cybertrust

SureServer for SAKURA/SureServer for SAKURA(EV)

Microsoft IIS7.0/7.5

CSR 作成/証明書インストール手順書

（新規・更新用）

Version 1.1

PUBLIC RELEASE

2015/04/21

改訂履歴

日付	バージョン	内容
2014/12/10	1.0	初版リリース
2015/04/21	1.1	サイバートラストの WEB ディレクトリ変更に伴うリンク先 URL の修正

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 7.0/7.5(以下、IIS7.0/7.5)」の環境下でサイバートラストのサーバー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、IIS7.0/7.5 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。

このドキュメントで説明するソフトウェアはライセンスに基づいて配布されるものであり、ライセンスの条項に従った使用のみ許可されます。このドキュメントは、本来の使用目的のために発行され、公に発行されるものではありません。

このドキュメントの一部または全部を複製することは禁じられており、提供または製造を目的として使用することはできません。

ただし、サイバートラスト株式会社との契約または同意文書で定められている場合に限り、この注記の添付を条件として複製することができます。

サイバートラスト株式会社から事前に書面による合意を得ない限り、このドキュメントまたはその一部から直接的または間接的に知り得た内容または主題に関して、個々の企業やその従業員などの第三者に対し、口頭、文書、またはその他のいかなる手段によっても伝達することはできません。

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。

※2048bit 未満の鍵長をご指定の場合、証明書の申請時にエラーとなりますのでご注意ください。

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。
・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。
・日本語は使用しないでください。
・個人事業主の方は入力項目が異なります。詳細につきましては、個人事業主のお申し込み方法をご参照ください。

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
		グローバル IP アドレス(※1)	https://212.xxx.xxx.xxx/index.html ⇒ 212.xxx.xxx.xxx
●	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 SureServer for SAKURA(EV) は、コモンネームをグローバル IP アドレスとしてご指定いただけません。

※2 申請法人以外の名称、屋号、商標、住所、場所、その他特定の自然人や法人を参照する値を指定することはできません。

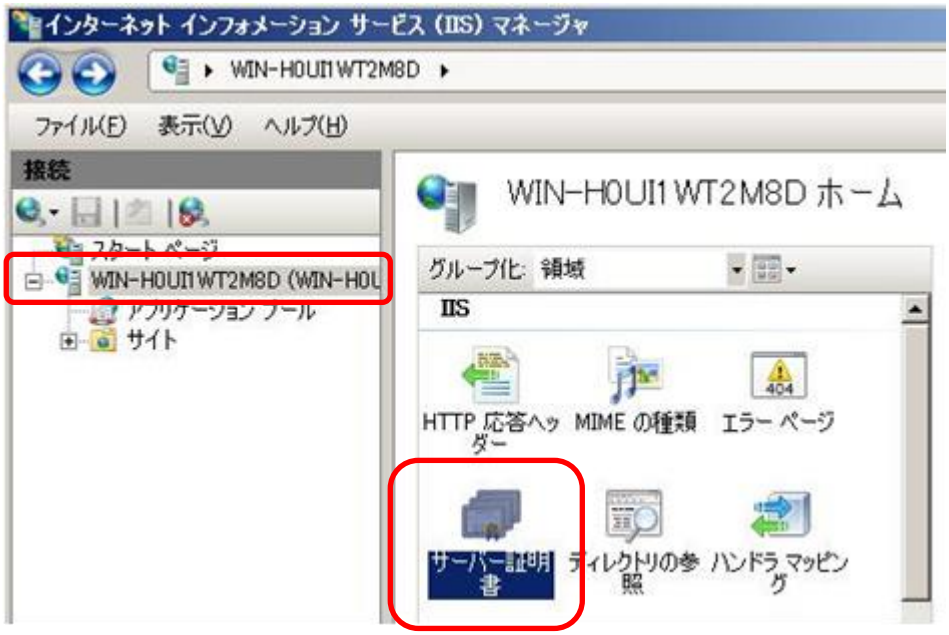
2. キーペア・CSR の作成

Microsoft Windows Server 2008 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】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。

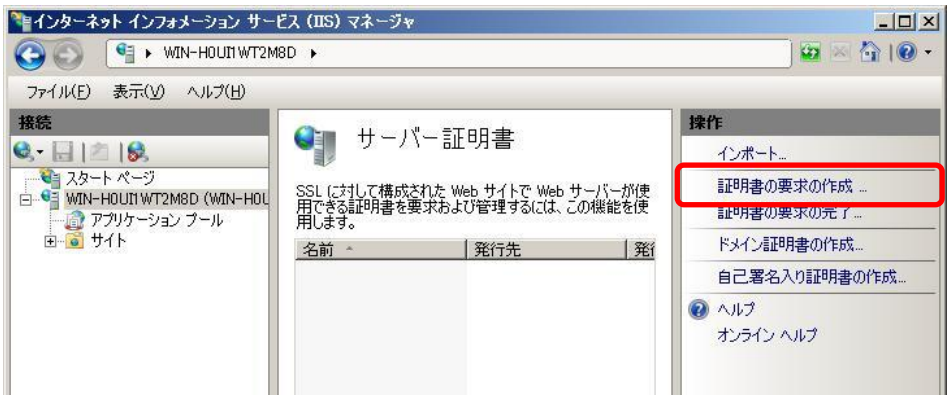
2.1. 作成方法

A) 【スタート】メニューから【コントロールパネル】→【管理ツール】→【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】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。

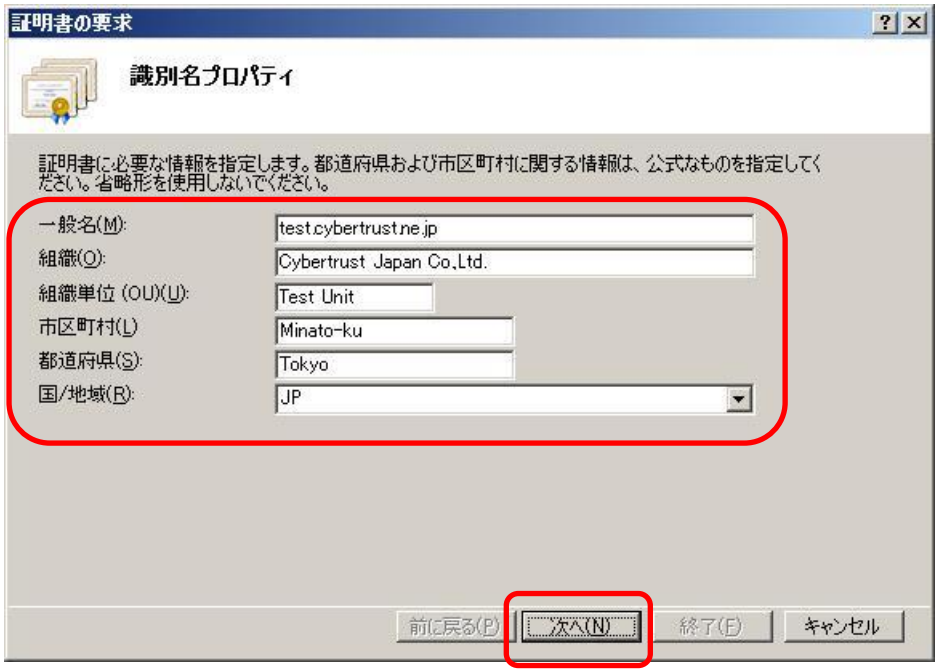


D) 識別名プロパティを入力する画面が表示されますので、CSR に設定する情報を入力して、【次へ】をクリックします。以下のルールに従って正確に入力してください。

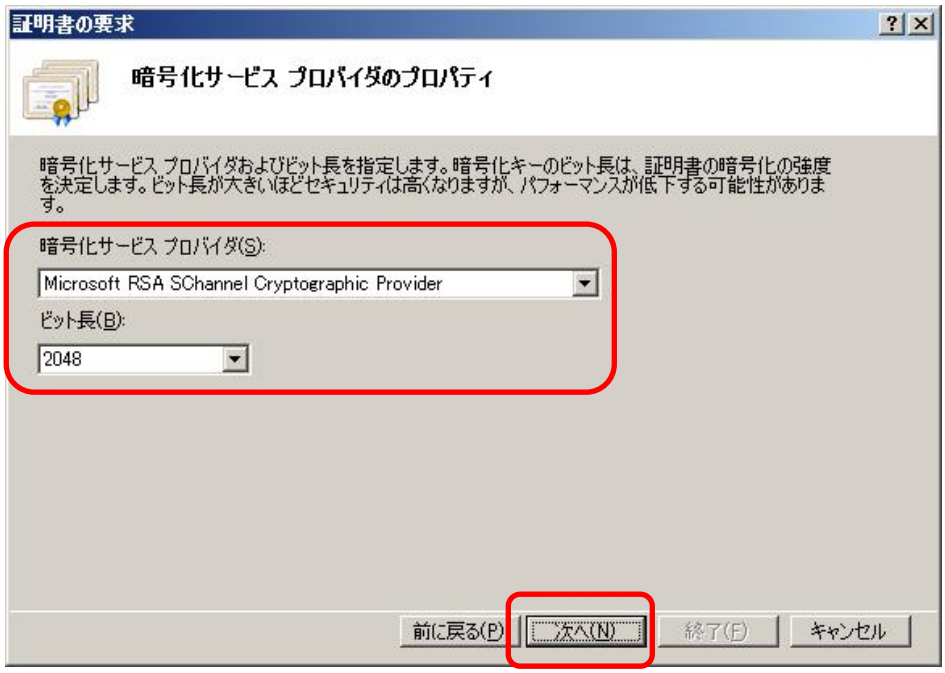
※半角英数字で入力してください。
※使用可能文字:スペース「a-z」「A-Z」「0-9」「'」「,」「.」「( )」「:」「-」「?」「&」

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

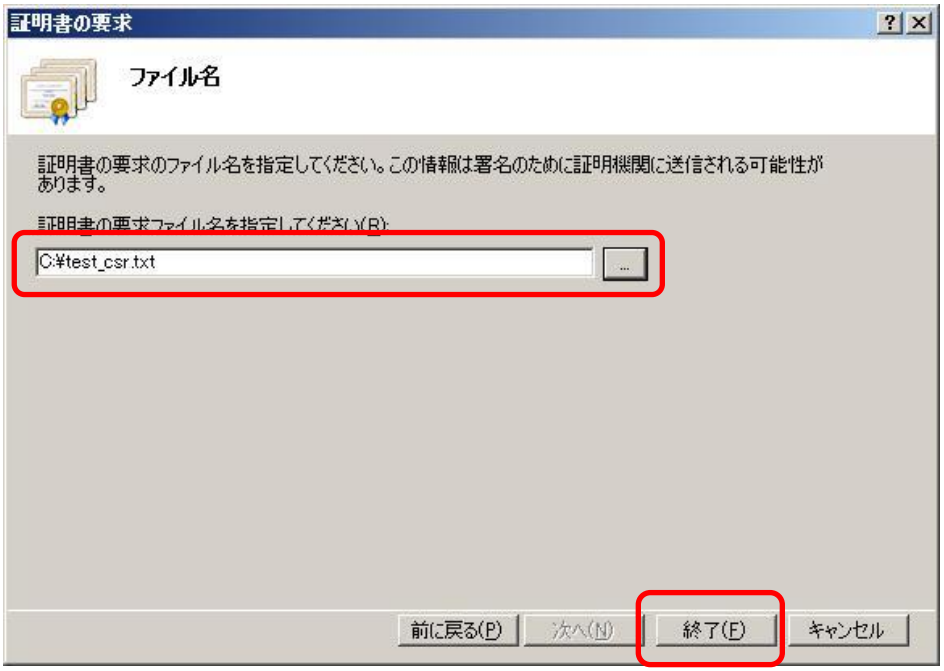
※申請法人以外の名称、屋号、商標、住所、場所、その他特定の自然人や法人を参照する値を指定することはできません。



E)【暗号化サービス プロバイダ】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、オンラインサインアップの入力フォームに貼り付けて、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
A1UEBwwJTWluYXRvLWt1MSIwIAYDVQQKDBlDeWJlcnRydXN0IEphcGFuIENvLixM
dGQuMRIwEAYDVQQLDAlUZXN0IFVuaXQxHjAcBgNVBAMMFXRlc3QuY3liZXJ0cnVz
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

IIS7.0/7.5 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、弊社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 URL からダウンロードしてください。

商品名	中間 CA 証明書
SureServer for SAKURA	https://www.cybertrust.ne.jp/sureserver/download/root_ca/PUBCAG3_sha2.txt
SureServer or SAKURA(EV)	中間 CA 証明書 1 https://www.cybertrust.ne.jp/sureserver/download/root_ca/evcag2_2_sha2.txt
	中間 CA 証明書 2 https://www.cybertrust.ne.jp/sureserver/download/root_ca/evcag2_sha2.txt

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、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。

A) SSL サーバー証明書の発行後にお送りするメール(件名:[さくらインターネット]《重要》SureServer サーバー証明書発行のお知らせ)に記載されている URL にアクセスします。

B) SSL サーバー証明書のダウンロード画面が表示されますので、お申し込み完了後にお送りしたメール(件名:【重要】お申込受付完了のお知らせ(ダウンロードパスワードご案内))に記載のパスワードを入力し、ダウンロードボタンをクリックしてください。

C) SSL サーバー証明書のダウンロード画面表示にならい、SSL サーバー証明書を任意のフォルダに保存してください。

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

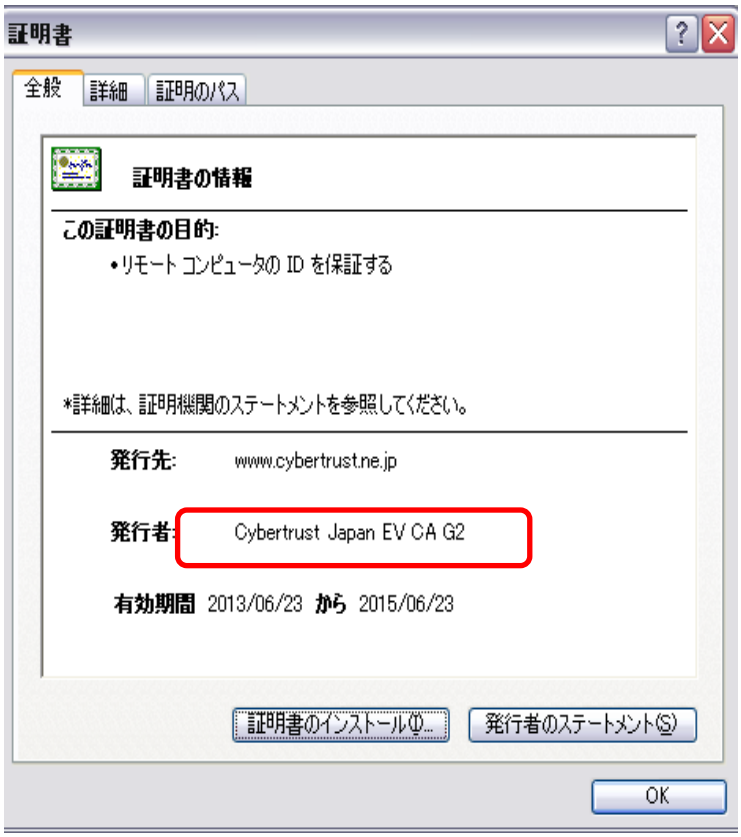
中間 CA 証明書を「Microsoft 管理コンソール (Microsoft Management Console:MMC)」からインストールします。

※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。

※SureServer for SAKURA(EV) では、同様の手順で「中間 CA 証明書 1」と「中間 CA 証明書 2」をインストールしてください。

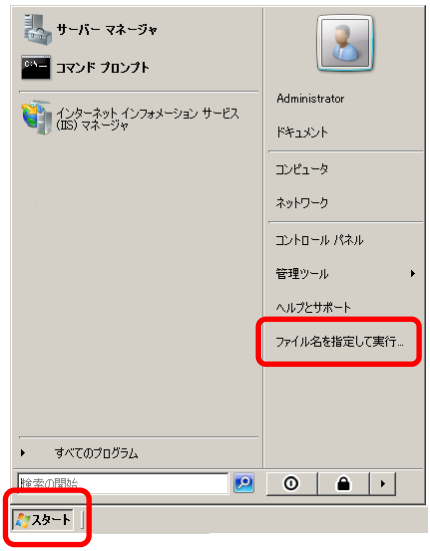
なお、必要な中間 CA 証明書のコモンネームが不明な場合は、サーバー証明書ファイルを開いて発行者のコモンネームの項目をご確認ください。

【例】SureServer for SAKURA(EV) の場合

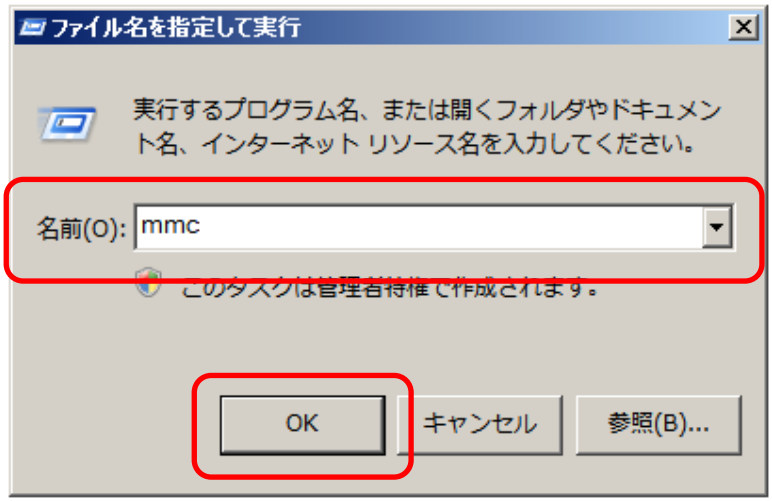


→必要な中間 CA 証明書のコモンネーム:Cybertrust Japan EV CA G2

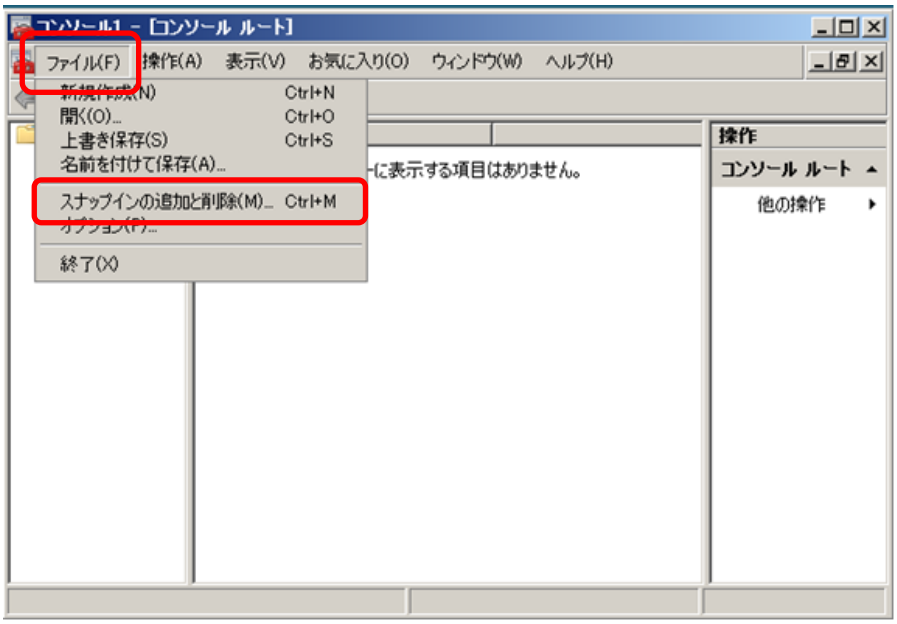
A) 【スタート】メニューから【ファイル名を指定して実行】をクリックします。



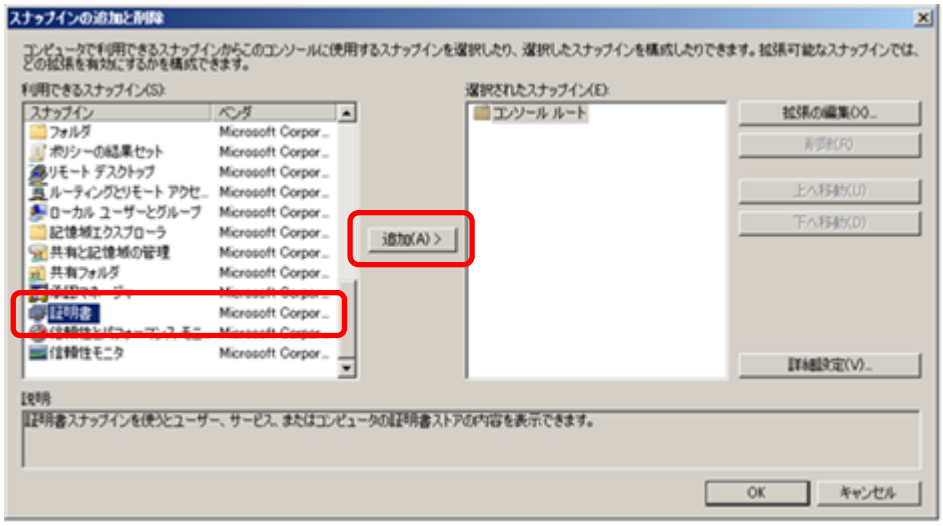
B) 【名前】へ「mmc」と入力して【OK】をクリックし、MMC を開きます。



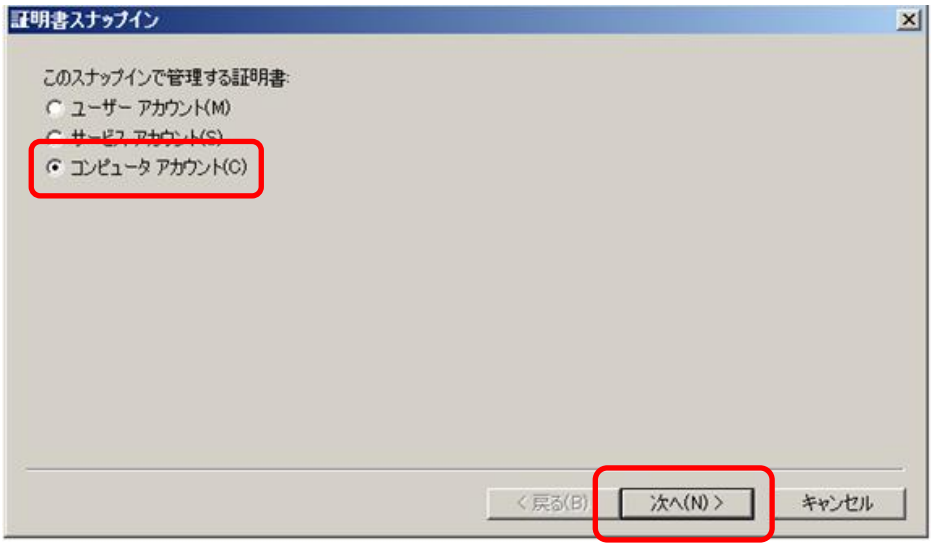
C) MMC 画面左上の【ファイル】メニューをクリックし、【スナップインの追加と削除】をクリックします。



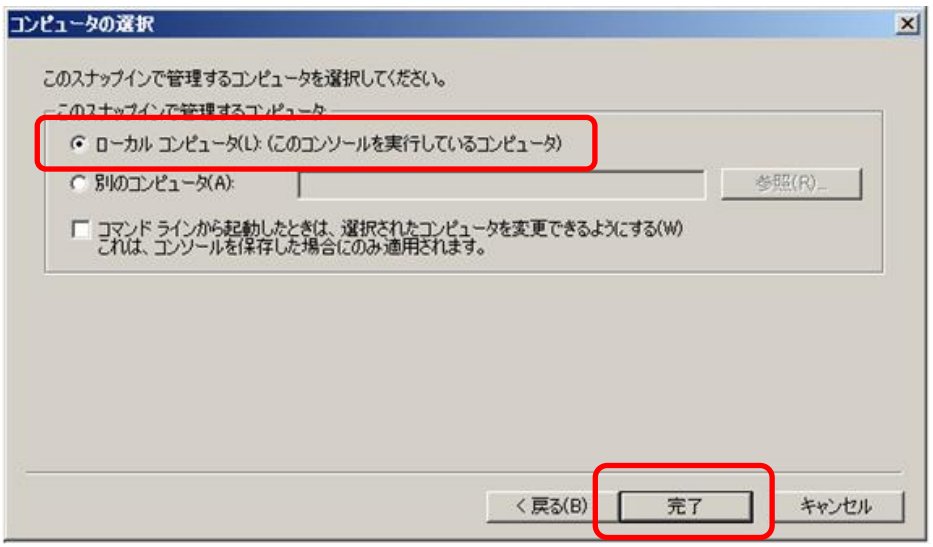
D) 【利用できるスナップイン】から【証明書】を選択し、【追加】をクリックします。



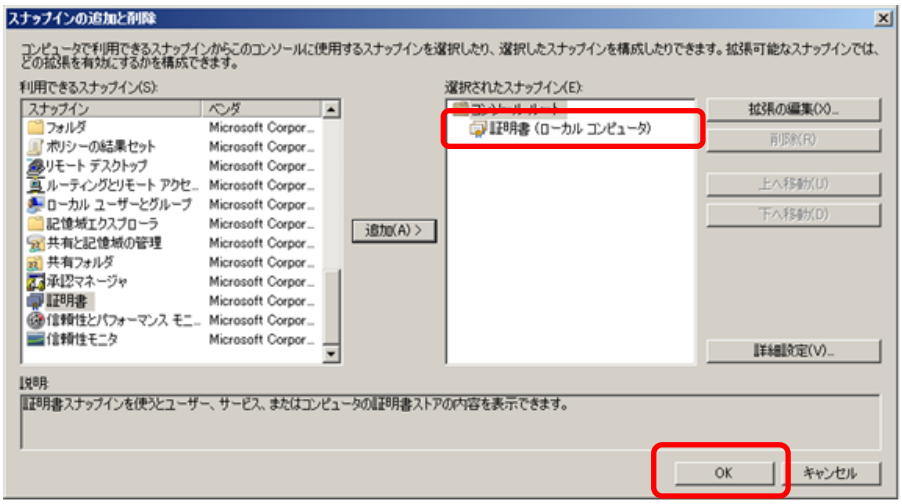
E) 【コンピュータアカウント】を選択し、【次へ】をクリックします。



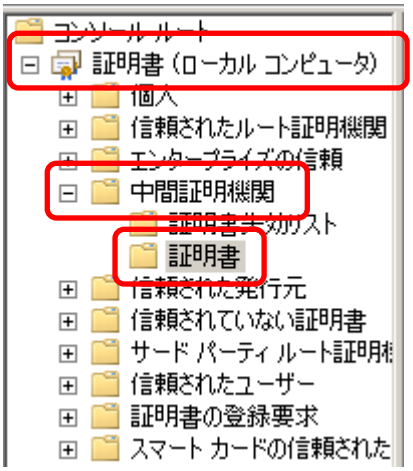
F) 【ローカルコンピュータ(このコンソールを実行しているコンピュータ)】を選択し、【完了】をクリックします。



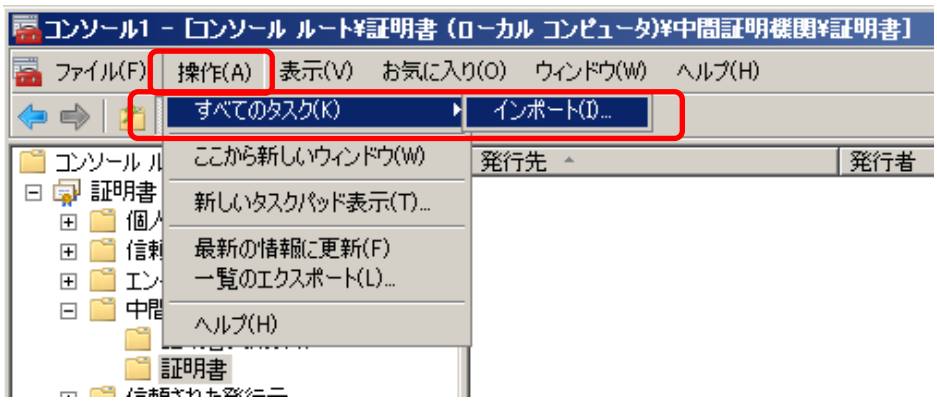
G) 【選択されたスナップイン】に【証明書(ローカルコンピュータ)】が追加されていることを確認し、【OK】をクリックします。



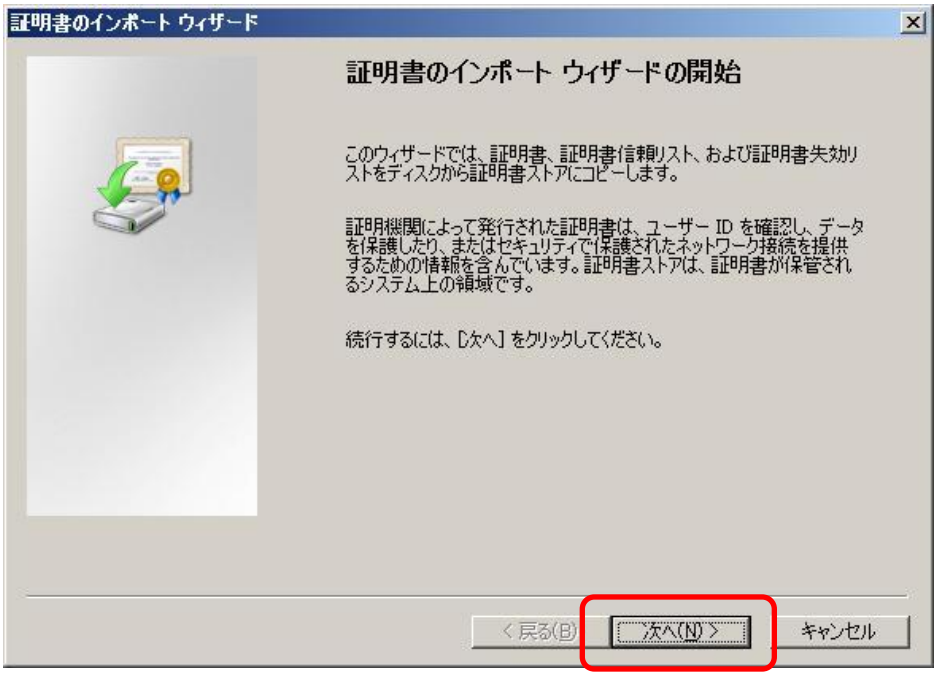
H) コンソールルートへ【証明書(ローカルコンピュータ)】が追加されたことを確認し、【証明書(ローカルコンピュータ)】→【中間証明機関】→【証明書】をクリックします。



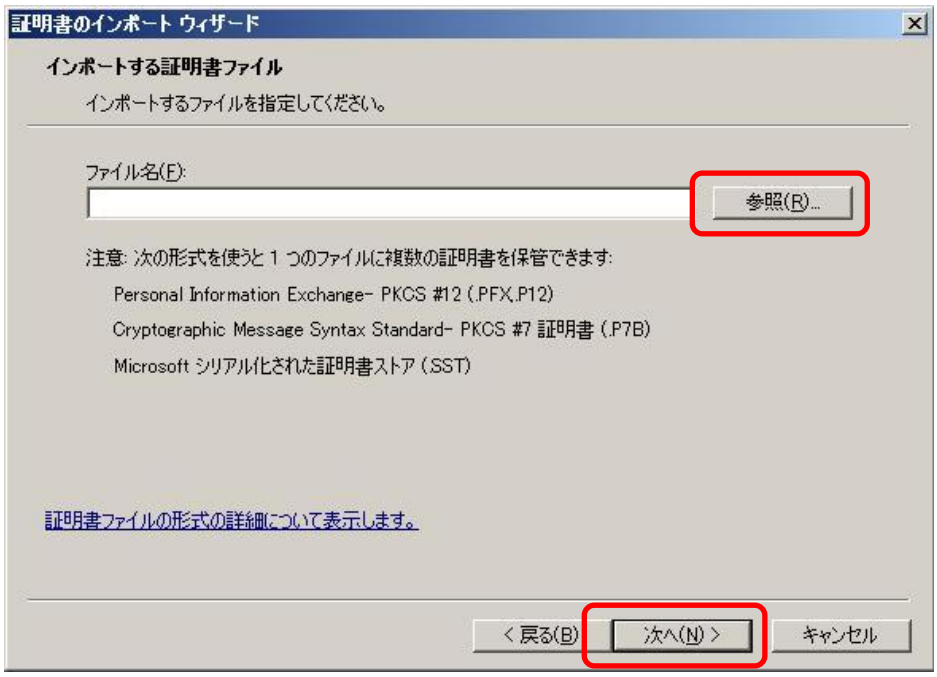
I) MMC 画面の左上の【操作】メニュー→【すべてのタスク】→【インポート】の順にクリックします。



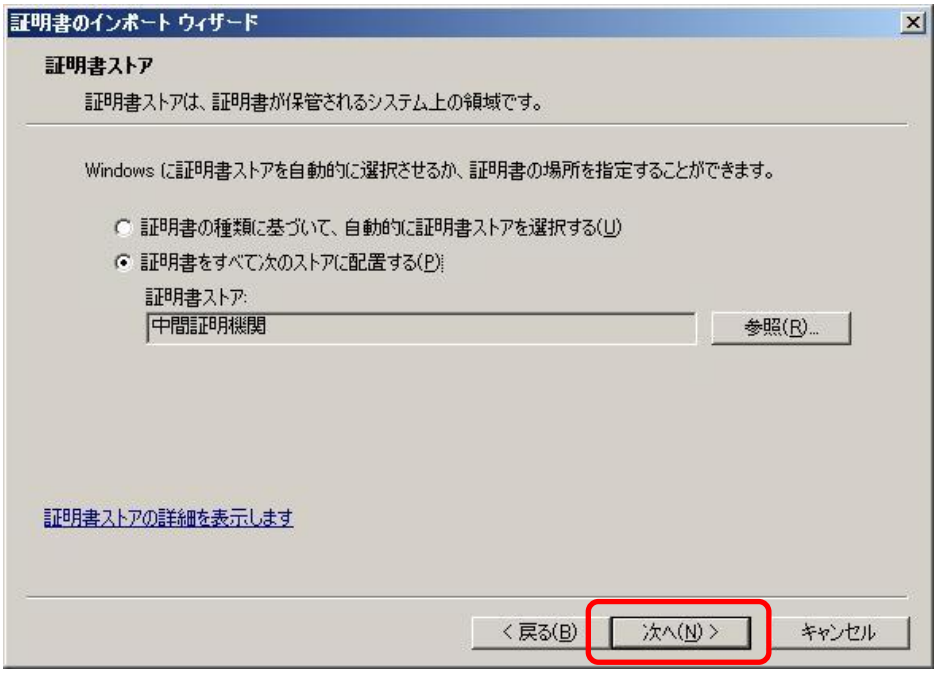
J) 証明書のインポートウィザードが表示されますので、【次へ】をクリックします。



K) 【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。



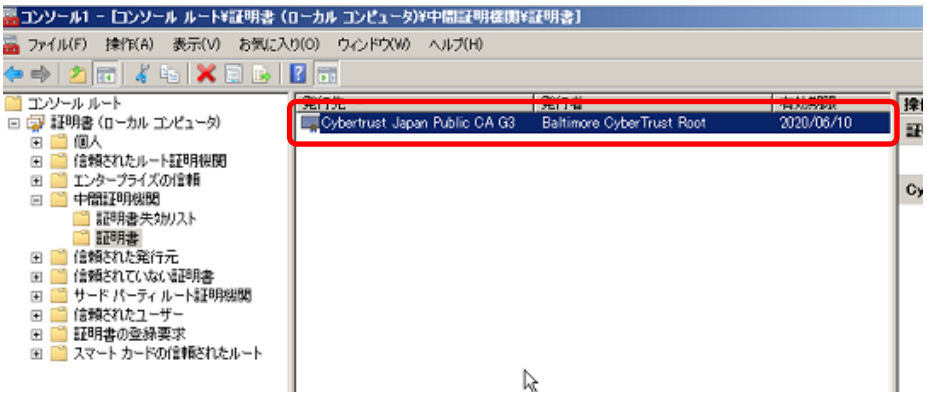
L) 【次へ】をクリックします。



M) 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。

N) 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。

O) 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。



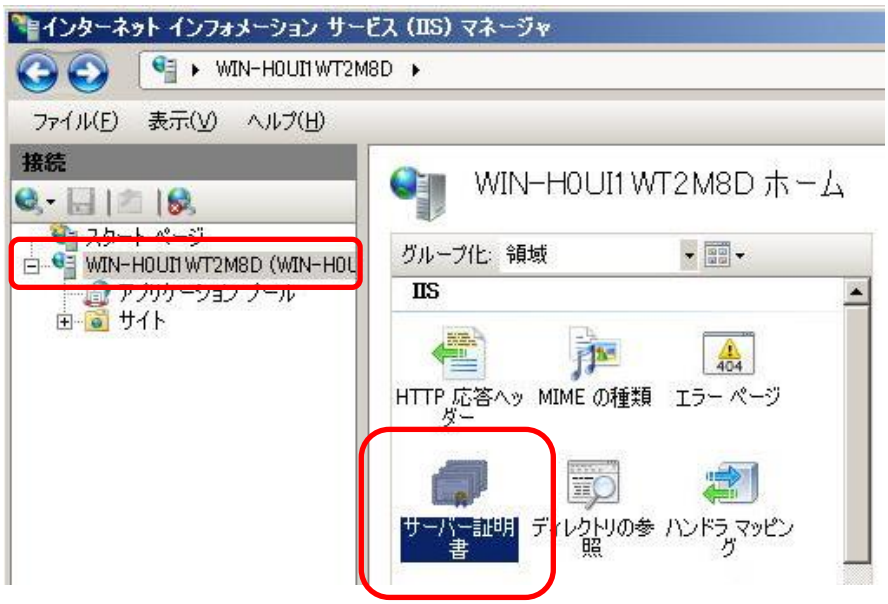
P) 上記画面を閉じる際に、「コンソールの設定をコンソール 1 に保存しますか？」と表示されますので、「いいえ」を選択して終了してください。

以上で中間 CA 証明書のインストールが完了します。

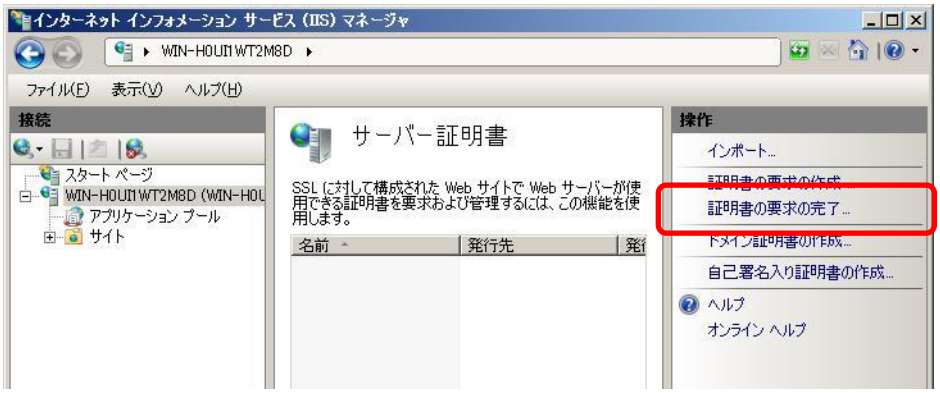
5.2. SSL サーバー証明書のインストール

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【コントロールパネル】→【管理ツール】→【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】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。

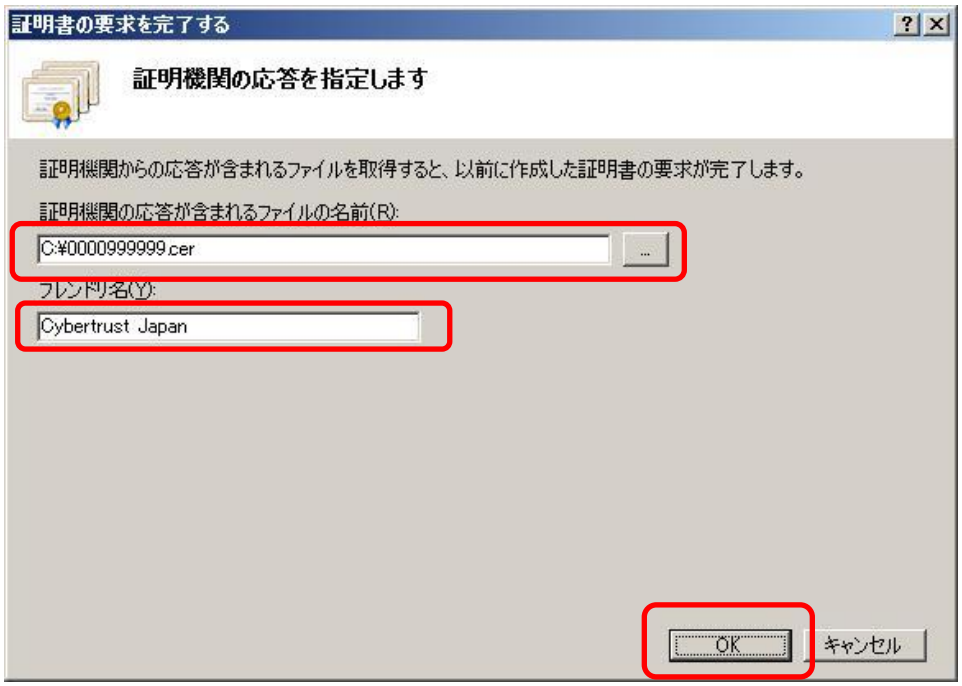


B) 画面右側の操作メニューから【証明書の要求の完了】をクリックします。



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。

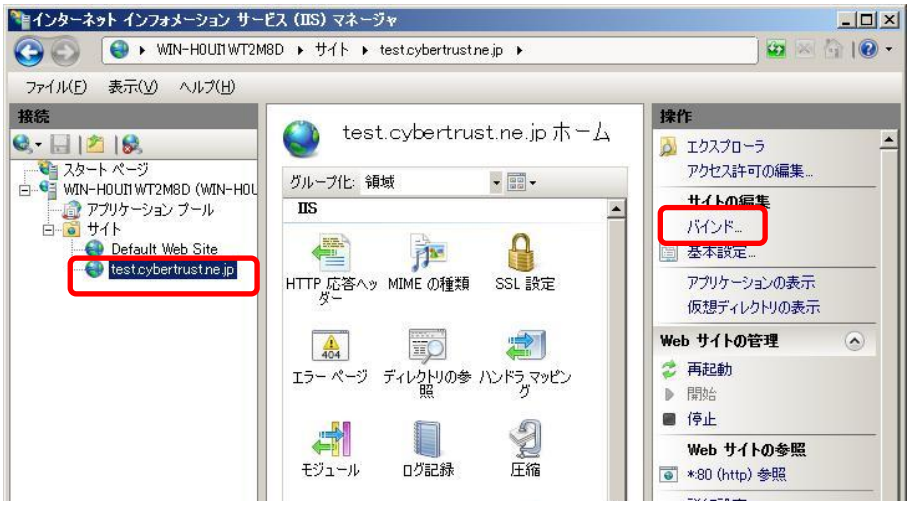


以上で SSL サーバー証明書のインストールは完了です。

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】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。

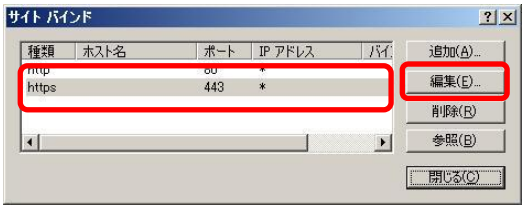


■ 新規の場合

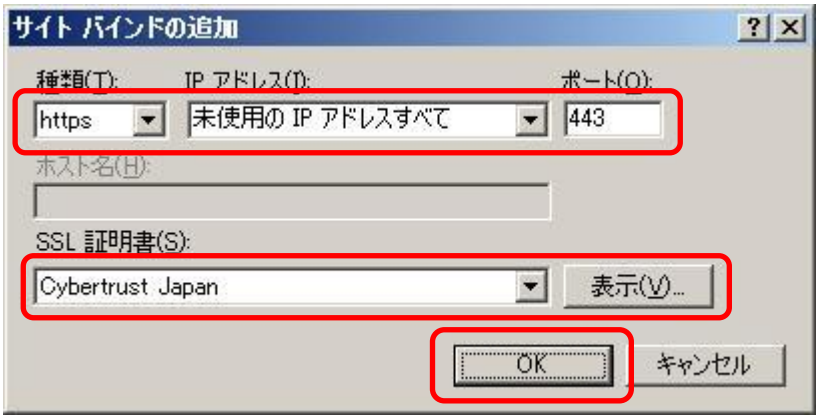
B) 「サイトバインド」画面が表示されますので、新規の場合は【追加】をクリックします。

■ 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。



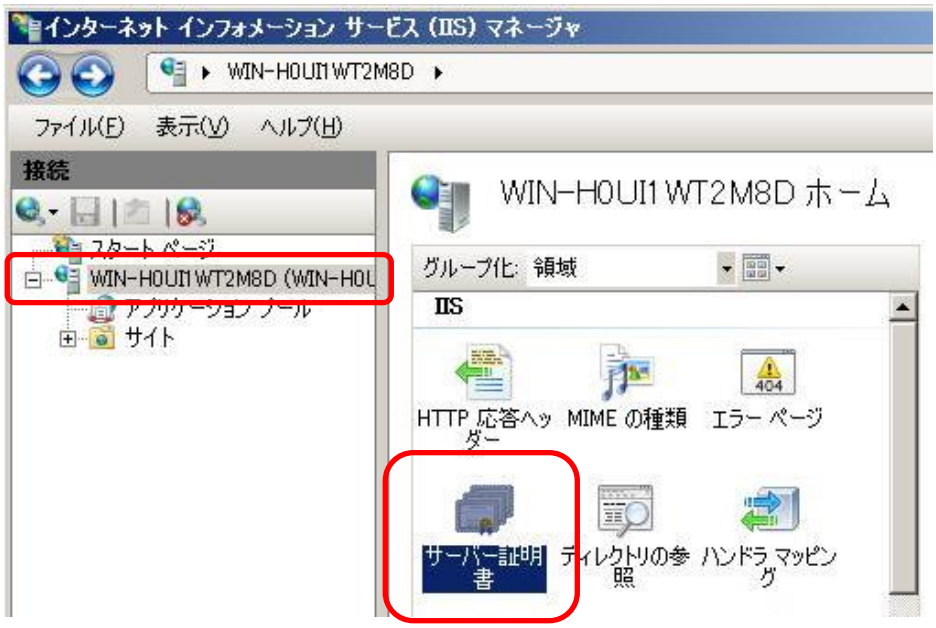
項目	入力内容
種類	https
IP アドレス	サーバー証明書を適用する Web サイトの IP アドレス
ポート	443 (もしくは、任意の SSL ポート番号)
SSL 証明書	インストール時に指定したフレンドリ名や証明書のコモンネームが表示されますので、適用したい SSL サーバー証明書を選択します。

以上で SSL サーバー証明書の適用は完了です。

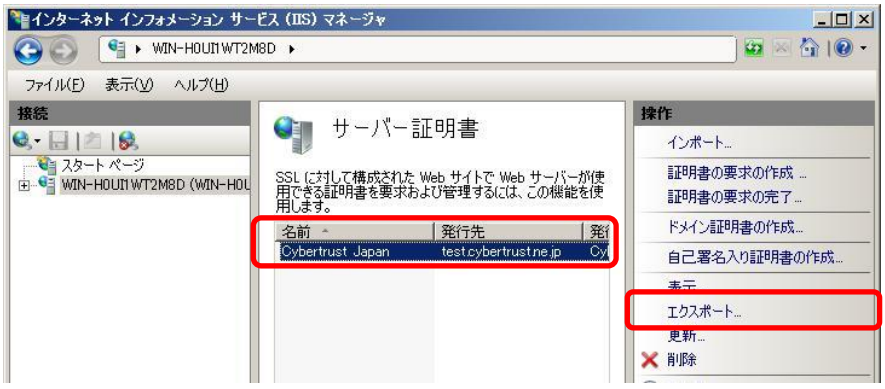
7. 鍵ペアファイルのバックアップ

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【コントロールパネル】→【管理ツール】→【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】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。

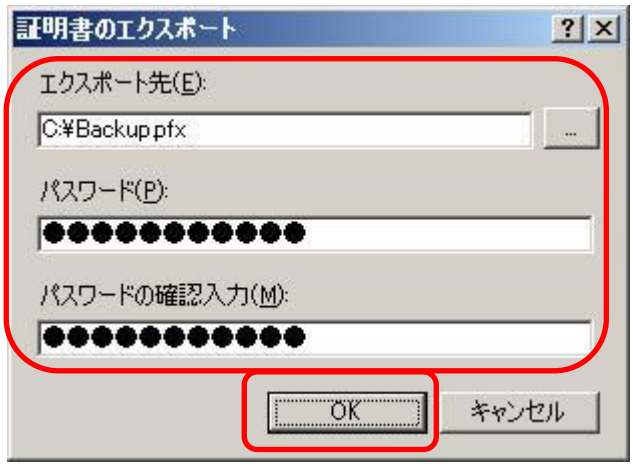


B) バックアップしたい SSL サーバー証明書を選択し、画面右側の操作メニューから【エクスポート】をクリックます。



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、「サーバー証明書の設定確認」から行うことを推奨します。

■ 設定確認例

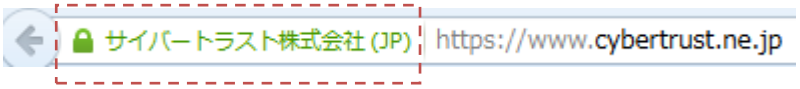
- Internet Explorer 10

＜SureServer for SAKURA(EV)＞

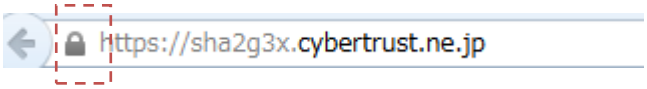
＜SureServer for SAKURA＞

- Firefox 34

＜SureServer forSAKURA(EV)＞



＜SureServer for SAKURA＞



なお、接続時にセキュリティ警告やエラーが表示される場合は、以下よくある質問の「SSL 通信時のセキュリティ警告やエラーについて」をご参照ください。

≫ SSL 通信時のセキュリティ警告やエラーについて