CHAPTER 58

ワークフローの概要と使用

ワークフローは Defense Center Web インターフェイス上でユーザに合わせて作成された一連のデータ ページです。アナリストはワークフローを使用して、システムで生成されたイベントを評価できます。Defense Center には、次の 3 つのタイプのワークフローがあります。

- *事前定義ワークフロー*: システムにインストールされているプリセット ワークフローで、ユーザは変更または削除できません。
- *保存済みのカスタム ワークフロー*: 事前に定義されているカスタム ワークフローで、ユーザは変更または削除できます。
- *カスタム ワークフロー*: ユーザが作成し、自身のニーズに合わせてカスタマイズするワークフローです。

たとえば、侵入イベントを分析する場合は、このタスク用に作成されたいくつかの事前定義ワークフローから選択することができます。

ワークフローに表示されるデータは、ほとんどの場合、管理対象デバイスのライセンスおよび導入方法、データを提供する機能を設定しているかどうか(シリーズ 2 アプライアンスおよび Blue Coat X-Series 向け Cisco NGIPS の場合は、アプライアンスがデータを提供する機能をサポートしているかどうか)によって異なります。たとえば、DC500 Defense Center およびシリーズ 2 のデバイスは、カテゴリおよびレピュテーションによる URL フィルタリングをサポートしていないため、DC500 Defense Center ではこの機能のデータが表示されず、シリーズ 2 デバイスはこのデータを検出しません。

事前定義ワークフローおよびカスタム ワークフローの使用に関する詳細は、次の項を参照してください。

- ワークフローのコンポーネント(58-2 ページ)
- ワークフローの使用(58-18 ページ)
- カスタムワークフローの使用(58-44 ページ)

ヒント カスタム ワークフローを、イベント レポートのベースとして使用することもできます。詳細については、レポートの操作(57-1 ページ)を参照してください。

ワークフローのコンポーネント

ライセンス: 任意（Any）

ワークフローには、以下の項に記載されているように、複数のタイプのページを含めることができます。

テーブル ビュー

テーブル ビューには、ワークフローのベースとなるデータベースの各フィールドに対するカラムが含まれています。

たとえば、ディスカバリ（検出）イベントのテーブル ビューには、[時刻（Time）]、[イベント（Event）]、[IP アドレス（IP Address）]、[ユーザ（User）]、[MAC アドレス（MAC Address）]、[MAC ベンダー（MAC Vendor）]、[ポート（Port）]、[説明（Description）]、および [デバイス（Device）] カラムが含まれています。

また、サーバのテーブル ビューには、[前回の使用（Last Used）]、[IP アドレス（IP Address）]、[ポート（Port）]、[プロトコル（Protocol）]、[アプリケーション プロトコル（Application Protocol）]、[ベンダー（Vendor）]、[バージョン（Version）]、[Web アプリケーション（Web Application）]、[アプリケーション リスク（Application Risk）]、[ビジネス関連性（Business Relevance）]、[ヒット件数（Hits）]、[ソース タイプ（Source Type）]、[デバイス（Device）]、および [現在のユーザ（Current User）] カラムが含まれています。

ドリルダウン ページ

ドリルダウン ページには、データベースで使用できるカラムのサブセットが含まれています。

たとえば、検出イベントのドリルダウン ページには、[IP アドレス（IP Address）]、[MAC アドレス（MAC Address）]、および [時刻（Time）] カラムのみが含まれています。また、侵入イベントのドリルダウン ページには、[優先度（Priority）]、[影響フラグ（Impact Flag）]、[インライン結果（Inline Result）]、および [メッセージ（Message）] カラムが含まれています。

一般的にドリルダウン ページは、テーブル ビューのページに移動する前にユーザが使用して調査対象を絞り込むための中間ページです。

グラフ

接続データに基づくワークフローには、グラフ ページ（*接続グラフ*とも呼ばれる）を含めることができます。

たとえば接続グラフには、一定期間にシステムで検出された接続の数を示す線グラフを表示することができます。一般的に接続グラフは、ドリルダウン ページと同様に、ユーザが調査対象を絞り込むために使用する中間ページです。詳細については、接続グラフの使用（39-18 ページ）を参照してください。

最終ページ

ワークフローの最終ページは、ワークフローがベースとするイベントのタイプによって異なります。

- ホスト ビューは、アプリケーション、アプリケーションの詳細、ディスカバリ（検出）イベント、ホスト、侵入の痕跡/兆候（IOC）、サーバ、または任意のタイプの脆弱性に基づくワークフローの最終ページです。このページからホスト プロファイルを表示することにより、ユーザは、複数のアドレスを持つホストに関連付けられているすべての IP アドレス上のデータを簡単に表示することができます。詳細については、ホスト プロファイルの使用（49-1 ページ）を参照してください。
- ユーザの詳細ビューは、ユーザ、およびユーザ アクティビティに基づいたワークフローの最終ページです。詳細については、ユーザの詳細とホストの履歴について（50-68 ページ）を参照してください。

– 脆弱性の詳細ビューは、Cisco の脆弱性に基づいたワークフローの最終ページです。詳細については、脆弱性の詳細の表示（49-31 ページ）を参照してください。

– パケット ビューは、侵入イベントに基づいたワークフローの最終ページです。詳細については、パケット ビューの使用（41-25 ページ）を参照してください。

他の種類のイベント（監査ログ イベントやマルウェア イベントなど）に基づいたワークフローには、最終ページがありません。

ワークフローの詳細については、以下の項を参照してください。

- 事前定義ワークフローとカスタム ワークフローの比較（58-3 ページ）
- 事前定義テーブルとカスタム テーブルのワークフローの比較（58-4 ページ）
- 事前定義の侵入イベント ワークフロー（58-4 ページ）
- 事前定義のマルウェア ワークフロー（58-7 ページ）
- 事前定義のファイル ワークフロー（58-7 ページ）
- 事前定義されたキャプチャ ファイル ワークフロー（58-8 ページ）
- 事前定義の接続データ ワークフロー（58-8 ページ）
- 事前定義のセキュリティ インテリジェンス ワークフロー（58-10 ページ）
- 事前定義のホスト ワークフロー（58-10 ページ）
- 事前定義の侵入の痕跡ワークフロー（58-11 ページ）
- 事前定義のアプリケーション ワークフロー（58-11 ページ）
- 事前定義のアプリケーション詳細ワークフロー（58-12 ページ）
- 事前定義のサーバ ワークフロー（58-13 ページ）
- 事前定義のホスト属性ワークフロー（58-13 ページ）
- 事前定義のディスカバリ イベント ワークフロー（58-14 ページ）
- 事前定義のユーザ ワークフロー（58-14 ページ）
- 事前定義の脆弱性ワークフロー（58-14 ページ）
- 事前定義のサードパーティの脆弱性ワークフロー（58-15 ページ）
- 事前定義の相関およびホワイトリスト ワークフロー（58-15 ページ）
- 事前定義のシステム ワークフロー（58-16 ページ）
- 保存済みのカスタム ワークフロー（58-16 ページ）

事前定義ワークフローとカスタム ワークフローの比較

ライセンス：任意（Any）

FireSIGHT システムには、（これ以降の項で説明されている）*事前定義*ワークフローのセットが備わっており、ユーザはこれを使用して、イベントや収集した他のデータを分析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。Defense 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。

Defense Center には、いくつかの*保存済みカスタム ワークフロー*が付属しています。このワークフローは、Defense Center に付属している保存済みのカスタム テーブルに基づいています。事前定義のテーブルとカスタム テーブルに基づいたワークフローの違いについては、次のセクション事前定義テーブルとカスタム テーブルのワークフローの比較で説明します。

事前定義テーブルとカスタム テーブルのワークフローの比較

ライセンス：FireSIGHT

カスタム テーブルの機能を使用して、複数のイベント タイプのデータを使用するテーブルを作成することができます。これにより、たとえば、ユーザが侵入イベントのデータと検出データを関連付けるテーブルおよびワークフローを作成して、重要なシステムに影響を及ぼすイベントを簡単に検索できるようになるため、役立ちます。カスタム テーブルの作成については、カスタム テーブルの使用（59-1 ページ）を参照してください。

それぞれのカスタム テーブルにはデフォルトでワークフローが含まれており、これを使用して、テーブルに関連付けられているイベントを表示することができます。ワークフローの機能は、使用するテーブルのタイプによって異なります。たとえば、侵入イベント テーブルに基づいたカスタム テーブルのワークフローは、必ずパケット ビューで終了します。ただし、検出イベントに基づいたカスタム テーブルのワークフローは、必ずホスト ビューで終了します。

事前定義のイベント テーブルに基づいたワークフローとは異なり、カスタム テーブルに基づいたワークフローには、他のタイプのワークフローへのリンクがありません。

事前定義の侵入イベント ワークフロー

ライセンス：Protection

次の表で、FireSIGHT システムに含まれている事前定義の侵入イベント ワークフローについて説明します。これらのワークフローへのアクセスについては、侵入イベントの表示（41-10 ページ）および侵入イベントの確認（41-18 ページ）を参照してください。

:

表 58-1　事前定義の侵入イベント ワークフロー

ワークフロー名	説明
[接続先ポート（Destination Port）]	宛先ポートは通常、アプリケーションに関連付けられているため、このワークフローは、通常以上に大量のアラートが発生しているアプリケーションを検出するのに役に立ちます。[接続先ポート（Destination Port）] カラムは、ネットワークに存在してはいけないアプリケーションを識別するうえでも役に立ちます。 このワークフローは、侵入イベントに関連付けられている宛先ポートを表示するページから始まり、その後に、生成されたイベント タイプを表示するページが続きます。ここで、（イベントのテーブル ビューと呼ばれる）イベント情報の表形式のビューを表示し、次に、各イベントに関連付けられているパケットの復号化されたコンテンツを表示するパケット ビューを表示することができます。
Event-Specific（イベントに特有）	このワークフローには、2 つの便利な機能があります。頻繁に発生するイベントには、以下のことを示している可能性があります。 • 誤検出 • ワーム • 設定が大幅に間違っているネットワーク 頻繁に発生するイベントはほとんどの場合、攻撃の対象にされており、特別な注意が必要であることを意味しています。 このワークフローは、生成されたイベントのタイプを示すページから始まります。ここで、2 つのテーブル（イベントに関連付けられている送信元 IP アドレスを示すテーブルと、イベントに関連付けられている宛先 IP アドレスを示すテーブル）を持つページを表示できます。ワークフローの最終ページは、イベントのテーブル ビューとパケット ビューです。
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、優先度のレベル、分類、および表示されている各イベントのカウントが含まれているドリルダウン ページから始まります。ワークフローの最終ページは、イベントのテーブル ビューとパケット ビューです。
イベントと宛先（Events to Destinations）	このワークフローは、どのホスト IP アドレスが攻撃されているか、また攻撃の性質について概要レベルのビューを提供します。可能な場合には、攻撃に関与している国の情報も表示することができます。 このワークフローは、イベント タイプと宛先 IP アドレスのペアが示されているページから始まります。これによりユーザは、特定の IP アドレスに対してどのタイプのイベントが発生しているかを調べることができます。ワークフローの最終ページは、イベントのテーブル ビューとパケット ビューです。
IP に特有（IP-Specific）	このワークフローは、最も多くのアラートを生成しているホスト IP アドレスを示します。最も多くのイベントが生じているホストは、公開されていて、ワーム タイプのトラフィックを受け取っている（チューニングに適した場所であることを示している）か、あるいはアラートの原因を決定するためにさらに調査が必要です。カウントが最も少ないホストも攻撃の対象となる可能性があるため、調査が必要です。カウントが少ないことは、ホストがネットワークに属していない可能性があることも示しています。 このワークフローは、2 つのテーブル（イベントに関連付けられている送信元 IP アドレスのテーブルと、イベントに関連付けられている宛先 IP アドレスのテーブル）を表示するページから始まります。次のページで、生成されたイベント タイプを示します。ワークフローの最終ページは、イベントのテーブル ビューとパケット ビューです。

表 58-1　事前定義の侵入イベント ワークフロー(続き)

ワークフロー名	説明
影響および優先度（Impact and Priority）	このワークフローを使用して、影響が大きく、繰り返し発生するイベントをすばやく見つけることができます。報告される影響レベルは、イベントが発生した回数と合わせて表示されます。この情報を使用して、最も頻繁に再発する、影響の大きいイベントを特定することができます。このようなイベントは、ネットワーク上の広範囲に攻撃が存在していることを示している可能性もあります。 このワークフローは、各イベントに関連付けられている影響のレベル、優先度、およびカウントを示すページから始まります。次に、各イベントの送信元および宛先の IP アドレスを示したドリルダウン ページが表示されます。2 ページ目のイベントは、カウントでソートされています。ワークフローの最終ページは、イベントのテーブル ビューとパケット ビューです。
影響および送信元（Impact and Source）	このワークフローは、進行中の攻撃の発生源を特定する場合に役立ちます。報告される影響レベルは、イベントに関連付けられている送信元 IP アドレスと合わせて表示されます。たとえば、特定の IP アドレスからレベル 1 の影響度のイベントが繰り返し発生している場合は、脆弱なシステムを特定し、それらのシステムをターゲットにしている攻撃者が存在していることを示している可能性があります。 このワークフローは、各イベントに関連付けられている影響のレベル、送信元 IP アドレス、優先度、およびカウントを示すページから始まります。各イベントのレベル内で、イベントはカウントでソートされ、次に優先度でソートされます。次に、各イベントの送信元および宛先の IP アドレスを示したドリルダウン ページが表示されます。2 ページ目のイベントは、カウントでソートされています。ワークフローの最終ページは、イベントのテーブル ビューとパケット ビューです。
影響と宛先（Impact to Destination）	このワークフローを使用して、脆弱なコンピュータで繰り返し発生しているイベントを特定することができます。これにより、システム上の脆弱性に対処し、進行中の攻撃を停止することが可能になります。 このワークフローは、各イベントに関連付けられている影響のレベル、インラインの結果（パケットがドロップしたか、またはドロップする可能性があったかどうか）、宛先 IP アドレス、優先度、およびカウントを示すページから始まります。各イベントのレベル内で、イベントはカウントでソートされ、次に優先度でソートされます。次に、各イベントの送信元および宛先の IP アドレスを示したドリルダウン ページが表示されます。2 ページ目のイベントは、カウントでソートされています。ワークフローの最終ページは、イベントのテーブル ビューとパケット ビューです。
送信元ポート	このワークフローは、最も多くのアラートを生成しているサーバを示します。この情報を使用して、調整が必要なエリアを特定し、注意が必要なサーバを決定することができます。 このワークフローは、侵入イベントに関連付けられている送信元ポートを表示するページから始まり、その後に、生成されたイベント タイプを表示するページが続きます。ワークフローの最終ページは、イベントのテーブル ビューとパケット ビューです。
送信元と宛先（Source and Destination）	このワークフローは、高レベルのアラートを共有しているホスト IP アドレスを特定します。リストの先頭のペアは誤検出である可能性がありますが、調整が必要なエリアを特定している場合があります。リストの下部に示されているペアをチェックして、対象となる攻撃、アクセスが禁止されているリソースにアクセスしているユーザ、ネットワークに属さないホストを調べることができます。 このワークフローは、各イベントの送信元および宛先 IP アドレスを表示するページから始まり、その後に、生成されたイベント タイプを表示するページが続きます。ワークフローの最終ページは、イベントのテーブル ビューとパケット ビューです。

事前定義のマルウェア ワークフロー

ライセンス:任意（Any）

サポートされるデバイス:機能に応じて異なる

サポートされる防御センター:機能に応じて異なる

次の表で、Defense Center に含まれている事前定義のマルウェア ワークフローについて説明します。すべての事前定義のマルウェア ワークフローは、マルウェア イベントのテーブル ビューを使用します。

DC500 シリーズ 2 Defense Center、シリーズ 2 のデバイス、および Blue Coat X-Series 向け Cisco NGIPS は、高度なマルウェア防御をサポートしていないため、DC500 Defense Center ではこの機能のデータが表示されないことと、シリーズ 2 デバイスおよび Blue Coat X-Series 向け Cisco NGIPS はこのデータを検出しないことに注意してください。

マルウェア イベントへのアクセスについては、マルウェア イベントの操作（40-18 ページ）を参照してください。

表 58-2　事前定義のマルウェア ワークフロー

ワークフロー名	説明
マルウェアの概要（Malware Summary）	このワークフローは、ネットワーク トラフィックで検出されたマルウェア、またはエンドポイントベースの FireAMP コネクタで検出されたマルウェアを、脅威ごとにグループ化して表示します。
マルウェア イベントの概要（Malware Event Summary）	このワークフローは、さまざまなマルウェア イベントのタイプおよびサブタイプについて詳細な情報を迅速に提供します。
マルウェアを受信するホスト（Hosts Receiving Malware）	このワークフローは、マルウェアを受信したホスト IP アドレスのリストを、マルウェア ファイルに関連付けられている処理ごとにグループ化して提供します。
マルウェアを送信するホスト（Hosts Sending Malware）	このワークフローは、マルウェアを送信したホスト IP アドレスのリストを、マルウェア ファイルに関連付けられている処理ごとにグループ化して提供します。
マルウェアを取り込んだアプリケーション（Applications Introducing Malware）	このワークフローは、ファイルを受信したホスト IP アドレスのリストを、これらのファイルに関連付けられているマルウェアの処理ごとにグループ化して提供します。

事前定義のファイル ワークフロー

ライセンス: Protection

次の表で、Defense Center に含まれている事前定義のファイル イベント ワークフローについて説明します。すべての事前定義のファイル イベント ワークフローは、ファイル イベントのテーブル ビューを使用します。ファイル イベントへのアクセスについては、ファイル イベントの操作（40-8 ページ）を参照してください。

表 58-3　事前定義のファイル ワークフロー

ワークフロー名	説明
ファイルの概要（File Summary）	このワークフローは、さまざまなファイル イベントのカテゴリとタイプ、および関連するすべてのマルウェアの処理について詳細な情報を迅速に提供します。
ファイルを受信したホスト（Hosts Receiving Files）	このワークフローは、ファイルを受信したホスト IP アドレスのリストを、これらのファイルに関連付けられているマルウェアの処理ごとにグループ化して提供します。
ファイルを送信したホスト（Hosts Sending Files）	このワークフローは、ファイルを送信したホスト IP アドレスのリストを、これらのファイルに関連付けられているマルウェアの処理ごとにグループ化して提供します。

事前定義されたキャプチャ ファイル ワークフロー

ライセンス：Malware

サポートされるデバイス：機能に応じて異なる

サポートされる防御センター：機能に応じて異なる

次の表で、Defense Center に含まれている事前定義のキャプチャ ファイルワークフローについて説明します。すべての事前定義のキャプチャ ファイル ワークフローは、キャプチャ ファイルのテーブル ビューを使用します。

DC500 シリーズ 2 Defense Center、シリーズ 2 のデバイス、および Blue Coat X-Series 向け Cisco NGIPS は、高度なマルウェア防御をサポートしていないため、DC500 Defense Center ではこの機能のデータが表示されないことと、シリーズ 2 デバイスおよび Blue Coat X-Series 向け Cisco NGIPS はこのデータを検出しないことに注意してください。

キャプチャされたファイルへのアクセスについては、キャプチャ ファイルの操作（40-33 ページ）を参照してください。

表 58-4　事前定義されたキャプチャ ファイル ワークフロー

ワークフロー名	説明
キャプチャ ファイルの概要（Captured File Summary）	このワークフローは、タイプ、カテゴリ、および脅威のスコアに基づいてキャプチャ ファイルについての詳細な情報を提供します。
動的分析ステータス（Dynamic Analysis Status）	このワークフローは、キャプチャ ファイルが動的解析用に送信されたかどうかに基づいて、キャプチャ ファイルのカウントを提供します。

事前定義の接続データ ワークフロー

ライセンス：FireSIGHT

次の表で、Defense Center に含まれている事前定義の接続データ ワークフローについて説明します。すべての事前定義の接続データ ワークフローは、接続データのテーブル ビューを使用します。接続データへのアクセスについては、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。

表 58-5　事前定義の接続データ ワークフロー

ワークフロー名	説明
接続イベント	このワークフローは、基本的な接続および検出されたアプリケーションの情報についての概要ビューを提供します。ユーザはこれを使用して、イベントのテーブル ビューへドリル ダウンすることができます。
接続に基づいたアプリケーション（Connections by Application）	このワークフローには、検出された接続の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のアプリケーションのグラフが含まれています。
接続に基づいた発信側（Connections by Initiator）	このワークフローには、ホストが接続トランザクションを開始した接続の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のホスト IP アドレスのグラフが含まれています。
接続に基づいたポート（Connections by Port）	このワークフローには、検出された接続の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のポートのグラフが含まれています。
接続に基づいた応答側（Connections by Responder）	このワークフローには、ホスト IP が接続トランザクションの応答側であった接続の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のホスト IP アドレスのグラフが含まれています。
一定期間の接続（Connections over Time）	このワークフローには、モニタリング対象のネットワーク セグメントにおける、一定期間の接続の合計数のグラフが含まれています。
トラフィックに基づいたアプリケーション（Traffic by Application）	このワークフローには、送信されたキロバイト数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のアプリケーションのグラフが含まれています。
トラフィックに基づいた発信側（Traffic by Initiator）	このワークフローには、各アドレスから送信されたキロバイト数の合計に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のホスト IP アドレスのグラフが含まれています。
トラフィックに基づいたポート（Traffic by Port）	このワークフローには、送信されたキロバイト数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のポートのグラフが含まれています。
トラフィックに基づいた応答側（Traffic by Responder）	このワークフローには、各アドレスが受信したキロバイト数の合計に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のホスト IP アドレスのグラフが含まれています。
時間の経過ごとのトラフィック	このワークフローには、モニタリング対象のネットワーク セグメントにおける、一定期間に送信されたキロバイト数の合計のグラフが含まれています。
一意の発信側に基づいた応答側（Unique Initiators by Responder）	このワークフローには、各アドレスに接続した一意の発信側の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな応答側の 10 個のホスト IP アドレスのグラフが含まれています。
一意の応答側に基づいた発信側（Unique Responders by Initiator）	このワークフローには、アドレスが接続した一意の応答側の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな送信側の 10 個のホスト IP アドレスのグラフが含まれています。

事前定義のセキュリティ インテリジェンス ワークフロー

ライセンス：Protection

サポートされるデバイス：すべて（シリーズ 2 を除く）

サポートされる防御センター：DC500 を除くいずれか

次の表で、Defense Center に含まれている事前定義のセキュリティ インテリジェンス ワークフローについて説明します。すべての事前定義のセキュリティ インテリジェンス ワークフローは、セキュリティ インテリジェンス イベントのテーブル ビューを使用します。セキュリティ インテリジェンス イベント データへのアクセスについては、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。

表 58-6　事前定義のセキュリティ インテリジェンス ワークフロー

ワークフロー名	説明
セキュリティ インテリジェンス イベント	このワークフローは、基本的なセキュリティ インテリジェンスおよび検出されたアプリケーションの情報についての概要ビューを提供します。ユーザはこれを使用して、イベントのテーブル ビューへドリル ダウンすることができます。
セキュリティ インテリジェンスの概要（Security Intelligence Summary）	このワークフローは [セキュリティ インテリジェンス イベント（Security Intelligence Events）] ワークフローと同じですが、[セキュリティ インテリジェンスの概要（Security Intelligence Summary）] ページで始まります。このページには、カテゴリおよびカウントのみによってセキュリティ インテリジェンス イベントが表示されます。

事前定義のホスト ワークフロー

ライセンス：FireSIGHT

次の表で、ホスト データで使用できる事前定義のワークフローについて説明します。

表 58-7　事前定義のホスト ワークフロー

ワークフロー名	説明
ホスト（Hosts）	このワークフローには、ホストのテーブル ビューが含まれており、その後にホスト ビューが続きます。ホスト テーブルに基づいたワークフロー ビューにより、ホストに関連付けられているすべての IP アドレスに関するデータを簡単に表示することができます。詳細については、ホストの表示（50-21 ページ）を参照してください。
オペレーティング システムの概要（Operating System Summary）	このワークフローを使用して、ネットワークで使用されているオペレーティング システムを分析することができます。このワークフローには一連のページがあり、ネットワーク上のオペレーティング システム、およびオペレーティング システムのベンダーのリストを示すページから始まり、オペレーティング システムの各バージョンを実行しているホスト数を示すページが続きます。次のページには、重要度、IP アドレス、および NetBIOS 名別にホストがリストされ、関連するオペレーティング システムおよびオペレーティング システムのベンダーも示されます。このワークフローは、ホストのテーブル ビュー、およびその後に続くホスト ビューで終了します。詳細については、ホストの表示（50-21 ページ）を参照してください。

事前定義の侵入の痕跡ワークフロー

ライセンス：FireSIGHT

次の表は、IOC（侵入の痕跡）データで使用できる事前定義のワークフローについて説明します。

表 58-8　事前定義の侵入の痕跡ワークフロー

ワークフロー名	説明
侵入の痕跡（Indications of Compromise）	このワークフローは、カウントおよびカテゴリによってグループ化された IOC データの概要ビューで始まり、その後で、イベント タイプによってサマリ データを細分化した詳細ビューが示されます。次に、IOC データの完全なテーブル ビューが示されます。このワークフローは、ホスト ビューで終了します。IOC データの表示と解釈の詳細については、侵入の痕跡の使用（50-35 ページ）を参照してください。
ホストごとの侵入の痕跡（Indications of Compromise by Host）	このワークフローを使用して、ネットワーク上のどのホストが最も侵入されそうかを（IOC データに基づいて）判断できます。このワークフローには、IOC データ カウント別のホスト IP アドレスのビューが含まれており、その後に IOC データのテーブル ビューがあり、ホスト ビューで終了します。IOC データの表示と解釈の詳細については、侵入の痕跡の使用（50-35 ページ）を参照してください。

事前定義のアプリケーション ワークフロー

ライセンス：FireSIGHT

次の表で、アプリケーション データで使用できる事前定義のワークフローについて説明します。

表 58-9　事前定義のアプリケーション ワークフロー

ワークフロー名	説明
アプリケーションのビジネスとの関連性	このワークフローを使用して、ネットワーク上で推定されるそれぞれのビジネスの関連性レベルの実行中アプリケーションを分析できます。これにより、ネットワーク リソースの適切な使用を監視することができます。このワークフローは、それぞれの関連性レベルのアプリケーションを実行しているホストのカウントで始まり、その後に対象のビジネスの関連性レベルおよびホスト カウントを持つ個々のアプリケーションのテーブルが続き、アプリケーションのテーブル ビュー、ホスト ビューと続きます。詳細については、アプリケーションの表示（50-46 ページ）を参照してください。
アプリケーションのカテゴリ（Application Category）	このワークフローを使用して、ネットワーク上の各カテゴリ（電子メール、検索エンジン、ソーシャル ネットワークなど）の実行中アプリケーションを分析できます。これにより、ネットワーク リソースの適切な使用を監視することができます。このワークフローは、各カテゴリのアプリケーションを実行しているホストのカウントで始まり、その後に個々のアプリケーションを実行しているホストのカウント、アプリケーションのテーブル ビュー、ホスト ビューと続きます。詳細については、アプリケーションの表示（50-46 ページ）を参照してください。

表 58-9　事前定義のアプリケーション ワークフロー（続き）

ワークフロー名	説明
アプリケーションのリスク	このワークフローを使用して、ネットワーク上で推定されるそれぞれのセキュリティ リスク レベルの実行中アプリケーションを分析できます。これにより、ユーザ アクティビティの潜在的なリスクを推定し、適切なアクションを実行することができます。このワークフローは、それぞれのリスク レベルのアプリケーションを実行しているホストのカウントで始まり、その後に対象のビジネスの関連性レベルおよびホスト カウントを持つ個々のアプリケーションのテーブルが続き、アプリケーションのテーブル ビュー、ホスト ビューと続きます。詳細については、アプリケーションの表示（50-46 ページ）を参照してください。
アプリケーションの概要（Application Summary）	このワークフローを使用して、ネットワーク上のアプリケーションおよび関連するホストの詳細情報を取得できます。これにより、ホスト アプリケーションのアクティビティについて詳しく調べることができます。このワークフローは、アプリケーションを実行する個々のホストの IP アドレスのリストで始まり、アプリケーションのテーブル ビュー、およびホスト ビューと続きます。
アプリケーション	このワークフローを使用して、ネットワーク上で実行中のアプリケーションを分析できます。これにより、ネットワークがどのように使用されているか、概要を理解することができます。このワークフローは、個々のアプリケーションを実行しているホストのカウントで始まり、アプリケーションのテーブル ビュー、およびホスト ビューと続きます。詳細については、アプリケーションの表示（50-46 ページ）を参照してください。

事前定義のアプリケーション詳細ワークフロー

ライセンス：FireSIGHT

次の表で、アプリケーションの詳細およびクライアント データで使用できる事前定義のワークフローについて説明します。

表 58-10　事前定義のアプリケーション詳細ワークフロー

ワークフロー名	説明
アプリケーション詳細（Application Details）	このワークフローを使用して、ネットワーク上のクライアント アプリケーションを詳しく分析することができます。このワークフローには、ネットワーク上のクライアント アプリケーションとアプリケーション製品のリスト、および各アプリケーションを実行しているホスト数のカウントを示す一連のページが含まれています。対象のアプリケーションの各バージョンを実行しているホストの数を表示できます。次のページでは、特定のホストに対して最も頻繁にアクセスしたアプリケーションを特定することができます。次にワークフローはクライアント アプリケーションのテーブル ビューを提供し、続いてホスト ビューを提供します。詳細については、アプリケーションの詳細の表示（50-50 ページ）を参照してください。
Clients	このワークフローには、クライアント アプリケーションのテーブル ビューが含まれており、その後にホスト ビューが続きます。詳細については、アプリケーションの詳細の表示（50-50 ページ）を参照してください。

事前定義のサーバ ワークフロー

ライセンス：FireSIGHT

次の表で、サーバ データで使用できる事前定義のワークフローについて説明します。

表 58-11　事前定義のサーバ ワークフロー

ワークフロー名	説明
カウントに基づいたネットワーク アプリケーション（Network Applications by Count）	このワークフローを使用して、ネットワークで最も頻繁に使用されるアプリケーションを分析することができます。このワークフローには、アプリケーション、および各アプリケーションが存在するホストのカウントを示す一連のページが含まれています。さらに、各アプリケーションのベンダーとバージョンも示されます。ワークフローは、ホストごとのアプリケーションを示すテーブル ビュー、およびその後に続くホスト ビューで終了します。詳細については、サーバの表示（50-40 ページ）を参照してください。
ヒットに基づいた ネットワーク アプリケーション（Network Applications by Hit）	このワークフローを使用して、ネットワークで最もアクティブなアプリケーションを分析することができます。このワークフローには、アプリケーション、および各アプリケーションがアクセスされた頻度のカウントを示す一連のページが含まれています。さらに、各アプリケーションのベンダーとバージョンの情報も示されます。ワークフローは、ホストごとのアプリケーションを示すテーブル ビュー、およびその後に続くホスト ビューが含まれているページで終了します。詳細については、サーバの表示（50-40 ページ）を参照してください。
サーバの詳細（Server Details）	このワークフローを使用して、検出されたサーバ アプリケーション プロトコルのベンダーおよびバージョンを詳しく分析することができます。ワークフローには、ベンダーに関連付けられているサーバのリストが含まれています。その後に、ベンダーとバージョンの両方に関連するサーバのリストが続き、サーバのテーブル ビューとホスト ビューで終了します。
サーバ	このワークフローには、アプリケーションのテーブル ビューが含まれており、その後にホスト ビューが続きます。詳細については、サーバの表示（50-40 ページ）を参照してください。

事前定義のホスト属性ワークフロー

ライセンス：FireSIGHT

次の表で、ホスト属性のデータで使用できる事前定義のワークフローについて説明します。

表 58-12　事前定義のホスト属性ワークフロー

ワークフロー名	説明
属性（Attributes）	このワークフローを使用して、ネットワーク上のホストの IP アドレスおよびホストのステータスを監視することができます。このワークフローは、個々の IP アドレス、および現行のユーザ、ホストの重要度、注記、およびホワイトリストのコンプライアンスを示したホスト属性のテーブル ビューで始まります。そして、ホスト ビューで終了します。詳細については、ホスト属性の表示（50-30 ページ）を参照してください。

事前定義のディスカバリ イベント ワークフロー

ライセンス：FireSIGHT

次の表で、ディスカバリ イベントのデータで使用できる事前定義のワークフローについて説明します。

表 58-13　事前定義のディスカバリ イベント ワークフロー

ワークフロー名	説明
検出イベント（Discovery Events）	このワークフローは、ディスカバリ（検出）イベントについてテーブル ビューの形式で詳細なリストを提供し、その後にホスト ビューが続きます。詳細については、ディスカバリ イベント テーブルについて（50-17 ページ）を参照してください。

事前定義のユーザ ワークフロー

ライセンス：FireSIGHT

次の表で、Defense Center に含まれている事前定義のユーザ ワークフローについて説明します。

表 58-14　事前定義のユーザ ワークフロー

ワークフロー名	説明
Users	このワークフローは、ユーザ イベントまたは LDAP サーバの接続から収集したユーザ情報のリストを提供します。ユーザ アイデンティティ ワークフローの詳細については、ユーザの表示（50-66 ページ）を参照してください。

事前定義の脆弱性ワークフロー

ライセンス：FireSIGHT

次の表で、Defense Center に含まれている事前定義の脆弱性ワークフローについて説明します。

表 58-15　事前定義の脆弱性ワークフロー

ワークフロー名	説明
脆弱性（Vulnerabilities）	このワークフローを使用して、データベース内のすべての脆弱性を示す脆弱性のテーブル ビューを確認することができます。その後に、ネットワーク上で検出されたホストに適合するアクティブな脆弱性のみのテーブル ビューが続きます。ワークフローは、脆弱性の詳細ビューで終了します。この詳細ビューには、ユーザの制約に一致するすべての脆弱性について詳しい説明が含まれています。詳細については、脆弱性の表示（50-55 ページ）を参照してください。

事前定義のサードパーティの脆弱性ワークフロー

ライセンス：FireSIGHT

次の表で、Defense Center に含まれている事前定義のサードパーティの脆弱性ワークフローについて説明します。

表 58-16　事前定義のサードパーティの脆弱性ワークフロー

ワークフロー名	説明
IP アドレスごとの脆弱性（Vulnerabilities by IP Address）	このワークフローを使用して、サードパーティの脆弱性が何個検出されたかを、モニタリング対象のネットワーク上のホスト IP アドレスごとにすぐに確認することができます。このワークフローは、サードパーティの脆弱性のテーブル ビュー、およびその後に続くホスト ビューで終了します。詳細については、サードパーティの脆弱性の表示（50-61 ページ）を参照してください。
ソースごとの脆弱性（Vulnerabilities by Source）	このワークフローを使用して、サードパーティの脆弱性が何個検出されたかを、サードパーティの脆弱性ソース（QualysGuard Scanner など）ごとにすぐに確認することができます。このワークフローは、中間のドリルダウン ページ上にこれらの脆弱性に関する詳細な情報を提供し、サードパーティの脆弱性のテーブル ビュー、およびその後に続くホスト ビューで終了します。詳細については、サードパーティの脆弱性の表示（50-61 ページ）を参照してください。

事前定義の相関およびホワイトリスト ワークフロー

ライセンス：FireSIGHT

相関データ、ホワイトリスト イベント、ホワイトリスト違反、および修正ステータス イベントの各タイプについて、1 つの事前定義ワークフローが用意されています。

表 58-17　事前定義の相関ワークフロー

ワークフロー名	説明
相関イベント（Correlation Events）	このワークフローには、相関イベントのテーブル ビューが含まれています。詳細については、相関イベントの操作（51-60 ページ）を参照してください。
ホワイト リスト イベント（White List Events）	このワークフローには、ホワイトリスト イベントのテーブル ビューが含まれています。詳細については、ホワイト リスト イベントの操作（52-34 ページ）を参照してください。
ホストの違反カウント（Host Violation Count）	このワークフローは、1 つ以上のホワイトリストに違反しているすべてのホスト IP アドレスを示す一連のページを提供します。最初のページはアドレスごとの違反の数に基づいてアドレスをソートし、違反数が最も多い IP アドレスがリストの最上部に示されます。あるホスト IP アドレスが複数のホワイトリストに違反している場合、違反したそれぞれのホワイトリストに対して別の行が示されます。ワークフローには、すべての違反を示すホワイトリスト違反のテーブル ビューも含まれ、最後に検出された違反がリストの最上部に示されます。テーブル内の各行に、検出された違反が 1 つずつ示されます。詳細については、ホワイト リスト違反の処理（52-39 ページ）を参照してください。

表 58-17　事前定義の相関ワークフロー（続き）

ワークフロー名	説明
ホワイト リスト違反（White List Violations）	このワークフローには、すべての違反を示すホワイトリスト違反のテーブル ビューも含まれ、最後に検出された違反がリストの最上部に示されます。テーブル内の各行に、検出された違反が 1 つずつ示されます。詳細については、ホワイト リスト違反の処理（52-39 ページ）を参照してください。
ステータス（Status）	このワークフローには、修正ステータスのテーブル ビューが含まれています。このテーブル ビューには、違反したポリシーの名前、適用された修正の名前とステータスが含まれています。詳細については、修復ステータス イベントの使用（54-18 ページ）を参照してください。

事前定義のシステム ワークフロー

ライセンス：任意（Any）

FireSIGHT システムには、ルール更新のインポートやアクティブ スキャンの結果を表示するワークフロー、およびシステム イベント（監査イベントやヘルス イベント）などのいくつかの追加ワークフローが用意されています。

表 58-18　その他の事前定義ワークフロー

ワークフロー名	説明
監査ログ（Audit Log）	このワークフローには、監査イベントを示す監査ログのテーブル ビューが含まれています。詳細については、監査レコードの表示（69-2 ページ）を参照してください。
ヘルス イベント（Health Events）	このワークフローは、ヘルス モニタリング ポリシーによってトリガーされたイベントを表示します。詳細については、ヘルス イベント テーブル ビューの操作（68-57 ページ）を参照してください。
ルール更新のインポート ログ（Rule Update Import Log）	このワークフローには、正常終了および失敗したルール更新のインポート両方の情報を示すテーブル ビューが含まれています。詳細については、ルールの更新とローカル ルール ファイルのインポート（66-16 ページ）を参照してください。
スキャン結果（Scan Results）	このワークフローには、完了したそれぞれのスキャンを示すテーブル ビューが含まれています。詳細については、アクティブ スキャンの結果での作業（47-22 ページ）を参照してください。

保存済みのカスタム ワークフロー

ライセンス：Protection + FireSIGHT

修正できない事前定義のワークフローに加えて、Defense Center には保存済みのカスタム ワークフローもいくつか含まれています。これらのワークフローはそれぞれ 1 つのカスタム テーブルに基づいており、修正することができます。これらのワークフローへのアクセスについては、カスタム テーブルに基づいたワークフローの表示（59-10 ページ）を参照してください。

表 58-19　保存済みのカスタム 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。 デフォルトでは、このワークフローは、影響レベルでソートされ、次にホストの重要度、さらにイベントの発生数でソートされたイベントの概要で始まります。ワークフローの 2 ページ目を使用して、特定のイベントが発生した送信元および宛先のアドレスに対してドリルダウンし、表示することができます。ワークフローは、[宛先の重大度に基づく侵入イベント（Intrusion Events with Destination Criticality）] のテーブル ビュー、およびパケット ビューで終了します。このワークフローは、[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 テーブルに基づいています。詳細については、カスタム テーブルについて（59-1 ページ）を参照してください。
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、優先度のレベル、分類、および表示されている各イベントのカウントが含まれているドリルダウン ページから始まります。ワークフローの最終ページは、イベントのテーブル ビューとパケット ビューです。このワークフローは、[侵入イベント（Intrusion Events）] カスタム テーブルに基づいています。詳細については、カスタム テーブルについて（59-1 ページ）を参照してください。
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。 デフォルトでは、このワークフローは、影響レベルでソートされた最近のイベントのリストで始まります。ワークフローの次のページは、[宛先の重大度に基づく侵入イベント（Intrusion Events with Destination Criticality）] のテーブル ビューを提供し、その後にパケット ビューが続きます。このワークフローは、[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 テーブルに基づいています。詳細については、カスタム テーブルについて（59-1 ページ）を参照してください。
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。 デフォルトでは、このワークフローはサーバに接続しているホストのテーブル ビューで始まり、その後にホスト ビューが続きます。このワークフローは、[サーバに接続しているホスト（Hosts with Servers）] カスタム テーブルに基づいています。詳細については、カスタム テーブルについて（59-1 ページ）を参照してください。
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。 デフォルトでは、このワークフローは宛先の重大度に基づく侵入イベント（Intrusion Events with Destination Criticality）のテーブル ビューで始まり、その後にパケット ビューが続きます。このワークフローは、[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 テーブルに基づいています。詳細については、カスタム テーブルについて（59-1 ページ）を参照してください。

表 58-19　保存済みのカスタム ワークフロー（続き）

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。 デフォルトでは、このワークフローは [送信元の重大度に基づく侵入イベント（Intrusion Events with Source Criticality）] のテーブル ビューで始まり、その後にパケット ビューが続きます。このワークフローは、[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 テーブルに基づいています。詳細については、カスタム テーブルについて（59-1 ページ）を参照してください。
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。 デフォルトでは、このワークフローは、各サービスにアクセスする頻度が示されたサーバの概要で始まります。次のページには、オペレーティング システムのベンダーとバージョンごとにサーバが示されます。このワークフローは、サーバを実行しているホストのテーブル ビュー、およびその後に続くホスト ビューで終了します。このワークフローは、[サーバに接続しているホスト（Hosts with Servers）] カスタム テーブルに基づいています。詳細については、カスタム テーブルについて（59-1 ページ）を参照してください。

ワークフローの使用

ライセンス：任意（Any）

ワークフローのドリル ダウンおよびテーブル ビューのページを使用して、データのビューをすばやく絞り込むことができます。これにより、分析にとって重要なイベントに集中することが可能です。ワークフローのタイプによってデータは異なりますが、すべてのワークフローが共通の機能セットを共有しています。以降の項では、これらの機能について、およびこれらの機能の使用方法について説明します。

- ワークフローの選択（58-19 ページ）では、ワークフローの選択ページについて、および使用するワークフローを選択する方法について説明します。
- ワークフローのツールバーについて（58-21 ページ）では、ワークフローで使用できるツールバー オプションについて説明します。
- ワークフローのページの使用（58-21 ページ）では、すべてのワークフロー ページに表示される機能について、およびそれらの機能の使用方法について説明します。
- イベント時間の制約の設定（58-27 ページ）では、イベントベースのワークフローに対して時間範囲を設定する方法について説明します。ワークフローには、指定された時間範囲に生成されたイベントが含まれます。
- イベントの制約（58-35 ページ）では、ワークフローでデータのビューを制約して（絞り込んで）、次のワークフロー ページに進むために使用する機能について説明します。
- 複合的な制約の使用（58-38 ページ）では、複合的な制約の使用方法を説明し、その例を示します。
- ドリルダウン ワークフロー ページのソート（58-39 ページ）では、ワークフローで表示されるデータをソートする機能について、および表示するテーブル カラムを削除および復元する機能について説明します。
- ワークフロー ページの行の選択（58-40 ページ）では、表示されるテーブル内で、分析の対象とする、または他のアクションを実行するデータ行を選択する方法について説明します。

- ワークフロー内の他のページへのナビゲート（58-40 ページ）では、選択されたすべてのイベントを含め、制約を使用して現行のワークフローから他のワークフローをオープンする方法について説明します。
- ワークフロー間のナビゲート（58-41 ページ）では、[移動先（Jump to）] ドロップダウン リストについて、およびこのリストを使用して現行の制約を他のワークフローに適用する方法について説明します。
- イベントの検索（60-1 ページ）では、イベント データの検索に使用する機能について説明します。
- ブックマークの使用（58-42 ページ）では、ブックマークの作成、管理、および使用方法について説明します。

ワークフローの選択

ライセンス：任意（Any）

FireSIGHT システムは、次の表に記載されているデータのタイプに対して、事前定義のワークフローを提供しています。

表 58-20　ワークフローを使用する機能

機能	メニュー パス	オプション
侵入イベント	[分析（Analysis）] > [侵入（Intrusions）]	イベント 確認済みイベント（Reviewed Events） クリップボード（Clipboard） [インシデント（Incidents）]
マルウェア イベント	[分析（Analysis）] > [ファイル（Files）]	マルウェア イベント（Malware Events）
ファイル イベント	[分析（Analysis）] > [ファイル（Files）]	ファイル イベント
キャプチャ ファイル	[分析（Analysis）] > [ファイル（Files）]	キャプチャ ファイル（Captured Files）
接続イベント	[分析（Analysis）] > [接続（Connections）]	イベント
セキュリティ インテリジェンス イベント	[分析（Analysis）] > [接続（Connections）]	セキュリティ インテリジェンス イベント
ホスト イベント	[分析（Analysis）] > [ホスト（Hosts）]	ネットワーク マップ（Network Map） Hosts Indications of Compromise アプリケーション アプリケーション詳細（Application Details） サーバ ホスト属性（Host Attributes） 検出イベント（Discovery Events）
ユーザ イベント	[分析（Analysis）] > [ユーザ（Users）]	ユーザ アクティビティ（User Activity） Users

表 58-20　ワークフローを使用する機能（続き）

機能	メニュー パス	オプション
脆弱性イベント	[分析（Analysis）] > [脆弱性（Vulnerabilities）]	脆弱性（Vulnerabilities） サードパーティの脆弱性（Third-Party Vulnerabilities）
相関イベント	[分析（Analysis）] > [相関（Correlation）]	相関イベント（Correlation Events） ホワイトリスト イベント（White List Events） ホワイトリスト違反（White List Violations） ステータス（Status）
監査イベント	[システム（System）] > [モニタリング（Monitoring）]	監査（Audit）
ヘルス イベント	[ヘルス（Health）] > [ヘルス イベント（Health Events）]	適用対象外
ルール更新のインポート ログ（Rule Update Import Log）	[システム（System）] > [更新（Updates）]	適用対象外
スキャン結果（Scan Results）	[ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]	適用対象外

上記の表に記載されているいずれかの種類のデータを表示する場合、そのデータのデフォルトのワークフローの最初のページにイベントが表示されます。

また、ワークフローのアクセスは、以下のとおりに、自身のユーザ ロールによって異なります（ユーザ ロールの設定（61-53 ページ）を参照してください）。

- 管理者（Administrator）ユーザはすべてのワークフローにアクセスできます。また、管理者（Administrator）は監査ログ、スキャン結果、およびルール更新のインポート ログにアクセスできる唯一のユーザです。
- メンテナンス（Maintenance）ユーザは、ヘルス イベントにアクセスできます。
- セキュリティ アナリスト（Security Analyst）およびセキュリティ アナリスト（Security Analyst）（読み取り専用）ユーザは、侵入、マルウェア、ファイル、接続、ディスカバリ、脆弱性、相関、およびヘルスのワークフローにアクセスできます。

デフォルト以外のワークフローを使用してデータを表示する方法：

アクセス：Admin/Any Security Analyst

手順 1　ワークフローを使用する機能の表に記載されているように、適切なメニュー パスとオプションを選択します。

対象のデータ タイプに対するデフォルト ワークフローの最初のページが表示されます。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。

手順 2　必要に応じて、別のワークフローを使用します。ワークフローのタイトルの隣にある [ワークフロー切り替え（switch workflow）] をクリックして、使用するワークフローを選択します。

手順 3　選択したワークフローの最初のページが表示されます。

ワークフローのツールバーについて

ライセンス：任意（Any）

ワークフローの各ページには、関連する機能へすばやくアクセスするためのツールバーが含まれています。次の表に、ツールバー上の各リンクについて説明します。

表 58-21　ワークフローのツールバー リンク

機能	説明
このページをブックマークする（Bookmark This Page）	後でそのページに戻れるように、現在のページをブックマークします。ブックマークすると、表示中のページに適用されている制約が取得され、（データがまだ存在していれば）後で同じデータに戻ることができます。ブックマークの作成については、ブックマークの使用（58-42 ページ）を参照してください。
レポート作成者	現在制約されているワークフローを選択基準として使用して、Report Designer を開きます。レポートの作成については、イベント ビューからのレポート テンプレートの作成（57-10 ページ）を参照してください。
ダッシュボード	現行のワークフローに関連するダッシュボードを開きます。たとえば、[接続イベント（Connection Events）] ワークフローは [接続サマリ（Connection Summary）] ダッシュボードと関連付けられています。ダッシュボードの使用については、ダッシュボードの使用（55-1 ページ）を参照してください。
ブックマークの表示（View Bookmarks）	ユーザが選択できる、保存したブックマークのリストを表示します。ブックマークの作成および管理については、ブックマークの使用（58-42 ページ）を参照してください。
検索（Search）	[検索（Search）] ページが表示され、ここでワークフローのデータについて高度な検索を実行することができます。下向きの矢印アイコンをクリックし、保存済みの検索を選択して使用することもできます。ワークフローの検索については、イベントの検索（60-1 ページ）を参照してください。

ワークフローのページの使用

ライセンス：任意（Any）

ユーザがワークフローのページ上で実行できるアクションは、ページのタイプによって異なります。テーブル ビュー ページおよびドリルダウン ページには、ユーザが表示するイベント セットの制約、またはワークフローへのナビゲートに使用できる多数の機能が含まれています。各タイプのページで使用できる機能の詳細については、以降の項を参照してください。

- 共通のテーブル ビューまたはドリルダウン ページ機能の使用（58-21 ページ）
- 地理位置情報の使用（58-24 ページ）
- テーブル ビュー ページの使用（58-25 ページ）
- ドリルダウン ページの使用（58-26 ページ）
- ホスト ビュー、パケット ビュー、または脆弱性の詳細ページの使用（58-26 ページ）

共通のテーブル ビューまたはドリルダウン ページ機能の使用

ライセンス：任意（Any）

テーブル ビューおよびドリルダウン ワークフローのページでは、テーブル見出しおよびテーブル行に一連のアイコンおよび他の機能が用意されています。これを使用して、表示されたデータについてアクションを実行できます。

次の表で機能について説明します。

表 58-22　テーブル ビューおよびドリルダウン ページの機能

機能	説明
	青色の下向き矢印のアイコンをクリックして、ワークフローの次ページの該当する行を表示します。
 (正常) (マルウェア) (カスタム検出) (不明) (利用不可)	ファイル名および SHA-256 ハッシュ値のカラムに表示されるネットワーク ファイルのトラジェクトリ アイコンをクリックして、ファイルのトラジェクトリ マップを新しいウィンドウに表示します。詳細については、ネットワーク ファイル トラジェクトリの分析 (40-42 ページ) を参照してください。 DC500 Defense Center、シリーズ 2 デバイス、および Blue Coat X-Series 向け Cisco NGIPS は高度なマルウェア防御をサポートしていないため、これらのアプライアンスでは、ネットワークベースのマルウェアおよびファイル イベントに対するネットワーク ファイルのトラジェクトリは表示できないことに注意してください。
  (侵入の可能性がある)  (ブラックリスト登録済み)  (ブラックリスト登録済み、監視対象に設定)	[IP アドレス (IP address)] カラムに表示されるホスト プロファイル アイコンをクリックして、IP アドレスに関連付けられているホスト プロファイルをポップアップ ウィンドウに表示します。詳細については、ホスト プロファイルの使用 (49-1 ページ) を参照してください。 トリガーされた侵入の痕跡 (IOC) ルールによって侵入の可能性があるとタグ付けされたホストには、通常のアイコンではなく、侵入されたホストのアイコンが表示されます。IOC の詳細については、侵害の兆候 (痕跡) について (45-22 ページ) を参照してください。 ホスト プロファイルのアイコンがグレー表示になっている場合は、ネットワーク マップ内にそのホストが存在することができないため、ホスト プロファイルを表示できません (0.0.0.0 など)。 セキュリティ インテリジェンス データに基づいてトラフィックのフィルタリングを実行する場合は、接続イベントで、ブラックリストに記載されている監視対象の IP アドレスの隣にあるホスト アイコンが少し異なります。これは、接続においてどのホストがブラックリストに記載されているかを識別するのに役に立ちます。DC500 Defense Center および シリーズ 2 のデバイスはセキュリティ インテリジェンスのデータをサポートしていないことに注意してください。
 (低脅威スコア)  (中脅威スコア)  (高脅威スコア)  (非常に高い脅威スコア)	脅威スコアのカラムに表示される脅威スコアのアイコンをクリックし、動的解析サマリ (Dynamic Analysis Summary) レポートで、ファイルに関連付けられている最高の脅威スコアを表示します。 DC500 Defense Center、シリーズ 2 デバイス、および Blue Coat X-Series 向け Cisco NGIPS は高度なマルウェア防御をサポートしているため、これらのアプライアンスでは動的解析サマリ (Dynamic Analysis Summary) レポートを表示することはできません。
	ユーザ アイデンティティのカラムに表示されるユーザ アイコンをクリックして、ユーザのプロファイル情報を表示します。詳細については、ユーザの詳細とホストの履歴について (50-68 ページ) を参照してください。 ユーザ アイコンがグレー表示になっている場合は、そのユーザがデータベース内に存在することができないため、ユーザ プロファイルは表示できません (FireAMP コネクタ ユーザなどの場合)。
	サードパーティの脆弱性 ID のカラムに表示される脆弱性アイコンをクリックし、サードパーティの脆弱性について詳細を表示します。詳細については、脆弱性の詳細の表示 (49-31 ページ) を参照してください。

表 58-22　テーブル ビューおよびドリルダウン ページの機能（続き）

機能	説明
チェック ボックス	ページ上で複数の行のチェック ボックスを選択して、処理を反映させる行を表示し、ページの下部にあるいずれかのボタン（[表示（View）] ボタンなど）をクリックします。行の先頭にあるチェック ボックスを選択して、ページ上のすべての行を選択することもできます。
国旗およびコード	接続イベント、侵入イベント、ファイル イベント、マルウェア イベントなどのワークフローのページの中には、ルート可能な IP アドレスに、関連する国の情報が含まれているものがあります。このような*地理情報*が使用可能な場合は、その国の国旗および ISO コードが該当するカラム（[送信元の国（Source Country）] など）に表示されます。国名を表示するには、ポインタを国旗の上に移動します。（集約されたデータではなく）個別のデータ ポイントを表示する場合は、国旗のアイコンをクリックして、詳細な地理情報を表示することができます。詳細については、地理位置情報の使用（58-24 ページ）を参照してください。 DC500 Defense Center は地理情報データをサポートしていないことに注意してください。
検索の制約	データ ビューを制約する値が存在する場合に、その値を表示します。展開の矢印（▲）をクリックすると、アクティブな制約および無効なカラムのリストが表示され、縮小の矢印（▶）をクリックすると、ビューからリストが非表示になります。デフォルトでは、このリストは縮小されています。これは制約のリストが長く、画面には収まらない場合に便利です。 1 つの制約を解除するには、その制約をクリックします。複合的な制約を解除するには、[複合的な制約（Compound Constraints）] をクリックします。 現行の 1 つの制約により値が事前に挿入された検索ページを開くには、[検索の編集（Edit Search）] または [検索の保存（Save Search）] をクリックします。詳細については、イベントの制約（58-35 ページ）を参照してください。 **（注）**　複合的な制約では、複数の不可算値を持つ行に基づいて制約が作成されます。複合的な制約について、検索および検索の保存を実行することはできません。
時間範囲（Time Range）	ページの右上隅に表示される日付範囲は、ワークフローに含めるイベントの時間範囲を設定します。詳細については、イベント時間の制約の設定（58-27 ページ）を参照してください。 イベント ビューを時間によって制約している場合は、（グローバルかイベントに特有かに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあることに注意してください。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。
ワークフロー ページのリンク	ワークフロー ページのリンクは、事前定義されたワークフロー テーブル ビュー、およびドリルダウン ページの左上隅の、イベントの上で、ワークフロー名の下に示されます。ワークフロー ページのリンクをクリックして、アクティブな制約を使用しているページを表示します。
ワークフロー名	ページの上部にワークフロー名が表示されます。該当する場合は、ワークフロー名の隣に（[ワークフロー切り替え（switch workflows）]）リンクがあります。これを使用して、同じタイプの他のワークフローを選択することができます。

地理位置情報の使用

ライセンス: FireSIGHT

サポートされるデバイス:機能に応じて異なる

サポートされる防御センター:任意（DC500 を除く）

ネットワークの監視中、*地理位置情報*機能によって、ルート可能な IP アドレスの地理的な送信元について、追加のデータ（国や大陸など）が提供されます。たとえば、このデータを使用して、自身の組織と未接続の国が接続の発信元または宛先であるかどうかを判断することができます。

地理位置情報は、侵入イベント、接続イベント、ファイル イベント、マルウェア イベント、ホスト プロファイル、およびユーザ プロファイルで使用することができます。地理位置情報は、Context Explorer およびダッシュボードでも使用できます。

この目的でカスタムな地理位置情報オブジェクトを作成するだけでなく、アクセス コントロール ルールの条件として地理位置情報データ（送信元および宛先の国/大陸）を使用することもできます。また、相関ルールおよびトラフィック プロファイルの条件として、送信元/宛先の国データを使用することもできます。詳細については、地理位置情報オブジェクトの操作（3-58 ページ）、ネットワークまたは地理的位置によるトラフィックの制御（15-4 ページ）、相関ポリシーのルールの作成（51-3 ページ）、およびトラフィック プロファイル条件の指定（53-3 ページ）を参照してください。

地理位置情報データベース（GeoDB）の更新をインストールすると [位置情報の詳細（Geolocation Details）] ページが表示され、IP アドレスに関して使用可能な詳細情報（郵便番号、緯度/経度の座標、タイム ゾーン、自律システム番号（ASN）、インターネット サービス プロバイダー（ISP）、使用タイプ（個人または会社）、組織、ドメイン名、接続タイプ、プロキシ情報など）が示されます。また、サードパーティの 4 つのマップ ツールのいずれかを使用して、検出された場所を特定することもできます。GeoDB が更新されていない場合は、国旗アイコンおよび国名のみが表示され、[位置情報の詳細（Geolocation Details）] ページを参照することはできません。GeoDB のインストールと更新については、位置情報データベースの更新（66-32 ページ）を参照してください。[ヘルプ（Help）] > [バージョン情報（About）] をクリックして GeoDB 更新の最新バージョンを表示することができます。

使用可能なデータに応じて、[位置情報の詳細（Geolocation Details）] ページに多数のフィールドが表示されることがあります。情報が含まれないフィールドは表示されません。次の表で、これらのフィールドの情報について示します。

表 58-23　地理位置情報の詳細フィールド

フィールド	目次
国（Country）	ホスト IP アドレスに関連付けられている国が国旗とともに示されます。大陸は括弧内に表示されます。例：米国（北アメリカ）（United States （North America））、赤道ギニア（アフリカ）（Equatorial Guinea （Africa））
地域	ホストが存在する国の州、県、またはその他の小区域。例：VA、35
市区町村郡（City）	ホストが存在する市。例：シアトル（Seattle）、福岡（Fukuoka）
[郵便番号（Postal Code）]	ホストが存在する地域の郵便番号。例：361000、90210
緯度/経度（Latitude/Longitude）	ホストの場所の正確な座標。例：40.0375, -76.1053、53.4050, -0.5484
マップ	外部のマッピング サイト（Google Maps、Yahoo Maps、Bing Maps、OpenStreetMap など）へのリンク。ホストのおよその位置のコンテキスト マップを表示するには、リンクをクリックします。
タイムゾーン（Timezone）	ホストの場所のタイム ゾーン（該当する場合には夏時間が示されます）。例：GMT+8:00、GMT-4:00 (In DST)

表 58-23　地理位置情報の詳細フィールド(続き)

フィールド	目次
ASN	ホスト IP アドレスに関連付けられている自律システム番号(ASN)、およびその ASN に関する追加情報。例:14618 (Amazon.com Inc.)、4837 (Cncgroup China169 Backbone)
ISP	ホストの IP アドレスに関連付けられているインターネット サービス プロバイダー(ISP)。例:Atlantic Broadband、China Unicom Ip Network
個人/会社(Home/Business)	ホストの接続が個人または会社のどちらの目的であるかを示します。
Organization	ホストの IP アドレスに関連付けられている組織。例:Amazon.com、Bank of America
ドメイン名(Domain Name)	ホストの IP アドレスに関連付けられているドメイン名。例:amazonaws.com、xmcnc.net
接続タイプ(Connection Type)	ホストの IP アドレスに関連付けられている接続タイプ。例:Broadband、DSL
プロキシ タイプ(Proxy Type)	使用するプロキシのタイプ。例:Anonymous、Corporate

地理位置情報の詳細を表示するには、以下を行います。

アクセス:任意(Any)

手順 1　イベント ビュー、ホスト プロファイル、またはその他の地理情報をサポートしているページで、個々のデータ ポイントのそばに表示される小さい国旗のアイコンまたは ISO 国コードをクリックします(国旗のアイコンが存在しても、[接続サマリ(Connection Summary)] ダッシュボードなどで、集約的な地理情報から詳細を表示することはできません)。

ヒント　イベント ビューで国旗のアイコンの上にポインタを移動すると、ツールチップとして国名が示されます。

[位置情報の詳細(Geolocation Details)] ページが新しいウィンドウに表示されます。

テーブル ビュー ページの使用

ライセンス:任意(Any)

デフォルトでカラムが有効になっている場合、テーブル ビューには、データベースの各フィールドに対するカラムが含まれています。テーブル ビューでカラムを無効にし、そのカラムを無効にすることによって同じ行が複数生成される場合には、FireSIGHT システムはイベント ビューに [カウント(Count)] カラムを追加します。テーブル ビュー ページで 1 つの値をクリックすると、その値によって制約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、[テーブル ビューの追加(Add Table View)] をクリックしてテーブル ビューを追加します。

テーブル ビュー ページには、ドリルダウン、ホスト ビュー、パケット ビュー、または脆弱性の詳細ページでは利用できない追加機能が用意されています。次の表で、これらの機能の詳細な情報について説明します。

表 58-24　テーブル ビュー ページの追加機能

機能	説明
✖	非表示にするカラムの見出しで、このアイコンをクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。 ヒント　他のカラムを表示または非表示にするには、[適用（Apply）] をクリックする前に、対象のチェック ボックスをオンまたはオフにします。
[無効になったカラム（Disabled Columns）] リスト	ページからカラムを削除した場合、またはデフォルトでカラムを無効になっている場合、[無効になったカラム（Disabled Columns）] リストにカラム名が表示されます。このリストは、テーブルの上にありますが、デフォルトでは非表示になっています。 無効になったカラムをイベント ビューに戻すには、[検索の制約（Search Constraints）] の展開アイコン（ ▲ ）をクリックして検索の制約を展開し、[無効になったカラム（Disabled Columns）] の下にあるカラム名をクリックします。 詳細については、ドリルダウン ワークフロー ページのソート（58-39 ページ）を参照してください。

ドリルダウン ページの使用

ライセンス：任意（Any）

ドリルダウン ページには、データベースで使用できるカラムのサブセットが含まれています。事前定義のワークフローに対するドリルダウン ページには、必ず [カウント（Count）] カラムがあることに注意してください。ドリルダウン ページでは、表示するイベントの範囲を絞り込んで、ワークフローの先へ進むことができます。ドリルダウン ページで 1 つの値をクリックすると（たとえば、その値によって制約を行い、ワークフローの次のページへ進むと）、選択した値に一致するイベントに絞り込むことができます。ドリルダウン ページで値をクリックした場合は、次のページがテーブル ビューであっても、値が存在するカラムは無効になりません。カスタム ワークフローを作成する場合は、[ページの追加（Add Page）] をクリックして、ドリルダウン ページを追加します。

ドリルダウン ページの機能を使用して、ワークフローを移動するときにイベント セットを制約する方法の詳細については、共通のテーブル ビューまたはドリルダウン ページ機能の使用（58-21 ページ）を参照してください。

ホスト ビュー、パケット ビュー、または脆弱性の詳細ページの使用

ライセンス：任意（Any）

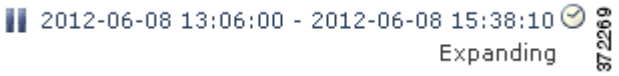
ディスカバリ（検出）イベント、ホスト、ホスト属性、侵入の痕跡（兆候）、サーバ、クライアント アプリケーション、または接続データのワークフローの最終ページはホスト ビューです。脆弱性のワークフローの最終ページは、脆弱性の詳細ページです。侵入イベントのワークフローは必ず、パケット ビューで終了します。ワークフローの最終ページで詳細セクションを展開して、ワークフローの進行中に絞り込んだセットの各オブジェクトについて、具体的な情報を表示することができます。Web インターフェイスは、ワークフローの最終ページに制約を表示しませんが、以前に設定した制約は保持されており、データのセットに適用されます。

イベント時間の制約の設定

ライセンス：任意（Any）

各イベントには、そのイベントがいつ発生したかを示すタイム スタンプがあります。時間枠（タイム ウィンドウ、時間範囲とも呼ばれる）を設定することによって、いくつかのワークフローに表示される情報を制約することができます。

時間によって制約できるイベントに基づいたワークフローには、ページの上部に次の図に示すような時間範囲を表す行が含まれています。



デフォルトでは、Cisco アプライアンス上のワークフローは、1 時間前が開始時間として設定された時間枠を使用します。たとえば、午前 11:30 にログインした場合、午前 10:30～11:30 の間に発生したイベントが表示されます。時間が経過するにしたがって、時間枠が拡張されます。午後 12:30 には、午前 10:30～午後 12:30 の間に発生したイベントが表示されます。

デフォルトで独自の時間枠を設定することによって、この動作を変更することができます。これにより、次の 3 つのプロパティが影響を受けます。

- 時間枠のタイプ（静的、拡張、またはスライディング）
- 時間枠の長さ
- 時間枠の数（複数の時間枠、または単一のグローバル時間枠）

デフォルトの時間枠の一般的な情報については、デフォルトの時間枠（71-6 ページ）を参照してください。

ページの上部にある時間範囲をクリックして [日時（Date/Time）] ポップアップ ウィンドウを表示し、デフォルトの時間枠の設定に関係なく、イベントの分析中に時間枠を手動で変更することができます。設定した時間枠の数、および使用しているアプライアンスのタイプに応じて [日時（Date/Time）] ウィンドウを使用して、表示しているイベントのタイプに対するデフォルトの時間枠を変更することもできます。

最後に、時間枠は一時停止することができるため、時間枠の変更と削除、または必要のないイベントを追加することなく、ワークフローで提供されたデータを調べることができます。ページの下部にあるリンクをクリックしてイベントの他のページを表示する場合は、異なるワークフロー ページで同じイベントを表示しないように、時間枠が自動的に一時停止することに注意してください。準備ができたら時間枠の一時停止を解除できます。

詳細については、次の項を参照してください。

- 時間枠の変更（58-27 ページ）
- イベント タイプのデフォルトの時間枠の変更（58-32 ページ）
- 時間枠の一時停止（58-34 ページ）

時間枠の変更

ライセンス：任意（Any）

デフォルトの時間枠（タイム ウィンドウ）に関係なく、イベントの分析中に時間枠を手動で変更することができます。

(注)　手動による時間枠の設定は、現行のセッションに対してのみ有効です。いったんログアウトしてからもう一度ログインすると、時間枠はデフォルトにリセットされます。

ユーザが設定した時間枠の数によっては、1 つのワークフローの時間枠の変更が、アプライアンス上の他のワークフローに影響を与えることがあります。たとえば、単一のグローバルな時間枠がある場合、1 つのワークフローの時間枠を変更すると、アプライアンス上の他のすべてのワークフローの時間枠が変更されます。一方、複数の時間枠を使用している場合は、監査ログまたはヘルス イベント ワークフローの時間枠を変更しても、他の時間枠には影響がありませんが、他の種類のイベントで時間枠を変更すると、時間によって制約されるすべてのイベント（監査イベントとヘルス イベントは除く）が影響を受けます。

すべてのワークフローを時間によって制約できるわけではないため、時間枠の設定は、ホスト、ホスト属性、アプリケーション、アプリケーションの詳細、脆弱性、ユーザ、またはホワイトリスト違反に基づいたワークフローには影響を与えないことに注意してください。

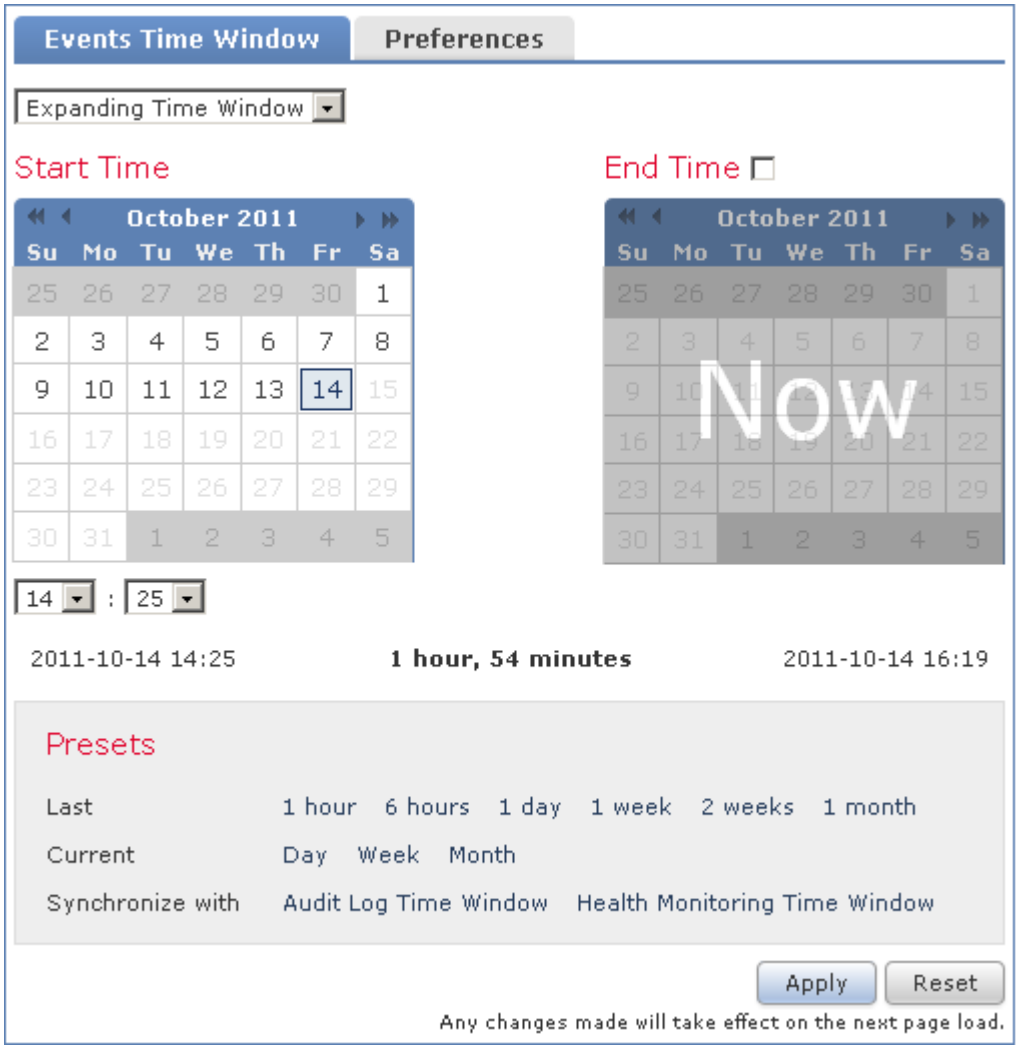
[日時（Date/Time）] ウィンドウの [タイム ウィンドウ（Time Window）] タブを使用して、時間枠を手動で設定します。デフォルトの時間枠設定で設定した時間枠の数によって、タブのタイトルは以下のいずれかになります。

- [イベント タイム ウィンドウ（Events Time Window）]：複数の時間枠を設定し、監査ログまたはヘルス イベント ワークフロー以外のワークフローに対して時間枠を設定している場合
- [ヘルス モニタリング タイム ウィンドウ（Health Monitoring Time Window）]：複数の時間枠を設定し、ヘルス イベント ワークフローに対して時間枠を設定している場合
- [監査ログ タイム ウィンドウ（Audit Log Time Window）]：複数の時間枠を設定し、監査ログに対して時間枠を設定している場合
- [グローバル タイム ウィンドウ（Global Time Window）]：単一の時間枠を設定している場合

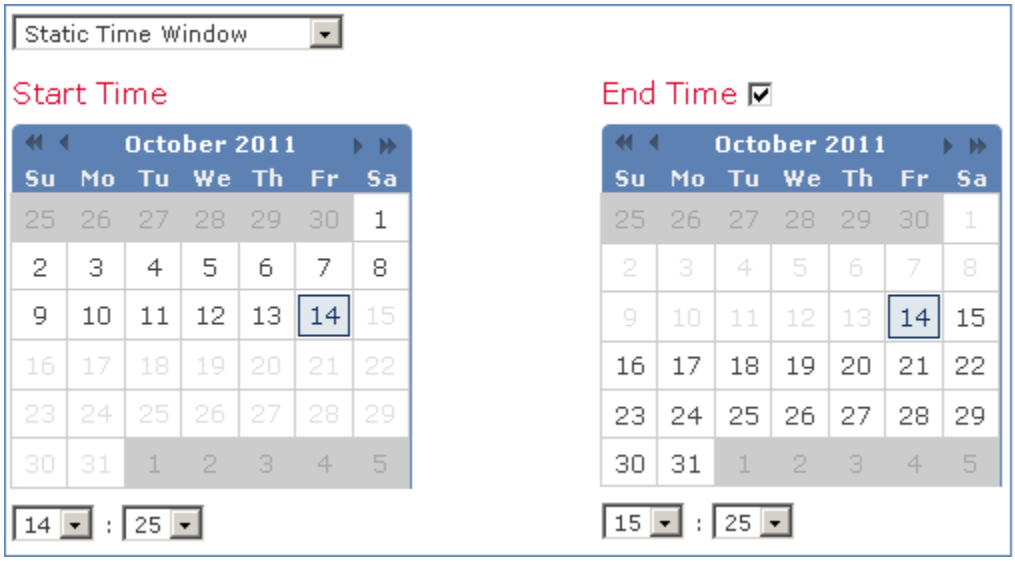
時間枠を設定する場合には、最初に、使用する時間枠のタイプを決定する必要があります。

- *静的な*時間枠は、特定の開始時間から特定の終了時間の間に生成されたすべてのイベントを表示します。
- *拡張*時間枠は、特定の開始時間から現在までの間に生成されたすべてのイベントを表示します。時間の経過とともに時間枠が拡張され、イベント ビューに新しいイベントが追加されます。
- *スライディング*時間枠は、特定の開始時間（1 週間前など）から現在までの間に生成されたすべてのイベントを表示します。時間の経過とともに時間枠が「スライド」し、自身が設定した範囲（この例では、過去 1 週間）のイベントのみが表示されます。

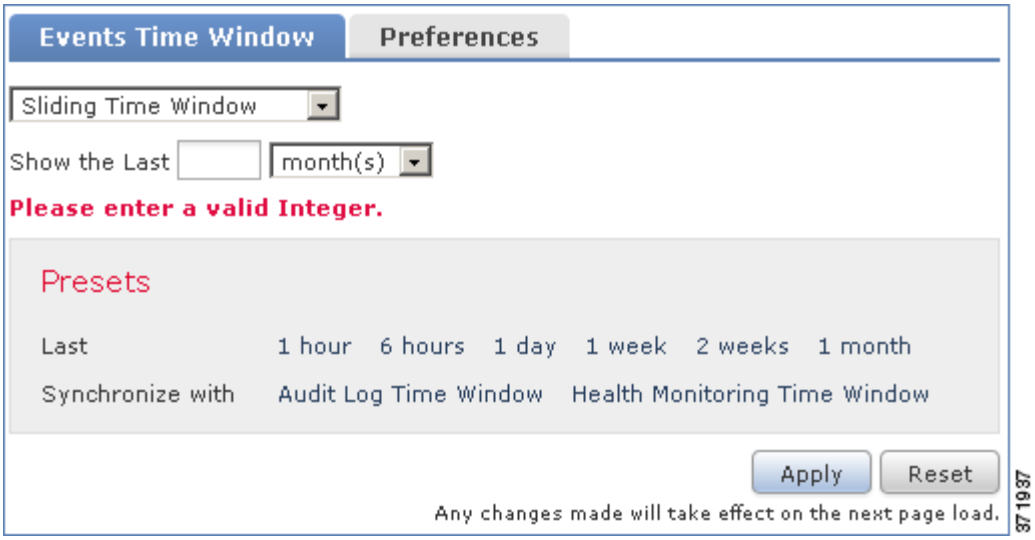
選択するタイプによっては、[日時（Date/Time）] ウィンドウが変化し、さまざまな設定オプションを提供します。次の図は、拡張の時間枠を使用するよう指定した [日時（Date/Time）] ウィンドウを示しています。拡張の時間枠では、[終了時間（End Time）] カレンダーがグレー表示され、終了時間は「現在（Now）」と示されます。



静的な時間枠を使用する場合は、終了時間を設定できます。



スライディング時間枠を使用するよう選択すると、オプションがさらに変わります。



(注)　FireSIGHT システムは、タイム ゾーンのプリファレンスに指定された時間に基づいて、24 時間の時計を使用します。タイム ゾーンの設定の詳細については、デフォルトのタイム ゾーン設定 (71-8 ページ) を参照してください。

次の表で、[タイム ウィンドウ(Time Window)] タブで設定できるさまざまな設定について説明します。

表 58-25　時間枠の設定

設定	時間枠(タイム ウィンドウ)のタイプ	説明
時間枠タイプのドロップダウン リスト	適用対象外	使用する時間枠のタイプを、静的、拡張、またはスライディングのいずれかから選択します。 イベント ビューを時間によって制約している場合は、(グローバルかイベントに特有かに関係なく)アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあることに注意してください。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。
[開始時間(Start Time)] カレンダー	静的および拡張	時間枠の開始日と時間を指定します。すべての時間枠の最大時間範囲は、1970 年 1 月 1 日午前 0 時(UTC)～ 2038 年 1 月 19 日午前 3 時 14 分 7 秒です。 ヒント　カレンダーを使用する代わりに、下記で説明するプリセット オプションを使用できます。

表 58-25　時間枠の設定（続き）

設定	時間枠（タイム ウィンドウ）のタイプ	説明
[終了時間（End Time）] カレンダー	静的	時間枠の終了日付と時間を指定します。すべての時間枠の最大時間範囲は、1970 年 1 月 1 日午前 0 時（UTC）～ 2038 年 1 月 19 日午前 3 時 14 分 7 秒です。 拡張時間枠を使用している場合は、[終了時間（End Time）] カレンダーがグレー表示になり、終了時間が「Now」と示されることに注意してください。 **ヒント**　カレンダーを使用する代わりに、下記で説明するプリセット オプションを使用できます。
[最終を表示（Show the Last）] フィールドおよびドロップダウン リスト	スライディング	スライディング時間枠の長さを設定します。
[プリセット（Presets）]：[最終（Last）]	すべて	リスト内のいずれかの時間範囲をクリックし、アプライアンスのローカル時刻に基づいて時間枠を変更します。たとえば、[1 週間（1 week）] をクリックすると、最後の 1 週間を反映するように時間枠が変わります。プリセットをクリックすると、選択したプリセットを反映するようにカレンダーが変わります。
[プリセット（Presets）]：[現在（Current）]	静的および拡張	リスト内のいずれかの時間範囲をクリックし、アプライアンスのローカル時間と日付に基づいて時間枠を変更します。プリセットをクリックすると、選択したプリセットを反映するようにカレンダーが変わります。 次の点に注意してください。 • 現在日付は午前 0 時から始まる • 現在の週は日曜日の午前 0 時から始まる • 現在の月は、月の最初の日の午前 0 時から始まる
[プリセット（Presets）]：[同期（Synchronize with）]	すべて（グローバルな時間枠を使用している場合は使用不可）	以下のいずれかをクリックします • [イベント タイム ウィンドウ（Events Time Window）]：現在の時間枠とイベントの時間枠を同期する場合 • [ヘルス モニタリング タイム ウィンドウ（Health Monitoring Time Window）]：現在の時間枠とヘルス モニタリングの時間枠を同期する場合 • [監査ログ タイム ウィンドウ（Audit Log Time Window）]：現在の時間枠と監査ログの時間枠を同期する場合

イベントの分析中に時間枠を変更する方法：

アクセス：Admin/Maint/Any Security Analyst

手順 1　時間に制約されるワークフローで、時間範囲のアイコン（）をクリックします。

[日時（Date/Time）] ウィンドウが表示されます。

手順 2　[タイム ウィンドウ（Time Window）] タブで、時間枠の設定の表に記載されているように時間枠を設定します。

ヒント　時間枠をデフォルトの設定に戻すには、[リセット(Reset)] をクリックします。

手順 3　[適用(Apply)] をクリックします。

ウィンドウが閉じて、イベント ビュー ページに新しい時間枠のイベントが表示されます。

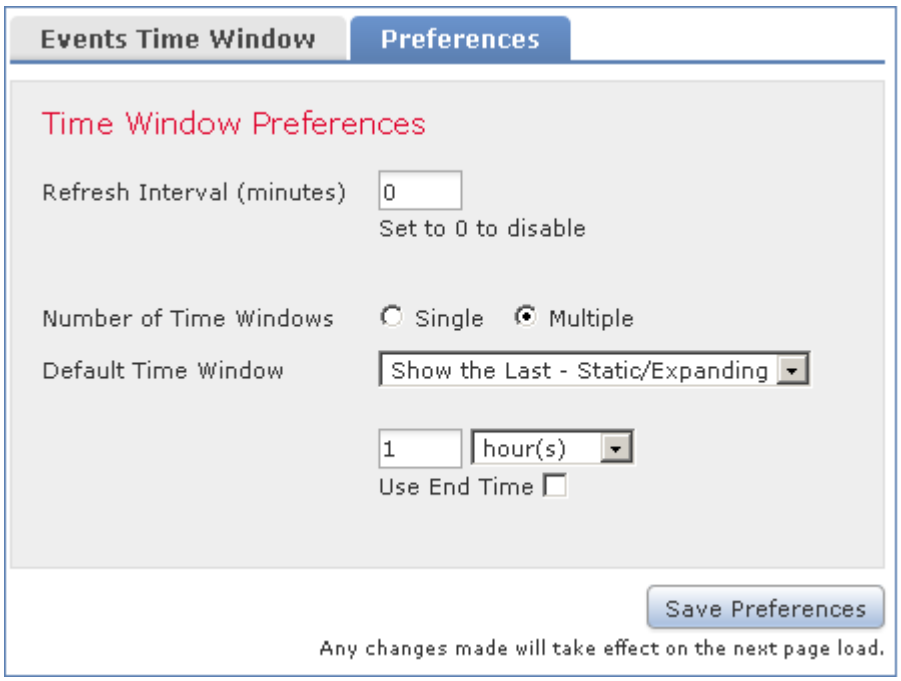
イベント タイプのデフォルトの時間枠の変更

ライセンス: 任意(Any)

イベントの分析中に、[日時(Date/Time)] ウィンドウの [設定(Preferences)] タブを使用し、表示しているイベントのタイプに対するデフォルトの時間枠を(イベント ビューの設定を使用せずに)変更することができます(デフォルトの時間枠(71-6 ページ)を参照してください)。

この方法でデフォルトの時間枠を変更すると、表示しているイベントのタイプのデフォルト時間枠のみが変わります。たとえば、複数の時間枠を設定した場合、[設定(Preferences)] タブでデフォルトの時間枠を変更すると、イベント、ヘルス モニタリング、または監査ログ ウィンドウのいずれかの設定が変更されます。つまり、最初のタブで示されている時間枠が変更されます。1 つの時間枠を設定した場合、[設定(Preferences)] タブでデフォルトの時間枠を変更すると、イベントのすべてのタイプのデフォルト時間枠が変わります。

次の図は、複数の時間枠が設定されているアプライアンスにおける、[設定(Preferences)] タブの Defense Center バージョンを示しています。



次の表で、[設定(Preferences)] タブで設定できるさまざまな設定について説明します。

表 58-26　時間枠の設定

設定	説明
更新間隔（Refresh Interval）	イベント ビューの更新間隔を分単位で設定します。ゼロを入力すると、更新オプションは無効になります。
タイム ウィンドウの数（Number of Time Windows）	使用する時間枠の数を指定します。 • 監査ログ、ヘルス イベント、および時間によって制約可能なイベントに基づいたワークフローに対してそれぞれ別のデフォルト時間枠を設定する場合は、[複数（Multiple）] を選択します。 • すべてのイベントに適用されるグローバルな時間枠を使用する場合は、[シングル（Single）] を選択します。
デフォルトのタイム ウィンドウ（Default Time Window）：最終を表示（Show the Last）- スライディング（Sliding）	この設定を選択すると、指定する長さのスライディングのデフォルト時間枠を設定できます。 アプライアンスは、特定の開始時刻（たとえば 1 時間前）から現在までに生成されたすべてのイベントを表示します。イベント ビューの変更と共に、時間枠は「スライド」して、常に最後の 1 時間内のイベントが表示されます。
デフォルトのタイム ウィンドウ（Default Time Window）：最終を表示（Show the Last）- 静的/拡張（Static/Expanding）	この設定を選択すると、指定する長さの、静的または拡張のデフォルト時間枠を設定できます。 **静的な**時間枠の場合（[終了時間を使用（Use End Time）] チェック ボックスをオンにした場合）、アプライアンスは特定の開始時間（1 時間前などの）から、最初にユーザがイベントを参照した時間までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。 **拡張**時間枠の場合（[終了時間を使用（Use End Time）] チェック ボックスをオフにしたの場合）、アプライアンスは特定の開始時間（1 時間前などの）から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。
デフォルトのタイム ウィンドウ（Default Time Window）：当日（Current Day）- 静的/スライディング（Static/Expanding）	この設定を選択すると、現在の日付に対して静的または拡張のデフォルト時間枠を設定できます。現在の日付は、現行セッションのタイム ゾーン設定に基づいて午前 0 時に始まります。 **静的な**時間枠の場合（[終了時間を使用（Use End Time）] チェック ボックスをオンにした場合）、アプライアンスは午前 0 時から、最初にユーザがイベントを参照した時間までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。 **拡張**時間枠の場合（[終了時間を使用（Use End Time）] チェック ボックスをオフにした場合）、アプライアンスは午前 0 時から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に 24 時間を超えて分析を続けた場合、この時間枠は 24 時間よりも長くなる可能性があることに注意してください。

表 58-26　時間枠の設定（続き）

設定	説明
デフォルトのタイム ウィンドウ（Default Time Window）：今週（Current Week）- 静的/拡張（Static/Expanding）	この設定を選択すると、現在の週に対して静的または拡張のデフォルト時間枠を設定できます。現在の週は、現行セッションのタイム ゾーン設定に基づいて直前の日曜日の午前 0 時に始まります。 **静的な**時間枠の場合（[終了時間を使用（Use End Time）] チェック ボックスをオンにした場合）、アプライアンスは午前 0 時から、最初にユーザがイベントを参照した時間までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。 **拡張**時間枠の場合（[終了時間を使用（Use End Time）] チェック ボックスをオフにした場合）、アプライアンスは日曜日の午前 0 時から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に 1 週間を超えて分析を続けた場合、この時間枠は 1 週間よりも長くなる可能性があることに注意してください。

イベントの分析中に時間枠の設定を変更するには、以下を行います。

アクセス：Admin/Maint/Any Security Analyst

手順 1　時間に制約されるワークフローで、時間範囲のアイコン（）をクリックします。

[日時（Date/Time）] ウィンドウが表示されます。

手順 2　[設定（Preferences）] タブを選択し、時間枠の設定の表に記載されているようにプリファレンスを変更します。

手順 3　[設定の保存（Save Preferences）] をクリックします。

設定が保存されます。

手順 4　以下の 2 つの対処法があります。

- 使用しているイベント ビューに新しいデフォルト時間枠の設定を適用するには、[適用（Apply）] をクリックして [日時（Date/Time）] ウィンドウを閉じてイベント ビューをリフレッシュします。
- デフォルトの時間枠設定を適用せずに分析を続けるには、[適用（Apply）] をクリックせずに [日時（Date/Time）] ウィンドウを閉じます。

時間枠の一時停止

ライセンス：任意（Any）

時間枠を一時停止することができます。これにより、ワークフローで提供されたデータのスナップショットを調べることができます。一時停止されないワークフローが更新されると、調査するイベントが削除されたり、調査対象外のイベントが追加されたりすることがあるため、この機能は有用です。

静的な時間枠は一時停止できないので注意してください。また、イベント時間枠の一時停止はダッシュボードには影響を与えず、ダッシュボードの一時停止も時間枠の一時停止に影響しません。

分析が完了したら、時間枠の一時停止を解除できます。時間枠の一時停止を解除すると、設定に従って時間枠が更新されます。また、一時停止を解除した時間枠を反映するようにイベント ビューが更新されます。

1 つのワークフロー ページで表示できるイベントよりも多くのイベントがデータベースに含まれている場合は、ページの下部にあるリンクをクリックして、他のイベントを表示できます（ワークフロー内の他のページへのナビゲート（58-40 ページ）を参照してください）。この際、同じイベントが 2 回表示されないように時間枠が自動的に一時停止します。準備ができたら、時間枠の一時停止を解除できます。

時間枠を一時停止する方法:

アクセス: Admin/Maint/Any Security Analyst

手順 1　時間枠のコントロールで、一時停止のアイコン（  ）をクリックします。

一時停止を解除するまで、時間枠は一時停止します。

時間枠の一時停止を解除する方法:

アクセス: Admin/Maint/Any Security Analyst

手順 1　時間範囲のコントロールで、再生のアイコン（  ）をクリックします。

時間枠の一時停止が解除され、設定に従って更新されます。現行の時間枠を反映するようにイベント ビューが更新されます。

イベントの制約

ライセンス: 任意（Any）

ワークフロー ページに表示される情報は、ユーザが設定した制約によって異なります。たとえばイベント ワークフローを最初に開いた場合、情報は、最後の 1 時間に生成されたイベントに制約されています。

ワークフローの次のページに進んで、表示されるデータを特定の値で制約する場合は、ページでこれらの値を持つ行を選択し、[表示（View）] をクリックします。現在の制約を保持し、すべてのイベントを含めた状態でワークフローの次のページに進むには、[すべて表示（View All）] を選択します。

（注）　複数の不可算値を持つ行を選択し、[表示（View）] を選択すると、複合的な制約が作成されます。複合的な制約の詳細については、複合的な制約の使用（58-38 ページ）を参照してください。

ワークフローのデータを制約するための 3 番目の方法があります自身が選択した値を持つ行のみが表示されるようページを制約し、ページの上部に示される制約リストに選択した値を追加するには、ページの行で値をクリックします。

たとえば、次のイベントでページ上の [イニシエータ IP（Initiator IP）] カラムの [10.10.60.119] をクリックすると、

	First Packet	Action	Initiator IP	Responder IP	Source Port / ICMP Type
	2013-03-10 23:27:34	Block	10.10.60.119	10.1.1.57	820 / tcp
	2013-03-10 23:27:34	Block	10.10.60.119	10.1.1.57	820 / tcp
	2013-03-10 22:19:28	Block	10.10.60.119	10.1.1.57	753 (rrh) / tcp
	2013-03-10 16:13:39	Block	10.10.32.124	10.10.60.165	856 / tcp

372156

制約されたページには、この IP アドレスを持つイベントのみが示されます。

Search Constraints (Edit Search Save Search)

Initiator IP　10.10.60.119

Connections | Intrusion | Malware | Files | Hosts | Applications | Application Details | Server

	First Packet	Action	Initiator IP	Responder IP	Source Port / ICMP Ty
	2013-03-10 23:27:34	Block	10.10.60.119	10.1.1.57	820 / tcp
	2013-03-10 23:27:34	Block	10.10.60.119	10.1.1.57	820 / tcp
	2013-03-10 22:19:28	Block	10.10.60.119	10.1.1.57	753 (rrh) / tcp
	2013-03-09 23:21:59	Block	10.10.60.119	10.1.1.57	822 / tcp

ヒント　監視ルールの条件に基づいて接続イベントを制約するための手順は少し異なり、いくつかの追加手順が必要になる場合があります。また、関連付けられているファイルや侵入情報によって接続イベントを制約することはできません。詳細については、接続およびセキュリティ インテリジェンスのデータ テーブルの使用 (39-30 ページ)を参照してください。

検索を使用して、ワークフローの情報を制約することもできます。検索ページで入力した検索条件はページの上部に制約として表示され、これに従って制約されたイベントが合わせて表示されます。Defense Center では、複合的な制約でない限り、他のワークフローにナビゲートしたときにも現在の制約が適用されます(ワークフロー間のナビゲート (58-41 ページ)を参照してください)。

検索する場合は、検索対象のテーブルに検索の制約を適用するかどうかに注意する必要があります。たとえば、クライアント データは接続サマリでは使用できません。接続で検出されたクライアントに基づいて接続イベントを検索し、結果を接続サマリ イベント ビューで表示すると、Defense Center では、制約が設定されていない場合と同じように接続データが表示されます。無効な制約は、非適用(N/A)とラベルが付けられ、取り消し線が付けられます。

次の表では、制約を適用する場合に実行できるそれぞれのアクションについて説明します。

表 58-27　検索の制約機能

目的	クリックする対象
ビューを、1 つの値に一致するイベントに制約する	テーブルの値。 たとえば、記録された接続のリストを表示する場合に、アクセス制御を使用して、自身が許可したものだけがリストに示されるよう制約する場合は、[アクション（Action）] カラムで [許可（Allow）] をクリックします。他の例では、侵入イベントを表示する場合に、宛先ポートが 80 のイベントのみがリストに示されるよう制約する場合は、[DST ポート/ICMP コード（DST Port/ICMP Code）] カラムで [80 (http)/tcp] をクリックします。
ビューを、複数の値に一致するイベントに制約する	これらの値を持つイベントのチェック ボックスをオンにし、[表示（View）] をクリックします。 行に複数の不可算値が含まれている場合は、複合的な制約が追加されることに注意してください。複合的な制約の詳細については、複合的な制約の使用（58-38 ページ）を参照してください。
制約を削除する	[制約の検索（Search Constraints）] ボックスで制約の名前をクリックします。
検索ページを使用して制約を編集する	[制約の検索（Search Constraints）] ボックスで [制約の編集（Edit Search）] をクリックします。 1 つのカラム内の複数の値について制約する場合は、この機能を使用します。たとえば、2 つの IP アドレスに関連しているイベントを表示する場合は、[検索の編集（Edit Search）] をクリックし、[検索（Search）] ページで対象の [IP アドレス（IP address）] フィールドを変更して両方のアドレスが含まれるようにして、[検索（Search）] をクリックします。
保存済みの検索として制約を保存する	[制約の検索（Search Constraints）] ボックスで [検索の保存（Save Search）] をクリックし、クエリに名前を指定します。 複合的な制約が含まれているクエリは保存できないことに注意してください。複合的な制約の詳細については、複合的な制約の使用（58-38 ページ）を参照してください。
別のイベント ビューで同じ制約を使用する	[移動先（Jump to）] をクリックしてイベント ビューを選択します。詳細については、ワークフロー間のナビゲート（58-41 ページ）を参照してください。 別のワークフローに切り替えると、複合的な制約は保持されないことに注意してください。複合的な制約の詳細については、複合的な制約の使用（58-38 ページ）を参照してください。
制約の表示を切り替える	展開の矢印（ ▲ ）をクリックします。制約のリストが長く、画面の大半を占有する場合に、この機能は役立ちます。

複合的な制約の使用

ライセンス: 任意（Any）

複合的な制約は、特定のイベントに対するすべての不可算値に基づいています。複数の不可算値を持つ行を選択する場合は、ページ上の対象行におけるすべての不可算値と一致するイベントのみを取得する複合的な制約を設定します。たとえば、送信元 IP アドレスが `10.10.31.17` で、宛先 IP アドレスが `10.10.31.15` である行と、送信元 IP アドレスが `172.10.10.17` で宛先 IP アドレスが `172.10.10.15` である行を選択すると、次のすべての結果が取得されます。

- 送信元 IP アドレスが 10.10.31.17 で、かつ宛先 IP アドレスが 10.10.31.15 のイベント

  または

- 送信元 IP アドレスが 172.10.31.17 で、かつ宛先 IP アドレスが 172.10.31.15 のイベント

複合的な制約と単純な制約を組み合わせると、複合的な制約の各セットに単純な制約が追加されます。たとえば、上記に記載されている複合的な制約に対して、プロトコル値 `tcp` の単純な制約を追加すると、次のすべての結果が取得されます。

- 送信元 IP アドレスが 10.10.31.17 で、かつ宛先 IP アドレスが 10.10.31.15 で、かつプロトコルが tcp であるイベント

  または

- 送信元 IP アドレスが 172.10.31.17 で、かつ宛先 IP アドレスが 172.10.31.15 で、かつプロトコルが tcp であるイベント

複合的な制約について、検索および検索の保存を実行することはできません。また、別のワークフローに切り替えるのに、イベント ビューのリンクを使用した場合、または [ワークフロー切り替え（switch workflow）] をクリックした場合は、複合的な制約は保持できません。複合的な制約が適用されているイベント ビューをブックマークしても、制約はブックマークに保存されません。

複合的な制約をすべて消去するには、[複合的な制約（Compound Constraints）] をクリックします。

テーブル ビュー ページのソートおよびレイアウトの変更

ライセンス: 任意（Any）

ワークフローのデータを表示する場合に、使用可能なカラムに基づいてデータをソートすることも、表示するカラムを削除して復元することもできます。カラムによってデータを昇順または降順でソートできます。

ヒント　カスタム ワークフローを作成すると、ページ上のカラムの配置を完全にカスタマイズしたり、ページのソート順を事前定義したりできます。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。

表 58-28　ソートおよびレイアウトの機能

目的	クリックする対象
カラムをソートする	カラムのタイトル。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。 ヒント　矢印のアイコン（▼）は、データのソート基準になっているカラム、およびソートが昇順である（上向き矢印のアイコン）か、または降順である（下向き矢印のアイコン）かを表します。
テーブル ビューからカラムを削除する	非表示にするカラムの見出しの閉じるアイコン（✖）。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。 カラムを無効にすると、そのカラムは（後で元に戻さない限り）そのセッションの期間中は無効になります。最初のカラムを無効にすると、[カウント（Count）] カラムが追加されることに注意してください。[カウント（Count）] カラムは無効にすることができません。 ヒント　他のカラムを表示または非表示にするには、[適用（Apply）] をクリックする前に、対象のチェック ボックスをオンまたはオフにします。無効になったカラムをビューに戻すには、展開アイコン（▲）をクリックして検索の制約を展開し、[無効になったカラム（Disabled Columns）] の下にあるカラム名をクリックします。
無効にしたカラムをビューに戻す	[無効になったカラム（Disabled Columns）] の下のカラム名。 デフォルトで無効になっているカラムを有効にすると、そのカラムは（後で無効にしない限り）セッションの期間中は有効になります。カラムを有効にしても同一行が複数作成されない場合、[カウント（Count）] カラムは削除されることに注意してください。

ドリルダウン ワークフロー ページのソート

ライセンス：任意（Any）

ワークフローまたはイベント ビューのデータを表示する場合に、使用可能なカラムに基づいてデータをソートしたり、表示するカラムを削除して復元したりすることができます。カラムによってデータを昇順または降順でソートできます。矢印のアイコン（▼）は、データのソート基準になっているカラム、およびソートが昇順である（上向き矢印のアイコン）か、または降順である（下向き矢印のアイコン）かを表します。

ヒント　カスタム ワークフローを作成すると、ページ上のカラムの配置を完全にカスタマイズしたり、ページのソート順を事前定義したりできます。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。

カラムをソートする方法：

アクセス：Admin/Maint/Any Security Analyst

手順 1　カラムのタイトルをクリックします。

ソートの順序を逆にする方法：

アクセス：Admin/Maint/Any Security Analyst

手順 1　カラムのタイトルをもう一度クリックします。

ワークフロー ページの行の選択

ライセンス：任意（Any）

ワークフロー ページで行を選択し、処理を行うにはいくつかの方法があります。

- ページ上のすべての行を選択するには、ページの上部にあるチェック ボックスをオンにします。

  ページの下部にあるいずれかのボタン（[表示（View）] や [削除（Delete）] など）をクリックすると、そのページ上のすべてのイベントにそのアクションを実行することができます。
- 1 行を選択するには、それぞれの行の隣にあるチェック ボックスをオンにします。

  ページの下部にあるいずれかのボタンをクリックすると、その行に関連付けられているイベントでのみ、そのアクションを実行することができます。
- 1 行を選択し、ワークフローの次のページでその行に関連するイベントを表示するには、矢印のアイコン（  ）をクリックします。

（注） 複数のページから一度に行を選択することはできません。

ワークフロー内の他のページへのナビゲート

ライセンス：任意（Any）

1 つのワークフロー ページで表示できるイベントよりも多くのイベントがデータベースに含まれている場合は、ページの下部にあるリンクをクリックして、さらにイベントを表示できます。

これらのリンクの 1 つをクリックすると時間枠が自動的に一時停止されるため、同じイベントが 2 回表示されません。準備ができたら時間枠の一時停止を解除できます。詳細については、イベント時間の制約の設定（58-27 ページ）を参照してください。

次の表で、ナビゲート リンクの使用方法について説明します。

表 58-29　ページのナビゲート

目的	クリックする対象
別のページを表示する	ページ番号をクリックし、表示するページを入力して Enter キーを押します
次のページを表示する	>
前のページを表示する	<
最後のページに移動する	>|
最初のページに移動する	|<

ワークフロー間のナビゲート

ライセンス：任意（Any）

ワークフロー ページの [移動先...（Jump to...）] ドロップダウン リストのリンクを使用して、他のワークフローへナビゲートできます。ドロップダウン リストを選択し、追加のワークフローを表示および選択します。

新しいワークフローを選択すると、（適切な場合は）、選択する行で共有されているプロパティおよび設定する制約が、新しいワークフローで使用されます。設定した制約またはイベントのプロパティが、新しいワークフローのフィールドにマップされない場合は、これらはドロップされます。また、ワークフローを切り替えた場合には、複合的な制約は保持されません。キャプチャ ファイルのワークフローの制約は、ファイルおよびマルウェアのイベント ワークフローのみに転送されます。

（注） 所定の時間範囲のイベント数を表示する場合、詳細なデータを利用できるイベントの数が、イベントの総数に反映されないことがあります。これは、ディスク領域の使用率を管理するために、古いイベントの詳細がシステムによってプルーニングされることがあるために発生します。イベント詳細のプルーニングを最小限にするために、対象の展開にとって最も重要なイベントだけを記録するようにイベント ロギングを調整できます。詳細については、ネットワーク トラフィックの接続のロギング（38-1 ページ）を参照してください。

時間枠を一時停止するか、または静的な時間枠を設定していない場合、ワークフローを変更したときに時間枠も変更されることに注意してください。詳細については、イベント時間の制約の設定（58-27 ページ）を参照してください。

[移動先（Jump to）] ドロップダウン リストを使用すると、次のテーブルのワークフローにすばやくアクセスできます。

- 接続イベント
- セキュリティ インテリジェンス イベント
- 侵入イベント
- マルウェア イベント
- ファイル イベント
- hosts
- 侵害の兆候
- アプリケーション
- アプリケーションの詳細
- サーバ
- ホスト属性
- 検出イベント
- ユーザ
- 脆弱性
- サードパーティの脆弱性
- 相関イベント
- ホワイトリスト イベント

この機能により、疑わしいアクティビティの調査が強化されます。たとえば、接続データを表示していて、内部ホストが異常に大量のデータを外部サイトに転送していることに気付いた場合は、応答側の IP アドレスとポートを制約として選択し、[アプリケーション（Applications）] ワークフローへ移動することができます。[アプリケーション（Applications）] ワークフローは応答側の IP アドレスとポートを IP アドレスとポートの制約として使用し、アプリケーションの種類などの追加情報を表示することができます。ページの上部にある [ホスト（Hosts）] をクリックして、リモート ホストのホスト プロファイルを表示することもできます。

アプリケーションに関する詳細を検索した後で、[相関イベント（Correlation Events）] を選択して接続データ ワークフローに戻る、制約から応答側の IP アドレスを削除する、制約にイニシエータの IP アドレスを追加する、[アプリケーションの詳細（Application Details）] を選択して、データをリモート ホストに転送するときに開始側のホストでユーザがどのクライアントを使用しているかを確認する、といったことができます。ポートの制約は、[アプリケーションの詳細（Application Details）] ページには転送されないことに注意してください。ローカル ホストを制約として保持したまま、追加情報を検索するために他のナビゲート ボタンを使用することもできます。

- ローカル ホストがいずれかのポリシーに違反しているかどうかを検出するには、IP アドレスを制約として保持したままで [移動先（Jump to）] 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。
- ホストに対して侵入ルールがトリガーされた（侵害を表している）かどうかを確認するには、[移動先（Jump to）] ドロップダウン リストから [侵入イベント（Intrusion Events）] を選択します。
- ローカル ホストのホスト プロファイルを表示し、ホストが、悪用された可能性のある脆弱性の影響を受けやすくなっているかどうかを判断するには、[移動先（Jump to）] ドロップダウン リストから [ホスト（Hosts）] を選択します。

ブックマークの使用

ライセンス：任意（Any）

イベントの分析中に所定の場所および時間にすばやく戻りたい場合には、ブックマークを作成します。ブックマークは、次の情報を保持します。

- 使用中のワークフロー
- 表示中のワークフローの部分
- ワークフローのページ番号
- 検索の制約
- 無効になっているカラム
- 使用している時間範囲

あるユーザが作成したブックマークは、ブックマーク アクセスを持っているすべてのユーザ アカウントで利用できます。これは、より詳細な分析を必要とするイベント セットを見つけた場合、簡単にブックマークを作成し、適切な権限を持った他のユーザに調査を引き継ぐことが可能であることを意味します。

（注） ブックマークに表示されているイベントが（ユーザによって直接、またはデータベースの自動クリーンアップによって）削除されると、そのブックマークにはイベントの元のセットは表示されません。

ブックマークの使用の詳細については、以下の項を参照してください。

- ブックマークの作成（58-43 ページ）では、新しいブックマークを作成する方法について説明します。
- ブックマークの表示（58-43 ページ）では、既存のブックマークを表示および使用する方法について説明します。
- ブックマークの削除（58-44 ページ）では、ブックマークを削除する方法について説明します。

ブックマークの作成

ライセンス：任意（Any）

新しいブックマークを作成するには、次の手順を使用します。

ブックマークを作成する方法：

アクセス：Admin/Maint/Any Security Analyst

手順 1　イベントの分析中に、表示されている対象のイベントで [このページをブックマーク（Bookmark This Page）] をクリックします。

[ブックマークの作成（Create a Bookmark）] ページが表示されます。

手順 2　[ブックマーク名（Bookmark Name）] フィールドで、ブックマークの名前を（最大 80 文字の英数字とスペースで）入力し、[ブックマークの保存（Save Bookmark）] をクリックします。

ブックマークが保存され、ブックマークしたイベントのページがもう一度表示されます。

ブックマークの表示

ライセンス：任意（Any）

既存のブックマークを表示して使用するには、次の手順を使用します。

ブックマークを表示する方法：

アクセス：Admin/Maint/Any Security Analyst

手順 1　イベント ビューから [ブックマークの表示（View Bookmarks）] をクリックします。

[ブックマーク（Bookmarks）] ページが表示されます。

手順 2　使用するブックマークの隣にある [表示（View）] をクリックします。

ブックマークしたページが表示されます。

（注）　最初にブックマークに表示されていたイベントが（ユーザによって直接、またはデータベースの自動クリーンアップによって）削除されると、そのブックマークにはイベントの元のセットは表示されません。

ブックマークの削除

ライセンス:任意（Any）

ブックマークを削除するには、次の手順を使用します。ブックマークを削除しても、そのブックマークによって取得されるイベントは影響を受けないことに注意してください。

ブックマークを削除する方法:

アクセス: Admin/Maint/Any Security Analyst

手順 1　イベント ビューから [ブックマークの表示（View Bookmarks）] をクリックします。

[ブックマーク（Bookmarks）] ページが表示されます。

手順 2　削除するブックマークの隣にある [削除（Delete）] をクリックします。

ブックマークが削除されます。

カスタムワークフローの使用

ライセンス:任意（Any）

Cisco提供の事前定義済みカスタム 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。

詳細については、以下を参照してください。

- カスタム ワークフローの作成（58-44 ページ）（カスタム ワークフローを作成する手順）
- カスタム接続データ ワークフローの作成（58-46 ページ）（接続データに基づいてカスタム ワークフローを作成する手順）
- カスタム ワークフローの表示（58-48 ページ）（イベントおよびカスタム テーブルに基づいてカスタム ワークフローを表示する手順）
- カスタム ワークフローの編集（58-49 ページ）（カスタム ワークフローを編集する手順）
- カスタム ワークフローの削除（58-50 ページ）（カスタム ワークフローを削除する手順）

カスタム ワークフローの作成

ライセンス:任意（Any）

Cisco 提供の事前定義済みカスタム 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。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 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。

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 58-30　カスタム ワークフローの最終ページ

ワークフローのベース	最終ページ
検出イベント	hosts
脆弱性	脆弱性の詳細
サードパーティの脆弱性	hosts
ユーザ	ユーザ
侵害の兆候	hosts
侵入イベント	packets

アプライアンスは、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）に基づいたカスタム ワークフローには最終ページを追加しません。

（注） 接続データに基づいてカスタム ワークフローを作成するための手順は少し異なります。詳細は、次の項カスタム接続データ ワークフローの作成を参照してください。

カスタム ワークフローを作成する方法:

アクセス: Admin/Any Security Analyst

手順 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。

[カスタム ワークフロー（Custom Workflows）] ページが表示されます。

手順 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。

[カスタム ワークフローの編集（Edit Custom Workflow）] ページが表示されます。

手順 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。

名前には最大 60 文字の英数字およびスペースを使用できます。

手順 4　オプションで、[説明（Description）] フィールドに、ワークフローの説明を入力します。

最大 80 文字の英数字およびスペースを使用できます。

手順 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。

手順 6　オプションで、[ページの追加（Add Page）] をクリックして、ワークフローに 1 つ以上のドリルダウン ページを追加します。

ドリルダウン ページのセクションが表示されます。

最大 80 文字の英数字（スペースは不可）を使用して、[ページ名（Page Name）] フィールドにページの名前を入力します。

[カラム 1（Column 1）] で、ソートの優先度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。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、[優先度のソート（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 [DST ポート/ICMP コード（DST Port/ICMP Code）] を選択します。

ページに表示するすべてのフィールドの指定が完了するまで、フィールドを選択してソートの優先度の設定を続けます。1 ページにつき最大 5 個のフィールドを指定できます。

（注）　ステップ 5 で [テーブル タイプ（Table Type）] として [脆弱性（Vulnerabilities）] を選択し、テーブル カラムとして [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。脆弱性の検索の詳細については、脆弱性の検索（50-58 ページ）を参照してください。

手順 7　オプションで、[テーブル ビューの追加（Add Table View）] をクリックして、ワークフローにテーブル ビュー ページを追加します。

（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。

手順 8　[保存（Save）] をクリックします。

新しいワークフローが保存され、カスタム ワークフローのリストに追加されます。

カスタム接続データ ワークフローの作成

ライセンス：FireSIGHT

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。接続のサマリ、接続グラフ、データセットなどの接続データの詳細については、接続およびセキュリティ インテリジェンスのデータについて（39-2 ページ）を参照してください。

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。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。

接続データに基づいてカスタム ワークフローを作成する方法:

アクセス: 管理

手順 1　[分析（Analysis）] > [カスタム（Custom）] > [カスタム ワークフロー（Custom Workflow）] を選択します。

手順 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。

[カスタム ワークフローの編集（Edit Custom Workflow）] ページが表示されます。

手順 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。

最大 60 文字の英数字およびスペースを使用できます。

手順 4　オプションで、[説明（Description）] フィールドに、ワークフローの説明を入力します。

最大 80 文字の英数字およびスペースを使用できます。

手順 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。

手順 6　オプションで、ワークフローに 1 つ以上のドリルダウン ページを追加します。

- 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。
- 接続のサマリ 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 ページの追加（Add Summary Page）] をクリックします。

いずれの場合も、ドリルダウン ページのセクションが表示されます。

最大 80 文字の英数字（スペースは不可）を使用して、[ページ名（Page Name）] フィールドにページの名前を入力します。

[カラム 1（Column 1）] で、ソートの優先度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。

ページに表示するすべてのフィールドの指定が完了するまで、フィールドを選択してソートの優先度の設定を続けます。1 ページにつき最大 5 個のフィールドを指定できます。

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、[優先度のソート（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 [受信側バイト数（Responder Bytes）] を選択します。

手順 7　オプションで、[グラフの追加（Add Graph）] をクリックして、ワークフローに 1 つ以上のグラフ ページを追加します。

グラフ セクションが表示されます。

最大 80 文字の英数字（スペースは不可）を使用して、[グラフ名（Graph Name）] フィールドにページの名前を入力します。

次に、ページに含めるグラフの種類（線グラフ、棒グラフ、または円グラフ）を選択します。

グラフの X 軸と Y 軸を選択し、どのようなデータをグラフ化するのかを指定します。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。

最後に、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。

手順 8　オプションで、[テーブル ビューの追加（Add Table View）] をクリックして、接続データのテーブル ビューを追加します。

手順 9　[保存（Save）] をクリックします。

新しいワークフローが保存され、カスタム ワークフローのリストに追加されます。

カスタム ワークフローの表示

ライセンス：任意（Any）

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 > ホスト（Analysis Hosts）] を選択します。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。

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。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。

詳細については、以下を参照してください。

- 事前定義のテーブルのカスタム ワークフローの表示（58-48 ページ）
- カスタム テーブルのカスタム ワークフローの表示（58-49 ページ）

事前定義のテーブルのカスタム ワークフローの表示

ライセンス：任意（Any）

カスタム テーブルに基づいて**いない**カスタム ワークフローを表示するには、次の手順を使用します。ワークフローの選択（58-19 ページ）に記載されているように、ワークフローのアクセスは使用しているプラットフォームとユーザ ロールによって異なることに注意してください。

事前定義のテーブルに基づいたカスタム ワークフローを表示する方法：

アクセス：Admin/Any Security Analyst

手順 1　ワークフローを使用する機能の表に記載されているように、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。

そのテーブルのデフォルト ワークフローの最初のページが表示されます。カスタム ワークフローも含め、別のワークフローを使用するには、現行のワークフロー タイトルの隣にある [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 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（58-27 ページ）を参照してください。

カスタム テーブルのカスタム ワークフローの表示

ライセンス：FireSIGHT

カスタム テーブルに基づいているカスタム ワークフローを表示するには、次の手順を使用します。

カスタム テーブルに基づいたカスタム ワークフローを表示する方法：

アクセス：Admin/Any Security Analyst

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、使用できるカスタム テーブルが示されます。

手順 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。

そのテーブルのデフォルト ワークフローの最初のページが表示されます。カスタム ワークフローも含め、別のワークフローを使用するには、現行のワークフロー タイトルの隣にある [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 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（58-27 ページ）を参照してください。

カスタム ワークフローの編集

ライセンス：任意（Any）

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。

カスタム ワークフローを編集する方法：

アクセス：Admin/Any Security Analyst

手順 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。

[カスタム ワークフロー（Custom Workflows）] ページが表示され、既存のカスタム ワークフローが示されます。

手順 2　編集するワークフロー名の隣にある編集アイコン（ ）をクリックします。

[ワークフローの編集（Edit Workflow）] ページが表示されます。

手順 3　ワークフローに必要な変更を加え、[保存（Save）] をクリックします。

ワークフローに対する変更が保存されます。

カスタム ワークフローの削除

ライセンス: 任意（Any）

次の手順は、不要になったカスタム ワークフローを削除する方法について説明します。

カスタム ワークフローを削除する方法:

アクセス: Admin/Any Security Analyst

手順 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。

[カスタム ワークフロー（Custom Workflows）] ページが表示され、使用できるカスタム ワークフローが示されます。

手順 2　削除するワークフロー名の隣にある削除アイコン（ ）をクリックします。

ワークフローが削除されます。