



相関ポリシー

次のトピックでは、相関ポリシーおよびルールの設定方法について説明します。

- [相関ポリシーとルールの概要 \(1 ページ\)](#)
- [コンプライアンスの要件と前提条件 \(3 ページ\)](#)
- [相関ポリシーの設定 \(3 ページ\)](#)
- [相関ルールの設定 \(5 ページ\)](#)
- [相関応答グループの設定 \(43 ページ\)](#)

相関ポリシーとルールの概要

相関機能を使用することで、ネットワークへの脅威に対して相関ポリシーを使用してリアルタイムで応答できます。

ネットワーク上のアクティビティによって、アクティブな相関ポリシー内の相関ルールまたはコンプライアンス allow リストのいずれかがトリガーされると、相関ポリシー違反が発生します。

相関ルール

アクティブな相関ポリシー内の相関ルールがトリガーされると、システムによって相関イベントが生成されます。相関ルールは、以下の場合にトリガーされます。

- 特定のタイプのイベント（接続、侵入、マルウェア、ディスクバリエーション、ユーザアクティビティなど）がシステムによって生成された。
- ネットワークトラフィックが通常のプロファイルから逸脱している。

以下の方法で相関ルールを制約することもできます。

- ホストプロファイル限定を追加すると、トリガーイベントに関連するホストのプロファイルからの情報に基づいてルールを制約できます。
- 接続トラッカーを相関ルールに追加すると、ルールの初期基準に一致した場合、システムは特定の接続を追跡し始めます。その後、追跡対象の接続がさらに追加の基準を満たす場合のみ、相関イベントが生成されます。

- ユーザ限定を関連ルールに追加すると、特定のユーザまたはユーザ グループを追跡します。たとえば、特定のユーザのトラフィックや特定の部門からのトラフィックに対してのみトリガーされるように関連ルールを制約することができます。
- スヌーズ期間の追加。関連ルールがトリガーされた後、スヌーズ期間により指定したインターバルの間、そのルールは再びトリガーされません。スヌーズ期間が経過すると、ルールは再びトリガー可能になり、新しいスヌーズ期間が始まります。
- 非アクティブ期間の追加。非アクティブ期間中は、関連ルールはトリガーされません。

展開のライセンスなしでも関連ルールを設定できますが、ライセンス許可のないコンポーネントを使用するルールはトリガーされません。

コンプライアンス 許可 (Allow) リスト

コンプライアンス allow リストでは、ネットワーク上のホストで許可されるオペレーティングシステム、アプリケーション (Web およびクライアント)、プロトコルを指定します。アクティブな関連ポリシーで使用されている allow リストにホストが違反した場合、allow リストイベントがシステムによって生成されます。

関連応答

関連ポリシー違反への応答には、シンプルなアラートや、さまざまな修復 (ホストのスキャンなど) が含まれます。それぞれの関連ルールまたはallowリストを、単一の応答または応答グループに関連付けることができます。

ネットワークトラフィックが複数のルールまたはallowリストをトリガーとして使用した場合、システムはそれぞれのルールとallowリストに関連付けられているすべての応答を起動します。

関連およびマルチテナンシー

マルチドメイン展開では、ドメインレベルで利用可能な任意のルール、allow リスト、および応答を使用して、任意のドメインレベルで関連ポリシーを作成できます。高位レベルドメインの管理者はドメイン内、および複数ドメインで関連付けを実行できます。

- ドメインによって関連ルールを制約すると、そのドメインの子孫で報告されるイベントが照合されます。
- 高位レベルドメインの管理者は複数ドメインでホストを評価するコンプライアンス allow リストを作成できます。同じ allow リストで、異なるドメイン内の異なるサブネットを対象にできます。



(注) システムは、各リーフ ドメインに個別のネットワーク マップを作成します。リテラルの設定 (IP アドレス、VLAN タグ、ユーザー名など) を使用してドメイン間の関連ルールを制約すると、予期しない結果になる可能性があります。

関連トピック

- [コンプライアンス許可 \(Allow\) リストの概要](#)
- [Secure Firewall Management Center アラート応答修復の概要](#)

コンプライアンスの要件と前提条件

モデルのサポート

任意 (Any)

サポートされるドメイン

任意

ユーザの役割

- 管理者

相関ポリシーの設定

相関ルール、コンプライアンスの allow リスト、アラート応答、および修復を使用して相関ポリシーを作成します。

マルチドメイン展開では、任意のドメインレベルで、そのレベルで使用可能な構成設定を使用して相関ポリシーを作成できます。

各相関ポリシーと、そのポリシーで使用される各ルールと allow リストにプライオリティを割り当てることができます。ルールと allow リストのプライオリティは、相関ポリシーのプライオリティをオーバーライドします。ネットワークトラフィックが相関ポリシーに違反した場合、違反があったルールまたは allow リストに独自のプライオリティがない限り、結果の相関イベントでポリシーのプライオリティ値が表示されます。

手順

- ステップ 1** [ポリシー (Policies)] > [相関 (Correlation)] を選択します。
- ステップ 2** [ポリシーの作成 (Create Policy)] をクリックします。
- ステップ 3** [ポリシー名 (Policy Name)] と [ポリシーの説明 (Policy Description)] を入力します。
- ステップ 4** [デフォルトプライオリティ (Default Priority)] ドロップダウンリストから、ポリシーのプライオリティを選択します。ルールのプライオリティのみを使用するには、[なし (None)] を選択します。

- ステップ 5** [ルールの追加 (Add Rules)]をクリックし、ポリシーで使用するルールと allow リストを選択して、[追加 (Add)]をクリックします。
- ステップ 6** 各ルールまたは allow リストの [優先順位 (Priority)]リストから、プライオリティを選択します。
- 1 ~ 5 のプライオリティ値
 - **None**
 - [デフォルト (Default)] (ポリシーのデフォルト プライオリティを使用)
- ステップ 7** [ルールと許可 \(Allow\) リストに応答を追加する \(4 ページ\)](#) の説明に従ってルールと allow リストに応答を追加します。
- ステップ 8** [保存 (Save)]をクリックします。

次のタスク


- スライダをクリックして、ポリシーをアクティブにします。

ルールと許可 (Allow) リストに応答を追加する

それぞれの関連ルールまたはallowリストを、単一の応答または応答グループに関連付けることができます。ネットワークトラフィックが複数のルールまたはallowリストをトリガーとして使用した場合、システムはそれぞれのルールとallowリストに関連付けられているすべての応答を起動します。トラフィックプロファイルの変更への応答として使用された場合は、Nmap 修復が開始されないことに注意してください。

マルチドメイン展開では、現在のドメインまたは先祖ドメインで作成された応答を使用できません。

手順

- ステップ 1** 関連ポリシーエディタで、応答を追加するルールまたは allow リストの横にある [応答 (Responses)] () をクリックします。
- ステップ 2** [未割り当ての応答 (Unassigned Responses)]の下で、ルールまたはallowリストがトリガーとして使用された場合に起動する応答を選択して、上矢印 (^) をクリックします。
- ステップ 3** [更新 (Update)]をクリックします。

関連トピック

[Secure Firewall Management Center アラート応答修復の概要](#)

相関ポリシーの管理

アクティブな相関ポリシーへの変更は、即座に反映されます。

相関ポリシーを有効化すると、システムは即座にイベントの処理を開始して、応答をトリガーします。システムは、最初の有効化後の評価時に、非準拠ホストの **allow** リストイベントを生成しない点に注意してください。

マルチドメイン展開では、現在のドメインで作成された相関ポリシーが表示されます。このポリシーは編集可能です。また、先祖ドメインからの選択した相関ポリシーも表示されますが、これは編集できません。下位のドメインで作成された相関ポリシーを表示および編集するには、そのドメインに切り替えます。






- (注) 設定に無関係なドメイン（名前、管理対象デバイスなど）に関する情報が公開されている場合、システムは先祖ドメインからの設定を表示しません。

手順

ステップ1 [ポリシー (Policies)] > [相関 (Correlation)] を選択します。

ステップ2 相関ポリシーを管理します。

- アクティブ化または非アクティブ化：スライダをクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 作成：[ポリシーの作成 (Create Policy)] をクリックします。[相関ポリシーの設定 \(3 ページ\)](#) を参照してください。
- 編集：[編集 (Edit)] () をクリックします。[相関ポリシーの設定 \(3 ページ\)](#) を参照してください。代わりに[表示 (View)] () が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 削除：[削除 (Delete)] () をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

相関ルールの設定

単純な相関ルールでは、特定のタイプのイベントが発生することのみが必要です。より具体的な条件を指定する必要はありません。たとえば、トラフィックプロファイル変化に基づく相関ルールでは、条件を指定する必要はありません。また、複数の条件と追加した制約を使用して複雑な相関ルールを作成することもできます。

相関ルールトリガー基準、ホストプロファイル限定、ユーザ限定、または接続トラッカーを作成するときの構文はそれぞれに異なりますが、メカニズムはすべて同じです。



(注) マルチドメイン展開では、関連ルールを先祖ドメインで制約すると、そのドメインの子孫によってレポートされるイベントと一致します。

始める前に

- 関連イベントをトリガーするために使用するタイプの情報が展開で収集されていることを確認します。たとえば、個々の接続イベントまたは接続サマリーイベントで使用可能な情報は、検出方法、ロギング方法、イベントタイプなど、いくつかの要因により異なります。システムは、エクスポートされた NetFlow レコードからネットワークマップにホストを追加できますが、これらのホストに使用できる情報は限られます ([NetFlow データと管理対象デバイス データの違い](#)を参照)。

手順

ステップ 1 [ポリシー (Policies)] > [関連 (Correlation)] を選択し、[ルール管理 (Rule Management)] をクリックします。

ステップ 2 [ルールの作成 (Create Rule)] をクリックします。

ステップ 3 [ルール名 (Rule Name)] と [ルールの説明 (Rule Description)] を入力します。

ステップ 4 必要に応じて、ルールの [ルールグループ (Rule Group)] を選択します。

ステップ 5 基本イベントタイプを選択し、必要に応じて、関連ルールの追加のトリガー条件を指定します。次の基本イベントタイプを選択できます。

- **VPN トラブルシューティングイベントが発生** : [VPN トラブルシューティングイベントトリガー条件の構文 \(8 ページ\)](#) を参照してください。
- **侵入イベントが発生** : [侵入イベントトリガー条件の構文 \(8 ページ\)](#) を参照してください。
- **マルウェア イベントが発生** : [マルウェア イベントトリガー条件の構文 \(11 ページ\)](#) を参照してください。
- **検出イベントが発生** : [ディスカバリ イベントトリガー条件の構文 \(13 ページ\)](#) を参照してください。
- **ユーザ アクティビティが検出された** : [ユーザー アクティビティのイベントトリガー条件の構文 \(16 ページ\)](#) を参照してください。
- **ホスト入力イベントが発生** : [ホスト入力イベントトリガー条件の構文 \(17 ページ\)](#) を参照してください。
- **接続イベントが発生** : [接続イベントトリガー条件の構文 \(18 ページ\)](#) を参照してください。
- **トラフィック プロファイルの変更** : [トラフィック プロファイル変化の構文 \(22 ページ\)](#) を参照してください。

ステップ 6 必要に応じて、次のいずれかまたはすべてを追加することによって関連ルールをさらに制約します。

- ホストプロファイル限定：[ホストプロファイル限定の追加（Add Host Profile Qualification）] をクリックします。[関連ホストプロファイル限定の構文（25 ページ）](#) を参照してください。
- 接続トラッカー：[接続トラッカーの追加（Add Connection Tracker）] をクリックします。[接続トラッカー（29 ページ）](#) を参照してください。
- ユーザ限定：[ユーザ限定の追加（Add User Qualification）] をクリックします。[ユーザー限定の構文（28 ページ）](#) を参照してください。
- スヌーズ期間：ルールオプションで、[スヌーズ（Snooze）] テキストフィールドとドロップダウンリストを使用して、関連ルールのトリガー後、次に関連ルールをトリガーするまで待機する間隔を指定します。
- 非アクティブ期間：ルールオプションで、[非アクティブ期間の追加（Add Inactive Period）] をクリックします。テキストフィールドとドロップダウンリストを使用して、関連ルールに基づくネットワークトラフィック評価をシステムに停止させる時点および頻度を指定します。

ヒント スヌーズ期間を削除するには、間隔を **0**（秒、分、または時間）に指定します。

ステップ 7 [Save Rule] をクリックします。

関連ルールの単純な例

新しいホストが特定のサブネットで検出されると、次の単純な関連ルールがトリガーされます。カテゴリが IP アドレスを表す場合、演算子として [is in] または [is not in] を選択すると、CIDR などの特殊な表記で表される IP アドレスブロックにその IP アドレスが含まれるのか、含まれないのかを指定できます。

Select the type of event for this rule

If and it meets the following conditions:

次のタスク

- [関連ポリシーの設定（3 ページ）](#) の説明に従って、関連ポリシーでルールを使用します。

関連トピック

- [関連ルールの管理（42 ページ）](#)
- [関連ルールの作成メカニズム（39 ページ）](#)
- [スヌーズ期間および非アクティブ期間（39 ページ）](#)
- [NetFlow データと管理対象デバイスデータの違い](#)

VPN トラブルシュート イベント トリガー条件の構文

VPN トラブルシュート イベント を基本イベントとして選択した場合、次の表で説明する方法に従って関連ルールの条件を作成します。

表 1: VPN トラブルシュート イベント の構文

指定する項目	選択する演算子と入力内容
デバイス	VPN トラブルシューティング Syslog が有効になっている 1 つ以上のデバイスを選択します。
Syslog メッセージクラス	VPN Syslog メッセージクラスを選択します。選択したメッセージクラスの Syslog が生成されると、関連ルールの条件が満たされ、関連イベントが生成されます。
Syslog メッセージ ID	関連ルールの VPN Syslog メッセージ ID を指定します。
Syslog メッセージテキスト	関連ルールの VPN Syslog メッセージテキストを指定します。
Syslog のシビラティ (重大度)	VPN Syslog の重大度を指定します。選択した重大度に対して生成された VPN トラブルシューティング Syslog によって、関連イベントがトリガーされます。
ユーザ名 (Username)	関連イベントを生成する必要があるトラフィックの VPN ユーザー名を指定します。

侵入イベント トリガー条件の構文

侵入イベントを基本イベントとして選択した場合、次の表で説明する方法に従って関連ルールの条件を作成します。

表 2: 侵入イベントの構文

指定する項目	選択する演算子と内容
アクセス コントロール ポリシー	侵入イベントを生成した侵入ポリシーを使用するアクセス コントロール ポリシーを 1 つ以上選択します。
アクセス コントロール ルール名	侵入イベントを生成した侵入ポリシーを使用するアクセス コントロール ルールの名前の全体またはその一部を入力します。
アプリケーション プロトコル	侵入イベントに関連付けられたアプリケーション プロトコルを 1 つ以上選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコルのカテゴリを 1 つ以上選択します。

指定する項目	選択する演算子と内容
分類	分類を1つ以上を選択します。
クライアント	侵入イベントに関連付けられたクライアントを1つ以上選択します。
クライアントカテゴリ	クライアントのカテゴリを1つ以上選択します。
接続先（国）または送信元（国）	侵入イベントの送信元または宛先 IP アドレスに関連付けられた国を1つ以上選択します。
宛先 IP、送信元 IP、送信元 IP と宛先 IP の両方、または、送信元 IP か宛先 IP のいずれか	単一の IP アドレスまたはアドレス ブロックを入力します。
宛先ポート/ICMP コードまたは送信元ポート/ICMP タイプ	送信元トラフィックのポート番号または ICMP タイプ、または宛先トラフィックのポート番号または ICMP コードを入力します。
Device	イベントを生成した可能性があるデバイスを1つ以上選択します。
ドメイン	1つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。
出力インターフェイスまたは入力インターフェイス	インターフェイスを1つ以上選択します。
出力セキュリティゾーンまたは入力セキュリティゾーン	1つ以上のセキュリティゾーンまたはトンネルゾーンを選択します。
ジェネレータ ID	プリプロセッサを1つ以上選択します。
影響フラグ	侵入イベントに割り当てられた影響レベルを選択します。 NetFlow データからネットワークマップに追加されたホストに使用可能なオペレーティングシステムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な（インパクトレベル1：赤）インパクトレベルを割り当てることができません。このような場合は、ホスト入力機能を使用して、ホストのオペレーティングシステム ID を手動で設定します。
インライン結果	システムは、侵入ポリシーの結果としてパケットを [ドロップした (dropped)] か [ドロップしたと想定 (would have dropped)] したのかを選択します。 システムは、インライン展開、スイッチド展開、またはルーテッド展開のパケットをドロップできます。侵入ポリシーのドロップ動作や侵入ルール状態とは無関係に、パッシブ展開（インラインセットがタップモードである場合を含む）ではシステムがパケットをドロップしません。

指定する項目	選択する演算子と内容
侵入ポリシー	侵入イベントを生成した侵入ポリシーを1つ以上選択します。
IOC タグ	侵入イベントの結果として侵害の兆候タグが設定されているかどうかを選択します。
[プライオリティ (Priority)]	<p>ルールの優先順位を選択します。</p> <p>ルールベースの侵入イベントの場合、優先順位は <code>priority</code> キーワードまたは <code>classtype</code> キーワードのいずれかの値に対応します。その他の侵入イベントの場合、プライオリティはデコーダまたはプリプロセッサによって決定されます。</p>
プロトコル	http://www.iana.org/assignments/protocol-numbers にリストされているトランスポートプロトコルの名前または番号を入力します。
ルール メッセージ	ルール メッセージの全体またはその一部を入力します。
ルール SID	<p>単一の [Snort ID] (SID) またはカンマ区切りの複数の SID を入力します。</p> <p>演算子として [に含まれる (is in)] または [に含まれない (is not in)] を選択する場合、複数選択ポップアップウィンドウを使用することはできません。SID のカンマ区切りリストを入力する必要があります。</p>
ルール タイプ	<p>ルールをローカルにするかどうかを指定します。</p> <p>ローカルルールには、カスタマイズされた標準テキスト侵入ルール、ユーザが変更した標準テキストルール、見出し情報を変更してルールを保存するときに作成される共有オブジェクトルールの新規インスタンスが含まれます。</p>
実際の SSL アクション	システムが暗号化された接続をどのように処理したかを示す SSL ルール アクションを選択します。
SSL 証明書のフィンガープリント	トラフィックの暗号化に使用された証明書のフィンガープリントを入力するか、フィンガープリントに関連付けられたサブジェクトの共通名を選択します。
SSL 証明書のサブジェクトの共通名 (CN)	セッションの暗号化に使用された証明書のサブジェクトの共通名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの国 (C)	セッションの暗号化に使用された証明書のサブジェクトの国番号を1つ以上選択します。
SSL 証明書のサブジェクトの組織 (O)	セッションの暗号化に使用された証明書のサブジェクトの組織名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの部門 (OU)	セッションの暗号化に使用された証明書のサブジェクトの部門名のすべてまたはその一部を入力します。
SSL フローのステータス	システムによるトラフィック復号化試行の結果に基づくステータスを1つ以上選択します。
[ユーザ名 (Username)]	侵入イベントで送信元ホストにログインしたユーザを示すユーザ名を入力します。

指定する項目	選択する演算子と内容
VLAN ID (Admin. VLAN ID)	侵入イベントをトリガーとして使用したパケットに関連付けられた最も内側のVLAN IDを入力します。
Web アプリケーション	侵入イベントに関連付けられた Web アプリケーションを1つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを1つ以上選択します。

関連トピック

[侵入イベント フィールド](#)

[IP アドレスの規則](#)

マルウェア イベント トリガー条件の構文

マルウェア イベントで関連ルールをベースとして使用するには、まず、使用するマルウェア イベントのタイプを指定します。選択肢が使用可能なトリガー条件の設定を決定します。次のオプションを選択できます。

- [エンドポイントベースのマルウェアの検出 (by endpoint-based malware detection)] (Cisco Secure Endpoint による検出)
- [ネットワークベースのマルウェアの検出 (by network-based malware detection)] (マルウェア 防御による検出)
- [レトロスペクティブ ネットワークベースのマルウェアの検出 (by retrospective network-based malware detection)] (マルウェア 防御によるレトロアクティブ 検出)

マルウェア イベントを基本イベントとして選択する場合、次の表で説明する方法に従って関連 ルールの条件を作成します。

表 3: マルウェア イベントの構文

指定する項目	選択する演算子と内容
アプリケーション プロト コル	マルウェア イベントに関連付けられたアプリケーション プロトコルを1つ以上選択しま す。
アプリケーション プロト コル カテゴリ	アプリケーション プロトコルのカテゴリを1つ以上選択します。
クライアント	マルウェア イベントに関連付けられたクライアントを1つ以上選択します。
クライアント カテゴリ	クライアントのカテゴリを1つ以上選択します。
接続先 (国) または送信元 (国)	マルウェア イベントの送信元または宛先 IP アドレスに関連付けられた国を1つ以上選択 します。

指定する項目	選択する演算子と内容
宛先 IP、ホスト IP、または送信元 IP	単一の IP アドレスまたはアドレス ブロックを入力します。
送信先ポート/ICMP コード	宛先トラフィックのポート番号または ICMP コードを入力します。
傾向	[マルウェア (Malware)] または [カスタム検出 (Custom Detection)]、あるいはその両方を選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。
イベントタイプ	Cisco Secure Endpoint により検出されたマルウェアイベントと関連付けられた 1 つ以上のイベントタイプを選択します。
ファイル名	ファイルの名前を入力します。
ファイルタイプ	ファイルタイプを選択します。
ファイルタイプカテゴリ	ファイルタイプカテゴリを 1 つ以上選択します。
IOC タグ	マルウェア イベントの結果として侵害の兆候タグが設定 [される (is)] か、設定 [されない (is not)] かを選択します。
SHA-256	ファイルの SHA-256 ハッシュ値を入力するか貼り付けます。
実際の SSL アクション	システムが暗号化された接続をどのように処理したかを示す SSL ルール アクションを選択します。
SSL 証明書のフィンガープリント	トラフィックの暗号化に使用された証明書のフィンガープリントを入力するか、フィンガープリントに関連付けられたサブジェクトの共通名を選択します。
SSL 証明書のサブジェクトの共通名 (CN)	セッションの暗号化に使用された証明書のサブジェクトの共通名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの国 (C)	セッションの暗号化に使用された証明書のサブジェクトの国番号を 1 つ以上選択します。
SSL 証明書のサブジェクトの組織 (O)	セッションの暗号化に使用された証明書のサブジェクトの組織名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの部門 (OU)	セッションの暗号化に使用された証明書のサブジェクトの部門名のすべてまたはその一部を入力します。
SSL フローのステータス	システムによるトラフィック復号化試行の結果に基づくステータスを 1 つ以上選択します。

指定する項目	選択する演算子と内容
送信元ポート/ICMPタイプ	送信元トラフィックのポート番号または ICMP タイプを入力します。
Web アプリケーション	マルウェア イベントに関連付けられた Web アプリケーションを 1 つ以上選択します。
Web アプリケーションの カテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。

関連トピック

[ファイルおよびマルウェア イベント フィールド](#)

[IP アドレスの規則](#)

ディスカバリ イベント トリガー条件の構文

ディスカバリ イベントで関連ルールをベースとして使用するには、まず、使用するディスカバリ イベントのタイプを指定します。選択肢が使用可能なトリガー条件の設定を決定します。次の表は、選択可能なディスカバリ イベントのタイプを示しています。

ホップ変更によって関連ルールをトリガーとして使用したり、ホスト制限到達のためにシステムが新しいホストをドロップした時点で関連ルールをトリガーとして使用したりすることはできません。ただし、[任意のタイプのイベントがある (there is any type of event)]を選択することで、任意のタイプのディスカバリ イベントの発生時にルールをトリガーできます。

表 4: 関連ルールのトリガー条件とディスカバリ イベントタイプ

選択するオプション	選択内容
クライアントが変更された	クライアント更新
クライアントがタイムアウトになった	クライアント タイムアウト
ホスト IP アドレスが再使用されている	DHCP : IP アドレスの再割り当て
ホスト制限に達したためホストが削除された	ホスト削除 : ホスト制限に到達
ホストがネットワーク デバイスとして識別されている	ネットワーク デバイスへのホスト タイプの変更
ホストがタイムアウトになった	ホスト タイムアウト
ホストの IP アドレスが変更された	DHCP : IP アドレスの変更
NETBIOS 名の変更が検出された	NETBIOS 名の変更
新しいクライアントが検出された	新しいクライアント
新しい IP ホストが検出された	新しいホスト
新しい MAC アドレスが検出された	ホストの追加 MAC の検出

選択するオプション	選択内容
新しい MAC ホストが検出された	新しいホスト
新しいネットワーク プロトコルが検出された	新しいネットワーク プロトコル
新しいトランスポート プロトコルが検出された	新しいトランスポート プロトコル
TCP ポートが閉じた	TCP ポート クローズ
TCP ポートがタイムアウトした	TCP ポート タイムアウト
UDP ポートが閉じた	UDP ポート クローズ
UDP ポートがタイムアウトした	UDP ポート タイムアウト
VLAN タグが更新された	VLAN タグ情報の更新
IOC が設定された	侵害の兆候
オープン TCP ポートが検出された	新しい TCP ポート
オープン UDP ポートが検出された	新しい UDP ポート
ホストの OS 情報が変更された	新しい OS
ホストの OS またはサーバー ID でコンフリクトが発生した	アイデンティティ競合
ホストの OS またはサーバー ID がタイムアウトした	アイデンティティ タイムアウト
任意のタイプのイベントがある	任意のイベント タイプ
MAC アドレスに関する新しい情報がある	MAC 情報の変更
TCP サーバーに関する新しい情報がある	TCP サーバ情報の更新
UDP サーバーに関する新しい情報がある	UDP サーバ情報の更新

次の表では、ディスカバリ イベントを基本イベントとして選択するときに、関連ルール条件を作成する方法を説明します。

表 5: ディスカバリ イベントの構文

指定する項目	選択する演算子と内容
アプリケーションプロトコル	アプリケーションプロトコルを1つ以上選択します。
アプリケーションプロトコルカテゴリ	アプリケーションプロトコルのカテゴリを1つ以上選択します。

指定する項目	選択する演算子と内容
アプリケーション ポート	アプリケーション プロトコルのポート番号を入力します。
クライアント	クライアントを1つ以上選択します。
クライアント カテゴリ	クライアントのカテゴリを1つ以上選択します。
クライアント バージョン	クライアントのバージョン番号を入力します。
Device	ディスカバリ イベントを生成した可能性があるデバイスを1つ以上選択します。
ドメイン	1つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。
ハードウェア	モバイルデバイスのハードウェア モデルを入力します。たとえば、すべての Apple iPhone に一致させるには iPhone と入力します。
ホスト タイプ	ホスト タイプを1つ以上選択します。ホスト、またはいずれかのタイプのネットワーク デバイスを選択できます。
IP アドレスまたは新しい IP アドレス	単一の IP アドレスまたはアドレス ブロックを入力します。
ジェイルブロークン	イベントのホストがジェイルブレイクされたモバイルデバイスであることを示すには [はい (Yes)] を、そうでない場合は [いいえ (No)] を選択します。
MAC アドレス	ホストの MAC アドレス全体またはその一部を入力します。 たとえば、特定のハードウェア 製造元のデバイスの MAC アドレスが 0A:12:34 で始まることがわかっている場合、演算子として [開始 (begins with)] を選択し、値として 0A:12:34 を入力できます。
MAC タイプ	MAC アドレスが [ARP/DHCP で検出 (ARP/DHCP Detected)] されたかどうかを選択します。 つまり、MAC アドレスがホストに属していることをシステムがポジティブに識別したのか ([ARP/DHCP で検出 (is ARP/DHCP Detected)])、または、管理対象デバイスとホストの間にルータがあるなどの理由で、その MAC アドレスを持つ多数のホストをシステムが認識しているのか ([ARP/DHCP で検出されない (is not ARP/DHCP Detected)]) を選択します。
MAC ベンダー	ディスカバリ イベントをトリガーとして使用したネットワーク トラフィックで使われている NIC の MAC ハードウェア ベンダーの名前全体またはその一部を入力します。
Mobile	イベントのホストがモバイルデバイスであることを示すには [はい (Yes)] を、そうでない場合は [いいえ (No)] を選択します。

指定する項目	選択する演算子と内容
NETBIOS 名	ホストの NetBIOS 名を入力します。
ネットワーク プロトコル	http://www.iana.org/assignments/ethernet-numbers にリストされているネットワーク プロトコル番号を入力します。
OS 名	オペレーティング システムの名前を 1 つ以上選択します。
OS ベンダー	オペレーティング システムのベンダーを 1 つ以上選択します。
OS バージョン	オペレーティング システムのバージョンを 1 つ以上選択します。
プロトコルまたは トランスポート プロトコル	http://www.iana.org/assignments/protocol-numbers にリストされているトランスポートプロトコルの名前または番号を入力します。
ソース (Source)	ホスト入力データのソースを選択します (オペレーティング システムとサーバのアイデンティティ変更およびタイムアウトの場合)。
ソース タイプ	ホスト入力データのソースのタイプを選択します (オペレーティング システムとサーバのアイデンティティ変更およびタイムアウトの場合)。
VLAN ID (Admin. VLAN ID)	イベントに関連しているホストの VLAN ID を入力します。
Web アプリケーション	Web アプリケーションを選択します。

関連トピック

- [ディスカバリ イベント タイプ](#)
- [ディスカバリ イベントのフィールド](#)
- [IP アドレスの規則](#)

ユーザー アクティビティのイベント トリガー条件の構文

ユーザー アクティビティで関連ルールをベースとして使用するには、まず、使用するユーザー アクティビティのタイプを選択します。選択肢が使用可能なトリガー条件の設定を決定します。次のオプションを選択できます。

- **a new user identity was detected** (新しいユーザ ID の検出)
- **a user logs into a host** (ユーザーがホストにログイン)

ユーザー アクティビティを基本イベントとして選択する場合、次の表で説明する方法に従って関連ルールの条件を作成します。

表 6: ユーザー アクティビティの構文

指定する項目	選択する演算子と内容
Device	ユーザー アクティビティを検出した可能性のあるデバイスを 1 つ以上選択します。

指定する項目	選択する演算子と内容
ドメイン	1つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。
[IPアドレス (IP Address)]	単一の IP アドレスまたはアドレスブロックを入力します。
[ユーザ名 (Username)]	ユーザー名を入力します。

関連トピック

[ユーザー アクティビティ データのフィールド](#)

[IP アドレスの規則](#)

ホスト入カイベント トリガー条件の構文

ホスト入カイベントで関連ルールをベースとして使用するには、まず、使用するホスト入カイベントのタイプを指定します。選択肢が使用可能なトリガー条件の設定を決定します。次の表では、選択可能なホスト入カイベントのタイプを示しています。

ユーザ定義によるホスト属性定義を追加/削除/変更するとき、あるいは脆弱性の影響限定を設定するときに、関連ルールをトリガーとして使用することはできません。

表 7: 関連ルールのトリガー条件とホスト入カイベントタイプ

選択するオプション	ルールをトリガーとして使用するイベントタイプ
クライアントが追加された	クライアントの追加 (Add Client)
クライアントが削除された	クライアントの削除 (Delete Client)
ホストが追加された	ホストの追加 (Add Host)
プロトコルが追加された	プロトコルの追加 (Add Protocol)
プロトコルが削除された	プロトコルの削除 (Delete Protocol)
スキャン結果が追加された	スキャン結果の追加 (Add Scan Result)
サーバー定義が設定された	サーバー定義の設定 (Set Server Definition)
サーバーが追加された	ポートの追加 (Add Port)
サーバーが削除された	ポートの削除 (Delete Port)
脆弱性が無効とマークされた	脆弱性を無効に設定 (Vulnerability Set Invalid)
脆弱性が有効とマークされた	脆弱性を有効に設定 (Vulnerability Set Valid)

選択するオプション	ルールをトリガーとして使用するイベントタイプ
アドレスが削除された	ホスト/ネットワークの削除 (Delete Host/Network)
属性値が削除された	ホスト属性値の削除 (Host Attribute Delete Value)
属性値が設定された	ホスト属性値の設定 (Host Attribute Set Value)
OS 定義が設定された	オペレーティング システム定義の設定 (Set Operating System Definition)
ホストの重要度が設定された	ホスト重要度の設定 (Set Host Criticality)

次の表では、ホスト入力イベントを基本イベントとして選択するときに、関連ルールの条件を作成する方法を説明します。

表 8: ホスト入力イベントの構文

指定する項目	選択する演算子と内容
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。
[IP アドレス (IP Address)]	単一の IP アドレスまたはアドレス ブロックを入力します。
ソース (Source)	ホスト入力データのソースを選択します。
ソース タイプ (Source Type)	ホスト入力データのソースのタイプを選択します。

関連トピック

- [ホスト入力イベント タイプ](#)
- [ディスカバリ イベントのフィールド](#)
- [IP アドレスの規則](#)

接続イベントトリガー条件の構文

接続イベントで関連ルールをベースとして使用するには、まず、使用する接続イベントのタイプを指定します。接続イベントで利用可能な情報は、システムが接続をログに記録した方法、理由、および時によって変わることにご注意してください。次のオプションを選択できます。

- 接続の開始または終了時のいずれか
- 接続の開始時
- 接続の終了時

次の表では、接続イベントを基本イベントとして選択するとき、関連ルールの条件を作成する方法を説明します。

表 9: 接続イベントの構文

指定する項目	選択する演算子と内容
アクセス コントロール ポリシー	接続をログに記録したアクセス コントロール ポリシーを 1 つ以上選択します。
アクセス コントロール ルールのアクション	接続をログに記録したアクセス コントロール ルールに関連付けられたアクションを 1 つ以上選択します。 あとで接続を処理するルールまたはデフォルトアクションとは無関係に、ネットワークトラフィックがいずれかのモニタ ルールの条件に一致した場合に相関イベントをトリガーとして使用するには、[モニタ (Monitor)] を選択します。
アクセス コントロール ルール	接続をログに記録したアクセス コントロール ルールの名前のすべてまたは一部を入力します。 あとで接続を処理したルールまたはデフォルトアクションとは無関係に、接続と一致した条件を持つモニタ ルールの名前を入力できます。
アプリケーションプロトコル	接続に関連付けられたアプリケーション プロトコルを 1 つ以上選択します。
アプリケーションプロトコルカテゴリ	アプリケーションプロトコルのカテゴリを 1 つ以上選択します。
クライアント	クライアントを 1 つ以上選択します。
クライアントカテゴリ	クライアントのカテゴリを 1 つ以上選択します。
クライアントバージョン	クライアントのバージョン番号を入力します。
接続時間	接続イベントの時間 (秒数) を入力します。
接続タイプ	接続情報がどのように取得されたかに基づいて、相関ルールをトリガーするかどうかを指定します。 <ul style="list-style-type: none"> • エクスポートされた NetFlow データから生成された接続イベントに、[生成元 (is)] および [Netflow] を選択します。 • 管理対象デバイスによって検出された接続イベントに、[生成元でない (is not)] および [Netflow] を選択します。
接続先 (国) または送信元 (国)	接続イベントの送信元または宛先 IP アドレスに関連付けられた国を 1 つ以上選択します。
Device	接続を検出したデバイスを 1 つ以上選択します。または (エクスポートされた NetFlow レコードからの接続データの場合) 接続を処理したデバイスを 1 つ以上選択します。

指定する項目	選択する演算子と内容
ドメイン	1つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。
出力インターフェイスまたは入力インターフェイス	インターフェイスを1つ以上選択します。
出力セキュリティゾーンまたは入力セキュリティゾーン	1つ以上のセキュリティゾーンまたはトンネルゾーンを選択します。
イニシエータバイト数、レスポндаバイト数、または合計バイト数	次のいずれかを入力します。 <ul style="list-style-type: none"> 送信されたバイト数 ([イニシエータバイト数 (Initiator Bytes)])。 受信されたバイト数 ([レスポндаバイト数 (Responder Bytes)])。 送受信されたバイト数 ([合計バイト数 (Total Bytes)])。
イニシエータ IP、レスポнда IP、イニシエータ IP およびレスポнда IP の両方、あるいはイニシエータ IP またはレスポнда IP のいずれか	単一の IP アドレスまたはアドレスブロックを指定します。
イニシエータ パケット数、レスポнда パケット数、または合計パケット数	次のいずれかを入力します。 <ul style="list-style-type: none"> 送信されたパケット数 ([イニシエータ パケット (Initiator Packets)])。 受信されたパケット数 ([レスポнда パケット数 (Responder Packets)])。 送受信されたパケット数 ([合計パケット数 (Total Packets)])
イニシエータ ポート/ICMP タイプまたはレスポнда ポート/ICMP コード	イニシエータ トラフィックのポート番号または ICMP タイプ、あるいはレスポнда トラフィックのポート番号または ICMP コードを入力します。
IOC タグ	接続イベントにより侵害の兆候タグが設定[される (is)] または設定[されない (is not)] かどうかを指定します。
NetBIOS 名	接続におけるモニタ対象ホストの NetBIOS 名を入力します。
NetFlow デバイス	関連ルールをトリガーするために使用する NetFlow エクスポートの IP アドレスを選択します。ネットワーク検出ポリシーに NetFlow エクスポートを追加していない場合、[NetFlow デバイス (NetFlow Device)] ドロップダウン リストは空白になります。
プレフィルタ ポリシー	接続を処理したプレフィルタ ポリシーを1つ以上選択します。

指定する項目	選択する演算子と内容
理由	接続イベントに関連付けられた理由を1つ以上選択します。
セキュリティ インテリジェンス カテゴリ (Security Intelligence Category)	接続イベントに関連付けられたセキュリティインテリジェンスのカテゴリを1つ以上選択します。 接続終了イベントの条件としてセキュリティ インテリジェンス カテゴリを使用するには、アクセス コントロール ポリシーでカテゴリを [ブロック (Block)] ではなく [モニタ (Monitor)] に設定します。
実際の SSL アクション	システムが暗号化された接続をどのように処理したかを示す SSL ルール アクションを指定します。
SSL 証明書のフィンガープリント	トラフィックの暗号化に使用された証明書のフィンガープリントを入力するか、フィンガープリントに関連付けられたサブジェクトの共通名を選択します。
SSL 証明書ステータス (SSL Certificate Status)	セッションの暗号化に使用された証明書に関連付けられたステータスを1つ以上選択します。
SSL 証明書のサブジェクトの共通名 (CN)	セッションの暗号化に使用された証明書のサブジェクトの共通名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの国 (C)	セッションの暗号化に使用された証明書のサブジェクトの国番号を1つ以上選択します。
SSL 証明書のサブジェクトの組織 (O)	セッションの暗号化に使用された証明書のサブジェクトの組織名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの部門 (OU)	セッションの暗号化に使用された証明書のサブジェクトの部門名のすべてまたはその一部を入力します。
SSL 暗号スイート (SSL Cipher Suite)	セッションの暗号化に使用された暗号スイートを1つ以上選択します。
SSL 暗号化セッション (SSL Encrypted Session)	[正常に復号 (Successfully Decrypted)] を選択します。
SSL フローのステータス	システムによるトラフィック復号化試行の結果に基づくステータスを1つ以上選択します。
SSL ポリシー	暗号化された接続をログに記録した SSL ポリシーを1つ以上選択します。
SSL ルール名	暗号化された接続をログに記録した SSL ルールの名前のすべてまたは一部を入力します。
SSL サーバ名	クライアントが暗号化された接続を確立したサーバの名前のすべてまたは一部を入力します。
SSL URL カテゴリ	暗号化された接続でアクセスされた URL のカテゴリを1つ以上選択します。

指定する項目	選択する演算子と内容
SSL バージョン	セッションの暗号化に使用された SSL または TLS バージョンを 1 つ以上選択します。
TCP フラグ	関連ルールをトリガーとして使用するために接続イベントに含まれていなければならない TCP フラグを選択します。NetFlow レコードから生成された接続データにのみ TCP フラグが含まれます。
トランスポート プロトコル	接続で使用されたトランスポート プロトコル: TCP または UDP を入力します。
トンネル/プレフィルタ ルール	接続を処理したトンネルまたはプレフィルタ ルールの名前のすべてまたは一部を入力します。
URL	接続でアクセスされた URL 全体またはその一部を入力します。
URL カテゴリ	接続でアクセスされた URL のカテゴリを 1 つ以上選択します。
URLレピュテーション	接続でアクセスされた URL のレピュテーション値を 1 つ以上選択します。
[ユーザ名 (Username)]	接続でいずれかのホストにログインしたユーザのユーザ名を入力します。
Web アプリケーション	接続に関連付けられた Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。

関連トピック

[接続およびセキュリティ関連の接続イベントフィールド](#)

[IP アドレスの規則](#)

トラフィック プロファイル変化の構文

トラフィックプロファイル変化で関連ルールをベースとして使用するには、まず、使用するトラフィックプロファイルを選択します。ルールは、選択するプロファイルによって特徴付けられるパターンからネットワークトラフィックが逸脱するときにトリガーされます。

raw データ、またはデータから計算された統計情報のいずれかに基づいてルールをトリガーできます。たとえば、ネットワーク内を移動するデータ量（バイト数で測定）が急激に変化した場合、攻撃または他のセキュリティポリシー違反が発生した可能性があります。そのような変動時にトリガーとして使用されるルールを作成できます。以下のいずれかの場合にトリガーとして使用されるよう、ルールを指定できます。

- ネットワーク内を移動するバイト数が特定のバイト数を上回る場合
- ネットワーク内を移動するバイト数が、平均トラフィック量より上または下の特定数の標準偏差を超えて急激に変化した場合

ネットワーク内を移動するバイト数が、特定数の標準偏差からなる範囲を（上または下に）超えたときにトリガーとして使用されるルールを作成するには、次の図に示すように、上限と下限を指定する必要があります。

Select the type of event for this rule

If a traffic profile changes and the profile is Sample Traffic Profile and it meets the following conditions:

OR

are greater than standard deviation(s) use velocity data
 are greater than standard deviation(s) use velocity data

移動するバイト数が、平均より上側の特定数の標準偏差を超えた場合にトリガーするルールを作成するには、以下の図に示されている最初の条件だけを使用します。

移動するバイト数が、平均を基準とした特定数の標準偏差の下側を超えた場合にトリガーとして使用されるルールを作成するには、2番目の条件だけを使用します。

[速度データを使用する (use velocity data)] チェックボックスを選択すると、データポイント間の変化率に基づいて相関ルールをトリガーできます。上記の例で仮に速度データを使用する場合は、次のいずれかの時点でルールがトリガーとして使用されるように指定できます。

- ネットワーク内を移動するバイト数の変化が、平均変化率より上または下の特定数の標準偏差を超えた場合
- ネットワーク内を移動するバイト数の変化が、特定のバイト数を上回った場合

トラフィックプロファイル変化を基準イベントとして選択した場合、以下の表で説明する方法に従って相関ルールの条件を作成します。

表 10: トラフィック プロファイル変化の構文

指定する項目	選択する演算子と入力内容	いずれかを選択
接続数	検出された接続の合計数 または 平均より上または下の標準偏差の数（検出された接続数がこれを超えるとルールがトリガーとして使用されます）	接続 standard deviation(s) : 標準偏差の数

指定する項目	選択する演算子と入力内容	いずれかを選択
合計バイト数、イニシエータバイト数、またはレスポндаバイト数	<p>次のいずれかになります。</p> <ul style="list-style-type: none"> • 送信された合計バイト数 ([合計バイト数 (Total Bytes)]) • 送信されたバイト数 ([イニシエータバイト数 (Initiator Bytes)]) • 受信されたバイト数 ([レスポндаバイト数 (Responder Bytes)]) <p>または</p> <p>平均より上または下の標準偏差の数 (上の条件のいずれかはルールがトリガーとして使用される必要があります)</p>	<p>bytes</p> <p>standard deviation(s) : 標準偏差の数</p>
合計パケット数、イニシエータパケット数、またはレスポндаパケット数	<p>次のいずれかになります。</p> <ul style="list-style-type: none"> • 送信された合計パケット数 ([合計パケット数 (Total Packets)]) • 送信されたパケット数 ([イニシエータパケット (Initiator Packets)]) • 受信されたパケット数 ([レスポндаパケット数 (Responder Packets)]) <p>または</p> <p>平均より上または下の標準偏差の数 (上の条件のいずれかはルールがトリガーとして使用される必要があります)</p>	<p>packets</p> <p>standard deviation(s) : 標準偏差の数</p>
一意のイニシエータ	<p>セッションを開始した個別のホストの数</p> <p>または</p> <p>平均より上または下の標準偏差の数 (検出された一意のイニシエータ数はルールがトリガーとして使用される必要があります)</p>	<p>initiators : イニシエータ数</p> <p>standard deviation(s) : 標準偏差の数</p>
一意のレスポнда	<p>セッションに回答した個別のホストの数</p> <p>または</p> <p>平均より上または下の標準偏差の数 (検出された一意のレスポнда数はルールがトリガーとして使用される必要があります)</p>	<p>responders : レスポнда数</p> <p>standard deviation(s) : 標準偏差の数</p>

相関ホスト プロファイル限定の構文

イベントに関連するホストのホストプロファイルに基づいて相関ルールを制約するには、[ホストプロファイル限定 (host profile qualification)] を追加します。マルウェア イベント、トラフィック プロファイル変化、または新しい IP ホスト検出によってトリガーとして使用される相関ルールには、ホストプロファイル限定を追加することはできません。

ホストプロファイル限定を作成するときには、まず、相関ルールを制約するために使用するホストを指定します。選択可能なホストは、ルールの基盤となるイベントのタイプによって異なります。

- 接続イベント : [レスポнда ホスト (Responder Host)] または [イニシエータ ホスト (Initiator Host)] を選択します。
- 侵入イベント : [宛先ホスト (Destination Host)] または [送信元ホスト (Source Host)] を選択します。
- ディスカバリ イベント、ホスト入力イベントは、またはユーザ アクティビティ : [ホスト (Host)] を選択します。

次の表では、相関ルールのホスト プロファイル限定を作成する方法について説明します。

表 11: ホスト プロファイル限定の構文

指定する項目	選択する演算子と内容
[アプリケーションプロトコル (Application Protocol)] > [アプリケーションプロトコル (Application Protocol)]	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 (Application Protocol)] > [アプリケーションポート (Application Port)]	アプリケーションプロトコルのポート番号を入力します。
[アプリケーションプロトコル (Application Protocol)] > [プロトコル (Protocol)]	プロトコルを選択します。
[アプリケーションプロトコルカテゴリ (Application Protocol Category)]	カテゴリを選択します。
[クライアント (Client)] > [クライアント (Client)]	クライアントを選択します。

指定する項目	選択する演算子と内容
[クライアント (Client)]> [クライアントバージョン (Client Version)]	クライアントバージョンを入力します。
[クライアントカテゴリ (Client Category)]	カテゴリを選択します。
ドメイン	1つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。
ハードウェア	モバイルデバイスのハードウェアモデルを入力します。たとえば、すべての Apple iPhone に一致させるには iPhone と入力します。
[ホストの重要度 (Host Criticality)]	ホストの重要度を選択します。
ホストタイプ	ホストタイプを1つ以上選択します。通常のホスト、またはいずれかのタイプのネットワーク デバイスを選択できます。
[IOC タグ (IOC Tag)]	侵害の兆候タグを1つ以上選択します。
ジェイルブローケン	イベントのホストがジェイルブレイクされたモバイル デバイスであることを示すには [はい (Yes)] を、そうでない場合は [いいえ (No)] を選択します。
[MAC アドレス (MAC Address)]>[MAC アドレス (MAC Address)]	ホストの MAC アドレス全体またはその一部を入力します。
[MAC アドレス (MAC Address)]>[MAC タイプ (MAC Type)]	MAC タイプが ARP/DHCP で検出されるかどうかを選択します。 <ul style="list-style-type: none"> • システムは MAC アドレスがホストに属していることをポジティブに識別した ([ARP/DHCP で検出 (is ARP/DHCP Detected)]) • たとえば、デバイスとホスト間にはルータがあるため、システムはその MAC アドレスを持つ多くのホストを認識している ([ARP/DHCP で検出されない (is not ARP/DHCP Detected)]) • MAC タイプが無関係 ([どれもない (is any)])
[MAC ベンダー (MAC Vendor)]	ホストが使用するハードウェアの MAC ベンダー全体またはその一部を入力します。
Mobile	イベントのホストがモバイル デバイスであることを示すには [はい (Yes)] を、そうでない場合は [いいえ (No)] を選択します。

指定する項目	選択する演算子と内容
[NetBIOS 名 (NetBIOS Name)]	ホストの NetBIOS 名を入力します。
ネットワーク プロトコル	http://www.iana.org/assignments/ethernet-numbers にリストされているネットワーク プロトコル番号を入力します。
[オペレーティングシステム (Operating System)]> [OS ベンダー (OS Vendor)]	オペレーティング システムのベンダー名を 1 つ以上選択します。
[オペレーティングシステム (Operating System)]> [OS 名 (OS Name)]	オペレーティング システムの名前を 1 つ以上選択します。
[オペレーティングシステム (Operating System)]> [OS バージョン (OS Version)]	オペレーティング システムのバージョンを 1 つ以上選択します。
[トランスポートプロトコル (Transport Protocol)]	http://www.iana.org/assignments/protocol-numbers にリストされているトランスポート プロトコルの名前または番号を入力します。
VLAN ID (Admin. VLAN ID)	ホストの VLAN ID 番号を入力します。
Web アプリケーション	Web アプリケーションを選択します。
[Web アプリケーションのカテゴリ (Web Application Category)]	カテゴリを選択します。
使用可能な任意のホスト属性 (デフォルト コンプライアンス allow リスト ホスト属性を含む)	ホスト属性タイプに応じて適切な値を入力または選択します。

暗黙的または汎用のクライアントを使用したホストプロファイル限定の作成

システムが client が続くアプリケーションプロトコルの名前 (たとえば、HTTPS client) を使用して検出されたクライアントをレポートする場合、このクライアントは暗黙的または汎用のクライアントです。これらの場合、システムは特定のクライアントを検出していませんが、サーバ応答トラフィックに基づいてクライアントの存在を推測しています。

暗黙的または汎用のクライアントを使用してホストプロファイル限定を作成するには、クライアントではなく、レスポンド 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使用して制約します。

イベントデータを使用したホスト プロファイル限定の作成

ホストプロファイル限定の制約時に、多くの場合、関連ルールの基本イベントからデータを使用できます。

たとえば、モニタ対象のいずれかのホストで特定のブラウザが使用されていることをシステムが検出した場合に、関連ルールがトリガーとして使用されるとします。さらに、この使用を検出するときに、ブラウザのバージョンが最新でない場合はイベントを生成すると仮定します。

この場合、[クライアント (Client)] は [イベントクライアント (Event Client)] ですが、[クライアントバージョン (Client Version)] が最新のバージョンでない場合にのみルールがトリガーされるように、この関連ルールをホストプロファイル限定に追加できます。

ホストプロファイル限定の例

次のホストプロファイル限定は、ルールの基礎となるディスカバリ イベントに関連するホストが Microsoft Windows のバージョンを実行している場合にのみ、ルールがトリガーとして使用されるように関連ルールを制約します。

Host Profile Qualification Remove Host Profile Qualification

Only collect connection information with the following properties:

Add condition Add complex condition

Initiator Host	Operating System	has the following properties
		OS Vendor is Microsoft
		OS Name is Windows
		OS Version is any

関連トピック

[ホスト データ フィールド](#)

ユーザー限定の構文

接続、侵入、ディスカバリ、またはホスト入力 of どれかのイベントを使用して関連ルールをトリガーとして使用する場合、イベントに関連するユーザのアイデンティティに基づいてルールを制約することができます。この制約は、ユーザ限定と呼ばれます。たとえば、送信元または宛先ユーザのアイデンティティが販売部門所属である場合にのみトリガーとして使用するよう、関連ルールを制約できます。

トラフィック プロファイル変化やユーザ アクティビティ検出によってトリガーとして使用される関連ルールに、ユーザ限定を追加することはできません。また、システムは、アイデンティティ レalmで確立された Management Center サーバの接続を介してユーザの詳細を取得します。この情報は、データベース内のすべてのユーザに関して入手可能とは限りません。

ユーザ限定を作成するときには、まず、関連ルールを制約するために使用するアイデンティティを指定します。選択可能なアイデンティティは、ルールの基本イベントのタイプによって異なります。

- 接続イベント : [イニシエータのアイデンティティ (Identity on Initiator)] または [レスポンドのアイデンティティ (Identity on Responder)] を選択します。

- 侵入イベント：[宛先のアイデンティティ (Identity on Destination)] または [送信元のアイデンティティ (Identity on Source)] を選択します。
- ディスカバリ イベント：[ホストのアイデンティティ (Identity on Host)] を選択します。
- ホスト入力イベント：[ホストのアイデンティティ (Identity on Host)] を選択します。

次の表では、関連ルールのユーザ限定を作成する方法について説明します。

表 12: ユーザ限定の構文

指定する項目	選択する演算子と内容
認証プロトコル (Authentication Protocol)	ユーザを検出するために使用される認証プロトコル (またはユーザタイプ) プロトコルを選択します。
部署名 (Department)	部署を入力します。
ドメイン (Domain)	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。
E メール	電子メールアドレスを入力します。
名	名を入力します。
姓	姓を入力します。
電話	電話番号を入力します。
[ユーザ名 (Username)]	ユーザー名を入力します。

関連トピック

[ユーザーデータのフィールド](#)

接続トラッカー

接続トラッカー は、ルールの最初の基準 (ホスト プロファイルおよびユーザ認定を含む) に一致した後にシステムが特定の接続のトラッキングを始めるよう、関連ルールを制約します。追跡される接続が、指定した期間にわたって収集された追加の基準を満たす場合には、システムがルールの関連イベントを生成します。



ヒント 通常、接続トラッカーは特定のトラフィックだけをモニタし、トリガーとして使用された場合には指定された一定期間だけ実行されます。接続トラッカーは、広範なネットワークトラフィックをモニタして持続的に実行されるトラフィック プロファイルとは対照的です。

接続トラッカーがイベントを生成する方法は2つあります。

条件に一致するとただちに起動する接続トラッカー

ネットワークトラフィックが接続トラッカーの条件に一致すると即座に関連ルールが起動するよう、接続トラッカーを設定できます。この場合、タイムアウト期間が満了していなくても、システムはその接続トラッカーインスタンスでの接続のトラッキングを停止します。関連ルールをトリガーとして使用したのと同じタイプのポリシー違反が再び発生した場合、システムは新しい接続トラッカーを作成します。

ただし、ネットワークトラフィックが接続トラッカーの条件に一致する前にタイムアウト期間が満了した場合、システムは関連イベントを生成せず、そのルールインスタンスの接続のトラッキングを停止します。

たとえば、特定のタイプの接続が特定の期間中に特定回数を超えて発生した場合にのみ関連イベントを生成させることで、接続トラッカーをある種のイベントしきい値として機能させることができます。あるいは、初回接続後に過剰なデータ転送量をシステムが検出した場合にのみ、関連イベントを生成させることもできます。

タイムアウト期間の満了時に起動する接続トラッカー

タイムアウト期間全体にわたって収集されるデータに依存するよう、接続トラッカーを設定できます。この場合、タイムアウト期間が満了するまでは起動しません。

たとえば、特定の期間内に検出された転送量が特定のバイト数を下回った場合に接続トラッカーを起動するよう設定すると、システムはその期間が経過するまで待って、ネットワークトラフィックがその条件に一致した場合はイベントを生成します。

接続トラッカーの追加

始める前に

- 接続、侵入、検出、ユーザID、ホスト入力イベントに基づいて関連ルールを作成します。VPN トラブルシューティング イベント、マルウェアイベント、またはトラフィックプロファイルの変更に基づいたルールに接続トラッカーを追加することはできません。

手順

- ステップ 1** 関連ルールエディタ ([**ポリシー (Policies)**] > [**関連 (Correlation)**] > [**ルールの管理 (Rule Management)**]) で、[**編集 (Edit)**]、[**接続トラッカーの追加 (Add Connection Tracker)**] の順にクリックします。

- ステップ2 追跡する接続を指定します。接続トラッカーの構文 (31 ページ) を参照してください。
- ステップ3 追跡する接続に応じて、いつ相関イベントを生成するかを指定します。接続トラッカーイベントの構文 (34 ページ) を参照してください。
- ステップ4 トラッカーの条件が満たされなければならない時間の間隔 (秒、分または時) を指定します。

接続トラッカーの構文

次の表は、どのような接続を追跡するかを指定する接続トラッカー条件の作成方法を説明しています。

表 13: 接続トラッカーの構文

指定する項目	選択する演算子と内容
アクセス コントロール ポリシー	追跡対象の接続を処理したアクセス コントロール ポリシーを 1 つ以上選択します。
アクセス コントロール ルールのアクション	追跡対象の接続をログに記録したアクセス コントロール ルールに関連付けられたアクセス コントロール ルールアクションを 1 つ以上選択します。 あとで接続を処理するルールまたはデフォルトアクションとは無関係に、任意のモニタールールの条件に一致する接続を追跡するには、[モニタ (Monitor)] を選択します。
アクセス コントロール ルール名	追跡対象の接続をログに記録したアクセス コントロール ルールの名前をすべてまたはその一部を入力します。 モニタールールに一致する接続を追跡するには、モニタールールの名前を入力します。あとで接続を処理するルールまたはデフォルトアクションとは無関係に、システムは該当する接続を追跡します。
アプリケーションプロトコル	アプリケーションプロトコルを 1 つ以上選択します。
アプリケーションプロトコルカテゴリ	アプリケーションプロトコルカテゴリを 1 つ以上選択します。
クライアント	クライアントを 1 つ以上選択します。
クライアントカテゴリ	クライアントカテゴリを 1 つ以上選択します。
クライアントバージョン	クライアントのバージョンを入力します。
接続時間	接続時間 (秒数) を入力します。

指定する項目	選択する演算子と内容
接続タイプ	<p>接続情報がどのように取得されたかに基づいて、関連ルールをトリガーするかどうかを指定します。</p> <ul style="list-style-type: none"> • エクスポートされた NetFlow レコードから生成された接続イベントに、[生成元 (is)] および [Netflow] を選択します。 • 管理対象デバイスによって検出された接続イベントに、[生成元でない (is not)] および [Netflow] を選択します。
接続先 (国) または送信元 (国)	<p>国を 1 つ以上選択します。</p>
Device	<p>追跡対象の接続を検出したデバイスを 1 つ以上選択します。NetFlow 接続を追跡する場合は、エクスポートされた NetFlow レコードからの接続データを処理するデバイスを選択します。</p>
入力インターフェイスまたは出力インターフェイス	<p>インターフェイスを 1 つ以上選択します。</p>
入力セキュリティゾーンまたは出力セキュリティゾーン	<p>1 つ以上のセキュリティゾーンまたはトンネルゾーンを選択します。</p>
イニシエータ IP、レスポнда IP、またはイニシエータ/レスポнда IP	<p>単一の IP アドレスまたはアドレス ブロックを入力します。</p>
イニシエータ バイト数、レスポнда バイト数、または合計バイト数	<p>次のいずれかを入力します。</p> <ul style="list-style-type: none"> • 送信されたバイト数 ([イニシエータ バイト数 (Initiator Bytes)]) • 受信されたバイト数 ([レスポнда バイト数 (Responder Bytes)]) • 送受信されたバイト数 ([合計バイト数 (Total Bytes)])
イニシエータ パケット数、レスポнда パケット数、または合計パケット数	<p>次のいずれかを入力します。</p> <ul style="list-style-type: none"> • 送信されたパケット数 ([イニシエータ パケット (Initiator Packets)]) • 受信されたパケット数 ([レスポнда パケット数 (Responder Packets)]) • 送受信されたパケット数 ([合計パケット数 (Total Pakets)])
イニシエータ ポート/ICMP タイプまたはレスポнда ポート/ICMP コード	<p>イニシエータ トラフィックのポート番号または ICMP タイプ、あるいはレスポнда トラフィックのポート番号または ICMP コードを入力します。</p>
IOC タグ	<p>侵害の兆候タグが設定されて [いる (is)] または設定されて [いない (is not)] かどうかを選択します。</p>

指定する項目	選択する演算子と内容
NETBIOS 名	接続におけるモニタ対象ホストの NetBIOS 名を入力します。
NetFlow デバイス	追跡する NetFlow エクスポートの IP アドレスを選択します。ネットワーク検出ポリシーに NetFlow エクスポートを追加していない場合、[NetFlow デバイス (NetFlow Device)] ドロップダウン リストは空白になります。
プレフィルタ ポリシー	追跡対象の接続を処理したプレフィルタ ポリシーを 1 つ以上選択します。
理由	追跡対象の接続に関連付けられている理由を 1 つ以上選択します。
セキュリティ インテリジェンス カテゴリ	追跡対象の接続に関連付けられているセキュリティ インテリジェンスのカテゴリを 1 つ以上選択します。
TCP フラグ	接続を追跡するために接続に含まれている必要のある TCP フラグを選択します。TCP フラグデータは、エクスポートされた NetFlow レコードから生成された接続にのみ含まれます。
トランスポート プロトコル	接続に使用されるトランスポート プロトコルを選択します。
URL	追跡対象の接続でアクセスされた URL のすべてまたはその一部を入力します。
URL Category	追跡対象の接続でアクセスされた URL のカテゴリを 1 つ以上選択します。
URL レピュテーション	追跡対象の接続でアクセスされた URL のレピュテーション値を 1 つ以上選択します。
[ユーザ名 (Username)]	追跡対象の接続でいずれかのホストにログインしたユーザのユーザ名を入力します。
Web アプリケーション	Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。

イベント データを使用した接続トラッカーの作成

接続トラッカーを作成するときに、多くの場合、関連ルールの基本イベントからデータを使用できます。

たとえば、システムが新しいクライアントを検出するときに、関連ルールがトリガーされると想定します。接続トラッカーをこのタイプの関連ルールに追加すると、システムは次の基本イベントを参照する制約のあるトラッカーを自動的に入力します。

- [イニシエータ/レスポンド IP (Initiator/Responder IP)] が [イベント IP アドレス (Event IP Address)] に設定される。
- [クライアント (Client)] が [イベント クライアント (Event Client)] に設定される。



ヒント 特定の IP アドレスまたは IP アドレス ブロックに関連する接続を追跡するには、[手動エントリにスイッチ (switch to manual entry)] をクリックして、手動で IP を指定します。[イベントフィールドにスイッチ (switch to event fields)] をクリックすると、イベントの IP アドレスを使用する設定に戻ります。

関連トピック

- [接続およびセキュリティ関連の接続イベントフィールド](#)
- [IP アドレスの規則](#)

接続トラッカー イベントの構文

追跡対象の接続に基づいてどのようなときに関連イベントを生成するかを指定する接続トラッカー条件を作成するには、次の表の説明に従います。

表 14: 接続トラッカー イベントの構文

指定する項目	選択する演算子と入力内容
接続数	検出された接続の合計数
SSL 暗号化セッションの数	検出された SSL または TLS 暗号化セッションの合計数
合計バイト数、イニシエータ バイト数、またはレスポンド バイト数	次のいずれかになります。 <ul style="list-style-type: none"> • 送信された合計バイト数 ([合計バイト数 (Total Bytes)]) • 送信されたバイト数 ([イニシエータ バイト数 (Initiator Bytes)]) • 受信されたバイト数 ([レスポンド バイト数 (Responder Bytes)])
合計パケット数、イニシエータ パケット数、またはレスポンド パケット数	次のいずれかになります。 <ul style="list-style-type: none"> • 送信された合計パケット数 ([合計パケット数 (Total Packets)]) • 送信されたパケット数 ([イニシエータ パケット (Initiator Packets)]) • 受信されたパケット数 ([レスポンド パケット数 (Responder Packets)])
一意のイニシエータまたは一意のレスポンド	次のいずれかになります。 <ul style="list-style-type: none"> • 検出されたセッションを開始した個別のホスト数 ([一意のイニシエータ (Unique Initiators)]) • 検出された接続に応答した個別のホスト数 ([一意のレスポンド (Unique Responders)])

外部ホストからの過剰な接続の設定例

ネットワーク 10.1.0.0/16 のセンシティブ ファイルをアーカイブし、通常、ネットワーク外のホストはネットワーク内のホストへの接続を開始することはないシナリオを考慮します。時にはネットワーク外部から接続が開始されることもあります。2分以内に4つ以上の接続が開始された場合には注意が必要だと判断するとします。

次の図に示すルールでは、接続が 10.1.0.0/16 ネットワーク外からネットワーク内に発生したときに、基準に適合するトラッキング接続を開始するように指定します。その後、2分以内に署名に一致する4つの接続（発信側の接続を含む）が検出されても相関イベントを生成します。

Rule Information

Rule Name	Archive Connections - Outside
Rule Description	Trigger on 4 ouside connections tc
Rule Group	Ungrouped

Select the type of event for this rule

If at either the beginning or the en and it meets the following conditions:

[Add condition](#) [Add complex condition](#)

OR	<input type="text" value="Initiator IP"/>	is not in	<input type="text" value="10.1.0.0/16"/>
	<input type="text" value="Responder IP"/>	is in	<input type="text" value="10.1.0.0/16"/>

Connection Tracker

... start tracking connections that meet the following conditions:

[Add condition](#) [Add complex condition](#)

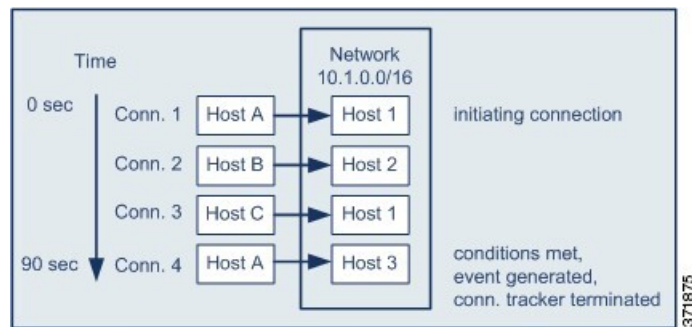
AND	<input type="text" value="Initiator IP"/>	is not in	<input type="text" value="10.1.0.0/16"/>
	<input type="text" value="Responder IP"/>	is in	<input type="text" value="10.1.0.0/16"/>

... and generate an event if:

[Add condition](#) [Add complex condition](#)

<input type="text" value="total"/>	Number of Connections	are greater than or equal to	<input type="text" value="4"/>
------------------------------------	-----------------------	------------------------------	--------------------------------

以下の図は、ネットワーク トラフィックが上記の相関ルールをトリガーとして使用できる方法を示します。



この例では、関連ルールの基本条件に一致する接続をシステムが検出しました。つまり、ネットワーク 10.1.0.0/16 の外部にあるホストからネットワーク内部のホストへの接続をシステムが検出しました。これにより、接続トラッカーが作成されました。

接続トラッカーは、次のステージで処理します。

- ネットワーク外のホスト A からネットワーク内のホスト 1 への接続が検出されると、トラッキング接続を開始します。
- 接続トラッカーの署名に一致する 2 つ以上の接続（ホスト B ~ ホスト 2、ホスト C ~ ホスト 1）を検出します。
- 2 分の時間制限内でホスト A がホスト 3 に接続すると、4 つの認定されている接続を検出します。ルール条件が適合します。
- 最後に、関連イベントを生成し、トラッキング接続を停止します。

BitTorrent の過剰なデータ転送の設定例

最初に監視対象のネットワークのホストに接続後、過剰な BitTorrent データの転送が検出された場合は関連イベントを生成するシナリオを考慮します。

次の図は、監視対象ネットワーク上に BitTorrent アプリケーションプロトコルを検出した場合にトリガーとして使用される関連ルールを示します。このルールには、監視対象ネットワークのホスト（この例では 10.1.0.0/16）が、最初のポリシー違反後の 5 分間に 7 MB を超えるデータ（7340032 バイト）を BitTorrent を介してまとめて転送する場合にのみルールがトリガーとして使用されるように制約する接続トラッカーがあります。

Select the type of event for this rule

If there is new information about a and it meets the following conditions:

AND is in

is

Connection Tracker

... start tracking connections that meet the following conditions:

AND is (switch to event fields)

is

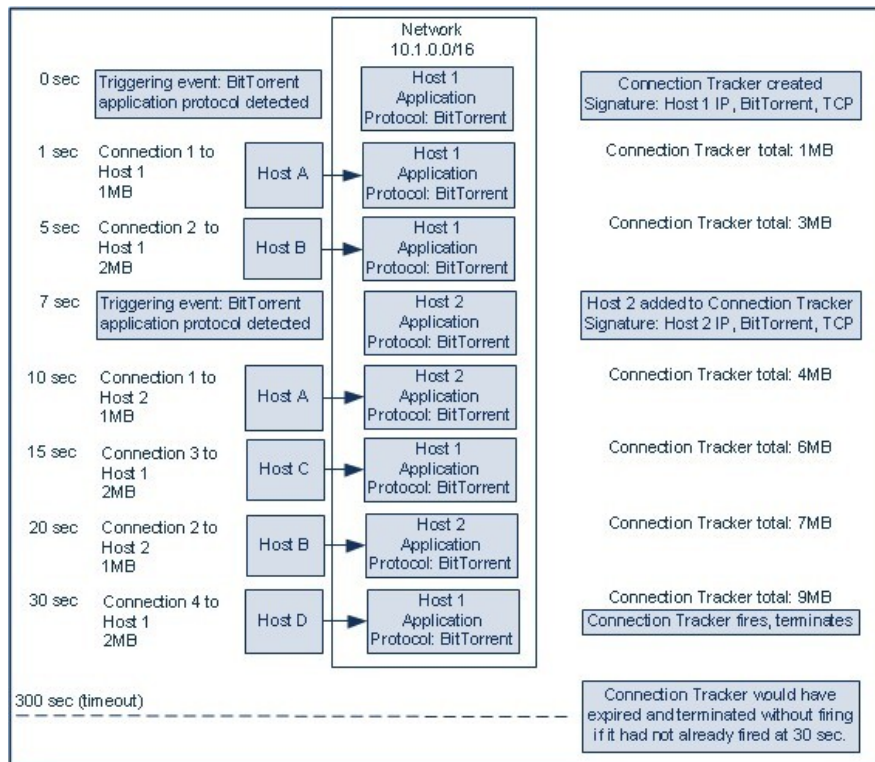
is

... and generate an event if:

are greater than

In the next minutes

以下の図は、ネットワークトラフィックが上記の関連ルールをトリガーとして使用できる方法を示します。



この例では、2つのホスト（ホスト1、ホスト2）に BitTorrent TCP アプリケーションプロトコルが検出されました。この2つのホストは、BitTorrent を介して4つの他のホスト（ホストA、ホストB、ホストC、ホストD）にデータを転送しました。

接続トラッカーは、次の工程で処理しました。

- まず、ホスト1で BitTorrent アプリケーションプロトコルが検出されると、0秒マーカーで接続のトラッキングを開始します。次の5分間に7MBの BitTorrent TCP データの転送が検出されない場合（300秒マーカーにより）、接続トラッカーは無効になる点にご注意ください。
- 5秒で、ホスト1は、署名に一致する3MBデータを転送します。
 - 1秒マーカーでは、ホスト1からホストAへ1MB（供給した接続トラッカーに対して数えた全 BitTorrent トラフィック1MB）
 - 5秒マーカーでホスト1からホストへB 2MB（合計3MB）
- 7秒では、ホスト2で BitTorrent アプリケーションプロトコルを検出し、ホスト2に対しても BitTorrent 接続のトラッキングを開始します。
- 20秒では、ホスト1とホスト2の両方から転送される署名に一致する追加のデータを検出します。
 - 10秒マーカーでホスト2からホストAへ1MB（合計4MB）
 - 15秒マーカーでホスト1からホストCへ2MB（合計6MB）
 - 20秒マーカーでホスト2からホストBへ1MB（合計7MB）
- ホスト1とホスト2が転送した BitTorrent データは合計で7MBになりましたが、転送された合計バイト数が7MBを超過していることが条件となっているため（**Responder Bytes are greater than 7340032**）、ルールはトリガーとして使用されません。この時点で、トラッカーのタイムアウト期間内の残りの280秒の間、追加の BitTorrent 転送が検出されない場合に、トラッカーは無効になり、関連イベントは作成されません。
- ただし、30秒の時点で、別の BitTorrent 転送が検出され、次のルールの条件が満たされません。
 - 30秒マーカーでは、ホスト1からホストDへ2MB（合計9MB）
- 最後に、関連イベントが生成されます。また、5分間が無効にならなくても接続トラッカーインスタンスについてはトラッキング接続を停止します。この時点で BitTorrent TCP アプリケーションプロトコルを用いて新しい接続が検出されると、新しい接続トラッカーが生成されます。ホスト1が2MBすべてをホストDに転送した後に関連イベントが生成される点にご注意ください。これは、セッションが終了するまで接続データを計算することはないためです。

スヌーズ期間および非アクティブ期間

相関ルールでスヌーズ期間を設定することができます。スヌーズ期間を設定すると、相関ルールがトリガーとして使用されたとき、指定した時間間隔内にルール違反が再び発生しても、システムはその期間中はルールのトリガーを停止します。スヌーズ期間が経過すると、ルールは再びトリガー可能になります（新しいスヌーズ期間が始まります）。

たとえば、通常はトラフィックを全く生成しないはずのホストがネットワーク上にあるとします。このホストが関与する接続がシステムで検出されるたびにトリガーとして使用される単純な相関ルールの場合、このホストで送受信されるネットワークトラフィックによっては、短時間に多数の相関イベントが生成される可能性があります。ポリシー違反を示す相関イベントの数を制限するために、スヌーズ期間を追加できます。これにより、（指定した期間内に）システムで検出されたそのホストに関連する最初の接続に対してのみ、システムは相関イベントを生成します。

また、相関ルールで非アクティブ期間を設定することもできます。非アクティブ期間中は、相関ルールはトリガーとして使用されません。非アクティブ期間を毎日、毎週、または毎月繰り返すように設定できます。たとえば、ホストオペレーティングシステム変更を探すために内部ネットワークで夜間にNmapスキャンを実行するとします。この場合、相関ルールが誤ってトリガーとして使用されないよう、毎日のスキャン時間帯に、該当する相関ルールで非アクティブ期間を設定することができます。

相関ルールの作成メカニズム

相関ルールは、ルールがトリガーされる条件を指定して作成します。条件で使用できるシンタックスは、作成しようとしている要素により異なりますが、メカニズムはすべて同じです。

ほとんどの条件は、カテゴリ、演算子、値の3つの部分からなります。

- 相関ルールトリガー、ホストプロファイル認定、接続トラッカー、ユーザ認定のどれを作成しているのかに応じて、選択できるカテゴリが異なります。相関ルールトリガーでは、さらにルールの基本イベントタイプにより選択できるカテゴリが異なります。条件によっては、それぞれ独自の演算子と値を持つ複数のカテゴリが含まれることがあります。
- 条件に使用可能な演算子はカテゴリによって異なります。
- 条件の値を指定するために使用できるシンタックスは、カテゴリと演算子に応じて異なります。場合によっては、テキストフィールドに値を入力する必要があります。それ以外の場合、ドロップダウンリストから値（1つあるいは複数の値）を選択できます。

たとえば、新しいホストが検出されるたびに相関イベントを生成するには、条件を一切含まない単純なルールを作成できます。

Select the type of event for this rule

If and and it meets the following conditions:

ルールをさらに制約して、新しいホストが 10.4.x.x ネットワークで検出された場合にのみイベントを生成するには、1つの条件を追加できます。

Select the type of event for this rule

If and and it meets the following conditions:

構造に複数の条件を含める場合は、それらの条件を **AND** または **OR** 演算子でつなげる必要があります。同じレベルにある複数の条件は、合わせて評価されます。

- **AND** 演算子は、制御対象のレベルにあるすべての条件を満たす必要があることを示します。
- **OR** 演算子は、制御対象のレベルにある少なくとも1つの条件が満たされなければならないことを示します。

10.4.x.x ネットワークおよび 192.168.x.x ネットワーク上の非標準ポートで SSH アクティビティを検出する以下のルールには、4つの条件が設定されており、下の2つは複合条件を形成しています。

Select the type of event for this rule

If and it meets the following conditions:

AND

OR

論理的には、ルールは次のように評価されます。

(A and B and (C or D))

表 15: ルールの評価

値	条件で指定する内容
A	アプリケーションプロトコルが SSH である
B	アプリケーションポートが 22 ではない
C	IP アドレスが 10.0.0.0/8 内にある
D	IP アドレスが 196.168.0.0/16 内にある



注意 頻繁に発生するイベントによってトリガーされる複雑な相関ルールを評価することにより、システムパフォーマンスが低下する可能性があります。たとえば、ロギングするすべての接続に対して、複数の条件からなるルールをシステムが評価しなければならない場合、リソースが過負荷になる可能性があります。

相関ルールへの条件の追加とリンク設定

手順

ステップ 1 相関ルールエディタ ([ポリシー (Policies)] > [相関 (Correlation)] > [ルール管理 (Rule Management)]) で、単純条件または複合条件を追加します。

- 単純: [条件の追加 (Add condition)] をクリックします。
- 複合: [複合条件の追加 (Add complex condition)] をクリックします。

ステップ 2 条件の左にあるドロップダウンリストから [AND] または [OR] 演算子を選択して条件を結合します。

例:単純条件と複合条件の対比

次の図は、単純条件 2 つを [OR] 演算子で結合した相関ルールを示したものです。

Select the type of event for this rule

If and it meets the following conditions:

次の図は、単純条件1つと、複合条件1つを[OR]演算子で結合した相関ルールを示したものです。複合条件は2つの単純条件を[AND]演算子で結合して構成します。

Select the type of event for this rule

If and it meets the following conditions:

相関ルール条件での複数の値の使用

相関条件を作成するときに、条件の構文でドロップダウンリストから値を選択できる場合、通常はリストから複数の値を選択できます。

手順

- ステップ1 相関ルールエディタで、演算子として[存在する (is in)]または[存在しない (is not in)]を選択して1つの条件を作成します。
- ステップ2 テキストフィールド内の任意の場所または[編集 (Edit)]リンクをクリックします。
- ステップ3 [使用可能 (Available)]の下にある複数の値を選択します。また、クリックしてドラッグすることで、隣接する複数の値を選択できます。
- ステップ4 右矢印 (>) をクリックして、選択した項目を [Selected] に移動します。
- ステップ5 [OK] をクリックします。

相関ルールの管理

マルチドメイン展開では、現在のドメインで作成された相関ルールとグループが表示されます。これらは編集可能です。また、先祖ドメインからの選択した相関ルールとグループも表示されますが、これらは編集できません。下位のドメインで作成された相関ルールとグループを表示および編集するには、そのドメインに切り替えます。



- (注) 設定に無関係なドメイン (名前、管理対象デバイスなど) に関する情報が公開されている場合、システムは先祖ドメインからの設定を表示しません。

アクティブな相関ポリシーのルールへの変更は、即座に反映されます。

始める前に

- ルールを削除する場合は、そのルールをすべての相関ポリシーから削除します。詳細については、[相関ポリシーの管理 \(5 ページ\)](#) を参照してください。

手順

ステップ 1 [ポリシー (Policies)] > [相関 (Correlation)] を選択し、[ルール管理 (Rule Management)] をクリックします。

ステップ 2 ルールを管理します。

- 作成 : [ルールの作成 (Create Rule)] をクリックします。[相関ルールの設定 \(5 ページ\)](#) を参照してください。
- グループの作成 : [グループの作成 (Create Group)] をクリックし、グループの名前を入力して、[保存 (Save)] をクリックします。グループにルールを追加するには、ルールを編集します。
- 編集 : [編集 (Edit)] (✎) をクリックします。[相関ルールの設定 \(5 ページ\)](#) を参照してください。代わりに [表示 (View)] (👁) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ルールまたはルールグループの削除 : [削除 (Delete)] (🗑) をクリックします。ルールグループを削除すると、ルールのグループ化が解除されます。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

相関応答グループの設定

アラートおよび修復の相関応答グループを作成し、グループをアクティブにして、アクティブな相関ポリシー内の相関ルールに割り当てることができます。システムは、ネットワークトラフィックが相関ルールに一致すると、すべてグループ化された応答を開始します。

アクティブなグループまたはいずれかのグループ化された応答に対する変更は、アクティブな相関ポリシーで行う場合、ただちに有効になります。

手順

ステップ 1 [ポリシー (Policies)] > [相関 (Correlation)] を選択し、[グループ (Group)] をクリックします。

ステップ 2 [グループの作成 (Create Group)] をクリックします。

ステップ 3 名前を入力します。

ステップ 4 作成時にグループをアクティブにする場合は、[アクティブ (Active)] チェックボックスをオンにします。

非アクティブ化されたグループは応答を開始しません。

ステップ 5 グループに [使用可能な応答 (Available Responses)] を選択し、右矢印 (>) をクリックして、それらを [グループ内の応答 (Responses in Group)] に移動します。応答を他の方法で移動するには、左矢印 (<) を使用します。

ステップ 6 [保存 (Save)] をクリックします。

次のタスク

- 作成時にグループをアクティブにしなかった場合、アクティブにするには、スライダをクリックします。

関連トピック

[Secure Firewall Management Center アラート応答修復の概要](#)

関連応答グループの管理

応答グループは、関連ポリシーで使用されていない場合は削除できます。応答グループを削除することで、その応答のグループ化を解除します。また、応答グループを削除せずに、一時的に非アクティブにすることもできます。これにより、グループはシステムに残りますが、ポリシーに違反するときにはグループが開始されなくなります。

マルチドメイン展開では、現在のドメインで作成されたグループが表示されます。これは編集できます。先祖ドメインで作成されたグループも表示されますが、これは編集できません。下位のドメインで作成されたグループを表示および編集するには、そのドメインに切り替えます。




アクティブな使用中の応答グループへの変更は、即座に反映されます。

手順

ステップ 1 [ポリシー (Policies)] > [関連 (Correlation)] を選択して、[グループ (Group)] をクリックします。

ステップ 2 応答グループを管理します。

- アクティブ化または非アクティブ化：スライダをクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 作成：[グループの作成 (Create Group)] をクリックします。[関連応答グループの設定 \(43 ページ\)](#) を参照してください。

- 編集：[編集 (Edit)] () をクリックします。[相関応答グループの設定 \(43 ページ\)](#) を参照してください。代わりに[表示 (View)] () が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
 - 削除：[削除 (Delete)] () をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
-

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。