



レポートの操作

FireSIGHT システムは柔軟なレポート作成システムを提供しており、Defense Center で表示されるイベント ビューやダッシュボードを使用して、複数のセクションがあるレポートを短時間で簡単に生成できます。独自のカスタム レポートを最初から設計することもできます。レポート作成は、Defense Center でのみ使用可能です。

レポートは、通信しようとしている内容が含まれるドキュメント ファイルで、PDF、HTML、または CSV 形式になります。レポート テンプレートは、データの検索設定とレポートおよびそのセクションの形式を指定します。FireSIGHT システム には強力なレポート デザインが含まれていて、レポート テンプレートの設計を自動的に行います。Web インターフェイスに表示されるイベント ビュー テーブルやダッシュボードのグラフィックの内容を複製できます。

レポート テンプレートは必要な数だけ作成できます。各レポート テンプレートは、レポートの個々のセクションを定義し、レポートの内容を作成するデータベース検索設定を指定し、表示形式(表、グラフ、詳細表示など)とタイム フレームも指定します。さらに、テンプレートでは、表紙や目次の情報、ドキュメント ページに見出しとフッターを付けるかどうかなどのドキュメント 属性も指定します(PDF 形式のレポートでのみ指定可能)。レポート テンプレートを 1 つの設定 パッケージ ファイルとしてエクスポートし、別の Defense Center にインポートして再使用できます。

テンプレートに入力パラメータを組み込んで実用性を向上させることができます。入力パラメータを使用すると、同じレポートを用途に合わせて異なるさまざまなレポートに変えることができます。入力パラメータのあるレポートを生成するときには、生成プロセスで各入力パラメータの値を入力するよう求められます。ユーザが入力する値は、レポートの内容をその 1 回だけ制約します。たとえば、侵入イベントのレポートを作成する検索の宛先 IP フィールドに入力パラメータを使用できます。この場合、レポートの生成時に、宛先 IP アドレスの入力を求められたときに特定の部門のネットワーク セグメントを指定できます。その結果、この特定の部門に関する情報だけが含まれるレポートが生成されます。

レポートやレポート テンプレートの詳細については、次の項を参照してください。

- [レポート テンプレートについて\(57-2 ページ\)](#)
- [レポート テンプレートの作成と編集\(57-4 ページ\)](#)
- [レポートの生成と表示\(57-29 ページ\)](#)
- [レポート生成オプションの使用法\(57-32 ページ\)](#)
- [レポート テンプレートとレポート ファイルの管理\(57-34 ページ\)](#)

レポートテンプレートについて

ライセンス:任意(Any)

FireSIGHT システムのレポート作成機能によって、Defense Center からイベント ビュー、ダッシュボード、またはワークフローの内容をすばやくキャプチャして、レポート形式で表示できます。レポートテンプレートを使用して、レポートの各セクション内のデータの内容と形式や、レポートファイルのドキュメント属性(表紙、目次、ページ見出し、ページフッター)を定義します。レポートの生成後、削除しない限りテンプレートは再利用可能な状態になります。

レポートには、1つ以上の情報セクションが含まれます。個々のセクションごとに形式(テキスト、表、またはグラフ)を選択します。セクションの形式の選択内容によっては、組み込めるデータが制約される場合があります。たとえば、円グラフの形式を使用すると、特定の表に時間ベースの情報を表示できません。いつでもセクションのデータの基準や形式を変更して、表示を最適にすることができます。

定義済みイベント ビューのレポートの初期設計をベースにするか、定義済みのダッシュボード、ワークフロー、または要約から内容をインポートして設計を開始できます。空のテンプレートシェルから始めて、1つずつセクションを追加したり属性を定義したりすることもできます。

レポートテンプレートのすべてのセクションには、タイトルバーと、セクションの内容や外観を制御する各種の属性フィールドがあります。詳細については、次のトピックを参照してください。

- [レポートセクションのタイトルバーの要素表](#)
- [レポートセクションのフィールド表](#)

次の表に、テンプレートセクションごとのタイトルバー上のコントロールについて説明します。

表 57-1 レポートセクションのタイトルバーの要素

| 属性 | 定義 |
|----------------|---|
| セクションタイトル | レポートに表示されるセクションの名前が含まれます。名前を変更するには、この名前をクリックして新しい名前を入力します。表示の問題を回避するため、長いセクションタイトル名は[レポートセクション(Report Sections)] ページで表示するときに切り詰められます。 |
| セクションタイトルのアイコン | レポートテンプレートにセクションの複製を追加するには、複製アイコン(+)をクリックします。 セクションを最小化するには、最小化アイコン(-)をクリックします。 セクションを削除するには、削除アイコン(×)をクリックして、その後確定します。 |

次の表は、レポートテンプレートの各セクション内のフィールドを定義します。

表 57-2 レポートセクションのフィールド

| フィールド名 | 定義 |
|---------------|---|
| テーブル(Table) | セクションデータの取り出し元のテーブルを選択できるドロップダウンメニューを表示します。 |
| プリセット(Preset) | 定義済み検索設定のドロップダウンメニューを表示します。新しい検索設定を定義する際に、該当する事前設定を選択して、検索条件を初期化できます。 |

表 57-2 レポート セクションのフィールド(続き)







| フィールド名 | 定義 |
|--|---|
| フォーマット (Format) | <p>セクション データの形式を選択できるアイコンを表示します。次のオプションがあります。</p> <p> 棒グラフ: 選択した変数の数量を比較します。</p> <p> 折れ線グラフ: 選択した変数の、時間の経過に伴う傾向/変化を示します。時間ベースのテーブルにのみ使用できます。</p> <p> 円グラフ: 選択した各変数を全体の割合として示します。数量がゼロの変数はグラフからドロップされます。ごくわずかな数量は、[その他 (Other)] というラベルのカテゴリに集められます。</p> <p> 表形式の表示: レコードごとの属性の値を示します。要約や統計のデータには使用できません。</p> <p> 詳細表示: パケット (侵入イベントの場合) やホスト プロファイル (ホスト イベントの場合) など、特定のイベントに関連付けられた複合オブジェクトのデータを示します。フォーマットは、この種のオブジェクトが関係する特定のイベント タイプだけに使用できます。出力が多数要求されている場合には、パフォーマンスが低下することがあります。</p> |
| 検索または フィルタ (Search or Filter) | <p>検索設定またはアプリケーション フィルタのドロップダウンメニューを表示します。</p> <p>ほとんどのテーブルの場合、定義済みまたは保存済みの 検索設定 を使用してレポートを制約できます。編集アイコン () をクリックして、新しい検索設定を作成することもできます。レポート テンプレート セクションの検索設定の操作 (57-19 ページ) を参照してください。</p> <p>Application Statistics テーブルの場合、ユーザ定義のアプリケーション フィルタを使用してレポートを制約できます。フィルタの作成については、アプリケーション フィルタの操作 (3-16 ページ) を参照してください。</p> |
| X 軸 (X-Axis) | <p>選択したグラフの X 軸に関する使用可能なデータ列のドロップダウンメニューを表示します。グラフの形式を選択する場合にのみ表示されます。折れ線グラフの場合、X 軸の値は常に 時刻 です。棒グラフと円グラフの場合、X 軸の値として 時刻 を選択できません。</p> |
| Y 軸 (Y-Axis) | <p>選択したグラフの Y 軸に関する使用可能なデータ カラムのドロップダウンメニューを表示します。</p> |
| セクションの 説明 (Section Description) | <p>セクション内で検索データの前にある説明テキストを定義します。テキストと入力パラメータの組み合わせを入力します。新しいセクションのデフォルトは、<code>\$(Time Window)</code> と <code>\$(Constraints)</code> の 2 つの入力パラメータのセットです。入力パラメータについて、詳しくは 入力パラメータの使用法 (57-20 ページ) を参照してください。</p> |
| 時間枠 (Time Window) | <p>セクションに表示されるデータの時間枠を定義します。セクションで時間ベースのテーブルが検索される場合、このチェック ボックスを選択して、レポートのグローバル時間枠を継承できます。または、セクションの特定の時間枠を設定することもできます。時間枠の設定については、レポート テンプレートのセクションの編集 (57-13 ページ) を参照してください。</p> |

表 57-2 レポート セクションのフィールド(続き)

| フィールド名 | 定義 |
|-------------|---|
| 結果(Results) | [トップ(Top)]か[ボトム(Bottom)]を選択し、セクションに含めるレコードの最大数を入力します。 |
| カラー(Color) | セクション内でグラフ化されるデータの色を定義します。必要に応じて、1つ以上の色を選択します。 |

レポート テンプレートの作成と編集

ライセンス:任意(Any)

次のいずれかの方法で新しいレポート テンプレートを構築できます。

- [新しいレポート テンプレートの作成\(57-4 ページ\)](#)
- [既存のテンプレートからのレポート テンプレートの作成\(57-7 ページ\)](#)
- [イベント ビューからのレポート テンプレートの作成\(57-10 ページ\)](#)
- [ダッシュボードまたはワークフローのインポートによるレポート テンプレートの作成\(57-12 ページ\)](#)

レポート テンプレートの変更とカスタマイズについては、次の項を参照してください。

- [レポート テンプレートのセクションの編集\(57-13 ページ\)](#)
- [レポート テンプレート セクションの検索設定の操作\(57-19 ページ\)](#)
- [入力パラメータの使用法\(57-20 ページ\)](#)
- [レポート テンプレート内のドキュメント属性の編集\(57-25 ページ\)](#)
- [表紙のカスタマイズ\(57-26 ページ\)](#)
- [ロゴの管理\(57-27 ページ\)](#)

新しいレポート テンプレートの作成

ライセンス:任意(Any)

既存のレポート テンプレートをコピーしない場合は、まったく新しいテンプレートを作成できます。最初に、デフォルトテンプレートのシェルを作成します。次に、ご希望の順序で、個々のテンプレート セクションを設計し、レポート ドキュメントの属性を設定します。これらの手順の詳細については、次の項を参照してください。

- [テンプレートのシェルの作成\(57-5 ページ\)](#)
- [テンプレート セクションの内容の設定\(57-6 ページ\)](#)
- [PDF および HTML レポート ドキュメントの属性の設定\(57-6 ページ\)](#)

テンプレートのシェルの作成

ライセンス:任意(Any)

レポートテンプレートは、独自のデータベース クエリから個別に構築されたセクションのフレームワークです。テンプレート作成の最初の手順として、セクションを追加したり形式設定したりできるフレームワーク シェルを生成します。

テンプレートのシェルを作成する方法:

アクセス:Admin/Any Security Analyst

-
- 手順 1 [概要(Overview)] > [レポート(Reporting)] を選択します。
 - 手順 2 [レポート テンプレート(Report Templates)] タブをクリックします。
[レポート テンプレート(Report Templates)] ページが表示されます。
 - 手順 3 [レポート テンプレートの作成(Create Report Template)] をクリックします。
[レポート セクション(Report Sections)] ページが表示され、デフォルトのテンプレート名 New Report が [レポート タイトル(Report Title)] フィールドに表示されます。
 - 手順 4 オプションで、[レポート タイトル(Report Title)] フィールドに新しいテンプレートの名前を入力し、[保存(Save)] をクリックします。レポート タイトルには英数字とスペースの組み合わせを使用できます。
新しいテンプレート名のエントリが [レポート テンプレート(Report Templates)] ページのリストに表示されます。
 - 手順 5 入力パラメータもレポート タイトルに使用できます。入力パラメータを追加するには、タイトル内で、パラメータの値を表示させるスポットにカーソルを置いてから、入力パラメータ挿入アイコン(+) をクリックします。
追加した入力パラメータが [レポート タイトル(Report Title)] フィールドに表示されます。入力パラメータの詳細については、[入力パラメータの使用法\(57-20 ページ\)](#) を参照してください。
 - 手順 6 必要に応じて、[レポート セクション(Report Sections)] タイトル バーの下にある追加アイコンのセットを使用し、セクション シェルを挿入します。セクションの形式設定の詳細については、[レポート セクションのフィールド表](#) を参照してください。
追加した各セクションは、テンプレートの下部に表示されます。セクションを正しい場所にドラッグします。
 - 手順 7 セクションのタイトル バーに表示されているセクションのタイトルをクリックし、セクションの名前を入力します(最大 120 文字を使用)。
 - 手順 8 [保存(Save)] をクリックして、テンプレートを保存します。
テンプレートが保存されます。
-

テンプレート セクションの内容の設定

ライセンス:任意(Any)

各テンプレート セクションは、検索設定やフィルタによって生成されたデータセットで構成され、表示モードを確定する形式の仕様(表や円グラフなど)があります。出力に含めるデータレコードのフィールドを選択し、タイム フレームと表示するレコード数も選択して、さらにセクションの内容を確定します。

レポートテンプレートセクションを設定する方法:

アクセス:Admin/Any Security Analyst

-
- 手順 1 [レポートテンプレートのセクションの編集\(57-13 ページ\)](#)で説明されているように、セクションの属性を編集します。
- 手順 2 オプションで、セクションのウィンドウの下部にある [プレビュー(Preview)] をクリックして、選択したカラムのレイアウトやグラフィックの形式を表示します。



(注) セクションプレビューユーティリティを使用して、カラムの選択内容や、円グラフの色などの出力の特性を検査します。このインジケータは、設定済みの検索設定を必ずしも正確に反映するとは限りません。

PDF および HTML レポート ドキュメントの属性の設定

ライセンス:任意(Any)

テンプレートから生成したレポートには、表紙、見出しとフッター、ページ番号など、すべてのセクションにまたがって機能を制御する複数のドキュメント属性があります。

レポートドキュメントの属性を設定する方法:

アクセス:Admin/Any Security Analyst

-
- 手順 1 [概要(Overview)] > [レポート(Reporting)] を選択します。
- 手順 2 [レポートテンプレート(Report Templates)] タブをクリックします。
[レポートテンプレート(Report Templates)] ページが表示されます。
- 手順 3 レポートの生成に使用するレポートテンプレートの [編集(Edit)] をクリックします。
このテンプレートの [レポートセクション(Report Sections)] ページが表示されます。
- 手順 4 [詳細設定(Advanced)] をクリックします。
[詳細設定(Advanced Settings)] ポップアップ ウィンドウが表示されます。
- 手順 5 PDF 形式か HTML 形式のドキュメントの場合は、[レポートテンプレート内のドキュメント属性の編集\(57-25 ページ\)](#)で説明されている作業を実行します。
CSV をドキュメントの形式として選択した場合は、ドキュメントの属性を設定できません。
-

既存のテンプレートからのレポートテンプレートの作成

ライセンス:任意(Any)

既存のテンプレートの中に適切なモデルがあれば、そのテンプレートをコピーして属性を編集することで、新しいレポートテンプレートを作成できます。また、シスコからは一連の定義済みレポートテンプレートが提供され、[レポート(Reports)] タブのテンプレートの一覧で確認できます。これらの属性の説明については、[定義済みレポートテンプレートの使用法\(57-7 ページ\)](#)を参照してください。

既存のテンプレートからレポートテンプレートを作成する方法:

アクセス:Admin/Any Security Analyst

-
- 手順 1 [概要(Overview)] > [レポート(Reporting)] を選択します。
 - 手順 2 [レポートテンプレート(Report Templates)] タブをクリックします。
[レポートテンプレート(Report Templates)] ページが表示されます。シスコが用意しているレポートテンプレートについては、[定義済みレポートテンプレートの使用法\(57-7 ページ\)](#)を参照してください。
 - 手順 3 モデルとしてコピーするレポートテンプレートの横のコピーアイコン()をクリックします。
コピーしたテンプレートが、新しいレポートテンプレートとして表示されます。
 - 手順 4 [レポートタイトル(Report Title)] フィールドに、新しいレポートテンプレートの名前を入力します。
 - 手順 5 [保存(Save)] をクリックします。
レポートテンプレートが保存され、新しいレポートテンプレートのエントリが [レポートテンプレート(Report Templates)] ページに表示されます。
 - 手順 6 必要に応じてテンプレートを変更します。
テンプレートのセクションやドキュメントの属性の定義の詳細については、以下を参照してください。
 - [レポートテンプレートのセクションの編集\(57-13 ページ\)](#)
 - [レポートテンプレート内のドキュメント属性の編集\(57-25 ページ\)](#)
-

定義済みレポートテンプレートの使用法

ライセンス:任意(Any)

次の定義済みレポートテンプレートは、現状のまま使用したり、編集を加えたり、独自のテンプレートのベースとして使用したりできます。

- [Host Report: \\$<Host>](#)
- [User Report: \\$<User>](#)
- [Attack Report: Attack \\$<Attack SID>](#)
- [Malware Report](#)
- [FireSIGHT Report: \\$<Customer Name>](#)
- [Files Report](#)

Host Report: \$<Host>

Host Report: \$<Host> レポートテンプレートは、ネットワーク上の特定のホストについての情報を提供します。このレポートテンプレートには、次のセクションがあります。

- サーバアプリケーション (Server Applications)
- クライアントアプリケーション
- このホストからの侵入イベント (Intrusion Events Originating from This Host)
- このホストへの侵入イベント (Intrusion Events Destined to This Host)
- このホストからの接続 (Connections Originating from This Host)
- このホストへの接続 (Connections Destined to This Host)
- このホストのユーザ (Users of This Host)
- このホストによるホワイトリスト違反 (White List Violations by This Host)

User Report: \$<User>

User Report: \$<User> レポートテンプレートは、ネットワーク上の特定のユーザに関する情報を提供します。このレポートテンプレートには、次のセクションがあります。

- このユーザによって使用されているクライアントアプリケーション (Client Applications Used by This User)
- このユーザによって使用されている Web アプリケーション (Web Applications Used by This User)
- このユーザによって使用されているアプリケーションプロトコル (Application Protocols Used by This User)
- このユーザによって使用されているアプリケーションの包括的リスト (Comprehensive List of Applications Used by This User)
- このユーザのマシンからの侵入イベント (Intrusion Events Originated By This User's Machines)
- このユーザのマシンへの侵入イベント (Intrusion Events Destined to This User's Machines)
- このユーザのマシンからの接続 (Connections Originating from This User's Machines)
- このユーザのマシンへの接続 (Connections Destined to This User's Machines)
- このユーザのホスト (Hosts for This User)

Attack Report: Attack \$<Attack SID>

Attack Report: Attack \$<Attack SID> レポートテンプレートは、ネットワーク上の特定の攻撃に関する情報を提供します。このレポートテンプレートには、次のセクションがあります。

- この攻撃に関する一般情報 (General Information About This Attack)
- 攻撃の数 (Number of Attacks)
- 攻撃を開始しているマシンの数 (Number of Machines Initiating Attack)
- 攻撃されているマシンの数 (Number of Machines Being Attacked)
- この攻撃の発生源 (Sources of This Attack)
- この攻撃の標的 (Destinations of This Attack)
- この攻撃のトラフィックパターン (Traffic Patterns of This Attack)

Malware Report

Malware Report レポート テンプレートは、ネットワークベースとエンドポイントベースのマルウェア イベントに関する情報を提供します。このレポート テンプレートには、次のセクションがあります。

- [マルウェア脅威 (Malware Threats)]
- 時間の経過に伴う脅威の検出 (Threat Detections over Time)
- マルウェアを転送しているアプリケーション プロトコル (Application Protocols Transferring Malware)
- マルウェアを受信するホスト (Hosts Receiving Malware)
- マルウェアを送信するホスト (Hosts Sending Malware)
- マルウェアの影響を受けるユーザ (Users Affected by Malware)
- マルウェア侵入 (Malware Intrusions)
- マルウェアに感染しているファイル タイプ (File Types Infected with Malware)
- マルウェアを取り込んだアプリケーション (Applications Introducing Malware)
- マルウェア イベントのテーブル ビュー (Table View of Malware Events)

シリーズ 2 デバイスと DC500 Defense Center のどちらもネットワークベースのマルウェア対策をサポートしておらず、検出されて表示されるデータに影響を与える可能性があることに注意してください。たとえば、シリーズ 2 デバイスだけを管理する Series 3 Defense Center は、エンドポイントベースのマルウェア イベントだけを表示できます。

FireSIGHT Report: \$<Customer Name>

FireSIGHT Report: \$<Customer Name> レポートテンプレートは、組織のネットワークに関する全体的な情報を提供します。このレポート テンプレートには、次のセクションがあります。

- リスト別アプリケーション トラフィックの概要 (Summary of Application Traffic by Risk)
- ビジネス関連性が低い危険なアプリケーション (Risky Applications with Low Business Relevance)
- 低い危険なアプリケーションのユーザ (Users of Risky Applications)
- アノニマイザーとプロキシ (Anonymizers and Proxies)
- 典型的な高帯域幅アプリケーション (Typically High Bandwidth Applications)
- 合計帯域幅別アプリケーション (Applications by Total Bandwidth)
- センシティブなネットワークにアクセスするホスト (Hosts Accessing Sensitive Network)
- センシティブなネットワークにアクセスするユーザ (Users Accessing Sensitive Network)
- センシティブなネットワーク上のアプリケーション (Applications on Sensitive Network)
- センシティブなネットワークに関連しているポートとプロトコル (Ports and Protocols Related to Sensitive Network)
- 悪意のある URL にアクセスするホスト (Hosts Visiting Malicious URLs)
- 悪意のある URL にアクセスするユーザ (Users Visiting Malicious URLs)
- 詳細なアプリケーション使用状況 (Granular Application Usage)
- Web アプリケーション
- クライアント アプリケーション
- アプリケーション プロトコル (Application Protocols)

- Webブラウザ バージョン (Web Browser Versions)
- オペレーティング システム バージョン (Operating System Versions)
- 全体的なユーザ アクティビティ (Overall User Activity)
- インパクト別侵入イベント (Intrusion Events by Impact)
- インパクト別侵入イベント:ブロック後 (Intrusion Events by Impact (After Blocking))
- アプリケーション別侵入イベント (Intrusion Events by Application)
- ランキング上位の侵入イベント (Top Intrusion Events)
- 包括的アプリケーション リスト (Comprehensive Application List)

Files Report

Files Report レポート テンプレートは、管理対象デバイスによってネットワーク トラフィックで検出されたファイルに関する情報を提供します。このレポート テンプレートには、次のセクションがあります。

- 時間の経過に伴うファイル転送 (File Transfers over Time)
- ファイル転送で使用されるアプリケーション プロトコル (Application Protocols Used by File Transfers)
- ファイル性質 (File Dispositions)
- ファイル アクション (File Actions)
- ファイルを受信したホスト (Hosts Receiving Files)
- ファイルを送信したホスト (Hosts Sending Files)
- ファイルを転送するユーザ (Users Transferring Files)
- ファイル カテゴリ (File Categories)
- ファイルタイプ (File Types)
- ファイル名 (File Names)
- ファイル イベントのテーブル ビュー (Table View of File Events)

イベント ビューからのレポート テンプレートの作成

ライセンス:任意 (Any)

レポートを生成する前に、レポート作成システムにより作成されるレポート テンプレートに、必要に合わせて変更を加えることができます。セクションを追加したり、自動的に組み込まれるセクションを変更したり、セクションを削除したりできます。

イベント ビューからレポート テンプレートを作成する方法:

アクセス:Admin/Any Security Analyst

-
- 手順 1** レポートに含めるイベントをイベント ビューに入力します。さまざまな方法で入力できます。
- イベント検索設定を使用して、表示するイベントを定義します。イベント検索設定の使用法の詳細については、[イベントの検索 \(60-1 ページ\)](#)を参照してください。
 - イベント ビューに該当するイベントが表示されるまでワークフローをドリルダウンします。ワークフローと、ワークフロー内のイベントを制約する方法の詳細については、[ワークフローの概要と使用 \(58-1 ページ\)](#)を参照してください。

- 手順 2** イベント ビューのページから、[レポート作成者(Report Designer)] をクリックします。
[レポート セクション(Report Sections)] ページが表示され、キャプチャされるワークフロー内のビューごとにセクションが示されます。
- 手順 3** オプションで、[レポート タイトル(Report Title)] フィールドに新しい名前を入力し、[保存(Save)] をクリックします。
- 手順 4** オプションで、セクションのタイトル バーの削除アイコン(✕)をクリックし、削除を確認して、レポートから除外するテンプレート セクションを削除します。
削除されたセクションは非表示になります。





(注) 一部のワークフロー内の最後のレポート セクションには詳細ビューが含まれ、ワークフローに応じてパケット、ホスト プロファイル、または脆弱性が示されます。レポートの生成時に、これらの詳細ビューがあるイベントを多数取得すると、Defense Center のパフォーマンスに影響を与えることがあります。

- 手順 5** オプションで、レポート セクション内のフィールドの設定を調整します。
レポート セクション内のフィールドの設定の詳細については、[レポート テンプレートのセクションの編集\(57-13 ページ\)](#)を参照してください。



ヒント セクションの現在のカラムのレイアウトやグラフの形式を表示する場合は、そのセクションの[プレビュー(Preview)] リンクをクリックします。

- 手順 6** オプションで、タイトル バーでセクションのタイトルをクリックして、そのセクションのタイトルを変更します。
[セクション タイトルの設定(Set Section Title)] ポップアップ ウィンドウが表示されます。セクションのタイトルを入力し、[OK] をクリックします。
- 手順 7** オプションで、改ページを追加します。改ページ追加アイコン()をクリックします。
新しい改ページ オブジェクトがテンプレートの下部に表示されます。そのオブジェクトを、新しいページの先頭にするセクションの前にドラッグします。改ページの使用法の詳細については、[レポート テンプレートのセクションの編集\(57-13 ページ\)](#)を参照してください。
- 手順 8** オプションで、テキスト セクションを追加します。テキスト セクション追加アイコン()をクリックします。
新しいテキスト セクションがテンプレートの下部に表示されます。そのセクションを、レポート テンプレート内の表示位置にドラッグします。テキスト セクションの編集については、[レポート テンプレートのセクションの編集\(57-13 ページ\)](#)を参照してください。



ヒント テキスト セクションはリッチ テキスト(太字、斜体、可変フォント サイズなど)やインポート済みイメージをサポートしており、レポートやレポート セクションの概要として活用できます。

- 手順 9** オプションで、[詳細設定(Advanced Settings)] をクリックして、表紙、目次、開始ページ番号、または見出しとフッターのテキストを追加します。詳細については、[レポート テンプレート内のドキュメント属性の編集\(57-25 ページ\)](#)を参照してください。
- 手順 10** レポート テンプレートが適切な場合は、[保存(Save)] をクリックします。
レポート テンプレートが保存され、レポート テンプレートのエントリが [レポート テンプレート(Report Templates)] ページに表示されます。

ダッシュボードまたはワークフローのインポートによるレポートテンプレートの作成

ライセンス:任意(Any)

ダッシュボード、ワークフロー、統計の要約をインポートして、新しいレポートをすばやく作成できます。インポートすると、ダッシュボードのウィジェット グラフィックごと、およびワークフローのイベント ビューごとにセクションが作成されます。最も重要な情報に焦点が当たるように不要なセクションを削除できます。次の表で、インポート オプションについて説明します。

表 57-3 [レポート セクションのインポート (Import Report Sections)] ウィンドウのデータ ソース オプション

| 選択オプション | インポート対象 |
|---|--|
| ダッシュボードのインポート (Import Dashboard) | 選択したダッシュボード上のカスタム分析ウィジェット。 |
| ワークフローのインポート (Import Workflow) | 定義済みのワークフローまたはカスタム ワークフロー。 ヒント 選択項目の形式は次のようになっています。 Table - Workflow name たとえば、Connection Events - Traffic by Port は、Connection Events (接続イベント) テーブルから生成された Traffic by Port (ポート別トラフィック) ワークフロー内のビューをインポートします。 |
| 要約セクションのインポート (Import Summary Sections) | 次の一般的な要約: <ul style="list-style-type: none"> • 侵入の詳細要約 (Intrusion Detailed Summary) • 侵入の短い要約 (Intrusion Short Summary) • ディスカバリの詳細要約 (Discovery Detailed Summary) • ディスカバリの短い要約 (Discovery Short Summary) |

ダッシュボード、ワークフロー、または統計情報の要約からレポートテンプレートを作成する方法:

アクセス: Admin/Any Security Analyst

- 手順 1 レポート内で複製するダッシュボード、ワークフロー、または要約を識別します。
- 手順 2 [概要 (Overview)] > [レポート (Reporting)] を選択します。
- 手順 3 [レポート テンプレート (Report Templates)] タブをクリックします。
[レポート テンプレート (Report Templates)] ページが表示されます。
- 手順 4 [レポート テンプレートの作成 (Create Report Template)] をクリックします。
[レポート セクション (Report Sections)] ページが表示されます。
- 手順 5 [レポート タイトル (Report Title)] フィールドに新しいレポート テンプレートの名前を入力します。
- 手順 6 新しい名前でもレポート テンプレートを保存する場合は、[保存 (Save)] をクリックします。
レポート テンプレートが保存され、レポート テンプレートのエントリが [レポート テンプレート (Report Templates)] ページに表示されます。

- 手順 7** ダッシュボード、要約、ワークフローのアイコン(🌐)からインポート セクションをクリックします。
- [レポート セクションのインポート (Import Report Sections)] ポップアップ ウィンドウが表示されます。[レポート セクションのインポート (Import Report Sections)] ウィンドウのデータ ソース オプション表で説明されているデータ ソースのいずれかを選択できます。
- 手順 8** ドロップダウンメニューからダッシュボード、ワークフロー、または要約を選択します。
- 手順 9** 追加しようとしているデータ ソースの、[インポート (Import)] をクリックします。
- テンプレートの [レポート セクション (Report Sections)] ページが再び表示され、選択したデータ ソースの要素ごとのセクションが示されます。ダッシュボードの場合、ウィジェット グラフィックごとに独自のセクションがあります。ワークフローの場合、イベント ビューごとに独自のセクションがあります。
- 手順 10** 必要に応じてセクションの内容を変更します。
- レポート テンプレートの編集については、[レポート テンプレートのセクションの編集 \(57-13 ページ\)](#) を参照してください。



(注) 一部のワークフロー内の最後のレポート セクションには詳細ビューが含まれ、ワークフローに応じてパケット、ホスト プロファイル、または脆弱性が示されます。レポートの生成時に、これらの詳細ビューがあるイベントを多数取得すると、Defense Center のパフォーマンスに影響を与えることがあります。

- 手順 11** レポート テンプレートが適切な場合は、[保存 (Save)] をクリックします。
- レポート テンプレートが保存され、レポート テンプレートのエントリが [レポート テンプレート (Report Templates)] ページに表示されます。

レポート テンプレートのセクションの編集

ライセンス:任意 (Any)

さまざまなレポート セクションの属性を変更して、セクションとそのデータ表示の内容を調整できます。詳しくは、次の項を参照してください。

- [レポート セクションのテーブルとデータ形式の設定 \(57-14 ページ\)](#)
- [レポート セクションの検索設定またはフィルタの指定 \(57-15 ページ\)](#)
- [表形式のセクションに表示される検索フィールドの設定 \(57-15 ページ\)](#)
- [レポート テンプレートへのテキスト セクションの追加 \(57-16 ページ\)](#)
- [レポート テンプレートへの改ページの追加 \(57-17 ページ\)](#)
- [レポートとそのセクションの時間枠の設定 \(57-17 ページ\)](#)
- [レポート セクションの名前変更 \(57-18 ページ\)](#)
- [レポート セクションのプレビュー \(57-19 ページ\)](#)



(注) セキュリティ アナリストは、自分が作成したレポート テンプレートだけを編集できます。

テンプレートセクションのテーブルとデータ形式の設定


ライセンス:任意(Any)

レポートテンプレート内の各セクションでは、データベーステーブルを照会して、そのセクションの内容を生成します。セクションのデータ形式を変更する際にも同じデータクエリが使用されますが、形式のタイプごとの分析の目的に従って、セクションに表示されるフィールドが変わります。たとえば、侵入イベントの表形式の表示では、イベントレコードごとに多数のデータフィールドがセクションに入力され、円グラフのセクションでは、選択した各属性が表すすべての一致レコードの割合が示され、個々のイベントに関する詳細情報は表示されません。棒グラフのセクションでは、特定の属性を持つ一致レコードの合計数が比較されます。折れ線グラフでは、1つの属性に関係する一致レコード数の変化が時系列で要約されます。折れ線グラフはデータベースのデータの場合のみ使用でき、ホスト、ユーザ、サードパーティの脆弱性などに関する情報の場合は使用できません。

使用できるさまざまな形式の詳細については、[レポートセクションのフィールド表](#)を参照してください。

テンプレートセクションのテーブルと出力形式を選択する方法:

アクセス:Admin/Any Security Analyst

-
- 手順 1** [テーブル(Table)] ドロップダウンメニューを使用して、このセクションで照会するテーブルを選択します。
- 選択したテーブルで使用できる出力形式ごとに、アイコンが[形式(Format)]フィールドに表示されます。
- 手順 2** セクションに該当する出力形式のアイコンを選択します。これらの形式については、[レポートセクションのタイトルバーの要素表](#)を参照してください。
- 出力に含められるフィールドが表示されます。
- 手順 3** 検索設定の制約を変更するには、[検索(Search)]フィールドか[フィルタ(Filter)]フィールドの横にある編集アイコン()をクリックします。
- [検索エディタ(Search Editor)]ポップアップウィンドウが表示され、検索設定の制約に関するオプションが示されます。このウィンドウの使用の詳細については、[レポートテンプレートセクションの検索設定の操作\(57-19 ページ\)](#)を参照してください。
- 手順 4** グラフ出力形式(円グラフや棒グラフなど)の場合、ドロップダウンメニューを使用して、[X軸(X-Axis)]と[Y軸(Y-Axis)]のパラメータを調整します。
- X軸の値を選択すると、互換性のある値だけがY軸のドロップダウンメニューに表示されます。その逆も同様です。
- 手順 5** 表出力の場合、出力内の列、表示順序、ソート順序を選択します。詳細については、[表形式のセクションに表示される検索フィールドの設定\(57-15 ページ\)](#)を参照してください。
- 手順 6** [保存(Save)]をクリックして、テンプレートを保存します。
- テンプレートが保存されます。
-

テンプレートセクションの検索設定またはフィルタの指定

ライセンス:任意(Any)

レポートセクションの検索設定やフィルタは、セクションの内容のベースになるデータベースクエリを指定します。ほとんどのテーブルの場合、定義済み検索設定か保存済み検索設定を使用してレポートを制約するか、新しい検索設定を即座に作成することができます。

- 定義済み検索設定は特定のイベントテーブルの検索サンプルの役割を果たし、レポートに含めようとしている、ネットワークに関する重要情報にクイックアクセスできます。
- 保存済みイベント検索設定には、自分や他のユーザが作成したすべてのパブリック イベント検索設定と、自分で保存したすべてのプライベート イベント検索設定が含まれます。保存済みイベント検索設定の定義、命名、使用法の詳細については、[イベントの検索 \(60-1 ページ\)](#)を参照してください。
- 現在のレポートテンプレートの保存済み検索設定は、そのレポートテンプレート自体に限りアクセスできます。保存済みレポートテンプレートの検索設定の名前は、末尾が文字列「Custom Search」になります。ユーザは、レポートの設計時にこれらの検索設定を作成します。

Application Statistics テーブルの場合、ユーザ定義のアプリケーションフィルタを使用してレポートを制約できます。フィルタの作成については、[アプリケーションフィルタの操作 \(3-16 ページ\)](#)を参照してください。

テンプレートセクションの検索設定やフィルタを指定する方法:

アクセス:Admin/Any Security Analyst

-
- 手順 1** [テーブル(Table)] ドロップダウンメニューから、照会するデータベース テーブルを選択します。
- ほとんどのテーブルの場合、[検索(Search)] ドロップダウン リストが表示されます。
 - Application Statistics テーブルの場合、[フィルタ(Filter)] ドロップダウン リストが表示されます。
- 手順 2** レポートの制約に使用する検索設定かフィルタを選択します。

編集アイコン(✎)をクリックして、検索条件を表示したり、新しい検索設定を作成したりできます。詳細については、[レポートテンプレートセクションの検索設定の操作 \(57-19 ページ\)](#)を参照してください。


表形式のセクションに表示される検索フィールドの設定

ライセンス:任意(Any)

セクションに表データを組み込む場合に、データレコード内のどのフィールドを表示するか選択できます。表形式のすべてのフィールドを組み込み対象にも除外対象にもすることができます。レポートの目的を達成するのに必要なフィールドを選択し、それに従って配列したりソートしたりします。

表形式のセクションでフィールドを追加したり削除したりする方法:

アクセス:Admin/Any Security Analyst

-
- 手順 1** 表形式のセクションで、[フィールド(Fields)]パラメータの横にある編集アイコン()をクリックします。
[テーブル フィールド セレクタ (Table Field Selector)] ウィンドウが表示されます。
- 手順 2** オプションで、フィールドを追加したり削除したりしてから、フィールドのアイコンをドラッグし、ご希望のカラム順にします。
- 手順 3** オプションで、カラムのソート順序を変更します。各フィールドアイコン上のドロップダウンリストを使用して、ソート順序と優先度を設定します。
- 手順 4** フィールドの順序が正しく、必要なソート特性がある場合は、[OK] をクリックします。
[レポート セクション(Report Sections)] ページが表示されます。
-


レポートテンプレートへのテキストセクションの追加

ライセンス:任意(Any)

テンプレートにテキスト セクションを追加して、レポート全体や個々のセクションに概要などのカスタム テキストを用意することができます。テキスト セクションには、複数のフォント サイズやフォント スタイル(太字や斜体など)を使用できるリッチ テキスト、入力パラメータ、インポート済みイメージを使用できます。入力パラメータの詳細については、[入力パラメータの使用法\(57-20 ページ\)](#)を参照してください。

テキストセクションをレポートテンプレートに追加する方法:

アクセス:Admin/Any Security Analyst

-
- 手順 1** テキスト セクション追加アイコン()をクリックします。
テキスト セクションがテンプレートの下部に表示されます。
- 手順 2** 新しいテキスト セクションを、レポート テンプレート内のご希望の位置にドラッグします。
- 手順 3** オプションで、テキスト セクションの前後に改ページを追加します。改ページの詳細については、[レポートテンプレートへの改ページの追加\(57-17 ページ\)](#)を参照してください。
- 手順 4** オプションで、タイトル バー内のテキスト セクションの総称名をクリックして、新しい名前を入力します。
- 手順 5** テキスト セクションの本文に形式設定済みのテキストやイメージを追加します。レポートの生成時に動的に更新する入力パラメータを組み込むことができます。
- 手順 6** 完了したら、[保存(Save)] をクリックします。
テンプレートが保存されます。
-


レポートテンプレートへの改ページの追加

ライセンス:任意(Any)

テンプレート内のどのセクションの前後にも改ページを追加できます。この機能は、複数のセクションから成るレポートで、各種セクションの概要を示すテキストページがある場合に特に便利です。

改ページを追加する方法:

アクセス:Admin/Any Security Analyst

-
- 手順 1 改ページ追加アイコン()をクリックします。
改ページがテンプレートの下部に表示されます。
- 手順 2 改ページを、セクションの前後のご希望の場所にドラッグします。
- 手順 3 テンプレートに追加するすべての改ページに対してこのプロセスを繰り返します。
-

テンプレートとそのセクションの時間枠の設定

ライセンス:任意(Any)

レポートテンプレートの時間枠は、テンプレートのレポート作成期間を定義します。時間ベースのデータ(侵入イベントや検出イベントなど)があるレポートテンプレートにはグローバル時間枠があります。この時間枠は、テンプレート内の時間ベースのセクションでデフォルトで作成時に継承されます。グローバル時間枠を変更すると、グローバル時間枠を継承するように設定されているセクションのローカル時間枠が変更されます。[時間枠を継承する(Inherit Time Window)]チェックボックスをクリアすると、個々のセクションの時間枠の継承を無効にできます。それから、ローカル時間枠を編集できます。





(注)

グローバル時間枠の継承は、侵入イベントや検出イベントなど、時間ベースのテーブルからのデータがあるレポートセクションだけに適用されます。ネットワークアセット(ホストやデバイス)と関連情報(脆弱性など)を報告するセクションの場合、各時間枠を個別に設定する必要があります。

レポートテンプレートのグローバル時間枠を変更する方法:

アクセス:Admin/Any Security Analyst

-
- 手順 1 [レポートテンプレート(Report Templates)] ページで、編集するレポートテンプレートの横にある編集アイコン()をクリックします。
[レポートセクション(Report Sections)] ページが表示されます。
- 手順 2 [生成(Generate)] をクリックします。
[レポートの生成(Generate Report)] ポップアップウィンドウが表示されます。
- 手順 3 グローバル時間枠を変更するには、時間枠のアイコン()をクリックします。
新しいウィンドウに[イベント時間枠(Events Time Window)] ページが表示されます。このページの使用方法に関する詳細については、[イベント時間の制約の設定\(58-26 ページ\)](#)を参照してください。

- 手順 4** 終了したら、[イベント時間枠 (Events Time Window)] ウィンドウで [適用 (Apply)] をクリックします。
- [レポートの生成 (Generate Report)] ポップアップ ウィンドウに新しい時間枠が再表示されます。
- 手順 5** [キャンセル (Cancel)] をクリックして [レポート セクション (Report Sections)] ページに戻るか、[OK] をクリックしてレポートを生成します。
- レポート内のセクションごとに別の時間枠を使用できます。たとえば、最初のセクションを月の要約にして、残りのセクションで週レベルの詳細情報へドリルダウンするようにできます。この場合、セクション レベルの時間枠を個別に設定します。

セクションのローカル時間枠を設定する方法:

アクセス: Admin/Any Security Analyst

- 手順 1** テンプレートの [レポート セクション (Report Sections)] ページで、セクションの [時間枠を継承する (Inherit Time Window)] チェック ボックスが存在する場合はクリアします。
- ローカル セクション時間枠のアイコンが表示されます。
- 手順 2** セクションのローカル時間枠を変更するには、時間枠のアイコン (🕒) をクリックします。
- [イベント時間枠 (Events Time Window)] ページが表示されます。このページの使用方法に関する詳細については、[イベント時間の制約の設定 \(58-26 ページ\)](#) を参照してください。



(注) 統計テーブルからのデータがあるセクションでは、スライド式の時間枠のみ使用できます。

- 手順 3** 新しいローカル時間枠を設定し終わったら、[イベント時間枠 (Events Time Window)] で [適用 (Apply)] をクリックします。
- 手順 4** [保存 (Save)] をクリックします。
- さらに編集できるように [レポート セクション (Report Sections)] ページが表示されます。

テンプレート セクションの名前変更

ライセンス: 任意 (Any)

新しいテンプレートの作成時に追加したセクションには総称セクション名が付けられるので、内容を表す名前に変更する必要があります。

テンプレート セクションの名前を変更する方法:

アクセス: Admin/Any Security Analyst

- 手順 1** セクション 見出し内の現在のセクション名をクリックします。
- [セクション タイトルの設定 (Set Section Title)] ポップアップ ウィンドウが表示されます。
- 手順 2** セクションの新しい名前を入力し (最大 120 文字)、[OK] をクリックします。
- セクションのタイトル バー内の名前が変わります。

テンプレートセクションのプレビュー

ライセンス:任意(Any)

プレビュー機能は、表形式の表示のフィールドのレイアウトとソート順序や、円グラフの色などのグラフの読みやすさに関する重要な特性を表示します。

テンプレートセクションをプレビューする方法:

アクセス:Admin/Any Security Analyst

-
- 手順 1** セクションの編集集中のいつでも、そのセクションの [プレビュー (Preview)] をクリックします。
[プレビュー (Preview)] ポップアップ ウィンドウが表示されます。
- 手順 2** ウィンドウの下部にある [OK] をクリックし、プレビューを閉じます。
[レポート セクション (Report Sections)] ページが表示されます。
-

レポートテンプレートセクションの検索設定の操作

ライセンス:任意(Any)

レポートが正常に作成されるかどうかは、レポートのセクションへの入力内容を決める検索設定の定義が重要な要素になります。FireSIGHT システムには検索エディタが備えられており、レポートテンプレートで使用できる検索設定を表示したり、新しいカスタム検索設定を定義したりできます。



ヒント

レポートテンプレート内で作成したカスタム検索設定は、そのテンプレートに固有になります。イベントビューアで、すべてのレポートテンプレートで再利用できる検索設定を作成できます。イベントビューアでカスタム検索設定を保存すると、すべてのレポートテンプレートの [検索 (Search)] ドロップダウンメニューに表示されます。イベントビューアを使用してカスタム検索設定を作成して保存する方法の詳細については、[イベントの検索 \(60-1 ページ\)](#) を参照してください。

カスタム検索設定を作成する方法:

アクセス:Admin/Any Security Analyst

-
- 手順 1** レポートテンプレート内の関連するセクションから、[検索 (Search)] フィールドの横にある編集アイコン(✎)をクリックします。
[検索エディタ (Search Editor)] ページが表示され、選択した検索対象のテーブルが示されます。
- 手順 2** オプションで、[保存済み検索 (Saved Searches)] ドロップダウンメニューから、定義済み検索設定を選択します。
ドロップダウンに、このテーブルに関する使用可能な定義済み検索設定がすべて表示されます。システム規模の定義済み検索設定とレポート固有の定義済み検索設定が含まれます。
- 手順 3** 該当するフィールドで検索条件を編集します。特定のフィールドの場合、制約にイベント検索設定と同じ演算子(< や <> など)を含めることができます。検索条件の構文については、[イベントの検索 \(60-1 ページ\)](#) を参照してください。
複数の基準を入力した場合は、すべての基準を満たすレコードだけが検索で返されます。

手順 4 オプションで、入力パラメータのアイコン(+)が表示されている位置で、制約値を入力する代わりにドロップダウンメニューから入力パラメータを挿入できます。レポートの設計で入力パラメータを使用する方法の詳細については、[入力パラメータの使用法\(57-20 ページ\)](#)を参照してください。

一部の検索フィールドの場合、ドロップダウンメニューにユーザ定義の管理対象オブジェクトが、入力パラメータの代わりに示されるか、入力パラメータと共に示される場合があります。管理対象オブジェクトは、検索設定を制約する値として使用できるシステム設定変数で、タイプに応じて固有なアイコンがあります。ただしこれらは、入力パラメータで行われるユーザ入力に関する生成時クエリを作成しません。管理対象オブジェクトの詳細については、[再利用可能なオブジェクトの管理\(3-1 ページ\)](#)を参照してください。



(注) レポートの検索設定の制約を編集すると、システムにより `section custom search` という名前で編集済みの検索設定が保存されます。`section` は、セクションのタイトルバーに示される文字列 `custom search` の前の名前の部分です。保存するカスタム検索設定の名前をわかりやすくするには、セクション名を変更した後に編集済みの検索設定を保存するようにしてください。保存したレポートの検索設定の名前を変更することはできません。

手順 5 検索エディタでフィールドを変更し終わったら、[OK] をクリックします。

[レポート セクション(Report Sections)] ページが再表示され、新しい定義済み検索設定がセクションの [検索(Search)] ドロップダウンメニューに表示されます。

入力パラメータの使用法

ライセンス:任意(Any)

レポートの生成時に動的に更新できる入力パラメータをレポートテンプレート内で使用できます。入力パラメータのアイコン(+)は、入力パラメータを処理できるフィールドを示します。次の2種類の入力パラメータがあります。

- 定義済み:[定義済みの入力パラメータ表](#)を参照
- ユーザ定義:[ユーザ定義の入力パラメータのタイプ表](#)を参照

定義済みの入力パラメータ

ライセンス:任意(Any)

定義済みの入力パラメータは、内部システム関数か設定情報によって解決されます。たとえば、レポートの生成時に、システムにより `$(Time)` パラメータは現在の日時に置き換えられます。次の表に、使用できるパラメータを定義します。たとえば、スケジューラの制御下で自動的に生成される月次要約レポートのタイトルに `$(Month)` を含めることもできます。その後、レポートのタイトルは正しい月で自動的に更新されます。

表 57-4 定義済みの入力パラメータ

| 挿入するパラメータ | テンプレートに含められる情報 |
|-------------------------------|---------------------|
| <code>\$(Logo)</code> | 選択したアップロード済みのロゴ |
| <code>\$(Report Title)</code> | レポートのタイトル |
| <code>\$(Time)</code> | レポートが実行された日時、精度 1 秒 |

表 57-4 定義済みの入力パラメータ(続き)

| 挿入するパラメータ | テンプレートに含まれる情報 |
|------------------|--------------------------|
| \$<Month> | 現在の月 |
| \$<Year> | 現在の年 |
| \$<System Name> | Defense Center の名前 |
| \$<Model Number> | Defense Center のモデル番号 |
| \$<Time Window> | 現在レポート セクションに適用されている時間枠 |
| \$<Constraints> | 現在レポート セクションに適用されている検索制約 |

次の表に、[レポートテンプレート (Report Templates)] ページ内のさまざまな領域で使用できる有効な入力パラメータをリストします。

表 57-5 定義済みの入力パラメータの使用法

| パラメータ | Report Template Cover Page (レポートテンプレートの表紙) | Report Template Report Title (レポートテンプレートのレポートタイトル) | Report Template Section Description (レポートテンプレートセクションの説明) | Report Template Text Section (レポートテンプレートテキストセクション) | Generate Report File Name (レポート生成ファイル名) | Generate Report Email Subject, Body (レポート生成電子メール件名、本文) |
|------------------|--|--|--|--|---|--|
| \$<Logo> | はい | いいえ | いいえ | いいえ | いいえ | いいえ |
| \$<Report Title> | はい | いいえ | はい | はい | はい | はい |
| \$<Time> | はい | はい | はい | はい | はい | はい |
| \$<Month> | はい | はい | はい | はい | はい | はい |
| \$<Year> | はい | はい | はい | はい | はい | はい |
| \$<System Name> | はい | はい | はい | はい | はい | はい |
| \$<Model Number> | はい | はい | はい | はい | はい | はい |
| \$<Time Window> | いいえ | いいえ | はい | いいえ | いいえ | いいえ |
| \$<Constraints> | いいえ | いいえ | はい | いいえ | いいえ | いいえ |

ユーザ定義の入力パラメータ

ライセンス:任意 (Any)

独自の入力パラメータを作成して、セクションの検索設定で制約として使用できます。入力パラメータを使用して検索設定を制約すると、レポートの生成時に要求者から値を収集するようにシステムに指示できます。この方法で、テンプレートを変更せずに、レポートを生成時に動的に調整して特定のデータのサブセットを表示できます。たとえば、レポートセクションの検索設定の [宛先 IP (Destination IP)] フィールドに入力パラメータを指定できます。指定後、レポートの生成時に、特定の部門の IP ネットワークのセグメントを入力して、その部門のデータだけを取得できます。



ヒント

また、入力パラメータフィールドに * を入力すると、制約が無視される効果があります。

文字列タイプの入力パラメータを定義して、電子メール(件名または本文)、レポート ファイル名、テキスト セクションなどのレポートの特定のフィールドに動的テキストを追加することもできます。すべて同じテンプレートを利用し、カスタマイズしたレポート ファイル名、電子メールアドレス、電子メール メッセージを使用して、さまざまな部門用にレポートをパーソナリ化できます。

定義する入力パラメータごとに名前とタイプがあります。次の表に、パラメータのタイプを示します。



表 57-6 ユーザ定義の入力パラメータのタイプ

| パラメータのタイプ | 使用先のフィールド内のデータ |
|-------------------------------|---|
| ネットワーク/IP | CIDR 形式の IP アドレスまたはネットワーク セグメント |
| アプリケーション | アプリケーション プロトコル、クライアント アプリケーション、または Web アプリケーションの名前 |
| イベント メッセージ | イベント ビュー メッセージ |
| デバイス | 3D アプライアンス (Defense Center または FireSIGHT システムの管理対象デバイス) |
| ユーザ名 | イニシエータ ユーザやレスポнда ユーザなどのユーザ ID |
| 番号 (VLAN ID、Snort ID、Vuln ID) | VLAN ID、Snort ID、または脆弱性 ID |
| 文字列 | アプリケーションや OS のバージョン、注記、説明などのテキスト フィールド |

入力パラメータのタイプにより、そのパラメータを使用できる検索フィールドが決まります。指定したタイプは、[ユーザ定義の入力パラメータのタイプ](#)表に示されている当該フィールドのみで使用できます。たとえば、ユーザ パラメータを文字列タイプとして定義すると、テキスト フィールド内への挿入には使用できますが、IP アドレスを使用するフィールドでは使用できません。

レポートテンプレートに関するユーザ定義の入力パラメータを作成する方法:

アクセス: Admin/Any Security Analyst

- 手順 1 [概要 (Overview)] > [レポート (Reporting)] を選択します。
- 手順 2 [レポート テンプレート (Report Templates)] タブを選択します。
[レポート テンプレート (Report Templates)] ページが表示されます。
- 手順 3 編集するテンプレートの編集アイコン()をクリックします。
[レポート セクション (Report Sections)] ページが表示されます。
- 手順 4 [詳細設定 (Advanced)] をクリックします。
[詳細設定 (Advanced Settings)] ポップアップ ウィンドウが表示されます。
- 手順 5 入力パラメータ追加アイコン()をクリックします。
[入力パラメータの追加 (Add Input Parameter)] ポップアップ ウィンドウが表示されます。
- 手順 6 [名前 (Name)] フィールドにパラメータ名を入力し、[タイプ (Type)] ドロップダウンメニューを使用してタイプを選択してから、[OK] をクリックします。
新しいパラメータが [入力パラメータ (Input Parameters)] メニューに表示されます。

手順 7 必要なパラメータをすべて定義し終えるまで、上記の手順を繰り返します。

手順 8 [OK] をクリックします。

このテンプレートの新しい入力パラメータが保存され、[レポート セクション (Report Sections)] ページが再表示されます。

レポート テンプレートを再利用する場合、入力パラメータの名前とタイプを変更して、新しいレポートの目的をいっそう反映させることができます。

レポート テンプレートに関するユーザ定義の入力パラメータを編集する方法:

アクセス: Admin/Any Security Analyst

手順 1 [概要 (Overview)] > [レポート (Reporting)] を選択します。

手順 2 [レポート テンプレート (Report Templates)] タブを選択します。

[レポート テンプレート (Report Templates)] ページが表示されます。

手順 3 編集するテンプレートの編集アイコン(✎)をクリックします。

[レポート セクション (Report Sections)] ページが表示されます。

手順 4 [詳細設定 (Advanced)] をクリックします。

[詳細設定 (Advanced Settings)] ポップアップ ウィンドウが表示されます。[入力パラメータ (Input Parameters)] セクションに、レポート テンプレートの使用可能なユーザ定義パラメータがすべてリストされます。

手順 5 編集アイコン(✎)をクリックします。

[入力パラメータの編集 (Edit Input Parameter)] ポップアップ ウィンドウが表示されます。

手順 6 [名前 (Name)] フィールドでパラメータ名を変更し、[タイプ (Type)] ドロップダウンメニューを使用してパラメータ タイプを変更してから、[OK] をクリックします。

変更したパラメータが、[入力パラメータ (Input Parameters)] セクションに表示されます。

手順 7 必要なパラメータをすべて定義し終えるまで、上記の手順を繰り返します。[OK] をクリックします。

変更が保存され、[レポート セクション (Report Sections)] ページが再表示されます。

レポート テンプレートに関するユーザ定義の入力パラメータを削除する方法:

アクセス: Admin/Any Security Analyst

手順 1 [概要 (Overview)] > [レポート (Reporting)] を選択します。

手順 2 [レポート テンプレート (Report Templates)] タブを選択します。

[レポート テンプレート (Report Templates)] ページが表示されます。

手順 3 編集するテンプレートの編集アイコン(✎)をクリックします。

[レポート セクション (Report Sections)] ページが表示されます。

- 手順 4 [詳細設定(Advanced)] をクリックします。
[詳細設定(Advanced Settings)] ポップアップ ウィンドウが表示されます。[入力パラメータ (Input Parameters)] セクションに、レポート テンプレートの使用可能なユーザ定義パラメータがすべてリストされます。
- 手順 5 入力パラメータの横の削除アイコン(🗑️) をクリックして確認します。
- 手順 6 [OK] をクリックします。
入力パラメータが削除され、[レポート セクション (Report Sections)] ページが再表示されます。

入力パラメータを使用して、検索設定の実用性を向上させます。入力パラメータは、レポート生成時にレポートの要求者から値を収集するようシステムに指示します。この方法で、検索設定を変更せずに、レポートを生成時に動的に制約して特定のデータのサブセットを表示できます。たとえば、レポート セクションの [宛先 IP (Destination IP)] フィールドに入力パラメータを指定して、部門レベルでセキュリティ イベントをドリルダウンできます。レポートの生成時に、特定の部門の IP ネットワークのセグメントを入力して、その部門のデータだけを取得できます。

ユーザ定義の入力パラメータを使用してレポート テンプレート内の検索設定を制約する方法:
アクセス: Admin/Any Security Analyst

- 手順 1 [概要 (Overview)] > [レポート (Reporting)] を選択します。
- 手順 2 [レポート テンプレート (Report Templates)] タブを選択します。
[レポート テンプレート (Report Templates)] ページが表示されます。
- 手順 3 編集するテンプレートの編集アイコン(✎) をクリックします。
[レポート セクション (Report Sections)] ページが表示されます。
- 手順 4 セクション内の [検索 (Search)] フィールドの横にある編集アイコン(✎) をクリックします。
[検索エディタ (Search Editor)] ポップアップ ウィンドウが表示されます。入力パラメータを使用できるフィールドは、入力パラメータのアイコン(⊕) のマークが付けられます。
- 手順 5 フィールドの横にある入力パラメータのアイコン(⊕) をクリックして、ドロップダウンメニューから入力パラメータを選択します。ユーザ定義の入力パラメータはアイコン(🔗) のマークが付けられます。
入力パラメータがフィールドに表示されます。



(注) 定義した入力パラメータは、そのパラメータのタイプと一致する検索フィールドでのみ使用できます。たとえば、ネットワーク/IP タイプのパラメータは、CIDR 形式の IP アドレスまたはネットワーク セグメントを受け入れるフィールドだけで使用できます。

- 手順 6 必要な入力パラメータをすべて追加し終えたら、[OK] をクリックします。
[レポート セクション (Report Sections)] ページと変更内容が表示されます。

レポートテンプレート内のドキュメント属性の編集

ライセンス:任意(Any)



レポートを生成する前に、レポートの外観に影響を与えるドキュメント属性を設定できます。これらの属性には、オプションの表紙と目次が含まれます。一部の属性のサポートは、レポートの形式に PDF、HTML、CSV のいずれを選択したかによって異なります。次の表で、形式別の属性のサポートについて詳しく説明します。

表 57-7 ドキュメント属性のサポート

| 属性 | PDF のサポート | HTML のサポート | CSV のサポート |
|--------------------|----------------------------|-----------------------|-----------|
| 表紙 | 可能、オプションでロゴと外観のカスタマイズ | 可能、オプションでロゴと外観のカスタマイズ | いいえ |
| 目次 | はい | はい | いいえ |
| ページの見出しとフッター | 可能、オプションで任意のフィールド内にテキストかロゴ | いいえ | いいえ |
| カスタムの開始ページ番号 | はい | いいえ | いいえNo |
| 先頭ページに番号を付けないオプション | はい | いいえ | いいえ |

PDF レポートや HTML レポートのドキュメント属性を設定する方法:

アクセス: Admin/Any Security Analyst

- 手順 1 [概要(Overview)] > [レポート(Reporting)] を選択します。
- 手順 2 [レポートテンプレート(Report Templates)] タブを選択します。
[レポートテンプレート(Report Templates)] ページが表示されます。
- 手順 3 編集するレポートテンプレートの編集アイコン()をクリックします。
[レポートセクション(Report Sections)] ページが表示されます。
- 手順 4 [詳細設定(Advanced)] をクリックします。
[詳細設定(Advanced Settings)] ポップアップウィンドウが表示されます。
- 手順 5 [表紙を含める(Include Cover Page)] を選択して表紙を追加します。
- 手順 6 [表紙のデザイン(Cover Page Design)] フィールドの横にある編集アイコン()をクリックして、表紙のデザインを編集します。
詳細については、[表紙のカスタマイズ\(57-26 ページ\)](#)を参照してください。
- 手順 7 [目次を含める(Include Table of Contents)] を選択して、目次を追加します。
- 手順 8 3 つの [ヘッダー(Header)] フィールドと [フッター(Footer)] フィールドのドロップダウンを使用して、見出しとフッターを設定します。ドロップダウンメニューから見出しとフッターのコンテンツとしてロゴ、日付、ページ番号などを選択します。
[ロゴ(Logo)] を選択すると、選択したフィールドにデフォルトのロゴイメージが表示されます。デフォルトのロゴイメージを変更する場合は、[ロゴの管理\(57-27 ページ\)](#)を参照してください。

- 手順 9** [先頭ページ番号 (Page Number Start)] フィールドで、レポートの先頭ページのページ番号を選択します。
- [先頭ページに番号を付けるか (Number First Page?)] を選択すると、表紙の次の先頭ページにページ番号が表示されます。これを選択すると、表紙には番号が付けられません。
- 手順 10** [OK] をクリックします。
- ドキュメント属性が保存され、[レポート セクション (Report Sections)] ページが再表示されます。
-

表紙のカスタマイズ

ライセンス:任意 (Any)

レポートテンプレートの表紙をカスタマイズできます。表紙には、複数のフォントサイズやフォントスタイル(太字や斜体など)を使用できるリッチテキスト、入力パラメータ、インポート済みイメージを使用できます。入力パラメータの詳細については、[入力パラメータの使用法 \(57-20 ページ\)](#)を参照してください。

レポートテンプレートの表紙をカスタマイズする方法:

アクセス:Admin/Any Security Analyst

- 手順 1** [概要 (Overview)] > [レポート (Reporting)] を選択します。
- 手順 2** [レポートテンプレート (Report Templates)] タブを選択します。
- [レポートテンプレート (Report Templates)] ページが表示され、テンプレートのリストが表示されます。
- 手順 3** レポートテンプレートの編集アイコン(✎)をクリックします。
- [レポートセクション (Report Sections)] ページが表示されます。
- 手順 4** [詳細設定 (Advanced)] をクリックします。
- [詳細設定 (Advanced Settings)] ポップアップウィンドウが表示されます。
- 手順 5** [表紙ページのデザイン (Cover Page Design)] の横にある編集アイコン(✎)をクリックします。
- [表紙ページの編集 (Edit Cover Page)] ウィンドウが表示され、デフォルトの表紙のデザインが表示されます。
- 手順 6** リッチテキストエディタで表紙のデザインを編集します。
- 手順 7** [OK] をクリックします。
- 表紙のデザインが保存され、[詳細設定 (Advanced Settings)] ウィンドウが再表示されます。
-

ロゴの管理

ライセンス:任意(Any)

Defense Center で複数のロゴを保存し、さまざまなレポート テンプレートに関連付けることができます。テンプレートを設計する際に、ロゴの関連付けを設定します。テンプレートをエクスポートすると、エクスポート パッケージにロゴが含まれます。

レポート内のロゴを挿入できる位置については、[レポート テンプレート内のドキュメント属性の編集\(57-25 ページ\)](#)を参照してください。

詳細については、次の関連した手順を参照してください。

- [新しいロゴの追加\(57-27 ページ\)](#)
- [レポート テンプレートのロゴの変更\(57-28 ページ\)](#)
- [ロゴの削除\(57-29 ページ\)](#)



新しいロゴの追加

ライセンス:任意(Any)

Defense Center にアップロードしたロゴは、その Defense Center 上のすべてのレポート テンプレートで利用できます。ロゴイメージは JPG 形式にする必要があります。

ロゴを Defense Center に追加する方法:

アクセス:Admin/Any Security Analyst

-
- 手順 1 [概要(Overview)] > [レポート(Reporting)] を選択します。
 - 手順 2 [レポート テンプレート(Report Templates)] タブを選択します。
[レポート テンプレート(Report Templates)] ページが表示されます。
 - 手順 3 編集するレポート テンプレートの編集アイコン()をクリックします。
[レポート セクション(Report Sections)] ページが表示されます。
 - 手順 4 [詳細設定(Advanced)] をクリックします。
[詳細設定(Advanced Settings)] ポップアップ ウィンドウが表示されます。テンプレートに現在関連付けられているロゴが、[一般設定(General Settings)] の [ロゴ(Logo)] の下に表示されます。
 - 手順 5 ロゴの編集アイコン()をクリックします。
[ロゴの選択(Select Logo)] ポップアップ ウィンドウが表示され、現在アップロードされているロゴのイメージが示されます。
 - 手順 6 [ロゴのアップロード(Upload Logo)] をクリックします。
[ロゴのアップロード(Upload Logo)] ポップアップ ウィンドウが表示されます。
 - 手順 7 次のいずれかの手順で、アップロードするロゴファイルを選択します。
 - ログ ファイルの場所を入力します。
 - [参照(Browse)] ボタンをクリックし、ファイルの場所を参照します。

- 手順 8 [アップロード(Upload)] をクリックします。
イメージが Defense Center にアップロードされ、[ロゴの選択(Select Logo)] ポップアップ ウィンドウに表示されます。
- 手順 9 オプションで、新しいロゴを選択して [OK] をクリックし、現在のテンプレートに関連付けます。
[詳細設定(Advanced Settings)] ウィンドウが再表示され、関連付けられたロゴイメージが表示されます。
-

レポートテンプレートのロゴの変更

ライセンス:任意(Any)

レポート内のロゴを、Defense Center にアップロードされている任意の JPG イメージに変更できます。たとえば、テンプレートを再使用する場合に、別の組織のロゴをレポートに関連付けることができます。

レポートテンプレートのロゴを変更する方法:

アクセス:Admin/Any Security Analyst

- 手順 1 [概要(Overview)] > [レポート(Reporting)] を選択します。
- 手順 2 [レポートテンプレート(Report Templates)] タブを選択します。
[レポートテンプレート(Report Templates)] ページが表示されます。
- 手順 3 編集するレポートテンプレートの編集アイコン(✎) をクリックします。
[レポートセクション(Report Sections)] ページが表示されます。
- 手順 4 [詳細設定(Advanced)] をクリックします。
[詳細設定(Advanced Settings)] ポップアップ ウィンドウが表示されます。テンプレートに現在関連付けられているロゴが、[一般設定(General Settings)] の [ロゴ(Logo)] の下に表示されます。
- 手順 5 ロゴの編集アイコン(✎) をクリックします。
[ロゴの選択(Select Logo)] ポップアップ ウィンドウが表示され、現在アップロードされているロゴのイメージが表示されます。
- 手順 6 レポートテンプレートに関連付けるロゴを選択します。
選択したロゴが強調表示されます。
- 手順 7 [OK] をクリックします。
[詳細設定(Advanced Settings)] ウィンドウが再表示され、関連付けられたロゴイメージが表示されます。
-

ロゴの削除

ライセンス:任意(Any)

ロゴを Defense Center から削除できます。ロゴを削除すると、そのロゴが使用されているすべてのテンプレートから削除されます。削除を取り消すことはできません。

定義済みのシスコのロゴを削除できないことに注意してください。

ロゴを Defense Center から削除する方法:

アクセス:Admin/Any Security Analyst

-
- 手順 1 [概要(Overview)] > [レポート(Reporting)] を選択します。
 - 手順 2 [レポート テンプレート(Report Templates)] タブを選択します。
[レポート テンプレート(Report Templates)] ページが表示されます。
 - 手順 3 編集するレポート テンプレートの編集アイコン(✎)をクリックします。
[レポート セクション(Report Sections)] ページが表示されます。
 - 手順 4 [詳細設定(Advanced)] をクリックします。
[詳細設定(Advanced Settings)] ポップアップ ウィンドウが表示されます。テンプレートに現在関連付けられているロゴが、[一般設定(General Settings)] の [ロゴ(Logo)] の下に表示されます。
 - 手順 5 ロゴの編集アイコン(✎)をクリックします。
[ロゴの選択(Select Logo)] ポップアップ ウィンドウが表示され、現在アップロードされているロゴのイメージが示されます。
 - 手順 6 削除するロゴを選択します。
選択したロゴが強調表示されます。
 - 手順 7 [ロゴの削除>Delete Logo] をクリックします。
削除したロゴが、[ロゴの選択(Select Logo)] ポップアップ ウィンドウで表示されなくなります。
 - 手順 8 [OK] をクリックします。
変更内容が保存され、[詳細設定(Advanced Settings)] ウィンドウが再表示されます。
-

レポートの生成と表示

ライセンス:任意(Any)

レポート テンプレートの作成とカスタマイズができれば、レポート生成の準備は終了です。生成プロセスで、レポートの形式(HTML、PDF、または CSV)を選択できます。レポートのグローバル時間枠を調整することもできます。この時間枠は、除外されていないすべてのセクションに一貫したタイム フレームを適用します。レポートの時間枠の設定については、[テンプレートとそのセクションの時間枠の設定\(57-17 ページ\)](#)を参照してください。

レポート テンプレートの検索の指定にユーザ入力パラメータが含まれている場合、生成プロセスで値を入力するよう求められ、このレポートの実行内容がデータのサブセットに合わせて調整されます。入力パラメータの詳細については、[入力パラメータの使用法\(57-20 ページ\)](#)を参照してください。

[レポート(Reports)] タブには、以前に生成されたすべてのレポートと、そのレポート名、生成日時、生成したユーザ、およびそのレポートがローカルに保存されたかリモートに保存されたかが一覧表示されます。ステータスのカラムには、レポートがすでに生成されているか、生成キュー内にある(スケジュール済みタスクの場合など)か、それとも生成できなかった(ディスク領域不足などの理由で)かが示されます。

[レポート(Reports)] タブのページには、ローカルに保存されたレポートがすべて示されます。リモートストレージが現在設定されている場合、リモートに保存されたレポートも示されます。ページの下部に、現在設定されているレポートストレージの場所が表示され、ローカル、NFS、SMB ストレージの場合はディスク使用率も表示されます。SSH を使用してリモートストレージにアクセスする場合、ディスク使用率のデータは利用できません。リモートストレージのセットアップの詳細については、[レポート用のリモートストレージの使用法\(57-33 ページ\)](#)を参照してください。



(注)

リモートに保存してから、ローカルストレージに切り替えた場合、リモートストレージ内のレポートは [レポート(Reports)] タブのリストに表示されません。同様に、あるリモートストレージの場所から別の場所に切り替えた場合、以前の場所にあるレポートはリストに表示されません。




Unicode(UTF8)文字を使用したファイル名は PDF レポートではサポートされません。PDF 形式のレポートを生成すると、特殊な Unicode ファイル名が含まれるレポートセクション(ファイルイベントやマルウェア イベントで表示されるセクションなど)では、そのファイル名は書き直された形式で表示されます。

DNS サーバの設定および IP アドレス解決が有効化されている場合、正常に解決されたホスト名がレポートに取り込まれます。詳細については、[管理インターフェイスの構成\(64-9 ページ\)](#)および[イベント設定\(71-4 ページ\)](#)を参照してください。

レポートを生成して表示するには、次の手順を実行します。管理者アクセス権を持つユーザはすべてのレポートを表示でき、その他のユーザは自分が生成したレポートだけを表示できることに注意してください。レポートファイルの管理については、[レポートのダウンロード\(57-36 ページ\)](#)および[レポートの削除\(57-37 ページ\)](#)を参照してください。

レポートテンプレートからレポートを生成する方法:

アクセス:Admin/Any Security Analyst

- 手順 1 [概要(Overview)] > [レポート(Reporting)] を選択します。
- 手順 2 [レポートテンプレート(Report Templates)] タブをクリックします。
[レポートテンプレート(Report Templates)] ページが表示されます。
- 手順 3 使用するテンプレートのレポート生成アイコン()をクリックします。
[レポートの生成(Generate Report)] ポップアップダイアログが表示されます。
- 手順 4 オプションで、[ファイル名(File Name)] フィールドに新しい名前を入力します。生成されるレポートファイルの名前が設定されます。入力パラメータのアイコン()を使用して、1つ以上の入力パラメータをファイル名に追加することもできます。入力パラメータの詳細については、[入力パラメータの使用法\(57-20 ページ\)](#)を参照してください。
- 手順 5 対応するアイコン(HTML、PDF、または CSV)をクリックして、レポートの出力形式を選択します。
- 手順 6 オプションで、時間枠のアイコン()をクリックして、グローバル時間枠を変更します。
[イベント時間枠(Events Time Window)] ポップアップウィンドウが表示されます。イベントの時間枠の設定については、[イベント時間の制約の設定\(58-26 ページ\)](#)を参照してください。



(注) グローバル時間枠を設定すると、個々のレポート セクションのうちグローバル設定を継承するように設定されているものの内容だけが影響を受けます。レポート セクションのグローバル時間枠の継承については、[テンプレートとそのセクションの時間枠の設定 \(57-17 ページ\)](#)を参照してください。

手順 7 [入力パラメータ (Input Parameters)] セクションに表示されるフィールドの値を入力します。



ヒント フィールドにワイルドカード文字 * を入力すると、ユーザ パラメータを無視できます。こうすると、検索設定がユーザ パラメータで制約されなくなります。

手順 8 オプションで、システム ポリシーで電子メール リレー ホストが設定されている場合、[電子メール (Email)] をクリックして、レポートの生成時電子メール配信を自動化します。電子メール配信機能については詳しくは、[レポートの生成時の電子メール配布 \(57-32 ページ\)](#)を参照してください。

手順 9 求められたら、[OK] をクリックして確認します。

[レポート生成完了 (Report Generation Complete)] ポップアップ ウィンドウと、レポートを表示するためのリンクが表示されます。

手順 10 次のいずれかをクリックします。

- 新しいウィンドウを開いてレポートを表示する場合は、レポートのリンク。
- [レポート セクション (Report Section)] ページに戻る場合は、[OK]。このページでレポートの設計を変更できます。

初めて生成した後に、完成したレポートをレビューすることもできます。

手順 11 オプションで、レポート ファイルを管理します。詳細については、[レポートのダウンロード \(57-36 ページ\)](#)および[レポートの削除 \(57-37 ページ\)](#)を参照してください。

生成したレポートを表示する方法:

アクセス: Admin/Any Security Analyst

手順 1 [概要 (Overview)] > [レポート (Reporting)] を選択します。

手順 2 [レポート (Reports)] タブをクリックします。

[レポート (Reports)] ページが表示されます。

手順 3 レポート名をクリックします。

ローカル ホスト上のデフォルトのプログラムにより、新しいウィンドウでレポートが開かれます。

手順 4 ドキュメントの確認が終わったら、ブラウザを使用して [レポート (Reports)] タブに戻ります。

レポート生成オプションの使用法

ライセンス:任意(Any)

レポートを生成する際の追加のオプションが複数あります。レポートの生成を自動的にスケジュールしたり、レポートを電子メールで送信したり、生成したレポートをリモートに保存したりできます。詳細については、次の項を参照してください。

- [スケジューラを使用したレポートの生成\(57-32 ページ\)](#)
- [レポートの生成時の電子メール配布\(57-32 ページ\)](#)
- [レポート用のリモート ストレージの使用法\(57-33 ページ\)](#)

スケジューラを使用したレポートの生成

ライセンス:任意(Any)

FireSIGHT システムのスケジューラを使用して、レポートの生成を自動化できます。毎日、毎週、毎月など、さまざまな範囲のタイム フレームに基づいたスケジュールでもカスタマイズできます。詳細については、[レポートの生成を自動化する方法\(62-9 ページ\)](#)を参照してください。

また、スケジューラを使用して電子メール レポートを配布する場合は、タスクをスケジュールする前に、レポート テンプレートとメール リレー ホストの設定が必要です。詳細については、[レポートの生成時の電子メール配布\(57-32 ページ\)](#)および[メール リレー ホストおよび通知アドレスの設定\(63-20 ページ\)](#)を参照してください。

レポートの生成時の電子メール配布

ライセンス:任意(Any)

レポートをテンプレートから生成するときには、レポートを電子メールの添付ファイルとして受信者リストに自動送信するよう選択できます。



(注)

レポートを電子メールで配信するように、メール リレー ホストを適切に設定していなければなりません。まだメール ホストをセットアップしていない場合は、[メール リレー ホストおよび通知アドレスの設定\(63-20 ページ\)](#)を参照してください。

レポートを生成時に電子メールで送信する方法:

アクセス:Admin/Any Security Analyst

- 手順 1 [概要(Overview)] > [レポート(Reporting)] を選択します。
- 手順 2 [レポート テンプレート(Report Templates)] タブを選択します。
[レポート テンプレート(Report Templates)] ページが表示されます。
- 手順 3 生成元のテンプレートのレポート生成アイコン()をクリックします。
[レポートの生成(Generate Report)] ポップアップ ウィンドウが表示されます。
- 手順 4 このウィンドウの [電子メール(Email)] セクションを展開します。
- 手順 5 [電子メール オプション(Email Options)] フィールドで、[電子メールの送信(Send Email)] を選択します。

手順 6 [受信者リスト (Recipient List)], [CC] および [BCC] フィールドで、カンマ区切りリストの形式で受信者の電子メール アドレスを入力します。

手順 7 [件名 (Subject)] フィールドに電子メールの件名を入力します。



ヒント

[件名 (Subject)] フィールドやメッセージ本文に入力パラメータを使用して、電子メール内にタイムスタンプや Defense Center の名前などの情報を動的に生成できます。詳細については、[入力パラメータの使用法 \(57-20 ページ\)](#) を参照してください。

手順 8 必要に応じて、電子メールの本文にカバレータを入力します。さまざまなフォント、番号リスト、箇条書きリストなどのリッチ テキスト機能を使用できます。

手順 9 [レポートの生成 (Generate Report)] ウィンドウのすべてのフィールドが正しい場合は、[OK] をクリックして確認します。

システムにより、生成されたレポートが電子メールで配布されます。システム ポリシーで、[電子メール通知 (Email Notification)] を利用して電子メールの送信元アドレスを設定できます。詳細については、[システム ポリシーの管理 \(63-1 ページ\)](#) を参照してください。

レポート用のリモート ストレージの使用法

ライセンス:任意 (Any)

新しく生成されたレポート ファイルを設定済みのリモート ストレージの場所に置くように、レポート作成システムを設定できます。ローカルに保存されたレポートを、リモート ストレージの場所に移動することもできます。



(注)

リモート ストレージ内のレポートを移動してローカル ストレージに戻すことはできません。

リモート ストレージを使用するには、まずリモート ストレージの場所を設定します。リモート ストレージの場所を設定すると、レポート リストの下部に表示されます。NFS および SMB がマウントされたストレージの場合、この場所には現在のディスク使用状況も示されますが、SSH の場合は示されません。設定情報については、[リモート ストレージの管理 \(64-17 ページ\)](#) を参照してください。

生成したレポートをリモートに保存する方法:

アクセス:Admin/Any Security Analyst

手順 1 [概要 (Overview)] > [レポート (Reporting)] を選択します。

手順 2 [レポート (Reports)] タブを選択します。

[レポート (Reports)] ページが表示されます。

手順 3 ページ下部の [レポートのリモート ストレージを有効にする (Enable Remote Storage of Reports)] チェック ボックスを選択します。

Defense Center により、新しく生成されたレポートが、ページの下部に示されているリモートの場所に保存されます。これらのレポートの [場所 (Location)] カラム データは、[リモート (Remote)] になります。

バッチ モードまたは単独で、ローカル ストレージ内のレポートをリモート ストレージの場所に移動できます。

生成したレポートをローカルストレージからリモートストレージに移動する方法:

アクセス: Admin/Any Security Analyst

手順 1 [概要 (Overview)] > [レポート (Reporting)] を選択します。

手順 2 [レポート (Reports)] タブを選択します。

[レポート (Reports)] ページが表示されます。

手順 3 移動するレポートの横にあるチェック ボックスを選択して、[移動 (Move)] をクリックします。



ヒント

ページ上のすべてのレポートを移動するには、そのページの左上にあるチェック ボックスを選択します。複数のレポートが複数のページにある場合は、2 つ目のチェック ボックスが表示され、すべてのページ上のすべてのレポートを移動するよう選択できます。

手順 4 レポートを移動することを確認します。

レポートが移動されます。

レポートテンプレートとレポートファイルの管理

ライセンス: 任意 (Any)

テンプレートの作成と編集に加えて、次のテンプレートの管理タスクを実行できます。

- [レポートテンプレートのエクスポートとインポート \(57-34 ページ\)](#)
- [レポートテンプレートの削除 \(57-36 ページ\)](#)

生成されたレポートファイルに対して次の管理タスクも実行できます。

- [レポートのダウンロード \(57-36 ページ\)](#)
- [レポートの削除 \(57-37 ページ\)](#)

レポートテンプレートのエクスポートとインポート

ライセンス: 任意 (Any)

レポートテンプレートをエクスポートする際に生成するファイルには、別の Defense Center で同じレポートを作成するのに必要なすべてのデータが含まれます。エクスポートファイルは独自の SFO 形式で、次のものが含まれます。

- レポートテンプレート、およびすべてのセクションの設計要素とドキュメント属性
- レポートで使用されるすべての保存済みの検索設定
- レポートで使用されるすべてのイメージ
- レポートで使用されるすべてのカスタム テーブル


別の Defense Center にテンプレートをインポートした後で必要になる可能性のある唯一の設定は、自動レポート生成スケジュールです。



(注) レポートテンプレートをインポートしたりエクスポートしたりするには、両方の Defense Center のソフトウェアバージョンレベルが同じである必要があります。

レポートテンプレートをエクスポートする方法:

アクセス:Admin

-
- 手順 1 [概要(Overview)]>[レポート(Reporting)]を選択します。
- 手順 2 [レポートテンプレート(Report Templates)]タブを選択します。
[レポートテンプレート(Report Templates)]ページが表示されます。
- 手順 3 エクスポートするテンプレートのエクスポートアイコン()をクリックします。
システムにより、拡張子が .sfo の設定パッケージファイルが作成され、[開いているオブジェクト(Opening Object)]ポップアップウィンドウが開いてパッケージのファイル名が表示されます。
- 手順 4 [ファイルの保存(Save file)]と [OK] を選択して、ローカルコンピュータにファイルを保存します。
- 手順 5 .sfo パッケージの名前を変更し、後で参考になるように説明的な名前にすることができます。パッケージ名にかかわらず、パッケージをインポートすると、インポート先の Defense Center では元の Defense Center と同じ名前がテンプレートに付けられます。
-

Defense Center からエクスポートされる SFO ファイルには、別の Defense Center にレポートテンプレートを追加するのに必要なすべての要素が含まれています。したがって、インポートプロセスに必要なのは、2 つ目の Defense Center にパッケージをアップロードすることと、インポートプロセスを実行することだけです。

レポートテンプレートをインポートする方法:

アクセス:Admin

-
- 手順 1 [システム(System)]>[ツール(Tools)]>[インポート/エクスポート(Import/Export)]を選択します。
[インポート/エクスポート(Import/Export)]ページが表示され、Defense Center 上のレポートテンプレートのリストが示されます。
- 手順 2 [パッケージのアップロード(Upload Package)]をクリックします。
[パッケージ名(Package Name)]ページが表示されます。
- 手順 3 次の 2 つの対処法があります。
- アップロードするパッケージへのパスを入力します。
 - [参照(Browse)]をクリックして、パッケージを見つけます。
- 手順 4 [アップロード(Upload)]をクリックします。
設定リストの [レポートテンプレート(Report Template)] セクションが表示され、インポートするテンプレートが示されます。
- 手順 5 テンプレートの横にあるチェックボックスを選択し、[インポート(Import)]をクリックします。
このテンプレートが、インポート先の Defense Center の設定のリストに表示されます。
-

レポートテンプレートの削除

ライセンス:任意(Any)

レポートテンプレートは、削除しない限り、再利用できるように [レポートテンプレート (Report Templates)] タブにリストされたままになります。シスコ提供のレポートテンプレートは削除できないことに注意してください。



(注) セキュリティアナリストは、自分が作成したレポートテンプレートだけを削除できます。

レポートテンプレートを削除する方法:

アクセス:Admin/Any Security Analyst

-
- 手順 1 [概要 (Overview)] > [レポート (Reporting)] を選択します。
- 手順 2 [レポートテンプレート (Report Templates)] タブを選択します。
[レポートテンプレート (Report Templates)] ページが表示されます。
- 手順 3 削除するテンプレートの隣にある削除アイコン(🗑️)をクリックして確認します。
テンプレート名がリストから削除されます。
-

レポートのダウンロード

ライセンス:任意(Any)

ローカルコンピュータにレポートファイルをダウンロードできます。そのコンピュータから、電子メールや他の使用可能な方法で電子的に配布できます。レポートを生成時に電子メールで自動的に配布することについて詳しくは、[レポートの生成時の電子メール配布 \(57-32 ページ\)](#)を参照してください。

レポートをダウンロードする方法:

アクセス:Admin/Any Security Analyst

-
- 手順 1 [概要 (Overview)] > [レポート (Reporting)] を選択します。
- 手順 2 [レポート (Reports)] タブを選択します。
[レポート (Reports)] ページが表示されます。
- 手順 3 ダウンロードするレポートの横にあるチェックボックスを選択し、[ダウンロード (Download)] をクリックします。



ヒント

ページ上のすべてのレポートをダウンロードするには、そのページの左上にあるチェックボックスを選択します。複数のレポートが複数のページにある場合は、2つ目のチェックボックスが表示され、すべてのページ上のすべてのレポートをダウンロードするよう選択できます。

- 手順 4 ブラウザのプロンプトに従って、レポートをダウンロードします。
複数のレポートを選択すると、1つの .zip ファイルでダウンロードされます。
-

レポートの削除

ライセンス:任意(Any)

レポートファイルはいつでも削除できます。この手順によりファイルが完全に削除され、リカバリ不能になります。レポートの生成に使用したレポートテンプレートがまだ残っていますが、時間枠を拡大したりスライドしたりした場合は、特定のレポートファイルを再生成するのが難しくなることがあります。時間枠の詳細については、[レポートテンプレートのセクションの編集 \(57-13 ページ\)](#)を参照してください。また、テンプレートで入力パラメータを使用した場合も、再生成するのが難しくなることがあります。入力パラメータの使用法の詳細については、[入力パラメータの使用法 \(57-20 ページ\)](#)を参照してください。

レポートを削除する方法:

アクセス:Admin/Any Security Analyst

-
- 手順 1 [概要(Overview)] > [レポート(Reporting)] を選択します。
 - 手順 2 [レポート(Reports)] タブを選択します。
[レポート(Reports)] ページが表示されます。
 - 手順 3 削除するレポートの隣のチェックボックスを選択し、[削除(Delete)] をクリックします。



ヒント ページ上のすべてのレポートを削除するには、そのページの左上にあるチェックボックスを選択します。複数のレポートが複数のページにある場合は、2つ目のチェックボックスが表示され、すべてのページ上のすべてのレポートを削除するよう選択できます。

-
- 手順 4 削除を確認します。
レポートが削除されます。
-

