

(参考資料としての利用に限る)

iKeyman/IBM HTTP Server CSR ファイル作成方法 (新規・更新)

1. はじめに

IBM HTTP Server 環境下での、CSR 作成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>

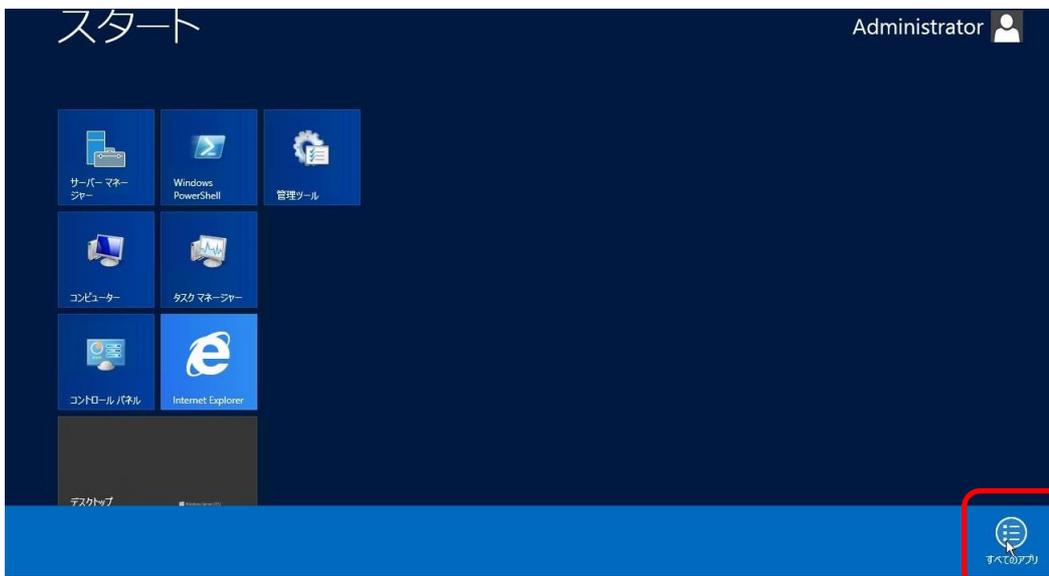
- (1) 鍵データベースファイルの作成
- (2) CSR の作成
- (3) CSR をジェイサートへお送りいただく

2. 鍵データベースファイルの作成

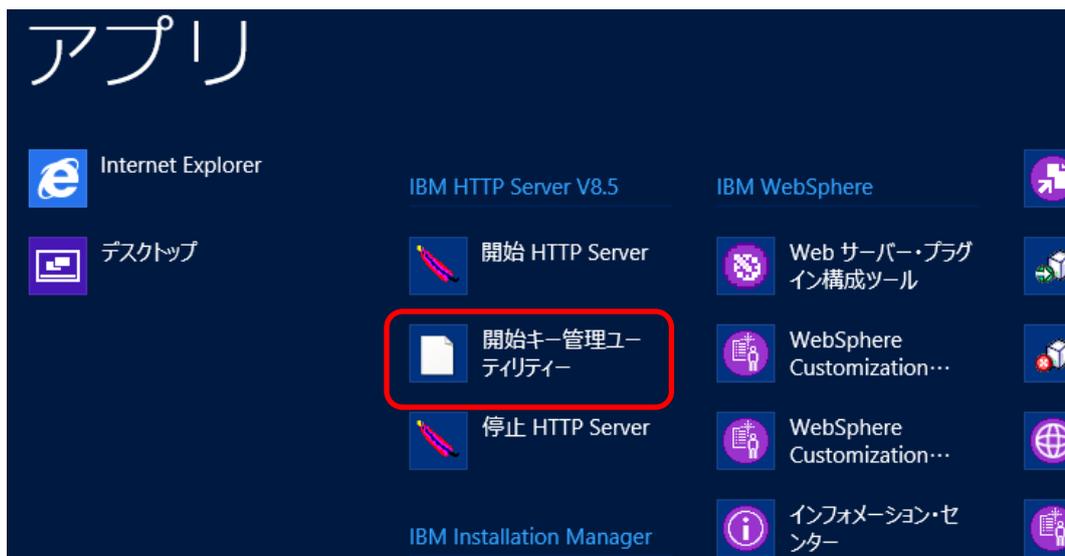
鍵データベースファイルは、IBM HTTP Server において、秘密鍵やサーバ証明書を管理するデータベースファイルです。一つの鍵データベースファイルに複数の鍵ペアを生成することや、1 台のサーバに複数の鍵データベースファイルを作成することも可能です。以下、鍵データベースファイルの作成手順になります。

2.1 IBM 鍵管理 (iKeyman) の起動

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。



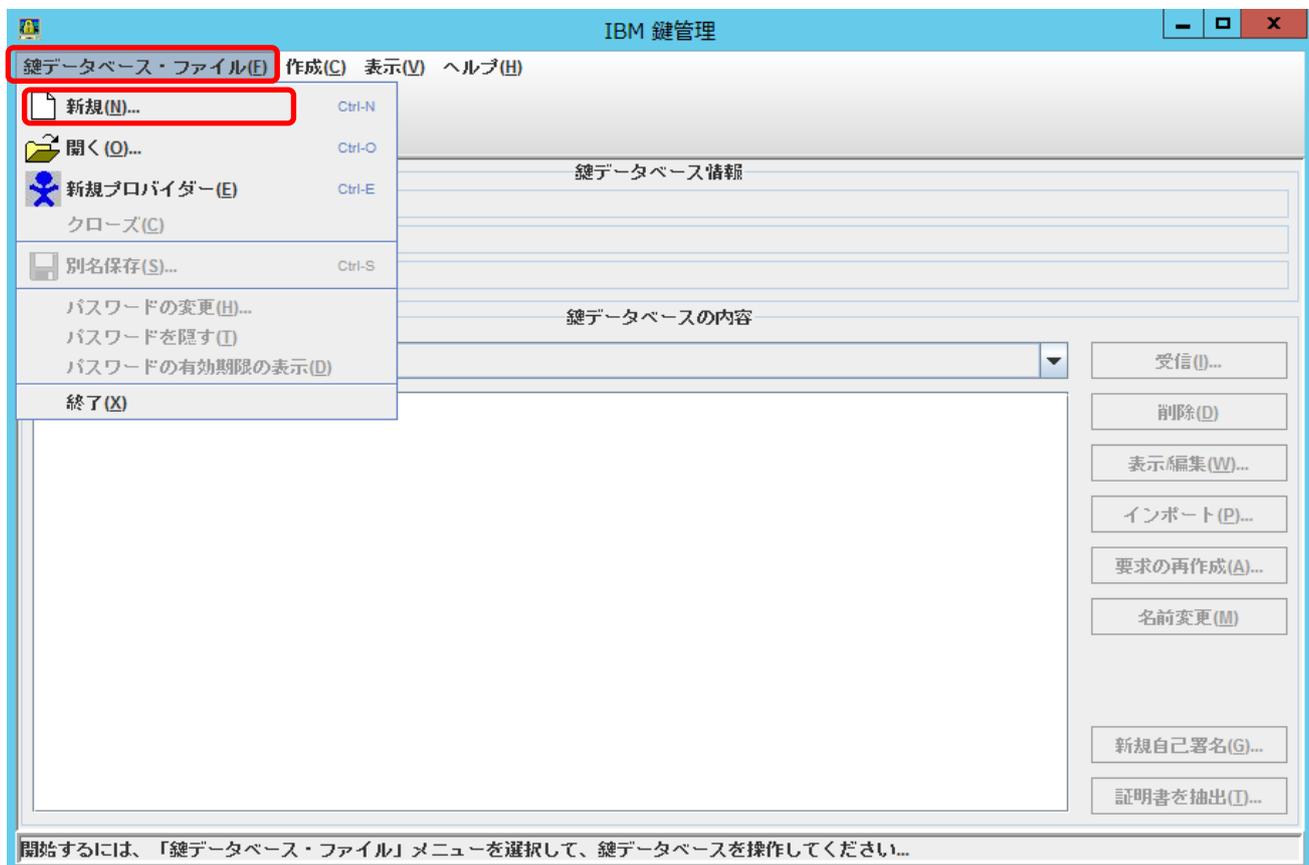
Unix の場合、ikeyman と入力してください。

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。

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



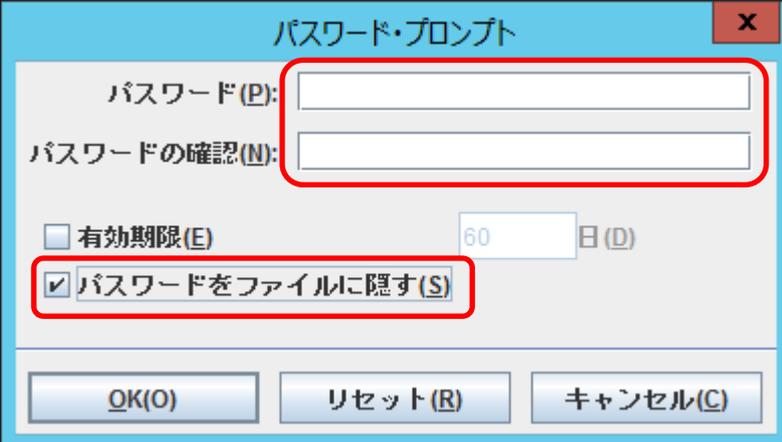
- 鍵データベース・タイプ：CMS を選択。
- ファイル名（鍵データベースファイル出力先）：デフォルトでは“key.kdb”となっていますが、作成日時が認識できる任意のファイル名とすることをお勧めします。**（くれぐれも既存鍵データベースファイルに上書きしないように注意してください！）**
- 場所：デフォルトでは、C:\Program Files (x86)\IBM\HTTPServer となっていますが、任意に設定してください。

入力後【OK】をクリックして下さい。

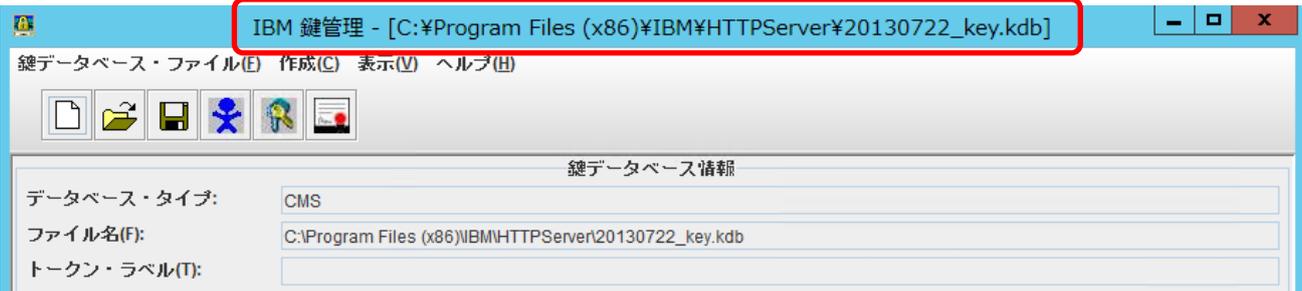


2.3 任意のパスワードを設定して、【OK】をクリックしてください。

- 【パスワードをファイルに隠す】を選択することをお勧めします。

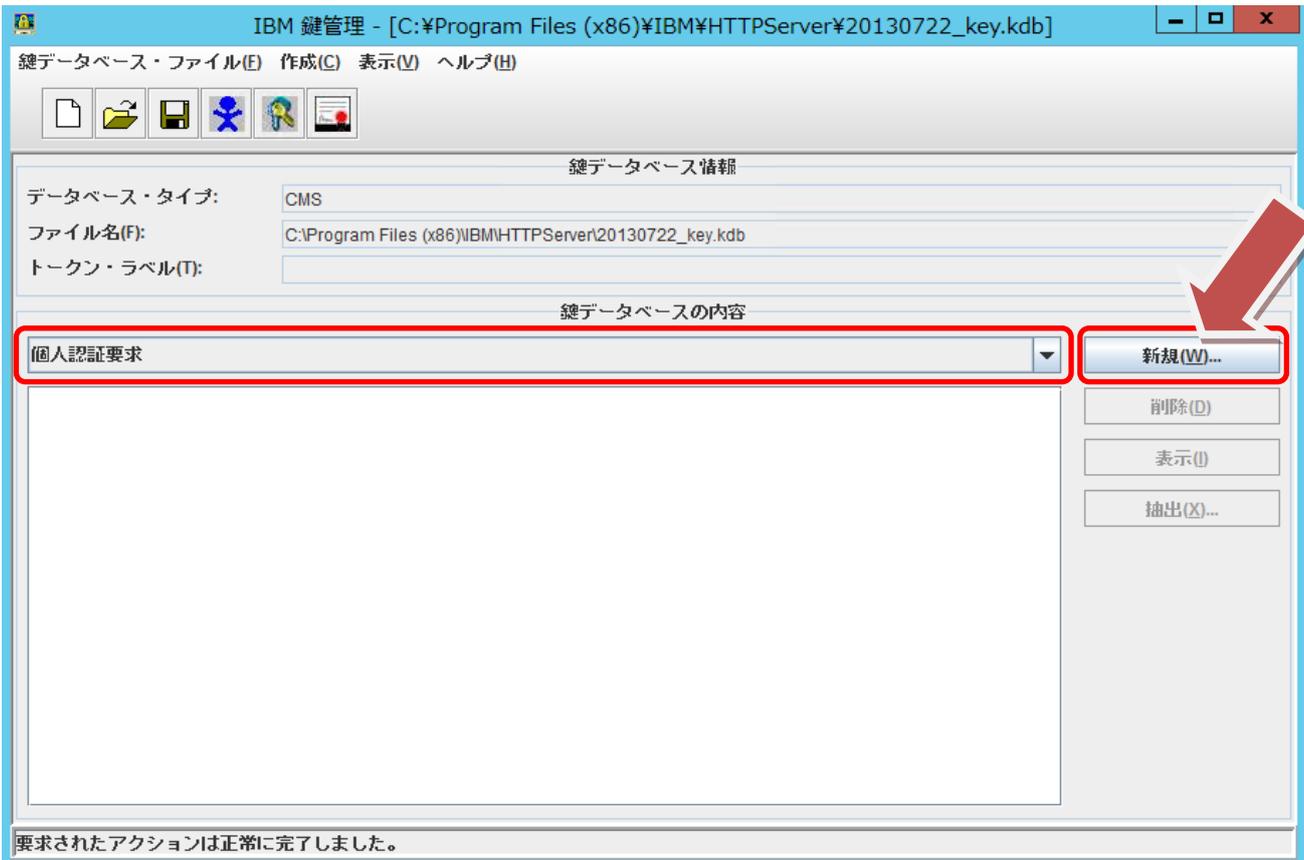


タイトルバーにファイル名が表示されていれば、鍵データベースファイルの作成が完了です。



3. CSR の生成

3.1 鍵データベース内容を【個人認証要求】とし、【新規】を選択してください。



3.2 CSR 情報登録画面で以下に即し情報入力を完了してください。

- 鍵ラベル：鍵ラベルにより 1 つの秘密鍵を特定するとても重要な情報です。サーバ証明書をインストールする際 IBM HTTP Server httpd-conf 設定時に利用しますので、ホスト名等を設定してください。
- 鍵サイズ：2048bit としてください。なお、ikeyman を使用して 2048bit の鍵サイズを持つ証明書要求を作成する為には、GSKitV7.0.4.14 以上に含まれる gskikm.jar を使用する必要があります。詳しくは、<http://www-01.ibm.com/support/docview.wss?uid=jpn1J1003363>
- 署名アルゴリズム：SHA1WithRSA を選択。(エンド証明書のハッシュ関数に関わらず)
- 共通名：証明書発行先 Common Name/FQDN
- 組織：会社等組織団体名/個人名
- 組織単位：部署名 (必ず何らかの情報を入力してください！)
- 地域：特別区名/市町村名
- 都道府県：都道府県名
- 郵便番号：郵便番号
- 国：文字国名 (2 文字の ISO CODE)
- 被認証者の代替名：入力不要です。

新規鍵および認証要求の作成

以下を指定してください:

鍵ラベル(K)

鍵サイズ(E)

署名アルゴリズム(S)

共通名(M) (オプション)

組織(G) (オプション)

組織単位(A) (オプション)

地域(L) (オプション)

都道府県(I) (オプション)

郵便番号(Z) (オプション)

国または地域(U) (オプション)

被認証者の代替名

Eメール・アドレス(D)(オプション)

IPアドレス(P) (オプション)

DNS名(N) (オプション)

認証要求を保管するファイルの名前を入力(H)

CSR 生成情報入力に使用できる文字には、以下の制限があります。これを守らないと、CSR が生成できません。 入力は、全て半角で行います。なお、コモンネームには以下の「英字」「数字」および「 - (ハイフン) 」のみが利用できます。

字種	使用できる範囲
英字、数字	大文字 A~Z 小文字 a~z 0~9
記号 スペース	'(アポストロフィ) - (ハイフン) .(ピリオド)

3.3 CSR はデフォルトでは **"certreq.arm"** なるファイル名で生成されます。

入力後 **【OK】** をクリックして下さい。



正常に完了のメッセージが表示されますので **【OK】** をクリックして下さい。



4. CSR を送付

生成された CSR ファイルをテキストエディタで開き、「ジェイストア」申請画面にコピー&ペーストしてください。以下に、CSR ファイルを開いた例を示します。

```
-----BEGIN CERTIFICATE REQUEST-----  
MIIBYTCCATICAQAwYgxCzAJBgNVBAYTAkpQMq4wDAYDVQQIEwVUub2t5bzETMBEg  
A1UEBxMKQ2hpeW9kYS1rdTEaMBGGA1UEChMRQ29tb2RvIEphcGFuIEluYy4xZmZAV  
:  
:  
RFi8OQRtKDSGL9mqC4FLk/cAxcNs4X+yzUNp9jn9IldCGEtTg4aRIBFKpWTobwh6  
m0jpoMYpQ8DNwO0vpjAGruzQ/ARdw/xalMqyqaU=  
-----END CERTIFICATE REQUEST-----
```

注： -----BEGIN CERTIFICATE REQUEST----- から、-----END CERTIFICATE REQUEST----- までは **ハイフンを含めて**、「ジェイストア」申請画面に貼り付けてください。

1文字でも欠けますと、CSR ファイルフォーマットエラーとなり、サーバ証明書のお申込を受付できません。

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。