ネットワーク ディスカバリの強化

FireSIGHT システムによって収集されるネットワーク トラフィックに関する情報は、この情報を関連付けて最も脆弱で最も重要なネットワークのホストを識別することができる場合に、最もその価値を発揮します。

たとえば、ネットワーク上に SuSE Linux のカスタマイズ バージョンを実行している複数のデバイスがある場合、システムはそのオペレーティング システムを識別することができません。そのため、脆弱性をそれらのホストにマッピングすることはできません。しかし、システムに SuSE Linux に関する脆弱性のリストがあるならば、同じオペレーティング システムを実行する他のホストを識別するために使用できるカスタム フィンガープリントを、ホストのいずれか 1 台に対して作成することができます。フィンガープリントに SuSE Linux の脆弱性リストのマッピングを含め、フィンガープリントに一致する各ホストとそのリストを関連付けることができます。

また、ホストの入力機能を使用して、ホスト データをサードパーティ システムからネットワーク マップに直接入力することもできます。ただし、サードパーティのオペレーティング システムやアプリケーション データは、脆弱性情報に自動的にマッピングされません。脆弱性を確認し、サードパーティのオペレーティング システム、サーバ、アプリケーション プロトコル データを使用してホストの影響の関連付けを実行する場合、サードパーティ システムからのベンダーとバージョンの情報を、脆弱性データベース（VDB）にリストされているベンダーとバージョンにマッピングする必要はあります。また、ホストの入力データを継続的に維持する必要がある場合もあります。アプリケーション データを FireSIGHT システム ベンダーおよびバージョン定義にマッピングしたとしても、インポートされたサードパーティの脆弱性はクライアントまたは Web アプリケーションの影響評価に使用されないことに注意してください。

システムがネットワーク上のホストで実行されているアプリケーション プロトコルを識別できない場合は、システムがポートまたはパターンに基づいてアプリケーションを識別できるようにする、ユーザ定義のアプリケーション プロトコル ディテクタを作成できます。また、特定のアプリケーション ディテクタをインポートしたり、アクティブ/非アクティブにしたりすることによって、FireSIGHT システムのアプリケーション検出機能をカスタマイズすることができます。

さらに、Nmap アクティブ スキャナのスキャン結果を使用してオペレーティング システムやアプリケーション データの検出を置き換えたり、サードパーティの脆弱性で脆弱性リストを拡張したりすることもできます。システムは複数のソースからのデータを照合して、アプリケーションの ID を判別できます。この実行方法の詳細については、「現在の ID について」（P.42-5）を参照してください。アクティブ スキャンの詳細については、「アクティブ スキャンの設定」（P.43-1）を参照してください。

詳細については、次の項を参照してください。

検出戦略の評価

ライセンス：FireSIGHT

システムのデフォルト検出機能に変更を加える前に、実装すべきソリューションを決定できるように、どのホストが正しく識別されないか、またその原因を分析する必要があります。以下を参考にして、ソリューションを決定します。

管理対象デバイスは正しく配置されていますか

ライセンス：FireSIGHT

ロード バランサ、プロキシ サーバ、NAT デバイスなどのネットワーク デバイスが、識別されていないホストまたは誤って識別されたホストと管理対象デバイスの間に存在する場合は、カスタム フィンガープリントを使用せずに、誤って識別されたホストの近くに管理対象デバイスを配置します。シスコでは、このシナリオでカスタム フィンガープリントを使用することを推奨しません。

未確認のオペレーティング システムに一意の TCP スタックがありますか

ライセンス：FireSIGHT

システムがホストを誤って識別した場合、カスタム フィンガープリントを作成してアクティブにするか、ディスカバリ データの代わりに Nmap またはホストの入力データを使用するかを決定するために、ホストが誤って識別された理由を調べる必要があります。

注意　ホストの誤認が発生した場合は、カスタム フィンガープリントを作成する前にサポート担当者にお問い合わせください。

ホストがデフォルトではシステムに検出されないオペレーティング システムを実行していて、識別している TCP スタックの特性を既存の検出されているオペレーティング システムと共有していない場合、カスタム フィンガープリントを作成する必要があります。

たとえば、システムが識別できない一意の TCP スタックで Linux のカスタマイズ バージョンが存在する場合、継続的に自分でデータを更新する必要のあるスキャン結果またはサードパーティのデータを使用するのではなく、システムがホストを監視し続けながらそのホストを識別できるカスタム フィンガープリントを作成すると便利です。

オープン ソースの Linux ディストリビューションの多くは同じカーネルを使用し、システムは Linux カーネル名を使用してそれらを識別します。Red Hat Linux システム用のカスタム フィンガープリントを作成する場合、同じフィンガープリントが複数の Linux ディストリビューションに一致するために、その他のオペレーティング システム（Debian Linux、Mandrake Linux、Knoppix など）が Red Hat Linux として識別されることがあります。

フィンガープリントはすべての状況で使用できるわけではありません。たとえば、ホストの TCP スタックが別のオペレーティング システムと似るように、または同一になるように、変更が加えられる事例がありました。たとえば、Apple Mac OS X のフィンガープリントが Linux 2.4 ホストと同じになるように Apple Mac OS X ホストが変更されます。これは、システムがホストを Mac OS X ではなく Linux 2.4 として識別してしまう原因となります。Mac OS X ホスト用にカスタム フィンガープリントを作成すると、正規の Linux 2.4 ホストすべてを Mac OS X ホストとして誤って識別する可能性があります。この場合、Nmap が正しくホストを特定するならば、そのホストに対して定期的な Nmap スキャンをスケジュールできます。

ホスト入力を使用して、サードパーティ システムからデータをインポートする場合、サーバおよびアプリケーション プロトコルを説明するためにサードパーティが使用するベンダー、製品、およびバージョンの文字列を、それらの製品のシスコ定義にマッピングする必要があります。詳細については、「サードパーティ製品マッピングの管理」（P.42-33）を参照してください。アプリケーション データを FireSIGHT システム ベンダーおよびバージョン定義にマッピングしたとしても、インポートされたサードパーティの脆弱性はクライアントまたは Web アプリケーションの影響評価に使用されないことに注意してください。

システムは複数のソースからのデータを照合して、オペレーティング システムまたはアプリケーションの現行 ID を判別できます。この実行方法の詳細については、「現在の ID について」（P.42-5）を参照してください。

Nmap データの場合、定期的な Nmap スキャンをスケジュールできます。ホスト入力データの場合、インポート用の Perl スクリプトまたはコマンド ライン ユーティリティを定期的に実行できます。ただし、アクティブ スキャン データおよびホスト入力データは、データ ディスカバリの頻度で更新されないことがあるので注意してください。

FireSIGHT システムはすべてのアプリケーションを識別できますか

ライセンス：FireSIGHT

ホストがシステムによって正しく識別されるものの、未確認のアプリケーションがある場合、ユーザ定義ディテクタを作成して、アプリケーションを識別するのに役立つポートおよびパターン マッチング情報をシステムに提供することができます。詳細については、「ユーザ定義のアプリケーション プロトコル ディテクタの作成」（P.42-20）を参照してください。

脆弱性を修正するパッチを適用しましたか

ライセンス：FireSIGHT

システムがホストを正しく識別するものの、適用した修正が反映されない場合、ホスト入力機能を使用してパッチ情報をインポートすることができます。パッチ情報をインポートする場合、修正名をデータベースの修正にマッピングする必要があります。詳細については、「サード パーティ製品の修正のマッピング」（P.42-35）を参照してください。

サードパーティの脆弱性を追跡しますか

ライセンス：FireSIGHT

影響の関連付けに使用するサードパーティ システムからの脆弱性情報がある場合、サーバおよびアプリケーション プロトコル用のサードパーティ脆弱性 ID をシスコ データベースの脆弱性 ID にマッピングし、ホスト入力機能を使用して脆弱性をインポートすることができます。ホスト入力機能の使用方法の詳細については、『*FireSIGHT System Host Input API Guide*』を参照してください。サードパーティの脆弱性マッピングの詳細については、「サードパーティの脆弱性のマッピング」（P.42-36）を参照してください。アプリケーション データを FireSIGHT システム ベンダーおよびバージョン定義にマッピングしたとしても、インポートされたサードパーティの脆弱性はクライアントまたは Web アプリケーションの影響評価に使用されないことに注意してください。

ネットワーク マップの強化

ライセンス：FireSIGHT

FireSIGHT システムは、パッシブにトラフィックを分析することによって検出されたデータを使用してネットワーク マップを作成します。また、ホスト入力機能や Nmap スキャナなどのアクティブ ソースを介して追加されたデータも使用します。アプリケーションまたはオペレーティング システムの ID に使用するデータをシステムがどのように決定するかを理解することは、アクティブ入力ソースでシステムのパッシブ検出機能を強化する最善の方法を決定するうえで役立ちます。

詳細については、次のトピックを参照してください。

- 「パッシブ検出について」（P.42-4）
- 「アクティブ検出について」（P.42-5）
- 「現在の ID について」（P.42-5）
- 「ID の競合について」（P.42-7）

パッシブ検出について

ライセンス：FireSIGHT

*パッシブ検出*とは、システムによってパッシブに収集されたトラフィックを分析することによって、ホストのオペレーティング システム、クライアント、およびアプリケーション情報を検出することです。システムは、ネットワーク資産を識別するのに役立つ VDB の情報を使用します。

システムがあるホストのオペレーティング システムを識別できない場合に、類似したオペレーティング システムの特性を持つ他のホストでそのオペレーティング システムを認識できるようにするため、手動でオペレーティング システムを判別し、サーバまたはクライアントのカスタム フィンガープリントを作成できます。

システムは、ホスト オペレーティング システムに関する収集されたすべてのパッシブ フィンガープリントを使用して、*派生フィンガープリント*を作成します。システムは、収集された各フィンガープリントの信頼値と ID 間の裏付けとなるフィンガープリント データの量を使用して、最も可能性の高い ID を計算する式を適用することによって、派生フィンガープリントを作成します。一般的な要素は ID 間で識別されます。

ネットワークでユーザ定義アプリケーション ディテクタを使用する場合、それらのアプリケーションを識別するために必要な情報をシステムに提供するカスタム ディテクタを作成することによって、システムのアプリケーション検出機能を強化できます。また NetFlow は、ネットワーク マップにパッシブに検出されたアプリケーション情報を追加することもできます。

システムは、データを解釈できないため、*不明*として分類されたアプリケーション プロトコルおよびオペレーティング システムのデータを使用しないことに注意してください。管理対象デバイスは ID を防御センターに不明として報告し、その ID データはフィンガープリントを取得するためには使用されません。

アクティブ検出について

ライセンス：FireSIGHT

*アクティブ検出*では、ホストのオペレーティング システムやアプリケーションの情報などアクティブ ソースによって収集されるデータをネットワーク マップに追加します。たとえば、Nmap スキャナを使用して、ネットワーク上の対象ホストをアクティブにスキャンできます。Nmap は、ホストでオペレーティング システムおよびアプリケーションを検出します。

さらに、ホスト入力機能によって、ネットワーク マップに*ホスト入力データ*をアクティブに追加することができます。ホスト入力データには 2 種類のカテゴリがあります。

- FireSIGHT システムのユーザ インターフェイスを使用して、ホストのオペレーティング システムやアプリケーションの ID を変更できます。このインターフェイスを使用して追加したデータは、*ユーザ入力データ*になります。
- コマンド ライン ユーティリティを使用してデータをインポートすることもできます。インポートしたデータは、*ホスト インポート入力データ*になります。

システムは、それぞれのアクティブ ソースに対して 1 個の ID を保持します。たとえば、Nmap スキャン インスタンスを実行すると、以前のスキャンの結果は新しいスキャン結果に置き換えられます。ただし、Nmap スキャンを実行し、それらの結果をクライアントからのデータ（コマンド ラインを使用してインポートした結果）と交換する場合、システムは Nmap の結果の ID とインポート クライアントの ID の両方を保持します。システムは、システム ポリシーで設定された優先順位を使用して、現在の ID として使用するアクティブ ID を判別します。

複数のユーザが入力したとしても、ユーザ入力は 1 ソースと見なされることに注意してください。たとえば、UserA がホスト プロファイルを使用してオペレーティング システムを設定し、UserB がホスト プロファイルを使用してその定義を変更した場合、UserB によって設定された定義が保持され、UserA によって設定された定義は破棄されます。また、ユーザ入力によって、他のアクティブ ソースすべてが上書きされ、存在する場合、現在の ID として使用されることに注意してください。

現在の ID について

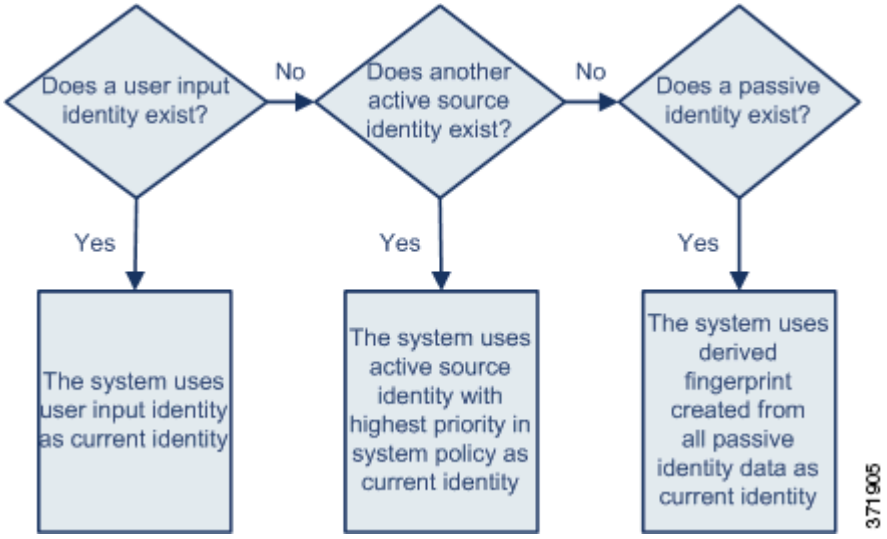
ライセンス：FireSIGHT

ホストのアプリケーションまたはオペレーティング システムの*現在の ID* は、ホストが最も正しい可能性が高いと認識する ID です。

システムは、以下の目的で、オペレーティング システムまたはアプリケーションの現在の ID を使用します。

- 脆弱性のホストへの割り当て
- 影響評価
- オペレーティング システムの識別、ホスト プロファイルの認定、およびコンプライアンスのホワイトリストに対して記述された相関ルールの評価
- ワークフローのホストおよびサーバのテーブル ビューでの表示
- ホスト プロファイルでの表示
- [Discovery Statistics] ページでのオペレーティング システムとアプリケーションの統計の計算

システムは、ソースの優先順位を使用して、アプリケーションまたはオペレーティング システムの現在の ID として使用するアクティブ ID を判別します。



たとえば、ユーザがホストでオペレーティング システムを Windows 2003 Server に設定した場合、Windows 2003 Server が現在の ID になります。そのホストの Windows 2003 Server の脆弱性を狙った攻撃により大きな影響力があると見なされ、ホスト プロファイルのそのホストについてリストされた脆弱性に、Windows 2003 Server の脆弱性が含められます。

データベースは、ホストのオペレーティング システムや特定のアプリケーションに関する複数のソースからの情報を保持する場合があります。

データのソースに最も高いソースの優先順位が付けられている場合に、システムはオペレーティング システムまたはアプリケーションの ID を現在の ID として扱います。使用される可能性のあるソースには、次の優先順位があります。

1.ユーザ

2.スキャナとアプリケーション（ネットワーク検出ポリシーで設定）

3.管理対象デバイス

4.NetFlow

新しい優先度の高いアプリケーション ID は、現在のアプリケーション ID ほど詳細でない場合は、現在の ID を上書きしないことに注意してください。

また、ID の競合が発生した場合、「ID の競合について」（P.42-7）で説明されているように、競合の解決はネットワーク検出ポリシーの設定または手動解決に依存することに注意してください。

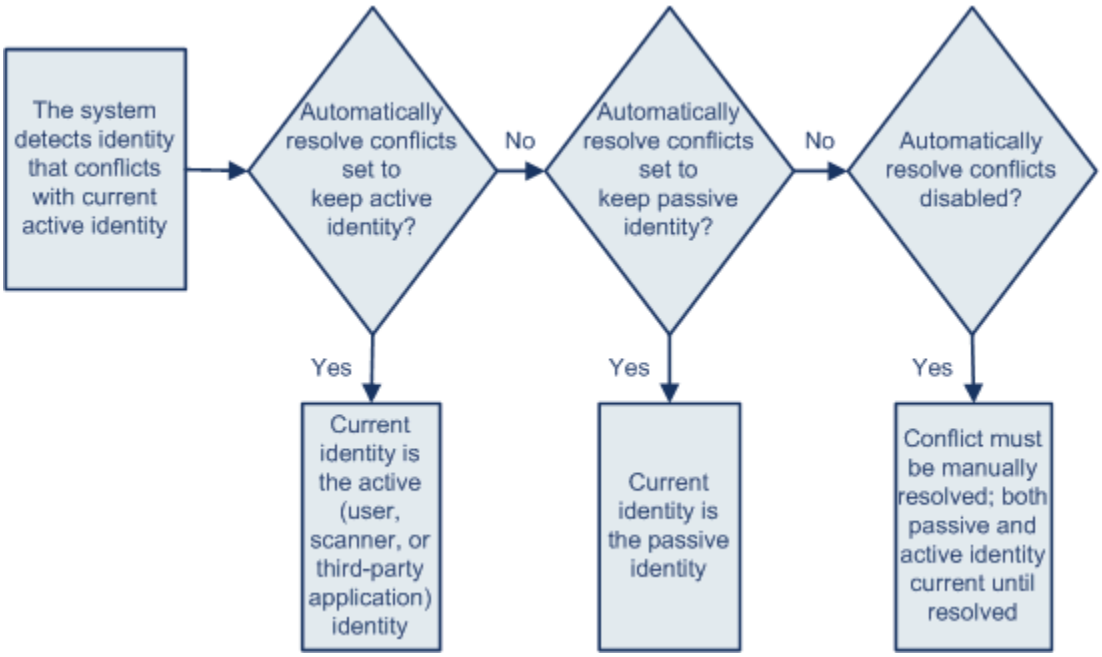
ID の競合について

ライセンス：FireSIGHT

現在のアクティブ ID および以前に報告されたパッシブ ID と競合する新しいパッシブ ID が報告されると、*ID の競合*が発生します。たとえば、オペレーティング システムの以前のパッシブ ID は Windows 2000 と報告され、Windows XP のアクティブ ID が現在の ID になります。次に、システムが Ubuntu Linux 8.04.1 の新しいパッシブ ID を検出します。Windows XP と Ubuntu Linux の ID が競合状態になります。

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 ID に対して ID の競合が存在する場合、システムは現在の ID として競合する両方の ID をリストし、競合が解決されるまで影響評価に両方の ID を使用します。

管理者特権を持つユーザは、パッシブ ID を常に使用するか、またはアクティブ ID を常に使用するかを選択することによって、自動的に ID の競合を解決できます。ID の競合の自動解決を無効にしない限り、ID の競合は常に自動的に解決されます。



管理者特権を持つユーザは、ID の競合が発生した場合に、イベントを生成するようにシステムを設定することもできます。そのユーザは、相関応答として Nmap スキャンを使用する相関ルールで相関ポリシーを設定できます。イベントが発生すると、Nmap はホストをスキャンして、更新されたホストのオペレーティング システムとアプリケーション データを取得します。

カスタム フィンガープリントの使用

ライセンス：FireSIGHT

FireSIGHT システムには、検出された各ホストのオペレーティング システムを識別するためにシステムが使用するオペレーティング システムの*フィンガープリント*が含まれます。しかし、オペレーティング システムに一致するフィンガープリントがないため、システムがホストのオペレーティング システムを識別できない、または誤って識別することがあります。この問題を

解決するために、不明または誤認されたオペレーティング システムに固有のオペレーティング システム特性のパターンを提供する*カスタム フィンガープリント*を作成し、識別用のオペレーティング システムの名前を提供することができます。

システムはオペレーティング システムのフィンガープリントから各ホストの脆弱性リストを取得するため、システムがホストのオペレーティング システムを照合できない場合、ホストの脆弱性を識別することはできません。たとえば、システムが Microsoft Windows を実行するホストを検出した場合、そのシステムには保存された Microsoft Windows の脆弱性リストが存在します。このリストは、検出した Windows オペレーティング システムに基づいて、そのホストのホスト プロファイルに追加されます。

たとえば、ネットワーク上に Microsoft Windows の新しいベータ バージョンを実行する複数のデバイスがある場合、システムはそのオペレーティング システムを識別することができません。そのため、脆弱性をそれらのホストにマッピングすることはできません。しかし、システムに Microsoft Windows に関する脆弱性のリストがあるならば、同じオペレーティング システムを実行する他のホストを識別するために使用できるカスタム フィンガープリントをいずれか 1 台のホストに対して作成できます。フィンガープリントに Microsoft Windows の脆弱性リストのマッピングを含め、フィンガープリントに一致する各ホストとそのリストを関連付けることができます。

カスタム フィンガープリントを作成するときは、オペレーティング システム情報のカスタマイズした表示を追加できます。また、システムがフィンガープリントの脆弱性リストのモデルとして使用する必要のあるオペレーティング システムのベンダー、製品名、製品バージョンを選択できます。防御センターは、同じオペレーティング システムを実行するすべてのホストに関するそのフィンガープリントに関連付けられた脆弱性のセットをリストします。ユーザが作成したカスタム フィンガープリントに脆弱性マッピングが 1 つも存在しない場合、システムはフィンガープリントを使用して、フィンガープリントで提供するカスタム オペレーティング システムの情報を割り当てます。すでに検出され、ネットワーク マップに現在存在しているホストからの新しいトラフィックが確認されると、システムはそのホストを新しいフィンガープリントの情報で更新します。また、最初に検出されたときに、新しいフィンガープリントを使用して、すべての新しいホストをそのオペレーティング システムで識別します。

ホストのフィンガープリントを作成する前に、ホストが正しく識別されない理由を特定して、カスタム フィンガープリントが実行可能なソリューションであるかどうかを判断する必要があります。詳細については、「検出戦略の評価」（P.42-2）を参照してください。

以下の 2 種類のフィンガープリントを作成できます。

- クライアントのフィンガープリント。ネットワーク上の別のホストで実行する TCP アプリケーションに接続されている場合、ホストが送信する SYN パケットに基づいてオペレーティング システムを識別します。

  ホストのクライアント フィンガープリントを取得する方法については、「クライアントのフィンガープリントの作成」（P.42-9）を参照してください。

- サーバのフィンガープリント。実行されている TCP アプリケーションへの着信接続に応答するためにホストが使用する SYN-ACK パケットに基づいてオペレーティング システムを識別します。

  ホストのサーバ フィンガープリントを取得する方法については、「サーバのフィンガープリントの作成」（P.42-12）を参照してください。

フィンガープリントを作成した後、システムがそれらをホストに関連付けるには、その前に、それらのフィンガープリントをアクティブにする必要があります。詳細については、「フィンガープリントの管理」（P.42-15）を参照してください。

注　クライアントとサーバの両方のフィンガープリントが同じホストに一致する場合、クライアントのフィンガープリントが使用されます。

クライアントのフィンガープリントの作成

ライセンス：FireSIGHT

クライアントのフィンガープリントは、ネットワーク上の別のホストで実行する TCP アプリケーションに接続されている場合、ホストが送信する SYN パケットに基づいてオペレーティング システムを識別します。

防御センターが監視対象ホストと直接通信することがない場合は、クライアントのフィンガープリントのプロパティを指定するときに、防御センターによって管理され、フィンガープリントを作成するホストに最も近いデバイスを指定することができます。

フィンガープリント作成プロセスを開始する前に、フィンガープリントを作成するホストに関する次の情報を取得します。

- ホストとフィンガープリントを取得するために使用する防御センターまたはデバイスの間のネットワーク ホップの数。（シスコでは、ホストが接続されている同じサブネットに防御センターまたはデバイスを直接接続することを強く推奨します。）
- ホストが存在するネットワークに接続されているネットワーク インターフェイス（防御センターまたはデバイス上）。
- ホストの実際のオペレーティング システム ベンダー、製品、バージョン。
- クライアント トラフィックを生成するためのホストへのアクセス。

ホストのクライアント フィンガープリントを取得する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] を選択し、[Custom Operating Systems] をクリックします。

[Custom Fingerprint] ページが表示されます。

ステップ 2　[Create Custom Fingerprint] をクリックします。

[Create Custom Fingerprint] ページが表示されます。

ステップ 3　[Device] ドロップダウン リストから、フィンガープリントを収集するために使用する防御センターまたはデバイスを選択します。

ステップ 4　[Fingerprint Name] フィールドに、フィンガープリントの識別名を入力します。

ステップ 5　[Fingerprint Description] フィールドに、フィンガープリントの説明を入力します。

ステップ 6　[Fingerprint Type] リストから、[Client] を選択します。

ステップ 7　[Target IP Address] フィールドで、フィンガープリントを作成するホストの IP アドレスを入力します。フィンガープリントは、ホストに他の IP アドレスが存在していても、ユーザが指定したホスト IP アドレスから送受信されるトラフィックのみに基づくことに注意してください。

注意　FireSIGHT システムのバージョン 5.2 以降を実行するアプライアンスでのみ IPv6 フィンガープリントをキャプチャできます。これらのアプライアンスでは、IPv6 の機能を有効にしておく必要があります。管理対象デバイスおよび防御センターでの IPv6 の有効化の詳細については、「ネットワーク設定の構成」（P.51-9）を参照してください。

ステップ 8　[Target Distance] フィールドで、ホストとステップ 3 で選択したデバイスの間のネットワーク ホップ数を入力します。

注意　これは、ホストへの実際の物理ネットワーク ホップ数である必要があります。システムによって検出されるホップ数と同じになる場合も、同じにならない場合もあります。

ステップ 9　[Interface] リストから、ホストが存在するネットワーク セグメントに接続されているネットワーク インターフェイスを選択します。

注意　シスコでは、いくつかの理由でフィンガープリントの作成に管理対象デバイスのセンシング インターフェイスを使用**しない**ことを推奨します。まず、フィンガープリントは、センシング インターフェイスが SPAN ポート上にあると機能しません。また、デバイスでセンシング インターフェイスを使用する場合、デバイスはフィンガープリントを収集している間、ネットワークの監視を停止します。ただし、フィンガープリントの収集を実行するために、管理インターフェイスまたはその他の使用可能なネットワーク インターフェイスを使用できます。どのインターフェイスがデバイスのセンシング インターフェイスであるかがわからない場合は、フィンガープリントの作成に使用している特定のモデルの*インストレーション ガイド*を参照してください。

ステップ 10　フィンガープリントを作成したホストのホスト プロファイルのカスタム情報を表示する場合（またはフィンガープリントを作成するホストが [OS Vulnerability Mappings] セクションに存在しない場合）、[Custom OS Display] セクションの [Use Custom OS Display] を選択し、以下のホスト プロファイルに表示する値を指定します。

- [Vendor String] フィールドに、オペレーティング システムのベンダー名を入力します。たとえば、Microsoft Windows のベンダーは「Microsoft」になります。
- [Product String] フィールドに、オペレーティング システムの製品名を入力します。たとえば、Microsoft Windows 2000 の製品名は「Windows」になります。
- [Version String] フィールドに、オペレーティング システムのバージョン番号を入力します。たとえば、Microsoft Windows 2000 のバージョン番号は「2000」になります。

ステップ 11　[OS Vulnerability Mappings] セクションで、脆弱性マッピングに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、カスタム フィンガープリントで Redhat Linux 9 の脆弱性リストを一致するホストに割り当てる場合、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、メジャー バージョンとして [9] を選択します。

ヒント　フィンガープリントを作成するとき、フィンガープリントに単一の脆弱性マッピングを割り当てます。フィンガープリントを作成してアクティブにした後、オペレーティング システムのその他のバージョンに関する別個の脆弱性マッピングを追加できます。詳細については、「アクティブなフィンガープリントの編集」（P.42-18）を参照してください。

フィンガープリントを使用して一致するホストの脆弱性を識別する場合、またはオペレーティング システムのカスタム表示情報を割り当てない場合、このセクションでベンダーと製品名を指定する必要があります。オペレーティング システムのすべてのバージョンの脆弱性をマッピングするには、ベンダーおよび製品名のみを指定します。たとえば、Palm OS のすべてのバージョンを追加するには、[Vendor] リストから [PalmSource, Inc.]、[Product] リストから [Palm OS] を選択し、その他のすべてのリストはデフォルトの設定のままにします。

注　[Major Version]、[Minor Version]、[Revision Version]、[Build]、[Patch]、および [Extension] ドロップダウン リストのオプションの中には、選択したオペレーティング システムに該当しないものもあります。また、フィンガープリントを作成するオペレーティング システムに一致するリストに表示される定義がない場合は、それらの値を空のままにすることができます。フィンガープリントで OS の脆弱性マッピングを作成しない場合、システムはそのフィンガープリントを使用して、脆弱性リストをフィンガープリントによって識別されるホストに割り当てることはできないことに注意してください。

ステップ 12　[Create] をクリックします。

[Custom Fingerprint] ステータス ページが再表示されます。当該のホストからデータを受信するまで、ステータス ページは 10 秒ごとに更新されます。

ヒント　[Create] をクリックすると、ステータスには [New] が一時的に表示され、すぐに [Pending] に切り替わります。このステータスは、トラフィックがフィンガープリントで確認されるまで継続します。確認されたら、ステータスは [Ready] に切り替わります。

ステップ 13　ターゲット IP アドレスとして指定した IP アドレスを使用して、フィンガープリントを作成しようとしているホストにアクセスし、アプライアンスへの TCP 接続を開始します。

たとえば、フィンガープリントを作成しようとしているホストから防御センターの Web インターフェイスに、または SSH でホストから防御センターにアクセスします。SSH を使用する場合、次のコマンドを使用します。

```
ssh -b localIPv6address DCmanagementIPv6address
```

ここで、*localIPv6address* は、現在ホストに割り当てられているステップ 7 で指定した IPv6 アドレスです。*DCmanagementIPv6address* は、防御センターの管理 IPv6 アドレスです。

これで、[Custom Fingerprint] ページが [Ready] ステータスでリロードされるはずです。

注　正確なフィンガープリントを作成するためには、トラフィックがフィンガープリントを収集するアプライアンスで認識される**必要**があります。スイッチを介して接続している場合は、アプライアンス以外のシステムへのトラフィックはシステムによって認識されない場合があります。

ステップ 14　フィンガープリントが作成された後、防御センターがそのフィンガープリントを使用してホストを識別するには、それをアクティブにする必要があります。詳細については、「フィンガープリントの管理」（P.42-15）を参照してください。

サーバのフィンガープリントの作成

ライセンス：FireSIGHT

サーバのフィンガープリントは、実行されている TCP アプリケーションへの着信接続に応答するためにホストが使用する SYN-ACK パケットに基づいてオペレーティング システムを識別します。開始する前に、フィンガープリントを作成するホストに関する次の情報を取得します。

- ホストとフィンガープリントを取得するために使用するアプライアンスの間のネットワーク ホップの数。シスコでは、ホストが接続されている同じサブネットにアプライアンスの使用されていないインターフェイスを直接接続することを強く推奨します。
- ホストが存在するネットワークに接続されているネットワーク インターフェイス（アプライアンス上）。
- ホストの実際のオペレーティング システム ベンダー、製品、バージョン。
- 現在使用されておらず、ホストが存在するネットワーク上で許可されている IP アドレス。

ヒント　防御センターが監視対象ホストと直接通信することがない場合は、サーバのフィンガープリントのプロパティを指定するときに、フィンガープリントを作成するホストに最も近い管理対象デバイスを指定することができます。

ホストのサーバ フィンガープリントを取得する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] を選択し、[Custom Operating Systems] をクリックします。

[Custom Fingerprint] ページが表示されます。

ステップ 2　[Create Custom Fingerprint] をクリックします。

[Create Custom Fingerprint] ページが表示されます。

ステップ 3　[Device] リストから、フィンガープリントを収集するために使用する防御センターまたは管理対象デバイスを選択します。

ステップ 4　[Fingerprint Name] フィールドに、フィンガープリントの識別名を入力します。

ステップ 5　[Fingerprint Description] フィールドに、フィンガープリントの説明を入力します。

ステップ 6　[Fingerprint Type] リストから、[Server] を選択します。

サーバのフィンガープリントのオプションが表示されます。

ステップ 7　[Target IP Address] フィールドで、フィンガープリントを作成するホストの IP アドレスを入力します。フィンガープリントは、ホストに他の IP アドレスが存在していても、ユーザが指定したホスト IP アドレスから送受信されるトラフィックのみに基づくことに注意してください。

注意　FireSIGHT システムのバージョン 5.2 以降を実行するアプライアンスでのみ IPv6 フィンガープリントをキャプチャできます。

ステップ 8　[Target Distance] フィールドで、ホストとステップ 3 で選択したデバイスの間のネットワーク ホップ数を入力します。

注意　これは、ホストへの実際の物理ネットワーク ホップ数である必要があります。システムによって検出されるホップ数と同じになる場合も、同じにならない場合もあります。

ステップ 9　[Interface] リストから、ホストが存在するネットワーク セグメントに接続されているネットワーク インターフェイスを選択します。

注意　シスコでは、いくつかの理由でフィンガープリントの作成に管理対象デバイスのセンシング インターフェイスを使用**しない**ことを推奨します。まず、フィンガープリントは、センシング インターフェイスが SPAN ポート上にあると機能しません。また、デバイスでセンシング インターフェイスを使用する場合、デバイスはフィンガープリントを収集している間、ネットワークの監視を停止します。ただし、フィンガープリントの収集を実行するために、管理インターフェイスまたはその他の使用可能なネットワーク インターフェイスを使用できます。どのインターフェイスがデバイスのセンシング インターフェイスであるかがわからない場合は、フィンガープリントの作成に使用している特定のモデルの*インストレーション ガイド*を参照してください。

ステップ 10　[Get Active Ports] をクリックします。

システムがホストでオープン ポートを検出した場合は、ドロップダウン リストに表示されます。

ステップ 11　[Server Port] フィールドに、フィンガープリントを収集するように選択したデバイスが通信を開始するポートを入力します。または、[Get Active Ports] ドロップダウン リストからポートを選択します。

ホストでオープンしていると判明しているすべてのサーバ ポートを使用できます（たとえば、ホストで Web サーバを実行している場合、80）。

ステップ 12　[Target IP Address] フィールドで、ホストとの通信を試行するために使用する IP アドレスを入力します。

ネットワークでの使用が許可されているものの、現在使用されていない送信元 IP アドレス（たとえば、現在使用されていない DHCP プール アドレス）を使用する必要があります。これにより、フィンガープリントを作成している間に、別のホストをオフラインで一時的にノックすることを防ぎます。

また、フィンガープリントを作成している間、ネットワーク検出ポリシーでのモニタリングからその IP アドレスを除外する必要があります。そうしないと、ネットワーク マップおよびディスカバリ イベント ビューに、その IP アドレスによって表されるホストに関する不正確な情報が混在することになります。詳細については、「検出データ収集について」（P.35-2）を参照してください。

ステップ 13　[Source Subnet Mask] フィールドでは、ユーザが使用している IP アドレスのサブネット マスクを入力します。

ステップ 14　[Source Gateway] フィールドが表示されたら、ホストへのルートを確立するために使用するデフォルトのゲートウェイ IP アドレスを入力します。

ターゲットの距離（ホップ数）が 1 以上であり、管理インターフェイス以外のインターフェイスを使用してホストが存在するネットワークに接続している場合に、[Source Gateway] フィールドが表示されます。

ステップ 15　フィンガープリントを作成したホストのホスト プロファイルのカスタム情報を表示する場合、または使用するフィンガープリントの名前が [OS Definition] セクションに存在しない場合、[Custom OS Display] セクションの [Use Custom OS Display] を選択します。

以下のように、ホスト プロファイルで表示する値を入力します。

- [Vendor String] フィールドに、オペレーティング システムのベンダー名を入力します。たとえば、Microsoft Windows のベンダーは「Microsoft」になります。
- [Product String] フィールドに、オペレーティング システムの製品名を入力します。たとえば、Microsoft Windows 2000 の製品名は「Windows」になります。
- [Version String] フィールドに、オペレーティング システムのバージョン番号を入力します。たとえば、Microsoft Windows 2000 のバージョン番号は「2000」になります。

ステップ 16　[OS Vulnerability Mappings] セクションで、脆弱性マッピングに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、カスタム フィンガープリントで Redhat Linux 9 の脆弱性リストを一致するホストに割り当てる場合、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、バージョンとして [9] を選択します。

ヒント　フィンガープリントを作成するとき、フィンガープリントに単一の脆弱性マッピングを割り当てます。フィンガープリントを作成してアクティブにした後、オペレーティング システムのその他のバージョンに関する別個の脆弱性マッピングを追加できます。詳細については、「アクティブなフィンガープリントの編集」（P.42-18）を参照してください。

フィンガープリントを使用して一致するホストの脆弱性を識別する場合、またはオペレーティング システムのカスタム表示情報を割り当てない場合、このセクションでベンダーと製品名を指定する必要があります。オペレーティング システムのすべてのバージョンの脆弱性をマッピングするには、ベンダーおよび製品名のみを指定します。たとえば、Palm OS のすべてのバージョンを追加するには、[Vendor] リストから [PalmSource, Inc.]、[Product] リストから [Palm OS] を選択し、その他のすべてのリストはデフォルトの設定のままにします。

注　[Major Version]、[Minor Version]、[Revision Version]、[Build]、[Patch]、および [Extension] ドロップダウン リストのオプションの中には、選択したオペレーティング システムに該当しないものもあります。また、フィンガープリントを作成するオペレーティング システムに一致するリストに表示される定義がない場合は、それらの値を空のままにすることができます。フィンガープリントで OS の脆弱性マッピングを作成しない場合、システムはそのフィンガープリントを使用して、脆弱性リストをフィンガープリントによって識別されるホストに割り当てることはできないことに注意してください。

ステップ 17　[Create] をクリックします。

ステップ 18　[Custom Fingerprint] ステータス ページが表示されます。このページは 10 秒ごとにリロードされ、[Ready] ステータスでリロードされる必要があります。

注　ターゲット システムがフィンガープリント プロセス時に応答を停止した場合、ステータスにはメッセージ「ERROR: No Response」が示されます。このメッセージが表示された場合は、フィンガープリントを再度送信します。3 ～ 5 分間（時間はターゲット システムによって異なる場合があります）待機して、編集アイコン（）をクリックし、[Custom Fingerprint] ページにアクセスしてから [Create] をクリックします。

ステップ 19　フィンガープリントが作成されたら、それをアクティブにし、オプションで脆弱性マッピングを追加します。詳細については、「フィンガープリントの管理」（P.42-15）を参照してください。

フィンガープリントの管理

ライセンス：FireSIGHT

カスタム フィンガープリントのアクティブ化、非アクティブ化、削除、表示、および編集を実行できます。フィンガープリントを作成するとき、フィンガープリントに単一の脆弱性マッピングを割り当てます。フィンガープリントの作成の詳細については、「クライアントのフィンガープリントの作成」（P.42-9）および「サーバのフィンガープリントの作成」（P.42-12）を参照してください。フィンガープリントを作成してアクティブにした後、フィンガープリントを編集して変更を加えたり、脆弱性マッピングを追加したりできます。

[Custom Fingerprints] ページにアクセスする方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] を選択し、[Custom Operating Systems] をクリックします。

[Custom Fingerprint] ページが表示されます。

システムがフィンガープリントを作成するデータを待機している場合、フィンガープリントが作成されるまで 10 秒ごとに自動的に更新されます。

詳細については、次の項を参照してください。

- 「フィンガープリントのアクティブ化」（P.42-15）
- 「フィンガープリントの非アクティブ化」（P.42-16）
- 「フィンガープリントの削除」（P.42-16）
- 「フィンガープリントの編集」（P.42-17）

フィンガープリントのアクティブ化

ライセンス：FireSIGHT

カスタム フィンガープリントを作成した後、システムがそのフィンガープリントを使用してホストを識別するには、その前に、それをアクティブにする必要があります。新しいフィンガープリントがアクティブにされた後は、以前に検出したホストを再識別し、新しいホストを検出するために使用されます。

フィンガープリントをアクティブにする方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] を選択し、[Custom Operating Systems] をクリックします。

[Custom Fingerprint] ページが表示されます。

ステップ 2　アクティブにするフィンガープリントの横にあるスライダをクリックします。

注　アクティブ化オプションは、作成したフィンガープリントが有効である場合に限り使用できます。スライダが使用できない場合、フィンガープリントを再作成してください。

防御センターは、フィンガープリントをアクティブにし、すべての管理対象デバイスに伝播します。フィンガープリントの名前の横にあるアイコンは変更され、そのフィンガープリントがアクティブであることが示されます。

フィンガープリントの非アクティブ化

ライセンス：FireSIGHT

フィンガープリントの使用を停止する場合は、それを非アクティブにすることができます。フィンガープリントを非アクティブにすると、フィンガープリントは使用できなくなりますが、システム上で維持できます。フィンガープリントを非アクティブにすると、オペレーティング システムは、フィンガープリントを使用しているホストに対して不明としてマークされます。ホストが再度検出され、別のアクティブなフィンガープリントに一致すると、ホストはそのアクティブなフィンガープリントによって識別されます。

フィンガープリントを削除すると、システムから完全に削除されます。フィンガープリントを非アクティブにした後に削除できます。

アクティブなフィンガープリントを非アクティブにする方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] を選択し、[Custom Operating Systems] をクリックします。

[Custom Fingerprint] ページが表示されます。

ステップ 2　非アクティブにするアクティブなフィンガープリントの横にあるスライダをクリックします。

防御センターは、フィンガープリントを非アクティブにし、すべての管理対象デバイスにその非アクティブ化を伝播します。

フィンガープリントの削除

ライセンス：FireSIGHT

フィンガープリントを使用しなくなった場合、システムから削除できます。フィンガープリントを削除する前に、そのフィンガープリントを非アクティブにする必要があることに注意してください。

フィンガープリントを削除する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] を選択し、[Custom Operating Systems] をクリックします。

[Custom Fingerprint] ページが表示されます。

ステップ 2　削除するフィンガープリントがアクティブである場合、それぞれの横にあるスライダ アイコンをクリックして、そのフィンガープリントを非アクティブにします。

ステップ 3　削除するフィンガープリントの横にある削除アイコン（ ）をクリックします。

ステップ 4　[OK] をクリックして、フィンガープリントを削除することを確認します。

フィンガープリントが削除されます。

フィンガープリントの編集

ライセンス：FireSIGHT

フィンガープリントを作成したら、それを表示または編集できます。フィンガープリントを変更して再送信したり、その他の脆弱性マッピングを追加したりすることができます。アクティブまたは非アクティブであるかに関わらずフィンガープリントを変更できますが、フィンガープリントの状態に応じて、変更できる事柄は異なります。

フィンガープリントが*非アクティブ*である場合は、フィンガープリントのすべての要素を変更し、それらを防御センターに再送信できます。これには、フィンガープリントのタイプ、ターゲットの IP アドレスとポート、脆弱性マッピングなど、フィンガープリントの作成時に指定したすべてのプロパティが含まれます。非アクティブのフィンガープリントを編集および送信すると、システムに再送信されます。また、それがクライアントのフィンガープリントである場合、アクティブにする前に、アプライアンスにトラフィックを再送信する必要があります。非アクティブのフィンガープリントに対して選択できる脆弱性マッピングは 1 つだけであることに注意してください。フィンガープリントをアクティブにした後、追加のオペレーティング システムおよびバージョンを脆弱性リストにマッピングすることができます。

フィンガープリントが *アクティブ*である場合、フィンガープリントの名前、説明、オペレーティング システムのカスタム表示の変更、および追加の脆弱性のフィンガープリントへのマッピングを行えます。

詳細については、次の項を参照してください。

- 「非アクティブなフィンガープリントの編集」（P.42-17）
- 「アクティブなフィンガープリントの編集」（P.42-18）

非アクティブなフィンガープリントの編集

ライセンス：FireSIGHT

フィンガープリントが非アクティブである場合は、フィンガープリントのプロパティを変更し、それらをシステムに再送信できます。これには、使用するフィンガープリントのタイプ、フィンガープリントのターゲット システムなどの変更が含まれます。

非アクティブなフィンガープリントを編集する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] を選択し、[Custom Operating Systems] をクリックします。

[Custom Fingerprint] ページが表示されます。

ステップ 2　編集するフィンガープリントの横にある編集アイコン（  ）をクリックします。

[Edit Custom Fingerprint] ページが表示されます。

ステップ 3　必要に応じてフィンガープリントを変更します。

- クライアントのフィンガープリントを変更する場合、設定できるオプションの詳細については、「クライアントのフィンガープリントの作成」（P.42-9）を参照してください。
- サーバのフィンガープリントを変更する場合、設定できるオプションの詳細については、「サーバのフィンガープリントの作成」（P.42-12）を参照してください。

ステップ 4　[Save] をクリックして、フィンガープリントを再送信します。

注　クライアントのフィンガープリントを変更した場合は、ホストからフィンガープリントを収集しているアプライアンスにトラフィックを必ず送信してください。

アクティブなフィンガープリントの編集

ライセンス：FireSIGHT

フィンガープリントがアクティブな場合、その名前、説明、および表示ラベルを変更できます。また、脆弱性マッピングの追加や削除など、脆弱性マッピングを管理することができます。

アクティブなフィンガープリントを編集する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Network Discovery] を選択し、[Custom Operating Systems] をクリックします。

[Custom Fingerprint] ページが表示されます。

ステップ 2　編集するフィンガープリントの横にある編集アイコン（  ）をクリックします。

[Edit Custom Fingerprint Product Mappings] ページが表示されます。

ステップ 3　必要に応じて、フィンガープリントの名前、説明、およびカスタム OS 表示を変更します。

ステップ 4　脆弱性マッピングを削除する場合は、ページの [Pre-Defined OS Product Maps] セクションのマッピングの横にある [Delete] をクリックします。

ステップ 5　脆弱性マッピングにその他のオペレーティング システムを追加する場合は、[Product] を選択し（該当する場合は [Major Version]、[Minor Version]、[Revision Version]、[Build]、[Patch]、および [Extension] も選択します）、[Add OS Definition] をクリックします。

脆弱性マッピングが、[Pre-Defined OS Product Maps] リストに追加されます。

ステップ 6　[Save] をクリックして変更を保存します。

アプリケーション ディテクタの使用

ライセンス：FireSIGHT

FireSIGHT システムが IP トラフィックを分析する場合、ネットワークで一般的に使用されるアプリケーションを識別するためにディテクタを使用します。[Detectors] ページ（[Policies] > [Application Detectors]）を使用して、FireSIGHT システムの検出機能をカスタマイズします。

このページには、各ディテクタに関する次のような情報が表示されます。

- ディテクタの名前
- ディテクタが検査するトラフィックのプロトコル（TCP、UDP、またはその両方）
- ディテクタのタイプがアプリケーション プロトコル、クライアント、Web アプリケーション、または内部ディテクタのいずれであるか
- ポートベースのアプリケーション ディテクタの場合、アプリケーション トラフィックによって使用されるポート
- 検出されたアプリケーションに関する詳細（ディテクタによって検出されたアプリケーションに関連付けられた名前、説明、リスク、ビジネスとの関連性、タグ、およびカテゴリ）
- ディテクタの状態（アクティブまたは非アクティブ）

システムは、アプリケーション トラフィックを分析するために、アクティブなディテクタのみを使用します。

リストされたディテクタに異なるプロパティが存在することがあります。たとえば、一部のディテクタの設定を表示できますが、その他のディテクタの設定は表示できません。同様に、一部のディテクタを削除できますが、その他のディテクタは削除できません。これは、次のセクションで説明しているように、シスコが提供するディテクタに複数の異なるタイプが存在するためです。

シスコが提供する内部ディテクタ

*内部ディテクタ*は、FireSIGHT システムへの更新によってのみ提供されるアプリケーション ディテクタです。内部ディテクタは、そのディテクタに応じて、クライアント、Web アプリケーション、またはアプリケーション プロトコルのトラフィックを検出します。しかし、それらが組み込みディテクタであり、非アクティブにすることができないという理由で、他のタイプのいずれでもなく、内部ディテクタとして分類されます。

内部ディテクタは常にアクティブです。それらを非アクティブにすることも、削除することも、または別の方法で設定することもできません。内部ディテクタの例には、組み込み Amazon ディテクタや組み込み AppleTalk ディテクタがあります。

シスコが提供するクライアント ディテクタ

シスコが提供する *クライアント ディテクタ*は、クライアント トラフィックを検出し、VDB アップデートを介して提供されますが、FireSIGHT システムへの更新によっても提供されることがあります。これらのディテクタは、インポート可能なディテクタとしてシスコ プロフェッショナル サービスによって提供されることもあります。

組織の必要に応じてクライアント ディテクタをアクティブまたは非アクティブにできます。VDB アップデートも、クライアント ディテクタをアクティブまたは非アクティブにすることがあります。インポートする場合のみ、クライアント ディテクタをエクスポートできます。

クライアント ディテクタの例には、Google Earth ディテクタや Immunet ディテクタがあります。

シスコが提供する Web アプリケーション ディテクタ

シスコが提供する *Web アプリケーション ディテクタ*は、HTTP トラフィックのペイロードで Web アプリケーションを検出し、VDB アップデートを介して提供されますが、FireSIGHT システムへの更新によっても提供されることがあります。

組織の必要に応じて Web アプリケーション ディテクタをアクティブまたは非アクティブにできます。VDB アップデートは、Web アプリケーション ディテクタをアクティブまたは非アクティブにすることがあります。Web アプリケーション ディテクタの例には、Blackboard ディテクタや LiveJournal ディテクタがあります。

シスコが提供するアプリケーション プロトコル（ポート）ディテクタ

*ポートベースの アプリケーション プロトコル ディテクタ*は、シスコによって提供され、既知のポートのネットワーク トラフィックの検出に基づきます。これらのディテクタは、VDB アップデートを介して提供されますが、FireSIGHT システムへの更新、またはインポート可能なディテクタとしてシスコ プロフェッショナル サービスによっても提供されることがあります。

組織の必要に応じてアプリケーション プロトコル ディテクタをアクティブまたは非アクティブにできます。カスタム ディテクタの基礎として使用するためにディテクタ定義を表示することもできます。VDB アップデートによって、アプリケーション プロトコル ディテクタがアクティブまたは非アクティブにされることがあります。

ポート ディテクタの例には、chargen ディテクタや finger ディテクタがあります。

シスコが提供するアプリケーション プロトコル（FireSIGHT）ディテクタ

FireSIGHTベースのアプリケーション プロトコル ディテクタは、シスコによって提供され、FireSIGHT アプリケーション フィンガープリントを使用したネットワーク トラフィックの検出に基づきます。これらのディテクタは、VDB アップデートを介して提供されますが、FireSIGHT システムへの更新によっても提供されることがあります。

組織の必要に応じてアプリケーション プロトコル ディテクタをアクティブまたは非アクティブにできます。VDB アップデートによって、シスコが提供するアプリケーション プロトコル ディテクタがアクティブまたは非アクティブにされることがあります。FireSIGHTベースのアプリケーション プロトコル ディテクタの例には、Jabber ディテクタや Steam ディテクタがあります。

アプリケーション プロトコル（パターン）ディテクタ

*パターンベースのアプリケーション ディテクタ*は、ネットワーク トラフィックからのパケットにおけるパターンの検出に基づきます。これらのディテクタは、インポート可能なディテクタとしてシスコ プロフェッショナル サービスによって提供されることも、ユーザが作成することもできます。これにより、FireSIGHT システム全体を更新せずに、新しいパターンベースのディテクタを用いてシステムの検出機能を強化することができます。

組織の必要に応じてアプリケーション プロトコル ディテクタをアクティブまたは非アクティブにできます。

インポートしたディテクタやユーザ定義のディテクタを完全に制御できます。つまり、これらのディテクタのアクティブ化、非アクティブ化、編集、インポート、エクスポート、および削除を実行できます。パターンベースのディテクタの例には、カスタム アプリケーションのトラフィックを検出するためにパケット 見出しのパターンを使用するユーザ定義のディテクタがあります。

ディテクタ リストは、FireSIGHT システムのバージョン、インストールした VDB、およびインポートまたは作成した個々のディテクタに応じて異なる可能性があることに注意してください。各 FireSIGHT システムの更新プログラムのリリース ノートや更新されたディテクタの情報に関する各 VDB アップデートのアドバイザリを注意深く読んでください。

詳細については、以下を参照してください。

- 「アプリケーション検出について」（P.35-12）
- 「ユーザ定義のアプリケーション プロトコル ディテクタの作成」（P.42-20）
- 「ディテクタの管理」（P.42-26）

ユーザ定義のアプリケーション プロトコル ディテクタの作成

ライセンス：FireSIGHT

ネットワークのカスタム アプリケーションを使用する場合、これらのアプリケーションを識別するために必要な情報をシステムに提供するユーザ定義のアプリケーション プロトコル ディテクタを作成できます。アプリケーション トラフィックによって使用されるポート、トラフィック内のパターン、またはポートとパターンの両方に基づいて、アプリケーション プロトコルの検出を実行できます。

たとえば、ポート 1180 を使用するカスタム アプリケーション プロトコルのトラフィックが予想される場合は、そのポートのトラフィックを検出するアプリケーション プロトコル ディテクタを作成できます。別の例として、アプリケーション プロトコルのトラフィックを格納するすべてのパケットの見出しに `ApplicationName` の文字列が含まれることを把握している場合、照合するパターンとして `ApplicationName` の ASCII 文字列を登録するディテクタを作成できます。

クライアントまたは Web アプリケーションではなく、アプリケーション プロトコルのユーザ定義アプリケーション ディテクタのみを作成できます。アプリケーション検出が発生するためには、クライアント セッションにサーバからの応答が含まれている必要があることに注意してください。

注意　新しいアプリケーション ディテクタを作成してアクティブにすると、管理対象デバイス上のトラフィック フローと処理で、短時間の一時停止が発生する場合があります。これは、いくつかのパケットが検査されずに通過する原因となる可能性があります。

ユーザ定義のアプリケーション プロトコル ディテクタでは、ポートまたはパターンのいずれかのマッチングを使用する必要があります。つまり、既存のディテクタに基づくディテクタを作成する場合であっても、いずれも使用しないディテクタは作成できません。これら両方の基準を使用するディテクタを作成することもできます。この場合、そのアプリケーション プロトコルのトラフィックを正しく識別する可能性が高くなります。

ヒント　すでに別の防御センターにディテクタを作成している場合、そのディテクタをエクスポートして、この防御センターにインポートすることができます。その後、必要に応じてインポートしたディテクタを編集できます。ユーザ定義のディテクタおよびシスコ プロフェッショナル サービスが提供するディテクタをエクスポートおよびインポートすることができます。ただし、シスコが提供するその他の種類のディテクタをエクスポートおよびインポートすることは**できません**。詳細については、「設定のインポートおよびエクスポート」（P.A-1）を参照してください。

ユーザ定義のアプリケーション プロトコル ディテクタを作成する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Application Detectors] を選択します。

[Detectors] ページが表示されます。

ステップ 2　[Create Detector] をクリックします。

[Create Detector] ページが表示されます。

ステップ 3　ディテクタの名前や説明など、基本的なディテクタの情報を指定します。

「基本的なアプリケーション プロトコル ディテクタ情報の提供」（P.42-22）を参照してください。

ステップ 4　オプションで、ディテクタのユーザ定義のアプリケーションを作成します。

「ユーザ定義のアプリケーションの作成」（P.42-23）を参照してください。

ステップ 5　ディテクタが検査する必要のあるトラフィックのプロトコルやトラフィックが使用するポートなど検出基準を指定します。

「アプリケーション プロトコル ディテクタの検出基準の指定」（P.42-23）を参照してください。

ステップ 6　オプションで、そのアプリケーション プロトコルのトラフィックで発生する 1 つ以上のパターンに一致するかどうかトラフィックを検査するようにディテクタを設定します。

「アプリケーション プロトコル ディテクタへの検出パターンの追加」（P.42-24）を参照してください。

ステップ 7　オプションで、1 つ以上の PCAP ファイルの内容に対して新しいディテクタをテストします。

「パケット キャプチャに対するアプリケーション プロトコル ディテクタのテスト」（P.42-25）を参照してください。

ステップ 8　[Save] をクリックします。

アプリケーション プロトコル ディテクタが保存されます。

注　アプリケーション プロトコルのトラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタをアクティブにする必要があります。詳細については、「ディテクタのアクティブ化と非アクティブ化」（P.42-30）を参照してください。アクセス コントロール ルールにアプリケーションを含めると、ディテクタは自動的にアクティブにされ、使用中は非アクティブにできないことに注意してください。

基本的なアプリケーション プロトコル ディテクタ情報の提供

ライセンス：FireSIGHT

それぞれのユーザ定義のアプリケーション プロトコル ディテクタに名前を付け、検出するアプリケーション プロトコルを識別する必要があります。オプションで、ディテクタの簡単な説明を提供できます。

ユーザが提供する情報に加えて、防御センターは、ディテクタがアクティブまたは非アクティブのいずれであるか、ディテクタがポート ディテクタまたはパターン ディテクタのいずれであるかを示します。ディテクタがポートとパターンによってアプリケーション プロトコルのトラフィックを識別する場合、FireSIGHT システムはそれをパターン ディテクタと見なします。

既存のディテクタを編集する場合、防御センターはディテクタの作成者も表示します。ユーザ定義のアプリケーション プロトコル ディテクタを作成したら、そのユーザが作成者になります。また、ディテクタをインポートまたは編集および保存した場合も作成者になります。

基本的なアプリケーション プロトコル ディテクタ情報を提供する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Create Detector] ページの [Please enter a name] フィールドに、ディテクタの名前を入力します。

ディテクタの名前は、検査するトラフィックのプロトコル内で一意である必要があります。つまり、同じ名前で TCP ディテクタと UDP ディテクタを作成できますが、同じ名前で 2 つの TCP ディテクタを作成することはできません。

ステップ 2　検出するアプリケーション プロトコルを識別します。次の選択肢があります。

- 既存のアプリケーション プロトコルのディテクタを作成する場合（たとえば、非標準ポートで特定のアプリケーション プロトコルを検出する場合）、[Application Protocol] ドロップダウン リストからアプリケーション プロトコルを選択します。「アプリケーション プロトコル ディテクタの検出基準の指定」（P.42-23）の手順に進みます。
- カスタム アプリケーションのディテクタを作成する場合は、次の項ユーザ定義のアプリケーションの作成の手順に進みます。

ユーザ定義のアプリケーションの作成

ライセンス：FireSIGHT

ネットワークのカスタム アプリケーションを識別するユーザ定義のアプリケーションを作成することができます。そのアプリケーションを記述するカスタム カテゴリとカスタム タグを作成することもできます。ここで作成するアプリケーション、カテゴリ、およびタグは、アクセス コントロール ルールやアプリケーション フィルタ オブジェクト マネージャで使用できます。

アプリケーション プロトコル、およびそれらを説明するために使用されるカテゴリ、タグ、リスク レベル、ビジネスとの関連性など、アプリケーション検出の詳細については、「アプリケーション検出について」（P.35-12）を参照してください。

ユーザ定義のアプリケーションを作成する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Create Detector] ページで、[Add] をクリックします。

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

ステップ 2　カスタム アプリケーションの [Name] に名前を入力します。

ステップ 3　カスタム アプリケーションの [Description] に説明を入力します。

ステップ 4　[Business Relevance] を選択します。

ステップ 5　[Risk] を選択します。

ステップ 6　[Categories] の横にある [Add] をクリックしてカテゴリを追加し、新しいカテゴリの名前を入力するか、または [Categories] ドロップダウン リストから既存のカテゴリを選択します。

ステップ 7　オプションで、[Tags] の横にある [Add] をクリックしてタグを追加し、新しいタグの名前を入力するか、または [Tags] ドロップダウン リストから既存のタグを選択します。

[OK] をクリックして、[Create Detector] ページに戻ります。

ステップ 8　次のセクションアプリケーション プロトコル ディテクタの検出基準の指定の手順に進みます。

アプリケーション プロトコル ディテクタの検出基準の指定

ライセンス：FireSIGHT

ユーザ定義のアプリケーション プロトコル ディテクタを作成する場合、ディテクタが検査するトラフィックのプロトコル（TCP、UDP、またはその両方）を指定する必要があります。オプションで、トラフィックが使用するポートを指定できます。

「アプリケーション プロトコル ディテクタへの検出パターンの追加」（P.42-24）で説明されているように、ポートを指定しなかった場合は、1 つ以上のパターンに一致するかどうかトラフィックを検査するようにディテクタを設定する必要があることに注意してください。

アプリケーション プロトコル ディテクタの検出基準を指定する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Create Detector] ページで、[Protocol] ドロップダウン リストから、ディテクタを検査する必要があるトラフィックのプロトコルを選択します。

ディテクタは、TCP、UDP、または TCP と UDP のトラフィックを検査できます。

ステップ 2　オプションで、使用するポートに基づいてアプリケーション プロトコルのトラフィックを指定するには、1 から 65535 までのポートを [Port(s)] フィールドに入力します。複数のポートを使用する場合は、カンマで区切ります。

ステップ 3　次の選択肢があります。

- そのアプリケーション プロトコルのトラフィックで発生する 1 つ以上のパターンに一致するかどうかトラフィックを検査するようにアプリケーション プロトコル ディテクタを設定する場合は、次のセクション[アプリケーション プロトコル ディテクタへの検出パターンの追加]の手順に進みます。
- 1 つ以上の PCAP ファイルの内容に対して新しいディテクタをテストする場合は、「パケット キャプチャに対するアプリケーション プロトコル ディテクタのテスト」（P.42-25）をスキップします。
- ディテクタの作成が完了したら、[Save] をクリックします。

  アプリケーション プロトコル ディテクタが保存されます。

アプリケーション プロトコルのトラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタをアクティブにする必要があることに注意してください。詳細については、「ディテクタのアクティブ化と非アクティブ化」（P.42-30）を参照してください。

アプリケーション プロトコル ディテクタへの検出パターンの追加

ライセンス：FireSIGHT

アプリケーション プロトコルのトラフィックを格納するすべてのパケットの見出しに特定の文字列が含まれていることを把握している場合、そのパターンを検索するように、ユーザ定義のアプリケーション プロトコル ディテクタを設定できます。

アプリケーション プロトコル ディテクタは、オフセットを使用して ASCII または 16 進数のパターンを検索できます。また、複数のパターンを検索するようにディテクタを設定することもできます。この場合は、アプリケーション プロトコルのトラフィックは、アプリケーション プロトコルを確実に識別するため、ディテクタのすべてのパターンとマッチングさせる必要があります。

「アプリケーション プロトコル ディテクタの検出基準の指定」（P.42-23）で説明されているように、パターンを指定しなかった場合は、1 つ以上のポートを使用するトラフィックを検査するようにディテクタを設定する必要があることに注意してください。

検出パターンをアプリケーション プロトコル ディテクタに追加する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Create Detector] ページの [Detection Patterns] セクションで、[Add] をクリックします。

[Add Pattern] ポップアップ ウィンドウが表示されます。

ステップ 2　検出するパターンのタイプ（[Ascii] または [Hex]）を指定します。

ステップ 3　[Pattern String] フィールドに指定したタイプの文字列を入力します。

ステップ 4　オプションで、システムがパターンの検索を開始するパケットの場所（オフセットと呼ばれます）を指定します。

[Offset] フィールドにオフセット（パケット ペイロードの先頭からのバイト数）を入力します。

パケット ペイロードは 0 バイトから始まるため、パケット ペイロードの先頭から数えたバイト数から 1 を減算することでオフセットを計算します。たとえば、パケットの 5 桁目のビット パターンを検索するには、[Offset] フィールドに「4」と入力します。

ステップ 5　オプションで、その他のパターンを追加するには、ステップ 1 から 4 を繰り返します。

ヒント　パターンを削除するには、削除するパターンの横の削除アイコン（）をクリックします。

ステップ 6　次の選択肢があります。

- 1 つ以上の PCAP ファイルの内容に対して新しいディテクタをテストする場合は、次のセクション[パケット キャプチャに対するアプリケーション プロトコル ディテクタのテスト]の手順に進みます。
- ディテクタの作成が完了したら、[Save] をクリックします。

  アプリケーション プロトコル ディテクタが保存されます。

注　アプリケーション プロトコルのトラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタをアクティブにする必要があります。詳細については、「ディテクタのアクティブ化と非アクティブ化」（P.42-30）を参照してください。

パケット キャプチャに対するアプリケーション プロトコル ディテクタのテスト

ライセンス：FireSIGHT

検出するアプリケーション プロトコルからのトラフィックを持つパケットが格納されたパケット キャプチャ（PCAP）ファイルが存在する場合、その PCAP ファイルに対してユーザ定義のアプリケーション プロトコル ディテクタをテストできます。PCAP ファイルは 32KB 以下である必要があることに注意してください。それより大きい PCAP ファイルに対してディテクタのテストを試行すると、防御センターは自動的にファイルを切り捨てます。

PCAP ファイルに対してアプリケーション プロトコル ディテクタをテストする方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Create Detector] ページの [Packet Captures] セクションで、[Add] 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。

ステップ 2　PCAP ファイルを参照し、[OK] をクリックします。

PCAP ファイルがパケット キャプチャのファイル リストに表示されます。

ステップ 3　PCAP ファイルの内容に対してディテクタをテストするには、PCAP ファイルの横にある評価アイコンをクリックします。

テストが成功したかどうかを示すメッセージが表示されます。

ステップ 4　必要に応じて、ステップ 1 から 3 までを繰り返して、その他の PCAP ファイルに対するディテクタをテストします。

ヒント　PCAP ファイルを削除するには、削除するファイルの横の削除アイコン（）をクリックします。

ステップ 5　ディテクタを保存するには、[Save] をクリックします。

注　アプリケーション プロトコルのトラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタをアクティブにする必要があります。詳細については、「ディテクタのアクティブ化と非アクティブ化」（P.42-30）を参照してください。

ディテクタの管理

ライセンス：FireSIGHT

[Detectors] ページでディテクタを表示および管理します。

[Detectors] ページから以下を実行できます。

- ディテクタが識別するアプリケーションの詳細の表示
- ディテクタ リストの並べ替え、フィルタリング、および参照
- シスコが提供する内部ディテクタのリストの表示
- シスコが提供するアプリケーション プロトコル ポート ディテクタのプロパティの表示、およびオプションで、変更可能なユーザ定義の新規ディテクタとしてのコピーの保存
- ユーザ定義のアプリケーション プロトコル ディテクタの作成、変更、削除、およびエクスポート
- 個別にインポートしたアプリケーション プロトコル ディテクタの削除とエクスポート
- ユーザ定義、インポート、またはシスコが提供する Web アプリケーション、クライアント、およびアプリケーション プロトコルのディテクタのアクティブ化と非アクティブ化

内部またはシスコが提供するアプリケーション プロトコル、クライアント、または Web アプリケーションのディテクタは変更および削除できないこと、また内部ディテクタを非アクティブ化できないことに注意してください。

詳細については、以下を参照してください。

- 「ディテクタの詳細の表示」（P.42-27）
- 「ディテクタ リストの並べ替え」（P.42-27）
- 「ディテクタ リストのフィルタリング」（P.42-27）
- 「他のディテクタのページへの移動」（P.42-29）
- 「ディテクタのアクティブ化と非アクティブ化」（P.42-30）
- 「アプリケーション ディテクタの変更」（P.42-31）
- 「ディテクタの削除」（P.42-31）

ディテクタの詳細の表示

ライセンス：FireSIGHT

アプリケーション ディテクタのリストからディテクタの詳細を表示できます。

アプリケーション ディテクタの詳細を表示する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Details] 列の情報アイコン（ⓘ）をクリックします。

ディテクタに関する情報ポップアップ ウィンドウが表示されます。

リスク、ビジネスとの関連性、タグ、およびカテゴリの詳細については、「アプリケーション検出について」（P.35-12）を参照してください。

ディテクタ リストの並べ替え

ライセンス：FireSIGHT

[Detectors] ページには、デフォルトで名前のアルファベット順にディテクタがリストされます。列見出しの横にある上矢印（▲）または下矢印は、その列のその方向でページが並べ替えられていることを示します。

ディテクタを並べ替えるには：

アクセス：Admin/Discovery Admin

ステップ 1　[Detectors] ページで、該当する列見出しをクリックします。

ディテクタは、列見出しに表示される矢印によって示される方向で並べ替えられます。反対方向でソートするには、見出しを再度クリックします。

ディテクタ リストのフィルタリング

ライセンス：FireSIGHT

単一の基準または複数の基準の組み合わせによって、[Detectors] ページに表示するディテクタをフィルタリングできます。構築したフィルタは、ページの上部に表示されます。複数のフィルタ グループを別個にまたは組み合わせて使用し、ディテクタのリストをフィルタリングすることができます。

名前

ユーザが入力した文字列を含む名前または説明でディテクタを検索します。文字列には任意の英数字または特殊文字を含めることができます。

カスタム フィルタ

オブジェクト管理ページで作成したカスタム アプリケーション フィルタに一致するディテクタを検索します。詳細については、「アプリケーション フィルタの操作」（P.5-16）を参照してください。

作成者

ディテクタを作成したユーザに照らしてディテクタを検索します。次によってディテクタをフィルタリングできます。

- ディテクタを作成またはインポートした個々のユーザ
- シスコ。これは、個別にインポートされたアドオン ディテクタを*除く*シスコが提供するすべてのディテクタを表します。ディテクタをインポートした場合、そのユーザはそのディテクタの作成者になります。
- Any User。これは、シスコによって提供されたのではないすべてのディテクタを表します。

状態

状態（つまり、アクティブまたは非アクティブ）に照らしてディテクタを検索します。詳細については、「ディテクタのアクティブ化と非アクティブ化」（P.42-30）を参照してください。

タイプ

ディテクタのタイプ（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、または内部ディテクタ）に照らして検索します。

アプリケーション プロトコル ディテクタには、ディテクタをさらにフィルタリングするために使用できる 3 つのサブタイプがあります。

- ポート アプリケーション プロトコル ディテクタには、シスコが提供するよく知られているポート ディテクタやポートベースのユーザ定義アプリケーション ディテクタが含まれます。
- パターン アプリケーション プロトコル ディテクタには、パターンベースまたはポートベースとパターンベースのユーザ定義アプリケーション ディテクタが含まれます。
- **FireSIGHT** アプリケーション プロトコル ディテクタは、アクティブにしたり、非アクティブにしたりできるシスコが提供するアプリケーション プロトコル フィンガープリント ディテクタです。

ディテクタ タイプの詳細については、「アプリケーション ディテクタの使用」（P.42-18）を参照してください。

プロトコル

ディテクタが検査するトラフィック プロトコルに照らしてディテクタを検索します。ディテクタは、TCP、UDP、または TCP と UDP のトラフィックを検査できます。

カテゴリ

検出するアプリケーションに割り当てられたカテゴリに照らしてディテクタを検索します。

タグ

検出するアプリケーションに割り当てられたタグに照らしてディテクタを検索します。

リスク

検出するアプリケーションに割り当てられたリスク（Very High、High、Medium、Low、Very Low）に照らしてディテクタを検索します。

ビジネスとの関連性

検出するアプリケーションに割り当てられたビジネスとの関連性（Very High、High、Medium、Low、Very Low）に照らしてディテクタを検索します。

フィルタを適用する方法：

Admin/Discovery Admin

ステップ 1　[Detectors] ページで、ディテクタをフィルタリングするために使用するフィルタ グループを展開します。

ステップ 2　名前を入力するか、使用する特定のフィルタを選択します。グループ内のすべてのフィルタを選択するには、グループ名を右クリックし、[Check All] を選択します。

ステップ 3　オプションで、使用するフィルタにサブフィルタが存在する場合、さらにディテクタをフィルタリングするサブフィルタを選択します。

フィルタを削除する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Filters] フィールドにあるフィルタの名前の削除アイコン（ ✖ ）をクリックするか、フィルタ リストでフィルタを無効にします。グループ内のすべてのフィルタを削除するには、グループ名を右クリックし、[Uncheck All] を選択します。

フィルタが削除され、結果が更新されます。

すべてのフィルタを削除する方法：

アクセス：Admin/Discovery Admin

ステップ 1　ディテクタに適用されているフィルタ リストの横にある [Clear all] をクリックします。

他のディテクタのページへの移動

ライセンス：FireSIGHT

[Detectors] ページには、一度に 25 個のディテクタが表示されます。次の表では、ページ下部のナビゲーション リンクを使用してディテクタの追加ページの表示方法について説明します。

アクセス：Admin/Discovery Admin

表 42-1　ディテクタ ページの移動

目的	操作
次のページを表示する	右矢印アイコン（ ❯ ）をクリックします。
前のページを表示する	左矢印アイコン（ ❮ ）をクリックします。
別のページを表示する	ページ番号を入力して、Enter キーを押します。
最後のページに移動する	右端矢印アイコン（ ❯| ）をクリックします。
最初のページに移動する	左端矢印アイコン（ |❮ ）をクリックします。

ディテクタのアクティブ化と非アクティブ化

ライセンス：FireSIGHT

ネットワーク トラフィックを分析するためにディテクタを使用できるようにするには、その前に、ディテクタをアクティブにする必要があります。デフォルトでは、シスコが提供するすべてのディテクタはアクティブにされています。

システムの検出機能を補完するために、ポートごとに複数のアプリケーション ディテクタをアクティブにすることができます。

ポリシーのアクセス コントロール ルールにアプリケーションを含め、そのポリシーを適用するときに、そのアプリケーションに対してアクティブなディテクタがない場合、1 つ以上のディテクタが自動的にアクティブになります。同様に、適用されているポリシーのアプリケーションが使用されているときに、そのアプリケーションのアクティブなディテクタをすべて非アクティブにしようとしても、ディテクタを非アクティブにすることはできません。

注意　既存のディテクタをアクティブまたは非アクティブにすると、管理対象デバイス上のトラフィック フローと処理で、短時間の一時停止が発生する場合があります。これは、いくつかのパケットが検査されずに通過する原因となる可能性があります。

ヒント　パフォーマンスを向上させるために、使用する予定のないアプリケーション プロトコル、クライアント、または Web アプリケーションのディテクタはすべて非アクティブにします。

ディテクタ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/Discovery Admin

ステップ 1　[Policies] > [Application Detectors] を選択します。

[Detectors] ページが表示されます。

ステップ 2　アクティブまたは非アクティブにするディテクタを見つけます。

アクティブまたは非アクティブにするディテクタが最初のページにない場合、ディテクタ リストのページを移動するか、1 つ以上のフィルタを適用することによって、そのディテクタを見つけることができます。詳細については、「ディテクタの管理」（P.42-26）を参照してください。

ステップ 3　次の選択肢があります。

- ディテクタを**アクティブ**にして、システムがネットワーク トラフィックを分析するときにそのディテクタを使用するようにするには、ディテクタの横にある非アクティブにされたスライダ（  ）をクリックします。
- ディテクタを**非アクティブ**にして、システムがネットワーク トラフィックを分析するときにそのディテクタを使用しないようにするには、ディテクタの横にあるアクティブにされたスライダ（  ）をクリックします。

一部のアプリケーション ディテクタはその他のディテクタによって必要とされることに注意してください。そのようなディテクタのいずれかを非アクティブにすると、それに依存するディテクタも無効にされることを示す警告が表示されます。

アプリケーション ディテクタの変更

ライセンス：FireSIGHT

ユーザ定義のアプリケーション ディテクタを変更するには、次の手順を使用します。

アプリケーション ディテクタを変更する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Applications] を選択します。

[Detectors] ページが表示されます。

ステップ 2　変更するディテクタを見つけます。

変更するディテクタが最初のページにない場合、ディテクタ リストのページを移動するか、1 つ以上のフィルタを適用することによって、そのディテクタを見つけることができます。詳細については、「ディテクタの管理」（P.42-26）を参照してください。

ステップ 3　ユーザ定義のディテクタを変更するには、変更するディテクタの横にある [Edit] をクリックします。

[Edit Application Detector] ページが表示されます。

ステップ 4　ディテクタを変更します。

変更可能なさまざまな設定の詳細については、「ユーザ定義のアプリケーション プロトコル ディテクタの作成」（P.42-20）を参照してください。

ステップ 5　次の選択肢があります。

- 非アクティブなユーザ定義ディテクタを変更する場合は、[Save] をクリックして変更を保存するか、[Save as New] をクリックしてディテクタを新規の非アクティブなユーザ定義ディテクタとして保存します。
- アクティブなユーザ定義ディテクタを変更する場合は、[Save and Reactivate] をクリックして変更を保存し、すぐに変更したディテクタの使用を開始するか、[Save as New] をクリックしてディテクタを新規の非アクティブなユーザ定義ディテクタとして保存します。

注　システムは、アプリケーション トラフィックを分析するために、ディテクタがアクティブなアプリケーションのみを使用します。詳細については、「ディテクタのアクティブ化と非アクティブ化」（P.42-30）を参照してください。

ディテクタの削除

ライセンス：FireSIGHT

ディテクタを削除するには、次の手順を使用します。ユーザ定義のディテクタおよびシスコ プロフェッショナル サービスが提供する個別にインポートされたアドオン ディテクタを削除することができます。その他のシスコが提供するディテクタを削除することはできませんが、その多くを非アクティブにすることはできます。

注　ディテクタが適用されたポリシーで使用されている間は、そのディテクタを非アクティブにしたり、削除したりすることはできません。

ディテクタを削除する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Application Detectors] を選択します。

[Detectors] ページが表示されます。

ステップ 2　削除するディテクタの横にあるチェック ボックスを選択し、[Delete] をクリックします。

削除するディテクタが最初のページにない場合、ディテクタ リストのページを移動するか、1 つ以上のフィルタを適用することによって、そのディテクタを見つけることができます。詳細については、「ディテクタの管理」（P.42-26）を参照してください。

ステップ 3　[OK] をクリックして、ディテクタを削除することを確認します。

ディテクタが削除されます。

ホスト入力データのインポート

ライセンス：FireSIGHT

サードパーティからネットワーク マップ データをインポートするために、組織にスクリプトを作成する機能、またはコマンドライン インポート ファイルを作成する機能がある場合、データをインポートしてネットワーク マップの情報を強化することができます。また、Web インターフェイスを使用して、オペレーティング システムまたはアプリケーションの ID を変更するか、アプリケーション プロトコル、プロトコル、ホスト属性、クライアントを削除することによって、ホスト入力機能を使用することができます。

システムは複数のソースからのデータを照合して、オペレーティング システムまたはアプリケーションの現行 ID を判別できます。この実行方法の詳細については、「現在の ID について」（P.42-5）を参照してください。

ネットワーク マップから影響を受けるホストを削除すると、サードパーティの脆弱性を除くすべてのデータは破棄されることに注意してください。スクリプトまたはインポート ファイルの設定方法の詳細については、『*FireSIGHT System Host Input API Guide*』を参照してください。

影響の関連付けにインポートしたデータを含めるには、データベースのオペレーティング システムおよびアプリケーション定義にデータをマッピングする必要があります。詳細については、次の項を参照してください。

- 「サードパーティ データの使用の有効化」（P.42-33）
- 「サードパーティ製品マッピングの管理」（P.42-33）
- 「サードパーティの脆弱性のマッピング」（P.42-36）
- 「カスタム製品マッピングの管理」（P.42-37）

サードパーティ データの使用の有効化

ライセンス：FireSIGHT

ネットワークのサードパーティ システムからネットワーク マップ データをインポートできます。ただし、FireSIGHTの推奨事項、適応型プロファイル、影響評価など、侵入データやディスカバリ データを一緒に使用する機能を有効にするには、可能な限り多くの要素を対応する定義にマッピングする必要があります。サードパーティ データを使用する場合、以下の要件を考慮します。

- ネットワーク資産に特定のデータを持つサードパーティ システムがある場合、ホスト入力機能を使用してそのデータをインポートできます。ただし、製品にはサードパーティによって異なる名前が付けられていることがあるため、対応するシスコ製品定義にサードパーティのベンダー、製品、バージョンをマッピングする必要があります。製品をマッピングした後、システム ポリシーでの影響評価のために脆弱性マッピングを有効にして、影響の関連付けを可能にする必要があります。バージョンレスまたはベンダーレスのアプリケーション プロトコルの場合、システム ポリシーでアプリケーション プロトコルの脆弱性をマッピングする必要があります。詳細については、「サードパーティ製品のマッピング」（P.42-34）を参照してください。
- サード パーティからパッチ情報をインポートし、そのパッチによって解決されたすべての脆弱性を無効としてマークする場合、データベースの修正定義にサードパーティの修正名をマッピングする必要があります。その修正によって解決されたすべての脆弱性は、その修正を追加したホストから除去されます。詳細については、「サード パーティ製品の修正のマッピング」（P.42-35）を参照してください。
- サードパーティからオペレーティング システムおよびアプリケーション プロトコルの脆弱性をインポートし、影響の関連付けに使用する場合、サードパーティの脆弱性の識別文字列をデータベースの脆弱性にマッピングする必要があります。多くのクライアントには関連付けられた脆弱性があり、クライアントが影響評価に使用されますが、サードパーティのクライアントの脆弱性をインポートしてマッピングすることはできないことに注意してください。脆弱性をマッピングした後、システム ポリシーでの影響評価のためにサードパーティの脆弱性マッピングを有効にする必要があります。詳細については、「サードパーティの脆弱性のマッピング」（P.42-36）を参照してください。アプリケーション プロトコルにベンダー情報またはバージョン情報がない場合に、脆弱性にマッピングするようするには、管理ユーザが、システム ポリシーでアプリケーションの脆弱性をマッピングする必要もあります。詳細については、「サーバの脆弱性のマッピング」（P.50-30）を参照してください。
- アプリケーション データをインポートし、影響の関連付けにそのデータを使用する場合は、対応するシスコ アプリケーション プロトコル定義に各アプリケーション プロトコルのベンダー文字列をマッピングする必要があります。詳細については、「カスタム製品マッピングの管理」（P.42-37）を参照してください。

サードパーティ製品マッピングの管理

ライセンス：FireSIGHT

ユーザ入力機能を使用してサードパーティからネットワーク マップにデータを追加する場合、シスコ製品定義にサードパーティが使用するベンダー、製品、バージョンの名前をマッピングする必要があります。製品をシスコの定義にマッピングすると、これらの定義に基づいて脆弱性が割り当てられます。

同様に、パッチ管理製品などサードパーティからパッチ情報をインポートする場合、修正の名前を適切なベンダーおよび製品およびデータベースの対応する修正にマッピングする必要があります。

詳細については、次の項を参照してください。

- 「サードパーティ製品のマッピング」（P.42-34）
- 「サード パーティ製品の修正のマッピング」（P.42-35）

サードパーティ製品のマッピング

ライセンス：FireSIGHT

サードパーティからデータをインポートする場合、そのデータを使用して脆弱性を割り当てたり、影響の関連付けを行ったりするために、シスコ製品をサードパーティの名前にマッピングする必要があります。製品をマッピングすることにより、シスコの脆弱性の情報をサードパーティ製品の名前に関連付けます。これにより、システムはそのデータを使用して、影響の関連付けを実行できます。

ホスト入力のインポート機能を使用してデータをインポートする場合、AddScanResult 機能を使用して、インポート中にサードパーティ製品をオペレーティング システムおよびアプリケーションの脆弱性にマップピングすることもできます。

例として、Apache Tomcat をアプリケーションとしてリストするサードパーティからデータをインポートするときに、それがバージョン 6 の製品であると分かっている場合、[Vendor Name] が `Apache`、[Product Name] が `Tomcat` に設定され、[Vendor] ドロップダウン リストから [Apache]、[Product] ドロップダウン リストから [Tomcat]、[Version] ドロップダウン リストから [6] が選択されているサードパーティ マップを追加できます。このマッピングによって、Apache Tomcat 6 のすべての脆弱性が、アプリケーションとして Apache Tomcat をリストするホストに割り当てられます。

バージョンレスまたはベンダーレスのアプリケーションの場合、システム ポリシーでアプリケーション タイプの脆弱性をマッピングする必要があります。詳細については、「サーバの脆弱性のマッピング」（P.50-30）を参照してください。多くのクライアントには関連付けられた脆弱性があり、クライアントが影響評価に使用されますが、サードパーティのクライアントの脆弱性をインポートしてマッピングすることはできないことに注意してください。

ヒント　すでに別の防御センターにサードパーティのマッピングを作成している場合、そのマッピングをエクスポートして、この防御センターにインポートすることができます。その後、必要に応じてインポートしたマッピングを編集できます。詳細については、「設定のインポートおよびエクスポート」（P.A-1）を参照してください。

サード パーティ製品をシスコ製品定義にマッピングする方法：

アクセス：Admin

ステップ 1　[Policies] > [Application Detectors] を選択し、[User Third-Party Mappings] をクリックします。

[User Third-Party Mappings] ページが表示されます。

ステップ 2　次の 2 つの選択肢があります。

- 既存のマップ セットを編集するには、マップ セットの横にある [Edit] をクリックします。
- 新しいマップ セットを作成するには、[Create Product Map Set] をクリックします。

[Edit Third-Party Product Mappings] ページが表示されます。

ステップ 3　[Mapping Set Name] フィールドにマッピング セットの名前を入力します。

ステップ 4　[Description] フィールドに説明を入力します。

ステップ 5　次の 2 つの選択肢があります。

- サード パーティ製品をマッピングするには、[Add Product Map] をクリックします。
- 既存のサード パーティ製品マップを編集するには、マップ セットの横にある [Edit] をクリックします。

[Add Product Map] ページが表示されます。

ステップ 6　[Vendor String] フィールドにサードパーティ製品によって使用されるベンダー文字列を入力します。

ステップ 7　[Product String] フィールドにサードパーティ製品によって使用される製品文字列を入力します。

ステップ 8　[Version String] フィールドにサードパーティ製品によって使用されるバージョン文字列を入力します。

ステップ 9　[Product Mappings] セクションで、以下のリストから脆弱性マッピングに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（該当する場合）。

- **Vendor**
- **Product**
- **Major Version**
- **Minor Version**
- **Revision Version**
- **Build**
- **Patch**
- **Extension**

たとえば、名前がサードパーティ文字列で構成される製品を実行するホストで Red Hat Linux 9 の脆弱性を使用する場合、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、バージョンとして [9] を選択します。

ステップ 10　[Save] をクリックします。

サード パーティ製品の修正のマッピング

ライセンス：FireSIGHT

修正名をデータベースの特定の修正セットにマッピングする場合、サードパーティのパッチ管理アプリケーションからデータをインポートし、修正を一連のホストに適用することができます。修正名がホストにインポートされると、システムはその修正によって解決されるすべての脆弱性をそのホストに対して無効としてマークします。

サードパーティの修正をシスコの修正定義にマッピングする方法：

アクセス：Admin/

ステップ 1　[Policies] > [Application Detectors] を選択し、[User Third-Party Mappings] をクリックします。

[User Third-Party Mappings] ページが表示されます。

ステップ 2　次の 2 つの選択肢があります。

- 既存のマップ セットを編集するには、マップ セットの横にある [Edit] をクリックします。
- 新しいマップ セットを作成するには、[Create Product Map Set] をクリックします。

[Edit Third-Party Product Mappings] ページが表示されます。

ステップ 3　[Mapping Set Name] フィールドにマッピング セットの名前を入力します。

ステップ 4　[Description] フィールドに説明を入力します。

ステップ 5　次の 2 つの選択肢があります。

- サード パーティ製品をマッピングするには、[Add Fix Map] をクリックします。
- 既存のサード パーティ製品マップを編集するには、その横にある [Edit] をクリックします。

[Add Fix Map] ページが表示されます。

ステップ 6　[Third-Party Fix Name] フィールドにマッピングする修正の名前を入力します。

ステップ 7　[Product Mappings] セクションで、以下のリストから修正マッピングに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（該当する場合）。

- **Vendor**
- **Product**
- **Major Version**
- **Minor Version**
- **Revision Version**
- **Build**
- **Patch**
- **Extension**

たとえば、マッピングで Red Hat Linux 9 から選択した修正をパッチが適用されるホストに割り当てる場合、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、バージョンとして [9] を選択します。

ステップ 8　[Save] をクリックして、修正マップを保存します。

サードパーティの脆弱性のマッピング

ライセンス：FireSIGHT

サードパーティから VDB に脆弱性情報を追加するには、インポートしたそれぞれの脆弱性のサードパーティ識別文字列を、既存のシスコ、Bugtraq、または Snort の ID にマッピングする必要があります。脆弱性のマッピングを作成したら、マッピングはネットワーク マップのホストにインポートされたすべての脆弱性に対して機能し、それらの脆弱性に対する影響の関連付けを可能にします。

サードパーティの脆弱性に対する影響の関連付けを有効にし、関連付けの実行を可能にする必要があることに注意してください。詳細については、「脆弱性影響評価マッピングの有効化」（P.35-38）を参照してください。バージョンレスまたはベンダーレスのアプリケーションの場合、システム ポリシーでアプリケーション タイプの脆弱性をマッピングする必要もあります。詳細については、「サーバの脆弱性のマッピング」（P.50-30）を参照してください。

また、多くのクライアントには関連付けられた脆弱性があり、クライアントが影響評価に使用されますが、サードパーティのクライアントの脆弱性は影響評価に使用できません。

ヒント　すでに別の防御センターにサードパーティのマッピングを作成している場合、そのマッピングをエクスポートして、この防御センターにインポートすることができます。その後、必要に応じてインポートしたマッピングを編集できます。詳細については、「設定のインポートおよびエクスポート」（P.A-1）を参照してください。

サードパーティの脆弱性を既存の脆弱性にマッピングする方法：

アクセス：Admin

ステップ 1　[Policies] > [Application Detectors] を選択し、[User Third-Party Mappings] をクリックします。

[User Third-Party Mappings] ページが表示されます。

ステップ 2　次の 2 つの選択肢があります。

- 既存の脆弱性セットを編集するには、脆弱性セットの横にある [Edit] をクリックします。
- 新しい脆弱性セットを作成するには、[Create Vulnerability Map Set] をクリックします。

[Edit Third-Party Vulnerability Mappings] ページが表示されます。

ステップ 3　[Add Vulnerability Map] をクリックします。

[Add Vulnerability Map] ポップアップ ウィンドウが表示されます。

ステップ 4　[Vulnerability ID] フィールドに脆弱性のサード パーティ ID を入力します。

ステップ 5　[Vulnerability Description] フィールドに説明を入力します。

ステップ 6　オプションで、[Snort Vulnerability ID Mappings] フィールドにシグニチャ ID を入力します。

ステップ 7　オプションで、[シスコ Vulnerability ID Mappings] フィールドにシスコの脆弱性 ID を入力します。

ステップ 8　オプションで、[Bugtraq Vulnerability ID Mappings] フィールドに Bugtraq ID 番号を入力します。

ステップ 9　[Add] をクリックします。

カスタム製品マッピングの管理

ライセンス：FireSIGHT

製品マッピングを使用して、サードパーティによるサーバ入力が適切なシスコ定義に関連付けられていることを確認できます。製品マッピングを定義してアクティブにした後、マッピングされたベンダー文字列が存在するネットワーク マップのホスト上のすべてのサーバまたはクライアントは、カスタム製品マッピングを使用します。したがって、サーバのベンダー、製品、バージョンを明示的に設定する代わりに、特定のベンダー文字列でネットワーク マップのすべてのサーバの脆弱性をマップすることをお勧めします。

詳細については、以下を参照してください。

- 「カスタム製品マッピングの作成」（P.42-38）
- 「カスタム製品マッピング リストの編集」（P.42-39）
- 「カスタム製品マッピングのアクティベーション状態の管理」（P.42-39）

カスタム製品マッピングの作成

ライセンス：FireSIGHT

システムがネットワーク マップのサーバを VDB 内のベンダーおよび製品にマッピングできない場合、サーバを識別するときに使用するシステムのマッピングを手動で作成できます。カスタム製品マッピングをアクティブにすると、システムは選択されたベンダーおよび製品の脆弱性を、そのベンダー文字列が発生するネットワーク マップのすべてのサーバにマッピングします。

注　カスタム製品マッピングは、アプリケーション データのソース（Nmap、ホスト入力機能、または FireSIGHT システム自体など）に関係なく、アプリケーション プロトコルのすべての発生に適用されます。ただし、ホスト入力機能を使用してインポートしたデータのサードパーティの脆弱性マッピングが、カスタム製品マッピングを介して設定したマッピングと競合する場合、サードパーティの脆弱性マッピングはカスタム製品マッピングをオーバーライドし、入力が発生したときにサードパーティの脆弱性マッピング設定を使用します。詳細については、「サードパーティの脆弱性のマッピング」（P.42-36）を参照してください。

製品マッピング リストを作成し、各リストをアクティブ化/非アクティブ化することによって、複数のマッピングの同時使用を有効にするか、無効にします。マッピングするベンダーを選択すると、そのベンダーによって作成された製品のみを含むように製品リストが更新されます。

カスタム製品マッピングを作成した後で、カスタム製品マッピング リストをアクティブにする必要があります。カスタム製品マッピング リストをアクティブにすると、指定されたベンダー文字列が発生するすべてのサーバが更新されます。ホスト入力機能を介してインポートされるデータでは、このサーバの製品マッピングをすでに明示的に設定していない限り、脆弱性が更新されます。

たとえば、組織が `Internal Web Server` を読み取るように Apache Tomcat Web サーバのバナーを変更した場合、ベンダー文字列 `Internal Web Server` をベンダー **Apache** および製品 **Tomcat** にマッピングできます。その後、そのマッピングを含むリストをアクティブにすると、`Internal Web Server` とラベル付けされたサーバが発生するすべてのホストで、Apache Tomcat の脆弱性がデータベースに保存されます。

ヒント　この機能を使用して、もう 1つの脆弱性にルールの SID をマッピングすることによって、ローカルの侵入ルールに脆弱性をマッピングすることができます。

カスタム製品マッピングを作成する方法：

アクセス：Admin

ステップ 1　[Policies] > [Application Detectors] を選択し、[Custom Product Mappings] をクリックします。

[Custom Product Mappings] ページが表示されます。

ステップ 2　[Create Custom Product Mapping List] をクリックします。

[Edit Custom Product Mappings List] ページが表示されます。

ステップ 3　名前を [Custom Product Mapping List Name] フィールドに入力します。

ステップ 4　[Add Vendor String] をクリックします。

[Add Vendor String] ポップアップ ウィンドウが表示されます。

ステップ 5　[Vendor String] フィールドに、選択したベンダーおよび製品値にマッピングする必要があるアプリケーションを識別するベンダー文字列を入力します。

ステップ 6　[Vendor] ドロップダウン リストから、マッピングするベンダーを選択します。

ステップ 7　[Product] ドロップダウン リストから、マッピングする製品を選択します。

ステップ 8　[Add] をクリックして、マッピングしたベンダー文字列をリストに追加します。

ステップ 9　オプションで、その他のベンダー文字列のマッピングをリストに追加するには、必要に応じてステップ 4 から 8 を繰り返します。

ステップ 10　終了したら、[Save] をクリックします。

[Custom Product Mappings] ページが、追加したリストとともに再度表示されます。

カスタム製品マッピング リストの編集

ライセンス：FireSIGHT

ベンダー文字列を追加または削除したり、リスト名を変更したりして、既存のカスタム製品マッピング リストを変更できます。

カスタム製品マッピングを編集する方法：

アクセス：Admin

ステップ 1　[Policies] > [Application Detectors] を選択し、[Custom Product Mappings] をクリックします。

[Custom Product Mappings] ページが表示されます。

ステップ 2　編集する製品マッピング リストの横にある編集アイコン（  ）をクリックします。

[Edit Custom Product Mappings List] ページが表示されます。

ステップ 3　必要に応じてリストを変更します。詳細については、「カスタム製品マッピングの作成」（P.42-38）を参照してください。

ステップ 4　終了したら、[Save] をクリックします。

[Custom Product Mappings] ページが、変更したリストとともに表示されます。

カスタム製品マッピングのアクティベーション状態の管理

ライセンス：FireSIGHT

カスタム製品マッピング リスト全体の使用を一度に有効または無効にすることができます。カスタム製品マッピング リストをアクティブにすると、そのリストの各マッピングが、管理対象デバイスによって検出されたか、またはホスト入力機能を介してインポートされたかに関わらず、指定したベンダー文字列を持つネットワーク マップのホスト上のすべてのアプリケーションに適用されます。

カスタム製品マッピング リスト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

ステップ 1　[Policies] > [Application Detectors] を選択し、[Custom Product Mappings] をクリックします。[Custom Product Mappings] ページが表示されます。

ステップ 2　以下のように、カスタム製品マッピング リストの状態を変更します。

- カスタム製品マッピング リストの使用を有効にするには、[Activate] をクリックします。
- カスタム製品マッピング リストの使用を無効にするには、[Deactivate] をクリックします。