相関ポリシーおよび相関ルールの設定

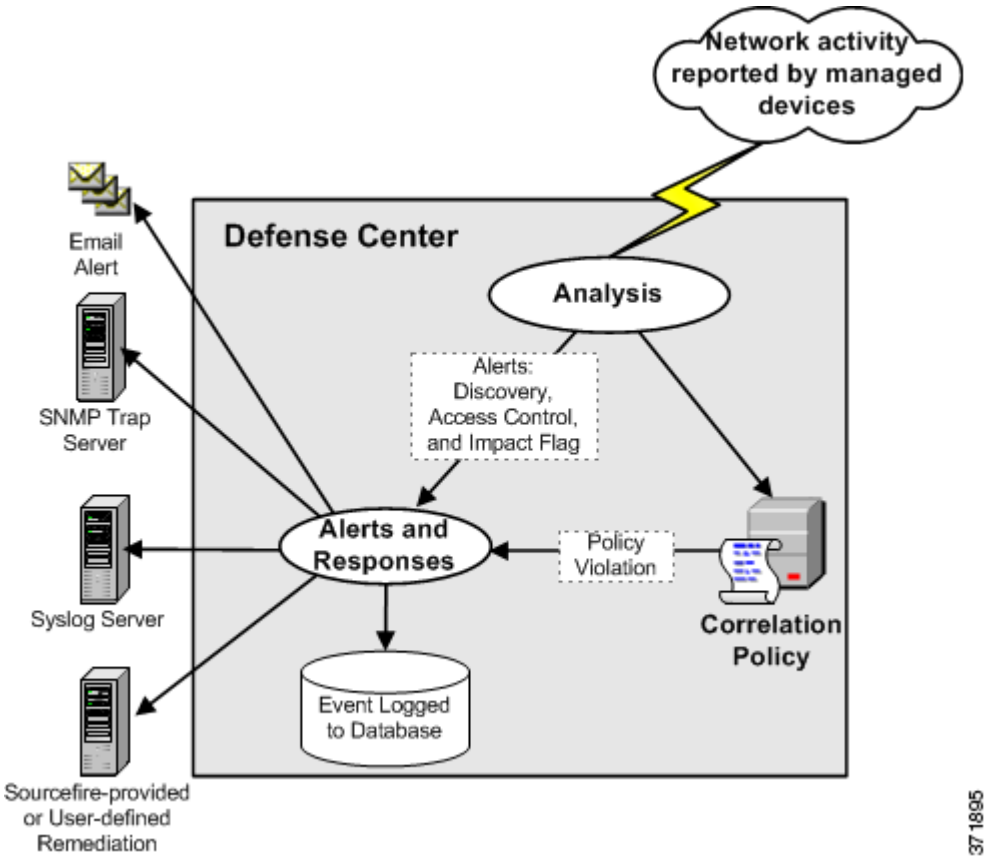
FireSIGHT システムの*相関*機能を使用すると、*相関ポリシー*を作成し、そこに*相関ルール*と*コンプライアンス ホワイトリスト*を含めることで、ネットワークに対する脅威にリアルタイムで対処できます。ネットワーク上のアクティビティによって相関ルールまたはホワイトリストのいずれかがトリガーとして使用されると、相関*ポリシー違反*が発生します。

相関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、イベント通知と相関のプロセスを示します。



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する方法、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」（P.39-3）
- 「相関ポリシーのルールの管理」（P.39-43）
- 「相関応答のグループ化」（P.39-45）
- 「相関ポリシーの作成」（P.39-48）
- 「相関ポリシーの管理」（P.39-52）
- 「相関イベントの操作」（P.39-54）

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」（P.27-1）
- 「アラート応答の使用」（P.15-2）
- 「相関ポリシーおよび相関ルールの設定」（P.39-1）

相関ポリシーのルールの作成

ライセンス：FireSIGHT、Protection、URL Filtering、または Malware

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

相関ポリシーを作成する前に、それに含める相関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、相関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」（P.27-9）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相関ルールがトリガーとして使用され、相関イベントが生成されます。相関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、以下の要素を相関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、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、相関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、相関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、相関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相関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、効果的な相関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相関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、「ライセンスのタイプと制約事項」（P.52-2）を参照してください。

表 39-1　相関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
侵入イベントによって相関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、またはユーザ アクティビティによって相関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相関ルールに追加する	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 イベントによって相関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	任意
URL データを使用して接続イベントによって相関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 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 データに基づいて相関ルールをトリガーとして使用する シリーズ 2 デバイスと DC500 防御センターはどちらも、ネットワークベースのマルウェア対策をサポートしていません。	Malware

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。詳細については、「ルールの作成メカニズムについて」（P.39-36）を参照してください。

相関ルールを作成する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Correlation] を選択し、[Rule Management] タブを選択します。

[Rule Management] ページが表示されます。

ステップ 2　[Create Rule] をクリックします。

[Create Rule] ページが表示されます。

ステップ 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」（P.39-5）を参照してください。

ステップ 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。

「相関ルール トリガー条件の指定」（P.39-6）を参照してください。

ステップ 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」（P.39-19）を参照してください。

ステップ 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相関ルールの制約」（P.39-23）を参照してください。

ステップ 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」（P.39-33）を参照してください。

ステップ 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」（P.39-35）を参照してください。

ステップ 9　[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相関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相関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

それぞれの相関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

ステップ 1　[Policies] > [Correlation] を選択し、[Rule Management] タブを選択します。

[Rule Management] ページが表示されます。

ステップ 2　[Create Rule] をクリックします。

[Create Rule] ページが表示されます。

ステップ 3　[Create Rule] ページの [Rule Name] フィールドに、ルールの名前を入力します。

ステップ 4　[Rule Description] フィールドに、ルールの説明を入力します。

ステップ 5　オプションで、[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、「相関ポリシーのルールの管理」（P.39-43）を参照してください。

ステップ 6　次の項（相関ルール トリガー条件の指定）の手順に進みます。

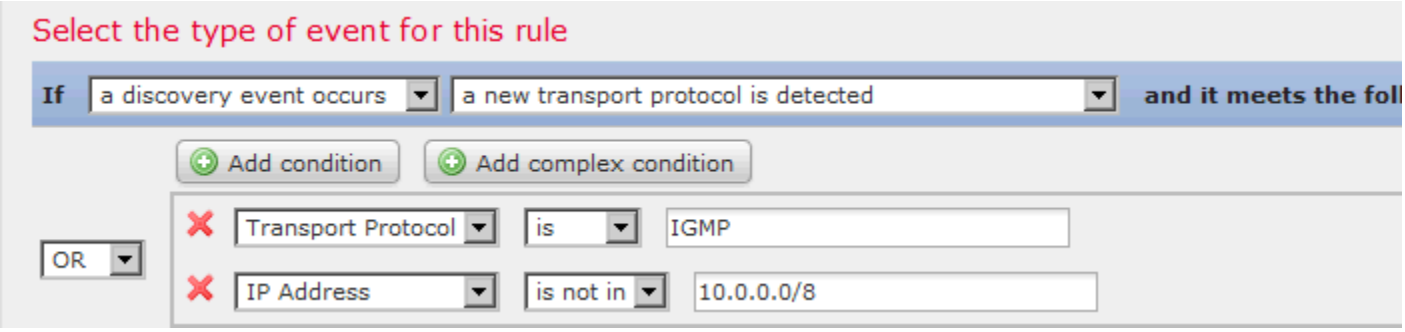
相関ルール トリガー条件の指定

ライセンス：FireSIGHT、Protection、URL Filtering、または Malware

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

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相関ルールでは、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相関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。



相関ルール トリガー基準を指定する方法：

アクセス：Admin/Discovery Admin

ステップ 1　ルールの基礎となるイベントのタイプを選択します。

相関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。[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、[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、[a Malware event occurs] を選択します。

  シリーズ 2 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対策をサポートしていません。したがって、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 データおよび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 イベントによる相関ルール トリガーをサポートしないことに注意してください。
- 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、[a discovery event occurs] を選択します。また、ディスカバリ イベントによって相関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もあります。「ディスカバリ イベントのタイプについて」（P.38-10）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）。ただし、[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、[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、[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相関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もあります。「ホスト入力イベントのタイプについて」（P.38-15）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、[a connection event occurs] を選択します。また、接続イベントによって相関ルールをトリガーとして使用する場合には、接続の開始または終了だけを表す接続イベントを使用するのか、それとも両者のいずれも表す接続イベントを使用するのかを選択する必要もあります。

  シリーズ 2 デバイスと DC500 防御センターは、カテゴリや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。したがって、これらのアプライアンスは、URL データを使用した接続イベントによる相関ルールのトリガー、および URL データを使用した接続トラッカーの作成をサポートしないことに注意してください。さらに、シリーズ 2 デバイスおよび DC 500 防御センターはセキュリティ インテリジェンスもサポートしていないため、イベントのセキュリティ インテリジェンス カテゴリによる相関ルールのトリガーをサポートしません。
- 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相関ルールをトリガーとして使用する場合は、[a traffic profile changes] を選択します。

ステップ 2　ルールの条件を指定します。

相関ルール 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」（P.39-36）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」（P.39-8）
- 「マルウェア イベントの構文」（P.39-10）
- 「ディスカバリ イベントの構文」（P.39-11）
- 「ユーザ アクティビティ イベントの構文」（P.39-14）
- 「ホスト入力イベントの構文」（P.39-14）
- 「接続イベントの構文」（P.39-15）
- 「トラフィック プロファイル変化の構文」（P.39-17）

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 [rule “MyDoom Worm” is true] および [rule “Kazaa (TCP) P2P” is true] を含めることができます。

ステップ 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」（P.39-19）
- 「経時的な接続データを使用した相関ルールの制約」（P.39-23）
- 「ユーザ限定の追加」（P.39-33）
- 「スヌーズ期間および非アクティブ期間の追加」（P.39-35）

相関ルールの作成が終了した場合は、「相関ポリシーのルールの作成」（P.39-3）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相関ルールの条件を作成します。

表 39-2　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
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。
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。
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。
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。
Classification	1 つ以上の分類を選択します。
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。
Client Category	クライアントのカテゴリを 1 つ以上選択します。
Destination IP、Source IP、または Source/Destination IP	単一の IP アドレス、アドレス ブロック、またはこれらを任意に組み合わせたカンマ区切りのリストを指定します。FireSIGHT システムで使用する IP アドレス表記およびプレフィクス長については、「IP アドレスの表記法」（P.1-19）を参照してください。 なお、条件の演算子として [is in] または [is not in] を選択した場合、カンマ区切りリストを入力することはできません。
Destination Port/ICMP Code または 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。
Egress Interface または Ingress Interface	インターフェイスを 1 つ以上選択します。
Egress Security Zone または Ingress Security Zone	セキュリティ ゾーンを 1 つ以上選択します。
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、「侵入ポリシーの詳細設定の使用」（P.22-1）を参照してください。

表 39-2　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
Impact Flag	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。 • 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） (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。 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」（P.18-37）を参照してください。
Inline Result	次のいずれかを選択します。 • **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。 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。詳細については、「ルール状態の設定」（P.21-22）、「インライン展開での破棄動作の設定」（P.20-15）、「パッシブ インターフェイスの設定」（P.7-1）、および「タップ モード」（P.7-8）を参照してください。
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 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。
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。
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 にリストされています。
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。
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。

表 39-2　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
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。詳細については、「既存のルールの変更」（P.32-110）を参照してください。
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	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 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 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：任意、またはMalware

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

マルウェア イベントに基づく相関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 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対策をサポートしていません。したがって、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 データおよび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 イベントによる相関ルール トリガーをサポートしないことに注意してください。

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相関ルールの条件を作成します。

表 39-3　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
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。
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。
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。
Client Category	クライアントのカテゴリを 1 つ以上選択します。
Destination IP、Host IP、または 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 アドレスの表記法」（P.1-19）を参照してください。
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。
Disposition	`Malware` または `Custom Detection`、あるいはその両方を選択します。

表 39-3　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
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」（P.34-23）を参照してください。
File Name	ファイルの名前を入力します。
File Type	ファイルのタイプを選択します（たとえば PDF、MSEXE など）。
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 Tag	マルウェア イベントの結果として IOC タブ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。
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 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 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 イベントに基づく相関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」（P.38-10）を参照してください。

表 39-4　相関ルール トリガー基準と ディスカバリ 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
a client has changed	クライアント更新
a client timed out	クライアント タイムアウト
a host IP address is reused	DHCP：IP アドレスの再割り当て
a host is deleted because the host limit was reached	ホスト削除：ホスト制限に到達
a host is identified as a network device	ネットワーク デバイスへのホスト タイプの変更
a host timed out	ホスト タイムアウト
a host's IP address has changed	DHCP：IP アドレスの変更
a NETBIOS name change is detected	NetBIOS 名の変更
a new client is detected	新しいクライアント
a new IP host is detected	新しいホスト
a new MAC address is detected	ホストの追加 MAC の検出
a new MAC host is detected	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

表 39-4　相関ルール トリガー基準と ディスカバリ イベント タイプ （続き）

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
a new transport protocol is detected	新しいトランスポート プロトコル
a TCP port closed	TCP ポート クローズ
a TCP port timed out	TCPポート タイムアウト
a UDP port closed	UDP ポート クローズ
a UDP port timed out	UDP ポート タイムアウト
a VLAN tag was updated	VLAN タグ情報の更新
an IOC was set	侵害の兆候
an open TCP port is detected	新しい TCPポート
an open UDP port is detected	新しい UDP ポート
the OS information for a host has changed	新しい OS
the OS or server identity for a host has a conflict	アイデンティティ競合
the OS or server identity for a host has timed out	アイデンティティ タイムアウト
there is any kind of event	（任意のイベント タイプ）
there is new information about a MAC address	MAC 情報の変更
there is new information about a TCP server	TCP サーバ情報の更新
there is new information about a UDP server	UDP サーバ情報の更新

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、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、[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相関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相関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 39-5　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
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。
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。
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。
Client	クライアントを 1 つ以上選択します。
Client Category	クライアントのカテゴリを 1 つ以上選択します。
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。

表 39-5　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
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。
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 Address または 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 アドレスの表記法」（P.1-19）を参照してください。
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 [Yes] を、そうでない場合は [No] を選択します。
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 [begins with] を選択し、値として `0A:12:34` を入力できます。
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 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 [Yes] を、そうでない場合は [No] を選択します。
NETBIOS Name	ホストの NetBIOS 名を入力します。
Network Protocol	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 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 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 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。
Protocol または 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 にリストされています。
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）。
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	イベントに関連しているホストの VLAN ID を入力します。
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相関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相関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相関ルールでは、IP アドレスを指定できません。

表 39-6　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 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 アドレスの表記法」（P.1-19）を参照してください。
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相関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」（P.38-15）を参照してください。

表 39-7　相関ルール トリガー基準と 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
a client is added	クライアントの追加
a client is deleted	クライアントの削除
a host is added	ホストの追加
a protocol is added	プロトコルの追加
a protocol is deleted	プロトコルの削除
a scan result is added	スキャン結果の追加
a server definition is set	サーバ定義の設定
a server is added	ポートの追加
a server is deleted	ポートの削除
a vulnerability is marked invalid	脆弱性を無効に設定
a vulnerability is marked valid	脆弱性を有効に設定
an address is deleted	ホスト/ネットワークの削除

表 39-7　相関ルール トリガー基準と ホスト入力イベント タイプ（続き）

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
an attribute value is deleted	ホスト属性値の削除
an attribute value is set	ホスト属性値の設定
an OS definition is set	オペレーティング システム定義の設定
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。

ホスト入力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相関ルールの条件を作成できます。選択したホスト入力イベント 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 39-8　ホスト入力イベントの構文

指定する項目	演算子を指定した後に行う操作
IP 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 アドレスの表記法」（P.1-19）を参照してください。
Source	ホスト入力データのソースを選択します。
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

接続イベントに基づく相関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、「表 39-9接続イベントの構文」（P.39-16）で説明されているように相関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。詳細については、「接続およびセキュリティ インテリジェンスのイベントで利用可能な情報」（P.16-11）を参照してください。

表 39-9　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
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。
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 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、[Monitor] を選択します。
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 ルールの名前を入力できます。
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。
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。
Client	クライアントを 1 つ以上選択します。
Client Category	クライアントのカテゴリを 1 つ以上選択します。
Client Version	クライアントのバージョン番号を入力します。
Connection Duration	接続イベントの期間（秒数）を入力します。
Connection Type	シスコ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基づいて相関ルールをトリガーとして使用するのか（**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相関ルールをトリガーとして使用するのか（**NetFlow**）を選択します。
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。
Egress Interface または Ingress Interface	インターフェイスを 1 つ以上選択します。
Egress Security Zone または Ingress Security Zone	セキュリティ ゾーンを 1 つ以上選択します。
Initiator Bytes、Responder Bytes、または Total Bytes	以下のいずれかを入力します。 • 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]）
Initiator IP、Responder IP、または Initiator/Responder IP	単一の IP アドレス、アドレス ブロック、またはこれらを任意に組み合わせたカンマ区切りのリストを指定します。FireSIGHT システムで使用する IP アドレス表記およびプレフィクス長については、「IP アドレスの表記法」（P.1-19）を参照してください。

表 39-9　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
Initiator Packets、Responder Packets、または Total Packets	以下のいずれかを入力します。 • 送信されたパケット数（[Initiator Packets]） • 受信されたパケット数（[Initiator Packets]） • 送受信されたパケット数（[Total Packets]）
Initiator Port/ICMP Type または 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 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 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 Device	相関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 Device] ドロップダウン リストは空白になります。
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。
TCP Flags	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。 **（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。
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 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。
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。
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 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 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

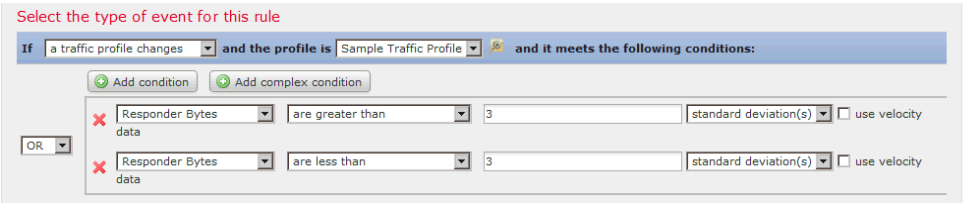
ライセンス：任意

トラフィック プロファイル変化に基づく相関ルールの場合、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」（P.40-1）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、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**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。

- 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

[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」（P.16-17）を参照）、データ ポイント間の速度変化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。NetFlow 対応デバイスから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」（P.35-20）を参照して、トラフィック プロファイル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 39-10　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
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）	connections：接続数 standard deviation(s)：標準偏差の数
Total Bytes、Initiator Bytes、または Responder Bytes	次のいずれかを入力します。 • 送信された合計バイト数（[Total Bytes]） • イニシエータから送信されたバイト数（[Initiator Bytes]） • レスポンダで受信されたバイト数（[Responder Bytes]） **または** 平均より上または下の標準偏差の数（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）	bytes：バイト数 standard deviation(s)：標準偏差の数

表 39-10　トラフィック プロファイル変化の構文（続き）

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
Total Packets、Initiator Packets、または Responder Packets	次のいずれかを入力します。 • 送信された合計パケット数（[Total Packets]） • イニシエータから送信されたパケット数（[Initiator Packets]） • レスポンダで受信されたパケット数（[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
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）	initiators：イニシエータ数 standard deviation(s)：標準偏差の数
Unique Responders	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）	responders：レスポンダ数 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、ディスカバリ、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相関ルールに、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相関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相関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ー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。接続のイニシエータ（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ー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、[Application Protocol] を [HTTPS] に設定した**レスポンダ 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、レスポンダ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相関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

ステップ 1　[Policies] > [Correlation] を選択し、[Rule Management] タブを選択します。

[Rule Management] ページが表示されます。

ステップ 2　[Create Rule] をクリックします。

[Create Rule] ページが表示されます。

ステップ 3　[Create Rule] ページで、[Add Host Profile Qualification] をクリックします。

[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、[Remove Host Profile Qualification] をクリックします。

ステップ 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」（P.39-36）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」（P.39-21）で説明しています。

ステップ 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相関ルールの制約」（P.39-23）
- 「ユーザ限定の追加」（P.39-33）
- 「スヌーズ期間および非アクティブ期間の追加」（P.39-35）

相関ルールの作成が終了した場合は、「相関ポリシーのルールの作成」（P.39-3）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、相関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 [Responder Host] または開始側を示す [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 [Destination Host] または送信元を示す [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、[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ダ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。システムが NetFlow レコードを処理するときには、各ホストが使用しているポート、およびそれらのポートが既知であるかどうかに基づき、アルゴリズムに従ってその情報が判別されます。詳細については、「NetFlow と FireSIGHT データの違い」（P.35-20）を参照してください。

表 39-11　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
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 Name	ホストの NetBIOS 名を入力します。
Operating System > 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。
Operating System > 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。
Operating System > 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。
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 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」（P.35-23）を参照してください。
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 [Yes] を、そうでない場合は [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 [Yes] を、そうでない場合は [No] を選択します。
Network Protocol	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。

表 39-11　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
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。
Host Criticality	ホストの重要度（**None**、**Low**、**Medium**、または **High**）を選択します。ホストの重要度の詳細については、「事前定義のホスト属性の使用」（P.37-35）を参照してください。
VLAN ID	ホストに関連付けられた VLAN ID を入力します。
Application Protocol > 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。
Application Protocol > 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相関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（[Destination Host] の場合は `dst_port`、[Source Host] の場合は `src_port`）。
Application Protocol > Protocol	プロトコルを 1 つ以上選択します。
Application Protocol Category	カテゴリを 1 つ選択します。
Client > Client	クライアントを 1 つ以上選択します。
Client > Client Version	クライアントのバージョンを入力します。
Client Category	カテゴリを 1 つ選択します。
Web Application	Web アプリケーションを選択します。
Web Application Category	カテゴリを 1 つ選択します。
MAC Address > 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 で始まることがわかっている場合、演算子として [begins with] を選択し、値として `0A:12:34` を入力できます。
MAC Address > 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 Vendor > 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）	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。 • 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。 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」（P.37-35）を参照してください。

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、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相関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相関ルールの制約

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、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、防御センターがルールの相関イベントを生成します。

接続、侵入、ディスカバリ、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相関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」（P.40-1）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追跡を停止します。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。

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、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。

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」（P.39-24）
- 「接続トラッカーの構文」（P.39-25）
- 「接続トラッカー イベントの構文」（P.39-28）
- 「例：外部ホストからの過剰な接続数」（P.39-28）
- 「例：過剰な BitTorrent データの転送」（P.39-30）

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、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、防御センターがルールの相関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
- 防御センターに相関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（相関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相関ルールに、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

ステップ 1　[Create Rule]ページで、[Add Connection Tracker] をクリックします。

[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、[Remove Connection Tracker] をクリックします。

ステップ 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」（P.39-36）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」（P.39-25）で説明しています。

ステップ 3　ステップ 2 で追跡対象として指定した接続に応じて、どのようなときに相関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。

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（相関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、「ルールの作成メカニズムについて」（P.39-36）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」（P.39-28）で説明しています。

ステップ 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」（P.39-33）
- 「スヌーズ期間および非アクティブ期間の追加」（P.39-35）

相関ルールの作成が終了した場合は、「相関ポリシーのルールの作成」（P.39-3）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

「接続トラッカーの構文」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。

シスコ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、相関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/レスポンダであるかを示す情報が含まれません。システムが NetFlow レコードを処理するときには、各ホストが使用しているポート、およびそれらのポートが既知であるかどうかに基づき、アルゴリズムに従ってその情報が判別されます。詳細については、「NetFlow と FireSIGHT データの違い」（P.35-20）を参照してください。

表 39-12　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
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。
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 ルールの条件に一致する接続を追跡するには、[Monitor] を選択します。
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 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/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。
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。
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。
Client	クライアントを 1 つ以上選択します。
Client Category	クライアントのカテゴリを 1 つ以上選択します。
Client Version	クライアントのバージョンを入力します。
Connection Duration	接続期間（秒数）を入力します。
Connection Type	シスコ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。
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てください。
Ingress Interface または Egress Interface	インターフェイスを 1 つ以上選択します。
Ingress Security Zone または Egress Security Zone	セキュリティ ゾーンを 1 つ以上選択します。
Initiator IP、Responder IP、または 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 アドレスの表記法」（P.1-19）を参照してください。
Initiator Bytes、Responder Bytes、または Total Bytes	以下のいずれかを入力します。 • イニシエータから送信されたバイト数（[Initiator Bytes]） • レスポンダで受信されたバイト数（[Responder Bytes]） • 送受信されたバイト数（[Total Bytes]）
Initiator Packets、Responder Packets、または Total Packets	以下のいずれかを入力します。 • イニシエータから送信されたパケット数（[Initiator Packets]） • レスポンダで受信されたパケット数（[Responder Packets]） • 送受信されたパケット数（[Total Packets]）

表 39-12　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
Initiator Port/ICMP Type または 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 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 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 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 Device] ドロップダウン リストは空白になります。
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。
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。
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 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 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。
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 Application	Web アプリケーションを 1 つ以上選択します。
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相関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 [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、このような相関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 [Initiator/Responder IP] が [Event IP Address] に設定され、[Client] が [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、[switch to manual entry] をクリックして、手動で IP を指定します。[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

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。

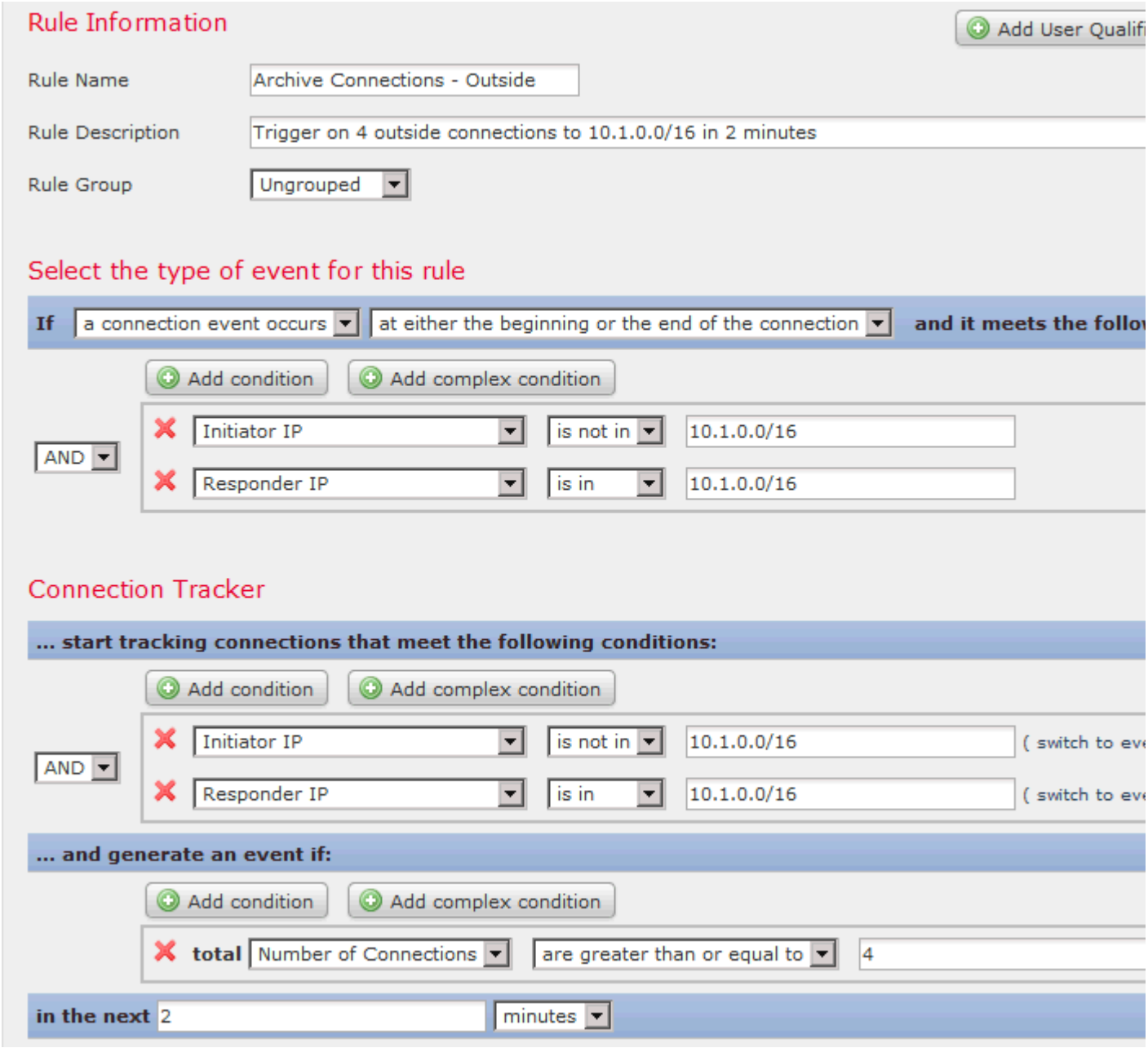
表 39-13　接続トラッカー イベントの構文

指定する項目	演算子を指定した後に行う操作
Number of Connections	検出された接続の合計数を入力します。
Total Bytes、Initiator Bytes、または Responder Bytes	以下のいずれかを入力します。 • 送信された合計バイト数（[Total Bytes]） • イニシエータから送信されたバイト数（[Initiator Bytes]） • レスポンダで受信されたバイト数（[Responder Bytes]）
Total Packets、Initiator Packets、または Responder Packets	以下のいずれかを入力します。 • 送信された合計パケット数（[Total Packets]） • イニシエータから送信されたパケット数（[Initiator Packets]） • レスポンダで受信されたパケット数（[Responder Packets]）
Unique Initiators または Unique Responders	以下のいずれかを入力します。 • 検出されたセッションを開始した個別のホストの数（[Unique Initiators]） • 検出された接続に応答した個別のホストの数（[Unique Responders]）

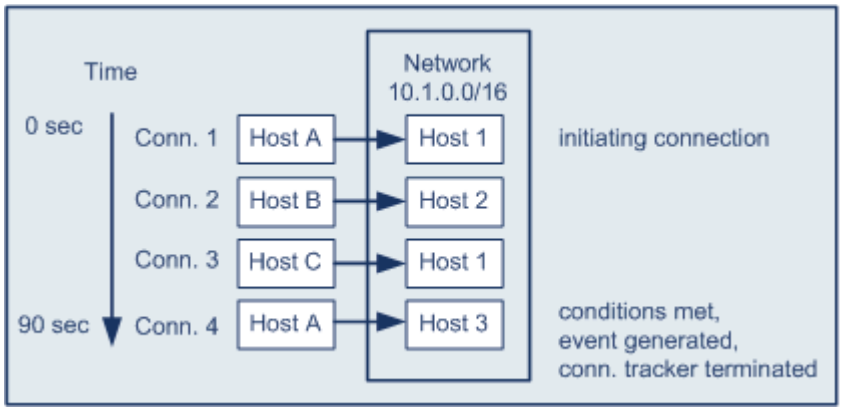
例：外部ホストからの過剰な接続数

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が、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 Qualifi
Rule Name
Archive Connections - Outside
Rule Description
Trigger on 4 outside connections to 10.1.0.0/16 in 2 minutes
Rule Group
Ungrouped
Select the type of event for this rule
If
a connection event occurs
at either the beginning or the end of the connection
and it meets the follo
Add condition
Add complex condition
AND
Initiator IP
is not in
10.1.0.0/16
Responder IP
is in
10.1.0.0/16
Connection Tracker
... start tracking connections that meet the following conditions:
Add condition
Add complex condition
AND
Initiator IP
is not in
10.1.0.0/16
(switch to eve
Responder IP
is in
10.1.0.0/16
(switch to eve
... and generate an event if:
Add condition
Add complex condition
total
Number of Connections
are greater than or equal to
4
in the next
2
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。



この例では、相関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。

ステップ 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。

ステップ 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）。

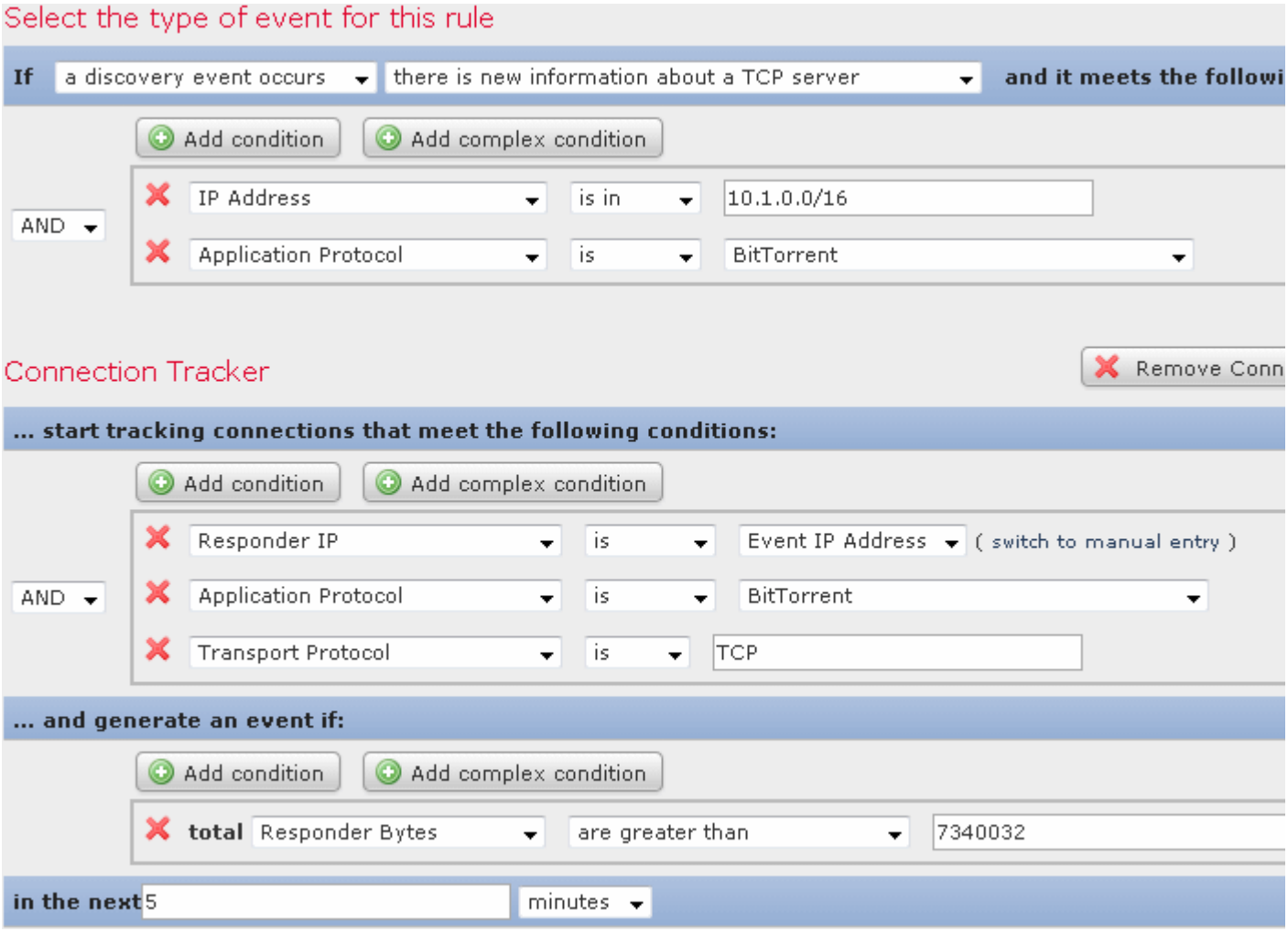
ステップ 3　2 分の制限時間内にホスト A がホスト 3 に接続すると、システムは 4 番目の該当する接続を検出します。これで、ルールの条件が満たされました。

ステップ 4　防御センターが相関イベントを生成し、システムは接続の追跡を停止します。

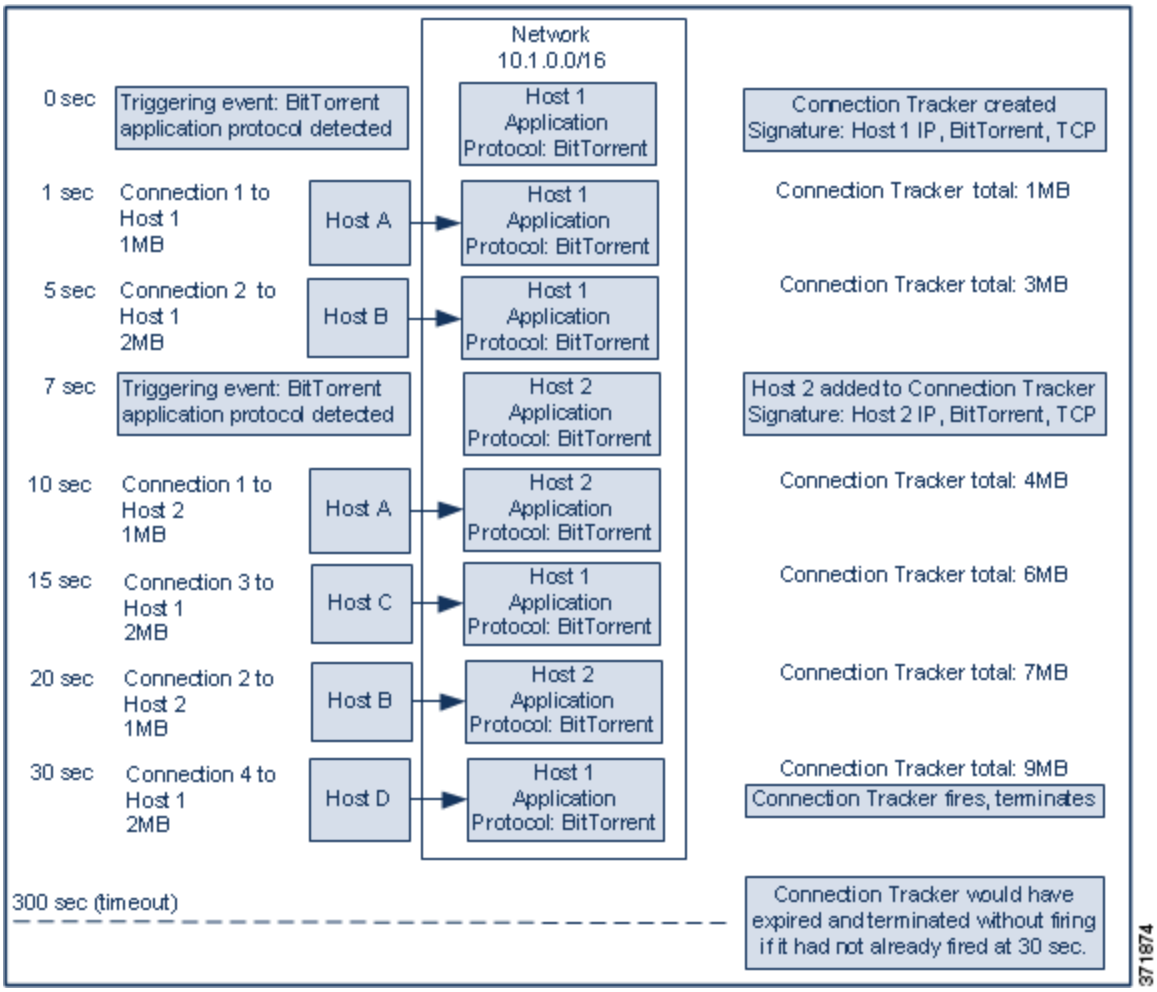
例：過剰な BitTorrent データの転送

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、相関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相関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
a discovery event occurs
there is new information about a TCP server
and it meets the followi
Add condition
Add complex condition
AND
IP Address
is in
10.1.0.0/16
Application Protocol
is
BitTorrent
Connection Tracker
Remove Conn
... start tracking connections that meet the following conditions:
Add condition
Add complex condition
AND
Responder IP
is
Event IP Address
(switch to manual entry)
Application Protocol
is
BitTorrent
Transport Protocol
is
TCP
... and generate an event if:
Add condition
Add complex condition
total
Responder Bytes
are greater than
7340032
in the next
5
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。

ステップ 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、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。

ステップ 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）
- 2 秒マーカーの時点で、ホスト 1 からホスト B に 2MB（合計 3MB）

ステップ 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。

ステップ 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、防御センターは相関イベントを生成しません。

ステップ 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。

ステップ 6　防御センターが相関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、相関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。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**。

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。

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

ステップ 1　[Create Rule] ページで、ユーザ限定の追加を示す [Add User Qualification] をクリックします。

[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、[Remove User Qualification] をクリックします。

ステップ 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」（P.39-36）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」（P.39-34）で説明しています。

ステップ 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」（P.39-35）に進みます。

相関ルールの作成が終了した場合は、「相関ポリシーのルールの作成」（P.39-3）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、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、[Identity on Initiator] または [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 [Identity on Destination] または送信元を示す [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、[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、[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（「防御センターとの LDAP 接続の構築」（P.35-44）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 39-14　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
Username	相関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。
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。
First Name	相関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。
Last Name	相関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。
Department	相関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。
Phone	相関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。
Email	相関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

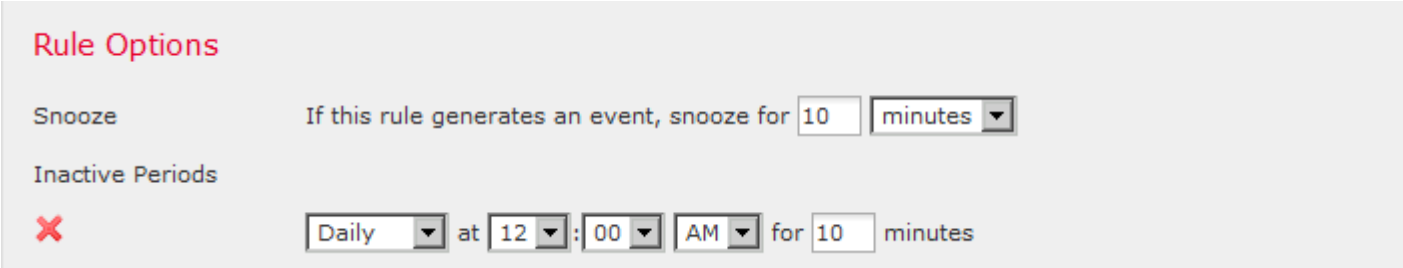
ライセンス：任意

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、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、防御センター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。

以下の図は、相関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。



スヌーズ期間を追加する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Create Profile]ページの [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　スム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

ステップ 1　[Create Profile]ページの [Rule Options] で、[Add Inactive Period] をクリックします。

ステップ 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、相関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、「相関ポリシーのルールの作成」（P.39-3）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。

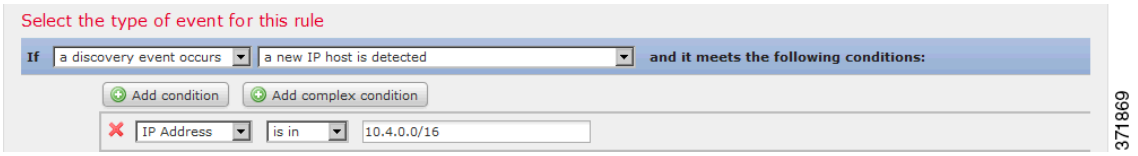
ルールの作成メカニズムについて

ライセンス：任意

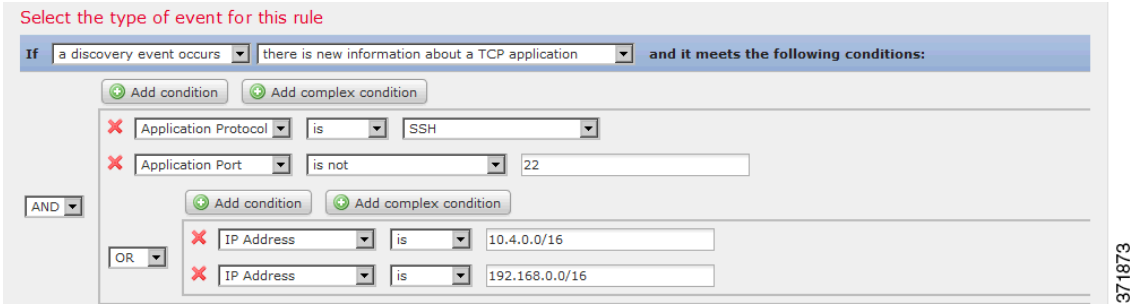
相関ルール、接続トラッカー、ユーザ限定、およびホスト プロファイル限定を作成するときには、それぞれをトリガーとして使用する条件を指定します。単純な条件を作成することも、複数の条件の組み合わせやネストを使って複雑な構造を作成することもできます。

たとえば、新しいホストが検出されるたびに相関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。



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相関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。

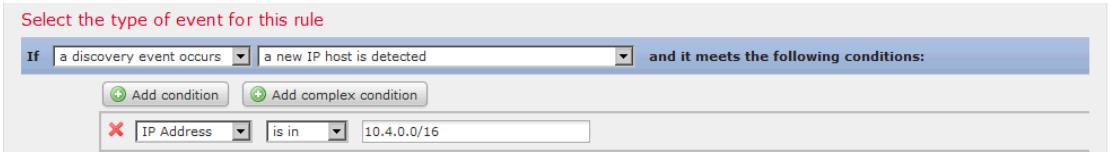
- 「単一の条件の作成」（P.39-37）
- 「条件の追加と結合」（P.39-39）
- 「複数の値を条件で使用する」（P.39-42）

単一の条件の作成

ライセンス：任意

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、以下の相関ルールは、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 Address]、演算子は [is in]、値は `10.4.0.0/16` です。



上記の例の相関ルール トリガー基準を作成する方法：

アクセス：Admin/Discovery Admin

ステップ 1　相関ルールの作成を開始します。

詳細については、「相関ポリシーのルールの作成」（P.39-3）を参照してください。

ステップ 2　[Create Rule] ページの [Select the type of event for this rule] で [a discovery event occurs] を選択した後、ドロップダウン リストから [a new IP host is detected] を選択します。

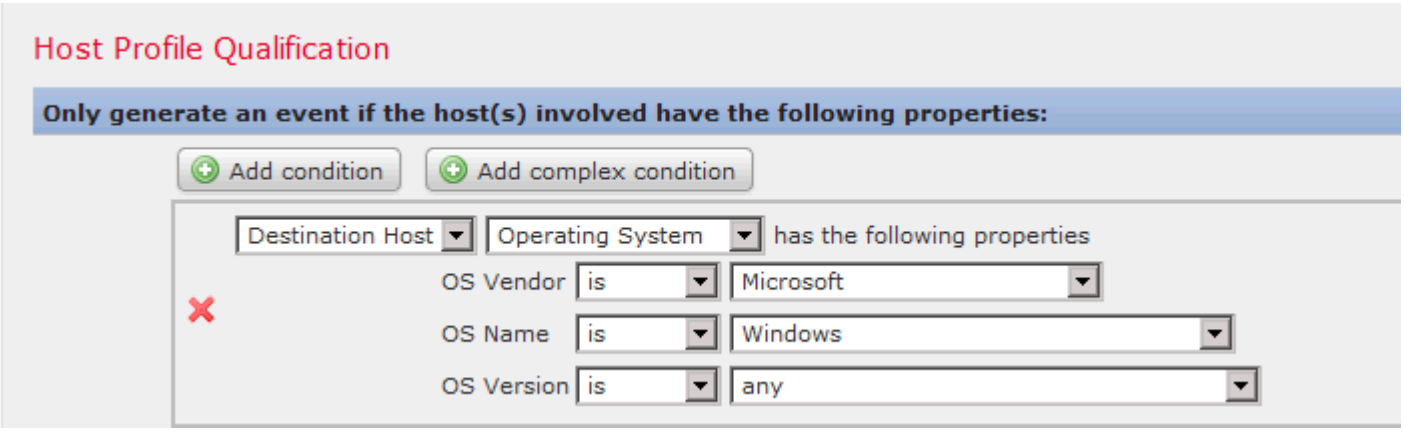
ステップ 3　ルールの単一の条件を作成するには、まず、最初の（つまり *カテゴリ*）ドロップダウン リストから [IP Address] を選択します。

ステップ 4　表示される演算子のドロップダウン リストから、[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 [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。FireSIGHT システムで使用する IP アドレス表記については、「IP アドレスの表記法」（P.1-19）を参照してください。

ステップ 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。これにより相関ルールが制約され、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。



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

ステップ 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」（P.39-3）を参照してください。

ステップ 2　[Create Rule] ページで、[Add Host Profile Qualification] をクリックします。

[Host Profile Qualification] セクションが表示されます。

ステップ 3　[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、ディスカバリ 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 [Host] のみです。

ステップ 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 [Operating System] カテゴリを選択します。

[OS Vendor]、[OS Name]、[OS Version] の 3 つのサブカテゴリが表示されます。

ステップ 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 [is] を使用します。

ステップ 6　最後に、サブカテゴリの値を指定します。

[OS Vendor] の値には [Microsoft]、[OS Name] の値には [Windows] を選択し、[OS Version] の値は [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」（P.39-42）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」（P.39-8）
- 「マルウェア イベントの構文」（P.39-10）
- 「ディスカバリ イベントの構文」（P.39-11）
- 「ユーザ アクティビティ イベントの構文」（P.39-14）
- 「ホスト入力イベントの構文」（P.39-14）
- 「接続イベントの構文」（P.39-15）
- 「トラフィック プロファイル変化の構文」（P.39-17）

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」（P.39-21）
- 「接続トラッカーの構文」（P.39-25）
- 「接続トラッカー イベントの構文」（P.39-28）
- 「ユーザ限定の構文」（P.39-34）

条件の追加と結合

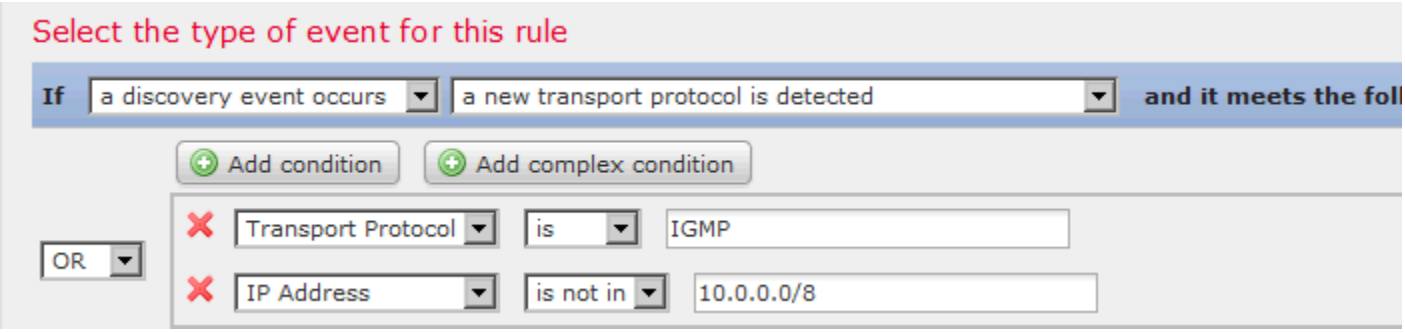
ライセンス：任意

単純な相関ルール 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。

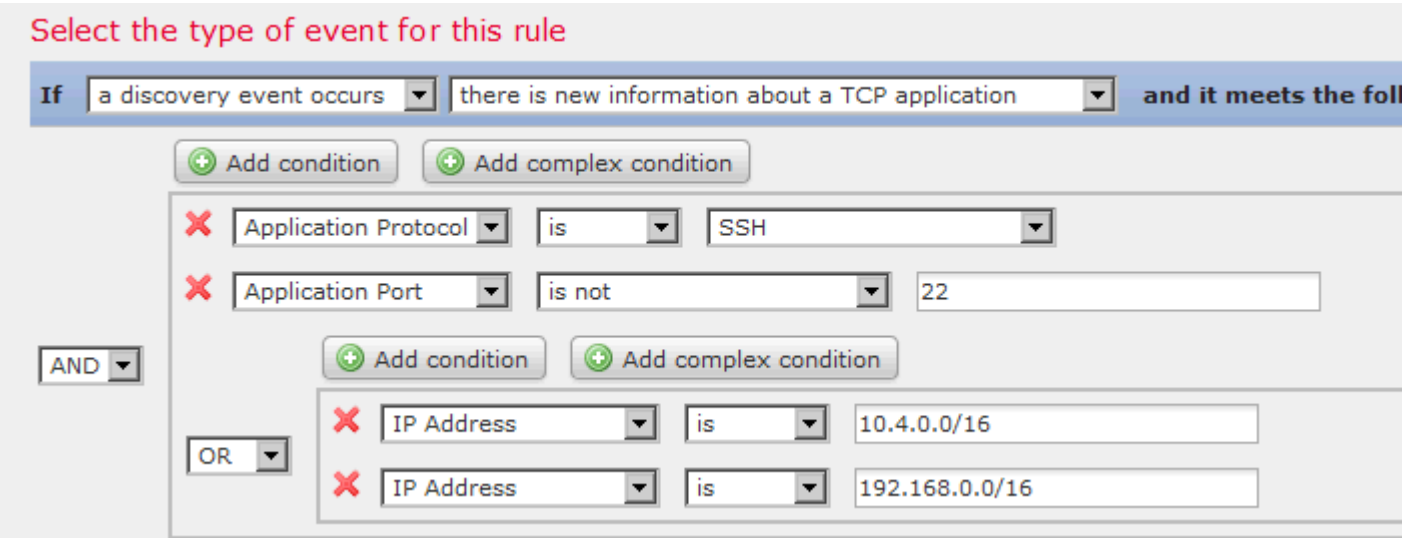
構造に複数の条件を含める場合は、それらの条件を **AND** または **OR** 演算子で結合する必要があります。同じレベルにある複数の条件は、一緒に評価されます。

- **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。

たとえば、以下の相関ルール 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。



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。



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 39-15　ルールの評価

項目	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 196.168.0.0/16 に含まれる

単一の条件を追加する方法：

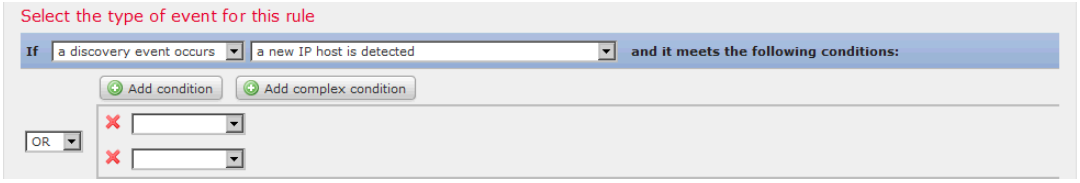
アクセス：Admin/Discovery Admin

ステップ 1　単一の条件を追加するには、現在の条件の上にある [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、

結果は以下のとおりです。



複合条件を追加する方法：

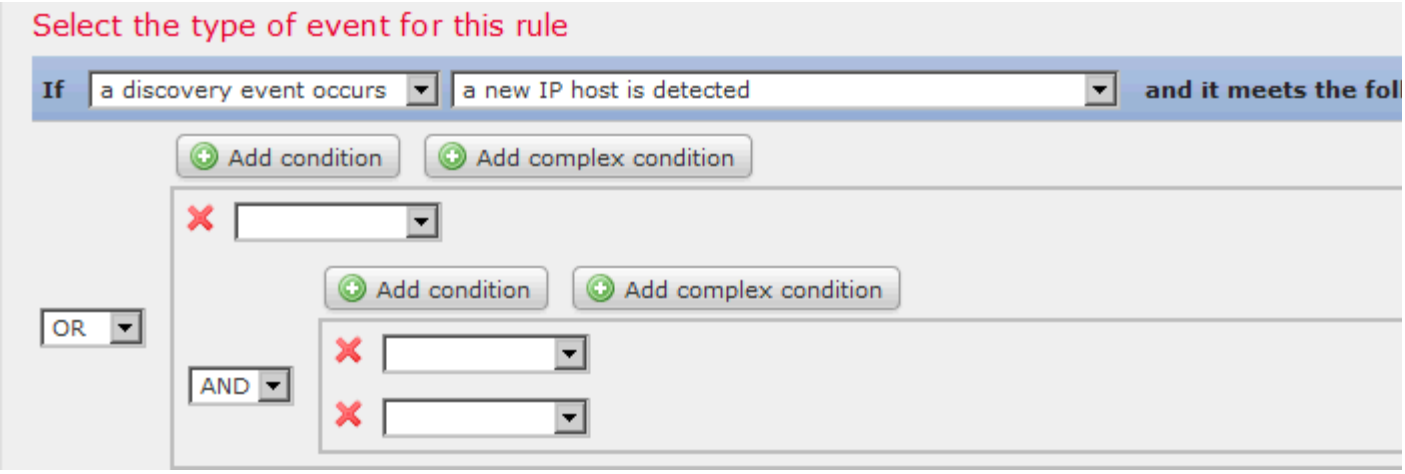
アクセス：Admin/Discovery Admin

ステップ 1　現在の条件の上にある [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、

結果は以下のとおりです。



条件を結合する方法：

アクセス：Admin/Discovery Admin

ステップ 1　条件セットの左側にあるドロップダウン リストを使用します。次のどちらかを選択します。

- **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

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

ステップ 1　演算子として [is in] または [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。

ステップ 2　テキスト フィールド内の任意の場所または [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。

ステップ 3　[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。

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。

[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。

相関ポリシーのルールの管理

ライセンス：任意

相関ポリシー内で使われている相関ルールを管理するには、[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相関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」（P.39-43）
- 「ルールの削除」（P.39-44）
- 「ルール グループの作成」（P.39-44）

ルールの作成の詳細については、「相関ポリシーのルールの作成」（P.39-3）を参照してください。

ルールの変更

ライセンス：任意

既存の相関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

ステップ 1　[Policies] > [Correlation] を選択し、[Rule Management] タブを選択します。

[Rule Management] ページが表示されます。

ステップ 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。

ステップ 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。

[Create Rule] ページが表示されます。

ステップ 4　必要に応じて変更した後、[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

1 つ以上の相関ポリシーで使用している相関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、「相関ポリシーの編集」（P.39-54）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

ステップ 1　[Policies] > [Correlation] を選択し、[Rule Management] タブを選択します。

[Rule Management] ページが表示されます。

ステップ 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。

ステップ 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。

ステップ 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

ルール グループを作成すると、相関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、単に相関ルールを編成しやすくするためです。1 つのルール グループを相関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。

- 「相関ポリシーのルールの作成」（P.39-3）
- 「ルールの変更」（P.39-43）

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

ステップ 1　[Policies] > [Correlation] を選択し、[Rule Management] タブを選択します。

[Rule Management] ページが表示されます。

ステップ 2　[Create Group] をクリックします。

[Create Group] ページが表示されます。

ステップ 3　[Group Name] フィールドにグループの名前を入力します。

ステップ 4　[Add Group] をクリックします。

グループが追加されます。

相関応答のグループ化

ライセンス：任意

アラート応答および修正を作成した後（「アラート応答の使用」（P.15-2）および「修復の作成」（P.41-1）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。応答グループを相関ルールに割り当てるには、その前に、[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。相関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。[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、次の項を参照してください。

- 「応答グループの作成」（P.39-45）
- 「応答グループの変更」（P.39-46）
- 「応答グループの削除」（P.39-47）
- 「応答グループのアクティブ化と非アクティブ化」（P.39-47）

応答グループの作成

ライセンス：任意

個々のアラートと修正を応答グループに含めた後、それを相関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：Admin

ステップ 1　[Policies] > [Correlation] を選択し、[Groups] をクリックします。

[Groups] ページが表示されます。

ステップ 2　[Create Group] をクリックします。

[Response Group] ページが表示されます。

ステップ 3　[Name] フィールドに、新しいグループの名前を入力します。

ステップ 4　[Active] を選択するとグループがアクティブになり、相関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。

ステップ 5　[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。

ステップ 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、[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。

ステップ 7　[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

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：Admin

ステップ 1　[Policies] > [Correlation] を選択し、[Groups] をクリックします。

[Groups] ページが表示されます。

ステップ 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。

[Response Group] ページが表示されます。

ステップ 3　必要に応じて変更を行い、[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

相関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：Admin

ステップ 1　[Policies] > [Correlation] を選択し、[Groups] をクリックします。

[Groups] ページが表示されます。

ステップ 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。

ステップ 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

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、相関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：Admin

ステップ 1　[Policies] > [Correlation] を選択し、[Groups] をクリックします。

[Groups] ページが表示されます。

ステップ 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。

相関ポリシーの作成

ライセンス：任意

相関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、それらを使用して相関ポリシーを作成できます。

アクティブ ポリシー内の相関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、防御センターは相関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。

相関ポリシーを作成するために使用できる相関ルール、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。

- 「相関ポリシーのルールの作成」（P.39-3）
- 「コンプライアンス ホワイト リストの作成」（P.27-9）
- 「外部アラートの設定」（P.15-1）
- 「修復の設定」（P.41-1）

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。

相関ポリシーを作成する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Correlation] を選択します。

[Policy Management] ページが表示されます。

ステップ 2　[Create Policy] をクリックします。

[Create Policy] ページが表示されます。

ステップ 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」（P.39-49）を参照してください。

ステップ 4　相関ポリシーに 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相関ポリシーに追加する」（P.39-49）を参照してください。

ステップ 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」（P.39-50）を参照してください。

ステップ 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」（P.39-51）を参照してください。

ステップ 7　[Save] をクリックします。

ポリシーが保存されます。

注　ポリシーで相関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、「相関ポリシーの管理」（P.39-52）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

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。相関ポリシーに対する違反の結果として生成される相関イベントには、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相関ポリシーに追加する」（P.39-49）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

ステップ 1　[Create Policy] ページで、[Policy Name] フィールドにポリシーの名前を入力します。

ステップ 2　[Policy Description] フィールドに、ポリシーの説明を入力します。

ステップ 3　[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、[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。

ステップ 4　次の項（「ルールとホワイトリストを相関ポリシーに追加する」（P.39-49））の手順に進みます。

ルールとホワイトリストを相関ポリシーに追加する

ライセンス：任意

1 つの相関ポリシーには、1 つ以上の相関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相関ルールからなる、さまざまな応答が設定された相関ポリシーを示しています。

ルールまたはホワイトリストを相関ポリシーに追加する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Create Policy] ページで、[Add Rules] をクリックします。

[Available Rules] ポップアップが表示されます。

ステップ 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。

ステップ 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、[Add] をクリックします。

[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。

ステップ 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」（P.39-50））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

相関ポリシーに含まれる個々の相関ルールやコンプライアンス ホワイトリストに、ユーザー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、結果としてできる相関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

ステップ 1　[Create Policy] ページで、ルールまたはホワイトリストごとの [Priority] リストから、デフォルト プライオリティを選択します。次のオプションを選択できます。

- 1 から 5 までのプライオリティ値（1 が最高、5 が最低）
- **None**
- **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 2　次の項（「ルールとホワイトリストに応答を追加する」（P.39-51））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

相関ポリシー内で、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」（P.15-1）
- 「修復の設定」（P.41-1）
- 「相関応答のグループ化」（P.39-45）

注　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相関ルールへの応答として、Nmap 修正を**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相関ルールからなる、さまざまな応答が設定された相関ポリシーを示しています。

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

ステップ 1　[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。

ステップ 2　[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。

ステップ 3　[Update] をクリックします。

[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。

相関ポリシーの管理

ライセンス：任意

相関ポリシーの管理は、[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。ポリシーで相関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。[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。

アクティブな相関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、相関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相関ポリシーに追加する必要があります（相関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」（P.27-1）を参照してください。

相関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。

- 「相関ポリシーのアクティブ化と非アクティブ化」（P.39-53）
- 「相関ポリシーの編集」（P.39-54）
- 「相関ポリシーの削除」（P.39-54）

新しいポリシーを作成する方法については、「相関ポリシーの作成」（P.39-48）を参照してください。

相関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

相関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

ステップ 1　[Policies] > [Correlation] を選択します。

[Policy Management] ページが表示されます。

ステップ 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。

相関ポリシーの編集

ライセンス：任意

相関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方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Correlation] を選択します。

[Policy Management] ページが表示されます。

ステップ 2　ポリシーの横にある編集アイコン（  ）をクリックします。

[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、「相関ポリシーの作成」（P.39-48）を参照してください。相関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、[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。

ステップ 3　必要に応じて変更を行い、[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。

相関ポリシーの削除

ライセンス：任意

相関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

ステップ 1　[Policies] > [Correlation] を選択します。

[Policy Management] ページが表示されます。

ステップ 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。

相関イベントの操作

ライセンス：任意

アクティブな相関ポリシーに含まれる相関ルールがトリガーとして使用されると、防御センターが相関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相関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」（P.50-15）を参照してください。

注　アクティブな相関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」（P.27-33）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。

- 「相関イベントの表示」（P.39-55）
- 「相関イベント テーブルについて」（P.39-57）
- 「相関イベントの検索」（P.39-58）

相関イベントの表示

ライセンス：任意

相関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。

相関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。相関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、特定の要件に一致する情報のみ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については、「カスタム ワークフローの作成」（P.47-45）を参照してください。

次の表では、相関イベント 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 39-16　相関イベントの操作

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 アイデンティティの横に表示されるユーザ 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」（P.38-65）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」（P.47-39）にある詳細情報を参照してください。
現在のワークフロー ページ内を移動する	「ワークフロー内の他のページへのナビゲート」（P.47-40）にある詳細情報を参照してください。
現在の制約を保持しながら、現在のワークフローのページ間を移動する	ワークフロー ページの左上にある、該当するページの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」（P.47-21）を参照してください。
表示されるカラムの詳細を調べる	「相関イベント テーブルについて」（P.39-57）にある詳細情報を参照してください。
表示するイベントの日時範囲を変更する	「イベント時間の制約の設定」（P.47-27）にある詳細情報を参照してください。 イベント ビューを時間で制約した場合、イベント ビューには（グローバルかイベント固有かにかかわらず）アプライアンスで設定されている時間枠の外で生成されたイベントが表示される場合があることに注意してください。アプライアンスでスライド時間枠を設定した場合でも、これが発生する可能性があります。

表 39-16　相関イベントの操作（続き）

目的	操作
特定の値に制約して、ワークフロー内の次のページにドリルダウンする	次のいずれかの方法を使用します。 • カスタム ワークフローに作成したドリルダウン ページで、行内の値を 1 つクリックします。テーブル ビューの行内の値をクリックすると、テーブル ビューが制約されることに注意してください（次のページにはドリルダウン**されません**）。 • 一部のユーザに制約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 ページに表示させるユーザの横のチェック ボックスを選択し、[View] をクリックします。 • 現在の制約を保持しながら、次のワークフロー ページにドリルダウンするには、[View All] をクリックします。 **ヒント**　テーブル ビューのページ名には必ず「Table View」が含まれます。 詳細については、「イベントの制約」（P.47-36）を参照してください。
システムから相関イベントを削除する	次のいずれかの方法を使用します。 • いくつか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 ボックスを選択し、[Delete] をクリックします。 • 現在の制約付きビューにあるすべてのイベントを削除するには、[Delete All] をクリックした後、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するイベント表示する	「ワークフロー間のナビゲート」（P.47-41）にある詳細情報を参照してください。

相関イベントを表示する方法：

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Correlation] > [Correlation Events] を選択します。

デフォルト相関イベント 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 タイトルの近くの [(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」（P.58-3）を参照してください。イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください（「イベント時間の制約の設定」（P.47-27）を参照）。

ヒント　相関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、[(switch workflow)] をクリックし、[Correlation Events] を選択します。

相関イベント テーブルについて

ライセンス：任意

相関ルールがトリガーとして使用されると、防御センターは相関イベントを生成します。相関イベント 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 39-17　相関イベントのフィールド

フィールド	説明
Time	相関イベントが生成された日時。
Impact	侵入データ、ディスカバリ データ、および脆弱性情報の間の相関に基づいて相関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」（P.18-37）を参照してください。
Inline Result	次のいずれか： • 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 [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 [Drop and Generate Events] に設定されていなかったことを示すます 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。詳細については、「ルール状態の設定」（P.21-22）、「インライン展開での破棄動作の設定」（P.20-15）、「パッシブ インターフェイスの設定」（P.7-1）、および「タップ モード」（P.7-8）を参照してください。
Source IP または 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。
Source User または 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。
Source Port/ICMP Type または 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。
Description	相関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。 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。
Policy	違反が発生したポリシーの名前。
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。
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。

表 39-17　相関イベントのフィールド（続き）

フィールド	説明
Source Host Criticality または 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。ホストの重要度の詳細については、「事前定義のホスト属性の使用」（P.37-35）を参照してください。
Ingress Security Zone または 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。
Ingress Interface または 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。
Count	各行に表示された情報に一致するイベントの数。[Count] フィールドは、制約を適用した後に 2 つ以上の同一行が生じた場合に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」（P.39-55）
- 「相関イベントの検索」（P.39-58）

相関イベントの検索

ライセンス：任意

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。以下の表に、使用できる検索基準を示します。

表 39-18　相関イベントの検索基準

フィールド	検索基準の規則
Policy	検索する相関ポリシーの名前を入力します。
Rule	検索する相関ルールの名前を入力します。
Description	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。
Priority	相関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相関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。相関ルールとポリシーのプライオリティを設定する方法については、「ポリシーの基本情報の指定」（P.39-49）および「ルールおよびホワイトリストのプライオリティの設定」（P.39-50）を参照してください。
Source IP、Destination IP、または Source/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コ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」（P.45-6）を参照してください。

表 39-18　相関イベントの検索基準（続き）

フィールド	検索基準の規則
Source User または 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を指定します。
Source Port/ICMP Type または 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 コードを指定します。
Impact	相関イベントに割り当てられた影響フラグを指定します。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（大文字/小文字は区別されません）。影響アイコンの色や部分文字列（たとえば `blue`、`level 1`、`0` など）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」（P.18-37）を参照してください。
Inline Result	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。 • 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。 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。詳細については、「ルール状態の設定」（P.21-22）、「インライン展開での破棄動作の設定」（P.20-15）、「タップ モード」（P.7-8）を参照してください。
Source Host Criticality または Destination Host Criticality	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。ホストの重要度の詳細については、「事前定義のホスト属性の使用」（P.37-35）を参照してください。
Ingress Security Zone、Egress Security Zone、または Ingress/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、出力、または入力/出力セキュリティ ゾーンを指定します。
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、グループ名、または IP アドレスを入力します。「デバイスの管理」（P.6-1）、「割り当てられたデバイス名の編集」（P.6-47）、および「デバイス グループの管理」（P.6-24）を参照してください。
Ingress Interface または 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を指定します。

相関イベントを検索する方法：

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　[Table] ドロップダウン リストから、[Correlation Events] を選択します。

ページが適切な制約を使用してリロードされます。

ステップ 3　オプションで、検索を保存するには、[Name] フィールドに検索の名前を入力します。

名前を入力しない場合、検索の保存時に自動的に名前が作成されます。

ステップ 4　「相関イベントの検索基準」の表に示すように、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カンマ区切りの列挙を使用できます。複数の条件を入力すると、すべての基準を満たすレコードのみが検索で返されます。
- 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（*）を使用できます。
- 任意のフィールドで `n/a` を指定すると、そのフィールドの情報がないイベントを識別できます。一方、フィールドに情報があるイベントを識別すには `!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あるオブジェクト追加アイコン（  ）をクリックします。

検索でのオブジェクトの使用を含む、検索の構文の詳細については、「イベントの検索」（P.45-1）を参照してください。

ステップ 5　他のユーザが再使用できるような形式で検索を保存する場合には、[Save As Private] チェックボックスをクリアします。そうでない場合は、このチェック ボックスを選択したままにして、検索をプライベートとして保存します。

カスタム ユーザ ロールに関するデータ制約として検索を使用する予定の場合は、それをプライベート検索として保存する**必要があります**。

ステップ 6　次の選択肢があります。

- 検索を開始するには、[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相関イベント 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 タイトルの近くの [(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」（P.58-3）を参照してください。
- 既存の検索を変更している場合、[Save] をクリックすると変更内容が保存されます。
- [Save as New Search] をクリックすると、検索条件が保存されます。検索が保存され（[Save As Private] を選択した場合はユーザ アカウントに関連付けられて保存され）、あとでそれを使用できます。