
# バックアップと復元の使用

バックアップと復元は、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からデータを復元できるようにデータをアーカイブするメカニズムが備わっています。

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。

- バックアップは、バックアップを作成する製品バージョンに対してのみ有効です。
- 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。
- 仮想の管理対象デバイス、Blue Coat X-Series 向け Cisco NGIPS、または Cisco ASA with FirePOWER Services 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。すべてのイベント データをバックアップするには、管理防御センターのバックアップを実行します。
- 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に限られます。

**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。

**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（64-17 ページ）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、次の各項を参照してください。

- 防御センターおよび物理管理対象デバイスのバックアップ ファイルの作成については、バックアップ ファイルの作成（70-2 ページ）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は、バックアップ プロファイルの作成（70-7 ページ）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は、ローカル ホストからのバックアップのアップロード（70-8 ページ）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は、バックアップ ファイルからのアプライアンスの復元（70-9 ページ）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（Any）

**サポートされるデバイス：**すべて（仮想、X-シリーズ、および ASA FirePOWER を除く）

**サポートされる防御センター：**任意（Any）

デバイス自体からの物理管理対象デバイスのバックアップ、管理する防御センターからの物理管理対象デバイスのバックアップ、および防御センターのバックアップを実行できます。システムは、実行するバックアップのタイプに応じて異なるデータをバックアップします。システムはキャプチャされたファイル データをバックアップ**しない**ことに注意してください。次の表を使用して、どんな種類のバックアップを実行するかを決定します。

***表 70-1　バックアップ タイプ別の保存データ***

| 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 |
|---|---|---|---|
| 防御センター | Yes | Yes | No |
| デバイス自体から実行される、物理管理対象デバイス | Yes | No | No |
| 管理用の防御センターから実行される、物理管理対象デバイス | Yes | No | Yes |

**（注）** 仮想の管理対象デバイス、Blue Coat X-Series 向け Cisco NGIPS、または Cisco ASA with FirePOWER Services 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、管理用の防御センターのバックアップを実行します。

既存のシステム バックアップを表示して使用するには、[バックアップ管理（Backup Management）] ページに移動します。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。

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 プロセスの使用スペースが使用可能なディスク スペースの 90% を超えると、バックアップに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 コンピュータからバックアップをアップロードできません。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（64-17 ページ）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いる間、データ相関は一時的に停止されます。

次の点に注意してください。

- PKI オブジェクトに関連付けられた秘密キーは、アプライアンスに保存されるときに、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た秘密キーを含むバックアップを実行する場合、秘密キーは、暗号化されないバックアップ ファイルに組み込まれる前に復号化されます。バックアップ ファイルを安全な場所に保存します。
- 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復元すると、システムはアプライアンスに保存する前にランダムに生成されたキーでキーを暗号化します。
- 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、削除された侵入イベントはそのバックアップで復元されますが、確認済み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、[確認済みイベント（Reviewed Events）] の下ではなく [侵入イベント（Intrusion Events）] の下に表示されます。侵入イベントの確認（41-18 ページ）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 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。詳細については、セキュリティ ゾーンの操作（3-44 ページ）を参照してください。

**防御センターのバックアップ ファイルの作成するには、次の手順を実行します。**

**アクセス：**Admin/Maint

**手順 1**　[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] の順に選択します。

[バックアップ管理（Backup Management）] ページが表示されます。

**手順 2**　[バックアップ（Backup）]**防御センター**をクリックします。

[バックアップの作成（Create Backup）] ページが表示されます。

**手順 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。英数字、句読記号、およびスペースを使用できます。

**手順 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、[バックアップ設定（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、[イベントのバックアップ（Back Up Events）] を選択します。

**手順 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、[電子メール（Email）] 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（63-20 ページ）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。

**手順 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、[完了時にコピー（Copy when complete）] チェック ボックスをオンにして、付随するテキスト 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。

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。

**手順 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、[バックアップを開始（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。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（64-17 ページ）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、[復元データベース（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は、バックアップ ファイルからのアプライアンスの復元（70-9 ページ）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、[新規保存（Save As New）] をクリックします。

  [システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] の順に選択してから [バックアップ プロファイル（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（70-7 ページ）を参照してください。

**物理管理対象デバイスのバックアップ ファイルをそのデバイス自体から作成するには、次の手順を実行します。**

**アクセス：**Admin/Maint

**手順 1**　[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] の順に選択します。

[デバイスのバックアップ（Device Backups）] ページが表示されます。

**手順 2**　[デバイスのバックアップ（Device Backup）] をクリックします。

[バックアップの作成（Create Backup）] ページが表示されます。

**手順 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。英数字、句読記号、およびスペースを使用できます。

**手順 4**　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、[電子メール（Email）] 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（63-20 ページ） 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。

**手順 5**　オプションで、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、[完了時にコピー（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。

- [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。

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。

**手順 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、[バックアップを開始（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。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（64-17 ページ） 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、[復元データベース（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は、バックアップ ファイルからのアプライアンスの復元（70-9 ページ） 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、[新規保存（Save As New）] をクリックします。

  [システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] の順に選択してから [バックアップ プロファイル（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（70-7 ページ）を参照してください。

**物理管理対象デバイスのバックアップ ファイルをその管理用防御センターから作成するには、次の手順を実行します。**

**アクセス：**Admin/Maint

**手順 1**　[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] の順に選択します。

[バックアップ管理（Backup Management）] ページが表示されます。

**手順 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。

[バックアップの作成（Create Backup）] ページが表示されます。

**手順 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。複数の管理対象デバイスを選択するには、Shift キーか Ctrl キーを使用します。

**手順 4**　構成データに加えて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 ボックスをオンにします。

**手順 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、[防御センターに保存（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）**　[防御センターに保存（Retrieve to Defense Center）] を選択した場合、バックアップのリモート ストレージが防御センターで設定されていれば、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。

**手順 6**　[バックアップの開始（Start Backup）] をクリックします。

操作の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 ファイルは `/var/sf/backup` ディレクトリに保存されます。防御センターを使用して、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（64-17 ページ）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、[復元データベース（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は、バックアップ ファイルからのアプライアンスの復元（70-9 ページ）を参照してください。

**手順 7**　オプションで、この設定をバックアップ プロファイルとして保存して後で使用するには、[新規保存（Save As New）] をクリックします。

[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] の順に選択してから [バックアップ プロファイル（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（70-7 ページ）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（Any）

**サポートされるデバイス：**すべて（仮想、X-シリーズ、および ASA FirePOWER を除く）

**サポートされる防御センター：**任意（Any）

[バックアップ プロファイル（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（70-2 ページ）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 プロファイルを作成するには、次の手順を実行します。**

**アクセス：**Admin/Maint

**手順 1**　[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] の順に選択します。

[バックアップ管理（Backup Management）] ページが表示されます。

**手順 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。

[バックアップ プロファイル（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。

**手順 3**　[プロファイルを作成（Create Profile）] をクリックします。

[バックアップの作成（Create Backup）] ページが表示されます。

**手順 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。

**手順 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は、バックアップ ファイルの作成（70-2 ページ）を参照してください。

**手順 6**　バックアップ プロファイルを保存するには、[新規保存（Save As New）] をクリックします。

[バックアップ プロファイル（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。

# 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（Any）

**サポートされるデバイス：**シリーズ 2およびシリーズ 3

**サポートされる防御センター：**任意（Any）

バックアップ管理（Backup Management）の表で説明されているダウンロード機能を使用してバックアップ ファイルをローカル ホストにダウンロードした場合、防御センターにそれをアップロードできます。

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、内部 CA と内部証明書オブジェクトに関連付けられた秘密キーは、アップロードの際にランダムに生成されるキーによって再暗号化されます。

**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（64-17 ページ）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には、次の手順を実行します。**

**アクセス：**Admin/Maint

**手順 1**　[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] の順に選択します。

[バックアップ管理（Backup Management）] ページが表示されます。

**手順 2**　[バックアップのアップロード（Upload Backup）] をクリックします。

[バックアップのアップロード（Upload Backup）] ページが表示されます。

**手順 3**　[参照（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、[バックアップのアップロード（Upload Backup）] をクリックします。

**手順 4**　[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。

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ら、[バックアップ管理（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（Any）

**サポートされるデバイス:** シリーズ 2 およびシリーズ 3

**サポートされる防御センター:** 任意（Any）

[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。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 Sourcefire 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。

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、内部 CA と内部証明書オブジェクトに関連付けられた秘密キーは、アップロードの際にランダムに生成されるキーによって再暗号化されます。

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。防御センターで、[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。

**（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、[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 70-2　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に注意してください。 |
| 作成日（Date Created） | 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 |

*表 70-2　バックアップ管理(Backup Management)(続き)*

| 機能 | 説明 |
|---|---|
| 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(Location) | 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 |
| 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) | 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これをクリックすると、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を復元するには、次の手順を実行します。**

**アクセス:** Admin

**手順 1**　[システム(System)] > [ツール(Tools)] > [バックアップ/復元(Backup/Restore)] の順に選択します。

[バックアップ管理(Backup Management)] ページが表示されます。

**手順 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。

**手順 3**　[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。

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

[バックアップの復元(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、[復元(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。

**手順 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。

**手順 6**　[復元（Restore）] をクリックして、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。

**手順 7**　アプライアンスを再起動します。

**手順 8**　最新の Sourcefire 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。

**手順 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。