



## Expressway での HSM デバイスの構成

- [重要：事前の確認事項](#) (1 ページ)
- [HSM を有効にして管理する方法](#) (1 ページ)
- [モジュールの削除方法](#) (5 ページ)
- [HSM の無効化方法](#) (6 ページ)

### 重要：事前の確認事項

**HSM の障害。** Expressway が HSM を使用するように設定されており、その後 HSM が失敗すると、暗号化を必要とするすべてのサービスが利用できなくなります。これには、MRA、コール、Web アクセスなどが含まれます。

**初期設定へのリセット。** 何らかの理由で HSM が恒久的に利用できない場合は、Expressway の初期設定化を行ってから、Expressway で新しい HSM を設定する必要があります。初期設定化のリセットでは、ソフトウェアイメージが再インストールされ、**Expressway** 設定がデフォルトで最も少ない機能がリセットされます（リセットの実行方法については、『Expressway 管理者ガイド』を参照してください）。

### HSM を有効にして管理する方法

[HSM構成 (HSM configuration)] ページ ([メンテナンス (Maintenance)] > [セキュリティ (Security)] > [HSM構成 (HSM configuration)]) で、Expressway に必要な情報を構成します。

設定はクラスタ全体に複製されます。

[HSM 設定 (HSM configuration)] ページの設定は、Expressway クラスタ内のすべてのピアにわたって複製されます。したがって、1 つのピアの設定を追加または削除すると、その変更は他のすべてのピアに複製されます。

## タスク 1: 前提条件の設定

Expressway のハードウェア セキュリティ モジュール (HSM) 機能を有効にする前に、次の手順を実行してください。

a.	HSM オプション キーを追加します。	<p><b>i.</b> [メンテナンス (Maintenance)] &gt; [オプションキー (Option keys)] に移動します。</p> <p><b>ii.</b> [ソフトウェアオプション (Software option)] セクションで、オプション キーを入力します。</p> <p><b>iii.</b> [オプションの追加 (Add option)] をクリックします。キーはページ上部のリストに表示されます。</p>
b.	<p>HSM TLP パッケージをインストールします。これは、Expressway ソフトウェア イメージと同じダウンロード サイトから入手できます。</p> <p>HSM TLP は、Expressway が HSM を使用するために必要な HSM プロバイダー固有のバイナリのアーカイブです。</p>	<p><b>i.</b> [メンテナンス (Maintenance)] &gt; [アップグレード (Upgrade)] に移動します。</p> <p><b>ii.</b> [コンポーネントのアップグレード (Upgrade component)] セクションで、[ファイルの選択 (Choose File)] をクリックして、ローカルマシンから TLP ファイルを選択します。</p> <p><b>iii.</b> [アップグレード (Upgrade)] をクリックします。「コンポーネントが正常にインストールされました (Component installation succeeded)」というメッセージがページ上部に表示され、HSM TLP もページ上部に表示されます。ドロップダウンで、インストールされているすべてのモジュールのリストを確認できます。</p> <p>(注) オプション キーを追加して、クラスタ内の各ピアに TLP をインストールする必要があります。すべてのピアにオプション キーと TLP がある場合を除き、クラスタで HSM モードを有効にすることはできません。</p>

c.	Expressway での HSM ボックスの展開	<p>nShield Connect XC HSM を設定するには、次のようにします。</p> <p><b>i.</b> nShield Connect のユーザガイドの説明に従って、Security World とリモートファイルシステム (RFS) を設定します。</p> <p><b>ii.</b> HSM が必要とするすべてのファイルのマスターコピーを含む nShield Connect に RFS を設定します。通常、RFS はクライアント コンピュータ上に存在しますが、ネットワーク上でアクセス可能な任意のコンピュータ上に配置することもできます。</p> <p><b>iii.</b> RFS および nShield Connect ボックスを展開した後、RFS で次のコマンドを実行します。 <code>/opt/nfast/bin/rfs-setup --gang-client --write-noauth &lt;Expressway_ip_address&gt;</code></p> <p>このコマンドが実行されていない場合、HSM 証明書管理は、Expressway で正しく機能しません。</p>
d.	署名認証局にアクセスします。	-
e.	HSM と互換性のある証明書の作成	手順については、『Expressway 管理者ガイド』の「セキュリティ」の章を参照してください。

## タスク 2 : Expressway での HSM の有効化

この手順は、Expressway で HSM を有効にするために推奨される手順です。

**ステップ 1** [メンテナンス (Maintenance)] > [セキュリティ (Security)] > [HSM 構成 (HSM configuration)] に移動します。

**ステップ 2** [HSM 構成 (HSM Settings)] で、[HSM モード (HSM Mode)] ドロップダウン リストから HSM プロバイダーを選択します。

**ステップ 3** nShield の設定

1. RFS IP アドレスと RFS ポートを入力します。デフォルトのポートは 9004 です。
2. [構成を保存 (Save Configuration)] をクリックします。  
ページの上部に次のメッセージが表示されます。

HSM 設定が更新されました

3. [モジュールの追加 (Add Module)] セクションで、デバイスの IP アドレス、ポート、ESN (電子シリアル番号)、および KNETI (ネットワーク整合性キー) を入力します。
4. [モジュールの追加 (Add Module)] をクリックします。

ページの上部に次のメッセージが表示されます。

HSM モジュールが正常に追加されました

5. [HSMモード (HSM Mode)] タブの下のテーブルにデバイスが表示されます。
6. デバイスを追加するには、モジュールの追加手順を繰り返します。

**ステップ 4** [HSMモード (HSM Mode)] を [オン (On)] に設定して、[モードを設定 (Set Mode)] をクリックします。ページの上部に次のメッセージが表示されます。

HSM モードが正常に更新されました

- (注) HSM モードのオン/オフを切り替えると、Web が利用できなくなる場合があります。この問題が発生した場合は、ブラウザページをリロードします。

---

**結果** : Expressway で HSM の使用が有効になります。

#### 次のタスク

HSM の動作ステータスを確認するには、次のセクション「[タスク 3 : HSM ステータス チェックのモニタリング](#)」を参照してください。

## タスク 3 : HSM ステータス チェックのモニタリング

HSM モードを有効にすると、[HSM構成 (HSM configuration)] ページに [HSMステータスチェック (HSM Status check)] セクションが表示されます。このセクションには、すべての Expressway クラスタピア用の HSM サーバと HSM 証明書、および各ピアのすべてのモジュールに関する情報が表示されます。

#### 実行中の HSM サーバ

1. **TRUE** : Expressway で HSM モードを有効にした後に、HSM ボックスとの通信を担当するプロセスが Expressway で実行されている場合。
2. **FALSE** : プロセスが Expressway で実行されておらず、HSM の障害のアラームが発行された場合。

#### 使用中の HSM 証明書

1. HSM 証明書と秘密キーが Expressway で使用されている場合は、TRUE になります。
2. Expressway が HSM 証明書と秘密キーを使用していない場合は、FALSE になります。デフォルトの状態は FALSE です。「HSM証明書が使用されていません (HSM certificate

is not used) 」というアラームが Expressway で表示されます。これは、HSM 証明書と秘密キーを使用していないことを警告するものです。

HSM 証明書と秘密キーが Expressway に展開されると、このアラームは引き下げられ、表示されるステータスは TRUE に変更されます。

ESN セクションには、HSM の設定中に追加され、その ESN で区別される HSM モジュールがリストされます。その他の列は、**接続ステータス**と**ハードウェアのステータス**を定義します。

#### 接続ステータス

1. Expressway と HSM モジュール間にネットワークの問題が存在しない場合は、OK となります。
2. ネットワークまたは HSM サーバの接続に関する問題が発生し、アラームが発生した場合、Failed となります。

#### ハードウェア ステータス

1. ハードウェアに関する問題が HSM ボックス自体で検出されない場合は、OK となります。
2. ハードウェアまたは HSM ボックスの設定に問題があり、アラームが発生すると、Failed となります。

## タスク 4 : 次のステップ - HSM 秘密キーの生成とインストール

HSM を有効にして正常に動作している場合は、HSM 秘密キーと証明書を生成し、Expressway にインストールする必要があります。詳しくは、『Expressway 管理者ガイド』の「HSM を使用した Expressway サーバ証明書の管理」を参照してください。

## モジュールの削除方法



(注) HSM モードが有効である場合、最後のデバイスは削除できません。まず、HSM モードを無効にする必要があります。

Expressway HSM 設定からデバイス (モジュール) を削除するには、次の手順を実行します。

**ステップ 1** [メンテナンス (Maintenance)] > [セキュリティ (Security)] >> [HSM 構成 (SSH configuration)] に移動します。

**ステップ 2** リストから必要なデバイスを選択し、[削除 (Delete)] をクリックします。

## HSM の無効化方法

いずれかの理由で HSM を無効にする場合は、次の手順を実行することを推奨します。

- 
- ステップ 1 [メンテナンス (Maintenance)] > [セキュリティ (Security)] > [HSM 構成 (HSM configuration)] に移動します。
  - ステップ 2 [HSM モード (HSM Mode)] を [オフ (Off)] に設定し、[モードの設定 (Set Mode)] をクリックします。これにより、Expressway での HSM の使用が無効になります。
  - ステップ 3 削除するテーブル内のすべてのモジュールを選択するには、個々のデバイスを確認するか、[すべて選択 (Select all)] をクリックします。(テーブルのすべてのデバイスを選択解除するには、[すべてを選択解除 (Unselect all)] をクリックします。)
  - ステップ 4 [削除 (Delete)] をクリックし、確認ダイアログボックスで [OK] をクリックします。
-

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。