CSR ファイルの作成方法 (Windows MMC)

サーバ証明書をインストールする Windows Server 上で作業してください。

1. 「ファイル名を指定して実行」へ「certlm.msc」を入力し実行します。

דיד 📨	ル名を指定して実行	×
	実行するプログラム名、または開くフォルダーやドキュメント名、 ンターネット リソース名を入力してください。	ſ
名前(<u>O</u>)	: certim.msd	~
	OK キャンセル 参照(<u>B</u>)	

2. 「個人」を右クリックして表示されるメニューをたどり、「カスタム要求の作成」をク リックします。

🙀 certim - [証明書 - ローカル コンピューター¥個人]		- 0	×
ファイル(F) 操作(A) 表示(V) ヘルプ(H)			
🗢 🔿 🙍 🖬 📋 🙆 😹 🗊			
□ 証明書 - ローカル コンピューター □ 個人	^ オブジェクトの種類		
> 🧰 信頼 証明書の検索(N)	このビ	ューに表示する項目はありません。	
> ゴンジ すべてのタスク(K) 、	証明書の検索(N)		
> 📫 信頼 表示(V) ,	新しい証明書の要求(R)_		
> 16 税 > 16 税 = サード 最新の情報に更新(F)	インポート(1)		
> 🧮 信頼 一覧のエクスポート(L)	詳細設定操作(A)	, カスタム要求の作成(C)	
> 251 フレビ ヘルプ(H)		登録ポリシーの管理(M)	
> iii 7,7,1,1,-,1			
> 📫 AAD Token Issuer			
> ほかの人			
 eSIM Certification Authorities Homogroup Machine Certificates 			
Homegroup Machine Certificates			
> McAfee Trust			
> 📫 リモート デスクトップ			
> 🎬 証明書の登録要求			
> 🧰 スマート カードの信頼されたルート			
> 📫 SPC	~ <		>
個人 ストアには証明書がありません。			

3. 「次へ」をクリックします。



4. 「登録ポリシーなしで続行する」を選択し、「次へ」をクリックします。

-	正明書の登録			
	証明書の登録ポリシーの選択			
	証明書の登録ポリシーは、あらかじめ定義された証明書テンプレートに基づく登録を可能にするもの 明書の登録ポリシーは既に構成されていることがあります。	です。場合	によっては、	証
	ユーザーが構成します カスタム要求		新規追	加
	登録ポリシーなしで続行する			
	×	(N)	キャンセ	JL.

5. 「(テンプレートなし) CNG キー」と「PKCS #10」を選択し、「次へ」をクリックしま す。

0			
	-		×
証明書の登録			
カスタム要求			
下の一覧からオプションを1つ選択し、必要に応じて証明書のオプションを構成してください。			
テンプレート: (テンプレートなし) CNG キー □ 既定の拡張機能の抑制(S)		Ÿ	
要求の形式: PKCS #10(P) ○ CMC(C)			
注意:キーのアーカイブは、このオプションが証明書テンプレートに指定されている場合でも、カスタム 明書では利用できません。	証明書要以	Rに基づく	Æ
×	^(N)	キャン	セル

6. 「詳細」を開いて、「プロパティ」をクリックします。

				×
- 2 II	明書の登録			
1	証明書情報 このテンブレートに対して既に選択されているオブションを使用する場合は (次へ) を、証明書要求を	<i>ከ</i> スタマイ:	(する場合)	‡[
	詳細)をクリックし、(ズベ)をクリックしてくない。 カスタム要求 、 、 、 、 、 、 、 、 、 、 、 、 、	7	詳細	[^]
	次/	(N)	キャンセ	!JV

7. 「フレンドリ名」に、サーバ証明書を識別するための任意の文字列を入力します。

≧般 サブジェクト 拡張機能 秘密キー			
フレンドリ名と説明によって、証明書の識別と使用が容易になります。			
フレンドリ名(N):			
test-serveripc.shimane-u.acjp			
说明(D):			
	OK	キャンセル	適田(A)

8. 「サブジェクト」タブを開き、「完全な DN」を選択後、以下の文字列を入力します。 「追加」をクリックします。

C=JP,ST=Shimane,L=Matsue,O=Shimane University,CN=[Web サーバの FQDN] ※[Web サーバの FQDN]には、サーバ証明書をインストールするサーバの FQDN を入 力します。

証明書のプロパティ	×
全般 サブジェクト 拡張機能 秘密キー	
証明書のサブジェクトとは、証明書の発行先であるユーザーまたはコンピューターです。証明書で使用可能なサブジョ 報を入力できます。	20ト名の種類と別名の値に関する情
証明書のサブジェクト 証明書を受け取るユーザーまたはコンピューター	証明書のプロパティ ×
サブジェクト名:	全般 サブジェクト 拡張機能 秘密キー
種類([]: 完金な DN	証明書のサブジェクトとは、証明書の発行先であるユーザーまたはコンピューターです。証明書で使用可能なサブジェクト名の種類と別名の値に関する情報を入力できます。
值(); C=IET-Shimana I-Mature O=Shimana I Injungih	証明書のサブジェクト 証明書を受け取るコーザーまたはコンピューター
0/2-	サブジェクト名:
種類()):	框项[[]: C=JP ST_Shimano
ディレクトリ名	完全な DN 」 」 』 「IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
値(U):	值仪: <削除
	別名:
	種類(<u>Y)</u> :
	ディレクトリ名
追加 >	值(U):
< 削除	
	追加 >
	. 8/10
	< H154
ОК	
·	
	OK キャンセル 適用(A)

 「秘密キー」タブを開き、「暗号化サービス プロバイダー」欄にて「RSA,Microsoft Software Key Storage Provider」を選択します。

証明書のプロパティ	×
全般 サブジェクト 拡張機能 秘密キー	
暗号化サービス プロバイダー(<u>C</u>)	^
CSPは、多数の証明書関連プロセスで使用される公開キーと秘密キーの組を生成するプログラムです。	
暗号化サービス プロバイダー (CSP)を選択してください:	
☑ RSA,Microsoft Software Key Storage Provider	^
DH,Microsoft Software Key Storage Provider	
DSA,Microsoft Software Key Storage Provider	
ECDH,Microsoft Software Key Storage Provider	
ECDH_brainpoolP160r1,Microsoft Software Key Storage Provider	
ECDH_brainpoolP160t1,Microsoft Software Key Storage Provider	~
ロ すべての CSP の表示(S)	
キーのオブション(<u>O</u>)	•
ハッシュ アルゴリズムの選択社)	*
署名の形式の選択(E)	*
キーのアクセス許可倒	
OK キャンセル	適用(A)

10. 「キーのオプション」欄にて「2048」と「秘密キーをエクスポート可能にする」を選択 します。次に、「ハッシュ アルゴリズムの選択」欄にて「sha256」を選択します。「OK」 をクリックします。

証明書のプロパティ	
全般 サブジェクト 拡張機能 秘密キー	
暗号化サービス プロバイダー(C)	*
キーのオブション(<u>O</u>)	^
キーの長さを設定し、秘密キーのオブションをエクスポートします。	
キーのサイズ: 2048	
◎ 秘密キーをエクスポート可能にする	
□ 秘密キーのアーカイブを許可する	
□ 強力な秘密キーの保護	
ハッシュ アルゴリズムの選択(出)	^
この要求に使用されるハッシュ アルゴリズムの選択	
ハッシュ アルゴリズム sha256	
署名の形式の選択(E)	^
□ 別の署名の形式の使用	
キーのアクセス許可(2)	^
秘密キーにアクセス許可を設定	
□ カスタム アクセス許可の使用	
アクセス許可の設定	
OK キャンセル 適用	(A)

11. 「次へ」をクリックします。



12. CSR ファイル名を入力後、「Base 64」を選択し「完了」をクリックします。



13. 以上で終了です。お疲れ様でした。