

「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





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





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



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_manu al.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。





- 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

Import SSL Certificate

This form lets you import an SSL certificate and private key.

Enter a short name to identify your certificate: Name:		
Enter the location of your certificate file:	(407)	
Enter the location of your private key file:		
Private key file:	参照	
If this key is stored on secure hardware (such as an nCipher NetHSM), additional steps may be required; please see the online help. Import certificate		

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。

Enter the location of th	e intermediate certificate file:
Certificate file:	参照
Upload intermediate certif	icate

- Your configuration nas 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。

This form helps you to sign your certificate.

Certificate Signing Request (CSR)

Your Certificate Authority will use this Certificate Request text to create and issue a trusted certificate, based on this certifica

----BEGIN NEW CERTIFICATE REQUEST----

MIIClTCCAX0CAQAwUDELMAkGA1UEBhMCSlAxETAPBgNVBACTCFlva29oYWlhMQww CgYDVQQKEwNaTlcxIDAeBgNVBAMTF3N0bTk1LTAwMS50ZWNoMS0yLmxvY2FsMIIB IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIBCgKCAQEApFChNElpZV4dqIE3BjK7NRxS r0XB0xjBirGmztDo6VAqFTsx2Mymz5vTaZLtBjrr6ZPM4JKTV/0g9ENn+f0Thf67 u+dH2k9dc3Wf10B5vwcdx9XMtfX+D28DLOMTeN4iQZL1sbUaWySw+0R3kD36PaJ8 mY/YBAMg100KFs6frElAcUWApb2sj4r47lo2U8zrRCgBa1CdGeOSxY01UaQ7wKvn Kp79leiHtt4e6Bj2fbNtpI/uj/cNcTEZEZgJxxNGyxEagw06vBHxWg/zHSf6SIGK SMJY2SVYJCJ8DXW3Chw9tZ/FI10i/7j4mUQvgBa1SA6+cHt03esk31uPVQmhVwID AQABoAAwDQYJKoZIhvcNAQEFBQADggEBAFrFLL/Jn7iRgyTV2H20JSA3wtQLb8Gd FZby1Pvmyt5IVf0WpcGcyQAOyrbcUjHgajNeE1XYkaSBg6fbA/MLdGn8dL0MGfGh xmiMDuMY66PaQOCJ3CbtaFQSbvem0LaEmYb61ZV2yLEjnYY8ME3WHqyLPMCiSYjj e/KdeF2XEcSjh2MqD0NDBzF5eNWSLKcSDY3HXuo201qoP7KBaHs9PFt6wm0UuION zwF0nm8PqeBOFRPfuxGAHvrItD+Nej0wkRMFzxWHY+qvvEGpSx8n9syVzhUIXVyi OFkledqKof0uxmWWTSkn0TVN7eNsJWHKTYKAqURCfKLzGhti4crEHU=

Replace certificate

Once you have received a new certificate, paste it here to replace your current certificate.

Replace certificateの項目

※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。