

証明書自動発行支援システム

サーバ証明書

インストールマニュアル

IBM HTTP Server編

2012/3/30

国立情報学研究所

改版履歴			
版数	日付	内容	担当
V.1.0	2009/5/15	初版	NII
V.1.1	2009/7/13	誤植修正	NII
V.1.2	2009/8/6	誤植修正	NII
V.1.3	2009/8/11	文言の変更	NII
V.1.4	2009/9/11	誤植の修正	NII
V.1.5	2009/10/13	DN 使用可能文字拡張 誤植の修正	NII
V.1.6	2011/2/28	サーバ証明書インストールマニュアルに IIS7.0・IIS7.5 を追加 DN のルール記載変更 2048bit の鍵サイズ生成方法について追記	NII
V.1.7	2011/6/3	文言を統一	NII
V.1.8	2012/03/30	暗号アルゴリズムのセキュリティ対応に伴いサーバ証 明書および CSR の鍵長 1024 ビット記載削除	NII

目次

1.はじめに.....	1
1-1.CSR とは	1
1-2.ikeyman とは	1
1-3.他のサーバ証明書インストールマニュアルとの比較について	2
1-4.本書の範囲	3
2.IBM HTTP SERVER によるサーバ証明書の利用	4
2-1.前提条件	4
2-2.事前準備	4
2-3.鍵データベースファイルの生成と CSR の作成	7
2-3-1 鍵データベースファイルの生成	7
2-3-2 CSR の生成	9
2-4.証明書の申請から取得まで	12
2-5.証明書のインストール.....	13
2-5-1 事前準備	13
2-5-2 ルート CA 証明書のインストール	15
2-5-3 中間 CA 証明書のインストール	16
2-5-4 サーバ証明書のインストール.....	17
2-6.httpd.conf の設定変更.....	18
2-7.証明書の更新	18
2-8.起動確認	18

1.はじめに

証明書自動発行支援システムサーバ証明書インストールマニュアル IBM HTTP Server 編(以下、「本マニュアル」)は、UPKI オープンドメイン証明書自動発行検証プロジェクト(以下、「プロジェクト」)から発行された証明書を IBM HTTP Server で使用するための CSR の作成方法、発行したサーバ証明書をインストールする方法について記載します。

1-1.CSR とは

CSR(証明書発行要求:Certificate Signing Request)は証明書を作成するための元となる情報で、その内容には、加入者が管理する SSL/TLS サーバの組織名、Common Name(サーバの FQDN)、公開鍵などの情報が含まれています。NII では、加入者に作成いただいた CSR の内容を元に、証明書を作成します。

CSR の例
<pre>-----BEGIN CERTIFICATE REQUEST----- MIIBSTCB9AIBADCBjjELMAkGA1UEBhMCSIAxEDA0BgNVBAcTB0FjYWRlbWUxKjAo BgNVBAoTIU5hdGlvbmFsIEluc3RpdHVOZSBvZiBJbmZvcmlhdGUiJGZEMCAGA1UE lGu3rQIDAQABoAAwDQYJKoZIhvcNAQEEBQADQQCqpoKhuE6W4GpUhpSAJX51z/ze BvHWjt2CBnDeyaIVNgr3+zdGKUpvWYG70RkIss4ST6PDF+RQw+TRdkzI8TUF -----END CERTIFICATE REQUEST-----</pre>

1-2.ikeyman とは

iKeyman は、証明書を管理するためのツールです。iKeyman を使用すると、新規の鍵データベースまたはテスト・証明書の作成、使用するデータベースへの CA ルートの追加、データベース間での証明書のコピー、証明書の要求と CA からの受信、デフォルト鍵の設定、およびパスワードの変更を実行できます。IBM HTTP Server では ikeyman を用いてサーバ証明書の管理を行います。

1-3.他のサーバ証明書インストールマニュアルとの比較について

本マニュアルでは、各サーバで使用する鍵ペア、CSR生成ツールとして、【鍵ペア生成時の共通事項】に記述したツールを使用して説明します。

また、各サーバへインストールする必要がある証明書を【サーバ証明書インストールに必要となる証明書一覧】に記述します。

【鍵ペア生成時に利用するツール】

○・・・該当する -・・・該当しない

	Openssl	JavaKeytool	iKeyman
Apache1.3 系+mod_ssl	○	-	-
Apache2.0 系+mod_ssl	○	-	-
Apache-SSL	○	-	-
Tomcat	-	○	-
IBM HTTP Server	-	-	○
IIS5.0	○	-	-
IIS6.0	○	-	-
IIS7.0	○	-	-
IIS7.5	○	-	-

【サーバ証明書インストールに必要となる証明書一覧】

○・・・該当する -・・・該当しない

	ルート CA 証明書	中間CA証明書	サーバ証明書
Apache1.3 系+mod_ssl	-	○	○
Apache2.0 系+mod_ssl	-	○	○
Apache-SSL	-	○	○
Tomcat	○	○	○
IBM HTTP Server	○	○	○
IIS5.0	○	○	○
IIS6.0	-	○	○
IIS7.0	-	○	○
IIS7.5	-	○	○

1-4.本書の範囲

本書では以下の(e, f)の作業について記述をします。

マニュアル名	内容
操作手順書 (加入者用)	a. 加入者が実施する本システムへのサーバ証明書発行申請・取得について (2章に記載) b. 加入者が実施する本システムへのサーバ証明書更新申請・取得について (3章に記載) c. 加入者が実施する本システムへのサーバ証明書失効申請について (4章に記載) d. 本システムへの証明書アップロードフォーマットについて(5章に記載)
サーバ証明書インストールマニュアル※1	e. CSRと鍵ペアの作成方法について f. サーバ証明書のインストール方法について

※1 以下のマニュアルを総称して「サーバ証明書インストールマニュアル」と呼びます。

- ・証明書自動発行支援システムサーバ証明書インストールマニュアル IBM HTTP Server 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル Tomcat(JavaKeytool)編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル Apache-SSL 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル Apache2.0 系+mod_ssl 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル Apache1.3 系+mod_ssl 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル IIS7.0・IIS7.5 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル IIS6.0 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル IIS5.0 編

2. IBM HTTP Server によるサーバ証明書の利用

2-1. 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。適時、サーバ証明書をインストールする加入者様の環境により、読み替えをお願い致します。(本マニュアルでは Windows2003 サーバ ikeyman7.03 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。更新時と同様に、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。

2-2. 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> (「2-3-1～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 (「2-3-1～手続き 2」で使用)
例) C:\Program Files\IBM HTTP Server\ (デフォルトでは C:\Program Files\IBM HTTP Server\ 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 (「2-3-1～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> (「2-3-2～手続き 2」で使用)
例) UPKI0001
5. サーバ DN (※サーバ DN については、本プロジェクト証明書ポリシーまたは、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、「2-3-2～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\IBM HTTP Server\certreq.arm (デフォルトでは C:\Program Files\IBM HTTP Server\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)	本認証局では使用しないでください。	×	
Locality Name (L)	本認証局では必ず「Academe2」と設定してください。 例)L=Academe2	○	Academe2 固定
Organization Name (O)	プロジェクト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
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 にはプロジェクト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、証明書発行が可能です。 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 2-7 をご確認ください。

2-3. 鍵データベースファイルの生成と CSR の作成

2-3-1 鍵データベースファイルの生成

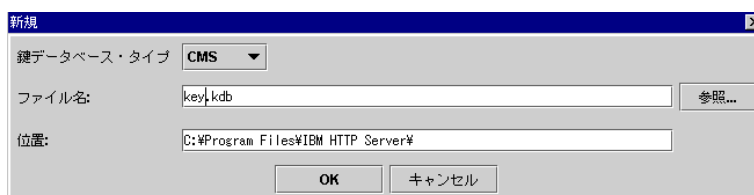
以下に鍵データベースファイルの生成方法を記述します。

鍵ペアの作成

1. iKeyman を実行します。Windows の場合「スタート」→「すべてのプログラム」→「IBM HTTP Server」→「鍵管理ユーティリティの開始」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\IBM HTTP Server\」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しておきますか? にチェックを入れることを推奨致します)。



以上で鍵データベースファイルの作成は完了です。

2-3-2 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。



2. 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 1024bit 以上に選択し、「2-2. 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。プロジェクトで必要な項目と 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¥IBM HTTP Server¥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)	国あるいは領域	本認証局では必ず「JP」と入力してください。
Locality Name(L)	所在地	本認証局では必ず「Academe2」と入力してください。
Organization Name(O)	組織	プロジェクト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)	組織団体	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)
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。

※バージョンによっては鍵サイズが 1024bit までしか選択することができません。暗号アルゴリズムのセキュリティ対応のため、鍵サイズは 2048bit としてください。

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。詳しくは以下のページをご確認ください。

(<http://www-06.ibm.com/jp/domino01/mkt/cnpages1.nsf/page/default-0008E6FF>)

共通名 : ウェブサーバの FQDN を設定してください。

例)www.nii.ac.jp

組織 : プロジェクト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

組織団体 : 組織内の部署名を設定してください。

例)System Planning Division

所在地 : 固定値で「Academe2」を設定してください。

都道府県:設定しないでください。

郵便番号:設定しないでください。

国あるいは領域:JPを選択してください。

**重量: 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。**

2-4. 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(加入者用)」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.nii.ac.jp/~> ←左記 URL にアクセスし証明書の取得を行ってください。

.....

2-5. 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。

2-5-1 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。「2-4.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。以下の中間 CA 証明書の「-----BEGIN CERTIFICATE----- から -----END CERTIFICATE-----」までをコピーして、nii-odca2.cer という名前で保存してください。(次の URL にアクセスすることで同様のファイルが公開されているリポジトリへアクセスできます。)

リポジトリ:<https://repo1.secomtrust.net/sppca/nii/odca2/>

-----BEGIN CERTIFICATE-----

```
MIIEVDCCAzygAwIBAgIEErmwxzANBgkqhkiG9w0BAQUFADBQMwswCQYDVQQGEwJK
UDEYMBYGA1UEChMPU0VDT00gVHJ1c3QubmVOMScwJQYDVQQLEw55TZW51cmI0eSBD
b21tdW5pY2F0aW9uIFJvb3RDQTEwHhcNMDkwMzI3MDMxMzUxWncNMTkwMzI3MDMx
MzUxWjBj9MQswCQYDVQQGEwJKUDERMA8GA1UEBxMIQWNhZGVtZTlXKjAoBgNVBAoT
IU5hdGlvbmFsIEluc3RpdHVOZSBvZiBJbWZvcmlhdGllczENMA8GA1UECxmEVVBL
STEgMB4GA1UECmXMTk1JIE9wZW4gRG9tYWluIENBIC0gRzIwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDgFG0JGEjnMbJg14i00KK4qPNr1gw0IZwJRIdh
4L3cYh6+sKhn/ISvlICcbKfSGas9bj27d9N4dnzhyQaarVmlFyFtYdv8feyKcm
SN7UYUM4SoeAeq6990CPTLIQw2aehkPSGHY7ech1JX6UYw/40pmFnc+ITIDjqf0+
mwJTRM8CtTwvegL7k5fZYinXXtXnh0aioho91/mqDErW0w+AIpPTCDoQBnq1BJzSJ
h+9eMBqj1BrjcxUL0pqBvzVz5lBXgrUq3zmVg3yjTGNERLnBg3xGxRwxgfCS06vZ
e6MpUepb7YarCGJ99L2ENGdOp53A0m8rXyWOK9WSLdbQ9h4jAgMBAAGjggEHMIIB
AzAdBgNVHQ4EFgQUewoH9xjKjA7W2rxQgGwsRwLRDfswHwYDVROjBBgwFoAUoHNJ
mWjchVtI45soL1efvT08B0gwEgYDVROTAQH/BAGwBgEB/wIBADA0BgNVHQ8BAf8E
BAMCAQYwSQYDVROfBEIwQDA+oDyg0oY4aHR0cDovL3JlcG9zaXRvcnkuc2Vjb210
cnVzdC5uZXQuU0MtUm9vdEUV0NSb290MUNSTC5jcmwwUgYDVROgBESwSTBHBgoq
gwiMmxtkhwUBMDkwNwYlKwYBBQUHAgEwK2h0dHBzOi8vcmlvd3NpdG9yeS5zZW5v
bXRydXN0Lm5ldC9TQy1Sb290MS8wDQYJKoZIhvcNAQEFBQADggEBAKoqogcGLHdD
IkXmNjckI9kXn9I8zHNn7x03YdMYkgsIkYSAic9+HwWHJPV12/ba0xigpGKkY2vc
SEDwAihqSsVTHrzY6QyERVSaalk+C74+sxjxw1JG5Lch+wtg+ExA4mZPAS7v0fgD
```



```
kni+7IP9YrILR19E6K2AQW6G3Df8zhnkOf2+kI+lavDvT74Krh0FojYZTGF6DFIo  
kBFfvNBdrux4CkIsKhpYQXCAIEuy12CFZUXEtHB5XxeBkntbs2IfP/rWbg2J1Ige  
zZc6shCn3VdrL2douVFjaAXlc8zwys/KIpLzNSx00GwJdKxFTaIzH/emcqKj93Jd  
DC1rrFMhoPE=  
-----END CERTIFICATE-----
```

3. ルート CA 証明書を準備します。以下 URL より Security Communication RootCA1 証明書 - Security Communication RootCA1 Certificate を取得して、scroot.cer という名前で場所に保存してください。本ファイルはデフォルトでは SCroot1ca.cer という名前でダウンロードされます。

リポジトリ:<https://repository.secomtrust.net/SC-Root1/index.html>

2-5-2 ルート CA 証明書のインストール

以下の手順に従って、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

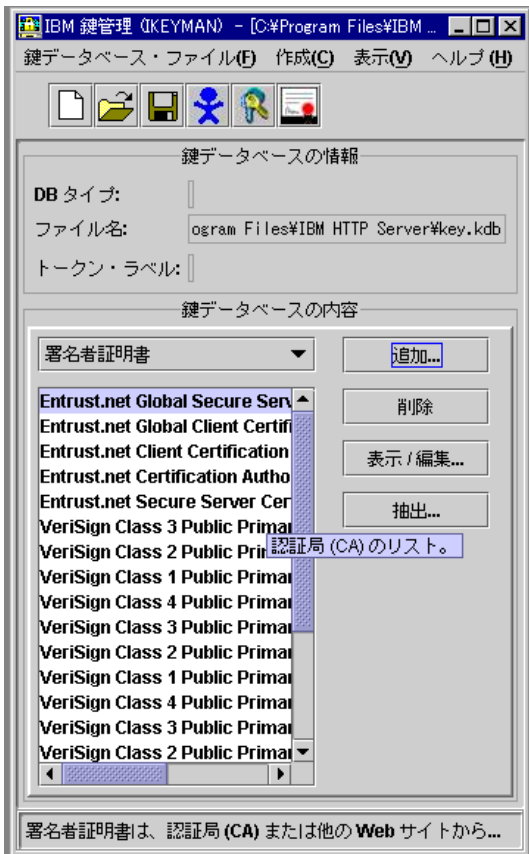
- 「2-5-1.事前準備」で取得したルート CA 証明書を鍵データベースファイルにインストールします。「鍵管理画面」→「鍵データベースの内容」を署名者証明書に変更し「追加」のボタンを押してください。

- データ型を「Base64 でエンコードされた ASCII データ」とし、「参照」をクリックし、「2-5-1.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。
- 証明書のラベル名として、RootCA 等わかりやすい文字列を入力して OK をクリックしてください。


2-5-3 中間 CA 証明書のインストール

以下の手順に従って、中間 CA 証明書のインストールを行ってください。

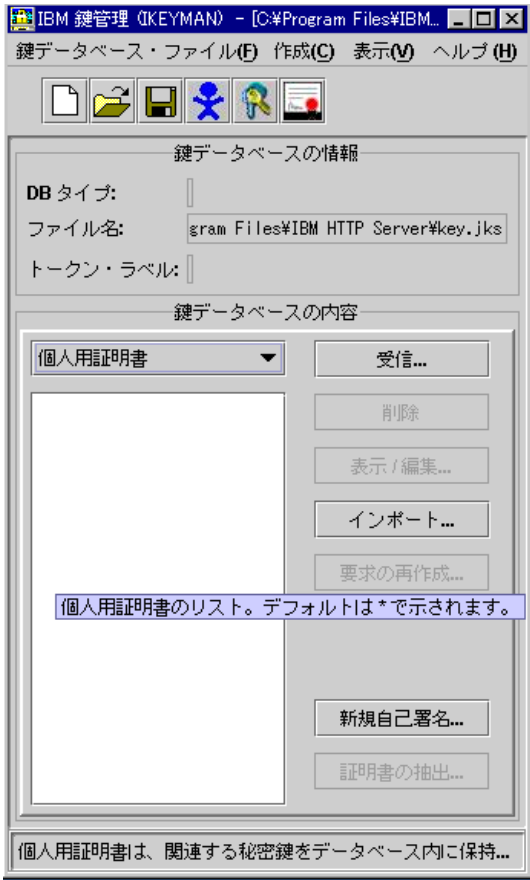
中間 CA 証明書のインストール

- 「2-5-1.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」を署名者証明書に変更し「追加」のボタンを押してください。
- データ型を「Base64 でエンコードされた ASCII データ」とし、「参照」をクリックし、「2-5-1.事前準備」手続き 2 で取得し中間CA証明書を選択し「OK」を押してください。
- 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して OK をクリックしてください。

2-5-4 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

- 「2-5-1.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」のボタンを押してください。

- データ型を「Base64 でエンコードされた ASCII データ」とし、「参照」をクリックし、「2-5-1. 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。

2-6.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:¥Program Files¥IBM HTTP Server¥conf”にある httpd.conf.sample 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  
.....  
<Virtual host:ドメイン名:443>  
SSLEnable  
SSLServerCert <Label Name>    ←2-3-2 手続き 2 で指定したラベル名を記述  
SSLClientAuth 0  
Keyfile C:¥Program Files¥IBM HTTP Server¥<key.kdb>    ←2-3-1 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  
<Virtual host>  
.....
```

2-7.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あります。本マニュアルに従い、鍵データベースファイルを作成後、「2-6.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。

2-8.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]→[プログラム]→[IBM HTTP ServerX.XX]→[HTTP Server の停止]の後、[HTTP Server の起動]
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。