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

システムがネットワークに関する情報を収集し、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、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、[カウント別のネットワーク アプリケーション（Network Applications by Count）] ワークフローの各ページのカラムは、[アプリケーション（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。

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。システムは、いくつかのシステム定義のカスタムテーブルとともに配布されますが、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、システムは、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ともに配布されます。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
ホストとサーバー（Hosts with Servers）	ホスト テーブルおよびサーバー テーブルのフィールドを含み、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やこれらのアプリケーションを実行す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します。

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
アプリケーション	• 相関イベント（Correlation Events） • 侵入イベント • 接続のサマリーデータ（Connection Summary Data） • ホスト属性（Host Attributes） • アプリケーションの詳細（Application Details） • 検出イベント • ホスト（Hosts） • サーバー • 許可（Allow） イベントの一覧表示

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
相関イベント（Correlation Events）	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts）
侵入イベント	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts） • サーバー
接続のサマリーデータ（Connection Summary Data）	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts） • サーバー
ホストの侵害の兆候（Host Indications of Compromise）	• アプリケーション • アプリケーションの詳細（Application Details） • キャプチャファイル（Captured Files） • 接続のサマリーデータ（Connection Summary Data） • 相関イベント（Correlation Events） • 検出イベント • ホスト属性（Host Attributes） • ホスト（Hosts） • 侵入イベント • セキュリティインテリジェンスイベント（Security Intelligence Events） • サーバー • 許可（Allow）イベントの一覧表示

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
ホスト属性（Host Attributes）	• アプリケーション • 相関イベント（Correlation Events） • 侵入イベント • 接続のサマリーデータ（Connection Summary Data） • アプリケーションの詳細（Application Details） • 検出イベント • ホスト（Hosts） • サーバー • 許可（Allow） イベントの一覧表示
アプリケーションの詳細（Application Details）	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts）
検出イベント	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts）
セキュリティ インテリジェンス イベント（Security Intelligence Events）	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts） • サーバー

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（Hosts）	• アプリケーション • 相関イベント（Correlation Events） • 侵入イベント • 接続のサマリーデータ（Connection Summary Data） • ホスト属性（Host Attributes） • アプリケーションの詳細（Application Details） • 検出イベント • サーバー • 許可（Allow）イベントの一覧表示
サーバー	• アプリケーション • 侵入イベント • 接続のサマリーデータ（Connection Summary Data） • ホスト属性（Host Attributes） • ホスト（Hosts）
許可（Allow）イベントの一覧表示	• アプリケーション • ホスト属性（Host Attributes） • ホスト（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。

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。

ユーザー定義のカスタム 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 Management Center からカスタム テーブルをエクスポートし、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、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　[ホスト（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、[相関イベント（Correlation Events）] テーブルと [ホスト（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、[相関イベント（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 [ホスト（Hosts）] テーブル 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
- 送信元ホストのシビラティ（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

手順

ステップ 1 **[分析（Analysis）] > [詳細（Advanced）] > [カスタムテーブル（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）]、[ホストのシビラティ（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

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。

手順

ステップ 1 **[分析（Analysis）]** > **[詳細（Advanced）]** > **[カスタムテーブル（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（Edit）]**（）をクリックします。

代わりに [表示（View）]（） 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 削除するフィールドの横にある[削除（Delete）]（）をクリックして、テーブルからフィールドを削除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削除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

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。

手順

ステップ 1 **[分析（Analysis）]** > **[詳細（Advanced）]** > **[カスタムテーブル（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（Delete）]（）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 テーブルに基づくワークフローの表示

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。

手順

ステップ 1 **[分析（Analysis）] > [詳細（Advanced）] > [カスタムテーブル（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（View）]（👁）をクリックします。

カスタム テーブルの検索

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。

手順

ステップ 1 **[分析（Analysis）] > [詳細（Advanced）] > [カスタムテーブル（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（View）]（👁）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（Object）]**（+）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 カスタムユーザー ロールのデータの制限として検索を使用する場合は、必ずプライベート検索として保存する**必要**があります。

ステップ 6 必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [保存（Save）] をクリックして、検索条件を保存します。[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）。

カスタムテーブルの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
カスタムテーブルの接続イベントのサポートが削除されました	6.6	任意（Any）	接続イベントを含むカスタムテーブルを作成することはできなくなりました。 バージョン 6.6 にアップグレードした場合、接続イベントを持つ既存のテーブルは廃止としてリストされ、データは表示されず、エクスポートまたは編集することはできません。既存のレポート、カスタムワークフロー、およびダッシュボードには廃止されたテーブルが含まれる場合があり、それらを確認することができます。 変更された画面：[Analysis] > [Advanced] > [Custom Tables] と、カスタムテーブルを追加または編集するためのページ。 影響を受けるプラットフォーム：Management Center

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。