カスタム ワークフロー

次のトピックでは、カスタム ワークフローの使用方法について説明します。

カスタム ワークフローの概要

シスコが提供する事前定義のカスタム ワークフローがニーズに合わない場合は、カスタム ワークフローを作成して管理することができます。

カスタム ワークフローは、組織に特有のニーズに合わせて作成するワークフローです。カスタム ワークフローを作成するときには、ワークフローのベースとなるイベント（またはデータベース テーブル）の種類を選択します。Firepower Management Center では、カスタム ワークフローをカスタム テーブルのベースにすることができます。また、カスタム ワークフローに含まれるページを選択することもできます。カスタム ワークフローには、ドリルダウン、テーブル ビュー、ホストまたはパケット ビューのページを含めることができます。

イベント評価プロセスが変わった場合には、新しいニーズを満たすようにカスタム ワークフローを編集することができます。事前定義のワークフローは編集できないことに注意してください。

ヒント 任意のイベント タイプについて、デフォルト ワークフローとしてカスタム ワークフローを設定することができます。

保存済みカスタム ワークフロー

Firepower Management Center は、変更可能な定義済みのワークフローの他に保存済みのカスタム ワークフローを含みます。それぞれのワークフローは、カスタム テーブルに基づき、いずれも変更可能です。

マルチドメイン展開では、これらの保存されたワークフローは、グローバル ドメインに属し、下位ドメインでは変更できません。

表 *1*: 保存済みカスタム ワークフロー

ワークフロー名	説明
影響、優先度、およびホストの重大度に基づいたイベント（Events by Impact, Priority, and Host Criticality）	このワークフローを使用して、ネットワークにとって重要で、現在は脆弱な状態にあり、攻撃を受ける可能性があるようなホストをすばやく見つけて表示することができます。 このワークフローは、宛先重要度のカスタム テーブルのある侵入イベントに基づいています。
優先度および分類に基づいたイベント（Events by Priority and Classification）	このワークフローは、イベントおよびイベントのタイプを、イベントの優先度の順に表示し、各イベントが発生した回数も示します。 このワークフローは、侵入イベントのカスタム テーブルに基づきます。
宛先、影響、およびホストの重大度に基づいたイベント（Events with Destination, Impact, and Host Criticality）	このワークフローを使用して、ネットワークにとって重要で、現在脆弱な状態にあるホスト上の最近の攻撃を見つけることができます。 このワークフローは、宛先重要度のカスタム テーブルのある侵入イベントに基づいています。
サーバに接続しているホストのデフォルト ワークフロー（Hosts with Servers Default Workflow）	このワークフローを使用して、[サーバに接続しているホスト（Hosts with Servers）] カスタム テーブルの基本情報をすばやく表示することができます。 このワークフローは、サーバのカスタム テーブルのあるホストに基づきます。
宛先の重大度に基づく侵入イベントのデフォルト ワークフロー（Intrusion Events with Destination Criticality Default Workflow）	このワークフローを使用して、宛先の重大度に基づく侵入イベント（Intrusion Events with Destination Criticality）カスタム テーブルの基本情報をすばやく表示することができます。 このワークフローは、宛先重要度のカスタム テーブルのある侵入イベントに基づいています。

ワークフロー名	説明
送信元の重大度に基づく侵入イベントのデフォルト ワークフロー（Intrusion Events with Source Criticality Default Workflow）	このワークフローを使用して、[送信元の重大度に基づく侵入イベント（Intrusion Events with Source Criticality）] カスタム テーブルの基本情報をすばやく表示することができます。 このワークフローは、送信元重要度のカスタム テーブルのある侵入イベントに基づいています。
サーバとホストの詳細（Server and Host Details）	このワークフローを使用して、ネットワーク上で最も頻繁に使用されているサーバ、およびそれらのサーバを実行しているホストを決定できます。 このワークフローは、サーバのカスタム テーブルのあるホストに基づきます。

カスタム ワークフローの作成

シスコが提供する事前定義のカスタム ワークフローがニーズに合わない場合は、カスタム ワークフローを作成することができます。

ヒント 新しいカスタム ワークフローを作成する代わりに、別のアプライアンスからカスタム ワークフローをエクスポートし、それを自身のアプライアンスへインポートすることができます。その後でニーズに合わせて、インポートしたワークフローを編集することができます。

カスタム ワークフローを作成する場合は、次の操作を行います。

- ワークフローのソースとなるテーブルを選択する
- ワークフローの名前を指定する
- ワークフローにドリル ダウン ページおよびテーブル ビュー ページを追加する

ワークフローの各ドリル ダウン ページでは、次のことができます。

- Web インターフェイスのページの上部に表示される名前を指定する
- 1 ページにつき最大 5 個のカラムを含める
- デフォルトのソート順（昇順または降順）を指定する

ワークフロー ページの順序において、任意の場所にテーブル ビュー ページを追加することができます。これらのページには編集可能なプロパティ（ページ名、ソート順、ユーザ定義可能なカラム位置など）がありません。

（注） カスタム ワークフローには、イベントのドリル ダウン ページまたはテーブル ビューを少なくとも 1 つ追加する必要があります。

（注） テーブル タイプに [脆弱性（Vulnerabilities）] を選択し、テーブル カラムに [IP アドレス（IP Address）] を追加しても、検索機能を使用して特定の IP アドレスまたはアドレスのブロックを表示するようワークフローを制約しない限り、カスタム ワークフローを使用して脆弱性を表示する場合に [IP アドレス（IP Address）] カラムは表示されません。

カスタム ワークフローの最終ページは、次の表に記載されているように、ワークフローのベースにしているテーブルによって異なります。これらの最終ページは、ワークフローを作成したときにデフォルトで追加されます。

表 *2:* カスタム ワークフローの最終ページ

イベント/アセット タイプ	最終ページ
ディスカバリ イベント	ホスト
脆弱性	脆弱性の詳細
サードパーティの脆弱性	ホスト
Users	Users
侵害の兆候	ホストまたはユーザ
侵入イベント	パケット

システムは、他の種類のイベント（監査ログやマルウェア イベントなど）に基づくカスタム ワークフローには最終ページを追加しません。

接続データに基づくカスタム ワークフローもその他のカスタム ワークフローと同様です。ただし、接続データに基づくカスタム ワークフローには接続の要約データを含むドリル ダウン ページや個々の接続とテーブル ビュー ページを含むドリル ダウン ページを入れることができます。

非接続データに基づくカスタム ワークフローの作成

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	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 **[分析（Analysis）] > [カスタム（Custom）] > [カスタムワークフロー（Custom Workflows）]** を選択します。

ステップ 2 [カスタム ワークフローの作成（Create Custom Workflow）] をクリックします。

ステップ 3 [名前（Name）] フィールドにワークフローの名前を入力します。

ステップ 4 必要に応じて、[説明（Description）] を入力します。

ステップ 5 [テーブル（Table）] ドロップダウン リストから、対象とするテーブルを選択します。

ステップ 6 ワークフローに1つ以上のドリルダウン ページを追加する場合は、[ページの追加（Add Page）] をクリックします。

ステップ 7 [ページ名（Page Name）] フィールドにページの名前を入力します。

ステップ 8 [カラム 1（Column 1）] で、ソートの優先順位およびテーブルのカラムを選択します。このカラムは、ページの最も左のカラムとして表示されます。

例：

たとえば、対象とする宛先ポートを示すページを作成し、カウントでページをソートするには、[ソートの優先順位（Sort Priority）] ドロップダウン リストから [2] を選択し、[フィールド（Field）] ドロップダウン リストから [宛先ポート/ICMP コード（Destination Port/ICMP Code）] を選択します。

ステップ 9 ページに表示するすべてのフィールドが指定されるまで、含めるフィールドの選択とソートの優先順位の設定を続けます。

ステップ 10 ワークフローにテーブル ビュー ページを追加するには、[テーブル ビューの追加（Add Table View）] をクリックします。

ステップ 11 [保存（Save）] をクリックします。

カスタム接続データ ワークフローの作成

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	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

接続データに基づいたカスタム ワークフローは他のカスタム ワークフローと似ていますが、ドリルダウン ページとテーブル ビュー ページだけでなく、接続データ グラフのページも含めることができます。必要に応じて、ワークフローにそれぞれのタイプのページを任意の数だけ、任意の順序で含めることができます。それぞれの接続データ グラフのページには1つのグラフ（線グラフ、棒グラフ、または円グラフ）が含まれます。線グラフと棒グラフには、複数のデータセットを含めることができます。

手順

ステップ 1 **[分析（Analysis）] > [カスタム（Custom）] > [カスタムワークフロー（Custom Workflows）]** を選択します。

ステップ 2 [カスタム ワークフローの作成（Create Custom Workflow）] をクリックします。

ステップ 3 [名前（Name）] フィールドにワークフローの名前を入力します。

ステップ 4 必要に応じて、[説明（Description）] を入力します。

ステップ 5 [テーブル（Table）] ドロップダウン リストから、[接続イベント（Connection Events）] を選択します。

ステップ 6 ワークフローに 1 つ以上のドリルダウン ページを追加する場合は、次の 2 つのオプションがあります。

- 個々の接続に関するデータが含まれているドリルダウン ページを追加するには、[ページの追加（Add Page）] をクリックします。
- 接続の概要データが含まれているドリルダウン ページを追加するには、[サマリー ページの追加（Add Summary Page）] をクリックします。

ステップ 7 [ページ名（Page Name）] フィールドにページの名前を入力します。

ステップ 8 [カラム 1（Column 1）] で、ソートの優先順位およびテーブルのカラムを選択します。このカラムは、ページの最も左のカラムとして表示されます。

ステップ 9 ページに表示するすべてのフィールドが指定されるまで、含めるフィールドの選択とソートの優先順位の設定を続けます。

例：

たとえば、監視対象ネットワーク経由で転送されるトラフィックの量を表示するページを作成し、トラフィックの転送量が最も多い応答側によってページをソートするには、[ソートの優先順位（Sort Priority）] ドロップダウン リストで [1] を選択し、[フィールド（Field）] ドロップダウン リストで [応答側のバイト数（Responder Bytes）] を選択します。

ステップ 10 ワークフローに 1 つ以上のグラフ ページを追加する場合は、[グラフの追加（Add Graph）] をクリックします。

ステップ 11 [グラフ名（Graph Name）] フィールドにページの名前を入力します。

ステップ 12 ページに含めるグラフのタイプを選択します。

- 線グラフ（  ）
- 棒グラフ（  ）
- 円グラフ（  ）

ステップ 13 グラフの X 軸と Y 軸を選択し、グラフ化するデータの種類を指定します。

円グラフでは、X 軸は独立変数を表し、Y 軸は従属変数を表します。

ステップ 14 グラフに含めるデータセットを選択します。

円グラフには 1 つのデータセットしか含めることができないことに注意してください。

ステップ 15 接続データのテーブル ビューを追加するには、[テーブル ビューの追加（Add Table View）] をクリックします。

テーブル ビューは設定できません。

ステップ 16 [保存（Save）] をクリックします。

カスタム ワークフローの使用と管理

ワークフローが、事前定義のイベント テーブルまたはカスタム テーブルのいずれに基づいているかによって、ワークフローの表示に使用する方法が異なります。

カスタム ワークフローが事前定義のイベント テーブルに基づいている場合は、アプライアンスに付属しているワークフローにアクセスするのと同じ方法でアクセスします。たとえば、ホスト テーブルに基づいているカスタム ワークフローにアクセスするには、**[分析（Analysis）]** > **[ホスト（Hosts）]** > **[ホスト（Hosts）]** を選びます。また、カスタム ワークフローがカスタム テーブルに基づいている場合は、[カスタム テーブル（Custom Tables）] ページからアクセスする必要があります。

イベント評価プロセスが変わった場合には、新しいニーズを満たすようにカスタム ワークフローを編集することができます。事前定義のワークフローは編集できないことに注意してください。

ヒント 任意のイベント タイプについて、デフォルト ワークフローとしてカスタム ワークフローを設定することができます。

事前定義されたテーブルに基づいたカスタム 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	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint/Any Security Analyst（ワークフローに応じて異なります）

手順

ステップ 1 ワークフローの選択の説明に従って、カスタム ワークフローのベースとなるテーブルについて、適切なメニュー パスとオプションを選択します。

ステップ 2 カスタム ワークフローも含め、別のワークフローを使用するには、現在のワークフロー タイトルの横にある [(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 イベントが表示されず、ワークフローを時間によって制約できる場合は、時間範囲の調整が必要なことがあります（イベント時間の制約を参照）。

カスタム テーブルに基づいたカスタム 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	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

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 ワークフローが表示されます。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 ワークフローも表示されますが、これは編集できません。下位のドメインのカスタム ワークフロー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）] > [カスタム（Custom）] > [カスタムテーブル（Custom Tables）]**を選択します。

ステップ 2 表示するカスタム テーブルの隣にある表示アイコン（  ）をクリックするか、またはカスタム テーブルの名前をクリックします。

ステップ 3 カスタム ワークフローも含め、別のワークフローを使用するには、現在のワークフロー タイトルの横にある [(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 4 イベントが表示されず、ワークフローを時間によって制約できる場合は、時間範囲の調整が必要なことがあります（イベント時間の制約を参照）。

カスタム ワークフローの編集

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	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

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 ワークフローが表示されます。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 ワークフローも表示されますが、これは編集できません。下位のドメインのカスタム ワークフロー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）] > [カスタム（Custom）] > [カスタムワークフロー（Custom Workflows）]** を選択します。

ステップ 2 編集するワークフロー名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 ワークフローに必要な変更を加えます。

ステップ 4 [保存（Save）] をクリックします。