CHAPTER 46

ネットワーク検出の拡張

FireSIGHT システムによって収集されるネットワーク トラフィック情報は、この情報を関連付けることでネットワーク上の最も脆弱かつ最も重要なホストを識別することができる場合に、その価値を最大限に発揮します。

たとえば、ネットワーク上の複数のデバイスで SuSE Linux のカスタマイズ バージョンを実行している場合、システムはそのオペレーティング システムを識別できないため、ホストに脆弱性をマッピングすることができません。しかし、システムに SuSE Linux に関する脆弱性のリストがあることが分かっていれば、いずれか 1 つのホストに関するカスタム フィンガープリントを作成し、これを使用して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にそのリストを関連付けることができます。

また、ホスト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があります。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や 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アイデンティティ（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（46-5 ページ）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（47-1 ページ）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、正しく識別されていないホストとその理由を分析する必要があります。これにより、実装すべきソリューションを決定できます。以下を参考にして、ソリューションを決定します。

管理対象デバイスが正しく配置されているか

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、管理対象デバイスと未確認ホストまたは誤認識されたホストと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するのではなく、誤認識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 スタックがあるか

ライセンス：FireSIGHT

システムがホストを誤認する場合、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 やホストの入力データを使用するかを決定するために、ホストが誤認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。

デフォルトでシステムによって検出されないオペレーティング システムをホストが実行していて、既存の検出済みオペレーティング システムとの間で識別対象の TCP スタック特性を共有していない場合は、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 スタックを実装した Linux のカスタマイズ バージョンが存在する場合、カスタム フィンガープリントを作成すると便利です。このようにすると、システムがホストを識別して監視を続行できるので、手動で継続的にデータを更新する必要のあるスキャン結果やサードパーティのデータを使用せずに済みます。

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をすべての状況で使用するのが適切なわけではありません。たとえば、ホストの TCP スタックに変更が加えられ、別のオペレーティング システムと類似する(または同じ)ものになることがあります。たとえば、Apple Mac OS X ホスト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変更されると、システムはホストを Mac OS X ではなく Linux 2.4 として識別します。この Mac OS X ホストのカスタム フィンガープリントを作成すると、すべての正規の Linux 2.4 ホストが Mac OS X ホストとして誤認される場合があります。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（46-34 ページ）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や 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アイデンティティ（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（46-5 ページ）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、ディスカバリ データ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 システムがすべてのアプリケーションを識別できるか

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、未確認アプリケーションが存在する場合には、ユーザ定義ディテクタを作成してポートとパターンのマッチング情報をシステムに提供し、アプリケーションの識別に利用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（46-21 ページ）を参照してください。

脆弱性の修正パッチを適用したか

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（46-36 ページ）を参照してください。

サードパーティの脆弱性を追跡するか

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 システム 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（46-37 ページ）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や 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 マップの拡張

ライセンス：FireSIGHT

FireSIGHT システムは、トラフィックをパッシブに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。アプリケーションやオペレーティング 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と、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拡張する最善の方法を決定するうえで役立ちます。

詳細は、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

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 アセット（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。

データを解釈できないため *unknown*（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システムが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アイデンティティを unknown として Defense Center に報告します。そのアイデンティティ 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

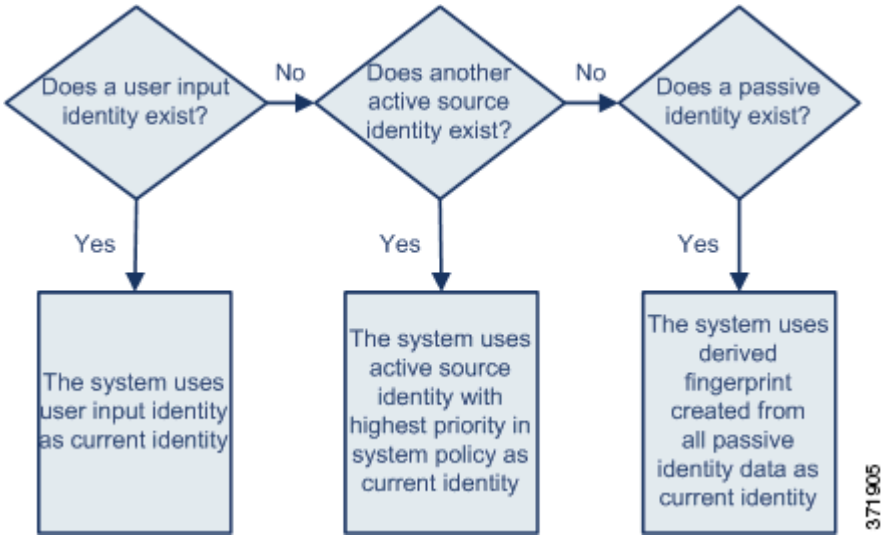
ホスト上のアプリケーションやオペレーティング システムの*現在のアイデンティティ（ID）*は、ホストが最も正しい可能性が高いと認識するアイデンティティです。

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
- [検出統計情報（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、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、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。詳細については、ID の競合について（46-7 ページ）を参照してください。

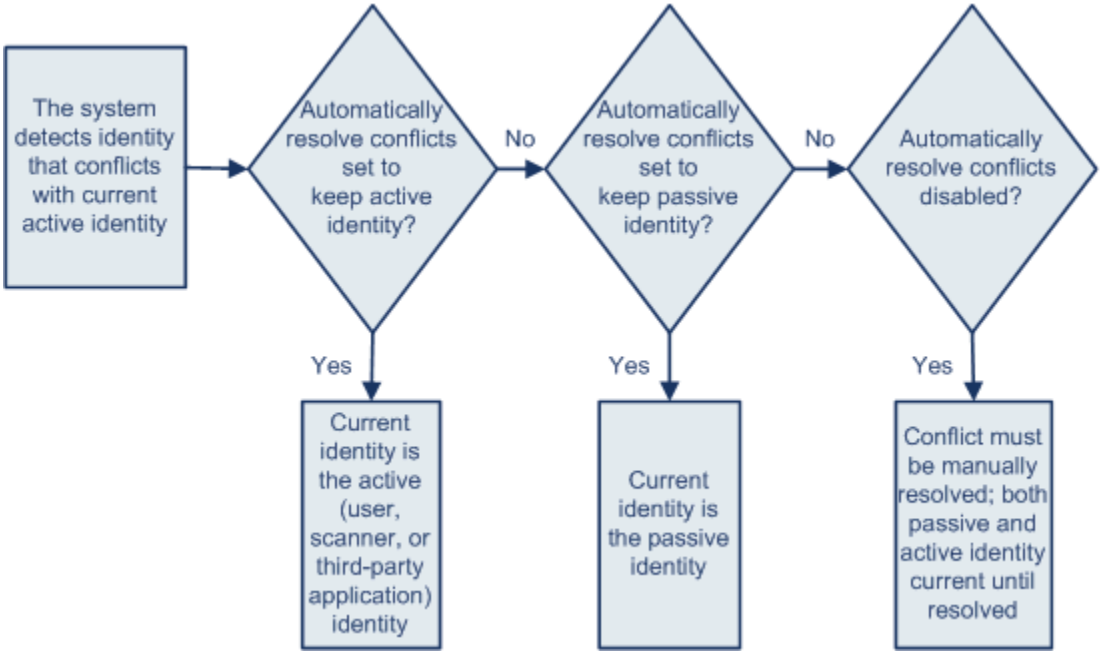
ID の競合について

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 システムと一致するフィンガープリントが存在しないために、システムがホスト オペレーティング システムを識別できないか誤認識する場合があります。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には、ホストの脆弱性を識別できません。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、ネットワーク上の複数のデバイスで Microsoft Windows の新しいベータ バージョンを実行している場合、システムはそのオペレーティング システムを識別できないため、それらのホストに脆弱性をマッピングできません。しかし、システムに Microsoft Windows に関する脆弱性のリストがあることが分かっていれば、いずれか 1 つのホストに関するカスタム フィンガープリントを作成し、これを使用して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。Defense Center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。ネットワーク マップにすでに存在する検出済みホストからの新しいトラフィックが確認されると、システムは新しいフィンガープリント情報を使ってそのホストを更新します。また、そのオペレーティング システムを実行する新しいホストが新たに検出されると、システムは新しいフィンガープリントを使用してそのホストを識別します。

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（46-2 ページ）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 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される TCP アプリケーションに接続するときにホストが送信する 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 フィンガープリントの作成（46-9 ページ）を参照してください。

- サーバ フィンガープリント。実行中の TCP アプリケーションから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 フィンガープリントの作成（46-12 ページ）を参照してください。

システムがフィンガープリントをホストに関連付けることを可能にするには、フィンガープリントの作成後に、それらのフィンガープリントをアクティブ化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（46-15 ページ）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 フィンガープリントの作成

ライセンス：FireSIGHT

クライアント 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される TCP アプリケーションに接続するときにホストが送信する 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。

Defense Center が監視対象ホストと直接通信しない場合は、クライアント 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作成対象のホストに最も近い、Defense Center によって管理される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の作成対象とな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 Defense Center 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 Defense Center 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（Defense Center 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

手順 1　[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）] を選択し、[カスタム オペレーティング システム（Custom Operating Systems）] をクリックします。

[カスタム フィンガープリント（Custom Fingerprint）] ページが表示されます。

手順 2　[カスタム フィンガープリントの作成（Create Custom Fingerprint）] をクリックします。

[カスタム フィンガープリントの作成（Create Custom Fingerprint）] ページが表示されます。

手順 3　[デバイス（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 Defense Center またはデバイスを選択します。

手順 4　[フィンガープリント名（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。

手順 5　[フィンガープリントの説明（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。

手順 6　[フィンガープリントのタイプ（Fingerprint Type）] リストから、[クライアント（Client）] を選択します。

手順 7　[ターゲット IP アドレス（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。ホストに他の IP アドレスが存在していても、フィンガープリントは、ここで指定したホスト 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　管理対象デバイスおよび Defense Center での IPv6 の有効化の詳細については、管理インターフェイスの構成（64-9 ページ）を参照してください。

手順 8　[ターゲットの距離（Target Distance）] フィールドで、ホストと手順 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。

手順 9　[インターフェイス（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。

手順 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 の脆弱性マッピング（OS Vulnerability Mappings）] セクションに存在しない場合）、[カスタム OS 表示（Custom OS Display）] セクションの [カスタム OS 表示を使用（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。

- [ベンダー文字列（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。
- [製品文字列（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。
- [バージョン文字列（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。

手順 11　[OS の脆弱性マッピング（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 [Redhat Linux]、メジャー バージョン [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（46-18 ページ）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、[ベンダー（Vendor）] リストから [PalmSource, Inc.]、[製品（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)　[メジャー バージョン（Major Version）]、[マイナー バージョン（Minor Version）]、[リビジョン バージョン（Revision Version）]、[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作成対象とな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。

手順 12　[作成（Create）] をクリックします。

[カスタム フィンガープリント（Custom Fingerprint）] ステータス ページが再表示されます。該当する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　[作成（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。

手順 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作成対象のホストから Defense Center の Web インターフェイスにアクセスするか、ホストから SSH で Defense Center 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手順 7 で指定した IPv6 アドレスです。*DCmanagementIPv6address* は、Defense Center の管理 IPv6 アドレスです。

これで、[カスタム フィンガープリント（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、フィンガープリントを収集するアプライアンスでトラフィックが認識される**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。

手順 14　Defense Center がフィンガープリントを使用してホストを識別できるようにするには、フィンガープリントの作成後にそのフィンガープリントをアクティブ化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（46-15 ページ）を参照してください。

サーバ フィンガープリントの作成

ライセンス: FireSIGHT

サーバ フィンガープリントは、実行中の TCP アプリケーションから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作成対象の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 Defense Center が監視対象ホストと直接通信しない場合は、サーバ 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

手順 1 [ポリシー(Policies)] > [ネットワーク検出(Network Discovery)] を選択し、[カスタム オペレーティング システム(Custom Operating Systems)] をクリックします。

[カスタム フィンガープリント(Custom Fingerprint)] ページが表示されます。

手順 2 [カスタム フィンガープリントの作成(Create Custom Fingerprint)] をクリックします。

[カスタム フィンガープリントの作成(Create Custom Fingerprint)] ページが表示されます。

手順 3 [デバイス(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 Defense Center または管理対象デバイスを選択します。

手順 4 [フィンガープリント名(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。

手順 5 [フィンガープリントの説明(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。

手順 6 [フィンガープリントのタイプ(Fingerprint Type)] リストから、[サーバ(Server)] を選択します。

サーバ フィンガープリントのオプションが表示されます。

手順 7 [ターゲット IP アドレス(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。ホストに他の IP アドレスが存在していても、フィンガープリントは、ここで指定したホスト 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。

手順 8　[ターゲットの距離（Target Distance）] フィールドで、ホストと手順 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。

手順 9　[インターフェイス（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。

手順 10　[アクティブなポートを取得（Get Active Ports）] をクリックします。

システムがホスト上のオープン ポートを検出した場合は、ドロップダウン リストにそれらが表示されます。

手順 11　[サーバ ポート（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、[アクティブなポートを取得（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）。

手順 12　[送信元 IP アドレス（Source 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、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（45-2 ページ）を参照してください。

手順 13　[送信元サブネットマスク（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。

手順 14　[送信元ゲートウェイ（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、[送信元ゲートウェイ（Source Gateway）] フィールドが表示されます。

手順 15　フィンガープリント対象となるホストのホスト 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 定義（OS Definition）] セクションに存在しない場合には、[カスタム OS 表示（Custom OS Display）] セクションの [カスタム OS 表示を使用（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。

- [ベンダー文字列（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。
- [製品文字列（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。
- [バージョン文字列（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。

手順 16　[OS の脆弱性マッピング（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]、バージョンは [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（46-18 ページ）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、[ベンダー（Vendor）] リストから [PalmSource, Inc.]、[製品（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）　[メジャー バージョン（Major Version）]、[マイナー バージョン（Minor Version）]、[リビジョン バージョン（Revision Version）]、[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作成対象とな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。

手順 17　[作成（Create）] をクリックします。

手順 18　[カスタム フィンガープリント（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はずです。

（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、[カスタム フィンガープリント（Custom Fingerprint）] ページにアクセスしてから [作成（Create）] をクリックします。

手順 19　フィンガープリントが作成されたら、そのフィンガープリントをアクティブにし、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（46-15 ページ）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 フィンガープリントの作成（46-9 ページ）およびサーバ フィンガープリントの作成（46-12 ページ）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化した後、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。

[カスタム フィンガープリント（Custom Fingerprints）] ページにアクセスする方法：

アクセス：Admin/Discovery Admin

手順 1　[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）] を選択し、[カスタム オペレーティング システム（Custom Operating Systems）] をクリックします。

[カスタム フィンガープリント（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、次の各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（46-15 ページ）
- フィンガープリントの非アクティブ化（46-16 ページ）
- フィンガープリントの削除（46-16 ページ）
- フィンガープリントの編集（46-17 ページ）

フィンガープリントのアクティブ化

ライセンス：FireSIGHT

システムがフィンガープリントを使用してホストを識別できるようにするには、カスタム フィンガープリントの作成後に、そのフィンガープリントをアクティブ化（有効化）する必要があります。アクティブ化された新しいフィンガープリントは、以前に検出したホストの再識別および新しいホストの検出に使用されます。

フィンガープリントをアクティブ化する方法：

アクセス：Admin/Discovery Admin

手順 1　[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）] を選択し、[カスタム オペレーティング システム（Custom Operating Systems）] をクリックします。

[カスタム フィンガープリント（Custom Fingerprint）] ページが表示されます。

手順 2　アクティブ化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適切なものである場合に限り使用できます。スライダが使用可能でない場合、フィンガープリントを再作成してみてください。

Defense Center はフィンガープリントをアクティブ化し、すべての管理対象デバイスに伝達します。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化（無効化）できます。非アクティブ化されたフィンガープリントは使用されなくなりますが、システム上には維持されます。フィンガープリントを非アクティブ化すると、オペレーティング システムは、そのフィンガープリントを使用するホストに対して「不明」とマークされます。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、そのフィンガープリントは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化した後でそれを削除できます。

アクティブなフィンガープリントを非アクティブ化する方法：

アクセス：Admin/Discovery Admin

手順 1　[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）] を選択し、[カスタム オペレーティング システム（Custom Operating Systems）] をクリックします。

[カスタム フィンガープリント（Custom Fingerprint）] ページが表示されます。

手順 2　非アクティブ化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。

Defense Center はフィンガープリントを非アクティブ化し、すべての管理対象デバイスにその非アクティブ化を伝達します。

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化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

手順 1　[ポリシー(Policies)] > [ネットワーク検出(Network Discovery)] を選択し、[カスタム オペレーティング システム(Custom Operating Systems)] をクリックします。

[カスタム フィンガープリント(Custom Fingerprint)] ページが表示されます。

手順 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化します。

手順 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。

手順 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。アクティブか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、変更できる項目が異なります。

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することができ、それらを Defense Center 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、それがシステムに再送信されます。クライアント フィンガープリントの場合は、アクティブ化する前に、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化した後、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(46-17 ページ)
- アクティブなフィンガープリントの編集(46-18 ページ)

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

手順 1　[ポリシー(Policies)] > [ネットワーク検出(Network Discovery)] を選択し、[カスタム オペレーティング システム(Custom Operating Systems)] をクリックします。

[カスタム フィンガープリント(Custom Fingerprint)] ページが表示されます。

手順 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。

[カスタム フィンガープリントの編集(Edit Custom Fingerprint)] ページが表示されます。

手順 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 フィンガープリントを変更する場合の設定できるオプションの詳細については、クライアント フィンガープリントの作成(46-9 ページ)を参照してください。
- サーバ フィンガープリントを変更する場合の設定できるオプションの詳細については、サーバ フィンガープリントの作成(46-12 ページ)を参照してください。

手順 4　[保存(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

手順 1　[ポリシー(Policies)] > [ネットワーク検出(Network Discovery)] を選択し、[カスタム オペレーティング システム(Custom Operating Systems)] をクリックします。

[カスタム フィンガープリント(Custom Fingerprint)] ページが表示されます。

手順 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。

[カスタム フィンガープリントのマッピングを編集(Edit Custom Fingerprint Product Mappings)] ページが表示されます。

手順 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。

手順 4　脆弱性マッピングを削除するには、このページの [事前定義された OS 製品マップ(Pre-Defined OS Product Maps)] セクションの横にある [削除(Delete)] をクリックします。

手順 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には、[製品(Product)] を選択し(該当する場合は [メジャー バージョン(Major Version)]、[マイナー バージョン(Minor Version)]、[リビジョン バージョン(Revision Version)]、[ビルド(Build)]、[パッチ(Patch)]、および [拡張機能(Extension)] も選択)、[OS 定義の追加(Add OS Definition)] をクリックします。

脆弱性マッピングが、[事前定義された OS 製品マップ(Pre-Defined OS Product Maps)] リストに追加されます。

手順 6　[保存(Save)] をクリックして変更内容を保存します。

アプリケーション ディテクタの操作

ライセンス：FireSIGHT

FireSIGHT システムが IP トラフィックを分析するときには、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。[ディテクタ（Detectors）] ページ（[ポリシー（Policies）] > [アプリケーション ディテクタ（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、アクティブなディテクタのみを使用してアプリケーション トラフィックを分析します。

リストされたディテクタによって、プロパティが異なる場合があります。たとえば、一部のディテクタで表示できる設定の中には、他のディテクタで表示できないものがあります。また、削除できるディテクタと削除できないディテクタがあります。これは、次のセクションで説明しているように、シスコ提供のディテクタには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、非アクティブ化できないことから、他の種類では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化することも、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。内部ディテクタには、組み込み Amazon ディテクタや組み込み AppleTalk ディテクタなどがあります。

シスコが提供するクライアント ディテクタ

シスコ提供の*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ます。これらは VDB アップデートを介して提供されることも、FireSIGHT システムの更新によって提供されることもあります。また、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 ディテクタには、Google Earth ディテクタや Immunet ディテクタなどがあります。

シスコが提供する Web アプリケーション ディテクタ

シスコ提供の *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ます。VDB アップデートを介して提供されることも、FireSIGHT システムへの更新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 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 アップデートにより、Web アプリケーション ディテクタがアクティブまたは非アクティブになることがあります。Web アプリケーション ディテクタには、Blackboard ディテクタや LiveJournal ディテクタなどがあります。

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もあります。

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。また、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させることもできます。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化または非アクティブ化されることがあります。

ポート ディテクタには、chargen ディテクタや finger ディテクタなどがあります。

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

シスコが提供する FireSIGHT ベースのアプリケーション プロトコル ディテクタは、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 システムの更新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、シスコ提供のアプリケーション プロトコル ディテクタがアクティブ化または非アクティブ化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 ディテクタには、Jabber ディテクタや Steam ディテクタなどがあります。

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の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（45-11 ページ）
- 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（46-21 ページ）
- ディテクタの管理（46-26 ページ）

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

ネットワークでカスタム 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ヘッダーに `ApplicationName` という文字列が含まれることが分かっている場合、照合パターンとして `ApplicationName` という 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 プロトコルに対して**のみ**、ユーザ定義アプリケーション ディテクタを作成できます。それぞれの説明については、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。システムがサーバ トラフィックでアプリケーション プロトコルの検出および識別を開始するように、クライアント セッションにサーバからの応答パケットを含める必要があります。UDP トラフィックの場合、応答パケットの送信元がサーバとして指定されることに注意してください。

ユーザ定義のアプリケーション プロトコル ディテクタでは、ポートかパターンのどちらかをマッチングに使用する必要があります。既存のディテクタに基づいてディテクタを作成する場合であっても、どちら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 Defense Center にディテクタを作成した場合、そのディテクタをエクスポートして、この Defense Center にインポートできます。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は、エクスポートもインポートも**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（A-1 ページ）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

手順 1　[ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）] を選択します。

[ディテクタ（Detectors）] ページが表示されます。

手順 2　[ディテクタの作成（Create Detector）] をクリックします。

[ディテクタの作成（Create Detector）] ページが表示されます。

手順 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（46-22 ページ）を参照してください。

手順 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。

ユーザ定義アプリケーションの作成（46-23 ページ）を参照してください。

手順 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（46-24 ページ）を参照してください。

手順 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（46-24 ページ）を参照してください。

手順 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（46-25 ページ）を参照してください。

手順 8　[保存（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）　システムがディテクタを使用してアプリケーション プロトコルのトラフィックを分析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化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（46-30 ページ）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化され、使用中は非アクティブ化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

ユーザ定義のアプリケーション プロトコル ディテクタそれぞれに名前を付け、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指定できます。

ユーザが提供する情報に加えて、Defense Center は、ディテクタがアクティブか非アクティブか、また、ポート ディテクタとパターン ディテクタのどちらであるかを識別します。ディテクタがポートとパターンを使用し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、Defense Center 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場合は、そのユーザが作成者になります。ディテクタをインポート、編集、および保存した場合も、そのユーザが作成者になります。

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

手順 1　[ディテクタの作成(Create Detector)] ページの [名前を入力(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。

手順 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)、[アプリケーション プロトコル(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(46-24 ページ)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、次の項ユーザ定義アプリケーションの作成の手順に進みます。

ユーザ定義アプリケーションの作成

ライセンス: FireSIGHT

ネットワーク上のカスタム アプリケーションを識別するユーザ定義アプリケーションを作成できます。また、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(45-11 ページ)を参照してください。

ユーザ定義アプリケーションを作成する方法:

アクセス: Admin/Discovery Admin

手順 1　[ディテクタの作成(Create Detector)] ページで、[追加(Add)] をクリックします。

[アプリケーション エディタ(Application Editor)] ポップアップ ウィンドウが表示されます。

手順 2　[名前(Name)] にカスタム アプリケーションの名前を入力します。

手順 3　[説明(Description)] にカスタム アプリケーションの説明を入力します。

手順 4　[ビジネスとの関連性(Business Relevance)] を選択します。

手順 5　[リスク(Risk)] を選択します。

手順 6　[カテゴリ(Categories)] の横にある [追加(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 [カテゴリ(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。

手順 7　オプションで、[タグ(Tags)] の横にある [追加(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 [タグ(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、[ディテクタの作成(Create Detector)] ページに戻ります。

手順 8　次の項(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。

ポートを指定しない場合は、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ります。詳細については、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（46-24 ページ）を参照してください。

アプリケーション プロトコル ディテクタの検出基準を指定する方法：

アクセス：Admin/Discovery Admin

手順 1　[ディテクタの作成（Create Detector）] ページで、[プロトコル（Protocol）] ドロップダウン リストから、ディテクタが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。

手順 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 [ポート（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。

手順 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（46-25 ページ）をスキップします。
- ディテクタの作成が完了したら、[保存（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。

システムがディテクタを使用してアプリケーション プロトコルのトラフィックを分析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化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（46-30 ページ）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パケットの見出しに特定のパターン文字列が含まれていることが判明している場合、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。

パターンを指定しない場合は、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ります。詳細については、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（46-24 ページ）を参照してください。

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

手順 1　[ディテクタの作成（Create Detector）] ページの [検出パターン（Detection Patterns）] セクションで、[追加（Add）] をクリックします。

[パターンの追加（Add Pattern）] ポップアップ ウィンドウが表示されます。

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

手順 3　[パターン文字列（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。

手順 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。

[オフセット（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、[オフセット（Offset）] フィールドに「4」と入力します。

手順 5　オプションで、さらにパターンを追加するには、手順 1 ～ 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。

手順 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、[保存（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）　システムがディテクタを使用してアプリケーション プロトコルのトラフィックを分析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化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（46-30 ページ）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、Defense Center 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

手順 1　[ディテクタの作成(Create Detector)] ページの [パケット キャプチャ(Packet Captures)] セクションで、[追加(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。

手順 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。

手順 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。

手順 4　必要に応じて手順 1 ～ 3 を繰り返し、その他の PCAP ファイルに対して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。

手順 5　ディテクタを保存するには、[保存(Save)] をクリックします。

(注)　システムがディテクタを使用してアプリケーション プロトコルのトラフィックを分析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化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(46-30 ページ)を参照してください。

ディテクタの管理

ライセンス: FireSIGHT

[ディテクタ(Detectors)] ページでディテクタを表示および管理します。

[ディテクタ(Detectors)] ページから、次の操作が可能です。

- 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
- シスコ提供の内部ディテクタのリストの表示
- シスコ提供のアプリケーション 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コピーを保存する
- 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、インポート済み、またはシスコ提供の 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

内部またはシスコ提供のアプリケーション 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

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

手順 1　[詳細（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（45-11 ページ）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

[ディテクタ（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

手順 1　[ディテクタ（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ています。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、[ディテクタ（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（Name）

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（Custom Filter）

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（3-16 ページ）を参照してください。

作成者（Author）

ディテクタを作成したユーザを基準にディテクタを検索します。次の方法で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*、シスコ提供の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ユーザが、そのディテクタの作成者になります。
- Any User。これは、シスコ提供ではないすべてのディテクタを表します。

状態（State）

状態（アクティブか非アクティブか）を基準に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（46-30 ページ）を参照してください。

タイプ（Type）

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）を基準に検索します。

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、シスコ提供の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、アクティブ化/非アクティブ化できるシスコ提供のアプリケーション 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 ディテクタの操作（46-19 ページ）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 プロトコルを基準に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（Category）

検出するアプリケーションに割り当てられたカテゴリを基準に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を基準に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）を基準に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）を基準に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

手順 1　[ディテクタ（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。

手順 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、[すべてオン（Check All）] を選択します。

手順 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

手順 1　[フィルタ（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、[すべてオフ（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

手順 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 [すべてクリア（Clear all）] をクリックします。

他のディテクタ ページへの移動

ライセンス：FireSIGHT

[ディテクタ（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 リンクを使用して追加のディテクタ ページを表示する方法について説明します。

アクセス：Admin/Discovery Admin

表 46-1　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

ディテクタを使用してネットワーク トラフィックを分析するには、その前に、ディテクタをアクティブ化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なっています。

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化できます。

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た場合、そのポリシーの適用時にそのアプリケーションに関するアクティブなディテクタがなければ、1 つ以上のディテクタが自動的にアクティブ化されます。同様に、適用済みポリシーでアプリケーションが使用されているときに、あるディテクタを非アクティブ化することでそのアプリケーションのアクティブ ディテクタがなくなってしまう場合には、そのディテクタを非アクティブ化できません。

ヒント　パフォーマンスを向上させるには、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、Web アプリケーションのディテクタをすべて非アクティブ化します。

ディテクタをアクティブ化または非アクティブ化する方法：

アクセス：Admin/Discovery Admin

手順 1　[ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）] を選択します。

[ディテクタ（Detectors）] ページが表示されます。

手順 2　アクティブ化または非アクティブ化するディテクタを見つけます。

アクティブ化または非アクティブ化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（46-26 ページ）を参照してください。

手順 3　次の選択肢があります。

- ディテクタを**アクティブ化**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**非アクティブ化**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化すると、それに依存するディテクタも無効にな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

手順 1　[ポリシー（Policies）] > [アプリケーション（Applications）] を選択します。

[ディテクタ（Detectors）] ページが表示されます。

手順 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（46-26 ページ）を参照してください。

手順 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 [編集（Edit）] をクリックします。

[アプリケーション ディテクタの編集（Edit Application Detector）] ページが表示されます。

手順 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（46-21 ページ）を参照してください。

手順 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、[保存（Save）] をクリックして変更を保存するか、[新規保存（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、[保存して再アクティブ化（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、[新規保存（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、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て、アプリケーション トラフィックを分析.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（46-30 ページ）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。シスコ提供のその他のディテクタは削除できません。ただし、それらの多くを非アクティブ化することはできます。

（注） 適用済みポリシーでディテクタが使用されている間は、そのディテクタを非アクティブ化したり、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

手順 1 [ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）] を選択します。

[ディテクタ（Detectors）] ページが表示されます。

手順 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、[削除（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（46-26 ページ）を参照してください。

手順 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 マップの情報を拡張できます。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（46-5 ページ）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 システム Host Input API Guide*』を参照してください。

インポートしたデータを影響の関連付け（相関）に含めるには、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（46-33 ページ）
- サードパーティ製品マッピングの管理（46-34 ページ）
- サードパーティの脆弱性のマッピング（46-37 ページ）
- カスタム製品マッピングの管理（46-38 ページ）

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、侵入データとディスカバリ 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それぞれ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は、以下の要件を考慮してください。

- ネットワーク アセット（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（46-34 ページ）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（46-36 ページ）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（46-37 ページ）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も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（63-33 ページ）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（46-38 ページ）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と製品、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（46-34 ページ）
- サード パーティ製品の修正のマッピング（46-36 ページ）

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には、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と、シスコの脆弱性情報がサードパーティ製品の名前に関連付けられます。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るようになります。

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、[ベンダー名（Vendor Name）] を `Apache`、[製品名（Product Name）] を `Tomcat` に設定し、[ベンダー（Vendor）] ドロップダウン リストから [Apache]、[製品（Product）] ドロップダウン リストから [Tomcat]、[バージョン（Version）] ドロップダウン リストから [6] を選択したサードパーティ 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（63-33 ページ）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 Defense Center でサードパーティ マッピングを作成した場合、そのマッピングをエクスポートして、この Defense Center 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（A-1 ページ）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

手順 1　[ポリシー(Policies)] > [アプリケーション ディテクタ(Application Detectors)] を選択し、[ユーザ サードパーティ マッピング(User Third-Party Mappings)] をクリックします。

[ユーザ サードパーティ マッピング(User Third-Party Mappings)] ページが表示されます。

手順 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 [編集(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、[製品マップ セットの作成(Create Product Map Set)] をクリックします。

[サードパーティ製品マッピングの編集(Edit Third-Party Product Mappings)] ページが表示されます。

手順 3　[マッピング セット名(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。

手順 4　[説明(Description)] フィールドに説明を入力します。

手順 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、[製品マップの追加(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 [編集(Edit)] をクリックします。

[製品マップの追加(Add Product Map)] ページが表示されます。

手順 6　[ベンダー文字列(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。

手順 7　[製品文字列(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。

手順 8　[バージョン文字列(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。

手順 9　[製品マッピング(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)。

- **ベンダー**
- **製品**
- **メジャー バージョン**
- **マイナー バージョン**
- **リビジョン バージョン**
- **ビルド(Build)**
- **パッチ**
- **内線番号**

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。

手順 10　[保存(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/

手順 1　[ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）] を選択し、[ユーザ サードパーティ マッピング（User Third-Party Mappings）] をクリックします。

[ユーザ サードパーティ マッピング（User Third-Party Mappings）] ページが表示されます。

手順 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 [編集（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、[製品マップ セットの作成（Create Product Map Set）] をクリックします。

[サードパーティ製品マッピングの編集（Edit Third-Party Product Mappings）] ページが表示されます。

手順 3　[マッピング セット名（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。

手順 4　[説明（Description）] フィールドに説明を入力します。

手順 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、[修正マップの追加（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 [編集（Edit）] をクリックします。

[修正マップの追加（Add Fix Map）] ページが表示されます。

手順 6　[サードパーティ修正名（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。

手順 7　[製品マッピング（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）。

- **ベンダー**
- **製品**
- **メジャー バージョン**
- **マイナー バージョン**
- **リビジョン バージョン**
- **ビルド（Build）**
- **パッチ**
- **内線番号**

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。

手順 8　[保存（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（45-37 ページ）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（63-33 ページ）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、クライアントは影響評価に使用されますが、サードパーティ製クライアントの脆弱性を影響評価に使用することはできません。

ヒント　すでに別の Defense Center でサードパーティ マッピングを作成した場合、そのマッピングをエクスポートして、この Defense Center 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（A-1 ページ）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

手順 1　[ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）] を選択し、[ユーザ サードパーティ マッピング（User Third-Party Mappings）] をクリックします。

[ユーザ サードパーティ マッピング（User Third-Party Mappings）] ページが表示されます。

手順 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 [編集（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、[脆弱性マップ セットの作成（Create Vulnerability Map Set）] をクリックします。

[サードパーティ脆弱性マッピングの編集（Edit Third-Party Vulnerability Mappings）] ページが表示されます。

手順 3　[脆弱性マップの追加（Add Vulnerability Map）] をクリックします。

[脆弱性マップの追加（Add Vulnerability Map）] ポップアップ ウィンドウが表示されます。

手順 4　[脆弱性 ID（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。

手順 5　[脆弱性の説明（Vulnerability Description）] フィールドに説明を入力します。

手順 6　オプションで、[Snort 脆弱性 ID マッピング（Snort Vulnerability ID Mappings）] フィールドに署名 ID を入力します。

手順 7　オプションで、[シスコ脆弱性 ID マッピング（**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。

手順 8　オプションで、[Bugtraq 脆弱性 ID マッピング（Bugtraq Vulnerability ID Mappings）] フィールドに Bugtraq ID 番号を入力します。

手順 9　[追加（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、次のトピックを参照してください。

- カスタム製品マッピングの作成（46-38 ページ）
- カスタム製品マッピング リストの編集（46-39 ページ）
- 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（46-40 ページ）

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 マップ内のサーバを VDB 内のベンダーおよび製品にマッピングできない場合、サーバの識別時にシステムが使用するマッピングを手動で作成することができます。カスタム製品マッピングをアクティブ化すると、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出現するネットワーク マップ内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出現に適用されます。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（46-37 ページ）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または無効にします。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の作成後に、カスタム製品マッピング リストをアクティブ化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化すると、指定されたベンダー文字列が出現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出現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　この機能を使用すると、ルールの SID を別の脆弱性に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

手順 1　[ポリシー(Policies)] > [アプリケーション ディテクタ(Application Detectors)] を選択し、[カスタム製品マッピング(Custom Product Mappings)] をクリックします。

[カスタム製品マッピング(Custom Product Mappings)] ページが表示されます。

手順 2　[カスタム製品マッピング リストの作成(Create Custom Product Mapping List)] をクリックします。

[カスタム製品マッピング リストの編集(Edit Custom Product Mappings List)] ページが表示されます。

手順 3　名前を [カスタム製品マッピング リスト名(Custom Product Mapping List Name)] フィールドに入力します。

手順 4　[ベンダー文字列の追加(Add Vendor String)] をクリックします。

[ベンダー文字列の追加(Add Vendor String)] ポップアップ ウィンドウが表示されます。

手順 5　[ベンダー文字列(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。

手順 6　[ベンダー(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。

手順 7　[製品(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。

手順 8　[追加(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。

手順 9　オプションで、さらにベンダー文字列のマッピングをリストに追加するには、必要に応じて手順 4 ～ 8 を繰り返します。

手順 10　終了したら、[保存(Save)] をクリックします。

[カスタム製品マッピング(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

手順 1　[ポリシー(Policies)] > [アプリケーション ディテクタ(Application Detectors)] を選択し、[カスタム製品マッピング(Custom Product Mappings)] をクリックします。

[カスタム製品マッピング(Custom Product Mappings)] ページが表示されます。

手順 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。

[カスタム製品マッピング リストの編集(Edit Custom Product Mappings List)] ページが表示されます。

手順 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(46-38 ページ)を参照してください。

手順 4　終了したら、[保存(Save)] をクリックします。

[カスタム製品マッピング(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化または無効化できます。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 リストを有効化または無効化する方法:

アクセス: Admin

手順 1　[ポリシー(Policies)] > [アプリケーション ディテクタ(Application Detectors)] を選択し、[カスタム製品マッピング(Custom Product Mappings)] をクリックします。

[カスタム製品マッピング(Custom Product Mappings)] ページが表示されます。

手順 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化するには、[有効化(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化するには、[無効化(Deactivate)] をクリックします。