JPRS サーバー証明書発行サービス

サーバー証明書 インストール手順

（Microsoft IIS10. x 新規/更新）

Version 1.2

株式会社日本レジストリサービス（JPRS）

Copyright© 2026 Japan Registry Services Co., Ltd.

更新履歴

日付	Version	
2016/07/29	1.0	初版リリース
2017/10/18	1.1	「3. サーバー証明書のインストール」修正
2026/04/28	1.2	クロスルート証明書の手順を追記

Copyright© 2026 Japan Registry Services Co., Ltd.

1 事前準備

1.1 中間 CA 証明書とクロスルート証明書のダウンロード

以下より中間 CA 証明書とクロスルート証明書をダウンロードし、保存してください。

■中間 CA 証明書について

https://jprs.jp/pubcert/info/intermediate/

1.2 サーバー証明書のダウンロード

1.2.1 JPRS から送付される場合

JPRS から送付されるメール「サーバー証明書ダウンロード手続きのご案内[FQDN]」に記載されている URL より証明書をダウンロードしてください。

1.2.2 指定事業者から提供される場合

それぞれの事業者の指定する方法にてダウンロードしてください。

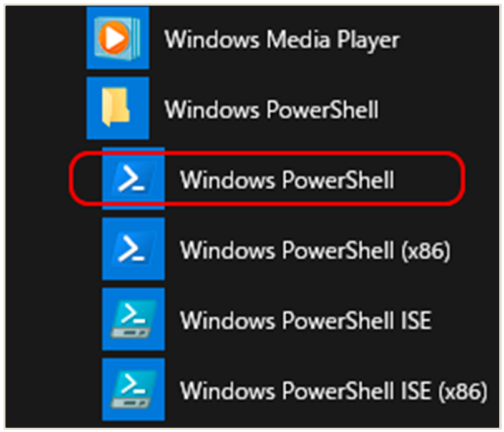
※詳細はサーバー証明書を購入した指定事業者にお問合せください。

Copyright© 2026 Japan Registry Services Co., Ltd.

2 中間 CA 証明書のインストール

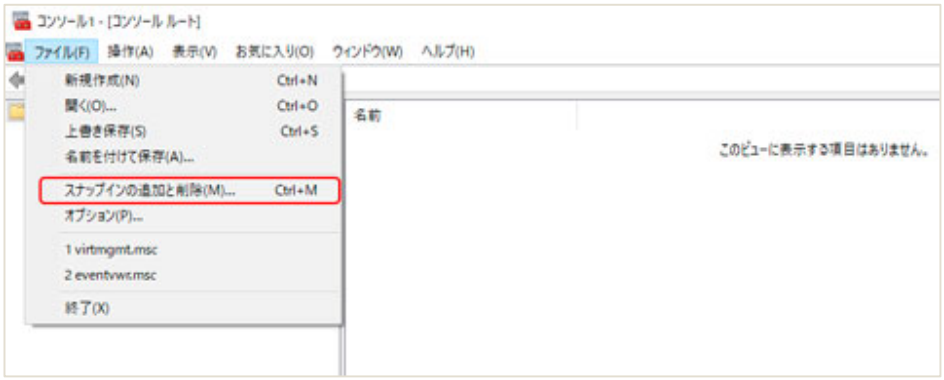
2.1 MMC コンソールの立ち上げ

画面左下のスタートより、W の欄にある[Windows PowerShell]より PowerShell を立ち上げ、「MMC」と入力し MMC コンソールを立ち上げます。



2.2 ［スナップインの追加と削除(M) ...］の選択

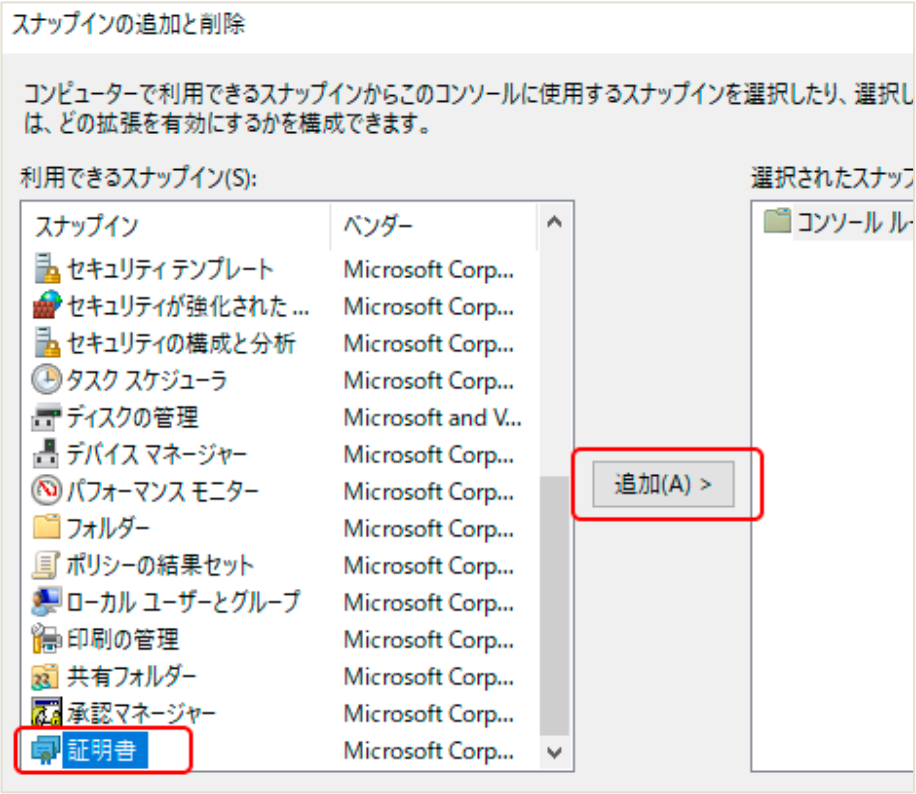
“コンソール”より[ファイル(F)]の［スナップインの追加と削除(M)］を選択します。



Copyright© 2026 Japan Registry Services Co., Ltd.

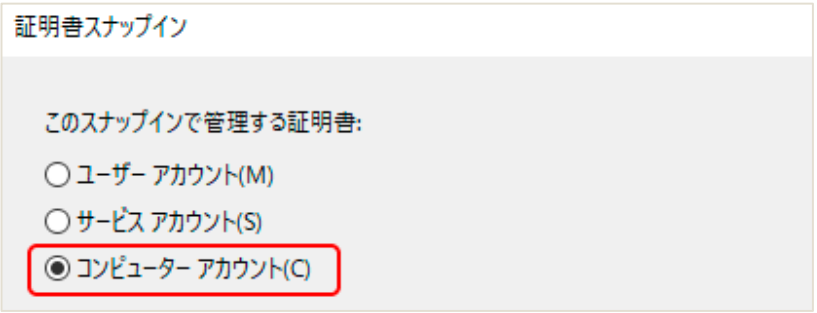
2.3 スナップインの追加

“スナップインの追加と削除”が立ち上がりますので、 「利用できるスナップイン(S)」から「証明書」を選択して [追加(A)] をクリックします。



2.4 「コンピューターアカウント(C)」の選択

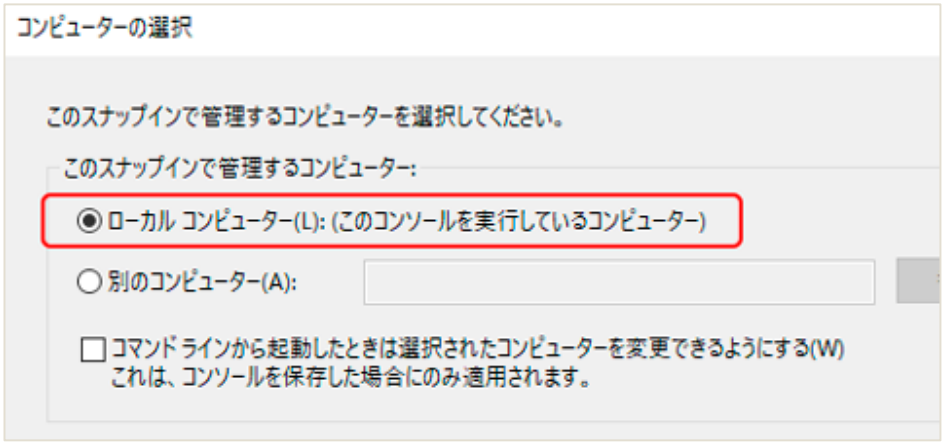
“証明書のスナップイン”で「コンピューターアカウント(C)」の選択し、[次へ(N)>] をクリックします。



Copyright© 2026 Japan Registry Services Co., Ltd.

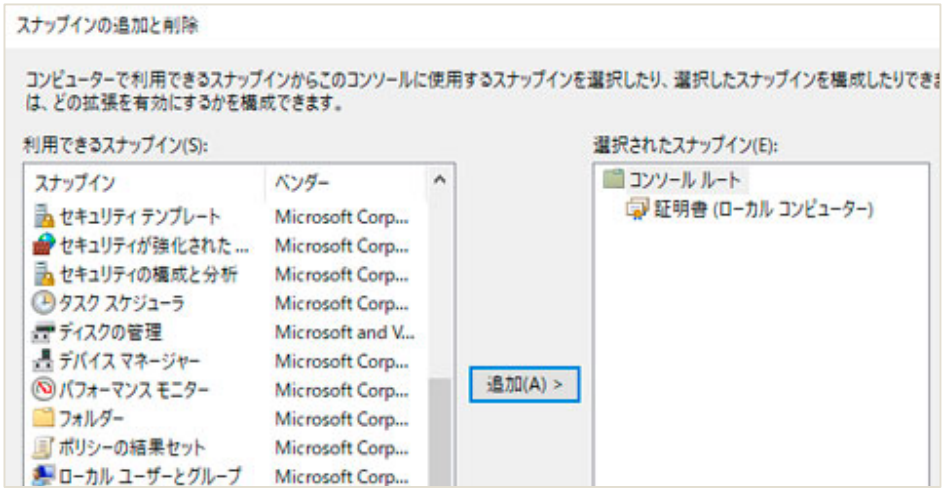
2.5 コンピューターの選択

“コンピューターの選択”で「ローカルコンピューター(L)」を選択して、[完了] をクリックします。



2.6 確認

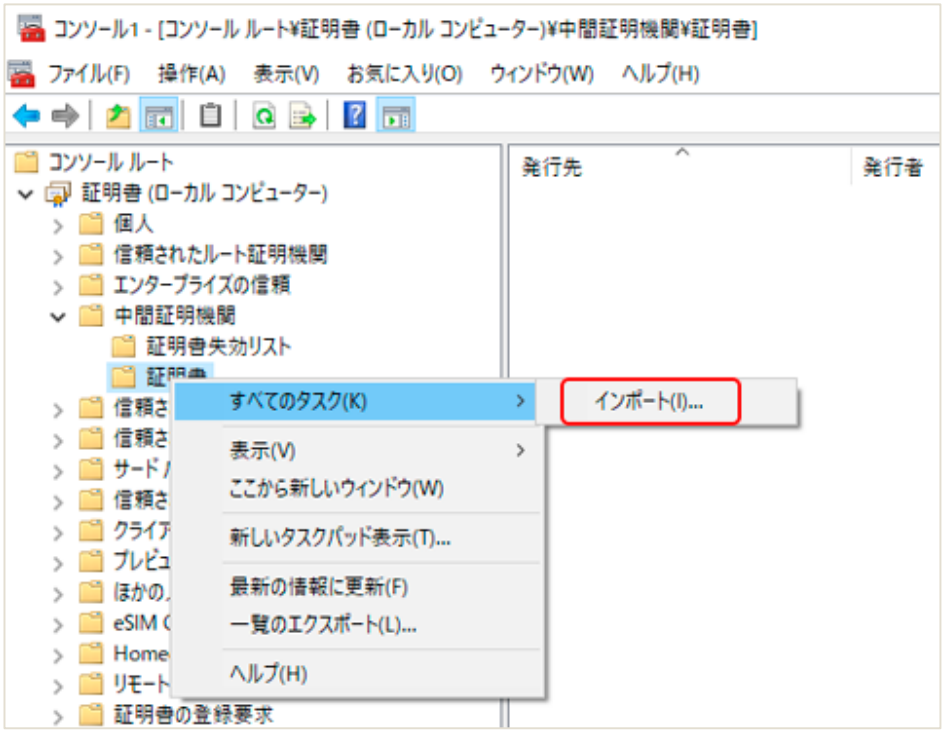
「選択されたスナップイン(E)」に証明書（ローカルコンピューター）が表示されていることを確認して、[OK]をクリックします。



Copyright© 2026 Japan Registry Services Co., Ltd.

2.7 中間証明書のインポート

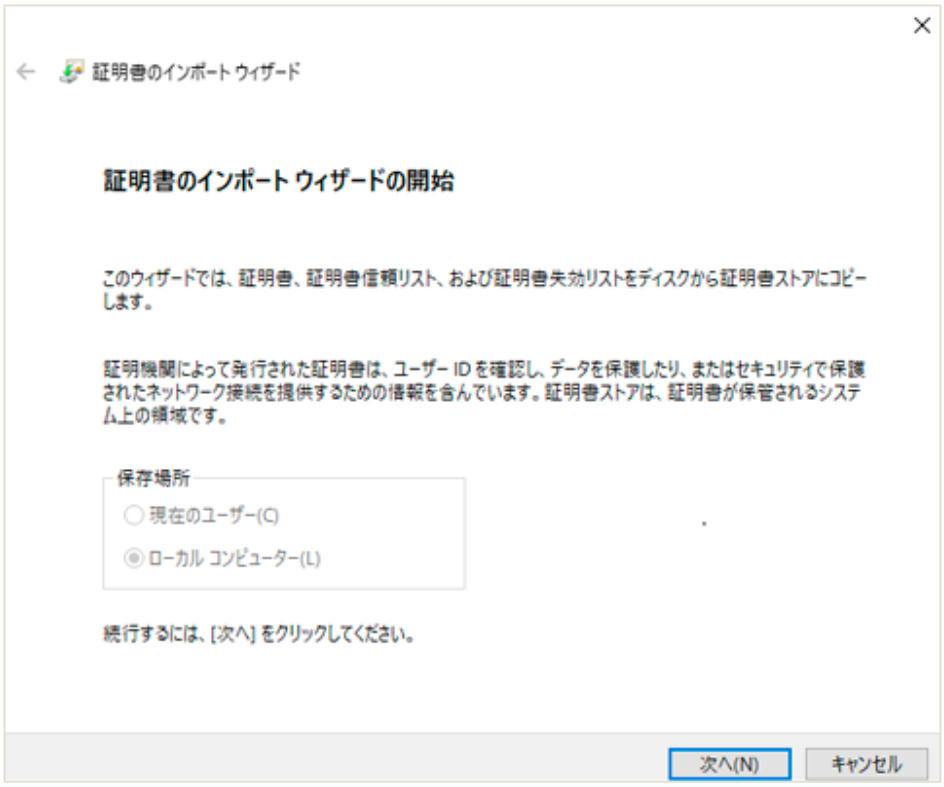
“コンソール”の[証明書(ローカルコンピューター)] → [中間証明機関] → [証明書] を右クリックし、[すべてのタスク(K)] → [インポート(I)...] をクリックします。



Copyright© 2026 Japan Registry Services Co., Ltd.

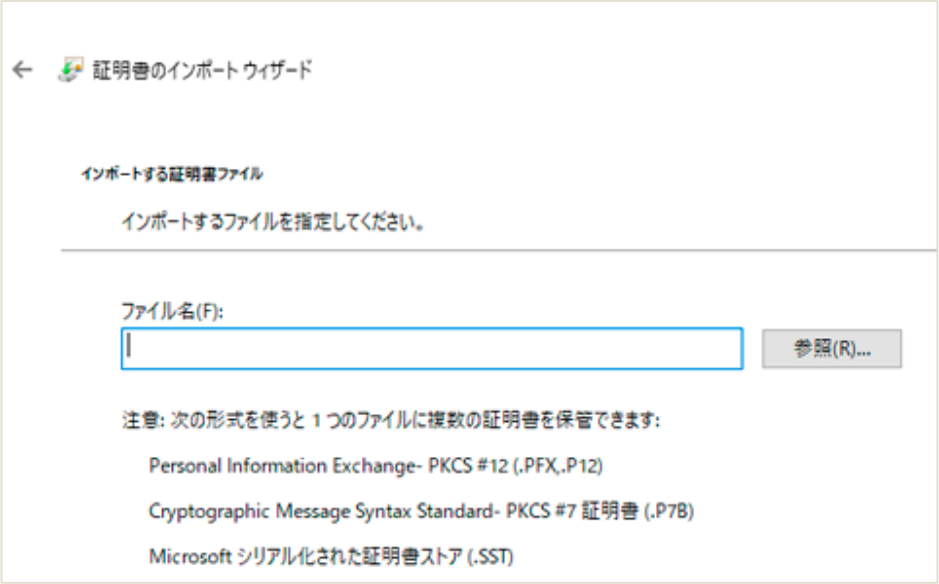
2.8 “証明書インポートウィザード”の立ち上げ

“証明書インポートウィザード”が立ち上がりますので、[次へ(N)]をクリックします。



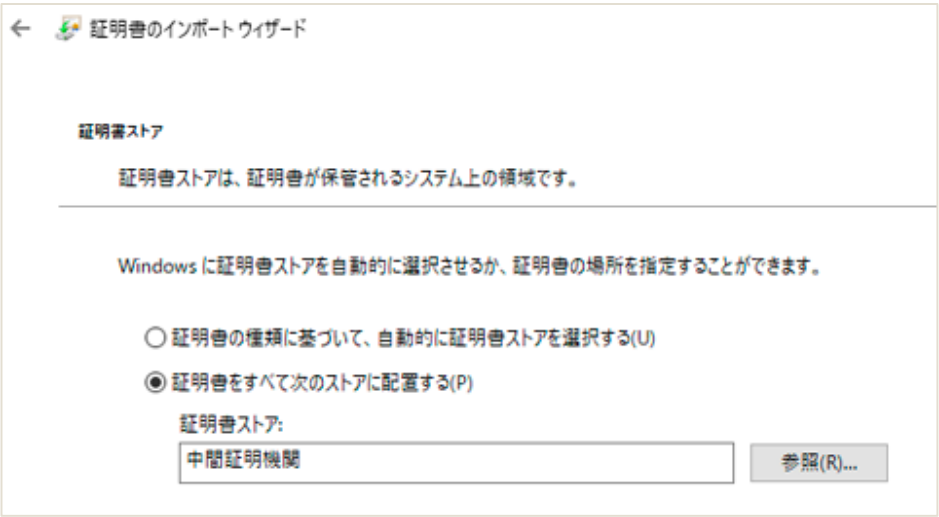
Copyright© 2026 Japan Registry Services Co., Ltd.

“インポートする証明書ファイル“では [参照(R)] をクリックし、管理画面でダウンロードした中間 CA 証明書を開き、ファイル名(F)に中間 CA 証明書が表示されていることを確認して、[次へ (N)>] をクリックします。



2.9 「証明書をすべて次のストアに配置する(P)」の選択

「証明書をすべて次のストアに配置する(P)」を選択し、証明書ストアが“中間証明機関“になっていることを確認して、[次へ(N)>] をクリックします。



Copyright© 2026 Japan Registry Services Co., Ltd.

2.10 完了

証明書インポートウィザードの[完了]をクリックします。

2.11 クロスルート証明書の追加

クロスルート証明書で、手順 2.7～2-10 を再実施します。

※手順 2-8 インポートする証明書ファイル"は、ダウンロードしたクロスルート証明書（tlsrsarootca2024cross-pem.cer）を選択してください。

以上で中間 CA 証明書のインストールは完了です

2.12 ルート証明書の削除

Windows サーバーでは、ルート CA への信頼された証明書パスが複数ある場合、ブラウザーで警告メッセージが表示されることがあります。

Microsoft 社のサイトに記載の回避策の通り、ルート証明書の削除およびルート証明書の自動更新を停止してください。
https://learn.microsoft.com/ja-jp/troubleshoot/windows-server/certificates-and-public-key-infrastructure-pki/secured-website-certificate-validation-fails

■回避策（参考）

1. システム管理者としてデバイスにログオンします。
2. 次の手順に従って、証明書スナップインを Microsoft Management Console に追加します。
   - [スタート] > [実行] をクリックし、「mmc」と入力して Enter キーを押します。
   - [ファイル] メニューの [スナップインの追加と削除] をクリックします。
   - [証明書] を選択して [追加] をクリックし、[コンピューター アカウント] を選択して [次へ] をクリックします。

Copyright© 2026 Japan Registry Services Co., Ltd.

- [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)] を選択して、[完了] をクリックします。
- [OK] をクリックします。

3. 管理コンソールで [証明書 (ローカル コンピューター)] を展開し、[信頼されたルート証明機関]－[証明書]をクリックします。
4. ルート証明書一覧から、発行先・発行者が[SECOM TLS RSA Root CA 2024]を見つけます。
    - 証明書を削除するには、証明書を右クリックし、[削除] をクリックします。
    - 証明書を無効にするには、証明書を右クリックし、[プロパティ] をクリックして [この証明書のすべての目的を無効にする] を選択し、[OK] をクリックします。
5. 問題がまだ発生している場合は、サーバーを再起動します。

さらに、サーバー上で [ルート証明書を自動更新しない] グループ ポリシー設定が無効になっているか、設定されていない場合は、次回チェーンビルドが発生したときに、使用しない証明書パスの証明書が有効化またはインストールされる可能性があります。 グループ ポリシー設定を変更するには、次の手順を実行します。

1. [スタート] > [実行] をクリックし、「gpedit.msc」と入力して Enter キーを押します。
2. [コンピューター構成] > [管理用テンプレート] > [システム] > [インターネット通信管理] を展開し、[インターネット通信の設定] をクリックします。
3. [ルート証明書を自動更新しない] をダブルクリックし、[有効] を選択して [OK] をクリックします。
4. ローカル グループ ポリシー エディターを修了します。

Copyright© 2026 Japan Registry Services Co., Ltd.

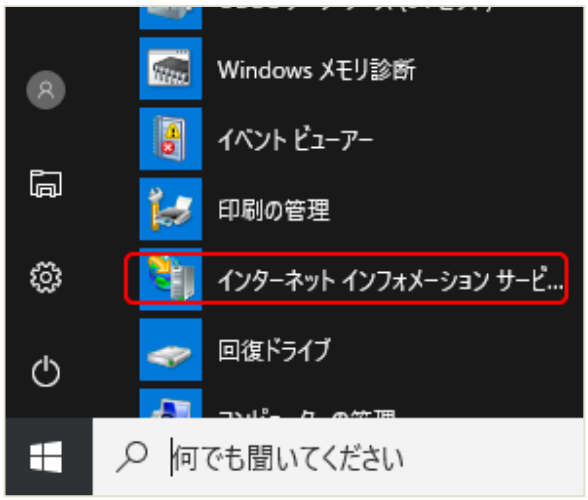
3 サーバー証明書のインストール

3.1 サーバー証明書の拡張子を *.cer に変更

JPRS が提供するサーバー証明書の拡張子は「*.crt」となっていますので、拡張子を「*.cer」に変更してください。

3.2 インターネット インフォメーション サービス (IIS) マネージャの実行

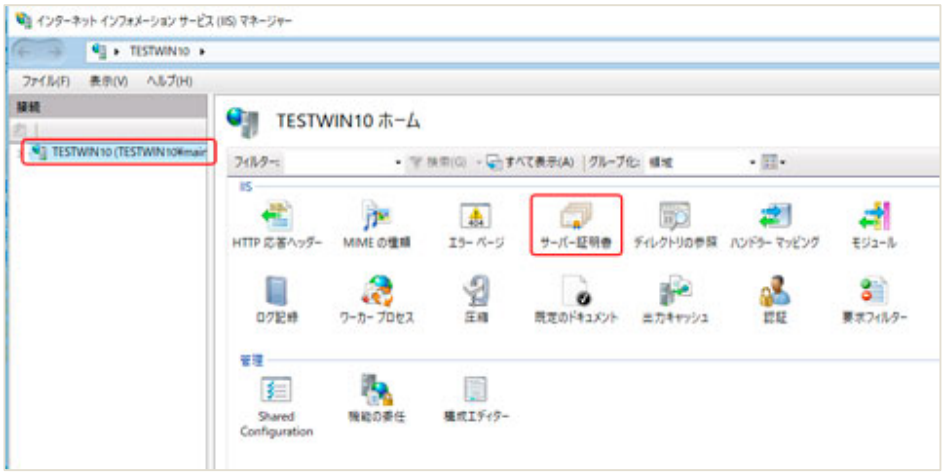
画面左下のスタートより、W の欄にある[Windows 管理ツール]［インターネット インフォメーション サービス (IIS) マネージャー タイル］ を実行します。



3.3 ［サーバー証明書］アイコンの実行

画面左にあるサーバー名を選択し、画面中央にある ［サーバー証明書］アイコンを実行します。

Copyright© 2026 Japan Registry Services Co., Ltd.



画面の中央が[サーバー証明書]に変わり、右の表示が変わります。

3.4 ＜証明書の要求を完了する＞ダイアログの表示

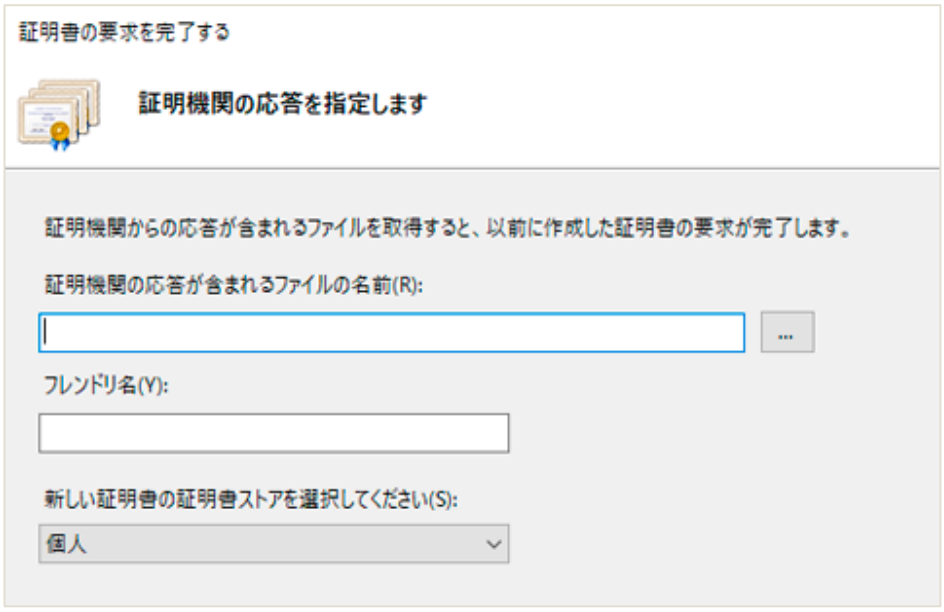
画面右にある ［証明書の要求の完了...］メニューを実行します。

＜証明書の要求を完了する＞ダイアログがポップアップします。

3.5 サーバー証明書のファイルの名前の入力

証明機関の応答を指定します。

Copyright© 2026 Japan Registry Services Co., Ltd.



［証明機関の応答が含まれるファイルの名前(R)］は、[…]をクリックしダウンロードしたサーバー証明書を指定します。

［フレンドリ名(Y)］は、証明書を識別するための任意の名前を入力します。
※フレンドリ名はわかりやすいよう、以下のような値をお勧めします。

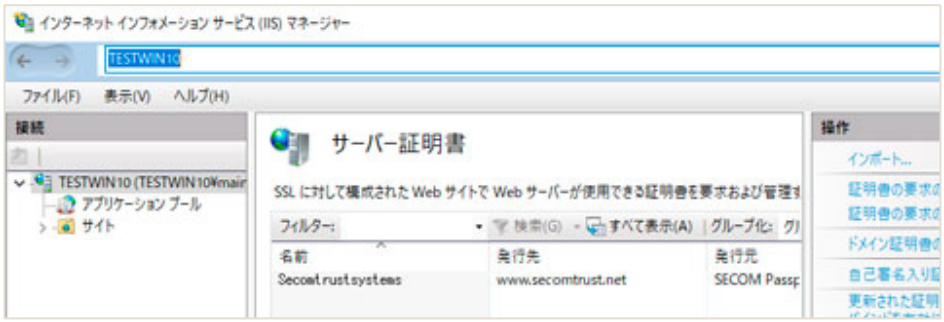
- ウェブ・サイト名
- 有効期間の満了年月
- 弊社が発行したこと (従来他社をご使用だった場合)

「新しい証明書の証明書ストアを選択してください(S)」では、証明書ストアを選択し、［OK］ ボタンを実行し、ダイアログを閉じます。

3.6 確認

インストールした証明書が、 [サーバー証明書]中央のリスト・ボックスに追加されたのを確認ください。

Copyright© 2026 Japan Registry Services Co., Ltd.



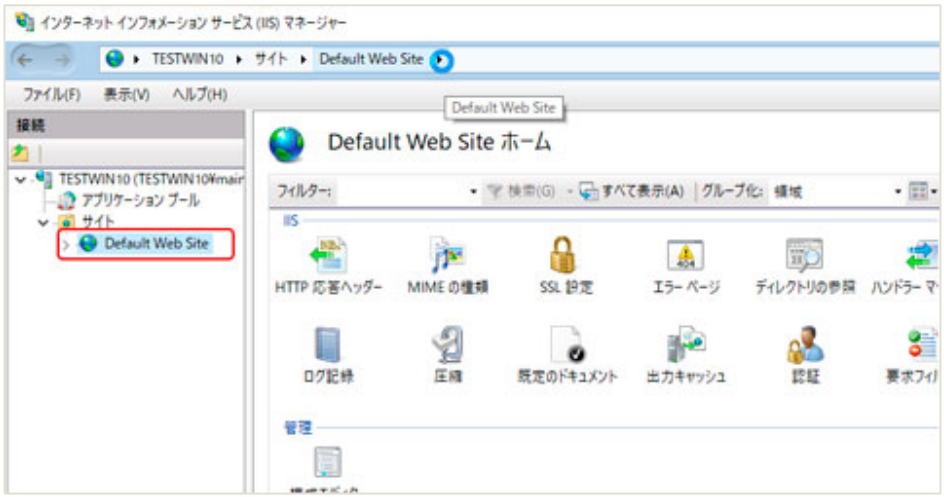
以上でサーバー証明書のインストールは完了です。

4 バインドの追加

4.1 証明書をインストールするサイトの択一

［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］の画面左にある［サイト］アイコンをクリックし、証明書をインストールするサイトを択一ください。

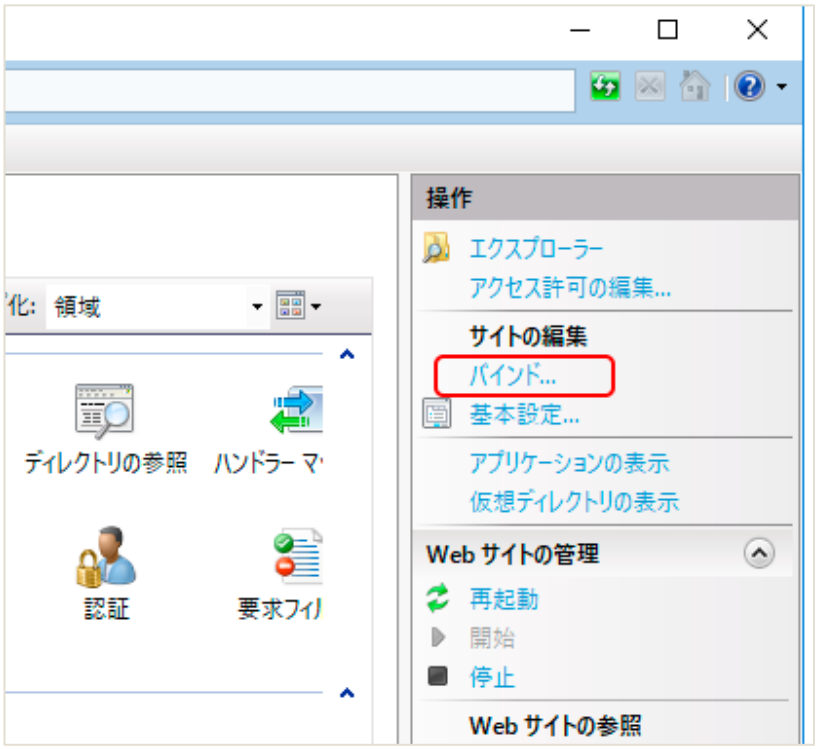
画面の中央にサイトのホームが表示され、画面右の表示が変わります。



Copyright© 2026 Japan Registry Services Co., Ltd.

4.2 ［バインド...］の実行

画面右の［操作］メニューから［バインド...］を実行します。



<サイト バインド> ダイアログが表示されます。

※バインドを初めて設定するとき(証明書の初導入)と、バインドを再設定するとき(証明書の再導入)で、手順が違います。

- 初めての場合は「新規バインドの設定」を参照ください。
- 再設定の場合は「既存バインドの再設定」を参照ください。

Copyright© 2026 Japan Registry Services Co., Ltd.

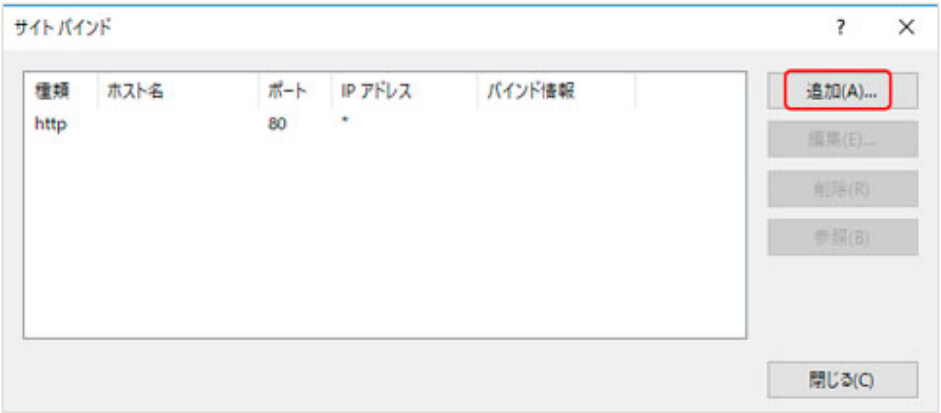
ご利用のサイトに初めてサーバー証明書を導入する場合

4.3 新規バインドの設定

こちらは、 初めてサーバー証明書を導入する場合の手順です。

4.3.1 <サイト バインド>の追加

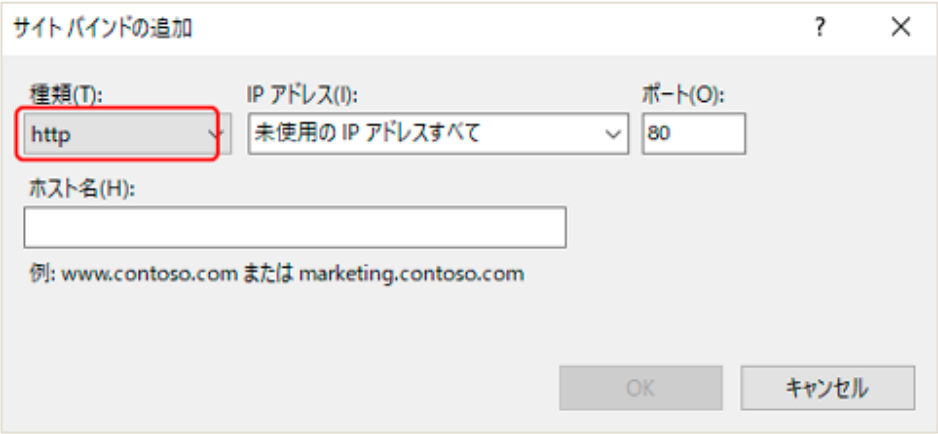
<サイト バインド>の［追加(A)...］ボタンを実行します。



<サイト バインドの追加>ダイアログがポップアップします。

4.3.2 種類の選択

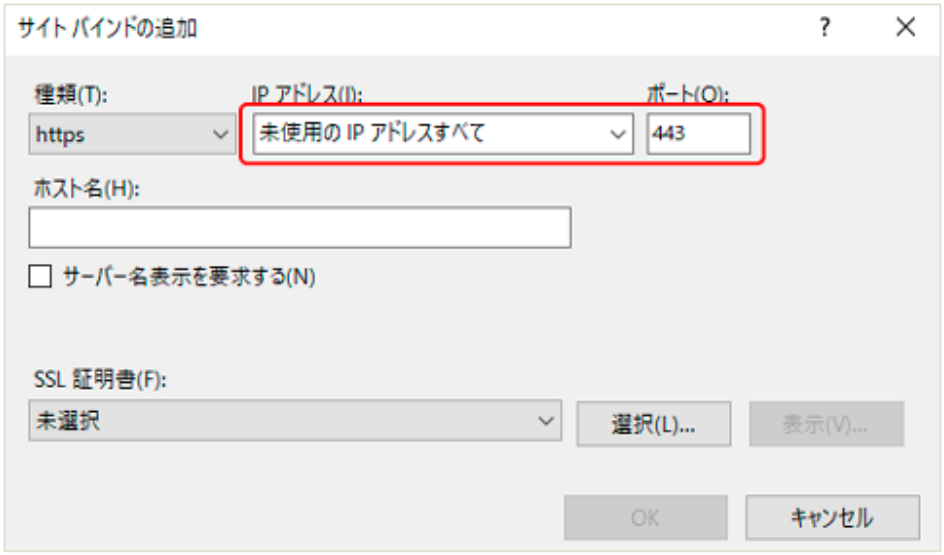
［種類(T)］プルダウンから［https］を択一して、［SSL 証明書(F)］を表示させます。



Copyright© 2026 Japan Registry Services Co., Ltd.

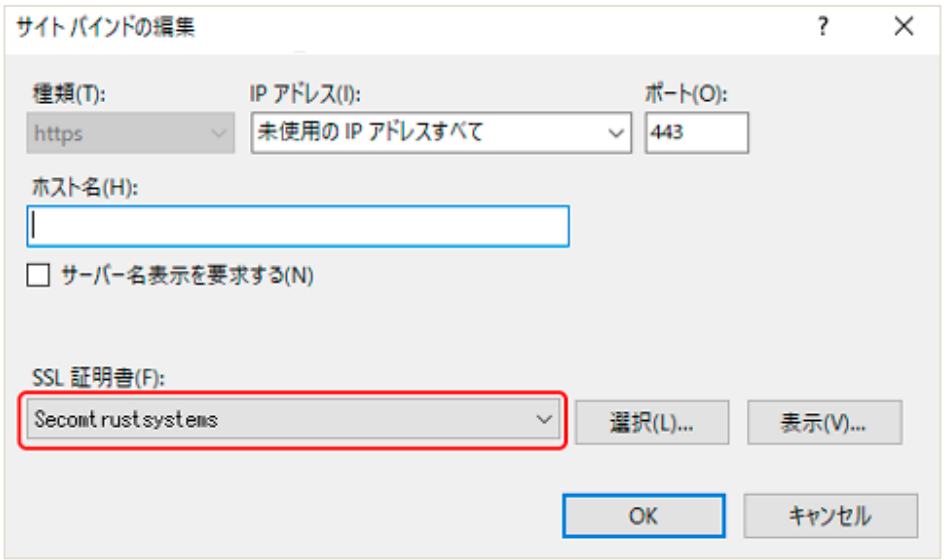
4.3.3 IP アドレスとポートの入力

［IP アドレス(I)］と［ポート(O)］(通常、SSL ポートとして 443 番を利用します)を入力します。



4.3.4 証明書の択一

［SSL 証明書(F)］のプルダウン・リストから、サイトに設定する証明書を択一します。



［OK］ボタンをクリックし、＜サイト バインドの追加＞のダイアログを閉じます。

Copyright© 2026 Japan Registry Services Co., Ltd.

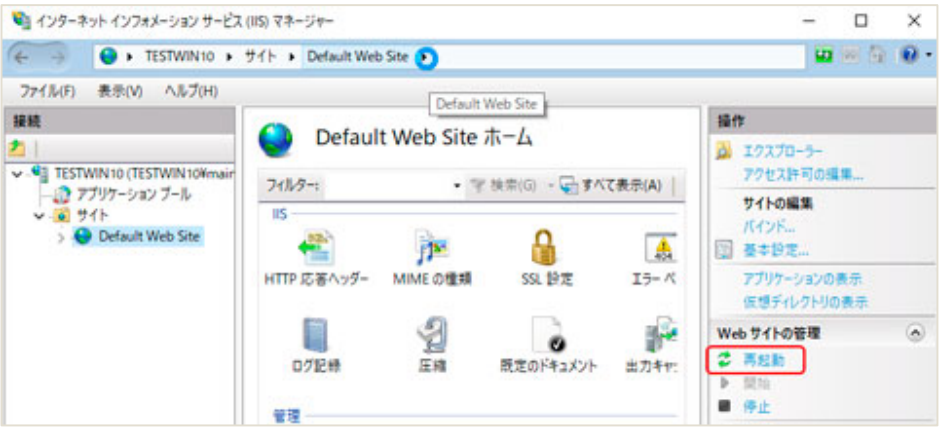
4.3.5 <サイト バインド> リストへの追加の確認

<サイト バインド> のリスト・ボックスに、「https」のバインドが追加されたことを確認します。

［閉じる(C)］ボタンを実行し、ダイアログを閉じます。

4.3.6 ［Web サイトの管理］の［再起動］の実行

画面右［操作］の［Web サイトの管理］の［再起動］を実行します。［再起動］の実行できないときは［開始］を実行してください。



以上で証明書のインストール(初導入) は完了です。

Copyright© 2026 Japan Registry Services Co., Ltd.

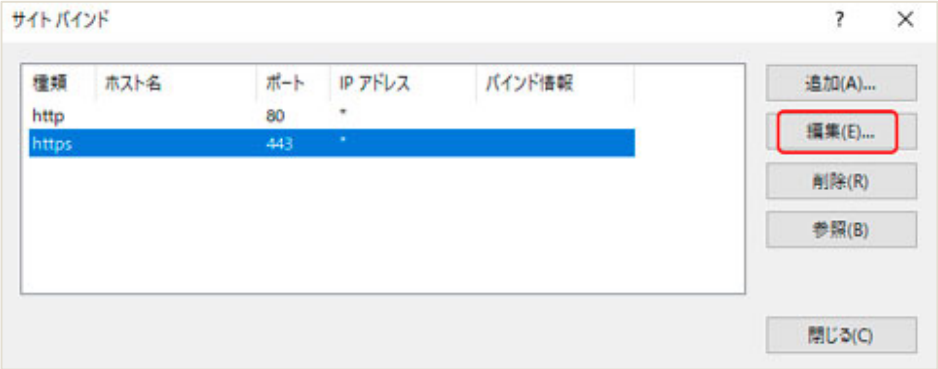
すでにご利用中のサーバー証明書を変更する場合

4.4 既存バインドの再設定

こちらは、すでに利用しているサーバー証明書を変更する場合の手順です。
バインドを初めて設定するとき(証明書の初導入)と、バインドを再設定するとき(証明書の再導入)で、手順が違いますので、ご注意ください。

4.4.1 インストールするバインドの択一

リスト・ボックスから証明書をインストールするバインドを択一します。［編集(E)...］ボタンが実行できるようになりますので、 ［編集(E)...］ボタンを実行します。

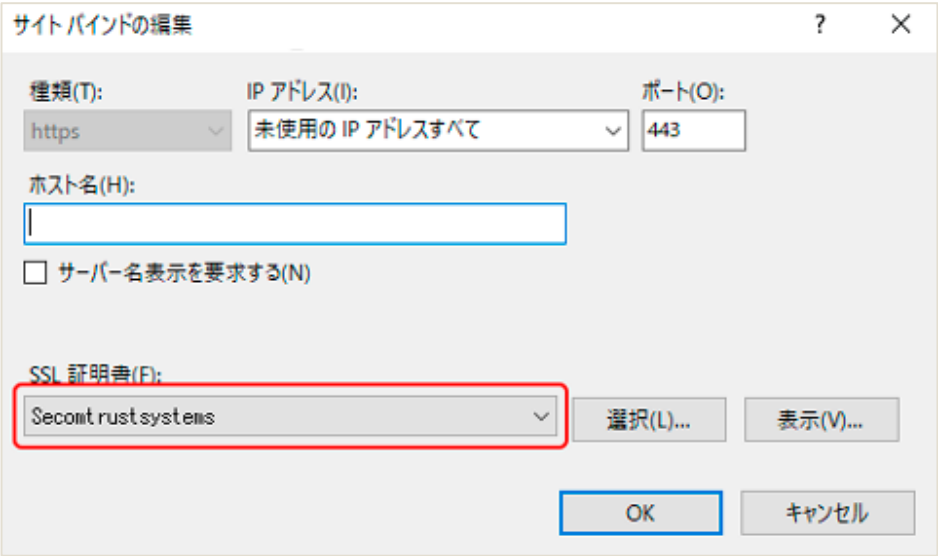


<サイト バインドの編集>ダイアログがポップアップします。

4.4.2 インストールする証明書の択一

［SSL 証明書(F)］プルダウン・リストから、サイトへ新しく設定する証明書を択一します。

Copyright© 2026 Japan Registry Services Co., Ltd.



［OK］ボタンを実行し、ダイアログを閉じます。

以上で証明書のインストール (再導入)は完了です。もしサーバーを起動していないときは［開始］を実行してください。

5 サーバー証明書および秘密鍵のバックアップ方法

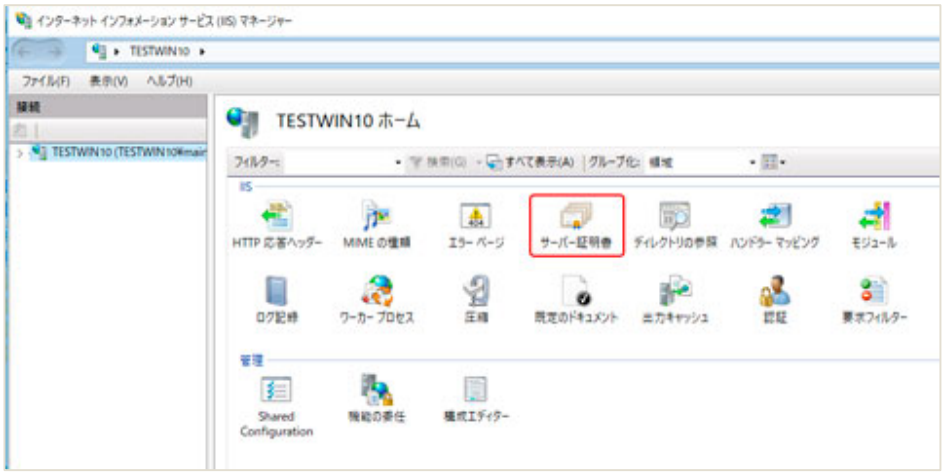
5.1 ［インターネット インフォメーション サービス (IIS) マネージャ］の実行

画面左下のスタートより、W の欄にある[Windows 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) マネージャー タイル］ を実行します。

5.2 ［サーバー証明書］アイコンの実行

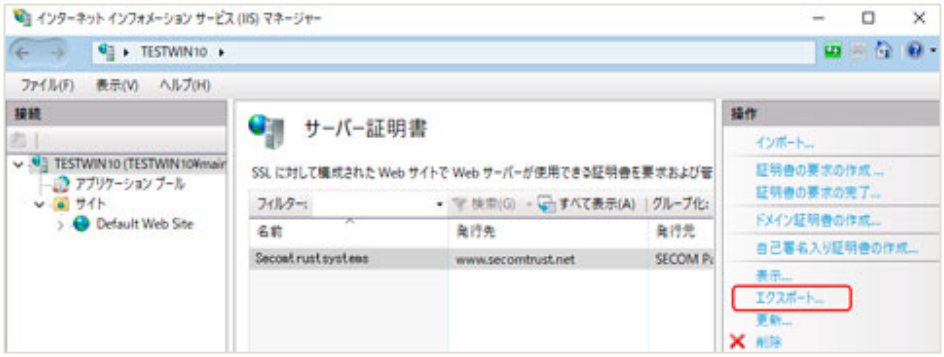
画面左の「接続」にあるサーバー名を選択し、画面中央にある ［サーバー証明書］アイコンを実行します。

Copyright© 2026 Japan Registry Services Co., Ltd.



5.3 バックアップをとる証明書の択一

画面の中央のリスト・ボックスから バックアップをとる証明書を択一します。 画面右の ［操作］ に ［エクスポート...］ が表示されますので、 ［エクスポート...］ を実行します。

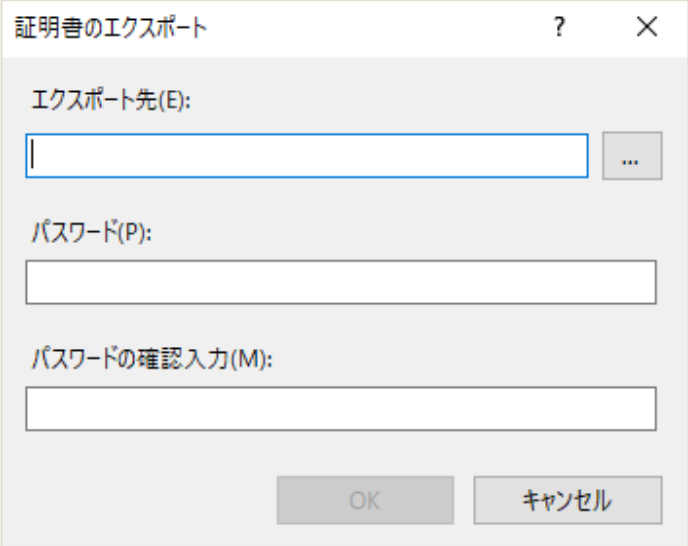


<証明書のエクスポート> ダイアログがポップアップします。

5.4 エクスポート先の指定

［エクスポート先(E)］と［パスワード(P)］［パスワードの確認入力(M)］を指定します。

Copyright© 2026 Japan Registry Services Co., Ltd.



5.5 エクスポートの完了

［OK］ボタンを実行し、ダイアログを閉じます。

以上でバックアップ作業は完了です。

決してパスワードを忘れないでください。

忘れると二度とバックアップファイルは使用できなくなります。

サーバー複数台でご利用されているお客様

※バックアップファイル (「.PFX」 ファイル) のインポート

この作業は、負荷分散で使用する別サーバーへ証明書のインポートを行う方法です。別のサーバーに証明書をインポートする必要があるお客様は、以下の作業を行ってください。

バックアップファイルを移動させてください。

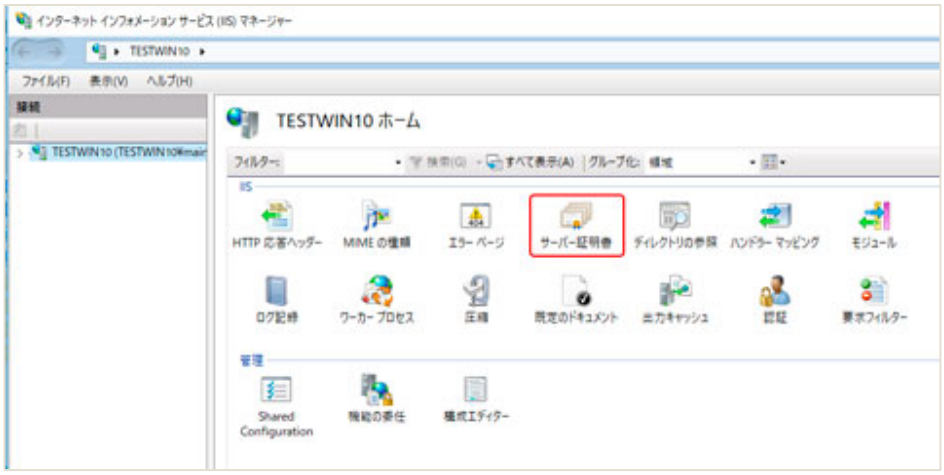
Copyright© 2026 Japan Registry Services Co., Ltd.

① ［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］ の実行

画面左下のスタートより、W の欄にある[Windows 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) マネージャー タイル］ を実行します。

② ［サーバー証明書］アイコンの実行

画面左の「接続」にあるサーバー名を選択し、画面中央にある ［サーバー証明書］アイコンを実行します。



③ インポートの実行

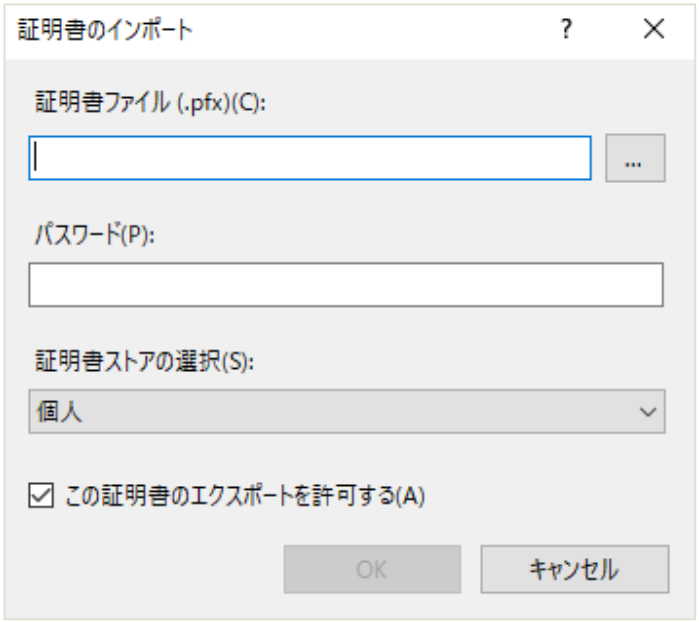
画面右の［操作］より、［インポート...］を実行します。

Copyright© 2026 Japan Registry Services Co., Ltd.

<証明書のインポート> ダイアログがポップアップします。

④ <証明書のインポート> ダイアログの表示

［証明書ファイル(.pfx)(C)］［パスワード(P)］を指定します。



⑤ インポートの完了

［OK］ボタンを実行してダイアログを閉じます。

以上でバックアップファイル (「.pfx」 ファイル) のインポート作業は完了です。

Copyright© 2026 Japan Registry Services Co., Ltd.