バックアップと復元の使用

バックアップ/復元は、システム保守プランの重要な部分です。各組織のバックアップ計画は高度に個別化されていますが、FireSIGHT システムには、障害発生時に防御センターや管理対象デバイスを復元できるようにデータをアーカイブするためのメカニズムが備わっています。バックアップはそれを作成した製品バージョンでのみ有効であり、仮想管理対象デバイスや Sourcefire Software for X-Series では、バックアップ ファイルを作成または復元できないことに注意してください。

代替のアプライアンスにバックアップを復元できるのは、2 台のアプライアンスが同じモデルで、同じバージョンの FireSIGHT システム ソフトウェアを実行している場合です。

注意 管理対象デバイス間でコンフィギュレーション ファイルをコピーする目的で、バックアップと復元のプロセスを使用しないでください。コンフィギュレーション ファイルはデバイスを固有に識別する情報を含むため、共有できません。

デフォルトでは、システム コンフィギュレーション ファイルはバックアップ ファイルに保存されます。また、イベント データをバックアップすることも選択できます。アプライアンスに保存されているキャプチャされたファイルは、バックアップできません。

注意 侵入ルールのアップデートを適用した場合、それらのアップデートはバックアップされません。復元**後に**、最新のルールのアップデートを適用する必要があります。

アプライアンスまたはローカル コンピュータにバックアップ ファイルを保存できます。さらに、防御センターを使用している場合は、「リモート ストレージの管理」（P.51-15）で詳述されているように、リモート ストレージを使用できます。

注意 3D9900 上の USB ポートに USB ドライブを挿入しないでください。また、デバイスをアップグレードまたは復元する前に、外部ストレージのあるデバイス（外部ストレージがある KVM スイッチなど）を 3D9900 から削除します。

詳細については、次の項を参照してください。

- アプライアンスのファイルをバックアップする方法について詳しくは、「バックアップ ファイルの作成」（P.57-2）を参照してください。
- バックアップ作成のテンプレートとして後で使用できるバックアップ プロファイルを作成する方法について詳しくは、「バックアップ プロファイルの作成」（P.57-4）を参照してください。

- 防御センターを使用して管理対象デバイスをバックアップする方法について詳しくは、「防御センターによる管理対象デバイスのバックアップ」（P.57-5）を参照してください。
- ローカル ホストからバックアップ ファイルをアップロードする方法について詳しくは、「ローカル ホストからのバックアップのアップロード」（P.57-6）を参照してください。
- アプライアンスにバックアップ ファイルを復元する方法について詳しくは、「バックアップ ファイルからのアプライアンスの復元」（P.57-6）を参照してください。

バックアップ ファイルの作成

ライセンス：任意

既存のシステム バックアップを表示して使用するには、[Backup Management] ページに移動します。イベントやパケット データに加えて、アプライアンスの復元に必要なすべてのコンフィギュレーション ファイルを含むバックアップ ファイルを定期的に保存する必要があります。設定の変更をテストする際にも、システムをバックアップして、必要に応じて保存されている設定に戻せるようにすることができます。バックアップ ファイルに、キャプチャされたファイルを含めることはできないことに注意してください。バックアップ ファイルを、アプライアンスに保存するか、ローカル コンピュータに保存するかを選択できます。

注意　アプライアンスに十分なディスク スペースがない場合は、バックアップ ファイルを作成できません。バックアップ プロセスが使用可能なディスク スペースの 85% 以上を使用する場合、バックアップは失敗することがあります。必要に応じて、古いバックアップ ファイルを削除するか、古いバックアップ ファイルをアプライアンスの外部に転送するか、リモート ストレージを使用してください。

あるいは、バックアップ ファイルが 4GB を超える場合は、SCP 経由でリモート ホストにコピーします。4 GB よりも大きなファイルのアップロードは、Web ブラウザでサポートされていないため、バックアップ ファイルがそのように大きい場合には、ローカル コンピュータからのバックアップのアップロードはできません。防御センターでは、バックアップ ファイルをリモート ロケーションに保存できます。詳しくは、「リモート ストレージの管理」（P.51-15）を参照してください。

注　バックアップ タスクがディスカバリ イベントを収集してるとき、データの関連付けは一時的に停止されます。

バックアップを実行してから確認済みの侵入イベントを削除した場合、そのバックアップによって、削除された侵入イベントは復元されますが確認済みのステータスは復元されません。復元されたそれらの侵入イベントは、[Reviewed Events] の下ではなく [Intrusion Events] の下に表示されます。「侵入イベントについて」（P.18-14）を参照してください。

侵入イベントのデータを含むバックアップを、そのデータがすでに含まれているアプライアンスに復元すると、重複したイベントが作成されることになります。これを回避するため、以前の侵入イベント データが含まれていないアプライアンスにのみ、侵入イベント バックアップを復元します。

注意　セキュリティ ゾーンとのインターフェイスのアソシエーションを設定してある場合、それらのアソシエーションはバックアップされません。それらは、復元後に再設定する必要があります。詳細については、「セキュリティ ゾーンの操作」（P.5-43）を参照してください。

管理対象デバイスをデバイス自体からバックアップするときは、設定のみをバックアップします。完全なバックアップを実行するには、物理デバイスを管理する防御センターを使用します。

バックアップ ファイルの作成方法：

アクセス：Admin/Maint

ステップ 1　[System] > [Tools] > [Backup]/[Restore] を選択します。

[Backup Management] ページが表示されます。

ステップ 2　[Managed Device Backup] または [防御センター Backup] をクリックします。

[Create Backup] ページが表示されます。

ステップ 3　[Name] フィールドに、バックアップ ファイルの名前を入力します。英数字、句読記号、およびスペースを使用できます。

ステップ 4　防御センターには、さらに以下の 2 つのオプションがあります。

- 設定をアーカイブするには、[Back Up Configuration] を選択します。
- イベント データベース全体をアーカイブするには、[Back Up Events] を選択します。

ステップ 5　オプションで、バックアップの完了時に通知を受けるためには、[Email when complete] チェックボックスをオンにして、用意されているテキスト ボックスに電子メール アドレスを入力します。

注　電子メール通知を受信するには、「メール リレー ホストおよび通知アドレスの設定」（P.50-19）で説明されているように、リレー ホストを設定する必要があります。

ステップ 6　オプションで、防御センターで、セキュアなコピー（SCP）を使用してバックアップ アーカイブを異なるマシンにコピーするには、[Copy when complete] チェック ボックスをオンにしてから、用意されているテキスト ボックスに以下の情報を入力します。

- [Host] フィールドに、バックアップのコピー先となるマシンのホスト名または IP アドレス
- [Path] フィールドに、バックアップのコピー先となるディレクトリへのパス
- [User] フィールドに、リモート マシンへのログインに使用するユーザ名
- [Password] フィールドに、そのユーザ名のパスワード
  パスワードの代わりに SSH 公開キーを使用してリモート マシンにアクセスする場合は、[SSH Public Key] フィールドの内容を、そのマシンの指定ユーザの `authorized_keys` ファイルにコピーします。

このオプションをオフにする場合、バックアップ中に使用された一時ファイルがシステムによってリモート サーバに保存されます。このオプションをオンにする場合は、一時ファイルはリモート サーバに保存されません。

ヒント　シスコは、システム障害が発生した場合にアプライアンスを復元できるように、バックアップをリモート ロケーションに定期的に保存することを推奨します。

ステップ 7　次の選択肢があります。

- バックアップ ファイルをアプライアンスに保存するには、[Start Backup] をクリックします。

  バックアップ ファイルは `/var/sf/backup` ディレクトリに保存されます。防御センターでは、リモート ロケーションをバックアップ ファイルの場所として指定できます。「リモート ストレージの管理」（P.51-15）を参照してください。

バックアップ プロセスが完了すると、[Restoration Database] ページでファイルを参照できます。バックアップ ファイルを復元する方法について詳しくは、「バックアップ ファイルからのアプライアンスの復元」（P.57-6）を参照してください。

- この設定を後で使用できるバックアップ プロファイルとして保存するには、[Save as New] をクリックします。

  [System] > [Tools] > [Backup]/[Restore] を選択してから [Backup Profiles] をクリックすることにより、バックアップ プロファイルを変更または削除できます。詳細については、「バックアップ プロファイルの作成」（P.57-4）を参照してください。

バックアップ プロファイルの作成

ライセンス：任意

[Backup Profiles] ページを使用して、さまざまな種類のバックアップに使用する設定値を含むバックアップ プロファイルを作成できます。後にアプライアンスのファイルをバックアップするときに、これらのプロファイルの 1 つを選択できます。

ヒント　「バックアップ ファイルの作成」（P.57-2）で説明されているようにバックアップ ファイルを作成すると、バックアップ プロファイルが自動的に作成されます。

バックアップ プロファイルの作成方法：

アクセス：Admin/Maint

ステップ 1　[System] > [Tools] > [Backup]/[Restore] を選択します。

[Backup Management] ページが表示されます。

ステップ 2　[Backup Profiles] タブをクリックします。

[Backup Profiles] ページが表示されて、既存のバックアップ プロファイルのリストが示されます。

ヒント　編集アイコン（）をクリックして既存のプロファイルを変更するか、または削除アイコン（）をクリックしてリストからプロファイルを削除することができます。

ステップ 3　[Create Profile] をクリックします。

[Create Backup] ページが表示されます。

ステップ 4　バックアップ プロファイルの名前を入力します。英数字、句読記号、およびスペースを使用できます。

ステップ 5　バックアップ プロファイルを必要に合わせて設定します。

このページのオプションについて詳しくは、「バックアップ ファイルの作成」（P.57-2）を参照してください。

ステップ 6　バックアップ プロファイルを保存するには、[Save as New] をクリックします。

[Backup Profiles] ページが表示されて、新しいプロファイルがリストに示されます。

防御センターによる管理対象デバイスのバックアップ

ライセンス：任意

防御センターを使用して管理対象デバイス上のデータをバックアップできます。バックアップ ファイルのデフォルト名には、管理対象デバイスの名前が使用されます。

ヒント　使用するバックアップ ファイル名にスペースや句読文字が含まれる場合、それらは下線に変更されます。

Sourcefire Software for X-Series のデータを管理するために、リモート バックアップと復元を実行することは**できません**。

防御センターから管理対象デバイスをバックアップするには、次のようにします。

アクセス：Admin/Maint

ステップ 1　[System] > [Tools] > [Backup]/[Restore] を選択します。

[Backup Management] ページが表示されます。

ステップ 2　[Managed Device Backup] をクリックします。

[Managed Device Backup] ページが表示されます。

ステップ 3　[Managed Devices] フィールドで、バックアップする管理対象デバイスを選択します。

ステップ 4　設定データと共にイベント データも含めるには、[Include All Unified Files] チェック ボックスをオンにします。統合ファイルは、FireSIGHT システムがイベント データをログに記録するために使用するバイナリ ファイルであることに注意してください。

ステップ 5　バックアップ ファイルを防御センターに保存するには、[Retrieve to Defense Center] チェック ボックスをオンにします。各デバイスのバックアップ ファイルをそのデバイス自体に保存するには、このチェック ボックスをオフにしておいてください。

注　[Retrieve to Defense Center] を選択した場合、防御センターがバックアップのリモート ストレージ用に設定されていれば、デバイスのバックアップ ファイルは防御センター自体ではなく設定されたリモート ロケーションに保存されます。

ステップ 6　[Start Backup] をクリックします。

成功を示すメッセージが表示されて、バックアップ タスクが作成されます。

バックアップの完了までに数分かかる場合があります。その進行状況は、[Task Status] ページ（[System] > [Monitoring] > [Task Status]）で監視できます。バックアップが完了すると、[Backup Management] ページにバックアップ ファイルが表示されます。

ローカル ホストからのバックアップのアップロード

ライセンス：任意

「バックアップ管理」の表で説明されているダウンロード機能を使用してローカル ホストにバックアップ ファイルをダウンロードした場合、それを防御センターにアップロードできます。

ヒント　4 GB よりも大きなファイルのアップロードは Web ブラウザでサポートされていないため、そのように大きなサイズのバックアップをローカル コンピュータからアップロードすることはできません。代わりに、バックアップを SCP 経由でリモート ホストにコピーし、そこから取得することができます。防御センターでは、バックアップ ファイルをリモート ロケーションに保存し、そこから取得できます。「リモート ストレージの管理」（P.51-15）を参照してください。

ローカル ホストからバックアップをアップロードする方法：

アクセス：Admin/Maint

ステップ 1　[System] > [Tools] > [Backup]/[Restore] を選択します。

[Backup Management] ページが表示されます。

ステップ 2　[Upload Backup] をクリックします。

[Upload Backup] ページが表示されます。

ステップ 3　[Browse] をクリックして、アップロードするバックアップ ファイルに移動します。

アップロードするファイルを選択した後に、[Upload Backup] をクリックします。

ステップ 4　[Backup Management] をクリックして、[Backup Management] ページに戻ります。

バックアップ ファイルがアップロードされ、バックアップ リストに表示されます。防御センター アプライアンスによってファイルの整合性が検証された後に、[Backup Management] ページを更新して、詳細なファイル システム情報を確認します。

バックアップ ファイルからのアプライアンスの復元

ライセンス：任意

[Backup Management] ページを使用して、バックアップ ファイルからアプライアンスを復元できます。バックアップを復元するには、バックアップ ファイル内の VDB のバージョンが、アプライアンスの現在の VDB のバージョンと一致している必要があります。復元プロセスが完了した後、最新のシスコ ルール アップデートを適用する**必要があります**。

注意　仮想防御センターで作成されたバックアップを物理防御センターに復元しないでください。これはシステム リソースに負荷をかける可能性があります。仮想バックアップを物理防御センターに復元する必要がある場合は、サポートに連絡してください。

ローカル ストレージを使用する場合、バックアップ ファイルは /var/sf/backup に保存されて、/var パーティションで使用されているディスク領域量と共に [Backup Management] ページの下部にリストされます。防御センターで、[Backup Management] ページの上部にある [Remote Storage] を選択して、リモート ストレージ オプションを設定します。その後、リモート ストレージを有効にするために、[Backup Management] ページの [Enable Remote Storage for Backups] チェック ボックスをオンします。リモート ストレージを使用している場合は、プロトコル、バックアップ システム、およびバックアップ ディレクトリがページの下部に表示されます。

注　バックアップが完了した後にライセンスを追加した場合は、このバックアップを復元するときに、それらのライセンスが削除されたり上書きされたりすることはありません。復元の際の競合を防止するためにも、バックアップを復元する前に、これらのライセンスを（それらが使用されている場所をメモした上で）削除し、バックアップを復元した後で、追加して再設定してください。競合が発生した場合は、サポートに連絡してください。

次の表では、[Backup Management] ページの各列とアイコンについて説明します。

表 57-1　バックアップ管理

機能	説明
System Information	元のアプライアンスの名前、タイプ、バージョン。バックアップを復元できるのは、同一のアプライアンス タイプとバージョンに対してだけであることに注意してください。
Date Created	バックアップ ファイルが作成された日時
File Name	バックアップ ファイルのフルネーム
VDB Version	バックアップ時にアプライアンスで実行されている脆弱性データベース（VDB）のビルド。
Location	バックアップ ファイルの場所
Size (MB)	バックアップ ファイルのサイズ（メガバイト）
Event	[Yes] は、バックアップにイベント データが含まれていることを示します
View	バックアップ ファイルの名前をクリックすると、圧縮されたバックアップ ファイルに含まれるファイルのリストが表示されます。
Restore	バックアップ ファイルが選択された状態でクリックすると、そのバックアップ ファイルがアプライアンスに復元されます。VDB バージョンがバックアップ ファイルの VDB のバージョンと一致しない場合、このオプションは無効になります。
Download	バックアップ ファイルが選択された状態でクリックすると、そのバックアップ ファイルがローカル コンピュータに保存されます。
Delete	バックアップ ファイルが選択された状態でクリックすると、そのバックアップ ファイルが削除されます。
Move	防御センターで、以前に作成したローカル バックアップが選択された状態でクリックすると、そのバックアップが指定のリモート バックアップ ロケーションに送信されます。

バックアップ ファイルからのアプライアンスの復元方法：

アクセス：Admin

ステップ 1　[System] > [Tools] > [Backup]/[Restore] を選択します。

[Backup Management] ページが表示されます。

ステップ 2　バック アップ ファイルの内容を確認するには、ファイルの名前をクリックします。

マニフェストが表示され、各ファイルの名前、所有者と権限、およびファイル サイズと日付がリストされます。

ステップ 3　[Backup Management] をクリックして、[Backup Management] ページに戻ります。

ステップ 4　復元するバックアップ ファイルを選択して、[Restore] クリックします。

[Restore Backup]ページが表示されます。

バックアップの VDB バージョンがアプライアンスに現在インストールされている VDB のバージョンと一致しない場合、[Restore] ボタンはグレー表示されることに注意してください。

注意　この手順により、すべてのコンフィギュレーション ファイルが上書きされ、管理対象デバイスでは、すべてのイベント データが上書きされます。

ステップ 5　ファイルを復元するには、次のいずれかまたは両方を選択します。

- **Replace Configuration Data**
- **Restore Event Data**

注　管理対象デバイスの設定をバックアップ ファイルから復元すると、デバイスの管理用の防御センターから行われたデバイス設定の変更も復元されることに注意してください。復元される変更には、そのバックアップ ファイルを作成した後に行った変更も含まれます。

ステップ 6　[Restore] クリックして、復元を開始します。

アプライアンスが、指定したバックアップ ファイルを使用して復元されます。

ステップ 7　アプライアンスをリブートします。

ステップ 8　最新のシスコ ルール アップデートを適用して、ルールのアップデートを再適用します。

ステップ 9　復元されたシステムにアクセス コントロール ポリシー、侵入ポリシー、ネットワーク検出ポリシー、ヘルス ポリシー、システム ポリシーを再適用します。