



バックアップと復元

次のトピックでは、Firepower システムでバックアップおよび復元機能を使用する方法について説明します。

- [バックアップと復元の概要 \(1 ページ\)](#)
- [バックアップと復元に関する制限事項 \(1 ページ\)](#)
- [バックアップ ファイル \(3 ページ\)](#)
- [Firepower Management Center のバックアップ \(4 ページ\)](#)
- [管理対象デバイスのローカルでのバックアップ \(5 ページ\)](#)
- [Firepower Management Center からの管理対象デバイスのバックアップ \(7 ページ\)](#)
- [バックアップ プロファイルの作成 \(8 ページ\)](#)
- [ローカル ホストからのバックアップのアップロード \(9 ページ\)](#)
- [\[バックアップ管理 \(Backup Management\) \] ページ \(10 ページ\)](#)
- [バックアップ ファイルからのアプライアンスの復元 \(11 ページ\)](#)

バックアップと復元の概要

災害から回復する能力は、システム保守計画の重要な部分を占めます。

Firepower Management Center または 7000/8000 シリーズ デバイスでデータをバックアップしたり復元したりすることができます。

バックアップと復元に関する制限事項

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。Firepower Management Center を使用してバックアップを実行する場合は、リモートストレージを使用できます。



(注) バックアップデータの収集中に、データの相関付けが一時的に停止してバックアップ関連の設定を変更できなくなることがあります。

バックアップと復元に関する次の制限事項に注意してください。

- 代替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あり、同じバージョンの Firepower システム ソフトウェアを実行している場合のみです。
- バックアップには、キャプチャされたファイル データは含まれません。
- NGIPSv、Firepower Threat Defense物理または仮想管理対象デバイス、あるいは ASA FirePOWER モジュールのバックアップファイルを作成または復元することはできません。イベントデータをバックアップするには、管理元の Firepower Management Center のバックアップを実行します。
- アプライアンス間で設定をコピーするためにバックアップおよび復元プロセスを使用しないでください。バックアップファイルは、アプライアンスを一意に識別する情報を含んでおり、共有することはできません。
- Firepower Management Center を復元した後、最新の侵入ルールの更新を適用する必要があります。
- PKI オブジェクトに関連付けられている秘密キーは、アプライアンスに保存されるたびに、ランダムに生成されたキーで暗号化されます。PKI オブジェクトに関連付けられている秘密キーを含むバックアップを実行すると、秘密キーは復号されてから、暗号化されていないバックアップ ファイルに含められます。バックアップ ファイルは安全な場所に保存してください。
- PKI オブジェクトに関連付けられている秘密キーを含むバックアップを復元すると、その秘密キーはランダムに生成されたキーで暗号化されてからアプライアンスに保存されます。
- クリーン リストとカスタム検出リストのいずれかを有効にしてファイル ポリシーを含むバックアップを復元すると、復元されるファイルのリストとあらゆる既存のファイルリストがマージされます。
- 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、そのバックアップを使用して復元すると、削除された侵入イベントは復元されますが、それらの確認済みステータスは復元されません。それらの復元された侵入イベントは、[確認済みイベント (Reviewed Events)] ではなく [侵入イベント (Intrusion Events)] に表示されます。
- 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となります。そのようなことが起こらないようにするため、侵入イベントのバックアップは、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復元してください。
- セキュリティ ゾーンまたはインターフェイス グループとのインターフェイス アソシエーションが設定されている場合、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。
- Firepower Management Center では、バックアップ機能と復元機能はグローバル ドメインのみで使用できます。サブドメインの範囲内では、バックアップと復元の代わりにエクスポート機能とインポート機能を使用することができます。

関連トピック

[リモートストレージ管理](#)[コンフィギュレーションのインポート/エクスポートについて](#)[侵入イベントを確認済みとしてマーク](#)[インターフェイス オブジェクト：インターフェイスグループとセキュリティゾーン](#)

バックアップ ファイル

実行するバックアップのタイプに応じて、さまざまなデータがバックアップされます。キャプチャされたファイルデータはバックアップされないことに注意してください。次の表を使用して、どのようなタイプのバックアップを実行するかを決定します。

表 1: それぞれのバックアップタイプで保存されるデータ

バックアップタイプ	構成データが含まれるか	イベントデータが含まれるか	統合ファイルが含まれるか
Firepower Management Center	○	○	[いいえ (No)]
7000 & 8000 シリーズ (デバイス自体から実行)	[はい (Yes)]	[いいえ (No)]	[いいえ (No)]
7000 & 8000 シリーズ (管理元の Firepower Management Center から実行)	[はい (Yes)]	[いいえ (No)]	○



(注) NGIPSv デバイス、Firepower Threat Defense 物理または仮想管理対象デバイス、あるいは ASA FirePOWER モジュールについては、バックアップ ファイルを作成または復元することはできません。イベントデータをバックアップするには、管理元の Firepower Management Center のバックアップを実行します。

イベントデータに加えて、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すことができます。バックアップ ファイルを、アプライアンスに保存するか、ローカル コンピュータに保存するかを選択できます。

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。4GB を超える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 コンピュータからバック

クアッブをアップロードすることはできません。Firepower Management Center 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。

関連トピック

[リモートストレージ管理](#)

Firepower Management Center のバックアップ

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin/Maint

始める前に

- アプライアンスに十分なディスク領域があることを確認してください。バックアップの処理で使用可能なディスク領域の90%以上を使用すると、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。[リモートストレージ管理](#) を参照してください。

手順

ステップ 1 [システム (System)] > [ツール (Tools)] > [バックアップ/復元 (Backup/Restore)] を選択します。

ステップ 2 [Firepower 管理バックアップ (Firepower Management Backup)] をクリックします。

ステップ 3 [名前 (Name)] を入力します。

ステップ 4 その他以下の2つの対処法があります。

- 設定をアーカイブするには、[設定をバックアップ (Back Up Configuration)] を選択します。マルチドメイン展開では、このオプションを無効にできません。
- イベント データベース全体をアーカイブするには、[イベントをバックアップ (Back Up Events)] を選択します。

ステップ 5 バックアップの完了時に通知を受けるためには、[電子メール (Email)] チェックボックスを選択して、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](#) 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 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、[完了時にコピー (Copy when complete)] チェックボックスを選択してから、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。

- [ホスト (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
- [パス (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
- [ユーザ (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
- [パスワード (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、そのマシンの指定ユーザの `authorized_keys` ファイルに、[SSH 公開キー (SSH Public Key)] フィールドの内容をコピーします。

ヒント 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。Cisco 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、[バックアップ開始 (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。
- 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、[新規として保存 (Save As New)] をクリックします。

次のタスク

- バックアップファイルに PKI オブジェクトデータが含まれる場合は、バックアップ内に暗号化されていない秘密キーが含まれています。このため、バックアップはセキュアな場所に保存してください。

管理対象デバイスのローカルでのバックアップ

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 & 8000 シリーズ	該当なし	Admin/Maint

アプライアンスのローカル Web インターフェイスを使用して、次の手順を実行する必要があります。

始める前に

- アプライアンスに十分なディスク領域があることを確認してください。バックアップの処理で使用可能なディスク領域の90%以上を使用すると、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してください。

手順

ステップ1 [システム (System)] > [ツール (Tools)] > [バックアップ/復元 (Backup/Restore)] を選択します。

ステップ2 [デバイス バックアップ (Device Backup)] をクリックします。

ステップ3 [名前 (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。

ステップ4 バックアップの完了時に通知を受けるためには、[電子メール (Email)] チェックボックスを選択して、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](#) 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5 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、[完了時にコピー (Copy when complete)] チェックボックスを選択してから、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。

- [ホスト (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。
- [パス (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。
- [ユーザ (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。
- [パスワード (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、そのマシンの指定ユーザの `authorized_keys` ファイルに、[SSH 公開キー (SSH Public Key)] フィールドの内容をコピーします。

ヒント 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。Cisco 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6 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、[バックアップ開始 (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。

- 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、[新規として保存 (Save As New)] をクリックします。

次のタスク

- バックアップファイルに PKI オブジェクトデータが含まれる場合は、バックアップ内に暗号化されていない秘密キーが含まれています。このため、バックアップはセキュアな場所に保存してください。

Firepower Management Center からの管理対象デバイスのバックアップ

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 & 8000 シリーズ	グローバルだけ	Admin/Maint

始める前に

- アプライアンスに十分なディスク領域があることを確認してください。バックアップの処理で使用可能なディスク領域の 90% 以上を使用すると、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。[リモートストレージ管理](#) を参照してください。

手順

- ステップ 1** [システム (System)] > [ツール (Tools)] > [バックアップ/復元 (Backup/Restore)] を選択します。
- ステップ 2** [管理対象デバイスのバックアップ (Managed Device Backup)] をクリックします。
- ステップ 3** [管理対象デバイス (Managed Devices)] フィールドで、1 つ以上の管理対象デバイスを選択します。
- ステップ 4** 設定データと共に統合ファイルも含めるには、[すべての統合ファイルを含める (Include All Unified Files)] チェックボックスを選択します。統合ファイルは、管理対象デバイスがまだ Firepower Management Center へ送っていない、分析と保管のためのイベントデータのバイナリファイルです。
- ステップ 5** Firepower Management Center にバックアップファイルのコピーを保存するには、[管理センターで取得する (Retrieve to Management Center)] チェックボックスを選択します。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のみに保存するには、このチェックボックスをオフにしておいてください。

(注) [管理センターで取得する (Retrieve to Management Center)] を選択したのに Firepower Management Center がリモートストレージにバックアップするよう設定されている場合は、デバイスのバックアップファイルはリモートに設定されている場所に保存されます。

ステップ 6 [バックアップ開始 (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。

次のタスク

- バックアップファイルに PKI オブジェクトデータが含まれる場合は、バックアップ内に暗号化されていない秘密キーが含まれています。このため、バックアップはセキュアな場所に保存してください。

バックアッププロファイルの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 & 8000 シリーズ	グローバルだけ	Admin/Maint

この手順は、デバイスの Web ユーザ インターフェイスを使用して実行する必要があります。

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 新規ファイル名を使用して Firepower Management Center のバックアップファイルを作成する場合、システムにより自動的に、その名前がバックアッププロファイルが作成されます。

手順

- ステップ 1** [システム (System)] > [ツール (Tools)] > [バックアップ/復元 (Backup/Restore)] を選択します。
- ステップ 2** [バックアッププロファイル (Backup Profiles)] タブをクリックします。
- ステップ 3** [プロファイルの作成 (Create Profile)] をクリックします。
- 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。

- ステップ5** バックアッププロファイルを設定します。[Firepower Management Center のバックアップ \(4 ページ\)](#) 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、[新規として保存 (Save As New)] をクリックします。

ローカルホストからのバックアップのアップロード

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 & 8000 シリーズ	グローバルだけ	Admin/Maint

ローカルホストからアプライアンスにバックアップファイルをアップロードできます。この手順は、デバイスの Web インターフェイスを使用して実行する必要があります。

バックアップファイルに PKI オブジェクトが含まれている場合、アップロード時に、システムはランダム生成されたキーを使用して、内部 CA および内部証明書オブジェクトに関連付けられた秘密キーを再暗号化します。

始める前に

- [\[バックアップ管理 \(Backup Management\) \] ページ \(10 ページ\)](#) の説明に従って、ダウンロード機能を使用し、バックアップファイルをローカルホストにダウンロードします。
- SCP を介してローカルホストからリモートホストに 4GB より大きいバックアップをコピーし、そこから Firepower Management Center に取り出します (Web ブラウザではその大きさのファイルのアップロードがサポートされていないため)。詳細については、[リモートストレージ管理](#) を参照してください。

手順

- ステップ1** [システム (System)] > [ツール (Tools)] > [バックアップ/復元 (Backup/Restore)] を選択します。
- ステップ2** [バックアップのアップロード (Upload Backup)] をクリックします。
- ステップ3** [参照 (Browse)] をクリックし、アップロードするバックアップファイルまで移動して選択します。
- ステップ4** [バックアップのアップロード (Upload Backup)] をクリックします。
- ステップ5** [バックアップ管理 (Backup Management)] をクリックして、[バックアップ管理 (Backup Management)] ページに戻ります。

次のタスク

- アプライアンスによってファイルの整合性が確認された後、[バックアップ管理 (Backup Management)] ページを更新し、詳細なファイル システム情報を表示します。

[バックアップ管理 (Backup Management)] ページ

バックアップ ファイルに PKI オブジェクトが含まれている場合は、アップロード時に、内部 CA および内部証明書オブジェクトに関連付けられている秘密キーが、ランダムに生成されたキーで再暗号化されます。

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 [バックアップ管理 (Backup Management)] ページの下部にリストされます。Firepower Management Center で、[バックアップ管理 (Backup Management)] ページの上部にある [リモートストレージ (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には [バックアップ管理 (Backup Management)] ページの [バックアップ用にリモートストレージを有効にする (Enable Remote Storage for Backups)] チェック ボックスをオンにします。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。

次の表では、[バックアップ管理 (Backup Management)] ページの各列とアイコンについて説明します。

表 2: バックアップ管理 (Backup Management)

機能	説明
システム情報 (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を注意してください。
作成日	バックアップ ファイルが作成された日時
ファイル名 (File Name)	バックアップ ファイルのフルネーム
VDBバージョン (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。
参照先	バックアップ ファイルの場所
サイズ (MB) (Size (MB))	バックアップファイルのサイズ (メガバイト)
イベント? (Events?)	[はい (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

機能	説明
表示 (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。
復元 (Restore)	バックアップファイルを選択し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。
ダウンロード (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。
削除 (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。
[移動 (Move)] をクリックします	Firepower Management Center 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

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 & 8000 シリーズ	グローバルだけ	Admin/Maint

[バックアップ管理 (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。この手順は、デバイスの Web インターフェイスを使用して実行する必要があります。

**注意**

- この操作により、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。
- 仮想 Firepower Management Center で作成されたバックアップを物理 Firepower Management Center 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。



- (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。

始める前に

- 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ことを確認します。詳細については、[ダッシュボードの表示](#)を参照してください。
- バックアップの完了後にアプライアンスに追加したライセンスは、リストア時の競合を避けるために、バックアップの復元前に削除します。詳細については、[Firepower の機能ライセンスについて](#)を参照してください。
- バックアップに保管されているものと同じ侵入イベントデータがアプライアンスに存在しないことを確認します。これは、そのような状況下でバックアップを復元すると、重複するイベントが作成されるためです。詳細については、[侵入イベントについて](#)を参照してください。

手順

- ステップ 1** [システム (System)] > [ツール (Tools)] > [バックアップ/復元 (Backup/Restore)] を選択します。
- ステップ 2** バックアップファイルをクリックして、そのコンテンツを表示します。詳細には、ファイルの所有者、ファイルの権限、ファイルサイズ、および日付が含まれています。
- ステップ 3** [システム (System)] > [ツール (Tools)] > [バックアップ/復元 (Backup/Restore)] を選択して、[バックアップ管理 (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ます。
- ステップ 5** [復元 (Restore)] をクリックします。

(注) 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、[復元 (Restore)] ボタンはグレー表示されません。

ステップ 6 ファイルを復元するには、次のいずれかまたは両方のオプションを選択します。

• **設定データの復元 (Restore Configuration 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 Firepower Management Center から行われたデバイス設定の変更も復元されます。バックアップファイルを復元することで、バックアップファイルの作成後に行った変更は上書きされます。

• **イベントデータの復元 (Restore Event Data)**

ステップ 7 [復元 (Restore)] をクリックします。

ステップ 8 アプライアンスを再起動します。

次のタスク

- 最新のシスコルールアップデートをインポートします。[侵入ルールのワンタイム手動更新](#)を参照してください。インポートの一環としてポリシーを再展開する場合、設定の変更を展開する必要はありません (後述)。
- 設定変更を展開します。[設定変更の導入](#)を参照してください。
- バックアップの復元前に、アプライアンスから削除したライセンスを追加して再設定します。
- 復元時にアプライアンスがライセンスの競合を示した場合は、サポートまでお問い合わせください。

