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

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することができます。

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 ホワイト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、ディスカバリ、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にのみ、相関イベントが生成されます。
- ユーザ限定を相関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相関ルールを制約することができます。
- スヌーズ期間の追加。相関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、相関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相関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 ホワイトリスト

コンプライアンス ホワイト リストは、ネットワーク上のホストでどのオペレーティング システム、アプリケーション（Web およびクライアント）、プロトコルが許可されるかを指定します。アクティブな相関ポリシーで使用されているホワイト リストにホストが違反した場合、ホワイト リスト イベントがシステムによって生成されます。

相関応答

相関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。それぞれの相関ルールまたはホワイトリストを、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ホワイト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ホワイト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。

相関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、ホワイトリスト、応答を使って、任意のドメイン レベルで相関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。

- ドメインによって相関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 ホワイトリストを作成できます。同じホワイトリストで、異なるドメイン内の異なるサブネットを対象にすることができます。

（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、ユーザ名など）を使用してドメイン間の相関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。

相関ポリシーの設定

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

相関ルール、コンプライアンスのホワイトリスト、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ホワイトリストにプライオリティを割り当てることができます。ルールとホワイトリストのプラオリティは、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ホワイト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 Desription）] 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ホワイトリストを選択して、[追加（Add）] をクリックします。

ステップ 6 各ルールまたはホワイトリストの [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
- なし

- 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 ルールとホワイト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ホワイト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。

次の作業

- 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。

ルールとホワイトリストに応答を追加する

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

それぞれの相関ルールまたはホワイトリストを、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ホワイト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ホワイト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す。

手順

ステップ 1 相関ポリシー エディタで、応答を追加するルールまたはホワイトリストの横にある応答アイコン（  ）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、ルールまたはホワイト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。

相関ポリシーの管理

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

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、非準拠ホストのホワイト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：編集アイコン（ ）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。代わりに表示アイコン（ ）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：削除アイコン（ ）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

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

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、相関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。

はじめる前に

- 相関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、ホストをエクスポートされた NetFlow レコードからネットワーク マップに追加できますが、これらのホストに使用できる情報は限られます（NetFlow データと管理対象デバイス データの違い を参照）。

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）] タブをクリックします。

ステップ 2 [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、相関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。

- 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 アクティビティのイベント トリガー条件の構文，（17 ページ）を参照してください。
- 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，（19 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，（23 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相関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。相関ホスト 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，（30 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。ユーザ限定の構文，（29 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、相関ルールのトリガー後、次に相関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、相関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。

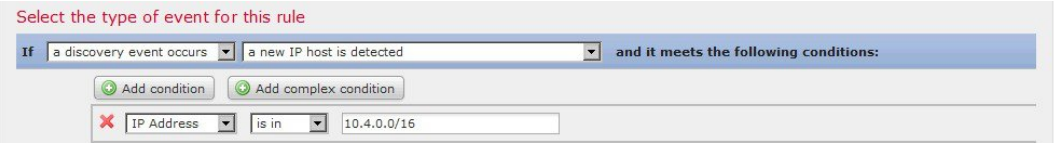
ヒント スヌーズ期間を削除するには、間隔を 0（秒、分、または時間）に指定します。

ステップ 7 [Save Rule] をクリックします。

相関ルールの単純な例

新しいホストが特定のサブネットで検出されると、次の単純な相関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。



次の作業

- 相関ポリシーの設定, （3 ページ）の説明に従って、相関ポリシーでルールを使用します。

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相関ルールの条件を作成します。

表 *1*：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。
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。

指定する項目	選択する演算子と内容
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 Firepower 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。
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。

指定する項目	選択する演算子と内容
[プライオリティ（Priority）]	ルールの優先順位を選択します。 ルールベースの侵入イベントの場合、優先順位は`priority`キーワードまたは`classtype`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。
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	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。 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。
ルール タイプ	ルールをローカルにするかどうかを指定します。 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。
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。

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相関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）]（エンドポイント向け AMP）
- [ネットワークベースのマルウェアの検出（by network-based malware detection）]（ネットワーク向け AMP）
- [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）]（ネットワーク向け AMP）

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相関ルールの条件を作成します。

表 *2*：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 Firepower 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（Event Type）	エンドポイントベースのマルウェア イベントに関連付けられたイベント タイプを 1 つ以上選択します。
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。

指定する項目	選択する演算子と内容
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。
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。

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 イベントで相関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相関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相関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 *3*：相関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

選択するオプション	選択内容
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
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 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 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、相関ルールの条件を作成する方法を説明します。

表 *4*：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。
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 Firepower 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。

指定する項目	選択する演算子と内容
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 [はいい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。
[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。
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。

ユーザ アクティビティのイベント トリガー条件の構文

ユーザ アクティビティで相関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 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（ユーザがホストにログイン）

ユーザ 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相関ルールの条件を作成します。

表 *5*：ユーザ 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 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。
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 Firepower 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）]	ユーザ名を入力します。

ホスト入力イベント トリガー条件の構文

ホスト入力イベントで相関ルールをベースとして使用するには、まず、使用するホスト入力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力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、相関ルールをトリガーとして使用することはできません。

表 *6*：相関ルールのトリガー条件とホスト入力イベント 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）

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
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）
サーバ定義が設定された	サーバ定義の設定（Set Server Definition）
サーバが追加された	ポートの追加（Add Port）
サーバが削除された	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）
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、相関ルールの条件を作成する方法を説明します。

表 7: **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 Firepower 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。

指定する項目	選択する演算子と内容
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。

接続イベント トリガー条件の構文

接続イベントで相関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に、相関ルールの条件を作成する方法を説明します。

表 *8*：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。

指定する項目	選択する演算子と内容
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。 • 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。 • Firepower システムの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。
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 Firepower 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 ゾーンまたはを選択します。
イニシエータ バイト数、レスポンダ 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。 • 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（[レスポンダ バイト数（Responder Bytes）]）。 • 送受信されたバイト数（[合計バイト数（Total Bytes）]）。

指定する項目	選択する演算子と内容
イニシエータ IP、レスポンダ IP、イニシエータおよびレスポンダ IP の両方、あるいはイニシエータ IP またはレスポンダ IP	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、レスポンダ 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。 • 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（[レスポンダ 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ンダ 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、あるいはレスポンダ 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	相関ルールをトリガーするために使用する NetFlow エクスポータの 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 エクスポータ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。
理由（Reason）	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。

指定する項目	選択する演算子と内容
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。
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	相関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。
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。

指定する項目	選択する演算子と内容
[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。

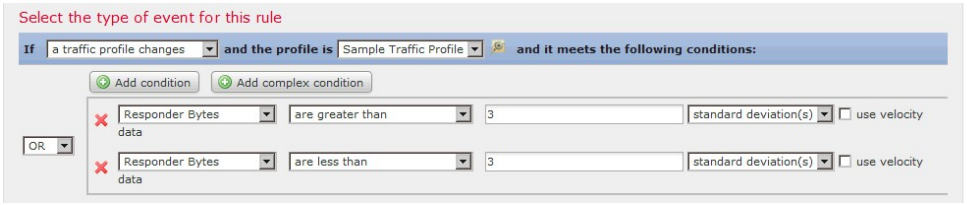
トラフィック プロファイル変化の構文

トラフィック プロファイル変化で相関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ー ポリシー違反が発生した可能性がありますが、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。



  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上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、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 *9*：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
合計バイト数、イニシエータ バイト数、またはレスポンダ バイト数	次のいずれかになります。 • 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（[レスポンダ バイト数（Responder Bytes）]） **または** 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）	bytes standard deviation(s)：標準偏差の数
合計パケット数、イニシエータ パケット数、またはレスポンダ パケット数	次のいずれかになります。 • 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 パケット数（Initiator Packets）]） • 受信されたパケット数（[レスポンダ パケット数（Responder Packets）]） **または** 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）	packets 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
一意のイニシエータ	セッションを開始した個別のホストの数 **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）	initiators：イニシエータ数 standard deviation(s)：標準偏差の数
一意のレスポンダ	セッションに応答した個別のホストの数 **または** 平均より上または下の標準偏差の数（検出された一意のレスポンダ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）	responders：レスポンダ数 standard deviation(s)：標準偏差の数

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：[レスポンダ 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 *10*：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。

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 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。
[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 Firepower 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
[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。 • 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（[どれでもない（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 [はいい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。
[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。

指定する項目	選択する演算子と内容
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ホワイト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、レスポンダ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

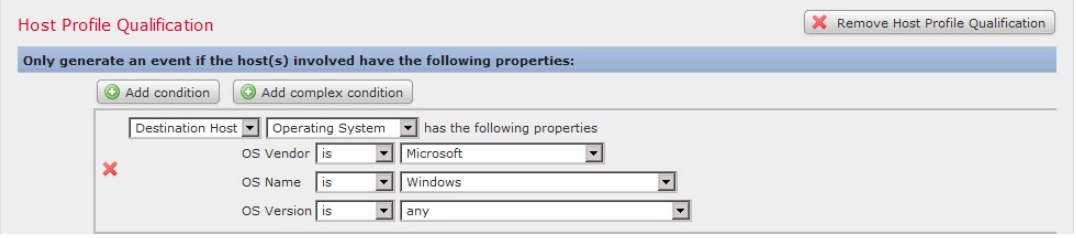
ホストプロファイル限定の制約時に、多くの場合、相関ルールの基本イベントからデータを使用できます。

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、相関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、この相関ルールをホスト 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相関ルールを制約します。



ユーザ限定の構文

接続、侵入、ディスカバリ、またはホスト入力のいずれかのイベントを使用して相関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、相関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相関ルールに、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ルムで確立された Firepower 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、相関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 [レスポンダ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、相関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 *11*：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。

指定する項目	選択する演算子と内容
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 Firepower 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）]	ユーザ名を入力します。

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、相関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相関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相関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。相関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、システムは相関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相関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、相関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

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

はじめる前に

- 接続、侵入、検出、ユーザID、ホスト入力イベントに基づいて相関ルールを作成します。マルウェア イベントやトラフィック 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 相関ルールエディタで、[接続トラッカーの追加（Add Connection Tracker）] をクリックします。

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, （35 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 *12*：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 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 ルールの名前のすべてまたはその一部を入力します。 モニタ ルールに一致する接続を追跡するには、モニタ 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。
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。 • 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。 • Firepower システムの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）	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
Device	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。
入力インターフェイスまたは出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。
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	1 つ以上のセキュリティ ゾーンまたはを選択します。
イニシエータ IP、レスポンダ IP、またはイニシエータ/レスポンダ 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。
イニシエータ バイト数、レスポンダ 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。 • 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（[レスポンダ 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、レスポンダ 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。 • 送信されたパケット数（[イニシエータ パケット数（Initiator Packets）]） • 受信されたパケット数（[レスポンダ 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ンダ 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、あるいはレスポンダ 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	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。
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 エクスポータの 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 エクスポータ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。
理由（Reason）	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。

指定する項目	選択する演算子と内容
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 Application Category）]	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、相関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、相関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相関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/レスポンダ 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。

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相関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。

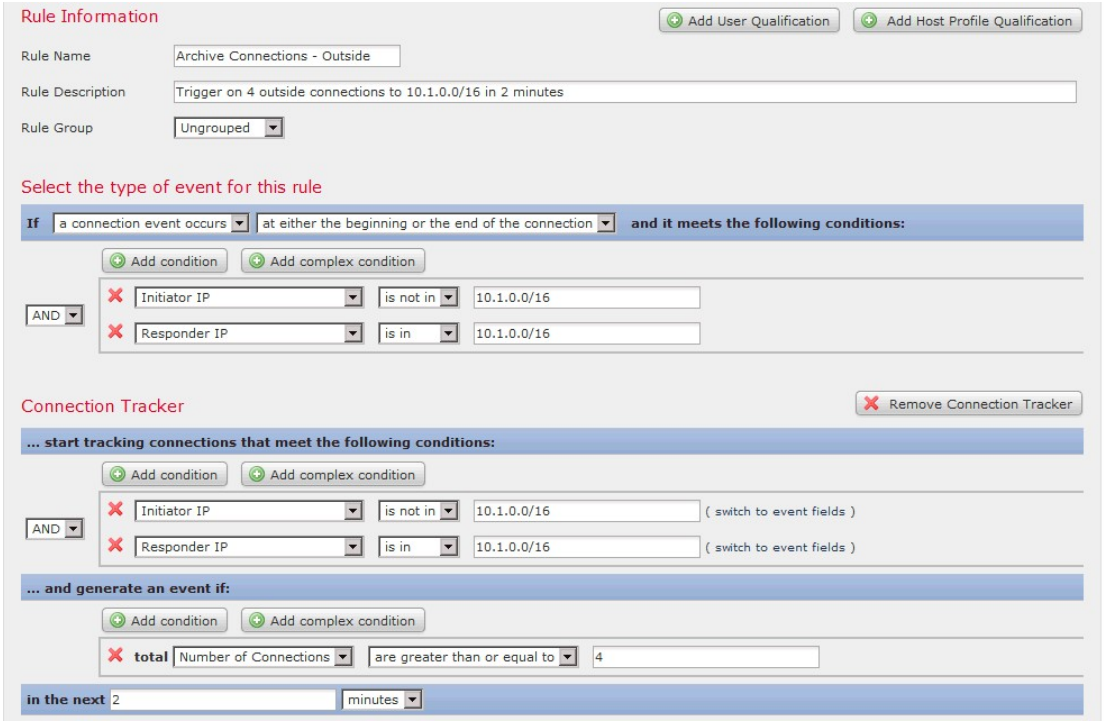
表 *13*：接続トラッカー イベントの構文

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、またはレスポンダ バイト数	次のいずれかになります。 • 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（[レスポンダ バイト数（Responder Bytes）]）
合計パケット数、イニシエータ パケット数、またはレスポンダ パケット数	次のいずれかになります。 • 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 パケット数（Initiator Packets）]） • 受信されたパケット数（[レスポンダ 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ダ	次のいずれかになります。 • 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（[一意のレスポンダ（Unique Responders）]）

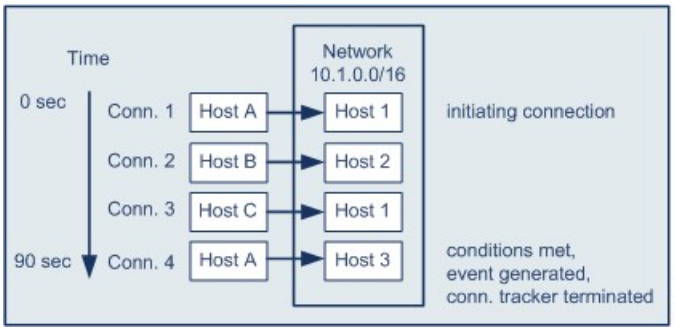
外部ホストからの過剰な接続の設定例

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。ネットワーク外から接続が開始される場合もありますが、2 分以内に 4 つ以上の接続が開始されたときに、これが懸念材料であると判断します。

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。



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、相関ルールの基本的条件に適合する接続が検出されました。つまり、接続が10.1.0.0/16ネットワーク外のホストからネットワーク内のホストへの接続が検出されました。これにより、接続トラッカーが生成されました。

接続トラッカーは、次のステージで処理します。

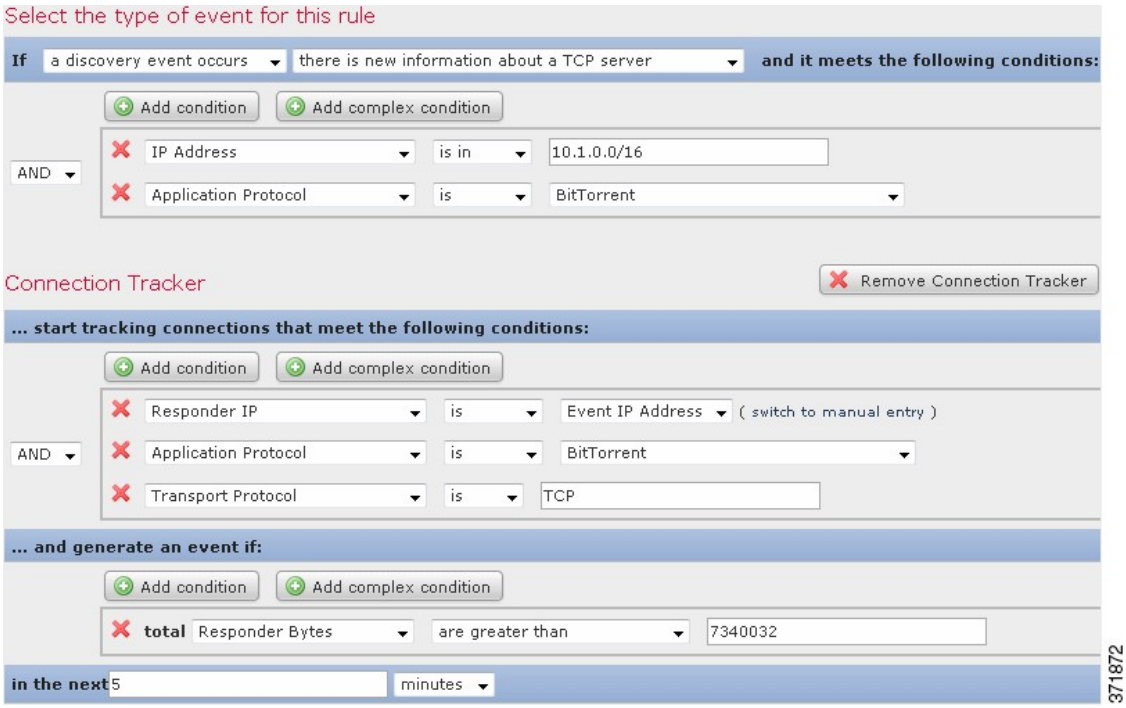
- ネットワーク外のホストAからネットワーク内のホスト1への接続が検出されると、トラッキング接続を開始します。
- 接続トラッカーの署名に一致する2つ以上の接続（ホストB～ホスト2、ホストC～ホスト1）を検出します。
- 2分の時間制限内でホストAがホスト3に接続すると、4つの認定されている接続を検出します。ルール条件が適合します。

- 最後に、相関イベントを生成し、トラッキング接続を停止します。

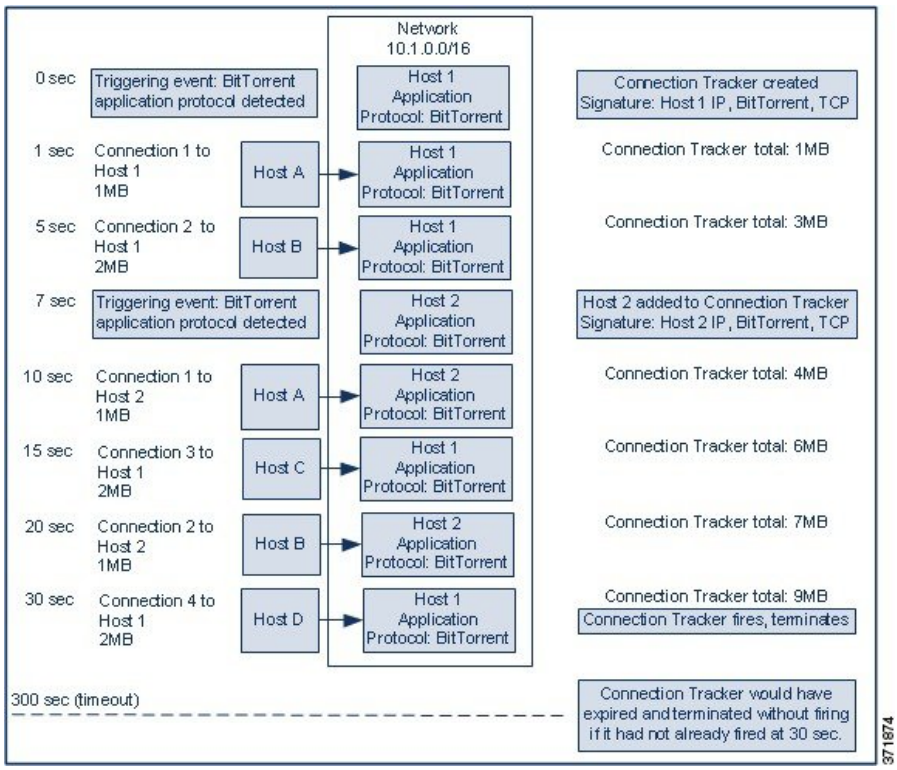
BitTorrent の過剰なデータ転送の設定例

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相関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相関ルールを示します。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。



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、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 分の間に 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 1 MB（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 1 MB）
  - 5 秒マーカーでホスト 1 からホストへ B 2 MB（合計 3 MB）
- 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 1 MB（合計 4 MB）
  - 15 秒マーカーでホスト 1 からホスト C へ 2 MB（合計 6 MB）

- 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 では、現在合わせて 7 MB の BitTorrent データが転送されていますが、ルールはトリガーとして使用されていません。これは、転送された合計バイト数が 7 MB を超えている（[レスポンダのバイトは 7340032 を超えています（Responder Bytes are greater than 7340032）]）必要があるためです。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、相関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す。
  - 30 秒マーカーでは、ホスト 1 からホスト D へ 2 MB（合計 9 MB）
- 最後に、相関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 2 MB すべてをホスト D に転送した後に相関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

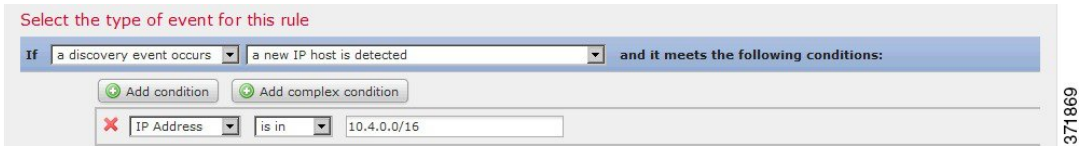
相関ルールは、ルールがトリガーされる条件を指定して作成します。条件で使用できるシンタックスは、作成しようとしている要素により異なりますが、メカニズムはすべて同じです。

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。

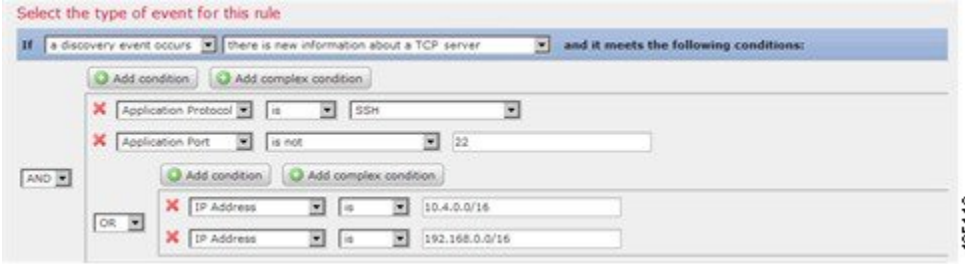
ルールをさらに制約して、新しいホストが 10.4.x.x ネットワークで検出された場合にのみイベントを生成するには、1 つの条件を追加できます。



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、次のように一緒に評価されます。

- AND 演算子は、制御対象のレベルにあるすべての条件が満たされなければならないことを示します。
- 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。



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 *14*：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

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

手順

ステップ 1 相関ルールエディタで、単純条件または複合条件を追加します。

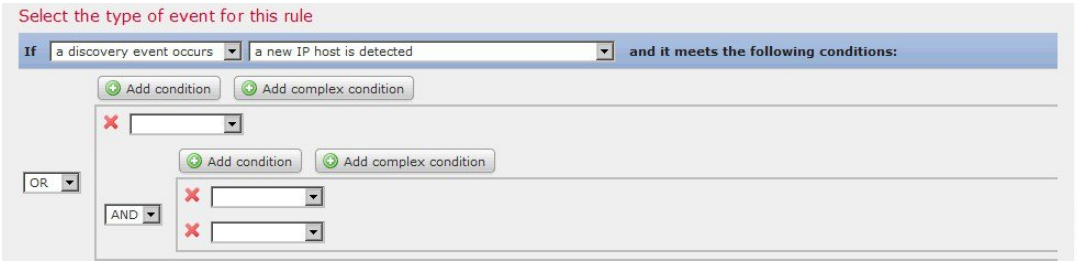
- 単純：[条件の追加（Add condition）] をクリックします。
- 複合：[複合条件の追加（Add complex condition）] をクリックします。

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。

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。



相関ルール条件での複数の値の使用

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

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

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

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。

はじめる前に

- 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）] を選択して、[ルール管理（Rule Management）] タブをクリックします。

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，（6 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：編集アイコン（  ）をクリックします。相関ルールの設定，（6 ページ）を参照してください。代わりに表示アイコン（  ）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：削除アイコン（  ）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

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

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。

次の作業

- 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。

相関応答グループの管理

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

応答グループは、相関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）] > [相関（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。相関応答グループの設定，（44 ページ）を参照してください。

- 編集：編集アイコン（  ）をクリックします。相関応答グループの設定, （44 ページ）を参照してください。代わりに表示アイコン（  ）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：削除アイコン（  ）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。