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。ディザスタ リカバリ計画の一環として、シスコは Firepower Management Center および管理対象デバイスを定期的にバックアップすることをお勧めします。バックアップは、問題または障害のある Firepower Management Center アプライアンスまたは 7000 または 8000 シリーズ デバイス、を交換する際に、情報を復元するために使用されます。次のトピックでは、バックアップを使用して Firepower システムの機能を復元する方法について説明します。

バックアップと復元のサポート

以下からデータのバックアップと復元を行うことができます。

- Firepower Management Center
- 7000 および 8000 シリーズ

バックアップと復元のガイドラインと制限事項

Firepower Management Center、7000 & 8000 シリーズ デバイス、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、必要に応じて、リモート ストレージを使用して使用可能な領域を最適化できます。詳細については、「リモート ストレージ」を参照してください。

（注） 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。

（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。

Firepower Management Center と 7000 および 8000 シリーズ デバイス

Firepower Management Center および 7000 & 8000 シリーズ デバイスのバックアップと復元に関する次のガイドラインと制限事項に注意してください。

- 代替アプライアンスまたはデバイ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またはデバイ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。
- Firepower Management Center Web インターフェイスまたはデバイスの Web インターフェイスの各々から、代替アプライアンスまたはデバイスにバックアップを復元することができます。
- 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。
- 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。
- アプライアンスまたはデバイ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になります。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。

Firepower Threat Defense

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、どんな種類のバックアップを実行するかを決定します。

警告 復元およびアップグレード プロセスが正しく機能するように、バックアップ ファイルは手動で変更しないでください。バックアップ ファイルへの不正アクセスがないことを確認する必要があります。

表 *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
Firepower Management Center	○	○	×
7000 & 8000 シリーズ（デバイス自体から実行）	○	×	×
7000 & 8000 シリーズ（管理元の Firepower Management Center から実行）	○	×	○

（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。

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
任意（Any）	任意（Any）	Firepower Management Center	グローバルだけ	Admin/Maint

この手順は、Firepower Management Center 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。

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。

7000または8000シリーズデバイスのローカルバックアップ

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
該当なし	任意（Any）	7000 & 8000 シリーズ	該当なし	Admin/Maint

7000 または 8000 シリーズ デバイスのローカル 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

この手順は、Firepower Management Center 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。

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。

次のタスク

バックアップ ファイルを検索するには、次の情報を使用します。

- 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。Firepower Management Center にバックアップのコピーを保存することを選択した場合、コピーは `/var/sf/remote-backup` ディレクトリに格納されます。
-

（注） バックアップにPKIオブジェクトのデータが含まれている場合、バックアップ内に暗号化されていない秘密キーが保存されるため、安全な場所にバックアップを保存します。

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
該当なし	任意（Any）	7000 & 8000 シリーズ、Firepower Management Center	グローバルだけ	Admin/Maint

次の手順は、デバイスの Web ユーザ インターフェイス、または Firepower Management Center Web インターフェイス（該当する場合）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、その名前でバックアップ 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）のステップ 4 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 Firepower Management Center、7000 または8000シリーズデバイスへ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）
該当なし	任意（Any）	Firepower Management Center 7000 & 8000 シリーズ	グローバルだけ	Admin/Maint

デバイスに応じて、Firepower Management Center Web インターフェイスまたはデバイスのローカル Web インターフェイスを使用して、ローカル ホストから Firepower Management Center, 7000 シリーズデバイス、または 8000 シリーズデバイスにバックアップ ファイル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、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 （11 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

[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] > [バックアップ管理（Backup Management）] で、Firepower Management Center Web インターフェイスの [バックアップ管理（Backup Management）] ページにアクセスできます。[バックアップ管理（Backup Management）] ページには、Firepower Management Center、7000 シリーズ デバイス、8000 シリーズ デバイスおよび のバックアップ情報が表示されます。

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。

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）] ページの各列およびボタ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 （注） 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のみです。
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
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。詳細については、次を参照してください。 バックアップ ファイルからの Firepower Management Center、7000 または 8000 シリーズ デバイスの復元 （13 ページ）
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。

機能	説明
[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 Firepower Management Center、7000 または 8000シリーズ デバイスの復元

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）
該当なし	任意（Any）	Firepower Management Center、7000 & 8000 シリーズ	グローバルだけ	Admin/Maint

Firepower Management Center Web インターフェイスまたはデバイスの Web インターフェイスの [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 Firepower Management Center、7000 シリーズ デバイス、または 8000 シリーズ デバイスを復元できます。

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。バックアップの完了後に Cisco Smart Software Manager から Firepower Management Center を登録解除し、このバックアップを復元する場合、Firepower Management Center を登録解除し Firepower Management Center を再度登録する必要があります。

（注） Firepower Management Center の登録解除の詳細については、Cisco Smart Software Manager から Firepower Management Center の登録解除を参照してください。Firepower Management Center を登録するには、スマート ライセンスの登録を参照してください。

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す。

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。設定変更の展開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。