



ワークフロー

以下のトピックでは、ワークフローの使用方法について説明します。

- [概要：ワークフロー](#) (1 ページ)
- [定義済みワークフロー](#) (2 ページ)
- [カスタム テーブル ワークフロー](#) (12 ページ)
- [ワークフローの使用](#) (13 ページ)
- [統合イベントビューアでの作業](#) (44 ページ)
- [ブックマーク](#) (45 ページ)
- [ワークフローの履歴](#) (47 ページ)

概要：ワークフロー

ワークフローは Management 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、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することができます。

Management Center では、以下のタイプのワークフローを使用できます。

定義済みワークフロー

システムに付属のプリセットワークフローです。定義済みのワークフローの編集や削除を行うことはできません。ただし、定義済みワークフローをコピーして、そのコピーをカスタム ワークフローの基礎として使用することができます。

保存済みのカスタム ワークフロー

Management Center に付属の保存済みカスタム テーブルに基づくカスタム ワークフロー。これらのワークフローは編集、削除、コピーすることができます。

カスタム ワークフロー

特定のニーズに対応するために作成してカスタマイズするワークフロー、またはカスタム テーブルを作成するとシステムによって自動的に生成されるワークフローです。これらのワークフローは編集、削除、コピーすることができます。

通常、ワークフローに表示されるデータは、管理対象デバイスのライセンスおよび展開状況や、データを提供する機能を設定しているかどうかによって異なります。

定義済みワークフロー

以下の項で説明する定義済みワークフローは、システムに付属しているものです。定義済みワークフローを編集または削除することはできません。ただし、定義済みワークフローをコピーして、そのコピーをカスタムワークフローのベースとして使用することができます。

定義済み侵入イベントのワークフロー

次の表では、システムに備わっている定義済み侵入イベントのワークフローについて説明します。

表 1: 定義済み侵入イベントのワークフロー

ワークフロー名	説明
接続先ポート	接続先ポートは、通常、アプリケーションに紐付けされているため、このワークフローにより、異常な大容量アラートを経験しているアプリケーションを検出できます。接続先ポートカラムにより、ネットワーク上に存在してはならないアプリケーションを特定できます。
イベント特定	このワークフローでは、2つの有用な特徴を提供します。イベントが頻繁に発生する場合には、次のことを示します： <ul style="list-style-type: none"> ・誤検出 ・ワーム ・不正確な誤設定ネットワーク 発生頻度の低いイベントは、対象となる攻撃を最も確実に示す証拠であり、特別な注意を必要とします。
優先度および分類によるイベント	このワークフローでは、イベントとタイプのリストをそれぞれのイベントが発生した回数と共にイベントの優先度の順に示します。
接続先に対するイベント	このワークフローでは、攻撃されているホスト IP アドレスや攻撃の本質のハイレベルビューを提示します。利用可能な場合、攻撃に関与する国に関する情報を確認することもできます。
IP 特定	このワークフローでは、最も多くのアラートを発生するホスト IP アドレスを示します。イベント数が最も多いホストは、対外に向けて、受信しているワームタイプのトラフィック（調整を必要とする適切な場所を示す）であるか、またはアラートの原因を決定するために更に調査を必要とします。イベント数が最も少ないホストは、対象となる攻撃を受ける可能性があるため、調査の根拠となります。イベント数が少ない場合は、ホストがネットワークに属していないことを示す場合もあります。

ワークフロー名	説明
影響度と優先度	このワークフローにより、すぐに再度発生している影響度の高いイベントを検索します。レポートによる影響レベルは、イベントが発生した時間数で示します。この情報を使用して、最も頻繁に再発する影響度の高いイベントを特定できます。これがネットワーク上での広範な攻撃の指標となります。
影響度と送信元	このワークフローにより、進行中の攻撃の送信元を特定できます。レポートされた影響レベルは、イベントに対する関連の送信元 IP アドレスにより示します。たとえば、影響レベルが 1 のイベントは、同じ送信元 IP アドレスから繰り返し発生している場合、これらは特定された脆弱なシステムであり、送信元 IP アドレスを対象としている攻撃者を示すこともあります。
接続先への影響	このワークフローを使用して、脆弱なコンピュータ上で繰り返し発生しているイベントを特定できます。このため、これらのシステムでの脆弱性を指定し、進行中の攻撃を停止できます。
送信元ポート	このワークフローは、最もアラートを発生しているサーバーを示します。この情報を使用して、調整が必要なエリアを特定し、注意を要するサーバを決定できます。
送信元と接続先	このワークフローでは、高いレベルのアラートを共有するホスト IP アドレスを特定します。リストのトップのペアは誤検出の可能性もあり、調整が必要なエリアを特定することもあります。評価する必要のないリソースを評価するユーザまたはネットワークに属していないホストについては、対象となる攻撃リストの下部にあるペアを確認できます。

定義済みマルウェアのワークフロー

次の表では、Management Center に備えられた定義済みマルウェアのワークフローについて説明します。定義済みマルウェアのワークフローでは、必ずマルウェア イベントのテーブルビューを使用します。

表 2: 定義済みマルウェアのワークフロー

ワークフロー名	説明
マルウェア サマリ	このワークフローでは、ネットワーク トラフィック内で検出されたか、または AMP for Endpoints Connector によって検出されたマルウェアのリストを提供します。これらのリストは、それぞれの脅威ごとにグループ化されます。
マルウェア イベント サマリ	このワークフローでは、異なるマルウェア イベントのタイプやサブタイプの明細が迅速に表示されます。
ホスト受信マルウェア	このワークフローでは、マルウェアを受信したホスト IP アドレスのリストが表示されます。このリストは、マルウェア ファイル関連の処理ごとにグループ化されます。
ホスト送信マルウェア	このワークフローでは、マルウェアを送信したホスト IP アドレスのリストが表示されます。このリストは、マルウェア ファイル関連の処理ごとにグループ化されます。

ワークフロー名	説明
アプリケーション導入マルウェア	このワークフローでは、ファイルを受信したホスト IP アドレスのリストが表示されます。このリストは、受信したファイルの関連したマルウェアの処理によってグループ化されません。

定義済みファイルのワークフロー

次の表では、Management Center に備えられる定義済みファイル イベントのワークフローについて説明しています。定義済みファイル イベントのワークフローでは、必ずファイル イベントのテーブル ビューを使用します。

表 3: 定義済みファイルのワークフロー

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)	このワークフローでは、ファイルを送信したホスト IP アドレスのリストを表示します。このリストは、これらのファイルの関連したマルウェアの処理によってグループ化されません。

定義済みキャプチャ ファイルのワークフロー

次の表では、Management Center での定義済みキャプチャ ファイルのワークフローについて説明しています。定義済みキャプチャ ファイルのワークフローは、必ずキャプチャ ファイルのテーブル ビューを使用します。

表 4: 定義済みキャプチャ ファイルのワークフロー

ワークフロー名	説明
キャプチャ ファイル サマリ	このワークフローでは、タイプ、カテゴリ、脅威スコアに基づいてキャプチャ ファイルの詳細を提示します。
ダイナミック分析ステータス (Dynamic Analysis Status)	このワークフローでは、ダイナミック分析用に提示されたか否かに基づいて、キャプチャ ファイルの数を表示します。

定義済み接続データのワークフロー

次の表では、Management Center に備えられる定義済み接続データのワークフローについて説明しています。定義済み接続データ ワークフローでは、必ず接続データのテーブル ビューを使用します。

表 5: 定義済み接続データのワークフロー

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。

ワークフロー名	説明
トラフィックに基づいたアプリケーション (Traffic by Application)	<p>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。</p> <p>アプリケーションカウントは、アプリケーション接続と照合した各ディテクタが反映されます。トラフィックを照合したアプリケーションプロトコル、Web アプリケーション、クライアント ディテクタ、または内部ディテクタと、トラフィックがモバイルデバイスから発信されたか、または暗号化セッションの一部かによって、同じアプリケーションセッションがリスト内に複数回表示される場合があります。アプリケーションがクライアントフローに表示されていても特定のクライアント ディテクタがない場合は、汎用クライアントが報告される場合があります。</p> <p>たとえば、同じ YouTube セッションが (YouTube Web アプリケーションディテクタと照合したため) YouTube と (内部 YouTube ディテクタがクライアントセッション内に通常観られる特性と照合したため) YouTube client として表示される場合があります。</p> <p>接続イベント内の情報とネットワークのネットワークマップを使用して特定のアプリケーション接続の他のコンテキストを特定します。</p>
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、アドレスにコンタクトする一意レスポンドの数に基づく、監視対象のネットワーク セグメントでの 10 個の最もアクティブな開始ホスト IP アドレスのグラフが含まれています。

定義済みセキュリティ インテリジェンスのワークフロー

次の表では、Management Center に備えられている定義済みセキュリティ インテリジェンスのワークフローについて説明しています。定義済みセキュリティ インテリジェンスのワークフローでは、必ずセキュリティ 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。

表 6: 定義済みセキュリティ インテリジェンスのワークフロー

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 イベントのワークフローと同じものですが、セキュリティ インテリジェンス サマリ ページから始まり、カテゴリや数ごとにセキュリティ インテリジェンス イベントのみのリストを表示します。
セキュリティ インテリジェンスと DNS 詳細	このワークフローは、セキュリティ インテリジェンス イベントのワークフローと同じものですが、DNS 詳細のあるセキュリティ インテリジェンス ページから始まり、カテゴリや DNS 関連特性ごとにセキュリティ インテリジェンス イベントのリストを表示します。

定義済みホストのワークフロー

次の表では、ホスト データと共に使用できる定義済みワークフローについて説明します。

表 7: 定義済みホストのワークフロー

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 テーブルに基づくワークフロー ビューでは、ホストに関連付けられているすべての IP アドレスのデータを容易に表示できます。
オペレーティング システム サマリ (Operating System Summary)	このワークフローを用いて、ネットワーク上で使用中のオペレーティングシステムを分析できます。

定義済み侵害の兆候のワークフロー

次の表では、IOC (侵害の兆候) と共に使用できる定義済みワークフローについて説明します。

表 8: 定義済み侵害の兆候のワークフロー

ワークフロー名	説明
ホストの侵害の兆候	このワークフローは、数とカテゴリごとにグループ化した IOC データのサマリー ビューから始まり、さらにサマリ データをイベント タイプごとに分割した詳細ビューを表示します。 [分析 (Analysis)] > [ホスト (Hosts)] メニューからこのワークフローにアクセスします。
ホストごとの侵害の兆候	このワークフローを使用して、最も侵害する可能性の高いネットワーク上のホストを判断できます (IOC データに基づく)。 [分析 (Analysis)] > [ホスト (Hosts)] メニューからこのワークフローにアクセスします。
ユーザの侵害の兆候	このワークフローは、数とカテゴリごとにグループ化した IOC データのサマリー ビューから始まり、さらにサマリ データをイベント タイプごとに分割した詳細ビューを表示します。 [分析 (Analysis)] > [ユーザ (Users)] メニューからこのワークフローにアクセスします。
ユーザごとの侵害の兆候	このワークフローを使用して、侵害に関与している可能性が最も高いネットワーク上のユーザを判断します (IOC データに基づく)。 [分析 (Analysis)] > [ユーザー (Users)] メニューからこのワークフローにアクセスします。

定義済みアプリケーションワークフロー

次の表では、アプリケーションデータと共に使用できる定義済みワークフローについて説明しています。

表 9: 定義済み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、ネットワーク上で実行中のそれぞれ予想されるビジネスとの関連性レベルのアプリケーションを分析できます。そのため、ネットワークリソースが適切に使用されているかを監視できます。
アプリケーション カテゴリ	このワークフローを使用して、ネットワーク上で各カテゴリの実行中のアプリケーションを分析できます (電子メール、検索エンジン、ソーシャルネットワーキングなど)。そのため、ネットワークリソースが適切に使用されているかを監視できます。
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、ネットワーク上でそれぞれ予想されるセキュリティリスクレベルの実行中のアプリケーションを分析できます。このため、ユーザのアクティビティの考えられるリスクを予想し、適切なアクションを取ることができます。

ワークフロー名	説明
アプリケーション サマリ	このワークフローを使用して、ネットワークのアプリケーションや関連するホストに関する詳細情報を取得できます。このため、ホストのアプリケーションのアクティビティを正確に調べることができます。
アプリケーション	このワークフローを使用して、ネットワーク上の実行中のアプリケーションを分析できます。このため、ネットワークの使用状況の概要を取得できます。

定義済みアプリケーション詳細ワークフロー

次の表では、アプリケーションの詳細とクライアントデータと共に使用できる定義済みワークフローについて説明しています。

表 10: 定義済み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
アプリケーションの詳細	このワークフローを用いて、ネットワーク上のクライアントアプリケーションをさらに詳しく分析することができます。また、このワークフローでは、クライアントアプリケーションのテーブルビューを表示し、その後ホストビューを表示します。
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と、その後にホストビューが含まれます。

定義済みサーバーのワークフロー

次の表では、サーバデータと共に使用できる定義済みワークフローについて説明します。

表 11: 定義済みサーバのワークフロー

ワークフロー名	説明
数別ネットワーク アプリケーション	このワークフローを使用して、ネットワーク上で最も多く使用されるアプリケーションを分析できます。
ヒット別ネットワーク アプリケーション	このワークフローを使用して、ネットワーク上で最もアクティブなアプリケーションを分析できます。
サーバの詳細	このワークフローを使用して、ベンダや検出されたサーバアプリケーションプロトコルのバージョンを詳細に分析できます。
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と、その後にホストビューが含まれます。

定義済みホスト属性のワークフロー

次の表では、ホスト属性データと共に使用できる定義済みワークフローについて説明します。

表 12: 定義済みホスト属性のワークフロー

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 IP アドレスやホスト ステータスを監視できます。

定義済み検出イベントのワークフロー

次の表では、検出データとアイデンティティデータの表示に使用できる定義済みワークフローについて説明しています。

表 13: 定義済み検出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	このワークフルーでは、テーブルビュー形式の検出イベント詳細リストが提示され、その次にホスト ビューが提示されます。

定義済みユーザー ワークフロー

次の表では、ユーザ検出データとユーザ アイデンティティ データの表示に使用できる定義済みワークフローを説明します。

表 14: 定義済みユーザワークフロー

ワークフロー名	説明
アクティブセッション (Active Sessions)	このワークフローでは、ユーザ ID ソースによって収集されるアクティブセッションが表示されます。
Users	このワークフローでは、ユーザ ID ソースによって収集されるユーザ情報リストが表示されます。

定義済み脆弱性のワークフロー

次の表では、Management Center に備えられている定義済み脆弱性のワークフローについて説明します。

表 15: 定義済み脆弱性のワークフロー

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、ネットワーク上で検出されたホストに適用するこれらのアクティブな脆弱性のみのテーブルビューなど、データベース内の脆弱性を検討できます。このワークフローにより脆弱性詳細ビューが提供され、これには制約に適合するそれぞれの脆弱性に関する詳細な説明が含まれています。

定義済みのサードパーティ脆弱性のワークフロー

次の表では、Management Centerに備えられた定義済みのサードパーティ脆弱性のワークフローについて説明します。

表 16: 定義済みのサードパーティ脆弱性のワークフロー

ワークフロー名	説明
IP アドレスごとの脆弱性	このワークフローを使用して、監視対象のネットワーク上のホスト IP アドレスごとに検出されたサードパーティの脆弱性の数をすぐに確認できます。
送信元ごとの脆弱性	このワークフローを使用して、QualysGuard Scanner などサードパーティの脆弱性の送信元ごとに検出されたサードパーティの脆弱性の数をすぐに確認できます。

定義済み関連ワークフロー、許可 (Allow) リストワークフロー

関連データ、allow リストイベント、allow 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 17: 定義済み関連ワークフロー

ワークフロー名	説明
関連イベント (Correlation Events)	このワークフローには、関連イベントのテーブルビューが含まれています。
許可 (Allow) イベントの一覧表示	このワークフローには、allow リストイベントのテーブルビューが含まれています。
ホスト違反数 (Host Violation Count)	このワークフローには、少なくとも1つのallow リストに違反しているすべてのホスト IP アドレスのリストを示す一連のページが表示されます。
許可 (Allow) 違反の一覧表示	このワークフローには、すべての違反を列挙し、リストのトップに直前に検出された違反を示す、allow リスト違反のテーブルビューが含まれています。テーブル内の各列には、検出された違反が1つずつ表示されます。

ワークフロー名	説明
ステータス (Status)	このワークフローには、修復ステータスのテーブルビューを含み、違反したポリシー名、適用された修復名や修復状況が表示されています。

定義済みのシステムのワークフロー

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 18: 追加の定義済みワークフロー

ワークフロー名	説明
Audit Log (監査ログ)	このワークフローでは、監査イベントをリストした監査ログのテーブルビューを含みます。
ヘルスイベント (Health Events)	このワークフローでは、ヘルス監視ポリシーによりトリガーされるイベントを表示します。
ルール更新インポートログ (Rule Update Import Log)	このワークフローは、成功したルールの更新インポートと失敗したルールの更新インポートに関する情報をリストしたテーブルビューを含みます。
スキャン結果 (Scan Results)	このワークフローには、それぞれ完了したスキャンをリストしたテーブルビューを含みます。

カスタム テーブル ワークフロー

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ディスカバリ 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 テーブルを作成すると、システムは自動的にワークフローを作成します。このテーブルを使って関連す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。

ワークフローの使用

手順

ステップ1 [ワークフローの選択 \(15 ページ\)](#) 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。

ステップ2 現在のワークフロー内で移動します。

- 選択したイベントデータタイプで利用可能な列をすべて表示するには、[テーブルビューページの使用 \(23 ページ\)](#) を参照してください。
- 選択したイベントデータタイプで利用可能な列のサブセットを表示するには、[ドリルダウンページの使用 \(22 ページ\)](#) を参照してください。
- ワークフローの次のページの対応する行を表示するには、[下矢印 (Down-Arrow)] (▼) をクリックします。
- マルチページワークフローのページ間を移動するには、各ページの下部にあるツールを使用します。[ワークフローページのトラバーサルツール \(19 ページ\)](#) を参照してください。
- 別のタイプのイベントに対してワークフロー内で適用された同じ制約を表示するには、[移動先 (Jump to)] をクリックし、ドロップダウンリストからイベントビューを選択します。

ステップ3 現在のワークフローの表示を変更します。

- ページ上で1つ以上の行のチェックボックスにマークを付けて、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)] など) をクリックして、選択したすべての行に対してそのアクションを実行します。
- 行の上部にあるチェックボックスにマークを付けて、ページ上のすべての行を選択し、ページの下部にあるいずれかのボタン ([表示 (View)] など) をクリックして、ページ上のすべての行に対してそのアクションを実行します。

- 非表示にする列ヘッダーの [閉じる (Close)] (✕) をクリックして、表示する列を制約します。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、該当するチェックボックスをオンまたはオフにします。無効にした列をビューに戻すには、展開の矢印をクリックして検索の制約を展開し、[無効な列 (Disabled Columns)] の下の列名をクリックします。

- 選択したフィールドに対して選択した値でデータビューを制約します。詳細については、[イベントビューの制約 \(40 ページ\)](#) および[複合イベントビューの制約 \(42 ページ\)](#) を参照してください。

- イベントビューの時間の制約を変更します。ページの右上隅に表示される日付の範囲は、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 \(33 ページ\)](#) を参照してください。
 - (注) 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关に關係なく) 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ります。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。
- データを列でソートするには、列の名前をクリックします。ソート順序を反転させるには、もう一度列の名前をクリックします。矢印は、データのソート基準になっている列、およびソートが昇順か降順かを表します。
- 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。

ステップ4 現在のワークフロー内の追加データを表示します。

- ファイルのトラジェクトリマップを新しいウィンドウで表示するには、ファイル名と SHA-256 ハッシュ値の列のネットワーク ファイル トラジェクトリ アイコンをクリックします。アイコンは、ファイルステータスによって異なります。[ファイル トラジェクトリ アイコン \(20 ページ\)](#) を参照してください。
- IPアドレスに関連付けられたホストプロファイルのポップアップウィンドウを表示するには、IPアドレスの列のホストプロファイルアイコンをクリックします。アイコンは、ファイルステータスによって異なります。[ホストプロファイルのアイコン \(20 ページ\)](#) を参照してください。
- ファイルに関連付けられた最も高い脅威スコアの動的分析サマリーレポートを表示するには、いずれかの脅威スコア列の脅威スコアアイコンをクリックします。アイコンは、ファイルの最も高い脅威スコアによって異なります。[脅威スコア アイコン \(21 ページ\)](#) を参照してください。
- ユーザープロファイル情報を表示するには、いずれかのユーザーID列で[ユーザー (User)] (または、侵害の兆候に関連付けられたユーザーの場合は、[赤色のユーザー (RedUser)]) をクリックします。ユーザーアイコンは、そのユーザーがデータベースにない場合 (つまり、AMP for Endpoints Connector ユーザーの場合) は淡色表示されます。
- サードパーティの脆弱性の脆弱性詳細を表示するには、いずれかのサードパーティの脆弱性の ID 列の [脆弱性 (Vulnerability)] をクリックします。
- 集約データポイントを表示する場合は、ポイントをフラグの上に合わせて国名を表示します。
- 個々のデータポイントを表示する場合は、フラグをクリックして、[位置情報 \(25 ページ\)](#) に記載されている地理位置情報詳細を表示します。

ステップ5 別のワークフローに移動します。

別のワークフローを使用して同じイベントタイプを表示するには、ワークフローのタイトルの横にある（ワークフローの切り替え）をクリックして、使用するワークフローを選択します。スキャン結果には別のワークフローを使用できないことに注意してください。

ユーザー ロールによるワークフローへのアクセス

ワークフローへのアクセスはユーザのロールにより異なります。詳細については、次の表を参照してください。

ユーザ ロール	アクセス可能なワークフロー
管理者 (Administrator)	すべてのワークフローにアクセスできます。また、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。
メンテナンスユーザ	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とセキュリティアナリスト (読み取り専用)	侵入、マルウェア、ファイル、接続、検出、脆弱性、相関、ヘルスワークフローにアクセスできます。

ワークフローの選択

システムには、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が用意されています。

表 19: 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
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
相関イベント	[分析 (Analysis)] > [相関 (Correlation)]	相関イベント 許可 (Allow) イベントの一覧表示 許可 (Allow) 違反の一覧表示 ステータス

機能	メニューパス	オプション
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
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
ホスト イベント	[分析 (Analysis)]>[ホスト (Hosts)]	ネットワークマップ ホスト 侵害の兆候 アプリケーション アプリケーションの詳細 (Application Details) サーバー ホスト属性侵害の兆候 検出イベント
侵入イベント	[分析 (Analysis)]>[侵入 (Intrusions)]	イベント 確認済みイベント
ユーザ イベント	[分析 (Analysis)]>[ユーザ (Users)]	アクティブ セッション (Active Sessions) ユーザー アクティビティ Users 侵害の兆候
脆弱性イベント	[分析 (Analysis)]>[ホスト (Hosts)]	脆弱性 サードパーティの脆弱性
スキャン結果	[ポリシー (Policies)]>[アクション (Actions)] >[スキャナ (Scanners)]	—
ヘルス イベント	[システム (System)]>[ヘルス (Health)]>[イベント (Events)]	—
監査イベント	[システム (System)]>[モニタリング (Monitoring)]	監査 (Audit)

機能	メニューパス	オプション
ルール更新インポート ログ	[システム (System)]>[更新 (Updates)] バージョン 7.2.0 ~ 7.2.5 : [システム (System)]>[更新 (Updates)] バージョン 7.4.1 以降 : [システム (System)]>[コンテンツの更新 (Content Updates)]	ルールの更新

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。イベントビューの設定項目を設定することによって、別のデフォルトワークフローを指定することができます。ワークフローへのアクセス権限は、ユーザーの役割によって異なります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

関連トピック

[イベントビューの設定](#)

ワークフローのページ

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で共通の機能セットを共有しています。ワークフローには、数種類のページを含めることができます。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。

ワークフローのドリルダウンのページとテーブルビューのページを使用すれば、データのビューをすばやく絞り込むことができるため、分析にとって重要なイベントに集中できます。テーブルビューのページとドリルダウンのページの両方で、ユーザが表示するイベントセットに制約を適用したり、ワークフローをナビゲートしたりするために使用できる機能が多数サポートされています。ドリルダウンページ、またはワークフロー内のテーブルビューでデータを表示する場合、ソートに使用できる任意のカラムに基づいてデータを昇順または降順でソートできます。1つのワークフローのページに表示できるイベント数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。準備ができたなら時間枠の一時停止を解除できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

テーブルビュー

ページがデフォルトで有効になっている場合、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。

最適なパフォーマンスを得るには、必要なカラムのみを表示します。表示されるカラムが多いほど、データを表示するために必要なリソースが多くなります。

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可能性がある場合に、([カウント (Count)]カラム以外に) 表示されるカラムが6つ以下であるときは、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。

ドリルダウン ページ

ドリルダウン ページは、通常テーブル ビューのページに移動する前に調査対象を絞り込むために使用する中間ページです。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)]カラムだけが含まれています。また、侵入イベントのドリルダウンページには、[優先順位 (Priority)]、[影響フラグ (Impact Flag)]、[インラインの結果 (Inline Result)]、および [メッセージ (Message)]カラムが含まれています。

ドリルダウンページを使用すれば、表示するイベントの範囲を絞り込んだり、ワークフローで先へ進んだりできます。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、その値で制約を加えて、ワークフローの次のページに進んだ場合)、選択した値に一致するイベントをさらに詳しく調べることができます。ドリルダウン ページで値をクリックした場合、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。事前定義のワークフローの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。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。

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。

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。

- ホストビューとは、アプリケーション、アプリケーションの詳細、検出イベント、ホスト、侵害の兆候 (IOC) 、サーバー、allowリスト違反、ホスト属性、またはサードパー

ティ製の脆弱性に基づいた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、ユーザーは、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。

- ユーザの詳細ビューとは、ユーザ、ユーザアクティビティ、およびユーザの侵害の兆候に基づいたワークフローの最終ページです。
- 脆弱性の詳細ビューとは、Cisco の脆弱性に基づいたワークフローの最終ページです。
- 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。

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 インターフェイスでは、ワークフローの最終ページに制約が表示されませんが、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。

ワークフロー ページのナビゲーション ツール

ワークフローのページには、ページ間の移動と、イベントの分析中に表示する情報の選択を容易にする視覚的なキューが用意されています。

ワークフロー ページのトラバーサル ツール

ワークフローに複数のデータ ページが含まれている場合は、各ページの下部にワークフロー内のページ数と、ページ間を移動するために使用できるツールが表示されます。これらのツールを次の表に示します。

表 20: ワークフロー ページのトラバーサル ツール

ページのトラバーサル ツール	操作
ページ番号 (別のページを表示するには、表示する番号を入力して Enter キーを押します。)	別のページを表示する
>	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

ファイルトラジェクトリアイコン

ワークフロー ページで、新しいウィンドウにファイルのトラジェクトリ マップを表示する機会があるときは、ネットワークトラジェクトリアイコンが表示されます。このアイコンは、ファイルのステータスによって変わります。





表 21: ファイルトラジェクトリアイコン

ファイルトラジェクトリアイコン	ファイルステータス
正常 (Clean)	クリーン
マルウェア	マルウェア
カスタム検出	カスタム検出
不明	不明
使用不可	使用不可

ホストプロファイルのアイコン

ワークフロー ページでは、IP アドレスに関連付けられたホストプロファイルをポップアップウィンドウで表示でき、ホストプロファイルアイコンが表示されます。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)。このアイコンは、ホストのステータスによって異なって表示されます。

表 22: ホストプロファイルのアイコン

ホストプロファイルのアイコン	ホストステータス
	ホストは潜在的に危険にさらされているとタグ付けされていません。
	ホストは、トリガーされた侵害の兆候 (IOC) ルールによって潜在的に危険にさらされているとタグ付けされています。
	ブロックリストに追加 (セキュリティインテリジェンスデータに基づいて、トラフィックフィルタリングを実行している場合にのみ表示されます)。
	モニターするように設定されたブロックリストに追加 (セキュリティインテリジェンスデータに基づいて、トラフィックフィルタリングを実行している場合にのみ表示されます)。

脅威スコアアイコン

ワークフローページで、ファイルに関連付けられているスコアが最も高い脅威に関する動的分析サマリレポートを表示すると、脅威スコアアイコンが表示されます。このアイコンは、ファイルの最も高い脅威スコアに応じて異なります。

表 23: 脅威スコアアイコン

脅威スコアアイコン	脅威スコアレベル
低	低 (Low)
中規模	中規模
高 (High)	大きい
非常に高い	非常に高い (Very high)

ユーザーアイコン

ワークフローページで、ユーザ名に関連付けられているユーザ ID がポップアップウィンドウで表示されると、同時にユーザアイコンも表示されます。

表 24: ユーザアイコン

ユーザアイコン	ユーザーステータス
ユーザー (User)	ユーザは侵害の兆候に関連付けられていません。
赤色のユーザー	ユーザは 1 つ以上の侵害の兆候に関連付けられています。

ワークフロー ツールバー

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あります。次の表で、ツールバー上の各リンクについて説明します。

表 25: ワークフロー ツールバーのリンク

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る場合は後で同じデータに戻ることができます。
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、レポートデザイナーを開きます。

機能	説明
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。
ブックマークの表示	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。
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。

関連トピック

- [イベントビューからのレポートテンプレートの作成](#)
- [ダッシュボードについて](#)
- [イベントの検索](#)
- [ブックマーク \(45 ページ\)](#)
- [ブックマークの作成 \(46 ページ\)](#)
- [ブックマークの表示 \(46 ページ\)](#)

ドリルダウン ページの使用

手順

ステップ 1 「[ワークフローを使用する機能](#)」の説明に従って、適切なメニューパスとオプションを選択してワークフローにアクセスします。

ステップ 2 すべてのワークフローで、次のオプションを選択できます。

- 特定の値に制限して、次のワークフロー ページにドリルダウンするには、行内の値をクリックします。この処理はドリルダウンページでのみ可能であることに注意してください。テーブルの行内の値をクリックしても、テーブルビューが制約されるだけで、次のページにはドリルダウンしません。
- いくつかのイベントによって制約したまま次のワークフローページにドリルダウンするには、次のワークフロー ページに表示させるイベントの横のチェック ボックスを選択し、[表示 (View)] をクリックします。
- 現在の制限を維持して次のワークフロー ページにドリルダウンするには、[すべて表示 (View All)] をクリックします。

ヒント テーブル ビューでは、必ずページ名に「Table View」が含まれます。

テーブルビューページの使用

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、脆弱性の詳細ページでは利用できない機能が用意されています。これらの機能は次のように使用します。

手順

- ステップ 1** [ワークフローの選択 \(15 ページ\)](#) の説明に従って、適切なメニューパスとオプションを選択してワークフローにアクセスします。
- ステップ 2** ワークフローの名前の下に表示されるワークフローパスからテーブルビューを選択します。
- ステップ 3** イベントデータがリモートに保存されている場合、ローカルデータとリモートデータのどちらを表示するかを選択するオプションが表示されることがあります。
「[Secure Network Analytics アプライアンスに保存されている接続イベントを使用した Secure Firewall Management Center での作業 \(23 ページ\)](#)」を参照してください。
- ステップ 4** 必要に応じて、次に示す機能を使用してテーブルビュー内に配置したり、移動したりします。
 - 無効なカラムのリストを表示するには、[検索制約 (Search Constraints)] の [展開矢印 (Expand Arrow)] (▶) をクリックします。
 - 無効なカラムのリストを非表示するには、[検索制約 (Search Constraints)] の [折りたたみ矢印 (Collapse Arrow)] (▼) をクリックします。
 - 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 [展開矢印 (Expand Arrow)] (▶) 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。
 - カラムを表示または非表示 (無効) にするには、各カラム名の横にある [クリア (Clear)] (X) 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、該当するチェックボックスをオンまたはオフにして、どのカラムを表示するかを指定し、[適用 (Apply)] をクリックします。

Secure Network Analytics アプライアンスに保存されている接続イベントを使用した Secure Firewall Management Center での作業

デバイスがセキュリティ分析とロギング (オンプレミス) を使用して Secure Network Analytics アプライアンスに接続イベントを送信している場合、Management Center のイベントビューアとコンテキストエクスプローラでリモートに保存されたイベントを表示および操作し、レポートの生成時にそれらのイベントを含めることができます。Management Center のイベントから相互起動して、Secure Network Analytics アプライアンスの関連データを表示することもできます。

デフォルトでは、指定した時間範囲に基づいて適切なデータソースが自動的に選択されます。データソースをオーバーライドする場合は、次の手順を使用します。



重要 データソースを変更すると、選択した内容は、サインアウト後でも、変更するまでは、イベントデータソース（レポートを含む）に依存するすべての関連する分析機能で維持されます。選択した内容は他の Management Center ユーザーには適用されません。

選択したデータソースは、優先順位の低い接続イベントにのみ使用されます。他のすべてのイベントタイプ（侵入、ファイル、マルウェアイベント、それらのイベントに関連付けられた接続イベント、およびセキュリティインテリジェンスイベント）は、データソースに関係なく表示されます。

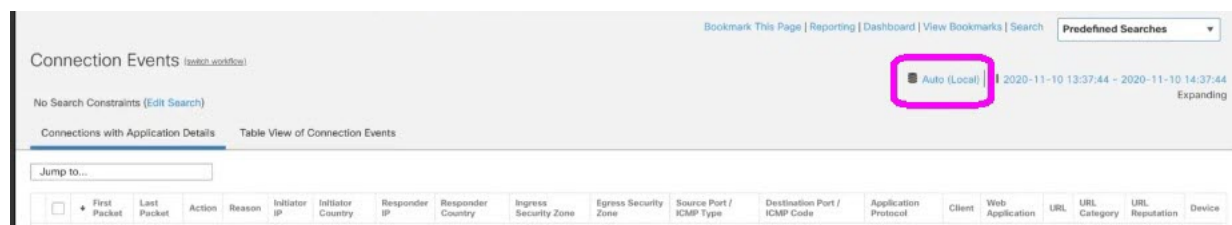
始める前に

ウィザードを使用して接続イベントをセキュリティ分析とロギング（オンプレミス）に送信しました。

手順

ステップ 1 Management Center Web インターフェイスで、接続イベントデータを表示するページ（[Analysis] > [Connections] > [Events] など）に移動します。

ステップ 2 ページに表示されるデータソースをクリックし、オプションを選択します。



注意 [Local] を選択すると、ローカルデータが選択した時間範囲全体で使用できない場合でも、Management Center で使用可能なデータのみ表示されます。この状況が発生していることは通知されません。

ステップ 3 （任意） Secure Network Analytics アプライアンスで関連データを直接表示するには、IP アドレスやドメインなどの値を右クリック（統合イベントビューアでクリック）し、相互起動オプションを選択します。

位置情報

地理位置情報データベース (GeoDB) を利用することで、国と大陸に基づいてトラフィックを表示およびフィルタ処理できます。国間を移動するモバイルデバイスやその他のホストが検出された場合、システムは特定の国ではなく大陸名を報告する可能性があります。

システムには IP アドレスを国/大陸にマップする初期 GeoDB カントリーコードパッケージが付属しているため、情報を常に利用できます。システムはコンテキストデータを含む IP パッケージもダウンロードします。たとえば次の設定が含まれます。

- 地域 (州、県、またはその他の国の小地域)、都市、郵便番号。
- 緯度/経度、タイムゾーン、クリック可能なマップ。
- 自律システム番号 (ASN) およびその ASN に関する追加情報。
- インターネット サービス プロバイダー (ISP)、接続の種類、プロキシの種類。
- 自宅/会社、組織、ドメイン名の情報。

この情報を表示するには、イベント、アセットプロファイル、コンテキストエクスプローラ、ダッシュボード、およびその他の分析ツールなどに表示される小さな国旗アイコンと ISO 国コードをクリックします。[接続のサマリ (Connection Summary)] ダッシュボードなど、集約的な地理位置情報から詳細の地理位置情報を表示することはできません。

シスコでは、GeoDB の定期的な更新を提供しています。正確な地理位置情報を取得するには、GeoDB を定期的に更新する必要があります。[地理位置情報データベース \(GeoDB\) の更新](#) を参照してください。

関連トピック

- [ネットワーク条件](#)
- [位置情報](#)
- [相関ポリシーとルールの概要](#)
- [トラフィック プロファイル条件](#)
- [地理位置情報データベース \(GeoDB\) の更新](#)

接続イベント グラフ

システムは、テーブル形式のドリルダウンページを使ったワークフローや最終的なイベントのテーブル表示に加えて、5 分間隔で集計されたデータを使用して、特定の接続データをグラフィック表示することができます。グラフ表示できるのは、データを集約するのに使用する情報 (送信元と宛先の IP アドレス (およびこれらのホストに関連するユーザ)、宛先ポート、トランスポートプロトコルとアプリケーションプロトコル) のみです。



ヒント セキュリティ インテリジェンス イベントを関連する接続イベントとは別にグラフ表示することはできません。セキュリティ インテリジェンスのフィルタリング アクティビティの概要をグラフィック表示するには、ダッシュボードとコンテキスト エクスプローラを使用します。

接続グラフは3種類あります。

- 円グラフは、1つのデータセットのデータをカテゴリ分けして表示します。
- 棒グラフは、1つあるいは複数のデータセットのデータをカテゴリ分けして表示します。
- 折れ線グラフは、時間の経過に伴って1つあるいは複数のデータセットのデータをプロットします。標準ビューあるいは速度（変化のペース）ビューを使用します。



(注) システムは、トラフィックプロファイルを線グラフで表示します。他の接続グラフと同様に操作可能ですが、いくつか規制があります。トラフィックプロファイルを表示するには、管理者アクセス権が必須です。

ワークフローテーブルと同様に、ワークフローグラフもドリルダウンし、制約を加えることで分析的を絞ることができます。

棒グラフおよび折れ線グラフはどちらも複数のデータセットを表示できます。つまり、各X軸データポイントに対し、Y軸に複数の値を表示できます。たとえば、一意のインシエータとレスポンドの総数を表示することができます。円グラフでは、1つのデータセットのみ表示できます。

X軸またはY軸、もしくは両方を変更することによって、接続グラフにさまざまなデータやデータセットを表示できます。円グラフでは、X軸を変更すると独立変数が変わり、Y軸を変更すると従属変数が変わります。

関連トピック

[接続の概要（グラフ用集約データ）](#)

接続イベントグラフの使用方法

Management Center では、検索する情報に応じて、接続イベントグラフを表示したり操作したりできます。

接続グラフにアクセスしたときに表示されるページは、使用するワークフローによって異なります。接続イベントのテーブルビューで終了する、事前定義されたワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタムワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ1 [分析 (Analysis)] > [接続 (Connections)] > [イベント (Events)] を選択します。

(注) 接続イベントテーブルがグラフの代わりに表示される場合、または別のグラフを表示する場合は、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)** をクリックし、グラフが含まれる事前定義されたワークフローまたはカスタムワークフローを選択します。接続グラフを含むすべての事前定義された接続イベントワークフローは、接続のテーブル ビューで終了します。

ステップ 2 次の選択肢があります。

- [時間範囲 (Time Range)] : 時間範囲を調整する場合は (グラフがブランクの場合に役立ちます) 、 **時間枠の変更 (37 ページ)** を参照してください。
- [フィールド名 (Field Name)] : ユーザが図示可能なデータの詳細については、 **接続およびセキュリティ関連の接続イベントフィールド** を参照してください。
- [ホスト プロファイル (Host Profiles)] : IP アドレスのホスト プロファイルを表示するには、発信側または応答側による接続データが表示されているグラフで、棒グラフの棒または円グラフの扇形をクリックし、[ホスト プロファイルの表示 (View Host Profile)] を選択します。
- [ユーザ プロファイル (User Profile)] : ユーザ プロファイル情報を表示するには、発信側ユーザによる接続データが表示されているグラフで、棒グラフの棒または円グラフの扇形をクリックし、[ユーザ プロファイルの表示 (View User Profile)] を選択します。
- [その他の情報 (Other Information)] : 図示されたデータに関する詳細については、折れ線グラフの点、棒グラフの棒、または円グラフの扇形の上にカーソルを置きます。
- [固定 (Constrain)] : ワークフローを次のページに進めずに接続グラフを X 軸 (独立した変数) 基準で固定するには、折れ線グラフの点、棒グラフの棒、または円グラフの扇形をクリックし、[表示方法 (View by)] を選択します。オプションが表示されます。
- [データ選択 (Data Selection)] : グラフに表示されるデータを変更するには、[X 軸 (X-Axis)] または [Y 軸 (Y-Axis)] をクリックし、図示する新しいデータを選択します。X 軸を [時間 (Time)] に変更、または [時間 (Time)] から変更すると、グラフ タイプも変更されます。Y 軸を変更すると、表示されるデータセットに影響します。
- [データセット (Datasets)] : グラフのデータセットを変更するには、[データセット (Datasets)] をクリックし、新しいデータセットを選択します。
- [切り離し (Detach)] : デフォルトの時間範囲に影響を与えることなくさらに分析を実行できるように接続グラフを分離するには、[切り離し (Detach)] をクリックします。
ヒント コピーを作成するには、分離したグラフで [新規ウィンドウ] をクリックします。分離した各グラフ上で、別々の分析ができるようになります。トラフィック プロファイルは、分離したグラフです。
- [詳細 (Drill-Down)] : ワークフローで次のページにドリルダウンするには、折れ線グラフの点、棒グラフの線、または円グラフの扇形をクリックし、[詳細 (Drill-Down)] を選択します。折れ線グラフで点をクリックすると、次のページの時間枠は、クリックした点を中心とする 10 分間に変更されます。棒グラフの棒または円グラフの扇形をクリックすると、その棒または扇形が表す基準に基づいて次のページが制約されます。

- [エクスポート (Export)] : グラフの接続データを CSV (カンマ区切り値) ファイルとしてエクスポートするには、[データのエクスポート (Export Data)] を選択します。次に、[CSV ファイルのダウンロード (Download CSV File)] をクリックし、ファイルを保存します。
- [グラフ タイプ (Graph Type)] : [折れ線 (Line)] - 標準と速度 (変化のペース) の折れ線グラフを切り替えるには、[速度 (Velocity)] をクリックし、[標準 (Standard)] または [速度 (Velocity)] を選択します。
- [グラフ タイプ (Graph Type)] : [棒と円 (Bar and Pie)] - 棒グラフと円グラフを切り替えるには、[棒グラフに切り替え (Switch to Bar)] または [円グラフに切り替え (Switch to Pie)] をクリックします。円グラフには複数のデータセットを表示できないため、複数のデータセットを持つ棒グラフから円グラフに切り替えた場合、円グラフは自動的に選択された 1 つのデータセットだけを表示します。表示するデータセットを選択する際、**Management Center** は、発信側と応答側の統計情報よりも全体の統計情報を優先し、応答側の統計情報よりも発信側の統計情報を優先します。
- [ページ間の移動 (Navigate Between Pages)] : 現在のワークフローで現在の制約を保持したままページ間を移動するには、ワークフロー ページの左上にある該当するページリンクをクリックします。
- イベントビュー間で移動する : 関連するイベントを表示するためその他のイベントビューに移動するには、[ジャンプ (Jump to)] をクリックし、ドロップダウンリストからイベントビューを選択します。
- [再センタリング (Recenter)] : 時間範囲の長さを変更せずにある時点を中心に折れ線グラフを再センタリングするには、その点をクリックし、[再センタリング (Recenter)] を選択します。
- [ズーム (Zoom)] : ズームインまたはズームアウトしながらある時点を中心に折れ線グラフを再センタリングするには、その点をクリックし、[ズーム (Zoom)] を選択してから新しい時間枠を選択します。

(注) 分離したグラフを使用している場合を除いて、制約、再センタリング、およびズームすると **Management Center** のデフォルトの時間範囲が変わります。

例

例 : 接続グラフの制約

ある期間の接続のグラフについて考えてみましょう。グラフ上の点をポートによって制約すると、検出された接続イベント数に基づいて、最もアクティブだった 10 のポートを示す棒グラフが表示されますが、クリックした点を中心とする 10 分間の時間枠によって制約されます。

棒の1つをクリックし、[発信側 IP による表示 (View by Initiator IP)] を選択してグラフをさらに制約すると、それまでと同じ10分間の時間枠だけでなく、クリックした棒が表すポートでも制約された新しい棒グラフが表示されます。

例：円グラフの X 軸と Y 軸の変更

ポートごとのキロバイト数を表示する円グラフについて考えてみましょう。この場合、X 軸は **レスポнда ポート**、Y 軸は **キロバイト** です。この円グラフは、ある間隔に監視対象ネットワークで送信されたデータの合計キロバイト数を表します。円の中の扇形は、各ポートで検出されたデータの比率を表します。

- グラフの X 軸を **アプリケーション プロトコル** に変更すると、引き続き円グラフは送信データの合計キロバイト数を表しますが、円の中の扇形は検出された各アプリケーションプロトコルの送信データの比率を表します。
- グラフの Y 軸を **パケット** に変更すると、円グラフはある間隔に監視対象ネットワークで送信された合計パケット数を表し、円の中の扇形は各ポートで検出された合計パケット数の割合を表します。

関連トピック

[ワークフローの使用](#) (13 ページ)

[イベント ビューの設定](#)

接続グラフ データ オプション

X 軸または Y 軸、もしくは両方を変更することによって、接続グラフにさまざまなデータを表示できます。円グラフでは、X 軸を変更すると独立変数が変わり、Y 軸を変更すると従属変数が変わります。

表 26: X 軸オプション

X 軸オプション	グラフの種類	次の基準でこのデータをグラフ化する
アプリケーションプロトコル (Application Protocol)	棒グラフまたは円グラフ	最もアクティブな 10 個のアプリケーションプロトコルに基づいて
Device	棒グラフまたは円グラフ	最もアクティブな 10 台の管理対象デバイスに基づいて
イニシエータ IP (Initiator IP)	棒グラフまたは円グラフ	最もアクティブな 10 個のイニシエータ ホスト IP アドレスに基づいて

X 軸オプション	グラフの種類	次の基準でこのデータをグラフ化する
イニシエータユーザ (Initiator User)	棒グラフまたは円グラフ	最もアクティブな 10 名のイニシエータ ユーザに基づいて
レスポнда IP (Responder IP)	棒グラフまたは円グラフ	最もアクティブな 10 個のレスポнда ホスト IP アドレスに基づいて
レスポнда ポート (Responder Port)	棒グラフまたは円グラフ	最もアクティブな 10 個のレスポнда ポートに基づいて
送信元デバイス (Source Device)	棒グラフまたは円グラフ	最もアクティブな 10 個の NetFlow データ エクスポートと、Firepower システムの管理対象デバイスによって検出されたすべての接続の Firepower という名前の送信元デバイスに基づいて。
時刻 (Time)	ライン	時系列 Y 軸と [時刻 (Time)] を切り替えることでグラフの種類も変わり、データセットを変更できます。

表 27: Y 軸オプション

Y 軸オプション	X 軸の基準を使用してこのデータをグラフ化する
バイト (Bytes)	送信バイト数
接続 (Connections)	接続数
KB (KBytes)	送信キロバイト数
KB/秒 (KBytes Per Second)	KB/秒
パケット (Packets)	送信パケット数
固有のホスト (Unique Hosts)	検出された固有のホスト数
固有のアプリケーション プロトコル (Unique Application Protocols)	固有のアプリケーション プロトコル数
固有ユーザ (Unique Users)	固有ユーザー数

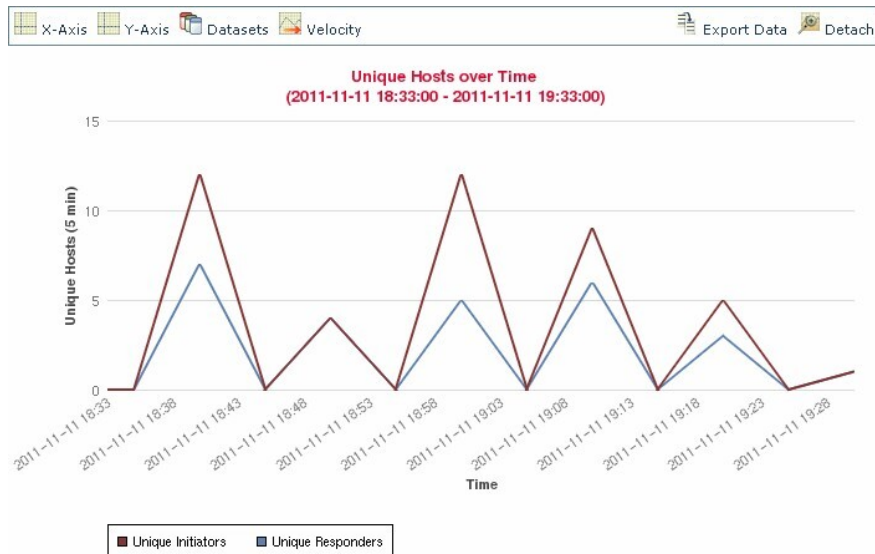
複数のデータセットの接続グラフ

棒グラフおよび折れ線グラフはどちらも複数のデータセットを表示できます。つまり、各 X 軸データポイントに対し、Y 軸に複数の値を表示できます。たとえば、一意のイニシエータとレスポンドの総数を表示することができます。

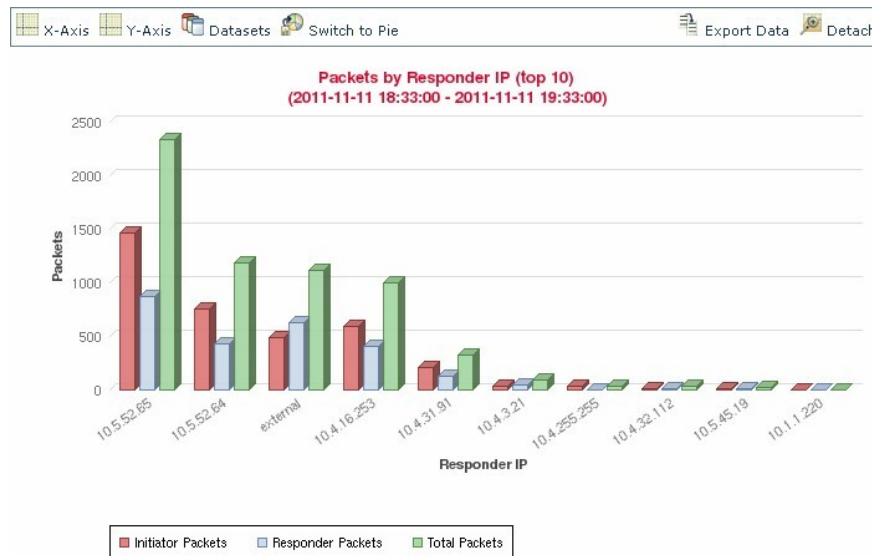


(注) 円グラフには複数のデータセットを表示できません。複数のデータセットを持つ棒グラフから円グラフに切り替えた場合、円グラフは自動的に選択された1つのデータセットだけを表示します。表示するデータセットを選択する際、Management Center は、イニシエータとレスポンドの統計情報よりも全体の統計情報を優先し、イニシエータの統計情報よりもレスポンドの統計情報を優先します。

折れ線グラフでは、複数のデータセットは複数の線として、それぞれ異なる色で表示されます。たとえば、次のグラフは、モニター対象ネットワークにおいて1時間間隔の1回で検出された一意のイニシエータの合計数と一意のレスポンドの合計数を表示しています。



棒グラフでは、複数のデータセットが X 軸データポイントごとに色分けされた棒として表示されます。たとえば次の棒グラフは、監視対象ネットワーク上で送信されたパケットの合計数と、イニシエータによって送信されたパケット数、レスポンドによって送信されたパケット数を表示しています。



371988

接続グラフ データセットオプション

次の表では、接続グラフの x 軸に表示できるデータセットについて説明します。

表 28: データセットオプション

y 軸が表示されている場合は、	データベースとして選択できます。
接続 (Connections)	デフォルトのみです。監視対象のネットワークで検出された接続数 ([接続 (Connections)]) です。これは、トラフィック プロファイル グラフ用の唯一のオプションです。
KB (KBytes)	以下を組み合わせています。 <ul style="list-style-type: none"> • モニター対象ネットワーク上で送信された合計キロバイト数 ([合計キロバイト数 (Total KBytes)]) • モニター対象ネットワーク上でホスト IP アドレスから送信されたキロバイト数 ([イニシエータ キロバイト数 (Initiator KBytes)]) • モニター対象ネットワーク上でホスト IP アドレスによって受信されたキロバイト数 ([レスポнда キロバイト数 (Responder KBytes)])
KB/秒 (KBytes Per Second)	デフォルトの、モニター対象ネットワークで 1 秒あたりに送信された合計キロバイト数のみ ([1 秒あたりの合計キロバイト数 (Total KBytes Per Second)])

y 軸が表示されている場合は、	データベースとして選択できます。
パケット (Packets)	以下を組み合わせています。 <ul style="list-style-type: none"> • モニター対象ネットワーク上で送信された合計パケット数 ([合計パケット (Total Packets)]) • モニター対象ネットワーク上でホスト IP アドレスから送信されたパケット数 ([イニシエータ パケット (Initiator Packets)]) • モニター対象ネットワーク上でホスト IP アドレスによって受信されたパケット数 ([レスポнда パケット (Responder Packets)])
固有のホスト (Unique Hosts)	以下を組み合わせています。 <ul style="list-style-type: none"> • モニター対象ネットワーク上の一意のセッション開始側の数 ([一意のイニシエータ (Unique Initiators)]) • モニター対象ネットワーク上の一意のセッション応答側の数 ([一意のレスポнда (Unique Responders)])
固有のアプリケーションプロトコル (Unique Application Protocols)	デフォルトの、モニター対象ネットワーク上の一意のアプリケーションプロトコル数のみ ([一意のアプリケーションプロトコル (Unique Application Protocols)])
固有ユーザー (Unique Users)	デフォルトのみです。監視対象のネットワークでのセッションイニシエータにログインした固有ユーザー数 ([固有イニシエータ ユーザー (Unique Initiator Users)]) です。

イベント時間の制約

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（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、ページの上部に時間範囲を表す行が含まれています。

デフォルトでは、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。

イベントビューの設定で独自のデフォルト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）

ページの上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、時間枠を一時停止すると同時にスライディングまたは拡張ワークフローを検証します。データセットを一時的に凍結するための時間枠の一時停止 (37 ページ) を参照してください。

関連トピック

[イベント ビューの設定](#)

[接続およびセキュリティ関連の接続イベントテーブルの使用](#)

イベントのセッションごとの時間枠のカスタマイズ

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、現在のセッションについてのみ有効です。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の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を与えませんが、他の種類のイベントの時間枠を変更すると、時間で制約でき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、ユーザー、または allow 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。

[日付/時刻 (Date/Time)] ウィンドウの [時間枠 (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。

- [イベントの時間枠 (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の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 (sliding)] 時間枠には、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が表示されます。ページを更新すると、時間枠が「スライド」するため設定した時間範囲 (この例では過去1週間) のイベントのみが表示されます。データセットを調べている間に一時的に更新されないようにするには、[データセットを一時的に凍結するための時間枠の一時停止 \(37 ページ\)](#) を参照してください。

選択したタイプによって、[日付/時刻 (Date/Time)] ウィンドウが変化し、さまざまな設定オプションが提供されます。



(注) システムでは、タイムゾーンの設定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。

時間枠の設定

次の表で、[時間枠 (Time Window)] タブで設定できるさまざまな項目について説明します。

表 29: 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 (time window type)] ドロップダウンリスト	適用対象外	<p>使用する時間枠のタイプとして、[静的 (static)]、[拡張 (expanding)]、または [スライディング (sliding)] のいずれかを選択します。</p> <p>イベント ビューを時間で制約している場合は、(グローバルであるかイベントに特有であるかに関係なく) 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。</p>

設定	時間枠（タイムウィンドウ）のタイプ	説明
[開始時間（Start Time）] カレンダー	静的および拡張	<p>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。</p> <p>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。</p>
[終了時間（End Time）] カレンダー	静的	<p>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。</p> <p>拡張時間枠を使用している場合は、[終了時刻（End Time）] カレンダーがグレー表示になり、終了時刻が「現在の時刻（Now）」と示されることに注意してください。</p> <p>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することもできます。</p>
[最後を表示（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	<p>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。</p> <p>次の点に注意してください。</p> <ul style="list-style-type: none"> • 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

設定	時間枠（タイムウィンドウ）のタイプ	説明
[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 <ul style="list-style-type: none"> • [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 • [監査ログの時間枠 (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

時間枠の変更

手順

ステップ 1 時間により制約されたワークフローで、[時間範囲 (Time Range)] () をクリックし、[日付と時間 (Date/Time)] ウィンドウを開きます。

ステップ 2 [イベントの時間枠 (Events Time Window)] で、[時間枠の設定 \(35 ページ\)](#) 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。

ステップ 3 [Apply] をクリックします。

データ セットを一時的に凍結するための時間枠の一時停止

スライディングまたは拡張時間枠を使用している場合、時間枠を一時停止してワークフローが提供する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。

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、時間枠が自動的に一時停止されます。準備ができたなら時間枠の一時停止を解除できます。

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。

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イベント時間枠の一時停止に影響しません。

手順

時間で制約されているワークフローでは、目的の時間範囲コントロールを選択できます。

- 時間枠を一時停止するには、時間範囲コントロールの[一時停止 (Pause)] (⏸) をクリックします。
- 時間枠の一時停止を解除するには、時間範囲コントロールの[再生 (Play)] (▶) をクリックします。

イベントのデフォルト時間枠

イベントの分析中に、[日付/時間 (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。

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ている場合に[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。

関連トピック

[デフォルト時間枠](#)

イベントタイプのデフォルトの時間枠オプション

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 30: 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。 <ul style="list-style-type: none"> • 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、[単一 (Single)] を選択します。

設定	説明
デフォルト時間枠：[最後を表示 - スライディング (Show the Last - Sliding)]	<p>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。</p> <p>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。</p>
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)	<p>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。</p> <p>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、最初にユーザー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。</p> <p>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。</p>
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)	<p>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。</p> <p>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、最初にユーザー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。</p> <p>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。</p>

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)	<p>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せん。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。</p> <p>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、最初にユーザー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。</p> <p>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。</p>

イベントタイプのデフォルトの時間枠の変更

手順

-
- ステップ 1** 時間により制約されたワークフローで、[時間範囲 (Time Range)] () をクリックし、[日付と時間 (Date/Time)] ウィンドウを開きます。
- ステップ 2** [優先 (Preferences)] をクリックし、[イベントタイプのデフォルトの時間枠オプション \(38 ページ\)](#) に記載されているようにプリファレンスを変更します。
- ステップ 3** [設定の保存 (Save Preferences)] をクリックします。
- ステップ 4** 次の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 [日付と時間 (Date/Time)] ウィンドウを閉じます。
-

イベント ビューの制約

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

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せん。

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、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、[宛先ポート/ICMP コード (Destination Port/ICMP Code)] カラムで [80 (http) /tcp (80 (http)/tcp)] をクリックします。



- ヒント モニター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。

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。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。

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。Management 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。

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ー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、結果を接続サマリー イベント ビューで表示すると、Management 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。

イベントの制約

手順

- ステップ 1** [ワークフローの選択 \(15 ページ\)](#) の説明に従って適切なメニュー パスとオプションを選択し、ワークフローにアクセスします。
- ステップ 2** すべてのワークフローで、次のオプションを選択できます。

- ビューを単一の値と一致するイベントに制約するには、ページの行内の目的の値をクリックします。
- ビューを複数の値と一致するイベントに制約するには、そ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。
(注) 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ます。
- 制約を解除するには、[制約の検索 (Search Constraints)] [展開矢印 (Expand Arrow)] (▶) をクリックし、展開された [制約の検索 (Search Constraints)] リスト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には、[検索の編集 (Edit Search)] をクリックします。
- 保存済み検索として制約を保存するには、[検索の保存 (Save Search)] をクリックし、クエリに名前を付けます。
(注) 複合的な制約が含まれているクエリは保存できません。
- 別のイベントビューで同じ制約を使用するには、[移動先 (Jump to)] をクリックし、イベントビューを選択します。
(注) 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ません。
- 制約の表示を切り替えるには、[制約の検索 (Search Constraints)] の [展開矢印 (Expand Arrow)] (▶) または [折りたたみ矢印 (Collapse Arrow)] (▼) 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。

複合イベントビューの制約

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。

複合イベントビュー制約の使用

手順

-
- ステップ 1** [ワークフローの選択 \(15 ページ\)](#) の説明に従って、適切なメニューパスとオプションを選択してワークフローにアクセスします。
- ステップ 2** 複合制約を管理する場合、次の選択肢があります。
- 複合制約を作成するには、カウント以外の値を持つ 1 つ以上の行を選択し、[表示 (View)] をクリックします。
 - 複合制約をクリアするには、[検索制約 (Search Constraints)] [展開矢印 (Expand Arrow)] (▶) をクリックし、[複合制約 (Compound Constraints)] をクリックします。
-

ワークフロー間のナビゲーション

ワークフローページの [移動 (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移動できます。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。

時間枠を一時停止していない場合、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。

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、[関連イベント (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、制約にインシエータの 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ー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 [移動先 (Jump to)] ドロップダウンリストから [関連イベント (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 (Jump to)] ドロップダウンリストから [ホスト (Hosts)] を選択します。

統合イベントビューアでの作業

統合イベントは、複数タイプのファイアウォールイベント (接続、侵入、ファイル、マルウェア、および一部のセキュリティ関連の接続イベント) の単一画面ビューを提供します。[統合イベント (Unified Events)] テーブルは、高度なカスタマイズが可能です。カスタムフィルタを作成して適用することにより、イベントビューアに表示される情報を微調整できます。統合

イベントテーブルの [ライブビュー (Live View)] オプションを使用すると、ファイアウォールイベントをリアルタイムで表示し、ネットワーク上のアクティビティをモニターすることができます。

統合イベントビューアを使用すると、次のことができます。

- 異なるタイプのイベント間の関係を調べる
- ポリシー変更の影響をリアルタイムで確認する

手順

ステップ 1 [分析 (Analysis)] > [統合イベント (Unified Events)] を選択します。

ステップ 2 時間範囲 (固定またはスライド) を選択して、特定の期間のファイアウォールイベントを表示します。デフォルトでは、統合イベントビューアテーブルには、過去1時間のイベントが表示されます。テーブルをフィルタ処理してセキュリティイベントのより詳細なコンテキストを取得したり、テーブルの列をカスタマイズしたり、ライブビューを有効にしてイベントの更新をリアルタイムで確認したりすることができます。

統合イベントの詳細については、「[統合イベント](#)」を参照してください。

ブックマーク

イベントの分析の特定の場所と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、次の情報が含まれます。

- 使用中のワークフロー
- ワークフローの表示中の部分
- 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発見した場合、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ー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（ユーザーによって直接、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あった元のイベントは表示されなくなります。

ブックマークの作成

マルチドメイン導入では、現在のドメインで作成されたブックマークのみを表示できます。

手順

- ステップ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。
- ステップ2 [名前 (Name)]フィールドに、名前を入力します。
- ステップ3 [ブックマークの保存 (Save Bookmark)]をクリックします。

ブックマークの表示

マルチドメイン導入では、現在のドメインで作成されたブックマークのみを表示できます。

手順

すべてのイベント ビューで、以下の2つの方法を選択できます。

- [ブックマークの表示 (View Bookmarks)]の上にポインタを合わせ、ドロップダウンメニューから目的のブックマークをクリックします。
- [ブックマークの表示 (View Bookmarks)]をクリックし、[ブックマークの表示 (View Bookmarks)]ページで目的のブックマーク名をクリックするか、その横にある [表示 (View)] (👁) をクリックします。

(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。

ワークフローの履歴

表 31:

機能	最小 Management Center	最小 Threat Defense	詳細
廃止：侵入インシデントとイベントクリップボード。	7.1	任意 (Any)	<p>侵入インシデントとイベントクリップボードは廃止されています。</p> <p>廃止された画面：</p> <ul style="list-style-type: none"> • [分析 (Analysis)] > [侵入 (Intrusions)] > [クリップボード (Clipboard)] • [分析 (Analysis)] > [侵入 (Intrusions)] > [インシデント (Incidents)]
統合イベントビューア。	7.0	任意 (Any)	<p>接続 (セキュリティインテリジェンスを含む)、侵入、ファイル、マルウェアの複数のイベントタイプを1つのテーブルで表示および操作します。</p> <p>新規/変更された画面： [分析 (Analysis)] > [統合イベント (Unified Events)]</p>
リモートに保存されたイベントの操作。	7.0	任意 (Any)	<p>FMCを使用して Secure Network Analytics アプライアンスに保存されている接続イベントを操作できます。システムに自動的に最適なデータソースを使用させるか、またはソースを明示的に選択できます。このオプションは、セキュリティ分析とロギング (オンプレミス) ウィザードを完了した場合にのみ表示されます。</p> <p>新規/変更された画面： イベントビューア、ダッシュボード、コンテキストエクスプローラ、レポートなど、接続イベントを表示するページ。</p>
特定のケースでのワークフローテーブルの読み込み速度の改善。	6.6	任意 (Any)	<p>ワークフローページのテーブルには、表示される列が6つ以下の場合にのみ、同一の行の Count 列が表示されるようになりました。これにより、必要な計算量が最小限に抑えられるため、テーブルの読み込み速度が向上します。</p> <p>新規/変更された画面： イベントビューア。</p>

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。