168.1.23
10.1.1.0
10.1.1.1
10.1.1.2/31
```

最適化が有効になっている場合、ポリシーを展開すると、結果のオブジェクトグループ設定が生成されます。

```
object-group network test
description (Optimized by management center)
network-object 10.1.1.0 255.255.255.252
network-object 192.168.1.0 255.255.255.0
```

最適化が無効になっている場合、グループ設定は次のようになります。

```
object-group network test
network-object 192.168.1.0 255.255.255.0
network-object 192.168.1.23 255.255.255.255
network-object 10.1.1.0 255.255.255.255
network-object 10.1.1.1 255.255.255.255
network-object 10.1.1.2 255.255.255.254
```

この最適化によってネットワーク/ホストオブジェクトの定義が変更されることも、新しいネットワーク/ホスト ポリシー オブジェクトが作成されることもありません。ネットワーク オブジェクト グループに別のネットワーク、ホストオブジェクト、またはオブジェクトグループが含まれている場合、オブジェクトは結合されません。代わりに、各ネットワーク オブジェクト

グループが個別に最適化されます。また、展開中の最適化プロセスの一環として、ネットワーク オブジェクト グループのインライン値のみが変更されます。

重要 最適化は、Management Center で機能が有効になった後の「最初の展開時」に「管理対象デバイス」で行われます（アップグレードで有効になった場合も含む）。ルールの数が多い場合、システムがポリシーを評価してオブジェクトの最適化を実行するのに数分から 1 時間かかることがあります。この間、デバイスの CPU 使用率も高くなることがあります。機能が無効になった後の最初の展開でも同様のことが発生します。この機能が有効または無効になった後は、メンテナンス時間帯やトラフィックの少ない時間帯など、影響が最小限になる時間に展開することを強く推奨します。

この機能は、以下のようにサポートされています。

- バージョン 7.4.0 では、この機能は、再イメージ化およびアップグレードされた Management Center に対してデフォルトで有効になっています。無効にするには、Cisco TAC にお問い合わせください。
- バージョン 7.4.1 以降では、この機能を設定できます。再イメージ化された Management Center ではデフォルトで有効になっていますが、アップグレード時には現在の設定が保持されます。

監査ログ

Management Center は、ユーザーのアクティビティを読み取り専用監査ログに記録します。監査ログのデータは、いくつかの方法で確認できます。

- Web インターフェイスの使用：監査と Syslog （497 ページ）。

  監査ログは標準イベント ビューに表示され、監査ビュー内の任意の項目に基づいて監査ログ メッセージを表示、ソート、およびフィルタリングできます。監査情報を簡単に削除したり、それに関するレポートを作成したりすることができ、ユーザーが行った変更に関する詳細なレポートを表示することもできます。

- syslog への監査ログ メッセージのストリーミング：syslog への監査ログのストリーミング（52 ページ）。。
- HTTP サーバーへの監査ログ メッセージのストリーミング：HTTP サーバーへの監査ログのストリーミング （54 ページ）。

監査ログデータを外部サーバーにストリーミングすると、Management Center の容量を節約できます。 外部 URL に監査情報を送信すると、システム パフォーマンスに影響を与える場合があるので注意してください。

オプションで監査ログストリーミングのチャネルを保護するには、TLS 証明書を使用して TLS および相互認証を有効にします。監査ログ証明書 （55 ページ）を参照してください。

複数の syslog サーバーへのストリーミング

監査ログデータは、最大 5 つの syslog サーバーにストリーミングできます。ただし、保護された監査ログストリーミングに対して TLS を有効にしている場合は、1 つの syslog サーバーにのみストリーミングできます。

設定変更の syslog へのストリーミング

構成データの形式とホストを指定することにより、構成変更を監査ログデータの一部として syslog にストリーミングできます。Management Center は、監査構成ログのバックアップと復元をサポートしています。高可用性の場合、アクティブな Management Center のみが設定変更 syslog を外部 syslog サーバーに送信します。ログファイルは HA ペア間で同期されるため、フェールオーバーまたはスイッチオーバー時には新しいアクティブ Management Center が変更ログの送信を再開します。HA ペアがスプリットブレインモードで動作している場合は、ペアの両方の Management Center が設定変更 syslog を外部サーバーに送信します。

syslog への監査ログのストリーミング

この機能を有効にすると、監査ログレコードは、syslog に次の形式で表示されます。

```
Date Time Host [Tag] Sender: User_Name@User_IP, Subsystem, Action
```

現地の日付、時刻、および発信元ホスト名の後に、角括弧で囲まれたオプション タグが続き、送信側デバイス名の後に監査ログ メッセージが続きます。

たとえば、Management Center からの監査ログメッセージに `FMC-AUDIT-LOG` のタグを指定すると、Management Center からのサンプル監査ログメッセージは次のように表示されます。

```
Mar 01 14:45:24 localhost [FMC-AUDIT-LOG] Dev-MC7000: admin@10.1.1.2, Operations >
Monitoring, Page View
```

重大度とファシリティを指定する場合、これらの値は syslog メッセージに表示されません。代わりに、これらの値は、syslog メッセージを受信するシステムにメッセージの分類方法を示します。

始める前に

Management Center が syslog サーバーと通信できることを確認します。設定を保存すると、システムは ICMP/ARP パケットと TCP SYN パケットを使用して syslog サーバーが到達可能であることを確認します。次に、システムのデフォルトでは、ポート 514/UDP を使用して監査ログがストリーミングされます。チャネルを保護する場合（任意、監査ログ証明書 （55 ページ）を参照）、TCP 用にポート 1470 を手動で設定する必要があります。

手順

ステップ 1 システム（⚙） > **[構成（Configuration）]** を選択します。

ステップ 2 [監査ログ（Audit Log）] をクリックします。

ステップ 3 [監査ログを Syslog に送信（Send Audit Log to Syslog）] ドロップダウン メニューから、[有効化（Enabled）] を選択します。

ステップ 4 次のフィールドは、syslog に送信される監査ログにのみ適用されます。

オプション	説明
設定変更の送信	設定変更の syslog を監査ログストリーミングに含めるには、ドロップダウンから関連するオプションを選択します。 • JSON：syslog には設定変更の詳しい相違点が含まれます。 • API：syslog には、設定変更の詳しい相違点を取得するための API が含まれます。 • なし：設定変更の詳細情報を除く、他のすべての監査ログを保持します。
ホスト（Host）	監査ログの送信先となる syslog サーバーの IP アドレスまたは完全修飾名。最大 5 つの syslog ホストをカンマで区切って追加できます。 （注） 監査サーバー証明書で TLS が無効になっている場合にのみ、複数の syslog ホストを指定できます。
ファシリティ	メッセージを作成するサブシステム。 Syslog アラート ファシリティ （678 ページ） で説明されているファシリティを選択します。たとえば、AUDIT を選択します。
重大度	The severity of the message. syslog 重大度レベル （679 ページ） で説明されている重大度を選択します。
タグ	監査ログ syslog メッセージに含めるオプションのタグ。 ベストプラクティス：このフィールドに値を入力すると、監査ログメッセージと他の類似した syslog メッセージ（ヘルスアラートなど）を簡単に区別できます。 たとえば、syslog に送信されるすべての監査ログレコードに `FMC-AUDIT-LOG` でラベル付けする場合は、このフィールドに `FMC-AUDIT-LOG` と入力します。

ステップ 5 （任意）syslog サーバーの IP アドレスが有効であるかどうかをテストするには、[syslogサーバーのテスト（Test Syslog Server）] をクリックします。

システムは、syslog サーバーが到達可能かどうかを確認するために次のパケットを送信します。

1. ICMP エコー要求
2. 443 ポートと 80 ポートで TCP SYN
3. ICMP タイムスタンプクエリ
4. ランダムポートで TCP SYN

（注） Management Center と syslog サーバーが同じサブネットにある場合は、ICMP の代わりに ARP が使用されます。

システムに、各サーバーの結果が表示されます。

ステップ 6 [保存（Save）] をクリックします。

HTTP サーバーへの監査ログのストリーミング

この機能を有効にすると、アプライアンスは、HTTP サーバーに次の形式で監査ログ レコードを送信します。

```
Date Time Host [Tag] Sender: User_Name@User_IP, Subsystem, Action
```

ローカルの日付、時刻、および発信元ホスト名の後に、角括弧で囲まれたオプション タグが続き、送信側アプライアンス名の後に監査ログ メッセージが続きます。

たとえば、FROMMC のタグを指定した場合は、監査ログメッセージ例は次のように表示されます。

```
Mar 01 14:45:24 localhost [FROMMC] Dev-MC7000: admin@10.1.1.2, Operations > Monitoring,
Page View
```

始める前に

デバイスが HTTP サーバーと通信できることを確認します。オプションで、チャネルを保護します。監査ログ証明書 （55 ページ）を参照してください。

手順

ステップ 1 システム（⚙） > **[構成（Configuration）]** を選択します。

ステップ 2 [監査ログ（Audit Log）] をクリックします。

ステップ 3 必要に応じて、[タグ（Tag）] フィールドに、メッセージとともに表示するタグ名を入力します。たとえば、すべての監査ログ レコードの前に FROMMC を付けるには、このフィールドに FROMMC を入力します。

ステップ 4 [HTTP サーバへの監査ログの送信（Send Audit Log to HTTP Server）] ドロップダウン リストから、[有効（Enabled）] を選択します。

ステップ 5 [監査情報を送信する URL（URL to Post Audit）] フィールドに、監査情報の送信先 URL を指定します。次にリストした HTTP POST 変数を要求するリスナー プログラムに対応する URL を入力します。

- subsystem
- actor
- event_type
- message

- `action_source_ip`
- `action_destination_ip`
- `result`
- `time`
- `tag`（定義されている場合。手順 3 を参照）

注意 暗号化されたポストを許可するには、HTTPS URL を使用します。外部 URL に監査情報を送信すると、システム パフォーマンスに影響を与える場合があります。

ステップ 6 [保存（Save）] をクリックします。

監査ログ証明書

Transport Layer Security（TLS）証明書を使用して、Management Center と信頼できる監査ログサーバー間の通信を保護することができます。

クライアント証明書（必須）

証明書署名要求（CSR）を生成して、署名のために認証局（CA）に送信してから、署名付き証明書を Management Center にインポートする必要があります。ローカルシステム設定を使用します。Management Center の署名付き監査ログ クライアント証明書の取得 （56 ページ） および Management Center への監査ログ クライアント証明書のインポート （57 ページ）。

サーバー証明書（オプション）

セキュリティを強化するために、Management Center と監査ログサーバー間の相互認証を要求することを推奨します。相互認証を実現するには、1 つ以上の証明書失効リスト（CRL）をロードします。これらの CRL にリストされている失効した証明書を使用して、サーバーに監査ログをストリーミングすることはできません。

Cisco Secure Firewall は、識別符号化規則（DER）形式でエンコードされた CRL をサポートしています。これらの CRL は、システムが Management Center Web インターフェイスの HTTPS クライアント証明書を検証するために使用する CRL と同じであることに注意してください。

ローカルシステム設定を使用します。有効な監査ログ サーバー証明書の要求 （58 ページ）。

監査ログのセキュアなストリーミング

信頼できる HTTP サーバーまたは syslog サーバーに監査ログをストリーミングする場合、Transport Layer Security（TLS）証明書を使用して Management Center とサーバー間のチャネルを保護できます。監査するアプライアンスごとに一意のクライアント証明書を生成する必要があります。

始める前に

クライアントおよびサーバー証明書を必須とする場合の影響については、監査ログ証明書 （55 ページ）を参照してください。

手順

ステップ 1 署名付きクライアント証明書を入手し、Management Center にインストールします。

a) Management Center の署名付き監査ログ クライアント証明書の取得 （56 ページ）：

システム情報と指定した ID 情報に基づいて、Management Center デバイスで証明書署名要求（CSR）を生成します。

CSR を認識済みの信頼できる認証局（CA）に送信して、署名付きクライアント証明書を要求します。

Management Center と監査ログサーバー間の相互認証が必要な場合、接続に使用するサーバー証明書に署名したのと同じ CA がクライアント証明書に署名する必要があります。

b) 認証局から署名付き証明書を受信した後は、その証明書を Management Center にインポートします。Management Center への監査ログ クライアント証明書のインポート （57 ページ）を参照してください。

ステップ 2 Transport Layer Security（TLS）を使用するサーバとの通信チャネルを設定し、相互認証を有効にします。

有効な監査ログ サーバー証明書の要求 （58 ページ）を参照してください。

ステップ 3 まだ行っていない場合は、監査ログ ストリーミングを設定します。

syslog への監査ログのストリーミング （52 ページ）またはHTTP サーバーへの監査ログのストリーミング （54 ページ）を参照してください。

Management Center の署名付き監査ログ クライアント証明書の取得

重要 ハイ アベイラビリティ設定のスタンバイ Management Center では [監査ログ証明書（Audit Log Certificate）] ページを使用できません。スタンバイ Management Center からこのタスクを実行することはできません。

システムは、ベース 64 エンコードの PEM 形式で証明書要求のキーを生成します。

始める前に

次の点を考慮してください。

- セキュリティを確保するには、グローバルに認識された信頼できる認証局（CA）を使用して、証明書に署名します。

- アプライアンスと監査ログ サーバー間で相互認証が必要な場合は、同じ認証局によってクライアント証明書とサーバー証明書の両方が署名される必要があります。

手順

ステップ 1 システム（⚙） > **[構成（Configuration）]**を選択します。
ステップ 2 [監査ログ証明書（Audit Log Certificate）] をクリックします。
ステップ 3 [新規 CSR の生成（Generate New CSR）] をクリックします。
ステップ 4 [国名（2 文字のコード）（Country Name (two-letter code)）] フィールドに国番号を入力します。
ステップ 5 [都道府県（State or Province）] フィールドに、都道府県名を入力します。
ステップ 6 [市区町村（Locality or City）] を入力します。
ステップ 7 [組織（Organization）] の名前を入力します。
ステップ 8 [組織単位（部署名）（Organizational Unit (Department)）] の名前を入力します。
ステップ 9 [共通名（Common Name）] フィールドに、証明書を要求するサーバーの完全修飾ドメイン名を入力します。

（注） 共通名と DNS ホスト名が一致しないと、監査ログのストリーミングは失敗します。

ステップ 10 [生成（Generate）] をクリックします。
ステップ 11 テキスト エディタで、新しい空のファイルを開きます。
ステップ 12 証明書要求のテキスト ブロック全体（`BEGIN CERTIFICATE REQUEST` 行と `END CERTIFICATE REQUEST` 行を含む）をコピーして、空のテキスト ファイルに貼り付けます。
ステップ 13 このファイルを *`clientname`*`.csr` として保存します。*`clientname`* は、証明書を使用する予定のアプライアンスの名前にします。
ステップ 14 [閉じる（Close）] をクリックします。

次のタスク

- この手順の「はじめる前に」セクションのガイドラインを使用して選択した認証局に、証明書署名要求を送信します。
- 署名された証明書を受け取ったら、アプライアンスにインポートします。Management Center への監査ログ クライアント証明書のインポート （57 ページ）を参照してください。

Management Center への監査ログ クライアント証明書のインポート

Management Center ハイアベイラビリティ設定では、アクティブピアを使用する必要があります。

始める前に

- Management Center の署名付き監査ログ クライアント証明書の取得 （56 ページ）。
- 正しい Management Center の署名付き証明書をインポートしていることを確認します。
- 証明書を生成した署名認証局から中間 CA を信頼するように要求された場合は、必要な証明書チェーン（証明書パスとも呼ばれる）を提供します。クライアント証明書に署名した CA は、証明書チェーンのいずれの中間証明書に署名した CA と同じである必要があります。

手順

ステップ 1 Management Center で、**システム**（⚙） > **[構成（Configuration）]** を選択します。

ステップ 2 [監査ログ証明書（Audit Log Certificate）] をクリックします。

ステップ 3 [監査クライアント証明書のインポート（Import Audit Client Certificate）] をクリックします。

ステップ 4 テキスト エディタでクライアント証明書を開いて、`BEGIN CERTIFICATE` の行と `END CERTIFICATE` の行を含むテキストのブロック全体をコピーします。このテキストを [クライアント証明書（Client Certificate）] フィールドに貼り付けます。

ステップ 5 秘密キーをアップロードするには、秘密キー ファイルを開いて、`BEGIN RSA PRIVATE KEY` の行と `END RSA PRIVATE KEY` の行を含むテキストのブロック全体をコピーします。このテキストを [秘密キー（Private Key）] フィールドに貼り付けます。

ステップ 6 必要な中間証明書をすべて開いて、それぞれのテキストのブロック全体をコピーして、[証明書チェーン（Certificate Chain）] フィールドに貼り付けます。

ステップ 7 [保存（Save）] をクリックします。

有効な監査ログ サーバー証明書の要求

システムは、識別符号化規則（DER）形式でインポートされている CRL を使用した、監査ログ サーバー証明書の検証をサポートしています。

（注） CRL を使用して証明書を確認する場合、システムは、監査ログ サーバー証明書の検証と、アプライアンスと Web ブラウザの間の HTTP 接続を保護する証明書の検証の両方に、同じ CRL を使用します。

重要 高可用性ペアのスタンバイ Management Center でこの手順を実行することはできません。

始める前に

- 相互認証を必須とし、証明書失効リスト（CRL）を使用して証明書の有効性を保持する場合の影響について説明します。監査ログ証明書 （55 ページ）を参照してください。
- 監査ログのセキュアなストリーミング （55 ページ）に記載されている手順およびその手順で参照されているトピックに従って、クライアント証明書を取得してインポートします。

手順

ステップ 1 Management Center で、**システム**（⚙） > **[構成（Configuration）]** を選択します。

ステップ 2 [監査ログ証明書（Audit Log Certificate）] をクリックします。

ステップ 3 Transport Layer Security を使用して監査ログを安全に外部サーバへストリーミングするには、[TLS の有効化（Enable TLS）] 選択します。

TLS が有効になっている場合、syslog クライアント（Management Center）は、サーバーから受信した証明書を検証します。クライアントとサーバーの間の接続は、サーバー証明書の検証が成功した場合にのみ成功します。この検証プロセスでは、次の条件を満たす必要があります。

- 証明書をクライアントに送信するように syslog サーバーを設定します。
- サーバー証明書を検証するために、CA 証明書をクライアントに追加（インポート）します。
  - クライアント証明書のインポート中に CA 証明書をインポートする必要があります。
  - 発行 CA が下位 CA の場合は、下位 CA（ルート CA）から署名 CA を追加する前に発行 CA を追加するといったことが必要になります。

ステップ 4 クライアントがサーバーに対して自分自身を認証することを望まないが、証明書が同じ CA によって発行されている場合にサーバー証明書を受け入れる場合は、次の手順を実行します（非推奨）。

a) [相互認証の有効化（Enable Mutual Authentication）] をオフにします。

重要 サーバーがクライアント証明書を検証せずにクライアントを信頼するように設定されていることを確認してください。

b) [保存（Save）] をクリックして、残りの手順をスキップします。

ステップ 5 （任意）監査ログサーバーによるクライアント証明書の検証を有効にするには、[相互認証の有効化（Enable Mutual Authentication）] をオンにします。

重要 [相互認証の有効化（Enable Mutual Authentication）] オプションは、TLS が有効になっている場合にのみ適用されます。

相互認証が有効になっている場合、syslog クライアント（Management Center）は、検証のためにクライアント証明書を syslog サーバーに送信します。クライアントは、syslog サーバーの

サーバー証明書に署名した CA の同じ CA 証明書を使用します。接続は、クライアント証明書の検証が成功した場合にのみ成功します。この検証プロセスでは、次の条件を満たす必要があります。

- クライアントから受信した証明書を検証するように syslog サーバーを設定します。
- syslog サーバーに送信するクライアント証明書を追加します。この証明書は、syslog サーバーのサーバー証明書に署名した CA によって署名されている必要があります。

（注） syslog サーバーへの監査ログのストリーミングに相互認証を使用する場合は、秘密キーに PKCS#1 形式ではなく PKCS#8 形式を使用します。PKCS#1 キーを PKCS#8 形式に変換するには、次のコマンドラインを使用してください。

```
openssl pkcs8 -topk8 -inform PEM -outform PEM
-nocrypt -in PKCS1 key file name -out PKCS8 key filename
```

ステップ 6 （任意）無効になっているサーバー証明書を自動的に認識するには、次の手順を実行します。

a) [CRLの取得の有効化（Enable Fetching of CRL）] をオンにします。

重要 このオプションは、[相互認証の有効化（Enable Mutual Authentication）] チェックボックスがオンになっている場合にのみ表示されます。ただし、[CRLの取得の有効化（Enable Fetching of CRL）] オプションは、TLS オプションが有効になっている場合にのみ適用されます。CRL の使用目的はサーバー証明書の検証であり、クライアント証明書の検証を可能にするための相互認証の使用には依存しません。

CRL の取得を有効にすると、定期的に CRL を更新（ダウンロード）するクライアントのスケジュールタスクが作成されます。CRL はサーバー証明書の検証に使用され、検証対象のサーバー証明書が CA によって取り消されたことを示す CA からの CRL がある場合、検証は失敗します。

b) 既存の CRL ファイルへの有効な URL を入力して、[CRL の追加（Add CRL）] をクリックします。

最大 25 個まで CRL の追加を繰り返します。

c) [CRL の更新（Refresh CRL）] をクリックして現在の CRL をロードするか、指定した URL から CRL をロードします。

ステップ 7 クライアント証明書を作成したものと同じ認証局によって生成された有効なクライアント証明書があることを確認します。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

（オプション）CRL 更新の頻度を設定します。証明書失効リストのダウンロードの設定（602 ページ） を参照してください。

Management Center での監査ログ クライアント証明書の表示

ログインしているアプライアンスの監査ログクライアント証明書のみ表示できます。Management Center 高可用性ペアでは、アクティブピアでのみ証明書を表示できます。

手順

ステップ 1 システム（⚙） > **[構成（Configuration）]**を選択します。

ステップ 2 [監査ログ証明書（Audit Log Certificate）] をクリックします。

変更調整

ユーザが行う変更をモニタし、変更が部門の推奨する標準に従っていることを確認するため、過去 24 時間に行われたシステム変更の詳細なレポートを電子メールで送信するようにシステムを構成できます。ユーザが変更をシステム構成に保存するたびに、変更のスナップショットが取得されます。変更調整レポートは、これらのスナップショットによる情報を組み合わせて、最近のシステム変更の概要を提供します。

次の図は、変更調整レポートの [ユーザー（User）] セクションの例を示しています。ここには、各構成の変更前の値と変更後の値の両方が一覧表示されています。ユーザが同じ構成に対して複数の変更を行った場合は、個々の変更の概要が最新のものから順に時系列でレポートに一覧表示されます。

過去 24 時間に行われた変更を参照できます。

変更調整の設定

始める前に

- 24 時間にシステムに行われた変更のメール送信されるレポートを受信する電子メールサーバーを設定します。詳細については、メール リレー ホストおよび通知アドレスの設定（69 ページ）を参照してください。

手順

ステップ 1 システム（⚙） > **[構成（Configuration）]**を選択します。

ステップ 2 [変更調整（Change Reconciliation）] をクリックします。

ステップ 3 **[有効（Enable）]** チェックボックスをオンにします。

ステップ 4 [実行する時間（Time to Run）] ドロップダウン リストから、システムが変更調整レポートを送信する時刻を選択します。

ステップ 5 [メール宛先（Email to）] フィールドにメール アドレスを入力します。

ヒント 電子メール アドレスを追加したら、いつでも [最新のレポートの再送信（Resend Last Report）] をクリックして、最新の変更調整レポートのコピーを受信者に再送信できます。

ステップ 6 ポリシーの変更を追加する場合は、[ポリシー設定を含める（Include Policy Configuration）] チェックボックスをオンにします。

ステップ 7 過去 24 時間のすべての変更を含める場合は、[全変更履歴を表示（Show Full Change History）] チェックボックスをオンにします。

ステップ 8 [保存（Save）] をクリックします。

関連トピック

監査ログを使って変更を調査する （503 ページ）

変更調整オプション

[ポリシー設定を含める（Include Policy Configuration）] オプションは、ポリシーの変更のレコードを変更調整レポートに含めるかどうかを制御します。これには、アクセス制御、侵入、システム、ヘルス、およびネットワーク検出の各ポリシーの変更が含まれます。このオプションを選択しなかった場合は、ポリシーの変更はどれもレポートに表示されません。このオプションは Management Center のみで使用できます。

[すべての変更履歴を表示する（Show Full Change History）] オプションは、過去 24 時間のすべての変更のレコードを変更調整レポートに含めるかどうかを制御します。このオプションを選択しなかった場合は、変更がカテゴリごとに統合された形でレポートに表示されます。

（注） 変更調整レポートには、Threat Defense インターフェイスおよびルーティング設定への変更は含まれません。

変更管理

変更を展開する前の監査追跡や正式な承認など、設定変更に関してより正式なプロセスを実装する必要がある組織の場合は、変更管理を有効にできます。

変更管理を有効にすると、**[チケット（Ticket）]**（） のショートカットがメニューバーに追加され、[変更管理ワークフロー（Change Management Workflow）] が **システム**（） メニューに追加されます。ユーザーは、これらの方法を使用してチケットを管理できます。

詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの「Change Management」の章を参照してください。

システム（⚙）>**[構成（Configuration）]**ページでは、次の設定を指定することができます。[保存（Save）] をクリックして変更を保存します。

- [変更管理の有効化（Enable Change Management）]：チケットと変更管理ワークフローを有効にします。有効にした場合、変更管理を無効にするには、すべてのチケットを承認または破棄する必要があります。

  この機能を無効にするには、オプションをオフにします。変更管理を無効にするには、すべてのチケットを承認または破棄する必要があります。いずれかのチケットが[処理中（In Progress）]、[保留中（On Hold）]、[拒否（Rejected）]、または [承認保留中（Pending Approval）] 状態になっている場合は、変更管理を無効にできません。

- [必要な承認の数（Number of approvals required）]：チケットを承認して展開可能にするために、変更を承認する必要がある管理者の人数。デフォルトは1人ですが、チケットごとに最大5人の承認者を要求できます。ユーザーは、チケットの作成時にこの数を上書きできます。

（注） 変更管理が有効になっており、使用中の場合、少なくとも 1 つのチケットが [処理中（In Progress）]、[保留中（On Hold）]、[拒否（Rejected）]、または [承認保留中（Pending Approval）] 状態になっていると、承認者の人数を変更できません。必要な承認者数を変更するには、すべてのチケットを承認または破棄する必要があります。

- [チケットの消去期間（Ticket Purge Duration）]：承認されたチケットを保持する日数（1 ～ 100 日）。デフォルトは 5 日間です。

- [電子メール通知（Email Notification）]（任意）：[返信先アドレス（Reply to Address）] と、[承認者アドレスのリスト（List of Approver Addresses）] の電子メールアドレスを入力します。電子メールを機能させるには、電子メール通知のシステム設定も指定する必要があります。

  クラウド提供型 Firewall Management Center の場合、返信先アドレスは表示されません。代わりに、電子メール通知のシステム設定でこのアドレスを指定してください。

注記

変更管理の有効化/無効化を妨げるシステムプロセスがいくつかあります。次のいずれかが処理中の場合は、これらの設定を変更する前に、それらが完了するまで待つ必要があります：バックアップ/復元、インポート/エクスポート、ドメインの移動、アップグレード、Flexconfig の移行、デバイスの登録、高可用性の登録/作成/解除/切り替え、クラスタノードの作成/登録/解除/編集/追加/削除、EPM のブレークアウト/参加。

これらの設定を変更した場合、アクセス コントロール ポリシーをロックすることはできません。ポリシーがロックされている場合は、この機能を有効または無効にする前に、ロックが解除されるまで待つ必要があります。

DNS キャッシュ

イベント表示ページで、IP アドレスを自動的に解決するようにシステムを設定できます。また、アプライアンスによって実行される DNS キャッシュの基本的なプロパティを設定できます。DNS キャッシングを設定すると、追加のルックアップを実行せずに、以前に解決した IP アドレスを識別できます。これにより、IPアドレスの解決が有効になっている場合に、ネットワーク上のトラフィックの量を減らし、イベントページの表示速度を速めることができます。

DNS キャッシュ プロパティの設定

DNS 解決のキャッシングは、以前に解決された DNS ルックアップのキャッシングを許可するシステム全体の設定です。

手順

ステップ 1 システム（⚙） > **[構成（Configuration）]**を選択します。

ステップ 2 [DNS キャッシュ（DNS Cache）] を選択します。

ステップ 3 [DNS 解決のキャッシング（DNS Resolution Caching）] ドロップダウン リストから、次のいずれかを選択します。

- [有効化（Enabled）]：キャッシングを有効にします。
- [無効化（Disabled）]：キャッシングを無効にします。

ステップ 4 [DNS キャッシュ タイムアウト（分）（DNS Cache Timeout（in minutes））] フィールドで、非アクティブのために削除されるまで DNS エントリがメモリ内にキャッシュされる時間（分単位）を入力します。

デフォルトは 300 分（5 時間）です。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

イベント ビューの設定 （241 ページ）

ダッシュボード

ダッシュボードでは、ウィジェットを使用することにより、現在のシステムステータスが一目でわかります。ウィジェットは小さな自己完結型コンポーネントであり、システムのさまざまな側面に関するインサイトを提供します。システムには、事前定義された複数のダッシュボードウィジェットが付属しています。

[カスタム分析（Custom Analysis）] ウィジェットがダッシュボードで有効になるように、Management Center を設定できます。

関連トピック

ダッシュボードについて （403 ページ）

ダッシュボードのカスタム分析ウィジェットの有効化

[カスタム分析（Custom Analysis）] ダッシュボード ウィジェットを使用して、柔軟でユーザーによる構成が可能なクエリに基づいてイベントのビジュアル表現を作成します。

手順

ステップ 1 システム（⚙） > **[構成（Configuration）]**を選択します。

ステップ 2 [ダッシュボード（Dashboard）] をクリックします。

ステップ 3 ユーザが [カスタム分析（Custom Analysis）] ウィジェットをダッシュボードに追加できるようにするには、[カスタム分析ウィジェットの有効化（Enable Custom Analysis Widgets）] チェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

ダッシュボードについて （403 ページ）

データベース

ディスク容量を管理するために、Management Center は、最も古い侵入イベント、監査レコード、セキュリティインテリジェンスデータ、URL フィルタリングデータをイベントデータベースから定期的にプルーニングします。イベントタイプごとに、Management Center がプルーニング後に保持するレコードの数を指定できます。そのタイプに設定された保持制限を超える数のレコードを含むイベントデータベースには依存しないでください。パフォーマンスを向上させるには、定期的に処理するイベント数に合わせてイベント制限を調整します。必要に応じて、プルーニングが発生したときに電子メール通知を受け取ることを選択できます。一部のイベント タイプでは、ストレージを無効にすることができます。

個々のイベントを手動で削除するには、イベントビューアを使用します。（バージョン 6.6.0 以降では、この方法で接続またはセキュリティ インテリジェンス イベントを手動で削除できないことに注意してください）。データベースを手動で消去することもできます。データの消去とストレージ （629 ページ）を参照してください。

データベース イベント数の制限の設定

始める前に

- Management Center のデータベースからイベントがプルーニングされた場合に電子メール通知を受信するには、電子メール サーバーを設定する必要があります。メール リレー ホストおよび通知アドレスの設定 （69 ページ）を参照してください。

手順

ステップ 1 システム（⚙） > **[構成（Configuration）]**を選択します。

ステップ 2 [データベース（Database）] を選択します。

ステップ 3 各データベースについて、保存するレコードの数を入力します。

各データベースが保持できるレコード数の詳細については、データベース イベント数の制限（66 ページ）を参照してください。

ステップ 4 必要に応じて、[データ プルーニング通知のアドレス（Data Pruning Notification Address）] フィールドに、プルーニング通知を受信する電子メール アドレスを入力します。

ステップ 5 [保存（Save）] をクリックします。

データベース イベント数の制限

次の表に、Management Center ごとに保存可能な各イベントタイプのレコードの最小数と最大数を示します。

表 *1:* データベース イベント数の制限

イベントタイプ	上限	下限
侵入イベント	1,000 万（Management Center Virtual） 3,000 万（Management Center1000、Management Center1600） 6,000 万（Management Center2500、Management Center2600、FMCv 300） 3 億（Management Center4500、Management Center4600） 4 億（Management Center4700）	10,000

イベントタイプ	上限	下限
検出イベント	1,000 万 （Management Center 仮想） 2,000 万（Management Center2500、Management Center2600、 Management Center4500、Management Center4600、Management Center4700、FMCv 300）	0（ストレージを無効化）
接続イベント セキュリティ インテリジェンス イベント	5,000 万（Management Center 仮想） 1 億（Management Center1000、Management Center1600） 3 億（Management Center2500、Management Center2600、FMCv 300） 10 億（Management Center4500、Management Center4600、Management Center4700） 制限は接続イベントとセキュリティ インテリジェンスイベントの間で共有されます。設定済みの最大数の合計がこの制限を超えることはできません。	0（ストレージを無効化） [最大接続イベント数（Maximum Connection Events）] の値をゼロに設定すると、セキュリティ インテリジェンス、侵入、ファイル、およびマルウェアの各イベントに関連付けられていない接続イベントは Management Center に保存されません。 **注意** [Maximum Connection Events] をゼロに設定すると、セキュリティ インテリジェンス イベント以外の既存の接続イベントがただちに消去されます。 この設定が最大フローレートに与える影響については、以下を参照してください。 これらの設定は、接続サマリーには影響しません。
接続の要約（集約された接続イベント）	5,000 万（Management Center 仮想） 1 億（Management Center1000、Management Center1600） 3 億（Management Center2500、Management Center2600、FMCv 300） 10 億（Management Center4500、Management Center4600、Management Center4700）	0（ストレージを無効化）

イベントタイプ	上限	下限
相関イベントおよびコンプライアンスの allow リスト イベント	100 万 （Management Center 仮想） 200 万（Management Center2500、Management Center2600、Management Center4500、Management Center4600、Management Center4700、FMCv 300）	1 つ
マルウェア イベント	1,000 万 （Management Center 仮想） 2,000 万（Management Center2500、Management Center2600、Management Center4500、Management Center4600、Management Center4700、FMCv 300）	10,000
ファイル イベント	1,000 万 （Management Center 仮想） 2,000 万（Management Center2500、Management Center2600、Management Center4500、Management Center4600、Management Center4700、FMCv 300）	0（ストレージを無効化）
ヘルス イベント	100 万	0（ストレージを無効化）
監査レコード	100,000	1 つ
修復ステータス イベント	1,000 万	1 つ
許可（Allow） リスト違反履歴	30 日間の違反履歴	1 日の履歴
ユーザ アクティビティ（ユーザ イベント）	1,000 万	1 つ
ユーザ ログイン（ユーザ履歴）	1,000 万	1 つ
侵入ルール更新のインポート ログ レコード	100 万	1 つ
VPN トラブルシューティング データベース	1,000 万	0（ストレージを無効化）

最大フローレート

Management Center ハードウェアモデルの [最大フローレート（Maximum flow rate）]（1 秒あたりのフロー数）の値は、https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html?cachemode=refresh の Management Center データシートの「Platform Specifications」の項で指定されています。

プラットフォーム設定の [最大接続イベント数（Maximum Connection Events）] の値をゼロに設定すると、セキュリティインテリジェンス、侵入、ファイル、およびマルウェアの各イベントに関連付けられていない接続イベントは、Management Center ハードウェアの最大フローレートにカウントされません。

このフィールドにゼロ以外の値を指定すると、すべての接続イベントが最大フローレートに対してカウントされます。

このページの他のイベントタイプは、最大フローレートにはカウントされません。

電子メール通知

次の処理を行う場合は、メール ホストを設定します。

- イベントベースのレポートの電子メール送信
- スケジュールされたタスクのステータス レポートの電子メール送信
- 変更調整レポートの電子メール送信
- データプルーニング通知の電子メール送信
- 検出イベント、影響フラグ、相関イベントアラート、侵入イベントアラート、および正常性イベントアラートに電子メールを使用します。

電子メール通知を設定する場合、システムとメール リレー ホスト間の通信に使用する暗号化方式を選択し、必要に応じて、メールサーバの認証クレデンシャルを指定できます。設定した後、接続をテストできます。

メール リレー ホストおよび通知アドレスの設定

手順

ステップ 1 システム（⚙） > **[構成（Configuration）]**を選択します。

ステップ 2 [電子メール通知（Email Notification）] をクリックします。

ステップ 3 [メール リレー ホスト（Mail Relay Host）] フィールドで、使用するメール サーバのホスト名または IP アドレスを入力します。入力したメール ホストはアプライアンスからのアクセスを許可している**必要があります**。

ステップ 4 [ポート番号（Port Number）] フィールドに、電子メール サーバで使用するポート番号を入力します。

一般的なポートには次のものがあります。

- 25。暗号化を使用しない場合
- 465。SSLv3 を使用する場合
- 587。TLS を使用する場合

ステップ 5 [暗号化方式（Encryption Method）] を選択します。

- [TLS]：Transport Layer Security を使用して通信を暗号化します。
- [SSLv3]：セキュア ソケット レイヤを使用して通信を暗号化します。
- [なし（None）]：暗号化されていない通信を許可します。

（注） アプライアンスとメール サーバとの間の暗号化された通信では、証明書の検証は不要です。

ステップ 6 [送信元アドレス（From Address）] フィールドに、アプライアンスから送信されるメッセージの送信元電子メール アドレスとして使用する有効な電子メール アドレスを入力します。

ステップ 7 必要に応じて、メール サーバに接続する際にユーザ名とパスワードを指定するには、[認証を使用（Use Authentication）] を選択します。[ユーザー名（Username）] フィールドにユーザー名を入力します。パスワードを [パスワード（Password）] フィールドに入力します。

ステップ 8 設定したメール サーバを使用してテスト メールを送信するには、[Test Mail Server Settings] をクリックします。

テストの成功または失敗を示すメッセージがボタンの横に表示されます。

ステップ 9 [保存（Save）] をクリックします。

外部データベース アクセス

サードパーティ製クライアントによるデータベースへの読み取り専用アクセスを許可するように、Management Center を設定できます。これによって、次のいずれかを使用して SQL でデータベースを照会できるようになります。

- 業界標準のレポート作成ツール（Actuate BIRT、JasperSoft iReport、Crystal Reports など）
- JDBC SSL 接続をサポートするその他のレポート作成アプリケーション（カスタム アプリケーションを含む）
- シスコが提供する RunQuery と呼ばれるコマンドライン型 Java アプリケーション（インタラクティブに実行することも、1 つのクエリの結果をカンマ区切り形式で取得することもできる）

Management Center のシステム設定を使用して、データベース アクセスを有効にして、選択したホストにデータベースの照会を許可するアクセス リストを作成します。このアクセス リストは、アプライアンスのアクセスは制御しません。

次のツールを含むパッケージをダウンロードすることもできます。

- RunQuery（シスコが提供するデータベース クエリ ツール）
- InstallCert（アクセスしたいManagement Centerから SSL 証明書を取得して受け入れるために使用できるツール）
- データベースへの接続時に使用する必要がある JDBC ドライバ

データベースアクセスを設定するためにダウンロードしたパッケージ内のツールの使用方法については、『*Cisco Secure Firewall Management Center Database Access Guide*』を参照してください。

データベースへの外部アクセスの有効化

手順

ステップ 1 **システム**（⚙） > **[構成（Configuration）]**を選択します。

ステップ 2 [外部データベース アクセス（External Database Access）] をクリックします。

ステップ 3 [外部データベース アクセスの許可（Allow External Database Access）] チェックボックスをオンにします。

ステップ 4 [サーバ ホスト名（Server Hostname）] フィールドに、適切な値を入力します。サードパーティ アプリケーションの要件に応じて、この値は、Management Center の完全修飾ドメイン名（FQDN）、IPv4 アドレス、または IPv6 アドレスにできます。

（注） Management Center のハイアベイラビリティ設定では、アクティブピアの詳細のみを入力します。スタンバイピアの詳細を入力することはお勧めしません。

ステップ 5 [クライアント JDBC ドライバ（Client JDBC Driver）] の横にある [ダウンロード（Download）] をクリックし、ブラウザのプロンプトに従って`client.zip`パッケージをダウンロードします。

ステップ 6 1 つ以上の IP アドレスからのデータベース アクセスを追加するため、[Add Hosts] をクリックします。[アクセスリスト（Access List）] フィールドに [IP アドレス（IP Address）] フィールドが表示されます。

ステップ 7 [IP アドレス（IP Address）] フィールドに、IP アドレスまたはアドレスの範囲を入力するか、`any` を入力します。

ステップ 8 [追加（Add）] をクリックします。

ステップ 9 [保存（Save）] をクリックします。

ヒント 最後に保存されたデータベース設定に戻すには、[更新（Refresh）] をクリックします。

関連トピック

IP アドレスの規則 （31 ページ）

HTTPS 証明書

Management Center デバイスは、セキュア ソケット レイヤ（SSL）証明書によりシステムと Web ブラウザ間に暗号化チャネルを確立することができます。すべての ファイアウォール デバイスにデフォルト証明書が含まれていますが、これはグローバルレベルで既知の CA から信頼された認証局（CA）によって生成された証明書ではありません。したがって、デフォルト証明書ではなく、グローバル レベルで既知の CA または内部で信頼された CA 署名付きのカスタム証明書の使用を検討してください。

注意 Management Center は 4096 ビット HTTPS 証明書をサポートしています。Management Center で使用する証明書が 4096 ビットを超える公開サーバー キーを使用して生成されている場合、Management Center Web インターフェイスにログインできません。この問題が発生した場合は、Cisco TACにお問い合わせください。

（注） HTTPS 証明書は、Management Center の REST API ではサポートされていません。

デフォルト HTTPS サーバー証明書

アプライアンスに提供されるデフォルトサーバー証明書を使用する場合、Web インターフェイスのアクセスに有効な HTTPS クライアント証明書が必要になるようにシステムを設定しないでください。これは、デフォルトサーバー証明書が、クライアント証明書に署名する CA によって署名されないためです。

デフォルトのサーバー証明書の有効期間は、証明書がいつ生成されたかによって異なります。デフォルトのサーバー証明書の期限日を表示するには、**システム**（⚙）>**[構成（Configuration）]** > [HTTPS証明書（HTTPS Certificate）] を選択します。

一部の Cisco Secure Firewall ソフトウェアのアップグレードでは、証明書を自動的に更新できることに注意してください。詳細については、該当するバージョンの『Cisco Cisco Secure FirewallRelease Notes』を参照してください。

Management Centerで、**システム**（⚙） > **[構成（Configuration）]** > [HTTPS証明書（HTTPS Certificate）] ページでデフォルトの証明書を更新します。

カスタム HTTPS サーバー証明書

Management Center Web インターフェイスを使用して、システム情報と指定した ID 情報に基づいて、サーバ証明書要求を生成できます。ブラウザによって信頼されている内部認証局（CA）

がインストールされている場合は、この要求を使用して証明書に署名することができます。生成された要求を認証局に送信して、サーバー証明書を要求することもできます。認証局（CA）から署名付き証明書を取得すると、その証明書をインポートできます。

HTTPS サーバー証明書の要件

HTTPS 証明書を使用して Web ブラウザと Cisco Secure Firewall アプライアンスの Web インターフェイスの間の接続を保護する場合は、インターネット X.509 公開キーインフラストラクチャ証明書および証明書失効リスト（CRL）プロファイル（RFC 5280）に準拠する証明書を使用する必要があります。サーバー証明書をアプライアンスにインポートする場合、証明書がその標準のバージョン 3（x.509 v3）に準拠していないと、システムによって証明書は拒否されます。

HTTPS サーバー証明書をインポートする前に、次のフィールドが含まれていることを確認してください。

証明書フィールド	説明
バージョン	エンコードされた証明書のバージョン。バージョン 3 を使用します。RFC 5280 のセクション 4.1.2.1 を参照してください。
Serial number	発行元 CA によって証明書に割り当てられた正の整数。発行者とシリアル番号を組み合わせて、証明書を一意に識別します。RFC 5280 のセクション 4.1.2.2 を参照してください。
シグネチャ	証明書の署名用に CA で使用されるアルゴリズムの識別子。signatureAlgorithm フィールドと一致している必要があります。RFC 5280 のセクション 4.1.2.3 を参照してください。
発行元（Issuer）	証明書を署名および発行したエンティティを識別します。RFC 5280 のセクション 4.1.2.4 を参照してください。
Validity	CA が証明書のステータスに関する情報を維持することを保証する期間。RFC 5280 のセクション 4.1.2.5 を参照してください。
Subject	サブジェクトの公開キーフィールドに保存された公開キーに関連付けられているエンティティを識別します。X.500 識別名（DN）を指定する必要があります。RFC 5280 のセクション 4.1.2.6 を参照してください。

証明書フィールド	説明
Subject Alternative Name	証明書によって保護されるドメイン名と IP アドレス。サブジェクト代替名は、RFC 5280 のセクション 4.2.1.6 で定義されています。 証明書が複数のドメインまたは IP アドレスに使用される場合は、このフィールドを使用することをお勧めします。
Subject Public Key Info	公開キーとそのアルゴリズムの識別子。RFC 5280 のセクション 4.1.2.7 を参照してください。
Authority Key Identifier	証明書の署名に使用される秘密キーに対応する公開キーを識別する手段を提供します。RFC 5280 のセクション 4.2.1.1 を参照してください。
サブジェクトキー識別子	特定の公開キーが含まれる証明書を識別する手段を提供します。RFC 5280 のセクション 4.2.1.2 を参照してください。
[キーの使用状況（Key Usage）]	証明書に含まれるキーの目的を定義します。RFC 5280 のセクション 4.2.1.3 を参照してください。
基本的制約	証明書のサブジェクトが CA で、この証明書を含む検証認証パスの最大深さかどうかを識別します。RFC 5280 のセクション 4.2.1.9 を参照してください。Cisco Secure Firewall アプライアンスで使用されるサーバー証明書の場合は、`critical CA:FALSE` を使用します。
拡張キーの用途拡張	キーの用途拡張で示されている基本的な目的に加えて、認定公開キーを使用する目的を 1 つ以上示します。RFC 5280 のセクション 4.2.1.12 を参照してください。サーバー証明書として使用できる証明書をインポートしてください。
signatureAlgorithm	証明書の署名用に CA で使用されるアルゴリズムの識別子。[署名（Signature）] フィールドと一致する必要があります。RFC 5280 のセクション 4.1.1.2 を参照してください。
signatureValue	デジタル署名。RFC 5280 のセクション 4.1.1.3 を参照してください。

HTTP クライアント証明書

クライアントブラウザの証明書チェック機能を使用して、システムの Web サーバーへのアクセスを制限できます。ユーザ証明書を有効にすると、Web サーバはユーザのブラウザ クライアントで有効なユーザ証明書が選択されていることを確認します。そのユーザ証明書は、サーバ証明書で使用されているのと同じ信頼できる認証局によって生成されている必要があります。以下の状況ではいずれの場合もブラウザは Web インターフェイスをロードできません。

- ユーザがブラウザに無効な証明書を選択する。
- ユーザがブラウザにサーバ証明書に署名した認証局が生成していない証明書を選択する。
- ユーザがブラウザにデバイスの証明書チェーンの認証局が生成していない証明書を選択する。

クライアントブラウザ証明書を確認するには、システムを設定してオンライン証明書ステータスプロトコル（OCSP）を使用するか、1 つ以上の証明書失効リスト（CRL）ファイルをロードします。OCSP を使用する場合、Web サーバは接続要求を受信すると、接続を確立する前に認証局と通信して、クライアント証明書の有効性を確認します。サーバーに 1 つ以上の CRL をロードするよう設定する場合、Web サーバーはクライアント証明書を CRL の一覧に照らして比較します。ユーザーが CRL にある失効した証明書の一覧に含まれる証明書を選択した場合、ブラウザは Web インターフェイスをロードできません。

（注） CRL を使用した証明書の確認を選択すると、システムはクライアント ブラウザ証明書、監査ログ サーバ証明書の両方の検証に同じ CRL を使用します。

現在の HTTPS サーバ証明書の表示

手順

ステップ 1 システム（⚙） > **[構成（Configuration）]**を選択します。
ステップ 2 [HTTPS Certificate] をクリックします。

HTTPS サーバー証明書署名要求の生成

広く知られている CA または内部的に信頼できる CA によって署名されていない証明書をインストールすると、Web インターフェイスに接続しようとするとブラウザにセキュリティ警告が表示されます。

証明書署名要求（CSR）は生成元のアプライアンスまたはデバイスに対して一意です。1 つのアプライアンスの複数のデバイスに対して CSR を生成することはできません。必須のフィー

ルドはありませんが、[CN]、[組織（Organization）]、[組織部門（Organization Unit）]、[市区町村（City/Locality）]、[州/都道府県（State/Province）]、[国/地域（Country/Region）]、および[サブジェクト代替名（Subject Alternative Name）] の値を入力することをお勧めします。

証明書要求用に生成されるキーは、ベース 64 エンコードの PEM 形式です。

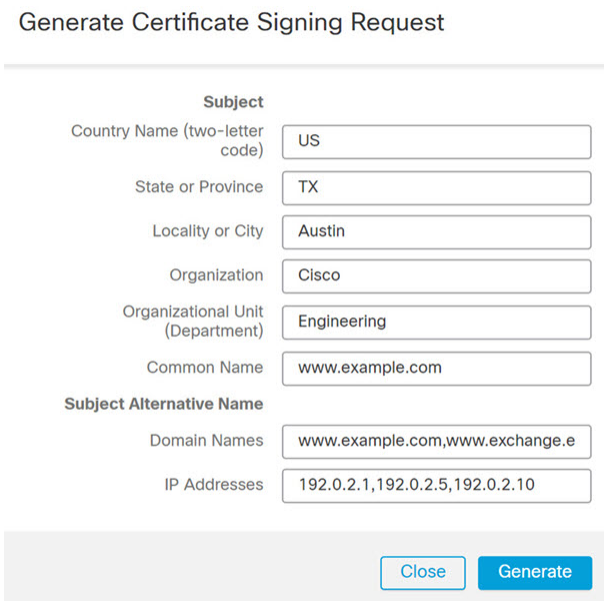
手順

ステップ 1 システム（⚙） > **[構成（Configuration）]**を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

ステップ 3 [新規 CSR の生成（Generate New CSR）] をクリックします。

次の図は例を示しています。



ステップ 4 [国名（2 文字のコード）（Country Name (two-letter code)）] フィールドに国番号を入力します。

ステップ 5 [都道府県（State or Province）] フィールドに、都道府県名を入力します。

ステップ 6 [市区町村（Locality or City）] を入力します。

ステップ 7 [組織（Organization）] の名前を入力します。

ステップ 8 [組織単位（部署名）（Organizational Unit (Department)）] の名前を入力します。

ステップ 9 [共通名（Common Name）] フィールドに、証明書を要求するサーバーの完全修飾ドメイン名を入力します。

（注） [共通名（Common Name）] フィールドには、証明書に表示されるとおりに、サーバの完全修飾ドメイン名を正確に入力する必要があります。共通名と DNS ホスト名が一致していないと、アプライアンスへの接続時に警告が表示されます。

ステップ 10 複数のドメイン名または IP アドレスを保護する証明書を要求するには、[サブジェクト代替名（Subject Alternative Name）] セクションに次の情報を入力します。

a) [ドメイン名（Domain Names）]：サブジェクト代替名で保護される完全修飾ドメインとサブドメイン（存在する場合）を入力します。

b) [IP アドレス（IP Addresses）]：サブジェクト代替名で保護される IP アドレスを入力します。

ステップ 11 [生成（Generate）] をクリックします。

ステップ 12 テキスト エディタを開きます。

ステップ 13 証明書要求のテキストブロック全体（`BEGIN CERTIFICATE REQUEST` 行と `END CERTIFICATE REQUEST` 行を含む）をコピーして、空のテキスト ファイルに貼り付けます。

ステップ 14 このファイルを *servername*`.csr` として保存します。*servername* は証明書を使用するサーバの名前です。

ステップ 15 [閉じる（Close）] をクリックします。

次のタスク

- 証明機関に証明書要求を送信します。
- 署名付き証明書を受け取ったら、Management Center にインポートします。HTTPS サーバー証明書のインポート （77 ページ）を参照してください。

HTTPS サーバー証明書のインポート

証明書を生成した署名認証局から中間 CA を信頼するように要求された場合は、証明書チェーン（証明書パス）も提供する必要があります。

クライアント証明書が必要な場合、サーバ証明書が次に示すいずれかの条件を満たしていないときに、Web インターフェイス経由でのアプライアンスへのアクセスに失敗します。

- 証明書が、クライアント証明書に署名したものと同じ CA によって署名されている。
- 証明書が、証明書チェーンの中間証明書に署名したものと同じ CA によって署名されている。

注意 Management Center は 4096 ビット HTTPS 証明書をサポートしています。Management Center で使用する証明書が 4096 ビットを超える公開サーバー キーを使用して生成されている場合、Secure Firewall Management Center Web インターフェイスにログインできません。HTTPS 証明書のバージョン 6.0.0 への更新に関する詳細は、*FirePOWER* システムリリースノート、バージョン *6.0* の「Update Management Center HTTPS Certificates to Version 6.0」を参照してください。HTTPS 証明書を生成またはインポートしていて、Management Center の Web インターフェイスにログインできない場合は、サポートまでお問い合わせください。

始める前に

- 証明書署名要求を生成します。HTTPS サーバー証明書署名要求の生成 （75 ページ）を参照してください。
- この CSR ファイルを証明書の要求先となる認証局にアップロードするか、この CSR を使用して自己署名証明書を作成します。
- 証明書がHTTPS サーバー証明書の要件 （73 ページ）で説明されている要件を満たしていることを確認します。

手順

ステップ 1 **システム**（⚙） > **[構成（Configuration）]**を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

ステップ 3 [HTTPSサーバ証明書のインポート（Import HTTPS Server Certificate）] をクリックします。

（注） 暗号化された HTTPS 証明書はインポートできません。

ステップ 4 テキスト エディタでサーバー証明書を開いて、`BEGIN CERTIFICATE` の行と `END CERTIFICATE` の行を含むテキストのブロック全体をコピーします。このテキストを [サーバー証明書（Server Certificate）] フィールドに貼り付けます。

ステップ 5 **秘密キー**を指定する必要があるかどうかは、証明書署名要求の生成方法によって異なります。

- Secure Firewall Management Center Web インターフェイスを使用して証明書署名要求を生成した場合（HTTPS サーバー証明書署名要求の生成 （75 ページ）に記載）、システムにはすでに秘密キーがあるため、ここで入力する必要はありません。
- 他の方法を使用して証明書署名要求を生成した場合、ここで秘密キーを指定する必要があります。秘密キー ファイルを開いて、`BEGIN RSA PRIVATE KEY` の行と `END RSA PRIVATE KEY` の行を含むテキストのブロック全体をコピーします。このテキストを [秘密キー（Private Key）] フィールドに貼り付けます。

ステップ 6 必要な中間証明書をすべて開いて、それぞれのテキストのブロック全体をコピーして、[証明書チェーン（Certificate Chain）] フィールドに貼り付けます。ルート証明書を受け取った場合は、ここに貼り付けます。中間証明書を受け取った場合は、ルート証明書の下に貼り付けます。どちらの場合も、`BEGIN CERTIFICATE` の行と `END CERTIFICATE` の行を含むテキストのブロック全体をコピーします。

ステップ 7 [保存（Save）] をクリックします。

有効な HTTPS クライアント証明書の強制

Management Center Webインターフェイスに接続するユーザーにユーザー証明書の提供を要求するには、次の手順を使用します。システムは、OCSP または PEM（Privacy-enhanced Electronic

Mail）形式でインポートされた CRL を使用した HTTPS クライアント証明書の検証をサポートしています。

CRL を使用する場合は、失効した証明書のリストを最新の状態に保つために、CRL を更新するスケジュールタスクを作成してください。システムは、最後に更新した CRL を表示します。

（注） クライアント認証を有効にした後で Web インターフェイスにアクセスするには、ブラウザに有効なクライアント証明書が存在している（またはリーダーに CAC が挿入されている）**必要があります**。

始める前に

- 接続に使用するクライアント証明書に署名した認証局と同じ認証局で署名されたサーバー証明書をインポートします。HTTPS サーバー証明書のインポート （77 ページ）を参照してください。
- サーバー証明書チェーンをインポートします（必要な場合）。HTTPS サーバー証明書のインポート （77 ページ）を参照してください。

手順

ステップ 1 システム（⚙） > **[構成（Configuration）]**を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

ステップ 3 [クライアント証明書の有効化（Enable Client Certificates）] を選択します。プロンプトが表示されたら、ドロップダウンリストから該当する証明書を選択します。

ステップ 4 次の 3 つのオプションがあります。

- 1 つ以上の CRL を使用してクライアント証明書を検証する場合は、[CRL のフェッチの有効化（Enable Fetching of CRL）] を選択して、手順 5 に進みます。
- OCSP を使用してクライアント証明書を検証する場合は、[OCSPの有効化（Enable OCSP）] を選択して、手順 7 に進みます。
- 失効の確認なしでクライアント証明書を承認する場合は、手順 8 に進みます。

ステップ 5 既存の CRL ファイルへの有効な URL を入力して、[CRL の追加（Add CRL）] をクリックします。最大 25 個まで CRL の追加を繰り返します。

ステップ 6 [CRL の更新（Refresh CRL）] をクリックして現在の CRL をロードするか、指定した URL から CRL をロードします。

（注） CRL のフェッチを有効にすると、定期的に CRL を更新するスケジュール タスクが作成されます。このタスクを編集して、更新の頻度を設定します。

ステップ 7 クライアント証明書がアプライアンスにロードされた認証局によって署名されていることと、サーバ証明書がブラウザの証明書ストアにロードされている認証局によって署名されていることを確認します。（これらは同じ認証局であることが必要です）。

注意 有効化したクライアント証明書で設定を保存している場合、ブラウザの証明書ストアに有効なクライアント証明書がないと、アプライアンスへの Web サーバ アクセスがすべて無効になります。設定を保存する前に、有効なクライアント証明書がインストールされていることを確認してください。

ステップ 8 [保存（Save）] をクリックします。

関連トピック

証明書失効リストのダウンロードの設定 （602 ページ）

デフォルトの HTTPS サービス証明書の更新

ログインしているアプライアンスのサーバー証明書のみを表示できます。

手順

ステップ 1 システム（⚙） > **[構成（Configuration）]**を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

システムがデフォルトの HTTPS サーバー証明書を使用するように設定されている場合にのみ、ボタンが表示されます。

ステップ 3 [HTTPS証明書の更新（Renew HTTPS Certificate）] をクリックします。（このオプションは、デフォルトの HTTPS サーバー証明書を使用するようにシステムが設定されている場合にのみ、証明書情報の下のディスプレイに表示されます）

ステップ 4 （オプション）[HTTPS 証明書の更新（Renew HTTPS Certificate）] ダイアログボックスで、[新しいキーの生成（Generate New Key）] を選択して証明書の新しいキーを生成します。

ステップ 5 [HTTPS 証明書の更新（Renew HTTPS Certificate）] ダイアログボックスで [保存（Save）] をクリックします。

次のタスク

[HTTPS 証明書（HTTPS Certificate）] ページに表示されている証明書の有効日が更新されていることを確認することによって証明書が更新されていることを確認できます。

情報

[システム（System）]>[設定（Configuration）]ページには、次の表に示す情報が含まれています。別途記載のない限り、フィールドはすべて読み取り専用です。

（注） 同様の情報が含まれている [ヘルプ（Help）] >[概要（About）] ページも参照してください。

フィールド	説明
名前	Management Center アプライアンスに割り当てられた説明的な名前。ホスト名をアプライアンスの名前として使用できますが、このフィールドに別の名前を入力しても、ホスト名が変更されることはありません。 この名前は、特定の統合で使用されます。たとえば、SecureX および SecureX Threat Response との統合のデバイスリストに表示されます。 名前を変更すると、登録されているすべてのデバイスが期限切れとしてマークされ、新しい名前をデバイスにプッシュするために展開が必要になります。
製品モデル（Product Model）	アプライアンスのモデル名。
シリアル番号（Serial Number）	アプライアンスのシリアル番号。
ソフトウェア バージョン（Software Version）	アプライアンスに現在インストールされているソフトウェアのバージョン。
オペレーティング システム（Operating System）	アプライアンス上で現在実行されているオペレーティング システム。
オペレーティング システム バージョン（Operating System Version）	アプライアンス上で現在実行されているオペレーティング システムのバージョン。
IPv4 アドレス（IPv4 Address）	デフォルト管理インターフェイス（`eth0`）の IPv4 アドレス。IPv4 の管理が無効になっている場合は、このフィールドにそのことが示されます。
IPv6 アドレス（IPv6 Address）	デフォルト管理インターフェイス（`eth0`）の IPv6 アドレス。IPv6 の管理が無効になっている場合は、このフィールドに表示されます。

フィールド	説明
現在のポリシー（Current Policies）	現在展開されているシステム レベルのポリシー。ポリシーが最後に適用された後で更新されていると、ポリシー名がイタリック体で表示されます。
モデル番号（Model Number）	内部フラッシュ ドライブに保存されているアプライアンス固有のモデル番号。この番号は、トラブルシューティングで重要になる場合があります。

侵入ポリシーの設定

さまざまな侵入ポリシー設定を指定して、展開内の重要なポリシーの変更をモニターおよび追跡します。

侵入ポリシー設定の指定

侵入ポリシー設定を指定します。

手順

ステップ 1 システム（⚙）> **[構成（Configuration）]**を選択します。

ステップ 2 [侵入ポリシー設定（Intrusion Policy Preferences）] をクリックします。

ステップ 3 次の選択肢があります。

- [ポリシーの変更に関するコメント（Comments on policy change）]：ユーザーが侵入ポリシーを変更するときに、コメント機能を使用してポリシー関連の変更を追跡するには、このチェックボックスをオンにします。ポリシー変更のコメントが有効にされていると、管理者はコメントにアクセスして、導入で重要なポリシーが変更された理由を素早く評価できます。

  ポリシーの変更に関するコメントを有効にした場合、コメントをオプションまたは必須に設定できます。Management Centerは、ポリシーに対する新しい変更が保存されるたびに、ユーザーにコメントを入力するようプロンプトを出します。

- [侵入ポリシーの変更を監査ログに書き込む（Write changes in Intrusion Policy to audit log）]：侵入ポリシーの変更を監査ログに記録するには、このチェックボックスをオンにします。このオプションは、デフォルトで有効です。

- [削除されたSnort 3ルールのユーザーオーバーライドの保持（Retain user overrides for deleted Snort 3 rules）]：LSP 更新中に「オーバーライドされた」システム定義ルールの変更に関する通知を受け取るには、このチェックボックスをオンにします。オンにすると、LSP 更新の一部として追加される新しい置換ルールのルールオーバーライドが保持されます。通

知を表示するには、Management Center メニューバーで、**[通知（Notification）]** > **[タスク（Tasks）]** をクリックします。このオプションは、デフォルトで有効です。

言語

[言語（Language）] ページを使用して、Web インターフェイス用に異なる言語を指定できます。

Web インターフェイスの言語の設定

ここで指定した言語は、すべてのユーザーの Web インターフェイスに使用されます。次の中から選択できます。

- 英語
- フランス語
- 中国語（簡体字）
- 中国語（繁体字）
- 日本語
- 韓国語

手順

ステップ 1 システム（⚙） > **[構成（Configuration）]**を選択します。
ステップ 2 [言語（Language）] をクリックします。
ステップ 3 使用する言語を選択します。
ステップ 4 [保存（Save）] をクリックします。

ログイン バナー

[ログイン バナー（Login Banner）] ページを使用して、セキュリティ アプライアンスまたは共有ポリシーのセッション バナー、ログイン バナー、カスタム メッセージ バナーを指定できます。

カスタムログインバナーを作成するには、ASCII 文字と改行を使用できます。タブによるスペース設定は維持されません。ログイン バナーが大きすぎる場合や、エラーの原因となる場

合、システムがバナーを表示しようとすると、TelnetまたはSSHセッションが失敗することがあります。

ログイン バナーのカスタマイズ

手順

ステップ 1 システム（⚙）>**[構成（Configuration）]**を選択します。

ステップ 2 [ログイン バナー（Login Banner）] を選択します。

ステップ 3 [カスタム ログイン バナー（Custom Login Banner）] フィールドに、使用するログイン バナー テキストを入力します。

ステップ 4 [保存（Save）] をクリックします。

管理インターフェイス

セットアップの完了後、管理ネットワーク設定を変更することができます。これには、Management Center での管理インターフェイス、ホスト名、検索ドメイン、DNS サーバー、HTTP プロキシの追加が含まれます。

Management Center 管理インターフェイスについて

デフォルトでは、Management Center はすべてのデバイスを 1 つの管理インターフェイス上で制御します。また、初期設定や、管理者として Management Center にログインする際にも管理インターフェイスで行うことができます。管理インターフェイスは、スマートライセンスサーバーとの通信、更新プログラムのダウンロード、その他の管理機能の実行にも使用します。

デバイス管理インターフェイスについては、Cisco Secure Firewall Management Center デバイス構成ガイドの「*About Device Management Interfaces*」を参照してください。

デバイス管理について

Management Center がデバイスを管理するときは、デバイスとの間に、双方向の SSL 暗号化通信チャネルをセットアップします。Management Center はこのチャネルを使用して、そのデバイスへのネットワーク トラフィックの分析および管理の方法に関する情報をそのデバイスに送信します。そのデバイスはトラフィックを評価すると、イベントを生成し、同じチャネルを使用してそれらのイベントを Management Center に送信します。

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

- すべてのデバイスのポリシーを一箇所から設定できるため、設定の変更が容易になります。

- さまざまなタイプのソフトウェア アップデートをデバイスにインストールできます。
- 正常性ポリシーを管理対象デバイスに適用して、Management Center からデバイスのヘルス ステータスをモニターできます。

（注） CDO 管理対象デバイスがあり、オンプレミス Management Center を分析のみに使用している場合、オンプレミス Management Center はポリシーの設定またはアップグレードをサポートしません。デバイス設定およびその他のサポートされていない機能に関連するこのガイドの章と手順は、プライマリマネージャが CDO のデバイスには適用されません。

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

Management Center を使用することで、デバイス動作のほぼすべての側面を管理できます。

（注） Management Center は、http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html で入手可能な互換性マトリックスで指定されている特定の以前のリリースを実行しているデバイスを管理できますが、これらの以前のリリースのデバイスでは、最新バージョンの Threat Defense ソフトウェアが必要な新しい機能は利用できません。一部の Management Center 機能は、以前のバージョンで使用できる場合があります。

管理接続

Management Center 情報を使用してデバイスを設定し、デバイスを Management Center に追加した後に、デバイスまたは Management Center のいずれかで管理接続を確立できます。初期設定に応じて、以下のようになります。

- デバイスまたは Management Center のいずれかから開始できる。
- デバイスのみが開始できる。
- Management Center のみが開始できる。

初期化は常に Management Center の eth0 またはデバイスの最も番号が小さい管理インターフェイスから始まります。接続が確立されていない場合は、追加の管理インターフェースが試行されます。Management Center の複数の管理インターフェイスにより、個別のネットワークに接続したり、管理トラフィックとイベントトラフィックを分離したりできます。ただし、イニシエータは、ルーティングテーブルに基づいて最適なインターフェイスを選択しません。

管理接続が安定しており、過度なパケット損失がなく、少なくとも 5 Mbps のスループットがあることを確認します。

（注） 管理接続は、それ自身とデバイスの間の安全な TLS-1.3 暗号化通信チャネルです。セキュリティ上の理由から、サイト間 VPN などの追加の暗号化トンネル経由でこのトラフィックを実行する必要はありません。たとえば、VPNがダウンすると、管理接続が失われるため、シンプルな管理パスをお勧めします。

Management Center 上の管理インターフェイス

Management Center では、初期セットアップ、管理者の HTTP アクセス、デバイスの管理、ならびにその他の管理機能（ライセンス管理や更新など）に、eth0インターフェイスが使用されます。

追加の管理インターフェイスを設定することもできます。Management Centerがさまざまなネットワーク上で多数のデバイスを管理している場合、管理インターフェイスをさらに追加することで、スループットとパフォーマンスの向上につながります。これらの管理インターフェイスをその他すべての管理機能に使用することもできます。管理インターフェイスごとに、対応する機能を限定することをお勧めします。たとえば、ある特定の管理インターフェイスを HTTP 管理者アクセス用に使用し、別の管理インターフェイスをデバイスの管理に使用するなどです。

デバイス管理用に、管理インターフェイスには 2 つの別個のトラフィック チャネルがあります。管理トラフィック チャネルはすべての内部トラフィック（デバイス管理に固有のデバイス間トラフィックなど）を伝送し、イベントトラフィック チャネルはすべてイベントトラフィック（Web イベントなど）を伝送します。オプションで、Management Center 上にイベントを処理するためのイベント専用インターフェイスを別個に設定することもできます。設定できるイベント専用インターフェイスは1つだけです。管理トラフィックチャネルの管理インターフェイスも常に必要です。イベントトラフィックは大量の帯域幅を使用する可能性があるので、管理トラフィックからイベント トラフィックを分離することで、Management Center のパフォーマンスを向上させることができます。たとえば、10 GigabitEthernet インターフェイスをイベント インターフェイスとして割り当て、可能なら、1 GigabitEthernet インターフェイスを管理用に使用します。たとえば、イベント専用インターフェイスは完全にセキュアなプライベートネットワーク上に設定し、通常の管理インターフェイスはインターネットにアクセスできるネットワーク上で使用することをお勧めします。同じネットワークで管理インターフェイスとイベントインターフェイスの両方を使用することもできますが、他のデバイスからManagement Centerへのルーティングの問題など、潜在的なルーティングの問題を回避するために、各インターフェイスを個別のネットワークに配置することをお勧めします。管理対象デバイスは、管理トラフィックを Management Center の管理インターフェイスに送信し、イベントトラフィックを Management Center のイベント専用インターフェイスに送信します。管理対象デバイスがイベント専用インターフェイスに到達できない場合、フォールバックして管理インターフェイスにイベントを送信します。ただし、イベント専用インターフェイスを介して管理接続を確立することはできません。

Management Centerからの管理接続の初期化は、常にeth0から試行され、その後に他のインターフェイスが順番に試行されます。ルーティングテーブルは、最適なインターフェイスの決定には使用されません。

（注） すべての管理インターフェイスは、アクセスリスト設定による制御に従ってHTTP管理者アクセスをサポートしています（アクセス リストの設定 （49 ページ））。逆に、インターフェイスをHTTPアクセスのみに制限することはできません。管理インターフェイスでは、常にデバイス管理がサポートされます（管理トラフィック、イベントトラフィック、またはその両方）。

（注） eth0 インターフェイスのみが DHCP IP アドレスをサポートします。他の管理インターフェイスはスタティック IP アドレスのみをサポートします。

Management Center モデルごとの管理インターフェイスサポート

管理インターフェイスの場所については、ご使用のモデルのハードウェアインストレーションガイドを参照してください。

各 Management Center モデルでサポートされる管理インターフェイスについては、以下の表を参照してください。

表 *2 : Management Center* でサポートされる管理インターフェイス

モデル	管理インターフェイス
MC1000	eth0（デフォルト） eth1
MC2500、MC4500	eth0（デフォルト） eth1 eth2 eth3
MC1600、MC2600、MC4600	eth0（デフォルト） eth1 eth2 eth3 CIMC（Lights-Out Management でのみサポート）

モデル	管理インターフェイス
FMC1700、FMC2700、FMC4700	eth0（デフォルト） eth1 eth2 eth3 CIMC（Lights-Out Management でのみサポート）
Management Center Virtual	eth0（デフォルト）

Management Center 管理インターフェイス上のネットワークルート

管理インターフェイス（イベント専用インターフェイスを含む）は、リモートネットワークに到達するためのスタティック ルートのみをサポートしています。Management Center をセットアップすると、セットアッププロセスにより、指定したゲートウェイ IP アドレスへのデフォルトルートが作成されます。このルートを削除することはできません。また、このルートで変更できるのはゲートウェイ アドレスのみです。

一部のプラットフォームでは、複数の管理インターフェイスを設定できます。デフォルトルートには出力インターフェイスが含まれていないため、選択されるインターフェイスは、指定したゲートウェイアドレスと、ゲートウェイが属するインターフェイスのネットワークによって異なります。デフォルトネットワーク上に複数のインターフェイスがある場合、デバイスは出力インターフェイスとして番号の小さいインターフェイスを使用します。

リモートネットワークにアクセスするには、管理インターフェイスごとに1つ以上のスタティックルートを使用することをお勧めします。他のデバイスから Management Center へのルーティングの問題など、潜在的なルーティングの問題を回避するために、各インターフェイスを個別のネットワークに配置することをお勧めします。

（注） 管理接続に使用されるインターフェイスは、ルーティングテーブルによって決定されません。接続は常に最初に eth0 を使用して試行され、その後、管理対象デバイスに到達するまで、後続のインターフェイスが順番に試行されます。

NAT 環境

ネットワーク アドレス変換（NAT）とは、ルータを介したネットワーク トラフィックの送受信方式であり、送信元または宛先 IP アドレスの再割り当てが行われます。NAT の最も一般的な用途は、プライベートネットワークがインターネットと通信できるようにすることです。スタティック NAT は 1:1 変換を実行し、デバイスとの Management Center 通信に支障はありませんが、ポート アドレス変換（PAT）がより一般的です。PAT では、単一のパブリック IP アドレスと一意のポートを使用してパブリック ネットワークにアクセスできます。これらのポート

は必要に応じて動的に割り当てられるため、PAT ルータの背後にあるデバイスへの接続は開始できません。

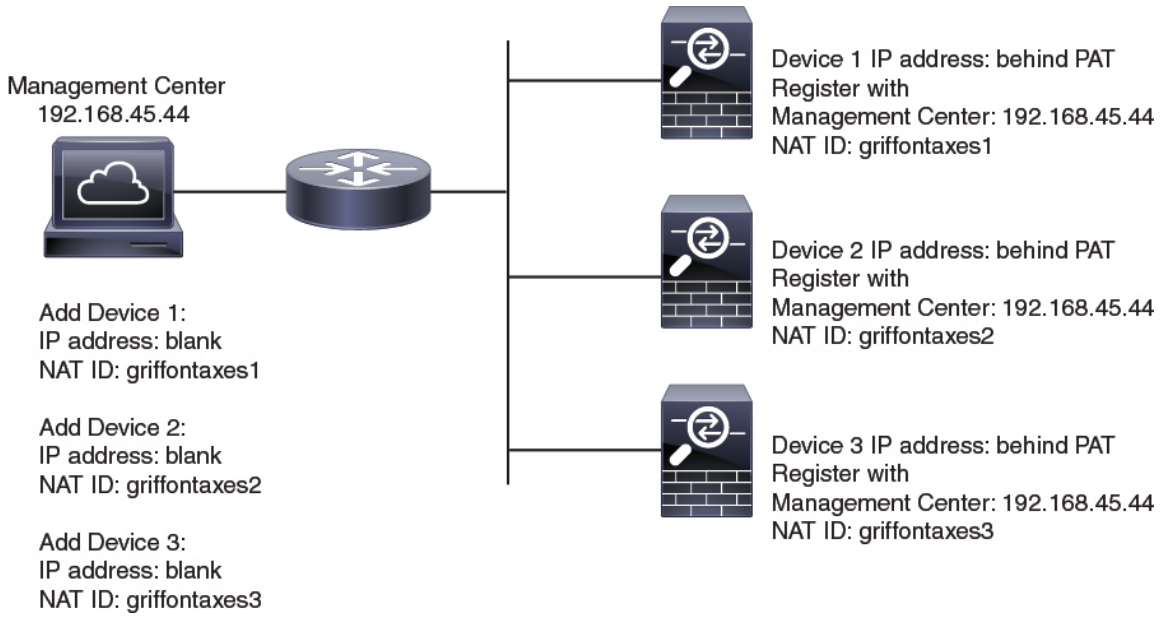
通常は、ルーティングと認証の両方の目的で両方の IP アドレス（登録キー付き）が必要です。デバイスを追加するときに、Management Center がデバイスの IP アドレスを指定し、デバイスが Management Center の IP アドレスを指定します。ただし、IP アドレスの 1 つのみがわかっている場合（ルーティング目的の最小要件）は、最初の通信用に信頼を確立して正しい登録キーを検索するために、接続の両側に一意の NAT ID を指定する必要もあります。Management Center およびデバイスでは、初期登録の認証と承認を行うために、登録キーおよび NAT ID（IP アドレスではなく）を使用します。

たとえば、デバイスを Management Center に追加したときにデバイスの IP アドレスがわからない場合（たとえばデバイスが PAT ルータの背後にある場合）は、NAT ID と登録キーのみを Management Center に指定します。IP アドレスは空白のままにします。デバイス上で、Management Center の IP アドレス、同じ NAT ID、および同じ登録キーを指定します。デバイスが Management Center の IP アドレスに登録されます。この時点で、Management Center は IP アドレスの代わりに NAT ID を使用してデバイスを認証します。

NAT 環境では NAT ID を使用するのが最も一般的ですが、NAT ID を使用することで、多数のデバイスを簡単に Management Center に追加することができます。Management Center で、追加するデバイスごとに IP アドレスは空白のままにして一意の NAT ID を指定し、次に各デバイスで、Management Center の IP アドレスと NAT ID の両方を指定します。注：NAT ID はデバイスごとに一意でなければなりません。

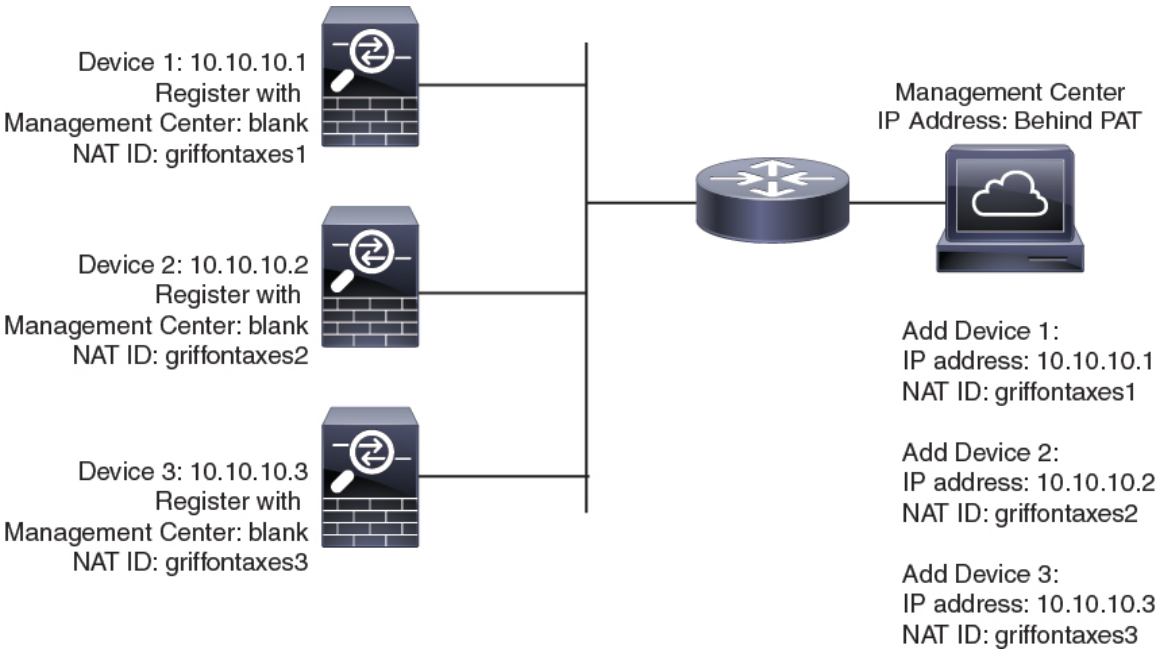
次の例に、PAT IP アドレスの背後にある 3 台のデバイスを示します。この場合、Management Center とデバイスの両方でデバイスごとに一意の NAT ID を指定し、デバイス上の Management Center の IP アドレスを指定します。

図 *2 : PAT* の背後にある管理対象デバイスの *NAT ID*



次の例に、PAT IP アドレスの背後にある Management Center を示します。この場合、Management Center とデバイスの両方でデバイスごとに一意の NAT ID を指定し、Management Center 上のデバイスの IP アドレスを指定します。

図 *3 : PAT* の背後にある *Management Center* の *NAT ID*

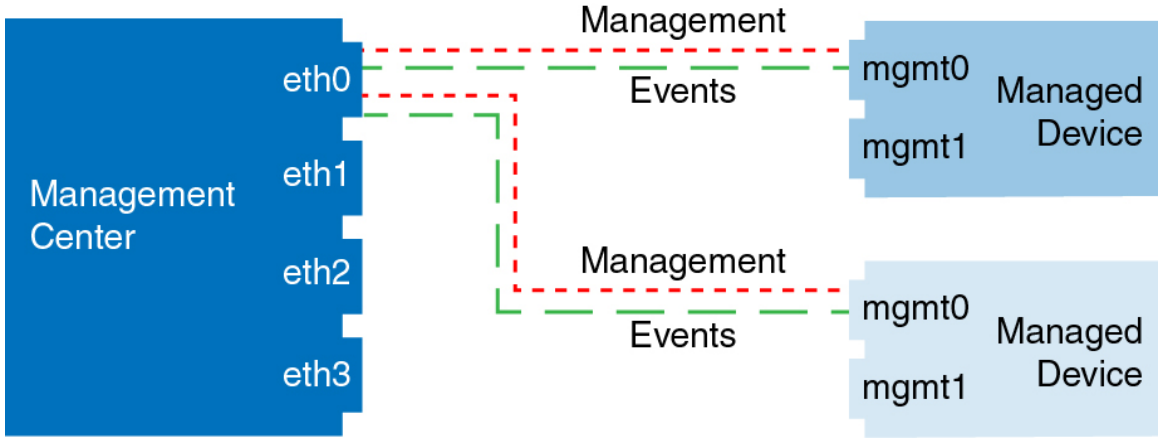


管理およびイベント トラフィック チャネルの例

（注） 管理用のデータインターフェイスを Threat Defense で使用する場合は、そのデバイスに個別の管理インターフェイスとイベントインターフェイスを使用することはできません。

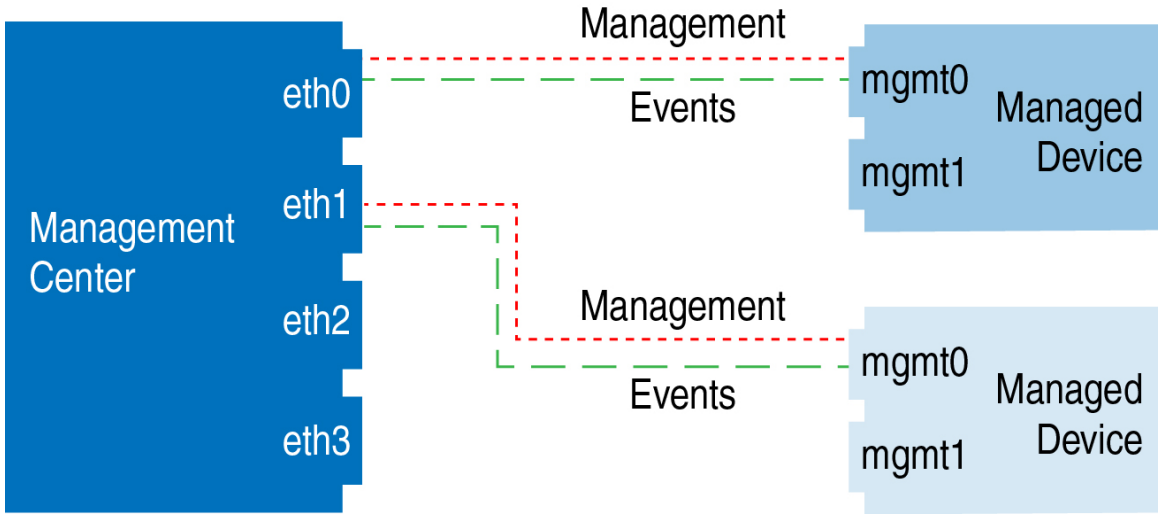
以下に、Management Center と管理対象デバイスでデフォルト管理インターフェイスのみを使用する例を示します。

図 *4 : Secure Firewall Management Center* 上で単一の管理インターフェイスを使用する場合



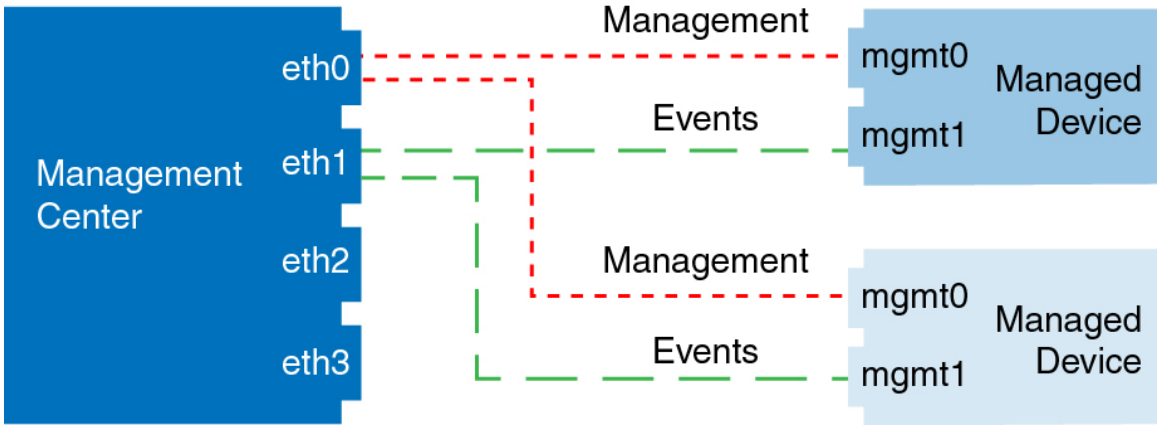
以下に、Management Center でデバイスごとに別個の管理インターフェイスを使用する例を示します。この場合、各管理対象デバイスが 1 つの管理インターフェイスを使用します。

図 *5 : Secure Firewall Management Center* の複数の管理インターフェイス



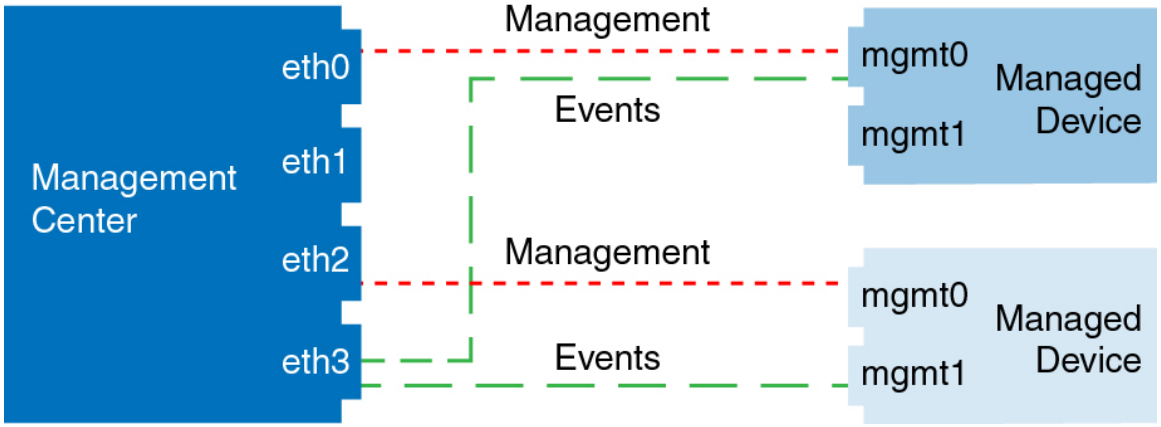
以下に、個別のイベント インターフェイスを使用する Management Center と管理対象デバイスの例を示します。

図 *6 : Secure Firewall Management Center*上の個別のイベント インターフェイスと管理対象デバイスを使用する場合



以下に、Management Center 上で複数の管理インターフェイスと個別のイベント インターフェイスが混在し、個別のイベントインターフェイスを使用する管理対象デバイスと単一の管理インターフェイスを使用する管理対象デバイスが混在する例を示します。

図 *7 :* 管理インターフェイスとイベント インターフェイスを混在させて使用する場合



Management Center 管理インターフェイスの変更

Management Center で管理インターフェイスの設定を変更します。オプションとして追加の管理インターフェイスを有効にしたり、イベントのみのインターフェイスを設定したりできます。

⚠

注意 接続されている管理インターフェイスを変更する場合は十分にご注意ください。設定エラーのために再接続できない場合は、Management Center コンソール ポートにアクセスして、Linux シェルでネットワーク設定を再設定する必要があります。この操作では、Cisco TAC に連絡する必要があります。

Management Center の IP アドレスを変更する場合は、Cisco Secure Firewall Management Center デバイス構成ガイド で『*Edit the Management Center IP Address or Hostname on the Device*』を参照してください。Management Center の IP アドレスまたはホスト名を変更する場合は、設定が一致するようにデバイス CLI で値を変更する必要があります。ほとんどの場合、管理接続はデバイスの Management Center IP アドレスまたはホスト名を変更せずに再確立されますが、少なくともデバイスを Management Center に追加して NAT ID のみを指定した場合は、接続が再確立されるようにするために、このタスクを実行する必要があります。他の場合でも、Management Center IP アドレスまたはホスト名を最新の状態に維持して、ネットワークの復元力を高めることを推奨します。

高可用性構成では、登録されたデバイスの管理 IP アドレスをデバイスの CLI または Management Center から変更した場合、HA 同期後も、セカンダリ Management Center には変更が反映されません。セカンダリ Management Center も更新されるようにするには、2 つの Management Center の間でロールを切り替えて、セカンダリ Management Center をアクティブユニットにします。現在アクティブな Management Center の [デバイス管理（Device Management）] ページで、登録されているデバイスの管理 IP アドレスを変更します。

始める前に

- デバイス管理の仕組みについては、Cisco Secure Firewall Management Center デバイス構成ガイドで『*About Device Management Interfaces*』を参照してください。
- プロキシを使用する場合：
  - NT LAN Manager（NTLM）認証を使用するプロキシはサポートされません。
  - スマートライセンスを使用しているか、または使用する予定がある場合は、プロキシの FQDN は 64 文字以内にする必要があります。

手順

ステップ 1 **システム**（⚙）**>[構成（Configuration）]** を選択し、次に [管理インターフェイス（Management Interfaces）] を選択します。

ステップ 2 [インターフェイス（Interfaces）] エリアで、設定するインターフェイスの横にある [編集（Edit）] をクリックします。

このセクションでは、利用可能なすべてのインターフェイスがリストされます。インターフェイスをさらに追加することはできません。

それぞれの管理インターフェイスに対して、以下のオプションを設定できます。

- [有効にする（Enabled）]：管理インターフェイスを有効にします。デフォルト eth0 管理インターフェイスを無効にしないでください。eth0 インターフェイスを必要とするプロセスもあります。
- [チャネル（Channels）]：[管理トラフィック（Management Traffic）] が有効になっているインターフェイスが常に少なくとも 1 つ必要です。必要に応じて、イベント専用インターフェイスを設定できます。Management Center で設定できるイベントインターフェイスは

1 つだけです。これを設定するには、[管理トラフィック（Management Traffic）] チェックボックスをオフにして、[イベント トラフィック（Event Traffic）] チェックボックスをオンのままにしておきます。必要に応じて、管理インターフェイスの [イベントトラフィック（Event Traffic）] を無効にすることができます。いずれの場合も、デバイスは、イベントのみのインターフェイスにイベントを送信しようとします。そのインターフェイスがダウンしていた場合は、イベントチャネルが無効になっていても、管理インターフェイス上でイベントを送信します。インターフェイス上でイベントチャネルと管理チャンネルの両方を無効にすることはできません。

- [モード（Mode）]：リンク モードを指定します。ギガビット イーサネット インターフェイスでは、自動ネゴシエーションの値を変更しても反映されないことに注意してください。
- [MDI/MDIX]：[自動-MDIX（Auto-MDIX）] を設定します。
- [MTU]：1280 ～ 1500 の最大伝送ユニット（MTU）を設定します。デフォルトは 1500 です。
- [IPv4 設定（IPv4 Configuration）]：IPv4 IP アドレスを設定します。次のどちらかを選択します。
  - [スタティック（Static）]：**IPv4 の管理 IP アドレス** と**ネットマスク**を手動で入力します。
  - [DHCP]：DHCP を使用するインターフェイスを設定します（eth0 のみ）。

    DHCP を使用する場合は、割り当てられたアドレスが変更されないように、DHCP 予約を使用する必要があります。DHCP アドレスが変更されると、Management Center ネットワーク設定が同期しなくなるため、デバイスの登録は失敗します。DHCPアドレスの変更から回復するには、Management Center に接続し（ホスト名または新しい IP アドレスを使用）、**システム**（⚙）>**[構成（Configuration）]**>[管理インターフェイス（Management Interfaces）] の順に選択してネットワークをリセットします。
  - [無効（Disabled）]：無効 IPv4。IPv4 と IPv6 の両方を無効に**しないでください**。
- [IPv6 設定（IPv6 Configuration）]：IPv6 IP アドレスを設定します。次のどちらかを選択します。
  - [スタティック（Static）]：**IPv6 の管理 IP アドレス**と **IPv6 のプレフィックス長**を手動で入力します。
  - [DHCP]：DHCPv6 を使用するインターフェイスを設定します（eth0 のみ）。
  - [ルータ割当て（Router Assigned）]：ステートレス自動設定を有効にします。
  - [無効（Disabled）]：IPv6 を無効にします。IPv4 と IPv6 の両方を無効に**しないでください**。
  - [IPv6 DAD]：IPv6 を有効にするときに [重複アドレス検出（DAD）] を有効または無効にします。DAD を使用することによってサービス拒否攻撃の可能性が拡大するため、DAD は無効にすることができます。この設定を無効にした場合は、すでに割り

当てられているアドレスがこのインターフェイスで使用されていないことを手動で確認する必要があります。

ステップ 3 [ルート（Routes）] エリアで、静的ルートを **[編集（Edit）]**（ ） をクリックして編集するか、または **Add** ( ) をクリックして追加します。

をクリックしてルートテーブルを表示します。

追加の各インターフェイスがリモート ネットワークに到達するには、スタティック ルートが必要です。新しいルートが必要な場合については、Management Center 管理インターフェイス上のネットワークルート （88 ページ）を参照してください。

（注） デフォルト ルートでは、ゲートウェイ IP アドレスのみを変更できます。出力インターフェイスは、指定したゲートウェイをインターフェイスのネットワークに照合することで自動的に選択されます。

次の設定をスタティック ルートに対して設定できます。

- [宛先（Destination）]：ルートを作成する宛先ネットワークのアドレスを設定します。
- [ネットマスク（Netmask）] または [プレフィックス長（Prefix Length）]：ネットワークのネットマスク（IPv4）またはプレフィックス長（IPv6）を設定します。
- [インターフェイス（Interface）]：出力管理インターフェイスを設定します。
- [ゲートウェイ（Gateway）]：ゲートウェイ IP アドレスを設定します。

ステップ 4 [共有設定（Shared Settings）] エリアで、すべてのインターフェイスで共有されているネットワーク パラメータを設定します。

（注） eth0 インターフェイスで [DHCP] を選択すると、DHCP サーバから取得する共有設定の一部を手動で指定することができなくなります。

次の共有設定を行うことができます。

- [ホスト名（Hostname）]：Management Center ホスト名を設定します。ホスト名は最大 64 文字を使用でき、アルファベットまたは数字で開始および終了する必要があります。使用できるのはアルファベット、数字、ハイフンのみです。ホスト名を変更する場合、syslog メッセージに反映される新しいホスト名を使用するには、Management Center を再起動します。再起動するまでは、新しいホスト名が Syslog メッセージに反映されません。
- [ドメイン（Domains）]：カンマで区切られた、Management Center の検索ドメインを設定します。これらのドメインは、コマンド（**ping system** など）に完全修飾ドメイン名を指定しない場合にホスト名に追加されます。ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。
- [プライマリ DNS サーバー（Primary DNS Serve）]、[セカンダリ DNS サーバー（Secondary DNS Server）]、[ターシャリ DNS サーバー（Tertiary DNS Server）]：優先度順に使用される DNS サーバーを設定します。

- [リモート管理ポート（Remote Management Port）]：管理対象デバイスとの通信用のリモート管理ポートを設定します。Management Center および管理対象デバイスは、双方向の SSL 暗号化通信チャネル（デフォルトではポート 8305）を使用して通信します。

  （注） シスコは、リモート管理ポートをデフォルト設定のままにしておくことを**強く**推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、導入内の相互に通信する必要がある**すべての**デバイスの管理ポートを変更する必要があります。

ステップ 5 [ICMPv6] 領域で、ICMPv6 の設定を行います。

- [エコー応答パケットの送信を許可する（Allow Sending Echo Reply Packets）]：エコー応答パケットを有効または無効にします。これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。エコー応答パケットを無効にすると、Management Center の管理インターフェイスにテスト目的で IPv6 ping を使用できなくなります。
- [宛先到達不能パケットの送信を許可する（Allow Sending Destination Unreachable Packets）]：宛先到達不能パケットを有効または無効にします。これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。

ステップ 6 [プロキシ（Proxy）] エリアで、HTTP プロキシ設定をします。

Management Center は、ポート TCP/443（HTTPS）および TCP/80（HTTP）でインターネットに直接接続するように構成されています。HTTP ダイジェスト経由で認証できるプロキシ サーバーを使用できます。

このトピックの前提条件のプロキシの要件を参照してください。

a) [有効（Enabled）] チェックボックスをオンにします。
b) [HTTP プロキシ（HTTP Proxy）] フィールドに、プロキシ サーバの IP アドレスまたは完全修飾ドメイン名を入力します。

   このトピックの前提条件の要件を参照してください。

c) [ポート（Port）] フィールドに、ポート番号を入力します。
d) [プロキシ認証の使用（Use Proxy Authentication）] を選択してから [ユーザ名（User Name）] と [パスワード（Password）] を入力して、認証資格情報を設定します。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 Management Center の IP アドレスを変更する場合は、Management Center の IP アドレスを変更する場合は、Cisco Secure Firewall Management Center デバイス構成ガイド で『*Edit the Management Center IP Address or Hostname on the Device*』を参照してください。

Management Center の IP アドレスまたはホスト名を変更する場合は、設定が一致するようにデバイス CLI で値を変更する必要があります。ほとんどの場合、管理接続はデバイスの Management Center IP アドレスまたはホスト名を変更せずに再確立されますが、少なくともデバイスを Management Center に追加して NAT ID のみを指定した場合は、接続が再確立されるようにするために、このタスクを実行する必要があります。他の場合でも、Management Center IP アドレ

スまたはホスト名を最新の状態に維持して、ネットワークの復元力を高めることを推奨します。

Management Center と Threat Defense の両 IP アドレスの変更

Management Center と Threat Defense の IP アドレスを新しいネットワークに移動する場合は、両方を変更することをお勧めします。

手順

ステップ 1 管理接続を無効にします。

高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

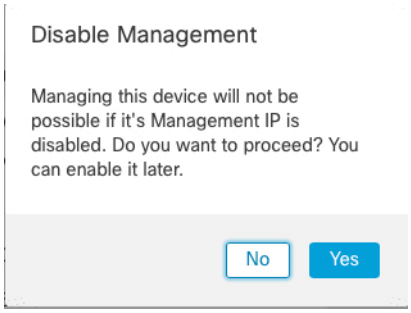
b) デバイスの横にある **[編集（Edit）]**（ ） をクリックします。

c) [Device] をクリックし、[Management] 領域を表示します。

d) スライダをクリックして管理を一時的に無効にすることで、（ ）を無効化します。

図 *8*: 管理を無効にする

管理の無効化を続行するように求められます。 [Yes] をクリックします。



ステップ 2 Management Center 内のデバイスの IP アドレスを新しいデバイスの IP アドレスに変更します。

デバイスの IP アドレスは後で変更します。

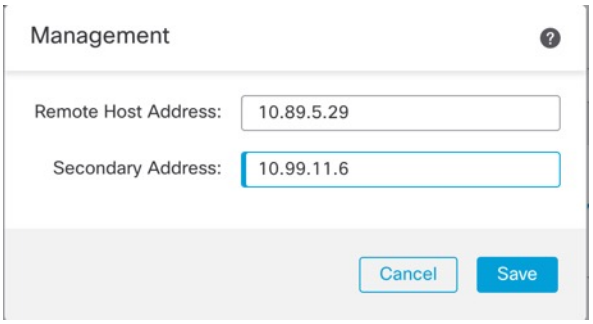
高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

a) **[リモートホストアドレス（Remote Host Address）]** の IP アドレスおよびオプションの [セカンダリアドレス（Secondary Address）]（冗長データインターフェイスを使用する場合）または **[編集（Edit）]**（）をクリックしてホスト名を編集します。

図 *9*：管理アドレスの編集

b) [管理（Management）] ダイアログボックスの **[リモートホストアドレス（Remote Host Address）]** フィールドおよびオプションの [セカンダリアドレス（Secondary Address）] フィールドで名前または IP アドレスを変更し、[保存（Save）] をクリックします。

図 *10*：管理 *IP* アドレス



ステップ 3 Management Center の IP アドレスを変更してください。

注意 Management Center インターフェイスを変更する場合は十分にご注意ください。設定エラーのために再接続できない場合は、Management Center コンソールポートにアクセスして、Linux シェルでネットワーク設定を再設定する必要があります。この操作では、Cisco TAC に連絡する必要があります。

a) **システム（）** > **[構成（Configuration）]** を選択し、次に [管理インターフェイス（Management Interfaces）] を選択します。
b) [インターフェイス（Interfaces）] エリアで、設定するインターフェイスの横にある [編集（Edit）] をクリックします。
c) IP アドレスを変更し、[保存（Save）] をクリックします。

ステップ 4 デバイスのマネージャ IP アドレスを変更します。

高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

a) Threat Defense CLI で、Management Center 識別子を表示します。

show managers

例：

```
> show managers
Type                    : Manager
Host                    : 10.10.1.4
Display name            : 10.10.1.4
Identifier              : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration            : Completed
Management type         : Configuration
```

b) Management Center IP アドレスまたはホスト名を編集します。

configure manager edit *identifier* {**hostname** {*ip_address* | *hostname*} | **displayname** *display_name*}

Management Center が **DONTRESOLVE** と NAT ID によって最初に識別された場合、このコマンドを使用して値をホスト名または IP アドレスに変更できます。IP アドレスまたはホスト名を **DONTRESOLVE** に変更することはできません。

例：

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

ステップ 5 コンソールポートでマネージャ アクセス インターフェイスの IP アドレスを変更します。

高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

専用管理インターフェイスを使用している場合：

configure network ipv4

configure network ipv6

専用管理インターフェイスを使用している場合：

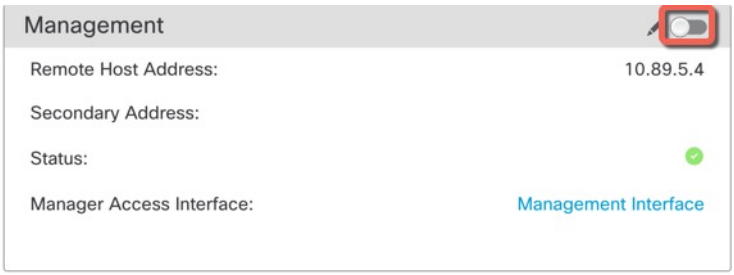
configure network management-data-interface disable

configure network management-data-interface

ステップ 6 スライダをクリックして管理を再度有効（ ）にします。

高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

図 *11* : 管理接続の有効化



ステップ 7 （マネージャアクセスにデータインターフェイスを使用している場合）Management Center でデータインターフェイス設定を更新します。

高可用性ペアの場合は、両方のユニットでこの手順を実行します。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [管理（Management）] > [マネージャアクセス - 構成詳細（Manager Access - Configuration Details）]** を選択し、[更新（Refresh）] をクリックします。
b) **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）]** を選択し、新しいアドレスと一致するように IP アドレスを設定します。
c) [マネージャアクセス - 構成詳細（Manager Access - Configuration Details）] [FMCアクセス - 構成詳細（FMC Access - Configuration Details] ダイアログボックスに戻り、[確認（Acknowledge）] をクリックして展開ブロックを削除します。

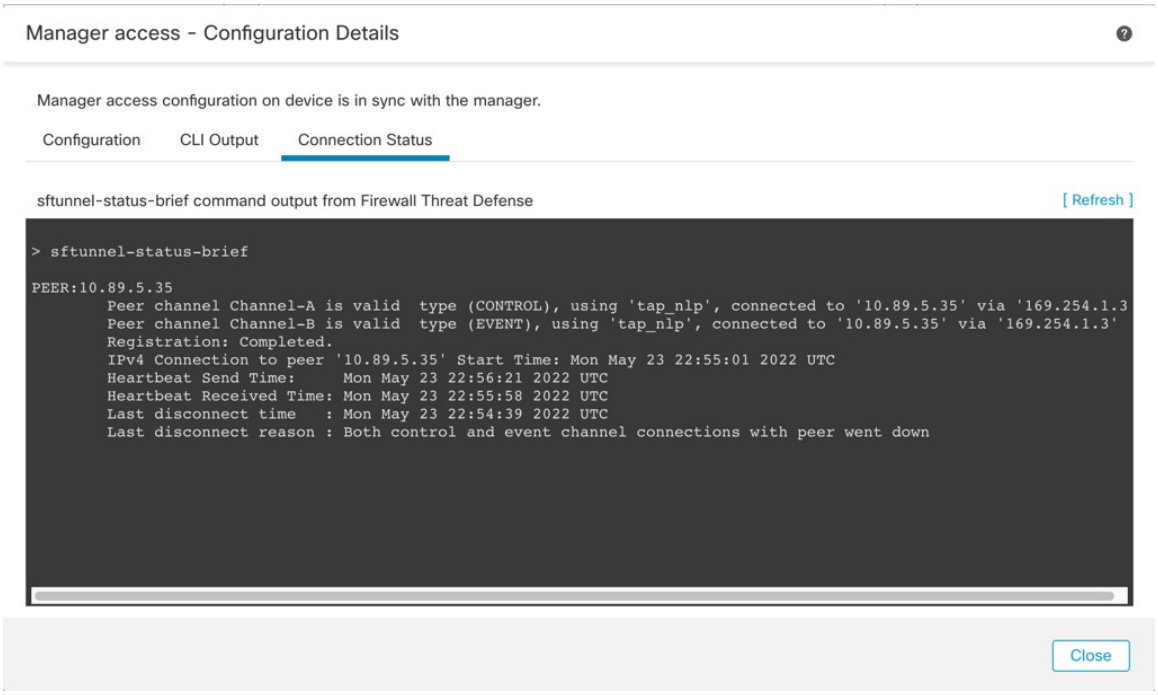
ステップ 8 管理接続が再確立されたことを確認します。

Management Center で、[Devices] [Device Management] [Device] [Management] [Manager Access - Configuration Details] [FMC Access - Configuration Details] [Connection Status] ページで管理接続ステータスを確認します。

管理接続のステータスを表示するには、Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。

次のステータスは、データインターフェイスの接続が成功したことを示し、内部の「tap_nlp」インターフェイスを示しています。

図 *12*：接続ステータス



ステップ 9 （高可用性 Management Center ペアの場合）セカンダリ Management Center で設定変更を繰り返します。

a) セカンダリ Management Center IP アドレスを変更します。
b) 両方のユニットで新しいピアアドレスを指定します。

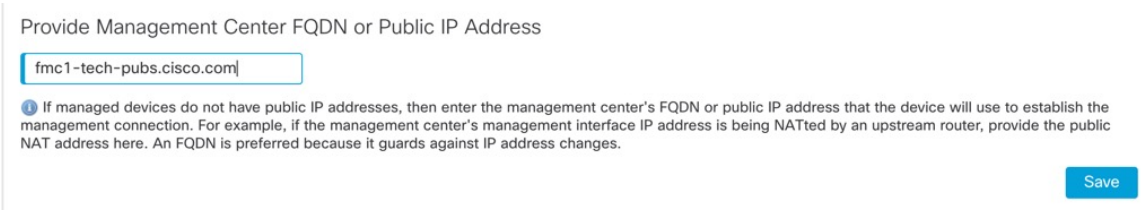
c) セカンダリユニットをアクティブユニットにします。
d) デバイスの管理接続を無効にします。
e) Management Center でデバイスの IP アドレスを変更します。
f) 管理接続を再度有効にします。

マネージャのリモートアクセス

管理対象デバイスにパブリック IP アドレスがない場合は、デバイスが管理接続を確立するために使用する Management Center の FQDN またはパブリック IP アドレスを入力します。たとえば、Management Center の管理インターフェイスの IP アドレスが上流のルータによって NAT されている場合は、ここにパブリック NAT アドレスを入力します。IP アドレスの変更を防ぐため、FQDN が優先されます。

シリアル番号（ゼロタッチプロビジョニング）方式を使用してデバイスを登録する場合、このフィールドはマネージャの IP アドレス/ホスト名の初期設定に自動的に使用されます。手動方式を使用する場合は、デバイスの初期設定を実行するときにこの画面の値を参照すると、パブリック Management Center IP アドレス/ホスト名を特定できます。

図 *13*：マネージャのリモートアクセス



ネットワーク分析ポリシーの設定

ユーザーがネットワーク分析ポリシーを変更した場合、ポリシー関連の変更をコメント機能を使用してトラッキングするようにシステムを設定できます。ポリシー変更のコメントが有効にされていると、管理者はコメントにアクセスして、導入で重要なポリシーが変更された理由を素早く評価できます。

ポリシーの変更に関するコメントを有効にした場合、コメントをオプションまたは必須に設定できます。システムは、ポリシーに対する新しい変更が保存されるたびに、ユーザにコメントを入力するようプロンプトを出します。

オプションで、ネットワーク分析ポリシーに対する変更を監査ログに書き込むこともできます。

プロセス

Management Center のプロセスのシャットダウンおよび再起動を制御するには、Web インターフェイスを使用します。次の操作を実行できます。

- シャットダウン：アプライアンスのグレースフル シャットダウンを開始します。

注意 電源ボタンを使用して Cisco Secure Firewall アプライアンスを停止しないでください。データが失われる可能性があります。Web インターフェイス（または CLI）を使用すると、設定データを失うことなく、安全にシステムの電源を切って再起動する準備が整います。

- リブート：シャットダウンしてグレースフルに再起動します。
- コンソールの再起動：通信、データベース、HTTP サーバーのプロセスを再起動します。これは通常、トラブルシューティングの際に使用されます。

ヒント 仮想デバイスの場合は、ご使用の仮想プラットフォームのマニュアルを参照してください。特に VMware の場合、カスタム電源オプションは VMware ツールの一部です。

Management Center のシャットダウンまたは再起動

手順

ステップ 1 **システム**（⚙）> **[構成（Configuration）]**を選択します。

ステップ 2 [プロセス（Process）] を選択します。

ステップ 3 次のいずれかを実行します。

シャットダウン	[管理センターのシャットダウン（Shutdown Management Center）] の横にある [コマンドの実行（Run Command）] をクリックします。
再起動	[管理センターの再起動（Reboot Management Center）] の横にある [コマンドの実行（Run Command）] をクリックします。 （注） 再起動するとログアウトします。システムはデータベースチェックを実行しますが、これは完了するのに 1 時間かかります。

コンソールの再起動	[管理センターコンソールの再起動（Restart Management Center Console）] の横にある [コマンドの実行（Run Command）] をクリックします。 （注） 再起動すると、ネットワーク マップ内に削除されたホストが再表示されることがあります。

REST API 設定

Management Center の REST API は、サードパーティ アプリケーションで REST クライアントおよび標準 HTTP メソッドを使用してデバイス設定を表示および管理するための軽量のインターフェイスを提供します。Management Center の REST API の詳細については、Cisco Secure Firewall Management Center REST API クイックスタートガイド を参照してください。

（注） HTTPS 証明書は、Management Center の REST API ではサポートされていません。

デフォルトでは、Management Center はアプリケーションからの REST API を使用した要求を許可します。このアクセスをブロックするように Management Center を設定できます。

REST API アクセスの有効化

（注） Management Center 高可用性を使用する展開では、この機能は、アクティブな Management Center でのみ使用できます。

手順

ステップ 1 右上隅の**[Cog]**（⚙）を選択して、システムメニューを開きます。

ステップ 2 [REST API 設定（REST API Preferences）] をクリックします。

ステップ 3 Management Center への REST API アクセスを有効または無効にするには、[REST APIの有効化（Enable REST API）] チェックボックスをオンまたはオフにします。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 `https://<management_center_IP_or_name>:<https_port>/api/api-explorer` で API エクスプローラにアクセスします。

リモート コンソールのアクセス管理

サポート対象システム上でリモート アクセスを行うため、VGA ポート（デフォルト）または物理アプライアンス上のシリアル ポートを介して Linux システムのコンソールを使用できます。[コンソール設定（Console Configuration）] ページを使用して、組織の Cisco Secure Firewall 展開環境の物理レイアウトに最も適したオプションを選択します。

サポートされている物理ハードウェアベースのシステムでは、Serial Over LAN（SOL）接続で Lights-Out 管理（LOM）を使用すると、システムの管理インターフェイスにログインすることなく、リモートでシステムをモニターまたは管理できます。アウト オブ バンド管理接続のコマンドライン インターフェイスを使用すると、シャーシのシリアル番号の表示や状態（ファン速度や温度など）のモニタなどの、限定タスクを実行できます。LOM をサポートするケーブル接続は、Management Center モデルによって異なります。

- Management Center モデル MC1600、MC2600、および MC4600 では、CIMC ポートとの接続を使用して LOM をサポートします。詳細は、『*Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide*』を参照してください。
- 他のすべての Management Center ハードウェアモデルでは、LOM をサポートするためにデフォルト（eth0）管理ポートとの接続を使用します。ご使用のハードウェアモデルの『*Navigating the Cisco Secure Firewall Threat Defense Documentation Guide*』『』を参照してください。

LOM は、システムとシステムを管理するユーザーの両方で有効にする必要があります。システムとユーザーを有効にした後、サードパーティ製の Intelligent Platform Management Interface（IPMI）ユーティリティを使用し、システムにアクセスして管理します。

システム上のリモート コンソール設定の構成

この手順を実行するには、管理者ユーザーである必要があります。

始める前に

- デバイスの管理インターフェイスに接続されたサードパーティ スイッチング装置で、スパニング ツリー プロトコル（STP）を無効にします。
- Lights-Out 管理を有効にする予定がある場合、インテリジェント プラットフォーム管理インターフェイス（IPMI）ユーティリティのインストールと使用については、アプライアンスのスタートアップガイドを参照してください。

手順

ステップ 1 システム（⚙）> **[構成（Configuration）]**を選択します。

ステップ 2 [コンソール構成（Console Configuration）] をクリックします。

ステップ 3 リモート コンソール アクセスのオプションを選択します。

- アプライアンスの VGA ポートを使用するには、[VGA] を選択します。
- アプライアンスのシリアルポートを使用する場合には、[物理シリアルポート（Physical Serial Port）] を選択します。
- Management Center で SOL 接続を使用するには、[Lights-Out管理（Lights-Out Management）] を選択します。（お使いの Management Center モデルに応じて、デフォルトの管理ポートまたはCIMC ポートを使用する場合があります。詳細については、モデルのスタートアップガイドを参照してください）。

ステップ 4 SOL を介して LOM を構成するには：

- システムのアドレスの [構成（Configuration）]（[DHCP] または [Manual（手動）]）を選択します。
- 手動構成を選択した場合は、必要な IPv4 設定を入力します。
  - LOM に使用する IP アドレスを入力します。

    （注） LOM IP アドレスは、Management Center管理インターフェイスの IP アドレスとは異なり、かつ同じサブネット内にある必要があります。

  - システムのネットマスクを入力します。
  - システムのデフォルト ゲートウェイを入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 「これらの変更を有効にするためには、システムを再起動する必要があります（You will have to reboot your system for these changes to take effect）」という警告が表示されます。[OK] をクリックしてすぐに再起動するか、[キャンセル（Cancel）] をクリックして後で再起動します。

次のタスク

- シリアルアクセスを設定した場合は、背面パネルのシリアルポートが、ローカルコンピュータ、ターミナルサーバー、またはお使いの Management Center モデルのスタートアップガイドで説明されている、イーサネット経由のリモートシリアルアクセスをサポートできるその他のデバイスに接続されていることを確認します。
- Lights-Out Management を設定した場合は、Lights-Out Management ユーザーを有効にします。Lights-Out 管理のユーザー アクセス設定 （105 ページ）を参照してください。

Lights-Out 管理のユーザー アクセス設定

Lights-Out 管理機能を使用するユーザーに対して、この機能の権限を明示的に付与する必要があります。LOM ユーザーには、次のような制約もあります。

- ユーザーに Administrator ロールを割り当てる必要があります。
- ユーザー名に使用できるのは英数字 16 文字までです。LOM ユーザーに対し、ハイフンやそれより長いユーザー名はサポートされていません。
- ユーザーの LOM パスワードは、そのユーザーのシステム パスワードと同じです。パスワードは、ユーザパスワード（143 ページ）で説明されている要件に準拠している必要があります。辞書に載っていない複雑な最大長のパスワードをアプライアンスに対して使用し、それを 3 か月ごとに変更することを推奨します。
- 物理 Management Center には、最大 13 人の LOM ユーザーを設定できます。

あるユーザーのログイン中に LOM でそのユーザーを非アクティブ化してから再アクティブ化した場合、そのユーザーは `ipmitool` コマンドへのアクセスを回復するために Web インターフェイスへのログインし直しが必要になることがあります。

（注） 高可用性同期は LOM ユーザーには適用されないため、高可用性 Management Center ではそれらのユーザーが複製されません。アクティブな Management Center で LOM を有効にした別の管理者ユーザーを作成する必要があります。

高可用性構成で、ローカルユーザーを作成するか、LOM 権限が有効になっているローカルユーザーのパスワードをリセットすると、その変更が、UCS ベースのアクティブな Management Center から、アクティブおよびスタンバイの両方の Management Center とアクティブな Management Center CIMC に同期されます。新しいパスワードは、CIMC ログイン用にスタンバイ Management Center と同期されません。スタンバイ Management Center も更新されるようにするには、スタンバイ Management Center のローカルユーザーの CIMC ログインパスワードをリセットします。

Lights-Out 管理ユーザー アクセスの有効化

この手順を実行するには、管理者ユーザーである必要があります。

このタスクを使用して、既存のユーザーに LOM アクセスを許可します。新しいユーザーに LOM アクセスを許可するには、内部ユーザーの追加または編集（147 ページ）を参照してください。

手順

ステップ 1 システム（⚙） > **[ユーザー（Users）]** > **[ユーザー（Users）]**を選択します。

ステップ 2 既存のユーザーに LOM ユーザーアクセスを許可するには、リスト内のユーザー名の横にある **[編集（Edit）]**（✎）をクリックします。

ステップ 3 [ユーザーの設定（User Configuration）] で、Administrator ロールを有効にします。

ステップ 4 [Lights-Out 管理アクセスの許可（Allow Lights-Out Management Access）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

Serial over LAN 接続の設定

アプライアンスへの Serial over LAN 接続を作成するには、コンピュータ上でサードパーティ製の IPMI ユーティリティを使用します。Linux 系環境または Mac 環境を使用するコンピュータでは IPMItool を使用します。Windows 環境では、使用している Windows バージョンによって IPMIutil または IPMItool を使用できます。

（注） シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

Linux

多くのディストリビューションで IPMItool が標準となっており、使用可能です。

Mac

Mac では、IPMItool をインストールする必要があります。最初に、Mac に Apple の XCode Apple Developer Tools がインストールされていることを確認します。これにより、コマンドライン開発用のオプション コンポーネント（新しいバージョンでは UNIX Development and System Tools、古いバージョンでは Command Line Support）がインストールされていることを確認できます。次に、MacPorts と IPMItool をインストールします。詳細については、好みの検索エンジンを使用するか、次のサイトを参照してください。

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
http://github.com/ipmitool/ipmitool/
```

Windows

Windows Subsystem for Linux（WSL）が有効になっている Windows バージョン 10 以降、および一部の古いバージョンの Windows Server では、IPMItool を使用できます。それ以外の場合は、Windows システムで IPMIutil をコンパイルする必要があります。IPMIutil 自体を使用してコンパイルできます。詳細については、好みの検索エンジンを使用するか、次のサイトを参照してください。

```
http://ipmiutil.sourceforge.net/man.html#ipmiutil
```

IPMI ユーティリティのコマンドについて

IPMI ユーティリティで使用するコマンドは、Mac での IPMItool に関する次の例に示したセグメントで構成されます。

```
ipmitool -I lanplus -H IP_address -U user_name command
```

引数の説明

- `ipmitool` はユーティリティを起動します。
- `-I lanplus` は、セッションに暗号化された IPMI v2.0 RMCP+ LAN インターフェイスを使用することを指定します。
- `-H IP_address` はアクセスするアプライアンスの Lights-Out 管理用に設定された IP アドレスを示します。
- `-U user_name` は権限を持つユーザーの名前です。
- `command` は使用するコマンドの名前です。

（注） シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

Windows での IPMIutil の同じコマンドは、次のようになります。

```
ipmiutil command -V 4 -J 3 -N IP_address -Uuser_name
```

このコマンドは、アプライアンスのコマンドラインにユーザーを接続します。これによって、ユーザーは物理的にそのアプライアンスの近くにいるときと同じようにログインできます。場合によっては、パスワードの入力を求められます。

IPMItool を使用した Serial Over LAN の設定

この手順を実行するには、LOM アクセス権限のある管理者ユーザーである必要があります。

手順

IPMItool を使用して、次のコマンドと、プロンプトが表示されたらパスワードを入力します:

```
ipmitool -I lanplus -H IP_address -U user_name sol activate
```

IPMIutil を使用した Serial Over LAN の設定

この手順を実行するには、LOM アクセス権限のある管理者ユーザーである必要があります。

手順

IPMIutil を使用して、次のコマンドと、プロンプトが表示されたらパスワードを入力します。

```
ipmiutil -J 3 -N IP_address -U username sol -a
```

Lights-Out 管理の概要

Lights-Out 管理（LOM）では、システムにログインすることなく、デフォルトの管理インターフェイス（eth0）から SOL 接続を介して一連の限定操作を実行できます。SOL 接続を作成するコマンドに続いて、次のいずれかの LOM コマンドを使用します。コマンドが完了すると、接続は終了します。

注意 まれに、コンピュータがシステムの管理インターフェイスとは異なるサブネットにあり、そのシステムに DHCP が構成されている場合は、LOM 機能にアクセスしようとすると失敗することがあります。この場合は、システムの LOM を無効にして再び有効にするか、または同じサブネット上のコンピュータをシステムとして使用して、その管理インターフェイスを ping することができます。その後、LOM を使用できるようになるはずです。

注意 シスコでは、Intelligent Platform Management Interface（IPMI）標準（CVE-2013-4786）に内在する脆弱性を認識しています。システムの Lights-Out 管理（LOM）を有効にすると、この脆弱性にさらされます。この脆弱性を軽減するために、信頼済みユーザだけがアクセス可能なセキュアな管理ネットワークにシステムを展開し、辞書に載っていない複雑な最大長のパスワードをシステムに対して使用し、それを 3 か月ごとに変更してください。この脆弱性のリスクを回避するには、LOM を有効にしないでください。

システムへのアクセス試行がすべて失敗した場合は、LOM を使用してリモートでシステムを再起動できます。SOL 接続がアクティブなときにシステムが再起動すると、LOM セッションが切断されるか、またはタイムアウトする可能性があります。

注意 システムが別の再起動の試行に応答している間は、システムを再起動**しないでください**。リモートでシステムを再起動すると、通常の方法でシステムがリブートしないため、データが失われる可能性があります。

表 *3 : Lights-Out* 管理のコマンド

IPMItool	IPMIutil	説明
（適用なし）	`-V 4`	IPMI セッションの管理者権限を有効にし
`-I lanplus`	`-J 3`	IPMI セッションの暗号化を有効にします。
`-H hostname/IP address`	`-N nodename/IP address`	次の LOM IP アドレスまたはホスト名を示し Management Center

IPMItool	IPMIutil	説明
-U	-U	認可されたLOMアカウントのユーザー名を指ます。
sol activate	sol -a	SOL セッションを開始します。
sol deactivate	sol -d	SOL セッションを終了します。
chassis power cycle	power -c	アプライアンスを再起動します
chassis power on	power -u	アプライアンスの電源を投入します。
chassis power off	power -d	アプライアンスの電源をオフにします
sdr	sensor	アプライアンスの情報（ファン速度や温度なを表示します。

たとえば、アプライアンスの情報のリストを表示する IPMItool のコマンドは、次のとおりです。

```
ipmitool -I lanplus -H IP_address -U user_name sdr
```

（注） シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

IPMIutil ユーティリティの同等のコマンドは次のとおりです。

```
ipmiutil sensor -V 4 -J 3 -N IP_address -U user_name
```

IPMItool を使用した Lights-Out 管理の設定

この手順を実行するには、LOM アクセス権限のある管理者ユーザーである必要があります。

手順

プロンプトが表示されたら、IPMItool の次のコマンドとパスワードを入力します。

```
ipmitool -I lanplus -H IP_address -U user_name command
```

IPMIutil を使用した Lights-Out 管理の設定

この手順を実行するには、LOM アクセス権限のある管理者ユーザーである必要があります。

手順

プロンプトが表示されたら、IPMIutil の次のコマンドとパスワードを入力します。

```
ipmiutil -J 3 -N IP_address -U username command
```

リモート ストレージ デバイス

Management Center では、バックアップおよびレポートのローカル ストレージまたはリモート ストレージとして、以下を使用することができます。

- ネットワーク ファイル システム（NFS）
- サーバ メッセージ ブロック（SMB）/Common Internet File System（CIFS）
- セキュア シェル（SSH）

1 つのリモート システムにバックアップを送信し、別のリモート システムにレポートを送信することはできませんが、どちらかをリモート システムに送信し、もう一方を Management Center に格納することは可能です。

ヒント リモート ストレージを構成して選択した後は、接続データベースの制限を**増やさなかった**場合に**のみ**、ローカル ストレージに戻すことができます。

Management Center リモートストレージ：サポートされるプロトコルとバージョン

Management Center のバージョン	NFS のバージョン	SSH Version	SMB のバージョン
6.4	V3/V4	openssh 7.3p1	V2/V3
6.5	V3/V4	ciscossh 1.6.20	V2/V3
6.6	V3/V4	ciscossh 1.6.20	V2/V3
6.7	V3/V4	ciscossh 1.6.20	V2/V3

プロトコルバージョンを有効にするコマンド

ルートユーザーとして次のコマンドを実行して、プロトコルバージョンを有効にします。

- **NFS**：`/bin/mount -t nfs '10.10.4.225':'/home/manual-check' '/mnt/remote-storage' -o 'rw,vers=4.0'`
- **SMB**：`/usr/bin/mount.cifs //10.10.0.100/pyallapp-share/testing-smb /mnt/remote-storage -o username=administrator,password=******,vers=3.0`

ローカル ストレージの設定

手順

ステップ 1 システム（⚙）>**[構成（Configuration）]**を選択します。
ステップ 2 [リモート ストレージ デバイス（Remote Storage Device）] を選択します。
ステップ 3 [ストレージ タイプ（Storage Type）] ドロップダウン リストから [ローカル（リモート ストレージなし）（Local (No Remote Storage)）] を選択します。
ステップ 4 [保存（Save）] をクリックします。

リモートストレージの NFS の設定

始める前に

- 外部リモート ストレージ システムが機能しており、Management Center からアクセスできることを確認します。

手順

ステップ 1 システム（⚙）>**[構成（Configuration）]**を選択します。
ステップ 2 [リモート ストレージ デバイス（Remote Storage Device）] をクリックします。
ステップ 3 [ストレージ タイプ（Storage Type）] ドロップダウン リストから [NFS] を選択します。
ステップ 4 接続情報を追加します。

- [ホスト（Host）] フィールドに、ストレージ システムの IPv4 アドレスまたはホスト名を入力します。
- [ディレクトリ（Directory）] フィールドに、ストレージ領域へのパスを入力します。

ステップ 5 必要に応じて、[詳細オプションの使用（Use Advanced Options）] チェックボックスをオンにして、必要なコマンドライン オプションを入力します。リモート ストレージ管理の詳細オプション（115 ページ）を参照してください。
ステップ 6 [システムの使用方法（System Usage）] で、次の手順を実行します。

- 指定したホストにバックアップを格納するには、[バックアップに使用（Use for Backups）] を選択します。
- 指定したホストにレポートを格納するには、[レポートに使用（Use for Reports）] を選択します。
- リモート ストレージへのバックアップに関する [ディスク容量のしきい値（Disk Space Threshold）] を入力します。デフォルトは 90% です。

ステップ 7 設定をテストするには、[テスト（Test）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

トラブルシューティング

ファイアウォールデバイスとの NFS 接続にランダムな遅延がある場合は、次のアクティビティを実行してから、トラブルシューティングについて Cisco TAC にお問い合わせください。

- 問題の発生前または発生後に、デバイスからトラブルシューティング ファイルを収集します。トラブルシューティング ファイルは、Web インターフェイスから、または CLI コマンドを使用して生成できます。トラブルシューティング ファイルの生成方法については、『Troubleshoot Firepower File Generation Procedures』を参照してください。
- 着信トラフィックと発信トラフィックの PCAP レコードを収集します。手順については、パケット キャプチャの概要 （540 ページ）を参照してください。
- デバイスで次のコマンドを使用して（CLISH モード）、NFS アプリケーションの障害発生中にシステム サポート トレース データを収集します。

```
> system support trace
```

- **show snort counters** コマンドを使用して、障害発生中に Snort カウンタを 2 回収集し、Snort プリプロセッサ接続の統計を表示します。このコマンドについては、「show snort counters」を参照してください。

リモート ストレージ用の SMB の設定

始める前に

外部リモートストレージシステムが機能していて、Management Center からアクセスできることを確認します。

- システムに認識されるのは、ファイルのフルパスではなく、最上位の SMB 共有です。使用する正確なディレクトリを共有するには、Windows を使用する必要があります。
- Management Center から SMB 共有にアクセスするために使用する Windows ユーザーが、共有場所の読み取り/変更のアクセス権を持っていることを確認してください。
- セキュリティを確保するには、SMB 2.0 以降をインストールする必要があります。

手順

ステップ 1 システム（⚙） > **[構成（Configuration）]**を選択します。

ステップ 2 [リモート ストレージ デバイス（Remote Storage Device）] をクリックします。

ステップ 3 [ストレージ タイプ（Storage Type）] ドロップダウン リストから [SMB] を選択します。

ステップ 4 接続情報を追加します。

- [ホスト（Host）] フィールドに、ストレージ システムの IPv4 アドレスまたはホスト名を入力します。
- [共有（Share）] フィールドに、ストレージ領域の共有を入力します。
- 必要に応じて、[ドメイン（Domain）] フィールドにリモート ストレージ システムのドメイン名を入力します。
- [ユーザ名（Username）] フィールドにストレージ システムのユーザ名を入力し、[パスワード（Password）] フィールドにそのユーザのパスワードを入力します。

ステップ 5 必要に応じて、[詳細オプションの使用（Use Advanced Options）] チェックボックスをオンにして、必要なコマンドライン オプションを入力します。リモート ストレージ管理の詳細オプション （115 ページ）を参照してください。

ステップ 6 [システムの使用方法（System Usage）] で、次の手順を実行します。

- 指定したホストにバックアップを格納するには、[バックアップに使用（Use for Backups）] を選択します。
- 指定したホストにレポートを格納するには、[レポートに使用（Use for Reports）] を選択します。

ステップ 7 設定をテストするには、[テスト（Test）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

リモート ストレージの SSH の設定

始める前に

- 外部リモート ストレージ システムが機能しており、Management Center からアクセスできることを確認します。

手順

ステップ 1 システム（⚙） > **[構成（Configuration）]**を選択します。

ステップ 2 [リモート ストレージ デバイス（Remote Storage Device）] をクリックします。

ステップ 3 [ストレージ タイプ（Storage Type）] ドロップダウン リストから [SSH] を選択します。

ステップ 4 接続情報を追加します。

- [ホスト（Host）] フィールドに、ストレージ システムの IP アドレスまたはホスト名を入力します。
- [ディレクトリ（Directory）] フィールドに、ストレージ領域へのパスを入力します。
- [ユーザ名（Username）] フィールドにストレージ システムのユーザ名を入力し、[パスワード（Password）] フィールドにそのユーザのパスワードを入力します。接続ユーザ名の一部としてネットワーク ドメインを指定するには、ユーザ名の前にドメインを入力し、スラッシュ（/）で区切ります。
- SSH キーを使用するには、[SSH 公開キー（SSH Public Key）] フィールドの内容をコピーして authorized_keys ファイルに貼り付けます。

ステップ 5 必要に応じて、[詳細オプションの使用（Use Advanced Options）] チェックボックスをオンにして、必要なコマンドライン オプションを入力します。リモート ストレージ管理の詳細オプション （115 ページ）を参照してください。

ステップ 6 [システムの使用方法（System Usage）] で、次の手順を実行します。

- 指定したホストにバックアップを格納するには、[バックアップに使用（Use for Backups）] を選択します。
- 指定したホストにレポートを格納するには、[レポートに使用（Use for Reports）] を選択します。

ステップ 7 設定をテストする場合は、[テスト（Test）] をクリックする必要があります。

ステップ 8 [保存（Save）] をクリックします。

リモート ストレージ管理の詳細オプション

Secure File Transfer Protocol（SFTP）を使用してレポートとバックアップを保存するために、ネットワーク ファイル システム（NFS）プロトコル、サーバーメッセージブロック（SMB）プロトコル、または SSH を選択すると、NFS、SMB、SSH マウントのメインページに記載されているいずれかのマウントバイナリオプションを使用するために、[詳細設定オプションの使用（Use Advanced Options）] チェック ボックスを選択できます。

SMB または NFS ストレージタイプを選択した場合、[コマンドラインオプション（Command Line Option）] フィールドで次の形式を使用してリモートストレージのバージョン番号を指定できます。

`vers=version`

ここで、`version` は、使用する SMB または NFS リモートストレージのバージョン番号です。たとえば、NFSv4 を選択するには、`vers=4.0` と入力します。

ファイルサーバーで SMB 暗号化が有効になっている場合、SMB バージョン 3.0 クライアントのみがファイルサーバーにアクセスできます。Management Center から暗号化された SMB ファ

イルサーバーにアクセスするには、[コマンドラインオプション（Command Line Option）]フィールドに次のように入力します。

```
vers=3.0
```

ここで、暗号化されたSMBv3を選択して、バックアップファイルをManagement Centerから暗号化されたSMBファイルサーバーにコピーまたは保存します。

SNMP

Simple Network Management Protocol（SNMP）のポーリングを有効にできます。SNMP機能は、SNMPプロトコルのバージョン1、2、3をサポートします。この機能を使用すると、標準Management Information Base（MIB）にアクセスできます。MIBには、連絡先、管理、場所、サービス情報、IPアドレッシングやルーティングの情報、トランスミッションプロトコルの使用状況の統計などのシステムの詳細が含まれます。

（注） SNMPプロトコルのSNMPバージョンを選択する場合、SNMPv2では読み取り専用コミュニティのみがサポートされ、SNMPv3では読取り専用ユーザーのみがサポートされることに注意してください。SNMPv3は、AES128での暗号化をサポートします。

SNMPポーリングを有効にすると、システムでSNMPトラップを送信できなくなり、MIBの情報はネットワーク管理システムによるポーリングでのみ使用可能になります。

SNMPポーリングの設定

始める前に

使用するコンピュータごとにSNMPアクセスを追加し、システムをポーリングします。アクセス リストの設定 （49 ページ）を参照してください。

（注） SNMP MIBには展開の攻撃に使用される可能性がある情報が含まれています。SNMPアクセスのアクセス リストをMIBのポーリングに使用される特定のホストに制限することを推奨します。SNMPv3を使用し、ネットワーク管理アクセスには強力なパスワードを使用することも推奨します。

手順

ステップ1 システム（⚙）>**[構成（Configuration）]**を選択します。

ステップ2 [SNMP]をクリックします。

ステップ 3 [SNMPバージョン（SNMP Version）] ドロップダウン リストから、使用する SNMP バージョンを選択します。

- [Version 1] または [Version 2]：[Community String] フィールドに読み取り専用の SNMP コミュニティ名を入力してから、手順の最後までスキップします。

  （注） SNMP コミュニティストリング名には、特殊文字（< > / % # & ? ', etc.）を使用できません。

- [バージョン3（Version 3）]：[ユーザーを追加（Add User）] をクリックすると、ユーザー定義ページが表示されます。SNMPv3 は、読み取り専用ユーザーと AES128 による暗号化のみをサポートしています。

ステップ 4 ユーザ名を入力します。

ステップ 5 [認証プロトコル（Authentication Protocol）] ドロップダウン リストから、認証に使用するプロトコルを選択します。

ステップ 6 [認証パスワード（Authentication Password）] フィールドに SNMP サーバの認証に必要なパスワードを入力します。

ステップ 7 [パスワードの確認（Verify Password）] フィールドに、認証パスワードを再度入力します。

ステップ 8 使用するプライバシー プロトコルを [プライバシー プロトコル（Privacy Protocol）] リストから選択するか、プライバシー プロトコルを使用しない場合は [なし（None）] を選択します。

ステップ 9 [プライバシー パスワード（Privacy Password）] フィールドに SNMP サーバで必要な SNMP プライバシー キーを入力します。

ステップ 10 [パスワードの確認（Verify Password）] フィールドに、プライバシー パスワードを再度入力します。

ステップ 11 [追加（Add）] をクリックします。

ステップ 12 [保存（Save）] をクリックします。

セッション タイムアウト

無人ログインセッションは、セキュリティ上のリスクを生じさせる場合があります。ユーザーのログインセッションが非アクティブになったためにタイムアウトするまでのアイドル時間を設定できます。

システムを長期間にわたってパッシブかつセキュアにモニターする予定のシナリオでは、特定の Web インターフェイスのユーザーがタイムアウトしないように設定できることに注意してください。メニューオプションへの完全なアクセス権がある管理者ロールのユーザーは、侵害が生じる場合、余分のリスクを生じさせますが、セッションタイムアウトから除外することはできません。

セッション タイムアウトの設定

手順

ステップ 1 システム（⚙） > **[構成（Configuration）]**を選択します。

ステップ 2 [CLIタイムアウト（CLI Timeout）] をクリックします。

ステップ 3 セッション タイムアウトの設定

- Web インターフェイス（Management Center のみ）：[ブラウザセッションタイムアウト（分）（Browser Session Timeout (Minutes)）] を設定します。デフォルト値は 60 で、最大値は 1440（24 時間）です。

  このセッションタイムアウトからユーザーを除外する場合は、内部ユーザーの追加または編集 （147 ページ）を参照してください。

- CLI：[CLIタイムアウト（分）（CLI Timeout (Minutes)）] フィールドを設定します。デフォルト値は 0 で、最大値は 1440（24 時間）です。

ステップ 4 [保存（Save）] をクリックします。

時刻

[ユーザー設定（User Preferences）] の [タイムゾーン（Time Zone）] ページで設定したタイムゾーン（デフォルトでは America/New York）を使用すると、ほとんどのページでローカル時刻で時刻設定が表示されますが、アプライアンスには UTC 時間を使用して格納されます。

制約事項 タイムゾーン機能（[ユーザー設定（User Preferences）]）は、デフォルトのシステム クロックが UTC 時間に設定されていることを前提としています。システム時刻を変更しようとしないでください。システム時刻の UTC からの変更はサポートされていません。また、システム時刻を変更した場合はデバイスを再イメージ化してサポートされていない状態から回復させる必要があります。

手順

ステップ 1 システム（⚙） > **[構成（Configuration）]**を選択します。

ステップ 2 [時間（Time）] をクリックします。

現在の時刻は、[ユーザー設定（User Preferences）] でアカウントに指定されたタイムゾーンを使用して表示されます。

アプライアンスで NTP サーバを使用する場合、テーブル エントリについては、NTP サーバーのステータス （119 ページ）を参照してください。

NTP サーバーのステータス

NTP サーバーから時刻を同期する場合は、[時間（Time）] ページ（[システム（System）] > [設定（Configuration）] を選択）で接続ステータスを確認できます。

表 *4 : NTP* ステータス

カラム	説明
NTP サーバー	設定済みの NTP サーバーの IP アドレスまたは名前。
ステータス	NTP サーバの時間同期のステータス。 • [使用中（Being Used）] は、アプライアンスが NTP サーバと同期していることを示します。 • [使用可能（Available）] は、NTP サーバーが使用可能であるものの、時間がまだ同期していないことを示します。 • [使用不能（Not Available）] は、NTP サーバーが構成に含まれているものの、NTP デーモンがその NTP サーバーを使用できないことを示します。 • [保留（Pending）] は、NTP サーバーが新しいか、または NTP デーモンが最近再起動されたことを示します。この値は、時間の経過とともに [使用中（Being Used）]、[使用可能（Available）]、または [使用不能（Not Available）] に変わるはずです。 • [不明（Unknown）] は、NTP サーバーのステータスが不明であることを示します。
認証	Management Center と NTP サーバー間の通信の認証ステータスは次のとおりです。 • [なし（none）] は、認証が設定されていないことを示します。 • [不良（bad）] は、認証が設定されているが失敗していることを示します。 • [OK] は認証が成功したことを示します。 認証が設定されている場合、ステータス値の後にキー番号とキータイプ（SHA-1、MD5、または AES-128 CMAC）が表示されます。例：[不良、キー2、MD5（bad, key 2, MD5）]。

カラム	説明
オフセット	アプライアンスと構成済みの NTP サーバ間の時間の差（ミリ秒）。負の値はアプライアンスの時間が NTP サーバより遅れていることを示し、正の値は進んでいることを示します。
最終更新	NTP サーバと最後に時間を同期してから経過した時間（秒数）。NTP デーモンは、いくつかの条件に基づいて自動的に同期時間を調整します。たとえば、更新時間が大きい（300 秒など）場合、それは時間が比較的安定しており、NTP デーモンが小さい更新増分値を使用する必要がないと判断したことを示します。

時刻の同期

システムを正常に動作させるには、Secure Firewall Management Center（Management Center）とその管理対象デバイスのシステム時刻を同期させる必要があります。Management Center 初期設定時に NTP サーバーを指定することを推奨しますが、初期設定の完了後に、このセクションの情報を使用して、時刻同期設定を確立または変更することができます。

Management Center とすべてのデバイスのシステム時刻を同期させるには、Network Time Protocol（NTP）サーバーを使用します。Management Center は、MD5、SHA-1、または AES-128 CMAC 対称キー認証を使用して NTP サーバーとのセキュア通信をサポートしています。システムセキュリティについては、この機能を使用することを推奨します。

Management Center は、認証済みの NTP サーバーのみと接続するように設定することもできます。このオプションを使用すると、混合認証環境で、またはシステムを別の NTP サーバーに移行するときに、セキュリティを向上させることができます。すべての到達可能な NTP サーバーが認証される環境でこの設定を使用することは、冗長になります。

（注） 初期設定時に Management Center 用の NTP サーバーを指定した場合、その NTP サーバーとの接続は保護されません。MD5、SHA-1、または AES-128 CMAC キーを指定するには、その接続の設定を編集する必要があります。

注意 Management Center と管理対象デバイスの時刻が同期していないと、意図しない結果になることがあります。

Management Center と管理対象デバイスの時刻を同期するには、次を参照してください。

- 推奨： Management Center と NTP サーバー間の時刻の同期 （121 ページ）

  このトピックでは、NTP サーバーと同期するように Management Center を設定する手順と、同じ NTP サーバーと同期するように管理対象デバイスを設定する手順へのリンクを示します。

- 該当しない場合は、次のようになります。 ネットワーク NTP サーバーにアクセスせずに時刻を同期 （122 ページ）

  このトピックでは、Management Center で時刻を設定する手順、NTP サーバーとして機能するように Management Center を設定する手順、および Management Center NTP サーバーと同期するように管理対象デバイスを設定する手順へのリンクを示します。

Management Center と NTP サーバー間の時刻の同期

システムのすべてのコンポーネント間で時刻を同期することは非常に重要です。

Management Center とすべての管理対象デバイス間で適切な時刻同期を維持する最適な方法は、ネットワークで NTP サーバーを使用することです。

Management Center は NTPv4 をサポートします。

この手順を実行するには、管理者権限またはネットワーク管理者権限が必要です。

始める前に

次の点に注意してください。

- Management Center および管理対象デバイスがネットワーク NTP サーバーにアクセスできない場合は、この手順を使用しないでください。代わりに、ネットワーク NTP サーバーにアクセスせずに時刻を同期 （122 ページ）を参照してください。
- 信頼できない NTP サーバーを指定しないでください。
- NTP サーバーとのセキュアな接続を確立する場合（システムセキュリティに推奨）、NTP サーバーで設定されている SHA-1、MD5、または AES-128 CMAC キーの番号と値を取得します。
- NTP サーバーへの接続では、構成されたプロキシ設定は使用されません。
- Firepower 4100 シリーズ デバイスと Firepower 9300 デバイスでは、この手順を使用してシステム時刻を設定できません。代わりに、この手順を使用して設定するものと同じ NTP サーバーを使用するように、これらのデバイスを設定してください。手順については、ご使用のハードウェアモデル用のマニュアルを参照してください。

⚠

注意 Management Center が再起動され、ここで指定したものとは異なる NTP サーバー レコードを DHCP サーバーが設定した場合、DHCP 提供の NTP サーバーが代わりに使用されます。この状況を回避するには、同じ NTP サーバーを使用するように DHCP サーバーを設定します。

手順

ステップ 1 システム（⚙） > **[構成（Configuration）]**を選択します。

ステップ 2 [時間同期（Time Synchronization）] をクリックします。

ステップ 3 [NTPを使用して時間を提供（Serve Time via NTP）] が [有効（Enabled）] の場合、[無効（Disabled）] を選択して、NTP サーバーの Management Center を無効にします。

ステップ 4 [Set My Clock] オプションの場合、[Via NTP] を選択します。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 [Add NTP Server] ダイアログボックスで、NTP サーバーのホスト名か IPv4 または IPv6 アドレスを入力します。

ステップ 7 任意Management Centerと NTP サーバー間の通信を保護するには、次のようにします。

a) [Key Type] ドロップダウンリストから [MD5]、[SHA-1]、または [AES-128 CMAC] を選択します。

b) 指定された NTP サーバーから、対応する MD5、SHA-1、または AES-128 CMAC キー番号とキー値を入力します。

ステップ 8 [Add] をクリックします。

ステップ 9 2つのNTPサーバーのみが設定されている場合、それらのオフセットの差は大きくなります。これにより、Management Center は、ローカル時刻を使用します。そのため、少なくとも 3 つの NTP サーバーを設定することをお勧めします。

NTP サーバーをさらに追加するには、手順 5 ～ 8 を繰り返します。

ステップ 10 （オプション）Management Center で正常に認証された NTP サーバーのみを使用するように強制するには、[認証されたNTPサーバーのみを使用する（Use the authenticated NTP server only）] チェックボックスをオンにします。

ステップ 11 [保存（Save）] をクリックします。

次のタスク

管理対象デバイスでは同じ NTP サーバーを使用して同期するように設定します。

- デバイスプラットフォーム設定を指定します：Cisco Secure Firewall Management Center デバイス構成ガイドの「*Configure NTP Time Synchronization for Threat Defense*」。

  Management Center に NTP サーバーとセキュアな接続を確立するように強制する場合でも（[認証されたNTPサーバーのみを使用する（Use the authenticated NTP server only）]）、そのサーバーへのデバイス接続では認証が使用されないことに注意してください。

- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

ネットワーク NTP サーバーにアクセスせずに時刻を同期

デバイスがネットワーク NTP サーバーに直接アクセスできない、または組織内にネットワーク NTP サーバーがない場合は、物理ハードウェア Management Center を NTP サーバーとして使用できます。

重要

- 他の NTP サーバーがない場合を除き、この手順は使用しないでください。代わりに、Management Center と NTP サーバー間の時刻の同期 （121 ページ） の手順を使用してください。
- 仮想 Management Center を NTP サーバーとして使用しません。

Management Center を NTP サーバーとして設定後、時刻を手動で変更するには、NTP オプションを無効にして時刻を手動で変更してから NTP オプションを再度有効にします。

手順

ステップ 1 Management Center でシステム時刻を手動で設定するには、次の手順を実行します。

a) **システム**（⚙） > **[構成（Configuration）]**を選択します。
b) [時間同期（Time Synchronization）] をクリックします。
c) [NTP を使用して時間を提供（Serve Time via NTP）] が [有効（Enabled）] の場合、[無効（Disable）] を選択します。
d) [保存（Save）] をクリックします。
e) [マイクロックの設定（Set My Clock）] で、[ローカル設定で手動（Manually in Local Configuration）] を選択します。
f) [保存（Save）] をクリックします。
g) 画面の左側のナビゲーション パネルで [時間（Time）] をクリックします。
h) [時間の設定（Set Time）] ドロップダウン リストを使用して時間を設定します。

（注） Management Center の時刻を 2 時間以上変更した場合は、誤動作を避けるために、できるだけ早く（たとえばメンテナンスウィンドウで）デバイスを再起動する必要があります。

i) 表示されるタイムゾーンが UTC ではない場合、クリックして、タイムゾーンを [UTC] に設定します。
j) **[Save（保存）]** をクリックします。
k) [完了（Done）] をクリックします。
l) [適用（Apply）] をクリックします。

ステップ 2 Management Center を NTP サーバとして機能するように設定します。

a) 画面の左側のナビゲーションパネルで [時刻同期（Time Synchronization）] をクリックします。
b) [NTPを使用して時間を提供（Serve Time via NTP）] で、[有効（Enabled）] を選択します。
c) [保存（Save）] をクリックします。

ステップ 3 管理対象デバイスでは Management Center NTP サーバーを使用して同期するように設定します。

a) 管理対象デバイスに割り当てられたプラットフォーム設定ポリシーの [Time Synchronization] 設定で、[Via NTP from Management Center] に同期するようにクロックを設定します。
b) 管理対象デバイスへの変更を導入します。

手順については、次を参照してください。

Threat Defense デバイスについては、Cisco Secure Firewall Management Center デバイス構成ガイドの「*Configure NTP Time Synchronization for Threat Defense*」を参照してください。

時刻同期の設定の変更について

- Management Center とその管理対象デバイスは正確な時刻に大きく依存しています。システムクロックは、システムの時刻を維持するシステム機能です。システム クロックは協定世界時（UTC）に設定されています。これは、時計と時刻を管理するために世界で使用されている基本的な標準時間です。

  システム時刻を変更しようとしないでください。システムタイムゾーンの UTC からの変更はサポートされていません。また、システムタイムゾーンを変更した場合はデバイスを再イメージ化してサポートされていない状態から回復させる必要があります。

- NTP を使用して時刻を提供するように Management Center を設定してから、後でそれを無効にした場合、管理対象デバイスの NTP サービスは引き続き Management Center と時刻を同期しようとします。新しい時刻ソースを確立するには、すべての該当するプラットフォーム設定ポリシーを更新および再展開する必要があります。

- Management Center を NTP サーバーとして設定後、時刻を手動で変更するには、NTP オプションを無効にして時刻を手動で変更してから NTP オプションを再度有効にします。

UCAPL/CC コンプライアンス

お客様の組織が、米国防総省およびグローバル認定組織によって確立されたセキュリティ基準に従う機器とソフトウェアだけを使用することを求められる場合があります。この設定の詳細については、セキュリティ認定準拠のモード （393 ページ）を参照してください。

構成のアップグレード

ポリシー属性、オブジェクト、またはその他のデバイス設定は、Management Center のアップグレードの一部として変更される場合があります。Management Center をメジャーバージョンにアップグレードすると、特定の機能がデフォルトで有効になる場合があります。[構成のアップグレード（Upgrade Configuration）] 設定を使用すると、Management Center の次のメジャーバージョンへのアップグレードを完了したときに、保留中の設定変更のレポートを生成できます。このレポートには、アップグレード後に管理対象デバイスへの展開が保留されているポリ

シーおよびデバイス設定の変更が表示されます。Management Center のアップグレードが完了したら、**[Message Center]** > **[タスク（Tasks）]** を選択してレポートをダウンロードします。

保留中の設定変更のレポートには、次のものが含まれます。

- **比較ビュー**：管理対象デバイスへの展開が保留されている、アップグレード後のすべての設定変更を、現在のデバイス設定と比較します。
- **詳細ビュー**：CLI を使用して、保留中の設定変更をプレビューできます。

保留中の設定変更に関するレポートの詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの「*Deployment Preview*」を参照してください。

アップグレード後のレポートの有効化

Management Center のメジャー バージョン アップグレード後に管理対象デバイスに展開される保留中のすべての設定変更に関するレポートを生成します。

手順

ステップ 1 **システム**（⚙） > **[構成（Configuration）]** を選択します。

ステップ 2 [アップグレード後レポートの有効化（Enable Post-Upgrade Report）] チェックボックスをオンにして、このオプションを有効にします。

レポートは、Management Center の次のメジャー バージョン アップグレード後に生成されます。このオプションは、アップグレード後にすべての管理対象デバイスのレポートを生成します。レポートの生成に必要な時間は、設定のサイズと管理対象デバイスの数によって異なります。

ステップ 3 [保存（Save）] をクリックします。

ユーザーの設定

グローバル ユーザーの設定は、Management Center のすべてのユーザーに影響します。[User Configuration] ページで次の設定を行います（**システム**（⚙） > **[構成（Configuration）]** > **[ユーザー構成（User Configuration）]**）。

- [パスワード再使用制限（Password Reuse Limit）]：ユーザーの最新の履歴の中で再利用できないパスワードの数。この制限は、すべてのユーザーの Web インターフェイスに適用されます。`admin` ユーザーの場合、これは CLI アクセスにも適用されます。システムは各アクセス形式に対して個別のパスワード リストを維持します。制限をゼロに設定すると（デフォルト）パスワードの再利用に制限は課せられません。パスワードの再使用制限の設定 （127 ページ）を参照してください。

- [成功したログインの追跡（Track Successful Logins）]：Management Center へのログインの成功をユーザーごとにアクセス方式（Web インターフェイスまたは CLI）別に追跡する日数。ユーザーがログインすると、使用しているインターフェイスで成功したログイン回数が表示されます。[成功したログインの追跡（Track Successful Logins）] をゼロに設定すると（デフォルト）、システムは成功したログインアクティビティを追跡せず、レポートもしません。成功したログインの追跡 （128 ページ）を参照してください。
- [ログイン失敗の最大数（Max Number of Login Failures）]：ユーザーが誤った Web インターフェイスのログインクレデンシャルを連続して入力できる回数。この回数を超えると、設定されている時間にわたって一時的にアカウントにアクセスできなくなります。一時的なロックアウトが適用されている間にユーザーがログインを試行し続けた場合：
  - 一時的なロックアウトが適用されていることをユーザーに通知せず、（有効なパスワードを使用したとしても）システムはそのアカウントへのアクセスを拒否します。
  - ログイン試行のたびにシステムはそのアカウントの失敗ログイン数を増やし続けます。
  - ユーザーが個人の [ユーザー設定（User Configuration）] ページでそのアカウントに設定した [ログイン失敗の最大数（Maximum Number of Failed Logins）] を超えた場合、管理者ユーザーがそのアカウントを再アクティブ化するまではそのアカウントはロックアウトされます。
- [一時的にユーザーをロックアウトする分単位の時間の設定（Set Time in Minutes to Temporarily Lockout Users）]：[ログイン失敗の最大数（Max Number of Failed Logins）] がゼロ以外の場合にユーザーが一時的に Web インターフェイスからロックアウトされる分単位の時間。
- [許可された最大同時セッション数（Max Concurrent Sessions Allowed）]：同時に開くことができる特定のタイプ（読み取り専用または読み取り/書き込み）のセッション数。セッションのタイプは、ユーザーに割り当てられたロールによって決定されます。ユーザーに読み取り専用ロールのみが割り当てられている場合、そのユーザーのセッションは、[（読み取り専用）（(Read Only)）] セッションの制限に対してカウントされます。ユーザーが書き込み権限があるロールを持っている場合、セッションは、[読み取り/書き込み（Read/Write）] セッションの制限に対してカウントされます。たとえば、ユーザーに Admin ロールが割り当てられていて、[読み取り/書き込み権限を持つユーザーおよびCLI ユーザーの最大セッション数（Maximum sessions for users with Read/Write privileges/CLI users）] が 5 に設定されている場合、読み取り/書き込み権限を持つ 5 人の他のユーザーがすでにログインしていると、そのユーザーはログインできません。

（注） システムが同時セッション制限の目的で読み取り専用と見なす定義済みユーザーロールおよびカスタムユーザーロールには、**システム**（⚙）>**[ユーザー（Users）]**>**[ユーザー（Users）]** と **システム**（⚙）>**[ユーザー（Users）]**>**[ユーザーロール（User Roles）]** にあるロール名に [(Read Only)] というラベルが付けられます。ユーザー ロールのロール名に [（読み取り専用）（(Read Only)）] が含まれていない場合、システムはそのロールを読み取り/書き込みと見なします。システムは、必要な条件を満たすロールに [（読み取り専用）（(Read Only)）] を自動的に適用します。読み取り専用のテキスト文字列をロール名に手動で追加してロールを読み取り専用にすることはできません。

セッションのタイプごとに、最大制限を 1 ～ 1024 の範囲で設定できます。[許可された最大同時セッション数（Max Concurrent Sessions Allowed）] がゼロ（デフォルト）に設定されている場合、同時セッション数は無制限になります。

同時セッションの制限をより限定的な値に変更しても、システムは現在開いているセッションを閉じません。ただし、指定された数を超えて新しいセッションが開かれないようにします。

パスワードの再使用制限の設定

[パスワード再利用の制限（Password Reuse Limit）] を有効にすると、システムに Management Center ユーザーの暗号化されたパスワード履歴が保持されます。ユーザーはパスワード履歴内のパスワードを再利用できません。各ユーザーの保存されたパスワードの数をアクセス方式（Web インターフェイスまたは CLI）ごとに指定できます。ユーザーの現在のパスワードはこの番号に対してカウントされます。制限を低くすると、システムは履歴から古い順にパスワードを削除します。制限を高くすると、削除されたパスワードが復元されません。

手順

ステップ 1 **システム**（⚙）>**[構成（Configuration）]** を選択します。

ステップ 2 [User Configuration] をクリックします。

ステップ 3 [Password Reuse Limit] を履歴に維持したいパスワードの数（最大 256）に設定します。

パスワード再利用のチェックを無効にするには、0 を入力します。

ステップ 4 [保存（Save）] をクリックします。

成功したログインの追跡

この手順を使用して、各ユーザーの成功したログインの追跡を指定した日数の間、有効にします。この追跡が有効になっている場合は、ユーザーがWebインターフェイスまたはCLIにログインしたときにシステムは成功したログイン数を表示します。

（注） 日数を少なくすると、システムはログインのレコードを古いものから削除します。制限値を大きくすると、システムはその日数からカウントを復元しません。その場合、成功したログインの復元された数は、一時的に実際の番号よりも少なくなる場合があります。

手順

ステップ 1 システム（⚙）>**[構成（Configuration）]** を選択します。

ステップ 2 [User Configuration] をクリックします。

ステップ 3 [成功したログイン日数の追跡（Track Successful Login Days）] を成功したログインを追跡する日数（最大 365）に設定します。

ログインの追跡を無効にするには、0 を入力します。

ステップ 4 [保存（Save）] をクリックします。

一時的なロックアウトの有効化

システムがロックアウトを有効にする前に連続して失敗したログイン試行を許可する回数を指定して、一時的な時限ロックアウト機能を有効にします。

手順

ステップ 1 システム（⚙）>**[構成（Configuration）]** を選択します。

ステップ 2 [User Configuration] をクリックします。

ステップ 3 [ログイン失敗の最大数（Max Number of Login Failures）] をユーザーが一時的にロックアウトされるまで連続して失敗できるログイン試行の最大回数に指定します。

一時的なロックアウトを無効にするには、ゼロを入力します。

ステップ 4 [ユーザーを一時的にロックアウトする分単位の時間（Time in Minutes to Temporarily Lockout Users）]は一時的なロックアウトをトリガーしたユーザーをロックアウトする分数に設定します。

この値がゼロの場合は、[ログイン失敗最大数（Max Number of Login Failures）] がゼロ以外でも、ユーザーはログインの再試行を待機する必要はありません。

ステップ 5 [保存（Save）] をクリックします。

同時セッションの最大数の設定

同時に開くことができる特定のタイプ（読み取り専用または読み取り/書き込み）のセッションの最大数を指定できます。セッションのタイプは、ユーザーに割り当てられたロールによって決定されます。ユーザーに読み取り専用ロールのみが割り当てられている場合、そのユーザーのセッションは、[（読み取り専用）（(Read Only)）] セッションの制限に対してカウントされます。ユーザーが書き込み権限があるロールを持っている場合、セッションは、[読み取り/書き込み（Read/Write）] セッションの制限に対してカウントされます。

手順

ステップ 1 **システム**（⚙） > **[構成（Configuration）]** を選択します。

ステップ 2 [User Configuration] をクリックします。

ステップ 3 セッションのタイプ（[（読み取り専用）（(Read Only)）] および [読み取り/書き込み（Read/Write）]）ごとに、[許可された最大同時セッション数（Max Concurrent Sessions Allowed）] をそのタイプのセッションの最大数（同時に開くことができる）に設定します。

セッション タイプごとに同時ユーザーの制限を適用しない場合は、0 を入力します。

（注） 同時セッションの制限をより限定的な値に変更しても、システムは現在開いているセッションを閉じません。ただし、指定された数を超えて新しいセッションが開かれないようにします。

ステップ 4 [保存（Save）] をクリックします。

VMware ツール

VMware Tools は、仮想マシン向けのパフォーマンスを向上させるためのユーティリティ スイートです。これらのユーティリティを使用すると、VMware 製品の便利な機能をすべて活用できます。VMware で実行されている Cisco Secure Firewall 仮想アプライアンスは、次のプラグインをサポートします。

- guestInfo
- powerOps
- timeSync
- vmbackup

サポートされるすべてのバージョンの ESXi で VMware Tools を有効にすることもできます。VMware Tools のすべての機能については、VMware の Web サイト（http://www.vmware.com/）を参照してください。

VMware 向け Secure Firewall Management Center での VMware ツールの有効化

手順

ステップ 1 システム（⚙）> **[構成（Configuration）]**を選択します。
ステップ 2 [VMware ツール（VMware Tools）] をクリックします。
ステップ 3 [VMware ツールの有効化（Enable VMware Tools）] をクリックします。
ステップ 4 [保存（Save）] をクリックします。

脆弱性マッピング

サーバーのディスカバリ イベント データベースにアプリケーション ID が含まれており、トラフィックのパケットヘッダーにベンダーおよびバージョンが含まれる場合、システムは、そのアドレスから送受信されるすべてのアプリケーション プロトコル トラフィックについて、脆弱性をホスト IP アドレスに自動的にマップします。

パケットにベンダー情報もバージョン情報も含まれないサーバすべてに対して、システムでこれらのベンダーとバージョンレスのサーバのサーバ トラフィックと脆弱性を関連付けるかどうかを設定できます。

たとえば、ホストがヘッダーにベンダーまたはバージョンが含まれていない SMTP トラフィックを提供しているとします。システム設定の [脆弱性マッピング（Vulnerability Mapping）] ページで SMTP サーバを有効にしてから、そのトラフィックを検出するデバイスを管理する Management Center にその設定を保存した場合、SMTP サーバと関連付けられているすべての脆弱性がそのホストのホスト プロファイルに追加されます。

ディテクタがサーバー情報を収集して、それをホスト プロファイルに追加しますが、アプリケーション プロトコル ディテクタは脆弱性のマッピングに使用されません。これは、カスタム アプリケーション プロトコル ディテクタにベンダーまたはバージョンを指定できず、また脆弱性マッピング用のサーバーを選択できないためです。

サーバの脆弱性のマッピング

この手順には、スマートライセンスまたは保護クラシックライセンスが必要です。

手順

ステップ 1 システム（⚙） > **[構成（Configuration）]**を選択します。

ステップ 2 [脆弱性マッピング（Vulnerability Mapping）] を選択します。

ステップ 3 次の選択肢があります。

- ベンダーまたはバージョンの情報が含まれていないアプリケーション プロトコル トラフィックを受信するホストに、サーバの脆弱性がマップされないようにするには、そのサーバのチェックボックスをオフにします。
- ベンダーまたはバージョンの情報が含まれていないアプリケーション プロトコル トラフィックを受信するホストに、サーバの脆弱性がマップされるようにするには、そのサーバのチェックボックスをオフにします。

ヒント [有効（Enabled）]の横にあるチェックボックスを使用すると、すべてのチェックボックスを一度にオンまたはオフにできます。

ステップ 4 [保存（Save）] をクリックします。

Web 分析

デフォルトでは、ファイアウォール製品の向上のために、ページの閲覧内容、ブラウザのバージョン、製品バージョン、ユーザーの場所、Management Center アプライアンスの管理 IP アドレスまたはホスト名など、個人を特定できない使用データがシスコによって収集されます。

データ収集は、エンド ユーザー ライセンス契約書に同意した後に開始されます。このデータの継続的な収集を拒否する場合は、次の手順を実行してオプト アウトできます。

手順

ステップ 1 [システム（System）] > [設定（Configuration）] を選択します。

ステップ 2 [Web 分析（Web Analytics）] をクリックします。

ステップ 3 適切に選択してから、[保存（Save）] をクリックします。

次のタスク

（オプション）Cisco Success Network の登録設定を介してデータを共有するかどうかを決定します。

システム設定の履歴

機能	最小 Management Center	最小 Threat Defense	詳細
アップグレード後のレポートの有効化	7.4.1	任意（Any）	Secure Firewall Management Center の次のメジャーバージョンアップグレード後に、管理対象デバイスに展開される保留中の設定変更のレポートを生成することを選択できるようになりました。 新規/変更された画面：**システム**（⚙）>**[設定（Configuration）]**>**[設定のアップグレード（Upgrade Configuration）]**。 必要最低限の Threat Defense：任意
アクセス制御のパフォーマンスの向上（オブジェクトの最適化）。	7.2.4 7.4.0	いずれか	**アップグレードの影響。7.2.4 ～ 7.2.5 または 7.4.0 への Management Center アップグレード後の最初の展開には時間がかかり、デバイスの CPU 使用率が高くなる可能性があります。** アクセス コントロール オブジェクトの最適化により、ネットワークが重複するアクセス コントロール ルールがある場合、パフォーマンスが向上し、デバイスリソースの消費が少なくなります。最適化は、Management Center で機能が有効になった後の最初の展開時に管理対象デバイスで行われます（アップグレードで有効になった場合も含む）。ルールの数が多い場合、システムがポリシーを評価してオブジェクトの最適化を実行するのに数分から 1 時間かかることがあります。この間、デバイスの CPU 使用率も高くなることがあります。機能が無効になった後の最初の展開でも同様のことが発生します（アップグレードによって無効になった場合も含む）。この機能が有効または無効になった後は、メンテナンス時間帯やトラフィックの少ない時間帯など、影響が最小限になる時間に展開することを強く推奨します。 新規/変更された画面：（バージョン /7.4.1 が必要）：**システム**（⚙）>**[設定（Configuration）]**>**[アクセス制御の設定（Access Control Preferences）]**>**[オブジェクトグループの最適化（Object-group optimization）]**。 その他のバージョン制限：Management Center バージョン 7.3.x ではサポートされていません。
監査ログの設定変更。	7.4	任意（Any）	設定データの形式とホストを指定することにより、設定変更を監査ログデータの一部として syslog にストリーミングできます。Management Center は、監査構成ログのバックアップと復元をサポートしています。この機能は、Management Center の高可用性設定でもサポートされています。 新規/変更された画面：**システム**（⚙）>**[設定（Configuration）]**>**[監査ログ（Audit Log）]**

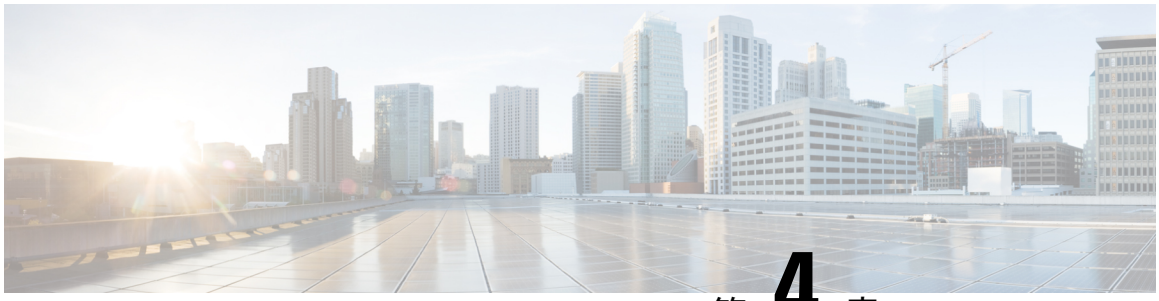
機能	最小 Management Center	最小 Threat Defense	詳細
フランス語オプション。	7.2	いずれか	Management Center の Web インターフェイスをフランス語に切り替えることができるようになりました。 新規/変更された画面：**システム**（⚙）>**[設定（Configuration）]**>**[言語（Language）]**。
ほとんどの接続イベントをイベントレート制限から除外します。	7.0	任意（Any）	接続データベースの [最大接続イベント数（Maximum Connection Events）] の値を 0 に設定すると、優先順位の低い接続イベントが FMC ハードウェアのフローレート制限にカウントされなくなります。以前は、この値を 0 に設定すると、イベントストレージにのみ適用され、フローレート制限には影響しませんでした。 新規/変更された画面：**システム**（⚙）>**[設定（Configuration）]**>**[データベース（Database）]** サポートされているプラットフォーム：ハードウェア FMC。
NTP サーバーの AES-128 CMAC 認証のサポート。	7.0	任意（Any）	FMC と NTP サーバー間の接続は、AES-128 CMAC キーと、以前にサポートされていた MD5 キーおよび SHA-1 キーを使用して保護できます。 新規/変更された画面：**システム**（⚙）>**[設定（Configuration）]**>**[時刻の同期（Time Synchronization）]**
サブジェクト代替名（SAN）。	6.6	任意（Any）	FMC の HTTPS 証明書を作成するときに、SAN フィールドを指定できます。証明書が複数のドメイン名または IP アドレスを保護する場合は、SAN を使用することを推奨します。SAN の詳細については、RFC 5280、セクション 4.2.1.6 を参照してください。 新規/変更された画面：**システム**（⚙）>**[設定（Configuration）]**>**[HTTPS証明書（HTTPS Certificate）]**
HTTPS 証明書。	6.6	任意（Any）	現在、システムとともに提供されるデフォルトの HTTPS サーバークレデンシャルは 800 日で期限が切れます。バージョン 6.6 にアップグレードする前に生成されたデフォルトの証明書がアプライアンスで使用されている場合、証明書の有効期限は、証明書が生成されたときに使用されていた Firepower バージョンによって異なります。詳細については、デフォルト HTTPS サーバー証明書 （72 ページ）を参照してください。 サポートされているプラットフォーム：ハードウェア FMC。
NTP の保護。	6.5	任意（Any）	FMC は、SHA1 または MD5 対称キー認証を使用して NTP サーバーとのセキュア通信をサポートしています。 新規/変更された画面：**システム**（⚙）>**[構成（Configuration）]**>**[時刻の同期（Time Synchronization）]**

機能	最小 Management Center	最小 Threat Defense	詳細
Web 解析。	6.5	任意（Any）	Web 分析データの収集は、EULA に同意した後に開始されます。以前と同様に、データの共有を停止することを選択できます。Web 分析（131 ページ）を参照してください。
FMC の自動 CLI アクセス。	6.5	任意（Any）	SSH を使用して FMC にログインすると、CLI に自動的にアクセスします。CLI `expert` コマンドを使用して Linux シェルにアクセスすることもできますが、このコマンドを使用しないことを強く推奨します。 （注） FMC の CLI アクセスを有効または無効にするバージョン 6.3 の機能は廃止されます。このオプションが廃止された結果、仮想 FMC には **システム**（⚙）>**[設定（Configuration）]**>**[コンソール設定（Console Configuration）]** ページは表示されなくなりました。このページは、物理 FMC では引き続き表示されます。
読み取り専用および読み取り/書き込みアクセスに設定可能なセッション制限。	6.5	任意（Any）	[許可された最大同時セッション数（Max Concurrent Sessions Allowed）] の設定が追加されました。この設定により、管理者は同時に開くことができる特定のタイプ（読み取り専用または読み取り/書き込み）のセッションの最大数を指定できます。 （注） 同時セッション制限の目的で読み取り専用と見なされる定義済みユーザーロールおよびカスタムユーザーロールには、**システム**（⚙）>**[ユーザー（Users）]**>**[ユーザー（Users）]**および**システム**（⚙）>**[ユーザー（Users）]**>**[ユーザーロール（User Roles）]**にあるロール名に [（読み取り専用）（(Read Only)）] というラベルが付けられます。ユーザー ロールのロール名に [（読み取り専用）（(Read Only)）] が含まれていない場合、システムはそのロールを読み取り/書き込みと見なします。 新規/変更された画面： • **システム**（⚙）>**[設定（Configuration）]**>**[ユーザー設定（User Configuration）]** • **システム**（⚙）>**[ユーザー（Users）]**>**[ユーザーロール（User Roles）]**

機能	最小 Management Center	最小 Threat Defense	詳細
管理インターフェイスで重複アドレス検出（DAD）を無効にする機能。	6.4	任意（Any）	IPv6 を有効にすると、DAD を無効にすることができます。DAD を使用することによってサービス拒否攻撃の可能性が拡大するため、DAD は無効にすることができます。この設定を無効にした場合は、すでに割り当てられているアドレスがこのインターフェイスで使用されていないことを手動で確認する必要があります。 新規/変更された画面：**システム**（⚙）>**[設定（Configuration）]**>**[管理インターフェイス（Management Interfaces）]** > **[インターフェイス（Interfaces）]** > **[インターフェイスの編集（Edit Interface）]** > **[IPv6 DAD]** サポート対象プラットフォーム: FMC
管理インターフェイス上の ICMPv6 エコー応答および宛先到達不能メッセージを無効にする機能。	6.4	任意（Any）	IPv6 を有効にすると、ICMPv6 エコー応答および宛先到達不能メッセージを無効できるようになりました。これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。エコー応答パケットを無効にすると、デバイスの管理インターフェイスにテスト目的で IPv6 ping を使用できなくなります。 新規/変更された画面：**システム**（⚙）> **[設定（Configuration）]** > **[ICMPv6]** 新規/変更されたコマンド：**configure network ipv6 destination-unreachable**、**configure network ipv6 echo-reply** サポートされているプラットフォーム：FMC（Web インターフェイスのみ）、FTD（CLI のみ）

機能	最小 Management Center	最小 Threat Defense	詳細
グローバルユーザー構成設定。	6.3	任意（Any）	[成功したログインの追跡（Track Successful Logins）]の設定を追加しました。システムは、選択した日数までに各 FMC アカウントで実行され、成功したログインの回数を追跡できます。この機能を有効にすると、ログイン中のユーザーには、設定した過去の日数内にシステムへのログインが何回成功したかを報告するメッセージが表示されます（Web インターフェイスとシェル/CLI アクセスに適用）。 [パスワード再利用制限（Password Reuse Limit）] の設定を追加しました。設定可能な過去のパスワード数について各アカウントのパスワードの履歴を追跡できます。システムは、すべてのユーザーがその履歴に表示されているパスワードを再利用できないようにします（Web インターフェイスとシェル/CLI アクセスに適用）。 [ログイン失敗の最大数（Max Number of Login Failures）] と [ユーザーを一時的にロックアウトする分単位の時間の設定（Set Time in Minutes to Temporarily Lockout Users）] の設定を追加しました。これらの機能によって、管理者はシステムが設定可能な時間にわたってアカウントを一時的にブロックするまでに、ユーザーが誤った Web インターフェイスのログインクレデンシャルを連続して入力できる回数を制限できます。 新規/変更された画面：**システム**（⚙）> **[設定（Configuration）]** > **[ユーザー設定（User Configuration）]** サポート対象プラットフォーム: FMC
HTTPS 証明書。	6.3	任意（Any）	現在、システムとともに提供されるデフォルトの HTTPS サーバー クレデンシャルは 3 年で期限が切れます。バージョン 6.3 にアップグレードされる前に生成されたデフォルトのサーバー証明書をアプライアンスが使用している場合、サーバー証明書は最初に生成されたときから 20 年後に期限切れとなります。デフォルトの HTTPS サーバー証明書を使用している場合、システムはその証明書を更新する機能を提供しています。 新規/変更された画面：**システム**（⚙）> **[設定（Configuration）]** > **[HTTPS証明書（HTTPS Certificate）]** > **[HTTPS証明書の更新（Renew HTTPS Certificate）]** サポート対象プラットフォーム: FMC

機能	最小 Management Center	最小 Threat Defense	詳細
FMC の CLI アクセスを有効化および無効化する機能。	6.3	任意（Any）	FMC の Web インターフェイスで管理者が使用可能な新しいチェックボックス：**システム**（⚙）>**[設定（Configuration）]**>**[コンソール設定（Console Configuration）]** の [CLIアクセスの有効化（Enable CLI Access）]。 • オン： SSH を使用して FMC にログインすると CLI にアクセスします。 • オフ：SSH を使用して FMC にログインすると Linux シェルにアクセスします。これは、バージョン 6.3 の新規インストールと、以前のリリースからバージョン 6.3 にアップグレードした場合のデフォルトの状態です。 バージョン 6.3 より前では、[コンソール設定（Console Configuration）] ページには 1 つの設定のみしかなく、物理デバイスのみに適用されていました。そのため、[コンソール設定（Console Configuration）] ページは仮想 FMC では使用できませんでした。この新しいオプションを追加することで、[コンソール設定（Console Configuration）] ページに物理 FMC とともに 仮想 FMC が表示されるようになりました。ただし、仮想FMCの場合、このページに表示されるのはこのチェックボックスのみです。 サポート対象プラットフォーム: FMC



第 4 章

Management Centerユーザー

Management Center には、Web および CLI アクセス用のデフォルトの**管理者**アカウントが含まれています。この章では、カスタムユーザーアカウントを作成する方法について説明します。ユーザーアカウントを使用して Management Center にログインする方法の詳細については、Management Center へのログイン （33 ページ）を参照してください。

ユーザについて

内部ユーザーとして、または LDAP または RADIUS サーバーの外部ユーザーとして、管理対象デバイスにカスタムユーザーアカウントを追加できます。各管理対象デバイスは、個別のユーザーアカウントを保持します。たとえば、Management Center にユーザーを追加した場合は、そのユーザーは Management Center にのみアクセスできます。そのユーザー名を使用して管理対象デバイスに直接ログインすることはできません。管理対象デバイスにユーザーを別途追加する必要があります。

内部および外部ユーザ

管理対象デバイスは次の 2 つのタイプのユーザーをサポートしています。

- 内部ユーザー：デバイスは、ローカル データベースでユーザー認証を確認します。

- 外部ユーザー：ユーザーがローカル データベースに存在しない場合は、システムは外部 LDAP または RADIUS の認証サーバーに問い合わせます。

Web インターフェイスおよび CLI によるアクセス

Management Center には、Web インターフェイス、CLI（コンソール（シリアルポートまたはキーボードとモニターのいずれか）から、または管理インターフェイスへの SSH を使用してアクセス可能）、および Linux シェルがあります。管理 UI の詳細については、システム ユーザー インターフェイス （35 ページ）を参照してください。

Management Center ユーザータイプと、それらがアクセスできる UI に関する次の情報を参照してください。

- admin ユーザー：Management Center は 2 種類の内部 **admin** ユーザーをサポートしています。Web インターフェイスのユーザーと、CLI アクセス権が付与されたユーザーです。システム初期化プロセスでは、これら 2 つの **admin** アカウントのパスワードが同期されるため、アカウントは同じように開始されますが、これらのアカウントは異なる内部メカニズムによって追跡され、初期設定後に分岐する場合があります。システム初期化の詳細については、ご使用のモデルの『Getting Started Guide』を参照してください。（Web インターフェイスの **admin** のパスワードを変更するには、**システム**（⚙）> **[ユーザー（Users）]** > [ユーザー（Users）] を使用します。CLI の **admin** のパスワードを変更するには、Management Center CLI コマンド **configure password** を使用します。）
- 内部ユーザー：Web インターフェイスで追加された内部ユーザーには、Web インターフェイスのアクセス権のみが付与されます。
- 外部ユーザー：外部ユーザーには Web インターフェイスのアクセス権が付与され、オプションで CLI のアクセス権を設定できます。
- SSO ユーザー：SSO ユーザーには Web インターフェイスのアクセス権のみが付与されます。

⚠

注意 CLI ユーザーは、**expert** コマンドを使用して Linux シェルにアクセスできます。Cisco TAC または Management Center マニュアルの明示的な手順による指示がない限り、Linux シェルを使用しないことを強くお勧めします。CLI ユーザーは Linux シェルで `sudoers` 権限を取得できます。このため、セキュリティ上のリスクが生じる可能性があります。システムセキュリティ上の理由から、次のことを強く推奨します。

- CLI アクセス権を持つ外部ユーザーのリストを適切に制限してください。
- Linux シェルでユーザを直接追加しないでください。この章の手順のみを使用してください。

ユーザの役割

CLI ユーザロール

Management Center の CLI 外部ユーザにはユーザ ロールがありません。そのため、それらのユーザは使用可能なすべてのコマンドを使用できます。

Web インターフェイスのユーザ ロール

ユーザ権限は、割り当てられたユーザ ロールに基づいています。たとえば、アナリストに対してセキュリティ アナリストや検出管理者などの事前定義ロールを付与し、デバイスを管理するセキュリティ管理者に対して管理者ロールを予約することができます。また、組織のニーズに合わせて調整されたアクセス権限を含むカスタム ユーザ ロールを作成できます。

Management Center には、次の定義済みユーザー ロールが含まれています。

（注） システムが同時セッション制限の目的で読み取り専用と見なす定義済みユーザーロールには、**システム**（⚙）>**[ユーザー（Users）]**>**[ユーザー（Users）]** と **システム**（⚙）>**[ユーザー（Users）]**>**[ユーザーロール（User Roles）]** でロール名に [(Read Only)] というラベルが付けられます。ユーザー ロールのロール名に [（読み取り専用）（(Read Only)）] が含まれていない場合、システムはそのロールを読み取り/書き込みと見なします。同時セッション制限の詳細については、ユーザーの設定 （125 ページ）を参照してください。

アクセス管理者

[ポリシー（Policies）] メニューでアクセス制御ポリシー機能や関連する機能へのアクセスが可能です。アクセス管理者は、ポリシーを展開できません。

管理者

管理者は製品内のすべてのものにアクセスできるため、セッションでセキュリティが侵害されると、高いセキュリティ リスクが生じます。このため、ログイン セッション タイムアウトから管理者を除外することはできません。

セキュリティ上の理由から、管理者ロールの使用を制限する必要があります。

検出管理者（Discovery Admin）

[ポリシー（Policies）] メニューのネットワーク検出機能、アプリケーション検出機能、相関機能にアクセス可能です。検出管理者は、ポリシーを展開できません。

外部データベース ユーザ（読み取り専用）

JDBC SSL 接続をサポートするアプリケーションを使用したデータベースへの読み取り専用アクセスを提供します。アプライアンスの認証を行うサードパーティのアプリケーションについては、システム設定内でデータベースアクセスを有効にする必要があります。Webインターフェイスでは、外部データベースユーザは、[ヘルプ（Help）] メニューのオンライン ヘルプ関連のオプションのみにアクセスできます。このロールの機能は、web イ

ンターフェイスに搭載されていないため、サポートやパスワードの変更を容易にするためにのみアクセスが可能です。

侵入管理者（Intrusion Admin）

[ポリシー（Policies）] メニューと [オブジェクト（Objects）] メニューの侵入ポリシー機能、侵入ルール機能、ネットワーク分析ポリシー機能のすべてにアクセスが可能です。侵入管理者は、ポリシーを展開できません。

メンテナンス ユーザ（Maintenance User）

監視機能やメインテナンス機能へのアクセスが可能です。メンテナンス ユーザは、[ヘルス（Health）] メニューや [システム（System）] メニューのメンテナンス関連オプションにアクセスできます。

ネットワーク管理者（Network Admin）

[ポリシー（Policies）] メニューのアクセス制御機能、SSL インスペクション機能、DNS ポリシー機能、アイデンティティ ポリシー機能、および [デバイス（Devices）] メニューのデバイス設定機能へのアクセスが可能です。ネットワーク管理者は、デバイスへの設定の変更を展開できます。

セキュリティ アナリスト

セキュリティ イベント分析機能へのアクセスと [概要（Overview）] メニュー、[分析（Analysis）] メニュー、[ヘルス（Health）] メニュー、[システム（System）] メニューのヘルス イベントに対する読み取り専用のアクセスが可能です。

セキュリティ アナリスト（読み取り専用）（Security Analyst (Read Only)）

[Overview] メニュー、[Analysis] メニュー、[Health] メニュー、[System] メニューのセキュリティイベント分析機能とヘルスイベント機能への読み取り専用アクセスを提供します。

このロールを持つユーザは、次のこともできます。

- 特定のデバイスのヘルスモニタのページから、トラブルシューティング ファイルを生成してダウンロードする。
- ユーザ設定で、ファイルのダウンロードの設定を行う。
- ユーザ設定で、イベントビューのデフォルトのタイムウィンドウを設定する（[Audit Log Time Window] を除く）。

セキュリティ承認者（Security Approver）

[ポリシー（Policies）] メニューのアクセス制御ポリシーや関連のあるポリシー、ネットワーク検出ポリシーへの制限付きのアクセスが可能です。セキュリティ承認者はこれらのポリシーを表示し、展開できますが、ポリシーを変更することはできません。

脅威インテリジェンス ディレクタ（TID）ユーザー

[インテリジェンス（Intelligence）] メニューの脅威インテリジェンス ディレクタ設定にアクセスできます。Threat Intelligence Director (TID) ユーザーは、TID の表示および設定が可能です。

ユーザ パスワード

Management Center の内部ユーザーアカウントのパスワードには、Lights-Out Management（LOM）が有効な場合と無効な場合に応じて、次のルールが適用されます。外部認証されたアカウントまたはセキュリティ認定コンプライアンスが有効になっているシステムには、異なるパスワード要件が適用されます。詳細については、Management Center の外部認証の設定（150 ページ）と セキュリティ認定準拠（393 ページ）を参照してください。

Management Center の初期設定時に、**admin** ユーザーは、以下の表に記載されている強力なパスワード要件に準拠するようにアカウントパスワードを設定する必要があります。物理 Management Center の場合、LOM が有効になっている強力なパスワード要件が使用され、仮想 Management Center の場合、LOM が有効になっていない強力なパスワード要件が使用されます。この時点で、システムは web インターフェイスの **admin** と CLI アクセスの **admin**のパスワードを同期します。初期設定後、Web インターフェイスの **admin** は強力なパスワード要件を削除できますが、CLI アクセスの **admin** は、LOM が有効になっていない状態では、常に強力なパスワード要件に準拠している必要があります。

	LOM が有効になっていない	LOM が有効になっている
パスワードの強度チェックがオンになっている	パスワードには以下を含める必要があります。 • 8 文字以上または管理者がユーザーに設定した文字数のいずれか大きい方。 • 同じ文字が 3 文字以上連続していない • 1 つ以上の小文字 • 少なくとも 1 つの大文字 • 少なくとも 1 つの数字 • ! など、少なくとも 1 つの特殊文字@ # * - _ + システムは、英語の辞書に載っている多くの単語だけでなく、一般的なパスワードハッキング技術で簡単に解読できるその他の文字列も含まれる特殊なディクショナリと照合してパスワードをチェックします。	パスワードには以下を含める必要があります。 • 8 ～ 20 文字（MC 1000、MC 2500、および MC 4500 の場合、上限は 20 文字ではなく 14 文字） • 同じ文字が 3 文字以上連続していない • 1 つ以上の小文字 • 少なくとも 1 つの大文字 • 少なくとも 1 つの数字 • ! など、少なくとも 1 つの特殊文字@ # * - _ + 特殊文字のルールは、物理 Management Center のシリーズ間で異なります。特殊文字の選択を、上記の最後の箇条書きに記載されている特殊文字に制限することをお勧めします。 パスワードにユーザー名を含めないでください。 システムは、英語の辞書に載っている多くの単語だけでなく、一般的なパスワードハッキング技術で簡単に解読できるその他の文字列も含まれる特殊なディクショナリと照合してパスワードをチェックします。

	LOM が有効になっていない	LOM が有効になっている

パスワードの強度チェックがオフになっている	パスワードは、管理者がユーザーに対して設定した最小文字数以上である必要があります。（詳細については、内部ユーザーの追加または編集（147 ページ）を参照してください）。	パスワードには以下を含める必要があります。
		• 8 ～ 20 文字（MC 1000、MC 2500、および MC 4500 の場合、上限は 20 文字ではなく 14 文字）
		• 次の 4 つのカテゴリの少なくとも 3 つのカテゴリに属する文字：
		  • 大文字の英字
		  • 小文字の英字
		  • ディジット
		  • ! などの特殊文字@ # * - _ +
		特殊文字のルールは、物理 Management Center のシリーズ間で異なります。特殊文字の選択を、上記の最後の箇条書きに記載されている特殊文字に制限することをお勧めします。
		パスワードにユーザー名を含めないでください。

Management Center のユーザーアカウントの注意事項と制約事項

- Management Center には、すべてのアクセス形式のローカルユーザーアカウントとして **admin** ユーザーが含まれています。**admin** ユーザーは削除できません。デフォルトの初期パスワードは **Admin123** です。初期化プロセス中に、この初期パスワードの変更が強制されます。システム初期化の詳細については、ご使用のモデルの『*Getting Started Guide*』を参照してください。
- デフォルトでは、Management Center のすべてのユーザーアカウントに次の設定が適用されます。
  - パスワードの再利用に制限はありません。
  - システムは正常なログインを追跡しません。

- システムは、不正なログインクレデンシャルを入力したユーザーに対して時間が指定された一時的なロックアウトを適用しません。
- 同時に開くことができる読み取り専用セッションと読み取り/書き込みセッションの数には、ユーザー定義の制限はありません。

すべてのユーザーのこれらの設定は、システム設定として変更できます（**システム**（⚙）> **[構成（Configuration）]** > **[ユーザー構成（User Configuration）]**）ユーザーの設定 （125 ページ）を参照してください。

- 初期設定時にデフォルトのアクセスロールをユーザーに割り当てる場合は、最小限の権限の原則に従うようにしてください。ユーザーがログイン情報を使用してシステムに初めてログインすると、アカウントにこのデフォルトのアクセスロールが割り当てられます。デフォルトのアクセスロールは、誰もがシステムにログインするために必要な最小限の権限にすることを推奨します。たとえば、共通ユーザーにはデフォルトのアクセスロールとしてセキュリティアナリスト（読み取り専用）ロールを付与し、管理者を別の管理者のグループに追加して完全な管理者権限を付与することができます。デフォルトのアクセスロールを割り当てるときに最小権限の原則に従わない場合、以降のログインでユーザーに意図しない権限レベルが割り当てられる可能性があります。これにより、必要なアクセスロールを超える権限がユーザーに付与される場合があります。このガイドラインは、すべてのユーザー（内部ユーザー、外部ユーザー、または CAC ユーザー）に適用されます。

  デフォルトのアクセスロールでログインしているユーザーが一時的に権限を昇格する必要がある場合、管理者権限を持つユーザーは、より高い権限を持つロールを割り当てることで、必要な高いレベルのアクセスを一時的にそのユーザーに提供できます。この権限は、非アクティブな状態が 24 時間続くと取り消され、ユーザーはデフォルトのアクセスロールに戻ります。

  ユーザーがより高い権限レベル（システム管理者など）に永続的なアクセスロールを再割り当てする必要がある場合は、グループ制御アクセスロール方式を使用して、管理者アクセス権をユーザーに付与します。この方法では、指定されたアクセスロールが 24 時間を超えて保持され、ユーザーはグループ割り当てに従って正しい権限レベルを持つことが保証されます。グループ制御アクセスロールの設定の詳細については、ステップ 15の項を参照してください。

Management Center のユーザーアカウントの要件と前提条件

サポート モデル

Management Center

サポートされるドメイン

- SSO 設定：グローバルのみ。

- 他のすべての機能：すべて。

ユーザ ロール

- SSO設定：内部で認証された、またはLDAPまたはRADIUSによって認証された管理ロールを持つユーザーのみが SSO を設定できます。
- その他すべての機能：管理者ロールを持つすべてのユーザー。
- LDAP を使用した共通アクセス カード認証の設定 （167 ページ）もネットワーク管理者ロールをサポートしています。

内部ユーザーの追加または編集

この手順では、Management Center のカスタム内部ユーザーアカウントを追加する方法について説明します。

[システム（System）]>[ユーザー（Users）]>[ユーザー（Users）]には、手動で追加した内部ユーザーと、LDAPまたはRADIUS認証でユーザーがログインしたときに自動的に追加された外部ユーザーの両方が表示されます。外部ユーザーについては、より高い権限を持つロールを割り当てると、この画面のユーザーロールを変更できます。パスワード設定を変更することはできません。

Management Center のマルチドメイン展開では、ユーザは作成されたドメインでのみ表示されます。グローバルドメインにユーザーを追加してからリーフドメインのユーザーロールを割り当てると、そのユーザーがリーフドメインに所属していても、追加されたグローバル[ユーザー（Users）] ページにそのユーザーが表示されます。

デバイスでセキュリティ認定コンプライアンスまたは Lights-Out Management（LOM）を有効にすると、異なるパスワード制限が適用されます。セキュリティ認定コンプライアンスの詳細については、セキュリティ認定準拠 （393 ページ）を参照してください。

リーフ ドメインにユーザーを追加した場合、そのユーザーはグローバル ドメインからは表示されません。

（注） 複数の管理者ユーザーが Management Center で同時に新しいユーザーを作成することは避けてください。ユーザーデータベースアクセスの競合によってエラーが発生する可能性があります。

手順

ステップ 1 システム（⚙） > **[ユーザー（Users）]**を選択します。

ステップ 2 新しいユーザを作成するには、以下の手順を実行します。

a) [ユーザの作成（Create User）] をクリックします。
b) [ユーザー名（User Name）] に入力します。

ユーザー名は、次の制限に従う必要があります。

- 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字。
- 文字は大文字と小文字を使用できます。
- ピリオド（.）、ハイフン（-）、アンダースコア（_）以外の句読点または特殊文字は使用できません。

ステップ 3 既存のユーザーを編集するには、編集するユーザーレイヤの横にある **[編集（Edit）]**（）をクリックします。

ステップ 4 [実際の名前（Real Name）]：アカウントが属しているユーザーまたは部門を識別するための説明情報を入力します。

ステップ 5 LDAP または RADIUS によりログインしたときに自動的に追加されたユーザーに対しては、[外部認証方式の使用（Use External Authentication Method）] チェックボックスがオンになっています。外部ユーザーを事前設定する必要はないので、このフィールドは無視できます。外部ユーザについては、このチェックボックスをオフにすることで、そのユーザを内部ユーザに戻すことができます。

ステップ 6 [パスワード（Password）] および [パスワードの確認（Confirm Password）] フィールドに値を入力します。

この値は、このユーザに設定したパスワード オプションに準拠している必要があります。

ステップ 7 [ログイン失敗の最大回数（Maximum Number of Failed Logins）] を設定します。

各ユーザーが、ログイン試行の失敗後に、アカウントがロックされるまでに試行できるログインの最大回数を指定する整数を、スペースなしで入力します。デフォルト設定は 5 回です。ログイン失敗回数を無制限にするには、**0** を使用します。**管理者**アカウントは、ログイン失敗回数が最大数に達してもロックアウトされません（ただし、セキュリティ認定コンプライアンスを有効にした場合は除きます）。

ステップ 8 [パスワードの最小長（Minimum Password Length）] を設定します。

ユーザーのパスワードの必須最小長（文字数）を指定する整数を、スペースなしで入力します。デフォルト設定は **8** です。値 **0** は、最小長が必須ではないことを示します。

ステップ 9 [パスワードの有効期限までの日数（Days Until Password Expiration）] を設定します。

ユーザのパスワードの有効期限までの日数を入力します。デフォルト設定は、パスワードが期限切れにならないことを示す **0** です。デフォルトから変更すると、[ユーザ（Users）] リストの [パスワードのライフタイム（Password Lifetime）] 列に、各ユーザのパスワードの残っている日数が表示されます。

ステップ 10 [パスワードの有効期限を事前に警告する日数（Days Before Password Expiration Warning）] を設定します。

パスワードが実際に期限切れになる前に、ユーザがパスワードを変更する必要があるという警告が表示される日数を入力します。デフォルト設定は 0 日間です。

ステップ 11 以下の**オプション**を設定します。

- [ログイン時にパスワードのリセットを強制（Force Password Reset on Login）]：次回のログイン時にユーザーにパスワード変更を強制します。
- [パスワードの強度のチェック（Check Password Strength）]：強力なパスワードを必須にします。パスワード強度チェックが有効になっている場合、パスワードは、ユーザ パスワード （143 ページ）で説明されている強力なパスワードの要件に従う必要があります。
- [ブラウザセッションタイムアウトの適用除外（Exempt from Browser Session Timeout）]：非アクティブ状態が原因で、ユーザーのログインセッションが終了しないようにします。管理者ロールが割り当てられているユーザーを除外することはできません。

ステップ 12 [ユーザーロールの設定（User Role Configuration）] エリアで、ユーザーロールを割り当てます。ユーザーロールの詳細については、Web インターフェイス用のユーザー ロールのカスタマイズ （231 ページ）を参照してください。

外部ユーザーについては、ユーザーロールがグループメンバーシップ（LDAP）を介して、またはユーザー属性（RADIUS）に基づいて割り当てられている場合、最小限のアクセス権限を削除することはできません。ただし、追加の権限を割り当てることはできます。ユーザ ロールがデバイスで設定したデフォルトのユーザ ロールの場合は、ユーザ アカウントのロールを制限なしに変更できます。ユーザー ロールを変更すると、[ユーザー（Users）] タブの [認証方式（Authentication Method）] 列に、[外部-ローカル変更（External - Locally Modified）] のステータスが表示されます。

表示されるオプションは、デバイスが単一ドメイン展開かマルチドメイン展開かによって異なります。

- 単一ドメイン：ユーザーを割り当てるユーザーロールをオンにします。
- マルチドメイン：マルチドメイン展開では、管理者アクセス権限があるドメインでユーザーアカウントを作成できます。ユーザーは各ドメインで異なる権限を持つことができます。先祖ドメインと子孫ドメインの両方でユーザ ロールを割り当てることができます。たとえば、あるユーザにグローバル ドメインでは読み取り専用権限を割り当て、子孫ドメインでは管理者権限を割り当てることができます。次の手順を参照してください。
  1. [ドメインの追加（Add Domain）] をクリックします。
  2. [ドメイン（Domain）] ドロップダウン リストからドメインを選択します。
  3. ユーザーを割り当てるユーザーロールをオンにします。
  4. **[Save（保存）]** をクリックします。

ステップ 13 （任意、物理 Management Center のみ）ユーザーに管理者ロールを割り当てている場合は、[管理者オプション（Administrator Options）] が表示されます。[Allow Lights-Out Management Access]

を選択すると、ユーザーに Lights-Out Management アクセスを許可できます。Lights-Out Management の詳細については、Lights-Out 管理の概要 （109 ページ）を参照してください。

ステップ 14 [保存（Save）] をクリックします。

Management Center の外部認証の設定

外部認証を有効にするには、1 つ以上の外部認証オブジェクトを追加する必要があります。

Management Center の外部認証について

外部認証を有効にすると、Management Center により外部認証オブジェクトで指定された LDAP または RADIUS サーバーを使用してユーザークレデンシャルが検証されます。

Web インターフェイスアクセス用に複数の外部認証オブジェクトを設定できます。たとえば、5 つの外部認証オブジェクトがある場合、いずれかのオブジェクトのユーザーを Web インターフェイスにアクセスするために認証できます。CLI アクセスに使用できる外部認証オブジェクトは 1 つのみです。複数の外部認証オブジェクトが有効になっている場合、ユーザーはリスト内の最初のオブジェクトのみを使用して認証できます。

外部認証オブジェクトは、Management Center および Threat Defense デバイスで使用できます。さまざまなアプライアンス/デバイス タイプで同じオブジェクトを共有することも、別々のオブジェクトを作成することもできます。

（注） タイムアウト範囲は Threat Defense と Management Center で異なるため、オブジェクトを共有する場合は、Threat Defense の小さめのタイムアウト範囲（LDAP の場合は 1 ー 30 秒、RADIUS の場合は 1 ー 300 秒）を超えないようにしてください。タイムアウトを高めの値に設定すると、Threat Defense 外部認証設定が機能しません。

Management Center では、**[システム（System）] > [ユーザー（Users）] > [外部認証（External Authentication）]** タブで外部認証オブジェクトを直接有効にします。この設定は、Management Center の使用にのみ影響し、管理対象デバイスを使用する場合には、このタブで有効にする必要はありません。Threat Defense のデバイスでは、デバイスに展開するプラットフォーム設定で外部認証オブジェクトを有効にする必要があります。

外部認証オブジェクト内の CLI ユーザーから Web インターフェイスのユーザーが個別に定義されます。RADIUS の CLI ユーザーの場合、外部認証オブジェクト内に RADIUS ユーザー名のリストを事前に設定しておく必要があります。LDAP では、LDAP サーバーの CLI ユーザーと一致するようにフィルタを指定できます。

CAC 認証用にも設定されている CLI アクセスの LDAP オブジェクトは使用できません。

（注） CLI へのアクセス権を持つユーザーは、**expert** コマンドを使用して Linux シェルにアクセスできます。Linux シェルユーザーは root 権限を取得できます。このため、セキュリティ上のリスクが生じる可能性があります。次のことを実行してください。

- CLI または Linux シェルアクセスが付与されるユーザーのリストを制限します。
- Linux シェルユーザーを作成しないでください。

LDAP について

Lightweight Directory Access Protocol（LDAP）により、ユーザ クレデンシャルなどのオブジェクトをまとめるためのディレクトリをネットワーク上の一元化されたロケーションにセットアップできます。こうすると、複数のアプリケーションがこれらのクレデンシャルと、クレデンシャルの記述に使用される情報にアクセスできます。ユーザーのクレデンシャルを変更する必要がある場合も、常に 1 箇所でクレデンシャルを変更できます。

Microsoft 社は、2020 年に Active Directory サーバーで LDAP バインディングと LDAP 署名の適用を開始すると発表しました。Microsoft 社がこれらを要件にするのは、デフォルト設定で Microsoft Windows を使用する場合に権限昇格の脆弱性が存在するために、中間者攻撃者が認証要求を Windows LDAP サーバーに正常に転送できる可能性があるからです。詳細については、Microwoft 社のサポートサイトで「2020 LDAP channel binding and LDAP signing requirement for Windows」を参照してください。

まだ行っていない場合は、Active Directory サーバーによる認証で TLS/SSL 暗号化の使用を開始することをお勧めします。

RADIUS について

Remote Authentication Dial In User Service（RADIUS）は、ネットワーク リソースへのユーザ アクセスの認証、認可、およびアカウンティングに使用される認証プロトコルです。RFC 2865 に準拠するすべての RADIUS サーバーで、認証オブジェクトを作成できます。

Cisco Secure Firewall デバイスは、SecurID トークンの使用をサポートします。SecurID を使用したサーバーによる認証を設定した場合、そのサーバーに対して認証されるユーザーは、自身の SecurID PIN の末尾に SecurID トークンを追加したものをログイン時にパスワードとして使用します。SecurID をサポートするために、Cisco Secure Firewall デバイスで追加の設定を行う必要はありません。

Management Center 用の LDAP 外部認証オブジェクトの追加

デバイス管理用に外部ユーザをサポートするために、LDAP サーバを追加します。

始める前に

- デバイス上にドメイン名ルックアップの DNS サーバーを指定する必要があります。この手順で LDAP サーバーのホスト名ではなく IP アドレスを指定した場合、ホスト名に含め

ることができる認証用の URI を LDAP サーバーが返す場合があります。ホスト名を解決するにはDNS ルックアップが必要です。DNS サーバーを追加するには「Management Center 管理インターフェイスの変更 （92 ページ）」を参照してください。

- CAC 認証に使用する LDAP 認証オブジェクトを設定する場合は、コンピュータに挿入されている CAC を取り外さないでください。ユーザー証明書を有効にした後では、CAC が常に挿入された状態にしておく必要があります。

手順

ステップ 1 システム（⚙） > **[ユーザー（Users）]**を選択します。

ステップ 2 [外部認証（External Authentication）] タブをクリックします。

ステップ 3 [外部認証オブジェクトの追加（Add External Authentication Object）][追加（Add）] アイコン（＋） をクリックします。

ステップ 4 [認証方式（Authentication Method）] を [LDAP] に設定します。

ステップ 5 （任意）CAC 認証および認可にこの認証オブジェクトを使用する予定の場合は、[CAC] チェックボックスをオンにします。

CAC 認証および認可を完全に設定するには、「LDAP を使用した共通アクセス カード認証の設定 （167 ページ）」の手順にも従う必要があります。このオブジェクトは、CLI ユーザーには使用できません。

ステップ 6 [CAC環境変数（CAC Environment Variable）] フィールドに、ログインに使用するユーザー名を含む環境変数を入力します。[CAC] チェックボックスをオンにすると、このフィールドが表示されます。CAC を有効にしてブラウザで使用してアプライアンスにアクセスすると、CAC 情報を含む環境変数をログインに使用できます。例：`SSL_CLIENT_S_DN_CN = last.first.1234567890`

ステップ 7 [CACユーザー名テンプレート（CAC User Name Template）] フィールドに、CAC 環境変数からユーザー名の部分を抽出するためのテンプレートを入力します。たとえば、CAC 環境変数文字列の最後の 10 桁を抽出する場合は、「`\.(\d{10})$`」と入力します。

ステップ 8 [名前（Name）] とオプションの [説明（Description）] を入力します。

ステップ 9 ドロップダウン リストから [サーバタイプ（Server Type）] を選択します。

ヒント [デフォルトの設定（Set Defaults）] をクリックした場合は、デバイスにより [ユーザー名テンプレート（User Name Template）]、[UIアクセス属性（UI Access Attribute）]、**[CLI アクセス属性（CLI Access Attribute）]**、[グループメンバー属性（Group Member Attribute）]、および [グループメンバーURL属性（Group Member URL Attribute）] フィールドに、サーバータイプのデフォルト値が入力されます。

ステップ 10 [プライマリサーバ（Primary Server）] の場合は、[ホスト名/IPアドレス（Host Name/IP Address）] を入力します。

証明書を使用して TLS または SSL 経由で接続する場合は、証明書のホスト名が、このフィールドに入力するホスト名と一致している必要がりあります。また、暗号化接続では IPv6 アドレスはサポートされていません。

ステップ 11 （任意）[ポート（Port）] をデフォルトから変更します。

ステップ 12 （任意）[バックアップサーバ（Backup Server）] パラメータを入力します。

ステップ 13 [LDAP固有のパラメータ（LDAP-Specific Parameters）] を入力します。

a) ユーザーがアクセスする LDAP ディレクトリの [ベースDN（Base DN）] を入力します。たとえば、Example 社のセキュリティ（Security）部門の名前を認証するには、`ou=security,dc=example,dc=com` と入力します。または、[DNの取得（Fetch DNs）] をクリックし、ドロップダウン リストから適切なベース識別名を選択します。

b) （任意）[基本フィルタ（Base Filter）] を入力します。たとえば、ディレクトリ ツリー内のユーザー オブジェクトに `physicalDeliveryOfficeName` 属性が設定されており、New York 支店のユーザーに対しこの属性に値 `NewYork` が設定されている場合、New York 支店のユーザーだけを取得するには、`(physicalDeliveryOfficeName=NewYork)` と入力します。

CAC認証を使用している場合、アクティブなユーザーアカウント（無効なユーザーアカウントを除く）のみをフィルタ処理するには、`(!(userAccountControl:1.2.840.113556.1.4.803:=2))` と入力します。この条件は、`ldpgrp` グループに属し、`userAccountControl` 属性値が `2`（無効）ではない AD 内のユーザーアカウントを取得します。

c) LDAP サーバを参照するために十分なクレデンシャルを持つユーザの [ユーザ名（User Name）] を入力します。たとえば、ユーザ オブジェクトに `uid` 属性が含まれている OpenLDAP サーバに接続し、Example 社のセキュリティ（Security）部門の管理者のオブジェクトの `uid` に値 `NetworkAdmin` が設定されている場合は、`uid=NetworkAdmin,ou=security,dc=example,dc=com` と入力します。

d) [パスワード（Password）] および [パスワードの確認（Confirm Password）] フィールドにユーザ パスワードを入力します。

e) （任意）[詳細オプションを表示（Show Advanced Options）] をクリックして、次の詳細オプションを設定します。

- **[暗号化（Encryption）]**：**[なし（None）]**、**[TLS]**、または **[SSL]** をクリックします。

  ポートを指定した後で暗号化方式を変更すると、ポートがその方式のデフォルト値にリセットされます。[なし（None）] または [TLS] の場合、ポートはデフォルト値の 389 にリセットされます。[SSL] 暗号化を選択した場合、ポートは 636 にリセットされます。

- [SSL証明書アップロードパス（SSL Certificate Upload Path）]：SSL または TLS 暗号化の場合は、[ファイルの選択（Choose File）] をクリックして証明書を選択する必要があります。

  アップロードされた証明書を削除するには、[ロードされた証明書のクリア（Clear load certificate ）] チェックボックスをオンにします。このオプションは、証明書をアップロード済みで、外部認証オブジェクトの編集モードの場合にのみ表示されます。

  以前にアップロードした証明書を置き換えるには、新しい証明書をアップロードし、設定をデバイスに再展開して、新しい証明書を上書きコピーします。

  （注） TLS 暗号化には、すべてのプラットフォームで証明書が必要です。中間者攻撃を防ぐため、SSL 証明書を常にアップロードしておくことをお勧めします。

- [ユーザー名テンプレート（User Name Template）]：[UIアクセス属性（UI Access Attribute）] に対応するテンプレートを入力します。たとえば、UI アクセス属性が `uid` である OpenLDAP サーバに接続し、Example 社のセキュリティ（Security）部門で働くすべてのユーザを認証するには、[ユーザ名テンプレート（User Name Template）] フィールドに `uid=%s,ou=security,dc=example,dc=com` と入力します。Microsoft Active Directory Server の場合は `%s@security.example.com` と入力します。

  CAC 認証では、このフィールドは必須です。

- [シェルユーザー名テンプレート（Shell User Name Template）]：CLI ユーザーを認証するために [CLIアクセス属性（CLI Access Attribute）] に対応するテンプレートを入力します。たとえば、CLI アクセス属性が `sAMAccountName` である OpenLDAP サーバーに接続し、セキュリティ（Security）部門で働くすべてのユーザーを認証するには、[シェルユーザー名テンプレート（Shell User Name Template）] フィールドに `%s` と入力します。

- [タイムアウト（秒）（Timeout (Seconds)）]：バックアップ接続にロールオーバーするまでの秒数（1 ー 1024 秒）を入力します。デフォルトは 30 です。

  （注） タイムアウト範囲は Threat Defense と Management Center で異なるため、オブジェクトを共有する場合は、Threat Defense の小さめのタイムアウト範囲（1 ー 30 秒）を超えないようにしてください。タイムアウトを高めの値に設定すると、Threat Defense LDAP 設定が機能しません。

ステップ 14 [属性マッピング（Attribute Mapping）] を設定して、属性に基づいてユーザーを取得します。

- [UIアクセス属性（UI Access Attribute）] を入力するか、[属性の取得（Fetch Attrs）] をクリックして利用可能な属性のリストを取得します。たとえば Microsoft Active Directory Server では、Active Directory Server ユーザーオブジェクトに `uid` 属性がないため、UI アクセス属性を使用してユーザーを取得することがあります。代わりに [UI アクセス属性（UI Access Attribute）] フィールドに `userPrincipalName` と入力して、`userPrincipalName` 属性を検索できます。

  CAC 認証では、このフィールドは必須です。

- ユーザー識別タイプ以外のシェルアクセス属性を使用する場合は、[CLIアクセス属性（CLI Access Attribute）] [シェルアクセス属性（Shell Access Attribute）]を設定します。たとえば、Microsoft Active Directory Server で、`sAMAccountName` CLI アクセス属性を使用して CLI アクセスユーザーを取得するには、`sAMAccountName` と入力します。

ステップ 15 （任意） [グループ制御アクセスロール（Group Controlled Access Roles）] を設定します。

グループ制御アクセスロールを使用してユーザの権限を事前に設定していない場合、ユーザには、外部認証ポリシーでデフォルトで付与される権限だけが与えられています。

a) （任意） ユーザー ロールに対応するフィールドに、これらのロールに割り当てる必要があるユーザーを含む LDAP グループの識別名を入力します。

参照するグループはすべてLDAPサーバーに存在している必要があります。スタティックLDAP グループまたはダイナミック LDAP グループを参照できます。スタティック LDAPグループとは、特定のユーザを指し示すグループオブジェクト属性によってメンバーシップが決定されるグループであり、ダイナミックLDAPグループとは、ユーザオブジェクト属性に基づいてグループユーザを取得するLDAP検索を作成することでメンバーシップが決定されるグループです。ロールのグループ アクセス権は、グループのメンバーであるユーザにのみ影響します。

ダイナミック グループを使用する場合、LDAP クエリは、LDAP サーバで設定されているとおりに使用されます。この理由から、検索構文エラーが原因で無限ループが発生することを防ぐため、Cisco Secure Firewall デバイスでは検索の再帰回数が 4 回に制限されています。

例：

Example 社の情報テクノロジー（Information Technology）部門の名前を認証するには、[管理者（Administrator）] フィールドに次のように入力します。

```
cn=itgroup,ou=groups, dc=example,dc=com
```

b) 指定したグループのいずれにも属していないユーザの [デフォルトユーザロール（Default User Role）] を選択します。

c) スタティック グループを使用する場合は、[グループ メンバー属性（Group Member Attribute）] を入力します。

例：

デフォルトのSecurity Analystアクセスのためのスタティック グループのメンバーシップを示すために `member` 属性を使用する場合は、`member` と入力します。

d) ダイナミック グループを使用する場合は、[グループ メンバー URL 属性（Group Member URL Attribute）] を入力します。

例：

デフォルトの管理者アクセスに対して指定したダイナミック グループのメンバーを取得する LDAP 検索が `memberURL` 属性に含まれている場合は、`memberURL` と入力します。

ユーザ ロールを変更する場合は、変更した外部認証オブジェクトを保存/展開し、[ユーザ（Users）] 画面からユーザを削除する必要があります。次回のログイン時に、ユーザーが自動的に再度追加されます。

ステップ 16 （任意）**[CLIアクセスフィルタ（CLI Access Filter）]** を設定します。

CLI アクセスの LDAP 認証を防止するには、このフィールドを空白にします。CLI ユーザーを指定するには、次のいずれかの方法を選択します。

- 認証設定の設定時に指定したものと同じフィルタを使用するには、[基本フィルタと同じ（Same as Base Filter）] チェックボックスをオンにします。
- 属性値に基づいて管理ユーザ項目を取得するには、属性名、比較演算子、およびフィルタとして使用する属性値を、カッコで囲んで入力します。たとえば、すべてのネットワーク

管理者の `manager` 属性に属性値 `shell` が設定されている場合は、基本フィルタ `(manager=shell)` を設定できます。

ユーザ名は、次のように Linux に対して有効である必要があります。

- 英数字、ピリオド（.）、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、アットマーク（@）やスラッシュ（/）は使用不可

（注） CLI へのアクセス権を持つユーザーは、**expert** コマンドを使用して Linux シェルにアクセスできます。Linux シェルユーザーは root 権限を取得できます。このため、セキュリティ上のリスクが生じる可能性があります。CLI または Linux シェルアクセスが付与されるユーザーのリストを制限してください。

（注） **[CLIアクセスフィルタ（CLI Access Filter）]** に含まれているユーザーと同じユーザー名を持つ内部ユーザーを作成しないでください。唯一の内部 Management Center ユーザーは **admin** である必要があります。**[CLIアクセスフィルタ（CLI Access Filter）]** に **admin** ユーザーを含めないでください。

ステップ 17 （任意） LDAP サーバーへの接続をテストするには、[テスト（Test）] をクリックします。

テスト出力には、有効なユーザー名と無効なユーザー名が示されます。有効なユーザ名は一意のユーザ名であり、アンダースコア（_）、ピリオド（.）、ハイフン（-）、英数字を使用できます。UI のページ サイズ制限のため、ユーザー数が 1000 を超えているサーバーへの接続をテストする場合、返されるユーザーの数は 1000 であることに注意してください。テストが失敗した場合は、「LDAP 認証接続のトラブルシューティング （237 ページ）」を参照してください。

ステップ 18 （任意） [追加のテストパラメータ（Additional Test Parameters）] を入力して、認証できるようにするユーザのユーザ クレデンシャルをテストすることもできます。[ユーザ名（User Name）] `uid` と [パスワード（Password）] を入力してから、[テスト（Test）] をクリックします。

Microsoft Active Directory Server に接続して `uid` の代わりに UI アクセス属性を指定する場合は、ユーザ名としてこの属性の値を使用します。ユーザの完全修飾識別名も指定できます。

ヒント テストユーザーの名前とパスワードを誤って入力すると、サーバー設定が正しい場合でもテストが失敗します。サーバー設定が正しいことを確認するには、最初に [追加のテスト パラメータ（Additional Test Parameters）] フィールドにユーザー情報を入力せずに [テスト（Test）] をクリックします。正常に完了した場合は、テストする特定ユーザーのユーザー名とパスワードを指定します。

例：

Example 社の `JSmith` ユーザ クレデンシャルを取得できるかどうかをテストするには、`JSmith` と正しいパスワードを入力します。

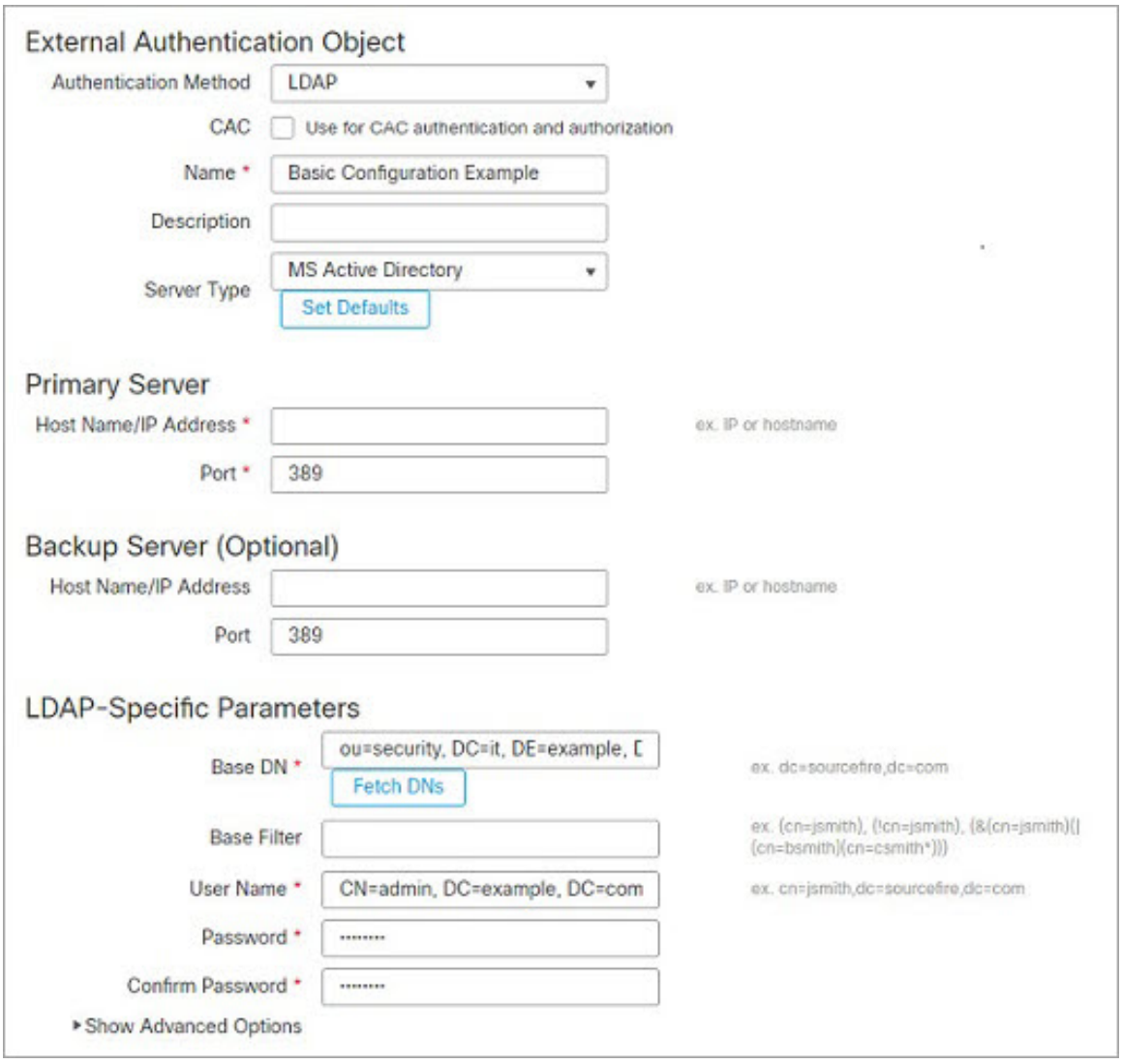
ステップ 19 [保存（Save）] をクリックします。

ステップ 20 このサーバーの使用を有効にします。Management Center でのユーザーの外部認証の有効化（166 ページ）を参照してください。

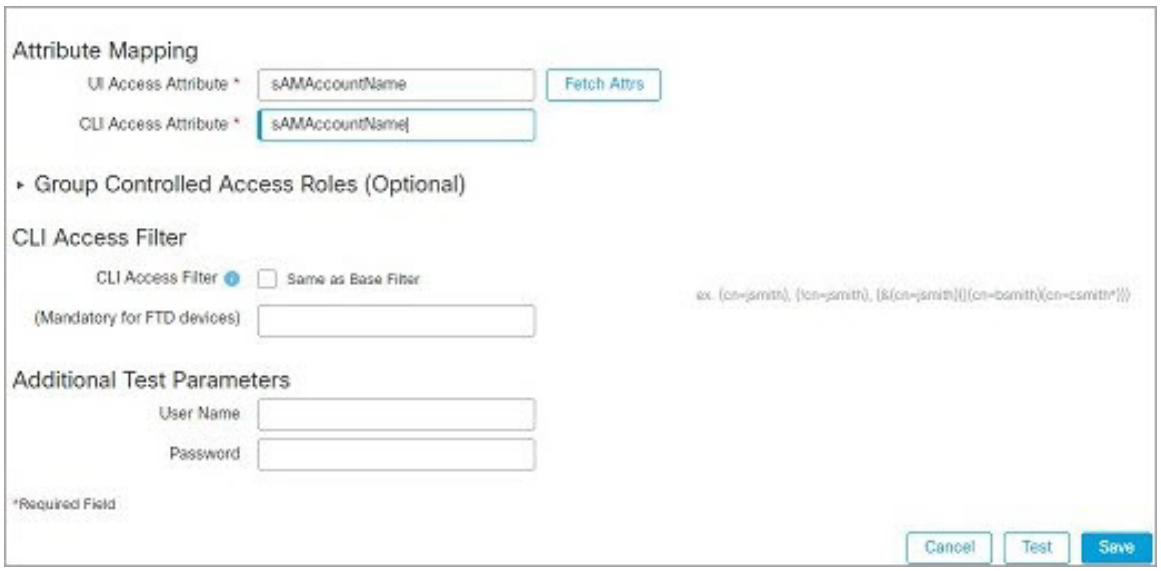
例

基本的な例

次の図は、Microsoft Active Directory Server の LDAP ログイン認証オブジェクトの基本設定を示します。この例の LDAP サーバの IP アドレスは 10.11.3.4 です。接続ではアクセスのためにポート 389 が使用されます。



この例では、Example 社の情報テクノロジー ドメインで、セキュリティ部門のベース識別名として `OU=security,DC=it,DC=example,DC=com` を使用した接続を示しています。



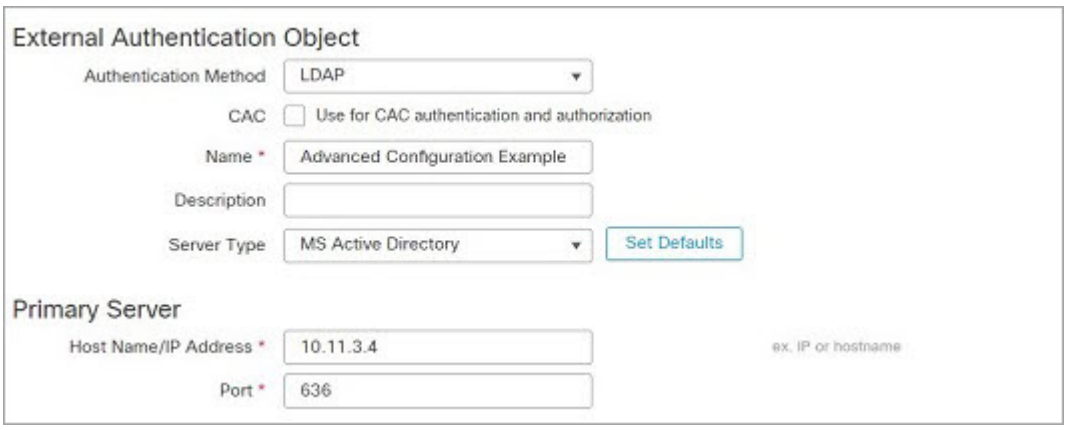
ただし、このサーバーが Microsoft Active Directory Server であるため、ユーザー名の保存に `uid` 属性ではなく `sAMAccountName` 属性が使用されます。サーバのタイプとして MS Active Directory を選択し、[デフォルトの設定（Set Defaults）] をクリックすると、[UI アクセス属性（UI Access Attribute）] が `sAMAccountName` に設定されます。その結果、ユーザーがシステムへのログインを試行すると、システムは各オブジェクトの `sAMAccountName` 属性を検査し、一致するユーザー名を検索します。

また、[CLIアクセス属性（CLI Access Attribute）] が `sAMAccountName` の場合、ユーザーがアプライアンスで CLI アカウントにログインすると、ディレクトリ内のすべてのオブジェクトの各 `sAMAccountName` 属性が検査され、一致が検索されます。

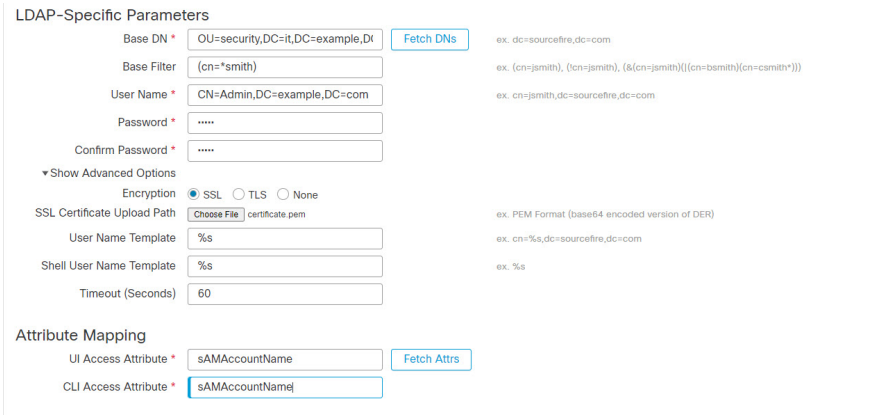
基本フィルタはこのサーバーに適用されないため、システムはベース識別名により示されるディレクトリ内のすべてのオブジェクトの属性を検査することに注意してください。サーバーへの接続は、デフォルトの期間（または LDAP サーバーで設定されたタイムアウト期間）の経過後にタイムアウトします。

高度な例

次の例は、Microsoft Active Directory Server の LDAP ログイン認証オブジェクトの詳細設定を示します。この例の LDAP サーバの IP アドレスは 10.11.3.4 です。接続ではアクセスのためにポート 636 が使用されます。



この例では、Example 社の情報テクノロジー ドメインで、セキュリティ部門のベース識別名として `OU=security,DC=it,DC=example,DC=com` を使用した接続を示しています。ただし、このサーバに基本フィルタ `(cn=*smith)` が設定されていることに注意してください。このフィルタは、サーバーから取得するユーザーを、一般名が `smith` で終わるユーザーに限定します。



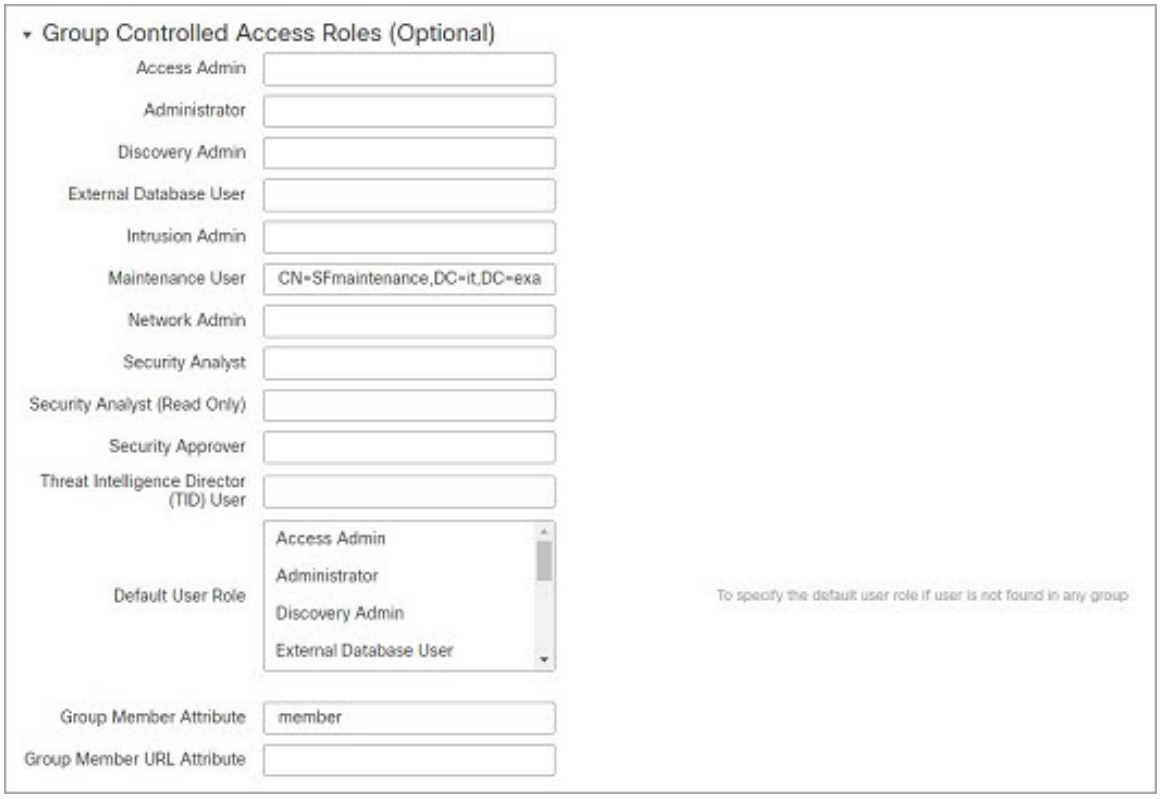
サーバへの接続が SSL を使用して暗号化され、`certificate.pem` という名前の証明書が接続に使用されます。また、[タイムアウト（秒）（Timeout (Seconds)）] の設定により、60 秒経過後にサーバーへの接続がタイムアウトします。

このサーバーが Microsoft Active Directory Server であるため、ユーザー名の保存に `uid` 属性ではなく `sAMAccountName` 属性が使用されます。設定では、[UI Access Attribute] が `sAMAccountName` であることに注意してください。その結果、ユーザーがシステムへのログインを試行すると、システムは各オブジェクトの `sAMAccountName` 属性を検査し、一致するユーザー名を検索します。

また、[CLIアクセス属性（CLI Access Attribute）] が `sAMAccountName` の場合、ユーザーがアプライアンスで CLI アカウントにログインすると、ディレクトリ内のすべてのオブジェクトの各 `sAMAccountName` 属性が検査され、一致が検索されます。

この例では、グループ設定も行われます。[メンテナンスユーザー（Maintenance User）] ロールが、`member` グループ属性を持ち、ベース ドメイン名が

CN=SFmaintenance,=it,=example,=com であるグループのすべてのメンバーに自動的に割り当てられます。



CLI アクセスフィルタは、基本フィルタと同一に設定されます。このため、同じユーザーが Web インターフェイスを使用する場合と同様に、CLI を介してアプライアンスにアクセスできます。

Management Center 用の RADIUS 外部認証オブジェクトの追加

デバイス管理用に外部ユーザをサポートするために、RADIUS サーバを追加します。

マルチドメイン展開では、外部認証オブジェクトは作成されたドメインでのみ使用できます。

手順

ステップ 1 **システム**（⚙） > **[ユーザー（Users）]**を選択します。

ステップ 2 [外部認証（External Authentication）] をクリックします。

ステップ 3 [追加（Add）] アイコン（➕） [外部認証オブジェクトの追加（Add External Authentication Object）] をクリックします。

ステップ 4 [認証方式（Authentication Method）] を [RADIUS] に設定します。

ステップ 5 [名前（Name）] とオプションの [説明（Description）] を入力します。

ステップ 6 [プライマリサーバ（Primary Server）] の場合は、[ホスト名/IPアドレス（Host Name/IP Address）] を入力します。

ステップ 7 （任意） [ポート（Port）] をデフォルトから変更します。

ステップ 8 [RADIUS秘密キー（RADIUS Secret Key）] を入力します。

ステップ 9 （任意） [バックアップサーバ（Backup Server）] パラメータを入力します。

ステップ 10 （任意） [RADIUS固有のパラメータ（RADIUS-Specific Parameters）] を入力します。

a) プライマリサーバーを再試行するまでの [タイムアウト（Timeout）] を 1 ～ 1024 の秒単位で入力します。デフォルトは 30 です。

（注） タイムアウト範囲は Threat Defense と Management Center で異なるため、オブジェクトを共有する場合は、Threat Defense の短いタイムアウト範囲（1 ー 300 秒）を超えないようにしてください。タイムアウトをもっと長い値に設定すると、Threat Defense RADIUS 設定が機能しません。

b) バックアップ サーバーにロールオーバーするまでの [再試行（Retries）] を入力します。デフォルトは 3 です。

c) ユーザ ロールに対応するフィールドに、各ユーザの名前を入力するか、またはこれらのロールに割り当てる必要がある属性と値のペアを指定します。

ユーザ名と属性と値のペアは、カンマで区切ります。

例：

セキュリティ アナリストとする必要があるすべてのユーザの `User-Category` 属性の値が `Analyst` である場合、これらのユーザにそのロールを付与するには、[セキュリティアナリスト（Security Analyst）] フィールドに `User-Category=Analyst` と入力します。

例：

ユーザ `jsmith` と `jdoe` に管理者ロールを付与する場合は、[管理者（Administrator）] フィールドに `jsmith, jdoe` と入力します。

例：

`User-Category` の値が `Maintenance` であるすべてのユーザにメンテナンス ユーザ ロールを付与するには、[メンテナンスユーザ（Maintenance User）] フィールドに `User-Category=Maintenance` と入力します。

d) 指定したグループのいずれにも属していないユーザの [デフォルトユーザロール（Default User Role）] を選択します。

ユーザ ロールを変更する場合は、変更した外部認証オブジェクトを保存/展開し、[ユーザ（Users）] 画面からユーザを削除する必要があります。次回のログイン時に、ユーザーが自動的に再度追加されます。

ステップ 11 （任意）[カスタムRADIUS属性を定義する（Define Custom RADIUS Attributes）]。

RADIUS サーバが、`/etc/radiusclient/` 内の `dictionary` ファイルに含まれていない属性の値を返し、これらの属性を使用してユーザにユーザ ロールを設定する予定の場合は、これらの属性を定義する必要があります。RADIUS サーバでユーザ プロファイルを調べると、ユーザについて返される属性を見つけることができます。

a) [属性名（Attribute Name）] を入力します。

属性を定義する場合は、英数字からなる属性名を指定します。属性名の中の単語を区切るには、スペースではなくダッシュを使用することに注意してください。

b) [属性ID（Attribute ID）] を整数で入力します。

属性 ID は整数にする必要があり、`etc/radiusclient/dictionary` ファイルの既存の属性 ID と競合していてはなりません。

c) ドロップダウン リストから [属性タイプ（Attribute Type）] を選択します。

属性のタイプ（文字列、IP アドレス、整数、または日付）も指定します。

d) [追加（Add）] をクリックして、カスタム属性を追加します。

RADIUS認証オブジェクトの作成時に、そのオブジェクトの新しいディクショナリ ファイルがデバイスの `/var/sf/userauth` ディレクトリに作成されます。追加したすべてのカスタム属性は、ディクショナリ ファイルに追加されます。

例：

シスコ ルータが接続しているネットワーク上で RADIUS サーバーが使用される場合に、`Ascend-Assign-IP-Pool` 属性を使用して、特定の IP アドレス プールからログインするすべてのユーザーに特定のロールを付与するとします。`Ascend-Assign-IP-Pool` は、ユーザがログインできるアドレス プールを定義する整数属性であり、割り当てられる IP アドレス プールの番号を示す整数が指定されます。

そのカスタム属性を宣言するには、属性名が `Ascend-IP-Pool-Definition`、属性 ID が `218`、属性タイプが `integer` のカスタム属性を作成します。

次に、`Ascend-IP-Pool-Definition` 属性値が `2` のすべてのユーザーに対し、読み取り専用の Security Analyst 権限を付与するには、`Ascend-Assign-IP-Pool=2` を [セキュリティ アナリスト（読み取り専用）（Security Analyst (Read Only)）] フィールドに入力します。

ステップ 12 （任意）**[CLIアクセスフィルタ（CLI Access Filter）]** エリアの **[管理者CLIアクセスユーザーリスト（Administrator CLI Access User List）]** フィールドに、CLI アクセスが必要なユーザー名をカンマ区切りで入力します。

これらのユーザー名がRADIUSサーバーのユーザー名と一致していることを確認します。名前は、次のように Linux に対して有効である必要があります。

- 英数字、ピリオド（.）、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、アットマーク（@）やスラッシュ（/）は使用不可

CLI アクセスの RADIUS 認証を防止するには、このフィールドを空白にします。

（注） CLI へのアクセス権を持つユーザーは、**expert** コマンドを使用して Linux シェルにアクセスできます。Linux シェルユーザーは root 権限を取得できます。このため、セキュリティ上のリスクが生じる可能性があります。CLI または Linux シェルアクセスが付与されるユーザーのリストを制限してください。

（注） シェルアクセスフィルタに含まれているユーザーと同じユーザー名を持つ内部ユーザーを削除します。Management Center の場合、内部 CLI ユーザーのみが **admin** です。そのため、**admin** 外部ユーザーを作成しないでください。

ステップ 13 （任意） RADIUS サーバーへの Management Center 接続をテストするには、[テスト（Test）] をクリックします。

ステップ 14 （任意）[追加のテストパラメータ（Additional Test Parameters）] を入力して、認証できるようにするユーザのユーザ クレデンシャルをテストすることもできます。[ユーザ名（User Name）] と [パスワード（Password）] を入力してから、[テスト（Test）] をクリックします。

ヒント テストユーザーの名前とパスワードを誤って入力すると、サーバー設定が正しい場合でもテストが失敗します。サーバー設定が正しいことを確認するには、最初に [追加のテスト パラメータ（Additional Test Parameters）] フィールドにユーザー情報を入力せずに [テスト（Test）] をクリックします。正常に完了した場合は、テストする特定ユーザーのユーザー名とパスワードを指定します。

例：

Example 社の `JSmith` ユーザ クレデンシャルを取得できるかどうかをテストするには、`JSmith` と正しいパスワードを入力します。

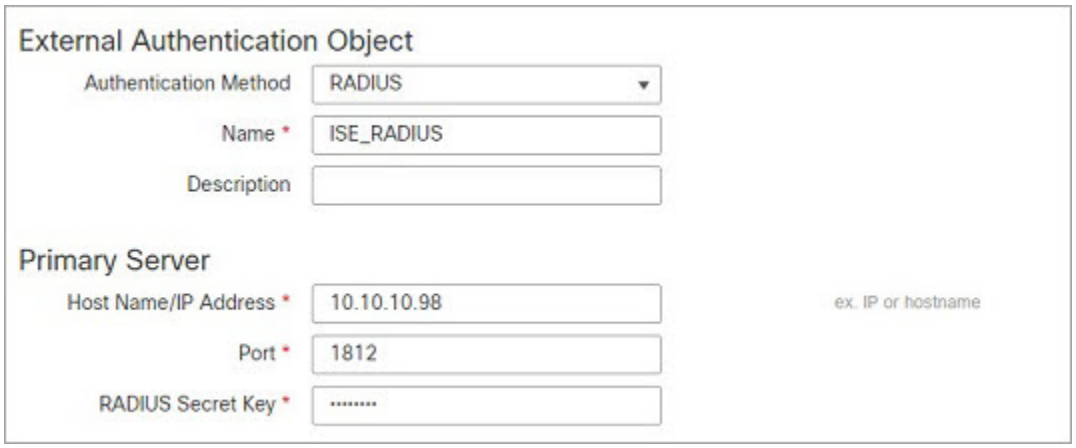
ステップ 15 [保存（Save）] をクリックします。

ステップ 16 このサーバーの使用を有効にします。Management Center でのユーザーの外部認証の有効化（166 ページ）を参照してください。

例

単純なユーザー ロールの割り当て

次の図は、IP アドレスが 10.10.10.98 のポート 1812 で Cisco Identity Services Engine（ISE）が稼働しているサーバーのサンプル RADIUS ログイン認証オブジェクトを示します。バックアップサーバーは定義されていません。



次の例は、Cisco Secure Firewall システムがバックアップサーバー（存在する場合）への接続を試みるまでのタイムアウト（30 秒）と失敗した再試行の数を含む、RADIUS 固有のパラメータを示しています。

次の例は、RADIUS ユーザー ロール設定の重要な特徴を示します。

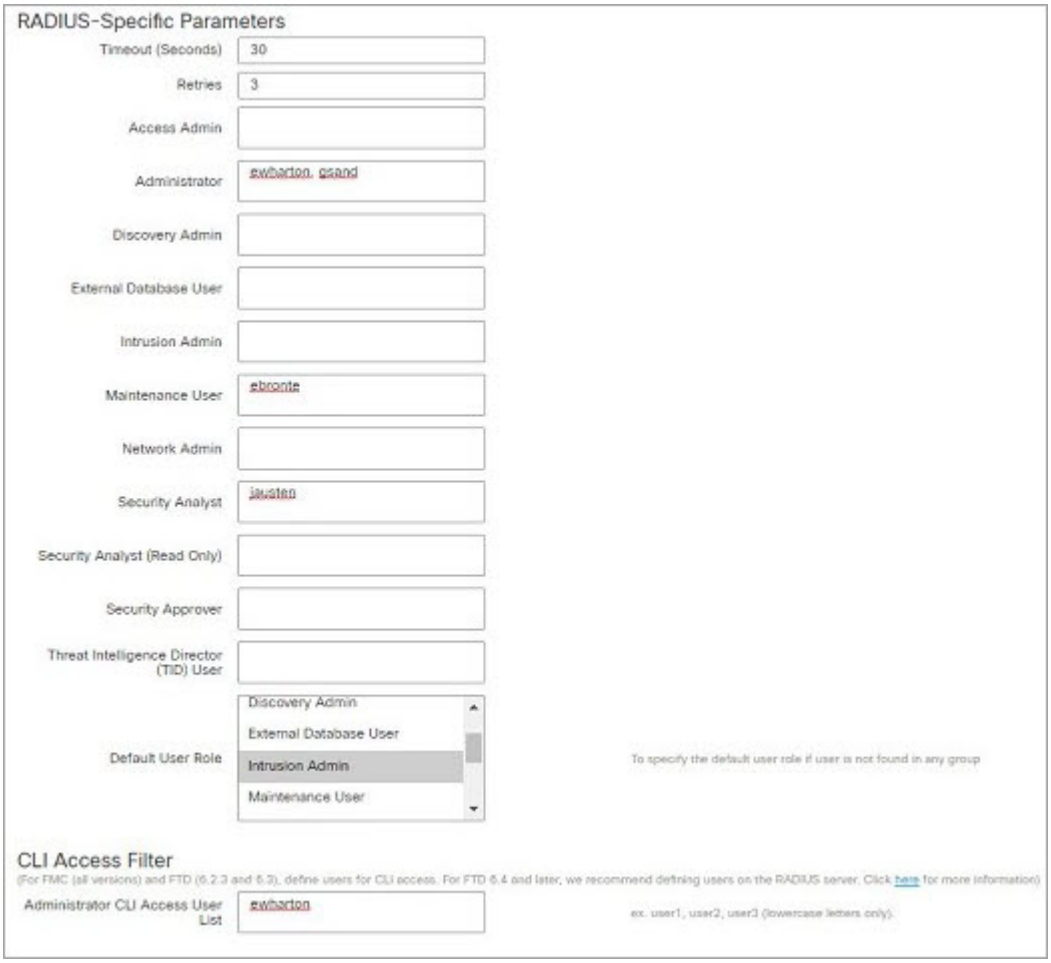
ユーザ `ewharton` および `gsand` には、Web インターフェイスの管理アクセスが付与されます。

ユーザ `cbronte` には、Web インターフェイスのメンテナンス ユーザ アクセスが付与されます。

ユーザー `jausten` には、Web インターフェイスのセキュリティ アナリスト アクセスが付与されます。

ユーザー `ewharton` は、CLI アカウントを使用してデバイスにログインできます。

次の図に、この例のロール設定を示します。

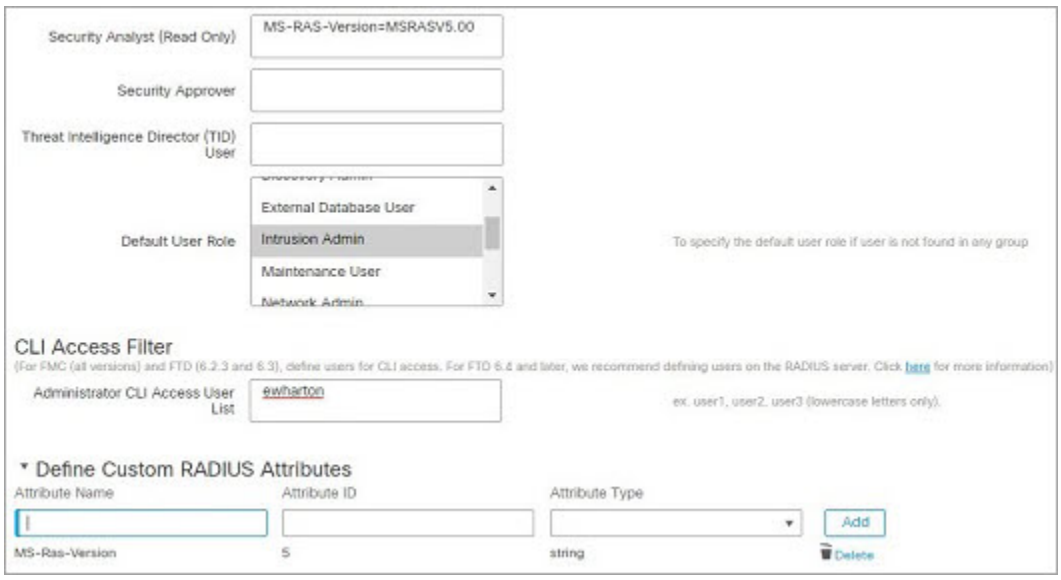


属性と値のペアに一致するユーザーのロール

属性と値のペアを使用して、特定のユーザー ロールが付与される必要があるユーザーを示すこともできます。使用する属性がカスタム属性の場合、そのカスタム属性を定義する必要があります。

次の図は、前述の例と同じ ISE サーバーのサンプル RADIUS ログイン認証オブジェクトでのロール設定とカスタム属性の定義を示します。

ただしこの例では、Microsoft リモート アクセス サーバーが使用されているため、1 つ以上のユーザーの `MS-RAS-Version` カスタム属性が返されます。`MS-RAS-Version` カスタム属性は文字列であることに注意してください。この例では、Microsoft v. 5.00 リモート アクセス サーバー経由で RADIUS にログインするすべてのユーザーに対し、[セキュリティ アナリスト（読み取り専用）（Security Analyst (Read Only)）] ロールが付与される必要があります。このため、属性と値のペア `MS-RAS-Version=MSRASV5.00` を [セキュリティ アナリスト（読み取り専用）（Security Analyst (Read Only)）] フィールドに入力します。



Management Center でのユーザーの外部認証の有効化

管理ユーザーの外部認証を有効にすると、Management Center により外部認証オブジェクトで指定された LDAP または RADIUS サーバーを使用してユーザー クレデンシャルが検証されます。

始める前に

Management Center 用の LDAP 外部認証オブジェクトの追加 （151 ページ）およびManagement Center 用の RADIUS 外部認証オブジェクトの追加 （160 ページ）に従って 1 つまたは複数の外部認証オブジェクトを追加します。

手順

ステップ 1 システム（⚙） > **[ユーザー（Users）]**を選択します。

ステップ 2 [外部認証（External Authentication）] をクリックします。

ステップ 3 外部 Web インターフェイスのユーザーにデフォルトのユーザー ロールを設定します。

ロールがないユーザーは、アクションを実行できません。外部認証オブジェクトで定義されたユーザー ロールは、このデフォルトのユーザー ロールをオーバーライドします。

a) [デフォルトのユーザーロール（Default User Role）] の値をクリックします（デフォルトでは何も選択されていません）。

a) [デフォルトのユーザーロール設定（Default User Role Configuration）] ダイアログ ボックスで、使用するロールをオンにします。

b) [保存（Save）] をクリックします。

ステップ 4 使用する外部認証オブジェクトそれぞれの横にある [有効なスライダ（Slider enabled）] （  ）をクリックします。複数のオブジェクトを有効にすると、ユーザは指定された順序でサーバと照合されます。サーバーの順序を変更する場合は、次の手順を参照してください。

シェル認証を有効にする場合は、**[CLIアクセスフィルタ（CLI Access Filter）]** を含む外部認証オブジェクトを有効にする必要があります。また、CLI アクセスのユーザーは、認証オブジェクトがリストの順序で最も高いサーバーに対してのみ認証できます。

ステップ 5 （任意）認証要求が行われたときに認証サーバーがアクセスされる順序を、サーバーをドラッグアンドドロップして変更できます。

ステップ 6 外部ユーザーに CLI アクセスを許可する場合は、**[シェル認証（Shell Authentication）]** > **[有効（Enabled）]** を選択します。

（注） マルチドメイン機能はCLIではサポートされていません。そのため、[シェル認証（Shell Authentication）] オプションは、グローバルドメインでのみ使用でき、サブドメインでは使用できません。

1 番目の外部認証オブジェクト名は、CLI アクセスに使用されるのは 1 番目のオブジェクトだけであることを示すため、[有効（Enabled）] オプションの横に表示されます。

ステップ 7 [Save and Apply] をクリックします。

LDAP を使用した共通アクセス カード認証の設定

組織で共通アクセスカード（CAC）を使用している場合は、Webインターフェイスにログインしている Management Center ユーザーを認証するように LDAP 認証を設定できます。CAC 認証により、ユーザーは、デバイスに個別のユーザー名とパスワードを指定せずに直接ログインすることができます。

CAC 認証ユーザーは、Electronic Data Interchange Personal Identifier（EDIPI）番号により識別されます。

非アクティブ状態が 24 時間続くと、デバイスにより CAC 認証ユーザが [ユーザ（Users）] タブから削除されます。その後のログインのたびにユーザーが再度追加されますが、ユーザーロールに対する手動の変更は再設定する必要があります。

注意 LDAP を使用して CAC 認証を設定する場合は、ユーザーにデフォルトのアクセスロールを割り当てる際に、最小限の権限の原則に従うようにしてください。ユーザーが CAC ログイン情報を使用してシステムに初めてログインすると、アカウントにこのデフォルトのアクセスロールが割り当てられます。

デフォルトのアクセスロールを割り当てるときに最小権限の原則に従わない場合、以降のログインでユーザーに意図しない権限レベルが割り当てられる可能性があります。これにより、必要なアクセスロールを超える権限がユーザーに付与される場合があります。

デフォルトのアクセスロールでログインしているユーザーが一時的に権限を昇格する必要がある場合、管理者権限を持つユーザーは、より高い権限を持つロールを割り当てることで、必要な高いレベルのアクセスを一時的にそのユーザーに提供できます。この権限は、非アクティブな状態が 24 時間続くと取り消され、ユーザーはデフォルトのアクセスロールに戻ります。

ユーザーがより高い権限レベル（システム管理者など）に永続的なアクセスロールを再割り当てする必要がある場合は、**グループ制御アクセスロール方式**を使用して、管理者アクセス権をユーザーに付与します。この方法では、指定されたアクセスロールが 24 時間を超えて保持され、ユーザーはグループ割り当てに従って正しい権限レベルを持つことが保証されます。グループ制御アクセスロールの設定の詳細については、ステップ 15の項を参照してください。

始める前に

CAC 設定プロセスの一部としてユーザ証明書を有効にするには、ブラウザに有効なユーザ証明書（この場合は CAC を介してユーザのブラウザに渡される証明書）が存在している必要があります。CAC 認証および認可の設定後に、ネットワーク上のユーザはブラウズ セッション期間にわたって CAC 接続を維持する必要があります。セッション中に CAC を削除または交換すると、Web ブラウザでセッションが終了し、システムにより Web インターフェイスから強制的にログアウトされます。

手順

ステップ 1 組織の指示に従い CAC を挿入します。

ステップ 2 ブラウザで **https://***ipaddress_or_hostname/* に移動します。ここで、*ipaddress* または *hostname* は使用しているデバイスに対応します。

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

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

ステップ 5 ログインページで、[ユーザ名（Username）] フィールドと [パスワード（Password）] フィールドに、管理者権限を持つユーザとしてログインします。CAC クレデンシャルを使用してログインすることは、まだ**できません**。

ステップ 6 **[システム（System）] > [ユーザ（Users）] > [外部認証（External Authentication）]** を選択します。

ステップ 7 「Management Center 用の LDAP 外部認証オブジェクトの追加 （151 ページ）」の手順に従い、CAC 専用の LDAP 認証オブジェクトを作成します。次の設定を行う必要があります。

- [CAC] チェックボックス。
- **[LDAP固有のパラメータ（LDAP-Specific Parameters）] > [詳細オプションを表示（Show Advanced Options）] > [ユーザー名テンプレート（User Name Template）]**。
- **[属性マッピング（Attribute Mapping）] > [UIアクセス属性（UI Access Attribute）]**。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 Management Center でのユーザーの外部認証の有効化 （166 ページ）の説明に従って、外部認証と CAC 認証を有効にします。

ステップ 10 **システム（⚙） > [構成（Configuration）]** を選択し、[HTTPS証明書（HTTPS Certificate）] をクリックします。

ステップ 11 HTTPS サーバ証明書をインポートし、必要に応じてHTTPS サーバー証明書のインポート （77 ページ）で説明する手順に従います。

使用する予定の CAC で、HTTPS サーバー証明書とユーザー証明書が同じ認証局（CA）により発行される必要があります。

ステップ 12 [HTTPS クライアント証明書設定（HTTPS Client Certificate Settings）] の [クライアント証明書を有効にする（Enable Client Certificates）] を選択します。詳細については、有効な HTTPS クライアント証明書の強制 （78 ページ）を参照してください。

ステップ 13 CAC クレデンシャルを使用した Secure Firewall Management Center へのログイン （40 ページ）に従い、デバイスにログインします。

SAML シングルサインオンの設定

シングルサインオンを使用するように Management Center を設定できます。これは、中央アイデンティティプロバイダー（IdP）が、組織内の他のアプリケーションだけでなく、Management Center にログインするユーザーに認証と承認を提供するシステムです。このような SSO 構成に参加するように設定されたアプリケーションは、フェデレーテッド サービス プロバイダー アプリケーションと呼ばれます。SSO ユーザーは、一度ログインすると、同じフェデレーションのメンバーであるすべてのサービス プロバイダー アプリケーションにアクセスできるようになります。

SAML シングルサインオンについて

SSO 用に設定された Management Center では、ログインページにシングルサインオンのためのリンクが表示されます。SSO アクセス用に設定されたユーザーは、このリンクをクリックすると、Management Center のログインページでユーザー名とパスワードを入力せずに、認証と承認のために IdP にリダイレクトされます。IdP による認証に成功すると、SSO ユーザーは Management Center Web インターフェイスに再度リダイレクトされて、ログインします。これを実現するための Management Center と IdP 間のすべての通信は、ブラウザを仲介として使用

して行われます。そのため、Management Center はアイデンティティ プロバイダーに直接アクセスするためにネットワーク接続を必要としません。

Management Center は、認証および承認のために、セキュリティ アサーション マークアップ言語（SAML）2.0 オープンスタンダードに準拠する任意の SSO プロバイダーを使用した SSO をサポートしています。

（注） Management Center は SAML 認証要求メッセージに署名できません。そのため、IdP が認証要求でサービスプロバイダーの署名を必要とする場合、Management Center での SSO は失敗します。

Management Center Web インターフェイスには、次の SSO プロバイダー用の設定オプションが用意されています。

- Okta
- OneLogin
- Azure
- お客様のクラウドソリューションの PingID の PingOne
- その他

（注） Cisco Secure Sign On SSO 製品は、Management Center を事前統合サービスプロバイダーとして認識しません。

Management Center の SSO ガイドライン

Management Center を SSO フェデレーションのメンバーとして設定するときは、次の点に注意してください。

- Management Center は、一度に 1 つの SSO プロバイダーのみで SSO をサポートできます。たとえば、SSO に Okta と OneLogin の両方を使用するように Management Center を設定することはできません。
- 高可用性設定の Management Center では SSO をサポートできますが、次の考慮事項に留意する必要があります。
  - SSO設定は、高可用性ペアのメンバー間で同期されません。ペアの各メンバーで個別に SSO を設定する必要があります。
  - 高可用性ペアの両方の Management Center は、SSO に同じ IdP を使用する必要があります。SSO 用に設定された各 Management Center の IdP で、サービス プロバイダー アプリケーションを設定する必要があります。

- 両方が SSO をサポートするように設定されている Management Center の高可用性ペアでは、ユーザーは SSO を使用してセカンダリ Management Center に初めてアクセスする前に、最初に SSO を使用してプライマリ Management Center に少なくとも 1 回ログインする必要があります。
- 高可用性ペアで Management Center の SSO を設定する場合：
  - プライマリ Management Center で SSO を設定する場合、セカンダリ Management Center で SSO を設定する必要はありません。
  - セカンダリ Management Center で SSO を設定する場合は、プライマリ Management Center でも SSO を設定する必要があります。（これは、SSO ユーザーがセカンダリ Management Center にログインする前に、プライマリ Management Center に少なくとも 1 回ログインする必要があるためです）。

- マルチテナントを使用する Management Center では、SSO 設定はグローバルドメインレベルでのみ適用でき、グローバルドメインとすべてのサブドメインに適用されます。
- 内部で認証された、または LDAP または RADIUS によって認証された管理ロールを持つユーザーのみが SSO を構成できます。
- Management Center は、IdP から開始された SSO をサポートしていません。
- Management Center は、SSO アカウントの CAC クレデンシャルを使用したログインをサポートしていません。
- CC モードを使用して展開中に SSO を設定できません。
- SSO アクティビティは、[サブシステム（Subsystem）] フィールドで指定されたログインまたはログアウトを使用して Management Center の監査ログに記録されます。

関連トピック

ハイ アベイラビリティ （361 ページ）
ドメイン （251 ページ）
CAC クレデンシャルを使用した Secure Firewall Management Center へのログイン （40 ページ）
セキュリティ認定準拠 （393 ページ）
監査レコード （499 ページ）

SSO ユーザーアカウント

アイデンティティ プロバイダーは、ユーザーとグループの構成を直接サポートできます。また、多くの場合、Active Directory、RADIUS、LDAP などの他のユーザー管理アプリケーションからユーザーとグループをインポートできます。このドキュメントでは、IdP と連携して SSO をサポートするように Management Center を設定することに焦点を当てています。ただし、IdP ユーザーおよびグループがすでに確立されていることを前提としています。他のユーザー管理アプリケーションのユーザーとグループをサポートするように IdP を設定するには、IdP ベンダーのドキュメントを参照してください。

ユーザー名とパスワードを含む、SSO ユーザーのほとんどのアカウント特性は、IdP で確立されます。SSO アカウントは、それらのアカウントが初めてログインするまで、Management Center Web インターフェイスの [ユーザー（Users）] ページに表示されません。

（注） システムでは、SSOアカウントのユーザー名と、SAML ログインプロセス中にIdPがManagement Center に送信する NameID 属性の両方が有効な電子メールアドレスである必要があります。多くの IdP は、ログインしようとしているユーザーのユーザー名を NameID 属性として自動的に使用しますが、これが IdP に適しているかを確認する必要があります。IdP でサービス プロバイダー アプリケーションを設定し、Management Center への SSO アクセス権限を持つ IdP ユーザーアカウントを作成する場合は、このことに注意してください。

SSO ユーザーの次のアカウント特性は、**システム**（⚙）> **[ユーザー（Users）]** > **[ユーザーの編集（Edit User）]** の下の Management Center Web インターフェイスから設定できます。

- 実際の名前
- ブラウザ セッション タイムアウトから除外する（Exempt from Browser Session Timeout）

SSO ユーザーのユーザーロールマッピング

デフォルトでは、Management Center への SSO アクセスが許可されているすべてのユーザーに、セキュリティアナリスト（読み取り専用）ロールが割り当てられます。このデフォルトを変更することも、特定の SSO ユーザーまたはグループに対してユーザーロールマッピングで上書きすることもできます。Management Center SSO 構成を確立してテストに成功したら、ユーザーロールマッピングを構成して、ログイン時に SSO ユーザーに割り当てられる Management Center ユーザーロールを確立できます。

ユーザーロールマッピングでは、Management Center の構成設定を SSO IdP アプリケーションの設定と調整する必要があります。ユーザーロールは、IdPアプリケーションで定義されたユーザーまたはグループに割り当てることができます。ユーザーはグループのメンバーである場合とそうでない場合があります。また、ユーザーまたはグループの定義は、Active Directory などの組織内の他のユーザー管理システムから IdP にインポートされる場合とインポートされない場合があります。このため、Management Center SSO ユーザーロールマッピングを効果的に構成するには、SSO フェデレーションがどのように編成されているか、および SSO IdP アプリケーションでユーザー、グループ、およびそれらのロールがどのように割り当てられているかを理解する必要があります。このドキュメントでは、IdP と連携してユーザーロールマッピングをサポートするように Management Center を構成することに焦点を当てています。IdP 内にユーザーまたはグループを作成したり、ユーザー管理アプリケーションから IdP にユーザーまたはグループをインポートしたりするには、IdPベンダーのドキュメントを参照してください。

ユーザーロールマッピングでは、IdP は Management Center サービス プロバイダー アプリケーションのロール属性を維持し、その Management Center にアクセスできる各ユーザーまたはグループは、ロール属性の文字列または式で構成されます（属性値の要件は IdP ごとに異なります）。Management Center では、そのロール属性の名前は SSO 構成の一部です。Management Center SSO 構成には、Management Center ユーザーロールのリストに割り当てられた式のリストも含まれています。ユーザーが SSO を使用して Management Center にログインすると、

Management Center はそのユーザー（または構成によってはそのユーザーのグループ）のロール属性の値を各 Management Center ユーザーロールの式と比較します。Management Center は、ユーザーが指定した属性値に式が一致するすべてのロールをユーザーに割り当てます。

（注） 個人ユーザー権限またはグループ権限に基づいて Management Center ロールがマッピングされるように構成できますが、単一の Management Center アプリケーションでは、グループと個人ユーザーの両方のロールマッピングはサポートできません。

Management Centerでのシングルサインオンの有効化

始める前に

- SAML SSO 管理アプリケーションで、Management Center のサービス プロバイダー アプリケーションを設定し、ユーザーまたはグループをサービス プロバイダー アプリケーションに割り当てます。
  - Okta の Management Center サービス プロバイダー アプリケーションを設定するには、Okta の Management Center サービス プロバイダー アプリケーションの設定 （176 ページ）を参照してください。
  - OneLogin の Management Center サービス プロバイダー アプリケーションを設定するには、OneLogin の Management Center サービス プロバイダー アプリケーションの設定 （190 ページ）を参照してください。
  - Azure の Management Center サービス プロバイダー アプリケーションを設定するには、Azure の Management Center サービス プロバイダー アプリケーションの設定 （204 ページ）を参照してください。
  - PingID の PingOne for Customers クラウドソリューションの Management Center サービス プロバイダー アプリケーションを設定するには、PingID PingOne for Customers の Management Center サービス プロバイダー アプリケーションの設定 （219 ページ）を参照してください。
  - SAML 2.0 準拠の SSO プロバイダーの Management Center サービス プロバイダー アプリケーションを設定するには、SAML 2.0 準拠の SSO プロバイダー用の Management Center サービス プロバイダー アプリケーションの設定 （225 ページ）を参照してください。

手順

ステップ 1 システム（⚙） > **[ユーザー（Users）]** > **[シングルサインオン（Single Sign-On）]** を選択します。

ステップ 2 [シングルサインオン（SSO）設定（Single Sign-On (SSO) Configuration）] スライダをクリックして、SSO を有効にします。

ステップ 3 [SSOの設定（Configure SSO）] ボタンをクリックします。

ステップ 4 [Firewall Management Center SAMLプロバイダーの選択（Select Firewall Management Center SAML Provider）] ダイアログボックスで、選択した SSO IdP のオプションボタンをクリックし、[次へ（Next）] をクリックします。

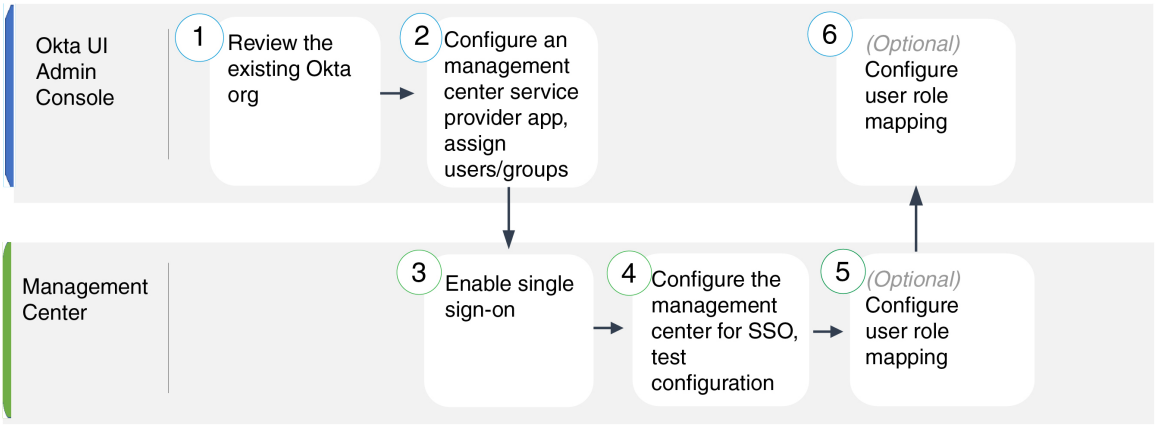
次のタスク

選択した SSO プロバイダーに適した手順に進みます。

- Okta SSO 用に Management Center を設定するには、Okta SSO 用の Management Center の設定 （178 ページ）を参照してください。
- PingID の PingOne for Customers クラウドソリューションを使用した SSO 用に Management Center を設定するには、PingID PingOne for Customers を使用した SSO 用の Management Center の設定 （221 ページ）を参照してください。
- Azure SSO 用に Management Center を設定するには、Azure SSO 用の Management Center の設定 （207 ページ）を参照してください。
- OneLogin SSO 用に Management Center を設定するには、OneLogin SSO 用の Management Center の設定 （192 ページ）を参照してください。
- SAML 2.0 準拠のプロバイダーを使用した SSO 用に Management Center を設定するには、SAML 2.0 準拠の SSO プロバイダーを使用した SSO 用の Management Center の設定 （227 ページ）を参照してください。

Okta を使用したシングルサインオンの設定

Okta を使用して SSO を設定するには、次のタスクを参照してください。



1	Okta UI 管理コンソール	Okta Org の確認 （175 ページ）
2	Okta UI 管理コンソール	Okta の Management Center サービス プロバイダー アプリケーションの設定 （176 ページ）
3	Management Center	Management Centerでのシングルサインオンの有効化 （173 ページ）
4	Management Center	Okta SSO 用の Management Center の設定 （178 ページ）
5	Management Center	Management Center での Okta のユーザーロールマッピングの設定 （179 ページ）
6	Okta UI 管理コンソール	Okta IdP におけるユーザーロールマッピングの設定 （180 ページ）

Okta Org の確認

Okta では、ユーザーが同じ SSO アカウントでアクセスできるすべてのフェデレーションデバイスとアプリケーションを含むエンティティは、*org* と呼ばれます。Management Center を Okta org に追加する前に、その設定についてよく理解してください。次の質問を考慮してください。

- Management Center にアクセスできるユーザーは何人ですか？
- ユーザーは、グループの Okta org のメンバーですか？
- ユーザーとグループの定義は Okta にネイティブですか。それとも Active Directory、RADIUS、LDAP などのユーザー管理アプリケーションからインポートされますか。
- Management Center で SSO をサポートするために、Okta org にユーザーまたはグループを追加する必要がありますか。
- どのようなユーザーロールの割り当てを行いますか。（ユーザーロールを割り当てない場合は、Management Center が構成可能なデフォルトのユーザーロールをすべての SSO ユーザーに自動的に割り当てます）。
- 必要なユーザーロールマッピングをサポートするには、Okta org 内のユーザーとグループをどのように編成する必要がありますか？

個人ユーザー権限またはグループ権限に基づいて Management Center ロールがマッピングされるように構成できますが、単一の Management Center アプリケーションでは、グループと個人ユーザーの両方のロールマッピングはサポートできないことに注意してください。

このドキュメントは、Okta クラシック UI 管理コンソールに精通していて、ネットワーク管理者権限を必要とする設定機能を実行できるアカウントを持っていることを前提としています。詳細が必要な場合は、オンラインで入手できる Okta のドキュメントを参照してください。

Okta の Management Center サービス プロバイダー アプリケーションの設定

Okta クラシック UI 管理コンソールでこれらの手順を使用して、Okta 内に Management Center サービス プロバイダー アプリケーションを作成し、そのアプリケーションにユーザーまたはグループを割り当てます。SAML SSO の概念と Okta 管理コンソールに精通している必要があります。このドキュメントでは、完全に機能する SSO 組織を確立するために必要なすべての Okta の機能について説明しているわけではありません。たとえば、ユーザーとグループを作成したり、別のユーザー管理アプリケーションからユーザーとグループの定義をインポートしたりするには、Okta のドキュメントを参照してください。

（注） Management Center アプリケーションにユーザーグループを割り当てることを計画している場合は、それらのグループ内のユーザーを個人として割り当てないでください。

（注） Management Center は、複数の SSO 属性を使用したロールマッピングをサポートできません。ユーザーロールマッピングまたはグループロールマッピングのいずれかを選択し、OneLogin から Management Center にユーザーロール情報を伝達する単一の属性を構成する必要があります。

始める前に

- SSO フェデレーションとそのユーザーおよびグループについて理解します。Okta Org の確認 （175 ページ）を参照してください。
- 必要に応じて、Okta org にユーザーアカウントやグループを作成します。

（注） システムでは、SSO アカウントのユーザー名と、SAML ログインプロセス中に IdP が Management Center に送信する NameID 属性の両方が有効な電子メールアドレスである必要があります。多くの IdP は、ログインしようとしているユーザーのユーザー名を NameID 属性として自動的に使用しますが、これが IdP に適しているかを確認する必要があります。IdP でサービス プロバイダー アプリケーションを設定し、Management Center への SSO アクセス権限を持つ IdP ユーザーアカウントを作成する場合は、このことに注意してください。

- ターゲット Management Center のログイン URL を確認します（`https://ipaddress_or_hostname`）。

（注） Management Center Web インターフェイスに複数の URL（たとえば、完全修飾ドメイン名と IP アドレス）でアクセスできる場合、SSO ユーザーは、一貫してこのタスクで構成するログイン URL を使用して Management Center にアクセスする必要があります。

手順

ステップ 1 Okta クラシック UI 管理コンソールから、Management Center のサービス プロバイダー アプリケーションを作成します。次の選択肢を使用して Management Center アプリケーションを設定します。

- [プラットフォーム（Platform）] に `Web` を選択します。
- [サインオン方式（Sign on method）] に `SAML 2.0` を選択します。
- [シングルサインオンURL（Single sign on URL）] を指定します。

  これは、ブラウザが IdP に代わって情報を送信する Management Center URL です。

  文字列 `saml/acs` を Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/acs`。
- [受信者URLおよび接続先URLにこれを使用する（Use this for Recipient URL and Destination URL）] を有効にします。
- [オーディエンスURI（SPエンティティID）（Audience URI (SP Entity ID)）] を入力します。

  これは、サービスプロバイダー（Management Center）のグローバルに一意の名前であり、多くの場合、URL としてフォーマットされます。

  文字列 `/saml/metadata` を Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/metadata`。
- [名前ID形式（Name ID Format）] に `Unspecified` を選択します。

ステップ 2 （グループをアプリケーションに割り当てる場合はオプション）個々の Okta ユーザーを Management Center アプリケーションに割り当てます。（Management Center アプリケーションにグループを割り当てることを計画している場合は、それらのグループのメンバーであるユーザーを個人として割り当てないでください。）

ステップ 3 （個人ユーザーをアプリケーションに割り当てる場合はオプション）Okta グループを Management Center アプリケーションに割り当てます。

ステップ 4 （オプション）Management Center での SSO セットアップを簡単にするために、Management Center サービス プロバイダー アプリケーションの SAML XML メタデータファイルを Okta からローカルコンピュータにダウンロードできます。

次のタスク

シングルサインオンを有効にします。Management Centerでのシングルサインオンの有効化 （173 ページ）を参照してください。

Okta SSO 用の Management Center の設定

Management Center Web インターフェイスでこれらの手順を使用します。

はじめる前に

- Okta クラシック UI 管理コンソールで Management Center サービス プロバイダー アプリケーションを作成します。Okta の Management Center サービス プロバイダー アプリケーションの設定 （176 ページ）を参照してください。
- シングルサインオンを有効にします。Management Centerでのシングルサインオンの有効化 （173 ページ）を参照してください

手順

ステップ 1 （このステップはManagement Centerでのシングルサインオンの有効化 （173 ページ）から直接続きます）。[Oktaメタデータの設定（Configure Okta Metadata）] ダイアログボックスには、2 つの選択肢があります。

- SSO 構成情報を手動で入力するには：
  1. [手動設定（Manual Configuration）] オプションボタンをクリックします。
  2. Okta SSO サービス プロバイダー アプリケーションから次の値を入力します（Okta クラシック UI 管理コンソールからこれらの値を取得します）。
     - **アイデンティティ プロバイダーのシングルサインオン（SSO）URL**
     - **アイデンティティ プロバイダー発行元**
     - **X.509 証明書**
- Okta によって生成された XML メタデータファイルをローカルコンピュータに保存した場合（Okta の Management Center サービス プロバイダー アプリケーションの設定 （176 ページ）のステップ 4）、ファイルを Management Center にアップロードできます。
  1. [XMLファイルのアップロード（Upload XML File）] オプションボタンをクリックします。
  2. 画面の指示に従って、ローカルコンピュータ上の XML メタデータファイルに移動して選択します。

ステップ 2 [次へ（Next）] をクリックします。

ステップ 3 [メタデータの検証（Verify Metadata）] ダイアログで、構成パラメータを確認し、[保存（Save）] をクリックします。

ステップ 4 [Test Configuration] をクリックします。システムにエラーメッセージが表示された場合は、Management Center の SSO 構成と Okta サービス プロバイダー アプリケーション構成を確認し、エラーを修正してから再試行します。

ステップ 5 システムが構成テストの成功を報告したら、[適用（Apply）] をクリックします。

次のタスク

オプションで、SSO ユーザーのユーザーロールマッピングを構成できます。Management Center での Okta のユーザーロールマッピングの設定 （179 ページ）を参照してください。ロールマッピングを構成しないことを選択した場合、デフォルトで、Management Center にログインするすべての SSO ユーザーに、Management Center での Okta のユーザーロールマッピングの設定 （179 ページ）のステップ 4 で構成したユーザーロールが割り当てられます。

Management Center での Okta のユーザーロールマッピングの設定

Management Center Web インターフェイスでユーザーロールマッピングを構成するフィールドは、SSO プロバイダーの選択に関係なく同じです。ただし、構成する値では、使用する SAML SSO プロバイダーのユーザーロールマッピングの導入方法を考慮する必要があります。

始める前に

- Okta ユーザーグループのマッピング情報を確認します。Okta Org の確認 （175 ページ）を参照してください。
- Management Center の SSO サービス プロバイダー アプリケーションを設定します。Okta の Management Center サービス プロバイダー アプリケーションの設定 （176 ページ）を参照してください。
- Management Center でシングルサインオンを有効にして設定します。Management Center でのシングルサインオンの有効化 （173 ページ）および Okta SSO 用の Management Center の設定 （178 ページ）を参照してください。

手順

ステップ 1 システム（⚙） > **[ユーザー（Users）]** を選択します。

ステップ 2 [シングルサインオン（SSO）（Single Sign-On (SSO)）] タブをクリックします。

ステップ 3 [詳細設定（ロールマッピング）（Advanced Configuration (Role Mapping)）] を展開します。

ステップ 4 [デフォルトのユーザーロール（Default User Role）] ドロップダウンから、ユーザーをデフォルト値として割り当てる Management Center ユーザーロールを選択します。

ステップ 5 [グループメンバーの属性（Group Member Attribute）] を入力します。この文字列は、ユーザーまたはグループのいずれかのユーザーロールマッピングのために Okta Management Center プロ

バイダーアプリケーションで設定された属性名と一致する必要があります。（Okta IdP におけるロールマッピングのためのユーザー属性の設定 （181 ページ）のステップ 1 またはOkta IdP におけるロールマッピングのためのグループ属性の設定 （182 ページ）のステップ 1 を参照）。

ステップ 6 SSO ユーザーに割り当てる各 Management Center ユーザーロールの横に、正規表現を入力します。（Management Center は、Golang と Perl でサポートされている、Google の RE2 正規表現標準規格の制限付きバージョンを使用します。）Management Center は、これらの値を、IdP が SSO ユーザー情報とともに Management Center に送信するユーザーロールマッピング属性値と比較します。Management Center は、一致が見つかったすべてのロールの和集合をユーザーに付与します。

次のタスク

- サービスプロバイダーアプリケーションでユーザーロールマッピングを構成します。Okta IdP におけるユーザーロールマッピングの設定 （180 ページ）を参照してください。

Okta IdP におけるユーザーロールマッピングの設定

個人ユーザーの権限またはグループの権限に基づいて、Okta クラシック UI 管理コンソールで SSO ユーザーロールマッピングを設定できます。

- 個人ユーザーの権限に基づいてマップするには、Okta IdP におけるロールマッピングのためのユーザー属性の設定 （181 ページ）を参照してください。
- グループの権限に基づいてマップするには、Okta IdP におけるロールマッピングのためのグループ属性の設定 （182 ページ）を参照してください。

SSO ユーザーが Management Center にログインすると、Okta は、Okta IdP で設定されたユーザーまたはグループロールの属性値を Management Center に提示します。Management Center は、その属性値を SSO 設定で各 Management Center ユーザーロールに割り当てられた正規表現と比較し、一致が見つかったすべてのロールをユーザーに付与します。（一致するものが見つからない場合、Management Center は設定可能なデフォルトのユーザーロールをユーザーに付与します）。各 Management Center ユーザーロールに割り当てる式は、Golang と Perl でサポートされている Google の RE2 正規表現標準規格の制限付きバージョンに準拠している必要があります。Management Center は、Okta から受け取った属性値を、Management Center ユーザーロール式との比較のために、同じ標準規格を使用する正規表現として扱います。

（注） Management Center 単一では、グループと個人ユーザーの両方のロールマッピングをサポートできません。Management Center サービス プロバイダー アプリケーションに対して 1 つのマッピング方法を選択し、それを一貫して使用する必要があります。さらに、Management Center は、Okta で設定された Management Center サービス プロバイダー アプリケーションごとに 1 つのグループ属性ステートメントのみを使用して、グループロールマッピングをサポートできます。一般に、グループベースのロールマッピングは、多数のユーザーがいる Management Center でより効率的です。Okta org 全体で確立されたユーザーとグループの定義を考慮する必要があります。

Okta IdP におけるロールマッピングのためのユーザー属性の設定

Okta クラシック UI 管理コンソールでこれらの手順を使用して、カスタムロールマッピング属性を Okta のデフォルト ユーザー プロファイルに追加します。

Okta サービス プロバイダー アプリケーションは、次の 2 種類のユーザープロファイルのいずれかを使用する場合があります。

- Okta ユーザープロファイル。カスタム属性で拡張できます。
- アプリのユーザープロファイル。サポートされている属性についてサードパーティのアプリケーションまたはディレクトリ（Active Directory、LDAP、Radius など）をクエリすることによって Okta が生成する事前定義されたリストの属性でのみ拡張できます。

Okta組織では、いずれかのタイプのユーザープロファイルを使用できます。それらの設定方法については、Oktaのドキュメントを参照してください。どのタイプのユーザープロファイルを使用しても、Management Center でユーザーロールマッピングをサポートするには、プロファイルでカスタム属性を設定して、各ユーザーのロールマッピング式を Management Center に伝える必要があります。

このドキュメントでは、Oktaユーザープロファイルを使用したロールマッピングについて説明します。アプリプロファイルを使用してマッピングするには、組織でカスタム属性を設定するために使用しているサードパーティのユーザー管理アプリケーションに精通している必要があります。詳細については、Okta のドキュメントを参照してください。

始める前に

- Okta の Management Center サービス プロバイダー アプリケーションの設定 （176 ページ）の説明に従って、Okta IdP で Management Center サービス プロバイダー アプリケーションを構成します。
- Management Center での Okta のユーザーロールマッピングの設定 （179 ページ）の説明に従って、Management Center で SSO ユーザーロールマッピングを設定します。

手順

ステップ 1 デフォルトの Okta ユーザープロファイルに新しい属性を追加します。

- [データ型（Data type）] では、`string` を選択します。
- ユーザーロールマッピングで照合する式が含まれる、Okta IdP が Management Center に送信する変数名を指定します。この変数名は、Management Center SSO 構成の [グループメンバー属性（Group Member Attribute）] で入力した文字列と一致する必要があります（Management Center での Okta のユーザーロールマッピングの設定 （179 ページ）のステップ 5 を参照してください）。

ステップ 2 このプロファイルを使用して Management Center サービス プロバイダー アプリケーションに割り当てられた各ユーザーについて、先ほど作成したユーザーロール属性に値を割り当てます。

Management Center からユーザーに割り当てるロールを表すために式を使用します。Management Center では、この文字列を、Management Center での Okta のユーザーロールマッピングの設定（179 ページ）の手順 6 で各 Management Center ユーザーロールに割り当てた式と比較します（Management Center ユーザーロール式との比較のために、Management Center では Okta から受け取った属性値を、Golang と Perl でサポートされている Google の RE2 正規表現標準の制限バージョンに準拠した式として扱います）。

Okta IdP におけるロールマッピングのためのグループ属性の設定

Okta クラシック UI 管理コンソールでこれらの手順を使用して、カスタム ロール マッピング グループ属性を Management Center サービス プロバイダー アプリケーションに追加します。Management Center は、Okta Management Center サービス プロバイダー アプリケーションごとに 1 つのグループ属性ステートメントのみを使用して、グループロールマッピングをサポートできます。

Okta サービス プロバイダー アプリケーションは、次の 2 種類のグループのいずれかを使用する場合があります。

- Okta グループ。カスタム属性で拡張できます。
- アプリケーショングループ。サポートされている属性についてサードパーティのアプリケーションまたはディレクトリ（Active Directory、LDAP、Radius など）をクエリすることによって Okta が生成する事前定義されたリストの属性でのみ拡張できます。

Okta 組織では、いずれかのタイプのグループを使用できます。それらの設定方法については、Okta のドキュメントを参照してください。どのタイプのグループを使用しても、Management Center でユーザーロールマッピングをサポートするには、グループのカスタム属性を設定して、ロールマッピング式を Management Center に伝える必要があります。

このドキュメントでは、Okta グループを使用したロールマッピングについて説明します。アプリケーショングループを使用してマッピングするには、組織でカスタム属性を設定するために使用しているサードパーティのユーザー管理アプリケーションに精通している必要があります。詳細については、Okta のドキュメントを参照してください。

始める前に

- Okta IdP の Management Center サービス プロバイダー アプリケーションを設定します。Okta の Management Center サービス プロバイダー アプリケーションの設定 （176 ページ）を参照してください。
- Management Center でのユーザーロールマッピングの設定Management Center での Okta のユーザーロールマッピングの設定 （179 ページ）

手順

Management Center サービス プロバイダー アプリケーションの新しい SAML グループ属性を作成します。

- [名前（Name）] には、Management Center SSO 設定で [グループメンバーの属性（Group Member Attribute）] に入力したものと同じ文字列を使用します。（Management Center での Okta のユーザーロールマッピングの設定 （179 ページ）のステップ 5 を参照してください）。
- [フィルタ（Filter）] には、Management Center からグループのメンバーに割り当てるロールを表す式を指定します。Okta は、この値をユーザーがメンバーであるグループの名前と比較し、一致するグループ名を Management Center に送信します。次に、Management Center では、これらのグループ名を、Management Center での Okta のユーザーロールマッピングの設定 （179 ページ）の手順 6 で各 Management Center ユーザーロールに割り当てた正規表現と比較します。

Okta ユーザーロールマッピングの例

次の例が示すように、ユーザーロールマッピングをサポートする Management Center での SSO 構成は、個々のユーザーとグループの両方で同じです。違いは、Okta の Management Center サービス プロバイダー アプリケーションの設定にあります。

（注） 個人ユーザー権限またはグループ権限に基づいて Management Center ロールがマッピングされるように構成できますが、単一の Management Center アプリケーションでは、グループと個人ユーザーの両方のロールマッピングはサポートできません。さらに、Management Center は、Okta で設定された Management Center サービス プロバイダー アプリケーションごとに 1 つのグループ属性ステートメントのみを使用して、グループロールマッピングをサポートできます。

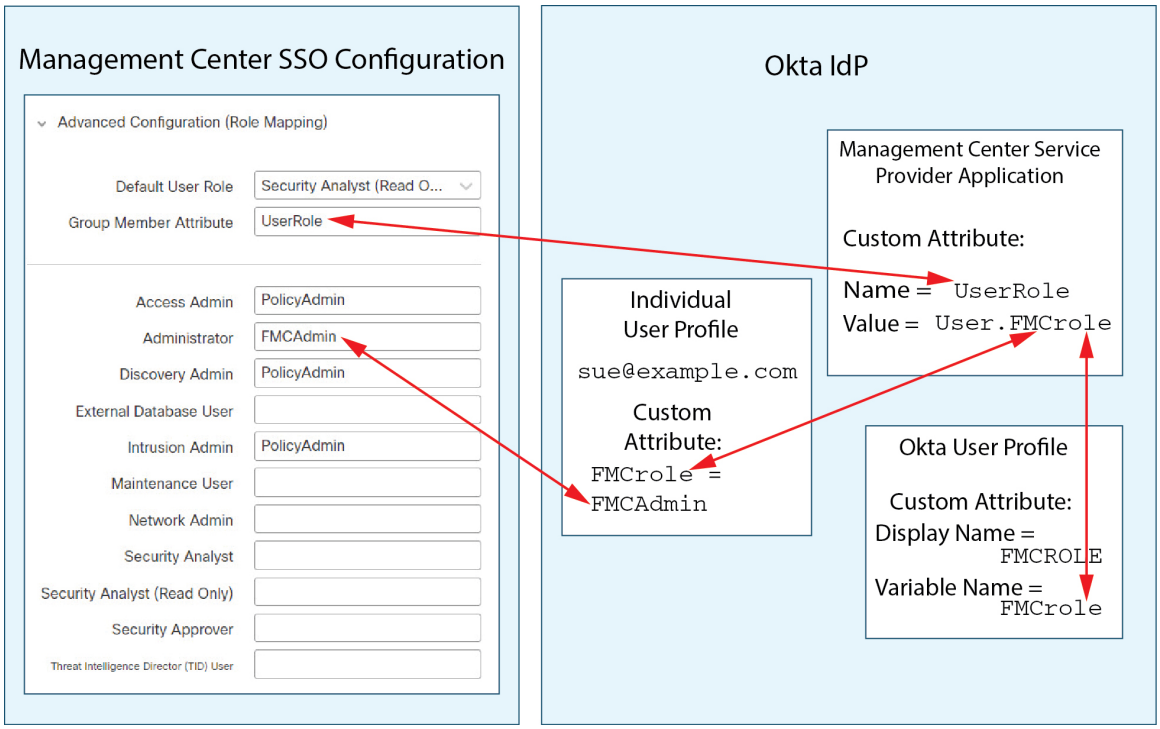
個人ユーザーアカウントの Okta ロールのマッピング例

個人ユーザーのロールマッピングでは、Okta Management Center サービスアプリケーションに、名前が Management Center でのグループメンバー属性の名前と一致するカスタム属性があります。（この例では、`UserRole`）。Okta のユーザープロファイルには、カスタム属性もあります（この例では、`FMCrole` という名前の変数）。アプリケーションのカスタム属性 `UserRole` の定義は、Okta がユーザーロールマッピング情報を Management Center に渡すときに、対象のユーザーに割り当てられたカスタム属性値を使用することを確立します。

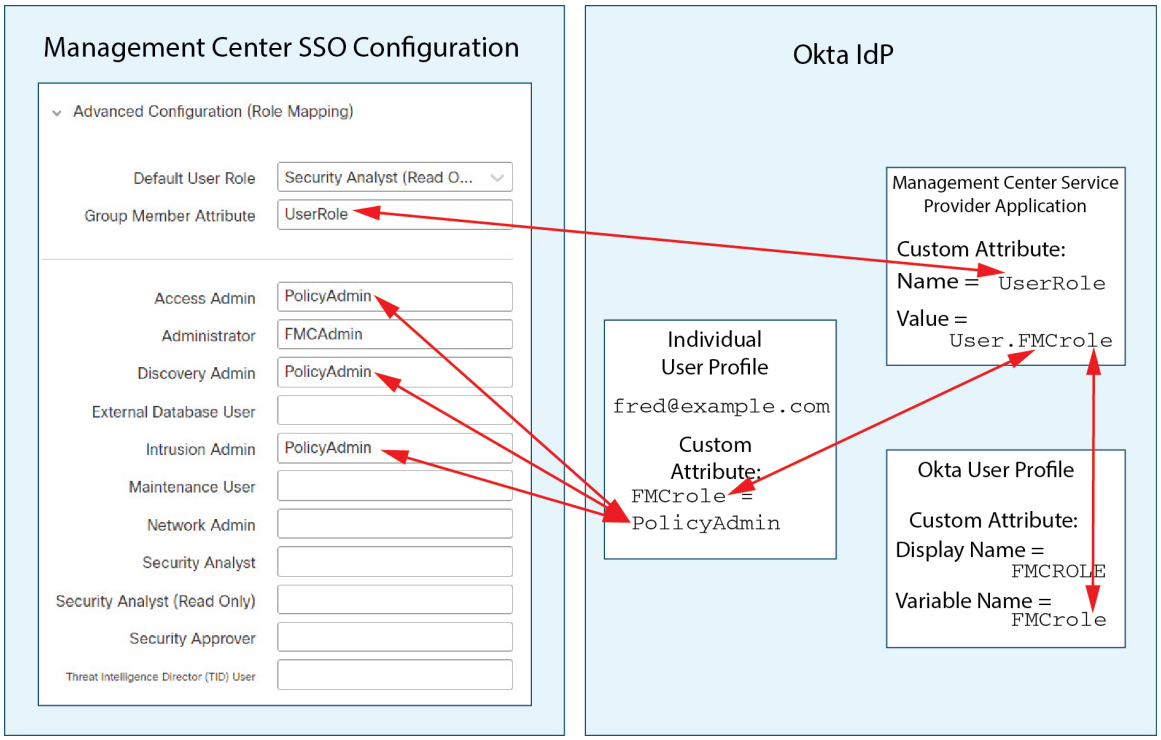
次の図は、Management Center および Okta 構成の関連するフィールドと値が、個人アカウントのユーザーロールマッピングで互いにどのように対応しているかを示しています。各図では、Management Center と Okta UI 管理コンソールで同じ SSO 設定を使用していますが、Management

Center で各ユーザーに異なるロールを割り当てるために、Okta UI 管理コンソールでの各ユーザーの設定は異なります。

- この図では、sue@example.com では `FMCrole` 値 `FMCAdmin` が使用されていて、Management Center が彼女に管理者ロールを割り当てます。



- この図では、fred@example.com では `FMCrole` 値 `PolicyAdmin` が使用されていて、Management Center が彼にアクセス管理者、検出管理者、侵入管理者のロールを割り当てます。



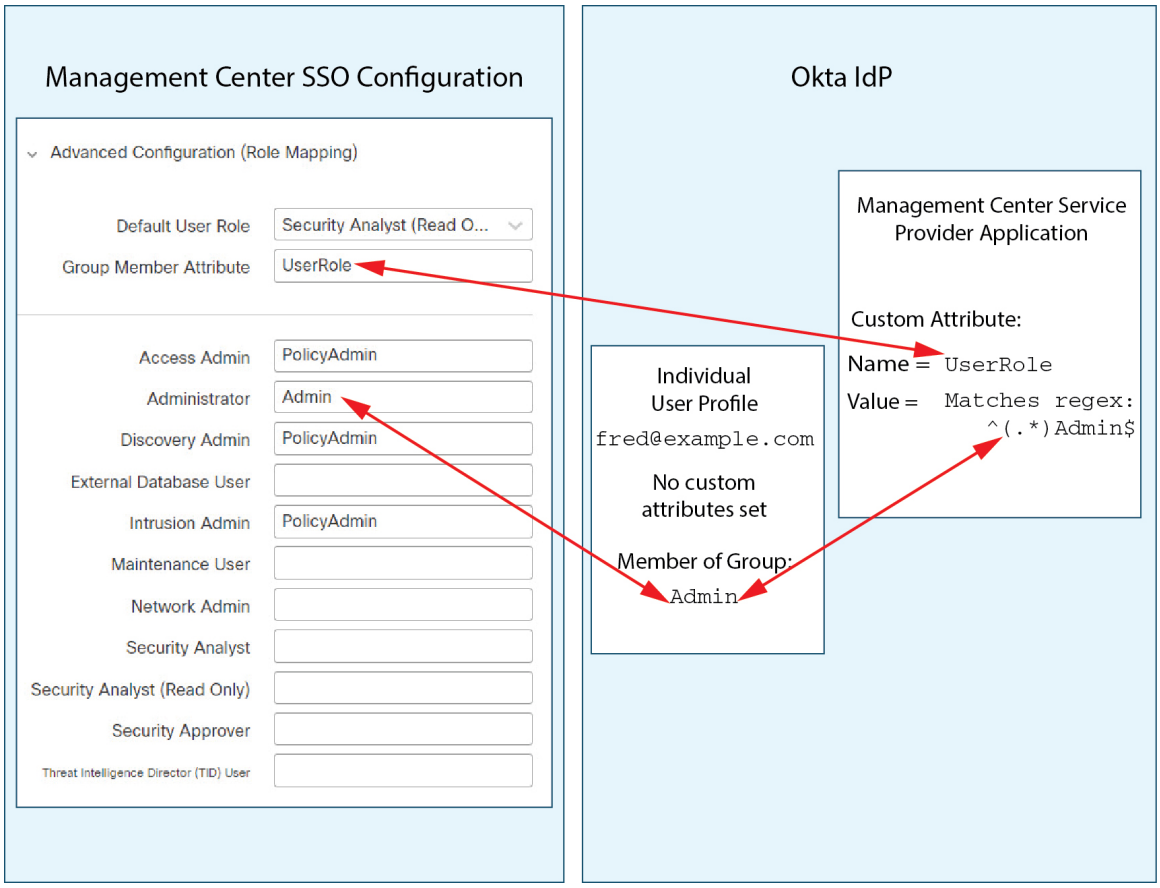
- この Management Center のために Okta サービスアプリケーションに割り当てられた他のユーザーには、次のいずれかの理由で、デフォルトのユーザーロールであるセキュリティアナリスト（読み取り専用）が割り当てられます。
  - Okta ユーザープロファイルの `FMCrole` 変数に値が割り当てられていません。
  - Okta ユーザープロファイルの `FMCrole` 変数に割り当てられた値が、Management Center の SSO 設定でユーザーロールに設定された式と一致しません。

グループの Okta ロールマッピングの例

グループのロールマッピングでは、Okta Management Center サービスアプリケーションに、名前が Management Center でのグループメンバー属性の名前と一致するカスタムグループ属性があります（この例では、`UserRole`）。Okta は Management Center の SSO ログインのリクエストを処理するときに、ユーザーのグループメンバーシップを Management Center サービス アプリケーション グループ属性に割り当てられた式と比較します（この例では、`^(.*)Admin$`）。Okta は、グループ属性に一致するユーザーのグループメンバーシップを Management Center に送信します。Management Center は、受信したグループ名を各ユーザーロールに設定された正規表現と比較し、それに応じてユーザーロールを割り当てます。

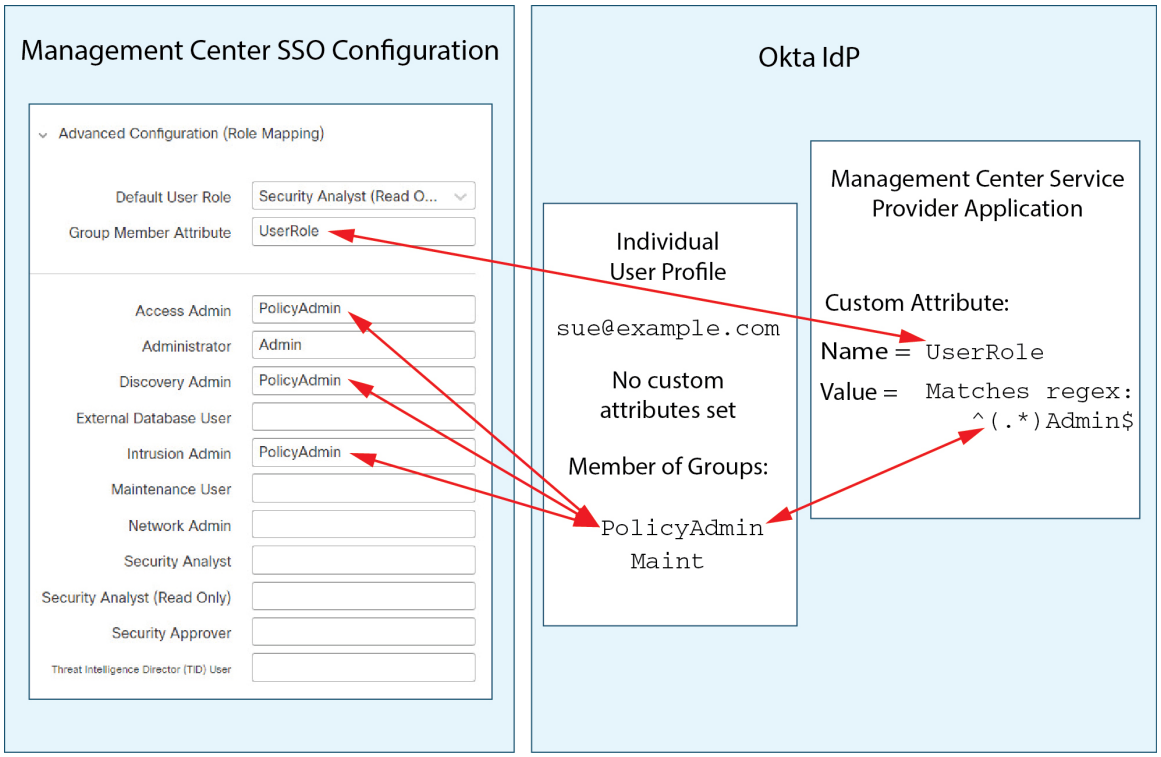
次の図は、Management Center および Okta 構成の関連するフィールドと値が、グループのユーザーロールマッピングで互いにどのように対応しているかを示しています。各図では、Management Center と Okta UI 管理コンソールで同じ SSO 設定を使用していますが、Management Center で各ユーザーに異なるロールを割り当てるために、Okta UI 管理コンソールでの各ユーザーの設定は異なります。

- この図では、fred@example.com は Okta IdP グループの `Admin` のメンバーであり、式 `^(.*)Admin$` に一致します。Okta は Management Center に Fred の `Admin` グループメンバーシップを送信し、Management Center は彼に管理者ロールを割り当てます。

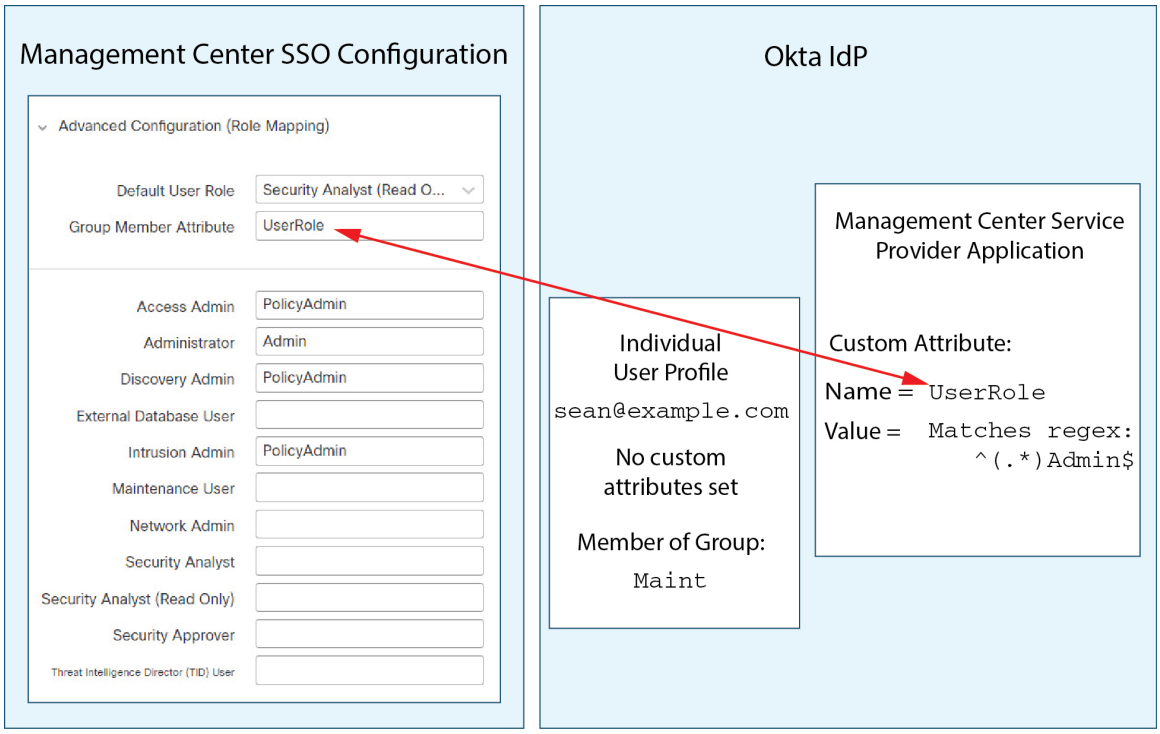


- この図では、sue@example.com は Okta IdP グループの `PolicyAdmin` のメンバーであり、式 `^(.*)Admin$` に一致します。Okta は Management Center に Sue の `PolicyAdmin` グループメンバーシップを送信し、Management Center は彼女にアクセス管理者、検出管理者、侵入管理者のロールを割り当てます。

  Sue は Okta グループの `Maint` のメンバーでもありますが、このグループ名は Okta Management Center サービスアプリケーションのグループメンバーシップ属性に割り当てられた式と一致しないため、Okta は Sue の `Maint` グループメンバーシップに関する情報を Management Center に送信しません。そのため、`Maint` グループでの彼女のメンバーシップは、Management Center が彼女に割り当てるロールには関与しません。



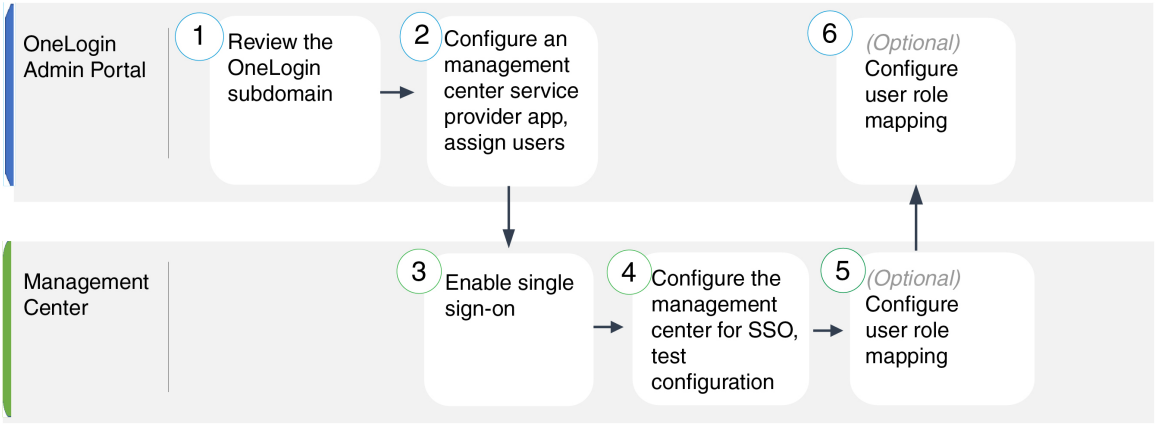
- この図では、sean@example.com は Okta IdP グループの `Maint` のメンバーです。このグループ名は式 `^(.*)Admin$` と一致しないため、sean@example.com が Management Center にログインしたときに、Okta は Sean の `Maint` グループメンバーシップに関する情報を Management Center に送信しません。そのため、Sean にはメンテナンスユーザーロールではなく、デフォルトのユーザーロール（セキュリティアナリスト（読み取り専用））が割り当てられます。



これらの図は、ロールマッピング戦略を確立する際の事前計画の重要性を示しています。この例では、`Maint` グループのみのメンバーである、この Management Center へのアクセス権を持つ Okta ユーザーには、デフォルトのユーザーロールのみを割り当てることができます。Management Center は、Okta サービスアプリケーション設定で、1 つのカスタムグループ属性のみの使用をサポートしています。その属性に割り当てる式と、その式と照合するために確立するグループ名は、慎重に作成する必要があります。Management Center SSO 設定のユーザーロール割り当て文字列で正規表現を使用することで、ロールマッピングをより柔軟に行うことができます。（各 Management Center ユーザーロールに割り当てる式は、Golang と Perl でサポートされている、Google の RE2 正規表現標準規格の制限付きバージョンに準拠している必要があります）。

OneLogin を使用したシングルサインオンの設定

OneLogin を使用して SSO を設定するには、次のタスクを参照してください。



1	Management Center	OneLogin サブドメインの確認 （189 ページ）
2	Management Center	OneLogin の Management Center サービス プロバイダー アプリケーションの設定 （190 ページ）
3	OneLogin 管理ポータル	Management Centerでのシングルサインオンの有効化 （173 ページ）
4	OneLogin 管理ポータル	OneLogin SSO 用の Management Center の設定 （192 ページ）
5	OneLogin 管理ポータル	Management Center における OneLogin のユーザーロールマッピングの設定 （193 ページ）
6	Management Center	OneLogin IdP におけるユーザーロールマッピングの設定 （194 ページ）

OneLogin サブドメインの確認

OneLogin では、ユーザーが同じ SSO アカウントでアクセスできるすべてのフェデレーションデバイスとアプリケーションを含むエンティティは、サブドメインと呼ばれます。Management Center を OneLogin サブドメインに追加する前に、その設定についてよく理解してください。次の質問を考慮してください。

- Management Center にアクセスできるユーザーは何人ですか？
- ユーザーは、グループの OneLogin サブドメインのメンバーですか？
- Active Directory、Google Apps、LDAP などのサードパーティディレクトリのユーザーとグループは、OneLogin サブドメインと同期されていますか？
- Management Center で SSO をサポートするために、OneLogin サブドメインにユーザーまたはグループを追加する必要がありますか？

- どのような Management Center のユーザーロールの割り当てを行いますか？（ユーザーロールを割り当てない場合は、Management Center が構成可能なデフォルトのユーザーロールをすべての SSO ユーザーに自動的に割り当てます）。
- 必要なユーザーロールマッピングをサポートするには、OneLogin サブドメイン内のユーザーとグループをどのように編成する必要がありますか？

個人ユーザーまたはグループに基づいて Management Center のロールがマッピングされるように構成できますが、単一の Management Center のアプリケーションでは、グループと個人ユーザーの両方のロールマッピングはサポートできないことに注意してください。

このドキュメントは、ユーザーが OneLogin 管理ポータルに精通していて、スーパーユーザー権限を持つアカウントを持っていることを前提としています。ユーザーロールマッピングを構成するには、カスタムユーザーフィールドをサポートする OneLogin Unlimited プランへのサブスクリプションも必要です。詳細が必要な場合は、オンラインで入手できる OneLogin のドキュメントを参照してください。

OneLogin の Management Center サービス プロバイダー アプリケーションの設定

OneLogin 管理ポータルでこれらの手順を使用して、OneLogin 内に Management Center サービスプロバイダーアプリケーションを作成し、そのアプリケーションにユーザーまたはグループを割り当てます。SAML SSO の概念と OneLogin 管理ポータルに精通している必要があります。このドキュメントでは、完全に機能する SSO 組織を確立するために必要なすべての OneLogin の機能について説明しているわけではありません。たとえば、ユーザーとグループを作成したり、別のユーザー管理アプリケーションからユーザーとグループの定義をインポートしたりするには、OneLogin のドキュメントを参照してください。

（注） Management Center アプリケーションにユーザーグループを割り当てることを計画している場合は、それらのグループ内のユーザーを個人として割り当てないでください。

（注） Management Center は、複数の SSO 属性を使用したロールマッピングをサポートできません。ユーザーロールマッピングまたはグループロールマッピングのいずれかを選択し、OneLogin から Management Center にユーザーロール情報を伝達する単一の属性を構成する必要があります。

始める前に

- OneLogin サブドメインとそのユーザーおよびグループについて理解します。OneLogin サブドメインの確認 （189 ページ）を参照してください。
- 必要に応じて、OneLogin サブドメイン内にユーザーアカウントを作成します。

（注） システムでは、SSO アカウントのユーザー名と、SAML ログイン プロセス中に IdP が Management Center に送信する NameID 属性の両方が有効な電子メールアドレスである必要があります。多くの IdP は、ログインしようとしているユーザーのユーザー名を NameID 属性として自動的に使用しますが、これが IdP に適しているかを確認する必要があります。IdP でサービス プロバイダー アプリケーションを設定し、Management Center への SSO アクセス権限を持つ IdP ユーザーアカウントを作成する場合は、このことに注意してください。

- ターゲット Management Center のログイン URL を確認します（`https://ipaddress_or_hostname/`）。

（注） Management Center Web インターフェイスに複数の URL （たとえば、完全修飾ドメイン名と IP アドレス）でアクセスできる場合、SSO ユーザーは、一貫してこのタスクで設定するログイン URL を使用して Management Center にアクセスする必要があります。

手順

ステップ 1 [SAMLテストコネクタ（詳細）（SAML Test Connector (Advanced)）] をベースとして使用して、Management Center サービス プロバイダー アプリケーションを作成します。

ステップ 2 次の設定を使用してアプリケーションを設定します。

- [対象者（エンティティID）（Audience (Entity ID)）] については、文字列 `/saml/metadata` を Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/metadata`。
- [受信者（Recipient）] については、文字列 `/saml/acs` を Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/acs`。
- [ACS（コンシューマ）URL検証（ACS (Consumer) URL Validator）] については、OneLogin が正しい Management Center URL を使用していることを確認するために使用する式を入力します。ACS URL を使用して次のように変更することで、単純なバリデータを作成できます。
  - ACS URL の先頭に ^ を追加します。
  - ACS URL の末尾に $ を追加します。
  - ACS URL 内のすべての / と ? の前に \ を挿入します。

たとえば、ACS URL が `https://ExampleFMC/saml/acs` の場合、適切な URL バリデータは `^https:\/\/ExampleFMC\/saml\/acs$` になります。

- [ACS（コンシューマ）URL（ACS (Consumer) URL）] については、文字列 `/saml/acs` を Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/acs`。
- [ログインURL（Login URL）] については、文字列 `/saml/acs` を Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/acs`。
- [SAMLイニシエータ（SAML Initiator）] には、`Service Provider` を選択します。

ステップ 3 OneLogin ユーザーを Management Center サービス プロバイダー アプリケーションに割り当てます。

ステップ 4 （オプション）Management Center での SSO セットアップを簡単にするために、Management Center サービス プロバイダー アプリケーションの SAML XML メタデータを OneLogin からローカルコンピュータにダウンロードできます。

次のタスク

シングルサインオンを有効にします。Management Center でのシングルサインオンの有効化 （173 ページ）を参照してください。

OneLogin SSO 用の Management Center の設定

Management Center Web インターフェイスでこれらの手順を使用します。

始める前に

- OneLogin 管理ポータルで Management Center サービス プロバイダー アプリケーションを作成します。OneLogin の Management Center サービス プロバイダー アプリケーションの設定 （190 ページ）を参照してください。
- シングルサインオンを有効にします。Management Center でのシングルサインオンの有効化 （173 ページ）を参照してください。

手順

ステップ 1 （このステップはManagement Center でのシングルサインオンの有効化 （173 ページ）から直接続きます）。[OneLoginメタデータの設定（Configure OneLogin Metadata）] ダイアログには、2 つの選択肢があります。

- SSO 構成情報を手動で入力するには：
  1. [手動設定（Manual Configuration）] オプションボタンをクリックします。
  2. OneLogin サービス プロバイダー アプリケーションから次の SSO 構成値を入力します。

- [アイデンティティプロバイダーのシングルサインオンURL（Identity Provider Single Sign-On URL）]：OneLogin からの **SAML 2.0 エンドポイント（HTTP）**を入力します。
- [アイデンティティプロバイダー発行元（Identity Provider Issuer）]：OneLogin からの**発行元 URL** を入力します。
- [X.509証明書（X.509 Certificate）]：OneLogin からの **X.509 証明書**を入力します。

- OneLogin によって生成された XML メタデータファイルをローカルコンピュータに保存した場合（OneLogin の Management Center サービス プロバイダー アプリケーションの設定（190 ページ）のステップ 4）、ファイルを Management Center にアップロードできます。
  1. [XMLファイルのアップロード（Upload XML File）]オプションボタンをクリックします。
  2. 画面の指示に従って、ローカルコンピュータ上の XML メタデータファイルに移動して選択します。

ステップ 2 [次へ（Next）] をクリックします。

ステップ 3 [メタデータの検証（Verify Metadata）]ダイアログで、構成パラメータを確認し、[保存（Save）] をクリックします。

ステップ 4 [Test Configuration] をクリックします。システムにエラーメッセージが表示された場合は、Management Center の SSO 構成と OneLogin サービス プロバイダー アプリケーション構成を確認し、エラーを修正してから再試行します。

ステップ 5 システムが構成テストの成功を報告したら、[適用（Apply）] をクリックします。

次のタスク

オプションで、SSO ユーザーのユーザーロールマッピングを構成できます。Management Center における OneLogin のユーザーロールマッピングの設定 （193 ページ）を参照してください。ロールマッピングを構成しないことを選択した場合、デフォルトで、Management Center にログインするすべての SSO ユーザーに、Management Center における OneLogin のユーザーロールマッピングの設定 （193 ページ）のステップ 4 で構成したユーザーロールが割り当てられます。

Management Center における OneLogin のユーザーロールマッピングの設定

Management Center Web インターフェイスでユーザーロールマッピングを構成するフィールドは、SSO プロバイダーの選択に関係なく同じです。ただし、構成する値では、使用する SAML SSO プロバイダーのユーザーロールマッピングの導入方法を考慮する必要があります。

始める前に

- OneLogin のユーザーとグループを確認します。OneLogin サブドメインの確認 （189 ページ）を参照してください。
- Management Center の SSO サービス プロバイダー アプリケーションを設定します。OneLogin の Management Center サービス プロバイダー アプリケーションの設定 （190 ページ）を参照してください。
- Management Center でシングルサインオンを有効にして設定します。Management Centerでのシングルサインオンの有効化 （173 ページ）およびOneLogin の Management Center サービス プロバイダー アプリケーションの設定 （190 ページ）を参照してください。

手順

ステップ 1 システム（⚙） > **[ユーザー（Users）]** > **[シングルサインオン（Single Sign-On）][システム（System）]** > **[ユーザー（Users）]** を選択します。

ステップ 2 [詳細設定（ロールマッピング）（Advanced Configuration (Role Mapping)）] を展開します。

ステップ 3 [デフォルトのユーザーロール（Default User Role）] ドロップダウンから、ユーザーをデフォルト値として割り当てる Management Center ユーザーロールを選択します。

ステップ 4 [グループメンバーの属性（Group Member Attribute）] を入力します。この文字列は、OneLogin の Management Center サービス プロバイダー アプリケーションでロールマッピング用に定義するカスタムパラメータのフィールド名と一致する必要があります。（OneLogin IdP における個人ユーザーのユーザーロールマッピングの設定 （195 ページ）のステップ 1 またはOneLogin IdP におけるグループのユーザーロールマッピングの設定 （196 ページ）のステップ 1 を参照）。

ステップ 5 SSO ユーザーに割り当てる各 Management Center ユーザーロールの横に、正規表現を入力します。Management Center は、これらの値を、IdP が SSO ユーザー情報とともに Management Center に送信するユーザーロールマッピング属性と比較します。Management Center は、一致が見つかったすべてのロールの和集合をユーザーに付与します。

次のタスク

サービス プロバイダー アプリケーションでユーザーロールマッピングを構成します。OneLogin IdP におけるユーザーロールマッピングの設定 （194 ページ）を参照してください。

OneLogin IdP におけるユーザーロールマッピングの設定

個々の権限またはグループの権限に基づいて、Onelogin 管理ポータルで SSO ユーザーロールマッピングを設定できます。

- 個人ユーザーの権限に基づいてマップするには、OneLogin IdP における個人ユーザーのユーザーロールマッピングの設定 （195 ページ）を参照してください。
- グループの権限に基づいてマップするには、OneLogin IdP におけるグループのユーザーロールマッピングの設定 （196 ページ）を参照してください。

SSO ユーザーが Management Center にログインすると、OneLogin は、OneLogin IdP で設定されたカスタムユーザーフィールドから値を取得するユーザーまたはグループロールの属性値を Management Center に提示します。Management Center はその属性値を SSO 設定で各 Management Center ユーザーロールに割り当てられた正規表現と比較し、一致が見つかったすべてのロールをユーザーに付与します。（一致するものが見つからない場合、Management Center は設定可能なデフォルトのユーザーロールをユーザーに付与します）。各 Management Center ユーザーロールに割り当てる式は、Golang と Perl でサポートされている Google の RE2 正規表現標準規格の制限付きバージョンに準拠している必要があります。Management Center は、OneLogin から受け取った属性値を、Management Center ユーザーロール式との比較のために、同じ標準規格を使用する正規表現として扱います。

（注） Management Center 単一では、グループと個人ユーザーの両方のロールマッピングをサポートできません。Management Center サービス プロバイダー アプリケーションに対して 1 つのマッピング方法を選択し、それを一貫して使用する必要があります。Management Center は、OneLogin で設定された 1 つのカスタムユーザーフィールドのみを使用してロールマッピングをサポートできます。一般に、グループベースのロールマッピングは、多数のユーザーがいる Management Center でより効率的です。OneLogin サブドメイン全体で確立されたユーザーとグループの定義を考慮する必要があります。

OneLogin IdP における個人ユーザーのユーザーロールマッピングの設定

OneLogin 管理ポータルを使用して、Management Center サービス プロバイダー アプリケーションのカスタムパラメータとカスタムユーザーフィールドを作成します。これらは、SSO ログインプロセス中に OneLogin がユーザーロール情報を Management Center に渡す手段を提供します。

始める前に

- OneLogin サブドメインとそのユーザーとグループを確認します。OneLogin サブドメインの確認 （189 ページ）を参照してください。
- OneLogin で Management Center サービス プロバイダー アプリケーションを作成して設定します。OneLogin の Management Center サービス プロバイダー アプリケーションの設定（190 ページ）を参照してください。
- Management Center における OneLogin のユーザーロールマッピングの設定 （193 ページ）の説明に従って、SSO ユーザーロールマッピングを設定します。

手順

ステップ 1 Management Center サービス プロバイダー アプリケーションのカスタムパラメータを作成します。

- [フィールド名（Field Name）] には、Management Center SSO 設定で [グループメンバーの属性（Group Member Attribute）] に使用したものと同じ名前を使用します（Management Center における OneLogin のユーザーロールマッピングの設定 （193 ページ）のステップ 4 を参照）。
- [値（Value）] には、`FMCUserRole` などのニーモニック名を指定します。これは、この手順のステップ 2 で構成する顧客ユーザーフィールドの名前と一致する必要があります。

ステップ 2 カスタムユーザーフィールドを作成して、Management Center のアクセス権を持つ各 OneLogin ユーザーのユーザーロール情報を含めます。

- フィールド [名前（Name）] には、`FMCUserRole` などのニーモニック名を指定します。これは、この手順のステップ 1 で説明されているアプリケーション カスタム パラメータに指定された値と一致する必要があります。
- [短縮名（Short name）] には、フィールドの省略された代替名を指定します（これは OneLogin プログラマチック インターフェイスに使用されます）。

ステップ 3 Management Center サービス プロバイダー アプリケーションへのアクセス権を持つ各ユーザーについて、この手順のステップ 2 で作成したカスタムユーザーフィールドに値を割り当てます。

ユーザーが SSO を使用して Management Center にログインする場合、そのユーザーに対してこのフィールドに割り当てる値は、Management Center が SSO 構成で Management Center ユーザーロールに割り当てた式と比較する値になります（Management Center における OneLogin のユーザーロールマッピングの設定 （193 ページ）のステップ 5 を参照してください）。

次のタスク

- さまざまなアカウントから SSO を使用して Management Center にログインし、期待どおりにユーザーに Management Center ユーザーロールが割り当てられることを確認することで、ロールマッピングスキームをテストします。

OneLogin IdP におけるグループのユーザーロールマッピングの設定

OneLogin 管理ポータルを使用して、Management Center サービス プロバイダー アプリケーションのカスタムパラメータとカスタムユーザーフィールドを作成します。OneLogin ユーザーをグループに割り当てます。次に、カスタムユーザーフィールドとユーザーグループの間に 1 つ以上のマッピングを作成し、OneLogin がユーザーのグループメンバーシップに基づいてカスタムユーザーフィールドに値を割り当てるようにします。これらは、SSO ログインプロセス中に OneLogin がグループベースのユーザーロール情報を Management Center に渡す手段を提供します。

OneLogin サービス プロバイダー アプリケーションは、次の 2 種類のグループのいずれかを使用する場合があります。

- OneLogin にネイティブなグループ。

- Active Directory、Google Apps、LDAP などのサードパーティ アプリケーションから同期されたグループ。

Management Center グループロールマッピングには、いずれかのタイプのグループを使用できます。このドキュメントでは、OneLogin グループを使用したロールマッピングについて説明します。サードパーティのアプリケーショングループを使用するには、組織で使用しているサードパーティのユーザー管理アプリケーションに精通している必要があります。詳細については、OneLogin のドキュメントを参照してください。

始める前に

- OneLogin サブドメインとそのユーザーとグループを確認します。OneLogin サブドメインの確認 （189 ページ）を参照してください。
- OneLogin で Management Center サービス プロバイダー アプリケーションを作成して設定します。OneLogin の Management Center サービス プロバイダー アプリケーションの設定（190 ページ）を参照してください。
- Management Center における OneLogin のユーザーロールマッピングの設定 （193 ページ）の説明に従って、SSO ユーザーロールマッピングを設定します。

手順

ステップ 1 Management Center サービス プロバイダー アプリケーションのカスタムパラメータを作成します。

- [フィールド名（Field Name）] には、Management Center SSO 設定で [グループメンバーの属性（Group Member Attribute）] に使用したものと同じ名前を使用します（Management Center における OneLogin のユーザーロールマッピングの設定 （193 ページ）のステップ 4 を参照）。
- [値（Value）] には、`FMCUserRole` などのニーモニック名を指定します。これは、この手順のステップ 2 で構成する顧客ユーザーフィールドの名前と一致する必要があります。

ステップ 2 カスタムユーザーフィールドを作成して、Management Center のアクセス権を持つ各 OneLogin ユーザーのユーザーロール情報を含めます。

- フィールド[名前（Name）]には、`FMCUserRole` などのニーモニック名を指定します。これは、この手順のステップ 1 で説明されているアプリケーション カスタム パラメータに指定された値と一致する必要があります。
- [短縮名（Short name）] には、フィールドの省略された代替名を指定します（これは OneLogin プログラマチック インターフェイスに使用されます）。

ステップ 3 1 つ以上のユーザー フィールドマッピングを作成して、この手順のステップ 2 で作成したカスタムユーザーフィールドにグループベースの値を割り当てます。各 OneLogin ユーザーグルー

プに正しい Management Center ユーザーロールを割り当てるために必要な数のマッピングを作成します。

- ユーザーの [グループ（Group）] フィールドをグループ名と比較して、マッピングの**条件**を 1 つ以上作成します。
- 複数の**条件**を作成する場合は、マッピングを行うために、ユーザーのグループが条件の一部または**すべて**に一致する必要があるかどうかを選択します。
- マッピングの**アクション**を作成して、この手順のステップ 2 で作成したカスタムユーザーフィールドに値を割り当てます。フィールド [名前（Name）] と、指定した**条件**に一致するすべてのユーザーに対して OneLogin がこのカスタムユーザーフィールドに割り当てる文字列を指定します。

  Management Center では、この文字列を、Management Center における OneLogin のユーザーロールマッピングの設定 （193 ページ）の手順 5 で各 Management Center ユーザーロールに割り当てた式と比較します。
- 変更が完了したら、**すべてのマッピングを再適用**します。

次のタスク

- さまざまなアカウントから SSO を使用して Management Center にログインし、期待どおりにユーザーに Management Center ユーザーロールが割り当てられることを確認することで、ロールマッピングスキームをテストします。

OneLogin ユーザーロールマッピングの例

次の例が示すように、ユーザーロールマッピングをサポートする Management Center での SSO 構成は、個々のユーザーとグループの両方で同じです。違いは、OneLogin の Management Center サービス プロバイダー アプリケーションの設定にあります。

（注） Management Center 単一では、グループと個人ユーザーの両方のロールマッピングをサポートできません。Management Center サービス プロバイダー アプリケーションに対して 1 つのマッピング方法を選択し、それを一貫して使用する必要があります。Management Center は、OneLogin で設定された 1 つのカスタムユーザーフィールドのみを使用してロールマッピングをサポートできます。一般に、グループベースのロールマッピングは、多数のユーザーがいる Management Center でより効率的です。OneLogin サブドメイン全体で確立されたユーザーとグループの定義を考慮する必要があります。

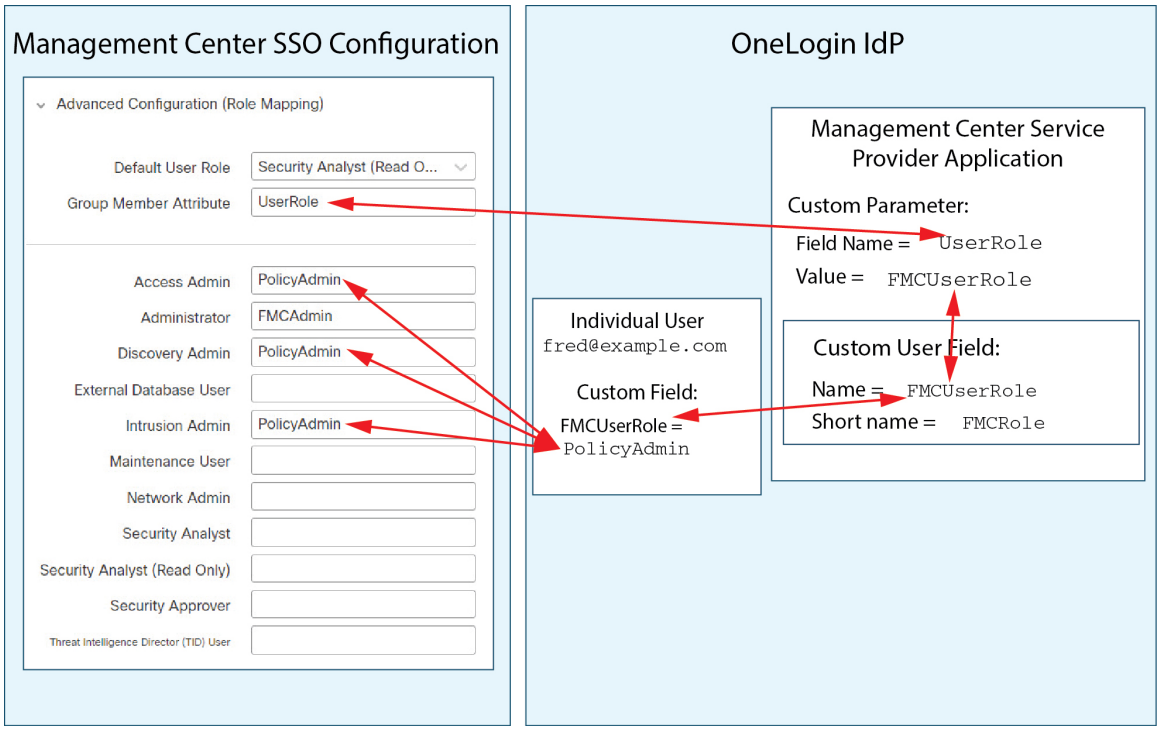
個人ユーザーアカウントの OneLogin ロールマッピングの例

個人ユーザーのロールマッピングでは、OneLogin Management Center サービスアプリケーションに、名前が Management Center でのグループメンバー属性の名前と一致するカスタムパラメー

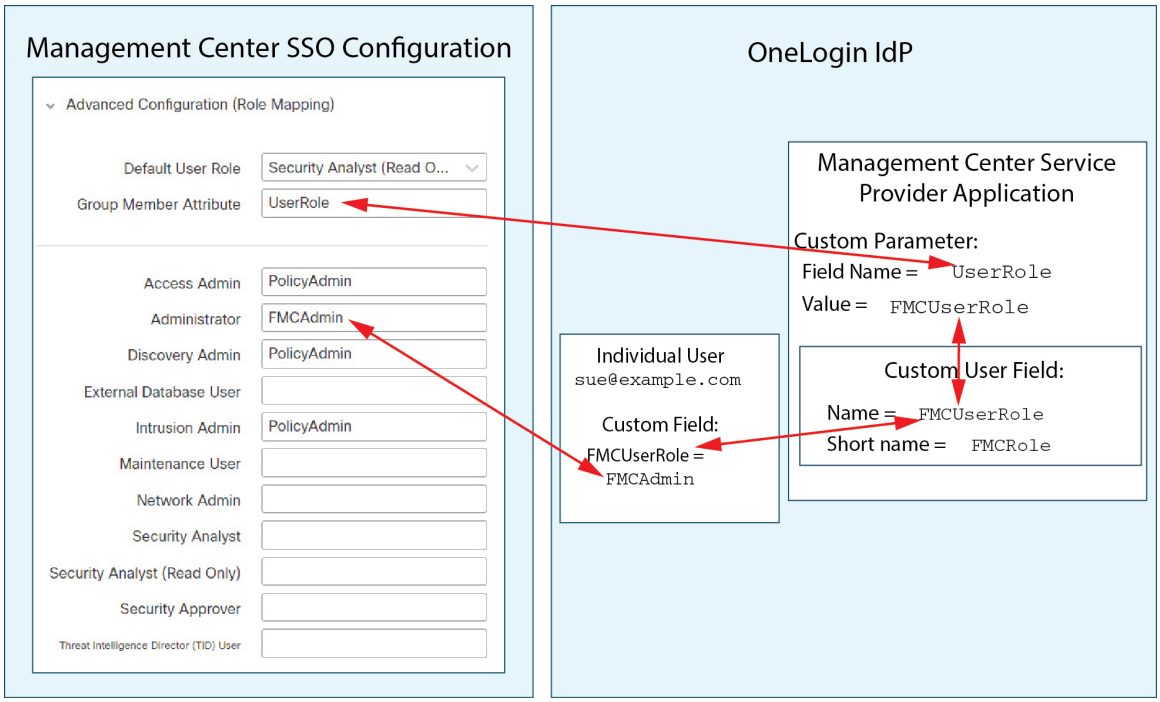
タがあります（この例では、`UserRole`）。OneLogin には、カスタムユーザーフィールドも定義されています（この例では `FMCUserRole`）。アプリケーションのカスタムパラメータ `UserRole` の定義により、OneLogin がユーザーロールマッピング情報を Management Center に渡すときに、問題のユーザーのカスタムユーザーフィールド `FMCUserRole` の値を使用することが確立されます。

次の図は、Management Center および OneLogin 構成の関連するフィールドと値が、個人アカウントのユーザーロールマッピングで互いにどのように対応しているかを示しています。各図は、Management Center と OneLogin Admin ポータルで同じ SSO 構成を使用していますが、OneLogin Admin ポータルでの各ユーザーの構成は、Management Center で各ユーザーに異なるロールを割り当てるために異なります。

- この図では、fred@example.com では `FMCUserRole` 値 `PolicyAdmin` が使用されていて、Management Center が彼にアクセス管理者、検出管理者、侵入管理者のロールを割り当てます。



- この図では、sue@example.com では `FMCUserRole` 値 `FMCAdmin` が使用されていて、Management Center が彼女に管理者ロールを割り当てます。



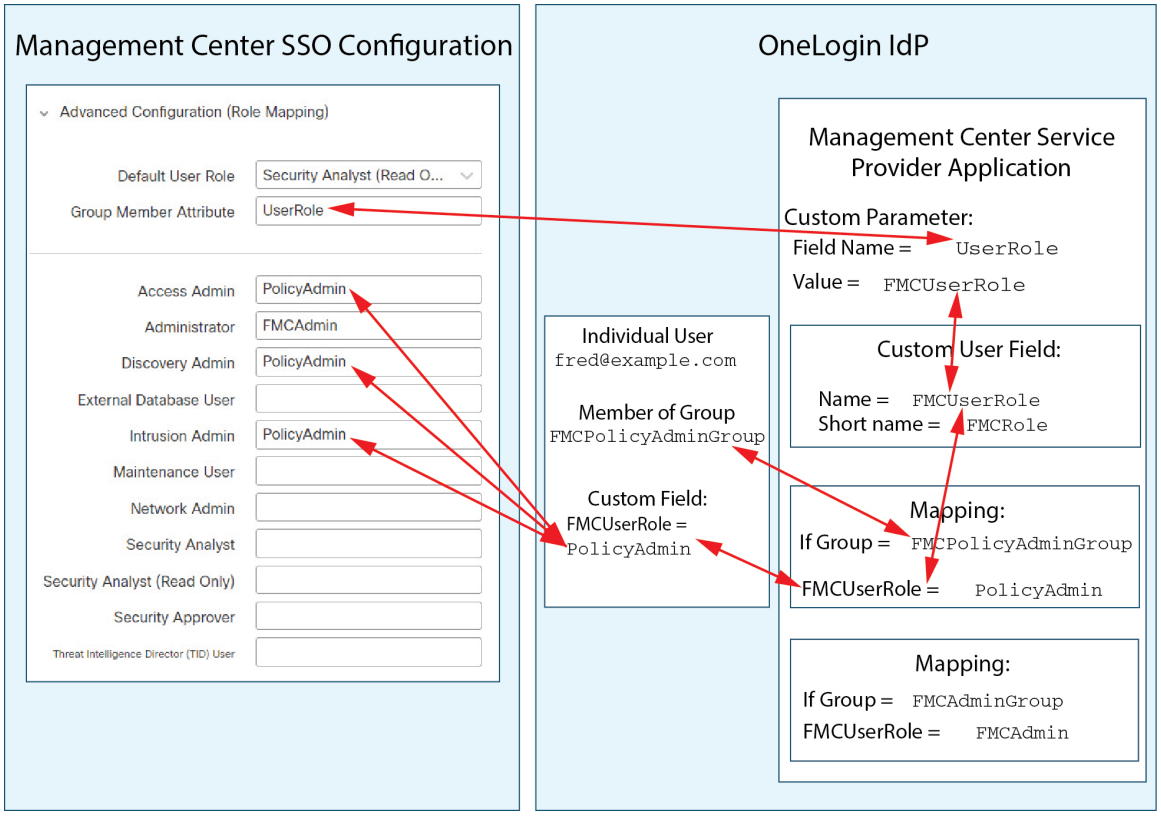
- この Management Center のために OneLogin サービスアプリケーションに割り当てられた他のユーザーには、次のいずれかの理由で、デフォルトのユーザーロールであるセキュリティアナリスト（読み取り専用）が割り当てられます。
  - `FMCUserRole` カスタムユーザーフィールドに値が割り当てられていません。
  - `FMCUserRole` カスタムユーザーフィールドに割り当てられた値が、Management Center の SSO 設定でユーザーロールに設定された式と一致しません。

グループの OneLogin ロールマッピングの例

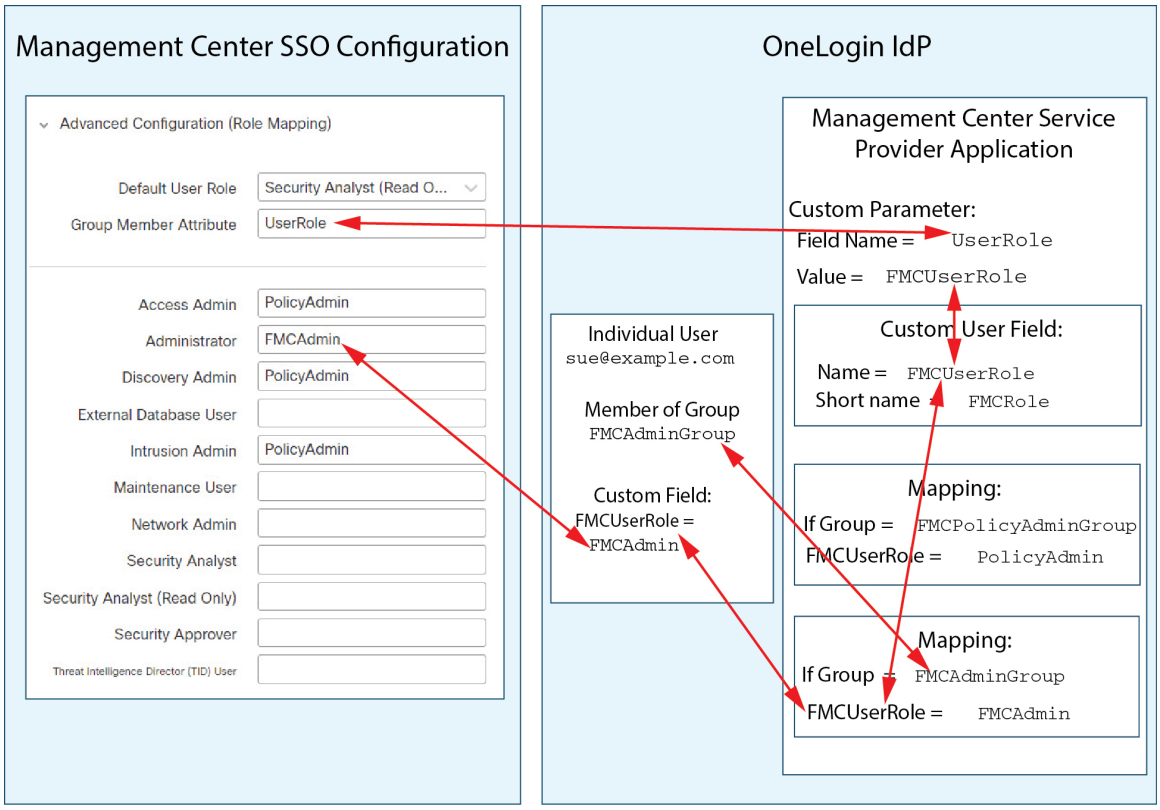
グループのロールマッピングでは、OneLogin Management Center サービスアプリケーションに、名前が Management Center でのグループメンバー属性の名前と一致するカスタムパラメータがあります（この例では、`UserRole`）。OneLogin には、カスタムユーザーフィールドも定義されています（この例では `FMCUserRole`）。アプリケーションのカスタムパラメータ `UserRole` の定義により、OneLogin がユーザーロールマッピング情報を Management Center に渡すときに、問題のユーザーのカスタムユーザーフィールド `FMCUserRole` の値を使用することが確立されます。ユーザーグループマッピングをサポートするには、OneLogin 内でマッピングを確立して、そのユーザーの OneLogin グループメンバーシップに基づいて各ユーザーの `FMCUserRole` フィールドに値を割り当てる必要があります。

次の図は、Management Center および OneLogin 構成の関連するフィールドと値が、グループのユーザーロールマッピングで互いにどのように対応しているかを示しています。各図は、Management Center と OneLogin Admin ポータルで同じ SSO 構成を使用していますが、OneLogin Admin ポータルでの各ユーザーの構成は、Management Center で各ユーザーに異なるロールを割り当てるために異なります。

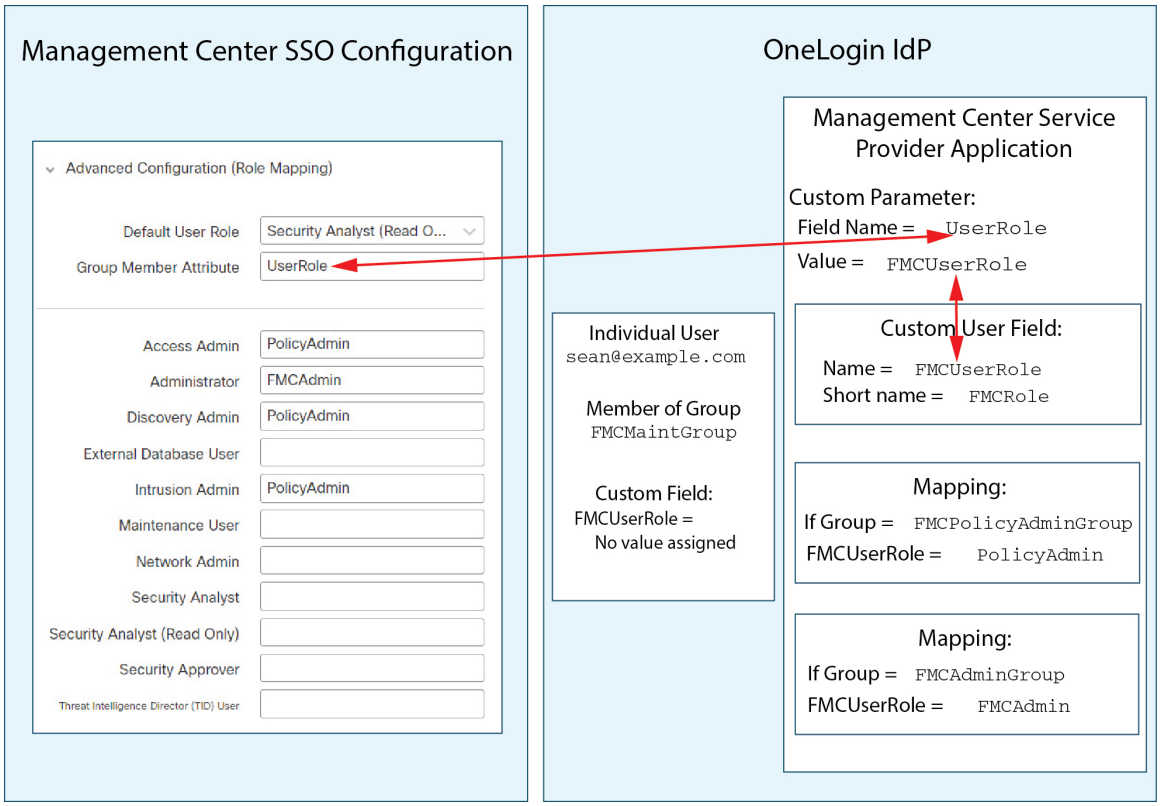
- この図では、fred@example.com は OneLogin IdP グループ `FMCPolicyAdminGroup` のメンバーです。OneLogin マッピングは、値 `PolicyAdmin` を `FMCPolicyAdminGroup` のメンバーのカスタムユーザーフィールド `FMCUserRole` に割り当てます。Management Center は Fred および `FMCPolicyAdminGroup` の他のメンバーにアクセス管理者、検出管理者、侵入管理者のロールを割り当てます。



- この図では、sue@example.com は OneLogin IdP グループの `FMCAdminGroup` のメンバーです。OneLogin マッピングは、値 FMCAdmin を `FMCAdminGroup` のメンバーのカスタムユーザーフィールド `FMCUserRole` に割り当てます。Management Center は、Sue と `FMCAdminGroup` の他のメンバーに管理者ロールを割り当てます。

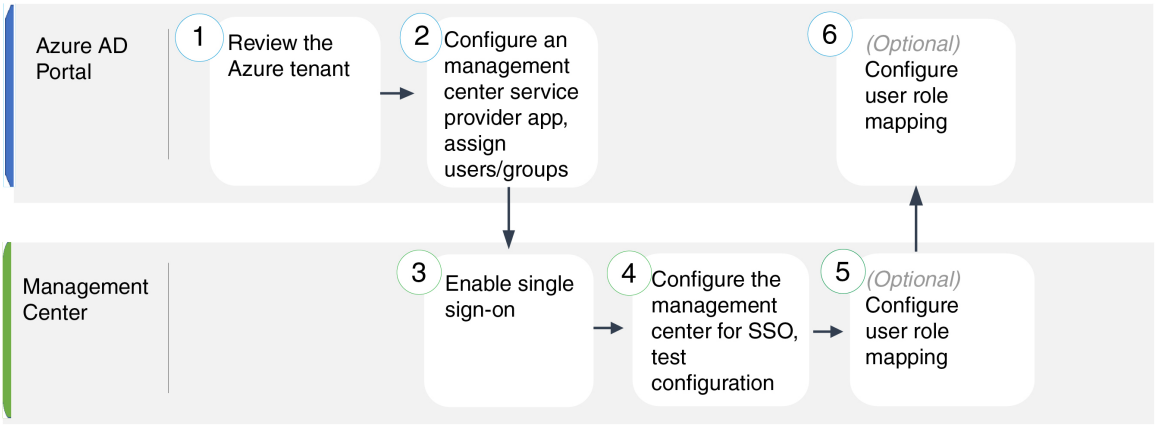


- この図では、sean@example.com は Idp グループ `FMCMaintGroup` のメンバーです。このグループには OneLogin マッピングが関連付けられていないため、OneLogin は Sean のカスタムユーザーフィールド `FMCUserRole` に値を割り当てません。Management Center は、メンテナンスユーザーロールではなく、デフォルトのユーザーロール（セキュリティアナリスト（読み取り専用））を Sean に割り当てます。



Azure AD を使用したシングルサインオンの設定

Azure を使用して SSO を構成するには、次のタスクを参照してください。



1	Azure AD ポータル	Azure テナントの確認 （204 ページ）
2	Azure AD ポータル	Azure の Management Center サービス プロバイダー アプリケーションの設定 （204 ページ）

3	Management Center	Management Centerでのシングルサインオンの有効化 （173 ページ）
4	Management Center	Azure SSO 用の Management Center の設定 （207 ページ）
5	Management Center	Management Center における Azure のユーザーロールマッピングの設定 （208 ページ）
6	Azure AD ポータル	Azure IdP におけるユーザーロールマッピングの設定 （209 ページ）

Azure テナントの確認

Azure AD は、Microsoft のマルチテナント クラウド ベースのアイデンティティおよびアクセス管理サービスです。Azure では、ユーザーが同じ SSO アカウントでアクセスできるすべてのフェデレーテッドデバイスが含まれているエンティティをテナントと呼びます。Management Center を Azure テナントに追加する前に、その組織についてよく理解してください。次の質問を考慮してください。

- Management Center にアクセスできるユーザーは何人ですか？
- ユーザーは、グループの Azure テナントのメンバーですか？
- 別のディレクトリ製品からのユーザーとグループですか？
- Management Center で SSO をサポートするために、Azure テナントにユーザーまたはグループを追加する必要がありますか？
- どのような Management Center のユーザーロールの割り当てを行いますか？（ユーザーロールを割り当てない場合は、Management Center が構成可能なデフォルトのユーザーロールをすべての SSO ユーザーに自動的に割り当てます）。
- 必要なユーザーロールマッピングをサポートするには、Azure テナント内のユーザーとグループをどのように編成する必要がありますか？
- 個人ユーザーまたはグループに基づいて Management Center のロールがマッピングされるように構成できますが、単一の Management Center のアプリケーションでは、グループと個人ユーザーの両方のロールマッピングはサポートできないことに注意してください。

このドキュメントは、ユーザーがすでに Azure Active Directory ポータルに精通していて、Azure AD テナントのアプリケーション管理者権限を持つアカウントを持っていることを前提としています。Management Center は、テナント固有のシングルサインオンおよびシングルサインアウトのエンドポイントでのみ Azure SSO をサポートしていることに注意してください。Azure AD Premium P1 以上のライセンスとグローバル管理者権限が必要です。詳細については、Azure のドキュメントを参照してください。

Azure の Management Center サービス プロバイダー アプリケーションの設定

Azure Active Directory ポータルを使用して、Azure Active Directory テナント内に Management Center サービス プロバイダー アプリケーションを作成し、基本的な構成設定を確立します。

（注） Management Center アプリケーションにユーザーグループを割り当てることを計画している場合は、それらのグループ内のユーザーを個人として割り当てないでください。

（注） Management Center は、複数の SSO 属性を使用したロールマッピングをサポートできません。ユーザーロールマッピングまたはグループロールマッピングのいずれかを選択し、OneLogin から Management Center にユーザーロール情報を伝達する単一の属性を構成する必要があります。

始める前に

- Azure テナントとそのユーザーおよびグループについて理解します。Azure テナントの確認 （204 ページ）を参照してください。
- 必要に応じて、Azure テナントにユーザーアカウントやグループを作成します。

（注） システムでは、SSO アカウントのユーザー名と、SAML ログインプロセス中に IdP が Management Center に送信する NameID 属性の両方が有効な電子メールアドレスである必要があります。多くの IdP は、ログインしようとしているユーザーのユーザー名を NameID 属性として自動的に使用しますが、これが IdP に適しているかを確認する必要があります。IdP でサービス プロバイダー アプリケーションを設定し、Management Center への SSO アクセス権限を持つ IdP ユーザーアカウントを作成する場合は、このことに注意してください。

- ターゲット Management Center のログイン URL を確認します（`https://ipaddress_or_hostname`）

（注） Management Center Web インターフェイスに複数の URL（たとえば、完全修飾ドメイン名と IP アドレス）でアクセスできる場合、SSO ユーザーは、一貫してこのタスクで構成するログイン URL を使用して Management Center にアクセスする必要があります。

手順

ステップ 1 Azure AD SAML Toolkit をベースとして使用して、Management Center サービス プロバイダー アプリケーションを作成します。

ステップ 2 [基本的なSAML設定（Basic SAML Configuration）] の次の設定を使用してアプリケーションを設定します。

- [識別子（エンティティID）（Identifier (Entity ID)）] については、文字列 `/saml/metadata` を Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/metadata`。
- [応答URL（Assertion Consumer Service URL）（Reply URL (Assertion Consumer Service URL)）] については、文字列 `/saml/acs` を Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/acs`。
- [サインオンURL（Sign on URL）] については、文字列 `/saml/acs` を Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/acs`。

ステップ 3 アプリケーションの**一意ユーザー識別子名（名前 ID）**請求を編集して、Management Center でのサインオンのユーザー名をユーザーアカウントに関連付けられた電子メールアドレスに強制します。

- [ソース（Source）] で `Attribute` を選択します。
- [ソース属性（Source attribute）]：`user.mail` を選択します。

ステップ 4 Management Center で SSO を保護するための証明書を生成します。証明書には次のオプションを使用します。

- [署名オプション（Signing Option）] で [SAML応答とアサーションに署名（Sign SAML Response and Assertion）] を選択します。
- [署名アルゴリズム（Signing Algorithm）] に [SHA-256] を選択します。

ステップ 5 Base-64 バージョンの証明書をローカルコンピュータにダウンロードします。Management Center Web インターフェイスで Azure SSO を構成するときに必要になります。

ステップ 6 アプリケーションの SAML ベースのサインオン情報で、次の値をメモします。

- **[ログイン URL（Login URL）]**
- [Azure AD識別子（Azure AD Identifier）]

Management Center Web インターフェイスで Azure SSO を構成するときに、これらの値が必要になります。

ステップ 7 （オプション）Management Center での SSO セットアップを簡単にするために、Management Center サービス プロバイダー アプリケーションの SAML XML メタデータファイル（Azure Portal では**フェデレーションメタデータ XML** と呼ばれます）をローカルコンピュータにダウンロードできます。

ステップ 8 既存の Azure ユーザーとグループを Management Center サービスアプリケーションに割り当てます。

（注） Management Center アプリケーションにユーザーグループを割り当てることを計画している場合は、それらのグループ内のユーザーを個人として割り当てないでください。

（注） ユーザーのロールマッピングを構成する場合、個人ユーザー権限またはグループ権限に基づいてロールがマッピングされるように構成できますが、単一の Management Center のアプリケーションでは、グループと個人ユーザーの両方のロールマッピングはサポートできないことに注意してください。

次のタスク

シングルサインオンを有効にします。Management Centerでのシングルサインオンの有効化（173 ページ）を参照してください。

Azure SSO 用の Management Center の設定

Management Center Web インターフェイスでこれらの手順を使用します。

始める前に

- Azure AD ポータルで Management Center サービス プロバイダー アプリケーションを作成します。Azure の Management Center サービス プロバイダー アプリケーションの設定（204 ページ）を参照してください。
- シングルサインオンを有効にします。Management Centerでのシングルサインオンの有効化（173 ページ）を参照してください。

手順

ステップ 1 （このステップはManagement Centerでのシングルサインオンの有効化（173 ページ）から直接続きます）。[Azureメタデータの設定（Configure Azure Metadata）] ダイアログには、2 つの選択肢があります。

- SSO 構成情報を手動で入力するには：
  1. [手動設定（Manual Configuration）] オプションボタンをクリックします。
  2. Azure SSO サービス プロバイダー アプリケーションから取得した値を入力します。
     - [アイデンティティプロバイダーのシングルサインオンURL（Identity Provider Single Sign-On URL）] には、Azure の Management Center サービス プロバイダー アプリケーションの設定（204ページ）のステップ6で書き留めた**ログイン URL** を入力します。
     - [アイデンティティプロバイダー発行元（Identity Provider Issuer）] には、Azure の Management Center サービス プロバイダー アプリケーションの設定（204 ページ）のステップ 6 で書き留めた **Azure AD 識別子**を入力します。
     - [X.509証明書（X.509 Certificate）] には、Azure の Management Center サービス プロバイダー アプリケーションの設定（204 ページ）のステップ 5 で Azure からダウンロー

ドした証明書を使用します。（テキストエディタを使用して証明書ファイルを開き、内容をコピーして [X.509証明書（X.509 Certificate）] フィールドに貼り付けます。）

- Azure によって生成された XML メタデータファイルをローカルコンピュータに保存した場合（Azure の Management Center サービス プロバイダー アプリケーションの設定 （204 ページ）のステップ 7）、ファイルを Management Center にアップロードできます。

  1. [XMLファイルのアップロード（Upload XML File）]オプションボタンをクリックします。
  2. 画面の指示に従って、ローカルコンピュータ上の XML メタデータファイルに移動して選択します。

ステップ 2 [次へ（Next）] をクリックします。

ステップ 3 [メタデータの検証（Verify Metadata）]ダイアログで、構成パラメータを確認し、[保存（Save）] をクリックします。

ステップ 4 [Test Configuration] をクリックします。システムにエラーメッセージが表示された場合は、Management Center の SSO 設定と Azure サービス プロバイダー アプリケーションを確認し、エラーを修正してから再試行します。

ステップ 5 システムが構成テストの成功を報告したら、[適用（Apply）] をクリックします。

次のタスク

オプションで、SSO ユーザーのロールマッピングを設定できます。Management Center における Azure のユーザーロールマッピングの設定 （208 ページ）を参照してください。ロールマッピングを設定しないことを選択した場合、デフォルトで、Management Center にログインするすべての SSO ユーザーに、Management Center における Azure のユーザーロールマッピングの設定 （208 ページ）のステップ 4 で設定したデフォルトユーザーロールが割り当てられます。

Management Center における Azure のユーザーロールマッピングの設定

Management Center Web インターフェイスでユーザーロールマッピングを構成するフィールドは、SSO プロバイダーの選択に関係なく同じです。ただし、構成する値では、使用する SAML SSO プロバイダーのユーザーロールマッピングの導入方法を考慮する必要があります。

始める前に

- 既存の Azure ユーザーとグループを確認します。Azure テナントの確認 （204 ページ）を参照してください。
- Management Center の SSO サービス プロバイダー アプリケーションを設定します。Azure の Management Center サービス プロバイダー アプリケーションの設定 （204 ページ）を参照してください。

- Management Center でシングルサインオンを有効にして設定します。Management Centerでのシングルサインオンの有効化 （173 ページ）およびAzure SSO 用の Management Center の設定 （207 ページ）を参照してください。

手順

ステップ 1 **[システム（System）] > [ユーザー（Users）]** を選択します。

ステップ 2 [Single Sign-On] タブをクリックします。

ステップ 3 [詳細設定（ロールマッピング）（Advanced Configuration (Role Mapping)）] を展開します。

ステップ 4 [デフォルトのユーザーロール（Default User Role）] ドロップダウンから、ユーザーをデフォルト値として割り当てる Management Center ユーザーロールを選択します。

ステップ 5 [グループメンバーの属性（Group Member Attribute）] を入力します。この文字列は、Azure の Management Center サービス プロバイダー アプリケーション用に作成するユーザーの請求の名前と一致する必要があります。Azure IdP における個人ユーザーのユーザーロールマッピングの設定 （210 ページ）のステップ 1 またはAzure IdP におけるグループのユーザーロールマッピングの設定 （211 ページ）のステップ 1 を参照してください。

ステップ 6 SSO ユーザーに割り当てる各 Management Center ユーザーロールの横に、正規表現を入力します。（Management Center は、Golang と Perl でサポートされている、Google の RE2 正規表現標準規格の制限付きバージョンを使用します。）Management Center は、これらの値を、IdP が SSO ユーザー情報とともに Management Center に送信するユーザーロールマッピング属性値と比較します。Management Center は、一致が見つかったすべてのロールの和集合をユーザーに付与します。

次のタスク

サービス プロバイダー アプリケーションでユーザーロールマッピングを構成します。Azure IdP におけるユーザーロールマッピングの設定 （209 ページ）を参照してください。

Azure IdP におけるユーザーロールマッピングの設定

個人ユーザーの権限またはグループの権限に基づいて、Azure AD ポータルで SSO ユーザーロールマッピングを設定できます。

- 個人ユーザーのアクセス許可に基づいてマップするには、「Azure IdP における個人ユーザーのユーザーロールマッピングの設定」を参照してください。
- グループのアクセス許可に基づいてマップするには、「Azure IdP におけるグループのユーザーロールマッピングの設定」を参照してください。

SSO ユーザーが Management Center にログインすると、Azure は、Azure AD ポータルで設定されたアプリケーションロールから値を取得するユーザーまたはグループロールの属性値を Management Center に提示します。Management Center はその属性値を SSO 設定で各 Management Center ユーザーロールに割り当てられた正規表現と比較し、一致が見つかったすべてのロール

をユーザーに付与します。（一致するものが見つからない場合、Management Center は設定可能なデフォルトのユーザーロールをユーザーに付与します）。各 Management Center ユーザーロールに割り当てる式は、Golang と Perl でサポートされている Google の RE2 正規表現標準規格の制限付きバージョンに準拠している必要があります。Management Center は、Azure から受け取った属性値を、Management Center ユーザーロール式との比較のために、同じ標準規格を使用する正規表現として扱います。

（注） Management Center 単一では、グループと個人ユーザーの両方のロールマッピングをサポートできません。Management Center サービス プロバイダー アプリケーションに対して 1 つのマッピング方法を選択し、それを一貫して使用する必要があります。Management Center は、Azure で構成された 1 つの要求のみを使用してロールマッピングをサポートできます。一般に、グループベースのロールマッピングは、多数のユーザーがいる Management Center でより効率的です。Azure テナント全体で確立されたユーザーとグループの定義を考慮する必要があります。

Azure IdP における個人ユーザーのユーザーロールマッピングの設定

Azure で Management Center サービスアプリケーションの個人ユーザーのロールマッピングを確立するには、Azure AD ポータルを使用してアプリケーションに要求を追加し、アプリケーションの登録マニフェストにロールを追加して、ロールをユーザーに割り当てます。

始める前に

- Azure テナントを確認します。Azure テナントの確認 （204 ページ）を参照してください。
- Azure で Management Center サービス プロバイダー アプリケーションを作成して設定します。Azure の Management Center サービス プロバイダー アプリケーションの設定 （204 ページ）を参照してください。
- Management Center における Azure のユーザーロールマッピングの設定 （208 ページ）の説明に従って、SSO ユーザーロールマッピングを設定します。

手順

ステップ 1 次の特性を使用して、Management Center サービスアプリケーションの SSO 設定にユーザー要求を追加します。

- [名前（Name）]：Management Center SSO 設定で [グループメンバーの属性（Group Member Attribute）] に入力したものと同じ文字列を使用します。（Management Center における Azure のユーザーロールマッピングの設定 （208 ページ）のステップ 5 を参照してください）。
- [名前識別子の形式（Name identifier format）]：[永続（Persistent）] を選択します。
- [ソース（Source）]：`Attribute` を選択します。
- [ソース属性（Source attribute）]：`user.assignedroles` を選択します。

ステップ 2 Management Center サービスアプリケーションのマニフェスト（JSON 形式）を編集し、アプリケーションロールを追加して、SSO ユーザーに割り当てる Management Center ユーザーロールを表します。最も簡単な方法は、既存のアプリケーションロール定義をコピーして、次のプロパティを変更することです。

- `displayName`：AD Azure ポータルで表示されるロールの名前。
- `description`：ロールの簡単な説明。
- `Id`：マニフェスト内の ID プロパティの中で一意である必要がある英数字。
- `value`：1 つ以上の Management Center ユーザーロールを表す文字列。（注：Azure では、この文字列にスペースを含めることはできません）。

ステップ 3 Management Center サービスアプリケーションに割り当てられたユーザーごとに、そのアプリケーションのマニフェストに追加したアプリケーションロールの 1 つを割り当てます。ユーザーが SSO を使用して Management Center にログインする場合、そのユーザーに割り当てるアプリケーションロールは、Azure がサービスアプリケーションの要求で Management Center に送信する値です。Management Center は、SSO 設定で Management Center ユーザーロールに割り当てた式と要求を比較し（Management Center における Azure のユーザーロールマッピングの設定 （208 ページ）のステップ 6 を参照）、一致するすべての Management Center ユーザーロールをユーザーに割り当てます。

次のタスク

- さまざまなアカウントから SSO を使用して Management Center にログインし、期待どおりにユーザーに Management Center ユーザーロールが割り当てられることを確認することで、ロールマッピングスキームをテストします。

Azure IdP におけるグループのユーザーロールマッピングの設定

Azure で Management Center サービスアプリケーションのユーザーグループのロールマッピングを確立するには、Azure AD ポータルを使用してアプリケーションに要求を追加し、アプリケーションの登録マニフェストにロールを追加して、ロールをグループに割り当てます。

始める前に

- Azure テナントを確認します。Azure テナントの確認 （204 ページ）を参照してください。
- Azure で Management Center サービス プロバイダー アプリケーションを作成して設定します。Azure の Management Center サービス プロバイダー アプリケーションの設定 （204 ページ）を参照してください。
- Management Center における Azure のユーザーロールマッピングの設定 （208 ページ）の説明に従って、SSO ユーザーロールマッピングを設定します。

手順

ステップ 1 次の特性を使用して、Management Center サービスアプリケーションの SSO 設定にユーザー要求を追加します。

- [名前（Name）]：Management Center SSO 設定で [グループメンバーの属性（Group Member Attribute）] に入力したものと同じ文字列を使用します。（Management Center における Azure のユーザーロールマッピングの設定 （208 ページ）のステップ 5 を参照してください）。
- [名前識別子の形式（Name identifier format）]：[永続（Persistent）] を選択します。
- [ソース（Source）]：`Attribute` を選択します。
- [ソース属性（Source attribute）]：`user.assignedroles` を選択します。

ステップ 2 Management Center サービスアプリケーションのマニフェスト（JSON 形式）を編集し、アプリケーションロールを追加して、SSO ユーザーに割り当てる Management Center ユーザーロールを表します。最も簡単な方法は、既存のアプリケーションロール定義をコピーして、次のプロパティを変更することです。

- `displayName`：Ad Azure ポータルで表示されるロールの名前。
- `description`：ロールの簡単な説明。
- `Id`：マニフェスト内の ID プロパティの中で一意である必要がある英数字。
- `value`：1 つ以上の Management Center ユーザーロールを表す文字列。（Azure では、この文字列にスペースを含めることはできません）。

ステップ 3 Management Center サービスアプリケーションに割り当てられたグループごとに、そのアプリケーションのマニフェストに追加したアプリケーションロールの 1 つを割り当てます。ユーザーが SSO を使用して Management Center にログインする場合、そのユーザーのグループに割り当てるアプリケーションロールは、Azure がサービスアプリケーションの要求で Management Center に送信する値です。Management Center は、SSO 設定で Management Center ユーザーロールに割り当てた式と要求を比較し（Management Center における Azure のユーザーロールマッピングの設定 （208 ページ）のステップ 6 を参照）、一致するすべての Management Center ユーザーロールをユーザーに割り当てます。

次のタスク

さまざまなアカウントから SSO を使用して Management Center にログインし、期待どおりにユーザーに Management Center ユーザーロールが割り当てられることを確認することで、ロールマッピングスキームをテストします。

Azure ユーザーロールマッピングの例

次の例が示すように、ユーザーロールマッピングをサポートする Management Center での SSO 構成は、個々のユーザーとグループの両方で同じです。違いは、Azure の Management Center サービス プロバイダー アプリケーションの設定にあります。

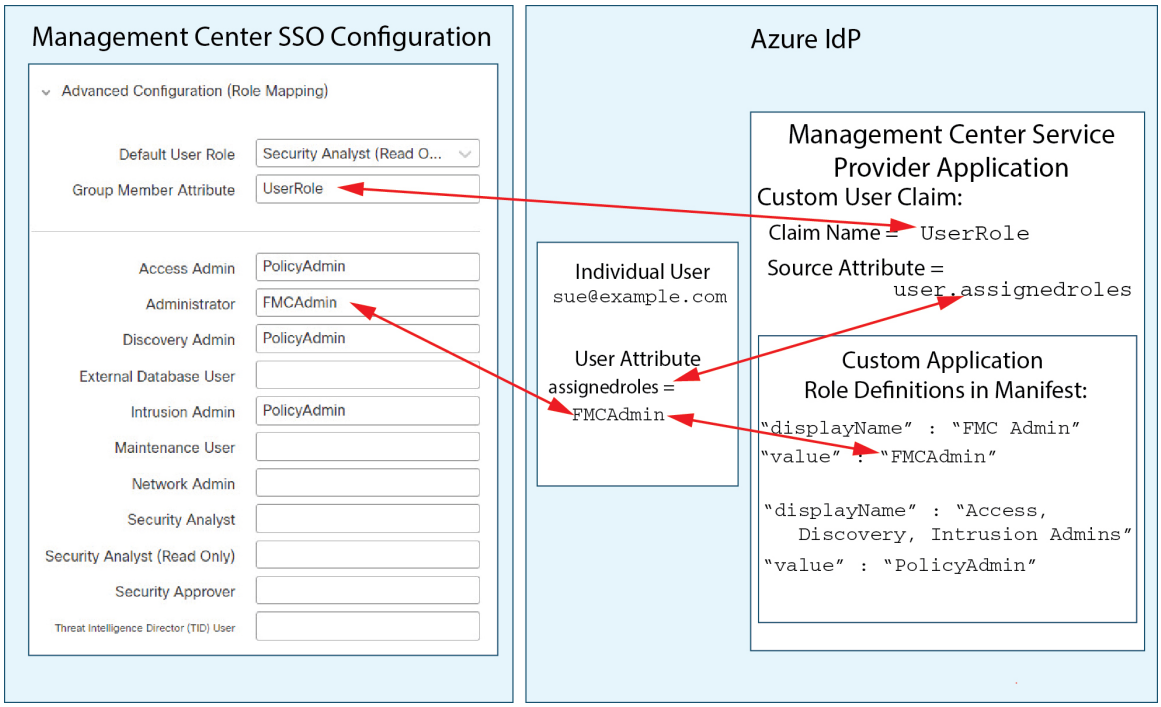
（注） 個別の権限またはグループ権限に基づいて Management Center ロールがマッピングされるように構成できますが、単一の Management Center アプリケーションでは、グループと個人ユーザーの両方のロールマッピングはサポートできないことに注意してください。Management Center は、Azure で構成された 1 つの要求のみを使用してロールマッピングをサポートできます。

個人ユーザーアカウントの Azure ロールマッピングの例

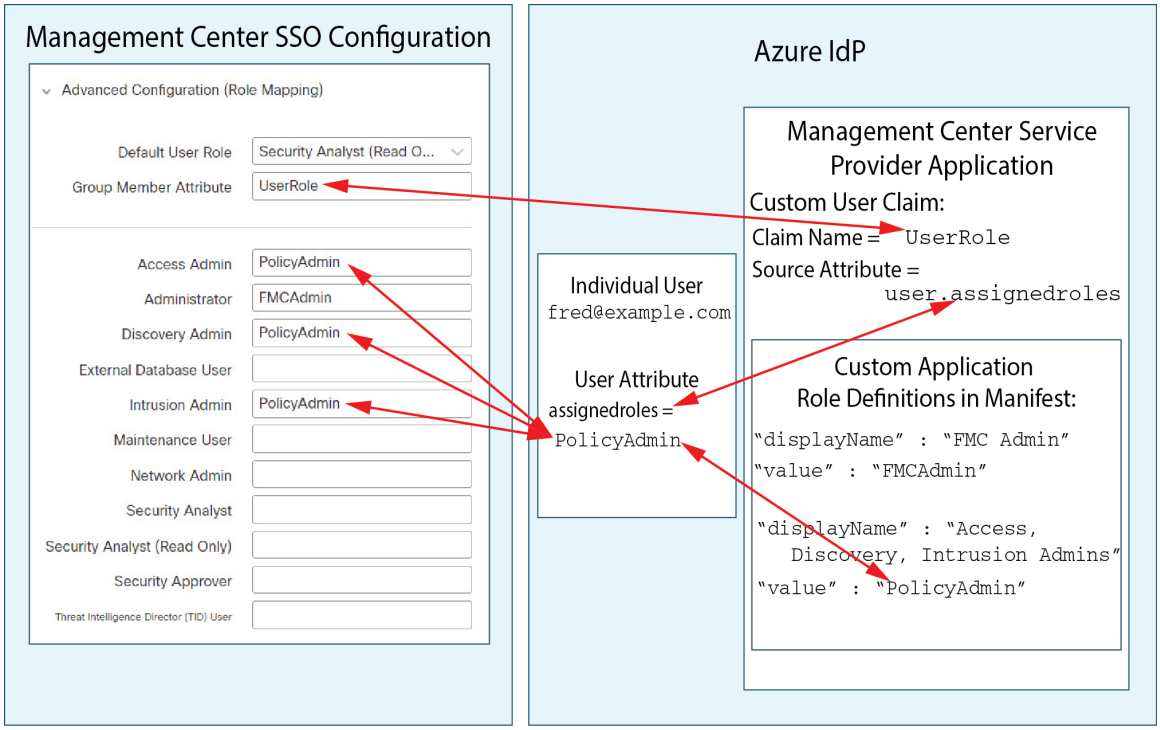
個人ユーザーのロールマッピングでは、Azure Management Center サービスアプリケーションのマニフェスト内にカスタムロールが定義されています（この場合、FMCAdmin と PolicyAdmin です）。これらのロールはユーザーに割り当てることができます。Azure は、各ユーザーのロールの割り当てをそのユーザーの assignedroles 属性に保存します。アプリケーションにはカスタムユーザークレームも定義されていて、このクレームは、SSO を使用して Management Center にログインしているユーザーに割り当てられたユーザーロールから値を取得するように構成されています。Azure は SSO ログインプロセス中にクレーム値を Management Center に渡し、Management Center はクレーム値を Management Center SSO 構成の各 Management Center ユーザーロールに割り当てられた文字列と比較します。

次の図は、Management Center および Azure 構成の関連するフィールドと値が、個人アカウントのユーザーロールマッピングで互いにどのように対応しているかを示しています。各図は、Management Center と Azure AD ポータルで同じ SSO 構成を使用していますが、Azure AD ポータルでの各ユーザーの構成は、Management Center で各ユーザーに異なるロールを割り当てるために異なります。

- この図では、sue@ example.com では assignedroles 属性値 `FMCAdmin` が使用されていて、Management Center が彼女に Management Center 管理者ロールを割り当てます。



- この図では、fred@example.com では assignedroles 属性値 `PolicyAdmin` が使用されていて、Management Center が彼にアクセス管理者、検出管理者、侵入管理者のロールを割り当てます。



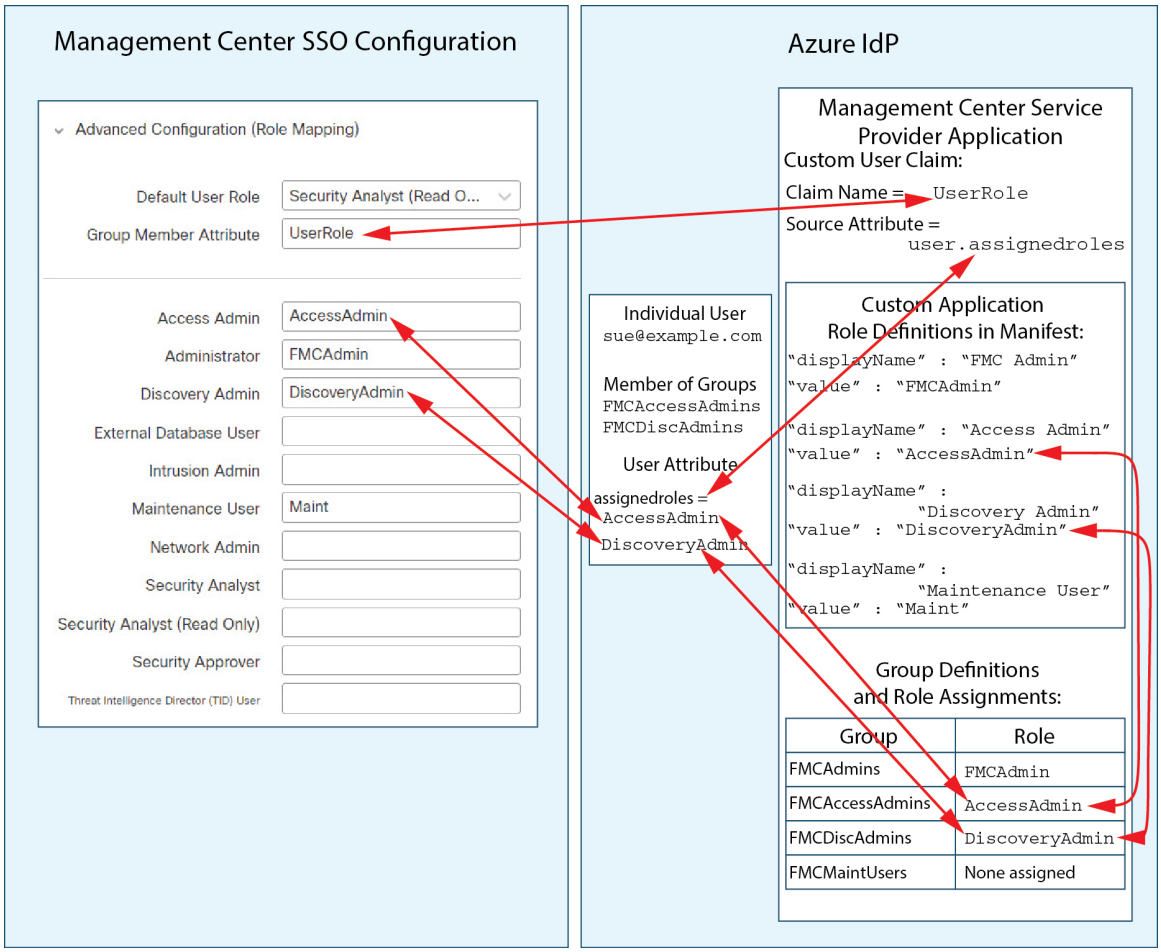
- この Management Center のために Azure サービスアプリケーションに割り当てられた他のユーザーには、次のいずれかの理由で、デフォルトのユーザーロールであるセキュリティアナリスト（読み取り専用）が割り当てられます。
  - これらには、assignedroles 属性に割り当てられた値がありません。
  - assignedroles 属性に割り当てられた値が、Management Center の SSO 設定でユーザーロールに設定された式と一致しません。

グループの Azure ロールマッピングの例

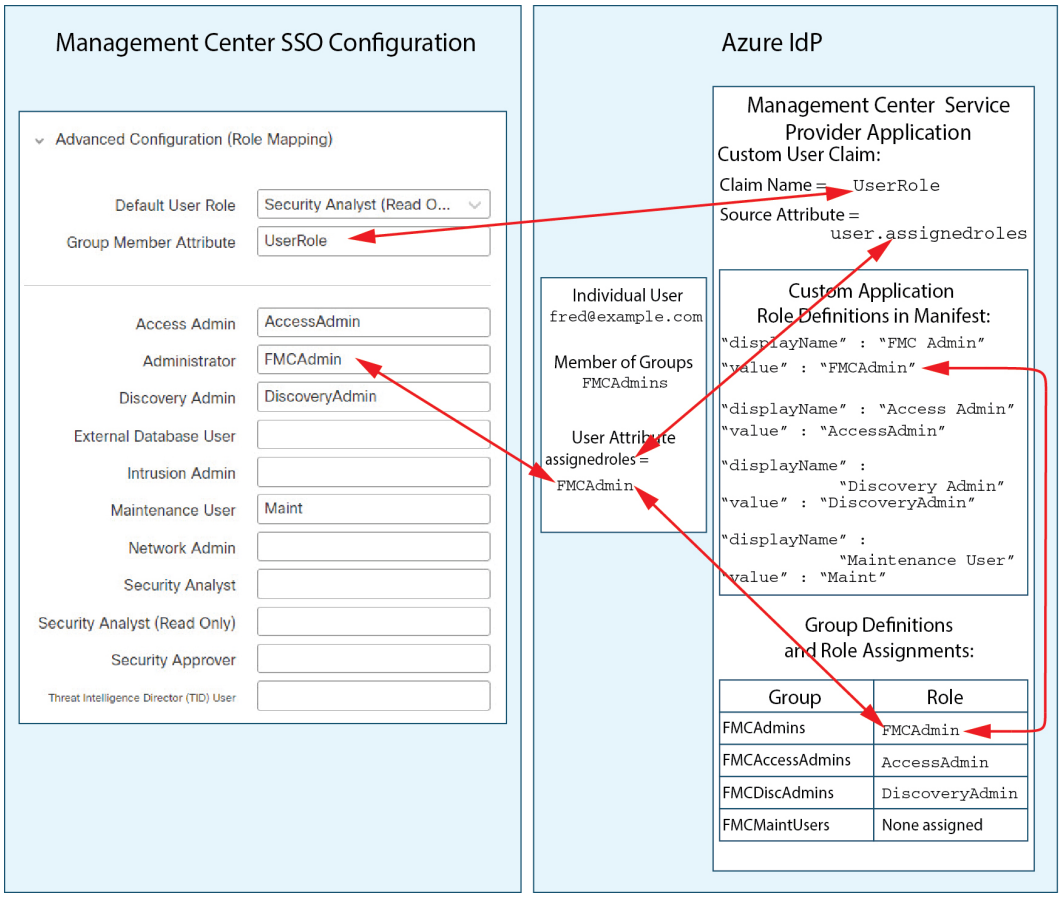
グループのロールマッピングでは、Azure Management Center サービスアプリケーションのマニフェスト内にカスタムロールが定義されています（この場合、FMCAdmin、AccessAdmin、Discovery Admin、Maint です）。これらのロールはグループに割り当てることができます。Azure は、各グループのロールの割り当てをグループメンバーの assignedroles 属性に渡します。アプリケーションにはカスタムユーザークレームも定義されていて、このクレームは、SSO を使用して Management Center にログインしているユーザーに割り当てられたユーザーロールから値を取得するように構成されています。Azure は SSO ログインプロセス中にクレーム値を Management Center に渡し、Management Center はクレーム値を Management Center SSO 構成の各 Management Center ユーザーロールに割り当てられた文字列と比較します。

次の図は、Management Center および Azure 構成の関連するフィールドと値が、グループのユーザーロールマッピングで互いにどのように対応しているかを示しています。各図は、Management Center と Azure AD ポータルで同じ SSO 構成を使用していますが、Azure AD ポータルでの各ユーザーの構成は、Management Center で各ユーザーに異なるロールを割り当てるために異なります。

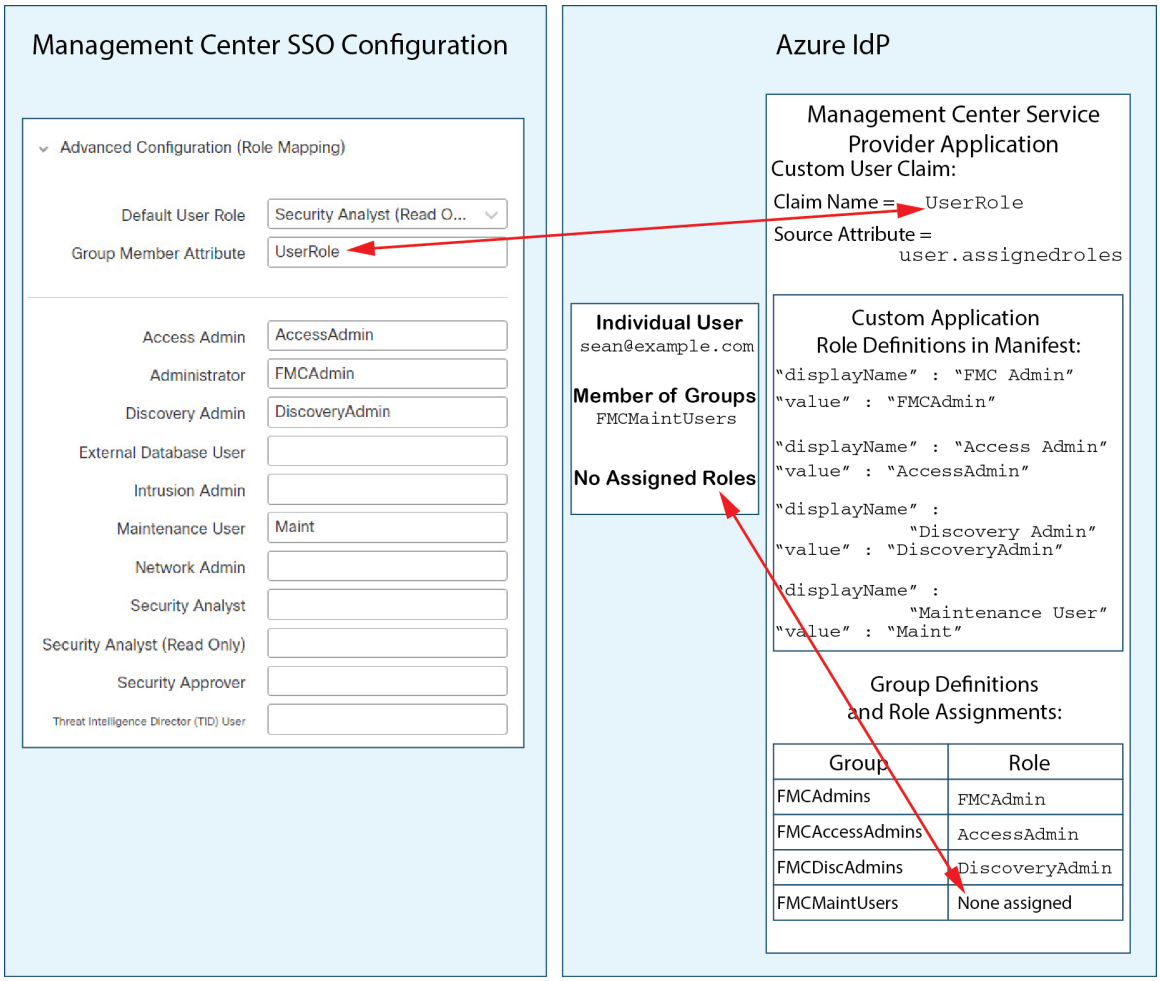
- この図では、sue@example.com は `FMCAccessAdmins` および `FMCDiscoveryAdmins` グループのメンバーです。これらのグループから、Sue はカスタムロール `AccessAdmin` および `DiscoveryAdmin` を継承します。Sue が SSO を使用して Management Center にログインすると、Management Center によってアクセス管理者および検出管理者のロールが割り当てられます。



- この図では、fred@example.com は `FMCAdmins` グループのメンバーであり、そこからカスタムロール `FMCAdmin` を継承しています。Fred が SSO を使用して Management Center にログインすると、Management Center によって管理者ロールが割り当てられます。

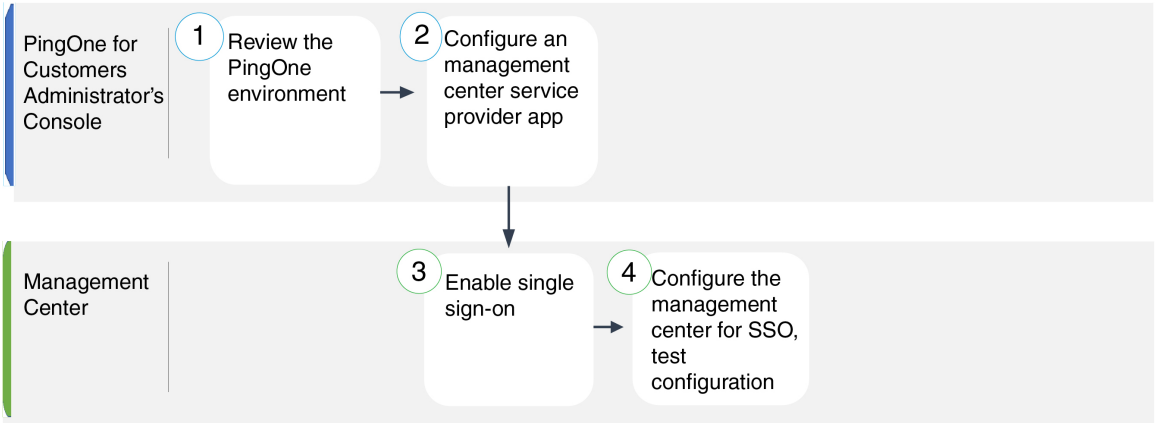


- この図では、sean@example.com は `FMCMaintUsers` グループのメンバーですが、Azure Management Center サービス プロバイダー アプリケーション内で `FMCMaintUsers` にカスタムロールが割り当てられていないため、Sean にはロールが割り当てられていません。このため、SSO を使用して Management Center にログインすると、Management Center によってデフォルトロールのセキュリティアナリスト（読み取り専用）が割り当てられます。



PingID を使用したシングルサインオンの設定

PingID の PingOne for Customers 製品を使用して SSO を設定するには、次のタスクを参照してください。



1	PingOne for Customers 管理者コンソール	PingID PingOne for Customers 環境の確認 （219 ページ）。
2	PingOne for Customers 管理者コンソール	PingID PingOne for Customers の Management Center サービス プロバイダー アプリケーションの設定 （219 ページ）。
3	Management Center	Management Centerでのシングルサインオンの有効化 （173 ページ）。
4	Management Center	PingID PingOne for Customers を使用した SSO 用の Management Center の設定 （221 ページ）。

PingID PingOne for Customers 環境の確認

PingOne for Customers は、PingID のクラウドでホストされる Identity-as-a-Service（IDaaS）製品です。PingOne for Customers では、ユーザーが同じ SSO アカウントでアクセスできるすべてのフェデレーテッドデバイスが含まれているエンティティを環境と呼びます。Management Center を PingOne 環境に追加する前に、その組織についてよく理解してください。次の質問を考慮してください。

- Management Center にアクセスできるユーザーは何人ですか？
- Management Center で SSO をサポートするために、ユーザーを追加する必要がありますか。

このドキュメントは、PingOne for Customers 管理者コンソールに精通していて、組織管理者ロールを持つアカウントを持っていることを前提としています。

PingID PingOne for Customers の Management Center サービス プロバイダー アプリケーションの設定

PingOne for Customers 管理者コンソールを使用して、PingOne for Customers 環境内に Management Center サービス プロバイダー アプリケーションを作成し、基本的な構成設定を確立します。このドキュメントでは、完全に機能する SSO 環境を確立するために必要な PingOne for Customers のすべての機能について説明しているわけではありません。たとえば、ユーザーを作成するには、PingOne for Customers のドキュメントを参照してください。

始める前に

- PingOne for Customers 環境とそのユーザーについてよく理解してください。
- 必要に応じて、追加のユーザーを作成します。

（注） システムでは、SSO アカウントのユーザー名と、SAML ログイン プロセス中に IdP が Management Center に送信する NameID 属性の両方が有効な電子メールアドレスである必要があります。多くの IdP は、ログインしようとしているユーザーのユーザー名を NameID 属性として自動的に使用しますが、これが IdP に適しているかを確認する必要があります。IdP でサービス プロバイダー アプリケーションを設定し、Management Center への SSO アクセス権限を持つ IdP ユーザーアカウントを作成する場合は、このことに注意してください。

- ターゲット Management Center のログイン URL を確認します（`https://ipaddress_or_hostname`）

（注） Management Center Web インターフェイスに複数の URL（たとえば、完全修飾ドメイン名と IP アドレス）でアクセスできる場合、SSO ユーザーは、一貫してこのタスクで構成するログイン URL を使用して Management Center にアクセスする必要があります。

手順

ステップ 1 PingOne for Customer 管理者コンソールを使用して、次の設定を使用して環境内にアプリケーションを作成します。

- [Webアプリケーション（Web App）] のアプリケーションタイプを選択します。
- [SAML] の接続タイプを選択します。

ステップ 2 SAML 接続に次の設定を使用してアプリケーションを設定します。

- [ACS URL] については、文字列 `/sam/acs` を Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/acs`。
- [署名証明書（Signing Certificate）] で、[アサーションと応答の署名（Sign Assertion & Response）] を選択します。
- [署名アルゴリズム（Signing Algorithm）] には、RSA_SHA256 を選択します。
- [エンティティID（Entity ID）] については、文字列 `/saml/metadata` を Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/metadata`。
- [SLOバインド（SLO Binding）] で [HTTP POST] を選択します。
- [アサーション有効期間（Assertion Validity Duration）] には、300 と入力します。

ステップ 3 アプリケーションの SAML 接続情報にある、次の値に注目してください。

- シングルサインオンサービス（Single Sign-On Service）
- 発行者 ID（Issuer ID）

これらの値は、Management Center Web インターフェイスで PingID の PingOne for Customers 製品を使用して SSO を設定するときに必要になります。

ステップ 4 [SAML属性（SAML ATTRIBUTES）] で、単一の必須属性に対して次の選択を行います。

- [PINGONEユーザー属性（PINGONE USER ATTRIBUTE）]：`Email Address`
- [アプリケーション属性（APPLICATION ATTRIBUTE）]：`saml_subject`

ステップ 5 署名証明書を X509 PEM（`.crt`）形式でダウンロードし、ローカルコンピュータに保存します。

ステップ 6 （オプション）Management Center での SSO セットアップを簡単にするために、Management Center サービス プロバイダー アプリケーションの SAML XML メタデータファイルをローカルコンピュータにダウンロードできます。

ステップ 7 アプリケーションを有効にします。

次のタスク

シングルサインオンを有効にします。Management Centerでのシングルサインオンの有効化（173 ページ）を参照してください。

PingID PingOne for Customers を使用した SSO 用の Management Center の設定

Management Center Web インターフェイスでこれらの手順を使用します。

始める前に

- PingOne for Customers 管理者コンソールで Management Center サービス プロバイダー アプリケーションを作成します。PingID PingOne for Customers の Management Center サービス プロバイダー アプリケーションの設定（219 ページ）を参照してください。
- シングルサインオンを有効にします。Management Centerでのシングルサインオンの有効化（173 ページ）を参照してください。

手順

ステップ 1 （このステップはManagement Centerでのシングルサインオンの有効化（173 ページ）から直接続きます）。[PingIDメタデータの設定（Configure PingID Metadata）] ダイアログには、2 つの選択肢があります。

- SSO 構成情報を手動で入力するには：

1. [手動設定（Manual Configuration）] オプションボタンをクリックします。
2. PingOne for Customers 管理者コンソールから取得した値を入力します。
   - [アイデンティティプロバイダーのシングルサインオンURL（Identity Provider Single Sign-On URL）] には、PingID PingOne for Customers の Management Center サービス プロバイダー アプリケーションの設定 （219 ページ）のステップ 3 で書き留めた**シングルサインオンサービス**を入力します。
   - [アイデンティティプロバイダー発行元（Identity Provider Issuer）] には、PingID PingOne for Customers の Management Center サービス プロバイダー アプリケーションの設定 （219 ページ）のステップ 3 で書き留めた**発行者 ID** を入力します。
   - [X.509証明書（X.509 Certificate）] には、PingID PingOne for Customers の Management Center サービス プロバイダー アプリケーションの設定 （219 ページ）のステップ 5 で PingOne for Customers からダウンロードした証明書を使用します。（テキストエディタを使用して証明書ファイルを開き、内容をコピーして [X.509証明書（X.509 Certificate）] フィールドに貼り付けます。）

- PingOne for Customers によって生成された XML メタデータファイルをローカルコンピュータに保存した場合（PingID PingOne for Customers の Management Center サービス プロバイダー アプリケーションの設定 （219 ページ）のステップ 6）、ファイルを Management Center にアップロードできます。
  1. [XMLファイルのアップロード（Upload XML File）] オプションボタンをクリックします。
  2. 画面の指示に従って、ローカルコンピュータ上の XML メタデータファイルに移動して選択します。

ステップ 2 [次へ（Next）] をクリックします。

ステップ 3 [メタデータの検証（Verify Metadata）] ダイアログで、構成パラメータを確認し、[保存（Save）] をクリックします。

ステップ 4 [詳細設定（ロールマッピング）（Advanced Configuration (Role Mapping)）] を展開します。

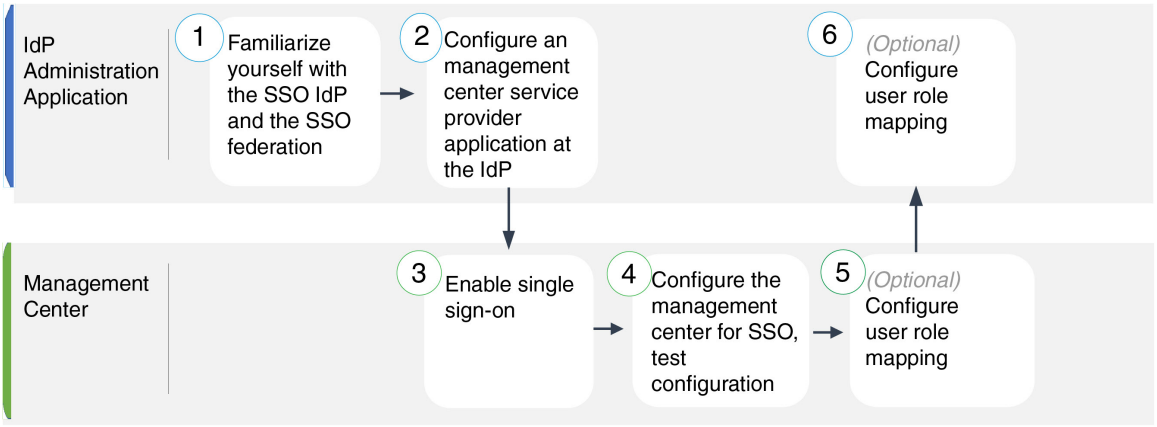
ステップ 5 [デフォルトのユーザーロール（Default User Role）] ドロップダウンから、ユーザーをデフォルト値として割り当てる Management Center ユーザーロールを選択します。

ステップ 6 [Test Configuration] をクリックします。システムにエラーメッセージが表示された場合は、Management Center の SSO 構成と PingOne for Customers サービス プロバイダー アプリケーションを確認し、エラーを修正してから再試行します。

ステップ 7 システムが構成テストの成功を報告したら、[適用（Apply）] をクリックします。

SAML 2.0 準拠の SSO プロバイダーでのシングルサインオンの設定

Management Center は、SAML 2.0 SSO プロトコル準拠の SSO アイデンティティ プロバイダー（IdP）によるシングルサインオンをサポートしています。幅広い SSO プロバイダーを使用するための一般的な手順では、実行するタスクの概要を扱う必要があります。このドキュメントで具体的に扱われていないプロバイダーを使用して SSO を確立するには、選択した IdP に習熟している必要があります。これらのタスクは、SAML 2.0 準拠の SSO プロバイダーを使用したシングルサインオンのために Management Center を設定する手順を判断するために役立ちます。



1	IdP 管理アプリケーション	SSO アイデンティティ プロバイダーおよび SSO フェデレーションの理解（224 ページ）。
2	IdP 管理アプリケーション	SAML 2.0 準拠の SSO プロバイダー用の Management Center サービス プロバイダー アプリケーションの設定（225 ページ）。
3	Management Center	Management Centerでのシングルサインオンの有効化（173 ページ）。
4	Management Center	SAML 2.0 準拠の SSO プロバイダーを使用した SSO 用の Management Center の設定（227 ページ）。
5	Management Center	SAML 2.0 準拠の SSO プロバイダーの Management Center でのユーザーロールマッピングの設定（228 ページ）。

6	IdP 管理アプリケーション	SAML 2.0 準拠の SSO プロバイダーの IdP での Management Center ユーザーロールマッピングの設定 （230 ページ）。

SSO アイデンティティ プロバイダーおよび SSO フェデレーションの理解

次の点を考慮して、IdP ベンダーのドキュメントを読んでください。

- SSO プロバイダーは、ユーザーが IdP を使用する前にサービスにサブスクライブまたは登録することを要求していますか。
- SSO プロバイダーは、一般的な SSO の概念にどのような用語を使用しますか。たとえば、フェデレーテッドサービスプロバイダーアプリケーションのグループを参照するために、Okta は「組織」を使用しますが、Azure は「テナント」を使用します。
- SSO プロバイダーは SSO のみをサポートしていますか、それとも一連の機能（多要素認証やドメイン管理など）をサポートしていますか（これは、機能間で共有される一部の要素、特にユーザーとグループの構成に影響を与える可能性があります）。
- SSO を構成するために IdP ユーザーアカウントに必要な権限は何ですか。
- SSO プロバイダーは、サービス プロバイダー アプリケーションに対してどのような構成を確立する必要がありますか。たとえば、Okta は Management Center との通信を保護するために X509 証明書を自動的に生成しますが、Azure では Azure portal インターフェイスを使用してその証明書を生成する必要があります。
- ユーザーとグループはどのように作成および構成されますか。ユーザーはどのようにグループに割り当てられますか。ユーザーおよびグループは、サービス プロバイダー アプリケーションへのアクセスをどのように許可されますか。
- SSO プロバイダーは、SSO 接続をテストする前に、サービス プロバイダー アプリケーションに少なくとも 1 人のユーザーを割り当てる必要がありますか。
- SSO プロバイダーはユーザーグループをサポートしていますか。ユーザー属性とグループ属性はどのように構成されますか。SSO 構成で属性を Management Center ユーザーロールにマップするにはどうすればよいですか。
- Management Center で SSO をサポートするために、フェデレーションにユーザーまたはグループを追加する必要がありますか。
- ユーザーはグループのフェデレーションメンバーですか。
- ユーザーとグループの定義は IdP にネイティブですか。それとも Active Directory、RADIUS、LDAP などのユーザー管理アプリケーションからインポートされますか。
- どのようなユーザーロールの割り当てを行いますか。（ユーザーロールを割り当てない場合は、Management Center が、ユーザーによる設定が可能なデフォルトのユーザーロールを、すべての SSO ユーザーに自動的に割り当てます）。

- 必要なユーザーロールマッピングをサポートする計画において、フェデレーション内のユーザーとグループをどのように編成する必要がありますか。

SAML 2.0 準拠の SSO プロバイダー用の Management Center サービス プロバイダー アプリケーションの設定

通常、SSO プロバイダーでは、フェデレーション アプリケーションごとに IdP でサービス プロバイダー アプリケーションを設定する必要があります。SAML 2.0 SSO をサポートするすべての IdP では、サービス プロバイダー アプリケーションに同一の構成情報が必要になりますが、一部の IdP では構成設定が自動的に生成され、他の IdP ではすべての設定を自分で構成する必要があります。

（注） Management Center アプリケーションにユーザーグループを割り当てることを計画している場合は、それらのグループ内のユーザーを個人として割り当てないでください。

（注） Management Center は、複数の SSO 属性を使用したロールマッピングをサポートできません。ユーザーロールマッピングまたはグループロールマッピングのいずれかを選択し、単一の属性を構成して、IdP からのユーザーロール情報を Management Center に伝達する必要があります。

始める前に

- SSO フェデレーションとそのユーザーおよびグループについて理解します。SSO アイデンティティ プロバイダーおよび SSO フェデレーションの理解 （224 ページ）を参照してください。
- IdP アカウントに、このタスクを実行するために必要な権限があることを確認します。
- 必要に応じて、SSO フェデレーションにユーザーアカウントやグループを作成します。

（注） システムでは、SSO アカウントのユーザー名と、SAML ログイン プロセス中に IdP が Management Center に送信する NameID 属性の両方が有効な電子メールアドレスである必要があります。多くの IdP は、ログインしようとしているユーザーのユーザー名を NameID 属性として自動的に使用しますが、これが IdP に適しているかを確認する必要があります。IdP でサービス プロバイダー アプリケーションを設定し、Management Center への SSO アクセス権限を持つ IdP ユーザーアカウントを作成する場合は、このことに注意してください。

- ターゲット Management Center のログイン URL を確認します（`https://ipaddress_or_hostname`）

（注） Management Center Web インターフェイスに複数の URL （たとえば、完全修飾ドメイン名と IP アドレス）でアクセスできる場合、SSO ユーザーは、一貫してこのタスクで設定するログイン URL を使用して Management Center にアクセスする必要があります。

手順

ステップ 1 IdP で新しいサービス プロバイダー アプリケーションを作成します。

ステップ 2 IdP に必要な値を設定します。Management Center で SAML 2.0 SSO 機能をサポートするために必要な、以下のフィールドを必ず含めてください。（SAML の概念には、さまざまな SSO サービスプロバイダーでさまざまな用語が使用されているため、このリストでは、IdP アプリケーションで適切な設定を見つけるために役立つこれらのフィールドの代替名を示しています）。

- サービスプロバイダーのエンティティ ID、サービスプロバイダー識別子、オーディエンス URI：サービスプロバイダー（Management Center）のグローバルに一意の名前で、URL としてフォーマットされます。これを作成するには、`https://ExampleFMC/saml/metadata` のように、Management Center ログイン URL に文字列 `/saml/metadata` を追加します。
- シングルサインオン URL、受信者 URL、アサーション コンシューマ サービス URL：ブラウザが IdP の代わりに情報を送信するサービスプロバイダー（Management Center）のアドレス。これを作成するには、`https://ExampleFMC/saml/acs` のように、Management Center ログイン URL に文字列 `saml/acs` を追加します。
- X.509 証明書：Management Center と IdP の間の通信を保護するための証明書。IdP の中には、証明書を自動的に生成するものもあれば、IDP インターフェイスを使用して明示的に生成する必要があるものもあります。

ステップ 3 （アプリケーションにグループを割り当てる場合はオプション）個人ユーザーを Management Center アプリケーションに割り当てます。（Management Center アプリケーションにグループを割り当てることを計画している場合は、それらのグループのメンバーを個人として割り当てないでください）。

ステップ 4 （個人ユーザーをアプリケーションに割り当てる場合はオプション）Management Center アプリケーションにユーザーグループを割り当てます。

ステップ 5 （オプション）一部の IdP には、SAML 2.0 標準に準拠するようにフォーマットされた、このタスクで設定した情報を含む SAML XML メタデータファイルを生成する機能があります。IdP にこの機能がある場合は、Management Center で SSO 設定プロセスを簡単に行うことができるように、ローカルコンピュータにこのファイルをダウンロードすることができます。

次のタスク

シングルサインオンを有効にします。Management Centerでのシングルサインオンの有効化（173 ページ）を参照してください。

SAML 2.0 準拠の SSO プロバイダーを使用した SSO 用の Management Center の設定

Management Center Web インターフェイスでこれらの手順を使用します。SAML 2.0 準拠の SSO プロバイダーを使用した SSO 用に Management Center を設定するには、IdP からの情報が必要です。

始める前に

- SSO フェデレーションの組織と、そのユーザーとグループを確認します。
- IdP の Management Center サービス プロバイダー アプリケーションを設定します。SAML 2.0 準拠の SSO プロバイダーを使用した SSO 用の Management Center の設定（227 ページ）を参照してください。
- IdP から、サービス プロバイダー アプリケーションの次の SSO 設定情報を収集します。SAML の概念には、さまざまな SSO サービスプロバイダーでさまざまな用語が使用されているため、このリストでは、IdP アプリケーションで適切な値を見つけるために役立つこれらのフィールドの代替名を示しています。
  - アイデンティティ プロバイダーのシングルサインオン URL、ログイン URL：ブラウザが Management Center の代わりに情報を送信する IdP URL。
  - アイデンティティプロバイダー発行元、アイデンティティプロバイダー発行元URL、発行元 URL：多くの場合 URL としてフォーマットされる、IdP のグローバルに一意の名前。
  - Management Center と IdP の間の通信を保護するための X.509 デジタル証明書。
- シングルサインオンを有効にします。Management Centerでのシングルサインオンの有効化（173 ページ）を参照してください。

手順

ステップ 1 （このステップはManagement Centerでのシングルサインオンの有効化（173 ページ）から直接続きます）。[SAMLメタデータの設定（Configure SAML Metadata）] ダイアログには、2 つの選択肢があります。

- SSO 構成情報を手動で入力するには：
  1. [手動設定（Manual Configuration）] オプションボタンをクリックします。
  2. SSO サービス プロバイダー アプリケーションから、以前に取得した次の値を入力します。
     - **アイデンティティ プロバイダーのシングルサインオン URL**

- アイデンティティ プロバイダー発行元
- X.509 証明書

- IdP で生成された XML メタデータファイルを保存した場合（SAML 2.0 準拠の SSO プロバイダー用の Management Center サービス プロバイダー アプリケーションの設定 （225 ページ）のステップ 5）、ファイルを Management Center にアップロードできます。

  1. [XMLファイルのアップロード（Upload XML File）] オプションボタンをクリックします。
  2. 画面の指示に従って、ローカルコンピュータ上の XML メタデータファイルに移動して選択します。

ステップ 2 [次へ（Next）] をクリックします。

ステップ 3 [メタデータの検証（Verify Metadata）] ダイアログで、構成パラメータを確認し、[保存（Save）] をクリックします。

ステップ 4 [Test Configuration] をクリックします。システムにエラーメッセージが表示された場合は、Management Center の SSO 設定と IdP でのサービス プロバイダー アプリケーション設定を確認し、エラーを修正してから再試行します。

ステップ 5 システムが構成テストの成功を報告したら、[適用（Apply）] をクリックします。

次のタスク

オプションで、SSO ユーザーのユーザーロールマッピングを構成できます。SAML 2.0 準拠の SSO プロバイダーの Management Center でのユーザーロールマッピングの設定 （228 ページ）を参照してください。ロールマッピングを設定しないことを選択した場合、デフォルトで、Management Center にログインするすべての SSO ユーザーに、SAML 2.0 準拠の SSO プロバイダーの Management Center でのユーザーロールマッピングの設定 （228 ページ）のステップ 4 で設定したデフォルトユーザーロールが割り当てられます。

SAML 2.0 準拠の SSO プロバイダーの Management Center でのユーザーロールマッピングの設定

SAML SSO ユーザーロールマッピングを導入するには、IdP および Management Center で調整設定を確立する必要があります。

- IdP で、ユーザーまたはグループの属性を確立して、ユーザーロール情報を伝達し、それらに値を割り当てます。IdP は、SSO ユーザーを認証および承認すると、これらを Management Center に送信します。
- Management Center で、ユーザーに割り当てる各 Management Center ユーザーロールに値を関連付けます。

IdP が承認ユーザーに関連付けられたユーザーまたはグループ属性を Management Center に送信すると、Management Center は属性値を各 Management Center ユーザーロールに関連付けられた値と比較し、一致するすべてのロールをユーザーに割り当てます。Management Center は、Golang と Perl でサポートされている Google の RE2 正規表現標準規格の制限付きバージョンに準拠している正規表現として両方の値を扱い、この比較を実行します。

Management Center Web インターフェイスでユーザーロールマッピングを構成するフィールドは、SSO プロバイダーの選択に関係なく同じです。ただし、構成する値では、使用する SAML SSO プロバイダーのユーザーロールマッピングの導入方法を考慮する必要があります。IdP は、ユーザーまたはグループ属性に構文制限を適用する場合があります。その場合、ロール名とそれらの要件と互換性のある正規表現を使用して、ユーザー ロール マッピング スキームを考案する必要があります。

始める前に

- Management Center の SSO サービス プロバイダー アプリケーションを設定します。SAML 2.0 準拠の SSO プロバイダー用の Management Center サービス プロバイダー アプリケーションの設定 （225 ページ）を参照してください。
- Management Center でシングルサインオンを有効にして設定します。Management Centerでのシングルサインオンの有効化 （173 ページ）およびSAML 2.0 準拠の SSO プロバイダーを使用した SSO 用の Management Center の設定 （227 ページ）を参照してください。

手順

ステップ 1 **[システム（System）] > [ユーザー（Users）]** を選択します。

ステップ 2 [Single Sign-On] タブをクリックします。

ステップ 3 [詳細設定（ロールマッピング）（Advanced Configuration (Role Mapping)）] を展開します。

ステップ 4 [デフォルトのユーザーロール（Default User Role）] ドロップダウンから、ユーザーをデフォルト値として割り当てる Management Center ユーザーロールを選択します。

ステップ 5 [グループメンバーの属性（Group Member Attribute）] を入力します。この文字列は、ユーザーまたはグループのいずれかを使用するユーザーロールマッピングのために IdP Management Center サービス プロバイダー アプリケーションで設定された属性名と一致する必要があります。（SAML 2.0 準拠の SSO プロバイダーの IdP での Management Center ユーザーロールマッピングの設定 （230 ページ）のステップ 1 を参照。）

ステップ 6 SSO ユーザーに割り当てる各 Management Center ユーザーロールの横に、正規表現を入力します。（Management Center は、Golang と Perl でサポートされている、Google の RE2 正規表現標準規格の制限付きバージョンを使用します。）Management Center は、これらの値を、IdP が SSO ユーザー情報とともに Management Center に送信するユーザーロールマッピング属性値と比較します。Management Center は、一致が見つかったすべてのロールの和集合をユーザーに付与します。

次のタスク

サービス プロバイダー アプリケーションでユーザーロールマッピングを構成します。SAML 2.0 準拠の SSO プロバイダーの IdP での Management Center ユーザーロールマッピングの設定（230 ページ）を参照してください。

SAML 2.0 準拠の SSO プロバイダーの IdP での Management Center ユーザーロールマッピングの設定

ユーザーロールマッピングを構成するための詳細な手順は、IdP ごとに異なります。サービスプロバイダーアプリケーションのカスタムユーザーまたはグループ属性を作成する方法を決定し、IdP で各ユーザーまたはグループの属性に値を割り当てて、ユーザーまたはグループの特権を Management Center に伝える必要があります。次の点を考慮してください。

- IdP がサードパーティのユーザー管理アプリケーション（Active Directory、LDAP、Radius など）からユーザーまたはグループプロファイルをインポートする場合、これはロールマッピングの属性の使用方法に影響を与える可能性があります。
- SSO フェデレーション全体でユーザーとグループのロール定義を考慮してください。
- Management Center は、複数の SSO 属性を使用したロールマッピングをサポートできません。ユーザーロールマッピングまたはグループロールマッピングのいずれかを選択し、単一の属性を構成して、IdP からのユーザーロール情報を Management Center に伝達する必要があります。
- 一般に、グループロールマッピングは、多数のユーザーがいる Management Center でより効率的です。
- Management Center アプリケーションにユーザーグループを割り当てる場合は、それらのグループ内のユーザーを個人として割り当てないでください。
- Management Center ユーザーロール式との一致を判断するために、Management Center では IdP から受け取ったユーザーおよびグループロール属性値を、Golang と Perl でサポートされている Google の RE2 正規表現標準の制限バージョンに準拠した正規表現として扱います。IdP は、ユーザーまたはグループ属性に特定の構文制限を適用する場合があります。その場合、ロール名とそれらの要件と互換性のある正規表現を使用して、ユーザー ロール マッピング スキームを考案する必要があります。

始める前に

- IdP アカウントに、このタスクを実行するために必要な権限があることを確認します。
- IdP の Management Center サービス プロバイダー アプリケーションを設定します（SAML 2.0 準拠の SSO プロバイダー用の Management Center サービス プロバイダー アプリケーションの設定 （225 ページ）を参照してください）。

手順

ステップ 1 IdP で、Management Center に送信する属性を作成または指定して、各ユーザーサインインのロールマッピング情報を含めます。これは、ユーザー属性、グループ属性、または IdP またはサードパーティのユーザー管理アプリケーションによって維持されるユーザーまたはグループ定義などのソースから値を取得する別の属性である場合があります。

ステップ 2 属性がその値を取得する方法を構成します。取り得る値を、Management Center SSO 構成のユーザーロールに関連付けられた値と調整します。

Webインターフェイス用のユーザーロールのカスタマイズ

各ユーザアカウントは、ユーザロールで定義する必要があります。このセクションでは、ユーザ ロールを管理する方法と、Web インターフェイス アクセス用のカスタム ユーザ ロールを設定する方法について説明します。ユーザー ロールの詳細については、「ユーザの役割 （141 ページ）」を参照してください。

カスタム ユーザー ロールの作成

カスタムユーザーロールには、メニューベースのアクセス許可とシステムアクセス許可の任意のセットを持たせることができます。また、完全にオリジナルのものを作成することや、定義済みのユーザーロールまたは別のカスタムユーザーロールからコピーすることや、別のManagement Centerからインポートすることができます。

（注） （バージョン 7.4.1 以降が必要）製品をアップグレードすることなくコンテンツの更新へのアクセスを有効にすることはできますが、その逆（コンテンツのない製品）はお勧めできません。つまり、カスタムユーザーロールで [製品のアップグレード（Product Upgrades）] を有効にする場合は、[コンテンツの更新（Content Updates）] も有効にしてください。そうしないと、アップグレードパッケージを手動でアップロードしたり、古い ASA FirePOWER および NGIPSv デバイスをアップグレードしたりする際に問題が発生する可能性があります。

手順

ステップ 1 システム（⚙） > **[ユーザー（Users）]**を選択します。

ステップ 2 [ユーザー ロール（User Roles）] をクリックします。

ステップ 3 次のいずれかの方法で新しいユーザー ロールを追加します。

- [ユーザ ロールの作成（Create User Role）] をクリックします。
- コピーするユーザ ロールの横にある[コピー（Copy）]（  ）をクリックします。
- 別のManagement Centerからカスタムユーザーロールをインポートします。
  1. 別のManagement Centerで、 をクリックしてロールをコンピュータに保存します。
  2. 新しいManagement Centerで、**システム**（）> **[ツール（Tools）]** > **[インポート/エクスポート（Import/Export）]** を選択します。
  3. [パッケージのアップロード（Upload Package）] をクリックし、指示に従って保存したユーザーロールを新しいManagement Centerにインポートします。

ステップ 4 新しいユーザ ロールの [名前（Name）] を入力します。ユーザ ロール名では、大文字と小文字が区別されます。

ステップ 5 （任意） [説明（Description）] を追加します。

ステップ 6 新しいロールの [メニューベースのアクセス許可（Menu-Based Permissions）] を選択します。

アクセス許可を選択すると、その下位にあるアクセス許可もすべて選択され、複数値を持つアクセス許可では最初の値が使用されます。上位のアクセス許可をクリアすると、下位のアクセス許可もすべてクリアされます。アクセス許可を選択しても、下位のアクセス許可を選択しない場合、アクセス許可がイタリックのテキストで表示されます。

カスタム ロールのベースとして使用する事前定義ユーザ ロールをコピーすると、その事前定義ロールに関連付けられているアクセス許可が事前選択されます。

カスタムユーザー ロールに制限付き検索を適用できます。これらの検索では、[分析（Analysis）] メニューの下にあるテーブルやページでユーザが確認できるデータが制限されます。制限付き検索を設定するには、最初に、プライベートの保存済み検索を作成し、該当するメニューベースのアクセス許可の下で [制限付き検索（Restrictive Search）] ドロップダウン メニューからその検索を選択します。

ステップ 7 （任意） 新しいロールのデータベースアクセス権限を設定するには、[外部データベースアクセス（読み取り専用）（External Database Access (Read Only)）] チェックボックスをオンにします。

このオプションにより、JDBC SSL接続に対応しているアプリケーションを用いて、データベースに対して読み取り専用アクセスが可能になります。Management Centerの認証を行うサードパーティのアプリケーションについては、システム設定内でデータベースアクセスを有効にする必要があります。

ステップ 8 （任意） 新しいユーザー ロールのエスカレーション権限を設定するには、「ユーザ ロール エスカレーションの有効化 （234 ページ）」を参照してください。

ステップ 9 [保存（Save）] をクリックします。
カスタムロールが保存されます。読み取り専用ロールであるとシステムが判断した場合は、そのロールに「(Read Only)」というラベルが付けられます。これは、読み取り専用ユーザーと読み取り/書き込みユーザーの同時セッション数を設定する場合に関連します。「(Read Only)」を

ロール名に手動で追加してロールを読み取り専用にすることはできません。同時セッション制限の詳細については、ユーザーの設定 （125 ページ）を参照してください。

例

アクセス コントロール関連機能のカスタム ユーザ ロールを作成して、ユーザのアクセス コントロールおよび関連付けられたポリシーの表示、変更権限の有無を指定できます。

次の表に、侵入設定を除くアクセス コントロール ポリシーのすべての側面を設定できる必要があるネットワーク管理者と、侵入関連機能のみを設定できる必要がある侵入管理者を区別する方法を示します。[脅威設定の変更（Modify Threat Configuration）] 権限では、侵入ポリシー、変数セット、およびルール内のファイルポリシー、ネットワーク分析および侵入ポリシーの詳細オプションの設定、アクセス コントロール ポリシーのセキュリティ インテリジェンス ポリシーの設定、およびポリシーのデフォルトアクションの侵入アクションを選択できます。[残りのアクセス コントロール ポリシー設定の変更（Modify Remaining Access Control Policy Configuration）] 権限は、ポリシーとルールの他のすべての側面（作成と削除を含む）をカバーします。この例では、ポリシー承認者（Policy Approver）はアクセス コントロール ポリシーと侵入ポリシーの表示が可能です（変更はできません）。また、ポリシー承認者は設定の変更をデバイスに展開することもできます。

表 *5*: アクセス制御のカスタムロールのサンプル

メニューベースのアクセス許可	ロールの例		
	アクセス制御エディタ	侵入およびネットワーク分析エディタ	ポリシー承認者
アクセス制御	はい	はい	はい
アクセス コントロール ポリシー（Access Control Policy）	はい	はい	はい
アクセス制御ポリシーの変更（Modify Access Control Policy）	いいえ	はい	いいえ
脅威設定の変更	いいえ	はい	いいえ
残りのアクセス コントロール ポリシー設定の変更	はい	いいえ	いいえ
侵入ポリシー	いいえ	はい	はい
侵入ポリシーの変更（Modify Intrusion Policy）	いいえ	はい	いいえ

メニューベースのアクセス許可	ロールの例		
	アクセス制御エディタ	侵入およびネットワーク分析エディタ	ポリシー承認者
設定をデバイスに展開	いいえ	いいえ	はい

ユーザ ロールの非アクティブ化

ロールを非アクティブにすると、そのロールが割り当てられているすべてのユーザーから、そのロールと関連するアクセス許可が削除されます。事前定義ユーザ ロールは削除できませんが、非アクティブにすることができます。

マルチドメイン展開では、現在のドメインで作成されたカスタムユーザロールが表示されます。これは編集できます。先祖ドメインで作成されたカスタムユーザロールも表示されますが、これは編集できません。下位のドメインのカスタムユーザロールを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 システム（⚙） > **[ユーザー（Users）]**を選択します。

ステップ 2 [ユーザー ロール（User Roles）] をクリックします。

ステップ 3 アクティブまたは非アクティブにするユーザー ロールの横にあるスライダをクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

Lights-Out Management を含むロールが割り当てられているユーザーがログインしているときに、このロールを非アクティブにしてから再度アクティブにする場合、またはユーザーのログイン セッション中にバックアップからユーザーまたはユーザー ロールを復元する場合、そのユーザーは Web インターフェイスに再度ログインして、IPMItool コマンドへのアクセスを再度取得する必要があります。

ユーザ ロール エスカレーションの有効化

カスタム ユーザ ロールにアクセス許可を付与し、パスワードを設定することで、ベース ロールの特権に加え、他のターゲット ユーザ ロールの特権を一時的に取得できます。この機能により、あるユーザーが不在であるときにそのユーザーを別のユーザーに容易に置き換えることや、拡張ユーザー特権の使用状況を緊密に追跡することができます。デフォルトのユーザ ロールでは、エスカレーションはサポートされません。

たとえば、ユーザのベース ロールに含まれている特権が非常に限られている場合、そのユーザは管理アクションを実行するために管理者ロールにエスカレーションできます。ユーザーが各

自のパスワードを使用するか、または指定された別のユーザーのパスワードを使用することができるように、この機能を設定できます。2番目のオプションでは、該当するすべてのユーザーのための 1 つのエスカレーション パスワードを容易に管理できます。

ユーザ ロール エスカレーションを設定するには、次のワークフローを参照してください。

手順

ステップ 1 エスカレーション ターゲット ロールの設定 （235ページ）。エスカレーション ターゲット ロールにすることができるユーザ ロールは一度に 1 つだけです。

ステップ 2 エスカレーション用のカスタム ユーザー ロールの設定 （235 ページ）。

ステップ 3 （ログイン後のユーザーの場合）ユーザー ロールのエスカレーション （236 ページ）

エスカレーション ターゲット ロールの設定

各自のユーザー ロール（事前定義またはカスタム）をシステム全体でのエスカレーション ターゲット ロールとして機能するように割り当てることができます。これは、カスタム ロールのエスカレーション先となるロールです（エスカレーションが可能な場合）。エスカレーション ターゲット ロールにすることができるユーザ ロールは一度に 1 つだけです。各エスカレーションはログイン セッション期間中保持され、監査ログに記録されます。

手順

ステップ 1 システム（⚙） > **[ユーザー（Users）]**を選択します。

ステップ 2 [ユーザー ロール（User Roles）] をクリックします。

ステップ 3 [アクセス許可エスカレーションの設定（Configure Permission Escalation）] をクリックします。

ステップ 4 [エスカレーション ターゲット（Escalation Target）] ドロップダウン リストからユーザ ロールを選択します。

ステップ 5 [OK] をクリックして変更を保存します。

エスカレーション ターゲット ロールの変更は即時に反映されます。エスカレーションされたセッションのユーザーには、新しいエスカレーション ターゲットのアクセス許可が付与されます。

エスカレーション用のカスタム ユーザー ロールの設定

エスカレーションを有効にするユーザーは、エスカレーションを有効にしたカスタム ユーザー ロールに属している必要があります。この手順では、カスタム ユーザー ロールのエスカレーションを有効にする方法について説明します。

カスタム ロールのエスカレーション パスワードを設定するときには、部門のニーズを考慮してください。多数のエスカレーションユーザを容易に管理するには、別のユーザを選択し、そのユーザのパスワードをエスカレーション パスワードとして使用することができます。そのユーザのパスワードを変更するか、またはそのユーザを非アクティブにすると、そのパスワードを必要とするすべてのエスカレーションユーザが影響を受けます。この操作により、特に一元管理できる外部認証ユーザを選択した場合に、ユーザ ロール エスカレーションをより効率的に管理できます。

始める前に

「エスカレーション ターゲット ロールの設定 （235 ページ）」に従って対象ユーザー ロールを設定します。

手順

ステップ 1 「カスタム ユーザー ロールの作成 （231 ページ）」の説明に従って、カスタム ユーザー ロールの設定を開始します。

ステップ 2 [システム権限（System Permissions）] で、[このロールをエスカレーションする：メンテナンスユーザー（Set this role to escalate to: Maintenance User）] チェックボックスをオンにします。

現在のエスカレーション ターゲット ロールは、チェックボックスの横に表示されます。

ステップ 3 このロールがエスカレーションするときに使用するパスワードを選択します。次の2つの対処法があります。

- このロールを持つユーザがエスカレーション時に自分のパスワードを使用するようにするには、[割り当てられたユーザのパスワードを使用して認証（Authenticate with the assigned user's password）] を選択します。
- このロールを持つユーザが別のユーザのパスワードを使用するようにするには、[指定したユーザのパスワードを使用して認証（Authenticate with the specified user's password）] を選択して、そのユーザ名を入力します。

  （注） 別のユーザのパスワードで認証するときには、任意のユーザ名（非アクティブなユーザまたは存在しないユーザを含む）を入力できます。エスカレーションにパスワードが使用されるユーザを非アクティブにすると、そのパスワードを必要とするロールが割り当てられているユーザのエスカレーションが不可能になります。この機能を使用して、必要に応じてエスカレーション機能をただちに削除できます。

ステップ 4 [保存（Save）] をクリックします。

ユーザー ロールのエスカレーション

エスカレーション権限のあるカスタム ユーザー ロールを割り当てられたユーザーは、いつでもターゲット ロールの権限にエスカレーションできます。エスカレーションはユーザー設定に影響しないことに注意してください。

手順

ステップ 1 ユーザー名の下にあるドロップダウン リストから、[アクセス許可のエスカレーション（Escalate Permissions）] を選択します。

このオプションが表示されない場合は、管理者はユーザ ロールのエスカレーションを有効にしていません。

ステップ 2 認証パスワードを入力します。

ステップ 3 [エスカレーション（Escalate）] をクリックします。これで、現行ロールに加え、エスカレーション ターゲット ロールのすべてのアクセス許可が付与されました。

エスカレーションはログイン セッションの残り期間にわたって保持されます。ベース ロールの特権だけに戻すには、ログアウトしてから新しいセッションを開始する必要があります。

LDAP 認証接続のトラブルシューティング

LDAP 認証オブジェクトを作成したが、選択したサーバーへの接続が失敗したか、または必要なユーザーのリストが取得されなかった場合は、そのオブジェクトの設定を調整できます。

接続のテストで接続が失敗する場合は、設定のトラブルシューティングに関する次の推奨手順を試してください。

- Web インターフェイス画面上部とテスト出力に示されるメッセージから、問題の原因となっているオブジェクトの部分を確認します。
- オブジェクトに使用したユーザー名とパスワードが有効であることを確認します。
  - サードパーティの LDAP ブラウザを使用して LDAP サーバーに接続し、ベース識別名に示されているディレクトリを参照する権限があることを確認します。
  - ユーザー名が、LDAP サーバーのディレクトリ情報ツリーで一意であることを確認します。
  - テスト出力に LDAP バインド エラー 49 が示される場合は、ユーザのユーザ バインディングが失敗しています。サードパーティ アプリケーションを使用してサーバ認証を試行し、その接続でも同様にバインディングが失敗するかどうかを確認します。
- サーバを正しく指定していることを確認します。
  - サーバの IP アドレスまたはホスト名が正しいことを確認します。
  - ローカル アプライアンスから、接続する認証サーバに TCP/IP でアクセスできることを確認します。
  - サーバへのアクセスがファイアウォールによって妨げられないこと、およびオブジェクトで設定されているポートがオープンしていることを確認します。

- 証明書を使用してTLSまたはSSL経由で接続する場合は、証明書のホスト名が、サーバーに使用されているホスト名と一致している必要があります。
- CLIアクセスを認証する場合は、サーバー接続にIPv6アドレスを使用していないことを確認します。
- サーバ タイプのデフォルトを使用している場合は、正しいサーバ タイプであることを確認し、[デフォルトを設定（Set Default）] をもう一度クリックしてデフォルト値をリセットします。

- ベース識別名を入力した場合は、[DNを取得（Fetch DNs）] をクリックし、サーバーで使用可能なすべてのベース識別名を取得し、リストから名前を選択します。
- フィルタ、アクセス属性、または詳細設定を使用している場合は、それぞれが有効であり正しく入力されていることを確認します。
- フィルタ、アクセス属性、または詳細設定を使用している場合は、各設定を削除し、設定なしでオブジェクトをテストしてみます。
- 基本フィルタまたはCLIアクセスフィルタを使用している場合は、フィルタがカッコで囲まれていて、有効な比較演算子を使用していることを確認します（囲み用のカッコを含めて最大 450 文字）。
- より制限された基本フィルタをテストするには、特定のユーザーだけを取得するため、フィルタにそのユーザーのベース識別名を設定します。
- 暗号化接続を使用する場合：
  - 証明書のLDAPサーバの名前が、接続に使用するホスト名と一致していることを確認します。
  - 暗号化されたサーバ接続で IPv6 アドレスを使用していないことを確認します。
- テストユーザを使用する場合、ユーザ名とパスワードが正しく入力されていることを確認します。
- テストユーザーを使用する場合、ユーザー資格情報を削除してオブジェクトをテストします。
- LDAP サーバーに接続し、次の構文を使用して、使用しているクエリをテストします。

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

たとえば、`domainadmin@myrtle.example.com` ユーザーと基本フィルタ (`cn=*`) を使用して `myrtle.example.com` のセキュリティ ドメインに接続する場合は、次のステートメントを使用して接続をテストできます。

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
```

```
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

接続のテストが正常に完了したが、プラットフォーム設定ポリシーの適用後に認証が機能しない場合は、使用する認証とオブジェクトの両方が、デバイスに適用されるプラットフォーム設定ポリシーで有効になっていることを確認します。

正常に接続したが、接続で取得されたユーザーリストを調整する必要がある場合は、基本フィルタまたはCLIアクセスフィルタを追加または変更するか、ベースDNをさらに制限するか制限を緩めて使用することができます。

Active Directory（AD）サーバーへの接続を認証しているときに、ADサーバーへの接続が成功しても、接続イベントログにブロックされたLDAPトラフィックが示されることはほとんどありません。この不正な接続ログは、ADサーバーが重複したリセットパケットを送信したときに発生します。脅威に対する防御デバイスは、2番目のリセットパケットを新しい接続要求の一部として識別し、ブロックアクションを使用して接続をログに記録します。

ユーザー設定の指定

ユーザーロールに応じて、ユーザーアカウントの特定の設定を指定できます。

マルチドメイン展開では、ユーザー設定は、アカウントでアクセスできるすべてのドメインに適用されます。ホームページ設定とダッシュボード設定を指定した場合、特定のページとダッシュボードウィジェットがドメインから制約を受けることに留意してください。

パスワードの変更

すべてのユーザーアカウントはパスワードで保護されています。パスワードはいつでも変更することができ、ユーザアカウントの設定によっては定期的にパスワードを変更しなければならない場合もあります。

パスワード強度チェックが有効になっている場合、パスワードは、Management Centerのユーザーアカウントの注意事項と制約事項（145ページ）で説明されている強力なパスワードの要件に従う必要があります。

LDAPまたはRADIUSユーザーの場合、Webインターフェイスを介してパスワードを変更することはできません。

手順

ステップ1 ユーザ名の下にあるドロップダウンリストから、[ユーザ設定（User Preferences）]を選択します。

ステップ2 [パスワードの変更]をクリックします。

ステップ3 必要に応じて、[パスワードの表示（Show password）]チェックボックスをオンにして、このダイアログの使用中にパスワードを確認します。

ステップ4 [現在のパスワード（Current Password）]フィールドに入力します。

ステップ 5 次の 2 つの対処法があります。

- [新しいパスワード（New Password）] と [パスワードの確認（Confirm Password）] に新しいパスワードを入力します。
- [パスワードの生成（Generate Password）] をクリックして、リストされた条件に準拠したパスワードをシステムで作成します（生成されるパスワードはニーモニックではありません。このオプションを選択した場合は、念のためにパスワードをメモしてください）。

ステップ 6 [Apply] をクリックします。

失効パスワードの変更

ユーザー アカウントの設定によっては、パスワードが期限切れになることがあります。パスワードの有効期間は、アカウントが作成されたときに設定されます。パスワードが期限切れになった場合、[パスワードの有効期限の警告（Password Expiration Warning）] ページが表示されます。

手順

パスワードの有効期限の警告のページには 2 つの選択肢があります。

- すぐにパスワードを変更するには、[パスワードの変更（Change Password）] をクリックします。残りの警告日数がゼロの場合は、パスワードを変更する**必要があります**。

  ヒント パスワード強度チェックが有効になっている場合、パスワードは、Management Center のユーザーアカウントの注意事項と制約事項（145 ページ）で説明されている強力なパスワードの要件に従う必要があります。

- 後でパスワードを変更するには、[後で（Skip）] をクリックします。

Web インターフェイス表示の変更

Web インターフェイスの表示方法を変更できます。

手順

ユーザー名の下にあるドロップダウンリストから、テーマを選択します。

- **低**
- **Dusk**

- **Classic** （バージョン 6.6 以前の外観と操作性）

ホームページの指定

Webインターフェイス内のページをアプライアンスのホームページに指定できます。ダッシュボードへのアクセス権がないユーザーアカウント（外部データベースユーザーなど）を除いて、デフォルトのホームページは、デフォルトダッシュボード（**[概要（Overview）]** > **[ダッシュボード（Dashboards）]**）です（デフォルト ダッシュボードの設定については、「デフォルト ダッシュボードの指定 （247 ページ）」を参照してください）。

マルチドメイン環境では、選択したデフォルトのホームページは、ユーザーアカウントがアクセスできるすべてのドメインに適用されます。複数のドメインに頻繁にアクセスするアカウントのホームページを選択する際、特定のページはグローバル ドメインに制限されることに注意してください。

手順

ステップ 1 ユーザ名の下にあるドロップダウン リストから、[ユーザ設定（User Preferences）] を選択します。

ステップ 2 [ホームページ（Home Page）] をクリックします。

ステップ 3 ホーム ページとして使用するページをドロップダウン リストから選択します。

ドロップダウン リスト内のオプションは、ユーザ アカウントのアクセス権限に基づいて表示されます。詳細については、ユーザの役割 （141 ページ）を参照してください。

ステップ 4 **[保存（Save）]** をクリックします。

イベント ビューの設定

[イベント ビュー設定（Event View Settings）] ページを使用して、Management Center のイベント ビューの特性を設定します。イベント ビュー設定は、特定のユーザ ロールでのみ使用可能であることに注意してください。External Database User ロールを持つユーザは、イベント ビュー設定のユーザインターフェイスの一部を表示できますが、それらの設定を変更しても意味のある結果は生じません。

手順

ステップ 1 ユーザ名の下にあるドロップダウン リストから、[ユーザ設定（User Preferences）] を選択します。

ステップ 2 [イベント ビュー設定（Event View Settings）] をクリックします。

ステップ 3 [イベント設定（Event Preferences）] セクションで、イベントビューの基本特性を設定します。イベント ビュー設定 （242 ページ）を参照してください。

ステップ 4 [ファイル設定（File Preferences）] セクションで、ファイルダウンロードを設定します。ファイル ダウンロード設定 （243 ページ）を参照してください。

ステップ 5 [デフォルト時間帯（Default Time Windows）] セクションで、デフォルトの時間帯を設定します。デフォルト時間枠 （244 ページ）を参照してください。

ステップ 6 [デフォルトワークフロー（Default Workflow）] セクションで、デフォルトワークフローを設定します。デフォルト ワークフロー （246 ページ）を参照してください。

ステップ 7 [保存（Save）] をクリックします。

イベント ビュー設定

[イベントビュー設定（Event View Settings）] ページの [イベント設定（Event Preferences）] セクションを使用して、イベントビューの基本特性を設定します。このセクションはすべてのユーザ ロールで使用可能ですが、イベントを表示できないユーザには、ほとんどまたはまったく意味がありません。

以下のフィールドが [イベント設定（Event Preferences）] セクションに表示されます。

- [「すべて」の操作を確認（Confirm “All” Actions）] フィールドは、イベント ビューのすべてのイベントに影響を与える操作について、アプライアンスがユーザーに確認を要求するかどうかを制御します。

  たとえば、この設定が有効な状態でイベント ビューの [すべて削除（Delete All）] をクリックした場合、アプライアンスがデータベースからこれらを削除する前に、現在の制約を満たすすべてのイベント（現在のページに表示されていないイベントを含む）を削除することをユーザーが確認する必要があります。

- [IP アドレスの解決（Resolve IP Addresses）] フィールドを使用すると、可能な場合には常に、アプライアンスで IP アドレスの代わりにホスト名がイベント ビューに表示されるようになります。

  多数の IP アドレスが含まれている場合、このオプションを有効にすると、イベント ビューの表示に時間がかかる可能性があることに注意してください。また、この設定を有効にするには、管理インターフェイス設定を使用して、システム設定で DNS サーバを確立する必要があることにも注意してください。

- [パケット ビューの展開（Expand Packet View）] フィールドでは、侵入イベントのパケット ビューをどのように表示するかを設定できます。デフォルトでは、アプライアンスによるパケット ビューの表示は折りたたまれた状態になっています。

  - [なし（None）] : パケット ビューの [パケット情報（Packet Information）] セクションのサブセクションをすべて折りたたんだ状態にします。
  - [パケット テキスト（Packet Text）] : [パケット テキスト（Packet Text）] サブセクションだけを展開します。

- [パケット バイト（Packet Bytes）]：[パケット バイト（Packet Bytes）] サブセクションだけを展開します。
- [すべて（All）]：すべてのセクションを展開します。

デフォルト設定に関係なく、パケット ビューのセクションを手動で展開することで、キャプチャされたパケットに関する詳細情報を常に表示することができます。

- [1 ページあたりの行数（Rows Per Page）] フィールドは、ドリル ダウン ページとテーブル ビューに表示する、ページごとのイベントの行数を制御します。
- [更新間隔（Refresh Interval）] フィールドは、イベント ビューの更新間隔を分単位で設定します。「0」を入力すると、更新オプションが無効になります。この間隔はダッシュボードに適用されないことに注意してください。
- [統計情報の更新間隔（Statistics Refresh Interval）] は、[侵入イベント統計（Intrusion Event Statistics）] や [ディスカバリ統計（Discovery Statistics）] ページなどのイベントのサマリー ページの更新間隔を制御します。「0」を入力すると、更新オプションが無効になります。この間隔はダッシュボードに適用されないことに注意してください。
- [ルールの非アクティブ化（Deactivate Rules）] フィールドは、標準テキスト ルールによって生成される侵入イベントのパケット ビューに、どのリンクを表示させるかを次のように制御します。
  - [すべてのポリシー（All Policies）]：すべてのローカルで定義されたカスタム侵入ポリシーで標準テキスト ルールを非アクティブにする単一リンク
  - [現在のポリシー（Current Policy）]：現在展開中の侵入ポリシーだけで標準テキスト ルールを非アクティブにする単一リンク。デフォルトのポリシーのルールは非アクティブにできないことに注意してください。
  - [質問（Ask）]：これらの個々のオプションへのリンク

パケット ビューでこれらのリンクを表示するには、Administrator または Intrusion Admin のアクセス権があるユーザー アカウントが必要です。

ファイル ダウンロード設定

[イベント ビュー設定（Event View Settings）] ページの [ファイル設定（File Preferences）] セクションを使用して、ローカル ファイル ダウンロードの基本特性を設定します。このセクションは、Administrator、Security Analyst、または Security Analyst（読み取り専用）ユーザー ロールを持つユーザーのみが利用できます。

キャプチャされたファイルのダウンロードをアプライアンスがサポートしていない場合、これらのオプションは無効になることに注意してください。

以下のフィールドが [ファイル設定（File Preferences）] セクションに示されます。

- [「ファイルのダウンロード」アクションを確認する（Confirm 'Download File' Actions）] チェックボックスは、ファイルをダウンロードするたびに [ファイル ダウンロード（File

Download）]ポップアップ ウィンドウが表示され、警告が示されて続行するかキャンセルするかを選択するためのプロンプトが出されるようにするかどうかを制御します。

⚠

注意 有害な結果が発生することがあるため、マルウェアをダウンロード**しない**ように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先を保護するために必要な予防措置を行っていることを確認します。

ファイルをダウンロードする際には、いつでもこのオプションを無効にできることに注意してください。

- キャプチャされたファイルをダウンロードすると、そのファイルを含むパスワード保護された .zip アーカイブがシステムによって作成されます。[zip ファイル パスワード（Zip File Password）] フィールドは、.zip ファイルへのアクセスを制限するためにユーザーが使用するパスワードを定義します。このフィールドを空欄にすると、パスワードなしのアーカイブ ファイルがシステムによって作成されます。
- [Zip ファイル パスワードの表示（Show Zip File Password）] チェック ボックスで、[Zip ファイルのパスワード（Zip File Password）] フィールドにプレーン テキストを表示するか不明瞭な文字を表示するかを切り替えます。このフィールドをオフにすると、[zip ファイル パスワード（Zip File Password）] には不明瞭な文字が表示されます。

デフォルト時間枠

時間枠（時間範囲と呼ばれることもある）は、任意のイベント ビューでイベントに時間制約を課します。[イベント ビュー設定（Event View Settings）] ページの [デフォルト時間枠（Default Time Windows）] セクションを使用して、時間枠のデフォルトの動作を制御します。

このセクションへのユーザ ロール アクセスは以下のとおりです。

- Administrators と Maintenance Users は、セクション全体にアクセスできます。
- Security Analysts と Security Analysts（読み取り専用）は、[監査ログの時間枠（Audit Log Time Window）] 以外のすべてのオプションにアクセスできます。
- Access Admins、Discovery Admins、External Database Users、Intrusion Admins、Network Admins、および Security Approvers は、[イベントの時間枠（Events Time Window）] オプションにのみアクセスできます。

デフォルトの時間枠設定に関係なく、イベントの分析中にはいつでも手動で個別のイベント ビューの時間枠を変更できます。また、時間枠の設定は、現在のセッションにだけ有効であることにも注意してください。ログアウトしてから再びログインすると、時間枠は、このページで設定したデフォルトにリセットされます。

以下のように、デフォルトの時間枠を設定できる 3 つのタイプのイベントがあります。

- [イベントの時間枠（Events Time Window）] は、時間で制約できるほとんどのイベントのために単一のデフォルトの時間枠を設定します。
- [監査ログの時間枠（Audit Log Time Window）] は、監査ログ用のデフォルトの時間枠を設定します。
- [ヘルス モニタリングの時間枠（Health Monitoring Time Window）] は、ヘルス イベント用のデフォルトの時間枠を設定します。

時間枠は、ユーザ アカウントがアクセスできるイベント タイプにのみ設定できます。すべてのユーザ タイプは、イベントの時間枠を設定できます。Administrators、Maintenance Users、および Security Analysts は、ヘルス モニタリングの時間枠を設定できます。Administrators と Maintenance Users は、監査ログの時間枠を設定できます。

すべてのイベントビューが時間で制約できるとは限らないので、時間枠の設定によって、ホスト、ホスト属性、アプリケーション、クライアント、脆弱性、ユーザーの ID、コンプライアンス allow リスト違反を表示するイベントビューは影響を受けないことに注意してください。

複数の時間枠を使用して、上記の各タイプのイベントに 1 つずつ適用するか、または**単一の**時間枠を使用して、それをすべてのイベントに適用することができます。単一の時間枠を使用すると、3 つのタイプの時間枠用の設定が非表示になり、新しく [グローバルな時間枠（Global Time Window）] 設定が表示されます。

以下の 3 つのタイプの時間枠があります。

- [静的（static）]：特定の開始時刻から特定の終了時刻までに生成されたすべてのイベントを表示します
- [拡張（expanding）]：特定の開始時刻から現在までに生成されたすべてのイベントを表示します。時間の進行と共に時間枠が拡張され、新しいイベントがイベント ビューに追加されます。
- [スライド（sliding）]：特定の開始時刻（たとえば 1 日前）から現在までに生成されたすべてのイベントを表示します。時間の進行と共に時間枠は「スライド」し、設定した範囲内（この例では直前の 1 日）のイベントだけが表示されます。

すべての時間枠の最大時間範囲は、1970 年 1 月 1 日午前 0 時（UTC）～ 2038 年 1 月 19 日午前 3 時 14 分 7 秒です。

次のオプションは、[時間枠の設定（Time Window Settings）] ドロップダウン リストに表示されます。

- [最後を表示 - スライディング（Show the Last - Sliding）] オプションにより、指定した長さのスライドするデフォルトの時間枠を設定できます。

  アプライアンスは、特定の開始時刻（たとえば 1 時間前）から現在までに生成されたすべてのイベントを表示します。イベント ビューの変更と共に、時間枠は「スライド」して、常に最後の 1 時間内のイベントが表示されます。
- [最後を表示（静的/拡張）（Show the Last - Static/Expanding）]：このオプションで、指定した長さのデフォルトの時間枠を静的または拡張のどちらかに設定できます。

静的時間枠の場合は、[終了時刻を使用（Use End Time）] チェック ボックスをオンにします。アプライアンスは、特定の開始時間（1 時間前など）から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

拡張時間枠にするには、[終了時刻を使用（Use End Time）] チェック ボックスをオフにします。アプライアンスは、特定の開始時刻（たとえば 1 時間前）から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。

- [現在の日付（静的/拡張）（Current Day - Static/Expanding）]：このオプションで、現在の日付のデフォルトの時間枠を静的または拡張のどちらかに設定できます。現在の日付は、現行セッションのタイム ゾーン設定に基づいて午前 0 時に始まります。

  静的時間枠の場合は、[終了時刻を使用（Use End Time）] チェック ボックスをオンにします。アプライアンスは、午前 0 時からユーザがイベントを初めて確認した時刻までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

  拡張時間枠にするには、[終了時刻を使用（Use End Time）] チェック ボックスをオフにします。アプライアンスは、午前 0 時から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に 24 時間を超えて分析を続けた場合、この時間枠は 24 時間よりも長くなる可能性があることに注意してください。

- [現在の週（静的/拡張）（Current Week - Static/Expanding）]：このオプションで、現在の週のデフォルトの時間枠を静的または拡張のどちらかに設定できます。現在の週は、現行セッションのタイム ゾーン設定に基づいて直前の日曜日の午前 0 時に始まります。

  静的時間枠の場合は、[終了時刻を使用（Use End Time）] チェック ボックスをオンにします。アプライアンスは、午前 0 時からユーザがイベントを初めて確認した時刻までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

  拡張時間枠にするには、[終了時刻を使用（Use End Time）] チェック ボックスをオフにします。アプライアンスは、日曜日の午前 0 時から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に 1 週間を超えて分析を続けた場合、この時間枠は 1 週間よりも長くなる可能性があることに注意してください。

デフォルト ワークフロー

ワークフローは、アナリストがイベントの評価に使用するデータが示された一連のページです。アプライアンスには、各イベント タイプに少なくとも 1 つの定義済みのワークフローが付属しています。たとえば、セキュリティ アナリストの場合、実行する分析のタイプに応じて、それぞれが侵入イベントのデータを別の形式で示している、10 の異なる侵入イベントのワークフローから選択できます。

アプライアンスには、イベント タイプごとにデフォルト ワークフローが設定されます。たとえば、[優先順位および分類に基づいたイベント（Events by Priority and Classification）] ワークフローが、侵入イベントのデフォルトになります。つまり、侵入イベント（確認済みの侵入イベントを含む）を表示するたびに、アプライアンスは [優先順位および分類に基づいたイベント（Events by Priority and Classification）] ワークフローを表示します。

ただし、イベント タイプごとにデフォルト ワークフローは変更できます。設定可能なデフォルトのワークフローは、ユーザ ロールによって異なります。たとえば、侵入イベントのアナリストがデフォルトのディスカバリ イベント ワークフローを設定することはできません。

デフォルト タイム ゾーンの設定

この設定は、タスクスケジュールやダッシュボードの表示などについて、自分のユーザーアカウントの Web インターフェイスにのみ表示される時間を決定します。この設定は、システム時刻を変更したり、他のユーザーに影響を与えたりせず、システムに保存されているデータ（通常は UTC を使用）にも影響を与えません。

警告 タイムゾーン機能（[ユーザー設定（User Preferences）]）は、システムクロックが UTC 時間に設定されていることを前提としています。システム時刻を変更しようとしないでください。システム時刻の UTC からの変更はサポートされていません。また、システム時刻を変更した場合はデバイスを再イメージ化してサポートされていない状態から回復させる必要があります。

（注） この機能は、時間ベースのポリシーの適用に使用されるタイムゾーンには影響しません。[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] でデバイスのタイムゾーンを設定します。

手順

ステップ 1 ユーザ名の下にあるドロップダウン リストから、[ユーザ プリファレンス（User Preferences）] を選択します。

ステップ 2 [タイムゾーン（Time Zone）] ドロップダウンをクリックします。

ステップ 3 使用するタイムゾーンを含む大陸または地域を選択します。

ステップ 4 使用するタイムゾーンに対応する国と州の名前を選択します。

デフォルト ダッシュボードの指定

[概要（Overview）] > [ダッシュボード（Dashboards）] を選択すると、デフォルトのダッシュボードが表示されます。変更しない限り、すべてのユーザーのデフォルトダッシュボードは、

[サマリー（Summary）] ダッシュボードです。ユーザーロールが管理者、メンテナンス、またはセキュリティアナリストの場合は、デフォルトダッシュボードを変更できます。

マルチドメイン環境では、選択したデフォルトのダッシュボードは、ユーザーアカウントがアクセスできるすべてのドメインに適用されます。複数のドメインに頻繁にアクセスするアカウントのダッシュボードを選択する際、ドメインが特定のダッシュボードウィジェットを制限することに注意してください。

手順

ステップ 1 ユーザ名の下にあるドロップダウン リストから、[ユーザ設定（User Preferences）] を選択します。

ステップ 2 [ダッシュボード設定（Dashboard Settings）] をクリックします。

ステップ 3 デフォルトとして使用するダッシュボードをドロップダウン リストから選択します。

ステップ 4 [保存（Save）] をクリックします。

[How To] の設定の指定

How To は、Management Center 上でタスク間を移動するためのウォークスルーを提供するウィジェットです。ウォークスルーでは、タスクを実行するために移動する必要があるかもしれない各種 UI 画面かどうかを問わず、各ステップを順次体験することでタスクを完遂するために必要なステップを実行します。[How To] ウィジェットはデフォルトで有効になっています。

Management Center でサポートされている機能ウォークスルーのリストについては、「Feature Walkthroughs Supported in Secure Firewall Management Center」を参照してください。

（注）
- 通常、ウォークスルーはすべての UI ページで利用でき、ユーザ ロールは区別されていません。ただし、ユーザーの権限によっては Management Center インターフェイスに表示されないメニュー項目もあります。そのため、そのようなページではウォークスルーは実行されません。
- この機能は、クラシックテーマでは使用できません。

手順

ステップ 1 ユーザ名の下にあるドロップダウン リストから、[ユーザ設定（User Preferences）] を選択します。

ステップ 2 [How Toの設定（How-To Settings）] をクリックします。

ステップ 3 [How Toの有効化（Enable How-To）] チェックボックスをオンにして [How To] を有効にします。

ステップ 4 **[Save（保存）]** をクリックします。

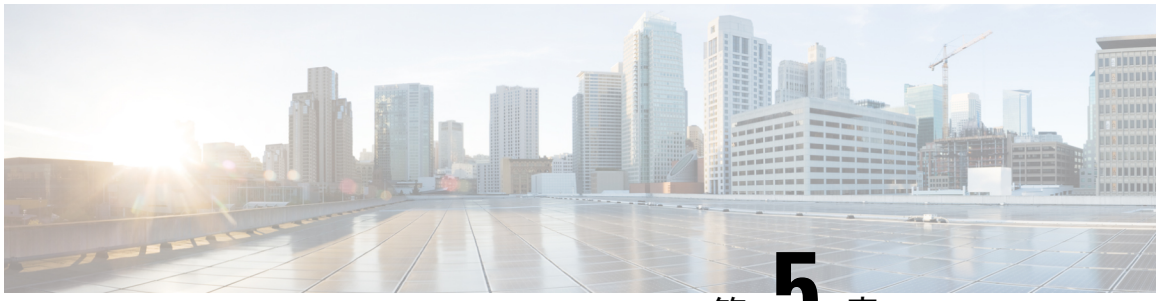
次のタスク

[How To] ウィジェットを開くには、**[ヘルプ（Help）]** > **[How-Tos]**を選択します。関心のあるタスクに対処する How To ウォークスルーを検索できます。詳細については、How To ウォークスルーの検索 （24 ページ）を参照してください。

Management Center ユーザーアカウントの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
アクセスコントロールポリシーとルールを変更するための詳細なアクセス許可。	7.4.0	いずれか	カスタムユーザーロールを定義して、アクセスコントロールポリシーおよびルールの侵入設定と、その他のアクセスコントロールポリシーおよびルールを区別できます。これらのアクセス許可を使用すると、ネットワーク管理チームと侵入管理チームの責任を分離できます。 ユーザーロールを定義するときに、**[ポリシー（Policies）]**>**[アクセス制御（Access Control）]** > **[アクセスコントロールポリシー（Access Control Policy）]** > **[アクセスコントロールポリシーの変更（Modify Access Control Policy）]** > **[脅威設定の変更（Modify Threat Configuration）]**オプションを選択して、侵入ポリシー、変数セット、およびルール内のファイルポリシー、ネットワーク分析および侵入ポリシーの詳細オプションの設定、アクセス コントロール ポリシーのセキュリティ インテリジェンス ポリシーの構成、およびポリシーのデフォルトアクションの侵入アクションを選択できるようにします。[残りのアクセスコントロールポリシー設定の変更（Modify Remaining Access Control Policy Configuration）] を使用して、ポリシーの他のすべての側面を編集する機能を制御できます。アクセス コントロール ポリシーの変更権限を含む既存の事前定義されたユーザーロールは、引き続きすべてのサブ権限をサポートします。詳細な権限を適用する場合は、独自のカスタムロールを作成する必要があります。
シェルユーザー名テンプレートを割り当てるための新しいフィールドの追加。	7.0.0	いずれか	LDAP 外部認証用の CLI アクセス属性のテンプレートを指定するプロビジョニング：シェルユーザー名テンプレートが導入されました。したがって、CLI 属性には、LDAP CLI ユーザーを識別するための独自のテンプレートがあります。 新規/変更された画面： **システム（⚙） > [ユーザー（Users）] > [外部認証（External Authentication）]**

機能	最小 Management Center	最小 Threat Defense	詳細
SAML 2.0 準拠の SSO プロバイダーを使用したシングルサインオンのサポートが追加されました。	6.7.0	いずれか	サードパーティの SAML 2.0 準拠アイデンティティプロバイダー（IdP）で設定された外部ユーザーのシングルサインオンのサポートが追加されました。これには、IdP のユーザーまたはグループロールを Management Center ユーザーロールにマッピングする機能が含まれます。 内部で認証された、または LDAP または RADIUS によって認証された管理ロールを持つユーザーのみが SSO を構成できます。 新規/変更された画面： **システム（⚙）> [ユーザー（Users）] > [シングルサインオン（Single Sign-On）]**
Web インターフェイスのテーマ。	6.6.0	任意（Any）	Web インターフェイスのルックアンドフィールを選択できます。ライトまたは Dusk テーマを選択するか、以前のリリースに登場したクラシックテーマを使用します。 新規/変更された画面： [ユーザー名（User Name）] > [ユーザー設定（User Preferences）] > [一般（General）] > [UIテーマ（UI Theme）]
ユーザーアカウントの名前用に新しいフィールドを追加しました。	6.6.0	任意（Any）	内部ユーザーアカウントを担当するユーザーまたは部門を識別できるフィールドを追加しました。 新規/変更された画面： **システム（⚙）> [ユーザー（Users）] > [ユーザー（Users）]** > [本名（Real Name）] フィールド
Cisco Security Manager シングルサインオンのサポートは終了しました。	6.5.0	いずれか	Management Center と Cisco Security Manager 間のシングルサインオンは、Firepower 6.5 ではサポートされなくなりました。 新規/変更された画面： **システム（⚙）> [ユーザー（Users）]**（[System] > [Users]）> [CSMシングルサインオン（CSM Single Sign-on）]
強化されたパスワードセキュリティ。	6.5.0	いずれか	この章内の 1 箇所に強力なパスワードの新しい要件が記載されるようになり、他の章から相互参照されます。 パスワード変更インターフェイスの追加された新しいフィールド：[パスワードの表示（Show Password）] および [パスワードの生成（Generate Password）] 新規/変更された画面： [ユーザー名（User Name）] > [ユーザー設定（User Preferences）] > [一般（General）] > [パスワードの変更（Change Password）]



第 5 章

ドメイン

次のトピックでは、ドメインを使用してマルチテナンシーを管理する方法について説明します。

ドメインを使用したマルチテナンシーの概要

Management Center では、ドメインを使用したマルチテナンシーを実装できます。ドメインは、管理対象デバイス、構成、およびイベントへのユーザーアクセスをセグメント化します。最上位のグローバルドメインの下に、2 つまたは 3 つのレベルで最大 100 のサブドメインを作成できます。

Management Center にログインすると、現在のドメインと呼ばれる単一ドメインにログインします。ユーザ アカウントによっては、他のドメインに切り替えることができる場合があります。

ユーザーロールによる制限に加えて、現在のドメインレベルによってさまざまな設定の変更が制限される場合もあります。Management Center では、システムソフトウェア更新などのほとんどの管理タスクは、グローバルドメインに制限されます。

Management Center では、その他のタスクは、サブドメインがないドメインであるリーフドメインに制限されます。たとえば、各管理対象デバイスをリーフ ドメインと関連付け、そのリーフ ドメインのコンテキストからデバイス管理タスクを実行する必要があります。各デバイスは単一のドメインにのみ属することができることに注意してください。

各リーフ ドメインは、そのリーフ ドメインのデバイスで集められた検出データに基づいて独自のネットワーク マップを作成します。管理対象デバイスによって報告されたイベント（接続、侵入、マルウェアなど）もデバイスのリーフ ドメインに関連付けられます。

1 ドメイン レベル：グローバル

マルチテナンシーを設定しない場合、すべてのデバイス、構成、およびイベントはグローバルドメインに属します。グローバル ドメインは、このシナリオの場合はリーフ ドメインでもあります。ドメイン管理を除き、サブドメインを追加するまでは、ドメイン固有の構成および分析オプションは非表示になります。

2 ドメイン レベル：グローバル、セカンドレベル

2 レベルのマルチドメイン展開では、グローバル ドメインには直接の子孫ドメインのみがあります。たとえば、マネージド セキュリティ サービス プロバイダー（MSSP）は、1 つの Management Center を使用して複数の顧客のネットワーク セキュリティを管理できます。

- グローバルドメインにログインしている MSSP の管理者は、顧客の展開を表示または編集することはできません。顧客の展開を管理するには、それぞれのセカンドレベルの指定されたサブドメインにログインする必要があります。
- 各顧客の管理者は、サブドメインと呼ばれるセカンドレベルにログインして、その組織に適用されるデバイス、構成、およびイベントのみを管理できます。これらのローカル管理者は、MSSP の他の顧客の展開を表示したり、その環境に影響を与えることはできません。

3 ドメイン レベル：グローバル、セカンドレベル、サードレベル

3 レベルのマルチドメイン展開では、グローバル ドメインにはサブドメインがあり、そのうち少なくとも 1 つに独自のサブドメインがあります。前の例を拡張するには、MSSP 顧客（すでにサブドメインに制限されている）がその展開をさらにセグメント化しようとしているシナリオを考えてみます。この顧客は、2 つのクラスのデバイス（ネットワーク エッジに配置されているデバイスと内部に配置されているデバイス）を個別に管理しようとしています。

- セカンドレベルサブドメインにログインしている顧客の管理者は、顧客のエッジネットワークの展開を表示または編集することはできません。ネットワークエッジで展開されたデバイスを管理するには、それぞれのリーフドメインにログインする必要があります。
- 顧客のエッジ ネットワークの管理者は、サードレベル（リーフ）ドメインにログインして、ネットワーク エッジに展開されているデバイスに適用されるデバイス、構成、およびイベントのみを管理できます。同様に、顧客の内部ネットワークの管理者は、別のサードレベル ドメインにログインして、内部のデバイス、構成、およびイベントを管理できます。エッジと内部の管理者は、互いの展開を表示できません。

（注） マルチテナントを使用する Management Center では、SSO 設定はグローバルドメインレベルでのみ適用でき、グローバルドメインとすべてのサブドメインに適用されます。

関連トピック

SAML シングルサインオンの設定 （169 ページ）

ドメインの用語

このマニュアルでは、ドメインおよびマルチドメイン展開を説明する際に次の用語を使用します。

グローバル ドメイン

マルチドメイン展開でのトップレベル ドメイン。マルチテナンシーを設定しない場合、すべてのデバイス、設定、およびイベントはグローバル ドメインに属します。グローバル ドメインの Administrators は、Cisco Secure Firewall システム全体の導入を管理できます。

サブドメイン

第 2 または第 3 レベルのドメイン。

第 2 レベル ドメイン

グローバル ドメインの子。第 2 レベル ドメインは、リーフ ドメインにするか、サブドメインを持つことができます。

第 3 レベル ドメイン

第 2 レベル ドメインの子。第 3 レベル ドメインは常にリーフ ドメインです。

リーフ ドメイン

サブドメインを持たないドメイン。各デバイスはリーフ ドメインに属している必要があります。

子孫ドメイン

階層の現在のドメインから下のドメイン。

子ドメイン

ドメインの直接子孫。

先祖ドメイン

現在のドメインより上にある同じ系統のドメイン。

親ドメイン

ドメインの直接先祖。

兄弟ドメイン

同じ親を持つドメイン。

現在のドメイン

現在ログインしているドメイン。システムでは、Web インターフェイスの右上のユーザ名の前に現在のドメイン名が表示されます。ユーザー ロールが制限されている場合を除き、現在のドメインの設定を編集できます。

ドメインのプロパティ

ドメインのプロパティを変更するには、そのドメインの親ドメインのAdministratorアクセス権が必要です。

名前（Name）と説明（Description）

各ドメインには、階層内で一意の名前が必要です。説明は任意です。

親ドメイン（Parent Domain）

第2および第3レベルのドメインには親ドメインがあります。ドメインを作成した後にドメインの親を変更することはできません。

デバイス（Devices）

リーフドメインにのみデバイスを含めることができます。つまり、1つのドメインにはサブドメインまたはデバイスを含めることができますが、両方を含めることはできません。非リーフドメインが直接デバイスを制御している展開を保存することはできません。

ドメインエディタで、ドメイン階層の現在の場所に応じて、Webインターフェイスに使用可能な選択されたデバイスが表示されます。

ホスト制限（Host Limit）

Management Centerがモニタでき、ネットワークマップに保存できるホストの数。モデルによって異なります。マルチドメイン展開では、リーフドメインは使用可能なモニタされたホストのプールを共有しますが、個別のネットワークマップを持っています。

各リーフドメインがネットワークマップに値を入力できるように、ホスト制限を各サブドメインレベルで設定できます。ドメインのホスト制限を**0**に設定すると、ドメインは一般的なプールで共有します。

ホスト制限を設定すると、各ドメインレベルで異なる効果があります。

- リーフ：リーフドメインの場合、ホスト制限は単に、リーフドメインがモニタできるホスト数の制限です。
- 第2レベル：第3レベルのリーフドメインを管理する第2レベルのドメインの場合、ホスト制限は、リーフドメインがモニタできるホストの総数を表します。リーフドメインは、使用可能なホストのプールを共有します。
- グローバル：グローバルドメインの場合、ホスト制限は、Management Centerがモニタできるホストの総数に等しくなります。変更することはできません。

サブドメインのホスト制限の合計を、親ドメインのホスト制限より多くすることができます。たとえば、グローバルドメインのホスト制限が150,000の場合、複数のサブドメインを設定して、それぞれのホスト制限を100,000にすることができます。これらのドメインのいずれか（すべてではない）が100,000のホストをモニタできます。

ホスト制限に到達した後に新しいホストを検出すると、ネットワーク検出ポリシーが制御を行います。新しいホストをドロップするか、または長期間非アクティブになっているホストを置換することができます。各リーフドメインには独自のネットワーク検出ポリシー

があるため、各リーフドメインは、システムが新しいホストを検出すると、独自の動作を制御します。

ドメインのホスト制限を軽減した場合に、そのネットワークマップに新しい制限より多くのホストが含まれている場合、システムは最も長い間非アクティブになっているホストを削除します。

関連トピック

ホスト制限（Host Limit）
ネットワーク検出のデータ ストレージ設定

ドメインの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者

ドメインの管理

ドメインのプロパティを変更するには、そのドメインの親ドメインへの管理者アクセス権が必要です。

手順

ステップ 1 システム（⚙） > **[ドメイン（Domains）]**を選択します。

ステップ 2 次のようにドメインを管理します。

- 追加：[ドメインの追加（Add Domain）]をクリックするか、または親ドメインの横にある[サブドメインの追加（Add Subdomain）]をクリックします（新しいドメインの作成（256 ページ） を参照）。
- 編集：変更するドメインの横 **[編集（Edit）]**（✎）をクリックします（ドメインのプロパティ（254 ページ） を参照）。
- 削除：削除する空のドメインの横[削除（Delete）]（🗑）をクリックして、選択内容を確認します。宛先ドメインを編集することによって、削除するドメインからデバイスを移動します。

ステップ 3 ドメイン構造への変更を行い、すべてのデバイスをリーフドメインに関連付けたら、[保存（Save）] をクリックして変更を実行します。

ステップ 4 プロンプトが表示されたら、追加の変更を行います。

- リーフドメインを親ドメインに変更した場合は、古いネットワークマップを移動または削除します（ドメイン間のデータの移動 （257 ページ） を参照）。
- ドメイン間でデバイスを移動し、新しいポリシーおよびセキュリティゾーンまたはインターフェイスグループを割り当てる必要がある場合は、ドメイン間のデバイスの移動 （258 ページ） を参照してください。

次のタスク

- 新しいドメインのユーザロールとポリシー（アクセス制御、ネットワーク検出など）を設定します。必要に応じてデバイスのプロパティを更新します。
- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

新しいドメインの作成

最上位のグローバルドメインの下に、2 つまたは 3 つのレベルで最大 100 のサブドメインを作成できます。

ドメイン設定を実装する前に、リーフ ドメインにすべてのデバイスを割り当てる必要があります。リーフドメインにサブドメインを追加すると、ドメインはリーフドメインではなくなるので、デバイスを再度割り当てる必要があります。

手順

ステップ 1 グローバルまたはセカンドレベルドメインで、**システム**（⚙）>**[ドメイン（Domains）]** を選択します。

ステップ 2 [ドメインの追加（Add Domain）] をクリックするか、または親ドメインの横にある [サブドメインの追加（Add Subdomain）] をクリックします。

ステップ 3 [名前（Name）] と [説明（Description）] に入力します。

ステップ 4 [親ドメイン（Parent Domain）] を選択します。

ステップ 5 [デバイス（Devices）] で、ドメインに追加する [使用可能なデバイス（Available Devices）] を選択し、[ドメインに追加（Add to Domain）] をクリックするか、または [選択されたデバイス（Selected Devices）] のリストにドラッグアンドドロップします。

ステップ 6 必要に応じて、[詳細設定（Advanced）]をクリックして、新しいドメインがモニタできるホスト数を制限します（ドメインのプロパティ （254 ページ） を参照）。

ステップ 7 [保存（Save）] をクリックして、ドメイン管理ページに戻ります。

デバイスが非リーフドメインに割り当てられている場合は、システムによって警告が表示されます。これらのデバイスに新しいドメインを作成するには、[新しいドメインの作成（Create New Domain）] をクリックします。デバイスを既存のドメインに移動する予定がある場合は、[未割り当てのままにする（Keep Unassigned）] をクリックします。

ステップ 8 ドメイン構造への変更を行い、すべてのデバイスをリーフドメインに関連付けたら、[保存（Save）] をクリックして変更を実行します。

ステップ 9 プロンプトが表示されたら、追加の変更を行います。

- リーフドメインを親ドメインに変更した場合は、古いネットワークマップを移動または削除します（ドメイン間のデータの移動 （257 ページ） を参照）。
- ドメイン間でデバイスを移動し、新しいポリシーおよびセキュリティゾーンまたはインターフェイスグループを割り当てる必要がある場合は、ドメイン間のデバイスの移動 （258 ページ） を参照してください。

次のタスク

- 新しいドメインのユーザロールとポリシー（アクセス制御、ネットワーク検出など）を設定します。必要に応じてデバイスのプロパティを更新します。
- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

ドメイン間のデータの移動

イベントおよびネットワークマップがリーフドメインに関連付けられているため、リーフドメインを親ドメインに変更する場合は、2 つの選択肢があります。

- ネットワークマップおよび関連付けられているイベントを新しいリーフドメインに移動します。
- ネットワークマップは削除しますが、イベントは保持します。この場合、システムが必要に応じてまたは設定されているようにイベントをプルーニングするまで、イベントは親ドメインに関連付けられたままとなります。または、古いイベントを手動で削除できます。

始める前に

以前のリーフドメインが現在の親ドメインになるドメイン設定を実行します（ドメインの管理 （255 ページ） を参照）。

手順

ステップ 1 現在は親ドメインである以前の各リーフドメインに対して、次の手順を実行します。

- **親ドメイン**のイベントおよびネットワークマップを継承するには、新しい**リーフドメイン**を選択します。
- 親ドメインのネットワークマップを削除するが、古いイベントは保持する場合は、[なし（None）] を選択します。

ステップ 2 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

ドメイン間のデバイスの移動

デバイスを移動するドメインでソースドメインとターゲットドメインが表示されている限り、ドメイン間でデバイスを移動できます。ドメイン間でデバイスを移動すると、デバイスに適用された設定とポリシーに影響する可能性があります。ドメイン間でデバイスを移動している間、システムは次のデバイス設定を保持します。

- インターフェイス
- インラインセット
- ルーティング
- DHCP
- 関連オブジェクト
- SNMP（利用可能な場合）

デバイスをドメイン間で移動すると、デバイスの設定に次の変更が発生する可能性があります。

- デバイスがターゲットドメインに移動した後もシステムでデバイス設定を保持するには、以下を確認してください。
  - 共有アクセス コントロール ポリシーがグローバルドメインにあること。他の共有ポリシーもグローバルドメイン内に配置することをお勧めします。
- VPN 設定の場合、
  - サイト間 VPN 設定がターゲットドメインにあること。
  - リモートアクセスVPN設定とデバイス証明書は、グローバルドメインまたはターゲットドメインにあります。

- リモート アクセス VPN ポリシーをデバイスに割り当てるときは、ターゲット ドメインがリモート アクセス VPN の設定されているドメインの子孫である場合のみ、ドメイン間でデバイスを移動できます。

- SNMP のネットワークオブジェクトがグローバルドメインにあること。

- デバイスは、デバイス上の登録済み証明書を削除することなく子ドメインに移動できます。具体的には次のとおりです。
  - 移動したデバイスに割り当てられた正常性ポリシーが新しいドメインでアクセス不能の場合、新しい正常性ポリシーを選択できます。
  - 移動したデバイスに割り当てられたアクセス コントロール ポリシーが有効でない場合、または新しいドメインでアクセスできない場合は、新しいポリシーを選択します。すべてのデバイスに、割り当てられたアクセス コントロール ポリシーが必要です。
  - 移動したデバイス上のインターフェイスが、新しいドメインでアクセスできないセキュリティゾーンに属している場合は、新しいゾーンを選択できます。
  - インターフェイスは、以下から削除されます。
    - 新しいドメインでアクセス不能で、アクセス コントロール ポリシーで使用されていないセキュリティゾーン。
    - すべてのインターフェイスグループ。

デバイスでポリシーの更新が必要だが、ゾーン間でインターフェイスを移動する必要がない場合は、ゾーン設定が最新であることを示すメッセージが表示されます。たとえば、デバイスのインターフェイスが共通の先祖ドメインに設定されているセキュリティゾーンに属している場合は、サブドメインからサブドメインにデバイスを移動する場合はゾーン設定を更新する必要はありません。

始める前に

- 新しいドメインを作成します。詳細については、新しいドメインの作成（256ページ）を参照してください。
- デバイスをドメインからドメインに移動し、次に新しいポリシーとセキュリティゾーンを割り当てる必要があるドメイン構成を実装します（ドメインの管理（255ページ）を参照）。

手順

ステップ1 グローバルドメインで、[システム（System）]（⚙）>[ドメイン（Domains）]を選択します。

ステップ2 デバイスを移動する予定のターゲットドメインを編集します。

ステップ 3 [ドメインの編集（Edit Domain）] ダイアログボックスで、次を実行します。

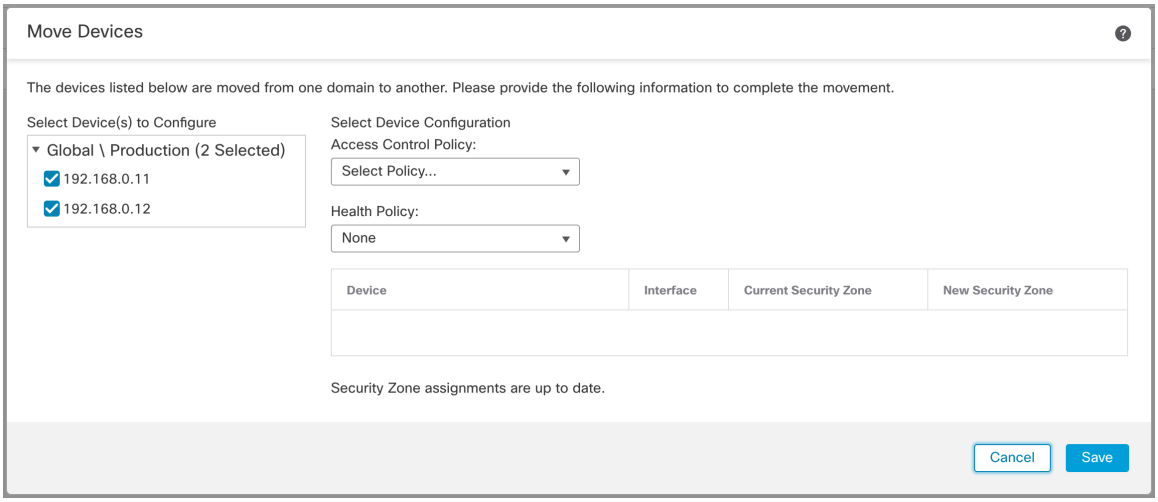
1. 移動するデバイスを選択し、[ドメインに追加（Add to Domain）] をクリックます。
2. [保存（Save）] をクリックします。

ステップ 4 [ドメイン（Domains）] ページで、[保存（Save）] をクリックします。

ステップ 5 **（アクセス コントロール ポリシーがグローバル ドメインにない場合）**[デバイスの移動（Move Devices）] ダイアログボックスで、次の手順を実行します。

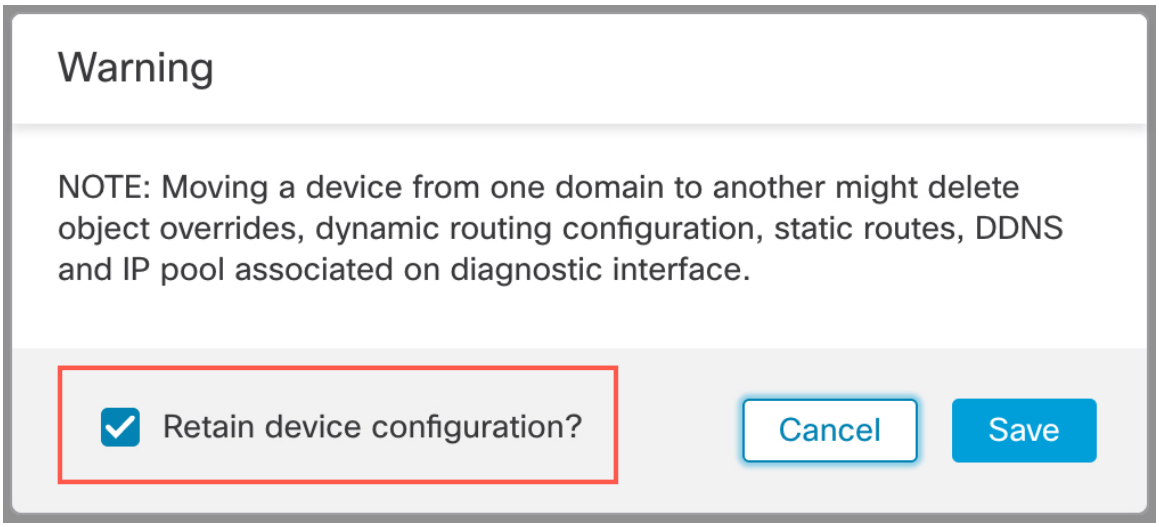
1. [設定するデバイスの選択（Select Device(s) to Configure）] で、設定するデバイスのチェックをオンにします。

   同じ正常性ポリシーとアクセス コントロール ポリシーを割り当てるには、複数のデバイスをオンにします。



2. デバイスに適用する [アクセスコントロールポリシー（Access Control Policy）] を選択するか、または新しいポリシーを作成するには[新しいポリシー（New Policy）] を選択します。
3. デバイスに適用する [正常性ポリシー（Health Policy）] を選択するか、またはデバイスに正常性ポリシーを適用しないままにするには [なし（None）] を選択します。
4. インターフェイスを新しいゾーンに割り当てるようにプロンプトが表示された場合は、リストされている各インターフェイスに [新しいセキュリティゾーン（New Security Zone）] を選択するか、または後で割り当てるには [なし（None）] を選択します。
5. すべての影響を受けるデバイスを設定した後、[保存（Save）] をクリックしてポリシーとゾーンの割り当てを保存します。

ステップ 6 移動後もデバイス設定を保持する場合は、[デバイス設定の保持（Retain device configuration?）] チェックボックスをオンにします。



このオプションを選択すると、デバイスがターゲットドメインに移動した後も、システムはデバイス設定を保持します。このオプションを選択しない場合、移動したデバイスのうち、移動による影響を受けたデバイスのデバイス設定を手動で更新する必要があります。

次の表は、さまざまなシナリオでオブジェクトがどのように処理されるかを示しています。

シナリオ	システムのアクション
オブジェクトは対象ドメインに存在します。	オブジェクトを再利用します。
ターゲットドメインに同じ名前と値のオブジェクトが存在します。	オブジェクトを再利用します。
ターゲットドメインに同じ名前で値が異なるオブジェクトが存在します。	• ネットワークとポート：オブジェクトのオーバーライドを作成します。 • インターフェイス オブジェクト：タイプが異なる場合に新しいオブジェクトを作成します。 • 名前の一致に応じて、他のすべてのオブジェクトタイプを再利用します。
ターゲットドメインにオブジェクトが存在しません。	新しいオブジェクトを作成します。

ステップ 7 [保存（Save）] をクリックして、ドメイン構成を実装します。

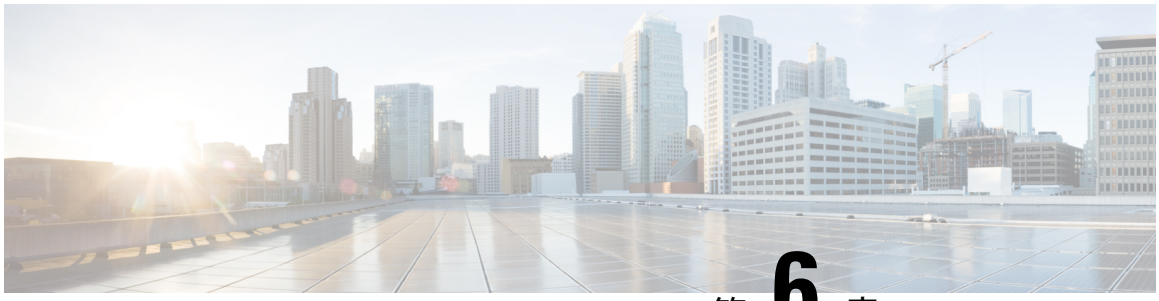
ステップ 8 ドメインの設定が完了したら、[OK] をクリックします。

次のタスク

- 移動の影響を受けた移動済みデバイスでその他の設定を更新します。
- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。
- ドメイン間でデバイスを移動した後にシステムがデバイス設定を保持できない場合は、手動でデバイス設定を復元できます。詳細については、『Cisco Secure Firewall Management Center デバイス構成ガイド』の「*Export and Import the Device Configuration*」を参照してください。

ドメイン管理の履歴

機能	最小 Management Center	最小 Threat Defense	詳細
サイト間 VPN に関連付けられたデバイス設定の保持	7.3	任意（Any）	ドメイン間でデバイスを移動するときに、サイト間 VPN がターゲットドメインで設定されている場合にのみ、サイト間 VPN に関連付けられているデバイス設定を保持できるようになりました。
デバイス設定の保持	7.2	任意（Any）	デバイスをドメイン間で移動しても、デバイス設定を保持できるようになりました。
サポートされているドメインの最大数の増加	6.5	任意（Any）	最大 100 ドメインを追加できるようになりました。以前は、最大で 50 ドメインでした。 サポートされているプラットフォーム： Secure Firewall Management Center



第 6 章

更新

この章では、コンテンツの更新方法について説明します。

重要 Management Center、または Threat Defense ソフトウェアやシャーシをアップグレードするには、*Management Center* が現在実行しているバージョンのアップグレードガイド：http://www.cisco.com/go/ftd-fmc-upgradehttp://www.cisco.com/go/ftd-fmc-upgrade-74を参照してください。

管理対象デバイスをアップグレードするには、クラウド提供型 Firewall Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイドを参照してください。

システムアップデートについて

Management Center を使用して、FMC 自体と FMC が管理するデバイスのシステムソフトウェアをアップグレードします。アドバンスドサービスを提供するさまざまなデータベースとフィードを更新することもできます。

Management Center がインターネットにアクセスできるときは、多くの場合、システムがシスコから直接更新を取得できます。可能な限り、コンテンツの自動更新をスケジュールするか、有効にすることを推奨します。一部の更新は、初期セットアッププロセスによって、または関連機能を有効にすると、自動的に有効になります。その他の更新は、自分でスケジュールする必要があります。初期セットアップ後に、すべての自動更新を確認し、必要に応じて調整することを推奨します。

表 *6*:アップグレードと更新

コンポーネント	説明（Description）	詳細
システム ソフトウェア	メジャー ソフトウェア リリースには、新機能、機能、および拡張機能が含まれます。インフラストラクチャまたはアーキテクチャの変更が含まれる場合があります。 メンテナンスリリースには、一般的なバグとセキュリティ関連の修正が含まれています。動作の変更はまれであり、これらの修正に関連しています。 パッチは、緊急性の高い重要な修正に限定されたオンデマンド更新です。 ホットフィックスは、特定のお客様の問題に対処できます。	**直接ダウンロード**：パッチおよびメンテナンスリリースのみを選択します。通常は、リリースが手動でダウンロードできるようになってからしばらく時間がかかります。遅延の長さは、リリースの種類、リリースの選択、およびその他の要因によって異なります。オンデマンドダウンロードとスケジュールされたダウンロードの両方がサポートされています。 （注） バージョン 7.4.1 では、すべてのリリース（ホットフィックスを除く）のオンデマンド直接ダウンロードのサポートが開始されました。ただし、メンテナンスリリースのスケジュールされたダウンロードのサポートは中止されました。 **スケジュールインストール**：パッチおよびメンテナンスリリースのみを、スケジュールされたタスクとしてインストールします。 **アンインストール**：パッチのみ。 **復元**：Threat Defense のメジャーリリースおよびメンテナンスリリースのみ。Management Center または従来型デバイスでは、復元機能はサポートされていません。 **再イメージ化**：メジャーリリースおよびメンテナンスリリースのみ。 **参照先**： Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
脆弱性データベース（VDB）	シスコ脆弱性データベース（VDB）は、オペレーティング システム、クライアント、およびアプリケーションのフィンガープリントだけでなく、ホストが影響を受ける可能性がある既知の脆弱性のデータベースです。システムでは、VDB を使用して、特定のホストで感染のリスクが高まるかどうかを判断します。	**直接ダウンロード**：あり。 **スケジュール**：あり（スケジュールタスクとして）。 **アンインストール**：VDB 357 以降、その Management Center の基準 VDB までさかのぼって任意の VDB をインストールできます。 **参照先**： 脆弱性データベース（VDB）の更新（266 ページ）

コンポーネント	説明（Description）	詳細
位置情報データベース（GeoDB）	シスコ地理位置情報データベース（GeoDB）は、ルーティング可能なIPアドレスに関連付けられている地理および接続関連のデータのデータベースです。	**直接ダウンロード**：あり。 **スケジュール**：あり（専用の更新ページから）。 **アンインストール**：なし。 **参照先**： 地理位置情報データベース（GeoDB）の更新（269 ページ）
侵入ルール（SRU/LSP）	侵入ルールの更新には、新規および更新された侵入ルールとプリプロセッサルール、既存のルールの変更されたステータス、変更されたデフォルト侵入ポリシーの設定が含まれています。 ルールの更新では、ルールが削除されたり、新しいルールカテゴリとデフォルトの変数が提供されたり、デフォルトの変数値が変更されたりすることもあります。	**直接ダウンロード**：あり。 **スケジュール**：あり（専用の更新ページから）。 **アンインストール**：なし。 **参照先**： 侵入ルールの更新 （271 ページ）
セキュリティインテリジェンスのフィード	セキュリティ インテリジェンスのフィードは、エントリに一致するトラフィックをすばやくフィルタリングするために使用できるIPアドレス、ドメイン名、およびURLのコレクションです。	**直接ダウンロード**：あり。 **スケジュール**：あり（オブジェクトマネージャから）。 **アンインストール**：なし。 **参照先**： Cisco Secure Firewall Management Center デバイス構成ガイド
URL カテゴリとレピュテーション	URL フィルタリングでは、URL の一般的な分類（カテゴリ）およびリスクレベル（レピュテーション）に基づいて、Webサイトへのアクセスを制御することができます。	**直接ダウンロード**：あり。 **スケジュール**：あり（統合/クラウドサービスを設定する場合、またはスケジュールタスクとして）。 **アンインストール**：なし。 **参照先**： Cisco Secure Firewall Management Center デバイス構成ガイド

システムアップデートの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

Global（特に明記のない場合）。

ユーザの役割

管理者

システムアップデートの注意事項と制約事項

更新する前に

展開のいずれかのコンポーネント（侵入ルール、VDB、GeoDB など）を更新する前に、更新に付属しているリリースノートまたはアドバイザリテキストを読んでください。これらは、互換性、前提条件、新機能、動作の変更、警告など、重要かつリリースに固有の情報を提供します。

スケジュールされた更新

システムは、タスク（更新を含む）を UTC でスケジュールします。そのため、いつ現地で実行されるかは、日付と場所によって異なります。また、更新は UTC でスケジュールされるため、サマータイムなど、所在地で実施される場合がある季節調整に合わせて調節されることもありません。このような影響を受ける場合、スケジュールされた更新は、現地時間を基準とすると、夏期では冬期の場合よりも 1 時間「遅れて」実行されることになります。

重要 スケジュールされた更新が意図したとおりに確実に実行されることの確認を強くお勧めします。

帯域幅のガイドライン

システムソフトウェアをアップグレードしたり準備状況チェックを実行するには、アップグレードパッケージがアプライアンス上に存在する必要があります。アップグレードパッケージには、さまざまなサイズがあります。管理対象デバイスに大容量のデータを転送するための帯域幅があることを確認します。『Guidelines for Downloading Data from the Firepower Management Center to Managed Devices』（トラブルシューティング テクニカルノーツ）を参照してください。

脆弱性データベース（VDB）の更新

シスコ脆弱性データベース（VDB）は、オペレーティング システム、クライアント、およびアプリケーションのフィンガープリントだけでなく、ホストが影響を受ける可能性がある既知の脆弱性のデータベースです。システムでは、VDB を使用して、特定のホストで感染のリスクが高まるかどうかを判断します。

シスコでは、VDB に対して定期的に更新を提供しています。Management Center で VDB と関連付けられたマッピングの更新にかかる時間は、ネットワークマップ内のホストの数によって異なります。一般的に、更新の実行にかかるおおよその時間（分）を判断するには、ホストの数を 1000 で割ります。

Management Center の初期設定では、1 回限りの操作でシスコから最新の VDB が自動的にダウンロードされてインストールされます。また、最新の VDB を含む最新の利用可能なソフトウェアアップデートをダウンロードする週次タスクもスケジュールされます。この週次タスクを確認し、必要に応じて調整することをお勧めします。必要に応じて、VDB を実際に更新し、構成を展開する新しい週次タスクをスケジュールしてください。詳細については、脆弱性データベースの更新の自動化 （613 ページ） を参照してください。

VDB 343 以降では、すべてのアプリケーションディテクタ情報は、Cisco Secure Firewall アプリケーションディテクタから入手できます。このサイトには、アプリケーションディテクタの検索可能なデータベースが含まれています。リリースノートには、特定の VDB リリースの変更に関する情報が記載されています。

VDB の更新のスケジュール

Management Center でインターネットアクセスができる場合、定期的な VDB 更新をお勧めします。脆弱性データベースの更新の自動化 （613 ページ） を参照してください。

VDB の手動更新

次の手順を使用して手動で VDB を更新します。VDB 357 以降、その Management Center の基準 VDB までさかのぼって任意の VDB をインストールできます。

注意 VDB の更新中に、マッピングされた脆弱性に関連するタスクを実行しないでください。メッセージセンターに進行状況が数分間表示されない、または更新が失敗したことが示されている場合でも、更新を再開しないでください。代わりに、Cisco TAC にお問い合わせください。

ほとんどの場合、VDB 更新後の最初の展開では Snort プロセスが再起動され、トラフィックインスペクションが中断されます。これが発生すると、システムから警告が表示されます（更新されたアプリケーションディテクタとオペレーティングシステムのフィンガープリントについては再起動が必要ですが、脆弱性情報については不要です）。この中断中にインスペクションを続行せずにトラフィックがドロップされるかパスするどうかは、対象デバイスによるトラフィックの処理方法によって異なります。詳細については、「Snort の再起動によるトラフィックの動作」を参照してください。

始める前に

Management Center がシスコ サポートおよびダウンロードサイトにアクセスできない場合は、ユーザー自身で更新を入手します：https://www.cisco.com/go/firepower-software。モデルを選択または検索し（または任意のモデルを選択して、すべての Management Center に同じ VDB を使

用します）、[カバレッジおよびコンテンツの更新（Coverage and Content Updates）] ページを参照します。

手順

ステップ 1 ルール更新ページに移動します。

- バージョン 7.4.0：**システム**（⚙）>**[更新（Updates）]**>**[製品の更新（Product Updates）]**
- バージョン 7.4.1 以降：**システム**（⚙）>**[Content Updates]**>**[VDB Updates]**

ステップ 2 VDB を Management Center に取得する方法を選択します。

- 直接ダウンロード：[アップデートのダウンロード（Download Updates）] ボタンすぐにダウンロードできます。
- 手動でアップロード：[更新のアップロード（Upload Update）] をクリックし、[ファイルの選択（Choose File）] をクリックして VDB を参照します。ファイルを選択したら、[アップロード（Upload）] をクリックします。

（注） バージョン 7.4.0 では、[更新のダウンロード（Download Updates）] をクリックすることでも、環境に適した最新のメンテナンスリリースおよび最新の重要パッチをすぐに取得できます。

ステップ 3 VDB をインストールします。

a) インストールする [脆弱性およびフィンガープリント データベースの更新（Vulnerability and Fingerprint Database update）] の横にある [インストール（Install）] アイコン（新しい VDB の場合）または [ロールバック（Rollback）] アイコン（古い VDB の場合）をクリックします。
b) Management Center を選択します。
c) [Install（インストール）] をクリックします。

Message Center で更新の進行状況をモニターします。更新の完了後に、システムで新しい脆弱性情報が使用されます。ただし、更新されたアプリケーションディテクタとオペレーティングシステム フィンガープリントを有効にするために、展開する必要があります。

ステップ 4 更新が成功したことを確認します。

VDB 更新ページと **[ヘルプ（Help）]**（?）>**[バージョン情報（About）]** の両方に現在のバージョンが表示されます。

次のタスク

- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

- 利用できなくなった脆弱性、アプリケーションディテクタ、またはフィンガープリントに基づいて設定を行っている場合は、それらの設定を調べて、トラフィックが期待どおりに処理されていることを確認します。また、VDB を更新するためのスケジュールされたタスクは、ロールバックを取り消すことができることに注意してください。これを回避するには、スケジュールされたタスクを変更するか、新しい VDB パッケージを削除します。

地理位置情報データベース（GeoDB）の更新

地理位置情報データベース（GeoDB）は、地理的な位置に基づいてトラフィックを表示およびフィルタリングするために利用できるデータベースです。シスコでは GeoDB を定期的に更新しています。正確な地理位置情報を取得するには、GeoDB を定期的に更新する必要があります。**[ヘルプ（Help）]**（?）>**[バージョン情報（About）]** で現在のバージョンを確認できます。

システムには IP アドレスを国/大陸にマッピングする GeoDB カントリー コード パッケージが付属しています。また、コンテキストデータを含む IP パッケージも提供されます。これには、追加の場所詳細のほか、ISP、接続タイプ、プロキシタイプ、ドメイン名などの接続情報が含まれます。

- バージョン 7.4.0 ～ 7.4.1 では、システムが（オンデマンドでまたはスケジュールに従って）GeoDB の更新をダウンロードする際、デフォルトで両方のパッケージがダウンロードされます。コンテキストデータが重要でない場合は、IP パッケージを無効化および削除することでディスク容量を節約できます。
- バージョン 7.4.2 以降では、デフォルトで国コードパッケージのみがダウンロードされますが、コンテキストデータが重要であり、十分なディスク容量がある場合は、両方のパッケージをダウンロードするように設定できます。

GeoDB の更新は、以前のバージョンをオーバーライドします。Management Center により、管理対象デバイスが自動的に更新されるため、展開する必要はありません。GeoDB の更新に必要な時間は展開によって異なりますが、更新のサイズによっては最大 45 分かかる場合があります（たとえば、完全な IP パッケージをダウンロードして処理する場合など）。GeoDB の更新は他のシステムの機能（実行中の地理情報の収集など）を中断することはありませんが、更新が完了するまでシステムのリソースを消費します。

初期構成の一環として、システムは週次 GeoDB 更新をスケジュールします。このタスクを確認し、必要に応じ、GeoDB 更新のスケジューリング （269 ページ）。

GeoDB 更新のスケジューリング

初期構成の一環として、システムは週次 GeoDB 更新をスケジュールします。このタスクを確認し、必要に応じ、この手順。

始める前に

Management Center で シスコ サポートおよびダウンロード サイト にアクセスできることを確認します。

手順

ステップ 1 GeoDB 更新ページに移動します。

- バージョン 7.4.0：**システム**（⚙）>**[更新（Updates）]**>**[地理位置情報の更新（Geolocation Updates）]**
- バージョン 7.4.1 以降：**システム**（⚙）>**[Content Updates]**>**[Geolocation Updates]**

ステップ 2 [IPパッケージの設定（IP Package Configuration）] で、[IPパッケージのダウンロード（IP Package Download）] オプションを使用して、必要な国コードパッケージのみをダウンロードするか IP パッケージもダウンロードするかを指定します。

IP パッケージを使用しないと、ディスク容量を節約できますが、IP アドレスのコンテキスト地理位置情報データも削除されます。この設定を変更した場合は、[保存（Save）] をクリックします。

ステップ 3 [Recurring Geolocation Updates] で、[Enable Recurring Weekly Updates] をオンにします。。

ステップ 4 [開始時刻の更新（Update Start Time）] を指定します。

ステップ 5 [保存（Save）] をクリックします。

地理位置情報データベース（GeoDB）の手動更新

オンデマンド GeoDB 更新を実行するには、次の手順を実行します。

始める前に

Management Center が シスコ サポートおよびダウンロード サイト にアクセスできない場合は、ユーザー自身で更新を入手します：「Software Download」。モデルを選択または検索し（または任意のモデルを選択して、すべての Management Center に同じ GeoDB を使用します）、[カバレッジおよびコンテンツの更新（Coverage and Content Updates）] ページを参照します。国コードパッケージと、オプションで、IP パッケージをダウンロードします。

手順

ステップ 1 GeoDB 更新ページに移動します。

- バージョン 7.4.0：**システム**（⚙）>**[更新（Updates）]**>**[地理位置情報の更新（Geolocation Updates）]**

- バージョン 7.4.1 以降：**システム**（⚙） > **[Content Updates]** > **[Geolocation Updates]**

ステップ 2 [1回限りの地理位置情報更新（One-Time Geolocation Update）] で、GeoDB の更新方法を選択します。

- 直接ダウンロード：[ダウンロードしてインストール...（Download and install...）] を選択します。
- 手動アップロード：[アップロードしてインストール...（Upload and install...）] を選択し、[ファイルを選択（Choose File）] をクリックして、事前にダウンロードした国コードパッケージを参照します。

ステップ 3 [IPパッケージの設定（IP Package Configuration）] で、[IPパッケージのダウンロード（IP Package Download）] オプションを使用して、国コードパッケージのみを使用するかIPパッケージも使用するかを指定します。

IP パッケージを使用しないと、ディスク容量を節約できますが、IP アドレスのコンテキスト地理位置データも削除されます。GeoDB パッケージを手動でアップロードする場合でも、IP パッケージのデータが必要ないときは、このオプションを無効にする必要があります。これは、オプションを無効にすると、既存の IP パッケージまたは古い IP パッケージが削除されるためです。

この設定を変更した場合は、[保存（Save）] をクリックします。

ステップ 4 [インポート（Import）] をクリックします。

Message Center で更新の進行状況をモニターします。

ステップ 5 更新が成功したことを確認します。

GeoDB 更新ページと **[ヘルプ（Help）]**（❓） > **[バージョン情報（About）]** の両方に現在のバージョンが表示されます。

ステップ 6 （任意）更新を手動でアップロードする場合は、IPパッケージに対してこの手順を繰り返します。

侵入ルールの更新

新たな脆弱性が発見されると、Talos インテリジェンスグループ は侵入ルールの更新をリリースします。それらの更新は、侵入ルール、プリプロセッサルール、およびルールを使用するポリシーに影響を及ぼします。侵入ルール更新は更新を累積されていくものなので、常に最新の更新をインポートすることをお勧めします。現在インストールされているルールのバージョン以前の侵入ルールの更新をインポートすることはできません。

侵入ルールの更新では、次のものを提供します。

- **新規または変更されたルールおよびルール状態**：ルール更新は、新規および更新された侵入ルールとプリプロセッサルールを提供します。新規ルールの場合は、システム付属の各侵入ポリシーでルール ステータスが異なることがあります。たとえば、新規ルールが、Security over Connectivity 侵入ポリシーでは有効になっており、Connectivity over Security 侵入ポリシーでは無効になっていることがあります。ルールの更新では、既存のルールのデフォルトの状態が変更されたり、既存のルールが完全に削除されることもあります。
- **新しいルール カテゴリ**：ルール更新には、常に追加される新しいルール カテゴリが含まれている場合があります。
- **変更されたプリプロセッサおよび詳細設定**：ルール更新によって、システム提供の侵入ポリシーの詳細設定、およびシステム提供のネットワーク分析ポリシーのプリプロセッサ設定が変更されることがあります。また、アクセス コントロール ポリシーの高度な前処理およびパフォーマンスのオプションのデフォルト値も変更される場合があります。
- **新規および変更された変数**：ルール更新によって、既存のデフォルト変数のデフォルト値が変更されることがありますが、ユーザによる変更は上書きされません。新しい変数が常に追加されます。

マルチドメイン展開では、ローカル侵入ルールを任意のドメインにインポートできますが、グローバル ドメイン内の Talos からでなければ、侵入ルールの更新をインポートすることはできません。

侵入ルールの更新によってポリシーが変更されるタイミングについて

侵入ルールの更新は、システムが提供するネットワーク分析ポリシーとカスタム ネットワーク分析ポリシーの両方だけでなく、すべてのアクセス コントロール ポリシーにも影響する場合があります。

- **システム提供**：システムが提供するネットワーク分析および侵入ポリシーへの変更は、その他のアクセスコントロールの詳細設定と同様に、更新後にポリシーを再展開すると自動的に有効になります。
- **カスタム**：すべてのカスタム ネットワーク分析ポリシーと侵入ポリシーは、システム付属ポリシーをそのベースとして、またはポリシーチェーンの根本的ベースとして使用しているので、ルール更新によってカスタム ネットワーク分析ポリシーと侵入ポリシーが影響を受けることがあります。ただし、ルール更新によるこれらの自動的な変更は回避することができます。これにより、ルール更新のインポートとは関係ないスケジュールで、システムによって提供される基本ポリシーを手動で更新できます。ユーザーによる選択（カスタム ポリシーごとに実装）とは関係なく、システム付属ポリシーに対する更新によって、カスタマイズ済みの設定が上書きされることは**ありません**。

ルール更新をインポートすると、ネットワーク分析ポリシーと侵入ポリシーのキャッシュされていた変更がすべて廃棄されるので注意してください。便宜のために、[ルールの更新（Rule Updates）]ページには、キャッシュされている変更があるポリシー、および変更を行ったユーザが表示されます。

侵入ルールの更新の展開

侵入ルールの更新によって行われた変更を有効にするには、設定を再導入する必要があります。侵入ルールの更新をインポートする際に、影響を受けるデバイスに自動的に再導入するようシステムを設定できます。この手法が特に役立つのは、侵入ルールの更新によるシステム提供の基本侵入ポリシーの変更を許可する場合です。

注意 ルールの更新自体は、展開時に Snort プロセスを再起動しませんが、加えた他の変更により再起動する可能性があります。Snort を再起動すると、高可用性/拡張性を備えた構成になっているものを含め、すべてのデバイスでトラフィックフローとインスペクションが一時的に中断されます。インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます。Snort を再起動せずに展開すると、リソース要求時にいくつかのパケットが検査なしでドロップされることがあります。

侵入ルールの更新の繰り返し

[ルールの更新（Rule Updates）] ページを使用して、ルール更新を日次、週次、または月次ベースでインポートすることができます。

展開に高可用性ペアのManagement Centerが含まれる場合は、プライマリ側だけに更新をインポートします。セカンダリ Management Center は、通常の同期プロセスの一環としてルールの更新を受け取ります。

侵入ルールの更新のインポートに適用されるサブタスクは、ダウンロード、インストール、ベースポリシーの更新、設定の展開の順で実行されます。1 つのサブタスクが完了すると、次のサブタスクが開始されます。

スケジュールされた時間になると、システムはルールの更新をインストールして、前のステップで指定したように変更後の設定を展開します。インポートの前、またはインポート中にログオフすることも、Web インターフェイスを使用して他のタスクを実行することもできます。インポート中に [ルールの更新ログ（Rule Update Log）] にアクセスすると、[赤色のステータス（Red Status）] （⛔） が表示され、[ルールの更新ログ（Rule Update Log）] 詳細ビューに表示されるメッセージを確認できます。ルール更新のサイズと内容によっては、ステータス メッセージが表示されるまでに数分かかることがあります。

初期構成の一環として、システムは日次の侵入ルール更新をスケジュールします。このタスクを確認し、必要に応じ、侵入ルールの更新のスケジュール （274 ページ）。

ローカル侵入ルールのインポート

ローカル侵入ルールは、ASCII または UTF-8 エンコーディングによるプレーン テキスト ファイルとしてローカル マシンからインポートするカスタム標準テキスト ルールです。Snort ユーザ マニュアル（http://www.snort.org で入手可能）の指示に従って、ローカル ルールを作成することができます。

マルチドメイン展開では、任意のドメインにローカル侵入ルールをインポートできます。現在のドメインと親ドメインにインポートされたローカル侵入ルールを表示できます。

侵入ルールの更新のスケジュール

初期構成の一環として、システムは日次の侵入ルール更新をスケジュールします。このタスクを確認し、必要に応じ、この手順。

始める前に

- 侵入ルールの更新プロセスが、自身のセキュリティポリシーに適合していることを確認します。
- 帯域幅の制約や Snort の再起動が発生するため、トラフィックフローとインスペクションに更新による影響があることを考慮します。メンテナンス ウィンドウ期間に更新を実行することをお勧めします。
- Management Center で シスコ サポートおよびダウンロード サイト にアクセスできることを確認します。

手順

ステップ 1 ルール更新ページに移動します。

- バージョン 7.4.0：**システム**（⚙） > **[更新（Updates）]** > **[ルールの更新（Rule Updates）]**
- バージョン 7.4.1 以降：**システム**（⚙） > **[Content Updates]** > **[Rule Updates]**

ステップ 2 [定期的なルール更新のインポート（Recurring Rule Update Imports）] で、[定期的なルール更新のインポートを有効にする（Enable Recurring Rule Update Imports）] をオンにします。

ステップ 3 [インポート頻度（Import Frequency）] と開始時刻を指定します。

ステップ 4 （オプション）各更新後に展開するには、[...すべてのポリシーを再適用（Reapply all policies...）] をオンにします。

ステップ 5 [保存（Save）] をクリックします。

侵入ルールの手動更新

オンデマンド侵入ルール更新を実行するには、次の手順を実行します。

始める前に

- 侵入ルールの更新プロセスが、自身のセキュリティポリシーに適合していることを確認します。
- 帯域幅の制約や Snort の再起動が発生するため、トラフィックフローとインスペクションに更新による影響があることを考慮します。メンテナンス ウィンドウ期間に更新を実行することをお勧めします。

- Management Center が シスコ サポートおよびダウンロード サイト にアクセスできない場合は、ユーザー自身で更新を入手します：「Software Download」。モデルを選択または検索し（または任意のモデルを選択して、すべての Management Center に同じ SRU または LSP を使用します）、[カバレッジおよびコンテンツの更新（Coverage and Content Updates）] ページを参照します。

手順

ステップ 1 ルール更新ページに移動します。

- バージョン 7.4.0：**システム**（⚙）> **[更新（Updates）]** > **[ルールの更新（Rule Updates）]**
- バージョン 7.4.1 以降：**システム**（⚙）> **[Content Updates]** > **[Rule Updates]**

ステップ 2 [ワンタイムルール更新/ルールインポート（One-Time Rule Update/Rules Import）] で、侵入ルールの更新方法を選択します。

- 直接ダウンロード：[新しいルール更新をダウンロードする...（Download new rule update...）] を選択します。
- 手動アップロード：[ルール更新またはテキストルールファイル...（Rule update or text rule file...）] を選択し、[ファイルの選択（Choose File）] をクリックして侵入ルール更新を参照します。

ステップ 3 （任意）更新後に展開するには、[すべてのポリシーを再適用する...（Reapply all policies...）] をオンにします。

ステップ 4 [インポート（Import）] をクリックします。

Message Center で更新の進行状況をモニターします。メッセージ センターに進行状況が数分間表示されない、または更新が失敗したことが示されている場合でも、更新を再開しないでください。代わりに、Cisco TAC にお問い合わせください。

ステップ 5 更新が成功したことを確認します。

ルール更新ページと **[ヘルプ（Help）]**（?）> **[バージョン情報（About）]** の両方に現在のバージョンが表示されます。

次のタスク

更新の一部として展開しなかった場合は、ここで展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

ローカル侵入ルールのインポート

ローカル侵入ルールをインポートするには、次の手順を使用します。インポートされた侵入ルールは、無効状態でローカル ルール カテゴリに表示されます。このタスクは、どのドメインでも実行できます。

始める前に

- ローカル ルール ファイルが、ローカル侵入ルールのインポートに関するガイドライン（277 ページ）に記載されているガイドラインに従っていることを確認します。
- ローカル侵入ルールのインポート プロセスが、自身のセキュリティ ポリシーに適合していることを確認します。
- 帯域幅の制約や Snort の再起動が発生するため、トラフィック フローとインスペクションにインポートによる影響があることを考慮します。メンテナンス ウィンドウ期間にルール更新をスケジュールすることをお勧めします。

手順

ステップ 1 ルール更新ページに移動します。

- バージョン 7.4.0：**システム**（⚙）> **[更新（Updates）]** > **[ルールの更新（Rule Updates）]**
- バージョン 7.4.1 以降：**システム**（⚙）> **[Content Updates]** > **[Rule Updates]**
- 任意のバージョン：侵入ルールエディタ（**[オブジェクト（Objects）]** > **[侵入ルール（Intrusion Rules）]**）で [ルールのインポート（Import Rules）] をクリックします。

ステップ 2 （オプション）既存のローカル ルールを削除します。

[すべてのローカルルールの削除（Delete All Local Rules）] をクリックして、すべての作成およびインポートされた侵入ルールを削除フォルダに移動することを確認します。

ステップ 3 [ワンタイムルール更新/ルールインポート（One-Time Rule Update/Rules Import）] で、[アップロードおよびインストールするルールの更新またはテキストルールファイル（Rule update or text rule file to upload and install）] を選択して、[ファイルの選択（Choose File）] をクリックしたら、ローカルルールファイルを参照します。

ステップ 4 [インポート（Import）] をクリックします。

メッセージセンターでインポートの進行状況をモニターできます。メッセージセンターに進行状況が数分間表示されない、または更新が失敗したことが示されている場合でも、インポートを再開しないでください。代わりに、Cisco TAC にお問い合わせください。

次のタスク

- 侵入ポリシーを編集し、インポートしたルールを有効にします。

- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

ローカル侵入ルールのインポートに関するガイドライン

ローカル ルール ファイルをインポートする際には次のガイドラインに従います。

- ルールのインポータには、すべてのカスタム ルールが ASCII または UTF-8 でエンコードされるプレーン テキスト ファイルにインポートされることが必要です。
- テキストファイル名には英数字とスペースを使用できますが、下線（_）、ピリオド（.）、ダッシュ（-）以外の特殊記号は使用できません。
- システムは、単一のポンド文字（#）で始まるローカル ルールをインポートしますが、これらには削除のフラグが立てられます。
- 単一のポンド文字（#）で始まるローカル ルールはインポートされますが、2 つのポンド文字（##）で始まるローカル ルールはインポートされません。
- ルールにはエスケープ文字を含めることはできません。
- マルチドメイン展開では、グローバル ドメインにインポートまたは作成されたルールに 1 の GID が割り当てられ、他のすべてのドメインには 1000 ～ 2000 の間のドメイン固有 GID が割り当てられます。
- ローカル ルールをインポートするときにはジェネレータ ID（GID）を指定する必要はありません。指定する場合は、標準テキスト ルールに GID 1 のみを指定します。
- ルールを初めてインポートするときには、[Snort ID]（SID）またはリビジョン番号を指定しないでください。これにより、削除されたルールを含むその他のルールの SID の競合を回避できます。システムはルールに対して、1000000 以上の次に使用できるカスタム ルール SID 、およびリビジョン番号 の 1 を自動的に割り当てます。

  SID を持つルールをインポートする必要がある場合、SID には 1,000,000 以上の一意の番号を指定できます。

  マルチドメイン展開で、複数の管理者がローカル ルールを同時にインポートする場合、個々のドメイン内の SID が連続していないように見える場合があります。これは、シーケンス内の途中の数字が別のドメインに割り込んで指定されたためです。
- 以前にインポートしたローカルルールの更新バージョンをインポートするとき、または削除したローカル ルールを元に戻すときは、システムによって指定された SID および現在のリビジョン番号より大きいリビジョン番号を含める必要があります。ルールを編集して、現在のルールまたは削除されたルールのリビジョン番号を判別できます。

（注） ローカル ルールを削除すると、システムは自動的にリビジョン番号を増やします。これは、ローカル ルールを元に戻すための方法です。削除されたすべてのローカル ルールは、ローカル ルール カテゴリから、削除されたルール カテゴリへ移動されます。

- SID 番号の問題を回避するには、高可用性ペアのプライマリ Management Center でローカルルールをインポートします。
- ルールに次のいずれかが含まれていると、インポートに失敗します。
  - 2147483647 より大きい SID。
  - 64 文字よりも長い送信元ポートまたは宛先ポートのリスト。
  - マルチドメイン展開でグローバル ドメインにインポートする場合、GID:SID の組み合わせでは、別のドメインに既に存在する GID 1 と SID を使用します。これは、バージョン 6.2.1 より前に組み合わせが存在していたことを示します。GID 1 と固有の SID を使用してルールを再インポートできます。
- 非推奨の `threshold` キーワードと侵入イベントしきい値機能を組み合わせて使用しているローカル ルールをインポートして、侵入ポリシーで有効にすると、ポリシーの検証に失敗します。
- インポートされたすべてのローカル ルールは、ローカル ルール カテゴリに自動的に保存されます。
- システムによって、インポートしたローカル ルールは常に無効なルール状態に設定されます。ローカル ルールを侵入ポリシーで使用できるようにするには、ローカル ルールの状態を手動で設定する必要があります。

侵入ルールの更新ログの表示

システムは、ルールの更新/インポートのログを生成します。これには、タイムスタンプ、ユーザー、および各更新の成功/失敗が示されます。これらのログには、更新されたすべてのルールおよびコンポーネントに関する詳細なインポート情報が含まれています。侵入ルール更新のログの詳細（279ページ）を参照してください。ルールインポートログを表示するには、次の手順を実行します。インポートログを削除してもインポートされたオブジェクトは削除されないことに注意してください。 マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 ルール更新ページに移動します。

- バージョン 7.4.0：**システム**（⚙）> **[更新（Updates）]** > **[ルールの更新（Rule Updates）]**
- バージョン 7.4.1 以降：**システム**（⚙）> **[Content Updates]** > **[Rule Updates]**

ステップ 2 [ルールアップデートログ（Rule Update Log）] をクリックします。

ステップ 3 （任意）ログファイルの横にある [表示（View）]（  ） をクリックして、ルール更新の詳細を表示します。

侵入ルール更新のログの詳細

ヒント 1 つのインポート ファイルのレコードのみが表示されている [ルール アップデートのインポート ログ（Rule Update Import Log）] 詳細ビューからツールバーの [検索（Search）] をクリックして検索を開始した場合でも、[ルール アップデートのインポート ログ（Rule Update Import Log）]データベースの全体が検索されます。検索の対象とするすべてのオブジェクトが含まれるように、時間制限が設定されていることを確認します。

表 *7*:侵入ルール更新のログの詳細

フィールド	説明
操作	オブジェクト タイプについて、次のいずれかが発生していることを示します。 • [新規（new）]（ルールで、このアプライアンスにルールが最初に格納された場合） • [変更済み（changed）]（ルール更新コンポーネントまたはルール用。ルール更新コンポーネントが変更された場合、またはルールのリビジョン番号が大きく、GID と SID が同じ場合） • [競合（collision）]（ルール更新コンポーネントまたはルールに関して、アプライアンス上の既存のコンポーネントまたはルールとリビジョンが競合しているため、インポートがスキップされた場合） • [削除済み（deleted）]（ルール用。ルール更新からルールが削除された場合） • [有効（enabled）]（ルール更新の編集で、プリプロセッサ、ルール、または他の機能が、システムで提供されるデフォルト ポリシーで有効になっていた場合） • [無効（disabled）]（ルールで、システム提供のデフォルト ポリシーでルールが無効になっていた場合） • [ドロップ（drop）]（ルールで、システムで提供されるデフォルト ポリシーで、ルールが[ドロップおよびイベントの生成（Drop and Generate Events）] に設定されていた場合） • [エラー（error）]（ルール更新またはローカル ルール ファイル用。インポートに失敗した場合） • [適用（apply）]（インポートに対して [ルール更新のインポート完了後にすべてのポリシーを再適用する（Reapply all policies after the rule update import completes）] オプションが有効だった場合）

フィールド	説明
デフォルト アクション（Default Action）	ルールの更新によって定義されたデフォルトのアクション。インポートされたオブジェクトのタイプが [ルール（rule）] の場合、デフォルトのアクションは [通過（Pass）]、[アラート（Alert）]、または [ドロップ（Drop）] になります。インポートされた他のすべてのオブジェクト タイプには、デフォルトのアクションはありません。
詳細	コンポーネントまたはルールに対する一意の文字列。ルールの場合、変更されたルールの GID、SID、および旧リビジョン番号は、`previously (GID:SID:Rev)` と表示されます。変更されていないルールについては、このフィールドは空白です。
ドメイン（Domain）	侵入ポリシーで更新されたルールを使用できるドメイン。子孫ドメインの侵入ポリシーもルールを使用できます。このフィールドは、マルチドメイン展開の場合にのみ存在します。
GID	ルールのジェネレータ ID。たとえば、`1`（標準テキスト ルール、グローバル ドメインまたは従来の GID）または `3`（共有オブジェクト ルール）。
名前	インポートされたオブジェクトの名前。ルールの場合はルールの [メッセージ（Message）] フィールドに対応した名前で、ルール更新コンポーネントの場合はコンポーネント名です。
ポリシー	インポートされたルールの場合、このフィールドには [すべて（All）] が表示されます。つまり、ルールが正常にインポートされ、適切なデフォルト侵入ポリシーすべてで有効にすることができます。インポートされた他のタイプのオブジェクトについては、このフィールドは空白です。
Rev	ルールのリビジョン番号。
ルール アップデート（Rule Update）	ルール更新のファイル名。
SID	ルールの SID。
Time	インポートが開始された日時。
タイプ	インポートされたオブジェクトのタイプで、有効な値は次のいずれかです。 • [ルール更新コンポーネント（rule update component）]（ルール パックやポリシー パックなどのインポートされたコンポーネント） • [ルール（rule）]（ルール用。新しいルールまたは更新されたルール）。 • [ポリシー適用（policy apply）]（インポートに対して [ルール更新のインポート完了後にすべてのポリシーを再適用する（Reapply all policies after the rule update import completes）] オプションが有効だった場合）
カウント（Count）	各レコードのカウント（`1`）。テーブルが制限されており、[ルール アップデート ログ（Rule Update Log）] 詳細ビューがデフォルトでルール更新レコードに制限されている場合は、テーブル ビューに [メンバー数（Count）] フィールドが表示されます。このフィールドは検索できません。

エアギャップ展開の維持

Management Center がインターネットに接続されていない場合、必要な更新は自動的に実行されません。それらの更新を手動で取得してインストールする必要があります。

詳細については、以下を参照してください。

- ソフトウェア アップグレード ガイド：https://cisco.com/go/ftd-fmc-upgrade
- VDB の手動更新 （267 ページ）
- 侵入ルールの手動更新 （274 ページ）
- 地理位置情報データベース（GeoDB）の手動更新 （270 ページ）

システムアップデートの履歴

表 *8 :* バージョン *7.4.1* の機能

機能	最小 Management Center	最小 Threat Defense	詳細
Threat Defense のアップグレード			
FXOS アップグレードに含まれるファームウェアのアップグレード。	任意（Any）	任意（Any）	**シャーシ/FXOS アップグレードの影響。ファームウェアのアップグレードにより、余分な再起動が発生します。** Firepower 4100/9300 の場合、バージョン 2.14.1 への FXOS アップグレードにファームウェアのアップグレードが含まれるようになりました。デバイス上のいずれかのファームウェア コンポーネントが FXOS バンドルに含まれているコンポーネントよりも古い場合、FXOS アップグレードによってファームウェアも更新されます。ファームウェアがアップグレードされると、デバイスは 2 回リブートします。1 回は FXOS 用、1 回はファームウェア用です。 ソフトウェアおよびオペレーティングシステムのアップグレードと同様に、ファームウェアのアップグレード中に設定変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、ファームウェアのアップグレード中は手動で再起動またはシャットダウンしないでください。 参照：Cisco Firepower 4100/9300 FXOS ファームウェア アップグレード ガイド

機能	最小 Management Center	最小 Threat Defense	詳細
マルチインスタンスモードでの Secure Firewall 3100 のシャーシのアップグレード	7.4.1	7.4.1	マルチインスタンスモードの Cisco Secure Firewall 3100 では、コンテナインスタンスのアップグレード（*Threat Defense* のアップグレード）とは別に、オペレーティングシステムとファームウェアがアップグレードの対象（シャーシのアップグレード）になります。 新規/変更された画面： • シャーシのアップグレード：**[デバイス（Devices）]** > **[シャーシのアップグレード（Chassis Upgrade）]** • Threat Defense のアップグレード：**[デバイス（Devices）]** > **[Threat Defenseのアップグレード（Threat Defense Upgrade）]** 参照： Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
Management Center のアップグレード			
Management Center のアップグレード後に設定変更レポートを自動的に生成します。	任意（Any）	任意（Any）	Management Center のメジャーおよびメンテナンスアップグレード後に、設定変更に関するレポートを自動的に生成できます。このレポートは、展開しようとしている変更を理解するのに役立ちます。レポートが生成されたら、メッセージセンターの [タスク（Tasks）] タブからレポートをダウンロードできます。 その他のバージョンの制限：バージョン 7.4.1 以降の Management Center のアップグレードでのみサポートされます。バージョン 7.4.1 以前のバージョンへのアップグレードはサポートされていません。 新規/変更された画面：**システム（⚙）** > **[設定（Configuration）]** > **[設定のアップグレード（Upgrade Configuration）]** > **[アップグレード後のレポートの有効化（Enable Post-Upgrade Report）]**

表 *9*：バージョン *7.4.0* の機能

機能	最小 Management Center	最小 Threat Defense	詳細
Management Center のアップグレード：廃止された機能			

機能	最小 Management Center	最小 Threat Defense	詳細
一時的に廃止された機能。	7.4.0	機能に依存	バージョン 7.2.6 以降を実行している場合、バージョン 7.4.0 にアップグレードすると、次のアップグレード関連機能が削除されます。 • アップグレードの開始ページとパッケージ管理が改善されました。 • Threat Defense のアップグレードウィザードからの復元の有効化。 • Threat Defense アップグレードウィザードから詳細なアップグレードステータスを表示します。 • 推奨リリースの通知。 • Management Center の新しいアップグレードウィザード。 • 同期を一時停止することなく、高可用性管理センターでホットフィックスを利用できます。 • ソフトウェアアップグレードの直接ダウンロードに関するインターネットアクセス要件を更新しました。アップグレードの影響。 • スケジュール済みタスクでは、パッチおよび VDB 更新のみダウンロードされます。アップグレードの影響。

表 *10* : バージョン *7.3.0* の機能

機能	最小 Management Center	最小 Threat Defense	詳細
廃止された機能			

機能	最小 Management Center	最小 Threat Defense	詳細
一時的に廃止された機能。	任意	機能に依存	バージョン 7.2.6 以降を実行している場合、バージョン 7.3.x にアップグレードすると、次のアップグレード関連機能が削除されます。 • アップグレードの開始ページとパッケージ管理が改善されました。 • Threat Defense のアップグレードウィザードからの復元の有効化。 • Threat Defense アップグレードウィザードから詳細なアップグレードステータスを表示します。 • 推奨リリースの通知。 • Management Center の新しいアップグレードウィザード。 • 同期を一時停止することなく、高可用性管理センターでホットフィックスを利用できます。 • ソフトウェアアップグレードの直接ダウンロードに関するインターネットアクセス要件を更新しました。 • 国コードの地理位置情報パッケージのみをダウンロードします。 • スケジュール済みタスクでは、パッチおよび VDB 更新のみダウンロードされます。 アップグレードはサポートされていますが、現在のバージョンに含まれている重要な修正および機能拡張が削除されます。バージョン 7.4.1 以降に直接アップグレードすることをお勧めします。
Threat Defense のアップグレード			
シスコからアップグレードパッケージを選択して、Management Center に直接ダウンロードします。	7.3.0	いずれか	Management Center に直接ダウンロードする Threat Defense アップグレードパッケージを選択できるようになりました。 > **[更新（Updates）]** > **[製品の更新（Product Updates）]** の新しい [の更新のダウンロード（Download Threat Defense Updates）] サブタブを使用します。 その他のバージョンの制限：バージョン 7.2.6/7.4.1 では、この機能は改善されたパッケージ管理システムに置き換えられています。 参照：Management Center を含むアップグレードパッケージのダウンロード

機能	最小 Management Center	最小 Threat Defense	詳細
Threat Defense のウィザードを使用してアップグレードパッケージを Management Center にアップロードします。	7.3.0	いずれか	ウィザードを使用して、脅威防御アップグレードパッケージをアップロードしたり、場所を指定したりできるようになりました。以前は（バージョンに応じて）、**システム**（⚙）>**[更新（Updates）]**または**システム**（⚙）>**[製品のアップグレード（Product Upgrades）]**を使用していました。 その他のバージョンの制限：バージョン 7.2.6/7.4.1 では、この機能は改善されたパッケージ管理システムに置き換えられています。 参照：脅威防御のアップグレード
Threat Defense のアップグレード完了後の Snort 3 への自動アップグレードはオプションではなくなりました。	7.3.0	いずれか	**アップグレードの影響。** Threat Defence をバージョン 7.3 以降にアップグレードする場合、[Snort 2からSnort 3にアップグレードする（Upgrade Snort 2 to Snort 3）] オプションは無効化できなくなりました。 ソフトウェアのアップグレード後、設定を展開すると、対象となるすべてのデバイスが Snort 2 から Snort 3 にアップグレードされます。個々のデバイスを元に戻すことはできますが、Snort 2 は将来のリリースで非推奨になるため、今すぐ使用を停止することを強く推奨します。 カスタム侵入ポリシーやネットワーク分析ポリシーを使用しているためにデバイスが自動アップグレード対象外になる場合は、検出とパフォーマンスを向上させるために、手動で Snort 3 にアップグレードすることを強く推奨します。移行のサポートについては、お使いのバージョンの Cisco Secure Firewall Management Center Snort 3 Configuration Guide を参照してください。

機能	最小 Management Center	最小 Threat Defense	詳細
Cisco Secure Firewall 3100 の統合アップグレードおよびインストールパッケージ。	7.3.0	7.3.0	

機能	最小 Management Center	最小 Threat Defense	詳細
			再イメージ化の影響。 バージョン 7.3 では、次のように、Secure Firewall 3100 の Threat Defense のインストールおよびアップグレードパッケージを組み合わせました。 • バージョン 7.1 ～ 7.2 インストールパッケージ：isco-ftd-fp3k.*version*.SPA • バージョン 7.1 ～ 7.2 アップグレードパッケージ：Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar • バージョン 7.3 以降の統合パッケージ：Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar Threat Defense は問題なくアップグレードできますが、古い Threat Defense および ASA バージョンから Threat Defense バージョン 7.3 以上に直接再イメージ化することはできません。これは、新しいイメージタイプに必要な ROMMON アップデートが原因です。これらの古いバージョンから再イメージ化するには、古い ROMMON でサポートされているだけでなく新しい ROMMON への更新も行う、ASA 9.19 以上を「通過」する必要があります。個別の ROMMON アップデータはありません。 Threat Defense バージョン 7.3 以上にするには、次のオプションがあります。 • Threat Defense バージョン 7.1 または 7.2 からのアップグレード — 通常のアップグレードプロセスを使用します。 該当するアップグレードガイドを参照してください。 • Threat Defense バージョン 7.1 または 7.2 からの再イメージ化 — 最初に ASA 9.19 以上に再イメージ化してから、Threat Defense バージョン 7.3 以上に再イメージ化します。 『Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド』の「Threat Defense→ASA: Firepower 1000, 2100; Secure Firewall 3100」、次に「ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100」を参照してください。 • ASA 9.17 または 9.18 からの再イメージ化 — 最初に ASA 9.19 以上にアップグレードしてから、Threat Defense バージョン 7.3 以上に再イメージ化します。 『Cisco Secure Firewall ASA アップグレードガイド』を参照し、次に『Cisco Secure Firewall ASA および Secure Firewall Threat Defense

機能	最小 Management Center	最小 Threat Defense	詳細
			再イメージ化ガイド』の「ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100」を参照してください。 • Threat Defense バージョン 7.3 以上からの再イメージ化 — 通常の再イメージ化プロセスを使用します。 『Cisco FXOS トラブルシューティング ガイド（Firepower Threat Defense を実行している Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 向け）』の「Reimage the System with a New Software Version」を参照してください。
コンテンツの更新（Content Updates）			
自動 VDB ダウンロード。	7.3.0	いずれか	Management Center の初期設定では、最新の脆弱性データベース（VDB）を含むようになった、利用可能な最新のソフトウェア更新をダウンロードするための週次タスクがスケジュールされています。この週次タスクを確認し、必要に応じて調整することをお勧めします。必要に応じて、VDB を実際に更新し、構成を展開する新しい週次タスクをスケジュールしてください。 新規/変更された画面：システムで作成された [週次ソフトウェアダウンロード（Weekly Software Download）] のスケジュールされたタスクで、[脆弱性データベース（Vulnerability Database）] チェックボックスがデフォルトで有効になりました。
任意の VDB をインストールします。	7.3.0	いずれか	VDB 357 以降、その Management Center の基準 VDB までさかのぼって任意の VDB をインストールできるようになりました。 VDB を更新したら、構成の変更を展開します。利用できなくなった脆弱性、アプリケーションディテクタ、またはフィンガープリントに基づいて設定を行っている場合は、それらの設定を調べて、トラフィックが期待どおりに処理されていることを確認します。また、VDB を更新するためのスケジュールされたタスクは、ロールバックを取り消すことができることに注意してください。これを回避するには、スケジュールされたタスクを変更するか、新しい VDB パッケージを削除します。 新しい/変更された画面：**システム**（⚙）> **[更新（Updates）]** > **[製品アップデート（Product Updates）]** > **[利用可能なアップデート（Available Updates）]**で、古い VDB をアップロードすると、[インストール（Install）] アイコンの代わりに新しい [ロールバック（Rollback）] アイコンが表示されます。

表 *11* : バージョン *7.2.0* の機能

機能	詳細
Threat Defense のアップグレード	
デバイス間のアップグレードパッケージのコピー（「ピアツーピア同期」）。	Management Center や内部 Web サーバーから各デバイスにアップグレードパッケージをコピーする代わりに、Threat Defense CLI を使用してデバイス間でアップグレード パッケージをコピーできます（「ピアツーピア同期」）。この安全で信頼性の高いリソース共有は、管理ネットワークを経由しますが、Management Center には依存しません。各デバイスは、5 つのパッケージの同時転送に対応できます。 この機能は、同じバージョン 7.2.x ー 7.4.x のスタンドアロン Management Center によって管理されるバージョン 7.2 以降のスタンドアロンデバイスでサポートされています。次の場合はサポートされていません。 • コンテナインスタンス。 • デバイスの高可用性ペアとクラスタ。これらのデバイスは通常の同期プロセスの一部として、相互にパッケージを取得します。アップグレードパッケージを 1 つのグループメンバーにコピーすると、自動的にすべてのグループメンバーと同期されます。 • 高可用性 Management Center によって管理されるデバイス。 • クラウド提供型 Firewall Management Center によって管理されるが、分析モードでオンプレミス Management Center に追加されたデバイス。 • 異なるドメインのデバイス、または NAT ゲートウェイによって分離されたデバイス。 • Management Center のバージョンに関係なく、バージョン 7.1 以前からアップグレードするデバイス。 新規/変更された CLI コマンド：**configure p2psync enable**、**configure p2psync disable**、**show peers**、**show peer details**、**sync-from-peer**、**show p2p-sync-status**

機能	詳細
Threat Defense のアップグレード完了後の Snort 3 への自動アップグレード。	バージョン 7.2 以降の Management Center を使用して Threat Defense をバージョン 7.2 以降にアップグレードする場合、**Snort 2 から Snort 3 へのアップグレード**を実行するかどうかを選択できるようになりました。 ソフトウェアのアップグレード後、設定を展開すると、対象のデバイスが Snort 2 から Snort 3 にアップグレードされます。カスタム侵入ポリシーやネットワーク分析ポリシーを使用しているためにデバイスがアップグレード対象外になる場合は、検出とパフォーマンスを向上させるために、手動で Snort 3 にアップグレードすることを強く推奨します。ヘルプについては、ご使用のバージョンの Cisco Secure Firewall Management Center Snort 3 Configuration Guide を参照してください。 バージョンの制限：Threat Defense のバージョン 7.0.x または 7.1.x へのアップグレードはサポートされていません。
単一ノードクラスタのアップグレード。	デバイスのアップグレードページ（[デバイス（Devices）] > [デバイスのアップグレード（Device Upgrade）]）を使用して、アクティブノードが 1 つだけのクラスタをアップグレードできるようになりました。非アクティブ化されたノードもアップグレードされます。以前は、このタイプのアップグレードは失敗していました。この機能は、システムの更新ページ（**システム**（⚙）**[更新（Updates）]**）ではサポートされていません。 この場合、ヒットレスアップグレードもサポートされません。トラフィックフローと検査の中断は、スタンドアロンデバイスと同様に、アクティブユニットのインターフェイス設定に依存します。 サポートされるプラットフォーム：Firepower 4100/9300、Secure Firewall 3100
CLI からの Threat Defense アップグレードの復元。	Management Center とデバイス間の通信が中断された場合、デバイスの CLI から Threat Defense のアップグレードを元に戻すことができるようになりました。高可用性や拡張性の展開では、すべてのユニットを同時に復元すると、復元が成功する可能性が高くなります。CLI を使用して復元する場合は、すべてのユニットでセッションを開き、それぞれで復元が可能であることを確認してから、プロセスを同時に開始します。 **注意** CLI から復元すると、アップグレード後に行った変更によっては、デバイスと Management Center 間で設定が同期されないことがあります。これにより、後に通信と展開の問題が発生する可能性があります。 新規/変更された CLI コマンド：**upgrade revert**、**show upgrade revert-info**。
Management Center のアップグレード	

機能	詳細
Management Center のアップグレードでは、トラブルシューティング ファイルは自動的に生成されません。	時間とディスク容量を節約するために、管理センターのアップグレードプロセスでは、アップグレードの開始前にトラブルシューティング ファイルを自動的に生成しなくなりました。デバイスのアップグレードは影響を受けず、引き続きトラブルシューティング ファイルが生成される点に注意してください。 管理センターのトラブルシューティング ファイルを手動で生成するには、**システム**（⚙）>**[正常性（Health）]**>**[モニタ（Monitor）]** を選択し、左側のパネルで [Firewall Management Center] をクリックし、[View System & Troubleshoot Details]、[Generate Troubleshooting Files] を選択します。
コンテンツの更新（Content Updates）	
GeoDB を 2 つのパッケージに分割。	2022 年 5 月、バージョン 7.2 リリースの直前に、GeoDB が 2 つのパッケージに分割されました。IP アドレスを国/大陸にマッピングする国コードパッケージと、ルーティング可能な IP アドレスに関連付けられた追加のコンテキストデータを含む IP パッケージです。IP パッケージのコンテキストデータには、追加のロケーションの詳細に加えて、ISP、接続タイプ、プロキシタイプ、ドメイン名などの接続情報を含めることができます。 バージョン 7.2.0 から 7.2.5 までの Management Center にインターネットアクセスがあり、定期的な更新を有効にしている場合、または シスコ サポートおよびダウンロード サイト から 1 回限りの更新を手動で開始した場合、両方のパッケージが自動的に取得されます。バージョン 7.2.6 以降または 7.4.0 以降では、システムに IP パッケージを取得させるかどうかを設定できます。 エアギャップ展開などで更新を手動でダウンロードする場合、パッケージを個別にインポートする必要があります。 • 国コードパッケージ：Cisco_GEODB_Update-*date-build*.sh.REL.tar • IP パッケージ：Cisco_IP_GEODB_Update-*date-build*.sh.REL.tar **[ヘルプ（Help）]**（?）>**[バージョン情報（About）]** には、システムで現在使用されているパッケージのバージョンが一覧表示されます。

表 *12 :* バージョン *7.1.0* の機能

機能	詳細
Threat Defense のアップグレード	

機能	詳細
正常なデバイスアップグレードを元に戻します。	メジャーおよびメンテナンスアップグレードを FTD に戻すことができるようになりました。復元すると、ソフトウェアは、最後のアップグレードの直前の状態に戻ります（スナップショットとも呼ばれます）。パッチのインストール後にアップグレードを元に戻すと、パッチだけでなく、メジャーアップグレードやメンテナンスアップグレードも元に戻されます。 **重要** 元に戻す必要がある可能性があると思われる場合は、**システム**（⚙）> **[更新（Updates）]** ページを使用して FTD をアップグレードする必要があります。[システムの更新（System Updates）] ページは、[アップグレード後の復元を有効にする（Enable revert after successful upgrade）] オプションを有効にできる唯一の場所です。このオプションでは、アップグレードの開始時に復元スナップショットを保存するようにシステムが設定されます。これは、[デバイス（Devices）]>[デバイスのアップグレード（Device Upgrade）] ページでウィザードを使用する通常の推奨とは対照的です。 この機能は、コンテナインスタンスではサポートされません。 必要最低限の FTD：7.1
クラスタ化された高可用性デバイスのアップグレードワークフローの改善。	クラスタ化された高可用性デバイスのアップグレードワークフローが次のように改善されました。 • アップグレードウィザードは、個々のデバイスとしてではなく、グループとして、クラスタ化された高可用性ユニットを正しく表示するようになりました。システムは、発生する可能性のあるグループ関連の問題を特定し、報告し、事前に修正を要求できます。たとえば、Firepower Chassis Manager で非同期の変更を行った場合は、Firepower 4100/9300 のクラスタをアップグレードできません。 • アップグレードパッケージをクラスタおよび高可用性ペアにコピーする速度と効率が向上しました。以前は、FMC はパッケージを各グループメンバーに順番にコピーしていました。これで、グループメンバーは通常の同期プロセスの一部として、相互にパッケージを取得できるようになりました。 • クラスタ内のデータユニットのアップグレード順序を指定できるようになりました。コントロールユニットは常に最後にアップグレードされます。

表 *13* : バージョン *7.0.0* の機能

機能	詳細
Threat Defense のアップグレード	

機能	詳細
FTDのアップグレードパフォーマンスとステータスレポートの改善。	FTD のアップグレードがより簡単かつ確実に、より少ないディスク容量で実行できるようになりました。メッセージセンターの新しい [アップグレード（Upgrades）] タブでは、アップグレードステータスとエラーレポートがさらに強化されています。

機能	詳細
FTDデバイスのわかりやすいアップグレードワークフロー。	FMC の新しいデバイス アップグレード ページ（[デバイス（Devices）] > [デバイスアップグレード（Device Upgrade）]）には、バージョン 6.4 以降の FTD デバイスをアップグレードするためのわかりやすいウィザードがあります。アップグレードするデバイスの選択、アップグレードパッケージのデバイスへのコピー、互換性と準備状況の確認など、アップグレード前の重要な段階を順を追って説明します。 開始するには、[デバイス管理（Device Management）] ページ（[デバイス（Devices）] > [デバイス管理（Device Management）] > [アクションの選択（Select Action）]）で新しい [Firepower ソフトウェアのアップグレード（Upgrade Firepower Software）] アクションを使用します。 続行すると、選択したデバイスに関する基本情報と、現在のアップグレード関連のステータスが表示されます。表示内容には、アップグレードできない理由が含まれます。あるデバイスがウィザードの 1 つの段階に「合格」しない場合、そのデバイスは次の段階には表示されません。 ウィザードから移動しても、進行状況は保持されます。ただし、管理者アクセス権を持つ他のユーザーはウィザードをリセット、変更、または続行できます。 （注） FTD のアップグレードパッケージの場所をアップロードまたは指定するには、引き続き **システム**（⚙）> **[更新（Updates）]**を使用する必要があります。また、[システム更新（System Updates）]ページを使用して、FMC 自体、およびすべての非 FTD 管理対象デバイスをアップグレードする必要があります。 （注） バージョン 7.0 では、ウィザードにクラスタまたは高可用性ペアのデバイスが正しく表示されません。これらのデバイスは 1 つのユニットとして選択してアップグレードする必要がありますが、ウィザードにはスタンドアロンデバイスとして表示されます。デバイスのステータスとアップグレードの準備状況は、個別に評価および報告されます。つまり、1 つのユニットが「合格」して次の段階に進んでいるように見えても、他のユニットは合格していない可能性があります。ただし、それらのデバイスはグループ化されたままです。1 つのユニットで準備状況チェックを実行すると、すべてのユニットで実行されます。1 つユニットでアップグレードを開始すると、すべてのユニットで開始されます。 時間がかかるアップグレードの失敗を回避するには、[次へ（Next）] をクリックする前に、すべてのグループメンバーがウィザードの次のステップに進む準備ができていることを手動で確認します。

機能	詳細
多くのFTDデバイスを一度にアップグレードします。	FTD アップグレードウィザードでは、次の制限が解除されます。 • デバイスの同時アップグレード。 一度にアップグレードできるデバイスの数は、同時アップグレードを管理するシステムの機能ではなく、管理ネットワークの帯域幅によって制限されます。以前は、一度に 5 台を上回るデバイスをアップグレードしないことを推奨していました。 **重要** この改善は、FTD バージョン 6.7 以降へのアップグレードでのみ確認できます。デバイスを古いFTDリリースにアップグレードする場合は、新しいアップグレードウィザードを使用している場合でも、一度に 5 台のデバイスに制限することをお勧めします。 • デバイスモデルによるアップグレードのグループ化。 システムが適切なアップグレードパッケージにアクセスできる限り、すべての FTD モデルのアップグレードを同時にキューに入れて呼び出すことができます。 以前は、アップグレードパッケージを選択し、そのパッケージを使用してアップグレードするデバイスを選択していました。つまり、アップグレードパッケージを共有している場合にのみ、複数のデバイスを同時にアップグレードできました。たとえば、2 台の Firepower 2100 シリーズデバイスは同時にアップグレードできますが、Firepower 2100 シリーズと Firepower 1000 シリーズはアップグレードできません。

表 *14 :* バージョン *6.7.0* の機能

機能	詳細
Threat Defense のアップグレード	
アップグレードでディスク容量を節約するためにPCAP ファイルが削除される。	アップグレードにより、ローカルに保存された PCAP ファイルが削除されるようになりました。アップグレードするには、十分な空きディスク容量が必要です。これがない場合、アップグレードは失敗します。

機能	詳細
FTDアップグレードステータス レポートとキャンセル/再試行オプションの改善。	[デバイス管理（Device Management）] ページで、進行中の FTD デバイスアップグレードと準備状況チェックのステータス、およびアップグレードの成功/失敗の 7 日間の履歴を確認できるようになりました。メッセージセンターでは、拡張ステータスとエラーメッセージも提供されます。 デバイス管理とメッセージセンターの両方からワンクリックでアクセスできる新しい [Upgrade Status] ポップアップに、残りのパーセンテージ/時間、特定のアップグレード段階、成功/失敗データ、アップグレードログなどの詳細なアップグレード情報が表示されます。 また、このポップアップで、失敗したアップグレードまたは進行中のアップグレードを手動でキャンセル（[Cancel Upgrade]）することも、失敗したアップグレードを再試行（[Retry Upgrade]）することもできます。アップグレードをキャンセルすると、デバイスはアップグレード前の状態に戻ります。 （注） 失敗したアップグレードを手動でキャンセルまたは再試行できるようにするには、FMC を使用して FTD デバイスをアップグレードするときに表示される新しい自動キャンセルオプションを無効にする必要があります（[Automatically cancel on upgrade failure and roll back to the previous version]）。オプションを有効にすると、アップグレードが失敗した場合、デバイスは自動的にアップグレード前の状態に戻ります。 パッチの自動キャンセルはサポートされていません。HA またはクラスタ展開では、自動キャンセルは各デバイスに個別に適用されます。つまり、1 つのデバイスでアップグレードが失敗した場合、そのデバイスだけが元に戻ります。 新規/変更された画面： • FTD アップグレードパッケージの **システム**（⚙） > **[更新（Updates）]** > **[製品の更新（Product Updates）]** > **[使用可能な更新（Available Updates）]** > **[インストール（Install）]** アイコン • **[Devices]** > **[Device Management]** > **[Upgrade]** • **[Message Center] > [Tasks]** 新規/変更された CLI コマンド：**show upgrade status detail**、**show upgrade status continuous**、**show upgrade status**、**upgrade cancel**、**upgrade retry**
コンテンツの更新（Content Updates）	

機能	詳細
カスタム侵入ルールのインポートでルール競合の際に警告表示。	カスタム（ローカル）侵入ルールをインポートする場合、FMC がルールの競合について警告するようになりました。以前は、システムは競合の原因となるルールをサイレントにスキップしていました。ただし、競合のあるルールのインポートが完全に失敗するバージョン 6.6.0.1 は除きます。 [ルールの更新（Rule Updates）] ページで、ルールのインポートに競合があった場合は、[ステータス（Status）] 列に警告アイコンが表示されます。詳細については、警告アイコンの上にポインタを置いて、ツールチップを参照してください。 既存のルールと同じ SID/リビジョン番号を持つ侵入ルールをインポートしようとすると、競合が発生することに注意してください。カスタムルールの更新バージョンには必ず新しいリビジョン番号を付けてください。 新規/変更された画面：**システム**（⚙） > **[更新（Updates）]** > **[ルールの更新（Rule Updates）]**に警告アイコンが追加されました。

表 *15* : バージョン *6.6.0* の機能

機能	詳細
Threat Defense のアップグレード	
内部 Web サーバーから FTD アップグレードパッケージを取得します。	FTD デバイスは、FMC からではなく、独自の内部 Web サーバーからアップグレードパッケージを取得できるようになりました。これは、FMC とそのデバイスの間の帯域幅が制限されている場合に特に役立ちます。また、FMC 上の領域も節約できます。 （注） この機能は、バージョン 6.6+ を実行している FTD デバイスでのみサポートされています。バージョン 6.6 へのアップグレードではサポートされておらず、FMC または従来のデバイスでもサポートされていません。 新規/変更された画面：アップグレードパッケージをアップロードするページに、[ソフトウェアアップデートソースの指定（Specify software update source）] オプションを追加しました。
コンテンツの更新（Content Updates）	
初期セットアップ中の自動VDB更新。	新規または再イメージ化された FMC をセットアップすると、システムは自動的に脆弱性データベース（VDB）の更新を試みます。 これは1回限りの操作です。FMCがインターネットにアクセスできる場合は、自動の定期 VDB 更新のダウンロードとインストールを実行するようにタスクをスケジュールしておくことを推奨します。

表 *16* : バージョン *6.5.0* の機能

機能	詳細
コンテンツの更新（Content Updates）	
ソフトウェアの自動ダウンロードとGeoDB の更新。	新規または再イメージ化されたFMC を設定すると、システムは自動的に次のスケジュールを設定します。 • FMC とその管理対象デバイスのソフトウェアアップデートをダウンロードする週次タスク。 • GeoDB の週次更新。 タスクはUTC でスケジュールされるため、いつ現地で実行されるかは、日付と場所によって異なります。また、タスクはUTC でスケジュールされるため、サマータイムなど、所在地で実施される場合がある季節調整に合わせて調節されることもありません。このような影響を受ける場合、スケジュールされたタスクは、現地時間を基準とすると、夏期では冬期の場合よりも 1 時間「遅れて」実行されることになります。自動スケジュール設定を確認し、必要に応じて調整することをお勧めします。

表 *17* : バージョン *6.4.0* の機能

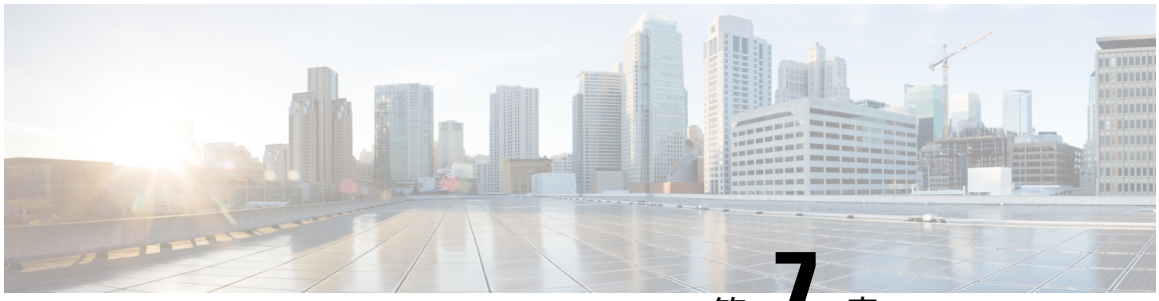
機能	詳細
Management Center のアップグレード	
アップグレードがスケジュールされたタスクを延期する。	Management Center のアップグレードプロセスによって、スケジュールされたタスクが延期されるようになりました。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。 （注） アップグレードを開始する前に、実行中のタスクが完了していることを確認する必要があります。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。 この機能は、サポートされているバージョンからのすべてのアップグレードでサポートされていることに注意してください。これには、バージョン6.4.0.10 以降のパッチ、バージョン 6.6.3 以降のメンテナンスリリース、およびバージョン 6.7.0 以降が含まれます。この機能は、サポートされていないバージョンからサポートされているバージョンへのアップグレードではサポートされていません。
コンテンツの更新（Content Updates）	

機能	詳細
署名済みのSRU、VDB、およびGeoDBの更新。	正しい更新ファイルを使用していることが確認できるため、バージョン6.4以降では署名済みの更新を侵入ルール（SRU）、脆弱性データベース（VDB）、および地理位置情報データベース（GeoDB）が使用されます。以前のバージョンでは、引き続き未署名の更新が使用されます。 シスコサポートおよびダウンロードサイトから手動で更新をダウンロードしない限り（たとえば、エアギャップ導入環境の場合）、機能の違いはわかりません。ただし、SRU、VDB、およびGeoDBの更新を手動でダウンロードしてインストールする場合は、必ず現在のバージョンに対応した正しいパッケージをダウンロードしてください。 署名付きの更新ファイルの先頭は、以下のように「Sourcefire」ではなく「Cisco」で、末尾は .sh ではなく .sh.REL.tar です。 • SRU：Cisco_Firepower_SRU-*date-build*-vrt.sh.REL.tar • VDB：Cisco_VDB_Fingerprint_Database-4.5.0-*version*.sh.REL.tar • GeoDB：Cisco_GEODB_Update-*date-build*.sh.REL.tar シスコは、署名なしの更新を必要とするバージョンのサポートが終了するまで、署名付きと署名なしの両方の更新を提供します。署名付きの（.tar）パッケージは解凍しないでください。古いFMCまたはASA FirePOWERデバイスに署名付きの更新を誤ってアップロードした場合は、手動で削除する必要があります。パッケージを残しておくと、ディスク領域が占有されるため、今後のアップグレードで問題が発生する可能性もあります。

表 *18 :* バージョン *6.2.3* の機能

機能	詳細
デバイスのアップグレード	
アップグレードの前に、アップグレードパッケージを管理対象デバイスにコピーします。	実際のアップグレードを実行する前に、FMCから管理対象デバイスにアップグレードパッケージをコピー（またはプッシュ）できるようになりました。帯域幅の使用量が少ない時間帯やアップグレードのメンテナンス期間外でプッシュできるため、この機能は便利です。 高可用性デバイス、クラスタデバイス、またはスタック構成デバイスにプッシュすると、アップグレードパッケージは最初にアクティブ/コントロール/プライマリに送信され、次にスタンバイ/データ/セカンダリに送信されます。 新規/変更された画面：**システム**（⚙）>**[更新（Updates）]**
コンテンツの更新（Content Updates）	

機能	詳細
VDB の更新前に、Snort の再起動について FMC から警告されます。	脆弱性データベース（VDB）の更新で Snort プロセスが再起動することが、FMC から警告されるようになりました。これにより、トラフィック インスペクションが中断され、管理対象デバイスによるトラフィックの処理方法によっては、トラフィックフローが中断される可能性があります。メンテナンス期間中など、都合の良い期間までインストールをキャンセルすることができます。 次のようなときに警告が表示される可能性があります。 • VDB をダウンロードして手動でインストールした後。 • スケジュールされたタスクを作成して VDB をインストールする場合。 • たとえば、以前にスケジュールされたタスクの実行中に、またはソフトウェアアップグレードの一部として、VDB がバックグラウンドでインストールされる場合。



第 7 章

ライセンス

この章では、さまざまなライセンスタイプ、サービスサブスクリプション、ライセンス要件などに関する詳細情報が提供されています。

（注） Management Center は、プラットフォームライセンスとして、スマートライセンスまたはレガシー PAK（製品アクティベーションキー）ライセンスをサポートしています。PAK ライセンスの使用についての詳細は、レガシー Management Center PAK ベースのライセンスの設定 （356 ページ）を参照してください。

ライセンスについて

シスコ スマート ライセンシングは、シスコ ポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンスモデルです。また、これは安全です。ユーザがアクセスできるものを制御できます。スマートライセンスを使用すると、次のことが可能になります。

- **簡単なアクティベーション**：スマートライセンスは、組織全体で使用できるソフトウェアライセンスのプールを確立します。PAK（製品アクティベーションキー）は不要です。

- **管理の統合**：My Cisco Entitlements（MCE）は、使いやすいポータルですべてのシスコ製品とサービスの完全なビューを提供するので、取得したもの、使用しているものを常に把握できます。
- **ライセンスの柔軟性**：ソフトウェアはハードウェアにノードロックされていないため、必要に応じてライセンスを簡単に使用および転送できます。

スマートライセンスを使用するには、まず Cisco Software Central でスマートアカウントを設定する必要があります（software.cisco.com）。

シスコライセンスの概要については詳しくは、cisco.com/go/licensingguide を参照してください。

Smart Software Manager とアカウント

1 つ以上のライセンスを購入する場合は、それらのライセンスを Smart Software Manager（https://software.cisco.com/#module/SmartLicensing）で管理します。Smart Software Manager を使用すると、組織のプライマリアカウントを作成できます。まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager を使用すると、組織のプライマリアカウントを作成できます。手順については、「シスコアカウントの作成」を参照してください。

デフォルトでは、ライセンスはプライマリアカウントの下のデフォルト仮想アカウントに割り当てられます。アカウントの管理者として、たとえば、地域、部門、または子会社ごとに、追加の仮想アカウントを作成できます。複数のバーチャルアカウントは、多数のライセンスおよびデバイスを管理するために役立ちます。

ライセンスは、バーチャルアカウント別に管理します。バーチャルアカウントに割り当てられているライセンスを使用できるのは、そのバーチャルカウントのデバイスのみです。追加のライセンスが必要な場合は、別の仮想アカウントから未使用のライセンスを転用できます。仮想アカウント間でデバイスを転送することもできます。

エアギャップ展開のライセンスのオプション

次の表に、インターネットにアクセスできない環境で使用可能なライセンスオプションを比較して示します。特定の状況については、販売担当者が他のアドバイスをできる場合があります。

表 *19*：エアギャップ ネットワークのライセンス オプションの比較

Smart Software Manager オンプレミス	特定のライセンスの予約
大量の製品に対する拡張性	少数のデバイスに最適
ライセンス管理、使用状況、および資産管理の可視性を自動化	使用状況および資産管理の可視性の制限
デバイスを追加するための運用コストの増加なし	デバイスを追加するための経時的な運用コストが線形

Smart Software Manager オンプレミス	特定のライセンスの予約
柔軟性、使いやすさ、少ないオーバーヘッド	移動、追加、および変更の際の管理および手動によるオーバーヘッドの多さ
初期およびさまざまな期限切れ状態でコンプライアンス不適合ステータスが許可される	コンプライアンス不適合ステータスはシステムの動作に影響を与える
詳細については、「Management Center の Smart Software Manager オンプレミスへの登録 （332 ページ）」を参照してください。	詳細については、「特定ライセンス予約（SLR）の設定 （343 ページ）」を参照してください。

Management Center およびデバイスのライセンシングの仕組み

Management Center は Smart Software Manager に登録し、各管理対象デバイスにライセンスを割り当てます。デバイスは、Smart Software Manager に直接登録しません。

物理 Management Center は、それ自体の使用にはライセンスを必要としません。Management Center Virtual にはプラットフォームライセンスが必要です。

Smart Software Manager との定期的な通信

製品ライセンスの権限付与を維持するために、製品は Smart Software Manager と定期的に通信する必要があります。

製品インスタンス登録トークンを使用して、Management Center を Smart Software Manager に登録できます。Smart Software Manager は、Management Center と Smart Software Manager が通信するための ID 証明書を発行します。この証明書の有効期間は 1 年ですが、6 ヵ月ごとに更新されます。ID 証明書の有効期限が切れた場合（1 年間通信がなかった場合）、Management Center がアカウントから削除されることがあります。

Management Center は Smart Software Manager と定期的に通信します。Smart Software Manager で変更を加えた場合は、Management Center 上で認証を更新すると、その変更がすぐに適用されます。また、スケジュールどおりにManagement Centerが通信するのを待つこともできます。

Management Center は、Smart Software Manager に直接インターネットアクセスできるか、エアギャップ展開のライセンスのオプション （302 ページ）で説明されているいずれかのオプションを使用する必要があります。非エアギャップ展開では、通常のライセンスに関する通信は30日ごとに行われますが、これには猶予期間があり、Management Centerは Smart Software Manager と通信することなく最大で 90 日間は動作します。90 日が経過する前に Management Center が Smart Software Manager と通信することを確認してください。そうでない場合、Management Center は未登録の状態に戻ります。

評価モード（Evaluation Mode）

Management Center は、Smart Software Manager への登録の前に 90 日間、評価モードで動作します。管理対象デバイスに機能ライセンスを割り当てることができ、評価モードの期間中はコンプライアンスに準拠した状態が維持されます。この期間が終了すると、Management Center は登録解除されます。

Management Center を Smart Software Manager に登録すると、評価モードが終了します。後で Management Center の登録を解除すると、最初に 90 日間すべてを使用していなくても、評価モードを再開することはできません。

未登録状態の詳細については、未登録状態 （304 ページ）を参照してください。

（注） 高度暗号化（3DES/AES）の評価ライセンスを受け取ることはできません。高度暗号化（3DES/AES）ライセンスを有効にするエクスポートコンプライアンス トークンを受け取るには、Smart Software Manager に登録する必要があります。

コンプライアンス逸脱状態

Management Center は、次の状況においてコンプライアンス違反になる可能性があります。

- 使用超過：管理対象デバイスまたは Management Center Virtual が、利用できないライセンスを使用している場合。
- ライセンスの有効期限切れ：管理対象デバイスの時間ベースライセンスの有効期限が切れている場合。

コンプライアンス違反状態になると、次のような影響が見られます。

- Management Center Virtual プラットフォームライセンス：動作は影響を受けません。
- すべての管理対象デバイスライセンス：動作は影響を受けません。

ライセンスの問題を解決すると、Management Center は、Smart Software Manager での定期的にスケジュールされた承認後に、コンプライアンス準拠状態になったことを示します。承認を強制するには、**システム**（⚙）> **[ライセンス（Licenses）]** > **[スマートライセンス（Smart Licenses）]** ページで [再承認（Re-Authorize）] をクリックします。

未登録状態

Management Center は、次の状況で登録解除される可能性があります。

- 評価モードの有効期限：評価モードは 90 日後に期限切れになります。
- Management Center の手動登録解除

- Smart Software Manager との通信の欠如：Management Center は、Smart Software Manager と 1 年間通信していません。注：90 日後に Management Center 認証は期限切れになりますが、1 年以内に通信を正常に再開して自動的に再認証することができます。1 年後、ID 証明書の有効期限が切れ、Management Center はアカウントから削除されるため、手動で Management Center を再登録する必要があります。

未登録状態では、Management Center はライセンスを必要とする機能の設定変更をデバイスに展開できません。

エンドユーザーライセンス契約書

本製品の使用について規定するシスコ エンドユーザー ライセンス契約書（EULA）および適用される補足契約書（SEULA）は、http://www.cisco.com/go/softwareterms から入手できます。

ライセンスのタイプと制約事項

ここでは、使用可能なライセンスのタイプについて説明します。

表 *20*：スマート ライセンス

自分で割り当てるライセンス	期間	付与される機能
Essentials	永久かサブスクリプションか （注） Essentials サブスクリプション ライセンスは、Threat Defense Virtual でのみサポートされます。	特定のライセンス予約と Cisco Secure Firewall 3100/4200 を除き、Essentials 永続的ライセンスがすべての Threat Defense に自動的に割り当てられます。 ユーザーおよびアプリケーション制御 スイッチングとルーティング NAT 詳細は、「Essentials ライセンス （307 ページ）」を参照してください。
IPS	サブスクリプション	侵入検知と防御 ファイル制御 セキュリティ インテリジェンス フィルタリング 詳細については、「IPS ライセンス （309 ページ）」を参照してください。

自分で割り当てるライセンス	期間	付与される機能
マルウェア防御	サブスクリプション	マルウェア防御 Secure Malware Analytics ファイル ストレージ （IPS ライセンスはマルウェア防御ライセンスの前提条件です）。 詳細については、マルウェア防御ライセンス （308 ページ） および Cisco Secure Firewall Management Center デバイス構成ガイドの「*License Requirements for File and Malware Policies*」を参照してください。
通信事業者	Firepower 4100/9300、Cisco Secure Firewall 3100/4200、および Threat Defense Virtual のサブスクリプション	Diameter、GTP/GPRS、M3UA、および SCTP インスペクション 詳細については、キャリア ライセンス （310 ページ）を参照してください。
URL フィルタリング	サブスクリプション	カテゴリとレピュテーションに基づく URL フィルタリング 詳細は、「URL フィルタリング ライセンス （311 ページ）」を参照してください。 （IPS ライセンスは URL フィルタリング ライセンスの前提条件です）。
Management Center Virtual	• 通常のスマートライセンス：永続 • 特定のライセンス予約：サブスクリプション	プラットフォームライセンスによって、Management Center Virtual が管理できるデバイスの数が決まります。 詳細は、「Management Center Virtual ライセンス （307 ページ）」を参照してください。
輸出管理機能	永続	国家安全保障、外交政策、反テロリズムに関する法律や規制の対象となる機能。「輸出規制対象の機能のライセンス （313 ページ）」を参照してください。

自分で割り当てるライセンス	期間	付与される機能
リモート アクセス VPN： • Secure Client Premier • Secure Client Advantage • Secure Client VPN のみ	サブスクリプションまたは永続	リモート アクセス VPN の設定リモート アクセス VPN を設定するには、アカウントによるエクスポート制御機能を許可する必要があります。デバイスを登録するときに、エクスポート要件を満たすかどうかを選択します。Threat Defense は、任意の有効な セキュアクライアント ライセンスを使用できます。使用できる機能はライセンスタイプによって異なります。 詳細については、セキュアクライアント ライセンス （312 ページ）およびCisco Secure Firewall Management Center デバイス構成ガイドの「*VPN Licensing*」 を参照してください。

（注） サブスクリプション ライセンスは、期間ベースのライセンスです。

Management Center Virtual ライセンス

Management Center Virtual には、管理できるデバイスの数に対応するプラットフォームライセンスが必要です。

Management Center Virtual は、スマートライセンスをサポートしています。

通常のスマートライセンスでは、これらのライセンスは永続的ライセンスです。

特定のライセンス予約では、これらのライセンスはサブスクリプションベースです。

（注） FMCv の新しいデバイスのアドオンライセンス要件がある場合は、追加のデバイスをサポートする上位の Management Center Virtual モデルに移行することをお勧めします。

Essentials ライセンス

Essentials ライセンスでは、次のことができます。

- スイッチングおよびルーティング（DHCP リレーおよび NAT を含む）を実行するようにデバイスを設定する
- デバイスをハイアベイラビリティペアとして設定する

- クラスタリングを設定する
- アクセスコントロールルールにユーザーとアプリケーションの条件を追加することで、ユーザーとアプリケーションの制御を実装する
- 脆弱性データベース（VDB）および地理位置情報データベース（GeoDB）を更新します。
- SRU/LSP などの侵入ルールをダウンロードします。ただし、IPS ライセンスが有効になっていない限り、アクセス コントロール ポリシーまたは侵入ポリシーを持つルールをデバイスに展開することはできません。

Cisco Secure Firewall 3100/4200

Cisco Secure Firewall 3100/4200 を購入すると、Essentials ライセンスが取得されます。

他のモデル

特定のライセンス予約を使用する展開の場合を除き、Essentialsライセンスはデバイスを Management Center に登録したときに、アカウントに自動的に追加されます。特定のライセンス予約の場合、アカウントにEssentialsライセンスを追加する必要があります。

マルウェア防御ライセンス

マルウェア防御ライセンスでは、マルウェア防御およびSecure Malware Analyticsを実行できます。この機能では、デバイスを使用して、ネットワーク上で伝送されるファイルのマルウェアを検出してブロックできます。この機能ライセンスをサポートするために、スタンドアロンサブスクリプションとしてマルウェア防御（AMP）サービスサブスクリプションを購入できます。また、IPS （TM）や IPS および URL フィルタリング（TMC）サブスクリプションと組み合わせて購入することもできます。IPS ライセンスは、マルウェア防御ライセンスの前提条件です。

（注） マルウェア防御ライセンスが有効になっている管理対象デバイスは、動的分析を設定していない場合でも、定期的に Secure Malware Analytics Cloud への接続を試行します。このため、デバイスの [インターフェイス トラフィック（Interface Traffic）] ダッシュボード ウィジェットには、送信済みトラフィックが表示されます。これは正常な動作です。

ファイル ポリシーの一部として マルウェア防御 を設定し、その後 1 つ以上のアクセス コントロール ルールを関連付けます。ファイル ポリシーでは、特定のアプリケーション プロトコルを介した特定のタイプのユーザーによるファイルのアップロードとダウンロードを検出できます。マルウェア防御 では、ローカル マルウェア分析とファイルの事前分類を使用して、それらの限られた一連のファイルタイプを検査できます。特定のファイルタイプをダウンロードして Secure Malware Analytics クラウドにアップロードして、動的 Spero 分析でマルウェアが含まれているかどうかを判別することもできます。これらのファイルでは、ファイルがネットワーク内で経由する詳細なパスを示すネットワーク ファイル トラジェクトリを表示できます。マルウェア防御 ライセンスでは、ファイル リストに特定のファイルを追加し、そのファイル リ

ストをファイルポリシー内で有効にすることもできます。これにより、検出時にこれらのファイルを自動的に許可またはブロックできます。

マルウェア防御ライセンスが必要なのは、マルウェア防御 および Secure Malware Analytics を展開する場合のみであることに注意してください。マルウェア防御ライセンスがなければ、Management Center は Secure Malware Analytics Cloud から Secure Endpoint マルウェアイベントおよび侵害の兆候（IOC）を受信できます。

Cisco Secure Firewall Management Center デバイス構成ガイド のファイルおよびマルウェアポリシーのライセンス要件で重要な情報も参照してください。

このライセンスを無効にすると、次の状況が発生します。

- システムは Secure Malware Analytics Cloud への問い合わせを停止し、Secure Malware Analytics Cloud から送信される遡及的イベントの確認応答も停止します。
- 既存のアクセス コントロール ポリシーに マルウェア防御 構成が含まれている場合は、それらのポリシーを再展開することができません。
- マルウェア防御ライセンスが無効にされた後、システムが既存のキャッシュファイルの性質を使用できるのはごく短時間のみです。この時間枠の経過後、システムは `Unavailable` という性質をこれらのファイルに割り当てます。

ライセンスの有効期限が切れると、前述の機能に対する利用資格が停止し、Management Center はコンプライアンス違反の状態に移行します。

IPS ライセンス

IPS ライセンスでは、侵入の検出と防御、ファイル制御、およびセキュリティ インテリジェンスのフィルタリングを実行できます。

- 侵入検知および防御により、侵入とエクスプロイトを検出するためネットワーク トラフィックを分析できます。またオプションで違反パケットをドロップできます。
- ファイル制御により、特定のアプリケーションプロトコルを介した特定タイプのファイルを検出し、オプションでこれらのファイルのアップロード（送信）またはダウンロード（受信）をユーザーからブロックできます。マルウェア防御ライセンスが必要なマルウェア防御 では、マルウェアの性質に基づいて限られたファイルタイプを検査およびブロックすることもできます。
- セキュリティ インテリジェンス フィルタリングにより、トラフィックをアクセスコントロールルールによる分析対象にする前に、特定の IP アドレス、URL、および DNS ドメイン名をブロック（その IP アドレスとの間のトラフィックを拒否）できます。ダイナミックフィードにより、最新の情報に基づいて接続をただちにブロックできます。オプションで、セキュリティ インテリジェンス フィルタリングに「モニターのみ」設定を使用できます。

IPS ライセンスは、スタンドアロン サブスクリプション（T）として、または URL フィルタリング（TC）、マルウェア防御（TM）、あるいはその両方（TMC）と組み合わせて購入できます。

このライセンスを無効にすると、次の状況が発生します。

- Management Center で、影響を受けたデバイスからの侵入イベントとファイルイベントの確認応答が停止されます。結果として、トリガー条件としてこれらのイベントを使用する相関ルールがトリガーしなくなります。
- また、Management Center はシスコ提供またはサードパーティのセキュリティ インテリジェンス情報を取得するためにインターネットに接続しなくなります。
- IPS を再度有効にするまでは、既存の侵入ポリシーを適用し直すことができません。

ライセンスの有効期限が切れると、前述の機能に対する利用資格が停止し、Management Center はコンプライアンス違反の状態に移行します。

キャリア ライセンス

キャリアライセンスでは、以下のプロトコルのインスペクションが有効になります。

- Diameter：Diameter は、LTE（Long Term Evolution）および IMS（IP Multimedia Subsystem）用の EPS（Evolved Packet System）などの次世代モバイルと固定電気通信ネットワークで使用される認証、認可、およびアカウンティング（AAA）プロトコルです。RADIUS や TACACS がこれらのネットワークで Diameter に置き換えられます。
- GTP/GPRS：GPRS トンネリングプロトコル（GTP）は、General Packet Radio Service（GPRS）トラフィック用に GSM、UMTS、および LTE ネットワークで使用されます。GTP は、トンネル制御および管理プロトコルを提供します。このプロトコルによるトンネルの作成、変更、および削除により、モバイル ステーションに GPRS ネットワーク アクセスが提供されます。GTP は、ユーザー データ パケットの伝送にもトンネリング メカニズムを使用します。
- M3UA：MTP3 User Adaptation（M3UA）は、Signaling System 7（SS7）Message Transfer Part 3（MTP3）レイヤと連動する IP ベースアプリケーション用の SS7 ネットワークへのゲートウェイを提供するクライアント/サーバープロトコルです。M3UA により、IP ネットワーク上で SS7 ユーザー パート（ISUP など）を実行することが可能になります。
- SCTP：Stream Control Transmission Protocol（SCTP）は、IP ネットワーク上で SS7 プロトコルをサポートするトランスポート層プロトコルです。4G LTE モバイル ネットワーク アーキテクチャをサポートしています。SCTP は、複数の同時ストリーム、多重化ストリームを処理でき、より多くのセキュリティ機能を提供します。

（注） デバイスでこのライセンスを有効にした後、FlexConfig ポリシーを使用してプロトコルインスペクションを有効にします。

キャリアライセンス PID は、デバイスモデルごとではなく、ファミリごとに利用できます。評価モードまたはスマートライセンスで、デバイスごとにこのライセンスを有効にすることができます。

Firepower 4100/9300、Cisco Secure Firewall 3100/4200、および Threat Defense Virtual のキャリアライセンスは期間ベースです。このライセンスは、特定のライセンス予約もサポートしています。

サポートされるデバイス

キャリアライセンスをサポートするデバイスは次のとおりです。

- Secure Firewall 3110
- Secure Firewall 3120
- Secure Firewall 3130
- Secure Firewall 3140
- Firepower 4112
- Firepower 4115
- Firepower 4125
- Firepower 4145
- Cisco Secure Firewall 4215
- Cisco Secure Firewall 4225
- Cisco Secure Firewall 4245
- Firepower 9300
- Threat Defense Virtual

URL フィルタリング ライセンス

URL フィルタリング ライセンスにより、モニター対象ホストにより要求される URL に基づいて、ネットワーク内を移動できるトラフィックを判別するアクセスコントロールルールを作成できます。この機能ライセンスをサポートするために、スタンドアロンサブスクリプションとして URL フィルタリング サービスサブスクリプションを購入できます。また、IPS （TC）や脅威およびマルウェア防御（TMC）サブスクリプションと組み合わせて購入することもできます。IPS ライセンスが、このライセンスの前提条件です。

ヒント URL フィルタリング ライセンスがない状態で、許可またはブロックする個別 URL または URL グループを指定できます。このオプションにより、Web トラフィックをカスタムできめ細かく制御できますが、URL カテゴリおよびレピュテーションデータをネットワークトラフィックのフィルタ処理に使用することはできません。

URL フィルタリング ライセンスがない状態でも、アクセスコントロールルールにカテゴリベースの URL 条件およびレピュテーションベースの URL 条件を追加できますが、Management Center は URL 情報をダウンロードしません。最初に URL フィルタリング ライセンスを

Management Center に追加し、ポリシー適用対象デバイスで有効にするまでは、アクセス コントロール ポリシーを展開できません。

このライセンスを無効にすると、次の状況が発生します。

- URL フィルタリングにアクセスできなくなる可能性があります。
- URL 条件によるアクセス コントロール ルールが、URL のフィルタリングをただちに停止します。
- Management Center で URL データの更新をダウンロードできなくなります。
- 既存のアクセス コントロール ポリシーに、カテゴリ ベースまたはレピュテーション ベースの URL 条件を含むルールが含まれている場合は、それらのポリシーを再展開することができません。

ライセンスの有効期限が切れると、前述の機能に対する利用資格が停止し、Management Center はコンプライアンス違反の状態に移行します。

セキュアクライアント ライセンス

セキュアクライアント および標準ベースの IPSec/IKEv2 を使用して、リモートアクセス VPN を設定できます。

リモートアクセス VPN を有効にするには、Secure Client Advantage、Secure Client Premier、または Secure Client VPN のみ のうちいずれかのライセンスを購入して有効にする必要があります。両方のライセンスがあり、そのどちらも使用する場合は、Secure Client Advantage と Secure Client Premier を選択できます。[Apex] または [Plus] と一緒に Secure Client VPN のみ ライセンスを使用することはできません。セキュアクライアントライセンスは、スマートアカウントと共有する必要があります。手順については、http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdfを参照してください。

指定されたデバイスに指定された セキュアクライアント ライセンスタイプの権限が 1 つ以上ない場合、リモートアクセス VPN 設定をそのデバイスに展開することはできません。登録されたライセンスがコンプライアンスに従っていない、または権限の有効期限が切れている場合は、システムにライセンス アラートとヘルス イベントが表示されます。

リモートアクセス VPN を使用する際は、スマートアカウントでエクスポート制御機能（高度な暗号化）を有効にしておく必要があります。セキュアクライアント とのリモートアクセス VPN 接続を確立するために、Threat Defense はより強力な暗号化を要求します（これは DES よりも高い暗号化です）。

次の条件に当てはまる場合、リモートアクセス VPN を展開できません。

- Management Center でスマート ライセンスが評価モードで実行されている。
- スマート アカウントがエクスポート制御機能（高度な暗号化）を使用するように設定されていない。

輸出規制対象の機能のライセンス

輸出規制対象の機能が必要な機能

特定のソフトウェア機能は、国家安全保障、外交政策、反テロリズムに関する法律や規制の対象となります。これらの輸出規制対象の機能は次のとおりです。

- セキュリティ認定コンプライアンス
- リモート アクセス VPN
- 強力な暗号化によるサイト間 VPN
- 強力な暗号化による SSH プラットフォーム ポリシー
- 強力な暗号化による SSL ポリシー
- 強力な暗号化による SNMPv3 などの機能

輸出規制対象の機能がシステムに対して現在有効になっているかどうかを判断する方法

輸出規制対象の機能がシステムに対して現在有効になっているかどうかを判断するには、[システム（System）] > [ライセンス（Licenses）] > [スマート ライセンス（Smart Licenses）] に移動し、[輸出規制対象の機能（Export-Controlled Features）] に [有効（Enabled）] と表示されているかどうかを確認します。

輸出規制対象の機能の有効化について

[輸出規制対象の機能（Export-Controlled Features）] に [無効（Disabled）] と表示されており、強力な暗号化が必要な機能を使用する場合、強力な暗号化機能を有効にする方法は2つあります。組織はどちらか一方を使用する（またはどちらも使用しない）ことができますが、両方を使用することはできません。

- Smart Software Manager で新しい製品インスタンス登録トークンを生成したときに輸出規制対象の機能を有効にするオプションがない場合は、アカウント担当者にお問い合わせください。

  シスコによって承認されたら、強力な暗号化ライセンスをアカウントに手動で追加して、輸出規制されている機能を使用できるようにすることができます。詳細については、グローバル権限のないアカウントの輸出規制機能の有効化（333 ページ）を参照してください。

- Smart Software Manager で新しい製品インスタンス登録トークンを生成するときに、[このトークンを使用して登録した製品で輸出管理機能を許可（Allow export-controlled functionality on the products registered with this token）] オプションが表示される場合は、トークンを生成する前にそれを確認してください。

  Management Center の登録に使用した製品インスタンス登録トークンの輸出規制機能を有効にしなかった場合は、登録を解除してから、輸出規制機能を有効にした新しい製品インスタンス登録トークンを使用して Management Center を再登録する必要があります。

評価モードで、または Management Center で強力な暗号化を有効にする前にデバイスを Management Center に登録した場合は、各管理対象デバイスを再起動して、強力な暗号化を使用できるようにします。高可用性展開では、アクティブ デバイスとスタンバイ デバイスを一緒に再起動してアクティブ/アクティブの状態を回避する必要があります。

これは永続的な付与資格であり、サブスクリプションは必要ありません。

詳細情報

輸出規制に関する一般情報については https://www.cisco.com/c/en/us/about/legal/global-export-trade.htmlを参照してください。

Threat Defense Virtual ライセンス

このセクションでは、Threat Defense Virtual で使用可能なパフォーマンス階層ライセンスの権限について説明します。

すべての Threat Defense Virtual ライセンスを、サポートされているすべての Threat Defense Virtual vCPU/メモリ構成で使用できます。これにより、Threat Defense Virtual を使用しているお客様は、さまざまなVMリソースフットプリントで実行できるようになります。また、サポート対象の AWS および Azure インスタンスタイプの数も増えます。Threat Defense Virtual VM を設定する場合、サポートされる最大コア（vCPU）数は 16 個です。また、サポートされる最大メモリ容量は 32 GB RAM です。

Threat Defense Virtual スマートライセンスのパフォーマンス階層

RA VPN に対するセッション制限は、インストールされている Threat Defense Virtual プラットフォームの権限付与階層によって決定され、レートリミッタによって適用されます。次の表は、権限付与層とレート制限に基づくセッション制限をまとめたものです。

表 *21 : Threat Defense Virtual* 権限付与に基づくライセンス機能の制限

パフォーマンス階層	デバイス仕様（コア/RAM）	レート制限	RA VPN セッション制限
FTDv5、100Mbps	4 コア/8 GB	100Mbps	50
FTDv10、1Gbps	4 コア/8 GB	1Gbps	250
FTDv20、3Gbps	4 コア/8 GB	3 Gbps	250
FTDv30、5Gbps	8 コア/16 GB	5 Gbps	250
FTDv50、10Gbps	12 コア/24 GB	10 Gbps	750
FTDv100、16 Gbps	16 コア/32 GB	16 Gbps	10,000

Threat Defense Virtual パフォーマンス階層ライセンスのガイドラインと制限事項

Threat Defense Virtual デバイスのライセンスを取得する際は、次の注意事項と制限事項に注意してください。

- Threat Defense Virtual は、導入要件に基づいて異なるスループットレベルと VPN 接続制限を提供するパフォーマンス階層型ライセンスをサポートしています。
- すべての Threat Defense Virtual ライセンスを、サポートされているすべての Threat Defense Virtual コア/メモリ構成で使用できます。これにより、Threat Defense Virtual を使用しているお客様は、さまざまな VM リソースフットプリントで実行できるようになります。
- Threat Defense Virtual を展開する際、デバイスが評価モードであるか、すでに Cisco Smart Software Manager に登録されているかに関係なく、パフォーマンス階層を選択できます。

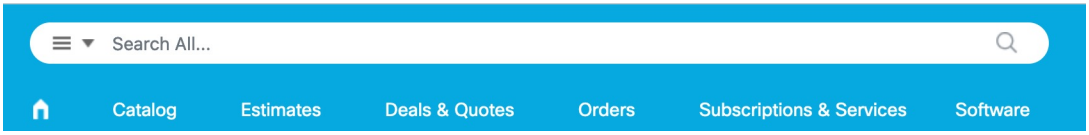
（注） お使いのスマート ライセンシング アカウントに、必要なライセンスが含まれていることを確認してください。使用アカウントにあるライセンスと一致する階層を選択することが重要です。Threat Defense Virtual をバージョン 7.0 にアップグレードする場合は、[FTDv - Variable] を選択して現在のライセンスコンプライアンスを維持できます。Threat Defense Virtual は、ご使用のデバイスの機能（コア/RAM の数）に基づいてセッション制限を引き続き実行します。

- REST API を使用して、新しい Threat Defense Virtual デバイスを展開する場合や Threat Defense Virtual をプロビジョニングする場合、デフォルトのパフォーマンス階層は FTDv50 です。
- Essentials ライセンスはサブスクリプションベースで、パフォーマンス階層にマッピングされます。バーチャルアカウントには、Threat Defense Virtual デバイスの Essentials ライセンス権限と、IPS、マルウェア防御、および URL フィルタリングのライセンスが必要です。
- 各 HA ピアは 1 つの権限を消費します。各 HA ピアの権限は Essentials ライセンスを含めて一致している必要があります。
- HA ペアのパフォーマンス階層の変更は、プライマリピアに適用される必要があります。
- 個別のノードではなく、クラスタ全体に機能ライセンスを割り当てます。ただし、クラスタの各ノードは機能ごとに個別のライセンスを使用します。クラスタリング機能自体にライセンスは必要ありません。
- ユニバーサル PLR ライセンスは、HA ペアの各デバイスに個別に適用されます。セカンダリデバイスが、プライマリデバイスのパフォーマンス階層を自動的にミラーリングすることはありません。手動で更新する必要があります。

ライセンス PID

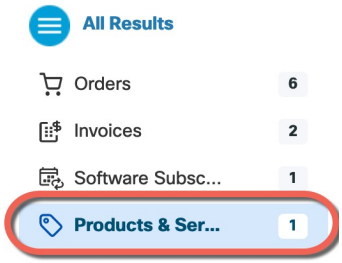
ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマート ソフトウェア ライセンシング アカウントにリンクされています。ただし、自身でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で [すべて検索（Search All）] フィールドを使用します。

図 *14 :* ライセンス検索



結果から、[製品とサービス（Products and Services）] を選択します。

図 *15 :* 結果



Management Center Virtual PID

- VMware：
  - SF-FMC-VMW-2-K9—2 デバイス
  - SF-FMC-VMW-10-K9—10 デバイス
  - SF-FMC-VMW-K9—25 デバイス
  - SF-FMC-VMW-300-K9—300 デバイス
- KVM：
  - SF-FMC-KVM-2-K9—2 デバイス
  - SF-FMC-KVM-10-K9—10 デバイス
  - SF-FMC-KVM-K9—25 デバイス
- PAK ベースの VMware：
  - FS-VMW-2-SW-K9—2 デバイス
  - FS-VMW-10-SW-K9—10 デバイス

- FS-VMW-SW-K9—25 デバイス

Threat Defense Virtual PID

FTDV-SEC-SUB を注文するときは、Essentialsライセンスとオプションの機能ライセンス（12か月の期間）を選択する必要があります。

- Essentialsライセンス：
  - FTD-V-5S-BSE-K9
  - FTD-V-10S-BSE-K9
  - FTD-V-20S-BSE-K9
  - FTD-V-30S-BSE-K9
  - FTD-V-50S-BSE-K9
  - FTD-V-100S-BSE-K9
- IPS 、マルウェア防御および URL ライセンスの組み合わせ：
  - FTD-V-5S-TMC
  - FTD-V-10S-TMC
  - FTD-V-20S-TMC
  - FTD-V-30S-TMC
  - FTD-V-50S-TMC
  - FTD-V-100S-TMC
- キャリア：FTDV_CARRIER
- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。

Firepower 1010 PID

- IPS 、マルウェア防御および URL ライセンスの組み合わせ：
  - L-FPR1010T-TMC=

  上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。

Firepower 1100 PID

- IPS 、マルウェア防御および URL ライセンスの組み合わせ：
  - L-FPR1120T-TMC=
  - L-FPR1140T-TMC=
  - L-FPR1150T-TMC=

  上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。
  - L-FPR1120T-TMC-1Y
  - L-FPR1120T-TMC-3Y
  - L-FPR1120T-TMC-5Y
  - L-FPR1140T-TMC-1Y
  - L-FPR1140T-TMC-3Y
  - L-FPR1140T-TMC-5Y
  - L-FPR1150T-TMC-1Y
  - L-FPR1150T-TMC-3Y
  - L-FPR1150T-TMC-5Y
- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。

Firepower 2100 PID

- IPS 、マルウェア防御および URL ライセンスの組み合わせ：
  - L-FPR2110T-TMC=
  - L-FPR2120T-TMC=
  - L-FPR2130T-TMC=
  - L-FPR2140T-TMC=

  上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。
  - L-FPR2110T-TMC-1Y
  - L-FPR2110T-TMC-3Y
  - L-FPR2110T-TMC-5Y
  - L-FPR2120T-TMC-1Y
  - L-FPR2120T-TMC-3Y
  - L-FPR2120T-TMC-5Y

- L-FPR2130T-TMC-1Y
- L-FPR2130T-TMC-3Y
- L-FPR2130T-TMC-5Y
- L-FPR2140T-TMC-1Y
- L-FPR2140T-TMC-3Y
- L-FPR2140T-TMC-5Y

- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。

Secure Firewall 3100 PID

- Essentialsライセンス：
  - L-FPR3110-BSE=
  - L-FPR3120-BSE=
  - L-FPR3130-BSE=
  - L-FPR3140-BSE=
- IPS 、マルウェア防御および URL ライセンスの組み合わせ：
  - L-FPR3110T-TMC=
  - L-FPR3120T-TMC=
  - L-FPR3130T-TMC=
  - L-FPR3140T-TMC=

  上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。
  - L-FPR3105T-TMC-1Y
  - L-FPR3105T-TMC-3Y
  - L-FPR3105T-TMC-5Y
  - L-FPR3110T-TMC-1Y
  - L-FPR3110T-TMC-3Y
  - L-FPR3110T-TMC-5Y
  - L-FPR3120T-TMC-1Y
  - L-FPR3120T-TMC-3Y
  - L-FPR3120T-TMC-5Y
  - L-FPR3130T-TMC-1Y
  - L-FPR3130T-TMC-3Y

- L-FPR3130T-TMC-5Y
- L-FPR3140T-TMC-1Y
- L-FPR3140T-TMC-3Y
- L-FPR3140T-TMC-5Y

- キャリア：L-FPR3K-FTD-CAR=
- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。

Firepower 4100 PID

- IPS 、マルウェア防御および URL ライセンスの組み合わせ：
  - L-FPR4112T-TMC=
  - L-FPR4115T-TMC=
  - L-FPR4125T-TMC=
  - L-FPR4145T-TMC=

  上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。
  - L-FPR4112T-TMC-1Y
  - L-FPR4112T-TMC-3Y
  - L-FPR4112T-TMC-5Y
  - L-FPR4115T-TMC-1Y
  - L-FPR4115T-TMC-3Y
  - L-FPR4115T-TMC-5Y
  - L-FPR4125T-TMC-1Y
  - L-FPR4125T-TMC-3Y
  - L-FPR4125T-TMC-5Y
  - L-FPR4145T-TMC-1Y
  - L-FPR4145T-TMC-3Y
  - L-FPR4145T-TMC-5Y

- キャリア：L-FPR4K-FTD-CAR=
- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。

Secure Firewall 4200 PID

- Essentialsライセンス：

- L-FPR4215-BSE=
- L-FPR4225-BSE=
- L-FPR4245-BSE=

- IPS 、マルウェア防御および URL ライセンスの組み合わせ：
  - L-FPR4215T-TMC=
  - L-FPR4225T-TMC=
  - L-FPR4245T-TMC=

  上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。
  - L-FPR4215T-TMC-1Y
  - L-FPR4215T-TMC-3Y
  - L-FPR4215T-TMC-5Y
  - L-FPR4225T-TMC-1Y
  - L-FPR4225T-TMC-3Y
  - L-FPR4225T-TMC-5Y
  - L-FPR4245T-TMC-1Y
  - L-FPR4245T-TMC-3Y
  - L-FPR4245T-TMC-5Y

- キャリア：L-FPR4200-FTD-CAR=
- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。

Firepower 9300 PID

- IPS 、マルウェア防御および URL ライセンスの組み合わせ：
  - L-FPR9K-40T-TMC=
  - L-FPR9K-48T-TMC=
  - L-FPR9K-56T-TMC=

  上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。
  - L-FPR9K-40T-TMC-1Y
  - L-FPR9K-40T-TMC-3Y
  - L-FPR9K-40T-TMC-5Y

- L-FPR9K-48T-TMC-1Y
- L-FPR9K-48T-TMC-3Y
- L-FPR9K-48T-TMC-5Y
- L-FPR9K-56T-TMC-1Y
- L-FPR9K-56T-TMC-3Y
- L-FPR9K-56T-TMC-5Y

- キャリア：L-FPR9K-FTD-CAR=
- Cisco Secure Client：Cisco AnyConnect 発注ガイド [英語] を参照してください。

ISA 3000 PID

- IPS 、マルウェア防御および URL ライセンスの組み合わせ：
  - L-ISA3000T-TMC=

  上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。
  - L-ISA3000T-TMC-1Y
  - L-ISA3000T-TMC-3Y
  - L-ISA3000T-TMC-5Y

- Cisco Secure Client：Cisco AnyConnect 発注ガイド [英語] を参照してください。

ライセンスの要件と前提条件

特定ライセンス予約の要件については、特定ライセンス予約の要件および前提条件（343 ページ）を参照してください。

一般的な前提条件

- Management Center と管理対象デバイスで NTP が設定されていることを確認します。登録を成功させるには、時刻を同期させる必要があります。

  Firepower 4100/9300 シャーシの場合は、Management Center と同じ NTP サーバーをシャーシに使用してシャーシに NTP を設定する必要があります。

サポートされるドメイン

Global。明記されている場合を除きます。

ユーザの役割

- 管理者

高可用性、クラスタリング、マルチインスタンスのためのライセンシングの要件および前提条件

このセクションでは、高可用性（デバイス高可用性と Management Center Virtual 高可用性）、クラスタリング、およびマルチインスタンス展開のライセンス要件について説明します。

Management Center 高可用性のライセンシング

各デバイスには、単一の Management Center によって管理されているか、ハイアベイラビリティペア（ハードウェアまたは仮想）の Management Center によって管理されているかにかかわらず、同じライセンスが必要です。

例：Management Center ペアで管理されている 2 つのデバイスに対して高度なマルウェア防御を有効にする場合は、2 つの マルウェア防御 ライセンスと 2 つの TM サブスクリプションを購入し、アクティブ Management Center を Smart Software Manager に登録してから、ライセンスをアクティブ Management Center 上の 2 つのデバイスに割り当てます。

アクティブな Management Center のみが Smart Software Manager に登録されます。フェールオーバーが実行されると、システムは Smart Software Manager と通信して、ライセンスの付与資格を最初にアクティブだった Management Center から解放し、新たにアクティブになる Management Center に割り当てます。

特定ライセンス予約の展開では、プライマリ Management Center のみが特定ライセンス予約を必要とします。

ハードウェア（Hardware） Management Center

ハイアベイラビリティペア内のハードウェア Management Center に特別なライセンスは必要ありません。

Management Center Virtual

同じライセンスの Management Center Virtual が 2 つ必要です。

例：10 台のデバイスを管理する Management Center Virtual ハイアベイラビリティペアの場合は、以下を使用できます。

- 2 個の Management Center Virtual 10 エンタイトルメント
- 10 個のデバイスライセンス

ハイアベイラビリティペアを解除すると、セカンダリ Management Center Virtual に関連付けられた Management Center Virtual エンタイトルメントが解放されます。（この例では、2 個のスタンドアロン Management Center Virtual 10 があります。）

デバイス高可用性のライセンシング

高可用性構成の両方の Threat Defense ユニットは、ライセンスが同じである必要があります。

高可用性構成には 2 つのライセンス資格（ペアの各デバイスに 1 つずつ）が必要です。

高可用性を確立する前に、どのライセンスがセカンダリ/スタンバイデバイスに割り当てられているかどうかは問題にはなりません。高可用性の設定中に、Management Center はスタンバイユニットに割り当てられている不要なライセンスをすべて削除し、プライマリ/アクティブユニットに割り当てられているのと同じライセンスで置き換えます。たとえば、アクティブユニットに Essentials ライセンスと IPS ライセンスが割り当てられており、スタンバイユニットに Essentials ライセンスのみが割り当てられている場合、Management Center は Cisco Smart Software Manager と通信して、アカウントからスタンバイユニット用に使用可能な IPS ラインセンスを取得します。ライセンスアカウントで十分な数の資格が購入されていなければ、正しい数のライセンスを購入するまで、アカウントは非準拠の状態になります。

デバイスクラスタのライセンス

各 Threat Defense Virtual クラスタノードには、同じパフォーマンス階層ライセンスが必要です。すべてのメンバーに同じ数の CPU とメモリを使用することをお勧めします。そうしないと、パフォーマンスが最小能力のメンバーに一致するようにすべてのノードで制限されます。スループットレベルは、一致するように制御ノードから各データノードに複製されます。

個別のノードではなく、クラスタ全体に機能ライセンスを割り当てます。ただし、クラスタの各ノードは機能ごとに個別のライセンスを使用します。クラスタリング機能自体にライセンスは必要ありません。

制御ノードを Management Center に追加する際に、そのクラスタに使用する機能ライセンスを指定できます。クラスタを作成する前に、データノードにどのライセンスが割り当てられているのかは問題になりません。制御ノードのライセンス設定は、各データノードに複製されます。クラスタのライセンスは、**システム**（⚙）> **[ライセンス（Licenses）]** > **[スマートライセンス（Smart Licenses）]** > **[ライセンスの編集（Edit Licenses）]** または**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[クラスタ（Cluster）]** > **[ライセンス（License）]** エリアで変更できます。

（注） Management Center にライセンスを取得する（および評価モードで実行する）前にクラスタを追加した場合、Management Center にライセンスを取得する際にポリシーの変更をクラスタに展開するとトラフィックの中断が発生することがあります。ライセンスモードを変更したことによって、すべてのデータユニットがクラスタをいったん離れてから再参加することになります。

複数インスタンス展開のライセンス

すべてのライセンスがコンテナ インスタンスごとではなく、セキュリティ エンジン/シャーシ（Firepower 4100 の場合）またはセキュリティ モジュール（Firepower 9300 の場合）ごとに使用されます。次の詳細情報を参照してください。

- Essentialsライセンスが セキュリティ モジュール/エンジン ごとに 1 つ自動的に割り当てられます。
- 機能ライセンスは各インスタンスに手動で割り当てますが、セキュリティ モジュール/エンジン につき機能ごとに 1 つのライセンスのみを使用します。たとえば、3 つのセキュリティモジュールを搭載した Firepower 9300 の場合、使用中のインスタンスの数に関係なく、モジュールにつき 1 つの URL フィルタリング ライセンスが必要で、合計 3 つのライセンスが必要になります。

次に例を示します。

表 *22 : Firepower 9300* のコンテナインスタンスのサンプルライセンスの使用状況

Firepower 9300	インスタンス	ライセンス
セキュリティ モジュール 1	インスタンス 1	Essentials、URL フィルタリング、マルウェア防御
	インスタンス 2	Essentials、URL フィルタリング
	インスタンス 3	Essentials、URL フィルタリング
セキュリティ モジュール 2	インスタンス 4	Essentials、IPS
	インスタンス 5	Essentials、URL フィルタリング、マルウェア防御、IPS
セキュリティ モジュール 3	インスタンス 6	Essentials、マルウェア防御、IPS
	インスタンス 7	Essentials、IPS

表 *23 :* ライセンスの総数

Essentials	URL フィルタリング	マルウェア防御	IPS
3	2	3	2

シスコアカウントの作成

スマートアカウントを要求し、シスコ製品のライセンスを取得するには、シスコアカウントが必要です。

手順

ステップ 1 URL https://id.cisco.com/signin/register を開き、新しいアカウントを作成します。

ステップ 2 アカウントを作成するには、すべての必須フィールドに入力します。

次の図は例を示しています。

ステップ 3 [登録（Register）] をクリックします。

電子メールアドレスを確認するために、アクティベーションコードが記載された電子メールが送信されます。

（注） 電子メールがまだ届いていない場合は、登録サポートチーム（web-help@cisco.com）に電子メールを送信してください。

ステップ 4 [電子メールでの確認（Verify with your email）] ページで、アクティベーションコードを入力して登録プロセスを完了し、[確認（Verify）] をクリックします。

登録が正常に完了すると、ログインページにリダイレクトされます。

次のタスク

ログインページで、新しく作成したアカウントの詳細を入力して、スマートアカウントを要求します。スマートアカウントの作成とライセンスの追加（326ページ）を参照してください。

スマートアカウントの作成とライセンスの追加

ライセンスを購入する前に、このアカウントを設定する必要があります。

始める前に

アカウント担当者または再販業者が、ユーザーのためにスマートアカウントを設定していることがあります。その場合は、この手順を使用するのではなく、その担当者からアカウントへのアクセスに必要な情報を取得してから、アカウントにアクセスできることを確認してください。

シスコアカウントをまだ作成していない場合は、新しいシスコアカウントを作成する必要があります。手順については、「シスコアカウントの作成」を参照してください。

スマート アカウントに関する一般情報については http://www.cisco.com/go/smartaccountsを参照してください。

手順

ステップ 1 [スマートアカウントの作成（Create a Smart Account）]https://software.cisco.com/software/csws/smartaccount/accountCreation/createSmartAccountページに移動します。シスコアカウントでログインするように求められます。

[スマートアカウントの作成（Create a Smart Account）] ページに、基本的なアカウント情報が表示されます。

ステップ 2 右上隅に表示される [マイアカウント（My Account）] アイコンをクリックし、[プロファイルの管理（Manage Profile）] をクリックします。

ステップ 3 [個人用（Personal）] をクリックします。

ステップ 4 [会社の詳細（Your Company Details）] セクションで、[編集（Edit）] をクリックします。

ステップ 5 [会社または組織（Company or organization）] フィールドに、組織名を入力します。

ステップ 6 会社の情報がすでにシスコのデータベースに存在する場合は、リストに表示されます。会社を選択できます。

[住所（Address）] ドロップダウンリストで、会社の住所を選択します。

ステップ 7 会社がシスコのデータベースに登録されていない場合は、引き続き [会社または組織（Company or organization）] フィールドに会社情報を入力できます。

a) [住所（Address）] ドロップダウンリストで、ドロップダウンの矢印をクリックして、[新しい住所の追加（Add New Address）] をクリックします。

b) 次のいずれかの [住所タイプ（Address Type）] オプションを選択できます。

- [会社/組織（Company/Organization）]：組織の住所を入力します。シスコは、この住所を確認します。住所と会社名がその国で確認できない場合は、続行できない可能性があります。そのため、正しい住所が入力されていることを確認する必要があります。
- [個人（Personal）]：個人の住所を入力します。

ステップ 8 会社に関連付けられているすべての必須フィールドに入力し、[更新（Update）] をクリックします。

[会社の詳細（Your Company Details）] セクションに、入力した会社の詳細が表示されます。

会社の詳細が確認されると、成功メッセージが表示されます。

ステップ 9 **[更新（Update）]**をクリックします。

会社の詳細が確認されると、成功メッセージが表示されます。

ステップ 10 前のタブで開いた [スマートアカウントの作成（Create a Smart Account）] ページを開きます。変更が反映されていない場合は、ページを更新してください。

または、URL「https://software.cisco.com/software/company/smartaccounts/home?route=module/accountcreation」を使用してこのページを開き、ログイン情報を使用してログインすることもできます。

ステップ 11 [アカウントの作成（Create Account）] をクリックします。

[アカウントサマリー（Account Summary）] ページにアカウントの詳細が表示されます。

ステップ 12 [完了（Done）] をクリックします。

ステップ 13 スマートアカウントの設定準備ができたことを知らせる電子メールが届くのを待ちます。電子メールが届いたら、指示に従って、メールに含まれているリンクをクリックします。

ステップ 14 お使いのスマート ライセンシング アカウントに、必要なライセンスが含まれていることを確認してください。

ライセンス PID については、ライセンス PID （316 ページ）を参照してください。

次のタスク

Smart Software Manager を使用してスマートライセンスを設定するには、スマート ライセンスの設定 （328 ページ）を参照してください。

スマート ライセンスの設定

ここでは、Smart Software Manager または Smart Software Manager On-Prem を使用してスマートライセンスを使用する方法について説明します。特定ライセンス予約を使用するには、特定ライセンス予約（SLR）の設定 （343 ページ）を参照してください。

スマートライセンシングに関する Management Center の登録

Management Center は、インターネット経由で Smart Software Manager に直接登録できます。また、エアギャップネットワークを使用している場合は、Smart Software Manager オンプレミスを使用して登録できます。

Smart Software Manager での Management Center の登録

Smart Software Manager で Management Center を登録します。

始める前に

- お使いのスマート ライセンシング アカウントに、必要なライセンスが含まれていることを確認してください。

  ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマートアカウントにリンクされています。ただし、主導でライセンスを追加する必要がある場合は、Cisco Commerce Workspace を参照します。ライセンス PID については、ライセンス PID （316 ページ）を参照してください。

- Management Center が smartreceiver.cisco.com で Smart Software Manager にアクセスできることを確認します。
- NTP を設定してください。登録時に、スマートエージェントと Smart Software Manager 間でキー交換が実行されるため、適切な登録には時刻の同期が必要です。

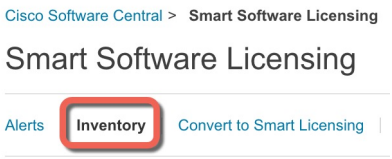
  Firepower 4100/9300 シャーシの場合は、Management Center と同じ NTP サーバーをシャーシに使用してシャーシに NTP を設定する必要があります。

- 組織に複数の Management Center がある場合は、各 Management Center に明確に識別できる一意の名前が付いており、同じバーチャルアカウントに登録されている可能性がある他の Management Center と区別できることを確認します。この名前は、スマート ライセンスの権限付与の管理にとって重要です。あいまいな名前だと後で問題が発生することがあります。

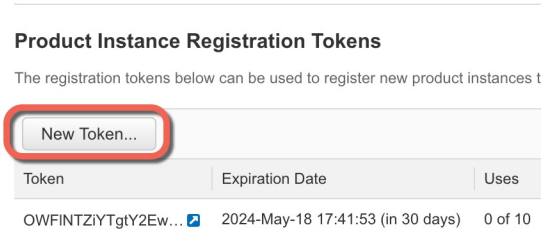
手順

ステップ 1 Smart Software Manager で、このデバイスを追加する仮想アカウントの登録トークンを要求してコピーします。

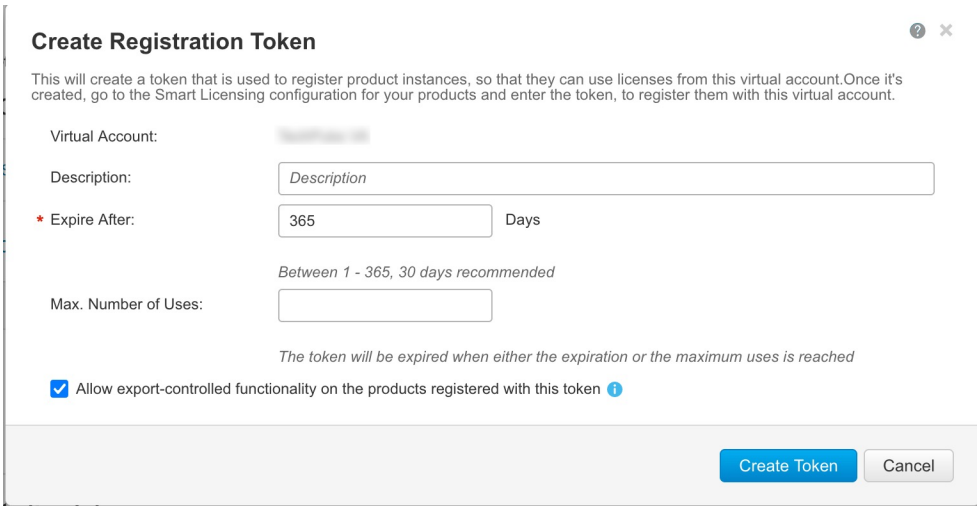
a) [Inventory] をクリックします。



b) [General] タブで、[New Token] をクリックします。



c) [登録トークンを作成（Create Registration Token）] ダイアログボックスで、以下の設定値を入力してから [トークンを作成（Create Token）] をクリックします。



- **説明**
- [有効期限（Expire After）]：推奨値は 30 日です。
- 最大使用回数（Max. Number of Uses）
- [このトークンに登録された製品で輸出管理機能を許可する（Allow export-controlled functionality on the products registered with this token）]：高度暗号化が許可されている国の場合は輸出コンプライアンスフラグを有効にします。この機能を使用する予定の場合、このオプションをここで選択する必要があります。後でこの機能を有効にする場合は、デバイスを新しいプロダクトキーで再登録し、デバイスをリロードする必要があります。このオプションが表示されない場合、アカウントは輸出規制機能をサポートしていません。

トークンはインベントリに追加されます。

d) トークンの右側にある矢印アイコンをクリックして [トークン（Token）] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。Threat Defense の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 *16*：トークンの表示

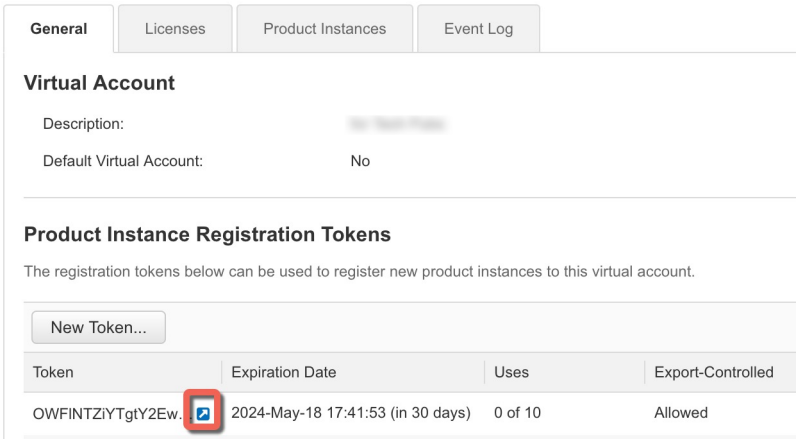
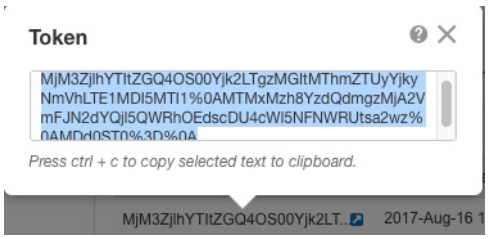


図 *17*：トークンのコピー



ステップ 2 Management Center で、**システム**（⚙）>**[ライセンス（Licenses）]**>**[スマートライセンス（Smart Licenses）]** を選びます。

ステップ 3 [登録（Register）] をクリックします。

ステップ 4 Smart Software Manager から生成されたトークンを [製品インスタンス登録トークン（Product Instance Registration Token）] フィールドに貼り付けます。

テキストの前後にスペースや空白の行がないことを確認します。

ステップ 5 Management Center インスタンスがすでにスマートライセンスに登録されている場合は、[既存の登録済みManagement Centerインスタンスのオーバーライド（Override Existing Registered Management Center Instance）] チェックボックスをオンにして、スマートライセンスの既存の登録済み Management Center インスタンスをオーバーライドできます。

ステップ 6 使用状況データをシスコに送信するかどうかを決定します。

- [Cisco Success Networkの有効化（Enable Cisco Success Network）] は、デフォルトで有効です。シスコによって収集されるデータの種類を表示するには、[サンプルデータ（sample data）] をクリックします。詳細については、Cisco Success Network の登録設定 （759 ページ） を参照してください。
- [Cisco Support Diagnosticsを有効にする（Enable Cisco Support Diagnostics）] はデフォルトで無効になっています。シスコが収集するデータの種類は、このチェックボックスの上に表示されているリンクで確認できます。詳細については、Cisco Support Diagnostics の登録設定 （760 ページ） を参照してください。

（注）
- 有効にすると、Cisco Support Diagnostics は、次の同期サイクルでデバイスで有効になります。Management Center とデバイスとの同期は、30 分ごとに 1 回実行されます。
- 有効にすると、この Management Center に登録される新しいデバイスでは、Cisco Support Diagnostics が自動的に有効になります。

ステップ 7 [変更を適用（Apply Changes）] をクリックします。

次のタスク

- Management Center にデバイスを追加します。Cisco Secure Firewall Management Center デバイス構成ガイドの「Add a Device to the Management Center」を参照してください。
- ライセンスをデバイスに割り当てます。複数の管理対象デバイスへのライセンスの割り当て （336 ページ）を参照してください。

Management Center の Smart Software Manager オンプレミスへの登録

Smart Software Manager との定期的な通信 （303 ページ）で説明されているように、Management Center は、ライセンス権限を維持するためにシスコと定期的に通信する必要があります。次の状況のいずれかの場合、Smart Software Manager と接続するためのプロキシとして Smart Software Manager オンプレミス（旧称「Smart Software Satellite Server」）を使用できます。

- Management Center がオフラインである、接続が制限されている、または接続がない（つまり、エアギャップ ネットワークに展開されている）場合。

  （エアギャップネットワーク向けの代替ソリューションについては、エアギャップ展開のライセンスのオプション （302 ページ）を参照してください。）
- Management Center に固定接続があるが、ネットワークからの単一の接続によってスマート ライセンスを制御する場合。

Smart Software Manager オンプレミス を使用すると、同期スケジュールを設定、またはスマートライセンス認証を Smart Software Manager と手動で同期させることができます。

Smart Software Manager オンプレミス の詳細については、https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html#~on-prem を参照してください。

手順

ステップ 1 Smart Software Manager オンプレミスを展開して設定します。

- Smart Software Manager オンプレミスのドキュメントを参照してください。https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html#~on-prem から入手できます。

- Smart Software Manager オンプレミスの TLS/SSL 証明書の CN をメモします。
- http://www.cisco.com/security/pki/certs/clrca.cer に移動し、TLS/SSL 証明書の本文全体（"-----BEGIN CERTIFICATE-----" から "-----END CERTIFICATE-----" まで）を、設定中にアクセスできる場所にコピーします。

ステップ 2 Management Center を Smart Software Manager オンプレミス に登録します。

a) **[統合（Integration）] > [その他の統合（Other Integrations）]**を選択します。
b) [スマート ソフトウェア サテライト（Smart Software Satellite）] をクリックします。
c) [Cisco Smart Software Satellite Serverに接続（Connect to Cisco Smart Software Satellite Server）] を選択します。
d) この手順の前提条件で収集した CN 値を使用して、Smart Software Manager オンプレミスの **URL** を次の形式で入力します。

`https://FQDN_or_hostname_of_your_SSM_On-Prem/SmartTransport`

FQDN またはホスト名は、Smart Software Manager オンプレミスによって提示された証明書の CN 値と一致している必要があります。

e) 新しい [SSL 証明書（SSL Certificate）] を追加し、以前にコピーした証明書テキストを貼り付けます。
f) [適用（Apply）] をクリックします。
g) [システム（System）]>[ライセンス（Licenses）]>[スマートライセンス（Smart Licenses）] を選択し、[登録（Register）] をクリックします。
h) Smart Software Manager オンプレミスに新しいトークンを作成します。
i) トークンをコピーします。
j) トークンを管理センター ページのフォームに貼り付けます。
k) [変更を適用（Apply Changes）] をクリックします。

管理センターが Smart Software Manager オンプレミスに登録されました。

ステップ 3 デバイスにライセンスを割り当てた後、Smart Software Manager オンプレミス を Smart Software Manager に同期させます。

上記のSmart Software Manager オンプレミスのドキュメントを参照してください。

ステップ 4 継続的な同期時刻をスケジュールします。

グローバル権限のないアカウントの輸出規制機能の有効化

スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。

始める前に

- 展開でまだ輸出規制対象の機能がサポート**されていない**ことを確認します。

展開で輸出規制対象の機能がサポートされている場合、Smart Software Manager の [登録トークンの作成（Create Registration Token）] ページに輸出規制対象の機能を有効にできるオプションが表示されます。詳細については、https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.htmlを参照してください。

- 展開で評価ライセンスが使用されていないことを確認します。
- Smart Software Manager の **[インベントリ（Inventory）]** > **[ライセンス（Licenses）]** ページで、Management Center に対応するライセンスがあることを確認します。

輸出規制ライセンス	Management Center モデル
Cisco Virtual FMC シリーズの強力な暗号化（3DES/AES）	すべての Management Center Virtual
Cisco FMC 1K シリーズの強力な暗号化（3DES/AES）	1000、 1600
Cisco FMC 2 K シリーズの強力な暗号化（3DES/AES）	2500、2600
Cisco FMC 4K シリーズの強力な暗号化（3DES/AES）	4500、4600

手順

ステップ 1 **[システム（System）]** > **[ライセンス（Licenses）]** > **[スマート ライセンス（Smart Licenses）]** を選択します。

（注） [輸出キーの要求（Request Export Key）] が表示されている場合は輸出規制対象の機能がアカウントに承認されています。そのため、必要な機能の使用に進むことができます。

ステップ 2 [エクスポート キーの要求（Request Export Key）] をクリックして、エクスポート キーを生成します。

ヒント エクスポート制御キーの要求に失敗した場合は、バーチャルアカウントに有効なエクスポート制御ライセンスがあることを確認します。

[輸出キーの返却（Return Export Key）] をクリックして、輸出規制ライセンスを無効にします

次のタスク

これで、輸出規制対象の機能を使用する設定またはポリシーを展開できるようになります。

メモ これによって有効にされた新しい輸出規制対象のライセンスとすべての機能は、Threat Defense デバイスが再起動されるまでそのデバイスでは有効になりません。それまでは、前のライセンスでサポートされていた機能のみがアクティブになります。

高可用性展開では、アクティブ/アクティブの状態を避けるために両方の Threat Defense デバイスを再起動する必要があります。

デバイスへのライセンスの割り当て

Management Center にデバイスを登録すると、ほとんどのライセンスを割り当てることができます。デバイスごと、または複数のデバイスにライセンスを割り当てることもできます。

単一のデバイスへのライセンスの割り当て

一部の例外はありますが、管理対象デバイスでライセンスを無効にすると、そのライセンスに関連づけられている機能は使用できなくなります。

（注） 同じ セキュリティ モジュール/エンジン のコンテナ インスタンスの場合は、ライセンスを各インスタンスに適用します。ただし、セキュリティ モジュール/エンジン のすべてのインスタンスについては、セキュリティ モジュール/エンジン は機能ごとに 1 つのライセンスのみを使用します。

（注） Threat Defense クラスタの場合は、クラスタ全体にライセンスを適用します。ただし、クラスタ内の各ユニットが機能ごとに個別のライセンスを使用します。

始める前に

このタスクを実行するには、管理者権限またはネットワーク管理者権限が必要です。複数のドメインを操作する場合は、このタスクをリーフドメインで実行する必要があります。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**を選択します。

ステップ 2 ライセンスを割り当てまたは無効にするデバイスの横にある **[編集（Edit）]**（✎） をクリックします。

ステップ 3 [デバイス（Device）] をクリックします。

ステップ 4 [ライセンス（License）] セクションの横にある **[編集（Edit）]**（✎） をクリックします。

ステップ 5 適切なチェックボックスをオンまたはオフにして、デバイスのライセンスを割り当て、または無効にします。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

次のタスク

ライセンスステータスの確認：**システム**（⚙）>**[ライセンス（Licenses）]**>**[スマートライセンス（Smart Licenses）]** に移動し、[スマートライセンス（Smart Licenses）] テーブル上部のフィルタにホスト名またはデバイスの IP アドレスを入力し、各デバイスおよび各ライセンスタイプに、[チェックマーク（Check Mark）]（✓）のある緑色の円のみが表示されることを確認します。その他のアイコンが表示される場合は、アイコンにマウスオーバーすると詳細を確認できます。

複数の管理対象デバイスへのライセンスの割り当て

Management Center によって管理されるデバイスは、ライセンスを、Smart Software Manager から直接ではなく Management Center 経由で取得します。

複数のデバイスでライセンスを一度に有効にするには、次の手順を使用します。

（注） 同じ セキュリティ モジュール/エンジン のコンテナ インスタンスの場合は、ライセンスを各インスタンスに適用します。ただし、セキュリティ モジュール/エンジン のすべてのインスタンスについては、セキュリティ モジュール/エンジン は機能ごとに 1 つのライセンスのみを使用します。

（注） Threat Defense クラスタの場合は、クラスタ全体にライセンスを適用します。ただし、クラスタ内の各ユニットが機能ごとに個別のライセンスを使用します。

手順

ステップ 1 **システム**（⚙）>**[ライセンス（Licenses）]**>**[スマートライセンス（Smart Licenses）]** または [特定のライセンス（Specific Licenses）] を選択します。

ステップ 2 [ライセンスの編集（Edit Licenses）] をクリックします。

ステップ 3 デバイスに追加するライセンスのタイプごとに、次の手順を実行します。

a) 該当するライセンスのタイプのタブをクリックします。

b) 左側のリスト内のデバイスをクリックします。

c) [追加（Add）] をクリックして、デバイスを右側のリストに移動させます。

d) 各デバイスが該当するタイプのライセンスを受信するまで、この手順をデバイスごとに繰り返します。

ここでは、追加するすべてのデバイスのライセンスをユーザが保持しているかどうかを気にする必要はありません。

e) 追加するライセンスのタイプごとに、この手順を繰り返します。

f) ライセンスを削除するには、デバイスの横にある [削除（Delete）]（ ） をクリックします。

g) [適用（Apply）] をクリックします。

クラスタを選択し、クラスタのすべてのノードに任意のライセンスを割り当てることができます。

次のタスク

ライセンスが正しくインストールされていることを確認します。「スマートライセンスのモニタリング （339 ページ）」の手順に従います。

スマートライセンスの管理

このセクションでは、スマートライセンスを管理する方法について説明します。

の登録解除Management Center

Smart Software Manager から Management Center の登録を解除して、すべてのライセンス資格をスマートアカウントに戻し、他のデバイスで使用できるようにします。たとえば、Management Center を廃止または再イメージ化する必要がある場合は、登録を解除します。

未登録の状態でのライセンス施行の詳細については、未登録状態 （304 ページ）を参照してください。

手順

ステップ 1 システム（ ）> **[ライセンス（Licenses）]** > **[スマートライセンス（Smart Licenses）]**を選択します。

ステップ 2 **[登録解除（Deregister）]**（ ） をクリックします。

Management Center の同期または再認証

デフォルトでは、アイデンティティ証明書は 6 ヵ月ごと、ライセンス資格は 30 日ごとに自動的に更新されます。インターネット アクセスの期間が限られている場合や、Smart Software

Manager でライセンスを変更した場合などは、これらの登録を手動で更新することもできます。

手順

ステップ 1 システム（⚙） > **[ライセンス（Licenses）]** > **[スマートライセンス（Smart Licenses）]**を選択します。

ステップ 2 アイデンティティ証明書を更新するには、**[同期（Synchronize）]**（↻） をクリックします。

ステップ 3 ライセンス資格を更新するには、[再認証（Re-Authorize）] をクリックします。

スマートライセンスのステータスのモニタリング

[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）] ページの [スマートライセンスのステータス（Smart License Status）] セクションでは、次に示すとおり、Management Center でのライセンスの使用状況の概要が提供されます。

使用の認証

可能なステータス値は次のとおりです。

- **[不遵守（In-compliance）]**（●） ：管理対象デバイスに割り当てられているすべてのライセンスが要求を満たしており、Management Center が Smart Software Manager と正常に通信しています。
- **ライセンスは要求を満たしているが、ライセンス認証局との通信に失敗した**：デバイスのライセンスは要求を満たしていますが、Management Center がシスコのライセンス認証局と通信できません。
- **コンプライアンス不適合のアイコンまたはライセンス認証局と通信できない**：1 つ以上の管理対象デバイスがコンプライアンス不適合のライセンスを使用しているか、Management Center が Smart Software Manager と通信していない期間が 90 日を超えています。

製品登録

Management Center が Smart Software Manager に連絡し登録された最終日を指定します。

割当済みの仮想アカウント

製品インスタンス登録トークンの生成に使用したスマートアカウントの下の仮想アカウントを指定し、Management Center を登録します。この展開がスマート アカウント内の特定の仮想アカウントに関連付けられていない場合は、この情報は表示されません。

輸出管理機能

このオプションが有効になっている場合、制限機能を展開できます。詳細は、「輸出規制対象の機能のライセンス （313 ページ）」を参照してください。

Cisco Success Network

Management Centerの Cisco Success Network を有効にしたかどうかを指定します。このオプションを有効にすると、テクニカルサポートを提供するために不可欠な使用状況に関する情報と統計がシスコに提供されます。また、この情報により、シスコは製品を向上させ、未使用の使用可能な機能を認識させるため、ネットワーク内にある製品の価値を最大限に生かすことができます。詳細については、Cisco Success Network の登録設定 （759 ページ）を参照してください。

スマートライセンスのモニタリング

Management Center とその管理対象デバイスのライセンスステータスを表示するには、[スマートライセンス（Smart Licenses）] ページを使用します。

このページには、展開におけるライセンスのタイプごとに、使用されているライセンスの総数、そのライセンスのコンプライアンスの適合または不適合の状態、デバイスタイプ、およびデバイスが展開されているドメインとグループが表示されます。また、Management Center のスマート ライセンス ステータスを表示できます。同じ セキュリティ モジュール/エンジン 上のコンテナインスタンスは セキュリティ モジュール/エンジン ごとに 1 つのライセンスのみを使用します。したがって、ライセンスタイプごとに各コンテナライセンスが個別に Management Center に表示されても、機能ライセンスタイプに使用されているライセンスの数は 1 つのみです。

[スマートライセンス（Smart Licenses）]ページ以外にも、ライセンスを表示できる方法がいくつかあります。

- [製品ライセンス（Product Licensing）] ダッシュボードウィジェットはライセンスの概要を示します。

  「ダッシュボードへのウィジェットの追加 （422 ページ）」、「ユーザー ロール別のダッシュボード ウィジェットの可用性 （406 ページ）」、および「[製品ライセンス（Product Licensing）] ウィジェット （418 ページ）」を参照してください。

- [デバイス管理（Device Management）] ページ（**[デバイス（Devices）]** > **[デバイス管理（Device Management）]**）は、各管理対象デバイスに適用されているライセンスをリストします。

- ヘルスポリシーで使用される際に、[スマートライセンスモニター（Smart License Monitor）] のヘルスモジュールはライセンスステータスを伝達します。

手順

ステップ 1 システム（⚙） > **[ライセンス（Licenses）]** > **[スマートライセンス（Smart Licenses）]**を選択します。

ステップ 2 [スマート ライセンス（Smart Licenses）] テーブルで、各 [ライセンス タイプ（License Type）] フォルダの左側にある矢印をクリックしてそのフォルダを展開します。

ステップ 3 各フォルダで、各デバイスの [ライセンスステータス（License Status）] 列に [チェックマーク（Check Mark）]（） 付きの緑の円が表示されていることを確認します。

（注） Management Center Virtual ライセンスが重複している場合は、それぞれが 1 つの管理対象デバイスを表します。

すべてのデバイスに [チェックマーク（Check Mark）]（） 付きの緑の円が表示されている場合、デバイスには適切なライセンスがあり、使用できる状態にあります。

[チェックマーク（Check Mark）]（） 付きの緑の円以外のライセンスステータスが表示されている場合は、ステータスアイコンにマウスカーソルを合わせてメッセージを確認します。

次のタスク

- [チェックマーク（Check Mark）]（） 付きの緑の円が表示されているデバイスがない場合は、追加ライセンスの購入が必要な可能性があります。

スマート ライセンスのトラブルシューティング

予期していたライセンスがスマート アカウントに表示されません。

表示されると思っていたライセンスがスマート アカウントにない場合は、次を試してください。

- 他の仮想アカウントにないことを確認します。この問題について、組織のライセンス管理者によるサポートが必要な場合があります。
- ライセンスを販売した担当者と、アカウントへの譲渡が完了していることを確認します。

スマートライセンスサーバーに接続できない

最初に、明らかな原因を確認します。たとえば、Management Center に外部接続があることを確認します。インターネット アクセス要件 （1278 ページ）を参照してください。

予期していなかったコンプライアンス不適合の通知またはその他のエラー

- デバイスが別の Management Center にすでに登録されている場合は、新しい Management Center にデバイスのライセンスを付与する前に元の Management Center の登録を解除する必要があります。の登録解除Management Center （337 ページ）を参照してください。
- サブスクリプション ライセンスの有効期限が切れているかどうかを確認します。

その他の問題のトラブルシュート

その他の一般的な問題の解決方法については、https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/215838-fmc-and-ftd-smart-license-registration-a.html を参照してください

Threat Defense で使用するためのクラシックライセンスの変換

ライセンス登録ポータルまたは Smart Software Manager のいずれかを使用してライセンスを変換し、未使用の製品認証キー（PAK）またはデバイスにすでに割り当てられているクラシックライセンスに変換することができます。

（注） このプロセスは元に戻すことはできません。そのライセンスが元々はクラッシク ライセンスであっても、スマート ライセンスをクラッシク ライセンスに変換することはできません。

Cosco.com のドキュメントでは、クラッシック ライセンスは「従来型の」ライセンスとも呼ばれています。

始める前に

- 製品インスタンスにまだ割り当てられていない未使用の PAK がある場合、従来のライセンスからスマート ライセンスへの変換は最も簡単です。
- ハードウェアで Threat Defense を実行できる必要があります。https://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html の『*Cisco Secure Firewall Threat Defense Compatibility Guide*』『』を参照してください。
- スマートアカウントが必要です。ない場合は作成します。「スマートアカウントの作成とライセンスの追加 （326 ページ）」を参照してください。
- 変換する PAK またはライセンスは、スマート アカウントに表示されている必要があります。
- Smart Software Manager ではなくライセンス登録ポータルを使用して変換する場合に変換プロセスを開始するには、スマート アカウント クレデンシャルを保有している必要があります。

手順

ステップ 1 実行する変換プロセスは、そのライセンスが使用されたことがあるかどうかによって異なります。

- 変換する PAK が使用されたことがない場合は、PAK の変換の手順を実行します。
- 変換する PAK がデバイスにすでに割り当てられている場合は、クラッシク ライセンスの変換の手順を実行します。

既存の従来のライセンスがまだデバイスに登録されていることを確認します。

ステップ 2 次のドキュメントで変換のタイプ（PAK またはインストール済みのクラシック ライセンス）の手順を参照してください。

- ライセンス登録ポータルを使用して PAK またはライセンスを変換するには、次の手順を実行します。
  - 変換プロセスのライセンス登録ポータル部分の手順がわかるビデオを表示する場合は、https://salesconnect.cisco.com/#/content-detail/7da52358-0fc1-4d85-8920-14a1b7721780 をクリックします。
  - https://cisco.app.box.com/s/mds3ab3fctk6pzonq5meukvcpjizt7wu のドキュメントで「変換（Convert）」を検索します。

    変換手順は 3 つあります。状況に該当する変換手順を選択します。
  - https://tools.cisco.com/SWIFT/LicensingUI/Home でライセンス登録ポータルにサインインし、上記のドキュメントの手順を実行します。
- Smart Software Manager を使用して PAK またはライセンスを変換するには、次の手順を実行します。
  - ハイブリッドライセンスをスマート ソフトウェア ライセンス *QRG* に変換するには、次の手順を実行します。

    https://community.cisco.com/t5/licensing-enterprise-agreements/converting-hybrid-licenses-to-smart-software-licenses-qrg/ta-p/3628609?attachment-id=134907
  - https://software.cisco.com/#SmartLicensing-LicenseConversion で Smart Software Manager にサインインし、上記のドキュメントの変換タイプ（PAK またはインストール済みのクラッシックライセンス）の手順を実行します。

ステップ 3 ハードウェアに Threat Defense を新たにインストールします。

インストールおよびアップグレードガイドにあるハードウェアに関する手順を参照してください。

ステップ 4 Device Manager を使用してこのデバイスをスタンドアロンデバイスとして管理するには、次の手順を実行します。

『Secure Firewall Device Manager Configuration Guides』にある Device Manager の設定ガイドに含まれるデバイスのライセンシングに関する説明を参照してください。

この手順の残りは省略してください。

ステップ 5 Management Center でスマート ライセンスをすでに展開している場合は、次の手順を実行します。

a) 新しい Threat Defense でスマートライセンスを設定します。

複数の管理対象デバイスへのライセンスの割り当て （336 ページ）を参照してください。

b) 新しいスマート ライセンスがデバイスに正常に適用されていることを確認します。

スマートライセンスのモニタリング （339 ページ）を参照してください。

ステップ 6 Management Center でスマート ライセンスをまだ展開していない場合は、次の手順を実行します。

スマートライセンスの設定（328ページ）を参照してください。（該当しないか、またはすでに完了しているステップはスキップします。）

特定ライセンス予約（SLR）の設定

特定のライセンスの予約機能を使用して、エアギャップ ネットワークにスマート ライセンスを展開できます。

（注） シスコでは、特定のライセンス予約に SLR、SPLR、PLR、永久ライセンス予約などのさまざまな名前を使用しています。シスコでは、これらの用語が、類似しているものの必ずしも同一ではないライセンスモデルを指すために使用される場合もあります。

特定のライセンスの予約が有効になっている場合、Management Center は、Smart Software Manager にアクセスせずに、または Smart Software Manager オンプレミス を使用せずに、バーチャルアカウントからライセンスを指定された期間予約します。

インターネットへのアクセスが必要なパブリック Web サイトに対する URL ルックアップや状況に応じた相互起動などの機能は動作しません。

シスコは、特定のライセンスの予約を使用する展開に関する Web 分析やテレメトリのデータを収集しません。

特定ライセンス予約の要件および前提条件

- 通常のスマートライセンスを現在使用している場合は、特定ライセンス予約を実装する前に Management Center の登録を解除します。詳細については、の登録解除Management Center（337 ページ）を参照してください。

  Management Center に現在展開されているすべてのスマートライセンスがアカウントで使用可能なライセンスのプールに戻され、特定のライセンスの予約を実装すると再利用できるようになります。

- 特定ライセンス予約は、通常のスマートライセンスと同じライセンスを使用します。
- （推奨）Management Center ペアを高可用性設定で展開する場合は、次の点に注意してください。

- ライセンスを割り当てる前に、高可用性を設定します。セカンダリ Management Center のデバイスにすでにライセンスを割り当てている場合は、それらの割り当てを解除してください。
- SLR ライセンスがプライマリ Management Center に割り当てられている場合、フェールオーバー後にセカンダリ Management Center がアクティブになると、SLR ライセンスをセカンダリ Management Center に追加できません。次のいずれかを実行する必要があります。
  - フェールオーバーを実行して、プライマリ Management Center をアクティブにします。
  - ライセンスの割り当てを解除し、セカンダリ Management Center に再割り当てします。

スマートアカウントが特定のライセンスの予約の展開の準備が整っているかどうかの確認

特定ライセンス予約の展開時の問題を防ぐため、Management Center に変更を加える前にこの手順を実行します。

始める前に

- 「特定ライセンス予約の要件および前提条件（343 ページ）」で説明した要件を満たしていることを確認します。
- Smart Software Manager のクレデンシャルがあることを確認します。

手順

ステップ 1 Smart Software Manager にサインインします。

https://software.cisco.com/#SmartLicensing-Inventory

ステップ 2 該当する場合は、ページの右上隅から正しいアカウントを選択します。

ステップ 3 必要に応じて、[インベントリ（Inventory）] をクリックします。

ステップ 4 [ライセンス（Licenses）] をクリックします。

ステップ 5 次のことを確認してください。

- [ライセンスの予約（License Reservation）] ボタンが表示されている。
- 該当する場合は、デバイスの Management Center Virtual の付与資格を含めて展開するデバイスおよび機能に十分なプラットフォームライセンスと機能ライセンスがある。

ステップ 6 これらのアイテムがないか、または誤っている場合は、アカウント担当者に連絡して問題を解決します。

（注） 問題が修正されるまではこのプロセスは続行しないでください。

[特定のライセンス（Specific Licenses）] メニューオプションの有効化

この手順では、Management Center の [スマートライセンス（Smart Licenses）] メニューオプションを [特定のライセンス（Specific Licenses）] に変更します。

手順

ステップ 1 USB キーボードと VGA モニターを使用して Management Center コンソールにアクセスするか、SSH を使用して管理インターフェイスにアクセスします。

ステップ 2 Management Center の CLI **管理者**アカウントにログインします。

ステップ 3 **expert** コマンドを入力して Linux シェルにアクセスします。

ステップ 4 特定のライセンスの予約のオプションにアクセスするには、次のコマンドを実行します。

sudo manage_slr.pl

例：

```
admin@fmc63betaslr: ~$ sudo manage_slr.pl
Password:


*************** Configuration Utility **************

1   Show SLR Status
2   Enable SLR
3   Disable SLR
0   Exit

************************************************************
Enter choice:
```

ステップ 5 オプション **2** を選択して、特定ライセンス予約を有効にします。

ステップ 6 オプション **0** を選択して、manage_slr ユーティリティを終了します。

ステップ 7 **exit** と入力し、Linux シェルを終了します。

ステップ 8 **exit** コマンドを入力してセキュアシェルのコマンドライン インターフェイスを終了します。

ステップ 9 Management Center の Web インターフェイスの [特定のライセンスの予約（Specific License Reservation）] ページにアクセスできることを確認します。

- [システム（System）]>[ライセンス（Licenses）]>[スマートライセンス（Smart Licenses）] ページが現在表示されている場合は、ページを更新します。

- それ以外の場合は、[システム（System）]>[ライセンス（Licenses）]>[特定のライセンス（Specific Licenses）] を選択します。

Management Center への特定のライセンス予約承認コードの入力

手順

ステップ 1 予約要求コードを生成します。

a) Management Center で、**[システム（System）]** > **[ライセンス（Licenses）]** > **[個別ライセンス（Specific Licenses）]** を選択します。
b) [生成（Generate）] をクリックします。
c) **予約要求コード**をメモします。

ステップ 2 予約承認コードを生成します。

a) Cisco Smart Software Manager に移動します：https://software.cisco.com/#SmartLicensing-Inventory
b) 必要に応じて、ページの右上から正しいアカウントを選択します。
c) 必要に応じて、[インベントリ（Inventory）] をクリックします。
d) [ライセンス（Licenses）] をクリックします。
e) [ライセンスの予約（License Reservation）] をクリックします。
f) 生成したコードを Management Center から [予約要求コード（Reservation Request Code）] ボックスに入力します。
g) [次へ（Next）] をクリックします。
h) [特定のライセンスの予約（Reserve a specific license）] を選択します。
i) 下にスクロールしてライセンス グリッド全体を表示します。
j) [予約する数量（Quantity To Reserve）] に、展開に必要な各プラットフォームと機能の数を入力します。

（注）
- 管理対象デバイスごとに（マルチインスタンス展開の場合はコンテナごとに）Essentials ライセンスを明示的に含める必要があります。
- Management Center Virtualを使用している場合は、各モジュール（マルチインスタンス展開において）または各管理対象デバイス（他のすべての展開において）にプラットフォームの資格を組み込む必要があります。
- 強力な暗号化機能を使用する場合は、次のとおりです。
  - スマートアカウント全体が輸出規制対象機能に対して有効になっている場合は、ここで何もする必要はありません。
  - 組織の資格が Management Center 単位の場合は、アプライアンス向けに適切なライセンスを選択する必要があります。

    Management Centerに適切なライセンス名を選択するには、「グローバル権限のないアカウントの輸出規制機能の有効化 （333 ページ）」の前提条件を参照してください。

k) [次へ（Next）] をクリックします。

l) [承認コードを生成（Generate Authorization Code）] をクリックします。

この時点で、ライセンスは、Smart Software Manager に従って使用中です。

m) Management Center に入力するための準備として承認コードをダウンロードします。

ステップ 3 Management Centerに承認コードを入力します。

a) Management Center で、[参照（Browse）] をクリックして、Smart Software Manager から生成した承認コードを含むテキストファイルをアップロードします。

b) [Install（インストール）] をクリックします。

c) [特定のライセンスの予約（Specific License Reservation）] ページに [使用の承認（Usage Authorization）] ステータスが [承認済み（authorized）] と表示されていることを確認します。

d)

ステップ 4 [予約済みライセンス（Reserved Licenses）] タブをクリックして、[承認コード（Authorization Code）] の生成時に選択したライセンスを確認します。

必要なライセンスが表示されていない場合は、必要なライセンスを追加します。詳細については、「特定のライセンスの予約の更新」を参照してください。

管理対象デバイスへの特定のライセンスの割り当て

この手順を使用して、複数の管理対象デバイスにライセンスを一度にすばやく割り当てます。

また、この手順を使用してライセンスを無効にするか、または1つのデバイスから別のデバイスにライセンスを移動できます。デバイスのライセンスを無効にすると、ライセンスに関連付けられた機能をそのデバイスで使用できません。

手順

ステップ1 [システム（System）] > [ライセンス（Licenses）] > [個別ライセンス（Specific Licenses）] を選択します。

ステップ2 [ライセンスの編集（Edit Licenses）] をクリックします。

ステップ3 各タブをクリックし、必要に応じてデバイスにライセンスを割り当てます。

ステップ4 [適用（Apply）] をクリックします。

ステップ5 [割り当て済みのライセンス（Assigned Licenses）] タブをクリックし、各デバイスでライセンスが正しくインストールされていることを確認します。

ステップ6 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

特定ライセンス予約の管理

このセクションでは、特定ライセンス予約を管理する方法について説明します。

重要：特定ライセンス予約展開の維持

展開を有効に保つ脅威に関するデータとソフトウェアを更新するには、「エアギャップ展開の維持 （281 ページ）」を参照してください。

すべての機能が中断せずに動作し続けるようにするには、ライセンスの有効期限を（[予約済みライセンス（Reserved Licenses）] タブ）で監視します。いずれかのライセンスの有効期限が切れたときに使用数が使用可能数よりも大きいと、Management Center は [不適合（Out of Compliance）] 状態になります。

特定のライセンスの予約の更新

Management Center で特定のライセンスが正常に展開された後は、この手順を使用して付与資格をいつでも追加または削除できます。

ライセンスの有効期限が切れた後にライセンスを更新する必要がある場合は、この手順を使用します。必要なライセンスがない場合、次のアクションが制限されます。

- デバイス登録に使用
- ポリシーの展開

手順

ステップ 1 Management Center で、この Management Center の一意の製品インスタンス識別子を取得します。

a) **[システム（System）]**>**[ライセンス（Licenses）]**>**[特定のライセンス（Specific Licenses）]** を選択します。

b) [製品インスタンス（Product Instance）] の値をメモします。

この値はこのプロセス中に何度か必要になります。

ステップ 2 Smart Software Manager で、更新する Management Center を特定します。

a) Smart Software Manager に移動します。

https://software.cisco.com/#SmartLicensing-Inventory

b) 必要に応じて、[インベントリ（Inventory）] をクリックします。

c) [製品インスタンス（Product Instances）] をクリックします。

d) [タイプ（Type）] 列に **FP**、[名前（Name）] 列に一般的な SKU（ホスト名ではない）が設定されている製品インスタンスを探します。また他のテーブル列の値を使用すると、どの Management Center が正しい Management Center かを判断するのに役立ちます。名前をクリックします。

e) **UUID** を調べ、変更しようとしている Management Center の UUID かどうかを確認します。

違う場合は、正しい Management Center が見つかるまで、これらの手順を繰り返す必要があります。

ステップ 3 Smart Software Manager で適切な Management Center が見つかったら、予約したライセンスを更新し、新しい承認コードを生成します。

a) 正しい UUID が表示されているページで、**[アクション（Actions）]**>**[予約済みのライセンスの更新（Update Reserved Licenses）]** を選択します。

b) 必要に応じて、予約済みライセンスを更新します。

（注）
- 管理対象デバイスごとに（マルチインスタンス展開の場合はコンテナごとに）Essentials ライセンスを明示的に含める必要があります。
- Management Center Virtualを使用している場合は、各モジュール（マルチインスタンス展開において）または各管理対象デバイス（他のすべての展開において）にプラットフォームの資格を組み込む必要があります。
- 強力な暗号化機能を使用する場合は、次のとおりです。
  - スマートアカウント全体が輸出規制対象機能に対して有効になっている場合は、ここで何もする必要はありません。
  - 組織の資格が Management Center 単位の場合は、アプライアンス向けに適切なライセンスを選択する必要があります。

    Management Centerに適切なライセンス名を選択するには、「グローバル権限のないアカウントの輸出規制機能の有効化 （333 ページ）」の前提条件を参照してください。

c) [次へ（Next）] をクリックして詳細を確認します。
d) [承認コードを生成（Generate Authorization Code）] をクリックします。
e) Management Center に入力するための準備として承認コードをダウンロードします。
f) [予約の更新（Update Reservation）] ページを開いたままにしておきます。この手順の後半でこのページに戻ります。

ステップ 4 Management Center で個別ライセンスを更新します。

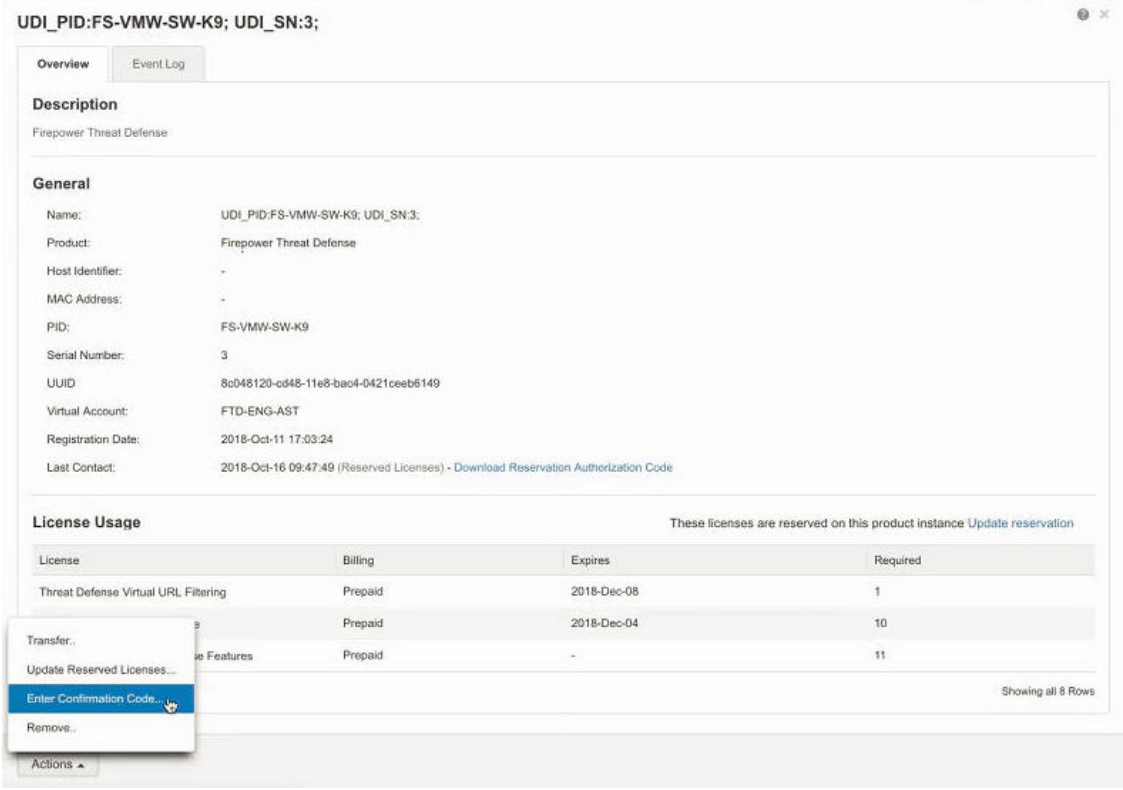
a) **[システム（System）] > [ライセンス（Licenses）] > [個別ライセンス（Specific Licenses）]** を選択します。
b) [SLR の編集（Edit SLR）] をクリックします。
c) [参照（Browse）] をクリックして、新たに生成された承認コードをアップロードします。
d) [インストール（Install）] をクリックしてライセンスを更新します。

   承認コードが正常にインストールされたら、Management Center の [予約済み（Reserved）] 列に表示されたライセンスが、Smart Software Manager で予約したライセンスと一致していることを確認します。

e) **確認コード**をメモします。

ステップ 5 Smart Software Manager に承認コードを入力するには、次の手順を実行します。

a) この手順の前半で開いたままにしておいた Smart Software Manager のページに戻ります。
b) **[アクション（Actions）] > [確認コードの入力（Enter Confirmation Code）]** を選択します。



c) Management Center から生成したコードを入力します。

ステップ 6 Management Center で、ライセンスが予期したとおりに予約されていること、および各管理対象デバイスの各機能に [チェックマーク（Check Mark）]（） が付いた緑色の丸が表示されていることを確認します。

詳細については「特定ライセンス予約のステータスのモニタリング（354ページ）」を必要に応じて参照してください。

ステップ 7 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

特定のライセンスの予約の非アクティブ化と返却

特定のライセンスが不要になった場合は、そのライセンスをスマートアカウントに戻す必要があります。スマートライセンシングアカウントを登録する場合は、[特定のライセンスの予約（Specific License Reservation）] を無効にする必要があります（以下の手順の手順 6）。

重要 この手順のすべてのステップを実行しないと、ライセンスは使用中の状態のままとなり、再利用できません。

この手順で、Management Center と関連付けられていたすべてのライセンス権限がバーチャルアカウントに戻されます。登録を解除すると、ライセンスが付与された機能への更新や変更が許可されなくなります。

手順

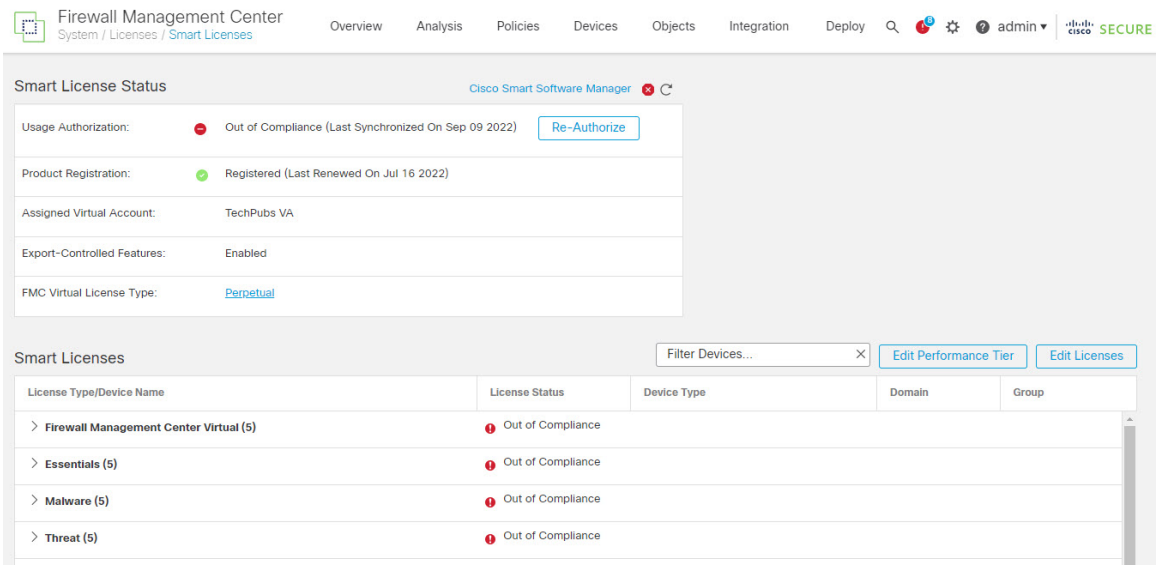
ステップ 1 Management Center の Web インターフェイスで、[システム（System）]>[ライセンス（Licenses）]>[特定のライセンス（Specific License）] を選択します。

ステップ 2 この Management Center の [製品インスタンス（Product Instance）] の識別子をメモします。

ステップ 3 Management Center からリターンコードを生成します。

a) [SLR の返却（Return SLR）] をクリックします。

次の図に、[SLR の返却（Return SLR）] を示します。



デバイスはライセンスのない状態になり、Management Center は登録解除状態に移行します。リターンコードが生成され、Management Center を SLR に再登録できます。

b) **返却コード**をメモします。

ステップ 4 Smart Software Manager で、登録解除する Management Center を特定します。

a) Smart Software Manager に移動します。

https://software.cisco.com/#SmartLicensing-Inventory

b) 必要に応じて、[インベントリ（Inventory）] をクリックします。

c) [製品インスタンス（Product Instances）] をクリックします。

d) [タイプ（Type）] 列に **FP**、[名前（Name）] 列に一般的な SKU（ホスト名ではない）が設定されている製品インスタンスを探します。また他のテーブル列の値を使用すると、どの Management Center が正しい Management Center かを判断するのに役立ちます。名前をクリックします。

e) **UUID** を調べ、変更しようとしている Management Center の UUID かどうかを確認します。

違う場合は、正しい Management Center が見つかるまで、これらの手順を繰り返す必要があります。

ステップ 5 正しい Management Center が特定されたら、ライセンスをスマートアカウントに戻します。

a) 正しい UUID が表示されたページで、[アクション（Actions）] > [削除（Remove）] を選択します。

b) Management Center から生成した予約リターンコードを [製品インスタンスの削除（Remove Product Instance）] ダイアログボックスに入力します。

c) [Remove Product Instance] をクリックします。

特定の予約済みライセンスがスマートアカウントの使用可能プールに戻り、この Management Center が Smart Software Manager の製品インスタンスリストから削除されます。

ステップ 6 Management Center の Linux シェルで、特定のライセンスを無効にします。

a) USB キーボードと VGA モニターを使用して Management Center コンソールにアクセスするか、SSH を使用して管理インターフェイスにアクセスします。

b) Management Center の CLI **管理者**アカウントにログインします。これにより、コマンドライン インターフェイスにアクセスできるようになります。

c) **expert** コマンドを入力して Linux シェルにアクセスします。

d) makecall ディレクトリで、次のコマンドを実行します。

sudo manage_slr.pl

例：

```
admin@fmc63betaslr: ~$ sudo manage_slr.pl
Password:


*************** Configuration Utility **************

1   Show SLR Status
2   Enable SLR
3   Disable SLR
0   Exit

************************************************************
Enter choice:
```

e) オプション **3** を選択して、特定のライセンスの予約を無効にします。

f) オプション **0** を選択して、manage_slr ユーティリティを終了します。

g) **exit** と入力し、Linux シェルを終了します。

h) **exit** コマンドを入力してセキュアシェルのコマンドライン インターフェイスを終了します。

特定ライセンス予約のステータスのモニタリング

次に示すように、[システム（System）]>[ライセンス（Licenses）]>[特定のライセンス（Specific Licenses）] ページには Management Center でのライセンスの使用状況の概要が表示されます。

使用の認証

可能なステータス値は次のとおりです。

- [承認済み（Authorized）]：Management Center は、アプライアンスのライセンスの付与資格を承認したライセンス認証局に準拠しており、正常に登録されています。
- [コンプライアンス不適合（Out-of-compliance）]：ライセンスの期限が切れているか、または Management Center が予約していないにもかかわらずライセンスを過剰に使用している場合、[コンプライアンス不適合（Out-of-Compliance）] がステータスに表示されます。[特定のライセンスの予約（Specific License Reservation）] にライセンスの付与資格が適用されるため、アクションを実行する必要があります。

製品登録

特定の登録ステータスと、Management Center で承認コードが最後にインストールされたか、または更新された日付を指定します。

輸出管理機能

Management Center の輸出規制対象機能を有効にしたかどうかを指定します。

輸出規制対象機能の詳細については、「輸出規制対象の機能のライセンス （313 ページ）」を参照してください。

製品インスタンス

この Management Center のユニバーサル一意識別子（UUID）。この値は Smart Software Manager でこのデバイスを識別します。

確認コード

特定のライセンスを更新するか、または非アクティブ化して返却する場合に [確認コード（Confirmation Code）] が必要です。

[割り当て済みライセンス（Assigned Licenses）] タブ

各デバイスとそれぞれのステータスに割り当てられているライセンスを表示します。

[予約済みライセンス（Reserved Licenses）] タブ

割当に使用されているライセンスと使用可能なライセンスの数、およびライセンスの有効期限を表示します。

特定のライセンスの予約のトラブルシューティング

Smart Software Manager の製品インスタンスリストから特定の Management Center を識別する方法を教えてください。

Smart Software Manager の [製品インスタンス（Product Instances）] ページで、テーブル内の列のいずれかの値に基づいて製品インスタンスが識別できない場合は、**FP** タイプの汎用製品インスタンスそれぞれの名前をクリックする必要があります。このページの **UUID** の値は 1 つの Management Center を一意に識別します。

Management Center の Web インターフェイスでは、Management Center の UUID は [システム（System）] > [ライセンス（Licenses）] > [特定のライセンス（Specific License）] ページに表示される [製品インスタンス（Product Instance）] の値です。

Smart Software Manager の [ライセンスの予約（License Reservation）] ボタンが表示されません。

[ライセンス予約（License Reservation）] ボタンが表示されない場合、お使いのアカウントでは特定のライセンスの予約が承認されていません。Linux シェルで特定のライセンスの予約をすでに有効にし、要求コードを生成している場合は、次の手順を実行します。

1. Management Center の Web インターフェイスですでに**要求コード**を生成している場合は、その要求コードをキャンセルします。
2. 「特定のライセンスの予約の非アクティブ化と返却 （351 ページ）」のセクションで説明しているように、Management Center の Linux シェルで特定のライセンスの予約を無効にします。
3. スマートトークンを使用して、通常モードで Management Center を Smart Software Manager に登録します。
4. Cisco TAC に連絡して、自分のスマート アカウントの個別ライセンスを有効にします。

ライセンス プロセスの最中に中断が発生しました。中断した場所を取得する方法を教えてください。

承認コードは生成したが、Smart Software Manager からまだダウンロードしていない場合は、Smart Software Manager の [製品インスタンス（Product Instance）] ページに移動し、製品インスタンスをクリックした後、[予約承認コードのダウンロード（Download Reservation Authorization Code）] をクリックします。

デバイスを Management Center Virtual に登録できません。

登録するデバイスをカバーするのに十分な Management Center Virtual の資格がスマートアカウントにあることを確認してから展開を更新し、必要な資格を追加します。

「特定のライセンスの予約の更新 （348 ページ）」を参照してください。

特定のライセンスを有効にしていましたが、[スマート ライセンス（Smart License）] ページが表示されなくなりました。

これは予期されている動作です。[特定のライセンス（Specific Licensing）] を有効にすると、スマート ライセンスは無効になります。[特定のライセンス（Specific License）] ページを使用してライセンスの操作を実行できます。

スマートライセンスを使用する場合は、特定のライセンスを返却する必要があります。詳細については、「特定のライセンスの予約の非アクティブ化と返却（351 ページ）」を参照してください。

Management Center Virtual に [特定のライセンス（Specific License）] ページが表示されません。

[特定のライセンス（Specific License）] ページを表示するには、特定のライセンスを有効にする必要があります。詳細については、「[特定のライセンス（Specific Licenses）] メニュー オプションの有効化（345 ページ）」を参照してください。

特定のライセンスを無効にしましたが、返却コードをコピーするのを忘れてしまいました。どうすればよいでしょうか。

リターンコードは Management Center Virtual に保存されています。Linux シェルから特定のライセンスをもう一度有効にし（「[特定のライセンス（Specific Licenses）] メニュー オプションの有効化（345 ページ）」を参照）、Management Center Virtual の Web インターフェイスを更新します。[戻りコード（Return Code）] が表示されます。

レガシー Management Center PAK ベースのライセンスの設定

Management Center は、プラットフォームライセンスとしてスマートライセンスまたはレガシー PAK（製品アクティベーションキー）ライセンスをサポートします。この手順では、PAK ベースのライセンスを適用する方法について説明します。

スマートアカウントを再登録した後、すべての従来型デバイスのクラシックライセンスを手動で追加する必要があります。

始める前に

- ライセンス購入時に Cisco が提供したソフトウェア権利証明書にある製品アクティベーションキー（PAK）をお手元にご用意ください。レガシーの、以前のシスコのライセンスの場合は、サポートに問い合わせてください。

手順

ステップ 1 ライセンスキーは、Smart Software Manager で Management Center を一意に識別します。これは、Management Center の製品コード（66 など）と管理ポート（eth0）の MAC アドレスで構成されます（66:00:00:77:FF:CC:88 など）。

a) **システム**（⚙）>**[ライセンス（Licenses）]**>**[クラシックライセンス（Classic Licenses）]** を選択します。

b) [新規ライセンスの追加（Add New License）] をクリックします。

c) [機能ライセンスの追加（Add Feature License）] ダイアログの上部にある [ライセンス キー（License Key）] フィールドの値をメモします。

ステップ 2 **システム**（⚙）>**[ライセンス（Licenses）]**>**[クラシックライセンス（Classic Licenses）]** を選択します。

ステップ 3 [新規ライセンスの追加（Add New License）] をクリックします。

ステップ 4 必要に応じ、続いて以下を行います。

- ライセンステキストをすでに取得している場合は、ステップ 8 にスキップしてください。
- ライセンスのテキストを取得する必要がある場合は、次の手順を実行します。

ステップ 5 [ライセンス取得（Get License）] をクリックして、ライセンス登録ポータルを開きます。

（注） ご使用のコンピュータからインターネットにアクセスできない場合は、アクセスできるコンピュータから http://cisco.com/go/licenseを探します。

ステップ 6 ライセンス登録ポータルで、PAK からライセンスを生成します：https://cisco.com/go/license。

この手順には、購入時に入手した PAK と、Management Center のライセンスキーが必要です。

このポータルの使用方法の詳細については、次を参照してください。

https://slexui.cloudapps.cisco.com/SWIFT/LicensingUI/Quickstart

これらのリンクにアクセスするには、アカウントのクレデンシャルが必要です。

ステップ 7 ライセンス登録ポータルの表示から、ないしはライセンス登録ポータルより送られてくるメールからライセンス テキストをコピーします。

重要 ポータルまたは電子メール メッセージ内のライセンス テキスト ブロックには、複数のライセンスを含めることができます。各ライセンスは、BEGIN LICENSE 行と END LICENSE 行で囲まれます。一度に 1 つのライセンスしかコピーして貼り付けることができません。

ステップ 8 Management Center Virtual の Web インターフェイスの [機能ライセンスの追加（Add Feature License）] ページに戻ります。

ステップ 9 [ライセンス（License）] フィールドにライセンス テキストを貼り付けます。

ステップ 10 [ライセンスの検証（Verify License）] をクリックします。

ライセンスが無効となる場合は、ライセンス テキストが正しくコピーされているか確認します。

ステップ 11 [ライセンスの提出（Submit License）] をクリックします。

ライセンスに関する追加情報

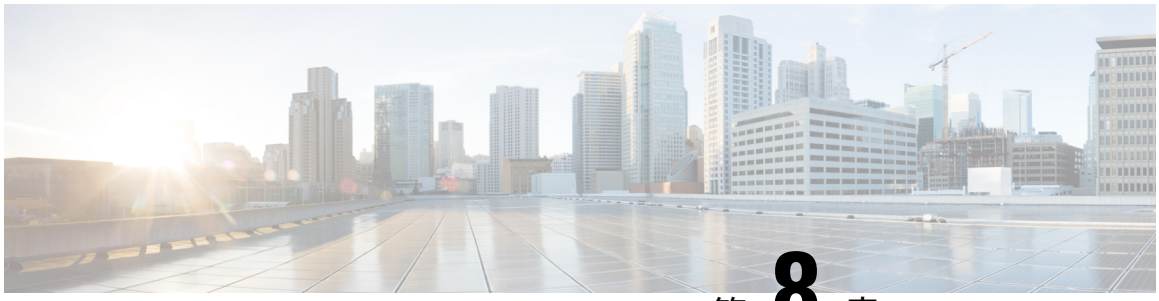
ライセンスに関するよくある質問の解決に役立つその他の情報については、次のドキュメントを参照してください。

- FAQ：ライセンスに関する FAQ
- ライセンスロードマップ

ライセンスの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
スマートライセンスの標準化	7.3	任意（Any）	Management Center の GUI で以下のライセンス名が変更されました。 • Base は Essentials に変更 • Threat は IPS に変更 • Malware は Malware Defense に変更 • RA VPN/AnyConnect License は Cisco Secure Client に変更 • AnyConnect Plus は Secure Client Advantage に変更 • AnyConnect Apex は Secure Client Premier に変更 • AnyConnect Apex および Plus は Secure Client Premier および Advantage に変更 • AnyConnect VPN Only は Secure Client VPN Only に変更
キャリアライセンスのサポート	7.3	任意（Any）	キャリアライセンスは、Diameter、GTP/GPRS、SCTP および M3UA プロトコルを有効にします。 新規/変更された画面：**[システム（System）] > [スマートライセンス（Smart Licenses）]**

機能	最小 Management Center	最小 Threat Defense	詳細
Threat Defense Virtual のパフォーマンス階層ライセンス	7.0	任意（Any）	パフォーマンス階層型ライセンスでは、導入要件に基づいて異なるスループットレベルと VPN 接続制限を提供します。ライセンス階層は新しい Threat Defense Virtual モデルにマッピングされます。
Firepower 4100/9300 の Threat Defense に対する複数インスタンス機能のライセンス	6.3	任意（Any）	Firepower 4100/9300 に複数の Threat Defense コンテナ インスタンスを展開できるようになりました。セキュリティ モジュール/エンジンの機能ごとに必要なライセンスは 1 つのみです。基本ライセンスは、各インスタンスに自動的に割り当てられます。 新規/変更された画面：**[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）]** サポート対象プラットフォーム：Firepower 4100/9300 の Threat Defense
エアギャップ展開に対する特定のライセンスの予約	6.3	任意（Any）	展開でインターネットに接続してシスコのライセンス認証局と通信できない顧客は特定のライセンスの予約を使用できます。 新規/変更された画面：**[システム（System）] > [ライセンス（Licenses）] > [特定のライセンス（Specific Licenses）]**（このオプションはデフォルトでは使用できません。） サポートされるプラットフォーム：Management Center、Threat Defense
制限付きの顧客の輸出規制対象機能	6.3	任意（Any）	スマートアカウントで制限付き機能を使用する資格を持たない特定の顧客は、期間ベースのライセンスを承認を受けて購入することができます。 サポートされるプラットフォーム：Management Center、Threat Defense



第 8 章

ハイ アベイラビリティ

以下のトピックでは、Cisco Secure Firewall Management Center のアクティブ/スタンバイ ハイ アベイラビリティを設定する方法を示します。

Management Center のハイ アベイラビリティについて

運用の継続性を確保するために、ハイ アベイラビリティ機能を使用して、冗長 Management Center でデバイスを管理するように指定することができます。Management Center では、1 つのアプライアンスがアクティブユニットであり、デバイスを管理する、アクティブ/スタンバイ高可用性がサポートされます。スタンバイ ユニットは、アクティブにデバイスを管理しません。アクティブ ユニットは、データ ストアに設定データを書き込み、両方のユニットのデータを複製し、必要な場合は同期を使用してスタンバイ ユニットと一部の情報を共有します。

アクティブ/スタンバイ ハイ アベイラビリティでは、プライマリ Management Center に障害が発生した場合、セカンダリ Management Center を設定して、プライマリの機能を引き継ぐこと

ができます。プライマリ Management Center に障害が発生した場合は、セカンダリ Management Center をプロモートしてアクティブ ユニットにする必要があります。

イベント データは、管理対象デバイスからハイ アベイラビリティ ペアの両方の Management Center に配信されます。一方の Management Center で障害が発生した場合、他方の Management Center の使用を中断せずにネットワークをモニタすることができます。

ハイ アベイラビリティ ペアとして設定する 2 つの Management Center は、信頼された同じ管理ネットワーク上に存在する必要も、同じ地理的ロケーションに存在する必要もありません。

注意 システムでは一部の機能をアクティブ Management Center に制限しているため、そのアプライアンスで障害が発生した場合は、スタンバイ Management Center をアクティブにプロモートする必要があります。

（注） 変更の展開が成功した直後に Management Center でスイッチオーバーがトリガーされると、新しいアクティブ Management Center でプレビュー設定が機能しなくなる可能性があります。これは、ポリシー展開機能に影響を与えません。必要な同期が完了した後に Management Center でスイッチオーバーをトリガーすることをお勧めします。

同様に、Management Center HA 同期が劣化状態の場合、スイッチオーバーをトリガーしたり、ロールを変更したりすると、Management Center HA によってデータベースが破損し、致命的な状態になる可能性があります。この問題を解決するための支援が必要な場合は、Cisco Technical Assistance Center（TAC）にただちに連絡することをお勧めします。

この HA 同期は、さまざまな理由で劣化状態になる可能性があります。この章にある「高可用性ペアでの Management Center の交換 （382 ページ）」の項では、いくつかの障害シナリオと、問題を修正するための後続の手順について説明しています。劣化状態の理由またはシナリオが説明されているシナリオと一致する場合は、手順に従って問題を修正します。それら以外の理由の場合は、TAC に連絡することをお勧めします。

リモート アクセス VPN のハイ アベイラビリティについて

プライマリ デバイスに、CertEnrollment オブジェクトを使用して登録された ID 証明書を使用したリモート アクセス VPN 設定がある場合、セカンダリ デバイスには、同じ CertEnrollment オブジェクトを使用して登録された ID 証明書が必要です。CertEnrollment オブジェクトは、デバイス固有のオーバーライドにより、プライマリデバイスとセカンダリデバイスに異なる値を持つことができます。この制限は、ハイ アベイラビリティの形成前に 2 つのデバイスに同じ CertEnrollment オブジェクトを登録することだけです。

Management Center High Availability での SNMP の動作

SNMP が設定された HA ペアでは、アラートポリシーを展開すると、プライマリ Management Center が SNMP トラップを送信します。プライマリ Management Center に障害が発生すると、セカンダリ Management Center がアクティブユニットになり、追加の設定を必要とせずに SNMP トラップを送信します。

Management Center 高可用性のロールとステータス

プライマリ/セカンダリの役割

Secure Firewall Management Center を高可用性ペアの形でセットアップする際は、一方の Secure Firewall Management Center をプライマリとして設定し、もう一方をセカンダリとして設定します。設定中に、プライマリ ユニットのポリシーは、セカンダリ ユニットに同期されます。この同期が完了すると、プライマリ Secure Firewall Management Center がアクティブ ピアになり、セカンダリ Secure Firewall Management Center がスタンバイ ピアになって、2 つのユニットが管理対象デバイスおよびポリシー設定に対して単一のアプライアンスとして機能します。

アクティブ/スタンバイ ステータス

高可用性ペアを構成する 2 つの Secure Firewall Management Center の間の主な違いは、どちらがアクティブ ピアで、どちらがスタンバイ ピアであるかという点です。アクティブ Secure Firewall Management Center は、完全に機能する状態に維持され、デバイスとポリシーを管理するために使用できます。スタンバイ Secure Firewall Management Center では機能が非表示になるため、設定の変更を行うことはできません。

Management Center 高可用性ペアでのイベント処理

ハイ アベイラビリティ ペアの両方の Management Center が管理対象デバイスからイベントを受信するため、アプライアンスの管理 IP アドレスは共有されません。これは、いずれかの Management Center で障害が発生した場合に、継続的な処理を確保するために介入する必要がないことを意味します。

AMP クラウド接続とマルウェア情報

ハイ アベイラビリティ ペアを構成する Management Center は、ファイル ポリシーおよび関連する設定は共有しますが、シスコ AMP クラウド接続およびマルウェア処理は共有しません。運用の継続性を確保し、検出されたファイルのマルウェア処理が両方の Management Center で同じであるようにするためには、プライマリとセカンダリ両方の Management Center が AMP クラウドにアクセスできる必要があります。

URL フィルタリングとセキュリティ インテリジェンス

URL フィルタリングとセキュリティ インテリジェンスの設定および情報は、ハイ アベイラビリティ展開の Secure Firewall Management Center の間で同期されます。ただし、プライマリ Secure Firewall Management Center だけが、セキュリティ インテリジェンス フィードの更新用の URL カテゴリおよびレピュテーション データをダウンロードします。

プライマリ Secure Firewall Management Center に障害が発生した場合は、セカンダリ Secure Firewall Management Center がインターネットにアクセスして脅威インテリジェンスを更新できることを確認する必要があるだけでなく、セカンダリ Secure Firewall Management Center の Web インターフェイスを使用してセカンダリをアクティブにプロモートする必要もあります。

Management Center のフェールオーバー中のユーザーデータの処理

プライマリ Management Center に障害が発生した場合、セカンダリ Management Center は、TS エージェント アイデンティティ ソースからのユーザーから IP へのマッピングと、ISE/ISE-PIC アイデンティティソースからの SGT マッピングを、管理対象デバイスに伝播します。アイデンティティソースでまだ認識されていないユーザーは、[不明（Unknown）] として識別されます。

ダウンタイム後、[不明（Unknown）]ユーザはアイデンティティ ポリシーのルールに従って再び識別され、処理されます。

Management Center 高可用性ペアの設定管理

ハイ アベイラビリティ展開では、アクティブな Management Center のみがデバイスを管理し、ポリシーを適用できます。両方の Management Center は継続的な同期状態を保ちます。

アクティブ状態の Management Center に障害が発生すると、ハイ アベイラビリティ ペアは縮退状態となります。縮退状態は、スタンバイ状態のアプライアンスを手動でアクティブ状態に上げるまで続きます。スタンバイ状態のアプライアンスをアクティブ状態に上げると、両アプライアンスのメンテナンス モードが終了します。

Management Center 高可用性ディザスタリカバリ

ディザスタリカバリの状況では、手動スイッチオーバーを実行する必要があります。プライマリ Management Center（FMC1）で障害が発生した場合は、セカンダリ Management Center（FMC2）の Web インターフェイスにアクセスしてピアを切り替えます。これは、逆に、セカンダリ（FMC2）に障害が発生した場合にも当てはまります。詳細については、Management Center のハイアベイラビリティペアにおけるピアの切り替え （379 ページ）を参照してください。

障害が発生した Management Center の復旧については、高可用性ペアでの Management Center の交換 （382 ページ）を参照してください。

シングルサインオンと高可用性ペア

高可用性設定の Management Center ではシングルサインオンをサポートできますが、次の考慮事項に留意する必要があります。

- SSO 設定は、高可用性ペアのメンバー間で同期されません。ペアの各メンバーで個別に SSO を設定する必要があります。
- 高可用性ペアの両方の Management Center は、SSO に同じアイデンティティ プロバイダー（IdP）を使用する必要があります。SSO 用に設定された各 Management Center の IdP で、サービス プロバイダー アプリケーションを設定する必要があります。
- 両方が SSO をサポートするように設定されている Management Center の高可用性ペアでは、ユーザーは SSO を使用してセカンダリ Management Center に初めてアクセスする前

に、最初に SSO を使用してプライマリ Management Center に少なくとも 1 回ログインする必要があります。

- 高可用性ペアで Management Center の SSO を設定する場合：
  - プライマリ Management Center で SSO を設定する場合、セカンダリ Management Center で SSO を設定する必要はありません。
  - セカンダリ Management Center で SSO を設定する場合は、プライマリ Management Center でも SSO を設定する必要があります。（これは、SSO ユーザーがセカンダリ Management Center にログインする前に、プライマリ Management Center に少なくとも 1 回ログインする必要があるためです）。

関連トピック

SAML シングルサインオンの設定 （169 ページ）

バックアップ中の Management Center の高可用性動作

Management Center 高可用性ペアでバックアップを実行する場合、バックアップ動作によってピア間の同期が一時停止します。この動作中は、引き続きアクティブな Management Center を使用できますが、スタンバイ ピアを使用することはできません。

バックアップが完了すると、同期が再開され、少しの間、アクティブ ピアでのプロセスが無効になります。この一時停止中、[高可用性（High Availability）] ページには、すべてのプロセスが再開されるまでは一時的に保留ページが表示されます。

Management Center 高可用性スプリットブレイン

高可用性ペアのアクティブな Management Center が（電源の問題、ネットワークや接続の問題で）ダウンした場合は、スタンバイ Management Center をアクティブ状態に昇格させることができます。元のアクティブなピアが起動すると、両方のピアがアクティブであるとみなされる場合があります。この状態は「スプリットブレイン」と定義されます。このような状況が発生すると、システムによってアクティブなアプライアンスを選択するように要求されます。それによって、もう一方のアプライアンスはスタンバイ状態に降格します。

アクティブな Management Center がダウンした（またはネットワーク障害により切断された）場合は、高可用性を中断するか、またはロールを切り替えることができます。スタンバイ Management Center は縮退状態になります。

（注） セカンダリとして使用するアプライアンスがどれであっても、スプリットブレインの解決時にデバイス登録とポリシー設定のすべてが失われます。たとえば、セカンダリに存在し、プライマリには存在しなかったポリシーへの変更は失われます。Management Center が両方のアプライアンスがアクティブな高可用スプリットブレインシナリオである場合に、スプリットブレインを解決する前に管理対象デバイスを登録してポリシーを展開する場合は、ハイアベイラビリティを再確立する前に、ポリシーをエクスポートして、管理対象デバイスを対象のスタンバイ Management Center から登録解除する必要があります。その後、管理対象デバイスを登録し、目的のアクティブ Management Center にポリシーをインポートすることができます。

高可用性ペアの Management Center のアップグレード

Cisco は、各種の更新プログラムを電子形式で定期的に配信します。更新プログラムには、システム ソフトウェアのメジャーおよびマイナー アップグレードが含まれます。ハイ アベイラビリティ セットアップでは、これらの更新を両方の Management Center にインストールする必要が生じることがあります。

警告 アップグレード中には、少なくとも 1 つの Management Center を動作状態に維持してください。

始める前に

アップグレードに付属しているリリース ノートまたはアドバイザリ テキストを読んでください。リリースノートでは、サポートされるプラットフォーム、互換性、前提条件、警告、特定のインストールおよびアンインストールの手順など重要なデータが提供されます。

手順

ステップ 1 アクティブ Management Center の Web インターフェイスにアクセスし、データ同期を一時停止します（ペアにされた Management Center 間での通信の一時停止 （380 ページ）を参照）。

ステップ 2 スタンバイ Management Center をアップグレードします。
アップグレードが完了すると、スタンバイユニットがアクティブになります。両方のピアがアクティブになると、ハイアベイラビリティペアが劣化状態(スプリットブレイン)になります。

ステップ 3 もう一方の Management Center をアップグレードします。

ステップ 4 どちらの Management Center をスタンバイとして使用するかを決定します。同期を一時停止した後にスタンバイに追加された追加のデバイスまたはポリシーは、アクティブ Management Center に同期されません。その追加のデバイスのみを登録解除し、維持する必要がある設定をエクスポートします。

新しいアクティブ Management Center を選択すると、セカンダリとして指定した Management Center は、同期されていないデバイス登録と展開されたポリシー設定を失います。

ステップ 5 最新のポリシーとデバイスに必要なすべての設定を含む新しいアクティブ Management Center を選択して、スプリットブレインを解決します。

Management Center のハイ アベイラビリティのトラブルシューティング

この項では、Management Center のハイ アベイラビリティ操作のいくつかの一般的なエラーに関するトラブルシューティング情報を示します。

エラー	説明	ソリューション
スタンバイにログインする前に、アクティブな Management Center でパスワードをリセットする必要があります。	アカウントの強制的なパスワードリセットが有効になっているときに、スタンバイ Management Center にログインしようとしました。	データベースはスタンバイ Management Center に対して読み取り専用であるため、アクティブな Management Center のログインページでパスワードをリセットします。
500 内部（500 Internal）	ピア ロールの切り替えや同期の一時停止と再開などのクリティカルな Management Center のハイ アベイラビリティ操作を実行しているときに Web インターフェイスにアクセスしようとすると表示されることがあります。	Web インターフェイスを使用する前に、操作が完了するまでお待ちください。

エラー	説明	ソリューション
システム プロセスが起動しています、お待ちください（System processes are starting, please wait） また、Web インターフェイスは応答しません。（Also, the web interface does not respond.）	ハイ アベイラビリティまたはデータ同期操作中に Management Center が再起動（手動でまたは電源切断からの回復中に）する場合に表示されることがあります。	**1.** Management Center シェルにアクセスし、`manage_hadc.pl` コマンドを使用して Management Center のハイ アベイラビリティ構成ユーティリティにアクセスします。 （注） `sudo` を使用して、ルートユーザとしてユーティリティを実行します。 **2.** オプション 5 を使用してミラーリング操作を一時停止します。 Management Center Web インターフェイスをリロードします。 **3.** Web インターフェイスを使用して同期を再開します。**[統合（Integration）] > [その他の統合（Other Integrations）]** を選択し、[高可用性（High Availability）] タブをクリックして、[同期の再開（Resume Synchronization）] を選択します。

エラー	説明	ソリューション
デバイス登録ステータス：ホスト <string> が到達不能（Device Registration Status:Host <*string*> is not reachable）	Threat Defense の初期設定時に、Management Center の IP アドレスと NAT ID が指定されている場合は、[ホスト（Host）] フィールドを空白のままにできます。ただし、両方の Management Center が NAT の背後にある HA 環境では、Threat Defense をセカンダリ Management Center に追加すると、このエラーが発生します。	1. プライマリ Management Center から Threat Defense を削除します。『Cisco Secure Firewall Management Center Device Configuration Guide』の「*Delete a Device from the* Management Center」を参照してください。 2. **configure manager delete** コマンドを使用して Threat Defense からマネージャを削除します。Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。 3. [ホスト（Host）] フィールドで、Threat Defense デバイスの IP アドレスまたは名前を使用して Threat Defense を Management Center に追加します。『Cisco Secure Firewall Management Center Device Configuration Guide』の「*Add a Device to the* Management Center」を参照してください。

エラー	説明	ソリューション
デバイス登録ステータス：ホスト <string> が到達不能（Device Registration Status:Host <*string*> is not reachable）	セカンダリ Management Center と Threat Defense デバイスの両方が NAT の背後にある高可用性展開で、Threat Defense デバイスをセカンダリ Management Center センターに追加すると、エラーが発生します。	スタンバイ Management Center Web インターフェイスで、**[統合（Integration）] > [その他の統合（Other Integrations）] > [高可用性（High Availability）]** をクリックします。保留中のデバイス登録のテーブルで、保留中のデバイスの IP アドレスをクリックし、IP アドレスを Threat Defense のパブリック IP アドレスに変更します。 または 1. Threat Defense シェルにアクセスし、`show manager` コマンドを使用して、スタンバイ Management Center のエントリ識別子の値を取得します。 2. Threat Defense シェルで、スタンバイ Management Center のホスト名をパブリック IP アドレスに編集します。エントリ識別子とホスト IP アドレスを使用して `configure manager edit <standby_uuid> hostname <standby_ip>` コマンドを実行します。 詳細については、「Management Center 高可用性で CLI を使用してデバイス登録を解決する（378 ページ）」を参照してください。

エラー	説明	ソリューション
高可用性 Management Center 間のデバイス設定の同期が停止しています。（Device configuration synchronization has been stopped between high availability Management Centers.）	Management Center HA 同期中にデバイス設定履歴ファイルが他の設定データと並行して同期されるようになりました。Management Center は、設定履歴ファイルの同期タスクをモニターし、過去 6 時間以内に同期が行われていない場合は通知します。この正常アラートは、アクティブとスタンバイの両方の Management Center に表示されます。	アクティブとスタンバイの両方の Management Center が劣化状態に移行します。問題のトラブルシューティングについては、シスコサポートにお問い合わせください。

Management Center 高可用性の要件

モデルのサポート

「ハードウェア要件 （371 ページ）」を参照してください。

仮想モデルのサポート

仮想プラットフォームの要件 （372 ページ） を参照してください。

サポートされるドメイン

Global

ユーザの役割

管理者

ハードウェア要件

- すべての Management Center ハードウェアが高可用性をサポートしている。ピアは同じモデルである必要がある。
- ピアは異なるデータセンターにあり、互いに物理的および地理的に分離可能である。
- 高可用性設定の帯域幅要件は、ネットワークのサイズ、管理対象デバイスの数、イベントとログの量、設定更新のサイズと頻度など、さまざまな要因によって異なります。

  一般的な Management Center 高可用性展開では、100 ミリ秒に近い高遅延のネットワークの場合、ピア間に 5 MBps 以上のネットワーク帯域幅が推奨されます。

- プライマリピアのバックアップをセカンダリに復元しないでください。
- Management Center ハイアベイラビリティ構成のライセンス要件 （373 ページ）も参照してください。

仮想プラットフォームの要件

高可用性は、次のパブリッククラウド プラットフォームでサポートされています。

- Amazon Web Services（AWS）
- Oracle Cloud Infrastrucure（OCI）

また、次のオンプレミス/プライベートクラウド プラットフォームでサポートされています。

- Cisco HyperFlex
- カーネルベース仮想マシン（KVM）
- Microsoft Hyper-V
- VMware vSphere/VMware ESXi

Management Center は、同じデバイス管理機能（FMCv2 ではサポートされていません）と同じライセンスを持っている必要があります。また、管理対象デバイスあたり 1 つの Threat Defense 権限が必要です。詳細については、「Management Center ハイアベイラビリティ構成のライセンス要件 （373 ページ）」を参照してください。

（注） バージョン 7.0.x のクラシックデバイス（NGIPSv または ASA FirePOWER）のみを管理している場合は、FMCv 権限は必要ありません。

ソフトウェア要件

[アプライアンス情報（Appliance Information）] ウィジェットにアクセスして、ソフトウェアバージョン、侵入ルールの更新バージョン、および脆弱性データベースの更新バージョンを確認します。デフォルトでは、[詳細ダッシュボード（Detailed Dashboard）] と [サマリーダッシュボード（Summary Dashboard）] の [ステータス（Status）] タブにウィジェットが表示されます。詳細については、[アプライアンス情報（Appliance Information）] ウィジェット （407 ページ）を参照してください。

- ハイ アベイラビリティ設定の 2 台の Management Center には、同じメジャー（最初の番号）、マイナー（2 番めの番号）、メンテナンス（3 番めの番号）バージョンのソフトウェアがインストールされている必要があります。
- ハイ アベイラビリティ構成内の 2 つの Management Center には、同じバージョンの侵入ルールの更新をインストールする必要があります。

- ハイ アベイラビリティ構成内の 2 つの Management Center には、同じバージョンの脆弱性データベースの更新をインストールする必要があります。
- ハイアベイラビリティ構成内の 2 つの Management Center には、同じバージョンの LSP（Lightweight Security Package）をインストールする必要があります。

警告 両方の Management Center でソフトウェア バージョン、侵入ルールの更新バージョン、および脆弱性データベースの更新バージョンが同一でない場合は、ハイ アベイラビリティを確立できません。

Management Center ハイアベイラビリティ構成のライセンス要件

各デバイスには、単一の Management Center によって管理されているか、ハイアベイラビリティペア（ハードウェアまたは仮想）の Management Center によって管理されているかにかかわらず、同じライセンスが必要です。

例：Management Center ペアで管理されている 2 つのデバイスに対して高度なマルウェア防御を有効にする場合は、2 つの マルウェア防御 ライセンスと 2 つの TM サブスクリプションを購入し、アクティブ Management Center を Smart Software Manager に登録してから、ライセンスをアクティブ Management Center 上の 2 つのデバイスに割り当てます。

アクティブな Management Center のみが Smart Software Manager に登録されます。フェールオーバーが実行されると、システムは Smart Software Manager と通信して、ライセンスの付与資格を最初にアクティブだった Management Center から解放し、新たにアクティブになる Management Center に割り当てます。

特定ライセンス予約の展開では、プライマリ Management Center のみが特定ライセンス予約を必要とします。

ハードウェア（Hardware） Management Center

ハイアベイラビリティペア内のハードウェア Management Center に特別なライセンスは必要ありません。

Management Center Virtual

同じライセンスの Management Center Virtual が 2 つ必要です。

例：10 台のデバイスを管理する Management Center Virtual ハイアベイラビリティペアの場合は、以下を使用できます。

- 2 個の Management Center Virtual 10 エンタイトルメント
- 10 個のデバイスライセンス

ハイアベイラビリティペアを解除すると、セカンダリ Management Center Virtual に関連付けられた Management Center Virtual エンタイトルメントが解放されます。（この例では、2 個のスタンドアロン Management Center Virtual 10 があります。）

Management Center 高可用性の前提条件

Management Center 高可用性ペアを確立する前に、次の操作を行います。

- 必要なポリシーを、対象のセカンダリ Management Center から対象のプライマリ Management Center にエクスポートします。詳細については、設定のエクスポート （624 ページ）を参照してください。
- 対象のセカンダリ Management Center にデバイスが追加されていないことを確認します。対象のセカンダリ Management Center からデバイスを削除し、そのデバイスを対象のプライマリ Management Center に登録します。詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの「Delete a Device from Management Center」および「Add a Device to Management Center」を参照してください。
- 対象のプライマリ Management Center にポリシーをインポートします。詳細については、設定のインポート （625 ページ）を参照してください。
- 対象のプライマリ Management Center で、インポートされたポリシーを確認して、必要に応じて編集し、適切なデバイスに展開します。詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの「*Deploy Configuration Changes*」を参照してください。
- 対象のプライマリ Management Center で、適切なライセンスを新しく追加したデバイスに関連付けます。詳細については、単一のデバイスへのライセンスの割り当て （335ページ）を参照してください。

これで、ハイ アベイラビリティの確立に進むことができます。詳細については、Management Centerのハイアベイラビリティの確立 （374 ページ）を参照してください。

Management Centerのハイアベイラビリティの確立

高可用性を確立するには、ピア間の帯域幅とポリシーの数に応じてかなりの時間がかかり、数時間かかることもあります。また、スタンバイ状態の Management Center と同期される必要のある、アクティブ Management Center に登録されたデバイスの数によっても異なります。[ハイアベイラビリティ（High Availability）]ページを表示すると、ハイ アベイラビリティ ピアのステータスを確認できます。

始める前に

- 両方の Management Center がハイ アベイラビリティ システム要件を満足していることを確認します。詳細については、Management Center 高可用性の要件 （371 ページ）を参照してください。

- ハイアベイラビリティを確立するための前提条件を満足していることを確認します。詳細については、Management Center 高可用性の前提条件 （374 ページ）を参照してください。

手順

ステップ 1 セカンダリとして指定する Management Center にログインします。

ステップ 2 **[統合（Integration）] > [その他の統合（Other Integrations）]**を選択します。

ステップ 3 [高可用性（High Availability）] を選択します。

ステップ 4 この Management Center の権限で、[セカンダリ（Secondary）] を選択します。

ステップ 5 **[プライマリファイアウォール Management Center ホスト（Primary Firewall Management Center Host）]** テキストボックスに、プライマリ Management Center のホスト名または IP アドレスを入力します。

ピア Management Center から到達可能な IP アドレス（パブリックまたはプライベート IP アドレス）がプライマリ Management Center にない場合は、これを空のままにできます。この場合は、[登録キー（Registration Key）] と [一意の NAT ID（Unique NAT ID）] の両方のフィールドを使用します。HA 接続を有効にするには、少なくとも 1 つの Management Center の IP アドレスを指定する必要があります。

ステップ 6 [登録キー（Registration Key）]テキストボックスに、1 回限り使用する登録キーを入力します。

登録キーは、ユーザ定義の最大 37 文字の英数字値です。この登録キーはセカンダリおよびプライマリ Management Center の登録に使用されます。

ステップ 7 プライマリ IP アドレスを指定しなかった場合、またはプライマリ Management Center でセカンダリ IP アドレスを指定しない場合は、[一意の NAT ID（Unique NAT ID）] フィールドに一意の英数字 ID を入力します。詳細については、NAT 環境 （88 ページ）を参照してください。

ステップ 8 [登録（Register）] をクリックします。

ステップ 9 管理者アクセス権限を持つアカウントを使用して、プライマリとして指定する Management Center にログインします。

ステップ 10 **[統合（Integration）] > [その他の統合（Other Integrations）]**を選択します。

ステップ 11 [高可用性（High Availability）] を選択します。

ステップ 12 この Management Center の権限で、[プライマリ（Primary）] を選択します。

ステップ 13 **[セカンダリファイアウォール Management Center ホスト（Secondary Firewall Management Center Host）]** テキストボックスに、セカンダリ Management Center のホスト名または IP アドレスを入力します。

ピア Management Center から到達可能な IP アドレス（パブリックまたはプライベート IP アドレス）がセカンダリ Management Center にない場合は、これを空のままにできます。この場合は、[登録キー（Registration Key）] と [一意の NAT ID（Unique NAT ID）] の両方のフィールドを使用します。HA 接続を有効にするには、少なくとも 1 つの Management Center の IP アドレスを指定する必要があります。

ステップ 14 [登録キー（Registration Key）] テキストボックスに、ステップ 6 で入力した 1 回限り使用する登録キーと同じものを入力します。

ステップ 15 必要に応じて、[一意の NAT ID（Unique NAT ID）] テキスト ボックスに手順 7 で使用したのと同じ NAT ID を入力します。

ステップ 16 [登録（Register）] をクリックします。

次のタスク

Management Center 高可用性ペアを確立すると、アクティブ Management Center に登録されたデバイスが自動的にスタンバイ Management Center に登録されます。

（注） 登録済みのデバイスに NAT IP アドレスが割り当てられている場合、デバイスの自動登録は失敗し、セカンダリ Management Center の [高可用性（High Availability）] ページには、そのデバイスがローカルで保留中であると表示されます。次に、スタンバイ Management Center の [ハイアベイラビリティ（High Availability）] ページで、異なる NAT IP アドレスをデバイスに割り当てることができます。自動登録がスタンバイ Management Center で失敗しても、デバイスがアクティブな Firepower Management Center に登録されているように見える場合は、Management Center 高可用性で CLI を使用してデバイス登録を解決する （378 ページ） を参照してください。

Management Center 高可用性ステータスの表示

アクティブおよびスタンバイ Management Center を識別した後、ローカル Management Center とそのピアに関する情報を表示できます。

（注） このコンテキストでは、ローカル ピアは、システム ステータスを表示するアプライアンスを参照します。リモート ピアは、アクティブ ステータスかスタンバイ ステータスかに関係なく、その他のアプライアンスを参照します。

手順

ステップ 1 ハイ アベイラビリティを使用してペアリングした Management Center のいずれか一方にログインします。

ステップ 2 **[統合（Integration）] > [その他の統合（Other Integrations）]**を選択します。

ステップ 3 [高可用性（High Availability）] を選択します。

次の情報を表示できます。

サマリー情報

- 高可用性ペアのヘルスステータススタンバイユニットがアクティブユニットから設定変更を受信すると、正常に機能しているシステムのステータスは [正常（Healthy）] と [同期タスクが進行中です（Synchronization task is in progress）] の間で変動します。
- ハイ アベイラビリティ ペアの現在の同期ステータス
- アクティブ ピアの IP アドレスと最後に同期された時間
- スタンバイ ピアの IP アドレスと最後に同期された時間

システム ステータス

- 両方のピアの IP アドレス
- 両方のピアのオペレーティング システム
- 両方のピアのソフトウェア バージョン
- 両方のピアのアプライアンス モデル

（注） エクスポート制御およびコンプライアンスステータスは、アクティブ Management Center でのみ表示できます。

Management Center 高可用性ペアで同期される設定

2 つの Management Center の間でハイ アベイラビリティを確立すると、次の設定データが同期されます。

- ライセンスの付与資格
- アクセス コントロール ポリシー
- 侵入ルール
- マルウェアおよびファイル ポリシー
- DNS ポリシー
- アイデンティティ ポリシー
- SSL ポリシー
- プレフィルタ ポリシー
- ネットワーク検出ルール
- アプリケーション ディテクタ
- 相関ポリシー ルール

- アラート（Alerts）
- スキャナ（Scanners）
- 応答グループ
- イベントを調査するための外部リソースのコンテキスト クロス起動
- 修復設定。ただし、両方の Management Center にカスタム モジュールをインストールする必要があります。修復設定の詳細については、修復モジュールの管理（1261 ページ）を参照してください。

高可用性ペアでの Management Center データベースへの外部アクセスの設定

高可用性設定では、アクティブなピアのみを使用して、データベースへの外部アクセスを設定することを推奨します。外部データベースアクセス用にスタンバイピアを設定すると、頻繁に切断されるようになります。接続を復元するには、スタンバイピアの同期をペアにされた Management Center 間での通信の一時停止してからペアにされた Management Center 間での通信の再開する必要があります。Management Center への外部データベースアクセスを有効にする方法については、データベースへの外部アクセスの有効化（71 ページ）を参照してください。

Management Center 高可用性で CLI を使用してデバイス登録を解決する

自動デバイス登録がスタンバイ Management Center で失敗したものの、アクティブ Management Center に登録されたと表示される場合、次の手順を実行します。

警告 セカンダリ Management Center の RMA を実行するか、セカンダリ Management Center を追加すると、管理対象デバイスが登録解除されます。その結果、管理対象デバイスの設定が削除されることがあります。

手順

ステップ 1 アクティブな Management Center からデバイスを削除します。Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド [英語] の「*Delete (Unregister) a Device from the Management Center*」を参照してください。

ステップ 2 スタンバイ Management Center でデバイスの自動登録をトリガーするには、次の手順を実行します。

1. 影響受けるデバイスの CLI にログインします。
2. CLI コマンドの **configure manager delete** を実行します。

   このコマンドは、現在の Management Center を無効にして削除します。
3. CLI コマンドの **configure manager add** を実行します。

   このコマンドは、デバイスを設定して Management Center への接続を開始します。

   ヒント デバイスのリモート管理を、アクティブな Management Center の場合のみ設定します。高可用性を確立すると、デバイスが自動的にスタンバイ Management Center に登録されます。
4. アクティブ Management Center にログインし、デバイスを登録します。

ステップ 3 スタンバイ Management Center が NAT の背後にある場合は、次の手順を実行してスタンバイ Management Center のホスト名を編集します。

1. Threat Defense シェルにアクセスし、`show manager` コマンドを使用して、スタンバイ Management Center のエントリ識別子の値を取得します。
2. Threat Defense シェルで、スタンバイ Management Center のホスト名をパブリック IP アドレスに編集します。エントリ識別子とホスト IP アドレスを使用して `configure manager edit <standby_uuid> hostname <standby_ip>` コマンドを実行します。

Management Center のハイアベイラビリティペアにおけるピアの切り替え

システムでは一部の機能をアクティブ Management Center に制限しているため、そのアプライアンスで障害が発生した場合は、スタンバイ Management Center をアクティブ ステータスにプロモートする必要があります。

手順

ステップ 1 ハイ アベイラビリティを使用してペアリングした Management Center のいずれか一方にログインします。

ステップ 2 **[統合（Integration）]** > **[その他の統合（Other Integrations）]**を選択します。

ステップ 3 [高可用性（High Availability）] を選択します。

ステップ 4 [ピア ロールの切り替え（Switch Peer Roles）] を選択して、ローカル ロールをアクティブからスタンバイ、またはスタンバイからアクティブに変更します。プライマリまたはセカンダリの指定は変更されずに、2 つのピア間でロールが切り替わります。

ペアにされた Management Center 間での通信の一時停止

一時的に高可用性を無効にする場合は、Management Center 間の通信チャネルを無効にすることができます。アクティブピアまたはスタンバイピアから同期を再開できます。

手順

ステップ 1 ハイ アベイラビリティを使用してペアリングした Management Center のいずれか一方にログインします。

ステップ 2 **[統合（Integration）] > [その他の統合（Other Integrations）]**を選択します。

ステップ 3 [高可用性（High Availability）] を選択します。

ステップ 4 [同期の一時停止（Pause Synchronization）] を選択します。

ペアにされた Management Center 間での通信の再開

一時的に高可用性を無効にしている場合は、Management Center 間の通信チャネルを有効にすることで、高可用性を再開することができます。アクティブピアまたはスタンバイピアから同期を再開できます。

手順

ステップ 1 ハイ アベイラビリティを使用してペアリングした Management Center のいずれか一方にログインします。

ステップ 2 **[統合（Integration）] > [その他の統合（Other Integrations）]**を選択します。

ステップ 3 [高可用性（High Availability）] を選択します。

ステップ 4 [同期の再開（Resume Synchronization）] を選択します。

高可用性ペアの Management Center の IP アドレスの変更

高可用性ピアのいずれかの IP アドレスを変更すると、高可用性が低下した状態になります。高可用性を回復するには、手動で IP アドレスを変更する必要があります。

手順

ステップ 1 ハイ アベイラビリティを使用してペアリングした Management Center のいずれか一方にログインします。

ステップ 2 **[統合（Integration）]** > **[その他の統合（Other Integrations）]**を選択します。

ステップ 3 [高可用性（High Availability）] を選択します。

ステップ 4 [ピア マネージャ（Peer Manager）] を選択します。

ステップ 5 **[編集（Edit）]**（ ） を選択します。

ステップ 6 アプライアンスの表示名を入力します。この表示名は、システムのコンテキストでのみ使用されます。

別の表示名を入力しても、アプライアンスのホスト名は変更されません。

ステップ 7 完全修飾ドメイン名を入力するか、ローカル DNS で有効な IP アドレス（ホスト名）に解決される名前、またはホストの IP アドレスを入力します。

ステップ 8 [保存（Save）] をクリックします。

Management Center ハイアベイラビリティの無効化

手順

ステップ 1 ハイ アベイラビリティ ペアのいずれか一方の Management Center にログインします。

ステップ 2 **[統合（Integration）]** > **[その他の統合（Other Integrations）]**を選択します。

ステップ 3 [高可用性（High Availability）] を選択します。

ステップ 4 [ハイ アベイラビリティの解消（Break High Availability）] を選択します。

ステップ 5 管理対象デバイスを処理するための以下のいずれかのオプションを選択します。

- この Management Center を使用してすべての管理対象デバイスを制御する場合には、[このコンソールから登録済みデバイスを管理（Manage registered devices from this console）] を選択します。すべてのデバイスがピアから登録解除されます。
- 他の Management Center を使用してすべての管理対象デバイスを制御する場合には、[ピアコンソールから登録済みデバイスを管理（Manage registered devices from peer console）] を選択します。すべてのデバイスがこの Management Center から登録解除されます。
- デバイスの管理をまとめて停止する場合には、[両方のコンソールからの登録済みデバイスの管理を停止（Stop managing registered devices from both consoles）] を選択します。すべてのデバイスが両方の Management Center から登録解除されます。

（注） セカンダリ Management Center から登録済みデバイスを管理する場合、そのデバイスはプライマリ Management Center から登録解除されます。そのデバイスは、セカンダリ Management Center によって管理されるように登録されます。ただし、そのデバイスに適用されていたライセンスは、ハイ アベイラビリティの中断操作のために登録解除されます。次に、セカンダリ Management Center からデバイス上でライセンスを再登録（有効化）する必要があります。詳細については、デバイスへのライセンスの割り当て（335 ページ）を参照してください。

ステップ 6 [OK] をクリックします。

高可用性ペアでの Management Center の交換

Management Center 高可用性ペアで障害が発生したユニットを交換する必要がある場合は、次に示すいずれかの手順に従う必要があります。次の表に、4 つの障害シナリオとそれに対応する交換手順を示します。

障害ステータス	データ バックアップ ステータス	交換手順
プライマリ Management Center の障害	データバックアップが成功	障害が発生したプライマリ Management Center の交換（バックアップが成功）（382 ページ）
	データバックアップが失敗	障害が発生したプライマリ Management Center の交換（バックアップが失敗）（384 ページ）
セカンダリ Management Center の障害	データバックアップが成功	障害が発生したセカンダリ Management Center の交換（バックアップが成功）（385 ページ）
	データバックアップが失敗	障害が発生したセカンダリ Management Center の交換（バックアップが失敗）（386 ページ）

障害が発生したプライマリ Management Center の交換（バックアップが成功）

2 つの Management Center（FMC1 と FMC2）が高可用性ペアを構成しています。FMC1 がプライマリ、FMC2 がセカンダリです。このタスクでは、プライマリからのデータバックアップが成功した場合に、障害が発生したプライマリ Management Center（FMC1）を交換する手順を説明します。

始める前に

障害が発生したプライマリ Management Center からのデータ バックアップが成功したことを確認します。

手順

ステップ 1 サポートに連絡して、障害が発生した Management Center（FMC1）の交換を依頼します。

ステップ 2 プライマリ Management Center（FMC1）で障害が発生した場合は、セカンダリ Management Center（FMC2）の Web インターフェイスにアクセスしてピアを切り替えます。詳細については、Management Center のハイアベイラビリティペアにおけるピアの切り替え （379 ページ）を参照してください。

これで、セカンダリ Management Center（FMC2）がアクティブに昇格します。

プライマリ Management Center（FMC1）の交換が完了するまで、FMC2 をアクティブ Management Center として使用できます。

注意 Management Center 高可用性を FMC2 から分断しないでください。分断すると、障害発生前に FMC1 から FMC2 に同期されていたライセンスが FMC2 から削除されるため、FMC2 から展開アクションを実行できなくなります。

ステップ 3 FMC1 と同じソフトウェアバージョンを使用して交換用 Management Center を再イメージ化します。

ステップ 4 FMC1 から取得したデータバックアップを新しい Management Center に復元します。

ステップ 5 FMC2 と適合するのに必要な Management Center パッチ、地理位置情報データベース（GeoDB）の更新、脆弱性データベース（VDB）の更新、システム ソフトウェア アップデートをインストールします。

これで、新しい Management Center と FMC2 の両方がアクティブピアとなるため、高可用性がスプリットブレイン状態になります。

ステップ 6 Management Center Web インターフェイスからアクティブアプライアンスを選択するプロンプトが表示されたら、FMC2 をアクティブとして選択します。

FMC2 の最新の設定が新しい Management Center（FMC1）に同期されます。

ステップ 7 設定が正常に同期されたら、セカンダリ Management Center（FMC2）の Web インターフェイスにアクセスし、ロールを切り替えてプライマリ Management Center（FMC1）をアクティブにします。詳細については、Management Center のハイアベイラビリティペアにおけるピアの切り替え （379 ページ）を参照してください。

次のタスク

これで、ハイアベイラビリティが再確立されたため、プライマリおよびセカンダリ Management Center が正常に動作するようになります。

障害が発生したプライマリ Management Center の交換（バックアップが失敗）

2 つの Management Center（FMC1 と FMC2）が高可用性ペアを構成しています。FMC1 がプライマリ、FMC2 がセカンダリです。このタスクでは、プライマリからのデータバックアップが失敗した場合に、障害が発生したプライマリ Management Center（*FMC1*）を交換する手順を説明します。

手順

ステップ 1 サポートに連絡して、障害が発生した Management Center（FMC1）の交換を依頼します。

ステップ 2 プライマリ Management Center（FMC1）で障害が発生した場合は、セカンダリ Management Center（FMC2）の Web インターフェイスにアクセスしてピアを切り替えます。詳細については、Management Center のハイアベイラビリティペアにおけるピアの切り替え （379 ページ）を参照してください。

これで、セカンダリ Management Center（FMC2）がアクティブに昇格します。

プライマリ Management Center（FMC1）の交換が完了するまで、FMC2 をアクティブ Management Center として使用できます。

注意 Management Center ハイアベイラビリティを *FMC2* から分断しないでください。分断すると、（障害前に）*FMC1* から *FMC2* に同期されていたライセンスが *FMC2* から削除されるため、*FMC2* から展開アクションを実行できなくなります。

ステップ 3 FMC1 と同じソフトウェアバージョンを使用して交換用 Management Center を再イメージ化します。

ステップ 4 FMC2 と適合するのに必要な Management Center パッチ、地理位置情報データベース（GeoDB）の更新、脆弱性データベース（VDB）の更新、システムソフトウェアの更新をインストールします。

ステップ 5 Management Center（*FMC2*）を Cisco Smart Software Manager から登録解除します。詳細については、の登録解除Management Center （337 ページ）を参照してください。

Cisco Smart Software Manager から Management Center の登録を解除すると、バーチャルアカウントから Management Center が削除されます。Management Center リリースに関連付けられているライセンス権限はすべて、ご使用のバーチャル アカウントに戻ります。登録解除後、Management Center は適用モードになり、ライセンスが適用される機能に対する更新および変更が許可されなくなります。

ステップ 6 セカンダリ Management Center（*FMC2*）の Web インターフェイスにアクセスして、Management Center ハイアベイラビリティを分断します。詳細については、Management Center ハイアベイラビリティの無効化（381 ページ）を参照してください。管理対象デバイスを処理する方法を選択するよう求められたら、[このコンソールから登録済みデバイスを管理（Manage registered devices from this console）] を選択します。

これにより、セカンダリ Management Center（*FMC2*）に同期されていたライセンスが削除されるため、*FMC2* から展開アクティビティを実行できなくなります。

ステップ 7 Management Center 高可用性を再確立するために、Management Center（*FMC2*）をプライマリ、Management Center（*FMC1*）をセカンダリとして設定します。詳細については、Management Centerのハイアベイラビリティの確立 （374 ページ）を参照してください。

ステップ 8 スマートライセンスをプライマリ Management Center（*FMC2*）に登録します。詳細については、Smart Software Manager での Management Center の登録 （328 ページ）を参照してください。

次のタスク

これで、ハイアベイラビリティが再確立されたため、プライマリおよびセカンダリ Management Center が正常に動作するようになります。

障害が発生したセカンダリ Management Center の交換（バックアップが成功）

2 つの Management Center（FMC1 と FMC2）が高可用性ペアを構成しています。FMC1 がプライマリ、FMC2 がセカンダリです。このタスクでは、セカンダリからのデータバックアップが成功した場合に、障害が発生したセカンダリ Management Center（FMC2）を交換する手順を説明します。

始める前に

障害が発生したセカンダリ Management Center からのデータ バックアップが成功したことを確認します。

手順

ステップ 1 サポートに連絡して、障害が発生した Management Center（FMC2）の交換を依頼します。

ステップ 2 引き続きプライマリ Management Center（FMC1）をアクティブ Management Center として使用します。

ステップ 3 FMC2 と同じソフトウェア バージョンを使用して交換用 Management Center を再イメージ化します。

ステップ 4 FMC2 から取得したデータバックアップを新しい Management Center に復元します。

ステップ 5 FMC1 と適合するのに必要な Management Center パッチ、地理位置情報データベース（GeoDB）の更新、脆弱性データベース（VDB）の更新、システム ソフトウェア アップデートをインストールします。

ステップ 6 新しい Management Center（FMC2）の Web インターフェイスからデータ同期を再開して（停止されていた場合）、プライマリ Management Center（FMC1）の最新の設定を同期させます。詳細については、ペアにされた Management Center 間での通信の再開 （380 ページ）を参照してください。

従来のライセンスとスマート ライセンスはシームレスに機能します。

次のタスク

これで、ハイアベイラビリティが再確立されたため、プライマリおよびセカンダリ Management Center が正常に動作するようになります。

障害が発生したセカンダリ Management Center の交換（バックアップが失敗）

2 つの Management Center（FMC1 と FMC2）が高可用性ペアを構成しています。FMC1 がプライマリ、FMC2 がセカンダリです。このタスクでは、セカンダリからのデータバックアップが失敗した場合に、障害が発生したセカンダリ Management Center（FMC2）を交換する手順を説明します。

手順

ステップ 1 サポートに連絡して、障害が発生した Management Center（FMC2）の交換を依頼します。

ステップ 2 引き続きプライマリ Management Center（FMC1）をアクティブ Management Center として使用します。

ステップ 3 FMC2 と同じソフトウェア バージョンを使用して交換用 Management Center を再イメージ化します。

ステップ 4 FMC1 と適合するのに必要な Management Center パッチ、地理位置情報データベース（GeoDB）の更新、脆弱性データベース（VDB）の更新、システム ソフトウェア アップデートをインストールします。

ステップ 5 プライマリ Management Center（FMC1）の Web インターフェイスにアクセスして、Management Center 高可用性を分断します。詳細については、Management Center ハイアベイラビリティの無効化（381 ページ）を参照してください。管理対象デバイスを処理する方法を選択するよう求められたら、[このコンソールから登録済みデバイスを管理（Manage registered devices from this console）] を選択します。

ステップ 6 Management Center 高可用性を再確立するために、Management Center（FMC1）をプライマリ、Management Center（FMC2）をセカンダリとして設定します。詳細については、Management Centerのハイアベイラビリティの確立 （374 ページ）を参照してください。

- 高可用性が正常に確立されると、プライマリ Management Center（FMC1）の最新の設定がセカンダリ Management Center（FMC2）に同期されます。
- 従来のライセンスとスマート ライセンスはシームレスに機能します。

次のタスク

これで、ハイアベイラビリティが再確立されたため、プライマリおよびセカンダリ Management Center が正常に動作するようになります。

Management Center 高可用性ディザスタリカバリ

ディザスタリカバリの状況では、手動スイッチオーバーを実行する必要があります。プライマリ Management Center（FMC1）で障害が発生した場合は、セカンダリ Management Center（FMC2）の Web インターフェイスにアクセスしてピアを切り替えます。これは、逆に、セカンダリ（FMC2）に障害が発生した場合にも当てはまります。詳細については、Management Center のハイアベイラビリティペアにおけるピアの切り替え （379 ページ）を参照してください。

障害が発生した Management Center の復旧については、高可用性ペアでの Management Center の交換 （382 ページ）を参照してください。

（ハードウェアの障害がない）高可用性ペアでの Management Center の復元

ハードウェア障害がないときに Management Center 高可用性ペアを復元するには、次の手順に従います。

- プライマリ管理センターでのバックアップの復元 （387 ページ）
- セカンダリ管理センターでのバックアップの復元 （388 ページ）

プライマリ管理センターでのバックアップの復元

始める前に

- 管理センターのハードウェアの故障や交換がない。
- バックアップと復元のプロセスに精通している。を参照してくださいバックアップ/復元（555 ページ）。

手順

ステップ 1 /var/sf/backup/ のローカルストレージ、またはリモートネットワークボリュームのいずれかで、プライマリ Management Center のバックアップが使用可能かどうかを確認します。

ステップ 2 プライマリ Management Center で、同期を一時停止します。**[統合（Integration）] > [その他の統合（Other Integrations）]** を選択し、[高可用性（High Availability）] タブに移動して同期を一時停止します。

ステップ 3 プライマリ Management Center でバックアップを復元します。復元が完了すると、Management Center が再起動します。

ステップ 4 プライマリ Management Center がアクティブになり、そのユーザーインターフェイスに到達できるようになったら、セカンダリ Management Center で同期を再開します。**[統合（Integration）]** > **[その他の統合（Other Integrations）]** を選択し、[高可用性（High Availability）] タブに移動して同期を再開します。

セカンダリ管理センターでのバックアップの復元

始める前に

- 管理センターのハードウェアの故障や交換がない。
- バックアップと復元のプロセスに精通している。を参照してくださいバックアップ/復元（555 ページ）。

手順

ステップ 1 /var/sf/backup/ のローカルストレージ、またはリモート ネットワーク ボリュームのいずれかで、セカンダリ Management Center のバックアップが使用可能かどうかを確認します。

ステップ 2 プライマリ Management Center で、同期を一時停止します。**[統合（Integration）]** > **[その他の統合（Other Integrations）]** を選択し、[高可用性（High Availability）] タブに移動して同期を一時停止します。

ステップ 3 セカンダリ Management Center でバックアップを復元します。復元が完了すると、Management Center が再起動します。

ステップ 4 セカンダリ Management Center がアクティブになり、そのユーザーインターフェイスに到達できるようになったら、プライマリ Management Center で同期を再開します。**[統合（Integration）]** > **[その他の統合（Other Integrations）]** を選択し、[高可用性（High Availability）] タブに移動して同期を再開します。

高可用性の Management Center の統合バックアップ

アクティブ Management Center で統合バックアップを実行できます。この場合、アクティブとスタンバイの両方の Management Center に対して単一のバックアップファイルが作成されます。統合バックアップは、設定のみのバックアップにのみ適用されます。イベントまたは TID バックアップが必要な場合は、アクティブおよびスタンバイ Management Center に対して個別のバックアップを取る必要があります。設定のみのバックアップを選択すると、デフォルトで統合バックアップが適用されます。統合バックアップでは、アクティブ Management Center がスタンバイ Management Center からバックアップ tar ファイルを取得できない場合、復元に使用でき

るアクティブユニットの通常のバックアップファイルが生成されます。統合バックアップには、通常のバックアップと比較していくつかの利点があります。

- 統合バックアップでは、アクティブとスタンバイ Management Center で個別のバックアップを取る必要はありません。
- 統合バックアップでは、バックアップ内の冗長データとストレージの制約が削除されます。
- 通常のバックアップでは、プライマリユニットに障害が発生した場合、セカンダリユニットのバックアップを使用できないと、セカンダリ RMA の高可用性ペアリングを解除する必要がありました。この状況は、統合バックアップでは解消されます。
- 通常、スタンバイユニットのバックアップはスケジュールできません。スケジュールされた統合バックアップでは、アクティブユニットとスタンバイユニットの両方のバックアップが取られます。
- 統合バックアップの実行中は、スタンバイユニットでバックアップを実行するために HA 同期を一時停止する必要はありません。

予期しないインシデントが発生した場合、統合バックアップを使用して新しい RMA デバイスを回復できます。統合バックアップのファイルは名前で識別できます。統合バックアップのファイル名には「Unified」というプレフィックスが追加されます。Management Center を選択して復元するとともに、その状態（アクティブ/スタンバイ）を選択することもできます。

スプリットブレインの競合を防ぐために、復元された Management Center の適切な状態を選択していることを確認してください。

統合バックアップからの Management Center の復元

のバックアップ Management Center（設定のみ）から Management Center を復元するには、次の手順を使用します。

手順

ステップ 1 復元する Management Center にログインします。

ステップ 2 **システム**（⚙）**>[ツール（Tools）]>[バックアップ/復元（Backup/Restore）]** を選択します。

[バックアップ管理（Backup Management）] ページには、統合バックアップファイル（設定のみ）を含め、ローカルとリモートで保存されたすべてのバックアップファイルが一覧表示されます。

統合バックアップファイルが一覧になく、ローカルコンピュータに保存している場合は、[バックアップのアップロード（Upload Backup）] をクリックします。バックアップとリモートストレージの管理 （590 ページ）を参照してください。

ステップ 3 復元する統合バックアップファイルを選択して、[復元（Restore）] をクリックします。

ステップ 4 [バックアップの復元（Restore Backup）]ページで、復元するユニットを選択します。統合バックアップにはプライマリとセカンダリの両方の Management Center のバックアップ設定が保存されるため、復元するユニットを選択する必要があります。

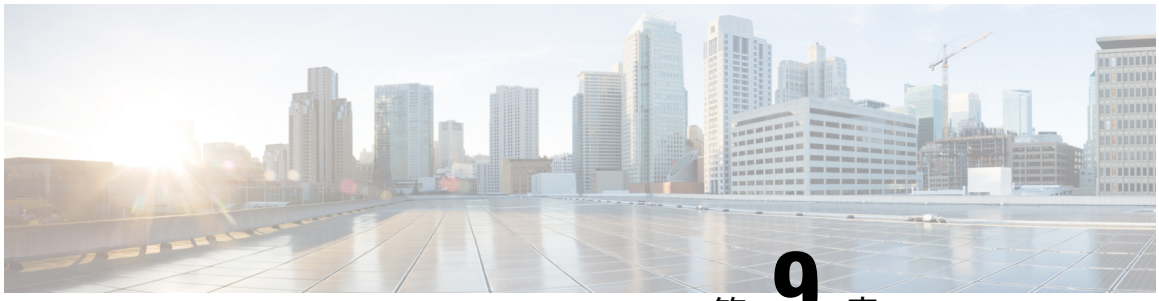
ステップ 5 復元される Management Center の状態を選択するには、[アクティブ（Active）] または [スタンバイ（Standby）] オプションボタンをクリックします。作業中の Management Center のロールと状態を確認して、両方のピアのロールと状態が同じ設定にならないようにする必要があります。復元時に Management Center に誤ったロールと状態を選択すると、HA 障害が発生する可能性があります。

ステップ 6 [復元（Restore）] をクリックし、[復元の確認（Confirm Restore）] をクリックして復元を開始します。

Management Center 高可用性の履歴

機能	最小 Management Center	最小 Threat Defense	詳細
高可用性 Management Center 用の単一のバックアップファイル。	7.4.1 7.2.6	いずれか	高可用性ペアのアクティブ Management Center の設定だけのバックアップを実行すると、いずれかのユニットの復元に使用できる単一のバックアップファイルが作成されるようになりました。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。
Management Center の高可用性同期の機能拡張。	7.4.1	任意（Any）	Management Center の高可用性（HA）には、次の同期機能拡張が含まれています。 • 設定履歴ファイルが大きいと、遅延の大きいネットワークで同期が失敗する可能性があります。これを防ぐために、デバイス設定履歴ファイルは他の設定データと並行して同期されるようになりました。この機能拡張により、同期時間も短縮されます。 • Management Center は、設定履歴ファイルの同期プロセスをモニターし、同期がタイムアウトした場合に正常性アラートを表示するようになりました。 新規/変更された画面：次の画面でこれらのアラートを確認できます。 • [通知（Notifications）] > [メッセージセンター（Message Center）] > [正常性（Health）] • [統合（Integration）] > [その他の統合（Other Integrations）] > [高可用性（High Availability）] > [ステータス （Status）]（[概要（Summary）] の下）

機能	最小 Management Center	最小 Threat Defense	詳細
Hyper-V での高可用性のサポート。	7.4.0	いずれか	Management Center Virtual で Hyper-V の高可用性がサポートされるようになりました。
KVM での高可用性のサポート。	7.3.0	いずれか	Management Center Virtual で KVM の高可用性がサポートされるようになりました。
AWS および OCI での高可用性のサポート。	7.1.0	いずれか	Management Center Virtual で AWS および OCI の高可用性がサポートされるようになりました。
HyperFlex での高可用性のサポート。	7.0.0	いずれか	Management Center Virtual で HyperFlex の高可用性がサポートされるようになりました。
VMware での高可用性のサポート。	6.7.0	いずれか	Management Center Virtual で VMware の高可用性がサポートされるようになりました。
シングルサインオン。	6.7.0	いずれか	シングルサインオン用に高可用性ペアの一方または両方のメンバーを設定するときは、特別な考慮事項を考慮する必要があります。



第 9 章

セキュリティ認定準拠

次のトピックでは、セキュリティ認定規格に準拠するようにシステムを設定する方法について説明します。

セキュリティ認定準拠のモード

お客様の組織が、米国防総省およびグローバル認定組織によって確立されたセキュリティ基準に従う機器とソフトウェアだけを使用することを求められる場合があります。Firepower では、以下のセキュリティ認定標準規格へのコンプライアンスをサポートします。

- コモンクライテリア（CC）：国際コモンクライテリア承認アレンジメントによって確立された、セキュリティ製品のプロパティを定義するグローバル標準規格
- Unified Capabilities Approved Products List（UCAPL）：米国国防情報システム局（DISA）によって確立された、セキュリティ要件を満たす製品のリスト

（注） 米国政府は、Unified Capabilities Approved Products List（UCAPL）の名称を Defense Information Network Approved Products List（DODIN APL）に変更しました。このドキュメントおよび Secure Firewall Management Center Web インターフェイスでの UCAPL の参照は、DODIN APL への参照として解釈できます。

- 連邦情報処理標準（FIPS）140：暗号化モジュールの要件に関する規定

セキュリティ認定コンプライアンスは、CC モードまたは UCAPL モードで有効にすることができます。セキュリティ認定コンプライアンスを有効にしても、選択したセキュリティモードのすべての要件との厳密なコンプライアンスが保証されるわけではありません。強化手順につ

いての詳細は、認定機関から提供されている本製品に関するガイドラインを参照してください。

⚠

注意 この設定を有効にした後は、無効にすることはできません。アプライアンスを CC モードまたは UCAPL モードから解除する必要がある場合は、再イメージ化する必要があります。

セキュリティ認定準拠特性

次の表は、CC または UCAPL モードを有効にしたときの動作の変更を示しています。（ログインアカウントの制約は、Webインターフェイスアクセスではなくコマンドラインアクセスを指します）

システムの変更	Secure Firewall Management Center		従来型管理対象デバイス		Secure Firewall Threat Defense	
	CC モード	UCAPL モード	CC モード	UCAPL モード	CC モード	UCAPL モード
FIPS コンプライアンスは有効です。	対応	対応	対応	対応	対応	対応
バックアップまたはレポートについては、リモート ストレージは利用できません。	対応	対応	—	—	—	—
追加のシステム監査デーモンが開始されます。	×	対応	×	対応	×	×
システム ブートローダは固定されています。	×	対応	×	対応	×	×
追加のセキュリティがログイン アカウントに適用されます。	×	対応	×	対応	×	×
再起動のキー シーケンス Ctrl+Alt+Del を無効にします。	×	対応	×	対応	×	×
最大 10 の同時ログインセッションを実行します。	×	対応	×	対応	×	×
パスワード長は少なくとも 15 文字で、大文字/小文字の英数字を組み合わせて 1 つ以上の数字を含む必要があります。	×	対応	×	対応	×	×
ローカル `admin` ユーザに必要な最小パスワード長を設定するには、ローカル デバイス CLI を使用できます。	×	×	×	×	対応	対応

システムの変更	Secure Firewall Management Center		従来型管理対象デバイス		Secure Firewall Threat Defense	
	CC モード	UCAPL モード	CC モード	UCAPL モード	CC モード	UCAPL モード
パスワードは、辞書に出現する単語であったり、連続する繰り返し文字を含んでいたりすることができません。	×	対応	×	対応	×	×
3 回連続してログインに失敗した場合、admin 以外のユーザはロックアウトされます。この場合は、管理者がパスワードをリセットする必要があります。	×	対応	×	対応	×	×
デフォルトでは、システムはパスワード履歴を保存します。	×	対応	×	対応	×	×
admin ユーザは、Web インターフェイスで設定可能な最大許容回数を超えてログイン試行に失敗した後、ロックアウトされます。	対応	対応	対応	対応	—	—
admin ユーザは、ローカル アプライアンス CLI で設定可能な最大許容回数を超えてログイン試行に失敗した後、ロックアウトされます。	×	×	対応（セキュリティ認定準拠の有効/無効にかかわらず）。	はい（セキュリティ認定準拠の有効/無効にかかわらず）。	対応	対応
次の場合、システムは、アプライアンスとの SSH セッションで自動的にキーを再生成します： • セッション アクティビティでキーが 1 時間使用された後 • キーを使用して接続で 1 GB のデータが伝送された後	対応	対応	対応	対応	対応	対応
システムは、ブート時にファイル システム整合性チェック（FSIC）を実行します。FSIC が失敗した場合、Firepower ソフトウェアは起動せず、リモート SSH アクセスが無効になり、ローカル コンソールを介してのみアプライアンスにアクセスできます。これが発生した場合は Cisco TAC に連絡してください。	対応	対応	対応	対応	対応	対応

セキュリティ認定準拠の推奨事項

セキュリティ認定コンプライアンスの使用が有効のときに、次のベストプラクティスを確認することをお勧めします。

- 展開時にセキュリティ認定準拠を有効にするには、最初にSecure Firewall Management Centerで有効にし、次に、管理対象のすべてのデバイスの同じモードで有効にします。

⚠

注意 両方が同じセキュリティ認定準拠モードで動作していない限り、Secure Firewall Management Center は管理対象デバイスからイベント データを受信しません。

- すべてのユーザーに対して、パスワードの強度確認を有効にし、パスワードの最小長を認証機関で求められる値に設定します。
- 高可用性設定でSecure Firewall Management Centerを使用すると、双方の設定を行い、同じセキュリティ認定準拠モードを使用します。
- Firepower 4100/9300で、CC または UCAPL モードで動作するように Secure Firewall Threat Defense を設定した場合は、Firepower 4100/9300も CC モードで動作するように設定する必要があります。詳細については、『*Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide*』を参照してください。
- 次の機能を使用するようにシステムを設定できません。
  - 電子メールレポート、アラート、データのプルーニング通知。
  - Nmap Scan、Cisco IOS Null Route、Set Attribute Value、ISE EPS の修復。
  - バックアップまたはレポート用のリモート ストレージ。
  - サードパーティ クライアントのシステム データベースへのアクセス。
  - 電子メール（SMTP）、SNMP トラップ、syslogから送信される外部通知、アラート。
  - アプライアンスとサーバの間のチャネルを保護するために、SSL 証明書を使用せずに、HTTP サーバまたは syslog サーバに送信された監査ログ メッセージ。
- CC モードを使用して展開する場合は、LDAP または RADIUS を使用して外部認証を有効にしないでください。
- CC モードを使用して展開中に CAC を有効にできません。
- CC または UCAPL モードを使用した展開では、Firepower REST API 経由で Secure Firewall Management Center および管理対象デバイスへのアクセスを無効にします。
- UCAPL モードを使用して展開中に CAC を有効にします。
- CC モードを使用して展開中に SSO を設定できません。

- Secure Firewall Threat Defense デバイスが両方とも同じセキュリティ認定準拠モードを使用していない限り、ハイ アベイラビリティ ペアに構成しないでください。

（注） システムは、以下に関する CC および UCAPL モードをサポートしていません。

- クラスタ内の Secure Firewall Threat Defense デバイス
- Secure Firewall Threat Defense のコンテナ インスタンス Firepower 4100/9300
- eStreamer を使用したイベント データの外部クライアントへのエクスポート。

アプライアンスの強化

システムの強化に使用可能な機能の詳細については、最新バージョンの『*Cisco Firepower Mangement Center Hardening Guide*』と『*Cisco Secure Firewall Threat Defense Hardening Guide*』、および本書の以降のトピックを参照してください。

- ライセンス （301 ページ）
- Management Centerユーザー （139 ページ）
- Management Center へのログイン （33 ページ）
- 監査ログ （51 ページ）
- 監査ログ証明書 （55 ページ）
- 時刻の同期 （120 ページ）
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Configure NTP Time Synchronization for Threat Defense*」
- 電子メール アラート応答の作成 （680 ページ）
- 侵入イベントに対する電子メール アラートの設定 （690 ページ）
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Configure SMTP*」
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*About SNMP for the Firepower 1000/2100*」
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Configure SNMP*」
- SNMP アラート応答の作成 （675 ページ）
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Configure Dynamic DNS*」
- DNS キャッシュ （64 ページ）
- 監査と Syslog （497 ページ）

- アクセス リスト （48 ページ）
- セキュリティ認定準拠 （393 ページ）
- リモート ストレージの SSH の設定 （114 ページ）
- 監査ログ証明書 （55 ページ）
- HTTPS 証明書 （72 ページ）
- Web インターフェイス用のユーザー ロールのカスタマイズ （231 ページ）
- 内部ユーザーの追加または編集 （147 ページ）
- セッション タイムアウト （117 ページ）
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*About Configuring Syslog*」
- Management Center のバックアップのスケジュール （600 ページ）
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Site-to-Site VPNs for Threat Defense* 」
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Remote Access VPN*」
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*FlexConfig Policies*」

ネットワークの保護

ネットワークを保護するために設定できる機能については、次のトピックを参照してください。

- アクセス コントロール ポリシー
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Security Intelligence*」
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Getting Started with Intrusion Policies*」
- Cisco Secure Firewall Management Center デバイス構成ガイドの「Tuning Intrusion Policies Using Rules」
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Custom Intrusion Rules*」
- 侵入ルールの更新 （271 ページ）
- Cisco Secure Firewall Management Center デバイス構成ガイドの「Global Limit for Intrusion Event Logging」
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Transport and Network Layer Preprocessors*」
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Specific Threat Detection*」

- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Application Layer Preprocessors*」
- 監査と Syslog （497 ページ）
- 侵入イベント （945 ページ）
- イベント検索 （845 ページ）
- ワークフロー （797 ページ）
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Device Management*」
- ログイン バナー （83 ページ）
- 更新 （263 ページ）

セキュリティ認定コンプライアンスの有効化

この設定は、Secure Firewall Management Center または管理対象デバイスに適用されます。

- Secure Firewall Management Center では、この設定はシステム設定の一部になります。
- 管理対象デバイスでは、この設定をプラットフォーム設定ポリシーの一部として Management Center から適用します。

いずれの場合も、システム設定変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで、設定は有効にはなりません。

注意 この設定を有効にした後に無効にすることはできません。アプライアンスを CC モードまたは UCAPL モードから解除する必要がある場合は、再イメージ化する必要があります。

始める前に

- アプライアンスでセキュリティ認定コンプライアンスを有効にする前に、展開に組み込む予定のあるすべてのデバイスを Management Center に登録することをお勧めします。
- Secure Firewall Threat Defense デバイスは評価ライセンスを使用できません。輸出管理機能を有効にするには、Smart Software Manager アカウントを有効にする必要があります。
- Secure Firewall Threat Defense デバイスはルーテッド モードで展開する必要があります。
- このタスクを実行するには、管理者ユーザーである必要があります。

手順

ステップ 1 Management Center を設定するか管理対象デバイスを設定するかに応じて、次の操作を実行します。

- Management Center：**システム**（⚙）>**[構成（Configuration）]** を選択します。
- Threat Defense デバイス：**[デバイス（Devices）]**>**[プラットフォーム設定（Platform Settings）]** を選択し、Secure Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 [UCAPL/CC コンプライアンス（UCAPL/CC Compliance）] をクリックします。

（注） UCAPL または CC コンプライアンスを有効にすると、アプライアンスがリブートします。Management Center は、システム設定を保存するとリブートし、管理対象デバイスは、設定の変更を展開するとリブートします。

ステップ 3 アプライアンスのセキュリティ認定コンプライアンスを永続的に有効にするには、2 つの選択肢があります。

- [コモン クライテリア（Common Criteria）] モードでセキュリティ認定コンプライアンスを有効にするには、ドロップダウン リストから [CC] を選択します。
- [Unified 機能承認製品リスト（Unified Capabilities Approved Products List）] モードでセキュリティ認定コンプライアンスを有効にするには、ドロップダウン リストから [UCAPL] を選択します。

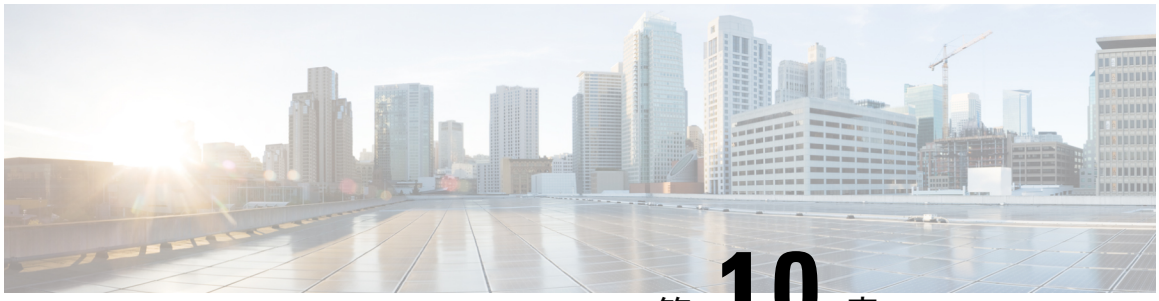
ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 認証エンティティによって提供されるこの製品のガイドラインの説明に従い、追加の設定変更を行います。
- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

第 III 部

正常性とモニタリング



第 10 章

ダッシュボード

次のトピックでは、ダッシュボードを使用する方法について説明します。

ダッシュボードについて

ダッシュボードは、システムによって収集および生成されたイベントに関するデータを含む、現在のシステムのステータスを概要的なビューとして提供します。またダッシュボードを使用して、展開のアプライアンスのステータスと全体の正常性に関する情報を表示することもできます。ダッシュボードが提供する情報はシステムのライセンス方法、設定方法、展開方法によって異なる点に注意してください。

（注） ダッシュボードに関連付けられたデバイスメトリックを表示するには、REST API（**[システム（System）] > [設定（Configuration）] > [REST API 設定（REST API Preferences）]**）が有効になっていることを確認します。

ヒント ダッシュボードは網羅的なデータを提供する複雑で高度にカスタマイズ可能なモニタリング機能です。モニター対象のネットワークについての広範、簡潔でカラフルな画像を得るには、Context Explorer を使ってください。

ダッシュボードはウィジェットの表示にタブを使用します。ウィジェットは小さな自己完結型のコンポーネントで、システムのさまざまな側面を理解するうえで役に立ちます。たとえば、定義済みの [アプライアンス情報（Appliance Information）] ウィジェットは、アプライアンスの名前、モデル、および現在実行中のソフトウェアバージョンを通知します。システムはダッシュボードの時間範囲によってウィジェットを制約します。この時間範囲は、最短で 1 時間前から、最長では 1 年前からの期間を反映するように変更できます。

システムには、いくつかの事前定義されたダッシュボードウィジェットが付属していて、使用および変更できます。ユーザロールにダッシュボードへのアクセス権が付与されている（管理者、メンテナンス ユーザ、セキュリティ アナリスト（読み取り専用）、およびダッシュボードの権限付きのカスタム ロール）場合、デフォルトでホームページは事前定義されたサマリダッシュボードになっています。ただし、ダッシュボード以外を含む別のデフォルト ホームページを設定できます。デフォルトのダッシュボードを変更することもできます。ダッシュボードへのアクセス権がないユーザロールの場合、デフォルトのホームページはロールに関連するページです。たとえば、Discovery Admin ロールの場合はネットワーク検出ページが表示されます。

また、事前定義済みのダッシュボードをカスタムダッシュボードのベースとして使用することもできます。これは共有することもプライベートとして制限することもできます。管理者アクセス権がない場合、他のユーザが作成したプライベートダッシュボードは表示も変更もできません。

（注） イベントのドリルダウン ページとテーブル ビューには、[ダッシュボード（Dashboard）] ツールバーのリンクが含まれているものがあります。このリンクをクリックして、関連する事前定義されたダッシュボードを表示することができます。事前定義されたダッシュボードまたはタブを削除すると、関連付けられているツールバーのリンクが機能しなくなります。

マルチドメイン展開では、先祖ドメインのダッシュボードを表示することはできません。ただし、高位レベルのダッシュボードをコピーした新規のダッシュボードを作成することはできます。

ダッシュボード ウィジェット

ダッシュボードには 1 つ以上のタブがあり、それぞれのタブには、3 列のレイアウトで 1 つ以上のウィジェットを表示できます。システムには、事前定義された多数のダッシュボードウィジェットが付属しています。それぞれのウィジェットは、システムのさまざまな側面を理解するうえで役に立ちます。ウィジェットは、次の 3 つのカテゴリに分類されます。

- [分析およびレポート（Analysis & Reporting）] ウィジェットは、システムで収集および生成されたイベントに関するデータを表示します。
- [その他（Miscellaneous ）] ウィジェットは、イベント データもオペレーション データも表示しません。現時点では、このカテゴリのウィジェットのみが RSS フィードを表示します。
- [オペレーション（Operations）] ウィジェットは、システムのステータスおよび全体の正常性に関する情報を表示します。

表示されるダッシュボード ウィジェットは、次の項目に応じて異なります。

- 使用しているアプライアンスのタイプ
- ユーザ ロール

- 現在のドメイン（マルチドメイン展開内）

また、各ダッシュボードには、動作を決定する一連のプリファレンスがあります。

ユーザーは、ウィジェットを最小化および最大化する、タブに対してウィジェットを追加および削除する、タブ上でウィジェットを再配置する、といったことができます。

（注） 所定の時間範囲でのイベント カウントを表示するウィジェットでは、[分析（Analysis）] メニューのページの表で利用できる詳細なデータのイベント数が、イベントの総数に反映されないことがあります。これは、ディスク領域の使用率を管理するために、古いイベントの詳細がシステムによってプルーニングされることがあるために発生します。イベント詳細のプルーニングを最小限にするために、対象の展開にとって最も重要なイベントだけを記録するようにイベント ロギングを調整できます。

ウィジェットの使用可能性

表示できるダッシュボード ウィジェットは、使用中のアプライアンスのタイプ、使用するユーザ ロール、および（マルチドメイン展開での）現在のドメインによって異なります。

マルチドメイン展開で、予期したウィジェットが表示されない場合、グローバル ドメインに切り替えます。Secure Firewall Management Center のドメインの切り替え （25 ページ）を参照してください。

次の点に注意してください。

- 無効なウィジェットとは、ユーザが誤ったタイプのアプライアンスを使用しているために表示できないウィジェットのことです。
- 不正なウィジェットとは、ユーザ アカウントに必要な権限がないために表示できないウィジェットのことです。

たとえば、[アプライアンスの状態（Appliance Status）] ウィジェットを使用できるのは、Management Center で、管理者（Administrator）、メンテナンス ユーザ（Maintenance User）、セキュリティ アナリスト（Security Analyst）、またはセキュリティ アナリスト（読み取り専用）（Security Analyst（Read Only））のアカウント権限を持つユーザだけです。

不正なウィジェットまたは無効なウィジェットはダッシュボードに追加できませんが、インポートしたダッシュボードに不正なウィジェットまたは無効なウィジェットが含まれていることがあります。たとえば、インポートしたダッシュボードが次の場合に、このようなウィジェットが含まれている可能性があります。

- 各種アクセス権限を持つユーザによって作成された場合、または
- 先祖ドメインに属している場合。

使用できないウィジェットは無効になり、それらのウィジェットを表示できない理由を示すエラー メッセージが表示されます。

これらのウィジェットがタイムアウトした場合、またはそれ以外で問題が発生した場合には、個々のウィジェットでもエラー メッセージが表示されます。

（注） 不正なウィジェットと無効なウィジェット、および表示するデータがないウィジェットは、削除または最小化できます。共有されているダッシュボード上でウィジェットを変更すると、アプライアンスのすべてのユーザーのウィジェットも変更されることに注意してください。

ユーザー ロール別のダッシュボード ウィジェットの可用性

次の表に、各ウィジェットを表示するために必要なユーザ アカウントの権限を示します。Administrator、Maintenance User、Security Analyst、または Security Analyst（読み取り専用）のアクセス権を持つユーザ アカウントのみがダッシュボードを使用できます。

カスタム ロールを持つユーザは、自身のユーザ ロールの許可によって、ウィジェットのいずれかの組み合わせにアクセスできる場合もあれば、どのウィジェットにもアクセスできない場合もあります。

表 *24 :* ユーザ ロールとダッシュボード ウィジェットの可用性

ウィジェット	管理者	メンテナンス ユーザー	セキュリティ アナリスト	セキュリティ アナリスト（RO）
アプライアンス情報	はい	はい	はい	はい
アプライアンス ステータス（Appliance Status）	はい	はい	はい	いいえ
相関イベント（Correlation Events）	はい	いいえ	はい	はい
現在のインターフェイス ステータス（Current Interface Status）	はい	はい	はい	はい
現在のセッション（Current Sessions）	はい	いいえ	いいえ	いいえ
カスタム分析（Custom Analysis）	はい	いいえ	はい	はい
ディスク使用量（Disk Usage）	はい	はい	はい	はい
インターフェイス トラフィック（Interface Traffic）	はい	はい	はい	はい

ウィジェット	管理者	メンテナンスユーザー	セキュリティ アナリスト	セキュリティアナリスト（RO）
侵入イベント	はい	いいえ	はい	はい
ネットワーク コンプライアンス（Network Compliance）	はい	いいえ	はい	はい
製品ライセンスの認証（Product Licensing）	はい	はい	いいえ	いいえ
製品アップデート（Product Updates）	はい	はい	いいえ	いいえ
RSS フィード（RSS Feed）	はい	はい	はい	はい
システム ロード（System Load）	はい	はい	はい	はい
システム タイム（System Time）	はい	はい	はい	はい
許可（Allow）イベントの一覧表示	はい	いいえ	はい	はい

定義済みダッシュボード ウィジェット

システムには、いくつかの定義済みウィジェットが付属しています。これらのウィジェットをダッシュボード上で使用することで、現在のシステムステータスを一目で確認できます。ウィジェットのビューには、以下の情報が表示されます。

- システムが収集および生成したイベントに関するデータ
- 使用している導入のアプライアンスのステータスと全体的なヘルスに関する情報

（注） 表示できるダッシュボードウィジェットは、使用しているアプライアンスのタイプとユーザーロール、およびマルチドメイン展開の場合は現在のドメインによって異なります。

[アプライアンス情報（Appliance Information）] ウィジェット

[アプライアンス情報（Appliance Information）] ウィジェットは、アプライアンスのスナップショットを提供します。このウィジェットは、**詳細ダッシュボード**および**サマリダッシュボード**の [ステータス（Status）] タブにデフォルトで表示されます。

Management Center が高可用性で設定されている場合、Management Center のアプライアンス情報ウィジェットには、Management Center 高可用性に関する情報が表示されます。たとえば、Management Center のロール、ステータス、詳細ステータス、および最後コンタクトに関する情報が表示されます。このウィジェットは以下の情報を提供します。

- アプライアンスの名前、IPv4 アドレス、IPv6 アドレス、およびモデル
- ダッシュボードでアプライアンスにインストールされている、システムソフトウェア、オペレーティングシステム、Snort、ルール更新、ルールパック、モジュールパック、脆弱性データベース（VDB）、および地理情報更新のバージョン（Management Center Virtualは除く）
- 管理対象アプライアンスの場合は、管理アプライアンスとの通信リンクの名前とステータス

単純なビューまたは高度なビューを表示するようにウィジェットのプリファレンスを変更することで、ウィジェットで表示する情報量を調整できます。プリファレンスでは、ウィジェットをアップデートする頻度を調整することもできます。

[アプライアンス ステータス（Appliance Status）] ウィジェット

[アプライアンス ステータス（Appliance Status）] ウィジェットは、アプライアンスの正常性、およびそのアプライアンスが管理しているアプライアンスの正常性を示します。Management Centerは、管理対象のデバイスに対して自動的に正常性ポリシーを適用しないため、ユーザーは正常性ポリシーをデバイスへ手動で適用する必要があります。このようにしないと、デバイスのステータスは `Disabled` として示されます。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス（Status）] タブにデフォルトで表示されます。

ウィジェットの設定を変更して、アプライアンスのステータスを円グラフまたは表で表示するように設定できます。

プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

円グラフの一部、またはアプライアンス ステータス表のいずれかの数字をクリックすると、[ヘルス モニター（Health Monitor）] ページが表示され、対象のアプライアンス、およびそのアプライアンスが管理しているすべてのアプライアンスのコンパイル済みの正常性ステータスを参照することができます。

[相関イベント（Correlation Events）] ウィジェット

[相関イベント（Correlation Events）] ウィジェットは、ダッシュボードの時間範囲における 1 秒あたりの相関イベントの平均数を、優先度ごとに示します。このウィジェットは、詳細ダッシュボードの [相関（Correlation）] タブにデフォルトで表示されます。

ウィジェットを設定して、線形（増分）や対数（10 の倍数）のスケールを選択するだけでなく、ウィジェットの設定を変更してさまざまな優先度の相関イベントを表示することができます。

優先度を持たないイベントも含めて、特定の優先度のイベントに対して別のグラフを表示するには、1 つ以上の [優先順位（Priorities）] チェックボックスをオンにします。優先度に関係な

くすべての相関イベントに対して追加のグラフを表示するには、[すべて表示（Show All）] を選択します。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

グラフをクリックして特定の優先度の相関イベントを表示することも、[すべて（All）] グラフをクリックしてすべての相関イベントを表示することもできます。いずれの場合も、イベントはダッシュボードの時間範囲に制限されます。ダッシュボードを介して相関イベントにアクセスすると、そのアプライアンスに対するイベント（またはグローバル）の期間が変わります。

[現在のインターフェイス ステータス（Current Interface Status）] ウィジェット

[現在のインターフェイス ステータス（Current Interface Status）] ウィジェットは、有効になっているか未使用のアプライアンスのすべてのインターフェイスのステータスを示します。Management Center では、管理（`eth0`、`eth1` など）インターフェイスを表示できます。管理対象デバイスでは、センシング（`s1p1` など）インターフェイスのみを表示するか、または管理インターフェイスとセンシングインターフェイスの両方を表示するかを選択できます。インターフェイスは、タイプ（管理、インライン、パッシブ、スイッチド、ルーテッド、未使用）別にグループ化されます。

ウィジェットは、各インターフェイスに対して次の情報を提供します。

- インターフェイスの名前
- インターフェイスのリンク状態
- インターフェイスのリンク モード（100Mb 全二重、または 10Mb 半二重など）
- インターフェイスのタイプ（銅線または光ファイバ）
- インターフェイスで受け取ったデータ量（Rx）および送信したデータ量（Tx）

リンク状態を表すボールの色は、次のように現在のステータスを示します。

- 緑色：リンクがフル スピードでアップ状態になっています
- 黄色：リンクはアップ状態ですがフル スピードではありません
- 赤色：リンクはアップ状態ではありません
- 灰色：リンクは管理上無効になっています
- 青色：リンク ステート情報は使用できません（たとえば ASA）

ウィジェットのプリファレンスでは、ウィジェットをアップデートする頻度を調整します。

[現在のセッション（Current Sessions）] ウィジェット

[現在のセッション（Current Sessions）] ウィジェットは、アプライアンスに現在ログインしているユーザー、セッションが生じたマシンに関連付けられている IP アドレス、各ユーザーがアプライアンス上のページにアクセスした最後の（アプライアンスのローカル時間に基づいた）時間を示します。自分を表すユーザー（現在ウィジェットを表示しているユーザー）には、**ユーザーアイコン**のマークが付けられ、太字で示されます。ログオフするか非アクティブになってから 1 時間以内に、セッションはこのウィジェットのデータからプルーニングされま

す。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス（Status）] タブにデフォルトで表示されます。

[現在のセッション（Current Sessions）] ウィジェットでは、次のことができます。

- いずれかのユーザー名をクリックして、[ユーザー管理（User Management）] ページでユーザー アカウントを管理します。
- **ホストアイコン**、またはIPアドレスの隣の**侵害を受けたホストアイコン**をクリックして、関連付けられているマシンのホストプロファイルを表示します。
- いずれかの IP アドレスまたはアクセス時間をクリックして、その IP アドレスおよびその IP アドレスに関連付けられているユーザーが Web インターフェイスにログオンした時間によって制約される監査ログを表示します。

ウィジェットのプリファレンスでは、ウィジェットをアップデートする頻度を調整します。

[カスタム分析（Custom Analysis）] ウィジェット

[カスタム分析（Custom Analysis）] ウィジェットは高度にカスタマイズ可能なウィジェットで、これを使用すると、システムで収集および生成されたイベントの詳細情報を表示できます。

このウィジェットには複数のプリセットが用意されており、導入に関する情報にすばやくアクセスできます。事前定義済みのダッシュボードから、これらのプリセットを幅広く使用できます。これらのプリセットを使用することも、カスタム設定を作成することもできます。カスタム構成では少なくとも、関心のあるデータ（表とフィールド）とそのデータの集計方法を指定します。イベントの相対的な発生数を表示するのか（棒グラフ）、一定期間のイベント数を表示するのか（折れ線グラフ）など、その他の表示関連の設定を適用することもできます。

このウィジェットは、ローカル時間に基づいて、最後にアップデートされた時間を表示します。ウィジェットのアップデートは、ダッシュボードの時間範囲に基づいた頻度で実行されます。たとえば、ダッシュボードの時間範囲を 1 時間に設定すると、ウィジェットは 5 分ごとにアップデートされます。また、ダッシュボードの時間範囲を 1 年に設定すると、ウィジェットは 1 週間ごとにアップデートされます。ダッシュボードが次にアップデートされるタイミングを設定するには、ウィジェットの左下にある [最終更新日（Last updated）] の通知にポインタを移動します。

（注） [カスタム分析（Custom Analysis）] ウィジェットに赤い影が付いている場合は、そのウィジェットの使用がシステムのパフォーマンスに悪影響を及ぼしています。ウィジェットが長時間赤い状態のままになっている場合は、そのウィジェットを削除してください。また、システム構成（**[システム（System）] > [設定（Configuration）] > [ダッシュボード（Dashboard）]**）のダッシュボード設定で、すべての [カスタム分析（Custom Analysis）] ウィジェットを無効にすることもできます。

イベントの相対的な発生数の表示（棒グラフ）

[カスタム分析（Custom Analysis）] ウィジェットの棒グラフでは、ウィジェットの背景の色付きバーが、各イベントの相対的な発生数を示します。バーは右から順にお読みください。

矢印のアイコン は、表示のソート順を示し、制御します。下向きのアイコンは降順を表し、上向きのアイコンは昇順を表します。ソート順を変更するには、アイコンをクリックします。

最新の結果以降何らかの変更点があることを示すために、ウィジェットでは、各イベントの横に次の 3 つのアイコンのうちの 1 つを表示します。

- 新しいイベントアイコン **Add** ( ) は、イベントが、最新の結果以降のものであることを示します。
- **上向き矢印のアイコン**は、ウィジェットが最後にアップデートされた後で、イベントがこの場所に上がってきたことを示します。イベントが何段階上がってきたかを表す数字が、アイコンの横に示されます。
- **下向き矢印のアイコン**は、ウィジェットが最後にアップデートされた後で、イベントがこの場所に下がってきたことを示します。イベントが何段階下がってきたかを表す数字が、アイコンの横に示されます。

一定期間のイベントの表示（折れ線グラフ）

一定期間のイベントまたは収集されたその他のデータに関する情報が必要な場合は、対象の展開で、一定期間に発生した侵入イベントの合計数を表示するような線グラフを表示するように [カスタム分析（Custom Analysis）] ウィジェットを設定することができます。

[カスタム分析（Custom Analysis）] ウィジェットの制限

[カスタム分析（Custom Analysis）] ウィジェットは、表示するように設定されたデータを表示する権限がないことを示すことがあります。たとえば、メンテナンスユーザには検出イベントを表示する権限がありません。また、このウィジェットは、ライセンスされていない機能に関連する情報を表示しません。ただし、そのユーザ（およびダッシュボードを共有している他のユーザ）は、ウィジェットの設定を変更して、自分が表示できるデータを表示することも、ウィジェットを削除することもできます。これを防ぐには、ダッシュボードをプライベート（非公開）で保存します。

ユーザ データを表示した場合は、権限のあるユーザのみが表示されます。

URL カテゴリ情報を表示した場合、分類されていない URL は表示されません。

[カウント（Count）] で集約された侵入イベントを表示すると、カウントには侵入イベントに関して確認済みのイベントが含められます。[分析（Analysis）] のページのテーブルにカウントを表示すると、カウントに確認済みイベントは含められません。

（注） マルチドメイン展開では、システムは、各リーフ ドメインに個別のネットワーク マップを作成します。その結果、リーフ ドメインには、ネットワーク内で一意である IP アドレスを含めることができますが、別のリーフ ドメイン内の IP アドレスと同じにすることができます。先祖ドメインで [カスタム分析（Custom Analysis）] ウィジェットを表示すると、繰り返し使用される IP アドレスの複数のインスタンスを表示できます。一見すると、エントリが重複しているように見えることがあります。ただし、各 IP アドレスのホスト プロファイル情報までドリル ダウンすると、それらが異なるリーフ ドメインに属していることがわかります。

デバイスのダッシュボードウィジェットを作成する方法

デバイスからのイベントを表示するウィジェットは、特定のデバイスまたは一連のデバイスのイベントの表示を制限するフィルタを使用するように構成できます。

1. 検索を作成して保存する：**[分析（Analysis）]** > **[検索（Search）]** に移動し、特定のデバイス名に一致する検索パラメータを入力します。

（注） 展開されたデバイス名をリストするドロップダウンはないため、完全に一致するテキストを指定する必要があります。

2. **[概要（Overview）]** > **[ダッシュボード（Dashboards）]** > **[ウィジェットの追加（Add Widgets）]** に移動して、[カスタム分析（Custom Analysis）] ウィジェットを作成します。
3. **[概要（Overview）]** > **[ダッシュボード（Dashboards）]** に戻り、新しいウィジェットを変更して、検索範囲でカスタマイズします。

例：[カスタム分析（Custom Analysis）] ウィジェットの構成

最近の侵入イベントのリストを表示するように [カスタム分析（Custom Analysis）] ウィジェットを設定するには、[侵入イベント（Intrusion Events）] テーブルのデータを表示するようにウィジェットを設定します。[分類（Classification）] フィールドを選択し、このデータを [カウント（Count）] で集約すると、各タイプで生成されたイベントの数が表示されます。

一方、[一意のイベント（Unique Events）] で集約すると、各タイプで一意の侵入イベントの数が表示されます（たとえばネットワークの Trojan、企業ポリシーの潜在的な違反、行われたサービス妨害攻撃の検出個数など）。

ウィジェットをさらにカスタマイズするには、保存されている検索（アプライアンスに付属している事前定義の検索、またはユーザーが作成したカスタム検索のいずれか）を使用します。たとえば、最初の例（[分類（Classification）] フィールドを使用して [カウント（Count）] で集約する）を、[ドロップされたイベント（Dropped Events）] の検索を使用して制約すると、各タイプでドロップされた侵入イベントの数が表示されます。

関連トピック

ダッシュボード時刻設定の変更 （426 ページ）

[カスタム分析（Custom Analysis）]ウィジェットのプリファレンス

次の表に、[カスタム分析（Custom Analysis）]ウィジェットで設定できるプリファレンスについて示します。

さまざまなプリファレンスは、ウィジェットを設定する方法に応じて表示されます。たとえば、イベントの相対頻度（棒グラフ）を表示する場合と、時系列のグラフ（線グラフ）を表示する場合とでは、ウィジェットの設定時に異なるプリファレンスセットが表示されます。フィルタなど、一部のプリファレンスは、表示するデータが存在する特定のテーブルを選択する場合にのみ表示されます。

表 *25 : [*カスタム分析（*Custom Analysis***）*]*ウィジェットのプリファレンス**

設定	詳細
役職（Title）	ウィジェットのタイトルを指定しない場合、システムは、設定済みのイベント タイプをタイトルとして使用します。
プリセット（Preset）	[カスタム分析（Custom Analysis）]のプリセットによって、展開に関する情報に簡単にアクセスできます。事前定義済みのダッシュボードから、これらのプリセットを幅広く使用できます。これらのプリセットを使用することも、カスタム設定を作成することもできます。
テーブル（Table）（必須）	ウィジェットが表示するデータを含むイベントまたはアセットのテーブル。
フィールド（Field）（必須）	表示するイベントタイプの特定のフィールド。時系列でデータ（線グラフ）を表示するには、[時間（Time）] を選択します。イベントの相対頻度（棒グラフ）を表示するには、もう一方のオプションを選択します。
集約（Aggregate）（必須）	集約方法は、表示するデータをウィジェットがどのようにグループ化するかを設定します。ほとんどのイベント タイプのデフォルト オプションは [カウント（Count）] です。
フィルタ	[アプリケーション統計（Application Statistics）] および [アプリケーション別の侵入イベント統計（Intrusion Event Statistics by Application）] テーブルのデータを制約するには、アプリケーション フィルタを使用できます。

設定	詳細
検索（Search）	保存した検索を使用して、ウィジェットが表示するデータを制約することができます。検索を指定する必要はありませんが、プリセットの中には事前定義された検索が使用されるものがあります。 ユーザがアクセスできる検索は、プライベートで保存した検索だけです。共有ダッシュボード上にウィジェットを設定し、プライベートの検索を使用してイベントを制約すると、ウィジェットは、他のユーザがログインしたときにその検索を使用しないようにリセットされます。ウィジェットのビューにも影響します。これを防ぐには、ダッシュボードをプライベート（非公開）で保存します。 接続イベントに基づいて [カスタム分析（Custom Analysis）] ダッシュボード ウィジェットを制約できるのは、接続サマリーを制限しているフィールドだけです。保存した無効な検索はグレー表示されます。 保存されている検索を使用して [カスタム分析（Custom Analysis）] ウィジェットを制約し、その後で検索を編集すると、次にアップデートされるまでウィジェットには変更が反映されません。
表示（Show）	最も高い（[最上位（Top）]）または最も低い（[最下位（Bottom）]）頻度で発生するイベントを表示するかどうかを選択します。
結果（Results）	表示する結果の行数を選択します。
Mover の表示（Show Movers）	最新の結果以降の変更を示すアイコンを表示するかどうかを選択します。
タイム ゾーン	結果の表示に使用するタイム ゾーンを選択します。
カラー（Color）	ウィジェットの棒グラフのバーの色を変更できます。

関連トピック

ウィジェットのプリファレンス設定 （423 ページ）

カスタム分析ウィジェットから関連するイベントを表示する

Custom Analysis ウィジェットから、ウィジェットに表示されるイベントに関する詳細情報を提供するイベント ビューア（ワークフロー）を起動することができます。イベントは、ダッシュボードの時間範囲によって制限されて、そのイベント タイプのデフォルトのワークフローで表示されます。設定した時間枠の数やイベント タイプに応じて、Management Center の時間枠が適宜変更されます。

次に例を示します。

- 複数の期間が設定されている場合に、Custom Analysis ウィジェットからヘルス イベントにアクセスすると、デフォルトのヘルス イベント ワークフローにイベントが表示され、ヘルス モニタリング期間はダッシュボードの時間範囲に変更されます。

- 1 つの時間枠を設定していて Custom Analysis ウィジェットから任意のタイプのイベントにアクセスすると、イベントはそのイベント タイプのデフォルト ワークフローに表示され、グローバル期間がダッシュボードの時間範囲に変更されます。

手順

次の選択肢があります。

- [カスタム分析（Custom Analysis）] ウィジェットの右下にある[表示（View）]（  ）をクリックして、ウィジェットの設定で制約して、すべての関連イベントを表示することができます。
- 関連するイベントの発生数（棒グラフ）を表示するように設定された Custom Analysis ウィジェットで、任意のイベントをクリックして、ウィジェットの設定、およびそのイベントで制約して、関連イベントを表示します。

[ディスク使用量（Disk Usage）] ウィジェット

[ディスク使用量（Disk Usage）] ウィジェットは、ディスク使用率のカテゴリに基づいて、ハードドライブで使用される領域のパーセンテージを表示します。また、アプライアンスのハードドライブの各パーティションで使用される領域のパーセンテージおよび容量も示します。Disk Usage ウィジェットがデバイスにインストールされている場合、またはManagement Centerが、マルウェア ストレージ パックが含まれているデバイスを管理している場合は、Disk Usage ウィジェットはマルウェア ストレージ パックについて同じ情報を表示します。このウィジェットは、デフォルト ダッシュボードおよびサマリ ダッシュボードの [ステータス（Status）] タブにデフォルトで表示されます。

By Category スタック バーは、各ディスク使用率のカテゴリを、使用可能な合計ディスク領域に対する使用量の割合として表示します。次の表で、使用可能なカテゴリについて説明します。

表 *26*：ディスク使用率のカテゴリ

ディスク使用率のカテゴリ	説明
イベント	システムで記録されたすべてのイベント
ファイル（Files）	システムに格納されたすべてのファイル
バックアップ	すべてのバックアップ ファイル
変更点	ルールのアップデートやシステムのアップデートなど、アップデートに関連するすべてのファイル
その他	システムのトラブルシューティング ファイルおよびその他のファイル

ディスク使用率のカテゴリ	説明
未使用	アプライアンス上の残りの空き領域

By Category スタック バーのディスク使用率カテゴリにポインタを合わせると、使用可能なディスク領域のうち、そのカテゴリで使用された領域の割合、ディスク上の実際のストレージ領域、およびそのカテゴリで使用可能なディスク領域の合計を表示することができます。マルウェア ストレージ パックがインストールされている場合、[ファイル（Files）] カテゴリで使用できるディスク領域の合計は、マルウェア ストレージ パックで使用できるディスク領域になることに注意してください。

マルウェア ストレージ パックがインストールされている場合は、ウィジェットのプリファレンスを変更して、[カテゴリ別（By Category）] スタック バーのみを表示したり、スタック バーと admin（/）、/Volume、および /boot パーティションの使用率、および /var/storage パーティションを表示したりするようにウィジェットを設定できます。

ウィジェットのプリファレンスは、ウィジェットのアップデート頻度、およびダッシュボードの時間範囲で現在のディスク使用率または収集したディスク使用率の統計のいずれかを表示するかも制御します。

[インターフェイス トラフィック（Interface Traffic）] ウィジェット

[インターフェイス トラフィック（Interface Traffic）] ウィジェットには、アプライアンスのインターフェイスで送受信された受信（Rx）トラフィックと送信（Tx）トラフィックの割合が示されます。このウィジェットは、事前定義されたダッシュボードにデフォルトでは表示されません。

マルウェア防御ライセンスが有効になっているデバイスは、動的分析を設定していない場合でも、定期的に AMP クラウドへの接続を試行します。そのため、これらのデバイスには送信トラフィックが表示されます。これは想定されている動作です。

ウィジェットのプリファレンスでは、ウィジェットをアップデートする頻度を調整します。

[侵入イベント（Intrusion Events）] ウィジェット

[侵入イベント（Intrusion Events）] ウィジェットは、ダッシュボードの時間範囲で発生した侵入イベントを、優先度ごとに表示します。これには、ドロップされたパケットおよびさまざまな影響を含む、侵入イベントの統計が含まれています。このウィジェットは、サマリ ダッシュボードの [侵入イベント（Intrusion Events）] タブにデフォルトで表示されます。

ウィジェットの設定では、次のことができます。

- [イベント フラグ（Event Flags）] には、パケットが欠落したイベント、パケットが欠落した可能性のあるイベント、または特定の影響を示すグラフが個別に表示されます。影響やルールの状態に関係なくすべての侵入イベントに対して追加のグラフを表示するには、[すべて（All）] を選択します。

アイコンの説明については、侵入イベント （945 ページ）を参照してください。影響レベルの数字の上に表示される矢印（ある場合）はインライン結果を表すもので、次のように定義されています。

表 *27*：ワークフロー ビューテーブル ビューの *[インライン結果（Inline Result）]* フィールドの内容

アイコン	意味
	ルールをトリガーしたパケットをシステムがドロップしました。
	[インライン時にドロップ（Drop when Inline）] 侵入ポリシーオプション（インライン展開環境）を有効にした場合、またはシステムがプルーニングしている間に [ドロップしてイベントを生成する（Drop and Generate）] ルールがイベントを生成した場合、IPS がパケットをドロップしたことを示します。
	IPS はパケットを宛先に送信または配信した可能性がありますが、このパケットを含む接続は現在ブロックされています。
アイコンなし（空白）	トリガーされたルールは [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されていませんでした

パッシブ展開では、侵入ポリシーのルールの状態やインライン ドロップ動作に関係なく、インライン インターフェイスがタップ モードの場合を含めて、システムはパケットをドロップしません。

- [表示（Show）] では、[1秒あたりの平均イベント数（Average Events Per Second）]（EPS）または [イベントの合計数（Total Events）] を選択できます。
- [縦方向スケール（Vertical Scale）] では、[線形（Linear）]（増分）または [対数（Logarithmic）]（10 の倍数）のスケールを選択できます。
- ウィジェットの更新頻度。

ウィジェットでは次のことができます。

- ドロップされたパケット、ドロップされた可能性のあるパケット、または特定の影響に対応するグラフをクリックして、そのタイプの侵入イベントを表示します。
- ドロップされたイベントに対応するグラフをクリックして、ドロップされたイベントを表示します。
- ドロップされたと考えられるイベントに対応するグラフをクリックして、ドロップされたと考えられるイベントを表示します。
- [すべて（All）] グラフをクリックして、すべての侵入イベントを表示します。

結果のイベント ビューは、ダッシュボードの時間範囲に制約されます。ダッシュボードを介して侵入イベントにアクセスすると、そのアプライアンスに対するイベント（またはグローバ

ル）の期間が変わります。侵入ルールの状態または侵入ポリシーのインライン ドロップ動作に関係なく、パッシブな配置のパケットはドロップされないことに注意してください。

ネットワーク コンプライアンス ウィジェット

[ネットワークコンプライアンス（Network Compliance）] ウィジェットは、ユーザーが設定したallowリストに対するホストのコンプライアンスを要約します。デフォルトではこのウィジェットに、アクティブな相関ポリシーにおけるすべてのコンプライアンスallowリストに対して準拠しているホスト、準拠していないホスト、および評価されなかったホストの数を示す円グラフが表示されます。このウィジェットは、詳細ダッシュボードの [相関（Correlation）] タブにデフォルトで表示されます。

ウィジェットの設定を変更して、すべてのallowリスト、または特定のallowリストのいずれかについてネットワーク コンプライアンスを表示するようにウィジェットを設定できます。

すべてのallowリストに対してネットワーク コンプライアンスを表示するよう選択すると、あるホストが、アクティブな相関ポリシーのいずれのallowリストにも準拠していない場合、ウィジェットはそのホストが非準拠であると見なします。

また、このウィジェットの設定を使用すると、ネットワーク コンプライアンスの表示で次の 3 つのスタイルのうちどれを使用するかを指定することができます。

[ネットワーク コンプライアンス（Network Compliance）] スタイル（デフォルト）は、準拠しているホスト、準拠していないホスト、および評価されなかったホストの数を示す円グラフを表示します。ホストの違反の件数を表示するには、円グラフをクリックします。このようにすると、少なくとも 1 つのallowリストに違反しているホストが表示されます。

[一定期間のネットワーク コンプライアンス（%）（Network Compliance over Time (%)）] スタイルは、ダッシュボードの時間範囲において準拠しているホスト、準拠していないホスト、およびまだ評価されていないホストの相対的な割合を示す積み重ね面積グラフを表示します。

[一定期間のネットワーク コンプライアンス（Network Compliance over Time）] スタイルは、ダッシュボードの時間範囲において準拠しているホスト、準拠していないホスト、およびまだ評価されていないホストの数を示す線グラフを表示します。

ウィジェットをアップデートする頻度は、設定で調整します。まだ評価されていないイベントを非表示にするには、[未評価を表示（Show Not Evaluated）] ボックスをオンにします。

[製品ライセンス（Product Licensing）] ウィジェット

[製品ライセンス（Product Licensing）] ウィジェットは、Management Center に現在インストールされているデバイスおよび機能のライセンスを示します。また、ライセンス契約されているアイテムの数、許可される残りのライセンス契約アイテム数も示します。これは、事前定義されたどのダッシュボードにおいてもデフォルトでは表示されません。

このウィジェットの上部のセクションには、一時的なライセンスも含めて、Management Center にインストールされているすべてのデバイスおよび機能のライセンスが表示されますが、[期限の切れたライセンス（Expiring Licenses）] セクションには、一時的なライセンスおよび期限の切れたライセンスのみが表示されます。

ウィジェットの背景のバーは、使用中のライセンスのそれぞれのタイプの割合を示しています。このバーは右から左へ読みます。期限の切れたライセンスには、取り消し線が付けられています。

ウィジェットのプリファレンスを変更して、現在ライセンス契約されている機能を表示するか、またはライセンス契約が可能なすべての機能を表示するようにウィジェットを設定することができます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

任意のライセンス タイプをクリックすると、ローカル設定の [ライセンス（License）] ページに移動して、機能ライセンスを追加または削除することができます。

[製品更新（Product Updates）] ウィジェット

[製品更新（Product Updates）] ウィジェットは、アプライアンスに現在インストールされているソフトウェアの概要、およびダウンロード済みだがまだインストールしていない更新プログラムの情報を提供します。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス（Status）] タブにデフォルトで表示されます。

このウィジェットは、スケジュールされたタスクを使用して最新バージョンを判別するため、更新プログラムをダウンロード、プッシュ、またはインストールするようにスケジュールされたタスクを構成するまで、`Unknown` と表示されます。

ウィジェットのプリファレンスを変更して、最新のバージョンを非表示にするようウィジェットを設定できます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

このウィジェットには、ソフトウェアを更新できるページへのリンクもあります。次の操作を実行できます。

- 現在のバージョンをクリックして、アプライアンスを手動で更新します。
- 最新バージョンをクリックして、更新プログラムをダウンロードするタスクをスケジュールします。

[RSS フィード（RSS Feed）] ウィジェット

[RSS フィード（RSS Feed）] ウィジェットは、ダッシュボードに RSS フィードを追加します。デフォルトでは、ウィジェットはシスコのセキュリティ ニュースのフィードを示します。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス（Status）] タブにデフォルトで表示されます。

また、企業ニュース、Snort.org ブログ、または Cisco 脅威調査ブログの事前設定済みのフィードを表示するようウィジェットを設定することができます。ウィジェットの設定で URL を指定して、他の RSS フィードに対するカスタム接続を作成することもできます。Management Center は、Management Center が認識している認証局（CA）によって署名された信頼できるサーバー証明書が使用されている場合にのみ、暗号化された RSS フィードを表示できます。Management Center が認識していない CA が使用されている、または自己署名証明書が使用されている暗号化された RSS フィードを表示するように RSS フィードウィジェットを設定すると、検証は失敗し、ウィジェットでフィードは表示されません。

フィードは24時間ごとに更新されます（ただしユーザーはフィードを手動で更新できます）。また、ウィジェットはアプライアンスのローカル時間に基づいて、フィードが最後に更新された時間を表示します。アプライアンスは、（事前設定された2つのフィードについて）Webサイトに対するアクセス権を持っている、または設定したいずれかのカスタムフィードに対するアクセス権を持っている必要があります。

ウィジェットを設定する場合には、フィードからいくつのストーリーをウィジェットに表示するか、およびヘッドラインとともにストーリーの説明を表示するかどうかを選択することができます。ただしすべてのRSSフィードで説明が使用できるわけではないことに注意してください。

[RSSフィード（RSS Feed）] ウィジェットでは、次のことができます。

- フィード内のストーリーのいずれかをクリックして、ストーリーを表示します
- [さらに表示（more）] リンクをクリックして、フィードのWebサイトへ移動します
- **アップデート**（[アップデート（update）] アイコン）をクリックして、フィードを手動で更新します

[システム負荷（System Load）] ウィジェット

[システム負荷（System Load）] ウィジェットは、アプライアンス上の（各CPUについての）CPUの使用率、メモリ（RAM）の使用率、およびシステムの負荷（実行を待機しているプロセスの数によって測定され、負荷平均とも呼ばれる）を現在、およびダッシュボードの時間範囲について表示します。このウィジェットは、Detailed DashboardおよびSummary Dashboardの[Status] タブにデフォルトで表示されます。

ウィジェットのプリファレンスを変更して、負荷平均を表示または非表示にするようウィジェットを設定できます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

[システム時刻（System Time）] ウィジェット

[システム時刻（System Time）] ウィジェットは、アプライアンスのローカル システム時間、稼動時間、およびブート時間を表示します。このウィジェットは、Detailed DashboardおよびSummary Dashboardの[Status] タブにデフォルトで表示されます。

ウィジェットのプリファレンスを変更して、ブート時間を非表示にするようウィジェットを設定できます。プリファレンスは、ウィジェットがアプライアンスの時計と同期する頻度も調整します。

許可（Allow）リストイベントウィジェット

許可（Allow）リストイベントウィジェットは、ダッシュボードの時間範囲における1秒あたりの平均イベント数を、優先順位ごとに表示します。このウィジェットは、デフォルト ダッシュボードの [相関（Correlation）] タブにデフォルトで表示されます。

ウィジェットの設定を変更して、さまざまな優先順位のallowリストイベントを表示するようウィジェットを設定できます。

ウィジェットの設定では、次のことができます。

- 優先度を持たないイベントも含めて、特定の優先度のイベントに対して別のグラフを表示するには、1 つ以上の [優先順位（Priorities）] チェックボックスをオンにします。
- 優先順位に関係なくすべてのallowリストイベントに対して追加のグラフを表示するには、[すべて表示（Show All）] を選択します
- [縦方向スケール（Vertical Scale）] を選択して、[線形（Linear）]（増分）または [対数（Logarithmic）]（10 の倍数）のスケールを選択します。

プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

グラフをクリックして特定の優先順位のallowリストイベントを表示することも、[すべて（All）] グラフをクリックしてすべてのallowリストイベントを表示することもできます。いずれの場合も、イベントは、ダッシュボードの時間範囲によって制約されます。ダッシュボードを介してallowリストイベントにアクセスすると、Management Center に対するイベント（またはグローバル）の期間が変わります。

ダッシュボードの管理

手順

ステップ 1 **[概要（Overview）] > [ダッシュボード（Dashboards）]** を選択して、変更するダッシュボードをメニューから選択します。

ステップ 2 ダッシュボードを管理します。

- ダッシュボードの作成：カスタム ダッシュボードを作成します。カスタム ダッシュボードの作成 （424 ページ）を参照してください。
- ダッシュボードの削除：ダッシュボードを削除するには、削除するダッシュボードの横にある[削除（Delete）]（）をクリックします。デフォルトのダッシュボードを削除する場合は、新しいデフォルトを定義する必要があります。そうしない場合、ダッシュボードを表示しようとするたびに、アプライアンスからダッシュボードを選択するように要求されます。
- オプションの編集：カスタムのダッシュボードオプションを編集します。ダッシュボードオプションの編集 （426 ページ）を参照してください。
- 時間の制約の変更：ダッシュボードの表示時間または一時停止/一時停止解除の時間を変更します。詳細は、ダッシュボード時刻設定の変更 （426 ページ）を参照してください。

ステップ 3 ダッシュボードを追加（ダッシュボードの追加 （422ページ）を参照）、削除（[閉じる（Close）]（）をクリック）、および名前変更（ダッシュボードの名前変更 （428ページ）を参照）します。

（注） ダッシュボードの順序は変更できません。

ステップ 4 ダッシュボード ウィジェットを管理します。

- ウィジェットの追加：ダッシュボードにウィジェットを追加します。ダッシュボードへのウィジェットの追加 （422 ページ）を参照してください。
- プリファレンスの設定：ウィジェットのプリファレンスを設定します。ウィジェットのプリファレンス設定 （423 ページ）を参照してください。
- 表示のカスタマイズ：ウィジェットの表示をカスタマイズします。ウィジェット表示のカスタマイズ （425 ページ）を参照してください。
- イベントの表示：カスタム分析ウィジェットから関連するイベントを表示します。カスタム分析ウィジェットから関連するイベントを表示する （414ページ）を参照してください。

ヒント シスコの事前定義のダッシュボード内のカスタム分析ウィジェットのすべての設定が、ウィジェットのシステムプリセットに対応しています。これらのウィジェットの1つを変更または削除した場合は、適切なプリセットをベースにして新しいカスタム分析ウィジェットを作成して復元することができます。

ダッシュボードの追加

手順

ステップ 1 変更するダッシュボードを表示します（ダッシュボードの表示 （428 ページ）を参照）。

ステップ 2 **Add** ( ) をクリックします。

ステップ 3 名前を入力します。

ステップ 4 [OK] をクリックします。

ダッシュボードへのウィジェットの追加

各タブには、3 列のレイアウトで 1 つ以上のウィジェットを表示できます。ダッシュボードにウィジェットを追加するには、ウィジェットを追加するタブを選択します。ウィジェットは、自動的にウィジェットが最も少ない列に追加されます。すべてのカラムに同じ数のウィジェットがある場合、新しいウィジェットは最も左のカラムに追加されます。ダッシュボードタブには最大 15 個のウィジェットを追加できます。

ヒント 追加したウィジェットは、タブの任意の場所に移動できます。ただし、別のタブにはウィジェットを移動できません。

表示されるダッシュボードウィジェットは、使用しているアプライアンスのタイプ、ユーザロールと（マルチドメイン環境では）現在のドメインにより異なります。すべてのユーザロー

ルがすべてのダッシュボード ウィジェットに対してアクセス権を持っているわけではないため、多くの権限を持つユーザが作成したダッシュボードを、それよりも少ない権限を持つユーザが参照する場合、ダッシュボードのすべてのウィジェットを使用できないことがあることに注意してください。ダッシュボード上に、許可されていないウィジェットが表示されることがありますが、これらのウィジェットは無効です。

手順

ステップ 1 ウィジェットを追加するダッシュボードを表示します。ダッシュボードの表示 （428 ページ）を参照してください。

ステップ 2 ウィジェットを追加するタブをクリックします。

ステップ 3 [ウィジェットの追加（Add Widgets）] をクリックします。カテゴリ名をクリックして各カテゴリのウィジェットを表示することも、[すべてのカテゴリ（All Categories）] をクリックしてすべてのウィジェットを表示することもできます。

ステップ 4 追加するウィジェットの横にある [追加（Add）] をクリックします。[ウィジェットの追加（Add Widgets）] ページには、追加するものも含め、各タブにあるウィジェットの数がタイプごとに表示されます。

ヒント （複数の RSS Feed ウィジェット、または複数の Custom Analysis ウィジェットを追加する場合など）同じタイプの複数のウィジェットを追加するには、[追加（Add）] をもう一度クリックします。

ステップ 5 ウィジェットの追加が終了したら、[完了（Done）] をクリックしてダッシュボードに戻ります。

次のタスク

- カスタム分析ウィジェットを追加した場合は、ウィジェットの設定が必要です。ウィジェットのプリファレンス設定 （423 ページ） を参照してください。

関連トピック

ウィジェットの使用可能性 （405 ページ）

ウィジェットのプリファレンス設定

各ウィジェットには、動作を決定する一連のプリファレンスがあります。

手順

ステップ 1 プリファレンスを変更するウィジェットのタイトルバーで、[表示設定（Show Preferences）]（  ） をクリックします。

ステップ 2 必要に応じて変更を加えます。

ステップ 3 プリファレンスセクションを非表示にするには、ウィジェットのタイトルバーで、[非表示設定（Hide Preferences）]（▼）をクリックします。

カスタム ダッシュボードの作成

ヒント 新しいダッシュボードを作成する代わりに、別のアプライアンスからダッシュボードをエクスポートし、それを自分のアプライアンスへインポートすることができます。その後でニーズに合わせて、インポートしたダッシュボードを編集することができます。

手順

ステップ 1 **[概要（Overview）] > [ダッシュボード（Dashboards）] > [管理（Management）]**を選択します。

ステップ 2 [ダッシュボードの作成（Create Dashboard）] をクリックします。

ステップ 3 カスタム ダッシュボード オプション （424 ページ）の説明に従って、カスタム ダッシュボード オプションを変更します。

ステップ 4 [保存（Save）] をクリックします。

カスタム ダッシュボード オプション

次の表に、カスタム ダッシュボードを作成または編集するときに使用できるオプションを示します。

表 *28*：カスタム ダッシュボード オプション

オプション	説明
ダッシュボードのコピー（Copy Dashboard）	カスタム ダッシュボードを作成する場合は、ユーザが作成した、またはシステムで事前定義されている既存のダッシュボードをベースとして使用するよう選択できます。このオプションは、ニーズに合わせて変更できる、既存のダッシュボードのコピーを取ります。必要に応じて、[なし（None）] を選択することで、空白の新規ダッシュボードを作成できます。このオプションは、新しいダッシュボードを作成する場合のみ使用可能になります。 マルチドメイン展開では、先祖ドメインのプライベート以外のダッシュボードはコピーできます。
名前	カスタム ダッシュボードの固有名。
説明	カスタム ダッシュボードの簡単な説明。

オプション	説明
タブを変更する間隔（Change Tabs Every）	ダッシュボードがそれぞれのタブを自動変更する頻度（分単位）を指定します。ダッシュボードを一時停止した場合や、ダッシュボードのタブが1つのみの場合を除き、この設定により、指定した間隔で次のタブが表示されます。タブの自動変更を無効にするには、[タブを変更する間隔（Change Tabs Every）] フィールドに 0 を入力します。
ページを更新する間隔（Refresh Page Every）	ダッシュボードのページ全体を自動的に更新する頻度を決定します。 ダッシュボード全体を更新すると、共有のダッシュボードに対して他のユーザが行ったプリファレンスまたはレイアウトの変更や、他のコンピュータ上のプライベートダッシュボードに対して、ダッシュボードが最後に更新された後で自分が行った変更を確認できます。ダッシュボードが常に表示されているネットワーク オペレーション センター（NOC）などでは、頻繁な更新が有効です。ローカル コンピュータでダッシュボードの変更を行なえば、ユーザーが指定する間隔でNOCのダッシュボードが自動的に更新されるため、手動による更新は必要ありません。 この更新によってデータはアップデートされません。データのアップデートを確認するためにダッシュボード全体を更新する必要はありません。個々のウィジェットは設定に従ってアップデートされます。 この値は、[タブを変更する間隔（Change Tabs Every）] の設定より大きい値にする必要があります。ダッシュボードを一時停止しない限り、この設定により、指定した間隔でダッシュボード全体が更新されます。定期的なページ更新を無効にするには、[ページを更新する間隔（Refresh Page Every）] フィールドに 0 を入力します。 （注） この設定は、個々のウィジェットの多くで使用可能なアップデート間隔とは異なります。ダッシュボードのページを更新すると個々のウィジェットのアップデート間隔はリセットされますが、[ページを更新する間隔（Refresh Page Every）]設定を無効にしていても、ウィジェットはそれ自身のプリファレンスに従ってアップデートされます。
プライベートとして保存（Save As Private）	カスタムダッシュボードは、アプライアンスのすべてのユーザが表示および変更可能か、またはユーザアカウントに関連付けて、独自の使用に限り予約可能かを決定します。ロールに関係なく、ダッシュボードへアクセスできるすべてのユーザは、共有ダッシュボードを変更できることに注意してください。特定のダッシュボードを自分のみが変更できるようにするには、そのダッシュボードをプライベートとして保存します。

ウィジェット表示のカスタマイズ

ウィジェットは、タブ上で最小化、最大化、および再配置することができます。

手順

ステップ 1 ダッシュボードを表示します（ダッシュボードの表示 （428 ページ）を参照）。

ステップ 2 次のように、ウィジェット表示をカスタマイズします。

- タブ上でウィジェットを再配置するには、移動するウィジェットのタイトルバーをクリックし、新しい場所へドラッグします。

  （注） 別のタブにウィジェットを移動することはできません。ウィジェットを別のタブに表示する場合は、現在のタブからいったん削除してから新しいタブに追加する必要があります。

- ダッシュボードでウィジェットを最小化または最大化するには、ウィジェットのタイトルバーにある **[最小化（Minimize）]**（−） または **[最大化（Maximize）]**（□） をクリックします。
- ウィジェットをタブ上に表示する必要がなくなった場合にそのウィジェットを削除するには、ウィジェットのタイトルバーにある [閉じる（Close）]（×） をクリックします。

ダッシュボードオプションの編集

手順

ステップ 1 編集するダッシュボードを表示します（ダッシュボードの表示 （428 ページ）を参照）。

ステップ 2 **[編集（Edit）]**（✎） をクリックします。

ステップ 3 カスタムダッシュボードオプション （424 ページ）の説明に従ってオプションを変更します。

ステップ 4 [保存（Save）] をクリックします。

ダッシュボード時刻設定の変更

最短で 1 時間前（デフォルト）から、最長では 1 年前からの期間を反映するように時間範囲を変更できます。時間範囲を変更する場合は、時間によって制約される可能性のあるウィジェットが自動でアップデートされ、新しい時間範囲が反映されます。

グラフ内のデータポイントの最大数は 300 で、時間設定によって、各データポイント内に集計される時間が決まります。以下は、各時間範囲のダッシュボードに表示されるデータポイントの数と対象期間です。

- 1 時間 = 12 データポイント、それぞれ 5 分
- 6 時間 = 72 データポイント、それぞれ 5 分

- 1 日 = 288 データポイント、それぞれ 5 分
- 1 週間 = 300 データポイント、それぞれ 33.6 分
- 2 週間 = 300 データポイント、それぞれ 67.2 分
- 30 日 = 300 データポイント、それぞれ 144 分
- 90 日 = 300 データポイント、それぞれ 432 分
- 180 日 = 300 データポイント、それぞれ 864 分
- 1 年 = 300 データポイント、それぞれ 1,752 分

すべてのウィジェットを時間で制約できるわけではないことに注意してください。たとえば、ダッシュボードの時間範囲は [アプライアンス情報（Appliance Information）] ウィジェットには影響を与えません。このウィジェットは、アプライアンスの名前、モデル、およびソフトウェアの現在のバージョンが含まれている情報を提供します。

企業による Firepower システムの展開では、新しいイベントが古いイベントを置き換える頻度によっては、時間範囲を長期に変更しても、[カスタム分析（Custom Analysis）] ウィジェットなどのウィジェットでは役立たない場合があることに注意してください。

また、ダッシュボードを一時停止することもできます。これにより変更を表示したり、分析を中断したりせずに、ウィジェットで提供されたデータを調べることができます。ダッシュボードを一時停止すると、次のような影響があります。

- Update Every ウィジェットの設定に関係なく、個々のウィジェットでアップデートが停止します。
- ダッシュボードのプロパティの [タブ周期頻度（Cycle Tabs Every）] 設定に関係なく、ダッシュボードのタブの自動変更が停止します。
- ダッシュボードのプロパティの [ページ更新頻度（Refresh Page Every）] 設定に関係なく、ダッシュボードのページの更新が停止します。
- 時間範囲を変更しても影響はありません。

分析が完了したら、ダッシュボードの一時停止を解除できます。ダッシュボードの一時停止を解除すると、ページ上で該当するすべてのウィジェットがアップデートされ、最新の時間範囲が反映されます。また、ダッシュボードのプロパティで指定した設定に従って、ダッシュボード タブの自動変更が再開され、ダッシュボード ページの更新が再開されます。

ダッシュボードに対するシステム情報のフローを中断するような接続の問題、または他の問題が発生した場合、ダッシュボードは自動的に一時停止し、問題が解決するまでエラー通知を表示します。

（注） ダッシュボードが一時停止しているかどうかに関係なく、セッションは通常、非アクティブな状態が1時間（または設定した他の時間）続いた場合、ユーザをログアウトします。ダッシュボードを長期間パッシブにモニタリングする場合は、一部のユーザをセッションタイムアウトしないよう設定したり、システムのタイムアウト設定を変更することを検討してください。

手順

ステップ1 ウィジェットを追加するダッシュボードを表示します。ダッシュボードの表示 （428ページ）を参照してください。

ステップ2 必要に応じて、ダッシュボードの時間範囲を変更するには、[表示経過時間（Show the Last）] ドロップダウンリストから時間範囲を選択します。

ステップ3 必要に応じて、[一時停止（Pause）]（ ） または [再生（Play）]（ ） を使用して、時間範囲コントロールでダッシュボードを一時停止または一時停止解除します。

ダッシュボードの名前変更

手順

ステップ1 変更するダッシュボードを表示します（ダッシュボードの表示 （428 ページ）を参照）。

ステップ2 名前を変更するダッシュボードのタイトルをクリックします。

ステップ3 名前を入力します。

ステップ4 [OK] をクリックします。

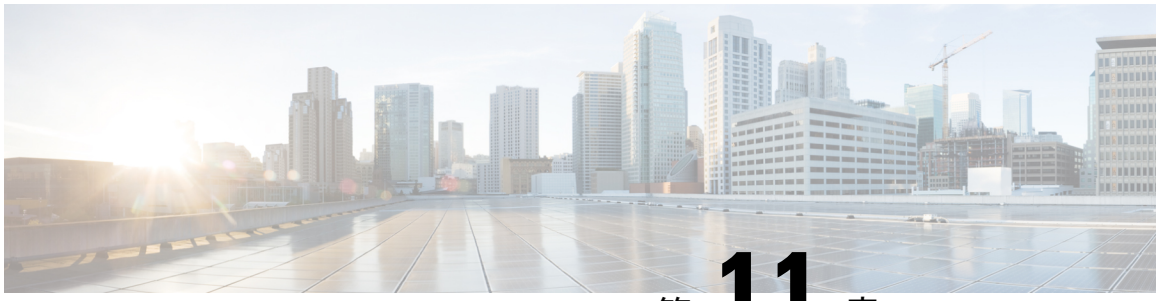
ダッシュボードの表示

デフォルトでは、アプライアンスのホームページにデフォルトのダッシュボードが表示されます。デフォルトのダッシュボードを定義していない場合は、ホーム ページに [ダッシュボードの管理（Dashboard Management）] ページが示され、ここで表示するダッシュボードを選択できます。

手順

いつでも次のいずれかの方法で操作できます。

- アプライアンスのデフォルトダッシュボードを表示するには、**[概要（Overview）]**>**[ダッシュボード（Dashboards）]** を選択します。
- 特定のダッシュボードを表示するには、**[概要（Overview）]** > **[ダッシュボード（Dashboards）]** を選択し、メニューからダッシュボードを選択します。
- 利用可能なすべてのダッシュボードを表示するには、**[概要（Overview）]**>**[ダッシュボード（Dashboards）]**>**[管理（Management）]** を選択します。個々のダッシュボードの横にある [表示（View）]（） を選択すると、そのダッシュボードを表示できます。



第 11 章

ヘルス

次のトピックでは、ヘルスモニタリングを使用する方法について説明します。

ヘルスモニタリングの要件と前提条件

モデルのサポート

任意（Any）

サポートされるドメイン

任意

ユーザの役割

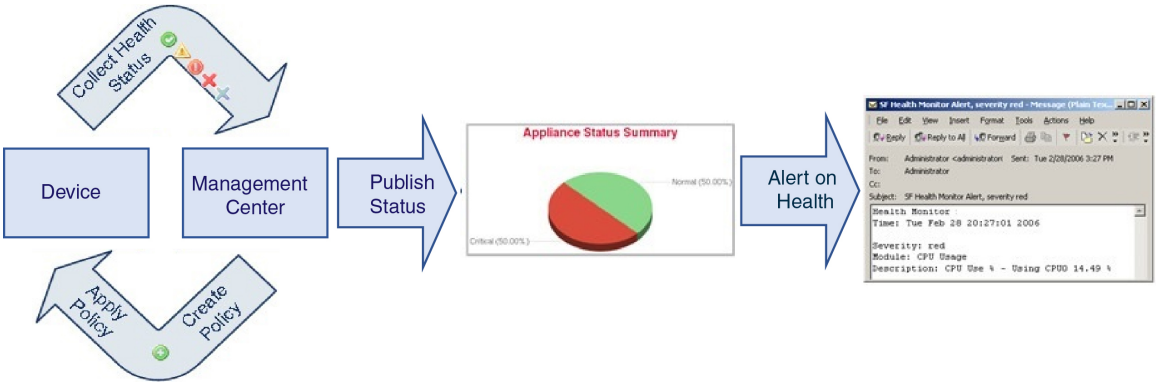
管理者

メンテナンス ユーザー

ヘルス モニタリングについて

Management Center の正常性モニターでは、さまざまな正常性インジケータを追跡して、システムのハードウェアとソフトウェアが正常に動作することを確認します。正常性モニターを使用して、展開全体の重要な機能のステータスを確認できます。

アラート用に正常性モジュールを実行する頻度を設定できます。Management Center は、時系列データ収集もサポートしています。デバイスとその正常性モジュールで時系列データを収集する頻度を設定できます。デフォルトでは、デバイスモニターは、いくつかの事前定義されたヘルス モニター ダッシュボードでこれらのメトリックを報告します。メトリックデータは分析のために収集されるため、アラートは関連付けられません。



ヘルスモニタを使用すれば、正常性ポリシーとも呼ばれるテストのコレクションを作成し、正常性ポリシーを1つ以上のアプライアンスに適用できます。正常性モジュールとも呼ばれるテストは、指定された基準に照らしてテストするスクリプトです。テストを有効または無効にするか、テスト設定を変更することによって、正常性ポリシーを変更したり、不要になった正常性ポリシーを削除したりできます。アプライアンスを除外することによって、選択したアプライアンスからのメッセージを抑制することもできます。

ヘルスモニタリングシステムは、設定された間隔で正常性ポリシーのテストを実行します。すべてのテストを実行することも、オンデマンドで特定のテストを実行することもできます。ヘルス モニターは設定されたテスト条件に基づいてヘルス イベントを収集します。

正常性モジュールには、レガシーベースとテレグラフベースの 2 つのタイプがあります。

レガシーベースの正常性モジュールは、ファン、電源、データベース完全性など、特定のシステムの正常性ステータスをモニターします。これらのモニター対象システムについて正常性ポリシーで指定された条件が満たされると、レガシー インフラストラクチャベースの正常性モジュールは、アラート（緑色、赤色、またはオレンジ色）とショートメッセージを直接生成します。

テレグラフベースの正常性モジュールは、モニター対象システムのメトリック情報を取得するテレグラフプラグインをモニターします。テレグラフベースの正常性モジュールの優先正常性メトリックを使用してカスタムダッシュボードを作成し、特定の統計をモニターしたり、特定の問題をトラブルシューティングすることができます。

（注） すべてのアプライアンスはハードウェアアラームのヘルスモジュール経由でハードウェアのステータスを自動的に報告します。また、Management Center はデフォルトの正常性ポリシーで設定されているモジュールを使用して自動的にステータスを報告します。アプライアンス ハートビートなどの一部の正常性モジュールは、Management Center 上で実行され Management Center の管理対象デバイスのステータスを報告します。正常性モジュールが管理対象デバイスのステータスを提供するには、すべての正常性ポリシーがデバイスに展開されている必要があります。

正常性モニターを使用して、システム全体、特定のアプライアンス、または特定のドメイン（マルチドメイン展開の場合）の正常性ステータス情報にアクセスできます。[正常性モニター（Health Monitor）]ページの六角形のチャートとステータステーブルにより、Management Center を含むネットワーク上のすべてのアプライアンスのステータスに関する視覚的なサマリーが提供されます。個々のアプライアンスのヘルスモニタを使用すれば、特定のアプライアンスのヘルス詳細にドリルダウンできます。

完全にカスタマイズ可能なイベント ビューを使用すれば、ヘルス モニタによって収集されたヘルス ステータス イベントを迅速かつ容易に分析できます。このイベント ビューでは、イベントデータを検索して表示したり、調査中のイベントに関係する他の情報にアクセスしたりできます。たとえば、特定のパーセンテージの CPU 使用率の全記録を表示する場合は、CPU 使用率モジュールを検索して、パーセンテージ値を入力できます。

ヘルス イベントに対応した電子メール、SNMP、または syslog アラートを設定することもできます。ヘルス アラートは、標準アラートとヘルス ステータス レベルを関連付けたものです。たとえば、アプライアンスでハードウェアの過負荷による障害が発生することが絶対にない状態を確保するために、電子メールアラートをセットアップできます。その後で、CPU、ディスク、またはメモリの使用率がそのアプライアンスに適用される正常性ポリシーで設定された警告レベルに達するたびに電子メールアラートがトリガーされる正常性アラートを作成できます。アラートしきい値を、受け取る反復アラートの数が最小になるように設定できます。

（注） ヘルスモニタリングでは、正常性イベントの発生から正常性アラートが生成されるまでに 5 ～ 6 分かかることがあります。

サポートから依頼された場合に、アプライアンスのトラブルシューティング ファイルを作成することもできます。

管理者ユーザーロール特権を持つユーザーのみがシステム正常性データにアクセスできます。

高可用性ペア

バージョン 6.7 以降を実行している Management Center 高可用性展開では、アクティブ Management Center が、REST API を使用して詳細なメトリックベースの情報を表示する正常性モニターページを作成します。スタンバイ Management Center は、アラート情報を表示し、円グラフとステータステーブルを使用して、ネットワーク上のすべてのアプライアンスのステータスに関する視

覚的なサマリーを提供する正常性モニターページを作成します。スタンバイ Management Center は、メトリックベースの情報を表示しません。

ヘルス モジュール

ヘルス モジュールまたはヘルス テストは、正常性ポリシーに指定した条件でテストします。

表 *29*: ヘルスモジュール（すべてのアプライアンス）

モジュール	モジュールのタイプ	説明
CPU Usage (per core)	テレブラフ	このモジュールは、すべてのコアのCPU使用率が過負荷になっていないことを確認し、CPU 使用率がモジュールに設定されたしきい値を超えた場合にアラートを出します。[Warning Threshold %] のデフォルト値は 80 です。[Critical Threshold %] のデフォルト値は 90 です。
ディスク ステータス	レガシー（Legacy）	このモジュールは、ハードディスクと、アプライアンス上のマルウェアストレージパック（設置されている場合）のパフォーマンスを調査します。 このモジュールは、ハードディスクと RAID コントローラ（設置されている場合）で障害が発生する恐れがある場合、または、マルウェア ストレージパックではない追加のハードドライブが設置されている場合に、警告（黄色）ヘルス アラートを生成します。また、設置されているマルウェア ストレージパックを検出できなかった場合はアラート（赤色）ヘルス アラートを生成します。

モジュール	モジュールのタイプ	説明
ディスク使用量	テレブラフ	このモジュールは、アプライアンスのハードドライブとマルウェアストレージパック上のディスク使用率をモジュールに設定された制限と比較し、その使用率がモジュールに設定されたしきい値を超えた時点でアラートを出します。また、モジュールしきい値に基づいて、システムが監視対象のディスク使用カテゴリ内のファイルを過剰に削除する場合、または、これらのカテゴリを除くディスク使用率が過剰なレベルに達した場合にもアラートを出します。ディスク使用率アラートのトラブルシューティング シナリオについては、ディスク使用率とイベントドレインの正常性モニターアラート （532 ページ）を参照してください。 デバイス設定履歴ファイルのサイズが許容制限サイズを超えると、[ディスク使用量（Disk Usage）] モジュールから正常性アラートが送信されます。ディスク使用率アラートのトラブルシューティング シナリオについては、「デバイス設定履歴ファイルのディスク使用量 を参照してください。この正常性アラートは、 Secure Firewall Management Center のバージョン 7.2.0 ～ 7.2.5、7.3.x、および 7.4.0 ではサポートされていません。 ディスク使用率ヘルス ステータス モジュールは、アプライアンス上の `/` パーティションと `/volume` パーティションのディスク使用率を監視して、ドレイン頻度を追跡するために使用します。ディスク使用率モジュールは `/boot` パーティションを監視対象パーティションとして列挙しますが、そのパーティションのサイズが固定のため、このモジュールはブート パーティションに基づいてアラートを出すことはしません。
ファイルシステムの整合性チェック	レガシー（Legacy）	このモジュールは、システムでCCモードまたはUCAPLモードが有効になっている場合、またはシステムがDEVキーで署名されたイメージを実行している場合に、ファイルシステムの整合性チェックを実行します。このモジュールはデフォルトでは有効になっています。
ヘルス モニター プロセス	レガシー（Legacy）	このモジュールは、ヘルス モニター自体のステータスを監視し、Management Center で受信された最後のステータス イベント以降の分数が警告制限または重大制限を超えた場合にアラートを出します。

モジュール	モジュールのタイプ	説明
Interface Statistics	レガシー（Legacy）	このモジュールは、デバイスが現在トラフィックを収集しているかどうかを確認して、物理インターフェイスおよび集約インターフェイスのトラフィック ステータスに基づいてアラートを出します。物理インターフェイスの情報には、インターフェイス名、リンク ステート、および帯域幅が含まれます。集約インターフェイスの情報には、インターフェイス名、アクティブ リンクの数、および総集約帯域幅が含まれます。 （注） このモジュールは、高可用性スタンバイデバイスのトラフィックフローも監視します。スタンバイデバイスがトラフィックを受信していないことがわかっていても、Management Center はインターフェイスがトラフィックを受信していないことを警告します。ポートチャネルの一部のサブインターフェイスでトラフィックが受信されない場合も、同じアラートの原則が適用されます。 **show interface** CLI コマンドを使用してデバイスのインターフェイス統計を確認する場合、CLI コマンドの結果の入出力レートは、このインターフェイスモジュールに表示されるトラフィックレートと異なる場合があります。 このモジュールは、Snort パフォーマンスモニタリングからの値に従ってトラフィックレートを表示します。Snort パフォーマンスモニタリングと Management Center インターフェイス統計のサンプリング間隔は異なります。サンプリング間隔の違いにより、Management Center GUI のスループット値が Threat Defense CLI の結果に表示されるスループット値と異なる場合があります。
ローカル マルウェア分析	レガシー（Legacy）	このモジュールはローカルマルウェア分析の ClamAV 更新をモニターします。

モジュール	モジュールのタイプ	説明
メモリ使用率	レガシー（Legacy）	このモジュールは、アプライアンス上のメモリ使用率をモジュールに設定された制限と比較し、使用率がモジュールに設定されたレベルを超えるとアラートを出します。 メモリ使用率を計算する場合、Management Center メモリ使用率正常性モジュールは、RAM、スワップメモリ、キャッシュメモリの使用率をモニタリングし、計算に含めます。 メモリが 4 GB を超えるアプライアンスの場合、プリセットされたアラートしきい値は、システム問題を引き起こす可能性のあるメモリ空き容量の割合を求める式に基づいています。4 GB を超えるのアプライアンスでは、警告しきい値と重大しきい値の時間間隔が非常に狭いため、[警告しきい値 %（Warning Threshold %）] の値を手動で 50 に設定することを推奨します。これにより、時間内にアプライアンスのメモリ アラートを受け取って問題を解決できる可能性がさらに高まります。しきい値の計算方法の詳細については、ヘルスモニターアラートのメモリ使用率しきい値 （530 ページ）を参照してください。 バージョン 6.6.0 以降では、バージョン 6.6.0 以降への Management Center Virtual のアップグレードに必要な最小 RAM 容量は 28 GB であり、Management Center Virtual の展開に推奨される RAM 容量は 32 GB です。デフォルト設定（ほとんどの Management Center Virtual インスタンスでは 32 GB、Management Center Virtual 300 では 64 GB の RAM）の値は小さくしないことをお勧めします。 **注目** • Management Center Virtual 展開に割り当てられた RAM が不十分である場合、ヘルスモニターによってクリティカルアラートが生成されます。 • Management Center がクリティカルシステムメモリ状態に達すると、システムは、メモリ使用量の多いプロセスを終了したり、高いメモリ使用率が続く場合には Management Center を再起動する可能性があります。 複雑なアクセス コントロール ポリシーやルールは、重要なリソースを消費し、パフォーマンスに悪影響を与える可能性があります。
Process Status	レガシー（Legacy）	このモジュールは、アプライアンス上のプロセスがプロセス マネージャの外部で停止または終了したかを確認します。 プロセスが故意にプロセス マネージャの外部で停止された場合は、モジュールが再開してプロセスが再起動するまで、モジュール ステータスが Warning に変更され、ヘルス イベント メッセージが停止されたプロセスを示します。プロセスがプロセス マネージャの外部で異常終了またはクラッシュした場合は、モジュールが再開してプロセスが再起動するまで、モジュール ステータスが Critical に変更され、ヘルス イベント メッセージが終了したプロセスを示します。

モジュール	モジュールのタイプ	説明
デバイスでの脅威データの更新	レガシー（Legacy）	

モジュール	モジュールのタイプ	説明
		デバイスが脅威の検出に使用する特定のインテリジェンスデータと設定は、Management Center 上で 30 分ごとにクラウドから更新されます。 このモジュールは、指定した期間内にデバイスでこの情報が更新されない場合にアラートを生成します。 モニターされる更新には次の点が含まれます。 • ローカル URL カテゴリおよびレピュテーション データ • セキュリティ インテリジェンス URL リストおよびフィード（Threat Intelligence Director からのグローバルブロックリストとブロックしないリストおよび URLを含む） • セキュリティ インテリジェンス ネットワーク リストおよびフィード（IP アドレス）（Threat Intelligence Director からのグローバルブロックリストとブロックしないリストおよび IP アドレスを含む） • セキュリティ インテリジェンス DNS リストおよびフィード（Threat Intelligence Director からのグローバルブロックリストとブロックしないリストおよびドメインを含む） • （ClamAV からの）ローカル マルウェア分析の署名 • Threat Intelligence Director からの SHA リスト（[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [セキュリティ インテリジェンス（Security Intelligence）] > [ネットワーク リストおよびフィード（Network Lists and Feeds）] ページにリストされている） • [統合（Integration）] > [AMP] > [動的分析接続（Dynamic Analysis Connections）] ページで設定された動的分析の設定 • キャッシュされた URL の期限切れに関連する [脅威設定（Threat Configuration）] の設定（**[統合（Integration）] > [その他の統合（Other Integrations）] > [クラウドサービス（Cloud Services）]** ページの [キャッシュされた URL の期限切れ（Cached URLs Expire）] の設定を含む）（このモジュールでは、URL キャッシュの更新はモニターされません。） • イベントを送信するためのシスコ クラウドとの通信の問題。**[統合（Integration）] > [その他の統合（Other Integrations）]** > [クラウドサービス（Cloud Services）] ページの [シスコクラウド（Cisco Cloud）] ボックスを確認します。 （注） システムに Threat Intelligence Director が設定されており、フィードがある場合にのみ、TID の更新が含まれます。 デフォルトでは、このモジュールは 1 時間後に警告を送信し、24 時間後に重大なアラートを送信します。

モジュール	モジュールのタイプ	説明
		Management Center またはいずれかのデバイスで障害が発生していることをこのモジュールが示している場合、Management Center がデバイスに到達できることを確認します。

表 *30 : Management Center* ヘルスモジュール

モジュール	モジュールのタイプ	説明
AMP for Endpoint のステータス	レガシー（Legacy）	このモジュールは、Management Center が初期接続の成功後に AMP クラウドまたは Cisco AMP Private Cloud に接続できない場合、またはプライベート クラウドがパブリック AMP クラウドに接続できない場合にアラートを出します。また、Secure Endpoint 管理コンソールを使用して AMP クラウド接続の登録が解除された場合にもアラートを出します。
AMP for Firepower のステータス	レガシー（Legacy）	このモジュールは、以下の場合にアラートを出します。 • Management Center が AMP クラウド（パブリックまたはプライベート）、Secure Malware Analytics クラウドまたはアプライアンスに接続できないか、または AMP プライベートクラウドがパブリック AMP クラウドに接続できない。 • 接続に使用する暗号化キーが無効である。 • デバイスが Secure Malware Analytics クラウドまたは Secure Malware Analytics アプライアンスに接続して動的分析用のファイルを送信できない。 • ファイル ポリシー設定に基づいてネットワーク トラフィックで過剰な数のファイルが検出された。 Management Center のインターネット接続が切断された場合、ヘルスアラートの生成に最大 30 分かかることがあります。
アプライアンス ハートビート	レガシー（Legacy）	このモジュールは、アプライアンス ハートビートがアプライアンスから届いているかどうかを確認し、アプライアンスのハートビート ステータスに基づいてアラートを出します。
データベースサイズ	レガシー（Legacy）	このモジュールは、設定データベースのサイズを確認し、サイズが、モジュールに設定されている値（ギガバイト単位）を超えた場合にアラートを出します。
ディスカバリホスト制限	レガシー（Legacy）	このモジュールは、Management Center がモニターできるホスト数が制限に近づいているかどうかを確認し、モジュールに設定された警告レベルに基づいてアラートを出します。詳細については、ホスト制限（Host Limit）を参照してください。

モジュール	モジュールのタイプ	説明
イベント バックログ ステータス	レガシー（Legacy）	このモジュールは、デバイスから Management Center に送信されるのを待機しているイベントデータのバックログのサイズが、30 分を超えて増大し続けた場合にアラートを発します。 バックログを減らすには、帯域幅を評価し、ログに記録するイベント数を減らすことを検討してください。
Event Monitor	テレブラフ	このモジュールは、Management Center への全体の着信イベントレートをモニターします。
イベント ストリーム ステータス	レガシー（Legacy）	このモジュールは、Management Center の Event Streamer を使用するサードパーティ製クライアント アプリケーションへの接続を管理します。
ハードウェア統計情報	テレブラフ	このモジュールは、Management Center ハードウェアエンティティのステータス、つまりファン速度、温度、電源を監視します。このモジュールは、設定された警告またはクリティカルな制限がしきい値を超えるとアラートを出します。
ISE 接続のモニター	レガシー（Legacy）	このモジュールは、Cisco Identity Services Engine（ISE）と Management Center 間のサーバー接続のステータスをモニターします。ISE は、追加のユーザーデータ、デバイスタイプデータ、デバイスロケーションデータ、SGT（セキュリティグループタグ）、および SXP（Security Exchange Protocol）サービスを提供します。
ライセンス モニター	レガシー（Legacy）	このモジュールはライセンスの有効期限をモニターします。
Management Center HA ステータス	レガシー（Legacy）	このモジュールは、Management Center ハイ アベイラビリティ ステータスについて、モニタし、アラートを出します。Management Center のハイ アベイラビリティを確立していない場合、HA ステータスは、「HA でない（Not in HA）」になります。 （注） このモジュールは、以前は Management Center の高可用性ステータスを提供していた高可用性ステータスモジュールに代わるものです。バージョン 7.0 では、管理対象デバイスの高可用性ステータスが追加されました。
MySQL 統計情報	テレブラフ	このモジュールは、データベースサイズ、アクティブな接続数、メモリ使用量など、MySQL データベースのステータスをモニターします。デフォルトでは、ディセーブルです。
RabbitMQ ステータス	テレブラフ	このモジュールは、RabbitMQ のさまざまな統計を収集します。

モジュール	モジュールのタイプ	説明
RRD サーバー プロセス	レガシー（Legacy）	このモジュールは、時系列データを格納するラウンドロビンサーバーが正常に機能しているかどうかを確認します。このモジュールは、RRDサーバーが前回の更新以降に再起動した場合にアラートを出します。また、RRDサーバーの再起動を伴う連続更新回数がモジュール設定で指定された数値に達した場合に[重大（Critical）] または [警告（Warning）] ステータスに遷移します。
レルム	レガシー（Legacy）	レルムまたはユーザーの不一致の次の警告しきい値を設定できます。 • ユーザーの不一致：ユーザーは、ダウンロードされることなく Management Center に報告されます。 ユーザーの不一致の一般的な理由は、ユーザーが Management Center へのダウンロードから除外されたグループに属していることです。Review the information discussed in Cisco Secure Firewall Management Center デバイス構成ガイド. • レルムの不一致：ユーザーが、Management Center に認識されていないレルムに対応するドメインにログインした場合に不一致が起きます。 詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。 このモジュールは、レルムごとにサポートされているダウンロードユーザーの最大数よりも多くのユーザーをダウンロードしようとすると、正常性アラートも表示します。単一のレルムのダウンロードユーザーの最大数は、管理センターのモデルによって異なります。 詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドのユーザー制限を参照してください。
セキュリティ インテリジェンス（Security Intelligence）	レガシー（Legacy）	このモジュールは、セキュリティインテリジェンスが使用中であり、Management Center がフィードを更新できないか、フィード データが破損している、またはフィードデータに認識可能な IP アドレスが含まれていない場合にアラートを発します。 Threat Data Updates on Devices モジュールも参照してください。

モジュール	モジュールのタイプ	説明
スマート ライセンス モニター	レガシー（Legacy）	このモジュールはスマートライセンスのステータスをモニタリングし、以下の場合にアラートを送信します。 • Smart Licensing Agent（スマートエージェント）と Smart Software Manager (SSM) の間の通信にエラーがある。 • 製品インスタンス登録トークンの有効期限が切れている。 • スマート ライセンスの使用状況がコンプライアンスに違反している。 • スマート ライセンスの権限モードまたは評価モードの有効期限が切れている。
Sybase 統計情報	テレブラフ	このモジュールは、データベースサイズ、アクティブな接続数、メモリ使用量など、Management Center 上の Sybase データベースのステータスをモニターします。
時系列データ（RRD）モニター	レガシー（Legacy）	このモジュールは、時系列データ（相関イベントカウントなど）が保存されるディレクトリ内の破損ファイルの存在を追跡して、ファイルが破損としてフラグが付けられ、削除された段階でアラートを出します。
タイムサーバーステータス	レガシー（Legacy）	このモジュールはNTPサーバーの設定をモニターし、NTPサーバーが使用できない場合、またはNTP サーバーの設定が無効な場合にアラートを出します。 このモジュールから重大なアラートを受信した場合は、**システム**（⚙） **[設定（Configuration）]** > **[時刻の同期（Time Synchronization ）]** を選択し、アラートで指定されている NTP サーバーの設定を確認します。
時刻同期ステータス	レガシー（Legacy）	このモジュールは、NTP を使用して時刻を取得するデバイス クロックと NTP サーバー上のクロックの同期を追跡して、クロックの差が10秒を超えた場合にアラートを出します。
未解決グループモニター	レガシー（Legacy）	ポリシーで使用される未解決グループをモニターします。
URL フィルタリング モニター	レガシー（Legacy）	このモジュールは、Management Centerが次のことに失敗した場合にアラートを出します。 • シスコクラウドへの登録 • シスコクラウドからの URL 脅威データの更新のダウンロード • URL ルックアップの実行 これらのアラートの時間しきい値を設定できます。 Threat Data Updates on Devices モジュールも参照してください。

表 *31* : デバイスヘルスモジュール

モジュール	モジュールのタイプ	説明
AMP 接続ステータス	テレブラフ	このモジュールは、Threat Defense が初期接続の成功後に AMP クラウドまたは Cisco AMP Private Cloud に接続できない場合、またはプライベート クラウドがパブリック AMP クラウドに接続できない場合にアラートを出します。デフォルトでは、ディセーブルです。
AMP Threat Grid の接続	テレブラフ	このモジュールは、Threat Defense が AMP Threat Grid クラウドに最初は正常に接続でき、その後接続できなくなった場合にアラートを出します。
ASP ドロップ	テレブラフ	このモジュールは、データプレーンの高速セキュリティパスによってドロップされた接続をモニターします。
自動アプリケーションバイパス	レガシー（Legacy）	このモジュールは、バイパスされた検出アプリケーションをモニターします。
シャーシ環境ステータス	レガシー（Legacy）	このモジュールは、ファン速度やシャーシ温度などのシャーシパラメータをモニターします。また、温度の警告しきい値とクリティカルしきい値を設定できます。クリティカルシャーシ温度（摂氏）のデフォルト値は85です。警告シャーシ温度（摂氏）のデフォルト値は 75 です。
クラスタ/HA障害ステータス	レガシー（Legacy）	このモジュールは、デバイス クラスタのステータスをモニターします。このモジュールは、以下の場合にアラートを出します。 • クラスタに新しいプライマリ ユニットが選択される。 • 新しいセカンダリ ユニットがクラスタに参加する。 • プライマリまたはセカンダリ ユニットがクラスタから離脱する。

モジュール	モジュールのタイプ	説明
設定のリソース使用率	レガシー（Legacy）	このモジュールは、展開された設定のサイズに基づき、デバイスがメモリ不足になるリスクがある場合にアラートを出します。 アラートには、設定に必要なメモリ量と、使用可能なメモリ量を超過した量が示されます。アラートが出た場合は、設定を再評価してください。ほとんどの場合、アクセス制御ルールまたは侵入ポリシーの数または複雑さを軽減できます。 [Snort Memory Allocation] • [Total Snort Memory] は、Threat Defense デバイスで実行されている Snort 2 インスタンスに割り当てられたメモリを示します。 • [Available Memory] は、システムによって Snort 2 インスタンスに割り当てられたメモリを示します。この値は、合計 Snort メモリと他のモジュール用に予約された合計メモリとの単なる差ではないことに注意してください。この値は、他のいくつかの計算の後に導出され、Snort 2 プロセスの数で除算されます。 [Available Memory] の値が負の場合、展開された設定に対して Snort 2 インスタンスに十分なメモリがないことを示します。サポートについては、Cisco Technical Assistance Center （TAC）にお問い合わせください。
接続統計情報	テレブラフ	このモジュールは、接続の統計情報と NAT 変換カウントをモニターします。
データプレーン CPU 使用率	テレブラフ	このモジュールは、デバイス上のすべてのデータプレーンプロセッサの平均 CPU 使用率が過負荷になっていないことを確認し、CPU 使用率がモジュールに設定されたパーセンテージを超えた場合にアラートを出します。[Warning Threshold %] のデフォルト値は 80 です。[Critical Threshold %] のデフォルト値は 90 です。
Snort の CPU 使用率	テレブラフ	このモジュールは、デバイス上の Snort プロセスの平均 CPU 使用率が過負荷になっていないことを確認し、CPU 使用率がモジュールに設定されたパーセンテージを超えた場合にアラートを出します。[Warning Threshold %] のデフォルト値は 80 です。[Critical Threshold %] のデフォルト値は 90 です。
システム CPU 使用率	テレブラフ	このモジュールは、デバイス上のすべてのシステムプロセスの平均CPU使用率が過負荷になっていないことを確認し、CPU 使用率がモジュールに設定されたパーセンテージを超えた場合にアラートを出します。[Warning Threshold %] のデフォルト値は 80 です。[Critical Threshold %] のデフォルト値は 90 です。
Critical Process Statistics	テレブラフ	このモジュールは、クリティカルプロセスの状態、リソース消費量、再起動回数をモニターします。
Deployed Configuration Statistics	テレブラフ	このモジュールは、展開された設定に関する統計情報（ACE の数や IPS ルールの数など）をモニターします。

モジュール	モジュールのタイプ	説明
Firewall Threat Defense のプラットフォームの障害	レガシー（Legacy）	このモジュールは、Firepower 1000、2100、Secure Firewall3100、4200 デバイスのプラットフォーム障害に関するアラートを生成します。障害は、Management Center によって管理される可変オブジェクトです。障害は、Threat Defense インスタンスの障害や、発生したしきい値のアラームを表します。障害のライフサイクルの間に、障害の状態または重大度が変化する場合があります。 各障害には、障害の発生時に影響を受けたオブジェクトの動作状態に関する情報が含まれます。障害の状態が移行して解決すると、そのオブジェクトは機能状態に移行します。 詳細については、『*Cisco Firepower 1000/2100 FXOS Faults and Error Messages Guide*』を参照してください。
Management Center アクセス設定の変更	レガシー（Legacy）	このモジュールは、configure network management-data-interface コマンドを直接使用して Management Center で行われたアクセス設定の変更をモニターします。
フローオフロード統計情報	テレブラフ	このモジュールは、管理対象デバイスのハードウェア フローオフロード統計情報をモニターします。
ハードウェア アラーム	レガシー（Legacy）	このモジュールは、物理管理対象デバイス上のハードウェアを交換する必要があるかどうかを確認し、ハードウェア ステータスに基づいてアラートを出します。このモジュールは、ハードウェア関連デーモンのステータスについても報告します。
インライン リンク不一致アラーム	レガシー（Legacy）	このモジュールは、インライン セットに関連付けられたポートを監視し、インライン ペアの 2 つのインターフェイスが別々の速度をネゴシエートした場合にアラートを出します。

モジュール	モジュールのタイプ	説明
侵入およびファイル イベント レート	レガシー（Legacy）	このモジュールは、1 秒あたりの侵入イベント数をこのモジュールに設定された制限と比較し、制限を超えた場合にアラートを出します。侵入およびファイル イベント レートが 0 の場合は、侵入プロセスがダウンしているか、管理対象デバイスがイベントを送信していない可能性があります。イベントがデバイスから送られているかどうかをチェックするには、**[分析（Analysis）] > [侵入（Intrusions）] > [イベント（Events）]** の順に選択します。 一般に、ネットワーク セグメントのイベント レートは平均で 1 秒あたり 20 イベントです。この平均レートのネットワーク セグメントでは、[1 秒あたりのイベント（重大）（Events per second (Critical)）] を 50 に設定し、[1 秒あたりのイベント（警告）（Events per second (Warning)）] を 30 に設定する必要があります。システムの制限を決定するには、デバイスの [統計情報（Statistics）] ページ（**システム**（⚙）**> [モニタリング（Monitoring）] > [統計（Statistics）]**）で [イベント/秒（Events/Sec）] 値を探してから、次の式を使用して制限を計算します。 • 1 秒あたりのイベント（重大）= イベント/秒 * 2.5 • イベント数/秒（警告）（Events per second (Warning)）= イベント数/秒（Events/Sec）* 1.5 両方の制限に設定可能な最大イベント数は 999 であり、重大制限は警告制限より大きくする必要があります。
リンク ステート伝達	レガシー（Legacy）	ISA 3000 のみ。 このモジュールは、ペア化されたインライン セット内のリンクで障害が発生した時点を特定して、リンク ステート伝達モードをトリガーとして使用します。リンク ステートがペアに伝達した場合は、そのモジュールのステータス分類が [重大（Critical）] に変更され、状態が次のように表示されます。 `Module Link State Propagation: ethx_ethy is Triggered` ここで、x と y はペア化されたインターフェイス番号です。
Memory Usage Data Plane	テレブラフ	このモジュールは、割り当て済みメモリのデータプレーンプロセスが占める割合を確認し、メモリ使用率がモジュールに設定されたパーセンテージを超えた場合にアラートを出します。[Warning Threshold %] のデフォルト値は 80 です。[Critical Threshold %] のデフォルト値は 90 です。
Memory Usage Snort	テレブラフ	このモジュールは、割り当て済みメモリの Snort プロセスが占める割合を確認し、メモリ使用率がモジュールに設定されたパーセンテージを超えた場合にアラートを出します。[Warning Threshold %] のデフォルト値は 80 です。[Critical Threshold %] のデフォルト値は 90 です。

モジュール	モジュールのタイプ	説明
ネットワークカードのリセット	レガシー（Legacy）	このモジュールは、リセット時に、ハードウェア障害原因で再起動されたネットワーク カードをチェックし、アラートを出します。
NTP 統計情報	テレブラフ	このモジュールは、管理対象デバイスの NTP クロック同期ステータスをモニターします。デフォルトでは、ディセーブルです。
電源モジュール	レガシー（Legacy）	このモジュールは、アプライアンスの電源が交換が必要かどうかを確認し、電源ステータスに基づいてアラートを出します。
ルーティング統計情報	テレブラフ	このモジュールは、ルーティングテーブルの現在の状態をモニターします。
Snort3 統計情報	テレブラフ	このモジュールは、イベント、フロー、およびパケットの Snort 3 統計情報をモニターします。
Snort アイデンティティ メモリ使用率	レガシー（Legacy）	Snort アイデンティティ処理の警告しきい値の設定を可能にするとともに、メモリ使用率がモジュールに設定されたレベルを超えるとアラートを生成します。[クリティカルしきい値（%）（Critical Threshold %）] のデフォルト値は 80 です。 このヘルスモジュールは、Snort のユーザーアイデンティティ情報に使用される合計領域を具体的に追跡します。現在のメモリ使用量の詳細、ユーザー/IP バインディングの合計数、およびユーザーグループマッピングの詳細が表示されます。Snort はこれらの詳細をファイルに記録します。メモリ使用率ファイルが使用できない場合は、このモジュールのヘルスアラートに「Waiting for data」と表示されます。これは、新しいインストールまたはメジャーアップデート、Snort 2 から Snort 3 の切り替え、またはその逆への切り替え、あるいはメジャーポリシーの展開によって、Snort の再起動中に発生する可能性があります。ヘルスモニタリングサイクルに応じ、かつ、ファイルが使用可能になると、警告が消え、ヘルスモニターにこのモジュールの詳細が表示され、そのステータスはグリーンになります。
Snort 再設定検出	テレブラフ	このモジュールは、デバイスの再設定が失敗した場合、アラートを出します。このモジュールは、Snort 2 と Snort 3 の両方のインスタンスの再設定失敗を検出します。
Snort Statistics	テレブラフ	このモジュールは、イベント、フロー、およびパケットの Snort 統計情報をモニターします。
Security Services Exchange の接続ステータス	テレブラフ	このモジュールは、Threat Defense が Security Services Exchange クラウドに最初は正常に接続でき、その後接続できなくなった場合にアラートを出します。デフォルトでは、ディセーブルです。

モジュール	モジュールのタイプ	説明
Threat Defense HA（スプリットブレインチェック）	レガシー（Legacy）	このモジュールは、Threat Defense の高可用性ステータスをモニターして、アラートを出し、スプリットブレーンのシナリオに対する正常性アラートを提供します。Threat Defense のハイ アベイラビリティを確立していない場合、HA ステータスは、「HA でない（Not in HA）」になります。
VPN 統計情報	テレブラフ	このモジュールは、Threat Defense デバイス間のサイト間およびリモートアクセス VPN トンネルをモニタリングします。
XTLS カウンタ	テレブラフ	このモジュールは、XTLS/SSL フロー、メモリ、およびキャッシュの有効性をモニターします。デフォルトでは、ディセーブルです。

ヘルス モニタリングの設定

手順

ステップ 1 ヘルス モジュール（434 ページ）で説明されているように、モニターするヘルス モジュールを決定します。

アプライアンスの種類ごとに固有のポリシーをセットアップして、そのアプライアンスに適切なテストだけを有効にすることができます。

ヒント モニタリング動作をカスタマイズすることなくすぐにヘルス モニタリングを有効にするには、そのために用意されたデフォルト ポリシーを適用できます。

ステップ 2 正常性ポリシーの作成（450 ページ）で説明されているように、ヘルス ステータスを追跡するアプライアンスごとに正常性ポリシーを適用します。

ステップ 3 （オプション）ヘルス モニター アラートの作成（465 ページ）で説明されているように、ヘルス モニタ アラートを設定します。

ヘルス ステータス レベルが特定のヘルス モジュールの特定の重大度レベルに達した段階でトリガーされる電子メール、Syslog、または SNMP アラートをセットアップできます。

正常性ポリシー

正常性ポリシーには、複数のモジュールに対して設定可能な正常性テスト基準が含まれます。アプライアンスごとにどのヘルス モジュールを実行するかを制御したり、モジュールごとに実行するテストで使用される特定の制限を設定したりできます。

正常性ポリシーを設定するときに、そのポリシーに対して各ヘルスモジュールを有効にするかどうかを決定します。また、有効にした各モジュールが、プロセスの正常性を評価するたびに報告するヘルス ステータスを制御するための基準を選択することもできます。

システム内のすべてのアプライアンスに適用可能な1つの正常性ポリシーを作成することも、適用を計画している特定のアプライアンス用に正常性ポリシーをカスタマイズすることも、付属のデフォルト正常性ポリシーを使用することもできます。

（注） アプライアンスを登録すると、Management Center によってデフォルトの正常性ポリシーが自動的に割り当てられます。正常性ポリシーとアプライアンスの関連付けを解除するには、まず、別の正常性ポリシーをアプライアンスに関連付ける必要があります。アプライアンスには、少なくとも 1 つの正常性ポリシーが割り当てられている必要があります。

デフォルトの正常性ポリシー

Management Center セットアッププロセスは、使用可能な正常性モジュールのほとんど（すべてではない）が有効になっている初期正常性ポリシーを作成して適用します。システムは、Management Center に追加されたデバイスにもこの初期ポリシーを適用します。

この初期の正常性ポリシーは、デフォルトの正常性ポリシーに基づいています。デフォルトの正常性ポリシーは、表示も編集もできませんが、カスタム正常性ポリシーを作成するときにコピーできます。

アップグレードとデフォルトの正常性ポリシー

Management Center をアップグレードすると、新しい正常性モジュールがすべての正常性ポリシーに追加されます。これには、初期の正常性ポリシー、デフォルトの正常性ポリシー、およびその他のカスタム正常性ポリシーが含まれます。通常、新しい正常性モジュールは有効な状態で追加されます。

（注） 新しい正常性モジュールでモニタリングとアラートを開始するには、アップグレード後に正常性ポリシーを再適用します。

正常性ポリシーの作成

アプライアンスで使用する正常性ポリシーをカスタマイズすることによって、新しいポリシーを作成できます。ポリシー内の設定は、最初に、新しいポリシーの基準として選択した正常性ポリシー内の設定を使用して生成されます。ポリシーを編集して、ポリシー内のモジュールの有効化または無効化などの設定を指定したり、必要に応じて各モジュールのアラート基準を変更したり、実行時間間隔を指定したりできます。

手順

ステップ 1 システム（⚙） > **[正常性（Health）]** > **[ポリシー（Policy）]**を選択します。

ステップ 2 [ポリシーの作成（Create Policy）] をクリックします。

ステップ 3 ポリシーの名前を入力します。

ステップ 4 [ベースポリシー（Base Policy）] ドロップダウンリストから、新しいポリシーの基準として使用する既存のポリシーを選択します。

ステップ 5 ポリシーの説明を入力します。

ステップ 6 **[保存（Save）]** を選択します。

次のタスク

- 正常性ポリシーの適用 （451ページ）で説明されているように、デバイスにヘルスポリシーを適用します。
- 正常性ポリシーの編集 （452ページ）で説明されているように、ポリシーを編集して、モジュールレベルのポリシー設定を指定します。

正常性ポリシーの適用

正常性ポリシーをアプライアンスに適用すると、ポリシー内で有効にしたすべてのモジュールのヘルステストが、アプライアンス上のプロセスとハードウェアの正常性を自動的に監視します。その後、ヘルステストは、ポリシー内で設定された時間間隔で実行を続け、アプライアンスのヘルス データを収集し、そのデータをManagement Centerに転送します。

正常性ポリシーでモジュールを有効にしてから、ヘルステストが必要ないアプライアンスにポリシーを適用した場合、ヘルス モニタはそのヘルス モジュールのステータスを無効として報告します。

すべてのモジュールが無効になっているポリシーをアプライアンスに適用すると、適用されたすべての正常性ポリシーがアプライアンスから削除されるため、どの正常性ポリシーも適用されません。ただし、アプライアンスには少なくとも1つの正常性ポリシーが割り当てられている必要があります。

すでにポリシーが適用されているアプライアンスに別のポリシーを適用した場合は、新しく適用されたテストに基づく新しいデータの表示が少し遅れる可能性があります。

手順

ステップ 1 システム（⚙） > **[正常性（Health）]** > **[ポリシー（Policy）]**を選択します。

ステップ 2 適用するポリシーの横にある [正常性ポリシーの展開（Deploy health policy）]（📥） をクリックします。

ステップ 3 正常性ポリシーを適用するアプライアンスを選択します。

（注） アプライアンスには、少なくとも 1 つの正常性ポリシーが割り当てられている必要があります。アプライアンスのヘルスモニタリングを停止するには、すべてのモジュールが無効になっている正常性ポリシーを作成し、それをアプライアンスに適用します。正常性ポリシーとアプライアンスの関連付けを解除するには、まず別の正常性ポリシーをアプライアンスに関連付ける必要があります。

ステップ 4 [適用（Apply）] をクリックして、選択したアプライアンスにポリシーを適用します。

次のタスク

- 必要に応じて、タスクのステータスをモニタします（タスクメッセージの表示（529 ページ） を参照）。

  アプライアンスのモニタリングは、ポリシーが正常に適用されると開始されます。

正常性ポリシーの編集

変更する正常性ポリシーを編集できます。

手順

ステップ 1 **システム**（⚙）> **[正常性（Health）]** > **[ポリシー（Policy）]**を選択します。

ステップ 2 変更するポリシーの横にある **[編集（Edit）]**（✎） をクリックします。

ステップ 3 ポリシー名とその説明を編集するには、ポリシー名に対して表示される **[編集（Edit）]**（✎）アイコンをクリックします。

ステップ 4 [ヘルスモジュール（Health Modules）] タブには、すべてのデバイスモジュールとその属性が表示されます。次のアクションを使用して、正常性モジュールを設定します。

- モジュールとその属性に対して表示されるトグルボタンをクリックします。オン（  ）またはオフ（  ）にして、それぞれヘルスステータスのテストを有効または無効にします。
- 正常性モジュールで一括有効化または無効化テストを実行するには、[すべて選択（Select All）] トグルボタンをクリックします。

（注）
- モジュールと属性には、サポートしているアプライアンス（Threat Defense 、Management Center、またはその両方）でフラグが付けられます。
- CPU およびメモリモジュールの個々の属性を含めるか除外するかを選択することはできません。

モジュールについては、ヘルス モジュール （434 ページ）を参照してください。

ステップ 5 該当する場合は、[重大（Critical）] および [警告（Warning）] しきい値のパーセンテージを設定します。

ステップ 6 **[設定（Settings）]** タブで、フィールドに関連する値を入力します。

- **[ヘルスモジュールの実行間隔（Health Module Run Time Interval）]**：ヘルスモジュールを実行する頻度。最小の間隔は 5 分です。
- [メトリック収集間隔（Metric Collection Interval）]：デバイスとそのヘルスモジュールで時系列データを収集する頻度。デフォルトでは、デバイスモニターは、いくつかの事前定義されたヘルスモニターダッシュボードでこれらのメトリックを報告します。ダッシュボードの詳細については、ダッシュボードについて （403 ページ）を参照してください。メトリックデータは分析のために収集されるため、アラートは関連付けられません。
- [OpenConfigストリーミングテレメトリ（OpenConfig Streaming Telemetry）]：ベンダー中立の OpenConfig モデルを使用する、Threat Defense デバイスから外部データ収集システムへのヘルス メトリクス テレメトリ ストリームを構成します。詳細については、OpenConfig ストリーミングテレメトリの設定を参照してください。

ステップ 7 ポリシーが割り当てられているデバイスを表示および変更するには、次の手順を実行します。

a) [ポリシーの割り当てと展開（Policy Assignments & Deploy）] をクリックします。
b) [使用可能なデバイス（Available Devices）] リストから、正常性ポリシーを割り当てるデバイスの横にある [+] アイコンをクリックします。
c) [適用（Apply）] をクリックします。

または、正常性ポリシーの適用 （451 ページ）の説明に従って、アプライアンスに正常性ポリシーを適用できます。

正常性ステータスを追跡するアプライアンスごとに正常性ポリシーを適用します。正常性ポリシーをアプライアンスに適用すると、ポリシー内で有効にしたすべてのモジュールが、アプライアンス上のプロセスとハードウェアの正常性をモニターし、そのデータを Management Center に転送します。

ステップ 8 [保存（Save）] をクリックします。

正常性ポリシーの削除

不要になった正常性ポリシーを削除できます。ただし、アプライアンスには少なくとも 1 つの正常性ポリシーが割り当てられている必要があります。アプライアンスに適用されているポリシーを削除した場合は、別のポリシーを適用するまでそのポリシー設定が有効のままになります。加えて、デバイスに適用されている正常性ポリシーを削除した場合、元となる関連アラート応答を無効にするまでは、そのデバイスに対して有効になっているヘルス モニタリング アラートがアクティブなままになります。

ヒント　アプライアンスのヘルスモニタリングを停止するには、すべてのモジュールが無効になっている正常性ポリシーを作成し、それをアプライアンスに適用します。

手順

ステップ 1　システム（⚙） > **[正常性（Health）]** > **[ポリシー（Policy）]**を選択します。

ステップ 2　削除するポリシーの横にある [削除（Delete）]（🗑） をクリックし、[正常性ポリシーの削除（Delete health policy）] をクリックして削除します。
削除が成功したかどうかを示すメッセージが表示されます。

OpenConfig を使用したベンダー中立のテレメトリストリーミングの送信

OpenConfigは、ネットワークを管理およびモニターするために単一の方法で複数のベンダーにネットワーク テレメトリ データをストリーミングすることを可能にする、ベンダーに依存しないソフトウェアレイヤです。Cisco Secure Firewall の OpenConfig ストリーミング テレメトリ オプションは、gNMI（gRPC ネットワーク管理インターフェイス）プロトコルを使用して、Threat Defense デバイスからデータ収集システムへのテレメトリストリームを制御および生成できるようにします。

Firewall Threat Defenseの正常性ポリシーには、OpenConfigストリーミングテレメトリ機能をサポートおよび有効化するためのすべての設定が含まれています。正常性ポリシーをデバイスに展開すると、OpenConfigストリーミングテレメトリ設定によってgNMIサーバーがアクティブ化され、データコレクターからのリモートプロシージャコール（RPC）メッセージのリッスンが開始されます。

OpenConfig ストリーミングテレメトリのサブスクリプションモデル

OpenConfigは、サブスクリプションベースのモデルを使用します。このモデルでは、データコレクターが、Threat Defense デバイスにテレメトリデータをクエリするか、ストリーミングされるテレメトリデータのコレクターとして動作します。データコレクタは、Threat Defense デバイスから更新とメトリックを受信する必要がある場合、Threat Defense gNMI サーバーに subscribeRequest RPC メッセージを送信します。サブスクリプション要求には、データコレクターがサブスクライブする必要がある1つ以上のパスの詳細が含まれます。このメッセージには、サブスクリプションの有効期間を示すサブスクリプションモードも含まれます。Threat Defense サーバーは、次のサブスクリプションモードをサポートしています。

- ワンタイム サブスクリプション（*Once subscription*）：Threat Defense デバイスは、要求されたデータを gNMI パスに 1 回だけ送信します。

- ストリーミング サブスクリプション（*Stream subscription*）：Threat Defense は、`SubscribeRequest` RPC メッセージで指定されたトリガーに従って、テレメトリデータを継続的にストリーミングします。
  - サンプリング サブスクリプション（*Sampled subscription*）：Threat Defense サーバーは、サブスクリプション メッセージで指定された間隔に従って、要求されたデータをストリーミングします。Threat Defense がサポートする最小間隔は 1 分です。
  - 変更時サブスクリプション（*On-change subscription*）：Threat Defense は、要求された値が変化するたびにデータを送信します。

Threat Defense サーバーは、作成されたサブスクリプションのタイプに従って、データコレクターによって要求された頻度で `SubscribeResponse` RPC メッセージを生成します。

OpenConfig ストリーミングテレメトリの展開モード

OpenConfig ストリーミングテレメトリ設定では、次の展開モードを使用できます。

- **ダイヤルイン（DIAL-IN）**：このモードでは、gNMI サーバーは、Threat Defense でポートを開き、データコレクターからの `SubscribeRequest` RPC メッセージを待ちます。デバイス正常性ポリシーでは、gNMI サーバーが使用するポート番号と、gNMI サービスに接続できるデータコレクターの IP アドレスを指定できます。指定しない場合、gNMI サーバーは、ポート番号 50051 を使用します。ダイヤルインモードは、テレメトリストリームをサブスクライブするエンドポイントが信頼されている、信頼できるネットワークでの使用に最適です。
- **ダイヤルアウト（DIAL-OUT）**：gNMI サービスは、gNMI データコレクターからのサブスクリプション要求を受け入れてテレメトリデータを提供するサーバーモードで動作するように設計されています。gNMI データコレクターが gNMI サーバーに到達できない場合、Threat Defense は、トンネルクライアントを使用し、外部サーバーとの gRPC トンネルを確立します。このトンネルにより、gNMI サーバーとクライアントの間での RPC メッセージの交換が可能になります。ダイヤルアウトモードは、データコレクターがクラウド上または信頼できるネットワークの外部でホストされている場合の使用に最適です。

ダイヤルインモードとダイヤルアウトモードのどちらでも、gNMI サーバーと gNMI クライアントの間でのすべての通信で TLS 暗号化が使用されるため、TLS 暗号化用の秘密キーを使用して一連の証明書を生成する必要があります。ダイヤルアウトモードでは、トンネルインフラストラクチャ用の追加のキーが必要です。詳細については、「秘密キーを使用して証明書を生成する方法」を参照してください。

証明書および秘密キーの生成

OpenConfig ストリーミングテレメトリ設定に必要な CA、サーバー、およびクライアント証明書/秘密キーセットを生成します。

（注） 確実に同じ CA を使用して証明書を生成するには、同じエンドポイントから次のコマンドを一緒に実行します。コマンドを再試行する場合は、すべてのコマンドを再試行する必要があります。

始める前に

手順

ステップ 1 次のコマンドを実行するエンドポイントに、フォルダ（keys など）を作成します。

例：

```
mkdir keys
```

ステップ 2 対応する秘密キーを使用して自己署名 CA 証明書を作成します。

例：

次のコマンド例は、新しい RSA 秘密キーを生成し、それを使用して、指定されたサブジェクト情報を含む自己署名 X.509 証明書を作成します。

```
openssl req -x509 -newkey rsa:4096 -days 365 -nodes -keyout keys/ca-key.pem -out
keys/ca-cert.pem -subj "/C=XX
/ST=YY/L=ZZZ/O=Example/OU=EN/CN=gnmi-ca/emailAddress=abc@example.com"
```

件名情報には、指定された国（C）、州（ST）、地域（L）、組織（O）、組織単位（OU）、共通名（CN）、および電子メールアドレスが含まれます。

秘密キーは ca-key.pem ファイルとして保存され、証明書は ca-cert.pem ファイルとして keys フォルダに保存されます。

ステップ 3 指定された共通名（CN）とサブジェクト代替名（SAN）を使用して自己署名サーバー証明書を作成します。

例：

次のコマンド例は、新しい RSA 秘密キーを生成し、それを使用して、指定されたサブジェクト情報を含む自己署名 X.509 証明書を作成します。この例では、192.168.0.200 が Threat Defense デバイスの IP アドレスであり、192.168.0.202 がクライアントの IP アドレスです。

（注） この証明書/キーセットをダイヤルインモードで使用する場合、クライアント IP は必要ありません。

```
CN="192.168.0.200"
SAN="IP:192.168.0.200,IP:192.168.0.202"
openssl req -newkey rsa:4096 -nodes -keyout keys/server-key.pem -out keys/server-req.pem
 -subj "/C=XX/ST=YY/L=ZZZ/O=Example/OU=EN/CN=${CN}/emailAddress=abc@example.com}"
openssl x509 -req -extfile <(printf "subjectAltName=${SAN}") -in keys/server-req.pem
-days 60 -CA keys/ca-cert.pem -CAkey keys/ca-key.pem -CAcreateserial -out
keys/server-cert.pem
cat keys/server-key.pem keys/server-cert.pem keys/ca-cert.pem > keys/server-combined.pem
```

`openssl req` コマンドは、新しい RSA 秘密キーと証明書署名要求（CSR）を生成します。秘密キーは `server-key.pem` ファイルとして保存され、CSR は `server-req.pem` ファイルとして `keys` フォルダに保存されます。

`openssl x509` コマンドは、CSR を処理し、サーバー証明書を生成します。サーバー証明書は `server-cert.pem` ファイルとして `keys` フォルダに保存されます。

`cat` コマンドは、サーバーキー、サーバー証明書、および CA 証明書を `server-combined.pem` という名前の単一のファイルに結合し、そのファイルを keys フォルダに保存します。

Management Center から **OpenConfig ストリーミングテレメトリ**を設定するときに、`server-combined.pem` をアップロードする必要があります。Threat Defense およびトンネルサーバー（ダイヤルアウトモード）で動作する gNMI サーバーは、TLS 通信にこの証明書を使用します。パスフレーズを使用して秘密キーを暗号化する場合は、必ず、Management Center に証明書をアップロードするときにパスフレーズを指定してください。

ステップ 4 指定された共通名（CN）とサブジェクト代替名（SAN）を使用してクライアント証明書を作成します。

例：

次のコマンド例は、新しい RSA 秘密キーを生成し、それを使用して、指定されたサブジェクト情報を含む自己署名 X.509 証明書を作成します。この例では、192.168.0.202 がクライアントの IP アドレスです。

```
CN="192.168.0.202"
SAN="IP:192.168.0.202"
openssl req -newkey rsa:4096 -nodes -keyout keys/client-key.pem -out keys/client-req.pem
 -subj "/C=XX/ST=YY/L=ZZZ/O=example/OU=EN/CN=${CN}/emailAddress=abc@example.com"
openssl x509 -req -extfile <(printf "subjectAltName=${SAN}") -in keys/client-req.pem
-days 60 -CA keys/ca-cert.pem -CAkey keys/ca-key.pem -CAcreateserial -out
keys/client-cert.pem
```

gNMI クライアントは、TLS 通信にクライアント証明書（`client-cert.pem`）と秘密キーを使用します。

ステップ 5 （任意）ダイヤルアウトモードの場合は、指定された共通名（CN）とサブジェクト代替名（SAN）を使用してトンネルサーバー証明書を作成します。

例：

次のコマンド例は、新しい RSA 秘密キーを生成し、それを使用して、指定されたサブジェクト情報を含む自己署名 X.509 証明書を作成します。この例では、192.168.0.202 がクライアントの IP アドレスです。

```
CN="192.168.0.202"
SAN="IP:192.168.0.202"
openssl req -newkey rsa:4096 -nodes -keyout keys/tunnel-server-key.pem -out
keys/tunnel-server-req.pem -subj "
/C=XX/ST=YY/L=ZZZ/O=Example/OU=EN/CN=${CN}/emailAddress=abc@example.com}"
openssl x509 -req -extfile <(printf "subjectAltName=${SAN}") -in keys/tunnel-server-req.pem
 -days 60 -CA keys/ca-cert.pem -CAkey keys/ca-key.pem -CAcreateserial -out
keys/tunnel-server-cert.pem
```

OpenConfig ストリーミングテレメトリの設定

始める前に

- 正常性ポリシー構成を展開する Threat Defense デバイスで、SSL 証明書と秘密キーのインストールが許可されていることを確認してください。
- OpenConfig ストリーミングテレメトリ実装をサポートする gNMI クライアントを設定していることを確認してください。このクライアントから、Threat Defense 上の gNMI サーバーに gRPC 要求を行うことができます。
- ダイヤルアウトモードを使用し、OpenConfig ストリーミングテレメトリを設定するために、管理システムで gRPC トンネルサーバーおよびクライアントを設定していることを確認してください。このトンネル設定により、gNMI クライアントと Threat Defense デバイスが通信できるようになります。
- 次のタスクを実行するには、管理者ユーザーである必要があります。

手順

ステップ 1 **[システム（System）] > [ポリシー（Policy）]**を選択します。

ステップ 2 変更する Threat Defense の正常性ポリシーの横にある [正常性ポリシーの編集（Edit health policy）] アイコンをクリックします。

ステップ 3 [設定（Settings）] タブに移動します。

ステップ 4 [OpenConfigストリーミングテレメトリ（OpenConfig Streaming Telemetry）] スライダを動かして、構成を有効にします。デフォルトでは、この設定は無効になっています。

ステップ 5 [SSL証明書（SSL Certificate）] をアップロードします。gNMI サーバーはこの証明書を使用して、TLS接続用のサーバー認証を有効にし、チャネルを介したすべての通信を暗号化します。

OpenConfig ストリーミングテレメトリ構成では、PEM 形式の証明書のみサポートされます。Management Center は、アプライアンスと gNMI コレクタが暗号化通信を接続障害なしで確実に実行できるように、次の証明書検証を実行します。

- ASCII テキストが有効な証明書ファイルであることを確認します。
- アップロードされた証明書の有効期限を確認します。
- アップロードされた PEM ファイルで予期される証明書と秘密キーの数を確認します。ファイルには少なくとも 1 つの証明書が必要であり、証明書内の秘密キーの数は常に 1 である必要があります。
- キーブロックタイプ PRIVATE KEY、RSA PRIVATE KEY、ENCRYPTED PRIVATE KEY、または RSA ENCRYPTED PRIVATE KEY を確認して受け入れます。
- 暗号化された PEM ファイルの場合は、Proc-Type: 4,ENCRYPTED? キーワードが存在することを確認します。
- 暗号化された PEM ファイルに対してパスフレーズが有効であることを確認します。

ステップ 6 （任意）秘密キーファイルが暗号化されている場合は、パスフレーズを指定します。

ステップ 7 gNMI プロトコルを介したテレメトリのストリーミングに使用する展開モードを選択します。

ダイヤルインモードの場合：

1. gNMI サービスのポート番号を割り当てます。

   gNMI サーバーはポートを開き、コレクタからの gRPC 要求を待ちます。

2. Threat Defense デバイスに接続できる gNMI コレクタの IPv4/IPv6 アドレスを指定します。

3. [コレクタの追加（Add Collector）] をクリックして、gNMI コレクタをさらに追加します。最大 5 つのコレクタを追加できます。

ダイヤルアウトモードの場合：

1. Threat Defense デバイスからのストリーミングテレメトリをサブスクライブできる gNMI コレクタのホスト名とポート番号を指定します。

2. [コレクタの追加（Add Collector）] をクリックして、gNMI コレクタをさらに追加します。最大 5 つのコレクタを追加できます。

ステップ 8 gNMI コレクタを検証するためのユーザー名とパスワードを指定します。

Threat Defense サーバーは、`SubscribeRequest` RPC メッセージを受信するときに、このログイン情報を使用して gNMI コレクタを認証します。各テレメトリメッセージは、ユーザー名とパスワードを使用して認証されません。システムは、以前に認証された暗号化されたストリーミングチャネルを使用して、テレメトリメッセージを伝送します。

ステップ 9 [保存（Save）] をクリックします。

次のタスク

構成の変更を有効にするために、正常性ポリシーを Threat Defense デバイスに展開します。

OpenConfig ストリーミングテレメトリのトラブルシューティング

不明な認証局によって署名された証明書

- Management Center に正しい証明書をアップロードしたことを確認します。
- 証明書およびキー生成手順を確認します。IP サブジェクト代替名（SAN）が正しく指定されていることを確認します。

証明書が無効

Management Center に「Request was made for (IP), but the certificate is not valid for (IP)」（（IP）の要求がありましたが、（IP）の証明書が有効ではありません）というエラーが表示される場合は、サーバー証明書およびキー生成手順を確認します。

- サーバー証明書でIP SANが正しく指定されていることを確認します。設定が複数のThreat Defense デバイスに適用される場合は、[IP SAN] フィールドですべてのデバイスを指定する必要があります。
- ダイヤルアウトモードを使用している場合は、クライアント IP がサーバー証明書で指定されていることを確認します。

応答オブジェクトの生成に失敗する

「Failed to generate response object, did not receive any data」（応答オブジェクトの生成に失敗し、データを受信しませんでした）というエラーメッセージが表示される場合、gNMI 入力プラグインは、メトリックのエクスポートを待機しています。次に、テレグラフの再起動時に表示される応答の例を示します。

```
root@cronserver:/home/secanup/openconfig-test# gnmic -a $ADDRESS:$PORT --tls-cert
$CLIENTCERT --tls-ca $CACERT --tls-key $CLIENTKEY -u $USER -p $PASS sub --mode once
--path "openconfig-system/system/memory"
rpc error: code = Aborted desc = Error in gnmi_server: failed to generate response
object.did not receive any data
Error: one or more requests failed
```

gNMI 入力プラグインが再起動するのを待ってから、要求を再試行します。

テレグラフの再起動

テレグラフが応答しない場合は、Threat Defense の CLI コンソールで次のコマンドを使用してプロセスを再起動します。

```
pmtool restartbyid hmdaemon
```

gNMI サーバーの現在のステータスの取得

OpenConfig ストリーミングテレメトリが有効になっている場合、gNMI サーバーのステータスを確認するには、Threat Defense の CLI コンソールを使用して次のコマンドを実行します。

```
curl localhost:9275/OpenConfig/status
```

次に、コマンドへの応答の例を示します。

```
root@firepower:/home/admin# curl localhost:9275/openconfig/status
Mode (Dialin/Dialout): DialIn
Subscription Details:
    Active Subscription Details:
        Stream Mode Subscription Details:
            Total Stream Subscription Request Count: 1
            'Ip of Collector- Subscribe paths:’
                172.16.0.101:45826:
                - /openconfig-system/system/state/hostname
            Sample Subscription Count: 1
            On Change Subscription Count: 0
        Once Mode Subscription Details:
            Total Subscription Request Count: 0
            Total Subscription Count: 0
            'Ip of Collector- Subscribe paths:’: {}
    Total Subscription Details:
        Stream Mode Subscription Details:
            Total Stream Subscription Request Count: 1
            'Ip of Collector- Subscribe paths:’:
```

```
                172.16.0.101:45826:
                - /openconfig-system/system/state/hostname
        Sample Subscription Count: 1
        On Change Subscription Count: 0
    Once Mode Subscription Details:
        Total Subscription Request Count: 0
        Total Subscription Count: 0
        'Ip of Collector- Subscribe paths:': {}
```

ヘルスモニタリングでのデバイスの除外

通常のネットワーク メンテナンスの一環として、アプライアンスを無効にしたり、一時的に使用不能にしたりすることがあります。このような機能停止は意図したものであり、アプライアンスからのヘルス ステータスに Management Center 上のサマリー ヘルス ステータスを反映させる必要はありません。

ヘルスモニターの除外機能を使用して、アプライアンスまたはモジュールに関するヘルス モニタリング ステータス レポートを無効にすることができます。たとえば、ネットワークのあるセグメントが使用できなくなることがわかっている場合は、そのセグメント上の管理対象デバイスのヘルス モニタリングを一時的に無効にして、Management Center上のヘルス ステータスにデバイスへの接続がダウンしたことによる警告状態または重大状態が表示されないようにできます。

ヘルス モニタリング ステータスを無効にしても、ヘルス イベントは生成されますが、そのステータスが無効になっているため、ヘルス モニターのヘルス ステータスには影響しません。除外リストからアプライアンスまたはモジュールを削除しても、除外中に生成されたイベントのステータスは [無効（Disabled）] のままです。

アプライアンスからのヘルスイベントを一時的に無効にするには、除外設定ページに移動して、アプライアンスをデバイス除外リストに追加します。設定が有効になると、システムが全体のヘルスステータスを計算するときに、除外されているアプライアンスが考慮されなくなります。[ヘルス モニター アプライアンス ステータスの概要（Health Monitor Appliance Status Summary）] にはこのアプライアンスが [無効（Disabled）] としてリストされます。

個々のヘルスモジュールを無効にすることもできます。たとえば、Management Center 上でホスト制限に達した場合、 ホスト制限ステータスメッセージを無効にできます。

メインの [ヘルスモニター（Health Monitor）] ページで、ステータス行内の矢印をクリックして特定のステータスを持つアプライアンスのリストを展開表示すれば、除外されたアプライアンスを区別できることに注意してください。

（注） Management Center では、ヘルスモニターの除外設定はローカル構成設定です。そのため、Management Center 上でデバイスを除外してから削除しても、後で再登録すれば、除外設定は元どおりになります。新たに再登録したデバイスは除外されたままです。

ヘルスモニタリングからのアプライアンスの除外

アプライアンスは個別に、またはグループ、モデル、関連付けられている正常性ポリシーにより、除外できます。

個別のアプライアンスのイベントと正常性ステータスを [無効（Disabled）] に設定する必要がある場合、アプライアンスを除外できます。除外設定が有効になると、アプライアンスが [正常性モニター アプライアンス モジュールの概要（Health Monitor Appliance Module Summary）] に [無効（Disabled）] として表示され、アプライアンスの正常性イベントのステータスが [無効（Disabled）] になります。

手順

ステップ 1 システム（⚙） > **[正常性（Health）]** > **[除外（Exclude）]**を選択します。

ステップ 2 [Add Device] をクリックします。

ステップ 3 [デバイスの除外（Device Exclusion）] ダイアログボックスの [使用可能なデバイス（Available Devices）] で、ヘルスモニタリングから除外するデバイスに対して **Add** (⊕) をクリックします。

ステップ 4 [除外（Exclude）] をクリックします。選択したデバイスが除外のメインページに表示されます。

ステップ 5 除外リストからデバイスを削除するには、[削除（Delete）]（🗑） をクリックします。

ステップ 6 [適用（Apply）] をクリックします。

次のタスク

アプライアンス上の個別の正常性ポリシーモジュールを除外するには、正常性ポリシーモジュールの除外 （462 ページ）を参照してください。

正常性ポリシーモジュールの除外

アプライアンス上の個別の正常性ポリシーモジュールを除外できます。この操作により、モジュールからのイベントによってアプライアンスのステータスが Warning または Critical に変更されないようにすることができます。

除外設定が有効になると、アプライアンスには、ヘルスモニタリングからデバイスで除外されているモジュールの数が表示されます。

ヒント 個別に除外したモジュールを追跡して、必要に応じてそれらを再アクティブ化できるようにしてください。誤ってモジュールを無効にすると、必要な警告または重大メッセージを見逃す可能性があります。

手順

ステップ 1 システム（⚙） > **[正常性（Health）]** > **[除外（Exclude）]** を選択します。

ステップ 2 変更するアプライアンスの横にある **[編集（Edit）]**（✎） をクリックします。

ステップ 3 [正常性モジュールの除外（Exclude Health Modules）] ダイアログボックスでは、デフォルトで、デバイスのすべてのモジュールがヘルスモニタリングから除外されます。一部のモジュールは特定のデバイスにのみ適用できます。詳細はヘルス モジュール（434 ページ）を参照してください。

ステップ 4 デバイスの除外期間を指定するには、[除外期間（Exclude Period）] ドロップダウンリストから期間を選択します。

ステップ 5 ヘルスモニタリングから除外するモジュールを選択するには、[モジュールレベルの除外の有効化（Enable Module Level Exclusion）] リンクをクリックします。[正常性モジュールの除外（Exclude Health Modules）] ダイアログボックスに、デバイスのすべてのモジュールが表示されます。関連付けられた正常性ポリシーに対応しないモジュールは、デフォルトで無効になります。モジュールを除外するには、次の手順を実行します。

1. 目的のモジュールの横にある **[スライダ（Slider）]**（⬭） ボタンをクリックします。
2. 選択したモジュールの除外期間を指定するには、[除外期間（Exclude Period）] ドロップダウンリストから期間を選択します。

ステップ 6 除外設定の [除外期間（Exclude Period）] で [無期限（Permanent）] 以外を選択した場合は、有効期限が切れたときに設定を自動的に削除することを選択できます。この設定を有効にするには、[期限切れの設定の自動削除（Auto-delete expiration configuration）] チェックボックスをオンにします。

ステップ 7 [OK] をクリックします。

ステップ 8 デバイス除外のメインページで、[適用（Apply）] をクリックします。

期限切れの正常性モニターの除外

デバイスまたはモジュールの除外期限が切れた場合、除外をクリアするか更新するかを選択できます。

手順

ステップ 1 システム（⚙） > **[正常性（Health）]** > **[除外（Exclude）]**を選択します。

[警告（Warning）]（⚠） アイコンがデバイスに対して表示されます。これは、デバイスまたはモジュールをアラートから除外する期間の期限が切れたことを示します。

ステップ 2 デバイスの除外を更新するには、アプライアンスの横にある **[編集（Edit）]**（） をクリックします。[正常性モジュールの除外（Exclude Health Modules）] ダイアログボックスで、[更新（Renew）] リンクをクリックします。デバイスの除外期間が現在の値で延長されます。

ステップ 3 デバイスの除外をクリアするには、アプライアンスの横にある [削除（Delete）]（） をクリックし、[デバイスを除外から削除（Remove the device from exclude）]、[適用（Apply）] の順にクリックします。

ステップ 4 モジュールの除外を更新またはクリアするには、アプライアンスの横にある **[編集（Edit）]**（） をクリックします。[正常性モジュールの除外（Exclude Health Modules）] ダイアログボックスで、[モジュールレベルの除外の有効化（Enable Module Level Exclusion）] リンクをクリックし、モジュールに対して [更新（Renew）] リンクまたは [クリア（Clear）] リンクをクリックします。[更新（Renew）] をクリックすると、モジュールの除外期間が現在の値で延長されます。

ヘルス モニター アラート

正常性ポリシー内のモジュールのステータスが変更された場合に電子メール、SNMP、または syslog経由で通知するアラートをセットアップできます。特定のレベルのヘルスイベントが発生したときにトリガーされ警告されるヘルス イベント レベルと、既存のアラート応答を関連付けることができます。

たとえば、アプライアンスがハード ディスク スペースを使い果たす可能性を懸念している場合は、残りのディスク スペースが警告レベルに達したときに自動的に電子メールをシステム管理者に送信できます。ハード ドライブがさらにいっぱいになる場合、ハード ドライブが重大レベルに達したときに 2 つ目の電子メールを送信できます。

ヘルス モニター アラート情報

ヘルス モニタによって生成されるアラートには次の情報が含まれます。

- アラートの重大度レベルを示す [重大度（Severity）]。
- テスト結果がアラートをトリガーとして使用したヘルス モジュールを示す [モジュール（Module）]。
- アラートをトリガーとして使用したヘルス テスト結果を含む [説明（Description）]。

次の表で、これらのシビラティ（重大度）レベルについて説明します。

表 *32*：アラートのシビラティ（重大度）

シビラティ（重大度）	説明
クリティカル	ヘルステスト結果がクリティカルアラート ステータスをトリガーとして使用する基準を満たしました。
警告	ヘルス テスト結果が警告アラート ステータスをトリガーとして使用する基準を満たしました。
標準	ヘルス テスト結果が通常のアラート ステータスをトリガーとして使用する基準を満たしました。
エラー（Error）	ヘルス テストが実行されませんでした。
回復済み（Recovered）	ヘルス テスト結果がクリティカルまたは警告のアラート ステータスから通常のアラート ステータスに戻るための基準を満たしました。

ヘルス モニター アラートの作成

この手順を実行するには、管理者ユーザーである必要があります。

ヘルスモニターアラートを作成するときに、重大度レベル、ヘルスモジュール、およびアラート応答の関連付けを作成します。既存のアラートを使用することも、新しいアラートをシステムヘルスの報告専用に設定することもできます。選択したモジュールがシビラティ（重大度）レベルに達すると、アラートがトリガーされます。

既存のしきい値と重複するようにしきい値を作成または更新すると、競合が通知されます。重複したしきい値が存在する場合、ヘルスモニタは最も少ないアラートを生成するしきい値を使用し、その他のしきい値を無視します。しきい値のタイムアウト値は、5 ～ 4,294,967,295 分の間にする必要があります。

始める前に

- ヘルス アラートを送信する SNMP、syslog、電子メール サーバーと Management Center との通信を制御するアラート応答を設定します。Secure Firewall Management Center アラート応答 （673 ページ）を参照してください。

手順

ステップ 1 システム（⚙） > **[正常性（Health）]** > **[モニタアラート（Monitor Alerts）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ヘルスアラートの追加（Add Health Alert）] ダイアログボックスの [ヘルスアラート名（Health Alert Name）] フィールドに、ヘルスアラートの名前を入力します。

ステップ 4 [重大度（Severity）] ドロップダウンリストから、アラートをトリガーするために使用する重大度レベルを選択します。

ステップ 5 [アラート（Alert）] ドロップダウンリストから、指定した重大度レベルに達したときにトリガーするアラート応答を選択します。まだSecure Firewall Management Center アラート応答していない場合は、[アラート（Alerts）] をクリックして [アラート（Alerts）] ページにアクセスし、アラートを設定します。

ステップ 6 [ヘルスモジュール（Health Modules）] リストから、アラートを適用する正常性ポリシーモジュールを選択します。

ステップ 7 オプションで、[しきい値タイムアウト（Threshold Timeout）] フィールドに、それぞれのしきい値期間が終了してしきい値がリセットされるまでの分数を入力します。

ポリシーの実行時間間隔の値がしきい値タイムアウトの値より小さい場合でも、特定のモジュールから報告される 2 つのヘルス イベント間の間隔のほうが常に大きくなります。たとえば、しきい値タイムアウトを 8 分に変更し、ポリシーの実行時間間隔が 5 分である場合、報告されるイベント間の間隔は 10 分（5 × 2）になります。

ステップ 8 [保存（Save）] をクリックして、ヘルス アラートを保存します。

ヘルス モニタ アラートの編集

この手順を実行するには、管理者ユーザーである必要があります。

既存のヘルス モニター アラートを編集して、ヘルス モニター アラートに関連付けられた重大度レベル、ヘルス モジュール、またはアラート応答を変更できます。

手順

ステップ 1 **システム**（⚙）**>[正常性（Health）]>[モニタアラート（Monitor Alerts）]**を選択します。

ステップ 2 変更する、必要な正常性アラートに対して表示される **[編集（Edit）]**（✎）アイコンをクリックします。

ステップ 3 [正常性アラートの編集（Edit Health Alert）] ダイアログボックスで、[アラート（Alert）] ドロップダウンリストから必要なアラートエントリを選択するか、[アラート（Alerts）] リンクをクリックして新しいアラートエントリを設定します。

ステップ 4 [保存（Save）] をクリックします。

ヘルス モニタ アラートの削除

手順

ステップ 1 システム（⚙） > **[正常性（Health）]** > **[モニタアラート（Monitor Alerts）]**を選択します。

ステップ 2 削除する正常性アラートの横にある [削除（Delete）]（🗑） をクリックし、[正常性アラートの削除（Delete health alert）] をクリックして削除します。

次のタスク

- アラートが継続しないようにするには、元になるアラート応答を無効にするか、または削除します。Secure Firewall Management Center アラート応答 （673 ページ）を参照してください。

ヘルスモニターについて

この手順を実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティアナリスト ユーザーである必要があります。

ヘルスモニターには、Management Centerによって管理されているすべてのデバイスに加えて、Management Center 自体に関して収集されたヘルスステータスが表示されます。ヘルス モニタは以下で構成されています。

- [ヘルスステータス（Health Status）] サマリーページ：Management Center と Management Centerが管理するすべてのデバイスの正常性を一目で確認できます。デバイスは、個別に一覧表示されるか、該当する場合は地理位置情報、高可用性、またはクラスタステータスに基づいてグループ化されます。
  - デバイスの正常性を表す六角形にマウスカーソルを合わせると、Management Center およびデバイスの正常性の概要が表示されます。
  - デバイスの左横にあるドットは、そのデバイスのヘルスを示しています。
    - 緑色：アラームなし。
    - オレンジ色：少なくとも 1 つのヘルス警告があります。
    - 赤色：少なくとも 1 つの重大なヘルスアラームがあります。
- [Monitoring（モニタリング）]ナビゲーションウィンドウ：デバイス階層を移動できます。ナビゲーションペインから個々のデバイスのヘルスモニターを表示できます。

手順

ステップ 1 システム（⚙） > **[正常性（Health）]** > **[モニタ（Monitor）]**を選択します。

ステップ 2 [ヘルスステータス（Health Status）] ランディングページで Management Center とその管理対象デバイスのステータスを確認します。

a) 六角形にポインタを合わせると、デバイスの正常性の概要が表示されます。ポップアップウィンドウに、上位 5 つの正常性アラートの概要の一部が表示されます。ポップアップをクリックすると、正常性アラート概要の詳細ビューが開きます。

b) デバイスリストで[展開（Expand）]（>）と[折りたたみ（Collapse ）]（⌄）をクリックして、デバイスの正常性アラートのリストを展開または折りたたみます。

行を展開すると、ステータス、タイトル、詳細を含めて、すべての正常性アラートが一覧表示されます。

（注） 正常性アラートは、シビラティ（重大度）レベルでソートされます。

ステップ 3 [Monitoring] ナビゲーションペインを使用して、デバイス固有の正常性モニターにアクセスします。[モニタリング（Monitoring）] ナビゲーションウィンドウを使用する場合：

a) [ホーム（Home）] をクリックして、[ヘルスステータス（Health Status）] 概要ページに戻ります。

b) **[Firewall Management Center]** をクリックして、Secure Firewall Management Center 自体の正常性モニターを表示します。

c) デバイスリストで [展開（Expand）]（>） と [折りたたみ（Collapse ）]（⌄） をクリックして、管理対象デバイスのリストを展開または折りたたみます。

行を展開すると、すべてのデバイスが一覧表示されます。

d) デバイスをクリックすると、デバイス固有のヘルスモニターが表示されます。

次のタスク

- Management Centerによって管理されるデバイスの収集されたヘルスステータスとメトリックについては、デバイスヘルスモニター （473 ページ）を参照してください。
- Management Center のヘルスステータスについては、Management Center 正常性モニターの使用 （468 ページ）を参照してください。

  [ホーム（Home）] をクリックすると、いつでも [ヘルスステータス（Health Status）] ランディングページに戻ることができます。

Management Center 正常性モニターの使用

この手順を実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティアナリスト ユーザーである必要があります。

Management Centerモニターは、Management Center のヘルスステータスの詳細ビューを提供します。ヘルス モニタは以下で構成されています。

- [高可用性（High Availability）]（設定されている場合）：[高可用性（High Availability）]（HA）パネルには、アクティブユニットとスタンバイユニットのステータス、最終同期時刻、および全体的なデバイスの正常性を含む、現在の HA ステータスが表示されます。
- [イベントレート（Event Rate）]：[イベントレート（Event Rate）] パネルには、ベースラインとしての最大イベントレートと、Management Center によって受信された全体のイベントレートが表示されます。
- [イベントキャパシティ（Event Capacity）]：[イベントキャパシティ（Event Capacity）] パネルには、イベントカテゴリごとの現在の消費量が表示されます。これには、イベントの保持時間、現在のイベントキャパシティと最大イベントキャパシティ、およびManagement Center の設定された最大キャパシティを超えてイベントが保存されたときに警告されるキャパシティ オーバーフロー メカニズムが含まれます。
- [プロセスの正常性（Process Health）]：[プロセスの正常性（Process Health）] パネルには、重要なプロセスの概要ビューと、すべての処理対象の状態（各プロセスの CPU およびメモリ使用率を含む）を表示できるタブがあります。
- [CPU]：[CPU] パネルでは、平均 CPU 使用率（デフォルト）とすべてのコアの CPU 使用率を切り替えることができます。
- [メモリ（Memory）]：[メモリ（Memory）] パネルには、Management Center での全体のメモリ使用率が表示されます。
- [インターフェイス（Interface）]：[インターフェイス（Interface）] パネルには、すべてのインターフェイスの平均入出力レートが表示されます。
- [ディスク使用率（Disk Usage）]：[ディスク使用率（Disk Usage）] パネルには、ディスク全体の使用状況と、Management Center データが保存されている重要なパーティションの使用状況が表示されます。
- [ハードウェア統計（Hardware Statistics）]：[ハードウェア統計（Hardware Statistics）] には、Management Center シャーシのファン速度、電源、および温度が表示されます。詳細については、「Management Center のハードウェア統計 （472 ページ）」を参照してください。

ヒント 通常は、非活動状態が 1 時間（または設定された他の時間間隔）続くと、ユーザーはセッションからログアウトされます。ヘルス ステータスを長期間受動的に監視する予定の場合は、一部のユーザのセッション タイムアウトの免除、またはシステム タイムアウト設定の変更を検討してください。詳細については、内部ユーザーの追加または編集 （147 ページ）とセッション タイムアウトの設定 （118 ページ）を参照してください。

手順

ステップ 1 システム（⚙） > **[正常性（Health）]** > **[モニタ（Monitor）]** を選択します。

ステップ 2 [モニタリング（Monitoring）] ナビゲーションウィンドウを使用して、Management Center およびデバイス固有のヘルスモニターにアクセスします。

- スタンドアロン Management Center は単一のノードとして表示されます。高可用性 Management Center は、ノードのペアとして表示されます。
- ヘルスモニターは、HA ペアのアクティブとスタンバイ両方の Management Center に使用できます。

ステップ 3 Management Center ダッシュボードを確認します。

Management Center ダッシュボードには、Management Center の HA 状態の概要ビュー（設定されている場合）と、Management Center のプロセスとデバイスのメトリック（CPU、メモリ、ディスク使用率など）の概要ビューが含まれています。

アプライアンスのすべてのモジュールの実行

この手順を実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティアナリスト ユーザーである必要があります。

ヘルス モジュール テストは、正常性ポリシーの作成時に設定されたポリシー実行時間間隔で自動的に実行されます。ただし、アプライアンスの最新の正常性情報を収集するためにすべてのヘルス モジュール テストをオンデマンドで実行することもできます。

手順

ステップ 1 アプライアンスのヘルスモニターを表示します。

ステップ 2 [すべてのモジュールの実行（Run All Modules）] をクリックします。ステータス バーにテストの進捗状況が表示されてから、[ヘルス モニター アプライアンス（Health Monitor Appliance）] ページが更新されます。

（注） ヘルス モジュールを手動で実行した場合は、自動的に発生する最初の更新に、手動で実行されたテストの結果が反映されない可能性があります。手動で実行したばかりのモジュールの値が変更されていない場合は、数秒待ってから、デバイス名をクリックしてページを更新します。ページが自動的に再び更新されるまで待機していてもかまいません。

特定のヘルス モジュールの実行

この手順を実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティ アナリスト ユーザーである必要があります。

ヘルス モジュール テストは、正常性ポリシーの作成時に設定されたポリシー実行時間間隔で自動的に実行されます。ただし、そのモジュールの最新のヘルス情報を収集するためにヘルス モジュール テストをオンデマンドで実行することもできます。

手順

ステップ 1 アプライアンスのヘルスモニターを表示します。

ステップ 2 [モジュール ステータスの概要] グラフで、表示するヘルス アラート ステータス カテゴリの色をクリックします。

ステップ 3 イベントのリストを表示するアラートの [アラート詳細（Alert Detail）] 行で、[実行（Run）] をクリックします。

ステータス バーにテストの進捗状況が表示されてから、[ヘルス モニター アプライアンス（Health Monitor Appliance）] ページが更新されます。

（注） ヘルス モジュールを手動で実行した場合は、自動的に発生する最初の更新に、手動で実行されたテストの結果が反映されない可能性があります。手動で実行したばかりのモジュールの値が変更されていない場合は、数秒待ってから、デバイス名をクリックしてページを更新します。ページが再び自動的に更新されるまで待機していてもかまいません。

ヘルス モジュール アラート グラフの生成

この手順を実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティ アナリスト ユーザーである必要があります。

特定のアプライアンスの特定のヘルス テストの一定期間にわたる結果をグラフ化できます。

手順

ステップ 1 アプライアンスのヘルスモニターを表示します。

ステップ 2 [ヘルス モニター アプライアンス（Health Monitor Appliance）] ページの [モジュール ステータスの概要（Module Status Summary）] グラフで、表示するヘルス アラート ステータス カテゴリの色をクリックします。

ステップ 3 イベントのリストを表示するアラートの [アラート詳細（Alert Detail）] 行で、[グラフ（Graph）] をクリックします。

ヒント イベントが1つも表示されない場合は、時間範囲を調整することを考慮してください。

Management Center のハードウェア統計

Management Center アプライアンス（物理のみ）のハードウェア統計には、ファン速度、電源、温度などのハードウェアエンティティに関する情報が含まれます。SNMP でポーリングし、トラップを送信して、Management Center の正常性をモニターするには、次の手順を実行します。

1. MIB をポーリングするために、Management Center で SNMP を有効にします。デフォルトでは、Management Center の SNMP は無効になっています。SNMP ポーリングの設定 （116 ページ）を参照してください。
2. トラップを有効にするために必要な SNMP ホストごとに ACL エントリを追加します。必ず、ホストの IP アドレスを指定し、ポートとして SNMP を選択してください。アクセスリストの設定 （49 ページ）を参照してください。

[正常性（Health）]>**[モニター（Monitor）]**ページでハードウェア統計を表示するには、次の手順を実行します。

1. **[正常性（Health）]** > **[ポリシー（Policy）]** ページで、[ハードウェア統計（Hardware Statistics）]モジュールが有効になっていることを確認します。デフォルトのしきい値は変更できます。
2. Management Center の正常性モニタリングダッシュボードにポートレットを追加します。[ハードウェア統計（Hardware Statistics）] メトリックグループを選択し、[ファン速度（Fan Speed）] メトリックと [温度（Temperature）] メトリックを選択してください。

電源のステータスは、**[ヘルスモニタリング（Health Monitoring）]**>**[ホーム（Home）]**ページの Firewall Management Center で確認できます。

（注）
- ファン速度は RPM 単位で表示されます。
- 温度は摂氏単位で表示されます。
- 電源の 1 つのスロットがアクティブである場合、ダッシュボードにはそのスロットが [オンライン（Online）] と表示され、もう 1 つのスロットは [電力なし（No Power）] と表示されます。
- グラフの各水平線は、各 PSU およびファンのステータスをそれぞれ示しています。
- グラフにカーソルを合わせると、個々の統計のデータが表示されます。

デバイスヘルスモニター

デバイスヘルスモニターには、Management Center によって管理されているすべてのデバイスに関して収集されたヘルスステータスが表示されます。デバイスヘルスモニターでは、システムイベントを予測して対応するために、Firepower デバイスのヘルスメトリックが収集されます。デバイスヘルスモニターは、次のコンポーネントで構成されています。

- システムの詳細：インストールされている Firepower バージョンやその他の展開の詳細などの、管理対象デバイスに関する情報が表示されます。
- トラブルシューティングとリンク：頻繁に使用されるトラブルシューティングのトピックと手順への便利なリンクを提供します。
- ヘルスアラート：ヘルスアラートモニターでは、デバイスの正常性を一目で確認できます。
- 時間範囲：さまざまなデバイス メトリック ウィンドウに表示される情報を制限するための調整可能な時間枠。
- デバイスメトリック：以下を含む、事前定義されたダッシュボード全体で分類されている、一連の主要な Firepower デバイスヘルスメトリック。
  - CPU：CPU 使用率。プロセス別および物理コア別の CPU 使用率を含みます。
  - Memory：デバイスのメモリ使用率。データプレーンと Snort のメモリ使用率を含みます。
  - Interfaces：インターフェイスのステータスおよび集約トラフィック統計情報。
  - Connections：接続統計（エレファントフロー、アクティブな接続数、ピーク接続数など）および NAT 変換カウント。
  - Snort：Snort プロセスに関連する統計情報。
  - ディスク使用率：パーティションごとのディスクサイズとディスク使用率を含む、デバイスのディスク使用率。
  - 重要なプロセス：プロセスの再起動や、CPU やメモリの使用率などのその他の選択されたヘルスモニターを含む、管理対象プロセスに関連する統計。

サポートされているデバイスメトリックの包括的なリストについては、「Cisco Secure Firewall Threat Defense Health Metrics」を参照してください。

システムの詳細の表示とトラブルシューティング

この手順を実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティアナリスト ユーザーである必要があります。

[システムの詳細（System Details）] セクションには、選択したデバイスの一般的なシステム情報が表示されます。そのデバイスのトラブルシューティング タスクを起動することもできます。

手順

ステップ 1 システム（⚙） > **[正常性（Health）]** > **[モニタ（Monitor）]** を選択します。

[Monitoring] ナビゲーションペインを使用して、デバイス固有の正常性モニターにアクセスします。

ステップ 2 デバイスリストで [展開（Expand）]（>） と [折りたたみ（Collapse）]（⌄） をクリックして、管理対象デバイスのリストを展開または折りたたみます。

ステップ 3 デバイスをクリックすると、デバイス固有のヘルスモニターが表示されます。

ステップ 4 [システムとトラブルシューティングの詳細を表示（View System & Troubleshooting Details）] のリンクをクリックします。

このパネルはデフォルトで折りたたまれています。リンクをクリックすると、折りたたまれたセクションが展開され、デバイスの [システムの詳細（System Details）] と [トラブルシューティングとリンク（Troubleshooting & Links）] が表示されます。システムの詳細は次のとおりです。

- [バージョン（Version）]：Firepower ソフトウェアのバージョン。
- [モデル（Model）]：デバイスのモデル。
- [モード（Mode）]：ファイアウォールのモード。Threat Defense は、通常のファイアウォール インターフェイスでルーテッドモードとトランスペアレントモードの 2 つのファイアウォールモードをサポートします。
- [VDB]：Cisco 脆弱性データベース（VDB）のバージョン。
- [SRU]：侵入ルールセットのバージョン。
- [Snort]：Snort のバージョン。

ステップ 5 次のトラブルシューティングの選択肢があります。

- トラブルシューティング ファイルを生成します（特定のシステム機能のトラブルシューティング ファイルの生成 （537 ページ）を参照）。
- 高度なトラブルシューティング ファイルを生成してダウンロードします（高度なトラブルシューティング ファイルのダウンロード （538 ページ）を参照）。
- 正常性ポリシーを作成および変更します（正常性ポリシーの作成（450ページ）を参照）。
- ヘルスモニターアラートを作成および変更します（ヘルス モニター アラートの作成 （465 ページ）を参照）。

デバイス正常性モニターの表示

この手順を実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティアナリスト ユーザーである必要があります。

デバイス正常性モニターには、ファイアウォールデバイスの正常性ステータスの詳細ビューが表示されます。デバイス正常性モニターは、デバイスメトリックをコンパイルし、一連のダッシュボードでデバイスの正常性ステータスとトレンドを提供します。

手順

ステップ 1 システム（⚙） > **[正常性（Health）]** > **[モニタ（Monitor）]** を選択します。

[Monitoring] ナビゲーションペインを使用して、デバイス固有の正常性モニターにアクセスします。

ステップ 2 デバイスリストで [展開（Expand）]（>） と [折りたたみ（Collapse）]（∨） をクリックして、管理対象デバイスのリストを展開または折りたたみます。

ステップ 3 ページ上部のデバイス名の右側にあるアラート通知で、デバイスの正常性アラートを確認します。

正常性アラートにポインタを合わせると、デバイスの正常性の概要が表示されます。ポップアップウィンドウに、上位5つの正常性アラートの概要の一部が表示されます。ポップアップをクリックすると、正常性アラート概要の詳細ビューが開きます。

ステップ 4 右上隅のドロップダウンで、時間範囲を設定できます。最短で1時間前（デフォルト）から、最長では 2 週間前からの期間を反映できます。ドロップダウンから [Custom] を選択して、カスタムの開始日と終了日を設定します。

更新アイコンをクリックして、自動更新を 5 分に設定するか、自動更新をオフに切り替えます。

ステップ 5 選択した時間範囲について、トレンドグラフの展開オーバーレイの **[グラフの最上部に展開の詳細を表示（Show the deployment details on top of the graph）]**（） アイコンをクリックします。

選択した時間範囲中の展開数をします**[グラフの最上部に展開の詳細を表示（Show the deployment details on top of the graph）]**（） アイコン。垂直の帯は、展開の開始時刻と終了時刻を示します。複数の展開の場合、複数の帯または線が表示されることがあります。展開の詳細を表示するには、点線の上部にあるアイコンをクリックします。

ステップ 6 デフォルトでは、デバイスモニターは、いくつかの事前定義されたダッシュボードで正常性およびパフォーマンスのメトリックを報告します。メトリックダッシュボードには次のものが含まれます。

- Overview：CPU、メモリ、インターフェイス、接続統計情報など、他の定義済みダッシュボードからの主要なメトリックを表示します。ディスク使用量と重要なプロセス情報も含まれます。
- CPU：CPU 使用率。プロセス別および物理コア別の CPU 使用率を含みます。
- Memory：デバイスのメモリ使用率。データプレーンと Snort のメモリ使用率を含みます。
- Interfaces：インターフェイスのステータスおよび集約トラフィック統計情報。

- Connections：接続統計（エレファントフロー、アクティブな接続数、ピーク接続数など）および NAT 変換カウント。
- Snort：Snort プロセスに関連する統計情報。
- [ASP Drops]：高速セキュリティパス（ASP）のパフォーマンスと動作に関連する統計情報。

ラベルをクリックすると、さまざまなメトリックダッシュボードに移動できます。サポートされているデバイスメトリックの包括的なリストについては、「Cisco Secure Firewall Threat Defense Health Metrics」を参照してください。

ステップ 7 **[新しいダッシュボードの追加（Add New Dashboard）]**（[+]）をクリックして、使用可能なメトリックグループから独自の変数セットを構成し、カスタム相関ダッシュボードを作成します。デバイスメトリックの相関分析 （476 ページ）を参照してください。

デバイスメトリックの相関分析

デバイス正常性モニターには、システムイベントを予測して対応するのに役立つ、一連の主要 Threat Defense デバイスメトリックが含まれています。Threat Defense デバイスの正常性は、これらの報告されたメトリックによって判断できます。

デフォルトでは、デバイスモニターは、いくつかの事前定義されたダッシュボードでこれらのメトリックを報告します。これらのダッシュボードには次のものがあります。

- Overview：CPU、メモリ、インターフェイス、接続統計情報など、他の定義済みダッシュボードからの主要なメトリックを表示します。ディスク使用量と重要なプロセス情報も含まれます。
- CPU：CPU 使用率。プロセス別および物理コア別の CPU 使用率を含みます。
- Memory：デバイスのメモリ使用率。データプレーンと Snort のメモリ使用率を含みます。
- Interfaces：インターフェイスのステータスおよび集約トラフィック統計情報。
- Connections：接続統計（エレファントフロー、アクティブな接続数、ピーク接続数など）および NAT 変換カウント。
- Snort：Snort プロセスに関連する統計情報。
- [ASP Drops]：高速セキュリティパス（ASP）のパフォーマンスと動作に関連する統計情報。

カスタムダッシュボードを追加して、相互に関連するメトリックの相関性を示すことができます。CPU や Snort などの事前定義された相関グループから選択します。または、使用可能なメトリックグループから独自の変数セットを作成して、カスタム相関ダッシュボードを作成します。サポートされているデバイスメトリックの包括的なリストについては、「Cisco Secure Firewall Threat Defense Health Metrics」を参照してください。

始める前に

- ヘルス モニター ダッシュボードで時系列データ（デバイスメトリック）を表示して関連付けるには、REST API を有効にします（**[Settings]** > **[Configuration]** > **[REST API Preferences]**）。
- この手順を実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティ アナリスト ユーザーである必要があります。

（注） デバイスメトリックの相関分析は、Threat Defense 6.7 以降のバージョンでのみ利用可能です。したがって、6.7 以前の Threat Defense バージョンでは、REST API を有効にしてもヘルス モニタリング ダッシュボードにはこれらのメトリックが表示されません。

手順

ステップ 1 システム（⚙） > **[正常性（Health）]** > **[モニタ（Monitor）]** を選択します。

[Monitoring] ナビゲーションペインを使用して、デバイス固有の正常性モニターにアクセスします。

ステップ 2 [デバイス（Devices）] リストで [展開（Expand）]（>） と [折りたたみ（Collapse ）]（⌄）をクリックして、管理対象デバイスのリストを展開または折りたたみます。

ステップ 3 ダッシュボードを変更するデバイスを選択します。

ステップ 4 [新しいダッシュボードの追加（Add New Dashboard）]（+）アイコンをクリックして、新しいダッシュボードを追加します。

ステップ 5 ダッシュボードを識別する名前を指定します。

ステップ 6 事前定義された相関グループからダッシュボードを作成するには、[事前定義された相関から追加（Add from Predefined Correlations）] ドロップダウンをクリックし、グループを選択して [ダッシュボードの追加（Add Dashboard）] をクリックします。

ステップ 7 カスタム相関ダッシュボードを作成するには、[メトリックグループの選択（Select Metric Group）] ドロップダウンからグループを選択し、[メトリックの選択（Select Metrics）] ドロップダウンから対応するメトリックを選択します。

サポートされているデバイスメトリックの包括的なリストについては、「Cisco Secure Firewall Threat Defense Health Metrics」を参照してください。

ステップ 8 [Add Metrics] をクリックして、別のグループからメトリックを追加して選択します。

ステップ 9 個別のメトリックを削除するには、項目の右側にある [x] アイコンをクリックします。削除アイコンをクリックしてグループ全体を削除します。

ステップ 10 **[ダッシュボードの追加（Add Dashboard）]** をクリックし、ダッシュボードを正常性モニターに追加します。

ステップ 11 事前定義されたダッシュボードとカスタム相関ダッシュボードは、**編集**または**削除**が可能です。

Cluster Health Monitor

Threat Defense がクラスタの制御ノードである場合、Management Center はデバイス メトリック データ コレクタからさまざまなメトリックを定期的に収集します。クラスタのヘルスモニターは、次のコンポーネントで構成されています。

- 概要ダッシュボード：クラスタトポロジ、クラスタ統計、およびメトリックチャートに関する情報を表示します。
  - トポロジセクションには、クラスタのライブステータス、個々の脅威防御の状態、脅威防御ノードのタイプ（制御ノードまたはデータノード）、およびデバイスの状態が表示されます。デバイスの状態は、[無効（Disabled）]（デバイスがクラスタを離れたとき）、[初期状態で追加（Added out of box）]（パブリッククラウドクラスタで Management Center に属していない追加ノード）、または [標準（Normal）]（ノードの理想的な状態）のいずれかです。
  - クラスタの統計セクションには、CPU使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、および NAT 変換数に関するクラスタの現在のメトリックが表示されます。

（注） CPU とメモリのメトリックは、データプレーンと Snort の使用量の個々の平均を示します。

  - メトリックチャート、つまり、CPU使用率、メモリ使用率、スループット、および接続数は、指定された期間におけるクラスタの統計を図表で示します。
- 負荷分散ダッシュボード：2 つのウィジェットでクラスタノード全体の負荷分散を表示します。
  - 分布ウィジェットには、クラスタノード全体の時間範囲における平均パケットおよび接続分布が表示されます。このデータは、ノードによって負荷がどのように分散されているかを示します。このウィジェットを使用すると、負荷分散の異常を簡単に特定して修正できます。
  - ノード統計ウィジェットには、ノードレベルのメトリックが表形式で表示されます。クラスタノード全体の CPU 使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、および NAT 変換数に関するメトリックデータが表示されます。このテーブルビューでは、データを関連付けて、不一致を簡単に特定できます。
- メンバー パフォーマンス ダッシュボード：クラスタノードの現在のメトリックを表示します。セレクタを使用してノードをフィルタリングし、特定ノードの詳細を表示できま

す。メトリックデータには、CPU使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、およびNAT変換数が含まれます。

- CCLダッシュボード：クラスタの制御リンクデータ、つまり入力レートと出力レートをグラフ形式で表示します。
- トラブルシューティングとリンク：頻繁に使用されるトラブルシューティングのトピックと手順への便利なリンクを提供します。
- 時間範囲：さまざまなクラスタ メトリック ダッシュボードやウィジェットに表示される情報を制限するための調整可能な時間枠。
- カスタムダッシュボード：クラスタ全体のメトリックとノードレベルのメトリックの両方に関するデータを表示します。ただし、ノードの選択は脅威防御メトリックにのみ適用され、ノードが属するクラスタ全体には適用されません。

クラスタのヘルスモニターの表示

この手順を実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティアナリスト ユーザーである必要があります。

クラスタヘルスモニターは、クラスタとそのノードのヘルスステータスの詳細なビューを提供します。このクラスタヘルスモニターは、一連のダッシュボードでクラスタのヘルスステータスと傾向を提供します。

始める前に

- Management Center の 1 つ以上のデバイスからクラスタを作成しているかを確認します。

手順

ステップ 1 システム（⚙） > **[正常性（Health）]** > **[モニタ（Monitor）]** を選択します。

[モニタリング（Monitoring）] ナビゲーションウィンドウを使用して、ノード固有のヘルスモニターにアクセスします。

ステップ 2 デバイスリストで [展開（Expand）]（>） と [折りたたみ（Collapse）]（⌄） をクリックして、管理対象のクラスタデバイスのリストを展開または折りたたみます。

ステップ 3 クラスタのヘルス統計を表示するには、クラスタ名をクリックします。デフォルトでは、クラスタモニターは、いくつかの事前定義されたダッシュボードで正常性およびパフォーマンスのメトリックを報告します。メトリックダッシュボードには次のものが含まれます。

- [概要（Overview）]：他の事前定義されたダッシュボードからの主要なメトリックを表示します。ノード、CPU、メモリ、入力レート、出力レート、接続統計情報、NAT変換情報などが含まれます。
- [負荷分散（Load Distribution）]：クラスタノード間のトラフィックとパケットの分散。

- [メンバーパフォーマンス（Member Performance）]：CPU 使用率、メモリ使用率、入力スループット、出力スループット、アクティブな接続、および NAT 変換に関するノードレベルの統計情報。
- [CCL]：インターフェイスのステータスおよび集約トラフィックの統計情報。

ラベルをクリックすると、さまざまなメトリックダッシュボードに移動できます。サポートされているクラスタメトリックの包括的なリストについては、「Cisco Secure Firewall Threat Defense Health Metrics」を参照してください。

ステップ 4 右上隅のドロップダウンで、時間範囲を設定できます。最短で1時間前（デフォルト）から、最長では 2 週間前からの期間を反映できます。ドロップダウンから [Custom] を選択して、カスタムの開始日と終了日を設定します。

更新アイコンをクリックして、自動更新を 5 分に設定するか、自動更新をオフに切り替えます。

ステップ 5 選択した時間範囲について、トレンドグラフの展開オーバーレイの展開アイコンをクリックします。

展開アイコンは、選択した時間範囲内の展開数を示します。垂直の帯は、展開の開始時刻と終了時刻を示します。複数の展開の場合、複数の帯または線が表示されます。展開の詳細を表示するには、点線の上部にあるアイコンをクリックします。

ステップ 6 （ノード固有のヘルスモニターの場合）ページ上部のデバイス名の右側にあるアラート通知で、ノードの正常性アラートを確認します。

正常性アラートにポインタを合わせると、ノードの正常性の概要が表示されます。ポップアップウィンドウに、上位5つの正常性アラートの概要の一部が表示されます。ポップアップをクリックすると、正常性アラート概要の詳細ビューが開きます。

ステップ 7 （ノード固有のヘルスモニターの場合）デフォルトでは、デバイスモニターは、いくつかの事前定義されたダッシュボードで正常性およびパフォーマンスのメトリックを報告します。メトリックダッシュボードには次のものが含まれます。

- Overview：CPU、メモリ、インターフェイス、接続統計情報など、他の定義済みダッシュボードからの主要なメトリックを表示します。ディスク使用量と重要なプロセス情報も含まれます。
- CPU：CPU 使用率。プロセス別および物理コア別の CPU 使用率を含みます。
- Memory：デバイスのメモリ使用率。データプレーンと Snort のメモリ使用率を含みます。
- Interfaces：インターフェイスのステータスおよび集約トラフィック統計情報。
- Connections：接続統計（エレファントフロー、アクティブな接続数、ピーク接続数など）および NAT 変換カウント。
- [Snort]：Snort プロセスに関連する統計情報。
- [ASP ドロップ（ASP drops）]：さまざまな理由でドロップされたパケットに関連する統計情報。

ラベルをクリックすると、さまざまなメトリックダッシュボードに移動できます。サポートされているデバイスメトリックの包括的なリストについては、「Cisco Secure Firewall Threat Defense Health Metrics」を参照してください。

ステップ 8 ヘルスモニターの右上隅にあるプラス記号（[+]）をクリックして、使用可能なメトリックグループから独自の変数セットを構成し、カスタムダッシュボードを作成します。

クラスタ全体のダッシュボードの場合は、クラスタのメトリックグループを選択してから、メトリックを選択します。

ヘルス モニター ステータスのカテゴリ

使用可能なステータス カテゴリを、シビラティ（重大度）別に次の表に示します。

表 33 : ヘルス ステータス インジケータ

ステータス レベル	ステータス アイコン	円グラフのステータスの色	説明
エラー（Error）	[エラー（Error）]（  ）	黒色	アプライアンス上の 1 つ以上のヘルス モニタリング モジュールで障害が発生し、それ以降、正常に再実行していないことを示します。テクニカル サポート担当者に連絡して、ヘルス モニタリング モジュールの更新プログラムを入手してください。
クリティカル	[クリティカル（Critical）]（  ）	赤	アプライアンス上の1つ以上のヘルス モジュールが重大制限を超え、問題が解決されていないことを示します。
警告	[警告（Warning）]（  ）	黄	アプライアンス上の1つ以上のヘルス モジュールが警告制限を超え、問題が解決されていないことを示します。 このステータスは、デバイス構成の変更が原因で、必要なデータが一時的に利用できないか処理できなかったという過渡的な状態も示しています。モニタリングサイクルに応じて、この過渡状態は自動修正されます。
標準	[標準（Normal）]（）	緑	アプライアンス上のすべてのヘルス モジュールがアプライアンスに適用された正常性ポリシーで設定された制限内で動作していることを示します。

ステータス レベル	ステータス アイコン	円グラフのステータスの色	説明
Recovered	[回復済み（Recovered）]（  ）	緑	アプライアンス上のすべてのヘルス モジュールがアプライアンスに適用された正常性ポリシーで設定された制限内で動作していることを示します。これには、前に Critical または Warning 状態だったモジュールも含まれます。
無効	[無効（Disabled）]（  ）	青	アプライアンスが無効または除外されている、アプライアンスに正常性ポリシーが適用されていない、またはアプライアンスが現在到達不能になっていることを示します。

ヘルス イベント ビュー

[ヘルス イベント ビュー（Health Event View）] ページでは、ヘルス モニタがログに記録したヘルス イベントを、Management Center ログ ヘルス イベントで表示できます。完全にカスタマイズ可能なイベント ビューを使用すれば、ヘルス モニタによって収集されたヘルス ステータス イベントを迅速かつ容易に分析できます。イベント データを検索して、調査中のイベントに関係する可能性のある他の情報に簡単にアクセスしたりできます。ヘルス モジュールごとにテストされる条件を理解していれば、ヘルス イベントに対するアラートをより効率的に設定できます。

ヘルス イベント ビュー ページで多くの標準イベント ビュー機能を実行できます。

ヘルス イベントの表示

この手順を実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティ アナリスト ユーザーである必要があります。

[ヘルス イベントのテーブル ビュー（Table View of Health Events）] ページには、指定したアプライアンス上のすべてのヘルス イベントのリストが表示されます。

Management Center 上の [ヘルス モニター（Health Monitor）] ページからヘルス イベントにアクセスした場合は、すべての管理対象アプライアンスのすべてのヘルス イベントが表示されます。

ヒント このビューをブックマークすれば、イベントの [ヘルス イベント（Health Events）] テーブルを含むヘルス イベント ワークフロー内のページに戻ることができます。ブックマークしたビューには、現在見ている時間範囲内のイベントが表示されますが、必要に応じて時間範囲を変更してテーブルを最新情報で更新することができます。

手順

システム（⚙） > **[正常性（Health）]** > **[イベント（Events）]**を選択します。

ヒント ヘルス イベントのテーブル ビューが含まれていないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックします。[ワークフローの選択（Select Workflow）] ページで、[ヘルス イベント（Health Events）] をクリックします。

（注） イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください。

モジュール/アプライアンス別のヘルス イベントの表示

手順

ステップ 1 アプライアンスのヘルス モニターを表示します（デバイス正常性モニターの表示 （474 ページ）を参照）。

ステップ 2 [モジュール ステータスの概要（Appliance Status Summary）] グラフで、表示するイベント ステータス カテゴリの色をクリックします。

[アラート詳細（Alert Detail）] リストで、表示を切り替えてイベントを表示または非表示にします。

ステップ 3 イベントのリストを表示するアラートの [アラート詳細（Alert Detail）] 行で、[イベント（Events）] をクリックします。

[ヘルス イベント（Health Events）] ページが開いて、制限としてアプライアンスの名前と指定したヘルス アラート モジュールの名前を含むクエリーの結果が表示されます。イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください。

ステップ 4 指定したアプライアンスのすべてのステータス イベントを表示する場合は、[検索制約（Search Constraints）] を展開し、[モジュール名（Module Name）] 制限をクリックして削除します。

ヘルス イベント テーブルの表示

ヘルスイベントテーブルを表示および変更できます。

手順

ステップ 1 システム（⚙） > **[正常性（Health）]** > **[イベント（Events）]**を選択します。

ステップ 2 次の選択肢があります。

- ブックマーク：すぐに現在のページに戻れるように、現在のページをブックマークするには、[このページのブックマーク（Bookmark This Page）] をクリックしてブックマークの名前を指定し、[保存（Save）] をクリックします。
- ワークフローの変更：別のヘルスイベントワークフローを選択するには、[(ワークフローの切り替え)（(switch workflow)）] をクリックします。
- イベントの削除：ヘルスイベントを削除するには、削除するイベントの横にあるチェックボックスをオンにして、[削除（Delete）] をクリックします。現在の制約されているビューですべてのイベントを削除するには、[すべて削除（Delete All）] をクリックしてから、すべてのイベントを削除することを確認します。
- レポートの生成：テーブル ビューのデータに基づいてレポートを生成するには、[レポート デザイナ（Report Designer）] をクリックします。
- 変更：ヘルス テーブル ビューに表示されるイベントの時刻と日付範囲を変更します。イベントビューを時間で制約している場合は、（グローバルであるかイベントに特有であるかに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベントビューに表示されることがあることに注意してください。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。
- 移動：イベント ビュー ページを使用して移動します。
- ブックマークの移動：ブックマーク管理ページに移動するには、任意のイベントビューから [ブックマークの表示（View Bookmarks）] をクリックします。
- その他に移動：他のイベント テーブルに移動して関連イベントを表示します。
- ソート：表示されたイベントをソートする、イベントテーブルに表示するカラムを変更する、または表示するイベントを制約します。
- すべて表示：すべてのイベントのイベントの詳細をビューに表示するには、[すべて表示（View All）] をクリックします。
- 詳細の表示：単一のヘルスイベントに関連付けられる詳細を表示するには、イベントの左側にある下矢印のリンクをクリックします。
- 複数表示：複数のヘルスイベントのイベント詳細を表示するには、詳細を表示するイベントに対応する行の横にあるチェックボックスをオンにして、[表示（View）] をクリックします。
- ステータスの表示：特定のステータスのすべてのイベントを表示するには、そのステータスのイベントの [ステータス（Status）] 列のステータスをクリックします。

[ヘルス イベント（Health Events）] テーブル

正常性ポリシー内で有効にされたヘルス モニタ モジュールが、さまざまなテストを実行してアプライアンスのヘルス ステータスを特定します。ヘルス ステータスが指定された基準を満たしている場合は、ヘルス イベントが生成されます。

次の表で、ヘルスイベントテーブルで表示および検索できるフィールドについて説明します。

表 *34 :* ヘルス イベント フィールド

フィールド	説明
モジュール名（Module Name）	表示するヘルスイベントを生成したモジュールの名前を指定します。たとえば、CPU パフォーマンスを測定するイベントを表示するには、「CPU」と入力します。検索によって、該当する CPU 使用率イベントと CPU 温度イベントが取得されます。
テスト名（Test Name） （検索専用）	イベントを生成したヘルス モジュールの名前。
時刻（Time） （検索専用）	ヘルス イベントのタイムスタンプ。
説明	イベントを生成したヘルスモジュールの説明。たとえば、プロセスが実行できない場合に生成されるヘルス イベントには [実行不可（Unable to Execute）] というラベルが付けられます。
値	イベントが生成されたヘルス テストから得られた結果の値（単位数）。 たとえば、モニター対象デバイスが 80% 以上の CPU リソースを使用しているときに生成されるヘルスイベントをManagement Centerが生成した場合の値は 80 ～ 100 です。
単位（Units）	結果の単位記述子。アスタリスク（*）を使用してワイルドカード検索を作成できます。 たとえば、モニター対象デバイスが 80% 以上の CPU リソースを使用しているときに生成されるヘルスイベントをManagement Centerが生成した場合の単位記述子はパーセント記号（%）です。
ステータス（Status）	アプライアンスに報告されるステータス（Critical、Yellow、Green、または Disabled）。
Device	ヘルス イベントが報告されたアプライアンス。

ヘルス モニタリングの履歴

表 *35*：

機能	最小 Management Center	最小 Threat Defense	詳細
Management Center メモリ使用量モジュールのデフォルトのしきい値を更新しました。	7.4.1	任意（Any）	Management Center のメモリ使用量の警告と重大アラームのデフォルトのしきい値が、それぞれ 88% と 90% に設定されました。 新規/変更された画面：**システム**（⚙）> **[正常性（Health）]** > **[ポリシー（Policy）]** > **[Firewall Management Center正常性ポリシー（Firewall Management Center Health Policy）]** > **[正常性モジュール（Health Modules）]** > **[メモリ使用量（Memory Usage）]**を編集します。
Management Center のメモリ使用量の計算が改善されました。	7.4.1	任意（Any）	Management Center のメモリ使用量モジュールは、メモリ使用量を計算するときに使用可能なスワップメモリとキャッシュメモリの量を考慮して、メモリ使用量を正確に判断し、正常性アラートを送信します。 新規/変更された画面：**システム**（⚙）> **[正常性（Health）]** > **[モニター（Monitor）]** > **[Firewall Management Center]** > **[新しいダッシュボードの追加（Add New Dashboard）]**。
NTP サーバーの同期の問題に関する正常性アラート。	7.4.1	任意（Any）	Cisco Secure Firewall Management Center の正常性ポリシーに **Time Sever Status** モジュールが導入されました。有効にすると、このモジュールは NTP サーバーの設定をモニターし、NTP サーバーが使用できない場合、または NTP サーバーの設定が無効な場合にアラートを出します。 新規/変更された画面：**システム**（⚙）> **[正常性（Health）]** > **[ポリシー（Policy）]** > **[Firewall Management Center正常性ポリシー（Firewall Management Center Health Policy）]** > **[正常性モジュール（Health Modules）]** > **[時刻の同期（Time Synchronization）]**。
OpenConfig を使用して、テレメトリを外部サーバーにストリーミング。	7.4	7.4	OpenConfig を使用して、メトリックとヘルスモニタリング情報を Threat Defense デバイスから外部サーバー（gNMI コレクタ）に送信できるようになりました。TLS により暗号化された接続を開始するように Threat Defense またはコレクタを設定できます。 新規/変更された画面：**システム**（⚙）> **[正常性（Health）]** > **[ポリシー（Policy）]** > **[Firewall Threat Defenseポリシー（Firewall Threat Defense Policies）]** > **[設定（Settings）]** > **[OpenConfigストリーミングテレメトリ（OpenConfig Streaming Telemetry）]**。

機能	最小 Management Center	最小 Threat Defense	詳細
ヘルスモニターの使いやすさの強化。	7.4	任意（Any）	カスタムダッシュボードを簡単に作成できる [新しいダッシュボードの追加（Add New Dashboard）] ダイアログボックスの改善。事前定義された Device Health 監視ダッシュボードを編集または削除するオプションが含まれています。 新規/変更された画面：**システム**（⚙）> **[正常性（Health）]** > **[モニター（Monitor）]** > **[デバイス（Devices）]** > **[新しいダッシュボードの追加（Add New Dashboard）]**。
新しいクラスタヘルスモニターダッシュボード。	7.3	任意（Any）	クラスタヘルスモニターメトリックを表示するための新しいダッシュボードが、次のコンポーネントで導入されました。 • [概要（Overview）]：クラスタトポロジ、クラスタ統計、およびメトリックチャートに関する情報を表示します。 • [負荷分散（Load Distribution）]：クラスタノード間の負荷分散を表示します。 • [メンバーパフォーマンス（Member Performance）]：クラスタのすべてのメンバーノードの現在のメトリックを表示します。 • [CCL]：クラスタの制御リンクデータ、つまり入力レートと出力レートをグラフ形式で表示します。 （注） これらの機能は、クラスタでのみ使用できます。したがって、クラスタダッシュボードを表示して使用するには、[モニタリング（Monitoring）] ペインの [デバイス（Devices）] リストでクラスタを選択する必要があります。 新規/変更された画面：**システム**（⚙）> **[正常性（Health）]** > **[モニター（Monitor）]**。

機能	最小 Management Center	最小 Threat Defense	詳細
新しいハードウェア統計モジュール。	7.3	任意（Any）	Management Center ハードウェアと環境のステータス統計がヘルス モニター ダッシュボードに追加されました。 • Management Center ハードウェアでハードウェアデーモンのモニタリングを有効にするために、新しいポリシーモジュールである [ハードウェア統計（Hardware Statistics）] が導入されました。メトリックには、ファン速度、温度、および電源が含まれました。 • モニタリングダッシュボードにハードウェアの正常性メトリックをグラフィカルに表示するためのカスタムメトリックグループの [ハードウェア統計（Hardware Statistics）] も追加されました。 • 電源ステータスは、Management Center の**正常性アラート**でキャプチャされます。 （注） これらの機能は、Management Center にのみ適用されるため、Management Center ダッシュボードでのみ使用できます。 新規/変更された画面： • **システム**（⚙） > **[正常性（Health）]** > **[モニター（Monitor）]** • **システム**（⚙） > **[正常性（Health）]** > **[ポリシー（Policy）]**
新しいハードウェアと環境のステータス メトリック グループ。	7.3	任意（Any）	Threat Defense ハードウェアと環境のステータス統計がヘルス モニター ダッシュボードに追加されました。 • Threat Defense に関するハードウェア関連の統計情報を表示するために、カスタムメトリックグループの [ハードウェア/環境ステータス（Hardware / Environment Status）] が導入されました。メトリックには、ファン速度、シャーシ温度、SSD ステータス、および電源が含まれました。 • デバイスの**正常性アラート**が拡張され、Threat Defense ハードウェアの電源ステータスが含まれるようになりました。異常な温度ステータスの場合は重大アラートが表示され、通常の温度ステータスの場合は正常アラートが表示されます。 （注） これらの機能は、Threat Defense でのみ使用できます。したがって、[モニタリング（Monitoring）] ペインの [デバイス（Devices）] リストで適切なデバイスを選択する必要があります。 新規/変更された画面：**システム**（⚙） > **[正常性（Health）]** > **[モニター（Monitor）]**。

機能	最小 Management Center	最小 Threat Defense	詳細
ヘルスモニターの使いやすさの強化。	7.1	任意（Any）	次の UI ページが改善され、データの使いやすさとプレゼンテーションが向上しました。 • ポリシー（Policy） • 除外（Exclude） • モニターアラート 新規/変更された画面： • **システム（⚙） > [正常性（Health）] > [ポリシー（Policy）]** • **システム（⚙） > [正常性（Health）] > [除外（Exclude）]** • **システム（⚙） > [正常性（Health）] > [アラートの監視（Monitor Alerts）]**
エレファントフローの検出。	7.1	任意（Any）	ヘルスモニターには、次の拡張機能が含まれます。 • 接続統計情報には、アクティブなエレファントフローが含まれます。 • 接続グループメトリックには、アクティブなエレファントフローの数が含まれます。 エレファントフロー検出機能は、Cisco Firepower 2100 シリーズではサポートされていません。
アンマネージドディスク使用率が高いアラートは廃止されました。	7.0.6	任意（Any）	ディスク使用状況モジュールは、管理対象外のディスク使用率が高い場合にアラートを出さなくなりました。アップグレード後も、正常性ポリシーを管理対象デバイスに展開する（アラートの表示を停止する）か、デバイスをアップグレードする（アラートの送信を停止する）まで、これらのアラートが表示され続ける場合があります。 （注） バージョン 7.0 ～ 7.0.5、7.1.x、7.2.0 ～ 7.2.3、および 7.3.x は、引き続きこれらのアラートをサポートします。Management Center がこれらのバージョンのいずれかを実行している場合、アラートが引き続き表示される場合があります。

機能	最小 Management Center	最小 Threat Defense	詳細
新しいヘルス モジュール。	7.0	任意（Any）	

機能	最小 Management Center	最小 Threat Defense	詳細
			次の正常性モジュールが追加されました。 • [Cisco Advanced Malware Protection接続ステータス（AMP Connection Status）]：Threat Defense からの Cisco Advanced Malware Protection クラウド接続をモニターします。 • [AMP Threat Gridのステータス（AMP Threat Grid Status）]：Threat Defense からの AMP Threat Grid クラウド接続をモニターします。 • [ASPドロップ（ASP Drop）]：データプレーンの高速セキュリティ パスによってドロップされた接続をモニターします。 • [高度なSnort統計情報（Advanced Snort Statistics）]：パケットパフォーマンス、フローカウンタ、およびフローイベントに関連する Snort 統計情報をモニターします。 • [イベントストリームステータス（Event Stream Status）]：イベントストリーマを使用するサードパーティ製クライアント アプリケーションへの接続をモニターします • [FMCアクセス設定の変更（FMC Access Configuration Changes）]：Management Center で直接加えられたアクセス設定の変更をモニターします。 • [FMC HAステータス（FMC HA Status）]：アクティブおよびスタンバイ Management Center と、デバイス間の同期ステータスをモニターします。[HAステータス（HA Status）] モジュールと置き換わります。 • [FTD HAステータス（FTD HA Status）]：アクティブおよびスタンバイ Threat Defense HA ペアと、デバイス間の同期ステータスをモニターします。 • [ファイルシステム整合性チェック（File System Integrity Check）]：システムで CC モードまたは UCAPL モードが有効になっている場合、ファイルシステム整合性チェックを実行します。 • [フローオフロード（Flow Offload）]：Firepower 9300 および 4100 プラットフォームのハードウェア フロー オフロード統計をモニターします。 • [ヒットカウント（Hit Count）]：アクセス コントロール ポリシーで特定のルールがヒットした回数をモニターします。 • [MySQLのステータス（MySQL Status）]：MySQL データベースのステータスをモニターします。 • [NTP

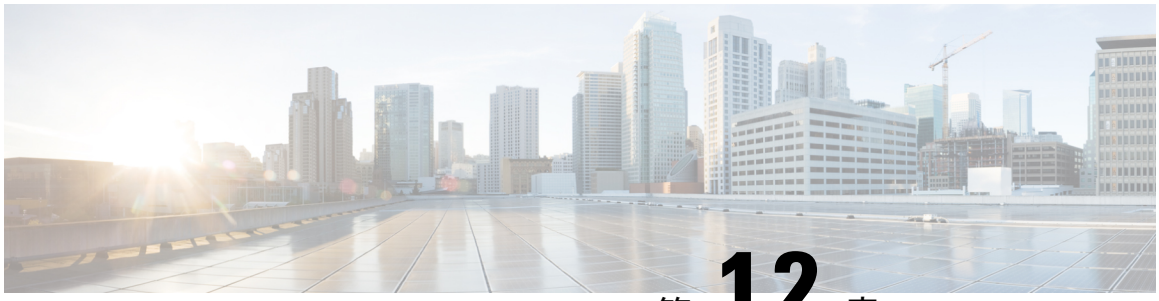
機能	最小 Management Center	最小 Threat Defense	詳細
			ステータスFTD（NTP Status FTD）]：管理対象デバイスのNTPクロック同期ステータスをモニターします。 • [RabbitMQステータス（RabbitMQ Status）]：RabbitMQメッセージングブローカのステータスをモニターします。 • [ルーティング統計情報（Routing Statistics）]：Threat Defense からの IPv4 と IPv6 の両方のルート情報をモニターします。 • [セキュリティサービス交換接続ステータス（Security Services Exchange Connection Status）]：Threat Defense からのセキュリティサービス交換クラウド接続をモニターします。 • [Sybaseのステータス（Sybase Status）]：Sybaseデータベースのステータスをモニターします。 • [未解決グループモニター（Unresolved Groups Monitor）]：アクセスコントロールポリシーで使用される未解決グループをモニターします。 • [VPN統計（VPN Statistics）]：サイト間およびリモートアクセスの VPN トンネルの統計をモニターします。 • [xTLSカウンタ（xTLS Counters）]：xTLS/SSL フロー、メモリ、およびキャッシュの有効性をモニターします。

機能	最小 Management Center	最小 Threat Defense	詳細
ヘルスモニターの機能拡張。	7.0	任意（Any）	ヘルスモニターには、次の機能拡張が追加されています。 • 次の概要ビューを備え、機能強化された Management Center ダッシュボード： • ハイ アベイラビリティ • イベントレートとキャパシティ • プロセスの正常性 • CPU しきい値 • メモリ • インターフェイスレート • ディスク使用率（Disk Usage） • 機能強化された Threat Defense ダッシュボード： • スプリットブレインシナリオのヘルスアラート • 新しいヘルスモジュールから使用できる追加のヘルスメトリック

機能	最小 Management Center	最小 Threat Defense	詳細
新しいヘルス モジュール。	6.7	任意（Any）	[CPU使用率（CPU Usage）] モジュールは使用されなくなりました。CPU 使用率については、代わりに次のモジュールを参照してください。 • CPU使用率（コアごと）：すべてのコアのCPU使用率をモニターします。 • CPU使用率データプレーン：デバイス上のすべてのデータプレーンプロセスの平均 CPU 使用率をモニターします。 • CPU 使用率 Snort：デバイス上の Snort プロセスの平均 CPU 使用率をモニターします。 • CPU使用率システム：デバイス上のすべてのシステムプロセスの平均 CPU 使用率をモニターします。 統計情報を追跡するために、次のモジュールが追加されました。 • [接続統計情報（Connection Statistics）]：接続統計情報と NAT 変換カウントをモニターします。 • クリティカルプロセス統計情報：クリティカルプロセスの状態、リソース消費量、再起動回数をモニターします。 • 展開された設定の統計情報：展開された設定に関する統計情報（ACE の数や IPS ルールなど）をモニターします。 • [Snort統計情報（Snort Statistics）]：イベント、フロー、およびパケットの Snort 統計情報をモニターします。 メモリ使用率を追跡するために、次のモジュールが追加されました。 • [メモリ使用率データプレーン（Memory Usage Data Plane）]：データプレーンプロセスで使用される割り当て済みメモリの割合をモニターします。 • メモリ使用率 Snort：Snort プロセスによって使用される割り当て済みメモリの割合をモニターします。

機能	最小 Management Center	最小 Threat Defense	詳細
ヘルスモニターの機能拡張。	6.7	任意（Any）	ヘルスモニターには、次の機能拡張が追加されています。 • [正常性ステータス（Health Status）] サマリーページでは、Firepower Management Center と Management Center が管理するすべてのデバイスの正常性を一目で確認できます。 • [Monitoring] ナビゲーションペインでは、デバイス階層を移動できます。 • 管理対象デバイスは、個別に一覧表示されるか、該当する場合は地理位置情報、高可用性、またはクラスタステータスに基づいてグループ化されます。 • ナビゲーションペインから個々のデバイスのヘルスモニターを表示できます。 • 相互に関連するメトリックを相互に関連付けるカスタムダッシュボード。CPU や Snort などの事前定義された相関グループから選択します。または、使用可能なメトリックグループから独自の変数セットを作成して、カスタム相関ダッシュボードを作成します。
[デバイスでの脅威データの更新（Threat Data Updates on Devices）] モジュールへの機能の移動。	6.7	任意（Any）	[ローカルマルウェア分析（Local Malware Analysis）] モジュールは使用されなくなりました。この情報については、代わりに [デバイスでの脅威データの更新（Threat Data Updates on Devices）] モジュールを参照してください。 以前は [セキュリティインテリジェンス（Security Intelligence）] モジュールと [URLフィルタリング（URL Filtering）] モジュールによって提供されていた一部の情報が、[デバイスでの脅威データの更新（Threat Data Updates on Devices）] モジュールによって提供されるようになりました。
新しい正常性モジュール：[構成メモリ割り当て（Configuration Memory Allocation）]。	7.0 6.6.3	任意（Any）	バージョン 6.6.3 では、デバイスのメモリ管理が改善され、新しい正常性モジュールである [構成メモリ割り当て（Configuration Memory Allocation）] が導入されています。 このモジュールは、展開された設定のサイズに基づき、デバイスのメモリが不足するリスクがある場合にアラートを出します。アラートには、設定に必要なメモリ量と、使用可能なメモリ量を超過した量が示されます。アラートが出た場合は、設定を再評価してください。ほとんどの場合、アクセス制御ルールまたは侵入ポリシーの数または複雑さを軽減できます。

機能	最小 Management Center	最小 Threat Defense	詳細
URLフィルタリングモニターの改善。	6.5	任意（Any）	[URLフィルタリングモニター（URL Filtering Monitor）] モジュールは、Management Center が Cisco Cloud への登録に失敗した場合にアラートを出すようになりました。
URLフィルタリングモニターの改善。	6.4	任意（Any）	URL フィルタリング モニター アラートの時間しきい値を設定できるようになりました。
新しい正常性モジュール：デバイス上での脅威データの更新。	6.3	任意（Any）	新しいモジュールの [デバイス上での脅威データの更新（Threat Data Updates on Devices）] を追加しました。 このモジュールは、デバイスが脅威の検出に使用する特定のインテリジェンス データと設定が指定した時間内にデバイス上で更新されなかった場合にアラートを発行します。



第 12 章

監査と Syslog

次のトピックでは、システム上のアクティビティを監査する方法について説明します。

システム ログ

[システム ログ（System Log）]（syslog）ページには、アプライアンスのシステム ログ情報が表示されます。

システム上のアクティビティを2つの方法で監査できます。システムの一部であるアプライアンスによって、Webインターフェイスとユーザーとの対話のそれぞれに対して監査レコードが生成され、システム ステータス メッセージがシステムログに記録されます。

システム ログには、システムによって生成された各メッセージが表示されます。次の項目が順にリストされます。

- メッセージが生成された日付
- メッセージが生成された時刻
- メッセージを生成したホスト
- メッセージ自体

システム ログの表示

システム ログ情報はローカルな情報です。たとえば、Management Center を使用して、管理対象デバイスのシステム ログ内のシステム ステータス メッセージを見ることは**できません**。

UNIX ファイル検索ユーティリティ Grep で処理可能なほとんどの構文を使用してメッセージをフィルタ処理できます。つまり、パターン マッチング用に Grep 互換の正規表現を使用できます。

始める前に

システム統計を表示するには、管理者またはメンテナンスユーザーであり、グローバルドメインにいる必要があります。

手順

ステップ 1 システム（⚙） > **[モニタリング（Monitoring）]** > **[Syslog]**を選択します。

ステップ 2 システム ログ内で特定のメッセージ内容を検索するには、次のようにします。

a) システム ログ フィルタの構文（498 ページ）に記載されているように、フィルタのフィールドに単語またはクエリを入力します。

Grep 互換の検索構文のみがサポートされています。

例：

ユーザ名 ”Admin” を含むすべてのログ エントリを検索するには `Admin` を使用します。

11 月 27 日に生成されたすべてのログ エントリを検索するには、（`Nov 27` や `Nov*27` ではなく）`Nov[[:space:]]*27` または `Nov.*27` を使用します。

11 月 5 日のデバッグ情報の認証を含むすべてのログ エントリを検索するには、`Nov[[:space:]]*5.*AUTH.*DEBUG` を使用します。

b) 検索で大文字と小文字を区別するには、[大文字と小文字を区別する（Case-sensitive）] を選択します。（デフォルトでは、フィルタで大文字/小文字は区別されません。）

c) 入力した基準を満たしていないすべてのシステム ログ メッセージを検索するには、[除外（Exclusion）] を選択します。

d) **[移動（Go）]** をクリックします。

システム ログ フィルタの構文

次の表に、システム ログ フィルタで使用できる正規表現構文を示します。

表 *36:* システム ログ フィルタ構文

構文のコンポーネント	説明	例
。	任意の文字またはスペースと一致します	`Admi.` は、`Admin`、`AdmiN`、`Admi1`、および致します。
`[[:alpha:]]`	任意の英文字と一致します	`[[:alpha:]]dmin` は、`Admin`、`bdmin`、お と一致します
`[[:upper:]]`	任意の大文字の英文字と一致します	`[[:upper:]]dmin` は、`Admin`、`Bdmin`、お と一致します

構文のコンポーネント	説明	例
[[:lower:]]	任意の小文字の英文字と一致します	[[:lower:]]dmin は、admin、bdmin、と一致します
[[:digit:]]	任意の数字と一致します	[[:digit:]]dmin は、0dmin、1dmin、と一致します
[[:alnum:]]	任意の英数字と一致します	[[:alnum:]]dmin は、1dmin、admin、bdmin と一致します
[[:space:]]	タブを含む、任意のスペースと一致します	Feb[[:space:]]29 は 2 月 29 日のロ
*。	その前にある文字または式のゼロ個以上のインスタンスと一致します	ab* は、a、ab、abb、ca、cab、およ します [ab]* はすべてのものと一致します
?	ゼロ個または 1 つのインスタンスと一致します	ab? は、a または ab と一致します
\	これを使用すると、通常は正規表現構文と解釈される文字を検索できます	alert\? は、alert? と一致します

システム監査について

システムの一部であるアプライアンスによって、Webインターフェイスとユーザーとの対話のそれぞれに対して監査レコードが生成されます。

関連トピック

標準レポートの概要 （641 ページ）

監査レコード

Secure Firewall Management Center ユーザ アクティビティに関する読み取り専用の監査情報をログに記録します。監査ログは標準イベント ビューに表示され、監査ビュー内の任意の項目に基づいて監査ログ メッセージを表示、ソート、およびフィルタリングできます。監査情報を簡単に削除したり、それに関するレポートを作成したりすることができ、ユーザが行った変更に関する詳細なレポートを表示することもできます。

監査ログには最大 100,000 のエントリが保存されます。監査ログ エントリの数が 100,000 を超えると、アプライアンスは最も古いレコードをデータベースからプルーニングして、100,000 エントリまで数を削減します。

監査ログには、ログインエラーのユーザーまたは送信元 IP は表示されません。

- 誤ったパスワードを使用すると、送信元 IP は表示されません。

- ユーザーアカウントが存在しない場合、送信元 IP とユーザーの両方が表示されません。
- LDAP ユーザーの試行が失敗した場合、監査ログはトリガーされません。

関連トピック

Management Center の SSO ガイドライン （170 ページ）

監査レコードの表示

Management Center で、監査レコードのテーブルを表示できます。事前定義された監査ワークフローには、イベントを示す単一のテーブル ビューが含まれます。ユーザは検索する情報に応じてテーブル ビューを操作することができます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

始める前に

この手順を実行するには、管理者ユーザーである必要があります。

手順

ステップ 1 システム（⚙） > **[モニタリング（Monitoring）]** > **[監査（Audit）]** を使用して監査ログのワークフローにアクセスします。

ステップ 2 イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください。詳細については、イベント時間の制約 （829 ページ）を参照してください。

（注） イベント ビューを時間によって制約している場合は、（グローバルかイベントに特有かに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあります。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

ステップ 3 次の選択肢があります。

これらの選択肢は、検索制約の結果に基づいてのみ適用されます。たとえば、**正常性イベント**を検索すると、結果のビューページに [ワークフロー（Workflow）] オプションが表示されます。同様に、[脆弱性（Vulnerabilities）] テーブルビューを使用している場合にのみ、特定の脆弱性を表示するオプション（[表示（View）]（👁））が表示されます。

- テーブルのカラムの内容について詳しく調べるには、システム ログ （497 ページ）を参照してください。
- 現在のワークフロー ページでイベントをソートしたり、制限したりするには、テーブル ビュー ページの使用 （819 ページ）を参照してください。
- 現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。詳細については、ワークフローの使用 （809 ページ）を参照してください。

- ワークフローの次のページにドリルダウンするには、ドリルダウン ページの使用 （818 ページ）を参照してください。
- 特定の値で制約するには、行内の値をクリックします。ドリルダウンページで値をクリックすると、次のページに移動し、その値だけに制約されます。テーブル ビューの行内の値をクリックすると、テーブル ビューが制限され、次のページに**ドリルダウンされない**ことに注意してください。詳細については、イベント ビューの制約 （836 ページ）を参照してください。

  ヒント テーブル ビューでは、必ずページ名に「Table View」が含まれます。

- 監査レコードを削除するには、削除するイベントの横にあるチェックボックスをオンにして [削除（Delete）] をクリックするか、[すべて削除（Delete All）] をクリックして現在の制約されているビューにあるすべてのイベントを削除します。
- 現在のページにすぐに戻れるようにページをブックマークするには、[このページをブックマーク（Bookmark This Page）] をクリックします。詳細については、ブックマーク （841 ページ）を参照してください。
- ブックマークの管理ページに移動するには、[ブックマークの表示（View Bookmarks）] をクリックします。詳細については、ブックマーク （841 ページ）を参照してください。
- 現在のビューのデータに基づいてレポートを生成するには、[レポート（Reporting）] をクリックします。詳細については、「イベント ビューからのレポート テンプレートの作成 （647 ページ）」を参照してください。
- 監査ログに記録されたシステム変更の概要を表示するには、[メッセージ（Message）] 列の該当するイベントの横にある [比較（Compare）] をクリックします。詳細については、監査ログを使って変更を調査する （503 ページ）を参照してください。

関連トピック

イベント ビューの制約 （836 ページ）

監査ログのワークフロー フィールド

次の表で、表示および検索できる監査ログ フィールドについて説明します。

表 *37*：監査ログのフィールド

フィールド	説明
時刻（Time）	アプライアンスが監査レコードを生成した日時。
ユーザー（User）	監査イベントをトリガーしたユーザーのユーザー名。

フィールド	説明
サブシステム	監査レコードが生成されたときにユーザがたどったフル メニュー パス。たとえば、**システム**（⚙）>**[モニタリング（Monitoring）]**>**[監査（Audit）]**は、監査ログを表示するためのメニュー パスです。 メニュー パスが該当しない数少ないケースでは、[サブシステム（Subsystem）] フィールドにイベント タイプのみが表示されます。たとえば、**Login** はユーザのログイン試行を分類します。
メッセージ（Message）	ユーザが実行したアクション、またはユーザがページでクリックしたボタン。 たとえば、`Page View` は、[サブシステム（Subsystem）] に示されているページをユーザーが単に表示したことを意味します。`Save` は、ユーザーがページの [保存（Save）] ボタンをクリックしたことを意味します。 システムに対する変更は**比較アイコン**付きで表示され、アイコンをクリックすると変更の概要を確認することができます。
ソース IP	ユーザが使用したホストに関連付けられている IP アドレス。 注：このフィールドを検索する場合は、特定の IP アドレスを入力する必要があります。監査ログの検索で IP 範囲を使用することはできません。
ドメイン（Domain）	監査イベントがトリガーされたときのユーザーの現行ドメイン。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。
設定の変更（Configuration Change） （検索専用）	設定の変更の監査レコードを検索結果に表示するかどうかを指定します。(`yes` または `no`)
カウント（Count）	各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

関連トピック

イベントの検索 （845 ページ）

[監査イベント（Audit Events）] テーブル ビュー

イベント ビューのレイアウトを変更したり、ビュー内のイベントをフィールド値で制限したりできます。カラムを無効にする場合は、非表示にするカラム見出しの [閉じる（Close）]（✕）をクリックした後、表示されるポップアップウィンドウで [適用（Apply）] をクリックします。カラムを無効にすると、そのカラムは（後で元に戻さない限り）そのセッションの期間中は無効になります。最初のカラムを無効にすると、[カウント（Count）] カラムが追加されることに注意してください。

他のカラムを表示/非表示にしたり、無効になったカラムをビューに再び追加したりするには、該当するチェックボックスを選択またはクリアしてから [適用（Apply）] をクリックします。

テーブル ビューの行内の値をクリックすると、テーブル ビューが制約されます（ワークフロー内の次のページにはドリルダウンされません）。

ヒント　テーブル ビューでは、必ずページ名に「Table View」が含まれます。

関連トピック

ワークフローの使用　（809 ページ）

監査ログを使って変更を調査する

監査ログを使用して、一部のシステムの変更に関する詳細レポートを表示できます。これらのレポートは、現在のシステム設定を、サポートされている変更が行われる直前の設定と比較します。

[設定の比較（Compare Configurations）] ページには、変更前のシステム設定と、現在実行中の設定との違いが横並び形式で表示されます。監査イベント タイプ、最終変更時間、および変更を行ったユーザ名が、各設定の上のタイトル バーに表示されます。

2 つの設定の違いは次のように強調表示されます。

- 青は、強調表示されている設定項目が 2 つの設定間で異なっていることを示し、異なっている部分は赤のテキストで表示されます。
- 緑は、強調表示されている設定項目が一方の設定に含まれ、もう一方の設定には含まれないことを示します。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

始める前に

この手順を実行するには、管理者ユーザーである必要があります。

手順

ステップ 1　システム（⚙） > **[モニタリング（Monitoring）]** > **[監査（Audit）]**を選択します。

ステップ 2　[メッセージ（Message）] 列の該当する監査ログイベントの横にある [比較（Compare）] をクリックします。

ヒント タイトル バーの上の [前へ（Previous）] または [次へ（Next）] をクリックすると、個々の変更の間を移動できます。また、変更の概要が複数のページにまたがる場合は、右側のスクロール バーを使って追加の変更を表示できます。

監査レコードの抑制

監査ポリシーで、システム/ユーザー間の特定タイプのインタラクションを監査する必要がない場合は、それらのインタラクションによって、監査レコードが生成されないように設定できます。たとえば、デフォルトでは、ユーザーがオンラインヘルプを表示するたびに、システムは監査レコードを生成します。このようなインタラクションのレコードを保持する必要がない場合は、これらを自動的に抑制できます。

監査イベントの抑制を設定するには、アプライアンスの`admin`ユーザアカウントにアクセスできる必要があり、アプライアンスのコンソールにアクセスできる（またはセキュアシェルを開くことができる）必要があります。

注意 許可された担当者だけが、アプライアンスとその`admin`アカウントにアクセスできることを確認してください。

始める前に

この手順を実行するには、管理者ユーザーである必要があります。

手順

`/etc/sf`ディレクトリに、次の形式で 1 つ以上の`AuditBlock`ファイルを作成します。タイプは、監査ブロック タイプ （504 ページ）で説明されているいずれかのタイプになります。

`AuditBlock.type`

（注） 特定のタイプの監査メッセージに関する`AuditBlock.type`ファイルを作成した後で、それらの抑制を解除することにした場合、`AuditBlock.type`ファイルの内容を削除する必要がありますが、ファイル自体はシステムに残してください。

監査ブロック タイプ

それぞれの監査ブロック タイプの内容は、以下の表に記載されているように、特定の形式でなければなりません。ファイル名の大文字/小文字が正しいことを確認します。また、ファイルの内容でも大文字と小文字が区別されることに注意してください。

`AuditBlock`ファイルを追加した場合、サブシステム`Audit`およびメッセージ`Audit Filter`*type*`Changed`を含む監査レコードが監査イベントに追加されることに注意してください。セキュリティ上の理由から、この監査レコードを抑制することは**できません**。

表 *38*：監査ブロック タイプ

タイプ	説明
アドレス	`AuditBlock.address` という名前のファイルを作成し、監査ログから抑制する IP アドレスを 1 行に 1 つずつ含めます。アドレスの先頭からマッピングされる場合に限り、部分的な IP アドレスを使用できます。たとえば、部分的なアドレス `10.1.1` は、`10.1.1.0` から `10.1.1.255` までのアドレスと一致します。
メッセージ	`AuditBlock.message` という名前のファイルを作成し、抑制するメッセージ部分文字列を 1 行に 1 つずつ含めます。 たとえば`backup` をこのファイルに含めた場合、部分文字列の照合により `backup` という語を含むすべてのメッセージが抑制されることに注意してください。
サブシステム	`AuditBlock.subsystem` という名前のファイルを作成し、抑制するサブシステムを 1 行に 1 つずつ含めます。 部分文字列は照合**されない**ことに注意してください。正確な文字列を使用する必要があります。監査対象のサブシステムのリストについては、監査対象のサブシステム （505 ページ）を参照してください。
ユーザー	`AuditBlock.user` という名前のファイルを作成し、抑制するユーザアカウントを 1 行に 1 つずつ含めます。ユーザー名の先頭からマッピングされる場合に限り、部分的な文字列の照合を使用できます。たとえば、部分的なユーザー名 `IPSAnalyst` はユーザー名 `IPSAnalyst1` および `IPSAnalyst2` と一致します。

監査対象のサブシステム

次の表に、監査対象のサブシステムを示します。

表 *39*：サブシステム名

名前	何に関するユーザー インタラクションを含んでいるか
管理（Admin）	管理機能（システムとアクセス権の設定、時刻の同期、バックアップと復元、デバイス管理、ユーザーアカウントの管理、スケジュール設定など）
アラート（Alerting）	アラート機能（電子メール アラート、SNMP アラート、Syslog アラートなど）
監査ログ（Audit Log）	監査イベントの表示
監査ログ検索（Audit Log Search）	監査イベントの検索
コマンド ライン	コマンドライン インターフェイス
設定	電子メール アラート機能

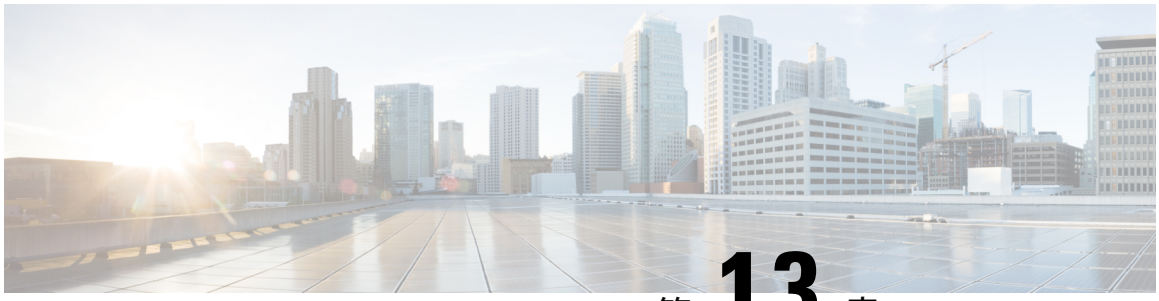
名前	何に関するユーザー インタラクションを含んでいるか
コンテキスト クロス起動	システムに追加された外部リソース、またはダッシュボードとイベント ビューからアクセスされた外部リソース
COOP	運用の継続性に関する機能
日付（Date）	イベント ビューの日時範囲
デフォルトのサブシステム（Default Subsystem）	サブシステムが割り当てられていないオプション
検出および防止ポリシー（Detection & Prevention Policy）	侵入ポリシーのメニュー オプション
エラー（Error）	システム レベルのエラー
eStreamer	eStreamer 構成
EULA	エンド ユーザ ライセンス契約書の確認
イベント	侵入および検出イベント ビュー
確認済みイベント（Events Reviewed）	確認済みの侵入イベント
イベント検索（Events Search）	あらゆるイベント検索
ルール更新のインストールの失敗（Failed to install rule update） `rule_update_id`	ルール更新のインストール
ヘッダー	ユーザー ログイン後のユーザー インターフェイスの初回表示
ヘルス	ヘルス モニタリング
ヘルス イベント（Health Events）	ヘルス モニタリング イベントの表示
ヘルプ	オンライン ヘルプ
高可用性	高可用性ペアでの Management Center の確立と処理
IDS インパクト フラグ（IDS Impact Flag）	侵入イベントの影響フラグの設定
IDS ポリシー（IDS Policy）	侵入ポリシー
IDS ルール SID：`sig_id` リビジョン：`rev_num`	SID 別の侵入ルール
インストール（Install）	更新のインストール

名前	何に関するユーザー インタラクションを含んでいるか
侵入イベント	侵入イベント
ログイン（Login）	Web インターフェイスのログイン/ログアウト機能
ログアウト	Web インターフェイス ログアウト機能
メニュー	あらゆるメニュー オプション
[設定のエクスポート（Configuration export）] > [config_type] > [config_name]	特定のタイプと名前の設定のインポート
権限のエスカレーション（Permission Escalation）	ユーザ ロールのエスカレーション
初期設定	ユーザー設定（ユーザー アカウントのタイム ゾーン、個々のイベント設定など）
ポリシー	侵入ポリシーを含む、あらゆるポリシー
登録	Management Center でのデバイスの登録
リモート ストレージ デバイス（RemoteStorageDevice）	リモート ストレージ デバイスの設定
レポート	レポート リスト機能およびレポート デザイナ機能
ルール（Rules）	侵入ルール（侵入ルール エディタとルールのインポート プロセスを含む）
ルール更新インポート ログ（Rule Update Import Log）	ルール更新インポート ログの表示
ルール更新インストール（Rule Update Install）	ルール更新のインストール
セッションの時間切れ	Web インターフェイスのセッション タイムアウト
ステータス（Status）	Syslog およびホストとパフォーマンスの統計
システム（System）	システム全体のさまざまな設定
タスク キュー（Task Queue）	バックグラウンド プロセス ステータスの表示
Users	ユーザー アカウントとロールの作成および変更

外部ロケーションへの監査ログの送信について

Management Center から監査ログを外部の場所に送信する場合は、以下を参照してください。

- 監査ログ （51 ページ）
- 監査ログ証明書 （55 ページ）



第 13 章

統計情報

以下のトピックでは、システムをモニターする方法を示します。

システム統計について

[統計情報（Statistics）] ページには、アプライアンスの現在の一般的ステータスに関する統計情報（ディスク使用量とシステム プロセス）、データ コリレータ統計情報、侵入イベント情報が表示されます。

[ホスト統計情報（Host Statistics）] セクション

次の表に、[統計情報（Statistics）] ページにリストされるホスト統計情報を示します。

表 *40 :* ホスト統計情報（*Host Statistics*）

カテゴリ	説明
時刻（Time）	システムの現在の時刻。
アップタイム（Uptime）	システムが前回起動してから経過した日数（該当する場合）、時間数、および分数。

カテゴリ	説明
メモリ使用率（Memory Usage）	使用中のシステム メモリの割合。
負荷平均（Load Average）	直前の 1 分間、5 分間、15 分間の CPU キュー内の平均プロセス数。
ディスク使用率（Disk Usage）	使用中のディスクの割合。詳細なホスト統計情報を表示するには、矢印をクリックします。
プロセス（Processes）	システムで実行されているプロセスの概要。

[ディスク使用量（Disk Usage）] セクション

[統計情報（Statistics）] ページの [ディスク使用率（Disk Usage）] セクションは、カテゴリ別およびパーティション ステータス別に、ディスク使用量のクイック概要を示します。マルウェア ストレージ パックがデバイスにインストールされている場合、そのパーティション ステータスも確認できます。このページを定期的に監視して、システム プロセスおよびデータベースで十分なディスク領域が使用可能であることを確認できます。

ヒント [ディスク使用量（Disk Usage）]ヘルスモニターを使用して、ディスク使用状況を監視し、ディスク容量不足の状態をアラートすることもできます。

[プロセス（Processes）] セクション

[統計情報（Statistics）] ページの [プロセス（Processes）] セクションでは、アプライアンスで現在実行中のプロセスを表示できます。これは、一般的なプロセス情報と、実行中の各プロセスに固有の情報を提供します。Management Center の Web インターフェイスを使用すると、管理対象デバイスのプロセスのステータスを表示できます。

アプライアンスで実行されるプロセスには、デーモンと実行可能ファイルの2種類があることに注意してください。デーモンは常に実行され、実行可能ファイルは必要に応じて実行されます。

プロセス使用状況フィールド

統計情報ページのプロセス セクションを展開すると、以下を表示できます。

[CPU（Cpu(s)）]

次の CPU 使用状況情報がリストされます：

- ユーザ プロセスの使用状況の割合
- システム プロセスの使用状況の割合
- nice 使用状況の割合（高い優先度を示す、負の nice 値を持つプロセスの CPU 使用状況）。nice 値は、システム プロセスのスケジュールされた優先度を示しており、-20（最も高い優先度）から 19（最も低い優先度）の範囲の値になります。
- アイドル状態の使用状況の割合

[メモリ（Mem）]

以下のメモリ使用状況情報がリストされます。

- メモリ内の合計キロバイト数
- メモリ内の使用キロバイト数の合計
- メモリ内の空きキロバイト数の合計
- メモリ内のバッファに書き出されたキロバイト数の合計

[切替（Swap）]

以下のスワップ使用状況情報がリストされます。

- スワップ内の合計キロバイト数
- スワップ内の使用キロバイト数の合計
- スワップ内の空きキロバイト数の合計
- スワップ内のキャッシュされたキロバイト数の合計

次の表に、プロセス セクションに表示される各列を示します。

表 *41* : プロセス リスト カラム

カラム	説明
Pid	プロセス ID 番号
ユーザ名（Username）	プロセスを実行しているユーザまたはグループの名前
Pri	プロセスの優先度
Nice	nice 値。プロセスのスケジューリング優先度を示す値です。値は -20（最も高い優先度）から 19（最も低い優先度）までの範囲になります。

カラム	説明
Size	プロセスで使用されるメモリ サイズ（値の後ろにメガバイトを表す m がない場合はキロバイト単位）
Res	メモリ内の常駐ページング ファイルの量（値の後ろにメガバイトを表す m がない場合はキロバイト単位）
State	プロセスの状態： • D：プロセスが中断不能スリープ状態（通常は入出力）にある • N：プロセスの nice 値が正の値 • R：プロセスが実行可能である（実行するキュー上で） • S：プロセスがスリープ モードにある • T：プロセスがトレースまたは停止されている • W：プロセスがページングしている • X：プロセスがデッド状態である • Z：プロセスが機能していない • <：プロセスの nice 値が負の値
Time	プロセスが実行されてきた時間の長さ（時間数:分数:秒数）
Cpu	プロセスが使用している CPU の割合
Command	プロセスの実行可能ファイル名

関連トピック

システム デーモン （512 ページ）
実行可能ファイルおよびシステム ユーティリティ （514 ページ）

システム デーモン

デーモンは、アプライアンスで継続的に実行されます。これにより、サービスが使用可能になり、必要に応じてプロセスが生成されるようになります。次の表では、[プロセスのステータス（Process Status）] ページに表示されるデーモンをリストし、その機能について簡単に説明しています。

（注） 次の表は、アプライアンスで実行される可能性があるすべてのプロセスの包括的なリストではありません。

表 *42 :* システム デーモン

デーモン	説明
crond	スケジュールされたコマンド（cron ジョブ）の実行を管理します
dhclient	ダイナミック ホスト IP アドレッシングを管理します
fpcollect	クライアントとサーバのフィンガープリントの収集を管理します
httpd	HTTP（Apache Web サーバ）プロセスを管理します
httpsd	HTTPS（SSL を使用した Apache Web サーバー）サービスを管理し、SSL お 明書の認証が機能しているかチェックし、アプライアンスへの安全な Web 供するためにバックグラウンドで実行します
keventd	Linux カーネルのイベント通知メッセージを管理します
klogd	Linux カーネル メッセージのインターセプションおよびロギングを管理し
kswapd	Linux カーネルのスワップ メモリを管理します
kupdated	ディスクの同期を実行する、Linux カーネルの更新プロセスを管理します
mysqld	データベース プロセスを管理します
ntpd	Network Time Protocol（NTP）プロセスを管理します
pm	すべてのシステムプロセスを管理し、必要なプロセスを始動し、予期せず セスをすべて再始動します
reportd	レポートを管理します
safe_mysqld	データベースのセーフ モード運用を管理し、エラーが発生した場合にはデ モンを再始動し、ランタイム情報をファイルに記録します
SFDataCorrelator	データ転送を管理します
sfestreamer （Management Center のみ）	Event Streamer を使用するサード パーティ製クライアント アプリケーショ 理します
sfmgr	アプライアンスへの sftunnel 接続を使用して、リモートでアプライアンス 定するための RPC サービスを提供します
SFRemediateD（Management Center のみ）	修復応答を管理します
sftimeserviced（Management Center のみ）	時間同期メッセージを管理対象デバイスに転送します

デーモン	説明
sfmbservice	アプライアンスへの sftunnel 接続を使用して、リモート アプライアンスで実行 sfmb メッセージ ブローカ プロセスへのアクセスを提供します。現在、ヘルス グでのみ使用されており、管理対象デバイスから Management Center へ正常な アラートを送信します。
sftroughd	着信ソケットで接続をリッスンしてから、正しい実行可能ファイル（通常は、 セージ ブローカ sfmb）を呼び出して要求を処理します
sftunnel	リモートアプライアンスとの通信を必要とするすべてのプロセスに対し、安全 ネルを提供します。
sshd	セキュア シェル（SSH）プロセスを管理し、アプライアンスへの SSH アクセ るためにバックグラウンドで実行します
syslogd	システム ロギング（syslog）プロセスを管理します

実行可能ファイルおよびシステム ユーティリティ

システム上には、他のプロセスまたはユーザー操作によって実行される実行可能ファイルが数多く存在します。次の表に、[プロセス ステータス（Process Status）] ページで表示される実行可能ファイルについて説明します。

表 *43 :* システムの実行可能ファイルおよびユーティリティ

実行可能ファイル	説明
awk	awkプログラミング言語で作成されたプログラムを実行するユーティリティ
bash	GNU Bourne-Again シェル
cat	ファイルを読み取り、コンテンツを標準出力に書き込むユーティリティ
chown	ユーザおよびグループのファイル権限を変更するユーティリティ
chsh	デフォルトのログイン シェルを変更するユーティリティ
SFDataCorrelator（Management Center のみ）	システムで作成されるバイナリ ファイルを分析し、イベント、接続データ、およびネットワーク マップを生成します。
cp	ファイルをコピーするユーティリティ
df	アプライアンスの空き領域の量をリストするユーティリティ
echo	コンテンツを標準出力に書き込むユーティリティ

実行可能ファイル	説明
egrep	指定された入力を、ファイルおよびフォルダで検索するユーティリティ。標準grepでサポートされていない正規表現の拡張セットをサポートします
find	指定された入力のディレクトリを再帰的に検索するユーティリティ
grep	指定された入力をファイルとディレクトリで検索するユーティリティ
halt	サーバを停止するユーティリティ
httpsdctl	セキュアな Apache Web プロセスを処理する
hwclock	ハードウェア クロックへのアクセスを許可するユーティリティ
ifconfig	ネットワーク構成実行可能ファイルを示します。MACアドレスが常に一定になるようにします
iptables	[アクセス権の設定（Access Configuration）]ページに加えられた変更に基づいてアクセス制限を処理します。
iptables-restore	iptables ファイルの復元を処理します
iptables-save	iptables に対する保存済みの変更を処理します
kill	セッションおよびプロセスを終了するために使用できるユーティリティ
killall	すべてのセッションおよびプロセスを終了するために使用できるユーティリティ
ksh	Korn シェルのパブリック ドメイン バージョン
logger	コマンドラインからsyslogデーモンにアクセスする方法を提供するユーティリティ
md5sum	指定したファイルのチェックサムとブロック数を印刷するユーティリティ
mv	ファイルを移動（名前変更）するユーティリティ
myisamchk	データベース テーブルの検査および修復を示します
mysql	データベース プロセスを示します。複数のインスタンスが表示されることがあります
openssl	認証証明書の作成を示します
perl	perl プロセスを示します
ps	標準出力にプロセス情報を書き込むユーティリティ

実行可能ファイル	説明
sed	1 つ以上のテキスト ファイルの編集に使用されるユーティリティ
sfheartbeat	アプライアンスがアクティブであることを示す、ハートビート ブロードキャストを識別します。ハートビートはデバイスとManagement Centerの間の接続を維持するのに使用されます。
sfmb	メッセージブローカ プロセスを示します。Management Centerとデバイスとの間の通信を処理します。
sh	Korn シェルのパブリック ドメイン バージョン
shutdown	アプライアンスをシャットダウンするユーティリティ
sleep	指定された秒数のあいだプロセスを中断するユーティリティ
smtpclient	電子メール イベント通知機能が有効な場合に、電子メール送信を処理するメール クライアント
snmptrap	SNMP 通知機能が有効な場合に、指定された SNMP トラップ サーバに SNMP トラップ データを転送します
snort	Snort が動作していることを示します
ssh	アプライアンスへのセキュア シェル（SSH）接続を示します
sudo	sudo プロセスを示します。これにより、admin 以外のユーザが実行可能ファイルを実行できるようになります
top	上位の CPU プロセスに関する情報を表示するユーティリティ （注） このユーティリティの CPU 使用率の出力は、CPU コアのさまざまなタイプの使用率が分離されたものです。実際の合計CPU使用率を知るには、ユーザープロセスとシステムプロセスの両方の使用率を加算する必要があります。 たとえば、top コマンドの出力が次の場合：`%Cpu(s): 76.6 us, 22.1 sy, 0.0 ni, 0.0 id, 0.0 wa, 0.0 hi, 1.3 si, 0.0 st` この場合、CPU 時間の 76.6% がユーザープロセスによって使用され、CPU 時間の 22.1% がシステム（カーネル）プロセスによって使用されています。合計 CPU 使用率は 98.7% です。 そのため、このユーティリティでレポートされる CPU 使用率は、ヘルス モニター ダッシュボードとは異なるように見えます。また、このユーティリティでは 3 秒の間隔を使用して CPU 使用率が計算されます。一方、Management Center のヘルスモニターでは 1 秒の間隔が使用されます。

実行可能ファイル	説明
touch	指定したファイルへのアクセス時刻や変更時刻を変更するために使用できるユーティリティ
vim	テキスト ファイルの編集に使用されるユーティリティ
wc	指定したファイルの行、ワード、バイトのカウントを実行するユーティリティ

関連トピック

アクセス リストの設定 （49 ページ）

[SFDataCorrelator プロセス統計情報（SFDataCorrelator Process Statistics）] セクション

Management Center では、現在の日付のデータコリレータとネットワーク検出プロセスに関する統計情報を表示できます。管理対象デバイスがデータの取得、復号化、および分析を実行する際に、ネットワーク検出プロセスはデータをフィンガープリントおよび脆弱性データベースと関連付けてから、Management Center で実行中のデータ コリレータで処理されるバイナリ ファイルを生成します。データ コリレータはバイナリ ファイルの情報を分析し、イベントを生成し、ネットワーク マップを作成します。

ネットワーク検出とデータ コリレータに表示される統計情報は、デバイスごとに 0:00 から 23:59 までの間に収集された統計情報を使用した、当日の平均です。

次の表に、データ コリレータ プロセスに表示される統計情報を示します。

表 *44* : データ コリレータ プロセスの統計情報

カテゴリ	説明
Events/Sec	データ コリレータが受信し処理する検出イベントの 1 秒あたりの数
Connections/Sec	データ コリレータが受信し処理する接続の 1 秒あたりの数
CPU Usage — User (%)	当日のユーザープロセスで使用される CPU 時間の平均パーセンテージ
CPU Usage — System (%)	当日のシステム プロセスで使用される CPU 時間の平均パーセンテージ
VmSize（KB）	データ コリレータに割り当てられたメモリの当日の平均サイズ（キロバイト単位）
VmRSS（KB）	当日のデータ コリレータで使用されるメモリの平均量（キロバイト単位）

[侵入イベント情報（Intrusion Event Information）] セクション

Management Center デバイスと管理対象デバイスのどちらでも、[統計情報（Statistics）] ページで、侵入イベントに関するサマリ情報を確認できます。表示される情報には、前回の侵入イベントの日時、過去 1 時間および過去 1 日に発生したイベントの合計数、データベース内のイベントの合計数などがあります。

（注） [統計情報（Statistics）] ページの [侵入イベント情報（Intrusion Event Information）] セクションにある情報は、Management Center に送信された侵入イベントではなく、管理対象デバイスに保存されている侵入イベントに基づいています。管理対象デバイスが侵入イベントをローカルに格納できない（または格納しないように設定されている）場合、侵入イベント情報はこのページに表示されません。

次の表に、[統計情報（Statistics）] ページの [侵入イベント情報（Intrusion Event Information）] セクションに表示される統計情報を示します。

表 *45 :* 侵入イベント情報（*Intrusion Event Information*）

統計	説明
前回のアラート（Last Alert Was）	前回のイベントが発生した日時
過去 1 時間のイベントの合計（Total Events Last Hour）	過去 1 時間に発生したイベントの合計数
過去 1 日のイベントの合計（Total Events Last Day）	過去 24 時間に発生したイベントの合計数
データベース内のイベントの合計（Total Events in Database）	イベント データベース内のイベントの合計数

システム統計情報の表示

この表示には、Management Center とその管理対象デバイスの統計情報が含まれています。

始める前に

システム統計を表示するには、管理者またはメンテナンスユーザーであり、グローバルドメインにいる必要があります。

手順

ステップ 1 システム（⚙） > **[モニタリング（Monitoring）]** > **[統計（Statistics）]**を選択します。

ステップ 2 [デバイスの選択（Select Device(s)）] リストからデバイスを選択し、[デバイスの選択（Select Devices）] をクリックします。

ステップ 3 使用可能な統計を表示します。

ステップ 4 [ディスク使用状況（Disk Usage）] セクションでは、次の操作を実行できます。

- [カテゴリ別（By Category）]積み上げ横棒で、ディスク使用量カテゴリの上にポインタを移動すると、以下が（順番に）表示されます。
  - そのカテゴリが使用する使用可能なディスク領域の割合
  - ディスク上の実際のストレージ領域
  - そのカテゴリで使用可能なディスク領域の合計
- [パーティション別（By Partition）] の横にある矢印をクリックして展開します。マルウェア ストレージ パックがインストールされている場合は、`/var/storage` パーティションの使用状況が表示されます。

ステップ 5 （オプション）[プロセス（Processes）] の横にある矢印をクリックすると、システム統計情報の表示 （518 ページ）で説明されている情報が表示されます。

第 14 章

トラブルシューティング

以下のトピックは、発生する可能性のある問題を診断する方法について説明します。

トラブルシューティングのベストプラクティス

- 問題の修正を試みるために変更を加える前に、トラブルシューティング ファイルを生成して元の問題をキャプチャします。トラブルシューティング用のヘルス モニター レポート （536 ページ）およびサブセクションを参照してください。

  サポートのために Cisco TAC に連絡する必要が生じた場合に、このトラブルシューティング ファイルが必要になることがあります。

- メッセージセンターのエラーメッセージと警告メッセージを調べて、調査を開始します。システム メッセージ （522 ページ）を参照してください

- お使いの製品の製品ドキュメント ページの「Troubleshoot and Alerts」という見出しの下にある、該当するテクニカル ノートとその他のトラブルシューティング リソースを探します。

システム メッセージ

システムで発生した問題を突き止める必要がある場合、調査の出発点となるのはメッセージセンターです。メッセージセンターでは、システムがシステムのアクティビティとステータスに関して継続的に生成するメッセージを表示できます。

メッセージセンターを開くには、メインメニューの [展開（Deploy）] メニューの隣にある [システムステータス（System Status）] アイコンをクリックします。このアイコンは、システムのステータスによって以下のように表示されます。

- ：1 つ以上のエラーと任意の数の警告がシステム上に存在することを示します。
- ：1つ以上の警告がシステム上に存在することを示します。エラーは発生していません。
- ：警告とエラーはいずれもシステム上に存在していないことを示します。

アイコンに数字が表示されている場合、その数字は現在のエラー メッセージまたは警告メッセージの数を示します。

メッセージセンターを閉じるには、Web インターフェイス内でメッセージセンターの外側をクリックします。

メッセージ センターに加え、Web インターフェイスには、ユーザーのアクティビティおよび進行中のシステム アクティビティに応じて即時にポップアップ通知が表示されます。ポップアップ通知のなかには 5 秒経過すると自動的に非表示になるものや、[表示を消す（Dismiss）]（ ） をクリックして明示的に表示を消さなければならない「スティッキー」通知もあります。通知リストの最上部にある [表示を消す（Dismiss）] リンクをクリックすると、すべての通知をまとめて非表示にすることができます。

ヒント スティッキー以外のポップアップ通知の上にマウスのカーソルを合わせると、その通知はスティッキーになります。

システムはユーザーのライセンス、ドメイン、アクセス ロールに基づいて、どのメッセージをポップアップ通知やメッセージ センターに表示するか決定します。

メッセージ タイプ

Message Center では、システムのアクティビティとステータスをレポートするメッセージが 3 つのタブに編成されて表示されます。

展開（Deployments）

このタブには、システムの各アプライアンスの設定展開に関連する現在のステータスがドメイン別にグループ化されて表示されます。システムでは、次の展開ステータス値がこのタブでレポートされます。[履歴の表示（Show History）] をクリックして、展開ジョブに関する追加情報を取得できます。

- [実行中（Running）]（**回転中**）：設定は展開の処理中です。
- [成功（Success）]：設定は正常に展開されました。
- [警告（Warning）]（  ）：警告展開ステータスは、**警告システムステータスアイコン**とともに表示されるメッセージ数に含まれます。
- [失敗（Failure）]：設定は展開に失敗しました。展開が必要な設定変更を参照してください。失敗した展開は、**エラー システム ステータス アイコン**とともに表示されるメッセージ数に含まれます。

アップグレード

このタブには、管理対象デバイスのソフトウェア アップグレード タスクに関連する現在のステータスが表示されます。システムでは、次のアップグレードステータス値がこのタブでレポートされます。

- [進行中（In progress）]：アップグレードタスクが進行中であることを示します。
- [完了（Completed）]：ソフトウェア アップグレード タスクが正常に完了したことを示します。
- [失敗（Failed）]：ソフトウェア アップグレード タスクが完了しなかったことを示します。

ヘルス

このタブには、システムの各アプライアンスの現在のヘルス ステータス情報がドメイン別にグループ化されて表示されます。ヘルス ステータスは、ヘルス モニタリングについて（431 ページ）に記載されているように、ヘルス モジュールによって生成されます。システムでは、次の正常性ステータス値がこのタブでレポートされます。

- [警告（Warning）]（  ）：アプライアンス上のヘルスモジュールが警告制限を超え、問題が解決されていないことを示します。[ヘルスモニタリング（Health Monitoring）]ページには、これらの状態が[黄色い三角形（Yellow Triangle）]（  ）で示されます。警告ステータスは、**警告システムステータスアイコン**とともに表示されるメッセージ数に含まれます。
- [クリティカル（Critical）]（  ）：アプライアンス上のヘルスモジュールが重大制限を超え、問題が解決されていないことを示します。[ヘルス モニタリング（Health Monitoring）]ページには、これらの状態が [クリティカル（Critical）]（  ）アイコンで示されます。重大ステータスは、**エラー システム ステータス アイコン**とともに表示されるメッセージ数に含まれます。
- [エラー（Error）]（  ）：アプライアンス上のヘルス モニタリング モジュールに障害が発生し、それ以降、正常に再実行されていないことを示します。[ヘルスモニタリング（Health Monitoring）]ページには、これらの状態が**エラーアイコン**で示されます。エラーステータスは、**エラー システム ステータス アイコン**とともに表示されるメッセージ数に含まれます。

[ヘルス（Health）] タブのリンクをクリックして、[ヘルス モニタリング（Health Monitoring）] ページで関連の詳細情報を表示できます。現在のヘルス ステータス状態がない場合、[ヘルス（Health）] タブにメッセージは表示されません。

タスク

特定のタスク（設定のバックアップや更新のインストールなど）は、完了するまで時間がかかる可能性があります。このタブには、これらの長時間実行タスクのステータスが表示され、自分が開始したタスクや、適切なアクセス権がある場合は、システムの他のユーザが開始したタスクが含まれることがあります。このタブには、各メッセージの最新の更新時間に基づいて時系列の逆順にメッセージが表示されます。一部のタスク ステータス メッセージには、問題となっているタスクについての詳細情報へのリンクが含まれています。システムでは、次のタスクステータス値がこのタブでレポートされます。

- [待機中（Waiting）]：別の進行中のタスクが完了するまで実行を待機しているタスクを示します。このメッセージ タイプでは、更新の経過表示バーが表示されます。
- [実行中（Running）]：進行中のタスクを示します。このメッセージ タイプでは、更新の経過表示バーが表示されます。
- [再試行中（Retrying）]：自動的に再試行しているタスクを示します。なお、すべてのタスクの再試行が許可されるわけではありません。このメッセージタイプでは、更新の経過表示バーが表示されます。
- [成功（Success）]：正常に完了したタスクを示します。
- [失敗（Failure）]：正常に完了しなかったタスクを示します。失敗したタスクは、**エラー システム ステータス アイコン**とともに表示されるメッセージ数に含まれます。
- [停止（Stopped）] または [中断（Suspended）]：システムアップデートのために中断されたタスクを示します。停止したタスクを再開することはできません。通常の動作が復元されたら、もう一度タスクを開始してください。
- [スキップ（Skipped）]：進行中のプロセスによって、タスクの開始が妨げられました。タスクの開始をもう一度試行してください。

新しいタスクが開始されると、新しいメッセージがこのタブに表示されます。タスクが完了すると（成功、失敗、または停止のステータス）、タスクを削除するまで、このタブには最終ステータスを示すメッセージが引き続き表示されます。[タスク（Tasks）]タブおよびメッセージデータベースがいっぱいにならないように、メッセージを削除することをお勧めします。

メッセージ管理

メッセージ センターから、以下を実行できます。

- ポップアップ通知の表示を選択します。
- システムデータベースからのタスクステータスメッセージをより多く表示します（削除されていないもので利用可能なものがある場合）。

- すべてのタスクマネージャ通知のレポートをダウンロードします。
- 個々のタスクのステータスメッセージを削除します。（これは、削除されたメッセージを確認できるすべてのユーザに影響します）。
- タスクのステータスメッセージを一括で削除します。（これは、削除されたメッセージを確認できるすべてのユーザに影響します）。

ヒント　シスコは、表示に加えてデータベースの不要なデータを削除するために、累積されたタスクのステータスメッセージを[タスク（Task）]タブから定期的に削除することを推奨します。データベースのメッセージ数が100,000に到達すると、削除したタスクのステータスメッセージが自動的に削除されます。

基本的なシステム情報の表示

[バージョン情報（About）]ページには、システムのさまざまなコンポーネントのモデル、シリアル番号、バージョン情報など、アプライアンスに関する情報が示されます。また、シスコの著作権情報も示されます。

手順

ステップ1　ページ上部のツールバーで、**[ヘルプ（Help）]**（  ）をクリックします。

ステップ2　[バージョン情報（About）]を選択します。

アプライアンス情報の表示

手順

システム（  ）>**[構成（Configuration）]**を選択します。

システムメッセージの管理

手順

ステップ 1 [Notification（通告）] をクリックして、メッセージセンターを表示します。

ステップ 2 次の選択肢があります。

- [展開（Deployments）] をクリックして、設定の展開に関連するメッセージを表示します。展開メッセージの表示（527ページ）を参照してください。展開メッセージを表示するには、管理者ユーザであるか、**デバイス設定の展開**権限が必要です。
- [アップグレード（Upgrades）] をクリックして、デバイスアップグレードタスクに関連するメッセージを表示します。「アップグレードメッセージの表示」を参照してください。「アップグレードメッセージの表示」を参照してください。これらのメッセージを表示するには、管理者ユーザーであるか、[更新（Updates）] 権限が必要です。

  新しい推奨アップグレードバージョンが表示されます。[通知する（Remind Me）] オプションまたは [詳細（Details）] オプションを使用して、リマインダの設定または詳細情報の表示をそれぞれ選択できます。

- [正常性（Health）] をクリックして、Management Center とそれに登録したデバイスの状況に関連するメッセージを表示します。正常性メッセージの表示（528ページ）を参照してください。展開メッセージを表示するには、管理者ユーザーであるか、[正常性（Health）] 権限が必要です。

  [正常性モニター（Health monitor）] リンクをクリックすると、[正常性モニター（Health Monitor）] ページに移動できます。

- [タスク（Tasks）] をクリックして、長時間実行タスクに関連するメッセージを表示または管理します。タスクメッセージの表示（529ページ）またはタスクメッセージの管理（530ページ）を参照してください。誰もが自分のタスクを表示できます。他のユーザのタスクを表示するには、管理者ユーザであるか、**他のユーザのタスク表示**権限が必要です。[完了したタスクの削除（Remove completed tasks）] リンクをクリックすると、完了したタスクを通知から削除できます。
- [レポートのダウンロード（Download Report）] アイコンをクリックして、タスクマネージャにおけるすべての通知のレポートを生成します。[CSVのダウンロード（Download CSV）] または [PDFのダウンロード（Download PDF）] を選択してレポートをダウンロードします。
- [通知を表示（Show Notifications）] スライダをクリックして、ポップアップ通知の表示を有効または無効にします。

展開メッセージの表示

展開メッセージを表示するには、管理者ユーザであるか、**デバイス設定の展開**権限が必要です。

手順

ステップ 1 [Notification（通告）] をクリックして、メッセージセンターを表示します。

ステップ 2 [導入（Deployments）] をクリックします。

ステップ 3 次の選択肢があります。

- 現在のすべての展開ステータスを表示するには、[total] をクリックします。
- 任意の展開ステータスに関するメッセージのみを表示するには、そのステータスの値をクリックします。
- 展開の経過時間、開始時刻および停止時刻を表示するには、メッセージの時間経過インジケータ（たとえば、[1m 5s]）の上にカーソルを置きます。

ステップ 4 展開ジョブの詳細情報を表示するには、[show deployment history] をクリックします。

[展開の履歴（Deployment History）] テーブルには、左側の列に展開ジョブが新しい順にリストされています。

a) 展開ジョブを選択します。

右側の列のテーブルには、ジョブに含まれていた各デバイスと、デバイスごとの展開ステータスが表示されます。

b) デバイスからの応答、および展開中にデバイスに送信されたコマンドを表示するには、デバイスの [Transcript] カラムにあるダウンロードアイコンをクリックします。

トランスクリプトには、次のセクションが含まれています。

- [Snort を適用（Snort Apply）]：Snort 関連ポリシーから障害または応答が発生すると、メッセージがこのセクションに表示されます。通常、このセクションは空です。
- [CLIを適用（CLI Apply）]：このセクションは、Lina プロセスに送信されたコマンドを使用して設定される機能を対象にしています。
- [インフラストラクチャメッセージ（Infrastructure Messages）]：このセクションには、さまざまな導入モジュールのステータスが表示されます。

[CLIを適用（CLI Apply）] セクションでは、展開トランスクリプトには、デバイスに送信されたコマンド、およびデバイスから返された応答が含まれます。これらの応答は、通知メッセージやエラーメッセージの場合があります。失敗した展開では、コマンドを含むエラーを示すメッセージを探します。これらのエラーを調べることは、FlexConfig ポリシーを使用してカスタマイズされた機能を設定している場合に特に有用になる場合があります。これらのエラーは、コマンドを設定しようとしている FlexConfig オブジェクトのスクリプトを修正するのに役立つ場合があります。

（注） 管理対象機能に送信されるコマンドと、FlexConfig ポリシーから生成されるコマンドとの間のトランスクリプトには違いはありません。

たとえば、次のシーケンスは、論理名が outside の GigabitEthernet0/0 を設定するコマンドを Management Center が送信したことを示しています。デバイスは、自動的にセキュリティレベルを 0 に設定したことを応答しました。Threat Defense は、何に対してもセキュリティレベルを使用しません。

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

アップグレードメッセージの表示

展開メッセージを表示するには、管理者ユーザーであるか、[更新（Updates）] 権限が必要です。

手順

ステップ 1 [Notification（通告）] をクリックして、メッセージセンターを表示します。

ステップ 2 [アップグレード（Upgrades）] をクリックします。

ステップ 3 次を実行できます。

- 現在のすべてのアップグレードタスクを表示するには、[合計（Total）] をクリックします。
- 特定のステータスを持つメッセージのみを表示するには、そのステータスの値をクリックします。
- アップグレードタスクの詳細を表示するには、[デバイスの管理（Device Management）] をクリックします。

正常性メッセージの表示

展開メッセージを表示するには、管理者ユーザーであるか、[正常性（Health）] 権限が必要です。

手順

ステップ 1 [Notification（通告）] をクリックして、メッセージセンターを表示します。

ステップ 2 [正常性（Health）] をクリックします。

ステップ 3 次の選択肢があります。

- 現在のすべての正常性ステータスを表示するには、[合計（total）] をクリックします。シビラティ（重大度）の内訳（つまり、警告、クリティカル、およびエラー）も表示されます。
- 任意のステータスに関するメッセージのみを表示するには、そのステータスの値をクリックします。
- メッセージが最も最近更新された時刻を表示するには、そのメッセージの相対時間インジケータ（たとえば [3日前（3 day(s) ago）]）の上にカーソルを置きます。
- 特定のメッセージの詳細な正常性ステータス情報を表示するには、メッセージをクリックします。
- [ヘルスモニタリング（Health Monitoring）] ページの完全な正常性ステータスを表示するには、[ヘルスモニター（Health Monitor）] をクリックします。

関連トピック

ヘルス モニタリングについて （431 ページ）

タスクメッセージの表示

誰もが自分のタスクを表示できます。他のユーザのタスクを表示するには、管理者ユーザであるか、**他のユーザのタスク表示**権限が必要です。

手順

ステップ 1 [通告（Notification）] をクリックして、メッセージセンターを表示します。

ステップ 2 [タスク（Tasks）] をクリックします。

ステップ 3 次の選択肢があります。

- 現在のすべてのタスクのステータスを表示するには、[合計（Total）] をクリックします。ステータス（待機中、実行中、再試行中、成功、失敗）に基づいてタスクを表示するには、それらをクリックします。
- 任意のステータスのタスクに関するメッセージのみを表示するには、そのステータスの値をクリックします。

（注） 停止したタスクのメッセージは、タスクのステータスメッセージの合計リストにのみ表示されます。停止したタスクではフィルタリングできません。

- メッセージが最も最近更新された時刻を表示するには、そのメッセージの相対時間インジケータ（たとえば [3 日前（3 day(s) ago）]）の上にカーソルを置きます。
- タスクに関する詳細を表示するには、メッセージ内のリンクをクリックします。
- さらにタスクのステータス メッセージが表示可能な場合は、メッセージ リストの下部にある [さらにメッセージを取得する（Fetch more messages）] をクリックして取得します。

タスクメッセージの管理

誰もが自分のタスクを表示できます。他のユーザのタスクを表示するには、管理者ユーザであるか、**他のユーザのタスク表示**権限が必要です。

手順

ステップ 1 [システムステータス（System Status）] アイコンをクリックして、メッセージセンターを表示します。

ステップ 2 [タスク（Tasks）] をクリックします。

ステップ 3 次の選択肢があります。

- さらにタスクのステータス メッセージが表示可能な場合は、メッセージ リストの下部にある [さらにメッセージを取得する（Fetch more messages）] をクリックして取得します。
- 完了したタスク（ステータスが停止、成功、または失敗のタスク）に関する 1 つのメッセージを削除するには、メッセージの横にある [削除（Remove）]（  ）をクリックします。
- すべての完了しているタスク（ステータスが停止、成功、または失敗のタスク）に関するメッセージをすべて削除するには、[総数（total）] でメッセージをフィルタリングして、[すべての完了タスクの削除（Remove all completed tasks）] をクリックします。
- すべての正常に完了したタスクに関するメッセージをすべて削除するには、[成功（success）] でメッセージをフィルタリングして、[すべての成功タスクの削除（Remove all successful tasks）] をクリックします。
- すべての失敗したタスクに関するメッセージをすべて削除するには、[失敗（failure）] でメッセージをフィルタリングして、[すべての失敗タスクの削除（Remove all failed tasks）] をクリックします。

ヘルスモニターアラートのメモリ使用率しきい値

メモリ使用率ヘルスモジュールは、アプライアンス上のメモリ使用率をモジュールに設定された制限と比較し、使用率がそのレベルを超えるとアラートを出します。このモジュールは、管理対象デバイスおよび Management Center 自体のデータをモニターします。

メモリー使用率の2つの設定可能なしきい値である「クリティカル」と「警告」は、使用されるメモリのパーセンテージとして設定できます。これらのしきい値を超えると、指定された重大度レベルでヘルスアラームが生成されます。ただし、ヘルスアラームシステムはこれらのしきい値を正確に計算しません。

高メモリデバイスでは、低メモリフットプリントデバイスよりも、特定のプロセスがシステムメモリ全体の大きな割合を使用することが予想されます。この設計では、物理メモリをできるだけ多く使用し、補助的なプロセス用に小さい値のメモリを解放します。

たとえば、32 GB のメモリを搭載したデバイスと 4 GB のメモリを搭載したデバイスを比較します。補助的なプロセスのために解放される 5 % のメモリは、32 GB のメモリを搭載したデバイスでは 1.6 GB、4 GB のメモリを搭載したデバイスでは 200 MB であり、前者の方がはるかに大きな値になります。

特定のプロセスによるシステムメモリの使用率が高いことを考慮して、Management Center は、合計物理メモリと合計スワップメモリの両方を含めて合計メモリを計算します。そのため、ユーザーが設定するしきい値入力に対して適用されるメモリしきい値により、イベントの「値」列が、超過しきい値を特定するために入力された値と一致しないようなヘルスイベントが発生する可能性があります。

バージョン 7.4.1 以降、メモリ使用率正常性モジュールは、使用可能な空きメモリ、使用可能なスワップメモリ、およびバッファキャッシュを考慮してメモリ使用率を計算します。メモリ使用率正常性アラートの早すぎる生成を回避するために、警告およびクリティカルアラームのしきい値である 88% と 90% を超えないようにすることをお勧めします。

次の表は、搭載するシステムメモリに応じた、ユーザー入力のしきい値と適用されるしきい値の例を示しています。

（注） この表の値は一例です。この情報を使用して、ここに示されている搭載 RAM と一致しないデバイスのしきい値を推定することができます。また、より正確なしきい値の計算について Cisco TAC に問い合わせることもできます。

表 *46 :* 搭載する *RAM* に基づくメモリ使用率しきい値

ユーザー入力しきい値	搭載するメモリ（RAM）ごとの適用しきい値			
	4 GB	**6 GB**	**32 GB**	**48 GB**
10%	10%	34 %	72%	81 %
20 %	20 %	41%	75%	83 %
30%	30%	48 %	78%	85 %
40%	40%	56 %	81 %	88 %
50%	50%	63 %	84 %	90%
60 %	60 %	70%	88 %	92%

ユーザー入力しきい値	搭載するメモリ（RAM）ごとの適用しきい値			
	4 GB	6 GB	32 GB	48 GB
70%	70%	78%	91 %	94%
80%	80%	85 %	94%	96%
90 %	90 %	93%	97%	98%
100 %	100 %	100 %	100 %	100 %

注意 Management Center がクリティカルシステムメモリ状態に達すると、システムは、メモリ使用量の多いプロセスを終了したり、高いメモリ使用率が続く場合には Management Center を再起動する可能性があります。

ディスク使用率とイベントドレインの正常性モニターアラート

Disk Usage 正常性モジュールは、管理対象デバイスのハードドライブとマルウェア ストレージ パック上のディスク使用率をモジュールに設定された制限と比較し、その使用率がモジュールに設定されたパーセンテージを超えた時点でアラートを出します。また、モジュールしきい値に基づいて、システムが監視対象のディスク使用カテゴリ内のファイルを過剰に削除する場合、または、これらのカテゴリを除くディスク使用率が過剰なレベルに達した場合にもアラートを出します。

このトピックでは、Disk Usage 正常性モジュールによって生成される未処理イベントのドレイン正常性アラートの症状とトラブルシューティングのガイドラインについて説明します。

ディスクマネージャのプロセスは、デバイスのディスク使用率を管理します。ディスクマネージャによってモニターされる各タイプのファイルには、サイロが割り当てられます。システムで使用可能なディスク容量に基づいて、ディスクマネージャは各サイロの最高水準点（High Water Mark、HWM）と最低水準点（Low Water Mark 、LWM）を計算します。

システムの各部分のディスク使用率の詳細情報（サイロ、LWM、HWM など）を表示するには、**show disk-manager** コマンドを使用します。

例

次に、ディスクマネージャ情報の例を示します。

```
> show disk-manager
Silo                                    Used        Minimum     Maximum
Temporary Files                         0 KB        499.197 MB  1.950 GB
Action Queue Results                    0 KB        499.197 MB  1.950 GB
User Identity Events                    0 KB        499.197 MB  1.950 GB
```

```
UI Caches                              4 KB         1.462 GB    2.925 GB
Backups                                0 KB         3.900 GB    9.750 GB
Updates                                0 KB         5.850 GB    14.625 GB
Other Detection Engine                 0 KB         2.925 GB    5.850 GB
Performance Statistics                 33 KB        998.395 MB  11.700 GB
Other Events                           0 KB         1.950 GB    3.900 GB
IP Reputation & URL Filtering          0 KB         2.437 GB    4.875 GB
Archives & Cores & File Logs           0 KB         3.900 GB    19.500 GB
Unified Low Priority Events            1.329 MB     4.875 GB    24.375 GB
RNA Events                             0 KB         3.900 GB    15.600 GB
File Capture                           0 KB         9.750 GB    19.500 GB
Unified High Priority Events           0 KB         14.625 GB   34.125 GB
IPS Events                             0 KB         11.700 GB   29.250 GB
```

正常性アラートの形式

Management Center の正常性モニタープロセスが実行されると（5 分ごとに 1 回、または手動実行がトリガーされると）、ディスク使用状況モジュールは diskmanager.log ファイルを調べ、該当する条件が満たされると、正常性アラートがトリガーされます。

正常性アラートの構造は、「Drain of unprocessed events from <*SILO NAME*>」です。

たとえば、「Drain of unprocessed events from Low Priority Events」のようになります。

重要 イベントサイロのみが Drain of unprocessed events from <SILO NAME> 正常性アラートを生成します。このアラートの重大度レベルは常に [重大（Critical）] です。

アラート以外のその他の症状には、次のものがあります。

- Management Center ユーザーインターフェイスの速度低下
- イベントの喪失

一般的なトラブルシューティング シナリオ

Drain of unprocessed events of <SILO NAME> 正常性アラートは、イベント処理パスのボトルネックが原因で発生します。

これらのディスク使用率アラートに関して、次の 3 つのボトルネックが存在する可能性があります。

- 過剰なロギング：Threat Defense の EventHandler プロセスがオーバーサブスクライブされています（Snort の書き込みよりも読み取りが遅い）。
- Sftunnel ボトルネック：イベント用インターフェイスが不安定またはオーバーサブスクライブ状態です。
- SFDataCorrerator のボトルネック：Management Center と管理対象デバイス間のデータ伝送チャネルがオーバーサブスクライブ状態です。

過剰なロギング

このタイプの正常性アラートの最も一般的な原因の1つは、過剰な入力です。**show disk-manager** コマンドから収集された最低水準点（LWM）と最高水準点（HWM）の差は、該当サイロが LWM（新たにドレインされた状態）から HWM 値に移行するまでに使用できる容量を示しています。未処理のイベントのドレインがある場合は、ロギング設定を確認してください。

- ダブルロギングを確認する：Management Center でコリレータ *perfstats* を調査すると、ダブルロギングのシナリオを特定できます。

  ```
  admin@FMC:~$ sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
  ```

- ACP のロギング設定を確認する：アクセス コントロール ポリシー（ACP）のロギング設定を確認します。ロギング設定に接続の「開始」と「終了」の両方が含まれている場合は、イベントの数を減らすために、終了のみをログに記録するように設定を変更します。

  接続のロギングのベストプラクティス（890ページ）に記載されているベストプラクティスに従っていることを確認します。

通信のボトルネック：Sftunnel

Sftunnel は、Management Center と管理対象デバイス間の暗号化通信を担当します。イベントはトンネルを介して Management Center に送信されます。管理対象デバイスと Management Center 間の通信チャネル（sftunnel）の接続性の問題や不安定性は、次の原因が考えられます。

- Sftunnel がダウンしているか、不安定（フラッピングしている）。

  Management Center と管理対象デバイスが、TCP ポート 8305 の管理インターフェイス間で到達可能であることを確認します。

  sftunnel プロセスは安定している必要があり、予期せず再起動することがあってはいけません。これを検証するには、**/var/log/message** ファイルを確認し、文字列 ***sftunneld*** を含むメッセージを検索します。

- Sftunnel がオーバーサブスクライブされている。

  正常性モニターからのトレンドデータを確認し、Management Center の管理インターフェイスのオーバーサブスクリプションの兆候を探します。この徴候には、管理トラフィックのスパイクや一定したオーバーサブスクリプションなどがあります。

  イベントのセカンダリ管理インターフェイスとして使用します。このインターフェイスを使用するには、Threat Defense CLI で **configure network management-interface** コマンドを使用して、IP アドレスなどのパラメータを設定する必要があります。

通信のボトルネック：SFDataCorrerator

SFDataCorrerator は、Management Center と管理対象デバイス間のデータ伝送を管理します。Management Center では、システムによって作成されたバイナリファイルを分析して、イベント、接続データ、およびネットワークマップを生成します。最初のステップでは、**diskmanager.log** ファイルを調べて、次のような重要な情報を収集します。

- ドレインの頻度。

- 未処理イベントを含むファイルがドレインされた数。
- 未処理イベントによるドレインの発生。

ディスクマネージャプロセスが実行されるたびに、各サイロのエントリが独自のログファイルに生成されます。エントリは、**[/ngfw]/var/log/diskmanager.log** 下に存在します。diskmanager.log（CSV形式）から収集された情報は、原因の検索を絞り込むために使用できます。

その他のトラブルシューティング手順：

- コマンド **stats_unified.pl** は、Management Center に送信する必要があるデータが管理対象デバイスにあるかどうかを判断するのに役立ちます。この状態は、管理対象デバイスと Management Center で接続の問題が生じた場合に発生する可能性があります。管理対象デバイスは、ログデータをハードドライブに保存します。

  ```
  admin@FMC:~$ sudo stats_unified.pl
  ```

- **manage_proc.pl** コマンドは、Management Center 側のコリレータを再設定できます。

  ```
  root@FMC:~# manage_procs.pl
  ```

Cisco Technical Assistance Center（TAC）に問い合わせる前に

Cisco TACに連絡する前に、次の項目を収集することを強く推奨します。

- 表示される正常性アラートのスクリーンショット。
- Management Center から生成されたトラブルシュートファイル。
- 影響を受ける管理対象デバイスから生成されたトラブルシュートファイル。

  問題が最初に検出された日時。

- ポリシーに最近加えられた変更に関する情報（該当する場合）。

  通信のボトルネック：SFDataCorrerator （534 ページ）で説明されている stats_unified.pl コマンドの出力。

デバイス設定履歴ファイルのディスク使用量

[ディスク使用量（Disk Usage）] 正常性モジュールは、Management Center 上のデバイス設定履歴ファイルのサイズをモニターし、サイズが許容制限を超えると正常性アラートを送信します。デバイス設定履歴ファイルの保存に関する最大許容ディスクサイズは 20 GB です。Management Center の高可用性展開では、この正常性アラートは、高可用性同期が一時停止されている場合にのみスタンバイ Management Center に表示されます。

デバイス設定履歴ファイルのサイズが許容制限を超えると、Management Center のアップグレード中にアップグレードの準備に失敗する可能性があります。Management Center の高可用性展開では、デバイス設定履歴ファイルのサイズ制限を超えると、高可用性同期速度が低下する可能性があります。

デバイス設定履歴ファイルサイズの正常性アラートを解消するには、**[展開（Deploy）]**>**[展開履歴（Deployment History）]**>**[展開設定（Deployment Setting）]**>**[設定バージョンの設定（Configuration Version Setting）]**を選択し、[保持するバージョンの数（Number of Versions to Retain）]を減らします。バージョンの数を減らすと、選択したバージョンサイズと一致するように最も古い設定バージョンが削除されます。[設定バージョンの推定サイズ（Estimated Configuration Version Size）]は、保持することを選択したバージョンの数に基づいて、Management Center 上の設定履歴ファイルのおおよそのサイズを提供します。推定値を使用してバージョンの数を変更し、設定バージョンのサイズを許容制限未満に減らします。

詳細については、『Cisco Secure Firewall Management Center Device Configuration Guide』の「*Set the Number of Configuration Versions*」を参照してください。

トラブルシューティング用のヘルス モニター レポート

アプライアンスで問題が発生したときに、問題の診断に役立つように、サポートからトラブルシューティング ファイルを提供するように依頼されることがあります。システムは、特定の機能分野を対象とした情報を含むトラブルシューティング ファイルと、高度なトラブルシューティング ファイル（このファイルはサポートと連携して取得します）を生成することができます。次の表に示すオプションのいずれかを選択して、特定の機能のトラブルシューティング ファイルの内容をカスタマイズできます。

一部のオプションは報告対象のデータの点で重複していますが、トラブルシューティング ファイルには、オプションの選択に関係なく冗長コピーは含まれません。

表 47: 選択可能なトラブルシュート オプション

オプション	報告内容
Snort のパフォーマンスと設定（Snort Performance and Configuration）	アプライアンス上の Snort に関連するデータと構成設定
ハードウェア パフォーマンスとログ（Hardware Performance and Logs）	アプライアンス ハードウェアのパフォーマンスに関連するデータとログ
システムの設定、ポリシー、ログ（System Configuration, Policy, and Logs）	アプライアンスの現在のシステム設定に関連する構成設定、データ、およびログ
検知機能の構成、ポリシー、ログ（Detection Configuration, Policy, and Logs）	アプライアンス上の検知機能に関連する構成設定、データ、およびログ
インターフェイスとネットワーク関連データ（Interface and Network Related Data）	アプライアンスのインラインセットとネットワーク設定に関連する構成設定、データ、およびログ
検知、認識、VDB データ、およびログ（Discovery, Awareness, VDB Data, and Logs）	アプライアンス上の現在の検出設定と認識設定に関連する構成設定、データ、およびログ
データおよびログのアップグレード（Upgrade Data and Logs）	アプライアンスの以前のアップグレードに関連するデータおよびログ

オプション	報告内容
All Database Data	トラブルシュート レポートに含まれるすべてのデータベース関連データ
All Log Data	アプライアンス データベースによって収集されたすべてのログ
ネットワーク マップ情報	現在のネットワーク トポロジ データ

特定のシステム機能のトラブルシューティング ファイルの生成

カスタマイズしたトラブルシューティング ファイルを生成およびダウンロードして、そのファイルをサポートに送信できます。

始める前に

このタスクを実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティ アナリスト ユーザー（読み取り専用）である必要があります。

手順

ステップ 1 デバイス正常性モニターの表示 （474 ページ）の手順を実行します。

ステップ 2 **システム**（⚙）**>[正常性（Health）]>[モニター（Monitor）]** の順に選択し、左側のパネルでデバイスをクリックして、[システムおよびトラブルシューティングの詳細を表示（View System & Troubleshoot Details）]、[トラブルシューティング ファイルの生成（Generate Troubleshooting Files）] の順にクリックします。

（注）
- Management Center Web インターフェイスから Management Center トラブルシューティング ファイルを生成すると、ファイルは Management Centerに保存されます。最新のトラブルシューティング ファイルのみが Management Center に保存されることに注意してください。
- Management Center Web インターフェイスから Threat Defense トラブルシューティング ファイルを生成すると、ファイルは Threat Defense で生成され、 Management Center にコピーされます。最新の Threat Defense トラブルシューティング ファイルのみが Management Center に保存されることに注意してください。
- Management Center と Threat Defense のトラブルシューティング ファイルが CLI から生成されると、トラブルシューティング ファイルのすべてのバージョンがそれぞれ Management Center と Threat Defense に保持されます。

ステップ 3 [全データ（All Data）] を選択して生成可能なすべてのトラブルシューティング データを生成することも、個別のボックスをオンにすることもできます。詳細については、タスクメッセージの表示 （529 ページ） を参照してください。

ステップ 4 [生成（Generate）] をクリックします。

ステップ 5 Message Center でタスク メッセージを表示します。タスクメッセージの表示 （529 ページ）を参照してください。

ステップ 6 生成されたトラブルシューティング ファイルに対応するタスクを探します。

ステップ 7 アプライアンスがトラブルシューティング ファイルを生成して、タスク ステータスが [完了（Completed）] に変わったら、[クリックして生成されたファイルを取得（Click to retrieve generated files）] をクリックします。

ステップ 8 ブラウザのプロンプトに従ってファイルをダウンロードします。(トラブルシューティング ファイルは、1 つの `.tar.gz` ファイルでダウンロードされます)。

ステップ 9 サポートの指示に従って、トラブルシューティング ファイルを Cisco に送信してください。

高度なトラブルシューティング ファイルのダウンロード

トラブルシューティング ファイルをダウンロードできます。

始める前に

このタスクを実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティ アナリスト ユーザー（読み取り専用）である必要があります。

手順

ステップ 1 アプライアンスの正常性モニターを表示します。、デバイス正常性モニターの表示 （474 ページ）を参照してください。

ステップ 2 **システム**（⚙） **>[正常性（Health）]>[モニター（Monitor）]** の順に選択し、左側のパネルでデバイスをクリックして、[システムおよびトラブルシューティングの詳細を表示（View System & Troubleshoot Details）]、[高度なトラブルシューティング（Advanced Troubleshooting）] の順にクリックします。

ステップ 3 [ファイルのダウンロード（File Download）] で、サポートから提供されたファイル名を入力します。

ステップ 4 [ダウンロード（Download）] をクリックします。

ステップ 5 ブラウザのプロンプトに従ってファイルをダウンロードします。

（注） 管理対象デバイスでは、システムはファイル名の前にデバイス名を付加してファイル名を変更します。

ステップ 6 サポートの指示に従って、トラブルシューティング ファイルを Cisco に送信してください。

一般的なトラブルシューティング

内部電源障害（ハードウェア障害、電源サージなど）や外部電源の障害（コードが外れている）によって、グレースフルでないシャットダウンまたは再起動が発生することがあります。これによってデータが破損することがあります。

接続ベースのトラブルシューティング

接続ベースのトラブルシューティングまたはデバッグにおいて、モジュール間で一貫したデバッグが提供され、特定の接続について適切なログを収集します。また、レベルベースのデバッグを最大7レベルまでサポートし、モジュール間で一貫したログ収集メカニズムを使用できます。接続ベースのデバッグでは、次の機能がサポートされています。

- Threat Defense の問題をトラブルシューティングする一般的な接続ベースのデバッグサブシステム
- モジュール間のデバッグメッセージで均一的な形式
- リブート後の永続的なデバッグメッセージ
- 既存の接続に基づくモジュール間のエンドツーエンドのデバッグ
- 進行中の接続のデバッグ

（注） 接続ベースのデバッグは、Firepower 2100 シリーズ デバイスではサポートされていません。

接続のトラブルシューティングの詳細については、接続のトラブルシューティング （539ページ）を参照してください。

接続のトラブルシューティング

手順

ステップ 1 **debug packet-condition** コマンドを使用して接続を識別するためのフィルタを設定します。

例：

```
Debug packet-condition match tcp 192.168.100.177 255.255.255.255 192.168.102.177
255.255.255.255
```

ステップ 2 対象モジュールおよび対応するレベルのデバッグを有効にします。**debug packet** コマンドを入力します。

例：

```
Debug packet acl 5
```

ステップ 3 次のコマンドを使用して、パケットのデバッグを開始します。

```
debug packet-start
```

ステップ 4 データベースからデバッグ メッセージを取得し、次のコマンドを使用してデバッグ メッセージを分析します。

```
show packet-debugs
```

ステップ 5 次のコマンドを使用して、パケットのデバッグを停止します。

```
debug packet-stop
```

Secure Firewall Threat Defense デバイスの高度なトラブルシューティング

Secure Firewall Threat Defense デバイスでは、パケットトレーサ機能とパケットキャプチャ機能を使って詳細なトラブルシューティング分析が可能です。パケットトレーサを使うと、ファイアウォール管理者はセキュリティアプライアンスに仮想パケットを注入し、入力から出力までのフローを追跡できます。このとき、パケットはフローおよびルーティング ルックアップ、ACL、プロトコルインスペクション、NAT、侵入検知に照らして評価されます。このユーティリティは、送信元および宛先のアドレスとプロトコルおよびポート情報を指定することにより、実際のトラフィックをシミュレートできるため、効果的です。パケットキャプチャにはトレースオプションがあり、このオプションを使用すれば、パケットがドロップされたか成功したかの判断を知ることができます。

トラブルシューティング ファイルの詳細については、高度なトラブルシューティング ファイルのダウンロード （538 ページ）を参照してください。

パケット キャプチャの概要

トレースオプションを有効にしたパケットキャプチャ機能では、入力インターフェイスでキャプチャされた実際のパケットをシステム内でトレースできます。トレース情報は後で表示されます。キャプチャしたパケットは、実際のデータ パス トラフィックであるため、出力インターフェイスでドロップされません。Threat Defense デバイスのパケットキャプチャは、データパケットのトラブルシューティングおよび分析をサポートします。

パケットをキャプチャすると、Snort がパケットで有効になっているトレースフラグを検出します。Snortは、パケットが通過するトレーサエレメントを書き込みます。パケットキャプチャの結果、Snort は次のいずれかの判定結果を出します。

表 *48* : *Snort* の判定

判定	説明
成功（Pass）	分析されたパケットを許可します。
ブロック（Block）	転送されないパケット。
置換（Replace）	変更されたパケット。
許可フロー（AllowFlow）	インスペクションなしで転送されるフロー。
ブロックフロー（BlockFlow）	フローがブロックされました。
無視	フローがブロックされました。パッシブインターフェイスでフローがブロックされているセッションでのみ発生します。
再試行	フローが停止し、enamelware またはURL カテゴリ/レピュテーションクエリを待機しています。タイムアウトが発生した場合、処理は続行され、結果は不明になります。enamelware の場合、ファイルは許可されます。URL カテゴリ/レピュテーションの場合、ACルールルックアップは未分類の不明なレピュテーションで続行されます。

Snort の判定に基づいて、パケットはドロップまたは許可されます。たとえば、Snort の判定が **[ブロックフロー（BlockFlow）]** である場合、パケットはドロップされ、セッション内の後続のパケットは Snort に到達する前にドロップされます。Snort の判定が [ブロック（Block）] または **[ブロックフロー（BlockFlow）]** の場合、[ドロップ理由（Drop Reason）] は次のいずれかになります。

表 *49* : ドロップ理由

ブロックまたはフローブロックの実行元	原因
Snort	Snort がパケットを処理できません。たとえば、パケットが破損しているか、無効な形式であるため、Snortがパケットを復号化できません。
前処理されたアプリケーション ID	アプリケーション ID モジュール/前処理されたアプリケーションIDは、それ自体はパケットをブロックしません。ただし、これは、アプリケーションID検出が原因で他のモジュール（ファイアウォールなど）がブロッキングルールに一致することを示している可能性があります。

ブロックまたはフローブロックの実行元	原因
前処理された SSL	SSL ポリシーにトラフィックと一致するブロック/リセットルールがあります。
ファイアウォール	ファイアウォールポリシーにトラフィックと一致するブロック/リセットルールがあります。
前処理されたキャプティブポータル	トラフィックと一致する、ID ポリシーを使用するブロック/リセットルールがあります。
前処理されたセーフサーチ	トラフィックと一致する、ファイアウォールポリシーのセーフサーチ機能を使用するブロック/リセットルールがあります。
前処理された SI	AC ポリシーの [セキュリティインテリジェンス（Security Intelligence）] タブに、トラフィックをブロックするブロック/リセットルールがあります（DNS または URL SI ルールなど）。
前処理された filterer	AC ポリシーの [filterer] タブに、トラフィックと一致するブロック/リセットルールがあります。
前処理されたストリーム	侵入ルールのブロッキング/リセットストリーム接続があります（TCP 正規化エラー時のブロッキングなど）。
前処理されたセッション	このセッションは他のモジュールによってすでにブロックされているため、前処理されたセッションが同じセッションの以降のパケットをブロックしています。
前処理されたフラグメンテーション	データの以前のフラグメントがブロックされているため、ブロックしています。
前処理された snort 応答	たとえば、特定の HTTP トラフィックで応答ページを送信する、react snort ルールがあります。
前処理された snort 応答	条件に一致するパケットに、カスタム応答を送信する snort ルールがあります。
前処理されたレピュテーション	パケットがレピュテーションルール（特定の IP アドレスのブロッキングなど）に一致しています。
前処理された x-Link2State	SMTP で検出されたバッファオーバーフローの脆弱性によるブロッキング。

ブロックまたはフローブロックの実行元	原因
前処理された back orifice	back orifice データの検出によるブロッキング。
前処理された SMB	SMB トラフィックをブロックする snort ルールがあります。
前処理されたファイルプロセス	ファイルをブロックするファイルポリシーがあります（enamelware ブロッキングなど）。
前処理された IPS	IPS を使用する snort ルールがあります（レートフィルタリングなど）。

パケット キャプチャ機能を使用すると、システム メモリに保存されているパケットをキャプチャしてダウンロードできます。ただし、メモリの制約により、バッファ サイズは 32 MB に制限されます。大量のパケット キャプチャを処理できるシステムはすぐに最大バッファ サイズを超過するため、パケットキャプチャの制限を増やす必要があります。これを行うには、セカンダリ メモリを使用します（ファイルを作成してキャプチャ データを書き込む）。サポートされている最大ファイル サイズは 10 GB です。

file-size を設定すると、キャプチャされたデータがファイルに保存され、キャプチャ名 **recapture** に基づいてファイル名が割り当てられます。

ファイル サイズ オプションは、32 MB 以上のサイズ制限のパケットをキャプチャする必要がある場合に使用されます。

詳細については、Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。

キャプチャ トレースの使用

パケットキャプチャは、定義された基準に基づいてデバイスの指定されたインターフェイスを通過するネットワークトラフィックのライブスナップショットを提供するユーティリティです。このプロセスは、一時停止していない限り、または割り当てられたメモリが使い果たされていない限り、パケットのキャプチャを続行します。

パケット キャプチャ データには、パケットの処理中にシステムが行う決定とアクションに関する Snort とプリプロセッサからの情報が含まれています。一度に複数のパケット キャプチャを実行できます。キャプチャの変更、削除、クリア、保存を実行するようにシステムを設定できます。

（注） パケットデータのキャプチャには、パケットのコピーが必要です。この操作によって、パケットの処理中に遅延が生じる可能性があります。また、パケットのスループットが低下する可能性もあります。特定のデータトラフィックをキャプチャするためにパケットフィルタを使用することをお勧めします。

始める前に

Secure Firewall Threat Defense デバイスでパケットキャプチャツールを使用するには、管理者またはメンテナンスユーザーである必要があります。

手順

ステップ 1 Management Center で、**[デバイス（Devices）]** > **[パケットキャプチャ（Packet Capture）]** を選択します。

ステップ 2 デバイスを選択します。

ステップ 3 **[キャプチャの追加（Add Capture）]** をクリックします。

ステップ 4 トレースのキャプチャの [名前（Name）] を入力します。

ステップ 5 トレースのキャプチャの [インターフェイス（Interface）] を選択します。

ステップ 6 以下の [一致基準（Match Criteria）] の詳細を指定します。

a) [プロトコル（Protocol）] を選択します。
b) [送信元ホスト（Source Host）] の IP アドレスを入力します。
c) [宛先ホスト（Destination Host）] の IP アドレスを入力します。
d) （オプション）[SGT 番号（SGT number）] チェックボックスをオンにし、セキュリティグループ タグ（SGT）を入力します。

ステップ 7 以下の [バッファ（Buffer）] の詳細を指定します。

a) （オプション）最大 [パケット サイズ（Packet Size）] を入力します。
b) （オプション）最小 [バッファ サイズ（Buffer Size）] を入力します。
c) 中断せずにトラフィックをキャプチャしたい場合は、[連続キャプチャ（Continuous Capture）] を選択し、最大バッファ サイズに到達したらキャプチャを停止したい場合は、[いっぱいになったら停止（Stop when full）] を選択します。

（注） [連続キャプチャ（Continues Capture）] がオンになっている場合、割り当てられたメモリがいっぱいになると、メモリ内の最も古いキャプチャ済みパケットが、新しくキャプチャされたパケットで上書きされます。

d) 各パケットの詳細をキャプチャする場合は、[トレース（Trace）] チェックボックスをオンにします。
e) [トレース数（Trace Count）] フィールドに値を入力します。デフォルト値は 128 です。1 ～ 1000 の範囲で値を入力できます。

ステップ 8 [保存（Save）] をクリックします。

パケットキャプチャ画面に、パケットキャプチャの詳細とそのステータスが表示されます。パケットキャプチャページを自動更新するには、[自動更新の有効化（Enable Auto Refresh）] チェックボックスをオンにして、自動更新間隔を秒単位で入力します。

パケットキャプチャでは、次の操作を実行できます。

- **[編集（Edit）]**（✎）：キャプチャ基準を変更できます。

- [削除（Delete）]（  ）：パケットキャプチャとキャプチャされたパケットを削除できます。
- **[クリア（Clear）]**（  ）：1 つのパケットキャプチャから、キャプチャされたすべてのパケットを消去できます。既存のすべてのパケットキャプチャから、キャプチャされたパケットを消去するには、[すべてのパケットをクリア（Clear All Packets）] をクリックします。
- [一時停止（Pause）]（  ）：パケットのキャプチャを一時的に停止できます。
- **[保存（Save）]**（  ）：キャプチャされたパケットのコピーを ASCII または PCAP 形式でローカルマシンに保存できます。必要な形式オプションを選択し、[保存（Save）] をクリックします。保存されたパケットキャプチャがローカルマシンにダウンロードされます。
- キャプチャされているパケットの詳細を表示するには、必要なキャプチャ行をクリックします。

パケット トレーサの概要

パケットトレーサツールを使用すると、送信元および宛先のアドレスとプロトコルの特性によってパケットをモデル化することにより、ポリシー設定をテストできます。トレースでは、ポリシールックアップが実行され、設定済みのアクセスルール、NAT、ルーティング、アクセスポリシー、レート制限ポリシーに基づいてパケットが許可されるか拒否されるかが確認されます。パケットフローは、インターフェイス、送信元アドレス、宛先アドレス、ポート、プロトコルに基づいてシミュレートされます。この方式でパケットをテストすることによって、ポリシーの有効性を確認し、必要に応じて、許可または拒否するトラフィックのタイプが処理されるかどうかをテストできます。

設定の確認に加えて、トレーサを使用して、アクセスを許可すべきパケットが拒否されるなどの予期せぬ動作をデバッグできます。パケットを完全にシミュレートするために、パケットトレーサはデータパス（低速パスモジュールと高速パスモジュール）をトレースします。当初は、処理が、セッション単位またはパケット単位のトランザクションとして行われていました。ファイアウォールがセッション単位またはパケット単位でパケットを処理する際は、パケットトレーサツールと「トレースによるキャプチャ」機能により、パケット単位でトレースデータがログに記録されます。

PCAP ファイル

PCAP ファイルを使用してパケットトレーサを開始できます。これにより、完全なフローが実現されます。現時点では、単一の TCP/UDP ベースのフローおよび最大 100 パケットでの PCAP のみがサポートされています。パケットトレーサツールは、PCAP ファイルを読み取り、クライアントとサーバーのリプレイエンティティの状態を初期化します。ツールは、後続の処理と表示のために PCAP 内の各パケットのトレース出力を収集して保存することで、同期方式でパケットのリプレイを開始します。

PCAP リプレイ

パケットリプレイは、PCAP ファイル内のパケットのシーケンスによって実行されます。リプレイアクティビティへの干渉があると、リプレイアクティビティが中断され、リプレイが終了します。指定された入力インターフェイスおよび出力インターフェイスにおける PCAP のすべてのパケットについてトレース出力が生成されるため、フロー評価の完全なコンテキストが提供されます。

PCAP リプレイは、リプレイ中にパケットを動的に変更する一部の機能（IPsec、VPN、SSL、HTTP 復号、NAT など）ではサポートされません。

パケット トレーサの使用

Secure Firewall Threat Defense デバイスでパケットトレーサを使用するには、管理者またはメンテナンスユーザーである必要があります。

手順

ステップ 1 Management Center で、**デバイス** > **パケットトレーサ** を選択します。

ステップ 2 [デバイスの選択（Select Device）] ドロップダウンリストから、トレースを実行するデバイスを選択します。

ステップ 3 [入力インターフェイス（Ingress Interface）] ドロップダウンリストから、パケットトレース用の入力インターフェイスを選択します。

（注） [VTI] を選択しないでください。パケットトレーサでは、入力インターフェイスとしての VTI はサポートされていません。

ステップ 4 パケットトレーサで PCAP リプレイを使用するには、次の手順を実行します。

a) [PCAPファイルの選択（Select a PCAP File）] をクリックします。

b) 新しい PCAP ファイルをアップロードするには、[PCAPファイルのアップロード（Upload a PCAP file）] をクリックします。最近アップロードしたファイルを再利用するには、リストからファイルをクリックします。

（注） .pcap および .pcapng ファイル形式のみがサポートされています。PCAP ファイルには、最大 100 パケットの TCP/UDP ベースのフローを 1 つだけ含めることができます。PCAP ファイル名（ファイル形式を含む）の最大文字数は 64 文字です。

c) [PCAPのアップロード（Upload PCAP）] ボックスで、PCAP ファイルをドラッグするか、ボックスをクリックしてファイルを参照およびアップロードすることができます。ファイルを選択すると、アップロードプロセスが自動的に開始されます。

d) このステップ 13に進みます。

ステップ 5 トレースパラメータを定義するには、[プロトコル（Protocol）] ドロップダウンメニューからトレースのパケットタイプを選択し、プロトコル特性を指定します。

- [ICMP]：ICMP タイプ、ICMP コード（0 ～ 255）、およびオプションで ICMP 識別子を入力します。
- [TCP/UDP/SCTP]：送信元および宛先のポート番号を入力します。

- [GRE/IPIP]：プロトコル番号（0 ～ 255）を入力します。
- [ESP]：送信元の SPI 値（0 ～ 4294967295）を入力します。
- [RAWIP]：プロトコル番号（0 ～ 255）を入力します。

ステップ 6 パケットトレースの [送信元タイプ（Source Type）] を選択し、送信元 IP アドレスを入力します。

送信元と宛先のタイプとして、IPv4、IPv6、完全修飾ドメイン名（FQDN）を選択できます。Cisco TrustSec を使用する場合、IPv4 または IPv6 アドレスと FQDN を指定できます。

ステップ 7 パケット トレースの [送信元ポート（Source Port）] を選択します。

ステップ 8 パケット トレースの [宛先（Destination）] タイプを選択し、宛先 IP アドレスを入力します。

宛先タイプのオプションは、選択した送信元タイプによって異なります。

ステップ 9 パケット トレースの [宛先ポート（Destination Port）] を選択します。

ステップ 10 オプションで、セキュリティ グループ タグ（SGT）値がレイヤ 2 CMD ヘッダー（TrustSec）に組み込まれているパケットをトレースする場合、有効な [SGT 番号（SGT number）] を入力します。

ステップ 11 パケット トレーサで親インターフェイスに入力する（後でサブインターフェイスにリダイレクトされる）場合は、[VLAN ID] を入力します。

インターフェイス タイプはすべてサブインターフェイスで設定するため、これはサブインターフェイスを使用しない場合だけのオプションです。

ステップ 12 パケット トレースの [宛先 MAC アドレス（Destination MAC Address）] を指定します。

Secure Firewall Threat Defense デバイスをトランスペアレント ファイアウォール モードで実行していて、入力インターフェイスが VTEP であるとき、[VLAN ID] に値を入力する場合は、[宛先 MAC アドレス（Destination MAC Address）] は必須になります。一方、インターフェイスがブリッジ グループのメンバーであるとき、[VLAN ID] に値を入力する場合は [宛先 MAC アドレス（Destination MAC Address）] はオプションですが、[VLAN ID] に値を入力しない場合は必須になります。

Secure Firewall Threat Defense をルーテッド ファイアウォール モードで実行しているときに、入力インターフェイスがブリッジグループのメンバーである場合、[VLAN ID] と [宛先MACアドレス（Destination MAC Address）] はオプションになります。

ステップ 13 （任意）パケットトレーサで、シミュレートされたパケットのセキュリティチェックを無視する場合は、[シミュレートされたパケットのすべてのセキュリティチェックをバイパスする（Bypass all security check for Simulated packet）] をクリックします。これにより、パケットトレーサは、これを設定しないとシステムを通過するときにドロップされるパケットのトレースを継続できるようになります。

ステップ 14 （任意）デバイスから出力インターフェイスを介してパケットを送信できるようにするには、[シミュレートされたパケットがデバイスから送信できるようにする（Allow Simulated packet to transmit from device）] をクリックします。

ステップ 15 （任意）パケットトレーサで、インジェクトされたパケットを IPsec/SSL VPN で復号されたパケットと見なすようにするには、[シミュレートされたパケットをIPsec/SSL VPN復号として扱う（Treat simulated packet as IPsec/SSL VPN decrypt）] をクリックします。

ステップ 16 [トレース（Trace）] をクリックします。

[トレース結果（Trace Result）] には、PCAP パケットがシステムを通過した各フェーズの結果が表示されます。個々のパケットのトレース結果を表示するには、そのパケットをクリックします。次を実行できます。

- トレース結果をクリップボードにコピー（）します。
- 表示される結果を展開したり折りたたんだり（）します。
- トレース結果画面を最大化（）します。

要した処理能力の測定に役立つ経過時間情報が、フェーズごとに表示されます。入力インターフェイスから出力インターフェイスへのパケットフロー全体にかかった合計時間も、結果セクションに表示されます。

[トレース履歴（Trace History）] ペインには、PCAP トレースごとに保存されたトレースの詳細が表示されます。最大 100 のパケットトレースを保存できます。保存されたトレースを選択して、パケット トレース アクティビティを再度実行できます。次を実行できます。

- 任意のトレースパラメータの使用してトレースを検索します。
- ボタンを使用して、履歴へのトレースの保存を無効にします。
- 特定のトレース結果を削除します。
- すべてのトレースをクリアします。

Web インターフェイスから Threat Defense 診断 CLI を使用する方法

Management Center から選択した Threat Defense 診断 CLI コマンドを実行できます。コマンド **ping**（**ping system** を除く）、**traceroute**、および一部の **show** コマンドは、通常の CLI ではなく診断 CLI で実行されます。

show コマンドを実行したときに、「`Unable to execute the command properly. Please see logs for more details`」（コマンドを正しく実行できません。詳細については、ログを参照してください）というメッセージが表示される場合は、そのコマンドが診断 CLI で無効であることを意味します。たとえば、**show access-list** は機能しますが、**show access-control-policy** と入力すると、このメッセージが表示されます。非診断コマンドを使用するには、SSH を使用して Management Center の外部のデバイスにログインします。

Threat Defense CLI の詳細については、Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。

始める前に

- 診断CLIを使用するには、管理者、メンテナンス、またはセキュリティアナリストである必要があります。
- 診断CLIの目的は、デバイスのトラブルシューティングに役立ついくつかのコマンドをすばやく使用できるようにすることです。すべてのコマンドにアクセスするには、デバイスとの SSH セッションを直接開きます。
- Management Center 高可用性を使用する展開では、診断 CLI は、アクティブ Management Center でのみ使用できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[脅威対策CLI（Threat Defense CLI）]**を選択します。

また、デバイスの正常性モニター（**システム**（⚙）> **[正常性（Health）]** > **[モニタ（Monitor）]**）から CLI ツールにアクセスすることもできます。そこから、デバイスを選択し、[システムとトラブルシューティングの詳細を表示（View System and Troubleshoot Details）] リンクをクリックし、[高度なトラブルシューティング（Advanced Troubleshooting）] をクリックして、そのページで [Threat Defense CLI] をクリックします。

ステップ 2 [デバイス（Device）] ドロップダウンリストから、診断コマンドを実行するデバイスを選択します。

ステップ 3 [コマンド（Command）] ドロップダウンリストから、実行するコマンドを選択します。

ステップ 4 [パラメータ（Parameters）] フィールドにコマンドパラメータを入力します。

有効なパラメータについては、Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。

たとえば、**show access-list** コマンドを実行するには、[コマンド（Command）] ドロップダウンリストから **show** を選択し、[パラメータ（Parameters）] フィールドに **access-list** と入力します。

（注） [パラメータ（Parameters）] フィールドにコマンド全体を入力しないでください。関連するキーワードのみを入力してください。

ステップ 5 [実行（Execute）] をクリックして、コマンド出力を表示します。

「`Unable to execute the command properly. Please see logs for more details.`」（コマンドを正しく実行できません。詳細については、ログを参照してください）というメッセージが表示される場合は、パラメータをよく確認してください。構文エラーがある可能性があります。

このメッセージは、実行しようとしているコマンドが診断 CLI（**system support diagnostic-cli** コマンドを使用してデバイスからアクセスした）のコンテキスト内で有効なコマンドではないことを意味する場合もあります。これらのコマンドを使用するには、SSH を使用してデバイスにログインします。

機能固有のトラブルシューティング

機能固有のトラブルシューティングのヒントやテクニックについては、次の表を参照してください。

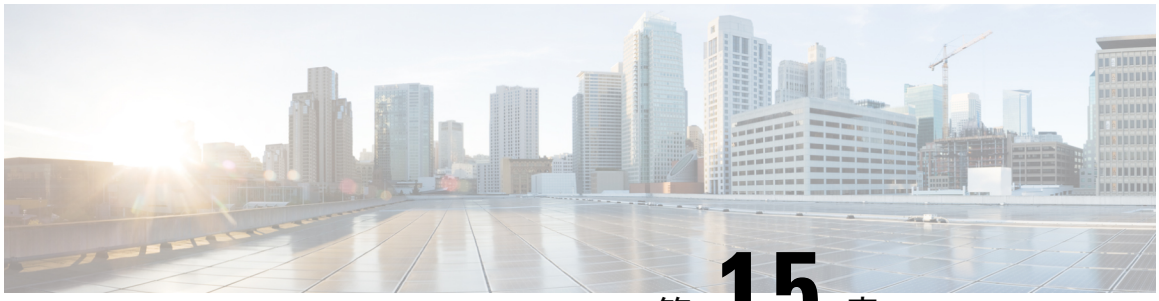
表 *50* : 機能固有のトラブルシューティング トピック

機能	関連するトラブルシューティング情報
アプリケーション制御	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Best Practices for Application Control*」
LDAP 外部認証	LDAP 認証接続のトラブルシューティング （237 ページ）
ライセンシング	スマート ライセンスのトラブルシューティング （340 ページ） 特定のライセンスの予約のトラブルシューティング （355 ページ）
Management Center ハイ アベイラビリティ	Management Center のハイ アベイラビリティのトラブルシューティング （367 ページ）
ユーザ ルール条件	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Troubleshoot User Control*」
ユーザ アイデンティティ ソース	ISE/ISE-PIC、TS エージェント アイデンティティ ソース、キャプティブ ポータル アイデンティティ ソース、およびリモートアクセス VPN アイデンティティソースに関するトラブルシューティング情報については、Cisco Secure Firewall Management Center デバイス構成ガイドの対応する項を参照してください。 LDAP 認証接続のトラブルシューティング （237 ページ）
URL フィルタリング	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Troubleshoot URL Filtering*」
レルムとユーザ データのダウンロード	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Troubleshoot Realms and User Downloads*」
ネットワーク検出	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Troubleshooting Your Network Discovery Strategy*」
カスタム セキュリティ グループ タグ（SGT）のルール条件	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Custom SGT Rule Conditions*」
SSL ルール	Cisco Secure Firewall Device Manager Configuration Guideの SSL ルールに関する章
Cisco Threat Intelligence Director（TID）	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Troubleshoot Secure Firewall Threat Intelligence Director*」

機能	関連するトラブルシューティング情報
Secure Firewall Threat Defense syslog	Cisco Secure Firewall Management Center デバイス構成ガイドの「*About Configuring Syslog*」
侵入パフォーマンス統計	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Intrusion Performance Statistic Logging Configuration*」
接続ベースのトラブルシューティング	接続ベースのトラブルシューティング （539 ページ）

第 IV 部

ツール



第 15 章

バックアップ/復元

バックアップと復元について

災害から回復する能力は、システム保守計画の重要な部分を占めます。災害復旧計画の一環として、セキュアなリモートの場所への定期的なバックアップを実行することをお勧めします。

オンデマンドバックアップ

Management Center から Management Centerおよび多数の Threat Defense デバイスのオンデマンドバックアップを実行できます。

詳細については、「Management Center または管理対象デバイスのバックアップ （566 ページ）」を参照してください。

スケジュール バックアップ

Management Centerでスケジューラを使用して、バックアップを自動化できます。Management Center からデバイスのリモートバックアップをスケジュールすることもできます。

Management Center のセットアッププロセスでは、設定のみのバックアップを毎週ローカルに保存するようにスケジュールされます。これは、オフサイトのフルバックアップの代わりにはなりません。初期設定が完了したら、スケジュールされたタスクを確認し、組織のニーズに合わせて調整する必要があります。

詳細については、「スケジュール バックアップ （600 ページ）」を参照してください。

バックアップファイルの保存

バックアップはローカルに保存することができます。ただし、NFS、SMB、またはSSHFSネットワークボリュームをリモートストレージとしてマウントして、Management Center および管理対象デバイスを安全なリモートロケーションにバックアップすることをお勧めします。これを実行すると、その後のすべてのバックアップがそのボリュームにコピーされますが、引き続き Management Center を使用してそれらを管理することができます。

詳細については、リモートストレージデバイス（111 ページ）およびバックアップとリモートストレージの管理 （590 ページ）を参照してください。

Management Center および管理対象デバイスの復元

ローカルの [バックアップ管理（Backup Management）] ページから Management Centerを復元します。Threat Defense デバイスを復元するには、Threat Defense CLI を使用する必要があります。ただし、SD カードと [Reset] ボタンを使用する ISA 3000 ゼロタッチ復元は除きます。

詳細については、「Management Center および管理対象デバイスの復元 （572 ページ）」を参照してください。

バックアップの内容

Management Center のバックアップには、次のものを含めることができます。

- 設定。

  Management Center Web インターフェイスで指定できるすべての設定は、リモートストレージと監査ログサーバー証明書の設定を除いて、設定のバックアップに含まれます。マルチドメイン展開では、設定をバックアップする必要があります。イベントまたはTIDデータのみをバックアップすることはできません。

- イベント。

  イベントのバックアップには、Management Center データベース内のすべてのイベントが含まれます。ただし、Management Center のイベントバックアップには侵入イベントのレビューステータスは含まれません。復元された侵入イベントは、[確認済みイベント（Reviewed Events）] ページには表示されません。

- Threat Intelligence Director（TID）データ。

  詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの「*About Backing Up and Restoring Threat Intelligence Director Data*」を参照してください。

デバイスバックアップは常に設定のみです。

復元の内容

設定を復元すると、ごくわずかの例外を除いて、バックアップされたすべての設定が上書きされます。Management Center では、イベントおよび TID データを復元すると、侵入イベントを除くすべての既存のイベントおよび TID データが上書きされます。

次のことを理解して計画してください。

- バックアップされていないものは復元できません。

  Management Center の設定のバックアップには、リモートストレージと監査ログサーバー証明書の設定が含まれないため、復元後にそれらを再設定する必要があります。また、Management Center のイベントのバックアップには侵入イベントのレビューステータスが含まれないため、復元された侵入イベントは [確認済みイベント（Reviewed Events）] ページには表示されません。

- VPN 証明書の復元は失敗します。

  Threat Defense 復元プロセスでは、VPN 証明書およびすべての VPN 設定が Threat Defense デバイスから削除されます。これには、バックアップの作成後に追加された証明書も含まれます。Threat Defense デバイスを復元した後に、すべての VPN 証明書を再追加/再登録し、デバイスを再展開する必要があります。

- 工場出荷時または再イメージ化された FMC ではなく、設定済みの Management Center に復元すると、侵入イベントおよびファイルリストがマージされます。

  Management Center のイベント復元プロセスでは、侵入イベントは上書きされません。代わりに、バックアップ内の侵入イベントがデータベースに追加されます。重複を避けるには、復元する前に既存の侵入イベントを削除してください。

  Management Center の設定復元プロセスでは、マルウェア防御 で使用されるクリーンおよびカスタム検出ファイルリストは上書きされません。代わりに、既存のファイルリストとバックアップ内のファイルリストがマージされます。ファイルリストを置き換えるには、復元する前に既存のファイルリストを削除してください。

バックアップと復元の要件

バックアップと復元には次の要件があります。

モデル要件：バックアップ

次をバックアップできます。

- Management Center。
- コンテナインスタンスを含むハードウェアで実行されている Threat Defense（）。
- プライベートクラウド用の Threat Defense Virtual （クラスタ化されたデバイスおよび KVM 用の Threat Defense Virtual を除く）。
- プライベートクラウド用の Threat Defense Virtual （KVM 用の Threat Defense Virtual を除く）。
- AWS のThreat Defense Virtual （クラスタ化されたデバイスを除く）。バックアップは、他のパブリッククラウド展開ではサポートされていません。
- AWS のThreat Defense Virtual （クラスタ化されたデバイスを除く）。バックアップは、他のパブリッククラウド展開ではサポートされていません。

バックアップと復元がサポートされていないデバイスを交換する必要がある場合は、デバイス固有の設定を手動で再作成する必要があります。ただし、Management Center をバックアップすると、管理対象デバイスに展開するポリシーやその他の設定のほか、デバイスから Management Center にすでに送信されているイベントはバックアップされます。

モデル要件：復元

交換用の管理対象デバイスは、交換するものと同じモデルで、同じ数のネットワークモジュールと同じタイプおよび数の物理インターフェイスを備えている必要があります。

Management Center の場合、RMA シナリオでバックアップと復元を使用できるだけでなく、Management Center 間で設定とイベントを移行するためにバックアップと復元を使用できます。サポート対象の移行先モデルなどの詳細については、Cisco Secure Firewall Management Center モデル移行ガイド を参照してください。

バージョン要件

バックアップの最初のステップとして、パッチレベルを書き留めておきます。バックアップを復元するには、新旧のアプライアンスで、同じソフトウェアバージョン（パッチも含む）が実行されている必要があります。Firepower 4100/9300 シャーシを復元するには、互換性のある FXOS バージョンが実行されている必要があります。

Management Center バックアップの場合、同じ VDB または SRU が必要ではありません。ただし、バックアップを復元すると、既存の VDB がバックアップファイル内の VDB に置き換えられることに注意してください。復元された SRU または VDB バージョンが シスコ サポートおよびダウンロードサイトで利用可能なものより古い場合は、新しいバージョンをインストールすることをお勧めします。

ライセンス要件

ベストプラクティスと手順の説明に従って、ライセンスまたは孤立した権限付与の問題に対処してください。ライセンスの競合に気付いた場合は、Cisco TAC にお問い合わせください。

ドメインの要件

方法：

- Management Center のバックアップまたは復元：グローバルのみ。
- Management Center からデバイスをバックアップ：グローバルのみ。
- デバイスの復元：なし。CLI でデバイスをローカルに復元してください。

マルチドメイン展開では、イベント/TID データのみをバックアップすることはできません。設定もバックアップする必要があります。

バックアップと復元の注意事項と制限事項

バックアップと復元には次の注意事項と制限事項があります。

バックアップと復元はディザスタリカバリ/RMA 用です

バックアップと復元は、主に RMA シナリオを対象としています。問題または障害がある物理アプライアンスの復元プロセスを開始する前に、交換用のハードウェアについて Cisco TAC にお問い合わせください。

Management Center 間で設定とイベントを移行するためにバックアップと復元を使用することもできます。これにより、組織の拡大、物理実装から仮想実装への移行、ハードウェアの更新など、技術面またはビジネス面の理由による Management Center の交換が容易になります。

バックアップと復元は、コンフィギュレーションのインポート/エクスポートではありません

バックアップファイルは、アプライアンスを一意に識別する情報を含んでおり、共有することはできません。アプライアンスまたはデバイス間で設定をコピーする目的で、または新しい設定をテストする際に設定を保存する方法としてバックアップおよび復元プロセスを使用しないでください。代わりに、インポート/エクスポート機能を使用してください。

たとえば、Threat Defense デバイスのバックアップには、デバイスの管理 IP アドレスと、デバイスが管理 Management Center に接続するために必要なすべての情報が含まれます。別の Management Center によって管理されているデバイスに Threat Defense バックアップを復元しないでください（復元されたデバイスがバックアップで指定された Management Center への接続を試みるため）。

復元は個別かつローカルです

Management Center および管理対象デバイスは、個別かつローカルに復元します。これは、以下を意味します。

- 高可用性またはクラスタ化 Management Center またはデバイスに一括で復元することはできません。
- Management Center を使用してデバイスを復元することはできません。Management Center の場合は、Web インターフェイスを使用して復元することができます。Threat Defense デバイスの場合は、SD カードとリセットボタンを使用する ISA 3000 ゼロタッチ復元を除き、Threat Defense CLI を使用する必要があります。
- Management Center のユーザーアカウントを使用して、いずれかの管理対象デバイスにログインし、復元することはできません。Management Center とデバイスでは、独自のユーザーアカウントが維持されます。

Firepower 4100/9300 のコンフィギュレーションのインポート/エクスポートに関するガイドライン

Firepower 4100/9300 シャーシの論理デバイスとプラットフォームのコンフィギュレーション設定を含む XML ファイルをリモートサーバまたはローカルコンピュータにエクスポートするコンフィギュレーションのエクスポート機能を使用できます。そのコンフィギュレーションファイルを後でインポートして Firepower 4100/9300 シャーシに迅速にコンフィギュレーション設定

を適用し、よくわかっている構成に戻したり、システム障害から回復させたりすることができます。

ガイドラインと制限

- コンフィギュレーション ファイルの内容は、修正しないでください。コンフィギュレーション ファイルが変更されると、そのファイルを使用するコンフィギュレーション インポートが失敗する可能性があります。
- 用途別のコンフィギュレーション設定は、コンフィギュレーションファイルに含まれていません。用途別の設定やコンフィギュレーションを管理するには、アプリケーションが提供するコンフィギュレーション バックアップ ツールを使用する必要があります。
- Firepower 4100/9300 シャーシへのコンフィギュレーションのインポート時、Firepower 4100/9300 シャーシのすべての既存のコンフィギュレーション（論理デバイスを含む）は削除され、インポートファイルに含まれるコンフィギュレーションに完全に置き換えられます。
- RMA シナリオを除き、コンフィギュレーションファイルのエクスポート元と同じFirepower 4100/9300 シャーシだけにコンフィギュレーション ファイルをインポートすることをお勧めします。
- インポート先の Firepower 4100/9300 シャーシのプラットフォーム ソフトウェア バージョンは、エクスポートしたときと同じバージョンになるはずです。異なる場合は、インポート操作の成功は保証されません。シスコは、Firepower 4100/9300 シャーシをアップグレードしたりダウングレードしたりするたびにバックアップ設定をエクスポートすることを推奨します。
- インポート先のFirepower 4100/9300 シャーシでは、エクスポートしたときと同じスロットに同じネットワークモジュールがインストールされている必要があります。
- インポート先のFirepower 4100/9300 シャーシでは、インポートするエクスポートファイルに定義されているすべての論理デバイスに、正しいソフトウェアアプリケーションイメージがインストールされている必要があります。
- 既存のバックアップファイルが上書きされるのを回避するには、バックアップ操作内のファイル名を変更するか、既存のファイルを別の場所にコピーします。

（注） FXOS のインポート/エクスポートはFXOS の設定のみをバックアップするため、ロジックアプリを個別にバックアップする必要があります。FXOS の設定をインポートすると、論理デバイスが再起動され、工場出荷時のデフォルト設定でデバイスが再構築されます。

バックアップと復元のベストプラクティス

バックアップと復元には、次のベストプラクティスがあります。

バックアップのタイミング

メンテナンスの時間帯やその他の使用率の低い時間帯にバックアップすることをお勧めします。

バックアップデータの収集中に、データの相関付けが一時的に停止して（Management Center のみ）、バックアップ関連の設定を変更できなくなることがあります。イベントデータを含める場合、eStreamer などのイベント関連機能は使用できません。

次の状況でバックアップする必要があります。

- 定期的なスケジュールバックアップまたはオンデマンドバックアップ。

  災害復旧計画の一環として、定期的なバックアップを実行することをお勧めします。

  Management Center のセットアッププロセスでは、設定のみのバックアップを毎週ローカルに保存するようにスケジュールされます。これは、オフサイトのフルバックアップの代わりにはなりません。初期設定が完了したら、スケジュールされたタスクを確認し、組織のニーズに合わせて調整する必要があります。詳細については、スケジュールバックアップ （600 ページ）を参照してください。

- SLR が変更された後。

  特定ライセンス予約（SLR）に変更を加えた後に、Management Center をバックアップします。変更を加えてから古いバックアップを復元すると、特定ライセンスの戻りコードに問題が発生し、孤立した権限付与が発生する可能性があります。

- アップグレードまたは再イメージ化の前。

  アップグレードが致命的な失敗であった場合は、再イメージ化を実行し、復元する必要がある場合があります。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。最近のバックアップがある場合は、通常の操作にすばやく戻ることができます。

（注） バックアップから復元しても、再イメージ化または RMA 後に設定したパスワードはリセットされません。

- アップグレードの後。

  アップグレード後にバックアップします。これにより、新しくアップグレードした展開のスナップショットが得られます。新しい Management Center バックアップファイルがデバイスがアップグレードされたことを「認識」するように、管理対象デバイスをアップグレードした後に Management Center をバックアップすることをお勧めします。

バックアップファイルのセキュリティの維持

バックアップは、暗号化されていないアーカイブ（.tar）ファイルとして保存されます。

PKI オブジェクトの秘密キー（展開をサポートするために必要な公開キー証明書とペアになった秘密キーを表す）は、バックアップされる前に復号されます。バックアップを復元すると、このキーはランダムに生成されるキーで再暗号化されます。

（注） Management Center とデバイスを安全なリモートロケーションにバックアップし、転送が成功することを確認することをお勧めします。ローカルに残っているバックアップは、手動または（ローカルに保存されたバックアップが消去される）アップグレードプロセスによって削除される可能性があります。

特に、バックアップファイルは暗号化されていないため、不正アクセスを許可しないでください。バックアップ ファイルが変更されていると、復元プロセスは失敗します。Admin/Maint ロールを持つユーザーは [バックアップ管理（Backup Management）] ページにアクセスでき、そこでリモートストレージからファイルを移動および削除できることに注意してください。

Management Center のシステム設定では、NFS、SMB、または SSHFS ネットワークボリュームをリモートストレージとしてマウントできます。これを実行すると、その後のすべてのバックアップがそのボリュームにコピーされますが、引き続き Management Center を使用してそれらを管理することができます。詳細については、リモートストレージデバイス（111 ページ）およびバックアップとリモートストレージの管理（590 ページ）を参照してください。

Management Center だけがネットワークボリュームをマウントすることに注意してください。管理対象デバイスのバックアップファイルは、Management Center を介してルーティングされます。Management Center とそのデバイスの間に大容量のデータを転送するための帯域幅があることを確認します。詳細については、『Guidelines for Downloading Data from the Firepower Management Center to Managed Devices』（トラブルシューティング テクニカルノーツ）を参照してください。

Management Center ハイアベイラビリティ展開でのバックアップと復元

Management Center ハイアベイラビリティ展開では、一方の Management Center をバックアップしても他方はバックアップされません。定期的に両方のピアをバックアップする必要があります。一方の HA ピアを他方のバックアップファイルで復元しないでください。バックアップファイルは、アプライアンスを一意に識別する情報を含んでおり、共有することはできません。

正常なバックアップがなくても HA Management Center を交換できることに注意してください。正常なバックアップの有無にかかわらず、HA Management Center の交換の詳細については、高可用性ペアでの Management Center の交換（382 ページ）を参照してください。

Threat Defense ハイアベイラビリティ展開でのバックアップと復元

Threat Defense ハイアベイラビリティ展開では、次のことを行う必要があります。

- Management Center からデバイスペアをバックアップしますが、復元は Threat Defense CLI から個別かつローカルに行います。

バックアッププロセスにより、Threat Defense 高可用性デバイスの一意のバックアップファイルが生成されます。一方の高可用性ピアを他方のバックアップファイルで復元しないでください。バックアップ ファイルは、アプライアンスを一意に識別する情報を含んでおり、共有することはできません。

Threat Defense 高可用性デバイスの役割は、バックアップファイル名に示されます。復元する際は、必ず、適切なバックアップファイル（プライマリまたはセカンダリ）を選択してください。

- 復元する前に高可用性を一時停止または解除しないでください。

  高可用性設定を維持することで、交換用デバイスを、復元後に簡単に再接続できます。これを行うには、高可用性同期を再開する必要があることに注意してください。

- 両方のピアで **restore** CLI コマンドを同時に実行しないでください。

  バックアップが正常に完了したら、高可用性ペアの一方または両方のピアを交換できます。任意の物理的な交換タスク（ラックからの取り外し、ラックへの再設置など）を同時に実行できます。ただし、再起動を含め、最初のデバイスの復元プロセスが完了するまで、2 台目のデバイスで **restore** コマンドを実行しないでください。

正常なバックアップがなくても Threat Defense 高可用性デバイスを交換できます。

Threat Defense クラスタリング展開でのバックアップと復元

Threat Defense クラスタリング展開では、次の操作を行う必要があります。

- Management Center からクラスタ全体をバックアップし、Threat Defense CLI から個別かつローカルにノードを復元します。

  バックアッププロセスにより、クラスタノードごとに一意のバックアップファイルを含むバンドルされた tar ファイルが生成されます。あるノードを別のノードのバックアップファイルで復元しないでください。バックアップファイルには、デバイスを一意に識別する情報が含まれており、共有できません。

  ノードの役割は、そのバックアップファイル名に示されます。復元する際は、適切なバックアップファイル（制御またはデータ）を選択してください。

  個々のノードはバックアップできません。データノードがバックアップに失敗した場合でも、Management Center は他のすべてのノードを引き続きバックアップします。制御ノードのバックアップに失敗した場合、バックアップはキャンセルされます。

- 復元する前にクラスタリングを一時停止または解除しないでください。

  クラスタ設定を維持することで、復元後に交換用デバイスを簡単に再接続できます。

- 複数のノードで **restore** CLI コマンドを同時に実行しないでください。最初に制御ノードを復元し、クラスタに再参加するまで待ってから、データノードを復元することを推奨します。

  バックアップが正常に実行されている場合、クラスタ内の複数のノードを交換できます。任意の物理的な交換タスク（ラックからの取り外し、ラックへの再設置など）を同時に実

行できます。ただし、再起動を含め、前のノードの復元プロセスが完了するまで、追加のノードで **restore** コマンドを実行しないでください。

Firepower 4100/9300 シャーシのバックアップと復元

Firepower 4100/9300 シャーシで Threat Defense ソフトウェアを復元するには、シャーシで互換性のある FXOS バージョンが実行されている必要があります。

Firepower 4100/9300 シャーシをバックアップする場合は、FXOS 設定もバックアップすることを強くお勧めします。追加のベストプラクティスについては、Firepower 4100/9300 のコンフィギュレーションのインポート/エクスポートに関するガイドライン（559 ページ）を参照してください。

バックアップ前

バックアップの前に、次のことを行う必要があります。

- Management Center で VDB と SRU を更新します。

  常に最新の脆弱性データベース（VDB）と侵入ルール（SRU）を使用することをお勧めします。Management Center をバックアップする前に、シスコ サポートおよびダウンロード サイト の新しいバージョンがないか確認してください。

- ディスク容量を確認します。

  バックアップを開始する前に、アプライアンスまたはリモートストレージサーバーに十分なディスク容量があることを確認します。使用可能な容量は、[バックアップ管理（Backup Management）] ページに表示されます。

  十分な容量がない場合、バックアップが失敗する可能性があります。特にバックアップをスケジュールする場合は、必ず、バックアップファイルを定期的にプルーニングするか、リモートの保存場所により多くのディスク容量を割り当ててください。

復元前

復元の前に、次のことを行う必要があります。

- ライセンスの変更を元に戻します。

  バックアップを実行した後に行われたライセンス変更を元に戻します。

  そうしないと、復元後にライセンスの競合や孤立した権限付与が発生する可能性があります。ただし、Cisco Smart Software Manager（CSSM）の登録を解除しないでください。CSSM の登録を解除すると、復元後に再度登録を解除してから再登録する必要があります。

  復元が完了したら、ライセンスを再設定します。ライセンスの競合や孤立した権限付与に気付いた場合は、Cisco TAC にお問い合わせください。

- 障害のあるアプライアンスを切断します。

  管理インターフェイスを切断し、デバイスの場合はデータインターフェイスも切断します。

Threat Defense デバイスを復元すると、交換用デバイスの管理 IP アドレスが古いデバイスの管理 IP アドレスに設定されます。IP の競合を回避するには、バックアップを交換用デバイスに復元する前に、古いデバイスを管理ネットワークから切断します。

Management Center を復元しても管理 IP アドレスが変更されないことに注意してください。交換時に手動で設定する必要があります。必ず、設定する前に、古いアプライアンスをネットワークから切断してください。

- 管理対象デバイスの登録を解除しないでください。

  Management Center または管理対象デバイスのいずれを復元する場合でも、アプライアンスをネットワークから物理的に切断しても、デバイスの Management Center 登録を解除しないでください。

  登録を解除した場合は、一部のデバイス設定（セキュリティゾーンとインターフェイスのマッピングなど）をやり直す必要があります。復元後、Management Center とデバイスは正常に通信を開始します。

- 再イメージ化します。

  RMA シナリオでは、交換用アプライアンスは、工場出荷時のデフォルト設定で納品されます。ただし、交換用アプライアンスがすでに設定されている場合は、再イメージ化することをお勧めします。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。メジャーバージョンにのみ再イメージ化できるため、再イメージ化後にパッチの適用が必要な場合があります。

  再イメージ化しない場合は、Management Center の侵入イベントおよびファイルリストが上書きされるのではなくマージされることに注意してください。

復元後

復元の後に、次のことを行う必要があります。

- 復元されなかったものをすべて再設定します。

  これには、ライセンス、リモートストレージ、および監査ログサーバー証明書設定の再設定が含まれる場合があります。 また、失敗した Threat Defense VPN 証明書を再追加/再登録する必要があります。

- Management Center で VDB と SRU を更新します。

  常に最新の脆弱性データベース（VDB）と侵入ルール（SRU）を使用することをお勧めします。バックアップ内の VDB によって交換用 Management Center 上の VDB が上書きされるため、これは VDB にとって特に重要です。デバイスに変更を展開する前に、VDB を最新バージョンに更新します。

- 展開します。

  Management Center を復元したら、すべての管理対象デバイスに展開します。デバイスを復元後、[デバイス管理（Device Management）] ページから強制的に展開する必要があります。『Cisco Secure Firewall Management Center デバイス構成ガイド』の「デバイスへの既

存の設定の再展開」を参照してください。Management Center を復元するかデバイスを復元するかを問わず、必ず展開する必要があります。

Management Center または管理対象デバイスのバックアップ

サポートされるアプライアンスのオンデマンドバックアップまたはスケジュールバックアップを実行できます。

Management Center からデバイスをバックアップする場合、バックアッププロファイルは必要ありません。ただし、Management Center のバックアップにはバックアッププロファイルが必要です。。オンデマンド バックアップ プロセスでは、新しいバックアッププロファイルを作成できます。

のバックアップ Management Center

Management Center のオンデマンドバックアップを実行するには、次の手順を実行します。

始める前に

要件、ガイドライン、制限事項、およびベストプラクティスを確認し、理解する必要があります。 手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。

- バックアップと復元の要件 （557 ページ）
- バックアップと復元の注意事項と制限事項 （558 ページ）
- バックアップと復元のベストプラクティス （560 ページ）

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[バックアップ/復元（Backup/Restore）]** を選択します。

[バックアップ管理（Backup Management）] ページには、ローカルとリモートで保存されたすべてのバックアップが一覧表示されます。また、バックアップの保存に使用できるディスク容量も一覧表示されます。十分な容量がない場合、バックアップが失敗する可能性があります。

ステップ 2 既存のバックアッププロファイルを使用するか、新しく開始するかを選択します。

Management Center のバックアップでは、バックアッププロファイルを使用または作成する必要があります。

- 既存のバックアッププロファイルを使用するには、[バックアッププロファイル（Backup Profiles）] をクリックします。

使用するプロファイルの横にある編集アイコンをクリックします。[バックアップの開始（Start Backup）] をクリックして、今すぐバックアップを開始することができます。プロファイルを編集する場合は、次の手順に進みます。

- [Firepower 管理バックアップ（Firepower Management Backup）] をクリックして新しく開始し、新しいバックアッププロファイルを作成します。

  [名前（Name）] にバックアップファイルの名前を入力します。

ステップ 3 バックアップするものを選択します。

- **設定のバックアップ**。Management Center の高可用性で、アクティブ Management Center 上の設定のみのバックアップを選択する場合、デフォルトでは、アクティブとスタンバイの Management Center の両方が単一の統合バックアップファイルにバックアップされます。高可用性での Management Center の統合バックアップについては、高可用性の Management Center の統合バックアップ （388 ページ）を参照してください。
- **イベントのバックアップ**
- **Threat Intelligence Director のバックアップ**

マルチドメイン展開では、設定をバックアップする必要があります。イベントまたは TID データのみをバックアップすることはできません。これらの各選択肢のバックアップ対象および対象外の詳細については、バックアップと復元について （555 ページ）を参照してください。

ステップ 4 Management Center バックアップファイルの**保存場所**に注意してください。

これは、ローカルストレージ（`/var/sf/backup/`）またはリモート ネットワーク ボリュームのいずれかにすることができます。詳細については、「バックアップとリモートストレージの管理 （590 ページ）」を参照してください。

ステップ 5 （任意）[完了時にコピー（Copy when complete）] を有効にして、完了した Management Center バックアップをリモートサーバーにコピーします。

ホスト名または IP アドレス、リモートディレクトリへのパス、およびユーザー名とパスワードを入力します。パスワードの代わりに SSH 公開キーを使用するには、[SSH 公開キー（SSH Public Key）] フィールドの内容を、リモートサーバー上の指定ユーザーの `authorized_keys` ファイルにコピーします。

（注） このオプションは、バックアップをローカルに保存し、リモートの場所にも SCP で保存する場合に便利です。SSH リモートストレージを設定した場合は、[完了時にコピー（Copy when complete）] を使用してバックアップファイルを同じディレクトリにコピーしないでください。

ステップ 6 （任意）[電子メール（Email）] を有効にして、バックアップの完了時に通知する電子メールアドレスを入力します。

電子メール通知を受信するには、メールサーバーに接続するように Management Center を設定する必要があります（メール リレー ホストおよび通知アドレスの設定 （69 ページ））。

ステップ 7 [バックアップの開始（Start Backup）] をクリックしてオンデマンドバックアップを開始します。

既存のバックアッププロファイルを使用しない場合、システムが自動的に作成し、それを使用します。今すぐバックアップを実行しない場合は、[保存（Save）] または [新規として保存（Save As New）] をクリックしてプロファイルを保存することができます。どちらの場合も、新しく作成されたプロファイルを使用して、スケジュールされたバックアップを設定できます。

ステップ 8 デバイスが再起動するまで、Message Center で進行状況をモニターします。

バックアップデータの収集中に、データの相関付けが一時的に停止してバックアップ関連の設定を変更できなくなることがあります。リモートストレージが設定されている場合または [完了時にコピー（Copy when complete）] が有効になっている場合は、Management Center が一時ファイルをリモートサーバーに書き込むことがあります。これらのファイルは、バックアッププロセスの最後にクリーンアップされます。

次のタスク

リモートストレージが設定されている場合または [完了時にコピー（Copy when complete）] が有効になっている場合は、バックアップファイルの転送が成功したことを確認します。

Management Center からのデバイスのバックアップ

次のいずれかのデバイスのオンデマンドバックアップを実行するには、この手順を使用してください。

- Threat Defense ：物理デバイス、スタンドアロン、高可用性、クラスタ
- Threat Defense Virtual：プライベートクラウド、スタンドアロン、高可用性、クラスタ

バックアップと復元は、他のプラットフォームまたは構成など）ではサポートされていません。

始める前に

要件、ガイドライン、制限事項、およびベストプラクティスを確認し、理解する必要があります。 手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。

- バックアップと復元の要件 （557 ページ）
- バックアップと復元の注意事項と制限事項 （558 ページ）
- バックアップと復元のベストプラクティス （560 ページ）

Firepower 4100/9300 シャーシをバックアップする場合は、FXOS 設定もバックアップすることが特に重要です（FXOS コンフィギュレーション ファイルのエクスポート （569 ページ））。

手順

ステップ 1 **システム**（⚙） > **[ツール（Tools）]** > **[バックアップ/復元（Backup/Restore）]** を選択し、[管理対象デバイスのバックアップ（Managed Device Backup）] をクリックします。

ステップ 2 1 つ以上の**管理対象デバイス**を選択します。

クラスタリングの場合は、クラスタを選択します。個々のノードでバックアップを実行することはできません。

ステップ 3 デバイスバックアップファイルの**保存場所**に注意してください。

これは、ローカルストレージ（`/var/sf/remote-backup/`）またはリモート ネットワーク ボリュームのいずれかにすることができます。ISA 3000 では、SD カードが取り付けられている場合、バックアップのコピーも SD カード（`/mnt/disk3/backup`）に作成されます。詳細については、「バックアップとリモートストレージの管理（590 ページ）」を参照してください。

ステップ 4 リモートストレージを設定しなかった場合は、[管理センターで取得する（Retrieve to Management Center）] を有効または無効にできます。

- 有効（デフォルト）：バックアップが Management Center の `/var/sf/remote-backup/` に保存されます。

  クラスタの場合は、このオプションが常にオンになります。個別のノードのバックアップファイルは、Management Center にコピーされ、単一の圧縮 tar ファイルにバンドルされてから、リモートストレージにコピーされます。

- 無効：バックアップがデバイスの `/var/sf/backup` に保存されます。

ステップ 5 [バックアップの開始（Start Backup）] をクリックしてオンデマンドバックアップを開始します。

ステップ 6 デバイスが再起動するまで、Message Center で進行状況をモニターします。

次のタスク

リモートストレージを設定した場合は、バックアップファイルの転送が成功したことを確認します。

FXOS コンフィギュレーション ファイルのエクスポート

エクスポート設定機能を使用して、Firepower 4100/9300 シャーシの論理デバイスとプラットフォーム構成設定を含む XML ファイルをリモート サーバまたはローカル コンピュータにエクスポートします。

（注） この手順では、脅威に対する防御 をバックアップするときに FXOS 設定をエクスポートするための Secure Firewall シャーシマネージャ の使用方法について説明します。CLI の手順については、該当するバージョンの『 Cisco Firepower 4100/9300 FXOS CLI Configuration Guide 』を参照してください。

始める前に

「Firepower 4100/9300 のコンフィギュレーションのインポート/エクスポートに関するガイドライン」を確認してください。

手順

ステップ 1 Secure Firewall シャーシマネージャ で **[システム（System）]** > **[設定（Configuration）]** > **[エクスポート（Export）]** の順に選択します。

ステップ 2 コンフィギュレーション ファイルをローカル コンピュータにエクスポートするには、次の手順を実行します。

a) [ローカル（Local）] をクリックします。

b) [エクスポート（Export）] をクリックします。
コンフィギュレーションファイルが作成され、ブラウザによって、ファイルがデフォルトのダウンロード場所に自動的にダウンロードされるか、またはファイルを保存するようプロンプトが表示されます。

ステップ 3 コンフィギュレーション ファイルをリモート サーバにエクスポートするには、次の操作を行います。

a) [リモート（Remote）] をクリックします。

b) リモート サーバとの通信で使用するプロトコルを選択します。選択できるプロトコルは、FTP、TFTP、SCP、または SFTP のいずれかです。

c) バックアップ ファイルを格納する場所のホスト名または IP アドレスを入力します。サーバ、ストレージ アレイ、ローカル ドライブ、または Firepower 4100/9300 シャーシがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどを指定できます。

IP アドレスではなくホスト名を使用する場合は、DNS サーバを設定する必要があります。

d) デフォルト以外のポートを使用する場合は、[ポート（Port）] フィールドにポート番号を入力します。

e) リモート サーバにログインするためのユーザ名を入力します。プロトコルが TFTP の場合、このフィールドは適用されません。

f) リモート サーバのユーザ名のパスワードを入力します。プロトコルが TFTP の場合、このフィールドは適用されません。

（注） パスワードは 64 文字以下にする必要があります。64 文字を超えるパスワードを入力すると、シャーシマネージャ に`org-root/cfg-exp-policy-default` のプロパティパスワードが範囲外であることを示すエラーが表示されます。

g) [場所（Location）] フィールドに、ファイル名を含む設定ファイルをエクスポートする場所のフル パスを入力します。
h) [エクスポート（Export）] をクリックします。
コンフィギュレーション ファイルが作成され、指定の場所にエクスポートされます。

バックアッププロファイルの作成

バックアッププロファイルとは、保存済みの一連の設定（何をバックアップするか、どこにバックアップファイルを保存するかなど）です。

Management Center のバックアップにはバックアッププロファイルが必要です。Management Centerからデバイスをバックアップする場合、バックアッププロファイルは必要ありません。

Management Centerのオンデマンドバックアップを実行する場合、既存のバックアッププロファイルを選択しないと、システムが自動的に作成し、それを使用します。その後、新しく作成されたプロファイルを使用して、スケジュールされたバックアップを設定できます。

次の手順では、オンデマンドバックアップを実行せずにバックアッププロファイルを作成する方法について説明します。

手順

ステップ 1 システム（⚙）>**[ツール（Tools）]**>**[バックアップ/復元（Backup/Restore）]** を選択し、[バックアッププロファイル（Backup Profiles）] をクリックします。

ステップ 2 [プロファイルの作成（Create Profile）] をクリックし、[名前（Name）] に名前を入力します。

ステップ 3 バックアップするものを選択します。

- **バックアップ構成**
- **イベントのバックアップ**
- **Threat Intelligence Director のバックアップ**

マルチドメイン展開では、設定をバックアップする必要があります。イベントまたはTIDデータのみをバックアップすることはできません。これらの各選択肢のバックアップ対象および対象外の詳細については、バックアップと復元について （555 ページ）を参照してください。

ステップ 4 バックアップファイルの**保存場所**に注意してください。

これは、ローカルストレージ（`/var/sf/backup/`）またはリモート ネットワーク ボリュームのいずれかにすることができます。ISA 3000 では、SD カードが取り付けられている場合、バックアップのコピーも SD カード（/mnt/disk3/backup）に作成されます。詳細については、「バックアップとリモートストレージの管理 （590 ページ）」を参照してください。

ステップ 5 （任意）[完了時にコピー（Copy when complete）] を有効にして、完了した Management Center のバックアップをリモートサーバーにコピーします。

ホスト名または IP アドレス、リモートディレクトリへのパス、およびユーザー名とパスワードを入力します。パスワードの代わりに SSH 公開キーを使用するには、[SSH 公開キー（SSH Public Key）] フィールドの内容を、リモートサーバー上の指定ユーザーの `authorized_keys` ファイルにコピーします。

（注） このオプションは、バックアップをローカルに保存し、リモートの場所にも SCP で保存する場合に便利です。SSHFS リモートストレージを設定した場合は、[完了時にコピー（Copy when complete）] を使用してバックアップファイルを同じディレクトリにコピーしないでください。

ステップ 6 （任意）[電子メール（Email）] を有効にして、バックアップの完了時に通知する電子メールアドレスを入力します。

電子メール通知を受信するには、メールサーバーに接続するように Management Center を設定する必要があります（メール リレー ホストおよび通知アドレスの設定 （69 ページ））。

ステップ 7 [保存（Save）] をクリックします。

Management Center および管理対象デバイスの復元

Management Center の場合は、Web インターフェイスを使用してバックアップから復元します。Threat Defense デバイスの場合、Threat Defense CLI を使用する必要があります。Management Center を使用してデバイスを復元することはできません。

ここでは、Management Center と管理対象デバイスを復元する方法について説明します。

バックアップからの Management Center の復元

Management Center のバックアップを復元する場合、バックアップファイルに含まれるコンポーネント（イベント、設定、TID データ）の一部またはすべての復元を選択できます。

（注） 設定を復元すると、ごくわずかの例外を除いて、すべての設定が上書きされます。また、Management Center が再起動されます。イベントおよび TID データを復元すると、侵入イベントを除くすべての既存のイベントおよび TID データが上書きされます。準備が整っていることを確認してください。

バックアップから Management Center を復元するには、次の手順を実行します。Management Center の HA 展開でのバックアップと復元の詳細については、高可用性ペアでの Management Center の交換 （382 ページ）を参照してください。

始める前に

要件、ガイドライン、制限事項、およびベストプラクティスを確認し、理解する必要があります。手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。

- バックアップと復元の要件 （557 ページ）
- バックアップと復元の注意事項と制限事項 （558 ページ）
- バックアップと復元のベストプラクティス （560 ページ）

手順

ステップ 1 復元する Management Center にログインします。

ステップ 2 システム（⚙） > **[ツール（Tools）]** > **[バックアップ/復元（Backup/Restore）]** を選択します。

[バックアップ管理（Backup Management）] ページには、ローカルとリモートで保存されたすべてのバックアップファイルが一覧表示されます。バックアップファイルをクリックすると、そのコンテンツが表示されます。

バックアップファイルが一覧になく、ローカルコンピュータに保存している場合は、[バックアップのアップロード（Upload Backup）] をクリックします。バックアップとリモートストレージの管理 （590 ページ）を参照してください。

ステップ 3 復元するバックアップファイルを選択し、[復元（Restore）] をクリックします。

ステップ 4 利用可能コンポーネントから復元するコンポーネントを選択し、もう一度 [復元（Restore）] をクリックして開始します。

ステップ 5 デバイスが再起動するまで、Message Center で進行状況をモニターします。

設定を復元する場合は、Management Center の再起動後に再度ログインできます。

次のタスク

- 必要に応じて、復元前に元に戻したライセンス設定を再指定します。ライセンスの競合や孤立した権限付与に気付いた場合は、Cisco TAC にお問い合わせください。
- 必要に応じて、リモートストレージと監査ログサーバー証明書の設定を再指定します。これらの設定は、バックアップには含まれていません。
- SRU と VDB を更新します。復元された SRU または VDB のバージョンが、シスコ サポートおよびダウンロード サイト で利用可能なバージョンよりも古い場合は、デバイスに変更を展開する前に、必ず VDB を最新バージョンに更新してください。
- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

バックアップからの Threat Defense の復元：Firepower 1000/2100、Cisco Secure Firewall 3100/4200、ISA 3000（非ゼロタッチ）

デバイスのバックアップと復元は、RMA を対象としています。設定を復元すると、管理 IP アドレスを含む、デバイス上のすべての設定が上書きされます。また、デバイスが再起動されます。

この手順では、ハードウェア障害が発生した場合にスタンドアロンまたは高可用性ペアの（またはクラスタとして）Firepower 1000/2100、Cisco Secure Firewall 3100/4200、または ISA 3000 Threat Defense デバイスを交換する方法の概要を示します。交換するデバイスの正常なバックアップにアクセスできることを前提としています。Management Center からのデバイスのバックアップ （568 ページ）を参照してください。SD カードを使用した ISA 3000 でのゼロタッチ復元については、バックアップからの Threat Defense のゼロタッチ復元：ISA 3000 （578 ページ）を参照してください。

高可用性デバイスおよびクラスタ化デバイスの場合は、この手順を使用してすべてのピアを交換できます。すべて交換するには、**restore** CLI コマンド自体を除き、すべてのデバイスですべての手順を同時に実行します。

（注） ネットワークからデバイスを切断する場合でも、Management Center の登録を解除しないでください。Threat Defense の高可用性デバイスまたはクラスタ化デバイスの場合は、高可用性またはクラスタリングを中断または解除しないでください。これらのリンクを維持することで、交換用デバイスを、復元後に自動的に再接続できます。

始める前に

要件、ガイドライン、制限事項、およびベストプラクティスを確認し、理解する必要があります。 手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。

- バックアップと復元の要件 （557 ページ）
- バックアップと復元の注意事項と制限事項 （558 ページ）
- バックアップと復元のベストプラクティス （560 ページ）

手順

ステップ 1 交換用ハードウェアについては、Cisco TAC にお問い合わせください。

同じ数のネットワークモジュールと同じタイプおよび数の物理インターフェイスを備えた同じモデルを入手してください。シスコ返品ポータル から RMA プロセスを開始できます。

ステップ 2 障害のあるデバイスの正常なバックアップを見つけます。

バックアップ設定に応じて、デバイスのバックアップは次の場所に保存されています。

- 障害のあるデバイス自体の `/var/sf/backup`。
- Management Center の `/var/sf/remote-backup`。
- リモートの保存場所。

Threat Defense の高可用性デバイスおよびクラスタ化デバイスの場合は、グループを 1 つのユニットとしてバックアップします。高可用性デバイスの場合は、バックアッププロセスによって一意のバックアップファイルが作成され、各デバイスのロールがバックアップファイル名に示されます。クラスタの場合は、制御ノードとデータノードのバックアップファイルが、単一の圧縮ファイルにバンドルされます。ファイルを抽出する必要があります。このファイルにもデバイスのロールが示されます。

バックアップの唯一のコピーが、障害のあるデバイス上にある場合は、ここで別の場所にコピーします。デバイスを再イメージ化すると、バックアップが消去されます。他に問題が発生した場合、バックアップを回復できなくなる可能性があります。詳細については、「バックアップとリモートストレージの管理 （590 ページ）」を参照してください。

交換用デバイスにはバックアップが必要ですが、復元プロセス中に SCP によってバックアップを取得できます。交換用デバイスに SCP でアクセス可能な場所にバックアップを配置しておくことをお勧めします。または、バックアップを交換用デバイス自体にコピーすることができます。

ステップ 3 障害のあるデバイスを取り外します（ラックから取り外します）。

すべてのインターフェイスの接続を切断します。Threat Defense の高可用性展開では、フェールオーバーリンクが対象に含まれます。クラスタリングの場合、クラスタ制御リンクが対象に含まれます。

ご使用のモデル用のハードウェア設置ガイドとスタートアップガイドを参照してください：http://www.cisco.com/go/ftd-quick。

（注） ネットワークからデバイスを切断する場合でも、Management Center の登録を解除しないでください。Threat Defense の高可用性デバイスまたはクラスタ化デバイスの場合は、高可用性またはクラスタリングを中断または解除しないでください。これらのリンクを維持することで、交換用デバイスを、復元後に自動的に再接続できます。

ステップ 4 交換用デバイスを取り付け、管理ネットワークに接続します。

デバイスを電源に接続し、管理インターフェイスを管理ネットワークに接続します。Threat Defense の高可用性展開では、フェールオーバーリンクを接続します。クラスタリングの場合は、クラスタ制御リンクを接続します。ただし、データインターフェイスは接続しないでください。

ご使用のモデル用のハードウェア設置ガイドを参照してください：http://www.cisco.com/go/ftd-quick。

ステップ 5 （任意）交換用の デバイスを再イメージ化します。

RMA シナリオでは、交換用デバイスは、工場出荷時のデフォルト設定で納品されます。交換用デバイスが障害のあるデバイスと同じメジャーバージョンを実行していない場合は、再イメージ化することをお勧めします。

Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイドを参照してください。

ステップ 6 交換用デバイスで初期設定を行います。

Threat Defense CLI に `admin` ユーザーとしてアクセスします。セットアップウィザードでは、管理 IP アドレス、ゲートウェイ、およびその他の基本ネットワーク設定を指定するように求められます。

障害のあるデバイスと同じ管理 IP アドレスを設定しないでください。それにより、パッチを適用するためにデバイスを登録する必要がある場合に問題が発生する可能性があります。復元プロセスにより、管理 IP アドレスが正しくリセットされます。

ご使用のモデル用のスタートアップガイドで、初期設定に関するトピックを参照してください：http://www.cisco.com/go/ftd-quick。

（注） 交換用デバイスにパッチを適用する必要がある場合は、スタートアップガイドの説明に従って Management Center 登録プロセスを開始します。パッチを適用する必要がない場合は、登録しないでください。

ステップ 7 交換用デバイスで、障害のあるデバイスと同じソフトウェアバージョン（パッチを含む）が実行されていることを確認します。

既存のデバイスが Management Center から削除されていないことを確認します。交換用デバイスは物理ネットワークからは管理できない必要があり、新しいハードウェアおよび交換する Threat Defense パッチは同じバージョンである必要があります。Threat Defense CLI には、upgrade コマンドはありません。パッチを適用するには、次の手順を実行します。

a) Management Center Web インターフェイスから、デバイス登録プロセスを完了します。

新しい AC ポリシーを作成し、デフォルトアクション「Network Discovery」を使用します。このポリシーはそのままにします。機能や変更を追加しないでください。これは、デバイスを登録して、機能が含まれないポリシーを展開するために使用されています。これにより、ライセンスを要求されなくなり、その後、デバイスにパッチを適用できます。バックアップが復元されると、ライセンスとポリシーが予想どおりの状態に復元されます。

b) デバイスにパッチを適用します：https://www.cisco.com/go/ftd-upgrade。

c) Management Center から、パッチを適用したばかりのデバイスの登録を解除します。

登録を解除しないと、復元プロセスによって「古い」デバイスが再起動された後で、非実体デバイスが Management Center に登録されます。

ステップ 8 交換用デバイスがバックアップファイルにアクセスできることを確認します。

復元プロセスでは SCP によってバックアップを取得できるため、バックアップをアクセス可能な場所に配置することをお勧めします。または、交換用デバイス自体（`/var/sf/backup`）

にバックアップを手動でコピーすることもできます。クラスタ化されたデバイスの場合は、バックアップバンドルから適切なバックアップファイルを抽出します。

ステップ 9 Threat Defense CLI から、バックアップを復元します。

Threat Defense CLI に `admin` ユーザーとしてアクセスします。コンソールを使用するか、新しく設定された管理インターフェイス（IP アドレスまたはホスト名）に SSH で接続することができます。復元プロセスによってこの IP アドレスが変更されることに注意してください。

復元するには、次の手順を実行します。

- SCP を使用：**restore remote-manager-backup location** *scp-hostname username filepath backup tar-file*
- ローカルデバイスから：**restore remote-manager-backup** *backup tar-file*

Threat Defense の高可用性とクラスタリングの展開では、適切なバックアップファイル（プライマリとセカンダリ、または制御とデータ）を選択してください。役割は、バックアップファイル名に示されます。すべてのデバイスを復元する場合は、この手順を順番に実行します。再起動を含め、最初のデバイスの復元プロセスが完了するまで、次のデバイスで **restore** コマンドを実行しないでください。

ステップ 10 Management Center にログインし、交換用デバイスが接続されるまで待ちます。

復元が完了すると、デバイスは、ユーザーを CLI からログアウトさせ、再起動して、自動的に Management Center に接続します。この時点では、デバイスが期限切れと表示されます。

ステップ 11 展開する前に、復元後のタスクを実行し、復元後の問題を解決します。

- ライセンスの競合や孤立した権限付与を解決します。Cisco TAC にお問い合わせください。
- ハイ アベイラビリティ同期を再開します。Threat Defense CLI から、`configure high-availability resume` と入力します。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Suspend and Resume High Availability*」を参照してください。
- すべての VPN 証明書を再追加/再登録します。復元プロセスでは、VPN 証明書（バックアップの実行後に追加された証明書を含む）が Threat Defense デバイスから削除されます。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Managing VPN Certificates*」を参照してください。

ステップ 12 設定を展開します。

この展開は必須です。デバイスを復元したら、[デバイス管理（Device Management）]ページから強制的に展開する必要があります。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Redeploy Existing Configurations to a Device*」を参照してください。

ステップ 13 デバイスのデータインターフェイスを接続します。

ご使用のモデル用のハードウェア設置ガイドを参照してください：http://www.cisco.com/go/ftd-quick。

次のタスク

復元が成功し、交換用デバイスが予期どおりにトラフィックを通過させていることを確認します。

バックアップからの Threat Defense のゼロタッチ復元：ISA 3000

デバイスのバックアップと復元は、RMA を対象としています。設定を復元すると、管理 IP アドレスを含む、デバイス上のすべての設定が上書きされます。また、デバイスが再起動されます。

ハードウェア障害が発生した場合のために、この手順で、スタンドアロンまたは HA ペアの ISA 3000 Threat Defense デバイスを交換する方法の概要を示します。SD カードに障害が発生したユニットのバックアップがあることを前提としています。Management Center からのデバイスのバックアップ （568 ページ）を参照してください。

高可用性デバイスおよびクラスタ化デバイスの場合は、この手順を使用してすべてのピアを交換できます。すべて交換するには、**restore** CLI コマンド自体を除き、すべてのデバイスですべての手順を同時に実行します。

（注） ネットワークからデバイスを切断する場合でも、Management Center の登録を解除しないでください。Threat Defense の高可用性デバイスまたはクラスタ化デバイスの場合は、高可用性またはクラスタリングを中断または解除しないでください。これらのリンクを維持することで、交換用デバイスを、復元後に自動的に再接続できます。

始める前に

要件、ガイドライン、制限事項、およびベストプラクティスを確認し、理解する必要があります。手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。

- バックアップと復元の要件 （557 ページ）
- バックアップと復元の注意事項と制限事項 （558 ページ）
- バックアップと復元のベストプラクティス （560 ページ）

手順

ステップ 1 交換用ハードウェアについては、Cisco TAC にお問い合わせください。

同じ数のネットワークモジュールと同じタイプおよび数の物理インターフェイスを備えた同じモデルを入手してください。シスコ返品ポータル から RMA プロセスを開始できます。

ステップ 2 障害のあるデバイスから SD カードを取り外し、デバイスをラックから外します。

すべてのインターフェイスの接続を切断します。Threat Defense の HA 展開では、フェールオーバーリンクが対象に含まれます。

（注） ネットワークからデバイスを切断する場合でも、Management Center の登録を解除しないでください。Threat Defense の高可用性デバイスまたはクラスタ化デバイスの場合は、高可用性またはクラスタリングを中断または解除しないでください。これらのリンクを維持することで、交換用デバイスを、復元後に自動的に再接続できます。

ステップ 3 交換用デバイスをラックに再度取り付け、管理ネットワークに接続します。Threat Defense の HA 展開では、フェールオーバーリンクを接続します。ただし、データインターフェイスは接続しないでください。

デバイスのイメージを再作成するか、ソフトウェアパッチを適用する必要がある場合は、電源コネクタを接続します。

ステップ 4 （任意）交換用のデバイスを再イメージ化します。

RMA シナリオでは、交換用デバイスは、工場出荷時のデフォルト設定で納品されます。交換用デバイスが障害のあるデバイスと同じメジャーバージョンを実行していない場合は、再イメージ化する必要があります。https://www.cisco.com/go/isa3000-software からインストーラを取得します。

再イメージ化するには、Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイドを参照してください。

ステップ 5 （任意）交換用デバイスが、障害のあるデバイスと同じ Firepower ソフトウェアバージョン（同じパッチバージョンを含む）を実行していることを確認します。デバイスにパッチを適用する必要がある場合は、Secure Firewall Device Manager（Device Manager）に接続してパッチをインストールできます。

次の手順は、工場出荷時のデフォルト設定を前提としています。デバイスをすでに設定している場合は、Device Manager にログインし、**[デバイス（Device）]** > **[アップグレード（Upgrades）]** ページに直接移動してパッチをインストールできます。

いずれの場合も、https://www.cisco.com/go/isa3000-software からパッチパッケージを取得します。

a) コンピュータを内部（イーサネット 1/2）インターフェイスに直接接続し、デフォルトの IP アドレス（https://192.168.95.1）で Device Manager にアクセスします。
b) ユーザー名（admin）とデフォルトのパスワード（Admin123）を入力して、[Login] をクリックします。
c) セットアップ ウィザードを完了します。Device Manager で設定した内容は保持されないことに注意してください。パッチを適用できるように、初期設定を行うだけなので、セットアップウィザードで入力した内容は関係ありません。
d) **[Device]** > **[Upgrades]** ページに移動します。

   [System Upgrade] セクションに、現在実行中のソフトウェアバージョンが表示されます。

e) [Browse] をクリックして、パッチファイルをアップロードします。
f) [インストール（Install）] をクリックして、インストール プロセスを開始します。

アイコンの隣の情報は、インストール中にデバイスが再起動するかどうかを示します。システムから自動的にログアウトされます。インストールには 30 分以上かかることがあります。

待機してからシステムに再度ログインしてください。[デバイスサマリー（Device Summary）] または [システム監視ダッシュボード（System monitoring dashboard）] には、新しいバージョンが表示されます。

（注） 単にブラウザ ウィンドウを更新するだけではありません。URL からパスを削除してホームページに再接続してください。これにより、最新のコードではキャッシュされている情報が更新されます。

ステップ 6 交換用デバイスに SD カードを挿入します。

ステップ 7 デバイスの電源をオンにするか、デバイスを再起動し、ブートアップの開始直後に、[Reset] ボタンを 3 ～ 15 秒間押し続けます。

パッチのインストールに Device Manager を使用した場合は、**[Device]** > **[System Settings]** > **[Reboot/Shutdown]** ページからリブートできます。Threat Defense CLI から、**reboot** コマンドを使用します。まだ電源を接続していない場合は、ここで接続します。

ワイヤゲージ 0.033 インチ以下の標準サイズの #1 ペーパークリップを使用して [Reset] ボタンを押します。復元プロセスは、ブートアップ時にトリガーされます。デバイスの設定が復元され、再起動します。その後、デバイスは自動的に Management Center に登録されます。

HA ペアの両方のデバイスを復元する場合は、この手順を順番に実行します。再起動を含め、最初のデバイスの復元プロセスが完了するまで、2 つ目のデバイス復元しないでください。

ステップ 8 Management Center にログインし、交換用デバイスが接続されるまで待ちます。

この時点では、デバイスが期限切れと表示されます。

ステップ 9 展開する前に、復元後のタスクを実行し、復元後の問題を解決します。

- ライセンスの競合や孤立した権限付与を解決します。Cisco TAC にお問い合わせください。
- ハイ アベイラビリティ同期を再開します。Threat Defense CLI から、`configure high-availability resume` と入力します。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Suspend and Resume High Availability*」を参照してください。
- すべての VPN 証明書を再追加/再登録します。復元プロセスでは、VPN 証明書（バックアップの実行後に追加された証明書を含む）が Threat Defense デバイスから削除されます。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Managing VPN Certificates*」を参照してください。

ステップ 10 設定を展開します。

この展開は必須です。デバイスを復元したら、[デバイス管理（Device Management）] ページから強制的に展開する必要があります。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Redeploy Existing Configurations to a Device*」を参照してください。

ステップ 11 デバイスのデータインターフェイスを接続します。

ご使用のモデル用のハードウェア設置ガイドを参照してください：http://www.cisco.com/go/ftd-quick。

次のタスク

復元が成功し、交換用デバイスが予期どおりにトラフィックを通過させていることを確認します。

バックアップからの Threat Defense の復元：Firepower 4100/9300 シャーシ

デバイスのバックアップと復元は、RMA を対象としています。設定を復元すると、管理 IP アドレスを含む、デバイス上のすべての設定が上書きされます。また、デバイスが再起動されます。

この手順では、ハードウェア障害が発生した場合にスタンドアロンまたは高可用性ペアの（またはクラスタとして）Firepower 4100/9300 を交換する方法の概要を示します。次の正常なバックアップにアクセスできることを前提としています。

- 交換する論理デバイス。Management Center からのデバイスのバックアップ （568 ページ）を参照してください。
- FXOS の設定。FXOS コンフィギュレーション ファイルのエクスポート （569 ページ）を参照してください。

高可用性デバイスおよびクラスタ化デバイスの場合は、この手順を使用してすべてのピアを交換できます。すべて交換するには、**restore** CLI コマンド自体を除き、すべてのデバイスですべての手順を同時に実行します。

（注） ネットワークからデバイスを切断する場合でも、Management Center の登録を解除しないでください。Threat Defense の高可用性デバイスまたはクラスタ化デバイスの場合は、高可用性またはクラスタリングを中断または解除しないでください。これらのリンクを維持することで、交換用デバイスを、復元後に自動的に再接続できます。

始める前に

要件、ガイドライン、制限事項、およびベストプラクティスを確認し、理解する必要があります。手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。

- バックアップと復元の要件 （557 ページ）
- バックアップと復元の注意事項と制限事項 （558 ページ）

- バックアップと復元のベストプラクティス （560 ページ）

手順

ステップ 1 交換用ハードウェアについては、Cisco TAC にお問い合わせください。

同じ数のネットワークモジュールと同じタイプおよび数の物理インターフェイスを備えた同じモデルを入手してください。シスコ返品ポータル から RMA プロセスを開始できます。

ステップ 2 障害のあるデバイスの正常なバックアップを見つけます。

バックアップ設定に応じて、デバイスのバックアップは次の場所に保存されています。

- 障害のあるデバイス自体の `/var/sf/backup`。
- Management Center の `/var/sf/remote-backup`。
- リモートの保存場所。

Threat Defense の高可用性デバイスおよびクラスタ化デバイスの場合は、グループを 1 つのユニットとしてバックアップします。高可用性デバイスの場合は、バックアッププロセスによって一意のバックアップファイルが作成され、各デバイスのロールがバックアップファイル名に示されます。クラスタの場合は、制御ノードとデータノードのバックアップファイルが、単一の圧縮ファイルにバンドルされます。ファイルを抽出する必要があります。このファイルにもデバイスのロールが示されます。

バックアップの唯一のコピーが、障害のあるデバイス上にある場合は、ここで別の場所にコピーします。デバイスを再イメージ化すると、バックアップが消去されます。他に問題が発生した場合、バックアップを回復できなくなる可能性があります。詳細については、「バックアップとリモートストレージの管理 （590 ページ）」を参照してください。

交換用デバイスにはバックアップが必要ですが、復元プロセス中に SCP によってバックアップを取得できます。交換用デバイスに SCP でアクセス可能な場所にバックアップを配置しておくことをお勧めします。または、バックアップを交換用デバイス自体にコピーすることができます。

ステップ 3 FXOS 設定の正常なバックアップを見つけます。

ステップ 4 障害のあるデバイスを取り外します（ラックから取り外します）。

すべてのインターフェイスの接続を切断します。Threat Defense の高可用性展開では、フェールオーバーリンクが対象に含まれます。クラスタリングの場合、クラスタ制御リンクが対象に含まれます。

ご使用のモデル用のハードウェア設置ガイドとスタートアップガイドを参照してください：http://www.cisco.com/go/ftd-quick。

（注） ネットワークからデバイスを切断する場合でも、Management Center の登録を解除しないでください。Threat Defense の高可用性デバイスまたはクラスタ化デバイスの場合は、高可用性またはクラスタリングを中断または解除しないでください。これらのリンクを維持することで、交換用デバイスを、復元後に自動的に再接続できます。

ステップ 5 交換用デバイスを取り付け、管理ネットワークに接続します。

デバイスを電源に接続し、管理インターフェイスを管理ネットワークに接続します。Threat Defense の高可用性展開では、フェールオーバーリンクを接続します。クラスタリングの場合は、クラスタ制御リンクを接続します。ただし、データインターフェイスは接続しないでください。

ご使用のモデル用のハードウェア設置ガイドを参照してください：http://www.cisco.com/go/ftd-quick。

ステップ 6 （任意）交換用の デバイスを再イメージ化します。

RMA シナリオでは、交換用デバイスは、工場出荷時のデフォルト設定で納品されます。交換用デバイスが障害のあるデバイスと同じメジャーバージョンを実行していない場合は、再イメージ化することをお勧めします。

該当するバージョンの Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager のコンフィギュレーションガイドに記載されている工場出荷時のデフォルト設定の復元に関する説明を参照してください。

ステップ 7 FXOS が互換性のあるバージョンを実行していることを確認します。

論理デバイスを再追加する前に、互換性のある FXOS バージョンを実行している必要があります。Chassis Manager を使用して、バックアップされた FXOS 設定をインポートできます（コンフィギュレーション ファイルのインポート （585 ページ）を参照）。

ステップ 8 Chassis Manager を使用して、論理デバイスを追加し、初期設定を行います。

障害のあるシャーシ上の 1 つまたは複数の論理デバイスと同じ管理 IP アドレスを設定しないでください。それにより、パッチを適用するために論理デバイスを登録する必要がある場合に問題が発生する可能性があります。復元プロセスにより、管理 IP アドレスが正しくリセットされます。

お使いのモデルのスタートアップガイドで、Management Center の展開に関する章を参照してください。http://www.cisco.com/go/ftd-quick

（注） 論理デバイスにパッチを適用する必要がある場合は、スタートアップガイドの説明に従って Management Center に登録します。パッチを適用する必要がない場合は、登録しないでください。

ステップ 9 交換用デバイスで、障害のあるデバイスと同じソフトウェアバージョン（パッチを含む）が実行されていることを確認します。

既存のデバイスが Management Center から削除されていないことを確認します。交換用デバイスは物理ネットワークからは管理できない必要があり、新しいハードウェアおよび交換する Threat Defense パッチは同じバージョンである必要があります。Threat Defense CLI には、upgrade コマンドはありません。パッチを適用するには、次の手順を実行します。

a) Management Center Web インターフェイスから、デバイス登録プロセスを完了します。

新しい AC ポリシーを作成し、デフォルトアクション「Network Discovery」を使用します。このポリシーはそのままにします。機能や変更を追加しないでください。これは、デバイ

スを登録して、機能が含まれないポリシーを展開するために使用されています。これにより、ライセンスを要求されなくなり、その後、デバイスにパッチを適用できます。バックアップが復元されると、ライセンスとポリシーが予想どおりの状態に復元されます。

b) デバイスにパッチを適用します：https://www.cisco.com/go/ftd-upgrade。

c) Management Center から、パッチを適用したばかりのデバイスの登録を解除します。

登録を解除しないと、復元プロセスによって「古い」デバイスが再起動された後で、非実体デバイスが Management Center に登録されます。

ステップ 10 交換用デバイスがバックアップファイルにアクセスできることを確認します。

復元プロセスでは SCP によってバックアップを取得できるため、バックアップをアクセス可能な場所に配置することをお勧めします。または、交換用デバイス自体（`/var/sf/backup`）にバックアップを手動でコピーすることもできます。クラスタ化されたデバイスの場合は、バックアップバンドルから適切なバックアップファイルを抽出します。

ステップ 11 Threat Defense CLI から、バックアップを復元します。

Threat Defense CLI に `admin` ユーザーとしてアクセスします。コンソールを使用するか、新しく設定された管理インターフェイス（IP アドレスまたはホスト名）に SSH で接続することができます。復元プロセスによってこの IP アドレスが変更されることに注意してください。

復元するには、次の手順を実行します。

- SCP を使用：**restore remote-manager-backup location** *scp-hostname username filepath backup tar-file*
- ローカルデバイスから：**restore remote-manager-backup** *backup tar-file*

Threat Defense の高可用性とクラスタリングの展開では、適切なバックアップファイル（プライマリとセカンダリ、または制御とデータ）を選択してください。役割は、バックアップファイル名に示されます。すべてのデバイスを復元する場合は、この手順を順番に実行します。再起動を含め、最初のデバイスの復元プロセスが完了するまで、次のデバイスで **restore** コマンドを実行しないでください。

ステップ 12 Management Center にログインし、交換用デバイスが接続されるまで待ちます。

復元が完了すると、デバイスは、ユーザーを CLI からログアウトさせ、再起動して、自動的に Management Center に接続します。この時点では、デバイスが期限切れと表示されます。

ステップ 13 展開する前に、復元後のタスクを実行し、復元後の問題を解決します。

- ライセンスの競合や孤立した権限付与を解決します。Cisco TAC にお問い合わせください。
- すべての VPN 証明書を再追加/再登録します。復元プロセスでは、VPN 証明書（バックアップの実行後に追加された証明書を含む）が Threat Defense デバイスから削除されます。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Managing VPN Certificates*」を参照してください。

ステップ 14 設定を展開します。

この展開は必須です。デバイスを復元したら、[デバイス管理（Device Management）]ページから強制的に展開する必要があります。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Redeploy Existing Configurations to a Device*」を参照してください。

ステップ 15 デバイスのデータインターフェイスを接続します。

ご使用のモデル用のハードウェア設置ガイドを参照してください：http://www.cisco.com/go/ftd-quick。

次のタスク

復元が成功し、交換用デバイスが予期どおりにトラフィックを通過させていることを確認します。

コンフィギュレーション ファイルのインポート

設定のインポート機能を使用して、Firepower 4100/9300 シャーシからエクスポートした構成設定を適用できます。この機能を使用して、既知の良好な構成に戻したり、システム障害を解決したりできます。

（注） この手順では、ソフトウェアを復元する前に、シャーシマネージャ を使用して FXOS の設定をインポートする方法について説明します。CLI の手順については、該当するバージョンの『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide 』を参照してください。

始める前に

「Firepower 4100/9300 のコンフィギュレーションのインポート/エクスポートに関するガイドライン」を確認してください。

手順

ステップ 1 で、シャーシマネージャ**[システム（System）]** > **[ツール（Tools）]** > **[インポート/エクスポート（Import/Export）]** を選択します。

ステップ 2 ローカルのコンフィギュレーション ファイルからインポートする場合は、次の操作を行います。

a) [ローカル（Local）] をクリックします。

b) [ファイルの選択（Choose File）] をクリックし、インポートするコンフィギュレーション ファイルを選択します。

c) [インポート（Import）] をクリックします。
操作の続行を確認するダイアログボックスが開き、シャーシの再起動についての警告が表示されます。

d) [はい（Yes）] をクリックして、指定したコンフィギュレーション ファイルをインポートします。
既存の設定が削除され、インポートしたファイルの設定が Firepower 4100/9300 シャーシに適用されます。インポート中にブレークアウトポートの設定が変更された場合は、Firepower 4100/9300 シャーシの再起動が必要になります。

ステップ 3 リモート サーバからコンフィギュレーション ファイルをインポートする場合は、次の操作を行います。

a) [リモート（Remote）] をクリックします。
b) リモートサーバとの通信で使用するプロトコルを選択します。選択できるプロトコルは、FTP、TFTP、SCP、または SFTP のいずれかです。
c) デフォルト以外のポートを使用する場合は、[ポート（Port）] フィールドにポート番号を入力します。
d) バックアップ ファイルが格納されている場所のホスト名または IP アドレスを入力します。サーバ、ストレージ アレイ、ローカル ドライブ、または Firepower 4100/9300 シャーシがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどを指定できます。

IP アドレスではなくホスト名を使用する場合は、DNS サーバを設定する必要があります。

e) リモート サーバにログインするためのユーザ名を入力します。プロトコルが TFTP の場合、このフィールドは適用されません。
f) リモート サーバのユーザ名のパスワードを入力します。プロトコルが TFTP の場合、このフィールドは適用されません。

（注） パスワードは 64 文字以下にする必要があります。64 文字を超えるパスワードを入力すると、シャーシマネージャ に`org-root/cfg-exp-policy-default のプロパティパスワードが範囲外である`ことを示すエラーが表示されます。

g) [ファイルパス（File Path）] フィールドに、コンフィギュレーション ファイルのフルパスをファイル名を含めて入力します。
h) [インポート（Import）] をクリックします。
操作の続行を確認するダイアログボックスが開き、シャーシの再起動についての警告が表示されます。
i) [はい（Yes）] をクリックして、指定したコンフィギュレーション ファイルをインポートします。
既存の設定が削除され、インポートしたファイルの設定が Firepower 4100/9300 シャーシに適用されます。インポート中にブレークアウトポートの設定が変更された場合は、Firepower 4100/9300 シャーシの再起動が必要になります。

バックアップからの Threat Defense Virtual の復元

問題または障害がある Threat Defense Virtual デバイスを交換するには、この手順を使用します。

高可用性デバイスおよびクラスタ化デバイスの場合は、この手順を使用してすべてのピアを交換できます。すべて交換するには、**restore** CLI コマンド自体を除き、すべてのデバイスですべての手順を同時に実行します。

（注） ネットワークからデバイスを切断する場合でも、Management Center の登録を解除しないでください。Threat Defense の高可用性デバイスまたはクラスタ化デバイスの場合は、高可用性またはクラスタリングを中断または解除しないでください。これらのリンクを維持することで、交換用デバイスを、復元後に自動的に再接続できます。

始める前に

要件、ガイドライン、制限事項、およびベストプラクティスを確認し、理解する必要があります。手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。

- バックアップと復元の要件 （557 ページ）
- バックアップと復元の注意事項と制限事項 （558 ページ）
- バックアップと復元のベストプラクティス （560 ページ）

手順

ステップ 1 障害のあるデバイスの正常なバックアップを見つけます。

バックアップ設定に応じて、デバイスのバックアップは次の場所に保存されています。

- 障害のあるデバイス自体の `/var/sf/backup`。
- Management Center の `/var/sf/remote-backup`。
- リモートの保存場所。

Threat Defense の高可用性デバイスおよびクラスタ化デバイスの場合は、グループを 1 つのユニットとしてバックアップします。高可用性デバイスの場合は、バックアッププロセスによって一意のバックアップファイルが作成され、各デバイスのロールがバックアップファイル名に示されます。クラスタの場合は、制御ノードとデータノードのバックアップファイルが、単一の圧縮ファイルにバンドルされます。ファイルを抽出する必要があります。このファイルにもデバイスのロールが示されます。

バックアップの唯一のコピーが、障害のあるデバイス上にある場合は、ここで別の場所にコピーします。デバイスを再イメージ化すると、バックアップが消去されます。他に問題が発生した場合、バックアップを回復できなくなる可能性があります。詳細については、「バックアップとリモートストレージの管理 （590 ページ）」を参照してください。

交換用デバイスにはバックアップが必要ですが、復元プロセス中に SCP によってバックアップを取得できます。交換用デバイスに SCP でアクセス可能な場所にバックアップを配置して

おくことをお勧めします。または、バックアップを交換用デバイス自体にコピーすることができます。

ステップ 2 障害のあるデバイスを取り外します。

仮想マシンをシャットダウンして電源を切り、削除します。手順については、ご使用の仮想環境のマニュアルを参照してください。

ステップ 3 交換用デバイスを展開します。

https://www.cisco.com/go/ftdv-quickを参照してください。

ステップ 4 交換用デバイスで初期設定を行います。

コンソールを使用して、Threat Defense CLI に `admin` ユーザーとしてアクセスします。セットアップウィザードでは、管理 IP アドレス、ゲートウェイ、およびその他の基本ネットワーク設定を指定するように求められます。

障害のあるデバイスと同じ管理 IP アドレスを設定しないでください。それにより、パッチを適用するためにデバイスを登録する必要がある場合に問題が発生する可能性があります。復元プロセスにより、管理 IP アドレスが正しくリセットされます。

スタートアップガイドで、CLI のセットアップに関するトピックを参照してください：https://www.cisco.com/go/ftdv-quick。

（注） 交換用デバイスにパッチを適用する必要がある場合は、スタートアップガイドの説明に従って Management Center 登録プロセスを開始します。パッチを適用する必要がない場合は、登録しないでください。

ステップ 5 交換用デバイスで、障害のあるデバイスと同じソフトウェアバージョン（パッチを含む）が実行されていることを確認します。

既存のデバイスが Management Center から削除されていないことを確認します。交換用デバイスは物理ネットワークからは管理できない必要があり、新しいハードウェアおよび交換する Threat Defense パッチは同じバージョンである必要があります。Threat Defense CLI には、upgrade コマンドはありません。パッチを適用するには、次の手順を実行します。

a) Management Center Web インターフェイスから、デバイス登録プロセスを完了します。

新しい AC ポリシーを作成し、デフォルトアクション「Network Discovery」を使用します。このポリシーはそのままにします。機能や変更を追加しないでください。これは、デバイスを登録して、機能が含まれないポリシーを展開するために使用されています。これにより、ライセンスを要求されなくなり、その後、デバイスにパッチを適用できます。バックアップが復元されると、ライセンスとポリシーが予想どおりの状態に復元されます。

b) デバイスにパッチを適用します：https://www.cisco.com/go/ftd-upgrade。

c) Management Center から、パッチを適用したばかりのデバイスの登録を解除します。

登録を解除しないと、復元プロセスによって「古い」デバイスが再起動された後で、非実体デバイスが Management Center に登録されます。

ステップ 6 交換用デバイスがバックアップファイルにアクセスできることを確認します。

復元プロセスでは SCP によってバックアップを取得できるため、バックアップをアクセス可能な場所に配置することをお勧めします。または、交換用デバイス自体（`/var/sf/backup`）にバックアップを手動でコピーすることもできます。クラスタ化されたデバイスの場合は、バックアップバンドルから適切なバックアップファイルを抽出します。

ステップ 7 Threat Defense CLI から、バックアップを復元します。

Threat Defense CLI に `admin` ユーザーとしてアクセスします。コンソールを使用するか、新しく設定された管理インターフェイス（IP アドレスまたはホスト名）に SSH で接続することができます。復元プロセスによってこの IP アドレスが変更されることに注意してください。

復元するには、次の手順を実行します。

- SCP を使用：**restore remote-manager-backup location** *scp-hostname username filepath backup tar-file*
- ローカルデバイスから：**restore remote-manager-backup** *backup tar-file*

Threat Defense の高可用性とクラスタリングの展開では、適切なバックアップファイル（プライマリとセカンダリ、または制御とデータ）を選択してください。役割は、バックアップファイル名に示されます。すべてのデバイスを復元する場合は、この手順を順番に実行します。再起動を含め、最初のデバイスの復元プロセスが完了するまで、次のデバイスで **restore** コマンドを実行しないでください。

ステップ 8 Management Center にログインし、交換用デバイスが接続されるまで待ちます。

復元が完了すると、デバイスは、ユーザーを CLI からログアウトさせ、再起動して、自動的に Management Center に接続します。この時点では、デバイスが期限切れと表示されます。

ステップ 9 展開する前に、復元後のタスクを実行し、復元後の問題を解決します。

- ライセンスの競合や孤立した権限付与を解決します。Cisco TAC にお問い合わせください。
- すべての VPN 証明書を再追加/再登録します。復元プロセスでは、VPN 証明書（バックアップの実行後に追加された証明書を含む）が Threat Defense デバイスから削除されます。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Managing VPN Certificates*」を参照してください。

ステップ 10 設定を展開します。

この展開は必須です。デバイスを復元したら、[デバイス管理（Device Management）]ページから強制的に展開する必要があります。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Redeploy Existing Configurations to a Device*」を参照してください。

ステップ 11 データインターフェイスを追加して設定します。

スタートアップガイドを参照してください：https://www.cisco.com/go/ftdv-quick。

次のタスク

復元が成功し、交換用デバイスが予期どおりにトラフィックを通過させていることを確認します。

バックアップとリモートストレージの管理

バックアップは、暗号化されていないアーカイブ（.tar）ファイルとして保存されます。ファイル名には、次のような識別情報が含まれる場合があります。

- バックアップに関連付けられているバックアッププロファイルまたはスケジュールタスクの名前。
- バックアップされたアプライアンスの表示名または IP アドレス。
- アプライアンスのロール（HA ペアのメンバーなど）。

アプライアンスを安全なリモートロケーションにバックアップし、転送が成功することを確認することをお勧めします。アプライアンスに残っているバックアップは、手動またはアップグレードプロセスによって削除できます。アップグレードすると、ローカルに保存されたバックアップは削除されます。オプションの詳細については、バックアップ保存場所（592 ページ）を参照してください。

注意 特に、バックアップファイルは暗号化されていないため、不正アクセスを許可しないでください。バックアップ ファイルが変更されていると、復元プロセスは失敗します。Admin/Maint ロールを持つユーザーは [バックアップ管理（Backup Management）] ページにアクセスでき、そこでリモートストレージからファイルを移動および削除できることに注意してください。

次の手順では、バックアップファイルを管理する方法について説明します。

手順

ステップ 1 システム（⚙）>**[ツール（Tools）]**>**[バックアップ/復元（Backup/Restore）]** を選択します。

[バックアップ管理（Backup Management）]ページには、使用可能なバックアップが一覧表示されます。また、バックアップの保存に使用できるディスク容量も一覧表示されます。十分な容量がない場合、バックアップが失敗する可能性があります。

ステップ 2 次のいずれかを実行します。

表 *51* : リモートストレージとバックアップファイルの管理

目的	操作手順
Management Center のシステム設定を編集せずに、バックアップのリモートストレージを有効または無効にします。	[バックアップのリモートストレージを有効にする（Enable Remote Storage for Backups）] をクリックします。 このオプションは、リモートストレージを設定した後にのみ表示されます。ここで切り替えると、システム設定（[システム（System）] > [設定（Configuration）] > [リモートストレージデバイス（Remote Storage Device）]）でも切り替わります。 **ヒント** リモートストレージ設定にすばやくアクセスするには、[バックアップ管理（Backup Management）] ページの右上にある [リモートストレージ（Remote Storage）] をクリックします。 （注） バックアップをリモート ストレージ ロケーションに保存するには、[Management Centerに取得（Retrieve to Management Center）] オプションを有効にする必要があります（Management Center からのデバイスのバックアップ （568 ページ） を参照）。
Management Center とリモートの保存場所の間でファイルを移動します。	[移動（Move）] をクリックします。 ファイルは必要に応じて何度でも移動したり戻すことができます。これにより、現在の場所では、ファイルがコピーされずに削除されます。 バックアップファイルをリモートストレージから Management Center に移動する場合、Management Center での保存場所は、バックアップの種類によって異なります。 • Management Center のバックアップ：`/var/sf/backup` • デバイスのバックアップ：`/var/sf/remote-backup`
バックアップの内容を表示します。	バックアップファイルをクリックします。
バックアップファイルを削除します。	バックアップファイルを選択し、[削除（Delete）] をクリックします。 ローカル保存とリモート保存のどちらのバックアップファイルも削除できます。
ご使用のコンピュータからバックアップファイルをアップロードします。	[バックアップのアップロード（Upload Backup）] をクリックし、バックアップファイルを選択して、もう一度 [バックアップのアップロード（Upload Backup）] をクリックします。

目的	操作手順
ご使用のコンピュータにバックアップをダウンロードします。	バックアップファイルを選択し、[ダウンロードして（Download）] をクリックします。 バックアップファイルの移動とは異なり、バックアップは Management Center から削除されません。ダウンロードしたバックアップを安全な場所に保存します。

バックアップ保存場所

次の表に、Management Center および管理対象デバイスのバックアップ ストレージ オプションを示します。

表 *52*：バックアップ保存場所

参照先	詳細
リモート。ネットワークボリューム（NFS、SMB、SSHFS）をマウントします。	（注） リモートストレージを構成し、[Management Centerに取得（Retrieve to Management Center）] オプションを有効にした場合にのみ、バックアップはリモート ストレージ ロケーションに保存されます（Management Center からのデバイスのバックアップ （568 ページ） を参照）。 Management Center のシステム設定では、NFS、SMB、または SSHFS ネットワークボリュームを Management Center およびデバイスバックアップのリモートストレージとしてマウントできます。リモート ストレージ デバイス （111 ページ） を参照してください。） これを実行すると、その後のすべての Management Center バックアップと *Management Center* が開始するデバイスバックアップがそのボリュームにコピーされますが、引き続き Management Center を使用してそれらを管理（復元、ダウンロード、アップロード、削除、移動）することができます。 Management Center だけがネットワークボリュームをマウントすることに注意してください。管理対象デバイスのバックアップファイルは、Management Center を介してルーティングされます。Management Center とそのデバイスの間に大容量のデータを転送するための帯域幅があることを確認します。詳細については、『Guidelines for Downloading Data from the Firepower Management Center to Managed Devices』（トラブルシューティング テクニカル ノーツ）を参照してください。

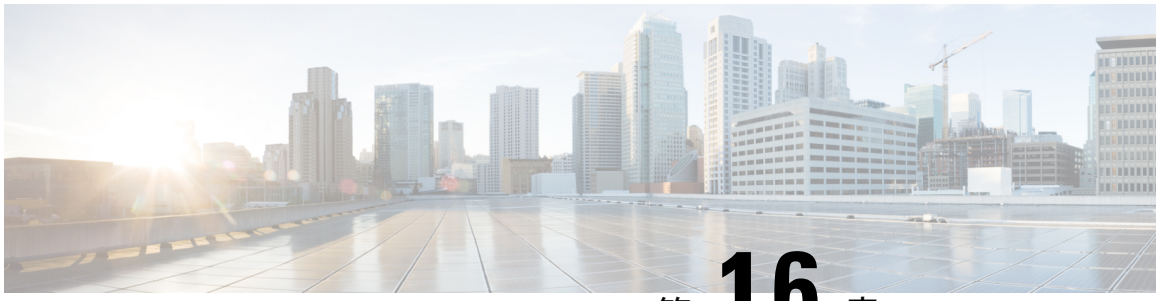
参照先	詳細
リモート。コピー（SCP）します。	（注） リモートストレージを構成し、[Management Centerに取得（Retrieve to Management Center）] オプションを有効にした場合にのみ、バックアップはリモート ストレージ ロケーションに保存されます（Management Center からのデバイスのバックアップ （568 ページ） を参照）。 Management Center の場合は、[完了時にコピー（Copy when complete）] オプションを使用して、完了したバックアップをリモートサーバーに安全にコピー（SCP）できます。 ネットワークボリュームをマウントすることによるリモートストレージとは異なり、[完了時にコピー（Copy when complete）] では NFS または SMB ボリュームにコピーすることはできません。CLI オプションを指定したり、ディスク容量のしきい値を設定することもできません。また、レポートのリモートストレージに影響を与えることはありません。さらに、コピーされたバックアップファイルを管理できません。 このオプションは、バックアップをローカルに保存するとともに、リモートの場所への SCP を実行する場合に便利です。 （注） Management Center のシステム設定で SSHFS リモートストレージを設定する場合は、[完了時にコピー（Copy when complete）] を使用してバックアップファイルを同じディレクトリにコピーしないでください。
ローカル、Management Center	ネットワークボリュームをマウントすることによってリモートストレージを設定しない場合は、Management Center にバックアップファイルを保存できます。 • Management Center のバックアップは `/var/sf/backup` に保存されます。 • バックアップの実行時に [管理センターで取得する（Retrieve to Management Center）] オプションを有効にすると、デバイスのバックアップは Management Center 上の `/var/sf/remote-backup` に保存されます。
ローカル（デバイスの内部フラッシュメモリ上）。	次の場合、デバイスのバックアップファイルはデバイス上の `/var/sf/backup` に保存されます。 • ネットワークボリュームをマウントすることによってリモートストレージを設定しない。 • [管理センターで取得する（Retrieve to Management Center）] を有効にしない。

参照先	詳細
ローカル（デバイスのSDカード上）。	ISA 3000 の場合、デバイスをローカルの内部フラッシュメモリの場所（/var/sf/backup）にバックアップするときに、SD カードを取り付けていると、バックアップはゼロタッチ復元で使用するために SD カード（/mnt/disk3/backup/）に自動的にコピーされます。

バックアップと復元の履歴

機能	最小 Management Center	最小 Threat Defense	詳細
高可用性 Management Center 用の単一のバックアップファイル。	7.4.1 7.2.6	いずれか	高可用性ペアのアクティブ Management Center の設定だけのバックアップを実行すると、いずれかのユニットの復元に使用できる単一のバックアップファイルが作成されるようになりました。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。
デバイスクラスタのバックアップと復元。	7.3.0	いずれか	Management Center を使用してデバイスクラスタをバックアップできるようになりました。ただし、パブリッククラウド（Threat Defense Virtual for AWS）ではバックアップできません。復元するには、デバイス CLI を使用します。 新規/変更された画面：**[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] > [管理対象デバイスのバックアップ（Managed Device Backup）]** 新規/変更されたコマンド： **restore remote-manager-backup**
AWS 向け Threat Defense Virtual のバックアップおよび復元。	7.2.0	いずれか	Management Center を使用して AWS 向け Threat Defense Virtual をバックアップできるようになりました（デバイスクラスタを除く）。復元するには、デバイス CLI を使用します。
SD カードを使用した ISA 3000 でのゼロタッチ復元。	7.0.0	7.0.0	ローカルバックアップを実行すると、バックアップファイルが SD カードにコピーされます（カードがある場合）。交換用デバイスの設定を復元するには、新しいデバイスに SD カードを取り付け、デバイスの起動中に [リセット（Reset）] ボタンを 3 ー 15 秒間押します。
FTD コンテナインスタンスのバックアップと復元。	6.7.0	6.7.0	FMC を使用して、Firepower 4100/9300 で FTD コンテナインスタンスのオンデマンド リモート バックアップを実行できるようになりました。
復元するために VDB を一致させる必要がなくなりました。	6.6.0	任意（Any）	バックアップから FMC を復元すると、既存の VDB がバックアップファイル内の VDB に置き換えられます。復元する前に VDB バージョンを一致させる必要がなくなりました。

機能	最小 Management Center	最小 Threat Defense	詳細
自動スケジュール済みバックアップ。	6.5.0	いずれか	新規または再イメージ化された FMC の場合、セットアッププロセスにより、FMC の設定をバックアップしてローカルに保存する、週次のスケジュール済みタスクが作成されます。
管理対象デバイスのオンデマンドでのリモートバックアップ。	6.3.0	6.3.0	FMC を使用して、特定の管理対象デバイスのリモート バックアップをオンデマンドで実行できるようになりました。 サポートされるプラットフォームについては、バックアップと復元の要件 （557 ページ）を参照してください。 新規/変更された画面：[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] > [管理対象デバイスのバックアップ（Managed Device Backup）] 新規/変更された FTD CLI コマンド： **restore**



第 16 章

スケジューリング

ここでは、タスクをスケジュールする方法について説明します。

タスクのスケジューリングについて

さまざまなタスクを、指定した回数（一度または繰り返し）実行するようにスケジュールを設定できます。

タスクはバックエンドにおいてUTCでスケジュールされるため、いつ現地で実行されるかは、日付と場所によって異なります。また、タスクはUTCでスケジュールされるため、サマータイムなど、所在地で実施される場合がある季節調整に合わせて調節されることもありません。このような影響を受ける場合、スケジュールされたタスクは、現地時間を基準とすると、夏期では冬期の場合よりも1時間「遅れて」実行されることになります。

一部のタスクは、初期設定プロセスによって自動的にスケジュールまたは実行されます。

- 最新のVDBをダウンロードしてインストールする1回限りのタスク。
- 最新の利用可能なソフトウェアの更新およびVDBをダウンロードするためにスケジュールされた週次タスク。
- ローカルに保存された構成のみのManagement Centerバックアップを実行するためにスケジュールされた週次タスク。

週次タスクを確認し、必要に応じて調整する必要があります。必要に応じて、VDBやソフトウェアを実際に更新し、構成を展開する新しい定期タスクをスケジュールしてください。

重要 スケジュールされたタスクが意図したとおりに確実に実行されることの確認を強くお勧めします。タスクによっては低帯域幅のネットワークに非常に負荷をかけることがあります（ソフトウェアの自動更新が含まれるタスクや、管理対象デバイスに更新をプッシュする必要があるタスクなど）。ネットワーク使用率が低い時間帯にこのようなタスクを実行するよう、スケジュールしてください。構成の展開など、他のタスクにより、トラフィックが中断される可能性があります。このようなタスクは、メンテナンス期間中にスケジュールする必要があります。

タスクスケジューリングの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- メンテナンス ユーザー

定期タスクの設定

定期タスクの頻度を設定する際には、すべてのタイプのタスクで同じ手順に従います。

Webインターフェイスのほとんどのページに表示される時間はローカル時刻であり、ローカル設定で指定したタイム ゾーンに従ってそれが決定されます。さらに、Management Centerは、該当する場合にはローカル時刻の表示を夏時間（DST）に合わせて自動的に調整します。ただし、DSTから標準時への移行日および元に戻る移行日をまたがる定期タスクは、移行を考慮して調整されません。つまり、標準時の午前2:00にタスク スケジュールを作成すると、DST期間中は午前3:00に実行されます。同様に、DSTの午前2:00にタスク スケジュールを作成すると、標準時には午前1:00に実行されます。

手順

ステップ1 システム（⚙）>**[ツール（Tools）]**>**[スケジューリング（Scheduling）]**を選択します。

ステップ2 [タスクの追加（Add Task）]をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] ドロップダウン リストから、スケジュールするタスクのタイプを選択します。

ステップ 4 [実行するタスクのスケジュール（Schedule task to run）] オプションの横にある [定期（Recurring）] をクリックします。

ステップ 5 [開始日付（Start On）] フィールドに、定期タスクを開始する日付を指定します。

ステップ 6 [繰り返し設定（Repeat Every）] フィールドに、タスクを繰り返す頻度を指定します。

数値を入力するか、[上へ（Up）]（▲）および[下へ（Down）]（▼）をクリックして、間隔を指定できます。たとえば、2 日おきにタスクを実行するには、2 を入力して [日（Days）] をクリックします。

ステップ 7 [実行時刻（Run At）] フィールドで、定期タスクを開始する時刻を指定します。

ステップ 8 週または月単位で実行するタスクの場合は、[繰り返す（オン）（Repeat On）] フィールドでタスクを実行する日付を選択します。

ステップ 9 ジョブに名前を付けます。

ステップ 10 作成するタスクのタイプについて残りのオプションを選択します。

- [バックアップ（Backup）]：Management Center のバックアップのスケジュール（600 ページ）の説明に従って、バックアップジョブをスケジュールします。
- [CRL のダウンロード（Download CRL）]：証明書失効リストのダウンロードの設定（602 ページ）の説明に従って、証明書失効リストのダウンロードをスケジュールします。
- [ポリシーの展開（Deploy Policies）]：ポリシー展開の自動化（603 ページ）の説明に従って、ポリシーの展開をスケジュールします。
- [Nmap スキャン（Nmap Scan）]：Nmap スキャンのスケジュール（605 ページ）の説明に従って、Nmap スキャンをスケジュールします。
- [レポート（Report）]：レポートの生成の自動化（606 ページ）の説明に従って、レポート生成をスケジュールします。
- [Cisco推奨ルール（CiscoFirepower Recommended Rules）]：Cisco 推奨の自動化（608 ページ）の説明に従って、自動更新をスケジュールします。
- [最新の更新のダウンロード（Download Latest Update）]：ソフトウェア ダウンロードの自動化（610 ページ）またはVDB 更新のダウンロードの自動化（613 ページ）の説明に従って、ソフトウェアまたは VDB の更新のダウンロードをスケジュールします。
- [最新の更新のインストール（Install Latest Update）]：ソフトウェア インストールの自動化（612 ページ）またはVDB 更新のインストールの自動化（614 ページ）の説明に従って、Management Center または管理対象デバイスでのソフトウェアまたは VDB の更新のインストールをスケジュールします。
- [最新の更新のプッシュ（Push Latest Update）]：ソフトウェア プッシュの自動化（611 ページ）の説明に従って、管理対象デバイスへのソフトウェア更新のプッシュをスケジュールします。

- [URLフィルタリングデータベースの更新（Update URL Filtering Database）]：スケジュール設定されたタスクを使用したURLフィルタリング更新の自動化（615ページ）の説明に従って、URL フィルタリングデータの自動更新をスケジュールします。

ステップ 11 [保存（Save）] をクリックします。

スケジュール バックアップ

Secure Firewall Management Centerでスケジューラを使用して、それ自体のバックアップを自動化することができます。Management Centerからデバイスのリモートバックアップをスケジュールすることもできます。バックアップの詳細については、バックアップ/復元（555ページ）を参照してください。

すべてのデバイスがリモートバックアップをサポートしているわけではないことに注意してください。

Management Center のバックアップのスケジュール

Management Center でスケジューラを使用して、Management Center とデバイスのバックアップを自動化することができます。すべてのデバイスがリモートバックアップをサポートしているわけではないことに注意してください。詳細については、バックアップ/復元（555ページ）を参照してください。

（注） 初期構成の一環として、システムは（ローカルに保存された）設定のみの週次 Management Center バックアップをスケジュールします。このタスクを確認し、必要に応じ、 このトピック。

始める前に

バックアップ設定を指定するバックアッププロファイルを作成します。バックアッププロファイルの作成（571 ページ）を参照してください。

このタスクを実行するには、グローバルドメインに属している必要があります。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [ジョブ タイプ（Job Type）] リストから、[バックアップ（Backup）] を選択します。

ステップ 3 [1回（Once）] または [定期（Recurring）] のどちらでバックアップするかを指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの場合、定期タスクの設定（598 ページ）を参照してください。

ステップ 4 [ジョブ名（Job Name）] を入力します。

ステップ 5 [バックアップタイプ（Backup Type）] で、[Management Center] をクリックします。

ステップ 6 [バックアッププロファイル（Backup Profile）] を選択します。

ステップ 7 （オプション）[コメント（Comment）] を入力します。

コメントは手短にします。それらはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。

ステップ 8 （オプション）[ステータスの送信先（Email Status To:）] フィールドに、メール アドレスまたはメール アドレスのコンマ区切りのリストを入力します。

タスクのステータス メッセージを送信するように電子メール リレー サーバーを設定する方法については、メール リレー ホストおよび通知アドレスの設定 （69 ページ）を参照してください。

ステップ 9 [保存（Save）] をクリックします。

リモート デバイス バックアップのスケジュール

Management Center でスケジューラを使用して、Management Center とデバイスの両方のバックアップを自動化することができます。すべてのデバイスがリモートバックアップをサポートしているわけではないことに注意してください。詳細については、バックアップ/復元 （555 ページ）を参照してください。

このタスクを実行するには、グローバルドメインに属している必要があります。

手順

ステップ 1 **システム**（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [ジョブ タイプ（Job Type）] リストから、[バックアップ（Backup）] を選択します。

ステップ 3 [1回（Once）] または [定期（Recurring）] のどちらでバックアップするかを指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの場合、定期タスクの設定 （598 ページ）を参照してください。

ステップ 4 [ジョブ名（Job Name）] を入力します。

ステップ 5 [バックアップのタイプ（Backup Type）] で、[デバイス（Device）] をクリックします。

ステップ 6 1 つ以上のデバイスを選択します。

お使いのデバイスがリストにない場合、リモートバックアップはサポートされていません。

ステップ 7 バックアップ用のリモートストレージを設定しなかった場合は、[管理センターで取得する（Retrieve to Management Center）] を有効または無効にできます。

- 有効（デフォルト）：バックアップが Management Center の `/var/sf/remote-backup/` に保存されます。
- 無効：バックアップがデバイスの `/var/sf/backup` に保存されます。

リモート バックアップ ストレージを設定している場合、バックアップ ファイルはリモートに保存され、このオプションは無効になります。詳細については、「バックアップとリモートストレージの管理 （590 ページ）」を参照してください。

ステップ 8 （オプション）[コメント（Comment）] を入力します。

コメントは手短にします。それらはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。

ステップ 9 （オプション）[ステータスの送信先（Email Status To:）] フィールドに、メール アドレスまたはメール アドレスのコンマ区切りのリストを入力します。

タスクのステータス メッセージを送信するように電子メール リレー サーバーを設定する方法については、メール リレー ホストおよび通知アドレスの設定 （69 ページ）を参照してください。

ステップ 10 [保存（Save）] をクリックします。

証明書失効リストのダウンロードの設定

Management Centerのローカル Web インターフェイスを使用して、この手順を実行する必要があります。

アプライアンスのユーザ証明書または監査ログ証明書を有効にするアプライアンスのローカル設定で証明書失効リスト（CRL）のダウンロードを有効にすると、CRL のダウンロード タスクが自動的に作成されます。スケジューラを使用してタスクを編集し、更新の頻度を設定できます。

始める前に

- ユーザ証明書または監査ログ証明書を有効にして設定し、1 つ以上の CRL のダウンロード URL を設定します。詳細については、有効な HTTPS クライアント証明書の強制 （78 ページ）と有効な監査ログ サーバー証明書の要求 （58 ページ）を参照してください。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブタイプ（Job Type）] から、[CRL のダウンロード（Download CRL）] を選択します。

ステップ 4 CRL ダウンロードをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （598 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 タスクについてコメントするには、[コメント（Comment）] フィールドにコメントを入力します。

[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 7 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、Management Centerで有効な電子メール中継サーバが設定されている必要があります。

ステップ 8 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定 （69 ページ）

ポリシー展開の自動化

Management Center の設定を変更した後は、影響を受けるデバイスへ変更を展開する必要があります。

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。Snort の再起動によるトラフィックの動作および展開またはアクティブ化された際に Snort プロセスを再起動する設定を参照してください。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブタイプ（Job Type）] から、[ポリシーの展開（Deploy Policies）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （598 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [デバイス（Device）] フィールドで、ポリシーを展開するデバイスを選択します。

ステップ 7 [最新のデバイスへの展開をスキップする（Skip deployment for up-to-date devices）] チェックボックスを、必要に応じてオンまたはオフにします。

デフォルトでは、ポリシーの展開プロセス中のパフォーマンスを向上させるため、[最新のデバイスへの展開をスキップする（Skip deployment for up-to-date devices）] オプションが有効になっています。

（注） システムは、Management Center の Web インターフェイスから開始されたポリシーの展開が進行中の場合、スケジュール設定されたポリシーの展開タスクを実行しません。同様に、システムは、スケジュール設定されたポリシーの展開タスクが進行中の場合、Web インターフェイスからポリシーの展開を開始することを許可しません。

ステップ 8 タスクについてコメントを付加するには、[コメント（Comment）] フィールドにコメントを入力します。

[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 9 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 10 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定 （69 ページ）
展開が必要な設定変更

Nmap スキャンの自動化

ネットワーク上のターゲットに対する定期的な Nmap スキャンをスケジュールできます。スキャンを自動化すると、Nmap スキャンによって以前に提供された情報を更新できます。システムは Nmap から提供されるデータを更新できないため、このデータを最新に保つには定期的に再スキャンする必要があります。また、ネットワーク上のホストに識別不能なアプリケーションやサーバがあるかどうか自動的に検査するよう、スキャンをスケジュールすることもできます。

さらに、Discovery Administrator が修正用に Nmap スキャンを使用する場合があることにも注意してください。たとえば、ホストでオペレーティング システム競合が発生したために、Nmap スキャンがトリガーされることがあります。スキャンが実行されると、そのホストでのオペレーティング システムの更新済み情報が取得され、こうして競合が解決されます。

以前に Nmap スキャン機能を使用したことがない場合は、スケジュール スキャンを定義する前に、Nmap スキャンを設定します。

関連トピック

Nmap スキャン

Nmap スキャンのスケジュール

システムで検出されたホストのオペレーティング システム、アプリケーション、またはサーバーが Nmap スキャンの結果で置き換えられると、システムは、Nmap によって置換されたホストに関する情報を更新しなくなります。Nmap によって提供されるサービスやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap を使用したホストのスキャンを計画している場合は、Nmap 提供のオペレーティング システム、アプリケーション、またはサーバを最新の状態に保つために、定期的なスキャン スケジュールをセットアップしてください。ネットワーク マップからホストが削除されて再び追加されると、Nmap スキャン結果はすべて破棄され、システムはホストに関するすべてのオペレーティング システムとサービスのデータのモニタリングを再開します。

手順

ステップ 1 **システム**（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブタイプ（Job Type）] から、[Nmap スキャン（Nmap Scan）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （598 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [Nmap 修復（Nmap Remediation）] フィールドで、Nmap 修復を選択します。

ステップ 7 [Nmap ターゲット（Nmap Target）] フィールドで、スキャン ターゲットを選択します。

ステップ 8 [ドメイン（Domain）] フィールドで、増補するネットワーク マップを持つドメインを選択します。

ステップ 9 タスクにコメントを付ける場合は、[コメント（Comment）] フィールドにコメントを入力します。

ヒント [コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 10 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）]フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 11 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定 （69 ページ）

レポートの生成の自動化

一定期間ごとにレポートを実行するよう自動化できます。

始める前に

- リスク レポート以外のレポートの場合：レポート テンプレートを作成します。詳細については、レポート テンプレート （642 ページ）を参照してください。
- スケジューラを使用してメール レポートを配布するには、メール リレーのホストを設定し、レポートの受信者およびメッセージ情報を指定します。メール リレー ホストおよび通知アドレスの設定 （69 ページ） と、（リスク レポート以外のレポートの場合）レポートの生成時の電子メール配布 （666 ページ）または（リスク レポートの場合）リスク レポートの生成、表示および印刷 （640 ページ）を参照してください。
- （オプション）スケジュール設定されたレポートのファイル名、出力フォーマット、時間枠、またはメール配布の設定を設定または変更します。スケジュールされたレポート生成設定の指定 （607 ページ）を参照してください。
- レポートの出力形式として PDF を選択する場合は、テンプレートの各セクションの結果数が PDF の制限を超えないことを、レポート テンプレートで確認してください。詳細については、レポート テンプレート フィールド （642 ページ）を参照してください。

手順

ステップ 1 **システム（⚙） > [ツール（Tools）] > [スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブタイプ（Job Type）] リストから、ジョブを選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （598 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [レポートテンプレート（Report Template）] フィールドで、リスクレポート、またはレポートテンプレートを選択します。

ステップ 7 タスクについてコメントを付加するには、[コメント（Comment）] フィールドにコメントを入力します。

[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 8 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータスメッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

（注） このオプションを設定しても、レポートは配布されません。

ステップ 9 レポートのデータがない場合（たとえばレポート期間中に特定のタイプのイベントが発生しなかった場合）にレポート電子メール添付ファイルを受信しないようにするには、[空のレポートも添付（If report is empty, still attach to email）] チェックボックスを選択します。

ステップ 10 [保存（Save）] をクリックします。

スケジュールされたレポート生成設定の指定

このタスクを実行するには、管理者権限またはセキュリティアナリスト権限が必要です。

スケジュールされたレポートのファイル名、出力形式、時間枠、電子メール配布の設定を指定または変更するには、次の手順に従います。

手順

ステップ 1 [概要（Overview）] > [レポート（Reporting）] > [レポート テンプレート（Report Templates）] の順に選択します。

ステップ 2 変更するレポート テンプレートの [編集（Edit）] をクリックします。

ステップ 3 PDF 出力を選択する場合は、次のようにします。

a) レポートのいずれかのセクションで、結果数の横に黄色い三角形が示されているかどうかを調べます。

b) 黄色の三角形が示されている場合、三角形の上にマウス カーソルを重ねると、PDF 出力のそのセクションに対して許容される結果の最大数が表示されます。

c) 黄色い三角形が示されているセクションごとに、結果数を最大数未満の数に削減します。

d) 黄色い三角形が示されなくなったら、[保存（Save）] をクリックします。

ステップ 4 [生成（Generate）] をクリックします。

（注） 今すぐレポートを生成せずにレポート生成の設定を変更する場合は、テンプレート設定ページで [生成（Generate）] をクリックする必要があります。レポートを生成しない限り、テンプレート リスト ビューで [生成（Generate）] をクリックしても変更は保存されません。

ステップ 5 設定を変更します。

ステップ 6 レポートを生成せずに新しい設定を保存するには、[キャンセル（Cancel）] をクリックします。

新しい設定を保存してレポートを生成するには、[生成（Generate）] をクリックし、この手順の残りのステップをスキップします。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 保存を求めるプロンプトが出されたら、まだ変更していない場合でも [OK] をクリックします。

Cisco 推奨の自動化

カスタム侵入ポリシーで保存済みの最新の設定を使用し、ネットワークのディスカバリ データに基づいてルール状態の推奨を自動的に生成することができます。

（注） 変更が未保存のまま、侵入ポリシーに関するスケジュール済み推奨がシステムによって自動生成される場合、自動生成された推奨をポリシーに反映させるには、そのポリシー内の変更を破棄してポリシーをコミットする必要があります。

タスクを実行すると、推奨ルール状態が自動的に生成され、ポリシーの設定に基づいて侵入ルールの状態が変更されます。変更されたルール状態は、侵入ポリシーを次回に展開するときに有効になります。

始める前に

- Cisco Secure Firewall Management Center デバイス構成ガイドの説明に従い、侵入ポリシーで Cisco 推奨ルールを設定します。
- タスクのステータス メッセージをメールで送るには、有効なメール リレー サーバーを設定します。
- 推奨を生成するには、IPS スマートライセンスまたは保護クラシックライセンスが必要です。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブタイプ（Job Type）] から、[Cisco推奨ルール（Cisco Recommended Rules）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （598 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [ポリシー（Policies）] の横で、推奨を生成する 1 つ以上の侵入ポリシーを選択します。[すべてのポリシー（All Policies）] チェックボックスをオンにして、すべての侵入ポリシーを選択します。

ステップ 7 （任意）[コメント（Comments）] フィールドにコメントを入力します。

コメントは手短にします。コメントはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。

ステップ 8 （任意）タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。

ステップ 9 [保存（Save）] をクリックします。

関連トピック

競合と変更：ネットワーク分析ポリシーと侵入ポリシー
シスコ推奨ルールについて
メール リレー ホストおよび通知アドレスの設定 （69 ページ）

ソフトウェアアップグレードの自動化

パッチを自動的にダウンロードし、メンテナンスリリースとパッチを適用することができます。

Management Center をアップグレードするには、ダウンロードタスクとインストールタスクをスケジュールします。管理対象デバイスをアップグレードするには、ダウンロードタスク、プッシュタスク、およびインストールタスクをスケジュールします。タスク間に十分な時間を空けるようにしてください。たとえば、プッシュがまだ実行されているときに実行するようにスケジュールされたインストールは失敗します。

この機能は、メジャーリリースではサポートされていません。アップグレードパッケージをダウンロードするには、インターネットアクセスが必要です。デバイスグループへのアップグレードをスケジュールすると、アップグレードは、グループ化されたすべてのデバイスで同時に実行されます。

（注） 初期構成の一環として、システムは週ごとのダウンロードをスケジュールします。このタスクを確認し、必要に応じ、ソフトウェア ダウンロードの自動化（610ページ）。このタスクは、更新のみをダウンロードします。ユーザは、このタスクがダウンロードした更新をインストールする必要があります。

関連トピック

管理インターフェイス （84 ページ）
更新 （263 ページ）

ソフトウェア ダウンロードの自動化

この手順を使用して、選択したパッチのダウンロードとメンテナンスリリースのスケジュールを設定します。グローバルドメインにいる必要があります。

（注） バージョン 7.4.1 以降では、このタスクではメンテナンスリリースをダウンロードしなくなりました。直接メンテナンス（およびメジャー）リリースを Management Center に直接ダウンロードするには、**システム**（⚙）> **[Product Upgrades]** を使用します。

始める前に

Management Center でインターネットにアクセスできることを確認します。

手順

ステップ 1 **システム**（⚙）> **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[最新の更新のダウンロード（Download Latest Update）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （598 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [アップデート項目（Update Items）] の横の [ソフトウェア（Software）] チェックボックスをオンにします。

ステップ 7 タスクについてコメントするには、[コメント（Comment）] フィールドにコメントを入力します。

[コメント（Comment）]フィールドはスケジュール予定表ページの[タスクの詳細（Task Details）]セクションに表示されます。コメントは手短にします。

ステップ 8 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）]フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 9 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定 （69 ページ）

ソフトウェア プッシュの自動化

管理対象デバイスでのソフトウェア更新のインストールを自動化するには、インストールの前に、更新をデバイスにプッシュする必要があります。

ソフトウェア更新を管理対象デバイスにプッシュするタスクを作成する際には、更新がデバイスに確実にコピーされるよう、プッシュ タスクとスケジュール済みインストール タスクの間に十分な時間を確保してください。

このタスクを実行するには、グローバルドメインに属している必要があります。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブタイプ（Job Type）] リストから、[最新の更新をプッシュ（Push Latest Update）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （598 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [デバイス（Device）] ドロップダウン リストから、更新するデバイスを選択します。

ステップ 7 タスクについてコメントするには、[コメント（Comment）]フィールドにコメントを入力します。

[コメント（Comment）]フィールドはスケジュール予定表ページの[タスクの詳細（Task Details）]セクションに表示されます。コメントは手短にします。

ステップ 8 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）]フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力

します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 9 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定 （69 ページ）

ソフトウェア インストールの自動化

管理対象デバイスへ更新をプッシュするタスクと、その更新をインストールするタスクの間に十分な時間を確保する必要があります。

このタスクを実行するには、グローバルドメインに属している必要があります。

注意 インストールする更新によっては、ソフトウェアのインストール後にアプライアンスがリブートする場合があります。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[最新の更新のインストール（Install Latest Update）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （598 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [デバイス（Device）] ドロップダウンリストから、更新をインストールするアプライアンス（Management Centerを含む）を選択します。

ステップ 7 [アップデート項目（Update Items）] の横の [ソフトウェア（Software）] チェックボックスをオンにします。

ステップ 8 タスクについてコメントするには、[コメント（Comment）] フィールドにコメントを入力します。

[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 9 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力

します。ステータスメッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 10 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定 （69 ページ）

脆弱性データベースの更新の自動化

スケジュール機能を使用してシスコの脆弱性データベース（VDB）を更新できるため、常に最新の情報を使ってネットワーク上のホストを評価することができます。ダウンロード、インストール、およびその後の展開を個別のタスクとしてスケジュールし、タスク間に十分な時間を確保する必要があります。

（注） Management Center の初期設定では、1 回限りの操作でシスコから最新の VDB が自動的にダウンロードされてインストールされます。また、最新の VDB を含む最新の利用可能なソフトウェアアップデートをダウンロードする週次タスクもスケジュールされます。この週次タスクを確認し、必要に応じて調整することをお勧めします。必要に応じて、VDB を実際に更新し、構成を展開する新しい週次タスクをスケジュールしてください。

関連トピック

管理インターフェイス （84 ページ）

VDB 更新のダウンロードの自動化

このタスクを実行するには、グローバルドメインに属している必要があります。

始める前に

Management Center にインターネット アクセスがあることを確認します。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[最新の更新のダウンロード（Download Latest Update）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （598 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [アップデート項目（Update Items）] の横の [脆弱性データベース（Vulnerability Database）] チェックボックスをオンにします。

ステップ 7 （任意）[コメント（Comments）] フィールドに簡単なコメントを入力します。

ステップ 8 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 9 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定 （69 ページ）

VDB 更新のインストールの自動化

VDB 更新をダウンロードするタスクと、その更新をインストールするタスクの間に十分な時間を確保してください。

このタスクを実行するには、グローバルドメインに属している必要があります。

注意 ほとんどの場合、VDB 更新後の最初の展開では Snort プロセスが再起動され、トラフィックインスペクションが中断されます。これが発生すると、システムから警告が表示されます（更新されたアプリケーションディテクタとオペレーティングシステムのフィンガープリントについては再起動が必要ですが、脆弱性情報については不要です）。この中断中にインスペクションを続行せずにトラフィックがドロップされるかパスするどうかは、対象デバイスによるトラフィックの処理方法によって異なります。詳細については、「Snort の再起動によるトラフィックの動作」を参照してください。

手順

ステップ 1 **システム（⚙）> [ツール（Tools）] > [スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[最新の更新のインストール（Install Latest Update）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （598 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [デバイス（Device）] ドロップダウン リストから Management Center を選択します。

ステップ 7 [アップデート項目（Update Items）] の横の [脆弱性データベース（Vulnerability Database）] チェックボックスをオンにします。

ステップ 8 （任意）[コメント（Comments）] フィールドに簡単なコメントを入力します。

ステップ 9 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータスメッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 10 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定 （69 ページ）

スケジュール設定されたタスクを使用した URL フィルタリング更新の自動化

URL フィルタリングの脅威データが最新であることを確認するため、システムは、Cisco（Collective Security Intelligencecsi）クラウドからデータ更新を取得する必要があります。

デフォルトでは、URL フィルタリングを有効にすると、自動更新が有効になります。ただし、これらの更新が発生する時間を制御する必要がある場合には、デフォルトの更新メカニズムではなく、このトピックで説明されている手順を使用します。

通常、毎日の更新は小規模ですが、最終更新日から 5 日を超えると、帯域幅によっては新しい URL フィルタリング データのダウンロードに最長 20 分かかる場合があります。その後、更新自体を実行するのに最長で 30 分かかることがあります。

始める前に

- Management Center にインターネットアクセス権があることを確認してください（セキュリティ、インターネット アクセス、および通信ポート （1277 ページ） を参照）。
- URL フィルタリングが有効にされていることを確認します。詳細については、Cisco Secure Firewall Management Center デバイス構成ガイド の「*Enable URL Filtering Using Category and Reputation*」を参照してください。
- **[統合（Integration）] > [その他の統合（Other Integrations）]** メニューの **クラウド サービス（Cloud Services）** で [自動更新を有効にする（Enable Automatic Updates）] が選択されていないことを確認します。
- このタスクを実行するには、グローバルドメインに属している必要があります。URL フィルタリングライセンスも必要です。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[URL フィルタリング データベースの更新（Update URL Filtering Database）] を選択します。

ステップ 4 更新をスケジュールする頻度として、ワンタイム更新を示す [1 回（Once）] または定期更新を示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （598 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 タスクについてコメントするには、[コメント（Comment）] フィールドにコメントを入力します。

[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 7 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 8 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定 （69 ページ）

スケジュール済みタスクの確認

スケジュール済みタスクを追加した後、それらのタスクを表示したり、状態を評価したりできます。ページの [表示オプション（View Options）] セクションで、カレンダーやスケジュール済みタスク リストを使用してスケジュール済みタスクを表示できます。

カレンダー表示オプションを使用すると、どの日にどのスケジュール済みタスクが行われるかを表示できます。

タスク リストには、タスクとその状態のリストが表示されます。タスク リストは、カレンダーを開いたときにカレンダーの下に表示されます。また、カレンダーで 1 つの日付またはタスクを選択して表示することもできます。

以前に作成したスケジュール済みタスクを編集できます。この機能は、パラメータが正しいことを確認するために、スケジュール済みタスクを 1 度テストする場合に特に役立ちます。タスクが正常に完了したら、後で定期タスクに変更できます。

[スケジュール表示（Schedule View）] ページから 2 種類の削除操作を実行できます。まだ実行されていない特定のワンタイム タスク、または定期タスクのすべてのインスタンスを削除できます。定期タスクの 1 つのインスタンスを削除すると、そのタスクのすべてのインスタンスが削除されます。1 度だけ実行するようスケジュールされているタスクを削除すると、そのタスクだけが削除されます。

タスク一覧の詳細

表 *53*：タスク一覧のカラム

カラム	説明
名前	スケジュール済みタスクの名前と、関連付けられているコメントを表示します。
タイプ	スケジュール済みタスクのタイプを表示します。
開始時刻（Start Time）	スケジュールされている開始日時を表示します。
頻度（Frequency）	タスクの実行頻度を表示します。
前回の実行時間（Last Run Time）	実際の開始日時を表示します。 定期タスクの場合、これは最新の実行に適用されます。
最終実行ステータス（Last Run Status）	スケジュール済みタスクの現在の状態を次のように示します。 • **[チェックマーク（Check Mark）]**（）は、タスクが正常に実行されたことを示します。 • 疑問符アイコン（**[疑問符（Question Mark）]**（））は、タスクの状態が不明であることを示します。 • 感嘆符アイコン（）は、タスクが失敗したことを示します。 定期タスクの場合、これは最新の実行に適用されます。
次回の実行時間（Next Run Time）	定期タスクの次の実行時間を表示します。 ワンタイム タスクの場合に「該当なし（N/A）」と表示します。
作成者（Creator）	スケジュール済みタスクを作成したユーザの名前を表示します。
編集（Edit）	スケジュール済みタスクを編集します。
削除（Delete）	スケジュール済みタスクを削除します。

カレンダーのスケジュール済みタスクの表示

スケジュールされたタスクは、カレンダーに表示できます。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 カレンダー ビューを使用して、次のタスクを実行できます。

- [二重左矢印（Double Left Arrow）]（«） をクリックすると、1 年前に戻ります。
- [左矢印（Single Left Arrow）]（‹） をクリックすると、1 か月前に戻ります。
- [右矢印（Single Right Arrow）]（›） をクリックすると、1 か月後に進みます。
- [二重右矢印（Double Right Arrow）]（») をクリックすると、1 年後に進みます。
- [今日（Today）] をクリックすると、現在の年月に戻ります。
- [タスクの追加（Add Task）] をクリックすると、新しいタスクをスケジュールできます。
- 1 つの日付をクリックすると、カレンダーの下にあるタスク リスト表に、特定の日付のスケジュール済みタスクがすべて表示されます。
- ある日付の特定のタスクをクリックすると、カレンダーの下にあるタスク リスト表にそのタスクが表示されます。

スケジュール済みタスクの編集

スケジュール済みタスクを編集できます。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 カレンダーで、編集するタスク、またはタスクが表示されている日付をクリックします。

ステップ 3 [タスクの詳細（Task Details）] テーブルで、編集するタスクの横にある**[編集（Edit）]**（✎）をクリックします。

ステップ 4 タスクを編集します。

ステップ 5 [保存（Save）] をクリックします。

スケジュール済みタスクの削除

スケジュール済みタスクを削除できます。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

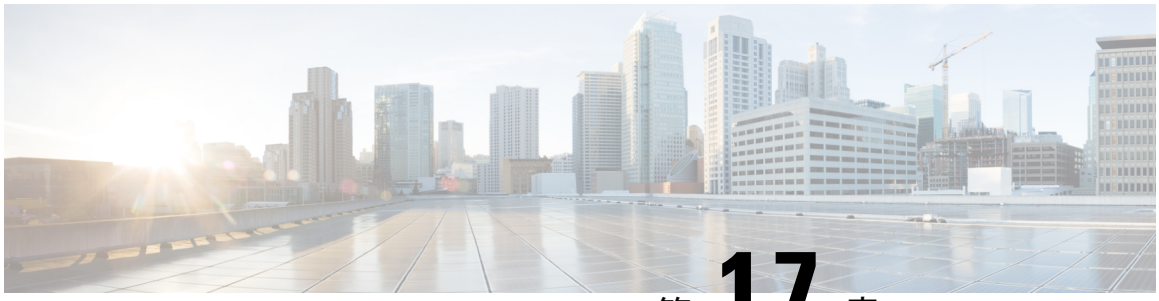
ステップ 2 カレンダーで、削除するタスクをクリックします。繰り返しタスクの場合は、タスクのインスタンスをクリックします。

ステップ 3 [タスク詳細（Task Details）] テーブルで、[削除（Delete）]（🗑） をクリックし、選択内容を確認します。

スケジュール済みタスクの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
スケジュール済みタスクでは、パッチおよびVDB 更新のみダウンロードされます。	7.4.1	任意（Any）	**アップグレードの影響。スケジュールされたダウンロードタスクは、メンテナンスリリースの取得を停止します。** [最新の更新のダウンロード（Download Latest Update）] スケジュール済みタスクでは、メンテナンスリリースはダウンロードされなくなり、適用可能な最新のパッチと VDB の更新のみがダウンロードされるようになりました。メンテナンス（およびメジャー）リリースを Management Center に直接ダウンロードするには、**システム**（⚙） > **[製品のアップグレード（Product Upgrades）]**を使用します。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。
自動 VDB ダウンロード。	7.3.0	いずれか	初期設定では、利用可能な最新のソフトウェアアップデート（最新の VDB を含む）をダウンロードするための週次タスクがスケジュールされます。この週次タスクを確認し、必要に応じて調整し、新しい週次タスクをスケジュールして実際に VDB を更新することを推奨します。アプリケーションディテクタとオペレーティングシステムフィンガープリントを有効にするためには、設定を展開する必要があります。 新規/変更された画面：システムで作成された [週次ソフトウェアダウンロード（Weekly Software Download）] のスケジュールされたタスクで、[脆弱性データベース（Vulnerability Database）] チェックボックスがデフォルトで有効になりました。

機能	最小 Management Center	最小 Threat Defense	詳細
侵入ルールの自動更新。	6.6	任意（Any）	初期設定では、毎日の侵入ルールの更新が有効になります。このタスクを確認し、必要に応じて調整することを推奨します。更新されたルールを有効にするには、設定を展開する必要があります。
ソフトウェアの自動ダウンロードと設定のバックアップ。	6.5	任意（Any）	初期設定では、次の週次タスクがスケジュールされます。 • FMC とその管理対象デバイスの利用可能な最新のソフトウェアアップデートをダウンロードする。 • ローカルに保存された設定のみのバックアップを実行する。 これらのタスクを確認し、必要に応じて調整することを推奨します。
多数の管理対象デバイスのリモートバックアップをスケジュールします。	6.4	任意（Any）	リモート デバイス バックアップ。 新規/変更された画面：定期バックアップを設定するときに、[バックアップタイプ（Backup Type）]（Management Center とデバイス）を選択できるようになりました。 プラットフォームの制限：デバイスはオンデマンドバックアップをサポートする必要があります。バックアップと復元の要件（557ページ）を参照してください。



第 17 章

インポート/エクスポート

次のトピックでは、インポート/エクスポート機能を使用する方法について説明します。

コンフィギュレーションのインポート/エクスポートについて

インポート/エクスポート機能を使用して、アプライアンス間で構成をコピーできます。インポート/エクスポートはバックアップ ツールではありませんが、展開に新しいアプライアンスを追加するプロセスを簡素化できます。

単一の設定をエクスポートすることや、（同じタイプまたは異なるタイプの）一連の設定を単一操作でエクスポートすることができます。後に別のアプライアンスにパッケージをインポートするとき、パッケージ内のどの設定をインポートするかを選択できます。

エクスポートされたパッケージには、その構成のリビジョン情報が含まれ、これにより、別のアプライアンスにその構成をインポートできるかどうかが決まります。アプライアンスに互換性があるものの、パッケージに重複構成が含まれていると、解決オプションが示されます。

（注） インポート側とエクスポート側のアプライアンスは、同じバージョンのソフトウェアを実行している必要があります。アクセスコントロールとそのサブポリシー（侵入ポリシーを含む）の場合、侵入ルールの更新バージョンも一致している必要があります。バージョンが一致しない場合、インポートは失敗します。インポート/エクスポート機能を使用して侵入ルールを更新することはできません。代わりに、最新バージョンのルール更新をダウンロードして適用します。

インポート/エクスポートをサポートする構成

インポート/エクスポートは、次の構成でサポートされます。

- アクセス コントロール ポリシーとそれが呼び出すポリシー：プレフィルタ、ネットワーク分析、侵入、SSL、ファイル、Threat Defense サービス ポリシー
- 侵入ポリシー（アクセス コントロールとは無関係に）
- NAT ポリシー（Secure Firewall Threat Defense のみ）
- FlexConfig ポリシー。ただし、すべての秘密鍵の変数の内容は、ポリシーをエクスポートする際にクリアされます。秘密鍵を使用するFlexConfigポリシーをインポートした後に手動ですべての秘密鍵の値を編集する必要があります。
- プラットフォーム設定
- 正常性ポリシー
- アラート応答
- アプリケーションディテクタ（ユーザ定義およびCisco Professionalサービスによって提供されるディテクタ）
- ダッシュボード
- カスタム テーブル
- カスタム ワークフロー
- 保存済み検索
- カスタム ユーザ ロール
- レポート テンプレート
- サードパーティ製品および脆弱性マッピング
- ユーザー制御用のユーザーおよびグループ

設定のインポート/エクスポートに関する特別な考慮事項

構成をエクスポートすると、他の必要な構成もエクスポートされます。たとえば、アクセスコントロールポリシーをエクスポートすると、そのポリシーが呼び出すサブポリシー、使用しているオブジェクトおよびオブジェクトグループ、先祖ポリシーなどもエクスポートされます。別の例として、外部認証が有効になっているプラットフォーム設定ポリシーをエクスポートした場合は、認証オブジェクトもエクスポートされます。ただし、いくつかの例外があります。

- システム提供のデータベースとフィード：URLフィルタリングカテゴリとレピュテーション データ、シスコ インテリジェンス フィードデータ、または地理位置情報データベース（GeoDB）はエクスポートされません。展開内のすべてのアプライアンスがシスコから最新情報を取得していることを確認してください。

- グローバルなセキュリティインテリジェンスのリスト：エクスポートされた構成に関連するグローバルなセキュリティインテリジェンスのブロックリストとブロックしないリストがエクスポートされますインポートプロセスはこれらのリストをユーザー作成リストに変換してから、インポートされた構成でそれらの新しいリストを使用します。これにより、インポートされたリストが既存のグローバルなブロックリストおよびブロックしないリストと競合することはありません。インポート側の Management Center のグローバルリストを使用するには、それらのリストをインポートされた設定に手動で追加します。
- 侵入ポリシー共有層：エクスポートプロセスにより、侵入ポリシー共有レイヤが切断されます。以前の共有レイヤはパッケージに含まれ、インポートされた侵入ポリシーには共有レイヤは含まれません。
- 侵入ポリシーのデフォルト変数セット：エクスポートパッケージには、カスタム変数とシステム提供の変数を含むデフォルト変数セットがユーザ定義値とともに含まれています。インポート プロセスでは、インポートされた値でインポート側の Management Center のデフォルト変数セットを更新します。ただし、インポートプロセスはエクスポートパッケージに存在しないカスタム変数を削除**しません**。また、エクスポートパッケージに設定されていない値については、インポート側の Management Center のユーザ定義値を元に戻しません。したがって、インポート側の Management Center で設定されているデフォルト変数が異なる場合は、インポートされた侵入ポリシーの動作が予想とは異なる可能性があります。
- カスタム ユーザ オブジェクト：Management Center でカスタム ユーザ グループまたはオブジェクトを作成済みで、そのようなカスタムユーザ オブジェクトがアクセス コントロール ポリシーのいずれかのルールに含まれている場合、エクスポート ファイル（.sfo）にはそのユーザ オブジェクト情報が格納されません。このため、そうしたポリシーをインポートする際、これらのカスタム ユーザ オブジェクトへの参照が削除され、宛先 Management Center にはインポートされません。不明なユーザ グループが原因で検出の問題が発生するのを避けるには、カスタマイズされたユーザ オブジェクトを新しい Management Center に手動で追加し、インポート後にアクセス コントロール ポリシーを再設定します。

オブジェクトおよびオブジェクト グループをインポートする場合：

- 通常、インポートプロセスはオブジェクトとグループを新規としてインポートしますが、既存のオブジェクトとグループを置き換えることはできません。ただし、インポートされた設定のネットワークやポートのオブジェクトまたはグループが既存のオブジェクトまたはグループと一致する場合、インポートした設定は、新しいオブジェクト/グループを作成せずに、既存のオブジェクト/グループを再利用します。システムは、名前（自動生成される番号は除外します）および各ネットワークとポートのオブジェクト/グループの内容を比較して、一致するかどうかを判別します。
- インポートしたオブジェクトの名前がインポートする Management Center 上の既存のオブジェクトと一致する場合、システムはそれらの名前を一意にするため、インポートされたオブジェクトとグループの名前に自動生成した番号を付加します。
- インポートした設定で使用されているセキュリティ ゾーンとインターフェイス グループを、インポート側の Management Center で管理されているタイプが一致するゾーンとグループにマッピングする必要があります。

- 秘密キーを含むPKIオブジェクトを使用する構成をエクスポートすると、エクスポートの前に秘密キーが復号されます。インポート時に、キーはランダムに生成されたキーで暗号化されます。

構成のインポート/エクスポートの要件と前提条件

モデルのサポート

任意（Any）

サポートされるドメイン

任意

ユーザの役割

- 管理者

設定のエクスポート

エクスポートされる設定の数や、それらのオブジェクトが参照する設定の数によっては、エクスポート プロセスに数分かかる場合があります。

ヒント　多くのリストページには、リスト項目の横に [YouTube EDU]（  ） があります。このアイコンがある場合は、それを使用することにより、その後のエクスポート操作を簡単に代行させることができます。

始める前に

- インポートおよびエクスポートするアプライアンスが同じソフトウェアバージョンを実行していることを確認します。アクセス制御とそのサブポリシー（侵入ポリシーを含む）の場合は、侵入ルールの更新バージョンも一致する必要があります。

手順

ステップ 1　システム（⚙） > **[ツール（Tools）]** > **[インポート/エクスポート（Import/Export）]**を選択します。

ステップ 2　[折りたたみ（Collapse）]（∨） か [展開（Expand）]（>） をクリックして、使用可能な設定のリストを折りたたんだり、展開したりします。

ステップ 3 エクスポートする構成をチェックして [エクスポート（Export）] をクリックします。

ステップ 4 Webブラウザのプロンプトに従って、エクスポートされたパッケージをコンピュータに保存します。

設定のインポート

インポートされる設定の数や、それらのオブジェクトが参照する設定の数によっては、インポート プロセスに数分かかる場合があります。

（注） システムからログアウトした場合、別のドメインに変更した場合、または[インポート（Import）] をクリックした後にユーザーセッションの期限が切れた場合、インポートプロセスは完了するまでバックグラウンドで続行されます。新しいオブジェクトまたはポリシーを作成する前に、インポートプロセスの完了を待つことをお勧めします。インポートプロセスの実行中にそれらを作成しようとすると、失敗する可能性があります。

始める前に

- インポートおよびエクスポートするアプライアンスが同じソフトウェアバージョンを実行していることを確認します。アクセス制御とそのサブポリシー（侵入ポリシーを含む）の場合は、侵入ルールの更新バージョンも一致する必要があります。

手順

ステップ 1 インポートするアプライアンスで、**システム**（⚙）> **[ツール（Tools）]** > **[インポート/エクスポート（Import/Export）]** を選択します。

ステップ 2 [パッケージのアップロード（Upload Package）] をクリックします。

ステップ 3 エクスポートしたパッケージへのパスを入力するか、そのパッケージの場所を参照して [アップロード（Upload）] をクリックします。

ステップ 4 バージョンが一致していないなどの問題がない場合は、インポートする設定を選択して、[インポート（Import）] をクリックします。
競合の解決やインターフェイス オブジェクトのマッピングを実行する必要がない場合は、インポートが完了して、成功メッセージが表示されます。この手順の残りは省略してください。

ステップ 5 プロンプトが表示されたら、[アクセス制御インポートの解決（AccessControl Import Resolution）][インポートの競合解決（Import Conflict Resolution）] ページで、インポートする Management Center で管理されているインターフェイス タイプと一致するゾーンおよびグループに、インポートした設定で使用されているインターフェイスオブジェクトをマップします。

インターフェイス オブジェクト タイプ（セキュリティ ゾーンまたはインターフェイス グループ）およびインターフェイスタイプ（パッシブ、インライン、ルーテッドなど）が送信元と宛

先で一致している必要があります。詳細については、インターフェイス（Interface）を参照してください。

インポートする設定が存在していないセキュリティ ゾーンまたはインターフェイス グループを参照する場合は、その設定を既存のインターフェイ オブジェクトにマップするか、新しいインターフェイ オブジェクトを作成します。

（注） 個別のアクセス コントロール ポリシーに対して、既存のポリシーをインポートしたポリシーに置き換えることができます。ただし、ネストされたアクセス コントロール ポリシーの場合は、新しいポリシーとしてのみインポートできます。

ステップ 6 [インポート（Import）] をクリックします。

ステップ 7 プロンプトが表示されたら、[インポートの解決（Import Resolution）] ページで、各設定を展開して適切なオプションを選択します。詳細については、インポート競合の解決 （627 ページ）を参照してください。

ステップ 8 [インポート（Import）] をクリックします。

ステップ 9 すべてのフィードを更新します。

たとえば、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [セキュリティ インテリジェンス（Security Intelligence）] に移動し、[URL]、[ネットワーク（Network）]、および [DNS リストとフィード（DNS Lists and Feeds）] ページにある [フィードの更新（Update Feed）] ボタンをクリックします。

インポートされたポリシーには、フィードコンテンツは含まれていません。

ステップ 10 ポリシーをデバイスに展開する前に、すべてのフィードの更新が完了するのを待ってください。

次のタスク

（注） Microsoft Active Directory のユーザーとグループを含む設定をインポートした場合は、インポート後にすべてのユーザーとグループをダウンロードして、復号ポリシー、アクセス コントロール ポリシー、および場合によっては他のポリシーの問題を回避することを強くお勧めします（**[統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）]**、（今すぐダウンロード）の順にクリックします）。

- 必要に応じて、インポートした設定の概要を示すレポートを表示します。タスク メッセージの表示 （529 ページ）を参照してください。

インポート競合の解決

構成をインポートしようとすると、同じ名前とタイプの構成がアプライアンスにすでに存在するかどうかがシステムによって確認されます。インポートに重複構成が含まれている場合、次の中から展開に適切な解決オプションが表示されます。

- **既存のものを維持する（Keep existing）**

  その構成はインポートされません。

- **既存のものを置換する（Replace existing）**

  インポート用に選択した構成で現在の構成が上書きされます。

- **最新バージョンを残す（Keep newest）**

  選択した構成は、タイムスタンプがアプライアンスの現在の構成のタイムスタンプより新しい場合にのみインポートされます。

（注） Microsoft Active Directory のユーザーとグループを含む設定をインポートした場合は、インポート後にすべてのユーザーとグループをダウンロードして、復号ポリシー、アクセス コントロール ポリシー、および場合によっては他のポリシーの問題を回避することを強くお勧めします（**[統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）]**、（今すぐダウンロード）の順にクリックします）。

- **新たにインポート（Import as new）**

  選択した重複する構成はインポートされ、システム生成の番号が適用されて一意の構成になります。（インポートプロセスが完了する前にこの名前を変更できます）。アプライアンスの元の構成は変更されません。

表示される解決オプションは、展開でドメインを使用するかどうか、およびインポートされた構成が現在のドメインで定義されている構成の複製であるか、または現在のドメインの先祖あるいは子孫で定義された構成であるかどうかによって異なります。次の表に、どの場合に解決オプションが表示されるか表示されないかを示します。

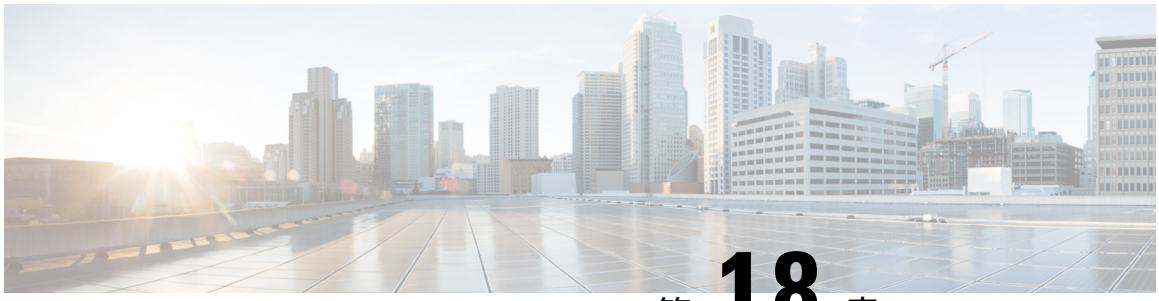
解決オプション	Secure Firewall Management Center		管理対象デバイス
	現在のドメインの複製	子孫または先祖ドメインの複製	
既存のものを維持する（Keep existing）	対応	対応	対応
既存のものを置換する（Replace existing）	対応	×	対応

解決オプション	Secure Firewall Management Center		管理対象デバイス
	現在のドメインの複製	子孫または先祖ドメインの複製	
最新バージョンを残す（**Keep newest**）	対応	×	対応
新たにインポート（**Import as new**）	対応	対応	対応

クリーンまたはカスタム定義ファイル リストを使用するファイル ポリシーとともにアクセス コントロール ポリシーをインポートし、ファイル リストに重複する名前競合が示されている場合、上記の表に示すように競合解決オプションが表示されますが、ポリシーおよびファイル リストに対して実行されるアクションは、次に表に示すように異なります。

解決オプション	システム アクション	
	アクセス コントロール ポリシーと関連ファイル ポリシーが新たにインポートされ、ファイル リストは統合される	既存のアクセスコントロールポリシーと関連ファイルポリシーおよびファイル リストは変更されない
既存のものを維持する（**Keep existing**）	×	対応
既存のものを置換する（**Replace existing**）	対応	×
新たにインポート（**Import as new**）	対応	×
最新バージョンを残す（Keep newest）。インポートされるアクセス コントロール ポリシーが最新	対応	×
最新バージョンを残す（Keep newest）。既存のアクセス コントロール ポリシーが最新	×	対応

アプライアンスにインポートされた構成を修正し、後で同じアプライアンスにその構成を再インポートする場合は、保持する構成のバージョンを選択する必要があります。



第 18 章

データの消去とストレージ

Management Center に保存されるデータ

対象	参照先
Management Center のデータストレージに関する一般情報	[ディスク使用量（Disk Usage）] ウィジェット（415 ページ）
古いデータの消去	Management Center データベースからのデータの消去 （630 ページ）
Management Center 上のデータへの外部アクセス許可（高度な機能）	外部データベース アクセス （70 ページ）
バックアップ	バックアップとリモートストレージの管理（590 ページ） およびサブトピック
レポート	ローカル ストレージの設定 （112 ページ）
イベント	接続ロギング （879 ページ） データベース （65 ページ） およびサブトピック
ネットワーク検出データ	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Network Discovery Data Storage Settings*」およびそれ以降のトピック

対象	参照先
ファイル（Files）	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Network Malware Protection and File Policies*」の章にあるファイルの保存に関する情報（ベストプラクティスを含む）。 Cisco Secure Firewall Management Center デバイス構成ガイドの「*Tuning File and Malware Inspection Performance and Storage*」
パケット データ	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Edit General Settings*」
ユーザーおよびユーザーアクティビティ	Cisco Secure Firewall Management Center デバイス構成ガイドの「*The Users Database*」 Cisco Secure Firewall Management Center デバイス構成ガイドの「*The User Activity Database*」

Management Center データベースからのデータの消去

データベース消去ページを使用すると、検出、アイデンティティ、接続、およびセキュリティインテリジェンスのデータ ファイルを Management Center データベースから消去できます。データベースを消去すると、該当するプロセスが再起動される点に注意してください。

⚠

注意 データベースを消去すると、Management Center から指定したデータが削除されます。削除されたデータは復元できません。

始める前に

データを消去するには、管理者権限またはセキュリティアナリスト権限が必要です。グローバルドメインでのみ可能です。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[データの削除（Data Purge）]**を選択します。

ステップ 2 [Discovery and Identity] の下で、次のいずれかまたはすべてを実行します。

- [ネットワーク検出イベント（Network Discovery Events）]チェックボックスをオンにして、データベースからすべてのネットワーク検出イベントを削除します。
- [ホスト（Hosts）]チェックボックスをオンにして、データベースからすべてのホストとホストの侵害の兆候フラグを削除します。

- [ユーザ アクティビティ（User Activity）] チェックボックスをオンにして、データベースからすべてのユーザ アクティビティ イベントを削除します。
- [ユーザ アイデンティティ（User Identities）] チェックボックスをオンにして、データベースからすべてのユーザ ログインとユーザ履歴データ、およびユーザの侵害の兆候フラグを削除します。

（注） Microsoft Azure AD レルムのユーザー アクティビティ イベント、ユーザーログイン、およびユーザー履歴データは削除「されません」。

ステップ 3 [接続（Connections）] で、次のいずれかまたはすべてを実行します。

- [接続イベント（Connection Events）] チェックボックスをオンにして、データベースからすべての接続データを削除します。
- [接続の概要イベント（Connection Summary Events）] チェックボックスをオンにして、データベースからすべての接続の概要データを削除します。
- [セキュリティ インテリジェンス イベント（Security Intelligence Events）] チェックボックスをオンにして、データベースからすべてのセキュリティ インテリジェンス データを削除します。

（注） [接続イベント（Connection Events）] チェックボックスをオンにしても、セキュリティ インテリジェンス イベントは削除されません。セキュリティ インテリジェンス データとの接続は、[セキュリティ インテリジェンス イベント（Security Intelligence Events）] ページに引き続き表示されます（[分析（Analysis）]>[接続（Connections）] メニューの下に表示）。同様に、[セキュリティ インテリジェンス イベント（Security Intelligence Events）] チェックボックスをオンにしても、セキュリティ インテリジェンス データに関連する接続イベントは削除されません。

ステップ 4 [選択したイベントの消去（Purge Selected Events）] をクリックします。
項目が消去され、該当するプロセスが再起動されます。

外部データストレージ

オプションで、特定のタイプのデータを保存するためにリモートデータストレージを使用できます。

対象	参照先
バックアップ	バックアップとリモートストレージの管理 （590 ページ） およびサブトピック リモート ストレージ デバイス （111 ページ） およびサブトピック

対象	参照先
レポート	リモート ストレージ デバイス （111 ページ） およびサブトピック リモート ストレージへのレポートの移動 （669 ページ）
イベント	外部ツールを使用したイベントの分析 （753 ページ） の syslog およびその他のリソースに関する情報 Cisco Secure Cloud Analytics でのリモートデータストレージ （633 ページ） Secure Network Analytics アプライアンスでのリモートデータストレージ （633 ページ） 接続イベントをリモートで保存する場合は、Management Center での接続イベントの保存を無効にすることを検討してください。詳細については、データベース （65 ページ） およびサブトピックを参照してください。

重要 syslog またはストアイベントを外部で使用する場合は、ポリシー名やルール名などのオブジェクト名に特殊文字を使用しないでください。オブジェクト名には、カンマなどの特殊文字を含めることはできません。受信側アプリケーションで区切り文字として使用される可能性があります。

セキュリティ分析とロギング リモート イベント ストレージ オプションの比較

イベントデータを Management Center の外部に保存するための類似しているが異なるオプション：

オンプレミス	SaaS
ファイアウォールの背後に設置するストレージシステムを購入し、ライセンスを取得してセットアップします。	ライセンスとデータストレージプランを購入し、データをシスコのクラウドに送信します。
サポートされるイベントタイプ： • 接続 • セキュリティインテリジェンス • 侵入 • ファイルおよびマルウェア • LINA	サポートされるイベントタイプ： • 接続 • セキュリティインテリジェンス • 侵入 • ファイルおよびマルウェア
syslog と直接統合の両方をサポートします。	syslog と直接統合の両方をサポートします。

オンプレミス	SaaS
• Secure Network Analytics Manager ですべてのイベントを表示します。 • FMC イベントビューアから相互起動して、Secure Network Analytics Manager でイベントを表示します。 • FMC でリモートに保存された接続およびセキュリティインテリジェンスイベントを表示します。	ライセンスに応じて CDO または Secure Network Analytics で、イベントを表示します。FMC イベントビューアから相互起動します。
詳細については、Secure Network Analytics アプライアンスでのリモートデータストレージ（633ページ）のリンクを参照してください。	詳細については、Cisco Secure Cloud Analytics でのリモートデータストレージ（633ページ）のリンクを参照してください。

Cisco Secure Cloud Analytics でのリモートデータストレージ

シスコのセキュリティ分析とロギング（SaaS） を使用して、選択した Firepower イベントデータを Secure Cloud Analytics に送信します。サポートされているイベント：接続、セキュリティインテリジェンス、侵入、ファイル、およびマルウェア。

詳細については、https://cisco.com/go/firepower-sal-saas-integration-docs にある『Firepower Management Center and Cisco Security Analytics and Logging (SaaS) Integration Guide』を参照してください。

イベントは直接送信するか、syslog 経由で送信することができます。

重要 syslog またはストアイベントを外部で使用する場合は、ポリシー名やルール名などのオブジェクト名に特殊文字を使用しないでください。オブジェクト名には、カンマなどの特殊文字を含めることはできません。受信側アプリケーションで区切り文字として使用される可能性があります。

Secure Network Analytics アプライアンスでのリモートデータストレージ

Firepowerアプライアンスが提供できる以上のデータストレージが必要な場合は、セキュリティ分析とロギング（オンプレミス） を使用してSecure Network Analyticsアプライアンスに Firepowerデータを保存することができます。詳細については、https://cisco.com/go/sal-on-prem-docs のマニュアルを参照してください。

接続イベントがSecure Network Analyticsアプライアンスに保存されている場合でも、Management Center で接続イベントを確認できます。Secure Network Analytics アプライアンスに保存されて

いる接続イベントを使用した Secure Firewall Management Center での作業 （819 ページ）を参照してください。

重要 syslog またはストアイベントを外部で使用する場合は、ポリシー名やルール名などのオブジェクト名に特殊文字を使用しないでください。オブジェクト名には、カンマなどの特殊文字を含めることはできません。受信側アプリケーションで区切り文字として使用される可能性があります。

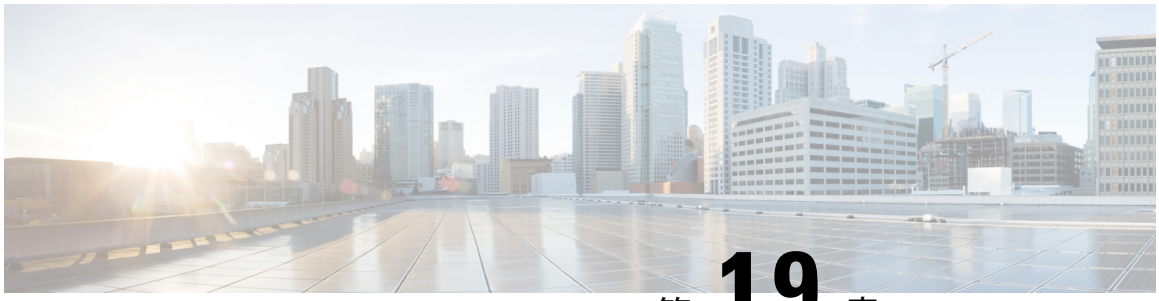
データストレージの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
イベントレート制限から優先順位の低い接続イベントを除外する	7.0	任意（Any）	接続イベントをリモートボリュームに保存しているために Management Center に接続イベントを保存しない場合、それらのイベントは Management Center ハードウェアデバイスのフローレート制限にカウントされません。 新しい 7.0 構成を使用して セキュリティ分析とロギング（オンプレミス）にイベントを送信する場合は、その統合の一環としてこの設定を構成します。 それ以外の場合は、データベース イベント数の制限 （66 ページ）の接続データベースに関する情報を参照してください。 新規/変更されたページ：なし。動作の変更のみ。

機能	最小 Management Center	最小 Threat Defense	詳細
Secure Network Analytics アプライアンスにイベントを送信するプロセスの改善	7.0	任意（Any）	新しいウィザードにより、セキュリティ分析とロギング（オンプレミス）を使用した Secure Network Analytics アプライアンスへのイベントの直接送信が合理化されます。 このウィザードでは、Management Center でイベントページを表示しながらリモートで保存された接続イベントを表示したり、Management Center から相互起動して Secure Network Analytics アプライアンスでイベントを表示したりもできます。 syslog を使用してイベントを送信するようにシステムをすでに設定している場合、その設定を無効にしない限り、syslog を使用してイベントが送信され続けます。 詳細については、Secure Network Analytics アプライアンスでのリモートデータストレージ（633 ページ）で参照されているマニュアルを参照してください。 新規/変更されたページ：[システム（System）]>[ロギング（Logging）]>[セキュリティ分析とロギング（Security Analytics & Logging）] ページに、相互起動オプションを作成するための設定ではなく、ウィザードが表示されるようになりました。
Secure Network Analytics アプライアンスでのリモートデータストレージ	6.7	任意（Any）	セキュリティ分析とロギング（オンプレミス）を使用して、大量の Firepower イベントデータをリモートで保存できるようになりました。Management Center でイベントを表示する場合、リモートデータストレージの場所にあるイベントをすばやく相互起動して表示できます。 サポートされているイベント：接続、セキュリティ インテリジェンス、侵入、ファイル、およびマルウェア。イベントは、syslog を使用して送信されます。 このソリューションは、Stealthwatch Enterprise（SWE）バージョン 7.3 を実行している Stealthwatch Management Console（SMC）バーチャルエディションの可用性に依存します。 Secure Network Analytics アプライアンスでのリモートデータストレージ（633 ページ）を参照してください。
Cisco Secure Cloud Analytics でのリモートデータストレージ	6.4	任意（Any）	syslog を使用して、選択した Firepower データを シスコのセキュリティ分析とロギング（SaaS）を使用して送信します。サポートされているイベント：接続、セキュリティ インテリジェンス、侵入、ファイル、およびマルウェア。 詳細については、https://cisco.com/go/firepower-sal-saas-integration-docs にある『Firepower Management Center and Cisco Security Analytics and Logging (SaaS) Integration Guide』を参照してください。

第 V 部

レポートとアラート



第 19 章

レポート

以下のトピックでは、レポートを操作する方法について説明します。

レポートの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- メンテナンス ユーザー（リスク レポートのみ）
- セキュリティ アナリスト（Security Analyst）

レポートの概要

システムは、次の 2 つのタイプのレポートを提供します。

- リスク レポート （640 ページ） - ネットワーク上で検出されたリスクの高レベル サマリ。

- 標準レポートの概要 （641 ページ） - システムのあらゆる側面に関する詳細でカスタマイズ可能なレポート。

リスク レポート

リスク レポートは、組織で検出されたリスクの概要を理解しやすい形で示す、移植可能なサマリーです。これらのレポートを使用することで、システムへのアクセス権がない人々や、ネットワーク セキュリティのエキスパートではない人々とも、リスク領域に関する情報やそれらのリスクに対処するための推奨案を共有できます。これらのレポートは、ネットワーク セキュリティへの投資領域に関する話し合いを促進することを目的としています。

リスクレポートテンプレート

- **高度なマルウェアリスクレポート**
- **攻撃リスクレポート**。このレポートのフィールドは次のとおりです。
  - [攻撃の総数（Total Attacks）]：IPS イベントの総数。
  - [関連の攻撃（Relevant Attacks）]：影響フラグが 1 の IPS イベントの数。
  - [ターゲットホスト（Hosts Targeted）]：影響フラグが 1 の IPS イベントからの一意の宛先 IP アドレスの数。
  - [無関係の攻撃（Irrelevant Attacks）]：影響フラグが 1 ではない IPS イベントのパーセンテージ。
  - [注意が必要なイベント（Events Requiring Attention）]：影響フラグが 1 の IPS イベントのパーセンテージ。
  - [CnCサーバーに接続されているホスト（Hosts Connected to CnC Servers）]：IOC カテゴリが [CnC接続済み（CnC Connected）] の一意のホストの総数。
- **ネットワークリスクレポート**

リスク レポートの生成、表示および印刷

標準レポートのテンプレートは、リスク レポートには適用されません。

レポートは現在のドメインに関するものになります。

各リスク レポートは、HTML ファイルとして生成されます。

リスク レポートの生成をスケジュールするには、レポートの生成の自動化（606ページ）を参照してください。

始める前に

- 概要を取得するリスクを検出するように、システムが設定されていることを確認します。
- レポートを電子メールで送信しようとしていて、まだリレーホストを設定していない場合は、ここで設定できます。詳細については、メール リレー ホストおよび通知アドレスの設定 （69 ページ）を参照してください。

手順

ステップ 1 **[概要（Overview）]** > **[レポート（Reporting）]**を選択します。

ステップ 2 [レポートテンプレート（Report Templates）] をクリックします。

ステップ 3 目的のレポートの [レポートの生成（Generate Report）] をクリックします。

ステップ 4 情報を入力します。

- [入力パラメータ（Input Parameters）] セクションに入力した情報は、レポートのタイトルページに表示されます。これらのフィールドは、空のままでもかまいません。

ステップ 5 [生成（Generate）] をクリックします。

ステップ 6 [OK] をクリックします。

次のタスク

- リスク レポートを表示、ダウロード、移動、または削除するには、生成されたレポートの操作について （667 ページ）を参照してください。
- ほとんどのサポート対象ブラウザから、リスク レポートを PDF に出力できます。最適な結果を得るために、ブラウザの印刷または印刷プレビューの設定で、背景色、画像、およびオプションでヘッダーとフッターを有効にします。サポートされるページ サイズは、A4 および US Letter です。

標準レポートの概要

システムは柔軟なレポート作成システムを提供しており、Management Center で表示されるイベントビューやダッシュボードを使用して、複数のセクションがあるレポートを短時間で簡単に生成できます。独自のカスタム レポートを最初から設計することもできます。

レポートは、通信しようとしている内容が含まれるドキュメントファイルで、PDF、HTML、または CSV 形式になります。レポート テンプレートは、データの検索設定とレポートおよびそのセクションの形式を指定します。システムには強力なレポートデザイナが含まれていて、レポートテンプレートの設計を自動的に行います。Web インターフェイスに表示されるイベント ビュー テーブルやダッシュボードのグラフィックの内容を複製できます。

レポート テンプレートは必要な数だけ作成できます。各レポート テンプレートは、レポートの個々のセクションを定義し、レポートの内容を作成するデータベース検索設定を指定し、表示形式（表、グラフ、詳細表示など）とタイムフレームも指定します。さらに、テンプレートでは、表紙や目次の情報、ドキュメントページに見出しとフッターを付けるかどうかなどのドキュメント属性も指定します（PDF 形式のレポートでのみ指定可能）。レポート テンプレートを 1 つの設定パッケージ ファイルとしてエクスポートし、別の Management Center にインポートして再使用できます。

テンプレートに入力パラメータを組み込んで実用性を向上させることができます。入力パラメータを使用すると、同じレポートを用途に合わせて異なるさまざまなレポートに変えることができます。入力パラメータのあるレポートを生成するときには、生成プロセスで各入力パラメータの値を入力するよう求められます。ユーザが入力する値は、レポートの内容をその1回だけ決定するものです。たとえば、侵入イベントのレポートを作成する検索の宛先 IP フィールドに入力パラメータを使用できます。この場合、レポートの生成時に、宛先 IP アドレスの入力を求められたときに特定の部門のネットワークセグメントを指定できます。その結果、この特定の部門に関する情報だけが含まれるレポートが生成されます。

レポートの設計について

レポート テンプレート

レポート テンプレートを使用して、レポートの各セクション内のデータの内容と形式や、レポート ファイルのドキュメント属性（表紙、目次、ページ ヘッダー、ページ フッター）を定義します。レポートの生成後、削除しない限りテンプレートは再利用可能な状態になります。

レポートには、1 つ以上の情報セクションが含まれます。個々のセクションごとに形式（テキスト、表、またはグラフ）を選択します。セクションの形式の選択内容によっては、組み込めるデータが制約される場合があります。たとえば、円グラフの形式を使用すると、特定の表に時間ベースの情報を表示できません。いつでもセクションのデータの基準や形式を変更して、表示を最適にすることができます。

定義済みイベント ビューのレポートの初期設計をベースにするか、定義済みのダッシュボード、ワークフロー、または要約から内容をインポートして設計を開始できます。空のテンプレート シェルから始めて、1つずつセクションを追加したり属性を定義したりすることもできます。

（注） マルチドメイン導入では、先祖ドメインに属するレポートテンプレートを表示することはできますが、編集することはできません。これらのテンプレートからレポートを生成するには、テンプレートを現在のドメインにコピーする必要があります。

レポート テンプレート フィールド

次の表では、レポートテンプレートにセクションを作成するために使用できるフィールドについて説明します。すべてのフィールドが、すべてのタイプのセクションで使用されるわけでは

ありません。セクションフォーマットを選択すると、システムにより適切なフィールドが表示されます。

フィールド名	セクションタイプ	定義
フォーマット（Format）	適用対象外	セクション データのフォーマットを選択します。 [棒グラフ（Bar Char）]（）：選択した変数の数量を比較します。 [折れ線グラフ（Line chart）]（）：選択した変数の、時間の経過に伴う傾向/変化を示します。時間ベースのテーブルにのみ使用できます。 [円グラフ（Pie chart）]（）：選択した各変数を全体の割合として示します。数量がゼロの変数はグラフからドロップされます。ごくわずかな数量は、[その他（Other）] というラベルのカテゴリに集められます。 [テーブル表示（Table view）]（）：レコードごとの属性の値を示します。要約や統計のデータには使用できません。 [詳細ビュー（Detail view）]（）：パケット（侵入イベントの場合）やホストプロファイル（ホストイベントの場合）など、特定のイベントに関連付けられた複合オブジェクトのデータを示します。このフォーマットは、この種のオブジェクトが関係する特定のイベントタイプだけに使用できます。出力が多数要求されている場合には、パフォーマンスが低下することがあります。
テーブル	すべて（All）	セクション データが抽出されるテーブルを選択します。
プリセット（Preset）	すべて（All）	定義済みの検索。新しい検索設定を定義する際に、該当するプリセットを選択して、検索条件を初期化します。
検索またはフィルタ（Search or Filter）	すべて（All）	ほとんどのテーブルの場合、定義済みまたは保存済みの [検索（Search）] を使用してレポートを制約できます。**[編集（Edit）]**（）をクリックして新しい検索を作成することもできます。 アプリケーション統計表では、ユーザー定義のアプリケーションの [フィルタ（Filter）] を使用して、レポートを制約できます。
X 軸（X-Axis）	棒グラフ 折れ線グラフ 円グラフ	選択したグラフの X 軸に利用可能なデータ。 折れ線グラフの場合、X 軸の値は常に [時刻（Time）] です。棒グラフと円グラフの場合、X 軸の値として [時刻（Time）] を選択できません。
Y 軸（Y-Axis）	棒グラフ 折れ線グラフ 円グラフ	選択したグラフの Y 軸に利用可能なデータ。

フィールド名	セクションタイプ	定義
セクションの説明（Section Description）	すべて（All）	セクション内で検索データの前にある説明テキスト。 テキストと入力パラメータの組み合わせを入力します。新しいセクションのデフォルトは `$<Time Window>` と `$<Constraints>` です。
時間枠（Time Window）	すべて（All）	セクションに表示されるデータの時間枠。 セクションで時間ベースのテーブルを検索する場合、チェックボックスを選択して、レポートのグローバル時間枠を継承できます。または、セクションの特定の時間枠を設定することもできます。
データ ソース	すべて（All）	セキュリティ分析とロギング（オンプレミス）を使用してリモート（外部）データストレージを設定するためにウィザードを使用した場合は、接続およびセキュリティ インテリジェンス イベントに使用するデータソースを選択できます。 次のオプションがあります。 • [自動（Auto）]：Management Center に保存されているデータが利用可能な場合は、これらのデータを表示します。選択した時間枠全体で Management Center のデータを使用できない場合は、リモートに保存されたデータのみを表示します。 • [ローカル（Local）]：選択した時間枠に関係なく、Management Center に保存されているデータのみを表示します。 リモートボリュームにイベントを送信するように設定されていないデバイスから生成されたイベントなど、リモートボリュームに存在しないデータを含めるには、このオプションを選択します。 • [Extended]：リモートボリュームに保存されているデータのみを表示します。
最大結果数（Maximum Results）	テーブル ビュー 詳細ビュー	含める一致するレコードの最大数。 PDF レポートには、CSV または HTML レポートよりも少ないレコードを含めることができます。数が大きすぎる場合、Web インターフェイスでは警告およびエラーのアイコンが使用されて、そのことが示されます。ポインタをアイコンの上に移動させると、制限が表示されます。
結果（Results）	棒グラフ 円グラフ	[上（Top）] または [下（Bottom）] を選択し、チャートを作成するために使用する一致するレコードの数を入力します。
カラー（Color）	棒グラフ 折れ線グラフ	セクション内でグラフ化されるデータの色。

レポート テンプレートの作成

レポート テンプレートは、独自のデータベース クエリから個別に構築されたセクションのフレームワークです。

新しいレポートテンプレートを作成するには、新しいテンプレートを作成する、既存のテンプレートを使用する、イベント ビューをテンプレートのベースにする、ダッシュボードまたはワークフローをインポートするという方法があります。

既存のレポートテンプレートをコピーしない場合は、まったく新しいテンプレートを作成できます。テンプレート作成の最初の手順として、セクションを追加したり形式設定したりできるフレームワーク シェルを生成します。次に、ご希望の順序で、個々のテンプレート セクションを設計し、レポート ドキュメントの属性を設定します。

各テンプレートセクションは、検索設定やフィルタによって生成されたデータセットで構成され、表示モードを確定する形式の仕様（表や円グラフなど）があります。出力に含めるデータレコードのフィールドを選択し、タイムフレームと表示するレコード数も選択して、さらにセクションの内容を確定します。

（注） セクション プレビュー ユーティリティを使用して、カラムの選択内容や、円グラフの色などの出力の特性を検査します。このインジケータは、設定済みの検索設定を必ずしも正確に反映するとは限りません。

テンプレートから生成したレポートには、表紙、ヘッダーとフッター、ページ番号など、すべてのセクションにまたがって機能を制御する複数のドキュメント属性があります。

CSVをドキュメントの形式として選択した場合は、ドキュメントの属性を設定できないことに注意してください。

既存のテンプレートの中に適切なモデルがあれば、そのテンプレートをコピーして属性を編集することで、新しいレポート テンプレートを作成できます。また、Cisco から一連の定義済みレポートテンプレートも提供されています。これらのテンプレートは、[レポート（Reports）] タブのテンプレートの一覧で確認できます。

イベントビューからレポートテンプレートを作成し、必要に応じて変更することができます。セクションを追加したり、自動的に組み込まれるセクションを変更したり、セクションを削除したりできます。

ダッシュボード、ワークフロー、統計の要約をインポートして、新しいレポートをすばやく作成できます。インポートすると、ダッシュボードのウィジェット グラフィックごと、およびワークフローのイベントビューごとにセクションが作成されます。最も重要な情報に焦点が当たるように不要なセクションを削除できます。

カスタム レポート テンプレートの作成

手順

ステップ 1 **[概要（Overview）] > [レポート（Reporting）]**を選択します。

ステップ 2 [レポートテンプレート（Report Templates）] をクリックします。

ステップ 3 [レポート テンプレートの作成（Create Report Template）] をクリックします。

ステップ 4 [レポートタイトル（Report Title）] フィールドに、新しいテンプレートの名前を入力します。

ステップ 5 レポートタイトルに入力パラメータを追加するには、タイトル内でパラメータ値を表示する位置にカーソルを置き、挿入[入力パラメータ（Input Parameter）]（＋）をクリックします。

ステップ 6 必要に応じて、[レポートセクション（Report Sections）] タイトルバーの下にある追加のセットを使用し、セクションを挿入します。

ステップ 7 レポートテンプレートの設定（649ページ）の説明に従ってセクション コンテンツを設定します。

ヒント セクションのウィンドウの下部にある [プレビュー（Preview）] をクリックして、選択したカラムのレイアウトやグラフィックの形式を表示できます。

ステップ 8 [詳細（Advanced）] をクリックし、レポート テンプレート内のドキュメント属性（658 ページ）の説明に従って PDF および HTML レポートの属性を設定します。

ステップ 9 [保存（Save）] をクリックします。

エラーが表示された場合は、各セクションの結果値の横にある黄色の三角形を探します。このような三角形が見つかった場合は、次のいずれかの操作を行います。

- 黄色の三角形が表示されたフィールドごとに、三角形をマウス オーバーして、結果の数を表示された数まで削減します。
- [生成（Generate）] をクリックして、PDF 以外の出力形式を含めます。

既存のテンプレートからのレポート テンプレートの作成

手順

ステップ 1 **[概要（Overview）] > [レポート（Reporting）]**を選択します。

ステップ 2 [レポートテンプレート（Report Templates）] をクリックします。

ステップ 3 コピーするレポートテンプレートの横にある[コピー（Copy）]（）をクリックします。

ステップ 4 [レポート タイトル（Report Title）] フィールドに、名前を入力します。

ステップ 5 必要に応じてテンプレートを変更します。

ステップ 6 [保存（Save）] をクリックします。

イベント ビューからのレポート テンプレートの作成

手順

ステップ 1 レポートに含めるイベントをイベント ビューに入力します。

- イベント検索設定を使用して、表示するイベントを定義します。
- イベント ビューに該当するイベントが表示されるまでワークフローをドリルダウンします。

ステップ 2 イベント ビューのページから、[レポート デザイナ（Report Designer）] をクリックします。

[レポート セクション（Report Sections）] ページが表示され、キャプチャされるワークフロー内のビューごとにセクションが示されます。

ステップ 3 オプションで、[レポート タイトル（Report Title）] フィールドに新しい名前を入力し、[保存（Save）] をクリックします。

ステップ 4 次の操作を実行できます。

- 表紙、目次、開始ページ番号、またはヘッダーおよびフッターテキストを追加します：[詳細（Advanced）] 設定をクリックします。
- 改ページを追加します：[改ページの追加（Add Page Break）]（）をクリックし、新しい改ページオブジェクトを、テンプレートの下部から新しいページを開始するセクションの先頭にドラッグします。
- テキストセクションを追加します：[テキストセクション追加（Add Text Section）]（）をクリックし、新しいテキストセクションを、テンプレートの下部からレポートテンプレート内で表示する位置にドラッグします。
- セクションのタイトルを変更します：タイトルバーでセクション タイトルをクリックし、セクション タイトルを入力して、[OK] をクリックします。
- レポート セクションを設定します。各セクションのフィールド設定を調整します。

  ヒント セクションの現在のカラムのレイアウトやグラフの形式を表示する場合は、そのセクションの [プレビュー（Preview）] リンクをクリックします。

- レポートからテンプレートセクションを除外します：セクションのタイトルバーで[削除（Delete）]（  ）をクリックし、削除を確認します。

  （注） 一部のワークフロー内の最後のレポートセクションには詳細ビューが含まれ、ワークフローに応じてパケット、ホストプロファイル、または脆弱性が示されます。レポートの生成時に、これらの詳細ビューがあるイベントを多数取得すると、Management Center のパフォーマンスに影響を与えることがあります。

ステップ 5 [保存（Save）] をクリックします。

ダッシュボードまたはワークフローのインポートによるレポート テンプレートの作成

手順

ステップ 1 レポート内で複製するダッシュボード、ワークフロー、または要約を識別します。

ステップ 2 **[概要（Overview）] > [レポート（Reporting）]**を選択します。

ステップ 3 [レポートテンプレート（Report Templates）] をクリックします。

ステップ 4 [レポート テンプレートの作成（Create Report Template）] をクリックします。

ステップ 5 [レポート タイトル（Report Title）] フィールドに新しいレポート テンプレートの名前を入力します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 **インポートセクション**（） をクリックします。[インポート レポート セクション（Import Report Sections）] のデータ ソース オプション （648 ページ）で説明されているデータ ソースのいずれかを選択できます。

ステップ 8 ドロップダウン メニューからダッシュボード、ワークフロー、または要約を選択します。

ステップ 9 追加するデータ ソースの、[インポート（Import）] をクリックします。

ダッシュボードの場合、ウィジェット グラフィックごとに独自のセクションがあります。ワークフローの場合、イベント ビューごとに独自のセクションがあります。

ステップ 10 必要に応じてセクションの内容を変更します。

（注） 一部のワークフロー内の最後のレポートセクションには詳細ビューが含まれ、ワークフローに応じてパケット、ホストプロファイル、または脆弱性が示されます。レポートの生成時に、これらの詳細ビューがあるイベントを多数取得すると、Management Center のパフォーマンスに影響を与えることがあります。

ステップ 11 [保存（Save）] をクリックします。

[インポート レポート セクション（Import Report Sections）] のデータ ソース オプション

表 *54 : [インポート レポート セクション（Import Report Sections）]* ウィンドウのデータ ソース オプション

選択オプション	インポート対象
ダッシュボードのインポート（Import Dashboard）	選択したダッシュボード上のカスタム分析ウィジェット。

選択オプション	インポート対象
ワークフローのインポート（Import Workflow）	定義済みのワークフローまたはカスタム ワークフロー。 選択項目の形式は次のようになっています。 `Table - Workflow name` たとえば、`Connection Events - Traffic by Port` は、Connection Events テーブルから生成された Traffic by Port ワークフロー内のビューをインポートします。
Import Summary Sections	次の一般的な要約： • 侵入の詳細サマリー（Intrusion Detailed Summary） • 侵入の概要サマリー（Intrusion Short Summary） • ディスカバリの詳細サマリー（Discovery Detailed Summary） • ディスカバリの概要サマリー（Discovery Short Summary）

レポート テンプレートの設定

レポートテンプレートを作成すれば、そのテンプレートを変更およびカスタマイズできます。さまざまなレポートセクションの属性を変更して、セクションとそのデータ表示の内容を調整できます。

レポート テンプレート内の各セクションでは、データベース テーブルを照会して、そのセクションの内容を生成します。セクションのデータ形式を変更する際にも同じデータ クエリーが使用されますが、形式のタイプごとの分析の目的に従って、セクションに表示されるフィールドが変わります。たとえば、侵入イベントの表形式の表示では、イベント レコードごとに多数のデータ フィールドがセクションに入力され、円グラフのセクションでは、選択した各属性が表すすべての一致レコードの割合が示され、個々のイベントに関する詳細情報は表示されません。棒グラフのセクションでは、特定の属性を持つ一致レコードの合計数が比較されます。折れ線グラフでは、1 つの属性に関係する一致レコード数の変化が時系列で要約されます。折れ線グラフは時間ベースのデータの場合のみ使用でき、ホスト、ユーザ、サードパーティの脆弱性などに関する情報の場合は使用できません。

レポートセクションの検索設定やフィルタは、セクションの内容のベースになるデータベース クエリーを指定します。ほとんどのテーブルの場合、定義済み検索設定か保存済み検索設定を使用してレポートを制約するか、新しい検索設定を即座に作成することができます。

- 定義済み検索設定は特定のイベントテーブルの検索サンプルの役割を果たし、レポートに含めようとしている、ネットワークに関する重要情報にクイック アクセスできます。
- 保存済みイベント検索設定には、自分や他のユーザが作成したすべてのパブリック イベント検索設定と、自分で保存したすべてのプライベート イベント検索設定が含まれます。
- 現在のレポート テンプレートの保存済み検索設定は、そのレポート テンプレート自体に限りアクセスできます。保存済みレポートテンプレートの検索設定の名前は、末尾が文字

列「Custom Search」になります。ユーザは、レポートの設計時にこれらの検索設定を作成します。

[アプリケーションの統計（Application Statistics）] テーブルにユーザ定義のアプリケーションフィルタを使用して、レポートに制約を適用します。

セクション内にテーブルのデータを組み込む場合、データ レコード内のどのフィールドを表示するか選択できます。テーブル内のすべてのフィールドを包含対象または除外対象にできます。レポートの目的を達成するのに必要なフィールドを選択し、それに従って配列したりソートしたりします。

テンプレートにテキストセクションを追加して、レポート全体や個々のセクションに概要などのカスタム テキストを用意することができます。

テンプレート内のどのセクションの前後にも改ページを追加できます。この機能は、複数のセクションから成るレポートで、各種セクションの概要を示すテキストページがある場合に特に便利です。

レポートテンプレートの時間枠によって、テンプレートのレポート作成期間が定義されます。

（注） セキュリティ アナリストは、自分が作成したレポート テンプレートだけを編集できます。マルチドメイン導入では、先祖ドメインのレポートテンプレートは編集できませんが、レポートテンプレートをコピーして子孫バージョンを作成することができます。

レポート テンプレート セクションのテーブルとデータ形式の設定

手順

ステップ 1 **[概要（Overview）]**>**[レポート（Reporting）]**>**[レポートテンプレート（Report Templates）]**>**[レポートテンプレートの作成（Create Report Template）]** をクリックします。

ステップ 2 [レポート テンプレート（Rreport Template）] セクションで、[テーブル（Table）] ドロップダウン メニューを使用して、問い合わせるテーブルを選択します。

[形式（Format）] フィールドでは、選択したテーブルで使用できる各出力形式が示されます。

ステップ 3 セクションに該当する出力形式を選択します。

ステップ 4 検索設定の制約を変更するには、[セクションの説明（Section description）] フィールドか[フィルタ（Filter）] フィールドの横にある**[編集（Edit）]**（）をクリックします。

ステップ 5 グラフ出力形式（円グラフや棒グラフなど）の場合、ドロップダウンメニューを使用して、[X 軸（X-Axis）] と [Y 軸（Y-Axis）] のパラメータを調整します。

X 軸の値を選択すると、互換性のある値だけが Y 軸のドロップダウンメニューに表示されます。その逆も同様です。

ステップ 6 テーブル出力の場合、出力内のカラム、表示順序、ソート順序を選択します。

ステップ 7 [保存（Save）] をクリックします。

関連トピック

レポート テンプレート フィールド （642 ページ）

レポート テンプレート セクションの検索またはフィルタの指定

手順

ステップ 1 [レポート テンプレート（Rreport Template）] セクションで、[テーブル（Table）] ドロップダウン メニューからクエリを行うデータベース テーブルを選択します。

- ほとんどのテーブルでは、[検索（Search）] ドロップダウン リストが表示されます。
- [アプリケーション統計（Application Statistics）] テーブルでは、[フィルタ（Filter）] ドロップダウン リストが表示されます。

ステップ 2 レポートの制約に使用する検索かフィルタを選択します。

[編集（Edit）]（✎）をクリックして、検索条件を表示したり、新しい検索設定を作成したりできます。

レポートテンプレート表形式セクションのフィールドの変更

手順

ステップ 1 表形式のレポートセクションで、[フィールド（Fields）] パラメータの横にある **[編集（Edit）]**（✎）アイコンをクリックします。

ステップ 2 セクションを変更する場合、カラムを追加/削除し、望む順番にそれらのカラムをドラッグします。

ステップ 3 どの列でもソート順序を変更する場合、各カラムの横にあるドロップダウンリストを使用して、ソート順序および優先順位を設定する必要があります。

ステップ 4 [OK] をクリックします。

レポートテンプレートへのテキストセクションの追加

テキスト セクションには、複数のフォント サイズやフォント スタイル（太字や斜体など）を使用できるリッチ テキスト、入力パラメータ、インポート済みイメージを使用できます。

ヒント テキスト セクションは、レポートやそのセクションの概要説明に役立ちます。

手順

ステップ 1 レポート テンプレート エディタで、[テキストセクション追加（Add Text Section）]（T）をクリックします。

ステップ 2 新しいテキスト セクションを、レポート テンプレート内のご希望の位置にドラッグします。

ステップ 3 テキスト セクションをページの最初または最後に移動するには、テキスト セクションの前または後に改ページを挿入します。

ステップ 4 テキストセクションの総称名を変更するには、タイトルバーのセクション名をクリックし、新しい名前を入力します。

ステップ 5 テキスト セクションの本文に形式設定済みのテキストやイメージを追加します。

レポートの生成時に動的に更新する入力パラメータを組み込むことができます。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

入力パラメータ （655 ページ）

レポートテンプレートへの改ページの追加

手順

ステップ 1 レポート テンプレート エディタで、[改ページの追加（Add Page Break）]（  ）をクリックします。

改ページがテンプレートの下部に表示されます。

ステップ 2 改ページを、セクションの前後のご希望の場所にドラッグします。

ステップ 3 [保存（Save）] をクリックします。

グローバル時間枠とレポート テンプレート セクション

時間ベースのデータ（侵入イベントや検出イベントなど）があるレポートテンプレートにはグローバル時間枠があります。この時間枠は、テンプレート内の時間ベースのセクションでデフォルトで作成時に継承されます。グローバル時間枠を変更すると、グローバル時間枠を継承するように設定されているセクションのローカル時間枠が変更されます。[時間枠を継承する（Inherit Time Window）] チェック ボックスをクリアすると、個々のセクションの時間枠の継承を無効にできます。それから、ローカル時間枠を編集できます。

（注） グローバル時間枠の継承は、侵入イベントや検出イベントなど、時間ベースのテーブルからのデータがあるレポート セクションだけに適用されます。ネットワーク アセット（ホストやデバイス）と関連情報（脆弱性など）を報告するセクションの場合、各時間枠を個別に設定する必要があります。

レポート テンプレートとそのセクションのグローバル時間枠の設定

ヒント レポート内のセクションごとに別の時間枠を使用できます。たとえば、最初のセクションを月の要約にして、残りのセクションで週レベルの詳細情報へドリルダウンするようにできます。この場合、セクション レベルの時間枠を個別に設定します。

手順

ステップ 1 レポート テンプレート エディタで [生成（Generate）] をクリックします。

ステップ 2 グローバル時間枠を変更するには、**[時間枠（Time Window）]**（）をクリックします。

ステップ 3 [イベント時間枠（Events Time Window）] で時間設定を変更します。

ステップ 4 [適用（Apply）] をクリックします。

ステップ 5 [生成（Generate）] をクリックしてレポートを生成し、[はい（Yes）] をクリックして確認します。

レポート テンプレート セクションのローカル時間枠の設定

手順

ステップ 1 テンプレートの [レポート セクション（Report Sections）] ページで、セクションの [時間枠を継承する（Inherit Time Window）] チェック ボックスが存在する場合はクリアします。

ステップ 2 セクションのローカル時間枠を変更するには、**[時間枠（Time Window）]**（） をクリックします。

（注） 統計テーブルからのデータがあるセクションでは、スライド式の時間枠のみ使用できます。

ステップ 3 [イベント時間枠（Events Time Window）] で [適用（Apply）] をクリックします。

ステップ 4 [保存（Save）] をクリックします。

レポート テンプレート セクションの名前変更

手順

ステップ 1 レポート テンプレート エディタで、セクション ヘッダーの現在のセクション名をクリックします。

ステップ 2 新しいセクション名を入力します。

ステップ 3 [OK] をクリックします。

レポート テンプレート セクションのプレビュー

プレビュー機能は、表形式の表示のフィールドのレイアウトとソート順序や、円グラフの色などのグラフの読みやすさに関する重要な特性を表示します。

手順

ステップ 1 レポート テンプレート セクションの編集中は、いつでも、そのセクションの [プレビュー（Preview）] をクリックできます。

ステップ 2 プレビューを閉じるには、[OK] をクリックします。

レポート テンプレート セクションでの検索

レポートが正常に作成されるかどうかは、レポートのセクションへの入力内容を決める検索設定の定義が重要な要素になります。システムには検索エディタが備わっており、レポートテンプレートで使用できる検索設定を表示したり、新しいカスタム検索設定を定義したりできます。

レポート テンプレートのセクションの検索

手順

ステップ 1 レポートテンプレート内の関連するセクションから、[検索（Search）] フィールドの横にある **[編集（Edit）]**（）をクリックします。

ステップ 2 事前定義済みの検索に基づいてカスタム検索を作成する場合は、[保存済み検索（Saved Searches）] ドロップダウンリストから事前定義された検索を選択する必要があります。

このリストには、このテーブルに対して使用可能な事前定義済みの検索設定がすべて表示されます。システム規模の事前定義済み検索設定とレポート固有の事前定義済み検索設定も含まれています。

ステップ 3 該当するフィールドで検索条件を編集します。

特定のフィールドでは、制約にイベント検索設定と同じ演算子（<や<>など）を含めることができます。複数の条件を入力すると、すべての基準を満たすレコードだけが検索で返されます。

ステップ 4 制約値を入力する代わりに、ドロップダウンメニューから入力パラメータを挿入する場合は、[入力パラメータ（Input Parameter）]（＋）をクリックする必要があります。

（注） レポートの検索設定の制約を編集すると、システムにより *section* custom search という名前で編集済みの検索設定が保存されます。*section* は、セクションのタイトル バーに示される文字列 custom search の前の名前の部分です。保存するカスタム検索設定の名前をわかりやすくするには、セクション名を変更した後に編集済みの検索設定を保存するようにしてください。保存したレポートの検索設定の名前は変更できません。

ステップ 5 **[OK]** をクリックします。

入力パラメータ

レポートの生成時に動的に更新できる入力パラメータをレポートテンプレート内で使用できます。[入力パラメータ（Input Parameter）]（＋）は、それらを処理できるフィールドを示します。次の 2 種類の入力パラメータがあります。

- 定義済みの入力パラメータは、内部システム関数か設定情報によって解決されます。たとえば、レポートの生成時に、システムにより $<Time> パラメータは現在の日時に置き換えられます。
- ユーザー定義の入力パラメータは、セクション検索で制約を行えます。入力パラメータを使用して検索設定を制約すると、レポートの生成時に要求者から値を収集するようにシステムに指示できます。この方法で、テンプレートを変更せずに、レポートを生成時に動的に調整して特定のデータのサブセットを表示できます。たとえば、レポートセクションの検索設定の [接続先 IP（Destination IP）] フィールドに入力パラメータを指定できます。指定後、レポートの生成時に、特定の部門の IP ネットワークのセグメントを入力して、その部門のデータだけを取得できます。

  文字列タイプの入力パラメータを定義して、電子メール（件名または本文）、レポートファイル名、テキストセクションなどのレポートの特定のフィールドに動的テキストを追加することもできます。すべて同じテンプレートを利用し、カスタマイズしたレポートファイル名、電子メール アドレス、電子メール メッセージを使用して、さまざまな部門用にレポートをパーソナライズできます。

定義済み入力パラメータ

表 *55*：定義済み入力パラメータ

このパラメータを入力すると、	テンプレートに次の情報が含まれます：
$<Logo>	選択した更新ロゴ

このパラメータを入力すると、	テンプレートに次の情報が含まれます：
$<Report Title>	レポート タイトル
$<Time>	レポートを実行する日付、時刻、粒度 1 秒
$<Month>	現在の月
$<Year>	現在の西暦
$<System Name>	Management Center 名
$<Model Number>	Management Center のモデル番号
$<Time Window>	レポート セクションに現在適用されている時間窓
$<Constraints>	レポート セクションに現在適用されている検索制約

表 *56*：定義済み入力パラメータの使用法

パラメータ	レポート テンプレート カバー ページ	レポート テンプレート レポート タイトル	レポート テンプレート セクションの説明	レポート テンプレート本文セクション	レポート ファイル名の作成	レポート電子メールの主題、本文の作成
$<Logo>	はい	いいえ	いいえ	いいえ	いいえ	いいえ
$<Report Title>	はい	いいえ	はい	はい	はい	はい
$<Time>	はい	はい	はい	はい	はい	はい
$<Month>	はい	はい	はい	はい	はい	はい
$<Year>	はい	はい	はい	はい	はい	はい
$<System Name>	はい	はい	はい	はい	はい	はい
$<Model Number>	はい	はい	はい	はい	はい	はい
$<Time Window>	いいえ	いいえ	はい	いいえ	いいえ	いいえ
$<Constraints>	いいえ	いいえ	はい	いいえ	いいえ	いいえ

ユーザー定義の入力パラメータ

入力パラメータを使用して、検索設定の実用性を向上させます。入力パラメータにより、レポートの生成時に要求者から値を収集するようにシステムに指示できます。この方法で、検索設定を変更せずに、レポートを生成時に動的に制約して特定のデータのサブセットを表示でき

ます。たとえば、レポートセクションの[宛先IP（Destination IP）]フィールドに入力パラメータを指定して、部門レベルでセキュリティ イベントをドリル ダウンできます。レポートの生成時に、特定の部門の IP ネットワークのセグメントを入力して、その部門のデータだけを取得できます。

入力パラメータのタイプにより、そのパラメータを使用できる検索フィールドが決まります。特定のタイプは、該当するフィールドでのみ使用できます。たとえば、ユーザ パラメータを文字列タイプとして定義すると、テキスト フィールド内への挿入には使用できますが、IP アドレスを使用するフィールドでは使用できません。

定義する入力パラメータごとに名前とタイプがあります。

表 *57*：ユーザ定義の入力パラメータのタイプ

パラメータのタイプ	使用先のフィールド内のデータ
ネットワーク/IP（Network/IP）	CIDR 形式の IP アドレスまたはネットワーク セグメント
Application	アプリケーションプロトコル、クライアントアプリケーション、または Web アプリケーションの名前
イベント メッセージ（Event Message）	イベント ビュー メッセージ
Device	Management Center または管理対象デバイス
[ユーザ名（Username）]	イニシエータ ユーザやレスポンダ ユーザなどのユーザ ID
番号（VLAN ID、Snort ID、Vuln ID）（Number (VLAN ID, Snort ID, Vuln ID)）	VLAN ID、[Snort ID]、または脆弱性 ID
文字列	アプリケーションやOSのバージョン、注記、説明などのテキスト フィールド

ユーザ定義の入力パラメータの作成

手順

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。

ステップ 2 [入力パラメータの追加（Add Input Parameter）]（＋） をクリックします。

ステップ 3 パラメータの [名前（Name）] を入力します。

ステップ 4 [タイプ（Type）] ドロップダウン リストから値を選択します。

ステップ 5 [OK] をクリックしてパラメータを追加します。

ステップ 6 [OK] をクリックしてエディタに戻ります。

ユーザー定義の入力パラメータの編集

レポートテンプレートの[入力パラメータ（Input Parameters）]セクションに、テンプレートに使用可能なユーザー定義パラメータがすべてリストされます。

手順

ステップ 1 レポート テンプレート エディタで、[詳細設定（Advanced）] をクリックします。

ステップ 2 変更するパラメータの横にある**[編集（Edit）]**（）をクリックします。

ステップ 3 [名前（Name）] に新しい名前を入力します。

ステップ 4 [タイプ（Type）] ドロップダウン リストを使用して、パラメータ タイプを変更します。

ステップ 5 [OK] をクリックして変更を保存します。

ステップ 6 入力パラメータを削除するには、入力パラメータの横にある[削除（Delete）]（）をクリックし、確認します。

ステップ 7 [OK] をクリックして、レポート テンプレート エディタに戻ります。

ユーザ定義の入力パラメータによる検索の制約

定義した入力パラメータは、そのパラメータのタイプと一致する検索フィールドでのみ使用できます。たとえば、**ネットワーク/IP** タイプのパラメータは、CIDR 形式の IP アドレスまたはネットワーク セグメントを受け入れるフィールドだけで使用できます。

手順

ステップ 1 レポート テンプレート エディタで、セクション内の [検索（Search）] フィールドの横にある**[編集（Edit）]**（）をクリックします。

入力パラメータを使用できるフィールドは、[入力パラメータ（Input Parameter）]（）のマークが付けられます。

ステップ 2 フィールドの横にある[入力パラメータ（Input Parameter）]（）をクリックして、ドロップダウンメニューから入力パラメータを選択します。

ユーザー定義の入力パラメータは、のマークが付けられます。

ステップ 3 [OK] をクリックします。

レポート テンプレート内のドキュメント属性

レポートを生成する前に、レポートの外観に影響を与えるドキュメント属性を設定できます。これらの属性には、オプションの表紙と目次が含まれます。一部の属性のサポートは、レポートの形式に PDF、HTML、CSV のいずれを選択したかによって異なります。

表 *58*：ドキュメント属性のサポート

属性	PDF のサポート	HTML のサポート	CSV のサポート
表紙	可能、オプションでロゴと外観のカスタマイズ	可能、オプションでロゴと外観のカスタマイズ	いいえ
目次	はい	はい	いいえ
ページのヘッダーとフッター	可能、オプションでフィールド内にテキストかロゴ	いいえ	いいえ
カスタムの開始ページ番号	はい	いいえ	いいえ
先頭ページに番号を付けないオプション	はい	いいえ	いいえ

レポート テンプレート内のドキュメント属性の編集

手順

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。

ステップ 2 次の選択肢があります。

- 表紙の追加：表紙を追加するには、[表紙を含める（Include Cover Page）] チェックボックスをオンにします。
- 表示のカスタマイズ：表紙のデザインを編集するには、表紙のカスタマイズ（660ページ）を参照してください。
- 目次の追加：目次を追加するには、[目次を含める（Include Table of Contents）] チェックボックスをオンにします。
- ロゴの管理：テンプレートに関連付けられたロゴ イメージを管理するには、レポート テンプレートのロゴの管理 （660 ページ）を参照してください。
- ヘッダーとフッターの設定：テンプレートのヘッダーとフッターの要素を指定するには、[ヘッダー（Header）] フィールドと [フッター（Footer）] フィールのドロップダウン リストを使用します。
- 最初のページ番号の設定：レポートの最初のページ番号を指定するには、[ページ番号の開始（Page Number Start）] の値を入力します。
- 最初のページ番号の表示：レポートの最初のページのページ番号を表示するには、[最初のページに番号を付けますか（Number First Page?）] チェックボックスをオンにします。このオプションを選択すると、表紙には番号が付けられません。

ステップ 3 [OK] をクリックして変更を保存します。

表紙のカスタマイズ

レポート テンプレートの表紙をカスタマイズできます。表紙には、複数のフォント サイズやフォント スタイル（太字や斜体など）を使用できるリッチ テキスト、入力パラメータ、インポート済みイメージを使用できます。

手順

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。

ステップ 2 [表紙ページのデザイン（Cover Page Design）] の横にある**[編集（Edit）]**（✎）をクリックします。

ステップ 3 リッチ テキスト エディタで表紙のデザインを編集します。

ステップ 4 [OK] をクリックします。

レポート テンプレートのロゴの管理

Management Center で複数のロゴを保存し、さまざまなレポート テンプレートに関連付けることができます。テンプレートを設計する際に、ロゴの関連付けを設定します。テンプレートをエクスポートすると、エクスポート パッケージにロゴが含まれます。

Management Center にロゴをアップロードすると、そのロゴは次のものに使用できます。

- Management Center のすべてのレポート テンプレート、または
- マルチドメイン展開では、現在のドメイン内のすべてのレポート テンプレート

ロゴ画像は、PNG 形式、JPG 形式、または GIF 形式することができます。

レポート内のロゴは、Management Center にアップロードされているいずれかの JPG 画像に変更できます。たとえば、テンプレートを再使用する場合は、別の組織のロゴをレポートに関連付けることができます。

アップロードしたロゴは、削除できます。ロゴを削除すると、そのロゴが使用されているすべてのテンプレートから削除されます。削除を取り消すことはできません。事前定義済のシスコ ロゴは削除できない点に注意してください。

手順

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。

テンプレートに現在関連付けられているロゴは、[一般設定（General Settings）] の [ロゴ（Logo）] の下に表示されます。

ステップ 2 ロゴの横にある **[編集（Edit）]**（✎）をクリックします。

ステップ 3 次の選択肢があります。

- 追加：新しいロゴを追加します。詳細については、新しいロゴの追加（661 ページ）を参照してください。
- 変更：レポートテンプレートのロゴを変更します。詳細については、レポートテンプレートのロゴの変更（661 ページ）を参照してください。
- 削除：ロゴを削除します。詳細については、ロゴの削除（661 ページ）を参照してください。

新しいロゴの追加

手順

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。

ステップ 2 [ロゴ（Logo）] フィールドの横にある**[編集（Edit）]**（✎）をクリックします。

ステップ 3 [ロゴのアップロード（Upload Logo）] をクリックします。

ステップ 4 [参照（Browse）] をクリックし、ファイルの場所を参照し、[開く（Open）] をクリックします。

ステップ 5 [アップロード（Upload）] をクリックします。

ステップ 6 新しいロゴを現在のテンプレートに関連付けるには、それを選択し、[OK] をクリックします。

レポート テンプレートのロゴの変更

手順

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。

ステップ 2 [ロゴ（Logo）] フィールドの横にある**[編集（Edit）]**（✎）をクリックします。

ステップ 3 [ロゴの選択（Select Logo）] ダイアログで、レポート テンプレートに関連付けるロゴを選択します。

ステップ 4 [OK] をクリックします。

ロゴの削除

手順

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。

ステップ 2 [ロゴ（Logo）] フィールドの横にある**[編集（Edit）]**（）をクリックします。
ステップ 3 [ロゴの選択（Select Logo）] ダイアログで、削除するロゴを選択します。
ステップ 4 [ロゴの削除（Delete Logo）] をクリックします。
ステップ 5 [OK] をクリックします。

レポート テンプレートの管理

マルチドメイン展開では、現在のドメインで作成されたレポート テンプレートが表示されます。このテンプレートは編集可能です。先祖ドメインで作成されたレポートテンプレートも表示されますが、これは編集できません。下位のドメインのレポートテンプレートを表示および編集するには、そのドメインに切り替えます。システムによって表示されるレポートは、現在のドメインで作成されたもののみです。

このタスクを実行するには、管理者ユーザーである必要があります。

手順

ステップ 1 **[概要（Overview）]** > **[レポート（Reporting）]**を選択します。
ステップ 2 [レポートテンプレート（Report Templates）] をクリックします。
ステップ 3 次の選択肢があります。

- 削除：削除するテンプレートの横にある[削除（Delete）]（）をクリックして確認します。

  システム付属のレポート テンプレートは削除できません。セキュリティ アナリストは、自分が作成したレポートテンプレートのみを削除できます。マルチドメイン展開では、現在のドメインに属しているレポート テンプレートのみを削除できます。

- 編集：レポートテンプレートを編集する場合は、レポートテンプレートの編集（663ページ）を参照してください。
- エクスポート：レポート テンプレートをエクスポートする場合は、レポート テンプレートのエクスポート（664ページ）を参照してください。

  ヒント また、標準設定のエクスポート プロセスを使用してレポート テンプレートをエクスポートすることもできます。設定のエクスポート（624ページ）を参照してください。

- インポート：レポート テンプレートをインポートする場合は、設定のインポート（625ページ）を参照してください。

レポート テンプレートの編集

マルチドメイン展開では、現在のドメインで作成されたレポート テンプレートが表示されます。このテンプレートは編集可能です。先祖ドメインで作成されたレポートテンプレートも表示されますが、これは編集できません。下位のドメインのレポートテンプレートを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[概要（Overview）]** > **[レポート（Reporting）]**を選択します。

ステップ 2 [レポートテンプレート（Report Templates）] をクリックします。

ステップ 3 編集するテンプレートの**[編集（Edit）]**（）をクリックします。

代わりに [表示（View）]（） が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 次の選択肢があります。

- 改ページを追加します。レポートテンプレートへの改ページの追加（652 ページ）を参照してください。
- テキストセクションを追加します。レポートテンプレートへのテキストセクションの追加（651 ページ）を参照してください。
- レポートテンプレートの設定（649 ページ）の説明に従ってセクション コンテンツを設定します。
- 入力パラメータを作成します。ユーザ定義の入力パラメータの作成（657 ページ）を参照してください。
- 入力パラメータを編集します。ユーザー定義の入力パラメータの編集（658 ページ）参照してください。
- ドキュメントの属性を編集します。レポート テンプレート内のドキュメント属性の編集（659 ページ）を参照してください。
- テンプレートセクションを検索します。レポートテンプレートのセクションの検索（654 ページ）を参照してください。
- [詳細設定（Advanced）]をクリックし、レポートテンプレート内のドキュメント属性（658 ページ）の説明に従ってドキュメント属性を設定します。
- グローバル時間枠を設定します。レポートテンプレートとそのセクションのグローバル時間枠の設定 （653 ページ）を参照してください。
- ローカル時間枠を設定します。レポート テンプレート セクションのローカル時間枠の設定 （653 ページ）を参照してください。
- 検索フィールドを設定します。レポートテンプレート表形式セクションのフィールドの変更 （651 ページ）参照してください。
- 表とデータ形式を設定します。レポート テンプレート セクションのテーブルとデータ形式の設定 （650 ページ）を参照してください。

- 検索とフィルタを指定します。レポート テンプレート セクションの検索またはフィルタの指定 （651 ページ）を参照してください。

レポート テンプレートのエクスポート

このタスクを実行するには、管理者ユーザーである必要があります。

手順

ステップ 1 **[概要（Overview）] > [レポート（Reporting）]**を選択します。
ステップ 2 [レポートテンプレート（Report Templates）] を選択します。
ステップ 3 エクスポートするテンプレートの [エクスポート（Export）] アイコンをクリックします。

レポートの生成について

レポートの生成

レポートテンプレートを作成してカスタマイズすると、レポート生成の準備は完了です。生成プロセスで、レポートの形式（HTML、 PDF、または CSV）を選択できます。レポートのグローバル時間枠を調整することもできます。この時間枠は、除外されていないすべてのセクションに一貫したタイム フレームを適用します。

PDF レポートの場合：

- Unicode（UTF-8）文字を使用したファイル名はサポートされません。
- 特殊な Unicode ファイル名が含まれるレポートセクション（ファイルイベントやマルウェアイベントで表示されるセクションなど）では、そのファイル名は書き直された形式で表示されます。
- 各レポートセクションに設定する結果の数は、特定の制限内にする必要があります。この制限を表示するには、レポートテンプレートに表示された黄色の三角形をマウスオーバーします。

レポートテンプレートの検索の指定にユーザー入力パラメータが含まれている場合、生成プロセスで値を入力するよう求められ、このレポートの実行内容がデータのサブセットに合わせて調整されます。

DNS サーバの設定および IP アドレス解決が有効化されている場合、正常に解決されたホスト名がレポートに取り込まれます。

マルチドメイン展開では、先祖ドメインでレポートを生成すると、そのレポートにはすべての子孫ドメインからの結果を含めることができます。特定のリーフ ドメインのレポートを生成するには、そのドメインに切り替えます。

手順

ステップ 1 **[概要（Overview）]** > **[レポート（Reporting）]**を選択します。

ステップ 2 [レポートテンプレート（Report Templates）] をクリックします。

ステップ 3 レポートの生成に使用するテンプレートの横にある [レポート（Report）]（） をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ヒント 先祖のテンプレートからレポートを生成するには、そのテンプレートを現在のドメインにコピーします。

ステップ 4 必要に応じて、レポート名を設定します。

- 新しい [ファイル名（File Name）] を入力します。新しい名前を入力しないと、システムはレポート テンプレートで指定した名前を使用します。
- [入力パラメータ（Input Parameter）]（）を使用して、1 つ以上の入力パラメータをファイル名に追加します。

ステップ 5 [HTML]、[PDF]、または [CSV] をクリックして、レポートの出力形式を選択します。

PDF オプションがグレー表示されている場合は、1 つ以上のレポート セクションで設定されている結果件数が大きすぎる可能性があります。特定の制限については、レポート テンプレートで黄色の三角形を探して、見つかったらそれにマウス オーバーします。

ステップ 6 グローバル時間枠を変更する場合は、**[時間枠（Time Window）]**（）をクリックします。

（注） グローバル時間枠の設定は、個々のレポート セクションのうちグローバル設定を継承するように設定されているものの内容だけに影響します。

ステップ 7 [入力パラメータ（Input Parameters）] セクションに表示されるフィールドの値を入力します。

ヒント フィールドにワイルドカード文字 * を入力すると、ユーザ パラメータを無視できます。こうすると、検索設定がユーザ パラメータで制約されなくなります。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、リテラルの IP アドレスまたは VLAN タグを使用してレポート結果を制約すると、予期しない結果になる可能性があります。

ステップ 8 電子メール リレー ホストを Management Center 構成で有効化した場合は、[電子メール（Email）] をクリックして、レポートの生成時にレポートが自動的に電子メール配信されるようにします。

ステップ 9 プロンプトが表示されたら、**[生成（Generate）]** をクリックして確認します。

[生成（Generate）] をクリックすると、レポート テンプレートと共に生成設定が保存されます。

[閉じる（Close）] または [キャンセル（Cancel）]をクリックすると、セッション期間中の選択のみが保存されます。

ステップ 10 次の選択肢があります。

- レポート リンクをクリックして、新しいウィンドウにレポートを表示します。
- [OK] をクリックして、レポート テンプレート エディタに戻ります。

レポートの生成オプション

レポートの生成オプションは、以下のように設定できます。

- 1 回のみまたは定期のいずれかの将来のレポート生成をスケジュールします。レポートの生成の自動化（606 ページ）を参照してください。毎日、毎週、毎月など、さまざまな範囲のタイム フレームに基づいたスケジュールでもカスタマイズできます。
- スケジューラを使用してメール レポートを配信します。タスクをスケジュールする**前に**、レポート テンプレートとメール リレー ホストを設定する必要があります。
- レポートを生成すると、そのレポートが受信者リストにメールの添付ファイルとして自動的に送信されます。レポートを電子メールで配信するように、メール リレー ホストを適切に設定する必要があります。
- 新しく生成されたレポート ファイルを、設定されたリモート ストレージの場所に保存します。リモート ストレージを使用するには、まずリモート ストレージの場所を設定します。

（注） リモートに保存してから、ローカルストレージに切り替えた場合、リモートストレージ内のレポートは [レポート（Reports）] タブのリストに表示されません。同様に、あるリモートストレージの場所から別の場所に切り替えた場合、以前の場所にあるレポートはリストに表示されません。

レポートの生成時の電子メール配布

手順

ステップ 1 **[概要（Overview）] > [レポート（Reporting）]**を選択します。

ステップ 2 [レポートテンプレート（Report Templates）] をクリックします。

ステップ 3 レポートの生成に使用するテンプレートの横にある [レポート（Report）]（） をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ヒント 先祖のテンプレートからレポートを生成するには、そのテンプレートを現在のドメインにコピーします。

ステップ 4 このウィンドウの [電子メール（Email）] セクションを展開します。

ステップ 5 [電子メール オプション（Email Options）] フィールドで、[電子メールの送信（Send Email）] を選択します。

ステップ 6 [受信者リスト（Recipient List）]、[CC] および [BCC] フィールドで、カンマ区切りリストの形式で受信者の電子メール アドレスを入力します。

ステップ 7 [件名（Subject）] フィールドに、電子メールの件名を入力します。

ヒント [件名（Subject）] フィールドやメッセージ本文に入力パラメータを使用して、電子メール内にタイムスタンプや Management Center の名前などの情報を動的に生成できます。

ステップ 8 必要に応じて、電子メールの本文にカバー レターを入力します。

ステップ 9 [OK] をクリックして確定します。

関連トピック

メール リレー ホストおよび通知アドレスの設定 （69 ページ）

将来のレポートのスケジュール

レポートの生成の自動化 （606 ページ） を参照してください。

生成されたレポートの操作について

以前に生成されたレポートには、[レポート（Reports）] タブのページからアクセスして操作します。

レポートの表示

[レポート（Reports）] には、以前に生成されたすべてのレポートと、そのレポート名、生成日時、生成したユーザー、およびそのレポートがローカルに保存されたかリモートに保存されたかが一覧表示されます。ステータスのカラムには、レポートがすでに生成されているか、生成キュー内にある（スケジュール済みタスクの場合など）か、それとも生成できなかった（ディスク領域不足などの理由で）かが示されます。

管理者アクセス権を持つユーザはすべてのレポートを表示でき、その他のユーザは自分が生成したレポートだけを表示できることに注意してください。

マルチドメイン展開では、現在のドメインで作成されたレポートだけを表示できます。

[レポート（Reports）]ページには、ローカルに保存されたレポートがすべて示されます。現在リモートストレージが設定されている場合、リモートに保存されたレポートも示されます。リモートで保存されたレポートの [場所（Location）] カラム データは、「Remote」になります。

（注） リモートに保存してから、ローカルストレージに切り替えた場合、リモートストレージ内のレポートは [レポート（Reports）] タブのリストに表示されません。同様に、あるリモートストレージの場所から別の場所に切り替えた場合、以前の場所にあるレポートはリストに表示されません。

手順

ステップ 1 **[概要（Overview）]** > **[レポート（Reporting）]**を選択します。

ステップ 2 [レポート（Reports）] をクリックします。

ステップ 3 表示するレポートを選択します。

レポートのダウンロード

ローカルコンピュータにレポートファイルをダウンロードできます。そのコンピュータから、電子メールや他の使用可能な方法で電子的に配布できます。

マルチドメイン導入では、現在のドメインで生成されたレポートのみをダウンロードできます。

手順

ステップ 1 **[概要（Overview）]** > **[レポート（Reporting）]**を選択します。

ステップ 2 [レポート（Reports）] をクリックします。

ステップ 3 ダウンロードするレポートの横にあるチェック ボックスをオンにして、[ダウンロード（Download）] をクリックします。

ヒント ページ上のすべてのレポートをダウンロードするには、そのページの左上にあるチェック ボックスをオンにします。複数のレポートが複数のページにある場合は、2 つ目のチェック ボックスが表示されます。これをクリックすると、すべてのページ上のすべてのレポートをダウンロードできます。

ステップ 4 ブラウザのプロンプトに従って、レポートをダウンロードします。複数のレポートを選択すると、1 つの .zip ファイルでダウンロードされます。

リモートでのレポートの保存

[概要（Overview）] > [レポート（Reporting）] > [レポート（Reports）] ページの下部に、現在設定されているレポート ストレージの場所が表示され、ローカル、NFS、SMB ストレージの場合はディスク使用率も表示されます。SSH を使用してリモート ストレージにアクセスする場合、ディスク使用率のデータは利用できません。

（注） リモートに保存してから、ローカルストレージに切り替えた場合、リモートストレージ内のレポートは [レポート（Reports）] タブのリストに表示されません。同様に、あるリモートストレージの場所から別の場所に切り替えた場合、以前の場所にあるレポートはリストに表示されません。

始める前に

- リモートストレージの場所を設定します。詳細については、リモート ストレージ デバイス （111 ページ）を参照してください。

手順

ステップ 1 **[概要（Overview）] > [レポート（Reporting）]**を選択します。

ステップ 2 [レポート（Reports）] を選択します。

ステップ 3 ページ下部の [レポートのリモート ストレージの有効化（Enable Remote Storage of Reports）] チェック ボックスをオンにします。

次のタスク

- ローカルストレージからリモートストレージにレポートを移動します（リモート ストレージへのレポートの移動 （669 ページ）を参照）。

関連トピック

リモート ストレージ デバイス （111 ページ）
リモート ストレージへのレポートの移動 （669 ページ）

リモート ストレージへのレポートの移動

バッチ モードまたは単独で、ローカル ストレージ内のレポートをリモート ストレージの場所に移動できます。

（注） リモートに保存してから、ローカルストレージに切り替えた場合、リモートストレージ内のレポートは [レポート（Reports）] タブのリストに表示されません。同様に、あるリモートストレージの場所から別の場所に切り替えた場合、以前の場所にあるレポートはリストに表示されません。

始める前に

- リモートストレージの場所を設定します。詳細については、リモート ストレージ デバイス （111 ページ）を参照してください。

手順

ステップ 1 **[概要（Overview）] > [レポート（Reporting）]**を選択します。

ステップ 2 [レポート（Reports）] を選択します。

ステップ 3 移動するレポートの横にあるチェックボックスをオンにして、[移動（Move）] をクリックします。

ヒント ページ上のすべてのレポートを移動するには、そのページの左上にあるチェックボックスをオンにします。レポートのページが複数にわたる場合は、2 つ目のチェックボックスが表示されます。すべてのページのすべてのレポートを移動する場合は、このチェックボックスをオンにします。

ステップ 4 レポートの移動を確認します。

レポートの削除

レポート ファイルはいつでも削除できます。この手順によりファイルが完全に削除され、リカバリ不能になります。レポートの生成に使用したレポート テンプレートがまだ残っていますが、時間枠を拡大したりスライドしたりした場合は、特定のレポート ファイルを再生成するのは難しくなることがあります。テンプレートで入力パラメータを使用した場合も、再生成するのが難しくなることがあります。

マルチドメイン導入では、現在のドメインで生成されたレポートのみを削除できます。

手順

ステップ 1 **[概要（Overview）] > [レポート（Reporting）]**を選択します。

ステップ 2 [レポート（Reports）] をクリックします。

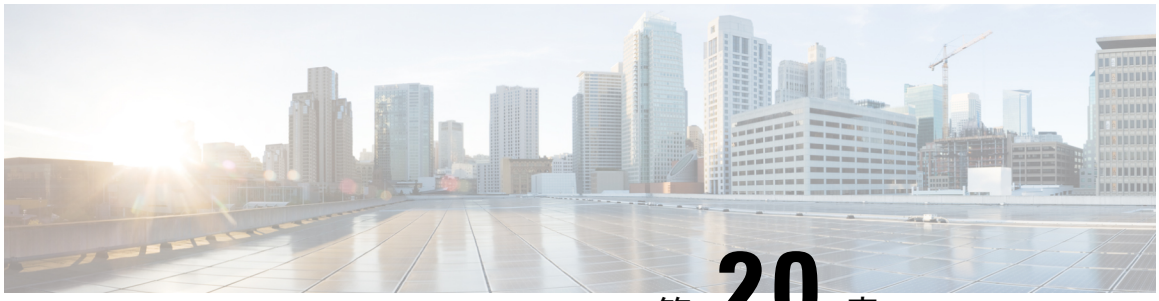
ステップ 3 次の選択肢があります。

- [選択項目の削除（Delete selected）]：削除するレポートの隣のチェック ボックスをオンにしてから、[削除（Delete）] をクリックします。
- [すべて削除（Delete all）]：ページ上のすべてのレポートを削除するには、そのページの左上にあるチェック ボックスをオンにします。複数のレポートが複数のページにある場合は、2つ目のチェック ボックスが表示され、すべてのページ上のすべてのレポートを削除するよう選択できます。

ステップ 4 削除を確認します。

レポートの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
レポートテンプレートで接続イベントのデータソースを選択する	7.0	任意（Any）	ウィザードを使用し、セキュリティ分析とロギング（オンプレミス）を使用してリモートデータストレージを設定する場合、そのボリュームに保存されているデータをレポートに含めることができます。 変更されたページ：[レポートテンプレート（Report template）]
脆弱性レポートの変更	6.7	任意（Any）	Bugtraqデータが使用できないため、レポート出力が調整されました。



第 20 章

アラートの応答を使用した外部アラート

次のトピックでは、アラート応答を使用して Secure Firewall Management Center から外部イベント アラートを送信する方法を示します。

Secure Firewall Management Center アラート応答

SNMP、syslog、または電子メールでの外部イベント通知はクリティカルなシステムのモニタリングに役立ちます。Secure Firewall Management Center はアラート応答を構成して外部サーバーと対話します。アラート応答は、電子メール、SNMP、syslog サーバへの接続を表す構成です。これが応答と呼ばれるのは、これを使用して Firepower により検出されたイベントに応答してアラートを送信できるためです。異なるタイプのアラートを異なるモニタリング サーバーまたはユーザー（あるいはその両方）に送信するための複数のアラート応答を構成できます。

（注） デバイスおよび Firepower のバージョンによっては、アラート応答は syslog メッセージを送信する最適な方法ではない可能性があります。『Cisco Secure Firewall Management Center デバイス構成ガイド』の「About Syslog」の章およびセキュリティ イベント syslog メッセージングを設定するためのベストプラクティス （769 ページ）を参照してください。。

（注） アラート応答を使用するアラートは、Secure Firewall Management Center によって送信されます。アラート応答を使用しない侵入の電子メール アラートも、Secure Firewall Management Center によって送信されます。対照的に、個別の侵入ルールのトリガーに基づく SNMP および syslog アラートは管理対象デバイスから直接送信されます。詳細については、侵入イベントの外部アラート （685 ページ）を参照してください。

ほとんどの場合、外部アラートに含まれる情報はデータベースにロギングされたいずれかの関連イベントに含まれる情報と同じです。ただし、相関ルールに接続トラッカーが含まれる相関イベントアラートについては、受信する情報はベースのイベントの種類に関係なく、トラフィック プロファイル変更のアラート情報と同じです。

アラート応答の作成や管理は [アラート（Alerts）] ページ（**[ポリシー（Policies）]** > **[アクション（Actions）]** > **[アラート（Alerts）]**）で行います。新しいアラート応答は自動的に有効になります。アラート応答を削除するのではなく無効にすることで、アラートの生成を一時的に止めることができます。

アラート応答への変更は、接続ログを SNMP トラップまたは syslog サーバーに送信する場合を除き、ただちに有効になります。

アラート応答のサポート設定

アラート応答を作成後、その応答を使用して、次の外部アラートを Secure Firewall Management Center から送信できます。

アラート/イベントのタイプ	詳細情報
侵入イベント（インパクト フラグ別）	影響フラグ アラートの設定 （681 ページ）
検出イベント（タイプ別）	検出イベント アラートの設定 （681 ページ）
マルウェア防御（「ネットワークベース」）によって検出されたマルウェアとレトロスペクティブ マルウェア イベント	マルウェア防御アラートの設定 （682 ページ）
相関イベント（相関ポリシー違反ごと）	ルールと許可（Allow）リストに応答を追加する （1192 ページ）
相関イベント（ログ ルールまたはデフォルト アクション別）（電子メールアラートのサポートなし）	ログ可能なその他の接続 （881 ページ）
ヘルス イベント（ヘルス モジュールおよび重大度レベル別）	ヘルス モニター アラートの作成 （465 ページ）

アラート応答の要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者

SNMP アラート応答の作成

Threat Defense を除くデバイスタイプでは、SNMPv1、SNMPv2、または SNMPv3 を使用して SNMP アラート応答を作成できます。

（注） SNMP プロトコルの SNMP バージョンを選択する場合、SNMPv2 では読み取り専用コミュニティのみがサポートされ、SNMPv3 では読取り専用ユーザーのみがサポートされることに注意してください。SNMPv3 は、AES128 での暗号化をサポートします。

SNMP で 64 ビット値をモニターする場合は、SNMPv2 または SNMPv3 を使用する必要があります。SNMPv1 は 64 ビットのモニタリングをサポートしていません。

始める前に

- ネットワーク管理システムで Secure Firewall Management Center の管理情報ベース（MIB）ファイルが必要な場合は、`/etc/sf/DCEALERT.MIB` で取得できます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクション（Actions）]** > **[アラート（Alerts）]**を選択します。

ステップ 2 [アラートの作成（Create Alert）] ドロップダウンメニューから、[SNMP アラートの作成（Create SNMP Alert）] を選択します。

ステップ 3 SNMP アラートの設定フィールドを編集します。

a) [名前（Name）]：SNMP 応答を識別する名前を入力します。

b) [トラップサーバー（Trap Server）]：SNMP トラップサーバーのホスト名または IP アドレスを入力します。

（注） このフィールドに無効なIPv4アドレス（192.169.1.456など）を入力した場合でも、システムは警告を**表示しません**。無効なアドレスはホスト名として扱われます。

c) [バージョン（Version）]：ドロップダウンリストから、使用する SNMP バージョンを選択します。SNMPv3 がデフォルトです。

次から選択します。

- [SNMPv1] または [SNMPv2]：[コミュニティストリング（Community String）] フィールドに読み取り専用のSNMPコミュニティ名を入力してから、手順の最後までスキップします。

  （注） SNMP コミュニティストリング名には、特殊文字（< > / % # & ? ', etc.）を使用できません。

- [SNMPv3] の場合：[ユーザー名（User Name）] フィールドに SNMP サーバーで認証するユーザーの名前を入力し、次の手順に進みます。

d) [認証プロトコル（Authentication Protocol）]：ドロップダウンリストから、認証の暗号化に使用するプロトコルを選択します。

次から選択します。

- [MD5]：Message Digest 5（MD5）のハッシュ関数。
- [SHA]：セキュア ハッシュ アルゴリズム（SHA）のハッシュ関数。

e) [認証パスワード（Authentication Password）]：認証を有効にするためのパスワードを入力します。

f) [プライバシープロトコル（Privacy Protocol）]：ドロップダウンリストから、プライベートパスワードの暗号化に使用するプロトコルを選択します。

次から選択します。

- [DES]：対称秘密鍵ブロックアルゴリズムで 56 ビットキーを使用する Data Encryption Standard（DES）。
- [AES]：対称暗号アルゴリズムで56ビットキーを使用するAdvanced Encryption Standard（AES）。
- [AES128]：対称暗号アルゴリズムで128ビットキーを使用するAES。キーが長いほど安全になりますが、パフォーマンスは低下します。

g) [プライバシーパスワード（Privacy Password）]：SNMP サーバーに必要なプライバシーパスワードを入力します。プライベートパスワードを指定すると、プライバシーが有効になり、認証パスワードも指定する必要があります。

h) [エンジンID（Engine ID）]：SNMPエンジンの識別子を偶数桁の16進表記で入力します。

SNMPv3を使用する場合、メッセージの符号化にはエンジンID値が使用されます。SNMPサーバーでは、メッセージをデコードするためにこの値が必要です。

Secure Firewall Management Center の IP アドレスの 16 進数バージョンを使用することを推奨します。たとえば、Secure Firewall Management Center の IP アドレスが 10.1.1.77 である場合、0a01014D0 を使用します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

変更内容は、次の場合を除き、ただちに有効になります。

アラート応答を使って接続ログを送信している場合、これらのアラート応答を編集したあとに設定の変更を展開する必要があります。

Syslog アラート応答の作成

syslog アラート応答を設定する際、syslog サーバーで確実に正しく処理されるようにするために、syslog メッセージに関連付けられる重大度とファシリティを指定できます。ファシリティはメッセージを作成するサブシステムを示し、シビラティ（重大度）はメッセージのシビラティ（重大度）を定義します。ファシリティとシビラティ（重大度）はsyslogに示される実際のメッセージには表示されませんが、syslog メッセージを受信するシステムに対して、メッセージの分類方法を指示するために使用されます。

ヒント syslog の機能とその設定方法の詳細については、ご使用のシステムのマニュアルを参照してください。UNIX システムでは、`syslog` および `syslog.conf` の `man` ページで概念情報および設定手順が説明されています。

syslog アラート応答の作成時に任意のタイプのファシリティを選択できますが、syslog サーバに基づいて意味のあるものを選択する必要があります。すべてのsyslogサーバがすべてのファシリティをサポートしているわけではありません。UNIX syslog サーバの場合、`syslog.conf` ファイルで、どのファシリティがサーバ上のどのログファイルに保存されるかを示す必要があります。

始める前に

- この手順は、多くの場合、syslog メッセージを送信するための推奨される方法ではありません。
- syslog サーバーがリモート メッセージを受け入れられることを確認します。

手順

ステップ 1 **[ポリシー（Policies）] > [アクション（Actions）] > [アラート（Alerts）]**を選択します。

ステップ 2 [アラートの作成（Create Alert）] ドロップダウン メニューから、[Syslog アラートの作成（Create Syslog Alert）] を選択します。

ステップ 3 [名前（Name）] にアラートの名前を入力します。

ステップ 4 [ホスト（Host）] フィールドに、syslog サーバのホスト名または IP アドレスを入力します。

（注） このフィールドに無効な IPv4 アドレス（192.168.1.456 など）を入力した場合でも、システムは警告を**表示しません**。無効なアドレスはホスト名として扱われます。

ステップ 5 [ポート（Port）] フィールドに、サーバが syslog メッセージに使用するポートを入力します。この値はデフォルトで 514 です。

ステップ 6 Syslog アラート ファシリティ （678 ページ）で説明されているとおりに、[ファシリティ（Facility）] リストからファシリティを選択します。

ステップ 7 syslog 重大度レベル （679 ページ）で説明されているとおりに、[シビラティ（重大度）（Severity）] リストからシビラティ（重大度）を選択します。

ステップ 8 [タグ（Tag）] フィールドに、syslog メッセージとともに表示するタグ名を入力します。

たとえば、syslog に送信されるすべてのメッセージの前に `FromMC` を付ける場合、このフィールドに `FromMC` と入力します。

ステップ 9 [保存（Save）] をクリックします。

次のタスク

変更内容は、次の場合を除き、ただちに有効になります。

アラート応答を使って syslog サーバーに接続ログを送信している場合、これらのアラート応答を編集したあとに設定の変更を展開する必要があります。

セキュリティ イベントに対するこのアラート応答を使用する場合は、ポリシーにアラート応答を指定する必要があります。セキュリティ イベントの syslog の設定場所 （775 ページ） を参照してください。

Syslog アラート ファシリティ

次の表に、選択可能な syslog ファシリティを示します。

表 *59* : 使用可能な *syslog* ファシリティ

ファシリティ	説明
AUTH	セキュリティと承認に関連するメッセージ。
AUTHPRIV	セキュリティと承認に関連する制限付きアクセス メッセージ。多くのシステムで、これらのメッセージはセキュア ファイルに転送されます。
CONSOLE	アラート メッセージ。

ファシリティ	説明
CRON	クロック デーモンによって生成されるメッセージ。 Linux オペレーティング システムを実行している syslog サーバは CRON ファシリティを使用することに注意してください。
DAEMON	システム デーモンによって生成されるメッセージ。
FTP	FTP デーモンによって生成されるメッセージ。
KERN	カーネルによって生成されるメッセージ。多くのシステムでは、これらのメッセージは表示されるときにコンソールに出力されます。
LOCAL0-LOCAL7	内部プロセスによって生成されるメッセージ。
LPR	印刷サブシステムによって生成されるメッセージ。
MAIL	メール システムで生成されるメッセージ。
NEWS	ネットワーク ニュース サブシステムによって生成されるメッセージ。
NTP	NTP デーモンによって生成されるメッセージ。
SECURITY	監査サブシステムによって生成されるメッセージ。
SYSLOG	syslog デーモンによって生成されるメッセージ。
SOLARIS-CRON	クロック デーモンによって生成されるメッセージ。 Windows オペレーティング システムを実行している syslog サーバは CLOCK ファシリティを使用することに注意してください。
USER	ユーザーレベルのプロセスによって生成されるメッセージ。
UUCP	UUCP サブシステムによって生成されるメッセージ。

syslog 重大度レベル

次の表に、選択可能な標準の syslog シビラティ（重大度）レベルを示します。

表 *60 : syslog* シビラティ（重大度）レベル

レベル	説明
ALERT	ただちに修正する必要がある状態。
CRIT	クリティカルな状態。
DEBUG	デバッグ情報を含むメッセージ。

レベル	説明
EMERG	すべてのユーザに配信されるパニック状態。
ERR	エラー状態。
INFO	情報メッセージ。
NOTICE	エラー状態ではないが、注意が必要な状態。
WARNING	警告メッセージ。

電子メール アラート応答の作成

始める前に

- Secure Firewall Management Center で、自身の IP アドレスを逆解決できることを確認します。
- メール リレー ホストおよび通知アドレスの設定 （69 ページ）の説明に従って、メール リレー ホストを設定します。

（注） 電子メールアラートを使用して、接続をログに記録することはできません。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクション（Actions）]** > **[アラート（Alerts）]**を選択します。

ステップ 2 [アラートの作成（Create Alert）] ドロップダウン メニューから、[電子メール アラートの作成（Create Email Alert）] を選択します。

ステップ 3 [名前（Name）] にアラート応答の名前を入力します。

ステップ 4 [宛先（To）] フィールドに、アラートを送信する電子メール アドレスをカンマで区切って入力します。

ステップ 5 [送信元（From）] フィールドに、アラートの送信者として表示する電子メール アドレスを入力します。

ステップ 6 [リレー ホスト（Relay Host）] の横に表示されるメール サーバーが、アラートの送信に使用するサーバーであることを確認します。

ヒント 電子メールサーバーを変更するには、**[編集（Edit）]** （） をクリックします。

ステップ 7 [保存（Save）] をクリックします。

影響フラグ アラートの設定

特定のインパクトフラグを持つ侵入イベントが発生するたびにアラートが生成されるようにシステムを設定できます。インパクトフラグは、侵入データ、ネットワーク検出データ、および脆弱性情報を関連付けることにより、侵入がネットワークに与える影響を評価するのに役立ちます。

これらのアラートを設定するには、IPS スマートライセンスまたは保護クラシックライセンスが必要です。

手順

ステップ 1 **[ポリシー（Policies）] > [アクション（Actions）] > [アラート（Alerts）]**を選択します。

ステップ 2 [インパクトフラグアラート（Impact Flag Alerts）] をクリックします。

ステップ 3 [アラート（Alerts）]セクションで、各アラートタイプで使用するアラート応答を選択します。

ヒント 新しいアラート応答を作成するには、任意のドロップダウンリストから[新規（New）]を選択します。

ステップ 4 [インパクト設定（Impact Configuration）] セクションで、該当するチェックボックスをオンにして、各インパクト フラグに対して受信するアラートを指定します。

インパクトフラグの定義については、侵入イベント影響レベル（962 ページ）を参照してください。

ステップ 5 [保存（Save）] をクリックします。

検出イベント アラートの設定

特定のタイプの検出イベントが発生するたびにアラートが生成されるようにシステムを設定できます。

始める前に

- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Network Discovery Policies*」の章の説明に従って、アラートを設定する検出イベントタイプを記録するようにネットワーク検出ポリシーを設定します。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクション（Actions）]** > **[アラート（Alerts）]**を選択します。

ステップ 2 [ディスカバリ イベント アラート（Discovery Event Alerts）] をクリックします。

ステップ 3 [アラート（Alerts）]セクションで、各アラートタイプで使用するアラート応答を選択します。

ヒント 新しいアラート応答を作成するには、任意のドロップダウンリストから[新規（New）]を選択します。

ステップ 4 [イベント設定（Events Configuration）] セクションで、各検出イベント タイプに対して、受信するアラートに対応するチェックボックスを選択します。

ステップ 5 [保存（Save）] をクリックします。

マルウェア防御 アラートの設定

レトロスペクティブイベントなどのマルウェアイベントが マルウェア防御 によって生成された（つまり、「ネットワークベースのマルウェアイベント」が生成された）場合は常に通知するようにシステムを設定できます。エンドポイント向け AMP によって生成されたマルウェア イベント（「エンドポイントベースのマルウェア イベント」）にはアラートを生成できません。

始める前に

- マルウェア クラウド ルックアップを実行するファイルポリシーを設定し、そのポリシーをアクセスコントロールルールに関連付けます。詳細については、『Cisco Secure Firewall Management Center デバイス構成ガイド』の「Access Control Overview」を参照してください。
- これらのアラートを設定するには、マルウェア防御ライセンスが必要です。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクション（Actions）]** > **[アラート（Alerts）]**を選択します。

ステップ 2 [高度なマルウェア保護アラート（Advanced Malware Protections Alerts）] をクリックします。

ステップ 3 [アラート（Alerts）]セクションで、各アラートタイプで使用するアラート応答を選択します。

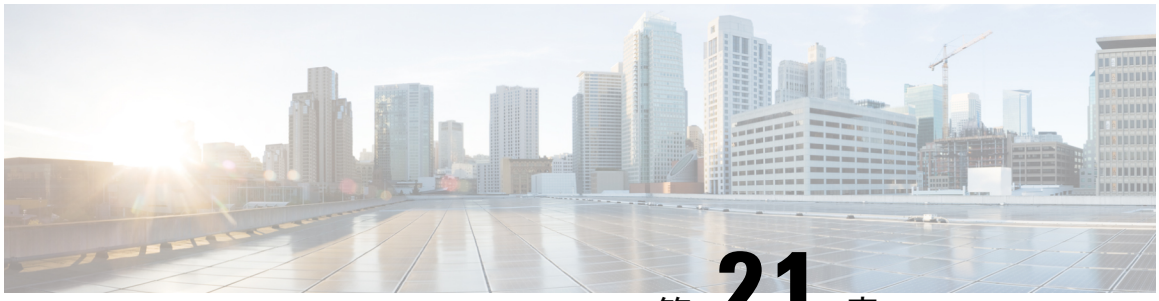
ヒント 新しいアラート応答を作成するには、任意のドロップダウンリストから[新規（New）]を選択します。

ステップ 4 [イベント設定（Event Configuration）]セクションで、各マルウェア イベント タイプに対して、受信するアラートに対応するチェックボックスを選択します。

[すべてのネットワークベースのマルウェア イベント（All network-based malware events）] には [レトロスペクティブ イベント（Retrospective Events）] が含まれることに注意してください。

（定義により、ネットワークベースのマルウェア イベントにはエンドポイント向け AMP によって生成されたイベントは含まれません。）

ステップ 5 [保存（Save）] をクリックします。



第 21 章

侵入イベントの外部アラート

次のトピックでは、侵入イベントに関する外部アラートを設定する方法について説明します。

侵入イベントの外部アラートについて

外部侵入イベント通知は、クリティカルなシステム モニタリングに役立ちます。

- SNMP：侵入ポリシーごとに設定し、管理対象デバイスが送信します。SNMP アラートは侵入ルールごとに有効にすることができます。
- syslog：侵入ポリシーごとに設定し、管理対象デバイスが送信します。1 つの侵入ポリシーの syslog アラートを有効にすると、ポリシーに含まれるすべてのルールに適用されます。
- 電子メール：すべての侵入ポリシーに設定され、Secure Firewall Management Center が送信します。電子メール アラートは侵入ルールごとに有効にすることができ、長さと頻度を制限することもできます。

侵入イベントの抑制やしきい値を設定すると、システムは、ルールがトリガーされるたびに侵入イベントを生成しなくなる（したがってアラートを送信しなくなる）場合があるのでご注意ください。

（注） Secure Firewall Management Center も SNMP、syslog、および電子メール アラート応答を使って種々の外部アラートを送信します。Secure Firewall Management Center アラート応答 （673 ページ）を参照してください。システムは、個々の侵入イベントに対するアラートを送信するためにアラート応答を使用**しません**。

関連トピック

侵入ポリシーの侵入イベント通知フィルタ

侵入イベントに関する外部アラートのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

侵入イベントに関する外部アラートの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

侵入イベントの SNMP アラートの設定

侵入ポリシーで外部 SNMP アラートを有効にした後、トリガー時に SNMP アラートを送信する個々のルールを設定できます。これらのアラートは管理対象デバイスから送信されます。

手順

ステップ 1 侵入ポリシー エディタのナビゲーション ウィンドウで、[詳細設定（Advanced Settings）] をクリックします。

ステップ 2 [SNMP アラート（SNMP Alerting）] が有効になっていることを確認し、[編集（Edit）] をクリックします。
ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。

ステップ 3 SNMP バージョンを選択し、侵入 SNMP アラートのオプション （687 ページ）の説明に従って構成オプションを指定します。

ステップ 4 ナビゲーション ウィンドウで [ルール（Rules）] をクリックします。

ステップ 5 [ルール（rules）] ペインで、SNMP アラートを設定するルールを選択し、**[アラート（Alerting）] > [SNMP アラートの追加（Add SNMP Alert）]** を選択します。

ステップ 6 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] を選択して、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

侵入 SNMP アラートのオプション

ネットワーク管理システムで Management Information Base（MIB）ファイルが必要な場合は、Secure Firewall Management Center の `/etc/sf/DCEALERT.MIB` から取得できます。

SNMP v2 オプション

オプション	説明
トラップ タイプ	アラートに表示される IP アドレスに使用するトラップ タイプ。 ネットワーク管理システムによって INET_IPV4 アドレス タイプが正常にレンダリングされた場合は、[バイナリとして（as Binary）] を選択します。それ以外の場合は、[文字列として（as String）] を選択します。たとえば、HP OpenView では [文字列として（as String）] が必要になります。
トラップ サーバー（Trap Server）	SNMP トラップ通知を受信するサーバ。 単一の IP アドレスまたはホスト名を指定できます。
コミュニティ ストリング（Community String）	コミュニティ名。

SNMP v3 オプション

管理対象デバイスは、エンジン ID の値を使用して SNMPv3 アラートをエンコードします。アラートをデコードするには、SNMP サーバにこの値が必要です。この値は、送信デバイスの管理インターフェイスの IP アドレスの 16 進数のバージョンで、「01」が付加されています。

たとえば、SNMP アラートを送信するデバイスの管理インターフェイスの IP アドレスが 172.16.1.50 である場合、エンジン ID の値は 0xAC10013201 です。

オプション	説明
トラップ タイプ	アラートに表示される IP アドレスに使用するトラップ タイプ。 ネットワーク管理システムによって INET_IPV4 アドレス タイプが正常にレンダリングされた場合は、[バイナリとして（as Binary）] を選択します。それ以外の場合は、[文字列として（as String）] を選択します。たとえば、HP OpenView では [文字列として（as String）] が必要になります。
トラップ サーバー（Trap Server）	SNMP トラップ通知を受信するサーバ。 単一の IP アドレスまたはホスト名を指定できます。
認証パスワード（Authentication Password）	認証に必要なパスワード。SNMP v3 は、設定に応じて Message Digest 5（MD5）ハッシュ関数またはセキュア ハッシュ アルゴリズム（SHA）ハッシュ関数のいずれかを使用し、このパスワードを暗号化します。 認証パスワードを指定すると、認証が有効になります。
プライベート パスワード（Private Password）	プライバシー用の SNMP キー。SNMP v3 は Data Encryption Standard（DES）ブロック暗号を使用して、このパスワードを暗号化します。SNMP v3 パスワードを入力すると、パスワードは初期設定時にはプレーン テキストで表示されますが、暗号化形式で保存されます。 プライベート パスワードを指定すると、プライバシーが有効になり、認証パスワードも指定する必要があります。
ユーザー名（User Name）	SNMP ユーザー名。

侵入イベントの Syslog アラートの設定

侵入ポリシーでsyslogアラートを有効にすると、管理対象デバイス自体または外部ホスト上の syslog にすべての侵入イベントが送信されます。外部ホストを指定した場合、syslog アラートは管理対象デバイスから送信されます。

手順

ステップ 1 侵入ポリシー エディタのナビゲーション ウィンドウで、[詳細設定（Advanced Settings）] をクリックします。

ステップ 2 [Syslog アラート（Syslog Alerting）] が有効になっていることを確認し、[編集（Edit）] をクリックします。

ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。[Syslogアラート（Syslog Alerting）] ページが [詳細設定（Advanced Settings）] ページの下に追加されます。

ステップ 3 syslog アラートを送信するロギング ホストの IP アドレスを入力します。

[ロギングホスト（Logging Hosts）] フィールドを空白のままにした場合、ロギングホストの詳細は関連付けられているアクセス制御ポリシーの [ロギング（Logging）] から取得されます。

ステップ 4 侵入syslogアラートの機能と重大度（689ページ）の説明に従って、[ファシリティ（Facility）] と **[重大度（Severity）]** のレベルを選択します。

ステップ 5 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] を選択して、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

侵入 syslog アラートの機能と重大度

管理対象デバイスは、特定のファシリティと [重大度（Severity）] を使用して、侵入イベントをsyslogアラートとして送信できるため、ロギングホストがアラートを分類できます。ファシリティには、それを生成したサブシステムを指定します。これらのファシリティと [重大度（Severity）] の値は、実際の syslog メッセージには表示されません。

ご使用の環境に基づいて意味のある値を選択します。ローカル設定ファイル（UNIX ベースのロギング ホストの syslog.conf など）では、どのログ ファイルにどのファシリティを保存するかを示すことができます。

Syslog アラート ファシリティ

ファシリティ	説明
AUTH	セキュリティと承認に関連するメッセージ。
AUTHPRIV	セキュリティと承認に関連する制限付きアクセス メッセージ。多くのシステムで、これらのメッセージはセキュア ファイルに転送されます。
CONSOLE	アラート メッセージ。
CRON	クロック デーモンによって生成されるメッセージ。
DAEMON	システム デーモンによって生成されるメッセージ。

ファシリティ	説明
FTP	FTP デーモンによって生成されるメッセージ。
KERN	カーネルによって生成されるメッセージ。多くのシステムでは、これらのメッセージは表示されるときにコンソールに出力されます。
LOCAL0-LOCAL7	内部プロセスによって生成されるメッセージ。
LPR	印刷サブシステムによって生成されるメッセージ。
MAIL	メール システムで生成されるメッセージ。
NEWS	ネットワーク ニュース サブシステムによって生成されるメッセージ。
SYSLOG	syslog デーモンによって生成されるメッセージ。
USER	ユーザーレベルのプロセスによって生成されるメッセージ。
UUCP	UUCP サブシステムによって生成されるメッセージ。

syslog アラートの重大度

レベル	説明
EMERG	すべてのユーザにブロードキャストするパニック状態
ALERT	すぐに修正する必要がある状態
CRIT	重大な状態
ERR	エラー状態
WARNING	警告メッセージ
NOTICE	エラー状態ではないが、注意が必要な状態
INFO	通知メッセージ
DEBUG	デバッグ情報を含むメッセージ

侵入イベントに対する電子メール アラートの設定

侵入の電子メールアラートを有効にした場合、どの管理対象デバイスまたは侵入ポリシーが侵入を検出したかに関係なく、システムは侵入イベントの生成時に電子メールを送信できます。これらのアラートは Secure Firewall Management Center から送信されます。

始める前に

- 電子メール アラートを受信するようにメール ホストを設定します。メール リレー ホストおよび通知アドレスの設定 （69 ページ）を参照してください。
- Secure Firewall Management Center が独自の IP アドレスを逆解決できることを確認します。

手順

ステップ 1 **[ポリシー（Policies）] > [アクション（Actions）] > [アラート（Alerts）]**を選択します。

ステップ 2 [侵入電子メール（Intrusion Email）] をクリックします。

ステップ 3 侵入電子メール アラートのオプション （691 ページ）の説明に従って、アラートを生成する侵入ルールや侵入グループを含むアラート オプションを選択します。

ステップ 4 [保存（Save）] をクリックします。

侵入電子メール アラートのオプション

On/Off

侵入電子メール アラートを有効または無効にします。

（注） 有効にすると、個々のルールが選択されていない限り、すべてのルールのアラートが有効になります。

アドレス送信元/宛先（From/To Addresses）

電子メールの送信者と受信者。受信者のカンマ区切りリストを指定できます。

最大アラート数と頻度（Max Alerts and Frequency）

Secure Firewall Management Center が時間間隔（[頻度（Frequency）]）ごとに送信する電子メール アラートの最大数（[最大アラート数（Max Alerts）]）。

合同アラート（Coalesce Alerts）

同じ送信元 IP とルール ID を持つアラートをグループ化することによって送信されるアラートの数を減らします。

サマリー出力（Summary Output）

テキスト制限されたデバイスに適した短いアラートを有効にします。短いアラートには、以下の情報が含まれています。

- Timestamp
- プロトコル
- 送信元と宛先の IP とポート
- メッセージ
- 同じ送信元 IP に対して生成された侵入イベントの数

例：`2011-05-18 10:35:10 10.1.1.100 icmp 10.10.10.1:8 -> 10.2.1.3:0 snort_decoder: Unknown Datagram decoding problem! (116:108)`

[サマリー出力（Summary Output）] を有効にする場合は、[合同アラート（Coalesce Alerts）] も有効にすることを検討してください。テキストメッセージの制限を超えないように、[最大アラート数（Max Alerts）] を下げることもできます。

タイム ゾーン

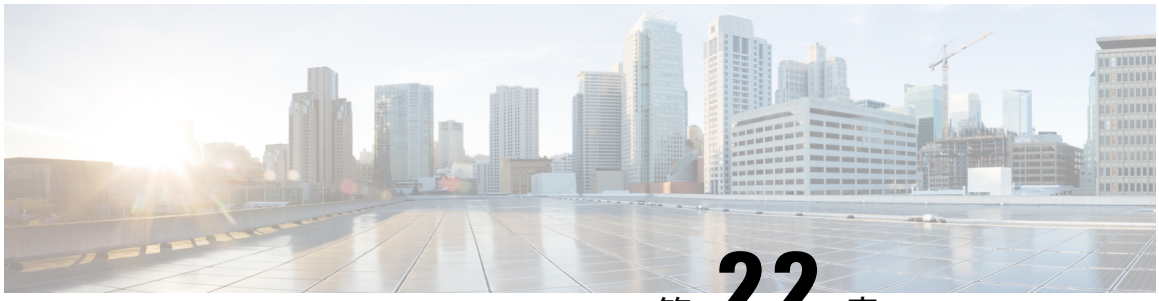
アラート タイムスタンプのタイム ゾーン。

特定のルール設定に基づく電子メール警告（Email Alerting on Specific Rules Configuration）

電子メール アラートを設定するルールを選択できます。

第 VI 部

イベントとアセットの分析ツール



第 22 章

コンテキストエクスプローラ

以下のトピックでは、コンテキストエクスプローラを使用する方法について説明します。

コンテキスト エクスプローラについて

システムの Context Explorer には、モニター対象ネットワークのステータスに関するコンテキストでの詳細でインタラクティブなグラフィカル情報が表示されます。これには、アプリケーション、アプリケーション統計、接続、位置情報、侵害の兆候、侵入イベント、ホスト、サーバー、セキュリティインテリジェンス、ユーザー、ファイル（マルウェアファイルを含む）、関連 URL に関するデータが含まれます。各セクションには、このデータが鮮やかな色の折れ線グラフ、棒グラフ、円グラフ、ドーナツ グラフの形式で表示され、グラフとともに詳しいリストが示されます。1 番目のセクションに表示される時間の経過に伴うトラフィックとイベント数の変化を示した折れ線グラフは、ネットワークのアクティビティにおける最近の傾向の概要を示します。

分析を細かく調整するためのカスタム フィルタを容易に作成および適用できます。またグラフ エリアをクリックするか、カーソルをグラフ エリアに置くことでデータ セクションを詳しく調べることができます。過去 1 時間から過去 1 年までの期間を反映するように Explorer の時間範囲を設定することもできます。Context Explorer にアクセスできるユーザは、管理者、セキュリティ アナリスト、またはセキュリティ アナリスト（読み取り専用）のユーザ ロールが割り当てられているユーザだけです。

ダッシュボードは細かなカスタマイズが可能で、区分化されており、リアルタイムで更新されます。一方、Context Explorer は手動で更新され、より幅広いデータのコンテキストを提供することを目的としており、アクティブなユーザ操作のために単一で一貫性のあるレイアウトを備えています。

特定のニーズに基づいてネットワークとアプライアンスのリアルタイムのアクティビティをモニタするには、ダッシュボードを使用します。逆に、詳細かつ明確なコンテキストで事前に定義されている最新のデータ セットを調査するには、Context Explorer を使用します。たとえば、ネットワークのホストのうち Linux を使用しているホストは 15% であるが、ほぼすべての YouTube トラフィックはこれらのホストによるものであることが判明した場合、Linux ホストのデータのみを表示するフィルタ、YouTube 関連のアプリケーション データのみを表示するフィルタ、あるいはこの両方のフィルタを簡単に適用できます。コンパクトで対象が絞り込まれているダッシュボードウィジェットとは異なり、Context Explorer の各セクションは、専門知識を持つユーザーと一般的なユーザーの両方に役立つ形式で、システムアクティビティを鮮明なビジュアル表現で提供します。

表示されるデータは、管理対象デバイスのライセンスおよび導入状況や、そのデータを提供する機能を設定しているかどうかによって異なります。また、Context Explorer のすべてのセクションで、フィルタを適用して表示するデータを制限することもできます。

マルチドメイン導入では、先祖ドメインで Context Explorer を表示すると、すべてのサブドメインからの集約データが表示されます。リーフ ドメインでは、そのドメインに固有のデータだけを表示できます。

ダッシュボードと Context Explorer の違い

次の表に、ダッシュボードと Context Explorer の主な相違点の要約を示します。

表 *61 :* 比較：ダッシュボードと *Context Explorer*

機能	ダッシュボード	コンテキストエクスプローラ
表示可能なデータ	システムによってモニターされるすべてのもの	アプリケーション、アプリケーション統計、位置情報、ホストの侵害の兆候、侵入イベント、ファイル（マルウェア ファイルを含む）、ホスト、セキュリティ インテリジェンスイベント、サーバ、ユーザ、およびURL
カスタマイズ可能かどうか	• ダッシュボードで選択されているウィジェットはカスタマイズ可能です • 個々のウィジェットはさまざまなレベルでカスタマイズ可能です	• 基本レイアウトは変更できません • 適用されたフィルタは Explorer URL に示され、後で使用するためにブックマークできます
データの更新頻度	自動（デフォルト）、ユーザ設定	手動（Manual）
データのフィルタリング	一部のウィジェットで可能です（ウィジェット設定を編集する必要があります）	Explorer のすべての部分で可能であり、複数フィルタに対応しています
グラフィカル コンテキスト	一部のウィジェット（特にカスタム分析（Custom Analysis））では、データをグラフ形式で表示できます	すべてのデータの豊富なグラフィカル コンテキスト（独自の詳細なドーナツ グラフを含む）

機能	ダッシュボード	コンテキストエクスプローラ
関連 Web インターフェイス ページへのリンク	一部のウィジェット	すべてのセクション
表示データの時間範囲	ユーザ設定	ユーザー設定

関連トピック

ダッシュボードについて （403 ページ）

[時系列のトラフィックおよび侵入イベント数（TrafficandIntrusionEvent Counts Time）] グラフ

Context Explorer の上部には、時間の経過に伴うトラフィックおよび侵入イベント数の変化を示す折れ線グラフが表示されます。X 軸は時間間隔を示します（選択されている時間枠に応じて、5 分～ 1 か月の範囲）。Y 軸は、KB 単位のトラフィック（青色の線）と侵入イベント数（赤色の線）を示します。

X 軸の最小間隔が 5 分であることに注意してください。これに対応するため、選択された時間範囲の開始点と終了点が、システムにより、最も近い 5 分間間隔に調整されます。

このセクションには、デフォルトでは選択された時間範囲のすべてのネットワーク トラフィックと、生成されたすべての侵入イベントが示されます。フィルタを適用すると、フィルタに指定されている条件に関連するトラフィックおよび侵入イベントのみがグラフに表示されます。たとえば、[OS 名（OS Name）] に `Windows` を指定してフィルタリングすると、時間グラフには Windows オペレーティング システムを使用するホストに関連するトラフィックとイベントだけが表示されます。

侵入イベントデータ（[優先順位（Priority）] が `High` に設定されたものなど）に基づいて Context Explorer をフィルタリングすると、青色のトラフィックを示す線が非表示になり、侵入イベントだけに集中することができます。

トラフィックおよびイベント数に関する正確な情報を確認するには、グラフ線上の任意のポイントにポインタを置きます。また、色付きの線の 1 つにポインタを置くと、その線がグラフの前面に移動し、コンテキストがより明確になります。

このセクションのデータは、主に [侵入イベント（Intrusion Events）] テーブルと [接続イベント（Connection Events）] テーブルから取得されます。

[侵害の兆候（Indications of Compromise）] セクション

コンテキスト エクスプローラの [侵害の兆候（IOC）（Indications of Compromise (IOC)）] セクションには、モニター対象ネットワーク上でセキュリティが侵害されている可能性があるホストの概要を示す 2 つのインタラクティブ セクション（トリガーとして使用された主な IOC 種類の割合のビューと、トリガーとして使用された兆候の数をホストごとに表したビュー）が表示されます。

IOC に関する詳細については、侵害の兆候データ （1107 ページ）を参照してください。

[兆候別ホスト（Hosts by Indication）] グラフ

[兆候別ホスト（Hosts by Indication）] グラフはドーナツ形式であり、モニタ対象ネットワーク上のホストでトリガーとして使用された侵害の兆候（IOC）を割合で表示します。内側のリングは IOC カテゴリ（[CnC 接続（CnC Connected）] や [マルウェア検出（Malware Detected）] など）ごとに分割されており、外側のリングではそれがさらに具体的なイベントの種類（[影響 2 侵入イベント - 管理者として試行（Impact 2 Intrusion Event — attempted-admin）] や [ファイル転送中に脅威を検出（Threat Detected in File Transfer）] など）ごとに分割されています。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフのデータは主に [ホスト（Hosts）] テーブルと [ホスト侵害の兆候（Indications of Compromise）] テーブルから取得されます。

[ホスト別兆候（Indications by Host）] グラフ

[ホスト別兆候（Indications by Host）] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最も IOC が顕著な 15 のホストでトリガーとして使用された固有の侵害の兆候（IOC）の数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフのデータは主に [ホスト（Hosts）] テーブルと [ホスト侵害の兆候（Indications of Compromise）] テーブルから取得されます。

[ネットワーク情報（Network Information）] セクション

Context Explorer の [ネットワーク情報（Network Information）] セクションには、モニター対象ネットワーク上の接続トラフィックの全体の概要（トラフィックに関連付けられている送信元、宛先、ユーザー、およびセキュリティゾーン、ネットワーク上のホストで使用されているオペレーティングシステムの内訳、ネットワークトラフィックに対して実行されたアクセス制御アクションの割合のビュー）を示す 6 つのインタラクティブグラフが含まれています。

[オペレーティング システム（Operating Systems）] グラフ

[オペレーティング システム（Operating Systems）] グラフはドーナツ グラフ形式で、モニタ対象ネットワークのホストで検出されたオペレーティング システムを割合で表示します。内側のリングは OS 名（`Windows` や `Linux` など）ごとに分割され、外側のリングではそのデータがさらにオペレーティング システムのバージョン（`Windows Server 2008` や `Linux 11.x` など）ごとに分割されています。密接に関連するいくつかのオペレーティング システム（Windows 2000、Windows XP、Windows Server 2003 など）は 1 つにまとめられます。ごく少数の認識されないオペレーティング システムは [その他（Other）] にまとめられます。

このグラフは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Context Explorer の時間範囲を変更しても、グラフは変化しません。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフのデータは、主に [ホスト（Hosts）] テーブルから取得されます。

[送信元 IP 別トラフィック（Traffic by Source IP）] グラフ

[送信元 IP 別トラフィック（Traffic by Source IP）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最もアクティブな上位 15 の送信元 IP アドレスのネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされた送信元IPアドレスごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[送信元IP別トラフィック（Traffic by Source IP）] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルから取得されます。

[送信元ユーザ別トラフィック（Traffic by Source User）] グラフ

[送信元ユーザ別トラフィック（Traffic by Source User）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最もアクティブな上位 15 の送信元ユーザのネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされた送信元IPアドレスごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

（注） 侵入イベントの情報でフィルタリングすると、[送信元ユーザー別トラフィック（Traffic by Source User）] グラフは非表示になります。

このグラフのデータは主に [接続イベント（Connection Events）] テーブルから取得されます。このグラフには、権限のあるユーザーのデータが表示されます。

[アクセス コントロール アクション別の接続（Connections by Access Control Action）] グラフ

[アクセス制御アクション別の接続（Connections by Access Control Action）] グラフは円グラフ形式であり、モニター対象トラフィックに対して実行されたアクセス制御アクション（[ブロック（Block）] や [許可（Allow）] など）の割合のビューを表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

（注） 侵入イベントの情報でフィルタリングすると、[送信元ユーザー別トラフィック（Traffic by Source User）] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルから取得されます。

[宛先 IP 別トラフィック（Traffic by Destination IP）] グラフ

[宛先 IP 別トラフィック（Traffic by Destination IP）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最もアクティブな上位 15 の宛先 IP アドレスのネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされた宛先IPアドレスごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[宛先 IP 別トラフィック（Traffic by Destination IP）] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルから取得されます。

[入力/出力のセキュリティ ゾーン別トラフィック（TrafficbyIngress/EgressSecurityZone）] グラフ

[入力/出力のセキュリティ ゾーン別トラフィック（Traffic by Ingress/Egress Security Zone）] グラフは棒グラフ形式で、モニタ対象ネットワークで設定されているセキュリティ ゾーンごとに、その着信/発信ネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。このグラフは、必要に応じて、入力（デフォルト）セキュリティゾーン情報または出力セキュリティ ゾーン情報のいずれかを表示するように設定できます。

リストされたセキュリティ ゾーンごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

ヒント グラフに制約を適用して、出力セキュリティゾーンのトラフィックのみが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [出力（Egress）] をクリックします。デフォルト ビューに戻すには [入力（Ingress）] をクリックします。Context Explorer から外部への移動でも、グラフがデフォルトの [入力（Ingress）] ビューに戻ることに注意してください。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[入力/出力のセキュリティ ゾーン別トラフィック（Traffic by Ingress/Egress Security Zone）] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルから取得されます。

[アプリケーション情報（Information）] セクション

Context Explorer の [アプリケーション情報（Information）] セクションには、3 つのインタラクティブ グラフと 1 つの表形式リストが表示されます。これらのグラフとリストは、モニタ対象ネットワーク上でのアプリケーションアクティビティの概要（アプリケーションに関連するトラフィック、侵入イベント、およびホストを、各アプリケーションに割り当てられている推定リスクまたは推定ビジネス関連度ごとに編成したもの）を示します。[アプリケーション詳細リスト（Application Details List）] は、各アプリケーションとそのリスク、ビジネス関連度、カテゴリ、ホスト数を示すインタラクティブなリストです。

このセクションのすべての「アプリケーション」インスタンスについて、[アプリケーション情報（Application Information）] のグラフのセットは、デフォルトでは特にアプリケーション プロトコル（DNS、SSH など）を検査します。クライアント アプリケーション（PuTTY や Firefox など）や Web アプリケーション（Facebook や Pandora など）を特に検査するように [アプリケーション情報（Application Information）] セクションを設定することもできます。

[アプリケーション情報（Application Information）] セクションへのフォーカスの移動

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[分析（Analysis）] > [コンテキストエクスプローラ（Context Explorer）]** を選択します。

ステップ 2 [アプリケーション プロトコル情報（Application Protocol Information）] セクションにポインタを重ねます。

（注） 以前に同じ Context Explorer セッションでこの設定を変更している場合は、セクション タイトルが [クライアント アプリケーション情報（Client Application Information）] または [Web アプリケーション情報（Web Application Information）] と表示されることがある点に注意してください。

ステップ 3 [アプリケーション プロトコル（Application Protocol）]、[クライアント アプリケーション（Client Application）]、または [Web アプリケーション（Web Application）] をクリックします。

[リスク/ビジネスとの関連性とアプリケーション別トラフィック（TrafficbyRisk/Business Relevance and Application）] グラフ

[リスク/ビジネスとの関連性とアプリケーション別トラフィック（Traffic by Risk/Business Relevance and Application）] グラフはドーナツ形式で、モニタ対象ネットワークで検出されたアプリケーショントラフィックを、アプリケーションの推定リスク（デフォルト）または推定のビジネスとの関連性（ビジネス関連度）ごとの割合で表示します。内側のリングは推定リスク/ビジネス関連度レベル（[中（Medium）] または [高（High）] など）ごとに分割され、外側のリングではそのデータがさらに具体的なアプリケーション（[SSH] または [NetBIOS] など）ごとに分割されます。稀に検出されるアプリケーションは [その他（Other）] にまとめられます。

このグラフは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Context Explorer の時間範囲を変更しても、グラフは変化しません。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

ヒント　グラフに制約を適用して、ビジネスとの関連性とアプリケーションごとにトラフィックが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Business Relevance] をクリックします。デフォルト ビューに戻すには [リスク（Risk）] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [リスク（Risk）] ビューに戻ることに注意してください。

（注）　侵入イベントの情報でフィルタ処理を実行すると、[リスク/ビジネスとの関連性とアプリケーション別トラフィック（Traffic by Risk/Business Relevance and Application）] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルと [アプリケーション統計（Application Statistics）] テーブルから取得されます。

[リスク/ビジネスとの関連度別侵入イベントおよびアプリケーション（IntrusionEventsby Risk/Business Relevance and Application）] グラフ

[リスク/ビジネスとの関連度別侵入イベントおよびアプリケーション（Intrusion Events by Risk/Business Relevance and Application）] グラフはドーナツ形式であり、モニタ対象ネットワークで検出された侵入イベントと、これらのイベントに関連するアプリケーションを、アプリケーションの推定リスク（デフォルト）または推定ビジネス関連度ごとの割合で表示します。内側のリングは推定リスク/ビジネス関連度レベル（[中（Medium）] または [高（High）] など）ごとに分割され、外側のリングではそのデータがさらに具体的なアプリケーション（[SSH] または [NetBIOS] など）ごとに分割されます。稀に検出されるアプリケーションは [その他（Other）] にまとめられます。

ドーナツ グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされるか、または（該当する場合には）アプリケーション情報が表示されます。

ヒント　グラフに制約を適用して、ビジネスとの関連性とアプリケーションごとに侵入イベントが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [ビジネスとの関連性（Business Relevance）] をクリックします。デフォルト ビューに戻すには [リスク（Risk）] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [リスク（Risk）] ビューに戻ることに注意してください。

このグラフのデータは主に [侵入イベント（Intrusion Events）] テーブルと [アプリケーションの統計（Application Statistics）] テーブルから取得されます。

[リスク/ビジネスとの関連度別ホストおよびアプリケーション（Hosts by Risk/Business Relevance and Application）] グラフ

[リスク/ビジネスとの関連度別ホストおよびアプリケーション（Hosts by Risk/Business Relevance and Application）] グラフはドーナツ形式であり、モニタ対象ネットワークで検出されたホストと、これらのホストに関連するアプリケーションを、アプリケーションの推定リスク（デフォルト）または推定ビジネス関連度ごとの割合で表示します。内側のリングは推定リスク/ビジネス関連度レベル（[中（Medium）] または [高（High）] など）ごとに分割され、外側のリングではそのデータがさらに具体的なアプリケーション（[SSH] または [NetBIOS] など）ごとに分割されます。非常に少数のアプリケーションは [その他（Other）] にまとめられます。

ドーナツ グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、ビジネスとの関連性とアプリケーションに基づいてホストが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [ビジネスとの関連性（Business Relevance）] をクリックします。デフォルト ビューに戻すには [リスク（Risk）] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [リスク（Risk）] ビューに戻ることに注意してください。

このグラフのデータは主に [アプリケーション（Applications）] テーブルから取得されます。

アプリケーション詳細リスト

[アプリケーション情報（Application Information）] セクション下部に表示される [アプリケーション詳細リスト（Application Details List）] は、モニタ対象ネットワークで検出される各アプリケーションの推定リスク、推定ビジネス関連度、カテゴリ、ホスト数の情報を示す表です。アプリケーションは、関連ホスト数の降順でリストされます。

[アプリケーション詳細リスト（Application Details List）] テーブルをソートすることはできませんが、テーブル内の項目をクリックして、その情報でフィルタリングまたはドリルダウンし

たり、（該当する場合に）アプリケーション情報を表示したりすることができます。このテーブルのデータは主に [アプリケーション（Applications）] テーブルから取得されます。

このリストは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Explorer の時間範囲を変更しても、リストは変化しません。

[セキュリティ インテリジェンス（Security Intelligence）] セクション

コンテキストエクスプローラの [セキュリティインテリジェンス（Security Intelligence）] セクションには、3つのインタラクティブな棒グラフが表示されます。これらのグラフは、モニター対象ネットワーク上でセキュリティインテリジェンスによってブロックまたはモニターされるトラフィックの概要を示します。これらのグラフでは、カテゴリ、送信元 IP アドレス、および宛先 IP アドレスに基づいてそれらのトラフィックがソートされ、トラフィックの量（KB/秒）と該当する接続の数の両方が表示されます。

[カテゴリ別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Category）] グラフ

[カテゴリ別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Category）] グラフは棒グラフ形式で、モニタ対象ネットワーク上のトラフィックのセキュリティインテリジェンスの上位のカテゴリに関する、ネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[カテゴリ別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Category）] グラフは非表示になります。

このグラフのデータは主に [セキュリティ インテリジェンス イベント（Security Intelligence Events）] テーブルから取得されます。

[送信元 IP 別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Source IP）] グラフ

[送信元 IP 別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Source IP）] グラフは棒グラフ形式で、モニタ対象ネットワーク上でセキュリティ インテリジェンスによってモニタされたトラフィックの上位の送信元 IP アドレスに関する、ネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。

（注） 侵入イベントの情報でフィルタリングすると、[送信元 IP 別のセキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Source IP）] グラフは非表示になります。

このグラフのデータは主に [セキュリティ インテリジェンス イベント（Security Intelligence Events）] テーブルから取得されます。

[宛先 IP 別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Destination IP）] グラフ

[宛先 IP 別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Destination IP）] グラフは棒グラフ形式で、モニタ対象ネットワーク上でセキュリティ インテリジェンスによってモニタされたトラフィックの上位の宛先 IP アドレスに関する、ネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。

（注） 侵入イベントの情報でフィルタリングすると、[宛先 IP 別のセキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Destination IP）] グラフは非表示になります。

このグラフのデータは主に [セキュリティ インテリジェンス イベント（Security Intelligence Events）] テーブルから取得されます。

[侵入情報（Intrusion Information）] セクション

Context Explorer の [侵入情報（Intrusion Information）] セクションには 6 つのインタラクティブ グラフと 1 つの表形式リストが表示されます。これらのグラフとリストは、モニター対象ネットワークの侵入イベントの概要（侵入イベントに関連付けられている影響レベル、攻撃元、攻撃対象先、ユーザー、優先レベル、およびセキュリティ ゾーンと、侵入イベントの分類、優先度、カウントを示す詳細なリスト）を示します。

[影響別侵入イベント（Intrusion Events by Impact）] グラフ

[影響別侵入イベント（Intrusion Events by Impact）] グラフは円グラフ形式であり、モニタ対象ネットワークの侵入イベントを推定影響レベル（0～4）のグループごとの割合で表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフのデータは、主に侵入検知（[IDS統計（IDS Statistics）] テーブル）および [侵入イベント（Intrusion Events）] テーブルから取得されます。

[上位の攻撃者（Top Attackers）] グラフ

[上位の攻撃者（Top Attackers）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の（侵入イベントを発生させた）上位の各攻撃元ホストIPアドレスの侵入イベント数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフのデータは、主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

[上位のユーザ（Top Users）] グラフ

[上位のユーザ（Top Users）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最大侵入イベント数に関連付けられたユーザと、イベント数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフのデータは、主に侵入検知（IDS）の [ユーザー統計（User Statistics）] テーブルおよび [侵入イベント（Intrusion Events）] テーブルから取得されます。このグラフには、権限のあるユーザーのデータが表示されます。

[優先度別侵入イベント（Intrusion Events by Priority）] グラフ

[優先度別侵入イベント（Intrusion Events by Priority）] グラフは円グラフ形式であり、モニタ対象ネットワークの侵入イベントを、推定優先度レベル（[高（High）]、[中（Medium）]、[低（Low）] など）のグループごとの割合で表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフのデータは、主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

[上位のターゲット（Top Targets）] グラフ

[上位のターゲット（Top Targets）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の（侵入イベントを発生させた接続で攻撃対象となった）上位のターゲットホスト（攻撃対象ホスト）のIPアドレスの侵入イベント数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフのデータは、主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

[入力/出力の上位セキュリティ ゾーン（Top Ingress/Egress Security Zones）] グラフ

[入力/出力の上位セキュリティ ゾーン（Top Ingress/Egress Security Zones）] グラフは棒グラフ形式で、モニタ対象ネットワーク上で設定されている各セキュリティゾーン（グラフ設定に応じて入力または出力）に関連付けられている侵入イベントの数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

ヒント　グラフに制約を適用して、出力セキュリティゾーンのトラフィックのみが表示されるようにするには、グラフにポインタを置き、表示されるトグルボタンの[出力（Egress）]をクリックします。デフォルト ビューに戻すには [入力（Ingress）] をクリックします。Context Explorer から外部への移動でも、グラフがデフォルトの [入力（Ingress）] ビューに戻ることに注意してください。

このグラフのデータは主に [侵入イベント（Intrusion Events）] 表から取得されます。

このグラフは、必要に応じて、入力（デフォルト）セキュリティゾーン情報または出力セキュリティ ゾーン情報のいずれかを表示するように設定できます。

侵入イベント詳細リスト

[侵入情報（Intrusion Information）] セクション下部に表示される [イベント詳細リスト（Event Details List）] は、モニタ対象ネットワークで検出された各侵入イベントの分類、推定優先度、イベント数の情報を示すテーブルです。イベントは、イベント数の降順でリストされます。

[イベント詳細リスト（Event Details List）] テーブルはソートできませんが、テーブルの項目をクリックして、その情報でフィルタリングまたはドリルダウンすることができます。このテーブルのデータは主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

[ファイル情報（Files Information）] セクション

Context Explorer の [ファイル情報（Files Information）] セクションには、6 つのインタラクティブ グラフが表示されます。これらのグラフは、モニター対象ネットワーク上のファイルとマルウェア イベントの概要を示します。

このうち 5 つのグラフには、（以前は AMP for Firepower と呼ばれていた）マルウェア防御 に関連するデータ（ネットワーク トラフィックで検出されたファイルのファイル タイプ、ファイル名、マルウェアの性質、これらのファイルを送信（アップロード）および受信（ダウンロード）したホスト）が表示されます。最後のグラフには、マルウェア防御 または Cisco Secure Endpoint のどちらで検出されたかにかかわらず、組織内で検出されたすべてのマルウェア脅威が表示されます。

（注）　侵入情報でフィルタリングすると、[ファイル情報（File Information）] セクション全体が非表示になります。

[上位のファイル タイプ（Top File Types）] グラフ

[上位のファイル タイプ（Top File Types）] グラフはドーナツ グラフ形式で、ネットワーク トラフィックで検出されたファイル タイプの割合のビュー（外側のリング）と、ファイル カテゴリのグループごとの割合のビュー（内側のリング）を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフに マルウェア防御 データを表示するには、マルウェア防御ライセンスが必要であることに注意してください。

このグラフのデータは主に [ファイル イベント（File Events）] 表から取得されます。

[上位のファイル名（Top File Names）] グラフ

[上位のファイル名（Top File Names）] グラフは棒グラフ形式で、ネットワーク トラフィックで検出された上位の一意のファイル名の数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフに マルウェア防御 データを表示するには、マルウェア防御ライセンスが必要であることに注意してください。

このグラフのデータは主に [ファイル イベント（File Events）] 表から取得されます。

[性質別ファイル（Files by Disposition）] グラフ

[上位のファイル タイプ（Top File Types）] グラフは円グラフ形式であり、（以前は AMP for Firepower と呼ばれていた）マルウェア防御 機能で検出されたファイルのマルウェアの性質の割合のビューを表示します。Secure Firewall Management Center がマルウェア クラウド検索を行ったファイルにのみ性質が設定されることに注意してください。クラウド検索をトリガーしなかったファイルには、`N/A` という性質が設定されます。`Unavailable` という性質は、Secure Firewall Management Center がマルウェア クラウド検索を実行できなかったことを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフに マルウェア防御 データを表示するには、マルウェア防御ライセンスが必要であることに注意してください。

このグラフのデータは主に [ファイル イベント（File Events）] 表から取得されます。

[送信ファイル数上位のホスト（Top Hosts Receiving Files）] グラフ

[送信ファイル数上位のホスト（Top Hosts Receiving Files）] グラフは棒グラフ形式で、ネットワーク トラフィックで検出された、送信ファイル数上位のホストの IP アドレスに関するファイルの数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

ヒント　グラフに制約を適用して、マルウェアを送信するホストだけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [マルウェア（Malware）] をクリックします。デフォルトのファイルのビューに戻すには[ファイル（Files）]をクリックします。Context Explorer から外部への移動でも、グラフがデフォルトのファイルのビューに戻ることに注意してください。

このグラフに マルウェア防御 データを表示するには、マルウェア防御ライセンスが必要であることに注意してください。

このグラフのデータは主に [ファイル イベント（File Events）] 表から取得されます。

[受信ファイル数上位のホスト（Top Hosts Receiving Files）] グラフ

[受信ファイル数上位のホスト（Top Hosts Receiving Files）] グラフは棒グラフ形式で、ネットワーク トラフィックで検出された、受信ファイル数上位のホストの IP アドレスに関するファイルの数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

ヒント　グラフに制約を適用して、マルウェアを受信するホストだけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [マルウェア（Malware）] をクリックします。デフォルトのファイルのビューに戻すには[ファイル（Files）]をクリックします。Context Explorer から外部への移動でも、グラフがデフォルトのファイルのビューに戻ることに注意してください。

このグラフに マルウェア防御 データを表示するには、マルウェア防御ライセンスが必要であることに注意してください。

このグラフのデータは主に [ファイル イベント（File Events）] 表から取得されます。

[上位のマルウェア検出（Top Malware Detections）] グラフ

[上位のマルウェア検出（Top Malware Detections）] グラフは棒グラフ形式で、マルウェア防御と Secure Endpoint のいずれによるものかに関係なく、組織で検出された上位のマルウェア脅威の数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフに マルウェア防御 データを表示するには、マルウェア防御ライセンスが必要であることに注意してください。

このグラフのデータは主に [ファイル イベント（File Events）] 表と [マルウェア イベント（Malware Events）] 表から取得されます。

[地理位置情報（Geolocation Information）] セクション

Context Explorer の [地理位置情報（Geolocation Information）] セクションには、3 つのインタラクティブなドーナツ グラフが表示されます。これらのグラフは、モニター対象ネットワークのホストがデータを交換している国の概要（イニシエータ国またはレスポンダ国ごとの固有接続数、送信元または宛先の国ごとの侵入イベント数、および送信側または受信側の国ごとのファイル イベント数）を示します。

[イニシエータ/レスポンダの国別接続（Connections by Initiator/Responder Country）] グラフの表示

[イニシエータ/レスポンダの国別接続（Connections by Initiator/Responder Country）] グラフはドーナツ グラフ形式であり、ネットワーク上での接続にイニシエータ（デフォルト）またはレスポンダとして関わる国の割合のビューを表示します。内側のリングでは、これらの国が大陸別にグループ化されています。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

ヒント　グラフに制約を適用して、接続でレスポンダとなっている国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [レスポンダ（Responder）] をクリックします。デフォルト ビューに戻すには [イニシエータ（Initiator）] をクリックします。Context Explorer から外部への移動でも、グラフがデフォルトの [イニシエータ（Initiator）] ビューに戻ることに注意してください。

このグラフのデータは主に [接続サマリー データ（Connection Summary Data）] テーブルから取得されます。

[送信元/宛先国別侵入イベント（Intrusion Events by Source/Destination Country）] グラフ

[送信元/宛先国別侵入イベント（Intrusion Events by Source/Destination Country）] グラフはドーナツ グラフ形式であり、ネットワーク上の侵入イベントにイベントの送信元（デフォルト）または宛先として関わる国の割合を表示します。内側のリングでは、これらの国が大陸別にグループ化されています。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

ヒント　グラフに制約を適用して、侵入イベントの宛先となっている国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [宛先（Destination）] をクリックします。デフォルト ビューに戻すには [送信元（Source）] をクリックします。Context Explorer から外部への移動でも、グラフがデフォルトの [送信元（Source）] ビューに戻ることに注意してください。

このグラフのデータは、主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

[送信側/受信側の国別ファイル イベント（File Events by Sending/Receiving Country）] グラフ

[送信側/受信側の国別ファイル イベント（File Events by Sending/Receiving Country）] グラフはドーナツ グラフ形式であり、ネットワーク上のファイルイベントでファイルの送信側（デフォルト）または受信側として検出された国の割合のビューを表示します。内側のリングでは、これらの国が大陸別にグループ化されています。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

ヒント　グラフに制約を適用して、ファイルを受信する国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [受信者（Receiver）] をクリックします。デフォルト ビューに戻すには [送信者（Sender）] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [送信者（Sender）] ビューに戻ることに注意してください。

このグラフのデータは主に [ファイル イベント（File Events）] 表から取得されます。

[URL 情報（URL Information）] セクション

Context Explorer の [URL 情報（URL Information）] セクションには、3 つのインタラクティブな棒グラフが表示されます。これらのグラフには、モニタ対象ネットワーク上のホストがデータを交換するために使用する URL の全体の概要（URL に関連付けられているトラフィックと固有接続数を個々の URL、URL カテゴリ、および URL レピュテーションでソートしたもの）が示されます。URL 情報でフィルタ処理を実行することはできません。

（注）　侵入イベントの情報でフィルタ処理を実行すると、[URL 情報（URL Information）] セクション全体が非表示になります。

このグラフで URL カテゴリとレピュテーションデータを含めるには、URL フィルタリング ライセンスを所有している必要があることに注意してください。

[URL 別トラフィック（Traffic by URL）] グラフ

[URL 別トラフィック（Traffic by URL）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最も要求される上位 15 の URL のネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされた URL ごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[URL 別トラフィック（Traffic by URL）] グラフは非表示になります。

このグラフで URL カテゴリとレピュテーションデータを含めるには、URL フィルタリングライセンスを所有している必要があることに注意してください。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルから取得されます。

[URL カテゴリ別トラフィック（Traffic by URL Category）] グラフ

[URL カテゴリ別トラフィック（Traffic by URL Category）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最も要求される URL カテゴリ（`Search Engines` や `Streaming Media` など）のネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされた URL カテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[URL カテゴリ別トラフィック（Traffic by URL Category）] グラフは非表示になります。

このグラフで URL カテゴリとレピュテーションデータを含めるには、URL フィルタリングライセンスを所有している必要があることに注意してください。

このグラフのデータは、主に [URL 統計（URL Statistics）] テーブルと [接続イベント（Connection Events）] テーブルから取得されます。

[URL レピュテーション別トラフィック（Traffic by URL Reputation）] グラフ

[URL レピュテーション別のトラフィック（Traffic by URL Reputation）] グラフは棒グラフ形式であり、モニター対象ネットワーク上の最も要求される URL レピュテーショングループ（Trusted や Neutral など）のネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。リストされた URL レピュテーションごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[URL レピュテーション別トラフィック（Traffic by URL Reputation）] グラフは非表示になります。

このグラフで URL カテゴリとレピュテーションデータを含めるには、URL フィルタリングライセンスを所有している必要があることに注意してください。

このグラフのデータは、主に[URL 統計（URL Statistics）]テーブルと [接続イベント（Connection Events）] テーブルから取得されます。

コンテキストエクスプローラの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- セキュリティ アナリスト（Security Analyst）

Context Explorer の更新

Context Explorer は、表示している情報を自動的に更新しません。新しいデータを組み込むには、Explorer を手動で更新する必要があります。

Context Explorer 自体をリロードすると（ブラウザ プログラムの更新または Context Explorer から外部へ移動した後に戻る操作など）、すべての表示情報が更新されますが、セクション設定（Ingress/Egress グラフや [アプリケーション情報（Application Information）] セクションなど）に対して行った変更は保持されず、また、読み込みに時間がかかることがある点に注意してください。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[分析（Analysis）] > [コンテキストエクスプローラ（Context Explorer）]**を選択します。

ステップ 2 右上にある [リロード（Reload）] をクリックします。

[リロード（Reload）] は、更新が終了するまでグレー表示になります。

Context Explorer の時間範囲の設定

過去 1 時間（デフォルト）から過去 1 年までの期間を反映するように、Context Explorer の時間範囲を設定できます。時間範囲を変更しても、Context Explorer は自動的に変更を反映する更新をしないことに注意してください。新しい時間範囲を適用するには、Explorer を手動で更新する必要があります。

時間範囲の変更は、Context Explorer から外部に移動したり、ログイン セッションを終了したりしても維持されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[分析（Analysis）] > [コンテキストエクスプローラ（Context Explorer）]**を選択します。

ステップ 2 [リストを表示（Show the last）] ドロップダウンリストから、時間範囲を選択します。

ステップ 3 オプションで、新しい時間範囲のデータを表示するには、[リロード（Reload）] をクリックします。

ヒント [フィルタの適用（Apply Filters）] をクリックすると、時間範囲の更新が適用されます。

Context Explorer のセクションの最小化および最大化

Context Explorer では 1 つ以上のセクションを最小化して非表示にできます。これは、特定のセクションだけを強調する場合や、ビューをシンプルにしたい場合に便利です。[トラフィックおよび侵入イベント数/時間（Traffic and Intrusion Event Counts Time）] グラフは最小化できません。

Context Explorer のセクションでは、ページを更新したり、アプライアンスからログアウトしたりしても、設定した最小化または最大化の状態が維持されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[分析（Analysis）] > [コンテキストエクスプローラ（Context Explorer）]**を選択します。

ステップ 2 セクションを最小化するには、セクションのタイトルバーにある **[折りたたみ矢印（Collapse Arrow）]**（▼） をクリックします。

ステップ 3 セクションを最大化するには、最小化されたセクションのタイトルバーにある最大化 **[展開矢印（Expand Arrow）]**（ ） をクリックします。

Context Explorer データのドリルダウン

Context Explorer で許容されている詳細レベルよりもさらに詳細にグラフを調べたりデータをリストしたりするには、当該データのテーブル ビューにドリルダウンします。（[経時トラフィックおよび侵入イベント（Traffic and Intrusion Events over Time）] グラフではドリル ダウンできないことに注意してください。）たとえば、[送信元 IP 別トラフィック（Traffic by Source IP）] グラフの IP アドレスでドリルダウンすると、[接続イベント（Connection Events）] 表の [アプリケーション詳細で接続（Connections with Application Details）] ビューが表示されます。このビューには、選択した送信元 IP アドレスに関連するデータのみが表示されます。

調べるデータのタイプに応じて、コンテキスト メニューに追加のオプションが表示されることがあります。特定の IP アドレスに関連付けられているデータ ポイントの場合、選択した IP アドレスのホストまたは whois 情報を表示するためのオプションが表示されます。特定のアプリケーションに関連付けられているデータ ポイントの場合、選択したアプリケーションに関するアプリケーション情報を表示するためのオプションが表示されます。特定のユーザーに関連付けられているデータ ポイントの場合、ユーザーのユーザー プロファイル ページを表示するためのオプションが表示されます。侵入イベントのメッセージに関連付けられているデータポイントの場合、そのイベントに関連する侵入ルールに関するルールドキュメントを表示するオプションが表示されます。特定の IP アドレスに関連付けられているデータポイントの場合、そのアドレスをブロックリストまたはブロックしないリストに追加するためのオプションが表示されます。これらのリストの詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの「グローバルおよびドメインのセキュリティ インテリジェンス リスト」を参照してください。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[分析（Analysis）] > [コンテキストエクスプローラ（Context Explorer）]**を選択します。

ステップ 2 [経時トラフィックおよび侵入イベント（Traffic and Intrusion Events over Time）] 以外の任意のセクションで、調査するデータポイントをクリックします。

ステップ 3 選択するデータ ポイントに応じて、表示されるオプションが異なります。

- テーブル ビューでこのデータの詳細を表示するには、[詳細な分析を表示（Drill into Analysis）] を選択します。
- 特定の IP アドレスに関連付けられているデータ ポイントを選択している場合に、関連するホストに関する詳細情報を参照するには、[ホスト情報の表示（View Host Information）] を選択します。

- 特定の IP アドレスのデータ ポイントを選択している場合に、そのアドレスで whois 検索を行うには、[Whois] を選択します。
- 特定のアプリケーションに関連付けられているデータ ポイントを選択している場合に、そのアプリケーションに関する詳細情報を参照するには、[アプリケーション情報の表示（View Application Information）] を選択します。
- 特定のユーザーに関連付けられているデータ ポイントを選択している場合に、そのユーザーに関する詳細情報を参照するには、[ユーザー情報の表示（View User Information）] を選択します。
- 特定の侵入イベント メッセージに関連付けらているデータ ポイントを選択している場合に、関連する侵入ルールに関する詳細情報を参照するには、[ルール ドキュメントの表示（View Rule Documentation）] を選択します。次に、必要に応じて、[ルール ドキュメント（Rule Documentation）] をクリックしてより具体的なルールの詳細を表示します。
- 特定の IP アドレスに関連付けられているデータポイントを選択している場合に、セキュリティインテリジェンスのグローバルのブロックリストまたはブロックしないリストにその IP アドレスを追加するには、該当するオプションを選択します。

コンテキスト エクスプローラのフィルタ

コンテキスト エクスプローラに最初に表示される基本的で広範なデータをフィルタリングして、ネットワーク上のアクティビティのより詳細な状況を把握することができます。フィルタは URL 情報以外のすべての種類のシステムデータに対応し、除外と包含がサポートされており、Context Explorer のグラフデータポイントをクリックするだけですぐに適用でき、Explorer 全体に反映されます。一度に最大 20 のフィルタを適用できます。

コンテキスト エクスプローラ データにフィルタを追加する方法はいくつかあります。

- [フィルタの追加（Add Filter）] ダイアログを使用する。
- コンテキストメニューを使用する（エクスプローラのデータ ポイントを選択する場合）。
- 特定の詳細表示ページ（[アプリケーションの詳細（Application Detail）]、[ホストプロファイル（Host Profile）]、[ルールの詳細（Rule Detail）]、[ユーザ プロファイル（User Profile）]）に表示されるテキストリンクを使用する。これらのリンクをクリックすると、コンテキストエクスプローラが自動的に開き、詳細表示ページの当該データに基づいてコンテキストエクスプローラがフィルタリングされます。たとえば、ユーザ `jenkins` のユーザ詳細ページで [コンテキスト エクスプローラ（Context Explorer）] リンクをクリックすると、エクスプローラにはそのユーザに関連するデータだけが表示されます。

ファイルタイプの中には、相互に互換性がないタイプがあります。たとえば、侵入イベント関連のフィルタ（**Device** や **Inline Result** など）を、接続イベント関連フィルタ（**Access Control Action** など）と同時に適用することはできません。これは、システムでは接続イベント データを侵入イベントデータによってソートできないためです。互換性のないフィルタの同時適用はシステムによって自動的に防止されます。互換性の問題が存在する場合、より後に適用された方のフィルタ タイプと互換性のないタイプのフィルタは非表示になります。

複数のフィルタがアクティブな場合、同じデータ タイプの値は OR 検索条件として扱われます。つまり、いずれか1つの値と一致するデータがすべて表示されます。異なるデータ タイプの値は AND 検索条件として扱われます。つまり、データは各フィルタ データ タイプの 1 つ以上の値と一致する必要があります。たとえば、`Application: 2channel`、`Application: Reddit`、および `User: edickinson` というフィルタ セットで表示されるデータは、ユーザ `edickinson` に関連付けられており、**かつ**アプリケーション `2channel` **または**アプリケーション `Reddit` に関連付けられている必要があります。

マルチドメイン展開では、先祖ドメインでコンテキストエクスプローラを表示している場合に複数の子孫ドメインでフィルタリングできます。この場合、**IP Address** フィルタも追加する場合は注意してください。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

表示されるデータは、管理対象デバイスのライセンスおよび展開方法やデータを提供する機能を設定するかどうかなどの要因によって異なります。

（注） フィルタは、必要とする正確なデータコンテキストをいつでも取得できるシンプルかつ俊敏性に優れたツールとして機能します。永続的に設定するものではなく、コンテキスト エクスプローラから外部に移動するか、セッションを終了すると消去されます。後で使用するためにフィルタ設定を保存するには、フィルタ処理されたコンテキスト エクスプローラ ビューの保存 （721 ページ）を参照してください。

データ タイプ フィールド オプション

次の表に、フィルタとして使用できるデータ タイプと、各データ タイプの例と説明を示します。

表 *62 :* フィルタ データ タイプ

タイプ	値の例	定義
アクセス コントロール アクション（Access Control Action）	`Allow`、`Block`	トラフィックを許可またはブロックするためにアクセス コントロール ポリシーにより実行されるアクション。
アプリケーション カテゴリ（Application Category）	`web browser`、`email`	アプリケーションの主要機能の一般的な分類。
アプリケーション	`Facebook`、`HTTP`	アプリケーションの名前。
アプリケーションのリスク（Application Risk）	`Very High`、`Medium`	アプリケーションの推定セキュリティ リスク。

タイプ	値の例	定義
アプリケーションタグ（Application Tag）	encrypts communications、sends mail	アプリケーションに関する追加情報。アプリケーションには任意の数のタグを使用できます（タグを使用しないことも可能です）。
アプリケーション タイプ（Application Type）	Client、Web Application	アプリケーション タイプ（アプリケーション プロトコル、クライアント、または Web アプリケーション）。
ビジネスとの関連性（Business Relevance）	Very Low、High	（娯楽ではない）ビジネス アクティビティに対するアプリケーションの推定関連度。
大陸（Continent）	North America、Asia	モニタ対象ネットワークで検出されたルーティング可能な IP アドレスに関連付けられている大陸。
国（Country）	Canada、Japan	モニタ対象ネットワークで検出されたルーティング可能な IP アドレスに関連付けられている国。
Device	device1.example.com、192.168.1.3	モニタ対象ネットワーク上のデバイスの名前または IP アドレス。
ドメイン（Domain）	Asia Division、Europe Division	グラフ表示するネットワーク アクティビティを行うデバイスのドメイン。このデータ タイプはマルチドメイン展開の場合にのみ存在します。
イベントの分類（Event Classification）	Potential Corporate Policy Violation、Attempted Denial of Service	侵入イベントの簡単な説明。侵入イベントをトリガーしたルール、デコーダ、またはプリプロセッサにより決定されます。
イベント メッセージ（Event Message）	dns response、P2P	イベントによって生成されるメッセージ。イベントをトリガーしたルール、デコーダ、またはプリプロセッサにより決定されます。
ファイルの性質	Malware、Clean	Secure Firewall Management Center によるマルウェア クラウド検索の実行対象ファイルの性質。
ファイル名	Packages.bz2	ネットワーク トラフィックで検出されたファイルの名前。
ファイル SHA256（File SHA256）	任意の 32 ビット文字列	Secure Firewall Management Center によるマルウェア クラウド検索の実行対象ファイルの SHA-256 ハッシュ値。
ファイル タイプ（File Type）	GZ、SWF、MOV	ネットワーク トラフィックで検出されたファイルのタイプ。
ファイル タイプ カテゴリ（File Type Category）	Archive、Multimedia、Executables	ネットワーク トラフィックで検出されたファイルのタイプの一般カテゴリ。

タイプ	値の例	定義
[IPアドレス（IP Address）]	`192.168.1.3`、`2001:0db8:85a3::0000/24`	IPv4 または IPv6 のアドレス、アドレス範囲、またはアドレス ブロック。 IPアドレスを検索すると、そのアドレスが送信元または宛先のいずれかになっているイベントが返されることに注意してください。
影響レベル（Impact Level）	`Impact Level 1`、`Impact Level 2`	モニタ対象ネットワークでのイベントの推定影響レベル。
インライン結果	`dropped`、`would have dropped`	トラフィックがドロップされたか、ドロップされた可能性があるか、またはシステムによりトラフィックが処理されていないかのいずれかです。
IOC カテゴリ（IOC Category）	`High Impact Attack`、`Malware Detected`	トリガーとして使用された侵害の兆候（IOC）イベントのカテゴリ。
IOC イベント タイプ（IOC Event Type）	`exploit-kit`、`malware-backdoor`	特定の侵害の兆候（IOC）に関連付けられている ID。その兆候をトリガーしたイベントを示します。
マルウェア脅威名（Malware Threat Name）	`W32.Trojan.a6b1`	マルウェア脅威の名前。
OS 名（OS Name）	`Windows`、`Linux`	オペレーティング システムの名前。
OS Version	`XP`、`2.6`	オペレーティング システムの特定のバージョン。
[プライオリティ（Priority）]	`high`、`low`	イベントの推定緊急度。
セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）	`Malware`、`Spam`	セキュリティ インテリジェンスにより判別される危険なトラフィックのカテゴリ。
セキュリティ ゾーン	`My Security Zone`、`Security Zone X`	トラフィックが分析されたインターフェイスのセット。インライン展開の場合は、トラフィックが通過するインターフェイスのセット。
SSL	`yes`、`no`	SSL暗号化トラフィックまたはTLS暗号化トラフィック。
ユーザ（User）	`wsmith`、`mtwain`	モニター対象ネットワーク上のホストにログインしたユーザーの ID。

[フィルタの追加（Add Filter）] ウィンドウからのフィルタの作成

この手順を使用して、[フィルタの追加（Add Filter）] ウィンドウでフィルタを最初から作成します。（コンテキストメニューを使用して、クイック フィルタを作成することもできます。）

コンテキストエクスプローラの左上にある [フィルタ（Filters）] の下の [プラス（Plus）]（＋）をクリックすると表示される [フィルタの追加（Add Filter）] ウィンドウには、次の 2 つのフィールドだけが表示されます。

- [データタイプ（Data Type）] ドロップダウンリストには、Context Explorer に制約を適用するために使用できる多数のデータタイプが含まれています。データ タイプの選択後に、そのタイプの固有の値を [フィルタ（Filter）] フィールドに入力します（たとえば、[大陸（Continent）] タイプの場合は値 [アジア（Asia）] など）。ユーザー支援のため、[フィルタ（Filter）] フィールドでは、選択したデータ タイプのさまざまな値の例がグレー表示で示されます。（フィールドにデータを入力すると、これらは消去されます。）
- [フィルタ（Filter）] フィールドには、イベント検索と同様に、* や ! などの特殊検索パラメータを入力できます。フィルタ パラメータの前に ! 記号を付けることで排他的なフィルタを作成できます。

（注） 追加したフィルタは自動的には適用されません。Context Explorer でフィルタを表示するには、[フィルタの適用（Apply Filters）] をクリックする必要があります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[分析（Analysis）] > [コンテキストエクスプローラ（Context Explorer）]** を選択します。

ステップ 2 左上にある [フィルタ（Filter）] の下で、[プラス（Plus）]（＋） をクリックします。

ステップ 3 [データ タイプ（Data Type）] ドロップダウンリストから、フィルタリングの条件として使用するデータ タイプを選択します。

ステップ 4 [フィルタ（Filter）] フィールドに、フィルタリングの条件として使用するデータ タイプ値を入力します。

ステップ 5 [OK] をクリックします。

ステップ 6 オプションで、前述の手順を繰り返し、必要なフィルタ セットが設定されるまで、フィルタを追加します。

ステップ 7 [フィルタの適用（Apply Filters）] をクリックします。

関連トピック

データ タイプ フィールド オプション （717 ページ）

検索の制約 （846 ページ）

コンテキスト メニューからのクイック フィルタの作成

Context Explorer のグラフとリスト データを詳しく調べるときに、データ ポイントをクリックし、コンテキストメニューを使用してそのデータに基づいてフィルタ（包含または除外）を簡単に作成できます。コンテキストメニューを使用して、[アプリケーション（Application）]、[ユーザー（User）]、[侵入イベントメッセージ（Intrusion Event Message）] データタイプの情報、あるいは任意の個別ホストでフィルタリングする場合、フィルタウィジェットには、そのデータタイプの該当する詳細ページ（アプリケーションデータの場合は [アプリケーションの詳細（Application Detail）] など）にリンクするウィジェット情報が表示されます。URL データではフィルタリングできないことに注意してください。

特定のグラフまたはリストのデータを詳しく調査する場合にもコンテキストメニューを使用できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[分析（Analysis）] > [コンテキストエクスプローラ（Context Explorer）]**を選択します。

ステップ 2 [一定期間のトラフィックおよび侵入イベント（Traffic and Intrusion Events over Time）] セクションと URL データを含むセクション以外の Explorer セクションで、フィルタリングするデータポイントをクリックします。

ステップ 3 次の 2 つの対処法があります。

- このデータにフィルタを追加するには、[フィルタの追加（Add Filter）] をクリックします。
- このデータに除外フィルタを追加するには、[除外フィルタの追加（Add Exclude Filter）] をクリックします。このフィルタが適用されると、除外された値に関連付けられて**いない**すべてのデータが表示されます。除外フィルタでは、フィルタ値の前に感嘆符（!）が表示されます。

フィルタ処理されたコンテキスト エクスプローラ ビューの保存

コンテキストエクスプローラから外部に移動した後、またはセッションを終了した後に、コンテキストエクスプローラのフィルタ設定を保持するには、適切なフィルタを適用したコンテキスト エクスプローラのブラウザ ブックマークを作成します。適用されるフィルタはコンテキスト エクスプローラ ページ URL に組み込まれているので、そのページのブックマークを読み込むと、対応するフィルタも読み込まれます。

手順

適切なフィルタが適用されたコンテキスト エクスプ ローラーのブラウザ ブックマークを作成します。

フィルタ データの表示

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[分析（Analysis）] > [コンテキストエクスプローラ（Context Explorer）]** を選択します。
ステップ 2 該当するフィルタウィジェットの**情報** をクリックします。

フィルタの削除

手順

ステップ 1 **[分析（Analysis）] > [コンテキストエクスプローラ（Context Explorer）]** を選択します。
ステップ 2 フィルタ処理ウィジェットを個別に削除するには、左上にある [フィルタ（Filters）] の下で、[閉じる（Close）]（×） をクリックします。

ヒント すべてのフィルタを一括削除するには、[クリア（Clear）] をクリックします。

第 23 章

統合イベント

次のトピックでは、統合イベントの使用方法について説明します。

統合イベントについて

統合イベントは、複数タイプのファイアウォールイベント（接続、侵入、ファイル、マルウェア、および一部のセキュリティ関連の接続イベント）の単一画面ビューを提供します。相互に関連付けられているイベントはテーブル内で一緒にスタックされ、セキュリティイベントに関する統合ビューと詳細なコンテキストが提供されます。[統合イベント（Unified Events）]テーブルに侵入イベントがある場合、その侵入イベントをクリックすると、関連付けられている接続イベントが強調表示されます。その後、複数のイベントビューアを切り替えることなく、接続イベントを侵入イベントと相関させて、ネットワークの問題をよりよく理解し、トラブルシューティングすることができます。

[統合イベント（Unified Events）]テーブルは、高度なカスタマイズが可能です。カスタムフィルタを作成して適用することにより、イベントビューアに表示される情報を微調整できます。統合イベントビューアには、特定のニーズに頻繁に使用するカスタムフィルタを保存し、保存したフィルタをすばやくロードするオプションもあります。また、列を追加または削除したり、列をピン留めしたり、列をドラッグして並べ替えたりすることで、イベントビューアテー

ブルを調整できます。Also, you can make a tailored event viewer table by adding or removing columns, pin columns, or drag and re-order the columns.

[統合イベント（Unified Events）] テーブルの [ライブビュー（Live View）] オプションを使用すると、ファイアウォールイベントをリアルタイムで表示し、ネットワーク上のアクティビティをモニターすることができます。たとえば、ファイアウォール管理者の場合、ポリシーの変更後にイベントの更新をリアルタイムで表示すると、ポリシーの変更がネットワークに正しく適用されていることを確認するために役立ちます。

統合イベントの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- セキュリティ アナリスト（Security Analyst）

統合イベントビューアでの作業

複数のイベントビューアを切り替えることなく、さまざまなタイプのファイアウォールイベントを 1 つのテーブルで表示および操作できます。

次のことを行うには、このビューを使用します。

- 異なるタイプのイベント間の関係を統合ビューで表示する。
- ポリシー変更の影響をリアルタイムで確認する。

始める前に

このタスクを実行するには、管理者 または セキュリティ アナリスト（Security Analyst） 権限が必要です。

手順

ステップ 1 [分析（Analysis）] > [統合イベント（Unified Events）]を選択します。

ステップ 2 時間範囲（固定またはスライド）を選択します。詳細については、「統合イベントビューアでの時間範囲の設定」を参照してください。

ステップ 3 Secure Network Analytics アプライアンスにリモートでイベントを保存していて、データソースを変更する正当な理由がある場合は、データソースを選択します。「Secure Network Analytics アプライアンスに保存されている接続イベントを使用した Secure Firewall Management Center での作業」で重要な情報を参照してください。

ステップ 4 統合イベントビューアが最初に表示するファイアウォールイベントの膨大なリストをフィルタ処理して、ネットワーク内のイベントのより詳細な状況を把握できます。詳細については、「統合イベントビューアのフィルタ」を参照してください。

ステップ 5 その他のオプションの選択：

目的	操作手順
列のカスタマイズ	• 列の追加または削除： 列ピッカー（）をクリックして、列を選択します。一部のフィールドの値は、イベントタイプによって異なります。各フィールドの横に表示される以下のアイコンは、対応するイベントタイプを示します。 • 接続イベント（（）） • セキュリティ関連の接続イベント（） • 侵入イベント（（）） • ファイルイベント（（）） • マルウェアイベント（（）） 列セットフィルタ処理オプションの横にあるイベントアイコンをクリックして、選択したイベントタイプに従ってイベントフィールドのリストをフィルタ処理します。 （注） 多くの列を含めると、パフォーマンスが低下する可能性があります。イベント行を展開してイベントの詳細を表示すると、非表示の列のデータを表示できます。 • 列の順序変更： 列の見出しをドラッグアンドドロップします。 • 列がスクロールしないようにするための、テーブルの左側または右側での列の固定（静止）： 列をテーブルの左まで右側までドラッグします。 または、列の見出しを固定エリアにドラッグアンドドロップします。 列の固定を解除するには、列を固定エリアの外にドラッグします。 • 列のサイズを変更します。 • 列をデフォルトの設定に戻します。 • 列の設定を保存します。詳細については、「統合イベントビューアでの列セットの保存」を参照してください。 データは常に時間順に並べ替えられ、最新のイベントが上に表示されます。

目的	操作手順
関連イベントの特定	行をクリックして、このイベントに関連する他のイベントを強調表示します。 必要に応じて、イベントをフィルタして、十分に少ないイベントのセットを表示します。 （注） 接続のイニシエータは、マルウェアファイルの送信者と同じである必要はありません。[送信元または宛先IP（Source or Destination IP）] フィルタを使用して統合イベントビューアをフィルタ処理することにより、接続イベントに関連付けられているファイルまたはマルウェアイベントを検索します。
イベントの詳細の表示	行の左端にある [>]（展開）アイコンをクリックします。イベントの詳細には、表示するデータがないフィールドは含まれません。 ヒント または、イベント行をダブルクリックして、[イベントの詳細（Event Details）]ペインを表示します。[イベントの詳細（Event Details）]ペインが開いている場合は、テーブル内の任意のイベント行をクリックして、そのイベントの詳細をロードします。
パケットトレーサを使用したイベントのトラブルシューティング	1. パケットトレースを実行する行の横にある省略記号アイコン（ ⋮ ）をクリックします。 2. [パケットトレーサで開く（Open in Packet Tracer）] を選択して、イベントの送信元アドレスと宛先アドレス、およびプロトコル特性に基づいてパケットトレーサツールでパケットをシミュレーションします。シミュレーションしたパケットをトレースし、トレース結果を使用してセキュリティイベントのトラブルシューティングを行います。パケットトレーサツールの使用方法の詳細については、パケット トレーサの使用 （546 ページ）を参照してください。
リアルタイムでのイベントの表示	[ライブ表示（Go Live）] をクリックします。詳細については、「統合イベントビューアでのイベントのライブビュー」を参照してください。 イベントのストリームが速すぎる場合は、フィルタ基準を入力します。
外部リソースへの相互起動	テーブルセルの省略記号 （⋮） をクリックすると、そのセル値に使用可能なオプションが表示されます（存在する場合）。 詳細については、Web ベースのリソースを使用したイベントの調査（763 ページ）を参照してください。

目的	操作手順
複数の統合イベントビューアのタブ/ウィンドウを開く	• 複数のブラウザのタブまたはウィンドウを使用して、統合イベントビューアのさまざまなビューを表示できます。 • 新しいタブまたはウィンドウには、最後に変更されたタブ/ウィンドウの特性があります。 • 開いているタブ/ウィンドウをテンプレートにするには、それに対して小さな変更を加えます。 • システムは、複数のタブのクエリを順番に処理します。 • ビューによっては（複雑なクエリや、着信イベントレートが高い場合のライブビューモードでの表示など）、4 つより多くのタブが同時に開かれていると、パフォーマンスが低下する場合があります。
検索の保存	カスタム検索をお気に入りとして保存し、後ですばやくロードできます。詳細については、「統合イベントビューアでの検索の保存」を参照してください。
クエリ結果のブックマークまたは共有	ブラウザウィンドウでURLをブックマークするか、コピーして貼り付けます。 • スライド時間範囲が使用されている場合、URL では後で異なるイベントが取得されます。 • 列の可視性、サイズ、順序、およびリアルタイムストリーミング設定は、URL にキャプチャされません。

統合イベントビューアでの時間範囲の設定

特定期間のファイアウォールイベントを表示するには、統合イベントビューアで時間範囲を設定します。時間範囲を変更すると、統合イベントビューアが自動的に更新され、変更が反映されます。

選択した時間範囲は、イベントビューアの他のテーブルには適用されません。たとえば、接続イベントを表示するときに選択した時間範囲は統合イベントビューアには適用されず、その逆も同様です。

重要 時間枠が接続イベントの保持期間を超える場合は、**[分析（Analysis）]**>**[接続（Connections）]**>**[セキュリティ関連の接続イベント（Security-Related Connection Events）]** のテーブルでセキュリティ関連の接続イベントを探します。

始める前に

このタスクを実行するには、管理者 権限または セキュリティ アナリスト（Security Analyst）権限が必要です。

手順

ステップ 1 **[分析（Analysis）]** > **[統合イベント（Unified Events）]** を選択します。

デフォルトでは、統合イベントビューアには、過去 1 時間のイベントが表示されます。

ステップ 2 現在の時間範囲をクリックします。

ステップ 3 次のいずれかを選択します。

- 固定時間範囲のイベントを表示する場合は、[固定時間範囲（Fixed Time Range）] をクリックし、[開始時刻（Start time）] と [終了時刻（End time）] を選択します。

  ヒント [終了時刻（End time）] を現在の時刻に素早く設定するには、[現在（Now）] をクリックします。

- 指定された長さのスライドするデフォルト時間枠を設定する場合は、[スライド時間枠（Sliding Time Range）] をクリックします。

  アプライアンスは、特定の開始時刻（たとえば1時間前）から現在までに生成されたすべてのイベントを表示します。イベントビューを更新すると時間枠がスライドして、常に最後の 1 時間内のイベントが表示されます。

ステップ 4 [Apply] をクリックします。

統合イベントビューアでのイベントのライブビュー

イベントビューアを手動で更新しなくてもファイアウォールイベントがリアルタイムで表示されるように統合イベントビューアを設定します。[ライブビュー（Live View）] モードでは、ネットワークでセキュリティイベントが発生すると、イベントログがリアルタイムで表示されるため、問題のトラブルシューティングに役立ちます。

始める前に

このタスクを実行するには、管理者 権限または セキュリティ アナリスト（Security Analyst）権限が必要です。

手順

ステップ 1 **[分析（Analysis）] > [統合イベント（Unified Events）]** を選択します。

デフォルトでは、統合イベントビューアには、過去 1 時間のイベントが表示されます。

ステップ 2 ライブイベント更新を表示するには、[ライブに移行（Go Live）] をクリックします。

新しいイベントは、イベントテーブルの一番上に表示されます。時間範囲セクションには、統合イベントビューアのライブ期間を通知するタイマーが表示されます。

次のタスク

ライブビューモードを終了するには、[ライブ（Live）] をクリックします。

統合イベントビューアのフィルタ

統合イベントビューアには、最初に過去1時間の複数タイプのファイアウォールイベントが表示されます。[統合イベント（Unified Events）] のデフォルトビューをフィルタ処理して、ネットワーク上のアクティビティのより詳細な状況を把握することができます。フィルタは、排他フィルタ条件と包含フィルタ条件をサポートしています。

フィルタを使用すると、重要な情報にすばやくアクセスできます。たとえば、ファイアウォール管理者は、特定のアプリケーションへのアクセスを一部のユーザーに許可または拒否する場合、ファイアウォールログをスキャンするようにユーザー検索条件を設定できます。イベントビューアに、検索条件に一致するイベントログが表示されます。

始める前に

次のタスクを実行するには、管理者 権限または セキュリティ アナリスト（Security Analyst）権限が必要です。

手順

ステップ 1 [分析（Analysis）] > [統合イベント（Unified Events）]を選択します。

ステップ 2 フィルタ条件を入力します。

- フィルタ条件を手動で入力するには、検索テキストフィールドに正確な条件を入力するか、ドロップダウンリストから条件を選択します。その後、フィルタ条件の値を指定します。値を入力する際、可能な場合は常に、ドロップダウンリストに候補が表示されます。
- テーブル内のイベントのセル内のドットをクリックし、その値をフィルタ基準に含めるか除外するオプションを選択します。

  ヒント
  - 包含フィルタ条件をすばやく追加するには、**Ctrl キーを押しながらクリック**（Windows）するか **Command キーを押しながらクリック**（Mac）します。
  - 排他フィルタ条件をすばやく追加するには、**Alt キーを押しながらクリック**（Windows）するか **Option キーを押しながらクリック**（Mac）します。

- フィルタ基準を絞り込みます。ワイルドカードと検索の動作に関する重要な情報については、イベントの検索 （845 ページ）を参照してください。
- 値フィールドの値の前に、演算子（<、>、！など）を含めます。たとえば、[アクション（Action）] フィールドに `!Allow` と入力して、Allow 以外のアクションを持つすべてのイベントを検索します。

ステップ 3 検索を実行します。

ヒント **Ctrl キーを押しながら Enter キーを押す**（Windows）か **Command キーを押しながら Enter キーを押す**（Mac）ことで、検索を開始できます。

統合イベントビューアのイベントは、表示されたすべての列が同じ値を保持している場合は、集約されません。フィルタ基準に一致するすべてのイベントが個別に表示されます。

次のタスク

カスタムフィルタを保存するには、トピック「統合イベントビューアでの検索の保存」を参照してください。

統合イベントビューアでの検索の保存

始める前に

検索を保存するには、管理者 または セキュリティ アナリスト（Security Analyst） 権限が必要です。

手順

ステップ 1 [分析（Analysis）] > [統合イベント（Unified Events）]を選択します。

ステップ 2 「統合イベントビューアのフィルタ」統合イベントビューアのフィルタ （730ページ） トピックの説明に従って、検索条件を確立します。

ステップ 3 検索テキストボックスの [お気に入り検索（Favorite Search）]（☆）アイコンをクリックします。

ステップ 4 次のいずれかを実行します。

- 新しい検索を保存するには、検索名を指定し、[新規として保存（Save as new）] をクリックします。
- 保存済みの検索を上書きするには、上書きする保存済み検索で [編集（Edit）] をクリックし、[上書き（Overwrite）] をクリックします。

次のタスク

保存した検索をロードするには、トピック「統合イベントビューアでの保存済み検索のロード」を参照してください。

統合イベントビューアでの保存済み検索のロード

始める前に

- このタスクを実行するには、管理者 または セキュリティ アナリスト（Security Analyst）権限が必要です。
- 「統合イベントビューアでの検索の保存」トピックの説明に従って、保存された検索を作成します。

手順

ステップ 1 **[分析（Analysis）] > [統合イベント（Unified Events）]** を選択します。

ステップ 2 検索テキストボックスの [お気に入り検索（Favorite Search）]（☆）アイコンをクリックします。

ステップ 3 ロードする保存済み検索をクリックします。

統合イベントビューアでの列セットの保存

始める前に

列セットを保存するには、管理者 または セキュリティ アナリスト（Security Analyst） 権限が必要です。

手順

ステップ 1 **[分析（Analysis）] > [統合イベント（Unified Events）]** を選択します。

ステップ 2 列ピッカーアイコン（）をクリックし、保存する列のセットを選択します。

ステップ 3 お気に入り列セット（☆）アイコンをクリックします。

ステップ 4 次のいずれかを実行します。

- 新しい列セットを保存するには、列セット名を指定し、[新規として保存（Save as new）] をクリックします。
- お気に入りの列セットを上書きするには、上書きする列セットで[編集（Edit）] （）をクリックし、[上書き（Overwrite）] をクリックします。

次のタスク

保存された列セットをロードするには、「統合イベントビューアでの保存済み列セットのロード」トピックを参照してください。

統合イベントビューアでの保存済み列セットのロード

始める前に

- このタスクを実行するには、管理者 権限またはセキュリティ アナリスト（Security Analyst） 権限が必要です。
- 「統合イベントビューアでの列セットの保存」トピックの説明に従って、お気に入りの列セットを保存します。

手順

ステップ 1 **[分析（Analysis）] > [統合イベント（Unified Events）]** を選択します。

ステップ 2 列ピッカーアイコン（）をクリックします。

ステップ 3 [お気に入りの列セット（Favorite column sets）] アイコン（☆）をクリックします。
ステップ 4 ロードする列セットをクリックします。

統合イベントビューアのカラムの説明

一部のフィールドの値は、イベントタイプによって異なります。デフォルトフィールドのフィールド対応は次のとおりです。

統合イベントビューアのフィールド名	接続イベントまたはセキュリティインテリジェンスイベントのフィールド名	侵入イベントのフィールド名	ファイルイベントのフィールド名	マルウェアイベントのフィールド名
時刻（Time）	最初のパケット（First Packet） 次の（注）を参照してください。	時刻（Time）	時刻（Time）	時刻（Time）
イベント タイプ	--	--	--	--
アクション（Action）	操作	インライン結果	操作	操作
理由	理由	理由	（非該当）	（非該当）
ソース IP（Source IP）	[イニシエータ IP（Initiator IP）]	ソース IP（Source IP）	送信側 IP（Sending IP）	送信側 IP（Sending IP）
宛先 IP（Destination IP）	レスポンダ IP（Responder IP）	宛先 IP（Destination IP）	受信側 IP（Receiving IP）	受信側 IP（Receiving IP）
送信元ポート/ICMP タイプ（Source Port/ICMP Type）	送信元ポート（Source Port）	送信元ポート（Source Port）	送信側のポート（Sending Port）	送信側のポート（Sending Port）
送信先ポート/ICMP タイプ（Destination Port/ ICMP Type）	宛先ポート	宛先ポート	受信側のポート（Receiving Port）	受信側のポート（Receiving Port）

統合イベントビューアのフィールド名	接続イベントまたはセキュリティインテリジェンスイベントのフィールド名	侵入イベントのフィールド名	ファイルイベントのフィールド名	マルウェアイベントのフィールド名
[Webアプリケーション（Web Application）]	Web アプリケーション	Web アプリケーション	Web アプリケーション	Web アプリケーション
Rule	アクセス コントロール ルール（Access Control Rule）	アクセス コントロール ルール（Access Control Rule）	（非該当）	（非該当）
ポリシー	アクセス コントロール ポリシー（Access Control Policy）	侵入ポリシー（Intrusion Policy）	ファイルポリシー（File Policy）	ファイルポリシー（File Policy）
Device	Device	Device	Device	デバイス

列ピッカー（▥）アイコンをクリックして、すべてのイベントフィールドとその対応関係を表示します。

フィールドの説明については、次のトピックを参照してください。

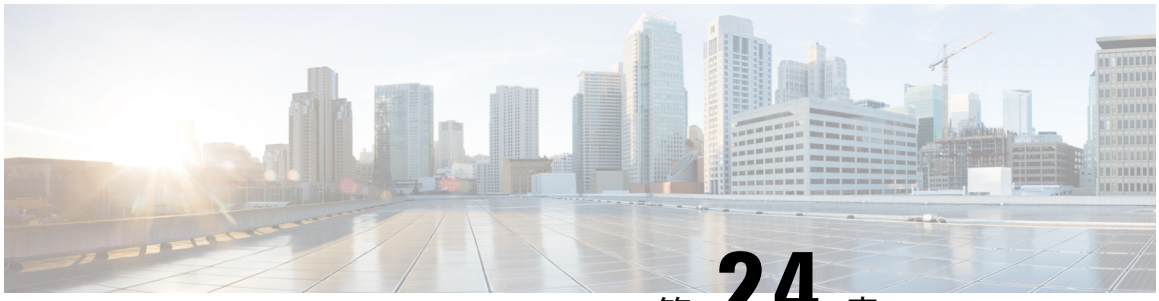
- 接続およびセキュリティ関連の接続イベントフィールド （902 ページ）
- 侵入イベント フィールド （948 ページ）
- ファイルおよびマルウェア イベント フィールド （1011 ページ）

イニシエータ/レスポンダ、送信元/接続先、および送信者/受信者フィールドに関する注意（922 ページ）も参照してください。

（注） 接続の開始時にロギングを有効にしていない場合でも、システムはこの値を持ち、統合イベントビューアの時間フィールドとして使用します。接続の開始時と終了時に接続イベントがログに記録されたかどうかを判断するには、イベントの行を展開して詳細を表示します。接続の両端がログに記録されている場合は、[最後のパケット（Last Packet）] フィールドが表示されます。

統合イベントの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
統合イベントビューアのパケットトレーサ	7.4.1	任意（Any）	[統合イベントビューア（Unified Event Viewer）] ページからパケットトレーサを開いて、セキュリティイベントをトラブルシューティングできるようになりました。 パケットトレースを実行するイベントの横にある省略記号アイコン（⋮）（[展開（Expand）]）をクリックし、[パケットトレーサで開く（Open in Packet Tracer）] をクリックします。
統合イベントビューアの改善	7.4	任意（Any）	お気に入りの列セットの保存と検索機能の改善。
お気に入りの検索を保存する	7.3	任意（Any）	列セットと検索をお気に入りとして保存し、後ですばやく起動できます。
統合イベントビューア	7.0	任意（Any）	接続（セキュリティインテリジェンスを含む）、侵入、ファイル、マルウェアの複数のイベントタイプを 1 つのテーブルで表示および操作します。 新規/変更されたページ：**[分析（Analysis）]** > **[統合イベント（Unified Events）]** の新しいページ。 サポートされているプラットフォーム： Management Center



第 24 章

ネットワークマップ

ここでは、ネットワーク マップの使用方法について説明します。

ネットワークマップの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

リーフ

ユーザの役割

- 管理者
- 検出管理者（Discovery Admin）

ネットワーク マップ

システムは、ネットワークを通じて送信されるトラフィックをモニターし、トラフィックデータを復号化してから、設定されているオペレーティングシステムおよびフィンガープリントとそのデータを比較します。このシステムでは、次にそのデータを使用して、ネットワーク マップというネットワークの詳細な表示を生成します。マルチドメイン展開では、システムはリーフ ドメインごとの個々のネットワーク マップを生成します。

システムは、ネットワーク検出ポリシーのモニタリングで特定された管理対象デバイスからデータを収集します。管理対象デバイスでは、モニタされたトラフィックから直接ネットワー

ク アセットを検出したり、処理された NetFlow レコードから間接的にネットワーク アセットを検出したりします。複数のデバイスで同じネットワーク アセットを検出した場合、システムではそれらの情報をまとめてそのアセットの複合表示を生成します。

パッシブ検出からのデータを補完するには、次のようにします。

- オープンソースの Nmap™ スキャナを使用してホストをアクティブにスキャンして、そのスキャン結果をネットワーク マップに追加します。
- ホスト入力機能を使用して、サードパーティ製のアプリケーションからホストデータを手動で追加できます。

ネットワーク マップには、検出されたホストとネットワーク デバイスの観点から見たネットワーク トポロジが表示されます。

ネットワーク マップを使用すれば、次のことを行えます。

- ネットワークの全体的なビューを即座に入手できます。
- 実行する分析に適したさまざまなビューを選択できます。ネットワーク マップの各ビューの形式は、展開可能なカテゴリおよびサブカテゴリを持つ階層ツリーからなる、同一の形式です。カテゴリをクリックすると、展開して、その下のサブカテゴリが表示されます。
- カスタム トポロジ機能を使用してサブネットを整理して識別できます。たとえば、組織の各部署が異なるサブネットを使用している場合、カスタム トポロジ機能を使用して、それらのサブネットに分かりやすいラベルを割り当てることができます。
- 任意のモニタ対象ホストのホスト プロファイルにドリルダウンすれば、詳細情報を表示できます。
- アセットの調査が不要になった場合は、そのアセットを削除できます。

（注） システムは、ネットワーク マップから削除されたホストに関連付けられているアクティビティを検出した場合、そのホストをネットワーク マップに再度追加します。同様に、削除されたアプリケーションは、システムでアプリケーションの変更（たとえば、Apache Web サーバが新しいバージョンにアップグレードされた場合）を検出すると、ネットワーク マップに再度追加されます。システムが特定のホストを脆弱にする変更を検出した場合、それらのホストの脆弱性が再びアクティブにされます。

ヒント ネットワーク マップからホストまたはサブネットを永続的に除外するには、ネットワーク検出ポリシーを変更します。ロード バランサおよび NAT デバイスで過剰なイベントまたは無関係なイベントを生成していることが判明した場合は、それらのデバイスをモニタリングから除外することができます。

ホスト ネットワーク マップ

[ホスト（Hosts）] タブのネットワーク マップには、ホスト数と、ホストの IP アドレスと プライマリ MAC アドレスのリストが表示されます。各アドレスまたはアドレスの一部は、次のレベルへのリンクです。このネットワーク マップ ビューは、ホストに 1 つの IP アドレスまたは複数の IP アドレスがあるかを問わず、システムによって検出されたすべての一意のホスト数を表示します。

ホストのネットワーク マップを使用して、サブネットによって階層ツリーに整理されたネットワークのホストを参照でき、特定のホストのホスト プロファイルにドリルダウンできます。

システムは、エクスポートされた NetFlow レコードからネットワークマップにホストを追加できますが、これらのホストに使用できる情報は限られます（NetFlow データと管理対象デバイス データの違いを参照）。

ネットワークのカスタム トポロジを作成して、サブネットに意味のあるラベル（部門名など）を割り当てることができます。これはホストのネットワーク マップで表示されます。また、カスタム トポロジで指定した組織に基づいてホストのネットワーク マップを表示することもできます。

ホストのネットワーク マップからネットワーク全体、サブネット、または個々のホストを削除できます。ホストがネットワークに接続されていないことがわかっている場合など、分析を効率化するために削除できます。システムは削除されたホストに関連付けられたアクティビティを後で検出すると、ネットワーク マップにホストを再追加します。ネットワーク マップからホストまたはサブネットを永続的に除外するには、ネットワーク検出ポリシーを変更します。

⚠

注意 ネットワーク デバイスをネットワーク マップから削除しないでください。システムがネットワーク トポロジを判断するために必要です。

ホストのネットワーク マップのページではプライマリ MAC アドレスのみを検索でき、ホストの [MAC] カウンタにはプライマリ MAC アドレスのみが含まれます。プライマリおよびセカンダリ MAC アドレスの説明については、ホスト プロファイルの基本ホスト情報（1050 ページ）を参照してください。

ネットワーク デバイスのネットワーク マップ

[ネットワーク デバイス（Network Devices）] タブのネットワーク マップには、ネットワークの 1 つのセグメントを別のセグメントに接続するネットワーク デバイス（ブリッジ、ルータ、NAT デバイス、およびロード バランサ）が表示されます。このマップには、IP アドレスで特定されたデバイスと、MAC アドレスで特定されたデバイスがリストされる 2 つのセクションがあります。

また、このマップには、デバイスに保持されている IP アドレスが 1 つか複数かに関係なく、システムによって検出されたすべての一意のネットワーク デバイスの数も表示されます。

ネットワークのカスタム トポロジを作成した場合、サブネットに割り当てられているラベルがネットワーク デバイスのネットワーク マップに表示されます。

ネットワーク デバイスを識別するためにシステムで使用される方法には、次のものがあります。

- Cisco Discovery Protocol（CDP）メッセージの分析。ネットワーク デバイスとそれらのタイプを識別できます（シスコ デバイスのみ）。
- スパニング ツリー プロトコル（STP）の検出。デバイスをスイッチまたはブリッジとして識別します。
- 同じ MAC アドレスを使用している複数のホストの検出。MAC アドレスを、ルータに属しているものとして識別します。
- クライアント側からの TTL 値の変更、または通常のブート時間よりも頻繁に変更されている TTL 値の検出。この検出では、NAT デバイスとロード バランサを識別します。

ネットワーク デバイスが CDP を使用して通信している場合、1 つ以上の IP アドレスを保持している可能性があります。ネットワーク デバイスが STP を使用して通信している場合は、1 つの MAC アドレスのみを保持している可能性があります。

ネットワーク デバイスをネットワーク マップから削除することはできません。これは、システムでそれらの場所を使用してネットワーク トポロジを判断するためです。

ネットワーク デバイスのホスト プロファイルには、[オペレーティング システム（Operating Systems）] セクションではなく [システム（Systems）] セクションがあります。このセクションには、ネットワーク デバイスの背後で検出されたモバイル デバイスすべてのハードウェア プラットフォームが反映された [ハードウェア（Hardware）] 列が含まれています。[システム（Systems）] の下にハードウェア プラットフォームの値が表示された場合、システムでは、ネットワーク デバイスの背後で検出された 1 つ以上のモバイル デバイスを示します。モバイル デバイスはハードウェア プラットフォームの情報を持っていることも、持っていないこともありますが、モバイル デバイスではないシステムではハードウェア プラットフォーム情報は検出されないことに注意してください。

モバイル デバイスのネットワーク マップ

[モバイル デバイス（Mobile Devices）] タブのネットワーク マップには、ネットワークに接続されているモバイル デバイスが表示されます。また、このネットワーク マップには、デバイスに設定されている IP アドレスが 1 つか複数かに関係なく、システムによって検出されたすべての一意のモバイル デバイスの数も表示されます。

各アドレスまたはアドレスの一部分は、次のレベルへのリンクです。また、サブネットまたは IP アドレスを削除することもできます。そして、システムでそのデバイスを再検出すると、そのデバイスをネットワーク マップに再度追加します。

さらに、ドリルダウンしてモバイル デバイスのホスト プロファイルを表示することもできます。

モバイル デバイスを特定するために、システムでは次のことを行います。

- モバイル デバイスのモバイル ブラウザからの HTTP トラフィック内のユーザ エージェントの文字列を分析します。

- 特定のモバイル アプリケーションの HTTP トラフィックをモニタします。

ネットワークのカスタム トポロジを作成した場合、サブネットに割り当てられているラベルがモバイル デバイスのネットワーク マップに表示されます。

侵害の兆候のネットワーク マップ

[侵害の兆候（Indications of Compromise）] タブのネットワーク マップには、ネットワーク上で侵害されたホストが IOS カテゴリ別に編成されて表示されます。影響を受けているホストは各カテゴリの下に表示されます。各アドレスまたはアドレスの一部は、次のレベルへのリンクです。

[侵害の兆候（Indications of Compromise）] タブのネットワーク マップから、何らかのセキュリティ侵害を受けたと判断される各ホストのホスト プロファイルを表示できます。さらに、IOC カテゴリまたは特定のホストを削除でき（解決済みにする）、これによって当該ホストから IOC タグが削除されます。たとえば、問題が対応済みで、繰り返し発生する可能性が低いと判断した場合に、IOC カテゴリをネットワーク マップから削除できます。

ネットワーク マップのホストや IOC カテゴリを解決済みにしても、ネットワークからは削除されません。システムがその IOC をトリガーする情報を新たに検出すると、解決済みのホストまたは IOC カテゴリはネットワーク マップに再表示されます。

侵害の兆候をシステムがどのように判断しているかの詳細については、侵害の兆候データ （1107 ページ）とサブトピックを参照してください。

アプリケーション プロトコルのネットワーク マップ

[アプリケーション プロトコル（Application Protocols）] タブのネットワーク マップには、ネットワークで稼働しているアプリケーションが、アプリケーション名、ベンダー、バージョン、各アプリケーションを実行しているホストを基準とした階層ツリー形式で表示されます。

システムが検出するアプリケーションは、システム ソフトウェアや VDB が更新された場合や、アドオン ディテクタをインポートした場合に変わることがあります。各システムまたは VDB アップデートのリリース ノートまたはアドバイザリ テキストには、新規および更新されたディテクタの情報が含まれています。ディテクタを網羅した最新のリストについては、Cisco のサポート サイト（http://www.cisco.com/cisco/web/support/index.html）を参照してください。

このネットワーク マップから、特定のアプリケーションを実行している各ホストのホスト プロファイルを確認できます。

また、アプリケーションのカテゴリ、すべてのホストで実行されているアプリケーション、あるいは特定のホストで実行されているアプリケーションを削除することもできます。たとえば、あるアプリケーションがホスト上で無効化されているとわかっており、システムによる影響レベルの認定で使用されないようにする場合は、そのアプリケーションをネットワーク マップから削除します。

ネットワーク マップからアプリケーションを削除しても、ネットワークからは削除されません。削除したアプリケーションは、システムがアプリケーションの変更（たとえば Apache Web

サーバが新しいバージョンにアップグレードされた）を検出するか、ユーザがシステムの検出機能を再起動すると、ネットワーク マップに再表示されます。

何を削除するかによって、動作は次のように異なります。

- アプリケーション カテゴリ：アプリケーション カテゴリを削除すると、そのアプリケーション カテゴリがネットワーク マップから除去されます。削除したカテゴリの下にあるすべてのアプリケーションは、そのアプリケーションを含むすべてのホスト プロファイルから削除されます。

  たとえば、[http] を削除した場合、[http] として示されるすべてのアプリケーションがすべてのホスト プロファイルから削除され、[http] はネットワーク マップのアプリケーション ビューに表示されなくなります。

- 特定のアプリケーション、ベンダー、バージョン：これらの要素を削除すると、関連するアプリケーションがネットワーク マップから除去され、そのアプリケーションを含むホスト プロファイルからもアプリケーションが除去されます。

  たとえば、[http] カテゴリを展開し、[Apache] を削除すると、[Apache] としてリストされているすべてのアプリケーションは、[Apache] の下にリストされているバージョンを問わず、それらを含むホスト プロファイルから削除されます。同様に、[Apache] を削除する代わりに、特定のバージョン（[1.3.17] など）を削除すると、影響を受けるホスト プロファイルから、選択されたバージョンだけが削除されます。

- 特定の IP アドレス：IP アドレスを削除すると、その IP アドレスがアプリケーション リストから除去され、選択した IP アドレスのホスト プロファイルからアプリケーション自体が除去されます。

  たとえば、[http]、[Apache]、[1.3.17 (Win32)] の順に展開し、[172.16.1.50:80/tcp] を削除すると、Apache 1.3.17（Win32）アプリケーションは IP アドレス 172.16.1.50 のホスト プロファイルから削除されます。

[脆弱性（Vulnerabilities）] のネットワーク マップ

[脆弱性（Vulnerabilities）] タブのネットワークマップには、システムによってネットワークで検出された脆弱性がレガシーの脆弱性 ID（SVID）、CVE ID、または [Snort ID] ごとに編成されて表示されます。

このネットワーク マップから、特定の脆弱性の詳細、および特定の脆弱性の影響を受けるホストのホストプロファイルを表示できます。この情報は、影響を受ける特定のホストに対するその脆弱性によって生じる脅威を評価するために役立ちます。

特定の脆弱性がネットワーク上のホストに該当しないと判断した場合（たとえば、パッチの適用が完了した場合）、その脆弱性を非アクティブ化できます。非アクティブ化された脆弱性はネットワーク マップに表示され続けますが、これまで影響を受けていたそれらのホストの IP アドレスはグレーのイタリック体で表示されます。それらのホストのホスト プロファイルには、非アクティブ化された脆弱性は無効と表示されますが、個々のホストについて手動で有効とマークすることができます。

ホスト上のアプリケーションまたはオペレーティング システムにアイデンティティの競合がある場合、システムは可能性のあるアイデンティティの両方について脆弱性をリスト表示します。アイデンティティの競合が解決された場合、その脆弱性は現在のアイデンティティに関連付けられたままになります。

ネットワーク マップには、デフォルトではパケットにアプリケーションのベンダーとバージョンが含まれている場合にのみ、検出されたアプリケーションの脆弱性が表示されます。ただし、Management Center の構成でアプリケーションの脆弱性マッピングの設定を有効化することで、ベンダーとバージョンのデータがないアプリケーションの脆弱性をリストするようにシステムを設定できます。

脆弱性 ID（または脆弱性 ID の範囲）の隣の数字は、次の 2 つのカウントを表しています。

影響を受けるホスト数

最初の数字は、1 つまたは複数の脆弱性の影響を受ける 1 台とは限らないホストのカウントです。1 台のホストが複数の脆弱性の影響を受ける場合、このカウントは複数回数えられます。このため、このカウントがネットワーク上のホスト数を上回ることがありえます。脆弱性を非アクティブ化すると、このカウントはその脆弱性の影響を受ける可能性のあるホスト数の分減少します。1 つまたは複数の脆弱性の影響を受ける可能性のあるホストについて、脆弱性を1つも非アクティブ化していない場合、このカウントは表示されません。

影響を受ける可能性のあるホスト数

2 番目の数字は、1 つまたは複数の脆弱性の影響を受ける可能性があるとシステムが判断した 1 台とは限らないホストの総数のカウントです。

脆弱性を非アクティブ化すると、指定したホストについてのみ脆弱性が非アクティブになります。脆弱と判断されたすべてのホストか、指定した個々の脆弱なホストの脆弱性を非アクティブ化することができます。脆弱性が非アクティブ化されると、該当するホストの IP アドレスはネットワーク マップにグレーのイタリック体で表示されます。また、それらのホストのホスト プロファイルでは、非アクティブ化された脆弱性が無効と表示されます。

その後でシステムが脆弱性が非アクティブ化されていないホストに（たとえば、ネットワーク マップ内の新しいホストに）その脆弱性を検出すると、システムはそのホストの脆弱性をアクティブ化します。新たに検出された脆弱性は明示的に非アクティブ化する必要があります。また、システムでは、ホストのオペレーティング システムまたはアプリケーションの変更を検出すると、関連付けられている非アクティブ化された脆弱性を再度アクティブ化することがあります。

ホスト属性ネットワーク マップ

[ホスト属性（Host Attributes）] タブのネットワークマップには、ネットワーク上のホストがユーザー定義ホスト属性またはコンプライアンスallowリストホスト属性のいずれかを基準に編成されて表示されます。この表示では、定義済みホスト属性を使用してホストを編成することはできません。

ホストを編成するために使用するホスト属性を選択すると、Management Center はネットワーク マップで使用可能なその属性の値をリストし、割り当てられた値に基づいてホストをグルー

プ化します。たとえば、allowリストホスト属性でホストを編成することにすると、システムは[準拠（Compliant）]、[非準拠（Non-Compliant）]、[評価されていない（Not Evaluated）] カテゴリでホストを表示します。

また、特定のホスト属性値が割り当てられた任意のホストのホストプロファイルを表示することもできます。

関連トピック

ホスト プロファイル内のホスト属性 （1067 ページ）

ネットワーク マップの表示

ネットワークマップを表示するには、管理者またはセキュリティアナリスト（Security Analyst）ユーザーである必要があります。

手順

ステップ 1 **[分析（Analysis）] > [ホスト（Hosts）] > [ネットワークマップ（Network Map）]** を選択します。

ステップ 2 表示するネットワークマップをクリックします。

ステップ 3 必要に応じて、以下の操作を続行します。

- ドメインの選択：マルチドメイン展開では、[ドメイン（Domain）] ドロップダウン リストからリーフ ドメインを選択します。
- ホストのフィルタリング：IPまたはMACアドレスでフィルタリングするには、検索フィールドにアドレスを入力します。検索をクリアするには、[クリア（Clear）]（✕）をクリックします。
- ドリル ダウン：カテゴリまたはホスト プロファイルを調べる場合、マップのカテゴリまたはサブネットからドリルダウンします。カスタムトポロジを定義した場合、[ホスト（Hosts）] から [（トポロジ）（(topology)）] をクリックしてそのトポロジを表示し、デフォルトのビューに戻したい場合は、[（ホスト）（(hosts)）] をクリックします。
- 削除：該当する要素の横にある[削除（Delete）]（🗑）をクリックし、以下のことを行います。
  - [ホスト（Hosts）]、[ネットワークデバイス（Network Devices）]、[モバイルデバイス（Mobile Devices）]、[アプリケーションプロトコル（Application Protocols）] のマップから要素を削除する。
  - [侵害の兆候（Indications of Compromise）] でIOCカテゴリ、侵害を受けたホスト、侵害を受けたホストのグループを解決済みとしてマークを付ける。
  - [脆弱性（Vulnerabilities）] ですべてのホストまたは単一ホストの脆弱性を非アクティブ化する。
- 脆弱性クラスの指定：[脆弱性（Vulnerabilities）] で、[脆弱性（Vulnerabilities）] ドロップダウンリストから、表示する脆弱性のクラスを選択します。

- 組織属性の指定：[ホスト属性（Host Attributes）] で、[属性（Attribute）] ドロップダウンリストから属性を選択します。

関連トピック

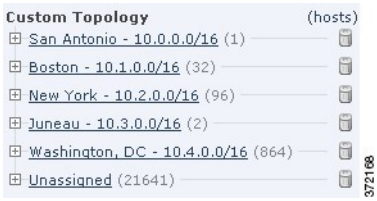
カスタム ネットワーク トポロジ （745 ページ）
ホスト プロファイル （1048 ページ）

カスタム ネットワーク トポロジ

ホストおよびネットワーク デバイスのネットワーク マップでサブネットを整理および識別するために、カスタム トポロジ機能を使用します。

たとえば、部門内の各部署が異なるサブネットを使用している場合、カスタム トポロジ機能を使用して、これらのサブネットにラベルを付けられます。

また、カスタム トポロジで指定した部門に基づいてホストのネットワーク マップを表示することもできます。



次のいずれかまたはすべての方法でカスタム トポロジのネットワークを指定できます。

- ネットワーク検出ポリシーからネットワークをインポートして、システムでモニタするように設定したネットワークをトポロジに追加します。
- 手動でネットワークをトポロジに追加します。

[カスタム トポロジ（Custom Topology）] ページにカスタム トポロジと各トポロジのステータスが一覧表示されます。ポリシー名の隣の電球アイコンが点灯している場合、そのトポロジはアクティブで、ネットワーク マップに影響します。消灯している場合、トポロジは非アクティブです。

関連トピック

ホスト ネットワーク マップ （739 ページ）
ネットワーク デバイスのネットワーク マップ （739 ページ）

カスタム トポロジの作成

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]**を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 ツールバーで [カスタム トポロジ（Custom Topology）] をクリックします。

ステップ 3 [トポロジの作成（Create Topology）] をクリックします。

ステップ 4 名前を入力します。

ステップ 5 必要に応じて、[説明（Description）] を入力します。

ステップ 6 トポロジにネットワークを追加します。次の方法のいずれかまたはすべてを使用できます。

- ネットワーク検出ポリシーからのネットワークのインポート （746 ページ）の説明に従って、ネットワーク検出ポリシーからネットワークをインポートします。
- 手動によるカスタム トポロジへのネットワークの追加 （747 ページ）の説明に従って、手動でネットワークを追加します。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- カスタム トポロジのアクティブおよび非アクティブの設定 （748 ページ）の説明に従って、トポロジをアクティブにします。

ネットワーク検出ポリシーからのネットワークのインポート

手順

ステップ 1 ネットワークをインポートするカスタム トポロジにアクセスします。

- カスタム トポロジを作成します。カスタム トポロジの作成 （746 ページ）を参照してください。
- 既存のカスタム トポロジを編集します。カスタム トポロジの編集 （748 ページ）を参照してください。

ステップ 2 [ポリシー ネットワークのインポート（Import Policy Networks）] をクリックします。

ステップ 3 [ロード（Load）]をクリックします。システムにより、ネットワーク検出ポリシーのトポロジ情報が表示されます。

ステップ 4 トポロジを修正するには、次の手順を実行します。

- トポロジ内のネットワーク名を変更するには、ネットワークの横にある**[編集（Edit）]**（）をクリックし、名前を入力してから [名前の変更（Rename）] をクリックします。
- トポロジからネットワークを削除するには、[削除（Delete）]（）をクリックしてから [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

- カスタムトポロジのアクティブおよび非アクティブの設定（748ページ）の説明に従って、トポロジをアクティブにします。

手動によるカスタム トポロジへのネットワークの追加

手順

ステップ 1 ネットワークを追加するカスタム トポロジにアクセスします。

- カスタム トポロジを作成します。カスタム トポロジの作成（746ページ）を参照してください。
- 既存のカスタム トポロジを編集します。カスタム トポロジの編集（748ページ）を参照してください。

ステップ 2 [ネットワークの追加（Add Network）] をクリックします。

ステップ 3 ホストとネットワーク デバイスのネットワーク マップでネットワークのカスタム ラベルを追加するには、[名前（Name）] を入力します。

ステップ 4 追加するネットワークを表す [IP アドレス（IP Address）] と [ネットマスク（Netmask）]（IPv4）を入力します。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- カスタムトポロジのアクティブおよび非アクティブの設定（748ページ）の説明に従って、トポロジをアクティブにします。

関連トピック

IP アドレスの規則 （31 ページ）

カスタムトポロジのアクティブおよび非アクティブの設定

（注） 常に 1 つのカスタム トポロジのみアクティブにできます。複数のトポロジを作成した場合、1 つをアクティブ化すると、自動的に現在アクティブなトポロジが非アクティブになります。

手順

ステップ 1 **[ポリシー（Policies）]** > **[ネットワーク検出（Network Discovery）]**を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタムトポロジ（Custom Topology）] を選択します。

ステップ 3 アクティブまたは非アクティブにするトポロジの横にあるスライダをクリックします。

カスタム トポロジの編集

アクティブ トポロジに加える変更はただちに有効になります。

手順

ステップ 1 **[ポリシー（Policies）]** > **[ネットワーク検出（Network Discovery）]**を選択します。

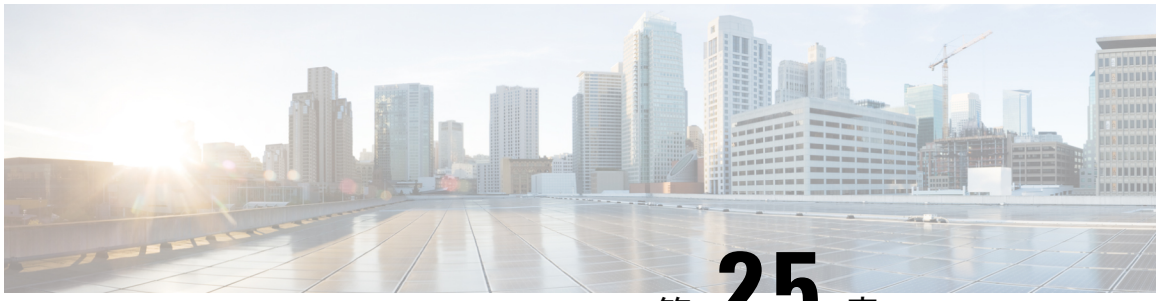
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム トポロジ（Custom Topology）] をクリックします。

ステップ 3 編集するトポロジの隣にある **[編集（Edit）]**（  ） をクリックします。

ステップ 4 カスタム トポロジの作成 （746 ページ）の説明に従って、トポロジを編集します。

ステップ 5 [保存（Save）] をクリックします。



第 25 章

ルックアップ

以下のトピックでは、システムで既知の（または未知の）エンティティに関する情報を検索する方法について説明します。

ルックアップの概要

Management Center がインターネットに接続している場合、手動ルックアップ機能を使って次の情報を検索できます。

- 任意の IP アドレスについての Regional Information Registries（RIR）情報（whois）。
- URL フィルタリング機能によって分類された URL カテゴリおよびレピュテーション。
- 任意の IP アドレスについての地理位置情報（国名、国番号および大陸名）（最新の地理位置情報を確実に使用するように、Management Center 上の地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします）。

Whois ルックアップの実行

始める前に

- Management Center がインターネットにアクセスできることを確認します。セキュリティ、インターネット アクセス、および通信ポート （1277 ページ）を参照してください。

手順

ステップ 1 **[分析（Analysis）]** > **[詳細（Advanced）]** > **[Whois]**を選択します。

ステップ 2 IP アドレスを入力して、[検索（Search）] をクリックします。

URL カテゴリとレピュテーションの検索

URL のカテゴリとレピュテーションは手動で検索できます。この機能は、ポリシー処理を計画、調整、またはトラブルシューティングするために特定の URL をどのように評価するかを確認する場合や、Cisco ソリューションの外部のソースから明らかになる問題のある可能性のある URL を調査する場合に使用します。次に示す結果のカテゴリとレピュテーションは、URL フィルタリング機能で使用されているものと同じです。

始める前に

- Management Center はインターネットにアクセスできる必要があります。セキュリティ、インターネット アクセス、および通信ポート （1277 ページ）を参照してください。
- URL フィルタ リングと **[不明な URL を Cisco Cloud に問い合わせる（Query Cisco cloud for unknown URLs）]** オプションを有効にする必要があります。Cisco Secure Firewall Management Center デバイス構成ガイドの「the *URL Filtering*」の章を参照してください。
- 少なくとも 1 台のデバイスが Management Center に登録されており、そのデバイスには有効な URL フィルタリング ライセンスが割り当てられている必要があります。
- このタスクを実行するには、管理者ユーザーまたはセキュリティ アナリスト ユーザーである必要があります。

手順

ステップ 1 **[分析（Analysis）]** > **[詳細（Advanced）]** > **[URL]** を選択します。

ステップ 2 最大 250 個の URL およびパブリックなルーティング可能 IP アドレスを一般的な任意の形式で入力します（たとえば、URL には "http"、"www" またはサブドメインが含まれていても、省略されていてもよく、短縮形式であってもかまいません）。各エンティティは、スペースまたは改行で区切ります。

アスタリスク（*）などのワイルドカードはサポートされていません。

ステップ 3 [検索（Search）] をクリックします。

入力した URL が多数あり、ネットワークが遅い場合は、処理に数分かかることがあります。

URL が無効であることを示すエラー メッセージが表示された場合は、スペリングを確認するか、URL の別のバリエーションを試行します。たとえば、「www」、「http」、「https」などのプレフィックスを追加または省略します。

URL は最大 6 つのカテゴリに属する可能性がありますが、レピュテーションは 1 つのみです。

ステップ 4 （オプション）列ヘッダーをクリックして、結果をソートします。

ステップ 5 （オプション）CSV ファイルとして結果を保存するには、[CSV のエクスポート（Export CSV）] をクリックします。

CSV ファイルには、レピュテーション レベル用の追加の列が含まれているため、リスク基準でのソートが可能です。ゼロ（0）は、システムにリスク データが不足している URL に対する不明なリスクを表しています。

次のタスク

有効なカテゴリとレピュテーションのリストを表示する場合は、[ポリシー（Policies）]>[アクセス制御（Access Control）] > [アクセス制御（Access Control）] に移動し、ポリシーをクリックするか新しいポリシーを追加して、[ルールの追加（Add Rule）] をクリックし、[URL（URLs）] をクリックします。

IP アドレスの地理位置情報の検出

地理位置情報ルックアップ機能を使用して、国名、ISO 3166-1 の 3 桁の国番号と、任意の IP アドレスに関連付けられた大陸名を検索します。

手順

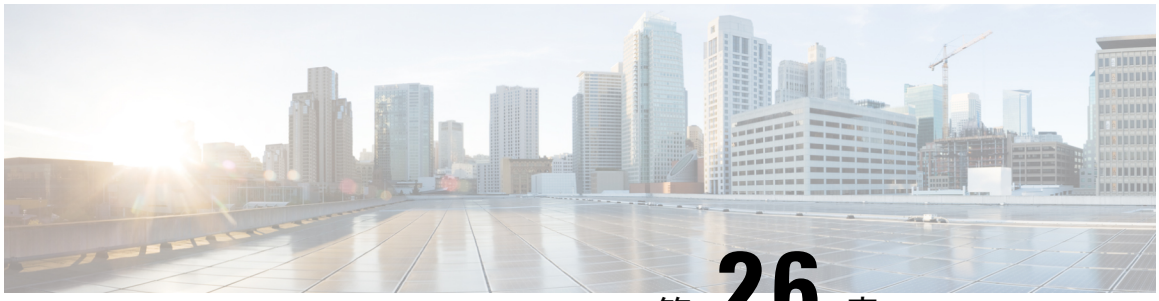
ステップ 1 **[分析（Analysis）] > [詳細（Advanced）] > [位置情報（Geolocation）]**を選択します。

ステップ 2 1 つ以上の IP アドレスの地理位置情報を表示するには、アドレス（複数可）を入力して、[検索（Search）] をクリックします。IPv4 アドレス、IPv6 アドレスのいずれか、または両方を指定できます。複数のアドレスは、カンマ、セミコロン、改行、スペース文字を使用して区切ります。

ヒント テキストボックスをクリアするには、[クリア（Clear）] をクリックします。

ステップ 3 データを並べ替えるには、列見出しをクリックします。IP アドレスを除くすべてのフィールドによって並べ替えが可能です。

ステップ 4 （オプション）CSV として結果を保存するには、[CSV をエクスポートする（Export CSV）] をクリックします。



第 26 章

外部ツールを使用したイベントの分析

シスコ SecureX との統合

単一のペインである SecureX クラウドポータルを使用して、すべてのシスコセキュリティ製品などのデータを表示および操作します。SecureX で利用可能なツールを使用して、脅威ハントと調査を強化します。SecureX は、それぞれが最適なソフトウェアバージョンを実行しているかどうかなど、有用なアプライアンスおよびデバイス情報も提供します。

SecureX の詳細については、Cisco SecureX ページを参照してください。

SecureX 統合の有効化

Cisco SecureX プラットフォームは、広範なシスコの統合型セキュリティポートフォリオとお客様のインフラストラクチャをつなぐことで、一貫した操作性を提供します。これにより可視性が統一され、自動化が実現し、ネットワーク、エンドポイント、クラウド、およびアプリケーションの全体でセキュリティが強化されます。SecureX の詳細については、Cisco SecureX 製品のページを参照してください。

SecureX と Management Center の統合により、Management Center の全データの概要が提供されます。Management Center と SecureX の統合の詳細については、『Cisco Secure Firewall Management Center（バージョン 7.2 以降）および SecureX 統合ガイド』を参照してください。

始める前に

組織に属する SecureX アカウントが必要です。SecureX アカウントがない場合は、CDO テナントを使用して SecureX アカウントを作成してください。詳細については、「CDO を使用した SecureX アカウントの作成」を参照してください。

手順

ステップ 1 Management Center で **[統合（Integration）]** > **[SecureX]** を選択します。

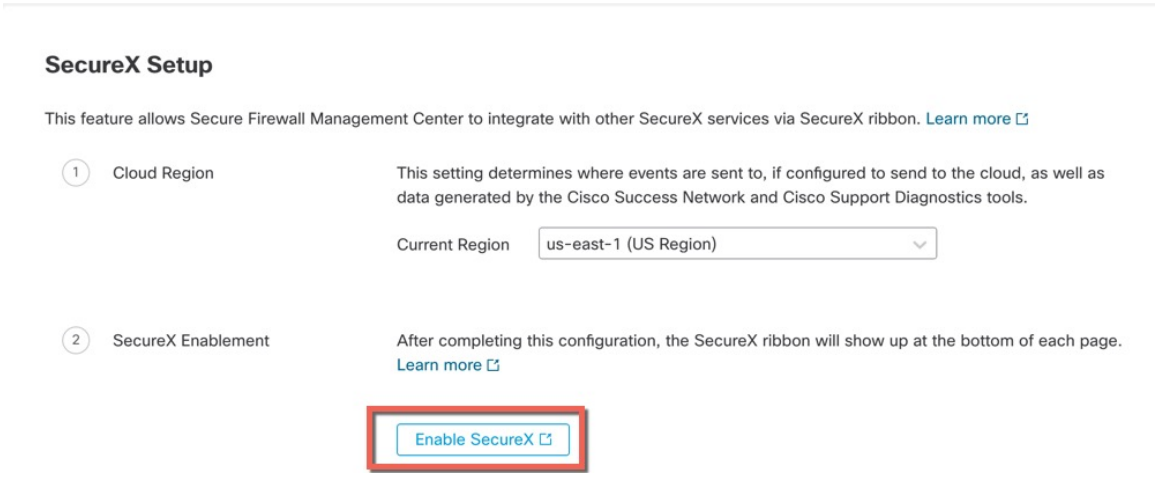
ステップ 2 （任意）[クラウドリージョン（Cloud Region）] で、[現在のリージョン（Current Region）] を選択します。

デフォルトで選択されるリージョンがスマートライセンスのリージョンと同じであるため、多くの場合、リージョンを変更する必要はありません。

ステップ 3 [SecureXの有効化（SecureX Enablement）] で、次の手順を実行します。

a) [SecureXの有効化（Enable SecureX）] をクリックします。

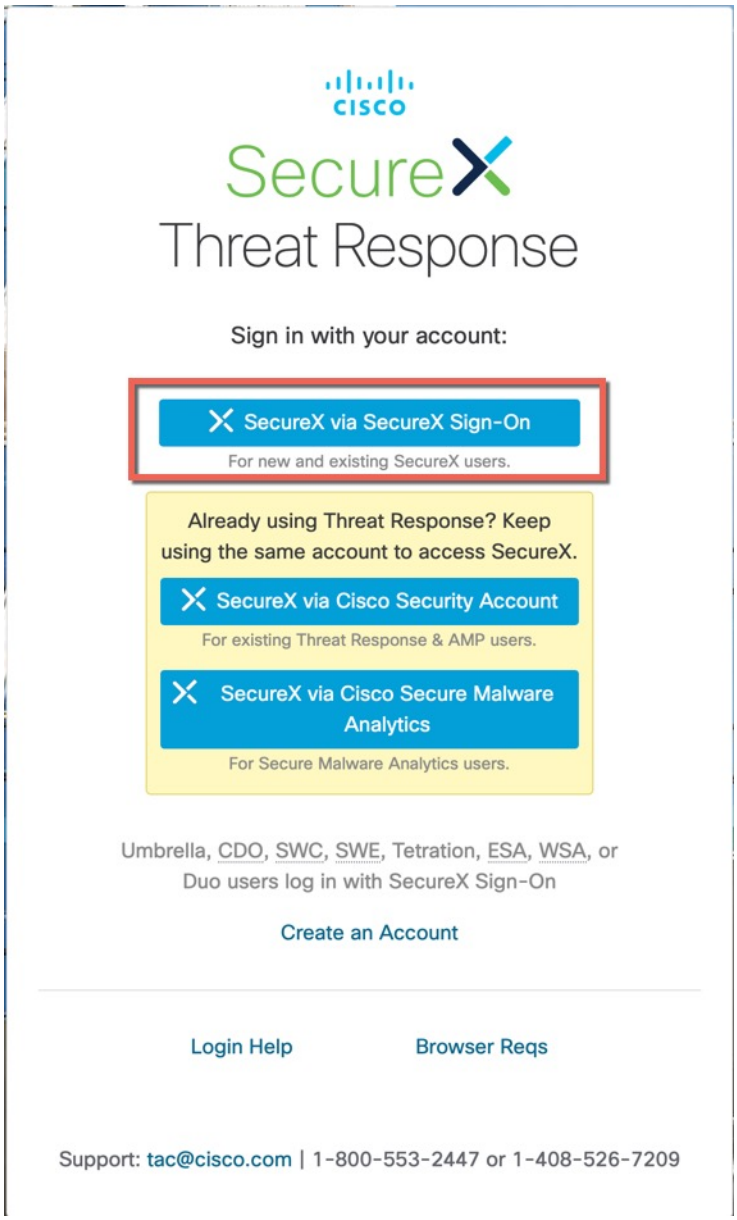
図 *18 : SecureX*の有効化



b) SecureX にログインします。

SecureXアカウントにログインするための別のブラウザタブまたはウィンドウが開きます。このページがポップアップブロッカーによってブロックされていないことを確認してください。

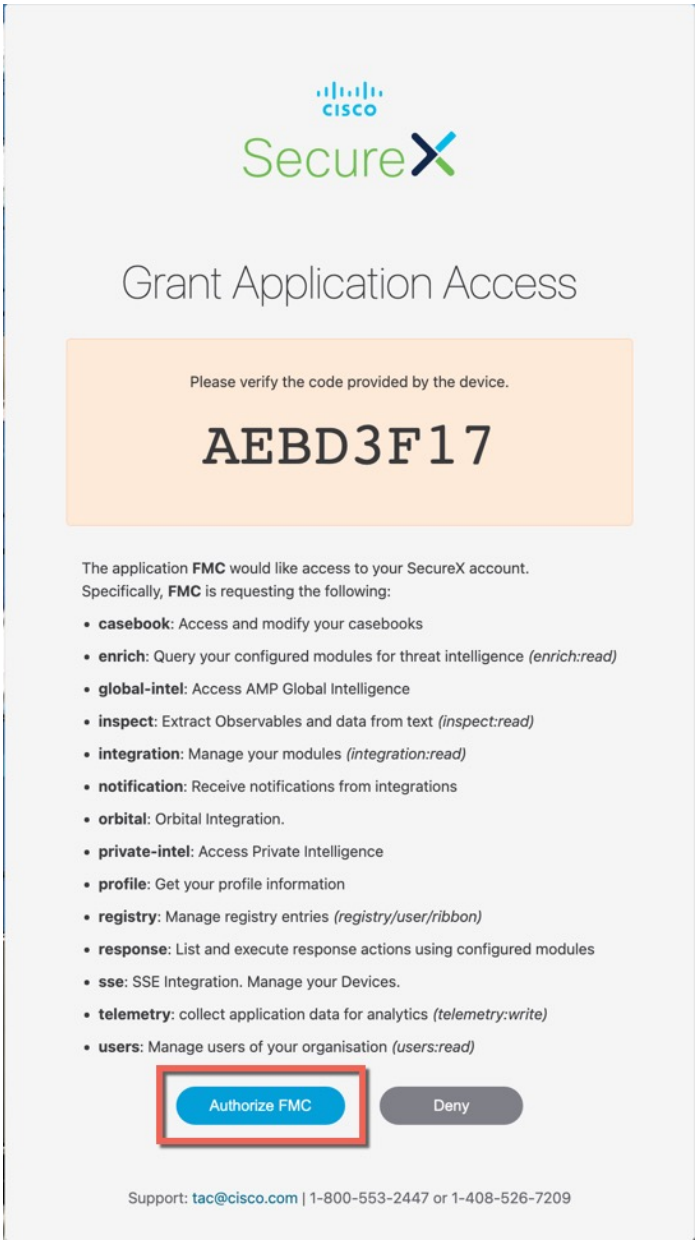
図 *19 : SecureX* サインイン



c) [FMCの許可（Authorize FMC）] をクリックします。

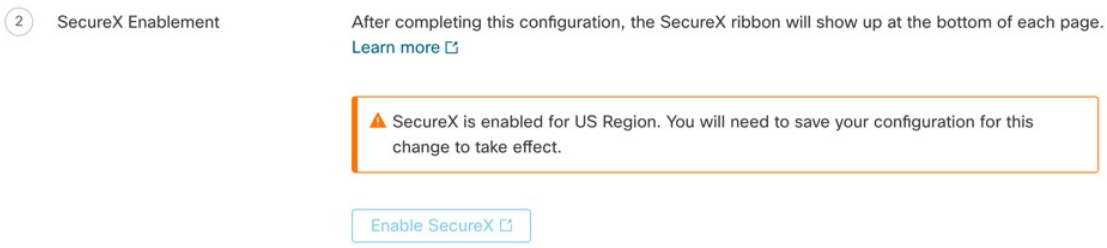
通常 Management Center で示されるコードと一致するコードが表示されます。

図 *20* : アプリケーションアクセスの許可



d) Management Center と SecureX が統合されると、成功メッセージが表示されます。[保存（Save）] をクリックします。

図 *21* : 成功メッセージ



イベントを Cisco Security Cloud に送信するための Management Center の設定

管理対象 脅威に対する防御 デバイスにイベントを直接 Cisco Security Cloud に送信させるように Management Center を設定します。このページで設定するクラウド地域とイベントタイプは、適用可能で有効になっている場合、複数の統合に使用できます。

始める前に

- Management Center をスマートライセンスに登録（**システム**（⚙）>**[スマートライセンス（Smart License）]**）しているか、Cisco Security Cloud 統合を有効にして、デバイスがファイアウォールイベントを Cisco Cloud に送信できるようになっていることを確認します。
- Management Center で次の手順を実行します。
  - [システム（System）] > [設定（Configuration）] ページに移動し、クラウドの [デバイス（Devices）] リストで明確に識別される一意の名前を Management Center に付けます。
  - 脅威に対する防御 デバイスを Management Center に追加し、それらにライセンスを割り当て、システムが正常に動作していることを確認します必要なポリシーが作成され、生成されたイベントが Management Center UI の [分析（Analysis）] メニューに想定どおりに表示されているかを確認します。
- Cisco Security Cloud Sign On ログイン情報があり、アカウントが作成された SecureX 地域クラウドにサインインできることを確認します。

  SecureX 地域クラウド URL とサポートされているデバイスバージョンの詳細については、『Cisco Secure Firewall Management Center and SecureX Integration Guide』を参照してください。
- 現在 syslog を使用してクラウドにイベントを送信している場合は、重複を避けるために無効にします。

手順

ステップ 1 ファイアウォールイベントの送信に使用するシスコ地域クラウドを決定します。地域クラウドの選択の詳細については、『Cisco Secure Firewall Management Center and SecureX Integration Guide』を参照してください。

（注） SecureX が有効になっていて、Management Center が選択した地域クラウドに登録されている場合、地域クラウドを変更すると SecureX が無効になります。地域クラウドを変更した後、SecureX を再度有効にすることができます。

ステップ 2 Management Center で、**[統合（Integration）]** > **[SecureX]** をクリックします。

ステップ 3 [現在のリージョン（Current Region）] ドロップダウンリストから地域クラウドを選択します。

ステップ 4 [クラウドにイベントを送信（Send events to the cloud）] チェックボックスをオンにして、クラウドイベント設定を有効にします。

ステップ 5 クラウドに送信するイベントのタイプを選択します。

（注） 次の表に示すように、クラウドに送信するイベントを複数の統合に使用できます。

統合	サポートされるイベントのオプション	注意
Cisco Security Analytics and Logging (SaaS)	すべて（All）	優先順位の高い接続イベントには、次のイベントが含まれます。 • セキュリティ関連の接続イベント • ファイルおよびマルウェア イベントに関連する接続イベント • 侵入イベントに関連する接続イベント
シスコ SecureX と Cisco SecureX Threat Response	お使いのバージョンに応じて、以下が含まれます。 • セキュリティ関連の接続イベント。 • 侵入イベント。 • ファイルイベントおよびマルウェアイベント。	すべての接続イベントを送信する場合でも、Cisco SecureX と Cisco SecureX Threat Response ではセキュリティ関連の接続イベントのみがサポートされます。

（注）
- [侵入イベント（Intrusion Events）] を有効にすると、イベントは影響フラグとともに Management Center から送信されます。
- [ファイルおよびマルウェアイベント（File and Malware Events）] を有効にすると、脅威に対する防御デバイスから送信されるイベントに加えて、レトロスペクティブイベントが Management Center から送信されます。

ステップ 6 [保存（Save）] をクリックします。

Cisco Success Network の登録設定

Cisco Success Network は、Management Center を有効にして Cisco Cloud とのセキュアな接続を確立するクラウドサービスで、使用情報と統計情報がストリーミングされます。このテレメトリをストリーミングすることによって、次の理由で、脅威に対する防御 デバイスから対象のデータを選択して構造化形式でリモートの管理ステーションに送信するメカニズムが提供されます。

- ネットワーク内の製品の有効性を向上させるために、使用可能でありながら未使用の機能について通知します。
- 製品に利用可能な、追加のテクニカルサポートサービスとモニタリングについて通知します。
- （SecureX と統合している場合）アプライアンスとデバイスのステータスを SecureX タイルにまとめ、すべてのデバイスで最適なソフトウェアバージョンが実行されているかどうかを確認します。
- シスコ製品の改善に役立ちます。

シスコによって収集されるテレメトリデータの詳細については、Cisco Secure Firewall Management Center デバイスによって収集される Cisco Success Network テレメトリデータ [英語] を参照してください。

Cisco Support Diagnostics または Cisco Success Network を有効にすると、Management Center によって Cisco Cloud とのセキュアな接続が確立されて維持されます。また一方で、Cisco Support Diagnostics を有効にすると、Management Center デバイスと 脅威に対する防御 デバイスによって Cisco Cloud とのセキュアな接続が確立されて維持されます。この接続は、Cisco Success Network および Cisco Support Diagnostics の両方を無効にすることで、いつでもオフにできます。これにより、Management Centerが Cisco Cloud から接続解除されます。

Smart Software Manager に Management Center を登録するときは、Cisco Success Network を有効にできます。

（注）
- Cisco Success Network は評価モードではサポートされていません。
-
- Management Center に有効な Smart Software Manager オンプレミス（以前の Smart Software Satellite Server）設定がある場合、または、特定のライセンス予約を使用している場合、Cisco Success Network は無効になっています。

始める前に

このタスクを実行するには、SecureX 統合を有効にするか、Management Center をスマートライセンスに登録します。

手順

ステップ 1 **[統合（Integration）]** > **[SecureX]** をクリックします。

ステップ 2 **[Cisco Cloudサポート（Cisco Cloud Support）]** で、[Cisco Success Networkの有効化（Enable Cisco Success Network）] チェックボックスをオンにして、このサービスを有効にします。

（注） 続行する前に、[Cisco Success Networkを有効化（Enable Cisco Success Network）] チェックボックスの横にある情報を読んでください。

ステップ 3 [保存（Save）] をクリックします。

Cisco Support Diagnostics の登録設定

Cisco Support Diagnostics は、ユーザーによって有効化されるクラウドベースの TAC サポートサービスです。有効にすると、Management Center と管理対象デバイスと Cisco Cloud のセキュアな接続が確立され、システムヘルスに関する情報がストリーミングされます。

Cisco Support Diagnostics は、Cisco TAC が TAC ケースの解決中にデバイスから重要なデータを安全に収集できるようにすることで、トラブルシューティングの際によりよいユーザーエクスペリエンスを提供します。さらに、シスコは自動問題検出システムによって定期的にヘルスデータを収集および処理し、問題がある場合はユーザーに通知します。TAC ケース解決時のデータ収集サービスはサポート契約を持つすべてのユーザーが利用できますが、通知サービスは、特定のサービス契約を持つユーザーのみが使用できます。

Cisco Support Diagnostics を使用すると、脅威に対する防御 デバイスと Management Center の両方で Cisco Cloud とのセキュアな接続が確立されて維持されます。Management Center は、収集したデータを **[SecureX統合（SecureX Integration）]** ページで選択された地域クラウドに送信します。

この接続は、Cisco Success Network および Cisco Support Diagnostics の両方を無効にすることで、いつでもオフにできます。これにより、これらの機能は Cisco Cloud から接続解除されます。

管理者が Management Center から収集されたデータのサンプルファイルを表示するには、「特定のシステム機能に関するトラブルシューティング ファイルの生成」に従います。

始める前に

このタスクを実行するには、SecureX 統合を有効にするか、Management Center をスマートライセンスに登録します。

手順

ステップ 1 **[統合（Integration）]** > **[SecureX]** をクリックします。

ステップ 2 **[Cisco Cloudサポート（Cisco Cloud Support）]** で、[Cisco Support Diagnosticsを有効化（Enable Cisco Support Diagnostics）] チェックボックスをオンにして、このサービスを有効にします。

（注） 続行する前に、[Cisco Support Diagnosticsを有効化（Enable Cisco Support Diagnostics）] チェックボックスの横にある情報を読んでください。

ステップ 3 [保存（Save）] をクリックします。

リボンを使用した SecureX へのアクセス

このリボンは、Management Center Web インターフェイスのすべてのページの下部に表示されます。このリボンを使用して、他のシスコのセキュリティ製品にすばやく切り替え、複数のソースからの脅威データを扱うことができます。

始める前に

- Management Center Web インターフェイスページの下部に SecureX リボンが表示されない場合は、この手順を使用しないでください。

  代わりに、『Cisco Secure Firewall Threat Defense and SecureX Integration Guide』を参照してください。

- SecureX アカウントがまだない場合は、IT 部門から入手します。

手順

ステップ 1 Management Center で、任意の Management Center ページの下部にあるリボンをクリックします。

ステップ 2 [Get SecureX] をクリックします。

ステップ 3 SecureX にサインインします。

ステップ 4 アクセスを許可するリンクをクリックします。

ステップ 5 リボンをクリックして展開し、使用します。

次のタスク

リボンの機能とその使用方法については、SecureX のオンラインヘルプを参照してください。

によるイベントの分析 SecureX Threat Response

SecureX Threat Response は、以前は Cisco Threat Response（CTR）と呼ばれていました。

SecureX Threat Response を使用して脅威を迅速に検出、調査、対応する Cisco Cloud の統合プラットフォームでは、Cisco Secure Firewall を含む複数の製品から集約されたデータを使用してインシデントを分析できます。

- SecureX Threat Response の一般情報については、次を参照してください。

  Cisco SecureX Threat Response 製品ページ。

- Firepower と SecureX Threat Response の統合の詳細な手順については、次を参照してください。

- Cisco Secure Firewall Threat Defense および Cisco SecureX Threat Response 統合ガイド [英語] を参照してください。

SecureX Threat Response でのイベントデータの表示

始める前に

- 『Cisco Secure Firewall Threat Defense and Cisco SecureX Threat Response Integration Guide』の説明に従って統合をセットアップします。
- SecureX Threat Response のオンライン ヘルプを確認し、脅威の検出、調査、およびアクションを実行する方法を習得します。
- SecureX Threat Response にアクセスするにはクレデンシャルが必要です。

手順

ステップ 1 Secure Firewall Management Center で、次の手順を実行します。

- 特定のイベントから SecureX Threat Response にピボットするには、次の手順を実行します。

a. [分析（Analysis）]>[侵入（Intrusions）] メニューで、サポートされているイベントが表示されているページに移動します。

b. 送信元または宛先の IP アドレスを右クリックし、**[Thereat Response IP]** を選択します。

ステップ 2 プロンプトが表示されたら、SecureX Threat Response にサインインします。

Web ベースのリソースを使用したイベントの調査

Secure Firewall Management Center 外部の Web ベースのリソースにおける潜在的な脅威についての情報をすばやく検索するには、コンテキスト クロス起動 機能を使用します。例：

- Cisco または既知の疑わしい脅威に関する情報を公開するサードパーティ製クラウドホステッド サービスの疑わしい送信元 IP アドレスを検索する、または
- 組織の履歴ログで特定の脅威に関する過去のインスタンスを検索する（組織がセキュリティ情報とイベント管理（SIEM）アプリケーションでそのデータを格納している場合）。
- 組織で Cisco Secure Endpoint を導入している場合は、ファイルトラジェクトリ情報などの特定のファイルに関する情報を検索します。

イベントを調査する際は、Secure Firewall Management Center のイベント ビューアまたはダッシュボードのイベントから直接、外部リソースの関連情報をクリックできます。これにより、その IP アドレス、ポート、プロトコル、ドメイン、または SHA 256 ハッシュに基づいて、特定のイベントに関連するコンテキストを迅速に収集できます。

たとえば、[上位攻撃者（Top Attackers）] ダッシュボード ウィジェットを表示し、記載されている送信元 IP アドレスのいずれかに関する詳細情報を検索すると仮定します。この IP アドレスに関して、Talos がどのような情報を公開しているか確認したいので、「Talos IP」リソースを選択します。Talos Web サイトが開き、この特定の IP アドレスに関する情報が書かれたページが表示されます。

一般的に使用されているシスコやサードパーティ製の脅威インテリジェンス サービスへの一連の事前定義されたリンクから選択し、その他の Web ベースのインターフェイスおよび Web インターフェイスを持つ SIEM または他の製品へのカスタム リンクを追加できます。一部のリソースでは、アカウントまたは製品の購入が必要になる場合があります。

コンテキスト クロス起動のリソースの管理について

[分析（Analysis）]>[詳細（Advanced）]>[コンテキスト クロス起動（Contextual Cross-Launch）] ページを使用して外部の Web ベースのリソースを管理します。

例外：Secure Network Analytics の相互起動リンクの設定 （766 ページ）の手順に従って、Secure Network Analytics アプライアンスへのクロス起動リンクを管理します。

シスコが提供している事前定義のリソースにはシスコのロゴが付いています。残りのリンクはサードパーティのリソースです。

必要がないリソースは無効にするか、または削除できます。あるいは、たとえば名前の前に小文字の「z」を追加するなどして名前を変更し、そのリソースをリストの下部に分類することができます。クロス起動リソースを無効にすると、すべてのユーザーに対して無効になります。削除されたリソースは、元に戻すことはできませんが、再作成できます。

リソースを追加するには、コンテキスト クロス起動のリソースの追加（764 ページ）を参照してください。

カスタム コンテキスト クロス起動のリソースの要件

カスタム コンテキスト クロス起動 リソースを追加する場合は、次の点に留意します。

- リソースは Web ブラウザを介してアクセスできる必要があります。
- http プロトコルと https プロトコルのみがサポートされています。
- GET 要求のみがサポートされています。POST 要求はサポートされていません。
- URL の変数のエンコーディングはサポートされていません。IPv6 アドレスをエンコードするにはコロンで区切る必要がある場合がありますが、ほとんどのサービスでこのエンコーディングは必要ありません。
- 事前に定義されたリソースを含めて、最大 100 のリソースを設定できます。
- 相互起動を作成するには管理者またはセキュリティ アナリスト（Security Analyst）のユーザーである必要がありますが、読み取り専用のセキュリティ アナリスト（Security Analyst）でも使用できます。

コンテキスト クロス起動のリソースの追加

脅威インテリジェンス サービスやセキュリティ情報とイベント管理（SIEM）の ツールなどのコンテキスト クロス起動 リソースを追加できです。

マルチドメイン展開環境では、親ドメインのリソースを表示および使用できますが、現在のドメインで実行できるのはリソースの作成と編集のみです。すべてのドメインのリソースの合計数は 100 に制限されています。

始める前に

- Secure Network Analytics アプライアンスにリンクを追加する場合は、必要なリンクがすでに存在するかどうかを確認してください。ほとんどのリンクは、セキュリティ分析とロギング（オンプレミス） の構成時に作成されます。
- カスタム コンテキスト クロス起動のリソースの要件（764 ページ）を参照してください。
- リソースに必要な場合は、アクセスに必要なアカウントとクレデンシャルにリンクするか、作成するか、または取得します。必要に応じて、アクセスが必要な各ユーザーにクレデンシャルを割り当てて配布します。
- リンク先のリソースのクエリ リンクのシンタックスを特定します。

ブラウザ経由でリソースにアクセスし、必要に応じてそのリソースのドキュメントを使用して、たとえばIPアドレスなど、検索するクエリ リンクの特定のタイプの情報の検索に必要なクエリ リンクを作成します。

クエリを実行して、結果のURLをブラウザのロケーション バーからコピーします。

たとえば、クエリ URL
`https://www.talosintelligence.com/reputation_center/lookup?search=10.10.10.10`
が表示される場合があります。

手順

ステップ1 [分析（Analysis）]>[詳細（Advanced）]>[コンテキストクロス起動（Contextual Cross-Launch）]を選択します。

ステップ2 [新しいクロス起動（New Cross-Launch）]をクリックします。

表示されたフォームのアスタリスクの付いたすべてのフィールドに値が必要です。

ステップ3 一意のリソース名を入力します。

ステップ4 作業中のURLの文字列をリソースから[URLテンプレート（URL Template）]フィールドに貼り付けます。

ステップ5 クエリ文字列内の特定のデータ（IPアドレスなど）を適切な変数で置き換えます。変数を挿入するには、カーソルを置いて変数（[ip]など）を1回クリックします。

上記の「開始する前に」の項の例では、URLは
`https://www.talosintelligence.com/reputation_center/lookup?search= {ip}`
になります。コンテキスト クロス起動 リンクを使用すると、URL内の{ip}変数は、イベントビューアまたはダッシュボードでユーザーが右クリックするIPアドレスに置き換わります。

各変数の説明については、変数の上にカーソルを置きます。

1つのツールまたはサービスに複数の コンテキスト クロス起動 リンクを作成するには、それぞれに異なる変数を使用します。

ステップ6 **[サンプルデータを使用したテスト（Test with example data）]**（  ）をクリックして、サンプルデータでリンクをテストします。

ステップ7 問題を修正します。

ステップ8 [保存（Save）]をクリックします。

コンテキスト クロス起動を使用したイベントの調査

始める前に

アクセスするリソースにクレデンシャルが必要な場合は、それらのクレデンシャルがあることを確認します。

手順

ステップ 1 Secure Firewall Management Center でイベントが表示される次のページのいずれかに移動します。

- ダッシュ ボード（[概要（Overview）] > [ダッシュボード（Dashboards）]）、または
- イベント ビューア ページ（イベントのテーブルが含まれている [分析（Analysis）] メニューにあるオプション）

ステップ 2 対象のイベントを右クリックして、使用する コンテキスト クロス起動 のリソースを選択します。

必要に応じて、コンテキスト メニューを下にスクロールして使用可能なすべてのオプションを確認します。

右クリックしたデータ タイプによって表示されるオプションが異なります。たとえば、IP アドレスを右クリックした場合は、IP アドレスに関連する コンテキスト クロス起動 のオプションのみが表示されます。

たとえば、侵入イベントの送信元 IP アドレスについて Cisco Talos から脅威インテリジェンスを取得するには、[Talos SrcIP] または [Talos IP] を選択します。

リソースに複数の変数が含まれている場合、そのリソースを選択するオプションは、含まれている各変数に可能な 1 つの値を持つイベントにのみ使用できます。

別のブラウザ ウィンドウに コンテキスト クロス起動 のリソースが開きます。

クエリを実行するデータの量、リソースの速度と需要によってはクエリが処理されるまでに時間がかかる場合があります。

ステップ 3 必要に応じて、リソースにサインインします。

Secure Network Analytics の相互起動リンクの設定

Secure Firewall Threat Defense のイベントデータから Secure Network Analytics アプライアンスの関連データに相互起動できます。Secure Network Analytics 製品の詳細については、Cisco Security Analytics and Logging の製品ページを参照してください。

コンテキストに応じた相互起動に関する一般的な情報については、コンテキスト クロス起動を使用したイベントの調査 （765 ページ）を参照してください。

Secure Network Analytics アプライアンスへの一連の相互起動リンクを設定するには、この手順を使用します。

（注）

- 相互起動リンクを後で変更する場合は、この手順に戻ります。コンテキストに応じた相互起動リストページで直接変更することはできません。
- コンテキストクロス起動のリソースの追加（764ページ）の手順を使用して、Secure Network Analytics アプライアンスに相互起動する追加のリンクを手動で作成できますが、それらのリンクは自動作成されたリソースからは独立しているため、手動で管理する必要があります。

始める前に

- 展開済みで実行中の Secure Network Analytics アプライアンスが必要です。
- 現在、イベントの直接送信をサポートしているデバイスのバージョンから Secure Network Analytics に syslog を使用してイベントを送信している場合、それらのデバイスの syslog を無効にして（または syslog の設定を含めないアクセス コントロール ポリシーをそれらのデバイスに割り当てて）リモートボリュームでイベントが重複しないようにします。
- 次のものが必要です。
  - Manager のホスト名または IP アドレス。
  - 管理者権限を持つ Secure Network Analytics アプライアンスのアカウントのログイン情報。

セキュリティ分析とロギング（オンプレミス） を使用して Secure Firewall Threat Defense データを Secure Network Analytics アプライアンスに送信する場合は、Secure Network Analytics アプライアンスでのリモートデータストレージ （633 ページ）を参照してください。

手順

ステップ 1 を選択します。

ステップ 2 Secure Network Analytics の展開には次の 2 つのオプションがあります。

- [Managerのみ（Manager Only）]：スタンドアロンの Manager を展開してイベントを受信および保存し、保存したイベントを確認およびクエリできます。
- データストア：Cisco Secure Network Analyticsフローコレクタを展開してイベントを受信し、Secure Network Analytics データストアでイベントを保存し、Manager で保存したイベントを確認およびクエリできます。

展開オプションを選択し、[開始（Start）] をクリックします。

ステップ 3 ウィザードを完了します。詳細については、Cisco Security Analytics and Logging ファイアウォールイベント統合ガイド [英語] の「Secure Firewall Management Center Configuration」を参照してください。

ステップ 4 新しい相互起動リンクを確認します。[分析（Analysis）] > [詳細（Advanced）] > [状況に応じた相互起動（Contextual Cross-Launch）] を選択します。

変更する場合は、この手順に戻ります。コンテキストに応じた相互起動リストページで直接変更することはできません。

次のタスク

イベントから Secure Network Analytics イベントビューアに相互起動するには、Secure Network Analytics のログイン情報を使用します。

Management Center イベントビューアまたはダッシュボードのイベントから相互起動するには、関連するイベントのテーブルセルを右クリックし、適切なオプションを選択します。

処理するデータの量、Secure Network Analytics Manager の速度と需要などによって、クエリの処理に時間がかかる場合があります。

セキュリティイベントの syslog メッセージの送信について

接続、セキュリティインテリジェンス、侵入、およびファイルとマルウェアのイベントに関連するデータは、syslog を介してセキュリティ情報およびイベント管理（SIEM）ツールまたは、外部のイベントストレージおよび管理ソリューションに送信できます。

これらのイベントを Snort® イベントと呼ぶこともあります。

syslog にセキュリティイベントデータを送信するためのシステムの設定について

セキュリティ イベントを syslog に送信するようにシステムを設定するには、次を知っておく必要があります。

- セキュリティ イベント syslog メッセージングを設定するためのベストプラクティス （769 ページ）
- セキュリティ イベントの syslog の設定場所 （775 ページ）
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Threat Defense Platform Settings that Apply to Security Event Syslog Messages*」
- ポリシーで syslog の設定を変更した場合、それらの変更を有効にするには展開する必要があります。

セキュリティ イベント syslog メッセージングを設定するためのベストプラクティス

デバイスとバージョン	設定の場所
すべて（All）	syslog またはストアイベントを外部で使用する場合は、ポリシー名やルール名などのオブジェクト名に特殊文字を使用しないでください。オブジェクト名には、カンマなどの特殊文字を含めることはできません。受信側アプリケーションで区切り文字として使用される可能性があります。
Secure Firewall Threat Defense	1. Threat Defense プラットフォーム設定（[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）]>[Threat Defense設定（Threat Defense Settings）]>[Syslog]）を設定します。 1. **[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）]** をクリックします。 2. Threat Defense 設定ポリシーを編集します。 3. 左側のナビゲーションペインで、[Syslog] をクリック。 Cisco Secure Firewall Management Center デバイス構成ガイド の「セキュリティイベントの *syslog* メッセージに適用する *Threat Defense* プラットフォームの設定」も参照してください。 2. アクセス コントロール ポリシーの [ロギング（Logging）] タブで、Threat Defense プラットフォーム設定の使用を選択します。 3. （侵入イベントの場合）アクセス コントロール ポリシーの [ロギング（Logging）] タブの設定を使用するように侵入ポリシーを設定します。（これはデフォルトです）。 これらの設定の上書きは推奨していません。 最低限必要な詳細情報については、Threat Defense デバイスからのセキュリティイベント syslog メッセージの送信 （770 ページ）を参照してください。

デバイスとバージョン	設定の場所
その他のすべてのデバイス	1. アラート応答を作成します。 2. アラート応答を使用するには、アクセス コントロール ポリシーの [ロギング（Logging）] を設定します。 3. （侵入イベントの場合）侵入ポリシーで syslog 設定を構成します。 詳細については、従来型デバイスからのセキュリティイベント syslog メッセージの送信 （773 ページ）を参照してください。

Threat Defense デバイスからのセキュリティイベント syslog メッセージの送信

この手順では、Threat Defense デバイスからセキュリティイベント（接続、セキュリティ インテリジェンス、侵入、ファイル、およびマルウェアイベント）の syslog メッセージを送信するためのベストプラクティス設定について説明します。

（注） 多くの Threat Defense syslog 設定は、セキュリティイベントには適していません。この手順で説明するオプションのみを設定してください。

始める前に

- Secure Firewall Management Center で、セキュリティイベントを生成するようにポリシーを設定するとともに、予期されるイベントが [分析（Analysis）] メニューの該当するテーブルに表示されることを確認します。
- syslog サーバーの IP アドレス、ポート、およびプロトコル（UDP または TCP）を収集します。
- デバイスが syslog サーバーに到達できることを確認します。
- syslog サーバーがリモートメッセージを受け入れられることを確認します。
- 接続ロギングに関する重要な情報については、接続ロギング （879 ページ）の関連する章を参照してください。

手順

ステップ 1 Threat Defense デバイスの syslog 設定を指定します。

a) [デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] をクリックします。

b) Threat Defense デバイスに関連付けられているプラットフォーム設定ポリシーを**編集**します。

c) 左側のナビゲーションペインで、[Syslog] をクリック。

d) [syslogサーバー（Syslog Servers）] をクリックし、**Add** ( ) をクリックして、サーバー、プロトコル、インターフェイス、および関連情報を入力します。

このページのオプションについて疑問がある場合は、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

e) [syslog 設定（Syslog Settings）] をクリックし、次の設定を行います。

- syslogメッセージのタイムスタンプを有効化（Enable timestamp on syslog messages）
- **タイムスタンプ形式**
- syslogデバイスIDを有効化（Enable syslog device ID）

f) [ロギングのセットアップ（Logging Setup）] をクリックします。

g) [Basic Logging Settings（基本ロギング設定）] で、EMBLEM 形式で syslog を送信するかどうかを選択します。

h) [保存（Save）] をクリックして設定を保存します。

ステップ 2 アクセス コントロール ポリシーの一般的なログ設定（ファイルおよびマルウェアロギングを含む）を指定します。

a) [ポリシー（Policies）] > [アクセスコントロール（Access Control）] をクリックします。

b) 該当するアクセス コントロール ポリシーを編集します。

c) **[詳細（More）]** > **[ロギング（Logging）]** をクリックします。

d) Threat Defense 6.3 以降：[デバイスに展開したFTDプラットフォーム設定のsyslog設定を使用する（Use the syslog settings configured in the FTD Platform Settings policy deployed on the device）] をオンにします。

e) （任意）**syslog の重大度**を選択します。

f) ファイルおよびマルウェアイベントを送信する場合は、[ファイル/マルウェアイベントのsyslogメッセージを送信する（Send Syslog messages for File and Malware events）] をオンにします。

g) **[保存（Save）]** をクリックします。

ステップ 3 アクセス コントロール ポリシーのセキュリティ インテリジェンス イベントのロギングを有効にします。

a) 同じアクセス コントロール ポリシーで、[セキュリティ インテリジェンス（Security Intelligence）] タブをクリックします。

b) 次の各場所で、[ロギング（Logging）] ( ) をクリックし、接続の開始および終了と [syslog サーバー（Syslog Server）] を有効にします。

- [DNS ポリシー（DNS Policy）] の横。
- [ブロックリスト（Block List）]ボックスの、[ネットワーク（Networks）] と [URL（URLs）]。

c) **[保存（Save）]** をクリックします。

ステップ 4 アクセス コントロール ポリシーの各ルールの syslog ロギングを有効にします。

a) 同じアクセス コントロール ポリシーで、**[アクセスコントロール（Access Control）]** > **[ルールの追加（Add Rule）]** をクリックします。
b) 編集するルールを選択します。
c) ルールの [ロギング（Logging）] タブをクリックします。
d) 接続の開始時または終了時あるいはその両方をログに記録するかどうかを選択します。

（接続ロギングでは大量のデータが生成されます。開始時と終了時の両方のロギングでは、生成されるデータの量がほぼ倍になります。すべての接続を開始時と終了時の両方でログに記録できるわけではありません）

e) ファイルイベントをログに記録する場合は、[ファイルのロギング（Log Files）] を選択します。
f) [syslog サーバー（Syslog Server）] を有効にします。
g) ルールが [アクセスコントロールログでデフォルトの syslog 設定を使用する（Using default syslog configuration in Access Control Logging）] であることを確認します。
h) [確認（Confirm）] をクリックします。
i) ポリシーの各ルールに対して手順を繰り返します。

ステップ 5 侵入イベントを送信する場合は、次の手順を実行します。

a) アクセス コントロール ポリシーに関連付けられている侵入ポリシーに移動します。
b) 侵入ポリシーで、[詳細設定（Advanced Settings）] > [Syslog アラート（Syslog Alerting）] > [有効（Enabled）] をクリックします。
c) 必要に応じて、[編集（Edit）] をクリックします。
d) オプションを入力します。

オプション	値
ロギングホスト	他の syslog メッセージを送信する syslog サーバーとは異なるサーバーに侵入イベントの syslog メッセージを送信するのでなければ、空白のままにします（前の手順で指定した設定が使用される）。
ファシリティ	この設定は、このページでロギングホストを指定した場合にのみ適用されます。 説明については、Syslog アラート ファシリティ （678 ページ） を参照してください。
重大度	この設定は、このページでロギングホストを指定した場合にのみ適用されます。 説明については、syslog 重大度レベル （679 ページ） を参照してください。

e) [戻る（Back）] をクリックします。

f) 左側にあるナビゲーションウィンドウの [ポリシー情報（Policy Information）] をクリックします。
g) [変更を確定（Commit Changes）] をクリックします。

次のタスク

- （任意）個別のポリシーおよびルールに異なるロギング設定を指定します。

  にある該当する表の行を参照してください。

  これらの設定には、Syslog アラート応答の作成 （677 ページ）の説明に従って設定される syslog アラート応答が必要です。この手順で指定したプラットフォーム設定は使用されません。

- 従来型デバイスのセキュリティイベント syslog ロギングを設定するには、従来型デバイスからのセキュリティイベント syslog メッセージの送信 （773 ページ）を参照してください。
- 変更が完了したら、変更を管理対象デバイスに展開します。

従来型デバイスからのセキュリティイベント syslog メッセージの送信

始める前に

- セキュリティイベントを生成するポリシーを設定します。
- デバイスが syslog サーバーに到達できることを確認します。
- syslog サーバーがリモートメッセージを受け入れられることを確認します。
- 接続ロギングに関する重要な情報については、接続ロギング （879 ページ）の章を参照してください。

手順

ステップ 1 従来型デバイスのアラート応答を設定します。

Syslog アラート応答の作成 （677 ページ） を参照してください。

ステップ 2 アクセス コントロール ポリシーで syslog 設定を指定します。

a) [ポリシー（Policies）] > [アクセスコントロール（Access Control）] をクリックします。
b) 該当するアクセス コントロール ポリシーを編集します。
c) [ロギング（Logging）] をクリックします。
d) [特定の syslog アラートを使用して送信する（Send using specific syslog alert）] をオンにします。
e) 上記で作成した **syslog アラート**を選択します。
f) [**保存（Save）**] をクリックします。

ステップ 3 ファイルイベントとマルウェアイベントを送信する場合は、次の手順を実行します。

a) [ファイル/マルウェアイベントの syslog メッセージを送信する（Send Syslog messages for File and Malware events）] をオンにします。

b) [**保存（Save**）] をクリックします。

ステップ 4 侵入イベントを送信する場合は、次の手順を実行します。

a) アクセス コントロール ポリシーに関連付けられている侵入ポリシーに移動します。

b) 侵入ポリシーで、[詳細設定（Advanced Settings）] > [Syslog アラート（Syslog Alerting）] > [有効（Enabled）] をクリックします。

c) 必要に応じて、[編集（Edit）] をクリックします。

d) オプションを入力します。

オプション	値
ロギングホスト	他の syslog メッセージを送信する syslog サーバーとは異なるサーバーに侵入イベントの syslog メッセージを送信するのでなければ、空白のままにします（前の手順で指定した設定が使用される）。
ファシリティ	この設定は、このページでロギングホストを指定した場合にのみ適用されます。 Syslog アラート ファシリティ （678 ページ） を参照してください。
重大度	この設定は、このページでロギングホストを指定した場合にのみ適用されます。 syslog 重大度レベル （679 ページ） を参照してください。

e) [戻る（Back）] をクリックします。

f) 左側にあるナビゲーションウィンドウの [ポリシー情報（Policy Information）] をクリックします。

g) [変更を確定（Commit Changes）] をクリックします。

次のタスク

- （オプション）アクセス コントロール ルールごとに異なるロギング設定を指定します。接続およびセキュリティ インテリジェンス イベント の syslog の設定場所（すべてのデバイス） （775 ページ） の該当するテーブル行を参照してください。これらの設定には、Syslog アラート応答の作成 （677 ページ）の説明に従って設定される syslog アラート応答が必要です。前の手順で指定した設定は使用されません。
- Threat Defense デバイスのセキュリティイベント syslog ロギングを設定するには、Threat Defense デバイスからのセキュリティイベント syslog メッセージの送信 （770 ページ） を参照してください。

セキュリティ イベントの syslog の設定場所

接続およびセキュリティ インテリジェンス イベント の syslog の設定場所（すべてのデバイス）

多くの場所でロギング設定を実行できます。次の表を使用して、必要なオプションが設定されていることを確認します。

重要

- syslog の設定を行う場合、特に他の設定から継承したデフォルトを使用する際には細心の注意が必要です。下の表に示すように、オプションの中にはすべての管理対象デバイス モデルやソフトウェア バージョンに使用できないものもあります。
- 接続ロギングを設定する際の重要な情報については、接続ロギング （879 ページ）の章を参照してください。

設定の場所	説明と詳細情報
[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）]、Threat Defense 設定ポリシー、[Syslog]	このオプションは、Threat Defense デバイスにだけ適用されます。 ここで行う設定は、アクセス コントロール ポリシーのロギング設定に指定でき、この表の残りのポリシーとルールに使用するか、それらをオーバーライドできます。 Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

設定の場所	説明と詳細情報
[ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[ロギング（Logging）]	ここで行う設定は、この表の残りの行で指定する場所の子孫のポリシーおよびルールにあるデフォルトをオーバーライドしない限り、すべての接続イベントとセキュリティ インテリジェンス イベントの syslog のデフォルト設定になります。 Threat Defense デバイスの推奨設定：Threat Defense プラットフォーム設定を使用します。詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。 その他のすべてのデバイスに必要な設定：syslog アラートを使用します。 syslog アラートを指定する場合は、Syslog アラート応答の作成 （677 ページ）を参照してください。 [ロギング（Logging）]タブの設定に関する詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。
[ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[ルール（Rules）]、[デフォルトアクション（Default Action）]行、[ロギング（Logging）]（ ）	ロギングのアクセス コントロール ポリシーに関連付けられているデフォルト アクションを設定します。 Cisco Secure Firewall Management Center デバイス構成ガイドおよびポリシーのデフォルト アクションによる接続のロギング （896 ページ）でロギングに関する情報を参照してください。
[ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[ルール（Rules）]、<各ルール>、[ロギング（Logging）]	特定のルールの設定をアクセス制御ポリシーにログインします。 ログ方法の詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

設定の場所	説明と詳細情報
[ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[セキュリティ インテリジェンス（Security Intelligence）]、[ロギング（Logging）]（  ）	セキュリティインテリジェンスブロックリストのロギング設定。 次のボタンをクリックして設定します。 • [DNS ブロック リスト ロギング オプション（DNS Block List Logging Options）] • [URL ブロック リスト ロギング オプション（URL Block List Logging Options）] • [ネットワーク ブロック リスト ロギング オプション（Network Block List Logging Options）]（ブロックされたリスト上の IP アドレス用） Cisco Secure Firewall Management Center デバイス構成ガイド
[ポリシー（Policies）]>[SSL]、<各ポリシー>、[デフォルトアクション（Default Action）] 行、[ロギング（Logging）]（  ）	SSL ポリシーに関連付けられているデフォルト アクションのロギング設定。 ポリシーのデフォルト アクションによる接続のロギング（896 ページ）を参照してください。
[ポリシー（Policies）]>[SSL]、<各ポリシー>、<各ルール>、[ロギング（Logging）]	SSL ルールのロギング設定。 Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。
[ポリシー（Policies）]>[プレフィルタ（Prefilter）]、<各ポリシー>、[デフォルトアクション（Default Action）] 行、[ロギング（Logging）]（  ）	プレフィルタ ポリシーに関連付けられているデフォルト アクションのロギング設定。 ポリシーのデフォルト アクションによる接続のロギング（896 ページ）を参照してください。
[ポリシー（Policies）]>[プレフィルタ（Prefilter）]、<各ポリシー>、<各プレフィルタルール>、[ロギング（Logging）]	プレフィルタ ポリシーの各プレフィルタのロギング設定。 参照：Cisco Secure Firewall Management Center デバイス構成ガイド
[ポリシー（Policies）]>[プレフィルタ（Prefilter）]、<各ポリシー>、<各トンネルルール>、[ロギング（Logging）]	プレフィルタ ポリシーの各トンネル ルールのロギング設定。 参照：Cisco Secure Firewall Management Center デバイス構成ガイド
Threat Defense クラスタ構成の追加 syslog の設定：	Cisco Secure Firewall Management Center デバイス構成ガイドには syslog について複数の言及があります。「syslog」の章を検索してください。

侵入イベントの syslog の設定場所（Threat Defense デバイス）

侵入ポリシーの syslog 設定はさまざまな場所で指定でき、必要に応じてアクセス コントロール ポリシーまたは Threat Defense プラットフォーム設定、あるいはその両方から設定を継承できます。

設定の場所	説明と詳細情報
[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]、Threat Defense 設定ポリシー、[Syslog]	ここで設定した syslog の宛先は、侵入ポリシーのデフォルトとして使用可能なアクセス コントロール ポリシーの [ロギング（Logging）] タブで指定できます。 Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。
[ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[ロギング（Logging）]	侵入ポリシーに他のロギング ホストが指定されていない場合は、侵入イベントの syslog の宛先のデフォルト設定。 Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。
[ポリシー（Policies）] > [侵入（Intrusion）]、<各ポリシー>、[詳細設定（Advanced Settings）]、[syslog アラート（Syslog Alerting）] を有効化、[編集（Edit）] をクリック	アクセス コントロール ポリシーの [ロギング（Logging）] タブで指定した宛先以外の syslog コレクタを指定するには、侵入イベントの Syslog アラートの設定 （688 ページ）を参照してください。 [重大度（Severity）] または [ファシリティ（Facility）]、あるいはその両方を侵入ポリシーで設定されているとおりに使用する場合は、ポリシーにロギング ホストを設定する必要があります。アクセス コントロール ポリシーに指定されているロギング ホストを使用する場合は、侵入ポリシーに指定されている重大度とファシリティは使用されません。
ポリシー > アクセス制御 > ロギング > IPS 設定	IPS イベントの syslog メッセージを送信したい場合。設定したデフォルトの syslog 設定は、IPS イベントの syslog 宛先に使用されます。

侵入イベントの syslog の設定場所（Threat Defense 以外のデバイス）

- （デフォルト）アクセス コントロール ポリシー（Cisco Secure Firewall Management Center デバイス構成ガイドsyslog アラートを指定した場合）（Syslog アラート応答の作成 （677 ページ）を参照）
- または侵入イベントの Syslog アラートの設定 （688 ページ）を参照してください。

デフォルトでは、侵入ポリシーはアクセス コントロール ポリシーの [ロギング（Logging）] タブの設定を使用します。Threat Defense 以外のデバイスに適用される設定がない場合は、Threat Defense 以外のデバイスの syslog は送信されず、警告は表示されません。

ファイルとマルウェア イベントの syslog の設定場所

設定の場所	説明と詳細情報
アクセス コントロール ポリシーで次の手順を実行します。 [ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[ロギング（Logging）]	これは、ファイルとマルウェアのイベントの syslog を送信するようにシステムを設定するための主要な場所です。 Threat Defense プラットフォーム設定の syslog 設定を使用しない場合は、アラート応答も作成する必要があります。Syslog アラート応答の作成 （677 ページ）を参照してください。
Threat Defense プラットフォーム設定で次の手順を実行します。 [デバイス（Devices）]>[プラットフォーム設定（Platform Settings）]、Threat Defense 設定ポリシー、[Syslog]	これらの設定は、サポート対象のバージョンを実行しており、Threat Defense プラットフォーム設定を使用するようにアクセス コントロール ポリシーの [ロギング（Logging）] タブを設定している場合にのみ、Threat Defense デバイスにのみ適用されます。 Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。
アクセス コントロール ルールで次の手順を実行します。 [ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、<各ルール>、[ロギング（Logging）]	Threat Defense プラットフォーム設定の syslog 設定を使用しない場合は、アラート応答も作成する必要があります。Syslog アラート応答の作成 （677 ページ） を参照してください。

セキュリティ イベントの syslog メッセージの分析

Threat Defense からのセキュリティ イベント メッセージの例（侵入イベント）

```
  0        1              2                3       4   5      6

<37>2018-06-27 192.168.0.81 SFIMS : %FTD-5-43000
192.168.1.10, DstIP: 192.168.1.102, SrcPort: 339
Protocol: tcp, Priority: 2, GID: 133, SID: 17, Re
Message: "DCE2_EVENT   SMB_INVALID_DSIZE", Classi
Potentially Bad Traffic, User: No Authentication
Client: NetBIOS-ssn (SMB) client, ApplicationPro
(SMB), ACPolicy: test, NAPPolicy: Balanced Secur
Connectivity, InlineResult: Blocked
```

表 *63* : セキュリティ イベントの *syslog* メッセージのコンポーネント

サンプル メッセージの項目数	ヘッダー要素	説明
[0]	PRI	ファシリティとアラートのシビラティ（重大度）の両方を表すプライオリティ値です。Management Center プラットフォーム設定を使用して EMBLEM 形式でのロギングを有効にした場合にのみ、この値が syslog メッセージに表示されます。アクセス コントロール ポリシーの [ロギング（Logging）] タブを使用して侵入イベントのロギングを有効にすると、PRI 値が自動的に syslog メッセージに表示されます。EMBLEM形式を有効にする方法については、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。PRI の詳細については、「RFC5424」を参照してください。

サンプル メッセージの項目数	ヘッダー要素	説明
1	タイムスタンプ	syslog メッセージがデバイスから送信された日付と時刻。 • （Threat Defense デバイスから送信された syslog）アクセス コントロール ポリシーとその子孫の設定を使用して送信した syslog の場合か、または [Threat Defenseプラットフォーム設定（Threat Defense Platform Settings）] のこの形式を使用するように指定されている場合、日付形式は RFC 5424 に指定されている ISO 8601 タイムスタンプ形式（yyyy-MM-ddTHH:mm:ssZ）に定義されている形式になります。この形式では文字 Z は UTC タイムゾーンを示しています。 • （その他すべてのデバイスから送信された syslog）アクセス コントロール ポリシーとその子孫の設定を使用して送信した syslog の場合、日付形式は RFC 5424 に指定されている ISO 8601 タイムスタンプ形式（yyyy-MM-ddTHH:mm:ssZ）に定義されている形式になります。この形式では文字 Z は UTC タイムゾーンを示しています。 • それ以外の場合は UTC タイム ゾーンの月、日、時刻になりますが、タイム ゾーンは表示されません。 [Threat Defenseプラットフォーム設定（Threat Defense Platform Settings）] でタイムスタンプ設定を指定するには、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。
2	メッセージが送信されたデバイスまたはインターフェイス。 ここに表示される値は次のとおりです。 • インターフェイスの IP アドレス • デバイスのホスト名 • カスタム デバイス識別子	（Threat Defense デバイスから送信された syslog の場合） [Threat Defenseプラットフォーム設定（Threat Defense Platform Settings）] を使用して syslog メッセージが送信された場合で、[SyslogデバイスIDの有効化（Enable Syslog Device ID）] オプションが指定されているときは、これはそのオプションの [Syslog設定（Syslog Settings）] に設定されている値になります。 それ以外の場合、この要素はヘッダーには表示されません。 [Threat Defenseプラットフォーム設定（Threat Defense Platform Settings）] でこの設定を指定するには、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

サンプル メッセージの項目数	ヘッダー要素	説明
3	カスタム値	アラート応答を使用してメッセージが送信された場合、これは、メッセージを送信したアラート応答に設定されている**タグ**値がある場合は、その値になります。（Syslogアラート応答の作成 （677 ページ） を参照）。 それ以外の場合、この要素はヘッダーには表示されません。
4	%FTD	メッセージを送信したデバイスのタイプ。%FTD は Cisco Secure Firewall Threat Defense です。
5	重大度	メッセージをトリガーしたポリシーの syslog 設定に指定されている重要度。 シビラティ（重大度）については、Cisco Secure Firewall Management Center デバイス構成ガイドの「*Severity Levels*」または syslog 重大度レベル （679 ページ） を参照してください。
6	イベント タイプ識別子	• 430001：侵入イベント • 430002：接続の開始時に記録された接続イベント • 430003：接続の終了時に記録された接続イベント • 430004：ファイル イベント • 430005：ファイル マルウェア イベント
--	ファシリティ	セキュリティ イベントの syslog メッセージのファシリティ （783 ページ） を参照してください。

サンプル メッセージの項目数	ヘッダー要素	説明
--	メッセージの残りの部分	コロンで区切られたフィールドと値。 空または不明な値のあるフィールドはメッセージから省略されます。 フィールドの説明については、次を参照してください。 • 接続およびセキュリティ関連の接続イベントフィールド（902 ページ）。 • 侵入イベント フィールド （948 ページ） • ファイルおよびマルウェア イベント フィールド（1011 ページ） （注） フィールド説明のリストには、syslog フィールドとイベントビューア（Management Center の Web インターフェイスの [分析（Analysis）] メニューのメニューオプション）に表示されるフィールドの両方が含まれています。syslog 経由で使用可能なフィールドはそれを示すラベルが付けられます。 イベント ビューアに表示される一部のフィールドは、syslog 経由では使用できません。また、一部の syslog フィールドはイベント ビューアには含まれていません（ただし、検索を使用すると表示できる場合があります）。また、一部のフィールドは結合されているか、または個別になっています。

セキュリティ イベントの syslog メッセージのファシリティ

一般に、セキュリティ イベントの syslog メッセージではファシリティ値は関連性がありません。ただし、ファシリティが必要な場合は、次の表を使用してください。

デバイス	接続イベントにファシリティを含める場合	侵入イベントにファシリティを含める場合	syslog メッセージ内の場所
Threat Defense	[Threat Defenseプラットフォーム設定（Threat Defense Platform Settings）] の [EMBLEM] オプションを使用します。 [Threat Defenseプラットフォーム設定（Threat Defense Platform Settings）] を使用してsyslogメッセージを送信すると、ファシリティは常に、接続イベントに対して [アラート（ALERT）] になります。	[Threat Defenseプラットフォーム設定（Threat Defense Platform Settings）] の [EMBLEM] オプションを使用するか、または侵入ポリシーのsyslog設定を使用してロギングを設定します。侵入ポリシーを使用した場合は、侵入ポリシー設定にロギング ホストも指定する必要があります。 syslog アラートを有効にし、侵入ポリシーでファシリティとシビラティ（重大度）を設定します。侵入イベントの Syslog アラートの設定 （688 ページ）を参照してください。	ファシリティはメッセージヘッダーには表示されませんが、syslog コレクタが RFC 5424、セクション 6.2.1 に基づいて値を派生させることができます。
Threat Defense 以外のデバイス	アラート応答を使用します。	侵入ポリシーの高度な設定のsyslog設定、またはアクセス コントロール ポリシーの [ロギング（Logging）] タブで識別されているアラート応答を使用します。	

詳細については、「侵入 syslog アラートの機能と重大度 （689 ページ）」および「Syslog アラート応答の作成 （677 ページ）」を参照してください。

Firepower syslog メッセージのタイプ

Firepower は、次の表で説明するように、複数の syslog データ タイプを送信できます。

syslog データ タイプ	参照先
Management Center からの監査ログ	syslog への監査ログのストリーミング （52 ページ）および監査と Syslog （497 ページ）の章
Threat Defense デバイスからのデバイス正常性およびネットワーク関連のログ	Cisco Secure Firewall Management Center デバイス構成ガイド

syslog データ タイプ	参照先
Threat Defense デバイスからの接続、セキュリティインテリジェンス、および侵入イベントログ	syslog にセキュリティイベントデータを送信するためのシステムの設定について （768 ページ）。
クラッシック デバイスからの接続、セキュリティインテリジェンスおよび侵入イベント ログ	syslog にセキュリティイベントデータを送信するためのシステムの設定について （768 ページ）
ファイルおよびマルウェアのイベントのログ	syslog にセキュリティイベントデータを送信するためのシステムの設定について （768 ページ）
IPS 設定	「IPS イベントの Syslog メッセージを送信する」。 侵入イベントの syslog の設定場所（Threat Defense デバイス）（778 ページ）

セキュリティ イベントの syslog の制限事項

- syslog またはストアイベントを外部で使用する場合は、ポリシー名やルール名などのオブジェクト名に特殊文字を使用しないでください。オブジェクト名には、カンマなどの特殊文字を含めることはできません。受信側アプリケーションで区切り文字として使用される可能性があります。
- syslog コレクタにイベントを表示するには最大 15 分かかる場合があります。
- 次のファイルおよびマルウェアのイベントのデータは syslog 経由で使用できません。
  - レトロスペクティブ イベント
  - Cisco Secure Endpoint によって生成されたイベント

eStreamer サーバー ストリーミング

Event Streamer（eStreamer）を使用すると、Secure Firewall Management Center からの数種類のイベント データを、カスタム開発されたクライアント アプリケーションにストリーム配信できます。詳細については、*Firepower System Event Streamer* 統合ガイド [英語] を参照してください。

eStreamer サーバとして使用するアプライアンスで eStreamer イベントの外部クライアントへのストリームを開始するには、その前に、イベントをクライアントに送信するように eStreamer サーバを設定し、クライアントに関する情報を指定して、通信を確立するときに使用する認証クレデンシャルを生成する必要があります。アプライアンスのユーザインターフェイスからこれらすべてのタスクを実行できます。設定が保存されると、選択したイベントが、要求時に、eStreamer クライアントに転送されます。

要求したクライアントに eStreamer サーバが送信できるイベント タイプを制御できます。

表 *64 : eStreamer* サーバで送信可能なイベント タイプ

イベントタイプ	説明
侵入イベント	管理対象デバイスによって生成される侵入イベント
侵入イベント パケット データ	侵入イベントに関連付けられたパケット
侵入イベント追加データ	HTTP プロキシまたはロード バランサ経由で Web サーバに接続しているクライアントの発信元 IP アドレスのような侵入イベントに関連付けられた追加データ
検出イベント	ネットワーク検出イベント
相関および許可リスト（Allow List）イベント	相関およびコンプライアンスのallowリストイベント
インパクト フラグ アラート	Management Center によって生成されたインパクト アラート
ユーザー イベント	ユーザ イベント
マルウェア イベント	マルウェア イベント
ファイル イベント	ファイル イベント
接続イベント	モニタ対象のホストとその他のすべてのホスト間のセッション トラフィックに関する情報

セキュリティ イベントの syslog と eStreamer の比較

一般に、現在 eStreamer に重大な既存イベントがない組織は、セキュリティ イベント データを外部で管理するのに eStreamer ではなく syslog を使用する必要があります。

Syslog	eStreamer
カスタマイズの必要なし	各リリースの変更に対応するには、大幅なカスタマイズと継続メンテナンスが必要
標準	専用
syslog 標準規格では、データ損失に対する保護はありません（特にUDPを使用している場合）	データ損失に対する保護
デバイスから直接送信	Management Center から送信（処理オーバーヘッドが加わる）

Syslog	eStreamer
ファイルイベントとマルウェアイベント、接続イベント（セキュリティ インテリジェンス イベントを含む）、および侵入イベントをサポートします。	eStreamer サーバー ストリーミング （785 ページ）に示されているすべてのイベント タイプをサポートします。
一部のイベントデータは、Management Center からのみ送信できます。eStreamer 経由でのみ送信でき、syslog 経由では送信できないデータ （787 ページ）を参照してください。	デバイスから syslog を介して直接送信することができないデータが含まれます。eStreamer 経由でのみ送信でき、syslog 経由では送信できないデータ （787 ページ） を参照してください。

eStreamer 経由でのみ送信でき、syslog 経由では送信できないデータ

次のデータは Secure Firewall Management Center からのみ使用可能であるため、デバイスから syslog を介して送信することはできません。

- パケット ログ
- 侵入イベント追加データ イベント

  説明については、eStreamer サーバー ストリーミング （785 ページ）を参照してください。
- 統計情報と集約イベント
- ネットワーク検出イベント
- ユーザー アクティビティとログイン イベント
- 相関イベント
- マルウェア イベントの場合：
  - レトロスペクティブな判定
  - 関連する SHA に関する情報がすでにデバイスに同期されている場合を除き、脅威の名前と性質
- 次のフィールド：
  - [Impact] および [ImpactFlag] フィールド

    説明については、eStreamer サーバー ストリーミング （785 ページ）を参照してください。
  - [IOC_Count] フィールド
- ほとんどの raw ID と UUID。

  次に例外を示します。

- 接続イベントの syslog には次のものがあります。FirewallPolicyUUID、FirewallRuleID、TunnelRuleID、MonitorRuleID、SI_CategoryID、SSL_PolicyUUID、および SSL_RuleID
- 侵入イベントの syslog には、IntrusionPolicyUUID、GeneratorID、および SignatureID が含まれます。

- 以下を含むがこれらに限定されない拡張メタデータ：
  - 氏名、部署、電話番号などの LDAP によって提供されるユーザーの詳細。

    syslog では、イベントのユーザー名のみが提供されます。
  - SSL 証明書の詳細などの状態ベースの情報の詳細。

    syslog は、証明書のフィンガープリントなどの基本的な情報を提供しますが、cert CN など、証明書のその他の詳細は提供しません。
  - アプリケーション タグやカテゴリなどの詳細なアプリケーション情報。

    syslog はアプリケーション名のみを提供します。

  一部のメタデータ メッセージには、オブジェクトに関する追加情報も含まれています。
- 地理位置情報

eStreamer イベントタイプの選択

eStreamer サーバーで送信可能なイベントの [eStreamer イベント設定（eStreamer Event Configuration）] チェックボックス管理。クライアントは、eStreamer サーバに送信する要求メッセージで受信するイベント タイプを具体的に要求する必要があります。詳細については、『*Firepower System Event Streamer Integration Guide*』を参照してください。

マルチドメイン展開では、どのドメインのレベルでも eStreamer のイベント構成を設定できます。ただし、先祖ドメインで特定のイベントタイプが有効になっている場合は、子孫ドメインのそのイベントタイプを無効にすることはできません。

Management Center に対してこのタスクを実行するには、管理者ユーザーである必要があります。

手順

ステップ 1 **[統合（Integration）] > [その他の統合（Other Integrations）]** を選択します。

ステップ 2 [eStreamer] をクリックします。

ステップ 3 [eStreamer イベント設定（eStreamer Event Configuration）] の下で、eStreamer サーバー ストリーミング（785 ページ）の説明に従って要求元のクライアントに転送するイベントタイプの横にあるチェックボックスをオンまたはオフにします。

ステップ 4 [保存（Save）] をクリックします。

eStreamer クライアント通信の設定

eStreamer がクライアントに eStreamer イベントを送信するには、その前に、eStreamer ページから eStreamer サーバーのピアデータベースにクライアントを追加しておく必要があります。また、eStreamer サーバーによって生成された認証証明書をクライアントにコピーする必要もあります。この手順を完了した後、クライアントが eStreamer サーバに接続できるように eStreamer サービスを再起動する必要はありません。

マルチドメイン展開では、任意のドメインで eStreamer クライアントを作成できます。認証証明書では、クライアントはクライアント証明書のドメインと子孫ドメインからのみイベントを要求することが許可されます。eStreamer 設定ページには、現在のドメインに関連付けられているクライアントのみが表示されるため、証明書をダウンロードまたは取り消す場合は、クライアントが作成されたドメインに切り替えます。

Management Center に対してこのタスクを実行するには、管理者または検出管理者ユーザーである必要があります。

手順

ステップ 1 **[統合（Integration）]** > **[その他の統合（Other Integrations）]** を選択します。

ステップ 2 [eStreamer] をクリックします。

ステップ 3 [クライアントの作成（Create Client）] をクリックします。

ステップ 4 [ホスト名（Hostname）] フィールドに、eStreamer クライアントを実行しているホストのホスト名または IP アドレスを入力します。

（注） DNS 解決を設定していない場合は、IP アドレスを使用します。

ステップ 5 証明書ファイルを暗号化するには、[パスワード（Password）] フィールドにパスワードを入力します。

ステップ 6 [Save] をクリックします。
これで、eStreamer サーバは、ホストが eStreamer サーバ上のポート 8302 にアクセスすることを許可し、クライアント/サーバ認証時に使用する認証証明書を作成します。

ステップ 7 クライアントのホスト名の横にある[ダウンロード（Download）]（ アイコン）をクリックして、証明書ファイルをダウンロードします。

ステップ 8 SSL 認証のためにクライアントが使用する適切なディレクトリに証明書ファイルを保存します。

ステップ 9 クライアントのアクセスを取り消すには、削除するホストの横にある[削除（Delete）]（ ）をクリックします。

eStreamer サービスを再起動する必要はありません。アクセスはただちに取り消されます。

Splunk でのイベント分析

（以前 Cisco Firepower App for Splunk と呼ばれていた）Cisco Secure Firewall（f.k.a. Firepower）app for Splunk を外部ツールとして使用して、Firepower イベントデータを表示して操作し、ネットワーク上の脅威をハントおよび調査することができます。

eStreamer が必要です。これは高度な機能です。eStreamer サーバー ストリーミング （785 ページ）を参照してください。

詳細については、https://cisco.com/go/firepower-for-splunkを参照してください。

IBM QRadar でのイベント分析

IBM QRadar 向けの Cisco Firepower アプリケーションをイベントデータを表示するための代替手段として使用して、ネットワークへの脅威の分析、ハント、および調査をすることができます。

eStreamer が必要です。これは高度な機能です。eStreamer サーバー ストリーミング （785 ページ）を参照してください。

詳細については、https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/QRadar/integration-guide-for-the-cisco-firepower-app-for-ibm-qradar.htmlを参照してください。

外部ツールを使用したイベント データの分析の履歴

機能	最小 Management Center	最小 Threat Defense	詳細
SecureX のリボン	7.0	任意（Any）	SecureX のリボンは SecureX にピボットされ、シスコのセキュリティ製品全体の脅威の状況を即座に確認できます。 Management Center で SecureX のリボンを表示するには、https://cisco.com/go/firepower-securex-documentation で『*Firepower and SecureX Integration Guide*』を参照してください。 新規/変更されたページ：新規ページ：[システム（System）]>[SecureX]
すべての接続イベントを Cisco Cloud に送信する	7.0	任意（Any）	優先順位の高い接続イベントだけでなく、すべての接続イベントを Cisco Cloud に送信できるようになりました。 新規/変更された画面：[システム（System）]>[統合（Integration）]>[クラウドサービス（Cloud Services）] ページの新しいオプション

機能	最小 Management Center	最小 Threat Defense	詳細
Secure Network Analytics でデータを表示するためのクロス起動	6.7	任意（Any）	この機能では、[分析（Analysis）] > [コンテキストクロス起動（Contextual Cross-Launch）] ページで Secure Network Analytics アプライアンスの複数のエントリをすばやく作成する方法が導入されています。 これらのエントリを使用すると、関連するイベントを右クリックして Secure Network Analytics をクロス起動し、クロス起動したデータポイントに関連する情報を表示できます。 新しいメニュー項目：[システム（System）] > [ロギング（Logging）] > [セキュリティ分析とロギング（Security Analytics and Logging）] Secure Network Analytics へのイベント送信を設定する新しいページ。
追加のフィールドタイプからのコンテキストクロス起動	6.7	任意（Any）	次のイベントデータの追加タイプを使用して、外部アプリケーションに相互起動できるようになりました。 • アクセス コントロール ポリシー • 侵入ポリシー • アプリケーションプロトコル • クライアント アプリケーション • Web アプリケーション • ユーザー名（レルムを含む） 新しいメニューオプション：[分析（Analysis）] メニューの下のページで、ダッシュボードウィジェットおよびイベントテーブルのイベントに関して上記のデータタイプを右クリックすると、コンテキストクロス起動オプションが使用できるようになりました。 サポートされているプラットフォーム： Secure Firewall Management Center
IBM QRadar との統合	6.0 以降	任意（Any）	IBM QRadar ユーザーは、新しい Firepower 固有のアプリを使用してイベントデータを分析できます。 どの機能を使用できるかは、Firepower のバージョンによって異なります。 IBM QRadar でのイベント分析 （790 ページ）を参照してください。

機能	最小 Management Center	最小 Threat Defense	詳細
と統合するための拡張機能 SecureX Threat Response	6.5	任意（Any）	• 地域的なクラウドをサポートします。 • 米国（北米） • 欧州 • 追加イベント タイプのサポート： • ファイルおよびマルウェアのイベント • 優先順位の高い接続イベント これらは、次に関連する接続イベントです。 • 侵入イベント • セキュリティ インテリジェンス イベント • ファイルおよびマルウェアのイベント 変更された画面：[システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）] の新規オプション。 サポートされるプラットフォーム：直接統合または syslog を介して、このリリースでサポートされているすべてのデバイス。
Syslog	6.5	任意（Any）	[AccessControlRuleName] フィールドが、侵入イベントの syslog メッセージで使用できるようになりました。
Cisco Security Packet Analyzer との統合	6.5	任意（Any）	この機能はサポートされなくなりました。
SecureX Threat Response との統合	6.3（syslog 経由、プロキシ コレクタを使用） 6.4（直接）	任意（Any）	SecureX Threat Response の強力な分析ツールを使用し、Firepower 侵入イベントデータを他のソースのデータと統合して、ネットワーク上の脅威を統合ビューに表示します。 変更された画面（バージョン 6.4）：[システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）] の新規オプション。 サポートされるプラットフォーム：バージョン 6.3（syslog 経由）または 6.4 を実行している Secure Firewall Threat Defense デバイス

機能	最小 Management Center	最小 Threat Defense	詳細
ファイルとマルウェアのイベントの syslog サポート	6.4	任意（Any）	完全修飾ファイルおよびマルウェアのイベントデータが syslog 経由で管理対象デバイスから送信できるようになりました。 変更された画面：[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）] > [ロギング（Logging）]。 サポート対象プラットフォーム：バージョン 6.4 を実行している管理対象のすべてのデバイス
Splunk との統合	すべての 6.x バージョンのサポート	任意（Any）	Splunk のユーザーは、新しい個別の Splunk アプリケーションである Cisco Secure Firewall（f.k.a. Firepower）app for Splunk を使用してイベントを分析できます。 どの機能を使用できるかは、Firepower のバージョンによって異なります。 Splunk でのイベント分析 （790 ページ）を参照してください。
Cisco Security Packet Analyzer との統合	6.3	任意（Any）	導入された機能：Cisco Security Packet Analyzer にイベントに関連するパケットについてすぐにクエリを実行した後、クリックして Cisco Security Packet Analyzer の結果を調べるか、またはダウンロードして別の外部ツールで分析します。 新規画面： **[システム（System）] > [統合（Integration）] > [パケットアナライザ（Packet Analyzer）]** **[分析（Analysis）] > [詳細（Advanced）] > [パケットアナライザのクエリ（Packet Analyzer Queries）]** 新規メニュー オプション：[ダッシュボード（Dashboard）] ページおよび [分析（Analysis）] メニューのページのイベント テーブルを右クリックしたときの [クエリ パケット アナライザ（Query Packet Analyzer）] のメニュー項目 サポートされるプラットフォーム Secure Firewall Management Center

機能	最小 Management Center	最小 Threat Defense	詳細
コンテキストクロス起動	6.3	任意（Any）	導入された機能：イベントを右クリックし、事前に定義されているか、またはカスタム URL ベースの外部リソースの関連情報を検索します。 新規画面：**[分析（Analysis）] > [詳細設定（Advanced）] > [コンテキストクロス起動（Contextual Cross-Launch）]** 新規メニュー オプション：[ダッシュボード（Dashboard）] ページおよび [分析（Analysis）] メニュー ページのイベント テーブルを右クリックしたときに表示される複数のオプション サポートされるプラットフォーム Secure Firewall Management Center
接続イベントと侵入イベントの syslog メッセージ	6.3	任意（Any）	統合され、簡略化された新しい設定を使用して、完全修飾接続および侵入イベントを外部ストレージおよびツールに syslog 経由で送信する機能。メッセージ ヘッダーが標準化されてイベント タイプ識別子が組み込まれ、メッセージが小型になりました。これは、不明な値や空の値が含まれたフィールドが省略されるためです。 サポート対象プラットフォーム： • すべての新機能：バージョン 6.3 を実行している Threat Defense デバイス。 • 一部の新機能：バージョン 6.3 を実行している Threat Defense 以外のデバイス。 • 少数の新機能：6.3 よりも前のバージョンを実行しているすべてのデバイス。 詳細については、セキュリティイベントの syslog メッセージの送信について（768ページ）のトピックとサブトピックを参照してください。
eStreamer	6.3	任意（Any）	eStreamer の内容をホストのアイデンティティ ソースに関する章からこの章に移動し、eStreamer と syslog を比較した概要を追加しました。

第 VII 部

ワークフローとテーブル

第 27 章

ワークフロー

以下のトピックでは、ワークフローの使用方法について説明します。

概要：ワークフロー

ワークフローは Management Center Web インターフェイス上でユーザに合わせて作成された一連のデータ ページで、アナリストはワークフローを使用して、システムで生成されたイベントを評価することができます。

Management Center では、以下のタイプのワークフローを使用できます。

定義済みワークフロー

システムに付属のプリセット ワークフローです。定義済みのワークフローの編集や削除を行うことはできません。ただし、定義済みワークフローをコピーして、そのコピーをカスタム ワークフローの基礎として使用することができます。

保存済みのカスタム ワークフロー

Management Center に付属の保存済みカスタム テーブルに基づくカスタム ワークフロー。これらのワークフローは編集、削除、コピーすることができます。

カスタム ワークフロー

特定のニーズに対応するために作成してカスタマイズするワークフロー、またはカスタム テーブルを作成するとシステムによって自動的に生成されるワークフローです。これらのワークフローは編集、削除、コピーすることができます。

通常、ワークフローに表示されるデータは、管理対象デバイスのライセンスおよび展開状況や、データを提供する機能を設定しているかどうかによって異なります。

定義済みワークフロー

以下の項で説明する定義済みワークフローは、システムに付属しているものです。定義済みワークフローを編集または削除することはできません。ただし、定義済みワークフローをコピーして、そのコピーをカスタム ワークフローのベースとして使用することができます。

定義済み侵入イベントのワークフロー

次の表では、システムに備わっている定義済み侵入イベントのワークフローについて説明します。

表 *65*：定義済み侵入イベントのワークフロー

ワークフロー名	説明
接続先ポート	接続先ポートは、通常、アプリケーションに紐付けされているため、このワークフローにより、異常な大容量アラートを経験しているアプリケーションを検出できます。接続先ポート カラムにより、ネットワーク上に存在してはならないアプリケーションを特定できます。
イベント特定	このワークフローでは、2つの有用な特徴を提供します。イベントが頻繁に発生する場合には、次のことを示します： • 誤検出 • ワーム • 不正確な誤設定ネットワーク 発生頻度の低いイベントは、対象となる攻撃を最も確実に示す証拠であり、特別な注意を必要とします。
優先度および分類によるイベント	このワークフローでは、イベントとタイプのリストをそれぞれのイベントが発生した回数と共にイベントの優先度の順に示します。
接続先に対するイベント	このワークフローでは、攻撃されているホスト IP アドレスや攻撃の本質のハイレベル ビューを提示します。利用可能な場合、攻撃に関与する国に関する情報を確認することもできます。
IP 特定	このワークフローでは、最も多くのアラートを発生するホストIPアドレスを示します。イベント数が最も多いホストは、対外に向けて、受信しているワーム タイプのトラフィック（調整を必要とする適切な場所を示す）であるか、またはアラートの原因を決定するために更に調査を必要とします。イベント数が最も少ないホストは、対象となる攻撃を受ける可能性があるため、調査の根拠となります。イベント数が少ない場合は、ホストがネットワークに属していないことを示す場合もあります。

ワークフロー名	説明
影響度と優先度	このワークフローにより、すぐに再度発生している影響度の高いイベントを検索します。レポートによる影響レベルは、イベントが発生した時間数で示します。この情報を使用して、最も頻繁に再発する影響度の高いイベントを特定できます。これがネットワーク上での広範な攻撃の指標となります。
影響度と送信元	このワークフローにより、進行中の攻撃の送信元を特定できます。レポートされた影響レベルは、イベントに対する関連の送信元IPアドレスにより示します。たとえば、影響レベルが1のイベントは、同じ送信元IPアドレスから繰返し発生している場合、これらは特定された脆弱なシステムであり、送信元IPアドレスを対象としている攻撃者を示すこともあります。
接続先への影響	このワークフローを使用して、脆弱なコンピュータ上で繰返し発生しているイベントを特定できます。このため、これらのシステムでの脆弱性を指定し、進行中の攻撃を停止できます。
送信元ポート	このワークフローは、最もアラートを発生しているサーバーを示します。この情報を使用して、調整が必要なエリアを特定し、注意を要するサーバを決定できます。
送信元と接続先	このワークフローでは、高いレベルのアラートを共有するホストIPアドレスを特定します。リストのトップのペアは誤検出の可能性もあり、調整が必要なエリアを特定することもあります。評価する必要のないリソースを評価するユーザまたはネットワークに属していないホストについては、対象となる攻撃リストの下部にあるペアを確認できます。

定義済みマルウェアのワークフロー

次の表では、Management Centerに備えられた定義済みマルウェアのワークフローについて説明します。定義済みマルウェアのワークフローでは、必ずマルウェア イベントのテーブルビューを使用します。

表 *66* : 定義済みマルウェアのワークフロー

ワークフロー名	説明
マルウェア サマリ	このワークフローでは、ネットワーク トラフィック内で検出されたか、またはAMP for Endpoints Connectorによって検出されたマルウェアのリストを提供します。これらのリストは、それぞれの脅威ごとにグループ化されます。
マルウェア イベント サマリ	このワークフローでは、異なるマルウェアイベントのタイプやサブタイプの明細が迅速に表示されます。
ホスト受信マルウェア	このワークフローでは、マルウェアを受信したホストIPアドレスのリストが表示されます。このリストは、マルウェア ファイル関連の処理ごとにグループ化されます。
ホスト送信マルウェア	このワークフローでは、マルウェアを送信したホストIPアドレスのリストが表示されます。このリストは、マルウェア ファイル関連の処理ごとにグループ化されます。

ワークフロー名	説明
アプリケーション導入マルウェア	このワークフローでは、ファイルを受信したホストIPアドレスのリストが表示されます。このリストは、受信したファイルの関連したマルウェアの処理によってグループ化されます。

定義済みファイルのワークフロー

次の表では、Management Center に備えられる定義済みファイル イベントのワークフローについて説明しています。定義済みファイル イベントのワークフローでは、必ずファイル イベントのテーブル ビューを使用します。

表 *67*：定義済みファイルのワークフロー

ワークフロー名	説明
ファイルの概要（File Summary）	このワークフローは、さまざまなファイルイベントのカテゴリとタイプ、および関連するすべてのマルウェアの処理について詳細な情報を迅速に提供します。
ファイルを受信したホスト（Hosts Receiving Files）	このワークフローは、ファイルを受信したホスト IP アドレスのリストを、これらのファイルに関連付けられているマルウェアの処理ごとにグループ化して提供します。
ファイルを送信したホスト（Hosts Sending Files）	このワークフローでは、ファイルを送信したホスト IP アドレスのリストを表示します。このリストは、これらのファイルの関連したマルウェアの処理によってグループ化されます。

定義済みキャプチャ ファイルのワークフロー

次の表では、Management Center での定義済みキャプチャ ファイルのワークフローについて説明しています。定義済みキャプチャ ファイルのワークフローは、必ずキャプチャ ファイルのテーブル ビューを使用します。

表 *68*：定義済みキャプチャ ファイルのワークフロー

ワークフロー名	説明
キャプチャ ファイル サマリ	このワークフローでは、タイプ、カテゴリ、脅威スコアに基づいてキャプチャ ファイルの詳細を提示します。
ダイナミック分析ステータス（Dynamic Analysis Status）	このワークフローでは、ダイナミック分析用に提示されたか否かに基づいて、キャプチャ ファイルの数を表示します。

定義済み接続データのワークフロー

次の表では、Management Center に備えられる定義済み接続データのワークフローについて説明しています。定義済み接続データ ワークフローでは、必ず接続データのテーブル ビューを使用します。

表 *69 :* 定義済み接続データのワークフロー

ワークフロー名	説明
接続イベント	このワークフローは、基本的な接続および検出されたアプリケーションの情報についての概要ビューを提供します。ユーザはこれを使用して、イベントのテーブル ビューへドリルダウンすることができます。
接続に基づいたアプリケーション（Connections by Application）	このワークフローには、検出された接続の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のアプリケーションのグラフが含まれています。
接続に基づいた発信側（Connections by Initiator）	このワークフローには、ホストが接続トランザクションを開始した接続の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のホスト IP アドレスのグラフが含まれています。
接続に基づいたポート（Connections by Port）	このワークフローには、検出された接続の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のポートのグラフが含まれています。
接続に基づいた応答側（Connections by Responder）	このワークフローには、ホスト IP が接続トランザクションの応答側であった接続の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のホスト IP アドレスのグラフが含まれています。
一定期間の接続（Connections over Time）	このワークフローには、モニタリング対象のネットワーク セグメントにおける、一定期間の接続の合計数のグラフが含まれています。

ワークフロー名	説明
トラフィックに基づいたアプリケーション（Traffic by Application）	このワークフローには、送信されたキロバイト数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のアプリケーションのグラフが含まれています。 アプリケーション カウントは、アプリケーション接続と照合した各ディテクタが反映されます。トラフィックを照合したアプリケーション プロトコル、Web アプリケーション、クライアント ディテクタ、または内部ディテクタと、トラフィックがモバイル デバイスから発信されたか、または暗号化セッションの一部かによって、同じアプリケーション セッションがリスト内に複数回表示される場合があります。アプリケーションがクライアント フローに表示されていても特定のクライアント ディテクタがない場合は、汎用クライアントが報告される場合があります。 たとえば、同じ YouTube セッションが（YouTube Web アプリケーション ディテクタと照合したため）**YouTube** と（内部 YouTube ディテクタがクライアント セッション内に通常観られる特性と照合したため）**YouTube client** として表示される場合があります。 接続イベント内の情報とネットワークのネットワーク マップを使用して特定のアプリケーション接続の他のコンテキストを特定します。
トラフィックに基づいた発信側（Traffic by Initiator）	このワークフローには、各アドレスから送信されたキロバイト数の合計に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のホスト IP アドレスのグラフが含まれています。
トラフィックに基づいたポート（Traffic by Port）	このワークフローには、送信されたキロバイト数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のポートのグラフが含まれています。
トラフィックに基づいた応答側（Traffic by Responder）	このワークフローには、各アドレスが受信したキロバイト数の合計に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のホスト IP アドレスのグラフが含まれています。
時間の経過ごとのトラフィック	このワークフローには、モニタリング対象のネットワーク セグメントにおける、一定期間に送信されたキロバイト数の合計のグラフが含まれています。
一意の発信側に基づいた応答側（Unique Initiators by Responder）	このワークフローには、各アドレスに接続した一意の発信側の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな応答側の 10 個のホスト IP アドレスのグラフが含まれています。
一意の応答側に基づいた発信側（Unique Responders by Initiator）	このワークフローには、アドレスにコンタクトする一意レスポンダの数に基づく、監視対象のネットワーク セグメントでの 10 個の最もアクティブな開始ホスト IP アドレスのグラフが含まれています。

定義済みセキュリティ インテリジェンスのワークフロー

次の表では、Management Center に備えられている定義済みセキュリティ インテリジェンスのワークフローについて説明しています。定義済みセキュリティ インテリジェンスのワークフローでは、必ずセキュリティ インテリジェンス イベントのテーブル ビューを使用します。

表 *70*：定義済みセキュリティ インテリジェンスのワークフロー

ワークフロー名	説明
セキュリティ インテリジェンス イベント	このワークフローは、基本的なセキュリティ インテリジェンスおよび検出されたアプリケーションの情報についての概要ビューを提供します。ユーザはこれを使用して、イベントのテーブル ビューへドリル ダウンすることができます。
セキュリティ インテリジェンスの概要（Security Intelligence Summary）	このワークフローは、セキュリティ インテリジェンス イベントのワークフローと同じものですが、セキュリティ インテリジェンス サマリ ページから始まり、カテゴリや数ごとにセキュリティ インテリジェンス イベントのみのリストを表示します。
セキュリティ インテリジェンスと DNS 詳細	このワークフローは、セキュリティ インテリジェンス イベントのワークフローと同じものですが、DNS 詳細のあるセキュリティ インテリジェンス ページから始まり、カテゴリや DNS 関連特性ごとにセキュリティ インテリジェンス イベントのリストを表示します。

定義済みホストのワークフロー

次の表では、ホスト データと共に使用できる定義済みワークフローについて説明します。

表 *71*：定義済みホストのワークフロー

ワークフロー名	説明
ホスト（Hosts）	このワークフローには、ホストのテーブル ビューが含まれており、その後にホスト ビューが続きます。ホスト テーブルに基づくワークフロー ビューでは、ホストに関連付けられているすべての IP アドレスのデータを容易に表示できます。
オペレーティング システム サマリ（Operating System Summary）	このワークフローを用いて、ネットワーク上で使用中のオペレーティング システムを分析できます。

定義済み侵害の兆候のワークフロー

次の表では、IOC（侵害の兆候）と共に使用できる定義済みワークフローについて説明します。

表 *72* : 定義済み侵害の兆候のワークフロー

ワークフロー名	説明
ホストの侵害の兆候	このワークフローは、数とカテゴリごとにグループ化した IOC データのサマリー ビューから始まり、さらにサマリ データをイベント タイプごとに分割した詳細ビューを表示します。 [分析（Analysis）]>[ホスト（Hosts）] メニューからこのワークフローにアクセスします。
ホストごとの侵害の兆候	このワークフローを使用して、最も侵害する可能性の高いネットワーク上のホストを判断できます（IOC データに基づく）。 [分析（Analysis）]>[ホスト（Hosts）] メニューからこのワークフローにアクセスします。
ユーザの侵害の兆候	このワークフローは、数とカテゴリごとにグループ化した IOC データのサマリー ビューから始まり、さらにサマリ データをイベント タイプごとに分割した詳細ビューを表示します。 [分析（Analysis）]>[ユーザ（Users）] メニューからこのワークフローにアクセスします。
ユーザごとの侵害の兆候	このワークフローを使用して、侵害に関与している可能性が最も高いネットワーク上のユーザを判断します（IOC データに基づく）。 [分析（Analysis）] > [ユーザー（Users）] メニューからこのワークフローにアクセスします。

定義済みアプリケーション ワークフロー

次の表では、アプリケーションデータと共に使用できる定義済みワークフローについて説明しています。

表 *73* : 定義済みアプリケーション ワークフロー

ワークフロー名	説明
アプリケーションのビジネスとの関連性	このワークフローを使用して、ネットワーク上で実行中のそれぞれ予想されるビジネスとの関連性レベルのアプリケーションを分析できます。そのため、ネットワーク リソースが適切に使用されているかを監視できます。
アプリケーション カテゴリ	このワークフローを使用して、ネットワーク上で各カテゴリの実行中のアプリケーションを分析できます（電子メール、検索エンジン、ソーシャルネットワーキングなど）。そのため、ネットワーク リソースが適切に使用されているかを監視できます。
アプリケーションのリスク	このワークフローを使用して、ネットワーク上でそれぞれ予想されるセキュリティ リスク レベルの実行中のアプリケーションを分析できます。このため、ユーザのアクティビティの考えられるリスクを予想し、適切なアクションを取ることできます。

ワークフロー名	説明
アプリケーション サマリ	このワークフローを使用して、ネットワークのアプリケーションや関連するホストに関する詳細情報を取得できます。このため、ホストのアプリケーションのアクティビティを正確に調べることができます。
アプリケーション	このワークフローを使用して、ネットワーク上の実行中のアプリケーションを分析できます。このため、ネットワークの使用状況の概要を取得できます。

定義済みアプリケーション詳細ワークフロー

次の表では、アプリケーションの詳細とクライアントデータと共に使用できる定義済みワークフローについて説明しています。

表 *74*：定義済みアプリケーション詳細ワークフロー

ワークフロー名	説明
アプリケーションの詳細	このワークフローを用いて、ネットワーク上のクライアントアプリケーションをさらに詳しく分析することができます。また、このワークフローでは、クライアント アプリケーションのテーブル ビューを表示し、その後ホスト ビューを表示します。
Clients	このワークフローには、クライアント アプリケーションのテーブル ビューと、その後にホスト ビューが含まれます。

定義済みサーバーのワークフロー

次の表では、サーバ データと共に使用できる定義済みワークフローについて説明します。

表 *75*：定義済みサーバのワークフロー

ワークフロー名	説明
数別ネットワーク アプリケーション	このワークフローを使用して、ネットワーク上で最も多く使用されるアプリケーションを分析できます。
ヒット別ネットワーク アプリケーション	このワークフローを使用して、ネットワーク上で最もアクティブなアプリケーションを分析できます。
サーバの詳細	このワークフローを使用して、ベンダや検出されたサーバ アプリケーション プロトコルのバージョンを詳細に分析できます。
サーバ	このワークフローには、アプリケーションのテーブル ビューと、その後にホスト ビューが含まれます。

定義済みホスト属性のワークフロー

次の表では、ホスト属性データと共に使用できる定義済みワークフローについて説明します。

表 *76*：定義済みホスト属性のワークフロー

ワークフロー名	説明
属性（Attributes）	このワークフローを使用して、ネットワーク上のホスト IP アドレスやホスト ステータスを監視できます。

定義済み検出イベントのワークフロー

次の表では、検出データとアイデンティティ データの表示に使用できる定義済みワークフローについて説明しています。

表 *77*：定義済み検出イベント ワークフロー

ワークフロー名	説明
検出イベント	このワークフルーでは、テーブル ビュー形式の検出イベント詳細リストが提示され、その次にホスト ビューが提示されます。

定義済みユーザー ワークフロー

次の表では、ユーザ検出データとユーザ アイデンティティ データの表示に使用できる定義済みワークフローを説明します。

表 *78*：定義済みユーザ ワークフロー

ワークフロー名	説明
アクティブ セッション（Active Sessions）	このワークフローでは、ユーザ ID ソースによって収集されるアクティブ セッションが表示されます。
Users	このワークフローでは、ユーザ ID ソースによって収集されるユーザ情報リストが表示されます。

定義済み脆弱性のワークフロー

次の表では、Management Center に備えられている定義済み脆弱性のワークフローについて説明します。

表 *79* : 定義済み脆弱性のワークフロー

ワークフロー名	説明
脆弱性（Vulnerabilities）	このワークフローを使用して、ネットワーク上で検出されたホストに適用するこれらのアクティブな脆弱性のみのテーブルビューなど、データベース内の脆弱性を検討できます。このワークフローにより脆弱性詳細ビューが提供され、これには制約に適合するそれぞれの脆弱性に関する詳細な説明が含まれています。

定義済みのサードパーティ脆弱性のワークフロー

次の表では、Management Centerに備えられた定義済みのサードパーティ脆弱性のワークフローについて説明します。

表 *80* : 定義済みのサードパーティ脆弱性のワークフロー

ワークフロー名	説明
IP アドレスごとの脆弱性	このワークフローを使用して、監視対象のネットワーク上のホスト IP アドレスごとに検出されたサードパーティの脆弱性の数をすぐに確認できます。
送信元ごとの脆弱性	このワークフローを使用して、QualysGuard Scannerなどサードパーティの脆弱性の送信元ごとに検出されたサードパーティの脆弱性の数をすぐに確認できます。

定義済み相関ワークフロー、許可（Allow）リストワークフロー

相関データ、allowリストイベント、allowリスト違反、および修正ステータスイベントの各タイプについて、1 つの事前定義ワークフローが用意されています。

表 *81* : 定義済み相関ワークフロー

ワークフロー名	説明
相関イベント（Correlation Events）	このワークフローには、相関イベントのテーブル ビューが含まれています。
許可（Allow）イベントの一覧表示	このワークフローには、allowリストイベントのテーブルビューが含まれています。
ホスト違反数（Host Violation Count）	このワークフローには、少なくとも 1 つのallowリストに違反しているすべてのホスト IP アドレスのリストを示す一連のページが表示されます。
許可（Allow）違反の一覧表示	このワークフローには、すべての違反を列挙し、リストのトップに直前に検出された違反を示す、allowリスト違反のテーブルビューが含まれています。テーブル内の各列には、検出された違反が 1 つずつ表示されます。

ワークフロー名	説明
ステータス（Status）	このワークフローには、修復ステータスのテーブル ビューを含み、違反したポリシー名、適用された修復名や修復状況が表示されています。

定義済みのシステムのワークフロー

システムには、ルール更新のインポートやアクティブスキャンの結果を表示するワークフロー、およびシステムイベント（監査イベントやヘルスイベント）などのいくつかの追加ワークフローが用意されています。

表 *82 :* 追加の定義済みワークフロー

ワークフロー名	説明
Audit Log（監査ログ）	このワークフローでは、監査イベントをリストした監査ログのテーブル ビューを含みます。
ヘルス イベント（Health Events）	このワークフローでは、ヘルス監視ポリシーによりトリガーされるイベントを表示します。
ルール更新インポート ログ（Rule Update Import Log）	このワークフローは、成功したルールの更新インポートと失敗したルールの更新インポートに関する情報をリストしたテーブル ビューを含みます。
スキャン結果（Scan Results）	このワークフローには、それぞれ完了したスキャンをリストしたテーブル ビューを含みます。

カスタム テーブル ワークフロー

カスタム テーブルの機能を使用して、複数のイベント タイプのデータを使用するテーブルを作成することができます。これにより、たとえば、ユーザが侵入イベントのデータとディスカバリ データを関連付けるテーブルおよびワークフローを作成して、重要なシステムに影響を及ぼすイベントを簡単に検索できるようになるため、役立ちます。

カスタムテーブルを作成すると、システムは自動的にワークフローを作成します。このテーブルを使って関連するイベントを表示することができます。ワークフローの機能は、使用するテーブルのタイプによって異なります。たとえば、侵入イベントテーブルに基づいたカスタム テーブルのワークフローは、必ずパケット ビューで終了します。ただし、検出イベントに基づいたカスタム テーブルのワークフローは、必ずホスト ビューで終了します。

事前定義のイベント テーブルに基づいたワークフローとは異なり、カスタム テーブルに基づいたワークフローには、他のタイプのワークフローへのリンクがありません。

ワークフローの使用

手順

ステップ 1 ワークフローの選択 （811 ページ）に記載されているように、適切なメニューパスとオプションを選択します。

ステップ 2 現在のワークフロー内で移動します。

- 選択したイベント データタイプで利用可能な列をすべて表示するには、テーブル ビュー ページを使用します。テーブル ビュー ページの使用 （819 ページ）を参照してください。
- 選択したイベントデータタイプで利用可能な列のサブセットを表示するには、ドリルダウン ページを使用します。ドリルダウン ページの使用 （818 ページ）を参照してください。
- ワークフローの次のページの対応する行を表示するには、[下矢印（Down-Arrow）]（▼）をクリックします。
- マルチページ ワークフローのページ間を移動するには、各ページの下部にあるツールを使用します。ワークフロー ページのトラバーサル ツール （815 ページ）を参照してください。
- 別のタイプのイベントに対してワークフロー内で適用された同じ制約を表示するには、[移動先（Jump to）] をクリックし、ドロップダウンリストからイベント ビューを選択します。

ステップ 3 現在のワークフローの表示を変更します。

- ページ上で 1 つ以上の行のチェックボックスにマークを付けて、処理を反映させる行を表示し、ページの下部にあるいずれかのボタン（[表示（View）] など）をクリックして、選択したすべての行に対してそのアクションを実行します。
- 行の上部にあるチェックボックスにマークを付けて、ページ上のすべての行を選択し、ページの下部にあるいずれかのボタン（[表示（View）] など）をクリックして、ページ上のすべての行に対してそのアクションを実行します。
- 非表示にする列ヘッダーの [閉じる（Close）]（✕） をクリックして、表示する列を制約します。表示されるポップアップウィンドウで、[適用（Apply）] をクリックします。

  ヒント 他のカラムを表示または非表示にするには、[適用（Apply）] をクリックする前に、該当するチェック ボックスをオンまたはオフにします。無効にした列をビューに戻すには、展開の矢印をクリックして検索の制約を展開し、[無効な列（Disabled Columns）] の下の列名をクリックします。

- 選択したフィールドに対して選択した値でデータ ビューを制約します。詳細については、イベント ビューの制約 （836 ページ）および複合イベント ビューの制約 （838 ページ）を参照してください。

- イベントビューの時間の制約を変更します。ページの右上隅に表示される日付の範囲は、ワークフローに含めるイベントの時間範囲を設定します。詳細については、イベント時間の制約 （829 ページ）を参照してください。

  （注） イベントビューを時間によって制約している場合は、（グローバルかイベントに特有かに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベントビューに表示されることがあります。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

- データを列でソートするには、列の名前をクリックします。ソート順序を反転させるには、もう一度列の名前をクリックします。矢印は、データのソート基準になっている列、およびソートが**昇順**か**降順**かを表します。

- ワークフローページのリンクをクリックして、アクティブな制約を使用しているページを表示します。ワークフロー ページのリンクは、事前定義されたワークフロー テーブル ビュー、およびドリルダウンページの左上隅の、イベントの上で、ワークフロー名の下に示されます。

ステップ 4 現在のワークフロー内の追加データを表示します。

- ファイルのトラジェクトリマップを新しいウィンドウで表示するには、ファイル名と SHA-256 ハッシュ値の列のネットワーク ファイル トラジェクトリ アイコンをクリックします。アイコンは、ファイル ステータスによって異なります。ファイル トラジェクトリ アイコン （816 ページ）を参照してください。

- IP アドレスに関連付けられたホストプロファイルのポップアップウィンドウを表示するには、IP アドレスの列のホストプロファイルアイコンをクリックします。アイコンは、ファイル ステータスによって異なります。ホストプロファイルのアイコン （816ページ）を参照してください。

- ファイルに関連付けられた最も高い脅威スコアの動的分析サマリーレポートを表示するには、いずれかの脅威スコア列の脅威スコアアイコンをクリックします。アイコンは、ファイルの最も高い脅威スコアによって異なります。脅威スコア アイコン （817ページ）を参照してください。

- ユーザープロファイル情報を表示するには、いずれかのユーザー ID 列で [ユーザー（User）] （または、侵害の兆候に関連付けられたユーザーの場合は、[赤色のユーザー（RedUser）]）をクリックします。ユーザー アイコンは、そのユーザーがデータベースにない場合（つまり、AMP for Endpoints Connector ユーザーの場合）は淡色表示されます。

- サードパーティの脆弱性の脆弱性詳細を表示するには、いずれかのサードパーティの脆弱性の ID 列の [脆弱性（Vulnerability）] をクリックします。

- 集約データポイントを表示する場合は、ポインタをフラグの上に合わせて国名を表示します。

- 個々のデータポイントを表示する場合は、フラグをクリックして、位置情報 （821ページ）に記載されている地理位置情報詳細を表示します。

ステップ 5 別のワークフローに移動します。

別のワークフローを使用して同じイベントタイプを表示するには、ワークフローのタイトルの横にある（**ワークフローの切り替え**）をクリックして、使用するワークフローを選択します。スキャン結果には別のワークフローを使用**できない**ことに注意してください。

ユーザー ロールによるワークフローへのアクセス

ワークフローへのアクセスはユーザのロールにより異なります。詳細については、次の表を参照してください。

ユーザ ロール	アクセス可能なワークフロー
管理者（Administrator）	すべてのワークフローにアクセスできます。また、Administrator は監査ログ、スキャン結果、およびルール更新のインポート ログにアクセスできる唯一のユーザです。
メンテナンスユーザ	ヘルス イベントにアクセスできます。
セキュリティアナリストとセキュリティアナリスト（読み取り専用）	侵入、マルウェア、ファイル、接続、検出、脆弱性、相関、ヘルスワークフローにアクセスできます。

ワークフローの選択

システムには、次の表に記載されているデータのタイプに対して、事前定義のワークフローが用意されています。

表 *83 :* ワークフローを使用する機能

機能	メニューパス	オプション
接続イベント	[分析（Analysis）] > [接続（Connections）]	イベント
セキュリティ インテリジェンス イベント	[分析（Analysis）] > [接続（Connections）]	セキュリティ インテリジェンス イベント
相関イベント	[分析（Analysis）] > [相関（Correlation）]	相関イベント 許可（Allow）イベントの一覧表示 許可（Allow） 違反の一覧表示 ステータス

機能	メニューパス	オプション
マルウェア イベント	[分析（Analysis）] > [ファイル（Files）]	マルウェア イベント
ファイル イベント	[分析（Analysis）] > [ファイル（Files）]	ファイル イベント
キャプチャ ファイル	[分析（Analysis）] > [ファイル（Files）]	キャプチャ ファイル
ホスト イベント	[分析（Analysis）] > [ホスト（Hosts）]	ネットワークマップ ホスト 侵害の兆候 アプリケーション アプリケーションの詳細（Application Details） サーバー ホスト属性侵害の兆候 検出イベント
侵入イベント	[分析（Analysis）] > [侵入（Intrusions）]	イベント 確認済みイベント
ユーザ イベント	[分析（Analysis）] > [ユーザ（Users）]	アクティブ セッション（Active Sessions） ユーザー アクティビティ Users 侵害の兆候
脆弱性イベント	[分析（Analysis）] > [ホスト（Hosts）]	脆弱性 サードパーティの脆弱性
スキャン結果	[ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]	—
ヘルス イベント	[システム（System）] > [ヘルス（Health）] > [イベント（Events）]	—
監査イベント	[システム（System）] > [モニタリング（Monitoring）]	監査（Audit）

機能	メニューパス	オプション
ルール更新インポート ログ	[システム（System）] > [更新（Updates）] バージョン 7.2.0 ～ 7.2.5：[システム（System）] > [更新（Updates）] バージョン 7.4.1 以降：[システム（System）] > [コンテンツの更新（Content Updates）]	ルールの更新

上記の表に記載されているいずれかの種類のデータを表示する場合、そのデータのデフォルトのワークフローの最初のページにイベントが表示されます。イベント ビューの設定項目を設定することによって、別のデフォルト ワークフローを指定することができます。ワークフローへのアクセス権限は、ユーザーの役割によって異なります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

関連トピック

イベント ビューの設定 （241 ページ）

ワークフローのページ

ワークフローのタイプによってデータは異なりますが、すべてのワークフローで共通の機能セットを共有しています。ワークフローには、数種類のページを含めることができます。ユーザがワークフローのページ上で実行できるアクションは、ページのタイプによって異なります。

ワークフローのドリル ダウンのページとテーブル ビューのページを使用すれば、データのビューをすばやく絞り込むことができるため、分析にとって重要なイベントに集中できます。テーブル ビューのページとドリルダウンのページの両方で、ユーザが表示するイベント セットに制約を適用したり、ワークフローをナビゲートしたりするために使用できる機能が多数サポートされています。ドリルダウン ページ、またはワークフロー内のテーブル ビューでデータを表示する場合、ソートに使用できる任意のカラムに基づいてデータを昇順または降順でソートできます。1 つのワークフローのページに表示できるイベント数よりも多くのイベントがデータベースに含まれている場合は、ページの下部にあるリンクをクリックして、さらにイベントを表示できます。これらのリンクの1つをクリックすると時間枠が自動的に一時停止されるため、同じイベントが2回表示されません。準備ができたら時間枠の一時停止を解除できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

テーブル ビュー

ページがデフォルトで有効になっている場合、テーブル ビューには、ワークフローのベースとなるデータベースの各フィールドに対するカラムが含まれています。

最適なパフォーマンスを得るには、必要なカラムのみを表示します。表示されるカラムが多いほど、データを表示するために必要なリソースが多くなります。

テーブルビューでカラムを無効にし、そのカラムを無効にすることによって同じ行が複数生成される可能性がある場合に、（[カウント（Count）] カラム以外に）表示されるカラムが 6 つ以下であるときは、システムはイベントビューに [カウント（Count）] カラムを追加します。

テーブル ビュー ページで 1 つの値をクリックすると、その値によって制約することができます。

カスタム ワークフローを作成する場合は、[テーブル ビューの追加（Add Table View）] をクリックしてテーブル ビューを追加します。

ドリルダウン ページ

ドリルダウン ページは、通常テーブル ビューのページに移動する前に調査対象を絞り込むために使用する中間ページです。ドリルダウンページには、データベースで使用できるカラムのサブセットが含まれています。

たとえば、検出イベントのドリルダウン ページには、[IP アドレス（IP Address）]、[MAC アドレス（MAC Address）]、および [時刻（Time）] カラムだけが含まれています。また、侵入イベントのドリルダウン ページには、[優先順位（Priority）]、[影響フラグ（Impact Flag）]、[インラインの結果（Inline Result）]、および [メッセージ（Message）] カラムが含まれています。

ドリルダウンページを使用すれば、表示するイベントの範囲を絞り込んだり、ワークフローで先へ進んだりできます。ドリルダウンページで1つの値をクリックすると（たとえば、その値で制約を加えて、ワークフローの次のページに進んだ場合）、選択した値に一致するイベントをさらに詳しく調べることができます。ドリルダウン ページで値をクリックした場合、次のページがテーブル ビューであっても、値が存在するカラムは無効になりません。事前定義のワークフローのドリルダウン ページには、必ず [カウント（Count）] カラムがあることに注意してください。カスタム ワークフローを作成する場合は、[ページの追加（Add Page）] をクリックしてドリルダウン ページを追加します。

グラフ

接続データに基づくワークフローには、グラフページ（接続グラフとも呼ばれる）を含めることができます。

たとえば接続グラフには、一定期間にシステムで検出された接続の数を示す線グラフを表示することができます。一般的に接続グラフは、ドリルダウンページと同様に、ユーザが調査対象を絞り込むために使用する中間ページです。

最終ページ

ワークフローの最終ページは、ワークフローがベースとするイベントのタイプによって異なります。

- ホストビューとは、アプリケーション、アプリケーションの詳細、検出イベント、ホスト、侵害の兆候（IOC）、サーバー、allowリスト違反、ホスト属性、またはサードパー

ティ製の脆弱性に基づいたワークフローの最終ページです。このページからホスト プロファイルを表示することにより、ユーザーは、複数のアドレスを持つホストに関連付けられているすべての IP アドレス上のデータを簡単に表示することができます。

- ユーザの詳細ビューとは、ユーザ、ユーザアクティビティ、およびユーザの侵害の兆候に基づいたワークフローの最終ページです。
- 脆弱性の詳細ビューとは、Cisco の脆弱性に基づいたワークフローの最終ページです。
- パケット ビューは、侵入イベントに基づいたワークフローの最終ページです。

他の種類のイベント（監査ログイベントやマルウェアイベントなど）に基づいたワークフローには、最終ページがありません。

ワークフローの最終ページで詳細セクションを展開して、ワークフローの進行中に絞り込んだセットの各オブジェクトについて、具体的な情報を表示することができます。Web インターフェイスでは、ワークフローの最終ページに制約が表示されませんが、以前に設定した制約は保持されており、データのセットに適用されます。

ワークフロー ページのナビゲーション ツール

ワークフローのページには、ページ間の移動と、イベントの分析中に表示する情報の選択を容易にする視覚的なキューが用意されています。

ワークフロー ページのトラバーサル ツール

ワークフローに複数のデータ ページが含まれている場合は、各ページの下部にワークフロー内のページ数と、ページ間を移動するために使用できるツールが表示されます。これらのツールを次の表に示します。

表 *84* : ワークフロー ページのトラバーサル ツール

ページのトラバーサル ツール	操作
ページ番号 （別のページを表示するには、表示する番号を入力して Enter キーを押します。）	別のページを表示する
>	次のページを表示する
<	前のページを表示する
>|	最後のページに移動する
|<	最初のページに移動する

ファイル トラジェクトリ アイコン

ワークフロー ページで、新しいウィンドウにファイルのトラジェクトリ マップを表示する機会があるときは、ネットワーク トラジェクトリ アイコンが表示されます。このアイコンは、ファイルのステータスによって変わります。

表 *85 :* ファイル トラジェクトリ アイコン

ファイル トラジェクトリ アイコン	ファイル ステータス
正常（Clean）	クリーン
マルウェア	マルウェア
カスタム検出	カスタム検出
不明	不明
使用不可	使用不可

ホスト プロファイルのアイコン

ワークフロー ページでは、IP アドレスに関連付けられたホスト プロファイルをポップアップ ウィンドウで表示でき、ホスト プロファイル アイコンが表示されます。ホスト プロファイルのアイコンがグレー表示になっている場合は、ネットワーク マップ内にそのホストが存在できないため、ホスト プロファイルを表示できません（0.0.0.0 など）。このアイコンは、ホストのステータスによって異なって表示されます。

表 *86 :* ホスト プロファイルのアイコン

ホスト プロファイルのアイコン	ホスト ステータス
	ホストは潜在的に危険にさらされているとタグ付けされていません。
	ホストは、トリガーされた侵害の兆候（IOC）ルールによって潜在的に危険にさらされているとタグ付けされています。
	ブロックリストに追加（セキュリティ インテリジェンス データに基づいて、トラフィック フィルタリングを実行している場合にのみ表示されます）。
	モニターするように設定されたブロックリストに追加（セキュリティ インテリジェンス データに基づいて、トラフィック フィルタリングを実行している場合にのみ表示されます）。

脅威スコア アイコン

ワークフローページで、ファイルに関連付けられているスコアが最も高い脅威に関する動的分析サマリ レポートを表示すると、脅威スコア アイコンが表示されます。このアイコンは、ファイルの最も高い脅威スコアに応じて異なります。

表 *87*：脅威スコア アイコン

脅威スコア アイコン	脅威スコア レベル
低	低（Low）
中規模	中規模
高（High）	大きい
非常に高い	非常に高い（Very high）

ユーザー アイコン

ワークフロー ページで、ユーザ名に関連付けられているユーザ ID がポップアップ ウィンドウで表示されると、同時にユーザ アイコンも表示されます。

表 *88*：ユーザ アイコン

ユーザ アイコン	ユーザー ステータス
ユーザー（User）	ユーザは侵害の兆候に関連付けられていません。
赤色のユーザー	ユーザは 1 つ以上の侵害の兆候に関連付けられています。

ワークフロー ツールバー

ワークフローの各ページには、関連する機能へすばやくアクセスするためのツールバーがあります。次の表で、ツールバー上の各リンクについて説明します。

表 *89*：ワークフロー ツールバーのリンク

機能	説明
このページをブックマークする（Bookmark This Page）	後でそのページに戻れるように、現在のページをブックマークします。ブックマークすると、表示中のページに適用されている制約が取得され、データがまだ存在している場合は後で同じデータに戻ることができます。
レポート作成者	現在制約されているワークフローを選択基準として使用して、レポート デザイナを開きます。

機能	説明
ダッシュボード	現行のワークフローに関連するダッシュボードを開きます。たとえば、[接続イベント（Connection Events）] ワークフローは [接続サマリ（Connection Summary）] ダッシュボードと関連付けられています。
ブックマークの表示	ユーザが選択できる、保存したブックマークのリストを表示します。
検索（Search）	[検索（Search）] ページが表示され、ここでワークフローのデータについて高度な検索を実行することができます。下向きの矢印アイコンをクリックし、保存済みの検索を選択して使用することもできます。

関連トピック

イベント ビューからのレポート テンプレートの作成 （647 ページ）
ダッシュボードについて （403 ページ）
イベントの検索 （845 ページ）
ブックマーク （841 ページ）
ブックマークの作成 （842 ページ）
ブックマークの表示 （842 ページ）

ドリルダウン ページの使用

手順

ステップ 1 「ワークフローを使用する機能」の説明に従って、適切なメニューパスとオプションを選択してワークフローにアクセスします。

ステップ 2 すべてのワークフローで、次のオプションを選択できます。

- 特定の値に制限して、次のワークフロー ページにドリルダウンするには、行内の値をクリックします。この処理はドリルダウンページでのみ可能でることに注意してください。テーブルの行内の値をクリックしても、テーブル ビューが制約されるだけで、次のページにはドリル ダウンしません。
- いくつかのイベントによって制約したまま次のワークフロー ページにドリルダウンするには、次のワークフロー ページに表示させるイベントの横のチェック ボックスを選択し、[表示（View）] をクリックします。
- 現在の制限を維持して次のワークフロー ページにドリルダウンするには、[すべて表示（View All）] をクリックします。

ヒント テーブル ビューでは、必ずページ名に「Table View」が含まれます。

テーブル ビュー ページの使用

テーブル ビュー ページには、ドリルダウン、ホスト ビュー、パケット ビュー、脆弱性の詳細ページでは利用できない機能が用意されています。これらの機能は次のように使用します。

手順

ステップ 1 ワークフローの選択 （811 ページ）の説明に従って、適切なメニュー パスとオプションを選択してワークフローにアクセスします。

ステップ 2 ワークフローの名前の下に表示されるワークフロー パスからテーブル ビューを選択します。

ステップ 3 イベントデータがリモートに保存されている場合、ローカルデータとリモートデータのどちらを表示するかを選択するオプションが表示されることがあります。

「Secure Network Analytics アプライアンスに保存されている接続イベントを使用した Secure Firewall Management Center での作業 （819 ページ）」を参照してください。

ステップ 4 必要に応じて、次に示す機能を使用してテーブル ビュー内に配置したり、移動したりします。

- 無効なカラムのリストを表示するには、[検索制約（Search Constraints）] の **[展開矢印（Expand Arrow）]**（ ） をクリックします。
- 無効なカラムのリストを非表示するには、[検索制約（Search Constraints）] の **[折りたたみ矢印（Collapse Arrow）]**（ ） をクリックします。
- 無効になったカラムをイベントビューに戻すには、[検索の制約（Search Constraints）] の **[展開矢印（Expand Arrow）]**（ ） をクリックして検索の制約を展開し、[無効になったカラム（Disabled Columns）] の下にあるカラム名をクリックします。
- カラムを表示または非表示（無効）にするには、各カラム名の横にある [クリア（Clear）]（ ）をクリックします。表示されるポップアップウィンドウで、該当するチェックボックスをオンまたはオフにして、どのカラムを表示するかを指定し、[適用（Apply）] をクリックします。

Secure Network Analytics アプライアンスに保存されている接続イベントを使用した Secure Firewall Management Center での作業

デバイスがセキュリティ分析とロギング（オンプレミス）を使用して Secure Network Analytics アプライアンスに接続イベントを送信している場合、Management Center のイベントビューアとコンテキストエクスプローラでリモートに保存されたイベントを表示および操作し、レポートの生成時にそれらのイベントを含めることができます。Management Center のイベントから相互起動して、Secure Network Analytics アプライアンスの関連データを表示することもできます。

デフォルトでは、指定した時間範囲に基づいて適切なデータソースが自動的に選択されます。データソースをオーバーライドする場合は、次の手順を使用します。

重要 データソースを変更すると、選択した内容は、サインアウト後でも、変更するまでは、イベントデータソース（レポートを含む）に依存するすべての関連する分析機能で維持されます。選択した内容は他の Management Center ユーザーには適用されません。

選択したデータソースは、優先順位の低い接続イベントにのみ使用されます。他のすべてのイベントタイプ（侵入、ファイル、マルウェアイベント、それらのイベントに関連付けられた接続イベント、およびセキュリティ インテリジェンス イベント）は、データソースに関係なく表示されます。

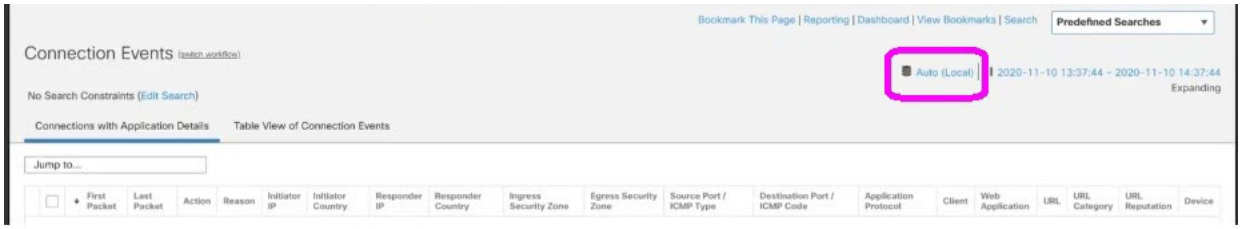
始める前に

ウィザードを使用して接続イベントを セキュリティ分析とロギング（オンプレミス） に送信しました。

手順

ステップ 1 Management Center Web インターフェイスで、接続イベントデータを表示するページ（[Analysis] > [Connections] > [Events] など）に移動します。

ステップ 2 ページに表示されるデータソースをクリックし、オプションを選択します。



注意 [Local] を選択すると、ローカルデータが選択した時間範囲全体で使用できない場合でも、Management Center で使用可能なデータのみ表示されます。この状況が発生していることは通知されません。

ステップ 3 （任意）Secure Network Analytics アプライアンスで関連データを直接表示するには、IP アドレスやドメインなどの値を右クリック（統合イベントビューアでクリック）し、相互起動オプションを選択します。

位置情報

地理位置情報データベース（GeoDB）を利用することで、国と大陸に基づいてトラフィックを表示およびフィルタ処理できます。国間を移動するモバイルデバイスやその他のホストが検出された場合、システムは特定の国ではなく大陸名を報告する可能性があります。

システムにはIPアドレスを国/大陸にマップする初期GeoDBカントリーコードパッケージが付属しているため、情報を常に利用できます。システムはコンテキストデータを含むIPパッケージもダウンロードします。たとえば次の設定が含まれます。

- 地域（州、県、またはその他の国の小地域）、都市、郵便番号。
- 緯度/経度、タイムゾーン、クリック可能なマップ。
- 自律システム番号（ASN）およびその ASN に関する追加情報。
- インターネット サービス プロバイダー（ISP）、接続の種類、プロキシの種類。
- 自宅/会社、組織、ドメイン名の情報。

この情報を表示するには、イベント、アセットプロファイル、コンテキストエクスプローラ、ダッシュボード、およびその他の分析ツールなどに表示される小さな国旗アイコンと ISO 国コードをクリックします。[接続のサマリ（Connection Summary）] ダッシュボードなど、集約的な地理位置情報から詳細の地理位置情報を表示することはできません。

シスコでは、GeoDBの定期的な更新を提供しています。正確な地理位置情報を取得するには、GeoDBを定期的に更新する必要があります。地理位置情報データベース（GeoDB）の更新（269ページ） を参照してください。

関連トピック

ネットワーク条件
位置情報
相関ポリシーとルールの概要 （1189 ページ）
トラフィック プロファイル条件 （1237 ページ）
地理位置情報データベース（GeoDB）の更新 （269 ページ）

接続イベント グラフ

システムは、テーブル形式のドリル ダウン ページを使ったワークフローや最終的なイベントのテーブル表示に加えて、5 分間隔で集計されたデータを使用して、特定の接続データをグラフィック表示することができます。グラフ表示できるのは、データを集約するのに使用する情報（送信元と宛先の IP アドレス（およびこれらのホストに関連するユーザ）、宛先ポート、トランスポート プロトコルとアプリケーション プロトコル）のみです。

ヒント セキュリティ インテリジェンス イベントを関連する接続イベントとは別にグラフ表示することはできません。セキュリティ インテリジェンスのフィルタリング アクティビティの概要をグラフィック表示するには、ダッシュボードとコンテキスト エクスプローラを使用します。

接続グラフは 3 種類あります。

- 円グラフは、1 つのデータセットのデータをカテゴリ分けして表示します。
- 棒グラフは、1 つあるいは複数のデータセットのデータをカテゴリ分けして表示します。
- 折れ線グラフは、時間の経過に伴って 1 つあるいは複数のデータセットのデータをプロットします。標準ビューあるいは速度（変化のペース）ビューを使用します。

（注） システムは、トラフィック プロファイルを線グラフで表示します。他の接続グラフと同様に操作可能ですが、いくつか規制があります。トラフィック プロファイルを表示するには、管理者アクセス権が必須です。

ワークフロー テーブルと同様に、ワークフロー グラフもドリル ダウンし、制約を加えることで分析の的を絞ることができます。

棒グラフおよび折れ線グラフはどちらも複数のデータセットを表示できます。つまり、各 X 軸データ ポイントに対し、Y 軸に複数の値を表示できます。たとえば、一意のイニシエータとレスポンダの総数を表示することができます。円グラフでは、1 つのデータセットのみ表示できます。

X 軸または Y 軸、もしくは両方を変更することによって、接続グラフにさまざまなデータやデータセットを表示できます。円グラフでは、X 軸を変更すると独立変数が変わり、Y 軸を変更すると従属変数が変わります。

関連トピック

接続の概要（グラフ用集約データ） （900 ページ）

接続イベント グラフの使用方法

Management Center では、検索する情報に応じて、接続イベント グラフを表示したり操作したりできます。

接続グラフにアクセスしたときに表示されるページは、使用するワークフローによって異なります。接続イベントのテーブル ビューで終了する、事前定義されたワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[分析（Analysis）]** > **[接続（Connections）]** > **[イベント（Events）]**を選択します。

（注） 接続イベントテーブルがグラフの代わりに表示される場合、または別のグラフを表示する場合は、ワークフロー タイトルの横にある（**ワークフローの切り替え**）をクリックし、グラフが含まれる事前定義されたワークフローまたはカスタム ワークフローを選択します。接続グラフを含むすべての事前定義された接続イベント ワークフローは、接続のテーブル ビューで終了します。

ステップ 2 次の選択肢があります。

- [時間範囲（Time Range）]：時間範囲を調整する場合は（グラフがブランクの場合に役立ちます）、時間枠の変更 （833 ページ）を参照してください。
- [フィールド名（Field Name）]：ユーザが図示可能なデータの詳細については、接続およびセキュリティ関連の接続イベントフィールド （902 ページ）を参照してください。
- [ホスト プロファイル（Host Profiles）]：IP アドレスのホスト プロファイルを表示するには、発信側または応答側による接続データが表示されているグラフで、棒グラフの棒または円グラフの扇形をクリックし、[ホスト プロファイルの表示（View Host Profile）] を選択します。
- [ユーザ プロファイル（User Profile）]：ユーザ プロファイル情報を表示するには、発信側ユーザによる接続データが表示されているグラフで、棒グラフの棒または円グラフの扇形をクリックし、[ユーザ プロファイルの表示（View User Profile）] を選択します。
- [その他の情報（Other Information）]：図示されたデータに関する詳細については、折れ線グラフの点、棒グラフの棒、または円グラフの扇形の上にカーソルを置きます。
- [固定（Constrain）]：ワークフローを次のページに進めずに接続グラフを X 軸（独立した変数）基準で固定するには、折れ線グラフの点、棒グラフの棒、または円グラフの扇形をクリックし、[表示方法（View by）] を選択します。オプションが表示されます。
- [データ選択（Data Selection）]：グラフに表示されるデータを変更するには、[X 軸（X-Axis）] または [Y 軸（Y-Axis）] をクリックし、図示する新しいデータを選択します。X 軸を [時間（Time）] に変更、または [時間（Time）] から変更すると、グラフ タイプも変更されます。Y 軸を変更すると、表示されるデータセットに影響します。
- [データセット（Datasets）]：グラフのデータセットを変更するには、[データセット（Datasets）] をクリックし、新しいデータセットを選択します。
- [切り離し（Detach）]：デフォルトの時間範囲に影響を与えることなくさらに分析を実行できるように接続グラフを分離するには、[切り離し（Detach）] をクリックします。

  ヒント コピーを作成するには、分離したグラフで [新規ウィンドウ] をクリックします。分離した各グラフ上で、別々の分析ができるようになります。トラフィック プロファイルは、分離したグラフです。

- [詳細（Drill-Down）]：ワークフローで次のページにドリルダウンするには、折れ線グラフの点、棒グラフの線、または円グラフの扇形をクリックし、[詳細（Drill-Down）] を選択します。折れ線グラフで点をクリックすると、次のページの時間枠は、クリックした点を中心とする 10 分間に変更されます。棒グラフの棒または円グラフの扇形をクリックすると、その棒または扇形が表す基準に基づいて次のページが制約されます。

- [エクスポート（Export）]：グラフの接続データを CSV（カンマ区切り値）ファイルとしてエクスポートするには、[データのエクスポート（Export Data）] を選択します。次に、[CSV ファイルのダウンロード（Download CSV File）] をクリックし、ファイルを保存します。
- [グラフ タイプ（Graph Type）]：[折れ線（Line）]- 標準と速度（変化のペース）の折れ線グラフを切り替えるには、[速度（Velocity）] をクリックし、[標準（Standard）] または [速度（Velocity）] を選択します。
- [グラフ タイプ（Graph Type）]：[棒と円（Bar and Pie）] - 棒グラフと円グラフを切り替えるには、[棒グラフに切り替え（Switch to Bar）] または [円グラフに切り替え（Switch to Pie）] をクリックします。円グラフには複数のデータセットを表示できないため、複数のデータセットを持つ棒グラフから円グラフに切り替えた場合、円グラフは自動的に選択された 1 つのデータセットだけを表示します。表示するデータセットを選択する際、Management Center は、発信側と応答側の統計情報よりも全体の統計情報を優先し、応答側の統計情報よりも発信側の統計情報を優先します。
- [ページ間の移動（Navigate Between Pages）]：現在のワークフローで現在の制約を保持したままページ間を移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。
- イベント ビュー間で移動する：関連するイベントを表示するためその他のイベント ビューに移動するには、[ジャンプ（Jump to）] をクリックし、ドロップダウン リストからイベント ビューを選択します。
- [再センタリング（Recenter）]：時間範囲の長さを変更せずにある時点を中心に折れ線グラフを再センタリングするには、その点をクリックし、[再センタリング（Recenter）] を選択します。
- [ズーム（Zoom）]：ズームインまたはズームアウトしながらある時点を中心に折れ線グラフを再センタリングするには、その点をクリックし、[ズーム（Zoom）] を選択してから新しい時間枠を選択します。

（注） 分離したグラフを使用している場合を除いて、制約、再センタリング、およびズームすると Management Center のデフォルトの時間範囲が変わります。

例

例：接続グラフの制約

ある期間の接続のグラフについて考えてみましょう。グラフ上の点をポートによって制約すると、検出された接続イベント数に基づいて、最もアクティブだった 10 のポートを示す棒グラフが表示されますが、クリックした点を中心とする 10 分間の時間枠によって制約されます。

棒の 1 つをクリックし、[発信側 IP による表示（View by Initiator IP）] を選択してグラフをさらに制約すると、それまでと同じ 10 分間の時間枠だけでなく、クリックした棒が表すポートでも制約された新しい棒グラフが表示されます。

例：円グラフの X 軸と Y 軸の変更

ポートごとのキロバイト数を表示する円グラフについて考えてみましょう。この場合、X 軸は **レスポンダ ポート**、Y 軸は **キロバイト** です。この円グラフは、ある間隔に監視対象ネットワークで送信されたデータの合計キロバイト数を表します。円の中の扇形は、各ポートで検出されたデータの比率を表します。

- グラフの X 軸を **アプリケーション プロトコル** に変更すると、引き続き円グラフは送信データの合計キロバイト数を表しますが、円の中の扇形は検出された各アプリケーション プロトコルの送信データの比率を表します。
- グラフの Y 軸を **パケット** に変更すると、円グラフはある間隔に監視対象ネットワークで送信された合計パケット数を表し、円の中の扇形は各ポートで検出された合計パケット数の割合を表します。

関連トピック

ワークフローの使用 （809 ページ）
イベント ビューの設定 （241 ページ）

接続グラフ データ オプション

X軸またはY軸、もしくは両方を変更することによって、接続グラフにさまざまなデータを表示できます。円グラフでは、X軸を変更すると独立変数が変わり、Y軸を変更すると従属変数を変わります。

表 *90 : X* 軸オプション

X 軸オプション	グラフの種類	次の基準でこのデータをグラフ化する
アプリケーション プロトコル（Application Protocol）	棒グラフまたは円グラフ	最もアクティブな 10 個のアプリケーション プロトコルに基づいて
Device	棒グラフまたは円グラフ	最もアクティブな 10 台の管理対象デバイスに基づいて
イニシエータ IP（Initiator IP）	棒グラフまたは円グラフ	最もアクティブな 10 個のイニシエータ ホスト IP アドレスに基づいて

X 軸オプション	グラフの種類	次の基準でこのデータをグラフ化する
イニシエータ ユーザ（Initiator User）	棒グラフまたは円グラフ	最もアクティブな 10 名のイニシエータ ユーザに基づいて
レスポンダ IP（Responder IP）	棒グラフまたは円グラフ	最もアクティブな 10 個のレスポンダ ホスト IP アドレスに基づいて
レスポンダ ポート（Responder Port）	棒グラフまたは円グラフ	最もアクティブな 10 個のレスポンダ ポートに基づいて
送信元デバイス（Source Device）	棒グラフまたは円グラフ	最もアクティブな 10 個の NetFlow データ エクスポータと、Firepower システムの管理対象デバイスによって検出されたすべての接続の `Firepower` という名前の送信元デバイスに基づいて。
時刻（Time）	ライン	時系列 Y 軸と [時刻（Time）] を切り替えることでグラフの種類も変わり、データセットを変更できます。

表 *91 : Y* 軸オプション

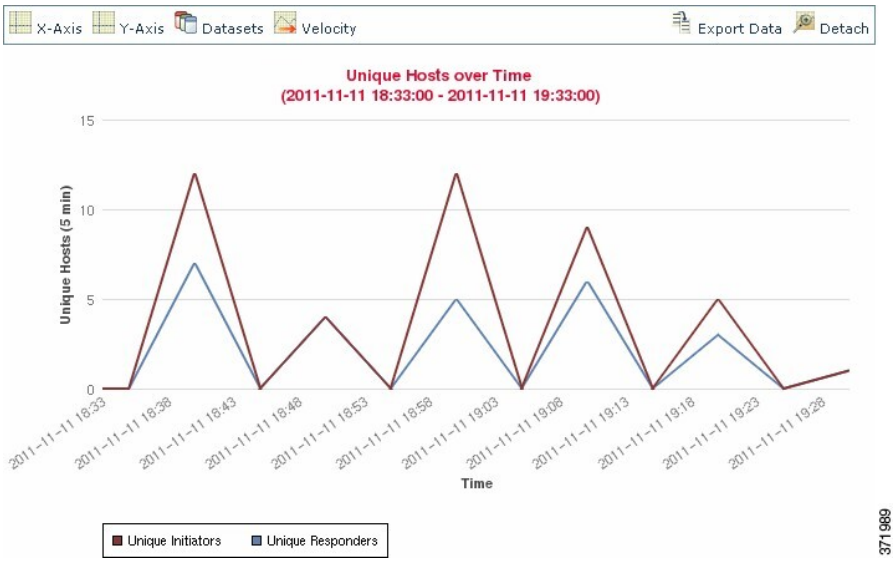
Y 軸オプション	X 軸の基準を使用してこのデータをグラフ化する
バイト（Bytes）	送信バイト数
接続（Connections）	接続数
KB（KBytes）	送信キロバイト数
KB/秒（KBytes Per Second）	KB/秒
パケット（Packets）	送信パケット数
固有のホスト（Unique Hosts）	検出された固有のホスト数
固有のアプリケーション プロトコル（Unique Application Protocols）	固有のアプリケーション プロトコル数
固有ユーザ（Unique Users）	固有ユーザー数

複数のデータセットの接続グラフ

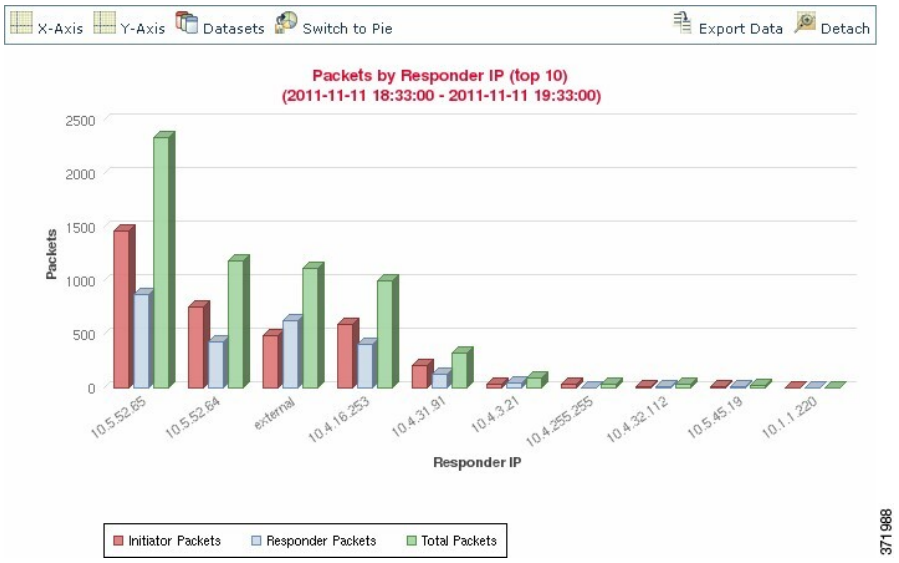
棒グラフおよび折れ線グラフはどちらも複数のデータセットを表示できます。つまり、各X軸データ ポイントに対し、Y軸に複数の値を表示できます。たとえば、一意のイニシエータとレスポンダの総数を表示することができます。

（注） 円グラフには複数のデータセットを表示**できません**。複数のデータセットを持つ棒グラフから円グラフに切り替えた場合、円グラフは自動的に選択された1つのデータセットだけを表示します。表示するデータセットを選択する際、Management Center は、イニシエータとレスポンダの統計情報よりも全体の統計情報を優先し、イニシエータの統計情報よりもレスポンダの統計情報を優先します。

折れ線グラフでは、複数のデータセットは複数の線として、それぞれ異なる色で表示されます。たとえば、次のグラフは、モニター対象ネットワークにおいて1時間間隔の1回で検出された一意のイニシエータの合計数と一意のレスポンダの合計数を表示しています。



棒グラフでは、複数のデータセットがX軸データ ポイントごとに色分けされた棒として表示されます。たとえば次の棒グラフは、監視対象ネットワーク上で送信されたパケットの合計数と、イニシエータによって送信されたパケット数、レスポンダによって送信されたパケット数を表示しています。



接続グラフ データセット オプション

次の表では、接続グラフの x 軸に表示できるデータセットについて説明します。

表 *92 :* データセット オプション

y 軸が表示されている場合は、	**データベースとして選択できます。**
接続（Connections）	デフォルトのみです。監視対象のネットワークで検出された接続数（[接続（Connections）]）です。これは、トラフィック プロファイル グラフ用の唯一のオプションです。
KB（KBytes）	以下を組み合わせています。 • モニター対象ネットワーク上で送信された合計キロバイト数（[合計キロバイト数（Total KBytes）]） • モニター対象ネットワーク上でホスト IP アドレスから送信されたキロバイト数（[イニシエータ キロバイト数（Initiator KBytes）]） • モニター対象ネットワーク上でホスト IP アドレスによって受信されたキロバイト数（[レスポンダ キロバイト数（Responder KBytes）]）
KB/秒（KBytes Per Second）	デフォルトの、モニター対象ネットワークで 1 秒あたりに送信された合計キロバイト数のみ（[1 秒あたりの合計キロバイト数（Total KBytes Per Second）]）

y 軸が表示されている場合は、	データベースとして選択できます。
パケット（Packets）	以下を組み合わせています。 • モニター対象ネットワーク上で送信された合計パケット数（[合計パケット（Total Packets）]） • モニター対象ネットワーク上でホスト IP アドレスから送信されたパケット数（[イニシエータ パケット（Initiator Packets）]） • モニター対象ネットワーク上でホスト IP アドレスによって受信されたパケット数（[レスポンダ パケット（Responder Packets）]）
固有のホスト（Unique Hosts）	以下を組み合わせています。 • モニター対象ネットワーク上の一意のセッション開始側の数（[一意のイニシエータ（Unique Initiators）]） • モニター対象ネットワーク上の一意のセッション応答側の数（[一意のレスポンダ（Unique Responders）]）
固有のアプリケーションプロトコル（Unique Application Protocols）	デフォルトの、モニター対象ネットワーク上の一意のアプリケーションプロトコル数のみ（[一意のアプリケーションプロトコル（Unique Application Protocols）]）
固有ユーザー（Unique Users）	デフォルトのみです。監視対象のネットワークでのセッション イニシエータにログインした固有ユーザー数（[固有イニシエータ ユーザー（Unique Initiator Users）]）です。

イベント時間の制約

各イベントには、そのイベントがいつ発生したかを示すタイム スタンプがあります。時間枠（時間範囲とも呼ばれる）を設定することによって、いくつかのワークフローに表示される情報を制約することができます。

時間によって制約できるイベントに基づいたワークフローには、ページの上部に時間範囲を表す行が含まれています。

デフォルトでは、ワークフローは、1 時間前が開始時間として設定された時間枠を使用します。たとえば、午前 11:30 にログインした場合、午前 10:30～11:30 の間に発生したイベントが表示されます。時間が経過するにしたがって、時間枠が拡張されます。午後 12:30 には、午前 10:30～午後 12:30 の間に発生したイベントが表示されます。

イベント ビューの設定で独自のデフォルト時間枠を設定することによって、この動作を変更することができます。これにより、次の 3 つのプロパティが影響を受けます。

- 時間枠のタイプ（静的、拡張、またはスライディング）
- 時間枠の長さ

- 時間枠の数（複数の時間枠、または単一のグローバル時間枠）

ページの上部にある時間範囲をクリックして [日時（Date/Time）] ポップアップ ウィンドウを表示し、デフォルトの時間枠の設定に関係なく、イベントの分析中に時間枠を手動で変更することができます。設定した時間枠の数、および使用しているアプライアンスのタイプに応じて [日時（Date/Time）] ウィンドウを使用して、表示しているイベントのタイプに対するデフォルトの時間枠を変更することもできます。

最後に、時間枠を一時停止すると同時にスライディングまたは拡張ワークフローを検討します。データセットを一時的に凍結するための時間枠の一時停止（833ページ）を参照してください。

関連トピック

イベント ビューの設定（241 ページ）
接続およびセキュリティ関連の接続イベントテーブルの使用（934 ページ）

イベントのセッションごとの時間枠のカスタマイズ

デフォルトの時間枠（タイム ウィンドウ）に関係なく、イベントの分析中に時間枠を手動で変更することができます。

（注） 手動による時間枠の設定は、現在のセッションについてのみ有効です。いったんログアウトしてからもう一度ログインすると、時間枠はデフォルトにリセットされます。

ユーザが設定した時間枠の数によっては、1 つのワークフローの時間枠の変更が、アプライアンス上の他のワークフローに影響を与えることがあります。たとえば、単一のグローバル時間枠がある場合、1 つのワークフローの時間枠を変更すると、アプライアンス上の他のすべてのワークフローの時間枠が変更されます。一方、複数の時間枠を使用している場合は、監査ログまたはヘルスイベントのワークフローの時間枠を変更しても、他の時間枠には影響を与えませんが、他の種類のイベントの時間枠を変更すると、時間で制約できるすべてのイベント（監査イベントとヘルス イベントは除く）が影響を受けます。

すべてのワークフローを時間によって制約できるわけではないため、時間枠の設定は、ホスト、ホスト属性、アプリケーション、アプリケーションの詳細、脆弱性、ユーザー、またはallowリスト違反に基づいたワークフローには影響を与えないことに注意してください。

[日付/時刻（Date/Time）] ウィンドウの [時間枠（Time Window）] タブを使用して、時間枠を手動で設定します。デフォルトの時間枠設定で設定した時間枠の数によって、タブのタイトルは以下のいずれかになります。

- [イベントの時間枠（Events Time Window）]：複数の時間枠を設定し、監査ログまたはヘルス イベントのワークフロー以外のワークフローに対して時間枠を設定している場合
- [ヘルス モニタリング タイム ウィンドウ（Health Monitoring Time Window）]：複数の時間枠を設定し、ヘルス イベント ワークフローに対して時間枠を設定している場合
- [監査ログ タイム ウィンドウ（Audit Log Time Window）]：複数の時間枠を設定し、監査ログに対して時間枠を設定している場合

- [グローバル タイム ウィンドウ（Global Time Window）]：単一の時間枠を設定している場合

時間枠を設定する場合には、最初に、使用する時間枠のタイプを決定する必要があります。

- 静的な時間枠は、特定の開始時間から特定の終了時間の間に生成されたすべてのイベントを表示します。
- 拡張時間枠は、特定の開始時間から現在までの間に生成されたすべてのイベントを表示します。時間の経過とともに時間枠が拡張され、イベント ビューに新しいイベントが追加されます。
- [スライディング（sliding）] 時間枠には、特定の開始時間（1 週間前など）から現在までの間に生成されたすべてのイベントが表示されます。ページを更新すると、時間枠が「スライド」するため設定した時間範囲（この例では過去 1 週間）のイベントのみが表示されます。データ セットを調べている間に一時的に更新されないようにするには、データセットを一時的に凍結するための時間枠の一時停止 （833 ページ）を参照してください。

選択したタイプによって、[日付/時刻（Date/Time）] ウィンドウが変化し、さまざまな設定オプションが提供されます。

（注） システムでは、タイムゾーンの設定に指定された時間に基づいて、24 時間の時計を使用します。

時間枠の設定

次の表で、[時間枠（Time Window）] タブで設定できるさまざまな項目について説明します。

表 *93*：時間枠の設定

設定	時間枠（タイム ウィンドウ）のタイプ	説明
[時間枠タイプ（time window type）] ドロップダウン リスト	適用対象外	使用する時間枠のタイプとして、[静的（static）]、[拡張（expanding）]、または [スライディング（sliding）] のいずれかを選択します。 イベント ビューを時間で制約している場合は、（グローバルであるかイベントに特有であるかに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあることに注意してください。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

設定	時間枠（タイム ウィンドウ）のタイプ	説明
[開始時間（Start Time）] カレンダー	静的および拡張	時間枠の開始日と時間を指定します。すべての時間枠の最大時間範囲は、1970 年 1 月 1 日午前 0 時（UTC）～ 2038 年 1 月 19 日午前 3 時 14 分 7 秒です。 カレンダーを使用する代わりに、下記で説明するプリセット オプションを使用できます。
[終了時間（End Time）] カレンダー	静的	時間枠の終了日付と時間を指定します。すべての時間枠の最大時間範囲は、1970 年 1 月 1 日午前 0 時（UTC）～ 2038 年 1 月 19 日午前 3 時 14 分 7 秒です。 拡張時間枠を使用している場合は、[終了時刻（End Time）] カレンダーがグレー表示になり、終了時刻が「現在の時刻（Now）」と示されることに注意してください。 カレンダーを使用する代わりに、下記で説明するプリセット オプションを使用することもできます。
[最後を表示（Show the Last）] フィールドおよびドロップダウン リスト	スライディング	スライディング時間枠の長さを設定します。
[プリセット（Presets）]：[最終（Last）]	すべて	リスト内のいずれかの時間範囲をクリックし、アプライアンスのローカル時刻に基づいて時間枠を変更します。たとえば、[1 週間（1 week）] をクリックすると、最後の 1 週間を反映するように時間枠が変わります。プリセットをクリックすると、選択したプリセットを反映するようにカレンダーが変わります。
[プリセット（Presets）]：[現在（Current）]	静的および拡張	リスト内のいずれかの時間範囲をクリックし、アプライアンスのローカル時間と日付に基づいて時間枠を変更します。プリセットをクリックすると、選択したプリセットを反映するようにカレンダーが変わります。 次の点に注意してください。 • 現在日付は午前 0 時から始まる • 現在の週は日曜日の午前 0 時から始まる • 現在の月は、月の最初の日の午前 0 時から始まる

設定	時間枠（タイム ウィンドウ）のタイプ	説明
[プリセット（Presets）]：[同期（Synchronize with）]	すべて（グローバルな時間枠を使用している場合は使用不可）	以下のいずれかをクリックします • [イベント タイム ウィンドウ（Events Time Window）]：現在の時間枠とイベントの時間枠を同期する場合 • [ヘルス モニタリング タイム ウィンドウ（Health Monitoring Time Window）]：現在の時間枠とヘルス モニタリングの時間枠を同期する場合 • [監査ログの時間枠（Audit Log Time Window）]：現在の時間枠と監査ログの時間枠を同期する場合

時間枠の変更

手順

ステップ 1 時間により制約されたワークフローで、[時間範囲（Time Range）]（  ）をクリックし、[日付と時間（Date/Time）] ウィンドウを開きます。

ステップ 2 [イベントの時間枠（Events Time Window）] で、時間枠の設定 （831 ページ）に記載されているように時間枠を設定します。

ヒント 時間枠をデフォルトの設定に戻すには、[リセット（Reset）] をクリックします。

ステップ 3 [Apply] をクリックします。

データ セットを一時的に凍結するための時間枠の一時停止

スライディングまたは拡張時間枠を使用している場合、時間枠を一時停止してワークフローが提供するデータのスナップショットを調べることができます。一時停止されないワークフローが更新されると、調査するイベントが削除されたり、調査対象外のイベントが追加されたりすることがあるため、この機能は有用です。

ページの下部にあるリンクをクリックしてイベントの他のページを表示する場合は、時間枠が自動的に一時停止されます。準備ができたら時間枠の一時停止を解除できます。

分析が完了したら、時間枠の一時停止を解除できます。時間枠の一時停止を解除すると、設定に従って時間枠が更新されます。また、一時停止を解除した時間枠を反映するようにイベントビューが更新されます。

イベント時間枠の一時停止はダッシュボードには影響を与えず、ダッシュボードの一時停止もイベント時間枠の一時停止に影響しません。

手順

時間で制約されているワークフローでは、目的の時間範囲コントロールを選択できます。

- 時間枠を一時停止するには、時間範囲コントロールの[一時停止（Pause）]（  ）をクリックします。
- 時間枠の一時停止を解除するには、時間範囲コントロールの [再生（Play）]（  ）をクリックします。

イベントのデフォルト時間枠

イベントの分析中に、[日付/時間（Date/Time）] ウィンドウの [設定（Preferences）] タブを使用し、表示しているイベントのタイプに対するデフォルトの時間枠を（イベント ビューの設定を使用せずに）変更することができます。

この方法でデフォルトの時間枠を変更すると、表示しているイベントのタイプのデフォルト時間枠のみが変わります。たとえば、複数の時間枠を設定した場合、[設定（Preferences）] タブでデフォルトの時間枠を変更すると、イベント、ヘルス モニタリング、または監査ログ ウィンドウのいずれかの設定が変更されます。つまり、最初のタブで示されている時間枠が変更されます。1 つの時間枠を設定している場合に [設定（Preferences）] タブでデフォルトの時間枠を変更すると、イベントのすべてのタイプのデフォルト時間枠が変わります。

関連トピック

デフォルト時間枠 （244 ページ）

イベント タイプのデフォルトの時間枠オプション

次の表で、[設定（Preferences）] タブで設定できるさまざまな設定について説明します。

表 *94 :* 時間枠の設定

設定	説明
更新間隔（Refresh Interval）	イベント ビューの更新間隔を分単位で設定します。ゼロを入力すると、更新オプションは無効になります。
タイム ウィンドウの数（Number of Time Windows）	使用する時間枠の数を指定します。 • 監査ログ、ヘルス イベント、および時間によって制約可能なイベントに基づいたワークフローに対してそれぞれ別のデフォルト時間枠を設定する場合は、[複数（Multiple）] を選択します。 • すべてのイベントに適用されるグローバルな時間枠を使用する場合は、[単一（Single）] を選択します。

設定	説明
デフォルト時間枠：[最後を表示 - スライディング（Show the Last - Sliding）]	この設定を選択すると、指定する長さのスライディングのデフォルト時間枠を設定できます。 アプライアンスは、特定の開始時刻（たとえば1時間前）から現在までに生成されたすべてのイベントを表示します。イベントビューの変更と共に、時間枠は「スライド」して、常に最後の1時間内のイベントが表示されます。
デフォルトのタイム ウィンドウ（Default Time Window）：最終を表示（Show the Last）- 静的/拡張（Static/Expanding）	この設定を選択すると、指定する長さの、静的または拡張のデフォルト時間枠を設定できます。 **静的な**時間枠の場合（[終了時間を使用（Use End Time）] チェック ボックスをオンにした場合）、アプライアンスは特定の開始時間（1時間前などの）から、最初にユーザーがイベントを参照した時間までに生成されたすべてのイベントを表示します。イベントビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。 **拡張**時間枠の場合（[終了時間を使用（Use End Time）] チェック ボックスをオフにしたの場合）、アプライアンスは特定の開始時間（1時間前などの）から現在までに生成されたすべてのイベントを表示します。イベントビューを変更すると、時間枠は現在まで拡張されます。
デフォルトのタイム ウィンドウ（Default Time Window）：当日（Current Day）- 静的/スライディング（Static/Expanding）	この設定を選択すると、現在の日付に対して静的または拡張のデフォルト時間枠を設定できます。現在の日付は、現行セッションのタイムゾーン設定に基づいて午前0時に始まります。 **静的な**時間枠の場合（[終了時間を使用（Use End Time）] チェック ボックスをオンにした場合）、アプライアンスは午前0時から、最初にユーザーがイベントを参照した時間までに生成されたすべてのイベントを表示します。イベントビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。 **拡張**時間枠の場合（[終了時間を使用（Use End Time）] チェック ボックスをオフにした場合）、アプライアンスは午前0時から現在までに生成されたすべてのイベントを表示します。イベントビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に24時間を超えて分析を続けた場合、この時間枠は24時間よりも長くなる可能性があることに注意してください。

設定	説明
デフォルトのタイム ウィンドウ（Default Time Window）：今週（Current Week）- 静的/拡張（Static/Expanding）	この設定を選択すると、現在の週に対して静的または拡張のデフォルト時間枠を設定できます。現在の週は、現行セッションのタイム ゾーン設定に基づいて直前の日曜日の午前0時に始まります。 **静的な**時間枠の場合（[終了時間を使用（Use End Time）] チェック ボックスをオンにした場合）、アプライアンスは午前0時から、最初にユーザーがイベントを参照した時間までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。 **拡張**時間枠の場合（[終了時間を使用（Use End Time）] チェック ボックスをオフにした場合）、アプライアンスは日曜日の午前0時から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に1週間を超えて分析を続けた場合、この時間枠は1週間よりも長くなる可能性があることに注意してください。

イベント タイプのデフォルトの時間枠の変更

手順

ステップ 1 時間により制約されたワークフローで、[時間範囲（Time Range）]（） をクリックし、[日付と時間（Date/Time）] ウィンドウを開きます。

ステップ 2 [優先（Preferences）] をクリックし、イベント タイプのデフォルトの時間枠オプション （834 ページ）に記載されているようにプリファレンスを変更します。

ステップ 3 [設定の保存（Save Preferences）] をクリックします。

ステップ 4 次の 2 つの対処法があります。

- 使用しているイベント ビューに新しいデフォルト時間枠の設定を適用するには、[適用（Apply）] をクリックして [日時（Date/Time）] ウィンドウを閉じてイベント ビューをリフレッシュします。
- デフォルトの時間枠設定を適用せずに分析を続けるには、[適用（Apply）] をクリックせずに [日付と時間（Date/Time）] ウィンドウを閉じます。

イベント ビューの制約

ワークフローページに表示される情報は、ユーザが設定した制約によって異なります。たとえばイベント ワークフローを最初に開いた場合、情報は、最後の1時間に生成されたイベントに制約されています。

ワークフローの次のページに進んで、表示されるデータを特定の値で制約する場合は、ページでこれらの値を持つ行を選択し、[表示（View）] をクリックします。現在の制約を保持し、す

べてのイベントを含めた状態でワークフローの次のページに進むには、[すべて表示（View All）] を選択します。

（注） 複数の不可算値を持つ行を選択し、[表示（View）] を選択すると、複合的な制約が作成されます。

ワークフローのデータを制約するための3番目の方法があります。自身が選択した値を持つ行のみが表示されるようページを制約し、ページの上部に示される制約リストに選択した値を追加するには、ページの行で値をクリックします。たとえば、記録された接続のリストを表示する場合に、アクセス制御を使用して、自身が許可したものだけがリストに示されるよう制約する場合は、[アクション（Action）] カラムで [許可（Allow）] をクリックします。他の例では、侵入イベントを表示する場合に、宛先ポートが 80 のイベントのみがリストに示されるよう制約する場合は、[宛先ポート/ICMP コード（Destination Port/ICMP Code）] カラムで [80（http）/tcp（80 (http)/tcp）] をクリックします。

ヒント モニタ ルールの条件に基づいて接続イベントを制約するための手順は少し異なり、いくつかの追加手順が必要になる場合があります。また、関連付けられているファイルや侵入情報によって接続イベントを制約することはできません。

検索を使用して、ワークフローの情報を制約することもできます。1 つのカラム内の複数の値について制約する場合は、この機能を使用します。たとえば、2つのIPアドレスに関連しているイベントを表示する場合は、[検索の編集（Edit Search）] をクリックし、[検索（Search）] ページで対象の [IP アドレス（IP address）] フィールドを変更して両方のアドレスが含まれるようにして、[検索（Search）] をクリックします。

検索ページで入力した検索条件はページの上部に制約として表示され、これに従って制約されたイベントが合わせて表示されます。Management Center では、複合的な制約でない限り、他のワークフローにナビゲートしたときにも現在の制約が適用されます。

検索する場合は、検索対象のテーブルに検索の制約を適用するかどうかに注意する必要があります。たとえば、クライアントデータは接続サマリーでは使用できません。接続で検出されたクライアントに基づいて接続イベントを検索し、結果を接続サマリ イベント ビューで表示すると、Management Center では、制約が設定されていない場合と同じように接続データが表示されます。無効な制約は、非適用（N/A）とラベルが付けられ、取り消し線が付けられます。

イベントの制約

手順

ステップ 1 ワークフローの選択 （811 ページ）の説明に従って適切なメニュー パスとオプションを選択し、ワークフローにアクセスします。

ステップ 2 すべてのワークフローで、次のオプションを選択できます。

- ビューを単一の値と一致するイベントに制約するには、ページの行内の目的の値をクリックします。
- ビューを複数の値と一致するイベントに制約するには、その値を持つイベントのチェックボックスをオンにし、[表示（View）] をクリックします。

  （注） 行に複数の不可算値が含まれている場合は、複合的な制約が追加されます。

- 制約を解除するには、[制約の検索（Search Constraints）] **[展開矢印（Expand Arrow）]**（ ） をクリックし、展開された [制約の検索（Search Constraints）] リストで制約の名前をクリックします。
- 検索ページを使用して制約を編集するには、[検索の編集（Edit Search）] をクリックします。
- 保存済み検索として制約を保存するには、[検索の保存（Save Search）] をクリックし、クエリに名前を付けます。

  （注） 複合的な制約が含まれているクエリは保存できません。

- 別のイベント ビューで同じ制約を使用するには、[移動先（Jump to）] をクリックし、イベント ビューを選択します。

  （注） 別のワークフローに切り替えると、複合的な制約は保持されません。

- 制約の表示を切り替えるには、[制約の検索（Search Constraints）] の **[展開矢印（Expand Arrow）]**（ ） または [制約の検索（Search Constraints）] の **[折りたたみ矢印（Collapse Arrow）]**（ ）をクリックします。制約のリストが長く、画面の大半を占有する場合に、この機能は役立ちます。

複合イベント ビューの制約

複合的な制約は、特定のイベントに対するすべての不可算値に基づいています。複数の不可算値を持つ行を選択する場合は、ページ上の対象行におけるすべての不可算値と一致するイベントのみを取得する複合的な制約を設定します。たとえば、送信元 IP アドレスが `10.10.31.17` で、宛先 IP アドレスが `10.10.31.15` である行と、送信元 IP アドレスが `172.10.10.17` で宛先 IP アドレスが `172.10.10.15` である行を選択すると、次のすべての結果が取得されます。

- 送信元 IP アドレスが 10.10.31.17 で、かつ宛先 IP アドレスが 10.10.31.15 のイベント

  または

- 送信元 IP アドレスが 172.10.31.17 で、かつ宛先 IP アドレスが 172.10.31.15 のイベント

複合的な制約と単純な制約を組み合わせると、複合的な制約の各セットに単純な制約が追加されます。たとえば、上記に記載されている複合的な制約に対して、プロトコル値 tcp の単純な制約を追加すると、次のすべての結果が取得されます。

- 送信元 IP アドレスが 10.10.31.17 で、かつ宛先 IP アドレスが 10.10.31.15 で、かつプロトコルが tcp であるイベント

  または

- 送信元 IP アドレスが 172.10.31.17 で、かつ宛先 IP アドレスが 172.10.31.15 で、かつプロトコルが tcp であるイベント

複合的な制約について、検索および検索の保存を実行することはできません。また、別のワークフローに切り替えるのに、イベント ビューのリンクを使用した場合、または [ワークフロー切り替え（switch workflow）] をクリックした場合は、複合的な制約は保持できません。複合的な制約が適用されているイベント ビューをブックマークしても、制約はブックマークに保存されません。

複合イベント ビュー制約の使用

手順

ステップ 1 ワークフローの選択 （811 ページ）の説明に従って、適切なメニュー パスとオプションを選択してワークフローにアクセスします。

ステップ 2 複合制約を管理する場合、次の選択肢があります。

- 複合制約を作成するには、カウント以外の値を持つ 1 つ以上の行を選択し、[表示（View）] をクリックします。
- 複合制約をクリアするには、[検索制約（Search Constraints）] **[展開矢印（Expand Arrow）]**（▶）をクリックし、[複合制約（Compound Constraints）] をクリックします。

ワークフロー間のナビゲーション

ワークフロー ページの [移動（Jump to...）] ドロップダウン リストのリンクを使用して、他のワークフローへ移動できます。ドロップダウン リストを選択し、追加のワークフローを表示および選択します。

新しいワークフローを選択すると、（適切な場合は）、選択する行で共有されているプロパティおよび設定する制約が、新しいワークフローで使用されます。設定した制約またはイベントのプロパティが、新しいワークフローのフィールドにマップされない場合は、これらはドロップされます。また、ワークフローを切り替えた場合には、複合的な制約は保持されません。キャプチャ ファイルのワークフローの制約は、ファイルおよびマルウェアのイベント ワークフローのみに転送されます。

（注） 所定の時間範囲のイベント数を表示する場合、詳細なデータを利用できるイベントの数が、イベントの総数に反映されないことがあります。これは、ディスク領域の使用率を管理するために、古いイベントの詳細がシステムによってプルーニングされることがあるために発生します。イベント詳細のプルーニングを最小限にするために、対象の展開にとって最も重要なイベントだけを記録するようにイベント ロギングを調整できます。

時間枠を一時停止していない場合、または静的な時間枠を設定していない場合、ワークフローを変更したときに時間枠も変更されることに注意してください。

この機能により、疑わしいアクティビティの調査が強化されます。たとえば、接続データを表示していて、内部ホストが異常に大量のデータを外部サイトに転送していることに気付いた場合は、応答側のIPアドレスとポートを制約として選択し、[アプリケーション（Applications）] ワークフローへ移動することができます。[アプリケーション（Applications）] ワークフローは応答側の IP アドレスとポートを IP アドレスとポートの制約として使用し、アプリケーションの種類などの追加情報を表示することができます。ページの上部にある [ホスト（Hosts）] をクリックして、リモート ホストのホスト プロファイルを表示することもできます。

アプリケーションに関する詳細を検索した後で、[相関イベント（Correlation Events）] を選択して接続データ ワークフローに戻る、制約から応答側の IP アドレスを削除する、制約にイニシエータのIPアドレスを追加する、[アプリケーションの詳細（Application Details）] を選択して、データをリモートホストに転送するときに開始側のホストでユーザーがどのクライアントを使用しているかを確認する、といったことができます。ポートの制約は、[アプリケーションの詳細（Application Details）] ページには転送されないことに注意してください。ローカルホストを制約として保持したまま、追加情報を検索するために他のナビゲートボタンを使用することもできます。

- ローカル ホストがいずれかのポリシーに違反しているかどうかを検出するには、IP アドレスを制約として保持したままで [移動先（Jump to）] ドロップダウン リストから [相関イベント（Correlation Events）] を選択します。
- ホストに対して侵入ルールがトリガーされた（侵害を表している）かどうかを確認するには、[移動先（Jump to）] ドロップダウン リストから [侵入イベント（Intrusion Events）] を選択します。
- ローカル ホストのホスト プロファイルを表示し、ホストが、悪用された可能性のある脆弱性の影響を受けやすくなっているかどうかを判断するには、[移動（Jump to）] ドロップダウン リストから [ホスト（Hosts）] を選択します。

統合イベントビューアでの作業

統合イベントは、複数タイプのファイアウォールイベント（接続、侵入、ファイル、マルウェア、および一部のセキュリティ関連の接続イベント）の単一画面ビューを提供します。[統合イベント（Unified Events）] テーブルは、高度なカスタマイズが可能です。カスタムフィルタを作成して適用することにより、イベントビューアに表示される情報を微調整できます。統合

イベントテーブルの [ライブビュー（Live View）] オプションを使用すると、ファイアウォールイベントをリアルタイムで表示し、ネットワーク上のアクティビティをモニターすることができます。

統合イベントビューアを使用すると、次のことができます。

- 異なるタイプのイベント間の関係を調べる
- ポリシー変更の影響をリアルタイムで確認する

手順

ステップ 1 **[分析（Analysis）] > [統合イベント（Unified Events）]** を選択します。

ステップ 2 時間範囲（固定またはスライド）を選択して、特定の期間のファイアウォールイベントを表示します。デフォルトでは、統合イベントビューアテーブルには、過去1時間のイベントが表示されます。テーブルをフィルタ処理してセキュリティイベントのより詳細なコンテキストを取得したり、テーブルの列をカスタマイズしたり、ライブビューを有効にしてイベントの更新をリアルタイムで確認したりすることができます。

統合イベントの詳細については、「統合イベントについて」を参照してください。

ブックマーク

イベントの分析の特定の場所と時間にすばやく戻りたい場合には、ブックマークを作成します。ブックマークは、次の情報が含まれます。

- 使用中のワークフロー
- ワークフローの表示中の部分
- ワークフローのページ番号
- 検索の制約
- 無効になっているカラム
- 使用している時間範囲

あるユーザが作成したブックマークは、ブックマーク アクセスを持っているすべてのユーザアカウントで利用できます。これは、より詳細な分析を必要とするイベントセットを発見した場合、簡単にブックマークを作成し、適切な権限を持った他のユーザーに調査を引き継ぐことが可能であることを意味します。

（注） ブックマークに表示されているイベントが（ユーザーによって直接、またはデータベースの自動クリーンアップによって）削除されると、そのブックマークにあった元のイベントは表示されなくなります。

ブックマークの作成

マルチドメイン導入では、現在のドメインで作成されたブックマークのみを表示できます。

手順

ステップ 1 イベントの分析中に、表示されている対象のイベントで[このページをブックマーク（Bookmark This Page）] をクリックします。

ステップ 2 [名前（Name）] フィールドに、名前を入力します。

ステップ 3 [ブックマークの保存（Save Bookmark）] をクリックします。

ブックマークの表示

マルチドメイン導入では、現在のドメインで作成されたブックマークのみを表示できます。

手順

すべてのイベント ビューで、以下の 2 つの方法を選択できます。

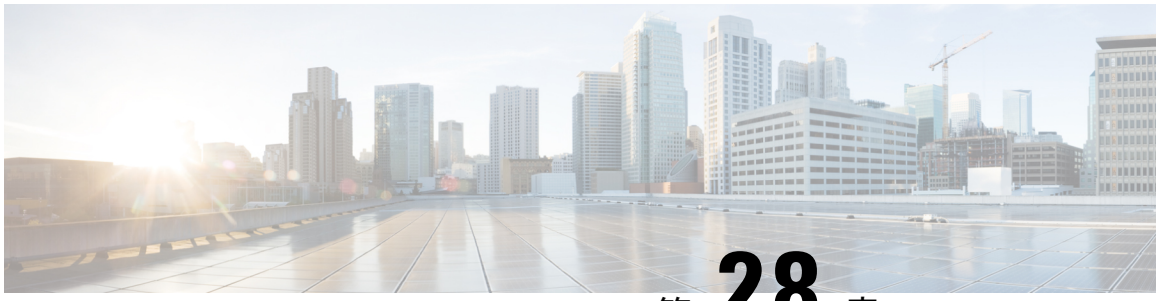
- [ブックマークの表示（View Bookmarks）] の上にポインタを合わせ、ドロップダウン メニューから目的のブックマークをクリックします。
- [ブックマークの表示（View Bookmarks）] をクリックし、[ブックマークの表示（View Bookmarks）] ページで目的のブックマーク名をクリックするか、その横にある [表示（View）]（） をクリックします。

  （注） 最初にブックマークに表示されていたイベントが（ユーザによって直接、またはデータベースの自動クリーンアップによって）削除されると、そのブックマークにはイベントの元のセットは表示されません。

ワークフローの履歴

表 *95*：

機能	最小 Management Center	最小 Threat Defense	詳細
廃止：侵入インシデントとイベントクリップボード。	7.1	任意（Any）	侵入インシデントとイベントクリップボードは廃止されています。 廃止された画面： • [分析（Analysis）] > [侵入（Intrusions）] > [クリップボード（Clipboard）] • [分析（Analysis）] > [侵入（Intrusions）] > [インシデント（Incidents）]
統合イベントビューア。	7.0	任意（Any）	接続（セキュリティインテリジェンスを含む）、侵入、ファイル、マルウェアの複数のイベントタイプを 1 つのテーブルで表示および操作します。 新規/変更された画面：**[分析（Analysis）] > [統合イベント（Unified Events）]**
リモートに保存されたイベントの操作。	7.0	任意（Any）	FMC を使用して Secure Network Analytics アプライアンスに保存されている接続イベントを操作できます。システムに自動的に最適なデータソースを使用させるか、またはソースを明示的に選択できます。このオプションは、セキュリティ分析とロギング（オンプレミス） ウィザードを完了した場合にのみ表示されます。 新規/変更された画面：イベントビューア、ダッシュボード、コンテキストエクスプローラ、レポートなど、接続イベントを表示するページ。
特定のケースでのワークフローテーブルの読み込み速度の改善。	6.6	任意（Any）	ワークフローページのテーブルには、表示される列が 6 つ以下の場合にのみ、同一の行の Count 列が表示されるようになりました。これにより、必要な計算量が最小限に抑えられるため、テーブルの読み込み速度が向上します。 新規/変更された画面：イベントビューア。



第 28 章

イベント検索

以下のトピックでは、ワークフロー内のイベントの検索方法について説明します。

イベントの検索

システムでは、データベーステーブルにイベントとして保存される情報が生成されます。イベントには、アプライアンスがイベントを生成する原因となったアクティビティを示すいくつかのフィールドが含まれます。ご使用の環境用にカスタマイズされた、さまざまなイベントタイプの検索を作成および保存し、後で再使用するために保存できます。

検索設定を保存するときには、その検索設定の名前を付け、それを自分だけで使用するか、それともアプライアンスの全ユーザが使用できるようにするかを指定します。カスタム ユーザ ロールのデータの制限として検索を使用する場合は、**必ず**プライベート検索として保存する必要があります。以前に検索設定を保存した場合、それをロードし、必要に応じて修正して、検索を開始することができます。カスタム分析のダッシュボード ウィジェット、レポート テンプレート、カスタム ユーザ ロールも、保存した検索を使用できます。保存済みの検索設定がある場合、[検索（Search）] ページからそれらを削除できます。

いくつかのイベントタイプに関しては、システムに備わっている定義済みの検索設定をサンプルとして使用すると、ネットワークについての重要な情報にすばやくアクセスできます。ネットワーク環境に合わせて定義済み検索設定のフィールドを変更し、検索設定を保存して、後で再利用することができます。

検索の種類に応じて、使用できる検索条件は異なりますが、メカニズムは同じです。検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。

（注） カスタム テーブルの検索には、若干異なる手順が必要です。

関連トピック

カスタム テーブルの検索 （873 ページ）

検索の制約

データベーステーブルごとに、検索を制約する値を入力できる独自の検索ページがあります。入力した値は、そのテーブルに定義されているフィールドに適用されます。フィールドのタイプによっては、特殊なシンタックスを使用して、ワイルドカード文字や数値の範囲などの基準を指定できます。

検索結果はワークフローページに表示され、カラム式レイアウトでテーブルの各フィールドが示されます。一部のデータベース テーブルは、ワークフロー ページにカラムとして表示されないフィールドを使用した検索も行えます。ワークフローページで結果を確認する際に、該当する制約が検索結果に適用されているかどうかを判別するには、**[展開矢印（Expand Arrow）]**（▶） をクリックして、検索に現在有効になっている制約を表示します。

一般的な検索の制約

イベントを検索するときは、次の一般的な注意事項を順守してください。

- 多くのフィールドでは、部分一致検索にワイルドカードが必要です。これらの検索では、すべてのフィールドでワイルドカードを使用できます。

  検索で使用するワイルドカードと記号 （847 ページ）を参照してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「A」または「B」または「C, D, E」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドにAまたはB、またはC、D、Eのすべてを含むレコードが一致します。

- フィールドでその情報を利用できないイベントを示すには、そのフィールドで `n/a` を指定します。フィールドに情報が入力されているイベントを示すには `!n/a` を使用します。
- 多くの数値フィールドの前には、より大きい（`>`）、以上（`>=`）、より小さい（`<`）、以下（`<=`）、等しい（`=`）または等しくない（`<>`）の演算子を付けることができます。

ヒント　長い複雑な値を（SHA-256ハッシュ値など）を含むフィールドを検索する場合は、ソース資料から検索基準値をコピーし、検索ページの適切なフィールドに貼り付けることができます。

検索で使用するワイルドカードと記号

接続イベントとセキュリティ インテリジェンス イベントのすべてのテキストフィールド、および他のイベントタイプのほとんどのテキストフィールドを検索する場合、テキストフィールドで部分一致を検索するには、文字列内の指定されていない文字を表すためにアスタリスク（*）が必要です。アスタリスクを使用しない検索は、これらのフィールドでの完全一致検索になります。ワイルドカードを必要としないフィールドでも、部分一致検索には常にワイルドカードを使用することを推奨します。

たとえば、`example.com`、`www.example.com`、または `department.example.com` を見つけるには、`*.example.com` で検索します。`example.com` で検索すると、ほとんどの場合、`example.com` のみが返されます。

英数字以外の文字（アスタリスク文字を含む）を検索するには、検索文字列を引用符で囲みます。たとえば、次の文字列を検索するとします。

```
Find an asterisk (*)
```

次のように入力します。

```
"Find an asterisk (*)"
```

検索でのオブジェクトとアプリケーションのフィルタ

システムでは、ネットワーク構成の一部として使用可能な名前付きオブジェクト、オブジェクトグループ、およびアプリケーションフィルタを作成できます。検索を実行または保存するときには、検索条件としてこれらのオブジェクト、グループ、およびフィルタを使用できます。

検索を実行するときに、オブジェクト、オブジェクトグループ、およびアプリケーションフィルタは `${object_name}` という形式で表示されます。たとえば、オブジェクト名 `ten_ten_network` であるネットワーク オブジェクトは、検索では `${ten_ten_network}` と表されます。

検索基準としてオブジェクトを使用できる検索フィールドの横には **[オブジェクト（Object）]**（⊕） が表示され、これをクリックすることができます。

関連トピック

オブジェクト マネージャ

検索で指定する時間制約

時間値を指定できる検索条件フィールドで使用可能な形式を、次の表に示します。

表 *96*：検索フィールドにおける時間指定

時間の形式	例
`today [at HH:MMam|pm]`	`today` `today at 12:45pm`
*YYYY-DD*MM- *HH*:*MM*:*SS*	`2006-03-22 14:22:59`

時間値の前に、以下のいずれか 1 つの演算子を指定できます。

表 *97*：時間指定の演算子

演算子	例	説明
<	`< 2006-03-22 14:22:59`	2006 年 3 月 22 日午後 2:23 より前のタイムスタンプを持つイベントを返します。
>	`> today at 2:45pm`	今日の午後 2 時 45 分より後のタイムスタンプを持つイベントを返します。

検索での IP アドレス

検索で IP アドレスを指定するときには、個別の IP アドレス、複数アドレスのカンマ区切りリスト、アドレス ブロック、またはハイフン（-）で区切った IP アドレス範囲を入力することができます。また、否定を使用することもできます。

IPv6 をサポートする検索（侵入イベント、接続データ、相関イベントの検索など）では、IPv4 アドレス、IPv6 アドレス、および CIDR/プレフィックス長アドレス ブロックを任意に組み合わせて入力できます。IP アドレスを使用してホストを検索した場合、結果には、少なくとも 1 つの IP アドレスが検索条件と一致するホストがすべて含まれます（つまり、IPv6 のアドレスの検索では、プライマリ アドレスが IPv4 であるホストが返されることがあります）。

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

IP アドレスをネットワークオブジェクトによって表すことができるため、IP アドレス検索フィールドの横にあるネットワークの追加の**[オブジェクト（Object）]**（+）をクリックして、ネットワークオブジェクトを IP アドレス検索基準として使用することもできます。

表 *98 :* 使用可能な *IP* アドレス構文

指定する項目	タイプ	例
単一の IP アドレス	その IP アドレス。	`192.168.1.1` `2001:db8::abcd`
リストを使用した複数の IP アドレス	IP アドレスからなるカンマ区切りリスト。カンマの前後にスペースを追加**しない**でください。	`192.168.1.1,192.168.1.2` `2001:db8::b3ff,2001:db8::0202`
CIDR ブロックまたはプレフィックス長で指定できる IP アドレスの範囲	IPv4 CIDR または IPv6 プレフィクス長表記の IP アドレス ブロック。	`192.168.1.0/24` これは、サブネット マスク 255.255.255.0 である 192.168.1.0 ネットワーク内の任意の IP を指定します（つまり 192.168.1.0 から 192.168.1.255 まで）。
CIDR ブロックやプレフィクスで指定できない IP アドレスの範囲	ハイフンを使用した IP アドレス範囲。ハイフンの前後にスペースを入力**しない**でください。	`192.168.1.1-192.168.1.5` `2001:db8::0202-2001:db8::8329`

他の方法で否定を使用して IP アドレスまたは IP アドレス範囲を指定	IP アドレス、ブロック、または範囲の先頭に感嘆符を付ける。	`192.168.0.0/32,!192.168.1.10`
		`!2001:db8::/32`
		`!192.168.1.10,!2001:db8::/32`

ブロックされたホストまたはモニター対象の（そうでなければブロックされた）ホスト ホスト プロファイルのアイコン（816 ページ）を参照してください。	接続イベントとセキュリティインテリジェンスイベントの、[イニシエータIP（Initiator IP）] フィールドと [レスポンダIP（Responder IP）] フィールド： • block • monitor	--

関連トピック

IP アドレスの規則 （31 ページ）

検索での URL

URL を検索するときは、ワイルドカードを含めます。たとえば、**`*example.com*`** を使用すると、**`https://example.com`**、**`division.example.com`**、**`example.com/division/`** など、ドメインのすべてのバリエーションを検索します。

検索での管理対象デバイス

デバイスをグループ化している場合（Management Center で、または実際の高可用性設定あるいは拡張性設定として）、グループの名前を検索すると、グループ内のすべてのデバイスに対する結果が正しく返されます。

システムでグループ、の一致が検出されると、検索を実行するために、そのグループ名名が適切なメンバー デバイス名に置き換えられます。デバイス フィールドのデバイス グループを使用する検索を保存すると、デバイス フィールドで指定した名前がシステムによって保存され、検索が実行されるたびにデバイス名の置換が再度実行されます。

検索でのポート

システムでは、ポート番号を表す特定の構文を検索で指定できます。次の入力が可能です。

- 1 つのポート番号
- コンマで区切られたポート番号リスト
- ポート番号範囲を示すのにダッシュで区切られた 2 つのポート番号
- 1 つのポート番号の後に、スラッシュで区切られたプロトコル省略形（侵入イベントを検索する場合のみ）
- 1 つのポート番号またはポート番号範囲の前に 1 つの感嘆符（指定されたポートの否定を表す）

（注） ポート番号や範囲を指定するときには、スペースを使用**しない**でください。

表 *99 :* ポート構文例

例	説明
`21`	ポート 21 でのすべてのイベントを返します（TCP および UDP イベントを含む）。
`!23`	ポート 23 上のイベントを除くすべてのイベントを返します。
`25/tcp`	ポート 25 の TCP 関連侵入イベントをすべて戻します。
`21/tcp,25/tcp`	ポート 21、25 の TCP 関連侵入イベントをすべて戻します。
`21-25`	ポート 21 から 25 のイベントをすべて戻します。

検索のイベント フィールド

イベントを検索するときは、検索条件として次のフィールドを使用できます。

- 監査ログのワークフロー フィールド （501 ページ）
- アプリケーション データ フィールド （1118 ページ）
- アプリケーションの詳細データ フィールド （1121 ページ）
- キャプチャされたファイルのフィールド （1032 ページ）
- 許可（Allow）リストイベントのフィールド （1160 ページ）
- 接続およびセキュリティ関連の接続イベントフィールド （902 ページ）
- 相関イベントのフィールド （1155 ページ）
- ディスカバリ イベントのフィールド （1096 ページ）
- [ヘルス イベント（Health Events）] テーブル （484 ページ）
- ホスト属性データ フィールド （1106 ページ）
- ホスト データ フィールド （1098 ページ）
- ファイルおよびマルウェア イベント フィールド （1011 ページ）
- 侵入イベント フィールド （948 ページ）
- 侵入ルール更新のログの詳細 （279 ページ）
- 修復ステータスのテーブル フィールド （1164 ページ）
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Nmap Scan Results Fields*」を参照してください
- サーバー データ フィールド （1114 ページ）
- サードパーティの脆弱性データのフィールド （1129 ページ）
- ユーザー関連フィールド （1130 ページ）
- 脆弱性データのフィールド （1123 ページ）
- 許可（Allow）リスト違反のフィールド （1162 ページ）

検索の実行

検索を実行するには、管理者権限またはセキュリティアナリスト権限が必要です。

手順

ステップ 1 **[分析（Analysis）] > [検索（Search）]** を選択します。

ヒント また、ワークフローの任意のページから [検索（Search）] をクリックすることもできます。

ステップ 2 テーブルのドロップダウンリストから、検索するイベントタイプまたはデータを選択します。

ステップ 3 該当するフィールドに検索基準を入力します。使用可能な検索条件の詳細については、次の項を参照してください。

- 検索の制約 （846 ページ）
- 監査ログのワークフロー フィールド （501 ページ）
- アプリケーション データ フィールド （1118 ページ）
- アプリケーションの詳細データ フィールド （1121 ページ）
- キャプチャされたファイルのフィールド （1032 ページ）
- 許可（Allow）リストイベントのフィールド （1160 ページ）
- 接続およびセキュリティ関連の接続イベントフィールド （902 ページ）
- 相関イベントのフィールド （1155 ページ）
- ディスカバリ イベントのフィールド （1096 ページ）
- [ヘルス イベント（Health Events）] テーブル （484 ページ）
- ホスト属性データ フィールド （1106 ページ）
- ホスト データ フィールド （1098 ページ）
- ファイルおよびマルウェア イベント フィールド （1011 ページ）
- 侵入イベント フィールド （948 ページ）
- 侵入ルール更新のログの詳細 （279 ページ）
- 修復ステータスのテーブル フィールド （1164 ページ）
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Nmap Scan Results Fields*」を参照してください
- サーバー データ フィールド （1114 ページ）
- サードパーティの脆弱性データのフィールド （1129 ページ）
- ユーザー データのフィールド
- ユーザー アクティビティ データのフィールド
- 脆弱性データのフィールド （1123 ページ）
- 許可（Allow）リスト違反のフィールド （1162 ページ）

ステップ 4 将来検索を再度使用する場合は、その検索を保存します。詳細については、検索設定の保存 （853 ページ）を参照してください。

ステップ 5 [検索（Search）] をクリックして、検索を開始します。検索結果は、検索されるテーブルのデフォルト ワークフローで表示され、該当する場合には時間で制約されます。

次のタスク

- ワークフローを使用して検索結果を分析する場合は、ワークフローの使用 （809 ページ）を参照してください。

関連トピック

イベント ビューの設定 （241 ページ）

検索設定の保存

検索を保存するには、管理者権限またはセキュリティアナリスト権限が必要です。

マルチドメイン展開では、現在のドメインで作成された保存済みの検索が表示されます。これは編集できます。先祖ドメインで作成された保存済みの検索も表示されますが、これは編集できません。下位のドメインで作成された検索を表示および編集するには、そのドメインに切り替えます。

始める前に

- 検索の実行 （851 ページ）で説明するように検索条件を設定するか、保存済み検索設定のロード （854 ページ）で説明するように保存した検索をロードします。

手順

ステップ 1 [検索（Search）] ページから、自分だけがアクセスできるように検索設定をプライベートとして保存する場合は、[プライベート（Private）] チェックボックスをオンにします。

ヒント カスタム ユーザ ロールのデータの制限として検索を使用する場合は、**必ず**プライベート検索として保存する必要があります。

ステップ 2 次の 2 つの対処法があります。

- ロードした検索設定の新しいバージョンを保存する場合は、[新規に保存（Save As New）] をクリックします。
- 新しい検索結果を保存する場合や、同じ名前を使用してカスタム検索を上書きする場合は、[保存（Save）] をクリックします。 コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

保存済み検索設定のロード

保存済み検索をロードするには、管理者権限またはセキュリティアナリスト権限が必要です。

マルチドメイン展開では、現在のドメインで作成された保存済みの検索が表示されます。これは編集できます。先祖ドメインで作成された保存済みの検索も表示されますが、これは編集できません。下位のドメインで作成された検索を表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[分析（Analysis）]** > **[検索（Search）]**を選択します。

ヒント また、ワークフローの任意のページから [検索（Search）] をクリックすることもできます。

ステップ 2 テーブルのドロップダウンリストから、検索するイベントまたはデータのタイプを選択します。

ステップ 3 [カスタム検索（Custom Searches）] リストまたは [定義済の検索（Predefined Searches）] リストから、ロードする検索を選択します。

ステップ 4 別の検索条件を使用するには、検索の制約を変更します。

ステップ 5 変更した検索を将来再度使用する場合は、検索を保存しておきます。詳細については、検索設定の保存 （853 ページ）を参照してください。

ステップ 6 **[検索（Search）]** をクリックします。

シェルによるクエリ オーバーライド

システム管理者は、Linux シェル ベースのクエリ管理ツールを使用して、実行時間の長いクエリを検出および停止することができます。

クエリ管理ツールでは指定した分数よりも実行時間が長いクエリを検索し、それらのクエリを停止することができます。ユーザーがクエリを停止すると、このツールにより監査ログと syslog にイベントが記録されます。

`admin` 内部ユーザーは Management Center CLI にアクセスできることに注意してください。CLI アクセスを与える外部認証オブジェクトを使用する場合、シェル アクセス フィルタに一致するユーザーもまた CLI にログインできます。

（注） Web インターフェイス内の検索ページを終了しても、クエリは停止しません。長い時間をかけて結果を返すクエリは、クエリ実行中にシステム全体のパフォーマンスに影響を与えます。

シェルベースのクエリ管理の構文

実行時間が長いクエリを管理するには、次の構文を使用します。

```
query_manager [-v] [-l [minutes]] [-k query_id [...]] [--kill-all minutes]
```

表 100 : query_manager オプション

オプション	説明
`-h, --help`	短いヘルプ メッセージを出力します。
`-l, --list [minutes]`	指定された時間（分単位）を超えるすべてのクエリをリストします。デフォルトで、1分より長くかかっているすべてのクエリを表示します。
`-k, --kill query_id [...]`	指定された ID を持つクエリを強制終了します。オプションは複数の ID を取得する場合があります。
`--kill-all minutes`	指定された時間（分単位）を超えるすべてのクエリを強制終了します。
`-v, --verbose`	完全な SQL クエリを含む詳細な出力。

注意 システム セキュリティ上の理由から、アプライアンスでは追加の Linux シェル ユーザーを確立しないことを強く推奨します。

実行時間が長いクエリの停止

CLI アクセス権がある **admin** ユーザーまたは外部で認証されたユーザーである必要があります

手順

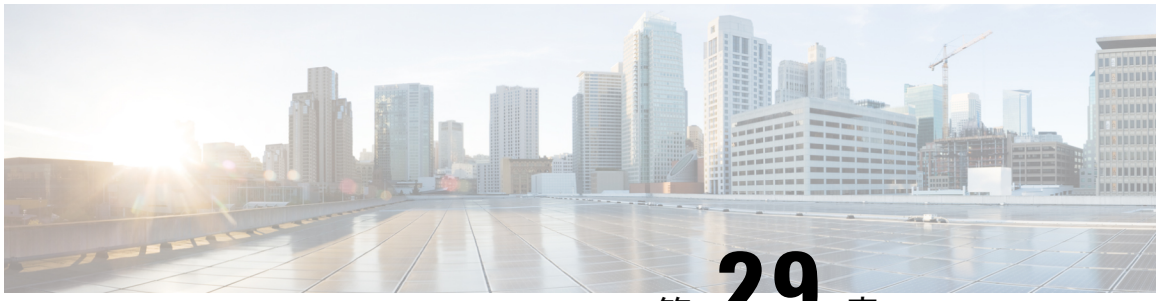
ステップ 1 `ssh` を使用して Secure Firewall Management Center に接続します。

ステップ 2 CLI `expert` コマンドを使用して Linux シェルにアクセスします。

ステップ 3 シェルベースのクエリ管理の構文 （855 ページ）で説明された構文を使用して、`sudo` で `query_manager` を実行します。

イベントの検索の履歴

機能	最小 Management Center	最小 Threat Defense	詳細
多くのフィールドでの部分一致検索では、ワイルドカードが必要になりました	6.6	任意（Any）	たとえば、URL を検索する場合、**`*example.com*`** を使用して、**`example.com`** のすべてのバリエーションを検索します。 この動作の変更は、接続またはセキュリティ インテリジェンス イベントを検索するときの、[分析（Analysis）] > [検索（Search）] ページでの検索に適用されます。この検索ページは、他のページのリンクからもアクセスできます。 部分一致検索にワイルドカードを必要としないフィールドでは、オプションでワイルドカードを使用できます。 影響を受けるプラットフォーム：Management Center



第 29 章

カスタムワークフロー

次のトピックでは、カスタム ワークフローの使用方法について説明します。

カスタム ワークフローの概要

シスコが提供する事前定義のカスタム ワークフローがニーズに合わない場合は、カスタム ワークフローを作成して管理することができます。

カスタム ワークフローは、組織に特有のニーズに合わせて作成するワークフローです。カスタム ワークフローを作成する場合は、ワークフローのベースとなるイベント（またはデータベース テーブル）の種類を選択します。Management Center では、カスタム ワークフローをカスタム テーブルのベースにすることができます。また、カスタム ワークフローに含まれるページを選択することもできます。カスタム ワークフローには、ドリルダウン、テーブル ビュー、ホストまたはパケット ビューのページを含めることができます。

イベント評価プロセスが変わった場合には、新しいニーズを満たすようにカスタム ワークフローを編集することができます。事前定義のワークフローは編集できないことに注意してください。

ヒント 任意のイベント タイプについて、デフォルト ワークフローとしてカスタム ワークフローを設定することができます。

保存済みカスタム ワークフロー

Management Center は、変更可能な定義済みのワークフローの他に保存済みのカスタム ワークフローを含みます。それぞれのワークフローは、カスタムテーブルに基づき、いずれも変更可能です。

マルチドメイン展開では、これらの保存されたワークフローは、グローバル ドメインに属し、下位ドメインでは変更できません。

表 *101* : 保存済みカスタム ワークフロー

ワークフロー名	説明
優先度および分類によるイベント	このワークフローでは、イベントとタイプのリストをそれぞれのイベントが発生した回数と共にイベントの優先度の順に示します。 このワークフローは、侵入イベントのカスタム テーブルに基づきます。
サーバのデフォルト ワークフローのあるホスト	このワークフローを使用すると、サーバのカスタムテーブルと共にホストの基本的な情報をすぐに表示できます。 このワークフローは、サーバのカスタム テーブルのあるホストに基づきます。
サーバとホストの詳細	このワークフローを使用して、ネットワークで最も高頻度で使用されているサーバやそのサーバを稼働しているホストを決定できます。 このワークフローは、サーバーのカスタム テーブルのあるホストに基づきます。

カスタム ワークフローの作成

シスコが提供する事前定義のカスタム ワークフローがニーズに合わない場合は、カスタム ワークフローを作成することができます。

ヒント 新しいカスタム ワークフローを作成する代わりに、別のアプライアンスからカスタム ワークフローをエクスポートし、それを自身のアプライアンスへインポートすることができます。その後でニーズに合わせて、インポートしたワークフローを編集することができます。

カスタム ワークフローを作成する場合は、次の操作を行います。

- ワークフローのソースとなるテーブルを選択する
- ワークフローの名前を指定する
- ワークフローにドリル ダウン ページおよびテーブル ビュー ページを追加する

ワークフローの各ドリル ダウン ページでは、次のことができます。

- Web インターフェイスのページの上部に表示される名前を指定する
- 1 ページにつき最大 5 個のカラムを含める
- デフォルトのソート順（昇順または降順）を指定する

ワークフロー ページの順序において、任意の場所にテーブル ビュー ページを追加することができます。これらのページには編集可能なプロパティ（ページ名、ソート順、ユーザ定義可能なカラム位置など）がありません。

（注） カスタム ワークフローには、イベントのドリル ダウン ページまたはテーブル ビューを少なくとも 1 つ追加する必要があります。

（注） テーブル タイプに [脆弱性（Vulnerabilities）] を選択し、テーブル カラムに [IP アドレス（IP Address）] を追加しても、検索機能を使用して特定の IP アドレスまたはアドレスのブロックを表示するようワークフローを制約しない限り、カスタム ワークフローを使用して脆弱性を表示する場合に [IP アドレス（IP Address）] カラムは表示されません。

カスタム ワークフローの最終ページは、次の表に記載されているように、ワークフローのベースにしているテーブルによって異なります。これらの最終ページは、ワークフローを作成したときにデフォルトで追加されます。

表 *102*：カスタム ワークフローの最終ページ

イベント/アセット タイプ	最終ページ
ディスカバリ イベント	ホスト
脆弱性	脆弱性の詳細
サードパーティの脆弱性	ホスト
Users	Users
侵害の兆候	ホストまたはユーザ
侵入イベント	パケット

システムは、他の種類のイベント（監査ログやマルウェア イベントなど）に基づくカスタム ワークフローには最終ページを追加しません。

接続データに基づくカスタム ワークフローもその他のカスタム ワークフローと同様です。ただし、接続データに基づくカスタム ワークフローには接続の要約データを含むドリル ダウン ページや個々の接続とテーブル ビュー ページを含むドリル ダウン ページを入れることができます。

非接続データに基づくカスタム ワークフローの作成

非接続データに基づいてカスタムワークフローを作成するには、管理者権限またはセキュリティアナリスト権限が必要です。

手順

ステップ 1 **[分析（Analysis）] > [詳細（Advanced）] > [カスタムワークフロー（Custom Workflows）]**を選択します。

ステップ 2 [カスタム ワークフローの作成（Create Custom Workflow）] をクリックします。

ステップ 3 [名前（Name）] フィールドにワークフローの名前を入力します。

ステップ 4 必要に応じて、[説明（Description）] を入力します。

ステップ 5 [テーブル（Table）] ドロップダウン リストから、対象とするテーブルを選択します。

ステップ 6 ワークフローに1つ以上のドリルダウンページを追加する場合は、[ページの追加（Add Page）] をクリックします。

ステップ 7 [ページ名（Page Name）] フィールドにページの名前を入力します。

ステップ 8 [カラム 1（Column 1）] で、ソートの優先順位およびテーブルのカラムを選択します。このカラムは、ページの最も左のカラムとして表示されます。

例：

たとえば、対象とする宛先ポートを示すページを作成し、カウントでページをソートするには、[ソートの優先順位（Sort Priority）] ドロップダウン リストから [2] を選択し、[フィールド（Field）] ドロップダウン リストから [宛先ポート/ICMP コード（Destination Port/ICMP Code）] を選択します。

ステップ 9 ページに表示するすべてのフィールドが指定されるまで、含めるフィールドの選択とソートの優先順位の設定を続けます。

ステップ 10 ワークフローにテーブル ビュー ページを追加するには、[テーブル ビューの追加（Add Table View）] をクリックします。

ステップ 11 [保存（Save）] をクリックします。

カスタム接続データ ワークフローの作成

接続データに基づいたカスタム ワークフローは他のカスタム ワークフローと似ていますが、ドリルダウン ページとテーブル ビュー ページだけでなく、接続データ グラフのページも含めることができます。必要に応じて、ワークフローにそれぞれのタイプのページを任意の数だけ、任意の順序で含めることができます。それぞれの接続データ グラフのページには1つのグラフ（線グラフ、棒グラフ、または円グラフ）が含まれます。線グラフと棒グラフには、複数のデータセットを含めることができます。

接続データに基づいてカスタムワークフローを作成するには、管理者権限が必要です。

手順

ステップ 1 **[分析（Analysis）] > [詳細（Advanced）] > [カスタムワークフロー（Custom Workflows）]**を選択します。

ステップ 2 [カスタム ワークフローの作成（Create Custom Workflow）] をクリックします。

ステップ 3 [名前（Name）] フィールドにワークフローの名前を入力します。

ステップ 4 必要に応じて、[説明（Description）] を入力します。

ステップ 5 [テーブル（Table）] ドロップダウン リストから、[接続イベント（Connection Events）] を選択します。

ステップ 6 ワークフローに 1 つ以上のドリルダウン ページを追加する場合は、次の 2 つのオプションがあります。

- 個々の接続に関するデータが含まれているドリルダウン ページを追加するには、[ページの追加（Add Page）] をクリックします。
- 接続の概要データが含まれているドリルダウン ページを追加するには、[サマリー ページの追加（Add Summary Page）] をクリックします。

ステップ 7 [ページ名（Page Name）] フィールドにページの名前を入力します。

ステップ 8 [カラム 1（Column 1）] で、ソートの優先順位およびテーブルのカラムを選択します。このカラムは、ページの最も左のカラムとして表示されます。

ステップ 9 ページに表示するすべてのフィールドが指定されるまで、含めるフィールドの選択とソートの優先順位の設定を続けます。

例：

たとえば、監視対象ネットワーク経由で転送されるトラフィックの量を表示するページを作成し、トラフィックの転送量が最も多い応答側によってページをソートするには、[ソートの優先順位（Sort Priority）] ドロップダウン リストで [1] を選択し、[フィールド（Field）] ドロップダウン リストで [応答側のバイト数（Responder Bytes）] を選択します。

ステップ 10 ワークフローに 1 つ以上のグラフ ページを追加する場合は、[グラフの追加（Add Graph）] をクリックします。

ステップ 11 [グラフ名（Graph Name）] フィールドにページの名前を入力します。

ステップ 12 ページに含めるグラフのタイプを選択します。

- 線グラフ（[折れ線グラフ（Line chart）]（  ））
- 棒グラフ（[棒グラフ（Bar Char）]（  ））
- 円グラフ（[円グラフ（Pie chart）]（））

ステップ 13 グラフの X 軸と Y 軸を選択し、グラフ化するデータの種類を指定します。

円グラフでは、X 軸は独立変数を表し、Y 軸は従属変数を表します。

ステップ 14 グラフに含めるデータセットを選択します。

円グラフには 1 つのデータセットしか含めることができないことに注意してください。

ステップ 15 接続データのテーブル ビューを追加するには、[テーブル ビューの追加（Add Table View）] をクリックします。

テーブル ビューは設定できません。

ステップ 16 [保存（Save）] をクリックします。

カスタム ワークフローの使用と管理

ワークフローが、事前定義のイベント テーブルまたはカスタム テーブルのいずれに基づいているかによって、ワークフローの表示に使用する方法が異なります。

カスタム ワークフローが事前定義のイベント テーブルに基づいている場合は、アプライアンスに付属しているワークフローにアクセスするのと同じ方法でアクセスします。たとえば、ホスト テーブルに基づいているカスタム ワークフローにアクセスするには、**[分析（Analysis）]** > **[ホスト（Hosts）]** > **[ホスト（Hosts）]** を選びます。また、カスタム ワークフローがカスタム テーブルに基づいている場合は、[カスタム テーブル（Custom Tables）] ページからアクセスする必要があります。

イベント評価プロセスが変わった場合には、新しいニーズを満たすようにカスタム ワークフローを編集することができます。事前定義のワークフローは編集できないことに注意してください。

ヒント 任意のイベント タイプについて、デフォルト ワークフローとしてカスタム ワークフローを設定することができます。

事前定義されたテーブルに基づいたカスタム ワークフローの表示

カスタムワークフローを表示するには、管理者、メンテナンス、またはセキュリティアナリストの権限が必要です。

手順

ステップ 1 ワークフローの選択 （811 ページ）の説明に従って、カスタム ワークフローのベースとなるテーブルについて、適切なメニュー パスとオプションを選択します。

ステップ 2 カスタム ワークフローも含め、別のワークフローを使用するには、現在のワークフロー タイトルの横にある [(ワークフローの切り替え)（(switch workflow)）] をクリックします。

ステップ 3 イベントが表示されず、ワークフローを時間によって制約できる場合は、時間範囲の調整が必要なことがあります（イベント時間の制約 （829 ページ）を参照）。

カスタム テーブルに基づくカスタム ワークフローの表示

カスタムテーブルに基づくカスタムワークフローを表示するには、管理者またはセキュリティアナリストの権限が必要です。

マルチドメイン展開では、現在のドメインで作成されたカスタムワークフローが表示されます。これは編集できます。先祖ドメインで作成されたカスタムワークフローも表示されますが、これは編集できません。下位のドメインのカスタムワークフローを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[分析（Analysis）]** > **[詳細（Advanced）]** > **[カスタムテーブル（Custom Tables）]** を選択します。

ステップ 2 表示するカスタムテーブルの隣にある [表示（View）]（  ） をクリックするか、またはカスタムテーブルの名前をクリックします。

ステップ 3 カスタム ワークフローも含め、別のワークフローを使用するには、現在のワークフロー タイトルの横にある [(ワークフローの切り替え)（(switch workflow)）] をクリックします。

ステップ 4 イベントが表示されず、ワークフローを時間によって制約できる場合は、時間範囲の調整が必要なことがあります（イベント時間の制約 （829 ページ）を参照）。

カスタム ワークフローの編集

カスタムワークフローを編集するには、管理者またはセキュリティアナリストの権限が必要です。

マルチドメイン展開では、現在のドメインで作成されたカスタムワークフローが表示されます。これは編集できます。先祖ドメインで作成されたカスタムワークフローも表示されますが、これは編集できません。下位のドメインのカスタムワークフローを表示および編集するには、そのドメインに切り替えます。

手順

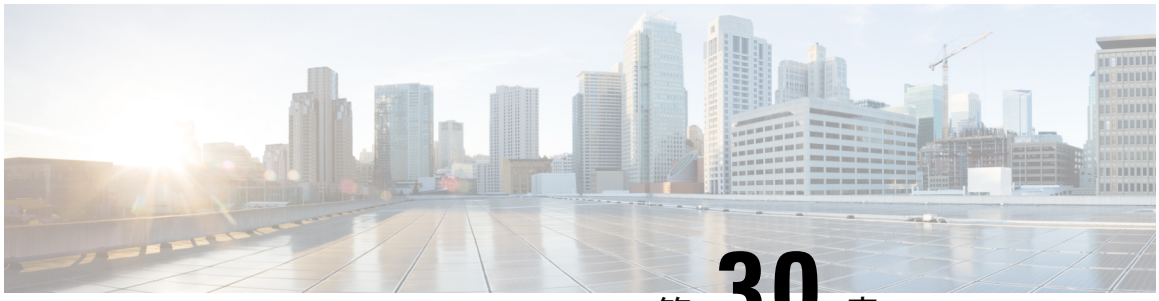
ステップ 1 **[分析（Analysis）]** > **[詳細（Advanced）]** > **[カスタムワークフロー（Custom Workflows）]** を選択します。

ステップ 2 編集するワークフロー名の隣にある**[編集（Edit）]**（  ）をクリックします。

代わりに [表示（View）]（  ） が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ワークフローに必要な変更を加えます。

ステップ 4 [保存（Save）] をクリックします。



第 30 章

カスタムテーブル

次のトピックでは、カスタム テーブルの使用方法について説明します。

カスタム テーブルの概要

システムがネットワークに関する情報を収集し、Management Center がその情報を一連のデータベーステーブルに保存します。結果として生成される情報を表示するためにワークフローを使用する場合、Management Center はそれらのテーブルのいずれかからデータを取り出します。たとえば、[カウント別のネットワーク アプリケーション（Network Applications by Count）] ワークフローの各ページのカラムは、[アプリケーション（Applications）] テーブルのフィールドから取得されます。

さまざまなテーブルのフィールドを結合することにより、ネットワークのアクティビティの分析が向上する場合、カスタム テーブルを作成できます。

定義済みのテーブルまたはカスタム テーブルのどちらについても、カスタム ワークフローを作成できます。

定義済みのカスタム テーブル

カスタム テーブルには、2 つまたは 3 つの定義済みテーブルのフィールドを含みます。システムは、いくつかのシステム定義のカスタムテーブルとともに配布されますが、特定のニーズに適合する情報のみを含む追加のカスタムテーブルを作成できます。

たとえば、システムは、侵入イベントとホストデータを相関するシステム定義のカスタムテーブルとともに配布されます。そのため、クリティカルシステムに影響を及ぼすイベントを検索でき、1 つのワークフローにその検索結果を表示できます。

マルチドメイン展開では、定義済みのカスタム テーブルは、グローバル ドメインに属し、下位ドメインで変更することはできません。

次の表では、システムと共に提供されるカスタム テーブルについて説明します。

表 *103*：システム定義カスタム テーブル

テーブル	説明
ホストとサーバー（Hosts with Servers）	ホスト テーブルおよびサーバー テーブルのフィールドを含み、ネットワーク上で実行されている検出されたアプリケーションに関する情報やこれらのアプリケーションを実行するホストに関する基本的なオペレーティング システム情報を提供します。

可能なテーブルの組み合わせ

カスタムテーブルを作成する場合、関連データのある定義済みのテーブルのフィールドを組み合わせことができます。次の表は、新しいカスタムテーブルを作成するために結合できる定義済みのテーブルをリストしています。2つ以上の定義済みのカスタムテーブルのフィールドを組み合わせるカスタム テーブルを作成できます。

表 *104*：カスタム テーブルの組み合わせ

組み合わせ可能なカスタム テーブル	以下のテーブルのフィールドと結合可能
アプリケーション	• 相関イベント（Correlation Events） • 侵入イベント • 接続のサマリーデータ（Connection Summary Data） • ホスト属性（Host Attributes） • アプリケーションの詳細（Application Details） • 検出イベント • ホスト（Hosts） • サーバー • 許可（Allow） イベントの一覧表示

組み合わせ可能なカスタムテーブル	以下のテーブルのフィールドと結合可能
相関イベント（Correlation Events）	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts）
侵入イベント	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts） • サーバー
接続のサマリーデータ（Connection Summary Data）	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts） • サーバー
ホストの侵害の兆候（Host Indications of Compromise）	• アプリケーション • アプリケーションの詳細（Application Details） • キャプチャファイル（Captured Files） • 接続のサマリーデータ（Connection Summary Data） • 相関イベント（Correlation Events） • 検出イベント • ホスト属性（Host Attributes） • ホスト（Hosts） • 侵入イベント • セキュリティインテリジェンスイベント（Security Intelligence Events） • サーバー • 許可（Allow）イベントの一覧表示

組み合わせ可能なカスタムテーブル	以下のテーブルのフィールドと結合可能
ホスト属性（Host Attributes）	• アプリケーション • 相関イベント（Correlation Events） • 侵入イベント • 接続のサマリーデータ（Connection Summary Data） • アプリケーションの詳細（Application Details） • 検出イベント • ホスト（Hosts） • サーバー • 許可（Allow） イベントの一覧表示
アプリケーションの詳細（Application Details）	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts）
検出イベント	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts）
セキュリティ インテリジェンス イベント（Security Intelligence Events）	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts） • サーバー

組み合わせ可能なカスタムテーブル	以下のテーブルのフィールドと結合可能
ホスト（Hosts）	• アプリケーション • 相関イベント（Correlation Events） • 侵入イベント • 接続のサマリーデータ（Connection Summary Data） • ホスト属性（Host Attributes） • アプリケーションの詳細（Application Details） • 検出イベント • サーバー • 許可（Allow）イベントの一覧表示
サーバー	• アプリケーション • 侵入イベント • 接続のサマリーデータ（Connection Summary Data） • ホスト属性（Host Attributes） • ホスト（Hosts）
許可（Allow）イベントの一覧表示	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts）

あるテーブルのフィールドが、別のテーブルの複数のフィールドにマップされる場合があります。

新しいカスタム テーブルを作成すると、テーブルのすべてのカラムを表示するデフォルトのワークフローが自動的に作成されます。定義済みのテーブルと同じように、ネットワーク分析で使用するデータをカスタムテーブルで検索することもできます。定義済みのテーブルを使用して可能であるように、カスタム テーブルに基づいてレポートを作成できます。

ユーザー定義のカスタム テーブル

ヒント　新しいカスタム テーブルを作成する代わりに、別の Management Center からカスタム テーブルをエクスポートし、Management Center にインポートすることができます。

カスタムテーブルを作成するには、どの定義済みテーブルに、カスタムテーブルに組み込むフィールドが含まれているかを判断します。その後、組み込むフィールドを選択できます。さらに、必要に応じて、共通フィールドのフィールド マッピングを設定することもできます。

ヒント　[ホスト（Hosts）] テーブルを含むデータでは、1 つの IP アドレスではなく、1 つのホストのすべての IP アドレスに関連したデータを表示できます。

例として、[相関イベント（Correlation Events）] テーブルと [ホスト（Hosts）] テーブルのフィールドを結合するカスタム テーブルについて考慮します。このカスタム テーブルを使用して、相関ポリシーの違反に関係するホストの詳細情報を取得できます。注意すべき点として、[相関イベント（Correlation Events）] テーブルの送信元 IP アドレスと宛先 IP アドレスのどちらと一致する [ホスト（Hosts）] テーブル データを表示するかを決定する必要があります。

このカスタム テーブルのイベントのテーブル ビューを表示する場合、相関イベントが 1 行に 1 つずつ表示されます。次の情報を含むようにカスタム テーブルを設定できます。

- イベントが生成された日時
- 違反された相関ポリシーの名前
- 違反をトリガーとして使用した規則の名前
- 相関イベントに関係する送信元ホスト（開始ホスト）に関連付けられた IP アドレス
- 送信元ホストの NetBIOS 名
- 送信元ホストが実行しているオペレーティング システムおよびバージョン
- 送信元ホストのシビラティ（重大度）

ヒント　宛先ホスト（応答ホスト）の同じ情報を表示する同様のカスタムテーブルを作成することもできます。

カスタム テーブルの作成

手順

ステップ 1 **[分析（Analysis）] > [詳細（Advanced）] > [カスタムテーブル（Custom Tables）]**を選択します。

ステップ 2 [カスタム テーブルの作成（Create Custom Table）] をクリックします。

ステップ 3 [名前（Name）] フィールドに、カスタム テーブルの名前を入力します。

例：

たとえば、`Correlation Events with Host Information（Src IP）`と入力します。

ステップ 4 [テーブル（Tables）] ドロップダウン リストから、[相関イベント（Correlation Events）] を選択します。

ステップ 5 [フィールド（Fields）] で [時間（Time）] を選択し、[追加（Add）] をクリックして、相関イベントが生成された日時を追加します。

ステップ 6 手順 5 を繰り返して、[ポリシー（Policy）]および[ルール（Rule）] フィールドを追加します。

ヒント Ctrl または Shift を押しながらクリックすることにより、複数のフィールドを選択できます。また、クリックしてドラッグすることで、隣接する複数の値を選択できます。ただし、テーブルに関連したイベントのテーブル ビューでフィールドが表示される順序を指定する場合は、フィールドを一度に 1 つずつ追加します。

ステップ 7 [テーブル（Tables）] ドロップダウンリストから [ホスト（Hosts）] を選択します。

ステップ 8 [IP アドレス（IP Address）]、[NetBIOS 名（NetBIOS Name）]、[OS 名（OS Name）]、[OS バージョン（OS Version）]、[ホストのシビラティ（重大度）（Host Criticality）] フィールドをカスタム テーブルに追加します。

ステップ 9 [相関イベント（Correlation Events）] の隣にある [共通フィールド（Common Fields）] で、[送信元 IP（Source IP）] を選択します。

相関イベントに関係する送信元ホスト（開始ホスト）用に手順 8 で選択したホスト情報を表示するように、カスタム テーブルが設定されます。

ヒント 相関イベントに関係する宛先ホスト（応答ホスト）に関する詳細なホスト情報を表示するカスタム テーブルを作成する場合も、この手順に従いますが、[送信元 IP（Source IP）] ではなく、[送信先 IP（Destination IP）] を選択します。

ステップ 10 [保存（Save）] をクリックします。

カスタム テーブルの変更

マルチドメイン展開では、現在のドメインで作成されたカスタムテーブルが表示されます。これは編集できます。先祖ドメインで作成されたカスタムテーブルも表示されますが、これは編

集できません。下位のドメインのカスタムテーブルを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[分析（Analysis）]** > **[詳細（Advanced）]** > **[カスタムテーブル（Custom Tables）]** を選択します。

ステップ 2 編集するテーブルの横にある**[編集（Edit）]**（）をクリックします。

代わりに [表示（View）]（） が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 削除するフィールドの横にある[削除（Delete）]（）をクリックして、テーブルからフィールドを削除することもできます。

（注） レポートで現在使用中のフィールドを削除すると、それらのフィールドを使用しているセクションをそれらのレポートから削除するか確認するプロンプトが表示されます。

ステップ 4 必要に応じて、その他の変更を実行します。

ステップ 5 [保存（Save）] をクリックします。

カスタム テーブルの削除

マルチドメイン導入では、現在のドメインで作成されたカスタムテーブルが表示されます。これは削除できます。先祖ドメインで作成されたカスタムテーブルも表示されますが、これは削除できません。下位のドメインのカスタムテーブルを削除するには、そのドメインに切り替えます。

手順

ステップ 1 **[分析（Analysis）]** > **[詳細（Advanced）]** > **[カスタムテーブル（Custom Tables）]**を選択します。

ステップ 2 削除するカスタムテーブルの隣にある[削除（Delete）]（）をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

カスタム テーブルに基づくワークフローの表示

カスタムテーブルを作成すると、そのデフォルトのワークフローがシステムによって自動的に作成されます。このワークフローの最初のページには、イベントのテーブル ビューが表示されます。カスタム テーブルに侵入イベントを含める場合、ワークフローの 2 番目のページはパケット ビューになります。それ以外の場合、ワークフローの 2 番目のページはホスト ページになります。カスタム テーブルに基づいて、独自のカスタム ワークフローを作成することもできます。

ヒント カスタム テーブルに基づいてカスタム ワークフローを作成する場合、それをそのテーブルのデフォルトのワークフローとして指定できます。

同じ手法を使用して、定義済みのテーブルに基づいたイベント ビューに使用するカスタムテーブルでイベントを表示できます。

マルチドメイン展開では、現在のドメインで作成されたカスタムテーブルが表示されます。これは編集できます。先祖ドメインで作成されたカスタムテーブルも表示されますが、これは編集できません。下位のドメインのカスタムテーブルを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[分析（Analysis）] > [詳細（Advanced）] > [カスタムテーブル（Custom Tables）]**を選択します。

ステップ 2 表示するワークフローに関連するカスタムテーブルの隣にある [表示（View）]（👁）をクリックします。

カスタム テーブルの検索

マルチドメイン展開では、現在のドメインで作成されたカスタムテーブルが表示されます。これは編集できます。先祖ドメインで作成されたカスタムテーブルも表示されますが、これは編集できません。下位のドメインのカスタムテーブルを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[分析（Analysis）] > [詳細（Advanced）] > [カスタムテーブル（Custom Tables）]** を選択します。

ステップ 2 検索するカスタムテーブルの隣にある[表示（View）]（👁）をクリックします。

ヒント カスタムワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [（ワークフローの切り替え）（(switch workflow)）] をクリックします。

ステップ 3 [検索（Search）] をクリックします。

ヒント 別の種類のイベントやデータについてデータベースを検索する場合は、その種類をテーブル ドロップダウンリストから選択します。

ステップ 4 該当するフィールドに、検索条件を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。

ヒント 検索基準としてオブジェクトを使用する場合は、検索フィールドの横にある**[オブジェクト（Object）]**（+）をクリックします。

ステップ 5 必要に応じて、検索を保存する場合は、[プライベート（Private）] チェックボックスをオンにして、プライベートとして検索を保存すると、その検索に本人のみがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント カスタムユーザー ロールのデータの制限として検索を使用する場合は、必ずプライベート検索として保存する**必要**があります。

ステップ 6 必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [保存（Save）] をクリックして、検索条件を保存します。[プライベート（Private）] チェックボックスをオンにすると、その検索は本人のアカウントでのみ表示できるようになります。
- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[新規に保存（Save As New）] をクリックします。[プライベート（Private）] チェックボックスをオンにすると、その検索は本人のアカウントでのみ保存および表示できるようになります。

ステップ 7 [検索（Search）] をクリックして、検索を開始します。

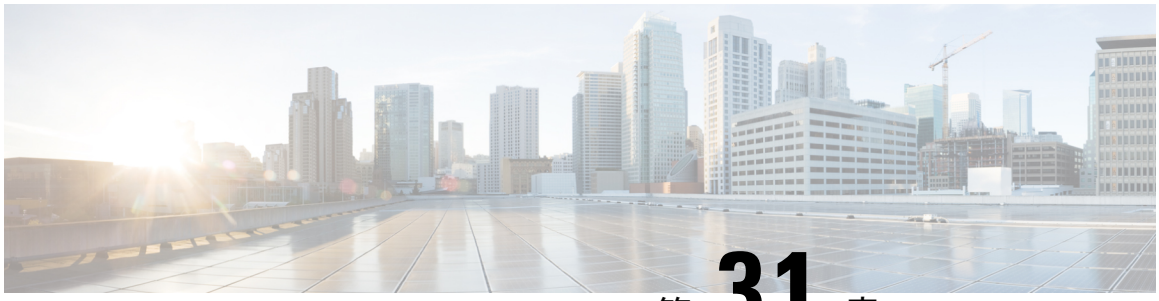
検索結果は、現在の時間範囲によって制限されている、カスタムテーブルのデフォルトのワークフローに表示されます（該当する場合）。

カスタムテーブルの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
カスタムテーブルの接続イベントのサポートが削除されました	6.6	任意（Any）	接続イベントを含むカスタムテーブルを作成することはできなくなりました。 バージョン 6.6 にアップグレードした場合、接続イベントを持つ既存のテーブルは廃止としてリストされ、データは表示されず、エクスポートまたは編集することはできません。既存のレポート、カスタムワークフロー、およびダッシュボードには廃止されたテーブルが含まれる場合があり、それらを確認することができます。 変更された画面：[Analysis] > [Advanced] > [Custom Tables] と、カスタムテーブルを追加または編集するためのページ。 影響を受けるプラットフォーム：Management Center

第 VIII 部

イベントとアセット



第 31 章

接続ロギング

次のトピックでは、モニター対象ネットワークでホストから実行される接続を記録するようにシステムを設定する方法について説明します。

接続ロギングについて

システムは管理対象デバイスで検出された接続のログを生成できます。このログは接続イベントと呼ばれます。ルールやポリシーの設定を行うことで、ログに記録する接続の種類、接続をログに記録するタイミング、およびデータを保存する場所をきめ細かく制御できます。セキュリティ関連の接続イベントと呼ばれる特別な接続イベントは、レピュテーションベースのセキュリティ インテリジェンス機能によってブロックされた接続を表します。

接続イベントには、検出されたセッションに関するデータも含まれています。個々の接続イベントで入手可能な情報はいくつかの要因に応じて異なりますが、一般的には次のものがあります。

- タイムスタンプ、送信元と宛先の IP アドレス、入出力ゾーン、接続を処理したデバイスなど、基本的な接続特性
- アプリケーション、要求されるURL、または接続に関連付けられているユーザなど、システムによって検出または推測される追加の接続特性
- どの設定がトラフィックを処理したか、接続が許可またはブロックされていたかどうか、暗号化された接続および復号された接続に関する詳細など、接続がログに記録された理由に関するメタデータ

部門のセキュリティ上およびコンプライアンス上の要件に従って接続をロギングしてください。接続ロギングを設定する際は、システムはさまざまな理由で接続をロギングすることがあり、1ヵ所でロギングを無効にしても一致する接続がログに記録されなくなるとは限りません。

接続イベント内の情報は、トラフィックの特性、最終的に接続を処理した設定など、いくつかの要因によって異なります。

（注） エクスポートしたNetFlowレコードから生成された接続データを使い、管理対象デバイスで収集された接続ログを補うことができます。これは、管理対象デバイスでモニターできないネットワーク上にNetFlow対応ルータやその他のデバイスを配置した場合に特に有効です。

常にログに記録される接続

接続イベントのストレージを無効にしない限り、システムは他のロギング設定に関係なく、Management Centerデータベースに次の接続終了イベントを保存します。

侵入に関連付けられた接続

システムは、接続がアクセス コントロール ポリシーのデフォルトのアクションで処理される限り、侵入イベントに関連付けられている接続を自動的に記録します。

アクセス コントロールのデフォルト アクションに関連付けられた侵入ポリシーによって侵入イベントが生成された場合、システムは、そのイベントに関連する接続の終了を自動的にログに記録しません。代わりに、デフォルトのアクション接続のロギングを明示的に有効にする必要があります。これは、接続データをログに記録する必要がない、侵入防御専用の展開環境で役立ちます。

ただし、デフォルトアクションで接続開始ロギングを有効にした場合、接続開始のロギングに加えて、関連する侵入ポリシーがトリガーしたときにシステムによって接続終了がログに記録されます。

ファイル イベントとマルウェア イベントに関連付けられた接続

システムは、ファイル イベントとマルウェア イベントに関連付けられた接続を自動的にログに記録します。

（注） NetBIOS-SSN（SMB）トラフィックのインスペクションによって生成されるファイルイベントは、即座には接続イベントを生成しません。これは、クライアントとサーバーが持続的接続を確立するためです。システムはクライアントまたはサーバーがセッションを終了した後に接続イベントを生成します。

インテリジェント アプリケーション バイパスに関連付けられた接続

システムは、IABに関連付けられたバイパスされた、およびバイパスされるはずだった接続をログに記録します。

モニタ対象の接続

システムは常に、モニタの対象のトラフィックの接続終了をロギングします。このことは、トラフィックに一致する他のルールがなく、デフォルトアクションのロギングを有効にしていない場合でも該当します。詳細については、モニターされた監視接続のロギング （882 ページ）を参照してください。

ログ可能なその他の接続

重要な接続のみがロギングされるように、ルールごとの接続ロギングを有効にします。あるルールに対し接続ロギングを有効にすると、システムはそのルールによって処理されたすべての接続をロギングします。

また、ポリシーのデフォルト アクションにより処理された接続をロギングすることもできます。ルールやデフォルトアクションにより（アクセス制御の場合は、ルールのインスペクション設定により）、ロギングのオプションは異なります。

プレフィルタ ポリシー：ルールとデフォルト アクション

プレフィルタ ポリシーによりファースト パスまたはブロックする接続（すべてのプレーン テキスト、パススルー トンネルを含む）をロギングすることができます。

プレフィルタは、外部ヘッダーを基準にしてトラフィックを処理します。ロギングするトンネルでは、結果の接続イベントには、外部のカプセル化ヘッダー情報が含まれます。

継続分析の対象となるトラフィックについては、一致する接続が他の設定によってロギングされることがあるかもしれませんが、プレフィルタ ポリシーによるロギングは無効となります。システムは内部ヘッダーを使ってすべての継続分析を行います。つまり、システムは、許可されたトンネル内の各接続を個別に処理、ロギングします。

復号ポリシー：ルールとデフォルトアクション

復号ルールまたは復号ポリシーのデフォルトアクションに一致する接続をロギングすることができます。

ブロックされた接続の場合、システムは即座にセッションを終了し、イベントを生成します。監視対象の接続やアクセス コントロール ルールに渡す接続の場合、システムはセッションが終了するとイベントを生成します。

アクセス コントロール ポリシー：セキュリティ インテリジェンスによる判断

接続がレピュテーションベースのセキュリティインテリジェンス機能によってブロックされる場合は、その接続をログに記録できます。

オプションで、セキュリティ インテリジェンス フィルタリングにはモニター専用設定を使用できます。パッシブ展開環境では、この設定が推奨されます。この設定では、セキュリティインテリジェンスによってブロックされるはずの接続をシステムがさらに分析できるだけでなく、一致する接続をログに記録することもできます。セキュリティ インテリジェンス モニタリングによって、セキュリティ インテリジェンス情報を使用してトラフィック プロファイルを作成することもできます。

セキュリティ インテリジェンスのフィルタリングの結果、システムが接続イベントをロギングすると、一致するセキュリティ インテリジェンス イベントもロギングされます。そのイベントは特殊なタイプの接続イベントで、個別に表示および分析することができ、また個別に保存、プルーニングされます。一致する IP アドレスが接続にあるかどうかを識別できるように、[分析（Analysis）] > [接続（Connections）] メニューのページの表では、ブロックされ、モニターされている IP アドレスの横のホストアイコンは見た目が少し異なります。

アクセス コントロール ポリシー：ルールとデフォルト アクション

アクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに一致する接続をロギングすることができます。

関連トピック

ルールとポリシーのアクションによるロギングへの影響 （882 ページ）

ルールとポリシーのアクションによるロギングへの影響

接続イベントには、接続がロギングされた理由を記述したメタデータが含まれています。メタデータにはトラフィックがどの設定によって処理されたかなどの情報が含まれます。接続ロギングを設定する場合、ルール アクションおよびポリシーのデフォルト アクションにより、一致するトラフィックをシステムがどのように検査、処理するのかだけでなく、一致するトラフィックの詳細をいつ、どのようにロギングするかが決まります。

関連トピック

接続およびセキュリティ関連の接続イベントフィールド （902 ページ）

FastPath された接続のロギング

FastPath された接続や非暗号化トンネルをロギングできます。ロギングには、プレフィルタ ポリシーの以下のルールとアクションに一致するトラフィックを含めることができます。

- トンネル ルール：[ファストパス（FastPath）] アクション（外部セッションをロギングします）
- プレフィルタ ルール：[ファストパス（FastPath）] アクション

FastPath されたトラフィックはアクセス コントロールと QoS の残りをバイパスするため、FastPath された接続の接続イベントに含まれる情報は限られます。

モニターされた監視接続のロギング

システムは常に、以下の設定と一致するトラフィックの接続終了をロギングします。このことは、トラフィックに一致する他のルールがなく、デフォルトアクションのロギングを有効にしていない場合でも該当します。

- セキュリティ インテリジェンス：モニターするように設定されたブロックリスト（セキュリティ インテリジェンス イベントも生成されます）
- SSL ルール：[モニター（Monitor）] アクション

- アクセス コントロール ルール：[モニタ（Monitor）] アクション

システムは、1 つの接続が 1 つのモニタ ルールに一致するたびに 1 つの別個のイベントを生成するわけではありません。1 つの接続が複数のモニタ ルールに一致する可能性があるため、各接続イベントには、接続が一致する最初の 8 つのモニタ アクセス コントロール ルールに関する情報だけでなく、最初の一致する SSL モニタ ルールに関する情報を含めて表示することができます。

同様に、外部 syslog または SNMP トラップ サーバーに接続イベントを送る場合、システムは 1 つの接続が 1 つのモニター ルールに一致するたびに 1 つの別個のアラートを送信するわけではありません。代わりに、接続の終了時にシステムから送られるアラートに、接続が一致したモニター ルールの情報が含まれます。

信頼されている接続のロギング

信頼されている接続の開始と終了をロギングできます。ロギングには、以下のルールとアクションに一致するトラフィックを含めることができます。

- アクセス コントロール ルール：[信頼する（Trust）] アクション
- アクセス コントロールのデフォルト アクション：[すべてのトラフィックを信頼する（Trust All Traffic）]

（注） 信頼できる接続を記録することはできますが、これはお勧めしません。信頼できる接続はディープインスペクションまたは検出の対象ではないため、信頼できる接続の接続イベントに含まれる情報は限定的であるためです。

信頼ルールによって最初のパケットで検出された TCP 接続は、接続終了イベントだけを生成します。システムは、最後のセッション パケットの 1 時間後にイベントを生成します。

ブロックされた接続のロギング

ブロックされた接続をロギングできます。ロギングには、以下のルールとアクションに一致するトラフィックを含めることができます。

- トンネル ルール：[ブロック（Block）]
- プレフィルタ ルール：[ブロック（Block）]
- プレフィルタのデフォルト アクション：[すべてのトンネル トラフィックをブロック（Block all tunnel traffic）]
- セキュリティ インテリジェンス：モニターするように設定されていないブロックリスト（セキュリティ インテリジェンス イベントも生成されます）
- 復号ルール：[ブロック（Block）] および [リセットしてブロック（Block with reset）]

- SSL のデフォルトアクション：[ブロック（Block）]および[リセットしてブロック（Block with reset）]
- アクセス コントロール ルール：[ブロック（Block）]、[リセットしてブロック（Block with reset）]、[インタラクティブ ブロック（Interactive Block）]
- アクセス コントロールのデフォルトアクション：[すべてのトラフィックをブロック（Block All Traffic）]

トラフィックをブロックできるデバイスは、インライン（つまり、ルーテッドインターフェイス、スイッチド インターフェイス、トランスペアレント インターフェイス、インライン インターフェイスのペア）で展開されているもののみです。ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

⚠

注意 サービス妨害（DoS）攻撃の間にブロックされた TCP 接続をロギングすると、システム パフォーマンスに影響し、複数の同様のイベントによってデータベースが過負荷になる可能性があります。ブロック ルールにロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたは DoS 攻撃を受けやすい他のインターフェイス上のトラフィックをモニタするかどうかを検討します。

ブロックされた接続の接続開始ロギングと接続終了ロギングとの比較

ブロックされた接続をロギングするときは、システムがその接続をどのようにロギングするかは接続がブロックされた理由によって異なります。これは、接続ログに基づいて相関ルールを設定する際に留意しておくことが重要です。

- 暗号化されたトラフィックをブロックする復号ルールおよび復号ポリシーのデフォルトアクションの場合、システムは接続**終了**イベントをロギングします。これは、システムが接続がセッション内で最初のパケットを使用して暗号化されているかどうかを決定できないためです。
- 他のブロッキング アクションについては、システムは接続**開始**イベントをロギングします。一致するトラフィックは、追加のインスペクションなしで拒否されます。

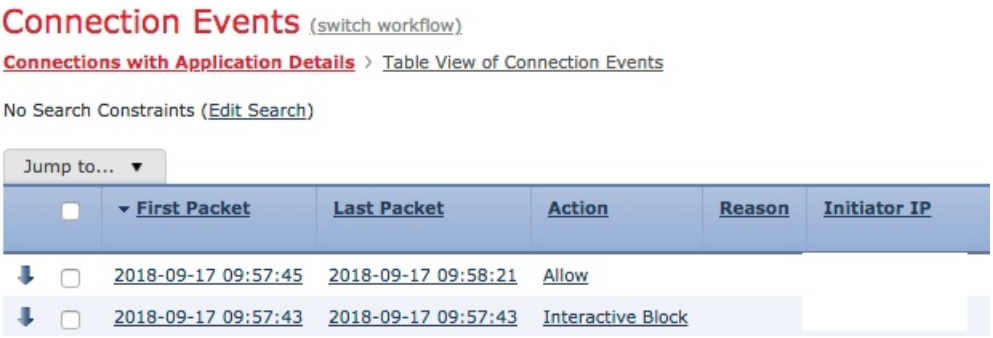
バイパスされるインタラクティブ ブロックのロギング

インタラクティブ ブロッキング アクセス コントロール ルール（このルールではユーザが禁止されている Web サイトを参照するとシステムによって警告ページが表示されます）を使用すると、接続終了ロギングを設定できます。その理由は、警告ページをユーザーがクリック スルーすると、その接続は新規の、許可された接続と見なされ、システムによってモニターとロギングができるためです。

したがって、[インタラクティブ ブロック（Interactive Block）] ルールまたは [リセットしてインタラクティブ ブロック（Interactive Block with reset）] ルールにパケットが一致する場合、システムは以下の接続イベントを生成できます。

- ユーザーの要求が最初にブロックされ警告ページが表示されたときの接続開始イベント。このイベントにはアクション [インタラクティブ ブロック（Interactive Block）] または [リセットしてインタラクティブ ブロック（Interactive Block with Reset）] が関連付けられます。
- 複数の接続開始または終了イベント（ユーザーが警告ページをクリック スルーし、要求した最初のページをロードした場合）。これらのイベントには [許可（Allow）] アクションおよび理由 [ユーザー バイパス（User Bypass）] が関連付けられます。

次の図に、許可を受けたインタラクティブ ブロックの例を示します。



許可された接続のロギング

許可された接続をロギングができます。ロギングには、以下のルールとアクションに一致するトラフィックを含めることができます。

- SSL ルール：[複合（Decrypt）] アクション
- SSL ルール：[複合しない（Do not decrypt）] アクション
- SSL のデフォルト アクション：[複合しない（Do not decrypt）] アクション
- アクセス コントロール ルール：[許可（Allow）] アクション
- アクセス コントロールのデフォルト アクション：[ネットワーク検出のみ（Network Discovery Only）] および任意の侵入防御オプション

これらの設定に対するロギングを有効にすると、接続が確実にロギングされると同時に、インスペクションおよびトラフィック処理の次のフェーズが許可（または指定）されます。SSL ロギングは常に接続終了ロギングですが、アクセス コントロール設定で接続開始ロギングも可能にすることができます。

トンネルおよびプレフィルタ ルールでの [分析（Analyze）] アクションを使用してアクセス コントロールで接続を続行することもできますが、このアクションを使用するルールではロギングが無効にされます。ただし、他の設定を使用して、一致する接続をロギングすることもできます。許可されたトンネルのカプセル化されたセッションは、個別に評価されてロギングされます。

アクセス コントロール ルールまたはデフォルト アクションでトラフィックを許可する場合、関連する侵入ポリシーを使用してトラフィックをさらに検査し、侵入をブロックすることがで

きます。アクセスコントロールルールでは、ファイルポリシーを使用して、マルウェアを含む禁止されたファイルを検出し、ブロックすることもできます。接続イベントストレージを無効にしない限り、システムは、侵入イベント、ファイル イベント、マルウェア イベントに関連する許可された接続のほとんどを自動的にロギングします。詳細については、常にログに記録される接続 （880 ページ）を参照してください。

ペイロードが暗号化される接続には、ディープインスペクションは適用されません。したがって、暗号化接続の接続イベントに含まれる情報は限定されます。

許可された接続のファイルおよびマルウェア イベントのロギング

ファイル ポリシーによってファイルが検出またはブロックされると、以下のいずれかのイベントが Management Center データベースにロギングされます。

- ファイル イベント：検出またはブロックされたファイル（マルウェア ファイルを含む）を表します。
- マルウェア イベント：検出されたまたはブロックされたマルウェア ファイルのみを表します。
- レトロスペクティブ マルウェア イベント：以前に検出されたファイルでのマルウェア処理が変化した場合に生成されます。

このロギングは、アクセス コントロール ルールごとに無効にすることができます。ファイル イベントおよびマルウェア イベント ストレージを完全に無効にすることもできます。

（注） ファイル イベントおよびマルウェア イベントのロギングは有効のままにすることを推奨しています。

接続開始のロギングと終了のロギングの比較

接続は、次の例外となるブロックされたトラフィックを除き、接続開始時あるいは終了時にログを記録することができます。

- ブロックされたトラフィック：ブロックされたトラフィックは、さらに検査されることなくすぐさま拒否されるため、通常、ブロックされたトラフィックについては、接続開始イベントのみ記録可能です。ログに記録される個々の接続終了はありません。
- ブロックされた暗号化トラフィック：復号ポリシーで接続のロギングを有効にすると、システムは接続開始イベントではなく接続終了イベントをログに記録します。これは、システムは接続がセッション内で最初のパケットを使用して暗号化されているかどうかを判定できず、暗号化されたセッションを即座にブロックできないためです。

パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。何らかの理由で接続をモニタリングすると、接続終了ロギングが強制されま

す。単一のブロックされていない接続の場合、接続終了イベントには、接続開始イベントに含まれるすべての情報に加えて、セッション期間中に収集された情報も含まれます。

次の表では、接続開始イベントと接続終了イベントの違い（それぞれをロギングする利点を含む）を詳細に説明します。

表 *105*：接続開始イベントと接続終了イベントの比較

	接続開始イベント	接続終了イベント
次の場合に生成可能です	システムが接続の開始を検出した場合（または、イベントの生成がアプリケーションまたはURLの識別に依存する場合は最初の数パケットの後）。	システムが以下の状態の場合 • 接続のクローズを検出した場合。 • 一定期間後に接続の終了を検出しない場合。 • メモリ制約によりセッションを追跡できなくなった場合。
次のものについてロギングが可能です	復号ポリシーによってブロックされた接続を除くすべての接続。	ほとんどの接続。
次を含みます	最初のパケット（または、イベントの生成がアプリケーションまたはURLの識別に依存する場合は最初の数パケット）で判定できる情報のみ。	接続開始イベント内のすべての情報と、セッション期間を通してトラフィックを検査して判別された情報（たとえば伝送されたデータ総量、接続の最後のパケットのタイムスタンプなど）。 （注） 接続イベントでは、脅威防御が接続のSnort判定を返した後に、または接続を高速パス処理した場合に、送信されたデータの量がカウントされません。

	接続開始イベント	接続終了イベント
次の場合に有用です	ログに記録する場合： • ブロックされている接続。 • 接続終了情報はユーザーにとって重要ではないので、接続の開始のみ。	目的 • 復号ポリシーによって処理される暗号化接続をロギングする場合。 • セッションの期間にわたって収集された情報であらゆる種類の詳細な分析を実行する場合、またはその情報を使用して相関ルールをトリガーする場合。 • カスタムワークフローで接続の概要（集約接続データ）を表示する場合、グラフ形式で接続データを表示する場合、またはトラフィックプロファイルを作成して使用する場合。

Secure Firewall Management Center と外部ロギング

接続およびセキュリティ インテリジェンス イベント ログを Management Center に保存する場合、システムのレポート、分析、およびデータ相関機能を使用することができます。次に例を示します。

- ダッシュボードおよびコンテキストエクスプローラでは、システムによってロギングされた接続をグラフ形式によって一目で確認できます。
- イベント ビュー（ほとんどのオプションは分析メニューで利用可能）には、システムが記録した接続に関する詳細情報が表示されます。これらの情報はグラフまたは表形式で表示したり、レポートにまとめたりすることもできます。
- トラフィック プロファイリングは、接続データを使用して正常なネットワーク トラフィックのプロファイルを作成します。ユーザーはそのプロファイルを基準として使用して、異常な動作を検出および追跡できます。
- 相関ポリシーを使用して、イベントを生成し、特定のタイプの接続またはトラフィック プロファイルの変更に対する応答（アラートや外部修復など）をトリガーできます。

Management Center に保存できるイベントの数はモデルによって異なります。

（注） これらの機能を使用するには、接続（ほとんどの場合、接続の開始ではなく接続の終了）をロギングする**必要があります**。システムがクリティカルな接続（ログに記録された侵入、禁止されたファイルおよびマルウェアに関連付けられているもの）を自動的にロギングするのはこのためです。

次を使用して、外部の syslog、SNMP トラップサーバー、またはその他の外部ツールにイベントを記録することもできます。

- 任意のデバイスでの外部ロギングの場合：

  設定する接続は、アラート応答と呼ばれます。

- Threat Defense デバイスでの外部ロギングの場合：

  Cisco Secure Firewall Management Center デバイス構成ガイドの「*About Configuring Syslog*」および「*Configure SNMP Traps*」を参照してください。

- 外部ロギングに関連するその他のオプションの場合：

  外部ツールを使用したイベントの分析 （753 ページ） を参照してください。

関連トピック

Secure Firewall Management Center アラート応答 （673 ページ）

接続ロギングの制限事項

以下はロギングできません。

- カプセル化された接続がアクセス制御によって検査されるプレーンテキスト、パススルートンネルの外部セッション
- 3 ウェイ ハンドシェイクが完了していない場合は TCP 接続。

  Firepower の展開環境に対するサービス拒否攻撃の機会を提供することになるため、これらの接続はログに記録されません。

  ただし、次の回避策を使用して失敗した接続をモニターまたはデバッグできます。

  - コマンドライン インターフェイスで **show asp drops** コマンドを使用します。
  - パケットキャプチャ機能を使用してこれらの接続に関する詳細情報を取得します。パケット キャプチャの概要 （540 ページ）およびサブトピックを参照してください。

接続イベントに必要と思われる情報が含まれていない場合は、接続イベントフィールドの入力の要件 （926 ページ）と接続イベントフィールドで利用可能な情報 （928 ページ）を参照してください。

イベント ビューアにイベントが表示された場合

次のポイントは、すべてのタイプのイベントに適用されます。

- [分析 (Analysis)] メニューの下にあるページを見ている場合は、ページを更新して新しいイベントを表示する必要があります。
- 通常、イベントは、トラフィックが検出されてから数秒以内に表示されます。ただし、トラフィックが非常に多い状態、Management Center が低帯域幅のネットワーク上で多数の

デバイスを管理している状況、またはイベントのバックアップなどのイベント処理が一時停止される操作が進行中である状況などでは、任意の遅延が生じることがあります。

- 定義されたルールに従って記録されたすべての接続イベントが、イベントビューアに表示されます。イベントをフィルタするオプションは、接続イベントの統合ロギングには使用できません。

接続のロギングのベスト プラクティス

次のベスト プラクティスを使用して、記録が必要な接続のみを記録するようにします。

重要な接続のみが記録されるように、アクセス制御ルールごとの接続ロギングを有効にします。

常に記録する接続

システムは次について自動的に記録します。

- 検出されたファイル、マルウェア、侵入、およびインテリジェント アプリケーション バイパス（IAB）に関連付けられている一部の接続。

  詳細については、常にログに記録される接続 （880 ページ）を参照してください。

- モニター対象の接続。

  詳細については、モニターされた監視接続のロギング （882 ページ）を参照してください。

記録されることがない接続

次についてはロギングを有効にしないでください。

- 信頼アクションがあるアクセス制御ルール

  信頼されている接続には、ディープインスペクションまたはディスカバリは適用されません。したがって、信頼されている接続の接続イベントに含まれる情報は限られます。

- パッシブ展開のブロック ルールについてはロギングを有効にしないでください。デバイスがインラインで展開された場合にシステムがブロックする接続を記録するには、ブロック ルールではなく、モニター ルールを使用します。

  トラフィックをブロックできるデバイスは、インライン（つまり、ルーテッド インターフェイス、スイッチド インターフェイス、トランスペアレント インターフェイス、インラインインターフェイスのペア）で展開されているもののみです。ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

- 対象外のトラフィック。次に例を示します。
  - 信頼されている DNS ホストへの DNS 要求などの特定の許可トラフィック。
  - サービス提供に関係のないインフラストラクチャ トラフィック。

（前述のように、この場合もこのトラフィックの脅威はモニターできます。）

常にログに記録される接続（880ページ）で説明したように、前述のロギングを無効にした場合も、侵入イベント、マルウェア、および IAB は記録されます。

どこかで記録されているものの記録の回避

別のデバイスまたはサービスがネットワークセグメントの接続データを記録している場合は、Management Center 内のそのセグメントのデータのロギングを無効にします。次に例を示します。

- Management Center と同じネットワークセグメント上の接続イベントをルータが記録している場合、相関ポリシーやトラフィックプロファイルなど何らかの目的で接続イベントが必要な場合を除き、Management Center 上での同じ接続を記録することは避けてください。

  相関ポリシーの詳細については、相関ポリシーとルールの概要（1189ページ）を参照してください。トラフィック プロファイルの詳細については、トラフィック プロファイルの概要（1235 ページ）を参照してください。

- Secure Network Analytics を使用してスイッチやルータから報告された NetFlow レコードを利用して潜在的な動作の異常や疑わしいトラフィックパターンを特定している場合、それらのセグメントをモニターしているルールの接続ロギングを無効することができます。その代りに、ネットワークのそれらの部分については Secure Network Analytics の動作分析に依存します。

  詳細については、Secure Network Analytics のドキュメントを参照してください。

接続の開始または終了のいずれか（両方ではない）のロギング

接続の開始と終了のロギングを選択できる場合は、接続終了時のロギングを有効にします。これは、接続終了時は接続開始イベントからの情報と、セッション中に収集された情報が記録されるからです。

ブロックされた接続を記録するか、または接続終了の情報に関心がない場合にのみ、接続の開始を記録します。

詳細については、接続開始のロギングと終了のロギングの比較（886ページ）を参照してください。

ブロックされたトラフィックのロギング

ブロックされたトラフィックは、それ以上調査されることなくすぐに拒否されるため、通常は接続開始イベントのみを記録できます。

詳細については、ブロックされた接続のロギング（883 ページ）を参照してください。

外部の場所へのイベントのロギング

会社のセキュリティポリシーで許可されている場合は、次のいずれかを使用して外部ソースにログをストリーミングすることで Management Center のディスク容量を節約できます。

- eStreamer は、Management Center あるいはからカスタム展開したクライアントアプリケーションへのログのストリーミングを可能にします。詳細については、『*Firepower eStreamer Integration Guide*』を参照してください。
- アラート応答と呼ばれている syslog または SNMP トラップ。詳細については、Secure Firewall Management Center アラート応答 （673 ページ）を参照してください。

イベント レコードの最大数を指定します。

データベースに保存できるレコードの最小数と最大数を考慮します。たとえば、デフォルトでは、仮想 Management Center は 1,000 万のイベントを保存できますが、イベントの最大数は 5,000 万です。**[システム（System）] > [設定（Configuration）] > [データベース（Database）]** に移動してニーズに合ったサイズに調整します。

Management Center のすべてのモデルとそれらのイベントデータベースのサイズのリストについては、データベース イベント数の制限 （66 ページ） を参照してください。

接続イベントに表示される内容を制御します。

接続イベントに表示される行数を指定するには、Management Center の右上にある自分のユーザー名をクリックし、**[ユーザー設定（User Preferences）] > [イベント表示設定（Event View Settings）]** をクリックします。設定可能なイベント数は 1 ページあたり最大で 1,000 です。

接続イベント レポートのセットアップ

接続イベントを見逃していないことを確認するには、.csv 形式の自動レポートをセットアップし、必要に応じて定期的に実行されるようにスケジュールを設定することができます。詳細については、次のトピックを参照してください。

- レポートデザイナを使用します（**[分析（Analysis）] > [接続（Connection）] > [イベント（Events）] > [レポートデザイナ（Report Designer）]**）。レポートの設計について （642 ページ）
- タスクのスケジュールを設定します（**[システム（System）] > [ツール（Tools）] > [スケジュール（Scheduling）]**）。タスクのスケジューリングについて （597 ページ）

接続ロギングの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

接続ロギングの設定

以降の項では、さまざまなルールと条件に一致する接続ロギングのセットアップ方法について説明します。

トンネル ルールおよびプレフィルタ ルールによる接続のロギング

プレフィルターポリシーは Secure Firewall Threat Defense デバイスにのみ適用されます。

始める前に

- ルール アクションを [ブロック（Block）] または [ファストパス（Fastpath）] に設定します。[分析（Analyze）]アクションのロギングは無効にします。これにより、接続のアクセス制御が引き続き可能になり、接続の処理とロギングは別の設定で決定されます。
- ロギングは、カプセル化フローではなく、内部フローで実行されます。

手順

ステップ 1 プレフィルタ ポリシー エディタで、ロギングを設定するルールの横にある **[編集（Edit）]**（） をクリックします。

代わりに [表示（View）]（） が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 2 [ロギング（Logging）] をクリックします。

ステップ 3 [接続の開始時にロギングする（Log at Beginning of Connection）] または [接続の終了時にロギングする（Log at End of Connection）] を指定します。

パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。ブロックされたトラフィックは、それ以上の検査なしで即座に拒否されるため、[ブロック（Block）] ルールの場合は接続終了時のイベントはロギングできません。

ステップ 4 接続イベントの送信先を指定します。

ステップ 5 [保存（Save）] をクリックしてルールを保存します。

ステップ 6 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

TLS/SSL ルールを使用した復号可能接続のロギング

手順

ステップ 1 復号ポリシーエディタで、ロギングを設定するルールの横にある **[編集（Edit）]**（✎）をクリックします。

代わりに [表示（View）]（👁）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 2 [ロギング（Logging）] をクリックします。

ステップ 3 [接続の終了時にロギングする（Log at End of Connection）] をオンにします。

モニタ対象トラフィックに対して、接続の終了時のロギングが必要になります。

ステップ 4 接続イベントの送信先を指定します。

接続イベントについて Management Center ベースの分析を実行する場合は、イベントをイベント ビューアに送信します。モニタ対象トラフィックに対して、これが必要になります。

ステップ 5 [保存（Save）] をクリックしてルールを保存します。

ステップ 6 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

セキュリティ インテリジェンスを使用した接続のロギング

セキュリティ インテリジェンス ポリシーには、脅威スマートライセンスまたは保護クラシックライセンスが必要です。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[セキュリティ インテリジェンス（Security Intelligence）] をクリックします。

ステップ 2 [ロギング（Logging）]（ ） をクリックし、次の基準を使用してセキュリティ インテリジェンス ロギングを有効にします。

- IP アドレス別：[ネットワーク（Networks）] の横にあるロギングアイコンをクリックします。
- URL 別：[URL（URLs）] の横にあるロギングアイコンをクリックします。
- ドメイン名別：[DNS ポリシー（DNS Policy）] ドロップダウンリストの横にあるロギングアイコンをクリックします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 3 [接続のロギング（Log Connections）] チェックボックスをオンにします。

ステップ 4 接続先およびセキュリティ関連の接続イベントを指定します。

Management Center ベースの分析を実行する場合や、ブロックリストをモニター専用に設定する場合は、イベントをイベントビューアに送信します。

ステップ 5 [OK] をクリックしてロギング オプションを設定します。

ステップ 6 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

アクセス コントロール ルールを使用した接続のロギング

ルール アクションと詳細検査のオプションの選択によって、ロギング オプションは異なります。ルールとポリシーのアクションによるロギングへの影響（882 ページ）を参照してください。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、ロギングを設定するルールの横にある**[編集（Edit）]**（ ）をクリックします。

代わりに [表示（View）]（ ） が表示される場合、設定は先祖ポリシーから継承されるか、または先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 2 [ロギング（Logging）] タブをクリックします。

ステップ 3 [接続の開始時にロギングする（Log at Beginning of Connection）] または [接続の終了時にロギングする（Log at End of Connection）] を指定します。

パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。

ステップ 4 （オプション）[ファイルのロギング（Log Files）] チェックボックスをオンにして、接続に関連付けられているファイル イベントとマルウェア イベントをロギングします。

シスコは、このオプションを有効のままにすることを推奨します。

ステップ 5 接続イベントの送信先を指定します。

- [イベントビューア（Event Viewers）]：Management Center にイベントを送信します。クラウド管理を使用している場合、イベント分析のみを実行するように設定しているときは、クラウド提供型 Management Center およびオンプレミス Management Center にイベントを送信します。どちらの製品のイベントビューアでもイベントを表示できます。
- [Syslog サーバー（Syslog Server）]：オーバーライドする場合を除き、アクセス コントロール ポリシーに設定されている syslog サーバーに接続イベントを送信します。

  [オーバーライドの表示（Show Overrides）]：アクセス コントロール ポリシーで設定されている設定をオーバーライドするためのオプションが表示されます。

  - [重大度をオーバーライドする（Override Severity）]：このオプションを選択し、ルールの重大度を選択した場合は、このルールの接続イベントはアクセス コントロール ポリシーの [ロギング（Logging）] タブに設定されている重大度に関わらず、選択した重大度が設定されます。
  - [デフォルトの Syslog の宛先をオーバーライドする（Override Default Syslog Destination）]：このルールの接続イベントに生成された syslog をこのアラートに指定されている宛先に送信します。
- [SNMP トラップ（SNMP Trap）]：接続イベントは、選択した SNMP トラップに送信されます。

ステップ 6 [保存（Save）] をクリックしてルールを保存します。

次のタスク

- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

ポリシーのデフォルト アクションによる接続のロギング

ポリシーのデフォルトアクションにより、システムがポリシー内のルールのいずれにも一致しないトラフィックを処理する方法が決定されます（ただし、トラフィックの照合およびロギングを実行し、トラフィックの処理や調査は実行しないアクセス コントロール ポリシーと復号ポリシー内のモニタールールを除きます）。

また、システムが複号できないセッションをロギングする方法は、復号ポリシーのデフォルトアクションのロギング設定でも制御されます。

始める前に

- プレフィルタのデフォルトアクションロギングについては、デフォルトアクションを[すべてのトンネル トラフィックをブロック（Block all tunnel traffic）] に設定します。[すべてのトンネル トラフィックを許可（Allow all tunnel traffic）] アクションのロギングは無効になります。これにより、接続のアクセス制御が引き続き可能になり、接続の処理とロギングは別の設定で決定されます。

手順

ステップ 1 ポリシーエディタで、[デフォルトアクション（Default Action）] ドロップダウンリストの横にある [ロギング（Logging）]（ ） をクリックします。

ステップ 2 一致する接続をロギングするタイミングを指定します。

- 接続の開始時にロギングする：SSL のデフォルト アクションではサポートされていません。
- 接続の終了時にロギングする：アクセス制御の [すべてのトラフィックをブロック（Block All Traffic）] デフォルト アクションまたはプレフィルタの [すべてのトンネル トラフィックをブロック（Block all tunnel traffic）] デフォルト アクションを選択するとサポートされなくなります。

パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。アクセス コントロール ポリシーでは、設定が先祖ポリシーから継承されることもあります。

ステップ 3 接続イベントの送信先を指定します。

接続イベントについて Management Center ベースの分析を実行する場合は、イベントをイベント ビューアに送信します。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

長い URL のロギング制限

HTTP トラフィックの接続の終了イベントは、監視対象ホストによって要求された URL を記録します。URL の保管を無効にすることや保管する URL 文字数を制限することで、システム パフォーマンスが向上する可能性があります。URL のロギングを無効化しても（保管する文字数を 0 にしても）、URL フィルタリングには影響しません。システムは、要求された URL に基づいてトラフィックをフィルタリングします。それらの URL を記録しない場合も同じです。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] をクリックして、[一般設定（General Settings）] の横にある **[編集（Edit）]**（✎） をクリックします。

代わりに [表示（View）]（👁） が表示される場合、設定は先祖ポリシーから継承されるか、または先祖ドメインに属しており、設定を変更する権限がありません。設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

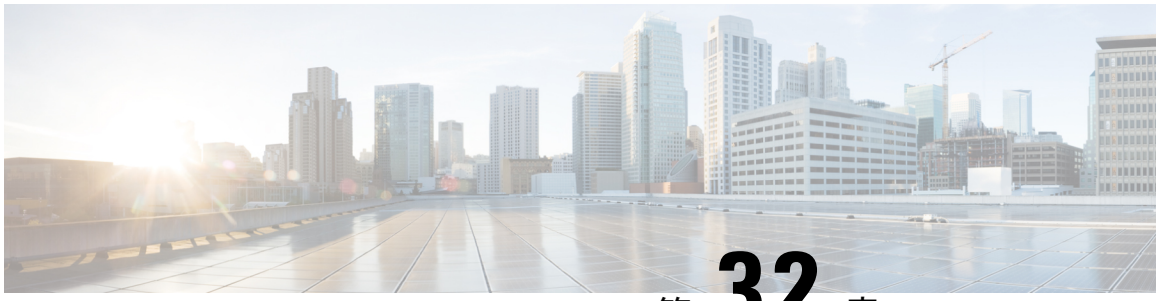
ステップ 2 [接続イベントで保存する URL の最大文字数（Maximum URL characters to store in connection events）] を入力します。

ステップ 3 [OK] をクリックします。

ステップ 4 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。



第 32 章

接続およびセキュリティ関連の接続イベント

次のトピックでは、接続およびセキュリティ イベント テーブルを使用する方法について説明します。

接続イベントについて

システムは管理対象デバイスで検出された接続のログを生成できます。このログは接続イベントと呼ばれます。接続イベントには、セキュリティ関連の接続イベント（レピュテーションベースのセキュリティ インテリジェンス機能によってブロックされた接続）が含まれます。

接続イベントには、一般に、次によって検出されたトランザクションが含まれます。

- アクセス コントロール ポリシー
- 復号化ポリシー
- （プレフィルタまたはトンネルルールによってキャプチャされた）プレフィルタ ポリシー
- DNS ブロックリスト
- URL ブロックリスト
- ネットワーク（IP アドレス）ブロックリスト

ルールやポリシーの設定を行うことで、ログに記録する接続の種類、接続をログに記録するタイミング、およびデータを保存する場所をきめ細かく制御できます。

詳細については、接続ロギング （879 ページ）を参照してください。

関連トピック

セキュリティ インテリジェンスについて

接続イベントとセキュリティ関連の接続イベントの比較

セキュリティ関連の接続イベントは、レピュテーションベースのセキュリティインテリジェンス機能によりセッションがブロックされたときに生成される接続イベントです。

ただし、すべてのセキュリティ関連の接続イベントに同一の接続イベントがあります。セキュリティ関連の接続イベントは個別に表示して分析できます。また、システムはセキュリティ関連の接続イベントを個別に保存およびプルーニングします。

システムは、より多くのリソースを消費する評価を行う前に、セキュリティインテリジェンスを実施することに注意してください。接続がセキュリティインテリジェンスによってブロックされた場合、結果として生成されるイベントには、その後の評価によってシステムで収集されることになっていた情報（ユーザ ID など）が含まれません。

（注） 本書では違うと明記されていない限り、接続イベントに関する情報は、セキュリティ関連の接続イベントに関する情報でもあります。

NetFlow 接続

管理対象デバイスで収集された接続データを補うために、NetFlowエクスポータによってブロードキャストされたレコードを使用して接続イベントを生成できます。この方法が特に役立つのは、NetFlow エクスポータが、管理対象デバイスでモニタしているネットワークとは別のネットワークをモニタしている場合です。

システムは NetFlow レコードを単方向の接続終了イベントとして Secure Firewall Management Centerデータベースに記録します。これらの接続に関して使用可能な情報は、アクセス コントロール ポリシーで検出された接続の情報とは若干異なります。NetFlowデータと管理対象デバイス データの違いを参照してください。

関連トピック

NetFlow データ

接続の概要（グラフ用集約データ）

システムは5分間隔で収集された接続データを集約し、接続の概要を作成します。この概要を使用して、接続グラフとトラフィックプロファイルがシステムで生成されます。必要に応じて、接続サマリーのデータに基づいてカスタム ワークフローを作成できます。これは、個々の接続イベントに基づいたワークフローと同じように使用できます。

セキュリティ関連の接続イベント専用の接続サマリーはないことに注意してください。ただし、対応する接続終了イベントは接続サマリーのデータに集約できます。

集約するには、複数の接続が以下の状態である必要があります。

- 接続終了を表している
- 送信元と宛先の IP アドレスが同じで、応答側（宛先）のホストで同じポートを使用している
- 同じプロトコルを使用している（TCP または UDP）
- 同じアプリケーション プロトコルを使用している
- 同じ管理対象デバイスまたは同じ NetFlow エクスポータによって検出される

各接続の概要には、接続数など全トラフィック統計情報が含まれています。NetFlowエクスポータは単一方向接続を生成するので、接続の概要では、NetFlow データに基づく接続ごとに接続数が 2 ずつ増えます。

接続の概要には、概要内の集約された接続に関するすべての情報が含まれているわけではありませんので注意してください。たとえば、接続の概要に集約される接続にはクライアント情報が使用されないため、概要にクライアント情報は含まれません。

長時間接続

接続データを集約する 5 分間隔の 2 回以上に監視対象のセッションがまたがる場合、その接続は長時間接続と見なされます。接続サマリーで接続数を計算する際には、長時間接続が開始された 5 分間隔の回のみカウントします。

また、長時間接続において発信側と応答側が送信したパケット数とバイト数を計算する際は、システムは5分間隔の各回で実際に送信されたパケット数とバイト数を報告しません。代わりにシステムは、送信された合計パケット数と合計バイト数、接続の長さ、5 分間隔の各回で接続のどの部分が行われたかに基づいて、一定の送信速度を仮定し、値を推定します。

外部応答側からの統合接続サマリ

接続データの保存に必要なスペースを減らし、接続グラフのレンダリングを高速化するために、システムは次の場合に接続サマリを統合します。

- 接続に関連するホストの 1 つが監視対象のネットワーク上にない場合
- 外部ホストの IP アドレス以外で、サマリ内の接続がサマリ集約条件を満たす場合

[分析（Analysis）] > [接続（Connections）] サブメニュー ページで接続サマリーを表示する場合や、接続グラフを使用する場合、システムは非モニタ対象ホストの IP アドレスの代わりに `external` と表示します。

この集約の結果として、外部応答側を含む接続サマリーまたはグラフから接続データのテーブル ビューにドリルダウンしようとすると（つまり、個別の接続データへのアクセス）、テーブル ビューには情報が何も表示されません。

接続およびセキュリティ関連の接続イベントフィールド

（注） 接続に関連付けられたイベントの検索に、接続/セキュリティ関連の接続イベントの検索ページは使用できません。

[アクセスコントロールポリシー（Access Control Policy）]（Syslog：ACPolicy）

接続をモニターしたアクセス コントロール ポリシー。

[アクセス制御ルール（Access Control Rule）]（Syslog：AccessControlRuleName）

接続を処理したアクセス コントロール ルールまたはデフォルト アクションと、その接続に一致した最大 8 つのモニター ルール。

接続が 1 つのモニター ルールに一致した場合、Secure Firewall Management Center は接続を処理したルールの名前を表示し、その後にモニタールール名を表示します。接続が複数のモニタールールに一致した場合、一致するモニタールールの数が表示されます（`Default Action + 2 Monitor Rules` など）。

接続に一致した最初の 8 つのモニター ルールのリストをポップアップ ウィンドウに表示するには、[N モニター ルール（*N*Monitor Rules）] をクリックします。

[アクション（Action）]（Syslog：AccessControlRuleAction）

接続をロギングした設定に関連付けられているアクション。

セキュリティ インテリジェンスによってモニタされている接続の場合、そのアクションは、接続によってトリガーされる最初のモニタ以外のアクセス コントロール ルールのアクションであるか、またはデフォルト アクションです。同様に、モニタ ルールに一致するトラフィックは常に後続のルールまたはデフォルト アクションによって処理されるため、モニタ ルールによってロギングされた接続と関連付けられたアクションが [モニタ（Monitor）] になることはありません。ただし、モニタ ルールに一致する接続の相関ポリシー違反をトリガーする可能性があります。

アクション	説明
許可（Allow）	アクセス コントロールによって明示的に許可された、またはユーザがインタラクティブ ブロックをバイパスしたために許可された接続。

アクション	説明
ブロック（Block）、リセットしてブロック（Block with reset）	次を含むブロックされた接続： • プレフィルタ ポリシーによってブロックされたトンネルおよびその他の接続 • セキュリティ インテリジェンスによってブロックされた接続。 • SSL ポリシーによってブロックされた暗号化接続。 • 侵入ポリシーによってエクスプロイトがブロックされた接続。 • ファイルポリシーによってファイル（マルウェアを含む）がブロックされた接続。 システムが侵入またはファイルをブロックする接続では、アクセス コントロールの許可ルールを使用してディープ インスペクションを呼び出す場合にも、システムは `Block` を表示します。
高速パス（Fastpath）	プレフィルタ ポリシーによって高速パスが適用された暗号化されていないトンネルおよびその他の接続。
インタラクティブ ブロック（Interactive Block）、リセット付きインタラクティブ ブロック（Interactive Block with reset）	システムがインタラクティブ ブロック ルールを使用してユーザの HTTP 要求を最初にブロックしたときにログに記録された接続。システムにより表示される警告ページでユーザがクリックスルーすると、そのセッションでログに記録されるその後の接続に許可アクションが付きます。
信頼（Trust）	アクセス コントロールによって信頼された接続。デバイス モデルに応じて、システムは信頼された TCP 接続を別にログに記録します。
デフォルト アクション（Default Action）	アクセス コントロール ポリシーのデフォルト アクションによって処理される接続。
（空白/空）	ルールに一致するのに十分なパケットが渡される前に接続が閉じられました。 侵入防御などのアクセス制御以外の機能によって接続がログに記録される場合にのみ発生します。

[アプリケーションプロトコル（Application Protocol）]（syslog：ApplicationProtocol）

Secure Firewall Management Center の Web インターフェイスでは、この値は概要とグラフを抑制します。

接続で検出された、ホスト間の通信を表すアプリケーション プロトコル。

アプリケーション プロトコル カテゴリおよびタグ（Application Protocol Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

アプリケーションのリスク（Application Risk）

接続で検出されたアプリケーション トラフィックに関連するリスク：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するリスクがあります。このフィールドでは、それらのうち最も高いものが表示されます。

ビジネスとの関連性（Business Relevance）

接続で検出されたアプリケーショントラフィックに関連するビジネス関連性：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するビジネスとの関連性があります。このフィールドでは、それらのうち最も低いもの（関連が最も低い）が表示されます。

[クライアントとクライアントバージョン（Client and Client Version）]（Syslog：Client、ClientVersion）

接続で検出されたクライアントのクライアント アプリケーションとバージョン。

接続に使用されている特定のクライアントをシステムが特定できなかった場合、このフィールドは汎用的な名称としてアプリケーション プロトコル名の後に「client」という語を付加して FTP client などと表示します。

クライアント カテゴリおよびタグ（Client Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

Connection Counter（Syslog のみ）

ある接続と別の同時接続を区別するカウンタ。このフィールドは、それ自体には意味がありません。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを識別できます。

Connection Instance ID（Syslog のみ）

接続イベントを処理した Snort インスタンス。このフィールドは、それ自体には意味がありません。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを識別できます。

ConnectionDuration(Syslog のみ)

このフィールドは syslog フィールドとしてのみ存在します。Secure Firewall Management Center の Web インターフェイスにはありません。（Web インターフェイスは、[最初のパケット（First Packet）] 列と [最後のパケット（Last Packet）] 列を使用してこの情報を伝送します。）

このフィールドは、接続の最後にロギングが発生した場合にのみ、値が備わっています。接続開始のsyslogメッセージでは、このフィールドは出力されません。その時点では不明であるためです。

接続終了のsyslogメッセージでは、このフィールどは最初のパケットと最後のパケットまでの秒数が表示されます。短時間の接続ではゼロになることがあります。たとえば、syslogのタイムスタンプが12:34:56でConnectionDurationが5の場合、最初のパケットは12:34:51に検出されました。

接続（Connections）

接続サマリーに含まれる接続数。長時間接続（複数回の接続サマリー間隔にまたがる接続）の場合、最初の接続サマリー間隔の分だけ増加します。[接続（Connections）]条件を使用した検索で意味のある結果を表示するには、接続サマリーページを持つカスタムワークフローを使用する必要があります。

メンバー数（Count）

各行に表示される情報に一致する接続数。[カウント（Count）]フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。カスタムワークフローを作成し、ドリルダウンページに[カウント（Count）]カラムを追加しない場合、各接続は個別に表示され、パケット数とバイト数は合計されません。

ピアの復号化（Decrypt Peer）

関連付けられた接続のパケットを復号するVPNピアのIPアドレス（ピアのIKEアドレス）。

VPNピアのIPアドレスを表示するには、接続の開始時と接続の終了時にログを記録するアクセス コントロール ポリシー ルールのログ設定を有効にする必要があります。復号されたトラフィックのアクセス コントロール ポリシーのバイパス（sysopt connection permit-vpn）オプションを有効にした場合、復号されたトラフィックの詳細を表示できません。

検出タイプ（Syslog：DetectionType）

このフィールドには、クライアントアプリケーションの検出元が表示されます。[AppID]または[暗号化された可視性（Encrypted Visibility）]のいずれかです。

[宛先ポート/ICMPコード（Destination Port/ICMP Code）]（Syslog：個別のフィールド - DstPort、ICMPCode）

Secure Firewall Management Centerのインターフェイスでは、これらの値は概要とグラフを抑制します。

セッション レスポンダが使用するポートまたはICMPコード。

DestinationSecurityGroup（Syslogのみ）

このフィールドには、**Destinationsecuritygrouptag**（使用可能な場合）の数値に関連付けられているテキスト値が保持されます。グループ名をテキスト値として使用できない場合、このフィールドには、[DestinationSecurityGroupTag]フィールドと同じ整数値が含まれます。

[DestinationSecurityGroupType] (Syslog のみ)

このフィールドには、セキュリティグループタグを取得した送信元が表示されます。

値	説明
インライン	送信元 SGT 値はパケットからのものです
Session Directory	送信元 SGT 値は、セッション ディレクトリ トピックによる ISE からのものです
SXP	送信元 SGT 値は SXP トピックによる ISE からのものです

宛先 SGT（Syslog：DestinationSecurityGroupTag）

接続に関係する宛先のセキュリティ グループ タグ（SGT）属性。

送信元 SGT 値は、[DestinationSecurityGroupType] フィールドで指定された送信元から取得されます。

[検出タイプ（Detection Type）]

このフィールドには、クライアントの検出元が表示されます。

デバイス

Secure Firewall Management Center の Web インターフェイスでは、この値は概要とグラフを抑制します。

接続を検出した管理対象デバイス。または、NetFlowデータから生成された接続の場合は、データを処理した管理対象デバイス。

DeviceUUID（Syslog のみ）

イベントを生成した Firepower デバイスの一意の識別子。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを識別できます。

[DNSクエリ（DNS Query）]（Syslog：DNSQuery）

ドメイン名を検索するために接続でネーム サーバーに送信された DNS クエリ。

このフィールドには、DNS フィルタリングが有効になっている場合の URL フィルタリング一致のドメイン名も保持できます。この場合、[URL] フィールドは空白になり、[URL Category] フィールドと [URL Reputation] フィールドにはドメインに関連付けられた値が含まれます。

DNS フィルタリングの詳細については、DNS フィルタリング：DNS ルックアップ中の URL レピュテーションとカテゴリの識別（ベータ版）を参照してください。

[DNSレコードタイプ（DNS Record Type）]（Syslog：DNSRecordType）

接続で送信された DNS クエリを解決するために使用された DNS リソース レコードのタイプ。

[DNS応答（DNS Response）]（Syslog：DNSResponseType）

問い合わせ時に接続でネーム サーバーに返された DNS レスポンス。

[DNSシンクホール名 （DNS Sinkhole Name）]（Syslog：DNS_Sinkhole）

システムが接続をリダイレクトしたシンクホール サーバーの名前。

DNS TTL（syslog：DNS_TTL）

DNS サーバーが DNS リソース レコードをキャッシュする秒数。

ドメイン（Domain）

接続を検出した管理対象デバイスのドメイン。または、NetFlow データから生成された接続の場合は、データを処理した管理対象デバイスのドメイン。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

ピアの暗号化（Encrypt Peer）

関連付けられた接続のパケットを暗号化する VPN ピアの IP アドレス（ピアの IKE アドレス）。

VPN ピアの IP アドレスを表示するには、接続の開始時と接続の終了時にログを記録するアクセス コントロール ポリシー ルールのログ設定を有効にする必要があります。

暗号化された可視性フィンガープリント（Syslog：EncryptedVisibilityFingerprint）

セッションの暗号化された可視化エンジン（EVE）によって検出された TLS フィンガープリント。

暗号化された可視性プロセス名（Syslog：EncryptedVisibilityProcessName）

暗号化された可視性エンジン（EVE）によって分析された TLS クライアント hello パケットのプロセスまたはクライアント。

暗号化された可視性信頼スコア（Syslog：EncryptedVisibilityConfidenceScore）

暗号化された可視性エンジンが適切なプロセスを検出しているかを示す 0 ー 100％ の範囲内の信頼値。たとえば、プロセス名が Firefox で、信頼スコアが 80％ の場合、エンジンが検出したプロセスが Firefox であると 80％ 信頼していることを示します。

暗号化された可視性脅威の信頼度（Syslog：EncryptedVisibilityThreatConfidence）

暗号化された可視性エンジンによって検出されたプロセスに脅威が含まれる確率のレベル。このフィールドは、脅威信頼スコアの値に基づいて、帯域（[Very High]、[High]、[Medium]、[Low]、または [Very Low]）を示します。

暗号化された可視性脅威信頼スコア（Syslog：EncryptedVisibilityThreatConfidenceScore）

暗号化された可視性エンジンによって検出されたプロセスに脅威が含まれていることを示す 0 ー 100％ の範囲内の信頼値。脅威信頼スコアが非常に高い場合（90% など）、[暗号化された可視性プロセス名（Encrypted Visibility Process Name）] フィールドには [マルウェア（Malware）] と表示されます。

エンドポイント ロケーション（Endpoint Location）

ISE で指定された、ユーザーの認証に ISE を使用したネットワーク デバイスの IP アドレス。

エンドポイントのプロファイル (Syslog:Endpoint Profile)

ISE で指定されたユーザーのエンドポイント デバイス タイプ。

Event Priority（Syslog のみ）

接続イベントが優先度の高いイベントであるかどうか。高優先度（`High`）イベントは、侵入、セキュリティ インテリジェンス、ファイル、またはマルウェアイベントに関連付けられた接続イベントです。他のすべてのイベントは低優先度（`Low`）イベントです。

ファイル (Syslog: FileCount)

1 つ以上のファイルイベントに関連付けられている接続で検出またはブロックされたファイル（マルウェア ファイルを含む）の数。

Secure Firewall Management Center の Web インターフェイスでは、[ファイルの表示（View Files）] アイコン（）はファイルのリストにリンクしています。アイコンの数字は、その接続で検出またはブロックされたファイル数（マルウェア ファイルを含む）を示します。

[最初のパケットまたは最後のパケット（First Packet or Last Packet）]（Syslog：ConnectionDuration フィールドを参照）

セッションの最初または最後のパケットが検出された日時。

First Packet Time（Syslog のみ）

システムが最初のパケットを検出した時間。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを識別できます。

HTTP Referrer (Syslog: HTTPReferer)

接続で検出された HTTP トラフィックの要求 URL のリファラを示す HTTP リファラ（他の URL へのリンクを提供した Web サイト、他の URL からリンクをインポートした Web サイトなど）。

HTTP 応答コード (Syslog:HTTPResponse)

クライアントからの接続経由の HTTP 要求に応じて送信される HTTP ステータス コード。

[入力/出力インターフェイス（Ingress/Egress Interface）]（Syslog：IngressInterface、EgressInterface）

接続に関連付けられた入力または出力のインターフェイス。展開に非対称のルーティング設定が含まれている場合は、入力と出力のインターフェイスが同じインラインペアに属する場合があります。

[入力/出力セキュリティゾーン（Ingress/Egress Security Zone）]（Syslog：IngressZone、EgressZone）

接続に関連付けられた入力または出力のセキュリティ ゾーン。

再区分されたカプセル化接続では、元の入力セキュリティゾーンの代わりに、割り当てたトンネル ゾーンが入力フィールドに表示されます。出力フィールドは空白です。

入力仮想ルータ/出力仮想ルータ（Syslog：Ingressvrf、 EgressVRF）

仮想ルーティングを使用するネットワークにおける、トラフィックがネットワークに出入りするときに通過する仮想ルータの名前。

イニシエータ/Responder バイト (Syslog: InitiatorBytes、 ResponderBytes)

セッション イニシエータが送信したバイトまたはセッション レスポンダが受信したバイトの総数。

イニシエータ/レスポンダ大陸（Initiator/Responder Continent）

ルーティング可能な IP が検出された場合の、セッション イニシエータまたはレスポンダの IP アドレスに関連付けられた大陸。

イニシエータ/レスポンダ国（Initiator/Responder Country）

ルーティング可能な IP が検出された場合の、セッション イニシエータまたはレスポンダの IP アドレスに関連付けられた国。システムにより、国旗のアイコンと、国の ISO 3166-1 alpha-3 国番号が表示されます。国旗アイコンの上にポインタを移動すると、国の完全な名称が表示されます。

[イニシエータ/レスポンダ IP（Initiator/Responder IP）]（Syslog：SrcIP、DstIP）

Secure Firewall Management Center のインターフェイスでは、これらの値は概要とグラフを抑制します。

セッション イニシエータまたはレスポンダの IP アドレス（および DNS 解決が有効化されている場合はホスト名）。

イニシエータ/レスポンダ、送信元/接続先、および送信者/受信者フィールドに関する注意（922 ページ）も参照してください。

Secure Firewall Management Center の Web インターフェイスでは、ホストアイコンは接続がブロックされる原因となった IP アドレスを示します。

プレフィルタポリシーによってブロックされるか、または高速パスが適用されたプレーンテキストのパススルートンネルでは、イニシエータとレスポンダの IP アドレスはトンネルエンドポイント（トンネルの両側のネットワークデバイスのルーテッドインターフェイス）を表します。

[イニシエータ/レスポンダのパケット数（Initiator/Responder Packets）]（Syslog：InitiatorPackets、ResponderPackets）

セッション イニシエータが送信したバイトまたはセッション レスポンダが受信したパケットの総数。

[イニシエータユーザー（Initiator User）]（Syslog：User）

Secure Firewall Management Center の Web インターフェイスでは、この値は概要とグラフを制限します。

セッションイニシエータにログインしていたユーザー。このフィールドに[認証なし（No Authentication）] が入力されている場合、ユーザ トラフィックは次のようになります。

- 関連付けられたアイデンティティ ポリシーがないアクセス コントロール ポリシーに一致しました。
- アイデンティティ ポリシーのいずれのルールにも一致しませんでした。

該当する場合、ユーザー名の前には `<realm>\` が付いています。

イニシエータ/レスポンダ、送信元/接続先、および送信者/受信者フィールドに関する注意（922 ページ）も参照してください。

[侵入イベント（Intrusion Events）]（syslog：IPSCount）

接続に関連付けられた侵入イベント（ある場合）の数。

Secure Firewall Management Center の Web インターフェイスでは、[侵入イベントの表示（View Intrusion Events）] アイコン（）はイベントのリストにリンクしています。

IOC

マルウェアイベントが、接続に関与したホストに対する侵入の痕跡（IOC）をトリガーしたかどうか。

[NAT Source/Destination IP (Syslog: NAT_InitiatorIP, NAT_ResponderIP)]

セッションのイニシエータまたはレスポンダの NAT 変換後の IP アドレス。

[NAT Source/Destination Port (Syslog: NAT_InitiatorPort, NAT_ResponderPort)]

セッションのイニシエータまたはレスポンダの NAT 変換後のポート。

[NetBIOSドメイン（NetBIOS Domain）]（Syslog：NetBIOSDomain）

セッションで使用された NetBIOS ドメイン。

NetFlow SNMP 入出力（NetFlow SNMP Input/Output）

NetFlow データから生成された接続の場合、接続トラフィックが NetFlow 対応デバイスに入ったか、NetFlowエクスポータから出た際のインターフェイスのインターフェイスインデックス。

NetFlow 送信元/宛先の自律システム（NetFlow Source/Destination Autonomous System）

NetFlow データから生成された接続の場合、接続のトラフィックの送信元または宛先に対する、Border Gateway Protocol の自律システム番号。

NetFlow 送信元/宛先のプレフィックス（NetFlow Source/Destination Prefix）

NetFlowデータから生成された接続の場合、送信元または宛先のIPアドレスに、送信元と宛先のプレフィックス マスクが追加されたもの。

NetFlow 送信元/宛先 TOS（NetFlow Source/Destination TOS）

NetFlow データから生成された接続の場合、接続トラフィックが NetFlow 対応デバイスに入ったか、NetFlow エクスポータから出たときの Type of Service（TOS）バイトの設定。

[ネットワーク分析ポリシー（Network Analysis Policy）]（Syslog：NAPPolicy）

イベントの生成に関連付けられているネットワーク分析ポリシー（NAP）（ある場合）。

クライアントのオリジナル国（Original Client Country）

元のクライアントの IP アドレスが属する国。この値を取得するために、システムは元のクライアント IP アドレスを X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義の HTTP ヘッダーから抽出し、それを地理位置情報データベース（GeoDB）を使用して国にマップします。このフィールドに入力するには、元のクライアントに基づいてプロキシ トラフィックを処理するアクセス コントロール ルールを有効にする必要があります。

[元のクライアントのIP（Original Client IP）]（Syslog：originalClientSrcIP）

X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義の HTTP ヘッダーからの、元のクライアント IP アドレス。このフィールドに入力するには、元のクライアントに基づいてプロキシ トラフィックを処理するアクセス コントロール ルールを有効にする必要があります。

プレフィルタ ポリシー (Syslog:Prefilter Policy)

接続を処理したプレフィルタ ポリシー。

プロトコル (Syslog:Protocol)

Secure Firewall Management Center の Web インターフェイスは、次のようになります。

- この値は概要とグラフを抑制します。
- このフィールドは検索フィールドとしてのみ使用できます。

接続に使用されるトランスポート プロトコルです。特定のプロトコルを検索するには、名前を使用するか、http://www.iana.org/assignments/protocol-numbers に記載されたプロトコルの番号を指定します。

QoS が適用されたインターフェイス（QoS-Applied Interface）

レート制限された接続で、レート制限を適用するインターフェイスの名前。

QoS がドロップされたイニシエータのバイト数（QoS-Dropped Initiator Bytes）/QoS がドロップされたレスポンダのバイト数（QoS-Dropped Responder Bytes）

レート制限によりセッション イニシエータまたはセッション レスポンダからドロップされたバイト数。

QoS がドロップされたイニシエータのパケット数（QoS-Dropped Initiator Packets）/QoS がドロップされたレスポンダのパケット数（QoS-Dropped Responder Packets）

レート制限によりセッション イニシエータまたはセッション レスポンダからドロップされたパケット数。

QoS ポリシー（QoS Policy）

接続のレートを制限する QoS ポリシー。

QoS ルール（QoS Rule）

接続のレートを制限する QoS ルール。

[理由（Reason）]（Syslog：AccessControlRuleReason）

多くの場合に接続がロギングされた 1 つまたは複数の原因。完全なリストについては、接続イベントの理由 （923 ページ）を参照してください。

IP ブロック、DNS ブロック、および URL ブロックの理由による接続には、固有のイニシエータ レスポンダ ペアごとに 15 秒のしきい値があります。システムがこれらのいずれかの接続をブロックした後、イベントを生成した時点から 15 秒の間、この 2 つのホスト間で接続がブロックされたとしても、ポートやプロトコルの違いに関わらず、接続イベントを生成しません。

[参照先ホスト（Referenced Host）]（Syslog：ReferencedHost）

接続のプロトコルが HTTP または HTTPS の場合、このフィールドにはそれぞれのプロトコルが使用していたホスト名が表示されます。

SecIntMatchingIP(Syslog のみ)

どの IP アドレスが一致しているか。

有効な値：**`None`**、**`Destination`**、または**`Source`**。

[セキュリティコンテキスト（Security Context）]（Syslog：Context）

ASA FirePOWER でマルチコンテキストモードで処理される接続で、トラフィックが通過した仮想ファイアウォールグループを特定するメタデータ。

[Security Intelligence Category (Syslog: URLSICategory, DNSSICategory , IPReputationSICategory)]

接続でブロックされた URL、ドメイン、または IP アドレスを表すか、またはそれを含むオブジェクトの名前。セキュリティ インテリジェンスのカテゴリは、ネットワークオブジェクトまたはグループ、ブロックリスト、カスタム セキュリティ インテリジェンスのリストまたはフィード、監視に関連する TID カテゴリ、またはインテリジェンスフィードのカテゴリのいずれかの名前にすることができます。

Secure Firewall Management Center の Web インターフェイスでは、DNS、ネットワーク（IP アドレス）、および URL セキュリティ インテリジェンスの接続イベントは 1 つのカテゴリ フィールドに結合されます。syslog メッセージでは、それらのイベントはタイプ別に固有です。

セキュリティ関連の接続イベントには、セキュリティ インテリジェンス イベントやその他の接続イベント（侵入イベントやマルウェアイベントをトリガーしたものなど）が含まれます。[セキュリティ インテリジェンスの概要（Security Intelligence Summary）] ワークフローには、すべてのセキュリティ インテリジェンス イベントがカテゴリや数ごとに表示されます。セキュリティ インテリジェンス カテゴリのないイベントは、グループ化され、数とのみ表示されます。

インテリジェンス フィードのカテゴリの詳細については、セキュリティ インテリジェンス カテゴリ を参照してください。

Source Device

Secure Firewall Management Center の Web インターフェイスでは、この値は概要とグラフを抑制します。

接続の生成に使用されたデータをブロードキャストする NetFlow エクスポータの IP アドレス。管理対象デバイスによって接続が検出された場合、このフィールドには`Firepower`と表示されます。

[送信元ポート/ICMPタイプ（Source Port/ICMP Type）]（Syslog：SrcPort、ICMPType）

Secure Firewall Management Center のインターフェイスでは、これらの値は概要とグラフを抑制します。

セッション イニシエータが使用するポートまたは ICMP タイプ。

SourceSecurityGroup（Syslog のみ）

このフィールドには、[SourceSecurityGroupTag]（使用可能な場合）の数値に関連付けられているテキスト値が保持されます。グループ名をテキスト値として使用できない場合、このフィールドには、[SourceSecurityGroupTag] フィールドと同じ整数値が含まれます。タグは、インラインデバイス（送信元SGT名が指定されていない）またはISE（送信元を指定している）から取得できます。

SourceSecurityGroupType (Syslog のみ)

このフィールドには、セキュリティグループタグを取得した送信元が表示されます。

値	説明
インライン	送信元 SGT 値はパケットからのものです
Session Directory	送信元 SGT 値は、セッション ディレクトリ トピックによる ISE からのものです
SXP	送信元 SGT 値は、SXP トピックによる ISE からのものです

送信元 SGT（Syslog：SourceSecurityGroupTag）

接続に関係するパケットのセキュリティグループタグ（SGT）属性の数値表現。SGT は、信頼ネットワーク内での、トラフィックの送信元の権限を指定します。セキュリティ グループ アクセス（Cisco TrustSec と Cisco ISE の両方に共通の機能）は、パケットがネットワークに入るときに属性を適用します。

SSL Actual Action (Syslog: SSLActualAction)

Secure Firewall Management Center の Web インターフェイスでは、このフィールドは検索フィールド専用です。

システムにより、検索ワークフローのページの [SSL ステータス（SSL Status）] フィールドにフィールド値が表示されます。

システムが SSL ポリシーの暗号化トラフィックに適用したアクション。

アクション	説明
ブロック/リセット付きブロック（Block/Block with reset）	ブロックされた暗号化接続を表します。
[復号（再署名）（Decrypt (Resign)）]	再署名サーバ証明書を使用して復号された発信接続を表します。
[復号（キーの交換）（Decrypt (Replace Key)）]	置き換えられた公開キーと自己署名サーバ証明書を使用して復号化された発信接続を表します。
[復号（既知のキー）（Decrypt (Known Key)）]	既知の秘密キーを使用して復号化された着信接続を表します。
[デフォルトアクション（Default Action）]	接続がデフォルト アクションによって処理されたことを示します。
[復号しない（Do not Decrypt）]	システムが復号化しなかった接続を表します。

[SSL証明書情報（SSL Certificate Information）]（Syslog：SSLCertificate）

Secure Firewall Management Center の Web インターフェイスでは、このフィールドは検索フィールド専用です。

トラフィックを暗号化するための公開キー証明書に保存される次の情報：

- サブジェクト/発行元共通名（Subject/Issuer Common Name）
- サブジェクト/発行元組織（Subject/Issuer Organization）
- サブジェクト/発行元組織単位（Subject/Issuer Organization Unit）
- 有効期間の開始/終了（Not Valid Before/After）

- シリアル番号（Serial Number）
- 証明書フィンガープリント（Certificate Fingerprint）
- 公開キー フィンガープリント（Public Key Fingerprint）

[SSL証明書ステータス（SSL Certificate Status）]（Syslog：SSLServerCertStatus）

これは、認証ステータスのSSLルール条件が設定されている場合にのみ適用されます。暗号化されたトラフィックがSSLルールに一致すると、このフィールドに次のサーバの証明書のステータス値の 1 つ以上が表示されます。

- [自署（Self Signed）]
- [有効（Valid）]
- [署名が無効（Invalid Signature）]
- [発行元が無効（Invalid issuer）]
- [期限切れ（Expired）]
- [不明（Unknown）]
- [まだ有効ではない（Not Valid Yet）]
- [失効（Revoked）]

復号できないトラフィックが SSL ルールと一致する場合、このフィールドには [未チェック（Not Checked）] と表示されます。

[SSL暗号スイート（SSL Cipher Suite）]（Syslog：SSSLCipherSuite）

接続を暗号化するのに使用される暗号スイートを表すマクロ値。暗号スイートの値の指定については、 https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtmlを参照してください。

接続に適用された SSL 暗号化（SSL Encryption applied to the connection）

このフィールドは、Firepower Management Center の Web インターフェイスで検索フィールドとしてのみ使用できます。

yes または **no** を [SSL] 検索フィールドに入力することで、TLS/SSL 暗号化された接続または暗号化されていない接続が表示されます。

[SSL 予期アクション（SSL Expected Action）]（syslog：SSLExpectedAction）

Secure Firewall Management Center の Web インターフェイスでは、このフィールドは検索フィールド専用です。

有効なSSLルールで指定された、暗号化トラフィックに適用されると予想されるアクション。

[SSL の実際の動作（SSL Actual Action）] にリストされている値を入力します。

[SSL失敗の理由（SSL Failure Reason）]（Syslog：SSLFlowStatus）

システムが暗号化されたトラフィックの復号化に失敗した理由。

- 不明
- 不一致（No Match）
- Success
- キャッシュされていないセッション（Uncached Session）
- 不明な暗号スイート（Unknown Cipher Suite）
- サポートされていない暗号スイート（Unsupported Cipher Suite）
- サポートされていない SSL バージョン（Unsupported SSL Version）
- 使用された SSL 圧縮（SSL Compression Used）
- パッシブ モードで復号化できないセッション（Session Undecryptable in Passive Mode）
- ハンドシェイク エラー（Handshake Error）
- 復号エラー（Decryption Error）
- 保留中のサーバー名カテゴリの検索（Pending Server Name Category Lookup）
- 保留中の共通名カテゴリの検索（Pending Common Name Category Lookup）
- 内部エラー（Internal Error）
- 未完了のハンドシェイク（Incomplete Handshake）
- 使用不可能なネットワーク パラメータ（Network Parameters Unavailable）
- 無効なサーバー証明書の処理（Invalid Server Certificate Handle）
- 使用不可能なサーバー証明書フィンガープリント（Server Certificate Fingerprint Unavailable）
- サブジェクト DN をキャッシュできない（Cannot Cache Subject DN）
- 発行元 DN をキャッシュできない（Cannot Cache Issuer DN）
- 不明な SSL バージョン（Unknown SSL Version）
- 使用不可能な外部証明書リスト（External Certificate List Unavailable）
- 使用不可能な外部証明書フィンガープリント（External Certificate Fingerprint Unavailable）
- 無効な内部証明書リスト（Internal Certificate List Invalid）
- 使用不可能な内部証明書リスト（Internal Certificate List Unavailable）
- 使用不可能な内部証明書（Internal Certificate Unavailable）

- 使用不可能な内部証明書フィンガープリント（Internal Certificate Fingerprint Unavailable）
- 使用不可能なサーバー証明書の検証（Server Certificate Validation Unavailable）
- サーバー証明書の検証エラー（Server Certificate Validation Failure）
- 無効なアクション（Invalid Action）

フィールド値は、検索ワークフロー ページの [SSL ステータス（SSL Status）] フィールドに表示されます。

SSL フロー エラー（SSL Flow Error）

エラーが TLS/SSL セッション中に発生した場合はエラー名および 16 進数コード。エラーが発生しない場合は [成功（Success）]。

[SSLフローフラグ（SSL Flow Flags）]

暗号化された接続の最初の 10 デバッグ レベル フラグ。ワークフロー ページでは、すべてのフラグを表示するには、省略記号（**...**）をクリックします。。

管理対象デバイスが過負荷の状態になっている場合は、OVER_SUBSCRIBED というメッセージが表示されます。詳細については、TLS/SSL オーバーサブスクリプションのトラブルシューティングを参照してください。

SSL フロー メッセージ（SSL Flow Messages）

次のキーワードは、暗号化トラフィックが TLS/SSL ハンドシェイク時にクライアントとサーバー間で交換される指定されたメッセージタイプに関連付けられていることを示します。詳細については、http://tools.ietf.org/html/rfc5246を参照してください。

- HELLO_REQUEST
- CLIENT_ALERT
- SERVER_ALERT
- CLIENT_HELLO
- SERVER_HELLO
- SERVER_CERTIFICATE
- SERVER_KEY_EXCHANGE
- CERTIFICATE_REQUEST
- SERVER_HELLO_DONE
- CLIENT_CERTIFICATE
- CLIENT_KEY_EXCHANGE
- CERTIFICATE_VERIFY
- CLIENT_CHANGE_CIPHER_SPEC
- CLIENT_FINISHED

- SERVER_CHANGE_CIPHER_SPEC
- SERVER_FINISHED
- NEW_SESSION_TICKET
- HANDSHAKE_OTHER
- APP_DATA_FROM_CLIENT
- APP_DATA_FROM_SERVER
- SERVER_NAME_MISMATCH

  セッションで表示されるサーバー証明書には、宛先ドメイン名に対応しない共通名または SAN 値があります。

- CERTIFICATE_CACHE_HIT

  宛先ドメイン名に一致する証明書がキャッシュ内で見つかりました。

- CERTIFICATE_CACHE_MISS

  宛先ドメイン名に一致する証明書がキャッシュ内で見つかりませんでした。

アプリケーションで TLS/SSL ハートビート エクステンションが使用されている場合は、HEARTBEAT というメッセージが表示されます。詳細については、TLS ハートビートについてを参照してください。

[SSLポリシー（SSL Policy）]（Syslog：SSLPolicy）

接続を処理した SSL ポリシー。

アクセス コントロール ポリシーの詳細設定で TLS サーバーのアイデンティティ検出が有効になっている場合で、そのアクセス コントロール ポリシーに関連付けられている SSL ポリシーがない場合、このフィールドにはどの SSL イベントについても何も保持されません。

[SSLルール（SSL Rule）]（Syslog：SSLRuleName）

接続を処理した SSL ルールまたはデフォルト アクションと、その接続に一致した最初のモニター ルール。接続がモニター ルールに一致した場合、フィールドには接続を処理したルールの名前が表示され、その後にモニター ルール名が表示されます。

SSLServerName（Syslog のみ）

このフィールドは syslog フィールドとしてのみ存在します。Secure Firewall Management Center の Web インターフェイスにはありません。

クライアントが暗号化された接続を確立した相手側サーバーのホスト名。

[SSL セッション ID（SSL Session ID）]（syslog：SSLSessionID）

TLS/SSL ハンドシェイク時にクライアントとサーバー間でネゴシエートされた 16 進数セッション ID。

SSL ステータス（SSL Status）

暗号化された接続を記録した、[SSL の実際の動作（SSL Actual Action）]（SSL ルール、デフォルトアクション、または復号できないトラフィック アクション）に関連したアクション。[ロック（Lock）] アイコン（）は、SSL 証明書の詳細にリンクしています。証明書を利用できない場合（たとえば、TLS/SSL ハンドシェイク エラーにより接続がブロックされる場合）、ロック アイコンはグレー表示になります。

システムが暗号化された接続の復号化に失敗した場合、実行された [SSL の実際のアクション（SSL Actual Action）]（復号化できないトラフィック アクション）と [SSL 障害の理由（SSL Failure Reason）] が表示されます。たとえば、不明な暗号スイートによって暗号化されたトラフィックをシステムが検出し、それ以上のインスペクションをせずにこれを許可した場合、このフィールドには [復号しない（不明な暗号スイート）（Do Not Decrypt (Unknown Cipher Suite)）] が表示されます。

暗号化された接続の SSL ハンドシェイクが未完了であり、システムがトラフィックの復号に失敗した場合、[SSLステータス（SSL Status）] フィールドに「Unknown (Incomplete Handshake)」（不明（未完了のハンドシェイク））と表示されます。

このフィールドを検索するときは、[SSL の実際のアクション（SSL Actual Action）] および [SSL 障害の理由（SSL Failure Reason）] の値を 1 つ以上を入力して、システムが処理した暗号化されたトラフィック、または復号化に失敗したトラフィックを表示します。

[SSLサブジェクト/発行元国（SSL Subject/Issuer Country）]

このフィールドは Secure Firewall Management Center の Web インターフェイスのみで、検索フィールドとしてのみ使用できます。

暗号化証明書に関連付けられている件名または発行者の国に関する 2 文字の ISO 3166-1 アルファ 2 国コード。

[SSL チケット ID（SSL Ticket ID）]（syslog：SSLTicketID）

TLS/SSL ハンドシェイク時に送信されたセッション チケット情報の 16 進数のハッシュ値。

SSLURLCategory（syslog のみ）

暗号化接続でアクセスされた URL の URL カテゴリ

このフィールドは syslog フィールドとしてのみ存在します。Secure Firewall Management Center の Web インターフェイスでは、このフィールドの値が URL カテゴリ列に組み込まれます。

URLを参照してください。

[SSL バージョン（SSL Version）]（syslog：SSLVersion）

接続の暗号化に使用された TLS/SSL プロトコル バージョン。

- 不明
- SSLv2.0
- SSLv3.0

- TLSv1.0
- TLSv1.1
- TLSv1.2
- TLSv1.3

[TCPフラグ（TCP Flags）]（Syslog：TCPFlags）

NetFlow データから生成された接続において、接続で検出された TCP フラグ。

このフィールドを検索する場合は、TCP フラグのカンマ区切りリストを入力することで、これらのフラグが *1* つ以上あるすべての接続が表示されます。

時刻（Time）

システムが接続を接続サマリーに集約するために使用した5分間隔の終了時刻。このフィールドは検索できません。

[合計パケット数（Total Packets）]

このフィールドは検索フィールドとしてのみ使用できます。

接続で送信された合計パケット数。

[トラフィック（KB）（Traffic (KB)）]

このフィールドは検索フィールドとしてのみ使用できます。

接続で送信されたデータの総量（キロバイト単位）。

トンネル/プレフィルタ ルール (Syslog:Tunnel または Prefilter Rule)

トンネル ルール、プレフィルタ ルール、または接続を処理したプレフィルタ ポリシーのデフォルト アクション。

[URL、URLカテゴリ、およびURLレピュテーション（URL, URL Category, and URL Reputation）]（syslog：URL、URLCategory および SSLURLCategory、URLReputation）

セッション中にモニター対象のホストによって要求された URL と、関連付けられたカテゴリおよびレピュテーション（利用できる場合）。

URL カテゴリとレピュテーションを表示するイベントでは、該当する URL ルールをアクセス コントロール ポリシーに含め、[URL] タブに URL カテゴリと URL レピュテーションを使用してルールを設定する必要があります。

URL ルールと一致する前に接続が処理される場合、URL カテゴリとレピュテーションはイベントに表示されません。

[URL] 列が空で、DNS フィルタリングが有効になっている場合、[DNS Query] フィールドにドメインが表示され、[URL Category] と [URL Reputation] の値がドメインに適用されます。

システムが TLS/SSL アプリケーションを識別またはブロックする場合、要求された URL は暗号化トラフィック内にあるため、システムは、SSL 証明書に基づいてトラフィックを

識別します。したがって TLS/SSL アプリケーションの場合、このフィールドは証明書に含まれる一般名を表示します。

上記は **SSLURLCategory** も参照してください。

[ユーザーエージェント（User Agent）]（Syslog：UserAgent）

接続で検出された HTTP トラフィックから取得したユーザー エージェント文字列アプリケーションの情報。

[VLAN ID]（Syslog：VLAN_ID）

接続をトリガーしたパケットに関連付けられている最内部 VLAN ID。

VPN Action

接続に関連付けられた VPN アクション。

値は以下のとおりです。

- [暗号化（Encrypt）]：VPN は、ログに記録された接続のトラフィックを暗号化します。接続を暗号化する VPN ピアの IP アドレスを確認するには、[暗号化ピア（Encrypt Peer）] 列を参照してください。
- [復号（Decrypt）]：VPNは、ログに記録された接続のトラフィックを復号します。接続を復号する VPN ピアの IP アドレスを確認するには、[復号ピア（Decrypt Peer）] 列を参照してください。
- [VPNルーティング（VPN Routing）]：トラフィックは VPN トンネルを通過します。VPNは、接続の開始時に復号を実行し、接続の終了時に暗号化を実行します。接続を暗号化および復号する VPN ピアの IP アドレスを確認すには、[暗号化ピア（Encrypt Peer）] 列および [復号ピア（Decrypt Peer）] 列を参照してください。

Webアプリケーション (Syslog: WebApplication)

接続で検出された HTTP トラフィックの内容または要求された URL を表す Web アプリケーション。

Web アプリケーションがイベントの URL に一致しない場合、そのトラフィックは通常、参照先のトラフィックです（アドバタイズメントのトラフィックなど）。システムは、参照先のトラフィックを検出すると、参照元のアプリケーションを保存し（可能な場合）、そのアプリケーションを Web アプリケーションとして表示します。

HTTP トラフィックに含まれる特定の Web アプリケーションをシステムが特定できなかった場合、このフィールドには [Web ブランジング（Web Browsing）] と表示されます。

Web アプリケーション カテゴリおよびタグ（Web Application Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

接続およびセキュリティ関連の接続イベントのフィールドについて

Secure Firewall Management Center の Web インターフェイスでは、[分析（Analysis）] > [接続（Connections）] サブメニューのテーブル形式とグラフィカルなワークフローを使用して、接続イベントとセキュリティ関連の接続イベントを表示したり検索することができます。

（注） 各セキュリティ関連の接続イベントには、同一の、個別に保存された接続イベントがあります。すべてのセキュリティ関連の接続イベントには、自動入力される [セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）] フィールドがあります。

個別のイベントで使用可能な情報は、システムがいつ、なぜ、どのようにして接続をログに記録したかによって異なります。

検索の制約

検索ページのアスタリスク（*）が付いたフィールドは、接続グラフおよび接続サマリーを制約します。接続グラフは接続サマリーに基づいているため、接続サマリーを制約しているのと同じ条件が接続グラフを制約します。無効な検索条件を使用して接続サマリーを検索し、カスタム ワークフローの接続サマリー ページを使用して結果を見る場合、無効な条件には適用不可（N/A）としてラベルが付けられ、取り消し線が引かれます。

syslog フィールド

ほとんどのフィールドは Secure Firewall Management Center Web インターフェイス内のほか、syslog メッセージとしても表示されます。同等にリストされている syslog のないフィールドは、syslog メッセージでは使用可能できません。いくつかのフィールドは（前述のように）syslog のみであり、その他のいくつかのフィールドは syslog メッセージ内の個別のフィールドですが、Web インターフェイス内では統合されたフィールドか、その逆です。

イニシエータ/レスポンダ、送信元/接続先、および送信者/受信者フィールドに関する注意

表 *106 :* 用語の比較

フィールド	イベント タイプ	説明
イニシエータ/レスポンダ	接続	接続のイニシエータ/レスポンダ。 接続のイニシエータは、侵入の送信元またはマルウェアファイルの送信者と同じである必要はありません。

フィールド	イベントタイプ	説明
Source/Destination	Intrusion	攻撃の送信元/接続先。 侵入イベントの送信元は、接続のイニシエータまたはレスポンダです。
送信者/受信者 （Sending..., Receiving...）	ファイル、マルウェア	ファイルまたはマルウェアの送信者/受信者。 ファイルはアップロードまたはダウンロードされる可能性があるため、ファイルの送信者は必ずしも接続のイニシエータではありません。

接続イベントの理由

接続イベントの [理由（Reason）] フィールドには、次の状況で接続がロギングされた理由が表示されます。

理由	説明
コンテンツ制限（Content Restriction）	セーフサーチ機能に関連したコンテンツ制限を実施するために、パケットが変更されました。
[DNS ブロック（DNS Block）]	ドメイン名とセキュリティインテリジェンスデータに基づいて、インスペクションなしで接続が拒否されました。[DNS ブロック（DNS Block）] の理由は、DNS ルール アクションに応じて、[ブロック（Block）]、[ドメインが見つかりません（Domain not found）]、[シンクホール（Sinkhole）] のアクションと対として組み合わされます。
DNS モニタ（DNS Monitor）	システムはドメイン名とセキュリティインテリジェンスデータに基づいて接続を拒否するはずでしたが、システムは接続を拒否するのではなくモニターするように設定されています。

理由	説明
エレファントフロー	接続は、エレファントフローと見なすのに十分な大きさです。このフローは、システム全体のパフォーマンスに影響を与えるのに十分な大きさです。デフォルトでは、エレファントフローとは1GB/10秒を超えるフローです。**system support elephant-flow-detection** コマンドを使用して、Threat Defense CLI でエレファントフローを識別するためのバイトしきい値と時間しきい値を調整できます。詳細については、Cisco Secure Firewall Threat Defense コマンドリファレンス [英語] を参照してください。 （注） フローは、バイトと時間の両方のしきい値を超えた場合にのみ、エレファントフローと見なされます。 カスタムダッシュボードを作成して、エレファントフローと他の相互に関連するメトリック（Snort、システム、物理コアなどの CPU メトリックなど）を関連付けることができます。詳細については、「システムモニタリングとトラブルシューティング」の章を参照してください。
エレファントフローの除外（Elephant Flow Exempted）	エレファントフローが検出され、それが、修復から除外する必要があるフローに関して定義されている L4 ACL ルールに一致する場合。
[ファイルブロック（File Block）]	ファイルまたはマルウェア ファイルが接続に含まれており、システムがその送信を防いでいます。[ファイルブロック（File Block）] の理由は必ず [ブロック（Block）] アクションと対として組み合わされます。
ファイル カスタム検出（File Custom Detection）	カスタム検出リストにあるファイルが接続に含まれており、システムがその送信を防いでいます。
[ファイルモニタ（File Monitor）]	システムが接続において特定のファイルの種類を検出しました。
[ファイル復帰許可（File Resume Allow）]	ファイル送信がはじめに [ファイルブロック（Block Files）] ルールまたは [マルウェアブロック（Block Malware）] ファイル ルールによってブロックされました。ファイルを許可する新しいアクセス コントロール ポリシーが展開された後、HTTP セッションが自動的に再開しました。この理由はインライン展開のみで表示されます。
[ファイル復帰ブロック（File Resume Block）]	ファイル送信がはじめに [ファイル検出（Detect Files）] ルールまたは [マルウェアクラウドルックアップ（Malware Cloud Lookup）] ファイル ルールによって許可されました。ファイルをブロックする新しいアクセス コントロール ポリシーが展開された後、HTTP セッションが自動的に停止しました。この理由はインライン展開のみで表示されます。

理由	説明
インテリジェント アプリケーション バイパス（Intelligent App Bypass）	インテリジェント アプリケーション バイパス（IAB）モード： • アクションが [信頼（Trust）] の場合、IAB はバイパス モードでした。一致するトラフィックは、追加のインスペクションなしで通過しました。 • アクションが [許可（Allow）] の場合、IAB はテスト モードでした。一致するトラフィックは、追加のインスペクションに使用できました。
[侵入ブロック（Intrusion Block）]	Snort2 エンジン：接続で検出されたエクスプロイト（侵入ポリシー違反）をシステムがブロックしたか、ブロックするはずでした。[侵入ブロック（Intrusion Block）] の理由は、ブロックされたエクスプロイトの場合は [ブロック（Block）]、ブロックされるはずだったエクスプロイトの場合は [許可（Allow）] のアクションと対として組み合わされます。 Snort3 エンジン：「ドロップするはず」の結果がある場合、接続イベントの理由は「侵入ブロック」ではなく空白です。「ドロップするはず」のイベントは、入力される接続イベントの理由に関して「許可」と同じように扱われます。
[侵入モニター（Intrusion Monitor）]	接続で検出されたエクスプロイトをシステムが検出したものの、ブロックしなかったことを示します。これは、トリガーされた侵入ルールの状態が [イベントを生成する（Generate Events）] に設定されている場合に発生します。
[IPブロック（IP Block）]	IP アドレスとセキュリティ インテリジェンス データに基づいて、インスペクションなしで接続が拒否されました。[IPブロック（IP Block）] の理由は必ず [ブロック（Block）] のアクションと対として組み合わされます。
IP モニタ（IP Monitor）	システムは IP アドレスとセキュリティ インテリジェンス データに基づいて接続を拒否するはずでしたが、システムは接続を拒否するのではなくモニターするように設定されています。
SSL ブロック（SSL Block）	システムが TLS/SSL インスペクション設定に基づいて暗号化接続をブロックしました。[SSL ブロック（SSL Block）] の理由は必ず [ブロック（Block）] のアクションと対として組み合わされます。
[URLブロック（URL Block）]	URL とセキュリティ インテリジェンス データに基づいて、インスペクションなしで接続が拒否されました。[URLブロック（URL Block）] の理由は必ず [ブロック（Block）] のアクションと対として組み合わされます。
URL モニタ（URL Monitor）	システムは URL とセキュリティ インテリジェンス データに基づいて接続を拒否するはずでしたが、システムは接続を拒否するのではなくモニタするように設定されています。

理由	説明
ユーザー バイパス（User Bypass）	最初にユーザのHTTP要求をブロックしましたが、ユーザのクリックによって警告ページからサイトを表示しました。[ユーザーバイパス（User Bypass）]の理由は必ず[許可（Allow）]のアクションと対として組み合わされます。

接続イベント フィールドの入力の要件

接続イベント、セキュリティ関連接続イベント、または接続サマリーで利用可能な情報は、いくつかの要因によって異なります。

アプライアンス モデルおよびライセンス

多くの機能は、ターゲットデバイスで特定のライセンス付与対象の機能を有効にしなければ使用できません。また、一部のモデルでしか使用できない機能も多くあります。

トラフィックの特性

システムは、ネットワーク トラフィック内に存在する（および検出可能な）情報だけを報告します。たとえば、イニシエータ ホストに関連付けられているユーザがいない、またはプロトコルが DNS、HTTP、または HTTPS ではない接続で検出される参照先ホストがいない可能性があります。

発信元/検出方法：トラフィック ベースの検出と NetFlow

NetFlow 専用フィールドを除き、NetFlow レコードで利用可能な情報は、トラフィック ベースの検出によって生成される情報よりも限定されます。NetFlowデータと管理対象デバイスデータの違いを参照してください。

評価ステージ

各タイプのトラフィックのインスペクションと制御は、最大限の柔軟性とパフォーマンスを引き出すために最も意味がある局面で実行されます。

たとえば、システムは、さらなるリソース集中型評価を行う前に、セキュリティ インテリジェンスを強制します。接続がセキュリティ インテリジェンスによってブロックされた場合、結果として生成されるイベントには、その後の評価によってシステムで収集されることになっていた情報（ユーザ ID など）が含まれません。

ロギング方法：接続の開始または終了

システムが接続の検出時にその接続の開始または終了（またはその両方）をログに記録できるかどうかは、システムがその接続をどのように検出して処理するように設定されているかによって異なります。

接続開始イベントには、セッション期間にわたってトラフィックを調査して判別しなければならない情報が伴ってません（送信されたデータの合計量や、接続の最終パケットのタイムスタンプなど）。また、接続開始イベントにセッションのアプリケーションや URL トラフィック

に関する情報が伴っている保証もなく、セッションの暗号化に関する詳細は含まれていません。通常、ブロックされる接続については、接続開始イベントのログへの記録が唯一のオプションになります。

接続イベント タイプ：個々またはサマリー

接続サマリーには、集約された接続に関連付けられたすべての情報が含まれているわけではありません。たとえば、接続の概要に集約される接続にはクライアント情報が使用されないため、概要にはクライアント情報は含まれません。

接続グラフは、接続終了ログのみを使用する接続サマリーのデータに基づいていることに注意してください。接続開始データだけをロギングするようにシステムが設定されている場合、接続グラフと接続サマリーのイベント ビューにはデータが表示されません。

（注） セキュリティ関連の接続イベントには、セキュリティ インテリジェンス イベントやその他の接続イベント（侵入イベントやマルウェアイベントをトリガーしたものなど）が含まれます。[セキュリティ インテリジェンスの概要（Security Intelligence Summary）] ワークフローは、セキュリティ インテリジェンス カテゴリを持たないセキュリティ関連の接続イベントをグループ化し、その数を [セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）] の値なしで表示します。

その他の設定

接続のロギングに影響するその他の設定には以下のものが含まれますが、これらに限定されるわけではありません。

- Active Directory ドメイン コントローラで認証するユーザに関連付けられている接続では、ISE が設定されている場合にのみ、ISE 関連のフィールドにデータが入力されます。接続イベントには、LDAP、RADIUS、RSA ドメイン コントローラで認証するユーザーの ISE データは含まれません。
- [セキュリティグループタグ（Security Group Tag）]（SGT）フィールドにデータが入力されるのは、ISE をアイデンティティ ソースとして設定した場合、またはカスタム SGT ルール条件を追加した場合のみです。
- プレフィルタ関連のフィールド（セキュリティ ゾーン フィールドのトンネル ゾーン情報を含む）には、プレフィルタ ポリシーで処理される接続の場合にのみ、データが入力されます。
- TLS/SSL 関連のフィールドには、復号ポリシーで処理される暗号化接続の場合にのみ、データが入力されます。トラフィックの復号化が必要ない場合、Do Not Decrypt ルールの操作を使用して、フィールドの値を表示することができます。
- ファイル情報フィールドには、ファイル ポリシーと関連付けられたアクセス コントロール ルールによってログに記録される接続の場合にのみ、データが入力されます。

- 侵入情報フィールドには、侵入ポリシーに関連付けられているアクセス コントロール ルールあるいはデフォルト アクションによってログに記録される接続の場合にのみ、データが入力されます。
- QoS 関連のフィールドには、レート制限が適用される接続の場合にのみ、データが入力されます。
- [理由（Reason）] フィールドには、特定の場合にのみデータが入力されます（ユーザがインタラクティブ ブロック設定をバイパスしている場合など）。
- [ドメイン（Domain）] フィールドが表示されるのは、マルチテナンシー用に Secure Firewall Management Center を設定した場合のみです。
- アクセス コントロール ポリシーの詳細設定では、HTTP セッションのモニタ対象ホストによって要求された URL ごとにシステムが接続ログに保存する文字数を制御できます。この設定を使用して URL のロギングを無効化する場合、システムは接続ログで個々の URL を表示しませんが、カテゴリとレピュテーション データは参照できます（存在する場合）。
- URL カテゴリとレピュテーションを表示する接続イベントでは、該当する URL ルールをアクセス コントロール ポリシーに含め、[URL] タブに URL カテゴリと URL レピュテーションを使用してルールを設定する必要があります。URL ルールと一致する前に接続が処理される場合、URL カテゴリとレピュテーションはイベントに表示されません。

関連トピック

NetFlow データと管理対象デバイス データの違い

接続イベント フィールドで利用可能な情報

このトピックの表に、システムが接続およびセキュリティ インテリジェンスのフィールドに値を読み込むことができるタイミングを示します。表の列は、次のイベント タイプを示しています。

- [発信元：直接（Origin: Direct）]：システム管理対象デバイスで検出および処理される接続を表すイベント。
- [発信元：NetFlow（Origin: NetFlow）]：NetFlow エクスポータでエクスポートされる接続を表すイベント。
- [ロギング：開始（Logging: Start）]：開始時にログに記録される接続を表すイベント。
- [ロギング：終了（Logging: End）]：終了時にログに記録される接続を表すイベント。

表内の「はい（yes）」は、システムが接続イベント フィールドに値を読み込む必要があることを意味するものではなく、読み込むことができることを意味します。システムは、ネットワーク トラフィック内に存在する（および検出可能な）情報だけを報告します。たとえば、TLS/SSL 関連のフィールドには、復号ポリシーによって処理される暗号化された接続のレコードについてのみ値が読み込まれます。

接続イベントフィールド	発信元：直接	発信元：**NetFlow**	ロギング：開始（**Logging: Start**）	ロギング：終了（**Logging: End**）
アクセス コントロール ポリシー（Access Control Policy）	はい	いいえ	はい	はい
アクセス コントロール ルール（Access Control Rule）	はい	いいえ	はい	はい
操作（Action）	はい	いいえ	はい	はい
アプリケーションプロトコル	はい	はい	利用可能な場合	はい
アプリケーション プロトコル カテゴリとタグ（Application Protocol Category & Tag）	はい	いいえ	利用可能な場合	はい
アプリケーションのリスク（Application Risk）	はい	いいえ	利用可能な場合	はい
ビジネスとの関連性（Business Relevance）	はい	いいえ	利用可能な場合	はい
クライアント（Client）	はい	いいえ	利用可能な場合	はい
クライアントカテゴリとタグ（Client Category & Tag）	はい	いいえ	利用可能な場合	はい
クライアントバージョン（Client Version）	はい	いいえ	利用可能な場合	はい
接続（Connections）	はい	はい	いいえ	はい
カウント（Count）	はい	はい	はい	はい
宛先ポート/ICMP タイプ（Destination Port/ICMP Type）	はい	はい	はい	はい
宛先 SGT（Destination SGT）	はい	いいえ	はい	はい
デバイス	はい	はい	はい	はい
ドメイン（Domain）	はい	はい	はい	はい
DNS クエリ（DNS Query）	はい	いいえ	はい	はい

接続イベントフィールド	発信元：直接	発信元：**NetFlow**	ロギング：開始（**Logging: Start**）	ロギング：終了（**Logging: End**）
DNS レコードタイプ（DNS Record Type）	はい	いいえ	はい	はい
DNS レスポンス（DNS Response）	はい	いいえ	はい	はい
DNS シンクホール名（DNS Sinkhole Name）	はい	いいえ	はい	はい
DNS TTL	はい	いいえ	はい	はい
出力インターフェイス（Egress Interface）	はい	いいえ	はい	はい
出力セキュリティゾーン（Egress Security Zone）	はい	いいえ	はい	はい
エンドポイントロケーション（Endpoint Location）	はい	いいえ	はい	はい
エンドポイントプロファイル（Endpoint Profile）	はい	いいえ	はい	はい
ファイル（Files）	はい	いいえ	いいえ	はい
最初のパケット（First Packet）	はい	はい	はい	はい
HTTP リファラ（HTTP Referrer）	はい	いいえ	いいえ	はい
HTTP 応答コード（HTTP Response Code）	はい	いいえ	はい	はい
入力インターフェイス（Ingress Interface）	はい	いいえ	はい	はい
入力セキュリティゾーン（Ingress Security Zone）	はい	いいえ	はい	はい
イニシエータバイト数（Initiator Bytes）	はい	はい	有用でない	はい
イニシエータの国（Initiator Country）	はい	いいえ	はい	はい
イニシエータ IP（Initiator IP）	はい	はい	はい	はい

接続イベントフィールド	発信元：直接	発信元：**NetFlow**	ロギング：開始（**Logging: Start**）	ロギング：終了（**Logging: End**）
イニシエータパケット（Initiator Packets）	はい	はい	有用でない	はい
イニシエータユーザ（Initiator User）	はい	はい	はい	はい
侵入イベント	はい	いいえ	いいえ	はい
侵入ポリシー（Intrusion Policy）	はい	いいえ	はい	はい
IOC（侵害の兆候）（IOC (Indication of Compromise)）	はい	いいえ	はい	はい
最後のパケット（Last Packet）	はい	はい	いいえ	はい
NetBIOS ドメイン（NetBIOS Domain）	はい	いいえ	はい	はい
NetFlow 送信元/宛先の自律システム（NetFlow Source/Destination Autonomous System）	いいえ	はい	いいえ	はい
NetFlow 送信元/宛先のプレフィックス（NetFlow Source/Destination Prefix）	いいえ	はい	いいえ	はい
NetFlow 送信元/宛先 TOS（NetFlow Source/Destination TOS）	いいえ	はい	いいえ	はい
NetFlow SNMP 入出力（NetFlow SNMP Input/Output）	いいえ	はい	いいえ	はい
ネットワーク分析ポリシー（Network Analysis Policy）	はい	いいえ	はい	はい
クライアントのオリジナル国（Original Client Country）	はい	いいえ	はい	はい
クライアントのオリジナル IP（Original Client IP）	はい	いいえ	はい	はい

接続イベントフィールド	発信元：直接	発信元：**NetFlow**	ロギング：開始（**Logging: Start**）	ロギング：終了（**Logging: End**）
プレフィルタポリシー（Prefilter Policy）	はい	いいえ	はい	はい
QoS が適用されたインターフェイス（QoS-Applied Interface）	はい	いいえ	いいえ	はい
QoS がドロップされたイニシエータのバイト数（QoS-Dropped Initiator Bytes）	はい	いいえ	いいえ	はい
QoS がドロップされたイニシエータのパケット数（QoS-Dropped Initiator Packets）	はい	いいえ	いいえ	はい
QoS がドロップされたレスポンダのバイト数（QoS-Dropped Responder Bytes）	はい	いいえ	いいえ	はい
QoS がドロップされたレスポンダのパケット数（QoS-Dropped Responder Packets）	はい	いいえ	いいえ	はい
QoS ポリシー（QoS Policy）	はい	いいえ	いいえ	はい
QoS ルール（QoS Rule）	はい	いいえ	いいえ	はい
理由	はい	いいえ	はい	はい
参照ホスト（Referenced Host）	はい	いいえ	いいえ	はい
レスポンダバイト数（Responder Bytes）	はい	はい	有用でない	はい
レスポンダの国（Responder Country）	はい	いいえ	はい	はい
レスポンダ IP（Responder IP）	はい	はい	はい	はい
レスポンダパケット（Responder Packets）	はい	はい	有用でない	はい

接続イベントフィールド	発信元：直接	発信元：**NetFlow**	ロギング：開始（**Logging: Start**）	ロギング：終了（**Logging: End**）
セキュリティコンテキスト（ASA のみ）（Security Context (ASA only)）	はい	いいえ	はい	はい
セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）	はい	いいえ	はい	はい
送信元デバイス（Source Device）	はい	はい	はい	はい
送信元ポート/ICMP タイプ（Source Port/ICMP Type）	はい	はい	はい	はい
送信元 SGT（Source SGT）	はい	いいえ	はい	はい
SSL 証明書ステータス（SSL Certificate Status）	はい	いいえ	いいえ	はい
SSL 暗号スイート（SSL Cipher Suite）	はい	いいえ	いいえ	はい
SSL フローエラー（SSL Flow Error）	はい	いいえ	いいえ	はい
SSL フローフラグ（SSL Flow Flags）	はい	いいえ	いいえ	はい
SSL フローメッセージ（SSL Flow Messages）	はい	いいえ	いいえ	はい
復号ポリシー	はい	いいえ	いいえ	はい
復号ルール	はい	いいえ	いいえ	はい
SSL セッション ID（SSL Session ID）	はい	いいえ	いいえ	はい
SSL ステータス（SSL Status）	はい	いいえ	いいえ	はい
SSL バージョン（SSL Version）	はい	いいえ	いいえ	はい
TCP フラグ（TCP Flags）	いいえ	はい	いいえ	はい
Time	はい	はい	いいえ	はい

接続イベントフィールド	発信元：直接	発信元：NetFlow	ロギング：開始（Logging: Start）	ロギング：終了（Logging: End）
トンネル/プレフィルタルール（Tunnel/Prefilter Rule）	はい	いいえ	はい	はい
URL	はい	いいえ	利用可能な場合	はい
URL カテゴリ（URL Category）	はい	いいえ	利用可能な場合	はい
URLレピュテーション（URL Reputation）	はい	いいえ	利用可能な場合	はい
ユーザエージェント（User Agent）	はい	いいえ	いいえ	はい
VLAN ID（Admin. VLAN ID）	はい	いいえ	はい	はい
Web アプリケーション	はい	いいえ	利用可能な場合	はい
Web アプリケーションのカテゴリとタグ（Web Application Category & Tag）	はい	いいえ	利用可能な場合	はい

接続およびセキュリティ関連の接続イベントテーブルの使用

Secure Firewall Management Center を使用して、接続イベントまたはセキュリティ関連の接続イベントのテーブルを表示することができます。ここでユーザーは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

接続グラフにアクセスしたときに表示されるページは、使用するワークフローによって異なります。イベントのテーブル ビューで終わる事前定義されたワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

接続またはセキュリティ インテリジェンス ワークフロー テーブルを使用すると、たくさんの一般的なアクションを実行できます。

ドリルダウンページで接続イベントを制約する場合、同一のイベントからのパケット数とバイト数が合計されることに注意してください。ただし、カスタム ワークフローを使用しており、ドリルダウン ページに [カウント（Count）] カラムを追加していない場合、イベントは個別に表示され、パケット数とバイト数は合計されません。

システムが生成した接続イベントが 25 個を超えると、[接続イベント（Connection Events）] テーブル ビューに、使用可能なイベントのページ数ではなく、「1 ofMany」と表示されます。

始める前に

このタスクを実行するには、管理者ユーザーまたはセキュリティ アナリスト ユーザーである必要があります。

手順

ステップ 1 次のいずれかを選択します。

- **[分析（Analysis）] > [接続（Connections）] > [イベント（Events）]**（接続イベントの場合）
- **[分析（Analysis）] > [接続（Connections）] > [セキュリティ関連のイベント（Security-Related Events）]**

（注） テーブルの代わりに接続グラフが表示された場合、ワークフロータイトルで [(ワークフローの切り替え)（(switch workflow)）] をクリックし、事前定義された [接続イベント（Connection Events）] ワークフローまたはカスタム ワークフローを選択します。事前定義されたすべての接続イベント（接続グラフを含む）は、接続のテーブル ビューで終了することに注意してください。

ステップ 2 次の選択肢があります。

- 時間範囲：時間範囲を調整（イベントが表示されない場合に役立ちます）する方法については、時間枠の変更 （833 ページ）を参照してください。
- データソース：データがセキュリティ分析とロギング（オンプレミス）を使用してリモートで保存されていて、データソースを変更する正当な理由がある場合は、データソースを選択します。このオプションに関する重要な情報については、Secure Network Analytics アプライアンスに保存されている接続イベントを使用した Secure Firewall Management Center での作業 （819 ページ）を参照してください。
- フィールド名：テーブルのカラムの内容について詳しく調べるには、接続およびセキュリティ関連の接続イベントフィールド （902 ページ）を参照してください。

  ヒント イベントのテーブルビューでは、デフォルトでこれらのフィールドは非表示にされています。表示されるフィールドを変更するには、任意の列名の [x] をクリックしてフィールド選択ツールを表示します。

- 追加情報：システムの外部にある利用可能なソース内のデータを表示するには、イベント値を右クリックします。表示されるオプションはデータ タイプによって異なり、パブリッ

クソースが含まれます。他のソースは設定したリソースによって異なります。詳細については、Webベースのリソースを使用したイベントの調査（763ページ）を参照してください。

- 外部インテリジェンス：イベントに関する情報を収集するには、テーブルでイベントの値を右クリックして、シスコまたはサードパーティのインテリジェンス ソースを選択します。たとえば、不審なIPアドレスに関する詳細情報をCisco Talosから入手できます。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。詳細については、Webベースのリソースを使用したイベントの調査（763ページ）を参照してください。
- ホストプロファイル：IPアドレスのホストプロファイルを表示するには、[ホストプロファイル（Host Profile）]をクリックします。アクティブな侵害の兆候（IOC）タグのあるホストの場合は、IPアドレスの横に表示される[侵害を受けたホスト（Compromised Host）]をクリックします。
- ユーザープロファイル：ユーザーID情報を表示するには、[ユーザーID（User Identity）]の隣に表示される[ユーザー（User）]アイコン、またはIOCに関連付けられているユーザーの場合は[レッドユーザー（Red User）]をクリックします。
- ファイルおよびマルウェア：接続で検出されたまたはブロックされたマルウェアを含むファイルを表示するには、[ファイルの表示（View Files）]をクリックし、接続で検出されたファイルとマルウェアの表示（937ページ）の説明に従って続行します。
- 侵入イベント：接続に関連付けられている侵入イベントを優先順位や影響とともに表示するには、[侵入イベント（Intrusion Events）]列の[侵入イベント（Intrusion Events）]をクリックして、接続に関連付けられた侵入イベントの表示（939ページ）の説明に従って続行します。

  ヒント 1つまたは複数の接続に関連付けられた侵入イベント、ファイルイベント、またはマルウェアイベントをすばやく表示するには、テーブルのチェックボックスを使用して接続を選択し、[ジャンプ（Jump to）]ドロップダウン リストから該当するオプションを選択します。セキュリティインテリジェンスによりブロックされている接続に関連するファイルまたは侵入が、アクセス制御ルールの評価の前にブロックされることによって、1つも存在しない可能性があることに注意してください。ブロックではなく、接続をモニターするようにセキュリティインテリジェンスを設定した場合に限り、セキュリティ インテリジェンス イベントに関するこの情報が表示されます。

- 証明書：接続を暗号化するために使用される利用可能な証明書についての詳細を表示するには、[SSLステータス（SSL Status）]列の[有効なロック（Enabled Lock）]をクリックします。
- 制約：表示される列を制約するには、非表示にする列の見出しにある[閉じる（Close）]（✕）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）]をクリックします。

ヒント 他のカラムを表示または非表示にするには、[適用（Apply）]をクリックする前に、該当するチェックボックスをオンまたはオフにします。無効になったカラムをビューに再び追加するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）]の下のカラム名をクリックします。

- イベントの削除：（セキュリティ関連の接続イベントテーブルのみ）現在の制約されたビューにある一部またはすべての項目を削除するには、削除する項目の横にあるチェックボックスをオンにして、[削除（Delete）] または [すべて削除（Delete All）] をクリックします。
- ドリル ダウン：ドリルダウン ページの使用 （818 ページ）を参照してください。

  ヒント ロギングされた接続に一致した複数のモニター ルールのうち 1 つにドリル ダウンするには、[*N* モニター ルール（N Monitor Rules）] の値をクリックします。表示されるポップアップ ウィンドウで、接続イベントを抑制するために使用するモニター ルールをクリックします。

- このページに移動する：ワークフロー ページのトラバーサル ツール （815 ページ）を参照してください。
- ページ間で移動する：現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。
- イベント ビュー間で移動する：関連するイベントを表示するためその他のイベント ビューに移動するには、[ジャンプ（Jump to）] をクリックし、ドロップダウン リストからイベント ビューを選択します。
- ソート：ワークフローでデータをソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。

関連トピック

概要：ワークフロー （797 ページ）
イベント ビューの設定 （241 ページ）

接続で検出されたファイルとマルウェアの表示

1 つまたは複数のアクセス コントロール ルールにファイル ポリシーを関連付けると、システムは一致するトラフィックのファイル（マルウェアを含む）を検出できます。[分析（Analysis）] > [接続（Connections）] メニュー オプションを使用して、各ルールによってロギングされた接続と関連付けられているファイルイベント（存在する場合）を確認します。ファイルリストの代わりに、Secure Firewall Management Center はファイル表示（  ）を [ファイル（Files）] 列に表示します。ファイル表示の数字は、その接続で検出またはブロックされたファイル数（マルウェアファイルを含む）を示します。

すべてのファイルおよびマルウェア イベントが接続に関連付けられるわけではありません。具体的には次のとおりです。

- Cisco Secure Endpoint によって検出されたマルウェアイベント（「エンドポイントベースのマルウェアイベント」）は接続に関連付けられません。これらのイベントはCisco Secure Endpoint 展開からインポートされます。
- IMAP に対応した電子メール クライアントの多くは単一 IMAP セッションを使用し、それはユーザがアプリケーションを終了したときに終了します。長時間接続はシステムによってロギングされますが、セッションでダウンロードされたファイルは、そのセッションが終了するまで接続に関連付けられません。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

始める前に

このタスクを実行するには、管理者ユーザーまたはセキュリティ アナリスト ユーザーである必要があります。

手順

ステップ 1 [分析（Analysis）] > [接続（Connections）] の順に移動して、関連するオプションを選択します。

ステップ 2 接続イベントテーブルを使用している場合、[ファイル表示（View Files）] をクリックします。ポップアップ ウィンドウが表示され、接続で検出されたファイルのリストとともに、そのタイプと、該当する場合はマルウェア処理が示されます。

ステップ 3 次の選択肢があります。

- 表示：ファイルイベントのテーブルビューを表示するには、[ファイルの表示（File's View）] をクリックします。
- 表示：マルウェアイベントのテーブルビューに詳細を表示するには、[マルウェアファイルの表示（Malware File's View）] をクリックします。
- 追跡：ネットワークを経由するファイルの伝送を追跡するには、[ファイルのトラジェクトリ（File's Trajectory）] をクリックします。
- 表示：接続で検出されたファイルやマルウェア防御によって検出されたマルウェアイベント（「ネットワークベースのマルウェアイベント」）のすべての詳細を表示するには、[ファイルイベントの表示（View File Events）] または [マルウェアイベントの表示（View Malware Events）] をクリックします。

関連トピック

概要：ワークフロー （797 ページ）
イベント ビューの設定 （241 ページ）

接続に関連付けられた侵入イベントの表示

アクセス コントロール ルールまたはデフォルト アクションに侵入ポリシーを関連付けると、システムは一致するトラフィックのエクスプロイトを検出できます。[分析（Analysis）] > [接続（Connections）] メニュー オプションを使用して、ロギングされた接続と関連付けられている侵入イベント（存在する場合）、およびそれらのイベントの優先順位と影響を確認します。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

始める前に

このタスクを実行するには、管理者ユーザーまたはセキュリティ アナリスト ユーザーである必要があります。

手順

ステップ 1 [分析（Analysis）] > [接続（Connections）] の順に移動して、関連するオプションを選択します。

ステップ 2 接続イベントテーブルを使用する場合、[侵入イベント（Intrusion Events）] 列の [侵入イベント（Intrusion Events）] をクリックします。

ステップ 3 表示されるポップアップ ウィンドウで、以下のオプションを選択できます。

- パケットビューで詳細を表示するには、[リストされたイベントの表示（Listed Event's View）] をクリックします。
- [侵入イベントの表示（View Intrusion Events）] をクリックして、接続に関連付けられた侵入イベントすべての詳細を表示します。

関連トピック

概要：ワークフロー （797 ページ）
イベント ビューの設定 （241 ページ）

暗号化接続の証明書の詳細

[分析（Analysis）] > [接続（Connections）] メニューを使用して、システムで処理される接続を暗号化するために使用される公開キー証明書（使用可能な場合）を表示できます。証明書には次の情報が含まれています。

表 *107*：暗号化接続の証明書の詳細

属性	説明
件名/発行元共通名（Subject/Issuer Common Name）	証明書のサブジェクトまたは証明書発行元のホストおよびドメイン名。

属性	説明
件名/発行元組織（Subject/Issuer Organization）	証明書のサブジェクトまたは証明書発行元の組織。
件名/発行元組織ユニット（Subject/Issuer Organization Unit）	証明書のサブジェクトまたは証明書発行元の部門。
有効期間の開始/終了（Not Valid Before/After）	証明書の有効期間。
シリアル番号（Serial Number）	発行元 CA によって割り当てられたシリアル番号。
証明書フィンガープリント（Certificate Fingerprint）	証明書の認証に使用する SHA ハッシュ値。
公開キーフィンガープリント（Public Key Fingerprint）	証明書に含まれる公開キーの認証に使用する SHA ハッシュ値。

関連トピック

概要：ワークフロー （797 ページ）
イベント ビューの設定 （241 ページ）

[接続サマリー（Connection Summary）] ページの表示

[接続サマリー（Connection Summary）] ページは、接続イベントの検索によって制限されたカスタム ロールを持ち、[接続サマリー（Connection Summary）] ページへのメニュー ベースの明示的なアクセスを許可されたユーザーにのみ表示されます。このページは、監視対象ネットワーク上のアクティビティをさまざまな条件で整理したグラフを表示します。たとえば [一定期間の接続数（Connections over Time）] グラフでは、選択した間隔における監視対象ネットワーク上の接続の合計数が表示されます。

接続グラフでできる操作と同じことが、接続サマリーのグラフでも、ほぼすべてできます。ただし、[接続の概要（Connection Summary）] ページのグラフは集約データに基づいているため、グラフの基になっている個々の接続イベントを調べることはできません。つまり、接続サマリーのグラフから接続データのテーブル ビューにドリルダウンすることはできません。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[概要（Overview）] > [概要（Summary）] > [接続の概要（Connection Summary）]**を選択します。

ステップ 2 [デバイスの選択（Select Device）] リストから、サマリーを表示したいデバイスを選択するか、もしくはすべてのデバイスのサマリーを表示するために [すべて（All）] を選択します。

ステップ 3 グラフ接続の操作および分析を行うには、接続イベント グラフの使用方法 （822 ページ）の説明に従って続行します。

ヒント デフォルトの時間範囲に影響を与えずにさらに分析を行えるように接続グラフ分離するには、[表示（View）] をクリックします。

関連トピック

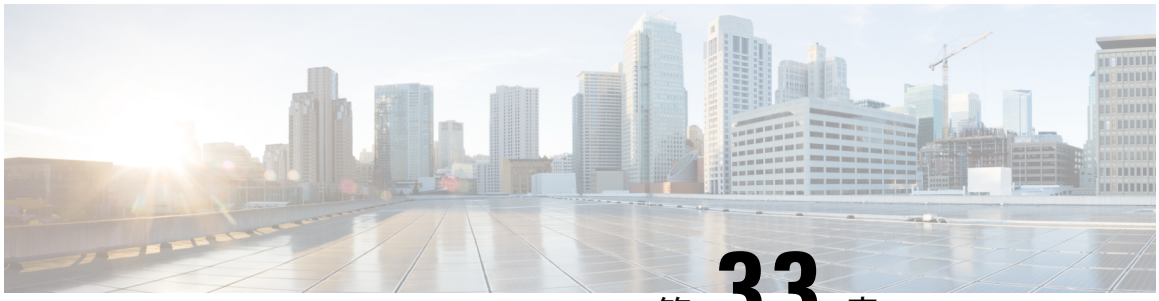
ユーザ ロール エスカレーションの有効化 （234 ページ）

接続イベントとセキュリティ インテリジェンス イベントの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
新しい接続イベントの理由：エレファントフロー。	7.1	任意（Any）	接続イベントの理由 （923 ページ）を参照してください。
NAT 変換済み IP アドレスとポート	7.1	任意（Any）	接続およびセキュリティ インテリジェンス イベント テーブルに 4 つの新しいフィールドが追加されました。 • NAT 送信元 IP（NAT Source IP） • NAT 宛先 IP（NAT Destination IP） • NAT 送信元ポート（NAT Source Port） • NAT 宛先ポート（NAT Destination Port）
リモートに保存された特定のイベントを操作するときにデータソースを選択する機能	7.0	任意（Any）	ワークフローの履歴 （843 ページ）を参照してください。

機能	最小 Management Center	最小 Threat Defense	詳細
DNS フィルタリング	7.0 6.7（ベータ機能）	任意（Any）	DNS フィルタ処理が有効な場合： • [DNSクエリ（DNS Query）] フィールドは、一致する DNS フィルタ処理に関連付けられたドメインを保留できます。 • [URL] フィールドが空で、[DNSクエリ（DNS Query）]、[URLカテゴリ（URL Category）]、および [URLレピュテーション（URL Reputation）] には値がある場合、イベントは DNS フィルタ処理機能によって生成され、カテゴリとレピュテーションが [DNSクエリ（DNS Query）] で指定されたドメインに適用されます。 • Cisco Secure Firewall Management Center デバイス構成ガイド の「*DNS* フィルタリングとイベント」も参照してください。
接続イベントのカスタムテーブル向けサポートの削除	6.6	任意（Any）	接続イベントのカスタムテーブルを作成することはできなくなりました。アップグレードした場合、接続イベントのカスタムテーブルのうちすでに存在していたものは引き続き利用可能ですが、常に結果は返されません。 他のタイプのカスタムテーブルに変更はありません。 新規/変更された画面：[分析（Analysis）] > [詳細（Advanced）] > [カスタムテーブル（Custom Tables）] の [テーブル（Tables）] オプション Platform：Management Center
接続イベントを削除およびすべて削除する機能の削除	6.6	任意（Any）	[削除（Delete）] および [すべて削除（Delete All）] ボタンは、接続イベントテーブルページから削除されました。 すべての接続イベントを消去するには、データの消去とストレージ（629 ページ）を参照してください。 新規/変更された画面：[分析（Analysis）]>[接続（Connections）]>[イベント（Events）] Platform：Management Center
VRF および SGT の新しいフィールド	6.6	任意（Any）	• 入力仮想ルータ（Syslog：IngressVRF） • 出力仮想ルータ（Syslog：EgressVRF） • [DestinationSecurityGroupType]（Syslog のみ） • [SourceSecurityGroupType]（Syslog のみ）

機能	最小 Management Center	最小 Threat Defense	詳細
新規および変更されたセキュリティグループタグのフィールド	6.5	任意（Any）	Management Center web インターフェイスのフィールドに変更を加えます： • 変更されたフィールド：[Security Group Tag] が [Source SGT] になりました • 新しいフィールド：[Destination SGT] Syslog フィールドへの変更： • 変更されたフィールド： [SecurityGroup] は [SourceSecurityGroupTag] になりました • 新しいフィールド： • [SourceSecurityGroup] • DestinationSecurityGroup • DestinationSecurityGroupTag サポートされるプラットフォーム：Management Center、管理対象デバイス
新しい syslog フィールド：[Event Priority]	6.5	任意（Any）	このフィールドは、接続イベントが侵入、ファイル、マルウェア、またはセキュリティ インテリジェンス イベントに関連付けられている場合に、その接続イベントを高優先度として識別します。
Syslog の接続イベントの固有識別子	6.4.0.4	任意（Any）	[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] の各 syslog フィールドの情報を総合すると、接続イベントを識別できます。



第 33 章

侵入イベント

以下のトピックでは、侵入イベントを操作する方法について説明します。

侵入イベントについて

システムは、ホストとそのデータの可用性、整合性、および機密性に影響する可能性のあるトラフィックがないかどうか、ネットワークをモニターするのに役立ちます。主要なネットワーク セグメントに管理対象デバイスを配置すると、悪意のあるアクティビティを目的としてネットワークを通過するパケットを検査できます。このシステムには、攻撃者が開発したさまざまなエクスプロイトを検索するのに使用できるいくつかのメカニズムがあります。

システムは、潜在的な侵入を特定すると侵入イベント（古い用語で「IPS イベント」と呼ばれることもあります）を生成します。これは、エクスプロイトの日付、時間、タイプ、および攻撃元とそのターゲットに関するコンテキスト情報のデータです。パケットベースのイベントの場合、イベントをトリガーとして使用したパケットのコピーも記録されます。管理対象デバイスは、Secure Firewall Management Center にイベントを送信します。ここで、集約データを確認し、ネットワーク アセットに対する攻撃を的確に把握できます。

管理対象デバイスをインライン、スイッチド、またはルーテッドの侵入システムとして展開することもできます。これにより、危険だと認識したパケットをドロップまたは置換するようデバイスを設定できます。

侵入イベントを確認および評価するためのツール

侵入イベントを検討し、それらがネットワーク環境やセキュリティポリシーの観点から重要かどうかを評価するために、次のツールを使用できます。

- 管理対象デバイスでの現在のアクティビティの概要について説明するイベント要約ページ
- 選択した任意の期間に生成できるテキストベースおよびグラフィカルなレポート。独自のレポートを設計し、スケジュールされた間隔で実行されるよう設定することもできます
- 攻撃に関連したイベントデータの収集に使用できるインシデント処理ツール。調査や応答のトラッキングに役立つ注記を追加することもできます
- SNMP、電子メール、および syslog で設定できる自動アラート
- 特定の侵入イベントに対する応答や修復に使用できる自動化された相関ポリシー
- データをドリルダウンして、さらに調査したいイベントを特定するのに使用できる定義済みカスタムワークフロー
- データを管理および分析するための外部ツール。syslog、eStreamer を使用して、これらのツールにデータを送信できます。詳細については、外部ツールを使用したイベントの分析（753 ページ）を参照してください。

また、[分析（Analysis）] > [詳細（Advanced）] > [状況に応じた相互起動（Contextual Cross-Launch）]ページで、事前定義されたリソースなどの公開情報を使用して、悪意のあるエンティティについて詳しく知ることができます。

特定のメッセージ文字列を検索し、イベントを生成したルールのドキュメントを取得するには、https://www.snort.org/rule_docs/ を参照してください。

侵入イベントのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

侵入イベントの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

侵入イベントの表示

侵入イベントは、ネットワークセキュリティに対する脅威があるかどうかを判断するために表示します。

初期の侵入イベントビューは、ページにアクセスするために使用するワークフローによって異なります。1つ以上のドリルダウンページ、侵入イベントのテーブルビュー、および終了パケットビューを含む、定義済みワークフローの1つを使用するか、独自のワークフローを作成できます。カスタムテーブルに基づいてワークフローを表示することもできます。これには、侵入イベントを含めることができます。

大量のIPアドレスが含まれている状態で、[IPアドレスの解決（Resolve IP Addresses）]イベントビュー設定が有効になっていると、イベントビューの表示が遅くなる場合があります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ1 **[分析（Analysis）]** > **[侵入（Intrusions）]** > **[イベント（Events）]**を選択します。

ステップ2 次の選択肢があります。

- 時間範囲の調整：時間枠の変更（833ページ）の説明に従って、イベントビューの時間範囲を調整します。
- ワークフローの変更：侵入イベントのテーブルビューが含まれないカスタムワークフローを使用している場合、ワークフローのタイトルの横にある[(ワークフローの切り替え)（(switch workflow)）]をクリックして、システム提供のワークフローのいずれかを選択します。
- 制約：表示する対象を分析において重要な侵入イベントに狭めるには、侵入イベントワークフローの使用（970ページ）を参照してください。
- イベントの削除：データベースからイベントを削除するには、[削除（Delete）]をクリックして表示しているパケットのイベントを削除するか、[すべて削除（Delete All）]をクリックして以前に選択したパケットのすべてのイベントを削除します。
- 確認済みのマークを付ける：侵入イベントに確認済みのマークを付けるには、侵入イベントを確認済みとしてマーク（964ページ）を参照してください。

- 接続データの表示：侵入イベントに関連付けられた接続データを表示するには、侵入イベントに関連付けられた接続データの表示 （964 ページ）を参照してください。
- 内容の表示：侵入イベント フィールド （948 ページ）の説明に従ってテーブルのカラムの内容を表示します。

関連トピック

侵入イベント パケット ビューの使用 （974 ページ）

侵入イベントのフィールドについて

システムは、潜在的な侵入を特定すると侵入イベントを生成します。これは、エクスプロイトの日付、時間、タイプ、および攻撃元とそのターゲットに関するコンテキスト情報のデータです。パケットベースのイベントの場合、イベントをトリガーとして使用したパケットのコピーも記録されます。

侵入イベント データは [分析（Analysis）] ト> [侵入（Intrusions）] > [イベント（Events）] で Secure Firewall Management Center Web インターフェイスでに表示できます。または外部ツールを使用して使用状況の syslog メッセージの特定のフィールドからデータをエミットします。Syslog のフィールドは下のリストに示されます。同等の syslog がリストされていないフィールドは、syslog メッセージでは使用可能できません。

侵入イベントを検索するときは、個別のイベントで利用可能な情報は、システムがいつ、なぜ、どのようにしてイベントを記録したかによって異なることに注意してください。たとえば、復号化されたトラフィックでトリガーされた侵入イベントだけが TLS/SSL 情報を含んでいます。

（注） Secure Firewall Management Center の Web インターフェイスの侵入イベントのテーブル ビューの一部のフィールドはデフォルトで無効になっています。セッション中にフィールドを有効にするには、検索制約を拡張してから、[無効の列（Disabled Columns）] の下の列名をクリックします。

侵入イベント フィールド

[アクセス コントロール ポリシー（Access Control Policy）]（syslog：ACPolicy）

イベントを生成した侵入ルール、プリプロセッサ ルール、またはデコーダ ルールが有効になっている侵入ポリシーに関連付けられているアクセス コントロール ポリシー。

アクセス コントロール ルール（Syslog：AccessControlRuleName）

イベントを生成した侵入ルールを呼び出したアクセス コントロール ルール。[デフォルト アクション（Default Action）] は、ルールが有効化されている侵入ポリシーが特定のアクセス コン

トロールルールに関連付けられておらず、代わりに、アクセスコントロールポリシーのデフォルト アクションとして設定されていることを示しています。

次の場合、このフィールドは空になります（または、syslog メッセージの場合は省略されます）。

- 関連ルール/デフォルトアクションなし：侵入インスペクションは、アクセス制御ルールにもデフォルトアクションにも関連付けられていません。たとえば、システムが適用するルールを決定する前に通過する必要があるパケットを処理するために指定された侵入ポリシーによってパケットが検査された場合が該当します。(このポリシーは、アクセス制御ポリシーの [詳細（Advanced）] タブで指定されます。)
- [関連付けられている接続イベントなし（No associated connection event）]：セッションに記録された接続イベントがデータベースから消去されている場合。たとえば、接続イベントに侵入イベントよりも高いターンオーバーがある場合などです。

[アプリケーション プロトコル（Application Protocol）]（syslog：ApplicationProtocol）

（使用可能な場合）侵入イベントをトリガーとして使用したトラフィックで検出されたホスト間の通信を表す、アプリケーション プロトコル。

アプリケーション プロトコル カテゴリおよびタグ（Application Protocol Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

アプリケーションのリスク（Application Risk）

侵入イベントをトリガーしたトラフィックで検出されたアプリケーションに関連付けられているリスク。[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]、および[非常に低い（Very Low）]。接続で検出されるアプリケーションのタイプごとに関連するリスクがあります。このフィールドは、それらのうち最も高いリスクを表示します。

ビジネスとの関連性（Business Relevance）

侵入イベントをトリガーしたトラフィックで検出されたアプリケーションに関連付けられているビジネスとの関連性。[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]、および[非常に低い（Very Low）]。接続で検出されるアプリケーションのタイプごとに関連するビジネスとの関連性があります。このフィールドは、それらのうち最も低い（関連性が最も低い）ものを表示します。

[分類（Classification）]（syslog：Classification）

イベントを生成したルールが属する分類。

侵入イベント詳細で使用可能な分類値のリストを参照してください。

このフィールドを検索するときは、表示するイベントを生成したルールの分類番号を入力するか、分類名または説明のすべてまたは一部を入力します。また、番号、名前、または説明のコンマ区切りリストを入力することもできます。最後に、カスタム分類を追加した場合、その名前または説明のすべてまたは一部を使用して検索することもできます。

[クライアント（Client）]（syslog：Client）

（使用可能な場合）侵入イベントをトリガーとして使用したトラフィックで検出されたモニター対象のホストで実行されているソフトウェアを表す、クライアント アプリケーション。

クライアント カテゴリおよびタグ（Client Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

Connection Counter （Syslog のみ）

ある接続と別の同時接続を区別するカウンタ。このフィールドは、それ自体には意味がありません。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定の侵入イベントに関連付けられた接続イベントを識別できます。

Connection Instance ID （Syslog のみ）

接続イベントを処理した Snort インスタンス。このフィールドは、それ自体には意味がありません。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定の侵入イベントに関連付けられた接続イベントを識別できます。

カウント（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

CVE ID

このフィールドは検索フィールド専用です。

MITRE の Common Vulnerabilities and Exposures（CVE）データベース（https://cve.mitre.org/）の脆弱性に関連付けられた識別番号による検索。

送信先の大陸（Destination Continent）

侵入イベントに関連する受信ホストの大陸。

送信先の国（Destination Country）

侵入イベントに関連する受信ホストの国。

宛先ホスト重要度（Destination Host Criticality）

イベントが生成されたときの宛先ホスト重要度（対応するホストのホスト重要度属性の値）。

ホストの重要度が変更されても、このフィールドは更新されないことに注意してください。ただし、新しいイベントは新しい重要度の値になります。

[宛先 IP（Destination IP）]（syslog：DstIP）

侵入イベントに関連する受信ホストが使用する IP アドレス。

イニシエータ/レスポンダ、送信元/接続先、および送信者/受信者フィールドに関する注意（922 ページ）も参照してください。

[宛先ポート/ICMP コード（Destination Port / ICMP Code）]（syslog：DstPort、ICMPCode）

トラフィックを受信するホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、このフィールドには ICMP コードが表示されます。

宛先ユーザー（Destination User）

接続イベントのレスポンダー IP に関連付けられたユーザー名。このホストは、エクスプロイトを受信するホストである場合とそうでない場合があります。この値は、通常、ネットワーク上のユーザーだけに知らされます。

。

イニシエータ/レスポンダ、送信元/接続先、および送信者/受信者フィールドに関する注意（922 ページ）も参照してください。

デバイス

アクセス コントロール ポリシーが展開された管理対象デバイス。

DeviceUUID （Syslog のみ）

イベントを生成した Firepower デバイスの一意の識別子。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定の侵入イベントに関連付けられた接続イベントを識別できます。

ドメイン（Domain）

侵入を検出したデバイスのドメイン。このフィールドは、マルチテナンシーのためにManagement Center を設定したことがある場合に表示されます。

[出力インターフェイス（Egress Interface）]（syslog：EgressInterface）

イベントをトリガーとして使用したパケットの出力インターフェイス。パッシブインターフェイスの場合、このインターフェイスの列には入力されません。

[出力セキュリティ ゾーン（Egress Security Zone）]：（syslog：EgressZone）

イベントをトリガーとして使用したパケットの出力セキュリティ ゾーン。パッシブ展開環境では、このセキュリティ ゾーンのフィールドには入力されません。

[出力仮想ルータ（Egress Virtual Router）]

仮想ルーティングを使用するネットワークでは、トラフィックがネットワークから出るときに通過する仮想ルータの名前。

電子メールの添付ファイル（Email Attachments）

[MIME コンテンツ - 傾向（MIME Content-Disposition）] 見出しから取得された MIME 添付ファイル名。添付ファイルの名前を表示するには、SMTP プリプロセッサの [MIME 添付ファイル名のログ（Log MIME Attachment Names）] オプションを有効にする必要があります。複数の添付ファイル名がサポートされます。

電子メールのヘッダー（Email Headers）

このフィールドは検索フィールド専用です。

電子メールのヘッダーから取得したデータ。

電子メールのヘッダーを SMTP トラフィックの侵入イベントと関連付けるには、SMTP プリプロセッサの [ヘッダーのログ（Log Headers）] オプションを有効にする必要があります。

メール受信者（Email Recipient）

SMTP RCPT TO コマンドから取得された電子メール受信者のアドレス。このフィールドの値を表示するには、SMTP プリプロセッサの [受信者アドレスのログ（Log To Addresses）] オプションを有効にする必要があります。複数の受信者アドレスがサポートされます。

メール送信者（Email Sender）

SMTP MAIL FROM コマンドから取得された電子メール送信者のアドレス。このフィールドの値を表示するには、SMTP プリプロセッサの [送信者アドレスのログ（Log From Address）] オプションを有効にする必要があります。複数の送信者アドレスがサポートされます。

First Packet Time （Syslog のみ）

システムが最初のパケットを検出した時間。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定の侵入イベントに関連付けられた接続イベントを識別できます。

ジェネレータ（Generator）

イベントを生成したコンポーネント。

次の侵入イベント フィールドに関する情報も参照してください。[GID]、[メッセージ（Message）]、および [Snort ID]

GID（syslog のみ）

ジェネレータ ID。イベントを生成したコンポーネントの ID。

次の侵入イベントフィールドに関する情報も参照してください。[ジェネレータ（Generator）]、[メッセージ（Message）]、および [Snort ID]

HTTP ホスト名（HTTP Hostname）

HTTP 要求のホスト見出しから取得されたホスト名（存在する場合）。要求パケットにホスト名が常に含まれているわけではないことに注意してください。

ホスト名を HTTP クライアント トラフィックの侵入イベントと関連付けるには、HTTP 検査プリプロセッサの [ホスト名のログ（Log Headers）] オプションを有効にする必要があります。

テーブル ビューで、この列には、取得されたホスト名の最初の 50 文字が表示されます。ホストの省略名の表示部分にポインタを合わせると、最大256バイトまでの完全な名前を表示することができます。また、最大256バイトまでの完全なホスト名をパケット ビューに表示することもできます。

[HTTP 応答コード（HTTP Response Code）]（syslog：HTTPResponse）

イベントをトリガーした接続を介してクライアントの HTTP 要求に応答して送信される HTTP ステータス コード。

HTTP URI

（存在する場合）侵入イベントをトリガーとして使用したHTTP要求パケットに関連付けられた raw URI。要求パケットに URI が常に含まれているわけではないことに注意してください。

URI を HTTP クライアント トラフィックの侵入イベントと関連付けるには、HTTP 検査プリプロセッサの [URI のログ（Log URI）] オプションを有効にする必要があります。

HTTP応答によってトリガーとして使用された侵入イベントの関連HTTP URIを参照するには、[両方のポートでのストリーム再構成の実行（Perform Stream Reassembly on Both Ports）] オプションにHTTPサーバのポートを設定する必要があります。ただし、これにより、トラフィックのリアセンブル用のリソース要求が増加することに注意してください。

この列には、取得された URI の最初の 50 文字が表示されます。省略 URI の表示部分にポインタを合わせると、最大 2048 バイトまでの完全な URI を表示することができます。また、最大 2048 バイトまでの完全な URI をパケット ビューに表示することもできます。

影響（Impact）

このフィールドの影響レベルは、侵入データ、ネットワーク検出データ、脆弱性情報との関係を示します。

このフィールドを検索するときは、影響アイコンの色または一部の文字列を指定しないでください。たとえば、**blue**、**level 1**、または **0** を使用しないでください。有効な大文字と小文字を区別しない値は次のとおりです。

- Impact 0、Impact Level 0
- Impact 1、Impact Level 1
- Impact 2、Impact Level 2
- Impact 3、Impact Level 3
- Impact 4、Impact Level 4

NetFlow データからネットワークマップに追加されたホストに使用可能なオペレーティングシステムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な（インパクト レベル 1：赤）インパクトレベルを割り当てることができません。このような場合は、ホスト入力機能を使用して、ホストのオペレーティングシステム ID を手動で設定します。

入力インターフェイス (Syslog：IngressInterface)

イベントをトリガーとして使用したパケットの入力インターフェイス。パッシブインターフェイスの場合、このインターフェイスの列だけに入力されます。

[入力セキュリティ ゾーン（Ingress Security Zone）]：（syslog：IngressZone）

イベントをトリガーとして使用したパケットの入力セキュリティ ゾーンまたはトンネル ゾーン。パッシブ展開環境では、このセキュリティ ゾーン フィールドだけに入力されます。

[入力仮想ルータ（Ingress Virtual Router）]

仮想ルーティングを使用するネットワークでは、トラフィックがネットワークに入るときに通過する仮想ルータの名前。

[インライン結果（Inline Result）]（syslog：InlineResult）

ワークフローとテーブル ビューでは、このフィールドには次のいずれかが表示されます。

表 *108*：ワークフロー ビュートテーブル ビューの *[インライン結果（Inline Result）]* フィールドの内容

アイコン	意味
	ルールをトリガーしたパケットをシステムがドロップしました。
	[インライン時にドロップ（Drop when Inline）]侵入ポリシーオプション（インライン展開環境）を有効にした場合、またはシステムがプルーニングしている間に [ドロップしてイベントを生成する（Drop and Generate）]ルールがイベントを生成した場合、IPS がパケットをドロップしたことを示します。

アイコン	意味
	IPS はパケットを宛先に送信または配信した可能性がありますが、このパケットを含む接続は現在ブロックされています。
アイコンなし（空白）	トリガーされたルールは [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されていませんでした

次の表に、インライン結果の考えられる理由の一覧を示します（「would have dropped」および「partially dropped」）。

インライン結果	理由	詳細な理由
would have dropped	パッシブモードまたはタップモードのインターフェイス	インラインのタップモードまたはパッシブモードでインターフェイスを構成しています。
	「検出」検査モードの侵入ポリシー	侵入ポリシーの検査モードを検出に設定しています。
	接続のタイムアウト	TCP/IP 接続がタイムアウトしたため、Snort 検査エンジンは検査を一時停止しました。
partially dropped	接続が終了しました（0x01）	新しいフローの作成中に、割り当てられたフローが許可されたフロー数を超える場合、Snort 検査エンジンは、最も使用頻度の低いフローをプルーニングします。
	接続が終了しました（0x02）	Snort 検査エンジンを再読み込みすると、メモリが調整され、エンジンは最も使用頻度の低いフローをプルーニングします。
	接続が終了しました（0x04）	Snort 検査エンジンが正常にシャットダウンすると、エンジンはすべてのアクティブなフローをパージします。

パッシブ展開では、侵入ポリシーのルールの状態やインライン ドロップ動作に関係なく、インライン インターフェイスがタップ モードの場合を含めて、システムはパケットをドロップしません。

このフィールドを検索するときは、次のいずれかを入力します。

- **dropped**：インライン展開環境でパケットをドロップするかどうかを指定します。
- **would have dropped**：インライン展開環境でパケットをドロップするように侵入ポリシーが設定されている場合に、パケットをドロップするかどうかを指定します。
- **partially dropped**：パケットが宛先に送信または配信されるかどうかを指定します。ただし、このパケットを含む接続は現在ブロックされています。

侵入ポリシー (Syslog: IntrusionPolicy)

イベントを生成した侵入ルール、プリプロセッサ ルール、またはデコーダ ルールが有効にされた侵入ポリシー。アクセス コントロール ポリシーのデフォルト アクションとして侵入ポリシーを選択するか、アクセス コントロール ルールと侵入ポリシーを関連付けることができます。

IOC（syslog：NumIOC）

侵入イベントをトリガーとして使用したトラフィックが、接続に関係するホストに対する侵入の痕跡（IOC）もトリガーとして使用したかどうか。

このフィールドを検索するときは、**triggered** または **n/a** を指定します。

[メッセージ（Message）]（syslog：メッセージ）

イベントを説明するテキスト。ルールベースの侵入イベントの場合、イベント メッセージはルールから取得されます。デコーダベースおよびプリプロセッサベースのイベントの場合は、イベント メッセージはハード コーディングされています。

ジェネレータおよび Snort ID（GID と SID）と SID バージョン（改訂）はカッコで囲んだコロン区切りの数字形式で各メッセージの末尾に付加されます（GID:SID:version）。例：**(1:36330:2)**。

MITRE

クリックしてモーダルを起動できる技術の数。これは、その階層内にある MITRE の戦術と技術の全リストを示します。

[MPLS ラベル（MPLS Label）]（syslog：MPLS_Label）

侵入イベントをトリガーしたパケットと関連付けられているマルチプロトコル ラベル スイッチング ラベル。

[ネットワーク分析ポリシー（Network Analysis Policy）]（syslog：NAPPolicy）

イベントの生成に関連付けられているネットワーク分析ポリシー（ある場合）。

このフィールドには、取得された URI の最初の 50 文字が表示されます。省略 URI の表示部分にポインタを合わせると、最大 2048 バイトまでの完全な URI を表示することができます。また、最大 2048 バイトまでの完全な URI をパケット ビューに表示することもできます。

クライアントのオリジナル IP（Original Client IP）

X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義の HTTP ヘッダーから取得された、元のクライアント IP アドレス。

このフィールドの値を表示するには、ネットワーク解析ポリシーで HTTP プリプロセッサ [元のクライアント IP アドレスの抽出（Extract Original Client IP Address）] オプションを有効にする必要があります。オプションで、ネットワーク解析ポリシーの同じエリアで、最大 6 つのカスタム クライアント IP 見出しを指定し、システムが [クライアントのオリジナル IP（Original Client IP）] イベント フィールドの値を選択する優先順位を設定します。

[優先度（Priority）]（syslog：Priority）

Talos インテリジェンスグループ で指定されたイベントの優先度。優先度は、`priority` キーワードの値または `classtype` キーワードの値に対応します。その他の侵入イベントの場合、プライオリティはデコーダまたはプリプロセッサによって決定されます。有効な値は、[高（high）]、[中（medium）]、および [低（low）] です。

[プロトコル（Protocol）]（syslog：Protocol）

Secure Firewall Management Center の Web インターフェイスでは、このフィールドは検索フィールド専用です。

http://www.iana.org/assignments/protocol-numbers に一覧表示されている、接続で使用するトランスポート プロトコルの名前または番号。これは、送信元および宛先ポート/ICMP の列と関連付けられたプロトコルです。

確認者（Reviewed By）

イベントを確認したユーザの名前。このフィールドを検索するときは、**`unreviewed`** と入力すると、まだ確認されていないイベントを検索できます。

Revision（syslog のみ）

イベントの生成に使用された署名のバージョン。

次の侵入イベント フィールドに関する情報も参照してください。[ジェネレータ（Generator）]、[GID]、[メッセージ（Message）]、[SID]、および [Snort ID]

ルールグループ

クリックしてモーダルを起動できる非 MITRE ルールグループの数。これは、ルールグループの全リストを示します。

[セキュリティ コンテキスト（Security Context）]（syslog：Context）

トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。システムがこのフィールドにデータを設定するのは、マルチコンテキストモードの ASA FirePOWER だけです。

SID（syslog のみ）

イベントを生成したルールの署名 ID（Snort ID ともいう）

次の侵入イベントフィールドに関する情報も参照してください。[ジェネレータ（Generator）]、[GID]、[メッセージ（Message）]、[改訂（Revision）]、および [Snort ID]

Snort ID

このフィールドは検索フィールド専用です。

（syslog フィールドについては、SID を参照してください。）

検索を実行する場合：イベントを生成したルールの（[Snort ID]SID）を指定するか、オプションで、ルールの複合ジェネレータ ID（GID）および SID を指定します。ここで、GID および SID はコロン（:）で区切られ、GID:SID の形式になります。次の表の任意の値を指定できます。

表 *109 : [Snort ID]* 検索値

値	例
単一の SID	10000
SID の範囲	10000-11000
SID より大きい	>10000
SID 以上	>=10000
SID 未満	<10000
SID 以下	<=10000
SID のカンマ区切りリスト	10000,11000,12000
単一の GID:SID の組み合わせ	1:10000
GID:SID の組み合わせのカンマ区切りリスト	1:10000,1:11000,1:12000
SID および GID:SID の組み合わせのカンマ区切りリスト	10000,1:11000,12000

表示しているイベントの SID が [メッセージ（Message）] 列に表示されます。詳細については、この項の [メッセージ（Message）] フィールドについての説明を参照してください。

ソースの大陸（Source Continent）

侵入イベントに関連する送信ホストのある大陸。

ソースの国（Source Country）

侵入イベントに関連する送信ホストのある国。

送信元ホスト重要度（Source Host Criticality）

イベントが生成されたときの送信元ホスト重要度（対応するホストのホスト重要度属性の値）。

ホストの重要度が変更されても、このフィールドは更新されないことに注意してください。ただし、新しいイベントは新しい重要度の値になります。

[送信元 IP（Source IP）]（syslog：SrcIP）

侵入イベントに関連する送信ホストが使用する IP アドレス。

イニシエータ/レスポンダ、送信元/接続先、および送信者/受信者フィールドに関する注意（922 ページ）も参照してください。

[送信元ポート/ICMP タイプ（Source Port/ICMP Type）]（syslog：SrcPort、ICMPType）

送信元ホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、このフィールドには ICMP タイプが表示されます。

[送信元ユーザー（Source User）]（syslog：User）

接続を開始したホストの IP アドレスに関連付けられたユーザー名。エクスプロイトの送信元ホストである場合とそうでない場合があります。このユーザー値は、通常、ネットワーク上のユーザーだけに知らされます。

該当する場合、ユーザー名の前には `<realm>\` が付いています。

SSL Actual Action (Syslog: SSLActualAction)

Secure Firewall Management Center の Web インターフェイスでは、このフィールドは検索フィールド専用です。

システムが暗号化されたトラフィックに適用したアクション。

ブロック/リセット付きブロック（Block/Block with reset）

ブロックされた暗号化接続を表します。

[復号（再署名）（Decrypt (Resign)）]

再署名サーバ証明書を使用して復号された発信接続を表します。

[復号（キーの交換）（Decrypt (Replace Key)）]

置き換えられた公開キーと自己署名サーバ証明書を使用して復号化された発信接続を表します。

[復号（既知のキー）（Decrypt (Known Key)）]

既知の秘密キーを使用して復号化された着信接続を表します。

[デフォルトアクション（Default Action）]

接続がデフォルト アクションによって処理されたことを示します。

[復号しない（Do not Decrypt）]

システムが復号化しなかった接続を表します。

フィールド値は、検索ワークフロー ページの [SSL ステータス（SSL Status）] フィールドに表示されます。

[SSL 証明書情報（SSL Certificate Information）]

このフィールドは検索フィールド専用です。

トラフィックを暗号化するための公開キー証明書に保存される次の情報：

- サブジェクト/発行元共通名（Subject/Issuer Common Name）
- サブジェクト/発行元組織（Subject/Issuer Organization）
- サブジェクト/発行元組織単位（Subject/Issuer Organization Unit）
- 有効期間の開始/終了（Not Valid Before/After）
- シリアル番号（Serial Number）
- 証明書フィンガープリント（Certificate Fingerprint）
- 公開キー フィンガープリント（Public Key Fingerprint）

SSL 失敗理由（SSL Failure Reason）

このフィールドは検索フィールド専用です。

システムが暗号化されたトラフィックの復号化に失敗した理由。

- 不明
- 不一致（No Match）
- Success
- キャッシュされていないセッション（Uncached Session）
- 不明な暗号スイート（Unknown Cipher Suite）
- サポートされていない暗号スイート（Unsupported Cipher Suite）
- サポートされていない SSL バージョン（Unsupported SSL Version）
- 使用された SSL 圧縮（SSL Compression Used）
- パッシブ モードで復号化できないセッション（Session Undecryptable in Passive Mode）
- ハンドシェイク エラー（Handshake Error）
- 復号エラー（Decryption Error）
- 保留中のサーバー名カテゴリの検索（Pending Server Name Category Lookup）

- 保留中の共通名カテゴリの検索（Pending Common Name Category Lookup）
- 内部エラー（Internal Error）
- 使用不可能なネットワーク パラメータ（Network Parameters Unavailable）
- 無効なサーバー証明書の処理（Invalid Server Certificate Handle）
- 使用不可能なサーバー証明書フィンガープリント（Server Certificate Fingerprint Unavailable）
- サブジェクト DN をキャッシュできない（Cannot Cache Subject DN）
- 発行元 DN をキャッシュできない（Cannot Cache Issuer DN）
- 不明な SSL バージョン（Unknown SSL Version）
- 使用不可能な外部証明書リスト（External Certificate List Unavailable）
- 使用不可能な外部証明書フィンガープリント（External Certificate Fingerprint Unavailable）
- 無効な内部証明書リスト（Internal Certificate List Invalid）
- 使用不可能な内部証明書リスト（Internal Certificate List Unavailable）
- 使用不可能な内部証明書（Internal Certificate Unavailable）
- 使用不可能な内部証明書フィンガープリント（Internal Certificate Fingerprint Unavailable）
- 使用不可能なサーバー証明書の検証（Server Certificate Validation Unavailable）
- サーバー証明書の検証エラー（Server Certificate Validation Failure）
- 無効なアクション（Invalid Action）

フィールド値は、検索ワークフロー ページの [SSL ステータス（SSL Status）] フィールドに表示されます。

SSL ステータス（SSL Status）

暗号化された接続を記録した、[SSLの実際の動作（SSL Actual Action）]（復号ルール、デフォルトアクション、または復号できないトラフィックアクション）に関連したアクション。

システムが暗号化された接続の復号化に失敗した場合、実行された [SSL の実際のアクション（SSL Actual Action）]（復号化できないトラフィック アクション）と [SSL 障害の理由（SSL Failure Reason）] が表示されます。たとえば、不明な暗号スイートによって暗号化されたトラフィックをシステムが検出し、それ以上のインスペクションをせずにこれを許可した場合、このフィールドには [復号しない（不明な暗号スイート）（Do Not Decrypt (Unknown Cipher Suite)）] が表示されます。

証明書の詳細を表示するには [ロック（Lock）] アイコン（）をクリックします。

このフィールドを検索するときは、[SSL の実際のアクション（SSL Actual Action）] および [SSL 障害の理由（SSL Failure Reason）] の値を 1 つ以上を入力して、システムが処理した暗号化されたトラフィック、または復号化に失敗したトラフィックを表示します。

[SSL サブジェクト/発行元国（SSL Subject/Issuer Country）]

このフィールドは検索フィールド専用です。

暗号化証明書に関連付けられている件名または発行者の国に関する 2 文字の ISO 3166-1 アルファ 2 国コード。

時刻（Time）

イベントの日付と時刻。このフィールドは検索できません。

[VLAN ID]（syslog：VLAN_ID）

侵入イベントをトリガーとして使用したパケットと関連付けられた最内部 VLAN ID。

[Web アプリケーション（Web Application）]（syslog：WebApplication）

侵入イベントをトリガーとして使用したトラフィックで検出された HTTP トラフィックの内容または要求された URL を表す、Web アプリケーション。

システムが HTTP のアプリケーション プロトコルを検出し、特定の Web アプリケーションを検出できなかった場合、システムは代わりに一般的な Web ブラウジング指定を提供します。

Web アプリケーション カテゴリおよびタグ（Web Application Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

関連トピック

イベントの検索 （845 ページ）

侵入イベント影響レベル

イベントがネットワークに与える影響を評価するために、Secure Firewall Management Center は侵入イベントのテーブル ビューに影響レベルを表示します。イベントごとに、システムは影響レベル アイコンを追加し、侵入データ、ネットワーク検出データ、脆弱性情報との関係を色で示します。

（注） NetFlow データからネットワークマップに追加されたホストに使用可能なオペレーティングシステムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な（インパクト レベル 1：赤）インパクトレベルを割り当てることができません。このような場合は、ホスト入力機能を使用して、ホストのオペレーティングシステム ID を手動で設定します。

次の表に、影響レベルで使用可能な値を示します。

表 *110*：影響レベル

影響レベル	脆弱性	カラー	説明
[不明（Unknown）]（0）	不明	グレー	送信元ホストと宛先ホストは両方ともネットワーク検出によってモニタされているネットワーク上に存在しません。
[脆弱（Vulnerable）]（1）	脆弱	赤色	次のいずれかを行います。 • 送信元ホストまたは宛先ホストはネットワークマップ内にあり、脆弱性はホストにマッピングされます • 送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵害される可能性があります。
[潜在的に脆弱（Potentially Vulnerable）]（2）	潜在的に脆弱	オレンジ	送信元ホストまたは宛先ホストはネットワークマップ内にあり、次のいずれかに当てはまります。 • ポート指向のトラフィックの場合、ポートはサーバアプリケーションプロトコルを実行しています • ポート指向ではないトラフィックの場合、ホストはプロトコルを使用します
[現在脆弱性のない（Currently Not Vulnerable）]（3）	現在は脆弱ではない	黄色	送信元ホストまたは宛先ホストはネットワークマップ内にあり、次のいずれかに当てはまります。 • ポート指向のトラフィック（たとえば、TCPまたはUDP）の場合、ポートが開いていません • ポート指向ではないトラフィック（たとえば、ICMP）の場合、ホストはプロトコルを使用しません
[不明なターゲット（Unknown Target）]（4）	不明なターゲット	青	送信元ホストまたは宛先ホストがモニター対象のネットワークにありますが、ネットワークマップ内にそのホストのエントリがありません。

侵入イベントに関連付けられた接続データの表示

システムは、侵入イベントが検出された接続を記録できます。このロギングは、アクセス コントロール ルールに関連付けられている侵入ポリシーに対して自動的に行われますが、デフォルト アクションに関連する接続データを参照するには、接続ロギングを手動で有効にする必要があります。

関連データの表示は、イベントのテーブル ビュー間を移動する場合に非常に役立ちます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[分析（Analysis）] > [侵入（Intrusions）] > [イベント（Events）]**を選択します。

ステップ 2 テーブルのチェックボックスを使用して侵入イベントを選択してから、[ジャンプ（Jump to）] ドロップダウン リストから [接続（Connections）] を選択します。

ヒント 同じ方法で、特定の接続に関連した侵入イベントを表示できます。詳細については、ワークフロー間のナビゲーション （839 ページ）を参照してください。

関連トピック

許可された接続のロギング （885 ページ）
侵入イベント ワークフローの使用 （970 ページ）
接続およびセキュリティ関連の接続イベントテーブルの使用 （934 ページ）

侵入イベントを確認済みとしてマーク

侵入イベントが悪意のあるものではないことがわかったら、そのイベントを確認済みとしてマークできます。

侵入イベントを調べて、そのイベントがネットワーク セキュリティに対して脅威ではないことがわかったら（たとえば、ネットワーク上のどのホストも検出されたエクスプロイトに対して脆弱でないことがわかっているなど）、そのイベントを確認済みとしてマークできます。確認済みのイベントはイベント データベースに保存され、イベント要約統計に含まれますが、デフォルトの侵入イベント ページには表示されなくなります。自分の名前がレビューアとして表示されます。

マルチドメイン展開では、イベントに確認済みのマークを付けると、そのイベントを表示可能なすべてのドメインでシステムによってイベントに確認済みのマークが付けられます。

バックアップを実行してから確認済みの侵入イベント ビューを削除した場合、バックアップを復元すると、削除された侵入イベント ビューは復元されますが、確認済みのステータスは復元されません。こうして復元された侵入イベントは、[確認済みイベント（Reviewed Events）] の下ではなく [侵入イベント（Intrusion Events）] の下に表示されます。

手順

侵入イベントが表示されるページで、次の 2 つの方法を選択できます。

- イベントのリストから 1 つまたは複数の侵入イベントにマークを付けるには、イベントの横にあるチェックボックスをオンにして、[レビュー（Review）] をクリックします。
- イベントのリストからすべての侵入イベントにマークを付けるには、[すべて確認（Review All）] をクリックします。

関連トピック

侵入イベント ワークフローの使用 （970 ページ）

以前に確認した侵入イベントの表示

マルチドメイン展開では、イベントに確認済みのマークを付けると、そのイベントを表示可能なすべてのドメインでシステムによってイベントに確認済みのマークが付けられます。

手順

ステップ 1 **[分析（Analysis）] > [侵入（Intrusions）] > [確認済みイベント（Reviewed Events）]**を選択します。

ステップ 2 次の選択肢があります。

- 時間枠の変更 （833 ページ）の説明に従って、時間範囲を調整します。
- 侵入イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合、ワークフローのタイトルの横にある [(ワークフローの切り替え)（(switch workflow)）] をクリックして、システム提供のワークフローのいずれかを選択します。
- 表示されるイベントの詳細については、侵入イベント フィールド （948 ページ）を参照してください。

関連トピック

侵入イベント ワークフローの使用 （970 ページ）

確認済み侵入イベントに未確認のマークを付ける

イベントに未確認のマークを付けることで、確認済みイベントをデフォルトの侵入イベント ビューに戻すことができます。

マルチドメイン展開では、イベントに確認済みのマークを付けると、そのイベントを表示可能なすべてのドメインでシステムによってイベントに確認済みのマークが付けられます。

手順

確認済みイベントが表示されるページで、次の 2 つの方法を選択できます。

- 確認済みイベント リストから個別の侵入イベントを削除するには、特定のイベントの横にあるチェックボックスをオンにして、[未確認（Unreview）] をクリックします。
- 確認済みイベント リストからすべての侵入イベントを削除するには、[すべて未確認（Unreview All）] をクリックします。

プリプロセッサ イベント

プリプロセッサが提供する機能は2つあります。1つは、パケットに対して指定されたアクション（HTTP トラフィックを復号して正規化するなど）を実行する機能、もう 1 つは、パケットが特定のプリプロセッサ オプションをトリガーしたときに関連するプリプロセッサ ルールが有効にされている場合は常にイベントを生成することで、指定のプリプロセッサ オプションの実行を報告するという機能です。たとえば、プリプロセッサが IIS の二重にエンコードされたトラフィックを検出した場合にイベントが生成されるようにするには、HTTP Inspect の [二重エンコード（Double Encoding）] オプションと、HTTP Inspect Generator（GID）119 および [Snort ID]（SID）2 が設定された関連するプリプロセッサ ルールを有効にします。

プリプロセッサの実行を報告するイベントを生成すると、異常なプロトコルエクスプロイトを検出するのに役立ちます。たとえば、攻撃者は重複している IP フラグメントを作成して、ホスト上で DoS 攻撃を仕掛ける可能性があります。IP 最適化プリプロセッサはこのタイプの攻撃を検出し、それに関する侵入イベントを生成できます。

プリプロセッサ イベントは、パケット ディスプレイにイベントの詳細なルールの説明が表示されないという点で、ルール イベントとは異なります。代わりに、パケット ディスプレイには、イベント メッセージ、GID、SID、パケット ヘッダー データおよびパケット ペイロードが表示されます。これにより、パケットのヘッダー情報を分析し、そのヘッダー オプションが使用中であるかをどうか判断して、それがシステムをエクスプロイトする可能性がある場合は、パケット ペイロードを検査できます。プリプロセッサによる各パケットの分析が完了すると、ルール エンジンは、その結果に応じて適切なルールを実行し（プリプロセッサが各パケットを最適化し、有効なセッションの一部として確立できた場合）、潜在的なコンテンツ レベルの脅威についてさらに分析を行い、それらのパケットについて報告します。

プリプロセッサのジェネレータ ID

各プリプロセッサには、独自のジェネレータ ID 番号（GID）があり、これはパケットによってトリガーとして使用されたプリプロセッサを示します。一部のプリプロセッサは関連した SID もあり、これは潜在的攻撃を分類する ID 番号です。ルールの [Snort ID]（SID）が、ルールをトリガーとして使用するパケットのコンテキストを提供できる方法とほぼ同じで、この ID 番号によりイベントのタイプを分類することによって、イベントをより効率的に分析するのに役立ちます。侵入ポリシー ルールのページのプリプロセッサ フィルター グループのプリプロセッサごとにプリプロセッサ ルールをリストできます。また、プリプロセッサのプリプロ

セッサ ルールとカテゴリ フィルター グループのパケット デコーダ サブグループをリストできます。

（注） 標準テキスト ルールによって生成されるイベントは、ジェネレータ ID が 1（グローバル ドメインまたはレガシー GID）または 1000 ～ 2000（子孫ドメイン）です。共有オブジェクト ルールの場合、イベントのジェネレータ ID は 3 です。どちらの場合も、トリガーした特定のルールがイベントの SID に示されます。

次の表では、各 GID を生成するイベントのタイプについて説明します。

表 *111* : ジェネレータ *ID*

ID	コンポーネント	説明
1	標準的なテキストルール	パケットが標準テキスト ルールをトリガーとして使用したときにイベントが生成されました（グローバル ドメインまたはレガシー GID）。
2	タグ付きパケット	タグ付きセッションからパケットを生成するタグ ジェネレータによって、イベントが生成されました。これは、`tag`ルール オプションが使用される場合に発生します。
3	共有オブジェクト ルール	パケットが共有オブジェクト ルールをトリガーとして使用したときにイベントが生成されました。
102	HTTP デコーダ	デコーダ エンジンが、パケット内の HTTP データを復号化しました。
105	Back Orifice ディテクタ	Back Orifice ディテクタが、パケットに関連付けられた Back Orifice 攻撃を特定しました。
106	RPC デコーダ	RPC デコーダがパケットを復号化しました。
116	パケット デコーダ	パケット デコーダによってイベントが生成されました。
119、120	HTTP Inspect プリプロセッサ	HTTP Inspect プリプロセッサによってイベントが生成されました。GID 120 ルールは、サーバ固有の HTTP トラフィックに関するルールです。
122	ポートスキャンディテクタ	ポートスキャン フロー ディテクタによってイベントが生成されました。
123	IP デフラグメンタ	断片化された IP データグラムを適切に再構成できなかったときに、イベントが生成されました。
124	SMTP デコーダ	SMTP プリプロセッサが SMTP バーブに対するエクスプロイトを検出したときに、イベントが生成されました。
125	FTP デコーダ	FTP/Telnet デコーダが FTP トラフィック内でエクスプロイトを検出したときに、イベントが生成されました。

ID	コンポーネント	説明
126	Telnet デコーダ	FTP/Telnet デコーダが Telnet トラフィック内でエクスプロイトを検出したときに、イベントが生成されました。
128	SSH プリプロセッサ	SSH プリプロセッサが SSH トラフィック内でエクスプロイトを検出したときに、イベントが生成されました。
129	ストリームプリプロセッサ	ストリーム プリプロセッサによるストリームの前処理中に、イベントが生成されました。
131	DNSプリプロセッサ	DNS プリプロセッサによってイベントが生成されました。
133	DCE/RPC プリプロセッサ	このイベントは、DCE/RPC プリプロセッサにより生成されました。
134	ルール遅延 パケット遅延	ルール遅延によって侵入ルールのグループが中断された（134:1）または再有効化された（134:2）とき、あるいはパケット遅延しきい値が超過したために、システムがパケットの検査を停止したとき（134:3）に、イベントが生成されました。
135	レートベースの攻撃ディテクタ	レートベースの攻撃ディテクタがネットワークのホストに対する過度の識別したときに、イベントが生成されました。
137	SSL プリプロセッサ	TLS/SSL プリプロセッサによってイベントが生成されました。
138、139	機密データプリプロセッサ	機密データ プリプロセッサによってイベントが生成されました。
140	SIP プリプロセッサ	SIP プリプロセッサによってイベントが生成されました。
141	IMAP プリプロセッサ	IMAP プリプロセッサによってイベントが生成されました。
142	POP プリプロセッサ	POP プリプロセッサによってイベントが生成されました。
143	GTP プリプロセッサ	GTP プリプロセッサによってイベントが生成されました。
144	Modbus プリプロセッサ	Modbus SCADA プリプロセッサによってイベントが生成されました。
145	DNP3 プリプロセッサ	DNP3 SCADA プリプロセッサによってイベントが生成されました。
148	CIP プリプロセッサ	CIP SCADA プリプロセッサによってイベントが生成されました。
149	S7Commplus プリプロセッサ	S7Commplus SCADA プリプロセッサによってイベントが生成されました。
1000～2000	標準的なテキストルール	パケットが標準テキスト ルールをトリガーとして使用したときにイベントが生成されました（子孫ドメイン）。

侵入イベントのワークフロー ページ

現在の侵入ポリシーで有効になっているプリプロセッサ、デコーダ、および侵入ルールは、モニタしているトラフィックがポリシーに違反するたびに、侵入イベントを生成します。

システムは、侵入イベントの表示および分析に使用できる、イベントデータが入力された定義済みワークフローのセットを提供します。これらのワークフローは、評価する侵入イベントの特定に役立つ一連のページを表示して手順を示します。

定義済みの侵入イベントのワークフローには、次の3種類のページまたはイベントビューがあります。

- 1つ以上のドリルダウン ページ
- 侵入イベントのテーブル ビュー
- パケット ビュー

ドリルダウン ページには通常、1つの特定の種類の情報を表示できるように1つのテーブル（一部のドリルダウン ビューでは複数のテーブル）に2つ以上の列が含まれます。

「ドリルダウン」して1つ以上の宛先ポートの詳細情報を検索すると、これらのイベントは自動的に選択され、ワークフローの次のページが表示されます。このように、ドリルダウンテーブルを使用すると、一度に分析するイベントの数を減らすことができます。

侵入イベントの最初のテーブル ビューでは、各侵入イベントが独自の行にリストされます。テーブルの列には、時間、発信元IPアドレスおよびポート、宛先IPアドレスおよびポート、イベントの優先度、イベント メッセージなどの情報が示されます。

イベントを選択してワークフローの次のページを表示する代わりに、テーブル ビューでイベントを選択した場合、イベントはいわゆる制約に追加されます。制約とは、分析するイベントの種類に加える制限のことです。

たとえば、任意の列で[閉じる（Close）]（×）をクリックして、ドロップダウンリストから[時間（Time）]をクリアすると、[時間（Time）]を列の1つとして削除できます。分析内でイベントのリストを絞り込むには、テーブル ビューの行のいずれかの値のリンクをクリックします。たとえば、分析を送信元IPアドレスの1つ（おそらく、潜在的な攻撃者）から生成されたイベントに制限するには、[送信元IPアドレス（Source IP Address）]列のIPアドレスをクリックします。

テーブル ビューの1つまたは複数の行を選択し、[表示（View）]をクリックすると、パケット ビューが表示されます。パケット ビューは、ルールをトリガーとして使用したパケットまたはイベントを生成したプリプロセッサに関する情報を提供します。パケット ビューの各セクションには、パケット内の特定の層についての情報が含まれます。折りたたまれたセクションを展開すると、より多くの情報を参照できます。

（注） それぞれのポートスキャン イベントは複数のパケットによってトリガーとして使用されるため、ポートスキャン イベントは特別なバージョンのパケット ビューを使用します。

事前定義済みのワークフローが特定のニーズに合致しない場合は、必要な情報だけを表示するカスタム ワークフローを作成できます。カスタム侵入イベントのワークフローには、ドリルダウン ページ、イベントのテーブル ビュー、またはその両方を含めることができます。システムはパケット ビューを最後のページとして自動的に組み込みます。イベントを調査する方法に応じて、定義済みワークフローと独自のカスタム ワークフローを簡単に切り替えることができます。

侵入イベント ワークフローの使用

イベントのドリルダウン ビューとテーブル ビューは、イベントのリストを絞り込み、関連するイベントのグループに分析を集中するために使用できる共通機能を共有します。

別のワークフローページで同じ侵入イベントを表示しないようにするため、ページの下部にあるリンクをクリックして別のページのイベントを表示すると時間範囲は一時停止し、クリックして後続のページでその他のアクションを実行すると再開します。

ヒント プロセスの任意の時点で、制約を検索条件のセットとして保存できます。たとえば、ネットワークが数日にわたり単一の IP アドレスから攻撃者によって探られていることに気付いた場合、調査中に制約をいったん保存し、後で使用することができます。ただし、複合制約を検索条件のセットとして保存することはできません。

手順

ステップ 1 **[分析（Analysis）]>[侵入（Intrusions）]>[イベント（Events）]** を使用して侵入イベント ワークフローにアクセスします。

ステップ 2 オプションで、侵入イベント ドリルダウン ページの制約 （972 ページ）または侵入イベント テーブル ビューの制約 （973 ページ）の説明に従って、イベント ビューに表示される侵入イベントの数を制限します。

ステップ 3 次の選択肢があります。

- 表示されるカラムの詳細については、侵入イベント フィールド （948 ページ）を参照してください。
- ホストのプロファイルを表示するには、ホスト IP アドレスの横に表示される [ホストプロファイル（Host Profile）] をクリックします。
- 地理位置情報の詳細を表示するには、[送信元の国（Source Country）] または [宛先の国（Destination Country）] 列に表示されるフラグをクリックします。

- システムの外部にある利用可能なソース内のデータを表示するには、イベント値を右クリックします。表示されるオプションはデータ タイプによって異なり、パブリック ソースが含まれます。他のソースは設定したリソースによって異なります。詳細については、Web ベースのリソースを使用したイベントの調査 （763 ページ）を参照してください。
- イベントに関する一般的なインテリジェンスを収集するには、テーブルでイベントの値を右クリックして、シスコまたはサードパーティのインテリジェンス ソースを選択します。たとえば、不審な IP アドレスに関する詳細情報を Cisco Talos から入手できます。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。詳細については、Web ベースのリソースを使用したイベントの調査 （763 ページ）を参照してください。
- 表示されたイベントの時刻と日付の範囲を変更するには、時間枠の変更 （833 ページ）を参照してください。

  ヒント 侵入イベントがイベント ビューに表示されない場合、指定した時間範囲を調整すると、結果が返される場合があります。古い時間範囲を指定した場合、その時間範囲内のイベントが削除されることがあります。ルールのしきい値の設定を調整すると、イベントが生成される場合があります。

  （注） イベント ビューを時間によって制約している場合は、（グローバルかイベント固有かに関係なく）アプライアンスに設定されている時間枠の外で生成されたイベントがイベント ビューに表示されます。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

- 現在のワークフロー ページのイベントをソートする、または現在のワークフロー ページ内で移動するには、ワークフローの使用 （809 ページ）を参照してください。
- 現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。
- イベント データベースからイベントを削除するには、削除するイベントの横にあるチェックボックスをオンにし、[削除（Delete）] または [すべて削除（Delete All）] をクリックします。
- イベントに確認済みのマークを付けて、侵入イベントのページからそれらを削除し、イベント データベースからは削除しないようにするには、侵入イベントを確認済みとしてマーク （964 ページ）を参照してください。
- 選択したイベントをトリガーしたパケットのローカル コピー（libpcap 形式のパケット キャプチャ ファイル）をダウンロードするには、ダウンロードするパケットによってトリガーされたイベントの横にあるチェックボックスをオンにして、[パケットのダウンロード（Download Packets）] または [すべてのパケットのダウンロード（Download All Packets）] をクリックします。キャプチャされたパケットは libpcap 形式で保存されます。この形式は、複数の一般的なプロトコル アナライザで使用されます。
- 他のイベント ビューに移動して関連イベントを表示するには、ワークフロー間のナビゲーション （839 ページ）を参照してください。

- 別のワークフローを一時的に使用するには、[(ワークフローの切り替え)（(switch workflow)）] をクリックします。
- 現在のページにすぐに戻れるようにページをブックマークするには、[このページをブックマーク（Bookmark This Page）] をクリックします。
- [サマリー ダッシュボード（Summary Dashboard）] の [侵入イベント（Intrusion Events）] セクションを表示するには、[ダッシュボード（Dashboards）] をクリックします。
- ブックマークの管理ページに移動するには、[ブックマークの表示（View Bookmarks）] をクリックします。
- 現在のビューのデータに基づいてレポートを生成するには、イベント ビューからのレポート テンプレートの作成 （647 ページ）を参照してください。

関連トピック

イベントの検索 （845 ページ）
ブックマーク （841 ページ）

侵入イベント ドリルダウン ページの制約

次の表では、ドリルダウン ページの使用方法について説明します。

表 *112*: ドリルダウン ページでのイベントの制約

目的	操作
次のワークフロー ページのドリルダウンを特定の値に制約する	値をクリックします。 たとえば、[宛先ポート（Destination Port）] ワークフローで、イベントを宛先がポート 80 であるものに制約するには、[DST ポート/ICMP コード（DST Port/ICMP Code）] 列で [80/tcp] をクリックします。ワークフローの次のページ [イベント（Events）] が表示され、ポート 80/tcp のイベントだけが含まれます。

目的	操作
次のワークフロー ページのドリルダウンを選択したイベントに制約する	次のワークフロー ページで表示するイベントの横にあるチェックボックスを選択し、[表示（View）] をクリックします。 たとえば、[宛先ポート（Destination Port）] ワークフローで、イベントを宛先がポート 20/tcp および 21/tcp であるものに制約するには、それらのポートの行の横にあるチェックボックスを選択し、[表示（View）] をクリックします。ワークフローの次のページ [イベント（Events）] が表示され、ポート 20/tcp および 21/tcp のイベントだけが含まれます。 複数の行を制約し、テーブルに複数の列が存在する場合（[数（Count）] 列を含まない）は、複合制約と呼ばれるものが作成されることに注意してください。複合制約により、必要以上のイベントを制約に含めないようにすることができます。たとえば、[イベント（Event）] と [宛先（Destination）] のワークフローを使用する場合は、最初のドリルダウン ページで選択した各行により、複合制約が作成されます。宛先 IP アドレス 10.10.10.100 のイベント 1:100 を選択し、宛先 IP アドレス 192.168.10.100 のイベント 1:200 も選択した場合、複合制約により、イベント タイプとして 1:100 を含むイベントや宛先 IP アドレスとして 192.168.10.100 を含むイベント、またはイベント タイプとして 1:200 を含むイベントや宛先 IP アドレスとして 10.10.10.100 を含むイベントが選択されないようになります。
現在の制約を保持しながら、次のワークフロー ページをドリルダウンする	[すべて表示（View All）] をクリックします。

侵入イベント テーブル ビューの制約

次の表では、テーブル ビューの使用方法について説明します。

表 *113*：イベントのテーブル ビューでのイベントの制約

目的	操作
1 つの属性を持つイベントにビューを制約する	属性をクリックします。 たとえば、宛先がポート 80 であるイベントにビューを制約するには、[DST ポート/ICMP コード（DST Port/ICMP Code）] 列で [80/tcp] をクリックします。
テーブルから列を削除する	非表示にする列の見出しで、[閉じる（Close）]（×）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。 他のカラムを表示または非表示にするには、[適用（Apply）] をクリックする前に、該当するチェックボックスをオンまたはオフにします。無効にした列をビューに戻すには、**展開の矢印** をクリックして検索の制約を展開し、[無効な列（Disabled Columns）] の下の列名をクリックします。

目的	操作
1つ以上のイベントに関連付けられたパケットを表示する	次のいずれかを行います。 • パケットを表示するイベントの横にある**下矢印** をクリックします。 • パケットを表示する1つ以上のイベントを選択し、ページの下部にある [表示（View）] をクリックします。 • ページの下部で、[すべて表示（View All）] をクリックして、現在の制約に一致するすべてのイベントのパケットを表示します。

侵入イベント パケット ビューの使用

パケット ビューは、侵入イベントを生成したルールをトリガーとして使用したパケットに関する情報を表示します。

ヒント イベントを検出するデバイスで [パケットの転送（Transfer Packet）] オプションが無効になっている場合、Secure Firewall Management Center でのパケット ビューにはパケット情報は含まれません。

パケット ビューは、パケットがトリガーとして使用した侵入イベントに関する情報を提供することによって、イベントのタイムスタンプ、メッセージ、分類、優先度、イベントを生成したルール（イベントが標準テキスト ルールによって生成された場合）など、特定のパケットがキャプチャされた理由を示します。パケット ビューは、パケットのサイズなど、パケットに関する一般情報も表示します。

さらに、パケット ビューにはパケット内の各層（データ リンク、ネットワーク、およびトランスポート）について説明したセクションと、パケットを構成するバイトについて説明したセクションがあります。システムがパケットを復号化した場合は、復号化されたバイトを表示できます。折りたたまれたセクションを展開すると、詳細情報を参照できます。

（注） それぞれのポートスキャン イベントは複数のパケットによってトリガーとして使用されるため、ポートスキャン イベントは特別なバージョンのパケット ビューを使用します。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 侵入イベント テーブル ビューの制約 （973 ページ）の説明に従って、侵入イベントのテーブル ビューで、表示するパケットを選択します。

ステップ 2 複数のイベントを選択した場合は、オプションで、ページの下部にあるページ番号を使用することによって、パケット ビューでパケットのページを切り替えることができます。

ステップ 3 次のオプションもあります。

- 調整：パケット ビューで日時範囲を変更するには、時間枠の変更（833 ページ）を参照してください。
- 設定：イベントをトリガした侵入ルールを設定するには、[アクション（Actions）]の横にある矢印をクリックし、パケット ビュー内での侵入ルールの設定（979 ページ）の説明に従って操作を続けます。
- 削除：データベースからイベントを削除するには、[削除（Delete）] をクリックして表示しているパケットのイベントを削除するか、[すべて削除（Delete All）]をクリックして以前に選択したパケットのすべてのイベントを削除します。
- ダウンロード：イベントをトリガーしたパケットのローカル コピー（libpcap 形式のパケット キャプチャ ファイル）をダウンロードするには、[パケットのダウンロード（Download Packet）]をクリックして表示しているイベントに関するキャプチャしたパケットのコピーを保存するか、[すべてのパケットをダウンロード（Download All Packets）] をクリックして以前に選択したパケットのすべてのイベントのキャプチャしたパケットのコピーを保存します。キャプチャされたパケットは libpcap 形式で保存されます。この形式は、複数の一般的なプロトコル アナライザで使用されます。

  （注） 単一のポートスキャン イベントは複数のパケットに基づいているため、ポートスキャン パケットをダウンロードできません。ただし、ポートスキャン ビューは使用可能なすべてのパケット情報を提供します。ダウンロードするには少なくとも 15 % の使用可能なディスク領域が必要です。

- 確認済みのマークを付ける：イベント データベースからは削除せずに、イベント ビューから削除するため確認済みのイベントにマークを付けるには、[確認（Review）]をクリックして表示しているパケットのイベントにマークを付けるか、[すべて確認（Review All）] をクリックして以前に選択したパケットのすべてのイベントにマーク付けます。詳細については、侵入イベントを確認済みとしてマーク （964 ページ）を参照してください。
- 追加情報の表示：ページセクションを展開したり、折りたたんだりするには、セクションの横にある矢印をクリックします。詳細については、イベント情報のフィールド（976 ページ）、フレーム情報のフィールド （983 ページ）、データリンク層情報フィールド （984 ページ）を参照してください。
- ネットワーク層の情報の表示：ネットワーク層情報の表示（985 ページ）を参照してください。
- パケット バイト情報の表示：パケット バイト情報の表示（991 ページ）を参照してください。
- トランスポート層の情報の表示：次を参照してください。 トランスポート層情報の表示（988 ページ）

関連トピック

ポートスキャン検出

イベント情報のフィールド

パケット ビューで、[イベント情報（Event Information）] セクションのパケットに関する情報を表示できます。

イベント

イベントのメッセージ。ルールベースのイベントの場合、これはルール メッセージに対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

イベントの ID は、(GID:SID:Rev) の形式でメッセージに付加されます。GID は、ルール エンジン、デコーダ、またはイベントを生成したプリプロセッサのジェネレータ ID です。SID は、ルール、デコーダ メッセージ、またはプリプロセッサ メッセージの ID です。Rev はルールのリビジョン番号です。

Timestamp

パケットがキャプチャされた時刻（UTC タイム ゾーン）。

分類（Classification）

イベントの分類。ルールベースのイベントの場合、これはルールの分類に対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

プライオリティ

イベントの優先度。ルールベースのイベントの場合、これは `priority` キーワードの値または `classtype` キーワードの値に対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

入力セキュリティ ゾーン（Ingress Security Zone）

イベントをトリガーとして使用したパケットの入力セキュリティ ゾーン。パッシブ展開環境では、このセキュリティ ゾーン フィールドだけに入力されます。

出力セキュリティ ゾーン（Egress Security Zone）

イベントをトリガーとして使用したパケットの出力セキュリティ ゾーン。パッシブ展開では、このフィールドには入力されません。

ドメイン（Domain）

管理対象デバイスが属するドメイン。このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

デバイス

アクセス コントロール ポリシーが展開された管理対象デバイス。

セキュリティ コンテキスト（Security Context）

トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。マルチ コンテキスト モードの ASA FirePOWER の場合に、システムがこのフィールドにデータを設定することに注意してください。

入力インターフェイス（Ingress Interface）

イベントをトリガーとして使用したパケットの入力インターフェイス。パッシブ インターフェイスの場合、このインターフェイスの列だけに入力されます。

出力インターフェイス（Egress Interface）

インラインセットの場合、イベントをトリガーとして使用したパケットの出力インターフェイス。

送信元/宛先 IP（Source/Destination IP）

イベントをトリガーとして使用したパケットの発生元（送信元）であるホスト IP アドレスまたはドメイン名、またはイベントをトリガーとして使用したトラフィックのターゲット（宛先）ホスト。

送信元ポート/ICMP タイプ（Source Port/ICMP Type）

イベントをトリガーとして使用したパケットの送信元ポート。ICMP トラフィックの場合は、ポート番号がないため、システムは ICMP タイプを表示します。

送信先ポート/ICMP コード（Destination Port/ICMP Code）

トラフィックを受信するホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、システムは ICMP コードを表示します。

電子メールのヘッダー（Email Headers）

電子メールのヘッダーから取得したデータ。電子メールのヘッダーは侵入イベントのテーブル ビューには表示されませんが、電子メール ヘッダー データは検索条件として使用できることに注意してください。

電子メールのヘッダーを SMTP トラフィックの侵入イベントと関連付けるには、SMTP プリプロセッサの [ヘッダーのログ（Log Headers）] オプションを有効にする必要があります。ルールベースのイベントの場合、この行は電子メール データが取得されたときに表示されます。

HTTP ホスト名（HTTP Hostname）

（存在する場合）HTTP 要求のホスト ヘッダーから取得されたホスト名。この行には、最大 256 バイトの完全なホスト名が表示されます。ホスト名が 1 行より長い場合は、完全なホスト名を展開できます。

ホスト名を表示するには、HTTP 検査プリプロセッサ [ホスト名のログ（Log Hostname）] オプションを有効にする必要があります。

HTTP要求パケットにホスト名が常に含まれているわけではないことに注意してください。ルールベースのイベントの場合、この行はパケットにHTTPホスト名またはHTTP URIが含まれる場合に表示されます。

HTTP URI

（存在する場合）侵入イベントをトリガーとして使用したHTTP要求パケットに関連付けられたraw URI。この行には、最大2048バイトの完全なURIが表示されます。URIが1行より長い場合は、完全なURIを展開できます。

URIを表示するには、HTTP検査プリプロセッサ[URIのログ（Log URI）]オプションを有効にする必要があります。

HTTP要求パケットにURIが常に含まれているわけではないことに注意してください。ルールベースのイベントの場合、この行はパケットにHTTPホスト名またはHTTP URIが含まれる場合に表示されます。

HTTP応答によってトリガーとして使用された侵入イベントの関連HTTP URIを参照するには、[両方のポートでのストリーム再構成の実行（Perform Stream Reassembly on Both Ports）]オプションにHTTPサーバのポートを設定する必要があります。ただし、これにより、トラフィックのリアセンブル用のリソース要求が増加することに注意してください。

侵入ポリシー（Intrusion Policy）

（存在する場合）侵入イベントを生成した侵入、プリプロセッサ、デコーダのルールが有効にされた侵入ポリシー。アクセス コントロール ポリシーのデフォルト アクションとして侵入ポリシーを選択するか、アクセス コントロール ルールと侵入ポリシーを関連付けることができます。

アクセス コントロール ポリシー（Access Control Policy）

イベントを生成した侵入ルール、プリプロセッサ ルール、またはデコーダ ルールが有効にされた侵入ポリシーが含まれるアクセス コントロール ポリシー。

アクセス コントロール ルール（Access Control Rule）

イベントを生成した侵入ルールと関連付けられたアクセス コントロール ルール。[デフォルト アクション（Default Action）]は、ルールが有効にされた侵入ポリシーがアクセス コントロール ルールに関連付けられていないことと、代わりにアクセス コントロール ポリシーのデフォルト アクションとして設定されていることを示します。

ルール（Rule）

標準テキスト ルール イベントの場合、イベントを生成したルール。

イベントが、共有オブジェクト ルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

ルールデータにはネットワークに関する機密情報が含まれるため、管理者はユーザがローカルルールの表示権限を使用してパケット ビューでルール情報を表示できる機能を、ユーザ ロール エディタで切り替えることができます。

アクション（Actions）

標準テキスト ルールとカスタム ルールのイベントの場合は、[アクション（Actions）] を展開して、イベントをトリガーとして使用したルールに次の操作のいずれかを実行します。

- ルールを編集する
- ルールのバージョンのドキュメントを表示します。標準的なテキストルールのみの場合、[アクション（Actions）] から [ドキュメントの表示（View Documentation）] をクリックした後、ドキュメントのポップアップ ウィンドウの [ルール ドキュメント（Rule Documentation）] をクリックすると、より具体的なルールの詳細を表示することができます。
- ルールにコメントを追加する
- ルールの状態を変更する
- ルールのしきい値を設定する
- ルールを抑制する

イベントが、共有オブジェクトルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

パケット ビュー内での侵入ルールの設定

侵入イベントのパケットビュー内で、イベントをトリガーとして使用したルールに対して複数のアクションを実行できます。イベントが、共有オブジェクトルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

手順

ステップ 1 侵入ルールによって生成された侵入イベントのパケット ビュー内で、[イベント情報（Event Information）] セクションの [アクション（Actions）] を展開します。

ステップ 2 次の選択肢があります。

- コメント：標準テキスト ルール イベントの場合、[ルール コメント（Rule Comment）] をクリックして、イベントを生成したルールにテキスト コメントを追加します。これにより、ルールや、特定されたエクスプロイトまたはポリシー違反に関するコンテキストおよび情報を提供できます。さらに、侵入ルールエディタでルールのコメントの追加および表示を行うこともできます。
- 無効化：このルールを無効にするには、次のオプションのいずれかをクリックします。
  - **現在のSnort 2ポリシー（<policy_name>）でこのルールを無効にします（Disable this rule in the current Snort 2 policy (<policy_name>)）**

- **ローカルで作成されたすべてのSnort 2ポリシーでこのルールを無効にします（Disable this rule in all locally created Snort 2 policies）**

このイベントが標準テキストルールによって生成された場合は、必要に応じてルールを無効にできます。ローカルで編集できるすべてのポリシーにルールを設定できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみにルールを設定することもできます。

現在のポリシーオプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタムポリシーを編集できますが、システムが提供するデフォルト ポリシーは編集できません。

（注） パケット ビューから共有オブジェクト ルールを無効にしたり、デフォルトのポリシーでルールを無効にしたりすることはできません。

- パケットのドロップとイベントの生成：トリガー元になったパケットをドロップしてイベントを生成するルールを設定するには、次のオプションのいずれかをクリックします。
  - **トリガーパケットをドロップし、現在のSnort 2ポリシー（<policy_name>）でイベントを生成するには、このルールを設定します（Set this rule to drop the triggering packet and generate an event in the current Snort 2 policy (<policy_name>)）**
  - **トリガーパケットをドロップし、ローカルで作成されたすべてのSnort 2インラインポリシーでイベントを生成するには、このルールを設定します（Set this rule to drop the triggering packet and generate an event in all locally created Snort 2 inline policies）**

管理対象デバイスがネットワーク上でインライン展開されている場合、イベントをトリガーとして使用したルールを設定して、ローカルで編集できるすべてのポリシーでルールをトリガーするパケットをドロップできます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみにルールを設定することもできます。

現在のポリシーオプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタムポリシーを編集できますが、システムが提供するデフォルト ポリシーは編集できません。このオプションは [インラインの場合ドロップ（Drop when Inline）] が現在のポリシーで有効になっている場合のみ表示されることに注意してください。

- 編集：標準テキストルールイベントの場合、[編集（Edit）]（Snort 2 を編集する場合）または [Snort 3ルールの編集（Edit Snort 3 Rule）] をクリックして、イベントを生成したルールを編集します。イベントが、共有オブジェクトルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できません。

（注） システムによって提供された（カスタム標準テキストルールではない）ルールを編集する場合、実際には新規のローカルルールを作成していることになります。ローカルルールを設定して、イベントを生成し、現在の侵入ポリシーで元のルールを無効にしていることを確認してください。ただし、デフォルトのポリシーのローカルルールは有効にできないことに注意してください。

- イベントの生成：[ローカルで作成されたすべてのSnort 2ポリシーでイベントを生成するには、このルールを設定します（Set this rule to generate events in all locally created Snort 2 policies）] をクリックして、イベントを生成するルールを設定します。

  このイベントが標準テキストルールによって生成された場合は、ルールを設定して、ローカルで編集できるすべてのポリシーでイベントを生成できます。

  現在のポリシーオプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタムポリシーを編集できますが、システムが提供するデフォルト ポリシーは編集できません。

  （注） 共有オブジェクト ルールでパケット ビューからイベントを生成したり、デフォルト ポリシーでルールを無効にしたりすることはできません。

- 抑制オプションの設定：パケット ビュー内での抑制オプションの設定（982 ページ）の説明に従って、[抑制オプションの設定（Set Suppression Options）] を展開し、続行します。

  このオプションを使用して、ローカルで編集できるすべてのポリシーで、このイベントをトリガーとして使用したルールを抑制できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみでルールを制約することもできます。

  現在のポリシーオプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタムポリシーを編集できますが、シスコが提供するデフォルト ポリシーは編集できません。

- しきい値オプションの設定：パケット ビュー内でのしきい値オプションの設定（981 ページ）の説明に従って、[しきい値オプションの設定（Set Thresholding Options）] を展開し、続行します。

  このオプションを使用して、ローカルで編集できるすべてのポリシーでも、これをトリガーとして使用したルールのしきい値を作成できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）でのみしきい値を作成することもできます。

  現在のポリシーオプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタムポリシーは編集できますが、システムが提供するデフォルトの侵入ポリシーは編集できません。

- ドキュメントの表示：[ドキュメントの表示（View Documentation）] をクリックして、イベントを生成したルールの説明を確認します。次に、必要に応じて [ルール ドキュメンテーション（Rule Documentation）] をクリックして、ルールの詳細を表示します。

パケット ビュー内でのしきい値オプションの設定

侵入イベントのパケット ビューでしきい値オプションを設定することによって、ルールごとに時間の経過とともに生成されるイベントの数を制御できます。ローカルで編集できるすべてのポリシーに、またはローカルで編集できる場合は現在のポリシー（つまり、イベントを生成したポリシー）のみに、しきい値オプションを設定できます。

手順

ステップ 1 侵入ルールによって生成された侵入イベントのパケット ビュー内で、[イベント情報（Event Information）] セクションの [アクション（Actions）] を展開します。

ステップ 2 [しきい値オプションの設定（Set Thresholding Options）] を展開し、次の 2 つの有効なオプションから 1 つを選択します。

- 現在のSnort 2ポリシー（<policy_name>）（in the current Snort 2 policy (<policy_name>)）
- ローカルで作成されたすべてのSnort 2ポリシー（in all locally created Snort 2 policies）

ステップ 3 設定するしきい値のタイプを選択します。

- 通知を期間ごとに指定したイベント インスタンスの数に制限する場合は、[制限（limit）] をクリックします。
- 期間ごとに指定したイベント インスタンス数に達するたびに通知を行う場合は、[しきい値（threshold）] をクリックします。
- 指定されたイベント インスタンス数に達した後で、期間あたり 1 回ずつ通知を行う場合は、[両方（Both）] をクリックします。

ステップ 4 該当するしきい値をクリックして、イベントインスタンスを [送信元（Source）] IP アドレスと [宛先（Destination）] IP アドレスのどちらで追跡するかを指定します。

ステップ 5 [カウント（Count）] フィールドに、しきい値として使用するイベント インスタンスの数を入力します。

ステップ 6 [秒（Seconds）] フィールドに、イベント インスタンスを追跡する期間を指定する数（1 ～ 86400）を入力します。

ステップ 7 既存の侵入ポリシーでこのルールの現在のしきい値をオーバーライドする場合は、[このルールの既存の設定をオーバーライドする（Override any existing settings for this rule）] チェックボックスをオンにします。

ステップ 8 [しきい値の保存（Save Thresholding）] をクリックします。

パケット ビュー内での抑制オプションの設定

抑制オプションを使用して、侵入イベントをまとめて、または送信元 IP アドレスまたは宛先 IP アドレスに基づいて抑制できます。ローカルで編集できるすべてのポリシーで抑制オプションを設定できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみに抑制オプションを設定することもできます。

手順

ステップ 1 侵入ルールによって生成された侵入イベントのパケット ビュー内で、[イベント情報（Event Information）] セクションの [アクション（Actions）] を展開します。

ステップ 2 [抑制オプションの設定（Set Suppression Options）] を展開し、次の 2 つの有効なオプションから 1 つを選択します。

- 現在のSnort 2ポリシー（<policy_name>）（in the current Snort 2 policy (<policy_name>)）
- ローカルで作成されたすべてのSnort 2ポリシー（in all locally created Snort 2 policies）

（注） 現在のポリシーオプションは、現在のポリシーを編集できる場合にのみ表示されます。たとえば、カスタムポリシーを編集できますが、シスコが提供するデフォルトポリシーは編集できません。

ステップ 3 次のいずれかの [追跡対象（Track By）] オプションを選択します。

- 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[送信元（Source）] をクリックします。
- 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[宛先（Destination）] をクリックします。
- このイベントをトリガーしたルールのイベントを完全に抑制する場合は、[ルール（Rule）] をクリックします。

ステップ 4 [IP アドレス（IP address）] または [CIDR ブロック（CIDR block）] フィールドに、送信元または宛先 IP アドレスとして指定する IP アドレスまたは CIDR ブロック/プレフィクス長を入力します。

ステップ 5 [抑制の保存（Save Suppression）] をクリックします。

関連トピック

IP アドレスの規則 （31 ページ）

フレーム情報のフィールド

パケット ビューで、[フレーム（Frame）] の横にある矢印をクリックして、キャプチャされたフレームに関する情報を表示します。パケット ビューには単一フレームまたは複数フレームを表示できます。各フレームには、個々のネットワークのパケットに関する情報が表示されます。たとえば、タグ付きパケットまたは再構成された TCP ストリーム内のパケットの場合、複数のフレームが表示されます。

フレーム n（Frame n）

キャプチャされたフレーム。*n* は単一フレーム パケットの場合は 1、複数フレーム パケットの場合は差分フレーム番号です。フレーム内のキャプチャされたバイト数はフレーム番号に追加されます。

到着時間（Arrival Time）

フレームがキャプチャされた日時。

キャプチャ済みのフレームの時間デルタ（Time delta from previous captured frame）

複数フレーム パケットの場合、前のフレームがキャプチャされてからの経過時間。

表示済みのフレームの時間デルタ（Time delta from previous displayed frame）

複数フレーム パケットの場合、前のフレームが表示されてからの経過時間。

参照以降または先頭フレームからの時間（Time since reference or first frame）

複数フレーム パケットの場合、最初のフレームがキャプチャされてからの経過時間。

フレーム番号（Frame Number）

差分フレーム番号。

フレーム長（Frame Length）

フレームの長さ（バイト単位）。

キャプチャ長（Capture Length）

キャプチャされたフレームの長さ（バイト単位）。

フレームはマーク済み（Frame is marked）

フレームがマークされているかどうか（true または false）。

フレーム内のプロトコル（Protocols in frame）

フレームに含まれるプロトコル。

関連トピック

tag キーワード
TCP ストリームの再構成

データリンク層情報フィールド

パケット ビューで、データリンク層プロトコル（たとえば、[イーサネット II（Ethernet II）]）の横にある矢印をクリックして、パケットに関するデータリンク層情報を表示します。これには、送信元ホストおよび宛先ホストの 48 ビットの Media Access Control（MAC）アドレスが含まれます。ハードウェア プロトコルに応じて、パケットに関する他の情報も表示されることがあります。

（注） この例では、イーサネット リンク層情報について説明していることに注意してください。他のプロトコルも表示されることがあります。

パケット ビューはデータリンク層で使用されるプロトコルを反映します。次のリストでは、パケット ビューでイーサネット II または IEEE 802.3 イーサネット パケットについて参照できる情報について説明します。

[接続先（Destination）]

宛先ホストの MAC アドレス。

（注） イーサネットは、宛先アドレスとしてマルチキャストおよびブロードキャストアドレスを使用することもできます。

ソース（Source）

送信元ホストの MAC アドレス。

タイプ（Type）

イーサネットIIパケットの場合、イーサネットフレームでカプセル化されるパケットの種類。たとえば、IPv6 または ARP データグラム。この項目はイーサネット II パケットの場合にのみ表示されることに注意してください。

長さ（Length）

IEEE 802.3イーサネットパケットの場合、チェックサムを含まないパケットのトータル長（バイト単位）。この項目は IEEE 802.3 イーサネット パケットの場合にのみ表示されることに注意してください。

ネットワーク層情報の表示

手順

パケット ビューで、パケットにネットワーク層プロトコル（たとえば、[インターネット プロトコル（Internet Protocol）]）の横にある矢印をクリックして、パケットに関連したネットワーク層の情報の詳細情報を表示します。

（注） この例では、IPパケットについて説明していることに注意してください。他のプロトコルも表示されることがあります。

IPv4 ネットワーク層の情報フィールド

以下のリストは、IPv4パケットで表示される可能性があるプロトコル固有の情報の説明です。

バージョン（Version）

インターネット プロトコルのバージョン番号。

ヘッダー長（Header Length）

すべての IP オプションを含む、見出しのバイト数。オプションのない IP 見出しの長さは 20 バイトです。

差別化サービス フィールド（Differentiated Services Field）

送信元ホストが明示的輻輳通知（ECN）サポートする方法を示す次の差別化サービスの値。

- `0x0`：ECN-Capable Transport（ECT）をサポートしません
- `0x1` および `0x2`：ECT をサポートします
- `0x3`：Congestion Experienced（CE）

トータル長（Total Length）

IP 見出しを差し引いた IP パケットの長さ（バイト単位）。

ID

送信元ホストから送信される IP データグラムを一意的に識別する値。この値は同じデータグラム フラグメントをトレースするために使用されます。

フラグ（Flags）

IP フラグメンテーションを制御する値。

[最後のフラグメント（Last Fragment）] フラグの値は、データグラムに関連付けられた追加のフラグメントが存在するかどうかを次のように示します。

- `0`：データグラムに関連付けられた追加のフラグメントは存在しない
- `1`：データグラムに関連付けられた追加のフラグメントが存在する

[フラグメント禁止（Don’t Fragment）] フラグの値は、データグラムをフラグメント化できるかどうかを次のように制御します。

- `0`：データグラムをフラグメント化できる
- `1`：データグラムをフラグメント化**してはならない**

フラグメント オフセット（Fragment Offset）

データグラムの先頭からのフラグメント オフセットの値。

存続可能時間（ttl）（Time to Live (ttl)）

データグラムが期限切れになる前にデータグラムがルータ間で作成できるホップの数。

プロトコル

IP データグラムにカプセル化されるトランスポート プロトコル。たとえば、ICMP、IGMP、TCP、または UDP。

ヘッダー チェックサム（Header Checksum）

IP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損したか、侵入回避の試行において使用中である可能性があります。

送信元または送信先（Source/Destination）

送信元（または宛先）ホストの IP アドレスまたはドメイン名。

ドメイン名を表示するには、IP アドレス解決を有効にする必要があることに注意してください。

アドレスまたはドメイン名をクリックしてコンテキストメニューを表示してから、whois 検索を実行する場合は [Whois] を、ホスト情報を表示する場合は [ホストプロファイルの表示（View Host Profile）] を、アドレスをグローバルブロックリストまたはブロックしないリストに追加するオプションを選択します。

IPv6 ネットワーク層の情報フィールド

以下のリストは、IPv6 パケットで表示される可能性があるプロトコル固有の情報の説明です。

トラフィック クラス（Traffic Class）

IPv4 で提供される差別化サービス機能と同じように、IPv6 パケット クラスまたは優先度を特定する IPv6 見出し内の Experimental 8 ビットのフィールド。未使用の場合、このフィールドはゼロに設定されます。

フロー ラベル（Flow Label）

非デフォルトの QoS またはリアルタイム サービスなどの特別なフローを特定する、1 から FFFF までの、オプションの 20 ビットの IPv6 16 進数値。未使用の場合、このフィールドはゼロに設定されます。

ペイロード長（Payload Length）

IPv6 ペイロードのオクテットの数を特定する 16 ビット フィールド。これは、任意の拡張子見出しを含む、IPv6 見出しに続くすべてのパケットで構成されます。

次ヘッダー（Next Header）

IPv4 プロトコル フィールドと同じ値を使用して、IPv6 見出しのすぐ後に続く、見出しの種類を特定する 8 ビットのフィールド。

ホップ リミット（Hop Limit）

パケットを転送するノードごとに 1 つずつデクリメントする 8 ビットの 10 進整数。デクリメントした値がゼロになると、パケットは破棄されます。

ソース（Source）

送信元ホストの 128 ビットの IPv6 アドレス。

[接続先（Destination）]

宛先ホストの 128 ビットの IPv6 アドレス。

トランスポート層情報の表示

手順

ステップ 1 パケット ビューで、トランスポート層プロトコル（たとえば [TCP]、[UDP]、または [ICMP]）の横にある矢印をクリックします。

ステップ 2 オプションで、存在する場合、[データ（Data）] をクリックして、パケット ビューの [パケット情報（Packet Information）] セクションで、プロトコルのすぐ上にあるペイロードの最初の 24 バイトを表示します。

ステップ 3 TCP パケット ビューのフィールド （988 ページ）、UDP パケット ビューのフィールド （989 ページ）、またはICMP パケット ビュー フィールド （990 ページ）の説明に従って、TCP、UDP、ICMP プロトコルのトランスポート層の内容を表示します。

（注） これらの例では、TCP、UDP、ICMP パケットについて説明していますが、他のプロトコルも表示されることがあることに注意してください。

TCP パケット ビューのフィールド

ここでは、TCP パケットのプロトコル固有の情報について説明します。

ソース ポート

発信元のアプリケーション プロトコルを識別する番号。

接続先ポート（Destination port）

受信側のアプリケーション プロトコルを識別する番号。

シーケンス番号（Sequence number）

TCP ストリームの初期シーケンス番号と連動する、現在の TCP セグメントの最初のバイトの値。

次のシーケンス番号（Next sequence number）

応答パケットにおける、送信する次のパケットのシーケンス番号。

確認応答番号（Acknowledgement number）

以前に受信されたデータのシーケンス番号に連動した TCP 確認応答。

ヘッダー長（Header Length）

ヘッダーのバイト数。

フラグ（Flags）

TCP セグメントの転送状態を示す 6 ビット。

- U：緊急ポインタが有効
- A：確認応答番号が有効
- P：受信者はデータをプッシュする必要がある
- R：接続をリセットする
- S：シーケンス番号を同期して新しい接続を開始する
- F：送信者はデータ送信を終了した

ウィンドウ サイズ（Window size）

受信ホストが受け入れる、確認応答されていないデータの量（バイト単位）。

チェックサム（Checksum）

TCP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損したか、回避の試行において使用中である可能性があります。

緊急ポインタ（Urgent Pointer）

緊急データが終了する TCP セグメントの位置（存在する場合）。U フラグとともに使用します。

オプション（Options）

TCP オプションの値（存在する場合）。

UDP パケット ビューのフィールド

ここでは、UDP パケットのプロトコル固有の情報について説明します。

ソース ポート

発信元のアプリケーション プロトコルを識別する番号。

接続先ポート（Destination port）

受信側のアプリケーション プロトコルを識別する番号。

長さ（Length）

UDP 見出しとデータを組み合わせた長さ。

チェックサム（Checksum）

UDPチェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損した可能性があります。

ICMP パケット ビュー フィールド

ここでは、ICMP パケットのプロトコル固有の情報について説明します。

タイプ

ICMP メッセージのタイプ。

- 0：エコー応答
- 3：宛先到達不能
- 4：ソース クエンチ（始点抑制要求）
- 5：リダイレクト
- 8：エコー要求
- 9：ルータ アドバタイズメント
- 10：ルータ送信要求
- 11：時間超過
- 12：パラメータの問題
- 13：タイムスタンプ要求
- 14：タイムスタンプ応答
- 15：情報要求（廃止）
- 16：情報応答（廃止）
- 17：アドレス マスク要求
- 18：アドレス マスク応答

コード

ICMP メッセージ タイプに付随するコード。ICMP メッセージ タイプ 3、5、11、および 12 には、RFC 792 で説明されている対応コードがあります。

チェックサム（Checksum）

ICMP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損した可能性があります。

パケット バイト情報の表示

手順

パケット ビューで、[パケット バイト（Packet Bytes）] の横にある矢印をクリックして、パケットを構成するバイトの 16 進数および ASCII バージョンを表示します。システムがトラフィックを復号化した場合は、復号化されたパケット バイトを表示できます。

内部ソースからの侵入イベント

内部ソースからの侵入イベントは、ネットワーク上の侵害を受けたホストを示しています。ソース IP アドレスがネットワーク上にある場合は、そのホストを調査する必要があることを示しています。

侵入イベントの統計情報の表示

[侵入イベントの統計情報（Intrusion Event Statistics）] ページは、アプライアンスの現在の状態の概要と、ネットワークで生成されたすべての侵入イベントを表示します。

このページに表示される IP アドレス、ポート、プロトコル、イベント メッセージなどはそれぞれリンクになっています。関連イベントの情報を表示するには、任意のリンクをクリックします。たとえば、上位 10 個の宛先ポートのいずれかが `80 (http) /tcp` である場合、そのリンクをクリックすると、デフォルトの侵入イベント ワークフローの最初のページが表示され、そのポートをターゲットとするイベントがリストされます。現在の時刻範囲で表示されるのはイベント（およびイベントを生成する管理対象デバイス）のみであることに注意してください。さらに、確認済みマークを付けた侵入イベントも統計に引き続き表示されます。たとえば、現在の時刻範囲が過去 1 時間であり、最初のイベントが 5 時間前に生成された場合、[最初のイベント（First Event）] リンクをクリックすると、そのイベントは時刻範囲を変更するまでイベント ページには表示されません。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[概要（Overview）] > [概要（Summary）] > [侵入イベント統計（Intrusion Event Statistics）]** を選択します。

ステップ 2 ページの上部にある2つの選択ボックスから、統計を表示するゾーンおよびデバイスを選択するか、[すべてのセキュリティ ゾーン（All Security Zones）] および [すべてのデバイス（All Devices）] を選択して、侵入イベントを収集するすべてのデバイスの統計を表示します。

ステップ 3 [統計の取得（Get Statistics）] をクリックします。

ヒント カスタム時刻範囲からデータを表示するには、右上のページエリアのリンクをクリックし、時間枠の変更 （833 ページ）にある指示に従います。

ホスト統計情報

[侵入イベント統計情報（Intrusion Event Statistics）] ページの [ホスト統計情報（Host Statistics）] セクションは、アプライアンス自体に関する情報を提供します。Secure Firewall Management Center では、このセクションはすべての管理対象デバイスに関する情報も提供します。

この情報には、次の内容が含まれます。

時刻（Time）

アプライアンスの現在の時刻。

アップタイム（Uptime）

アプライアンス自体が再起動してから経過した日数、時間、および分数。Secure Firewall Management Center では、[アップタイム（Uptime）] に各管理対象デバイスの最終起動時刻、ログインしたユーザの数、および負荷平均も示されます。

ディスク使用率（Disk Usage）

使用中のディスクの割合。

メモリ使用率（Memory Usage）

使用中のシステム メモリの割合。

負荷平均（Load Average）

直前の 1 分間、5 分間、15 分間の CPU キュー内の平均プロセス数。

イベントの概要

[侵入イベント統計（Intrusion Event Statistics）] ページの [イベントの概要（Event Overview）] セクションは、侵入イベント データベースにある情報の概要を示します。

これらの統計には、次の情報が含まれています。

イベント

侵入イベント データベースのイベントの数。

時間範囲内のイベント（Events in Time Range）

現在選択されている時間範囲と、時間範囲内に収まるデータベースのイベントの割合。

最初のイベント（First Event）

イベント データベース内の最初のイベントのイベント メッセージ。

最後のイベント（Last Event）

イベント データベース内の最後のイベントのイベント メッセージ。

（注） Secure Firewall Management Center で侵入イベント データを表示中に管理対象デバイスを選択した場合は、そのデバイスの [イベントの概要（Event Overview）] セクションが代わりに表示されます。

イベント統計

[侵入イベント統計（Intrusion Event Statistics）] ページの [イベント統計（Event Statistics）] セクションでは、侵入イベント データベース内の情報に関する具体的な情報が表示されます。

この情報には、次に関する詳細が含まれます。

- 上位 10 個のイベント タイプ
- 上位 10 個の送信元 IP アドレス
- 上位 10 個の宛先 IP アドレス
- 上位 10 個の宛先ポート
- イベント数が最大であるプロトコル、イングレスとイーグレスのセキュリティ ゾーン、およびデバイス

（注） マルチドメイン展開では、システムは、各リーフ ドメインに個別のネットワーク マップを作成します。その結果、リーフ ドメインには、ネットワーク内で一意である IP アドレスを含めることができますが、別のリーフ ドメイン内の IP アドレスと同じにすることができます。先祖ドメインでイベントの統計情報を表示すると、システムで、その IP アドレスの複数のインスタンスが繰り返し表示される場合があります。一見すると、エントリが重複しているように見えることがあります。ただし、各 IP アドレスのホスト プロファイル情報までドリル ダウンすると、それらが異なるリーフ ドメインに属していることがわかります。

侵入イベントのパフォーマンス グラフの表示

[侵入イベントのパフォーマンス（Intrusion Event Performance）] ページでは、Secure Firewall Management Center または管理対象デバイスの指定された期間の侵入イベントのパフォーマンス統計情報を示すグラフを生成できます。グラフを生成することにより、1 秒あたりの侵入イベントの数、1 秒あたりのメガビット数、1 パケットあたりの平均バイト数、Snort によって検査されていないパケットの割合、および TCP 正規化の結果としてブロックされたパケットの数を反映できます。これらのグラフは、過去 1 時間、前日、先週、または先月の操作の統計を表示できます。

（注） 新しいデータは 5 分ごとに統計グラフに蓄積されます。したがって、グラフをすばやくリロードしても、次の 5 分の差分更新が実行されるまでデータは変更されていない場合があります。各グラフには、選択した時間間隔（前月、週、日、または時間）に対応した間隔（日、時間、または 5 分）で平均値が表示されます。平均値が 1 未満の場合は、小数値で表示されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[概要（Overview）] > [概要（Summary）] > [侵入イベントパフォーマンス（Intrusion Event Performance）]**を選択します。

ステップ 2 [デバイスの選択（Select Device）] リストから、データを表示するデバイスを選択します。

ステップ 3 侵入イベントのパフォーマンス統計情報グラフの種類（994 ページ）で説明されているように、[グラフの選択（Select Graph(s)）] リストから、作成するグラフの種類を選択します。

ステップ 4 [時間範囲の選択（Select Time Range）] リストから、グラフに使用する時間範囲を選択します。

ステップ 5 [グラフ（Graph）] をクリックします。

ステップ 6 グラフを保存するには、グラフを右クリックし、ブラウザでイメージを保存する手順に従います。

侵入イベントのパフォーマンス統計情報グラフの種類

次の表に、表示可能なグラフの種類を示します。ネットワーク分析ポリシーの [インライン モード（Inline Mode）] 設定の影響を受けるデータを含むグラフ タイプでは、表示が異なるので注意してください。[インライン モード（Inline Mode）] が無効になっている場合、Web インターフェイスでアスタリスク（*）が付いているグラフタイプ（下記の表では列に [はい（yes）] と記載）には、[インライン モード（Inline Mode）] が有効になっている場合に変更またはドロップされるトラフィックに関するデータが含まれています。

表 *114*：侵入イベントのパフォーマンス グラフの種類

データの生成対象となるグラフ	実行する操作	説明	インラインモードによる影響
平均バイト/パケット（Avg Bytes/Packet）	適用対象外	各パケットに含まれる平均バイト数。	いいえ
TCP トラフィックまたはパケットで正規化された ECN フラグ（ECN Flags Normalized in TCP Traffic/Packet）	[明示的輻輳通知（Explicit Congestion Notification）] を有効にして、[パケット（Packet）] を選択します。	ネゴシエーションに関係なく、パケット単位で ECN フラグがクリアされたパケットの数。	Yes
TCP トラフィックまたはセッションで正規化された ECN フラグ（ECN Flags Normalized in TCP Traffic/Session）	[明示的輻輳通知（Explicit Congestion Notification）] を有効にして、[ストリーム（Stream）] を選択します。	ECN の使用がネゴシエートされなかった場合にストリーム単位で ECN フラグがクリアされた回数。	Yes
イベント/秒（Events/Sec）	適用対象外	デバイスで生成された 1 秒あたりのイベント数。	いいえ
ICMPv4 エコーの正規化（ICMPv4 Echo Normalizations）	[ICMPv4 の正規化（Normalize ICMPv4）] を有効にします。	エコー（要求）またはエコー応答メッセージの 8 ビット コード フィールドがクリアされた ICMPv4 パケットの数。	Yes
ICMPv6 エコーの正規化（ICMPv6 Echo Normalizations）	[ICMPv6 の正規化（Normalize ICMPv6）] を有効にします。	エコー（要求）またはエコー応答メッセージの 8 ビット コード フィールドがクリアされた ICMPv6 パケットの数。	Yes
IPv4 DF フラグの正規化	[IPv4 の正規化（Normalize IPv4）] と [DF ビットの正規化（Normalize Don't Fragment Bit）] を有効にします。	[IPv4 フラグ（IPv4 Flags）] ヘッダー フィールドのシングル ビット [フラグメント禁止（Don't Fragment）] サブフィールドがクリアされた IPv4 パケットの数。	Yes
IPv4 オプションの正規化（IPv4 Options Normalizations）	[IPv4 の正規化（Normalize IPv4）] を有効にします。	オプション オクテットが「1」（操作なし（No Operation））に設定された IPv4 パケットの数。	はい
IPv4 予約済みフラグの正規化	[IPv4 の正規化（Normalize IPv4）] と [予約済みビットの正規化（Normalize Reserved Bit）] を有効にします。	[IPv4 フラグ（IPv4 Flags）] ヘッダー フィールドのシングル ビット [予約済み（Reserved）] サブフィールドがクリアされた IPv4 パケットの数。	Yes

データの生成対象となるグラフ	実行する操作	説明	インラインモードによる影響
IPv4 サイズ変更の正規化（IPv4 Resize Normalizations）	[IPv4 の正規化（Normalize IPv4）] を有効にします。	超過ペイロードが IP ヘッダーで指定されたデータグラム長に切り詰められた IPv4 パケットの数。	Yes
IPv4 TOS の正規化	[IPv4 の正規化（Normalize IPv4）] と [TOS ビットの正規化（Normalize TOS Bit）] を有効にします。	1 バイトの [差別化サービス（DS）（Differentiated Services (DS)）] フィールド（旧 [タイプ オブ サービス（ToS）（Type of Service (TOS)）] フィールド）がクリアされた IPv4 パケットの数。	Yes
IPv4 TTL の正規化（IPv4 TTL Normalizations）	[IPv4 の正規化（Normalize IPv4）]、[最大 TTL（Maximum TTL）]、および [TTL のリセット（Reset TTL）] を有効にします。	IPv4 存続時間（TTL）正規化の数。	はい
IPv6 オプションの正規化（IPv6 Options Normalizations）	[IPv6 の正規化（Normalize IPv6）] を有効にします。	[ホップバイホップ オプション（Hop-by-Hop Options）] または [宛先オプション（Destination Options）] 拡張ヘッダーの [オプション タイプ（Option Type）] フィールドが、00（スキップして処理を続行）に設定された IPv6 パケットの数。	Yes
IPv6 TTL の正規化（IPv6 TTL Normalizations）	[IPv6 の正規化（Normalize IPv6）]、[最小 TTL（Minimum TTL）]、および [TTL のリセット（Reset TTL）] を有効にします。	IPv6 ホップ リミット（TTL）正規化の数。	はい
メガビット/秒（Mbits/Sec）	適用対象外	デバイスをパススルーするトラフィックの 1 秒あたりのメガビット数。	いいえ
MSS に合わせてサイズ変更されたパケットの正規化（Packet Resized to Fit MSS Normalizations）	[データを MSS にトリミング（Trim Data to MSS）] を有効にします。	ペイロードが TCP データ フィールドよりも長かったため、ペイロードが最大セグメント サイズに切り詰められたパケットの数。	はい
TCP ウィンドウに合わせてサイズ変更されたパケットの正規化（Packet Resized to Fit TCP Window Normalizations）	[データをウィンドウにトリミング（Trim Data to Window）] を有効にします。	受信側ホストの TCP ウィンドウに合わせて TCP データ フィールドが切り詰められたパケットの数。	はい

データの生成対象となるグラフ	実行する操作	説明	インラインモードによる影響
ドロップされたパケットの割合（Percent Packets Dropped）	適用対象外	選択されたすべてのデバイスにおける未検査のパケットの平均割合。たとえば、2 つのデバイスを選択した場合、平均が 50 % であるというのは、1 つのデバイスのドロップ率が 90 % であり、もう 1 つのデバイスのドロップ率が 10 % であることを示している可能性があります。また、両方のデバイスのドロップ率が 50% である可能性もあります。グラフは、1 つのデバイスを選択した場合にのみ合計ドロップ率を表します。	いいえ
データが除去された RST パケットの正規化（RST Packets With Data Stripped Normalizations）	[RST に関するデータを削除（Remove Data on RST）] を有効にします。	TCP リセット（RST）パケットからデータが削除されたパケットの数。	はい
データが除去された SYN パケットの正規化（SYN Packets With Data Stripped Normalizations）	[SYN に関するデータを削除（Remove Data on SYN）] を有効にします。	TCP オペレーティング システムが Mac OS でない場合に、SYN パケットからデータが削除されたパケットの数。	はい
TCP ヘッダー パディングの正規化（TCP Header Padding Normalizations）	[オプション パディング バイトの正規化またはクリア（Normalize/Clear Option Padding Bytes）] を有効にします。	オプションの埋め込みバイトが 0 に設定された TCP パケットの数。	はい
TCP オプションなしの正規化（TCP No Option Normalizations）	[これらの TCP オプションを許可（Allow These TCP Options）] を有効にして、[任意（any）] 以外のオプションに設定します。	タイムスタンプ オプションがストリップされたパケットの数。	はい
TCP NS フラグの正規化（TCP NS Flag Normalizations）	[明示的輻輳通知（Explicit Congestion Notification）] を有効にして、[パケット（Packet）] を選択します。	ECN Nonce Sum（NS）オプション正規化の数。	はい

データの生成対象となるグラフ	実行する操作	説明	インラインモードによる影響
TCP オプションの正規化（TCP Options Normalizations）	[これらの TCP オプションを許可（Allow These TCP Options）] を有効にして、[任意（any）] 以外のオプションに設定します。	オプション フィールドが [操作なし（No Operation）]（TCP オプション 1）に設定されているオプションの数（[MSS]、[ウィンドウ スケール（Window Scale）]、[タイム スタンプ（Time Stamp）]、および明示的に許可されたオプションを除く）。	はい
正規化によってブロックされた TCP パケット（TCP Packets Blocked By Normalizations）	[TCP ペイロードの正規化（Normalize TCP Payload）] を有効にします（セグメントのリアセンブリは失敗します）。	TCP セグメントを正常にリアセンブルできなかったためにドロップされたパケットの数。	はい
TCP 予約済みフラグの正規化（TCP Reserved Flags Normalizations）	[予約済みビットの正規化またはクリア（Normalize/Clear Reserved Bits）] を有効にします。	予約済みビットがクリアされた TCP パケットの数。	はい
TCP セグメント リアセンブリの正規化（TCP Segment Reassembly Normalizations）	[TCP ペイロードの正規化（Normalize TCP Payload）] を有効にします（セグメントのリアセンブリは成功します）。	再送信データの一貫性を確保するために [TCP データ（TCP Data）] フィールドが正規化されたパケットの数。（正しくリアセンブルできないセグメントはすべてドロップされます）。	はい
TCP SYN オプションの正規化（TCP SYN Option Normalizations）	[これらの TCP オプションを許可（Allow These TCP Options）] を有効にして、[任意（any）] 以外のオプションに設定します。	SYN 制御ビットが設定されていないため、[最大セグメント サイズ（Maximum Segment Size）] または [ウィンドウ スケール（Window Scale）] オプションが [操作なし（No Operation）]（TCP オプション 1）に設定されたオプションの数。	はい
TCP タイムスタンプ ECR の正規化（TCP Timestamp ECR Normalizations）	[これらの TCP オプションを許可（Allow These TCP Options）] を有効にして、[任意（any）] 以外のオプションに設定します。	確認応答（ACK）制御ビットが設定されていないため、[タイム スタンプ エコー応答（TSecr）（Time Stamp Echo Reply (TSecr)）] オプション フィールドがクリアされたパケットの数。	はい
TCP 緊急ポインタの正規化（TCP Urgent Pointer Normalizations）	[緊急ポインタの正規化（Normalize Urgent Pointer）] を有効にします。	TCP ヘッダーの [緊急ポインタ（Urgent Pointer）] フィールド（2 バイト）がペイロード長を超えていたため、ペイロード長に合わせて設定されたパケットの数。	Yes

データの生成対象となるグラフ	実行する操作	説明	インラインモードによる影響
ブロックされたパケットの総数（Total Blocked Packets）	[インライン モード（Inline Mode）] または [インライン時にドロップ（Drop when Inline）] を設定します。	ルール、デコーダ、およびプリプロセッサのドロップを含めて、ドロップされたパケットの総数。	いいえ
インジェクションされたパケットの総数（Total Injected Packets）	[インライン モード（Inline Mode）] を設定します。	再送信前にサイズ変更されたパケットの数。	いいえ
TCP フィルタ適用パケットの総数（Total TCP Filtered Packets）	TCP ストリームの前処理を設定します。	TCP ポートフィルタリングのためにストリームによってスキップされたパケットの数。	いいえ
UDP フィルタ適用パケットの総数（Total UDP Filtered Packets）	UDP ストリームの前処理を設定します。	UDP ポートフィルタリングのためにストリームによってスキップされたパケットの数。	いいえ
緊急フラグ クリア済みの正規化（Urgent Flag Cleared Normalizations）	[緊急ポインタが設定されていない場合 URG をクリア（Clear URG if Urgent Pointer is Not Set）] を有効にします。	緊急ポインタが設定されていなかったため、TCP ヘッダーの URG 制御ビットがクリアされたパケットの数。	はい
緊急ポインタおよび緊急フラグ クリア済みの正規化（Urgent Pointer and Urgent Flag Cleared Normalizations）	[空のペイロードに設定された緊急ポインタまたは URG をクリア（Clear Urgent Pointer/URG on Empty Payload）] を有効にします。	ペイロードがなかったため、TCP ヘッダーの [緊急ポインタ（Urgent Pointer）] フィールドと URG 制御ビットがクリアされたパケットの数。	はい
緊急ポインタ クリア済みの正規化（Urgent Pointer Cleared Normalizations）	[URG=0 の場合に緊急ポインタをクリア（Clear Urgent Pointer if URG=0）] を有効にします。	緊急（URG）制御ビットが設定されていなかったため、TCP ヘッダーの [緊急ポインタ（Urgent Pointer）] フィールド（16 ビット）がクリアされたパケットの数。	はい

関連トピック

インライン正規化プリプロセッサ
インライン導入でのプリプロセッサによるトラフィックの変更
インライン展開でのドロップ動作

侵入イベント グラフの表示

システムは、経時的な侵入イベントの傾向を示すグラフを表示します。1 つまたはすべての管理対象デバイスについて、過去1時間から先月までの範囲の経時的な侵入イベント グラフを生成できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[概要（Overview）]** > **[概要（Summary）]** > **[侵入イベントグラフ（Intrusion Event Graphs）]** を選択します。

ステップ 2 [デバイスの選択（Select Device）] で、[すべて（all）] を選択してすべてのデバイスを含めるか、グラフに含める特定のデバイスを選択します。

ステップ 3 [グラフの選択（Select Graph(s)）] で、生成するグラフの種類を選択します。

- 上位 10 個の宛先ポート
- 上位 10 個の送信元 IP アドレス
- 上位 10 個のイベント メッセージ

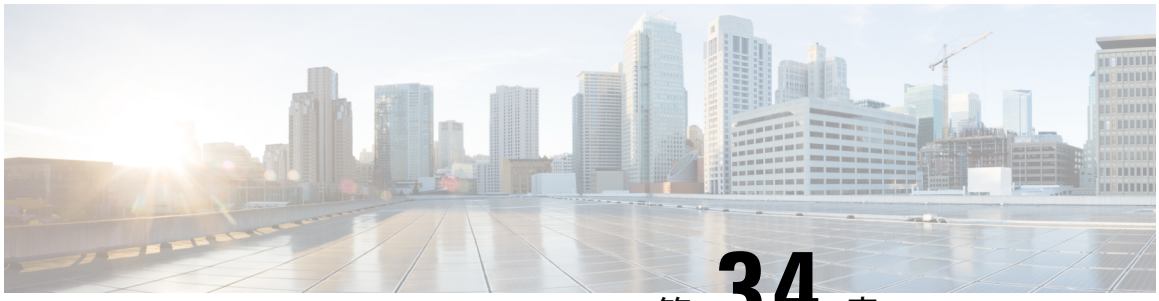
ステップ 4 [時間範囲の選択（Select Time Range）] で、グラフの時間範囲を選択します。

- 直近の 1 時間（Last Hour）
- 前日（Last Day）
- 先週（Last Week）
- 先月（Last Month）

ステップ 5 [グラフ（Graph）] をクリックします。

侵入イベントの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
IPS イベントデータストアの交換	7.1	任意（Any）	• 侵入インシデント、侵入イベントクリップボード、およびデフォルトのカスタムテーブル（侵入イベント列（[送信元重要度を持つ侵入イベント（Intrusion Events with Source Criticality）] および [宛先重要度を持つ侵入イベント（Intrusion Events with Destination Criticality）]）を使用するテーブルは廃止されています。 [コピー（Copy）] ボタンと [すべてコピー（Copy All）] ボタンを使用してクリップボードにイベントを追加できなくなりました。 廃止されたページ： • [分析（Analysis）] > [侵入（Intrusions）] > [クリップボード（Clipboard）] • [分析（Analysis）] > [侵入（Intrusions）] > [インシデント（Incidents）] • メインの侵入イベントテーブルに、[送信元ホストの重要度（Source Host Criticality）] と [宛先ホストの重要度（Destination Host Criticality）] という新しい 2 つのフィールドが追加されました。 サポートされているプラットフォーム： Secure Firewall Management Center
Syslog の接続イベントの固有識別子	6.4.0.4	任意（Any）	syslog の [DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを一意に識別できます。これらのフィールドは、侵入イベントの syslog に含まれます。
[IntrusionPolicy] フィールドが syslog に含まれるようになりました。	6.4	任意（Any）	侵入イベントの syslog が、イベントをトリガーした侵入ポリシーを指定するようになりました。
新しい侵入イベント検索フィールド：[CVE ID]	6.4	任意（Any）	MITRE の Common Vulnerabilities and Exposures 番号で検索できるようになりました。 変更された画面：[分析（Analysis）] > [侵入（Intrusions）] > [イベント（Events）] > [検索の編集（Edit Search）] サポート対象プラットフォーム：すべて



第 34 章

ファイル イベント/マルウェア イベントとネットワーク ファイル トラジェクトリ

次のトピックでは、ファイル/マルウェア イベント、ローカル マルウェア分析、動的分析、キャプチャされたファイル、およびネットワーク ファイル トラジェクトリの概要を示します。

ファイル イベント/マルウェア イベントとネットワーク ファイル トラジェクトリについて

ファイル ポリシーは、一致したトラフィックのファイル イベントおよびマルウェア イベントを自動的に生成し、キャプチャされたファイル情報をログに記録します。また、ファイル ポリシーでファイル イベントまたはマルウェア イベントが生成されるか、ファイルがキャプチャされると、システムは関連する接続の終了を Secure Firewall Management Center データベースに自動的に記録します。このデータを分析して、悪影響への対処および将来の攻撃のブロックをすることができます。

ファイル分析結果に基づいて、キャプチャされたファイル、生成されたマルウェアとファイル イベントを、[分析（Analysis）]>[ファイル（Files）] メニューで使用可能なページの表を使用して確認することができます。使用可能な場合は、ファイルの構成、性質、脅威スコア、動的分析のサマリー レポートを調べ、マルウェア分析をさらに詳細に把握できます。

分析のターゲットをさらに絞り込むために、マルウェア ファイルの [ネットワークファイルトラジェクトリ（network file trajectory）]（さまざまなファイル プロパティに加え、ファイルがどのようにネットワークを通過し、ホスト間で渡されてきたかを示すマップ）を使用して、ホスト間での個々の脅威の広がりを時系列で追跡できます。これにより、最も効果的なアウトブレイク制御と防止対策に集中できます。

ファイル ルールでローカル マルウェア分析または動的分析を設定すると、システムによってルールに一致するファイルが事前分類され、ファイル構成レポートが生成されます。

組織で *Cisco Secure Endpoint* が展開されていて、その展開が Secure Firewall Management Center と統合されている場合は、その製品により、スキャン、マルウェア検出、および検疫のレコードと侵害の兆候（IOC）をインポートすることもできます。このデータは、ネットワーク上のマルウェアの全体像をより完全に把握するために、Firepower によって収集されたイベントデータとともに表示されます。

コンテキスト エクスプローラ、およびレポート機能を使用すると、検出/キャプチャ/ブロックされたファイルとマルウェアについてより詳しく理解できます。また、イベントを使用して相関ポリシー違反をトリガーしたり、電子メール、SMTP、または syslog によるアラートを発行したりすることもできます。

（注） マルウェアを検出し、ファイルおよびマルウェアイベントを生成するようにシステムを設定するには、Cisco Secure Firewall Management Center デバイス構成ガイドの「*Network Malware Protection and File Policies*」を参照してください。

ファイルおよびマルウェア イベント

Secure Firewall Management Center は、さまざまなタイプのファイルおよびマルウェア イベントをログに記録できます。個々のイベントに関する情報は、イベントの生成方法と生成理由に応じて異なります。

- ファイルイベントとは、システム（マルウェア防御）によって検出されたマルウェアを含むファイルを意味します。ファイルイベントには、Cisco Secure Endpoint 関連のフィールドは含まれません。
- マルウェアイベントとは、マルウェア防御 または Cisco Secure Endpoint によって検出されたマルウェアを意味します。また、マルウェアイベントは、スキャンや検疫など、Cisco Secure Endpoint 展開からの脅威以外のデータも記録できます。
- レトロスペクティブ マルウェア イベントとは、性質（ファイルがマルウェアかどうか）が変更された、マルウェア防御 によって検出されたファイルを意味します。

（注）

- マルウェア防御 によってマルウェアとして識別されたファイルは、ファイル イベントとマルウェア イベントの両方を生成します。Cisco Secure Endpoint によって生成されたマルウェアイベントは、対応するファイルイベントを持っていません。
- NetBIOS-ssn（SMB）トラフィックのインスペクションによって生成されるファイル イベントは、即座には接続イベントを生成しません。これは、クライアントとサーバーが持続的接続を確立するためです。システムはクライアントまたはサーバーがセッションを終了した後に接続イベントを生成します。
- システムでは、Unicode（UTF-8）文字を使用するファイル名の表示および入力がサポートされます。ただし、Unicode のファイル名は PDF レポートに変換された形式で表示されます。また、SMB プロトコルによって、ファイル名の印刷不能な文字がピリオドに置き換えられます。

ファイル イベントおよびマルウェア イベントの種類

ファイル イベント

システムは、現在展開されているファイル ポリシーのルールに従って、管理対象デバイスがネットワーク トラフィック内のファイルを検出またはブロックしたときに生成されたファイル イベントを記録します。

システムがファイル イベントを生成する際に、呼び出しを行うアクセス コントロール ルールのログ設定に関係なく、システムは Secure Firewall Management Center データベースへの関連する接続の終わりも記録します。

マルウェア イベント（Malware Events）

システム（特に マルウェア防御 の機能）は、全体的なアクセスコントロール設定の一部としてネットワークトラフィック内のマルウェアを検出すると、マルウェアイベントを生成します。マルウェアイベントには、結果として生じたイベントの性質や、いつどこでどのようにしてマルウェアが検出されたかに関するコンテキスト データが含まれます。

表 *115*：でのマルウェア イベントの生成シナリオ

システムがファイルを検出し、次の状態になった場合	性質
AMP クラウドにファイルの性質についてクエリを行い（マルウェア クラウド ルックアップを実行）、クエリに成功した場合	マルウェア、クリーン、または不明

システムがファイルを検出し、次の状態になった場合	性質
AMP クライドにクエリを行ったものの、接続を確立できないか、他の理由でクライドが利用可能でない場合	応対不可 この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。
ファイルに関連付けられている脅威スコアが、ファイルを検出したファイルポリシーで定義されたマルウェアしきい値の脅威スコアを超えた場合、またはローカル マルウェア分析でマルウェアが識別された場合	マルウェア
ファイルがカスタム検出リストに設定されている場合（手動でマルウェアとしてマークされている場合）	カスタム検出
ファイルがクリーンリストに設定されている場合（手動でクリーンとしてマークされている場合）	正常（Clean）

ファイルの性質とマルウェアイベントにおけるファイルアクション

各ファイルルールには、ルールの条件に一致するトラフィックがシステムによってどのように処理されるかを決定する1つのアクションが関連付けられます。ファイルルールアクションとして [マルウェアブロック（Block Malware）] または [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] を選択すると、システムは、AMP クラウドに問い合わせて、ネットワークを通過するファイルにマルウェアが含まれているかどうかを判断し、脅威を示しているファイルをブロックします。クラウドルックアップを使用すると、SHA-256ハッシュ値に基づいてファイルの性質を取得してログに記録できます。

次の表では、AMP クラウドによって返されるファイルの性質に関連付けられたファイルアクションについて説明します。

表 *116 :* ファイルの性質とマルウェアイベントにおけるファイルアクション

選択されたファイルルールアクション	ファイルの性質	マルウェアイベントにおけるファイルアクション
• マルウェア ブロック（Block Malware） • マルウェア クラウド ルックアップ（Malware Cloud Lookup）	マルウェア	ブロック（Block）
	• クリーン • 不明 • 使用不可 • NA	クラウドルックアップ （注） ファイルポリシーエディタの [詳細設定（Advanced Settings）] で、[AMPクラウドの判定結果が不明な場合は、脅威スコアに基づいて判定結果をオーバーライドする（If AMP Cloud disposition is Unknown, override disposition based upon threat score）] オプションのしきい値脅威スコアを設定できます。脅威スコアのしきい値を設定すると、動的分析スコアがしきい値以下である場合、AMP クラウドの判定が [不明（Unknown）] のファイルはマルウェアと見なされます。

レトロスペクティブ マルウェア イベント

ネットワーク トラフィックで検出されたマルウェアの場合、性質が変わることがあります。たとえば、AMP クラウドによる判定の結果、以前はクリーンであると考えられていたファイルが今はマルウェアとして識別されるようになったり、その逆、つまりマルウェアと識別されたファイルが実際にはクリーンであったりする可能性があります。先週クエリしたファイルの性質が変わると、AMP クラウドがシステムに通知します。その場合、以下の 2 つが行われます。

- Secure Firewall Management Center が新しいレトロスペクティブ マルウェア イベントを生成します。

  この新しいレトロスペクティブ マルウェア イベントは、前の週に検出され、同じ SHA-256 ハッシュ値を持つ同じすべてのファイルの性質変更を表します。そのため、これらのイベントには限られた情報（Secure Firewall Management Center に性質変更が通知された日時、新しい性質、ファイルの SHA-256 ハッシュ値、および脅威名）が含まれます。IP アドレスや他のコンテキスト情報は含まれません。

- Secure Firewall Management Center はレトロスペクティブ イベントの関連する SHA-256 ハッシュ値を持つすでに検出済みのファイルのファイル性質を変更します。

  ファイルの性質が Malware に変更されると、Secure Firewall Management Center は新しいマルウェア イベントをデータベースに記録します。新しい性質を除き、この新しいマルウェア イベントの情報は、ファイルが最初に検出されたときに生成されたファイル イベントのものと同じです。

ファイルの性質が [クリーン（Clean）] に変更された場合、Secure Firewall Management Centerはそのマルウェア イベントを削除しません。代わりに、イベントに性質の変更が反映されます。つまり、マルウェア テーブルには性質が [クリーン（Clean）] のファイルが含められることがありますが、それはそのファイルが最初マルウェアと識別されていた場合だけです。マルウェアとして識別されたことのないファイルは、ファイルのテーブルにのみ含められます。

Cisco Secure Endpoint によって生成されたマルウェアイベント

所属部門が Cisco Secure Endpoint を使用している場合、個々のユーザーはエンドポイント（つまり、コンピュータやモバイルデバイス）に軽量コネクタをインストールします。コネクタでは、アップロード、ダウンロード、実行、オープン、コピー、移動などのときにファイルを検査できます。検査対象のファイルにマルウェアが含まれるかどうかを判断するために、これらのコネクタは AMP クラウドと通信します。

ファイルがマルウェアとして識別された場合、AMP クラウドは脅威の特定情報を Secure Firewall Management Center に送ります。さらに AMP クラウドは、スキャン、検疫、実行のブロッキング、クラウド リコールなど、他の種類のデータを Secure Firewall Management Center に送ることもできます。Secure Firewall Management Center はこれらの情報をマルウェア イベントとしてログに記録します。

（注） Cisco Secure Endpoint によって生成されたマルウェアイベントで報告される IP アドレスは、ネットワークマップに（および監視対象ネットワークにも）含まれない場合もあります。展開、コンプライアンスのレベル、およびその他の要因によっては、Cisco Secure Endpoint によってモニターされる組織内のエンドポイントが、マルウェア防御によってモニターされているものと同じホストではない可能性があります。

Secure Endpoint を使用したマルウェアイベント分析

Cisco Secure Endpoint を導入している組織は、次のことができます。

- Secure Endpoint によって検出されたマルウェアイベントを、マルウェア防御によって検出されたイベントとともに Management Center のイベントページに表示するようにシステムを設定できます。
- AMP パブリッククラウドを使用している場合は、Secure Endpoint の特定の SHA に関するファイルトラジェクトリやその他の情報を表示できます。

前述の機能を設定するには、Cisco Secure Firewall Management Center デバイス構成ガイドの「*Integrate Firepower and Secure Endpoint*」を参照してください。

Secure Endpoint からのイベントデータ

組織でマルウェア防御のために Secure Endpoint を展開している場合は、Secure Endpoint からのファイルおよびマルウェアデータを使用した作業を Management Center 上でできるようにシステムを設定できます。

ただし、Secure Endpointからのファイルおよびマルウェアデータとシステムのマルウェア防御機能からのファイルおよびマルウェアデータの相違点に注意する必要があります。

管理対象デバイスはネットワークトラフィックのマルウェアを検出しますが、Secure Endpointのマルウェア検出はダウンロード時または実行時にエンドポイントで行われるため、この2種類のマルウェアイベントの情報は異なります。たとえば、Secure Endpointによって検出されたマルウェアイベント（「エンドポイントベースのマルウェア」）には、ファイルパス、呼び出し元クライアントアプリケーションなどの情報が含まれるのに対して、ネットワークトラフィックでのマルウェア検出には、ファイル伝送に使われた接続のポート、アプリケーションプロトコル、発信元 IP アドレス情報が含まれます。

その他にも、マルウェア防御によって検出されたマルウェアイベント（「ネットワークベースのマルウェアイベント」）の場合、ユーザー情報は、ネットワーク検出で判別された、マルウェアの送信先であるホストに最後にログインしたユーザーを示すことが挙げられます。一方、Secure Endpoint で報告されるユーザーは、マルウェアが検出されたエンドポイントに現在ログインしているユーザーを示します。

（注） 展開に応じて、Secure Endpoint によってモニタされるエンドポイントは マルウェア防御 でモニタされるものと同じホストにならない場合があります。このため、Secure Endpoint によって生成されたマルウェアイベントはネットワークマップにホストを追加しません。ただし、システムは IP アドレスおよび MAC アドレスのデータを使用して、Secure Endpoint の展開から取得した侵害の兆候をモニタ対象のホストにタグ付けします。異なるマルウェアソリューションによってモニタされる 2 つの異なるホストが同じ IP アドレスと MAC アドレスを持っている場合、システムは Secure Endpoint の IOC をモニタ対象のホストに誤ってタグ付けする場合があります。

次の表に、マルウェア防御 ライセンスを使用する場合に Firepower によって生成されるイベントデータと、Secure Endpoint によって生成されるイベントデータの違いを要約します。

表 *117 : AMP* 製品間のデータの相違点の要約

機能	マルウェア防御	Secure Endpoint
生成されるイベント	ファイル イベント、キャプチャされたファイル、マルウェア イベント、およびレトロスペクティブ マルウェア イベント	マルウェア イベント
マルウェア イベントに含まれる情報	基本的なマルウェア イベント情報、および接続データ（IP アドレス、ポート、アプリケーション プロトコル）	詳細なマルウェア イベント情報（接続データなし）
ネットワーク ファイル トラジェクトリ	Management Center ベース	Management Center と Secure Endpoint の管理コンソールには、それぞれネットワーク ファイル トラジェクトリがあります。いずれも使用可能です。

関連項目

Cisco Secure Firewall Management Center デバイス構成ガイドの「*Integrate Firepower and Secure Endpoint*」

ファイルおよびマルウェア イベントのワークフローの使用

次の手順を使用して、テーブル内のファイルおよびマルウェアイベントを表示し、分析に関連する情報に基づいてイベント ビューを操作します。イベントにアクセスしたときに表示されるページは、ワークフローによって異なります。ワークフローは、大まかなビューから詳細なビューに移動してイベントを評価するために使用できる、一連のページです。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

このタスクを実行するには、管理者ユーザーまたはセキュリティ アナリスト ユーザーである必要があります。

手順

次のいずれかを実行します。

- **[分析（Analysis）] > [ファイル（Files）] > [ファイルイベント（File Events）]**
- **[分析（Analysis）] > [ファイル（Files）] > [マルウェアイベント（Malware Events）]**

ヒント イベントのテーブル ビューでは、一部のフィールドがデフォルトで非表示にされています。イベント ビューに非表示フィールドを表示するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のフィールド名をクリックします。

ヒント 特定のファイルが検出された接続をすぐに表示するには、テーブルでチェックボックスを使用してファイルを選択してから、[ジャンプ（Jump to）] ドロップダウン リストで [接続イベント（Connections Events）] を選択します。

ヒント オプションを表示するには、テーブル内の項目を右クリックします（オプションが表示されない列もあります）。

関連トピック

ファイルおよびマルウェア イベント フィールド （1011 ページ）
定義済みファイルのワークフロー （800 ページ）
定義済みマルウェアのワークフロー （799 ページ）
イベント ビューの設定 （241 ページ）

ファイルおよびマルウェア イベント フィールド

ワークフローを使用して表示および検索できるマルウェアイベントには、このセクションにリストするフィールドがあります。個別のイベントで利用可能な情報は、いつ、どのように生成されたかによって異なることに注意してください。

（注） マルウェア防御 によってマルウェアとして識別されたファイルは、ファイル イベントとマルウェア イベントの両方を生成します。Secure Endpointによって生成されたマルウェアイベントには、対応するファイルイベントはありません。また、ファイルイベントにはSecure Endpoint関連のフィールドはありません。

syslog メッセージにはメッセージに初期値が入力され、たとえば、レトロスペクティブな判定などで Management Center Web インターフェイスの同等なフィールドが更新されたとしても更新されません。

[アクション（Action）]（syslog：FileAction）

ファイルを検出したファイル ポリシー ルールに関連したアクション、および関連するファイル アクション オプション。

AMP クラウド（AMP Cloud）

AMP for Endpoints イベントが発信された AMP クラウドの名前。

アプリケーション ファイル名（Application File Name）

AMP for Endpoints 検出が行われたときに、マルウェア ファイルにアクセスしていたクライアントアプリケーション。これらのアプリケーションはネットワーク検出またはアプリケーション制御とは関係ありません。

アプリケーション ファイル SHA256（Application File SHA256）

検出が行われたときに、AMP for Endpoints で検出された、または隔離されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。

統合イベントビューアでは、このフィールドは**アプリケーションファイル SHA-256** として表示されます。

[アプリケーションプロトコル（Application Protocol）]（syslog：ApplicationProtocol）

管理対象デバイスがファイルを検出したトラフィックで使用されるアプリケーションプロトコル。

アプリケーション プロトコル カテゴリまたはタグ（Application Protocol Category or Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

アプリケーションのリスク（Application Risk）

接続で検出されたアプリケーション トラフィックに関連するリスク：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するリスクがあります。このフィールドでは、それらのうち最も高いものが表示されます。

[アーカイブの深さ（Archive Depth）]（syslog：ArchiveDepth）

アーカイブ ファイル内でファイルがネストされたレベル（存在する場合）。

[アーカイブ名（Archive Name）]（syslog：ArchiveFileName）

マルウェア ファイルが含まれていたアーカイブ ファイル（ある場合）の名前。

アーカイブ ファイルの内容を表示するには、[分析（Analysis）] >[ファイル（Files）]にある、アーカイブ ファイルの一覧が表示されるいずれかのテーブルに移動し、アーカイブ ファイルのテーブルの行を右クリックしてコンテキスト メニューを開いてから、[アーカイブの内容の表示（View Archive Contents）] をクリックします。

[SHA256のアーカイブ（Archive SHA256）]（syslog：ArchiveSHA256）

マルウェア ファイルを含むアーカイブ ファイル（ある場合）の SHA-256 ハッシュ値。

アーカイブ ファイルの内容を表示するには、[分析（Analysis）]>[ファイル（Files）]にある、アーカイブ ファイルの一覧が表示されるいずれかのテーブルに移動し、アーカイブ ファイルのテーブルの行を右クリックしてコンテキスト メニューを開いてから、[アーカイブの内容の表示（View Archive Contents）] をクリックします。

ArchiveFileStatus（syslog のみ）

調査中のアーカイブのステータス。次のいずれかの値になります。

- [保留中（Pending）]：アーカイブは調査中です
- [取得済み（Extracted）]：調査が問題なく正常に実行されました
- [失敗（Failed）]：システムのリソース不足のため調査に失敗しました。
- [深度の超過（Depth Exceeded）]：調査は正常に実行されましたが、アーカイブがネストされた調査の深度を超過しました
- [暗号化（Encrypted）]：部分的に正常に実行されましたが、アーカイブが暗号化されているか、暗号化されたアーカイブが含まれています
- [調査できませんでした（Not Inspectable）]：部分的に正常に実行されましたが、ファイルは形式が不正であるか破損しています

ビジネスとの関連性（Business Relevance）

接続で検出されたアプリケーション トラフィックに関連するビジネス関連性：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、

関連するビジネスとの関連性があります。このフィールドでは、それらのうち最も低いもの（関連が最も低い）が表示されます。

カテゴリ（Category）/ファイル タイプ カテゴリ（File Type Category）

ファイルタイプの一般的なカテゴリ（Office ドキュメント、アーカイブ、マルチメディア、実行可能ファイル、PDF ファイル、エンコード ファイル、グラフィック、システム ファイルなど）。

[クライアント（Client）]（syslog：Client）

1 つのホストで実行され、ファイルを送信するためにサーバーに依存するクライアント アプリケーション。

クライアント カテゴリまたはタグ（Client Category or Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

Connection Counter （Syslog のみ）

ある接続と別の同時接続を区別するカウンタ。このフィールドは、それ自体には意味がありません。

[DeviceUUID]、[最初のパケット時間（First Packet Time）]、[接続インスタンスID（Connection Instance ID）]、および [接続数カウンタ（Connection Counter）] フィールドの情報を総合すると、特定のファイルまたはマルウェアイベントに関連付けられた接続イベントを一意に識別できます。

Connection Instance ID （Syslog のみ）

接続イベントを処理した Snort インスタンス。このフィールドは、それ自体には意味がありません。

[DeviceUUID]、[最初のパケット時間（First Packet Time）]、[接続インスタンスID（Connection Instance ID）]、および [接続数カウンタ（Connection Counter）] フィールドの情報を総合すると、特定のファイルまたはマルウェアイベントに関連付けられた接続イベントを一意に識別できます。

カウント（Count）

複数の同じ行を作成する制約を適用した後の、各行の情報に一致するイベントの数。

検出名（Detection Name）

検出されたマルウェアの名前。

ディテクタ（Detector）

マルウェアを識別した AMP for Endpoints ディテクタ（ClamAV、Spero、SHA など）。

デバイス

ファイルイベントおよびFirepowerデバイスによって生成されたマルウェアイベントの場合は、ファイルを検出したデバイスの名前。

エンドポイント向け AMP によって生成されたマルウェア イベントと AMP クラウドによって生成されたレトロスペクティブ マルウェア イベントの場合は、Management Center の名前。

DeviceUUID （Syslog のみ）

イベントを生成した Firepower デバイスの一意の識別子。

[DeviceUUID]、[最初のパケット時間（First Packet Time）]、[接続インスタンスID（Connection Instance ID）]、および [接続数カウンタ（Connection Counter）] フィールドの情報を総合すると、特定のファイルまたはマルウェアイベントに関連付けられた接続イベントを一意に識別できます。

[後処理/ファイルの後処理（Disposition / File Disposition）]（syslog：SHA_Disposition）

ファイルの性質：

マルウェア

AMP クラウドでそのファイルがマルウェアとして分類された、ローカル マルウェア分析でマルウェアとして識別された、またはファイルポリシーで定義されたマルウェアしきい値をファイルの脅威スコアが超えたことを示します。

クリーン

AMP クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。クリーンのファイルがマルウェア テーブルに含められるのは、そのファイルがクリーンに変更された場合だけです。

Unknown

システムが AMP クラウドに問い合わせましたが、ファイルの性質が割り当てられていませんでした。言い換えると、AMPクラウドがファイルを正しく分類していませんでした。

Custom Detection

ユーザがカスタム検出リストにファイルを追加したことを示します。

Unavailable

システムがAMPクラウドに問い合わせできなかったことを示します。この性質に関するイベントが、わずかながら存在する可能性があります。これは予期された動作です。

[該当なし（N/A）]

[ファイル検出（Detect Files）] または [ファイル ブロック（Block Files）] ルールがファイルを処理し、Secure Firewall Management Center が AMP クラウドに問い合わせなかったことを示します。

ファイルの後処理は、システムが AMP クラウドにクエリを実行したファイルについてのみ表示されます。

syslog フィールドには最初の後処理のみが反映されます。レトロスペクティブな判定を反映するようには更新されません。

ドメイン

ファイルイベントおよびFirepowerデバイスによって生成されたマルウェアイベントの場合は、ファイルを検出したデバイスのドメイン。エンドポイント向け AMP によって生成されたマルウェアイベントおよびAMP クラウドによって生成される遡及的マルウェア イベントの場合、イベントを報告した AMP クラウド接続に関連付けられたドメイン。

このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

DstIP（syslog のみ）

接続に応答したホストの IP アドレス。これは、FileDirection フィールドの値によってファイルの送信者または受信者の IP アドレスとなる場合があります。

FileDirection が **`Upload`** の場合、これはファイル受信者の IP アドレスです。

FileDirection が **`Download`** の場合、これはファイル送信者の IP アドレスです。

SrcIP も参照してください。

イニシエータ/レスポンダ、送信元/接続先、および送信者/受信者フィールドに関する注意（922 ページ）も参照してください。

DstPort（syslog のみ）

DstIP で説明されている接続で使用されるポート。

[出力仮想ルータ（Egress Virtual Router）]

仮想ルーティングを使用するネットワークでは、トラフィックがネットワークから出るときに通過する仮想ルータの名前。

イベント サブタイプ（Event Subtype）

マルウェア検出につながった AMP for Endpoints アクション（[作成（Create）]、[実行（Execute）]、[移動（Move）]、[スキャン（Scan）] など）。

イベントタイプ

マルウェア イベントのサブタイプ。

[ファイル名（File Name）]（syslog：FileName）

ファイルの名前。

ファイル パス（File Path）

AMP for Endpoints によって検出されたマルウェア ファイルのファイル パス（ファイル名を含まない）。

[ファイルポリシー（File Policy）]（syslog：FilePolicy）

ファイルを検出したファイル ポリシー。

[ファイルストレージ/保存済み（File Storage / Stored）]（syslog：FileStorageStatus）

イベントに関連付けられたファイルのストレージ ステータス：

Stored

関連するファイルが現在保存されているすべてのイベントを返します。

Stored in connection

関連するファイルが現在保存されているかどうかに関係なく、関連するファイルをシステムがキャプチャおよび保存したすべてのイベントを返します。

Failed

関連するファイルをシステムが保存できなかったすべてのイベントを返します。

syslog フィールドには、初期のステータスのみが含まれています。これらのステータスは変更後のステータスを反映するようには更新されません。

ファイルのタイムスタンプ（File Timestamp）

AMP for Endpoints が検出したマルウェア ファイルが作成された日時。

FileDirection（syslog のみ）

接続中にファイルがダウンロードされたか、またはアップロードされたか。値は次のとおりです。

- Download：ファイルは DstIP から SrcIP に転送されました。
- Upload：ファイルは SrcIP から DstIP に転送されました。

FileSandboxStatus（syslog のみ）

ファイルが動的分析のために送信されたかとその場合のステータスを示します。

First Packet Time （Syslog のみ）

システムが最初のパケットを検出した時間。

[DeviceUUID]、[最初のパケット時間（First Packet Time）]、[接続インスタンスID（Connection Instance ID）]、および [接続数カウンタ（Connection Counter）] フィールドの情報を総合すると、特定のファイルまたはマルウェアイベントに関連付けられた接続イベントを一意に識別できます。

FirstPacketSecond（syslog のみ）

ファイルのダウンロード フローまたはアップロード フローが開始された時刻。

イベントが発生した時刻がメッセージ ヘッダーのタイムスタンプにキャプチャされます。

HTTP 応答コード（HTTP Response Code）

ファイルの転送時にクライアントの HTTP 要求に応じて送信される HTTP ステータス コード。

[入力仮想ルータ（Ingress Virtual Router）]

仮想ルーティングを使用するネットワークでは、トラフィックがネットワークに入るときに通過する仮想ルータの名前。

IOC

マルウェア イベントが、接続に関与したホストに対する侵入の痕跡（IOC）をトリガーしたかどうか。AMP for Endpoints データが IOC ルールをトリガーした場合、タイプ AMP IOC で、完全なマルウェア イベントが生成されます。

メッセージ（Message）

マルウェア イベントに関連付けられる追加情報。ファイルイベントおよび Firepower デバイスによって生成されたマルウェアイベントでは、このフィールドは、後処理が変更された、つまり関連付けられたレトロスペクティブイベントがあるファイルに対してのみ入力されます。

MITRE

クリックしてモーダルを起動できる技術の数。これは、その階層内にある MITRE の戦術と技術の全リストを示します。

Protocol（syslog のみ）

接続に使用されたプロトコル（TCP や UDP など）。

受信側の大陸（Receiving Continent）

ファイルを受信するホストの大陸。

受信側の国（Receiving Country）

ファイルを受信するホストの国。

受信側 IP（Receiving IP）

Management Center の Web インターフェイスでは、ファイルイベントおよび Firepower デバイスによって生成されたマルウェアイベントの場合、ファイルを受信するホストの IP アドレス。イニシエータ/レスポンダ、送信元/接続先、および送信者/受信者フィールドに関する注意（922 ページ）も参照してください。

エンドポイント向け AMP によって生成されたマルウェアのイベントの場合、コネクタがイベントを報告したエンドポイントの IP アドレス。

syslog の同等のイベント（Firepower デバイスで生成されたイベントのみ）については、**DstIP** および **SrcIP** を参照してください。

受信側のポート（Receiving Port）

Management Center の Web インターフェイスでは、ファイルが検出されたトラフィックによって使用される宛先ポート。

Syslog と同等なものについては、**DstIP** および **SrcIP** と **DstPort** および **SrcPort** を参照してください。

[セキュリティ コンテキスト（Security Context）]（syslog：Context）

トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。複数のコンテキストモードで実行している 1 台以上の ASA FirePOWER デバイスを管理する場合、システムはこのフィールドのみを表示します。

送信側の大陸（Sending Continent）

ファイルを送信するホストの大陸。

送信側の国（Sending Country）

ファイルを送信するホストの国。

送信側 IP（Sending IP）

Management Center の Web インターフェイスでは、ファイルを送信するホストの IP アドレス。イニシエータ/レスポンダ、送信元/接続先、および送信者/受信者フィールドに関する注意（922 ページ）も参照してください。

同等な syslog については、 **DstIP** と **SrcIP** を参照してください。

送信側のポート（Sending Port）

Management Center の Web インターフェイスでは、ファイルが検出されたトラフィックによって使用される送信元ポート。

同等な syslog については、**DstIP** および **SrcIP** と **DstPort** および **SrcPort** を参照してください。

[SHA256/ファイルSHA256/（SHA256/File SHA256）]（syslog：FileSHA256）

ファイルの SHA-256 ハッシュ値。

SHA256 値を得るには、ファイルが次のいずれかによって処理されている必要があります。

- [ファイルの保存（Store files）] が有効になっているファイル検出ファイル ルール。
- [ファイルの保存（Store files）] が有効になっているファイル ブロック ファイル ルール。

- マルウェア クラウド ルックアップ ファイル ルール
- マルウェア ブロック ファイル ルール
- AMP for Endpoints

また、この列には最後に検出されたファイルイベントおよびファイルの後処理を表し、ネットワーク ファイル トラジェクトリにリンクするネットワーク ファイル トラジェクトリ アイコンも表示されます。

[サイズ（KB）/ファイルサイズ（KB）（Size (KB) / File Size (KB)）]（syslog：FileSize）

Management Center の Web インターフェイスでは、ファイルのサイズ（KB 単位）。

In syslog messages: The size of the file, in bytes.

ファイルが完全に受信される前にシステムがファイルのタイプを特定した場合は、ファイルサイズが計算されない場合があります。この状況では、このフィールドは空白です。

SperoDisposition(Syslog のみ)

SPERO 署名がファイル分析で使用されたかどうかを示します。有効な値：

- ファイルで実行された Spero の検出
- ファイルで実行されなかった Spero の検出

SrcIP（syslog のみ）

接続を開始したホストの IP アドレス。これは、FileDirection フィールドの値によってファイルの送信者または受信者の IP アドレスとなる場合があります。

FileDirection が **`Upload`** の場合、これはファイル送信者の IP アドレスです。

FileDirection が **`Download`** の場合、これはファイル受信者の IP アドレスです。

DstIP も参照してください。

イニシエータ/レスポンダ、送信元/接続先、および送信者/受信者フィールドに関する注意（922 ページ）も参照してください。

SrcPort（syslog のみ）

SrcIP で説明されている接続で使用されるポート。

SSL Actual Action (Syslog: SSLActualAction)

システムが暗号化されたトラフィックに適用したアクション。

Block または Block with reset

ブロックされた暗号化接続を表します。

[復号（再署名）（Decrypt (Resign)）]

再署名サーバ証明書を使用して復号された発信接続を表します。

[復号（キーの交換）（Decrypt (Replace Key)）]

置き換えられた公開キーと自己署名サーバ証明書を使用して復号化された発信接続を表します。

[復号（既知のキー）（Decrypt (Known Key)）]

既知の秘密キーを使用して復号化された着信接続を表します。

[デフォルトアクション（Default Action）]

接続がデフォルト アクションによって処理されたことを示します。

[復号しない（Do not Decrypt）]

システムが復号化しなかった接続を表します。

フィールド値は、検索ワークフロー ページの [SSL ステータス（SSL Status）] フィールドに表示されます。

[SSL 証明書情報（SSL Certificate Information）]

トラフィックを暗号化するための公開キー証明書に保存される次の情報：

- サブジェクト/発行元共通名（Subject/Issuer Common Name）
- サブジェクト/発行元組織（Subject/Issuer Organization）
- サブジェクト/発行元組織単位（Subject/Issuer Organization Unit）
- 有効期間の開始/終了（Not Valid Before/After）
- シリアル番号（Serial Number）、証明書フィンガープリント（Certificate Fingerprint）
- 公開キー フィンガープリント（Public Key Fingerprint）

syslog の場合は、**SSLCertificate** を参照してください。

[SSL失敗の理由（SSL Failure Reason）]（syslog：SSLFlowStatus）

システムが暗号化されたトラフィックの復号化に失敗した理由。

- 不明
- 不一致（No Match）
- Success
- キャッシュされていないセッション（Uncached Session）
- 不明な暗号スイート（Unknown Cipher Suite）
- サポートされていない暗号スイート（Unsupported Cipher Suite）

- サポートされていない SSL バージョン（Unsupported SSL Version）
- 使用された SSL 圧縮（SSL Compression Used）
- パッシブ モードで復号化できないセッション（Session Undecryptable in Passive Mode）
- ハンドシェイク エラー（Handshake Error）
- 復号エラー（Decryption Error）
- 保留中のサーバー名カテゴリの検索（Pending Server Name Category Lookup）
- 保留中の共通名カテゴリの検索（Pending Common Name Category Lookup）
- 内部エラー（Internal Error）
- 使用不可能なネットワーク パラメータ（Network Parameters Unavailable）
- 無効なサーバー証明書の処理（Invalid Server Certificate Handle）
- 使用不可能なサーバー証明書フィンガープリント（Server Certificate Fingerprint Unavailable）
- サブジェクト DN をキャッシュできない（Cannot Cache Subject DN）
- 発行元 DN をキャッシュできない（Cannot Cache Issuer DN）
- 不明な SSL バージョン（Unknown SSL Version）
- 使用不可能な外部証明書リスト（External Certificate List Unavailable）
- 使用不可能な外部証明書フィンガープリント（External Certificate Fingerprint Unavailable）
- 無効な内部証明書リスト（Internal Certificate List Invalid）
- 使用不可能な内部証明書リスト（Internal Certificate List Unavailable）
- 使用不可能な内部証明書（Internal Certificate Unavailable）
- 使用不可能な内部証明書フィンガープリント（Internal Certificate Fingerprint Unavailable）
- 使用不可能なサーバー証明書の検証（Server Certificate Validation Unavailable）
- サーバー証明書の検証エラー（Server Certificate Validation Failure）
- 無効なアクション（Invalid Action）

フィールド値は、検索ワークフロー ページの [SSL ステータス（SSL Status）] フィールドに表示されます。

SSL ステータス（SSL Status）

暗号化された接続を記録した、[SSLの実際の動作（SSL Actual Action）]（復号ルール、デフォルトアクション、または復号できないトラフィックアクション）に関連したアクション。[ロック（Lock）] アイコン（）は、TLS/SSL 証明書の詳細にリンクしています。証明書を利用できない場合（たとえば、TLS/SSL ハンドシェイク エラーにより接続がブロックされる場合）、ロック アイコンはグレー表示になります。

システムが暗号化された接続の復号化に失敗した場合、実行された [SSL の実際のアクション（SSL Actual Action）]（復号化できないトラフィック アクション）と [SSL 障害の理由（SSL Failure Reason）] が表示されます。たとえば、不明な暗号スイートによって暗号化されたトラフィックをシステムが検出し、それ以上のインスペクションをせずにこれを許可した場合、このフィールドには [復号しない（不明な暗号スイート）（Do Not Decrypt (Unknown Cipher Suite)）] が表示されます。

このフィールドを検索する場合は、[SSL の実際の動作（SSL Actual Action）] と [SSL 失敗理由（SSL Failure Reason）] の 1 つ以上の値を入力し、システムが処理した、または復号に失敗した暗号化トラフィックを表示します。

[SSLサブジェクト/発行元国（SSL Subject/Issuer Country）]

暗号化証明書に関連付けられた件名または発行元国の 2 文字の ISO 3166-1 alpha-2 国番号。

SSLCertificate（syslog のみ）

TLS/SSL サーバーの証明書のフィンガープリント。

[脅威の名前（Threat Name）]（syslog：ThreatName）

検出されたマルウェアの名前。

[脅威スコア（Threat Score）]（syslog：ThreatScore）

このファイルに関連付けられている最新の脅威スコア。これは、動的分析中に観察された悪意がある可能性がある動作に基づいた 0 ～ 100 の値です。

脅威スコア アイコンは、[動的分析要約（Dynamic Analysis Summary）] レポートにリンクされています。

Time

イベントが生成された日時。このフィールドは検索できません。

syslog メッセージでは、 **FirstPacketSecond** を参照してください。

[タイプ/ファイルタイプ（Type/File Type）]（syslog：FileType）

ファイルのタイプ（HTML や MSEXE など）。

[URI/ファイルURI（URI/File URI）]（syslog：URI）

ファイル トランザクションに関連付けられている接続の URI。たとえば、ユーザーがファイルをダウンロードした URL など。

[ユーザー（User）]（syslog：User）

接続を開始した IP アドレスに関連付けられているユーザー名。この IP アドレスがネットワークの外部にある場合、関連付けられているユーザー名は通常不明です。

該当する場合、ユーザー名の前には <realm>\ が付いています。

ファイルイベントおよびFirepowerデバイスによって生成されたマルウェアイベントの場合、このフィールドには、IDポリシーまたは権限のあるログインによって決定されたユーザー名が表示されます。IDポリシーがない場合、認証は必要ありませんと表示されます。

エンドポイント向けAMPによって生成されたマルウェア イベントの場合、エンドポイント向けAMPがユーザー名を判別します。これらのユーザーをユーザー検出または制御に関連付けることはできません。それらは[ユーザー（Users）]テーブルに含まれず、それらのユーザーの詳細を表示することもできません。

Webアプリケーション (Syslog: WebApplication)

接続で検出されたHTTPトラフィックについて、内容を表すまたはURLを要求したアプリケーション。

Web アプリケーションのカテゴリまたはタグ（Web Application Category or Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

マルウェア イベントのサブタイプ

次の表に、マルウェアイベントのサブタイプ、マルウェア防御（「ネットワークベースのマルウェアイベント」）かCisco Secure Endpoint（「エンドポイントベースのマルウェアイベント」）のどちらでそのサブタイプを指定できるかどうかと、そのサブタイプを使用してネットワーク ファイル トラジェクトリが構築されるかどうかを一覧で示します。

表 *118 :* マルウェア イベントのタイプ

マルウェアイベントのサブタイプ/検索値	マルウェア防御	Secure Endpoint	ファイル トラジェクトリ
ネットワーク ファイル転送時に検出された脅威（Threat Detected in Network File Transfer）	はい	いいえ	はい
ネットワーク ファイル転送時に検出された脅威（遡及的）（Threat Detected in Network File Transfer (retrospective)）	はい	いいえ	はい
検出された脅威（Threat Detected）	いいえ	はい	はい
除外項目内で検出された脅威（Threat Detected in Exclusion）	いいえ	はい	はい
検疫された脅威（Threat Quarantined）	いいえ	はい	はい
AMP IOC（侵害の兆候）（AMP IOC (Indications of compromise)）	いいえ	はい	いいえ

マルウェアイベントのサブタイプ/検索値	マルウェア防御	Secure Endpoint	ファイル トラジェクトリ
ブロックされた実行（Blocked Execution）	いいえ	はい	いいえ
隔離のクラウドリコール（Cloud Recall Quarantine）	いいえ	はい	いいえ
隔離のクラウドリコールの試行に失敗（Cloud Recall Quarantine Attempt Failed）	いいえ	はい	いいえ
隔離のクラウドリコールの開始（Cloud Recall Quarantine Started）	いいえ	はい	いいえ
隔離からのクラウドリコールの復元（Cloud Recall Restore from Quarantine）	いいえ	はい	いいえ
隔離からのクラウドリコールの復元に失敗（Cloud Recall Restore from Quarantine Failed）	いいえ	はい	いいえ
隔離からのクラウドリコールの復元の開始（Cloud Recall Restore from Quarantine Started）	いいえ	はい	いいえ
隔離エラー（Quarantine Failure）	いいえ	はい	いいえ
隔離されたアイテムの復元（Quarantined Item Restored）	いいえ	はい	いいえ
隔離の復元に失敗（Quarantine Restore Failed）	いいえ	はい	いいえ
隔離の復元の開始（Quarantine Restore Started）	いいえ	はい	いいえ
スキャン完了、検出なし（Scan Completed, No Detections）	いいえ	はい	いいえ
スキャンが検出ありで完了（Scan Completed With Detections）	いいえ	はい	いいえ
スキャンに失敗（Scan Failed）	いいえ	はい	いいえ
スキャン開始（Scan Started）	いいえ	はい	いいえ

ファイルおよびマルウェア イベント フィールドで利用可能な情報

次の表に、システムが各ファイルおよびマルウェア イベント フィールドの情報を表示するかどうかを示します。

組織で Cisco Secure Endpoint が導入されていて、その製品を Firepower 展開と統合している場合は、次のようになります。

- Cisco Secure Endpoint の展開からインポートされたマルウェアイベントと侵害の兆候（IOC）には、コンテキスト接続情報は含まれていませんが、ダウンロード時または実行時に取得された情報（ファイルパス、呼び出し元クライアントアプリケーションなど）が含まれています。
- ファイル イベント テーブル ビューには、Cisco Secure Endpoint 関連のフィールドは表示されません。

表 *119*: ファイルおよびマルウェア イベント フィールドで利用可能な情報

フィールド	ファイルイベント	システムによって検出されたマルウェアイベント	システムによって検出されたレトロスペクティブイベント	**Cisco Secure Endpoint** によって生成されたマルウェアイベント
操作（Action）	はい	はい	はい	いいえ
AMP クラウド（AMP Cloud）	いいえ	いいえ	いいえ	はい
アプリケーション ファイル名（Application File Name）	いいえ	いいえ	いいえ	はい
アプリケーション ファイル SHA256（Application File SHA256）	いいえ	いいえ	いいえ	はい
アプリケーションプロトコル	はい	はい	いいえ	いいえ
アプリケーション プロトコル カテゴリまたはタグ（Application Protocol Category or Tag）	はい	はい	はい	いいえ
アプリケーションのリスク（Application Risk）	はい	はい	はい	いいえ
アーカイブ深度（Archive Depth）	はい	はい	いいえ	はい
アーカイブ名（Archive Name）	はい	はい	いいえ	はい
アーカイブ SHA256（Archive SHA256）	はい	はい	いいえ	はい

フィールド	ファイルイベント	システムによって検出されたマルウェアイベント	システムによって検出されたレトロスペクティブイベント	**Cisco Secure Endpoint** によって生成されたマルウェアイベント
ビジネスとの関連性（Business Relevance）	はい	はい	はい	いいえ
カテゴリ/ファイル タイプ カテゴリ（Category / File Type Category）	はい	はい	いいえ	はい
クライアント（Client）	はい	はい	はい	いいえ
クライアント カテゴリまたはタグ（Client Category or Tag）	はい	はい	はい	いいえ
カウント（Count）	はい	はい	はい	はい
検出名（Detection Name）	いいえ	はい	いいえ	いいえ
ディテクタ（Detector）	いいえ	いいえ	いいえ	はい
デバイス	はい	はい	はい	はい
性質/ファイル性質（Disposition / File Disposition）	はい	はい	はい	いいえ
ドメイン（Domain）	はい	はい	はい	はい
イベント サブタイプ（Event Subtype）	いいえ	いいえ	いいえ	はい
イベントタイプ	いいえ	はい	はい	はい
ファイル名（File Name）	はい	はい	いいえ	はい
ファイル パス（File Path）	いいえ	いいえ	いいえ	はい
ファイル ポリシー（File Policy）	はい	いいえ	いいえ	いいえ
ファイルのタイムスタンプ（File Timestamp）	いいえ	いいえ	いいえ	はい
HTTP 応答コード（HTTP Response Code）	はい	はい	いいえ	いいえ
IOC（侵害の兆候）（IOC (Indication of Compromise)）	いいえ	はい	はい	はい
メッセージ（Message）	はい	はい	いいえ	はい
受信側の大陸（Receiving Continent）	はい	はい	はい	いいえ

フィールド	ファイルイベント	システムによって検出されたマルウェアイベント	システムによって検出されたレトロスペクティブイベント	**Cisco Secure Endpoint** によって生成されたマルウェアイベント
受信側の国（Receiving Country）	はい	はい	いいえ	いいえ
受信側 IP（Receiving IP）	はい	はい	いいえ	はい
受信側のポート（Receiving Port）	はい	はい	いいえ	いいえ
セキュリティ コンテキスト（Security Context）	はい	はい	はい	はい
送信側の大陸（Sending Continent）	はい	はい	はい	いいえ
送信側の国（Sending Country）	はい	はい	いいえ	いいえ
送信側 IP（Sending IP）	はい	はい	いいえ	いいえ
送信側のポート（Sending Port）	はい	はい	いいえ	いいえ
SHA256/ファイル SHA256（SHA256 / File SHA256）	はい	はい	はい	はい
サイズ（KB）/ファイルサイズ（KB）（Size (KB) / File Size (KB)）	はい	はい	いいえ	はい
SSL の実際のアクション（SSL Actual Action）（検索のみ）	はい	はい	いいえ	いいえ
SSL 証明書情報（SSL Certificate Information）（検索のみ）	はい	はい	いいえ	いいえ
SSL 障害の理由（SSL Failure Reason）（検索のみ）	はい	はい	いいえ	いいえ
SSL ステータス（SSL Status）	はい	はい	いいえ	いいえ
SSL 件名/発行者の国（SSL Subject/Issuer Country）（検索のみ）	はい	はい	いいえ	いいえ
ファイル ストレージ/保存済み（File Storage / Stored）（検索のみ）	はい	はい	いいえ	いいえ
脅威名（Threat Name）	いいえ	はい	はい	はい
脅威スコア（Threat Score）	はい	はい	いいえ	いいえ
Time	はい	はい	はい	はい

フィールド	ファイルイベント	システムによって検出されたマルウェアイベント	システムによって検出されたレトロスペクティブイベント	**Cisco Secure Endpoint** によって生成されたマルウェアイベント
タイプ/ファイル タイプ（Type / File Type）	はい	はい	いいえ	はい
URI/ファイル URI（URI / File URI）	はい	はい	いいえ	いいえ
ユーザ（User）	はい	はい	いいえ	はい
Web アプリケーション	はい	はい	はい	いいえ
Web アプリケーション カテゴリまたはタグ（Web Application Category or Tag）	はい	はい	はい	いいえ

分析されたファイルに関する詳細の表示

ヒント　追加のオプションを表示するには、イベント ページのテーブルでファイル SHA を右クリックします。詳細については、Web ベースのリソースを使用したイベントの調査（763 ページ）を参照してください。

ファイル構成レポート

ローカルマルウェアの分析または動的分析を設定すると、ファイルの分析後にファイル構成レポートが生成されます。このレポートを使用して、ファイルをさらに分析し、ファイルにマルウェアが組み込まれているかどうかを判断することができます。

ファイル構成レポートでは、ファイルのプロパティ、ファイルに組み込まれているオブジェクト、および検出されたウイルスが示されます。また、ファイル構成レポートでは、そのファイルタイプに固有の追加情報が示される場合があります。保存されているファイルのプルーニング時に、関連ファイル構成レポートもプルーニングされます。

ファイル構成の情報を表示するには、ネットワーク ファイル トラジェクトリの使用（1041 ページ）を参照してください。

AMP プライベート クラウドでのファイルの詳細の表示

AMP プライベート クラウドを導入している場合は、プライベート クラウドで分析されたファイルに関する追加の詳細を表示できます。

詳細については、お使いのプライベート クラウドのマニュアルを参照してください。

手順

AMP プライベート クラウドのコンソールに直接サインインします。

脅威スコアと動的分析のサマリ レポート

脅威スコア

表 *120 :* 脅威スコア レーティング

脅威スコア	数値スコア	アイコン
Low	0 ～ 24	低
Medium	25 ～ 69	中規模
High	70 ～ 94	高（**High**）
Very High	95 ～ 100	非常に高い

Secure Firewall Management Center は、ファイルの性質と同じ期間だけ、ファイルの脅威スコアをキャッシュに入れます。これらのファイルが後で検出されると、Secure Malware Analytics Cloud または Secure Malware Analytics アプライアンスにもう一度クエリが実行される代わりに、キャッシュされた脅威スコアが表示されます。ファイルの脅威スコアが、定義済みのマルウェアしきい値の脅威スコアを超える場合は、そのファイルにマルウェアの性質を自動的に割り当てることができます。

動的分析のサマリ

動的分析のサマリが生成可能な場合、脅威スコアアイコンをクリックすると、サマリが表示されます。複数のレポートが存在する場合、このサマリは、脅威スコアと完全に一致する最新のレポートに基づいて生成されます。完全に一致する脅威スコアがない場合、最も高い脅威スコアに関するレポートが表示されます。複数のレポートがある場合は、脅威スコアを選択して、それぞれのレポートを表示することができます。

サマリには、脅威スコアを構成する各コンポーネントの脅威がリストされます。各コンポーネントの脅威を展開すると、そのコンポーネントの脅威に関連するプロセスだけでなく、AMP クラウドの調査結果もリストされます。

プロセスツリーには、Secure Malware Analytics Cloud がファイルの実行を試みたときに開始されたプロセスが示されています。これは、マルウェアを含むファイルが、想定外のプロセスやシステム リソースへアクセスしようとしているかどうか（たとえば、Word ドキュメントを実

行すると、Microsoft Word が開き、次に Internet Explorer が起動し、さらに Java Runtime Environment が実行されるなど）を識別するのに役立ちます。

リストされる各プロセスには、実際のプロセスを検査するのに使用できるプロセス ID が含まれます。プロセス ツリー内の子ノードは、親プロセスの結果として開始されたプロセスを表します。

動的分析のサマリから [完全なレポートを表示（View Full Report）] をクリックすることにより、AMP クラウドの完全な分析を詳述する完全版分析レポートを表示できます。レポートには、ファイルの一般情報、検出されたすべてのプロセスの詳細な説明、ファイル分析の概要、およびその他の関連情報が含まれます。

Cisco Secure Malware Analytics Cloud の動的分析結果の表示

Secure Malware Analytics では、分析されたファイルに関して、Management Center で使用できるレポートよりもさらに詳細なレポートが提供されます。組織に Secure Malware Analytics Cloud アカウントがある場合、Secure Malware Analytics ポータルに直接アクセスして、管理対象デバイスから分析のために送信されたファイルに関する追加の詳細を表示できます。

始める前に

- Management Center を Secure Malware Analytics Cloud アカウントに関連付けます。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Enabling Access to Dynamic Analysis Results in the Public Cloud*」を参照してください。
- ライセンス要件：マルウェア
- このタスクでは、グローバルドメインに属している必要があります。
- 次のいずれかのユーザーロールが必要です：管理者、アクセス管理者、ネットワーク管理者

手順

ステップ 1 Secure Malware Analytics のマニュアルに記載されているアドレスで、Secure Malware Analytics Cloud のポータルにアクセスします。

ステップ 2 このタスクへの前提条件で関連付けを作成するために使用したアカウントの資格情報を使用してログインします。

ステップ 3 組織によって送信されたファイルを表示するか、SHA を使用して特定のファイルを検索します。

不明な点がある場合は、Secure Malware Analytics のマニュアルを参照してください。

キャプチャされたファイル ワークフローの使用

管理対象デバイスは、ネットワーク トラフィックで検出されたファイルをキャプチャすると、イベントをログに記録します。

（注） デバイスがマルウェアを含むファイルをキャプチャすると、デバイスは、ファイルを検出した場合はファイル イベント、マルウェアを識別した場合はマルウェア イベントの 2 種類のイベントを生成します。

次の手順を使用して、テーブル内のキャプチャ ファイルの一覧を表示し、分析に関連する情報に基づいてイベント ビューを操作します。キャプチャ ファイルにアクセスしたときに表示されるページは、ワークフローによって異なります。ワークフローは、大まかなビューから詳細なビューに移動してイベントを評価するために使用できる、一連のページです。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

ファイル ポリシーの更新など設定を変更した後に、システムがファイルを再キャプチャする場合、そのファイルの既存の情報が更新されます。

たとえば、[マルウェア クラウド ルックアップ（Malware Cloud Lookup）] アクションを使用してファイルをキャプチャするようにファイル ポリシーを設定した場合、システムはそのファイルと一緒にファイル処理と脅威スコアを保存します。その後、ファイル ポリシーを更新し、新しい [ファイルの検出（Detect Files）] アクションのためにシステムが同じファイルを再キャプチャすると、システムはファイルの [最終変更時刻（Last Changed）] の値を更新します。ただし、別のマルウェア クラウド ルックアップを実行しなかったとしても、システムは既存の処理や脅威スコアを削除しません。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

始める前に

このタスクを実行するには、管理者ユーザーまたはセキュリティ アナリスト ユーザーである必要があります。

手順

[分析（Analysis）] > [ファイル（Files）] > [キャプチャ ファイル（Captured Files）] を選択します。

ヒント イベントのテーブル ビューでは、一部のフィールドがデフォルトで非表示にされています。イベント ビューに非表示フィールドを表示するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のフィールド名をクリックします。

関連トピック

キャプチャされたファイルのフィールド （1032 ページ）
定義済みキャプチャ ファイルのワークフロー （800 ページ）
イベント ビューの設定 （241 ページ）

キャプチャされたファイルのフィールド

キャプチャされたファイルのテーブル ビューは、定義済みファイル イベントのワークフローの最後のページであり、カスタム ワークフローに追加できます。このテーブル ビューには、ファイル テーブルの各フィールドの列が含まれます。

このテーブルを検索する場合、検索結果は、検索対象のイベントで使用可能なデータによって決まることに留意してください。使用可能なデータによって、検索の制約が適用されないことがあります。たとえば、ダイナミック分析のためにファイルが送信されていない場合は、関連する脅威スコアがない可能性があります。

表 *121* : キャプチャされたファイルのフィールド

フィールド	説明
アーカイブ検査ステータス（Archive Inspection Status）	アーカイブ ファイルのアーカイブ検査ステータスであり、次のいずれかになります。 • [保留中（Pending）] は、システムがアーカイブ ファイルとその内容をまだ検査していることを示します。ファイルが再びシステムを通過すると、完全な情報が使用可能になります。 • [抽出済み（Extracted）] は、アーカイブの内容を抽出し、検査できたことを示します。 • [失敗（Failed）] は、まれなケースですが、システムが抽出を処理できない場合に発生します。 • [深さ超過（Depth Exceeded）] は、許可されている最大深さを超えるネストされたアーカイブ ファイルがアーカイブに含まれていることを示します。 • [暗号化（Encrypted）] は、アーカイブ ファイルの内容が暗号化されていて、検査できなかったことを示します。 • [検査不可（Not Inspectable）] は、システムがアーカイブの内容を抽出して検査しなかったことを示しています。このステータスの主な理由としては、ポリシー ルール アクション、ポリシー設定、破損ファイルの 3 つがあります。 アーカイブ ファイルの内容を表示するには、表で該当の行を右クリックしてコンテキスト メニューを開いてから、[アーカイブの内容の表示（View Archive Contents）] を選択します。
カテゴリ	ファイル タイプの一般的なカテゴリ（Office ドキュメント、アーカイブ、マルチメディア、実行可能ファイル、PDF ファイル、エンコード ファイル、グラフィック、システム ファイルなど）。
検出名（Detection Name）	検出されたマルウェアの名前。

フィールド	説明
傾向（Disposition）	ファイルの マルウェア防御 での性質： • [マルウェア（Malware）]は、ファイルがローカルのマルウェア分析でマルウェアとして認識され、クラウドでマルウェアとして分類されていること、または、ファイルの脅威スコアが、ファイルポリシーで定義されたマルウェアしきい値を超えていることを示します。 • [クリーン（Clean）]は、ファイルがAMPクラウドでクリーンとして分類されていること、または、ファイルをユーザがクリーン リストに追加したことを示します。 • [不明（Unknown）] は、システムが AMP クラウドに問い合わせましたが、ファイルの傾向が割り当てられていないこと、つまり、ファイルが AMP クラウドで正しく分類されていないことを示します。 • [カスタム検出（Custom Detection）] は、ファイルをユーザがカスタム検出リストに追加したことを示します。 • [使用不可（Unavailable）]は、システムがAMPクラウドに問い合わせできなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。 • [N/A] は、[ファイルを検出する（Detect Files）] または [ファイルをブロックする（Block Files）] ルールによってファイルが処理され、Secure Firewall Management Center が AMP クラウドに問い合わせなかったことを示します。
ドメイン（Domain）	キャプチャされたファイルが検出されたドメイン。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

フィールド	説明
動的分析ステータス（Dynamic Analysis Status）	ファイルが動的分析のために送信されたかどうかを示すものであり、次の値のうちの 1 つ以上が表示されます。 • [分析完了（Analysis Complete）]：ファイルがダイナミック分析のために送信され、脅威スコアおよびダイナミック分析のサマリー レポートを受け取りました。 • [処理予定の容量（Capacity Handled）]：送信できなかったため、ファイルが保存されました。 • [処理予定の容量（ネットワークの問題）（Capacity Handled (Network Issue)）]：ネットワーク接続の問題が原因で送信できなかったため、ファイルが保存されました。 • [処理予定の容量（レート制限）（Capacity Handled (Rate Limit)）]：最大数に達したことが原因で送信できなかったため、ファイルが保存されました。 • [非アクティブなデバイス（Device Not Activated）]：デバイスがオンプレミスの Secure Malware Analytics アプライアンスでアクティブになっていないため、ファイルが送信されません。このステータスが表示された場合は、サポート担当に連絡してください。 • [失敗（分析タイムアウト）（Failure (Analysis Timeout)）]：ファイルが送信されましたが、まだ AMP から結果が返されていません。 • [失敗（ファイル実行不可）（Failure (Cannot Run File)）]：ファイルが送信されましたが、AMP クラウドがテスト環境でファイルを実行できませんでした。 • [失敗（ネットワークの問題）（Failure (Network Issue)）]：ネットワーク接続の問題のため、ファイルが送信されませんでした。 • [分析のための送信なし（Not Sent for Analysis）]：ファイルが送信されませんでした。 • [疑わしくないファイル（分析のための送信なし）（Not Suspicious (Not Sent For Analysis)）]：ファイルがマルウェアではないものとして事前に分類されています。 • [以前に分析済み（Previously Analyzed）]：ファイルにキャッシュされた脅威スコアがあり、以前に送信されたことを示します。 • [分析のために拒否（Rejected for Analysis）]：静的分析に基づいて、たとえば動的要素が含まれていないため、ファイルがリスクをもたらす可能性はほとんどありません。 • [分析のために送信（Sent for Analysis）]：ファイルがマルウェアとして事前に分類されており、ダイナミック分析のためにキューに入れられました。
ダイナミック分析ステータスの変更（Dynamic Analysis Status Changed）	前回、ファイルのダイナミック分析のステータスが変更された日時。
ファイル名	ファイルの SHA-256 ハッシュ値に関連付けられているものとして最後に検出されたファイル名。

フィールド	説明
前回の変更（Last Changed）	このファイルに関連する情報が最後に更新された時刻。
最終送信日時（Last Sent）	ファイルが動的分析のために AMP クラウドに最後に送信された時刻。
ローカル マルウェア分析ステータス（Local Malware Analysis Status）	ローカルマルウェア分析が実行されたかどうかを示すものであり、次のいずれかになります。 • [分析完了（Analysis Complete）]：ローカル マルウェア分析を使用してファイルが検査され、事前に分類されました。 • [分析失敗（Analysis Failed）]：ローカル マルウェア分析を使用してファイルを検査しようとし、失敗しました。 • [手動による要求の送信（Manual Request Submitted）]：ユーザがローカル マルウェア分析のためにファイルを送信しました。 • [分析なし（Not Analyzed）]：システムでローカルマルウェア分析を使用してファイルが検査されませんでした。
SHA256	ファイルの SHA-256 ハッシュ値と、最後に検出されたファイル イベントおよびファイルの性質を表すネットワーク ファイル トラジェクトリ アイコン。ネットワーク ファイル トラジェクトリを表示するには、トラジェクトリ アイコンをクリックします。
ストレージ ステータス（Storage Status）	ファイルが管理対象デバイスに保存されているかどうかを示し、次のいずれかになります。 • ファイル保存済み（File Stored） • 保存なし（性質分析の保留）（Not Stored (Disposition Was Pending)）
脅威スコア（Threat Score）	このファイルに関連付けられている最新の脅威スコア。 ダイナミック分析のサマリー レポートを表示するには、脅威スコア アイコンをクリックします。
タイプ	ファイルのタイプ（HTML や MSEXE など）。

保存されているファイルのダウンロード

デバイスによって保存されたファイルは、Secure Firewall Management Center がそのデバイスと通信可能であり、ファイルが削除されていない限り、長期間保存し分析するためにローカルホストにダウンロードし、手動でファイルを分析できます。関連ファイルイベント、マルウェアイベント、キャプチャ ファイル ビュー、またはファイルのトラジェクトリからファイルをダウンロードできます。

マルウェアによる被害を防ぐため、デフォルトでは、ファイルのダウンロードのたびに確認を行う必要があります。ただし、この確認は[ユーザ設定（User Preferences）]で無効にすることもできます。

性質が使用不可のファイルにはマルウェアが含まれている可能性があるため、ファイルをダウンロードすると、システムはまずそのファイルを.zipパッケージにアーカイブします。.zipファイル名には、ファイルの性質とファイルタイプ（存在する場合）さらにSHA-256ハッシュ値が含まれます。誤って解凍してしまわないように、.zipファイルをパスワードで保護できます。.zipファイルのデフォルトパスワードは、[ユーザ設定（User Preferences）]で編集または削除できます。

注意 有害な結果が発生することがあるため、マルウェアをダウンロード**しない**ように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先を保護するために必要な予防措置を行っていることを確認します。

分析用ファイルの手動での送信

分析用ファイルを手動で送信すると、システムはローカル分析を実行してから、それらのファイルをダイナミック分析対象としてクラウドに送信します。ただし、ローカル分析がファイルポリシーで有効になっておらず、分析用のファイルを手動で送信する場合は、ファイルが動的分析用としてしか送信されません。

実行可能ファイルの他に、自動送信に適格ではないファイル タイプ（.swf、.jar など）も送信できます。これにより、ファイルの性質に関わらず、さまざまなファイルをより迅速に分析し、問題の正確な原因を突き止めることができます。

（注） 動的分析に適格なファイル タイプのリストと送信可能な最小および最大のファイル サイズに関して更新がないか、システムはAMP クラウドを検査します（この検査は、一日に1回だけ行われます）。

分析用ファイルを送信する方法は、状況により、次の2種類があります。

始める前に

分析用にキャプチャしたファイルを手動で送信するには、ファイルを保存するように1つまたは複数のファイル ルールを設定する必要があります。詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの「*Network Malware Protection and File Policies*」の章を参照してください。

手順

ステップ 1 1 つの分析用ファイルを送信する場合：

a) 次のいずれかを選択します。

- **[分析（Analysis）] > [ファイル（Files）] > [ファイルイベント（File Events）]**
- **[分析（Analysis）] > [ファイル（Files）] > [マルウェアイベント（Malware Events）]**
- **[分析（Analysis）] > [ファイル（Files）] > [キャプチャファイル（Captured Files）]**

b) [イベントタイプまたはファイル（Event type or files）] の [テーブルビュー（Table View）] をクリックします。

c) テーブル内のファイルを右クリックし、[ファイルの分析（Analyze file）] を選択します。

ステップ 2 複数のキャプチャした分析用ファイル（一度に最大 25 ファイル）を送信する場合：

a) [分析（Analysis）] > [ファイル（Files）] > [キャプチャファイル（Captured Files）] を選択します。

b) 分析する各ファイルの横にあるチェック ボックスをオンにします。

c) [Analyze（分析）] をクリックします。

ネットワーク ファイル トラジェクトリ

ネットワーク ファイルのトラジェクトリ機能は、ネットワーク全体でホストがどのようにファイル（マルウェア ファイルを含む）を転送したかをマッピングします。トラジェクトリは、ファイル転送データ、ファイルの性質、ファイル転送がブロックされたかどうか、ファイルが隔離されたかどうかをグラフに示します。これにより、マルウェアを転送したおそれのあるホストおよびユーザやリスクがあるホストがどれであるかを判定したり、ファイル転送の傾向を観測したりできます。

AMP クラウドで性質が割り当てられているファイルであれば、どのファイルの送信でも追跡できます。システムは、マルウェア防御 と Cisco Secure Endpoint の両方によるマルウェアの検出およびブロック情報を使用して、トラジェクトリを作成します。

最近検出されたマルウェアおよび分析済みトラジェクトリ

[ネットワーク ファイル トラジェクトリ リスト（Network File Trajectory List）] ページには、ネットワークで最近検出されたマルウェアと最後に表示したトラジェクトリ マップのファイルが表示されます。これらのリストから、ネットワークで各ファイルが最後に発見されたのはいつか、ファイルのSHA-256のハッシュ値、名前、タイプ、現在のファイルの性質、内容（アーカイブ ファイルの場合）、ファイルに関連付けられたイベント数を確認できます。

また、このページに含まれる検索ボックスを使用して、SHA-256ハッシュ値またはファイル名を基準に、あるいはファイルを送信または受信するホストの IP アドレスによってファイルを

見つけることができます。ファイルを見つけた後、[ファイル SHA256（File SHA256）] 値をクリックすると詳細なトラジェクトリ マップが表示されます。

ネットワーク ファイル トラジェクトリの詳細ビュー

詳細なネットワーク ファイル トラジェクトリを表示して、ネットワーク全体でファイルを追跡できます。ファイルの SHA 256 値を検索するか、[ネットワーク ファイル トラジェクトリ（Network File Trajectory）] リスト内の [ファイルの SHA 256（File SHA 256）] リンクをクリックして、そのファイルに関する詳細を表示します。

ネットワーク ファイル トラジェクトリの詳細ページには、3 つの部分があります。

- サマリー情報：ファイルのトラジェクトリ ページには、ファイルに関するサマリー情報（ファイル識別情報、ネットワーク上でファイルが最初に表示された時間および最後に表示された時間と表示したユーザ、ファイルに関連したイベントおよびホストの数、ファイルの現在の性質など）が表示されます。このセクションから、管理対象デバイスがファイルを保存した場合に、そのファイルをローカルにダウンロードしたり、ファイルを動的分析用に送信したり、ファイルをファイル リストに追加したりできます。
- トラジェクトリー マップ：ファイルのトラジェクトリ マップは、ネットワークで最初に検出された時点から直近までファイルを視覚的に追跡します。このマップは、ホストがファイルを転送または受信した時点、ファイルを転送した頻度、ファイルがブロックまたは隔離された時点を示します。データ ポイント間の縦線は、ホスト間のファイル転送を表します。データ ポイントをつなぐ横棒は、時間の経過に応じたホストのファイルアクティビティを示します。

  また、そのファイルでファイルイベントが発生した頻度や、システムがファイルに性質または遡及的性質を割り当てた時点についても示します。マップでデータ ポイントを選択し、ホストがそのファイルを転送した最初のインスタンスに遡るパスを強調表示できます。また、このパスは、ファイルの送信側または受信側としてホストが関与する各オカレンスと交差します。このパスにより、関与するユーザが識別されます。
- 関連イベント：[イベント（Events）] テーブルに、マップ内の各データ ポイントに関するイベント情報がリストされます。テーブルおよびマップを使用して、特定のファイルイベント、このファイルを転送または受信したネットワーク上のホストとユーザー、マップ内の関連するイベント、選択した値で制限されたテーブル内の他の関連するイベントを特定することができます。

ネットワーク ファイル トラジェクトリのサマリー情報

次の概要情報は、ネットワーク ファイル トラジェクトリのリストに表示されるファイルの詳細ページの上部に表示されます。

ヒント　関連するファイルイベントを表示するには、フィールド値のリンクをクリックします。ファイルイベントのデフォルトのワークフローの最初のページが新しいウィンドウで開き、選択した値を含むすべてのファイル イベントも表示されます。

表 *122*：ネットワーク ファイル トラジェクトリのサマリー情報フィールド

名前	説明
コンテンツのアーカイブ（Archive Contents）	検査されたアーカイブ ファイルで、アーカイブに含まれているファイルの数。
現在の性質（Current Disposition）	次のいずれかの マルウェア防御 ファイルの性質です。 • マルウェア（Malware）：ファイルが AMP クラウドでマルウェアと分類されていること、ローカル マルウェア分析でマルウェアとして識別されたこと、またはファイルの脅威スコアがファイルポリシーに定義されたマルウェアのしきい値を超えたこと示します。 • [クリーン（Clean）]：AMP クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。 • 不明（Unknown）：システムはAMPクラウドでファイルの性質をクエリしましたが、ファイルには性質が割り当てられていませんでした。言い換えると、AMP クラウドがファイルを分類できませんでした。 • カスタム検出（Custom Detection）：ユーザがカスタム検出リストにファイルを追加したことを示します。 • 利用不可（Unavailable）：システムが AMP クラウドでクエリを行えなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。 • [該当なし（N/A）]：[ファイル検出（Detect Files）] または [ファイル ブロック（Block Files）] ルールがファイルを処理し、Secure Firewall Management Center が AMP クラウドに問い合わせなかったことを示します。
検出名（Detection Name）	ローカル マルウェア分析によって検出されたマルウェアの名前。
イベント カウント（Event Count）	ファイルに関連付けられたネットワークで発見されたイベントの数、検出されたイベントの数が 250 を超える場合は、マップに表示されるイベントの数。
ファイル カテゴリ（File Category）	ファイル タイプの一般的なカテゴリ（Office Documents や System Files など）。
ファイル名（File Names）	ネットワーク上で発見された、イベントに関連したファイルの名前。 複数のファイル名がSHA-256ハッシュ値に関連付けられている場合、最後に検出されたファイル名がリストされます。[詳細（more）] をクリックすると、これが展開されて、残りのファイル名が表示されます。

名前	説明
[ファイルSHA256（File SHA256）]	ファイルの SHA-256 ハッシュ値。 デフォルトで、ハッシュは簡略化された形式で表示されます。完全なハッシュ値を表示するには、その上にポインタを移動させます。複数の SHA-256 ハッシュ値がファイル名に関連付けられている場合、リンクの上にポインタを移動されると、すべてのハッシュ値が表示されます。
[ファイル サイズ（File Size）（KB）]	ファイルのサイズ（KB 単位）。
ファイル タイプ（File Type）	ファイルのタイプ（`HTML` や `MSEXE` など）。
最初の確認日時（First Seen）	マルウェア防御 または Cisco Secure Endpoint による初めてのファイル検出に加えて、ファイルを初めてアップロードしたホストの IP アドレス、および関与するユーザーの識別情報。
Last Seen	マルウェア防御 または Cisco Secure Endpoint による最新のファイル検出に加えて、ファイルを最後にダウンロードしたホストの IP アドレス、および関与するユーザーの識別情報。
親アプリケーション（Parent Application）	Cisco Secure Endpoint による検出が行われたときに、マルウェアファイルにアクセスしていたクライアント アプリケーション。これらのアプリケーションはネットワーク検出またはアプリケーション制御とは関係**ありません**。
表示日（Seen On）	ファイルを送信または受信したホストの数。1 つのホストが 1 つのファイルのアップロードおよびダウンロードを時を異にして行う場合があるため、ホストの合計数が、[送受信ホスト数の内訳（Seen On Breakdown）] フィールドの送信側の総数と受信側の総数の合計と一致しないことがあります。
分析（Seen On Breakdown）	ファイルを送信したホストの数とファイルを受信したホストの数。
脅威名（Threat Name）	エンドポイント向け AMP によって検出されたマルウェアに関連付けられている脅威の名前。
脅威スコア（Threat Score）	ファイルの脅威スコア。

ネットワーク ファイル トラジェクトリ マップと関連イベント リスト

ファイル トラジェクトリ マップの Y 軸には、ファイルと対話したすべてのホストの IP アドレスがリストされます。IP アドレスは、システムがそのホストでファイルを最初に検出した時点に基づいて降順でリストされます。各行には、その IP アドレスに関連付けられたすべてのイベント（単一のファイル イベント、ファイル転送、レトロスペクティブ イベント）が含まれます。X 軸には、システムが各イベントを検出した日時が含まれます。タイムスタンプは時間順にリストされます。複数のイベントが 1 分以内に発生する場合、すべてが同じ列内にリストされます。マップを左右および上下にスクロールして、イベントおよび IP アドレスをさらに表示できます。

マップには、ファイルの SHA-256 ハッシュに関連した最大 250 のイベントが表示されます。イベントが 250 を超える場合、マップには最初の 10 個が表示され、余分のイベントは省略されて**矢印** が示されます。その後ろに、マップは残りの 240 個のイベントを表示します。

デフォルトの [File Events（ファイル イベント）] ワークフローの最初のページが新しいウィンドウで開き、ファイル タイプに基づいて制限されて、すべての余分のイベントが表示されます。Cisco Secure Endpoint によって生成されたマルウェアイベントが表示されない場合、[マルウェアイベント（Malware Events）] テーブルに切り替えてそれらを表示する必要があります。

各データ ポイントは、イベントの他にファイル性質を表しています。マップの下の凡例を参照してください。たとえば、[マルウェア ブロック（Malware Block）] イベント アイコンは、[悪意のある性質（Malicious Disposition）] アイコンと [ブロック イベント（Block Event）] アイコンを結合したものです。

Cisco Secure Endpoint によって生成されたマルウェアイベント（「エンドポイントベースのマルウェアイベント」）には 1 つのアイコンが含まれています。レトロスペクティブ イベントでは、ファイルで検出された各ホストのコラムにアイコンが表示されます。ファイル転送イベントでは、縦線でつながれた 2 つのアイコン（ファイル送信アイコンとファイル受信アイコン）が常に含まれます。矢印は、送信側から受信側へのファイル転送方向を示します。

ネットワークを介したファイルの進行状況を追跡するために、データ ポイントをクリックして、選択したデータ ポイントに関連するすべてのデータ ポイントを含むパスを強調表示できます。これには、次のタイプのイベントに関連付けられたデータ ポイントが含まれます。

- 関連付けられている IP アドレスが送信側または受信側だったファイル転送
- 関連付られた IP アドレスを含めて、Cisco Secure Endpoint によって生成されたマルウェアイベント（「エンドポイントベースのマルウェアイベント」）
- 別の IP アドレスが関係する場合、その関連する IP アドレスが送信側または受信側であったすべてのファイル転送
- 別の IP アドレスが関係していた場合、その他方の IP アドレスが関係する Cisco Secure Endpoint によって生成されたマルウェアイベント（「エンドポイントベースのマルウェアイベント」）

強調表示されたデータ ポイントに関連付けられたすべての IP アドレスとタイムスタンプも強調表示されます。[イベント（Events）] テーブルの対応するイベントも強調表示されます。省略されたイベントがパスに含まれている場合、そのパス自体が点線で強調表示されます。省略されたイベントがパスを交差している場合がありますが、マップに表示されません。

ネットワーク ファイル トラジェクトリの使用

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ヒント　組織で Secure Endpoint を展開している場合、その製品にはネットワーク ファイル トラジェクトリ機能もあります。Management Center から Secure Endpoint にピボットするには、Secure Endpoint コンソールでのイベントデータの使用 （1044 ページ）を参照してください。Secure Endpoint のファイルトラジェクトリ機能の詳細については、Secure Endpoint のマニュアルを参照してください。

始める前に

マルウェア防御 を使用している場合は、マルウェア防御 ライセンスが必要です。

このタスクを実行するには、管理者ユーザーまたはセキュリティ アナリスト ユーザーである必要があります。

手順

ステップ 1　**[分析（Analysis）] > [ファイル（Files）] > [ネットワークファイルトラジェクトリ（Network File Trajectory）]**を選択します。

ヒント　また、ファイル情報を使用して、コンテキストエクスプローラ、ダッシュボード、またはイベント ビューからファイルのトラジェクトリにアクセスできます。

ステップ 2　リストの [ファイル SHA 256（File SHA 256）] リンクをクリックします。

ステップ 3　オプションで、追跡するファイルの完全な SHA-256 ハッシュ値、ホスト IP アドレス、またはファイル名を検索フィールドに入力して、Enter を押します。

ヒント　1 つの結果だけが一致する場合、そのファイルの [ネットワーク ファイル トラジェクトリ（Network File Trajectory）] ページが表示されます。

ステップ 4　[サマリー情報（Summary Information）] セクションでは、以下を実行できます。

- ファイルリストにファイルを追加する：クリーンリストまたはカスタム検出リストにファイルを追加したり、ファイルを削除したりするには、**[編集（Edit）]**（✎）をクリックします。
- ファイルをダウンロードする：ファイルをダウンロードするには、[ダウンロード（Download）]（⬇ アイコン）をクリックし、プロンプトが表示されたら、ファイルをダウンロードすることを確認します。ファイルをダウンロードできない場合、このダウンロードファイルは淡色表示されます。
- レポートする：脅威スコアをクリックすると、動的分析サマリーレポートが表示されます。
- 動的分析のために送信する：**AMP クラウド** をクリックすると、動的分析のためにファイルを送信できます。ファイルを送信できない場合、または AMP クラウドに接続できない場合は、この AMP クラウドは淡色表示されます。

- アーカイブの内容を表示する：アーカイブファイルの内容に関する情報を表示するには、[表示（View）]（）をクリックします。
- ファイル構成を表示する：ファイルの構成を表示するには、**ファイルリスト**をクリックします。システムがファイル構成レポートを生成していなければ、このファイルリストは淡色表示されます。
- 同じ脅威スコアでキャプチャされたファイルを表示する：脅威スコア リンクをクリックすると、その脅威スコアでキャプチャされたすべてのファイルが表示されます。

（注） 有害な結果が発生することがあるため、マルウェアをダウンロード**しない**ように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先を保護するために必要な予防措置を行っていることを確認します。

ステップ 5 トラジェクトリ マップでは、以下を実行できます。

- 最初のインスタンスを見つける：IP アドレスをクリックして、IP アドレスが含まれる、最初に発生したファイル イベントを見つけます。これにより、そのデータ ポイントへのパスが強調表示され、その最初のファイル イベントに関連した仲介ファイル イベントと IP アドレスがあればそれも強調表示されます。[イベント（Events）] テーブルの対応するイベントも強調表示されます。そのデータ ポイントが現在表示されていない場合、表示されるまでマップがスクロールされます。
- 追跡する：データ ポイントをクリックすると、選択したデータ ポイントに関連するすべてのデータ ポイントが含まれるパスが強調表示されます。これにより、ネットワークを介してファイルの進捗を追跡できます。
- 非表示のイベントを表示する：矢印をクリックすると、[ファイルサマリー（File Summary）] イベントビューに表示されていないすべてのイベントが表示されます。
- ファイルの一致イベントを表示する：**ファイルの一致イベント**の上にポインタを合わせると、イベントのサマリー情報が表示されます。いずれかのイベント サマリー情報リンクをクリックすると、デフォルトの [ファイル イベント（File Events）] ワークフローの最初のページが新しいウィンドウで開き、そのファイル タイプのすべての余分のイベントが表示されます。[ファイル サマリー（File Summary）] イベント ビューが新しいウィンドウで表示され、クリックした条件値に一致するすべてのファイル イベントが表示されます。

ステップ 6 [イベント（Events）] テーブルでは、以下を実行できます。

- 強調表示：テーブル行を選択すると、マップ上のデータ ポイントが強調表示されます。選択したファイルイベントが現在表示されていない場合、表示されるまでマップがスクロールされます。
- ソート：カラム見出しをクリックすると、昇順または降順で情報をソートできます。

Secure Endpoint コンソールでのイベントデータの使用

組織で Secure Endpoint を導入している場合は、Secure Endpoint コンソールで のマルウェアイベントデータを表示して、当該アプリケーションのグローバルネットワーク ファイル トラジェクトリ ツールを使用することができます。

ヒント　Secure Endpoint とそのコンソールの使用については、コンソールのオンラインヘルプや、https://www.cisco.com/c/en/us/support/security/fireamp-endpoints/tsd-products-support-series-home.html で入手可能なその他のドキュメンテーションを参照してください。

Secure Firewall Management Center から Secure Endpoint コンソールにアクセスするには、次のいずれかを実行します。

始める前に

- Secure Endpoint への接続が設定され（『Cisco Secure Firewall Management Center デバイス構成ガイド』の「*Integrate Firepower and Secure Endpoint*」を参照してください）、Secure Firewall Management Center が AMP クラウドに接続可能になっている必要があります。
- Secure Endpoint の資格情報が必要です。
- このタスクを実行するには、管理者ユーザーである必要があります。
- Management Center のマルウェアイベントからピボットする場合は、Secure Endpoint のコンテキストクロス起動オプションが適切に有効になっていることを確認します。Web ベースのリソースを使用したイベントの調査（763 ページ）の各トピックを参照してください。

手順

ステップ 1　方法 1：

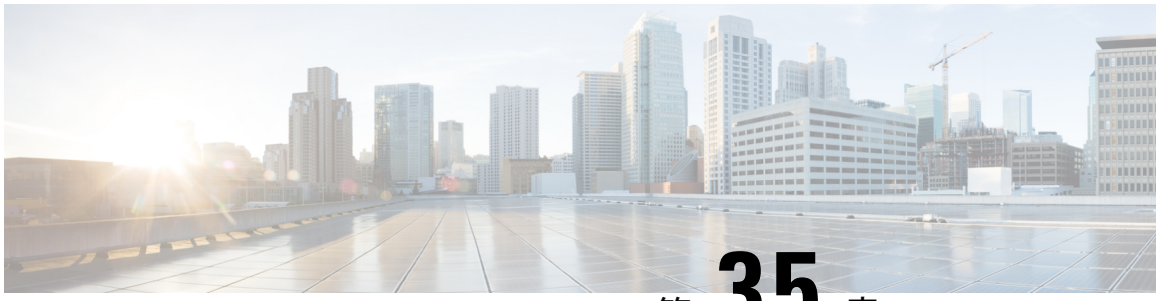
a) **[統合（Integration）] > [AMP] > [AMP管理（AMP Management）]**を選択します。
b) テーブルでクラウド名をクリックします。

ステップ 2　方法 2：

a) [Analysis（分析）]>[ファイル（Files）] にあるテーブルで、マルウェア イベントに移動します。
b) ファイル SHA を右クリックし、Secure Endpoint オプションを選択します。

ファイルおよびマルウェアイベントとネットワーク ファイル トラジェクトリの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
ファイルおよびマルウェアイベントに含まれる MITRE 情報。	7.4	7.4	ファイルおよびマルウェアイベントにMITRE情報（ローカルマルウェア分析結果）が含まれるようになりました。MITRE情報は、クラシックイベントビューと統合イベントビューの両方で表示できます。MITRE列は、両方のイベントビューでデフォルトで非表示になっていることに注意してください。
動的分析のためのファイルの事前分類の改善。	6.7	任意（Any）	追加の評価により、動的分析のためにファイルを不必要に送信することが回避されます。この評価に基づいてクラウドに送信されなかったファイルの新しい動的分析ステータスは、[分析のために拒否（Rejected for Analysis）] です。 新規/変更された画面：**[分析（Analysis）] > [キャプチャされたファイル（Captured Files）] > [キャプチャされたファイルのテーブルビュー（Table View of Captured Files）]**
Syslog の接続イベントの固有識別子。	6.4.0.4	任意（Any）	syslog の [DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および[Connection Counter] フィールドの情報を総合すると、接続イベントを一意に識別できます。これらのフィールドは、ファイルおよびマルウェアイベントの syslog に含まれます。
Syslog を介してファイルイベントおよびマルウェアイベントを送信します。	6.4	任意（Any）	この章のフィールドの説明は、syslog メッセージに含まれるフィールドを指しています。 設定情報については、ファイルとマルウェアイベントの syslog の設定場所 （779 ページ）を参照してください。



第 35 章

ホスト プロファイル

ここでは、ホスト プロファイルの使用方法について説明します。

ホストプロファイルの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者

- セキュリティ アナリスト（Security Analyst）

ホスト プロファイル

ホストプロファイルは、システムが1つのホストについて収集したすべての情報の完全なビューを提供します。ホスト プロファイルにアクセスするには、以下のいずれかを実行します。

- 任意のネットワーク マップ ビューから選択します。
- モニタ対象ネットワークでホストの IP アドレスを含む任意のイベント ビューから選択します。

ホストプロファイルは、ホスト名やMACアドレスなど、検出されたホストやデバイスに関する基本的な情報を提供します。ライセンスやシステム設定によっては、ホストプロファイルは次の情報を提供することもできます。

- ホスト上で実行中のオペレーティング システム
- ホスト上で実行中のサーバ
- ホスト上で実行中のクライアントと Web アプリケーション
- ホスト上で実行中のプロトコル
- ホスト上の侵害の兆候（IOC）タグ
- ホスト上の VLAN タグ
- ネットワーク上での過去 24 時間のユーザー アクティビティ
- ホストに関連するコンプライアンスallow違反
- ホストの最新のマルウェア イベント
- ホストに関連付けられている脆弱性
- ホストの Nmap スキャン結果

プロファイルには、ホスト属性もリストされます。ホスト属性を使用して、ネットワーク環境にとって重要な方法でホストを分類することができます。例えば、以下を行うことができます。

- ホストが存在する建物を示すホスト属性を割り当てる
- ホストの重要度の属性を使用して、特定のホストのビジネス重要度を指定し、ホストの重要度に基づいて相関ポリシーとアラートを作成する

ホストプロファイルで、そのホストに適用されている既存のホスト属性を表示し、そのホスト属性値を変更できます。

パッシブ侵入防御展開の一部としてadaptive profile updatesを使用している場合、ホスト上のオペレーティングシステム、およびホストが実行しているサーバとクライアントのタイプに最も適合するように、システムがトラフィックを処理する方法を調整することができます。

オプションで、ホストプロファイルからNmapスキャンを実行し、ホストプロファイルのサーバ情報とオペレーティング システムの情報を増やすことができます。Nmapスキャナはホストをアクティブに調査し、ホストを実行しているオペレーティングシステムおよびサーバの情報を取得します。スキャンの結果は、ホストのオペレーティング システムおよびサーバー アイデンティティのリストに追加されます。

関連トピック

ホスト プロファイルの表示 （1050 ページ）

ホストプロファイルの制限事項

利用できないホスト

ホストプロファイルは、ネットワーク上のすべてのホストでは使用できない可能性があります。考えられる原因は次のとおりです。

- タイムアウトしたため、ネットワーク マップからホストが削除された。
- ホストの制限に達した。
- ネットワーク検出ポリシーでモニタリングされないネットワーク セグメントに、ホストが存在している。

利用できない情報

ホストプロファイルに表示される情報は、ホストのタイプ、および利用可能なホストの情報によって異なる可能性があります。

次に例を示します。

- 非 IP ベースのプロトコル（STP、SNAP、IPX など）を使用してシステムでホストを検出した場合、そのホストはMACホストとしてネットワーク マップに追加され、IPホストに比べて使用できる情報はかなり少なくなります。
- システムは、エクスポートされたNetFlowレコードからネットワークマップにホストを追加できますが、これらのホストに使用できる情報は限られます（NetFlow データと管理対象デバイス データの違いを参照）。

（VRF を実行している導入）1 つの IP アドレスが複数のホストを表す場合がある

VRF を実行しているデバイスによってホストが報告された場合、1 つの IP アドレスが実際には複数のホストを表している可能性があります。VRF は、重複する IP アドレスを持つ複数のネットワークをモニターできます。そのため、同じ IP アドレスを異なるネットワークに存在させることができます。

ホスト プロファイルの表示

手順

次の 2 つの選択肢があります。

- ネットワーク マップで、プロファイルを表示するホストの IP アドレスをドリル ダウンします。
- 任意のイベントビューで、[ホストプロファイル（Host Profile）] をクリックするか、プロファイルを表示するホストの IP アドレスの隣にある、[侵害を受けたホスト（Compromised Host）] をクリックします。

ホスト プロファイルの基本ホスト情報

各ホストプロファイルは、検出されたホストまたは他のデバイスに関する基本情報を提供します。

次に、基本的なホスト プロファイルのフィールドについて説明します。

ドメイン（Domain）

ホストに関連付けられているドメイン。

IP アドレス

ホストに関連付けられているすべての IP アドレス（IPv4 と IPv6 の両方）。システムは、ホストに関連付けられている IP アドレスを検出し、サポートされている場合は、同じホストで使用される複数の IP アドレスをグループ化します。多くの場合、IPv6 ホストには、少なくとも 2 つの IPv6 アドレス（ローカルのみでルーティング可能なものと、グローバルにルーティング可能なもの）があり、その他に IPv4 アドレスを持っていることがあります。IPv4 専用ホストは、複数の IPv4 アドレスを持っていることがあります。

ホスト プロファイルは、そのホストに関連付けられている、検出されたすべての IP アドレスを一覧で示します。可能な場合は、ルーティング可能なホスト IP アドレスに、フラグ アイコン、およびアドレスに関連付けられている地理情報データを表す国コードも含まれています。

デフォルトでは最初の 3 つのアドレスだけが表示されることに注意してください。[すべて表示（Show All）] をクリックすると、ホストのすべてのアドレスが表示されます。

ホストネーム

ホストの完全修飾ドメイン名（わかる場合）。

NetBIOS 名（NetBIOS Name）

ホストの NetBIOS 名（使用できる場合）。Microsoft Windows ホストだけでなく Macintosh、Linux、または NetBIOS を使用するように設定されたその他のプラットフォームに NetBIOS 名を指定できます。たとえば、Samba サーバとして設定されている Linux ホストに NetBIOS 名を指定します。

デバイス (ホップ数)（Device (Hops)）

次のいずれかを行います。

- ホストが存在しているネットワークに関するレポート作成デバイス（ネットワーク検出ポリシーで定義されている）、または
- ホストをネットワーク マップへ追加する NetFlow データを処理したデバイス

デバイス名の後に、ホストを検出したデバイスとホスト自身の間のネットワーク ホップの数が丸括弧で囲まれて表示されます。複数のデバイスで対象のホストを参照できる場合は、報告元のデバイスが太字で表示されます。

このフィールドが空白の場合は、次のいずれかです。

- ホストがデバイスによってネットワーク マップに追加されたが、このデバイスは、ホストが存在しているネットワークに対してネットワーク検出ポリシーに定義されているとおりに明示的に監視していない。または、
- ホストの入力機能を使用してホストが追加されたが、システムによって検出されていない。

MAC アドレス（TTL）（MAC Addresses (TTL)）

ホストについて検出された 1 つ以上の MAC アドレスおよび関連付けられている NIC ベンダー。NIC のハードウェア ベンダーと現在の存続可能時間（TTL）値が括弧で囲まれて表示されます。

複数のデバイスが同じホストを検出した場合、Management Center には、どのデバイスがホストを報告したかに関係なく、ホストに関連付けられているすべての MAC アドレスと TTL 値が表示されます。

MAC アドレスが太字で表示されている場合、その MAC アドレスは、ARP および DHCP トラフィックを通じた検出により、IP アドレスに明確に関連付けられた、ホストの実際の/該当する/プライマリの MAC アドレスです。

太字フォントで表示されない MAC アドレスはセカンダリ アドレスなので、ホストの IP アドレスに明確に関連付けることはできません。たとえば、Firepowerデバイスは自身のネットワーク セグメント上のホストの MAC アドレスのみを取得できるため、トラフィックが Firepower デバイスが直接接続されていないネットワーク セグメントから発生している場合、監視されている MAC アドレス（ルータの MAC アドレス）は、ホストのセカンダリ MAC アドレスとして表示されます。

ホスト タイプ（Host Type）

システムで検出されたデバイスのタイプ（ホスト、モバイルデバイス、ジェイルブレイクされたモバイル デバイス、ルータ、ブリッジ、NAT デバイス、またはロード バランサ）。

ネットワーク デバイスを区別するためにシステムでは次の方法を使用します。

- Cisco Discovery Protocol（CDP）メッセージの分析。ネットワークのデバイスおよびそれらのタイプ（シスコ デバイスのみ）を特定できます。
- スパニング ツリー プロトコル（STP）の検出。デバイスをスイッチまたはブリッジとして識別します。
- 同じ MAC アドレスを使用している複数のホストの検出。MAC アドレスを、ルータに属しているものとして識別します。
- クライアント側からの TTL 値の変更、または通常のブート時間よりも頻繁に変更されている TTL 値の検出。この検出では、NAT デバイスとロード バランサを識別します。
- モバイル デバイスを区別するためにシステムでは次の方法を使用します。
- モバイル デバイスのモバイル ブラウザからの HTTP トラフィックのユーザ エージェント文字列の分析
- 特定のモバイル アプリケーションの HTTP トラフィックのモニタリング

デバイスがネットワーク デバイスまたはモバイル デバイスとして識別されない場合は、ホストとして分類されます。

前回の検出（Last Seen）

ホストのいずれかの IP アドレスが最後に検出された日時。

現在のユーザ（Current User）

このホストに最後にログインしたユーザ。

既存の現在のユーザが権限のあるユーザでない場合、ホストにログインしている権限を持たないユーザは、現在のユーザとして登録されるだけであることに注意してください。

表示（View）

接続、検出、マルウェア、および侵入イベント データのビューへのリンク。このリンクは、そのイベント タイプのデフォルト ワークフローを使用し、ホストに関連するイベントを表示するように制限されています。可能な場合は、これらのイベントには、ホストに関連付けられているすべての IP アドレスが含まれます。

ホスト プロファイルのオペレーティング システム

システムは、ホストで生成されたトラフィック内のネットワークおよびアプリケーション スタックを分析したり、User Agent でレポートされたホストデータを分析することによって、ホスト上で稼動しているオペレーティング システムのアイデンティティをパッシブに検出します。システムでは、他のソース（Nmap スキャナ、ホストの入力機能によりインポートされたアプリケーション データ）のオペレーティング システムの情報も照合します。どのアイデンティティを使用するかを判断する場合、システムは、各アイデンティティのソース（発生源）に割り当てられている優先度を考慮します。デフォルトでは、ユーザ入力が最も高い優先度を持ち、以降は高い順にアプリケーションまたはスキャナ ソース、検出されたアイデンティティ、となります。

システムでは、オペレーティング システムの具体的な定義ではなく、全般的な定義を提供することがあります。これは、トラフィックおよび他のアイデンティティ ソースで、対象のアイデンティティを詳しく調べるための十分な情報が提供されないためです。システムは、できるだけ詳しい定義を使用するために、ソースの情報を照合します。

オペレーティング システムは、ホストの脆弱性リスト、およびホストを対象とするイベントの影響の相関関係に影響するため、オペレーティング システムの特定の情報を手動で入力することもできます。また、オペレーティング システムに対して、サービス パックやアップデートなどの修正ファイルが適用されたことを示すことも、修正ファイルによって対処された脆弱性を無効にすることもできます。

たとえば、システムでホストのオペレーティング システムが Microsoft Windows 2003 であると特定されたが、実際にはホストが Microsoft Windows XP Professional および Service Pack 2 を実行していることがわかっている場合、オペレーティング システムのアイデンティティを実際のとおりに設定することができます。より具体的なオペレーティング システムのアイデンティティを設定すると、ホストの脆弱性のリストの精度が向上するため、対象のホストに対する影響の相関関係が、より限定的かつ正確になります。

システムでホストに対するオペレーティング システム情報が検出され、その情報が、アクティブなソースによって提供されている現行のオペレーティング システムのアイデンティティと競合している場合、アイデンティティの競合が発生します。実際にアイデンティティの競合が発生している場合、システムは脆弱性と影響の相関関係の両方のアイデンティティを使用します。

ネットワーク検出ポリシーを設定して、NetFlow エクスポータによってモニタされるホストのネットワーク マップに検出データを追加することができます。ただし、オペレーティング システムの ID を設定するためにホスト入力機能の使用を設定しない限り、これらのホストで使用可能なオペレーティング システム データはありません。

オペレーティングシステムを実行しているホストが、有効なネットワーク検出ポリシーのコンプライアンス allow リストに違反している場合、Management Center はオペレーティングシステムの情報にallow リストの**違反**のマークを付けます。また、ジェイルブレイクされたモバイルデバイスが有効なallowリストに違反している場合、そのデバイスのオペレーティングシステムの隣にアイコンが表示されます。

ホストのオペレーティング システムのアイデンティティに対して、カスタム表示文字列を設定できます。この表示文字列は、ホスト プロファイルで使用されます。

（注） あるホストについてオペレーティングシステムの情報を変更すると、ホストのコンプライアンス、およびコンプライアンスのallowリストが変わる可能性があります。

ネットワーク デバイスに対するホスト プロファイルでは、[オペレーティング システム（Operating Systems）] セクションのラベルが [システム（Systems）] に変わり、[ハードウェア（Hardware）] カラムが新しく表示されます。[システム（Systems）] の下にハードウェア プラットフォームの値が表示された場合、システムでは、ネットワーク デバイスの背後で検出された 1 つ以上のモバイル デバイスを示します。モバイル デバイスはハードウェア プラットフォームの情報を持っていることも、持っていないこともありますが、モバイルデバイスではないシステムではハードウェア プラットフォーム情報は検出されないことに注意してください。

次に、ホスト プロファイルで表示されるオペレーティング システムの情報フィールドについて説明します。

ハードウェア（Hardware）

モバイル デバイスのハードウェア プラットフォーム。

OS ベンダー/ベンダー（OS Vendor/Vendor）

オペレーティング システムのベンダー。

OS 製品/製品（OS Product/Product）

次の値のいずれかを指定します。

- すべてのソースから収集されたアイデンティティ データに基づいて、実行されている可能性が最も高いと判断されたオペレーティング システム。
- [Pending]：システムがオペレーティング システムをまだ識別しておらず、他に使用可能なアイデンティティ データがない場合。
- [unknown]：システムがオペレーティング システムを識別できず、オペレーティング システムに関して他に使用可能なアイデンティティ データがない場合。

（注） ホストのオペレーティングシステムをシステムで検出できない場合には、を参照してください。

OS バージョン/バージョン（OS Version/Version）

オペレーティング システムのバージョン。ホストがジェイルブレイクされたモバイル デバイスの場合、バージョンの後に括弧で囲まれて `Jailbroken` と示されます。

ソース（Source）

次の値のいずれかを指定します。

- [ユーザ（User）]：user_name
- [アプリケーション（Application）]：app_name
- [スキャナ（Scanner）]：scanner_type（Nmap またはその他のスキャナ）
- Firepower

システムでは、オペレーティング システムのアイデンティティを判断するために、複数のソースのデータを統合することができます。

オペレーティング システム アイデンティティの表示

検出された、またはホストに追加された特定のオペレーティング システムのアイデンティティを表示することができます。システムはソースの優先度を使用して、ホストに対する現行のアイデンティティを判断します。アイデンティティのリストでは、現行のアイデンティティが太字で強調されます。

1 つのホストに対して複数のオペレーティングシステムのアイデンティティが存在している場合のみ、[表示（View）] が有効になっていることに注意してください。

手順

ステップ 1 ホスト プロファイルの [オペレーティング システム（Operating System）] または [オペレーティング システムの競合（Operating System Conflicts）] セクションで [表示（View）] をクリックします。

ステップ 2 ホスト プロファイルのオペレーティング システム（1053 ページ）の説明に従って情報を入力します。

ステップ 3 必要に応じて、オペレーティングシステムのアイデンティティの横にある [削除（Delete）]（）をクリックします。

（注） シスコが検出したオペレーティング システムのアイデンティティは削除できません。

該当する場合は、このシステムは [オペレーティング システムのアイデンティティ情報（Operating System Identity Information）] ポップアップ ウィンドウからアイデンティティを削除し、ホスト プロファイルのオペレーティング システムの現在のアイデンティティを更新します。

現在のオペレーティング システムのアイデンティティの設定

Webインターフェイスを使用して、ホストに対する現行のオペレーティングシステムのアイデンティティを設定できます。Webインターフェイスを介してアイデンティティを設定すると、他のすべてのアイデンティティ ソースが上書きされるため、このアイデンティティが、脆弱性の評価および影響の相関関係で使用されます。ただし、オペレーティング システムを編集した後で、ホストに対するオペレーティング システムのアイデンティティの競合がシステムで検出されると、オペレーティング システムの競合が発生します。競合が解決されるまで、両方のオペレーティング システムが現行のものであるとみなされます。

手順

ステップ 1 ホスト プロファイルの [オペレーティング システム（Operating System）] セクションで [編集（Edit）] をクリックします。

ステップ 2 ここでは次のオプションがあります。

- [OS 定義（OS Definition）] ドロップダウンリストから [現在の定義（Current Definition）] を選択して、ホスト入力によって現行のオペレーティング システムのアイデンティティを確認して、手順 6 に進みます。
- [OS 定義（OS Definition）] ドロップダウン リストから現行のオペレーティング システムのアイデンティティのバリエーションを選択し、手順 6 に進みます。
- [OS 定義（OS Definition）] ドロップダウンリストから [ユーザ定義（User-Defined）] を選択して、手順 3 に進みます。

ステップ 3 必要に応じて、[カスタム表示文字列を使用する（Use Custom Display String）] を選択し、[ベンダー文字列（Vendor String）]、[製品文字列（Product String）]、および [バージョン文字列（Version String）] フィールドに表示するカスタム文字列を変更します。

ステップ 4 必要に応じて、別のベンダーからのオペレーティング システムに変更するには、[ベンダー（Vendor）] と [製品（Product）] のドロップダウンリストから選択します。

ステップ 5 必要に応じて、オペレーティング システムの製品リリース レベルを設定するには、[メジャー（Major）]、[マイナー（Minor）]、[リビジョン（Revision）]、[ビルド（Build）]、[パッチ（Patch）]、および [拡張（Extension）] ドロップダウン リストから選択します。

ステップ 6 必要に応じて、オペレーティング システムに対して修正ファイルが適用されたことを示す場合は、[修正の設定（Configure Fixes）] をクリックします。

ステップ 7 ドロップダウン リストから適用可能な修正を選択し、[追加（Add）] をクリックします。

ステップ 8 必要に応じて、[パッチ（Patch）] および [拡張（Extension）] ドロップダウン リストを使用して、対象のパッチと拡張機能を追加します。

ステップ 9 [終了（Finish）] をクリックします。

関連トピック

オペレーティング システムのアイデンティティの競合 （1057 ページ）

オペレーティング システムのアイデンティティの競合

システムで検出された新しいアイデンティティと現行のアイデンティティが競合しており、そのアイデンティティが、スキャナやアプリケーション、ユーザなどのアクティブなソースによって提供されていた場合、オペレーティング システムのアイデンティティで競合が発生します。

ホスト プロファイルでは、競合状態のオペレーティング システムのアイデンティティのリストは太字で表示されます。

システムの Web インターフェイスを介して、アイデンティティの競合を解決し、ホストに対する現行のオペレーティング システムのアイデンティティを設定することができます。Web インターフェイスを介してアイデンティティを設定すると、他のすべてのアイデンティティ ソースが上書きされるため、このアイデンティティが、脆弱性の評価および影響の相関関係で使用されます。

競合するオペレーティング システム アイデンティティを現行に設定する

手順

ステップ 1 ホスト プロファイルの [オペレーティング システム（Operating System）] セクションに移動します。

ステップ 2 次の 2 つの選択肢があります。

- ホストのオペレーティング システムとして設定するオペレーティング システムのアイデンティティの隣にある、[現行にする（Make Current）] をクリックします。
- アクティブなソースで、現行のアイデンティティとして使用しないアイデンティティが表示された場合は、使用しないアイデンティティを削除します。

オペレーティング システムのアイデンティティ競合の解決

手順

ステップ 1 ホスト プロファイルの [オペレーティング システムの競合（Operating System Conflicts）] セクションにある [解決（Resolve）] をクリックします。

ステップ 2 次の選択肢があります。

- [OS 定義（OS Definition）] ドロップダウンリストから [現在の定義（Current Definition）] を選択して、ホスト入力によって現行のオペレーティング システムのアイデンティティを確認して、手順 6 に進みます。
- [OS 定義（OS Definition）] ドロップダウンリストから、競合しているオペレーティング システムのアイデンティティのいずれかのバリエーションを選択して、手順 6 に進みます。

- [OS 定義（OS Definition）] ドロップダウンリストから [ユーザ定義（User-Defined）] を選択して、手順 3 に進みます。

ステップ 3 必要に応じて、[カスタム表示文字列の使用（Use Custom Display String）] を選択して、表示するカスタム文字列を [ベンダー文字列（Vendor String）]、[製品文字列（Product String）]、および [バージョン文字列（Version String）] フィールドに入力します。

ステップ 4 必要に応じて、別のベンダーからのオペレーティング システムに変更するには、[ベンダー（Vendor）] と [製品（Product）] のドロップダウンリストから選択します。

ステップ 5 必要に応じて、オペレーティング システムの製品リリース レベルを設定するには、[メジャー（Major）]、[マイナー（Minor）]、[リビジョン（Revision）]、[ビルド（Build）]、[パッチ（Patch）] および [拡張（Extension）] ドロップダウンリストから選択します。

ステップ 6 必要に応じて、オペレーティング システムに対して修正ファイルが適用されたことを示す場合は、[修正の設定（Configure Fixes）] をクリックします。

ステップ 7 適用した修正ファイルを、修正ファイル リストに追加します。

ステップ 8 [終了（Finish）] をクリックします。

ホスト プロファイルのサーバー

ホスト プロファイルのサーバ セクションでは、監視対象ネットワーク上のホストで検出されるか、エクスポートされた NetFlow レコードから追加されるか、スキャナまたはホスト入力機能のようなアクティブなソースを介して追加されるサーバを列挙します。

リストは 1 つのホストにつき最大 100 台のサーバを表示します。100 個の制限に達すると、ホストからサーバを削除するか、またはサーバがタイムアウトになるまで、いずれかのソースの新しいサーバ情報は、アクティブであってもパッシブであっても廃棄されます。

Nmap を使用してホストをスキャンすると、オープンな TCP ポート上で稼動している、以前に検出されなかったサーバの結果が Nmap によって Servers リストに追加されます。Nmap スキャンを実行した場合、または Nmap の結果をインポートした場合、ホストプロファイルに拡張可能な [スキャン結果（Scan Results）] セクションも表示され、Nmap スキャンによってホスト上で検出されたサーバ情報が示されます。さらに、ネットワーク マップからホストが削除されると、ホストのそのサーバーに対する Nmap スキャンの結果は廃棄されます。

（注） システムは、エクスポートされた NetFlow レコードからネットワークマップにホストを追加できますが、これらのホストに使用できる情報は限られます（NetFlow データと管理対象デバイス データの違いを参照）。

ホストプロファイルでサーバーを使用するためのプロセスは、ユーザーがプロファイルにアクセスする方法によって異なります。

- ネットワーク マップを介したドリル ダウンによりホスト プロファイルにアクセスする場合は、サーバーの名前が太字で強調されて、サーバーの詳細が表示されます。ホストの他

のサーバーの詳細を表示する場合は、対象のサーバー名の隣にある[表示（View）]（  ）をクリックします。

- 他の方法でホストプロファイルにアクセスする場合は、[サーバー（Servers）]セクションを展開し、詳細を表示するサーバーの隣にある[表示（View）]（）をクリックします。

（注） ホストが、有効な相関ポリシーにおけるコンプライアンスのallowリストに違反しているサーバーを実行している場合、Management Center は非準拠サーバーに、allowリストの [違反（Violation）] のマークを付けます。

次に、[Servers リスト（Servers list）] の列について説明します。

プロトコル

サーバが使用するプロトコルの名前。

[ポート（Port）]

サーバが実行されているポート。

アプリケーション プロトコル（Application Protocol）

次のいずれかになります。

- アプリケーション プロトコルの名前
- [保留中（pending）]：システムで、いずれかの理由のでアプリケーション プロトコルをポジティブまたはネガティブに識別できない場合
- [未知（unknown）]：既知のアプリケーション プロトコルのフィンガープリントに基づいてシステムでアプリケーションプロトコルを識別できない場合、または（対応するサーバは追加せずに、ポート情報での脆弱性を追加することにより）ホストの入力を介してサーバが追加された場合

アプリケーション プロトコルの名前にマウスを重ねると、タグが表示されます。

ベンダーおよびバージョン（Vendor and Version）

システム、Nmap、または他のアクティブなソースで識別されたベンダーとバージョン、またはホストの入力機能を介して取得したベンダーとバージョン。有効なソースで識別が行われなかった場合、フィールドは空白になります。

ホスト プロファイルのサーバーの詳細

Management Center は、1 つのサーバについてパッシブに検出されるアイデンティティを最大16個表示します。パッシブな検出ソースには、ネットワーク検出データおよびNetFlow レコードが含まれます。システムで、このサーバの複数のベンダーまたはバージョンを検出した場

合、サーバは複数のパッシブなアイデンティティを持つことができます。たとえば、複数のWeb サーバーで同じバージョンのサーバー ソフトウェアが実行されていない場合、管理対象デバイスと Web サーバー ファーム間にロード バランサがあると、システムでは HTTP について複数のパッシブ アイデンティティが識別されることがあります。Management Centerは、アクティブなソース（ユーザー入力、スキャナ、その他のアプリケーションなど）からのサーバー アイデンティティの数を制限することはありません。

Management Centerは現行のアイデンティティを太字で表示します。システムでは、さまざまな目的でサーバーの現行のアイデンティティが使用されます。このような目的には、1 つのホストに対する脆弱性の割り当て、影響の評価、ホストプロファイルの証明書およびコンプライアンスallowリストに対して記載された相関ルールの評価などがあります。

サーバーの詳細には、選択されたサーバーについて知られている、更新済みのサブサーバー情報が表示されることもあります。

サーバの詳細にサーバのバナーが表示されることもあります。これは、ホストプロファイルからサーバを表示したときに、サーバの詳細の下に表示されます。サーバのバナーは、サーバを識別するのに役立つサーバに関する追加情報を提供します。攻撃者がサーバのバナー文字列を意図的に変更した場合、システムは誤ったアイデンティティが示されたサーバを識別または検出できません。サーバのバナーには、そのサーバについて検出された最初のパケットの最初の 256 文字が表示されます。この情報は、サーバがシステムによって最初に検出されたときに一度だけ収集されます。バナーの内容は 2 列で表示されます。左側の列は 16 進表記で示され、右側の列は対応する ASCII 表記で示されます。

（注） サーバーのバナーを表示するには、ネットワーク検出ポリシーで[バナーのキャプチャ（Capture Banners）]チェックボックスをオンにする必要があります。このオプションはデフォルトでは無効になっています。

ホスト プロファイルのサーバの詳細セクションには、次の情報が含まれています。

プロトコル

サーバが使用するプロトコルの名前。

[ポート（Port）]

サーバが実行されているポート。

ヒット数（Hits）

管理対象デバイスまたはNmapスキャナによってサーバーが検出された回数。ホストの入力によってインポートされたサーバについては、システムがそのサーバについてトラフィックを検出しない場合、検出回数は 0 になります。

前回の使用（Last Used）

サーバが最後に検出された日時。システムで対象のサーバについて新しいトラフィックを検出しない場合、ホスト入力のデータが最後に使用された時間は、データの最初のインポート時間を反映しています。ホストの入力機能を介してインポートされたスキャナおよびアプリケーションのデータは、Management Center の設定に応じてタイム アウトします

が、Management Center の Web インターフェイスを介したユーザ入力の場合はタイム アウトしません。

アプリケーション プロトコル（Application Protocol）

サーバによって使用されるアプリケーション プロトコルの名前（既知の場合）。

[ベンダー（Vendor）]

サーバのベンダー。ベンダーがわからない場合、このフィールドは表示されません。

バージョン（Version）

サーバのバージョン。バージョンがわからない場合、このフィールドは表示されません。

ソース（Source）

次の値のいずれかを指定します。

- [ユーザ（User）]：user_name
- [アプリケーション（Application）]：app_name
- [スキャナ（Scanner）]：scanner_type（Nmap またはその他のスキャナ）
- システムで検出されたアプリケーションの場合、`Firepower`、`Firepower Port Match`、または `Firepower Pattern Match`
- NetFlow レコードからネットワーク マップに追加されたサーバの場合、`NetFlow`

システムでは、サーバーのアイデンティティを判断するために、複数のソースのデータを統合することができます。

サーバ詳細情報の表示

手順

ホストプロファイルの[サーバー（Servers）]セクションで、サーバーの横にある[表示（View）]（👁）をクリックします。

サーバーのアイデンティティの編集

ホスト上のサーバーのアイデンティティ設定を手動で更新し、修正ファイルによって対処された脆弱性を削除するために、ホストに適用した何らかの修正ファイルを設定することができます。サーバのアイデンティティを削除することもできます。

アイデンティティを削除した場合、削除したアイデンティティが唯一のアイデンティティであっても、サーバは削除されません。アイデンティティを削除すると、[サーバの詳細（Server

Detail）] ポップアップ ウィンドウからアイデンティティが削除されます。可能な場合は、ホスト プロファイルでそのサーバの現行のアイデンティティを更新します。

シスコ管理対象デバイスによって追加されたサーバのアイデンティティは、編集または削除できません。

手順

ステップ 1 ホスト プロファイルの [サーバ（Servers）] セクションに移動します。

ステップ 2 [表示（View）] をクリックし、[サーバーの詳細（Server Detail）] ポップアップ ウィンドウを開きます。

ステップ 3 サーバーのアイデンティティを削除するには、削除するサーバーアイデンティティの隣にある [削除（Delete）]（）をクリックします。

ステップ 4 サーバーのアイデンティティを変更するには、サーバーリストでサーバーの隣にある**[編集（Edit）]**（）をクリックします。

ステップ 5 次の 2 つの選択肢があります。

- [サーバ タイプの選択（Select Server Type）] ドロップダウン リストから現行の定義を選択します。
- [サーバー タイプの選択（Select Server Type）] ドロップダウン リストからサーバーのタイプを選択します。

ステップ 6 オプションで対象のサーバー タイプのベンダーと製品のみを表示するには、[サーバー タイプで制限（Restrict by Server Type）] チェックボックスをオンにします。

ステップ 7 オプションでサーバの名前とバージョンをカスタマイズするには、[カスタム表示文字列の使用（Use Custom Display String）] を選択し、[ベンダー文字列（Vendor String）] と [バージョン文字列（Version String）] に入力します。

ステップ 8 [製品マッピング（Product Mappings）] セクションで、使用するオペレーティング システム、製品、およびバージョンを選択します。

例：

たとえば、サーバを Red Hat Linux 9 にマップする場合は、ベンダーとして [Redhat, Inc.] を、製品として [Redhat Linux] を選択し、バージョンとして [9] を選択します。

ステップ 9 サーバの修正が適用されていることを示す場合は、[修正の設定（Configure Fixes）] をクリックして、そのサーバに適用するパッチを修正リストに追加します。

ステップ 10 [終了（Finish）] をクリックします。

サーバー アイデンティティの競合の解決

アプリケーションやスキャナなどのアクティブなソースが、サーバーのアイデンティティデータをホストへ追加したときに、サーバーアイデンティティの競合が発生します。その後で、システムはサーバーアイデンティティの競合を示しているポートのトラフィックを検出します。

手順

ステップ 1 ホスト プロファイルで、[サーバー（Servers）] セクションに移動します。

ステップ 2 サーバーの横にある解決をクリックします。

ステップ 3 [サーバー タイプの選択（Select Server Type）] ドロップダウン リストからサーバーのタイプを選択します。

ステップ 4 オプションで対象のサーバー タイプのベンダーと製品のみを表示するには、[サーバー タイプで制限（Restrict by Server Type）] チェックボックスをオンにします。

ステップ 5 必要に応じて、サーバの名前とバージョンをカスタマイズする場合は、[カスタム表示文字列の使用（Use Custom Display String）] を選択して、[ベンダー文字列（Vendor String）] と [バージョン文字列（Version String）] を入力します。

ステップ 6 [製品マッピング（Product Mappings）] セクションで、使用するオペレーティング システム、製品、およびバージョンを選択します。

例：

たとえば、サーバを Red Hat Linux 9 にマップする場合は、ベンダーとして [Redhat, Inc.] を、製品として [Redhat Linux] を選択し、バージョンとして [9] を選択します。

ステップ 7 サーバの修正が適用されていることを示す場合は、[修正の設定（Configure Fixes）] をクリックして、そのサーバに適用するパッチを修正リストに追加します。

ステップ 8 [終了（Finish）] をクリックします。

ホスト プロファイルの Web アプリケーション

ホスト プロファイルの [Web アプリケーション（Web Application）] セクションには、ネットワーク内のホスト上で動作していることをシステムが識別したクライアントと Web アプリケーションが表示されます。システムでは、パッシブ検出ソースとアクティブ検出ソースの両方から取得されるクライアントと Web アプリケーションの情報を識別できます。ただし、NetFlow レコードから追加されたホストに関する情報は一部しか取得することができません。

このセクションには、ホスト上で検出されたアプリケーションの製品とバージョン、使用できるクライアントまたは Web アプリケーションの情報、アプリケーションが最後に使用中であると検出された時間などの詳細情報が表示されます。

ホスト上で稼動している最大 16 個のクライアントが、このセクションに表示されます。16 個の制限に達すると、ユーザがホストからクライアントアプリケーションを削除するか、または

非アクティブである（クライアントがタイムアウトしている）ためにシステムによってホストプロファイルからクライアントが削除されるまで、新しいクライアント情報は、どのソースのものであるか、アクティブかパッシブかにかかわらず、廃棄されます。

また、検出されたそれぞれの Web ブラウザについては、アクセスされた最初の 100 個の Web アプリケーションが表示されます。この制限に達すると、ブラウザに関連付けられている新しい Web アプリケーションは、どのソースのものであるか、アクティブかパッシブかにかかわらず、次の条件を満たすまで廃棄されます。

- Web ブラウザのクライアント アプリケーションがタイムアウトになる、または
- ユーザーが、Web アプリケーションに関連付けられているアプリケーション情報をホストプロファイルから削除する

ホストが、有効な相関ポリシーにおけるコンプライアンス allow リストに違反しているアプリケーションを実行している場合、Management Center は非準拠アプリケーションに、allowリストの**違反** のマークを付けます。

ヒント ホスト上の特定のアプリケーションに関連付けられている接続イベントを分析するには、アプリケーションの隣にある [ロギング（Logging）]（） をクリックします。接続イベントに対する優先ワークフローの最初のページが表示され、ホストのIPアドレスの他、アプリケーションのタイプ、製品、およびバージョンによって制限された接続イベントが示されます。接続イベントに対する優先ワークフローがない場合、ワークフローを選択する必要があります。

次に、ホスト プロファイルに表示されるアプリケーション情報について説明します。

アプリケーション プロトコル（Application Protocol）

アプリケーション（HTTPブラウザ、DNSクライアントなど）で使用されるアプリケーションプロトコルを表示します。

クライアント（Client）

ペイロードから派生したクライアント情報。この情報は、システムが識別するか、Nmapがキャプチャするか、またはホスト入力機能によって取得されます。有効なソースで識別が行われなかった場合、フィールドは空白になります。

バージョン（Version）

クライアントのバージョンを表示します。

Web アプリケーション

Web ブラウザの場合は、http トラフィックでシステムによって検出されたコンテンツ。Web アプリケーションの情報は、システムによって識別された、Nmap によってキャプチャされた、他のアクティブなソースによって取得された、またはホストの入力機能を介して取得された特

定のタイプのコンテンツ（WMV や QuickTime など）を表します。有効なソースで識別が行われなかった場合、フィールドは空白になります。

ホスト プロファイルから Web アプリケーションを削除する

ホスト上で稼働していないことが判明しているアプリケーションを削除するには、ホストプロファイルからアプリケーションを削除します。ホストからアプリケーションを削除すると、そのホストにallowリストのコンプライアンスが適用されることがあります。

（注） システムでアプリケーションが再検出されると、アプリケーションはネットワーク マップおよびホスト プロファイルに再度追加されます。

手順

ステップ 1 ホスト プロファイルで、[アプリケーション（Applications）] セクションに移動します。

ステップ 2 削除するアプリケーションの横にある[削除（Delete）]（🗑）をクリックします。

ホスト プロファイルのホスト プロトコル

各ホスト プロファイルには、ホストに関連付けられているネットワーク トラフィックで検出されたプロトコルに関する情報が含まれています。この情報には次のものが含まれます。

プロトコル

ホストが使用するプロトコルの名前。

層（Layer）

プロトコルを実行しているネットワーク層（`Network`または`Transport`）。

ホストプロファイルに表示されているプロトコルが、有効な相関ポリシーのコンプライアンス allow リストに違反する場合、Management Center は非準拠プロトコルに、allow リストの**違反**のマークを付けます。

ホストプロファイルに、ホスト上で実行していないことがわかっているプロトコルがリストされている場合は、これらのプロトコルを削除できます。ホストからプロトコルを削除すると、ホストがコンプライアンス allow リストに準拠する可能性があります。

（注） システムでプロトコルが再検出されると、プロトコルはネットワーク マップおよびホスト プロファイルに再度追加されます。

ホスト プロファイルからプロトコルを削除する

手順

ステップ 1 ホスト プロファイルの [プロトコル（Protocols）] セクションに移動します。

ステップ 2 削除するプロトコルの横にある [削除（Delete）]（  ） をクリックします。

ホスト プロファイル内の侵害の兆候

システムは、モニタリング対象のネットワーク上でホストが悪意のある手段によって侵害されている可能性があるかどうかを判断するために、ホストに関連付けられているさまざまなタイプのデータ（侵入イベント、セキュリティ インテリジェンス、接続イベント、ファイルまたはマルウェア イベント）との関連性を示します。イベント データの特定の組み合わせと頻度は、影響を受けたホストの侵害の痕跡（IOC）タグをトリガーとして使用します。

ホスト プロファイルの [侵害の兆候（Indications of Compromise）] セクションには、ホストのすべての侵害の兆候のタグが表示されます。

侵害の兆候にタグを付けるように設定するには、Cisco Secure Firewall Management Center デバイス構成ガイドの「Enabling Indications of Compromise Rules」を参照してください。

侵害の兆候についての作業の詳細については、侵害の兆候データ （1107 ページ）とそのトピックのサブトピックを参照してください。

ホスト プロファイルの VLAN タグ

ホストが仮想 LAN（VLAN）のメンバである場合、ホスト プロファイルの [VLAN タグ（VLAN Tag）] セクションが表示されます。

物理ネットワーク機器は、多くの場合に VLAN を使用して、さまざまなネットワーク ブロックから論理ネットワーク セグメントを作成します。システムは 802.1q VLAN タグを検出し、それぞれに対して以下の情報を表示します。

- [VLAN ID] は、ホストがメンバである VLAN を表します。これは、802.1q VLAN の場合、0 ～ 4095 の任意の整数となります。
- [タイプ（Type）] は、VLAN タグが含まれている、カプセル化されたパケットを表します。値は Ethernet または Token Ring となります。
- [優先順位（Priority）] は、VLAN タグの優先度を表します。これは 0 ～ 7 の任意の整数で、7 は最も高い優先度です。

VLAN タグがパケット内でネスト構造になっている場合、システムは最も内側の VLAN タグを処理し、Management Center は最も内側の VLAN タグを表示します。システムは、ARP および DHCP トラフィックを通じて識別される MAC アドレスのみの VLAN タグ情報を収集し、これらのタグを表示します。

たとえば全体がプリンタで構成されている VLAN があり、システムがこの VLAN で Microsoft Windows 2000 のオペレーティング システムを検出した場合などは、VLAN タグ情報が有用です。VLAN 情報により、システムは正確性の高いネットワーク マップを生成できるようになります。

ホスト プロファイル内のユーザー履歴

ホスト プロファイルのユーザ履歴の部分には、過去 24 時間のユーザ アクティビティがグラフィック表示されます。一般的なユーザーは夕方にログオフし、また他のユーザーとホストのリソースを共有することがあります。電子メールのチェックなどの目的で行われる定期的なログインの要求は、短い標準の棒で示されます。ユーザーのアイデンティティ リストは棒グラフで提示され、ユーザー ログインが検出されたタイミングを示します。権限のないログインの場合は、棒グラフがグレーになっていることに注意してください。

システムは、ホストに対する権限のないユーザー ログインを、そのホストの IP アドレスに関連付けるため、そのユーザーはそのホストのユーザー履歴に表示されます。ただし、権限のあるユーザ ログインが同じホストで検出された場合、その権限のあるユーザ ログインに関連付けられているユーザが、そのホストの IP アドレスとの関連付けを引き継ぐため、新しい権限のないユーザ ログインがそのホストの IP アドレスとのそのユーザの関連付けを壊すことはありません。ネットワーク検出ポリシーで、失敗したログインのキャプチャを設定した場合、リストにはこのホストへのログインに失敗したユーザーが含まれます。

ホスト プロファイル内のホスト属性

ホスト属性を使用して、ネットワーク環境にとって重要な方法でホストを分類することができます。システムには以下の 3 つのタイプの属性があります。

- 定義済みホスト属性
- コンプライアンスの *allow* リストのホスト属性
- ユーザー定義ホスト属性

定義済みホスト属性を設定後、またはユーザ定義ホスト属性を作成後は、ホスト属性の値を割り当てる必要があります。

（注） ホスト属性は、どのドメイン レベルでも定義できます。現在のドメインと先祖ドメインで作成されたホスト属性を割り当てることができます。

定義済みホスト属性

Management Center には、2 つの定義済みホスト変数が用意されています。

ホストの重要度（Host Criticality）

特定のホストの業務の重要性を指定し、ホストの重要性に応じて相関ポリシーの応答を調整するには、この属性を使用します。たとえば、業務にとって組織のメールサーバが一般的なユーザ ワークステーションよりも重要であるとみなしている場合は、メール サーバと業務に重要なその他のデバイスに [高（High）] の値を割り当て、他のホストには [中（Medium）] または [低（Low）] の値を割り当てることができます。その上で、影響を受けるホストの重要度に基づいて異なるアラートを起動する相関ポリシーを作成できます。

注記（Notes）

他のアナリストに確認してもらいたいホストに関する情報を記録するには、このホスト固有の属性を使用します。たとえば、ネットワーク上のコンピュータに、パッチが適用されていない古いバージョンのテスト用オペレーティング システムが搭載されている場合、[注記（Notes）] 属性を使用して、システムは意図的にパッチを適用していないことを明示できます。

許可（Allow）リストのホスト属性

ユーザーが作成するコンプライアンス allow リストごとに、各allowリストと同じ名前でホスト属性が自動的に作成されます。allowリストのホスト属性に設定可能な値は、次のとおりです。

- 準拠（Compliant）：allowリストに準拠しているホストを識別します。
- 非準拠（Non-Compliant）：allowリストに違反しているホストを識別します。
- 未評価（Not Evaluated）：allowリストの有効な対象ではないホスト、または何らかの理由で評価されていないホストを識別します。

allowリストのホスト属性の値を編集したり、allowリストのホスト属性を削除したりすることはできません。

ユーザ定義のホスト属性

定義済みのホスト属性またはコンプライアンス allow リストのホスト属性で使用されている基準と異なる基準を使用してホストを識別する場合、ユーザー定義のホスト属性を作成することができます。例えば、以下を行うことができます。

- ホストに対してファシリティ コード、市町村、部屋番号などの物理的なロケーション ID を割り当てます。
- 特定のホストを担当するシステム管理者を示す担当者 ID を割り当てます。ホストに関連する問題が検出された場合、相関ルールとポリシーを作成して、適切なシステム管理者にアラートを送信することができます。

- ホストの IP アドレスに基づいて、事前定義されたリストからホストへ自動的に値を割り当てます。この機能は、ネットワーク上にホストが初めて表示されたときに、その新しいホストへ値を割り当てるために役立ちます。

ユーザ定義のホスト属性は、ホストプロファイルのページに表示されます。ここでホストごとに値を割り当てることができます。次のことも実行できます。

- 相関ポリシーと検索でホスト属性を使用します。
- イベントのホスト属性テーブルビューで属性を表示して、それに基づいてレポートを生成します。

ユーザ定義のホスト属性として、次のタイプのいずれか 1 つを使用できます。

テキスト（Text）

ホストに対してテキスト文字列を手動で割り当てることができます。

整数（Integer）

正の整数の範囲の最初の数と最後の数を指定してから、ホストに対してこれらの数の 1 つを手動で割り当てることができます。

リスト（List）

文字列値のリストを作成してから、ホストに対してこの値のいずれかを割り当てることができます。また、ホストの IP アドレスに基づいて、ホストに対して値を自動的に割り当てることもできます。

複数の IP アドレスを持つホストの 1 つの IP アドレスに基づいて値を自動的に割り当てると、これらの値は、ホストに関連付けられているすべてのアドレスに適用されます。[ホスト属性（Host Attributes）] テーブルを表示する場合は、このことに留意してください。

リストの値を自動的に割り当てる場合は、リテラルの IP アドレスではなくネットワークオブジェクトの使用を検討してください。このアプローチによって保守容易性を向上でき、特にマルチドメイン展開で有効です。これは、マルチドメイン展開でオーバーライドが有効になったオブジェクトを使用すると、子孫ドメインの管理者が先祖ドメインの設定を自分のローカル環境に合わせて調整できるためです。マルチドメイン展開では、子孫ドメインで重複した IP アドレスを使用している場合に意図しないホストに一致するのを避けるために、先祖ドメイン レベルで自動割り当てリストを定義する場合は注意してください。

URL

ホストに対して手動で URL の値を割り当てることができます。

ユーザー定義のホスト属性を削除すると、その属性が使用されているすべてのホストプロファイルから削除されます。

テキストまたは URL に基づくホスト属性の作成

手順

ステップ 1 **[分析（Analysis）] > [ホスト（Hosts）] > [ホスト属性（Host Attributes）]**を選択します。
ステップ 2 [ホスト属性管理（Host Attribute Management）] をクリックします。
ステップ 3 [属性の作成（Create Attribute）] をクリックします。
ステップ 4 名前を入力します。
ステップ 5 ユーザ定義のホスト属性 （1068 ページ） の説明に従って作成する属性の [タイプ（Type）] を選択します。
ステップ 6 [保存（Save）] をクリックします。

整数ベースのホスト属性の作成

整数ベースのホスト属性を定義する場合は、その属性が受け入れる数値の範囲を指定する必要があります。

手順

ステップ 1 **[分析（Analysis）] > [ホスト（Hosts）] > [ホスト属性（Host Attributes）]**を選択します。
ステップ 2 [ホスト属性管理（Host Attribute Management）] をクリックします。
ステップ 3 [属性の作成（Create Attribute）] をクリックします。
ステップ 4 名前を入力します。
ステップ 5 ユーザ定義のホスト属性 （1068 ページ） の説明に従って、作成する属性の [タイプ（Type）] を選択します。
ステップ 6 [最小（Min）] フィールドに、ホストに対して割り当てることができる範囲の最小の整数値を入力します。
ステップ 7 [最大値（Max）] フィールドに、ホストに対して割り当てることができる範囲の最大の整数値を入力します。
ステップ 8 [保存（Save）] をクリックします。

リストに基づくホスト属性の作成

リストベースのホストの属性を定義する場合は、リストに対してそれぞれの値を提供する必要があります。これらの値には、英数字、スペース、および記号を含めることができます。

手順

ステップ 1 **[分析（Analysis）] > [ホスト（Hosts）] > [ホスト属性（Host Attributes）]**を選択します。
ステップ 2 [ホスト属性管理（Host Attribute Management）] をクリックします。
ステップ 3 [属性の作成（Create Attribute）] をクリックします。
ステップ 4 名前を入力します。
ステップ 5 ユーザ定義のホスト属性 （1068 ページ）の説明に従って、作成する属性の [タイプ（Type）] を選択します。
ステップ 6 リストに値を追加するには、[値の追加（Add Value）] をクリックします。
ステップ 7 [名前（Name）] フィールドに、追加する最初の値を入力します。
ステップ 8 オプションで、ホストに追加した属性値を自動で割り当てるには、[ネットワークを追加（Add Networks）] をクリックします。
ステップ 9 [値（Value）] ドロップダウン リストから、追加した値を選択します。
ステップ 10 [IP アドレス（IP Address）] および [ネットマスク（Netmask）] フィールドに、この値を自動的に割り当てる IP アドレスのブロックを表す IP アドレスとネットワーク マスク（IPv4）を入力します。
ステップ 11 リストにさらに値を追加して、IP アドレス ブロックの範囲内の新しいホストにこれらの値を自動的に割り当てるには、手順 6 ～ 10 を繰り返します。
ステップ 12 [保存（Save）] をクリックします。

ホスト属性値の設定

事前定義またはユーザ定義のホスト属性に値を設定できます。システムによって生成されたコンプライアンス allow リストのホスト属性値は設定できません。

手順

ステップ 1 変更するホスト プロファイルを開きます。
ステップ 2 [属性（Attributes）] セクションで、[属性の編集（Edit Attributes）] をクリックします。
ステップ 3 必要に応じて、属性を更新します。
ステップ 4 [保存（Save）] をクリックします。

ホストプロファイル内の許可（Allow）リスト違反

コンプライアンスallowリスト（またはallowリスト）は一連の基準で、ユーザーはこれを使用して、特定のサブネット上での実行が許可されるオペレーティングシステム、アプリケーショ

ンプロトコル、クライアント、Webアプリケーション、およびプロトコルを指定することができます。

アクティブな相関ポリシーにallowリストを追加した場合に、システムでallowリストに違反しているホストがあることが検出されると、Management Center はallowリストのイベント（相関イベントの特別な種類）をデータベースに記録します。これらのallowリストイベントはそれぞれallowリスト違反に関連付けられます。これには、特定のホストがどのようにallowリストに違反しているか、および違反している理由が含まれています。あるホストが1つ以上のallowリストに違反している場合、ホストプロファイルにおいて、2 つの方法でこれらの違反を参照することができます。

ホストプロファイルには最初に、ホストに関連付けられている個々のallowリストの違反がすべて一覧表示されます。

次に、ホストプロファイルにおけるallowリスト違反の説明が続きます。

タイプ

違反のタイプ（つまり、違反がオペレーティングシステム、アプリケーション、サーバ、またはプロトコルの非準拠の結果として生じたかどうか）。

理由

違反についての特別な理由。たとえば、Microsoft Windows のホストのみを許可するallowリストがある場合、ホストプロファイルには、ホストで稼働している現行のオペレーティングシステム（`Linux Linux 2.4、2.6` など）が表示されます。

許可（Allow）リスト

違反に関連付けられているallowリストの名前。

次に、オペレーティングシステム、アプリケーション、プロトコル、およびサーバーに関連付けられているセクションで、Management Center が、非準拠の要素にallowリストの [違反（Violation）] のマークを付けます。たとえば、Microsoft Windows ホストのみを許可するようなallowリストでは、ホストプロファイルは、ホストのオペレーティングシステム情報の隣にallowリスト違反のアイコンを表示します。

（注） ホストのプロファイルを使用すると、コンプライアンスallowリストの共有ホストプロファイルを作成することができます。

共有許可（Allow）リストホストプロファイルの作成

コンプライアンスallowリストの共有ホストプロファイルは、複数のallowリストで、ターゲットホスト上で実行を許可されるオペレーティングシステム、アプリケーションプロトコル、クライアント、Web アプリケーション、およびプロトコルを指定します。つまり、複数のallowリストを作成するが、同じホストプロファイルを使用して複数のallowリストで特定のオペレーティングシステムを実行するホストを評価する場合は、共有ホストプロファイルを使用します。

既知の IP アドレスが割り当てられている任意のホストのホストプロファイルを使用して、コンプライアンスallowリストで使用できる共有ホストプロファイルを作成することができます。ただし、システムでホストのオペレーティングシステムをまだ特定していない場合は、個々のホストのホスト プロファイルに基づいて共有ホスト プロファイルを作成することはできないことに注意してください。

手順

ステップ 1 ホストプロファイルで、[**許可リスト（Allow List**）プロファイルの生成（Generate White List Profile）] をクリックします。

ステップ 2 特別なニーズに応じて、共有ホスト プロファイルを変更し、保存します。

関連トピック

許可（Allow） リスト ホスト プロファイルの作成 （1179 ページ）

ホスト プロファイルでのマルウェア検出

[最後に検出されたマルウェア（Most Recent Malware Detections）] セクションには、ホストがマルウェア ファイルを送信または受信した、最近のマルウェア イベントが最大 100 個表示されます。ホストプロファイルには、ネットワークベースのマルウェアイベント（マルウェア防御 によって生成されたもの）とエンドポイントベースのマルウェアイベント（Cisco Secure Endpoint によって生成されたもの）の両方のリストが示されます。

ファイルが遡ってマルウェアと識別されたファイル イベントにホストが関係している場合、ファイルが送信された元のイベントは、マルウェアの特定が行われた後で、マルウェアの検出リストに表示されます。マルウェアとして識別されたファイルが、マルウェアではないと遡って判断された場合、そのファイルに関連するマルウェア イベントはリストには表示されなくなります。たとえば、ファイルの性質が `Malware` であり、これが `Clean` に変わった場合、そのファイルのイベントは、ホスト プロファイル上のマルウェア検出リストから削除されます。

ホストプロファイルでマルウェアの検出を確認する際には、[マルウェア（Malware）]をクリックして、そのホストのマルウェアイベントを確認できます。

次に、ホスト プロファイルの [最新のマルウェア検出（Most Recent Malware Detections）] セクションの列について説明します。

Time

イベントが生成された日時。

ファイルがマルウェアであると遡って特定されたイベントでは、これはマルウェアが特定された時刻ではなく、元のイベントの時刻であることに注意してください。

[ホスト ロール（Host Role）]

検出されたマルウェアの伝送におけるホストのロール（送信側または受信側）。Cisco Secure Endpointによって生成されたマルウェアイベント（「エンドポイントベースのマルウェアイベント」）の場合、ホストは常に受信者になります。

[脅威名（Threat Name）]

検出されたマルウェアの名前。

ファイル名（File Name）

マルウェア ファイルの名前。

[ファイル タイプ（File Type）]

ファイルのタイプ（`PDF` や `MSEXE` など）。

ホスト プロファイルの脆弱性

ホスト プロファイルの [脆弱性（Vulnerabilities）] セクションには、ホストに影響を与える脆弱性が示されます。これらの脆弱性は、システムがホスト上で検出したオペレーティング システム、サーバ、およびアプリケーションに基づきます。

ホストのオペレーティング システムのアイデンティティ、またはホスト上のアプリケーション プロトコルのアイデンティティのいずれかで、アイデンティティの競合が発生している場合、システムは、競合が解決するまで両方のアイデンティティに対して脆弱性を表示します。

NetFlow データからネットワークマップに追加されたホストに使用可能なオペレーティングシステムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な（インパクト レベル 1：赤）インパクトレベルを割り当てることができません。このような場合は、ホスト入力機能を使用して、ホストのオペレーティングシステム ID を手動で設定します。

サーバーのベンダーおよびバージョンの情報は、ほとんどの場合はトラフィックに含まれていません。デフォルトでは、システムはこのようなトラフィックの送信側および受信側に対して、関連付けられている脆弱性をマップしません。ただし、ベンダーまたはバージョンの情報を持たない特定のアプリケーション プロトコルに対して脆弱性をマップするよう、システムを設定することができます。

ホストの入力機能を使用して、ネットワーク上のホストにサードパーティの脆弱性情報を追加すると、追加の [脆弱性（Vulnerabilities）] セクションが表示されます。たとえば QualysGuard Scanner から脆弱性をインポートすると、ホスト プロファイルには [QualysGuard 脆弱性（QualysGuard Vulnerabilities）] セクションが含まれます。サードパーティの脆弱性の場合は、ホスト プロファイルの対応する [脆弱性（Vulnerabilities）] セクションの情報は、ホストの入力機能を使用して脆弱性データをインポートしたときに提供した情報に制限されます。

サードパーティの脆弱性をオペレーティング システムおよびアプリケーション プロトコルと関連付けることはできますが、クライアントに関連付けることはできません。サードパーティ

の脆弱性のインポートについては、『*Firepower* システムホスト入力 *API* ガイド』を参照してください。

次に、ホスト プロファイルの [脆弱性（Vulnerabilities）] セクションのカラムについて説明します。

名前

脆弱性の名前。

[リモート（Remote）]

脆弱性がリモートで不正利用される可能性があるかどうかを示します。この列が空白の場合、脆弱性の定義にはこの情報は含まれていません。

コンポーネント

脆弱性に関連付けられているオペレーティング システム、アプリケーション プロトコル、またはクライアントの名前。

ポート

ポート番号（脆弱性が、特定のポート上で実行されているアプリケーションプロトコルに関連付けられている場合）。

関連トピック

脆弱性データのフィールド （1123 ページ）
脆弱性の非アクティブ化 （1124 ページ）

脆弱性に対するパッチのダウンロード

ネットワーク上のホストで検出された脆弱性を軽減するためのパッチをダウンロードできます。

手順

ステップ 1 パッチをダウンロードするホストのホスト プロファイルにアクセスします。
ステップ 2 [脆弱性（Vulnerabilities）] セクションを展開します。
ステップ 3 パッチを適用する脆弱性の名前をクリックします。
ステップ 4 [修正（Fixes）] セクションを展開して、脆弱性に対するパッチの一覧を表示します。
ステップ 5 ダウンロードするパッチの隣の [ダウンロード（Download）] をクリックします。
ステップ 6 パッチをダウンロードして、影響を受けるシステムに適用します。

個々のホストに関する脆弱性の非アクティブ化

ホストの脆弱性エディタを使用して、ホストごとに脆弱性を非アクティブにすることができます。ホストの脆弱性を非アクティブにしても、そのホストの影響の相関に対して脆弱性は使用されますが、影響レベルは自動的に 1 レベル減少します。

手順

ステップ 1 ホスト プロファイルの [脆弱性（Vulnerabilities）] セクションに移動します。

ステップ 2 [脆弱性の編集（Edit Vulnerabilities）] をクリックします。

ステップ 3 [有効な脆弱性（Valid Vulnerabilities）] リストから脆弱性を選択し、下矢印をクリックして [無効な脆弱性（Invalid Vulnerabilities）] リストに移動します。

ヒント 隣接している複数の脆弱性を選択するには、クリックおよびドラッグを使用します。脆弱性をダブルクリックして、リスト間を移動することもできます。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 必要に応じて、ホストの脆弱性を [無効な脆弱性（Invalid Vulnerabilities）] リストから [有効な脆弱性（Valid Vulnerabilities）] リストに移動して、脆弱性をアクティブ化します。

関連トピック

個々の脆弱性の非アクティブ化 （1076 ページ）
複数の脆弱性の非アクティブ化 （1127 ページ）

個々の脆弱性の非アクティブ化

ホスト プロファイルで脆弱性を非アクティブ化すると、ネットワーク マップにあるすべてのホストに対して脆弱性が非アクティブ化されます。ただし、いつでもその脆弱性を再アクティブ化することができます。

マルチドメイン展開では、先祖ドメインの脆弱性を非アクティブ化すると、すべての子孫ドメインでその脆弱性が非アクティブ化されます。リーフ ドメインでは、脆弱性が先祖ドメインでアクティブ化された場合、リーフ ドメインのデバイスの脆弱性をアクティブ化または非アクティブ化できます。

手順

ステップ 1 次のようにして、脆弱性の詳細にアクセスします。

- 影響を受けるホストプロファイルで、[脆弱性（Vulnerabilities）]セクションを展開し、有効または無効にする脆弱性の名前をクリックします。
- 事前定義されたワークフローで、**[分析（Analysis）]** > **[ホスト（Hosts）]** > **[脆弱性（Vulnerabilities）]** を選択し、有効または無効にする脆弱性の横にある [表示（View）]（） をクリックします。

ステップ 2 [影響を受ける条件（Impact Qualification）] ドロップダウン リストから [無効（Disabled）] を選択します。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ネットワーク マップ上のすべてのホストに対して、[影響を受ける条件（Impact Qualification）] の値を変更することを確認します。

ステップ 4 [完了（Done）] をクリックします。

次のタスク

- オプションで、上記の手順を実行中に、[影響を受ける条件（Impact Qualification）] ドロップダウン リストから [有効（Enabled）] を選択することによって、脆弱性をアクティブにします。

関連トピック

個々のホストに関する脆弱性の非アクティブ化 （1076 ページ）
複数の脆弱性の非アクティブ化 （1127 ページ）
オペレーティング システムのアイデンティティの競合 （1057 ページ）

ホスト プロファイルのスキャン結果

Nmap を使用してホストをスキャンする場合、または Nmap のスキャンから結果をインポートする場合、これらの結果は、スキャンに含まれているすべてのホストのホストプロファイルに表示されます。

Nmap が、ホストのオペレーティング システムについて、およびオープンでフィルタリングされていないポート上で稼動している任意のサーバーについて収集した情報が、ホストプロファイルの [オペレーティング システム（Operating System）] と [サーバー（Servers）] セクションにそれぞれ追加されます。また、Nmap は、そのホストのスキャン結果のリストを [スキャン結果（Scan Results）] セクションに追加します。プロファイルに [スキャン結果（Scan Results）] セクションが表示されるのは、スキャンでホスト上のオープン ポートが検出された場合のみであることに注意してください。

各結果には、情報のソース、スキャンしたポートの番号とタイプ、ポート上で稼動しているサーバの名前、Nmap で検出された任意の追加情報（ポートの状態やサーバのベンダー名など）が示されます。UDP ポートをスキャンする場合、そのポートで検出されたサーバーは [スキャン結果（Scan Results）] セクションにのみ表示されます。

ホスト プロファイルから Nmap スキャンを実行できることに注意してください。

ホスト プロファイルからのホストのスキャン

ホストプロファイルから、ホストに対してNmapスキャンを実行できます。スキャンが完了すると、ホスト プロファイルでそのホストのサーバーおよびオペレーティング システムの情報が更新されます。追加のスキャン結果は、すべてホスト プロファイルの [スキャン結果（Scan Results）] セクションに追加されます。

注意 Nmap 提供のサーバおよびオペレーティング システムのデータは、別の Nmap スキャンを実行するか、より優先度の高いホスト入力で上書きするまでスタティックなままになります。Nmap を使用したホストのスキャンを計画している場合は、定期的にスキャンをスケジュールします。

始める前に

- Nmap スキャンインスタンスを追加します。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Host Identity Sources*」の章を参照してください。

手順

ステップ 1 ホスト プロファイルで、[ホストのスキャン（Scan Host）] をクリックします。

ステップ 2 ホストのスキャンに使用するスキャン修復の横にある [スキャン（Scan）] をクリックします。

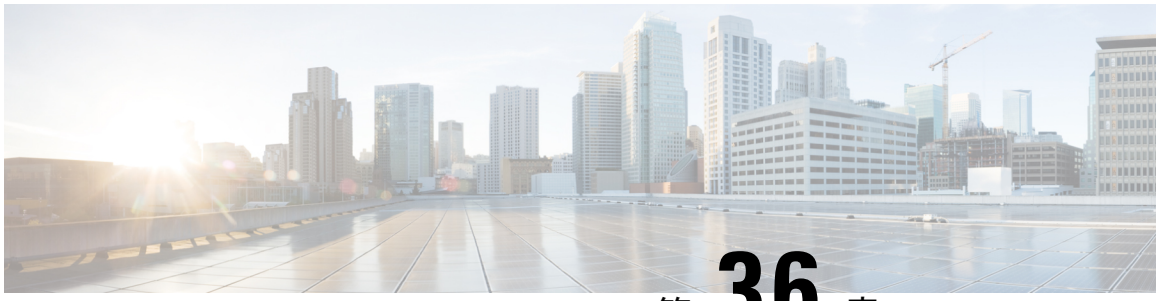
システムによってホストがスキャンされ、ホスト プロファイルに結果が追加されます。

関連トピック

Nmap スキャンの自動化 （604 ページ）

ホストプロファイルの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
VRF を使用する場合の制限事項	6.6	任意（Any）	仮想ルーティングおよび転送が環境内で使用されている場合、VRF に重複するネットワークスペースが含まれている可能性があるため、単一の IP アドレスが複数のホストを表すことがあります。 サポート対象プラットフォーム： Management Center



第 36 章

検出イベント

以下のトピックでは、ディスカバリ イベントを操作する方法について説明します。

検出イベントの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- セキュリティ アナリスト（Security Analyst）

検出イベントの検出データとアイデンティティ データ

システムは、モニタ対象のネットワークで検出された変更を表すイベントのテーブルを生成します。このテーブルを使用して、ネットワークのユーザアクティビティを確認し、応答方法を決定できます。ネットワーク検出およびアイデンティティポリシーは、収集するデータ、モニ

タするネットワーク セグメント、およびそのために使用する特定のハードウェア インターフェイスの種類を指定します。

検出およびアイデンティティ イベント テーブルを使用して、ネットワークのホスト、アプリケーション、およびユーザに関連付けられている脅威を特定できます。システムには事前定義のワークフローセットが用意されており、これを使用して、システムで生成されるイベントを分析することができます。また、特定のニーズに合った情報のみを表示するカスタム ワークフローを作成することもできます。

分析用にネットワーク検出およびアイデンティティ データを収集し、保存するには、ネットワーク検出およびアイデンティティ ポリシーを設定する必要があります。アイデンティティ ポリシーを設定した後、アクセス コントロール ポリシーで呼び出して、トラフィックのモニタに使用するデバイスに展開する必要があります。

ネットワーク検出ポリシーは、ホスト、アプリケーション、および権限のないユーザ データを提供します。アイデンティティ ポリシーは、権限のあるユーザー データを提供します。

次の検出イベント テーブルは、[分析（Analysis）] > [ホストおよび分析（Hosts and Analysis）] > [ユーザ（Users）] メニューにあります。

検出イベント テーブル	検出データが入力されますか。	アイデンティティ データが入力されますか。
ホスト（Hosts）	対応	×
ホストの侵害の兆候	対応	×
アプリケーション	対応	×
アプリケーション詳細（Application Details）	対応	×
サーバ	対応	×
ホスト属性（Host Attributes）	対応	×
検出イベント	対応	対応
ユーザの侵害の兆候（User Indications of Compromise）	対応	対応
アクティブ セッション（Active Sessions）	対応	対応
ユーザ アクティビティ（User Activity）	対応	対応
[ユーザー （Users）]	対応	対応
脆弱性（Vulnerabilities）	対応	×
サード パーティの脆弱性（Third-Party Vulnerabilities）	対応	×

ディスカバリ イベントの統計情報の表示

[ディスカバリ統計情報（Discovery Statistics）]ページには、システムで検出されたホスト、イベント、プロトコル、アプリケーション プロトコル、オペレーティング システムの概要が表示されます。

ページには、最後の 1 時間の統計情報、および累計の統計情報が示されます。特定のデバイス、またはすべてのデバイスについての統計情報を表示することができます。サマリに示されているイベント、サーバー、オペレーティング システム、またはオペレーティング システムのベンダーをクリックして、ページ上のエントリに一致するイベントを表示することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[概要（Overview）] > [概要（Summary）] > [検出統計（Discovery Statistics）]**を選択します。

ステップ 2 [デバイスの選択（Select Device）] リストから、統計情報を表示するデバイスを選択します。オプションで、Management Center で管理されるすべてのデバイスの統計情報を表示するには、[すべて（All）] を選択します。

ステップ 3 次の選択肢があります。

- [統計情報サマリ（Statistics Summary）]セクション（1082 ページ）で説明されているように、[統計サマリー（Statistics Summary）] に一般的な統計情報を表示します。
- [イベントの中断（Event Breakdown）] で、表示するイベント タイプをクリックします。イベントが 1 つも表示されない場合は、時間枠の変更（833 ページ）で説明されているように、時間範囲を調整する必要があるかもしれません。
- [プロトコルの中断（Protocol Breakdown）] で、検出されたホストによって現在使用されているプロトコルを表示します。
- [アプリケーション プロトコルの中断（Application Protocol Breakdown）] で、表示するアプリケーション プロトコルの名前をクリックします。
- [OS の中断（OS Breakdown）] で、[OS 名（OS Name）] または [OS ベンダー（OS Vendor）] をクリックします。

関連トピック

[イベント分類（Event Breakdown）] セクション （1083 ページ）
[プロトコル分類（Protocol Breakdown）] セクション （1083 ページ）
[アプリケーション プロトコル分類（Application Protocol Breakdown）] セクション （1083 ページ）

[OS 分類（OS Breakdown）] セクション （1084 ページ）

[統計情報サマリ（Statistics Summary）] セクション

[統計情報サマリ（Statistics Summary）] セクションの行の説明は次のとおりです。

合計イベント数（Total Events）

Management Center に格納されているディスカバリ イベントの合計数。

過去 1 時間のイベントの合計（Total Events Last Hour）

最後の 1 時間に生成されたディスカバリ イベントの合計数。

過去 1 日のイベントの合計（Total Events Last Day）

最後の 1 日に生成されたディスカバリ イベントの合計数。

アプリケーションプロトコル合計数（Total Application Protocols）

検出されたホストで実行されているサーバのアプリケーション プロトコルの合計数。

IP ホストの合計（Total IP Hosts）

一意の IP アドレスによって特定された検出済みホストの合計数。

MAC ホストの合計（Total MAC Hosts）

IP アドレスで特定されない検出済みホストの合計数。

すべてのデバイス、または特定のデバイスのどちらについてのディスカバリ統計情報を参照している場合でも、[MAC ホストの合計（Total MAC Hosts）] の統計情報は同じになることに注意してください。これは、管理対象デバイスが IP アドレスに基づいてホストを検出するためです。この統計情報は、他の方法によって識別され、特定の管理対象デバイスに依存しないすべてのホストの合計を表します。

ルータの合計（Total Routers）

ルータとして識別された検出ノードの合計数。

ブリッジの合計（Total Bridges）

ブリッジとして識別された検出ノードの合計数。

ホスト制限の使用（Host Limit Usage）

使用中のホスト制限のパーセンテージ合計。ホストの制限は、Management Center のモデルによって定義されます。すべての管理対象デバイスについての統計情報を表示している場合は、ホストの使用制限のみが表示されることに注意してください。

（注） ホストの制限に達してホストが削除されると、ディスカバリ データを消去するネットワークマップ上にホストは表示されなくなります。

最後に受け取ったイベント（Last Event Received）

最後のディスカバリ イベントが行われた日付と時間。

最後に受信した接続（Last Connection Received）

最後の接続が完了した日付と時間。

[イベント分類（Event Breakdown）] セクション

[イベント分類（Event Breakdown）] セクションには、データベースに格納されている各イベントタイプの合計数のカウントの他に、ネットワーク検出の各タイプのカウント、および最後の 1 時間で発生したホスト入力イベントが示されます。

[イベント分類（Event Breakdown）] セクションを使用して、ディスカバリ イベントおよびホスト入力イベントの詳細を表示することもできます。

関連トピック

検出イベントおよびホスト入力イベント （1088 ページ）

[プロトコル分類（Protocol Breakdown）] セクション

[プロトコル分類（Protocol Breakdown）] セクションには、検出されたホストで使用されているプロトコルが示されます。このセクションには、検出されたそれぞれのプロトコル名、プロトコル スタックの「レイヤ」、およびプロトコルを使用して通信しているホストの合計数が表示されます。

[アプリケーション プロトコル分類（Application Protocol Breakdown）] セクション

[アプリケーション プロトコル分類（Application Protocol Breakdown）] セクションには、検出されたホストで使用されているアプリケーション プロトコルが示されます。このセクションには、プロトコル名、最後の 1 時間にアプリケーション プロトコルを実行したホストの合計数、いずれかのポイントでプロトコルの実行が検出されたホストの合計数が表示されます。

[アプリケーション プロトコル分類（Application Protocol Breakdown）] セクションではさらに、検出されたプロトコルを使用しているサーバーの詳細を表示することもできます。

関連トピック

サーバー データ （1113 ページ）

[OS 分類（OS Breakdown）] セクション

[OS 分類（OS Breakdown）] セクションには、監視対象ネットワーク上で稼動しているオペレーティング システム、およびオペレーティング システムのベンダー、各オペレーティング システムを実行しているホストの合計数が示されます。

オペレーティング システムの名前またはバージョンの値が unknown の場合は、オペレーティング システムまたはそのバージョンが、システムのフィンガープリントの内容と一致しないことを意味します。値が pending の場合は、オペレーティング システムまたはそのバージョンを識別するための十分な情報がシステムで収集されていないことを意味します。

[OS 分類（OS Breakdown）] セクションを使用して、検出されたオペレーティング システムの詳細を表示することができます。

関連トピック

ホスト データ （1097 ページ）

ディスカバリ パフォーマンス グラフの表示

ディスカバリ イベントを使用して、管理対象デバイスのパフォーマンス統計情報を示すグラフを生成することができます。

新しいデータは5分ごとに統計グラフに蓄積されます。したがって、グラフをすばやくリロードしても、次の5分の差分更新が実行されるまでデータは変更されていない場合があります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

始める前に

適切なネットワーク検出ポリシーを編集して、アプリケーション、ホスト、およびユーザーを含めます（これは、システム パフォーマンスに影響を与える可能性があります）。ネットワーク検出ルールの設定およびアクションと検出されるアセットを参照してください。

このタスクを実行するには、管理者ユーザーまたはメンテナンスユーザーである必要があります。

手順

ステップ 1 **[概要（Overview）] > [概要（Summary）] > [検出パフォーマンス（Discovery Performance）]** を選択します。

ステップ 2 [デバイスの選択（Select Device）] リストから、Management Center または対象とする管理対象デバイスを選択します。

ステップ 3 ディスカバリ パフォーマンス グラフ タイプ （1085 ページ） で説明されているように、[グラフの選択（Select Graph(s)）] リストから、作成するグラフの種類を選択します。

ステップ 4 [時間範囲の選択（Select Time Range）] リストから、グラフに使用する時間範囲を選択します。

ステップ 5 [グラフ（Graph）] をクリックして、選択した統計情報をグラフ化します。

ディスカバリ パフォーマンス グラフ タイプ

次に、使用できるグラフのタイプについて説明します。

処理されたイベント数/秒

Data Correlator が 1 秒間に処理するイベントの数を表します。

処理された接続数/秒

Data Correlator が 1 秒間に処理する接続の数を表します。

生成されたイベント数/秒

システムが 1 秒間に生成するイベントの数を表します。

メガビット/秒

ディスカバリ プロセスによって 1 秒間に分析されたトラフィック数（メガビット）を表します。

平均バイト/パケット

ディスカバリ プロセスによって分析された各パケットに含まれるバイト数の平均を表します。

キロパケット/秒

ディスカバリ プロセスで 1 秒間に分析されるパケット数を 1000 単位で表します。

ディスカバリおよびアイデンティティ ワークフローの使用

Management Center は、ネットワークで生成されるディスカバリおよびアイデンティティ データの分析で使用できるイベント ワークフローセットを提供します。ワークフローはネットワーク マップとともに、ネットワーク資産に関する主要な情報源になります。

Management Center には、ディスカバリおよびアイデンティティ データ、検出されたホストとそのホストの属性、サーバ、アプリケーション、アプリケーションの詳細、脆弱性、ユーザアクティビティ、ユーザに関する事前定義されたワークフローが用意されています。ユーザはカスタム ワークフローを作成することもできます。

手順

ステップ 1 事前定義されたワークフローにアクセスするには、以下を実行します。

- ディスカバリとホスト入力データ：ディスカバリ イベントとホスト入力イベントの表示（1095 ページ）を参照してください。
- ホスト データ：ホスト データの表示 （1097 ページ）を参照してください。
- ホスト属性データ：ホスト属性の表示 （1105 ページ）を参照してください。
- ホストまたはユーザの侵害の兆候データ：侵害兆候データの表示と処理（1108 ページ）を参照してください。
- サーバ データ：サーバー データの表示 （1113 ページ）を参照してください。
- アプリケーションデータ：アプリケーションデータの表示（1117 ページ）を参照してください。
- アプリケーション詳細データ：アプリケーション詳細データの表示（1120 ページ）を参照してください。
- アクティブセッションデータ：アクティブ セッション データの表示 （1142 ページ） を参照してください。
- ユーザー データ：ユーザー データの表示 （1145 ページ）を参照してください。
- ユーザアクティビティデータ：ユーザー アクティビティ データの表示 （1148 ページ）を参照してください。
- ネットワーク マップ：ネットワーク マップの表示 （744 ページ）を参照してください。

ステップ 2 カスタム ワークフローにアクセスするには、**[分析（Analysis）] > [詳細（Advanced）] > [カスタムワークフロー（Custom Workflows）]** を選択します。

ステップ 3 カスタム テーブルに基づいたワークフローにアクセスするには、**[分析（Analysis）] > [詳細（Advanced）] > [カスタムテーブル（Custom Tables）]** を選択します。

ステップ 4 以下のいずれかのアクションを実行します。これらは、ネットワーク検出ワークフローでアクセスするすべてのページに共通です。

- 列の制約：表示される列を制約するには、非表示にする列の見出しにある[閉じる（Close）]（×）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。

  ヒント 他のカラムを表示または非表示にするには、[適用（Apply）] をクリックする前に、該当するチェック ボックスをオンまたはオフにします。無効にした列をビューに戻すには、展開の矢印をクリックして検索の制約を展開し、[無効な列（Disabled Columns）] の下の列名をクリックします。

- 削除：現在の制約されたビューにある一部またはすべての項目を削除するには、削除する項目の横にあるチェックボックスをオンにし、[削除（Delete）] または [すべて削除（Delete

All）]をクリックします。これらのアイテムが再検出されても、システムのディスカバリ機能が再開されるまで、これらのアイテムは削除されたままになります。

注意 [分析（Analysis）]>[ユーザー（Users）]>[ユーザー（Users）]**[分析（Analysis）]>[ユーザー（Users）]>[アクティブセッション（Active Sessions）]**ページで非 VPN セッションを削除する前に、そのセッションが実際に閉じられていることを確認します。アクティブなセッションを削除すると、該当するポリシーはデバイス上のセッションを検出できなくなります。そのため、モニターしたり、ブロックしたりするようポリシーが設定されていたとしても、セッションはそれらのアクションを実行しません。

（注） [分析（Analysis）]>[ユーザ（Users）]>[アクティブ セッション（Active Sessions）]ページの VPN セッションに関する詳細については、「リモート アクセス VPN の現在のユーザの表示」を参照してください。

（注） サードパーティの場合とは異なり、シスコの脆弱性は削除**できません**。ただし、確認済みとしてマークすることはできます。

- ドリル ダウン：ワークフローの次のページにドリルダウンするには、ドリルダウン ページの使用 （818 ページ）を参照してください。
- 現在のページを移動する：現在のワークフロー ページ内を移動するには、ワークフロー ページのナビゲーション ツール （815 ページ）を参照してください。
- ワークフロー内で移動する：現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。
- 他のワークフローに移動する：関連するイベントを調べるために、その他のイベント ビューに移動するには、ワークフロー間のナビゲーション （839 ページ）を参照してください。
- データのソート：ワークフローでデータをソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。
- ホストプロファイルの表示：IP アドレスのホストプロファイルを表示するには、[ホストプロファイル（Host Profile）]をクリックします。アクティブな侵害の兆候（IOC）タグのあるホストの場合は、IP アドレスの横に表示される [侵害を受けたホスト（Compromised Host）] をクリックします。
- ユーザープロファイル：ユーザー ID 情報を表示するには、[ユーザーID（User Identity）]の隣に表示される [ユーザー（User）] アイコン、または IOC に関連付けられているユーザーの場合は [レッドユーザー（Red User）] をクリックします。 の表示

関連トピック

ワークフローの使用 （809 ページ）
Management Center データベースからのデータの消去 （630 ページ）

検出イベントおよびホスト入力イベント

システムは検出イベントを生成します。このイベントは、監視対象ネットワークセグメントにおける変更の詳細をやり取りします。新しく検出されたネットワーク機能に対しては、新しいイベントが生成され、以前に認識されたネットワークアセットにおける何らかの変更に対しては、変更のイベントが生成されます。

最初のネットワーク検出のフェーズ中に、システムは各ホスト、および各ホスト上での稼動が検出されたTCPまたはUDPサーバについて、新しいイベントを生成します。必要に応じて、エクスポートされたNetFlowレコードを使用してこれらの新しいホストおよびサーバのイベントを生成するよう、システムを設定することができます。

またシステムは、検出された各ホスト上で稼動しているネットワーク、トランスポート、およびアプリケーションプロトコルのそれぞれに対して新しいイベントを生成します。設定されている検出ルールでアプリケーションプロトコルの検出を無効にして、NetFlowエクスポータをモニターできますが、管理対象デバイスをモニターするよう設定された検出ルールではできません。NetFlow以外の検出ルールでホストまたはユーザの検出を有効にすると、アプリケーションが自動的に検出されます。

最初のネットワークマッピングが完了すると、続けてシステムは変更イベントを生成し、ネットワークの変更を記録します。変更イベントは、以前に検出されたアセットの設定が変更されるたびに生成されます。

検出イベントが生成されると、データベースに記録されます。Management CenterのWebインターフェイスを使用して、検出イベントを表示、検索、および削除できます。また、相関ルールで検出イベントを使用することもできます。ユーザが指定する他の基準だけでなく、生成される検出イベントのタイプに基づいて、相関ルールを作成することができます。相関ルールは相関ポリシーで使用され、ネットワークトラフィックが基準を満たしたときに、修復、syslog、SNMP、および電子メールアラートの応答を起動します。

ホスト入力機能を使用して、ネットワークマップにデータを追加することができます。オペレーティングシステムの情報を追加、修正、または削除することができますが、この場合、システムは対象のホストに対する情報の更新を停止します。アプリケーションプロトコル、クライアント、サーバ、およびホストの属性を手動で追加、変更、または削除することも、脆弱性の情報を変更することもできます。この処理を行う場合、システムはホスト入力機能を生成します。

ディスカバリイベントタイプ

ネットワーク検出ポリシーにシステムが記録するディスカバリイベントのタイプを設定できます。ディスカバリイベントのテーブルを表示すると、[イベント（Event）]カラムにイベントタイプが表示されます。次に、ディスカバリイベントタイプについて説明します。

ホストの追加 MAC の検出

このイベントは、以前に検出したホストに対してシステムが新しいMACアドレスを検出したときに生成されます。

このイベントは多くの場合、ルータを通じてトラフィックを渡すホストをシステムが検出したときに生成されます。それぞれのホストには 1 つの IP アドレスがありますが、これらの IP アドレスはすべて、ルータに関連付けられている MAC アドレスを持っているように見えます。システムは IP アドレスに関連付けられている実際の MAC アドレスを検出すると、ホスト プロファイル内でその MAC アドレスを太字で表示し、イベント ビューのイベント説明に「ARP/DHCP detected」のメッセージを表示します。

クライアント タイムアウト

このイベントは、非アクティブであるという理由で、システムがデータベースからクライアントをドロップしたときに生成されます。

クライアント更新

このイベントは、HTTP トラフィック内でシステムがペイロード（つまり音声やビデオ、Web メールなどの特別なタイプのコンテンツ）を検出したときに生成されます。

DHCP：IP アドレスの変更

このイベントは、DHCP アドレスの割り当てによってホスト IP アドレスが変わったことがシステムで検出された場合に生成されます。

DHCP：IP アドレスの再割り当て

このイベントは、ホストが IP アドレスを再利用するとき、つまり他の物理ホストが以前に使用した IP アドレスを、別のホストが DHCP の IP アドレス割り当てによって取得した場合に生成されます。

ホップ数の変更

このイベントは、ホストと、そのホストを検出するデバイス間でシステムがネットワーク ホップ数の変更を検出した場合に生成されます。これは次のような場合に発生します。

- デバイスがさまざまなルータを介してホストのトラフィックを監視しており、ホストの場所についてより適切な決定ができる場合。
- デバイスがホストから ARP 送信を検出し、ホストがローカル セグメント上にあることを示している場合。

ホスト削除：ホスト制限に到達

このイベントは、Management Center 上でホストの制限を超えて、のネットワーク マップから監視対象のホストが削除されたときに生成されます。

ホスト ドロップ：ホスト制限に到達

このイベントは、Management Center 上でホストの制限に達して新しいホストがドロップされたときに生成されます。このイベントとの相違点として、前述のイベントでは、ホストの制限に達したときに古いホストがネットワーク マップから削除されます。

ホストの制限に達したときに新しいホストをドロップするには、**[ポリシー（Policies）]**>**[ネットワーク検出（Network Discovery）]**>**[詳細（Advanced）]** を選択し、[ホストの制限に達した場合（When Host Limit Reached）] を [ホストをドロップ（Drop hosts）] に設定します。

ホスト IOC 設定

このイベントは、ホストに対してIOC（侵害の痕跡）が設定され、アラートが生成されたときに生成されます。

ホスト タイムアウト

このイベントは、ネットワーク検出ポリシーで定義された間隔内でホストがトラフィックを生成しなかったために、ネットワーク マップからホストがドロップされたときに生成されます。個々のホストのIPアドレスとMACアドレスはそれぞれタイムアウトになることに注意してください。関連付けられているアドレスがすべてタイムアウトになるまで、ホストはネットワーク マップから消えません。

ネットワーク検出ポリシーで監視するネットワークを変更する場合は、ネットワーク マップから古いホストを手動で削除して、それらのホストがホストの制限に不利に作用しないようにします。

ネットワーク デバイスへのホスト タイプの変更

このイベントは、システムが、検出されたホストが実際はネットワーク デバイスであったことを認識したときに生成されます。

アイデンティティ競合

このイベントは、システムが、新しいサーバまたはオペレーティング システムに対する現行のアクティブなアイデンティティと競合する、そのサーバまたはオペレーティング システムのアイデンティティを検出したときに生成されます。

より新しいアクティブなアイデンティティ データを取得するためにホストを再スキャンして、アイデンティティの競合を解決する場合は、Identity Conflict イベントを使用して Nmap の修復をトリガーできます。

アイデンティティ タイムアウト

このイベントは、アクティブなソースからのサーバまたはオペレーティング システムの ID データがタイムアウトしたときに生成されます。

より新しいアクティブなアイデンティティ データを取得するために、ホストを再スキャンしてアイデンティティ データをリフレッシュする場合は、Identity Conflict イベントを使用して Nmap の修復をトリガーできます。

MAC 情報の変更

このイベントは、特定のMACアドレスまたはTTL値に関連付けられている情報で、システムが変更を検出したときに生成されます。

このイベントは多くの場合、ルータを通じてトラフィックを渡すホストをシステムが検出したときに発生します。それぞれのホストには 1 つの IP アドレスがありますが、これらの IP アドレスはすべて、ルータに関連付けられている MAC アドレスを持っているように見えます。システムは IP アドレスに関連付けられている実際の MAC アドレスを検出すると、ホスト プロファイル内でその MAC アドレスを太字で表示し、イベント ビューのイベント説明に「ARP/DHCP detected」のメッセージを表示します。TTL は変わる可能性がありますが、これはトラフィックが複数のルータを通じて渡される可能性があるためです。また、システムがホストの実際の MAC アドレスを検出した場合も TTL が変わる可能性があります。

NETBIOS 名の変更

このイベントは、システムがホストの NetBIOS 名に対する変更を検出したときに生成されます。このイベントは、NetBIOS プロトコルを使用するホストに対してのみ生成されます。

新しいクライアント

このイベントは、システムが新しいクライアントを検出したときに生成されます。

（注） 分析用にクライアントデータを収集および格納するには、ネットワーク検出ポリシーのディスカバリ ルールでアプリケーションの検出が有効になっていることを確認します。

新しいホスト

このイベントは、システムがネットワーク上で稼動している新しいホストを検出したときに生成されます。

このイベントは、デバイスが新しいホストを含むNetFlowデータを処理するときも生成できます。この状況でイベントを生成するには、NetFlow データを管理するネットワーク検出ルールでホストを検出するように設定します。

新しいネットワーク プロトコル

このイベントは、ホストが新しいネットワーク プロトコル（IP、ARP など）と通信していることをシステムが検出したときに生成されます。

新しい OS

このイベントは、システムがホストの新しいオペレーティング システムを検出した、またはホストのオペレーティング システムで変更を検出したときに生成されます。

新しい TCP ポート

このイベントは、ホスト上でアクティブな新しい TCP サーバ ポート（SMTP または Web サービスで使用されているポートなど）をシステムが検出したときに生成されます。このイベントは、アプリケーション プロトコル、またはアプリケーション プロトコルに関連付けられているサーバの識別には使用されません。情報は、TCP Server Information Update イベントで伝送されます。

このイベントは、デバイスがネットワーク マップにすでに存在しないモニタ対象ネットワーク上のサーバを含むNetFlowデータを処理するときも生成できます。この状況でイベントを生成するには、NetFlow データを管理するネットワーク検出ルールでアプリケーションを検出するように設定します。

新しいトランスポート プロトコル

このイベントは、ホストが新しいトランスポート プロトコル（TCP、UDP など）と通信していることをシステムが検出したときに生成されます。

新しい UDP ポート

このイベントは、システムが、ホスト上で稼動している新しい UDP サーバ ポートを検出したときに生成されます。

このイベントは、デバイスがネットワーク マップにすでに存在しないモニタ対象ネットワーク上のサーバを含むNetFlowデータを処理するときも生成できます。この状況でイベントを生成するには、NetFlow データを管理するネットワーク検出ルールでアプリケーションを検出するように設定します。

TCP ポート クローズ

このイベントは、システムが、ホスト上で TCP ポートがクローズしたことを検出したときに生成されます。

TCP ポート タイムアウト

このイベントは、システムのネットワーク検出ポリシーに定義された間隔内で、システムが TCP ポートからアクティビティを検出しなかったときに生成されます。

TCP サーバ情報の更新

このイベントは、ホスト上で稼動しており、すでに検出されている TCP サーバでシステムが変更を検出したときに生成されます。

このイベントは、TCP サーバが更新されたときに生成される場合があります。

UDP ポート クローズ

このイベントは、システムが、ホスト上で UDP ポートがクローズしたことを検出したときに生成されます。

UDP ポート タイムアウト

このイベントは、ネットワーク検出ポリシーに定義された間隔内で、システムが UDP ポートからアクティビティを検出しなかったときに生成されます。

UDP サーバ情報の更新

このイベントは、ホスト上で稼動しており、すでに検出されている UDP サーバでシステムが変更を検出したときに生成されます。

このイベントは、UDP サーバが更新されたときに生成される場合があります。

VLAN タグ情報の更新

このイベントは、システムが、VLAN タグ内でホストに起因する変更を検出したときに生成されます。

関連トピック

ホスト入力イベント タイプ （1093 ページ）

ホスト入力イベント タイプ

ディスカバリ イベントのテーブルを表示すると、[イベント（Event）] カラムにイベント タイプが表示されます。

ユーザが（手動でホストを追加するなどの）特定のアクションを実行したときに生成されるホスト入力イベントとは異なり、ディスカバリ イベントは、システムが、監視対象ネットワークで変更を検出したとき（以前は検出されなかったホストでトラフィックを検出した場合など）に生成されます。

ネットワーク検出ポリシーを変更して、システムが記録するホスト入力イベントのタイプを設定できます。

さまざまなタイプのホスト入力イベントが提示する情報を理解すると、どのイベントを記録およびアラートの対象にするか、相関ポリシーでこれらのアラートをどのように使用するかを効率よく判断できるようになります。また、イベント タイプの名前がわかると、より効率のよいイベント検索を作成するうえで役に立ちます。次に、ホスト入力イベントのさまざまなタイプについて説明します。

クライアントの追加（Add Client）

このイベントは、ユーザがクライアントを追加したときに生成されます。

ホストの追加（Add Host）

このイベントは、ユーザがホストを追加したときに生成されます。

プロトコルの追加（Add Protocol）

このイベントは、ユーザがプロトコルを追加したときに生成されます。

スキャン結果の追加（Add Scan Result）

このイベントは、システムが Nmap スキャンの結果をホストに追加したときに生成されます。

ポートの追加（Add Port）

このイベントは、ユーザがサーバ ポートを追加したときに生成されます。

クライアントの削除（Delete Client）

このイベントは、ユーザがシステムからクライアントを削除したときに生成されます。

ホスト/ネットワークの削除（Delete Host/Network）

このイベントは、ユーザがシステムから IP アドレスまたはサブネットを削除したときに生成されます。

プロトコルの削除（Delete Protocol）

このイベントは、ユーザがシステムからプロトコルを削除したときに生成されます。

ポートの削除（Delete Port）

このイベントは、ユーザがシステムからサーバ ポートまたはサーバ ポートのグループを削除したときに生成されます。

ホスト属性の追加（Host Attribute Add）

このイベントは、ユーザが新しいホスト属性を作成したときに生成されます。

ホスト属性の削除（Host Attribute Delete）

このイベントは、ユーザが、ユーザ定義のホスト属性を削除したときに生成されます。

ホスト属性値の削除（Host Attribute Delete Value）

このイベントは、ユーザが、ホスト属性に割り当てられている値を削除したときに生成されます。

ホスト属性値の設定（Host Attribute Set Value）

このイベントは、ユーザがホストに対してホスト属性値を設定したときに生成されます。

ホスト属性の更新（Host Attribute Update）

このイベントは、ユーザが、ユーザ定義のホスト属性の定義を変更したときに生成されます。

ホスト重要度の設定（Set Host Criticality）

このイベントは、ユーザがホストに対してホストの重要度の値を設定した、または変更したときに生成されます。

オペレーティング システム定義の設定（Set Operating System Definition）

このイベントは、ユーザがホストに対してオペレーティング システムを設定したときに生成されます。

サーバ定義の設定（Set Server Definition）

このイベントは、ユーザがサーバに対してベンダーおよびバージョンの定義を設定したときに生成されます。

脆弱性影響認定の設定（Set Vulnerability Impact Qualification）

このイベントは、脆弱性の影響の認定が設定されたときに生成されます。

脆弱性が、影響の認定に対する使用でグローバル レベルで無効になったとき、または脆弱性がグローバル レベルで有効になったときに、このイベントが生成されます。

脆弱性を無効に設定（Vulnerability Set Invalid）

このイベントは、ユーザが 1 つ以上の脆弱性を無効にした（または確認した）ときに生成されます。

脆弱性を有効に設定（Vulnerability Set Valid）

このイベントは、ユーザーが、以前に無効であるとマークされた脆弱性を有効にしたときに生成されます。

関連トピック

ディスカバリ イベント タイプ （1088 ページ）

ディスカバリ イベントとホスト入力イベントの表示

ディスカバリ イベント ワークフローでは、ディスカバリ イベントとホスト入力イベント両方からのデータを表示できます。ユーザーは検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザーがイベントにアクセスするときに表示されるページは、使用するワークフローによって異なります。ユーザは事前定義のワークフローを使用できますが、これにはディスカバリ イベントのテーブル ビューと、ホスト ビューの最終ページが含まれています。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 **[分析（Analysis）] > [ホスト（Hosts）] > [検出イベント（Discovery Events）]**を選択します。

ステップ 2 次の選択肢があります。

- 時間枠の変更 （833 ページ）の説明に従って、時間範囲を調整します。

（注） イベント ビューを時間によって制約している場合は、（グローバルかイベントに特有かに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあります。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （1085 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（ディスカバリ イベントのフィールド（1096 ページ）を参照）。

関連トピック

ディスカバリおよびアイデンティティ ワークフローの使用 （1085 ページ）

ディスカバリ イベントのフィールド

以下に、ディスカバリ イベント テーブルで表示および検索できるフィールドについて説明します。

時刻（Time）

システムがイベントを生成した時間。

イベント

ディスカバリ イベント タイプまたはホスト入力イベント タイプ。

[IPアドレス（IP Address）]

イベントに関連するホストに関連付けられている IP アドレス。

ユーザー（User）

イベントが生成される前に、イベントに関係するホストに最後にログインしたユーザ。権限のあるユーザの後に、権限のないユーザのみがログインした場合、権限のあるユーザが次にログインするまで、権限のあるユーザが現行のユーザとして保持されます。

[MAC アドレス（MAC Address）]

ディスカバリ イベントをトリガーとして使用したネットワーク トラフィックが使用する NIC の MAC アドレス。この MAC アドレスは、イベントに関連するホストの実際の MAC アドレスであるか、またはトラフィックが通過したネットワーク デバイスの MAC アドレスになります。

[MAC ベンダー（MAC Vendor）]

ディスカバリ イベントをトリガーとして使用したネットワーク トラフィックが使用する NIC の MAC ハードウェア ベンダー。

[ポート（Port）]

イベントをトリガーとして使用したトラフィックが使用するポート（該当する場合）。

説明

テキストによるイベントの説明。

ドメイン

ホストを検出したデバイスのドメイン。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

デバイス

イベントを生成した管理対象デバイスの名前。NetFlow データに基づいた新しいホストおよび新しいサーバーのイベントの場合、これはそのデータを処理した管理対象デバイスになります。

関連トピック

イベントの検索 （845 ページ）

ホスト データ

システムがホストを検出し、ホストプロファイルを作成するためにホストに関する情報を収集したときに、イベントが生成されます。Management Center Web インターフェイスを使用して、ホストを表示、検索、および削除できます。

ホストの表示中に、選択したホストに基づいてトラフィックのプロファイル、およびコンプライアンスのallowリストを作成できます。また、（ビジネスの重要度を設定する）ホストの重要度の値などのホスト属性をホストグループに割り当てることもできます。その後で、相関ルールおよびポリシーの中でこれらの重要度の値、allowリスト、およびトラフィックプロファイルを使用できます。

システムは、エクスポートされたNetFlow レコードからネットワークマップにホストを追加できますが、これらのホストに使用できる情報は限られます（NetFlow データと管理対象デバイス データの違いを参照）。

ホスト データの表示

Management Center を使用して、システムが検出したホストのテーブルを表示することができます。その後、探している情報に応じて表示方法を操作できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがホストにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローは両方ともホスト ビューで終了しますが、このホスト ビューには、ユーザーの制約を満たすすべてのホストのホスト プロファイルが含まれています。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 次のように、ホスト データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[分析（Analysis）] > [ホスト（Hosts）] > [ホスト（Hosts）]** を選択します。
- ホストのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [ホスト（Hosts）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （1085 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（ホスト データ フィールド （1098 ページ）を参照）。
- オプションを表示するには、テーブル内の項目を右クリックします（オプションが表示されない列もあります）。
- ホスト属性を特定のホストに割り当てます（選択したホストのホスト属性の設定（1107ページ）を参照）。
- 特定のホストのトラフィック プロファイルを作成します（選択したホストのトラフィック プロファイルの作成 （1103 ページ）を参照）。
- 特定のホストに基づいて、コンプライアンスの allow リストを作成します（選択したホストに基づいたコンプライアンスの許可（Allow）リストの作成（1104 ページ）を参照）。

ホスト データ フィールド

システムはホストを検出したときに、そのホストに関するデータを収集します。そのデータには、ホストの IP アドレス、ホストが実行しているオペレーティング システムなどが含めることが可能です。ユーザは、ホストのテーブル ビューでこれらの情報の一部を表示することができます。

ホスト テーブルで表示および検索できるフィールドの説明が続きます。

前回の検出（Last Seen）

システムによっていずれかのホストの IP アドレスが最後に検出された日付と時間。[前回の検出（Last Seen）] の値は、ホストの IP アドレスに対してシステムが新しいホスト イベントを生成したときだけでなく、少なくともユーザがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。

ホスト入力機能を使用して、オペレーティング システムのデータを更新しているホストでは、[前回の検出（Last Seen）] の値は、そのデータが最初に追加された日付と時間を表します。

[IPアドレス（IP Address）]

ホストに関連付けられている IP アドレス。

MAC アドレス（MAC Address）

ホストが検出した NIC の MAC アドレス。

[MAC アドレス（MAC Address）] フィールドは、[ホスト（Hosts）] ワークフローの [ホストのテーブル ビュー（Table View of Hosts）] に表示されます。以下のものに対して [MAC アドレス（MAC Address）] フィールドを追加できます。

- [ホスト（Hosts）] テーブルのフィールドが含まれているカスタム テーブル
- [ホスト（Hosts）] テーブルに基づいたカスタム ワークフローのドリルダウン ページ

MAC ベンダー（MAC Vendor）

ホストが検出した NIC の MAC ハードウェア ベンダー。

[MAC ベンダー（MAC Vendor）] フィールドは、[ホスト（Hosts）] ワークフローの [ホストのテーブル ビュー（Table View of Hosts）] に表示されます。以下のものに対して [MAC ベンダー（MAC Vendor）] フィールドを追加できます。

- [ホスト（Hosts）] テーブルのフィールドが含まれているカスタム テーブル
- [ホスト（Hosts）] テーブルに基づいたカスタム ワークフローのドリルダウン ページ

このフィールドを検索する場合は、`virtual_mac_vendor` を入力して、仮想ホストに関係するイベントを照合します。

現在のユーザー（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることができます。ただし、権限のあるユーザーがそのホストにログインした後は、別の権限のあるユーザーによるログインだけが現行ユーザーを変更します。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

ホストの重要度（Host Criticality）

ホストに割り当てられている、ユーザ指定の重要度の値。

NetBIOS 名（NetBIOS Name）

ホストのNetBIOS名。NetBIOSプロトコルを実行しているホストにのみ、NetBIOS名があります。

VLAN ID（Admin. VLAN ID）

ホストが使用する VLAN ID。

ホップ（Hops）

ホストを検出したデバイスからホストへのネットワークのホップ数。

ホスト タイプ（Host Type）

ホストのタイプ。ホスト、モバイル デバイス、jailbroken モバイル デバイス、ルータ、ブリッジ、NAT デバイス、ロード バランサのいずれかにできます。

ネットワーク デバイスを区別するためにシステムでは次の方法を使用します。

- Cisco Discovery Protocol（CDP）メッセージの分析。ネットワークのデバイスおよびそれらのタイプ（シスコ デバイスのみ）を特定できます。
- スパニング ツリー プロトコル（STP）の検出。デバイスをスイッチまたはブリッジとして識別します。
- 同じ MAC アドレスを使用している複数のホストの検出。MAC アドレスを、ルータに属しているものとして識別します。
- クライアント側からの TTL 値の変更、または通常のブート時間よりも頻繁に変更されている TTL 値の検出。この検出では、NAT デバイスとロード バランサを識別します。

デバイスがネットワーク デバイスとして識別されない場合は、ホストとして分類されます。

このフィールドを検索するときは、`!host` と入力してすべてのネットワーク デバイスを検索します。

ハードウェア（Hardware）

モバイル デバイスのハードウェア プラットフォーム。

OS

次のいずれかです。

- ホスト上で検出されたオペレーティング システム（名前、ベンダー、およびバージョン）、または Nmap かホスト入力機能を使用して更新されたオペレーティング システム。
- オペレーティング システムが既知のフィンガープリントに一致しない場合は `unknown`

- オペレーティング システムを識別するための十分な情報がシステムで収集されていない場合は pending

システムが複数のアイデンティティを検出した場合は、これらのアイデンティティはカンマ区切りリストで表示されます。

このフィールドは、ダッシュボード上で [カスタム分析（Custom Analysis）] ウィジェットからホスト イベント ビューを起動したときに表示されます。また、これは [ホスト（Hosts）] テーブルに基づいたカスタム テーブルのフィールド オプションです。

このフィールドを検索するときは、n/a と入力して、オペレーティング システムがまだ識別されていないホストを含めます。

OS 競合（OS Conflict）

このフィールドは検索専用です。

OS ベンダー（OS Vendor）

次のいずれかです。

- ホストで検出されたオペレーティング システムのベンダー、またはNmapかホスト入力機能を使用して更新されたオペレーティング システムのベンダー。
- オペレーティング システムが既知のフィンガープリントに一致しない場合は unknown
- オペレーティング システムを識別するための十分な情報がシステムで収集されていない場合は pending

システムが複数のベンダーを検出した場合は、これらのベンダーはカンマ区切りリストで表示されます。

このフィールドを検索するときは、n/a と入力して、オペレーティング システムがまだ識別されていないホストを含めます。

OS 名（OS Name）

次のいずれかです。

- ホスト上で検出されたオペレーティング システム、またはNmapかホスト入力機能を使用して更新されたオペレーティング システム。
- オペレーティング システムが既知のフィンガープリントに一致しない場合は unknown
- オペレーティング システムを識別するための十分な情報がシステムで収集されていない場合は pending

システムが複数の名前を検出した場合は、これらの名前はカンマ区切りリストで表示されます。

このフィールドを検索するときは、n/a と入力して、オペレーティング システムがまだ識別されていないホストを含めます。

OS バージョン（OS Version）

次のいずれかです。

- ホストで検出されたオペレーティング システムのバージョン、またはNmapかホスト入力機能を使用して更新されたオペレーティング システムのバージョン。
- オペレーティング システムが既知のフィンガープリントに一致しない場合は `unknown`
- オペレーティング システムを識別するための十分な情報がシステムで収集されていない場合は `pending`

システムが複数のバージョンを検出した場合は、これらのバージョンはカンマ区切りリストで表示されます。

このフィールドを検索するときは、`n/a` と入力して、オペレーティング システムがまだ識別されていないホストを含めます。

ソース タイプ（Source Type）

ホストのオペレーティング システムのアイデンティティを確立するために使用されるソースのタイプは次のとおりです。

- [ユーザ（User）]：user_name
- [アプリケーション（Application）]：app_name
- スキャナ：scanner_type（ネットワーク検出の設定を介して追加されたNmapまたはスキャナ）
- システムによって検出されたオペレーティング システムの場合は `Firepower`

システムでは、オペレーティング システムのアイデンティティを判断するために、複数のソースのデータを統合することができます。

信頼性（Confidence）

次のいずれかです。

- システムで検出されたホストについて、ホスト上で稼動しているオペレーティング システムのアイデンティティ内にシステムが保持している信頼度（パーセンテージ）。
- 100%（ホスト入力機能やNmapスキャナなどのアクティブなソースによって識別されたオペレーティング システムの場合）。
- `unknown`（システムがオペレーティング システムのアイデンティティを特定できないホスト、およびNetFlowデータに基づいてネットワーク マップに追加されたホストの場合）。

このフィールドを検索するときは、`n/a` と入力して、NetFlow データに基づいてネットワーク マップに追加されたホストを含めます。

注記（Notes）

[注記（Notes）] ホスト属性の、ユーザ定義のコンテンツ。

ドメイン（Domain）

ホストに関連付けられているドメイン。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

デバイス

トラフィックを検出した管理対象デバイスか、NetFlow またはホスト入力データを処理したデバイスのいずれか。

このフィールドが空白の場合は、次のいずれかの条件を満たします。

- ホストがデバイスによってネットワークマップに追加されたが、このデバイスは、ホストが存在しているネットワークに対してネットワーク検出ポリシーに定義されているとおりに明示的に監視していない。
- ホストの入力機能を使用してホストが追加されたが、システムによって検出されていない。

カウント（Count）

各行に表示される情報と一致するイベントの数。このフィールドが表示されるのは、2 つ以上の同一の行を作成する制限を適用した後のみです。

関連トピック

イベントの検索 （845 ページ）
オペレーティング システムのアイデンティティの競合 （1057 ページ）

選択したホストのトラフィック プロファイルの作成

トラフィック プロファイルは、指定した期間に収集された接続データに基づいた、ネットワーク上のトラフィックのプロファイルです。トラフィック プロファイルを作成した後、正常なネットワーク トラフィックを表すと想定されるプロファイルに照らして新しいトラフィックを評価することにより、異常なネットワーク トラフィックを検出できます。

[ホスト（Hosts）] ページを使用して、指定するホスト グループのトラフィック プロファイルを作成できます。トラフィック プロファイルは、指定したホストのいずれかが発信元ホストである、検出された接続に基づいています。ソートおよび検索機能を使用して、プロファイルを作成するホストを分離することができます。

始める前に

このタスクを実行するには、管理者ユーザーである必要があります。

手順

ステップ 1 ホスト ワークフローのテーブル ビューで、トラフィック プロファイルを作成するホストの隣にあるチェック ボックスをオンにします。

ステップ 2 ページの下部で [トラフィック プロファイルの作成（Create Traffic Profile）] をクリックします。

ステップ 3 特別なニーズに応じて、トラフィック プロファイルを変更し、保存します。

関連トピック

トラフィック プロファイルの概要 （1235 ページ）

選択したホストに基づいたコンプライアンスの許可（Allow）リストの作成

コンプライアンスのallowリストでは、ネットワーク上で許可されるオペレーティングシステム、クライアント、ネットワーク、トランスポート、またはアプリケーションプロトコルを指定することができます。

[ホスト（Hosts）]ページを使用して、ユーザーが指定するホストグループのホストプロファイルに基づいて、コンプライアンスのallowリストを作成することができます。ソートおよび検索機能を使用して、allowリストの作成に使用するホストを分離することができます。

始める前に

このタスクを実行するには、管理者ユーザーである必要があります。

手順

ステップ 1 ホストワークフローのテーブルビューで、allowリストを作成するホストの隣にあるチェックボックスをオンにします。

ステップ 2 ページの下部で [**許可リスト（Allow List**）の作成（Create White List）] をクリックします。

ステップ 3 特別なニーズに応じて、allowリストを変更し、保存します。

関連トピック

コンプライアンス許可（Allow）リストの概要 （1169 ページ）

ホスト属性データ

システムは、検出したホストに関する情報を収集し、その情報を使用してホストプロファイルを作成します。ただし、ネットワーク上のホストについて、アナリストに提供する追加情報が存在する場合があります。ユーザは、ホストプロファイルにメモを追加する、ホストのビジネス重要度を設定する、選択する他の情報を提供する、といったことが可能です。それぞれの情報は、ホスト属性と呼ばれます。

ホストプロファイルの認定でホスト属性を使用することができます。これにより、トラフィックプロファイルの作成中に収集するデータを制約し、相関ルールをトリガーする条件を制限することができます。相関ルールに応じて属性値を設定することもできます。

関連トピック

ホスト属性の表示 （1105 ページ）
セット属性修復の設定 （1259 ページ）

ホスト属性の表示

Management Center を使用して、システムで検出されたホストのテーブル、およびそのホスト属性を表示することができます。その後、探している情報に応じて表示方法を操作できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがホスト属性にアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフロー（検出されたすべてのホスト、およびそのホストの属性が記載されているホスト属性のテーブル ビューが含まれており、ホスト ビュー ページで終了するワークフロー）を使用することができます。このワークフローには、制約を満たすすべてのホストについて 1 つのホスト プロファイルが含まれています。

また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 次のように、ホスト属性データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[分析（Analysis）]** > **[ホスト（Hosts）]** > **[ホスト属性（Host Attributes）]** を選択します。
- ホスト属性のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [属性（Attributes）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （1085 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（ホスト属性データ フィールド （1106 ページ）を参照）。
- ホスト属性を特定のホストに割り当てます（選択したホストのホスト属性の設定 （1107ページ）を参照）。

ホスト属性データ フィールド

ホスト属性テーブルには、MAC アドレスでのみ識別されるホストは表示されないことに注意してください。

ホスト属性テーブルで表示および検索できるフィールドの説明が続きます。

[IPアドレス（IP Address）]

ホストに関連付けられている IP アドレス。

現在のユーザー（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることができます。ただし、権限のあるユーザーがそのホストにログインした後は、別の権限のあるユーザーによるログインだけが現行ユーザーを変更します。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

ホストの重要度（Host Criticality）

ユーザが割り当てた、企業にとってのホストの重要度。ホストの重要度を相関ルールおよびポリシーで使用して、イベントに関するホストの重要度に対して、ポリシー違反および違反の応答を作成することができます。ホストの重要度に[低（Low）]、[中（Medium）]、[高（High）]、または [なし（None）] を割り当てることができます。

注記（Notes）

他のアナリストに提示する、ホストに関する情報。

コンプライアンス allow リストの属性を含む、ユーザー定義のホスト属性（Any user-defined host attribute, including those for compliance allow lists）

ユーザー定義のホスト属性の値。ホスト属性テーブルには、ユーザ定義のそれぞれのホスト属性のフィールドが含まれています。

ドメイン（Domain）

ホストに関連付けられているドメイン。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

カウント（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

関連トピック

イベントの検索 （845 ページ）

選択したホストのホスト属性の設定

ホストワークフローから、事前定義済のホスト属性とユーザー定義のホスト属性を設定できます。

手順

ステップ 1 ホストワークフローで、ホスト属性を追加するホストの横にあるチェックボックスをオンにします。

ヒント ソート機能と検索機能を使用して、特別な属性を割り当てるホストを分離することができます。

ステップ 2 ページの下部にある [属性の設定（Set Attributes）] をクリックします。

ステップ 3 必要に応じて、選択したホストに対してホストの重要度を設定します。[なし（None）]、[低（Low）]、[中（Medium）]、または [高（High）] を選択できます。

ステップ 4 必要に応じて、テキスト ボックスで、選択したホストのホスト プロファイルにメモを追加します。

ステップ 5 必要に応じて、自分で設定したユーザ定義のホストの属性を設定します。

ステップ 6 [保存（Save）] をクリックします。

侵害の兆候データ

システムは、モニタリング対象のネットワーク上でホストが悪意のある手段によって侵害されている可能性があるかどうかを判断するために、ホストに関連付けられているさまざまなタイプのデータ（侵入イベント、セキュリティインテリジェンス、接続イベント、ファイルまたはマルウェアイベント）との関連性を示します。イベントデータの特定の組み合わせと頻度は、影響を受けたホストの侵害の痕跡（IOC）タグをトリガーとして使用します。このようなホストのIPアドレスは**侵害を受けているホストの赤いアイコン**でイベントビューに表示されます。

ホストが侵害されている可能性があると識別された場合、その侵害に関連付けられているユーザにもタグが付けられます。そのようなユーザーは、**赤色のユーザーアイコン**でイベントビューに表示されます。

マルウェアが含まれているファイルが300秒以内にIOCというタグが付けられて再度表示される場合は、別のIOCは生成されません。同じファイルが300秒以上経ってから表示された場合は、新しいIOCが生成されます。

侵害の兆候としてイベントにタグを付けるように設定するには、Cisco Secure Firewall Management Centerデバイス構成ガイドの「Enabling Indications of Compromise Rules」を参照してください。

関連トピック

サーバーのアイデンティティの編集 （1061 ページ）

侵害兆候データの表示と処理

Management Center を使用して、侵害の兆候（IOC）を示すテーブルを表示できます。検索する情報に応じてイベント ビューを操作します。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

表示されるページは、使用するワークフローによって異なります。事前定義の IOC ワークフローはプロファイル ビューで終了しますが、これには、制約を満たすすべてのホストまたはユーザのホストプロファイルまたはユーザプロファイルが含まれています。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

始める前に

- システムで侵害の兆候（IOC）を検出してタグを付けるには、ネットワーク検出ポリシーの IOC 機能をアクティブにして、少なくとも 1 つの IOC ルールを有効にする必要があります。『Cisco Secure Firewall Management Center デバイス構成ガイド』の「侵害の兆候ルールの有効化」を参照してください。
- アクティブなアイデンティティ ポリシーでユーザーが認識される必要があります。

手順

ステップ 1 Web インターフェイスのどの場所のニーズを満たす情報があるかを特定します。

侵害兆候データを表示または処理するには、次の場所を使用できます。

- イベントビューア（[分析（Analysis）] メニューの下）：接続、セキュリティ インテリジェンス、侵入、マルウェアや IOC 検出のイベントビューでそのイベントが IOC をトリガーしたかどうかを表示します。IOC ルールをトリガーする、Secure Endpoint によって生成されたマルウェアイベントは、イベントタイプが `AMP IOC` であり、侵害を指定するイベントサブタイプと一緒に表示されることに注意してください。
- ダッシュボード：ダッシュボードでは、サマリーダッシュボードの [脅威（Threats）] に、ホスト別とユーザー別の IOC タグがデフォルトで表示されます。カスタム分析ウィジェットは IOC データに基づくプリセットを提供します。
- コンテキスト エクスプローラ：コンテキスト エクスプローラの [侵害の兆候（Indications of Compromise）] セクションに、IOC カテゴリ別のホストとホスト別の IOC カテゴリのグラフが表示されます。
- [ネットワークマップ（Network Map）] ページ：[分析（Analysis）] > [ホスト（Hosts）] > [ネットワークマップ（Network Map）] にある [侵害の兆候（Indications of Compromise）] には、侵害されている可能性があるネットワーク上のホストが侵害のタイプと IP アドレス別にグループ分けして示されます。

- [ネットワーク ファイル トラジェクトリ（Network File Trajectory）] 詳細ページ：[分析（Analysis）] > [ファイル（Files）] > [ネットワーク ファイル トラジェクトリ（Network File Trajectory）] の下に一覧表示されているファイルの詳細ページでは、ネットワークの侵害の兆候を追跡できます。
- [ホストの侵害の兆候（Host Indications of Compromise）] ページ：[分析（Analysis）] > [ホスト（Hosts）] メニューの下の [ホストの侵害の兆候（Host Indications of Compromise）] ページには、モニタ対象ホストの一覧がIOCタグ別にグループ分けされて表示されます。このページのワークフローを使ってデータをドリルダウンできます。
- [ユーザの侵害の兆候（User Indications of Compromise）] ページ：[分析（Analysis）] > [ユーザ（Users）] メニューの下の [ユーザの侵害の兆候（User Indications of Compromise）] ページには、IOCの可能性があるイベントに関連付けられているユーザの一覧がIOCタグ別にグループ分けされて表示されます。このページのワークフローを使ってデータをドリルダウンできます。
- ホスト プロファイル ページ：侵害されている可能性があるホストのホスト プロファイルには、そのホストに関連付けられているすべてのIOCタグが表示され、IOCタグの解決とIOC ルール状態の設定ができます。
- ユーザ プロファイル ページ：IOC の可能性があるイベントに関連付けられているユーザのユーザ プロファイルには、そのユーザに関連付けられているすべての IOC タグが表示され、IOC タグの解決と IOC ルール状態の設定ができます（Management Center の Web インターフェイスでは、ユーザープロファイルは「ユーザーアイデンティティ（User Identity）」とラベルが付けられています）。

ステップ 2 必要に応じて、次のうちのいずれかを実行し、この手順の残りのステップを使用します。

オプション	説明
ホストのIOCを調べるには、以下を実行します。	• 事前定義されたワークフローを使用する場合、**[分析（Analysis）] > [ホスト（Hosts）] > [侵害の兆候（Indications of Compromise）]** を選択します。 • ホスト IOC のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [ホストの侵害の兆候（Host Indications of Compromise）] を選択します。
ユーザに関連付けられているIOCを調べるには、以下を実行します。	• 事前定義されたワークフローを使用する場合、[分析（Analysis）] > [ユーザ（Users）] > [侵害の兆候（Indications of Compromis）] を選択します。 • ユーザ IOC のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [ユーザの侵害の兆候（User Indications of Compromise）] を選択します。

ステップ 3 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （1085 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（侵害の兆候データ フィールド （1110 ページ）を参照）。
- [ホストの侵害の兆候（Host Indications of Compromise）] ページ：[IPアドレス（IP Address）] 列にある [侵害を受けたホスト（Compromised Host）] をクリックして、侵害を受けたホストのホストプロファイルを表示します。
- [ユーザーの侵害の兆候（User Indications of Compromise）]：[ユーザー（User）] 列の [赤色のユーザー（Red User）] をクリックして、侵害に関連付けられているユーザープロファイルを表示します。
- IOC イベントに解決済みとマークして、リストに表示されないようにします。これを実行するには、編集する IOC イベントの横にあるチェック ボックスをオンにして、[解決済みとマークを付ける（Mark Resolved）] をクリックします。
- [最初の確認日時（First Seen）] または [前回の検出（Last Seen）] 列にある[表示（View）]（  ）をクリックして、IOC をトリガーしたイベントの詳細を表示します。
- その他のオプションを表示するには、テーブル内の値を右クリックします。

侵害の兆候データ フィールド

以下は、ホストまたはユーザの IOC（侵害の兆候）テーブル内のフィールドです。すべての IOC 関連のテーブルにすべてのフィールドが含まれているわけではありません。

IP アドレス（IP Address）（ホストの IOC データを表示する場合）

IOC をトリガーとして使用したホストに関連付けられている IP アドレス。

ユーザ（User）（ユーザの IOC データを表示する場合）

IOC をトリガーしたイベントに関連付けられているユーザのユーザ名、レルム、および認証ソース。

カテゴリ

`Malware Executed` や `Impact 1 Attack` など、示された侵害のタイプの簡単な説明。

イベントタイプ

特定の IOC に関連付けられている識別子で、トリガーとして使用したイベントを参照します。

説明

侵害される可能性のあるホストへの影響の説明（[このホストはリモート制御下にある可能性があります（This host may be under remote control）] や [このホスト上でマルウェアが実行されました（Malware has been executed on this host）] など）。

最初の確認日時/最新の確認日時（First Seen/Last Seen）

IOC をトリガーとして使用したイベントが発生した最初（または最新）の日付と時刻。

ドメイン（Domain）

IOC をトリガーとして使用したホストのドメイン。このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

関連トピック

イベントの検索 （845 ページ）

単一ホストまたはユーザにおける侵害の兆候のルール状態の編集

ネットワーク検出ポリシーで有効になっている場合、侵害の兆候ルールは監視対象ネットワーク内のすべてのホストと、そのネットワーク上の IOC イベントに関連付けられている権限のあるユーザーに適用されます。個々のホストまたはユーザのルールを無効にして、無用な IOC タグを回避できます（たとえば、DNS サーバに対する IOC タグが表示されないようにできます）。適用可能なネットワーク検出ポリシーでルールを無効にすると、特定のホストまたはユーザに対して有効にすることができません。特定のホストに対してルールを無効にしても、同じイベントに関与するユーザーのタグ付けには影響がなく、その逆もまた同じです。

手順

ステップ 1 ホストまたはユーザ プロファイルの [侵害の兆候（Indications of Compromise）] セクションに移動します。

ステップ 2 [ルール状態の編集（Edit Rule States）] をクリックします。

ステップ 3 ルールの [有効（Enabled）] 列で、スライダをクリックしてこれを有効または無効にします。

ステップ 4 [保存（Save）] をクリックします。

侵害の兆候のタグのソース イベントの表示

ホスト プロファイルやユーザー プロファイルの [侵害の兆候（Indications of Compromise）] セクションを使用して、IOC タグをトリガーしたイベントにすばやく移動することができます。これらのイベントを分析すると、侵害される脅威に対処するのに必要なアクション、およびアクションが必要かどうかを判断するための情報が提供されます。

IOC タグのタイムスタンプの隣の[表示（View）]（）をクリックすると、関連するイベントタイプのイベントのテーブルビューに移動します。ここでは、IOC タグをトリガーしたイベントのみが表示されます。

ユーザー IOC の最初のインスタンスのみが Management Center に表示されます。後続のインスタンスは DNS サーバによって捕捉されます。

手順

ステップ 1 ホストまたはユーザープロファイルで、[侵害の兆候（Indications of Compromise）] セクションに移動します。

ステップ 2 調べたい IOC タグの [最初の痕跡（First Seen）] または [最後の痕跡（Last Seen）] 列にある[表示（View）]（）をクリックします。

侵害の兆候タグの解決

侵害の兆候（IOC）タグで示された脅威が分析および対処された後、または IOC タグが誤検出を示していると判断した場合、イベントに解決済みのマークを付けることができます。イベントに解決済みのマークを付けると、そのイベントはホストプロファイルおよびユーザープロファイルから削除されます。プロファイル上のアクティブな IOC タグがすべて解決されると、**侵害されたホスト** またはユーザーが侵害の兆候に関連付けられていることを示す**赤色のユーザーアイコン** は表示されなくなります。解決した IOC についても、IOC のトリガー元であるイベントは引き続き表示できます。

IOC タグをトリガーしたイベントが繰り返された場合、ホストまたはユーザに対する IOC ルールが無効にされていない限り、このタグが再び設定されます。

手順

ステップ 1 ホストまたはユーザ プロファイルで、[侵害の兆候（Indications of Compromise）] セクションに移動します。

ステップ 2 次の 2 つの選択肢があります。

- 個別の IOC タグに解決済みとマークするには、解決するタグの右にある [削除（Delete）]（） をクリックします。
- プロファイル上のすべての IOC タグに解決済みのマークを付けるには、[すべてに解決済みのマークを付ける（Mark All Resolved）] をクリックします。

サーバー データ

システムは、モニター対象ネットワークセグメント上のホストで稼動しているすべてのサーバーに関する情報を収集します。この情報には次のものが含まれます。

- サーバの名前
- サーバが使用するアプリケーションとネットワーク プロトコル
- サーバのベンダーとバージョン
- サーバを実行しているホストに関連付けられている IP アドレス
- サーバが通信するポート

システムはサーバを検出すると、関連するホストがまだサーバの最大数に達していない場合は、ディスカバリ イベントを生成します。Management Center の Web インターフェイスを使用して、サーバ イベントを表示、検索、削除できます。

また、サーバイベントを相関ルールのベースにすることもできます。たとえばシステムが、いずれかのホスト上で稼働している ircd などのチャット サーバーを検出したときに相関ルールをトリガーできます。

システムは、エクスポートされた NetFlow レコードからネットワークマップにホストを追加できますが、これらのホストに使用できる情報は限られます（NetFlow データと管理対象デバイス データの違いを参照）。

サーバー データの表示

Management Center を使用して、検出されたサーバーのテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがサーバにアクセスしたときに表示されるページは、使用するワークフローによって異なります。事前定義のすべてのワークフローはホスト ビューで終了しますが、このホスト ビューには、制約を満たすすべてのホストに対して 1 つずつホスト プロファイルが含まれています。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 次のように、サーバ データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[分析（Analysis）]** > **[ホスト（Hosts）]** > **[サーバー（Servers）]** を選択します。
- サーバのテーブル ビューが含まれていないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [サーバ（Servers）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （1085 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（サーバーデータ フィールド（1114ページ）を参照）。
- 編集するサーバーのイベントの横にあるチェック ボックスをオンにし、[サーバー アイデンティティの設定（Set Server Identity）] をクリックすることによって、サーバーのアイデンティティを編集します。
- オプションを表示するには、テーブル内の項目を右クリックします（オプションが表示されない列もあります）。

サーバー データ フィールド

サーバ テーブルで表示および検索できるフィールドの説明は次のとおりです。

前回の使用（Last Used）

ネットワーク上でサーバが最後に使用された日付と時間、またはホスト入力機能を使用してサーバが最初に更新された日付と時間。[前回の使用（Last Used）] の値は、システムがサーバ情報の更新を検出したときだけでなく、少なくともユーザがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。

[IPアドレス（IP Address）]

サーバを実行しているホストに関連付けられている IP アドレス。

ポート

サーバが稼動しているポート。

プロトコル

サーバが使用するネットワークまたはトランスポート プロトコル。

アプリケーション プロトコル（Application Protocol）

次のいずれかです。

- サーバのアプリケーション プロトコルの名前
- `pending`：システムで、いずれかの理由でサーバをポジティブまたはネガティブに識別できない場合

- unknown：既知のサーバ フィンガープリントに基づいてシステムでサーバを識別できない場合、またはホストの入力を介してサーバが追加され、アプリケーションプロトコルが含まれていなかった場合

アプリケーションプロトコルのカテゴリ、タグ、リスク、またはビジネスとの関連性（Category, Tags, Risk, or Business Relevance for Application Protocols）

アプリケーション プロトコルに割り当てられているカテゴリ、タグ、リスク レベル、およびビジネスとの関連性。これらのフィルタを使用して、特定のデータ セットを対象にすることができます。

ベンダー（Vendor）

次のいずれかです。

- サーバのベンダー：システム、Nmap、その他のアクティブなソースで識別された、またはホスト入力機能を使用して指定されたサーバのベンダー
- 空白：システムが既知のサーバフィンガープリントに基づいてベンダーを識別できなかった場合、またはNetFlowデータを使用してサーバがネットワーク マップに追加された場合

バージョン（Version）

次のいずれかです。

- サーバのバージョン：システム、Nmap、その他のアクティブなソースで識別された、またはホスト入力機能を使用して指定されたサーバのバージョン
- 空白：システムが既知のサーバ フィンガープリントに基づいてバージョンを識別できなかった場合、またはNetFlowデータを使用してサーバがネットワーク マップに追加された場合

Web アプリケーション（Web Application）

HTTP トラフィックでシステムが検出したペイロード コンテンツに基づいた Web アプリケーション。システムが HTTP のアプリケーション プロトコルを検出したものの、特定の Web アプリケーションを検出できない場合は、一般的な Web ブラウジングの指定が提示されるので注意してください。

Web アプリケーションのカテゴリ、タグ、リスク、またはビジネスとの関連性（Category, Tags, Risk, or Business Relevance for Web Applications）

Web アプリケーションに割り当てられているカテゴリ、タグ、リスク レベル、およびビジネスとの関連性。これらのフィルタを使用して、特定のデータ セットを対象にすることができます。

ヒット数（Hits）

サーバがアクセスされた回数。ホスト入力機能を使用して追加されたサーバの場合、この値は必ず 0 になります。

ソース タイプ（Source Type）

次の値のいずれかを指定します。

- [ユーザ（User）]：user_name
- [アプリケーション（Application）]：app_name
- スキャナ：scanner_type（ネットワーク検出の設定を介して追加された Nmap またはスキャナ）
- システムによって検出されたサーバーの `Firepower`、`Firepower Port Match`、または `Firepower Pattern Match`
- NetFlow データを使用して追加されたサーバの `NetFlow`

ドメイン（Domain）

サーバーを実行しているホストのドメイン。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

デバイス

トラフィックを検出した管理対象デバイスか、NetFlow またはホスト入力データを処理したデバイスのいずれか。

現在のユーザー（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザーがホストにログインすると、そのログインはユーザーおよびホストの履歴に記録されます。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることができます。ただし、権限のあるユーザーがそのホストにログインした後は、別の権限のあるユーザーによるログインだけが現行ユーザーを変更します。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

カウント（Count）

各行に表示される情報と一致するイベントの数。このフィールドが表示されるのは、2 つ以上の同一の行を作成する制限を適用した後のみです。

関連トピック

イベントの検索 （845 ページ）

アプリケーション データとアプリケーション詳細データ

監視対象ホストが別のホストに接続すると、システムは多くの場合、どのアプリケーションが使用されたかを判断することができます。システムは、電子メール、インスタントメッセージ、ピアツーピア、Webアプリケーション、およびその他のタイプのアプリケーションが多用されると検出します。

検出されたそれぞれのアプリケーションに対してシステムは、アプリケーションを使用したIPアドレス、製品、バージョン、および使用が検出された回数を記録します。Webインターフェイスを使用して、アプリケーションイベントを表示、検索、および削除できます。ホスト入力機能を使用して、1つ以上のホスト上のアプリケーションデータを更新することもできます。

どのアプリケーションがどのホストで稼動しているかがわかっている場合は、その情報をもとにホスト プロファイルの認定を作成し、この認定によって、トラフィック プロファイルの作成中に収集するデータを制約することができます。また、相関ルールをトリガーする条件を制約することもできます。また、アプリケーションの検出を相関ルールのベースにすることもできます。たとえば、従業員に特定のメールクライアントを使用させたい場合は、システムが、いずれかの対象ホストで別のメール クライアントが稼動していることを検出したときに相関ルールをトリガーすることができます。

アプリケーションディテクタに関する最新情報は、各システム更新のリリースノート、各VDB更新のアドバイザリをよくご確認ください。

分析用にアプリケーションデータを収集および保存するには、ネットワーク検出ポリシーでアプリケーションの検出が有効になっていることを確認します。

アプリケーション データの表示

Management Center を使用して、検出されたアプリケーションのテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがアプリケーションにアクセスするときに表示されるページは、使用するワークフローによって異なります。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 次のようにして、アプリケーション データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[分析（Analysis）]** > **[ホスト（Hosts）]** > **[アプリケーション詳細（Application Details）]** を選択します。
- アプリケーションの詳細のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [クライアント（Clients）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （1085 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（アプリケーション データ フィールド（1118 ページ）を参照）。
- クライアント、アプリケーションプロトコル、Web アプリケーションの横にある [アプリケーション詳細ビュー（Application Detail View）] をクリックすることによって、特定のアプリケーションの [アプリケーション詳細ビュー（Application Detail View）] を開きます。
- イベント値を右クリックして、システムの外部にあるソース内のデータを表示します。表示されるオプションはデータ タイプによって異なり、パブリック ソースが含まれます。他のソースは設定したリソースによって異なります。詳細については、Web ベースのリソースを使用したイベントの調査 （763 ページ）を参照してください。
- テーブルでイベントの値を右クリックしてシスコまたはサードパーティのインテリジェンス ソースを選択して、イベントに関するインテリジェンスを収集します。たとえば、不審な IP アドレスに関する詳細情報を Cisco Talos から入手できます。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。詳細については、Web ベースのリソースを使用したイベントの調査 （763 ページ）を参照してください。

アプリケーション データ フィールド

システムは、既知のクライアント、アプリケーションプロトコル、またはWebアプリケーションについてトラフィックを検出すると、アプリケーションおよびそのアプリケーションを実行しているホストに関する情報をログに記録します。

次に、アプリケーション テーブルで表示および検索できるフィールドについて説明します。

Application

検出されたアプリケーションの名前。

IP アドレス

アプリケーションを使用しているホストに関連付けられている IP アドレス。

タイプ（Type）

アプリケーションのタイプであり、次のものがあります。

アプリケーション プロトコル（Application Protocols）

ホスト間の通信を意味します。

クライアント アプリケーション

ホスト上で動作しているソフトウェアを意味します。

Web アプリケーション（Web Applications）

HTTP トラフィックの内容や要求された URL を意味します。

カテゴリ

アプリケーションの最も不可欠な機能を表す一般的な分類。各アプリケーションは、少なくとも 1 つのカテゴリに属します。

タグ

アプリケーションに関する追加情報。アプリケーションには任意の数のタグを付けることができます（タグなしも可能）。

リスク（Risk）

アプリケーションが組織のセキュリティポリシーに違反することがある目的で使用される可能性。アプリケーションのリスクの範囲は、[極めて低（Very Low）] から [極めて高（Very High）] までです。

侵入イベントをトリガーしたトラフィックで検出される Application Protocol Risk、Client Risk、Web Application Risk の 3 つ（存在する場合）の中で最も高いものとなります。

ビジネスとの関連性（Business Relevance）

アプリケーションが、娯楽目的ではなく、組織のビジネス活動の範囲内で使用される可能性。アプリケーションのビジネスとの関連性の範囲は、[極めて低（Very Low）] から [極めて高（Very High）] までです。

侵入イベントをトリガーしたトラフィックで検出される Application Protocol Business Relevance、Client Business Relevance、Web Application Business Relevance の 3 つ（存在する場合）の中で最も低いものとなります。

現在のユーザー（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることができます。ただし、権限のあるユーザーがそのホストにログインした後は、別の権限のあるユーザーによるログインだけが現行ユーザーを変更します。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

ドメイン（Domain）

アプリケーションを使用しているホストのドメイン。このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

カウント（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

関連トピック

イベントの検索 （845 ページ）

アプリケーション詳細データの表示

Management Center を使用して、検出されたアプリケーションの詳細テーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがアプリケーションの詳細にアクセスするときに表示されるページは、使用するワークフローによって異なります。2つの事前定義されたワークフローがあります。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 次のようにして、アプリケーション詳細データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[分析（Analysis）] > [ホスト（Hosts）] > [アプリケーション詳細（Application Details）]** を選択します。
- アプリケーションの詳細のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [クライアント（Clients）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （1085 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（アプリケーションの詳細データ フィールド （1121 ページ）を参照）。
- クライアントの横にある [アプリケーション詳細ビュー（Application Detail View）] をクリックして、特定のアプリケーションの [アプリケーション詳細ビュー（Application Detail View）] を開きます。
- イベント値を右クリックして、システムの外部で利用可能なソース内のデータを表示します。表示されるオプションはデータ タイプによって異なり、パブリック ソースが含まれ

ます。他のソースは設定したリソースによって異なります。詳細については、Webベースのリソースを使用したイベントの調査 （763 ページ）を参照してください。

- テーブルでイベントの値を右クリックしてシスコまたはサードパーティのインテリジェンス ソースを選択して、イベントに関するインテリジェンスを収集します。たとえば、不審な IP アドレスに関する詳細情報を Cisco Talos から入手できます。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。詳細については、Web ベースのリソースを使用したイベントの調査 （763 ページ）を参照してください。

アプリケーションの詳細データ フィールド

システムは、既知のクライアント、アプリケーションプロトコル、またはWebアプリケーションについてトラフィックを検出すると、アプリケーションおよびそのアプリケーションを実行しているホストに関する情報をログに記録します。

次に、アプリケーションの詳細テーブルで表示および検索できるフィールドについて説明します。

前回の使用（Last Used）

アプリケーションが前回使用された時間、またはホスト入力機能を使用してアプリケーションデータが更新された時間。[前回の使用（Last Used）]の値は、システムがアプリケーション情報の更新を検出したときだけでなく、少なくともユーザがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。

IP アドレス

アプリケーションを使用しているホストに関連付けられている IP アドレス。

クライアント（Client）

アプリケーションの名前。ただし、システムがアプリケーションプロトコルを検出したにも関わらず特定のクライアントを検出できなかった場合は、アプリケーション プロトコル名に `client` が付加されて一般名が表示されます。

バージョン（Version）

アプリケーションのバージョン。

クライアント、アプリケーション プロトコル、および Web アプリケーションのカテゴリ、タグ、リスク、またはビジネスとの関係性（Category, Tags, Risk, or Business Relevance for Clients, Application Protocols, and Web Applications）

アプリケーションに割り当てられているカテゴリ、タグ、リスク レベル、およびビジネスとの関連性。これらのフィルタを使用して、特定のデータ セットを対象にすることができます。

アプリケーション プロトコル（Application Protocol）

アプリケーションで使用されるアプリケーションプロトコル。ただし、システムがアプリケーションプロトコルを検出したにも関わらず特定のクライアントを検出できなかった場合は、アプリケーション プロトコル名に `client` が付加されて一般名が表示されます。

Web アプリケーション（Web Application）

HTTP トラフィックでシステムが検出したペイロード コンテンツまたは URL に基づく Web アプリケーション。ただし、HTTP のアプリケーションプロトコルが検出されたにも関わらず特定の Web アプリケーションを検出できない場合、ここには、標準の Web 閲覧先が表示されます。

ヒット数（Hits）

システムが使用中のアプリケーションを検出した回数。ホスト入力機能を使用して追加されたアプリケーションの場合、この値は常に `0` になります。

ドメイン（Domain）

アプリケーションを使用しているホストのドメイン。このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

デバイス

アプリケーションの詳細が含まれている検出イベントを生成したデバイス。

現在のユーザー（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることができます。ただし、権限のあるユーザーがそのホストにログインした後は、別の権限のあるユーザーによるログインだけが現行ユーザーを変更します。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

カウント（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

関連トピック

イベントの検索 （845 ページ）

脆弱性データ

システムには、独自の脆弱性追跡データベースが含まれています。これはシステムのフィンガープリンティング機能と組み合わせて使用して、ネットワーク上のホストに関連付けられている脆弱性を特定します。ホストで稼動しているオペレーティングシステム、サーバ、およびクライアントには、関連付けられている異なる脆弱性一式があります。

Management Center を使用して次のことを行えます。

- ホストごとの脆弱性を追跡および確認できます。
- ホストにパッチを適用した後、またはホストが脆弱性に影響されないと判断した場合は、そのホストの脆弱性を非アクティブにすることができます。

サーバで使用されるアプリケーション プロトコルが Management Center 構成内でマップされない限り、ベンダーレスおよびバージョンレスのサーバの脆弱性はマップされません。ベンダーレスおよびバージョンレスのクライアントの脆弱性はマップできません。

関連トピック

サーバの脆弱性のマッピング （130 ページ）

脆弱性データのフィールド

注記がある場合を除き、これらのフィールドは、[分析（Analysis）] > [ホスト（Hosts）] > [脆弱性（Vulnerabilities）] の下のすべてのページに表示されます。

カウント（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

CVE ID

MITRE の Common Vulnerabilities and Exposures（CVE）データベース（https://cve.mitre.org/）の脆弱性に関連付けられた識別番号。

National Vulnerability Database（NVD）でこの脆弱性の詳細を表示するには、CVE ID を右クリックし、[NVDで説明を表示する（View description in NVD）] を選択します。

発行日（Date Published）

脆弱性が公開された日付。

説明

National Vulnerability Database（NVD）からの脆弱性の簡単な説明。

完全な説明については、CVE ID を右クリックし、[NVDで説明を表示する（View description in NVD）] を選択して、National Vulnerability Database（NVD）の詳細を表示します。

影響

「脆弱性の影響（Vulnerability Impact）」（下記）を参照してください。

影響修飾子（Impact Qualification）

このフィールドは、[脆弱性の詳細（Vulnerability Details）] ページでのみ使用できます。

ドロップダウン リストを使用して、脆弱性を有効または無効にします。Management Center は、影響の相関関係において、無効な脆弱性を無視します。

ユーザがここで指定する設定によって、システム全体で脆弱性がどのように処理されるか、およびユーザが値を選択するホスト プロファイルに脆弱性が限定されないかが決まります。

[リモート（Remote）]

脆弱性がリモートで不正利用されるかどうかを示します（TRUE/FALSE）。

重大度

National Vulnerability Database（NVD）の基本スコアと Common Vulnerability Scoring System スコア（CVSS）。

Snort ID

[Snort ID]（SID）データベースにおいて脆弱性に関連付けられている識別番号。つまり、侵入ルールで特定の脆弱性を悪用するネットワーク トラフィックを検出できる場合、その脆弱性は、侵入ルールの SID に関連付けられます。

脆弱性は複数の SID に関連付けることが可能（または SID に関連付けないことも可能）であることに注意してください。脆弱性が複数の SID に関連付けられている場合、脆弱性テーブルには、各 SID に対して 1 つのローが含まれています。

SVID

脆弱性を追跡するためにシステムで使用する脆弱性の識別番号。

この脆弱性の詳細を表示するには、[表示（View）]（👁）をクリックします。

脆弱性の影響/影響

脆弱性のシビラティ（重大度）。0～10 の値で、10 は最も重大であることを示します。

関連トピック

イベントの検索 （845 ページ）

脆弱性の非アクティブ化

脆弱性を非アクティブ化すると、システムでこの脆弱性を使用して侵入の影響の関連付けを評価することができなくなります。ネットワーク上のホストにパッチを適用した後、またはホストが脆弱性の影響を受けないと判断した後に、脆弱性を非アクティブ化できます。システム

が、この脆弱性から影響を受けている新しいホストを検出すると、この脆弱性はこのホストに対して有効であると見なされます（自動的には非アクティブ化されません）。

IPアドレスによって制約されて**いない**脆弱性ワークフロー内である1つの脆弱性を非アクティブ化すると、ネットワーク上の検出されたすべてのホストに対してその脆弱性が非アクティブ化されます。脆弱性ワークフロー内の脆弱性を非アクティブ化できるのは、次の各ページだけです。

- デフォルトの脆弱性ワークフローの2ページ目の[ネットワーク上の脆弱性（Vulnerabilities on the Network）]。これには、ネットワーク上のホストに適用される脆弱性のみが表示されます。
- 脆弱性ワークフロー（カスタムまたは事前定義）のページ。このワークフローは、検索を使用して IP アドレスに基づいて制約されます。

1 台のホストに対して 1 つの脆弱性を非アクティブ化できます。この非アクティブ化は、ネットワーク マップの使用、ホストのホスト プロファイルの使用、または脆弱性を非アクティブ化する対象の 1 つ以上のホストの IP アドレスに基づいて脆弱性ワークフローを制約することによって行えます。関連付けられた複数の IP アドレスを持つホストの場合、この機能はそのホストの選択された 1 つの IP アドレスのみに適用されます。

マルチドメイン展開では、先祖ドメインの脆弱性を非アクティブ化すると、すべての子孫ドメインでその脆弱性が非アクティブ化されます。リーフ ドメインでは、脆弱性が先祖ドメインでアクティブ化された場合、リーフ ドメインのデバイスの脆弱性をアクティブ化または非アクティブ化できます。

関連トピック

個々のホストに関する脆弱性の非アクティブ化 （1076 ページ）
個々の脆弱性の非アクティブ化 （1076 ページ）
複数の脆弱性の非アクティブ化 （1127 ページ）

脆弱性データの表示

Management Center を使用して、脆弱性のテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

脆弱性にアクセスするときに表示されるページは、使用するワークフローによって異なります。ユーザは事前定義のワークフローを使用できますが、これには脆弱性のテーブル ビューが含まれています。検出されたいずれかのホストが脆弱性を示しているかどうかに関係なく、テーブル ビューにはデータベース内の各脆弱性に対して1つのローが含まれています。事前定義のワークフローの2ページ目には、ネットワーク上で検出されたホストに適用されるそれぞれの脆弱性（まだユーザが非アクティブにしていないもの）に対して1つのローが含まれています。事前定義のワークフローは脆弱性の詳細ビューで終了しますが、このビューには、制約を満たすすべての脆弱性について詳細な説明が含まれています。

ヒント 単一のホストまたはホストのセットに適用される脆弱性を表示する場合は、ホストの IP アドレスまたは IP アドレスの範囲を指定して、脆弱性の検索を実行します。

また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

脆弱性のテーブルは、マルチドメイン展開のドメインによって制限されません。

手順

ステップ 1 次のように、脆弱性のテーブルにアクセスします。

- 事前定義された脆弱性ワークフローを使用する場合、**[分析（Analysis）]** > **[ホスト（Hosts）]** > **[脆弱性（Vulnerabilities）]** を選択します。
- 脆弱性テーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [脆弱性（Vulnerabilities）] を選択します。

ステップ 2 次の選択肢があります。

- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （1085 ページ）を参照）。
- 脆弱性を非アクティブにして、現在脆弱な状態にあるホストについて、侵入の影響の相関に使用しないようにします（複数の脆弱性の非アクティブ化 （1127 ページ）を参照）。
- SVID カラムの [表示（View）]（👁） をクリックして、脆弱性に関する詳細を表示します。または、脆弱性 ID を制約して脆弱性の詳細ページへドリルダウンします。脆弱性の詳細の表示 （1126 ページ）でその他の詳細を表示するオプションを確認してください。
- タイトルを右クリックして [フルテキストの表示（Show Full Text）] を選択することによって、脆弱性タイトルのフルテキストを表示します。

脆弱性の詳細の表示

手順

脆弱性の詳細は、次の方法のいずれかで表示できます。

- **[分析（Analysis）]** > **[ホスト（Hosts）]** > **[脆弱性（Vulnerabilities）]** を選択し、SVID の横にある [表示（View）]（👁） をクリックします。
- **[分析（Analysis）]** > **[ホスト（Hosts）]** > **[サードパーティの脆弱性（Third-Party Vulnerabilities）]** を選択し、SVID の横にある [表示（View）]（👁） をクリックします。
- **[分析（Analysis）]** > **[ホスト（Hosts）]** > **[ネットワークマップ（Network Map）]** を選択し、[脆弱性（Vulnerabilities）] をクリックします。
- 脆弱性の影響を受けるホストのプロファイルを表示し（**[分析（Analysis）]** > **[ホスト（Hosts）]** > **[ネットワークマップ（Network Map）]**（[Analysis] > [Hosts] > [Network Map]）、[ホスト（Hosts）]をクリックし、調査しているホストをドリルダウンしてクリックします）、そのプロファイルの [脆弱性（Vulnerabilities）] セクションを展開します。

- [分析（Analysis）] > [ホスト（Hosts）] > [脆弱性（Vulnerabilities）] の下にある任意のテーブルで、[CVE ID] 列の値を右クリックし、[NVDで説明を表示する（View description in NVD）] を選択して、NVD（National Vulnerabilities Database）Web サイトでその CVE を表示します。

複数の脆弱性の非アクティブ化

IP アドレスで制約されて**いない**脆弱性ワークフロー内で脆弱性を非アクティブにすると、ネットワーク上で検出されたすべてのホストに対する脆弱性が非アクティブ化されます。

マルチドメイン導入では、先祖ドメインで脆弱性を非アクティブ化すると、すべての子孫ドメインでも脆弱性が非アクティブ化されます。リーフ ドメインは、先祖ドメインで脆弱性がアクティブ化されていれば、自分のデバイスの脆弱性をアクティブ化または非アクティブ化できます。

手順

ステップ 1 次のように、脆弱性のテーブルにアクセスします。

- 事前定義された脆弱性ワークフローを使用する場合、**[分析（Analysis）] > [ホスト（Hosts）] > [脆弱性（Vulnerabilities）]** を選択します。
- 脆弱性テーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [脆弱性（Vulnerabilities）] を選択します。

ステップ 2 [ネットワークの脆弱性（Vulnerabilities on the Network）] をクリックします。

ステップ 3 非アクティブにする脆弱性の横にあるチェックボックスをオンにします。

ステップ 4 ページ下部の [レビュー（Review）] をクリックします。

関連トピック

個々のホストに関する脆弱性の非アクティブ化 （1076 ページ）
個々の脆弱性の非アクティブ化 （1076 ページ）

サードパーティの脆弱性データ

システムには、独自の脆弱性追跡データベースが含まれています。これはシステムのフィンガープリンティング機能と組み合わせて使用して、ネットワーク上のホストに関連付けられている脆弱性を特定します。

システムの脆弱性データは、サードパーティ製のアプリケーションからインポートしたネットワーク マップ データで補完できます。これを行うには、組織で、このデータをインポートするためのスクリプトを記述できるか、コマンドラインでファイルのインポートを作成できなけ

ればなりません。詳細については、*Firepower* システムホスト入力 *API* ガイドを参照してください。

インポートしたデータを影響の相関に含めるには、サードパーティの脆弱性情報を、データベース内のオペレーティングシステムおよびアプリケーションの定義にマップする必要があります。サードパーティの脆弱性情報は、クライアントの定義にマップすることはできません。

サードパーティの脆弱性データの表示

ホスト入力機能を使用してサードパーティの脆弱性データをインポートした後で、Management Center を使用してサードパーティの脆弱性のテーブルを表示することができます。ここでユーザーは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

サードパーティの脆弱性にアクセスするときに表示されるページは、使用するワークフローによって異なります。2 つの事前定義されたワークフローがあります。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 次のようにして、サードパーティの脆弱性データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[分析（Analysis）] > [ホスト（Hosts）] > [サードパーティの脆弱性（Third-Party Vulnerabilities）]** を選択します。
- サードパーティの脆弱性のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [送信元別の脆弱性（Vulnerabilities by Source）] または [IP アドレス別の脆弱性（Vulnerabilities by IP Address）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （1085 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（サードパーティの脆弱性データのフィールド （1129 ページ）を参照）。
- SVID カラムの [表示（View）]（👁）をクリックして、サードパーティの脆弱性に関する詳細を表示します。または、脆弱性 ID を制約して脆弱性の詳細ページへドリルダウンします。

サードパーティの脆弱性データのフィールド

サードパーティの脆弱性テーブルで表示および検索できるフィールドの詳細は以下のとおりです。

脆弱性ソース（Vulnerability Source）

サードパーティの脆弱性のソース（QualysGuard、NeXpose など）。

脆弱性 ID（Vulnerability ID）

ソースの脆弱性に関連付けられている ID 番号。

IPアドレス（IP Address）

脆弱性の影響を受けるホストに関連付けられている IP アドレス。

ポート

ポート番号（脆弱性が、特定のポート上で実行されているサーバに関連付けられている場合）。

Bugtraq ID

Bugtraq データベースにおいて脆弱性に関連付けられている識別番号。（http://www.securityfocus.com/bid/）

CVE ID

MITRE の Common Vulnerabilities and Exposures（CVE）データベース（https://cve.mitre.org/）の脆弱性に関連付けられた識別番号。

SVID

脆弱性を追跡するためにシステムで使用する従来の脆弱性識別番号。

SVID について脆弱性の詳細にアクセスするには、[表示（View）]（  ）をクリックします。

Snort ID

[Snort ID]（SID）データベースにおいて脆弱性に関連付けられている識別番号。つまり、侵入ルールで特定の脆弱性を悪用するネットワーク トラフィックを検出できる場合、その脆弱性は、侵入ルールの SID に関連付けられます。

脆弱性は複数の SID に関連付けることが可能（または SID に関連付けないことも可能）であることに注意してください。脆弱性が複数の SID に関連付けられている場合、脆弱性テーブルには、各 SID に対して 1 つのローが含まれています。

タイトル（Title）

脆弱性のタイトル。

説明

脆弱性についての簡単な説明。

ドメイン（Domain）

この脆弱性を持つホストのドメイン。このフィールドは、マルチテナンシーのためにManagement Center を設定したことがある場合に表示されます。

カウント（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

関連トピック

イベントの検索 （845 ページ）

アクティブ セッション、ユーザー、およびユーザー アクティビティ データ

アイデンティティ ソースは、アクティブなセッション データ、ユーザ データ、およびユーザ アクティビティ データを収集します。データは、次の個々のユーザ関連のワークフローに表示されます。

- [アクティブなセッション（Active Sessions）]：このワークフローには、ネットワーク上の現在のすべてのユーザ セッションが表示されます。複数の同時アクティブ セッションを実行する単一ユーザは、この表で複数の行を占めます。このワークフローに表示されるユーザ データの種類について、詳しくはアクティブ セッション データ （1141 ページ）を参照してください。
- ユーザ：このワークフローは、ネットワークで認識されるすべてのユーザを表示します。この表では 1 ユーザが 1 つの行を占めます。このワークフローに表示されるユーザ データの種類について、詳しくはユーザー データ（User Data） （1143 ページ）を参照してください。
- ユーザ アクティビティ：このワークフローは、ネットワークで認識されるすべてのユーザ アクティビティを表示します。この表では、複数のユーザ アクティビティ インスタンスを持つ 1 ユーザが複数の行を占めます。このワークフローに表示されるユーザ アクティビティの種類の詳細については、ユーザー アクティビティ データ （1146 ページ）を参照してください。

これらのワークフローの入力元であるユーザー アイデンティティ ソースの詳細については、『Cisco Secure Firewall Management Center デバイス構成ガイド』の「」を参照してください。

ユーザー関連フィールド

ユーザ関連データは、アクティブ セッション、ユーザ、およびユーザ アクティビティのテーブルに表示されます。

（注） Azure AD レルムユーザーのアクティブセッションは、新しい UI レイアウトの [アクティブセッション（Active Sessions）] にのみ表示され、レガシー UI には表示されません。

表 *123*：アクティブ セッション、ユーザ、およびユーザ アクティビティのフィールドの説明

フィールド	説明	[アクティブなセッション（**Active Sessions**）] テーブル	[ユーザテーブル（**Users Table**）]	[ユーザアクティビティ（**User Activity**）] テーブル
アクティブセッション数（Active Session Count）	ユーザに関連付けられているアクティブセッションの数。	×	対応	×
認証タイプ（Authentication Type）	認証のタイプ：[認証なし（No Authentication）]、[パッシブ認証（Passive Authentication）]、[アクティブ認証（Active Authentication）]、[ゲスト認証（Guest Authentication）]、[失敗した認証（Failed Authentication）]、または [VPN 認証（VPN Authentication）]。 各認証タイプでサポートされるアイデンティティソースの詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。	対応	×	対応
ポリシーに使用可能	値 [はい（Yes）] は、ユーザーがユーザー ストア（Active Directory など）から取得されたことを意味します。 値 [いいえ（No）] は、Management Center がそのユーザーのログインのレポートを取得したものの、そのユーザーがユーザーストアに存在しないことを意味します。これは、除外されたグループのユーザーがユーザー ストアにログインした場合に発生することがあります。レルムを設定するときにグループをダウンロード対象から除外することができます。 ポリシーに使用できないユーザーは、Management Center には記録されますが、管理対象デバイスには送信されません。	×	対応	×

フィールド	説明	[アクティブなセッション（**Active Sessions**）] テーブル	[ユーザテーブル（**Users Table**）]	[ユーザアクティビティ（**User Activity**）] テーブル
メンバー数（Count）	（注） [カウント（Count）] フィールドは、制約を適用した結果、同じ行が複数作成された場合にのみ表示されます。 テーブルに応じて、特定の行に表示される情報と一致するセッション、ユーザー、またはアクティビティ イベントの数。	対応	対応	対応
現在の IP（Current IP）	（「現在の IP/ドメイン（Current IP/Domain）」および「IP アドレス（IP address）」も参照してください） ユーザがログインしたホストに関連付けられている IP アドレス。 ユーザにアクティブセッションがない場合、[ユーザ（Users）] テーブルでこのフィールドが空白になります。	対応	×	×
部署名（Department）	ユーザの部署（レルムが取得）。サーバ上のユーザに明示的に関連付けられている部門がない場合、この部門は、サーバが割り当てるいずれかのデフォルト グループとして示されます。たとえば、Active Directory では、これは `Users (ad)` となります。以下の場合、このフィールドは空白になります。 • レルムを設定していない。 • Management Center が、Management Center データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）。	対応	対応	×
説明	セッション、ユーザ、またはユーザ アクティビティについての詳細情報（利用可能な場合）。	×	×	対応

フィールド	説明	[アクティブなセッション（**Active Sessions**）] テーブル	[ユーザテーブル（**Users Table**）]	[ユーザアクティビティ（**User Activity**）] テーブル
Device	トラフィックベースの検出またはアクティブ認証アイデンティティ ソースによって検出されたユーザ アクティビティの場合は、ユーザを識別したデバイスの名前。 他のタイプのユーザー アクティビティの場合は、管理している側の Management Center になります。 （注） 高可用性展開で VPN を構成した場合、アクティブな VPN セッションに対して表示されるデバイス名は、ユーザーセッションを識別したプライマリデバイスまたはセカンダリデバイスである可能性があります。	対応	×	対応
ディスカバリ アプリケーション（Discovery Application）	ユーザの検出に使用されるアプリケーションまたはプロトコル。 • トラフィックベースの検出によって検出されたユーザ アクティビティの場合は、ldap、pop3、imap、oracle、sip、http、ftp、mdns、または aim のいずれか。 （注） ユーザは SMTP ログインに基づいてデータベースに追加されません。 • 他のすべてのユーザ アクティビティの場合：ldap。	対応	対応	対応
[現在の IP ドメイン（Current IP Domain）]/[ドメイン（Domain）]	[アクティブセッション（Active Sessions）] テーブルでは、ユーザー アクティビティが検出されたマルチテナンシー ドメイン。 [ユーザー（Users）] テーブルでは、ユーザーのレルムに関連付けられたマルチテナンシー ドメイン。 [ユーザ アクティビティ（User Activity）] テーブルでは、ユーザ アクティビティが検出されたマルチテナンシー ドメイン。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。	対応	対応	対応

フィールド	説明	[アクティブなセッション（**Active Sessions**）] テーブル	[ユーザテーブル（**Users Table**）]	[ユーザアクティビティ（**User Activity**）] テーブル
E メール（Email）	ユーザーのメール アドレス。以下の場合、このフィールドは空白になります。 • AIM ログインによってユーザがデータベースに追加された。 • LDAP ログインによってユーザがデータベースに追加されており、LDAP サーバ上にユーザと関連付けられている電子メールアドレスが存在しない。	対応	対応（電子メールとして）	×
終了ポート（End Port）	TS エージェントによってユーザが報告され、そのユーザのセッションが現在アクティブである場合、このフィールドは、ユーザに割り当てられたポート範囲の終了値を示します。ユーザの TS エージェントセッションが非アクティブである場合、またはユーザが別のアイデンティティ ソースによって報告された場合、このフィールドは空白になります。	×	×	対応
エンドポイントロケーション（Endpoint Location）	ISE で指定された、ユーザの認証に ISE を使用したネットワーク デバイスの IP アドレス。ISE を設定していない場合、このフィールドは空白です。	×	×	対応
エンドポイントプロファイル（Endpoint Profile）	Cisco ISE によって識別されるユーザのエンドポイント デバイス タイプ。ISE を設定していない場合、このフィールドは空白です。	×	×	対応
イベント	ユーザ アクティビティのタイプ。	×	×	対応

フィールド	説明	[アクティブなセッション（**Active Sessions**）] テーブル	[ユーザテーブル（**Users Table**）]	[ユーザアクティビティ（**User Activity**）] テーブル
First Name	ユーザの名（レルムが取得）。以下の場合、このフィールドは空白になります。 • レルムを設定していない。 • Management Center が、Management Center データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）。 • サーバに、対象のユーザと関連付けられている名がない。	対応	対応	×

フィールド	説明	[アクティブなセッション（**Active Sessions**）] テーブル	[ユーザテーブル（**Users Table**）]	[ユーザアクティビティ（**User Activity**）] テーブル
[IPアドレス（IP Address）]	[ユーザー ログイン（User Login）] ユーザー アクティビティの場合は、次のログインに関連するIPアドレスまたは内部 IP アドレス。 • LDAP、POP3、IMAP、FTP、HTTP、MDNS、および AIM ログイン：ユーザのホストのアドレス • SMTP および Oracle のログイン：サーバのアドレス • SIP ログイン：セッション発信者のアドレス （「現在の IP（Current IP）」および「現在の IP/ドメイン（Current IP/Domain）」も参照してください） 関連付けられているIPアドレスは、そのユーザがIPアドレスの現行のユーザであることを意味するわけではありません。権限を持たないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されます。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることができます。ただし、権限のあるユーザーがそのホストにログインした後は、別の権限のあるユーザーによるログインだけが現行ユーザーを変更します。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	×	×	対応

フィールド	説明	[アクティブなセッション（Active Sessions）] テーブル	[ユーザテーブル（Users Table）]	[ユーザアクティビティ（User Activity）] テーブル
Last Name	ユーザの姓（レルムが取得）。以下の場合、このフィールドは空白になります。 • レルムを設定していない。 • Management Center が、Management Center データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）。 • サーバに、対象のユーザと関連付けられている姓がない。	対応	対応	×
前回の検出（Last Seen）	ユーザのセッションが最後に開始された（またはユーザ データが更新された）日時。	対応	対応	×
ログイン時刻（Login Time）	ユーザのセッションが開始した日時。	対応	×	×
Phone Number	ユーザの電話番号（レルムが取得）。以下の場合、このフィールドは空白になります。 • レルムを設定していない。 • Management Center が、Management Center データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）。 • サーバに、対象のユーザと関連付けられている電話番号が存在しない。	対応（電話として）	対応	×
レルム	ユーザに関連付けられているアイデンティティ レルム。	対応	対応	対応
セキュリティ グループ タグ（Security Group Tag）	パケットが信頼できる TrustSec ネットワークへ送信されたときに、Cisco TrustSec によって適用される [セキュリティ グループ タグ（Security Group Tag）]（SGT）属性。ISE を設定していない場合、このフィールドは空白です。	×	×	対応

フィールド	説明	[アクティブなセッション（Active Sessions）] テーブル	[ユーザテーブル（Users Table）]	[ユーザアクティビティ（User Activity）] テーブル
セッション時間（Session Duration）	[ログイン時刻（Login Time）] と現在の時刻から計算されたユーザ セッションの期間。	対応	×	×
開始ポート（Start Port）	TS エージェントによってユーザが報告され、そのユーザのセッションが現在アクティブである場合、このフィールドは、ユーザに割り当てられたポート範囲の開始値を示します。ユーザのTSエージェントセッションが非アクティブである場合、またはユーザが別のアイデンティティ ソースによって報告された場合、このフィールドは空白になります。	×	×	対応
時刻（Time）	システムがユーザ アクティビティを検出した時間。	×	×	対応
[ユーザー（User）]	このフィールドには少なくとも、ユーザのレルムとユーザ名が表示されます。たとえば、`Lobby\jsmith` と表示された場合は、Lobby がレルム、jsmith がユーザ名です。 レルムがLDAPサーバから追加のユーザデータをダウンロードし、システムがそれをユーザに関連付けた場合は、このフィールドにユーザの名、姓、タイプも表示されます。たとえば、`John Smith (Lobby\jsmith, LDAP)` と表示された場合は、John Smith がユーザの名前、LDAP がそのタイプです。 （注） トラフィックベースの検出では失敗した AIM ログインが記録される可能性があるため（たとえば、ユーザが正しくないユーザ名を入力した場合など）、Management Center は無効な AIM ユーザを保存する可能性があります。	対応	対応	×
Username	ユーザに関連付けられているユーザ名。	対応	対応	対応

フィールド	説明	[アクティブなセッション（**Active Sessions**）] テーブル	[ユーザテーブル（**Users Table**）]	[ユーザアクティビティ（**User Activity**）] テーブル
VPN 受信バイト数（VPN Bytes In）	リモートアクセス VPN の報告によるユーザーアクティビティの場合は、Threat Defense がリモートピアまたはクライアントから受信した合計バイト数。 （注） ユーザの VPN セッションが終了した後、受信した合計バイト数を表示できます。継続中の VPN セッションでは、これは動的カウンタではありません。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	対応	×	対応
VPN 送信バイト数（VPN Bytes Out）	リモートアクセス VPN の報告によるユーザーアクティビティの場合は、Threat Defense がリモートピアまたはクライアントに伝送された合計バイト数。 （注） ユーザの VPN セッションが終了した後、送信した合計バイト数を表示できます。継続中の VPN セッションでは、これは動的カウンタではありません。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	×	×	対応
VPN クライアントのアプリケーション（VPN Client Application）	リモートアクセス VPN の報告によるユーザーアクティビティの場合は、リモートユーザーの Cisco Secure Client の AnyConnect VPN モジュール アプリケーション。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	対応	×	対応
VPN クライアントの国（VPN Client Country）	リモートアクセス VPN の報告によるユーザーアクティビティの場合は、セキュアクライアント VPN クライアントによって報告された国名。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	×	×	対応

フィールド	説明	[アクティブなセッション（**Active Sessions**）] テーブル	[ユーザテーブル（**Users Table**）]	[ユーザアクティビティ（**User Activity**）] テーブル
VPN クライアントの OS（VPN Client OS）	リモートアクセス VPN の報告によるユーザーアクティビティの場合は、セキュアクライアント VPNによって報告されたリモートユーザーのエンドポイント オペレーティング システム。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	対応	×	対応
VPN クライアントのパブリック IP（VPN Client Public IP）	リモートアクセス VPN の報告によるユーザーアクティビティの場合は、セキュアクライアント VPN デバイスのパブリックルーティング可能な IP アドレス。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	対応	×	対応
VPN 接続期間（VPN Connection Duration）	リモート アクセス VPN の報告によるユーザ アクティビティの場合は、セッションがアクティブだった合計時間（HH:MM:SS）。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	×	×	対応
VPN 接続プロファイル（VPN Connection Profile）	リモート アクセス VPN の報告によるユーザ アクティビティの場合は、VPNセッションで使用される接続プロファイル（トンネル グループ）の名前。接続プロファイルは、リモートアクセス VPN ポリシーに含まれます。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	対応	×	対応

フィールド	説明	[アクティブなセッション（**Active Sessions**）] テーブル	[ユーザテーブル（**Users Table**）]	[ユーザアクティビティ（**User Activity**）] テーブル
VPN グループ ポリシー（VPN Group Policy）	リモート アクセス VPN の報告によるユーザ アクティビティの場合は、VPNセッションが確立されたときにクライアントに割り当てられたグループ ポリシーの名前。これは VPN 接続プロファイルに関連付けられた静的に割り当てられたグループ ポリシー、またはRADIUS が認証に使用されている場合は動的に割り当てられたグループ ポリシーです。RADIUS サーバによって割り当てられている場合、このグループ ポリシーは VPN 接続プロファイル用に設定された静的ポリシーよりも優先されます。グループ ポリシーは、リモート アクセス VPN ポリシーのユーザ グループに共通の属性を設定します。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	対応	×	対応
VPN セッション タイプ（VPN Session Type）	リモート アクセス VPN の報告によるユーザ アクティビティの場合は、セッションのタイプ（[LAN 間（LAN-to-LAN）] または [リモート（Remote）]）。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	対応	×	対応

アクティブ セッション データ

[分析（Analysis）] > [ユーザ（Users）] > [アクティブなセッション（Active Sessions）] ワークフローには、現在のユーザ セッションに関する選択情報が表示されます。ネットワーク上のユーザーが複数のセッションを同時に実行するとき、システムは次の場合にセッションを一意に識別できます。

- 一意の **IP アドレス**値を持っている。
- Cisco Terminal Services（TS）エージェントによって提供される、一意の**開始ポート**値と**終了ポート**値を持っている。
- 一意の**現在の IP ドメイン**値を持っている。
- 異なるアイデンティティ ソースによって認証された。
- 異なるアイデンティティ レルムと関連付けられた。

システムによって保存されるユーザおよびユーザ アクティビティ データの詳細については、ユーザーデータ（User Data）（1143 ページ）およびユーザーアクティビティデータ（1146 ページ）を参照してください。

一般的なユーザー関連イベントのトラブルシューティングとリモートアクセス VPN のトラブルシューティングの詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの「the *Troubleshoot Realms and User Downloads*」および「*VPN Troubleshooting*」を参照してください。

アクティブ セッション データの表示

アクティブ セッションのテーブルを表示して、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローを使用することができますが、これには、検出されたすべてのユーザが記載されているユーザのテーブル ビューが含まれています。このワークフローは、ユーザの詳細ページで終了します。ユーザの詳細ページは、制約を満たす各ユーザについての情報を提供します。

手順

ステップ 1 次のように、ユーザ データにアクセスします。

- 事前定義されたワークフローを使用している場合は、**[分析（Analysis）] > [ユーザー（Users）] > [アクティブセッション（Active Sessions）]** をクリックします。
- アクティブ セッションのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [アクティブなセッション（Active Sessions）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用（1085 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べるには、アクティブセッションデータ（1141 ページ）およびユーザー関連フィールド（1130 ページ）を参照してください。

ユーザー データ（User Data）

アイデンティティ ソースが、データベースに存在しないユーザーのユーザー ログインを報告した場合、そのログイン タイプが特に制限されていない限り、そのユーザーはデータベースに追加されます。

次のいずれかが発生すると、システムはユーザ データベースを更新します。

- Management Center のユーザーが、[ユーザー（Users）] テーブルから権限のないユーザーを手動で削除する。
- アイデンティティ ソースが、そのユーザによるログオフを報告する。
- レルムがレルムの [ユーザ セッションのタイムアウト：認証されたユーザ（User Session Timeout: Authenticated Users）] 設定、[ユーザ セッションのタイムアウト：認証に失敗したユーザ（User Session Timeout: Failed Authentication Users）] 設定、または [ユーザ セッションのタイムアウト：ゲスト ユーザ（User Session Timeout: Guest Users）] 設定で指定されているユーザ セッションを終了した。

（注） ISE/ISE-PIC が設定されている場合は、ユーザ テーブルにホスト データが表示されることがあります。ISE/ISE-PIC によるホスト検出は完全にはサポートされていないため、ISE によって報告されたホスト データを使用してユーザー制御を実行することはできません。

システムによって検出されたユーザ ログインのタイプに応じて、新しいユーザのどの情報が保存されるかが決まります。

ID ソース	ログイン タイプ	格納されるユーザ データ
ISE/ISE-PIC	Active Directory LDAP RADIUS RSA	• ユーザ名 • 現行の IP アドレス • セキュリティ グループ タグ（SGT）（ISE-PIC ではサポートされていない） • エンドポイントのプロファイル/デバイス タイプ（ISE-PIC ではサポートされていない） • エンドポイントの場所/場所 IP（ISE-PIC ではサポートされていない） • タイプ（LDAP）

ID ソース	ログイン タイプ	格納されるユーザ データ
TS エージェント	Active Directory	• ユーザ名 • 現行の IP アドレス • 開始ポート • 終了ポート • タイプ（LDAP）
キャプティブ ポータル	Active Directory LDAP	• ユーザ名 • 現行の IP アドレス • タイプ（LDAP）
トラフィック ベースの検出	LDAP AIM Oracle SIP HTTP FTP MDNS	• ユーザ名 • 現行の IP アドレス • タイプ（AD）
	POP3 IMAP	• ユーザ名 • 現行の IP アドレス • 電子メール アドレス • タイプ（`pop3` または `imap`）

（注） このテーブルには、Microsoft Azure Active Directory ユーザーに関するデータは表示されません。

ユーザを自動的にダウンロードするようにレルムを設定すると、Management Center は指定した間隔に基づいてサーバに対するクエリを実行します。システムが新しいユーザのログインを検出してから、Management Center データベースがユーザのメタデータを更新するまでに、5～10 分かかることがあります。Management Centerは、ユーザごとに次の情報とメタデータを取得します。

- ユーザ名
- 姓と名

- 電子メール アドレス
- 部署
- 電話番号
- 現行の IP アドレス
- セキュリティ グループ タグ（SGT）（使用可能な場合）
- エンドポイントのプロファイル（使用可能な場合）
- エンドポイントの場所（使用可能な場合）
- 開始ポート（使用可能な場合）
- 終了ポート（使用可能な場合）

Management Center がデータベースに格納できるユーザの数は、Management Center のモデルによって異なります。ホストに対して権限を持たないユーザがログインしていることが検出された場合、そのログインはユーザおよびホストの履歴に記録されます。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることができます。ただし、ホストに対して権限を持つユーザのログインが検出された後は、権限を持つ別のユーザがログインした場合にのみ、現行ユーザが変わります。

AIM、Oracle、および SIP のログインがトラフィックベースで検出された場合は、システムが LDAP サーバから取得したどのユーザ メタデータにも関連付けられないため、これらのログインにより重複したユーザ レコードが作成されることに注意してください。これらのプロトコルから重複したユーザ レコードを取得することに起因するユーザ カウントの過度な使用を回避するには、これらのプロトコルを無視するようにトラフィックベースの検出を設定します。

データベースからユーザを検索、表示、削除することができます。また、データベースからすべてのユーザを消去することもできます。

一般的なユーザー関連のイベント トラブルシューティングについては、Cisco Secure Firewall Management Center デバイス構成ガイド を参照してください。

ユーザー データの表示

ユーザーのテーブルを表示して、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローを使用することができますが、これには、検出されたすべてのユーザが記載されているユーザのテーブル ビューが含まれています。このワークフローは、ユーザの詳細ページで終了します。ユーザの詳細ページは、制約を満たす各ユーザについての情報を提供します。

手順

ステップ 1 次のように、ユーザ データにアクセスします。

- 事前定義されたワークフローを使用する場合は、**[分析（Analysis）]**>**[ユーザー（Users）]**>**[ユーザー（Users）]** を選択します。
- ユーザのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [ユーザ（Users）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （1085 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（ユーザー関連フィールド（1130ページ）を参照）。

ユーザー アクティビティ データ

システムは、ネットワーク上のユーザーアクティビティの詳細を伝達するイベントを生成します。システムがユーザアクティビティを検出すると、そのユーザアクティビティデータはデータベースに記録されます。ユーザアクティビティは、表示、検索、および削除することも、すべてのユーザ アクティビティをデータベースから消去することもできます。

あるユーザがネットワーク上で初めて確認されると、システムはそのユーザ アクティビティ イベントをログに記録します。そのユーザがその後に確認された場合、新しいユーザアクティビティイベントはログに記録されません。ただし、そのユーザのIPアドレスが変わった場合、システムは新しいユーザ アクティビティ イベントをログに記録します。

システムは、ユーザーアクティビティと他のタイプのイベントとの関連付けも行います。たとえば、侵入イベントは、そのイベントの発生時に送信元ホストと宛先ホストにログインしていたユーザを通知することができます。この関連付けにより、攻撃の対象になったホストにログインしていたユーザ、または内部攻撃やポートスキャンを開始したユーザがわかります。

ユーザ アクティビティは、相関ルールで使用することもできます。相関ルールは、ユーザ アクティビティのタイプだけでなく、指定した他の条件に基づいて作成することができます。相関ルールが相関ポリシーで使用される場合、ネットワーク トラフィックが条件を満たしたときは、相関ルールが修復およびアラートの応答を起動します。

（注） ISE/ISE-PIC が設定されている場合は、ユーザ テーブルにホスト データが表示されることがあります。ISE/ISE-PIC によるホスト検出は完全にはサポートされていないため、ISE によって報告されたホスト データを使用してユーザー制御を実行することはできません。

次に、4 つのタイプのユーザ アクティビティ データについて説明します。

新しいユーザのアイデンティティ（New User Identity）

このタイプのイベントは、システムがデータベースに存在しない不明なユーザによるログインを検出したときに生成されます。

あるユーザがネットワーク上で初めて確認されると、システムはそのユーザ アクティビティ イベントをログに記録します。そのユーザがその後に確認された場合、新しいユーザアクティビティイベントはログに記録されません。ただし、そのユーザのIPアドレスが変わった場合、システムは新しいユーザ アクティビティ イベントをログに記録します。

ユーザ ログイン（User Login）

このタイプのイベントは、次のことが発生した後に生成されます。

- キャプティブ ポータルのユーザー認証の実行が成功または失敗した。
- トラフィック ベースの検出がユーザ ログインの成功または失敗を検出した。

（注） トラフィック ベースの検出で検出された SMTP ログインは、一致する電子メール アドレスを持つユーザがデータベースにすでに存在する場合を除いて記録されません。

権限のないユーザーがホストにログインすると、そのログインはユーザーおよびホストの履歴に記録されます。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることができます。ただし、権限のあるユーザーがそのホストにログインした後は、別の権限のあるユーザーによるログインだけが現行ユーザーを変更します。

キャプティブ ポータルまたはトラフィック ベースの検出を使用する場合、失敗したユーザ ログインと失敗したユーザ認証データについて、次の点に注意してください。

- トラフィック ベースの検出（LDAP、IMAP、FTP、および POP3 トラフィック）から報告された失敗したログインは、ユーザアクティビティのテーブル ビューに表示されますが、ユーザのテーブル ビューには表示されません。既知のユーザがログインに失敗した場合、システムではそのユーザをそのユーザ名で識別します。不明なユーザがログインに失敗した場合、システムではそのユーザ名として [失敗した認証（Failed Authentication）] を使用します。
- キャプティブ ポータルから報告された失敗した認証は、ユーザ アクティビティのテーブル ビューとユーザのテーブル ビューの両方に表示されます。既知のユーザが認証に失敗した場合、システムではそのユーザをそのユーザ名で識別します。不明なユーザが認証に失敗した場合、システムではそのユーザをそのユーザが入力したユーザ名で識別します。

ユーザのアイデンティティの削除（Delete User Identity）

このタイプのイベントは、データベースからユーザを手動で削除したときに生成されます。

ドロップ（廃棄）されたユーザのアイデンティティ：ユーザ制限に到達（User Identity Dropped: User Limit Reached）

このタイプのイベントは、システムがデータベースに存在しないユーザを検出したものの、Management Center のモデルで決定されているデータベースの最大ユーザ数に達したためにユーザを追加できなかったときに生成されます。

ユーザー制限に達すると、ほとんどの場合、データベースへの新しいユーザーの追加が停止されます。新しいユーザーを追加するには、古いユーザーまたは非アクティブなユーザーをデータベースから手動で削除するか、データベースからすべてのユーザーを消去する必要があります。

ただし、システムでは権限のあるユーザが優先されます。すでに制限に達しており、これまでに検出されていない権限のあるユーザのログインが検出された場合、システムは長期間非アクティブな状態が続いている権限のないユーザを削除して、権限のある新しいユーザに置き換えます。

ユーザの侵害の兆候イベント

次のユーザの IOC の変化がユーザ アクティビティ データベースに記録されます。

- 侵害の兆候が解決された場合。
- 侵害の兆候ルールがユーザーに対して有効または無効にされた場合。

一般的なユーザー関連のイベント トラブルシューティングについては、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

ユーザー アクティビティ データの表示

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザー アクティビティのテーブルを表示して、検索する情報に応じてイベント ビューを操作することができます。ユーザアクティビティにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローを使用することができます。このワークフローにはユーザ アクティビティのテーブル ビューが含まれており、制約を満たすすべてのユーザの詳細が含まれている、ユーザの詳細ページで終了します。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 次のように、ユーザ アクティビティ データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[分析（Analysis）]**>**[ユーザー（Users）]**>**[ユーザーアクティビティ（User Activity）]** を選択します。
- ユーザ アクティビティのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [ユーザ アクティビティ（User Activity）] を選択します。

ヒント イベントが表示されない場合は、時間範囲の調整が必要な可能性があります（時間枠の変更 （833 ページ）を参照）。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）]をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （1085 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（ユーザー関連フィールド（1130ページ）を参照）。

ユーザー プロファイルとホスト履歴

特定のユーザーの詳細については、[ユーザー（User）]ポップアップ ウィンドウを表示して確認することができます。表示されるページ（このマニュアルでは「ユーザ プロファイル」と呼んでいます）には、Web インターフェイスで「ユーザのアイデンティティ（User Identity）」というタイトルが付いています。

このウィンドウは、次のビューから表示できます。

- ユーザー データを他の種類のイベントに関連付けるすべてのイベント ビュー
- アクティブなセッションのテーブル ビュー
- ユーザーのテーブル ビュー

ユーザ情報は、ユーザ ワークフローの最終ページにも表示されます。

表示されるユーザー データは、ユーザーのテーブル ビューで表示されるものと同じです。

[侵害の兆候（Indications of Compromise）] セクション

このセクションについては、次のセクションを参照してください。

- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Indications of Compromise*」
- 侵害の兆候データ フィールド （1110 ページ）
- 単一ホストまたはユーザにおける侵害の兆候のルール状態の編集 （1111 ページ）
- 侵害の兆候タグの解決 （1112 ページ）
- 侵害の兆候のタグのソース イベントの表示 （1111 ページ）

[ホストの履歴（Host History）] セクション

ホストの履歴には、過去 24 時間のユーザ アクティビティがグラフィック表示されます。ユーザーがログインおよびログオフしたホストの IP アドレスのリストには、ログインとログアウトの概算時間が棒グラフで示されます。一般的なユーザは、1 日の間に複数のホストに対してログオンおよびログオフする可能性があります。たとえば、メール サーバに対する定期的な自

動ログインは複数回の短時間のセッションとして示されますが、（勤務時間中などの）長時間のログインは、長時間のセッションとして示されます。

トラフィック ベースの検出またはキャプティブ ポータルを使用して失敗したログインをキャプチャした場合、ホストの履歴にはユーザがログインに失敗したホストも含まれます。

ホストの履歴を生成するために使用されるデータは、ユーザの履歴データベースに格納されます。このデータベースには、デフォルトで 1000 万のユーザ ログイン イベントが格納されます。ホストの履歴に特定のユーザーに関するデータが表示されない場合、そのユーザーが非アクティブであるか、またはデータベースの制限を増やさなければならないことがあります。

関連トピック

ユーザー データのフィールド

ユーザの詳細およびホスト履歴の表示

手順

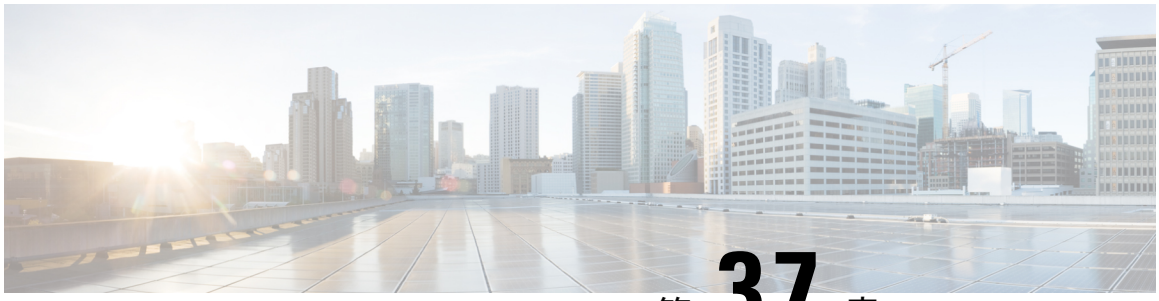
以下の 2 つの対処法があります。

- ユーザーをリストする任意のイベントビューで、ユーザー ID の**ユーザーアイコン**、または、侵入の痕跡に関連付けられているユーザーの場合は**赤色のユーザーアイコン**の横に表示されるユーザーをクリックします。
- いずれかのユーザ ワークフローで、[ユーザ（Users）] の最終ページをクリックします。

検出イベントの操作の履歴

表 *124 :*

機能	最小 Management Center	最小 Threat Defense	詳細
脆弱性ページの変更	6.7	任意（Any）	Bugtraq とその脆弱性データは使用できなくなりました。次の変更が行われました。 • 現在、ほとんどの脆弱性データは National Vulnerability Database（NVD）から取得されています。 • 廃止された冗長なフィールドが削除されました。 • 新しい [CVE ID] 列がテーブルビューに追加され、新しい [シビラティ（重大度）（Severity）] フィールドがテーブルと詳細のページに追加されました。 • テーブルで CVE ID を右クリックすると、NVD のその脆弱性に関する詳細を表示できるようになりました。 • テーブルの [脆弱性の影響（Vulnerability Impact）] 列の名前が [影響（Impact）] に変更されました。（詳細ビューのフィールド名は変更されていません。） • [分析（Analysis）] > [ホスト（Hosts）] > [ネットワークマップ（Network Map）] > [ホスト（Hosts）] でホストプロファイルの脆弱性を表示するときに、脆弱性の詳細（サードパーティの脆弱性を除く）により新しい一連のフィールドが使用されます。 • [分析（Analysis）] > [ホスト（Hosts）] > [ネットワークマップ（Network Map）] > [脆弱性（Vulnerabilities）] ページの [脆弱性（Vulnerabilities）] オプションから、[Bugtraq] オプションが削除されました。 変更された画面： • [分析（Analysis）] > [ホスト（Hosts）] > [脆弱性（Vulnerabilities）] の下のすべてのページ • [分析（Analysis）] > [ホスト（Hosts）] > [ネットワークマップ（Network Map）] ページの [ホスト（Hosts）] タブと [脆弱性（Vulnerabilities）] タブ サポート対象プラットフォーム： Management Center



第 37 章

相関イベントとコンプライアンス イベント

次のトピックでは、相関イベントとコンプライアンスイベントを表示する方法について説明します。

相関イベントの表示

アクティブな相関ポリシーに含まれる相関ルールがトリガーとして使用されると、システムが相関イベントを生成してデータベースにそれを記録します。

（注） アクティブな相関ポリシーに含まれるコンプライアンスallowリストがトリガーとして使用されると、システムがallowリストイベントを生成します。

相関イベントのテーブルを表示し、検索対象の情報に応じてイベント ビューを操作できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

相関イベントにアクセスしたときに表示されるページは、使用するワークフローによって異なります。相関イベントのテーブル ビューが含まれる定義済みワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

始める前に

このタスクを実行するには、管理者またはセキュリティ アナリスト（Security Analyst）ユーザーである必要があります。

手順

ステップ 1 **[分析（Analysis）] > [相関（Correlation）] > [相関イベント（Correlation Events）]**を選択します。

オプションで、カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [(ワークフローの切り替え)（(switch workflow)）] をクリックします。

ヒント 相関イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックし、[相関イベント（Correlation Events）] を選択します。

ステップ 2 オプションで、時間枠の変更 （833 ページ）の説明に従って、時間範囲を調整します。

ステップ 3 次のいずれかの操作を実行します。

- 表示されるカラムの詳細については、相関イベントのフィールド（1155 ページ）を参照してください。
- IP アドレスのホストプロファイルを表示するには、IP アドレスの横に表示されるホストプロファイルをクリックします。
- ユーザー ID 情報を表示するには、[ユーザーID（User Identity）] の隣に表示される [ユーザー（User）]アイコン、またはIOCに関連付けられているユーザーの場合は[レッドユーザー（Red User）] をクリックします。
- 現在のワークフロー ページ内でイベントをソートしたり制限したり、または移動するには、ワークフローの使用 （809 ページ）を参照してください。
- 現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフローページの左上にある該当するページ リンクをクリックします。
- 特定の値に制限して、ワークフロー内の次のページにドリルダウンするには、ドリルダウン ページの使用 （818 ページ）を参照してください。
- 一部またはすべての相関イベントを削除するには、削除するイベントの横にあるチェックボックスをオンにして [削除（Delete）] をクリックするか、[すべて削除（Delete All）] をクリックして現在の制約されているビューにあるすべてのイベントを削除することを確認します。
- 他のイベント ビューに移動して関連イベントを表示するには、ワークフロー間のナビゲーション （839 ページ）を参照してください。
- システムの外部にある利用可能なソース内のデータを表示するには、イベント値を右クリックします。表示されるオプションはデータ タイプによって異なり、パブリック ソースが含まれます。他のソースは設定したリソースによって異なります。詳細については、Web ベースのリソースを使用したイベントの調査 （763 ページ）を参照してください。
- イベントに関するインテリジェンスを収集するには、テーブルでイベントの値を右クリックして、シスコまたはサードパーティのインテリジェンス ソースを選択します。たとえば、不審な IP アドレスに関する詳細情報を Cisco Talos から入手できます。表示されるオ

プションは、データタイプやシステムに設定されている統合によって異なります。詳細については、Web ベースのリソースを使用したイベントの調査（763 ページ）を参照してください。

関連トピック

データベース イベント数の制限（66 ページ）
ワークフローのページ（813 ページ）

相関イベントのフィールド

相関ルールがトリガーとして使用されると、システムは相関イベントを生成します。次の表では、表示および検索可能な相関イベント テーブルのフィールドについて説明します。

表 *125*：相関イベントのフィールド

フィールド	説明
説明	相関イベントについての説明。説明に示される情報は、ルールがどのようにトリガーとして使用されたかによって異なります。 たとえば、オペレーティング システム情報の更新イベントによってルールがトリガーとして使用された場合、新しいオペレーティング システムの名前と信頼度レベルが表示されます。
Device	ポリシー違反をトリガーとして使用したイベントを生成したデバイスの名前。
ドメイン（Domain）	ポリシー違反をトリガーとして使用したモニター対象トラフィックのデバイスのドメイン。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。
影響（Impact）	侵入データ、ディスカバリ データ、および脆弱性情報の間の相関に基づいて相関イベントに割り当てられた影響レベル。 このフィールドを検索する場合、大文字と小文字を区別しない有効な値は、`Impact 0`、`Impact Level 0`、`Impact 1`、`Impact Level 1`、`Impact 2`、`Impact Level 2`、`Impact 3`、`Impact Level 3`、`Impact 4`、および `Impact Level 4` です。影響アイコンの色または部分文字列は使用しないでください（たとえば、`blue`、`level 1`、または `0` を使用しないでください）。
入力インターフェイス（Ingress Interface）または出力インターフェイス（Egress Interface）	ポリシー違反をトリガーとして使用した侵入イベントまたは接続イベントの入力または出力インターフェイス。

フィールド	説明
入力セキュリティ ゾーン（Ingress Security Zone）または出力セキュリティ ゾーン（Egress Security Zone）	ポリシー違反をトリガーとして使用した侵入イベントまたは接続イベントの入力または出力セキュリティ ゾーン。
インライン結果	次のいずれかになります。 • 黒の下矢印：侵入ルールをトリガーとして使用したパケットがシステムによってドロップされたことを示します • グレーの下矢印：侵入ポリシー オプション [インライン時にドロップ（Drop when Inline）] を有効にした場合、インライン型、スイッチ型、またはルーティング型展開でパケットがシステムによってドロップされたと想定されることを示します • 空白：トリガーとして使用された侵入ルールが [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されていなかったことを示します 侵入イベントによってトリガーとして使用されたポリシー違反を検索するためにこのフィールドを使用する場合は、次のいずれかを入力します。 • `dropped`は、インライン型、スイッチ型、またはルーティング型展開でパケットがドロップされたかどうかを示します。 • would have dropped は仮定を表します。インライン型、スイッチ型、またはルーティング型展開でパケットをドロップするよう侵入ポリシーが設定されていると仮定した場合、パケットがドロップされるかどうかを示します。 侵入ポリシーのドロップ動作やルール状態とは無関係に、パッシブ展開（インライン セットがタップ モードである場合を含む）ではシステムがパケットをドロップしないことに注意してください。
ポリシー	違反が発生したポリシーの名前。
[プライオリティ（Priority）]	相関イベントのプライオリティ。これは、トリガーとして使用されたルールのプライオリティまたは違反が発生した相関ポリシーのプライオリティによって決まります。このフィールドを検索するとき、プライオリティなしの場合は `none` を入力します。
ルール（Rule）	ポリシー違反をトリガーとして使用したルールの名前。
セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）	ポリシー違反をトリガーしたイベントでブロックされたIPアドレスを表すか、またはそれを含むオブジェクトの名前。 このフィールドを検索する場合は、ポリシー違反をトリガーとして使用した相関イベントに関連付けられたセキュリティ インテリジェンスのカテゴリを指定します。セキュリティ インテリジェンスのカテゴリとして、セキュリティ インテリジェンス オブジェクト、グローバルブロックリスト、カスタム セキュリティ インテリジェンス リストまたはフィード、あるいはインテリジェンス フィードに含まれるいずれかのカテゴリを指定できます。

フィールド	説明
送信元の大陸（Source Continent）または宛先の大陸（Destination Continent）	ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホストIPアドレスに関連付けられた大陸。
送信元の国（Source Country）または宛先の国（Destination Country）	ポリシー違反をトリガーとして使用したイベントの送信元または宛先IPアドレスに関連付けられた国。
送信元ホストのシビラティ（重大度）（Source Host Criticality）または宛先ホストのシビラティ（重大度）（Destination Host Criticality）	相関イベントに関連する送信元または宛先ホストにユーザが割り当てたホスト重要度。`None`、`Low`、`Medium`、または `High` のいずれかです。 ディスカバリイベント、ホスト入力イベント、または接続イベントに基づくルールによって生成された相関イベントにのみ、送信元ホスト重要度が含まれることに注意してください。
送信元IP（Source IP）または宛先IP（Destination IP）	ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホストのIPアドレス。
送信元ポート/ICMPタイプ（Source Port/ICMP Type）または宛先ポート/ICMPコード（Destination Port/ICMP Code）	ポリシー違反をトリガーとして使用したイベントに関連付けられた、送信元トラフィックの送信元ポート/ICMPタイプまたは宛先トラフィックの宛先ポート/ICMPコード。
送信元ユーザ（Source User）または宛先ユーザ（Destination User）	ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホストにログインしたユーザの名前。
時刻（Time）	相関イベントが生成された日時。このフィールドは検索できません。
カウント（Count）	各行に表示される情報と一致するイベントの数。[カウント（Count）]フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません

関連トピック

イベントの検索 （845 ページ）

コンプライアンス許可（Allow）リストワークフローの使用

Management Centerは、ネットワークで生成されるallowリストのイベントおよび違反の分析で使用できるワークフローセットを提供します。ワークフローはネットワークマップやダッシュボードとともに、ネットワーク資産のコンプライアンスに関する主要な情報源になります。

システムは、allowリストのイベントと違反のために事前定義されたワークフローを提供します。ユーザはカスタム ワークフローを作成することもできます。コンプライアンスallowリストワークフローを使用すると、多くの一般的なアクションを実行できます。

始める前に

このタスクを実行するには、管理者、セキュリティ アナリスト（Security Analyst）、または検出管理者（Discovery Admin）ユーザーである必要があります。

手順

ステップ 1 **[分析（Analysis）]** > **[相関（Correlation）]** メニューを使用してallowリストワークフローにアクセスします。

ステップ 2 次の選択肢があります。

- ワークフローの切り替え：カスタム ワークフローなどの別のワークフローを使用するには、[(ワークフローの切り替え)（(switch workflow)）] をクリックします。
- 時間範囲：時間範囲を調整（イベントが表示されない場合に役立ちます）する方法については、時間枠の変更 （833 ページ）を参照してください。
- ホストプロファイル：IPアドレスのホストプロファイルを表示するには、**ホストプロファイル**（）をクリックします。アクティブな侵害の兆候（IOC）タグのあるホストの場合は、IP アドレスの横に表示される**侵害されたホスト**をクリックします。
- ユーザ プロファイル（イベントのみ）：ユーザー ID 情報を表示するには、[ユーザーID（User Identity）] の隣に表示される [ユーザー（User）] アイコン、または IOC に関連付けられているユーザーの場合は [レッドユーザー（Red User）] をクリックします。
- 制約：表示される列を制約するには、非表示にする列の見出しにある[閉じる（Close）]（）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。

  ヒント 他のカラムを表示または非表示にするには、[適用（Apply）]をクリックする前に、該当するチェックボックスをオンまたはオフにします。無効になったカラムをビューに再び追加するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のカラム名をクリックします。

- ドリル ダウン：ドリルダウン ページの使用 （818 ページ）を参照してください。
- ソート：ワークフローでデータをソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。
- このページに移動する：ワークフロー ページのトラバーサル ツール （815 ページ）を参照してください。
- ページ間で移動する：現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。

- イベントビュー間で移動する：関連するイベントを表示するためその他のイベントビューに移動するには、[ジャンプ（Jump to）] をクリックし、ドロップダウン リストからイベント ビューを選択します。
- イベントの削除（イベントのみ）：現在の制約されているビューにある一部またはすべての項目を削除するには、削除する項目の横にあるチェックボックスをオンにし、[削除（Delete）] または [すべて削除（Delete All）] をクリックします。

関連トピック

ワークフローのページ （813 ページ）
イベント ビューの設定 （241 ページ）

許可（Allow）リストイベントの表示

最初の評価が行われた後、監視対象ホストがアクティブなallowリストに準拠しなくなると、システムはallowリストイベントを生成します。リストイベントは、相関イベントの特殊な形態で、Management Center 相関イベントデータベースに記録されます。

Management Center を使用して、コンプライアンスallowリストイベントのテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

allowリストイベントにアクセスしたときに表示されるページは、使用しているワークフローによって異なります。イベントのテーブル ビューで終わる事前定義されたワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

始める前に

このタスクを実行するには、管理者、セキュリティ アナリスト（Security Analyst）、または検出管理者（Discovery Admin）ユーザーである必要があります。

手順

ステップ 1 **[分析（Analysis）] > [相関（Correlation）] > 許可リスト（Allow List）[イベント（Events）]**を選択します。

ステップ 2 次の選択肢があります。

- 基本的なワークフロー操作を実行するには、コンプライアンス許可（Allow）リストワークフローの使用 （1157 ページ）を参照してください。
- テーブルのカラムの内容について詳しく調べるには、許可（Allow）リストイベントのフィールド （1160 ページ）を参照してください。

- その他のオプションを表示するには、テーブル内の値を右クリックします。

許可（Allow）リストイベントのフィールド

ワークフローを使用して表示および検索できる許可（Allow）リストイベントには、次のフィールドがあります。

デバイス

allowリスト違反を検出した管理対象デバイスの名前。

説明

allowリスト違反の説明。次に例を示します。

```
Client “AOL Instant Messenger” is not allowed.
```

アプリケーションプロトコルに関係する違反には、アプリケーションプロトコルの名前とバージョンだけでなく、使用されているポートとプロトコル（TCP または UDP）も示されます。禁止を特定のオペレーティング システムに限定する場合は、説明にオペレーティング システム名が含まれます。次に例を示します。

```
Server "ssh / 22 TCP (OpenSSH 3.6.1p2)" is not allowed on Operating
System “Linux Linux 2.4 or 2.6”.
```

ドメイン（Domain）

allowリストに準拠しなくなったホストのドメイン。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

ホストの重要度（Host Criticality）

allowリストに準拠していないホストに対してユーザーが割り当てた重要度（[なし（None）]、[低（Low）]、[中（Medium）]、または [高（High）]）。

IP アドレス

allowリストに準拠しなくなったホストの IP アドレス。

ポリシー

違反した相関ポリシー、つまりallowリストを含む相関ポリシーの名前。

[ポート（Port）]

アプリケーションプロトコルallowリスト違反（非準拠アプリケーションプロトコルの結果として発生した違反）をトリガーした検出イベントに関連付けられているポート（存在する場合）。他のタイプのallowリスト違反の場合、このフィールドは空白です。

プライオリティ

ポリシーまたはポリシー違反をトリガーしたallowリストに指定されている優先順位。これは、相関ポリシー内のallowリストの優先順位または相関ポリシー自体の優先順位によって決まります。allowリストの優先順位は、そのポリシーの優先順位より優先されることに注意してください。このフィールドを検索するとき、プライオリティなしの場合は `none` を入力します。

Time

allowリストイベントが生成された日時。このフィールドは検索できません。

ユーザー（User）

allowリストに準拠しなくなったホストにログインしている既知のユーザーのアイデンティティ。

許可（Allow）リスト

allowリストの名前。

カウント（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

許可（Allow）リスト違反の表示

システムは、ネットワークの現在のallowリスト違反のレコードを保持します。違反はそれぞれ、ホストのいずれかで実行することが禁止されている事柄を表します。ホストが準拠するようになると、システムは、修正された違反をデータベースから削除します。

Management Center を使用して、アクティブなすべてのallowリストに対するallowリスト違反のテーブルを表示できます。ここでユーザは、検索する情報に応じてイベントビューを操作することができます。

allowリスト違反にアクセスしたときに表示されるページは、使用しているワークフローによって異なります。事前定義されたワークフローはホスト ビューで終了しますが、このホスト ビューには、制約を満たすすべてのホストに対して1つずつホストプロファイルが含まれています。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[分析（Analysis）]** > **[相関（Correlation）]** > [違反（Violations）]**許可リスト（Allow List）**を選択します。

ステップ 2 次の選択肢があります。

- 基本的なワークフロー操作を実行するには、コンプライアンス許可（Allow）リストワークフローの使用 （1157 ページ）を参照してください。
- テーブルのカラムの内容について詳しく調べるには、許可（Allow）リスト違反のフィールド （1162 ページ）を参照してください。
- その他のオプションを表示するには、テーブル内の値を右クリックします。

許可（Allow）リスト違反のフィールド

ワークフローを使用して表示および検索できる許可（Allow）リスト違反には、次のフィールドがあります。

ドメイン

非準拠ホストが存在するドメイン。このフィールドは、マルチテナンシーのためにManagement Centerを設定したことがある場合に表示されます。

情報

allowリスト違反に関連付けられたすべての利用可能なベンダー、製品、またはバージョン情報。allowリストに違反するプロトコルの場合、このフィールドには、違反の原因がネットワークプロトコルとトランスポートプロトコルのどちらであるのかも示されます。

[IPアドレス（IP Address）]

非準拠ホストのIPアドレス。

[ポート（Port）]

アプリケーション プロトコルallowリスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーしたイベントに関連付けられているポート（存在する場合）。他のタイプのallowリスト違反の場合、このフィールドは空白です。

プロトコル

アプリケーション プロトコルallowリスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーしたイベントに関連付けられているプロトコル（存在する場合）。他のタイプのallowリスト違反の場合、このフィールドは空白です。

時刻（Time）

allowリスト違反が検出された日時。

タイプ

allowリスト違反のタイプ、つまり、非準拠の結果として違反が発生したかどうか。

- オペレーティング システム（os）（このフィールドを検索する場合は、**os** または **operating system** と入力してください）。
- アプリケーション プロトコル（サーバ）
- クライアント
- プロトコル
- Web アプリケーション（web）（このフィールドを検索する場合は、**web application** と入力してください）。

許可（Allow）リスト

違反されたallowリストの名前。

カウント（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

修復ステータス イベント

修復がトリガーされると、システムは修復ステータスイベントをデータベースに記録します。これらのイベントは、[修復ステータス（Remediation Status）] ページで確認できます。修復ステータス イベントを検索、表示、削除できます。

関連トピック

修復ステータスのテーブル フィールド （1164 ページ）

修復ステータス イベントの表示

修復ステータスイベントにアクセスするときに表示されるページは、使用するワークフローにより異なります。修復のテーブル ビューを含む定義済みワークフローを使用できます。テーブル ビューには、各修復ステータス イベントの行が含まれます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

始める前に

このタスクを実行するには、管理者 ユーザーである必要があります。

手順

ステップ 1 **[分析（Analysis）]** > **[相関（Correlation）]** > **[ステータス（Status）]**を選択します。

ステップ 2 オプションで、時間枠の変更 （833 ページ）の説明に従って、時間範囲を調整します。

ステップ 3 オプションで、カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [(ワークフローの切り替え)（(switch workflow)）] をクリックします。

ヒント 修復のテーブル ビューが含まれないカスタム ワークフローを使用する場合、ワークフローのタイトルの横の [(ワークフローの切り替え)（(switch workflow)）] メニューをクリックし、[修復ステータス（Remediation Status）] を選択します。

ステップ 4 次の選択肢があります。

- 表示されるカラムの詳細については、修復ステータスのテーブル フィールド （1164 ページ）を参照してください。
- イベントをソートしたり、制約したりするには、ワークフローの使用 （809 ページ）を参照してください。
- 相関イベント ビューに移動し関連するイベントを確認するには、[相関イベント（Correlation Events）] をクリックします。
- 現在のページにすぐに戻れるようにページをブックマークするには、[このページをブックマーク（Bookmark This Page）] をクリックします。ブックマークの管理ページに移動するには、[ブックマークの表示（View Bookmarks）] をクリックします。
- テーブル ビューのデータに基づいてレポートを生成するには、イベント ビューからのレポート テンプレートの作成 （647 ページ） で説明されているように、[レポート デザイナ（Report Designer）] をクリックします。
- ワークフローの次のページにドリルダウンするには、ドリルダウン ページの使用 （818 ページ）を参照してください。
- システムから修復ステータス イベントを削除するには、削除するイベントの横にあるチェックボックスをオンにして [削除（Delete）] をクリックするか、[すべて削除（Delete All）] をクリックして現在の制約されているビューにあるすべてのイベントを削除することを確認します。
- 修復ステータス イベントを検索するには、[検索（Search）] をクリックします。

関連トピック

ワークフローの使用 （809 ページ）

修復ステータスのテーブル フィールド

次の表に、表示および検索できる修復のステート テーブルのフィールドを示します。

表 *126* : 修復ステータス フィールド

フィールド	説明
ドメイン	監視対象のトラフィックがポリシー違反をトリガーとして使用し、次に修復をトリガーとして使用するデバイスのドメイン。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。
ポリシー	違反し、修復をトリガーとして使用した相関ポリシーの名前。
修復名	起動された修復の名前。
結果メッセージ	修復が起動したときに発生した事象を示すメッセージ。ステータス メッセージには以下が含まれます。 • `Successful completion of remediation` • `Error in the input provided to the remediation module` • `Error in the remediation module configuration` • `Error logging into the remote device or server` • `Unable to gain required privileges on remote device or server` • `Timeout logging into remote device or server` • `Timeout executing remote commands or servers` • `The remote device or server was unreachable` • `The remediation was attempted but failed` • `Failed to execute remediation program` • `Unknown/unexpected error` カスタム修復モジュールがインストールされている場合、カスタム モジュールによって実装される追加のステータス メッセージが表示される場合があります。
ルール（Rule）	修復をトリガーとして使用したルールの名前。
時刻（Time）	Management Centerが修復を起動した日付と時刻。
カウント（Count）	各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

関連トピック

イベントの検索 （845 ページ）

修復ステータス イベント テーブルの使用

イベント ビューのレイアウトを変更したり、ビュー内のイベントをフィールド値で制限したりできます。

カラムを無効にすると、そのカラムは（後で元に戻さない限り）そのセッションの期間中は無効になります。最初のカラムを無効にすると、[カウント（Count）] カラムが追加されます。

テーブル ビューの行内の値をクリックすると、テーブル ビューが制約されます（次のページにはドリルダウンされません）。

ヒント テーブル ビューでは、必ずページ名に「Table View」が含まれます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

始める前に

このタスクを実行するには、管理者 ユーザーである必要があります。

手順

ステップ 1 **[分析（Analysis）] > [相関（Correlation）] > [ステータス（Status）]**を選択します。

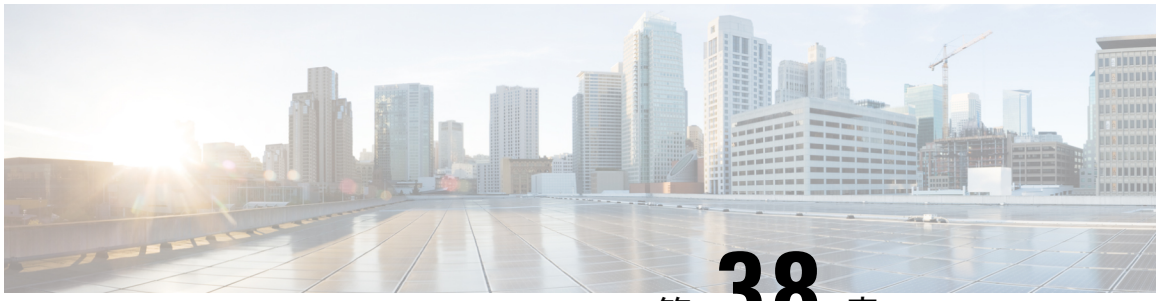
ヒント 修復のテーブル ビューが含まれないカスタム ワークフローを使用する場合、ワークフローのタイトルの横の [(ワークフローの切り替え)（(switch workflow)）] メニューをクリックし、[修復ステータス（Remediation Status）] を選択します。

ステップ 2 次の選択肢があります。

- 表示されるカラムの詳細については、修復ステータスのテーブル フィールド （1164 ページ）を参照してください。
- イベントをソートしたり、制約したりするには、ワークフローの使用 （809ページ）を参照してください。

第 IX 部

相関とコンプライアンス



第 38 章

コンプライアンスリスト

次のトピックでは、相関ポリシーに追加する前にコンプライアンス allow リストを設定する方法について説明します。

コンプライアンス許可（Allow）リストの概要

コンプライアンスallowリスト（allowリストと省略されることもある）は、どのオペレーティングシステム、アプリケーション（Webとクライアント）、およびプロトコルがネットワーク上のホストで許可されるかを指定する一連の条件です。システムはホストがこのリストにないとイベント（違反）を生成します。

コンプライアンスallowリストには 2 つの主要な構成要素があります。

- ターゲットは、コンプライアンス評価の対象として選択するホストです。サブネット、VLAN、およびホスト属性で制約して、全部または一部のモニター対象ホストを評価できます。マルチドメイン展開では、ドメインと、ドメイン内またはドメインをまたいだサブネットを対象にすることができます。
- ホスト プロファイルは、ターゲットのコンプライアンス基準を指定します。グローバルホストプロファイルはオペレーティングシステムに依存しません。また、各オペレーティングシステム専用のホストプロファイルを設定できます。これは、単一のallowリスト専用としても、複数のallowリストの共有プロファイルとしても設定できます。

Talos インテリジェンスグループ は、推奨設定が指定されたデフォルトのallowリストを提供しています。カスタムallowリストを作成することもできます。単純なカスタムリストでは、特定のオペレーティングシステムを実行するホストのみを許可できます。より複雑なリストでは、すべてのオペレーティングシステムを許可するとともに、特定のポートで特定のアプリケーションプロトコルを実行する際にホストが使用する必要のあるオペレーティングシステムを指定できます。

（注） システムは、エクスポートされたNetFlowレコードからネットワークマップにホストを追加できますが、これらのホストに使用できる情報は限られます（NetFlow データと管理対象デバイス データの違いを参照）。この制限は、コンプライアンスallowリストの作成方法に影響する場合があります。

コンプライアンス許可（Allow）リストの実装

allowリストを実装するには、アクティブな相関ポリシーにリストを追加します。システムはターゲットを評価し、対応する属性を各ホストに割り当てます。

- 準拠（Compliant）：ホストはリストに違反していません。
- 非準拠（Non-Compliant）：ホストはリストに違反しています。
- 評価されていない（Not Evaluated）：ホストがリストのターゲットではないか、現在評価中であるか、またはシステムに十分な情報がないためホストが準拠しているかどうかを判断できません。

（注） ホスト属性を削除するには、対応するallowリストを削除します。1 つのallowリストを非アクティブ化、削除、または相関ポリシーから削除しても、各ホストのホスト属性は削除**されず**、属性の値が変更されることもありません。

最初の評価後、モニター対象ホストがアクティブなallowリストに違反するたびにallowリストイベントが生成されます。また、allowリスト違反が記録されます。

ワークフロー、ダッシュボード、およびネットワークマップを使用して、システム全体のコンプライアンス アクティビティをモニターし、個々のホストがallowリストにいつどのように違反したのかを判断できます。修復およびアラートでこのような違反に自動的に応答することもできます。

例：Web サーバーへの HTTP の制限

セキュリティ ポリシーは、Web サーバーのみが HTTP を実行できることを指定しています。HTTP を実行しているホストを特定するために Web ファーム以外のネットワーク全体を評価するallowリストを作成します。

ネットワーク マップとダッシュボードを使用して、ネットワークのコンプライアンスの概要を一目で把握できます。数秒で、ポリシーに違反して HTTP を実行している組織内のホストを正確に特定して適切に対処できます。

その後で、相関機能を使用して、Web ファーム内に存在しないホストが HTTP の実行を開始するたびに警告するようにシステムを設定できます。

関連トピック

相関ポリシーの設定 （1191 ページ）

コンプライアンス許可（Allow）リストのターゲットネットワーク

ターゲットネットワークは、コンプライアンス評価の対象となるホストを指定します。allowリストには、複数のターゲットネットワークを含めることができ、いずれかのターゲットの基準を満たすホストが評価されます。

最初は、ターゲット ネットワークは IP アドレスまたはアドレス範囲で制約されています。マルチドメイン展開では、初期の制約にドメインも含まれます。

システム提供のデフォルトのallowリストでは、すべてのモニター対象ホスト（0.0.0.0/0および::/0）がターゲット設定されています。マルチドメイン展開では、デフォルトのallowリストはグローバルドメインに制約されています（グローバルドメインでのみ使用可能です）。

ホストがallowリストに対して有効ではなくなるようにターゲットネットワークまたはホストを変更すると、ホストはこのリストで評価されなくなり、準拠と非準拠のいずれとしても見なされなくなります。

ターゲット ネットワークの調査と改善

allowリストにターゲットネットワークを追加すると、システムにより、準拠ホストの特徴を確認できるようにネットワークマップを調査するよう求められます。調査により、ターゲットは、調査済みのホストを表すallowリストに追加されます。

サブネットまたは個別のホストを調査できます。マルチドメイン展開では、ドメイン全体を調査することも、ドメインをまたいで調査することもできます。先祖ドメインを調査すると、システムによってこのドメインの子孫が調査されます。

追加されたターゲットに加えて、調査では、調査で検出されたオペレーティングシステムごとに 1 つのホストプロファイルがallowリストに入力されます。デフォルトで、これらのホストプロファイルは、システムが該当するオペレーティング システム上で検出したクライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルのすべてを許可します。

ターゲット ネットワークを調査（または調査をスキップ）した後、対象を絞り込みます。IP アドレスを使用してホストを除外するか、ホスト属性または VLAN によりターゲット ネットワークを制約します。

コンプライアンス許可（Allow）リストを使用したドメインの対象化

マルチドメイン展開では、ドメインとターゲットネットワークは密接にリンクされています。

- リーフドメインの管理者は、自分のリーフドメイン内のホストを評価するallowリストを作成できます。
- 上位ドメインの管理者は、ドメインをまたいでホストを評価するallowリストを作成できます。同じ allow リストで、異なるドメイン内の異なるサブネットを対象にできます。

グローバル ドメインの管理者であり、展開全体の Web サーバに同じコンプライアンス基準を導入する必要があるというシナリオを考えてみます。コンプライアンス基準を定義するグローバルドメインに1つのallowリストを作成できます。次に、各リーフドメイン内の Web サーバーの IP スペース（または個別の IP アドレス）を指定するターゲットネットワークを使用して、allowリストを制約します。

（注） リーフ ドメインの IP アドレスと範囲を対象にすることに加えて、上位のドメインを使用してターゲットネットワークを制約することもできます。上位ドメインのサブネットを対象にすることにより、各子孫リーフ ドメインの同じサブネットが対象となります。システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

コンプライアンス 許可（Allow） リストのホストプロファイル

コンプライアンス allow リストにおいて、ホストプロファイルは、ターゲットホスト上で実行を許可するオペレーティングシステム、クライアント、アプリケーションプロトコル、Web アプリケーション、およびプロトコルを指定します。コンプライアンス allow リストで使用できるホストプロファイルは 3 種類あります。3 種類のホストプロファイルはそれぞれ、エディタ上での表示が異なります。

表 *127*：コンプライアンス 許可（*Allow*） リストのホストプロファイルタイプ

ホスト プロファイル タイプ	表示	説明
グローバル	すべてのオペレーティング システム	オペレーティング システムに関係なく、ターゲット ホスト上で実行が許可されている内容を指定します。
オペレーティング システム別	プレーン テキストで表示	特定のオペレーティング システムを使用するターゲット ホスト上で実行が許可されている内容を指定します。
共有	イタリックで表示	複数の allow リストで使用可能なオペレーティング システム条件を指定します。

オペレーティング システム固有のホスト プロファイル

コンプライアンスallowリストでは、オペレーティングシステム固有のホストプロファイルで、ネットワーク上での実行を許可するオペレーティングシステムだけでなく、それらのオペレーティングシステム上での実行を許可するアプリケーションプロトコル、クライアント、Web アプリケーション、およびプロトコルも指定します。

たとえば、準拠ホストでは Microsoft Windows の特定のバージョンを実行することを要件にすることができます。別の例として、SSH の実行を Linux ホストのポート 22 で許可した上で、SSH クライアントのベンダーとバージョンをさらに制限することもできます。

ネットワーク上での実行を許可するオペレーティング システムごとに 1 つのホスト プロファイルを作成します。ネットワーク上でオペレーティング システムを禁止する場合は、そのオペレーティング システム用のホスト プロファイルを作成しないでください。たとえば、ネットワーク上のすべてのホストで Windows が実行されるようにするには、そのオペレーティング システム用のホストプロファイルのみを含めるようにallowリストを設定します。

（注） 未確認ホストは、確認されるまで、すべてのallowリストに準拠していると見なされます。ただし、不明ホストのallowリストホストプロファイルを作成することはできます。未確認ホストとは、オペレーティング システムを識別するために十分な情報が収集されていないホストのことです。不明ホストとは、既知のフィンガープリントと一致しないオペレーティング システムを使用しているホストのことです。

共有ホスト プロファイル

コンプライアンスallowリストでは、共有ホストプロファイルが特定のオペレーティングシステムに関連付けられますが、それぞれの共有ホストプロファイルを複数のallowリスト内で使用できます。

たとえば、世界中にオフィスがあり、拠点ごとに別々のallowリストを使用する一方、Apple Mac OS X を実行しているすべてのホストに対しては常に同じプロファイルを使用するとします。その場合、該当するオペレーティングシステム用の共有プロファイルを作成し、そのプロファイルをすべてのallowリストで使用するという方法があります。

デフォルトallowリストでは、組み込みホストプロファイルと呼ばれる特殊なカテゴリの共有ホストプロファイルが使用されます。これらのプロファイルは、組み込みのアプリケーションプロトコル、Webアプリケーション、プロトコル、クライアントを使用します。コンプライアンスallowリストエディタでは、システムはこれらのプロファイルを**組み込みホストプロファイル アイコン**で示します。

マルチドメイン展開では、現在のドメインで作成された共有ホストプロファイルが表示されます。このプロファイルは編集できます。先祖ドメインで作成された共有ホストプロファイルも表示されますが、これは編集できません。下位のドメインで作成された共有ホストプロファイルを表示および編集するには、そのドメインに切り替えます。

（注） 共有ホストプロファイル（ビルトインを含む）を変更した場合、またはビルトインアプリケーションプロトコル、プロトコル、クライアントを変更した場合、これらのプロファイルを使用するすべてのallowリストに影響します。意図しない変更を加えた場合や、該当する組み込みの要素を削除した場合は、工場出荷時の初期状態にリセットできます。

許可（Allow）リスト違反のトリガー

ホストのallow リスト コンプライアンスは、システムで次のことが発生すると変化する場合があります。

- ホストのオペレーティング システムの変更を検出
- ホストのオペレーティング システムまたはホスト上のアプリケーション プロトコルに関するアイデンティティの競合を検出
- ホスト上でアクティブになっている新しい TCP サーバ ポート（SMTP または Web サーバによって使用されるポートなど）、または、ホスト上で実行中の新しい UDP サーバを検出
- ホスト上で実行中の検出された TCP サーバまたは UDP サーバで、アップグレードのためのバージョン変更などの変更を検出
- ホスト上で実行中の新しいクライアント アプリケーションまたは Web アプリケーションを検出
- クライアント アプリケーションまたは Web アプリケーションを非アクティブを理由にそのデータベースからドロップ
- ホストが新しいネットワークまたはトランスポート プロトコルと通信していることを検出
- 新しいジェイルブレイクされたモバイル デバイスを検出
- ホスト上で TCP ポートまたは UDP ポートが閉じられたか、タイムアウトしたことを検出

さらに、ホスト入力機能またはホストプロファイルを使用して次の操作を実行することによって、ホストのコンプライアンスの変化をトリガーできます。

- ホストにクライアント、プロトコル、またはサーバを追加する
- ホストからクライアント、プロトコル、またはサーバを削除する
- ホストのオペレーティング システム定義を設定する
- ホストが有効なターゲットでなくなるようにホストのホスト属性を変更する

（注） 非常に多数のイベントが発生しないように、システムでは、その最初の評価に基づいて非準拠のホストにallowリストイベントを生成せず、またユーザーがアクティブなallowリストまたは共有ホストプロファイルを変更した結果としてホストを非準拠にしません。ただし、違反は記録されます。すべての非準拠ターゲットに対してallowリストイベントを生成する場合は、検出データを消去してください。ネットワークアセットを再検出すると、allowリストイベントをトリガーすることがあります。

オペレーティングシステムのコンプライアンス

allowリストで Microsoft Windows ホストのみがネットワーク上で許可されるように指定されている場合、システムでは、Mac OS X を実行中のホストを検出するとallowリストイベントを生成します。さらに、allowリストに関連付けられているホスト属性が、そのホストに関して [準拠（Compliant）] から [非準拠（Non-Compliant）] に変更されます。

この例のホストが準拠に復帰するには、次のいずれかが行われる必要があります。

- Mac OS X オペレーティングシステムを許可するようにallowリストを編集する
- ホストのオペレーティング システム定義を手動で Microsoft Windows に変更する
- オペレーティング システムが変更されて Microsoft Windows に戻ったことをシステムが検出する

非準拠のアセットをネットワークマップから削除する

allowリストでFTPの使用が許可されていない場合に、アプリケーションプロトコルのネットワークマップ、またはイベントビューから FTP を削除すると、FTP を実行中のホストは準拠になります。ただし、システムがアプリケーションプロトコルをもう一度検出すると、allowリストイベントが生成され、ホストは非準拠になります。

完全な情報に基づいてのみトリガーを実行

allowリストでポート 21 で TCP FTP トラフィックだけを許可していた場合、システムでポート 21/TCP で不明なアクティビティを検出すると、allowリストはトリガーを実行しません。allowリストがトリガーを実行するのは、システムがトラフィックを FTP 以外のトラフィックとして識別するか、またはユーザーがホスト入力機能を使用してトラフィックを非 FTP トラフィックとして指定した場合だけです。システムは、部分的な情報のみを使用して違反を記録することはありません。

コンプライアンスの要件と前提条件

モデルのサポート

任意（Any）

サポートされるドメイン

任意

ユーザの役割

- 管理者

コンプライアンス許可（Allow）リストの作成

コンプライアンスallowリストを作成する際には、ネットワークを調べて最初のターゲットを作成するよう求めるプロンプトが表示されます。これは、コンプライアンスに準拠するホストの特徴を指定するのに役立ちます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[相関（Correlation）]** を選択し、[**許可リスト（Allow List**）] をクリックします。

ステップ 2 [新規（New）] **許可リスト（Allow List**） をクリックします。

ステップ 3 必要に応じて、最初のターゲット ネットワークの [IP アドレス（IP Address）] および [ネットマスク（Netmask）] を入力します。マルチドメイン導入では、ターゲット ネットワークが存在する [ドメイン（Domain）] を選択します。

ヒント モニタリング対象のネットワーク全体を調査するには、デフォルト値の 0.0.0.0/0 と ::/0 を使用します。

（注） ターゲットネットワークのドメインを選択した後は、ドメインを変更できません。より高いレベルのドメインのサブネットをターゲットにすると、**各**子孫リーフドメイン内の**同じ**サブネットがターゲットになります。システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 4 ターゲット ネットワークを追加します。

- [追加（Add）]：調査せずにターゲット ネットワークを追加する場合は、[追加（Add）] をクリックします。
- [ネットワークの追加および調査（Add and Survey Network）]：ターゲットネットワークを追加して調査する場合は、[ネットワークの追加および調査（Add and Survey Network）] をクリックします。
- [スキップ（Skip）]：ネットワークを調査せずにallowリストを作成する場合は、[スキップ（Skip）] をクリックします。

ステップ 5 必要に応じて、allowリストの新しい [名前（Name）] および [説明（Description）] を入力します。

ステップ 6 必要に応じて、[脱獄モバイルデバイスを許可（Allow Jailbroken Mobile Devices）] を選択して、ネットワークで脱獄モバイルデバイスを許可します。このオプションを無効にすると、ジェイルブレイク済みデバイスによってallowリスト違反が生成されます。

ステップ 7 コンプライアンス 許可（Allow） リストのターゲットネットワークの設定 （1177 ページ）の説明に従って、1 つ以上の [ターゲットネットワーク（Target Network）] をallowリストに追加します。

ステップ 8 [許可されるホストプロファイル（Allowed Host Profiles）] を使用して、準拠ホストの特徴を指定します。

- グローバル ホストプロファイル：allowリストのグローバル ホストプロファイルを編集するには、[任意のオペレーティングシステム（Any Operating System）] をクリックし、許可（Allow） リスト ホスト プロファイルの作成 （1179 ページ）の説明に従います。
- 調査済みプロファイルの編集：ネットワーク調査によって作成された既存のオペレーティング システム固有のホスト プロファイルを編集するには、その名前をクリックし、許可（Allow） リスト ホスト プロファイルの作成 （1179 ページ）の説明に従います。
- 新規プロファイルの作成：このallowリストに新しいオペレーティングシステム固有のホストプロファイルを作成するには、[許可されるホストプロファイル（Allowed Host Profiles）] の隣にある**Add** (＋)をクリックし、許可（Allow） リスト ホスト プロファイルの作成 （1179 ページ）の説明に従います。
- 共有ホストプロファイルの追加：allowリストに既存の共有ホストプロファイルを追加するには、[共有ホストプロファイルの追加（Add Shared Host Profile）] をクリックし、追加する共有ホストプロファイルを選択して、[OK] をクリックします。共有ホスト プロファイルは斜体で表示されます。

ステップ 9 [保存（Save）] **許可リスト（Allow List）**をクリックします。

次のタスク

- 相関ポリシーの設定 （1191 ページ）の説明に従って、アクティブな相関ポリシーにallowリストを追加します。システムはすぐにallowリストの評価および違反の生成を開始します。

関連トピック

コンプライアンス許可（Allow）リストのターゲットネットワーク （1171 ページ）
選択したホストに基づいたコンプライアンスの許可（Allow）リストの作成（1104ページ）
IP アドレスの規則 （31 ページ）

コンプライアンス 許可（Allow） リストのターゲットネットワークの設定

ターゲット ネットワークを追加するときには、ターゲット ネットワークを調査して、準拠しているホストを特定することができます。この調査によって、調査で検出された各オペレーティングシステムの1つのホストプロファイルがallowリストに追加されます。これらのホストプロファイルは、システムが該当するオペレーティング システム上で検出したクライアント、

アプリケーション プロトコル、Web アプリケーション、およびプロトコルのすべてを許可します。

手順

ステップ 1 コンプライアンス allow リスト エディタで、[ターゲットネットワークの追加（Add Target Network）] をクリックします。

ステップ 2 ターゲット ネットワークの [IP アドレス（IP Address）] と [ネットマスク（Netmask）] を入力します。

ステップ 3 マルチドメイン展開では、ターゲット ネットワークが存在する [ドメイン（Domain）] を選択します。

（注） ターゲットネットワークのドメインを選択した後は、ドメインを変更できません。より高いレベルのドメインのサブネットをターゲットにすると、**各**子孫リーフ ドメイン内の**同じ**サブネットがターゲットになります。システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 4 ターゲット ネットワークを追加します。

- 追加（Add）：調査なしでターゲット ネットワークを追加するには、[追加（Add）] をクリックします。
- ネットワークの追加と調査（Add and Survey Network）：ターゲット ネットワークを追加および調査するには、[ネットワークの追加と調査（Add and Survey Network）] をクリックします。

ステップ 5 必要に応じて、新しいターゲットをクリックしてさらに構成します。

- 名前（Name）：新しい [名前（Name）] を入力します。
- ネットワークの追加（Add Networks）：追加のホストをターゲットにするには、**Add** (＋) をクリックして、[IPアドレス（IP Address）] と [ネットマスク（Netmask）] を入力します。ネットワークをallow リスト コンプライアンスから除外するには、[除外（Exclude）] を選択します。
- ホスト属性の追加（Add Host Attributes）：特定のホスト属性を持つホストをターゲットにするには、**Add** (＋) をクリックして、[属性（Attribute）] とその [値（Value）] を指定します。
- VLANの追加（Add VLANs）：VLAN をターゲットにするには、**Add** (＋) をクリックして VLAN 番号を入力します（802.1q VLAN の場合）。
- 削除（Delete）：ターゲット制限を削除するには、[削除（Delete）]（🗑） をクリックします。

ステップ 6 前回の保存以降に行ったすべての変更をすぐに実装するには、[**許可リスト（Allow List**）の保存（Save White List）] をクリックします。

関連トピック

コンプライアンス許可（Allow）リストのターゲットネットワーク （1171 ページ）
IP アドレスの規則 （31 ページ）

許可（Allow） リスト ホスト プロファイルの作成

ホストプロファイルは、ターゲットホスト上での実行を許可するオペレーティングシステム、クライアント、アプリケーションプロトコル、Web アプリケーション、およびプロトコルといった、allow リストの適合基準を指定します。

すべての allow リストには、オペレーティングシステムに依存しないグローバル ホスト プロファイルがあります。たとえば、Mozilla Firefox を許可するように複数の Microsoft Windows ホストプロファイルと Linux ホストプロファイルを編集する代わりに、検出されたオペレーティング システムに関係なく、Firefox を許可するようにグローバル ホスト プロファイルを設定できます。

また、各オペレーティングシステム専用のホストプロファイルを設定できます。これは、単一の allow リスト専用としても、複数の allow リストの共有プロファイルとしても設定できます。

（注） 共有ホストプロファイル（ビルトインを含む）を変更した場合、またはビルトインアプリケーションプロトコル、プロトコル、クライアントを変更した場合、これらのプロファイルを使用するすべてのallowリストに影響します。意図しない変更を加えた場合や、該当する組み込みの要素を削除した場合は、工場出荷時の初期状態にリセットできます。

始める前に

- コンプライアンス許可（Allow） リストの編集 （1184 ページ）の説明に従い、allow リスト内でホストプロファイルを作成または編集します。または、共有ホストプロファイルの管理 （1186 ページ）の説明に従い、共有ホストプロファイルを作成または編集します。

手順

ステップ 1 allow リスト適合ホストプロファイルエディタで、以下のホストプロファイルを設定します。

- 名前：[名前（Name）] を入力します。
- オペレーティング システム：ホスト プロファイルを特定のオペレーティング システム専用にするには、[OS ベンダ（OS Vendor）]、[OS 名（OS Name）]、[バージョン（Version）] ドロップダウンリストを使用します。グローバルホストプロファイルはすべてのオペレー

ティングシステムを実行するホストへ適用されることを目的としたプロファイルであるため、これに制限を設定することはできません。

- アプリケーションプロトコル：アプリケーションプロトコルを許可するには、**Add** ( ) をクリックし、コンプライアンス許可（Allow）リストへのアプリケーションプロトコルの追加 （1180 ページ）の説明に従います。
- クライアント：クライアントを許可するには、**Add** ( ) をクリックし、コンプライアンス許可（Allow）リストへのクライアントの追加 （1181 ページ）の説明に従います。
- Web アプリケーション：Web アプリケーションを許可するには、**Add** ( ) をクリックし、コンプライアンス許可（Allow）リストへの Web アプリケーションの追加 （1182 ページ）の説明に従います。
- プロトコル：プロトコルを許可するには、**Add** ( ) をクリックし、コンプライアンス許可（Allow）リストへのプロトコルの追加 （1182 ページ）の説明に従います。
- 削除：一度許可した項目への許可を解除するには、[削除（Delete）] （ ） をクリックします。
- プロパティの編集：許可されているアプリケーションプロトコルのプロパティ、クライアント、プロトコルを編集するには、その名前をクリックします。変更は、変更した要素を使用する各ホストプロファイルに反映されます。

ヒント プロファイルに一致するホストにすべてのアプリケーションプロトコル、クライアント、web アプリケーションを許可するには、該当する [すべて許可（Allow all...）] チェックボックスを選択します。

ステップ 2 最後の保存以降に施した変更をすぐに適用するには、[許可リストの保存（Save **許可リスト（Allow List）**）] （または、共有ホストプロファイルを編集している場合は [すべてのプロファイルを保存（Save All Profiles）]）をクリックします。

コンプライアンス許可（Allow）リストへのアプリケーションプロトコルの追加

allow リストホストプロファイルを使用して、グローバルにまたは特定のオペレーティングシステムに対して、アプリケーションプロトコルを許可できます。オプションで、ポート、ベンダー、バージョンによって、アプリケーションプロトコルを制限できます。たとえば、ポート 22/TCP で、Linux ホスト上で実行する OpenSSH の特定のバージョンを許可することができます。

手順

ステップ 1 コンプライアンス allow リストホストプロファイルを作成または変更しているときに、[許可されるアプリケーションプロトコル（Allowed Application Protocols）] （またはグローバル ホスト

プロファイルを変更している場合は [グローバルに許可されるアプリケーションプロトコル（Globally Allowed Application Protocols）] の横にある **Add** ( ) をクリックします。

ステップ 2 次の 2 つの対処法があります。

- 許可するアプリケーション プロトコルが表示されたら、これらを選択します。Web インターフェイスには、allowリストによって、過去に許可されたアプリケーションプロトコル、または今許可しようとしているアプリケーションプロトコルが表示されます。
- リストにないアプリケーション プロトコルを許可するには、[<新規アプリケーション プロトコル>（<New Application Protocol>）] を選択し、[OK] をクリックしてアプリケーション プロトコル エディタを表示します。許可するアプリケーション プロトコル [タイプ（Type）] と [プロトコル（Protocol）] を選択します。オプションで、[ポート（port）]、[ベンダー（Vendor）]、[バージョン（Version）] によって、アプリケーション プロトコルを制限します。

  （注） アプリケーションのテーブル ビューに表示されているとおり正確にベンダーやバージョンを入力する必要があります。ベンダーまたはバージョンを指定しなかった場合は、タイプとプロトコルが一致している限り、allowリストではすべてのベンダーとバージョンが許可されます。

ステップ 3 [OK] をクリックします。

ステップ 4 前回の保存以降に行ったすべての変更をすぐに実装するには、[**許可リスト（Allow List**）の保存（Save White List）] をクリックします。

コンプライアンス許可（Allow）リストへのクライアントの追加

allowリスト ホスト プロファイルを使用して、グローバルにまたは特定のオペレーティングシステムに対して、クライアントを許可できます。オプションで、クライアントを特定のバージョンに限定することができます。たとえば、Microsoft Windows ホスト上での実行を Microsoft Internet Explorer 10 のみに許可することができます。

手順

ステップ 1 コンプライアンスallowリストホストプロファイルを作成または変更しているときに、[許可されるクライアント（Allowed Clients）]（またはグローバル ホスト プロファイルを変更している場合は [グローバルに許可されるクライアント（Globally Allowed Clients）]）の横にある**Add** ( )をクリックします。

ステップ 2 次の 2 つの対処法があります。

- 許可するクライアントが表示されたら、これらを選択します。Web インターフェイスには、allowリストによって、過去に許可されたクライアント、または今許可しようとしているクライアントが表示されます。

- リストにないクライアントを許可するには、[<新規クライアント>（<New Client>）] を選択し、[OK] をクリックしてクライアント エディタを表示します。ドロップダウン リストから許可する [クライアント（Client）] を選択し、オプションで許可するクライアントの [バージョン（Version）] を制限します。

  （注） クライアントのテーブル ビューに表示されているとおり正確にバージョンを入力する必要があります。バージョンを指定しない場合、すべてのバージョンが許可されます。

ステップ 3 [OK] をクリックします。

ステップ 4 前回の保存以降に行ったすべての変更をすぐに実装するには、[**許可リスト（Allow List**）の保存（Save White List）] をクリックします。

コンプライアンス許可（Allow）リストへの Web アプリケーションの追加

allowリストホストプロファイルを使用して、グローバルにまたは特定のオペレーティングシステムに対して、Web アプリケーションを許可できます。

手順

ステップ 1 コンプライアンスallowリストホストプロファイルを作成または変更しているときに、[許可されるWebアプリケーション（Allowed Web Applications）]（またはグローバル ホスト プロファイルを変更している場合は [グローバルに許可されるWebアプリケーション（Globally Allowed Web Applications）]）の横にある**Add** (＋)をクリックします。

ステップ 2 許可する Web アプリケーションを選択します。

ステップ 3 [OK] をクリックします。

ステップ 4 前回の保存以降に行ったすべての変更をすぐに実装するには、[**許可リスト（Allow List**）の保存（Save White List）] をクリックします。

コンプライアンス許可（Allow）リストへのプロトコルの追加

allowリスト ホスト プロファイルを使用して、グローバルにまたは特定のオペレーティングシステムに対して、プロトコルを許可できます。ARP、IP、TCP、UDP は、常にすべてのホスト上での実行が許可されます。これらを禁止することはできません。

手順

ステップ 1 コンプライアンスallowリストホストプロファイルを作成または変更しているときに、[許可されるプロトコル（Allowed Protocols）]（またはグローバル ホスト プロファイルを変更してい

る場合は[グローバルに許可されるプロトコル（Globally Allowed Protocols）]）の横にある **Add** (＋) をクリックします。

ステップ 2 次の 2 つの対処法があります。

- 許可するプロトコルが表示されたら、これらを選択します。Webインターフェイスには、allowリストによって、過去に許可されたプロトコル、または今許可しようとしているプロトコルが表示されます。
- リストにないプロトコルを許可するには、[<新規プロトコル>（<New Protocol>）] を選択し、[OK] をクリックしてプロトコル エディタを表示します。[タイプ（Type）] ドロップダウン リストから、プロトコル タイプ（[ネットワーク（Network）] や [トランスポート（Transport）]）を選択し、ドロップダウン リストから [プロトコル（Protocol）] を選択します。

  ヒント リスト内に存在しないプロトコルを指定するには、[その他(手動入力)（Other(manual entry)）] を選択します。ネットワーク プロトコルの場合は、http://www.iana.org/assignments/ethernet-numbers/ に記載されている適切な番号を入力します。トランスポート プロトコルの場合は、http://www.iana.org/assignments/protocol-numbers/ に記載されている適切な番号を入力します。

ステップ 3 [OK] をクリックします。

ステップ 4 前回の保存以降に行ったすべての変更をすぐに実装するには、[**許可リスト（Allow List**）の保存（Save White List）] をクリックします。

コンプライアンス 許可（Allow） リストの管理

[許可（Allow）リスト（White List）] ページは、コンプライアンス allow リストと共有ホストプロファイルの管理に使用できます。デフォルトallowリストは、推奨設定を表すものであり、組み込みホストプロファイルと呼ばれる特殊なカテゴリの共有ホストプロファイルを使用します。

マルチドメイン展開では、現在のドメインで作成されたコンプライアンス allow リストが表示されます。これは、編集が可能なリストです。また、先祖ドメインからの選択したallowリストも表示されますが、これは編集できません。下位のドメインで作成されたallow リストを表示および編集するには、そのドメインに切り替えます。

（注） 設定に無関係なドメイン（名前、管理対象デバイスなど）に関する情報が公開されている場合、システムは先祖ドメインからの設定を表示しません。デフォルト allow リストは、グローバルドメインでのみ使用できます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[相関（Correlation）]** を選択し、[**許可リスト（Allow List）**] をクリックします。

ステップ 2 コンプライアンス allow リストを管理します。

- 作成：新しいallowリストを作成するには、[新規**許可リスト（Allow List）**（New White List）] をクリックして、コンプライアンス許可（Allow）リストの作成（1176ページ）で説明する手順を実行します。
- 削除：使用していないallowリストを削除するには、[削除（Delete）]（）をクリックして、allowリストの削除を確認します。また、allowリストを削除すると、ネットワーク上のすべてのホストから、そのリストに関連付けられたホスト属性も削除されます。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 編集：既存のallowリストを変更するには、**[編集（Edit）]**（）をクリックし、コンプライアンス許可（Allow）リストの編集（1184ページ）で説明する手順を実行します。代わりに [表示（View）]（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 共有ホストプロファイル：allowリストの共有ホストプロファイルを管理するには、[共有プロファイルの編集（Edit Shared Profiles）] をクリックして、共有ホストプロファイルの管理（1186ページ）で説明する手順を実行します。

コンプライアンス 許可（Allow） リストの編集

アクティブな相関ポリシーに含まれるコンプライアンス allow リストを修正して保存すると、システムは、allowリストのターゲットネットワークのホストのコンプライアンスを再評価します。この再評価で一部のホストがコンプライアンス準拠または違反とされた場合でも、allowリストイベントは生成されません。

手順

ステップ 1 **[ポリシー（Policies）]** > **[相関（Correlation）]** を選択し、[**許可リスト（Allow List）**] をクリックします。

ステップ 2 変更するallowリストの横にある **[編集（Edit）]**（）をクリックします。

代わりに [表示（View）]（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 コンプライアンス allow リストを編集します。

- 名前と説明：名前または説明を変更するには、左側のパネルでallowリストの名前をクリックしてallowリストの基本情報を表示し、新しい情報を入力します。
- ジェイルブレイクされたデバイスの許可：ネットワーク上でジェイルブレイクされたモバイルデバイスを許可するには、左側のパネルでallowリストの名前をクリックしてallowリストの基本情報を表示し、[ジェイルブレイクされたモバイルデバイスを許可（Allow Jailbroken Mobile Devices）] を有効にします。このオプションを無効にすると、ジェイルブレイク済みデバイスによってallowリスト違反が生成されます。
- 許可されるホストプロファイルの追加：このallowリストに新しいオペレーティングシステム固有のホストプロファイルを作成するには、[許可されるホストプロファイル（Allowed Host Profiles）] の隣にある **Add** (＋) をクリックし、許可（Allow） リスト ホスト プロファイルの作成 （1179 ページ）の説明に従います。
- 共有ホストプロファイルの追加：allowリストに既存の共有ホストプロファイルを追加するには、[共有ホストプロファイルの追加（Add Shared Host Profile）] をクリックし、追加する共有ホストプロファイルを選択して [OK] をクリックします。共有ホスト プロファイルは斜体で表示されます。
- ターゲットネットワークの追加：ホストを調査することなく新しいターゲットネットワークを追加するには、ターゲットネットワークの横にある **Add** (＋) をクリックし、コンプライアンス 許可（Allow） リストのターゲットネットワークの設定 （1177 ページ）の説明に従って続行します。
- ホストプロファイルの削除：allowリストから共有またはオペレーティングシステム固有のホストプロファイルを削除するには、ホストプロファイルの横にある [削除（Delete）]（🗑） をクリックし、選択内容を確認します。共有ホストプロファイルを削除すると、それがallowリストから除外されますが、プロファイルは削除されず、それを使用する他のallowリストからも除外されません。allowリストのグローバル ホスト プロファイルは削除できません。
- ターゲットネットワークの削除：allowリストからターゲットネットワークを削除するには、ネットワークの横にある [削除（Delete）]（🗑） をクリックし、選択内容を確認します。
- グローバル ホスト プロファイルの編集：allowリストのグローバル ホスト プロファイルを編集するには、[任意のオペレーティングシステム（Any Operating System）] をクリックし、許可（Allow） リスト ホスト プロファイルの作成 （1179 ページ）の説明に従います。
- 他のホスト プロファイルの編集：共有またはオペレーティング システム固有のホスト プロファイルを編集するには、ホストプロファイルの名前をクリックし、許可（Allow） リスト ホスト プロファイルの作成 （1179 ページ）の説明に従って続行します。
- ターゲット ネットワークの編集：ターゲット ネットワークを編集するには、ネットワークの名前をクリックし、コンプライアンス 許可（Allow） リストのターゲットネットワークの設定 （1177 ページ）の指示に従って続行します。

ステップ 4 前回の保存以降に行ったすべての変更をすぐに実装するには、[**許可リスト（Allow List**）の保存（Save White List）] をクリックします。

共有ホスト プロファイルの管理

コンプライアンスallowリストでは、共有ホストプロファイルが特定のオペレーティングシステムに関連付けられますが、それぞれの共有ホストプロファイルを複数のallowリスト内で使用できます。複数の allow リストを作成するが、同じホストプロファイルを使用して複数の allow リストで特定のオペレーティングシステムを実行するホストを評価する場合は、共有のホストプロファイルを使用します。

マルチドメイン展開では、現在のドメインで作成された共有ホストプロファイルが表示されます。このプロファイルは編集できます。先祖ドメインで作成された共有ホストプロファイルも表示されますが、これは編集できません。下位のドメインで作成された共有ホストプロファイルを表示および編集するには、そのドメインに切り替えます。

（注） 共有ホストプロファイル（ビルトインを含む）を変更した場合、またはビルトインアプリケーションプロトコル、プロトコル、クライアントを変更した場合、これらのプロファイルを使用するすべてのallowリストに影響します。意図しない変更を加えた場合や、該当する組み込みの要素を削除した場合は、工場出荷時の初期状態にリセットできます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[相関（Correlation）]** を選択し、[**許可リスト（Allow List**）] をクリックします。

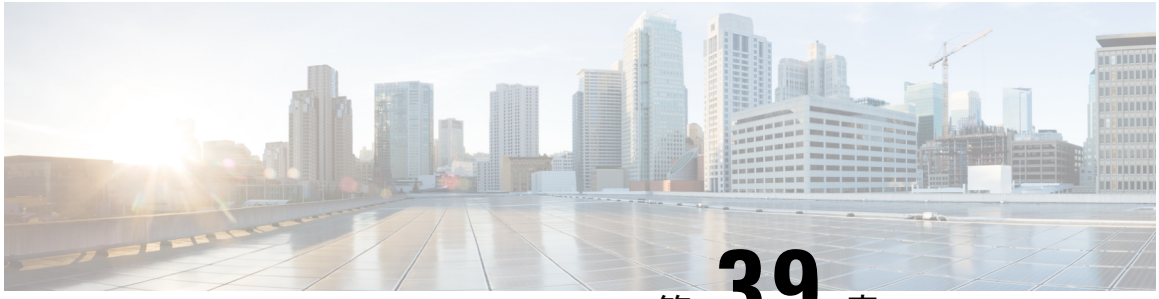
ステップ 2 [共有プロファイルの編集（Edit Shared Profiles）] をクリックします。

ステップ 3 共有ホスト プロファイルを管理します。

- 共有ホストプロファイルの作成：ホストの調査なしで新しい共有ホストプロファイルを作成するには、[共有ホストプロファイル（Shared Host Profiles）] の横にある **Add** ( ) をクリックし、許可（Allow） リスト ホストプロファイルの作成 （1179 ページ） で説明する手順を実行します。
- 調査によるホストプロファイルの作成：ネットワークの調査によって複数の新しい共有ホストプロファイルを作成するには、[ターゲットネットワークの追加（Add Target Network）] をクリックして、コンプライアンス 許可（Allow） リストのターゲットネットワークの設定 （1177 ページ） で説明する手順を実行します。
- 削除：共有ホストプロファイルを削除するには、[削除（Delete）] （ ） をクリックして、選択内容を確認します。

- 編集：既存の共有ホスト プロファイル（組み込み共有ホスト プロファイルを含む）を変更するには、そのプロファイルの名前をクリックして、許可（Allow）リスト ホスト プロファイルの作成 （1179 ページ）で説明する手順を実行します。
- 組み込みのホスト プロファイルのリセット：すべての組み込みホスト プロファイルを工場出荷時の初期状態にリセットするには、[組み込みホストプロファイル（Built-in Host Profiles）] をクリックして、[工場出荷時の初期状態にリセット（Reset to Factory Defaults）] をクリックしてから、選択内容を確認します。

ステップ 4 最後の保存以降に行われたすべての変更をすぐに実装するには、[すべてのプロファイルの保存（Save All Profiles）] をクリックします。



第 39 章

相関ポリシー

次のトピックでは、相関ポリシーおよびルールの設定方法について説明します。

相関ポリシーとルールの概要

相関機能を使用することで、ネットワークへの脅威に対して相関ポリシーを使用してリアルタイムで応答できます。

ネットワーク上のアクティビティによって、アクティブな相関ポリシー内の相関ルールまたはコンプライアンス allow リストのいずれかがトリガーされると、相関ポリシー違反が発生します。

相関ルール

アクティブな相関ポリシー内の相関ルールがトリガーされると、システムによって相関イベントが生成されます。相関ルールは、以下の場合にトリガーされます。

- 特定のタイプのイベント（接続、侵入、マルウェア、ディスカバリ、ユーザ アクティビティなど）がシステムによって生成された。
- ネットワーク トラフィックが通常のプロファイルから逸脱している。

以下の方法で相関ルールを制約することもできます。

- ホスト プロファイル限定を追加すると、トリガー イベントに関連するホストのプロファイルからの情報に基づいてルールを制約できます。
- 接続トラッカーを相関ルールに追加すると、ルールの初期基準に一致した場合、システムは特定の接続を追跡し始めます。その後、追跡対象の接続がさらに追加の基準を満たす場合にのみ、相関イベントが生成されます。

- ユーザ限定を相関ルールに追加すると、特定のユーザまたはユーザ グループを追跡します。たとえば、特定のユーザのトラフィックや特定の部門からのトラフィックに対してのみトリガーされるように相関ルールを制約することができます。
- スヌーズ期間の追加。相関ルールがトリガーされた後、スヌーズ期間により指定したインターバルの間、そのルールは再びトリガーされません。スヌーズ期間が経過すると、ルールは再びトリガー可能になり、新しいスヌーズ期間が始まります。
- 非アクティブ期間の追加。非アクティブ期間中は、相関ルールはトリガーされません。

展開のライセンスなしでも相関ルールを設定できますが、ライセンス許可のないコンポーネントを使用するルールはトリガーされません。

コンプライアンス 許可（Allow） リスト

コンプライアンス allow リストでは、ネットワーク上のホストで許可されるオペレーティングシステム、アプリケーション（Web およびクライアント）、プロトコルを指定します。アクティブな相関ポリシーで使用されている allow リストにホストが違反した場合、allow リストイベントがシステムによって生成されます。

相関応答

相関ポリシー違反への応答には、シンプルなアラートや、さまざまな修復（ホストのスキャンなど）が含まれます。それぞれの相関ルールまたはallowリストを、単一の応答または応答グループに関連付けることができます。

ネットワークトラフィックが複数のルールまたはallowリストをトリガーとして使用した場合、システムはそれぞれのルールとallowリストに関連付けられているすべての応答を起動します。

相関およびマルチテナンシー

マルチドメイン展開では、ドメインレベルで利用可能な任意のルール、allow リスト、および応答を使用して、任意のドメインレベルで相関ポリシーを作成できます。高位レベル ドメインの管理者はドメイン内、および複数ドメインで関連付けを実行できます。

- ドメインによって相関ルールを制約すると、そのドメインの子孫で報告されるイベントが照合されます。
- 高位レベルドメインの管理者は複数ドメインでホストを評価するコンプライアンス allow リストを作成できます。同じ allow リストで、異なるドメイン内の異なるサブネットを対象にできます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。リテラルの設定（IP アドレス、VLAN タグ、ユーザー名など）を使用してドメイン間の相関ルールを制約すると、予期しない結果になる可能性があります。

関連トピック

コンプライアンス許可（Allow）リストの概要 （1169 ページ）
Secure Firewall Management Center アラート応答 （673 ページ）
修復の概要 （1249 ページ）

コンプライアンスの要件と前提条件

モデルのサポート

任意（Any）

サポートされるドメイン

任意

ユーザの役割

- 管理者

相関ポリシーの設定

相関ルール、コンプライアンスの allow リスト、アラート応答、および修復を使用して相関ポリシーを作成します。

マルチドメイン展開では、任意のドメイン レベルで、そのレベルで使用可能な構成設定を使用して相関ポリシーを作成できます。

各相関ポリシーと、そのポリシーで使用される各ルールと allow リストにプライオリティを割り当てることができます。ルールと allow リストのプライオリティは、相関ポリシーのプライオリティをオーバーライドします。ネットワークトラフィックが相関ポリシーに違反した場合、違反があったルールまたは allow リストに独自のプライオリティがない限り、結果の相関イベントでポリシーのプライオリティ値が表示されます。

手順

ステップ 1 **[ポリシー（Policies）] > [相関（Correlation）]**を選択します。

ステップ 2 [ポリシーの作成（Create Policy）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] と [ポリシーの説明（Policy Description）] を入力します。

ステップ 4 [デフォルト プライオリティ（Default Priority）] ドロップダウン リストから、ポリシーのプライオリティを選択します。ルールのプライオリティのみを使用するには、[なし（None）] を選択します。

ステップ 5 [ルールの追加（Add Rules）] をクリックし、ポリシーで使用するルールと allow リストを選択して、[追加（Add）] をクリックします。

ステップ 6 各ルールまたは allow リストの [優先順位（Priority）] リストから、プライオリティを選択します。

- 1 ～ 5 のプライオリティ値
- **None**
- [デフォルト（Default）]（ポリシーのデフォルト プライオリティを使用）

ステップ 7 ルールと許可（Allow）リストに応答を追加する （1192 ページ）の説明に従ってルールと allow リストに応答を追加します。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- スライダをクリックして、ポリシーをアクティブにします。

ルールと許可（Allow）リストに応答を追加する

それぞれの相関ルールまたはallowリストを、単一の応答または応答グループに関連付けることができます。ネットワークトラフィックが複数のルールまたはallowリストをトリガーとして使用した場合、システムはそれぞれのルールとallowリストに関連付けられているすべての応答を起動します。トラフィックプロファイルの変更への応答として使用された場合は、Nmap 修復が開始されないことに注意してください。

マルチドメイン展開では、現在のドメインまたは先祖ドメインで作成された応答を使用できます。

手順

ステップ 1 相関ポリシーエディタで、応答を追加するルールまたは allow リストの横にある **[応答（Responses）]**（) をクリックします。

ステップ 2 [未割り当ての応答（Unassigned Responses）] の下で、ルールまたはallowリストがトリガーとして使用された場合に起動する応答を選択して、上矢印（^）をクリックします。

ステップ 3 **[更新（Update）]**をクリックします。

関連トピック

Secure Firewall Management Center アラート応答 （673 ページ）
修復の概要 （1249 ページ）

相関ポリシーの管理

アクティブな相関ポリシーへの変更は、即座に反映されます。

相関ポリシーを有効化すると、システムは即座にイベントの処理を開始して、応答をトリガーします。システムは、最初の有効化後の評価時に、非準拠ホストの allow リストイベントを生成しない点に注意してください。

マルチドメイン展開では、現在のドメインで作成された相関ポリシーが表示されます。このポリシーは編集可能です。また、先祖ドメインからの選択した相関ポリシーも表示されますが、これは編集できません。下位のドメインで作成された相関ポリシーを表示および編集するには、そのドメインに切り替えます。

（注） 設定に無関係なドメイン（名前、管理対象デバイスなど）に関する情報が公開されている場合、システムは先祖ドメインからの設定を表示しません。

手順

ステップ 1 **[ポリシー（Policies）]** > **[相関（Correlation）]**を選択します。

ステップ 2 相関ポリシーを管理します。

- アクティブ化または非アクティブ化：スライダをクリックします。 コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 作成：[ポリシーの作成（Create Policy）] をクリックします。相関ポリシーの設定 （1191 ページ）を参照してください。
- 編集：**[編集（Edit）]**（）をクリックします。相関ポリシーの設定 （1191 ページ）を参照してください。 代わりに [表示（View）]（） が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 削除：[削除（Delete）]（） をクリックします。 コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

相関ルールの設定

単純な相関ルールでは、特定のタイプのイベントが発生することのみが必要です。より具体的な条件を指定する必要はありません。たとえば、トラフィック プロファイル変化に基づく相関ルールでは、条件を指定する必要はありません。また、複数の条件と追加した制約を使用して複雑な相関ルールを作成することもできます。

相関ルール トリガー基準、ホスト プロファイル限定、ユーザ限定、または接続トラッカーを作成するときの構文はそれぞれに異なりますが、メカニズムはすべて同じです。

（注） マルチドメイン展開では、相関ルールを先祖ドメインで制約すると、そのドメインの子孫によってレポートされるイベントと一致します。

始める前に

- 相関イベントをトリガーするために使用するタイプの情報が展開で収集されていることを確認します。たとえば、個々の接続イベントまたは接続サマリーイベントで使用可能な情報は、検出方法、ロギング方法、イベント タイプなど、いくつかの要因により異なります。システムは、エクスポートされたNetFlowレコードからネットワークマップにホストを追加できますが、これらのホストに使用できる情報は限られます（NetFlow データと管理対象デバイス データの違いを参照）。

手順

ステップ 1 **[ポリシー（Policies）]** > **[相関（Correlation）]** を選択し、[ルール管理（Rule Management）] をクリックします。

ステップ 2 [ルールの作成（Create Rule）] をクリックします。

ステップ 3 [ルール名（Rule Name）] と [ルールの説明（Rule Description）] を入力します。

ステップ 4 必要に応じて、ルールの [ルール グループ（Rule Group）] を選択します。

ステップ 5 基本イベント タイプを選択し、必要に応じて、相関ルールの追加のトリガー条件を指定します。次の基本イベント タイプを選択できます。

- **VPN トラブルシューティング イベントが発生**：VPN トラブルシュート イベント トリガー条件の構文 （1196 ページ）を参照してください。
- **侵入イベントが発生**：侵入イベント トリガー条件の構文（1196ページ）を参照してください。
- **マルウェア イベントが発生**：マルウェア イベント トリガー条件の構文 （1199 ページ）を参照してください。
- **検出イベントが発生**：ディスカバリ イベント トリガー条件の構文（1201ページ）を参照してください。
- **ユーザ アクティビティが検出された**：ユーザー アクティビティのイベント トリガー条件の構文 （1204 ページ）を参照してください。
- **ホスト入力イベントが発生**：ホスト入力イベント トリガー条件の構文（1205ページ）を参照してください。
- **接続イベントが発生**：接続イベント トリガー条件の構文（1206ページ）を参照してください。
- **トラフィック プロファイルの変更**：トラフィック プロファイル変化の構文（1210ページ）を参照してください。

ステップ 6 必要に応じて、次のいずれかまたはすべてを追加することによって相関ルールをさらに制約します。

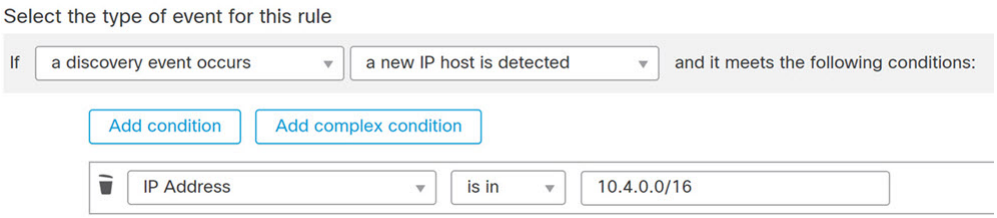
- ホストプロファイル限定：[ホストプロファイル限定の追加（Add Host Profile Qualification）] をクリックします。相関ホストプロファイル限定の構文 （1213 ページ）を参照してください。
- 接続トラッカー：[接続トラッカーの追加（Add Connection Tracker）] をクリックします。接続トラッカー （1217 ページ）を参照してください。
- ユーザ限定：[ユーザ限定の追加（Add User Qualification）] をクリックします。ユーザー限定の構文 （1216 ページ）を参照してください。
- スヌーズ期間：ルール オプションで、[スヌーズ（Snooze）] テキスト フィールドとドロップダウン リストを使用して、相関ルールのトリガー後、次に相関ルールをトリガーするまで待機する間隔を指定します。
- 非アクティブ期間：ルール オプションで、[非アクティブ期間の追加（Add Inactive Period）] をクリックします。テキスト フィールドとドロップダウン リストを使用して、相関ルールに基づくネットワーク トラフィック評価をシステムに停止させる時点および頻度を指定します。

ヒント スヌーズ期間を削除するには、間隔を **0**（秒、分、または時間）に指定します。

ステップ 7 [Save Rule] をクリックします。

相関ルールの単純な例

新しいホストが特定のサブネットで検出されると、次の単純な相関ルールがトリガーされます。カテゴリが IP アドレスを表す場合、演算子として [is in] または [is not in] を選択すると、CIDR などの特殊な表記で表される IP アドレス ブロックにその IP アドレスが含まれるのか、含まれないのかを指定できます。



次のタスク

- 相関ポリシーの設定 （1191 ページ）の説明に従って、相関ポリシーでルールを使用します。

関連トピック

相関ルールの管理 （1230 ページ）
相関ルールの作成メカニズム （1227 ページ）
スヌーズ期間および非アクティブ期間 （1227 ページ）
NetFlow データと管理対象デバイス データの違い

VPN トラブルシュート イベント トリガー条件の構文

VPN トラブルシュートイベントを基本イベントとして選択した場合、次の表で説明する方法に従って相関ルールの条件を作成します。

表 *128 : VPN* トラブルシュートイベントの構文

指定する項目	選択する演算子と入力内容
デバイス	VPN トラブルシューティング Syslog が有効になっている 1 つ以上のデバイスを選択します。
Syslog メッセージクラス	VPN Syslog メッセージクラスを選択します。選択したメッセージクラスの Syslog が生成されると、相関ルールの条件が満たされ、相関イベントが生成されます。
Syslog メッセージ ID	相関ルールの VPN Syslog メッセージ ID を指定します。
Syslog メッセージテキスト	相関ルールの VPN Syslog メッセージテキストを指定します。
Syslog のシビラティ（重大度）	VPN Syslog の重大度を指定します。選択した重大度に対して生成された VPN トラブルシューティング Syslog によって、相関イベントがトリガーされます。
ユーザ名（Username）	相関イベントを生成する必要があるトラフィックの VPN ユーザー名を指定します。

侵入イベント トリガー条件の構文

侵入イベントを基本イベントとして選択した場合、次の表で説明する方法に従って相関ルールの条件を作成します。

表 *129 :* 侵入イベントの構文

指定する項目	選択する演算子と内容
アクセス コントロール ポリシー	侵入イベントを生成した侵入ポリシーを使用するアクセス コントロール ポリシーを 1 つ以上選択します。
アクセス コントロール ルール名	侵入イベントを生成した侵入ポリシーを使用するアクセス コントロール ルールの名前の全体またはその一部を入力します。
アプリケーション プロトコル	侵入イベントに関連付けられたアプリケーション プロトコルを 1 つ以上選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコルのカテゴリを 1 つ以上選択します。

指定する項目	選択する演算子と内容
分類	分類を 1 つ以上を選択します。
クライアント	侵入イベントに関連付けられたクライアントを 1 つ以上選択します。
クライアント カテゴリ	クライアントのカテゴリを 1 つ以上選択します。
接続先（国）または送信元（国）	侵入イベントの送信元または宛先 IP アドレスに関連付けられた国を 1 つ以上選択します。
宛先 IP、送信元 IP、送信元 IP と宛先 IP の両方、または、送信元 IP か宛先 IP のいずれか	単一の IP アドレスまたはアドレス ブロックを入力します。
宛先ポート/ICMP コードまたは送信元ポート/ICMP タイプ	送信元トラフィックのポート番号または ICMP タイプ、または宛先トラフィックのポート番号または ICMP コードを入力します。
Device	イベントを生成した可能性があるデバイスを 1 つ以上選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。
出力インターフェイスまたは入力インターフェイス	インターフェイスを 1 つ以上選択します。
出力セキュリティ ゾーンまたは入力セキュリティ ゾーン	1 つ以上のセキュリティ ゾーンまたはトンネルゾーンを選択します。
ジェネレータ ID	プリプロセッサを 1 つ以上選択します。
影響フラグ	侵入イベントに割り当てられた影響レベルを選択します。 NetFlow データからネットワークマップに追加されたホストに使用可能なオペレーティングシステムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な（インパクト レベル 1：赤）インパクトレベルを割り当てることができません。このような場合は、ホスト入力機能を使用して、ホストのオペレーティングシステム ID を手動で設定します。
インライン結果	システムは、侵入ポリシーの結果としてパケットを [ドロップした（dropped）] か [ドロップしたと想定（would have dropped）] したのかを選択します。 システムは、インライン展開、スイッチド展開、またはルーテッド展開のパケットをドロップできます。侵入ポリシーのドロップ動作や侵入ルール状態とは無関係に、パッシブ展開（インライン セットがタップ モードである場合を含む）ではシステムがパケットをドロップしません。

指定する項目	選択する演算子と内容
侵入ポリシー	侵入イベントを生成した侵入ポリシーを 1 つ以上選択します。
IOC タグ	侵入イベントの結果として侵害の兆候タグが設定されているかどうかを選択します。
[プライオリティ（Priority）]	ルールの優先順位を選択します。 ルール ベースの侵入イベントの場合、優先順位は `priority` キーワードまたは `classtype` キーワードのいずれかの値に対応します。その他の侵入イベントの場合、プライオリティはデコーダまたはプリプロセッサによって決定されます。
プロトコル	http://www.iana.org/assignments/protocol-numbers にリストされているトランスポート プロトコルの名前または番号を入力します。
ルール メッセージ	ルール メッセージの全体またはその一部を入力します。
ルール SID	単一の [Snort ID]（SID）またはカンマ区切りの複数の SID を入力します。 演算子として [に含まれる（is in）] または [に含まれない（is not in）] を選択する場合、複数選択ポップアップ ウィンドウを使用することはできません。SID のカンマ区切りリストを入力する必要があります。
ルール タイプ	ルールをローカルにするかどうかを指定します。 ローカル ルールには、カスタマイズされた標準テキスト侵入ルール、ユーザが変更した標準テキスト ルール、見出し情報を変更してルールを保存するときに作成される共有オブジェクト ルールの新規インスタンスが含まれます。
実際の SSL アクション	システムが暗号化された接続をどのように処理したかを示す SSL ルール アクションを選択します。
SSL 証明書のフィンガープリント	トラフィックの暗号化に使用された証明書のフィンガープリントを入力するか、フィンガープリントに関連付けられたサブジェクトの共通名を選択します。
SSL 証明書のサブジェクトの共通名（CN）	セッションの暗号化に使用された証明書のサブジェクトの共通名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの国（C）	セッションの暗号化に使用された証明書のサブジェクトの国番号を 1 つ以上選択します。
SSL 証明書のサブジェクトの組織（O）	セッションの暗号化に使用された証明書のサブジェクトの組織名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの部門（OU）	セッションの暗号化に使用された証明書のサブジェクトの部門名のすべてまたはその一部を入力します。
SSL フローのステータス	システムによるトラフィック復号化試行の結果に基づくステータスを 1 つ以上選択します。
[ユーザ名（Username）]	侵入イベントで送信元ホストにログインしたユーザを示すユーザ名を入力します。

指定する項目	選択する演算子と内容
VLAN ID（Admin. VLAN ID）	侵入イベントをトリガーとして使用したパケットに関連付けられた最も内側の VLAN ID を入力します。
Web アプリケーション	侵入イベントに関連付けられた Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。

関連トピック

侵入イベント フィールド （948 ページ）
IP アドレスの規則 （31 ページ）

マルウェア イベント トリガー条件の構文

マルウェア イベントで相関ルールをベースとして使用するには、まず、使用するマルウェア イベントのタイプを指定します。選択肢が使用可能なトリガー条件の設定を決定します。次のオプションを選択できます。

- [エンドポイントベースのマルウェアの検出（by endpoint-based malware detection）]（Cisco Secure Endpoint による検出）
- [ネットワークベースのマルウェアの検出（by network-based malware detection）]（マルウェア防御による検出）
- [レトロスペクティブ ネットワークベースのマルウェアの検出（by retrospective network-based malware detection）]（マルウェア防御によるレトロアクティブ検出）

マルウェア イベントを基本イベントとして選択する場合、次の表で説明する方法に従って相関ルールの条件を作成します。

表 *130*：マルウェア イベントの構文

指定する項目	選択する演算子と内容
アプリケーション プロトコル	マルウェア イベントに関連付けられたアプリケーション プロトコルを 1 つ以上選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコルのカテゴリを 1 つ以上選択します。
クライアント	マルウェア イベントに関連付けられたクライアントを 1 つ以上選択します。
クライアント カテゴリ	クライアントのカテゴリを 1 つ以上選択します。
接続先（国）または送信元（国）	マルウェア イベントの送信元または宛先 IP アドレスに関連付けられた国を 1 つ以上選択します。

指定する項目	選択する演算子と内容
宛先 IP、ホスト IP、または送信元 IP	単一の IP アドレスまたはアドレス ブロックを入力します。
送信先ポート/ICMP コード	宛先トラフィックのポート番号または ICMP コードを入力します。
傾向	[マルウェア（Malware）] または [カスタム検出（Custom Detection）]、あるいはその両方を選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。
イベントタイプ	Cisco Secure Endpoint により検出されたマルウェアイベントと関連付けられた 1 つ以上のイベントタイプを選択します。
ファイル名	ファイルの名前を入力します。
ファイル タイプ	ファイル タイプを選択します。
ファイル タイプ カテゴリ	ファイル タイプ カテゴリを 1 つ以上選択します。
IOC タグ	マルウェア イベントの結果として侵害の兆候タグが設定 [される（is）] か、設定 [されない（is not）] かを選択します。
SHA-256	ファイルの SHA-256 ハッシュ値を入力するか貼り付けます。
実際の SSL アクション	システムが暗号化された接続をどのように処理したかを示す SSL ルール アクションを選択します。
SSL 証明書のフィンガープリント	トラフィックの暗号化に使用された証明書のフィンガープリントを入力するか、フィンガープリントに関連付けられたサブジェクトの共通名を選択します。
SSL 証明書のサブジェクトの共通名（CN）	セッションの暗号化に使用された証明書のサブジェクトの共通名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの国（C）	セッションの暗号化に使用された証明書のサブジェクトの国番号を 1 つ以上選択します。
SSL 証明書のサブジェクトの組織（O）	セッションの暗号化に使用された証明書のサブジェクトの組織名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの部門（OU）	セッションの暗号化に使用された証明書のサブジェクトの部門名のすべてまたはその一部を入力します。
SSL フローのステータス	システムによるトラフィック復号化試行の結果に基づくステータスを 1 つ以上選択します。

指定する項目	選択する演算子と内容
送信元ポート/ICMP タイプ	送信元トラフィックのポート番号または ICMP タイプを入力します。
Web アプリケーション	マルウェア イベントに関連付けられた Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。

関連トピック

ファイルおよびマルウェア イベント フィールド （1011 ページ）
IP アドレスの規則 （31 ページ）

ディスカバリ イベント トリガー条件の構文

ディスカバリ イベントで相関ルールをベースとして使用するには、まず、使用するディスカバリ イベントのタイプを指定します。選択肢が使用可能なトリガー条件の設定を決定します。次の表は、選択可能なディスカバリ イベントのタイプを示しています。

ホップ変更によって相関ルールをトリガーとして使用したり、ホスト制限到達のためにシステムが新しいホストをドロップした時点で相関ルールをトリガーとして使用したりすることはできません。ただし、[任意のタイプのイベントがある（there is any type of event）] を選択することで、任意のタイプのディスカバリ イベントの発生時にルールをトリガーできます。

表 *131 :* 相関ルールのトリガー条件とディスカバリ イベント タイプ

選択するオプション	選択内容
クライアントが変更された	クライアント更新
クライアントがタイムアウトになった	クライアント タイムアウト
ホスト IP アドレスが再使用されている	DHCP：IP アドレスの再割り当て
ホスト制限に達したためホストが削除された	ホスト削除：ホスト制限に到達
ホストがネットワーク デバイスとして識別されている	ネットワーク デバイスへのホスト タイプの変更
ホストがタイムアウトになった	ホスト タイムアウト
ホストの IP アドレスが変更された	DHCP：IP アドレスの変更
NETBIOS 名の変更が検出された	NETBIOS 名の変更
新しいクライアントが検出された	新しいクライアント
新しい IP ホストが検出された	新しいホスト
新しい MAC アドレスが検出された	ホストの追加 MAC の検出

選択するオプション	選択内容
新しい MAC ホストが検出された	新しいホスト
新しいネットワーク プロトコルが検出された	新しいネットワーク プロトコル
新しいトランスポート プロトコルが検出された	新しいトランスポート プロトコル
TCP ポートが閉じた	TCP ポート クローズ
TCP ポートがタイムアウトした	TCP ポート タイムアウト
UDP ポートが閉じた	UDP ポート クローズ
UDP ポートがタイムアウトした	UDP ポート タイムアウト
VLAN タグが更新された	VLAN タグ情報の更新
IOC が設定された	侵害の兆候
オープン TCP ポートが検出された	新しい TCP ポート
オープン UDP ポートが検出された	新しい UDP ポート
ホストの OS 情報が変更された	新しい OS
ホストの OS またはサーバー ID でコンフリクトが発生した	アイデンティティ競合
ホストの OS またはサーバー ID がタイムアウトした	アイデンティティ タイムアウト
任意のタイプのイベントがある	任意のイベント タイプ
MAC アドレスに関する新しい情報がある	MAC 情報の変更
TCP サーバーに関する新しい情報がある	TCP サーバ情報の更新
UDP サーバーに関する新しい情報がある	UDP サーバ情報の更新

次の表では、ディスカバリ イベントを基本イベントとして選択するときに、相関ルールの条件を作成する方法を説明します。

表 *132*: ディスカバリ イベントの構文

指定する項目	選択する演算子と内容
アプリケーション プロトコル	アプリケーション プロトコルを 1 つ以上選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコルのカテゴリを 1 つ以上選択します。

指定する項目	選択する演算子と内容
アプリケーション ポート	アプリケーション プロトコルのポート番号を入力します。
クライアント	クライアントを 1 つ以上選択します。
クライアント カテゴリ	クライアントのカテゴリを 1 つ以上選択します。
クライアント バージョン	クライアントのバージョン番号を入力します。
Device	ディスカバリ イベントを生成した可能性があるデバイスを 1 つ以上選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。
ハードウェア	モバイルデバイスのハードウェア モデルを入力します。たとえば、すべての Apple iPhone に一致させるには **`iPhone`** と入力します。
ホスト タイプ	ホスト タイプを 1 つ以上選択します。ホスト、またはいずれかのタイプのネットワーク デバイスを選択できます。
IP アドレスまたは新しい IP アドレス	単一の IP アドレスまたはアドレス ブロックを入力します。
ジェイルブロークン	イベントのホストがジェイルブレイクされたモバイル デバイスであることを示すには [はい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。
MAC アドレス	ホストの MAC アドレス全体またはその一部を入力します。 たとえば、特定のハードウェア製造元のデバイスの MAC アドレスが 0A:12:34 で始まることがわかっている場合、演算子として [開始（begins with）] を選択し、値として **`0A:12:34`** を入力できます。
MAC タイプ	MAC アドレスが [ARP/DHCP で検出（ARP/DHCP Detected）] されたかどうかを選択します。 つまり、MAC アドレスがホストに属していることをシステムがポジティブに識別したのか（[ARP/DHCP で検出（is ARP/DHCP Detected）]）、または、管理対象デバイスとホストの間にルータがあるなどの理由で、その MAC アドレスを持つ多数のホストをシステムが認識しているのか（[ARP/DHCP で検出されない（is not ARP/DHCP Detected）]）を選択します。
MAC ベンダー	ディスカバリ イベントをトリガーとして使用したネットワーク トラフィックで使われている NIC の MAC ハードウェア ベンダーの名前全体またはその一部を入力します。
Mobile	イベントのホストがモバイル デバイスであることを示すには [はい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。

指定する項目	選択する演算子と内容
NETBIOS 名	ホストの NetBIOS 名を入力します。
ネットワーク プロトコル	http://www.iana.org/assignments/ethernet-numbers にリストされているネットワーク プロトコル番号を入力します。
OS 名	オペレーティング システムの名前を 1 つ以上選択します。
OS ベンダー	オペレーティング システムのベンダーを 1 つ以上選択します。
OS バージョン	オペレーティング システムのバージョンを 1 つ以上選択します。
プロトコルまたは トランスポート プロトコル	http://www.iana.org/assignments/protocol-numbers にリストされているトランスポート プロトコルの名前または番号を入力します。
ソース（Source）	ホスト入力データのソースを選択します（オペレーティング システムとサーバのアイデンティティ変更およびタイムアウトの場合）。
ソース タイプ	ホスト入力データのソースのタイプを選択します（オペレーティング システムとサーバのアイデンティティ変更およびタイムアウトの場合）。
VLAN ID（Admin. VLAN ID）	イベントに関連しているホストの VLAN ID を入力します。
Web アプリケーション	Web アプリケーションを選択します。

関連トピック

ディスカバリ イベント タイプ （1088 ページ）
ディスカバリ イベントのフィールド （1096 ページ）
IP アドレスの規則 （31 ページ）

ユーザー アクティビティのイベント トリガー条件の構文

ユーザ アクティビティで相関ルールをベースとして使用するには、まず、使用するユーザ アクティビティのタイプを選択します。選択肢が使用可能なトリガー条件の設定を決定します。次のオプションを選択できます。

- **a new user identity was detected（新しいユーザ ID の検出）**
- **a user logs into a host（ユーザーがホストにログイン）**

ユーザーアクティビティを基本イベントとして選択する場合、次の表で説明する方法に従って相関ルールの条件を作成します。

表 *133 :* ユーザ アクティビティの構文

指定する項目	選択する演算子と内容
Device	ユーザ アクティビティを検出した可能性のあるデバイスを 1 つ以上選択します。

指定する項目	選択する演算子と内容
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。
[IPアドレス（IP Address）]	単一の IP アドレスまたはアドレス ブロックを入力します。
[ユーザ名（Username）]	ユーザー名を入力します。

関連トピック

ユーザー アクティビティ データのフィールド
IP アドレスの規則 （31 ページ）

ホスト入力イベント トリガー条件の構文

ホスト入力イベントで相関ルールをベースとして使用するには、まず、使用するホスト入力イベントのタイプを指定します。選択肢が使用可能なトリガー条件の設定を決定します。次の表では、選択可能なホスト入力イベントのタイプを示しています。

ユーザ定義によるホスト属性定義を追加/削除/変更するとき、あるいは脆弱性の影響限定を設定するときに、相関ルールをトリガーとして使用することはできません。

表 *134 :* 相関ルールのトリガー条件とホスト入力イベント タイプ

選択するオプション	ルールをトリガーとして使用するイベント タイプ
クライアントが追加された	クライアントの追加（Add Client）
クライアントが削除された	クライアントの削除（Delete Client）
ホストが追加された	ホストの追加（Add Host）
プロトコルが追加された	プロトコルの追加（Add Protocol）
プロトコルが削除された	プロトコルの削除（Delete Protocol）
スキャン結果が追加された	スキャン結果の追加（Add Scan Result）
サーバー定義が設定された	サーバー定義の設定（Set Server Definition）
サーバーが追加された	ポートの追加（Add Port）
サーバーが削除された	ポートの削除（Delete Port）
脆弱性が無効とマークされた	脆弱性を無効に設定（Vulnerability Set Invalid）
脆弱性が有効とマークされた	脆弱性を有効に設定（Vulnerability Set Valid）

選択するオプション	ルールをトリガーとして使用するイベント タイプ
アドレスが削除された	ホスト/ネットワークの削除（Delete Host/Network）
属性値が削除された	ホスト属性値の削除（Host Attribute Delete Value）
属性値が設定された	ホスト属性値の設定（Host Attribute Set Value）
OS 定義が設定された	オペレーティング システム定義の設定（Set Operating System Definition）
ホストの重要度が設定された	ホスト重要度の設定（Set Host Criticality）

次の表では、ホスト入力イベントを基本イベントとして選択するときに、相関ルールの条件を作成する方法を説明します。

表 *135 :* ホスト入力イベントの構文

指定する項目	選択する演算子と内容
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。
[IPアドレス（IP Address）]	単一の IP アドレスまたはアドレス ブロックを入力します。
ソース（Source）	ホスト入力データのソースを選択します。
ソース タイプ（Source Type）	ホスト入力データのソースのタイプを選択します。

関連トピック

ホスト入力イベント タイプ （1093 ページ）
ディスカバリ イベントのフィールド （1096 ページ）
IP アドレスの規則 （31 ページ）

接続イベント トリガー条件の構文

接続イベントで相関ルールをベースとして使用するには、まず、使用する接続イベントのタイプを指定します。接続イベントで利用可能な情報は、システムが接続をログに記録した方法、理由、および時によって変わることに注意してください。次のオプションを選択できます。

- **接続の開始または終了時のいずれか**
- **接続の開始時**
- **接続の終了時**

次の表では、接続イベントを基本イベントとして選択するときに、相関ルールの条件を作成する方法を説明します。

表 *136* : 接続イベントの構文

指定する項目	選択する演算子と内容
アクセス コントロール ポリシー	接続をログに記録したアクセス コントロール ポリシーを 1 つ以上選択します。
アクセス コントロール ルールのアクション	接続をログに記録したアクセス コントロール ルールに関連付けられたアクションを 1 つ以上選択します。 あとで接続を処理するルールまたはデフォルトアクションとは無関係に、ネットワークトラフィックがいずれかのモニタ ルールの条件に一致した場合に相関イベントをトリガーとして使用するには、[モニタ（Monitor）] を選択します。
アクセス コントロール ルール	接続をログに記録したアクセス コントロール ルールの名前のすべてまたは一部を入力します。 あとで接続を処理したルールまたはデフォルトアクションとは無関係に、接続と一致した条件を持つモニタ ルールの名前を入力できます。
アプリケーション プロトコル	接続に関連付けられたアプリケーション プロトコルを 1 つ以上選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコルのカテゴリを 1 つ以上選択します。
クライアント	クライアントを 1 つ以上選択します。
クライアント カテゴリ	クライアントのカテゴリを 1 つ以上選択します。
クライアント バージョン	クライアントのバージョン番号を入力します。
接続時間	接続イベントの時間（秒数）を入力します。
接続タイプ	接続情報がどのように取得されたかに基づいて、相関ルールをトリガーするかどうかを指定します。 • エクスポートされた NetFlow データから生成された接続イベントに、[生成元（is）] および [Netflow] を選択します。 • 管理対象デバイスによって検出された接続イベントに、[生成元でない（is not）] および [Netflow] を選択します。
接続先（国）または送信元（国）	接続イベントの送信元または宛先 IP アドレスに関連付けられた国を 1 つ以上選択します。
Device	接続を検出したデバイスを 1 つ以上選択します。または（エクスポートされた NetFlow レコードからの接続データの場合）接続を処理したデバイスを 1 つ以上選択します。

指定する項目	選択する演算子と内容
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。
出力インターフェイスまたは入力インターフェイス	インターフェイスを 1 つ以上選択します。
出力セキュリティ ゾーンまたは入力セキュリティ ゾーン	1 つ以上のセキュリティ ゾーンまたはトンネルゾーンを選択します。
イニシエータ バイト数、レスポンダ バイト数、または合計バイト数	次のいずれかを入力します。 • 送信されたバイト数（[イニシエータ バイト数（Initiator Bytes）]）。 • 受信されたバイト数（[レスポンダ バイト数（Responder Bytes）]）。 • 送受信されたバイト数（[合計バイト数（Total Bytes）]）。
イニシエータ IP、レスポンダ IP、イニシエータ IP およびレスポンダ IP の両方、あるいはイニシエータ IP またはレスポンダ IP のいずれか	単一の IP アドレスまたはアドレス ブロックを指定します。
イニシエータ パケット数、レスポンダ パケット数、または合計パケット数	次のいずれかを入力します。 • 送信されたパケット数（[イニシエータ パケット（Initiator Packets）]）。 • 受信されたパケット数（[レスポンダ パケット数（Responder Packets）]）。 • 送受信されたパケット数（[合計パケット数（Total Packets）]）
イニシエータ ポート/ICMP タイプまたはレスポンダ ポート/ICMP コード	イニシエータ トラフィックのポート番号または ICMP タイプ、あるいはレスポンダ トラフィックのポート番号または ICMP コードを入力します。
IOC タグ	接続イベントにより侵害の兆候タグが設定[される（is）]または設定[されない（is not）]かどうかを指定します。
NetBIOS 名	接続におけるモニタ対象ホストの NetBIOS 名を入力します。
NetFlow デバイス	相関ルールをトリガーするために使用する NetFlow エクスポータの IP アドレスを選択します。ネットワーク検出ポリシーに NetFlow エクスポータを追加していない場合、[NetFlow デバイス（NetFlow Device）] ドロップダウン リストは空白になります。
プレフィルタ ポリシー	接続を処理したプレフィルタ ポリシーを 1 つ以上選択します。

指定する項目	選択する演算子と内容
理由	接続イベントに関連付けられた理由を 1 つ以上選択します。
セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）	接続イベントに関連付けられたセキュリティインテリジェンスのカテゴリを1つ以上選択します。 接続終了イベントの条件としてセキュリティ インテリジェンス カテゴリを使用するには、アクセス コントロール ポリシーでカテゴリを [ブロック（Block）] ではなく [モニタ（Monitor）] に設定します。
実際の SSL アクション	システムが暗号化された接続をどのように処理したかを示す SSL ルール アクションを指定します。
SSL証明書のフィンガープリント	トラフィックの暗号化に使用された証明書のフィンガープリントを入力するか、フィンガープリントに関連付けられたサブジェクトの共通名を選択します。
SSL証明書ステータス（SSL Certificate Status）	セッションの暗号化に使用された証明書に関連付けられたステータスを1つ以上選択します。
SSL証明書のサブジェクトの共通名（CN）	セッションの暗号化に使用された証明書のサブジェクトの共通名のすべてまたはその一部を入力します。
SSL証明書のサブジェクトの国（C）	セッションの暗号化に使用された証明書のサブジェクトの国番号を 1 つ以上選択します。
SSL証明書のサブジェクトの組織（O）	セッションの暗号化に使用された証明書のサブジェクトの組織名のすべてまたはその一部を入力します。
SSL証明書のサブジェクトの部門（OU）	セッションの暗号化に使用された証明書のサブジェクトの部門名のすべてまたはその一部を入力します。
SSL 暗号スイート（SSL Cipher Suite）	セッションの暗号化に使用された暗号スイートを 1 つ以上選択します。
SSL暗号化セッション（SSL Encrypted Session）	[正常に復号（Successfully Decrypted）] を選択します。
SSL フローのステータス	システムによるトラフィック復号化試行の結果に基づくステータスを1つ以上選択します。
SSL ポリシー	暗号化された接続をログに記録した SSL ポリシーを 1 つ以上選択します。
SSL ルール名	暗号化された接続をログに記録した SSL ルールの名前のすべてまたは一部を入力します。
SSL サーバ名	クライアントが暗号化された接続を確立したサーバの名前のすべてまたは一部を入力します。
SSL URL カテゴリ	暗号化された接続でアクセスされた URL のカテゴリを 1 つ以上選択します。

指定する項目	選択する演算子と内容
SSL バージョン	セッションの暗号化に使用された SSL または TLS バージョンを 1 つ以上選択します。
TCP フラグ	相関ルールをトリガーとして使用するために接続イベントに含まれていなければならない TCP フラグを選択します。NetFlow レコードから生成された接続データにのみ TCP フラグが含まれます。
トランスポート プロトコル	接続で使用されたトランスポート プロトコル：**TCP** または **UDP** を入力します。
トンネル/プレフィルタ ルール	接続を処理したトンネルまたはプレフィルタ ルールの名前のすべてまたは一部を入力します。
URL	接続でアクセスされた URL 全体またはその一部を入力します。
URL カテゴリ	接続でアクセスされた URL のカテゴリを 1 つ以上選択します。
URLレピュテーション	接続でアクセスされた URL のレピュテーション値を 1 つ以上選択します。
[ユーザ名（Username）]	接続でいずれかのホストにログインしたユーザのユーザ名を入力します。
Web アプリケーション	接続に関連付けられた Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。

関連トピック

接続およびセキュリティ関連の接続イベントフィールド （902 ページ）
IP アドレスの規則 （31 ページ）

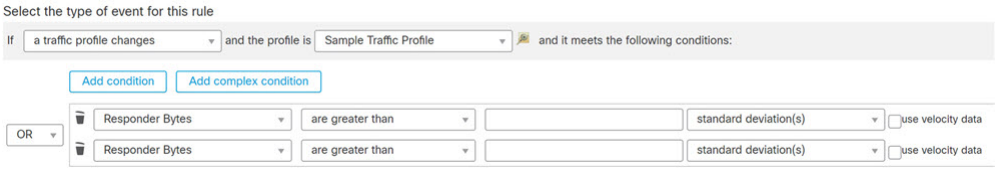
トラフィック プロファイル変化の構文

トラフィック プロファイル変化で相関ルールをベースとして使用するには、まず、使用するトラフィック プロファイルを選択します。ルールは、選択するプロファイルによって特徴付けられるパターンからネットワーク トラフィックが逸脱するときにトリガーされます。

raw データ、またはデータから計算された統計情報のいずれかに基づいてルールをトリガーできます。たとえば、ネットワーク内を移動するデータ量（バイト数で測定）が急激に変化した場合、攻撃または他のセキュリティー ポリシー違反が発生した可能性がありますが、そのような変動時にトリガーとして使用されるルールを作成できます。以下のいずれかの場合にトリガーとして使用されるよう、ルールを指定できます。

- ネットワーク内を移動するバイト数が特定のバイト数を上回る場合
- ネットワーク内を移動するバイト数が、平均トラフィック量より上または下の特定数の標準偏差を超えて急激に変化した場合

ネットワーク内を移動するバイト数が、特定数の標準偏差からなる範囲を（上または下に）超えたときにトリガーとして使用されるルールを作成するには、次の図に示すように、上限と下限を指定する必要があります。



移動するバイト数が、平均より上側の特定数の標準偏差を超えた場合にトリガーするルールを作成するには、以下の図に示されている最初の条件だけを使用します。

移動するバイト数が、平均を基準とした特定数の標準偏差の下側を超えた場合にトリガーとして使用されるルールを作成するには、2 番目の条件だけを使用します。

[速度データを使用する（use velocity data）] チェックボックスを選択すると、データ ポイント間の変化率に基づいて相関ルールをトリガーできます。上記の例で仮に速度データを使用する場合は、次のいずれかの時点でルールがトリガーとして使用されるように指定できます。

- ネットワーク内を移動するバイト数の変化が、平均変化率より上または下の特定数の標準偏差を超えた場合
- ネットワーク内を移動するバイト数の変化が、特定のバイト数を上回った場合

トラフィック プロファイル変化を基準イベントとして選択した場合、以下の表で説明する方法に従って相関ルールの条件を作成します。

表 *137*: トラフィック プロファイル変化の構文

指定する項目	選択する演算子と入力内容	いずれかを選択
接続数	検出された接続の合計数 **または** 平均より上または下の標準偏差の数（検出された接続数がこれを超えるとルールがトリガーとして使用されます）	接続 standard deviation(s)：標準偏差の数

指定する項目	選択する演算子と入力内容	いずれかを選択
合計バイト数、イニシエータ バイト数、またはレスポンダ バイト数	次のいずれかになります。 • 送信された合計バイト数（[合計バイト数（Total Bytes）]） • 送信されたバイト数（[イニシエータ バイト数（Initiator Bytes）]） • 受信されたバイト数（[レスポンダ バイト数（Responder Bytes）]） **または** 平均より上または下の標準偏差の数（上の条件のいずれかはルールがトリガーとして使用される必要があります）	bytes standard deviation(s)：標準偏差の数
合計パケット数、イニシエータ パケット数、またはレスポンダ パケット数	次のいずれかになります。 • 送信された合計パケット数（[合計パケット数（Total Packets）]） • 送信されたパケット数（[イニシエータ パケット（Initiator Packets）]） • 受信されたパケット数（[レスポンダ パケット数（Responder Packets）]） **または** 平均より上または下の標準偏差の数（上の条件のいずれかはルールがトリガーとして使用される必要があります）	packets standard deviation(s)：標準偏差の数
一意のイニシエータ	セッションを開始した個別のホストの数 **または** 平均より上または下の標準偏差の数（検出された一意のイニシエータ数はルールがトリガーとして使用される必要があります）	initiators：イニシエータ数 standard deviation(s)：標準偏差の数
一意のレスポンダ	セッションに応答した個別のホストの数 **または** 平均より上または下の標準偏差の数（検出された一意のレスポンダ数はルールがトリガーとして使用される必要があります）	responders：レスポンダ数 standard deviation(s)：標準偏差の数

相関ホスト プロファイル限定の構文

イベントに関連するホストのホスト プロファイルに基づいて相関ルールを制約するには、[ホスト プロファイル限定（host profile qualification）] を追加します。マルウェア イベント、トラフィック プロファイル変化、または新しい IP ホスト検出によってトリガーとして使用される相関ルールには、ホスト プロファイル限定を追加することはできません。

ホストプロファイル限定を作成するときには、まず、相関ルールを制約するために使用するホストを指定します。選択可能なホストは、ルールの基盤となるイベントのタイプによって異なります。

- 接続イベント：[レスポンダ ホスト（Responder Host）] または [イニシエータ ホスト（Initiator Host）] を選択します。
- 侵入イベント：[宛先ホスト（Destination Host）] または [送信元ホスト（Source Host）] を選択します。
- ディスカバリ イベント、ホスト入力イベントは、またはユーザ アクティビティ：[ホスト（Host）] を選択します。

次の表では、相関ルールのホスト プロファイル限定を作成する方法について説明します。

表 *138* : ホスト プロファイル限定の構文

指定する項目	選択する演算子と内容
[アプリケーションプロトコル（Application Protocol）]>[アプリケーションプロトコル（Application Protocol）]	アプリケーション プロトコルを選択します。
[アプリケーションプロトコル（Application Protocol）]>[アプリケーション ポート（Application Port）]	アプリケーション プロトコルのポート番号を入力します。
[アプリケーションプロトコル（Application Protocol）]>[プロトコル（Protocol）]	プロトコルを選択します。
[アプリケーションプロトコル カテゴリ（Application Protocol Category）]	カテゴリを選択します。
[クライアント（Client）]>[クライアント（Client）]	クライアントを選択します。

指定する項目	選択する演算子と内容
[クライアント（Client）] > [クライアント バージョン（Client Version）]	クライアント バージョンを入力します。
[クライアント カテゴリ（Client Category）]	カテゴリを選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。
ハードウェア	モバイルデバイスのハードウェア モデルを入力します。たとえば、すべての Apple iPhone に一致させるには **iPhone** と入力します。
[ホストの重要度（Host Criticality）]	ホストの重要度を選択します。
ホスト タイプ	ホスト タイプを 1 つ以上選択します。通常のホスト、またはいずれかのタイプのネットワーク デバイスを選択できます。
[IOC タグ（IOC Tag）]	侵害の兆候タグを 1 つ以上選択します。
ジェイルブロークン	イベントのホストがジェイルブレイクされたモバイル デバイスであることを示すには [はいい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。
[MAC アドレス（MAC Address）] > [MAC アドレス（MAC Address）]	ホストの MAC アドレス全体またはその一部を入力します。
[MAC アドレス（MAC Address）] > [MAC タイプ（MAC Type）]	MAC タイプが ARP/DHCP で検出されるかどうかを選択します。 • システムは MAC アドレスがホストに属していることをポジティブに識別した（[ARP/DHCP で検出（is ARP/DHCP Detected）]） • たとえば、デバイスとホスト間にはルータがあるため、システムはその MAC アドレスを持つ多くのホストを認識している（[ARP/DHCP で検出されない（is not ARP/DHCP Detected）]） • MAC タイプが無関係（[どれでもない（is any）]）
[MAC ベンダー（MAC Vendor）]	ホストが使用するハードウェアの MAC ベンダー全体またはその一部を入力します。
Mobile	イベントのホストがモバイル デバイスであることを示すには [はい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。

指定する項目	選択する演算子と内容
[NetBIOS 名（NetBIOS Name）]	ホストの NetBIOS 名を入力します。
ネットワーク プロトコル	http://www.iana.org/assignments/ethernet-numbers にリストされているネットワーク プロトコル番号を入力します。
[オペレーティング システム（Operating System）] > [OS ベンダー（OS Vendor）]	オペレーティング システムのベンダー名を 1 つ以上選択します。
[オペレーティング システム（Operating System）] > [OS 名（OS Name）]	オペレーティング システムの名前を 1 つ以上選択します。
[オペレーティング システム（Operating System）] > [OS バージョン（OS Version）]	オペレーティング システムのバージョンを 1 つ以上選択します。
[トランスポート プロトコル（Transport Protocol）]	http://www.iana.org/assignments/protocol-numbers にリストされているトランスポート プロトコルの名前または番号を入力します。
VLAN ID（Admin. VLAN ID）	ホストの VLAN ID 番号を入力します。
Web アプリケーション	Web アプリケーションを選択します。
[Web アプリケーションのカテゴリ（Web Application Category）]	カテゴリを選択します。
使用可能な任意のホスト属性（デフォルト コンプライアンス allow リスト ホスト属性を含む）	ホスト属性タイプに応じて適切な値を入力または選択します。

暗黙的または汎用のクライアントを使用したホスト プロファイル限定の作成

システムが `client` が続くアプリケーション プロトコルの名前（たとえば、`HTTPS client`）を使用して検出されたクライアントをレポートする場合、このクライアントは暗黙的または汎用のクライアントです。これらの場合、システムは特定のクライアントを検出していませんが、サーバ応答トラフィックに基づいてクライアントの存在を推測しています。

暗黙的または汎用のクライアントを使用してホスト プロファイル限定を作成するには、クライアントではなく、レスポンダ ホストで実行されているアプリケーション プロトコルを使用して制約します。

イベント データを使用したホスト プロファイル限定の作成

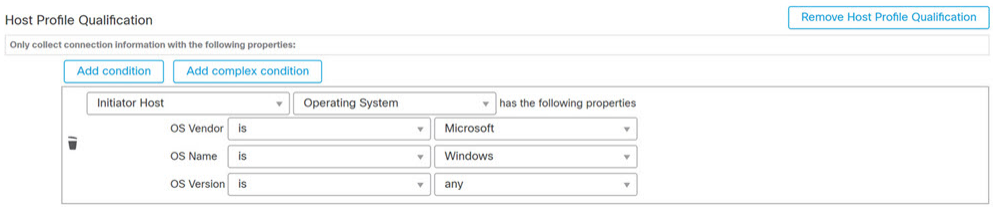
ホストプロファイル限定の制約時に、多くの場合、相関ルールの基本イベントからデータを使用できます。

たとえば、モニタ対象のいずれかのホストで特定のブラウザが使用されていることをシステムが検出した場合に、相関ルールがトリガーとして使用されるとします。さらに、この使用を検出するときに、ブラウザのバージョンが最新でない場合はイベントを生成すると仮定します。

この場合、[クライアント（Client）] は [イベント クライアント（Event Client）] ですが、[クライアント バージョン（Client Version）] が最新のバージョンでない場合にのみルールがトリガーされるように、この相関ルールをホスト プロファイル限定に追加できます。

ホスト プロファイル限定の例

次のホストプロファイル限定は、ルールの基礎となるディスカバリ イベントに関連するホストが Microsoft Windows のバージョンを実行している場合にのみ、ルールがトリガーとして使用されるように相関ルールを制約します。



関連トピック

ホスト データ フィールド （1098 ページ）

ユーザー限定の構文

接続、侵入、ディスカバリ、またはホスト入力のいずれかのイベントを使用して相関ルールをトリガーとして使用する場合、イベントに関連するユーザのアイデンティティに基づいてルールを制約することができます。この制約は、ユーザ限定と呼ばれます。たとえば、送信元または宛先ユーザのアイデンティティが販売部門所属である場合にのみトリガーとして使用するよう、相関ルールを制約できます。

トラフィック プロファイル変化やユーザ アクティビティ検出によってトリガーとして使用される相関ルールに、ユーザ限定を追加することはできません。また、システムは、アイデンティティ レルムで確立された Management Center サーバの接続を介してユーザの詳細を取得します。この情報は、データベース内のすべてのユーザに関して入手可能とは限りません。

ユーザ限定を作成するときには、まず、相関ルールを制約するために使用するアイデンティティを指定します。選択可能なアイデンティティは、ルールの基本イベントのタイプによって異なります。

- 接続イベント：[イニシエータのアイデンティティ（Identity on Initiator）] または [レスポンダのアイデンティティ（Identity on Responder）] を選択します。

- 侵入イベント：[宛先のアイデンティティ（Identity on Destination）] または [送信元のアイデンティティ（Identity on Source）] を選択します。
- ディスカバリ イベント：[ホストのアイデンティティ（Identity on Host）] を選択します。
- ホスト入力イベント：[ホストのアイデンティティ（Identity on Host）] を選択します。

次の表では、相関ルールのユーザ限定を作成する方法について説明します。

表 *139* : ユーザ限定の構文

指定する項目	選択する演算子と内容
認証プロトコル（Authentication Protocol）	ユーザを検出するために使用される認証プロトコル（またはユーザ タイプ）プロトコルを選択します。
部署名（Department）	部署を入力します。
ドメイン（Domain）	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。
E メール	電子メール アドレスを入力します。
名	名を入力します。
姓	姓を入力します。
電話	電話番号を入力します。
[ユーザ名（Username）]	ユーザー名を入力します。

関連トピック

ユーザー データのフィールド

接続トラッカー

接続トラッカー は、ルールの最初の基準（ホスト プロファイルおよびユーザ認定を含む）に一致した後にシステムが特定の接続のトラッキングを始めるよう、相関ルールを制約します。追跡される接続が、指定した期間にわたって収集された追加の基準を満たす場合には、システムがルールの相関イベントを生成します。

ヒント　通常、接続トラッカーは特定のトラフィックだけをモニタし、トリガーとして使用された場合には指定された一定期間だけ実行されます。接続トラッカーは、広範なネットワーク トラフィックをモニタして持続的に実行されるトラフィック プロファイルとは対照的です。

接続トラッカーがイベントを生成する方法は 2 つあります。

条件に一致するとただちに起動する接続トラッカー

ネットワーク トラフィックが接続トラッカーの条件に一致すると即座に相関ルールが起動するよう、接続トラッカーを設定できます。この場合、タイムアウト期間が満了していなくても、システムはその接続トラッカーインスタンスでの接続のトラッキングを停止します。相関ルールをトリガーとして使用したのと同じタイプのポリシー違反が再び発生した場合、システムは新しい接続トラッカーを作成します。

ただし、ネットワーク トラフィックが接続トラッカーの条件に一致する前にタイムアウト期間が満了した場合、システムは相関イベントを生成せず、そのルール インスタンスの接続のトラッキングを停止します。

たとえば、特定のタイプの接続が特定の期間中に特定回数を超えて発生した場合にのみ相関イベントを生成させることで、接続トラッカーをある種のイベントしきい値として機能させることができます。あるいは、初回接続後に過剰なデータ転送量をシステムが検出した場合にのみ、相関イベントを生成させることもできます。

タイムアウト期間の満了時に起動する接続トラッカー

タイムアウト期間全体にわたって収集されるデータに依存するよう、接続トラッカーを設定できます。この場合、タイムアウト期間が満了するまでは起動しません。

たとえば、特定の期間内に検出された転送量が特定のバイト数を下回った場合に接続トラッカーを起動するよう設定すると、システムはその期間が経過するまで待って、ネットワーク トラフィックがその条件に一致した場合はイベントを生成します。

接続トラッカーの追加

始める前に

- 接続、侵入、検出、ユーザID、ホスト入力イベントに基づいて相関ルールを作成します。VPN トラブルシューティング イベント、マルウェアイベント、またはトラフィックプロファイルの変更に基づいたルールに接続トラッカーを追加することはできません。

手順

ステップ 1　相関ルールエディタ（**[ポリシー（Policys）]** > **[相関（Correlation）]** > **[ルールの管理（Rule Management）]**）で、[編集（Edit）]、[接続トラッカーの追加（Add Connection Tracker）] の順にクリックします。

ステップ 2 追跡する接続を指定します。接続トラッカーの構文 （1219 ページ） を参照してください。

ステップ 3 追跡する接続に応じて、いつ相関イベントを生成するかを指定します。接続トラッカーイベントの構文 （1222 ページ） を参照してください。

ステップ 4 トラッカーの条件が満たされなければならない時間の間隔（秒、分または時）を指定します。

接続トラッカーの構文

次の表は、どのような接続を追跡するかを指定する接続トラッカー条件の作成方法を説明しています。

表 *140* : 接続トラッカーの構文

指定する項目	選択する演算子と内容
アクセス コントロール ポリシー	追跡対象の接続を処理したアクセス コントロール ポリシーを 1 つ以上選択します。
アクセス コントロール ルールのアクション	追跡対象の接続をログに記録したアクセス コントロール ルールに関連付けられたアクセス コントロール ルール アクションを 1 つ以上選択します。 あとで接続を処理するルールまたはデフォルト アクションとは無関係に、任意のモニタ ルールの条件に一致する接続を追跡するには、[モニタ（Monitor）] を選択します。
アクセス コントロール ルール名	追跡対象の接続をログに記録したアクセス コントロール ルールの名前のすべてまたはその一部を入力します。 モニタ ルールに一致する接続を追跡するには、モニタ ルールの名前を入力します。あとで接続を処理するルールまたはデフォルト アクションとは無関係に、システムは該当する接続を追跡します。
アプリケーション プロトコル	アプリケーション プロトコルを 1 つ以上選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコル カテゴリを 1 つ以上選択します。
クライアント	クライアントを 1 つ以上選択します。
クライアント カテゴリ	クライアント カテゴリを 1 つ以上選択します。
クライアント バージョン	クライアントのバージョンを入力します。
接続時間	接続時間（秒数）を入力します。

指定する項目	選択する演算子と内容
接続タイプ	接続情報がどのように取得されたかに基づいて、相関ルールをトリガーするかどうかを指定します。 • エクスポートされた NetFlow レコードから生成された接続イベントに、[生成元（is）] および [Netflow] を選択します。 • 管理対象デバイスによって検出された接続イベントに、[生成元でない（is not）] および [Netflow] を選択します。
接続先（国）または送信元（国）	国を 1 つ以上選択します。
Device	追跡対象の接続を検出したデバイスを 1 つ以上選択します。NetFlow 接続を追跡する場合は、エクスポートされた NetFlow レコードからの接続データを処理するデバイスを選択します。
入力インターフェイスまたは出力インターフェイス	インターフェイスを 1 つ以上選択します。
入力セキュリティ ゾーンまたは出力セキュリティ ゾーン	1 つ以上のセキュリティ ゾーンまたはトンネルゾーンを選択します。
イニシエータ IP、レスポンダ IP、またはイニシエータ/レスポンダ IP	単一の IP アドレスまたはアドレス ブロックを入力します。
イニシエータ バイト数、レスポンダ バイト数、または合計バイト数	次のいずれかを入力します。 • 送信されたバイト数（[イニシエータ バイト数（Initiator Bytes）]） • 受信されたバイト数（[レスポンダ バイト数（Responder Bytes）]） • 送受信されたバイト数（[合計バイト数（Total Bytes）]）
イニシエータ パケット数、レスポンダ パケット数、または合計パケット数	次のいずれかを入力します。 • 送信されたパケット数（[イニシエータ パケット（Initiator Packets）]） • 受信されたパケット数（[レスポンダ パケット数（Responder Packets）]） • 送受信されたパケット数（[合計パケット数（Total Pakets）]）
イニシエータ ポート/ICMP タイプまたはレスポンダ ポート/ICMP コード	イニシエータ トラフィックのポート番号または ICMP タイプ、あるいはレスポンダ トラフィックのポート番号または ICMP コードを入力します。
IOC タグ	侵害の兆候タグが設定されて [いる（is）] または設定されて [いない（is not）] かどうかを選択します。

指定する項目	選択する演算子と内容
NETBIOS 名	接続におけるモニタ対象ホストの NetBIOS 名を入力します。
NetFlow デバイス	追跡する NetFlow エクスポータの IP アドレスを選択します。ネットワーク検出ポリシーに NetFlow エクスポータを追加していない場合、[NetFlow デバイス（NetFlow Device）] ドロップダウン リストは空白になります。
プレフィルタ ポリシー	追跡対象の接続を処理したプレフィルタ ポリシーを 1 つ以上選択します。
理由	追跡対象の接続に関連付けられている理由を 1 つ以上選択します。
セキュリティ インテリジェンス カテゴリ	追跡対象の接続に関連付けられているセキュリティ インテリジェンスのカテゴリを 1 つ以上選択します。
TCP フラグ	接続を追跡するために接続に含まれている必要のある TCP フラグを選択します。TCP フラグ データは、エクスポートされた NetFlow レコードから生成された接続にのみ含まれます。
トランスポート プロトコル	接続に使用されるトランスポート プロトコルを選択します。
URL	追跡対象の接続でアクセスされた URL のすべてまたはその一部を入力します。
URL Category	追跡対象の接続でアクセスされた URL のカテゴリを 1 つ以上選択します。
URL レピュテーション	追跡対象の接続でアクセスされた URL のレピュテーション値を 1 つ以上選択します。
[ユーザ名（Username）]	追跡対象の接続でいずれかのホストにログインしたユーザのユーザ名を入力します。
Web アプリケーション	Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。

イベント データを使用した接続トラッカーの作成

接続トラッカーを作成するときに、多くの場合、相関ルールの基本イベントからデータを使用できます。

たとえば、システムが新しいクライアントを検出するときに、相関ルールがトリガーされると想定します。接続トラッカーをこのタイプの相関ルールに追加すると、システムは次の基本イベントを参照する制約のあるトラッカーを自動的に入力します。

- [イニシエータ/レスポンダ IP（Initiator/Responder IP）] が [イベント IP アドレス（Event IP Address）] に設定される。
- [クライアント（Client）] が [イベント クライアント（Event Client）] に設定される。

ヒント　特定の IP アドレスまたは IP アドレス ブロックに関連する接続を追跡するには、[手動エントリにスイッチ（switch to manual entry）] をクリックして、手動で IP を指定します。[イベントフィールドにスイッチ（switch to event fields）] をクリックすると、イベントの IP アドレスを使用する設定に戻ります。

関連トピック

接続およびセキュリティ関連の接続イベントフィールド （902 ページ）
IP アドレスの規則 （31 ページ）

接続トラッカー イベントの構文

追跡対象の接続に基づいてどのようなときに相関イベントを生成するかを指定する接続トラッカー条件を作成するには、次の表の説明に従います。

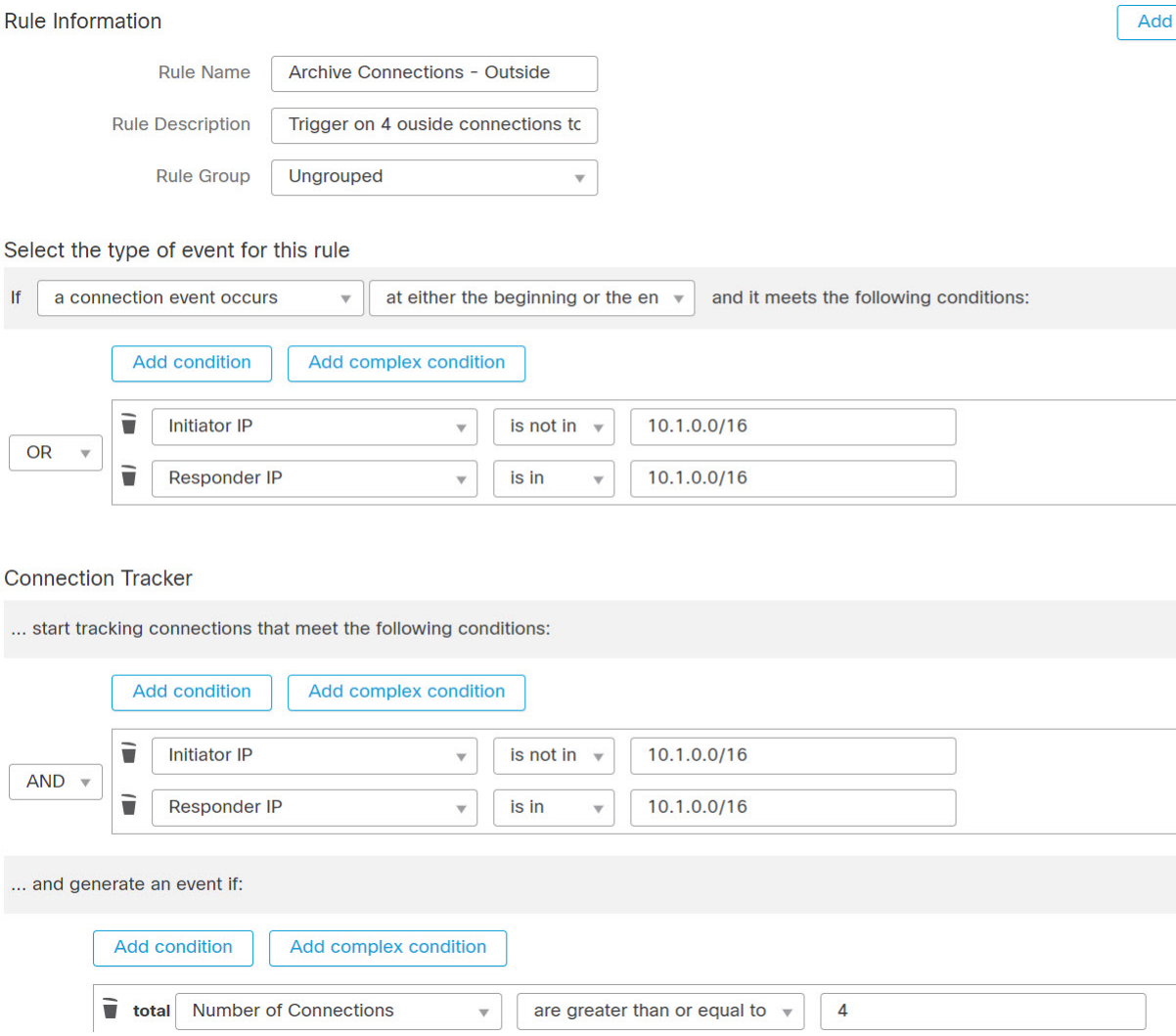
表 *141* : 接続トラッカー イベントの構文

指定する項目	選択する演算子と入力内容
接続数	検出された接続の合計数
SSL暗号化セッションの数	検出された SSL または TLS 暗号化セッションの合計数
合計バイト数、イニシエータ バイト数、またはレスポンダ バイト数	次のいずれかになります。 • 送信された合計バイト数（[合計バイト数（Total Bytes）]） • 送信されたバイト数（[イニシエータ バイト数（Initiator Bytes）]） • 受信されたバイト数（[レスポンダ バイト数（Responder Bytes）]）
合計パケット数、イニシエータ パケット数、またはレスポンダ パケット数	次のいずれかになります。 • 送信された合計パケット数（[合計パケット数（Total Packets）]） • 送信されたパケット数（[イニシエータ パケット（Initiator Packets）]） • 受信されたパケット数（[レスポンダ パケット数（Responder Packets）]）
一意のイニシエータまたは一意のレスポンダ	次のいずれかになります。 • 検出されたセッションを開始した個別のホスト数（[一意のイニシエータ（Unique Initiators）]） • 検出された接続に応答した個別のホスト数（[一意のレスポンダ（Unique Responders）]）

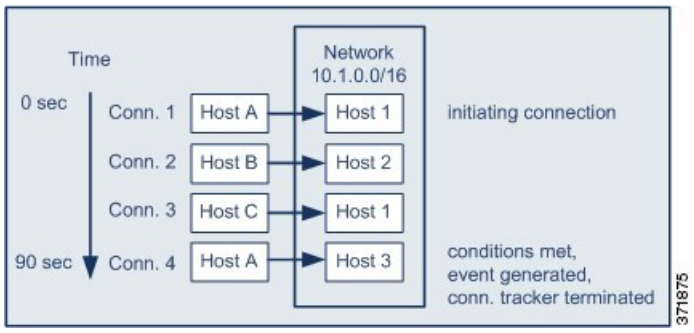
外部ホストからの過剰な接続の設定例

ネットワーク 10.1.0.0/16 のセンシティブ ファイルをアーカイブし、通常、ネットワーク外のホストはネットワーク内のホストへの接続を開始することはないシナリオを考慮します。時にはネットワーク外部から接続が開始されることもありますが、2 分以内に 4 つ以上の接続が開始された場合には注意が必要だと判断するとします。

次の図に示すルールでは、接続が 10.1.0.0/16 ネットワーク外からネットワーク内に発生したときに、基準に適合するトラッキング接続を開始するように指定します。その後、2 分以内に署名に一致する 4 つの接続（発信側の接続を含む）が検出されても相関イベントを生成します。



以下の図は、ネットワーク トラフィックが上記の相関ルールをトリガーとして使用できる方法を示します。



この例では、相関ルールの基本条件に一致する接続をシステムが検出しました。つまり、ネットワーク 10.1.0.0/16 の外部にあるホストからネットワーク内部のホストへの接続をシステムが検出しました。これにより、接続トラッカーが作成されました。

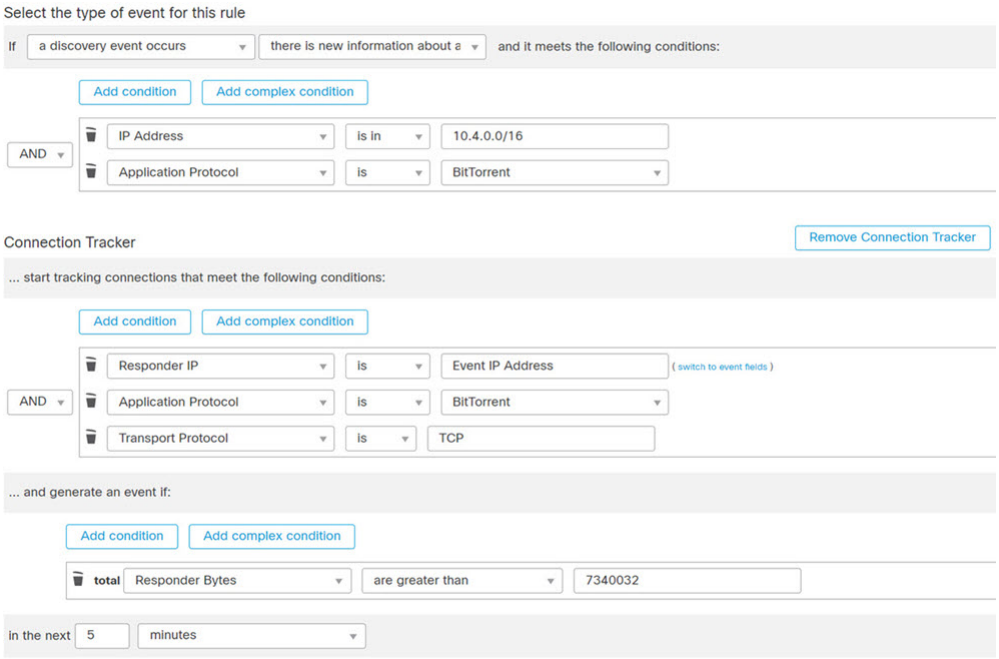
接続トラッカーは、次のステージで処理します。

- ネットワーク外のホスト A からネットワーク内のホスト 1 への接続が検出されると、トラッキング接続を開始します。
- 接続トラッカーの署名に一致する 2 つ以上の接続（ホスト B ～ホスト 2、ホスト C ～ホスト 1）を検出します。
- 2 分の時間制限内でホスト A がホスト 3 に接続すると、4 つの認定されている接続を検出します。ルール条件が適合します。
- 最後に、相関イベントを生成し、トラッキング接続を停止します。

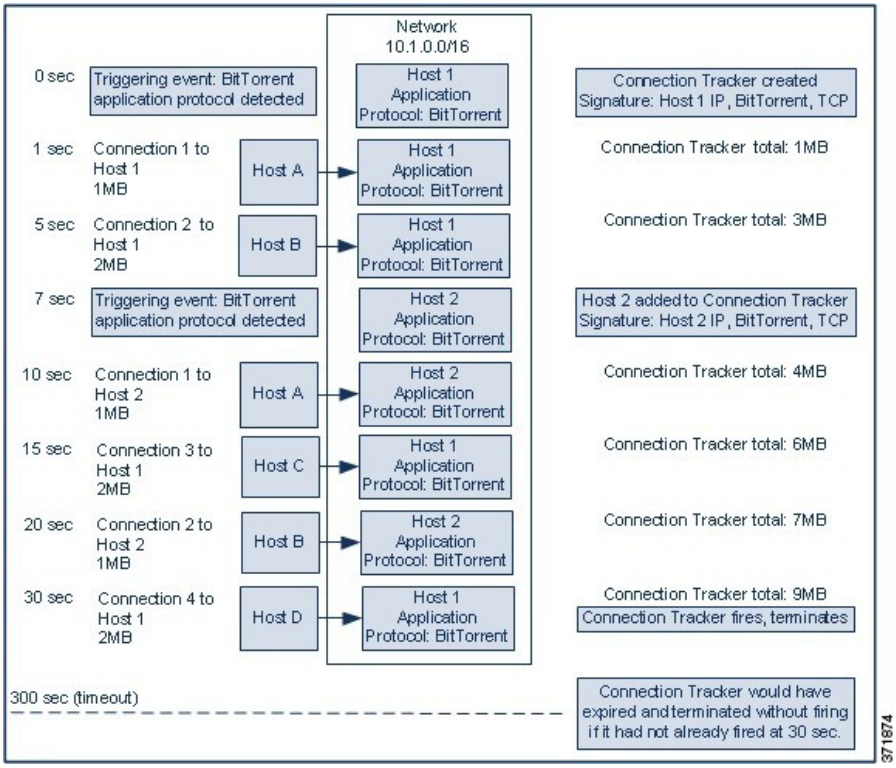
BitTorrent の過剰なデータ転送の設定例

最初に監視対象のネットワークのホストに接続後、過剰な BitTorrent データの転送が検出された場合は相関イベントを生成するシナリオを考慮します。

次の図は、監視対象ネットワーク上に BitTorrent アプリケーション プロトコルを検出した場合にトリガーとして使用される相関ルールを示します。このルールには、監視対象ネットワークのホスト（この例では 10.1.0.0/16）が、最初のポリシー違反後の 5 分間に 7 MB を超えるデータ（7340032 バイト）を BitTorrent を介してまとめて転送する場合にのみルールがトリガーとして使用されるように制約する接続トラッカーがあります。



以下の図は、ネットワーク トラフィックが上記の相関ルールをトリガーとして使用できる方法を示します。



この例では、2 つのホスト（ホスト 1、ホスト 2）に BitTorrent TCP アプリケーション プロトコルが検出されました。この 2 つのホストは、BitTorrent を介して 4 つの他のホスト（ホスト A、ホスト B、ホスト C、ホスト D）にデータを転送しました。

接続トラッカーは、次の工程で処理しました。

- まず、ホスト 1 で BitTorrent アプリケーション プロトコルが検出されると、0 秒マーカーで接続のトラッキングを開始します。次の 5 分の間に 7MB の BitTorrent TCP データの転送が検出されない場合（300 秒マーカーにより）、接続トラッカーは無効になる点にご注意ください。
- 5 秒で、ホスト 1 は、署名に一致する 3MB データを転送します。
  - 1 秒マーカーでは、ホスト 1 からホスト A へ 1 MB（供給した接続トラッカーに対して数えた全 BitTorrent トラフィック 1 MB）
  - 5 秒マーカーでホスト 1 からホストへ B 2 MB（合計 3 MB）
- 7 秒では、ホスト 2 で BitTorrent アプリケーション プロトコルを検出し、ホスト 2 に対しても BitTorrent 接続のトラッキングを開始します。
- 20 秒では、ホスト 1 とホスト 2 の両方から転送される署名に一致する追加のデータを検出します。
  - 10 秒マーカーでホスト 2 からホスト A へ 1 MB（合計 4 MB）
  - 15 秒マーカーでホスト 1 からホスト C へ 2 MB（合計 6 MB）
  - 20 秒マーカーでホスト 2 からホスト B へ 1MB（合計 7MB）
- ホスト 1 とホスト 2 が転送した BitTorrent データは合計で 7MB になりましたが、転送された合計バイト数が 7MB を**超過**していることが条件となっているため（**Responder Bytes are greater than 7340032**）、ルールはトリガーとして使用されません。この時点で、トラッカーのタイムアウト期間内の残りの 280 秒の間、追加の BitTorrent 転送が検出されない場合に、トラッカーは無効になり、相関イベントは作成されません。
- ただし、30 秒の時点で、別の BitTorrent 転送が検出され、次のルールの条件が満たされます。
  - 30 秒マーカーでは、ホスト 1 からホスト D へ 2 MB（合計 9 MB）
- 最後に、相関イベントが生成されます。また、5分間が無効にならなくても接続トラッカーインスタンスについてはトラッキング接続を停止します。この時点で BitTorrent TCP アプリケーションプロトコルを用いて新しい接続が検出されると、新しい接続トラッカーが生成されます。ホスト 1 が 2 MB すべてをホスト D に転送した後に相関イベントが生成される点にご注意ください。これは、セッションが終了するまで接続データを計算することはないためです。

スヌーズ期間および非アクティブ期間

相関ルールでスヌーズ期間を設定することができます。スヌーズ期間を設定すると、相関ルールがトリガーとして使用されたとき、指定した時間間隔内にルール違反が再び発生しても、システムはその期間中はルールのトリガーを停止します。スヌーズ期間が経過すると、ルールは再びトリガー可能になります（新しいスヌーズ期間が始まります）。

たとえば、通常はトラフィックを全く生成しないはずのホストがネットワーク上にあるとします。このホストが関与する接続がシステムで検出されるたびにトリガーとして使用される単純な相関ルールの場合、このホストで送受信されるネットワーク トラフィックによっては、短時間に多数の相関イベントが生成される可能性があります。ポリシー違反を示す相関イベントの数を制限するために、スヌーズ期間を追加できます。これにより、（指定した期間内に）システムで検出されたそのホストに関連する最初の接続に対してのみ、システムは相関イベントを生成します。

また、相関ルールで非アクティブ期間を設定することもできます。非アクティブ期間中は、相関ルールはトリガーとして使用されません。非アクティブ期間を毎日、毎週、または毎月繰り返すように設定できます。たとえば、ホスト オペレーティング システム変更を探すために内部ネットワークで夜間にNmapスキャンを実行するとします。この場合、相関ルールが誤ってトリガーとして使用されないよう、毎日のスキャン時間帯に、該当する相関ルールで非アクティブ期間を設定することができます。

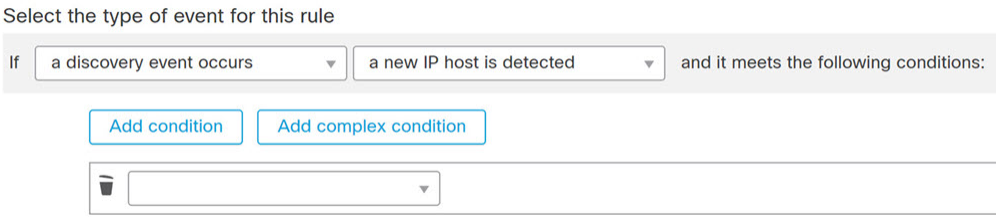
相関ルールの作成メカニズム

相関ルールは、ルールがトリガーされる条件を指定して作成します。条件で使用できるシンタックスは、作成しようとしている要素により異なりますが、メカニズムはすべて同じです。

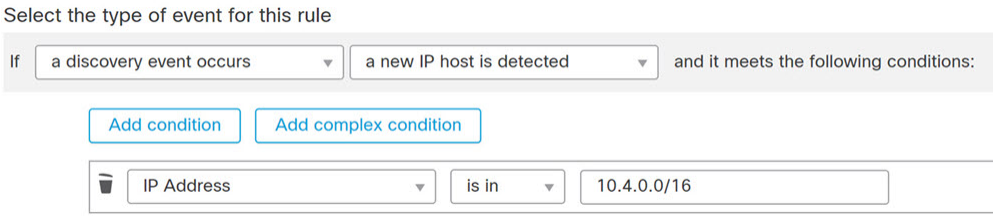
ほとんどの条件は、カテゴリ、演算子、値の 3 つの部分からなります。

- 相関ルール トリガー、ホスト プロファイル認定、接続トラッカー、ユーザ認定のどれを作成しているのかに応じて、選択できるカテゴリが異なります。相関ルール トリガーでは、さらにルールの基本イベントタイプにより選択できるカテゴリが異なります。条件によっては、それぞれ独自の演算子と値を持つ複数のカテゴリが含まれることがあります。
- 条件に使用可能な演算子はカテゴリによって異なります。
- 条件の値を指定するために使用できるシンタックスは、カテゴリと演算子に応じて異なります。場合によっては、テキストフィールドに値を入力する必要があります。それ以外の場合、ドロップダウンリストから値（1 つあるいは複数の値）を選択できます。

たとえば、新しいホストが検出されるたびに相関イベントを生成するには、条件を一切含まない単純なルールを作成できます。



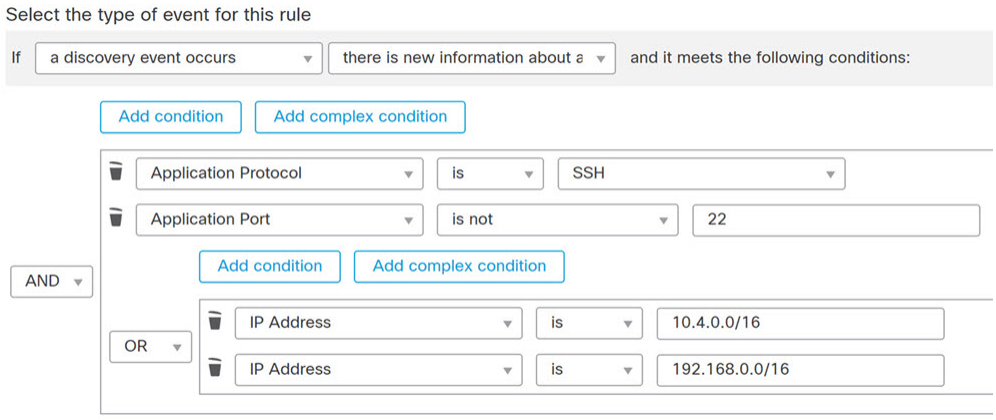
ルールをさらに制約して、新しいホストが 10.4.x.x ネットワークで検出された場合にのみイベントを生成するには、1 つの条件を追加できます。



構造に複数の条件を含める場合は、それらの条件を **AND** または **OR** 演算子でつなげる必要があります。同じレベルにある複数の条件は、合わせて評価されます。

- **AND** 演算子は、制御対象のレベルにあるすべての条件を満たす必要があることを示します。
- **OR** 演算子は、制御対象のレベルにある少なくとも 1 つの条件が満たされなければならないことを示します。

10.4.x.x ネットワークおよび 192.168.x.x ネットワーク上の非標準ポートで SSH アクティビティを検出する以下のルールには、4 つの条件が設定されており、下の 2 つは複合条件を形成しています。



論理的には、ルールは次のように評価されます。

```
(A and B and (C or D))
```

表 *142 :* ルールの評価

値	条件で指定する内容
A	アプリケーション プロトコルが SSH である
B	アプリケーション ポートが 22 ではない
C	IP アドレスが 10.0.0.0/8 内にある
D	IP アドレスが 196.168.0.0/16 内にある

注意 頻繁に発生するイベントによってトリガーされる複雑な相関ルールを評価することにより、システムパフォーマンスが低下する可能性があります。たとえば、ロギングするすべての接続に対して、複数の条件からなるルールをシステムが評価しなければならない場合、リソースが過負荷になる可能性があります。

相関ルールへの条件の追加とリンク設定

手順

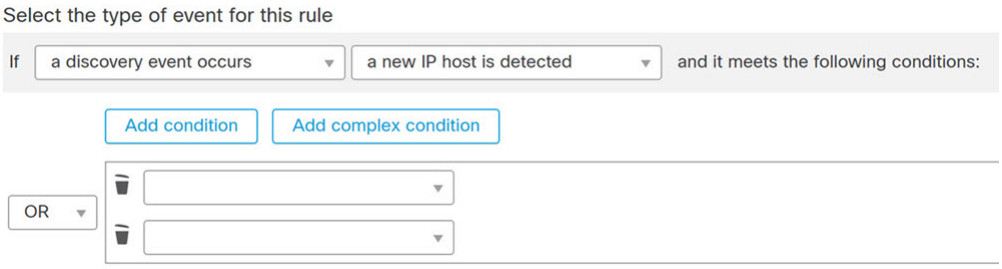
ステップ 1 相関ルールエディタ（**[ポリシー（Polices）]** > **[相関（Correlation）]** > **[ルール管理（Rule Management）]**）で、単純条件または複合条件を追加します。

- 単純：[条件の追加（Add condition）] をクリックします。
- 複合：[複合条件の追加（Add complex condition）] をクリックします。

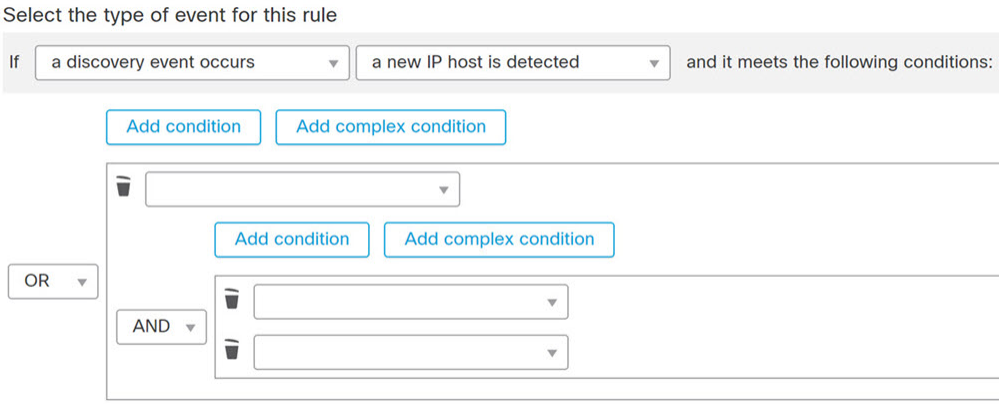
ステップ 2 条件の左にあるドロップダウン リストから [AND] または [OR] 演算子を選択して条件を結合します。

例:単純条件と複合条件の対比

次の図は、単純条件 2 つを [OR] 演算子で結合した相関ルールを示したものです。



次の図は、単純条件 1 つと、複合条件 1 つを [OR] 演算子で結合した相関ルールを示したものです。複合条件は 2 つの単純条件を [AND] 演算子で結合して構成します。



相関ルール条件での複数の値の使用

相関条件を作成するときに、条件の構文でドロップダウン リストから値を選択できる場合、通常はリストから複数の値を選択できます。

手順

ステップ 1 相関ルール エディタで、演算子として [存在する（is in）] または [存在しない（is not in）] を選択して 1 つの条件を作成します。

ステップ 2 テキスト フィールド内の任意の場所または [編集（Edit）] リンクをクリックします。

ステップ 3 [使用可能（Available）] の下にある複数の値を選択します。また、クリックしてドラッグすることで、隣接する複数の値を選択できます。

ステップ 4 右矢印（>）をクリックして、選択した項目を [Selected] に移動します。

ステップ 5 [OK] をクリックします。

相関ルールの管理

マルチドメイン展開では、現在のドメインで作成された相関ルールとグループが表示されます。これらは編集可能です。また、先祖ドメインからの選択した相関ルールとグループも表示されますが、これらは編集できません。下位のドメインで作成された相関ルールとグループを表示および編集するには、そのドメインに切り替えます。

（注） 設定に無関係なドメイン（名前、管理対象デバイスなど）に関する情報が公開されている場合、システムは先祖ドメインからの設定を表示しません。

アクティブな相関ポリシーのルールへの変更は、即座に反映されます。

始める前に

- ルールを削除する場合は、そのルールをすべての相関ポリシーから削除します。詳細については、相関ポリシーの管理 （1193 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[相関（Correlation）]** を選択し、[ルール管理（Rule Management）] をクリックします。

ステップ 2 ルールを管理します。

- 作成：[ルールの作成（Create Rule）] をクリックします。相関ルールの設定 （1193 ページ）を参照してください。
- グループの作成：[グループの作成（Create Group）] をクリックし、グループの名前を入力して、[保存（Save）] をクリックします。グループにルールを追加するには、ルールを編集します。
- 編集：**[編集（Edit）]**（ ）をクリックします。相関ルールの設定 （1193 ページ）を参照してください。 代わりに [表示（View）]（ ） が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ルールまたはルールグループの削除：[削除（Delete）]（ ） をクリックします。ルールグループを削除すると、ルールのグループ化が解除されます。 コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

相関応答グループの設定

アラートおよび修復の相関応答グループを作成し、グループをアクティブにして、アクティブな相関ポリシー内の相関ルールに割り当てることができます。システムは、ネットワークトラフィックが相関ルールに一致すると、すべてグループ化された応答を開始します。

アクティブなグループまたはいずれかのグループ化された応答に対する変更は、アクティブな相関ポリシーで行う場合、ただちに有効になります。

手順

ステップ 1 **[ポリシー（Policies）]** > **[相関（Correlation）]** を選択し、[グループ（Group）] をクリックします。

ステップ 2 [グループの作成（Create Group）] をクリックします。

ステップ 3 名前を入力します。

ステップ 4 作成時にグループをアクティブにする場合は、[アクティブ（Active）] チェックボックスをオンにします。

非アクティブ化されたグループは応答を開始しません。

ステップ 5 グループに [使用可能な応答（Available Responses）] を選択し、右矢印（>）をクリックして、それらを [グループ内の応答（Responses in Group）] に移動します。応答を他の方法で移動するには、左矢印（<）を使用します。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- 作成時にグループをアクティブにしなかった場合、アクティブにするには、スライダをクリックします。

関連トピック

Secure Firewall Management Center アラート応答 （673 ページ）
修復の概要 （1249 ページ）

相関応答グループの管理

応答グループは、相関ポリシーで使用されていない場合は削除できます。応答グループを削除することで、その応答のグループ化を解除します。また、応答グループを削除せずに、一時的に非アクティブにすることもできます。これにより、グループはシステムに残りますが、ポリシーに違反するときにはグループが開始されなくなります。

マルチドメイン展開では、現在のドメインで作成されたグループが表示されます。これは編集できます。先祖ドメインで作成されたグループも表示されますが、これは編集できません。下位のドメインで作成されたグループを表示および編集するには、そのドメインに切り替えます。

アクティブな使用中の応答グループへの変更は、即座に反映されます。

手順

ステップ 1 **[ポリシー（Policies）] > [相関（Correlation）]** を選択して、[グループ（Group）] をクリックします。

ステップ 2 応答グループを管理します。

- アクティブ化または非アクティブ化：スライダをクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 作成：[グループの作成（Create Group）] をクリックします。相関応答グループの設定 （1231 ページ） を参照してください。

- 編集：**[編集（Edit）]**（）をクリックします。相関応答グループの設定（1231 ページ）を参照してください。 代わりに [表示（View）]（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 削除：[削除（Delete）]（）をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

第 40 章

トラフィック プロファイル

ここでは、トラフィック プロファイルの設定方法について説明します。

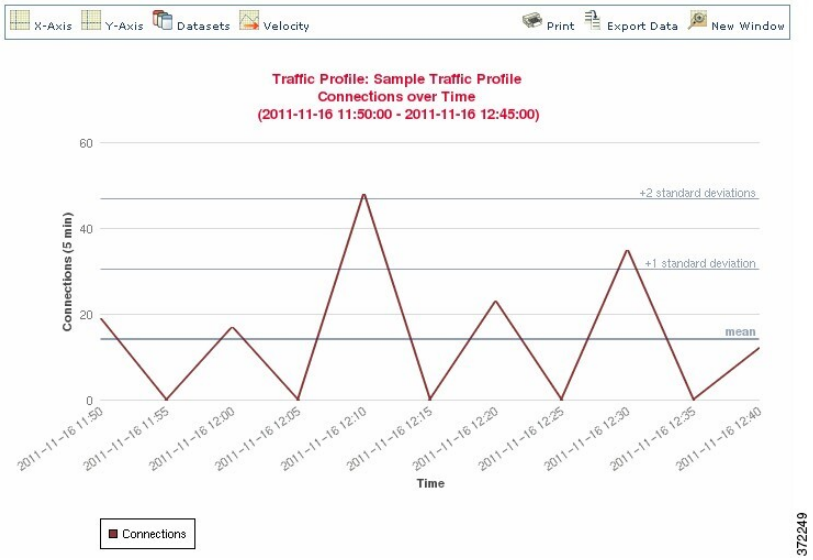
トラフィック プロファイルの概要

トラフィック プロファイルはプロファイル生成時間枠（PTW）内に収集した接続データを基に、ネットワーク トラフィックをグラフで表したものです。この測定結果が正常なネットワーク トラフィックを表しているものと推定します。学習期間が経過すると、新たなトラフィックをプロファイルに照らして評価することで異常なネットワーク トラフィックを検出します。

デフォルト PTW は 1 週間ですが、最短で 1 時間、最長で数週間に変更できます。デフォルトで、トラフィック プロファイルは5分間隔でシステム生成の接続イベントに関する統計情報を生成します。ただし、このサンプリング レートは最大 1 時間間隔まで拡大することができます。

ヒント シスコは少なくとも 100 のデータ ポイントを含む PTW の設定を推奨します。統計的に意味のある十分なデータがトラフィック プロファイルに含まれるように、PTW とサンプリング レートを設定する必要があります。

次の図は、PTW を 1 日、サンプリング レートを 5 分としたトラフィック プロファイルを示しています。



また、トラフィック プロファイルの非アクティブ期間を設定することもできます。トラフィック プロファイルは非アクティブ期間もデータ収集を行いますが、収集したデータをプロファイル統計の計算に使用しません。トラフィック プロファイルの時系列グラフでは、非アクティブ期間が網掛け領域として示されます。

たとえば、すべてのワークステーションが毎日深夜 0:00 にバックアップされるネットワーク インフラストラクチャがあるとします。バックアップには約30分かかり、その間はネットワーク トラフィックが急増します。予定されたバックアップ時間に合わせてトラフィック プロファイルの非アクティブ期間を繰り返すよう設定します。

（注） システムは接続の終了データを使って接続グラフとトラフィック プロファイルを作成します。トラフィック プロファイルを使用するには、必ず Management Center データベースに接続の終了イベントをロギングしてください。

トラフィック プロファイルの実装

トラフィック プロファイルを有効にすると、システムは設定した学習期間（PTW）の間接続データを収集し、評価します。システムは学習期間が経過すると、トラフィック プロファイルを対象にした相関ルールを評価します。

たとえば、ネットワークを通過するデータ量（パケット数、KB数、または接続数で測定）が、平均トラフィック量に比べて標準偏差の3倍も急激に上昇した場合、攻撃または他のセキュリティ ポリシー違反を示す可能性があると判断してトリガーするルールを作成できます。その後、このルールを相関ポリシーに組み込んで、トラフィックの急増に関するアラートを出したり、応答として修復を実行したりできます。

トラフィック プロファイルの対象設定

トラフィック プロファイルは、プロファイル条件とホスト プロファイル限定による制約を受けます。

プロファイル条件を使って、すべてのネットワーク トラフィックをプロファイリングすることもできます。また、トラフィック プロファイルの対象を絞って、特定のドメイン、特定のドメイン内や複数のドメイン内のサブネット、または個別のホストをモニタすることもできます。マルチドメイン展開では次のプロファイリングが可能です。

- リーフ ドメイン管理者は、リーフ ドメイン内のネットワーク トラフィックをプロファイリングできます。
- 高位レベル ドメインの管理者は、ドメイン内または複数ドメインでトラフィックのプロファイリングができます。

また、プロファイル条件では接続データに基づく基準を設けてトラフィック プロファイルを制約することもできます。たとえば、特定のポート、プロトコル、アプリケーションが使われているセッションのみトラフィック プロファイルでプロファイリングを行うようにプロファイル条件を設定できます。

また、トラッキング対象のホストに関する情報を使用してトラフィック プロファイルを制約することもできます。この制約は、ホストプロファイル限定と呼ばれます。たとえば、重要度の高いホストに限定して接続データを収集できます。

（注） トラフィック プロファイルを高位レベルのドメインに制約すると、各子孫リーフ ドメインのトラフィックと同じ種類のトラフィックが集約され、プロファイリングされることになります。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、ドメイン間のトラフィックをプロファイルすると、予期しない結果になる可能性があります。

関連トピック

相関ポリシーとルールの概要 （1189 ページ）

トラフィック プロファイル条件

単純なトラフィック プロファイル条件とホスト プロファイル限定を作成できます。また、複数の条件の組み合わせとネストによってより複雑な構造を作成することもできます。

条件には、カテゴリ、演算子、および値という 3 つの部分があります。

- 使用できるカテゴリは、トラフィック プロファイル条件を作成しているか、それともホスト プロファイル限定を作成しているかに応じて異なります。
- 使用できる演算子は、選択したカテゴリによって異なります。

- 条件の値を指定するために使用できる構文は、カテゴリと演算子に応じて異なります。場合によっては、テキストフィールドに値を入力する必要があります。それ以外の場合、ドロップダウンリストから 1 つ以上の値を選択できます。

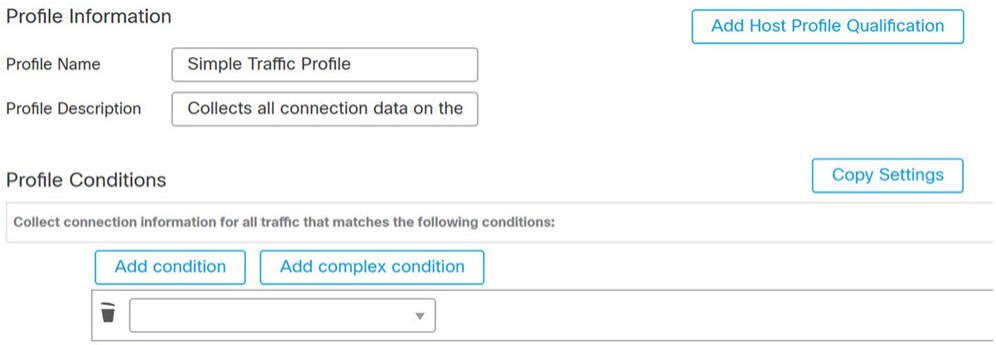
ホストプロファイル限定の場合、開始側または応答側のホストに関する情報のデータを使用して、トラフィック プロファイルに制約を適用するかどうかを指定する必要もあります。

構造に複数の条件を含める場合は、それらの条件を **AND** または **OR** 演算子でつなげる必要があります。同じレベルにある複数の条件は、合わせて評価されます。

- **AND** 演算子は、制御対象のレベルにあるすべての条件を満たす必要があることを示します。
- **OR** 演算子は、制御対象のレベルにある少なくとも 1 つの条件が満たされなければならないことを示します。

制約が適用されていないトラフィック プロファイル

モニター対象ネットワーク セグメント全体のデータを収集するトラフィック プロファイルを作成する場合、次の図に示すように、条件を含まない非常に単純なプロファイルを作成できます。



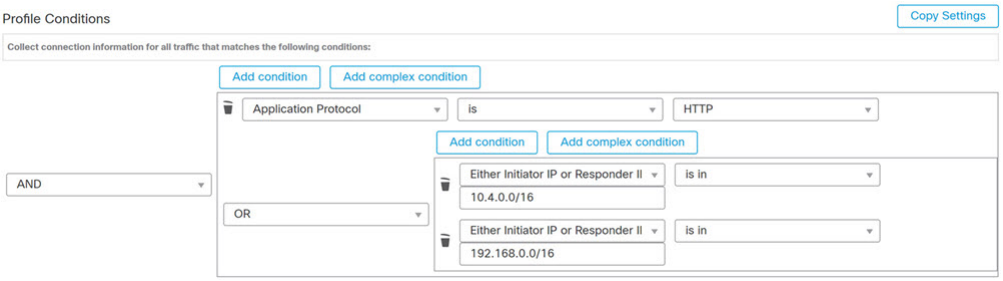
単純なトラフィック プロファイル

プロファイルに制約を適用して、1 つのサブネットのデータのみを収集するには、次の図に示すように 1 つの条件を追加できます。

複雑なトラフィック プロファイル

次のトラフィック プロファイルには、[および（AND）] で結合された 2 つの条件が含まれています。つまり、両方の条件とも満たされる場合に限り、このトラフィック プロファイルは接続データを収集します。この例では、特定のサブネット内の IP アドレスを持つすべてのホストに関する HTTP 接続を収集します。

一方、次のトラフィック プロファイルでは、2 つのサブネットのいずれかの HTTP アクティビティに関する接続データを収集しますが、最後は複合条件を構成しています。



論理的には、上記のトラフィック プロファイルは次のように評価されます。

```
(A and (B or C))
```

値	条件で指定する内容
A	アプリケーション プロトコル名が HTTP である
B	IP アドレスが 10.4.0.0/16 内にある
C	IP アドレスが 192.168.0.0/16 内にある

トラフィックプロファイルの要件と前提条件

モデルのサポート

任意（Any）

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 検出管理者（Discovery Admin）

トラフィック プロファイルの管理

アクティブで完全なトラフィック プロファイルに対して記述されたルールのみが、相関ポリシー違反をトリガーできます。各トラフィックプロファイルの横にあるスライダは、プロファイルがアクティブでありデータを収集しているかどうかを示します。経過表示バーは、トラフィック プロファイルの学習期間のステータスを示します。

マルチドメイン展開では、現在のドメインで作成されたトラフィック プロファイルが表示されます。これは、編集が可能なプロファイルです。また、先祖ドメインからの選択したトラフィックプロファイルも表示されますが、これは編集できません。下位のドメインで作成されたトラフィック プロファイルを表示および編集するには、そのドメインに切り替えます。

（注） プロファイルの条件が無関係なドメインに関する情報（名前や管理対象デバイスなど）を公開する場合、システムは先祖ドメインからのトラフィック プロファイルを表示しません。

手順

ステップ 1 **[ポリシー（Policies）]** > **[相関（Correlation）]** を選択し、[トラフィックプロファイル（Traffic Profiles）] をクリックします。

ステップ 2 トラフィック プロファイルを管理します。

- アクティブ化/非アクティブ化：トラフィック プロファイルをアクティブ化または非アクティブ化するには、スライダをクリックします。トラフィックプロファイルを非アクティブ化すると、そのプロファイルに関連するデータが削除されます。プロファイルを再度アクティブ化する場合は、そのプロファイルに関して作成されたルールがトリガーするようになるまで、PTW の長さだけ待つ必要があります。
- 作成：新しいトラフィック プロファイルを作成するには、[新規プロファイル（New Profile）]をクリックして、トラフィック プロファイルの設定（1241 ページ） で説明する手順を実行します。また、[コピー（Copy）]（）をクリックして、既存のトラフィックプロファイルのコピーを編集することもできます。
- 削除：トラフィックプロファイルを削除するには、[削除（Delete）]（）をクリックして、選択内容を確認します。

- 編集：既存のトラフィックプロファイルを変更するには、**[編集（Edit）]**（）をクリックして、トラフィックプロファイルの設定（1241ページ）で説明する手順を実行します。トラフィック プロファイルがアクティブな場合は、そのプロファイルの名前と説明のみを変更できます。
- グラフ：グラフとしてトラフィックプロファイルを表示するには、[グラフ（Graph）]（）をクリックします。マルチドメイン展開では、グラフが無関係なドメインに関する情報を公開する場合、先祖ドメインに属しているトラフィック プロファイルのグラフを表示できません。

トラフィック プロファイルの設定

トラフィック プロファイルを高位レベルのドメインに制約すると、各子孫リーフ ドメインのトラフィックと同じ種類のトラフィックが集約され、プロファイリングされることになります。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、ドメイン間のトラフィックをプロファイルすると、予期しない結果になる可能性があります。

手順

ステップ 1 **[ポリシー（Policies）]** > **[相関（Correlation）]** を選択し、[トラフィックプロファイル（Traffic Profiles）] をクリックします。

ステップ 2 [新規プロファイル（New Profile）] をクリックします。

ステップ 3 プロファイル名を入力し、オプションでプロファイルの説明を入力します。

ステップ 4 オプションで、トラフィック プロファイルを制約します。

- 設定のコピー：既存のトラフィック プロファイルから設定をコピーするには、[設定のコピー（Copy Settings）] をクリックし、使用するトラフィック プロファイルを選択して [ロード（Load）] をクリックします。
- プロファイル条件：トラッキング対象の接続の情報を使用してトラフィック プロファイルを制約するには、トラフィック プロファイル条件の追加（1242ページ）の説明に従って続行します。
- ホスト プロファイル認定：トラッキング対象のホストの情報を使用してトラフィック プロファイルを制約するには、トラフィック プロファイルへのホスト プロファイル認定の追加（1243 ページ）の説明に従って続行します。
- プロファイルの時間帯（PTW）：プロファイルの時間帯を変更するには、時間の単位を入力し、[時間（hour(s)）]、[日（day(s)）]、または [週（week(s)）] を選択します。
- サンプリング レート：サンプリング レートを分単位で選択します。
- 非アクティブ期間：[非アクティブ期間の追加（Add Inactive Period）] をクリックし、ドロップダウン リストを使用して、トラフィック プロファイルを非アクティブなままにする日時と頻度を指定します。非アクティブなトラフィック プロファイルは、相関ルールを

トリガーしません。トラフィック プロファイルでは、プロファイルの統計情報に非アクティブな期間のデータを含めません。

ステップ 5 トラフィック プロファイルを保存します。

- プロファイルを保存し、ただちにデータを収集し始めるには、[保存してアクティブにする（Save & Activate）] をクリックします。
- アクティブ化せずにプロファイルを保存するには、[保存（Save）] をクリックします。

トラフィック プロファイル条件の追加

手順

ステップ 1 トラフィック プロファイル エディタの [プロファイル条件（Profile Conditions）] で、追加する各条件について [条件の追加（Add condition）] または [複合条件の追加（Add complex condition）] をクリックします。同レベルの条件は一緒に評価されます。

- 演算子で結ばれた同一のレベルのすべての条件が満たされるべきことを指定するには、[AND] を選択します。
- 演算子で結ばれた同一のレベルの 1 つの条件だけが満たされるべきことを指定するには、[OR] を選択します。

ステップ 2 トラフィック プロファイル条件の構文（1244 ページ） と トラフィック プロファイル条件（1237 ページ） の説明に従い、各条件のカテゴリ、演算子、値を指定します。

演算子として [含まれる（is in）] または [含まれない（is not in）] を選択した場合は、トラフィック プロファイル条件での複数の値の使用（1248 ページ） に説明してあるように単一の条件で複数の値を選択できます。

カテゴリが IP アドレスを表している場合、演算子として [含まれる（is in）] または [含まれない（is not in）] を選択すると、IP アドレス範囲内にその IP アドレスが含まれるのか、含まれないのかを指定できます。

例

次のトラフィック プロファイルは、特定のサブネットの情報を集めます。条件のカテゴリは [イニシエータ/レスポンダ IP（Initiator/Responder IP）]、演算子は [含まれる（is in）]、値は `10.4.0.0/16` です。

関連トピック

IP アドレスの規則 （31 ページ）

トラフィック プロファイルへのホスト プロファイル認定の追加

手順

ステップ 1 トラフィック プロファイル エディタで、[ホスト プロファイル認定の追加（Add Host Profile Qualification）] をクリックします。

ステップ 2 [ホスト プロファイル認定（Host Profile Qualification）] で、追加する各条件について [条件の追加（Add condition）] または [複合条件の追加（Add complex condition）] をクリックします。同レベルの条件は一緒に評価されます。

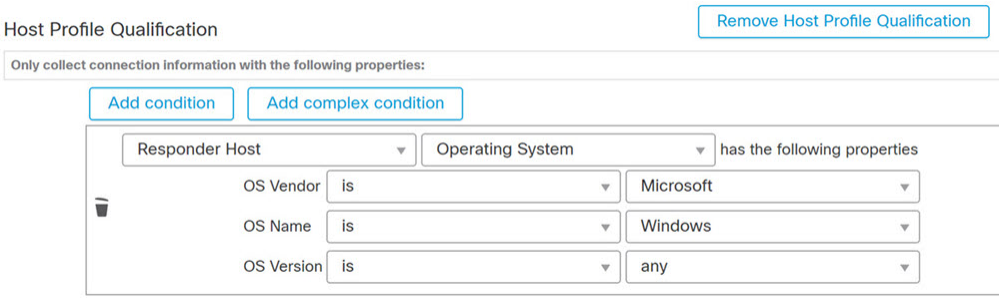
- 演算子で結ばれた同一のレベルのすべての条件が満たされるべきことを指定するには、[AND] を選択します。
- 演算子で結ばれた同一のレベルの 1 つの条件だけが満たされるべきことを指定するには、[OR] を選択します。

ステップ 3 トラフィック プロファイルのホスト プロファイル限定の構文 （1245 ページ） と トラフィック プロファイル条件 （1237 ページ） の説明に従い、各条件のホストタイプ、カテゴリ、演算子、値を指定します。

演算子として [含まれる（is in）] または [含まれない（is not in）] を選択した場合は、トラフィック プロファイル条件での複数の値の使用 （1248 ページ） に説明してあるように単一の条件で複数の値を選択できます。

例

次のホスト プロファイル認定によりトラフィック プロファイルが制約され、検出された接続内の応答側ホストで任意のバージョンの Microsoft Windows が実行されている場合にのみ、接続データが収集されます。



トラフィック プロファイル条件の構文

次の表で、トラフィック プロファイル条件を作成する方法について説明します。トラフィック プロファイルの作成に使用可能な接続データは、トラフィックの特性と検出方法を含む複数の要因によって変わることに留意してください。

表 *143*: トラフィック プロファイル条件の構文

次を選択できます。	選択する演算子と内容
アプリケーション プロトコル	アプリケーション プロトコルを 1 つ以上選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコル カテゴリを 1 つ以上選択します。
クライアント	クライアントを 1 つ以上選択します。
クライアント カテゴリ	クライアント カテゴリを 1 つ以上選択します。
接続タイプ	プロファイルが管理対象デバイスによってモニターされるトラフィックからの接続データ、またはエクスポートされた NetFlow レコードからの接続データを使用するかどうかを選択します。 接続タイプを指定しない場合、トラフィック プロファイルには両方が含まれます。
接続先（国）または送信元（国）	国を 1 つ以上選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。
イニシエータ IP、レスポンダ IP、またはイニシエータ/レスポンダ IP	IP アドレス、または IP アドレスの範囲を入力します。 システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

次を選択できます。	選択する演算子と内容
NetFlow デバイス	トラフィック プロファイルの作成に使用するデータの NetFlow エクスポータを選択します。
レスポンダ ポート/ICMP コード	ポート番号または ICMP コードを入力します。
セキュリティ インテリジェンス カテゴリ	セキュリティ インテリジェンスのカテゴリを 1 つ以上選択します。 トラフィック プロファイル条件にセキュリティ インテリジェンスのカテゴリを使用するには、アクセス コントロール ポリシーでそのカテゴリを [ブロック（Block）] ではなく [モニタ（Monitor）] に設定する必要があります。
SSL 暗号化セッション（SSL Encrypted Session）	[正常に復号（Successfully Decrypted）] を選択します。
トランスポート プロトコル	トランスポート プロトコルとして **TCP** または **UDP** と入力します。
Web アプリケーション	Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。

関連トピック

接続イベント フィールドの入力の要件 （926 ページ）
IP アドレスの規則 （31 ページ）

トラフィック プロファイルのホスト プロファイル限定の構文

ホスト プロファイル限定の条件を作成するときには、まず、トラフィック プロファイルを制約するために使用するホストを選択する必要があります。[レスポンダ ホスト（Responder Host）] または [イニシエータ ホスト（Initiator Host）] のいずれかを選択できます。ホスト ロールを選択したら、ホスト プロファイル限定の条件の作成を続行します。

NetFlow レコードを使用してネットワーク マップにホストを追加できますが、これらのホストに関する利用可能な情報は限定されています。たとえば、これらのホストに利用可能なオペレーティング システム データは得られません（ただしホスト入力機能を使って指定する場合を除く）。さらに、エクスポートされた NetFlow レコードからの接続データをトラフィック プロファイルで使用する場合、NetFlow レコードには、どのホストが接続のイニシエータで、どのホストがレスポンダであるかを示す情報が含まれないことに注意してください。システムは、NetFlow レコードを処理するときに、それぞれのホストが使用しているポートとそれらのポートが既知かどうかに基づいて、この情報を判断するアルゴリズムを使用します。

暗黙的（または汎用の）クライアントを照合するには、クライアントに応答するサーバで使われるアプリケーション プロトコルに基づいてホスト プロファイル限定を作成します。接続のイニシエータ（または送信元）として機能するホスト上のクライアント リストに含まれるアプ

リケーションプロトコル名の後に**クライアント**が続いている場合、そのクライアントは実際には暗黙的クライアントである可能性があります。つまり、検出されたクライアントトラフィックに基づいてではなく、そのクライアントのアプリケーションプロトコルを使用するサーバ応答トラフィックに基づいて、システムがそのクライアントを報告します。

たとえば、ホスト上のクライアントとして**HTTPS クライアント**がシステムにより報告される場合、[アプリケーション プロトコル（Application Protocol）] を [HTTPS] に設定した [レスポンダ ホスト（Responder Host）] のホスト プロファイル限定を作成します。これは、レスポンダまたは宛先ホストから送られる HTTPS サーバ応答トラフィックに基づいて HTTPS クライアントが汎用クライアントとして報告されるためです。

表 *144 :* ホスト プロファイル限定の構文

次を選択できます。	選択する演算子と内容
[アプリケーションプロトコル（Application Protocol）]>[アプリケーションプロトコル（Application Protocol）]	アプリケーション プロトコルを 1 つ以上選択します。
[アプリケーションプロトコル（Application Protocol）]>[アプリケーション ポート（Application Port）]	アプリケーション プロトコルのポート番号を入力します。
[アプリケーションプロトコル（Application Protocol）]>[プロトコル（Protocol）]	プロトコルを選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコル カテゴリを 1 つ以上選択します。
[クライアント（Client）]>[クライアント（Client）]	クライアントを 1 つ以上選択します。
[クライアント（Client）]>[クライアント バージョン（Client Version）]	クライアント バージョンを入力します。
クライアント カテゴリ	クライアント カテゴリを 1 つ以上選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。
ハードウェア	モバイルデバイスのハードウェア モデルを入力します。たとえば、すべての Apple iPhone に一致させるには `iPhone` と入力します。
[ホストの重要度（Host Criticality）]	ホストの重要度を選択します。

次を選択できます。	選択する演算子と内容
ホスト タイプ	ホスト タイプを 1 つ以上選択します。通常のホスト、またはいずれかのタイプのネットワーク デバイスを選択できます。
[IOC タグ（IOC Tag）]	IOC タグを 1 つ以上選択します。
ジェイルブロークン	イベントのホストがジェイルブレイクされたモバイル デバイスであることを示すには [はいい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。
[MAC アドレス（MAC Address）] > [MAC アドレス（MAC Address）]	ホストの MAC アドレス全体またはその一部を入力します。
[MAC アドレス（MAC Address）] > [MAC タイプ（MAC Type）]	MAC タイプが [ARP/DHCP で検出（ARP/DHCP Detected）] されるかどうかを選択します。つまり、次のいずれかです。 • システムは MAC アドレスがホストに属していることをポジティブに識別した（[ARP/DHCP で検出（is ARP/DHCP Detected）]） • たとえば、デバイスとホスト間にはルータがあるため、システムはその MAC アドレスを持つ多くのホストを認識している（[ARP/DHCP で検出されない（is not ARP/DHCP Detected）]） • MAC タイプが無関係（[どれでもない（is any）]）
[MAC ベンダー（MAC Vendor）]	ホストが使用するハードウェアの MAC ベンダー全体またはその一部を入力します。
Mobile	イベントのホストがモバイル デバイスであることを示すには [はい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。
NETBIOS 名	ホストの NetBIOS 名を入力します。
ネットワーク プロトコル	http://www.iana.org/assignments/ethernet-numbers にリストされているネットワーク プロトコル番号を入力します。
[オペレーティング システム（Operating System）] > [OS ベンダー（OS Vendor）]	オペレーティング システムのベンダー名を 1 つ以上選択します。
[オペレーティング システム（Operating System）] > [OS 名（OS Name）]	オペレーティング システムの名前を 1 つ以上選択します。
[オペレーティング システム（Operating System）] > [OS バージョン（OS Version）]	オペレーティング システムのバージョンを 1 つ以上選択します。

次を選択できます。	選択する演算子と内容
[トランスポートプロトコル（Transport Protocol）]	http://www.iana.org/assignments/protocol-numbers にリストされているトランスポート プロトコルの名前または番号を入力します。
VLAN ID（Admin. VLAN ID）	ホストの VLAN ID 番号を入力します。 システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際の VLAN タグを使用してこの設定を抑制すると、予期しない結果になる可能性があります。
Web アプリケーション	Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。
使用可能な任意のホスト属性（デフォルト コンプライアンス allow リスト ホスト属性を含む）	選択するホスト属性のタイプに応じて、適切な値を次のように指定します。 • ホスト属性タイプが Integer の場合、その属性で定義されている範囲内の整数値を入力します。 • ホスト属性タイプが Text の場合、テキスト値を入力します。 • ホスト属性タイプが List の場合、有効なリスト文字列を選択します。 • ホスト属性タイプが URL の場合、URL 値を入力します。

トラフィック プロファイル条件での複数の値の使用

条件を作成するときに、条件の構文でドロップダウン リストから値を選択できる場合、通常はリストから複数の値を選択できます。

たとえば、ホストで何らかの UNIX フレーバを実行している必要があることを示すホスト プロファイル限定をトラフィック プロファイルに追加するには、多数の条件を OR 演算子で結合する代わりに、以下の手順を使用できます。

手順

ステップ 1 トラフィック プロファイルまたはホスト プロファイルの資格条件を作成するときに、演算子として [存在する（is in）] または [存在しない（is not in）] を選択します。
ドロップダウン リストがテキスト フィールドに変わります。

ステップ 2 テキスト フィールド内の任意の場所または [編集（Edit）] リンクをクリックします。

ステップ 3 [使用可能（Available）] の下にある複数の値を選択します。

ステップ 4 右矢印をクリックして、選択した項目を [選択済み（Selected）] に移動します。

ステップ 5 [OK] をクリックします。

第 41 章

修復

以下のトピックでは、修復の設定について説明します。

修復の要件と前提条件

モデルのサポート

任意（Any）

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 検出管理者（Discovery Admin）

修復の概要

修復はシステムが相関ポリシー違反に応じて起動するプログラムです。

修復を実行すると、システムは修復ステータス イベントを生成します。修復ステータス イベントには、修復の名前、相関ポリシー、修復をトリガーしたルール、終了ステータス メッセージなどの詳細が含まれています。

システムは以下に挙げる複数の修復モジュールをサポートしています。

- Cisco ISE 適応型ネットワーク制御（ANC）：相関ポリシー違反に関連する ISE 設定 ANC ポリシーが適用またはクリアされます。
- Cisco IOS Null ルート：相関ポリシー違反に関連するホストやネットワークへ送信されるトラフィックをブロックします（Cisco IOS バージョン 12.0 以降が必要）。
- Nmap スキャン：ホストをスキャンして、実行中のオペレーティング システムおよびサーバを決定します。
- 属性値の設定：相関ポリシー違反に関連するホストのホスト属性を設定します。

ヒント　他のタスクを実行するカスタム モジュールをインストールすることもできます。*Firepower System Remediation API Guide*を参照してください。

修復の実装

修復を実装するには、まず選択したモジュールに対して少なくとも 1 つのインスタンスを作成します。モジュールごとに複数のインスタンスを作成することができ、各インスタンスは別々に設定できます。たとえば、Cisco IOS Null ルート修復モジュールを使用して複数のルータと通信するには、そのモジュールのインスタンスを複数設定します。

次に、ポリシー違反の際に実行するアクションを説明する複数の修復を各インスタンスに追加します。

最後に、相関ポリシーに応じてシステムが修復を開始するように相関ポリシーで修復とルールを関連付けます。

修復およびマルチテナンシー

マルチドメイン展開では、どのドメインのレベルでもカスタムの修復モジュールをインストールできます。システム提供のモジュールはグローバル ドメインに属します。

先祖ドメインで作成されたインスタンスに修復を追加することはできませんが、現在のドメインで同様に設定されるインスタンスを作成し、そのインスタンスに修復を追加することは可能です。また、先祖ドメインで作成した修復は、相関応答として使用することもできます。

関連トピック

Secure Firewall Management Center アラート応答 （673 ページ）
Nmap スキャン
ルールと許可（Allow）リストに応答を追加する （1192 ページ）

Cisco ISE EPS 修復

ISE 導入環境で、エンドポイント保護サービス（EPS）が設定され、有効になっている場合、Management Center を設定することで、ISE を使った修復を起動させることが可能です。ISE EPS 修復は、完全に設定された状態では、相関ポリシー違反を起こした送信元または宛先ホストに対し、次の**緩和アクション（Mitigation Actions）**を実行します。

- **検疫（quarantine）**：エンドポイントのネットワークへのアクセスを制限または拒否します。
- **隔離解除（unquarantine）**：エンドポイントの検疫ステータスを解除し、ネットワークへのフル アクセスを許可します。
- **シャットダウン（shotdown）**：エンドポイントのNASポートを非アクティブ化し、ネットワークから切断します。

特定の IP アドレスを ISE EPS 修復から除外することもできます。

（注） 使用する ISE のバージョンと設定は、ISE の使用方法に影響を与えます。たとえば、ISE-PIC では、ISE EPS 修復を実行できません。詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの「*User Control with ISE/ISE-PIC*」の章を参照してください。

ISE EPS アクションの詳細については、『*Cisco Identity Services Engine User Guide*』を参照してください。

ISE EPS 修復の設定

送信元または宛先ホストで ISE EPS 修復を実行することによって、相関ポリシー違反に応答できます。

（注） ISE-PIC は ISE EPS 修復を実行できません。

始める前に

- ISE サーバ上で EPS 操作を設定します。
- Cisco Secure Firewall Management Center デバイス構成ガイドの ISE/PIC の設定に関する章を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]>[アクション（Actions）]>[インスタンス（Instances）]**を選択します。

ステップ 2 ISE EPS インスタンスの追加 （1252 ページ）の説明に従ってpxGrid緩和インスタンスを追加します。

ステップ 3 ISE EPS 修復の追加 （1252 ページ）の説明に従って 1 つ以上の ISE EPS 修復を追加します。

次のタスク

- ルールと許可（Allow）リストに応答を追加する （1192 ページ）の説明に従って相関ポリシー違反への応答として修復を割り当てます。

ISE EPS インスタンスの追加

ISE EPS インスタンスを作成し、ロギング タイプごとに個々の修復をグループ化します。

手順

ステップ 1 **[ポリシー（Policies）]>[アクション（Actions）]>[インスタンス（Instances）]**を選択します。

ステップ 2 [新規インスタンスの追加（Add a New Instance）] リストから、モジュール タイプとして [pxGrid Mitigation(v1.0)] を選択し、[追加（Add）] をクリックします。

ステップ 3 [インスタンス名（Instance Name）] と [説明（Description）] に入力します。

ステップ 4 [ロギングの有効化（Enable Logging）] オプションを設定し、システムロギングを有効または無効にします。

ステップ 5 [作成（Create）] をクリックします。

次のタスク

- セット属性値修復の追加 （1260 ページ）の説明に従って ISE EPS 修復を作成します。

関連トピック

IP アドレスの規則 （31 ページ）

ISE EPS 修復の追加

相関ポリシー違反に含まれる送信元または宛先ホストで [緩和アクション（Mitigation Actions）] を実行するため、インスタンス内に 1 つ以上の ISE EPS 修復を作成します。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

始める前に

- ISE EPS インスタンスの追加 （1252 ページ）の説明に従って ISE EPS インスタンスを作成します。

手順

ステップ 1 **[ポリシー（Policies）]>[アクション（Actions）]>[インスタンス（Instances）]**を選択します。

ステップ 2 修復を追加するインスタンスの横にある[表示（View）]（👁）をクリックします。

ステップ 3 [設定済み修復（Configured Remediations）] セクションで、[宛先の緩和（Mitigate Destination）] または [送信元の緩和（Mitigate Source）] を選択し、[追加（Add）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] に入力します。

ステップ 5 次のいずれかの緩和アクションを選択します。[検疫（quarantine）]、[隔離解除（unquarantine）]、[シャットダウン（shutdown）] 。

ステップ 6 （任意）IP アドレスまたは範囲を修復から除外するには、それらを [許可リスト（Allow List）] ボックスに入力します。

ステップ 7 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールと許可（Allow）リストに応答を追加する （1192 ページ） を参照）。

Cisco IOS Null ルート修復

Cisco IOS Null ルート修復モジュールでは、シスコ「null route」コマンドを使って、個別の IP アドレスまたは IP アドレスの範囲をブロックすることができます。これにより、ホストまたはネットワークに送信されるすべてのトラフィックがルータの NULL インターフェイスにルーティングされ、ドロップされます。違反ホストまたはネットワークから送信されるトラフィックはブロックされません。

（注） ディスカバリまたはホスト入力イベントに基づく相関ルールへの応答として接続先ベースの修復を使用しないでください。これらのイベントは、送信元ホストに関連付けられています。

注意 Cisco IOS 修復がされている間は、タイムアウト期間はありません。IP アドレスまたはネットワークのブロックを解除するには、ルータから手動でルーティング変更をクリアする必要があります。

Cisco IOS ルータ用修復の設定

（注） ディスカバリまたはホスト入力イベントに基づく相関ルールへの応答として接続先ベースの修復を使用しないでください。これらのイベントは、送信元ホストに関連付けられています。

⚠

注意 Cisco IOS 修復がされている間は、タイムアウト期間はありません。IP アドレスまたはネットワークのブロックを解除するには、ルータから手動でルーティング変更をクリアする必要があります。

始める前に

- Cisco ルータが Cisco IOS 12.0 以降を実行していることを確認します。
- ルータへのレベル 15 の管理アクセス権を持っていることを確認します。

手順

ステップ 1 Cisco ルータまたは IOS ソフトウェアに付属のドキュメントの説明に従って、Cisco ルータで Telnet を有効にします。

ステップ 2 Management Center で、使用する予定の各 Cisco IOS ルータに対する Cisco IOS ヌル ルート インスタンスを追加します。Cisco IOS インスタンスの追加 （1254 ページ）を参照してください。

ステップ 3 相関ポリシーに違反した場合にルータで実現する応答のタイプに基づき、インスタンスごとに修復を作成します。

- Cisco IOS ブロック宛先の修復の追加 （1255 ページ）
- Cisco IOS ブロック宛先ネットワークの修復の追加 （1256 ページ）
- Cisco IOS ブロック送信元の修復の追加 （1257 ページ）
- Cisco IOS ブロック送信元ネットワークの修復の追加 （1258 ページ）

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールと許可（Allow）リストに応答を追加する （1192 ページ） を参照）。

Cisco IOS インスタンスの追加

修復を送信するルータが複数ある場合は、各ルータに対して別々のインスタンスを作成します。

始める前に

- ルータまたは IOS ソフトウェアのドキュメントの説明に従って、Cisco IOS ルータの Telnet アクセスを設定します。

手順

ステップ 1 **[ポリシー（Policies）]**>**[アクション（Actions）]**>**[インスタンス（Instances）]**を選択します。

ステップ 2 [新しいインスタンスの追加（Add a New Instance）] リストから [Cisco IOS Null ルート（Cisco IOS Null Route）] を選択し、[追加（Add）] をクリックします。

ステップ 3 [インスタンス名（Instance Name）] と [説明（Description）] を入力します。

ステップ 4 [ルータ IP（Router IP）] フィールドに、修復のために使用する Cisco IOS ルータの IP アドレスを入力します。

ステップ 5 [ユーザー名（Username）] フィールドに、ルータの Telnet ユーザー名を入力します。このユーザは、ルータでレベル 15 管理アクセスを持っている必要があります。

ステップ 6 [接続パスワード（Connection Password）] フィールドに、Telnet ユーザのパスワードを入力します。

ステップ 7 [イネーブル パスワード（Enable Password）] フィールドに、Telnet ユーザのイネーブル パスワードを入力します。これは、ルータの特権モードに入るために使用するパスワードです。

ステップ 8 **[許可リスト（Allow List）]** フィールドに、修復から除外する IP アドレスまたは範囲を 1 行につき 1 つ入力します。

（注） システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 9 [作成（Create）] をクリックします。

次のタスク

- Cisco IOS ブロック宛先の修復の追加 （1255 ページ）、Cisco IOS ブロック宛先ネットワークの修復の追加 （1256 ページ）、Cisco IOS ブロック送信元の修復の追加 （1257 ページ）、および Cisco IOS ブロック送信元ネットワークの修復の追加 （1258 ページ）の説明に従い、相関ポリシーで使用する特定の修復を追加します。

関連トピック

IP アドレスの規則 （31 ページ）

Cisco IOS ブロック宛先の修復の追加

Cisco IOS ブロック宛先修復は、ルータから、相関ポリシー違反に関与している宛先ホストに送信されるトラフィックをブロックします。この修復を、検出またはホスト入力イベントに基づく相関ルールへの応答として使用しないでください。これらのイベントは、送信元ホストに関連付けられています。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

始める前に

- Cisco IOS インスタンスの追加 （1254 ページ） の説明に従い、Cisco IOS インスタンスを追加します。

手順

ステップ 1 **[ポリシー（Policies）]>[アクション（Actions）]>[インスタンス（Instances）]**を選択します。

ステップ 2 修復を追加するインスタンスの横にある[表示（View）]（👁）をクリックします。

ステップ 3 [設定されている修復（Configured Remediations）] セクションで、[宛先のブロック（Block Destination）] を選択し、[追加（Add）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] を入力します。

ステップ 5 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールと許可（Allow）リストに応答を追加する （1192 ページ） を参照）。

Cisco IOS ブロック宛先ネットワークの修復の追加

Cisco IOS ブロック宛先ネットワーク修復は、ルータから、相関ポリシー違反に関与している宛先ホストのネットワークに送信されるトラフィックをブロックします。この修復を、検出またはホスト入力イベントに基づく相関ルールへの応答として使用しないでください。これらのイベントは、送信元ホストに関連付けられています。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

始める前に

- Cisco IOS インスタンスの追加 （1254 ページ） の説明に従い、Cisco IOS インスタンスを追加します。

手順

ステップ 1 **[ポリシー（Policies）]>[アクション（Actions）]>[インスタンス（Instances）]**を選択します。

ステップ 2 修復を追加するインスタンスの横にある[表示（View）]（👁）をクリックします。

ステップ 3 [設定されている修復（Configured Remediations）] セクションで、[宛先ネットワークのブロック（Block Destination Network）] を選択し、[追加（Add）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] を入力します。

ステップ 5 [ネットマスク（Netmask）] フィールドに、サブネット マスクを入力するか、または CIDR 表記を使用して、トラフィックをブロックするネットワークを記述します。

たとえば、1 つのホストがルールをトリガーとして使用したときにクラス C ネットワーク全体へのトラフィックをブロックするには、ネットマスクとして `255.255.255.0` または `24` を使用します。

別の例として、トリガーの IP アドレスを含む 30 個のアドレスへのトラフィックをブロックするには、ネットマスクとして `255.255.255.224` または `27` を指定します。この場合、IP アドレス `10.1.1.15` が修復をトリガーとして使用し、`10.1.1.1` と `10.1.1.30` の間のすべての IP アドレスがブロックされます。トリガーの IP アドレスのみをブロックするには、このフィールドは空のままにして、`32` を入力するか、または `255.255.255.255` を入力します。

ステップ 6 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールと許可（Allow）リストに応答を追加する （1192 ページ） を参照）。

関連トピック

IP アドレスの規則 （31 ページ）

Cisco IOS ブロック送信元の修復の追加

Cisco IOS ブロック送信元修復は、ルータから、相関ポリシー違反に関与している送信元ホストに送信されるトラフィックをブロックします。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

始める前に

- Cisco IOS インスタンスの追加 （1254 ページ） の説明に従い、Cisco IOS インスタンスを追加します。

手順

ステップ 1 **[ポリシー（Policies）]>[アクション（Actions）]>[インスタンス（Instances）]**を選択します。

ステップ 2 修復を追加するインスタンスの横にある[表示（View）]（  ）をクリックします。

ステップ 3 [設定されている修復（Configured Remediations）] セクションで、[送信元のブロック（Block Source）] を選択し、[追加（Add）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] を入力します。

ステップ 5 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールと許可（Allow）リストに応答を追加する （1192 ページ） を参照）。

Cisco IOS ブロック送信元ネットワークの修復の追加

Cisco IOS ブロック送信元ネットワーク修復は、ルータから、相関ポリシー違反に関与している送信元ホストのネットワークに送信されるトラフィックをブロックします。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

始める前に

- Cisco IOS インスタンスの追加 （1254 ページ） の説明に従い、Cisco IOS インスタンスを追加します。

手順

ステップ 1 **[ポリシー（Policies）]>[アクション（Actions）]>[インスタンス（Instances）]**を選択します。

ステップ 2 修復を追加するインスタンスの横にある[表示（View）]（👁）をクリックします。

ステップ 3 [設定されている修復（Configured Remediations）]セクションで、[送信元ネットワークのブロック（Block Source Network）] を選択し、[追加（Add）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] を入力します。

ステップ 5 [ネットマスク（Netmask）] フィールドに、トラフィックをブロックするネットワークの説明となるサブネット マスクまたは CIDR 表記を入力します。

たとえば、1 つのホストがルールをトリガーとして使用したときにクラス C ネットワーク全体へのトラフィックをブロックするには、ネットマスクとして `255.255.255.0` または `24` を使用します。

別の例として、トリガーの IP アドレスを含む 30 個のアドレスへのトラフィックをブロックするには、ネットマスクとして 255.255.255.224 または 27 を指定します。この場合、IP アドレス 10.1.1.15 が修復をトリガーとして使用し、10.1.1.1 と 10.1.1.30 の間のすべての IP アドレスがブロックされます。トリガーの IP アドレスのみをブロックするには、このフィールドは空のままにして、32 を入力するか、または 255.255.255.255 を入力します。

ステップ 6 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールと許可（Allow）リストに応答を追加する （1192 ページ） を参照）。

関連トピック

IP アドレスの規則 （31 ページ）

Nmap スキャン修復

システムには、Nmap™ という、ネットワーク調査およびセキュリティ監査を目的としたオープンソースのアクティブスキャナが統合されています。Nmap 修復を使用して、相関ポリシー違反に対応できます。これは、Nmap スキャン修復をトリガーします。

Nmap スキャンの詳細については、Nmap スキャンを参照してください。

セット属性値修復

トリガーイベントが発生したホストでホスト属性値を設定することにより、相関ポリシー違反に応答できます。テキストのホスト属性の場合、イベントの説明を属性値として使用できます。

セット属性修復の設定

手順

ステップ 1 **[ポリシー（Policies）]>[アクション（Actions）]>[インスタンス（Instances）]**を選択します。

ステップ 2 セット属性値インスタンスの追加 （1260ページ）の説明に従って、セット属性インスタンスを作成します。

ステップ 3 セット属性値修復の追加 （1260 ページ）の説明に従って、セット属性修復を追加します。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールと許可（Allow）リストに応答を追加する （1192 ページ） を参照）。

関連トピック

定義済みホスト属性 （1068 ページ）
ユーザ定義のホスト属性 （1068 ページ）

セット属性値インスタンスの追加

手順

ステップ 1 **[ポリシー（Policies）]>[アクション（Actions）]>[インスタンス（Instances）]**を選択します。
ステップ 2 [新しいインスタンスの追加（Add a New Instance）] リストから [セット属性値（Set Attribute Value）] を選択し、[追加（Add）] をクリックします。
ステップ 3 [インスタンス名（Instance Name）] と [説明（Description）] を入力します。
ステップ 4 [作成（Create）] をクリックします。

次のタスク

- セット属性値修復の追加 （1260ページ） の説明に従って、セット属性修復を作成します。

セット属性値修復の追加

セット属性値修復は相関ポリシー違反に関与したホストにホスト属性を設定します。属性を設定する各属性の値について修復を作成します。テキスト属性の場合、トリガーイベントの説明を属性値として使用できます。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

始める前に

- セット属性値インスタンスの追加 （1260ページ） の説明に従って、セット属性インスタンスを作成します。

手順

ステップ 1 **[ポリシー（Policies）]>[アクション（Actions）]>[インスタンス（Instances）]**を選択します。
ステップ 2 修復を追加するインスタンスの横にある[表示（View）]（👁）をクリックします。
ステップ 3 [設定されている修復（Configured Remediations）] セクションで、[セット属性値（Set Attribute Value）] を選択し、[追加（Add）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] を入力します。

ステップ 5 送信元データ、宛先データをもつイベントへの応答としてこの修復を使用するには、[イベントが決定するホストを更新（Update Which Host(s) From Event）] オプションを選択します。

ステップ 6 テキスト属性の場合、以下に従い [属性値にイベントからの説明を使用（Use Description From Event For Attribute Value）] を指定します。

- イベントの説明を属性値として使用するには、[オン（On）] をクリックし、設定する [属性値（Attribute Value）] を入力します。
- 修復の [属性値（Attribute Value）] 設定を属性値として使用するには、[オフ（Off）] をクリックします。

ステップ 7 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールと許可（Allow）リストに応答を追加する （1192 ページ） を参照）。

修復モジュールの管理

マルチドメイン展開では、現在のドメインでインストールされた修復モジュールが表示されます。このモジュールは削除可能です。また、先祖ドメインでインストールされたモジュールも表示されますが、これは削除できません。下位ドメインの修復モジュールを管理するには、そのドメインに切り替えます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクション（Actions）] > [モジュール（Modules）]**を選択します。

ステップ 2 修復モジュールを管理します。

- 設定：モジュールの [モジュール詳細（Module Detail）] ページを表示して、そのモジュールのインスタンスと修復を設定するには、[表示（View）]（  ） をクリックします。マルチドメイン展開では、[モジュール詳細（Module Detail）] ページを使用して、先祖ドメインでインストールされたモジュールに対応する現在のドメイン内のインスタンスを追加、削除、または編集することはできません。代わりに、[インスタンス（Instances）]ページ（**[ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]**）を使用します。修復インスタンスの管理 （1262 ページ）を参照してください。
- 削除：使用されていないカスタムモジュールを削除するには、[削除（Delete）]（  ） をクリックします。システム付属のモジュールは削除できません。

- インストール：カスタム モジュールをインストールするには、[ファイルの選択（Choose File）] をクリックしてモジュールを参照し、[インストール（Install）] をクリックします。詳細については、*Firepower System Remediation API Guide*を参照してください。

修復インスタンスの管理

[インスタンス（Instances）] ページには、すべての修復モジュールのすべての設定済みインスタンスがリスト表示されます。

マルチドメイン展開では、現在のドメインで作成された修復インスタンスが表示されます。このインスタンスは編集可能です。また、先祖ドメインで作成されたインスタンスも表示されますが、これは編集できません。下位ドメインの修復インスタンスを管理するには、そのドメインに切り替えます。

先祖ドメインで作成されたインスタンスに修復を追加することはできませんが、現在のドメインで同様に設定されるインスタンスを作成し、そのインスタンスに修復を追加することは可能です。また、先祖ドメインで作成した修復は、相関応答として使用することもできます。

手順

ステップ 1 **[ポリシー（Policies）]**>**[アクション（Actions）]**>**[インスタンス（Instances）]**を選択します。

ステップ 2 修復インスタンスを管理します。

- 追加：インスタンスを追加するには、インスタンスを追加する修復モジュールを選択して、[追加（Add）] をクリックします。システム付属のモジュールについては、次を参照してください。
  - ISE EPS インスタンスの追加 （1252 ページ）
  - Cisco IOS インスタンスの追加 （1254 ページ）
  - Cisco Secure Firewall Management Center デバイス構成ガイド
  - セット属性値インスタンスの追加 （1260 ページ）

  カスタム モジュールを追加する際のヘルプは、そのモジュールのドキュメントを参照してください（使用可能な場合）。
- 設定：インスタンスの詳細を設定して、インスタンスに修復を追加するには、[表示（View）]（）をクリックします。
- 削除：使用されていないインスタンスを削除するには、[削除（Delete）]（  ）をクリックします。

1 つの修復モジュールのインスタンスの管理

[モジュール詳細（Module Detail）] ページには、特定の修復モジュールに設定されたインスタンスと修復がすべて表示されます。

マルチドメイン展開では、現在のドメインと先祖ドメインにインストールされた修復モジュールの [モジュール詳細（Module Detail）] ページにアクセスできます。ただし、[モジュール詳細（Module Detail）] ページを使用して、先祖ドメインにインストールされているモジュールに対応する現在のドメイン内のインスタンスを追加、削除または編集することはできません。代わりに、[インスタンス（Instances）] ページ（**[ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]**）を使用します。修復インスタンスの管理 （1262 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）] > [アクション（Actions）] > [モジュール（Modules）]**を選択します。

ステップ 2 管理するインスタンスを持つ修復モジュールの横にある[表示（View）]（👁）をクリックします。

ステップ 3 修復インスタンスを管理します。

- 追加：インスタンスを追加するには、[追加（Add）] をクリックします。システム付属のモジュールについては、次を参照してください。
  - ISE EPS インスタンスの追加 （1252 ページ）
  - Cisco IOS インスタンスの追加 （1254 ページ）
  - Cisco Secure Firewall Management Center デバイス構成ガイド
  - セット属性値インスタンスの追加 （1260 ページ）

  カスタムモジュールのインスタンスを追加する際のヘルプは、そのモジュールのドキュメントを参照してください（提供されている場合）。
- 設定：インスタンスの詳細を設定して、インスタンスに修復を追加するには、[表示（View）]（👁）をクリックします。
- 削除：使用されていないインスタンスを削除するには、[削除（Delete）]（🗑）をクリックします。

第 X 部

参照先

第 42 章

Secure Firewall Management Center のコマンド ライン リファレンス

このリファレンスでは、Secure Firewall Management Center のコマンドライン インターフェイス（CLI）について説明します。

（注） Secure Firewall Threat Defense については、Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。

Secure Firewall Management Center CLI について

SSH を使用して Management Center にログインすると、CLI にアクセスします。`expert` コマンドを使用して Linux シェルにアクセスすることもできますが、このコマンドを使用しないことを強く推奨します。

注意 Cisco TAC または Firepower ユーザー マニュアルの明示的な手順による指示がない限り、Linux シェルにアクセスしないことを強くお勧めします。

⚠

注意 Linux シェルへのアクセス権があるユーザーはルート権限を取得できるため、セキュリティ上のリスクが生じる可能性があります。システムセキュリティ上の理由から、次の点を強くお勧めします。

- 外部認証を確立した場合は、Linux シェル アクセスが付与されるユーザーのリストを適切に制限してください。
- 事前定義された `admin` ユーザーに加えて、Linux シェル ユーザーを確立しないでください。

この付録で説明されているコマンドを使用して Secure Firewall Management Center を表示してトラブルシューティングを行うとともに、限定された設定操作を実行できます。

Secure Firewall Management Center CLI モード

CLI には 4 つのモードが含まれています。デフォルト モードである CLI 管理には、CLI 自体の内部を移動するためのコマンドが含まれています。残りのモードには、Secure Firewall Management Center の機能の 3 つの異なる領域に対処するコマンドが含まれています。これらのモード内のコマンドは、モード名の`system`ム、`show`、または `configure` で始まります。

モードを入力すると、CLI は、現在のモードを反映するように変更を求められます。たとえば、システム コンポーネントのバージョン情報を表示するには、標準 CLI プロンプトに完全なコマンドを入力します。

```
> show version
```

これまでに `show` モードに入ったことがある場合は、show モードの CLI プロンプトで `show` キーワードを使用せずにコマンドを入力できます。

```
show> version
```

Secure Firewall Management Center CLI 管理コマンド

CLI 管理コマンドを使用して、CLI とやりとりすることができます。これらのコマンドはデバイスの処理に影響しません。

exit

CLI コンテキストを、次に高い CLI コンテキスト レベルへ移動します。デフォルト モードからこのコマンドを発行すると、ユーザーは現行の CLI セッションからログアウトします。

構文

```
exit
```

例

```
system> exit
>
```

expert

Linux シェルを起動します。

構文

```
expert
```

例

```
> expert
```

?（疑問符）

CLI コマンドと CLI パラメータの状況依存ヘルプを表示します。以下のように疑問符（?）コマンドを使用します。

- 現在の CLI コンテキスト内で使用できるコマンドのヘルプを表示するには、コマンド プロンプトで疑問符（?）を入力します。
- 特定文字セットから始まる使用可能なコマンドのリストを表示するには、疑問符（?）に続けて短縮されたコマンドを入力します。
- コマンドの正式な引数のヘルプを表示するには、コマンドプロンプトの引数の代わりに疑問符（?）を入力します。

疑問符（?）は、コンソールにエコーバックされないことに注意してください。

構文

```
?
abbreviated_command ?
command [arguments] ?
```

例

```
> ?
```

Secure Firewall Management Center CLI の show コマンド

Show コマンドは、アプライアンスの状態に関する情報を提供します。これらのコマンドはアプライアンスの動作モードを変更しません。また、これらのコマンドを実行しても、システムの動作に対する影響は最小限になります。

version

製品のバージョンおよびビルドと、UUID などの情報を表示します。

構文

```
show version
```

例

```
> show version
-------------------[ fmc-austin ]-------------------
Model                     : Cisco Secure Firewall Management Center for VMware (66)
Version 7.6.0 (Build 1385)
UUID                      : a904b8b2-ca9a-11ee-a583-5e804c16b2fd
Rules update version      : 2024-05-13-001-vrt
LSP version               : lsp-rel-20240513-1955
VDB version               : 380
----------------------------------------------------
```

Secure Firewall Management Center CLI 設定コマンド

コンフィギュレーション コマンドを使用して、システムを設定および管理することができます。これらのコマンドはシステムの動作に影響を与えます。

password

現在の CLI ユーザーは自身のパスワードを変更できます。

⚠

注意 システム セキュリティ上の理由により、いかなるアプライアンスでも、事前定義された **admin** に加えて、Linux シェル ユーザーを確立しないことをお勧めします。

（注） `password` コマンドは、エクスポートモードではサポートされていません。Secure Firewall システムで管理ユーザーのパスワードをリセットするには、詳細をご覧ください。エキスパートモードで `password` コマンドを使用して管理者パスワードをリセットする場合は、`configure user admin password` コマンドを使用してパスワードを再設定することをお勧めします。パスワードを再設定したら、エキスパートモードに切り替え、管理者ユーザーのパスワードハッシュが /opt/cisco/config/db/sam.config ファイルおよび /etc/shadow ファイルで同じであることを確認します。

コマンドを発行すると、CLI は現在の（古い）パスワードを入力するようユーザーに要求し、その後で新しいパスワードを 2 回入力するよう要求します。

構文

```
configure password
```

例

```
> configure password
Changing password for admin.
(current) UNIX password:
New UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Secure Firewall Management Center CLI システム コマンド

system コマンドを使用して、システム全体のファイルおよびアクセス コントロールの設定を管理することができます。

generate-troubleshoot

シスコが解析に使用するトラブルシューティング データを生成します。

構文

```
system generate-troubleshoot option1 optionN
```

オプションが次の 1 つまたは複数の場合は、スペースで区切ります。

- `ALL`：次のすべてのオプションを実行します。
- `SNT`：Snort のパフォーマンスと設定
- `PER`: ハードウェアのパフォーマンスとログ

- SYS：システム設定、ポリシー、およびログ
- DES：検出設定、ポリシー、およびログ
- NET：インターフェイスとネットワーク関連データ
- VDB：検出、認知、VDB データ、およびログ
- UPG：データとログのアップグレード
- DBO：すべてのデータベース データ
- LOG：すべてのログ データ
- NMP：ネットワーク マップ情報

例

```
> system generate-troubleshoot VDB NMP
starting /usr/local/sf/bin/sf_troubleshoot.pl…
Please, be patient. This may take several minutes.
The troubleshoot options codes specified are VDB,NMP.
Getting filenames from [usr/local/sf/etc/db_updates/index]
Getting filenames from [usr/local/sf/etc/db_updates/base-6.2.3]
Troubleshooting information successfully created at
/var/common/results-06-14-2018—222027.tar.gz
```

lockdown

expert コマンドを削除し、デバイス上の Linux シェルへアクセスします。

⚠

注意 このコマンドは、サポートからのホットフィックスがない場合は取り消すことはできません。使用には注意が必要です。

構文

```
system lockdown
```

例

```
> system lockdown
```

reboot

アプライアンスのリブート。

構文

```
system reboot
```

例

```
> system reboot
```

restart

アプライアンス アプリケーションを再起動します。

構文

```
system restart
```

例

```
> system restart
```

shutdown

アプライアンスをシャット ダウンします。

構文

```
system shutdown
```

例

```
> system shutdown
```

安全消去

ハードドライブデータを完全に消去します。

このコマンドを使用する前に、シリアルポートを使用して Management Center に接続する必要があります。このコマンドを実行すると、デバイスが再起動し、すべてのデータが完全に削除されます。プロセスが完了するまでに数時間かかることがあります。ドライブの容量が大きいほど、時間がかかります。安全な消去プロセス中の中断を防ぐために、電源を確保してください。消去が完了したら、新しいソフトウェアイメージをインストールできます。

⚠

注意 ハードドライブの消去処理では、アプライアンスのすべてのデータ（ISOイメージを含む）が失われます。

サポートされるデバイス

- Firepower Management Center 1600、2600、4600
- Firewall Management Center 1700、2700、4700

構文

```
secure-erase
```

例

```
> secure-erase
***************************** Caution ********************************

 If you run this command:
     - The management center hard drive data, including configurations
       and bootable images, will be permanently erased.
     - The device will reboot and reinitialize.

Note: Do not power off your device during this procedure.

**********************************************************************

Do you want to proceed? (Yes/No)
```

Secure Firewall Management Center CLI の履歴

機能	最小 Management Center	最小 Threat Defense	詳細
Management Center を対象とした自動 CLI アクセス	6.5	任意（Any）	SSH を使用して Management Center にログインすると、CLI に自動的にアクセスします。CLI `expert` コマンドを使用して Linux シェルにアクセスすることもできますが、このコマンドを使用しないことを強く推奨します。 （注） Management Center の CLI アクセスを有効または無効にするバージョン 6.3 の機能は廃止されます。このオプションが廃止された結果、仮想 Management Center は、**[システム（System）] > [設定（Configuration）] > [コンソールの設定（Console Configuration）]** ページを表示しなくなりました。このページは、物理 Management Center では引き続き表示されます。

機能	最小 Management Center	最小 Threat Defense	詳細
Management Center の CLI アクセスを有効化および無効化する機能	6.3	任意（Any）	新しい/変更された画面： Management Center の Web インターフェイスで管理者が使用可能な新しいチェックボックス：**システム**（⚙）> **[構成（Configuration）]** の [CLI アクセスの有効化（Enable CLI Access）] > [コンソール設定（Console Configuration）] ページ。 • オン： SSH を使用して Management Center にログインすると CLI にアクセスします。 • オフ：SSH を使用して Management Center にログインすると Linux シェルにアクセスします。これは、バージョン 6.3 の新規インストールと、以前のリリースからバージョン 6.3 にアップグレードした場合のデフォルトの状態です。 サポートされているプラットフォーム： Management Center
Management Center CLI	6.3	任意（Any）	導入された機能。 初期状態では、次のコマンドがサポートされています。 • `exit` • `expert` • `?` • `show version` • `configure password` • `system generate-troubleshoot` • `system lockdown` • `system reboot` • `system restart` • `system shutdown` サポートされているプラットフォーム： Management Center

第 43 章

セキュリティ、インターネットアクセス、および通信ポート

以下のトピックでは、システム セキュリティ、インターネット アクセス、および通信ポートに関する情報を提供します。

セキュリティ要件

Secure Firewall Management Centerを保護するには、保護された内部ネットワークにそれをインストールしてください。Management Centerは必要なサービスとポートだけを使用するよう設定されますが、ファイアウォール外部からの攻撃がそこまで（または管理対象デバイスまで）決して到達できないようにする必要があります。

Management Center とその管理対象デバイスが同じネットワーク上に存在する場合は、デバイス上の管理インターフェイスを、Management Center と同じ保護された内部ネットワークに接続できます。これにより、Management Centerからデバイスを安全に制御することができます。また、他のネットワーク上のデバイスからのトラフィックを Management Center で管理および分離できるように、複数の管理インターフェイスを設定することもできます。

アプライアンスの展開方法に関係なく、アプライアンス間通信は暗号化されます。それでも、分散型サービス拒否（DDoS）や中間者攻撃などの手段でアプライアンス間の通信が中断、ブロック、または改ざんされないよう何らかの対策を講じる必要があります。

シスコ クラウド

Management Center は次の機能で Cisco Cloud のリソースと通信します。

- **高度なマルウェア防御**

パブリッククラウドはデフォルトで設定されています。変更を加えるには、Cisco Secure Firewall Management Center デバイス構成ガイドの「Change AMP Options」を参照してください。

- **URL フィルタリング**

  詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの「URL filtering」の章を参照してください。

- **との統合シスコのセキュリティ分析とロギング（SaaS）**

  Cisco Secure Cloud Analytics でのリモートデータストレージ （633 ページ）を参照してください。

- **SecureX および SecureX Threat Response** との統合

  詳細については、以下からリンクされている統合ドキュメントを参照してください。

  - シスコ SecureX との統合 （753 ページ）
  - によるイベントの分析 SecureX Threat Response （762 ページ）

- **プロアクティブなサポート機能**

  詳細については、「Cisco Support Diagnostics の登録設定」を参照してください。

- **Cisco Success Network**

  詳細については、Cisco Success Network の登録設定 （759 ページ） を参照してください。

- **Cisco Umbrella 接続**

  詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの「DNS Policies」を参照してください。

インターネット アクセス要件

デフォルトでは、システムはポート 443/tcp（HTTPS）および 80/tcp（HTTP）でインターネットに接続するように設定されています。アプライアンスがインターネットに直接アクセスしないようにするには、プロキシサーバを設定できます。多くの機能では、場所によってシステムがアクセスできるリソースが決まります。

ほとんどの場合、インターネットにアクセスするのは Management Center です。高可用性ペアの Management Center の両方にインターネット アクセスがある必要があります。機能に応じて、両方のピアがインターネットにアクセスすることも、アクティブ ピアのみがインターネットにアクセスすることもあります。

管理対象デバイスがインターネットにアクセスする場合もあります。たとえば、マルウェア保護設定が動的分析を使用する場合、管理対象デバイスはファイルを直接 Secure Malware Analytics クラウドに送信します。または、外部 NTPサーバーにデバイスを同期することができます。

さらに、Web 分析トラッキングを無効にした場合を除き、ブラウザは Google（google.com）または、Amplitude（amplitude.com） の Web 分析サーバーに連絡し、個人を特定可能でない使用状況データを Cisco に提供することができます。

表 *145*：インターネット アクセス要件

機能	理由	Management Centerハイ アベイラビリティ	リソース
マルウェア防御	マルウェア クラウドルックアップ。	両方のピアが検索を実行します。	「適切な Cisco Secure エンドポイントおよびマルウェア分析操作に必要なサーバーアドレス」を参照してください。
	ファイル事前分類とローカルのマルウェア分析のシグニチャ更新をダウンロードします。	アクティブ ピアでダウンロードが実行され、スタンバイへ同期します。	updates.vrt.sourcefire.com amp.updates.vrt.sourcefire.com
	動的分析（管理対象デバイス）のファイルを送信します。 動的分析結果のクエリ（Management Center）。	両方のピアが動的分析レポートのクエリを実行します。	fmc.api.threatgrid.com fmc.api.threatgrid.eu
エンドポイント向け AMP	エンドポイント向け AMP によって検出されたマルウェア イベントを AMP クラウドから受信します。 システムによって検出されたマルウェアイベントを Cisco Advanced Malware Protection for Endpoints で表示します。 AMP クラウドからの性質をオーバーライドするには、AMP for Endpoints で作成された一元的なファイルブロックリストおよび許可リストを使用します。	両方のピアがイベントを受信します。 両方のピア（設定が同期されていない）でクラウド接続を設定する必要もあります。	「適切な Cisco Secure エンドポイントおよびマルウェア分析操作に必要なサーバーアドレス」を参照してください。
セキュリティ インテリジェンス	セキュリティインテリジェンス フィードをダウンロードします。	アクティブ ピアでダウンロードが実行され、スタンバイへ同期します。	intelligence.sourcefire.com

機能	理由	Management Centerハイ アベイラビリティ	リソース
URL フィルタリング	URLカテゴリおよびレピュテーションデータをダウンロードします。 URLカテゴリおよびレピュテーション データを手動でクエリ（ルックアップ）します。 未分類 URL のクエリ。	アクティブ ピアでダウンロードが実行され、スタンバイへ同期します。	URL： • regsvc.sco.cisco.com • est.sco.cisco.com • updates-talos.sco.cisco.com • updates.ironport.com IPv4 ブロック： • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 IPv6 ブロック： • 2a04:e4c7:ffff::/48 • 2a04: e4c7: fffe::/48
Cisco Secure 動的属性コネクタ	Amazon Elastic Container Registry（Amazon ECR）からパッケージを取得する	アクティブピアとスタンバイピアがフィールドイメージを取得します。	https://public.ecr.aws https://csdac-cosign.s3.us-west-1.amazonaws.com
Cisco Smart Licensing	Cisco Smart Software Manager と通信します。	アクティブなピアが通信します。	smartreceiver.cisco.com www.cisco.com
Cisco Success Network	使用状況情報および統計情報を送信します。	アクティブなピアが通信します。	api-sse.cisco.com:8989 dex.sse.itd.cisco.com dex.eu.sse.itd.cisco.com
Cisco Support Diagnostics	許可された要求を受け入れ、使用状況の情報と統計情報を送信します。	アクティブなピアが通信します。	api-sse.cisco.com:8989

機能	理由	Management Centerハイ アベイラビリティ	リソース
システムの更新プログラム	更新プログラムを Cisco から直接 Management Center にダウンロードします。 • システム ソフトウェア • 侵入ルール（SRU/LSP） • 脆弱性データベース（VDB） • 位置情報データベース（GeoDB）	侵入ルール、VDB、および GeoDB をアクティブなピアで更新し、アクティブなピアはその後スタンバイへ同期します。 各ピアで個別にシステム ソフトウェアをアップグレードします。	amazonaws.com cisco.com
SecureX Threat Response 統合	適切なインテグレーションガイドを参照してください。		
時刻の同期	展開内で時間を同期します。 プロキシサーバではサポートされません。	外部 NTP サーバを使用するアプライアンスはインターネットにアクセスできる必要があります。	time.cisco.com
RSS フィード	ダッシュ ボードで Cisco 脅威調査ブログを表示します。	RSS フィードを表示するアプライアンスはインターネットにアクセスできる必要があります。	blog.talosintelligence.com
[Whois]	外部ホストの whois 情報を要求します。 プロキシサーバではサポートされません。	whois 情報を要求するすべてのアプライアンスがインターネットにアクセスできる必要があります。	whois クライアントは、クエリ対象の適切なサーバの推測を試みます。推測できない場合、次を使用します。 • NIC ハンドル：whois.networksolutions.com • IPv4 アドレスとネットワーク名：whois.arin.net

通信ポートの要件

Management Center と管理対象デバイスは、ポート 8305/tcp の双方向型 SSL 暗号化通信チャネルを使用して通信します。このポートは、基本的な通信のためにオープンの状態で保持する必要があります。

他のポートでは、特定の機能に必要な外部リソースへのアクセスとともにセキュアな管理をすることができます。一般に、機能関連のポートは、該当する機能を有効化または設定する時点まで、閉じたままになります。開いたポートを閉じると展開にどのような影響が及ぶか理解するまでは、開いたポートを変更したり閉じたりしないでください。

表 *146 :* 通信ポートの要件

ポート	プロトコル/機能	プラットフォーム	方向	詳細
22/tcp	SSH	Management Center Threat Defense	着信	アプライアンスへのリモート接続を保護します。
53/tcp 53/udp	DNS		発信	DNS
67/udp 68/udp	DHCP		発信	DHCP
123/udp	NTP		発信	時刻を同期します。
161/udp	SNMP	Management Center Threat Defense	着信	SNMP ポーリング経由で MIB にアクセスできるようにします。
162/udp	SNMP		発信	リモート トラップ サーバーに SNMP アラートを送信します。
389/tcp 636/tcp	LDAP		発信	外部認証用に LDAP サーバーと通信します。 検出された LDAP ユーザに関するメタデータを取得します（Management Center のみ）。 設定可能。
443/tcp	HTTPS	Management Center	着信	Web インターフェイスにアクセスします。
443/tcp	リモート アクセス VPN（SSL/IPSec）	Threat Defense	着信	リモート ユーザーからネットワークへのセキュアな VPN 接続を許可します。
500/udp 4500/udp	リモート アクセス VPN（IKEv2）	Threat Defense	着信	リモート ユーザーからネットワークへのセキュアな VPN 接続を許可します。
443/tcp	HTTPS	Management Center Threat Defense	着信	Cisco Terminal Services（TS）エージェントを含め、Firepower REST API を使用して、統合製品やサードパーティ製品と通信します。

ポート	プロトコル/機能	プラットフォーム	方向	詳細
443/tcp	HTTPS		発信	インターネットからデータを送受信します。 詳細については、インターネット アクセス要件（1278ページ）を参照してください。
443	HTTPS	Management Center	両方	AMP for Endpoints との統合
514/udp	Syslog（アラート）		発信	リモート syslog サーバーにアラートを送信します。
623/udp	SOL/LOM	Management Center	着信	Serial Over LAN（SOL）接続を使用した Lights-Out Management（LOM）。
885/tcp	キャプティブポータル	Threat Defense	着信	キャプティブ ポータルのアイデンティティ ソースと通信します。
1500/tcp 2000/tcp	データベースアクセス	Management Center	着信	サードパーティ クライアントによるイベント データベースへの読み取り専用アクセスを可能にします。
1812/udp 1813/udp	RADIUS		発信	外部認証とアカウンティングのために RADIUS サーバーと通信します。 設定可能。
8302/tcp	eStreamer	Management Center	着信	eStreamer クライアントと通信します。
8305/tcp	アプライアンス通信		両方	展開におけるアプライアンス間で安全に通信します。 設定可能。このポートを変更する場合は、展開内のすべてのアプライアンスについて変更する必要があります。デフォルトを維持することをお勧めします。
8307/tcp	ホスト入力クライアント	Management Center	着信	ホスト入力クライアントと通信します。
8989/tcp	Cisco Support Diagnostics		両方	許可された要求を受け入れ、使用状況の情報と統計情報を送信します。

関連トピック

Management Center 用の LDAP 外部認証オブジェクトの追加 （151 ページ）
Management Center 用の RADIUS 外部認証オブジェクトの追加 （160 ページ）

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