「SSLサーバー証明書のインポート」

図研ネットウエイブ株式会社

2016-10

Ver.2.4

NetWave

人を社会をＩＴがつなぐ

確認済み証明書

- サイバートラスト
  - SureServer（forクラウド/MDを含む）[2048bit/SHA-2]
  - SureServer EV（forクラウド/MDを含む） [2048bit/SHA-2]
- Global Sign
  - 企業認証SSL
- シマンテック
  - セキュア・サーバーID
- GEO Trust
  - トゥルービジネスID
- Let’s Encrypt
  ※自動更新はできません

- マルチドメイン、ワイルドカード証明書に対応しています。
- 以下の機能を持つ証明書には対応しておりません
  - SGC機能
  - 脆弱性・マルウェア検知機能

1. 新規に証明書を申請/発行する場合

Brocade Virtual Traffic Manager(vTM）上で証明書申請に必要な情報を取得する場合

① vTM上でCSRの作成
② 証明書の申請
③ 発行された証明書でvTMの証明書をアップデート
④ 中間証明書／クロスルート証明書のインポート
⑤ Virtual Serverでの利用設定

※クロスルート証明書が含まれた中間証明書が提供されてる場合があります。

手順はサイバートラスト様のサイトに公開されております。
https://www.cybertrust.ne.jp/SureServer/STM_manual.pdf

2. 既存または外部発行の証明書を利用する場合

既にお持ちのSSL証明書を使用する場合、

① 秘密鍵の変換
② 証明書と秘密鍵のインポート
③ 中間証明書／クロスルート証明書のインポート
④ Virtual Serverでの利用設定

③、④の手順はサイバートラスト様のサイトで公開されている手順と同じになります。
https://www.cybertrust.ne.jp/SureServer/STM_manual.pdf

※クロスルート証明書が含まれた中間証明書が提供されてる場合があります。

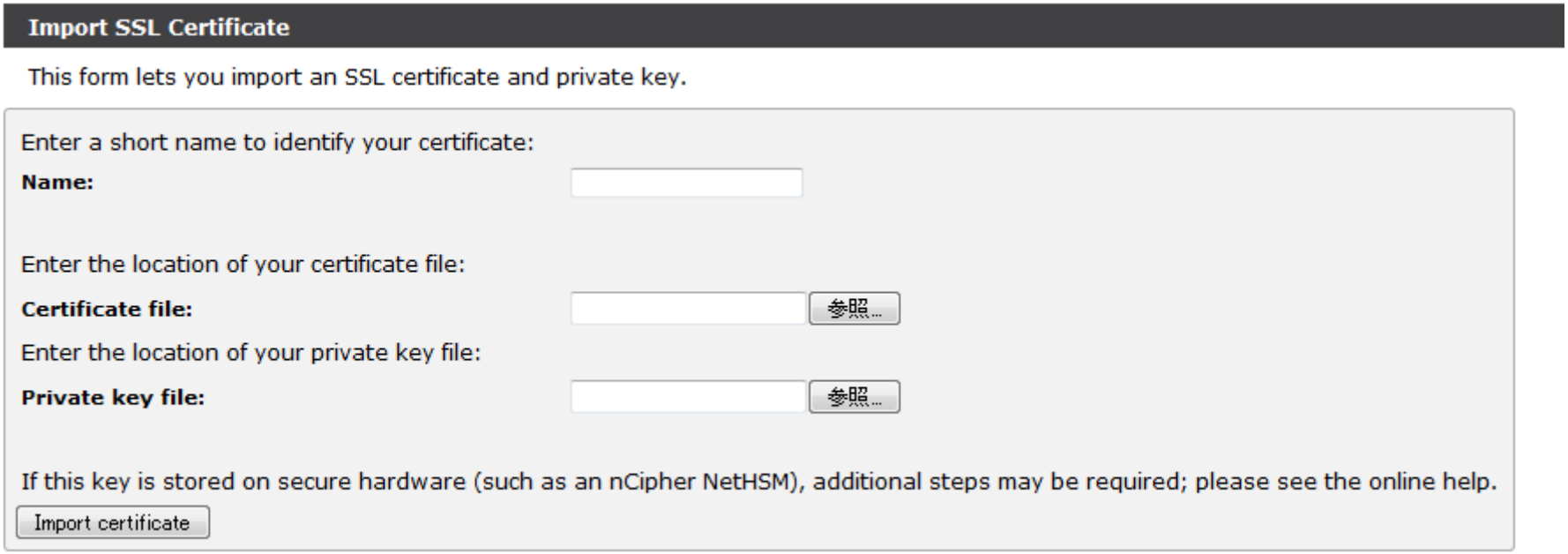
① 秘密鍵の変換

- OpenSSLコマンドが利用できる環境に秘密鍵のファイルをアップロードします。
  ※vTMの仮想マシン上にアップロードすることもできます。
- 以下のコマンド2つのうちどちらかを実行し、出力結果を使用します。

openssl rsa -in <秘密鍵ファイル> -out <出力ファイル>
　出力されたファイルを取り出します。
openssl rsa -in <秘密鍵ファイル>
　表示された内容をテキストエディタ等を使用して
　-----BEGIN RSA PRIVATE KEY----- から
　-----END RSA PRIVATE KEY-----　までを
　コピーしファイルに保存します。

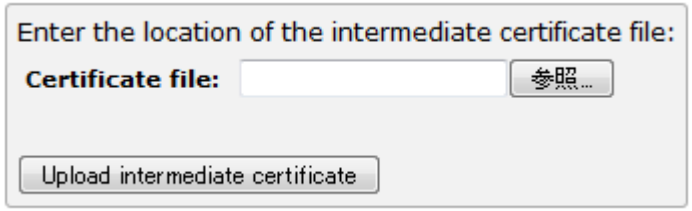
② 証明書と秘密鍵のインポート

- Catalogs>SSL >SSL Catalogs > SSL Certificates catalog のEditをクリックします
- Import SSL certificateを選択します
  - 秘密鍵は「① 秘密鍵の変換」のファイルを使用します。
  - 証明書ファイル、秘密鍵を選択し、インポートします。
- インポート完了後、SSL Certificates catalogにインポートされた証明書が登録されます



③ 中間証明書／クロスルート証明書のインポート

- Catalogs>SSL >SSL Catalogs > SSL Certificates catalogを選択します
- インポートした証明書のEditを選択します
- Certificate signingの項目でUpdate / Add Intermediate Certificateを選択します
- Enter the location of the intermediate certificate file:の項目で証明書ファイルを選択し、Upload intermediate certificateをクリックします。



- Your configuration has been updated.と表示されます
- [Intermediate Certificate: Issuer:]として、インストールした中間証明書,クロスルート証明書の情報が表示されます

④ Virtual Serverでの利用設定

- Virtual Serverを作成します
  - Wizardsメニューなどを使い、Virtual Serverを作成します。
  - プロトコル：HTTP、ポート：443を指定します。
    ※ポート80番で作成した後、変更していただくことも可能です
- 作成したVirtual Serverの設定を変更します
  - SSL Decryption> ssl_decrypt:の設定をYesに変更します。
  - certificate:Default Certificateの項目で使用するサーバー証明書を選択します。
  - 画面下部のApply ChangesにてUpdateをクリックします。

  - 証明書の有効期間が短い場合は選択された証明書、マッピング設定の項目の色が変わって表示し、WARNINGが表示されます。
    ※動作上は問題ありません。

証明書更新について

- 証明書の期限切れなどで更新される場合は、Catalog>SSL Server Certificates catalogから対象証明書のEditをクリックしてください
- Certificate signingメニューのExport CSR / Sign Certificateをクリックしていただき、Replace certificateに新しい証明書ファイルの内容を貼り付けてUpdateを実施してください。

※更新後、中間CA証明書を再度インポートしてください。

ご注意事項

- 証明書のインポート時にエラーが出力され、インポートできない場合はお手数ですがサポートセンターまでお問い合わせください。

- 鍵サイズが異なる証明書への更新はできません。新規と同じ手順でインポートしていただきます
- OUなど証明書の情報を変更した場合、証明書の更新ができないことがあります。新規と同じ手順でインポートしていただきます。

- Ver.10.4ではCSRを作成する際にECDSAの鍵タイプを指定することができます。証明書の鍵タイプはご利用の暗号化スィートと関連します。SSLの設定にご注意ください。