

(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/webservers/httpservers/doc/v52/jpn/icswq021.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。





Internet Explorer 7 IBM HTTP Server V8.5 IBM WebSphere デスクトップ 開始 HTTP Server Web サーバー・プラグ đ -85 イン構成ツール 開始キー管理ユー WebSphere đ ٥ ティリティー Customization... 停止 HTTP Server WebSphere Customization... インフォメーション・セ IBM Installation Manager ンター

一覧画面から【開始キー管理ユーティリティー】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。

<u>A</u>		IBM 鍵管理	_ 🗆 X
鍵データベース・ファイル(E) f	作成(<u>C</u>) 表示	(⊻) ヘルプ(出)	
┣ 新規(Ŋ	Ctrl-N		
┌── 開く(○)	Ctrl-O	くぬー" ト ついたまに	
😪 新規プロバイダー(E)	Ctrl-E	誕ナータベース 道報	
クローズ(<u>C</u>)			
】 別名保存(<u>S</u>)	Ctrl-S		
パスワードの変更(出) パスワードを隠す(T)		鍵データベースの内容	
パスワードの有効期限の表	示(<u>D</u>)	•	受信(!)
終了(<u>X</u>)			肖·耶余 (<u>D</u>)
			表示編集(<u>W</u>)
			インポート(<u>P</u>)
			要求の再作成(<u>A</u>)
			名前変更(∭)
			新規自己署名(<u>G</u>)
			証明書を抽出(<u>T</u>)
開始するには、「鍵データベース・ファイル」メニューを選択して、鍵データベースを操作してください			



- 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薦めします。
(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。

	新規	x
鍵データベース・タイプ(<u>K</u>)	CMS 👻	
ファイル名(E):	20130722_key.kdb	参照(<u>B</u>)
場所(<u>L</u>):	C:\Program Files (x86)\IBM\HTTPServer\	
	<u>O</u> K(0) キャンセル(<u>C</u>)	

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薦めします。

パスワード・プロンプト
バスワード(<u>P</u>):
パスワードの確認(<u>N</u>):
□ 有効期限(E) 60 日(D) ビ パスワードをファイルに隠す(S)
<u>O</u> K(O) リセット(<u>R</u>) キャンセル(<u>C</u>)

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。

<u>0</u>	IBM 鍵管理 - [C:¥Program Files (x86)¥IBM¥HTTPServer¥20130722_key.kdb]	_ _ ×		
鏈データベース・ファイル(E) 作成(C) 表示(V) ヘルプ(H)				
継データベース 情報				
データベース・タイプ:	CMS			
ファイル名(F):	C:\Program Files (x86)\IBM\HTTPServer\20130722_key.kdb			
トークン・ラベル(T):				

CSR_ikeyman ver.2 © J Cert, Inc. All rights reserved. Page3



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。

IB IB	3M 鍵管理 - [C:¥Program Files (x86)¥IBM¥HTTPServer¥20130722_key.kdb]		
鍵データベース・ファイル(E)	作成(<u>C</u>) 表示(⊻) ヘルプ(出)		
🗅 🚄 🖶 🎽 🛛			
	鍵データベース情報		
データベース・タイプ:	CMS		
ファイル名(F):	C:\Program Files (x86)\IBM\HTTPServer\20130722_key.kdb		
トークン・ラベル <mark>(</mark> T):			
	継データベースの内容		
個人認証要求	_	新規(<u>W</u>)	
		肖 切 际(<u>D</u>)	
		表示(!)	
		抽出(<u>X</u>)	
要求されたアクションは正常に完了しました。			
,			

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:入力は不要です。



	第 弟	f規鍵および認	証要求の作成
ļ	以下を指定してください);	
	鍵ラベル(<u>K</u>)		server
	鏈サイズ(<u>E</u>)		2048 🔻
	署名アルゴリズム(<u>S</u>)		SHA1WithRSA 💌
	共通名(<u>M</u>)	(オプション)	www.jcert.biz
	組織(<u>G</u>)	(オプション)	J Cert Inc.
	組織単位(<u>A</u>)	(オプション)	SSL Servces
	地域(<u>L</u>)	(オプション)	Chiyoda-ku
	都道府県 <mark>(T</mark>)	(オプション)	Tokyo
	郵便番号 <mark>(Z</mark>)	(オプション)	
N	国または地域(U)	(オプション)	JP 🔻
	被認証者の代替名		
	Eメール・アドレス(<u>D)(オプション)</u>	
	IEアドレス(P)	(オプション <mark>)</mark>	
	D <u>N</u> S 名(N)	(オプション <mark>)</mark>	
認証要求を保管するファイルの名前を入力(出)			
C:\Program Files (x86)\IBM\HTTPServer\certreq.arm 参照(B)			
<u>O</u> K(O) リセット(<u>R</u>) キャンセル(<u>C</u>)			

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-----

MIIByTCCATICAQAwgYgxCzAJBgNVBAYTAkpQMQ4wDAYDVQQIEwVUb2t5bzETMBEG A1UEBxMKQ2hpeW9kYS1rdTEaMBgGA1UEChMRQ29tb2RvIEphcGFuIEluYy4xFzAV

:

RFi8OQRtKDSGL9mqC4FLk/cAxcNs4X+yzUNp9jn9IldCGEtTg4aRIBFKpWTobwh6 m0jpoMYpQ8DNwO0vpjAGruzQ/ARdw/xaLmQyqaU= -----END CERTIFICATE REQUEST-----

注: -----BEGIN CERTIFICATE REQUEST----- から、-----END CERTIFICATE REQUEST----- までを<mark>ハイフ</mark> <mark>ンを含めて</mark>、「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。	