cybertrust

DigiCert SSL/TLS 証明書

Microsoft IIS8.0/8.5

CSR 作成/証明書インストール手順書

（新規・更新用）

Version 1.4

PUBLIC RELEASE

2018/10/25

改訂履歴

日付	バージョン	内容
2017/03/08	1.0	初版リリース
2017/04/28	1.1	「OU」に関する記述内容を修正
2018/08/09	1.2	ドメイン名変更に伴い記述内容を修正
2018/10/01	1.3	「グローバル IP」「OU」に関する記述内容を修正
2018/10/25	1.4	ドメイン名変更に伴い記述内容を修正

目次

cybertrust

はじめに

【！】本手順書をご利用の前に必ずお読みください

本ドキュメントは、Microsoft 社の「Internet Information Services 8.0/8.5（以下、IIS8.0/8.5）」の環境下で DigiCert SSL/TLS 証明書をご利用いただく際の CSR 作成とサーバー証明書のインストールについて解説するドキュメントです。

実際の手順はお客様の環境により異なる場合があり、IIS8.0/8.5 の動作を保証するものではございません。あらかじめご了承ください。

なお、このドキュメントは予告なく変更される場合があり、サイバートラスト株式会社はその内容に対して責任を負うものではありません。

また、このドキュメント内に誤りがあった場合、サイバートラスト株式会社は一切の責任を負いません。

サーバー証明書お申込みフロー

サーバー証明書のご購入については、以下のお申込みフローをご確認ください。

本手順では、赤枠で囲まれた部分のフローをご案内しています。

STEP1	CSR の作成　P6～
↓	
STEP2	WEB からのお申し込み(Cert Station)
↓	
STEP3	必要書類送付/申請の意思確認(電話) 証明書の発行
↓	
STEP4	証明書のダウンロード　P14～
↓	
STEP5	証明書のインストール　P15～
↓	
STEP6	SSL 通信の確認　P30～

cybertrust

CSR の作成

1. CSR 作成前のご確認事項

CSR 作成前に以下についてご確認ください。

1.1. 公開鍵長のご指定について

公開鍵長は「2048bit」をご指定ください。

1.2. CSR 作成時に指定する項目(DN)について

CSR 作成時に以下の項目を指定いただきますので、あらかじめ必要項目をご確認ください。

【!】以下の点についてご注意ください。

・●印がついている項目は必須設定項目です。
・各項目の最大文字数は半角 64 文字(半角スペースを含む)です。日本語は 20 文字です。
・CSR に使用出来る文字は半角英数字(a～z, A～Z, 0～9)と記号(「"」「#」「;」「+」を除く)です。
・組織名(O)、市町村名(L)、都道府県(S)については、CSR 作成時の値に関わらず、
申請法人で指定した値(日本語 or 英語)が証明書情報へ反映されます。

入力項目		内容	入力例
●	コモンネーム(CN)	実際に接続する URL の FQDN	https://www.cybertrust.ne.jp/index.html ⇒ www.cybertrust.ne.jp
●	組織単位名(OU)	部署名(※2)	Technical Division
●	組織名(O)	申請組織の名称(英名)	Cybertrust Japan Co.,Ltd.
●	市町村名(L)	申請組織の事業所住所の「市町村名」(英名) ※東京は 23 区	Minato-ku
●	都道府県名 (S/ST)	申請組織の事業所住所の「都道府県名」(英名)	Tokyo
●	国名(C)	申請組織の国名(JP 固定)	JP

※1 DigiCert SSL/TLS 証明書は、グローバル IP アドレス、プライベート IP アドレスならびにベースドメイン名、ホスト名はコモンネームとしてご指定いただけませんのでご注意ください。

※2 OU の値につきましては、申請の際に申請サイト上にて空欄に変更することをお勧めします。
詳細はこちらをご覧ください。

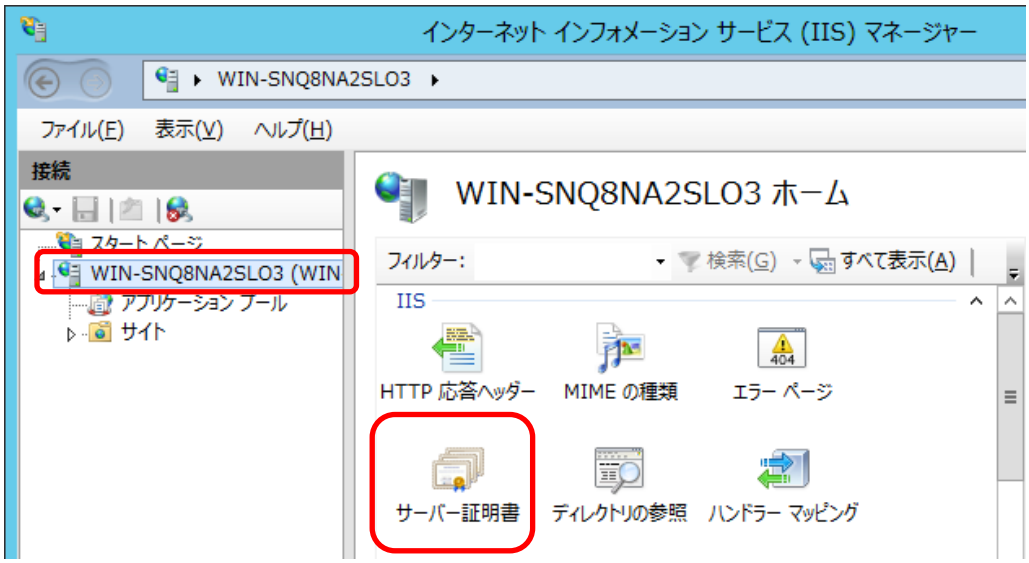
2. キーペア・CSR の作成

Microsoft Windows Server 2012 の【インターネット インフォメーション サービス (IIS) マネージャー】を使って、SSL で使用するキーペア(公開鍵・秘密鍵のペア)と CSR を作成します。

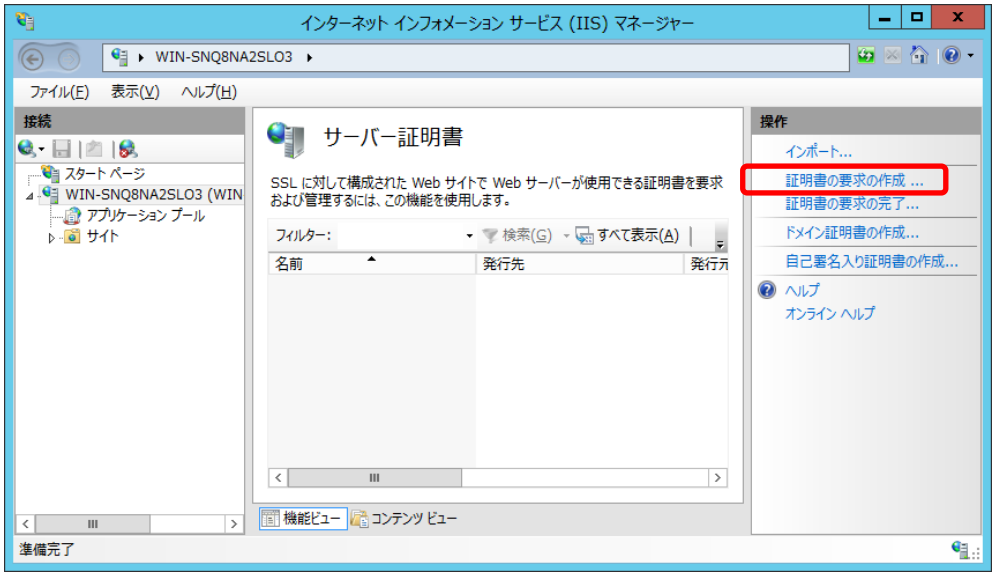
2.1. 作成方法

A) 【スタート】メニューから【インターネット インフォメーション サービス (IIS) マネージャー】を選択して起動します。

B) 以下の画面から、【サーバー証明書】をダブルクリックします。



C) 画面右側の操作メニューから【証明書の要求の作成】をクリックします。

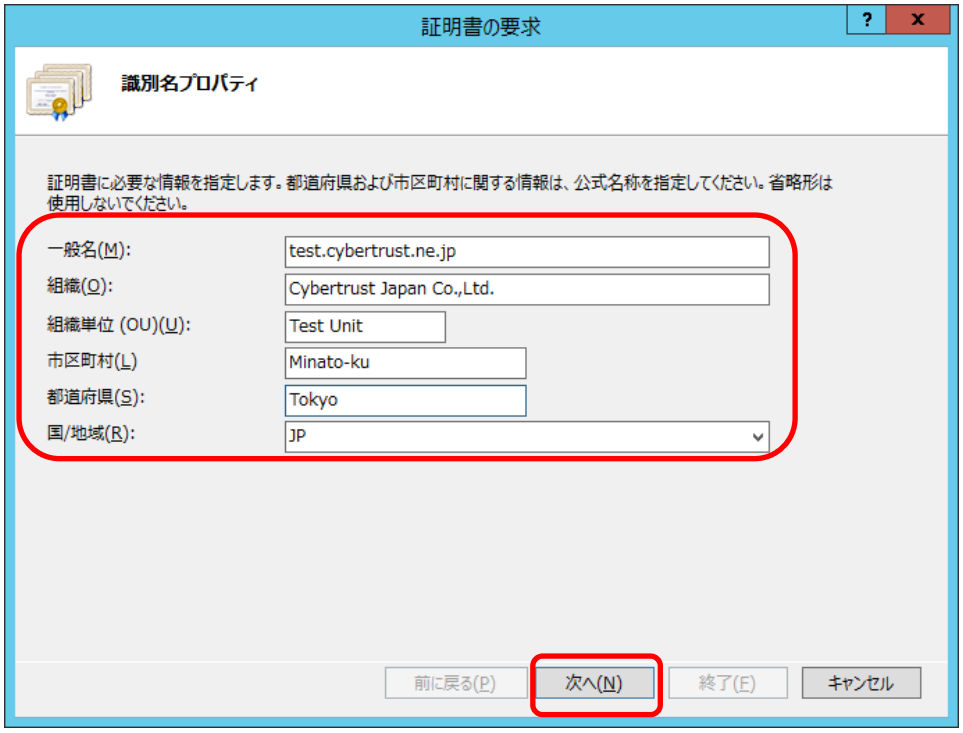


D) 識別名プロパティを入力する画面が表示されますので、CSR に設定する情報を入力して、【次へ】をクリックします。以下のルールに従って正確に入力してください。

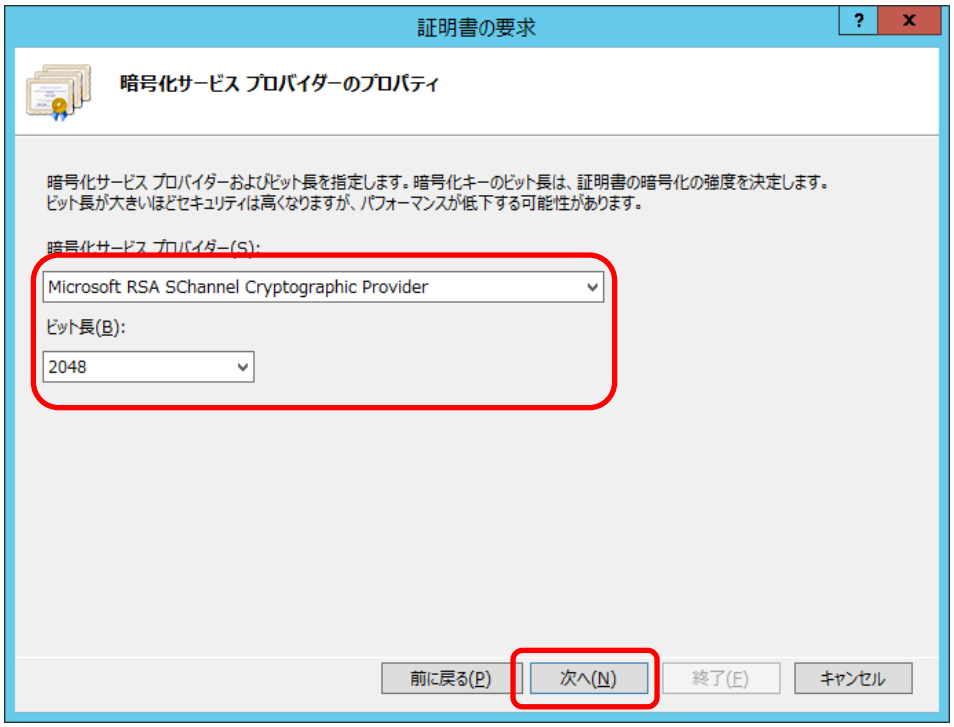
※半角英数字で入力してください。
※使用可能文字:スペース「a-z」「A-Z」「0-9」「'」「,」「.」「( )」「:」「-」「?」「&」

入力項目	内容	入力例
一般名	完全なドメイン名(FQDN)	test.cybertrust.ne.jp
組織	申請組織の名称((英語)	Cybertrust Japan Co.,Ltd.
組織単位	「部署名」(※)	Test Unit
市区町村	申請組織の事業所住所の「市町村名」(英語) ※東京は 23 区	Minato-ku
都道府県	申請組織の事業所住所の「都道府県名」(英語)	Tokyo
国/地域	申請組織の国名	JP

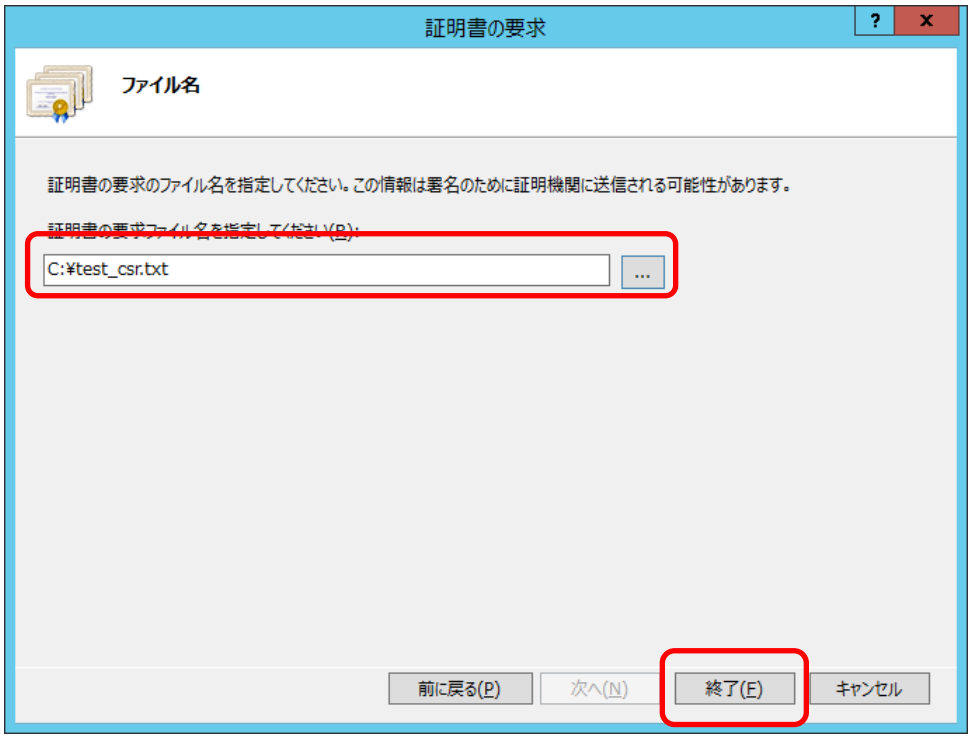
※OU の値につきましては、申請の際に申請サイト上にて空欄に変更することをお勧めします。
詳細はこちらをご覧ください。



E) 【暗号化サービス プロバイダー】は、表示された情報(Microsoft RSA SChannel Cryptographic Provider)を選択し、「ビット長」は「2048」と指定してください。



F) CSR のファイル名と保存先を指定し、【終了】をクリックします。



以上で、CSR の作成は完了です。

3. 証明書のお申し込み

作成した CSR をテキストエディタで開いて内容をコピーし、WEB の申請サイト(Cert Station)の申請フォームへ貼り付けて、弊社へお申し込みください。

＜CSR サンプル＞ ※申請にはご利用いただけません。

```
-----BEGIN NEW CERTIFICATE REQUEST-----
・・・・・
MIIEhDCCA2wCAQAwgYkxCzAJBgNVBAYTAkpQMQ4wDAYDVQQIDAVUb2t5bzESMBAG
A1UEBwwJTWluYXRvLWt1MSIwIAYDVQQKDBlDeWJlcnRydXNOIEphcGFuIENvLixM
dGQuMRIwEAYDVQQLDAlUZXNOIFVuaXQxHjAcBgNVBAMMFXRlc3QuY3liZXJOcnVz
2t/rD9fTPgo7u4aYzw4BpnAqLmGgy3XpsvCo6f4ROcFsgrk05FgeUCaeDFyllEST
・・・・・
-----END NEW CERTIFICATE REQUEST-----
```

「-----BEGIN NEW CERTIFICATE REQUEST-----」から、「-----END NEW CERTIFICATE REQUEST-----」までをハイフンを含め、すべてコピーし申請画面に貼り付けてください。

1 文字でも欠けるとフォーマットエラーとなりますのでご注意ください。

【！】CSR 作成後の注意事項

IIS8.0/8.5 では、CSR 作成後にキーペアのバックアップを取ることができない仕様となっております。そのため、SSL サーバー証明書のインストールが完了するまでは、証明書の登録要求を絶対に削除しないでください。

※証明書の登録要求を削除されますと、元の CSR で発行した SSL サーバー証明書のインストールができなくなり、サイバートラストへの再申請が必要になります。あらかじめ、ご注意ください。

証明書のインストール

【！】本手順はサーバー証明書の発行後に行います。

4. 証明書のダウンロード

インストールが必要となる中間 CA 証明書・SSL サーバー証明書を事前にダウンロードします。

4.1. 中間 CA 証明書のダウンロード

サーバー証明書をご利用の際、お使いの機器へ中間 CA 証明書のインストールが必要となります。

ご選択いただいた商品により必要な証明書が異なりますので、証明書の種類をご確認のうえ、以下弊社ホームページからダウンロードしてください。

≫ EV SSL Plus 中間 CA 証明書ダウンロード

≫ SSL Plus 中間 CA 証明書ダウンロード

4.2. SSL サーバー証明書のダウンロード

SSL サーバー証明書が発行されましたら、証明書発行のお知らせのメール内リンクより事前にダウンロードし、【.cer】や【.txt】などの拡張子で保存してください。

5. 証明書のインストール

中間 CA 証明書と SSL サーバー証明書のインストールを行います。

5.1. 中間 CA 証明書のインストール

中間 CA 証明書を「Microsoft 管理コンソール (Microsoft Management Console:MMC)」からインストールします。

※証明書更新時、すでに同じ内容の中間 CA 証明書がインストールされている場合は、この手順をスキップしてください。

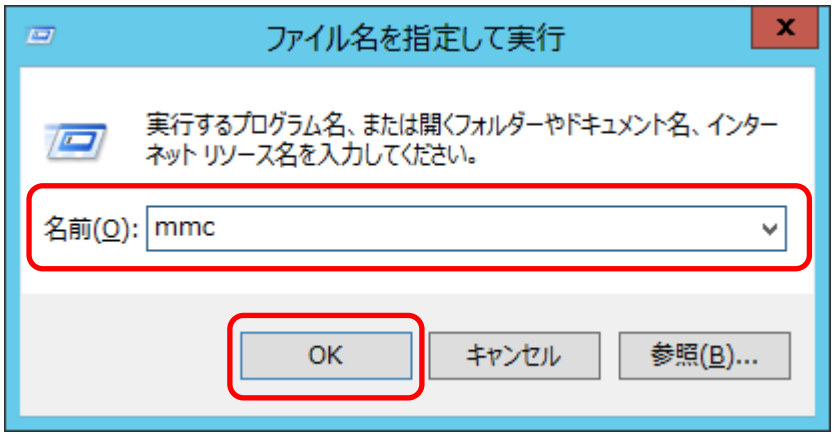
なお、必要な中間 CA 証明書のコモンネームが不明な場合は、サーバー証明書ファイルを開いて発行者のコモンネームの項目をご確認ください。

【例】EV SSL Plus の場合

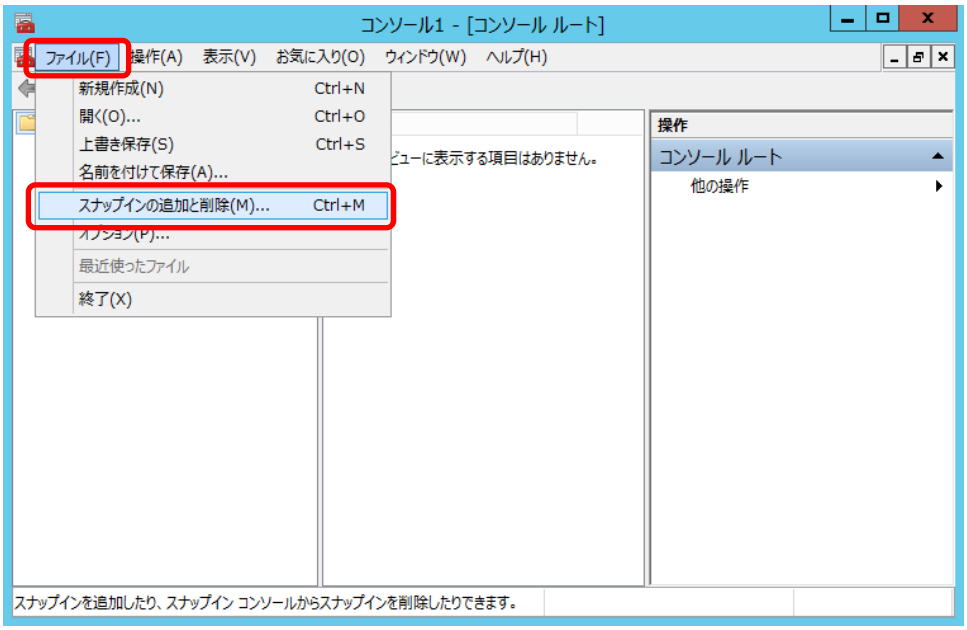
必要な中間 CA 証明書のコモンネーム

→Cybertrust Japan Extended Validation Server CA

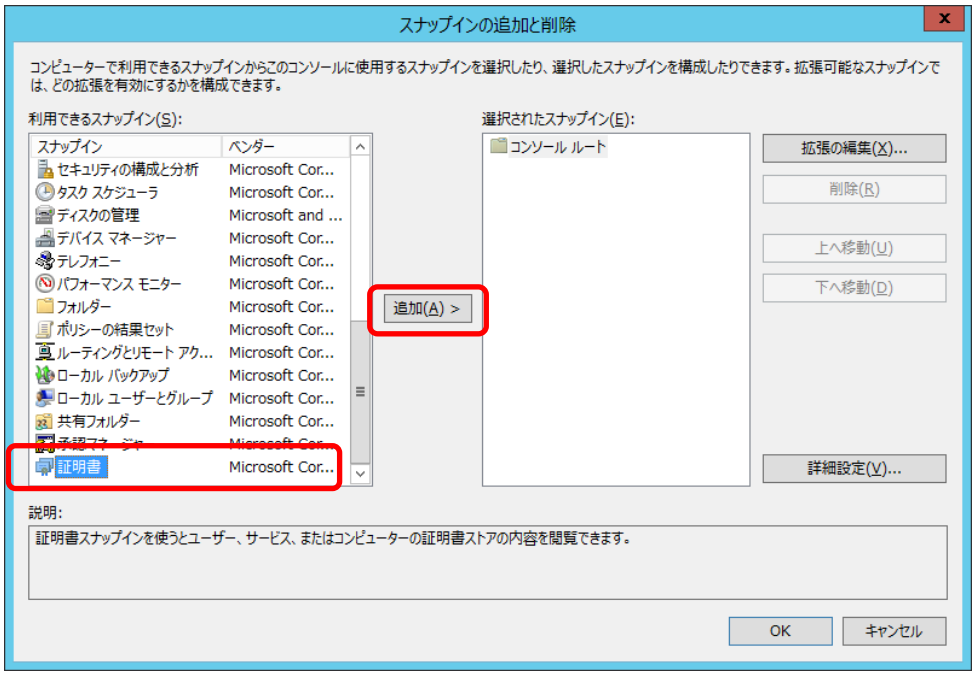
A) 【Windows ロゴ＋R キー】から【ファイル名を指定して実行】を開きます。
【名前】に「mmc」と入力して【OK】をクリックします。



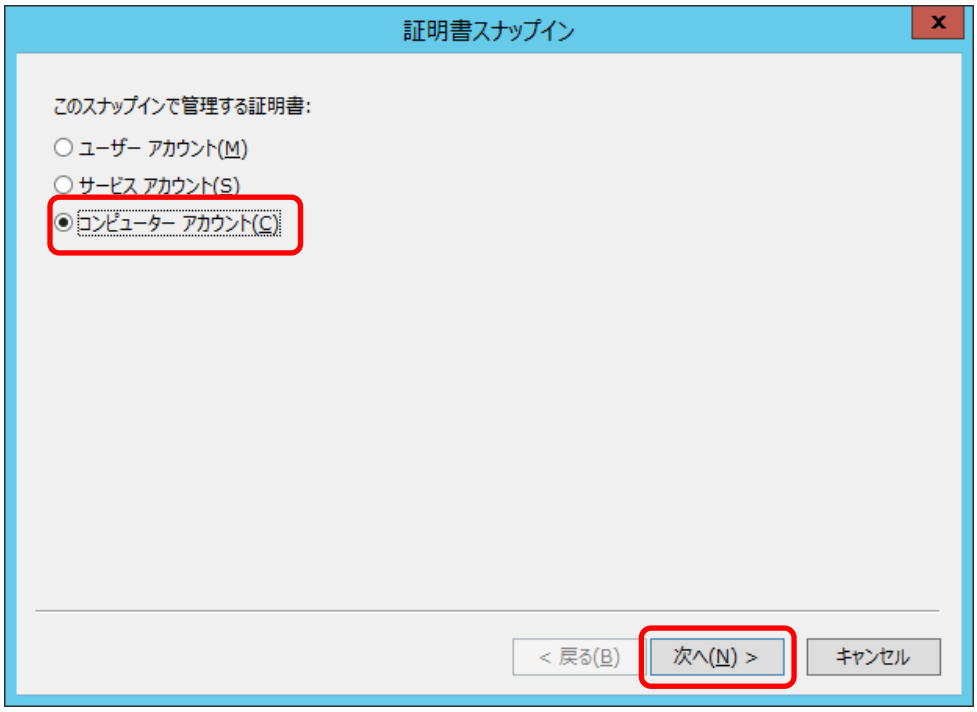
B) MMC 画面左上の【ファイル】メニューをクリックし、【スナップインの追加と削除】をクリックします。



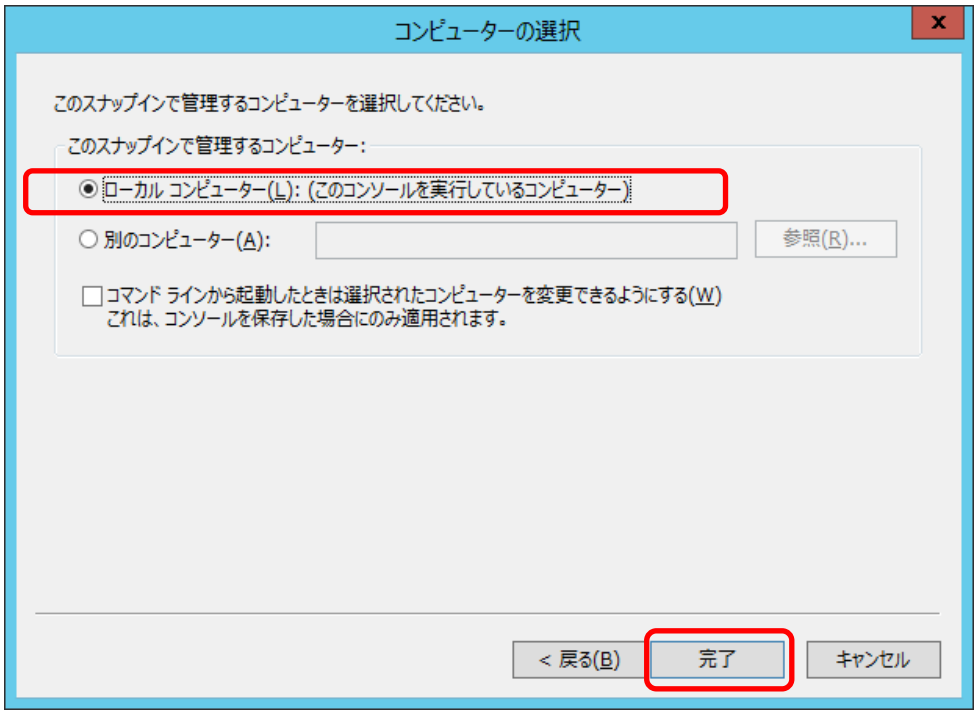
C) 【利用できるスナップイン】から【証明書】を選択し、【追加】をクリックします。



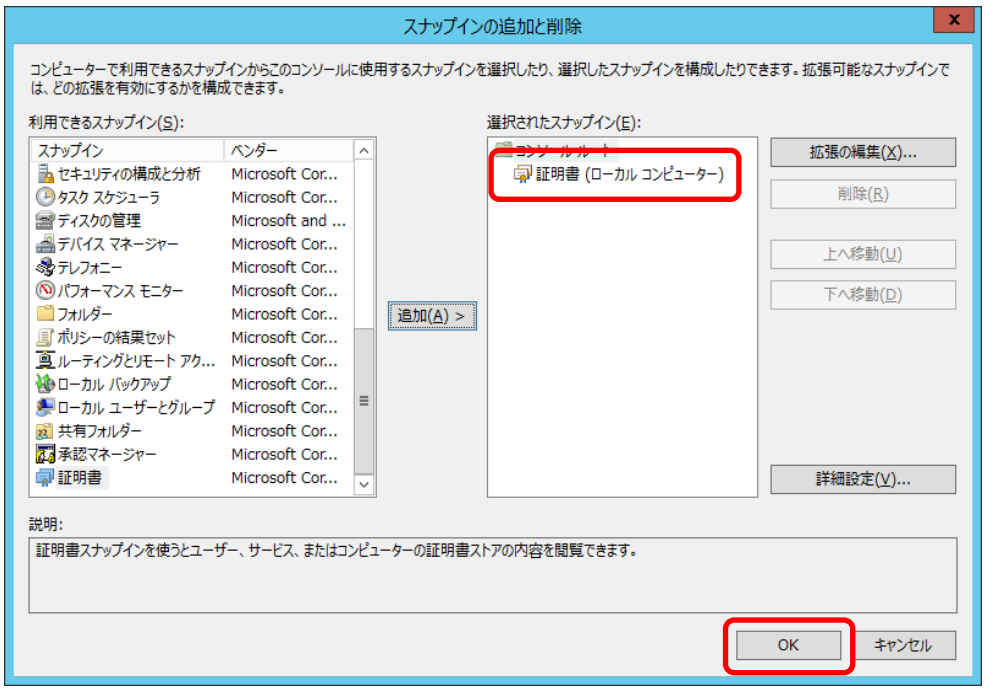
D) 【コンピューターアカウント】を選択し、【次へ】をクリックします。



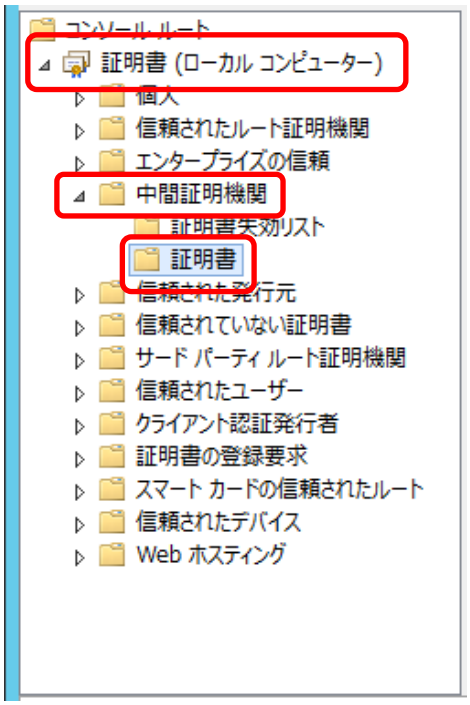
E)【ローカルコンピューター(このコンソールを実行しているコンピューター)】を選択し、【完了】をクリックします。



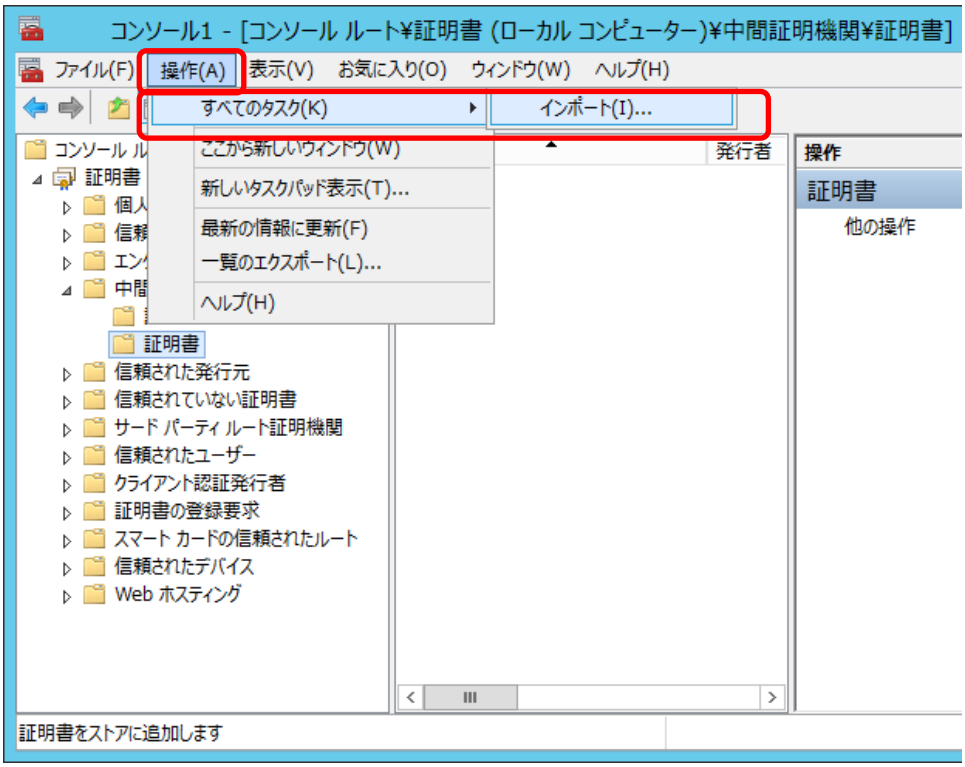
F)【選択されたスナップイン】に【証明書(ローカルコンピューター)】が追加されていることを確認し、【OK】をクリックします。



G) コンソールルートへ【証明書(ローカルコンピューター)】が追加されたことを確認し、【証明書(ローカルコンピューター)】→【中間証明機関】→【証明書】をクリックします。

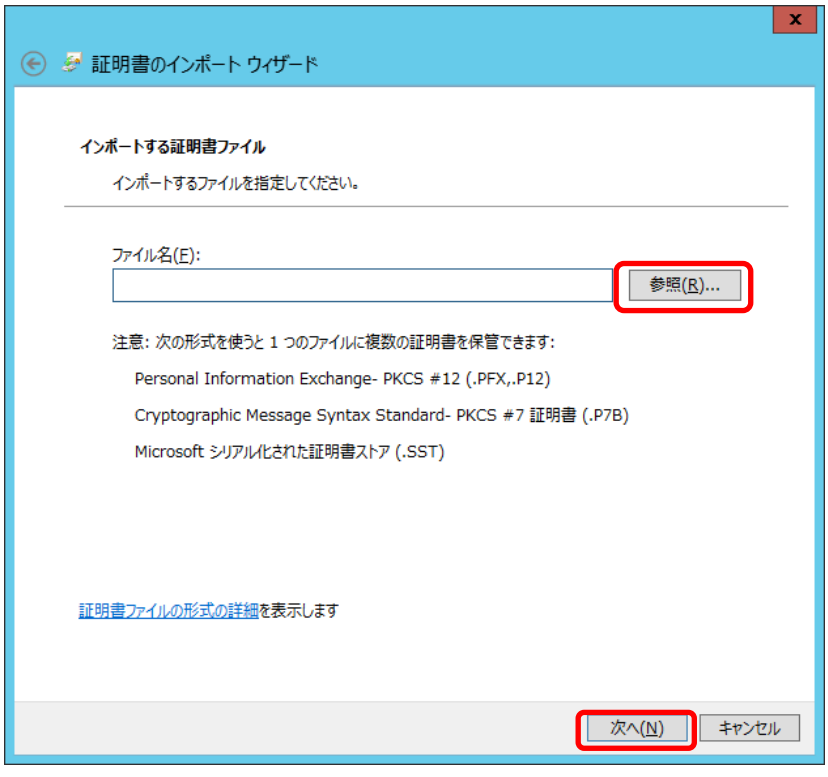


H) MMC 画面の左上の【操作】メニュー→【すべてのタスク】→【インポート】の順にクリックします。

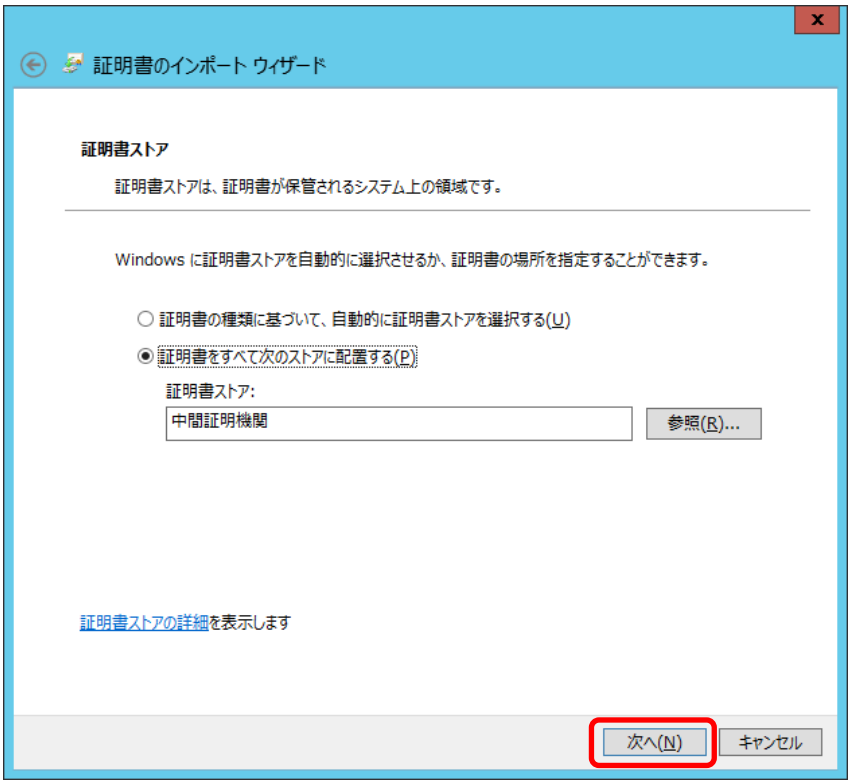


I) 証明書のインポートウィザードが表示されますので、【次へ】をクリックします。

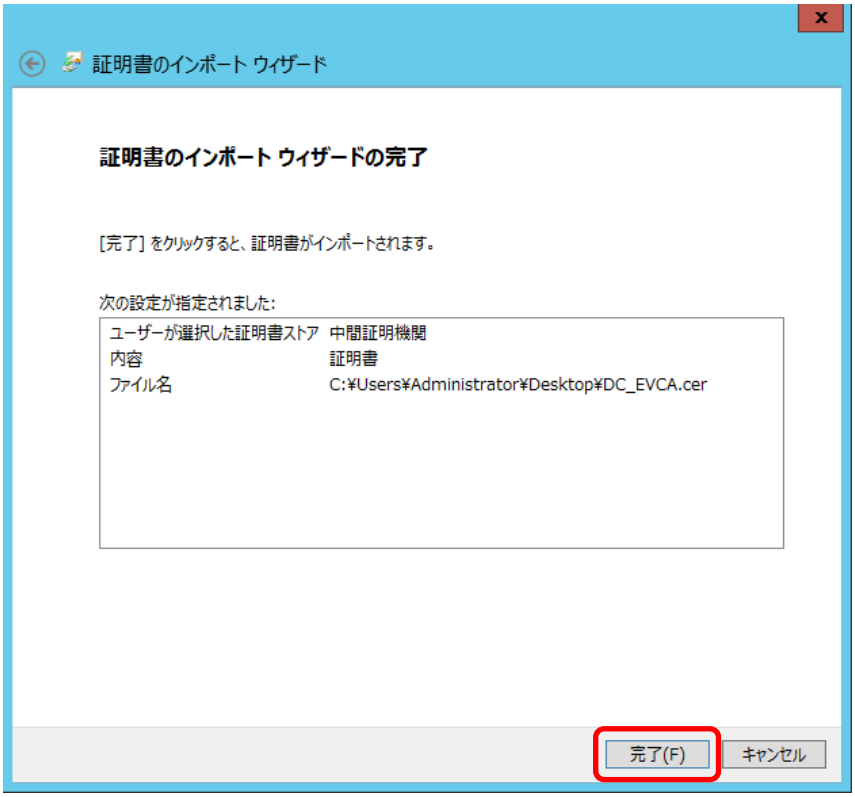
J) 【参照】をクリックしてインストールする中間 CA 証明書を指定し、【次へ】をクリックします。



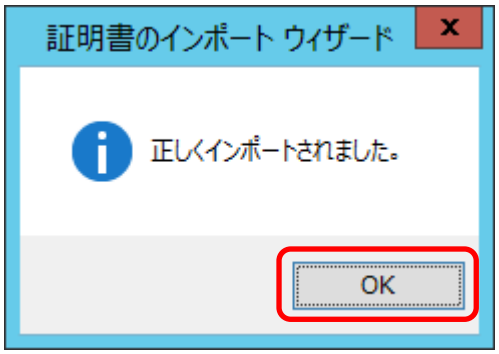
K) 【次へ】をクリックします。



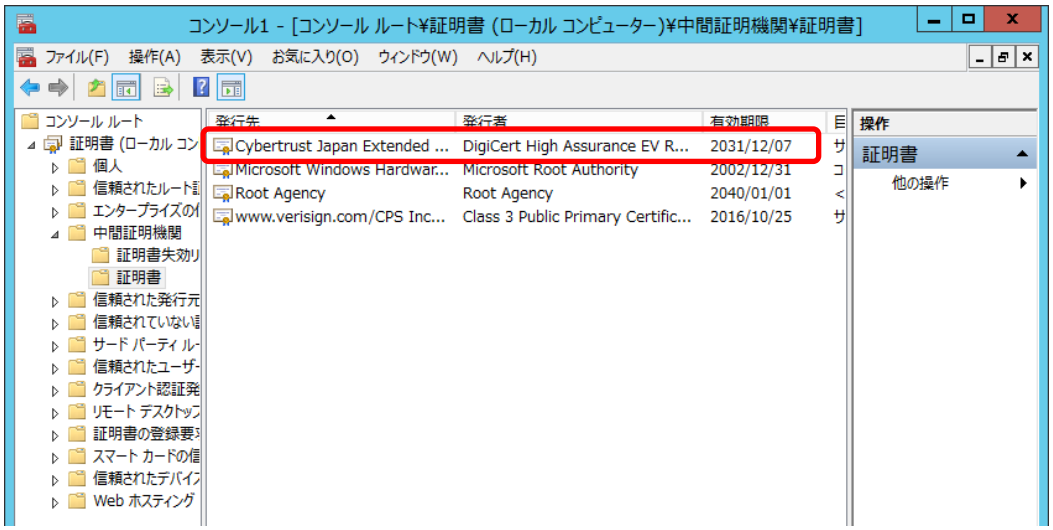
L) 次の画面が表示されたら内容を確認して、【完了】をクリックします。



M) インポート正常終了のメッセージが表示されますので、【OK】をクリックします。



N) 証明書の一覧にインストールした中間 CA 証明書が表示されていることを確認します。



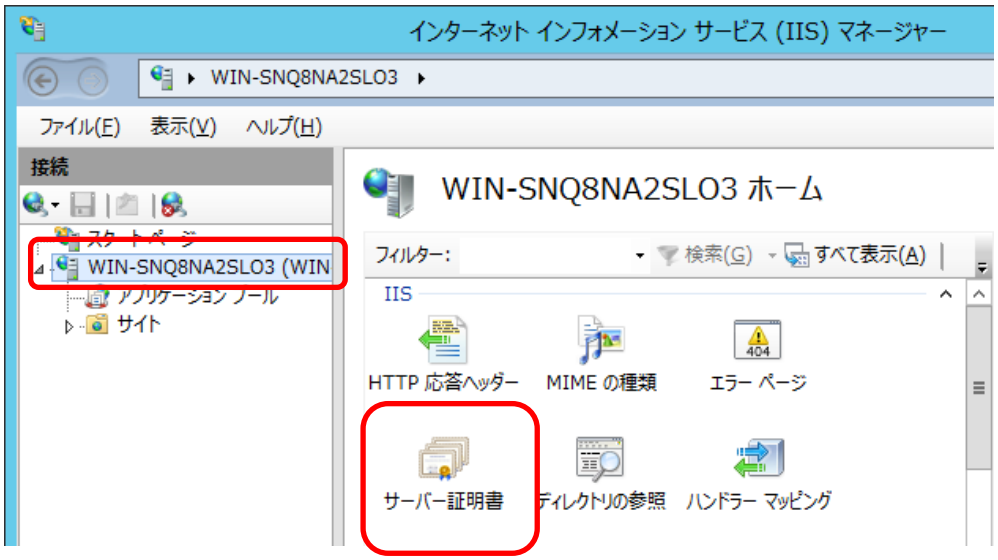
O) 上記画面を閉じる際に、「コンソールの設定をコンソール 1 に保存しますか？」と表示されますので、「いいえ」を選択して終了してください。

以上で中間 CA 証明書のインストールが完了します。

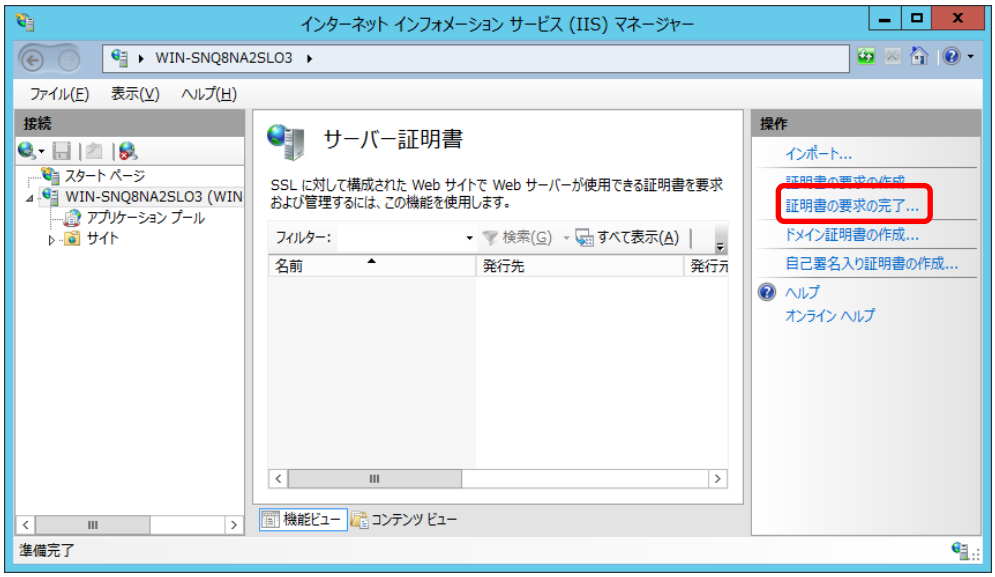
5.2. SSL サーバー証明書のインストール

SSL サーバー証明書のインストールを行います。

A) 【スタート】メニューから→【インターネット インフォメーション サービス (IIS) マネージャー】を選択して起動し、以下の画面から、【サーバー証明書】をダブルクリックします。



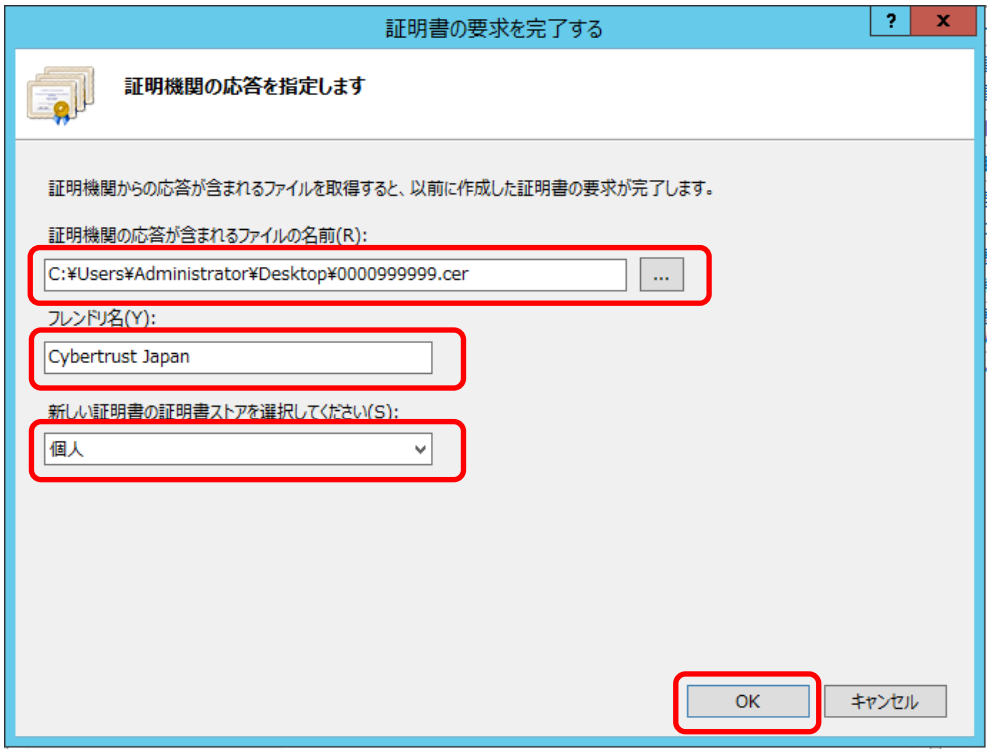
B) 画面右側の操作メニューから【証明書の要求の完了】をクリックします。



C) 【証明機関の応答が含まれるファイルの名前】に事前にダウンロードしたお客様の SSL サーバー証明書ファイルを指定し、【OK】をクリックします。

※【フレンドリ名】は任意の文字列を入力してください。わかりやすい文字列の入力をおすすめいたします。

※【新しい証明書の証明書ストアを選択してください】は「個人」を選択してください。「Web ホスティング」を選択するとエラーが発生します。

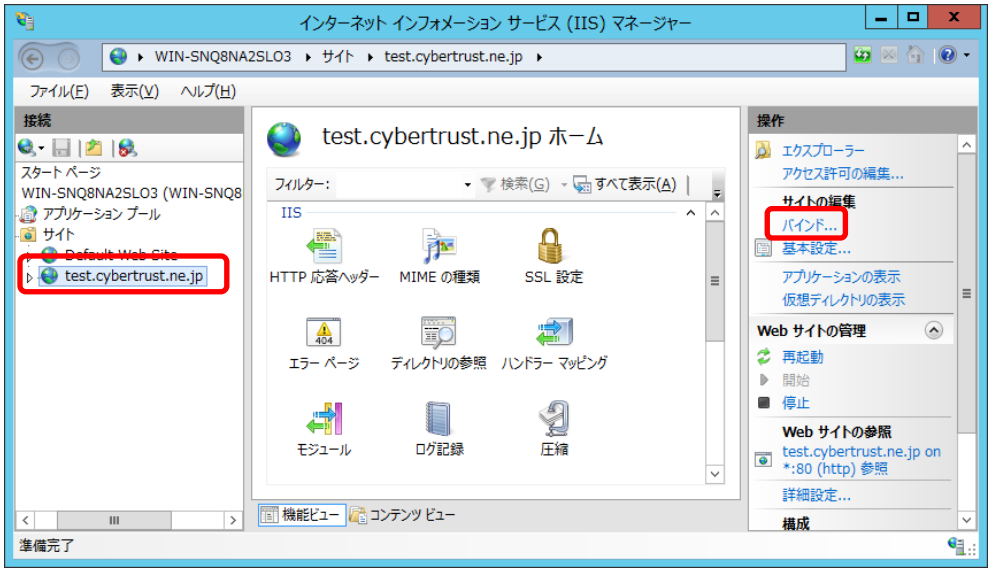


以上で SSL サーバー証明書のインストールは完了です。

6. SSL サーバー証明書の適用

インストールした SSL サーバー証明書をご利用の Web サイトへ適用します。

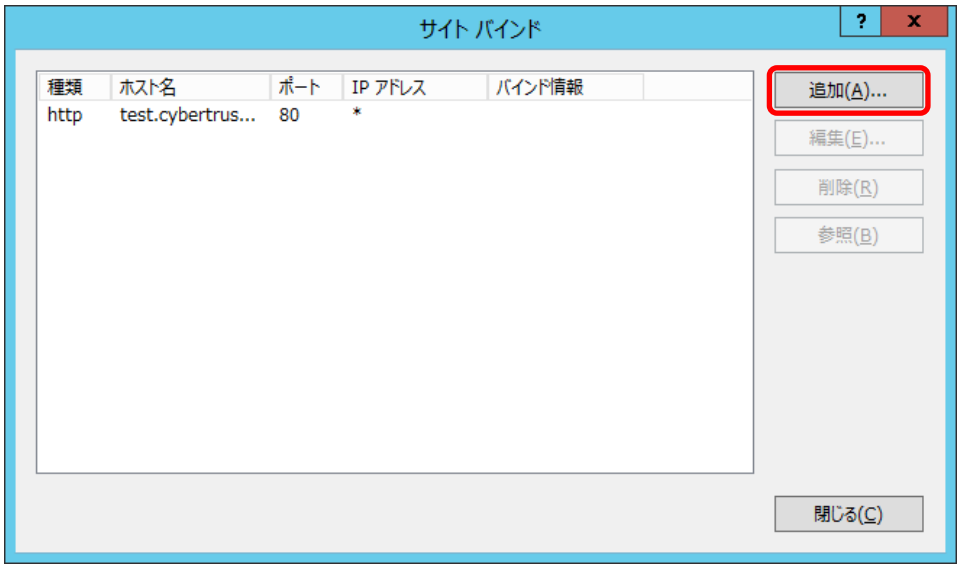
A) 【インターネット インフォメーション サービス (IIS) マネージャー】画面に戻り、SSL サーバー証明書を適用したい Web サイトを選択し、画面右側の操作メニューから【バインド】をクリックします。



B) 「サイトバインド」画面が表示されますので、新規の場合は【追加】をクリックします。

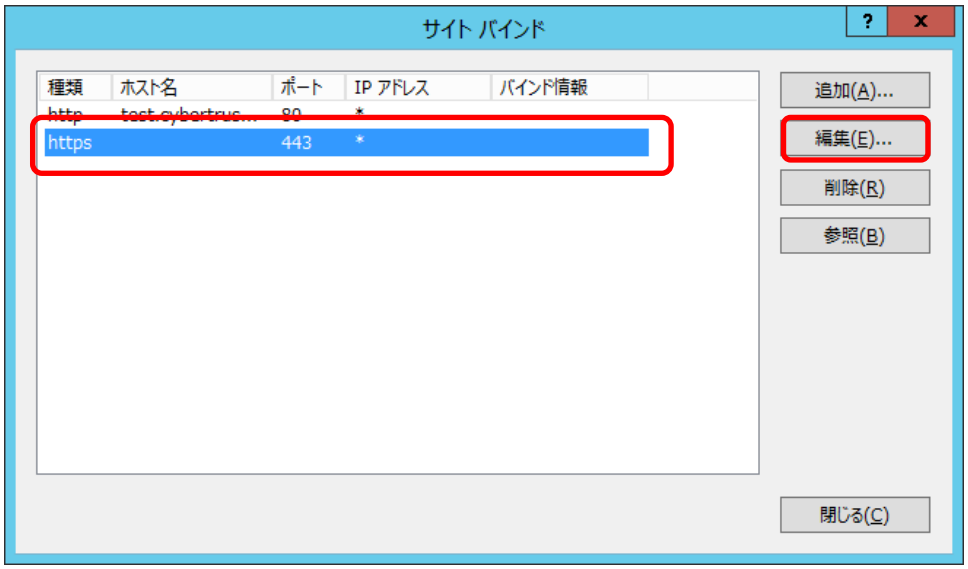
項目	入力内容
種類	https
IP アドレス	サーバー証明書を適用する Web サイトの IP アドレス
ポート	443 (もしくは、任意の SSL ポート番号)
SSL 証明書	インストール時に指定したフレンドリ名や証明書のコモンネームが表示されますので、適用したい SSL サーバー証明書を選択します。

■ 新規の場合

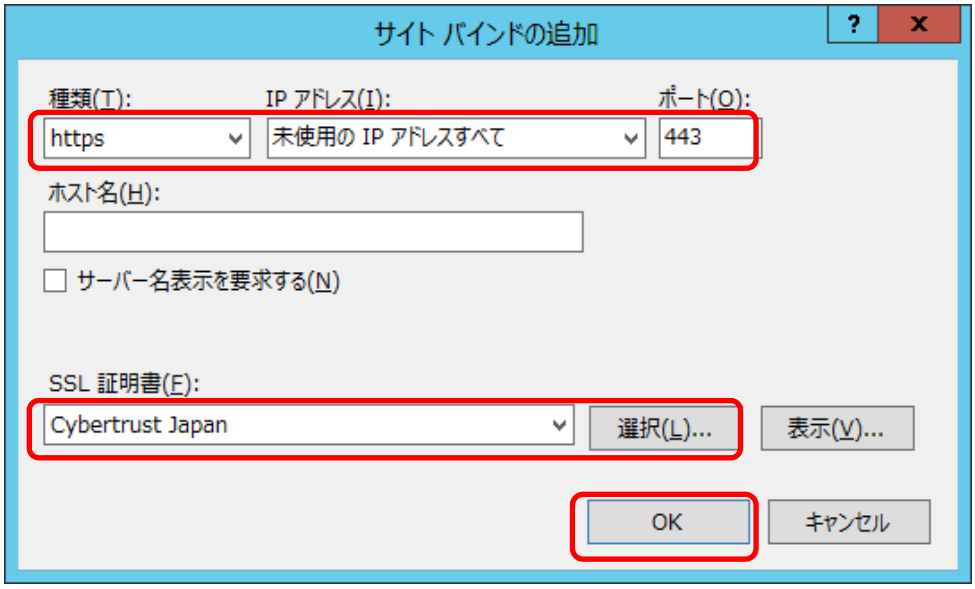


■ 更新の場合

C) 証明書更新の場合は既に https のバインド設定が存在しますので、そちらを選択して【編集】をクリックします。



D) **【サイトバインドの追加】または【サイトバインドの編集】画面が表示されますので、以下の情報を選択して【OK】をクリックします。**

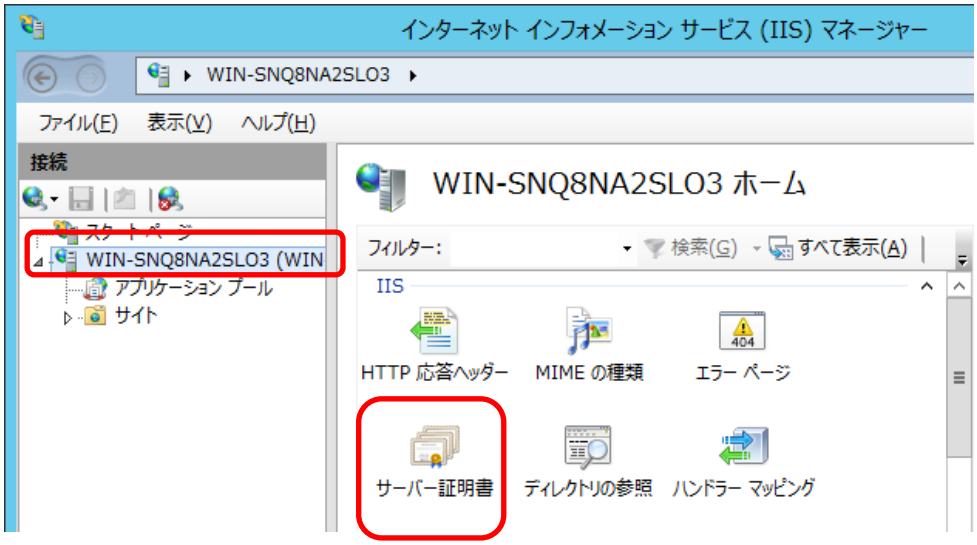


以上で SSL サーバー証明書の適用は完了です。

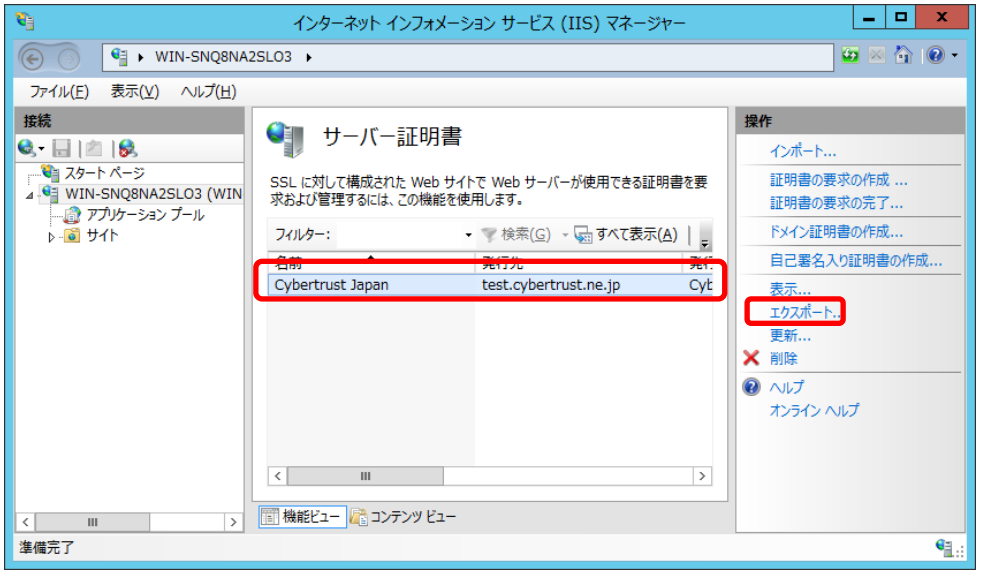
7. 鍵ペアファイルのバックアップ

鍵ペアファイルをバックアップします。

A) 【スタート】メニューから【インターネット インフォメーション サービス (IIS) マネージャー】を選択して起動します。以下の画面から、【サーバー証明書】をダブルクリックします。

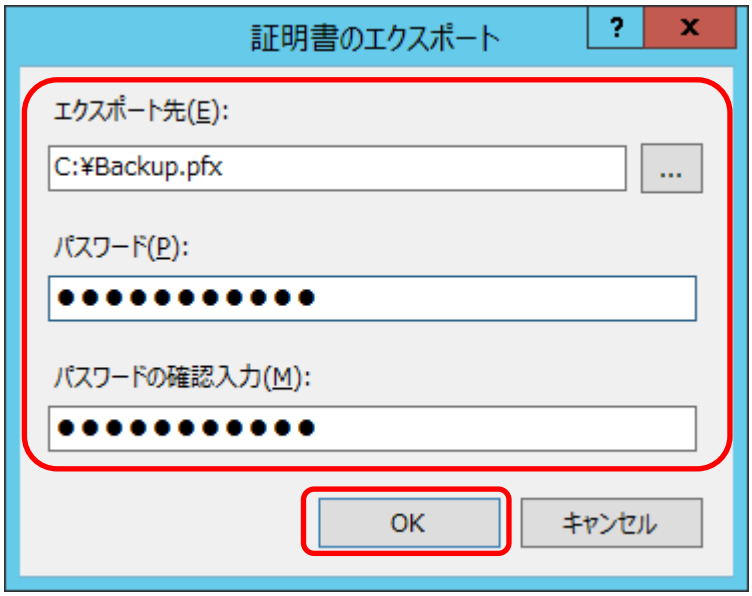


B) バックアップしたい SSL サーバー証明書を選択し、画面右側の操作メニューから【エクスポート】をクリックます。



C) 【エクスポート先】に保存先のフォルダとファイル名を指定します。ファイルの拡張子は【.pfx】を指定し、【パスワード】、【パスワードの確認入力】に同じパスワードを入力し、【OK】をクリックします。

※指定するパスワードは任意の文字列です。証明書のインポート時に入力が必要となります。



以上で、鍵ペアファイルのバックアップは終了です。

【!】注意事項

- パスワードを紛失した場合には、バックアップに利用できなくなりますので、取り扱いには十分注意してください。
- バックアップファイルは必ず別なメディア(USB や CD 等)にコピーして、安全な場所に保管してください。
- 弊社がお客様の秘密鍵ファイルの情報を受け取ることはございません。あらかじめご了承ください。

SSL 通信の確認

8. SSL 通信の確認

サーバー証明書が正しくインストールされ、エラーやセキュリティ警告が表示されず、正常に SSL 通信が可能であることを確認します。

SSL 通信の確認は設定を行っているサーバー以外の Web ブラウザや携帯電話、スマートフォンなどの携帯端末などから行うことを推奨します。

■ 設定確認例

- Internet Explorer 11

＜EV SSL Plus＞

＜SSL Plus＞

- Firefox 51

＜EV SSL Plus＞

＜SSL Plus＞