JPRS サーバー証明書発行サービス

CSR 生成手順

Microsoft IIS 8.x （新規/更新）

Version 1.1

株式会社日本レジストリサービス（JPRS）

更新履歴

日付	Version	
2016/07/29	1.0	初版リリース
2017/10/18	1.1	「5. 識別名（DN）情報の入力」を更新

1. ログオン

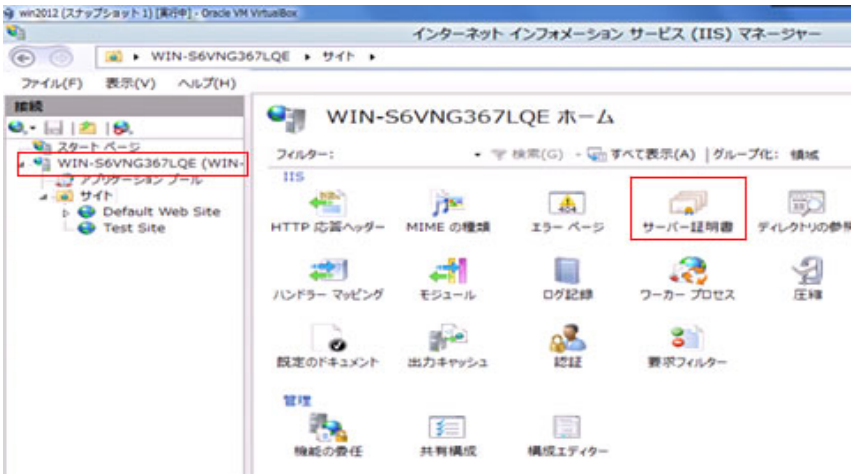
Windows Server 2012 に Administrator 権限でログオンします。

2. インターネットインフォメーションサービス(IIS)マネージャの実行

画面左下にあるサーバーマネージャーを起動します。ダッシュボードを選択し、右上のツールより［インターネットインフォメーションサービス(IIS)マネージャタイル］を実行します。

3. ［サーバー証明書］アイコンの選択

画面左の「接続」にあるサーバー名を選択し、画面中央「ホーム」にある［サーバー証明書］アイコンをダブルクリックします。

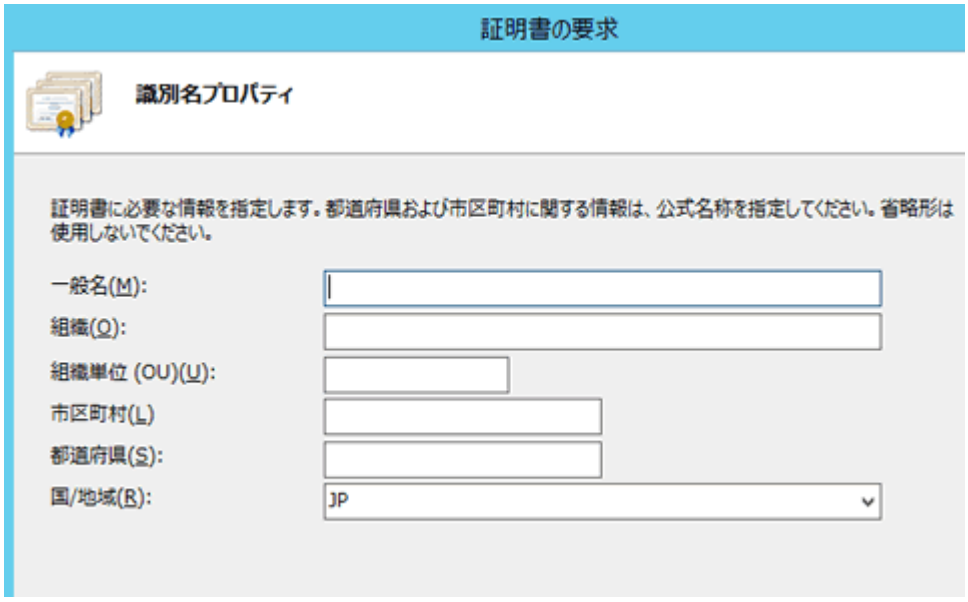


画面の中央と右の表示が変わります。

4. 証明書の要求ウィザードの表示

画面の中央に「サーバー証明書」のリスト・ボックスが表示されます。画面右にある［証明書の要求の作成...］メニューをクリックします。

<証明書の要求>ダイアログがポップアップします。



5. 識別名(DN)情報の入力

「識別名プロパティ」に証明書内に組み込む識別名(DN)情報を入力してください。
この情報を入力するには以下の点にご注意ください。

- 各項目の入力はすべて半角の英数字 64 文字以内で入力してください。半角英数字ではない入力項目がある場合、証明書が発行されません。
- &が含まれる場合、半角英語の and 等に置き換えて入力してください。
- スペースのみの入力はお控えください。スペースのみの入力項目がある場合、**証明書が発行されません。**

識別名の入力には、以下の文字が使用できます。

一般名：

- 半角英数字
- "-"(ハイフン)
- "."(ドット)
- "*"(アスタリスク)

その他の各項目：

- 半角英数字
- 半角スペース
- ","(カンマ)
- "-"(ハイフン)
- "."(ドット)
- "/"(スラッシュ)
- "("(かっこ)
- ")"(閉じかっこ)
- "'"(アポストロフィ)
- ":"(コロン)
- "="(イコール)

各項目については以下を参照してください。

一般名(M)：

TLS/SSL 通信を行うサイトの Web サーバー名(コモン・ネーム)になります。
例）TLS/SSL 通信を行うサイトの URL が＜https://www.jprs.co.jp/＞である場合、Web サーバー名は「**www.jprs.co.jp**」になります。

※注意点
Web サーバー名に以下を使用することはできません。

- プロトコル特定子(http://)
- IP アドレスやポート番号
- パス名
- 「*」や「?」といったワイルドカード文字（※）

※：ワイルドカード証明書の場合「*.example.jp」のように、一番左側のラベルにワイルドカード文字を指定します。ワイルドカード証明書以外の証明書では、ワイルドカード文字は使用できません。

Web サーバー名は、TLS/SSL 通信を行うサイトの URL の FQDN（Fully Qualified Domain Name）と同一でなければなりません。証明書に登録する Web サーバー名とサイトの URL のホスト名が一致しない場合、ブラウザがサイトへの安全な接続を拒否する場合があります。

例えば、コモン・ネームを「jprs.co.jp」として証明書を発行した場合、＜https://www.jprs.co.jp/＞でアクセスすると、Web サーバー名と(後方の一部は一致していますが)完全には一致していないため、ブラウザに警告が表示されます。なお、JPRS では「www」が含まれている名前と含まれている名前の双方について同一の証明書を利用可能にする「ダブルアドレスオプション」を提供しております。

※：ワイルドカード証明書の場合、サイトの URL の FQDN の一番左側のラベルとして、任意のホスト名を使用できます。ただし、*.example.jp に対し、test1.test2.example.jp など、複数の階層を持つ Web サーバー名を指定することはできません。

組織(O)：

申請組織名（証明書発行先の組織名）です。

例）株式会社日本レジストリサービス(JPRS)の場合

「**Japan Registry Services Co., Ltd.**」

組織単位(OU)(U)：

部署またはグループの名前になります。

この項目は省略できません。また、以下の情報は入力しないでください。

- ドメイン名および IP アドレス
- 記号のみ、およびスペースのみの値
- 「空欄」「該当なし」などの意味を示す文字列（「null」、「N/A」など）
- 申請組織以外の情報と誤解される恐れのある名称・社名・商号・商標
- 法人格を示す文字列（「CO.,Ltd」など）
- 特定の自然人を参照させる文字列
- 住所を示す文字列
- 電話番号

市区町村(L)：

通常、組織の本店(代表)が置かれている市区町村名になります。

例）千代田区の場合「**Chiyoda-ku**」

都道府県(S)：

都道府県名になります。

例）東京都の場合「**Tokyo**」

国/地域(R)：

ISO による 2 文字の国名の符号になります。「**JP(日本)**」を選択ください。

入力内容をよく確認し、［次へ(N)］ボタンをクリックします。暗号化サービスプロバイダを選択する画面になります。

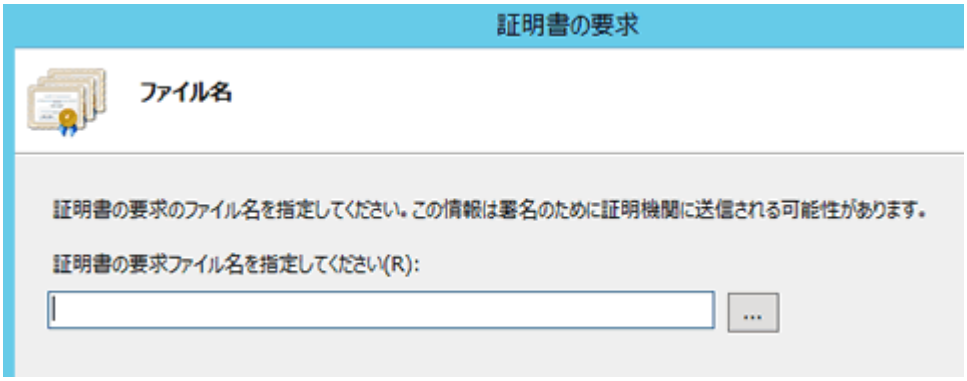
6. 暗号化サービスプロバイダのプロパティの設定

［暗号化サービス プロバイダ(S)］のプルダウンから［Microsoft RSA SChannel Cryptographic Provider］を選択し、作成する鍵の［ビット長(B)］から［2048］を選択してください。

内容を確認し、［次へ(N)］ボタンをクリックします。

7. ファイル名の入力

CSR を保存するファイル名を入力します。



入力したファイル名を確認し、［終了(F)］ボタンをクリックします。
CSR が生成され、指定したファイルに格納され、ダイアログが閉じます。

8. 生成されたファイルの確認

CSR を含むファイルをメモ帳などで開きます。

以下の「-----BEGINNEWCERTIFICATEREQUEST-----」から「-----ENDNEWCERTIFICATEREQUEST-----」までの部分が CSR です。

CSR サンプル

```
----BEGIN NEW CERTIFICATE REQUEST-----
MIICdzCCAiECA0AwZzEQMA4GA1UEAxMHbHJhLXRmczEQMA4GA1UECxMHczEQMA4GA1UE
ChMHbHJhLXRmczESMBAGA1UEBxMJTWIOYWthc2hpMQ4wEwVUb2t5bzELMAkGA1UEBhMC
SlAwXDANBgkqhkiG9w0BAQEFAANLADBIAktF2t+iHqA2nWqt7UYwApptgsYVFrkmXIUH
tZifBz8FOhsBelFbCT33po+9zrWzmRga8DDhxSdujmxGZHOwlDA0ABoIIBUzAaBgorBg
EEAYI3DQIDMQwWCjUuMC4LjIwNQYKKwYBBAGCNwIBDjEnMCUwDgYDVR0PAQH/BA0DAgT
wMBMGA1UCCsGA0UFBwMBMIH9BgorBgEEAYI3DQICMYHuMIHrAgEBHloATQBpAGMAcbwB
mAHQAIABSAFMA0QAgAFMAQwBoAGEAbg
-----END NEW CERTIFICATE REQUEST-----
```

ここで生成した CSR を、申し込み画面に貼り付けて申請いただきます。

以上で CSR の生成は完了です。

※重要
鍵ペアのエクスポート/インポートは行えません。必要な場合はシステムのフルバックアップをお取りください。フルバックアップ方法につきましては製品のマニュアル等をご確

認ください。

同じコモンネーム（一般名）で複数の CSR を生成する場合は、DN 情報の一部（部門名など）を変更してください。