cybertrust

# SureServer/SureServer EV

## Microsoft IIS7.0/7.5

## 証明書インストール手順書

## （サーバ移行用）

Version 1.4

PUBLIC RELEASE

2016/12/15

# 改訂履歴

| 日付 | バージョン | 内容 |
|---|---|---|
| 2012/06/22 | 1.0 | 初版リリース |
| 2013/08/02 | 1.1 | Cybertrust Japan Public CA G3 の提供開始に伴う修正 |
| 2014/01/06 | 1.2 | SureServer(1024bit)の終了に伴う修正 |
| 2015/02/09 | 1.3 | クロスルート証明書の変更に伴う修正 |
| 2016/12/15 | 1.4 | 「はじめに」の記述内容を修正 |

# 目次

# 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 pfx ファイルと中間 CA 証明書ファイルをインストールする手順について解説するドキュメントです。

IIS7.0/7.5 単独での動作確認ができていることを前提としております。

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。

# 1. 事前準備

IIS7.0/7.5 へインストールする中間 CA 証明書ファイルと pfx ファイル（SSL サーバ証明書ファイルと秘密鍵ファイル）を準備します。

## 1.1. 中間 CA 証明書のダウンロード

サーバ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。

≫ ルート・中間 CA 証明書のダウンロード

また、ご利用商品や必要な証明書の種類がご不明の場合は、以下をご覧ください。

≫どの中間 CA 証明書をダウンロードすればよいですか？

## 1.2. pfx ファイルの保存

インストールする pfx ファイルを IIS7.0/7.5 の任意のディレクトリへ保存します。

# 2. 証明書のインストール

「Microsoft 管理コンソール（Microsoft Management Console：MMC）」から中間 CA 証明書と pfx ファイル（SSL サーバ証明書と秘密鍵ファイル）のインストールを行います。

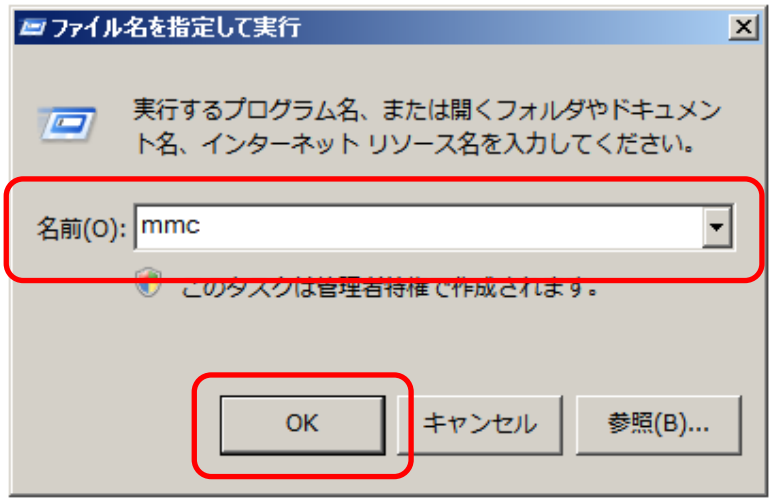
## 2.1. 中間 CA 証明書のインストール

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。

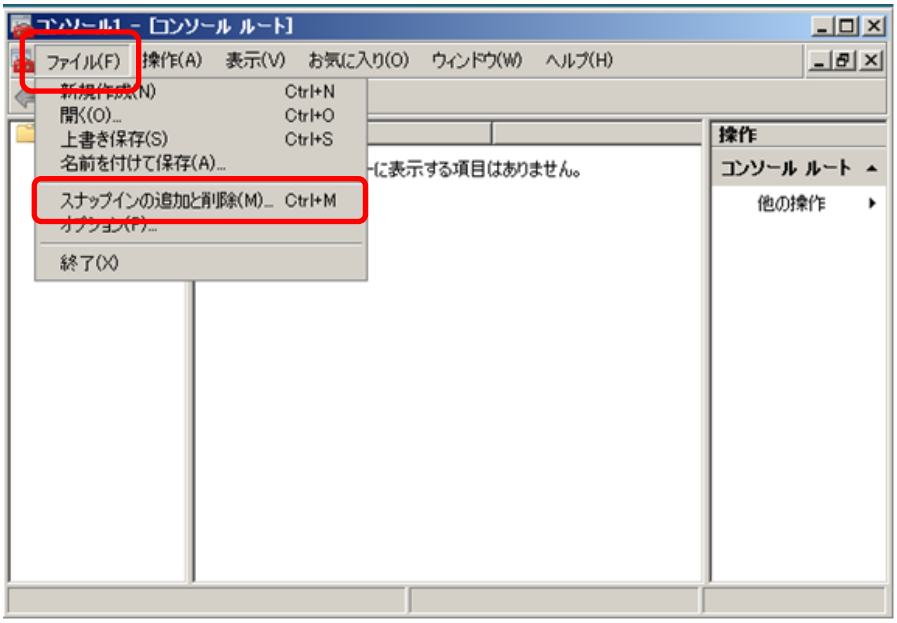
※SureServer EV[2048bit]・SureServer EV[SHA-2]、および、SureServer[2048bit]用クロスルート方式では、同様の手順で「クロスルート用中間 CA 証明書」と「中間 CA 証明書」をインストールしてください。

### 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。

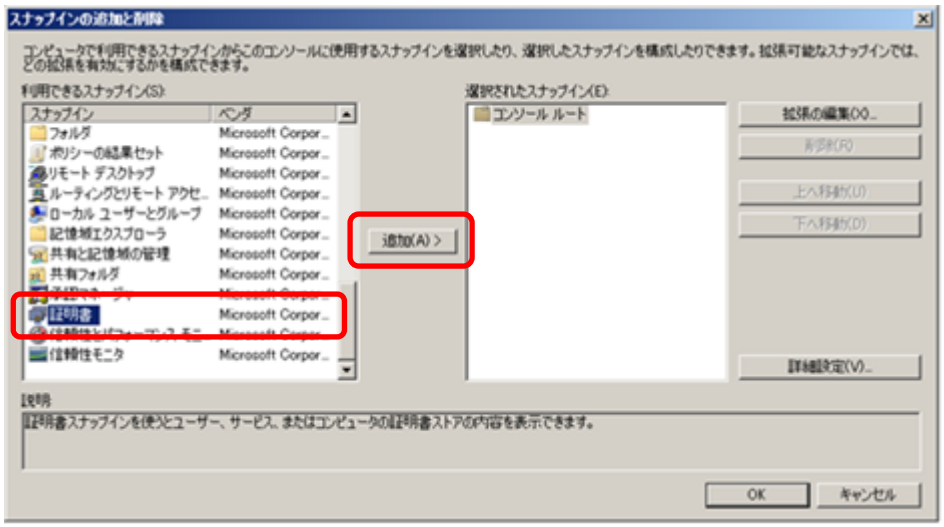
B）【名前】へ「mmc」と入力して【OK】をクリックし、MMC を開きます。



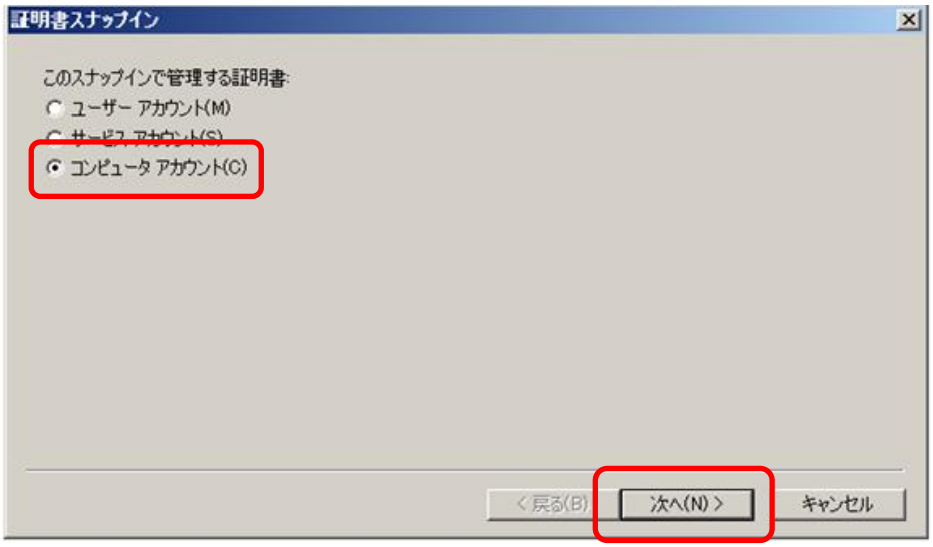

C）MMC 画面左上の【ファイル】メニューをクリックし、【スナップインの追加と削除】をクリックします。



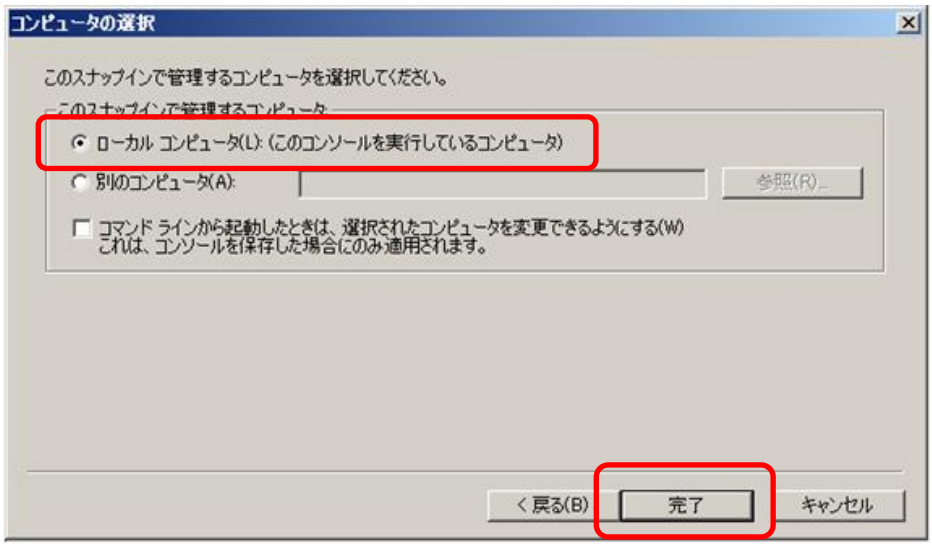
D）【利用できるスナップイン】から【証明書】を選択し、【追加】をクリックします。



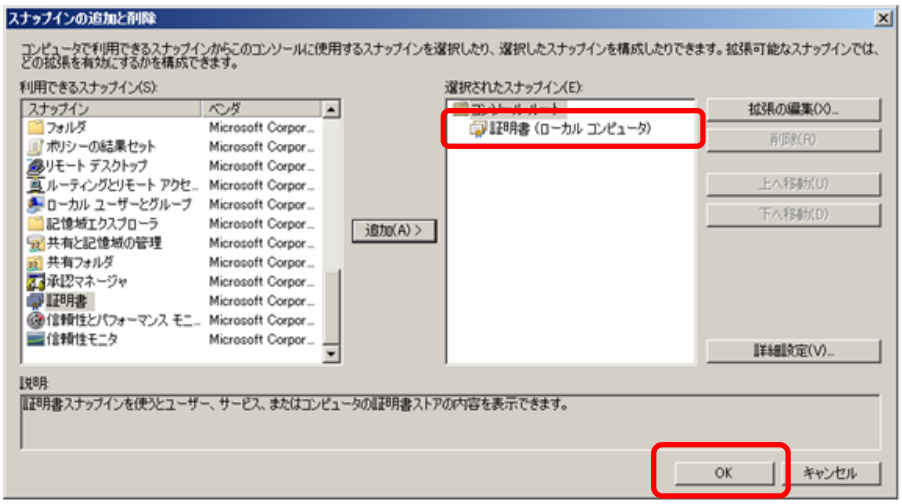

E）【コンピュータアカウント】を選択し、【次へ】をクリックします。



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。

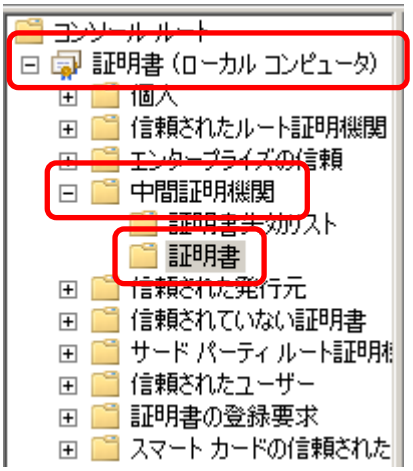



G）【選択されたスナップイン】に【証明書（ローカルコンピュータ）】が追加されていることを確認し、【OK】をクリックします。

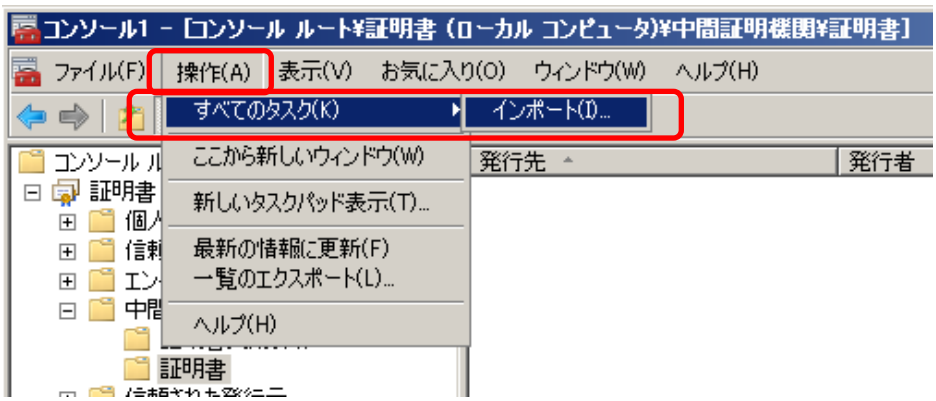


**H) コンソールルートへ【証明書（ローカルコンピュータ）】が追加されたことを確認し、【証明書（ローカルコンピュータ）】→【中間証明機関】→【証明書】をクリックします。**

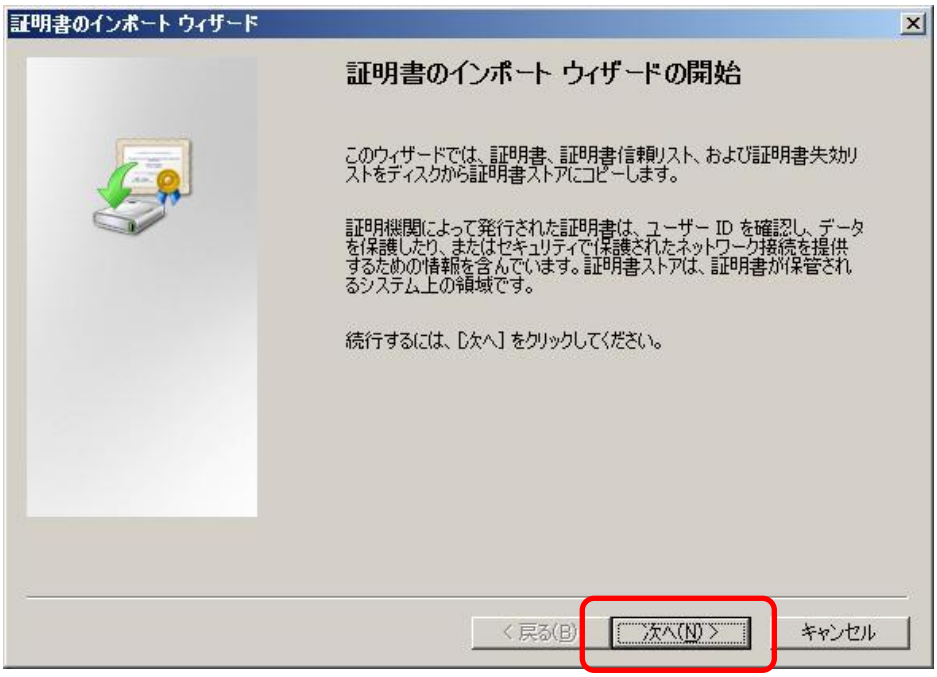
※証明書が未登録の場合は【証明書】が表示されないため、【中間証明書機関】をクリックします。



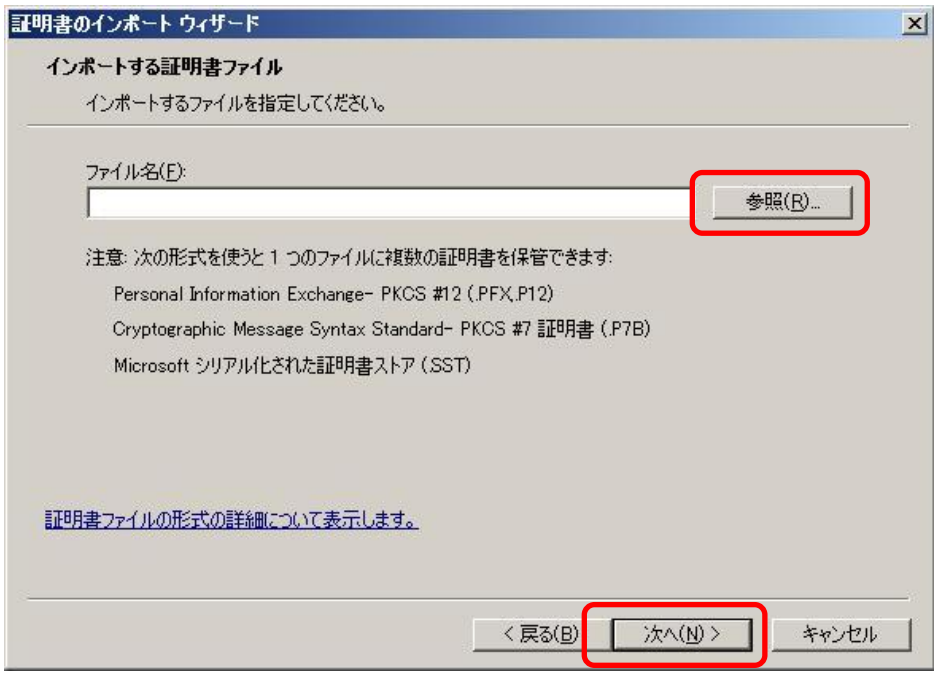

**I) MMC 画面の左上の【操作】メニュー→【すべてのタスク】→【インポート】の順にクリックします。**



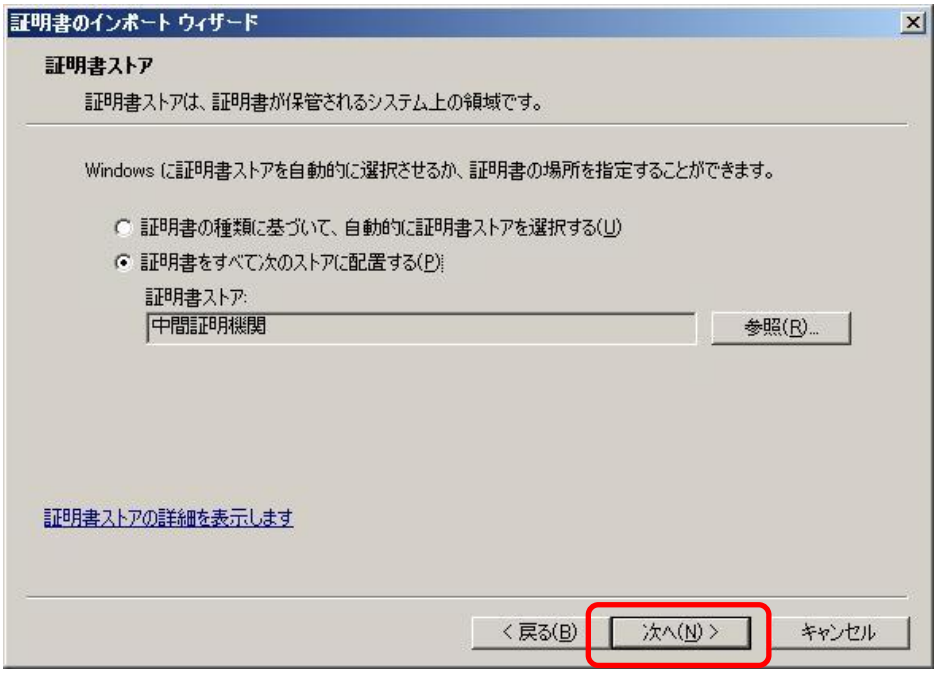
J）証明書のインポートウィザードが表示されますので、【次へ】をクリックします。



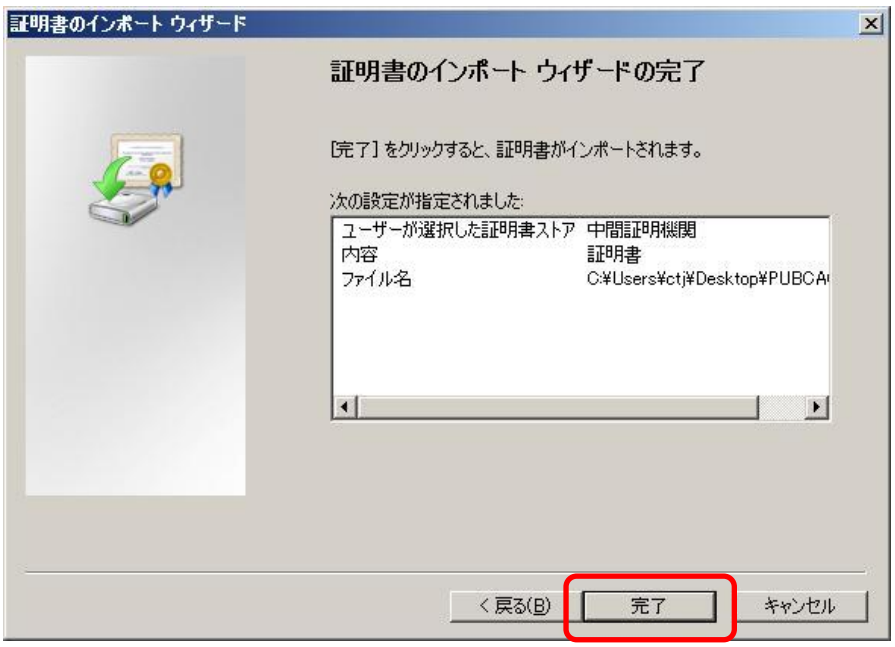

K）【参照】をクリックしてインストールする中間 CA 証明書を指定し、【次へ】をクリックします。



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。**


※中間 CA 証明書が 2 種類ある場合は、同じ手順を繰り返してください。

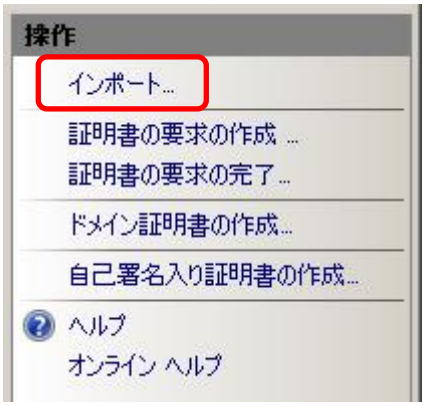
以上で中間 CA 証明書のインストールが完了します。

## 2.2. pfx ファイルのインストール

pfx ファイル(SSL サーバ証明書と秘密鍵ファイル)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。**

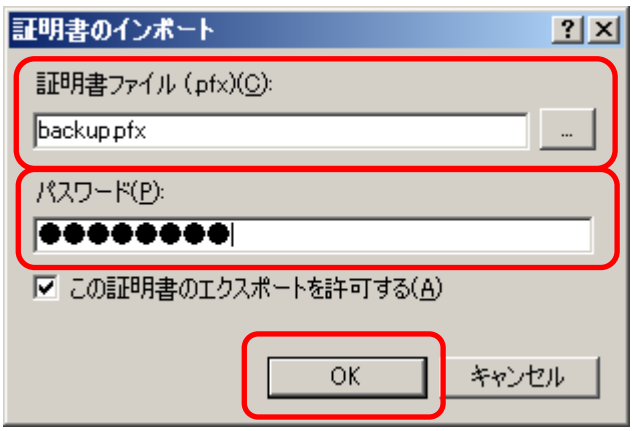

**B) 画面右側に表示される【インポート...】をクリックします。**



### C）【証明書ファイル】へインストールする pfx ファイル名を入力し、【パスワード】へパスワードを入力して、【OK】をクリックします。

※パスワードは pfx ファイルの作成・エクスポート時に設定した任意の文字列です。

※SSL サーバ証明書のエクスポートを許可する場合は、【この証明書のエクスポートを許可する】にチェックを入れてください。

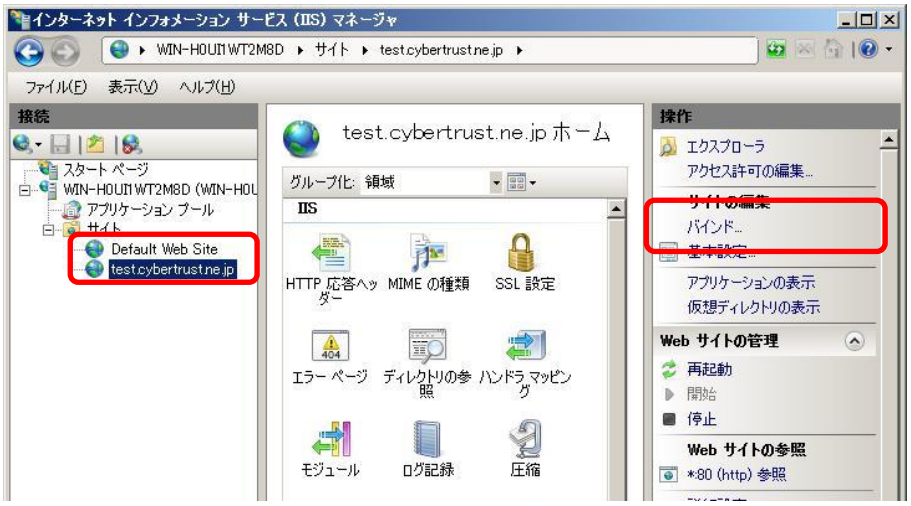



以上で pfx ファイル（SSL サーバ証明書と秘密鍵ファイル）のインストールは完了です。

# 2.3. SSL サーバ証明書の適用

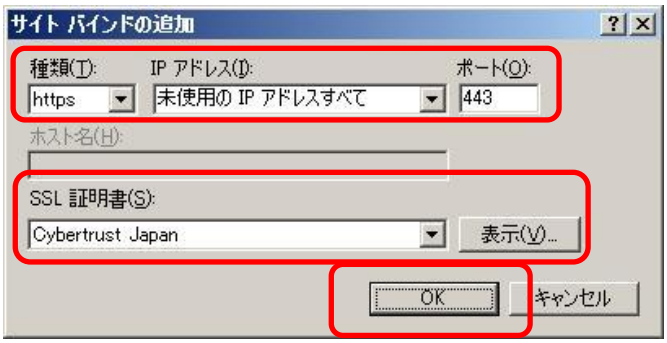
インストールした SSL サーバ証明書をご利用の Web サイトへ適用します。

**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、【追加】をクリックします。**

C）【サイトバインドの追加】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 | サーバ証明書を適用する<br>Web サイトの IP アドレス |
| ポート | 443<br>（もしくは、任意の SSL ポート番号） |
| SSL 証明書 | 適用したい SSL サーバ証明書を選択します。 |

以上で SSL サーバ証明書の設定は完了です。

# 3. pfx ファイルのバックアップ

pfxファイルは、万が一に備えて必ず別のメディア（CDやUSB等）にコピーして安全な場所に保管してください。

なお、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。

# 4. SSL 通信の確認

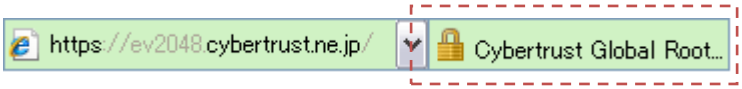
サーバ証明書が正しくインストールされ、エラーやセキュリティ警告が表示されず、正常に SSL 通信が可能であることを確認します。

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 8

＜SureServer EV[2048bit]＞




＜SureServer[2048bit]（クロスルート方式を含む）＞


- Firefox 12.0

＜SureServer EV[2048bit]＞


＜SureServer[2048bit]（クロスルート方式を含む）＞


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