



関連ポリシーおよび関連ルールの設定

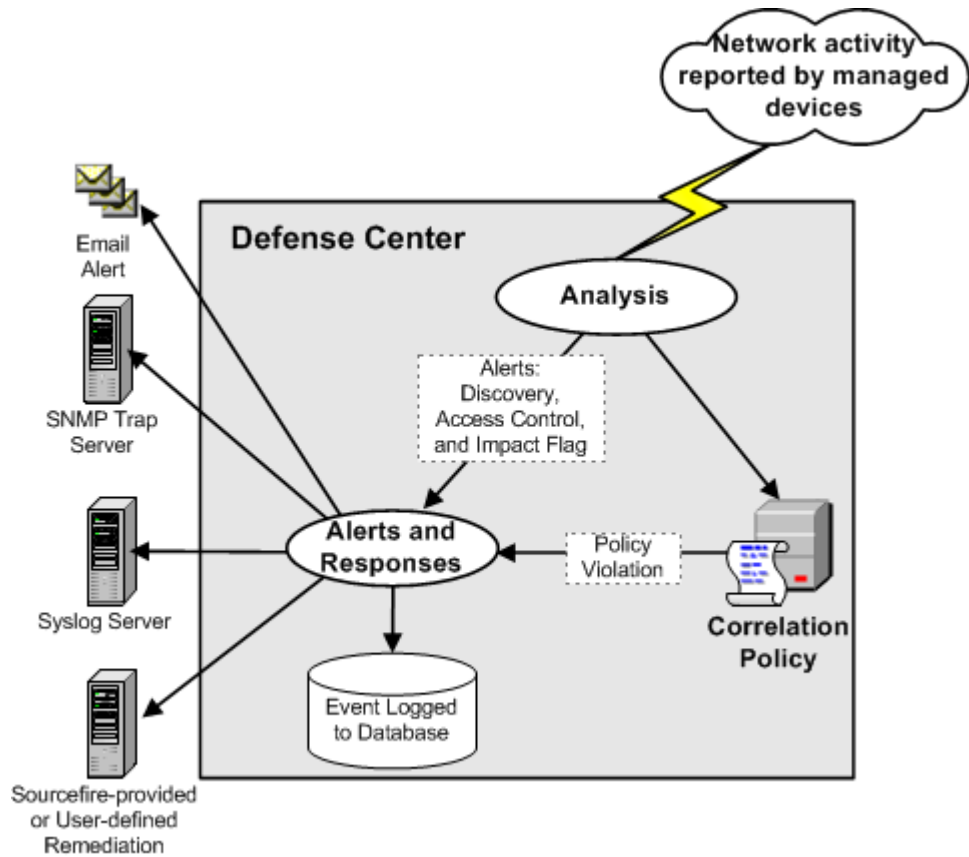
FireSIGHT システムの *関連機能* を使用すると、*関連ポリシー* を作成し、そこに *関連ルール* と *コンプライアンス ホワイト リスト* を含めることで、ネットワークに対する脅威にリアルタイムで対処できます。ネットワーク上のアクティビティによって関連ルールまたはホワイト リストのいずれかがトリガーとして使用されると、*関連ポリシー違反* が発生します。

関連ルールがトリガーとして使用されるのは、FireSIGHT システムによって生成された特定のイベントがユーザ指定の基準に一致した場合、あるいは既存のトラフィック プロファイルで特徴付けられる通常のネットワーク トラフィック パターンからネットワーク トラフィックが逸脱した場合です。

一方、コンプライアンス ホワイト リストがトリガーとして使用されるのは、ネットワーク上のホストが、禁止されているオペレーティング システム、クライアント アプリケーション (またはクライアント)、アプリケーション プロトコル、またはプロトコルを実行しているとシステムが判断した場合です。

ポリシー違反への応答を開始するよう、FireSIGHT システムを設定できます。応答には、単純なアラートやさまざまな修正 (ホストのスキャンなど) が含まれます。応答をグループ化すると、1 つのポリシー違反に対してシステムに複数の応答を開始させることができます。

以下の図に、イベント通知と関連のプロセスを示します。



371895

この章では、相関ルールの作成方法、相関ルールをポリシーで使用方法、応答や応答グループを相関ルールに関連付ける方法、および相関イベントを分析する方法について主に説明します。詳細については、以下を参照してください。

- [相関ポリシーのルールの作成 \(51-3 ページ\)](#)
- [相関ポリシーのルールの管理 \(51-49 ページ\)](#)
- [相関応答のグループ化 \(51-51 ページ\)](#)
- [相関ポリシーの作成 \(51-53 ページ\)](#)
- [相関ポリシーの管理 \(51-58 ページ\)](#)
- [相関イベントの操作 \(51-60 ページ\)](#)

コンプライアンス ホワイトリストおよび相関応答(アラートと修正)を作成する方法の詳細については、以下の項を参照してください。

- [FireSIGHT システムのコンプライアンス ツールとしての使用 \(52-1 ページ\)](#)
- [アラート応答の使用 \(43-2 ページ\)](#)
- [相関ポリシーおよび相関ルールの設定 \(51-1 ページ\)](#)。

関連ポリシーのルールの作成

ライセンス: FireSIGHT、Protection、URL フィルタリング (URL Filtering) または Malware

サポートされるデバイス: 機能に応じて異なる

サポートされる防御センター: 機能に応じて異なる

関連ポリシーを作成する前に、それに含める関連ルールまたはコンプライアンス ホワイト リスト (あるいはその両方) を作成する必要があります。



(注) この項では、関連ルールの作成方法を説明します。コンプライアンス ホワイト リストを作成する方法については、[コンプライアンス ホワイト リストの作成 \(52-8 ページ\)](#) を参照してください。

ユーザ指定の基準にネットワーク トラフィックが一致すると関連ルールがトリガーとして使用され、関連イベントが生成されます。関連ルールを作成するときには、単純な条件を使用することも、条件と制約の組み合わせやネストによって複雑な構造を作成することもできます。

さらに、以下の要素を関連ルールに追加することができます。

- **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**を関連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、関連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、送信元または宛先ユーザのアイデンティティが特定のユーザである場合、または特定の部門 (マーケティング部門など) のユーザ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。
- **スヌーズ期間**および**非アクティブ期間**を追加できます。スヌーズ期間で時間間隔を指定すると、関連ルールが一度トリガーとして使用された後、その時間間隔内にルール違反が再び発生しても、ルールが再びトリガーとして使用されることはありません。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ます (そして新しいスヌーズ期間が始まります)。非アクティブ期間中は、関連ルールはトリガーとして使用されません。



注意

頻繁に発生するイベントによってトリガーとして使用される複雑な関連ルールを評価することにより、防御センターのパフォーマンスが低下する可能性があります。たとえば、システムで記録されるすべての接続に対して、複数の条件からなるルールを 防御センター 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。

次の表は、効果的な関連ルールを作成するために必要となるライセンスを示しています。該当するライセンスがない場合、ライセンス供与されていない FireSIGHT システム機能を使用する関連ルールはトリガーとして使用されません。特定のライセンスの詳細については、[サービス サブスクリプション \(65-8 ページ\)](#) を参照してください。

表 51-1 関連ルールを作成するためのライセンス要件

| 目的 | 必要なライセンス |
|---|-----------------------------|
| 侵入イベントまたはセキュリティ インテリジェンス イベントによって関連ルールをトリガーとして使用する | Protection |
| ディスカバリ イベント、ホスト入力イベント、位置情報データ、またはユーザ アクティビティによって関連イベントをトリガーとして使用する、またはホスト プロファイルやユーザ限定を関連ルールに追加する | FireSIGHT |
| 接続イベントまたはエンドポイント ベースのマルウェア イベントによって関連イベントをトリガーとして使用する、または接続トラッカーをルールに追加する | Any |
| URL データを使用して接続イベントによって関連ルールをトリガーとして使用する、または URL データを使用して接続トラッカーを作成する シリーズ 2 デバイスと DC500 防御センター はどちらも、カテゴリまたはレピュテーションによる URL フィルタリングをサポートしていません。また、シリーズ 2 デバイスはリテラル URL または URL グループによる URL フィルタリングをサポートしていません。 | URL フィルタリング (URL Filtering) |
| ネットワークベースのマルウェア データまたはレトロスペクティブなネットワークベースのマルウェア データに基づいて関連ルールをトリガーとして使用する シリーズ 2 および Blue Coat X-Series 向け Cisco NGIPS デバイスと DC500 防御センター は、ネットワークベースのマルウェア防御をサポートしていないことに注意してください。 | Malware |

メモリの制約上、一部のモデルでは、小規模でそれほど細分化されていないカテゴリとレピュテーションによって URL フィルタリングが実行されます。たとえば、親ドメインのサブサイトがそれぞれ異なる URL カテゴリとレピュテーションを持っている場合、デバイスによっては、すべてのサブサイトで親サイトのデータを使用することがあります。これらのデバイスには、7100 ファミリと、次の ASA FirePOWER モデルが含まれます。ASA 5506- 5506H-X、ASA 5506W-X、ASA 5508-X、ASA -X、ASA 5516-X、ASA 5525-X。

仮想デバイスの場合は、インストール ガイドを参照して、レピュテーション ベースの URL フィルタリングを実行するための適切なメモリ量の割り当てを確認してください。

関連ルール 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。詳細については、[ルールの作成メカニズムについて \(51-41 ページ\)](#)を参照してください。

関連ルールを作成する方法:

アクセス: Admin/Discovery Admin

-
- 手順 1** [ポリシー (Policies)] > [関連 (Correlation)] を選択し、[ルール管理 (Rule Management)] タブを選択します。
- [ルール管理 (Rule Management)] ページが表示されます。
- 手順 2** [ルールの作成 (Create Rule)] をクリックします。
- [ルールの作成 (Create Rule)] ページが表示されます。

- 手順 3 ルールの基本情報(ルールの名前、説明、グループなど)を指定します。
[ルールの基本情報の指定\(51-5 ページ\)](#)を参照してください。
- 手順 4 ルールをトリガーとして使用させる基本的な基準を指定します。
[関連ルール トリガー条件の指定\(51-6 ページ\)](#)を参照してください。
- 手順 5 オプションで、ホスト プロファイル限定をルールに追加します。
[ホスト プロファイル限定の追加\(51-24 ページ\)](#)を参照してください。
- 手順 6 オプションで、接続トラッカーをルールに追加します。
[経時的な接続データを使用した関連ルールの制約\(51-28 ページ\)](#)を参照してください。
- 手順 7 オプションで、ユーザ限定をルールに追加します。
[ユーザ限定の追加\(51-38 ページ\)](#)を参照してください。
- 手順 8 オプションで、非アクティブ期間またはスヌーズ期間(あるいはその両方)をルールに追加します。
[スヌーズ期間および非アクティブ期間の追加\(51-40 ページ\)](#)を参照してください。
- 手順 9 [ルールの保存(Save Rule)]をクリックします。
ルールが保存されます。こうして作成したルールを関連ポリシーの中で使用することも、同じイベントタイプによってトリガーとして使用される他の関連ルールの中で使用することもできます。

ルールの基本情報の指定

ライセンス:任意(Any)

それぞれの関連ルールの名前を入力する必要があり、オプションで簡単な説明を入力できます。また、ルールをルール グループに含めることもできます。

ルールの基本情報を指定する方法:

アクセス:Admin/Discovery Admin

- 手順 1 [ポリシー(Policies)]>[関連(Correlation)]を選択し、[ルール管理(Rule Management)]タブを選択します。
[ルール管理(Rule Management)]ページが表示されます。
- 手順 2 [ルールの作成(Create Rule)]をクリックします。
[ルールの作成(Create Rule)]ページが表示されます。
- 手順 3 [ルールの作成(Create Rule)]ページの[ルール名(Rule Name)]フィールドに、ルールの名前を入力します。
- 手順 4 [ルールの説明(Rule Description)]フィールドに、ルールの説明を入力します。
- 手順 5 オプションで、[ルール グループ(Rule Group)]ドロップダウンリストからルールのグループを選択します。
ルール グループの詳細については、[関連ポリシーのルールの管理\(51-49 ページ\)](#)を参照してください。
- 手順 6 次の項([関連ルール トリガー条件の指定](#))の手順に進みます。

関連ルール トリガー条件の指定

ライセンス:機能に応じて異なる

サポートされるデバイス:機能に応じて異なる

サポートされる防御センター:機能に応じて異なる

単純な関連ルールでは、特定のタイプのイベントが発生することだけを指定します。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関連ルールでは、条件を指定する必要はまったくありません。一方、複数の条件がネストされた複雑な関連ルールにすることもできます。たとえば、以下の図に示すルールは、10.x.x.x サブネットに含まれない IP アドレスから IGMP メッセージが送信された場合にルールをトリガーとして使用するという基準で構成されています。

メモリの制約上、一部のモデルでは、小規模でそれほど細分化されていないカテゴリとレピュテーションによって URL フィルタリングが実行されます。たとえば、親 URL のサブサイトがそれぞれ異なる URL カテゴリとレピュテーションを持っている場合、一部のデバイスでは、すべてのサブサイトに対して親 URL のデータが使用されます。具体的な例として、システムは google.com カテゴリとレピュテーションを使用して mail.google.com を評価します。これに該当するデバイスは、71xx ファミリ と次の ASA モデルです。ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X、ASA5525-X。

Select the type of event for this rule

If and it meets the fol



(注) イベントに基づく条件を作成するときに、関連ルール トリガー基準を追加できるのは、デバイスがその条件に必要な情報を収集でき、しかも 防御センター でその情報を管理できる場合に限られます。たとえば、シリーズ 2 デバイスと DC500 防御センター はいずれも SSL インスペクション、カテゴリまたはレピュテーション別の URL フィルタリング、またはセキュリティ インテリジェンスをサポートしないので、それらの機能に基づいてそれらのアプライアンスでイベント条件を設定することはできません。詳細については、[関連ポリシーのルールの作成 \(51-3 ページ\)](#) を参照してください。

関連ルール トリガー基準を指定する方法:

アクセス: Admin/Discovery Admin

手順 1 ルールの基礎となるイベントのタイプを選択します。

関連ルールを作成するときは、まず始めに、ルールの基礎となるイベントのタイプを選択する必要があります。[このルールのイベントのタイプを選択する (Select the type of event for this rule)] の下には、次のオプションがあります。

- 特定の侵入イベントが発生したときにルールをトリガーとして使用する場合は、[侵入イベントの発生 (an intrusion event occurs)] を選択します。
- 特定のマルウェア イベントが発生したときにルールをトリガーとして使用する場合は、[マルウェア イベントの発生 (a Malware event occurs)] を選択します。
- 特定のディスカバリ イベントが発生したときにルールをトリガーとして使用する場合は、[ディスカバリ イベントの発生 (a discovery event occurs)] を選択します。また、ディスカバリ イベントによって関連ルールをトリガーとして使用する場合は、使用するイベントのタイプを選択する必要があります。[ディスカバリ イベントのタイプについて \(50-10 ページ\)](#) で説明されているディスカバリ イベントのサブセットから選択可能です (たとえばホップ変更によって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)。ただし、[任意のタイプのイベント発生時 (there is any type of event)] を選択すると、あらゆる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。
- 新しいユーザが検出されたとき、またはユーザがホストにログインしたときにルールをトリガーとして使用する場合は、[ユーザ アクティビティの検出 (user activity is detected)] を選択します。
- 特定のホスト入力イベントが発生したときにルールをトリガーとして使用する場合は、[ホスト入力イベントの発生 (a host input event occurs)] を選択します。また、ホスト入力イベントによって関連ルールをトリガーとして使用する場合は、使用するイベントのタイプを選択する必要があります。[ホスト入力イベントのタイプについて \(50-14 ページ\)](#) で説明されているイベントのサブセットから選択可能です。
- 接続データが特定の基準を満たすときにルールをトリガーとして使用する場合は、[接続イベントの発生 (a connection event occurs)] を選択します。また、接続イベントで関連ルールをトリガーとして使用する場合には、接続の開始、終了のどちら (またはその両方) を表す接続イベントを使用するかを選択する必要があります。
- 既存のトラフィック プロファイルで特徴付けられた通常のネットワーク トラフィック パターンからネットワーク トラフィックが逸脱したときに関連ルールをトリガーとして使用する場合は、[トラフィック プロファイルの変更 (a traffic profile changes)] を選択します。

手順 2 ルールの条件を指定します。

関連ルール トリガー基準の条件で使用できる構文は、ステップ 1 で選択した基本イベントにより異なりますが、メカニズムは同じです。詳細については、[ルールの作成メカニズムについて \(51-41 ページ\)](#) を参照してください。

条件を作成するために使用できる構文については、以下の項で説明します。

- [侵入イベントの構文 \(51-8 ページ\)](#)
- [マルウェア イベントの構文 \(51-11 ページ\)](#)
- [ディスカバリ イベントの構文 \(51-13 ページ\)](#)
- [ユーザ アクティビティ イベントの構文 \(51-16 ページ\)](#)
- [ホスト入力イベントの構文 \(51-17 ページ\)](#)
- [接続イベントの構文 \(51-18 ページ\)](#)
- [トラフィック プロファイル変化の構文 \(51-22 ページ\)](#)



ヒント

ステップ 1 で指定した同じ基本イベント タイプを共有する複数のルールをネストさせることができます。たとえば、オープン TCP ポートの検出に基づく新しいルールを作成する場合、その新規ルールのトリガー基準に [「MyDoom Worm」ルールが真である (rule “MyDoom Worm” is true)] および [「Kazaa (TCP) P2P」ルールが真である (rule “Kazaa (TCP) P2P” is true)] を含めることができます。

手順 3 オプションで、以下の項の手順に進みます。

- [ホスト プロファイル限定の追加 \(51-24 ページ\)](#)
- [経時的な接続データを使用した関連ルールの制約 \(51-28 ページ\)](#)
- [ユーザ限定の追加 \(51-38 ページ\)](#)
- [スヌーズ期間および非アクティブ期間の追加 \(51-40 ページ\)](#)

関連ルールの作成が終了した場合は、[関連ポリシーのルールの作成 \(51-3 ページ\)](#) で説明している手順のステップ 9 に進んでルールを保存します。

侵入イベントの構文

ライセンス:Protection

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。

ルール条件を作成するときには、ネットワーク トラフィックによってルールをトリガーできることを確認してください。個々の侵入イベントで使用可能な情報は、検出方法やロギング方法など、いくつかの要因によって異なります。詳細については、[侵入イベントについて \(41-12 ページ\)](#) を参照してください。

表 51-2 侵入イベントの構文

| 指定する項目 | 演算子を指定した後に行う操作 |
|---|--|
| アクセス コントロール ポリシー (Access Control Policy) | 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 (Access Control Rule Name) | 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 (Application Protocol) | 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 (Application Protocol Category) | 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 (Classification) | 1 つ以上の分類を選択します。 |
| クライアント (Client) | 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 (Client Category) | クライアントのカテゴリを 1 つ以上選択します。 |

表 51-2 侵入イベントの構文(続き)

| 指定する項目 | 演算子を指定した後に行う操作 |
|--|--|
| 宛先国 (Destination Country) または送信元国 (Source Country) | 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 (Destination Ip)、送信元 IP (Source IP)、または送信元/宛先 IP (Source/Destination 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。FireSIGHT システムで使用する IP アドレス表記およびプレフィックス長については、 IP アドレスの表記規則 (1-24 ページ) を参照してください。 |
| 宛先ポート/ICMP コード (Destination Port/ICMP Code) または送信元ポート/ICMP タイプ (Source Port/ICMP Type) | 送信元トラフィックのポート番号または ICMP タイプ、あるいは宛先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。 |
| 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。 |
| 出力インターフェイス (Egress Interface) または入力インターフェイス (Ingress Interface) | 1 つ以上のインターフェイスを選択します。 |
| 出力セキュリティゾーン (Egress Security Zone) または入力セキュリティゾーン (Ingress Security Zone) | セキュリティゾーンを 1 つ以上選択します。 |
| ジェネレータ ID (Generator ID) | プリプロセッサを 1 つ以上選択します。使用可能なプリプロセッサの詳細については、 ネットワーク分析ポリシーでのプリプロセッサの設定 (26-7 ページ) を参照してください。 |
| 影響フラグ (Impact Flag) | <p>侵入イベントに割り当てられる影響レベルを選択します。is、is not、is greater than などを指定する演算子と一緒に、以下のいずれかを選択します。</p> <ul style="list-style-type: none"> • 0: グレー (不明) • 1: レッド (脆弱) • 2: オレンジ (脆弱の可能性あり) • 3: イエロー (現在は脆弱でない) • 4: ブルー (不明なターゲット) <p>(注) NetFlow データに基づいてネットワーク マップに追加されたホストに関して使用可能なオペレーティング システム情報はありません。そのため、ホスト入力機能を使って手動でホスト オペレーティング システム アイデンティティを設定しない限り、防御センターは、これらのホストが関与する侵入イベントに「脆弱」(レベル 1: レッド) 影響レベルを割り当てることができません。</p> <p>詳細については、影響レベルを使用してイベントを評価する (41-41 ページ) を参照してください。</p> |

表 51-2 侵入イベントの構文(続き)

| 指定する項目 | 演算子を指定した後に行う操作 |
|---|---|
| インライン結果 (Inline Result) | 次のいずれかを選択します。 <ul style="list-style-type: none"> dropped は、インライン型、スイッチ型、またはルーティング型展開でパケットがドロップされたかどうかを示します。 would have dropped は仮定を表します。インライン型、スイッチ型、またはルーティング型展開でパケットをドロップするよう侵入ポリシーが設定されていると仮定した場合、パケットがドロップされるかどうかを示します。 <p>侵入ポリシーのドロップ動作や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ないことに注意してください。</p> |
| 侵入ポリシー (Intrusion Policy) | 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 (IOC Tag) | 侵入イベントの結果として IOC タグが設定されているか (is)、または設定されていないか (is not) を選択します。 |
| [プライオリティ (Priority)] | ルールのプライオリティとして、 low 、 medium または high のいずれかを選択します。ルールベースの侵入イベントの場合、プライオリティは 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 | 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。プロトコル番号は、 Http://www.iana.org/assignments/protocol-numbers にあります。 |
| ルール メッセージ (Rule Message) | ルール メッセージ全体またはその一部を入力します。 |
| ルール SID (Rule SID) | 単一の Snort ID 番号 (SID) またはカンマで区切った複数の SID を入力します。 (注) 演算子として [is in] または [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。複数 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 (Rule Type) | ルールがローカルか、ローカルでないかを指定します。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したときに作成される共有オブジェクトのルールの新規インスタンスが含まれます。詳細については、 既存のルールの変更 (36-114 ページ) を参照してください。 |
| 実際の SSL アクション (SSL Actual Action) | 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 (SSL Certificate Fingerprint) | 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 証明書サブジェクトの共通名 (CN) (SSL Certificate Subject Common Name (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共通名またはその一部を入力します。 |
| SSL 証明書サブジェクトの国 (C) (SSL Certificate Subject Country (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国別コードを 1 つ以上選択します。 |

表 51-2 侵入イベントの構文(続き)

| 指定する項目 | 演算子を指定した後に行う操作 |
|---|---|
| SSL 証明書サブジェクトの組織 (O)(SSL Certificate Subject Organization (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組織名またはその一部を入力します。 |
| SSL 証明書サブジェクトの組織単位 (OU)(SSL Certificate Subject Organizational Unit (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組織単位名またはその一部を入力します。 |
| SSL フロー ステータス (SSL Flow Status) | 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 1 つ以上のステータスを選択します。 |
| [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。 |
| 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 (Web Application) | 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 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。 |

マルウェア イベントの構文

ライセンス: Any、または Malware

サポートされるデバイス: 機能に応じて異なる

サポートされる防御センター: 機能に応じて異なる

マルウェア イベントに基づく関連ルール条件の構文は、イベントがエンドポイント ベースのマルウェア エージェントによって報告されるのか、管理対象デバイスによって検出されるのか、または管理対象デバイスによって検出されレトロスペクティブにマルウェアとして識別されるのかによって異なります。

シリーズ 2 および Blue Coat X-Series 向け Cisco NGIPS デバイスと DC500 防御センター はネットワークベースのマルウェア防御をサポートしていないので、これらのアプライアンスは、ネットワークベースのマルウェア データまたはレトロスペクティブなネットワークベースのマルウェア データに基づくマルウェア イベントによる関連ルール トリガーをサポートしないことに注意してください。

ルール条件を作成するときには、ネットワーク トラフィックによってルールをトリガーできることを確認してください。個々の接続イベントまたは接続サマリ 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。詳細については、[マルウェア イベント テーブルについて \(40-22 ページ\)](#) を参照してください。

■ 関連ポリシーのルール作成

マルウェア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 51-3 マルウェアイベントの構文

| 指定する項目 | 演算子を指定した後に行う操作 |
|---|---|
| アプリケーションプロトコル (Application Protocol) | 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 (Application Protocol Category) | 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 (Client) | 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 (Client Category) | クライアントのカテゴリを 1 つ以上選択します。 |
| 宛先国 (Destination Country) または送信元国 (Source Country) | 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。 |
| 宛先 IP (Destination IP)、ホスト IP (Host IP)、または送信元 IP (Source 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。FireSIGHT システムで使用する IP アドレス表記については、 IP アドレスの表記規則 (1-24 ページ) を参照してください。 |
| 宛先ポート/ICMP コード (Destination Port/ICMP Code) | 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 (Disposition) | Malware または Custom Detection、あるいはその両方を選択します。 |
| イベント タイプ (Event Type) | マルウェア イベントに関連付けられたエンドポイント ベースのイベント タイプを 1 つ以上選択します。詳細については、 マルウェア イベントのタイプ (40-28 ページ) を参照してください。 |
| ファイル名 (File Name) | ファイルの名前を入力します。 |
| ファイル タイプ (File Type) | ファイルのタイプを選択します (たとえば PDF、MSEXE など)。 |
| ファイル タイプ カテゴリ (File Type Category) | ファイル タイプのカテゴリを 1 つ以上選択します (たとえば Office Documents、Executables など)。 |
| IOC タグ (IOC Tag) | マルウェア イベントの結果として IOC タグが設定されているか (is)、または設定されていないか (is not) 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 (SSL Actual Action) | 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 (SSL Certificate Fingerprint) | 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 証明書サブジェクトの共通名 (CN) (SSL Certificate Subject Common Name (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共通名またはその一部を入力します。 |

表 51-3 マルウェア イベントの構文(続き)

| 指定する項目 | 演算子を指定した後に行う操作 |
|---|--|
| SSL 証明書サブジェクトの国 (C)(SSL Certificate Subject Country (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国別コードを 1 つ以上選択します。 |
| SSL 証明書サブジェクトの組織 (O)(SSL Certificate Subject Organization (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組織名またはその一部を入力します。 |
| SSL 証明書サブジェクトの組織単位 (OU)(SSL Certificate Subject Organizational Unit (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組織単位名またはその一部を入力します。 |
| SSL フロー ステータス (SSL Flow Status) | 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 1 つ以上のステータスを選択します。 |
| 送信元ポート/ICMP タイプ (Source Port/ICMP Type) | 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 (Web Application) | 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 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。 |

ディスカバリ イベントの構文

ライセンス:FireSIGHT

ディスカバリ イベントに基づく関連ルールにする場合は、まず、使用するイベントのタイプをドロップダウンリストから選択する必要があります。次の表に、トリガー基準としてドロップダウンリストから選択できるイベントをリストし、対応するイベントタイプを示します。ディスカバリ イベントタイプの詳細については、[ディスカバリ イベントのタイプについて \(50-10 ページ\)](#)を参照してください。

表 51-4 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 |
|---|------------------------|
| クライアントが変更された (a client has changed) | クライアント更新 |
| a client timed out (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 |
| a host IP address is reused (ホスト IP アドレスが再使用された) | DHCP:IP アドレスの再割り当て |
| a host is deleted because the host limit was reached (ホスト制限に達したためホストが削除される) | ホスト削除:ホスト制限に到達 |
| a host is identified as a network device (ホストがネットワーク デバイスとして定義されている) | ネットワーク デバイスへのホストタイプの変更 |

表 51-4 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(続き)

| 選択オプション | ルールをトリガーとして使用するイベント タイプ |
|--|-------------------------|
| a host timed out(ホストがタイムアウトになった) | ホスト タイムアウト |
| a host's IP address has changed(ホストの IP アドレスが変更された) | DHCP:IP アドレスの変更 |
| a NETBIOS name change is detected(NETBIOS 名の変更が検出された) | NetBIOS 名の変更 |
| a new client is detected(新しいクライアントが検出された) | 新しいクライアント |
| a new IP host is detected(新しい IP ホストが検出された) | 新しいホスト |
| a new MAC address is detected(新しい MAC アドレスが検出された) | ホストの追加 MAC の検出 |
| a new MAC host is detected(新しい MAC ホストが検出された) | 新しいホスト |
| a new network protocol is detected(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 |
| a new transport protocol is detected(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 |
| a TCP port closed(TCP ポートが閉じられた) | TCP ポート クローズ |
| a TCP port timed out(TCP ポートがタイムアウトになった) | TCP ポート タイムアウト |
| a UDP port closed(UDP ポートが閉じられた) | UDP ポート クローズ |
| a UDP port timed out(UDP ポートがタイムアウトになった) | UDP ポート タイムアウト |
| a VLAN tag was updated(VLAN タグがアップデートされた) | VLAN タグ情報の更新 |
| an IOC was set(IOC が設定された) | 侵害の痕跡(兆候) |
| an open TCP port is detected(開いた TCP ポートが検出された) | 新しい TCP ポート |
| an open UDP port is detected(開いた UDP ポートが検出された) | 新しい UDP ポート |
| the OS information for a host has changed(ホストの OS 情報が変更された) | 新しい OS |
| the OS or server identity for a host has a conflict(OS またはホストのサーバ ID でコンフリクトが発生) | アイデンティティ競合 |
| the OS or server identity for a host has timed out(OS またはホストのサーバ ID がタイムアウトになった) | アイデンティティ タイムアウト |
| there is any kind of event(任意のタイプのイベント発生時) | (任意のイベント タイプ) |
| there is new information about a MAC address(MAC アドレスに関する新しい情報がある) | MAC 情報の変更 |

表 51-4 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(続き)

| 選択オプション | ルールをトリガーとして使用するイベント タイプ |
|---|-------------------------|
| there is new information about a TCP server (TCP サーバについて新情報がある) | TCP サーバ情報の更新 |
| there is new information about a UDP server (UDP サーバについて新情報がある) | UDP サーバ情報の更新 |

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、ライセンス 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発生時 (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。

ディスカバリ イベントのタイプを選択した後、以下の表で説明されているように関連ルールの条件を作成できます。選択したイベントタイプに応じて、以下の表に示す基準のサブセットを使用して条件を作成できます。たとえば、新しいクライアントの検出時に関連ルールをトリガーとして使用する場合、ホストの IP または MAC アドレス、クライアントの名前、タイプ、バージョン、およびイベントを検出したデバイスに基づいて条件を作成できます。

表 51-5 ディスカバリ イベントの構文

| 指定する項目 | 演算子を指定した後に行う操作 |
|--|--|
| 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 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 (Application Protocol Category) | 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 (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。 |
| クライアント (Client) | 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 (Client Category) | 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 (Client Version) | 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。 |
| ハードウェア (Hardware) | 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 (Host Type) | ドロップダウンリストから 1 つ以上のホストタイプを選択します。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 (IP Address) または新しい IP アドレス (New 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。FireSIGHT システム で使用する IP アドレス表記については、 IP アドレスの表記規則 (1-24 ページ) を参照してください。 |
| ジェイルブレイク (Jailbroken) | 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。 |

表 51-5 ディスカバリ イベントの構文(続き)

| 指定する項目 | 演算子を指定した後に行う操作 |
|---|---|
| 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。 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 [次で始まる (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 Type) | MAC アドレスが ARP/DHCP で検出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識別したのか (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 (is not ARP/DHCP Detected) を選択します。 |
| MAC ベンダー (MAC Vendor) | 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。 |
| [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 (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。 |
| OS ベンダー (OS Vendor) | 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 のバージョン (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。 |
| プロトコル (Protocol) ま たは トランスポートプロトコ ル (Transport Protocol) | 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。プロトコル番号は、 Http://www.iana.org/assignments/protocol-numbers にあります。 |
| 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 (Source Type) | 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 Application) | 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 イベントの構文

ライセンス: FireSIGHT

ユーザ アクティビティに基づく関連ルールにする場合は、まず、使用するユーザ アクティビ
ティのタイプをドロップダウンリストから選択する必要があります。

- a user logged into a host (ホストへのユーザ ログイン) または
- a new user identity was detected (新しいユーザ ID の検出)

ユーザ アクティビティのタイプを選択した後、以下の表で説明されているように関連ルールの条件を作成できます。選択したユーザ アクティビティのタイプに応じて、以下の表に示す基準のサブセットを使って条件を作成できます。新しいユーザ ID によってトリガーとして使用される関連ルールでは、IP アドレスを指定できません。

表 51-6 ユーザ アクティビティの構文

| 指定する項目 | 演算子を指定した後に行う操作 |
|------------------------|---|
| 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。 |
| [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。FireSIGHT システム で使用する IP アドレス表記については、 IP アドレスの表記規則 (1-24 ページ) を参照してください。 |
| [ユーザ名 (Username)] | ユーザ名を入力します。 |

ホスト入力イベントの構文

ライセンス: FireSIGHT

ホスト入力イベントに基づく関連ルールにする場合は、まず、使用するホスト入力イベントのタイプをドロップダウンリストから選択する必要があります。次の表に、トリガー基準としてドロップダウンリストから選択できるイベントをリストし、対応するホスト入力イベントタイプを示します。ホスト入力イベントタイプの詳細については、[ホスト入力イベントのタイプについて \(50-14 ページ\)](#) を参照してください。

表 51-7 関連ルールのトリガー条件とホストの入力イベントタイプ

| 選択オプション | 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ました (a client is added) | クライアントの追加 |
| クライアントが削除されました (a client is deleted) | クライアントの削除 |
| ホストが追加されました (a host is added) | ホストの追加 |
| プロトコルが追加されました (a protocol is added) | プロトコルの追加 |
| プロトコルが削除されました (a protocol is deleted) | プロトコルの削除 |
| スキャン結果が追加されました (a scan result is added) | スキャン結果の追加 |
| サーバ定義が設定されました (a server definition is set) | サーバ定義の設定 |
| サーバが追加されました (a server is added) | ポートの追加 |
| サーバが削除されました (a server is deleted) | ポートの削除 |
| 脆弱性が無効とマークされています (a vulnerability is marked invalid) | 脆弱性を無効に設定 |

表 51-7 関連ルールのトリガー条件とホストの入カイベントタイプ(続き)

| 選択オプション | ルールをトリガーとして使用するイベントタイプ |
|--|------------------------|
| 脆弱性が有効とマークされています (a vulnerability is marked valid) | 脆弱性を有効に設定 |
| アドレスが削除されました (an address is deleted) | ホスト/ネットワークの削除 |
| 属性値が削除されました (an attribute value is deleted) | ホスト属性値の削除 |
| 属性値が設定されました (an attribute value is set) | ホスト属性値の設定 |
| OS 定義が設定されました (an OS definition is set) | オペレーティング システム定義の設定 |
| ホスト重要度が設定されました (host criticality is set) | ホスト重要度の設定 |

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。

ホスト入カイベントのタイプを選択した後、以下の表で説明されているように関連ルールの条件を作成できます。選択したホスト入カイベントタイプに応じて、以下の表に示す基準のサブセットを使用して条件を作成できます。たとえば、クライアントの削除時に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ホストの IP アドレス、削除のソースタイプ(手動、サードパーティアプリケーション、またはスキャナ)、およびソース自体(特定のスキャナタイプまたはユーザ)に基づいて条件を作成することができます。

表 51-8 ホスト入カイベントの構文

| 指定する項目 | 演算子を指定した後に行う操作 |
|------------------------|---|
| [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。FireSIGHT システム で使用する IP アドレス表記については、 IP アドレスの表記規則 (1-24 ページ) を参照してください。 |
| 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。 |

接続イベントの構文

ライセンス:任意 (Any)

接続イベントに基づく関連ルールにする場合には、まず、接続の開始または終了だけを表すイベントを評価するのか、それとも開始/終了のいずれも表すイベントを評価するのかを選択する必要があります。接続イベントのタイプを選択した後、[接続イベントの構文](#)の表で説明されているように関連ルールの条件を作成できます。

ルール条件を作成するときには、ネットワークトラフィックによってルールをトリガーできることを確認してください。個々の接続イベントまたは接続サマリ 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。詳細については、[接続イベントとセキュリティインテリジェンス イベントで利用可能な情報 \(39-12 ページ\)](#) を参照してください。

表 51-9 接続イベントの構文

| 指定する項目 | 演算子を指定した後に行う操作 |
|---|--|
| アクセスコントロールポリシー (Access Control Policy) | 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 (Access Control Rule Action) | 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。 (注) あとで接続を処理するルール/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ー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、[モニターする (Monitor)] を選択します。 |
| アクセスコントロールルール名 (Access Control Rule Name) | 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またはその一部を入力します。 (注) あとで接続を処理したルール/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ー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 (Application Protocol) | 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 (Application Protocol Category) | 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 (Client) | 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 (Client Category) | 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 (Client Version) | クライアントのバージョン番号を入力します。 |
| 接続期間 (Connection Duration) | 接続イベントの期間 (秒数) を入力します。 |
| 接続タイプ (Connection Type) | Cisco の管理対象デバイスによって接続が検出されたかどうかに基づいて関連ルールをトリガーとして使用するの (FireSIGHT)、それとも NetFlow 対応デバイスによって接続がエクスポートされたかどうかに基づいて関連ルールをトリガーとして使用するの (NetFlow) を選択します。 |
| 宛先国 (Destination Country) または送信元国 (Source Country) | 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 (NetFlow 対応デバイスによってエクスポートされた接続データの場合) 接続を処理したデバイスを 1 つ以上選択します。 |
| 出力インターフェイス (Egress Interface) または入力インターフェイス (Ingress Interface) | 1 つ以上のインターフェイスを選択します。 |

表 51-9 接続イベントの構文(続き)

| 指定する項目 | 演算子を指定した後に行う操作 |
|---|--|
| 出力セキュリティゾーン (Egress Security Zone) または 入力セキュリティゾーン (Ingress Security Zone) | セキュリティゾーンを 1 つ以上選択します。 |
| イニシエータ バイト数 (Initiator Bytes)、レスポнда バイト数 (Responder Bytes)、または Total Bytes | 以下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 (Initiator IP)、レスポнда IP (Responder IP)、または イニシエータ/レスポнда IP (Initiator/Responder 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。FireSIGHT システムで使用する IP アドレス表記およびプレフィックス長については、 IP アドレスの表記規則 (1-24 ページ) を参照してください。 |
| イニシエータ パケット (Initiator Packets)、レスポнда パケット (Responder Packets)、または Total Packets | 以下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 (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 (Initiator Port/ICMP Type) または レスポнда ポート/ICMP コード (Responder Port/ICMP Code) | 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 (IOC Tag) | 接続イベントの結果として IOC タグが設定されているか (is)、または設定されていないか (is not) を選択します。 |
| NETBIOS 名 (NETBIOS Name) | 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 (NetFlow Device) | 関連ルールをトリガーとして使用するために使用される接続データをエクスポートした NetFlow 対応デバイスの IP アドレスを選択します。展開環境に NetFlow 対応デバイスをまだ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 インテリジェンスのカテゴリ (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。 (注) 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 ポリシーの [セキュリティ インテリジェンス (Security Intelligence)] セクションで、その条件を [ブロック (Block)] ではなく [モニタ (Monitor)] に設定する必要があります。詳細については、 セキュリティ インテリジェンスのホワイトリストおよびブラックリストの作成 (13-4 ページ) を参照してください。 |
| 実際の SSL アクション (SSL Actual Action) | 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。 |

表 51-9 接続イベントの構文(続き)

| 指定する項目 | 演算子を指定した後に行う操作 |
|--|--|
| SSL 証明書のフィンガープリント (SSL Certificate Fingerprint) | 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 証明書サブジェクトの共通名 (CN) (SSL Certificate Subject Common Name (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共通名またはその一部を入力します。 |
| SSL 証明書サブジェクトの国 (C) (SSL Certificate Subject Country (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国別コードを 1 つ以上選択します。 |
| SSL 証明書サブジェクトの組織 (O) (SSL Certificate Subject Organization (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組織名またはその一部を入力します。 |
| SSL 証明書サブジェクトの組織単位 (OU) (SSL Certificate Subject Organizational Unit (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組織単位名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) | [復号が成功 (Successfully Decrypted)] を選択します。 |
| SSL フロー ステータス (SSL Flow Status) | 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 1 つ以上のステータスを選択します。 |
| SSL ポリシー (SSL Policy) | 暗号化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 (SSL Rule Name) | 暗号化接続をログに記録した SSL ルールの名前またはその一部を入力します。 |
| SSL サーバ名 (SSL Server Name) | クライアントが暗号化接続を確立した相手のサーバの名前、またはその一部を入力します。 |
| SSL URL カテゴリ (SSL URL Category) | 暗号化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 (SSL Version) | セッションの暗号化に使用された SSL または TLS のバージョンを 1 つ以上選択します。 |
| TCP フラグ (TCP Flags) | <p>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い TCP フラグを選択します。</p> <p>(注) TCP フラグが含まれるのは、NetFlow 対応デバイスによってエクスポートされた接続データのみです。</p> |
| トランスポート プロトコル (Transport Protocol) | 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 (URL Category) | 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。 |

表 51-9 接続イベントの構文(続き)

| 指定する項目 | 演算子を指定した後に行う操作 |
|--|--|
| URLレピュテーション(URL Reputation) | 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)] | この接続でいずれかの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。 |
| Web アプリケーション (Web Application) | 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 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。 |

トラフィック プロファイル変化の構文

ライセンス:任意 (Any)

トラフィック プロファイル変化に基づく関連ルールの場合、既存のトラフィック プロファイルで特徴付けられた通常のネットワーク トラフィック パターンからネットワーク トラフィック が逸脱したときに、ルールがトリガーとして使用されます。トラフィック プロファイルを作成する方法については、[トラフィック プロファイルの作成 \(53-1 ページ\)](#) を参照してください。

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、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。

- 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

[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([グラフ タイプの変更 \(39-20 ページ\)](#) を参照)、データ ポイント間の速度変化に基づいて関連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関連ルールの条件を作成します。NetFlow 対応デバイスによってエクスポートされる接続データをトラフィック プロファイルで使用する場合は、[NetFlow と FireSIGHT データの違い \(45-19 ページ\)](#)を参照して、トラフィック プロファイルの作成に使われるデータが、検出方法に応じてどのように異なるかを確認してください。

表 51-10 トラフィック プロファイル変化の構文

| 指定する項目 | 演算子を指定した後に入力する内容 | その後、さらに次のいずれかを選択 |
|--|---|---|
| 接続数 (Number of Connections) | 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 (Total Bytes)、 イニシエータ バイト数 (Initiator Bytes)、 または レスポнда バイト数 (Responder Bytes) | 次のいずれかを入力します。 <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нда 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(上記のいずれかの基準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) | bytes: バイト数 standard deviation(s): 標準偏差の数 |
| 合計パケット数 (Total Packets)、 イニシエータ パケット (Initiator Packets)、 または レスポнда パケット (Responder Packets) | 次のいずれかを入力します。 <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нда パケット (Responder Packets)]) または 平均より上または下の標準偏差の数(上記のいずれかの基準がこれを超えると、ルールがトリガーとして使用されます) | packets: パケット数 standard deviation(s): 標準偏差の数 |
| ユニークなイニシエータ (Unique Initiators) | 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(検出されたユニーク イニシエータ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) | initiators: イニシエータ数 standard deviation(s): 標準偏差の数 |
| ユニークなレスポнда (Unique Responders) | セッションに回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(検出されたユニーク レスポнда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) | responders: レスポнда数 standard deviation(s): 標準偏差の数 |

ホスト プロファイル限定の追加

ライセンス:FireSIGHT

接続、侵入、ディスクバリエーション、ユーザアクティビティ、またはホスト入力のいず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ホストのプロファイル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、**ホスト プロファイル限定**と呼ばれます。



(注) 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関連ルールに、ホスト プロファイル限定を追加することは**できません**。

たとえば、ルールの作成対象となる脆弱性が Microsoft Windows コンピュータにのみ存在するため、Microsoft Windows ホストが有害トラフィックのターゲットとなっている場合にのみ関連ルールをトリガーとして使用するよう、制約することができます。別の例として、ホストがホワイトリストに準拠していない場合にのみ関連ルールがトリガーとして使用されるよう、制約することもできます。

暗黙的(または汎用の)クライアントを照合するには、クライアントに応答するサーバで使われるアプリケーションプロトコルに基づいてホスト プロファイル限定を作成します。接続のインシエンタ(または送信元)として機能するホスト上のクライアントリストに含まれるアプリケーションプロトコル名の後に**クライアント**が続いている場合、そのクライアントは実際には暗黙的クライアントである可能性があります。つまり、検出されたクライアント トラフィックに基づいてではなく、そのクライアントのアプリケーションプロトコルを使用するサーバ応答トラフィックに基づいて、システムがそのクライアントを報告します。

たとえば、ホストのクライアントとして **HTTPS クライアント**がシステムにより報告される場合、[アプリケーションプロトコル(Application Protocol)] を [HTTPS] に設定したレスポンド ホストまたは宛先ホストのホスト プロファイル限定を作成します。これは、レスポンドまたは宛先ホストから送られる HTTPS サーバ応答トラフィックに基づいて **HTTPS クライアント**が汎用クライアントとして報告されるためです。

ホスト プロファイル限定を使用するには、そのホストがネットワーク マップに存在すること、および限定として使用するホスト プロファイル プロパティがホスト プロファイルにすでに含まれていることが必要です。たとえば、Windows を実行するホストでの侵入イベントが生成されると関連ルールがトリガーとして使用されるよう設定した場合、そのルールがトリガーとして使用されるのは、侵入イベント生成時にホストがすでに Windows として識別されている場合だけです。

ホスト プロファイル限定を追加する方法:

アクセス:Admin/Discovery Admin

- 手順 1 [ポリシー(Policies)] > [関連(Correlation)] を選択し、[ルール管理(Rule Management)] タブを選択します。
[ルール管理(Rule Management)] ページが表示されます。
- 手順 2 [ルールの作成(Create Rule)] をクリックします。
[ルールの作成(Create Rule)] ページが表示されます。
- 手順 3 [ルールの作成(Create Rule)] ページで、[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。
[ホスト プロファイル限定(Host Profile Qualification)] セクションが表示されます。



ヒント

ホスト プロファイル限定を削除するには、[ホスト プロファイル限定の削除 (Remove Host Profile Qualification)] をクリックします。

手順 4 ホスト プロファイル限定の条件を作成します。

1 つの単純な条件を作成することも、複数の条件の組み合わせやネストを使って複雑な構造を作成することもできます。Web インターフェイスを使用して条件を作成する方法については、[ルールの作成メカニズムについて \(51-41 ページ\)](#) を参照してください。

条件を作成するために使用できる構文については、[ホスト プロファイル限定の構文 \(51-25 ページ\)](#) で説明しています。

手順 5 オプションで、以下の項の手順に進みます。

- [経時的な接続データを使用した関連ルールの制約 \(51-28 ページ\)](#)
- [ユーザ限定の追加 \(51-38 ページ\)](#)
- [スヌーズ期間および非アクティブ期間の追加 \(51-40 ページ\)](#)

関連ルールの作成が終了した場合は、[関連ポリシーのルールの作成 \(51-3 ページ\)](#) で説明している手順のステップ 9 に進んでルールを保存します。

ホスト プロファイル限定の構文

ライセンス: FireSIGHT

ホスト プロファイル限定の条件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ホストを選択する必要があります。選択できるホストは、ルールをトリガーとして使用するために使われるイベントのタイプに応じて次のように異なります。

- 接続イベントを使用する場合は、応答側を示す [レスポンドャ ホスト (Responder Host)] または開始側を示す [イニシエータ ホスト (Initiator Host)] を選択します。
- 侵入イベントを使用する場合は、宛先を示す [宛先ホスト (Destination Host)] または送信元を示す [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、またはユーザ アクティビティを使用する場合は、[ホスト (Host)] を選択します。

ホスト タイプを選択した後、以下の表の説明に従ってホスト プロファイル限定条件の作成を続けます。

NetFlow 対応デバイスによってエクスポートされたデータに基づき、ネットワーク マップにホストを追加するようネットワーク検出ポリシーを設定することはできますが、これらのホストに関して使用可能な情報は限られています。たとえば、これらのホストのオペレーティング システム データは得られません (ただしホスト入力機能を使って指定する場合を除く)。さらに、NetFlow 対応デバイスによってエクスポートされた接続データを使用する場合、NetFlow レコードには、どのホストがイニシエータで、どのホストがレスポンドャであるかを示す情報が含まれないことに注意してください。システムは、NetFlow レコードを処理するときに、それぞれのホストが使用しているポートとそれらのポートが既知かどうかに基づいて、この情報を判断するアルゴリズムを使用します。詳細については、[NetFlow と FireSIGHT データの違い \(45-19 ページ\)](#) を参照してください。

表 51-11 ホストプロファイル限定の構文

| 指定する項目 | 演算子を指定した後に行う操作 |
|---|--|
| [ホスト タイプ (Host Type)] | 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。 |
| [NETBIOS 名 (NETBIOS Name)] | ホストの NetBIOS 名を入力します。 |
| [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 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 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。 |
| [ハードウェア (Hardware)] | 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。 |
| [IOC タグ (IOC Tag)] | IOC タグを 1 つ以上選択します。IOC タグ タイプの詳細については、 侵害の兆候タイプについて (45-22 ページ) を参照してください。 |
| ジェイルブレイク (Jailbroken) | 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。 |
| 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。 |
| 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。 |
| [トランスポート プロトコル (Transport Protocol)] | トランスポート プロトコルの名前、または http://www.iana.org/assignments/protocol-numbers にリストされている番号を入力します。 |
| [ホストの重要度 (Host Criticality)] | ホストの重要度 (None 、 Low 、 Medium 、または High) を選択します。ホスト重要度の詳細については、 事前定義のホスト属性の使用 (49-34 ページ) を参照してください。 |
| VLAN ID (Admin. VLAN ID) | ホストに関連付けられた VLAN ID を入力します。 |
| [アプリケーション プロトコル (Application Protocol)] > [アプリケーション プロトコル (Application Protocol)] | 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 (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。 侵入イベントを使って関連ルールをトリガーとして使用する場合、ホスト プロファイル限定で選択したホストに応じて、イベントのポートがこのフィールドに事前入力されます ([宛先ホスト (Destination Host)] の場合は dst_port、[送信元ホスト (Source Host)] の場合は src_port)。 |
| [アプリケーション プロトコル (Application Protocol)] > プロトコル | プロトコルを 1 つ以上選択します。 |

表 51-II ホストプロファイル限定の構文(続き)

| 指定する項目 | 演算子を指定した後に行う操作 |
|---|---|
| [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 1 つ選択します。 |
| [クライアント (Client)] > [クライアント (Client)] | クライアントを 1 つ以上選択します。 |
| [クライアント (Client)] > [クライアントバージョン (Client Version)] | クライアントの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 1 つ選択します。 |
| [Web アプリケーション (Web Application)] | Web アプリケーションを選択します。 |
| [Web アプリケーションカテゴリ (Web Application Category)] | カテゴリを 1 つ選択します。 |
| [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。 たとえば、特定のハードウェア デバイスの MAC アドレスが 0A:12:34 で始まる場合、演算子として [次で始まる (begins with)] を選択し、値として 0A:12:34 を入力できます。 |
| [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識別したのか (is ARP/DHCP Detected)、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 (is not ARP/DHCP Detected)、または MAC タイプが無関係であるのか (is any) を選択します。 |
| [MAC ベンダー (MAC Vendor)] > [MAC ベンダー (MAC Vendor)] | ホストの MAC ハードウェア ベンダーの名前またはその一部を入力します。 |
| 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) | <p>選択するホスト属性のタイプに応じて、適切な値を次のように指定します。</p> <ul style="list-style-type: none"> ホスト属性タイプが Integer の場合、その属性で定義されている範囲内の整数値を入力します。 ホスト属性タイプが Text の場合、テキスト値を入力します。 ホスト属性タイプが List の場合、有効なリスト文字列を選択します。 ホスト属性タイプが URL の場合、URL 値を入力します。 <p>ホスト属性の詳細については、ユーザ定義のホスト属性の使用 (49-35 ページ) を参照してください。</p> |

ホストプロファイル限定を作成する際に、イベントデータを使用できる場合がよくあります。たとえば、モニタ対象のいずれかのホストで Internet Explorer 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、使用が検出された場合、ブラウザのバージョンが最新でなければイベントを生成するとします(この例では最新バージョンが 9.0 であると想定します)。

この場合、クライアントがイベントクライアント(つまり Internet Explorer)であり、しかもクライアントバージョンが 9.0 でない場合にのみルールがトリガーとして使用されるよう、ホストプロファイル限定をこの関連ルールに追加することができます。

経時的な接続データを使用した関連ルールの制約

ライセンス:FireSIGHT

接続トラッカーは、(ホストプロファイル限定およびユーザ限定を含む)ルールの初期基準に一致した後にシステムが特定の接続を追跡し始めるよう、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、防御センターがルールの関連イベントを生成します。

接続、侵入、ディスクバリエーション、ユーザアクティビティ、またはホスト入力のいず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は、接続トラッカーをルールに追加できます。マルウェアイベントやトラフィックプロファイル変化によってトリガーとして使用されるルールに、接続トラッカーを追加することはできません。



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([トラフィックプロファイルの作成\(53-1 ページ\)](#)を参照)。

次に示すように、接続トラッカーをどのように作成するかに応じて、接続トラッカーは 2 つの方法でイベントを生成できます。

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追跡を停止します。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。

一方、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、防御センター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追跡を停止します。

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、初期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。

詳細については、次の項を参照してください。

- [接続トラッカーの追加\(51-29 ページ\)](#)
- [接続トラッカーの構文\(51-30 ページ\)](#)
- [接続トラッカー イベントの構文\(51-33 ページ\)](#)
- [例:外部ホストからの過剰な接続数\(51-34 ページ\)](#)
- [例:過剰な BitTorrent データの転送\(51-35 ページ\)](#)

接続トラッカーの追加

ライセンス:FireSIGHT

接続トラッカーは、(ホスト プロファイル限定およびユーザ限定を含む)初期基準が満たされた後にシステムが特定の接続を追跡し始めるよう、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、防御センター がルールの関連イベントを生成します。

接続トラッカーを設定するときには、次の項目を指定する必要があります。

- どの接続を追跡するか
- 防御センター に関連イベントを生成させるために、追跡対象の接続が満たす必要のある条件
- 接続トラッカーの最大有効期間(関連イベントが生成されるためには、この期間内に指定の条件が満たされる必要があります)



ヒント

接続、侵入、ディスカバリ、ユーザアイデンティティ、またはホスト入力 of のいずれかのイベントが発生することだけを必要とする単純な関連ルールに、接続トラッカーを追加することができます。

接続トラッカーを追加する方法:

アクセス:Admin/Discovery Admin

手順 1 [ルールの作成(Create Rule)] ページで、[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(Connection Tracker)] セクションが表示されます。



ヒント

接続トラッカーを削除するには、[接続トラッカーの削除(Remove Connection Tracker)] をクリックします。

手順 2 接続トラッカーの基準を設定することにより、追跡対象の接続を指定します。

接続トラッカーの基準を設定するときには、1 つの単純な条件を作成することも、複数の条件の組み合わせやネストを使って複雑な構造を作成することもできます。

Web インターフェイスを使用して条件を作成する方法については、[ルールの作成メカニズムについて\(51-41 ページ\)](#)を参照してください。接続トラッカーの条件を作成するために使用できる構文については、[接続トラッカーの構文\(51-30 ページ\)](#)で説明しています。

手順 3 ステップ 2 で追跡対象として指定した接続に応じて、どのようなときに関連イベントを生成するかを記述します。

イベント生成時を記述する 1 つの単純な条件を作成することも、複数の条件の組み合わせやネストを使って複雑な構造を作成することもできます。

■ 関連ポリシーのルール作成

また、期間を秒数、分数、または時間数で指定する必要があります(関連イベントが生成されるためには、この期間内に指定の条件が満たされる必要があります)。

Web インターフェイスを使用して条件を作成する方法については、[ルール作成メカニズムについて\(51-41 ページ\)](#)を参照してください。接続トラッカーの条件を作成するために使用できる構文については、[接続トラッカー イベントの構文\(51-33 ページ\)](#)で説明しています。

手順 4 オプションで、以下の項の手順に進みます。

- [ユーザ限定の追加\(51-38 ページ\)](#)
- [スヌーズ期間および非アクティブ期間の追加\(51-40 ページ\)](#)

関連ルールの作成が終了した場合は、[関連ポリシーのルール作成\(51-3 ページ\)](#)で説明している手順のステップ 9 に進んでルールを保存します。

接続トラッカーの構文

ライセンス:任意(Any)

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。

Ciscoの管理対象デバイスによって検出された接続と、NetFlow 対応デバイスによってエクスポートされた接続データには、異なる情報が含まれていることに注意してください。たとえば、管理対象デバイスによって検出された接続には、TCP フラグ情報が含まれません。したがって、関連ルールをトリガーとして使用するために特定の TCP フラグが接続イベントに含まれる必要があると指定した場合、管理対象デバイスによって検出された接続がルールをトリガーとして使用させることは決してありません。

別の例として、NetFlow レコードには、接続の中でどのホストがイニシエータ/レスポンドであるかを示す情報が含まれません。システムは、NetFlow レコードを処理するときに、それぞれのホストが使用しているポートとそれらのポートが既知かどうかに基づいて、この情報を判断するアルゴリズムを使用します。詳細については、[NetFlow と FireSIGHT データの違い\(45-19 ページ\)](#)を参照してください。

表 51-12 接続トラッカーの構文

| 指定する項目 | 演算子を指定した後に行う操作 |
|--|---|
| アクセス コントロール ポリシー (Access Control Policy) | 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 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 (Access Control Rule Action) | 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。 (注) あとで接続を処理するルール/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、[モニターする (Monitor)] を選択します。 |
| アクセス コントロール ルール名 (Access Control Rule Name) | 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 ルールの名前またはその一部を入力します。 (注) 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/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 (Application Protocol) | アプリケーション プロトコルを 1 つ以上選択します。 |

表 51-12 接続トラッカーの構文(続き)

| 指定する項目 | 演算子を指定した後に行う操作 |
|--|---|
| アプリケーションプロトコルカテゴリ (Application Protocol Category) | 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 (Client) | 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 (Client Category) | 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 (Client Version) | クライアントのバージョンを入力します。 |
| 接続期間 (Connection Duration) | 接続期間(秒数)を入力します。 |
| 接続タイプ (Connection Type) | Cisco の管理対象デバイスによって検出された接続を追跡するのか (FireSIGHT)、または NetFlow 対応デバイスによってエクスポートされた接続を追跡するのか (NetFlow) を選択します。 |
| [宛先国 (Destination Country)] または [送信元国 (Source Country)] | 1 つ以上の国を選択します。 |
| Device | 追跡対象の接続が検出されるデバイスを 1 つ以上選択します。NetFlow 接続を追跡する場合は、NetFlow 対応デバイスによってエクスポートされた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 (Ingress Interface) または 出力インターフェイス (Egress Interface) | 1 つ以上のインターフェイスを選択します。 |
| 入力セキュリティゾーン (Ingress Security Zone) または 出力セキュリティゾーン (Egress Security Zone) | セキュリティゾーンを 1 つ以上選択します。 |
| イニシエータ IP (Initiator IP)、レスポнда IP (Responder IP)、 または イニシエータ/レスポнда IP (Initiator/Responder 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。FireSIGHT システムで使用する IP アドレス表記については、IP アドレスの表記規則 (1-24 ページ) を参照してください。 |
| イニシエータバイト数 (Initiator Bytes)、 レスポндаバイト数 (Responder Bytes)、または Total Bytes | 以下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 ([Initiator Bytes]) 受信されたバイト数 ([Responder Bytes]) 送受信されたバイト数 ([Total Bytes]) |
| イニシエータパケット (Initiator Packets)、 レスポндаパケット (Responder Packets)、または Total Packets | 以下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 (Responder Packets)]) 送受信されたパケット数 ([合計パケット数 (Total Pakets)]) |

表 51-12 接続トラッカーの構文(続き)

| 指定する項目 | 演算子を指定した後に行う操作 |
|---|---|
| イニシエータ ポート/ICMP タイプ (Initiator Port/ICMP Type) またはレスポナー ポート/ICMP コード (Responder Port/ICMP Code) | 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、あるいはレスポナー 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 (IOC Tag) | IOC タグが設定されているか (is)、設定されていないか (is not) を選択します。 |
| NETBIOS 名 (NETBIOS Name) | 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 (NetFlow Device) | 追跡対象の接続をエクスポートした NetFlow 対応デバイスの IP アドレスを選択します。展開環境に NetFlow 対応デバイスをまだ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 インテリジェンスのカテゴリ (Security Intelligence Category) | 追跡対象の接続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。 |
| TCP フラグ (TCP Flags) | 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。 (注) NetFlow 対応デバイスによってエクスポートされた接続にのみ、TCP フラグ データが含まれます。 |
| トランスポート プロトコル (Transport Protocol) | 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 | 追跡対象の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 (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 (URL Reputation) | 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を示すユーザ名を入力します。 |
| Web アプリケーション (Web Application) | 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 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。 |

接続トラッカーを作成する際に、イベントデータを使用できる場合がよくあります。たとえば、いずれかのモニタ対象ホストで新しいクライアントをシステムが検出したときに関連ルールがトリガーとして使用されるとします。つまり、基本イベントタイプ [新しいクライアントの検出 (a new client is detected)] であるシステム イベントが生成されたときにこのルールがトリガーとして使用します。

さらに、この新しいクライアントが検出されたとき、検出場所のホストでそのクライアントに関連する接続を追跡するとします。システムはホストの IP アドレスとクライアントの名前を認識しているため、これらの接続を追跡する単純な接続トラッカーを作成できます。

実際、このような関連ルールに接続トラッカーを追加すると、接続トラッカーにはデフォルト制約が設定されます。つまり [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、[クライアント (Client)] が [イベント クライアント (Event Client)] に設定されます。



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接続トラッカーで追跡するよう指定するには、[手動入力に切り替え (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 フィールドに切り替え (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

ライセンス:任意 (Any)

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 51-13 接続トラッカー イベントの構文

| 指定する項目 | 演算子を指定した後に行う操作 |
|---|--|
| 接続数 (Number of Connections) | 検出された接続の合計数を入力します。 |
| SSL 暗号化セッションの数 (Number of SSL Encrypted Sessions) | 検出された SSL または TLS 暗号化セッションの合計数を入力します。 |
| 合計バイト数 (Total Bytes)、イニシエータ バイト数 (Initiator Bytes)、またはレスポンド バイト数 (Responder Bytes) | 以下のいずれかを入力します。 <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 (Total Packets)、イニシエータ パケット (Initiator Packets)、またはレスポンド パケット (Responder Packets) | 以下のいずれかを入力します。 <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 (Responder Packets)]) |
| ユニークなイニシエータ (Unique Initiators) またはユニークなレスポンド (Unique Responders) | 以下のいずれかを入力します。 <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の数 ([ユニークなイニシエータ (Unique Initiators)]) 検出された接続に応答した個別のホストの数 ([ユニークなレスポンド (Unique Responders)]) |

例:外部ホストからの過剰な接続数

たとえば、ネットワーク 10.1.0.0/16 で機密ファイルをアーカイブしていて、このネットワーク外部のホストは通常、ネットワーク内部のホストとの接続を開始しないとします。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。

以下の図に示されているルールは、ネットワーク 10.1.0.0/16 の外部からネットワーク内部への接続が発生した場合、その基準に一致する接続をシステムが追跡し始めることを指定します。システムが、そのシグニチャに一致する4つの接続(元の接続を含む)を2分以内に検出した場合、防御センターは相関イベントを生成します。

Rule Information + Add User Qualifier

Rule Name:

Rule Description:

Rule Group:

Select the type of event for this rule

If at either the beginning or the end of the connection and it meets the following conditions:

+ Add condition + Add complex condition

is not in

is in

Connection Tracker

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

+ Add condition + Add complex condition

is not in (switch to event)

is in (switch to event)

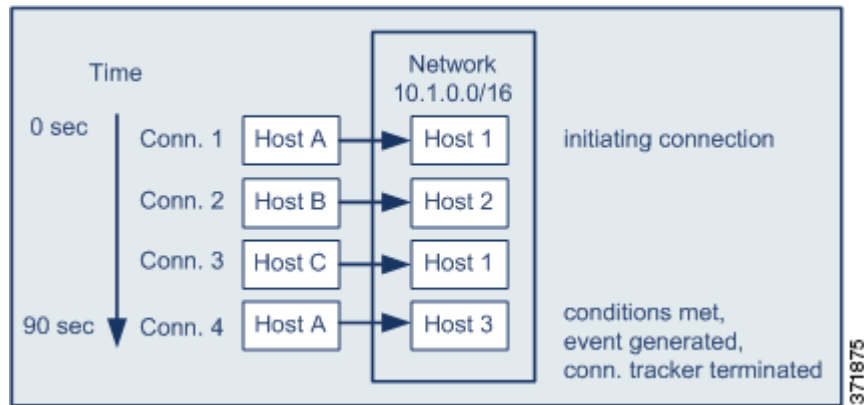
... and generate an event if:

+ Add condition + Add complex condition

total are greater than or equal to

in the next minutes

ネットワークトラフィックがこの関連ルールをどのようにトリガーとして使用するか、以下の図に示します。



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。

接続トラッカーは以下の手順で処理されます。

-
- 手順 1 システムがネットワーク外部のホスト A からネットワーク内部のホスト 1 への接続を検出すると、その接続の追跡を開始します。
 - 手順 2 システムは接続トラッカーのシグニチャに一致する接続をさらに 2 つ検出します(ホスト B からホスト 2、ホスト C からホスト 1)。
 - 手順 3 2 分の制限時間内にホスト A がホスト 3 に接続すると、システムは 4 番目の適格性確認の接続を検出します。これで、ルールの条件が満たされました。
 - 手順 4 防御センターが関連イベントを生成し、システムは接続の追跡を停止します。
-

例: 過剰な BitTorrent データの転送

このシナリオでは、モニタ対象ネットワーク上のいずれかのホストへの初期接続が発生した後、過剰な BitTorrent データ転送をシステムが検出すると、関連イベントを生成します。

モニタ対象ネットワークでシステムが BitTorrent アプリケーションプロトコルを検出したときにトリガーとして使用される関連ルールを以下の図に示します。このルールの接続トラッカーは、モニタ対象ネットワーク(この例では 10.1.0.0/16)上のホストが、最初のポリシー違反から 5 分間に BitTorrent を介して合計 7MB (7340032 バイト) のデータを転送した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します。

Select the type of event for this rule

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

AND IP Address is in 10.1.0.0/16

Application Protocol is BitTorrent

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

AND Responder IP is Event IP Address (switch to manual entry)

Application Protocol is BitTorrent

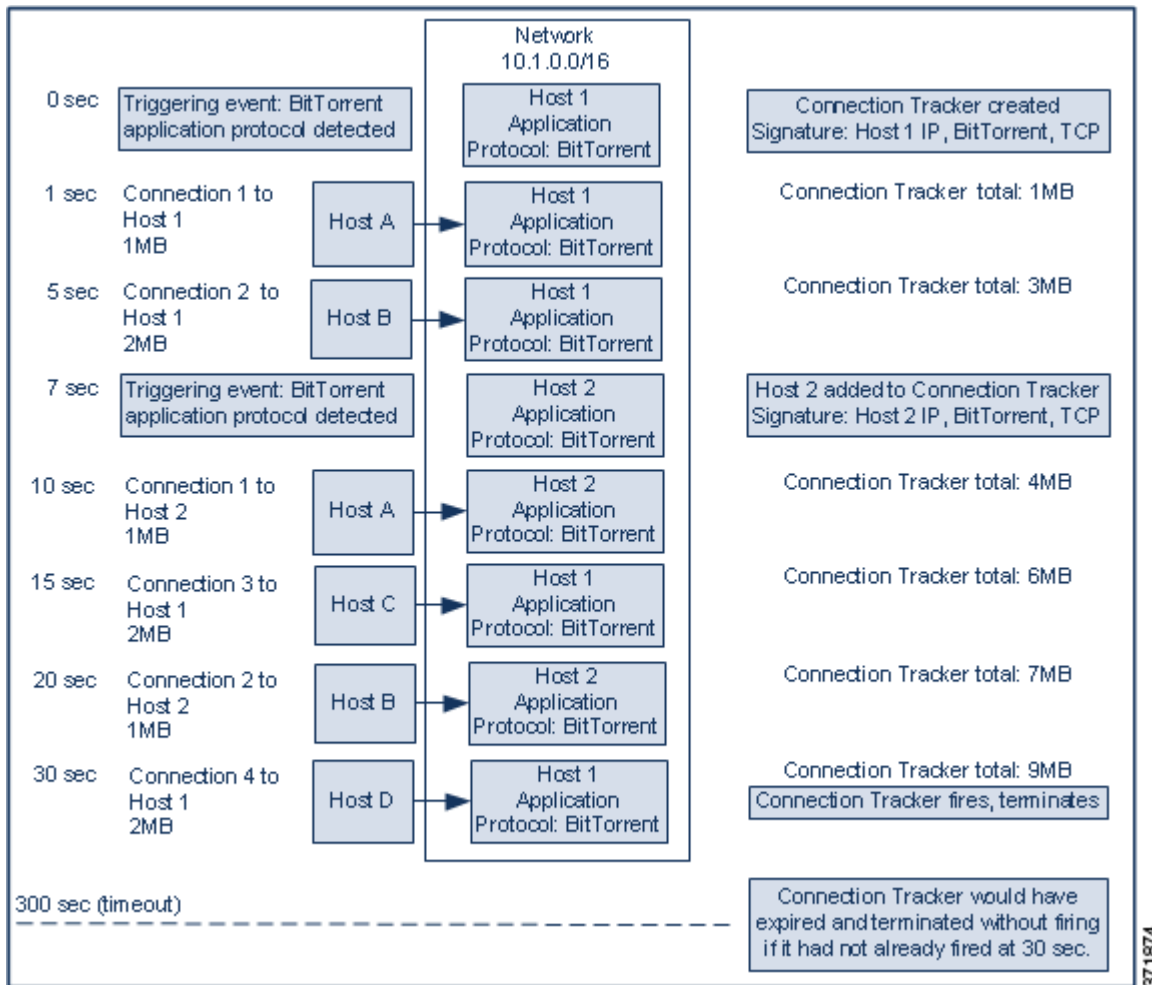
Transport Protocol is TCP

... and generate an event if:

total Responder Bytes are greater than 7340032

in the next minutes

ネットワークトラフィックがこの相関ルールをどのようにトリガーとして使用するか、以下の図に示します。



この例で、システムは2つの異なるホスト(ホスト1とホスト2)で BitTorrent TCP アプリケーションプロトコルを検出しました。この2つのホストは、他の4つのホスト(ホストA、ホストB、ホストC、ホストD)に BitTorrent を介してデータを転送しました。

この接続トラッカーは以下の手順で処理されます。

- 手順 1 システムがホスト1で BitTorrent アプリケーションプロトコルを検出すると、システムは0秒マーカーで接続を追跡し始めます。
これに続く(300秒マーカーによる)5分間で、7MBの BitTorrent TCP データ転送をシステムが検出しなければ、接続トラッカーは期限切れになります。
- 手順 2 5秒経過した時点で、ホスト1はシグニチャに一致する3MBのデータを次のように送信しました。
 - 1秒マーカーの時点で、ホスト1からホストAに1MBを転送(接続トラッカーの条件適合に向けて合計1MBの BitTorrent トラフィックをカウント)
 - 5秒マーカーの時点で、ホスト1からホストBに2MB(合計3MB)
- 手順 3 7秒経過した時点で、システムはホスト2での BitTorrent アプリケーションプロトコルを検出し、そのホストでも BitTorrent 接続を追跡し始めます。

手順 4 20 秒経過した時点で、システムは、シグニチャに一致するさらに他のデータがホスト 1 およびホスト 2 から転送されていることを検出しました。

- 10 秒マーカーの時点で、ホスト 2 からホスト A に 1MB (合計 4MB)
- 15 秒マーカーの時点で、ホスト 1 からホスト C に 2MB (合計 6MB)
- 20 秒マーカーの時点で、ホスト 2 からホスト B に 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、仮にトラッカー タイムアウト期間の残り 280 秒間にシステムが他の BitTorrent 転送を検出しない場合は、トラッカーが期限切れになり、防御センターは関連イベントを生成しません。

手順 5 しかし、30 秒経過した時点でシステムは別の BitTorrent 転送を次のように検出しました。

- 30 秒マーカーの時点で、ホスト 1 からホスト D に 2MB (合計 9MB)

これで、ルールの条件が満たされました。

手順 6 防御センターが関連イベントを生成します。

さらに、まだ 5 分の期間が経過していませんが、防御センターはこの接続トラッカーインスタンスの接続の追跡を停止します。この時点で、BitTorrent TCP アプリケーションプロトコルを使用した新しい接続を検出した場合は、システムは新しい接続トラッカーを作成します。

防御センターはセッション終了まで接続データを集計しないため、関連イベントが生成されるのは、ホスト 1 がホスト D に 2MB を全部転送し終わった後であることに注意してください。

ユーザ限定の追加

ライセンス:FireSIGHT

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。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。

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。

ユーザ アイデンティティ 限定を追加する方法:

アクセス:Admin/Discovery Admin

手順 1 [ルールの作成 (Create Rule)] ページで、ユーザ限定の追加を示す [ユーザ限定の追加 (Add User Qualification)] をクリックします。

[ユーザ アイデンティティ 限定 (User Identity Qualification)] セクションが表示されます。



ヒント ユーザ限定を削除するには、[ユーザ限定の削除 (Remove User Qualification)] をクリックします。

手順 2 ユーザ限定の条件を作成します。

1 つの単純な条件を作成することも、複数の条件の組み合わせやネストを使って複雑な構造を作成することもできます。Web インターフェイスを使用して条件を作成する方法については、[ルールの作成メカニズムについて \(51-41 ページ\)](#) を参照してください。

条件を作成するために使用できる構文については、[ユーザ限定の構文 \(51-39 ページ\)](#) で説明しています。

手順 3 オプションで、[スヌーズ期間および非アクティブ期間の追加 \(51-40 ページ\)](#) に進みます。

関連ルールの作成が終了した場合は、[関連ポリシーのルールの作成 \(51-3 ページ\)](#) で説明している手順のステップ 9 に進んでルールを保存します。

ユーザ限定の構文

ライセンス:FireSIGHT

ユーザ限定の条件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選択する必要があります。選択できるアイデンティティは、ルールをトリガーとして使用するために使われるイベントのタイプに応じて次のように異なります。

- 接続イベントを使用している場合は、[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。
- 侵入イベントを使用している場合は、宛先を示す [宛先のアイデンティティ (Identity on Destination)] または送信元を示す [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 イベントを使用している場合は、[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を使用している場合は、[ホストのアイデンティティ (Identity on Host)] を選択します。

ユーザタイプを選択した後、以下の表の説明に従ってユーザ限定条件の作成を続けます。

防御センターは、オプションの 防御センター-LDAP サーバ間接続から、ユーザに関する特定の情報 (姓名、部門、電話番号、電子メールアドレスなど) を取得します ([Active Directory のログインを報告するためのユーザエージェントの使用 \(17-11 ページ\)](#) を参照)。データベース内のすべてのユーザに関して、この情報が入手可能とは限りません。

表 51-14 ユーザ限定の構文

| 指定する項目 | 演算子を指定した後に行う操作 |
|-----------------------------------|--|
| [ユーザ名 (Username)] | 関連ルールを制約するために使用するユーザを示すユーザ名を入力します。 |
| 認証プロトコル (Authentication Protocol) | 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。これは、ユーザの検出に使用されたプロトコルです。 |
| 名 | 関連ルールを制約するために使用するユーザの名前 (ファーストネーム) を入力します。 |
| 姓 | 関連ルールを制約するために使用するユーザの姓を入力します。 |
| 部署名 (Department) | 関連ルールを制約するために使用するユーザの部門/部署を入力します。 |
| 電話 | 関連ルールを制約するために使用するユーザの電話番号を入力します。 |
| Eメール | 関連ルールを制約するために使用するユーザの電子メールアドレスを入力します。 |

スヌーズ期間および非アクティブ期間の追加

ライセンス:任意(Any)

関連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、関連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、防御センター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まった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関連ルールの場合、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、短時間に多数の関連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関連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、防御センターは関連イベントを生成します。

また、関連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、関連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、関連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、該当する関連ルールで非アクティブ期間を設定することができます。

以下の図は、関連ルールの中でスヌーズ期間と非アクティブ期間を設定する部分を示しています。

Rule Options

Snooze If this rule generates an event, snooze for 10 minutes

Inactive Periods  Daily at 12:00 AM for 10 minutes

スヌーズ期間を追加する方法:

アクセス:Admin/Discovery Admin

- 手順 1** [プロファイルの作成(Create Profile)] ページの [ルール オプション(Rule Options)] で、ルールのトリガー後に再びルールをトリガーとして使用させるまで 防御センター に待機させる間隔を指定します。



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。

非アクティブ期間を追加する方法:

アクセス: Admin/Discovery Admin

- 手順 1** [プロファイルの作成(Create Profile)] ページの [ルール オプション(Rule Options)] で、[非アクティブ期間の追加(Add Inactive Period)] をクリックします。
- 手順 2** ドロップダウンリストとテキスト フィールドを使用して、関連ルールに基づくネットワークトラフィック評価を 防御センター に停止させる時点および頻度を指定します。



ヒント

非アクティブ期間を削除するには、削除対象の非アクティブ期間の横にある削除アイコン(✖)をクリックします。

スヌーズ期間と非アクティブ期間を追加し終わったら、[関連ポリシーのルール作成\(51-3 ページ\)](#)で説明している手順のステップ 9 に進んでルールを保存します。

ルールの作成メカニズムについて

ライセンス:任意(Any)

関連ルール、接続トラッカー、ユーザ限定、およびホスト プロファイル限定を作成するときには、それぞれをトリガーとして使用する条件を指定します。単純な条件を作成することも、複数の条件の組み合わせやネストを使って複雑な構造を作成することもできます。

たとえば、新しいホストが検出されるたびに関連イベントを生成するには、以下の図に示すように、条件をまったく含まない非常に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、以下の図に示すような 1 つの条件を追加できます。

一方、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 fol

条件で使用できる構文は、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。



注意

頻繁に発生するイベントによってトリガーとして使用される複雑な関連ルールを評価することにより、防御センターのパフォーマンスが低下する可能性があります。たとえば、システムで記録されるすべての接続に対して、複数の条件からなるルールを防御センター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。

条件の作成の詳細については、以下の項を参照してください。

- [単一の条件の作成 \(51-42 ページ\)](#)
- [条件の追加と結合 \(51-45 ページ\)](#)
- [複数の値を条件で使用する \(51-48 ページ\)](#)

単一の条件の作成

ライセンス:任意 (Any)

ほとんどの条件はカテゴリ、演算子、値の 3 つの要素で構成されます。より複雑な、複数のカテゴリを含む条件もあり、各カテゴリに固有の演算子と値が含まれることがあります。

たとえば、以下の関連ルールは、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トリガーとして使用されます。条件のカテゴリは [IP アドレス (IP Address)]、演算子は [含まれる (is in)]、値は 10.4.0.0/16 です。

Select the type of event for this rule

If and it meets the fol

上記の例の関連ルール トリガー基準を作成する方法:

アクセス: Admin/Discovery Admin

- 手順 1 関連ルールの作成を開始します。
詳細については、[関連ポリシーのルールの作成\(51-3 ページ\)](#)を参照してください。
- 手順 2 [ルールの作成(Create Rule)] ページの [このルールのイベント タイプを選択 (Select the type of event for this rule)] で [ディスカバリ イベントが発生 (a discovery event occurs)] を選択した後、ドロップダウン リストから [新しい IP ホストの検出 (a new IP host is detected)] を選択します。
- 手順 3 ルールの単一の条件を作成するには、まず、最初の(つまりカテゴリ)ドロップダウンリストから [IP アドレス (IP Address)] を選択します。
- 手順 4 表示される演算子のドロップダウンリストから、[含まれる (is in)] を選択します。



ヒント カテゴリが IP アドレスを表す場合、演算子として [含まれる (is in)] または [含まれない (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。FireSIGHT システム で使用する IP アドレス表記については、[IP アドレスの表記規則\(1-24 ページ\)](#)を参照してください。

- 手順 5 テキスト フィールドに 10.4.0.0/16 と入力します。
一方、以下のホスト プロファイル限定はより複雑です。これにより関連ルールが制約され、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ます。

Host Profile Qualification

Only generate an event if the host(s) involved have the following properties:

has the following properties

上記の例のホスト プロファイル限定を作成する方法:

アクセス: Admin/Discovery Admin

-
- 手順 1** ディスカバリ イベントによってトリガーとして使用される相関ルールを作成します。
詳細については、[相関ポリシーのルールの作成 \(51-3 ページ\)](#) を参照してください。
- 手順 2** [ルールの作成 (Create Rule)] ページで、[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。
[ホスト プロファイル限定 (Host Profile Qualification)] セクションが表示されます。
- 手順 3** [ホスト プロファイル限定 (Host Profile Qualification)] の最初の条件で、相関ルールを制約するために使用するホスト プロファイルを持つホストを指定します。
このホスト プロファイル限定は、ディスクバリ イベントに基づく相関ルールの一部であるため、使用可能なカテゴリは [ホスト (Host)] のみです。
- 手順 4** ホストのオペレーティング システムの詳細を指定するために、まず [オペレーティング システム (Operating System)] カテゴリを選択します。
[OS ベンダー (OS Vendor)]、[OS 名 (OS Name)]、[OS バージョン (OS Version)] の 3 つのサブカテゴリが表示されます。
- 手順 5** ホストが Microsoft Windows のどのバージョンを実行していても差し支えないことを指定するには、3 つのサブカテゴリすべてに同じ演算子 [一致する (is)] を使用します。
- 手順 6** 最後に、サブカテゴリの値を指定します。
[OS ベンダー (OS Vendor)] の値には [Microsoft]、[OS 名 (OS Name)] の値には [Windows] を選択し、[OS バージョン (OS Version)] の値は [任意 (any)] のままにします。
-

相関ルール トリガー、ホスト プロファイル限定、接続トラッカー、またはユーザ限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 トリガーの中でも、相関ルールの基礎となるイベントの種類に応じてカテゴリがさらに異なります。

また、選択するカテゴリに応じて、条件で使用できる演算子が異なります。さらに、条件の値を指定するために使用できる構文は、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を選択できます。



- (注) 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。詳細については、[複数の値を条件で使用する \(51-48 ページ\)](#) を参照してください。
-

相関ルール トリガー基準を作成するための構文の詳細については、以下の項を参照してください。

- [侵入イベントの構文 \(51-8 ページ\)](#)
- [マルウェア イベントの構文 \(51-11 ページ\)](#)
- [ディスクバリ イベントの構文 \(51-13 ページ\)](#)
- [ユーザ アクティビティ イベントの構文 \(51-16 ページ\)](#)
- [ホスト入力イベントの構文 \(51-17 ページ\)](#)
- [接続イベントの構文 \(51-18 ページ\)](#)
- [トラフィック プロファイル変化の構文 \(51-22 ページ\)](#)

ホストプロファイル限定、ユーザ限定、および接続トラッカーを作成するための構文の詳細については、以下の項を参照してください。

- [ホストプロファイル限定の構文\(51-25 ページ\)](#)
- [接続トラッカーの構文\(51-30 ページ\)](#)
- [接続トラッカー イベントの構文\(51-33 ページ\)](#)
- [ユーザ限定の構文\(51-39 ページ\)](#)

条件の追加と結合

ライセンス:任意(Any)

単純な関連ルールトリガー、接続トラッカー、ホストプロファイル限定、ユーザ限定を作成することも、複数の条件の組み合わせやネストを使って複雑な構造を作成することもできます。

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** 演算子で結合する必要があります。同じレベルにある複数の条件は、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。

たとえば、以下の関連ルールトリガー基準には、**OR** で結合された 2 つの条件が含まれます。これは、いずれかの条件が真であれば、ルールがトリガーとして使用されることを意味します。つまり、ホストの IP アドレスが 10.x.x.x サブネットに含まれない場合、またはホストが IGMP メッセージを送信する場合です。

The screenshot shows a configuration window titled "Select the type of event for this rule". It features a blue header bar with the text "If" followed by two dropdown menus: "a discovery event occurs" and "a new transport protocol is detected", and the text "and it meets the fol". Below the header are two buttons: "Add condition" and "Add complex condition". Underneath, there is a section for conditions. On the left, there is a dropdown menu set to "OR". To its right, there are two condition entries, each with a red "X" icon in a box to its left. The first entry consists of a dropdown menu set to "Transport Protocol", followed by a dropdown menu set to "is", and a text input field containing "IGMP". The second entry consists of a dropdown menu set to "IP Address", followed by a dropdown menu set to "is not in", and a text input field containing "10.0.0.0/8".

一方、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 there is new information about a TCP application and it meets the fol

is

is not

is

is

このルールは、非標準ポートで SSH が検出された場合にトリガーとして使用されます。最初 2 つの条件は、アプリケーションプロトコルの名前が SSH であること、およびポートが 22 でないことを指定します。このルールはさらに、イベントに関連するホストの IP アドレスが 10.4.x.x ネットワークまたは 192.168.x.x ネットワークのいずれかに含まれていなければならないことを指定します。

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 51-15 ルールの評価

| 条件 | 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 10.4.0.0/8 に含まれる |
| D | IP アドレスが 192.168.0.0/16 に含まれる |

単一の条件を追加する方法:

アクセス: Admin/Discovery Admin

手順 1 単一の条件を追加するには、現在の条件の上にある [条件の追加 (Add condition)] をクリックします。

現在の条件セットの下に、現在の条件セットと同じレベルで新しい条件が追加されます。デフォルトでは、同じレベルの条件に OR 演算子で結合されますが、演算子を AND に変更することもできます。

たとえば、以下のルールに単純な条件を追加すると、

Select the type of event for this rule

If

and it meets the following conditions:

371877

結果は以下のとおりです。

Select the type of event for this rule

If and it meets the following conditions:

OR

371877

複合条件を追加する方法:

アクセス: Admin/Discovery Admin

手順 1 現在の条件の上にある [複合条件の追加 (Add complex condition)] をクリックします。

現在の条件セットの下に複合条件が追加されます。1 つの複合条件は 2 つの副条件からなり、演算子(その上のレベルにある条件を結合するために使われているものとは逆の演算子)を使って副条件が互いに結合されます。

たとえば、以下のルールに複合条件を追加すると、

Select the type of event for this rule

If

and it meets the following conditions:

371877

結果は以下のとおりです。

Select the type of event for this rule

If and it meets the fol

条件を結合する方法:

アクセス: Admin/Discovery Admin

- 手順 1 条件セットの左側にあるドロップダウンリストを次のように使用します。次のいずれかを選択します。
- **AND** 演算子: 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: 制御対象のレベルにある 1 つの条件だけが満たされればよいことを示します

複数の値を条件で使用する

ライセンス: 任意 (Any)

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。たとえば、ホストで何らかの UNIX フレーバを実行している必要があることを示すホスト プロファイル限定をルールに追加するには、多数の条件を OR 演算子で結合する代わりに、以下の手順を使用できます。

複数の値を 1 つの条件に含めるには:

アクセス: Admin/Discovery Admin

- 手順 1 演算子として [含まれる (is in)] または [含まれない (is not in)] を選択して 1 つの条件を作成します。
- ドロップダウンリストがテキスト フィールドに変わります。
- 手順 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。
- ポップアップ ウィンドウが表示されます。
- 手順 3 [利用可能 (Available)] の下で、Ctrl キーまたは Shift キーを押しながら複数の値をクリックして選択します。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。

手順 4 右矢印(>)をクリックして、選択した項目を [選択済み(Selected)] に移動します。

手順 5 [OK] をクリックします。

[ルールの作成(Create Rule)] ページが再び表示されます。選択した内容が、条件の値フィールドに表示されます。

関連ポリシーのルールの管理

ライセンス:任意(Any)

関連ポリシー内で使われている関連ルールを管理するには、[ルール管理(Rule Management)] ページを使用します。ルールを作成、変更、および削除することができます。また、ルールグループを作成すると関連ルールを簡単に編成できます。ルールを変更/削除する方法、およびルールグループを作成する方法の詳細については、以下の項を参照してください。

- [ルールの変更\(51-49 ページ\)](#)
- [ルールの削除\(51-50 ページ\)](#)
- [ルールグループの作成\(51-50 ページ\)](#)

ルールの作成の詳細については、[関連ポリシーのルールの作成\(51-3 ページ\)](#)を参照してください。

ルールの変更

ライセンス:任意(Any)

既存の関連ルールを変更するには、以下の手順に従います。


既存のルールを変更する方法:

アクセス:Admin/Discovery Admin

手順 1 [ポリシー(Policies)] > [関連(Correlation)] を選択し、[ルール管理(Rule Management)] タブを選択します。

[ルール管理(Rule Management)] ページが表示されます。

手順 2 ルールがルールグループに含まれている場合は、グループ名をクリックしてグループを展開します。

手順 3 変更するルールの横にある編集アイコン()をクリックします。

[ルールの作成(Create Rule)] ページが表示されます。

手順 4 必要に応じて変更を加え、[保存(Save)] をクリックします。

ルールが更新されます。


ルールの削除

ライセンス:任意(Any)

1 つ以上の関連ポリシーで使用している関連ルールを削除することはできません。そのようなルールを削除する前に、それを含んでいるすべてのポリシーからそのルールを削除する必要があります。ポリシーからルールを削除する方法については、[関連ポリシーの編集\(51-60 ページ\)](#)を参照してください。

既存のルールを削除する方法:

アクセス:Admin/Discovery Admin

-
- 手順 1 [ポリシー(Policies)]>[関連(Correlation)]を選択し、[ルール管理(Rule Management)]タブを選択します。
- [ルール管理(Rule Management)] ページが表示されます。
- 手順 2 ルールがルール グループに含まれている場合は、グループ名をクリックしてグループを展開します。
- 手順 3 削除するルールの横にある削除アイコン()をクリックします。
- 手順 4 ルールを削除することを確認します。
- ルールが削除されます。
-

ルール グループの作成

ライセンス:任意(Any)


ルール グループを作成すると、関連ルールを簡単に編成できます。FireSIGHT システムには多数のデフォルトルールが備わっており、これらのルールは機能に応じてグループ化されています。たとえば、Worms ルールグループには、一般的なワームのアクティビティを検出するルールが含まれます。ルールグループの目的は、単に関連ルールを編成しやすくするためです。1 つのルールグループを関連ポリシーに割り当てることはできません。そうする代わりに、各ルールを個別に追加する必要があります。

ルールを作成するときに、そのルールを既存のグループに追加できます。また、既存のルールを変更して、グループに追加することもできます。詳細については、次の項を参照してください。

- [関連ポリシーのルールの作成\(51-3 ページ\)](#)
- [ルールの変更\(51-49 ページ\)](#)



ヒント

ルールグループを削除するには、削除するグループの横にある削除アイコン()をクリックします。ルールグループを削除しても、そのグループに含まれていたルールは削除されません。単にグループ化が解除されるだけです。

ルール グループを作成する方法:

アクセス: Admin/Discovery Admin

-
- 手順 1 [ポリシー (Policies)] > [関連 (Correlation)] を選択し、[ルール管理 (Rule Management)] タブを選択します。
[ルール管理 (Rule Management)] ページが表示されます。
 - 手順 2 [グループの作成 (Create Group)] をクリックします。
[グループの作成 (Create Group)] ページが表示されます。
 - 手順 3 [グループ名 (Group Name)] フィールドにグループの名前を入力します。
 - 手順 4 [グループの追加 (Add Group)] をクリックします。
グループが追加されます。
-

関連応答のグループ化

ライセンス: 任意 (Any)

アラート応答および修正 (修復) を作成した後 ([アラート応答の使用 \(43-2 ページ\)](#)) および [修復の作成 \(54-1 ページ\)](#) を参照)、それらをグループ化すると、グループに含まれるすべての応答がポリシー違反によってトリガーとして使用されます。応答グループを関連ルールに割り当てるには、その前に、[\[グループ \(Groups\)\]](#) ページでグループを作成する必要があります。

グループの横にあるスライダは、グループがアクティブであるかどうかを示します。関連ポリシー内のルールに応答グループを割り当てるには、それをアクティブにする必要があります。[並べ替え (Sort by)] ドロップダウンリストを使用すると、応答グループを状態別 (アクティブ/非アクティブ) または名前のアルファベット順でソートできます。

詳細については、次の各項を参照してください。

- [応答グループの作成 \(51-51 ページ\)](#)
- [応答グループの変更 \(51-52 ページ\)](#)
- [応答グループの削除 \(51-53 ページ\)](#)
- [応答グループのアクティブ化と非アクティブ化 \(51-53 ページ\)](#)

応答グループの作成

ライセンス: 任意 (Any)

個々のアラートと修正 (修復) を応答グループに含めた後、それを関連ポリシー内のルールに割り当てると、ポリシー違反が発生したときにアラートや修正のグループを起動させることができます。アクティブ ポリシー内のルールにグループが割り当てられた後、グループまたはグループ内のアラートや修正を変更すると、それが自動的にアクティブ ポリシーに適用されます。

応答グループを作成する方法:

アクセス:管理

-
- 手順 1 [ポリシー(Policies)] > [関連(Correlation)] を選択し、[グループ(Groups)] をクリックします。
[グループ(Groups)] ページが表示されます。
- 手順 2 [グループの作成(Create Group)] をクリックします。
[応答グループ(Response Group)] ページが表示されます。
- 手順 3 [名前(Name)] フィールドに、新しいグループの名前を入力します。
- 手順 4 [アクティブ(Active)] を選択するとグループがアクティブになり、関連ポリシー違反に対する応答としてこれを使用できるようになります。
- 手順 5 [利用可能な応答(Available Responses)] リストから、グループに含めるアラートと修正を選択します。



ヒント 複数の応答を選択するには、Ctrl キーを押したままクリックします。

- 手順 6 右矢印(>)をクリックして、アラートと修正をグループに移動します。
反対に、[グループ内の応答(Responses in Group)] リストからアラートと修正を選択して左矢印(<)をクリックすると、応答グループの外にアラートを移動することができます。
- 手順 7 [保存(Save)] をクリックします。
グループが作成されます。
-


応答グループの変更

ライセンス:任意(Any)

応答グループを変更するには、以下の手順に従います。

応答グループを変更する方法:

アクセス:管理

-
- 手順 1 [ポリシー(Policies)] > [関連(Correlation)] を選択し、[グループ(Groups)] をクリックします。
[グループ(Groups)] ページが表示されます。
- 手順 2 変更するグループの横にある編集アイコン()をクリックします。
[応答グループ(Response Group)] ページが表示されます。
- 手順 3 必要な変更を行い、[保存(Save)] をクリックします。
グループがアクティブで、使用中の場合は、変更内容がすぐに適用されます。
-


応答グループの削除

ライセンス:任意(Any)

関連ポリシーで使用されていない応答グループを削除することができます。応答グループを削除しても、そのグループに含まれている応答は**削除されません**。相互の関連付けが解除されるだけです。

応答グループを削除する方法:

アクセス:管理

-
- 手順 1 [ポリシー(Policies)] > [関連(Correlation)] を選択し、[グループ(Groups)] をクリックします。
[グループ(Groups)] ページが表示されます。
 - 手順 2 削除するグループの横にある削除アイコン() をクリックします。
 - 手順 3 グループを削除することを確認します。
グループが削除されます。
-

応答グループのアクティブ化と非アクティブ化

ライセンス:任意(Any)

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ができます。これにより、グループはシステムに残りますが、そのグループが割り当てられているポリシーに対する違反が発生しても、グループは起動されません。なお、関連ポリシーで使用されている応答グループを非アクティブにした場合、その応答グループは非アクティブであっても使用中とみなされます。使用中の応答グループを削除することはできません。

応答グループをアクティブまたは非アクティブにする方法:

アクセス:管理

-
- 手順 1 [ポリシー(Policies)] > [関連(Correlation)] を選択し、[グループ(Groups)] をクリックします。
[グループ(Groups)] ページが表示されます。
 - 手順 2 アクティブまたは非アクティブにする応答グループの横にあるスライダをクリックします。
グループがアクティブ化されていた場合は、非アクティブになります。非アクティブ化されていた場合は、アクティブになります。
-

関連ポリシーの作成

ライセンス:任意(Any)

関連ルールまたはコンプライアンス ホワイト リスト(あるいはその両方)、およびオプションでアラート応答と修正を作成した後、それらを使用して関連ポリシーを作成できます。

アクティブ ポリシー内の関連ルールまたはホワイト リストで指定されている基準をネットワークトラフィックが満たす場合、防御センターは関連イベントまたはホワイトリストイベントを生成します。また、ルールあるいはホワイト リストに割り当てられた応答も起動します。それぞれの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マッピングできます。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、防御センター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。

関連ポリシーを作成するために使用できる関連ルール、コンプライアンス ホワイト リスト、および応答を作成する方法の詳細については、以下の項を参照してください。

- [関連ポリシーのルールの作成\(51-3 ページ\)](#)
- [コンプライアンス ホワイト リストの作成\(52-8 ページ\)](#)
- [外部アラートの設定\(43-1 ページ\)](#)
- [修復の設定\(54-1 ページ\)](#)



ヒント

オプションで、スケルトン ポリシーを作成し、あとでそれを変更してルールと応答を追加できます。

関連ポリシーを作成する方法:

アクセス:Admin/Discovery Admin

- 手順 1 [ポリシー (Policies)] > [関連 (Correlation)] を選択します。
[ポリシー管理 (Policy Management)] ページが表示されます。
- 手順 2 [ポリシーの作成 (Create Policy)] をクリックします。
[ポリシーの作成 (Create Policy)] ページが表示されます。
- 手順 3 ポリシーの基本情報(名前や説明など)を指定します。
[ポリシーの基本情報の指定\(51-55 ページ\)](#)を参照してください。
- 手順 4 関連ポリシーに 1 つ以上のルールまたはホワイト リストを追加します。
[ルールとホワイト リストを関連ポリシーに追加する\(51-55 ページ\)](#)を参照してください。
- 手順 5 オプションで、ルールおよびホワイト リストのプライオリティを設定します。
[ルールおよびホワイト リストのプライオリティの設定\(51-56 ページ\)](#)を参照してください。
- 手順 6 オプションで、追加したルールまたはホワイト リストに、応答を追加します。
[ルールとホワイト リストに応答を追加する\(51-57 ページ\)](#)を参照してください。
- 手順 7 [保存 (Save)] をクリックします。
ポリシーが保存されます。



(注)

ポリシーで関連イベントやホワイトリスト イベントを生成したり、ポリシー違反に対する応答を起動したりするには、その前にポリシーをアクティブにする必要があります。詳細については、[関連ポリシーの管理\(51-58 ページ\)](#)を参照してください。

ポリシーの基本情報の指定

ライセンス:任意(Any)

各ポリシーを識別する名前を指定する必要があります。オプションで、簡単な説明をポリシーに追加できます。

また、ユーザ定義のプライオリティをポリシーに割り当てることもできます。関連ポリシーに対する違反の結果として生成される関連イベントには、そのポリシーに割り当てたプライオリティが表示されます(ただし、トリガーとして使用されたルールに独自のプライオリティが設定されている場合を除く)。



(注) ルールとホワイトリストのプライオリティは、ポリシーのプライオリティをオーバーライドします。詳細については、[ルールとホワイトリストを関連ポリシーに追加する \(51-55 ページ\)](#) を参照してください。

ポリシーの基本情報を指定する方法:

アクセス:Admin/Discovery Admin

-
- 手順 1 [ポリシーの作成(Create Policy)] ページで、[ポリシー名(Policy Name)] フィールドにポリシーの名前を入力します。
- 手順 2 [ポリシーの説明(Policy Description)] フィールドに、ポリシーの説明を入力します。
- 手順 3 [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。
- 1 から 5 までのプライオリティ値を選択できます。1 が最高、5 が最低です。または、[なし(None)] を選択すると、特定のルールに割り当てられたプライオリティだけが使用されます。
- 手順 4 次の項([ルールとホワイトリストを関連ポリシーに追加する \(51-55 ページ\)](#))の手順に進みます。
-

ルールとホワイトリストを関連ポリシーに追加する

ライセンス:任意(Any)

1つの関連ポリシーには、1つ以上の関連ルールまたはホワイトリストが含まれます。ポリシー内のいずれかのルールまたはホワイトリストに対する違反が発生すると、システムはイベントをデータベースに記録します。ルールまたはホワイトリストに1つ以上の応答がすでに割り当てられている場合、それらの応答が起動されます。

以下の図は、コンプライアンス ホワイトリストと一連の関連ルールからなる、さまざまな応答が設定された関連ポリシーを示しています。

z

Policy Rules

| Rule | Responses |
|--|---|
| Bugbear Worm Detects the Bugbear HTTP server backdoor | Sample Email Alert Response (Email) |
| Default White List | Sample SNMP Alert Response (SNMP) |
| Lovgate Worm Detects activity by the Lovgate worm backdoor component | Sample Syslog Alert Response (Syslog) |
| MyDoom Worm Detects activity by the backdoor component of MyDoom | Sample Syslog Alert Response (Syslog) Sample SNMP Alert Response (SNMP) Sample Email Alert Response (Email) |
| NetSky.S Detects the backdoor component of the NetSky.S worm. | This rule does not have any responses |

ルールまたはホワイト リストを関連ポリシーに追加する方法:

アクセス: Admin/Discovery Admin

-
- 手順 1 [ポリシーの作成(Create Policy)] ページで、[ルールの追加(Add Rules)] をクリックします。
[利用可能なルール(Available Rules)] ポップアップが表示されます。
 - 手順 2 該当するフォルダ名をクリックしてフォルダを展開します。
 - 手順 3 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。
[ポリシーの作成(Create Policy)] ページが再び表示されます。選択したルールとホワイト リストがポリシーに含まれます。
 - 手順 4 次の項([ルールおよびホワイト リストのプライオリティの設定\(51-56 ページ\)](#))の手順に進みます。
-

ルールおよびホワイト リストのプライオリティの設定

ライセンス:任意(Any)

関連ポリシーに含まれる個々の関連ルールやコンプライアンス ホワイト リストに、ユーザ定義のプライオリティを割り当てることができます。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結果として生成されるイベントには、そのルールまたはホワイト リストに割り当てたプライオリティが表示されます。一方、プライオリティ値を割り当てない状態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ると、結果として生成されるイベントには、ポリシーのプライオリティ値が表示されます。

たとえば、あるポリシー自体のプライオリティが 1 に設定され、そのポリシー内の 1 つのルールにプライオリティ 3 が設定され、他のルールまたはホワイト リストにはデフォルト プライオリティが設定されているとします。プライオリティ 3 のルールがトリガーとして使用された場合、結果としてできる関連イベントのプライオリティ値は 3 と表示されます。ポリシー内の他の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、結果としてできるイベントには、ポリシーのプライオリティから得られたプライオリティ値 1 が表示されます。

ルールまたはホワイトリストのプライオリティを設定する方法:

アクセス: Admin/Discovery Admin

-
- 手順 1 [ポリシーの作成 (Create Policy)] ページで、ルールまたはホワイトリストごとの [プライオリティ (Priority)] リストから、デフォルトプライオリティを選択します。次のいずれかを選択できます。
- 1 から 5 までのプライオリティ値 (1 が最高、5 が最低)
 - なし (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)
- 手順 2 次の項(ルールとホワイトリストに応答を追加する (51-57 ページ))の手順に進みます。
-

ルールとホワイトリストに応答を追加する

ライセンス: 任意 (Any)

関連ポリシー内で、個々のルールまたはホワイトリストを 1 つの応答または応答のグループにマッピングできます。ポリシー内のいずれかのルールまたはホワイトリストに対する違反が発生した場合、システムは関連するイベントをデータベースに記録し、そのルールまたはホワイトリストに割り当てられている応答を起動します。ポリシー内の複数の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、防御センターはそれぞれのルールまたはホワイトリストに関連付けられている応答を起動します。

応答と応答グループを作成する方法の詳細については、以下の項を参照してください。

- [外部アラートの設定 \(43-1 ページ\)](#)
- [修復の設定 \(54-1 ページ\)](#)
- [関連応答のグループ化 \(51-51 ページ\)](#)



(注)

トラフィック プロファイルの変更でトリガーとして使用する関連ルールへの応答として Nmap 修復を割り当てないでください。修正は起動されません。

以下の図は、コンプライアンス ホワイトリストと一連の関連ルールからなる、さまざまな応答が設定された関連ポリシーを示しています。

z

Policy Rules

| Rule | Responses |
|--|---|
| Bugbear Worm Detects the Bugbear HTTP server backdoor | Sample Email Alert Response (Email) |
| Default White List | Sample SNMP Alert Response (SNMP) |
| Lovgate Worm Detects activity by the Lovgate worm backdoor component | Sample Syslog Alert Response (Syslog) |
| MyDoom Worm Detects activity by the backdoor component of MyDoom | Sample Syslog Alert Response (Syslog) Sample SNMP Alert Response (SNMP) Sample Email Alert Response (Email) |
| NetSky.S Detects the backdoor component of the NetSky.S worm. | This rule does not have any responses. |

ルールとホワイトリストに応答を追加する方法:

アクセス: Admin/Discovery Admin

手順 1 [ポリシーの作成(Create Policy)] ページで、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。

ポップアップ ウィンドウが表示されます。

手順 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 1 つ以上の応答または応答グループを選択して、上矢印をクリックします。



ヒント 複数の応答を選択するには、Ctrl キーを押したままクリックします。

手順 3 [更新(Update)] をクリックします。

[ポリシーの作成(Create Policy)] ページが再び表示されます。指定した応答がルールまたはホワイトリストに追加されます。

関連ポリシーの管理

ライセンス: 任意 (Any)

関連ポリシーの管理は、[ポリシー管理(Policy Management)] ページで行います。ポリシーを作成、変更、ソート、アクティブ化、非アクティブ化、および削除できます。

ポリシーの横にあるスライダは、ポリシーがアクティブであるかどうかを示します。ポリシーで関連イベントやホワイトリスト イベントを生成するためには、ポリシーをアクティブにする必要があります。[並べ替え(Sort by)] ドロップダウン リストを使用すると、ポリシーを状態別(アクティブ/非アクティブ)または名前のアルファベット順でソートできます。

アクティブな関連ポリシーにコンプライアンス ホワイトリストが含まれている場合、以下のアクションによって、そのホワイトリストに関連付けられているホスト属性が削除されることも、ホスト属性の値が変更されることもありません。

- ポリシーの非アクティブ化
- ポリシーの変更(ホワイトリストを削除)
- ポリシーの削除

つまり、たとえばアクションを実行した時点で準拠していたホストは、ホスト属性ネットワークマップで引き続き準拠ホストとして表示されます。ホスト属性を削除するには、対応するホワイトリストを削除する必要があります。

ネットワーク上のホストのホワイトリストコンプライアンスを更新するには、関連ポリシー再びアクティブ化するか(以前に非アクティブ化した場合)、またはホワイトリストを別のアクティブな関連ポリシーに追加する必要があります(関連ポリシーからホワイトリストを削除した場合、またはポリシー自体を削除した場合)。この操作を実行すると発生するホワイトリストの再評価によって、ホワイトリストイベントが生成されることはありません。したがって、ホワイトリストに関連付けられた応答がトリガーとして使用されることもありません。コンプライアンス ホワイトリストの詳細については、[FireSIGHT システムのコンプライアンス ツールとしての使用 \(52-1 ページ\)](#)を参照してください。

関連ポリシーを管理する方法の詳細については、以下の項を参照してください。

- [関連ポリシーのアクティブ化と非アクティブ化 \(51-59 ページ\)](#)
- [関連ポリシーの編集 \(51-60 ページ\)](#)
- [関連ポリシーの削除 \(51-60 ページ\)](#)

新しいポリシーを作成する方法については、[関連ポリシーの作成 \(51-53 ページ\)](#)を参照してください。

関連ポリシーのアクティブ化と非アクティブ化

ライセンス:任意(Any)

関連ポリシーをアクティブまたは非アクティブにするには、以下の手順に従います。

ポリシーをアクティブ化または非アクティブ化する方法:

アクセス:Admin/Discovery Admin

-
- 手順 1** [ポリシー (Policies)] > [関連 (Correlation)] を選択します。
[ポリシー管理 (Policy Management)] ページが表示されます。
- 手順 2** アクティブまたは非アクティブにするポリシーの横にあるスライダをクリックします。
ポリシーがアクティブであった場合は、非アクティブになります。非アクティブ化されていた場合は、アクティブになります。
-

関連ポリシーの編集

ライセンス:任意(Any)

関連ポリシーを変更するには、以下の手順に従います。

ポリシーを編集するには、次の手順を実行します。

アクセス:Admin/Discovery Admin

-
- 手順 1 [ポリシー(Policies)] > [関連(Correlation)] を選択します。
[ポリシー管理(Policy Management)] ページが表示されます。
- 手順 2 ポリシーの横にある編集アイコン(✎)をクリックします。
[ポリシーの作成(Create Policy)] ページが表示されます。変更可能なさまざまな設定の詳細については、[関連ポリシーの作成\(51-53 ページ\)](#)を参照してください。関連ポリシーからルールまたはホワイトリストを削除するには、[ポリシーの作成(Create Policy)] ページで、削除するルールまたはホワイトリストの横にある削除アイコン(🗑️)をクリックします。
- 手順 3 必要な変更を行い、[保存(Save)] をクリックします。
ポリシーが変更されます。ポリシーがアクティブな場合は、変更内容がすぐに適用されます。
-

関連ポリシーの削除

ライセンス:任意(Any)

関連ポリシーを削除するには、以下の手順に従います。

ポリシーを削除する方法:

アクセス:Admin/Discovery Admin

-
- 手順 1 [ポリシー(Policies)] > [関連(Correlation)] を選択します。
[ポリシー管理(Policy Management)] ページが表示されます。
- 手順 2 削除するポリシーの横にある削除アイコン(🗑️)をクリックします。
ポリシーが削除されます。
-

関連イベントの操作

ライセンス:任意(Any)

アクティブな関連ポリシーに含まれる関連ルールがトリガーとして使用されると、防御センターが関連イベントを生成してデータベースにそれを記録します。データベースに保存される関連イベントの数を設定する方法については、[データベース イベント制限の設定\(63-16 ページ\)](#)を参照してください。



(注) アクティブな関連ポリシーに含まれるコンプライアンス ホワイトリストがトリガーとして使用されると、防御センターがホワイトリスト イベントを生成します。詳細については、[ホワイトリスト イベントの操作 \(52-34 ページ\)](#) を参照してください。

詳細については、次の項を参照してください。

- [関連イベントの表示 \(51-61 ページ\)](#)
- [関連イベント テーブルについて \(51-63 ページ\)](#)
- [関連イベントの検索 \(51-64 ページ\)](#)

関連イベントの表示

ライセンス:任意(Any)

関連イベントのテーブルを表示し、検索対象の情報に応じてイベント ビューを操作できます。関連イベントにアクセスしたときに表示されるページは、使用するワークフローによって異なります。関連イベントのテーブル ビューが含まれる定義済みワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。カスタム ワークフローの作成方法については、[カスタム ワークフローの作成 \(58-44 ページ\)](#) を参照してください。

次の表では、関連イベント ワークフローのページで実行できる操作をいくつか説明します。

表 51-16 関連イベントの操作


| 目的 | 操作 |
|---------------------------------|--|
| IP アドレスのホスト プロファイルを表示する | IP アドレスの横に表示されるホスト プロファイル アイコンをクリックします。 |
| ユーザ プロファイル情報を表示する | ユーザ ID の隣に表示されているユーザ アイコン()をクリックします。詳細については、 ユーザの詳細とホストの履歴について (50-68 ページ) を参照してください。 |
| 現在のワークフロー ページでイベントをソートおよび制約する | ドリルダウン ワークフロー ページのソート (58-39 ページ) で詳細を参照してください。 |
| 現在のワークフロー ページ内で移動する | ワークフロー内の他のページへのナビゲート (58-40 ページ) で詳細を参照してください。 |
| 現在の制限を維持して、現在のワークフロー内のページ間を移動する | ワークフロー ページの左上で、該当するページ リンクをクリックします。詳細については、 ワークフローのページの使用 (58-21 ページ) を参照してください。 |
| 表示された列の詳細を表示する | 関連イベント テーブルについて (51-63 ページ) で詳細を参照してください。 |
| 表示されたイベントの時刻と日付の範囲を変更する | イベント時間の制約の設定 (58-27 ページ) で詳細を参照してください。 イベント ビューを時間によって制約している場合は、(グローバルかイベントに特有关係なく) アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあることに注意してください。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。 |

表 51-16 関連イベントの操作(続き)

| 目的 | 操作 |
|----------------------------------|--|
| 特定の値に制限して、ワークフロー内の次のページにドリルダウンする | <p>次のいずれかの方法を使用します。</p> <ul style="list-style-type: none"> カスタム ワークフローで作成したドリルダウン ページで、行内の値をクリックします。テーブル ビューの行内の値をクリックすると、テーブル ビューが制限され、次のページにドリルダウンされないことに注意してください。 一部のユーザに制限して次のワークフロー ページにドリルダウンするには、次のワークフロー ページに表示するユーザの横にあるチェック ボックスをオンにしてから、[表示(View)] をクリックします。 現在の制限を維持して次のワークフロー ページにドリルダウンするには、[すべてを表示(View All)] をクリックします。 <p>ヒント テーブル ビューでは、必ずページ名に「Table View」が含まれます。</p> <p>詳細については、イベントの制約(58-35 ページ)を参照してください。</p> |
| システムから関連イベントを削除する | <p>次のいずれかの方法を使用します。</p> <ul style="list-style-type: none"> 特定のイベントを削除するには、削除するイベントの横にあるチェック ボックスをオンしてから、[削除(Delete)] をクリックします。 現在の制限ビュー内のすべてのイベントを削除するには、[すべて削除(Delete All)] をクリックしてから、すべてのイベントを削除することを確認します。 |
| 他のイベント ビューに移動して関連イベントを表示する | <p>ワークフロー間のナビゲート(58-41 ページ)で詳細を参照してください。</p> |

関連イベントを表示する方法:

アクセス:Admin/Any Security Analyst

手順 1 [分析(Analysis)] > [関連(Correlation)] > [関連イベント(Correlation Events)] を選択します。

デフォルト関連イベント ワークフローの最初のページが表示されます。カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [(ワークフローの切り替え)((switch workflow))] をクリックします。別のデフォルト ワークフローの指定方法については、[イベント ビュー設定の設定\(71-3 ページ\)](#)を参照してください。イベントが表示されない場合は、時間範囲の調整が必要な可能性があります。[イベント時間の制約の設定\(58-27 ページ\)](#)を参照してください。



ヒント

関連イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)((switch workflow))] をクリックし、[関連イベント(Correlation Events)] を選択します。

関連イベント テーブルについて

ライセンス:任意(Any)

関連ルールがトリガーとして使用されると、防御センター は関連イベントを生成します。関連イベント テーブルのフィールドについて、以下の表で説明します。

表 51-17 関連イベントのフィールド

| フィールド | 説明 |
|--|--|
| 時刻 (Time) | 関連イベントが生成された日時。 |
| 影響 (Impact) | 侵入データ、ディスクバリ データ、および脆弱性情報の間の相関に基づいて関連イベントに割り当てられた影響レベル。詳細については、 影響レベルを使用してイベントを評価する (41-41 ページ) を参照してください。 |
| インライン結果 (Inline Result) | 次のいずれかになります。 <ul style="list-style-type: none"> 黒の下矢印: 侵入ルールをトリガーとして使用したパケットがシステムによってドロップされたことを示します グレーの下矢印: 侵入ポリシー オプション [インライン時にドロップ (Drop when Inline)] を有効にした場合、インライン型、スイッチ型、またはルーティング型展開でパケットがシステムによってドロップされたことと想定されることを示します 空白: トリガーとして使用された侵入ルールが [ドロップしてイベントを生成する (Drop and Generate Events)] に設定されていなかったことを示します <p>侵入ポリシーのドロップ動作や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ないことに注意してください。</p> |
| 送信元 IP (Source IP) または宛先 IP (Destination IP) | ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホストの IP アドレス。 |
| 送信元国 (Source Country) または宛先国 (Destination Country) | ポリシー違反をトリガーとして使用した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。 |
| セキュリティ インテリジェンスのカテゴリ (Security Intelligence Category) | ブラックリスト化されたオブジェクトの名前。これは、ポリシー違反をトリガーとして使用したイベントでブラックリスト化された IP アドレスを示す (またはその IP アドレスを含む) オブジェクトです。 |
| 送信元ユーザ (Source User) または宛先ユーザ (Destination User) | ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホストにログインしたユーザの名前。 |
| 送信元ポート/ICMP タイプ (Source Port/ICMP Type) または宛先ポート/ICMP コード (Destination Port/ICMP Code) | ポリシー違反をトリガーとして使用したイベントに関連付けられた、送信元トラフィックの送信元ポート/ICMP タイプまたは宛先トラフィックの宛先ポート/ICMP コード。 |
| 説明 | <p>関連イベントについての説明。説明に示される情報は、ルールがどのようにトリガーとして使用されたかによって異なります。</p> <p>たとえば、オペレーティング システム情報の更新イベントによってルールがトリガーとして使用された場合、新しいオペレーティング システムの名前と信頼度レベルが表示されます。</p> |
| ポリシー | 違反が発生したポリシーの名前。 |

表 51-17 相関イベントのフィールド(続き)

| フィールド | 説明 |
|---|--|
| ルール(Rule) | ポリシー違反をトリガーとして使用したルールの名前。 |
| [プライオリティ(Priority)] | ポリシー違反をトリガーとして使用したポリシーまたはルールで指定されたプライオリティ。 |
| 送信元ホスト重要度(Source Host Criticality)または宛先ホスト重要度(Destination Host Criticality) | 相関イベントに関連する送信元または宛先ホストにユーザが割り当てたホスト重要度。None、Low、Medium、または High のいずれかです。 ディスカバリ イベント、ホスト入力イベント、または接続イベントに基づくルールによって生成された相関イベントにのみ、送信元ホスト重要度が含まれることに注意してください。ホスト重要度の詳細については、 事前定義のホスト属性の使用(49-34 ページ) を参照してください。 |
| 入力セキュリティゾーン(Ingress Security Zone)または出力セキュリティゾーン(Egress Security Zone) | ポリシー違反をトリガーとして使用した侵入イベントまたは接続イベントの入力または出力セキュリティゾーン。 |
| Device | ポリシー違反をトリガーとして使用したイベントを生成したデバイスの名前。 |
| 入力インターフェイス(Ingress Interface)または出力インターフェイス(Egress Interface) | ポリシー違反をトリガーとして使用した侵入イベントまたは接続イベントの入力または出力インターフェイス。 |
| メンバー数(Count) | 各行に表示された情報と一致するイベントの数。[カウント(Count)] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。 |

相関イベント テーブルの表示の詳細については、以下の項を参照してください。

- [相関イベントの表示\(51-61 ページ\)](#)
- [相関イベントの検索\(51-64 ページ\)](#)

相関イベントの検索

ライセンス:任意(Any)

特定の相関イベントを検索できます。実際のネットワーク環境に合わせてカスタマイズされた検索を作成して保存すると、あとで再利用できます。次の表に、使用可能な検索基準の説明を示します。

表 51-18 相関イベントの検索基準

| フィールド | 検索基準ルール |
|-----------|--|
| ポリシー | 検索する相関ポリシーの名前を入力します。 |
| ルール(Rule) | 検索する相関ルールの名前を入力します。 |
| 説明 | 相関イベントの説明またはその一部を入力します。説明に含まれる情報は、ルールをトリガーとして使用させたイベントによって異なります。 |

表 51-18 関連イベントの検索基準(続き)

| フィールド | 検索基準ルール |
|---|--|
| [プライオリティ (Priority)] | <p>関連イベントのプライオリティを指定します(これは、トリガーとして使用されたルールのプライオリティまたは違反が発生した関連ポリシーのプライオリティによって決まります)。プライオリティなしを指定するには、「none」と入力します。関連ルールとポリシーの優先度の設定方法については、ポリシーの基本情報の指定 (51-55 ページ)とルールおよびホワイトリストのプライオリティの設定 (51-56 ページ)を参照してください。</p> |
| 送信元国 (Source Country)、宛先国 (Destination Country)、または送信元/宛先の国 (Source/Destination Country) | <p>ポリシー違反をトリガーとして使用したイベントの送信元 IP アドレス、宛先 IP アドレス、または送信元/宛先 IP アドレスに関連付けられた国を指定します。</p> |
| 送信元の大陸 (Source Continent)、宛先の大陸 (Destination Continent)、または送信元/宛先の大陸 (Source/Destination Continent) | <p>ポリシー違反をトリガーとして使用したイベントの送信元 IP アドレス、宛先 IP アドレス、または送信元/宛先 IP アドレスに関連付けられた大陸を指定します。</p> |
| セキュリティ インテリジェンスのカテゴリ (Security Intelligence Category) | <p>ポリシー違反をトリガーとして使用した関連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指定します。セキュリティ インテリジェンスのカテゴリとして、セキュリティ インテリジェンス オブジェクト、グローバルブラックリスト、カスタム セキュリティ インテリジェンス リストまたはフィード、あるいはインテリジェンス フィードに含まれるいずれかのカテゴリを指定できます。詳細については、セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録 (13-1 ページ)を参照してください。</p> |
| 送信元 IP (Source IP)、宛先 IP (Destination IP)、または送信元/宛先 IP (Source/Destination IP) | <p>ポリシー違反をトリガーとして使用したイベントの送信元ホスト、宛先ホスト、または送信元/宛先ホストの IP アドレスを指定します。単一の IP アドレスまたはアドレスブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。また、否定を使用することもできます。詳細については、検索での IP アドレスの指定 (60-6 ページ)を参照してください。</p> |
| 送信元ユーザ (Source User) または宛先ユーザ (Destination User) | <p>ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホストにログインしたユーザを指定します。</p> |
| 送信元ポート/ICMP タイプ (Source Port/ICMP Type) または宛先ポート/ICMP コード (Destination Port/ICMP Code) | <p>ポリシー違反をトリガーとして使用したイベントに関連付けられた、送信元トラフィックの送信元ポート/ICMP タイプまたは宛先トラフィックの宛先ポート/ICMP コードを指定します。</p> |
| 影響 (Impact) | <p>関連イベントに割り当てられた影響を指定します。大文字と小文字を区別しない有効な値は、Impact 0、Impact Level 0、Impact 1、Impact Level 1、Impact 2、Impact Level 2、Impact 3、Impact Level 3、Impact 4、および Impact Level 4 です。影響アイコンの色または部分文字列は使用しないでください(たとえば、blue、level 1、または 0 を使用しないでください)。詳細については、影響レベルを使用してイベントを評価する (41-41 ページ)を参照してください。</p> |

表 51-18 関連イベントの検索基準(続き)

| フィールド | 検索基準ルール |
|---|---|
| インライン結果 (Inline Result) | <p>侵入イベントによってトリガーとして使用されたポリシー違反の場合、以下のいずれかを入力します。</p> <ul style="list-style-type: none"> dropped は、インライン型、スイッチ型、またはルーティング型展開でパケットがドロップされたかどうかを示します。 would have dropped は仮定を表します。インライン型、スイッチ型、またはルーティング型展開でパケットをドロップするよう侵入ポリシーが設定されていると仮定した場合、パケットがドロップされるかどうかを示します。 <p>侵入ポリシーのドロップ動作や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ないことに注意してください。</p> |
| 送信元ホスト重要度 (Source Host Criticality) または宛先ホスト重要度 (Destination Host Criticality) | <p>ポリシー違反に関連する送信元または宛先ホストの重要度として、None、Low、Medium、または High のいずれかを指定します。ディスカバリ イベント、ホスト入力イベント、または接続イベントに基づくルールによって生成された関連イベントにのみ、送信元ホスト重要度が含まれることに注意してください。ホスト重要度の詳細については、事前定義のホスト属性の使用 (49-34 ページ) を参照してください。</p> |
| 入力セキュリティゾーン (Ingress Security Zone) 出力セキュリティゾーン (Egress Security Zone)、または入力/出力セキュリティゾーン (Ingress/Egress Security Zone) | <p>ポリシー違反をトリガーとして使用した侵入イベントまたは接続イベントの入力、出力、または入力/出力セキュリティゾーンを指定します。</p> |
| Device | <p>ポリシー違反をトリガーしたイベントを生成した特定のデバイスに検索を制限するには、デバイス名または IP アドレス、またはデバイスグループ、スタック、またはクラスタ名を入力します。検索での FireSIGHT システムによるデバイス フィールドの処理方法については、検索でのデバイスの指定 (60-7 ページ) を参照してください。</p> |
| 入力インターフェイス (Ingress Interface) または出力インターフェイス (Egress Interface) | <p>ポリシー違反をトリガーとして使用した侵入イベントまたは接続イベントの入力または出力インターフェイスを指定します。</p> |

関連イベントを検索する方法:

アクセス: Admin/Any Security Analyst

-
- 手順 1 [分析 (Analysis)] > [検索 (Search)] を選択します。
[検索 (Search)] ページが表示されます。
- 手順 2 テーブル ドロップダウン リストから [関連イベント (Correlation Events)] を選択します。
ページが適切な制約によって更新されます。
- 手順 3 表「[関連イベントの検索基準](#)」に記載されているように、該当するフィールドに検索基準を入力します。
- すべてのフィールドで否定 (!) を使用できます。
 - すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。

- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
 - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、A, B, "C, D, E" を検索すると、指定したフィールドに「A」または「B」または「C, D, E」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
 - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
 - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、A, B, "C, D, E" をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに A または B、または C、D、E のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク (*) を受け入れます。
- フィールドでその情報を利用できないイベントを示すには、そのフィールドで n/a を指定します。フィールドに情報が入力されているイベントを示すには !n/a を使用します。
- 検索条件としてオブジェクトを使用するには、検索フィールドの横に表示されるオブジェクトの追加アイコン (+) をクリックします。

検索でのオブジェクトの使用を含む検索構文の詳細については、[イベントの検索 \(60-1 ページ\)](#) を参照してください。

- 手順 4** 必要に応じて検索を保存する場合は、[プライベート (Private)] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。



ヒント

カスタム ユーザ ロールのデータの制限として検索を使用する場合は、必ずプライベート検索として保存する**必要**があります。

- 手順 5** 必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [保存 (Save)] をクリックして、検索条件を保存します。
新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [保存 (Save)] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され ([プライベート (Private)] を選択した場合は本人のアカウントでのみ閲覧可能)、後で実行できます。
- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[新規として保存 (Save As New)] をクリックします。
ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [保存 (Save)] をクリックします。検索が保存され ([プライベート (Private)] を選択した場合は本人のアカウントでのみ閲覧可能)、後で実行できます。

- 手順 6** 検索を開始するには、[検索 (Search)] ボタンをクリックします。

現在の時間範囲によって制約されたデフォルト関連イベント ワークフローに、検索結果が表示されます。カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [(ワークフローの切り替え) ((switch workflow))] をクリックします。別のデフォルト ワークフローの指定方法については、[イベント ビュー設定の設定 \(71-3 ページ\)](#) を参照してください。

