CHAPTER 53

トラフィック プロファイルの作成

トラフィック プロファイルは、指定した期間にわたって収集された接続データに基づく、ネットワーク上のトラフィックに関する単なるプロファイルです。デバイスによって収集された接続データ、いずれか（またはすべて）の 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、またはその両方を使用できます。

トラフィック プロファイルを作成した後、正常なネットワーク トラフィックを表すと想定されるプロファイルに照らして新しいトラフィックを評価することにより、異常なネットワーク トラフィックを検出できます。

FireSIGHT システムは接続データを使用して、トラフィック プロファイルを作成したり、トラフィック プロファイルの変化に基づいて相関ルールをトリガーしたりすることに注意してください。防御センター データベースにログとして記録されない接続をトラフィック プロファイルに含めることはできません。接続の要約（接続サマリーについて（39-3 ページ）を参照）の生成には、接続終了時のデータだけが使用されます。システムはその後、この要約を使って接続グラフやトラフィック プロファイルを作成します。したがって、トラフィック プロファイルを作成/使用するには、必ず接続終了時における接続イベントをログに記録してください。

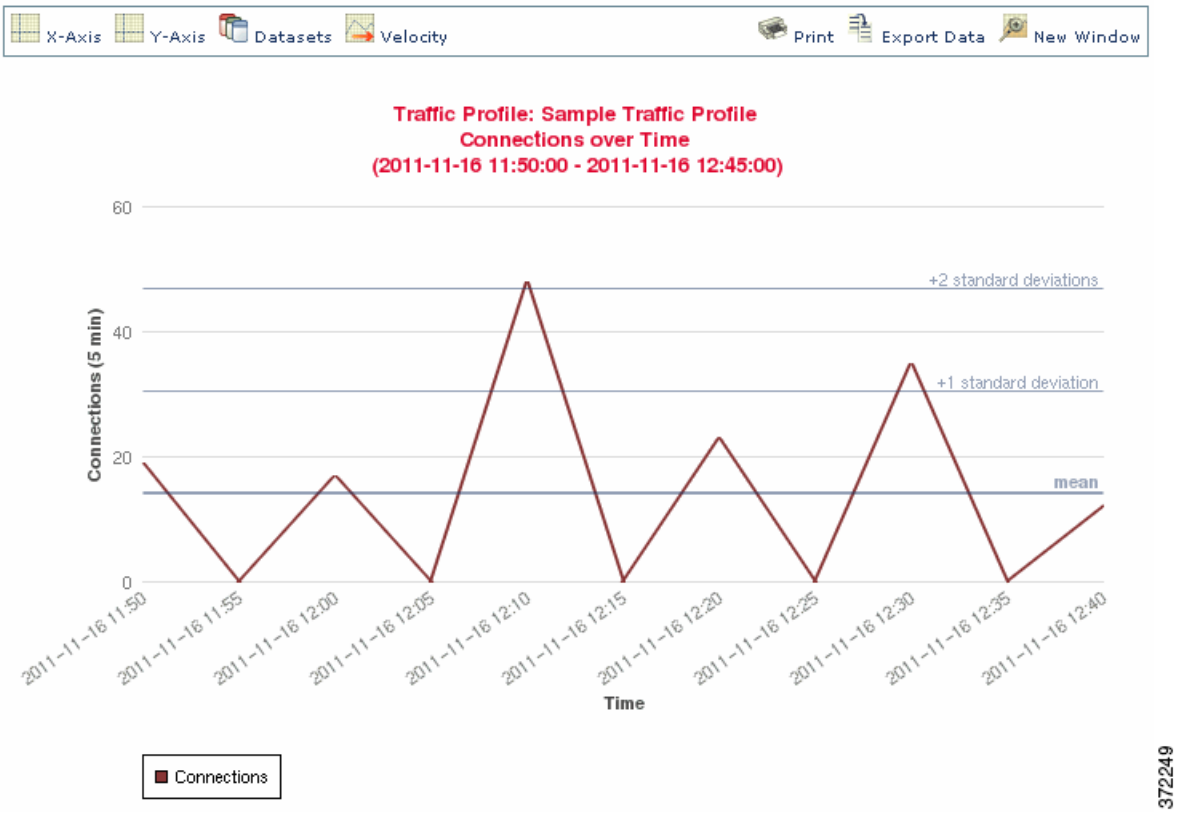
トラフィック プロファイルを構築するためのデータ収集期間を、プロファイル作成時間枠（PTW）と呼びます。PTW はスライディング時間枠です。つまり、PTW が 1 週間（デフォルト）の場合、先週の間に収集された接続データがトラフィック プロファイルに含まれます。PTW を最短で 1 時間、最長で数週間に変更できます。

初めてトラフィック プロファイルをアクティブにすると、学習期間（PTW と等しい時間）にわたる接続データが、設定した基準に従って収集され、評価されます。トラフィック プロファイルに関して作成したルールは、学習期間が完了するまでは防御センターで評価されません。

モニタ対象のネットワーク セグメント上のすべてのトラフィックを使ってプロファイルを作成することも、接続イベント内のデータに基づく基準を使用して、さらにターゲットを絞ったプロファイルを作成することもできます。たとえば、検出されたセッションで特定のポート、プロトコル、アプリケーションが使われている場合にのみトラフィック プロファイルでデータを収集するよう、プロファイル条件を設定できます。あるいは、ホスト重要度が**高**であるホストのデータだけを収集するよう、トラフィック プロファイルにホスト プロファイル限定を追加することもできます。

最後に、トラフィック プロファイルを作成する際には、非アクティブ期間を指定できます。この期間内は、接続データがプロファイル統計情報に影響を及ぼさず、プロファイルに関して作成されたルールはトリガーしません。また、収集済みの接続データをどれほどの頻度でトラフィック プロファイルで集約し、統計情報を計算するかを変更することもできます。

次の図は、PTW 1 日、およびサンプリング レート 5 分のトラフィック プロファイルを示しています。



トラフィック プロファイルを作成してアクティブにした後、その学習期間が完了したら、異常なトラフィックの検出時にトリガーされる相関ルールを作成することができます。たとえば、ネットワークを通過するデータ量（パケット数、KB 数、または接続数で測定）が、平均トラフィック量に比べて標準偏差の 3 倍も急激に上昇した場合、攻撃または他のセキュリティ ポリシー違反を示す可能性があると判断してトリガーするルールを作成できます。その後、このルールを相関ポリシーに組み込んで、トラフィックの急増に関するアラートを出したり、応答として修復を実行したりできます。トラフィック プロファイルを使用して異常なネットワーク トラフィックを検出する方法については、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。

[トラフィック プロファイル（Traffic Profiles）] ページでトラフィック プロファイルを作成します。各プロファイルの隣にあるスライダ アイコンは、プロファイルがアクティブであるかどうかを示します。トラフィック プロファイルの変化に基づく相関ルールを使用するには、プロファイルをアクティブにする必要があります。スライダ アイコンが青色でチェック マークが付いている場合は、そのプロファイルがアクティブです。灰色で x が表示されている場合は、プロファイルが非アクティブです。詳細については、トラフィック プロファイルのアクティブ化と非アクティブ化（53-10 ページ）を参照してください。

経過表示バーは、トラフィック プロファイルの学習期間の状態を示します。経過表示バーが 100 % に達すると、プロファイルに関して作成された相関ルールがトリガーとして使用されます。

ヒント　[並べ替え（Sort by）] ドロップダウン リストを使用すると、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トラフィック プロファイルをソートできます。

詳細については、以下を参照してください。

基本的なプロファイル情報の指定

ライセンス：FireSIGHT

トラフィック プロファイルを作成するときには、名前を付ける必要があり、オプションで短い説明を入力します。

トラフィック プロファイルの作成を開始する方法：

アクセス：Admin/Discovery Admin

手順 1　[ポリシー（Policies）] > [相関（Correlation）] を選択してから、[トラフィック プロファイル（Traffic Profiles）] をクリックします。

[トラフィック プロファイル（Traffic Profiles）] ページが表示されます。

手順 2　[新規プロファイル（New Profile）] をクリックします。

[プロファイルの作成（Create Profile）] ページが表示されます。

手順 3　[プロファイル名（Profile Name）] フィールドに、新しいトラフィック プロファイルの名前を最大 255 文字で入力します。

手順 4　[プロファイルの説明（Profile Description）] フィールドに、新しいトラフィック プロファイルの短い説明を最大 255 文字で入力します。

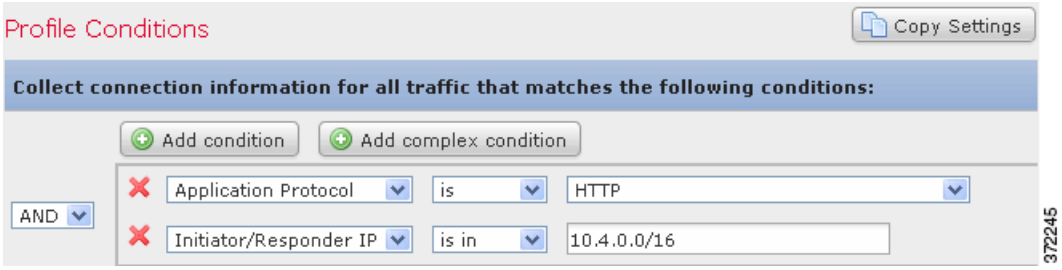
手順 5　トラフィック プロファイル条件の指定に進みます。

トラフィック プロファイル条件の指定

ライセンス：FireSIGHT

プロファイル条件は、トラフィック プロファイルで追跡する接続データの種類を制約します。単純なトラフィック プロファイルは、モニタ対象のネットワーク セグメント上のすべてのトラフィックに関するプロファイルを無条件で作成します。これに対し、複数の条件がネストされた、複雑なトラフィック プロファイルもあります。

たとえば、次の図のトラフィック プロファイル条件は、10.4.x.x サブネットでの HTTP 接続を収集します。



[プロファイルの作成(Create Profile)] ページの [プロファイル条件(Profile Conditions)] セクションで、トラフィック プロファイル条件を作成します。条件の作成の詳細については、条件の作成手順について(53-11 ページ)を参照してください。また、条件を作成するために使用できる構文については、トラフィック プロファイル条件の構文(53-4 ページ)で詳しく説明しています。

ヒント　既存のトラフィック プロファイルの設定を使用するには、[設定のコピー(Copy Settings)] をクリックし、ポップアップ ウィンドウで、使用するトラフィック プロファイルを選択して [ロード(Load)] をクリックします。

トラフィック プロファイル条件の構文

ライセンス:FireSIGHT

次の表で、トラフィック プロファイル条件を作成する方法について説明します。

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。

トラフィック プロファイル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 53-1　プロファイル条件の構文

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)	使用可能なプロトコルを示すドロップダウン リストから、アプリケーション プロトコルの名前を選択します。
アプリケーション プロトコル カテゴリ(Application Protocol Category)	使用可能なカテゴリを示すドロップダウン リストから、アプリケーション プロトコルのカテゴリ名を選択します。
クライアント(Client)	使用可能なクライアントを示すドロップダウン リストから、クライアント名を選択します。
クライアント カテゴリ(Client Category)	使用可能なカテゴリを示すドロップダウン リストから、クライアントのカテゴリ名を選択します。

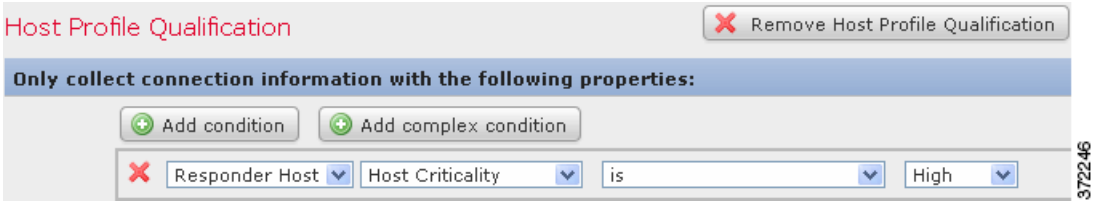
表 53-1　プロファイル条件の構文(続き)

指定する項目	演算子を指定した後に行う操作
接続タイプ(Connection Type)	トラフィック プロファイル内で、Cisco デバイスによって収集された接続データと NetFlow 対応デバイスによって収集された接続データのどちらを使用するかを指定します。接続タイプを指定しない場合、トラフィック プロファイルには両方が含まれます。
宛先国(Destination Country)または送信元国(Source Country)	選択可能な国を示すドロップダウン リストから、国を選択します。これは、ネットワーク トラフィック内で識別される送信元 IP アドレスや宛先 IP アドレスに関連付けられる国を表します。
イニシエータ IP(Initiator IP)、レスポンダ IP(Responder IP)、またはイニシエータ/レスポンダ IP(Initiator/Responder IP)	IP アドレスの範囲を指定するには、特定の IP アドレスか CIDR 表記を使用します。 IP アドレスに使用できる構文の説明については、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。なお、モニタ対象のネットワーク内またはネットワーク外の IP アドレスを指定するためにキーワード `local` および `remote` を使用**できない**ことに注意してください。
NetFlow デバイス(NetFlow Device)	トラフィック プロファイルの作成に使われるデータのエクスポート元となる NetFlow 対応デバイスを選択します。(ローカル設定を使用して)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。
レスポンダ ポート/ICMP コード(Responder Port/ICMP Code)	ポート番号または ICMP コードを入力します。
セキュリティ インテリジェンスのカテゴリ(Security Intelligence Category)	使用可能なカテゴリを示すドロップダウン リストから、セキュリティ インテリジェンスのカテゴリ名を選択します。トラフィック プロファイル条件でセキュリティ 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、そのカテゴリを [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。
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。
トランスポート プロトコル(Transport Protocol)	トランスポート プロトコルとして `TCP` または `UDP` と入力します。
Web アプリケーション(Web Application)	使用可能な Web アプリケーションを示すドロップダウン リストから、Web アプリケーションの名前を選択します。
Web アプリケーション カテゴリ(Web Application Category)	使用可能なカテゴリを示すドロップダウン リストから、Web アプリケーションのカテゴリ名を選択します。

ホスト プロファイル限定の追加

ライセンス: FireSIGHT

追跡対象のホストのプロファイル情報を使用して、トラフィック プロファイルを制約できます。この制約は、*ホスト プロファイル限定*と呼ばれます。たとえば、次の図に示すように、ホスト重要度に**高**が割り当てられたホストの接続データだけを収集することができます。



ホスト プロファイル限定を使用するには、そのホストがデータベース内に存在すること、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侵入イベントが生成されると相関ルールがトリガーされるよう設定した場合、そのルールがトリガーされるのは、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　[プロファイルの作成（Create Profile）] 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 2　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。条件の作成の詳細については、条件の作成手順について（53-11 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（53-6 ページ）で説明しています。

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。

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、トラフィック プロファイ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。[レスポンダ ホスト（Responder Host）] または [イニシエータ ホスト（Initiator Host）] を選択できます。ホストの役割を選択した後、ホスト プロファイル限定の構文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トラフィック プロファイルで使用する場合、NetFlow レコードには、どのホストが接続のイニシエータで、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。

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、ホスト上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 [レスポンダ ホスト（Responder Host）] 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。

表 53-2　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）]	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。通常のホスト、またはいずれかのタイプのネットワーク デバイスを選択できます。
[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 ベンダー（OS Vendor）]	ドロップダウン リストから、1 つ以上のオペレーティング システム ベンダー名を選択します。
[オペレーティング システム（Operating System）] > [OS 名（OS Name）]	ドロップダウン リストから、1 つ以上のオペレーティング システムの名前を選択します。
[オペレーティング システム（Operating System）] > [OS バージョン（OS Version）]	ドロップダウン リストから、1 つ以上のオペレーティング システムのバージョンを選択します。
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）]	表示されるリストから、ホストの重要度を選択します。[なし（None）]、[低（Low）]、[中（Medium）]、または [高（High）] を選択できます。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）	ホストの VLAN ID 番号を入力します。

表 53-2　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（Application Protocol）] > [アプリケーション プロトコル（Application Protocol）]	ドロップダウン リストから、アプリケーション プロトコルを選択します。
[アプリケーション プロトコル（Application Protocol）] > [アプリケーション ポート（Application Port）]	アプリケーション プロトコルのポート番号を入力します。
[アプリケーション プロトコル（Application Protocol）] > プロトコル	ドロップダウン リストからプロトコルを選択します。
[クライアント（Client）] > [クライアント（Client）]	ドロップダウン リストからクライアントを選択します。
[クライアント（Client）] > [クライアント バージョン（Client Version）]	クライアントのバージョンを入力します。
[Web アプリケーション（Web Application）]	ドロップダウン リストからクライアントを選択します。
[MAC アドレス（MAC Address）] > [MAC アドレス（MAC Address）]	ホストの MAC アドレス全体またはその一部を入力します。
[MAC アドレス（MAC Address）] > [MAC タイプ（MAC Type）]	MAC タイプが ARP/DHCP で検出され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（**ARP/DHCP 検出である**）、デバイスとホストの間にルータがあるなどの理由で、その MAC アドレスを持つ多数のホストをシステムが認識しているのか（**ARP/DHCP 検出ではない**）、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）]	ホストで使用されているハードウェアの MAC ベンダー全体またはその一部を入力します。
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 の場合は、ドロップダウン リストから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（49-35 ページ）を参照してください。

プロファイル オプションの設定

ライセンス：FireSIGHT

プロファイル作成時間枠（PTW）はスライド時間枠です。これは、FireSIGHT システムでトラフィック プロファイルの統計情報の計算に使用される、学習期間と同じ長さの時間です。デフォルト PTW は 1 週間ですが、最短で 1 時間、最長で数週間に変更できます。

また、トラフィック プロファイルは集約された接続データに基づきます。デフォルトで、トラフィック プロファイルは 5 分間隔でシステム生成の接続イベントに関する統計情報を生成します。ただし、デフォルトの 5 分から 1 時間までの範囲で、このサンプリング レートを設定できます。

統計的に意味のある十分なデータがトラフィック プロファイルに含まれるように、PTW とサンプリング レートを設定する必要があることに注意してください。たとえば PTW が 1 日、サンプリング レートが 1 時間の場合、それに含まれるデータ ポイントは 24 個だけであるため、ネットワーク トラフィックのパターンを正確に分析するには不十分な可能性があります。

ヒント　PTW には少なくとも 100 個のデータ ポイントを含めてください。

また、トラフィック プロファイル内で非アクティブ期間をセットアップすることもできます。たとえば、すべてのワークステーションが毎日深夜 0:00 にバックアップされるネットワーク インフラストラクチャがあるとします。バックアップには約 30 分かかり、ネットワーク トラフィックが急増します。この場合、スケジュール済みバックアップと同じ時間帯にトラフィック プロファイルの非アクティブ期間を繰り返すようセットアップできます。非アクティブ期間中は、トラフィック プロファイルがデータを収集します（したがってトラフィック プロファイルのグラフにトラフィックが表示されます）が、プロファイル統計情報の計算時にはこのデータが使用されません。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。非アクティブ期間は最短で 5 分、最長で 1 時間にすることができます。トラフィック プロファイルの時系列グラフでは、非アクティブ期間が網掛け領域として示されます。

プロファイル オプションを設定する方法：

アクセス：Admin/Discovery Admin

表 53-3　プロファイル オプション

目的	操作
プロファイル作成時間枠の変更	[プロファイル時間枠（Profiling Time Window）] フィールドで、時間、日、または週の数値を入力します。次に、ドロップダウン リストから [時間（hour(s)）]、[日（day(s)）]、または [週（week(s)）] を選択します。
サンプリング レートの変更	[サンプリング レート（Sampling Rate）] ドロップダウン リストからレートを選択します。
非アクティブ期間の追加	[非アクティブ期間の追加（Add Inactive Period）] をクリックします。次に、ドロップダウン リストを使用して、トラフィック プロファイルでのデータ収集を中断する時点と頻度を指定します。
非アクティブ期間の削除	削除する非アクティブ期間の横の [削除（Delete）] をクリックします。

トラフィック プロファイルの保存

ライセンス: FireSIGHT

トラフィック プロファイルを保存するには、次の手順に従います。

トラフィック プロファイルを保存する方法:

アクセス: Admin/Discovery Admin

手順 1　以下の 2 つの対処法があります。

- アクティブ化せずにプロファイルを保存するには、[保存(Save)] をクリックします。
- プロファイルを保存し、ただちにデータを収集し始めるには、[保存とアクティブ化(Save & Activate)] をクリックします。

トラフィック プロファイルのアクティブ化と非アクティブ化

ライセンス: FireSIGHT

モニタ対象ネットワーク セグメント上のトラフィックのプロファイル作成を開始するには、トラフィック プロファイルをアクティブにする必要があります。

接続データの収集と評価を停止するには、プロファイルを非アクティブにします。非アクティブ化されトラフィック プロファイルに関して作成されたルールは、トリガーされません。さらに、トラフィック プロファイルを非アクティブにすると、そのプロファイルによってすでに収集/集約されたデータがすべて削除されます。非アクティブにしたトラフィック プロファイルを後で再度アクティブにした場合、そのプロファイルに関して作成されたルールがトリガーするようになるまで、PTW の長さだけ待つ必要があります。

トラフィック プロファイル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/Discovery Admin

手順 1　[ポリシー(Policies)] > [相関(Correlation)] を選択してから、[トラフィック プロファイル(Traffic Profiles)] をクリックします。

[トラフィック プロファイル(Traffic Profiles)] ページが表示されます。

手順 2　以下の 2 つの対処法があります。

- 非アクティブなトラフィック プロファイルをアクティブにするには、プロファイルの隣の [アクティブ化(Activate)] をクリックします。
- アクティブなトラフィック プロファイルを非アクティブにするには、プロファイルの隣の [非アクティブ化(Deactivate)] をクリックします。[OK] をクリックして、プロファイルを非アクティブにすることを確認します。

トラフィック プロファイルの編集

ライセンス：FireSIGHT

アクティブなトラフィック プロファイルを実質的に編集することはできません。トラフィック プロファイルがアクティブな場合には、名前と説明のみを変更できます。トラフィック プロファイルの条件オプションを編集するには、まず非アクティブにする必要があります。なお、トラフィック プロファイルを非アクティブにすると、すでに収集されたデータがすべて削除されることに注意してください。

トラフィック プロファイルのアクティブ化と非アクティブ化の詳細については、トラフィック プロファイルのアクティブ化と非アクティブ化（53-10 ページ）を参照してください。

トラフィック プロファイルを編集する方法：

アクセス：Admin/Discovery Admin

手順 1　[ポリシー（Policies）] > [相関（Correlation）] を選択してから、[トラフィック プロファイル（Traffic Profiles）] をクリックします。

[トラフィック プロファイル（Traffic Profiles）] ページが表示されます。

手順 2　編集するトラフィック プロファイルの横にある [編集（Edit）] をクリックします。

[プロファイルの作成（Create Profile）] ページが表示されます。

手順 3　プロファイルを変更して、[保存（Save）] をクリックします。

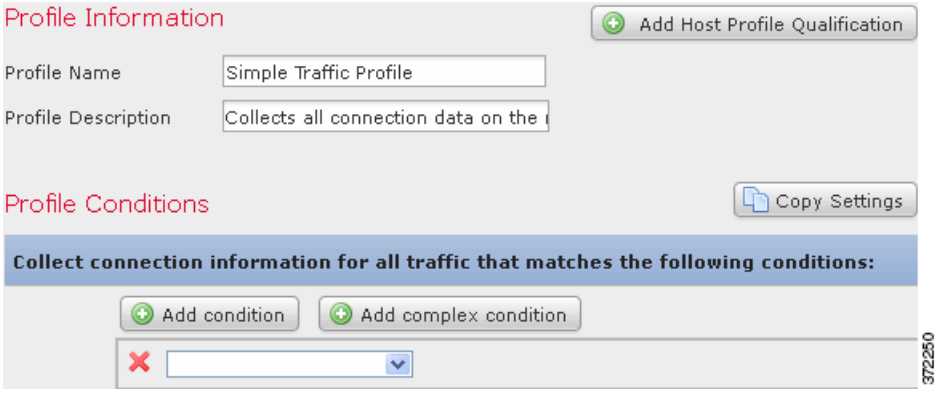
プロファイルが更新されます。

条件の作成手順について

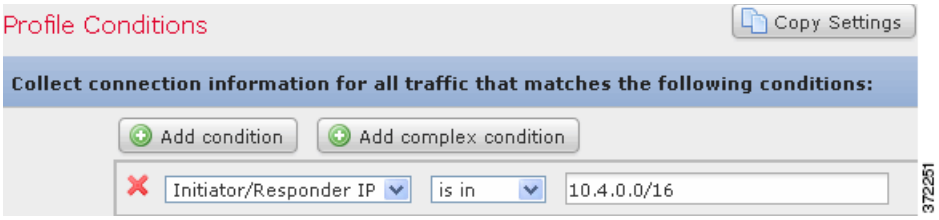
ライセンス：FireSIGHT

トラフィック プロファイルを作成する際には、データの収集に使われる条件を指定します。単純な条件を作成することも、条件をネストさせた複雑な構造を作成することもできます。

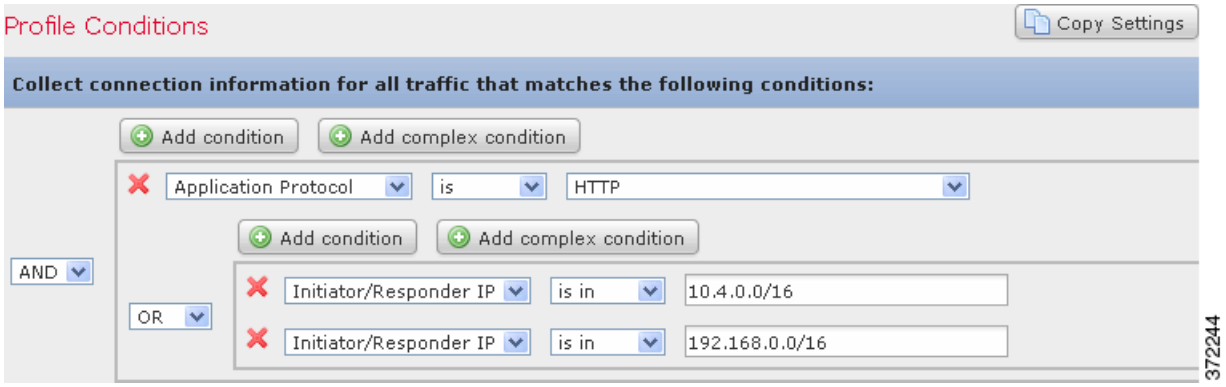
たとえば、モニタ対象ネットワーク セグメント全体のデータを収集するトラフィック プロファイルを作成するには、次の図のように、条件を含まない非常に単純なプロファイルを作成できます。



プロファイルを制約して、10.4.x.x ネットワークのデータのみを収集するには、次の図のように 1 つの条件を追加できます。



一方、次のトラフィック プロファイルは 10.4.x.x ネットワークと 192.168.x.x ネットワーク上の HTTP アクティビティを収集しますが、3 つの条件のうち最後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。詳細については、以下を参照してください。

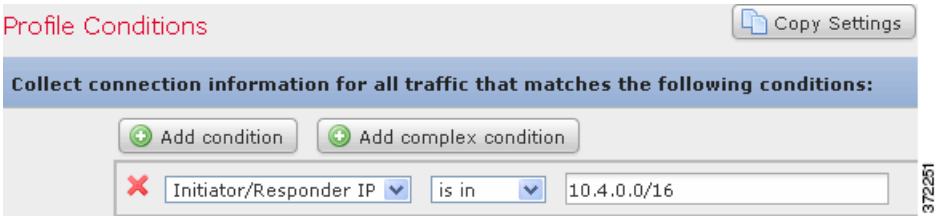
- 単一の条件の作成（53-12 ページ）
- 条件の追加と結合（53-14 ページ）
- 複数の値を条件で使用する（53-17 ページ）

単一の条件の作成

ライセンス：FireSIGHT

ほとんどの条件は、カテゴリ、演算子、値の 3 つの部分からなります。もっと複雑な条件もあり、それぞれ独自の演算子と値を持つ複数のカテゴリが含まれることがあります。

たとえば、次のトラフィック プロファイルは 10.4.x.x ネットワーク上の情報を収集します。条件のカテゴリは [イニシエータ/レスポンダ IP（Initiator/Responder IP）]、演算子は [含まれる（is in）]、値は `10.4.0.0/16` です。



次の手順では、このトラフィック プロファイル条件を作成する方法について説明します。

単一の条件を作成する方法:

アクセス: Admin/Discovery Admin

手順 1　[ポリシー(Policies)] > [相関(Correlation)] を選択してから、[トラフィック プロファイル(Traffic Profiles)] をクリックします。

[トラフィック プロファイル(Traffic Profiles)] ページが表示されます。

手順 2　[新規プロファイル(New Profile)] をクリックします。

[プロファイルの作成(Create Profile)] ページが表示されます。

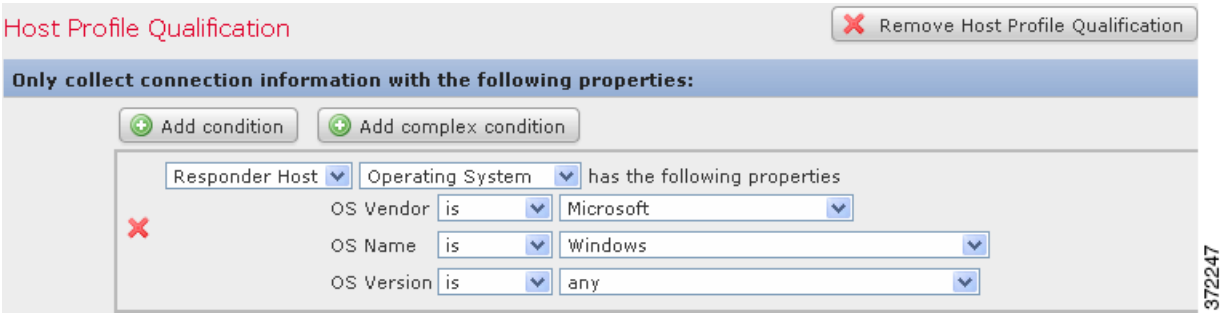
手順 3　[プロファイル条件(Profile Conditions)] の下で、最初の(カテゴリ)ドロップダウン リストから [イニシエータ/レスポンダ IP(Initiator/Responder IP)] を選択して、プロファイルの単一条件を作成し始めます。

手順 4　2 番目の(演算子)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 アドレスを表している場合、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 表記で表される IP アドレス範囲内にその 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 システムでの CIDR 表記の使用法の詳細については、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、次のホスト プロファイル限定はもっと複雑です。これによりトラフィック プロファイルが制約され、検出された接続内の応答側ホストで任意のバージョンの Microsoft Windows が実行されている場合にのみ、接続データが収集されます。



次の手順では、このホスト プロファイル限定の作成方法について説明します。

このホスト 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　[ポリシー(Policies)] > [相関(Correlation)] を選択してから、[トラフィック プロファイル(Traffic Profiles)] をクリックします。

[トラフィック プロファイル(Traffic Profiles)] ページが表示されます。

手順 2　[新規プロファイル(New Profile)] をクリックします。

[プロファイルの作成(Create Profile)] ページが表示されます。

手順 3　[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。

手順 4　[ホスト プロファイル限定(Host Profile Qualification)] の下の最初の条件で、情報を収集する対象となるホストを指定します。

この例では、接続内の応答側ホストに関する情報だけが必要なので、[レスポンダ ホスト(Responder Host)] を選択します。

手順 5　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 6　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 7　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。

トラフィック プロファイル条件を作成しているか、それともホスト プロファイル限定を作成しているかに応じて、選択できるカテゴリが異なることに注意してください。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(53-17 ページ)を参照してください。

トラフィック プロファイルの条件とホスト プロファイル限定を作成するための構文については、以下の項を参照してください。

- トラフィック プロファイル条件の構文(53-4 ページ)
- ホスト プロファイル限定の構文(53-6 ページ)

条件の追加と結合

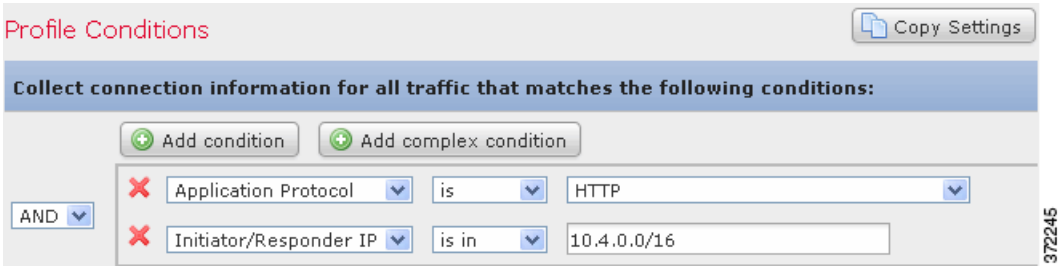
ライセンス: FireSIGHT

単純なトラフィック プロファイル条件やホスト プロファイル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。

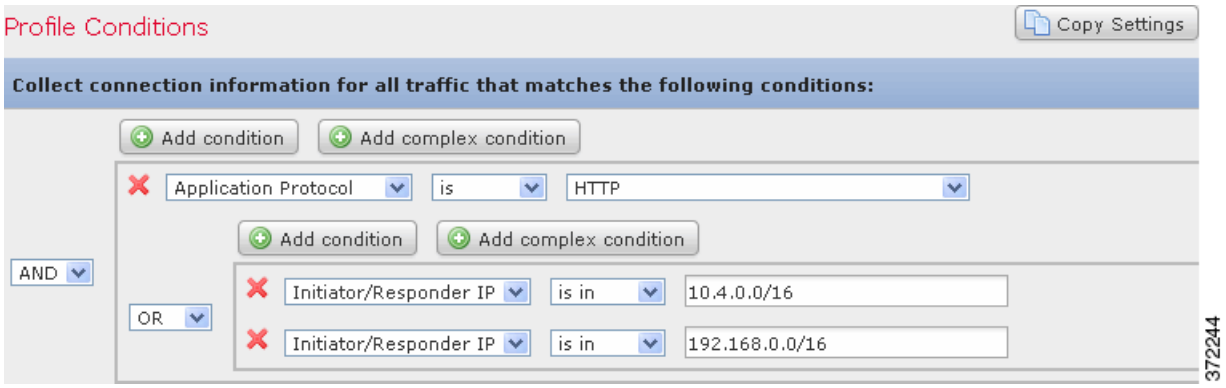
構造に複数の条件を含める場合は、それらの条件を **AND** または **OR** 演算子で結合する必要があります。同じレベルにある複数の条件は、一緒に評価されます。

- **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、次のトラフィック プロファイルには、**AND** で結合された 2 つの条件が含まれます。つまり、両方の条件とも満たされる場合に限り、このトラフィック プロファイルが接続データを収集します。この例では、10.4.x.x サブネット内の IP アドレスを持つすべてのホストに関する HTTP 接続を収集します。



一方、次のトラフィック プロファイルは、10.4.x.x ネットワークまたは 192.168.x.x ネットワーク内の HTTP アクティビティに関する接続データを収集しますが、3 つの条件のうち最後は複合条件を形成しています。



論理的には、上記のトラフィック プロファイルは次のように評価されます。

```
(A and (B or C))
```

Where...	Is the condition that states...
A	Application Protocol Name is HTTP
B	IP Address is in 10.4.0.0/16
C	IP Address is in 192.168.0.0/16

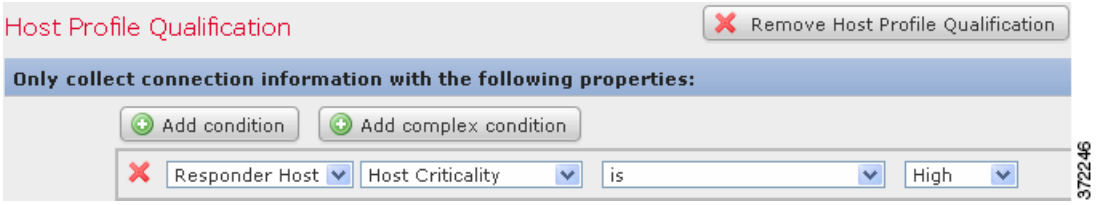
単一の条件を追加する方法:

アクセス: Admin/Discovery Admin

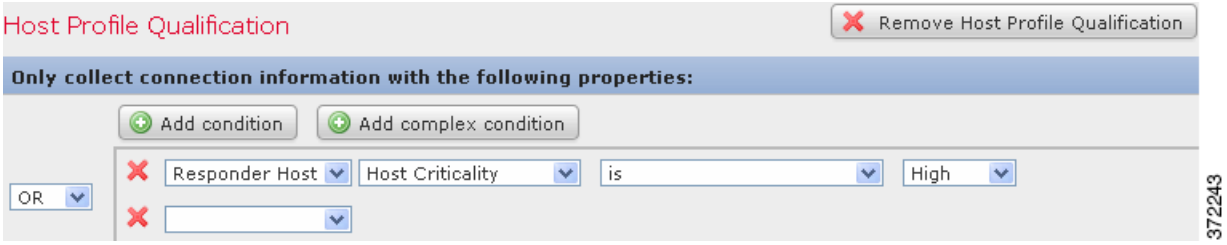
手順 1　単一の条件を追加するには、現在の条件の上にある [条件の追加(Add condition)] をクリックします。

新しい条件が、現在の条件セットと同じ論理レベルに追加されます。デフォルトでは、そのレベルの条件に **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、次のホスト プロファイル限定に単純な条件を追加すると、



結果は以下のとおりです。



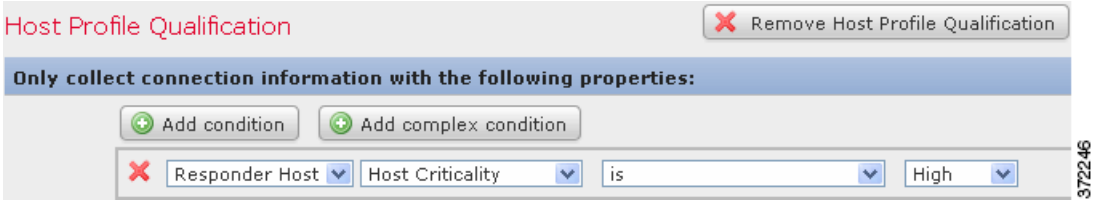
複合条件を追加する方法:

アクセス: Admin/Discovery Admin

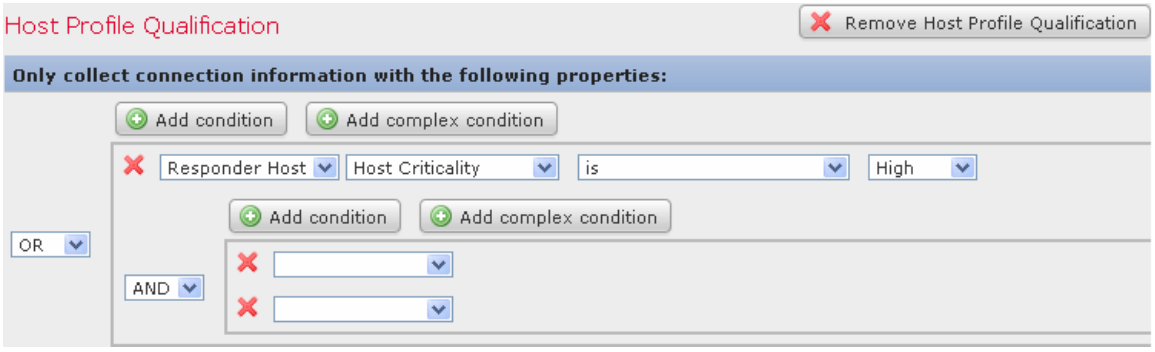
手順 1　現在の条件の上にある [複合条件の追加(Add complex condition)] をクリックします。

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、次のホスト プロファイル限定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

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。

- 演算子で制御されるレベルのすべての条件が満たされるべきことを指定するには、[AND] を選択します。
- 演算子で制御されるレベルの 1 つの条件だけが満たされるべきことを指定するには、[OR] を選択します。

複数の値を条件で使用する

ライセンス: FireSIGHT

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トラフィック プロファイルに追加するには、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。

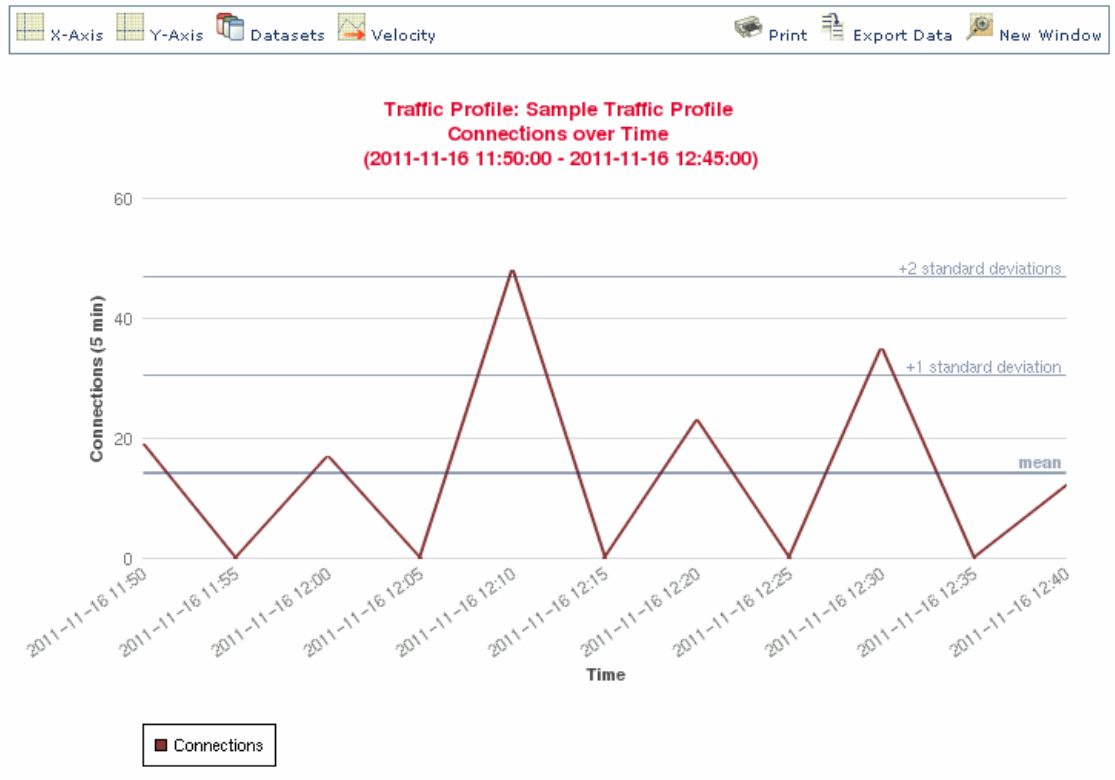
手順 5　[OK] をクリックします。

選択した内容が [プロファイルの作成（Create Profile）] ページの条件の値フィールドに表示されます。

トラフィック プロファイルの表示

ライセンス: FireSIGHT

トラフィック プロファイルは接続データに基づいているため、トラフィック プロファイルのグラフを表示できます。次の図は、PTW 1 週間、サンプリング レート 5 分、非アクティブ期間として毎日深夜 12:00 から 12:30 までの 30 分間が設定されているトラフィック プロファイルを示します。



接続データ グラフで実行できるほとんどすべてのアクションを、トラフィック プロファイル グラフでも実行できます。ただし、トラフィック プロファイルは集約データ（接続の要約）に基づいているため、グラフの基礎となる個々の接続イベントを調べることはできません。つまり、トラフィック プロファイル グラフから接続データ テーブル ビューにドリル ダウンすることはできません。詳細については、接続データとセキュリティ インテリジェンスのデータの表示（39-17 ページ）を参照してください。また、トラフィック プロファイルは分離グラフとして表示されます。詳細については、接続グラフの分離（39-29 ページ）を参照してください。

さらに、トラフィック プロファイルの時系列グラフでは、Y 軸の中間（平均）値が太い横棒で示されます。また、時系列グラフでは、ネットワーク トラフィックが正規分布することを前提に、最初の 4 つの標準偏差値が平均の上下に示されます。デフォルトではこれらの統計情報が PTW 期間にわたって計算されますが、グラフの時間設定を変更すると、防御センターにより統計情報が再計算されます。ただし、トラフィック プロファイル統計情報に関して作成されたルールは、常に PTW 期間の統計情報に照らして評価されます。

トラフィック プロファイルに関するグラフを表示する方法:

アクセス: Admin/Discovery Admin

手順 1　[ポリシー（Policies）] > [相関（Correlation）] を選択してから、[トラフィック プロファイル（Traffic Profiles）] をクリックします。

[トラフィック プロファイル（Traffic Profiles）] ページが表示されます。

手順 2　グラフを表示する対象のトラフィック プロファイルの隣にあるグラフ アイコン（ ）をクリックします。

トラフィック プロファイルのグラフが、別のブラウザ ウィンドウで表示されます。