設定のインポートおよびエクスポート

インポート / エクスポート機能を使用して、ポリシーを含む複数のタイプの設定を、1 つのアプライアンスから同じタイプの別のアプライアンスにコピーにできます。設定のインポートおよびエクスポートは、バックアップ ツールとして設計されてはいませんが、FireSIGHT システムに新しいアプライアンスを追加するプロセスを効率化するために使用できます。

以下の設定をインポートおよびエクスポートできます。

- アクセス コントロール ポリシー
- アラート応答
- アプリケーション ディテクタ
- カスタム テーブル
- カスタム ユーザ ロール
- カスタム ワークフロー
- ダッシュボード
- ヘルス ポリシー
- 侵入ポリシー
- レポート テンプレート
- 保存済み検索
- システム ポリシー
- サードパーティ製品マッピング
- サードパーティ脆弱性マッピング

エクスポートされた設定をインポートするには、両方のアプライアンスで同じバージョンの FireSIGHT システムが稼動していなければなりません。エクスポートされた侵入ポリシー（または侵入ポリシーが組み込まれているアクセス コントロール ポリシー）をインポートするには、両方のアプライアンスに同じバージョンのルール アップデートが適用されている必要もあります。

詳細については、次の項を参照してください。

- 「設定のエクスポート」（P.A-2）
- 「設定のインポート」（P.A-5）

設定のエクスポート

ライセンス：任意

単一の設定をエクスポートすることや、（同じタイプまたは異なるタイプの）一連の設定を同時にエクスポートすることができます。後に別のアプライアンスにパッケージをインポートするとき、パッケージ内のどの設定をインポートするかを選択できます。

設定をエクスポートするとき、アプライアンスは、その設定のリビジョン情報もエクスポートします。FireSIGHT システムはその情報を使用して、別のアプライアンスにその設定をインポートできるかどうかを判別します。アプライアンスにすでに存在する設定リビジョンをインポートすることはできません。

また、設定をエクスポートするとき、その設定が依存する認証オブジェクトなどのシステム設定も、アプライアンスによってエクスポートされます。たとえば、LDAP サーバへの認証を防御センターにセットアップしてから、認証を有効にして防御センターのシステム ポリシーをエクスポートする場合、認証オブジェクトも同様にエクスポートされます。

ヒント　FireSIGHT システムの多くのリスト ページ には、リスト項目の横にエクスポート アイコン（ ）があります。このアイコンがある場合は、それを使用することにより、その後のエクスポート操作を簡単に代行させることができます。

以下の設定をエクスポートできます。

- *アラート応答*：アラート応答は、アラートの送信先とする予定の外部システムと FireSIGHT システムが対話できるようにするための一連の設定です。
- *カスタム テーブル*：カスタム テーブルは、FireSIGHT システムに付属している事前定義された複数のテーブルのフィールドを結合する、構築可能なテーブルです。
- *カスタム ユーザ ロール*：カスタム ユーザ ロールは、専用のアクセス権限セットを持つ、ユーザが作成するユーザ ロールです。保存済み検索を必要とするカスタム ユーザ ロールをエクスポートすると、必要なすべての保存済み検索もエクスポートされます。
- *カスタム ワークフロー*：カスタム ワークフローは、組織の固有のニーズを満たすためにユーザが作成するワークフローです。防御センターでは、作成したカスタム ワークフロー、およびアプライアンスに付属の事前定義されたカスタム ワークフローをエクスポートできます。

  エクスポートされたカスタム ワークフローの基礎となるテーブルを防御センターで表示できない場合、ワークフローをインポートすることはできますが、それを表示できないことに注意してください。
- *ダッシュボード*：ダッシュボードは、現在のシステム ステータスの概要を表示する、カスタマイズ可能なタブ付きのビューです。ダッシュボードは、さまざまなウィジェットを使用して、FireSIGHT システムで収集されたイベントや生成されたイベントに関するデータ、および展開に含まれるアプライアンスの状態と全体的な正常性に関する情報を表示します。

  自分が表示できるダッシュボードは、使用しているアプライアンスのタイプ、および自分のユーザ ロールによって異なることに注意してください。詳細については、「ウィジェットの可用性について」（P.3-5）を参照してください。
- *アクセス コントロール ポリシー*：アクセス コントロール ポリシーには、システムがネットワーク トラフィックをどのように管理するかを指定するために設定できる、さまざまなコンポーネントが含まれます。これらのコンポーネントには、アクセス コントロール ルールとそのルールが使用するオブジェクトが含まれ、参照先の侵入ポリシーとファイル ポリシーが含まれることもあります。アクセス コントロール ポリシーをエクスポートすると、

そのポリシーのすべての設定とコンポーネントもエクスポートされます。ただし、複数のアプライアンスで同等であり、ユーザが変更できない URL レピュテーションとカテゴリは（それらが存在しても）エクスポートされません。

エクスポートするアクセス コントロール ポリシーに侵入ポリシーが含まれる場合は、エクスポート元とインポート先のアプライアンスに同じバージョンのルール アップデートが適用されている必要があります。

エクスポートするアクセス ポリシーに位置情報データを参照するルールが含まれる場合、インポート先の防御センターの位置情報データベース（GeoDB）のアップデート バージョンが使用されます。

エクスポートするアクセス コントロール ポリシーが、サポートされていない DC500 や、シリーズ 2 のデバイス ポリシー機能またはルール条件を参照している場合、DC 500 を使用してポリシーを適用することも、ポリシーをシリーズ 2 デバイスに適用することもできません。DC500 も シリーズ 2 デバイスも、マルウェア ブロック アクションやマルウェア クラウド ルックアップ アクションを使用するルールの含まれる、ユーザまたは URL のルール条件、セキュリティ インテリジェンス、ファイル ポリシーをサポートしません。さらに、シリーズ 2 デバイスはアプリケーション ルール条件をサポートしません。

- *ヘルス ポリシー*：ヘルス ポリシーは、展開内でのアプライアンスの正常性、つまりシスコのハードウェアとソフトウェアが正しく動作しているかどうかを検査する際に使用する基準で構成されます。
- *侵入ポリシー*：侵入ポリシーには、ネットワーク トラフィックを検査して侵入やポリシー違反を見つけるように設定できる、さまざまなコンポーネントが組み込まれています。これらのコンポーネントには、プリプロセッサ、侵入ルール（プロトコル 見出し値、ペイロードの内容、および特定のパケット サイズ特性を検査する）、適応型プロファイルの設定、FireSIGHT の推奨ルール設定、およびイベントのログ記録と表示の頻度を制御するためのツールが含まれます。

  侵入ポリシーをエクスポートすると、そのポリシーのすべての設定もエクスポートされます。たとえば、イベントを生成するルールを設定するように選択した場合、ルールの SNMP アラートを設定した場合、ポリシーで SMTP プリプロセッサをオンにした場合は、エクスポートされるポリシー内にそれらの設定値が保持されます。カスタム ルール、カスタム ルールの分類、およびユーザ定義変数も、ポリシーと共にエクスポートされます。

  レイヤを使用する侵入ポリシーをエクスポートする場合、そのレイヤが 2 番目の侵入ポリシーによって共有されているときは、エクスポートするポリシーにその共有レイヤがコピーされて、共有関係はなくなることに注意してください。侵入ポリシーを別のアプライアンスにインポートするときは、インポートするポリシーをニーズに合うように編集できます。レイヤの削除、追加、共有などができます。

  1 つの防御センターから別の防御センターに侵入ポリシーをエクスポートする場合、2 つ目の防御センターでデフォルト変数が別の設定になっている場合は、インポートされたポリシーの動作が異なる可能性があります。

（注）　インポート / エクスポート機能を使用して、シスコの脆弱性調査チーム（VRT）が作成したルールをアップデートすることはできません。代わりに、最新バージョンのルール アップデートをダウンロードして適用します。「ルールの更新とローカル ルール ファイルのインポート」（P.53-16）を参照してください。

- *レポート テンプレート*：レポートは、特定の FireSIGHT システムのデータを照合する、PDF、HTML、または CSV 形式のドキュメント ファイルです。レポート テンプレートは、レポートとそのセクション用にデータの検索と形式を指定します。レポート テンプレートをエクスポートすると、すべての保存済み検索、画像、ネットワーク オブジェクト、オブジェクト マネージャで作成されたオブジェクト、およびレポートに必要なカスタム テーブルもエクスポートされます。
- *保存済み検索*：保存済み検索は、アクセス許可の制限されたユーザが、事前定義された FireSIGHT システム データにアクセスできるようにします。保存済み検索を必要とするカスタム ユーザ ロールをエクスポートすると、必要な保存済み検索もエクスポートされます。また、個別のユーザ定義の保存済み検索もエクスポートできます。
- *システム ポリシー*：システム ポリシーは、データベース イベント制限、時間設定、ログイン バナーなど、展開内の他の FireSIGHT システム アプライアンスに類似する可能性のあるアプライアンスの局面を制御します。

  エクスポートするシステム ポリシーで外部認証が有効の場合、関連する認証オブジェクトもエクスポートされます。

  防御センターのシステム ポリシーには、管理対象デバイスに適用されないデータベース設定が含まれることに注意してください。システム ポリシーを管理対象デバイスからエクスポートした後に防御センターにインポートする場合、デバイスでは設定できなかったデータベース制限が、防御センターではデフォルト値に設定されます。
- *サードパーティ製品マッピング*：サードパーティ アプリケーションからデータをインポートする場合、そのデータを使用して脆弱性を割り当てたり、影響の関連付けを行ったりするために、製品をサードパーティの名前にマッピングする必要があります。製品をマッピングすることにより、シスコの脆弱性情報をサードパーティ製品の名前に関連付けます。これにより、FireSIGHT システムはそのデータを使用して、影響の関連付けを実行できます。サードパーティ製品マッピングを作成する方法について詳しくは、「サードパーティ製品のマッピング」（P.42-34）を参照してください。
- *サードパーティ脆弱性マッピング*：サードパーティ アプリケーションから脆弱性データベースに脆弱性情報を追加するには、インポートしたそれぞれの脆弱性のサードパーティ識別文字列を、既存のシスコ、Bugtraq、または Snort の ID にマッピングする必要があります。脆弱性のマッピングを作成したら、マッピングはネットワーク マップのホストにインポートされたすべての脆弱性に対して機能し、それらの脆弱性に対する影響の関連付けを可能にします。サードパーティ脆弱性マッピングを作成する方法について詳しくは、「サードパーティの脆弱性のマッピング」（P.42-36）を参照してください。
- *アプリケーション ディテクタ*：システムは IP トラフィックを分析するとき、ディテクタを使用して関連情報を収集してから、ネットワークのホストで一般的に使用されるアプリケーションを識別します。2 種類のディテクタをエクスポートできます。それらは、ユーザ定義のディテクタとシスコ Professional サービスが提供する個別のアドオン ディテクタです。ディテクタについて詳しくは、「アプリケーション ディテクタの使用」（P.42-18）を参照してください。

（注）　エクスポートされる設定の数や、それらのオブジェクトが参照する設定の数によっては、エクスポート プロセスに数分かかる場合があります。

一つ以上の設定をエクスポートする方法：

アクセス：Admin

ステップ 1　設定のエクスポート元のアプライアンスと設定のインポート先のアプライアンスで、同じバージョンの FireSIGHT システムが稼働していることを確認します。侵入ポリシー（または侵入ポリシーが組み込まれたアクセス コントロール ポリシー）をエクスポートする場合、ルールのアップデート バージョンが一致することも確認する必要があります。

FireSIGHT システムのバージョン（および該当する場合はルールのアップデート バージョン）が一致しない場合、インポートは失敗します。

ステップ 2　[Systems] > [Tools] > [Import/Export] を選択します。

[Import/Export] ページが表示され、アプライアンス上の設定のリストが示されます。エクスポートする設定がない設定カテゴリは、このリストに表示されないことに注意してください。

ヒント　設定のリストは、設定タイプの横にある折りたたみアイコン（）をクリックして折りたたむことができます。設定を確認するには、設定タイプの横にあるフォルダ展開アイコン（）をクリックします。

ステップ 3　エクスポートする設定の横にあるチェック ボックスを選択して、[Export] をクリックします。

ステップ 4　Web ブラウザのプロンプトに従って、エクスポートされたパッケージをコンピュータに保存します。

設定のインポート

ライセンス：任意

アプライアンスから設定をエクスポートした後に、その設定が別のアプライアンスでもサポートされていれば、そのアプライアンスにインポートできます。ただし、使用するアプライアンスのタイプやユーザ ロールによっては、一部のインポートされた設定が役立たない場合があることに注意してください。

インポートしている設定のタイプに応じて、以下の点に注意する必要があります。

- 設定をインポートするアプライアンスが、設定のエクスポートに使用したアプライアンスと、同じバージョンの FireSIGHT システムを実行していることを確認します。エクスポートされた侵入ポリシー（または侵入ポリシーが組み込まれているアクセス コントロール ポリシー）をインポートする場合、両方のアプライアンスに同じバージョンのルール アップデートが適用されている必要もあります。バージョンが一致しない場合、インポートは失敗します。
- 保存済み検索を必要とするカスタム ユーザ ロールをインポートすると、必要な保存済み検索もインポートされます。
- 表示できるダッシュボード ウィジェットは、使用しているアプライアンスのタイプと、自分のユーザ ロールによって異なります。たとえば、防御センターで作成され、管理対象デバイスにインポートされるダッシュボードは、無効なウィジェットを表示する場合があります。

- ゾーンに基づいてトラフィックを評価するアクセス コントロール ポリシーをインポートした場合、インポートされたポリシー内のゾーンを、インポート先の防御センターによって管理されるデバイスのゾーンにマッピングする必要があります。ゾーンをマッピングするときは、それらのタイプが一致している必要があります。したがって、インポートを開始する前に、インポート先の防御センターで必要となるゾーン タイプを作成する必要があります。セキュリティ ゾーンについて詳しくは、「セキュリティ ゾーンの操作」（P.5-43）を参照してください。
- 既存のオブジェクトやグループと同一の名前を持つオブジェクトやオブジェクト グループを含むアクセス コントロール ポリシーまたは保存済み検索をインポートする場合は、オブジェクトやグループの名前を変更する必要があります。
- アクセス コントロール ポリシーや侵入ポリシーをインポートする場合、インポート プロセスによって、デフォルト変数セットに含まれる既存のデフォルト変数が、インポートされたデフォルト変数に置換されます。既存のデフォルト変数セットに、インポートされたカスタム変数セットに存在しないカスタム変数が含まれる場合、一意的な変数が保持されます。
- 侵入ポリシーをインポートするとき、その侵入ポリシーが 2 番目の侵入ポリシーの共有レイヤを使用していた場合は、エクスポート プロセスによって共有関係が切断されて、それまで共有されていたレイヤがパッケージにコピーされます。つまり、インポートされた侵入ポリシーに共有レイヤは含まれません。

（注）　インポート / エクスポート機能を使用して、シスコの脆弱性調査チーム（VRT）が作成したルールをアップデートすることはできません。代わりに、最新バージョンのルール アップデートをダウンロードして適用します。「ルールの更新とローカル ルール ファイルのインポート」（P.53-16）を参照してください。

- 外部認証が有効になっている防御センターからエクスポートされたシステム ポリシーをインポートするときは、そのシステム ポリシーが依存する認証オブジェクトもインポートします。

1 つのパッケージで複数の設定をエクスポートできるため、パッケージのインポート時に、パッケージ内のどの設定をインポートするかを選択する必要があります。インポート先のアプライアンスでサポートされる設定だけがインポート可能です。

設定をインポートしようとすると、アプライアンスは、その設定がアプライアンスにすでに存在しているかどうかを判別します。競合がある場合は、以下の操作が可能です。

- 既存の設定を維持する、
- 既存の設定を新しい設定に置き換える、
- 最新の設定を維持する、または
- 設定を新しい設定としてインポートする。

設定をインポートした後に、宛先システムで設定を変更してその設定を再インポートすると、保持する設定のバージョンを選択する必要があります。

インポートされる設定の数や、それらのオブジェクトが参照する設定の数によっては、プロセスに数分かかる場合があります。

インポートした設定の使用方法について詳しくは、以下の項を参照してください。

- 「アラート応答の使用」（P.15-2）
- 「カスタム テーブルの使用」（P.46-1）
- 「カスタム ユーザ ロールの管理」（P.48-55）

- 「カスタムワークフローの使用」（P.47-44）
- 「ダッシュボードの操作」（P.3-39）
- 「アクセス コントロール ポリシーの適用」（P.13-39）
- 「正常性ポリシーの適用」（P.55-32）
- 「侵入ポリシーの管理」（P.20-4）
- 「レポート テンプレートのエクスポートとインポート」（P.44-34）
- 「保存済み検索設定のロード」（P.45-3）
- 「システム ポリシーの適用」（P.50-4）
- 「サードパーティ製品のマッピング」（P.42-34）
- 「サードパーティの脆弱性のマッピング」（P.42-36）
- 「ディテクタのアクティブ化と非アクティブ化」（P.42-30）

一つ以上の設定をインポートする方法：

アクセス：Admin

ステップ 1　設定のエクスポート元のアプライアンスと設定のインポート先のアプライアンスで、同じバージョンの FireSIGHT システムが稼働していることを確認します。侵入ポリシー（または侵入ポリシーが組み込まれたアクセス コントロール ポリシー）をインポートする場合、ルールのアップデート バージョンが一致することも確認する必要があります。

FireSIGHT システムのバージョン（および該当する場合はルールのアップデート バージョン）が一致しない場合、インポートは失敗します。

ステップ 2　インポートする設定をエクスポートします。「設定のエクスポート」（P.A-2）を参照してください。

ステップ 3　設定をインポートするアプライアンスで、[System] > [Tools] > [Import/Export] を選択します。

[Import/Export] ページが表示されます。

ヒント　設定のリストを折りたたむには、設定タイプの横にある折りたたみアイコン（）をクリックします。設定を確認するには、設定タイプの横にあるフォルダ展開アイコン（）をクリックします。

ステップ 4　[Upload Package] をクリックします。

[Upload Package] ページが表示されます。

ステップ 5　次の 2 つのオプションから選択できます。

- アップロードするパッケージのパスを入力します。
- [Browse] をクリックして参照し、パッケージを見つけます。

ステップ 6　[Upload] をクリックします。

アップロードの結果は、パッケージの内容によって異なります。

- パッケージ内の設定が、アプライアンスにすでに存在するバージョンと正確に一致する場合、そのバージョンが存在することを示すメッセージが表示されます。アプライアンスに最新の設定が存在するので、それらをインポートする必要はありません。

- 使用するアプライアンスとパッケージのエクスポート元のアプライアンスとの間に、FireSIGHT システムまたは（該当する場合）ルール アップデートのバージョンの不一致がある場合、パッケージをインポートできないことを示すメッセージが表示されます。FireSIGHT システムまたはルール アップデートのバージョンを更新して、プロセスを再試行します。
- アプライアンスに存在しない設定やルールのバージョンがパッケージに含まれている場合、[Package Import] ページが表示されます。次の手順に進んでください。

ステップ 7　インポートする設定を選択して、[Import] をクリックします。

インポート プロセスが解決されて、以下のような結果になります。

- アプライアンスに、インポートする設定の以前のリビジョンが存在しない場合でも、インポートは自動的に完了し、成功メッセージが表示されます。残りの手順は省略してください。
- セキュリティ ゾーンを含むアクセス コントロール ポリシーをインポートする場合、[Access Control Import Resolution] ページが表示されます。手順 8 に進みます。
- インポートする設定に対してアプライアンスに以前のリビジョンが存在する場合、[Import Resolution] ページが表示されます。手順 9 に進みます。

ステップ 8　取り込まれる各セキュリティ ゾーンの横で、同じタイプの既存のローカル セキュリティ ゾーンをマップ先として選択し、[Import] をクリックします。

手順 7 に戻ります。

ステップ 9　各設定を展開して、以下の該当するオプションを選択します。

- アプライアンスの設定を保持するには、[Keep existing] を選択します。
- アプライアンスの設定をインポートした設定に置き換えるには、[Replace existing] を選択します。
- 最新の設定を保持するには、[Keep newest] を選択します。
- インポートした設定を新しい設定として保存するには、[Import as new] を選択し、オプションとして設定名を編集します。

  クリーン リストまたはカスタム検出リストが有効になっているファイル ポリシーを含むアクセス コントロール ポリシーをインポートする場合、[Import as new] オプションは使用できません。
- 従属オブジェクトを含むアクセス コントロール ポリシーや保存済み検索をインポートする場合、提案された名前を受け入れるか、またはオブジェクトの名前を変更します。システムは常にこれらの従属オブジェクトを新規としてインポートします。既存のオブジェクトを保存したり置き換えたりするオプションはありません。システムではオブジェクトもオブジェクト グループも同様に処理されることに注意してください。

ステップ 10　[Import] をクリックします。

設定がインポートされます。