



# SureServer/SureServer EV

Microsoft IIS6.0

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
2012/6/22	1.0	初版リリース
2013/8/2	1.1	Cybertrust Japan Public CA G3 の提供開始に伴う修正
2014/1/6	1.2	SureServer(1024bit)の終了に伴う修正
2015/2/9	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.....	4
1. 事前準備.....	5
1.1. 中間 CA 証明書のダウンロード.....	5
1.2. pfx ファイルの保存.....	5
2. 証明書のインストール.....	6
2.1. MMC の起動.....	6
2.2. スナップインの追加.....	7
2.3. 中間 CA 証明書のインストール.....	11
2.4. pfx ファイルのインストール.....	14
2.5. SSL サーバ証明書の適用.....	19
3. pfx ファイルのバックアップ.....	23
4. SSL 通信の確認.....	23

# 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 6.0(以下、IIS6.0)」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。

IIS6.0 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ます、IIS6.0 の動作を保証するものではありません。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ます、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

IIS6.0 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

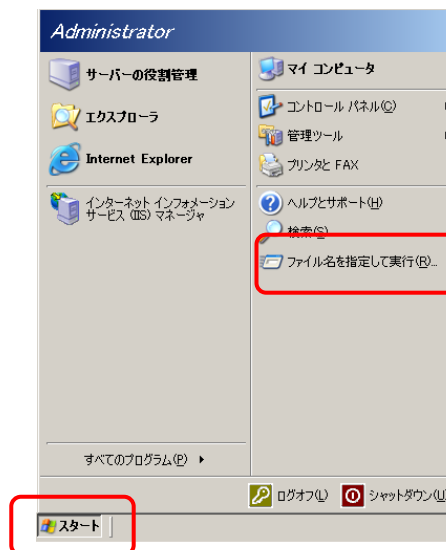
インストールする pfx ファイルを IIS6.0 の任意のディレクトリへ保存します。

## 2. 証明書のインストール

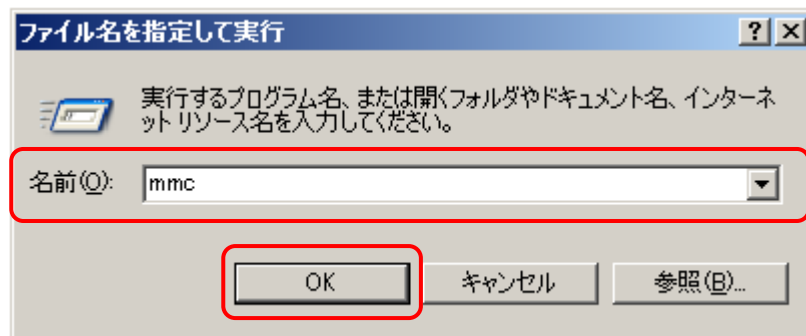
「Microsoft 管理コンソール (Microsoft Management Console: MMC)」から中間 CA 証明書と pfx ファイル (SSL サーバ証明書と秘密鍵ファイル) のインストールを行います。

### 2.1. MMC の起動

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。

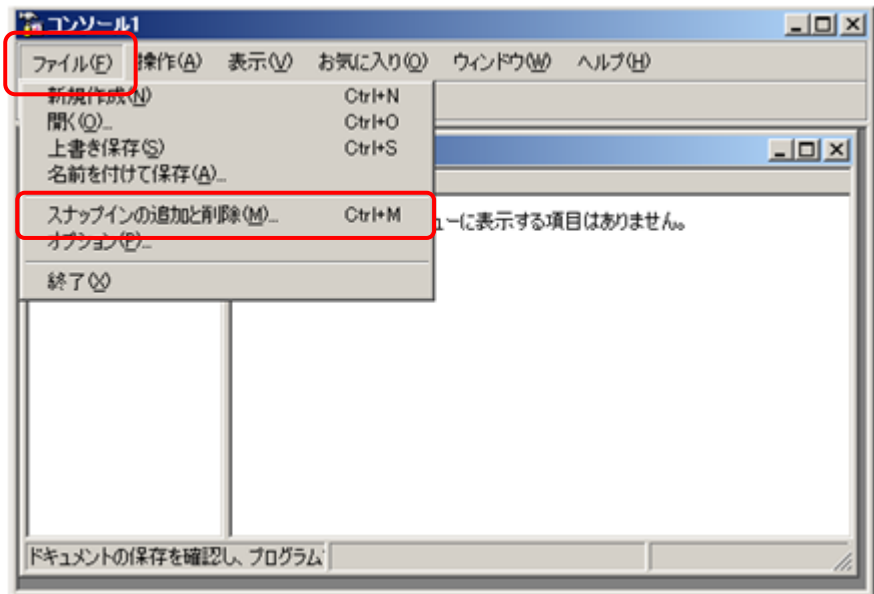


B) 【名前】へ「mmc」と入力して【OK】をクリックし、「Microsoft 管理コンソール」を開きます。

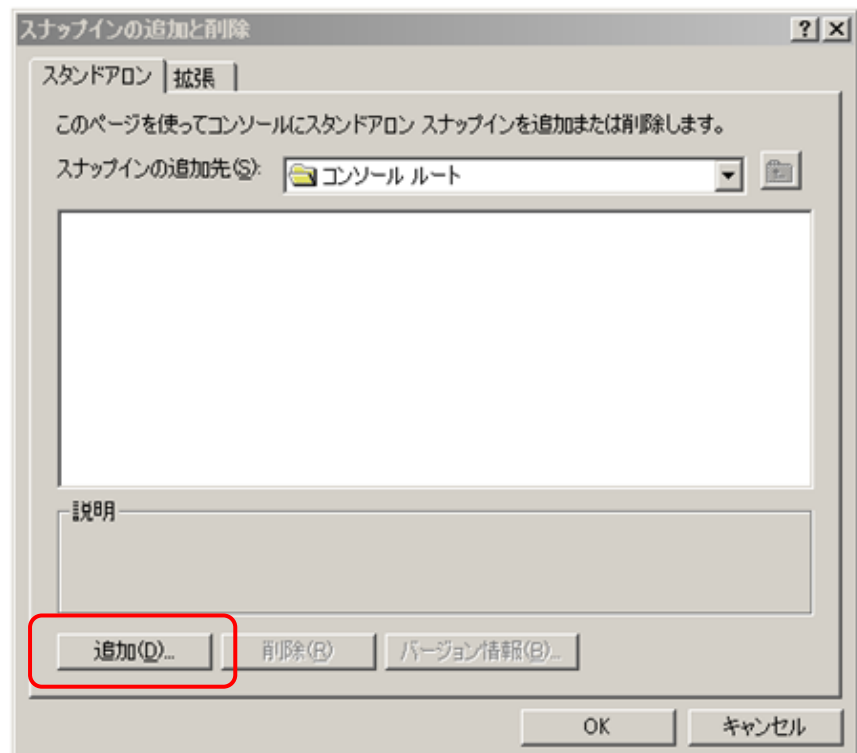


## 2.2. スナップインの追加

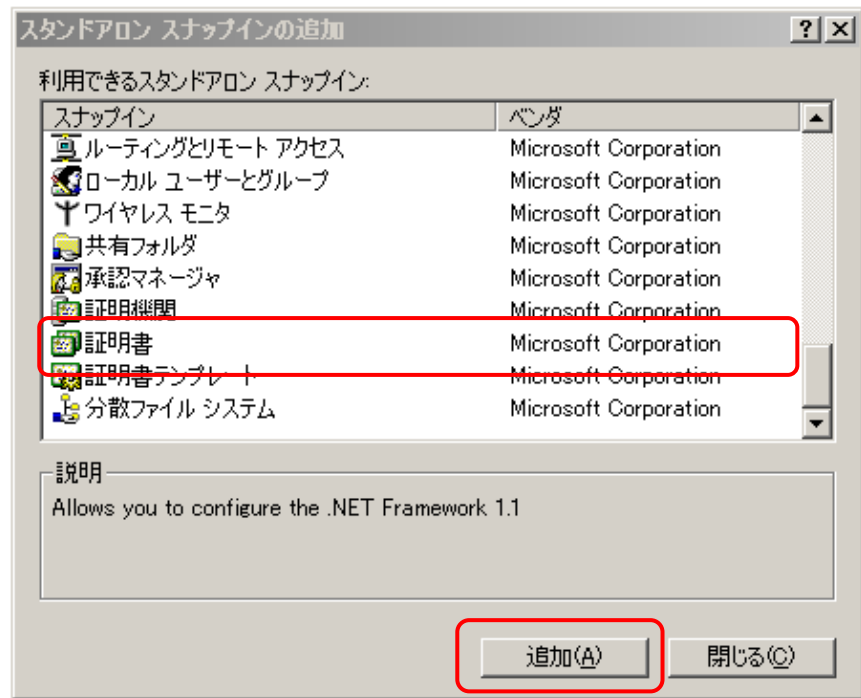
- A) 画面左上の【ファイル】メニューをクリックし、【スナップインの追加と削除】をクリックします。



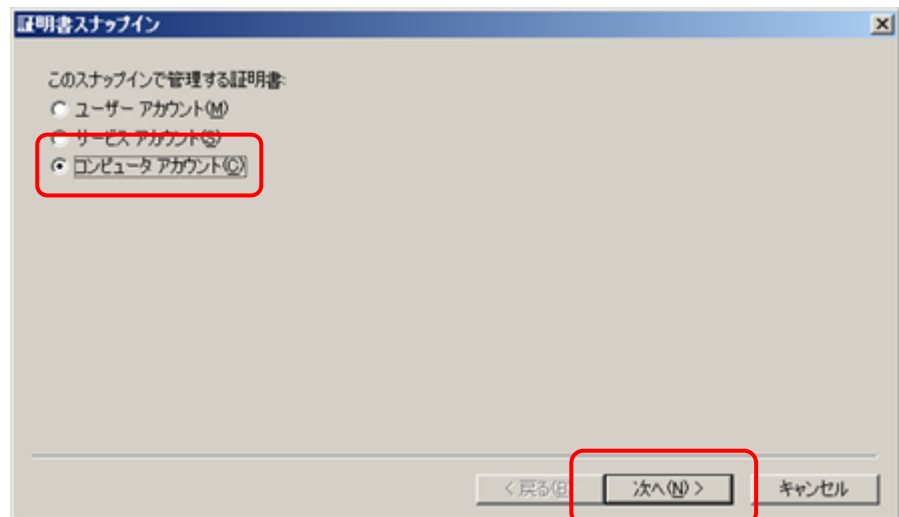
- B) 【スナップインの追加と削除】内の【追加】をクリックします。



- C) 【利用できるスタンドアロン スナップイン】の中から【証明書】を選択し、【追加】をクリックします。

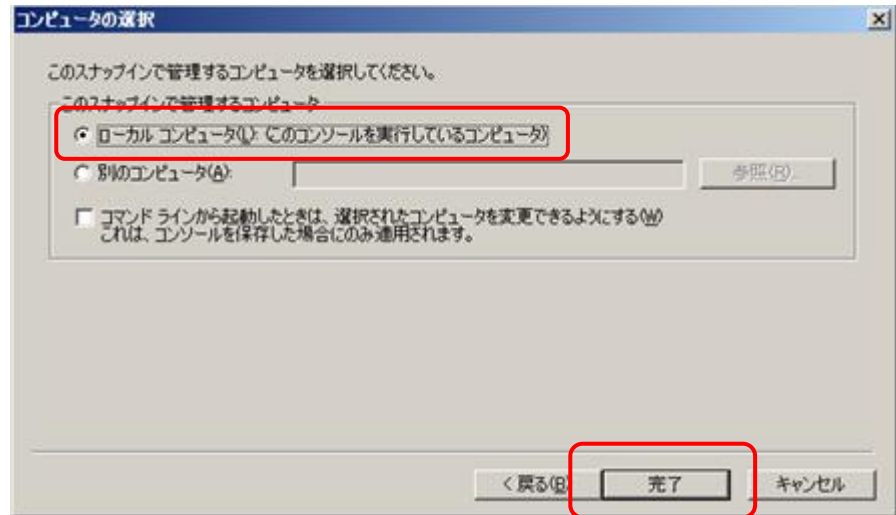


- D) 【コンピュータアカウント】を選択し、【次へ】をクリックします。





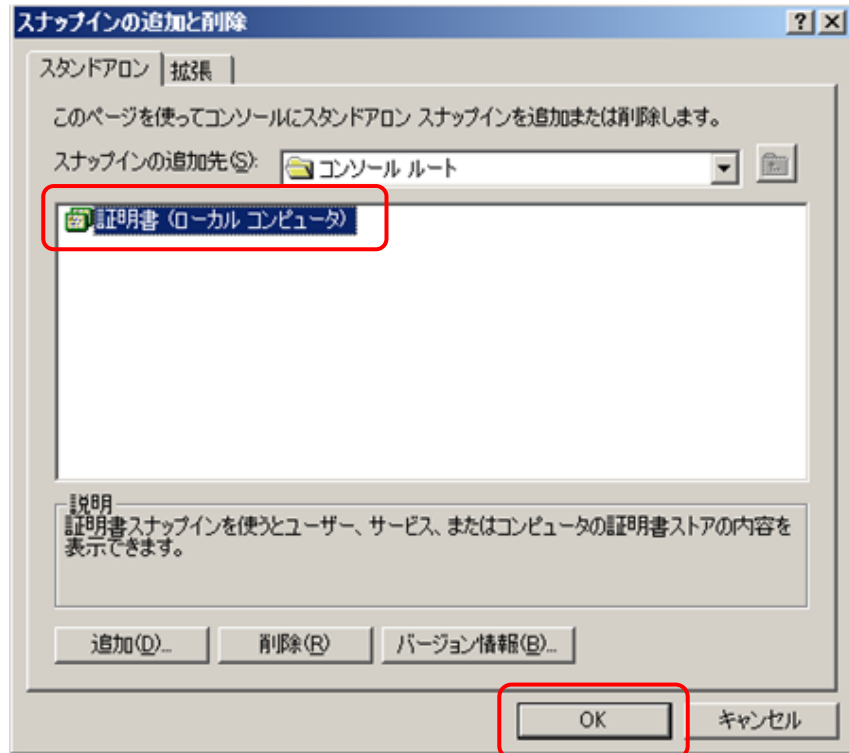
- E) 【ローカルコンピュータ(このコンソールを実行しているコンピュータ)】を選択し、【完了】をクリックします。



- F) 【利用できるスタンドアロン スナップイン】の【閉じる】をクリックします。



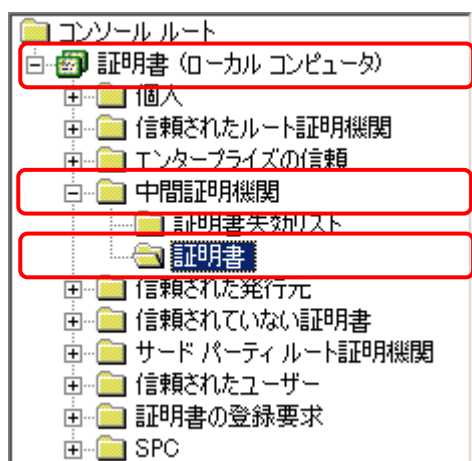
- G) 【証明書(ローカルコンピュータ)】が追加されていることを確認し、【OK】をクリックします。



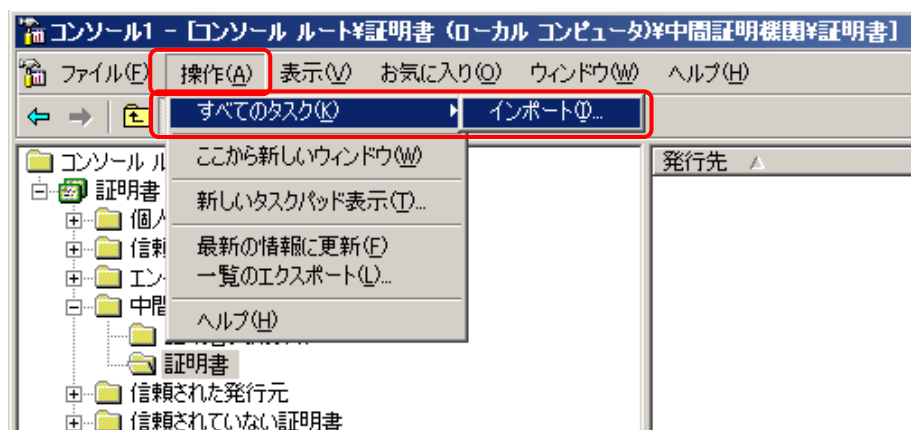
## 2.3. 中間 CA 証明書のインストール

A) 【証明書(ローカルコンピュータ)】→【中間証明機関】→【証明書】の順にクリックします。

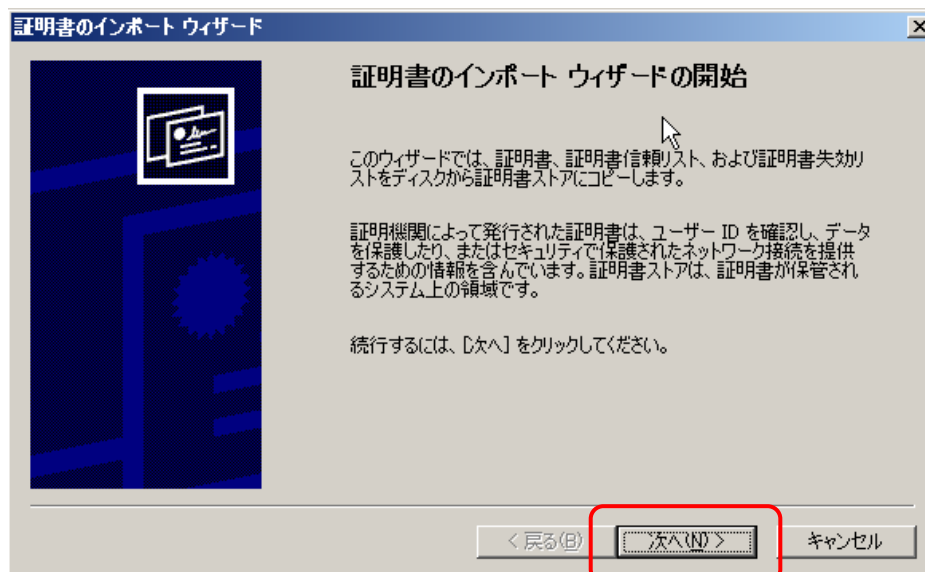
※証明書が未登録の場合は【証明書】が表示されないため、【中間証明書機関】をクリックします。



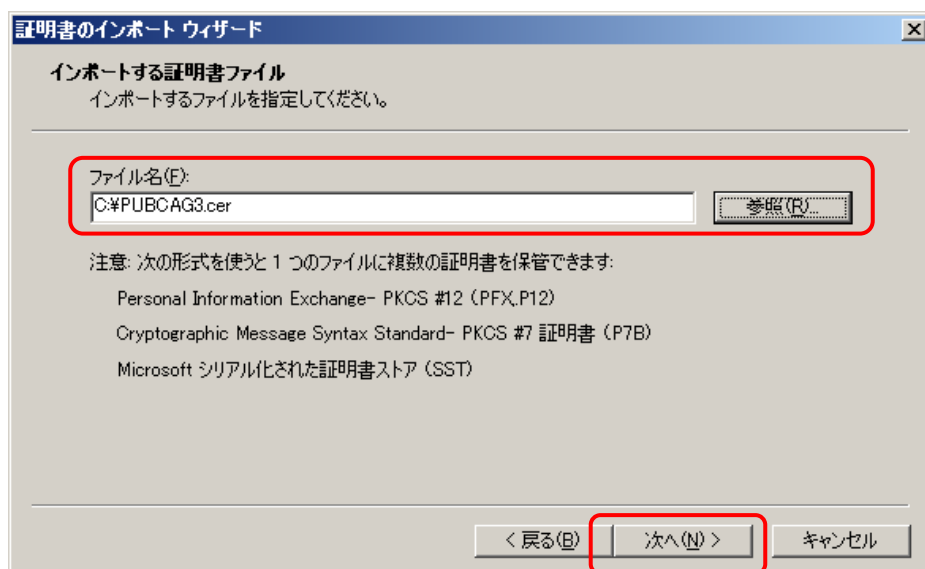
B) 画面の左上の【操作】メニュー→【すべてのタスク】→【インポート】の順にクリックします。



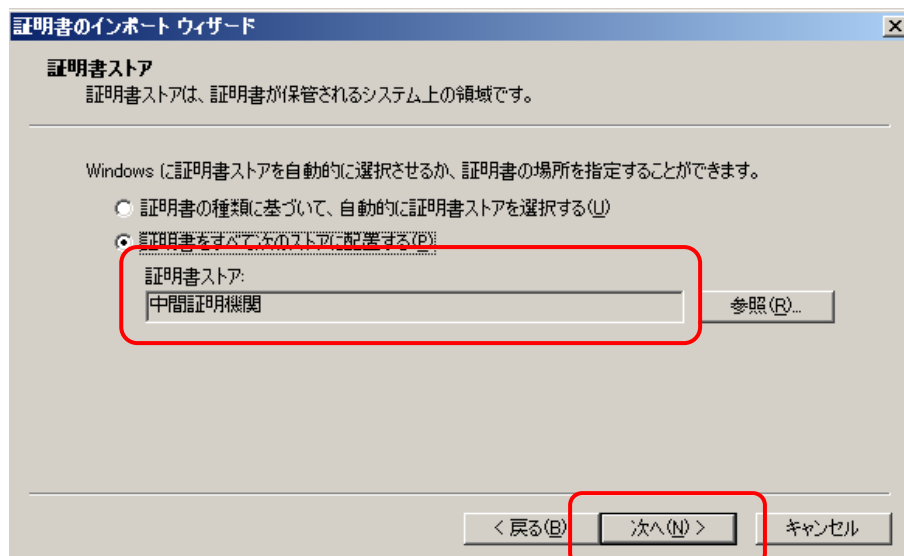
- C) 証明書のインポート ウィザードが表示されますので、【次へ】をクリックします。



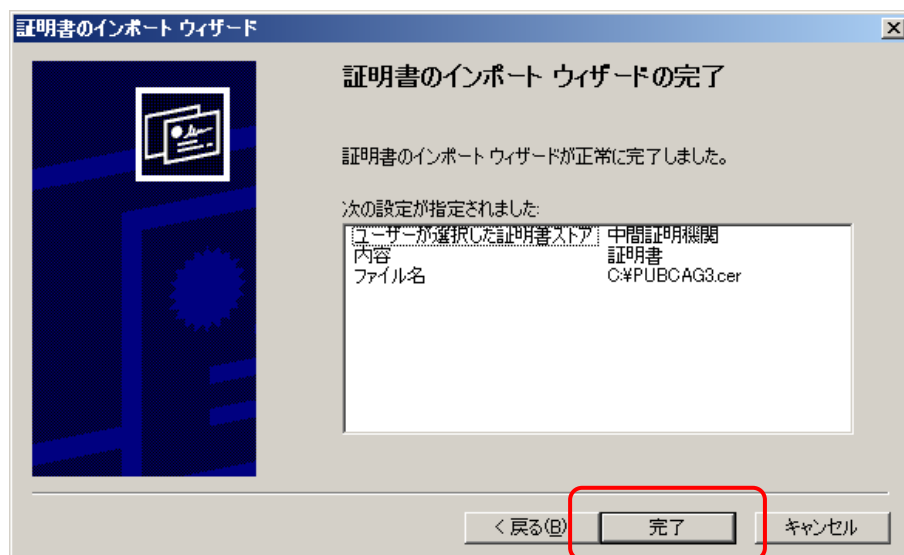
- D) 【ファイル名】へインストールする中間 CA 証明書ファイル名を指定し、【次へ】をクリックします。



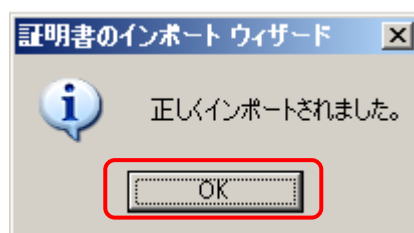
- E) 証明書ストアに【中間証明機関】が表示されていることを確認し、【次へ】をクリックします。



- F) 証明書のインポート ウィザードの完了画面の表示内容を確認し、【完了】をクリックします。



- G) 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】を押して終了となります。



※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。

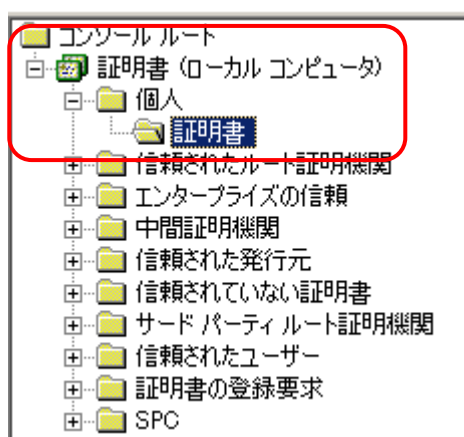
以上で中間 CA 証明書のインストールは完了です。

## 2.4. pfx ファイルのインストール

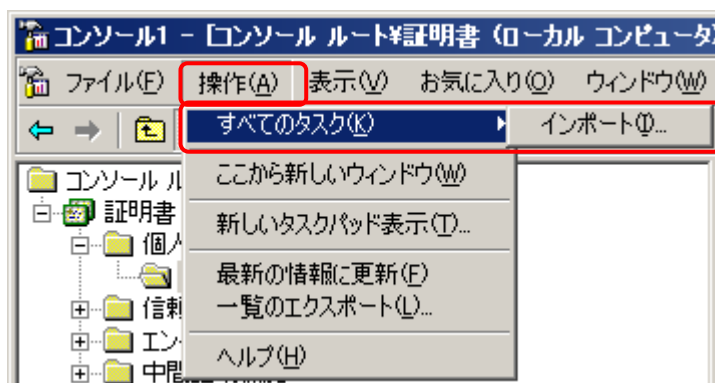
pfx ファイル(SSL サーバ証明書と秘密鍵ファイル)のインストールを行います。

- A) 【証明書(ローカルコンピュータ)】→【個人】→【証明書】の順にクリックします。

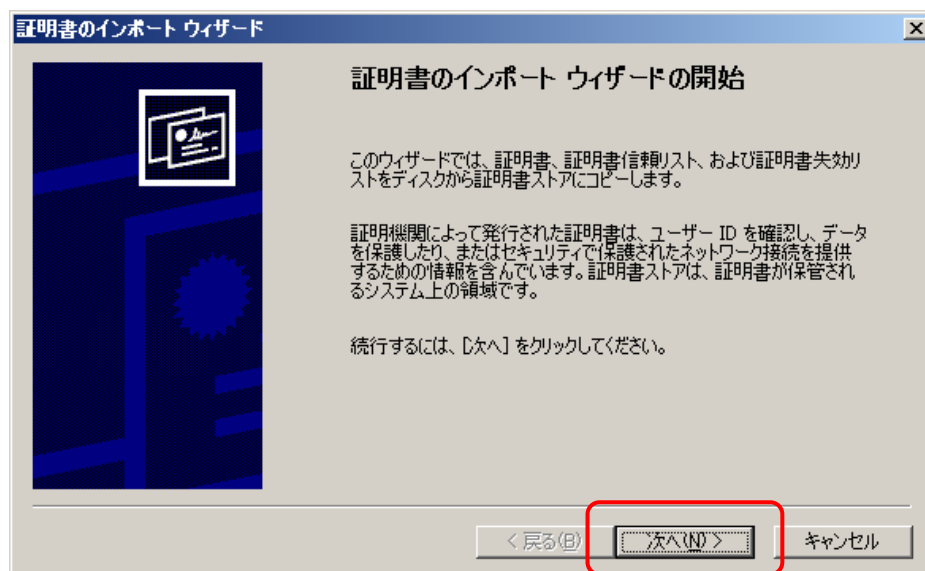
※証明書が未登録の場合は【証明書】が表示されないため、【個人】をクリックします。



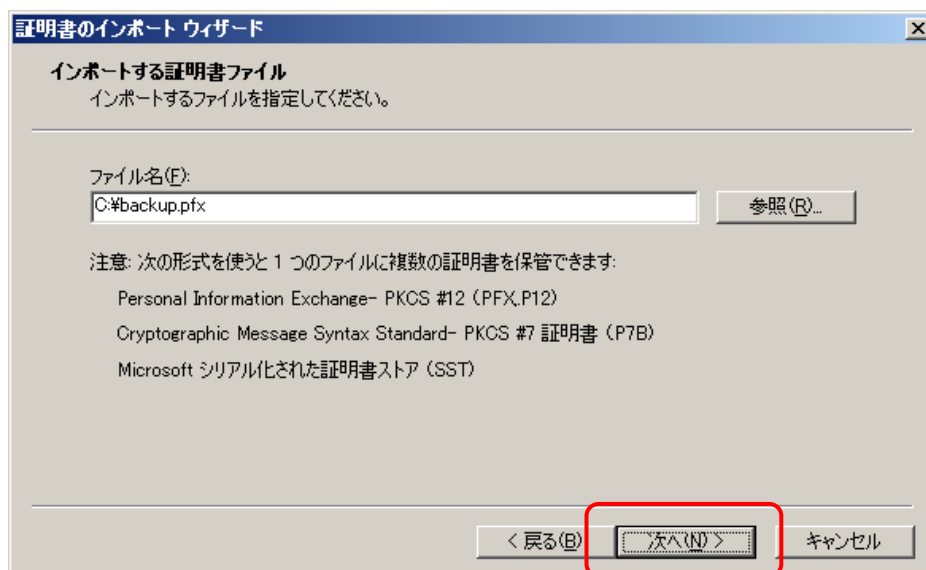
- B) 画面の左上の【操作】メニュー→【すべてのタスク】→【インストール】の順にクリックします。



- C) 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。

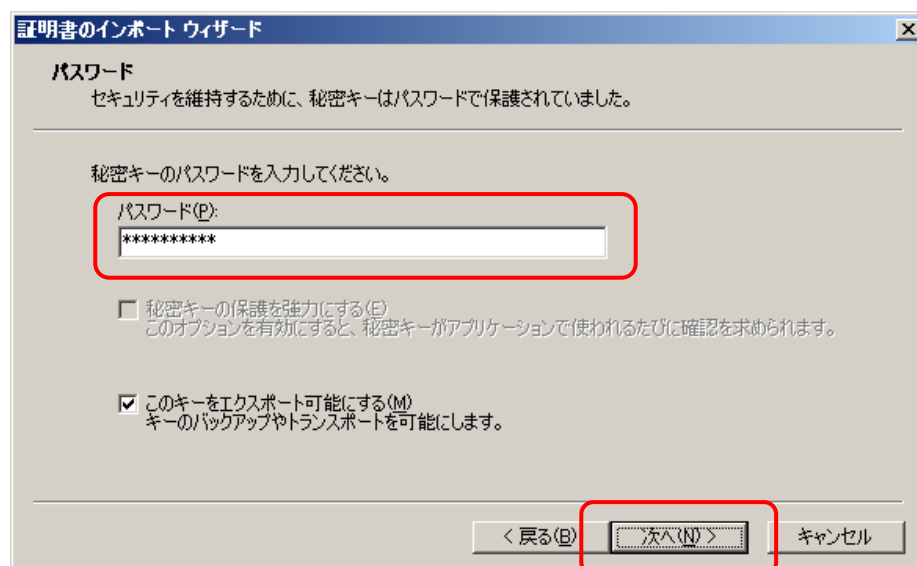


- D) 【ファイル名】へインストールする pfx ファイル名を指定し、【次へ】をクリックします。



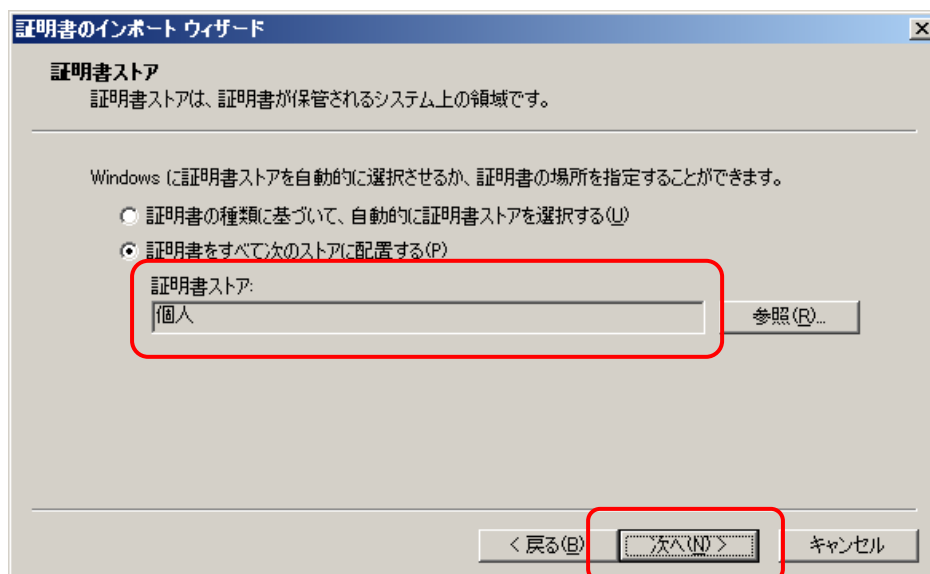
- E) 【パスワード】へ pfx ファイルに設定されているパスワードを入力し、【次へ】をクリックします。

※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、【このキーをエクスポート可能にする】にチェックを入れてください。

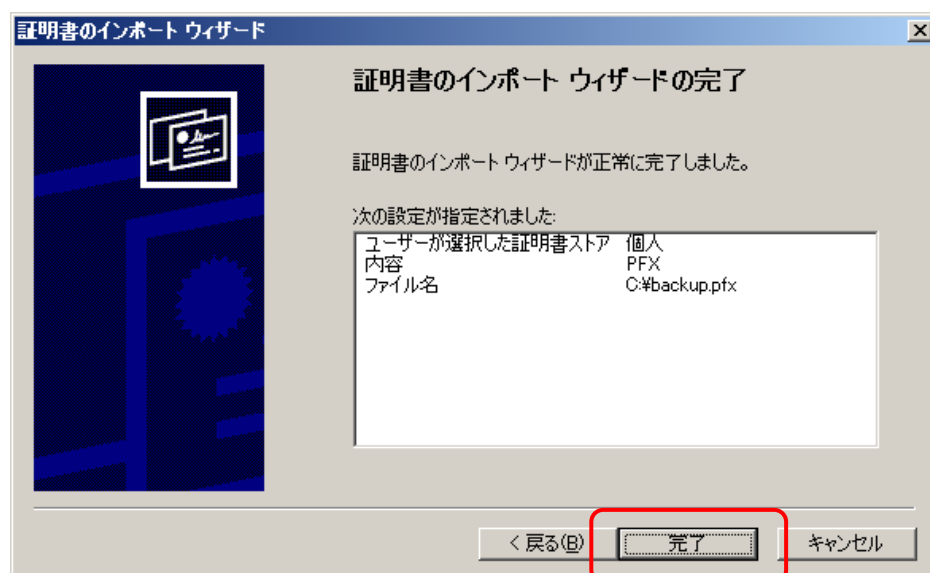




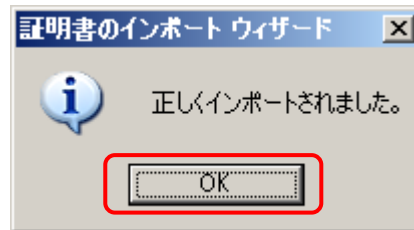
- F) 証明書ストアに【個人】が表示されていることを確認し、【次へ】をクリックします。



- G) 証明書のインポート ウィザードの完了画面の表示内容を確認し、【完了】をクリックします。



H) 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】を押して終了となります。

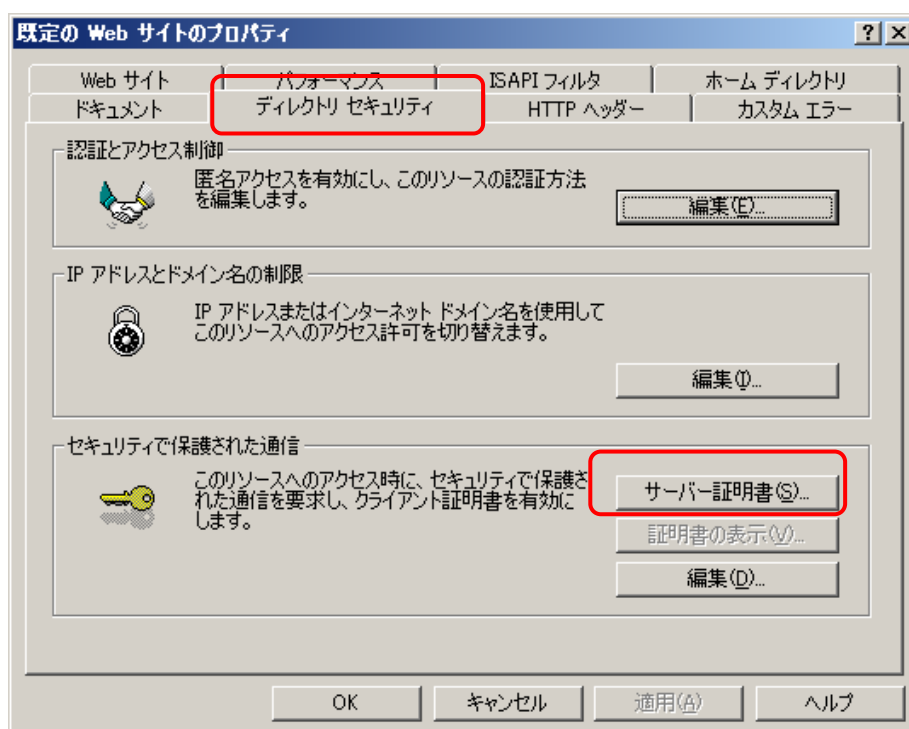


以上で pfx ファイル (SSL サーバ証明書と秘密鍵ファイル) のインストールは完了です。

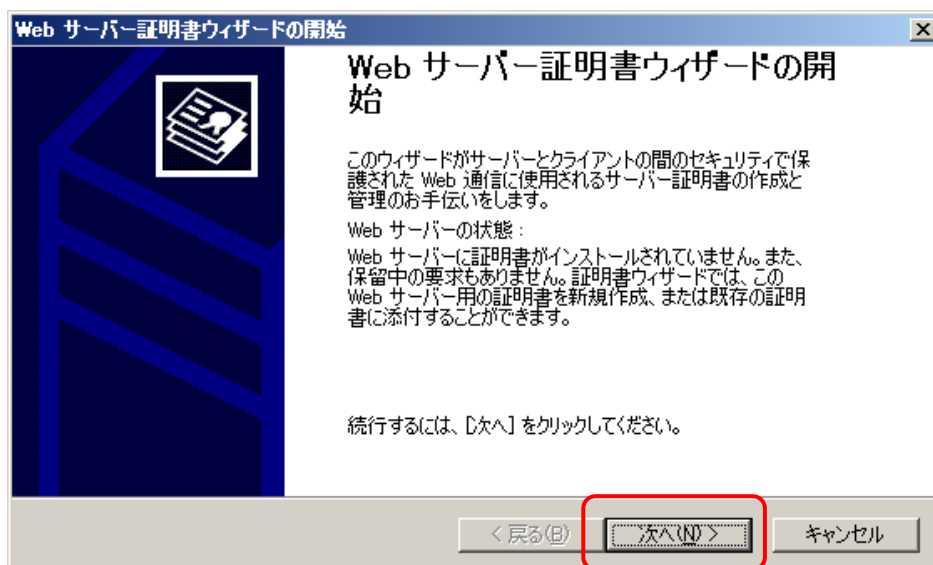
## 2.5. SSL サーバ証明書の適用

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。

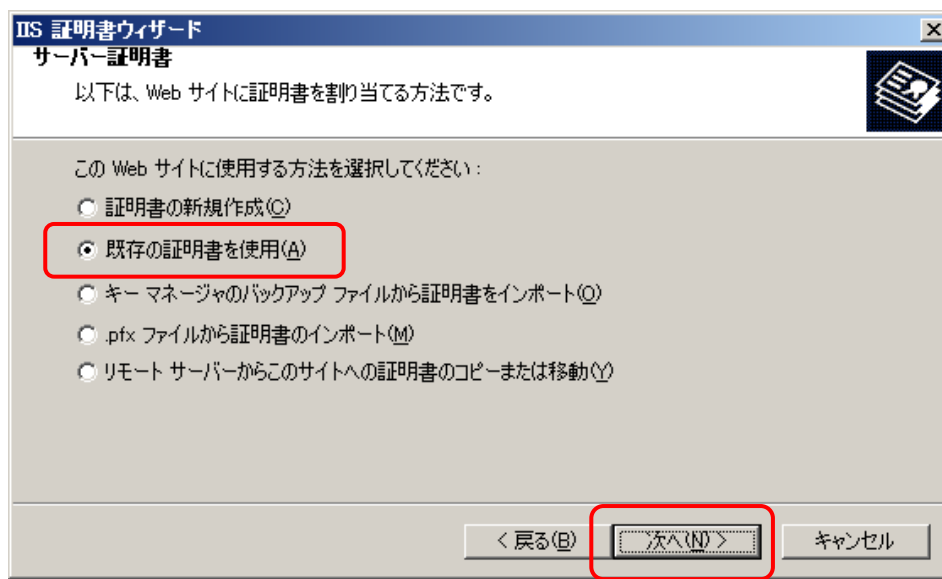
- A) 【スタート】メニューから【管理ツール】→【インターネット インフォメーション サービス(IIS) マネージャ】を選択し、IIS マネージャを起動します。
- B) SSL サーバ証明書を適用する Web サイトを選択し、プロパティを表示します。
- C) 【ディレクトリ セキュリティ】タブ→【サーバー証明書】をクリックして、Web サーバー証明書ウィザードを起動します。



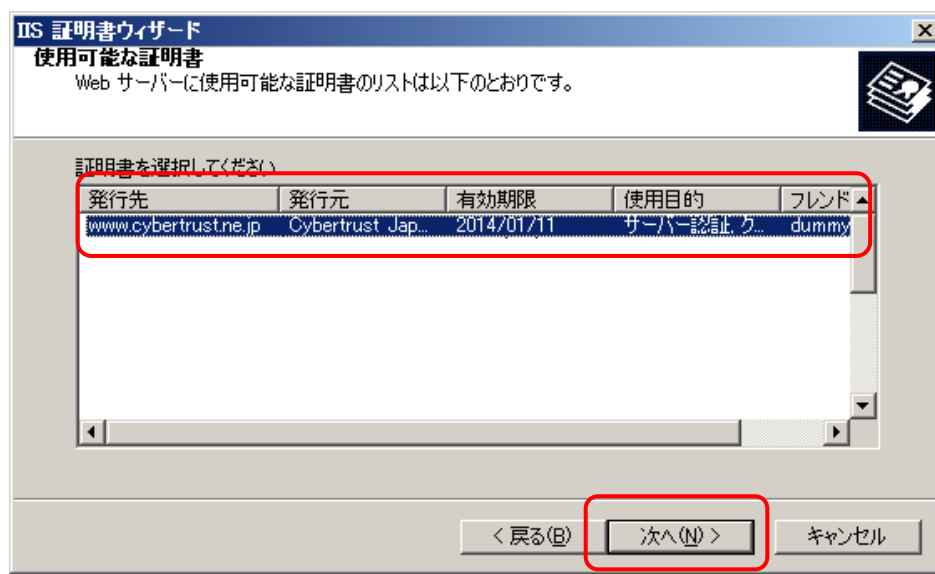
- D) Web サーバー証明書ウィザードが表示されますので、【次へ】をクリックします。



- E) 【既存の証明書を使用】を選択して【次へ】をクリックします。



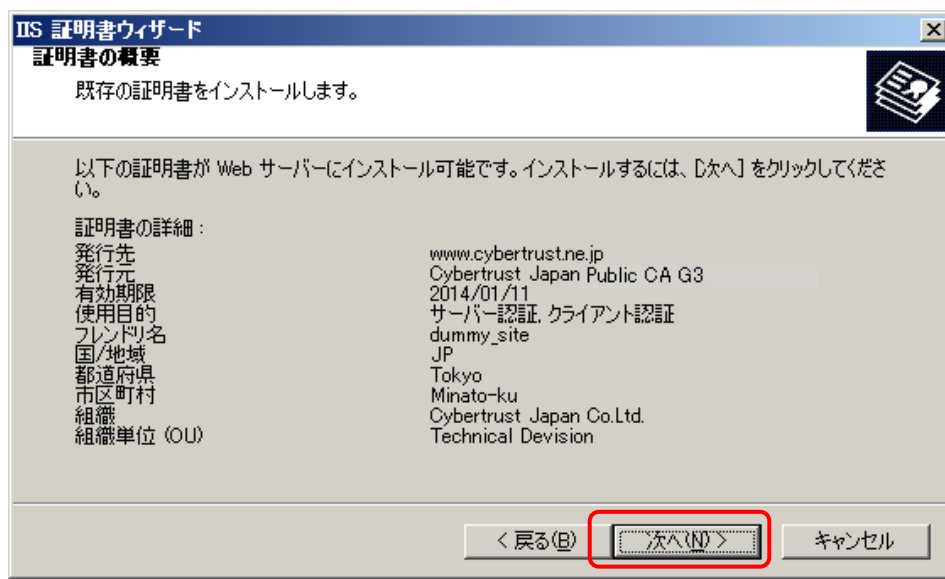
F) インストールした SSL サーバ証明書を指定し、【次へ】をクリックします。



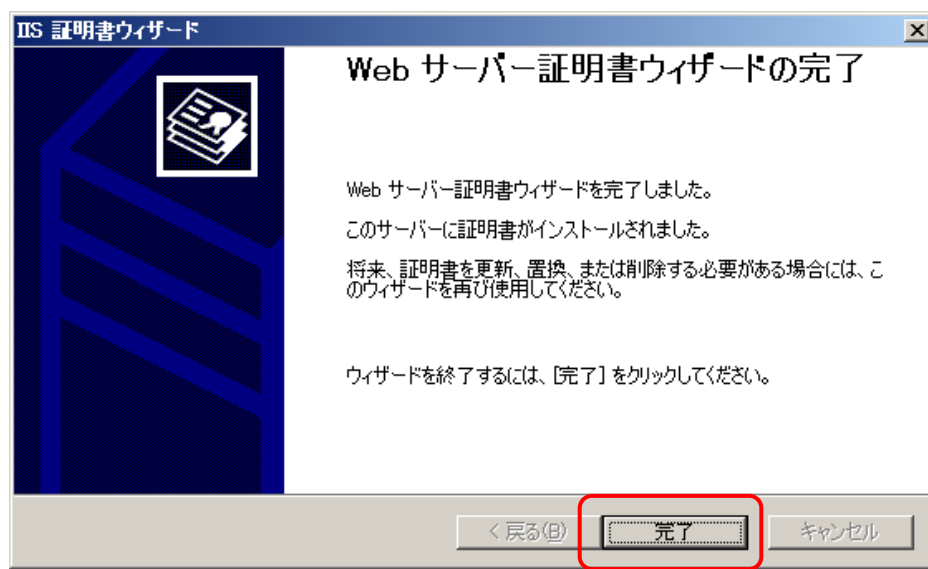
G) SSL 接続を行う TCP ポート(SSL 接続では通常 443 ポート)を入力し、【次へ】をクリックします。



- H) 適用する SSL サーバ証明書の内容が表示されますので、確認後、【次へ】をクリックします。



- I) Web サーバ証明書ウィザードの完了の画面が表示されますので、【完了】をクリックします。



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

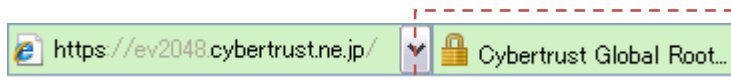
サーバ証明書が正しくインストールされ、エラーやセキュリティ警告が表示されず、正常に SSL 通信が可能であることを確認します。

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。

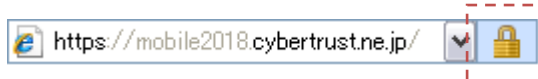
#### ■ 設定確認例

- 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](#)