cybertrust

F5 ネットワークス BIG-IP
CSR作成/証明書インストール手順書

はじめに

【！】本手順書をご利用の前に必ずお読みください

1. 本ドキュメントは、「F5 ネットワークス/BIG-IP」の環境下でサイバートラストのサーバー証明書をご利用いただく際の CSR 作成とサーバー証明書のインストールについて解説するドキュメントです。
2. 本資料のサンプル画面は、「BIG-IP1500（Version：BIG-IP 9.3.0 Build178.5）」を使用して作成しています。
3. 実際の手順はお客様の環境により異なる場合があり、BIG-IP の動作を保証するものではございません。あらかじめご了承ください。
4. このドキュメントは予告なく変更される場合があり、サイバートラスト株式会社はその内容に対して責任を負うものではありません。また、このドキュメント内に誤りがあった場合、サイバートラスト株式会社は一切の責任を負いません。
5. このドキュメントの一部または全部を複製することは禁じられており、提供または製造を目的として使用することはできません。ただし、サイバートラスト株式会社との契約または同意文書で定められている場合に限り、この注記の添付を条件として複製することができます。

はじめに

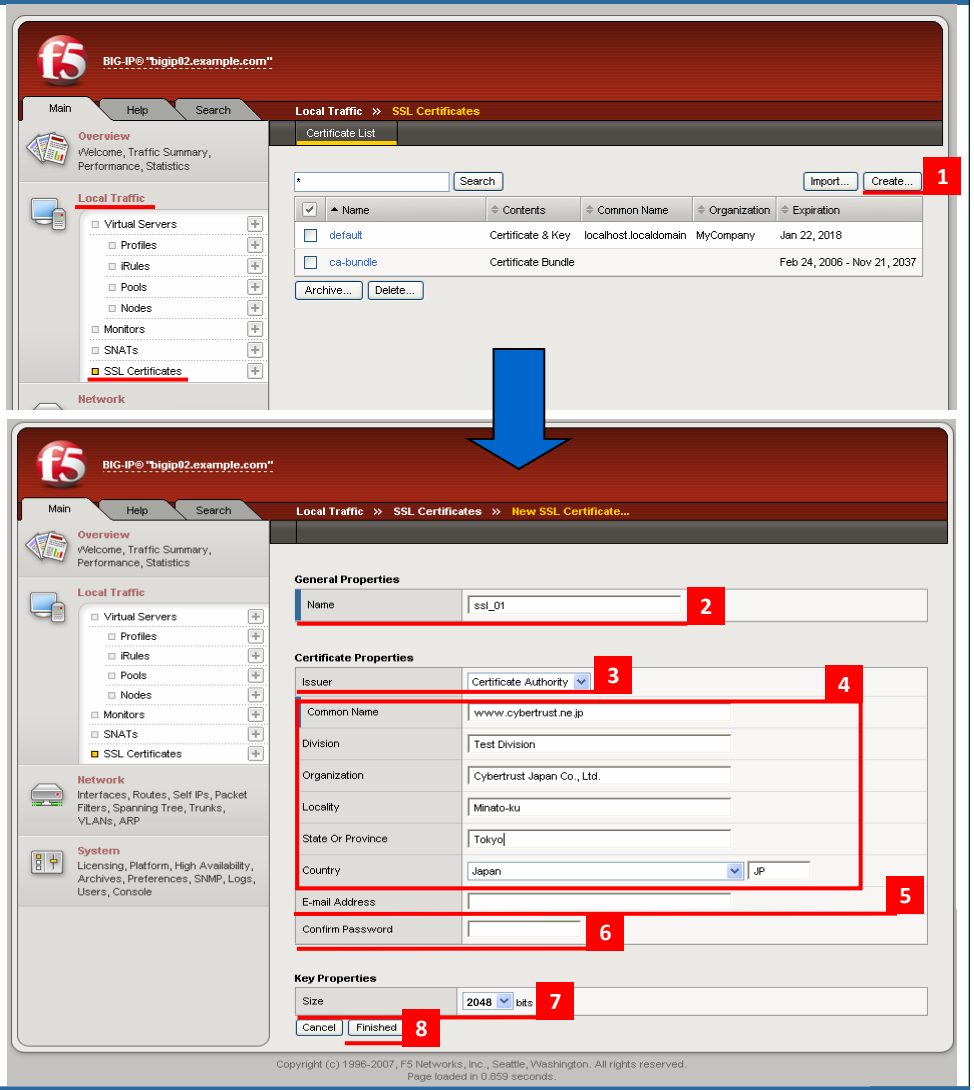
目　次

1. CSR作成手順

■CSRを作成します。

※CSRの作成方法は、以下の弊社ホームページもご参照下さい。
https://www.cybertrust.co.jp/ssl/support/csr.html

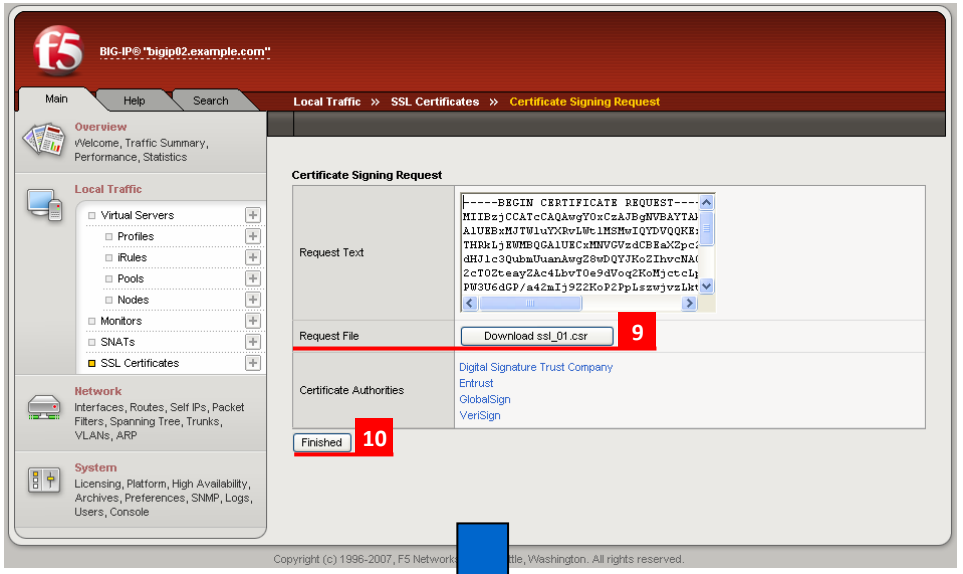
1. [Local Traffic]/[SSL Certificates]を選択し、[Certificate List]から、画面右上の[Create]ボタンをクリックします。
2. [Name]は任意の半角文字を入力します。
3. [Issuer]は[Certificate Authority]を選択します。
4. 証明書識別情報を入力します。
   [Common Name]、[Organization]、[Locality]、[State Or Province]、[Country]の値は必須項目です。
5. [E-mail Address]は任意で入力します。
   ※弊社システムでのご申請時は空欄でも問題ありません。
6. [Confirm Password]は任意で入力します。
   ※弊社システムでのご申請時は空欄でも問題ありません。
7. [Key Properties]の[Size]は「2048」を指定します。
8. [Finished]をクリックします。



1. CSR作成手順

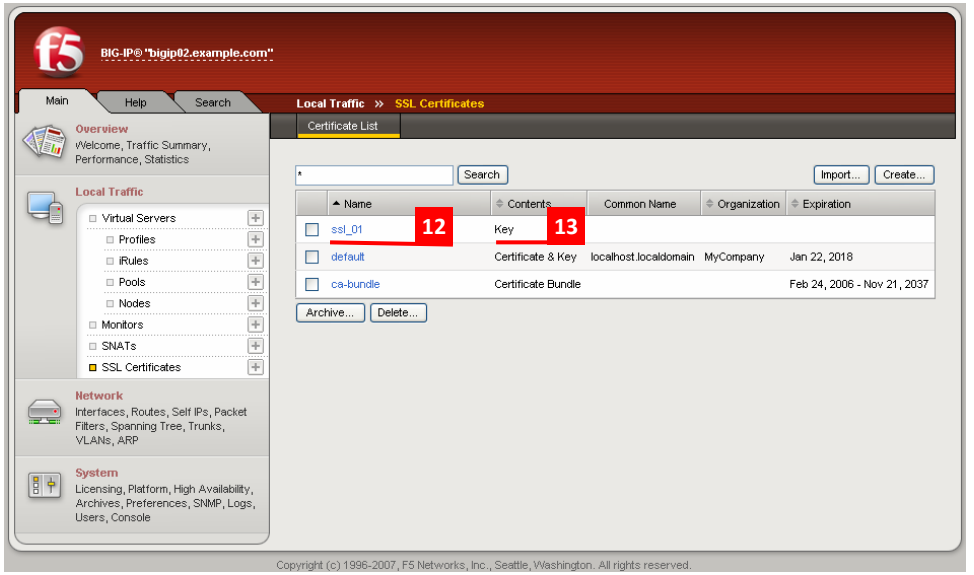
9. [Request File]のダウンロードボタンをクリックしてCSRを任意の場所に保存します。
   ※[Request Text]に表示されている文字列すべてをテキストエディタなどに貼り付けて保存する事も可能です。
10. CSR保存後に[Finished]をクリックします。
11. [Certificate Subject(s)]が[No Certificate]と表示されます。

【！】ここで作成・保存したCSRで申請・発行された「サーバー証明書」のみ[Import]可能ですので、ご留意下さい。。



1. CSR作成手順

12. [Local Traffic]/[SSL Certificates] を選択し、[Certificate List] を再度表示させると、「1.CSR作成手順 - 2.」で入力した [Name]が一覧に表示されます。
13. [Contents]欄の値が[Key]と表示されている事を確認します。
※秘密鍵ファイルのみ保存されている状態となります。



以上で、**CSRの作成は完了です。**

CSR作成後、秘密鍵ファイルのバックアップをご推奨いたします。

秘密鍵ファイルのバックアップ方法につきましては 「7.秘密鍵ファイルエクスポート（バックアップ）」 をご参照下さい。

2. 証明書のお申し込み

■証明書のお申し込みを行います。

作成したCSRをテキストエディタで開いて「-----BEGIN CERTIFICATE REQUEST-----」から、「-----END CERTIFICATE REQUEST-----」までをハイフンを含めすべてコピーし、WEBの申請サイト(※)の申請フォームへ貼り付けて、弊社へお申し込みください。なお、1文字でも欠けると正しく解析できませんのでご注意ください。

※WEBの申請サイトは以下よりご利用いただけます。

▼SureBoard

https://sstra.cybertrust.ne.jp/IRA/loginSb/

▼SureHandsOn

https://sstra.cybertrust.ne.jp/IRA/loginSho/

＜CSRサンプル＞ ※お申し込みにはご利用いただけません。

```
-----BEGIN CERTIFICATE REQUEST-----
.....
MIIEhDCCA2wCAQAwgYkxCzAJBgNVBAYTAkpQMQ4wDAYDVQQIDAVUb2t5bzESMBAG
A1UEBwwJTWluYXRvLWt1MSIwIAYDVQQKDBlDeWJlcnRydXN0IEphcGFuIENvLixM
dGQuMRIwEAYDVQQLDAlUZXN0IFVuaXQxHjAcBgNVBAMMFXRlc3QuY3liZXJ0cnVz
2t/rD9fTPgo7u4aYzw4BpnAqLmGgy3XpsvCo6f4ROcFsgrk05FgeUCaeDFyllEST
.....
-----END CERTIFICATE REQUEST-----
```

弊社にてお申し込み内容の審査を行い、すべてのお手続き完了後にサーバー証明書を発行いたします。(発行はメールにてお知らせいたします。)

サーバー証明書が発行されましたら、次のステップへお進みください。

3. 証明書のダウンロード

■インストールが必要となるサーバー証明書と中間CA証明書を事前にダウンロードします。

【1】サーバー証明書のダウンロード

サーバー証明書が発行されましたら、証明書発行のお知らせのメール内リンクより事前にダウンロードし、【.cer】や【.txt】などの拡張子で保存してください。

※サーバー証明書のダウンロードについては、以下をご参考ください。

https://www.cybertrust.co.jp/ssl/support/download.html

【2】中間CA証明書のダウンロード

サーバー証明書をご利用の際、お使いの機器へ中間CA証明書のインストールが必要となります。

ご選択いただいた商品により必要な証明書が異なりますので、証明書の種類をご確認のうえ、以下弊社ホームページからダウンロードしてください。

▼ルート・中間CA証明書のダウンロード

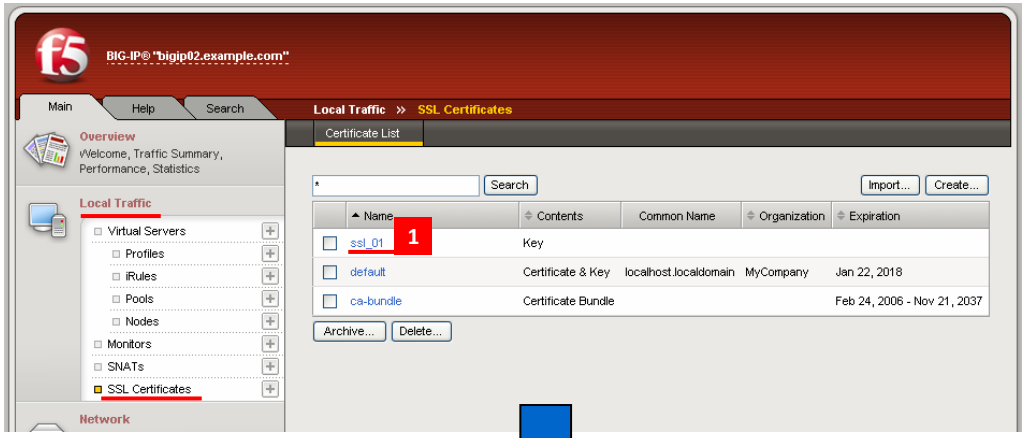
https://www.cybertrust.ne.jp/ssl/download-ca/

4. 証明書のインストール

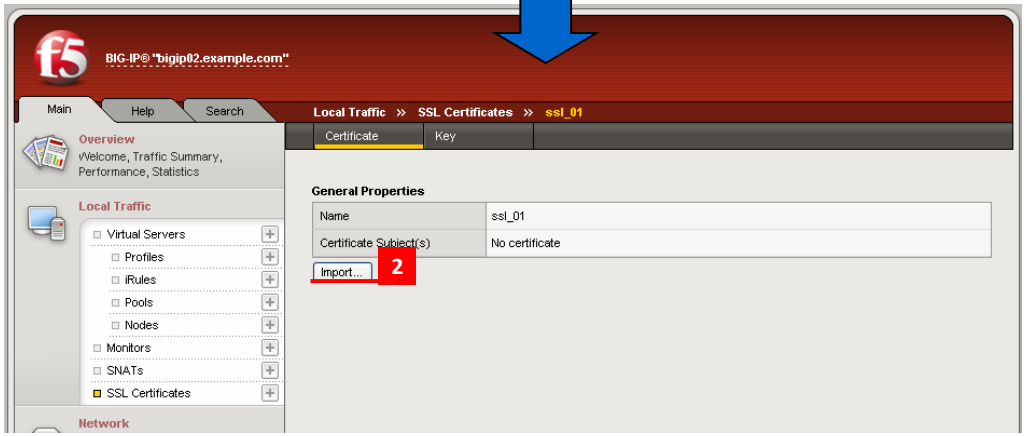
■サーバー証明書と中間CA証明書をインストールします。

【1】サーバー証明書のインストール

1. [Local Traffic]/[SSL Certificate]を選択し、[Certificate List]から、「CSR」を作成した[Name] をクリックします。

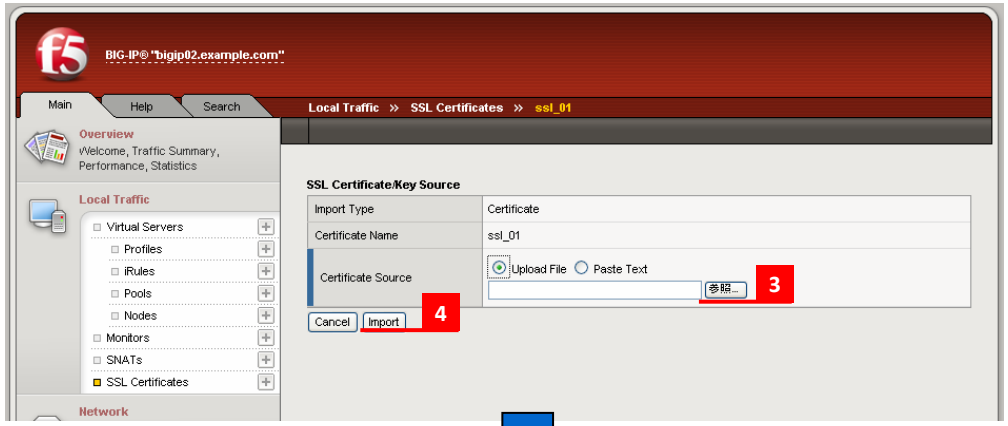


2. [Import]をクリックします。

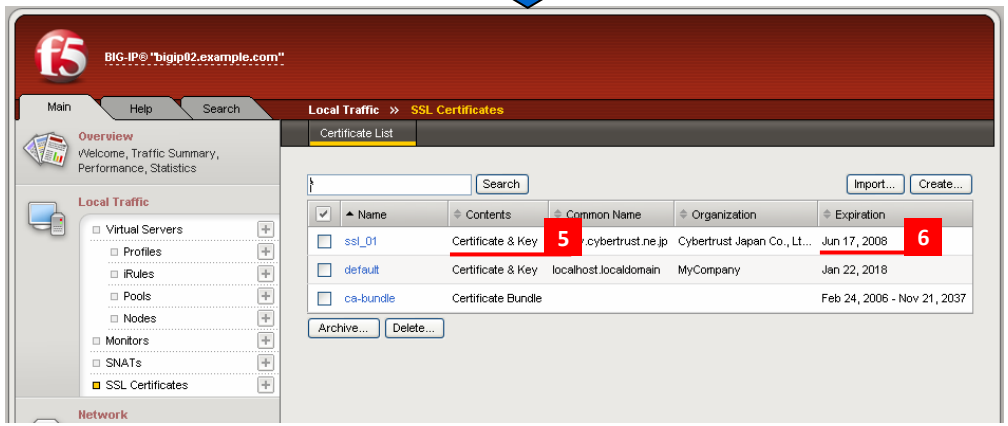


4. 証明書のインストール

3. [参照]ボタンをクリックし、発行されたサーバー証明書ファイル（デフォルトファイル名は「7桁の数字.cer」）を選択します。
4. サーバー証明書を選択後、[Import]をクリックします。



5. [Certificate List]中の、[Contents]欄の表示が 「Key」から「Certificate & Key」と変化した事を確認します。
6. 有効期限が最新の日付になっている事を確認します。



以上でサーバー証明書のインストールは完了です。

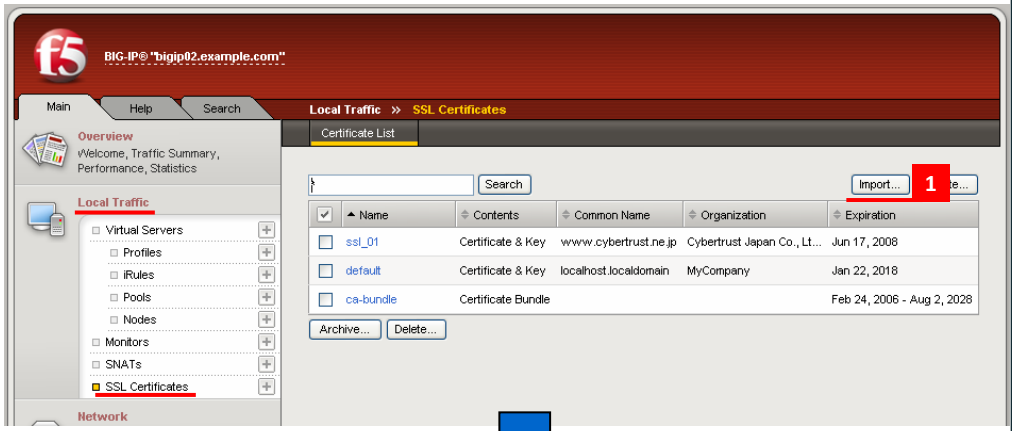
続いて、中間CA証明書のインストールを行います。

4. 証明書のインストール

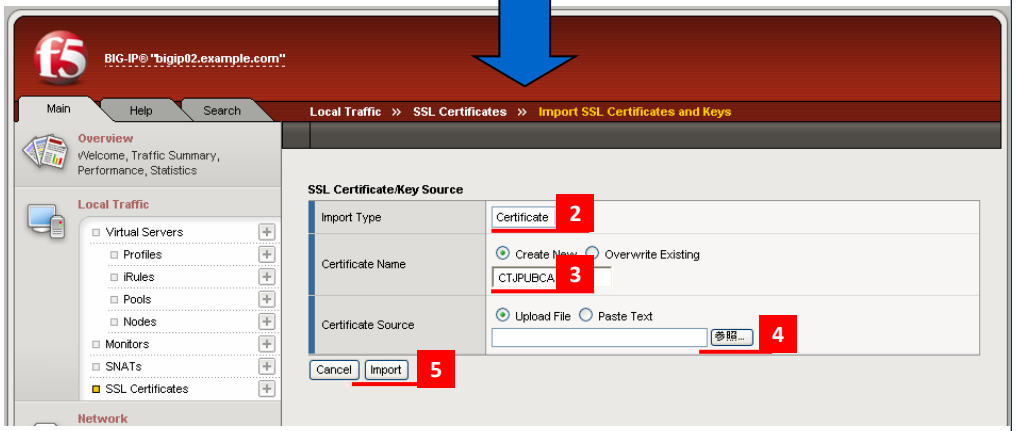
【2】中間CA証明書のインストール

※必要な中間CA証明書がすでにインストールされている場合は、設定不要です。

1. [Local Traffic]/[SSL Certificate]を選択し、[Import] をクリックします。

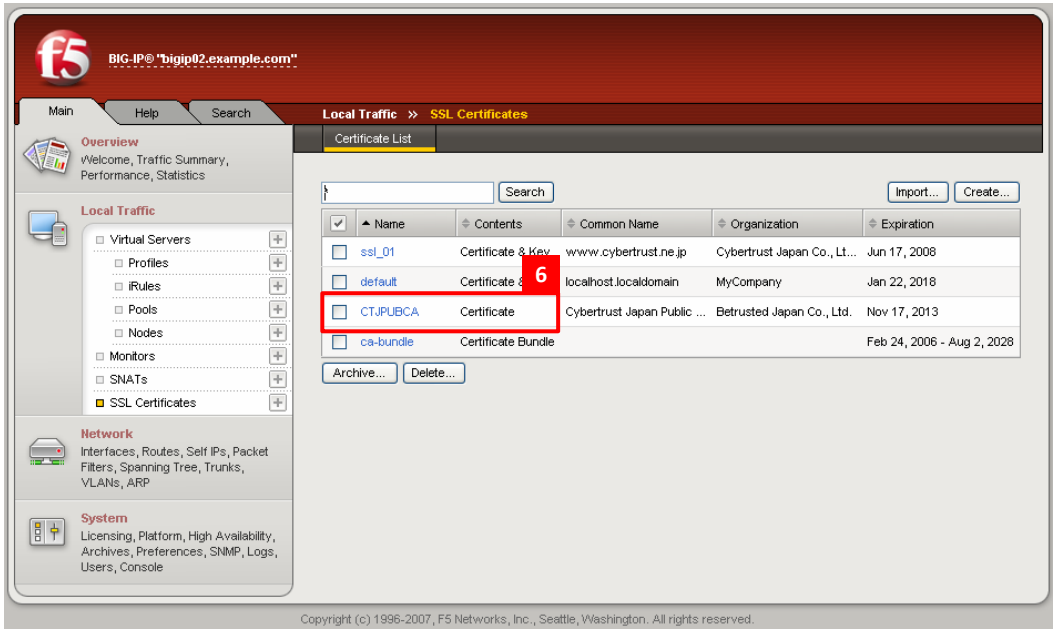


2. [Import Type]は「Certificate」を選択します。
3. [Certificate Name]は任意の名前を入力します。
4. [参照]をクリックし、あらかじめテキスト形式でダウンロードした中間CA証明書を選択します。
5. 中間CA証明書の選択後、「Import」をクリックします。



4. 証明書のインストール

6. 前ページの[Certificate Name]へ入力した名前が、一覧に表示されますので、[Contents] 欄の表示が「Certificate」である事を確認します。



以上で中間CA証明書のインストールは完了です。

【！】クロスルート証明書をご利用の場合（2025年6月1日現在、クロスルート証明書は提供しておりません）

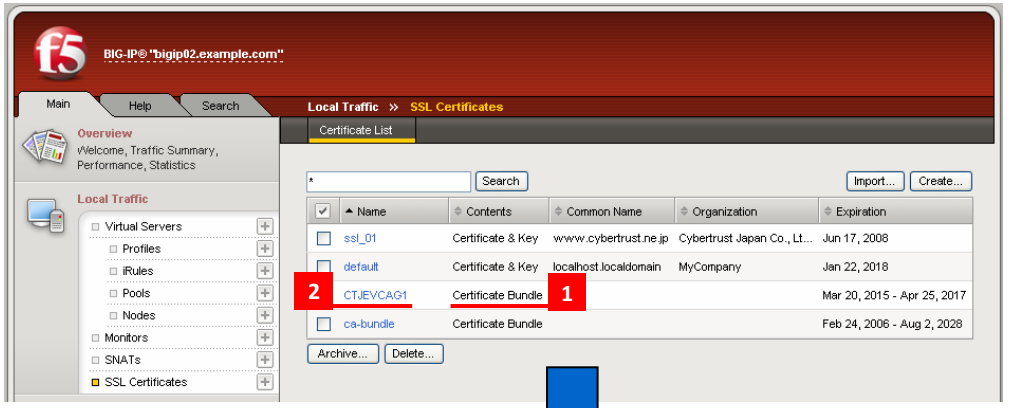
2種類の中間CA証明書を連結して1つにしたファイルは、[Contents] 欄の表示が「**Certificate Bundle**」と表示されます。

詳細は次ページ（P13）をご参照下さい。

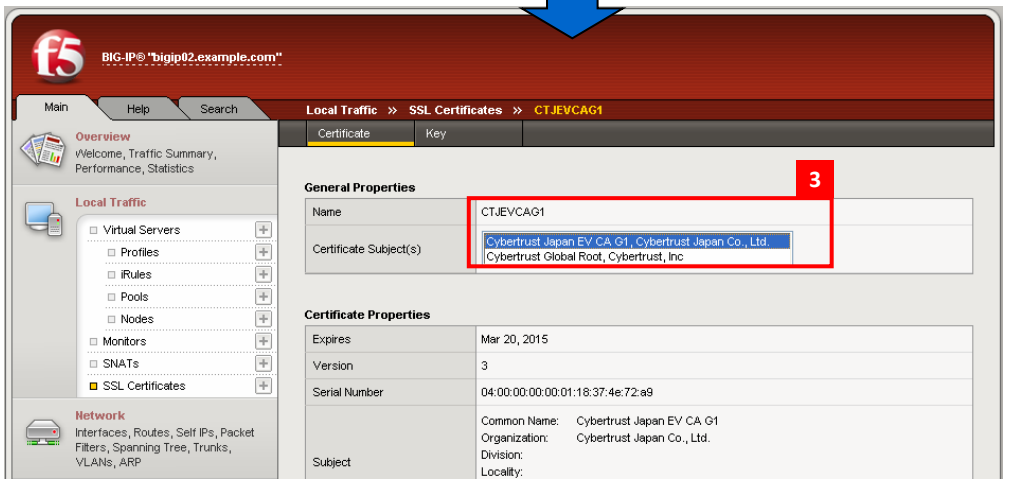
4. 証明書のインストール

【ご参考】2種類の中間CA証明書を連結して1つにしたファイルの確認方法

1. 2種類の中間CA証明書を連結して1つにしたファイルをインストールした場合、[Contents]欄の表示が「**Certificate Bundle**」と表示されます。
2. インストール時に入力した任意の[Name]をクリックし、詳細を確認します。



3. [Certificate Subject(s)]に2つの証明書情報が表示されている事を確認します。



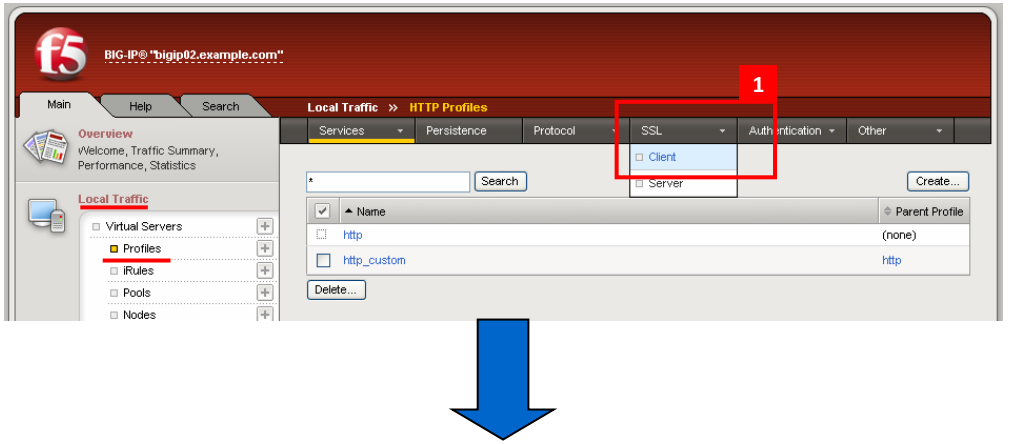
5. 証明書インストール後の設定（例）

■サーバー証明書および中間CA証明書インストール後の設定

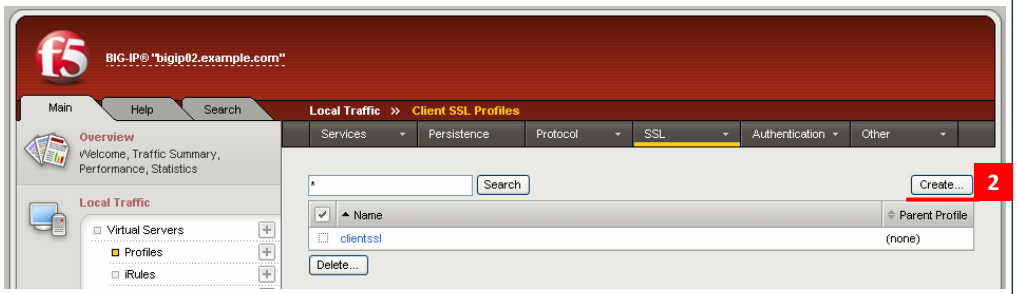
設定方法は例となります。詳細の設定方法につきましては、マニュアルなどをご参照下さい。

【1】プロファイルの作成

1. [Local Traffic]/[Profiles]を選択し、[SSL]タブの「Client」を選択します。



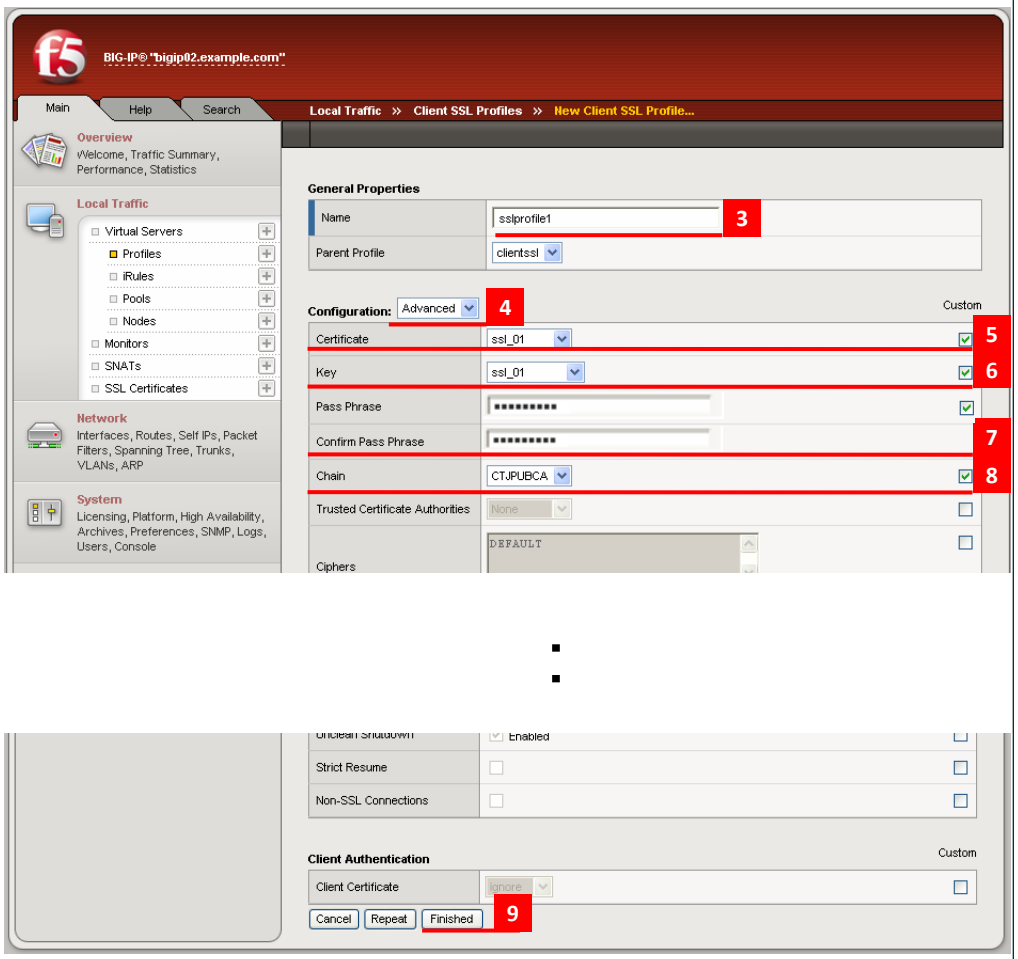
2. [Client SSL Profiles]が表示されます。 新しいプロファイルを作成する場合、「Create」をクリックします。



5. 証明書インストール後の設定(例)

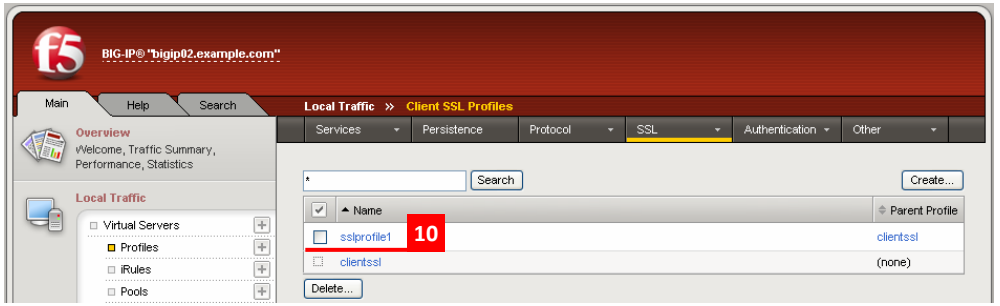
3. [Name]に任意の半角文字を入力します。
4. [Configuration]は「Advanced」を選択します。
5. [Certificate]の「Custom」ボックスにチェックをし、サーバ証明書の[Name]を選択します。
6. [Key]の「Custom」ボックスにチェックをし、秘密鍵ファイルの[Name]を選択します。
7. [Pass Phrase]の[Custom]ボックスにチェックをし、[Pass Phrase]と[Confirm Pass Phrase]を入力します。
8. [Chain]の「Custom」ボックスにチェックをし、中間CA証明書の[Name]を選択します。

9. [Finished]をクリックします。



5. 証明書インストール後の設定(例)

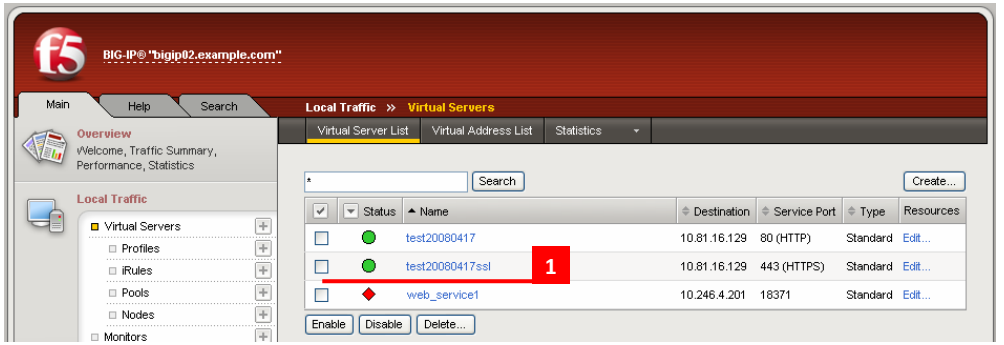
10. [Client SSL Profile]が新しく作成された事を確認します。



【2】仮想サーバーへのプロファイル適用

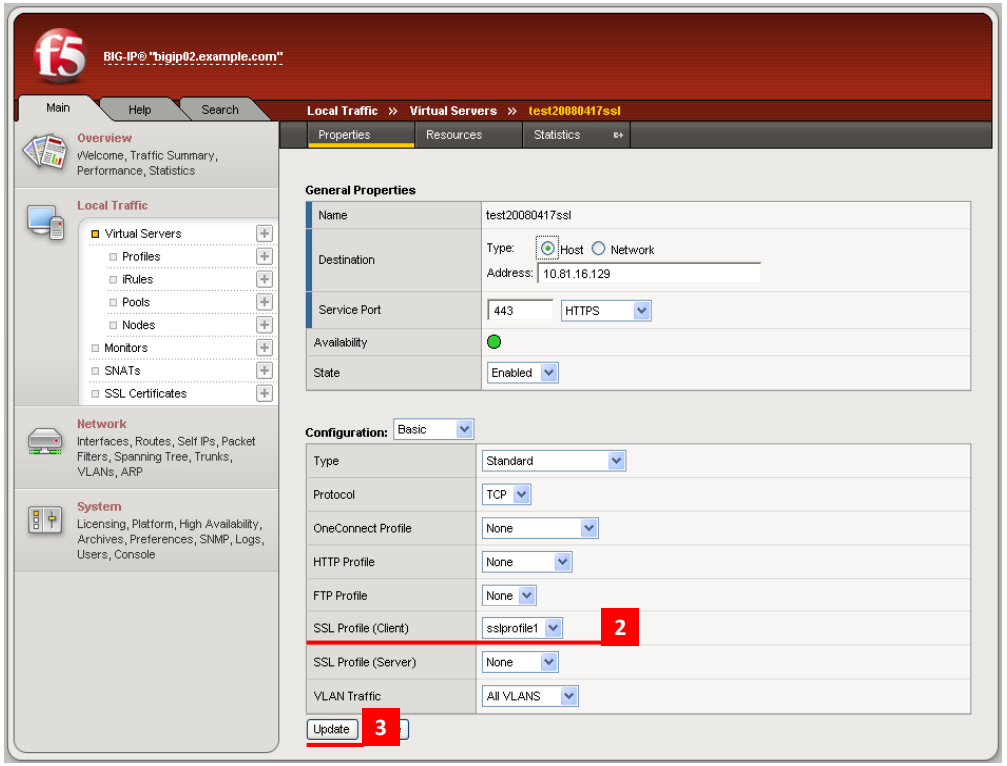
※本項は、仮想サーバーがあらかじめ設定されており、[Service Port]が「443(HTTPS)」である事を前提としています。

1. [Local Traffic]/[Virtual Servers]を選択し、[Virtual Server List] から、SSL通信を行いたい任意の仮想サーバーを選択します。



5. 証明書インストール後の設定（例）

2. [SSL Profile (Client)]の値を、作成したプロファイル名に変更します。
3. [Update]をクリックします。



証明書インストール後の設定は以上で終了です。

※その他詳細設定およびサーバーの起動方法につきましては、マニュアルをご参照下さい。

6. SSL通信の確認

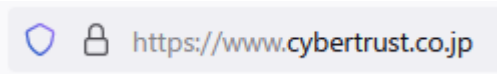
サーバー証明書が正しく設定され、エラーやセキュリティ警告が表示されず、正常にSSL通信が可能であることを確認します。

- SSL通信の確認は設定を行っているサーバー以外のWEBブラウザやスマートフォンなどの携帯端末、弊社「SSLサーバ証明書　導入サポートツール」のサーバ証明書の設定確認から行うことを推奨します。

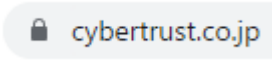
■設定確認例

<Edge>

<Firefox>



<Chrome>



※接続時にセキュリティ警告やエラーが表示される場合は、以下よくある質問の「SSL通信時のセキュリティ警告やエラーについて」をご参照ください。

https://www.cybertrust.co.jp/ssl/support/faq/

7. 秘密鍵ファイルエクスポート（バックアップ）

1. [Local Traffic]/[SSL Certificate]を選択し、バックアップを行う秘密鍵ファイルの[Name]をクリックします。
2. [key]タブを選択し、[Export]ボタンをクリックします。
3. [Key File]のダウンロードボタンをクリックして秘密鍵ファイルをメディア（USBやCD等）にコピーして保存します。

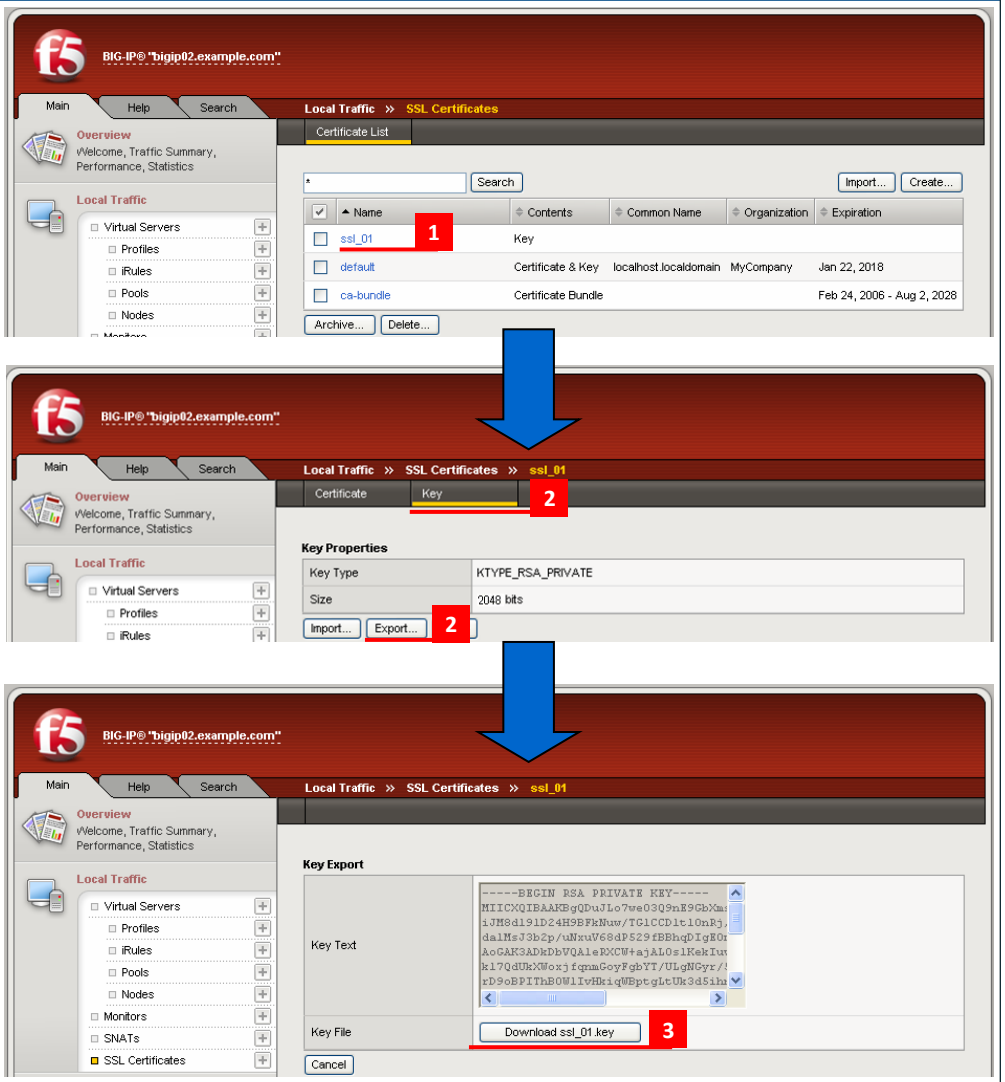
秘密鍵ファイルのバックアップは以上で終了です。

【！】注意事項

・パスワードを紛失した場合には、バックアップに利用できなくなりますので、取り扱いには十分注意してください。

・バックアップファイルは安全な場所に保管してください。

・弊社がお客様の秘密鍵ファイルの情報を受け取ることはございません。あらかじめご了承ください。



8. 秘密鍵ファイルインポート

1. [Local Traffic]/[SSL Certificate]を選択し、[Import]をクリックします。

2. [Import Type]に「key」を選択します。
3. [Key Name]に任意の名前を入力します。
4. [参照]ボタンをクリックし、インポートを行いたい秘密鍵ファイルを選択します。
5. 秘密鍵ファイルの選択後、[Import]をクリックします。

6. インポートした[Key Name]の表示が確認できます。

秘密鍵ファイルのインポートは以上で終了です。