CHAPTER 49

ホスト プロファイルの使用

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。ユーザは、プロファイルを通じてホスト名やオペレーティング システムなど、ホストの全般的な情報にアクセスできます。たとえば、ホストの MAC アドレスをすぐに見つける必要がある場合は、ホスト プロファイルを見ればわかります。

プロファイルには*ホスト属性*も示されています。ホスト属性は、ホストに適用することができるユーザ定義の記述です。たとえば、ホストが存在するビルディングを示すホスト属性を割り当てることがあります。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。別の例として、*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特定し、ホストの重要度に基づいて相関ポリシーとアラートを調整できます。

またホスト プロファイルは、特定のホスト上で稼働しているサーバ、クライアント、およびホスト プロトコルに関する情報（コンプライアンスのホワイト リストに準拠しているかどうかなど）を提供します。サーバ リストからサーバを削除することも、サーバの詳細を表示することも可能です。サーバの*接続イベント*、サーバのトラフィックが検出されたセッションのログ情報も表示できます。また、クライアントの詳細および接続イベントを表示したり、ホスト プロファイルからサーバ、クライアント、またはホスト プロトコルを削除したりできます。

FireSIGHT システム 導入環境に FireSIGHT のライセンスが含まれている場合は、ホスト プロファイルで*侵害の兆候*（IOC）を確認できます。これらの兆候は、モニタ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る可能性があるどうかを判断できるように、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、Security Intelligence、接続イベント、ファイルまたはマルウェア イベント）との関連性を示しています。ホスト プロファイルでは、ホストの IOC タグの概要の確認、IOC に関連付けられているイベントの確認、IOC タグへの解決済みのマーク付け、ディスカバリ ポリシーの IOC ルール状態の編集などを実行できます。

導入環境に Protection のライセンスが含まれている場合は、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。詳細については、パッシブ展開における前処理の調整（30-1 ページ）を参照してください。

履歴情報を追跡するようシステムを設定している場合は、ホスト上のユーザの履歴情報を表示することもできます。過去 24 時間のユーザ アクティビティをグラフィック表示できます。

ホスト プロファイルから、ホストの脆弱性のリストを変更できます。この機能を使用して、ホストに対してどの脆弱性が対処されたかを追跡できます。脆弱性に対して修正ファイルを適用することもできます。このようにすると、修正ファイルで対処されたすべての脆弱性が自動的に無効とマークされることになります。

シスコで生成された脆弱性の情報を使用できます。また、サードパーティのスキャナで検出された脆弱性の情報を、ホスト入力機能によって防御センターにインポートして使用することもできます。

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 アイデンティティのリストに追加されます。

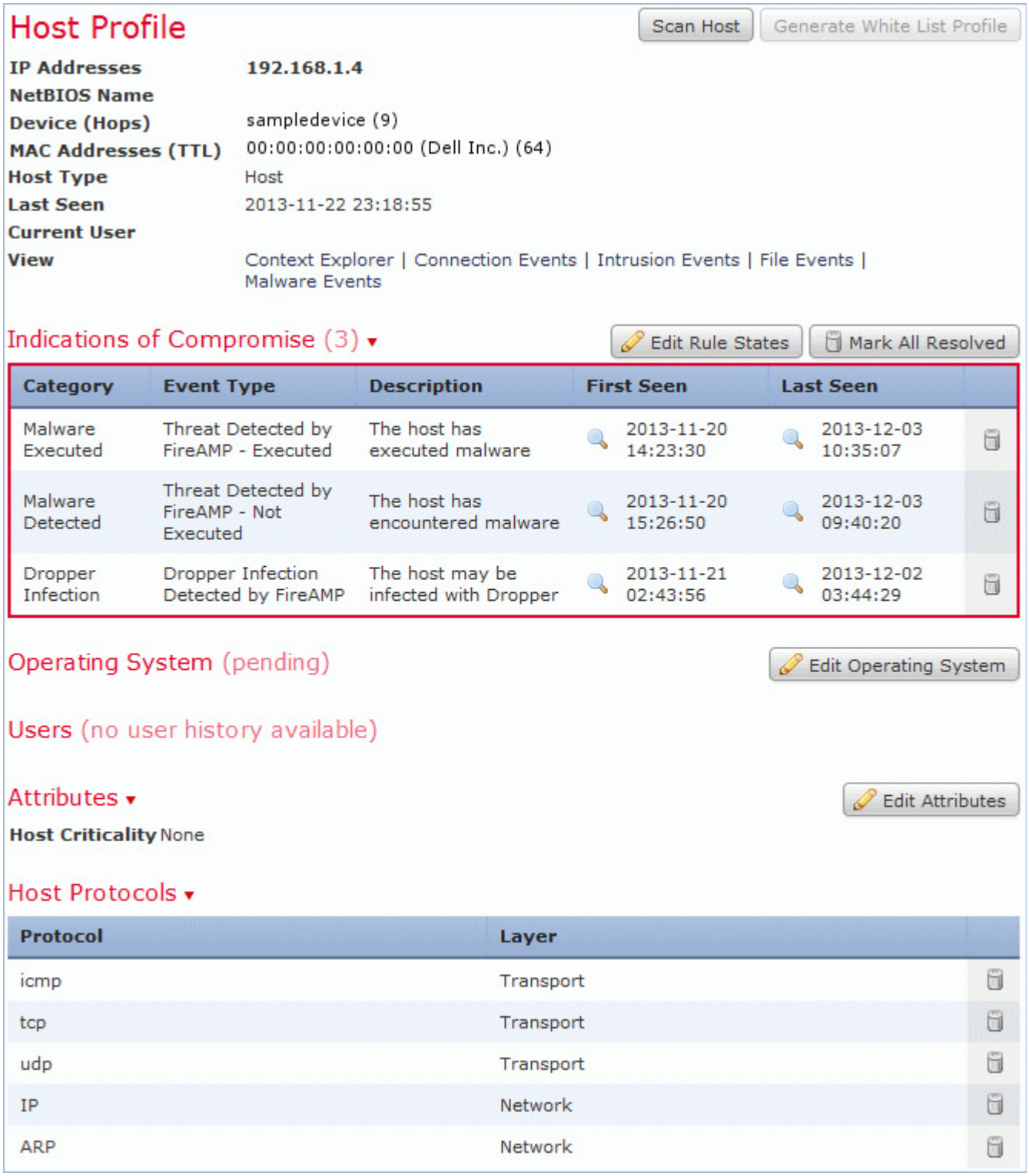
ホスト プロファイルは、ネットワーク上のすべてのホストでは使用できない可能性があることに注意してください。考えられる原因は次のとおりです。

- 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
- FireSIGHT ホストのライセンス制限に達した
- 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

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ることに注意してください。たとえば、非 IP ベースのプロトコル（STP、SNAP、IPX など）を使用する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。

別の例として、NetFlow 対応のデバイスによってエクスポートされたデータに基づいて、ホスト、サーバ、およびクライアントをネットワーク マップに追加するようネットワーク検出ポリシーを設定することができますが、これらのホスト、サーバ、およびクライアントについて利用できる情報は制限されます。たとえば、スキャナや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提供していない場合、ホストではこれらのデータを使用できません。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

次の図は、ホスト プロファイルの例を示しています。



Host Profile

Scan Host | Generate White List Profile

IP Addresses	**192.168.1.4**
NetBIOS Name	
Device (Hops)	sampledevice (9)
MAC Addresses (TTL)	00:00:00:00:00:00 (Dell Inc.) (64)
Host Type	Host
Last Seen	2013-11-22 23:18:55
Current User	
View	Context Explorer | Connection Events | Intrusion Events | File Events | Malware Events

Indications of Compromise (3)

Edit Rule States | Mark All Resolved

Category	Event Type	Description	First Seen	Last Seen
Malware Executed	Threat Detected by FireAMP - Executed	The host has executed malware	2013-11-20 14:23:30	2013-12-03 10:35:07
Malware Detected	Threat Detected by FireAMP - Not Executed	The host has encountered malware	2013-11-20 15:26:50	2013-12-03 09:40:20
Dropper Infection	Dropper Infection Detected by FireAMP	The host may be infected with Dropper	2013-11-21 02:43:56	2013-12-02 03:44:29

Operating System (pending)

Edit Operating System

Users (no user history available)

Attributes

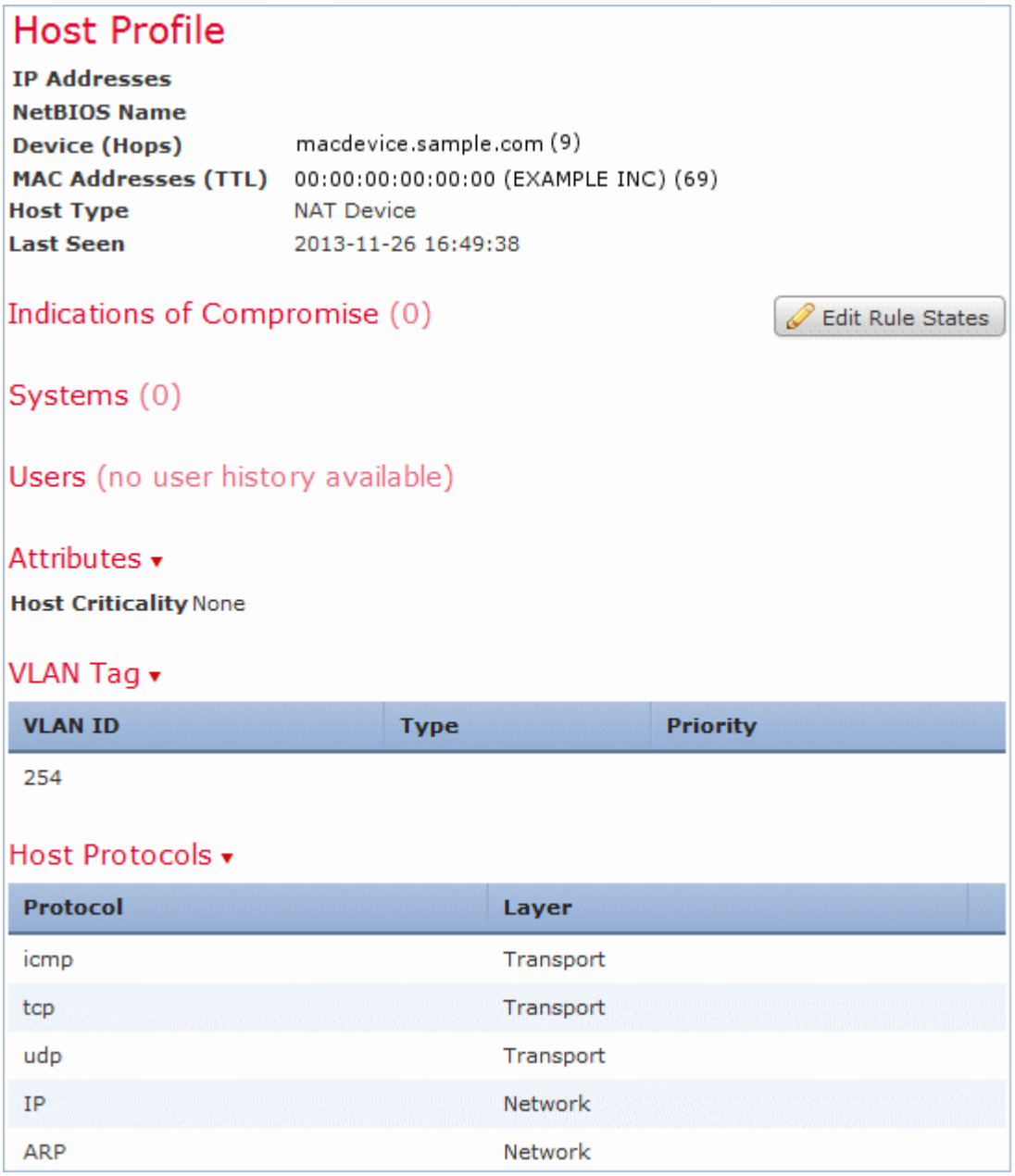
Edit Attributes

Host Criticality None

Host Protocols

Protocol	Layer
icmp	Transport
tcp	Transport
udp	Transport
IP	Network
ARP	Network

次の図は、MAC のホストのホスト プロファイルの例を示しています。



ホスト プロファイルの各セクションの詳細については、以下を参照してください。

- ホスト プロファイルの表示（49-5 ページ）では、ホスト プロファイルへのアクセス方法について説明します。
- ホスト プロファイルの基本的なホスト情報の使用（49-6 ページ）では、ホスト プロファイルの [ホスト（Host）] セクションで提供される情報について説明します。
- ホスト プロファイルの IP アドレスの操作（49-8 ページ）では、ホスト プロファイルの [IP アドレス（IP Addresses）] セクションで提供される情報について説明します。
- ホスト プロファイルでの侵害の兆候の使用（49-9 ページ）では、ホスト プロファイルの [侵害の兆候（Indications of Compromise）] セクションで提供される情報について説明します。

- ホスト プロファイルでのオペレーティング システムの使用（49-12 ページ）では、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）] セクションで提供される情報と、オペレーティング システムの編集方法、オペレーティング システムの競合の解決方法について説明します。
- ホスト プロファイルでのサーバの使用（49-17 ページ）では、ホスト プロファイルの [サーバ（Servers）] セクション、[サーバの詳細（Server Detail）] セクション、および [サーバ バナー（Server Banner）] セクションで提供される情報について説明します。
- ホスト プロファイルでのアプリケーションの使用（49-22 ページ）では、ホスト プロファイルの [クライアント（Clients）] セクションで提供される情報について説明します。
- ホスト プロファイルでの VLAN タグの使用（49-24 ページ）では、ホスト プロファイルの [VLAN タグ（VLAN Tag）] セクションで提供される情報について説明します。
- ホスト プロファイルでのユーザ履歴の使用（49-25 ページ）では、ホスト プロファイルの [ユーザ履歴（User History）] セクションで提供される情報について説明します。
- ホスト プロファイルでのホスト属性の使用（49-25 ページ）では、ホスト プロファイルの [属性（Attributes）] セクションで提供される情報について説明します。
- 事前定義のホスト属性の使用（49-34 ページ）では、ホストの重要度の属性を設定する方法、およびホスト プロファイルにメモを追加する方法について説明します。
- ユーザ定義のホスト属性の使用（49-35 ページ）では、ユーザ定義のホスト属性の作成および使用に関する情報を示します。
- ホスト プロファイルでのホスト プロトコルの使用（49-26 ページ）では、ホスト プロファイルの [ホスト プロトコル（Host Protocols）] セクションで提供される情報について説明します。
- ホスト プロファイルにおけるホワイト リスト違反の使用（49-27 ページ）では、ホスト プロファイルの [ホワイト リスト違反（White List Violations）] セクションで提供される情報について説明します。
- ホスト プロファイルでのマルウェア検出の使用（49-29 ページ）では、ホスト プロファイルの [最新のマルウェア検出（Most Recent Malware Detections）] セクションで提供される情報について説明します。
- ホスト プロファイルでの脆弱性の使用（49-29 ページ）では、ホスト プロファイルの [脆弱性（Vulnerabilities）] セクション、および [脆弱性の詳細（Vulnerability Detail）] セクションで提供される情報について説明します。

ホスト プロファイルの表示

ライセンス：FireSIGHT

モニタ対象のネットワーク上のホストの IP アドレスを含む任意のネットワーク マップまたはイベント ビューから、ホスト プロファイルにアクセスできます。たとえば、ディスカバリ イベントのテーブル ビューには、[IP アドレス（IP Address）] 列のすべてのエントリの隣に、ホスト プロファイルへのリンクが含まれています。侵害の兆候（IOC）ルールで有効になっているものがある場合は、侵害される可能性のあるホストが、異なるホスト プロファイル アイコンで示されます。

イベント ビューからホスト プロファイルを表示する方法

アクセス：Admin/Any Security Analyst

手順 1　任意のイベント ビューで、ホスト プロファイル アイコン（  ）をクリックするか、または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、侵害されたホスト アイコン（  ）をクリックします。

ポップアップ ウィンドウにホスト プロファイルが表示されます。

ネットワーク マップからホスト プロファイルを表示する方法：

アクセス：Admin/Any Security Analyst

手順 1　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 アドレスまでドリルダウンします。

ホスト プロファイルが表示されます。ネットワーク マップからホスト プロファイルにアクセスする方法の例については、ホストのネットワーク マップの操作（48-2 ページ）を参照してください。

ホスト プロファイルの基本的なホスト情報の使用

ライセンス：FireSIGHT

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。

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）。多くの場合 IPv6 ホストでは、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）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。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位置情報データを表す国コードも含まれています。この機能、および他の地理位置情報機能の詳細については、地理位置情報の使用（58-24 ページ）を参照してください。

ホストネーム（Hostname）

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た Linux ホストに NetBIOS 名を指定します。

[デバイス（ホップ）（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、デバイス、およびホストを検出したデバイスとホスト自体の間のネットワーク ホップの数が丸括弧で囲まれて示されます。複数のデバイスで対象のホストを参照できる場合は、レポート作成デバイスが太字で示されます。
- 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を、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モニタしていない。または、
- ホスト入力機能を使用してホストが追加されたが、FireSIGHT 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））]

ホストの検出された 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 ベンダーおよび現在の存続可能時間（TTL）値が括弧内に示されます。MAC アドレスが太字で示されている場合、この MAC アドレスは、ARP および DHCP トラフィックでシステムによって検出されたホストの実際の MAC アドレスです。複数のデバイスが同じホストを検出した場合、防御センターにはどのデバイスがホストをレポートしたかに関係なく、ホストに関連付けられているすべての MAC アドレスおよび TTL 値が表示されます。

MAC アドレスをクリックして、同じ MAC アドレスを持つホストのリストを表示できます。ルータのホスト プロファイルは通常、このリスト内でルーティングしているネットワーク セグメント内のホスト（IP アドレス）を示します。モニタリング対象のルータの IP アドレスは多くの場合、モニタリングされるワークステーションとサーバのリストに表示されます。MAC アドレスの実際の IP アドレスは太字で表示されます。

[ホスト タイプ（Host Type）]

システムが検出し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（Cisco 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 ストリングの分析
- 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

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。

[最終表示（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。

既存の現行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、現行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。詳細については、ユーザ データベース（45-8 ページ）を参照してください。

表示（View）

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。詳細については、次の項を参照してください。

- [Context Explorer]：詳細については、Context Explorer の使用（56-1 ページ）を参照してください。
- [接続イベント（Connection Events）]：詳細については、接続およびセキュリティ インテリジェンスのデータについて（39-2 ページ）を参照してください。
- [ディスカバリ イベント（Discovery Events）]：詳細については、ディスカバリ イベントの使用（50-1 ページ）を参照してください。
- [マルウェア イベント（Malware Events）]：詳細については、マルウェア イベントの操作（40-18 ページ）を参照してください。
- [送信元別侵入イベント（Intrusion Events by Source）]：詳細については、侵入イベントの操作（41-1 ページ）を参照してください。
- [宛先別侵入イベント（Intrusion Events by Destination）]：詳細については、侵入イベントの操作（41-1 ページ）を参照してください。

ホスト プロファイルの IP アドレスの操作

ライセンス：FireSIGHT

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。IPv6 ホストには通常、少なくとも 2 つの IPv6 アドレス（ローカルのみのものと、グローバルにルーティング可能なもの）があります。また、1 つ以上の IPv4 アドレスが割り当てられ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、IP アドレスには小さいフラグ アイコンと、関連付けられている国を示す ISO の国コードも示されます。フラグ アイコンまたは国コードをクリックすると、地理位置情報の詳細を確認できます。詳細については、地理位置情報の使用（58-24 ページ）を参照してください。

デフォルトでは、最初の 3 つのアドレスだけが示されることに注意してください。ホストのすべてのアドレスを表示するには、[すべて表示（show all）] をクリックします。

ホスト プロファイルでの侵害の兆候の使用

ライセンス：FireSIGHT

FireSIGHT 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）との関連性を示すことができます。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 IOC タグが表示されます。このセクションでは、対象ではなくなった IOC タグを解決済みにするだけでなく、ホストが直面している脅威の詳細を表示する、IOC タグをトリガーしたイベントに移動する、IOC ルールの状態を編集する、といったことが可能です。

IOC の機能を使用するには、機能、およびディスカバリ ポリシー内の少なくとも 1 つの IOC ルールを有効にする必要があります。対象ホストのホスト プロファイル ページから、個々のホストの IOC ルール状態を編集することもできます。各 IOC ルールは、IOC タグの 1 つのタイプに対応しています。組織のニーズに応じていずれかのルールまたはすべてのルールを有効にできます。ディスカバリ ポリシーおよび全般的な IOC に関する詳細は、侵害の兆候（痕跡）について（45-22 ページ）を参照してください。

IOC はホスト プロファイル内に存在しているだけではなく、イベント ビューアで IOC データを分析することもできます。詳細については、侵入の痕跡の使用（50-35 ページ）を参照してください。

次に、ホスト プロファイルで表示される IOC 情報のフィールドについて説明します。

[IPアドレス（IP Address）]
IOC をトリガーしたホストに関連付けられている IP アドレス。

カテゴリ（Category）
`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（Event Type）
特定の侵害の兆候（IOC）に関連付けられている識別子であり、その IOC をトリガー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の脅威の原因についての説明（`This host may be under remote control` や `Malware has been executed on this host` など）。

[初回確認日時/最新確認日時（First/Last Seen）]
ホストの IOC をトリガーしたイベントが発生した最初（または最新）の日付と時刻。

ホスト プロファイルにおける IOC データの使用の詳細については、次の項を参照してください。

- 単一ホストにおける侵害の兆候のルール状態の編集（49-10 ページ）
- 侵害の兆候に対するソース イベントの表示（49-10 ページ）
- 侵害の兆候を解決済みにする（49-11 ページ）

単一ホストにおける侵害の兆候のルール状態の編集

ライセンス：FireSIGHT

システムで侵害の兆候（IOC）を検出してタグを付けるには、最初にディスカバリ ポリシーの IOC 機能を有効にして、少なくとも 1 つの IOC ルールを（ポリシー全体または個別のホストに対して）有効にする必要があります。ホスト プロファイルから、個別のホストに適用される IOC ルールの状態を設定することができます。ディスカバリ ポリシーでの IOC の設定、およびポリシー全体での IOC ルール状態の設定の詳細については、侵害の兆候ルールの設定（45-38 ページ）を参照してください。

ホスト プロファイルから [侵害の兆候（Indications of Compromise）] セクションの [ルール状態の編集（Edit Rule States）] リンクを使用して IOC ルールのリストにアクセスし、編集することができます。ネットワークや組織のニーズに合わせて、一部またはすべてのルールを有効にすることができます。たとえば、Microsoft Excel などのソフトウェアを使用しているホストがモニタ対象ネットワーク上に出現することがない場合は、Excel ベースの脅威に関係する IOC タグを有効にしないようにできます。

すべての IOC ルールはシスコで事前に定義されています。ユーザはオリジナルのルールを作成することはできませんが、トリガーされた IOC タグについてコンプライアンス ルールを作成できます。詳細については、相関ポリシーおよび相関ルールの設定（51-1 ページ）を参照してください。各 IOC ルールはイベントの 1 つのタイプのみ（マルウェアや侵害など）でトリガーされ、特定の IOC タグに対応します。ルールとタグは簡単に対応できるよう、[カテゴリ（Category）]、[イベント タイプ（Event Type）]、および [説明（Description）] に同じデータが設定されています。IOC ルール状態の [編集（Edit）] ページには、ルールによりトリガーする必要があるシステム機能を明確にするために、各ルールのソース イベント データも表示されます。

ホストの侵害の兆候のルール状態を編集する方法：

アクセス：Admin/Any Security Analyst

手順 1　ホスト プロファイルの [侵害の兆候（Indications of Compromise）] セクションで [ルール状態の編集（Edit Rule States）] をクリックします。

新しいウィンドウに [侵害の兆候のルール状態の編集（Edit Indication of Compromise Rule States）] ページが表示されます。

手順 2　ルールの [有効（Enabled）] 列で、スライダをクリックして有効と無効を切り替えます。

手順 3　[保存（Save）] をクリックします。

変更が保存されます。

侵害の兆候に対するソース イベントの表示

ライセンス：FireSIGHT

[侵害の兆候（Indications of Compromise）] セクションを使用して、ホスト上で IOC タグをトリガーしたイベントへすばやくナビゲートすることができます。これらのイベントを分析すると、侵害される可能性があるホストへの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アイコン（  ）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 ビューにナビゲートします。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。

IOC タグをトリガーするイベントのタイプと機能の詳細については、以下を参照してください。

- 接続およびセキュリティ インテリジェンスのデータの使用（39-1 ページ）
- 侵入イベントの操作（41-1 ページ）
- マルウェア防御とファイル制御について（37-2 ページ）

[侵害の兆候（Indications of Compromise）] タグのソース イベントを表示する方法:

アクセス: Admin/Any Security Analyst

手順 1 ホスト プロファイルの [侵害の兆候（Indications of Compromise）] セクションで、調べる IOC タグの [初回確認日時（First Seen）] または [最終確認日時（Last Seen）] 列の表示アイコン（  ）をクリックします。

IOC をトリガーした該当イベントについて、イベントのテーブル ビューが表示されます。ここでは、トリガーしたイベントのみが表示されます。ホスト プロファイル ページを別のウィンドウで表示している場合は、メイン ウィンドウにイベント ビューが表示されます。

侵害の兆候を解決済みにする

ライセンス: FireSIGHT

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、このタグを解決済みとしてマークすることができます。IOC タグを解決済みとしてマークすると、このタグがホスト プロファイルから削除されます。ホスト上でアクティブなすべての IOC タグが解決済みになると、ホストでは、侵害されたホスト アイコン（  ）が表示されなくなります。解決済みの IOC についても、IOC のトリガー元イベントは引き続き表示できます。

イベントがホストの IOC タグを再度トリガーすると、タグがもう一度設定されます。ホスト上の個別の IOC タグを解決することも、ホスト上のすべてのタグに解決済みとマークすることもできます。

[侵害の兆候（Indications of Compromise）] タグを解決済みにする方法:

アクセス: Admin/Any Security Analyst

手順 1 ホスト プロファイルの [侵害の兆候（Indications of Compromise）] セクションで、次の 2 つの方法のいずれかを実行します。

- 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解決のアイコン（  ）をクリックします。
- ホスト上のすべての IOC タグを解決済みとマークするには、[すべて解決済みとしてマークする（Mark All Resolved）] をクリックします。

変更が保存され、選択した IOC タグが削除されます。

ホスト プロファイルでのオペレーティング システムの使用

ライセンス：FireSIGHT

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、ホスト上で稼働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、ユーザ入力の優先度が最も高く、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、シスコにより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 ソースから、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。

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）]

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。

オペレーティング システムが [保留中（Pending）] の場合、システムはオペレーティング 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 データはありません。オペレーティング システムが [不明（unknown）] の場合、システムはオペレーティング 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 データはありません。

ホストのオペレーティング システムがシステムで検出可能なものでなかった場合、以下の方針のいずれかを使用できます。

- カスタム フィンガープリントの使用（46-8 ページ）に記載されているとおりに、ホストのカスタム フィンガープリントを作成する
- ホスト プロファイルからのホストのスキャン（49-40 ページ）に記載されているとおりに、ホストに対して Nmap スキャンを実行する
- 『*FireSIGHT システム Host Input API Guide*』に記載されているホスト入力機能を使用して、データをネットワーク マップにインポートする
- ホスト プロファイルでのオペレーティング システムの使用（49-12 ページ）に記載されているとおりに、オペレーティング システムの情報を手動で入力する

[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_name*
- アプリケーション:*app_name*
- スキャナ:*scanner_type*(Nmap、またはシステム ポリシーによって追加されたスキャナ)
- FireSIGHT

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。現在の ID について(46-5 ページ)を参照してください。

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はオペレーティング システムによって異なるため、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。

NetFlow 対応デバイスによってエクスポートされたデータに基づきネットワーク マップにホストを追加するようネットワーク検出ポリシーを設定することはできますが、オペレーティング システムのアイデンティティを設定していない場合は、これらのホストで使用できるオペレーティング システムのデータはありません。詳細については、NetFlow と FireSIGHT データの違い(45-19 ページ)を参照してください。

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のホワイト リストに違反している場合、防御センターはオペレーティング システムの情報にホワイト リストの違反アイコン( )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 デバイスが有効なホワイト 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ホワイト リストが変わる可能性があることに注意してください。

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)] 列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、システムは、ネットワーク デバイスの背後で 1 つ以上のモバイル デバイスが検出されたことを示しています。モバイル デバイスにはハードウェア プラットフォームの情報がある場合とない場合がありますが、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。

オペレーティング システムのアイデンティティの表示

ライセンス：FireSIGHT

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。

各オペレーティング システムのアイデンティティでは、ホスト プロファイルに、ホスト プロファイルでのオペレーティング システムの使用（49-12 ページ）に記載されている情報が含まれていることがあります。

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）] ボタンが有効になっていることに注意してください。

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 リストを表示する方法：

アクセス：Admin/Any Security Analyst

手順 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。

[オペレーティング システム アイデンティティ情報（Operating System Identity Information）] ポップアップ ウィンドウが表示されます。

ヒント　いずれかのオペレーティング システムのアイデンティティの隣にある削除アイコン（ ）をクリックして、[オペレーティング システム 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、可能な場合は、ホスト プロファイルでオペレーティング システムの現行のアイデンティティを更新します。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、削除できないことに注意してください。

オペレーティング システムの編集

ライセンス：FireSIGHT

FireSIGHT システム 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た場合、オペレーティング システムの競合が発生することに注意してください。

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。詳細については、オペレーティング システムのアイデンティティの競合を解決する（49-15 ページ）を参照してください。

オペレーティング システムのアイデンティティを変更する方法:

アクセス: Admin/Any Security Analyst

手順 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。

ポップアップ ウィンドウが表示され、ここでオペレーティング 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。

手順 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 [現行の定義（Current Definition）] を選択し、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、6 の手順に進みます。
- [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、6 の手順に進みます。
- [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、3 の手順に進みます。

手順 3　オプションとして、[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）] フィールドで表示するカスタム文字列を修正します。

手順 4　オプションで別のベンダーからオペレーティング システムを変更するには、[ベンダー（Vendor）] および [製品（Product）] ドロップダウン リストから、ベンダーおよび他のオペレーティング システムの詳細を選択します。

手順 5　オプションでオペレーティング 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 [拡張機能（Extension）] ドロップダウン リストから対象のアイテムを選択します。

手順 6　オプションで、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、[修正ファイルの設定（Configure Fixes）] をクリックします。

パッケージの有効な修正リストが表示されます。

手順 7　ドロップダウン リストから適用可能な修正ファイルを選択し、[追加（Add）] をクリックします。

手順 8　オプションで、[パッチ（Patch）] および [拡張機能（Extension）] ドロップダウン リストを使用して、対象のパッチおよび拡張機能を追加します。

手順 9　[終了（Finish）] をクリックして、オペレーティング システムのアイデンティティの設定を完了します。

オペレーティング システムのアイデンティティの競合を解決する

ライセンス: FireSIGHT

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。

競合しているアイデンティティのいずれかを現行のアイデンティティにする方法:

アクセス: Admin/Any Security Analyst

手順 1　以下の 2 つの対処法があります。

- 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、[現行アイデンティティにする(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の競合を解決する方法:

アクセス: Admin/Any Security Analyst

手順 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)] セクションで [解決(Resolve)] をクリックします。

ポップアップ ウィンドウが表示され、ここで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。

手順 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 [現行の定義(Current Definition)] を選択し、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、6 の手順に進みます。
- [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、6 の手順に進みます。
- [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、3 の手順に進みます。

手順 3　オプションとして、[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)] フィールドで表示するカスタム文字列を入力します。

手順 4　オプションで別のベンダーからオペレーティング システムを変更するには、ベンダーおよび他のオペレーティング システムの詳細を選択します。

手順 5　オプションでオペレーティング 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 [拡張機能(Extension)] ドロップダウン リストから対象のアイテムを選択します。

手順 6　オプションで、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、[修正ファイルの設定(Configure Fixes)] をクリックします。

手順 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。

手順 8　[終了(Finish)] をクリックして、オペレーティング システムのアイデンティティの設定を終了し、ホスト プロファイルに戻ります。

ホスト プロファイルでのサーバの使用

ライセンス：FireSIGHT

システムが、モニタリング対象のネットワーク上のホストで稼働しているサーバを検出した場合、またはホスト入力機能、スキャナ、他の有効なソースを介してサーバが追加された場合は、防御センターは、ホスト プロファイルの [サーバ（Servers）] セクションにこれらのサーバを表示します。

防御センターは 1 つのホストにつき最大 100 台のサーバを表示します。100 台の制限に達すると、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。詳細については、ホスト制限と検出イベント ロギング（45-15 ページ）を参照してください。

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、検出されなかったサーバの結果が Nmap によって [サーバ（Servers）] リストに追加されます。ホストで 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 [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。詳細については、ホスト プロファイルでのスキャン結果の使用（49-39 ページ）と Nmap スキャンのセットアップ（47-10 ページ）を参照してください。ネットワーク マップからホストが削除されると、ホストのそのサーバに対する Nmap スキャンの結果は廃棄されることに注意してください。

（注）　NetFlow 対応のデバイスによってエクスポートされたデータに基づいて、サーバとクライアントをネットワーク マップに追加するようネットワーク検出ポリシーを設定することができますが、これらのアプリケーションについて利用できる情報は限定的です。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

ホスト プロファイルでサーバを使用するためのプロセスは、ユーザがプロファイルにアクセスした方法によって異なります。

- Servers 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した場合は、サーバの名前が太字で強調されて、サーバの詳細が表示されます。ホストの他のサーバの詳細を表示する場合は、対象のサーバ名の隣にある表示アイコン（）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した場合は、[サーバ（Servers）] セクションを展開し、詳細を表示するサーバの隣にある表示アイコン（  ）をクリックします。

また、次の操作も実行できます。

- ホスト上の特定のサーバに関連付けられている接続イベントを分析するには、サーバの隣にあるイベント アイコンをクリックします。

  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、サーバのポートおよびプロトコル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。接続データの詳細については、接続およびセキュリティ インテリジェンスのデータの使用（39-1 ページ）を参照してください。
- ホスト プロファイルからサーバを削除するには、サーバの隣にある削除アイコン（  ）をクリックします。

  サーバはホスト プロファイルから削除されますが、システムがサーバからトラフィックを再度検出すると、そのサーバがもう一度表示されます。ホストからサーバを削除すると、そのホストにホワイト 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。

- サーバのアイデンティティの競合を解決するには、サーバの隣にある解決のアイコンをクリックします。

  競合しているアイデンティティのいずれかを選択して、これらのアイデンティティのいずれか 1 つのバリエーションを選択するか、またはユーザ定義の新しいアイデンティティ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編集するには、サーバの隣にある編集アイコン( )をクリックします。

  現行のアイデンティティの選択、そのアイデンティティのバリエーションの選択、またはユーザ定義の新しいアイデンティティの設定を実行できます。

次に、[サーバ リスト(Servers list)] の列について説明します。

Protocol

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、何らかの理由でアプリケーションをポジティブまたはネガティブに識別できない場合
- [不明(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カーソルを移動すると、タグが表示されます。タグの詳細については、アプリケーション検出について(45-11 ページ)を参照してください。

[ベンダーおよびバージョン(Vendor and Version)]

FireSIGHT 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。有効なソースから識別情報が提供されない場合、このフィールドは空白になります。

ホストが、有効な相関ポリシーのコンプライアンス ホワイト リストに違反するサーバを実行している場合、防御センターは非準拠サーバに、ホワイト リストの違反アイコン( )のマークを付けます。

詳細については、次の各項を参照してください。

- サーバの詳細(49-19 ページ)
- サーバのアイデンティティの編集(49-20 ページ)
- サーバ アイデンティティの競合の解決(49-22 ページ)

サーバの詳細

ライセンス：FireSIGHT

防御センターは、1 つのサーバについてパッシブに検出される（シスコまたは NetFlow で検出される）アイデンティティを最大 16 個表示します。システムにより、このサーバのベンダーまたはバージョンが複数検出された場合、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 サーバで同じバージョンのサーバ 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 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。防御センターは、アクティブなソース（ユーザ入力、スキャナ、その他のアプリケーションなど）からのサーバ アイデンティティの数を制限することはありません。

防御センター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 ホワイト 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。

ヒント　サーバの詳細からのサーバ アイデンティティの変更、およびアイデンティティの競合の解決については、サーバのアイデンティティの編集（49-20 ページ）およびサーバ アイデンティティの競合の解決（49-22 ページ）を参照してください。

サーバの詳細には、選択されたサーバに関する既知の最新サブサーバ情報が表示されることがあります。最後に、サーバの詳細にサーバのバナーが表示されることがあります。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、サーバの識別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。

次に、サーバの詳細情報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。

[ヒット件数（Hits）]
シスコの管理対象デバイスまたは Nmap によってサーバが検出された回数。ホスト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 になることに注意してください。

[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ることに注意してください。また、ホスト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、システム ポリシーの設定に従ってタイムアウトになりますが、防御センターの Web インターフェイスを介したユーザ入力はタイムアウトにならないことに注意してください。

[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。ベンダーが不明な場合、このフィールドは表示されません。

Version

サーバのバージョン。バージョンが不明な場合、このフィールドは表示されません。

ソース

次の値のいずれかを指定します。

- ユーザ: *user_name*
- アプリケーション: *app_name*
- スキャナ: *scanner_type*(Nmap、またはシステム ポリシーによって追加されたスキャナ)
- `FireSIGHT`、`FireSIGHT Port Match`、または `FireSIGHT Pattern Match`(シスコが検出したアプリケーションの場合)
- `NetFlow`(NetFlow データに基づいてネットワーク マップに追加されたサーバの場合)

システムでは、サーバ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。現在の ID について(46-5 ページ)を参照してください。

サーバの詳細を表示する方法:

アクセス: Admin/Any Security Analyst

手順 1　ホスト プロファイルの [サーバ(Servers)] セクションで、サーバの隣にある表示アイコン( )をクリックします。

[サーバの詳細(Server Detail)] ポップアップ ウィンドウが表示されます。

サーバのアイデンティティの編集

ライセンス: FireSIGHT

ホスト上のサーバ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ても、(アイデンティティが 1 つしかない場合でも)サーバは削除されないことに注意してください。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。

シスコの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。

サーバのアイデンティティを編集する方法:

アクセス: Admin/Any Security Analyst

手順 1　ホスト プロファイルの [サーバ(Servers)] セクションで、[表示(View)] をクリックして [サーバの詳細(Server Detail)] ポップアップ ウィンドウを表示します。

手順 2　以下の 2 つの対処法があります。

- サーバのアイデンティティを削除するには、削除するサーバ アイデンティティの隣にある削除アイコン( )をクリックします。
- サーバのアイデンティティを変更するには、サーバ リストでサーバの隣にある編集アイコン( )をクリックします。

  [サーバのアイデンティティ(Server Identity)] ポップアップ ウィンドウが表示されます。

手順 3　以下の 2 つの対処法があります。

- [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 タイプの選択(Select Server Type)] ドロップダウン リストからサーバのタイプを選択します。

手順 4　オプションで対象のサーバ タイプのベンダーと製品のみを表示するには、[サーバ タイプにより制限する(Restrict by Server Type)] チェックボックスをオンにします。

手順 5　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を使用する(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。

手順 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。

たとえば、サーバを Red Hat Linux 9 へマップする場合は、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。

手順 7　サーバに対して修正ファイルが適用されていることを示す場合は、[修正ファイルの設定(Configure Fixes)] をクリックします。それ以外の場合は、9 の手順に進みます。

[使用可能なパッケージ修正ファイル(Available Package Fixes)] ページが表示されます。

手順 8　サーバに適用するパッチを、修正ファイル リストに追加します。

手順 9　[終了(Finish)] をクリックしてサーバ アイデンティティの設定を完了します。

サーバ アイデンティティの競合の解決

ライセンス：FireSIGHT

サーバ アイデンティティの競合が発生するのは、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、サーバのアイデンティティ データをホストへ追加したときに、競合するサーバ アイデンティティを示しているポートのトラフィックをシステムが検出した場合です。

サーバ アイデンティティの競合を解決する方法：

アクセス：Admin/Any Security Analyst

手順 1　[サーバ（Server）] リストで、サーバの隣にある解決のアイコンをクリックします。

[サーバのアイデンティティ（Server Identity）] ポップアップ ウィンドウが表示されます。

手順 2　[サーバ タイプの選択（Select Server Type）] ドロップダウン リストからサーバのタイプを選択します。

手順 3　オプションで対象のサーバ タイプのベンダーと製品のみを表示するには、[サーバ タイプにより制限する（Restrict by Server Type）] チェックボックスをオンにします。

手順 4　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を使用する（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。

手順 5　[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。

たとえば、サーバを Red Hat Linux 9 へマップする場合は、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。

手順 6　サーバに対して修正ファイルが適用されていることを示す場合は、[修正ファイルの設定（Configure Fixes）] をクリックします。それ以外の場合は、9の手順に進みます。

[使用可能なパッケージ修正ファイル（Available Package Fixes）] ページが表示されます。

手順 7　サーバに適用するパッチを、修正ファイル リストに追加します。

手順 8　[終了（Finish）] をクリックしてサーバ アイデンティティの設定を完了し、ホスト プロファイルへ戻ります。

ホスト プロファイルでのアプリケーションの使用

ライセンス：FireSIGHT

ホスト プロファイルで、ホスト上で稼働しているアプリケーションを表示することができます。ホスト プロファイルからアプリケーションを削除する場合は、そのアプリケーションを削除します。

ホスト プロファイルでのアプリケーションの管理については、以下を参照してください。

- ホスト プロファイルでのアプリケーションの表示（49-23 ページ）
- ホスト プロファイルからのアプリケーションの削除（49-24 ページ）

ホスト プロファイルでのアプリケーションの表示

ライセンス：FireSIGHT

システムは、ネットワーク上のホストで稼働しているさまざまなクライアントと Web アプリケーションを検出できます。

(注)　モニタ対象のネットワーク内のホストでアプリケーションを検出するには、システムのネットワーク検出ポリシー内の NetFlow デバイスに対するディスカバリ ルールで、[アプリケーション（Applications）] 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、NetFlow ルールではデフォルトで有効になっており、管理対象デバイスを介した検出で使用されるルールに対しては無効にすることはできません。

ホスト プロファイルは、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、および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を表示します。

防御センターは、ホスト上で稼働している最大 16 個のクライアントを表示します。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 ブラウザについてホスト プロファイルは、アクセスされた最初の 100 個の Web アプリケーションを表示します。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

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）

FireSIGHT システムで識別された場合、Nmap または他のアクティブなソースで取得された場合、あるいはホスト入力機能を介して取得された場合に、ペイロードから派生したクライアント情報。有効なソースから識別情報が提供されない場合、この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、特定のタイプのコンテンツ（WMV や QuickTime など）を表します。これらのコンテンツは、FireSIGHT システムによって識別されるか、Nmap によって取得されるか、他のアクティブなソースによって取得されるか、またはホスト入力機能を介して取得されます。有効なソースから識別情報が提供されない場合、このフィールドは空白になります。

ホストが、有効な相関ポリシーのコンプライアンス ホワイト リストに違反するアプリケーションを実行している場合、防御センターは非準拠アプリケーションに、ホワイト リストの違反アイコン( )のマークを付けます。

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イベント アイコン( )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。接続データの詳細については、接続およびセキュリティ インテリジェンスのデータの使用（39-1 ページ）を参照してください。

ホスト プロファイルからのアプリケーションの削除

ライセンス：FireSIGHT

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、そのホストにホワイト リストに準拠することがあります。

（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。

ホスト プロファイルからアプリケーションを削除する方法：

アクセス：Admin/Any Security Analyst

手順 1 ホスト プロファイルの [アプリケーション（Applications）] セクションで、削除するアプリケーションの隣にある削除アイコン( )をクリックします。

そのホストでアプリケーションが削除されます。

ホスト プロファイルでの VLAN タグの使用

ライセンス：FireSIGHT

ホストが仮想 LAN（VLAN）のメンバーである場合、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、検出した各タグについて以下の情報を表示します。

- [VLAN ID] は、ホストがメンバーである 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、防御センターは最も内側の 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、防御センターは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 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、システムはより正確なネットワーク マップを生成できるようになります。

ホスト プロファイルでのユーザ履歴の使用

ライセンス：FireSIGHT

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。一般的なユーザは夜間にログオフし、他のユーザとホストのリソースを共有します。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 アイデンティティ リストは棒グラフで提示され、ユーザの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、棒グラフが灰色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を持たないユーザのログインを、そのホストの IP アドレスに関連付けて、ホストのユーザ履歴にユーザが表示されるようにします。ただし、同じ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ると、権限を持つユーザのログインに関連付けられているユーザは、ホスト IP アドレスとの関連付けを引き継ぎます。権限を持たない別のユーザがログインしても、ホスト IP アドレスとユーザとの関連付けは解消されません。ユーザのタイプの詳細については、ユーザ データベース（45-8 ページ）を参照してください。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、ホストへのログインに失敗したユーザが含まれます。

ホスト プロファイルでのホスト属性の使用

ライセンス：FireSIGHT

*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ホストをさまざまに分類することができます。ホスト属性の値として、正の整数、文字列、または URL を使用できます。また、文字列の値のリストを作成し、ホスト IP アドレスに基づいて、それらを自動的に割り当てることができます。ユーザ定義のホスト属性の作成および管理の詳細については、ユーザ定義のホスト属性の使用（49-35 ページ）を参照してください。

FireSIGHT システムには、[ホストの重要度（Host Criticality）] と [メモ（Notes）] の 2 つの事前定義ホスト属性が含まれています。これらの定義済みホスト属性の使用については、事前定義のホスト属性の使用（49-34 ページ）を参照してください。

また、ユーザがコンプライアンス ホワイト リストを作成すると、ホワイト リストと同じ名前のホスト属性が自動的に作成されます。使用される値は、[標準（Compliant）]（ホワイト リストに準拠しているホストの場合）、[非標準（Non-Compliant）]（ホワイト リストに違反しているホストの場合）、または [未評価（Not Evaluated）]（ホワイト リストの正当な対象ではないホスト、または何らかの理由で評価されないホストの場合）です。ホワイト リストのホスト属性の値は、手動で変更**できません**。ホワイト リストの詳細については、FireSIGHT システムのコンプライアンス ツールとしての使用（52-1 ページ）を参照してください。

ホスト属性の値の割り当て

ライセンス: FireSIGHT

既存のホスト属性の値として、正の整数、文字列、または URL を指定できます。

ヒント　ホスト プロファイルのページの [属性(Attributes)] セクションの [編集(Edit)] リンクをクリックして、ホストのホスト属性を簡単に割り当てることができます。これにより、すべてのホスト属性のフィールドが含まれているポップアップ ウィンドウが起動されます。

ホスト属性の値を割り当てる方法:

アクセス: Admin/Any Security Analyst

手順 1　ホスト プロファイルを開きます。

手順 2　[属性(Attributes)] の下で、値を割り当てるホスト属性の名前をクリックします。

ポップアップ ウィンドウが表示されます。

手順 3　属性の値を入力するか、またはドロップダウン リストから値を選択します。

手順 4　[保存(Save)] をクリックします。

ホスト属性の値が保存されます。

ホスト プロファイルでのホスト プロトコルの使用

ライセンス: FireSIGHT

ホスト プロファイルで、ホスト上で稼働しているプロトコルを確認ができます。必要に応じて、特定のホストのホスト プロトコルをプロファイルから削除することもできます。

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。

次に、プロトコルとネットワークのレイヤ情報について説明します。

[プロトコル(Protocol)]

ホストが使用するプロトコルの名前。

[レイヤ(Layer)]

プロトコルを実行しているネットワーク層([ネットワーク(Network)] または [トランスポート(Transport)])。

ホストが、有効な相関ポリシーのコンプライアンス ホワイト リストに違反するプロトコルを実行している場合、防御センターは非準拠プロトコルを、ホワイト リストの違反アイコン( )でマークします。

ホスト上で稼働していないことが判明しているプロトコルを削除するには、ホスト プロファイルからプロトコルを削除します。ホストからプロトコルを削除すると、そのホストがホワイト リストに準拠することがある点に注意してください。

(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方法:

アクセス: Admin/Any Security Analyst

手順 1　ホスト プロファイルの [プロトコル(Protocols)] セクションで、削除するプロトコルの隣にある削除アイコン( )をクリックします。

そのホストでプロトコルが削除されます。

ホスト プロファイルにおけるホワイト リスト違反の使用

ライセンス: FireSIGHT

コンプライアンス ホワイト リスト(または*ホワイト リスト*)は一連の基準で、ユーザはこれを使用して、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ホワイト リストを追加した場合に、システムでホワイト 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、防御センターはホワイト 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。これらのホワイト リスト イベントはそれぞれ*ホワイト 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ホワイト 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 つ以上のホワイト 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ホワイト 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ホワイト リスト違反の説明が続きます。

タイプ(Type)

違反のタイプ(つまり、非準拠のオペレーティング システム、アプリケーション、サーバ、またはプロトコルのいずれが原因で違反が生じたか)。

理由(Reason)

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ホワイト 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。

ホワイト リスト(White List)

違反に関連付けられているホワイト リストの名前。

さらに、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、およびサーバに関連付けられたセクションでは、防御センターによって非準拠の要素にホワイト リスト違反のアイコン（）が付けられます。たとえば、Microsoft Windows ホストのみを許可するようなホワイト 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ホワイト リスト違反のアイコンを表示します。

ホストのプロファイルを使用して、コンプライアンス ホワイト リストに対して共有ホスト プロファイルを作成できることに注意してください。詳細は、次の項ホスト プロファイルからのホワイト リスト ホスト プロファイルの作成を参照してください。

ホスト プロファイルからのホワイト リスト ホスト プロファイルの作成

ライセンス：FireSIGHT

コンプライアンス ホワイト リストの共有ホスト プロファイルは、複数のホワイト 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、複数のホワイト 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ホワイト 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 ホワイト 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。

ホスト プロファイルに基づいてコンプライアンス ホワイト リストに対する共有ホスト プロファイルを作成する方法：

アクセス：管理

手順 1　任意のネットワーク マップまたはイベント ビューからホスト プロファイルにアクセスします。

詳細については、ホスト プロファイルの表示（49-5 ページ）を参照してください。

手順 2　[ホワイト リスト プロファイルの生成（Generate White List Profile）] をクリックします。

[共有プロファイルの編集（Edit Shared Profiles）] ページが表示されます。このページのフィールドには、アクセスしたホスト プロファイルの情報に基づいて値が挿入されています。

手順 3　各自のニーズに応じて、共有ホスト プロファイルを変更し、保存します。

コンプライアンス ホワイト リストに対する共有ホスト プロファイルの作成については、共有ホスト プロファイルの操作（52-28 ページ）を参照してください。

ホスト プロファイルでのマルウェア検出の使用

ライセンス：FireSIGHT および Malware

[最新のマルウェア検出（Most Recent Malware Detections）] セクションには、最近のマルウェア イベント（ホストによるマルウェア ファイルの送受信）が最大 100 個表示されます。ホスト プロファイルは、ネットワークベースのマルウェア イベントとエンドポイントベースのマルウェア イベントの両方を表示します。

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。マルウェア イベントの詳細については、マルウェア イベントの操作（40-18 ページ）を参照してください。

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。

時刻（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）。エンドポイントベースのマルウェア イベントの場合は、ホストは常に受信側であることに注意してください。

[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 プロファイルでマルウェアの検出を確認する際には、イベント ビューアで、そのホストのマルウェア イベントを確認できます。イベントを確認するには、マルウェアのアイコン（  ）をクリックします。

ホスト プロファイルでの脆弱性の使用

ライセンス：FireSIGHT

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。

[Sourcefire の脆弱性（Sourcefire Vulnerabilities）] セクションには、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いた脆弱性が示されます。

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、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 データに基づいてネットワーク マップに追加されたホストで使用できるオペレーティング システムの情報がないため、ホスト入力機能を使用してホストのオペレーティング システムのアイデンティティを手動で設定しない限り、防御センターはどの脆弱性がホストに影響を与えるかを判断できません。

サーバ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、システム ポリシーを使用して、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。詳細については、サーバの脆弱性のマッピング（63-33 ページ）を参照してください。

ホスト入力機能を使用して、ネットワーク上のホストに関する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 の脆弱性（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、『*FireSIGHT システム Host Input API Guide*』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）] セクションの列について説明します。

[名前（Name）]
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（Port）]
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）。

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。

ホスト プロファイルで脆弱性を表示する場合には、次のことが可能です。

- 列ヘッダーをクリックして、[脆弱性（Vulnerabilities）] セクションの列をソートする。ソートを反転させるには、再度クリックします。
- 脆弱性の名前をクリックして、脆弱性に関する技術的な詳細（既知の解決方法など）を表示する。詳細については、脆弱性の詳細の表示（49-31 ページ）を参照してください。脆弱性のイベント ビュー、または Vulnerabilities ネットワーク マップから、脆弱性の詳細にアクセスできることに注意してください。
- 脆弱性が、影響の相関関係を評価するために使用されないようにする。詳細については、脆弱性の Impact Qualification の設定（49-32 ページ）を参照してください。

- 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する。詳細については、脆弱性に対するパッチのダウンロード（49-33 ページ）を参照してください。
- ホストにパッチが適用されたことが判明している場合は、個々の脆弱性について脆弱ではないとホストをマークする。詳細については、個々のホストに対する脆弱性の設定（49-34 ページ）を参照してください。

脆弱性の詳細の表示

ライセンス：FireSIGHT

脆弱性の詳細には、脆弱性および既知の解決方法に関する技術的な説明が含まれています。

特定の脆弱性について脆弱性の詳細にアクセスするには、[分析（Analysis）] > [脆弱性（Vulnerabilities）]、または [分析（Analysis）] > [サードパーティの脆弱性（Third-Party Vulnerabilitie）] を選択し、SVID の隣の表示アイコン（ ）をクリックします。ネットワーク マップおよびホスト プロファイルから脆弱性の詳細にアクセスすることもできます。

次に、[脆弱性の詳細（Vulnerability Detail）] ページのフィールドについて説明します。

[シスコ脆弱性 ID（Cisco Vulnerability ID）]

脆弱性を追跡するためにシステムで使用する識別番号（SVID）。

[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と、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。脆弱性に関連付けられている SID がない場合は、このフィールドは表示されません。

[BugTraq ID]

Bugtraq データベースで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）データベースで、脆弱性に関連付けられている識別番号（http://www.cve.mitre.org/）。

役職（Title）

脆弱性のタイトル。

[Impact Qualification]

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。防御センターは、影響の相関関係において、無効な脆弱性を無視します。

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るかどうかが決まります。この機能を使用して脆弱性を有効および無効にするための情報については、脆弱性の Impact Qualification の設定（49-32 ページ）を参照してください。

[公開日（Date Published）]
脆弱性が公開された日付。

[脆弱性の影響（Vulnerability Impact）]
Bugtraq データベースにおいて脆弱性に割り当てられている重大度。1～10 の値で、10 は最も重大であることを示します。脆弱性の影響は、Bugtraq エントリの作成者によって決定されます。この作成者は、SANS Critical Vulnerability Analysis（CVA）の基準に従い、自身の判断に基づいて脆弱性の影響レベルを決定します。

[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。

利用可能なエクスプロイト（Available Exploits）
脆弱性に対して既知のエクスプロイトがあるかどうかを示します。

Description
脆弱性に関する概要的な説明。

[技術的な説明（Technical Description）]
脆弱性に関する詳細な技術的説明。

[解決策（Solution）]
脆弱性の修復に関する情報。

[その他の情報（Additional Information）]
既知のエクスプロイトや可用性、エクスプロイトのシナリオ、脆弱性を軽減する方針など、脆弱性に関する追加情報を（利用可能な場合に）表示するには、矢印をクリックします。

[修正ファイル（Fixes）]
選択した脆弱性に対して、ダウンロード可能なパッチへのリンクを示します。

ヒント　修正ファイルまたはパッチのダウンロードへの直接リンクが表示されている場合は、リンクを右クリックして、自分のローカル コンピュータに保存します。

脆弱性の Impact Qualification の設定

ライセンス：FireSIGHT

システムが、ネットワークに対して適用されない脆弱性を報告した場合は、インパクト フラグの相関を評価するときにこの脆弱性が使用されないようにすることができます。ホスト プロファイルで脆弱性を非アクティブにした場合、ネットワーク上のすべてのホストに対してその脆弱性が非アクティブになることに注意してください。ただし、脆弱性は随時に再アクティブ化できます。

ホストのオペレーティング システム、またはホスト上のいずれかのアプリケーションのアイデンティティについて競合が存在する場合、システムは、競合が解決されるまで、競合している両方のアイデンティティに対して脆弱性を示します。詳細については、ID の競合について（46-7 ページ）およびオペレーティング システムのアイデンティティの競合を解決する（49-15 ページ）を参照してください。

システムは、Impact Qualification 機能を使用して無効にする脆弱性に基づいて、侵入ルールのルール状態を推奨しないことにも注意してください。詳細については、ネットワーク資産に応じた侵入防御の調整（33-1 ページ）を参照してください。

ヒント　ネットワーク マップおよび脆弱性のイベント ビューから脆弱性を非アクティブにすることもできます。詳細については、脆弱性のネットワーク マップの操作（48-8 ページ）および脆弱性の非アクティブ化（50-58 ページ）を参照してください。

システム全体で脆弱性の使用を変更する方法:

アクセス: Admin/Any Security Analyst

手順 1　非アクティブにする脆弱性の影響を受けるホストのホスト プロファイルにアクセスします。

手順 2　[脆弱性（Vulnerabilities）] セクションを展開します。

手順 3　有効または無効にする脆弱性の名前をクリックします。

ポップアップ ウィンドウが表示され、脆弱性の詳細が示されます。詳細については、脆弱性の詳細の表示（49-31 ページ）を参照してください。

手順 4　[Impact Qualification] ドロップダウン リストから [無効（Disabled）] または [有効（Enabled）] を選択して、脆弱性がどのように使用されるかを指定します。

手順 5　ネットワーク マップ上のすべてのホストに対して、Impact Qualification を変更することを確認します。

脆弱性が有効または無効になります。

手順 6　[完了（Done）] をクリックして、脆弱性の詳細のポップアップ ウィンドウを閉じます。

脆弱性に対するパッチのダウンロード

ライセンス: FireSIGHT

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が利用可能な場合には、これらのパッチをダウンロードすることができます。

脆弱性に対するパッチをダウンロードする方法:

アクセス: Admin/Any Security Analyst

手順 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。

手順 2　[脆弱性（Vulnerabilities）] セクションを展開します。

手順 3　パッチを適用する脆弱性の名前をクリックします。

[脆弱性の詳細（Vulnerability Detail）] ページが表示されます。

手順 4　[修正ファイル（Fixes）] セクションを展開します。

脆弱性に対してダウンロード可能なパッチの一覧が表示されます。

手順 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。

パッチ ベンダーのダウンロード ページが表示されます。

手順 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。

個々のホストに対する脆弱性の設定

ライセンス：FireSIGHT

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アクティブまたは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、インパクト レベルは自動的に 1 レベル減少します。

1 つのホストに対して脆弱性をアクティブまたは非アクティブにする方法：

アクセス：Admin/Security Analyst

手順 1　ホスト プロファイルを開きます。

手順 2　[脆弱性（Vulnerabilities）] の隣で [編集（Edit）] をクリックします。

[ホストの脆弱性エディタ（Host Vulnerabilities editor）] ページが表示されます。

ヒント　脆弱性に関する詳細を表示するには、[表示（View）] をクリックします。詳細については、脆弱性の詳細の表示（49-31 ページ）を参照してください。

手順 3　以下の 2 つの対処法があります。

- 脆弱性を非アクティブにするには、[有効な脆弱性（Valid Vulnerabilities）] リストから脆弱性を選択し、下向きの矢印をクリックします。
- 脆弱性をアクティブにするには、[無効な脆弱性（Invalid Vulnerabilities）] リストから脆弱性を選択し、上向きの矢印をクリックします。

ヒント　複数の脆弱性を選択するには、Ctrl キーまたは Shift キーを押しながらクリックします。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。

手順 4　[保存（Save）] をクリックします。

変更が保存されます。

事前定義のホスト属性の使用

ライセンス：FireSIGHT

各ホストに割り当てることができる事前定義のホスト属性として、ホストの重要度とホスト特有のメモの 2 つの属性があります。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できます。たとえば業務にとって、組織のメール サーバは一般的なユーザ 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、および業務にとって重要なその他のデバイスに [高（High）] 値を割り当てて、他のホストに [中（Medium）] または [低（Low）] 値を割り当てることができます。次に相関ポリシーを作成できます。これは、影響を受けるホストの重要度に基づいてさまざまなアラートを起動します。

メモ機能を使用して、他の分析を表示するホストの情報を記録します。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、メモ機能を使用して、システムは意図的にパッチが適用されていないと示すことができます。

ホスト プロファイルで事前定義のホスト属性を設定する方法:

アクセス: Admin/Security Analyst

手順 1　ビジネスの重要度を設定するホストのホスト プロファイルを開きます。

手順 2　[属性(Attributes)] の隣の鉛筆型のアイコン( )をクリックします。

[ホスト属性(Host Attributes)] ポップアップ ウィンドウが表示されます。

手順 3　[ホストの重要度(Host Criticality)] ドロップダウン リストから、適用する値として [なし(None)]、[低(Low)]、[中(Medium)]、または [高(High)] を選択します。

手順 4　[保存(Save)] をクリックします。

選択した内容が保存されます。

ユーザ定義のホスト属性の使用

ライセンス: FireSIGHT

FireSIGHT システムには、ホストの重要度とホスト メモの 2 つの事前定義のホスト属性があります。これらの属性を使用して、ネットワーク上のホストのビジネスでの重要度を示すことができます。ホストを識別するための他の基準がある場合は、ユーザ定義のホスト属性を作成できます。

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。相関ポリシーまたは検索でこれらの属性を使用することができます。また、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することもできます。

(注)　ホスト属性は、ポリシーごとではなくグローバルに定義されます。作成したホスト属性は、適用されるポリシーに関係なく使用できます。

ユーザ定義のホスト属性の例として、次のものがあります。

- ホストに対する物理的なロケーション ID(ファシリティ コード、市町村、部屋番号など)の割り当て。
- 特定のホストを担当するシステム管理者を示す Responsible Party Identifier の割り当て。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。

ホスト属性として、テキスト文字列、テキストの事前定義されたリストから選択した値、または数字の範囲を使用できます。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ることもできます。この機能を使用すると、ネットワーク上にホストが初めて表示されたときに、新しいホストへ値を自動的に割り当てることができます。

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

ホストに対して最大 255 文字の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

正の整数の番号範囲の最初の数と最後の数を指定し、ホストに対してこれらの番号を手動で割り当てることができます。

リスト

文字列値のリストを作成し、ホストに対してこの値のいずれかを手動で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。

（注） 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、割り当てられた値は、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）] テーブルを参照する場合は、このことに注意してください。

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。

ユーザがコンプライアンス ホワイト リストを作成すると、ホワイト リストと同じ名前のホスト属性が自動的に作成されることに注意してください。使用される値は、[準拠（Compliant）]（ホワイト リストに準拠しているホストの場合）、[非準拠（Non-Compliant）]（ホワイト リストに違反しているホストの場合）、および [未評価（Not Evaluated）]（ホワイト リストの正当な対象ではないホスト、または何らかの理由で評価されないホストの場合）です。ホワイト リストのホスト属性の値は、手動で変更**できません**。ホワイト リストの詳細については、FireSIGHT システムのコンプライアンス ツールとしての使用（52-1 ページ）を参照してください。

詳細については、次の各項を参照してください。

- ユーザ定義のホスト属性の作成（49-36 ページ）
- ユーザ定義ホスト属性の編集（49-38 ページ）
- ユーザ定義ホスト属性の削除（49-39 ページ）

ユーザ定義のホスト属性の作成

ライセンス：FireSIGHT

次の手順では、ユーザ定義のホスト属性の作成方法について説明します。

（注） ホスト属性は、ポリシーごとではなくグローバルに定義されます。作成したホスト属性は、適用されるポリシーに関係なく使用できます。

新しいホスト属性を作成する方法：

アクセス：Admin/Discovery Admin

手順 1　[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（Host Attributes）] ページが表示されます。

手順 2　[ホスト属性の管理（Host Attribute Management）] をクリックします。

[ホスト属性の管理(Host Attribute Management)] ページが表示されます。

手順 3　[属性の作成(Create Attribute)] をクリックします。

[属性の作成(Create Attribute)] ページが表示されます。

手順 4　[名前(Name)] フィールドに、英数字および空白を使用してホスト属性の名前を入力します。

手順 5　ホスト プロファイルでのホスト属性の使用(49-25 ページ)の説明に従って、[タイプ(Type)] ドロップダウン リストから、作成する属性のタイプを選択します。

- [テキスト(Text)] または [URL] ホスト属性を作成する場合は、続いて 6 の手順を実行します。
- [整数(Integer)] ホスト属性を作成する場合は、整数ホスト属性の作成(49-37 ページ)を参照してください。
- [リスト(List)] ホスト属性を作成する場合は、リスト ホスト属性の作成(49-37 ページ)を参照してください。

手順 6　[保存(Save)] をクリックします。

新しいユーザ定義のホスト属性が保存されます。

整数ホスト属性の作成

ライセンス: FireSIGHT

整数ベースのホスト属性を定義する場合は、その属性に使用できる数字の範囲を指定する必要があります。

整数ベースのホスト属性を作成する方法:

アクセス: Admin/Discovery Admin

手順 1　[最小値(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。

手順 2　[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。

手順 3　[保存(Save)] をクリックします。

新しい整数ベースのホスト属性が保存されます。

リスト ホスト属性の作成

ライセンス: FireSIGHT

リストベースのホスト属性を定義する場合は、リストに対してそれぞれの値を指定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。

ホスト属性の値を作成する場合は、IP アドレスのブロックに値を自動的に割り当てて、新しいホストが検出されたときに、ホスト属性の値が自動的に割り当てられるようにすることもできます。

リストベースのホスト属性を作成する方法:

アクセス: Admin/Discovery Admin

手順 1　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。

[値のリスト(List Values)] セクションが展開されます。

手順 2　[名前(Name)] フィールドに、英数字、記号、およびスペースを使用して、追加する最初の値を入力します。

手順 3　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、[ネットワークの追加(Add Networks)] をクリックします。

[ネットワークの自動割り当て(Auto-Assign Networks)] セクションが展開されます。

手順 4　[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。

手順 5　[IP アドレス(IP Address)] および [ネットマスク(Netmask)] フィールドに、IP アドレス、およびこの値を自動割り当てする IP アドレスのブロックを表すネットワーク マスクを(CIDR 表記で)入力します。

FireSIGHT システムでの CIDR 表記の使用法の詳細については、IP アドレスの表記規則 (1-24 ページ)を参照してください。

手順 6　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 1 ～ 5 を繰り返します。

ヒント　特定の IP ブロック内のホストに対してリストの値を自動割り当てしない場合は、事前定義のホスト属性の使用 (49-34 ページ)の説明に従って手動で割り当てることができます。

ユーザ定義ホスト属性の編集

ライセンス: FireSIGHT

ユーザ定義の既存のホスト属性を変更する場合、値の定義は変更できますが、属性のタイプ(テキスト、リスト、整数、URL)は変更できません。また、コンプライアンス ホワイト リストのホスト属性を変更することは**できません**。

ユーザ定義の既存のホスト属性を編集する方法:

アクセス: Admin/Discovery Admin

手順 1　[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(Host Attributes)] ページが表示されます。

手順 2　[ホスト属性の管理(Host Attribute Management)] をクリックします。

[ホスト属性の管理(Host Attribute Management)] ページが表示されます。

手順 3　編集するホストの属性の隣にある編集アイコン( )をクリックします。

ホスト属性のページには、選択した属性の設定が表示されます。

手順 4　必要に応じて設定を変更し、[保存(Save)] をクリックします。

編集可能な属性タイプと、それらの属性に指定できる値については、ユーザ定義のホスト属性の作成(49-36 ページ)を参照してください。

ユーザ定義ホスト属性の削除

ライセンス: FireSIGHT

ユーザ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。コンプライアンス ホワイト リストのホスト属性を削除することは**できません**。

ホスト属性を削除する方法:

アクセス: Admin/Discovery Admin

手順 1　[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(Host Attributes)] ページが表示されます。

手順 2　[ホスト属性の管理(Host Attribute Management)] をクリックします。

[ホスト属性の管理(Host Attribute Management)] ページが表示されます。

手順 3　削除するホスト属性の隣にある削除アイコン( )をクリックします。

選択したホスト属性がシステムから削除されます。

ホスト プロファイルでのスキャン結果の使用

ライセンス: FireSIGHT

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働している任意のサーバ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(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。

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、ポート上で稼働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。詳細は、次の項ホスト プロファイルからのホストのスキャンを参照してください。

ホスト プロファイルからのホストのスキャン

ライセンス: FireSIGHT

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 を使用してホストをスキャンする場合は、Nmap で提供されるオペレーティング システムとサーバのデータを最新にしておくために、スケジュールされたスキャンを定期的にセットアップすることもできます。詳細については、Nmap スキャンの自動化(62-5 ページ)を参照してください。

ホスト プロファイルからホストをスキャンする方法:

アクセス: 管理

手順 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。

[ホストのスキャン(Scan Host)] ポップアップ ウィンドウが表示されます。

手順 2 ホストのスキャンで使用するスキャン修復の隣にある [スキャン(Scan)] をクリックします。

ホストがスキャンされ、結果がホスト プロファイルに追加されます。