ホスト プロファイルの使用

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

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 アクティビティ
- ホストに関連付けられているホワイト リスト違反
- 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アダプティブ プロファイルの更新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 アイデンティティのリストに追加されます。

ホスト プロファイルには、次の制限事項があります。

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 ライセンスの制限に達した。

- 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、ホストを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）。

関連トピック

ホスト プロファイルの表示 （3 ページ）

ホスト プロファイルの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

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 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。

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、Firepower 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。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 トラフィックで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、Firepower 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。

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のホワイト リストに違反している場合、Firepower Management Center 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、ホスト オペレーティング システムの識別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

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

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）] ボタン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 （6 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アイコン（  ）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

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

Firepower 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 （10 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。

関連トピック

ネットワーク検出アイデンティティ競合の解決の設定

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現行化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

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

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

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。

関連トピック

ネットワーク検出アイデンティティ競合の解決の設定

ホスト プロファイルのサーバ

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、ホストを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

サーバについて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する場合は、[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。

（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ホワイトリストに違反しているサーバを実行している場合、Firepower Management Center 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。

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）

Firepower 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。

関連トピック

ホスト制限と検出イベント ロギング
NetFlow データと管理対象デバイス データの違い
アプリケーション ディテクタの基本

ホスト プロファイルのサーバの詳細

Firepower 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。Firepower Management Center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。

Firepower 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、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、いくつかの目的のためにサーバの現行のアイデンティティを使用します。

サーバの詳細には、選択されたサーバについて知られている、更新済みのサブサーバ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）

Firepower システムの管理対象デバイスまたは Nmap スキャナによってサーバが検出された回数。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、Firepower 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）
- Firepower 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。

関連トピック

アプリケーションおよびオペレーティング システムの現在の ID

サーバに関する詳細情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

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

サーバのアイデンティティの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

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 サーバのアイデンティティを削除するには、削除するサーバのアイデンティティの横にある削除アイコン（  ）をクリックします。

ステップ 4 サーバのアイデンティティを変更するには、サーバ リストでサーバの横にある編集アイコン（  ）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 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。

ステップ 6 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 アイデンティティの競合の解決

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

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、サーバ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 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（Servers）] セクションに移動します。

ステップ 2 サーバの横にある解決アイコンをクリックします。

ステップ 3 [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。

ステップ 4 必要に応じて、対象のサーバ タイプのベンダーと製品のみを表示する場合は、[サーバ タイプ別に制限（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。

関連トピック

ネットワーク検出アイデンティティ競合の解決の設定

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のホワイト 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、Firepower Management Center 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。

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。

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、Firepower 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、Firepower 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 プロファイルからの Web アプリケーションの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

ホスト プロファイルからアプリケーションを削除して、ホスト上で稼動していないことがわかっているアプリケーションを削除することができます。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アイコン（）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（ネットワークまたはトランスポート）。

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 ホワイト リストに違反する場合、Firepower Management Center は非準拠プロトコルに、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 ホワイト 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 プロファイルからのプロトコルの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

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アイコン（  ）をクリックします。

ホスト プロファイル内の侵害の兆候

Firepower システムは、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、接続イベントおよびファイルまたはマルウェア イベント）を関連付け、モニタ対象ネットワーク上のホストが悪意のある手段によって侵害された可能性があるかどうかを判断します。イベント データの特定の組み合わせと頻度が、影響を受けるホストの侵害の兆候（IOC）タグをトリガーします。

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システムを構成するには、侵害の兆候ルールの有効化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、侵害の兆候データとそのトピックのサブトピックを参照してください。

関連トピック

侵害の兆候

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、Firepower 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。一般的なユーザは夕方にログオフし、また他のユーザ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 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 ログインを、そのホストの IP アドレスに関連付けるため、そのユーザはそのホストのユーザ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。Firepower 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
- ホワイトリスト ホスト属性
- ユーザ定義ホスト属性

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

Firepower 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。

ホワイト リストのホスト属性

ユーザが作成するそれぞれのコンプライアンス ホワイト リストによって、そのホワイト 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。ホワイト 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）：ホワイト リストに準拠しているホストを識別します。
- 非準拠（Non-Compliant）：ホワイト リストに違反しているホストを識別します。
- 未評価（Not Evaluated）：ホワイト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。

ホワイト リストのホスト属性の値を編集したり、ホワイト 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ホワイト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 ベースのホスト属性の作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

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 作成する属性の [タイプ（Type）] を選択します。 ユーザ定義のホスト属性 （23 ページ）
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

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

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 （23 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。

リストベースのホスト属性の作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

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 （23 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

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

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ホワイト 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 プロファイル内のホワイト リスト違反

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）は一連の基準であり、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、Firepower Management Center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、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（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。

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、およびサーバに関連付けられているセクションで、Firepower Management Center が、非準拠の要素にホワイト リスト違反のアイコン（  ）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ホワイト リストでは、ホスト プロファイルで、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が表示されます。

（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 ホワイト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。

共有ホワイト リスト ホスト プロファイルの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

コンプライアンス ホワイト リストに対する共有ホスト プロファイルは、複数のホワイト リストをまたがる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 アドレスを持つ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。

手順

ステップ 1 ホスト プロファイルで、[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。

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

ホワイト リスト ホスト プロファイルの作成

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 プロファイルは、ネットワークベース（ネットワーク向け AMP）とエンドポイントベース（AMP for Endpoints）のマルウェア イベントを一覧で示します。

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。

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 アイコン（  ）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。

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役割（送信者または受信者）。エンドポイントベースのマルウェア イベントの場合は、ホストは常に受信者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 System 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）] セクションのカラム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）。

関連トピック

脆弱性データのフィールド
脆弱性の非アクティブ化

脆弱性に対するパッチのダウンロード

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

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。

個々のホストに対する脆弱性の非アクティブ化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

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 （32 ページ）
複数の脆弱性の非アクティブ化

個々の脆弱性の非アクティブ化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

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。先祖ドメインで脆弱性をアクティブにした場合、リーフ ドメインでは、そのドメインにあるデバイスに対して脆弱性のアクティブ化または非アクティブ化を実行できます。

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）]** > **[脆弱性（Vulnerabilities）]** > **[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アイコン（  ）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

個々のホストに対する脆弱性の非アクティブ化 （31 ページ）
複数の脆弱性の非アクティブ化
オペレーティング システムのアイデンティティの競合 （10 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。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

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

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。Nmap スキャン インスタンスの追加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