



# ネットワーク検出ポリシー

以下のトピックでは、ネットワーク検出ポリシーを作成、設定、管理する方法について説明します。

- [概要：ネットワーク検出ポリシー \(1 ページ\)](#)
- [ネットワーク検出ポリシーの要件と前提条件 \(2 ページ\)](#)
- [ネットワーク検出のカスタマイズ \(2 ページ\)](#)
- [ネットワーク検出ルール \(4 ページ\)](#)
- [高度なネットワーク検出オプションの設定 \(14 ページ\)](#)
- [ネットワーク検出戦略のトラブルシューティング \(25 ページ\)](#)

## 概要：ネットワーク検出ポリシー

Management Center 上のネットワーク検出ポリシーは、システムが組織のネットワーク アセットに関するデータを収集する方法と、どのネットワークセグメントとポートをモニタ対象とするかを制御します。

システムがモニターしてトラフィック内のネットワークデータに基づいて検出データを生成するネットワークとポート、およびポリシーを展開するゾーンは、ポリシー内の検出ルールで指定します。ルール内では、ホスト、アプリケーション、権限のないユーザを検出するかどうかを設定できます。検出からネットワークとゾーンを除外するルールを作成できます。NetFlow エクスポートからのデータの検出を設定して、ネットワーク上でユーザデータが検出されるトラフィックのプロトコルを制限できます。

ネットワーク検出ポリシーに用意されている単一のデフォルトルールは、すべてのモニタ対象トラフィックからアプリケーションを検出するように設定されています。このルールが除外するネットワーク、ゾーン、ポートはなく、ホストとユーザの検出も設定されていません。また、このルールはNetFlow エクスポートをモニタするように設定されてはいません。このポリシーは、管理対象デバイスが Management Center に登録されると、デフォルトでそのデバイスに導入されます。ホストまたはユーザデータの収集を開始するには、検出ルールを追加または変更して、ポリシーをデバイスに再展開する必要があります。

ネットワーク検出の範囲を調整する場合は、追加の検出ルールを作成して、デフォルトルールを変更または削除できます。

管理対象デバイスごとのアクセスコントロールポリシーは、そのデバイスに許可されたトラフィック、つまり、ネットワーク検出を使用してモニタ可能なトラフィックを定義することに注意してください。アクセスコントロールを使用して特定のトラフィックをブロックすると、システムでホスト、ユーザ、またはアプリケーションのアクティビティに関するトラフィックを検査できなくなります。たとえば、アクセスコントロールポリシーでソーシャルネットワークングアプリケーションへのアクセスをブロックすると、システムはそれらのアプリケーションに関する検出データを一切提供できなくなります。

検出ルールでトラフィックベースのユーザ検出を有効にすると、一連のアプリケーションプロトコル全体のトラフィック内のユーザログインアクティビティを通して権限のないユーザを検出できます。必要に応じて、すべてのルールにわたって特定のプロトコル内の検出を無効にできます。一部のプロトコルを無効にすると、Management Center モデルに関連付けられたユーザ制限に達するのを防ぐのに役立ち、他のプロトコルからのユーザに使用可能なユーザカウントを確保できます。

詳細ネットワーク検出設定を使用すれば、記録するデータの種類、検出データの保存方法、アクティブにする侵害の兆候 (IOC) ルール、影響評価に使用する脆弱性マッピング、送信元からの検出データが競合していた場合の対処を管理できます。また、ホスト入力の送信元や NetFlow エクスポートをモニター対象として追加することもできます。

## ネットワーク検出ポリシーの要件と前提条件

### モデルのサポート

任意

### サポートされるドメイン

リーフ

### ユーザの役割

- 管理者
- 検出管理者 (Discovery Admin)

## ネットワーク検出のカスタマイズ

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システムのベンダーとバージョンの定義にマッピングした場合でも、インポートされたサードパーティ製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は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、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。

## ネットワーク検出ポリシーの設定

### 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

**ステップ 2** ポリシーの次のコンポーネントを設定します。

- 検出ルール : [ネットワーク検出ルールの設定 \(4 ページ\)](#) を参照してください。
- ユーザのトラフィックベースの検出 : [トラフィックに基づくユーザー検出の設定 \(14 ページ\)](#) を参照してください。
- 高度なネットワーク検出オプション : [高度なネットワーク検出オプションの設定 \(14 ページ\)](#) を参照してください。
- カスタム オペレーティング システム定義 (フィンガープリント) : [クライアント用のカスタム フィンガープリントの作成およびサーバ用のカスタム フィンガープリントの作成](#) を参照してください。

## ネットワーク検出ルール

ネットワーク検出ルールを使用すれば、ネットワーク マップに対して検出される情報を調整し、必要な特定のデータだけを含めるようにすることができます。ネットワーク検出ポリシー内のルールは順番に評価されます。モニタリング基準が重複したルールを作成できますが、その場合はシステム パフォーマンスに影響する可能性があります。

モニタリングからホストまたはネットワークを除外すると、そのホストまたはネットワークがネットワークマップに表示されず、それに対するイベントが報告されません。ただし、ローカル IP のホスト検出ルールが無効になっている場合、検出エンジンインスタンスは既存のホストデータを使用せずに各フローから新たにデータを構築するため、より高い処理負荷の影響を受けます。

モニタリングからロードバランサ（またはロードバランサ上の特定のポート）と NAT デバイスを除外することを推奨します。これらのデバイスは紛らわしいイベントを過剰に生成するため、データベースがいっぱいになったり、**Management Center** が過負荷になったりする可能性があります。たとえば、モニター対象 NAT デバイスが短期間にオペレーティング システムの複数の更新を表示する場合があります。ロードバランサと NAT デバイスの IP アドレスがわかっている場合は、モニタリングからそれらを除外できます。



---

**ヒント** システムは、ネットワーク トラフィックを検査することにより、複数のロードバランサと NAT デバイスを識別できます。

---

加えて、カスタム サーバフィンガープリントを作成する必要がある場合は、フィンガープリントを行っているホストとの通信に使用されている IP アドレスをモニタリングから一時的に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。フィンガープリントを作成したら、その IP アドレスをモニタするようにポリシーを設定し直すことができます。

シスコでは、NetFlow エクスポートと管理対象デバイスを使用して、同じネットワークセグメントをモニターしないことも推奨しています。重複しないルールを使用してネットワーク検出ポリシーを設定するのが理想です。管理対象デバイスによって生成された重複接続ログはシステムによって破棄されます。ただし、管理対象デバイスと NetFlow エクスポートの両方で検出された接続に関する重複接続ログを破棄することはできません。

## ネットワーク検出ルールの設定

検出ルールを設定し、ニーズに合わせてホスト データとアプリケーション データの検出を調整できます。



---

**ヒント** ほとんどの場合、RFC 1918 のアドレスに検出を制限することを推奨します。

---

### 始める前に

- ネットワークデータを検出するトラフィックの接続を記録していることを確認します。  
『Cisco Secure Firewall Management Center アドミニストレーションガイド』の「*Best Practices for Connection Logging*」を参照してください。
- エクスポートされた NetFlow レコードを収集する場合は、[NetFlow エクスポートのネットワーク検出ポリシーへの追加 \(20 ページ\)](#) の説明に従って NetFlow エクスポートを追加します。
- 検出パフォーマンスグラフを表示するには、検出ルールでホスト、ユーザー、およびアプリケーションを有効にする必要があります。これは、システムパフォーマンスに影響を与える可能性があることに注意してください。

### 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

**ステップ 2** [ルールの追加 (Add Rule)] をクリックします。

**ステップ 3** [アクションと検出されるアセット \(5 ページ\)](#) の説明に従って、ルールの [アクション (Action)] を設定します。

**ステップ 4** オプションの検出パラメータを設定します。

- ルールアクションを特定のネットワークに制限します。[モニター対象ネットワークの制限 \(7 ページ\)](#) を参照してください。
- ルールアクションを特定のゾーン内のトラフィックに制限します。[ネットワーク検出ルールのゾーンの設定 \(11 ページ\)](#) を参照してください。
- ポートをモニタリングから除外します。[ネットワーク検出ルールでのポート除外 \(9 ページ\)](#) を参照してください。
- NetFlow データ検出のルールの設定します。[NetFlow データ検出のルールの設定 \(8 ページ\)](#) を参照してください。

**ステップ 5** [保存 (Save)] をクリックします。

### 次のタスク

- 設定変更を展開します。[設定変更の展開](#) を参照してください。

## アクションと検出されるアセット

検出ルールを設定する場合は、ルールのアクションを選択する必要があります。アクションの効果は、管理対象デバイスと NetFlow エクスポートのどちらからデータを検出するルールを使用しているかによって異なります。

次の表に、これら2つのシナリオで指定されたアクション設定を使用したルールで検出されるアセットの説明を示します。

表 1: 検出ルールアクション

操作	オプション	管理対象デバイス	NetFlow エクスポート
除外 (Exclude)	--	指定されたネットワークをモニタリング対象から除外します。接続の発信元ホストまたは宛先ホストを検出から除外すると、接続は記録されますが、除外したホストの検出イベントは作成されません。	指定されたネットワークをモニタリング対象から除外します。接続の発信元ホストまたは宛先ホストを検出から除外すると、接続は記録されますが、除外したホストの検出イベントは作成されません。
Discover	ホスト (Hosts)	検出イベントに基づいて、ネットワークマップにホストを追加します。(任意。ユーザ検出が有効になっていない場合は必須)。	NetFlow レコードに基づいて、ネットワークマップにホストを追加し、接続をログに記録します。(必須)
Discover	アプリケーション	アプリケーション検出に基づいて、ネットワークマップにアプリケーションを追加します。アプリケーションも検出しないルールでは、ホストまたはユーザを検出できないことに注意してください。(必須)	NetFlow レコードと /etc/sf/services 内のポートとアプリケーションプロトコルの関連付けに基づいて、ネットワークマップにアプリケーションプロトコルを追加します。(オプション)
Discover	Users	ネットワーク検出ポリシーで設定されたユーザープロトコルに関するトラフィックベースの検出に基づいてユーザーをユーザーテーブルに追加し、ユーザーアクティビティをログに記録します。(オプション)	適用対象外
NetFlow 接続のロギング (Log NetFlow Connections)	--	適用対象外	NetFlow 接続のみをログに記録します。ホストまたはアプリケーションは検出しません。

ルールを使用して管理対象デバイスのトラフィックをモニタする場合は、アプリケーションロギングが必要です。ルールを使用してユーザをモニタする場合は、ホストロギングが必要です。ルールを使用して、エクスポートされた NetFlow レコードをモニタする場合は、ユーザをログに記録するように設定することはできず、アプリケーションロギングは任意です。



(注) ネットワーク検出ポリシーの [アクション (Action)] の設定に基づいて、エクスポートされた NetFlow レコードで接続が検出されます。アクセスコントロールポリシーの設定に基づいて、管理対象デバイス ラフィックで接続が検出されます。

## モニター対象ネットワーク

検出ルールは、モニター対象アセットの検出を、指定されたネットワーク上のホストとの間のトラフィックだけを対象に行います。検出ルールでは、指定されたネットワーク内の1つ以上のIPアドレスが割り当てられた接続に対して検出が行われ、モニター対象ネットワーク内のIPアドレスに対してのみイベントが生成されます。デフォルトの検出ルールでは、モニターされているすべてのトラフィックのアプリケーションを検出します（すべてのIPv4トラフィックについては0.0.0.0/0、すべてのIPv6トラフィックについては::/0）。

NetFlow 検出を処理し、接続データだけを記録するルールを設定すると、システムは、指定のネットワークの接続元と接続先のIPアドレスを記録します。ネットワーク検出ルールがNetFlow ネットワーク接続を記録する唯一の方法を提供することに注意してください。

また、ネットワーク オブジェクトまたはオブジェクト グループを使用してモニター対象ネットワークを指定することもできます。

### モニター対象ネットワークの制限

すべての検出ルールに1つ以上のネットワークを含める必要があります。

#### 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

**ステップ 2** [ルールの追加 (Add Rule)] をクリックします。

**ステップ 3** [ネットワーク (Networks)] をクリックします（表示されていない場合）。

**ステップ 4** (オプション) [使用可能なネットワーク (Available Networks)] リストにネットワークオブジェクトを追加します。詳細については、「[ディスカバリ ルール設定時にネットワーク オブジェクトを作成する \(8 ページ\)](#)」を参照してください。

ネットワーク検出ポリシーで使用されるネットワークオブジェクトを変更した場合、その変更は設定の変更を展開するまで反映されません。

**ステップ 5** ネットワークを指定します。

- [使用可能なネットワーク (Available Networks)] リストからネットワークを選択します。ネットワークがすぐにリストに表示されない場合は、[Reload] (🔄) をクリックします。
- [使用可能なネットワーク (Available Networks)] ラベルの下にあるテキスト ボックスに IP アドレスを入力します。

**ステップ 6** [追加 (Add)] をクリックします。

**ステップ 7** [保存 (Save)] をクリックします。

#### 次のタスク

- 設定変更を展開します [設定変更の展開](#) を参照してください。

## NetFlow データ検出のルールの設定

システムは、NetFlow エクスポートからのデータを使用して、接続および検出イベントを生成し、ネットワークマップにホストとアプリケーションのデータを追加できます。

検出ルール内で NetFlow エクスポートを選択する場合、ルールは指定されたネットワークの NetFlow データの検出に制限されます。NetFlow デバイスを選択すると使用可能なルールアクションが変更されるため、モニタする NetFlow デバイスを選択してからルール動作の他の側面を設定します。NetFlow エクスポートをモニタするためのポートの除外を設定することはできません。

### 始める前に

- NetFlow-enabled デバイスをネットワーク検出ポリシーに追加します。[NetFlow エクスポートのネットワーク検出ポリシーへの追加 \(20 ページ\)](#) を参照してください。

### 手順

---

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

**ステップ 2** [ルールの追加 (Add Rule)] をクリックします。

**ステップ 3** [NetFlow デバイス (NetFlow Device)] を選択します。

**ステップ 4** [NetFlow デバイス (NetFlow Device)] ドロップダウンリストから、モニタする NetFlow エクスポートの IP アドレスを選択します。

**ステップ 5** システムの管理対象デバイスで収集する NetFlow データのタイプを指定します。

- 接続のみ: [アクション (Action)] ドロップダウン リストから Log NetFlow Connections を選択します。
- ホスト、アプリケーション、および接続: [アクション (Action)] ドロップダウン リストから Discover を選択します。[ホスト (Hosts)] チェックボックスが自動的にオンになり、接続データの収集が有効になります。オプションで、[アプリケーション] チェックボックスをオンにして、アプリケーション データを収集できます。

**ステップ 6** [保存 (Save)] をクリックします。

---

### 次のタスク

- 設定変更を展開します。[設定変更の展開](#) を参照してください。

## ディスカバリ ルール設定時にネットワーク オブジェクトを作成する

新規ネットワーク オブジェクトを再使用可能なネットワーク オブジェクトおよびグループのリストに追加することで、検出ルールに表示される使用可能なネットワークのリストにそれらのオブジェクトを追加できます。

## 手順

- ステップ1 [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。
- ステップ2 [ネットワーク (Networks)] で、[ルール追加 (Add Rule)] をクリックします。
- ステップ3 [使用可能なネットワーク (Available Networks)] の横にある **Add (+)** をクリックします。
- ステップ4 [ネットワークオブジェクトの作成](#)の説明に従って、ネットワークオブジェクトを作成します。
- ステップ5 [ネットワーク検出ルール設定 \(4 ページ\)](#) の説明に従って、ネットワーク検出ルールの追加を完了します。

## ポート除外

モニタリングからホストを除外できるのと同様に、モニタリングから特定のポートを除外できます。次に例を示します。

- ロードバランサは短期間に同じポート上の複数のアプリケーションを報告する可能性があります。モニタリングからそのポートを除外する (Web ファームを処理するロードバランサ上のポート 80 を除外するなど) ようにネットワーク検出ルールを設定できます。
- 組織で特定の範囲のポートを使用するカスタムクライアントを使用しているとします。このクライアントからのトラフィックが紛らわしいイベントを過剰に生成する場合は、モニタリングからそれらのポートを除外できます。同様に、DNS トラフィックをモニタしないように設定することもできます。この場合は、検出ポリシーがポート 53 をモニタしないように、ルールを設定します。

除外するポートを追加するときには、[利用可能なポート (Available Ports)] リストから再利用可能なポートオブジェクトを選択するのか、送信元または宛先除外リストにポートを直接追加するのか、新しい再利用可能なポートを作成してからそれを除外リストに移動するのかを決定できます。



(注) NetFlow データの検出を処理するルールでポートを除外することはできません。

### ネットワーク検出ルールでのポート除外

NetFlow データ検出を処理するルールにあるポートを除外することはできません。

## 手順

- ステップ1 [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。
- ステップ2 [ルール追加 (Add Rule)] をクリックします。
- ステップ3 [ポート除外 (Port Exclusions)] をクリックします。

**ステップ 4** 必要に応じて、[ディスカバリ ルール設定時にポート オブジェクトを作成する \(10 ページ\)](#) で説明されているように、使用可能なポート リストにポート オブジェクトを追加します。

**ステップ 5** 次のいずれかの方法を使用して、モニタリング対象から特定の送信元ポートを除外します。

- [使用可能なポート (Available Ports) ] リストから1つまたは複数のポートを選択して、[送信元に追加 (Add to Source) ] をクリックします。
- ポート オブジェクトを追加せずに特定の送信元ポートからのトラフィックを除外するには、[選択済の送信元ポート リスト (Selected Source Ports) ] で、[プロトコル (Protocol) ] を選択し、[ポート (Port) ] 番号 (1 から 65535 の数値) を入力して、[追加 (Add) ] をクリックします。

**ステップ 6** 次のいずれかの方法を使用して、モニタリング対象から特定の宛先ポートを除外します。

- [使用可能なポート (Available Ports) ] リストから1つまたは複数のポートを選択して、[宛先に追加 (Add to Destination) ] をクリックします。
- ポート オブジェクトを追加せずに特定の宛先ポートからのトラフィックを除外するには、[選択済の宛先ポート リスト (Selected Destination Ports) ] で、[プロトコル (Protocol) ] を選択し、[ポート (Port) ] 番号を入力して、[追加 (Add) ] をクリックします。

**ステップ 7** [保存 (Save) ] をクリックして、変更を保存します。

### 次のタスク

- 設定変更を展開します [設定変更の展開](#) を参照してください。

## ディスカバリ ルール設定時にポート オブジェクトを作成する

新規ポートオブジェクトを、システム内の任意の場所で使用できる再使用可能なポートオブジェクトおよびグループのリストに追加することで、検出ルールに表示される使用可能なポートのリストにそれらのオブジェクトを追加できます。

### 手順

**ステップ 1** [ポリシー (Policies) ] > [ネットワーク検出 (Network Discovery) ] を選択します。

**ステップ 2** [ネットワーク (Networks) ] で、[ルール追加 (Add Rule) ] をクリックします。

**ステップ 3** [ポート除外 (Port Exclusions) ] をクリックします。

**ステップ 4** [利用可能なポート (Available Ports) ] リストにポートを追加するには、**Add (+)** をクリックします。

**ステップ 5** 名前を入力します。

**ステップ 6** [プロトコル (Protocol) ] フィールドで、除外するトラフィックのプロトコルを指定します。

**ステップ 7** [ポート (Port) ] フィールドに、モニタリングから除外するポートを入力します。

単一のポート、ダッシュ (-) を使用したポートの範囲、またはポートとポート範囲のカンマ区切りのリストを指定できます。許容されるポート値は 1 ~ 65535 です。

**ステップ 8** [保存 (Save) ] をクリックします。

**ステップ 9** ポートがすぐにリストに表示されない場合は、[更新 (Refresh) ] をクリックします。

---

#### 次のタスク

- 設定変更を展開します [設定変更の展開](#) を参照してください。

## ネットワーク検出ルールのゾーン

パフォーマンスを向上させるために、ルール内の監視対象ネットワークに物理的に接続されている管理対象デバイス上のセンシング インターフェイスがルール内のゾーンに含まれるように、検出ルールを設定することができます。

残念ながら、ネットワーク設定の変更は通知されないことがあります。ネットワーク管理者が通知せずにルーティングやホストの変更によりネットワーク設定を変更した場合、正しいネットワーク検出ポリシー設定を完全に把握するのが難しくなります。管理対象デバイス上のセンシングインターフェイスがどのようにネットワークに物理的に接続されているかが不明な場合は、ゾーンの設定はデフォルト値のままにしておいてください。このデフォルト値によって、システムは展開環境内のすべてのゾーンに検出ルールを展開します（ゾーンが除外されない場合、システムではすべてのゾーンに検出ポリシーを展開します。）。

### ネットワーク検出ルールのゾーンの設定

#### 手順

---

**ステップ 1** [ポリシー (Policies) ] > [ネットワーク検出 (Network Discovery) ] を選択します。

**ステップ 2** [ルールの追加 (Add Rule) ] をクリックします。

**ステップ 3** [ゾーン (Zones) ] をクリックします。

**ステップ 4** [使用可能なゾーン (Available Zones) ] リストでゾーンを選択します。

**ステップ 5** [保存 (Save) ] をクリックして、変更を保存します。

---

#### 次のタスク

- 設定変更を展開します [設定変更の展開](#) を参照してください。

## トラフィック ベース検出のアイデンティティ ソース

トラフィックベースの検出は、システムでサポートされている唯一の権限のないアイデンティティソースです。トラフィックベース検出を設定すると、管理対象デバイスは、指定したネットワークでのLDAP、AIM、POP3、IMAP、Oracle、SIP (VoIP) 、FTP、HTTP、MDNS、SMTPのログインを検出します。トラフィックベースの検出から取得されたデータは、ユーザ認識にのみ使用できます。権威のあるアイデンティティソースとは異なり、トラフィックベースの

検出はネットワーク検出ポリシーで設定します。[トラフィックに基づくユーザー検出の設定 \(14 ページ\)](#) を参照してください。

次の制限事項に注意してください。

- トラフィック ベースの検出では、LDAP 接続に対する Kerberos ログインのみを LDAP 認証として解釈します。また、管理対象デバイスは、SSL や TLS などのプロトコルを使用して暗号化された LDAP 認証を検出できません。
- トラフィック ベースの検出では OSCAR プロトコルを使用した AIM ログインだけを検出します。TOC2 を使用する AIM ログインは検出できません。
- トラフィック ベースの検出では SMTP ログインを制限することができません。これは、ユーザが SMTP ログインに基づいてデータベースに追加されていないためです。システムが SMTP ログインを検出しても、一致する電子メールアドレスのユーザがデータベース内に存在しなければ、そのログインは記録されません。

トラフィック ベースの検出は、失敗したログイン試行も記録します。失敗ログイン試行で新しいユーザがデータベース内のユーザのリストに追加されることはありません。トラフィック ベースの検出により検出された失敗ログインアクティビティのユーザー アクティビティタイプは [失敗したユーザー ログイン (Failed User Login)] です。



(注) システムは失敗した HTTP ログインと成功した HTTP ログインを区別できません。HTTP ユーザ情報を表示するには、トラフィック ベースの検出設定で [失敗したログイン試行の取得 (Capture Failed Login Attempts)] を有効にする必要があります。



**注意** ネットワーク検出ポリシーを使用して、HTTP、FTP、MDNS プロトコルを介した非権限、トラフィック ベースのユーザ検出を有効/無効にすると 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細は[Snort の再起動によるトラフィックの動作](#)を参照してください。

### トラフィック ベースの検出データ

デバイスがトラフィック ベースの検出を使用してログインを検出すると、次の情報をユーザー アクティビティとして記録するために Management Center に送信します。

- ログインで識別されたユーザー名。
- ログインの時刻。
- ログインに関する IP アドレス。このアドレスは、ユーザーのホスト (LDAP、POP3、IMAP、および AIM ログインの場合)、サーバー (HTTP、MDNS、FTP、SMTP および

Oracle ログインの場合)、またはセッション発信元 (SIP ログインの場合) の IP アドレスになります。

- ユーザーの電子メールアドレス (POP3、IMAP、および SMTP ログインの場合)。
- ログインを検出したデバイスの名前。

ユーザがすでに検出されている場合、Management Centerはそのユーザのログイン履歴を更新します。Management Center は POP3 および IMAP ログイン内の電子メールアドレスを使用して LDAP ユーザに関連付ける場合があることに注意してください。これは、Management Center が新しい IMAP ログインを検出して、その IMAP ログイン内の電子メールアドレスが既存の LDAP ユーザのアドレスと一致した場合は、IMAP ログインで新しいユーザが作成されるのではなく、LDAP ユーザの履歴が更新されることを意味します。

ユーザが以前に検出されなかった場合、Management Center はユーザ データベースにユーザを追加します。AIM、SIP、Oracle ログインでは、常に新しいユーザ レコードが作成されます。これは、それらのログインイベントには Management Center が他のログインタイプに関連付けることができるデータが含まれていないためです。

Management Center は、次の場合に、ユーザ アイデンティティまたはユーザ ID を記録しません。

- そのログインタイプを無視するようにネットワーク検出ポリシーを設定した場合
- 管理対象デバイスが SMTP ログインを検出したものの、ユーザーデータベースに電子メールアドレスが一致する、検出済みの LDAP、POP3、または IMAP ユーザーが含まれていない場合

ユーザ データはユーザ テーブルに追加されます。

### トラフィック ベースの検出戦略

ユーザーアクティビティを検出するプロトコルを制限して、検出するユーザーの総数を削減することにより、ほぼ完全なユーザー情報を提供していると思われるユーザーに焦点を絞ることができます。プロトコルの検出を制限すると、ユーザ名の散乱を最小限に抑え、Management Center 上の記憶域を節約することができます。

トラフィック ベースの検出プロトコルを選択する際には、以下を検討してください。

- AIM、POP3、IMAPなどのプロトコル経由でユーザ名を取得すると、契約業者、訪問者、およびその他のゲストからのネットワークアクセスによって組織に無関係なユーザ名が収集される可能性があります。
- AIM、Oracle、および SIP ログインは、無関係なユーザ レコードを作成する可能性があります。この現象は、このようなログインタイプが、システムが LDAP サーバから取得するユーザメタデータのいずれにも関連付けられていないうえ、管理対象デバイスが検出するその他のログインタイプに含まれている情報のいずれにも関連付けられていないために発生します。そのため、Management Centerは、これらのユーザーとその他のユーザータイプを関連付けることができません。

## トラフィックに基づくユーザー検出の設定

ネットワーク検出ルールでトラフィックベースのユーザー検出を有効にすると、ホスト検出が自動で有効になります。トラフィックベースの検出の詳細については、[トラフィックベース検出のアイデンティティソース \(11 ページ\)](#) を参照してください。

### 手順

- 
- ステップ 1 [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。
  - ステップ 2 [ユーザー (Users)] をクリックします。
  - ステップ 3 [編集 (Edit)] (✎) をクリックします。
  - ステップ 4 ログインを検出するプロトコルのチェックボックスをオンにするか、ログインを検出しないプロトコルのチェックボックスをオフにして、[失敗したログイン試行のキャプチャ (Capture Failed Login Attempts)] を有効にするかどうかを選択します。
  - ステップ 5 [保存 (Save)] をクリックします。
- 

### 次のタスク



**注意** ネットワーク検出ポリシーを使用して、HTTP、FTP、MDNS プロトコルを介した非権限、トラフィックベースのユーザー検出を有効/無効にすると設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細は[Snort の再起動によるトラフィックの動作](#)を参照してください。

- [ネットワーク検出ルールの設定 \(4 ページ\)](#) の説明に従って、ユーザーを検出するようにネットワーク検出ルールを設定します。
- 設定変更を展開します [設定変更の展開](#) を参照してください。

## 高度なネットワーク検出オプションの設定

ネットワーク検出ポリシーの [詳細 (Advanced)] を使用すれば、検出するイベント、検出データの保存期間と更新頻度、影響相関に使用する脆弱性マッピング、およびオペレーティングシステム ID とサーバー ID の競合の解決方法に関するポリシー全体の設定を構成できます。加えて、ホスト入力ソースと NetFlow エクスポートを追加して、他のソースからのデータのインポートを許可できます。



(注) 検出イベントとユーザ活動イベントのデータベースイベント制限はシステム構成で設定されません。

### 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

**ステップ 2** [詳細設定 (Advanced)] をクリックします。

**ステップ 3** 変更する設定の隣にある[編集 (Edit)] (✎) またはAdd (+) をクリックします。

- [データ ストレージ設定 (Data Storage Settings)] : [ネットワーク検出データ ストレージの設定 \(23 ページ\)](#) の説明に従って、設定を更新します。
- [イベント ロギング設定 (Event Logging Settings)] : [ネットワーク検出イベント ロギングの設定 \(23 ページ\)](#) の説明に従って、設定を更新します。
- [全般設定 (General Settings)] : [ネットワーク検出の一般設定を行う \(16 ページ\)](#) の説明に従って、設定を更新します。
- [ID 競合設定 (Identity Conflict Settings)] : [ネットワーク検出アイデンティティ競合の解決の設定 \(17 ページ\)](#) の説明に従って、設定を更新します。
- [侵害の兆候設定 (General Settings)] : [侵害の兆候ルールの有効化 \(19 ページ\)](#) の説明に従って、設定を更新します。
- [NetFlow エクスポート (NetFlow Exporters)] : [NetFlow エクスポートのネットワーク検出ポリシーへの追加 \(20 ページ\)](#) の説明に従って、設定を更新します。
- [OS およびサーバの ID ソース (OS and Server Identity Sources)] : [ネットワーク検出 OS およびサーバー アイデンティティ ソースの追加 \(24 ページ\)](#) の説明に従って、設定を更新します。
- [影響評価に使用する脆弱性 (Vulnerabilities to use for Impact Assessment)] : [ネットワーク検出の脆弱性影響評価の有効化 \(18 ページ\)](#) の説明に従って、設定を更新します。

**ステップ 4** [保存 (Save)] をクリックします。

### 次のタスク

- 設定変更を展開します [設定変更の展開](#) を参照してください。

## ネットワーク検出の一般設定

一般設定は、システムがネットワーク マップを更新する頻度と、検出中にサーババナーをキャプチャするかどうかを制御します。

### [バナーのキャプチャ (Capture Banners)]

サーバー ベンダーとバージョン（「バナー」）をアダプタイズするネットワーク トラフィックからの見出し情報をシステムで保存させる場合、このチェックボックスをオンにします。この情報は、収集された情報に追加のコンテキストを提供できます。サーバ詳細にアクセスすることによって、ホストに関して収集されたサーババナーにアクセスできます。

### [アップデート間隔 (Update Interval)]

システムが情報を更新する時間間隔（ホストの IP アドレスのいずれかが最後に検出された時点、アプリケーションが使用された時点、アプリケーションのヒット数など）。デフォルト設定は 3600 秒（1 時間）です。

更新タイムアウトの時間間隔を短く設定すると、より正確な情報がホスト画面に表示されますが、より多くのネットワーク イベントが生成されることに注意してください。

## ネットワーク検出の一般設定を行う

### 手順

- ステップ 1 [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。
- ステップ 2 [詳細設定 (Advanced)] をクリックします。
- ステップ 3 [全般設定 (General Settings)] の横にある[編集 (Edit)] (✎) をクリックします。
- ステップ 4 [ネットワーク検出の一般設定 \(15 ページ\)](#) の説明に従って設定を更新します。
- ステップ 5 [保存 (Save)] をクリックして、全般設定を保存します。

### 次のタスク

- 設定変更を展開します [設定変更の展開](#) を参照してください。

## ネットワーク検出アイデンティティ競合の設定

システムは、オペレーティングシステムとサーバのフィンガープリントをトラフィック内のパターンに照合することで、どのオペレーティングシステムおよびアプリケーションがホストで実行されているかを判別します。最も信頼できるオペレーティングシステムとサーバの ID 情報を提供するために、システムは複数のソースからのフィンガープリント情報を照合します。

システムは、すべてのパッシブデータを使用して、オペレーティングシステム ID を抽出し、信頼値を割り当てます。

デフォルトでは、ID 競合が存在しなければ、スキャナまたはサードパーティアプリケーションによって追加された ID データで、システムによって検出された ID データが上書きされます。[アイデンティティソース (Identity Sources)] 設定を使用して、スキャナとサードパーティアプリケーションのフィンガープリントソースをプライオリティでランク付けできます。シス

テムはソースごとに1つずつのIDを保持しますが、プライオリティが最も高いサードパーティアプリケーションまたはスキャナソースからのデータのみが最新のIDとして使用されます。ただし、プライオリティに関係なく、ユーザ入力データによって、スキャナまたはサードパーティアプリケーションのデータが上書きされることに注意してください。

ID競合は、[アイデンティティソース (Identity Sources)] 設定に列挙されたアクティブスキャナソースまたはサードパーティアプリケーションソースとシステムユーザーのどちらかから取得された、既存のIDと競合するIDをシステムが検出した場合に発生します。デフォルトでは、ID競合は自動的に解決されないため、ホストプロファイルを通して、または、ホストをスキャンし直すか新しいIDデータを追加し直してパッシブIDを上書きすることにより、解決する必要があります。ただし、パッシブIDまたはアクティブなIDのいずれかを維持することで、競合を自動的に解決するようにシステムを設定できます。

#### [ID競合イベントを生成する (Generate Identity Conflict Event)]

ID競合が発生したときにシステムがイベントを生成するかどうかを指定します。

#### [自動的に競合を解決する (Automatically Resolve Conflicts)]

[自動的に競合を解決する (Automatically Resolve Conflicts)] ドロップダウンリストから、次のいずれかを選択します。

- ID競合の手動での競合解決を強制する場合は、[無効 (Disabled)]
- ID競合が発生したときにシステムがパッシブフィンガープリントを使用するようにする場合は、[アイデンティティ (Identity)]
- ID競合が発生したときにシステムが優先度が最も高いアクティブなソースの現在のIDを使用するようにする場合は、[キープアクティブ (Keep Active)]

## ネットワーク検出アイデンティティ競合の解決の設定

### 手順

- ステップ1 [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。
- ステップ2 [詳細設定 (Advanced)] をクリックします。
- ステップ3 [ID競合設定 (Identity Conflict Settings)] の横にある [編集 (Edit)] (✎) をクリックします。
- ステップ4 [ネットワーク検出アイデンティティ競合の設定 \(16 ページ\)](#) の説明に従って、[ID競合設定の編集 (Edit Identity Conflict Settings)] ポップアップウィンドウの設定を更新します。
- ステップ5 [保存 (Save)] をクリックして、ID競合設定を保存します。

### 次のタスク

- 設定変更を展開します [設定変更の展開](#) を参照してください。

## ネットワーク検出の脆弱性の影響の評価オプション

システムで侵入イベントとの影響相関を実行する方法を設定できます。有効な選択肢は次のとおりです。

- システム ベースの脆弱性情報を使用して影響相関を実行する場合は、[ネットワーク検出の脆弱性マッピングを使用 (Use Network Discovery Vulnerability Mappings)] チェックボックスをオンにします。
- サードパーティの脆弱性参照を使用して影響相関を実行する場合は、[サードパーティの脆弱性マッピングを使用 (Use Third-Party Vulnerability Mappings)] チェックボックスをオンにします。詳細については、*Firepower* システムホスト入力 API ガイドを参照してください。

チェックボックスのどちらかまたは両方を選択できます。システムが侵入イベントを生成し、選択された脆弱性マッピング セット内の脆弱性のあるサーバまたはオペレーティング システムがそのイベントに関係するホストに含まれている場合、侵入イベントは脆弱 (レベル1: 赤) 影響アイコンでマークされます。ベンダーまたはバージョン情報のないサーバの場合は、Management Center 構成で脆弱性マッピングを有効にする必要があることに注意してください。

両方のチェックボックスをオフにした場合は、侵入イベントが脆弱 (レベル1: 赤) 影響アイコンでマークされません。

### 関連トピック

[サードパーティの脆弱性のマッピング](#)

## ネットワーク検出の脆弱性影響評価の有効化

### 手順

- ステップ 1 [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。
- ステップ 2 [詳細設定 (Advanced)] をクリックします。
- ステップ 3 [影響評価を使用するための脆弱性 (Vulnerabilities to use for Impact Assessment)] の横にある[編集 (Edit)] (✎) をクリックします。
- ステップ 4 [ネットワーク検出の脆弱性の影響の評価オプション \(18 ページ\)](#) 説明に従って、[脆弱性設定の編集 (Edit Vulnerability Settings)] ポップアップ ウィンドウで設定を更新します。
- ステップ 5 [保存 (Save)] をクリックして、脆弱性設定を保存します。

### 次のタスク

- 設定変更を展開します [設定変更の展開](#) を参照してください。

## 侵害の兆候

システムでは、ネットワーク検出ポリシー内のIOCルールを使用して悪意のある手段によって侵害されている可能性があるホストが特定されます。ホストがこれらのシステム提供のルールで指定されている条件を満たしている場合、そのホストはシステムによって侵害の兆候 (IOC) でタグ付けされます。関連のルールは *IOC* ルールと呼ばれます。各 IOC ルールは 1 種類の IOC タグに対応しています。IOC タグは可能性のある侵害の性質を指定します。

次のうちいずれかの事態が発生すると、関与しているホストおよびユーザーに Management Center がタグを付けます。

- システムは、侵入、接続、セキュリティ インテリジェンス、およびファイルまたはマルウェアイベントを使用してモニタ対象のネットワークとそのトラフィックについて集められたデータを関連付け、潜在的な IOC が発生したと判断します。
- Management Center は AMP クラウドを経由してエンドポイント向け AMP の展開から IOC データをインポートすることができます。このデータがホスト自体の活動（個別のプログラムによってまたはプログラム上で実行されるアクションなど）を検査するため、ネットワーク専用データでは理解するのが難しい可能性がある脅威に対する理解が促されます。便宜上、Management Center はシスコが開発した新しい IOC タグを AMP クラウドから自動的に取得します。

この機能を設定するには、[侵害の兆候ルールの有効化 \(19 ページ\)](#) を参照してください。

また、ホストの IOC データに対する関連ルールと、IOC でタグ付けされたホストから成るコンプライアンス allow リストも記述することができます。

タグ付けされた IOC の調査や操作を行うには、[Cisco Secure Firewall Management Center アドミニストレーションガイド](#)参照してください。

## 侵害の兆候ルールの有効化

システムで侵害の兆候 (IOC) を検出してタグを付けるには、まず、ネットワーク検出ポリシーで 1 つ以上の IOC ルールを有効化する必要があります。IOC ルールのそれぞれが IOC タグの 1 つのタイプに対応します。すべての IOC ルールはシスコが事前定義しています。オリジナルルールを作成することはできません。ネットワークや組織のニーズに合わせて、一部またはすべてのルールを有効にすることができます。たとえば、Microsoft Excel などのソフトウェアを使用しているホストが絶対に監視対象ネットワーク上に出現しない場合は、Excel ベースの脅威に関係する IOC タグを有効にしないようにできます。



**ヒント** 個別のホストまたはその関連ユーザーの IOC ルールを無効にするには、[Cisco Secure Firewall Management Center アドミニストレーションガイド](#)の「Discovery Events」の章を参照してください。

### 始める前に

IOCルールはシステムの他のコンポーネントと、AMP for Endpoints によって提供されるデータに基づいてトリガーされるため、これらのコンポーネントが正しくライセンス付与され、IOC タグを設定できるように設定されている必要があります。侵入検知および防御（IPS）および Advanced Malware Protection（AMP）など、有効にする予定の IOC ルールに関連付けられているシステムの機能を有効にします。IOCルールの関連機能が有効になっていないと、関連データが収集されず、ルールをトリガーできません。

### 手順

- ステップ 1 [ポリシー（Policies）]>[ネットワーク検出（Network Discovery）]を選択します。
- ステップ 2 [詳細設定（Advanced）]をクリックします。
- ステップ 3 [侵害の兆候設定（Indications of Compromise Settings）]の横にある[編集（Edit）]（) をクリックします。
- ステップ 4 IOC 機能全体のオンとオフを切り替えるには、[IOC の有効化（Enable IOC）]の横にあるスライダをクリックします。
- ステップ 5 個別の IOC ルールをグローバルに有効または無効にするには、ルールの [有効（Enabled）] 列のスライダをクリックします。
- ステップ 6 [保存（Save）]をクリックして IOC ルール設定を保存します。

### 次のタスク

- 設定変更を展開します [設定変更の展開](#) を参照してください。

## NetFlow エクスポートのネットワーク検出ポリシーへの追加

この手順に従って、NetFlow エクスポートを追加します。検出ルールで現在使用中のエクスポートは削除できないことに注意してください。

### 始める前に

- 「[NetFlow データを使用するための要件](#)」で前提条件を確認します。
- 「[NetFlow データ](#)」で NetFlow エクスポートを設定します。

### 手順

- ステップ 1 [ポリシー（Policies）]>[ネットワーク検出（Network Discovery）]を選択します。
- ステップ 2 [詳細設定（Advanced）]をクリックします。
- ステップ 3 [NetFlow デバイス（NetFlow Devices）]の横にある **Add** () をクリックします。

ステップ4 エクスポートの [IPアドレス (IP Address)] を入力します。

ステップ5 [保存 (Save)] をクリックします。

---

#### 次のタスク

- 「[ネットワーク検出ルールの設定 \(4 ページ\)](#)」で NetFlow トラフィックをモニタリングするネットワーク検出ルールを設定します。
- 設定変更を展開します [設定変更の展開](#) を参照してください。

## ネットワーク検出のデータ ストレージ設定

ディスクバリのデータ ストレージ設定では、ホスト制限とタイムアウトの設定が行われます。

#### ホスト制限の到達時 (When Host Limit Reached)

Secure Firewall Management Center がモニタでき、ネットワーク マップに保存できるホストの数。モデルによって異なります。ホスト制限に到達した後に新しいホストを検出すると、[ホスト制限の到達時 (When Host Limit Reached)] オプションが制御を行います。次の操作を実行できます。

#### ホストをドロップ (Drop hosts)

システムは、長期間非アクティブになっているホストをドロップして、新しいホストを追加します。これがデフォルトの設定です。

#### 新しいホストを挿入しない (Don't insert new hosts)

システムは、新たに検出されたホストを追跡しません。システムが新しいホストを追跡するのは、管理者がドメインのホスト制限を増加させた後などに、ホストカウントが制限を下回る場合、ネットワークマップからホストを手動で削除する場合、またはホストが非アクティブであることからタイムアウトと見なされる場合のみです。

表 2: マルチテナンシーによるホスト制限への到達

設定	ドメインのホスト制限の有無	ドメインのホスト制限に到達した場合	先祖ドメインのホスト制限に到達した場合
ホストをドロップ	Yes	制限付きドメインの最も古いホストをドロップします。	ホストをドロップするように設定されているすべての子孫リーフドメインで最も古いホストをドロップします。  ドロップされるホストがなければ、ホストの追加は行われません。
	No	適用対象外	ホストをドロップし、一般プールを共有するように設定されているすべての子孫リーフドメインで最も古いホストをドロップします。
新しいホストを挿入しない	YesまたはNo	ホストの追加は行われません。	ホストの追加は行われません。

### ホストタイムアウト (Host Timeout)

システムが、非アクティブであるという理由でネットワークマップからホストを除外するまでの分単位の時間。デフォルト設定は 10080 分 (1 週間) です。ホスト IP アドレスと MAC アドレスは個別にタイムアウトすることができますが、関連するアドレスのすべてがタイムアウトするまで、ホストはネットワークマップから削除されません。

ホストの早期タイムアウトを避けるために、ホストのタイムアウト値がネットワーク検出ポリシーの一般設定内の更新間隔より長いことを確認します。

### サーバタイムアウト (Server timeout)

システムが、非アクティブであるという理由でネットワークマップからサーバを除外するまでの分単位の時間。デフォルト設定は 10080 分 (1 週間) です。

サーバの早期タイムアウトを避けるために、サービスのタイムアウト値がネットワーク検出ポリシーの一般設定内の更新間隔より長いことを確認します。

### クライアントアプリケーションのタイムアウト (Client Application Timeout)

システムが、非アクティブであるという理由でネットワークマップからクライアントを除外するまでの分単位の時間。デフォルト設定は 10080 分 (1 週間) です。

クライアントのタイムアウト値がネットワーク検出ポリシーの一般設定内の更新間隔より長いことを確認します。

### 関連トピック

[ホスト制限 \(Host Limit\)](#)

## ネットワーク検出データ ストレージの設定

### 手順

- ステップ 1 [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。
- ステップ 2 [詳細設定 (Advanced)] をクリックします。
- ステップ 3 [ネットワーク検出のデータストレージ設定 (Network Discovery Data Storage Settings)] の横にある [編集 (Edit)] (✎) をクリックします。
- ステップ 4 [ネットワーク検出のデータ ストレージ設定 \(21 ページ\)](#) の説明に従って、[データ ストレージ設定 (Data Storage Settings)] ダイアログの設定を更新します。
- ステップ 5 [保存 (Save)] をクリックして、データ ストレージ設定を保存します。

### 次のタスク

- 設定変更を展開します [設定変更の展開](#) を参照してください。

## ネットワーク検出イベント ログिंगの設定

イベントログिंग設定は、検出イベントとホスト入力イベントを記録するかどうかを制御します。イベントを記録しない場合は、イベントビューで検索することも、相関ルールをトリガーするために使用することもできません。

### 手順

- ステップ 1 [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。
- ステップ 2 [詳細設定 (Advanced)] をクリックします。
- ステップ 3 [イベントログिंग設定 (Event Logging Settings)] の横にある [編集 (Edit)] (✎) をクリックします。
- ステップ 4 [Cisco Secure Firewall Management Center アドミニストレーション ガイド](#) の「*Discovery Events*」の章の説明に従って、データベースに記録する検出イベントタイプとホスト入力イベントタイプの横にあるチェックボックスをオンまたはオフにします。
- ステップ 5 [保存 (Save)] をクリックして、イベント ログिंग設定を保存します。

### 次のタスク

- 設定変更を展開します [設定変更の展開](#) を参照してください。

## ネットワーク検出 OS およびサーバー アイデンティティ ソースの追加

ネットワーク検出ポリシーの [詳細 (Advanced)] で、新しいアクティブソースを追加し、また、既存の送信元の優先度やタイムアウトの設定を変更できます。

このページにスキャナを追加しても、Nmap スキャナ用の完全な統合機能は追加されませんが、インポートされたサードパーティアプリケーションまたはスキャン結果の統合が可能になります。

サードパーティアプリケーションまたはスキャナからデータをインポートする場合は、ソースからの脆弱性がネットワークで検出された脆弱性にマップされていることを確認してください。

### 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

**ステップ 2** [詳細設定 (Advanced)] をクリックします。

**ステップ 3** [OS とサーバー ID ソース (OS and Server Identity Sources)] の横にある [編集 (Edit)] () をクリックします。

**ステップ 4** 新しいソースを追加するには、[ソースの追加 (Add Sources)] をクリックします。

**ステップ 5** 名前を入力します。

**ステップ 6** ドロップダウンリストからインプットソースの [タイプ (Type)] を選択します。

- AddScanResult 機能を使用してスキャン結果をインポートする場合は、[スキャナ (Scanner)] を選択します。
- スキャン結果をインポートしない場合は、[アプリケーション (Application)] を選択します。

**ステップ 7** このソースによるネットワーク マップへの ID の追加からその ID の削除までの期間を指定するには、[タイムアウト (Timeout)] ドロップダウンリストから、[時間 (Hours)]、[日 (Days)]、または [週 (Weeks)] を選択し、該当する期間を入力します。

**ステップ 8** 必要に応じて、以下を行います。

- ソースを昇格させて、オペレーティング システム ID とアプリケーション ID よりもリストでは下にあるソースを優先的に使用するには、そのソースを選択して上矢印をクリックします。
- ソースを降格させて、リストで上にあるソースから提供される ID が存在しない場合のみオペレーティング システム ID とアプリケーション ID を使用するには、そのソースを選択して下矢印をクリックします。
- ソースを削除するには、ソースの横にある [削除 (Delete)] () をクリックします。

**ステップ 9** [保存 (Save)] をクリックして、ID ソース設定を保存します。

### 次のタスク

- ・設定変更を展開します。設定変更の展開を参照してください。

### 関連トピック

[サードパーティの脆弱性のマッピング](#)

## ネットワーク検出戦略のトラブルシューティング

システムのデフォルトの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ていないかと、その原因を分析してください。

### 管理対象デバイスは正しく配置されていますか

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、誤って識別されたホストのより近くに管理対象デバイスを配置します。このシナリオでは、カスタムフィンガープリントの使用は推奨しません。

### 識別されないオペレーティング システムに一意の TCP スタックがありますか

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、検出（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、識別用の 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、システムで識別できない一意の TCP スタックを保持する 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が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、システムがそのホストを識別してそのホストを監視し続けることができるカスタムフィンガープリントを作成する方が便利です。

オープンソースの Linux ディストリビューションの多くで同じカーネルを使用しているため、システムでは Linux のカーネル名を使用してそれらを識別することに注意してください。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 が正しくホストを識別するならば、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、サードパーティ製の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Cisco の定義にマッピングする必要があります。アプリケーションデータをシステムのベンダーとバージョンの定義にマッピングした場合でも、インポートされたサードパーティ製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は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在のIDを判別することがあります。

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行うことができます。ただし、アクティブのスキャンデータとホスト入力データは、検出(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。

### システムがすべてのアプリケーションを識別できるか

ホストがシステムによって正しく識別されるものの、識別されないアプリケーションがホストにある場合、ユーザ定義のディテクタを作成して、アプリケーションを識別するため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。

### 脆弱性を修正するパッチを適用しましたか

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内の修正にマッピングする必要があります。

### サードパーティ製の脆弱性を追跡しますか

影響の関連付け(相関)に使用したいサードパーティ製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の脆弱性IDをCiscoのデータベース内の脆弱性IDにマッピングしてから、ホスト入力機能を使用してそれらの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の詳細については、『Firepower システムホスト入力APIガイド』を参照してください。アプリケーションデータをシステムのベンダーとバージョンの定義にマッピングした場合でも、インポートされたサードパーティ製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は使用されないことに注意してください。

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。