カスタム テーブルの使用

FireSIGHT システムがネットワークに関する情報を収集し、Defense 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、Defense 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。たとえば、定義済みの [ホスト属性(Host Attributes)] テーブルのホスト重大度情報と、定義済みの [接続データ(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。カスタム ワークフローの作成の詳細については、カスタム ワークフローの作成 (58-44 ページ)を参照してください。

以下のセクションでは、独自のカスタム テーブルを作成して使用する方法について説明します。

カスタム テーブルについて

ライセンス: FireSIGHT

カスタム テーブルには、2 つ以上の定義済みのテーブルのフィールドが含まれます。FireSIGHT システムでは、システム定義のカスタム テーブルが多数提供されていますが、自分のニーズに合った情報だけを含むカスタム テーブルをさらに作成できます。

たとえば、FireSIGHT システムでは、侵入イベント データをホスト データと相関させるシステム定義のカスタム テーブルが提供されているので、重要なシステムに影響を与えるイベントを検索して、その検索の結果を 1 つのワークフローで表示できます。次の表は、システムに付属しているカスタム テーブルについて説明します。

表 59-1　システム定義のカスタム テーブル

テーブル	説明
ホストとサーバ（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、[ホスト（Hosts）] および [サーバ（Servers）] テーブルのフィールドが含まれます。
侵入イベントと送信先の致命度（Intrusion Events with Destination Criticality）	侵入イベントに関する情報と、各侵入イベントに関係する宛先ホストのホスト重大度に関する情報を提供する、[侵入イベント（Intrusion Events）] および [ホスト（Hosts）] テーブルのフィールドが含まれます。 ヒント　このテーブルは、ホスト重大度が高い宛先ホストが関係する侵入イベントを検索するために使用します。
侵入イベントと送信元の致命度（Intrusion Events with Source Criticality）	侵入イベントに関する情報と、各侵入イベントに関係する送信元ホストのホスト重大度に関する情報を提供する、[侵入イベント（Intrusion Events）] および [ホスト（Hosts）] テーブルのフィールドが含まれます。 ヒント　このテーブルは、ホスト重大度が高い送信元ホストが関係する侵入イベントを検索するために使用します。

可能なテーブルの結合について

ライセンス：FireSIGHT + Protection

カスタム テーブルを作成する場合、関連データを含む定義済みのテーブルのフィールドを結合できます。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。3 つ以上の定義済みのカスタム テーブルのフィールドを結合してカスタム テーブルを作成できることに留意してください。

表 59-2　カスタム テーブルの結合

以下のテーブルのフィールドを	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） • アプリケーション詳細（Application Details） • 検出イベント（Discovery Events） • 接続イベント • ホスト（Hosts） • サーバ • ホワイトリスト イベント（White List Events）

表 59-2　カスタム テーブルの結合(続き)

以下のテーブルのフィールドを	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
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
侵害の兆候(Indications of Compromise)	• アプリケーション • アプリケーション詳細(Application Details) • キャプチャ ファイル(Captured Files) • 接続イベント • 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(Discovery Events) • 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 • ホワイトリスト イベント(White List Events)

表 59-2　カスタム テーブルの結合(続き)

以下のテーブルのフィールドを	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) • アプリケーション詳細(Application Details) • 検出イベント(Discovery Events) • 接続イベント • ホスト(Hosts) • サーバ • ホワイトリスト イベント(White List Events)
アプリケーション詳細(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(Discovery Events)	• アプリケーション • ホスト属性(Host Attributes) • ホスト(Hosts)
接続イベント	• アプリケーション • ホスト属性(Host Attributes) • ホスト(Hosts) • サーバ
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

表 59-2　カスタム テーブルの結合（続き）

以下のテーブルのフィールドを	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） • アプリケーション詳細（Application Details） • 検出イベント（Discovery Events） • 接続イベント • サーバ • ホワイトリスト イベント（White List Events）
サーバ	• 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） • 接続イベント • ホスト（Hosts）
ホワイトリスト イベント（White List Events）	• 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。たとえば、定義済みの [侵入イベントと送信先の致命度（Intrusion Events with Destination Criticality）] カスタム テーブルは、[侵入イベント（Intrusion Events）] テーブルと [ホスト（Hosts）] テーブルのフィールドを結合します。[侵入イベント（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、[侵入イベント（Intrusion Events）] テーブルと [ホスト（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、[ホスト（Hosts）] テーブルから表示するデータが [侵入イベント（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。また、定義済みのテーブルで行うのと同じように、カスタム テーブルに基づいてレポートを生成することもできます。

カスタム テーブルの作成の詳細については、以下を参照してください。

カスタム テーブルの作成

ライセンス：FireSIGHT

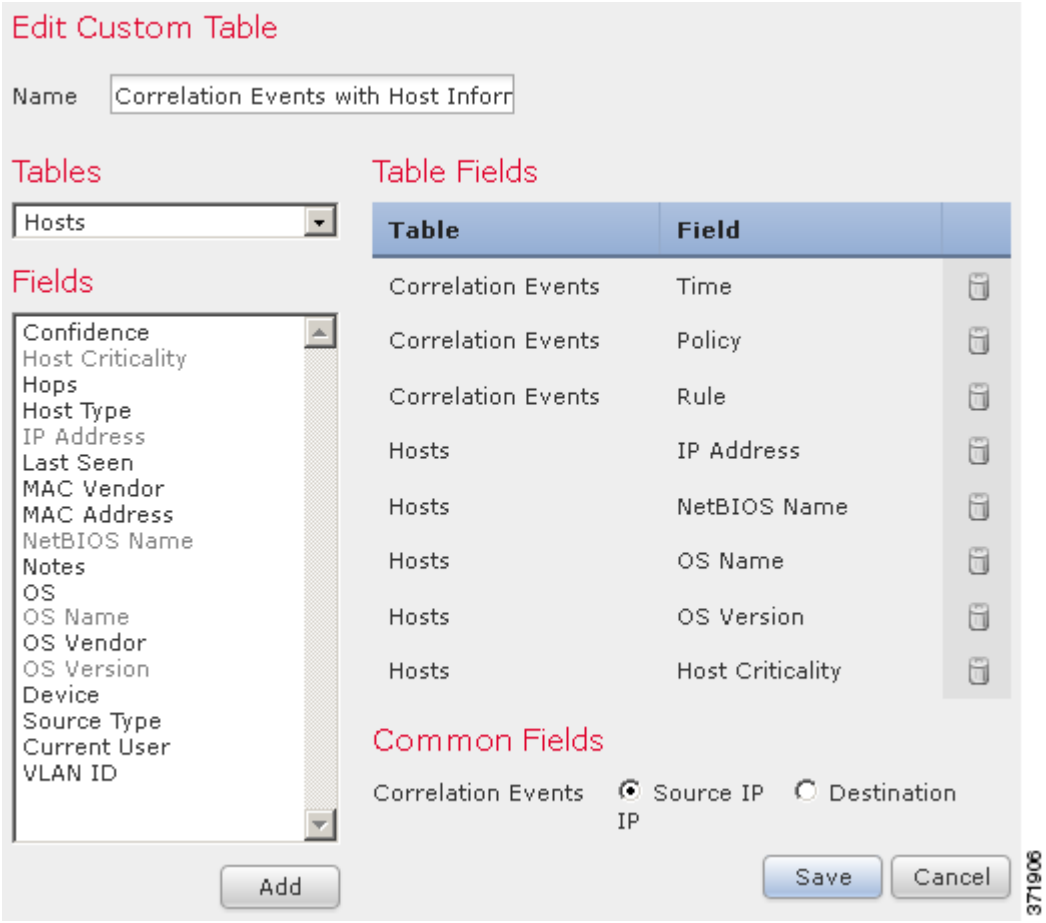
さまざまなテーブルのフィールドを結合することにより、ネットワークのアクティビティの分析が向上する場合、カスタム テーブルを作成できます。

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 Defense Center からカスタム テーブルをエクスポートし、Defense Center にインポートできます。その後、必要に合わせて、インポートしたカスタム テーブルを編集できます。詳細については、設定のインポートおよびエクスポート（A-1 ページ）を参照してください。

カスタム テーブルを作成するには、FireSIGHT 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　[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。次の情報が表示されます。

- 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じようなカスタム テーブルを作成することもできます。

上述の例のカスタム テーブルを作成する方法:

アクセス: Admin

手順 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。

[カスタム テーブル(Custom Tables)] ページが表示されます。

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

[カスタム テーブルの作成(Create Custom Table)] ページが表示されます。

手順 3　[名前(Name)] フィールドに、`Correlation Events with Host Information (Src IP)` などのカスタム テーブルの名前を入力します。

手順 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。

[相関イベント(Correlation Events)] テーブルのフィールドが [フィールド(Fields)] リストに表示されます。

手順 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。

手順 6　ステップ 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。しかし、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、フィールドを一度に 1 つずつ追加します。

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

[ホスト(Hosts)] テーブルのフィールドが [フィールド(Fields)] リストに表示されます。これらのフィールドの詳細については、ホスト テーブルについて(50-22 ページ)を参照してください。

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

手順 9　[相関イベント(Correlation Events)] の隣にある [共通フィールド(Common Fields)] で、[ソース 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)用にステップ 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、この手順に従うものの、[ソース IP(Source IP)] ではなく、[宛先 IP(Destination IP)] を選択します。

手順 10　[保存(Save)] をクリックします。

カスタム テーブルが保存されます。

カスタム テーブルの変更

ライセンス：FireSIGHT

ニーズの変化に応じて、カスタム テーブルのフィールドを追加したり削除したりできます。

カスタム テーブルを変更する方法：

アクセス：Any/Admin

手順 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。

[カスタム テーブル（Custom Tables）] ページが表示されます。

手順 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。

[カスタム テーブルの編集（Edit Custom Table）] 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、カスタム テーブルの作成（59-6 ページ）を参照してください。

手順 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出されます。

手順 4　必要に応じて他の変更を行い、[保存（Save）] をクリックします。

カスタム テーブルが更新されます。

カスタム テーブルの削除

ライセンス：FireSIGHT

必要なくなったカスタム テーブルを削除できます。カスタム テーブルを削除すると、そのカスタム テーブルを使用する保存済み検索も削除されます。

カスタム テーブルを削除する方法：

アクセス：Any/Admin

手順 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。

[カスタム テーブル（Custom Tables）] ページが表示されます。

手順 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。

テーブルが削除されます。

カスタム テーブルに基づいたワークフローの表示

ライセンス：FireSIGHT

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。詳細については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

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。詳細については、ワークフローのページの使用（58-21 ページ）を参照してください。

カスタム テーブルに基づいたワークフローを表示する方法：

アクセス：Any/Admin

手順 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。

[カスタム テーブル（Custom Tables）] ページが表示されます。

手順 2　表示するワークフローが基づくカスタム 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 テーブルのデフォルトのワークフローの最初のページが表示されます。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にある[ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルトのワークフローを指定する方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。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の設定（58-26 ページ）を参照してください。

カスタム テーブルの検索

ライセンス：FireSIGHT

カスタム テーブルの検索を作成して保存できます。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。カスタム テーブルを削除すると、そのカスタム テーブル用に保存したすべての検索も削除されるので注意してください。

使用できる検索基準は、カスタム テーブルを作成するために使用した定義済みのテーブルの基準と同じです。使用できる検索基準の詳細については、以下の表に示されているセクションを参照してください。

表 59-3　テーブルの検索基準

検索基準	参照先
監査イベント（Audit Events）	監査レコードの検索（69-9 ページ）
アプリケーション詳細（Application Details）	アプリケーションの詳細の検索（50-53 ページ）
相関イベント（Correlation Events）	相関イベントの検索（51-64 ページ）
接続データ（Connection Data）	接続およびセキュリティ インテリジェンスのデータの検索（39-35 ページ）
ホスト（Hosts）	ホストの検索（50-27 ページ）
ホスト属性（Host Attributes）	ホスト属性の検索（50-33 ページ）
ホストとアプリケーション（Hosts with Applications）	ホストの検索（50-27 ページ）およびサーバの検索（50-43 ページ）
侵入イベント	侵入イベントの検索（41-45 ページ）
侵入イベントと送信先の致命度（Intrusion Events with Destination Criticality）	侵入イベントの検索（41-45 ページ）およびホストの検索（50-27 ページ）
侵入イベントと送信元の致命度（Intrusion Events with Source Criticality）	侵入イベントの検索（41-45 ページ）およびホストの検索（50-27 ページ）
ステータス イベント（Status Events）	修復ステータス イベントの検索（54-23 ページ）
検出イベント（Discovery Events）	ディスカバリ イベントの検索（50-18 ページ）
ユーザ イベント（User Events）	ユーザ アクティビティの検索（50-75 ページ）
ルール更新のインポート ログ（Rule Update Import Log）	ルール アップデートのインポート ログの検索（66-29 ページ）
アプリケーション	アプリケーションの検索（50-48 ページ）
セキュリティ インテリジェンス イベント（Security Intelligence Events）	接続およびセキュリティ インテリジェンスのデータの検索（39-35 ページ）
ユーザ（Users）	ユーザの検索（50-70 ページ）
脆弱性（Vulnerabilities）	脆弱性の検索（50-59 ページ）
ホワイトリスト イベント（White List Events）	コンプライアンス ホワイト リスト イベントの検索（52-36 ページ）
ホワイトリスト違反（White List Violations）	ホワイト リスト違反の検索（52-41 ページ）

テーブル検索にそれらの基準を実装するには、次の手順を参照してください。

カスタム テーブルで検索を実行する方法:

アクセス: Any/Admin

手順 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。

[カスタム テーブル(Custom Tables)] ページが表示されます。

手順 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。

カスタム テーブルのデフォルトの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、ワークフローのタイトルの横の [ワークフロー切り替え(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(71-3 ページ)を参照してください。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の設定(58-26 ページ)を参照してください。

手順 3　[検索(Search)] をクリックします。

カスタム テーブルの検索ページが表示されます。

ヒント　さまざまな種類のイベントまたはデータをデータベースで検索するには、[テーブル(Table)] ドロップダウンリストから選択します。

手順 4　該当するフィールドに検索基準を入力します。検索基準を選択する方法の詳細については、テーブルの検索基準を参照してください。

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。特別な検索構文、検索でのオブジェクトの使用、検索の保存およびロードなど、検索の詳細については、検索設定の実行と保存(60-1 ページ)を参照してください。

手順 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、本人だけ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。

手順 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。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [保存(Save)] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され([プライベート(Private)] を選択した場合は本人のアカウントでのみ閲覧可能)、後で実行できます。

- 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、[新規として保存(Save As New)] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [保存(Save)] をクリックします。検索が保存され([プライベート(Private)] を選択した場合は本人のアカウントでのみ閲覧可能)、後で実行できます。

手順 7　検索を開始するには、[検索(Search)] ボタンをクリックします。

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 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 [ワークフロー切り替え(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(71-3 ページ)を参照してください。