

(参考資料としての利用に限る)

ikeyman/IBM HTTP Server サーバ証明書インストール方法

1. はじめに

IBM HTTP Server 環境下での、サーバ証明書インストール手順を以下に説明します。

大まかな手順は以下のとおりですが、必要に応じ提供元の詳細情報もご参照ください。

<http://www-01.ibm.com/software/webervers/httpservers/doc/v52/jpn/icswg021.html>

- (1) ルート証明書のインストール
- (2) 中間証明書のインストール
- (3) お客様に発行されたサーバ証明書のインストール
- (4) IBM HTTP Server の httpd.conf の設定および再起動、動作確認

ディレクトリ等は、セットアップされる環境に合わせて読み替えてください。

2. 証明書の受理とインストール準備

証明書が発行されますと、**お客様のサーバ証明書（エンド証明書）**が添付ファイルとしてメールにて送信されますので、名前をつけて保存します。

2.1 お客様のサーバ証明書の受理と保存

お客様のサーバ証明書は、発行時のメールに添付されていますので、名前をつけて IBM HTTP Server に保存します。 仮にファイル名は YOURSERVER.crt とします。

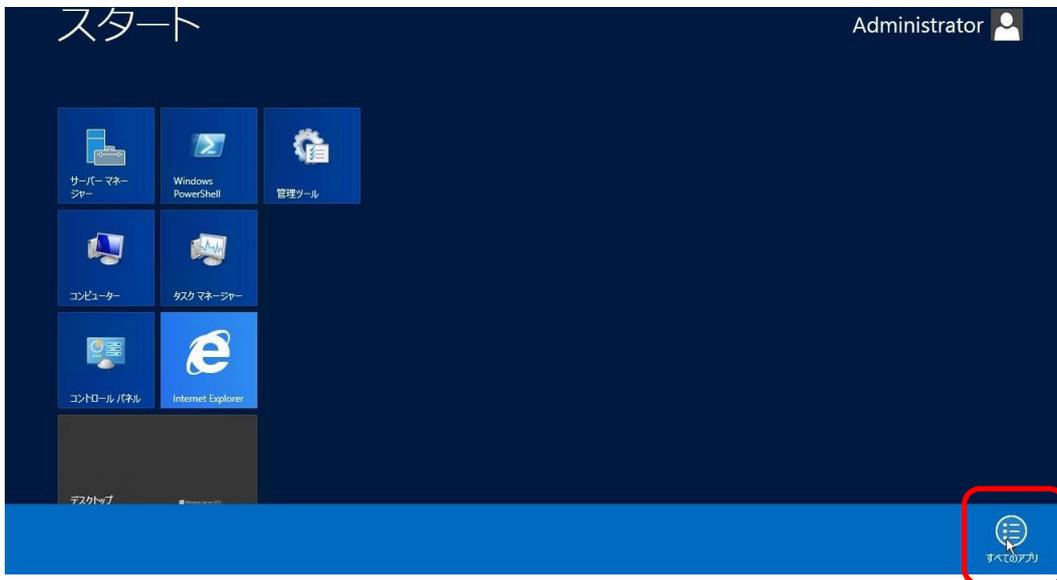
2.2 ルート証明書および中間 CA 証明書の受理と保存

サーバ証明書を IBM HTTP Server で使用するには、ルート証明書および中間 CA 証明書が必要になります。ルート証明書および中間 CA 証明書 (intermediate.crt) は、「証明書を設定する前に (準備作業)」をご一読頂き、中間証明書一覧から取得してください。 <https://www.jcert.co.jp/support/certificate/>

保存したルート証明書および中間 CA 証明書のファイル名を仮に YOURSERVER.root.crt および YOURSERVER.sf_intermediate.crt へと変更します。

3. ikeyman への証明書ファイルのインストール

Windows の場合、Windows キーを押して【スタートメニュー】を表示し右クリックから【すべてのアプリ】にアクセスします。



一覧画面から【開始キー管理ユーティリティ】にアクセスします。



Unix の場合、ikeyman と入力してください。

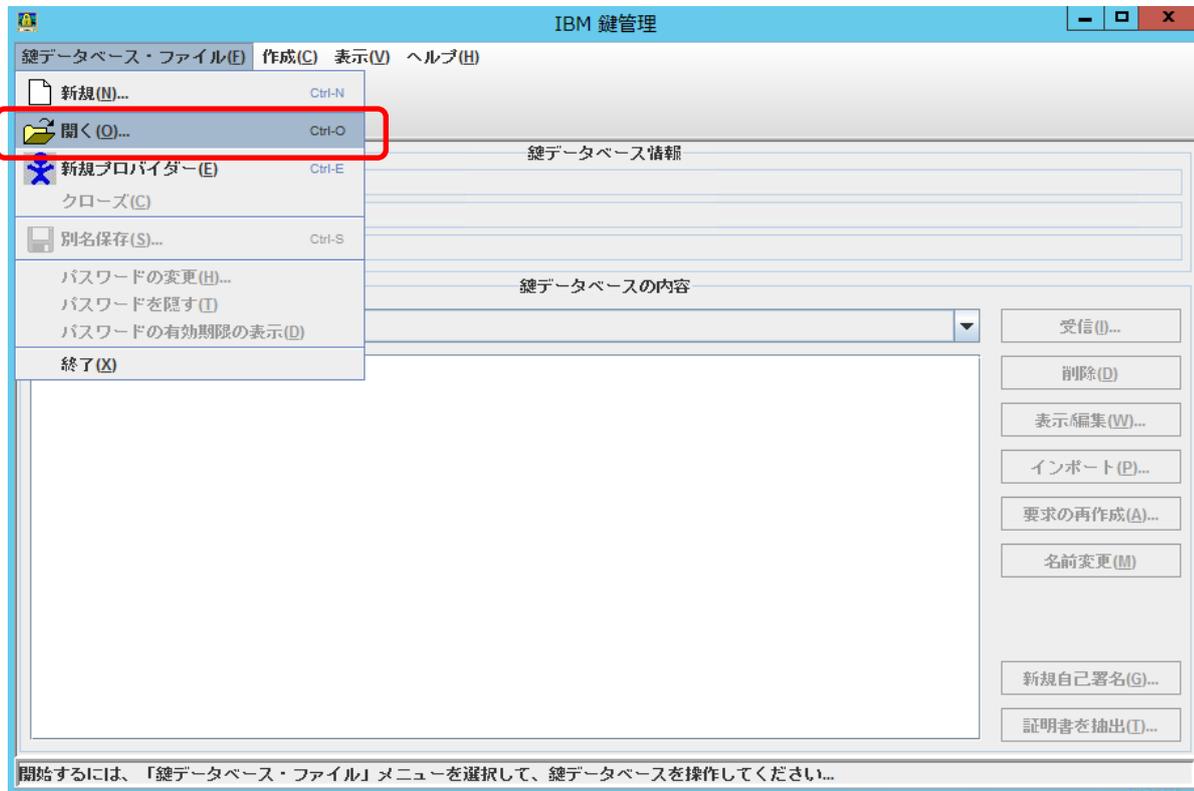
ikeyman が見つからない場合、インストールパスを含めて指定します。

プログラムの初期インストールパスは /opt/IBM/HTTPServer/bin/ になります。

初期インストールパスの場合は /opt/IBM/HTTPServer/bin/ikeyman と実行します。

3.1 ルート証明書および中間証明書のインストール

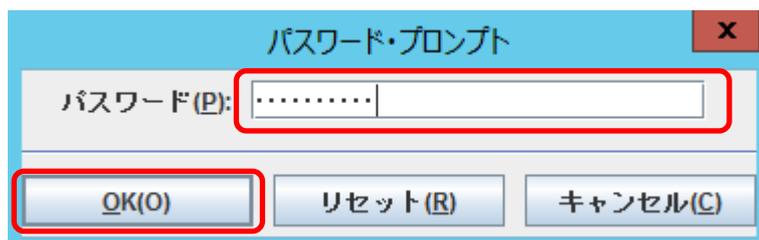
- メニューラインの【鍵データベース・ファイル】->【開く】を選択してください。



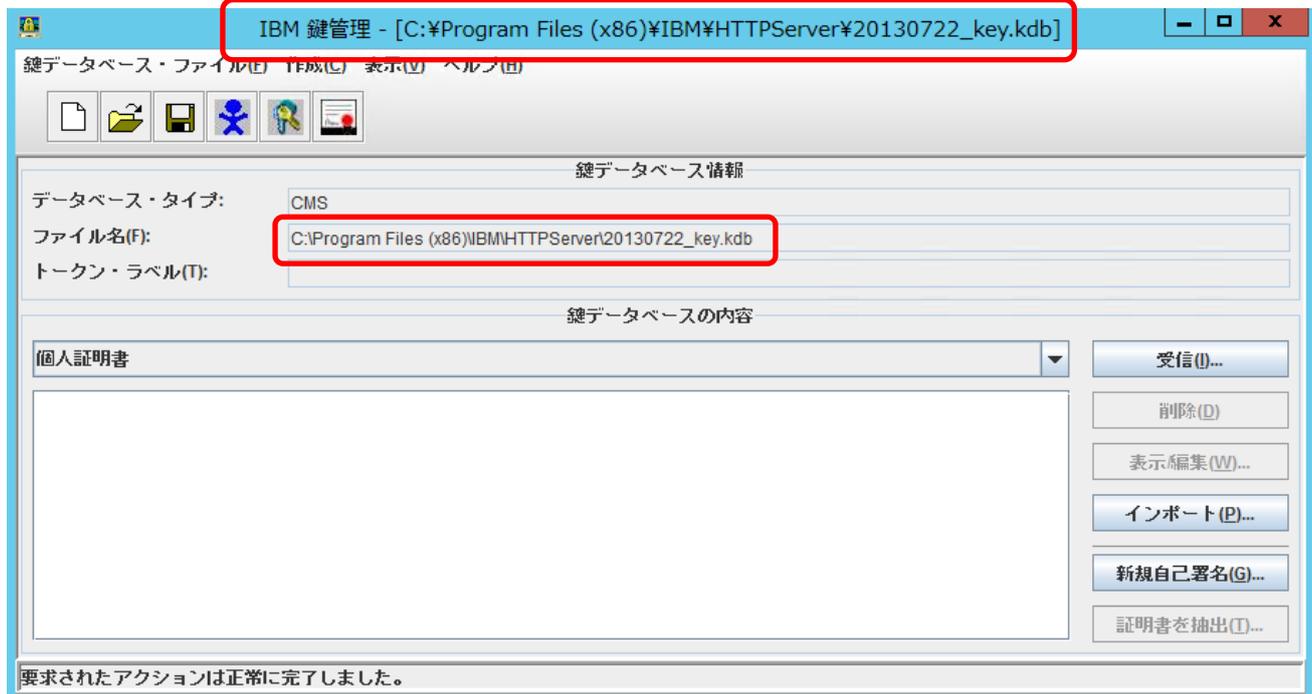
- 【ファイル名】、【場所】に CSR 生成時に作成した鍵データベースファイルを入力し、【OK】をクリックします。



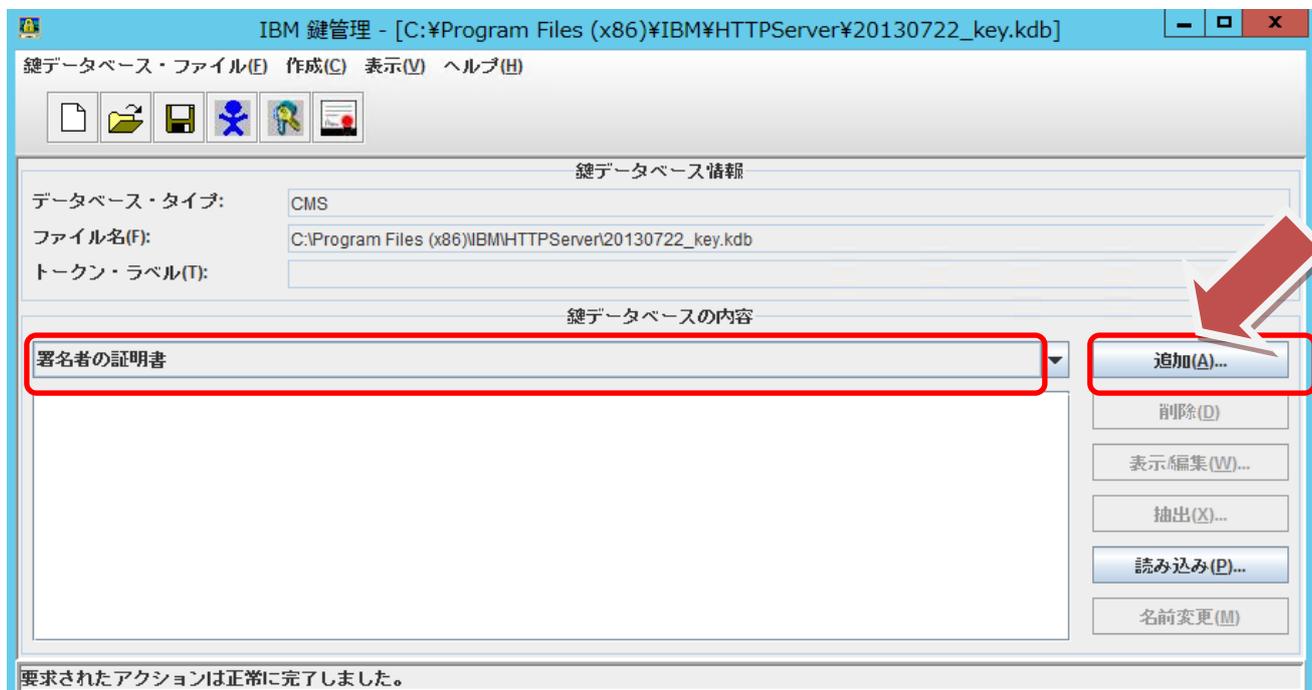
- 鍵データベースファイルのパスワードを入力し【OK】をクリックします。



タイトル、ファイル名が対象の鍵データベースファイル名を示していることを確認して下さい。



鍵データベース内容を【署名者の証明書】に変更し、【追加】を選択してください。

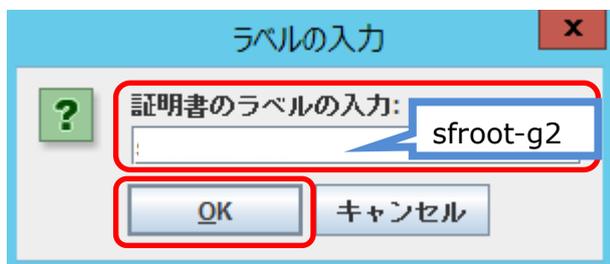


次に現れる画面で、ルート証明書ファイル YOURSERVER.root.crt を参照のうえ選択し、【OK】をクリックします。(中間証明書の場合には、YOURSERVER.sf_intermediate.crt を選択)

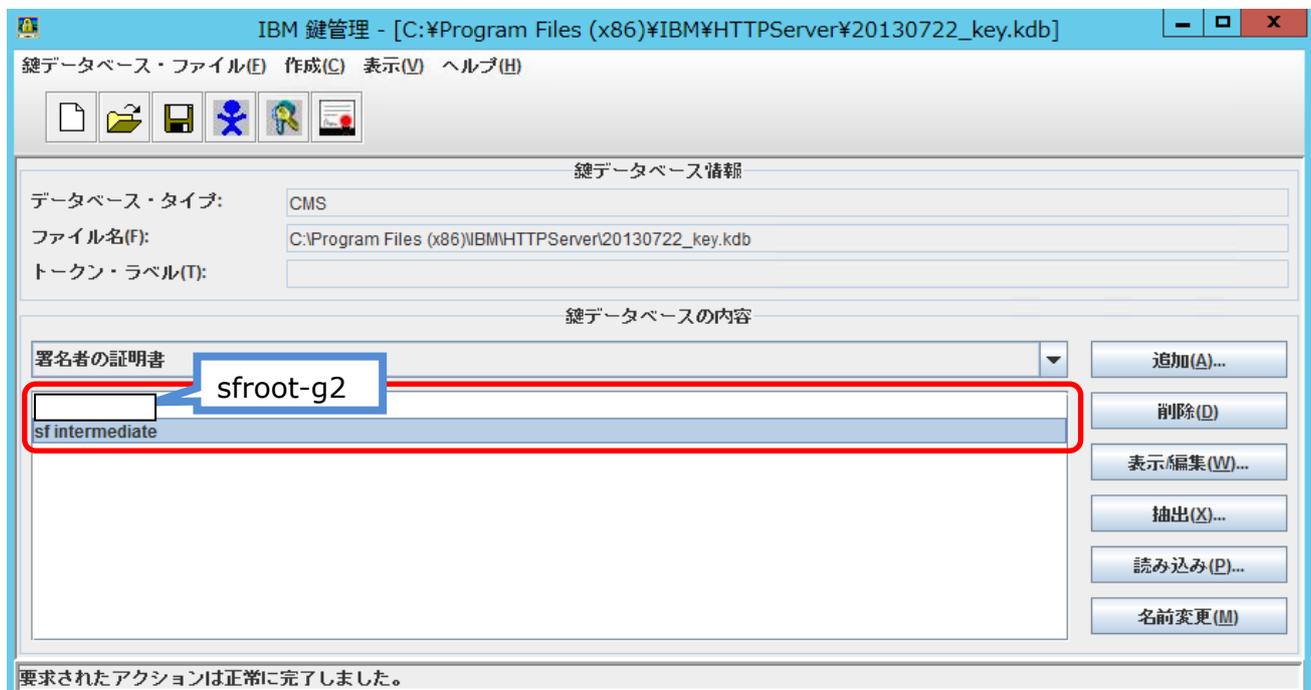
なお、かならず「ルート証明書」->「中間証明書」の順でインストールするようにしてください。



証明書のラベルは分かり易い名前、たとえば **sfroot-g2** あるいは **gdroot-g2** と入力し、【OK】をクリックします。(中間証明書の場合には、**sf intermediate** あるいは **gd intermediate** を入力)

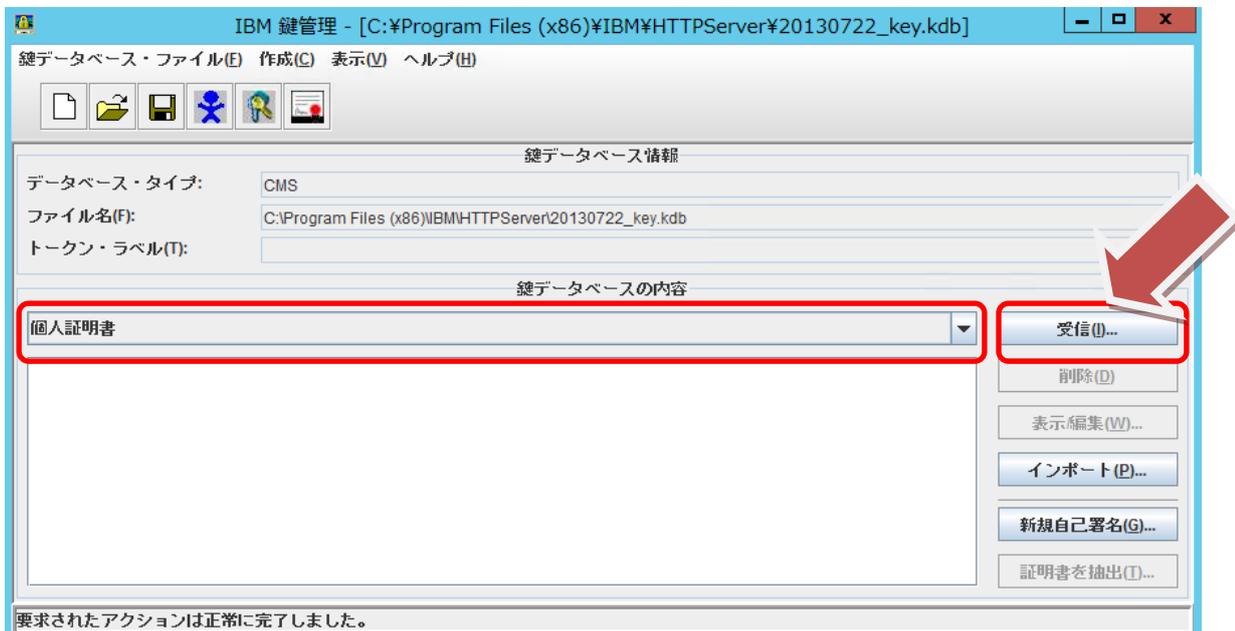


「ルート証明書」、「中間証明書」の登録後は以下のように上記で設定したラベル名で表示されます。



3.2 サーバ証明書のインストール

鍵データベース内容を【個人証明書】とし、【受信】を選択してください。



次に現れる画面で、お客様サーバ証明書ファイル YOURSERVER.crt を参照のうえ選択し、【OK】ボタンを押してください。



「証明書」の登録後は以下のように表示されます。
 鍵ラベル名に登録された名前が表示されています。ここでは「server」。



4. IBM HTTP Server の httpd.conf の設定および再起動、動作確認

4.1 httpd.conf の設定

詳細は IBM HTTP Server 付属マニュアルを参照してください。

※初期インストールパスの場合 C:\Program Files (x86)\IBM\HTTPServer\conf\httpd.conf になります。

上記で開いたファイルの以下の行を書き換えます。

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen [IP address]:443
...
<VirtualHost :[Common Name/FQDN]: 443>
    SSLENABLE
    SSLClientAuth 0
    SSLServerCert [鍵ラベル]
    Keyfile [/path/key.kdb:鍵データベースファイルまでの絶対パス]
</VirtualHost>
...
```

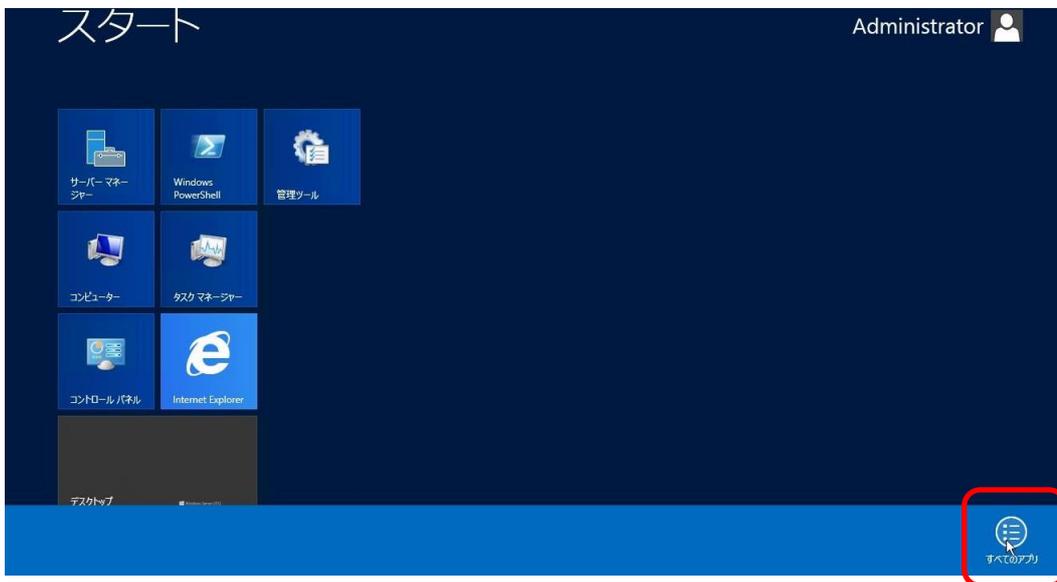
4.2 IBM HTTP Server の再起動

IBM HTTP Server 付属のマニュアル等にしたがって、IBM HTTP Server を再起動します。

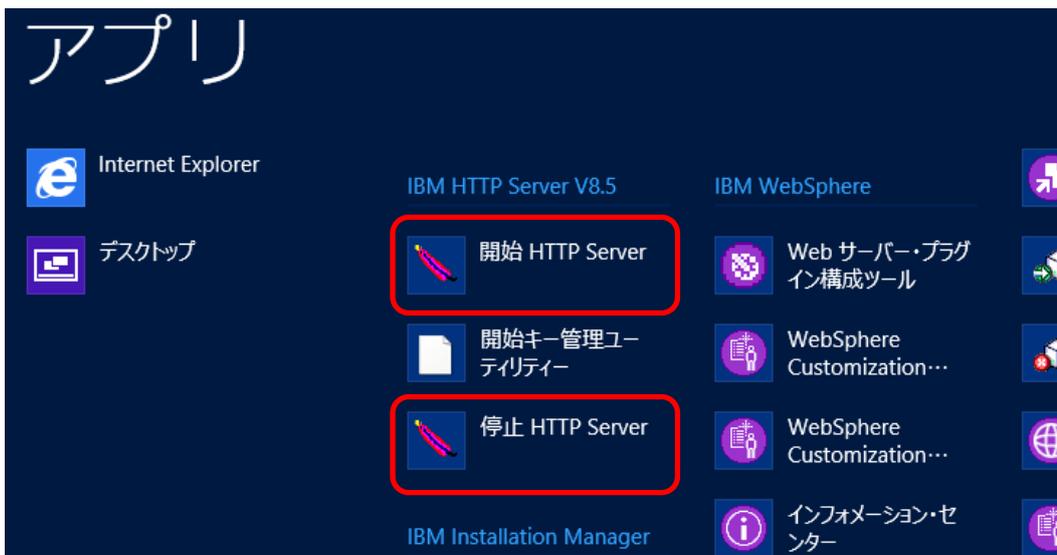
他の PC から証明書をインストールしたサイトにアクセスし、SSL の正常動作を確認します。

再起動操作の一例は以下の通りです。

Windows の場合、Windows キーを押して【スタートメニュー】を表示し右クリックから【すべてのアプリ】にアクセスします。



一覧画面から【停止 HTTP Server】、【開始 HTTP Server】を順にクリックします。



Unix の場合、`apachectl` コマンドを実行します。

プログラムの初期インストールパスは `/opt/IBM/HTTPServer/bin/apachectl` になります。

初期インストールパスの場合の再起動は以下のように行います。

再起動: `/opt/IBM/HTTPServer/bin/apachectl restart`

5. 外部生成した「秘密鍵+証明書」のインポート
別途、当社お客様限定の詳細なる資料を用意しております。

<https://jstore-v2.jcert.co.jp/user/contact>

からお問い合わせ下さい。

この文書に記載されている情報は予告なしに変更されることがあります。この文書に記載されている情報に従ってユーザーが操作を行った結果、ユーザーが被る損害については、ジェイサートでは一切責任を負いません。ユーザーは自己責任においてのみ、この文書を使用するものとします。