cybertrust

SureServer/SureServer EV

Microsoft IIS5.0

CSR 作成/証明書インストール手順書

（新規用）

Version 1.7

PUBLIC RELEASE

2017/04/28

改訂履歴

日付	バージョン	内容
2012/6/22	1.0	初版リリース
2012/8/27	1.1	「OU」に関する記述内容を修正
2013/6/26	1.2	SureServer(1024bit)の受付終了に伴う修正
2013/8/2	1.3	Cybertrust Japan Public CA G3 の提供開始に伴う修正
2014/1/6	1.4	SureServer(1024bit)の終了に伴う修正
2015/2/9	1.5	クロスルート証明書の変更に伴う修正
2016/12/15	1.6	「はじめに」の記述内容を修正
2017/04/28	1.7	「OU」に関する記述内容を修正

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 5.0（以下、IIS5.0）」の環境下でサイバートラストのサーバ証明書をご利用いただく際の CSR 作成とサーバ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、IIS5.0 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。

サーバ証明書お申込みフロー

サーバ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	お申込み前の確認	お申込み前の確認
	CSR の作成　P6～	
STEP2	WEB からのお申し込み(SureBoard / SureHandsOn)	
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　P17～	
STEP5	証明書のインストール　P18～	
STEP6	SSL 通信の確認　P30～	

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。

※クラウド商品（for クラウド）、マルチドメイン商品（SureServer MD など）を含みます。

1.2. CSR 作成時に指定する項目（DN）について

詳細は以下をご確認ください。

≫CSR 作成時に指定する項目について

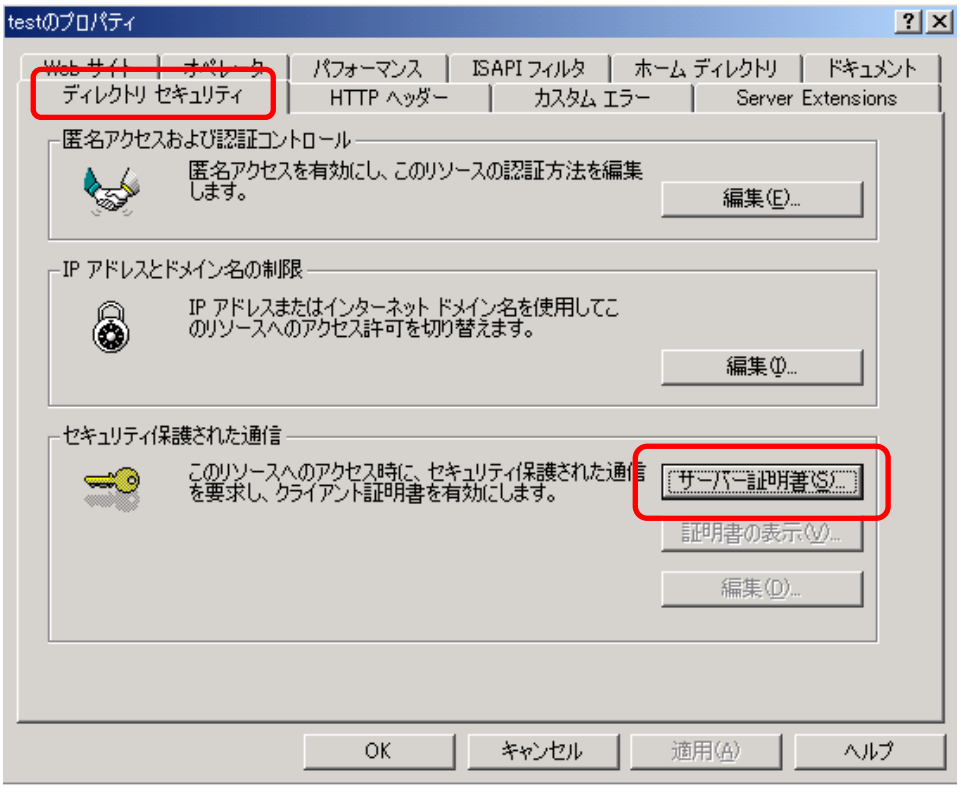
2. キーペア・CSR の作成

Microsoft Windows Server 2000 の【インターネットサービスマネージャ】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。

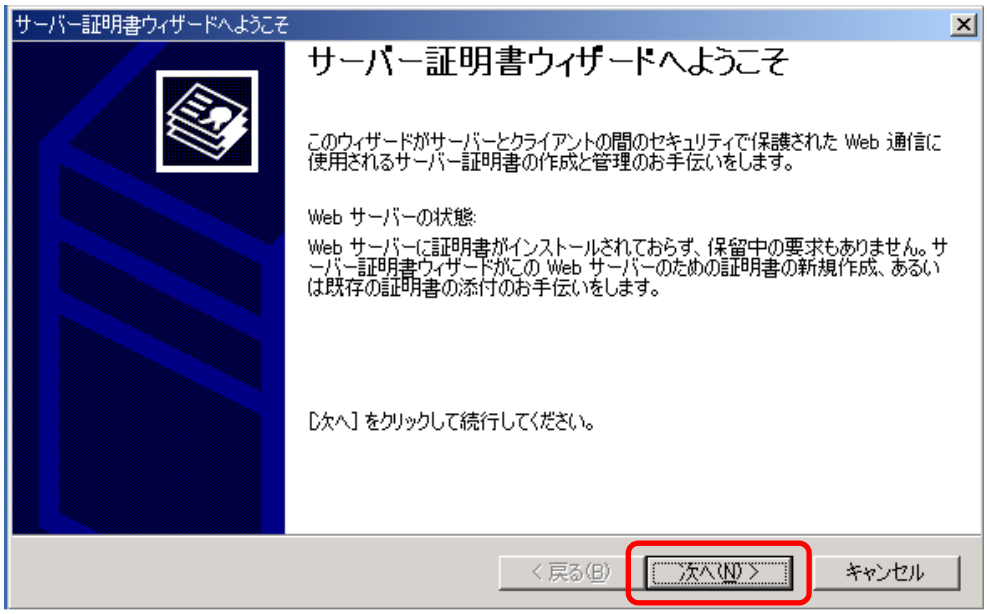
2.1. 作成方法

A) 【スタート】メニューから【管理ツール】→【インターネット サービスマネージャ】を選択し、IIS マネージャを起動します。

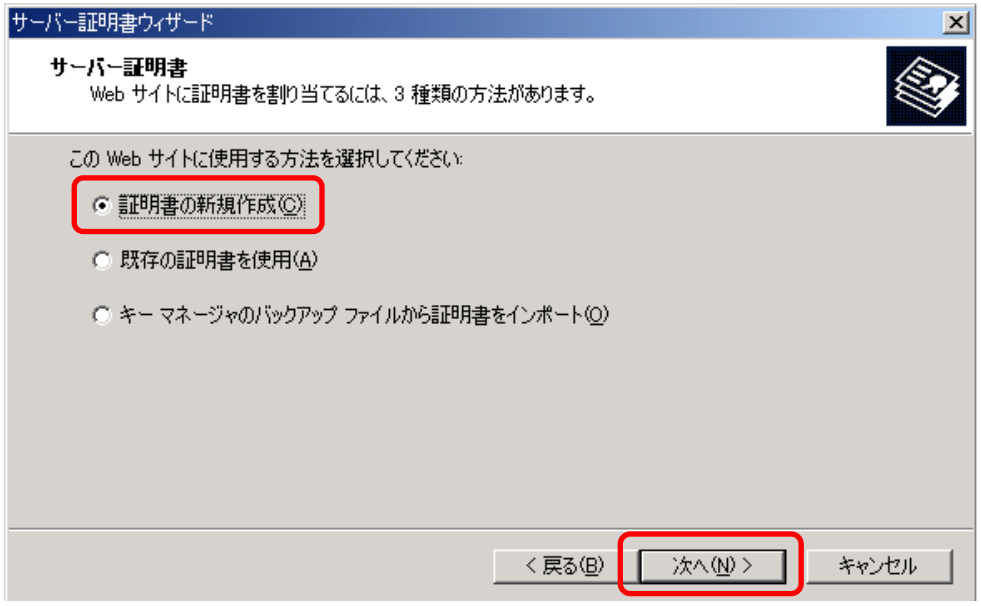
B) 証明書を発行したい Web サイトのプロパティを表示し、【ディレクトリ セキュリティ】タブ→【サーバー証明書】をクリックして、サーバー証明書ウィザードを起動します。



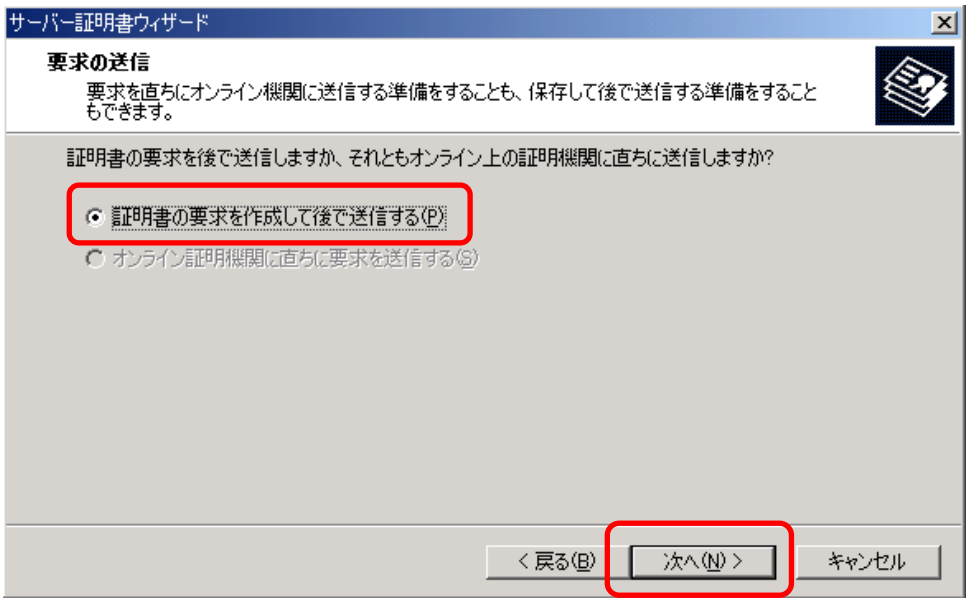
C) サーバー証明書ウィザードが表示されますので、【次へ】をクリックします。



D) 【証明書の新規作成】を選択し、【次へ】をクリックします。

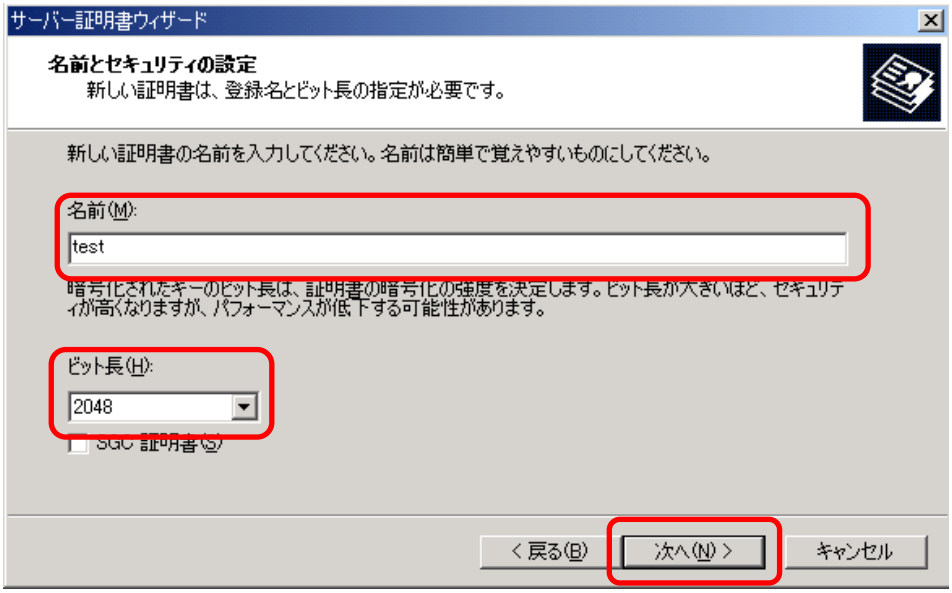


E）【証明書の要求を作成して後で送信する】を選択し、【次へ】をクリックします。



F）「名前」の欄に任意のキー名を入力、「ビット長」を「2048」と指定し、【次へ】をクリックします。

※SGC 証明書にチェックを入れないでください。

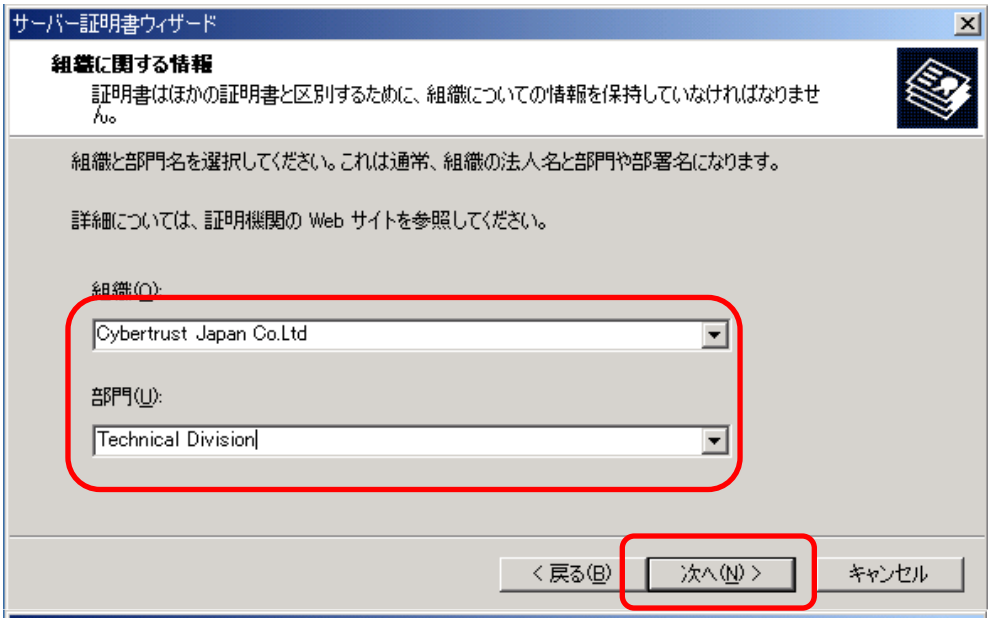


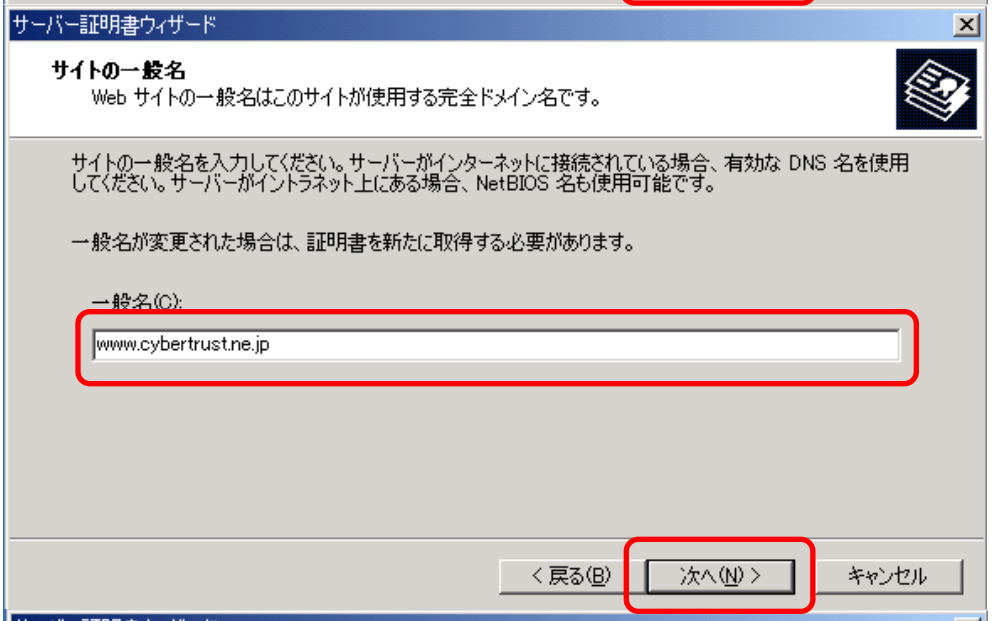
G) 組織に関する情報を入力する画面が表示されますので、CSR に設定する情報を入力します。以下のルールに従って正確に入力してください。

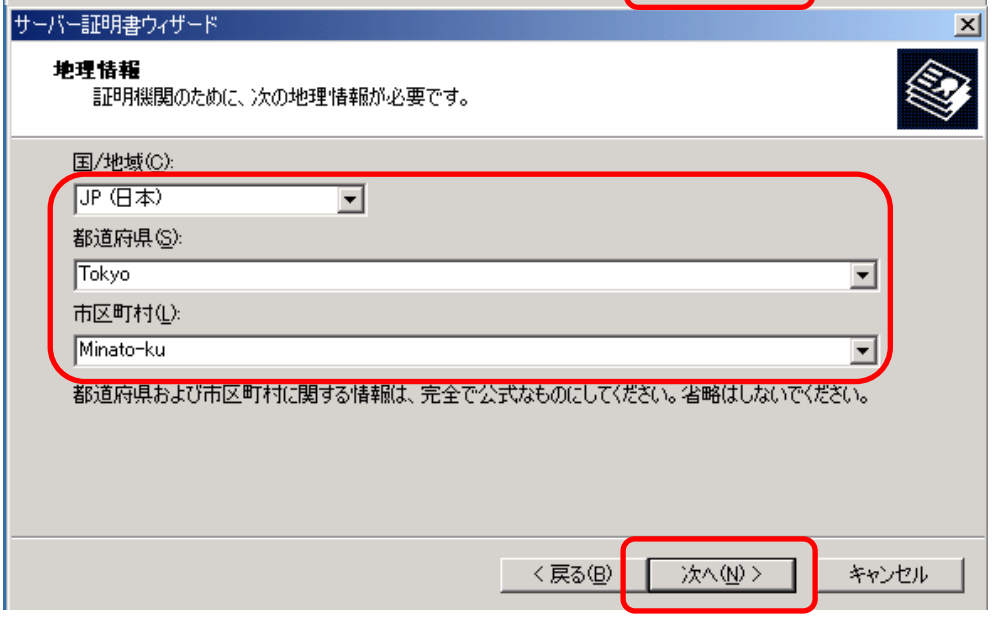
※半角英数字で入力してください。
※使用文字:スペース「a-z」「A-Z」「0-9」「'」「,」「.」「( )」「:」「-」「?」「&」

入力項目	内容	入力例
組織	申請組織の名称((英語)	Cybertrust Japan Co.,Ltd.
部門	「部署名」(※)	Technical Division
一般名	完全なドメイン名(FQDN)	www.cybertrust.ne.jp
国/地域	申請組織の国名	JP
都道府県	申請組織の事業所住所の「都道府県名」(英語)	Tokyo
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

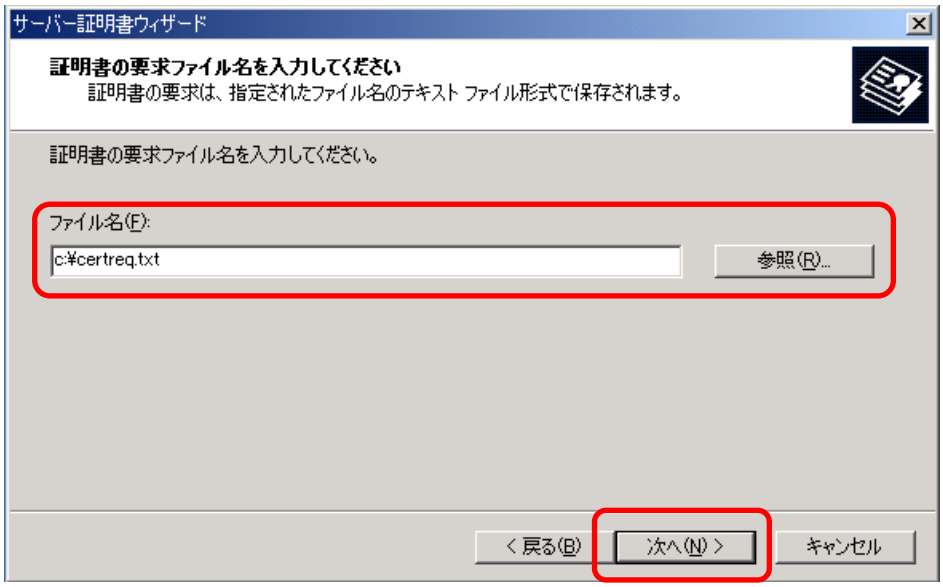
※指定可能な値については、「組織単位名(OU)について」をご覧ください。





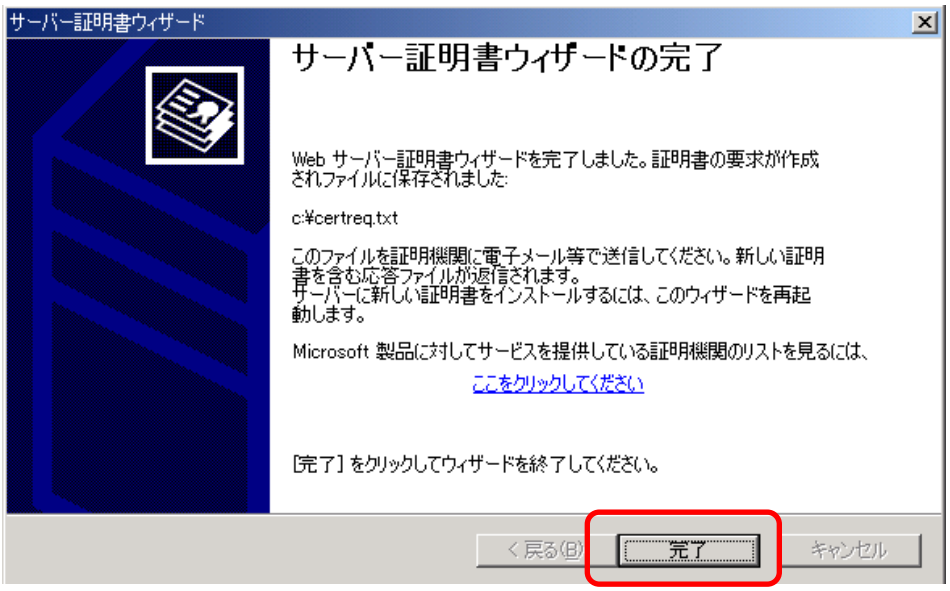


H) CSR の保存先とファイル名を任意に指定し、【次へ】をクリックします。



I) 入力情報を確認して、【次へ】をクリックします。

J）サーバー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、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(SureBoard / SureHandsOn)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/rD9fTPgo7u4aYzw4BpnAqLmGgy3XpsvCo6f4ROcFsgrkO5FgeUCaeDFyllEST
・・・・・
-----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

IIS5.0 では、CSR 作成後に秘密鍵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 サーバ証明書のインストールが完了するまでは、「保留中の要求」を絶対に削除しないでください。

※「保留中の要求」を削除されますと、元の CSR で発行した SSL サーバ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？

4.2. SSL サーバ証明書のダウンロード

SSL サーバ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。

≫ SSL サーバ証明書のダウンロードについて

5. 証明書のインストール

中間 CA 証明書と SSL サーバ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

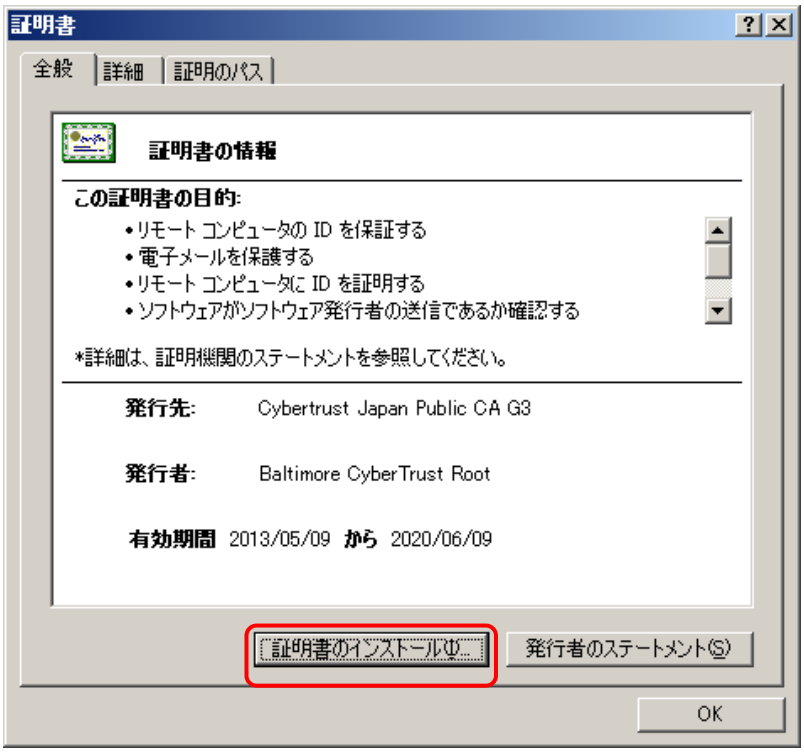
中間 CA 証明書のインストールを行います。

IIS で中間 CA 証明書のインストールを行う際、中間 CA 証明書より先に SSL サーバ証明書のインストールを行うと IIS の再起動が必要になる場合がありますので、中間 CA 証明書、SSL サーバ証明書の順でインストールを行うことをおすすめいたします。

※本手順に従いインストールした場合でも、お客様の環境によっては再起動が必要な場合もございます。あらかじめ、ご了承ください。

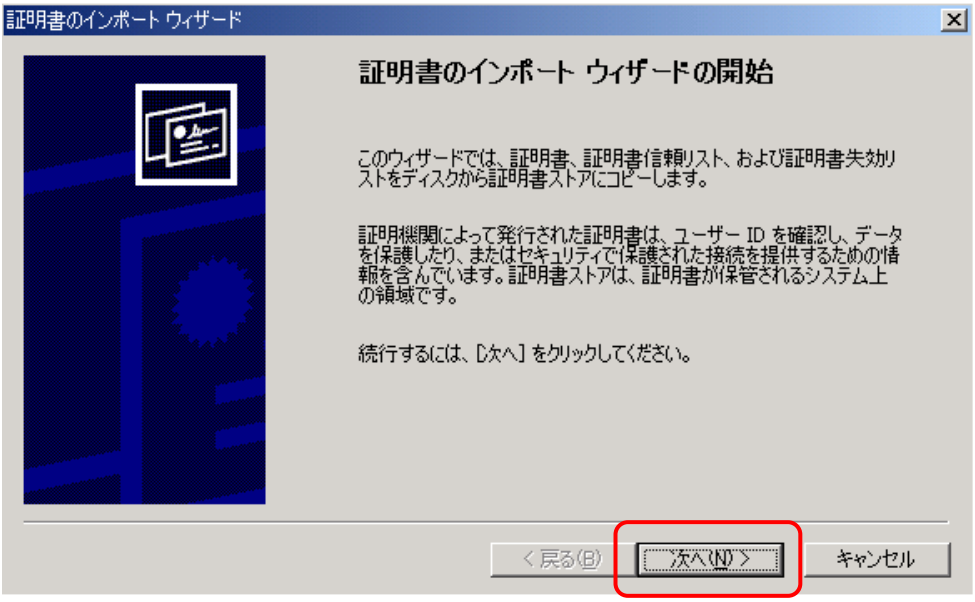
※SureServer EV[2048bit]・SureServer EV[SHA-2]、および、SureServer[2048bit]用クロスルート方式では、同様の手順で「クロスルート用中間 CA 証明書」と「中間 CA 証明書」をインストールしてください。

A) ダウンロードした中間 CA 証明書ファイルをダブルクリックで開き、【証明書のインストール】をクリックします。

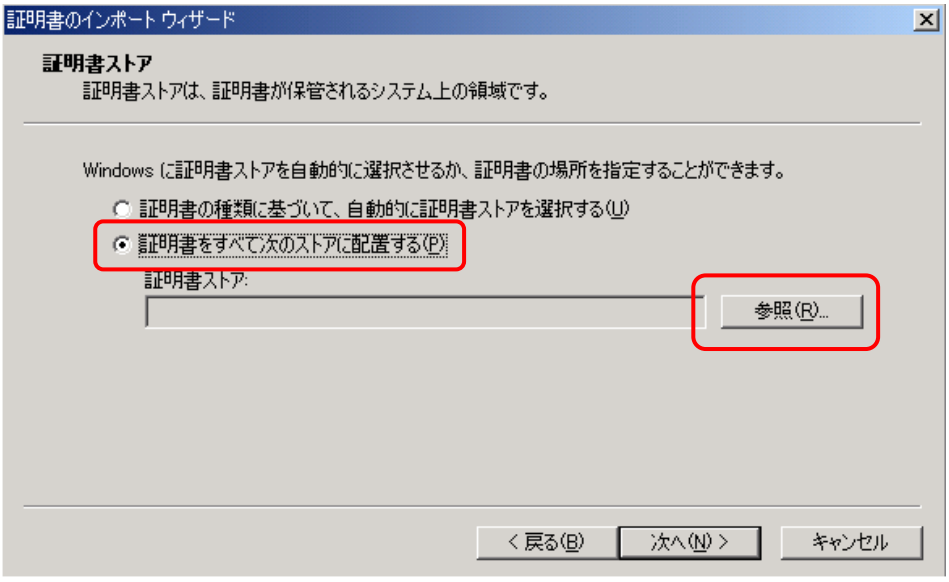


※画像はサンプルです。ご利用の中間 CA 証明書と内容が異なる場合があります。

B）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。

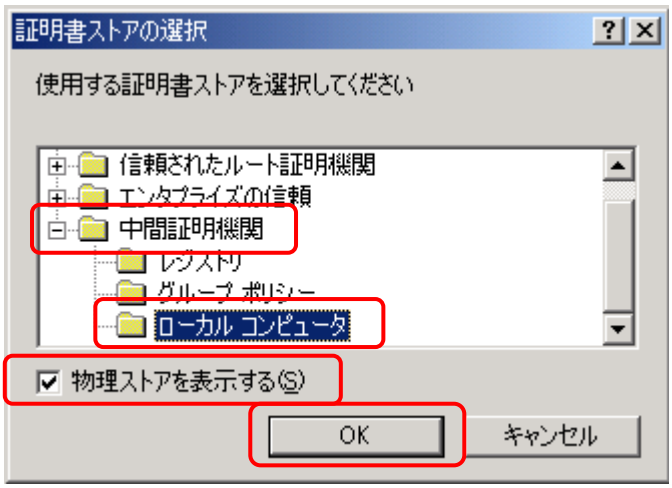


C）【証明書をすべて次のストアに配置する】を選択して、【参照】ボタンをクリックします。

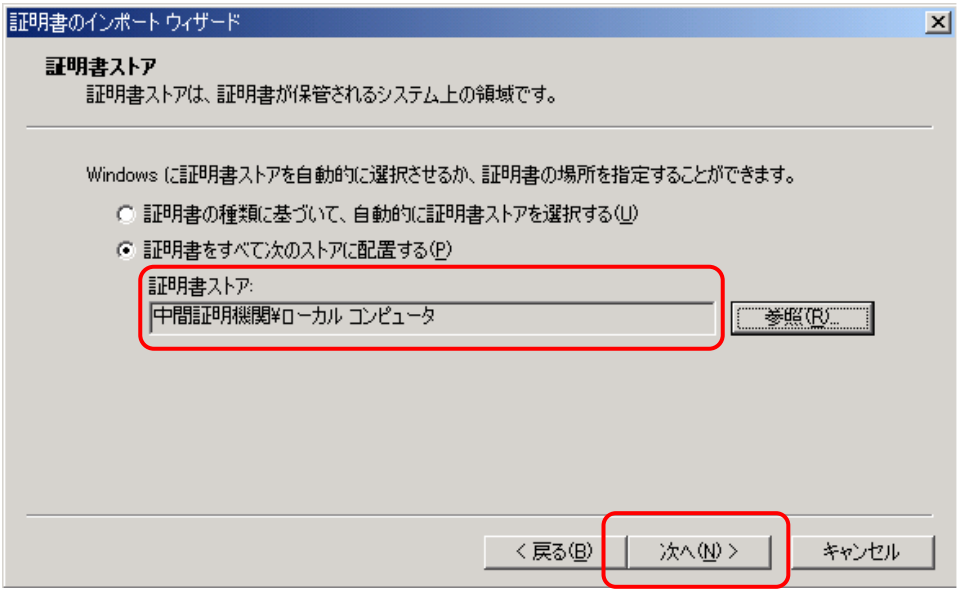


D）【物理ストアを表示する】をチェックして、【中間証明機関】→【ローカルコンピュータ】→【OK】をクリックします。

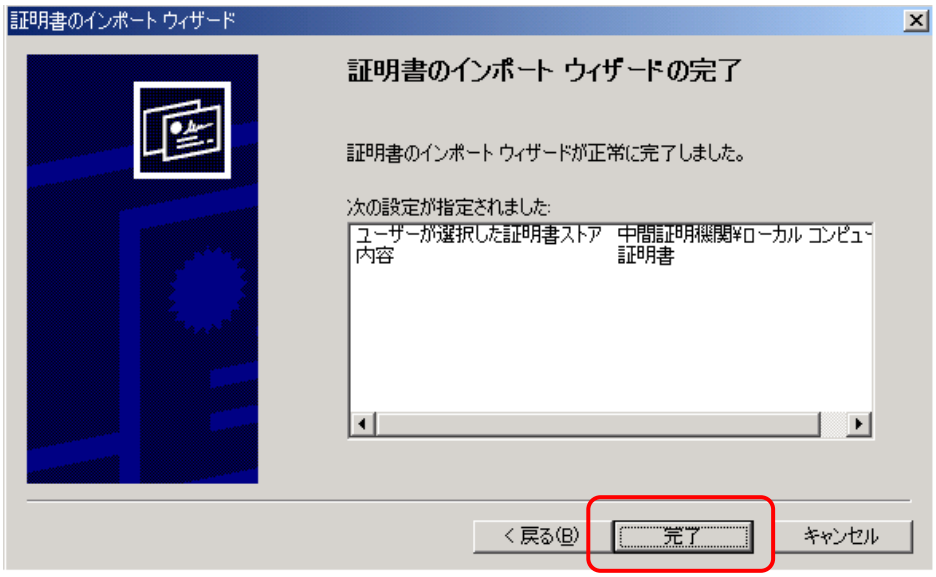
※【ローカルコンピュータ】が表示されない場合は、「8.「Microsoft 管理コンソール」での中間 CA 証明書のインストールと確認」をご参照ください。



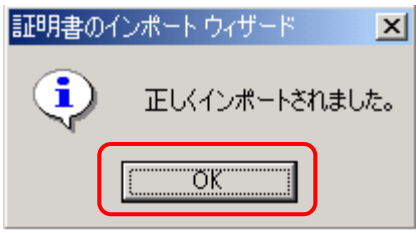
E）証明書ストアに【中間証明機関￥ローカル コンピュータ】が表示されていることを確認し、【次へ】をクリックします。



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。



※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。

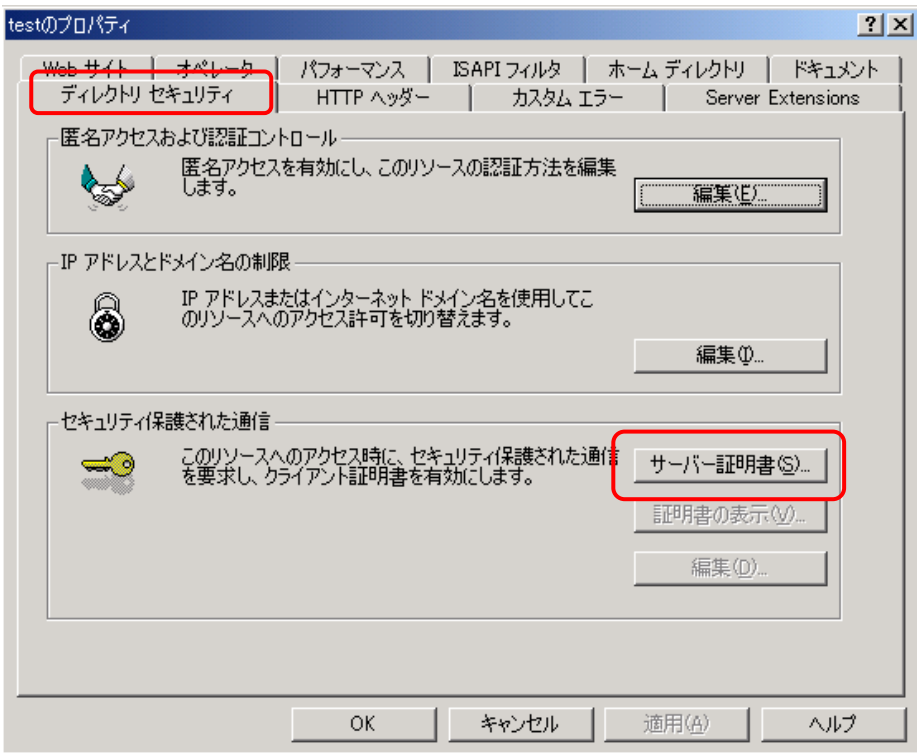
5.2. SSL サーバ証明書のインストール

SSL サーバ証明書のインストールを行います。

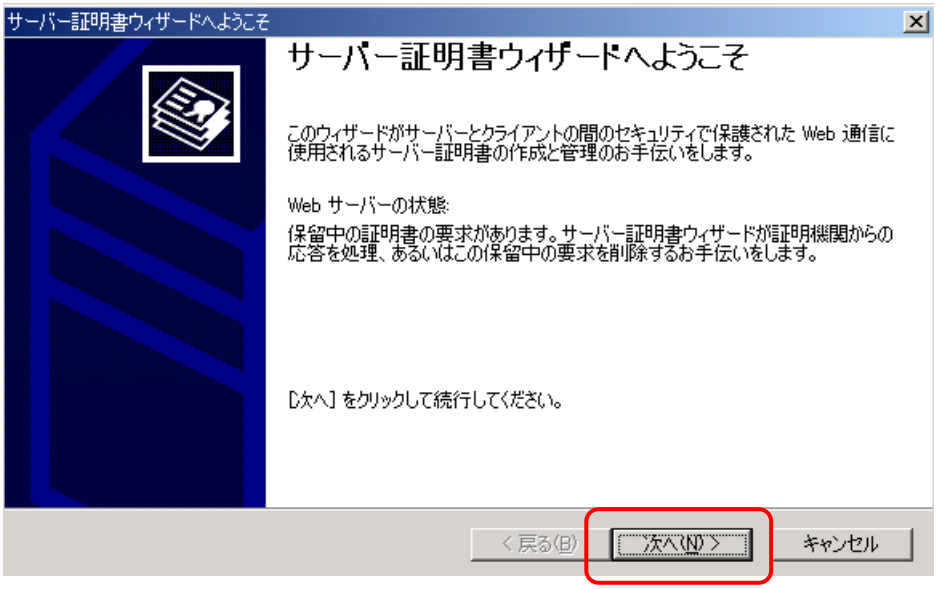
A) 【スタート】メニューから【管理ツール】→【インターネット サービスマネージャ】を選択し、IIS マネージャを起動します。

B) SSL サーバ証明書をインストールする Web サイトのプロパティを表示します。

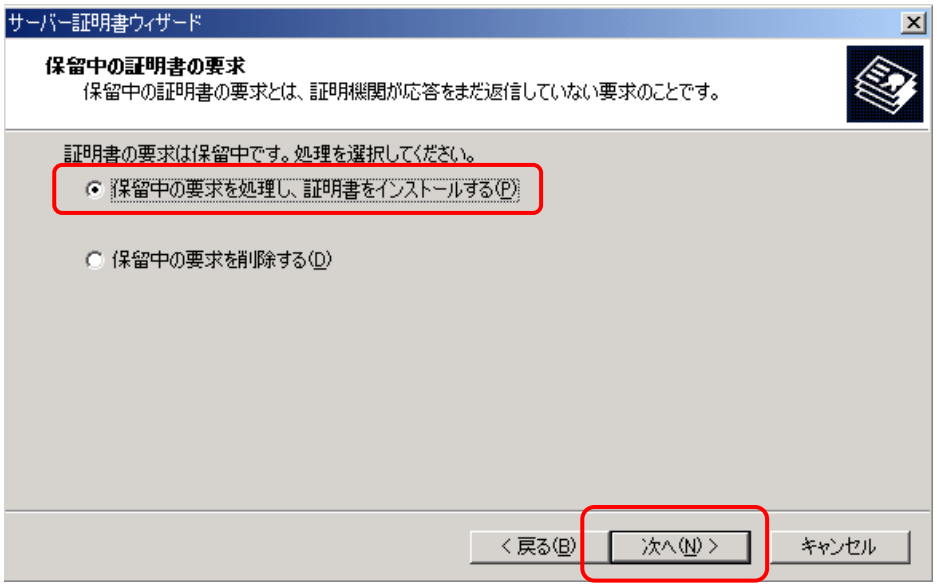
C）【ディレクトリ セキュリティ】タブ→【サーバー証明書】をクリックし、サーバー証明書ウィザードを起動します。



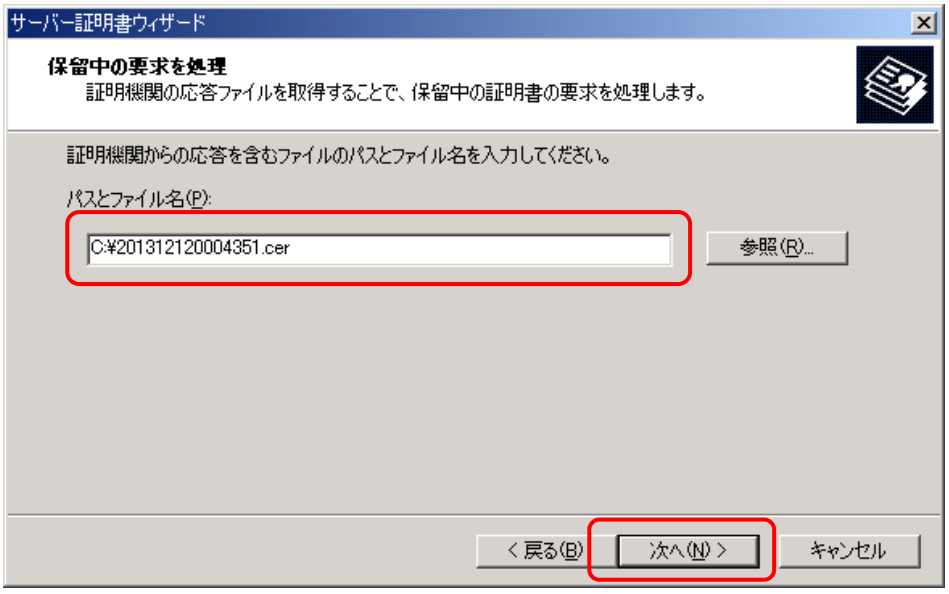
D）サーバー証明書ウィザードが表示されますので、【次へ】をクリックします。



E）【保留中の要求を処理し、証明書をインストールする】を選択して【次へ】をクリックします。

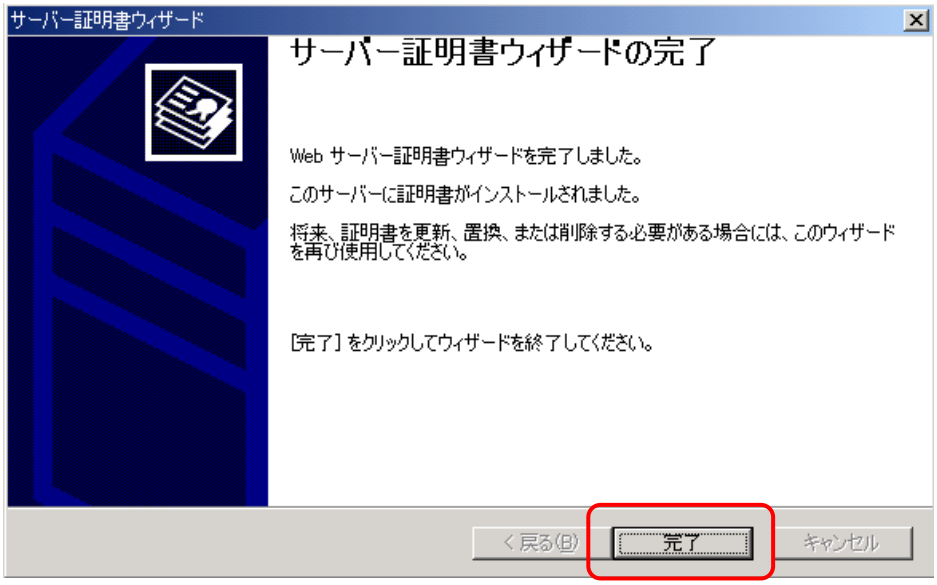


F）【パスとファイル名】に保存した SSL サーバ証明書のファイル名を入力し、【次へ】をクリックします。



G) インストールする証明書の内容を確認し、【次へ】をクリックします。

H) サーバー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。



以上でサーバ証明書のインストールは完了です。

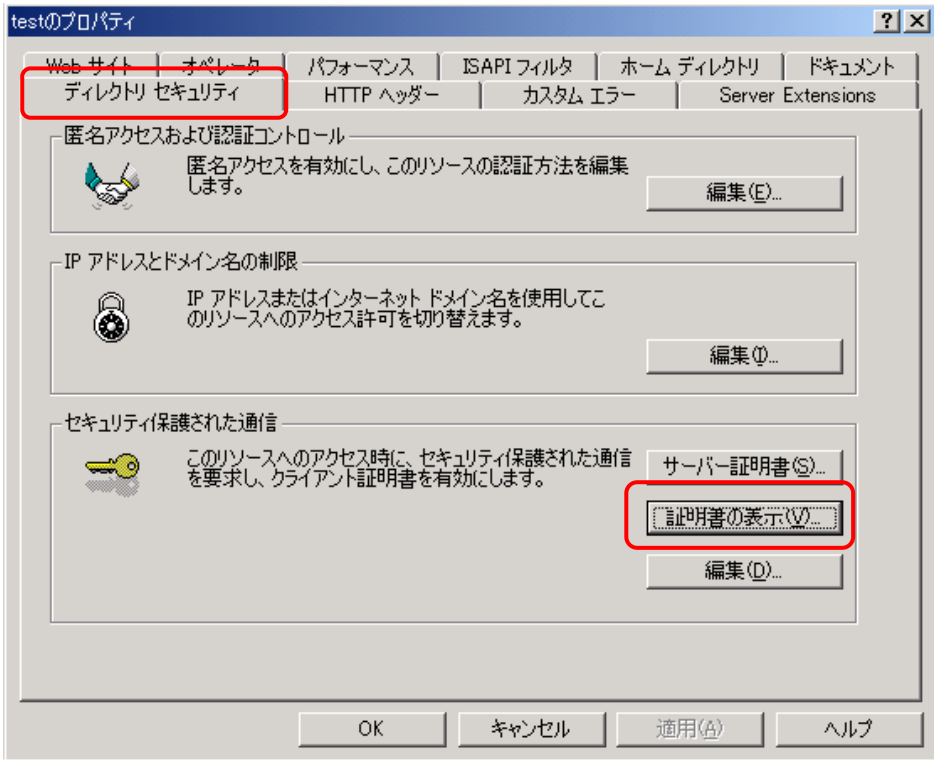
6. 鍵ペアファイルのバックアップ

鍵ペアファイルをバックアップします。

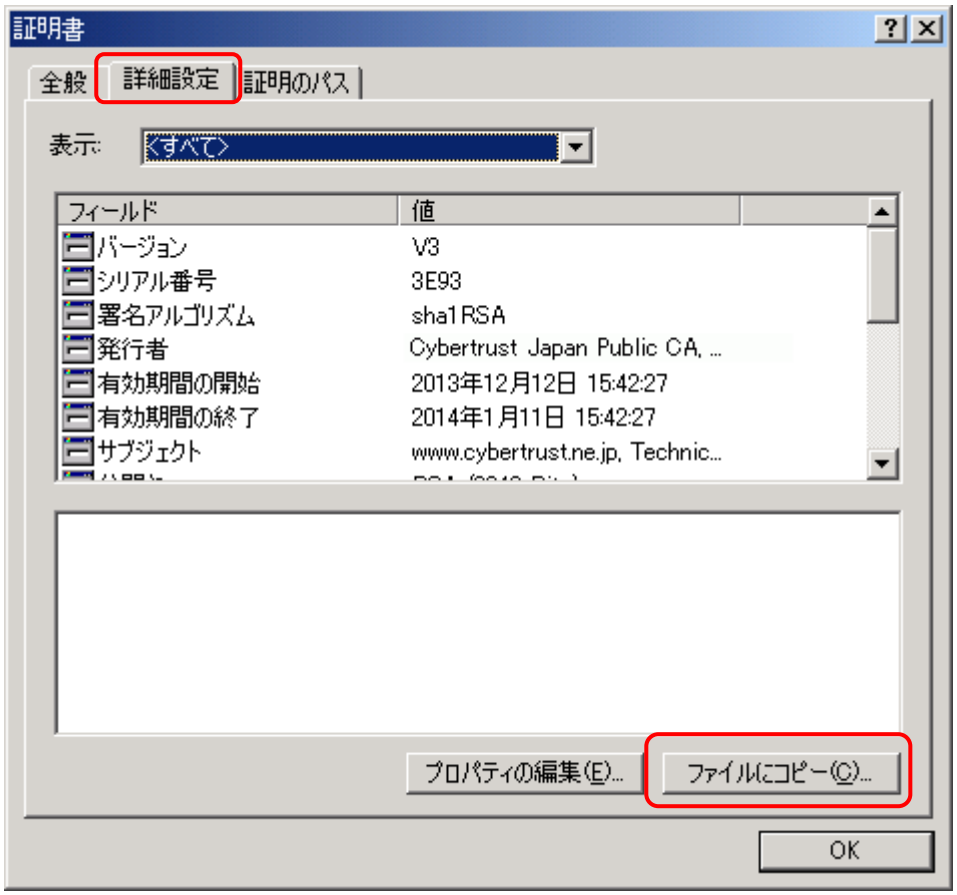
A) 【スタート】メニューから【管理ツール】→【インターネット サービスマネージャ】を選択し、IIS マネージャを起動します。

B) SSL サーバ証明書をインストールする Web サイトのプロパティを表示します。

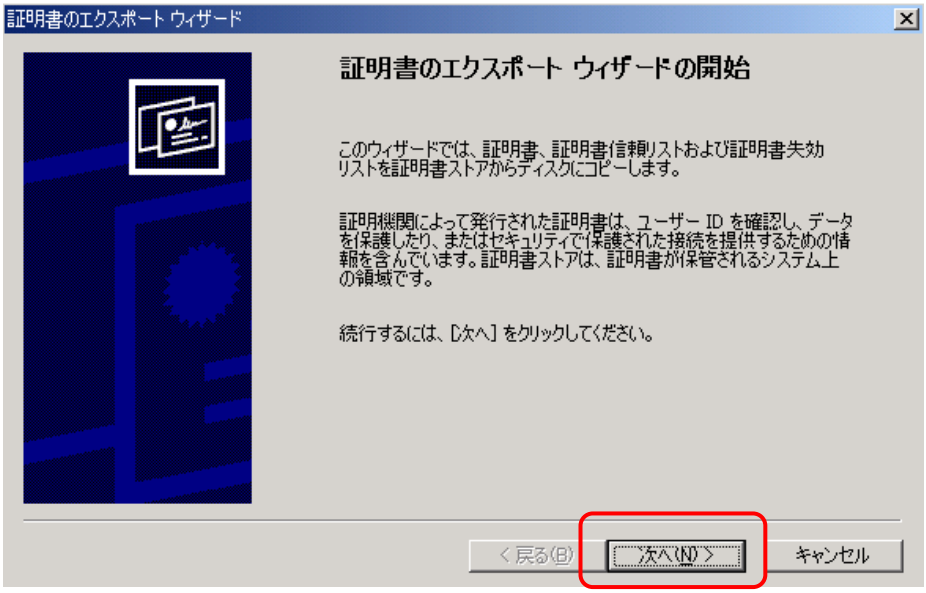
C) 【ディレクトリ セキュリティ】タブ→【証明書の表示】をクリックします。



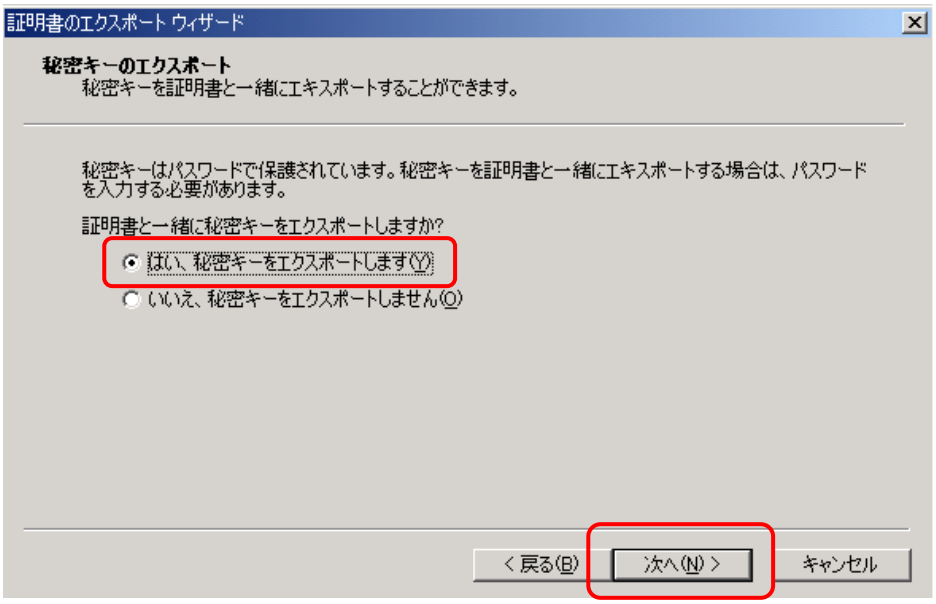
D）【詳細設定】タブ→【ファイルにコピー】をクリックし、エクスポートウィザードを起動します。



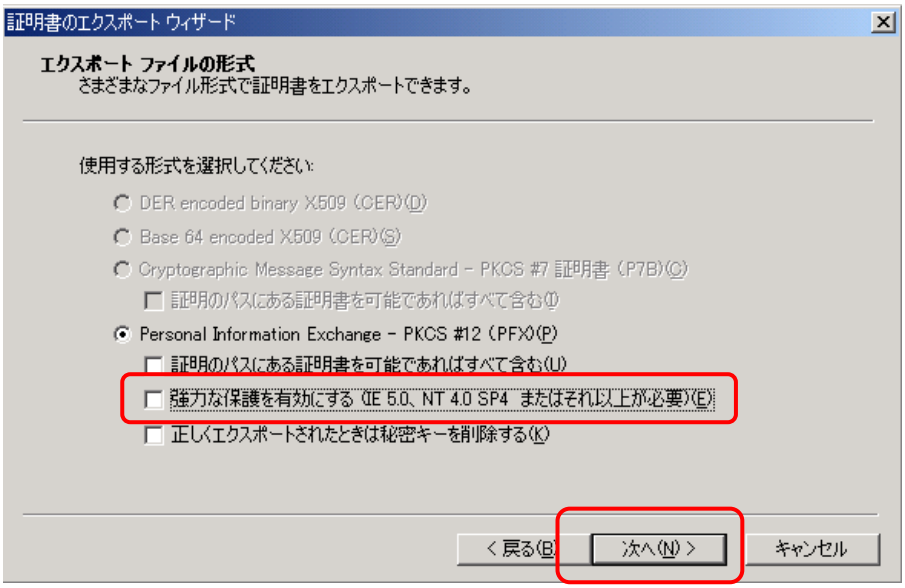
E）証明書のエクスポートウィザードが表示されますので、【次へ】をクリックします。



F）【はい、秘密キーをエクスポートします】を選択し、【次へ】をクリックします。

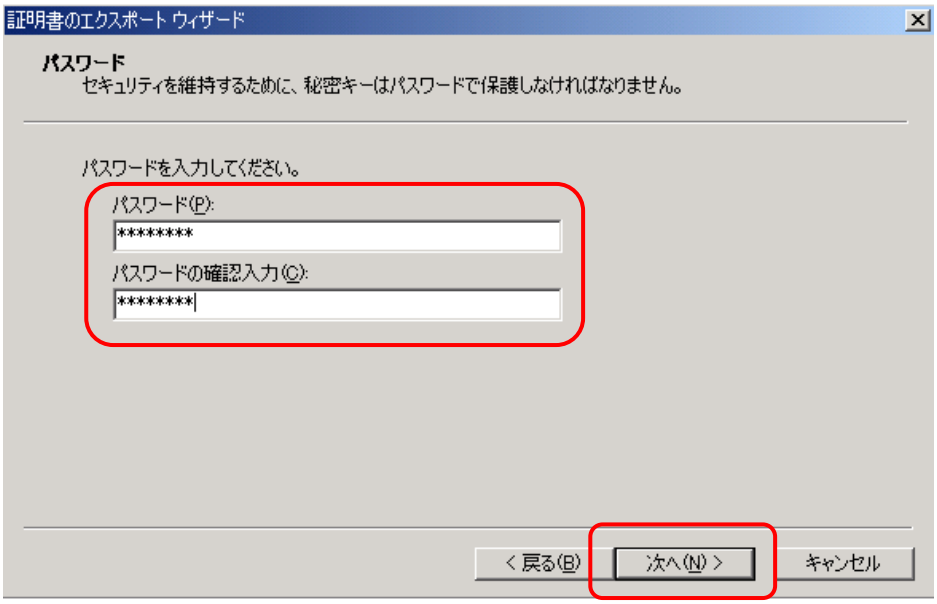


G）【強力な保護を有効にする】のチェックをはずし、【次へ】をクリックします。

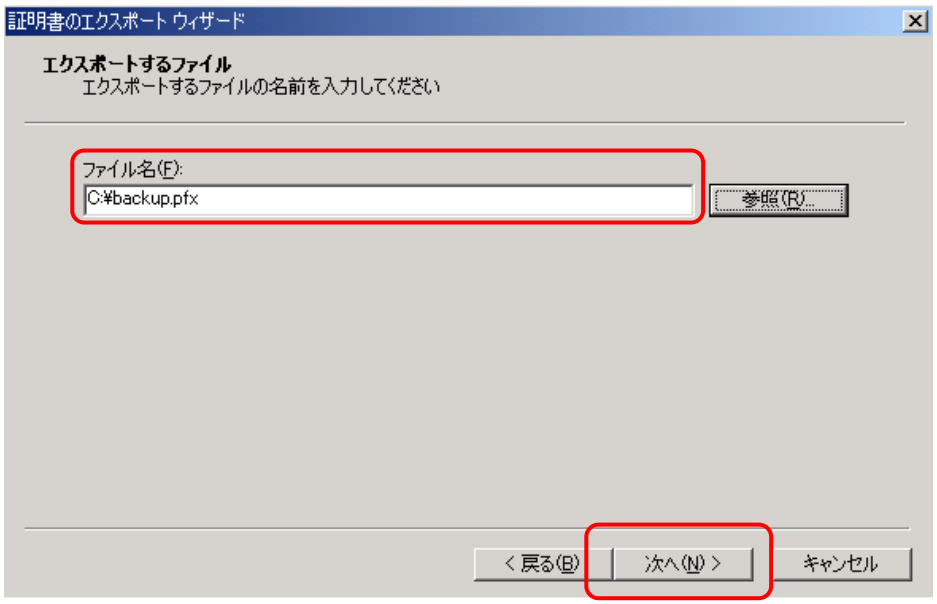


H) 【パスワード】、【パスワードの確認入力】に同じパスワードを入力し、【次へ】をクリックします。

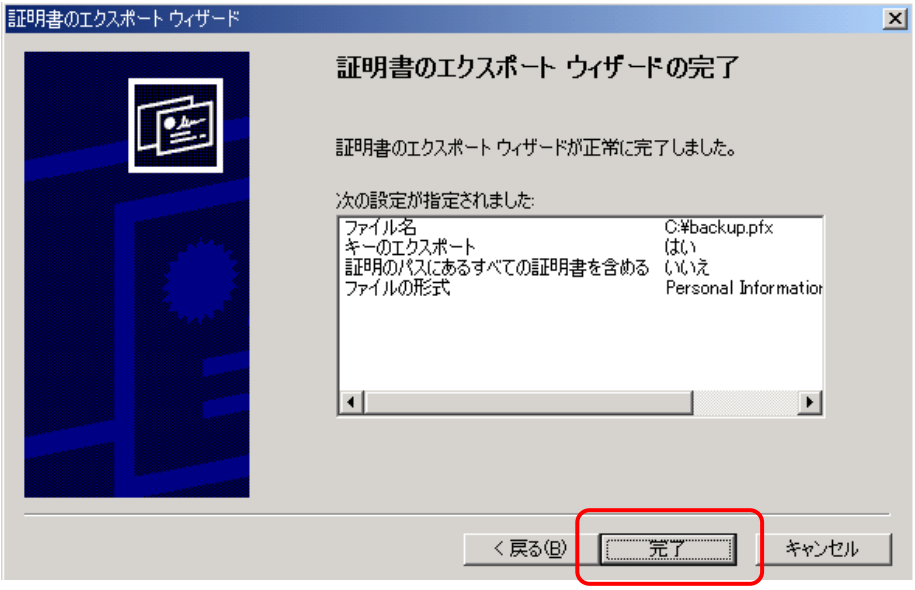
※パスワードは証明書インポート時に使用しますので大切に管理してください。



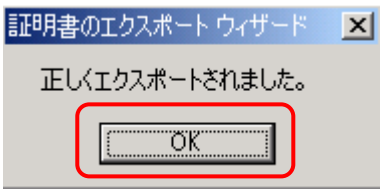
I) エクスポート先のファイル名(拡張子は.pfx)を指定し、【次へ】をクリックします。



J）証明書のエクスポートウィザードが正常に完了したことを確認し、【完了】をクリックします。



K）エクスポート終了のメッセージが表示されます。【OK】を押してバックアップ完了となります。



以上で、鍵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

7. 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

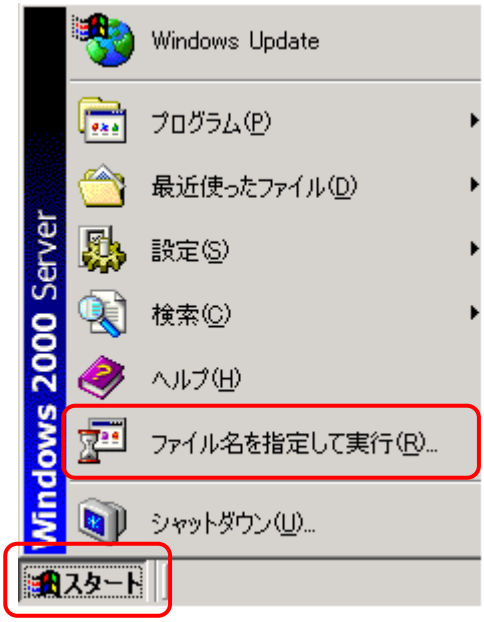
8.「Microsoft 管理コンソール」での中間 CA 証明書のインストールと確認

「信頼された証明機関から発行されていない」という警告が表示される場合は、中間 CA 証明書が正しくインストールされているか確認してください。

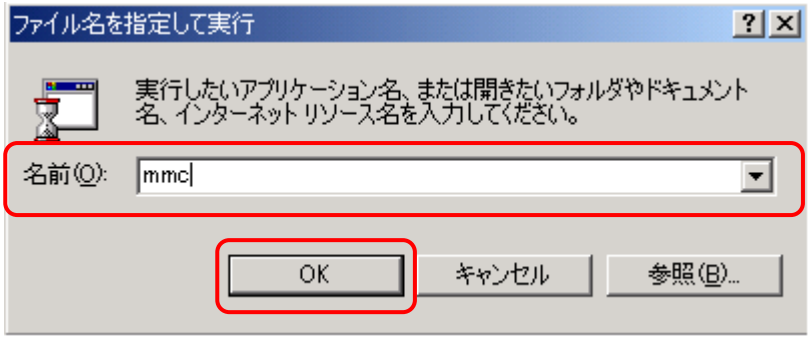
また、中間 CA 証明書をインストールする際に物理ストアとして「ローカルコンピュータ」が表示されない場合は、「Microsoft 管理コンソール (Microsoft Management Console:MMC)」から中間 CA 証明書のインポートを行ってください。

8.1. MMC の起動

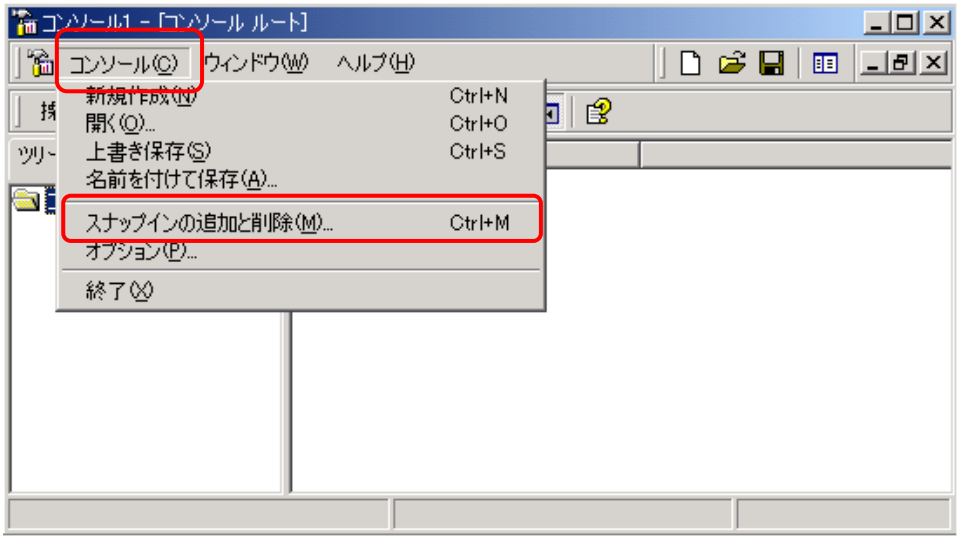
A) 【スタート】メニューから【ファイル名を指定して実行】をクリックします。



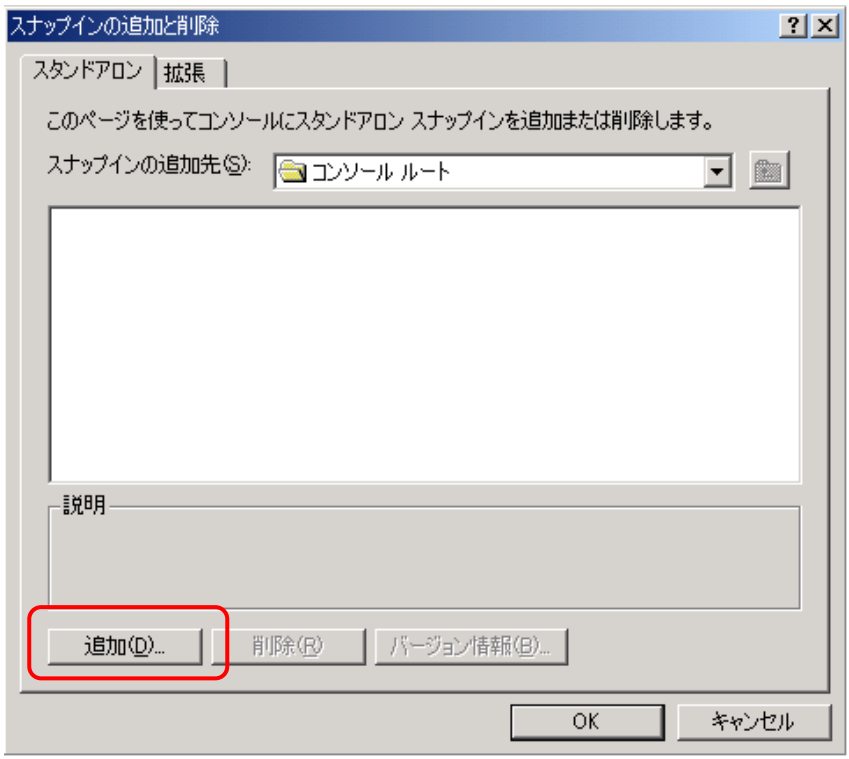
B) 【名前】へ「mmc」と入力して【OK】をクリックし、「Microsoft 管理コンソール」を開きます。



C) 画面左上の【コンソール】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。

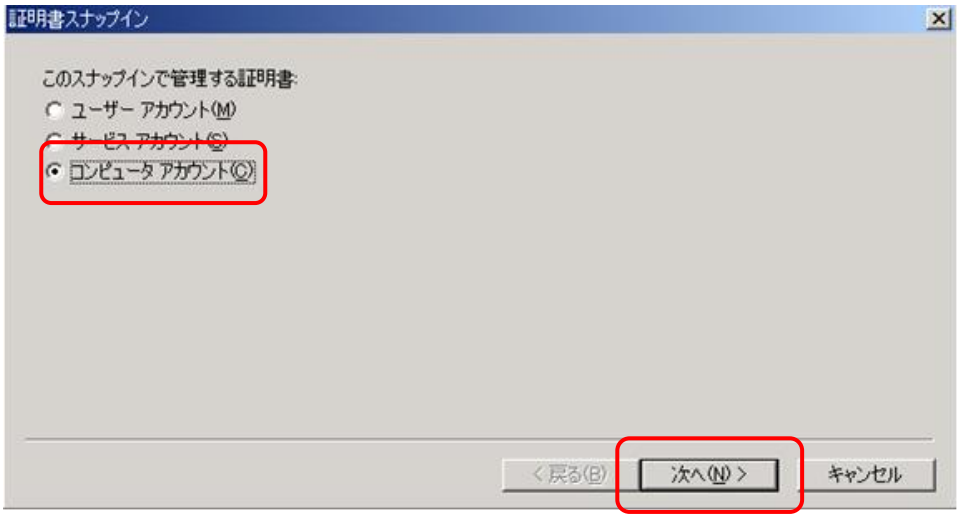


D）【スナップインの追加と削除】内の【追加】をクリックします。

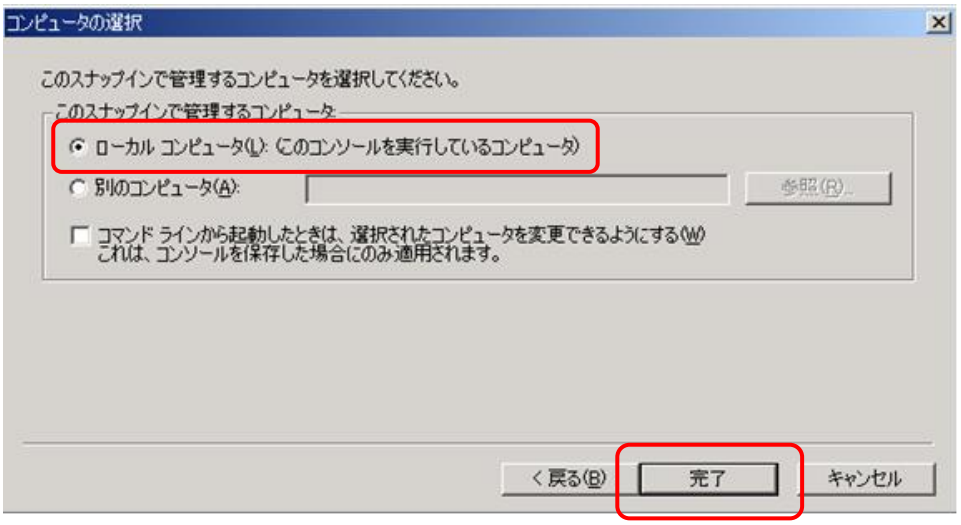


E）【利用できるスタンドアロン スナップイン】の中から【証明書】を選択し、【追加】をクリックします。

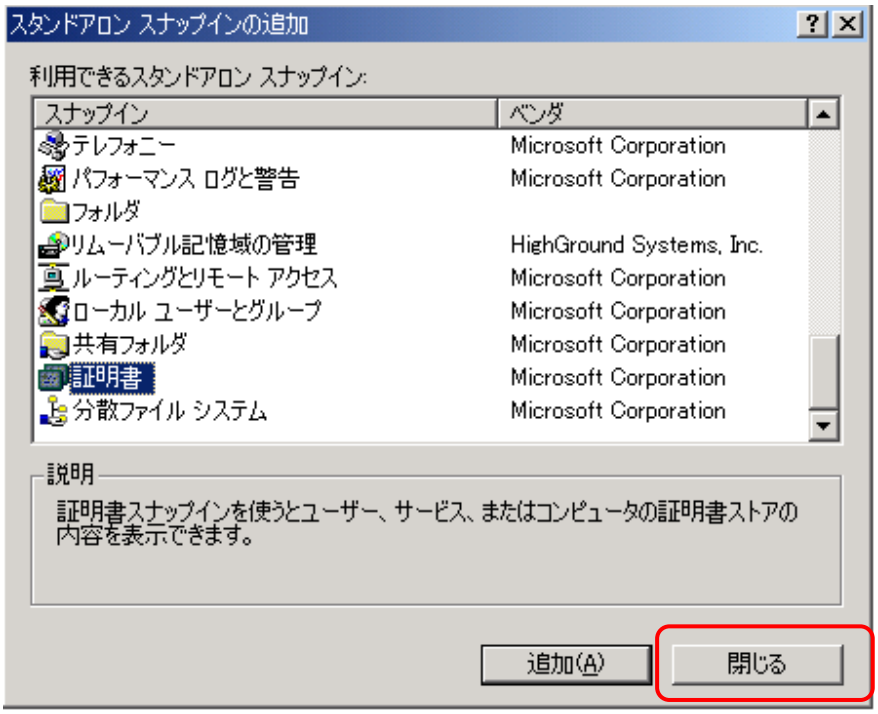
F）【コンピュータアカウント】を選択し、【次へ】をクリックします。



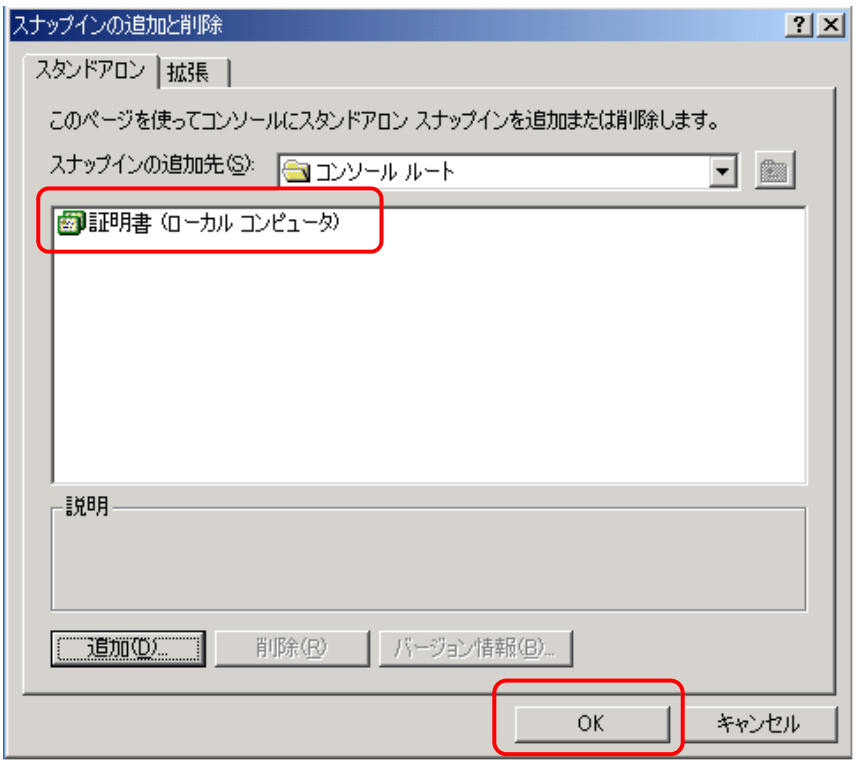
G）【ローカルコンピュータ（このコンソールを実行しているコンピュータ）】を選択し、【完了】をクリックします。



H）【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。



I） 【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。

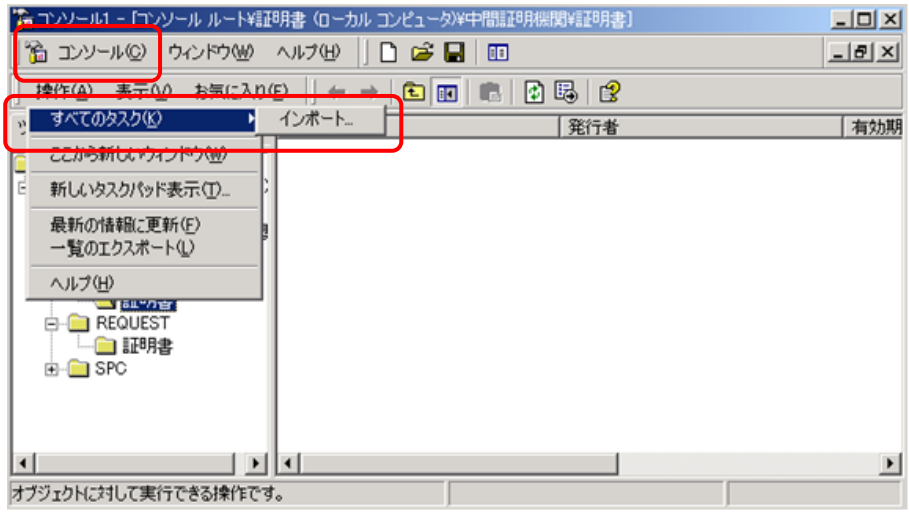


8.2. MMC から中間 CA 証明書をインストール

MMC から中間 CA 証明書をインストールします。

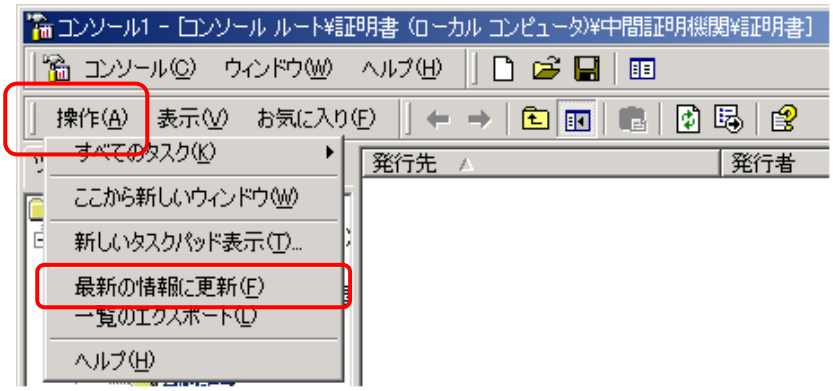
※中間 CA 証明書のインストールが完了している場合は手順をスキップしてください。

A) 画面の左上の【コンソール】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。



B) 証明書のインポートウィザードが表示されますので、「5.1 中間 CA 証明書のインストール」の「B) ～ G)」の手順に沿って、中間 CA 証明書をインストールします。

C) 【操作】メニュー→【最新の情報に更新】の順にクリックします。

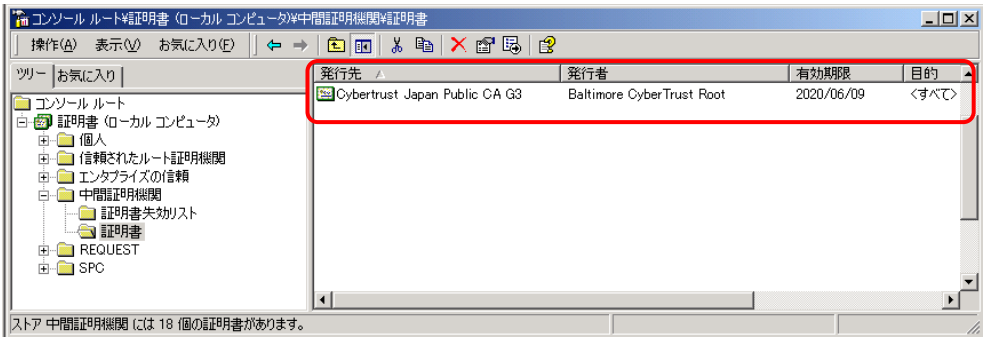


8.3. 中間 CA 証明書のインストール確認

正しく中間 CA 証明書がインストールされているか、確認します。

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。

B) 「発行先」の中間 CA 証明書のコモンネームと SSL サーバ証明書の「発行者」のコモンネームが一致しているかご確認ください。



【例】SureServer(2048bit)の場合