カスタム テーブル

次のトピックでは、カスタム テーブルの使用方法について説明します。

カスタム テーブルの概要

Firepower システムがネットワークに関する情報を収集し、Firepower Management Center がその情報を一連のデータベーステーブルに保存します。結果として生成される情報を表示するためにワークフローを使用する場合、Firepower Management Center はそれらのテーブルのいずれかからデータを取り出します。たとえば、[Network Applications by Count] ワークフローの各ページのカラムは、[Applications] テーブルのフィールドから取得されます。

さまざまなテーブルのフィールドを結合することにより、ネットワークのアクティビティの分析が向上する場合、カスタム テーブルを作成できます。たとえば、定義済みの [Host Attributes] テーブルのホスト重大度情報と、定義済みの [Connection Data] テーブルのフィールドを結合してから、新しいコンテキストで接続データを検証できます。

定義済みのテーブルまたはカスタム テーブルのどちらについても、カスタム ワークフローを作成できます。

定義済みのカスタム テーブル

カスタム テーブルには、2 つまたは 3 つの定義済みテーブルのフィールドを含みます。Firepower System は、いくつかのシステム定義のカスタム テーブルと共に配布されますが、特定のニーズに適合する情報のみを含む追加のカスタム テーブルを作成できます。

たとえば、Firepower System は、侵入イベントとホスト データを相関するシステム定義のカスタム テーブルと共に配布されます。そのため、クリティカル システムに影響を及ぼすイベントを検索でき、1 つのワークフローにその検索結果を表示できます。

マルチドメイン展開では、定義済みのカスタム テーブルは、グローバル ドメインに属し、下位ドメインで変更することはできません。

次の表では、システムと共に提供されるカスタム テーブルについて説明します。

表 *1*: システム定義カスタム テーブル

テーブル	説明
Hosts with Servers	ネットワーク上で実行されている検出されたアプリケーションに関する情報と、それらのアプリケーションを実行しているホストに関する基本的なオペレーティング システム情報を提供する、[Hosts] および [Servers] テーブルのフィールドが含まれます。
Intrusion Events with Destination Criticality	侵入イベント テーブルとホスト テーブルのフィールドを含み、侵入イベントに関する情報と各侵入イベントに含まれる宛先ホストのホスト重要度を提供します。 このテーブルを使用して、ホスト重要度の高い宛先ホストに関与する侵入イベントを検索できます。
侵入イベントと送信元重要度（Intrusion Events with Source Criticality）	侵入イベント テーブルとホスト テーブルのフィールドを含み、侵入イベントに関する情報と各侵入イベントに含まれる送信元ホストのホスト重要度を提供します。 このテーブルを使用して、ホスト重要度の高い送信元ホストに関与する侵入イベントを検索できます。

可能なテーブルの組み合わせ

カスタムテーブルを作成する場合、関連データのある定義済みのテーブルのフィールドを組み合わせことができます。次の表は、新しいカスタムテーブルを作成するために結合できる定義済みのテーブルをリストしています。2つ以上の定義済みのカスタムテーブルのフィールドを組み合わせるカスタム テーブルを作成できます。

表 *2:* カスタム テーブルの組み合わせ

組み合わせ可能なカスタム テーブル	以下のテーブルのフィールドと結合可能
Applications	• Correlation Events • Intrusion Events • Connection Summary Data • Host Attributes • Application Details • Discovery Events • Connection Events • Hosts • Servers • White List Events
Correlation Events	• Applications • Host Attributes • Hosts
Intrusion Events	• Applications • Host Attributes • Hosts • Servers
Connection Summary Data	• Applications • Host Attributes • Hosts • サーバ

組み合わせ可能なカスタム テーブル	以下のテーブルのフィールドと結合可能
ホストの侵害の兆候（Host Indications of Compromise）	• アプリケーション • Application Details • Captured Files • Connection Events • Connection Summary Data • Correlation Events • Discovery Events • Host Attributes • Hosts • Intrusion Events • Security Intelligence Events • Servers • White List Events
Host Attributes	• Applications • Correlation Events • Intrusion Events • Connection Summary Data • Application Details • Discovery Events • Connection Events • Hosts • Servers • White List Events
Application Details	• Applications • Host Attributes • Hosts
Discovery Events	• Applications • Host Attributes • Hosts

組み合わせ可能なカスタム テーブル	以下のテーブルのフィールドと結合可能
Connection Events	• Applications • Host Attributes • Hosts • Servers
Security Intelligence Events	• Applications • Host Attributes • Hosts • Servers
Hosts	• Applications • Correlation Events • Intrusion Events • Connection Summary Data • Host Attributes • Application Details • Discovery Events • Connection Events • Servers • White List Events
Servers	• Applications • Intrusion Events • Connection Summary Data • Host Attributes • Connection Events • Hosts
White List Events	• Applications • Host Attributes • Hosts

あるテーブルのフィールドが、別のテーブルの複数のフィールドにマップされる場合があります。たとえば、定義済みの [Intrusion Events with Destination Criticality] カスタム テーブルは、[Intrusion Events] テーブルと [Hosts] テーブルのフィールドを結合します。[Intrusion Events] テーブルの各イベントは、2 つの IP アドレス（送信元 IP アドレスと宛先 IP アドレス）と関連付けられています。しかし、[ホスト（Hosts）]テーブルの「イベント」はそれぞれ、単一のホスト IP アドレスを表します（ホストに複数の IP アドレスが存在する場合があります）。したがって、[Intrusion Events] テーブルと [Hosts] テーブルに基づいてカスタム テーブルを作成する場合は、[Hosts] テーブルから表示するデータが [Intrusion Events] テーブルのホストの送信元 IP アドレスまたはホストの宛先 IP アドレスのどちらに適用されるかを選択する必要があります。

新しいカスタム テーブルを作成すると、テーブルのすべてのカラムを表示するデフォルトのワークフローが自動的に作成されます。定義済みのテーブルと同じように、ネットワーク分析で使用するデータをカスタムテーブルで検索することもできます。定義済みのテーブルを使用して可能であるように、カスタム テーブルに基づいてレポートを作成できます。

ユーザ定義のカスタム テーブル

ヒント　新しいカスタム テーブルを作成する代わりに、別の Firepower Management Center からカスタム テーブルをエクスポートし、Firepower Management Center にインポートすることができます。

カスタム テーブルを作成するには、Firepower システムに付属しているどの定義済みテーブルに、カスタムテーブルに組み込むフィールドが含まれているかを判断します。その後、組み込むフィールドを選択できます。さらに、必要に応じて、共通フィールドのフィールドマッピングを設定することもできます。

ヒント　[Hosts] テーブルを含むデータでは、1 つの IP アドレスではなく、1 つのホストのすべての IP アドレスに関連したデータを表示できます。

例として、[Correlation Events] テーブルと [Hosts] テーブルのフィールドを結合するカスタム テーブルについて考慮します。このカスタムテーブルを使用して、相関ポリシーの違反に関係するホストの詳細情報を取得できます。注意すべき点として、[Correlation Events] テーブルの送信元 IP アドレスと宛先 IP アドレスのどちらと一致する [Hosts] テーブルのデータを表示するかを決定する必要があります。

このカスタム テーブルのイベントのテーブル ビューを表示する場合、相関イベントが 1 行に 1 つずつ表示されます。次の情報を含むようにカスタム テーブルを設定できます。

- イベントが生成された日時
- 違反された相関ポリシーの名前
- 違反をトリガーとして使用した規則の名前
- 相関イベントに関係する送信元ホスト（開始ホスト）に関連付けられた IP アドレス

- 送信元ホストの NetBIOS 名
- 送信元ホストが実行しているオペレーティング システムおよびバージョン
- 送信元ホストの重大度

ヒント　宛先ホスト（応答ホスト）の同じ情報を表示する同様のカスタムテーブルを作成することもできます。

カスタム テーブルの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Any/Admin

ステップ 1　**[Analysis]** > **[Advanced]** > **[Custom Tables]**を選択します。

ステップ 2　[カスタム テーブルの作成（Create Custom Table）] をクリックします。

ステップ 3　[名前（Name）] フィールドに、カスタム テーブルの名前を入力します。

例：

たとえば、`Correlation Events with Host Information (Src IP)` と入力します。

ステップ 4　[テーブル（Tables）] ドロップダウン リストから、[相関イベント（Correlation Events）] を選択します。

ステップ 5　[フィールド（Fields）] で [時間（Time）] を選択し、[追加（Add）] をクリックして、相関イベントが生成された日時を追加します。

ステップ 6　手順 5 を繰り返して、[ポリシー（Policy）] および [ルール（Rule）] フィールドを追加します。

ヒント　Ctrl または Shift を押しながらクリックすることにより、複数のフィールドを選択できます。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。ただし、テーブルに関連したイベントのテーブル ビューでフィールドが表示される順序を指定する場合は、フィールドを一度に 1 つずつ追加します。

ステップ 7　[テーブル（Tables）] ドロップダウンリストから [ホスト（Hosts）] を選択します。

ステップ 8　[IP アドレス（IP Address）]、[NetBIOS 名（NetBIOS Name）]、[OS 名（OS Name）]、[OS バージョン（OS Version）]、[ホストの重大度（Host Criticality）] フィールドをカスタム テーブルに追加します。

ステップ 9　[相関イベント（Correlation Events）] の隣にある [共通フィールド（Common Fields）] で、[送信元 IP（Source IP）] を選択します。

相関イベントに関係する送信元ホスト（開始ホスト）用に手順 8 で選択したホスト情報を表示するように、カスタム テーブルが設定されます。

ヒント　相関イベントに関係する宛先ホスト（応答ホスト）に関する詳細なホスト情報を表示するカスタム テーブルを作成する場合も、この手順に従いますが、[送信元 IP（Source IP）] ではなく、[送信先 IP（Destination IP）] を選択します。

ステップ 10　**[保存（Save）]** をクリックします。

カスタム テーブルの変更

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Any/Admin

マルチドメイン展開では、現在のドメインで作成されたカスタムテーブルが表示されます。これは編集できます。先祖ドメインで作成されたカスタムテーブルも表示されますが、これは編集できません。下位のドメインのカスタムテーブルを表示および編集するには、そのドメインに切り替えます。

ステップ 1　**[Analysis]** > **[Advanced]** > **[Custom Tables]**を選択します。

ステップ 2　編集するテーブルの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3　除外するフィールドの横にある削除アイコン（  ）をクリックして、テーブルからフィールドを除外することもできます。

（注）　レポートで現在使用中のフィールドを削除すると、それらのフィールドを使用しているセクションをそれらのレポートから除外するか確認するプロンプトが表示されます。

ステップ 4　必要に応じて、その他の変更を実行します。

ステップ 5　**[保存（Save）]** をクリックします。

カスタム テーブルの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Any/Admin

マルチドメイン導入では、現在のドメインで作成されたカスタムテーブルが表示されます。これは削除できます。先祖ドメインで作成されたカスタムテーブルも表示されますが、これは削除できません。下位のドメインのカスタムテーブルを削除するには、そのドメインに切り替えます。

ステップ 1 **[Analysis]** > **[Advanced]** > **[Custom Tables]**を選択します。

ステップ 2 削除するカスタム テーブルの隣にある削除アイコン（  ）をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

カスタム テーブルに基づいたワークフローの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Any/Admin

カスタムテーブルを作成すると、そのデフォルトのワークフローがシステムによって自動的に作成されます。このワークフローの最初のページには、イベントのテーブル ビューが表示されます。カスタム テーブルに侵入イベントを含める場合、ワークフローの 2 番目のページはパケット ビューになります。それ以外の場合、ワークフローの 2 番目のページはホスト ページになります。カスタム テーブルに基づいて、独自のカスタム ワークフローを作成することもできます。

ヒント カスタム テーブルに基づいてカスタム ワークフローを作成する場合、それをそのテーブルのデフォルトのワークフローとして指定できます。

同じ手法を使用して、定義済みのテーブルに基づいたイベント ビューに使用するカスタムテーブルでイベントを表示できます。

マルチドメイン展開では、現在のドメインで作成されたカスタムテーブルが表示されます。これは編集できます。先祖ドメインで作成されたカスタムテーブルも表示されますが、これは編集できません。下位のドメインのカスタムテーブルを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Analysis]** > **[Advanced]** > **[Custom Tables]**を選択します。

ステップ 2 表示するワークフローに関連するカスタム テーブルの隣にある表示アイコン（  ）をクリックします。

カスタム テーブルの検索

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Any/Admin

マルチドメイン展開では、現在のドメインで作成されたカスタムテーブルが表示されます。これは編集できます。先祖ドメインで作成されたカスタムテーブルも表示されますが、これは編集できません。下位のドメインのカスタムテーブルを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Analysis]** > **[Advanced]** > **[Custom Tables]**を選択します。

ステップ 2 検索するカスタム テーブルの隣にある表示アイコン（）をクリックします。

ヒント カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [（ワークフローの切り替え）（(switch workflow)）] をクリックします。

ステップ 3 [検索（Search）] をクリックします。

ヒント 別の種類のイベントやデータについてデータベースを検索する場合は、その種類をテーブル ドロップダウンリストから選択します。

ステップ 4 該当するフィールドに、検索条件を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。

ヒント 検索基準としてオブジェクトを使用する場合は、検索フィールドの横にあるオブジェクト アイコン（）をクリックします。

ステップ 5 必要に応じて、検索を保存する場合は、[プライベート（Private）] チェックボックスをオンにして、プライベートとして検索を保存すると、その検索に本人のみがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント カスタム ユーザ ロール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 （任意）検索を保存して、後でそれを再使用できます。次の選択肢があります。

- [保存（Save）] をクリックして、検索条件を保存します。[プライベート（Private）] チェックボックスをオンにすると、その検索は本人のアカウントでのみ表示できるようになります。
- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[新規に保存（Save As New）] をクリックします。[プライベート（Private）] チェックボックスをオンにすると、その検索は本人のアカウントでのみ保存および表示できるようになります。

ステップ 7 [検索（Search）] をクリックして、検索を開始します。
検索結果は、現在の時間範囲によって制限されている、カスタム テーブルのデフォルトのワークフローに表示されます（該当する場合）。