IBM HTTPServer編

改版履歴			
版数	日付	内容	担当
V.1.1	2014/12/22	初版	NII
V.1.2	2015/5/25	中間CA証明書のファイル名を修正	NII
V.1.3	2015/12/11	誤記修正	NII
V.2.0	2018/2/26	SHA1の記載内容の削除	NII
V.2.1	2018/3/26	CT対応版の中間CA証明書について説明を追加	NII
V.2.2	2018/7/9	1-1前提条件に注意事項を追記 誤記修正 DNのルールの修正 CSRの生成にてSTの追加とLの修正	NII
V.2. 5	2019/6/10	1-2事前準備 DNのルール(Locality Name)の修正	NII
V.2.6	2020/4/13	DNのルール(State or Province Name、Locality Name)の修正	NII
V.2.7	2020/7/15	DNのルール、TSVファイル形式のSTおよびLの値の説明、リンクの変更	NII
V.2.8	2020/8/25	中間CA証明書の記載内容を修正	NII
V.2.9	2020/12/22	中間CA証明書を修正 サーバー証明書L、STを必須に修正 サーバー証明書OUの利用条件を修正	NII

目次

1. IBM HTTP Serverによるサーバ証明書の利用

1-1. 前提条件

IBM HTTP Serverでサーバ証明書を使用する場合の前提条件について記載します。

適宜、サーバ証明書をインストールする利用管理者様の環境により、読み替えをお願い致します。（本マニュアルではWindows Server 2012,ikeyman8.0.315での実行例を記載しております。）

前提条件
1. IBM HTTP Serverがインストールされていること

CSR作成時は既存の鍵ペアは使わずに、必ず新たにCSR作成用に生成した鍵ペアを利用してください。

更新時も同様に、鍵ペアおよびCSRを新たに作成してください。鍵ペアの鍵長は2048bitにしてください。

※ IBM HTTP Server でサポートされているのは RSA 証明書 (鍵) のみです。 ECC 証明書 はサポートされていません。

1-2. 事前準備

鍵ペア・CSRを生成する前に、事前に以下の項目の準備をしてください。

事前準備

1. 鍵データベースファイル名:***<key.kdb>***（「**1-3-1～手続き2**」で使用）
   例)**yyyymmdd_key.kdb**(デフォルトでは、**key.kdb**が表示されます)

2. 鍵データベースファイルの位置（「**1-3-1～手続き2**」で使用）
   例) **C:\Program Files (x86)\IBM\HTTPServer* (デフォルトでは**C:\Program Files (x86)\IBM\HTTPServerが表示されます)

3. 鍵データベースファイルのパスワード（「**1-3-1～手続き3**」で使用）

4. 鍵データベースファイルのラベル名：***<Label Name>***「**1-3-2～手続き2**」で使用）
   例）UPKI0001

5. サーバ DN（※サーバDNについては、本サービス証明書ポリシまたは、下記DNのルールをご確認ください。また、ikeymanとの設定項目の突き合わせにつきましては、「**1-3-2～手続き2**」をご確認ください。）

6. CSRファイル名と保存先
   例)**C:\Program Files (x86)\IBM\HTTPServer\certreq.arm** (デフォルトでは**C:\Program Files (x86)\IBM\HTTPServer\certreq.arm**に保存されます)

CSRに記述するDNのルールは以下のとおりとなります。

DNのルール

項目	指定内容の説明と注意	必須	文字数および注意点
Country (C)	本認証局では必ず「JP」と設定してください。 例）C=JP	○	JP固定
State or Province Name(ST)	「都道府県」（ST）は利用管理者及び利用者が所属する組織の所在地の都道府県名としサービス窓口に事前に届出したとおりの所在地の都道府県名をローマ字表記で指定してください。この情報は各所属機関の登録担当者にお問い合わせください。 例）ST=Tokyo	○	STとして指定できる値は下記リンクを参照してください。機関ごとに固定となります。 UPKI証明書 主体者DNにおける ST および L の値一覧 ※STおよびLが必須。（2020年12月22日以降）
Locality Name(L)	「場所」（L）は利用管理者及び利用者が所属する組織の所在地の市区町村名とし、サービス窓口に事前に届出したとおりの所在地の市区町村名をローマ字表記で指定してください。この情報は各所属機関の登録担当者にお問い合わせください。 例)L=Chiyoda-ku	○	Lとして指定できる値は下記リンクを参照してください。機関ごとに固定となります。 UPKI証明書 主体者DNにおける ST および L の値一覧 ※STおよびLが必須。（2020年12月22日以降）
Organization Name (O)	サービス参加申請時の機関名英語表記を設定してください。この情報は各所属機関の登録担当者にお問い合わせください。 例)O=National Institute of Informatics	○	半角の英数字64文字以内(記号は「'(),-./:=」と半角スペースのみ使用可能)
Organizational Unit Name (OU)	証明書を使用する部局等の名前を設定してください。 （この値は省略可能です） （この値は複数設定することが可能です。複数指定する方法につきましては、CSR作成時ご使用のアプリケーションのマニュアルをご確認ください。） 例)OU=Cyber Science Infrastructure Development Department	△	・半角の英数字64文字以内(記号は「'(),-./:=」と半角スペースのみ使用可能) ・複数OUを指定する場合は、全体で64文字以内 UPKI証明書 主体者DNにおける OU の値一覧
Common Name (CN)	サーバ証明書URLに表示されるウェブ・サーバの名前をFQDNで設定してください。例えばSSL/TLSを行うサイトが https://www.nii.ac.jpの場合には、「www.nii.ac.jp」となります。 FQDNにはサービス参加申請時に登録いただいた対象ドメイン名を含むFQDNのみ、証明書発行が可能となります。 例)www.nii.ac.jp	○	証明書をインストールする対象サーバのFQDNで64文字以内 半角英数字、”．“、 “-”のみ使用可能。また、先頭と末尾に “.” と “-” は使用不可
Email	本認証局では使用しないでください。	×	
鍵長			

RSA 2048bit

○・・・必須　×・・・入力不可　△・・・省略可

注意：証明書の更新を行う場合は、先に1-7をご確認ください。

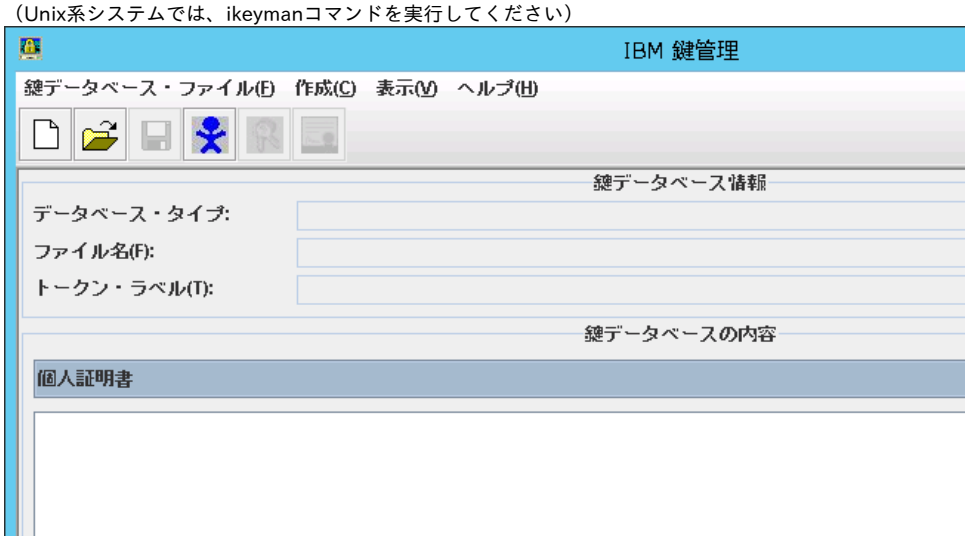
1-3. 鍵データベースファイルの生成とCSRの作成

1-3-1. 鍵データベースファイルの生成

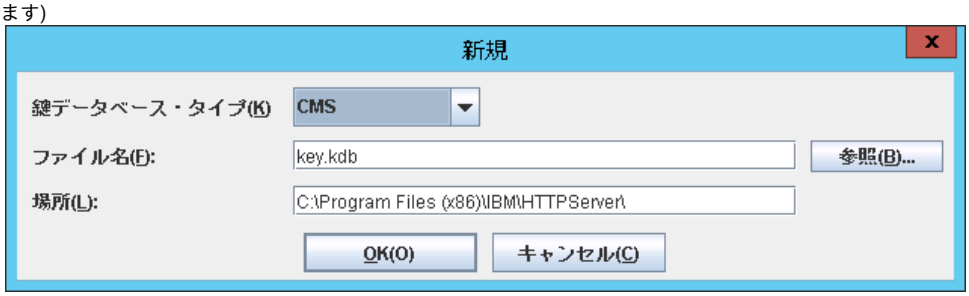
以下に鍵データベースファイルの生成方法を記述します。

鍵ペアの作成

1. iKeymanを実行します。Windowsの場合「スタート」→「アプリ」→「IBM HTTP Server VX.X」→「Start Key Management Utility」を選択してください。
（Unix系システムでは、ikeymanコマンドを実行してください）

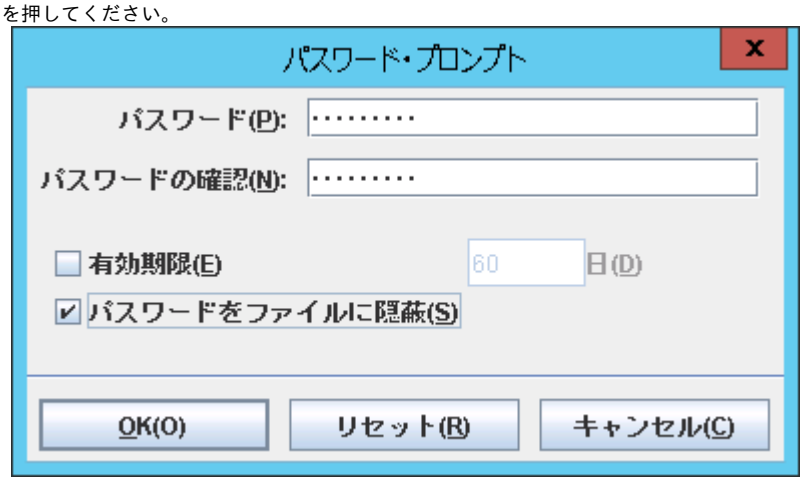


2. メニューより、「鍵データベース・ファイル」→「新規」を選択してください。鍵データベース・タイプを「ＣＭＳ」、鍵データベースファイルの出力先として、位置を指定してください。
ファイル名に関しては、鍵データベース作成日時がわかるようなファイル名にしておくことを推奨します。
位置はデフォルト値でかまいません。(デフォルトでは、ファイル名「key.kdb」、位置「C:\Program Files (x86)\IBM\HTTPServer」となっています)



重要：更新時、以前の鍵データベースファイルと区別がつくように、鍵データベースファイル名に日付等を入力することを推奨します。

3. パスワード・確認パスワードを入力してください（パスワードをファイルに隠蔽　にチェックを入れることを推奨致します）。入力後、「ＯＫ」を押してください。



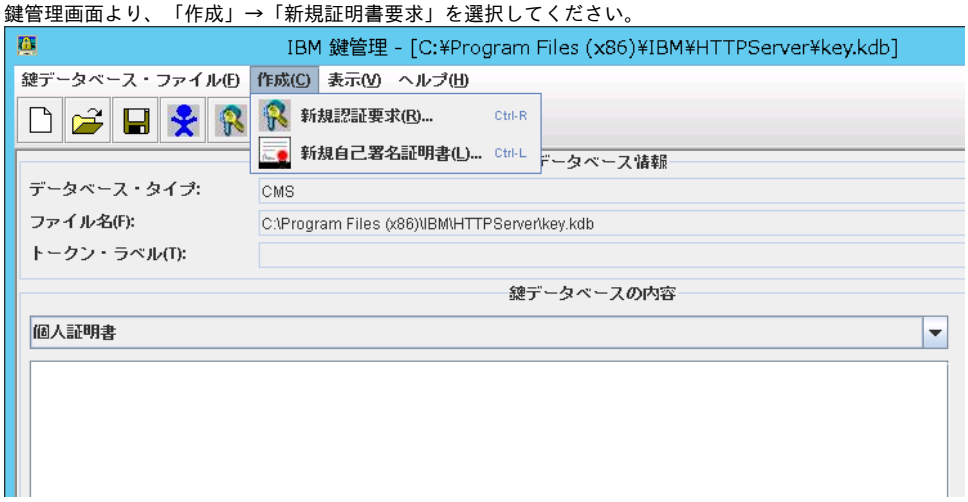
以上で鍵データベースファイルの作成は完了です。

1-3-2. CSRの生成

鍵データベースファイルが作成されたことを確認後、CSRを生成します。

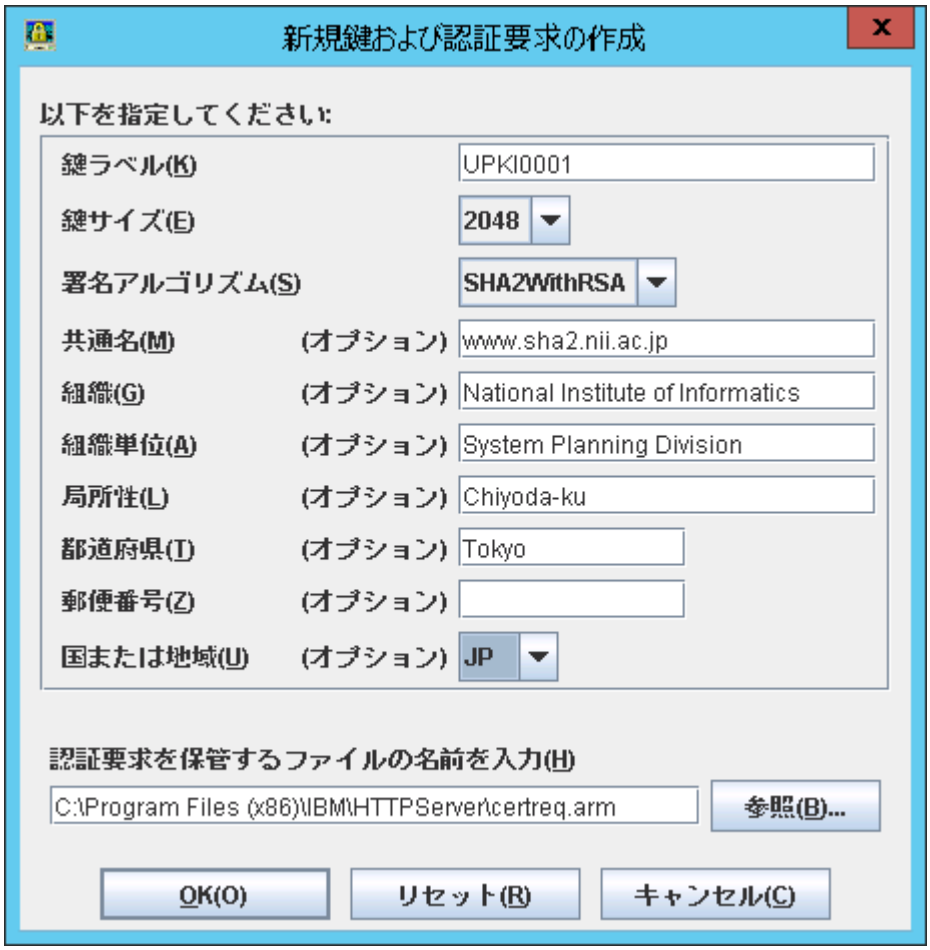
CSRの作成

1. 鍵管理画面より、「作成」→「新規証明書要求」を選択してください。



新規の鍵および証明書要求の作成画面が開かれます。
鍵ラベルを入力し、鍵サイズを2048bitに選択し、「1-2. 事前準備」に記述されているＤＮのルールを参照に、各項目の入力を行ってください。
サービスで必要な項目とiKeymanで表示される項目の対応は以下を参照してください。入力が終了したら、ファイルパス、ファイル名の名前を入力し「ＯＫ」を押してください。
デフォルトではC:\Program Files (x86)\IBM\HTTPServer\certreq.armとなっています。拡張子は.armとしてください。

証明書要求作成画面とＤＮの対応表		
項目	ikeymanの項目	指定内容の説明と注意
Country(C)	国または地域	本認証局では必ず「JP」と入力してください。
State or Province Name(ST)	都道府県	利用管理者及び利用者が所属する組織の所在地の都道府県名を入力してください。 使用可能な値は、ST固有値一覧を参照してください。
Locality Name(L)	局所性	利用管理者及び利用者が所属する組織の所在地の市区町村名を入力してください。
Organization Name(O)	組織単位	サービス参加申請時の機関名英語表記を記入してください。この情報は各所属機関の登録担当者にお問い合わせください。
Organizational Unit Name(OU)	組織	証明書を使用する部局等の名前を入力してください。（この値は省略可能です） 使用可能な値は、UPKI証明書 主体者DNにおける OU の値一覧を参照してください。
Common Name(CN)	共通名	サーバのFQDNを入力してください。



鍵ラベル：キーデータベース中で使用される鍵の名前です。ホスト名等を設定してください。
例）UPKI0001

鍵サイズ：鍵のサイズを選択してください。2048bitとしてください。

署名アルゴリズム：SHA2WithRSAとしてください。
例)SHA2WithRSA

共通名：ウェブ・サーバのFQDNを設定してください。
例)www.sha2.nii.ac.jp

組織：サービス参加申請時の機関名英語表記を記入してください。
例)National Institute of Informatics

組織単位：組織内の部署名を設定してください。
例)System Planning Division

局所性：利用管理者及び利用者が所属する組織の所在地の市区町村名を入力してください。
例）Chiyoda-ku

都道府県：利用管理者及び利用者が所属する組織の所在地の都道府県名を入力してください。
例）Tokyo

郵便番号：設定しないでください。

国または地域：ＪＰを選択してください。

重要：ファイル名およびパス名に日本語が含まれていると、ＣＳＲが正しく保管されない場合があります。英数字、ハイフン、ピリオド、ドライブの指定文字(:)、パス名の区切り文字(\ /)以外の文字は使用しないことを推奨します。

1-4. 証明書の申請から取得まで

CSRを作成しましたら登録担当者へ送付するための証明書発行申請TSVファイルを作成し申請します。
証明書発行申請TSVファイルの作成方法、申請方法等につきましては、「**証明書自動発行支援システム操作手順書(利用管理者用)**」をご確認ください。
証明書の発行が完了すると、本システムより以下のメールが送信されます。メール本文に記載された証明書取得URLにアクセスし、証明書の取得を実施してください。

証明書取得URLの通知
【件名】 Webサーバ証明書発行受付通知 ・・・・・ **#以下に証明書の取得先が記述されています。** 貴機関の登録担当者経由で発行申請をいただきましたサーバ証明書を配付いたします。 本日から1ヶ月以内に以下の証明書取得URLへアクセスし、サーバ証明書の取得を行ってください。 証明書取得URL：https://scia.secomtrust.net/～　←左記URLにアクセスし証明書の取得を行ってください。 ・・・・・

1-5. 証明書のインストール

本章ではIBM HTTP Serverへの証明書のインストール方法について記述します。

1-5-1. 事前準備

事前準備として、サーバ証明書、中間CA証明書、ルートCA証明書を取得してください。

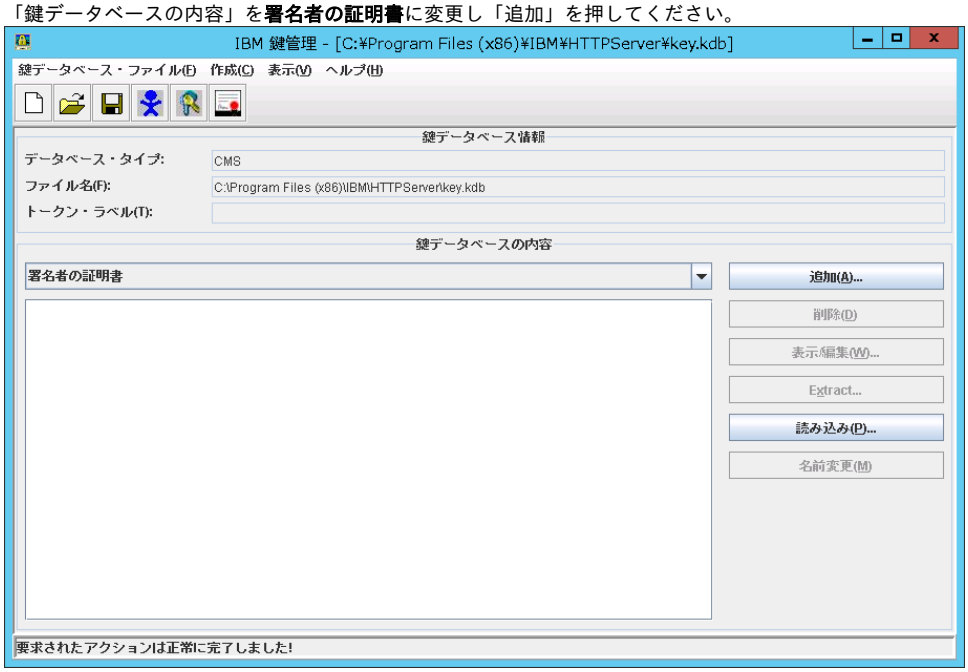
前提条件
1. サーバ証明書を準備します。「1-4.証明書の申請から取得まで」で受領したサーバ証明書をserver.cerという名前で保存してください。 2. 中間CA証明書を準備します。 次のURLにアクセスすることでリポジトリにアクセスすることが可能です。 リポジトリ：https://repo1.secomtrust.net/sppca/nii/odca4/ SHA-2認証局 CA証明書 (CT対応版)をnii-odca3sha2ct.cerという名前で保存したと仮定して以降記載します。 3. ルートCA証明書を準備します。 以下URLよりSecurity Communication RootCA2 証明書 - Security Communication RootCA2 Certificateを取得して、SCRoot2ca.cerという名前で場所に保存してください。 リポジトリ：https://repository.secomtrust.net/SC-Root2/index.html

1-5-2. ルートCA証明書のインストール

以下の手続きに従って、ルートCA証明書のインストールを行ってください。

ルートCA証明書のインストール

1. 「1-5-1.事前準備」で取得したルートCA証明書を鍵データベースファイルにインストールします。
「鍵データベースの内容」を**署名者の証明書**に変更し「追加」を押してください。



2. オープン画面で「参照」をクリックし、「1-5-1.事前準備」　手続き3 で取得したルートCA証明書を選択し「ＯＫ」を押してください。

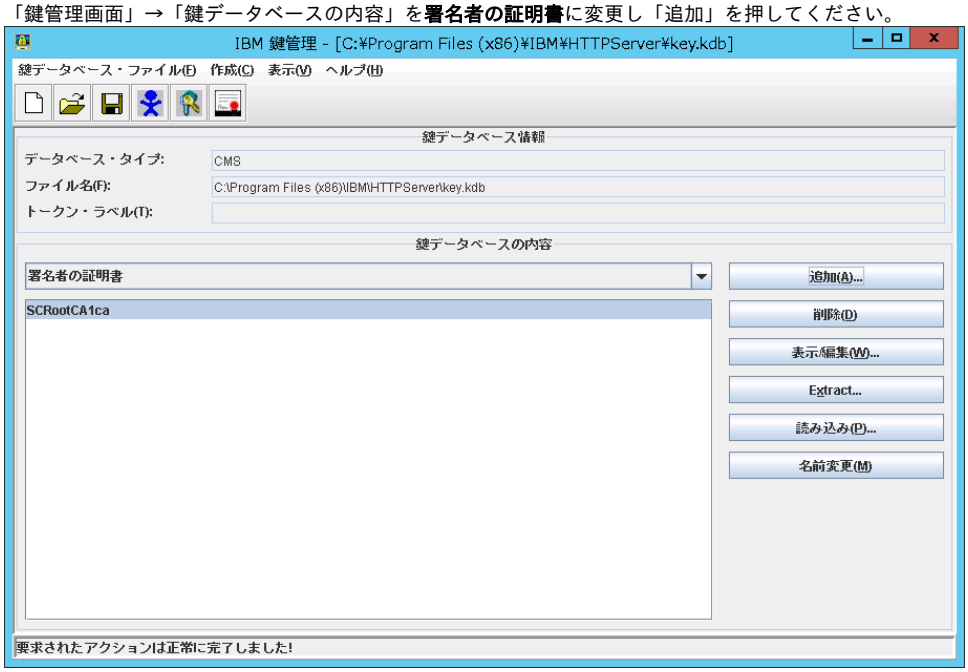
3. 証明書のラベル名として、SCRootCA1ca等わかりやすい文字列を入力後、「ＯＫ」を押してください。

1-5-3. 中間CA証明書のインストール

以下の手続きに従って、中間CA証明書のインストールを行ってください。

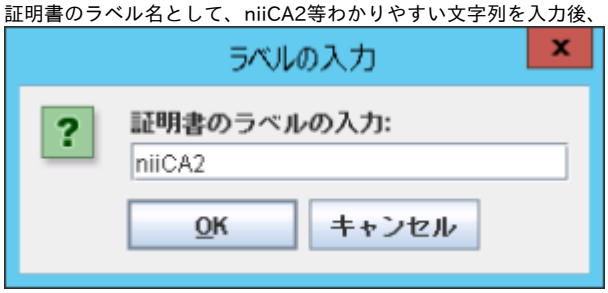
中間CA証明書のインストール

1. 「1-5-1.事前準備」で取得した中間CA証明書を鍵データベースファイルにインストールします。
「鍵管理画面」→「鍵データベースの内容」を**署名者の証明書**に変更し「追加」を押してください。



2. オープン画面で「参照」をクリックし、「1-5-1.事前準備」　手続き2 で取得した中間ＣＡ証明書を選択し「ＯＫ」を押してください。

3. 証明書のラベル名として、niiCA2等わかりやすい文字列を入力後、「ＯＫ」を押してください。



1-5-4. サーバ証明書のインストール

サーバ証明書をインストールする場合は以下の手続きによりサーバ証明書のインストールを実施してください。

サーバ証明書のインストール

1. 「1-5-1.事前準備」で取得したサーバ証明書を鍵データベースファイルにインポートします。「鍵管理画面」→「鍵データベースの内容」を**個人証明書**に変更し、「受信」を押してください。

2. オープン画面で「参照」を選択します。「1-5-1.事前準備」　手続き1 で取得したサーバ証明書を選択し「ＯＫ」を押してください。

1-6. httpd.confの設定変更

本章ではIBM HTTP Serverへの証明書の設定方法について記述します。

httpd.confの設定変更

"C:\IBM\HTTPServer¥conf"にあるhttpd.conf.defaultを参考に、httpd.confを編集してください。
以下に設定の例を記載いたします。詳細な設定につきましては、IBMHTTPServer付属のマニュアルをご確認ください。

```
・・・・
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen <IPアドレス>:443
・・・・
<VirtualHost <IPアドレス>:443>
SSLEnable
SSLServerCert <Label Name> ←1-3-2手続き2で指定したラベル名を記述
SSLClientAuth 0
Keyfile "C:Program Files (x86)\IBM\HTTPServer{color:#ff0000}<key.kdb>"←1-3-1手続き2で指定した鍵データベースファイルまでの絶対パスを記述
</VirtualHost>
・・・・
```

1-7. 証明書の更新

証明書の更新時は鍵データベースファイルを新たに作成して頂く必要がございます。
本マニュアルに従い、鍵データベースファイルを作成後、「1-6.httpd.confの設定変更」の**keyfile**の値、**SSLServerCert**の値を新たに作成した鍵データベースファイルに合わせて変更してください。

1-8. 起動確認

本章ではインストールした証明書によるSSL通信に問題がないか確認する方法を記述します。

証明書の反映・確認

1. HTTPサーバの再起動を行い、設定内容を反映してください。[スタート]→[アプリ]→[IBM HTTP Server VX.X]→[Stop HTTP Server]の後、[Start HTTP Server]
2. ブラウザ経由で、当該のサーバへアクセスし、SSL通信に問題が無いことを確認してください。