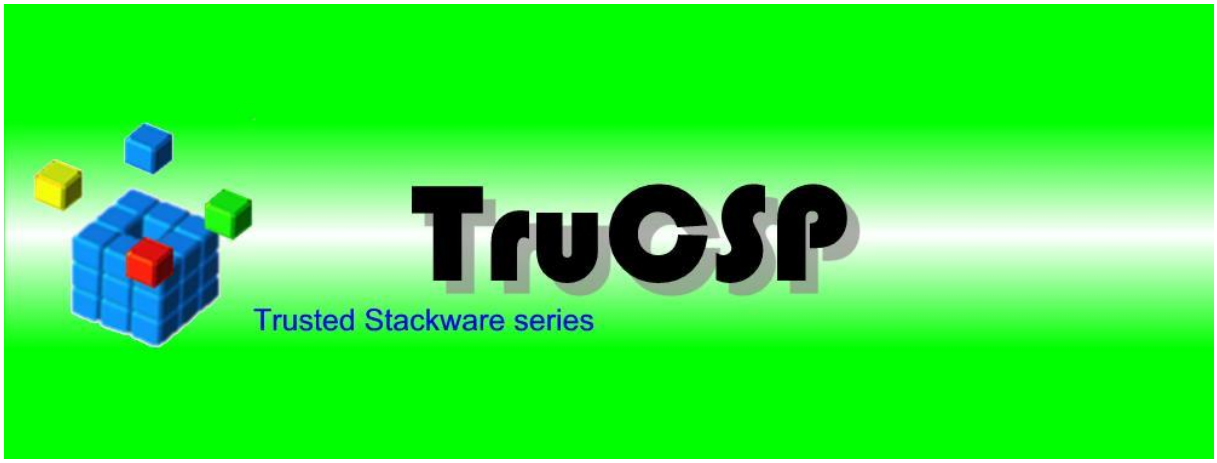
TruCSP

TruGate 用認証機能付き
Windows Cryptographic Provider

ユーザーズガイド

Rev. 1.0.4



有限会社ディーオーアイネット

免責事項

1） 本資料に掲載された内容に起因する直接的および間接的な損害またはその他の権利の侵害に関して当社は一切その責任を負わない。
2） 本資料によって第三者または当社の特許権その他の権利を承諾するものではない。
3） 本資料の一部または全部を当社に無断で転載複製する事を禁ずる。
4） 本資料に記載された仕様等は改良などの目的で予告なく変更する場合がある。

本資料に記載された会社名ならびに製品名は各社の商標もしくは登録商標です。
本製品を輸出する場合は外国為替及び外国貿易法並びに米国の輸出管理法規などの規制をご確認の上、必要な手続きをお取りください。

変更履歴

Rev.	発行年月日	修正内容
1.0.0	2012/04/17	初版。
1.0.1	2013/05/09	対応 OS に Windows 8、Windows Server 2012 を追記。 試用期間の変更。
1.0.2	2014/12/04	対応 OS から日本語版の表記を削除。
1.0.3	2015/07/21	対応 OS に Windows 10 を追記。
1.0.4	2023/10/27	対応 OS を変更。

目次

図表目次

1. はじめに

本ユーザーズガイドでは、ディーオーアイネット社製 TruCSP の取り扱い方法を説明します。

2. 動作環境について

a. 対応 OS

Windows 10 32bit/64bit

Windows 11

Windows Server 2016

Windows Server 2019

b. 対応認証フレームワーク

TruGate ver.5.0.10 以上

c. 利用可能な認証デバイス

TruGate に依存します。詳細は、TruGate のユーザーズガイドをご参照ください。

d. 必要なデバイスプラグイン

TruGate に依存します。詳細は、TruGate のユーザーズガイドをご参照ください。

e. インストール要件

TruGate がインストールされている事。

f. 動作要件

TruGate がインストールされており、認証に利用出来るように初期設定されている事。「TruStack Gina の有効化」は任意ですが、利用する認証デバイスのテンプレートを必ず登録してください。詳細は、TruGate のユーザーズガイドをご参照ください。

3. 製品概要

a. 製品機能

TruCSP は、証明書格納プロバイダーである TruStack Certificate Store Provider（以下 TSCert と呼称）、ならびに暗号サービスプロバイダーである TruStack Cryptographic Service Provider（以下 TSCSP と呼称）の 2 つのモジュールで構成されています。

TSCert は、Microsoft CryptoAPI が備える証明書格納関数の拡張を行うものであり、ディーオーアイネット社が提供する認証フレームワーク製品 TruGate と連動し、証明書へのアクセスに認証機能を追加するものです。

TSCSP は、Microsoft CryptoSPI（System Program Interface）準拠の API を備え、Microsoft

CSP 規格に則った暗号サービスを提供すると共に、TSCert 同様に、ディーオーアイネット社が提供する認証フレームワーク製品 TruGate と連動し、公開/秘密鍵ペアの格納先へのアクセスに認証機能を追加するものです。

注）TSCert ならびに TSCSP は、認証フレームワークとして TruGate を利用します。ご利用には TruGate を別途ご用意ください。

b. パッケージ

インストーラパッケージにはシングルライセンス版とボリュームライセンス版の 2 種類があります。

i. シングルライセンス版

主に個人ユーザー向けの製品パッケージです。exe インストーラパッケージで提供されます。試用期間は 1 ヶ月です。試用期間中の機能制限はありません。

ii. ボリュームライセンス版

主に企業ユーザー向けの製品パッケージです。msi インストーラパッケージで提供されます。また、インストールされた PC 上の OS の「アプリと機能」からは削除できません。削除は Active Directory サーバーもしくは msi インストーラを再起動して実施します。32bit 版と 64bit 版があり、試用期間は 3 ヶ月です。試用期間中の機能制限はありません。

4. 制限および注意事項

1. TSCert が格納可能な証明書の最大サイズは、エンコード後サイズで 2KB 弱です。
2. TSCert は複数の証明書を格納できません。単一の証明書の新規書込みもしくは書替えのみ可能です。
3. TSCert では、証明書失効リストおよび証明書信頼リストは、TSCert の格納域に格納できません。
4. OS の「証明書のインポートウィザード」を用いて、既存の証明書を TSCert ストアにインポートする場合、[証明書の種類に基づいて、自動的に証明書ストアを選択する]を選択してください。
5. TSCSP では、格納可能な公開鍵の最大長は、1024 ビットまでです。
6. TSCSP では、複数の鍵ペアを格納することはできません。単一の鍵ペアの新規書込みもしくは削除のみ可能です。

5. インストールとアンインストール手順

注）インストールする前に、TruCSP のインストール要件をご確認ください。インストール及びアンインストールは、ローカルコンピュータの管理者権限でログオンして行ってください。

a. インストール

TruCSP Trusted Stackware Crypto Service Provider.exe を実行すると下記に示す画面が表

示されますので「次へ」ボタンをクリックしてください。

図 1 セットアップウィザード起動画面

次に、使用許諾契約画面が表示されますので、画面中の「ソフトウェア使用許諾契約書」をよくお読みになった上、ご同意頂ける場合のみ「使用許諾契約書のすべての条項に同意します」ラジオボタンをチェックし、「次へ」ボタンをクリックしてください。

図 2 使用許諾契約画面

次に、セットアップタイプの選択画面が表示されたら、利用環境に応じて選択してください。

図 3 セットアップタイプの選択画面

次に、インストール準備完了画面が表示されますので、ここまでの操作で変更の必要が無い場合は、「インストール」ボタンをクリックしてください。変更したい場合は、「戻る」ボタンをクリックし、変更を希望する画面まで戻って、やり直してください。

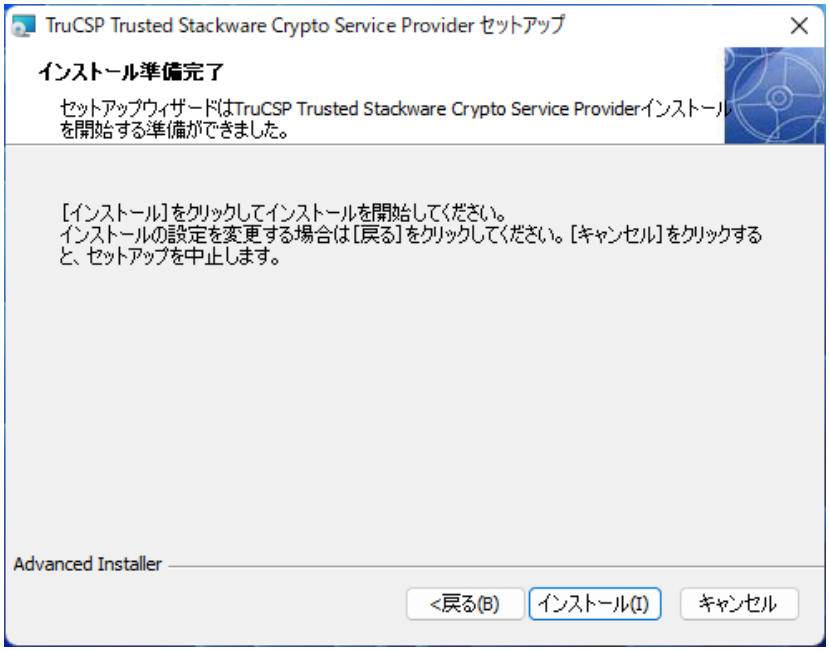


図 4 インストール準備完了画面

インストール中は、下記に示すインジケータ画面が表示されます。

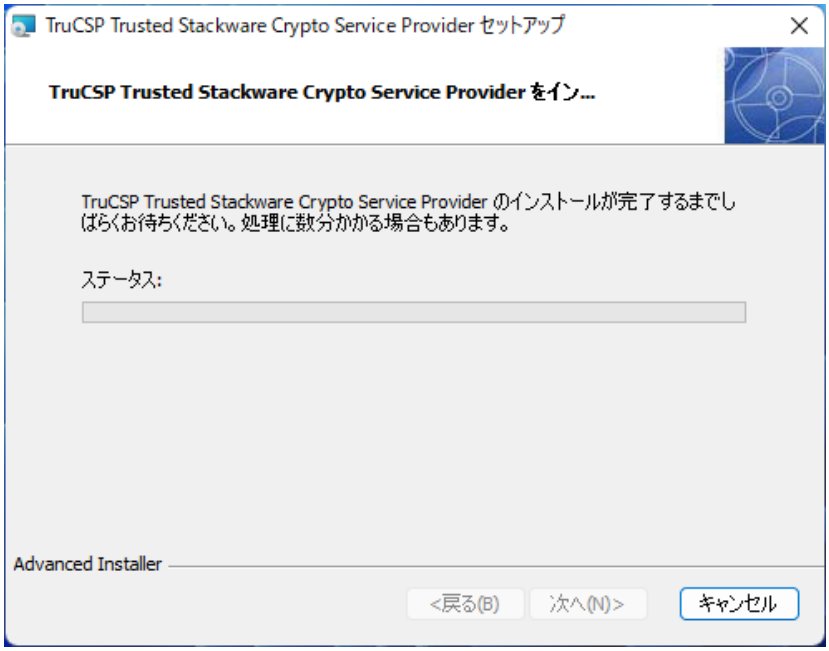


図 5 インストールインジケータ画面

インストールが終了すると、下記に示すインストール完了画面が表示されますので、「完了」ボタンをクリックしてください。

図 6 インストール完了画面

b. アンインストール

OS の「アプリと機能」から TruCSP Trusted Stackware Crypto Service Provider を選択してく

ださい。

以下は、Windows 11 での操作例です。

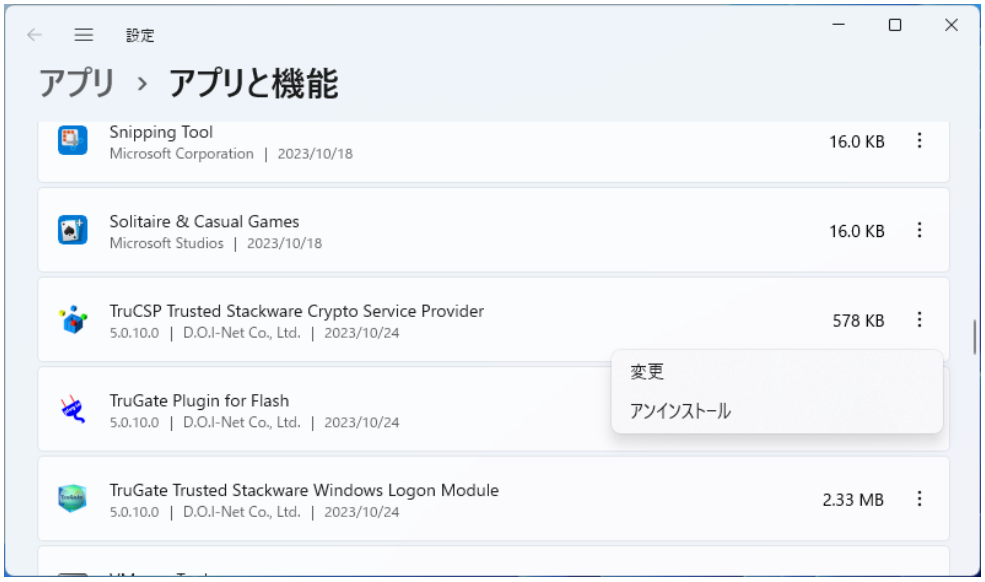


図 7 アプリと機能画面

アンインストールをクリックし、メッセージに従って TruCSP のアンインストールを行ってください。

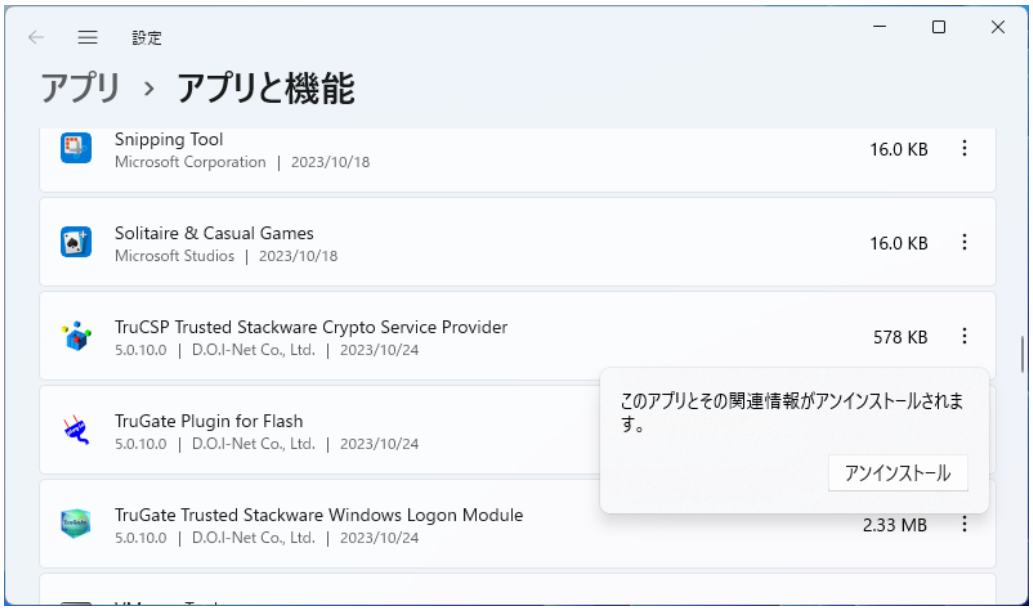


図 8 アンインストール確認画面

アンインストール中は、下記に示すインジケータ画面が表示されます。

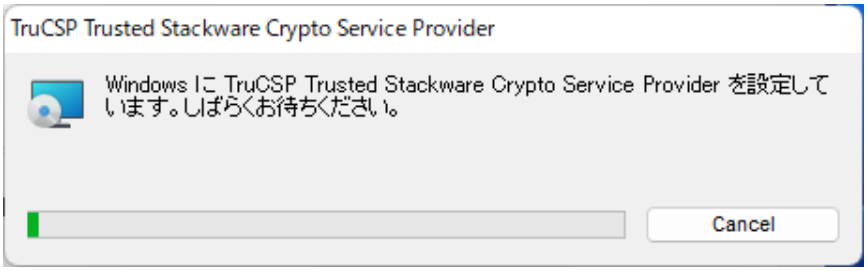


図 9 アンインストールインジケータ画面

アンインストールが終了すると、インジケータ画面が消えます。

6. 操作方法

a. ライセンスの検証

試用期間中の場合、下記に示す様なポップアップメッセージが表示されます。メッセージが表示された場合は、「OK」ボタンをクリックしてください。

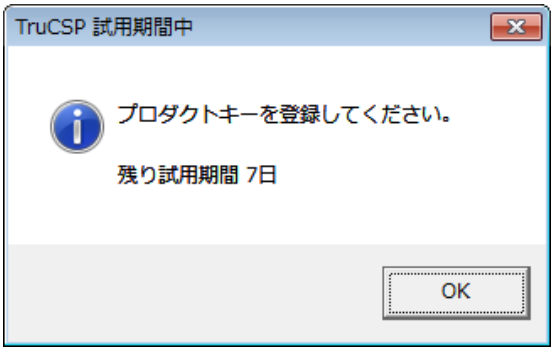


図 10 試用期間中注意画面

注） シングルライセンス版の試用期間は１ヶ月、ボリュームライセンス版の試用期間は３ヶ月です。インストール後、試用期間を経過すると使用できなくなります。引き続き使用する場合は、製品登録を行ってください。

試用期間が過ぎた場合は、下記に示す様なダイアログボックスが表示されます。継続して使用する場合は、プロダクトキーをエディットボックスに入力した後、「OK」ボタンをクリックしてください。試用を終了する場合は「キャンセル」ボタンをクリックし、TruCSP をアンインストールしてください。

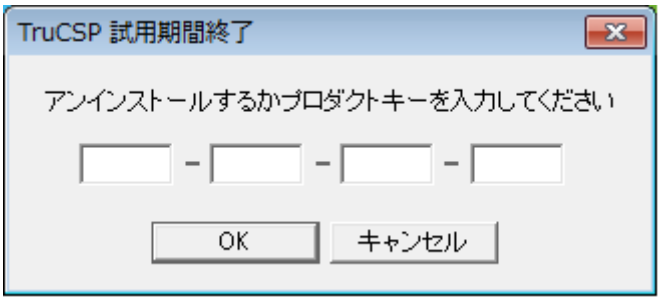


図 11 試用期間終了注意画面

b. TruCSP の証明書ストアコレクションへの登録状況の確認方法

1. TruCSP のインストール後にシステムをリブートし、TruGate にてログオンするか、TruStack Gina を有効化していない場合は認証デバイスを利用可能にしてください。
2. MMC を起動し、作成済みの証明書コンソールファイルを開き、証明書コンソールを起動します。

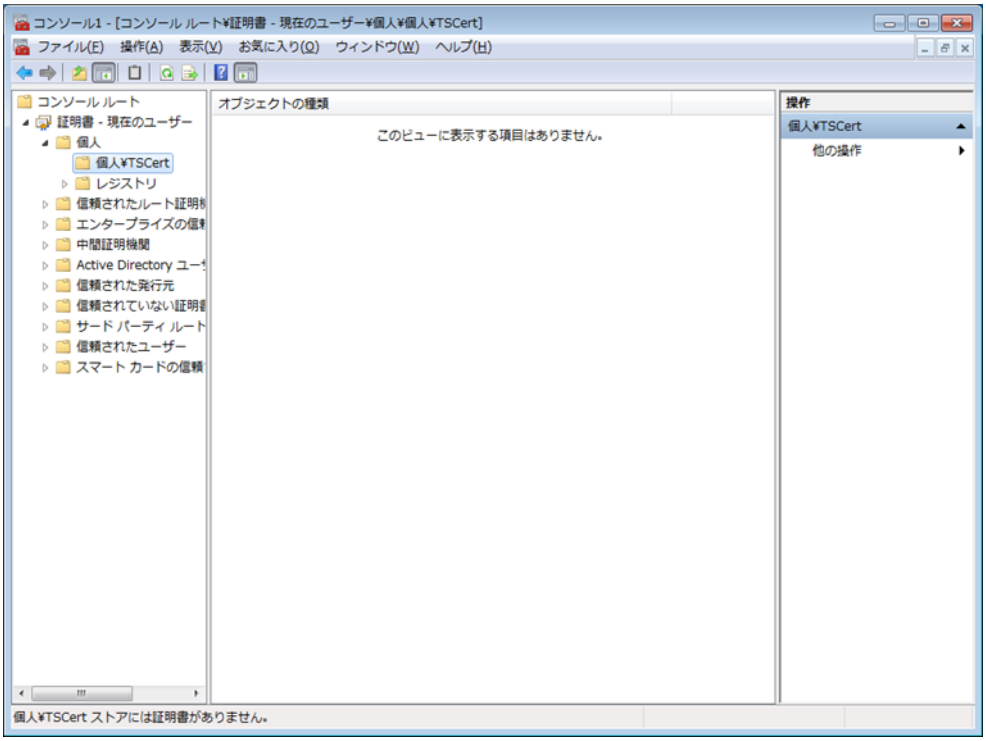


図 12 証明書コンソールの起動

証明書コンソールをまだ作成していない場合は、下記手順に従って作成します。

(ア)「スタート」を右クリックした後、「ファイル名を指定して実行」をクリックします。

(イ)「ファイル名を指定して実行」ダイアログボックスが表示されたら、mmc と入力し「OK」ボタンをクリックします。

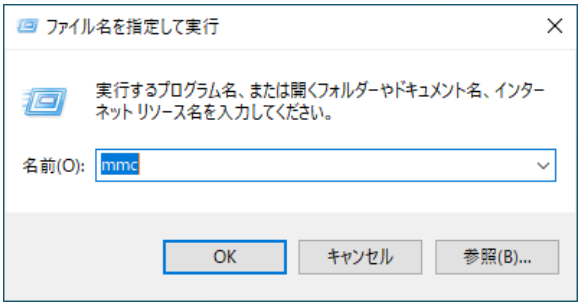


図 13 mmc 実行画面

(ウ) コンソール画面が表示されます。

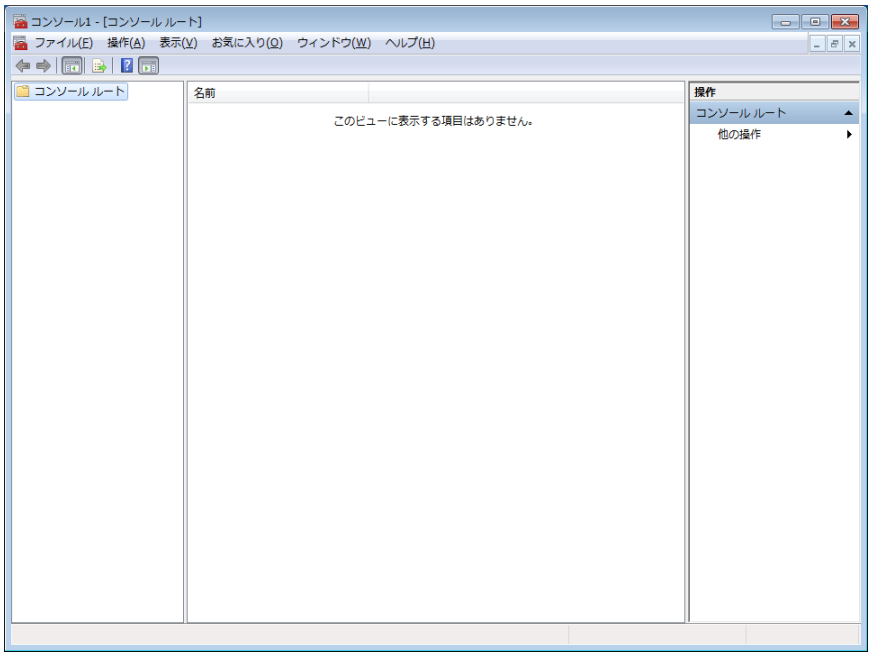


図 14 コンソール起動画面

(エ) コンソール画面から、「ファイル」ー「スナップインの追加と削除」を選択します。

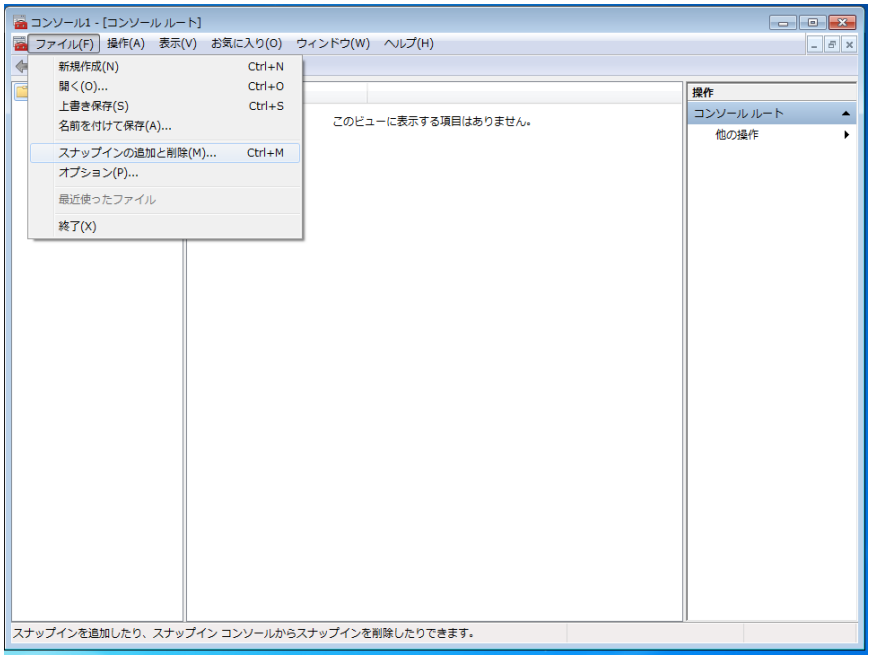


図 15 スナップインの追加と削除選択画面

(オ) スナップインの追加と削除画面が表示されたら、利用できるスナップインから「証明書」を選択し、「追加」ボタンをクリックします。

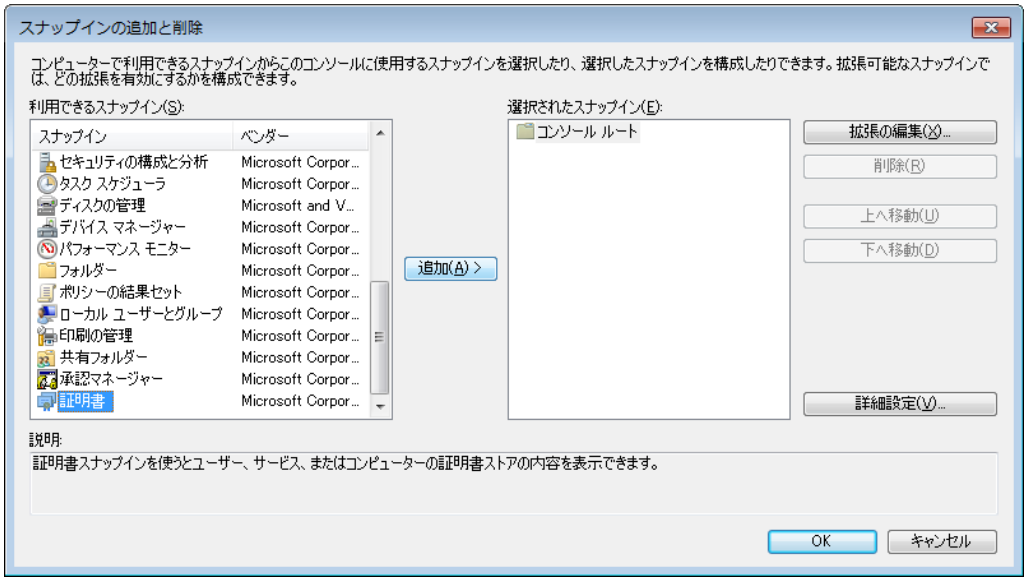


図 16 スナップインの追加と削除起動画面

(カ) 証明書スナップイン画面が表示されたら、「ユーザー アカウント」ラジオボタンを選択し、「完了」ボタンをクリックします。

図 17 証明書スナップイン起動画面

(キ) スナップインの追加と削除画面に戻ったら、「OK」ボタンをクリックし、スナップインの追加と削除画面を閉じます。

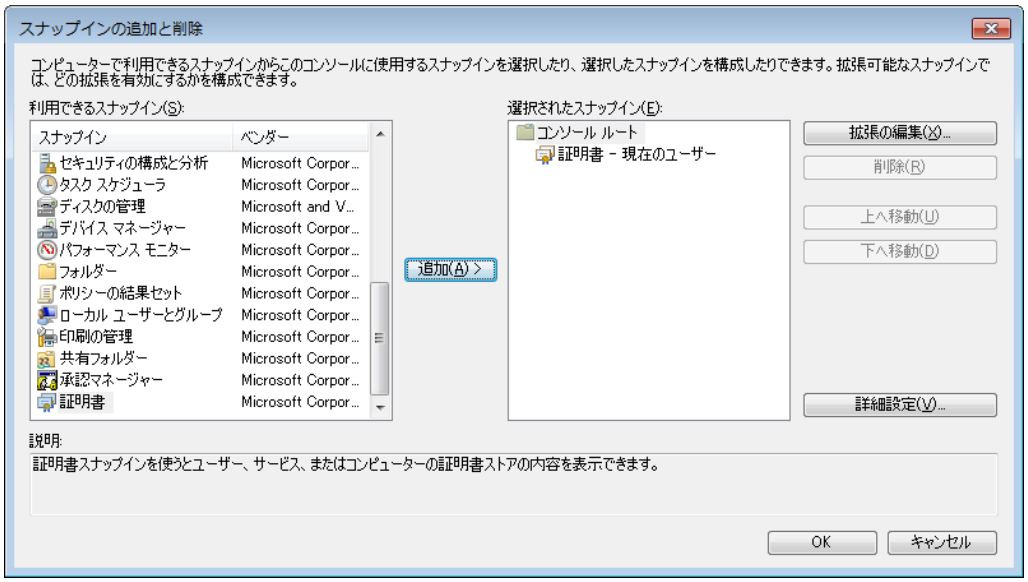


図 18 スナップインの追加と削除終了画面

(ク) コンソール画面に戻ったら、「ファイル」ー「名前を付けて保存」を選択します。

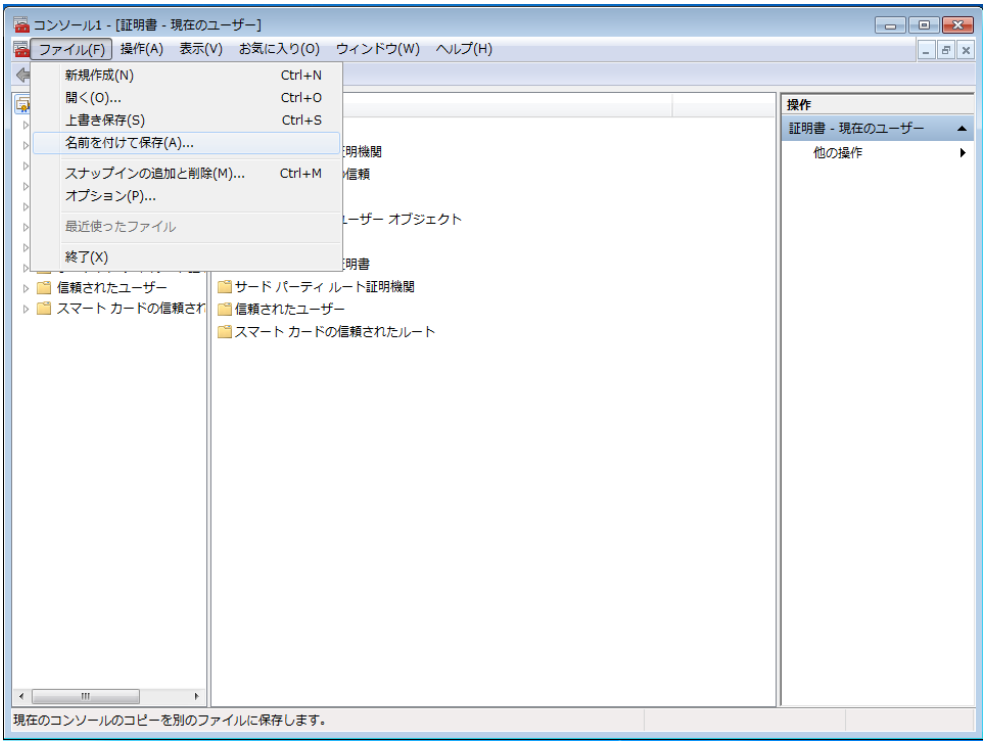


図 19 コンソール画面 ― 名前を付けて保存

(ケ) 名前を付けて保存画面が表示されたら、ファイル名に「証明書」とタイプし、「保存」ボタンをクリックします。

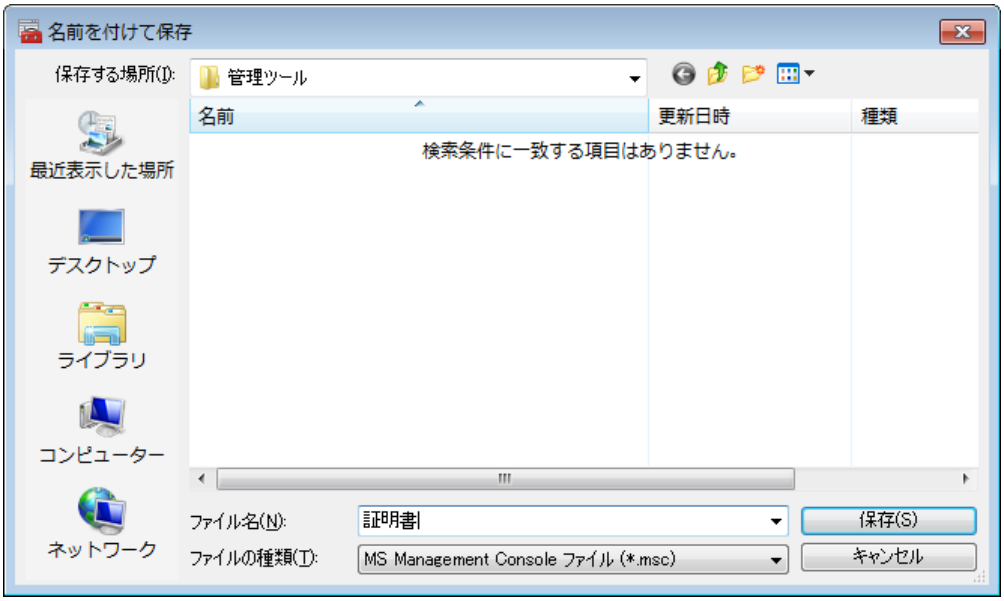


図 20 名前を付けて保存画面

3. 証明書コンソール画面が表示されたら、証明書の上でマウスを右クリックし、「表示」―「オプション」を選択します。

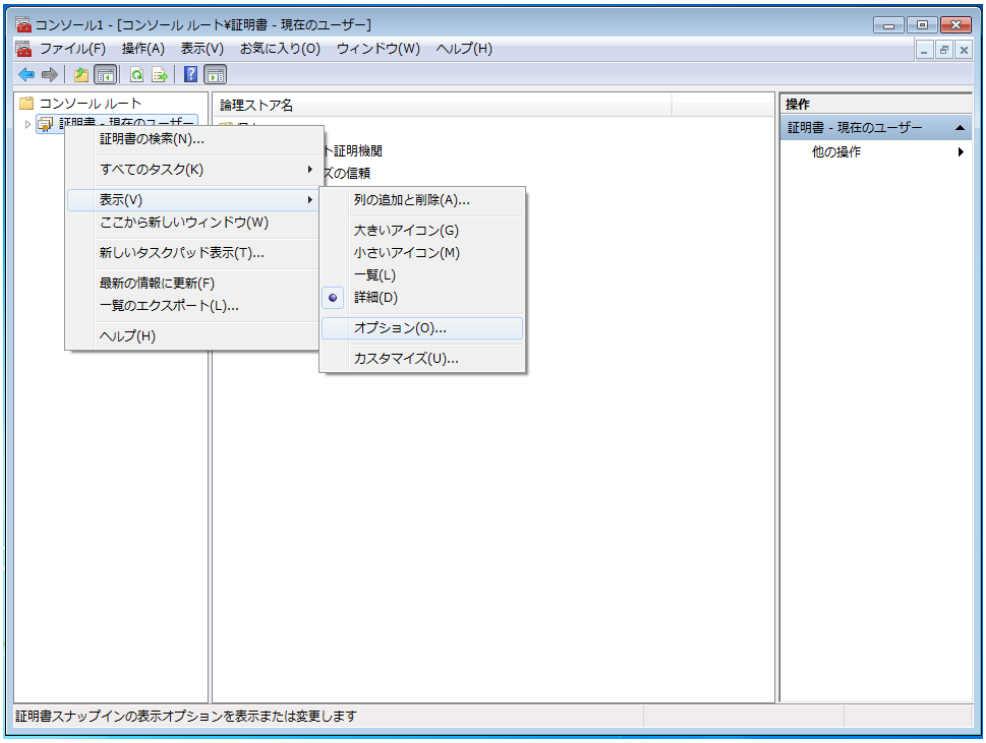


図 21 表示オプションの選択画面

4. 表示のオプション画面が表示されたら、「表示モードの分類」の「論理証明書ストア」ラジオボタンをオンにし、「物理証明書ストア」チェックボックスにチェックを入れ、「OK」ボタンをクリックします。

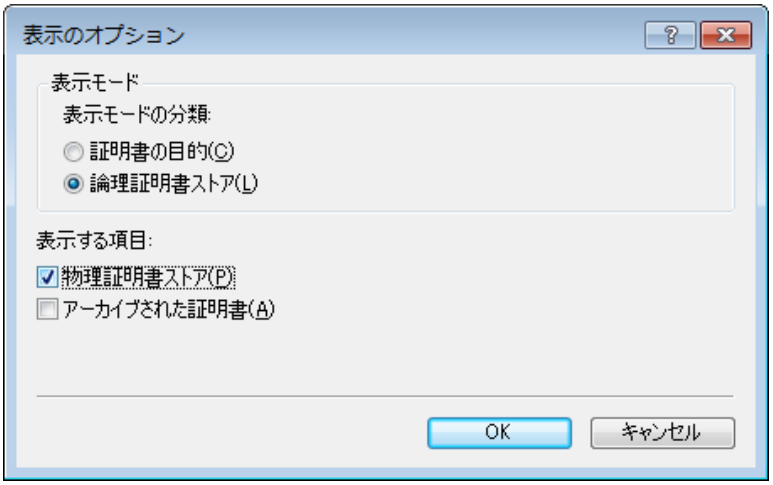


図 22 表示のオプション起動画面

5. コンソール画面に戻り、左側ペインの「個人」ツリー下に TruCSP が表示されていれば、正常に登録されたものと判断されます。

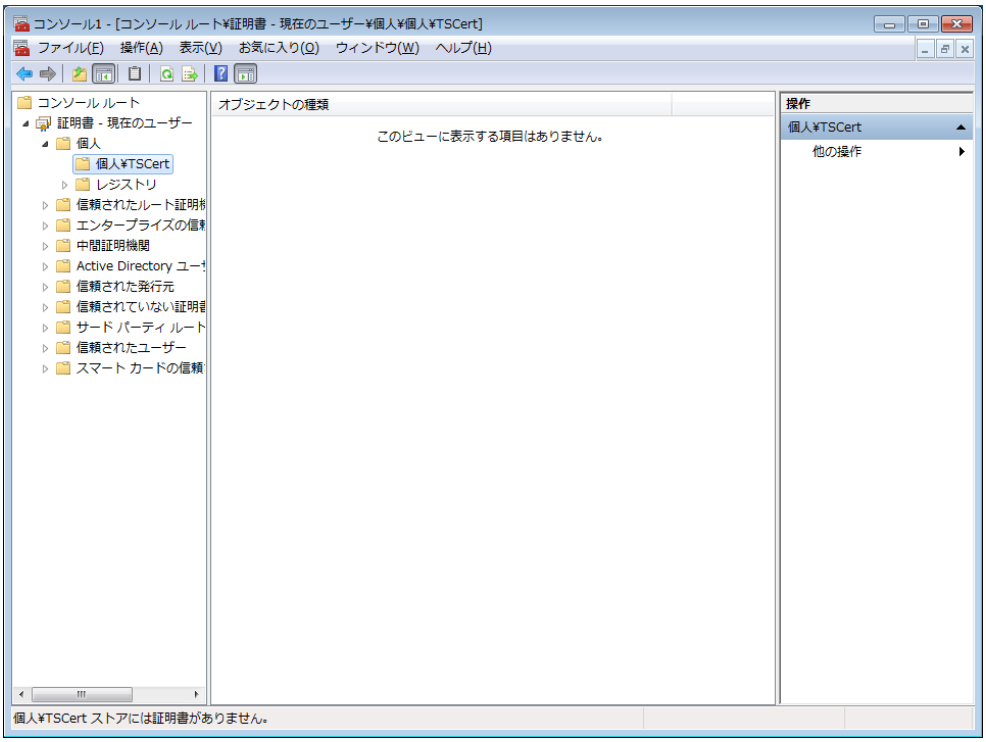


図 23 コンソール画面 ― TruCSP 追加

c. TruCSP による証明書の取得

i. 商用 CA からの取得例

以下に、VeriSign の Digital ID Services を使用し、個人用電子証明書を TruCSP に格納する例を示します。

1. TruGate にてログオンするか、TruStack Gina を有効化していない場合は認証デバイスを利用可能にしてください。
2. Web ブラウザを起動し、VeriSign の Digital ID Services 申請サイトにアクセスします。

図 24 VeriSign 個人用電子証明書申請サイト

3. 「申請する」ボタンをクリックすると、下記のような Web ブラウザを選択するページが表示されますので、電子証明書を利用する Web ブラウザを選択してください。この例では、Microsoft Internet Explorer を選択します。

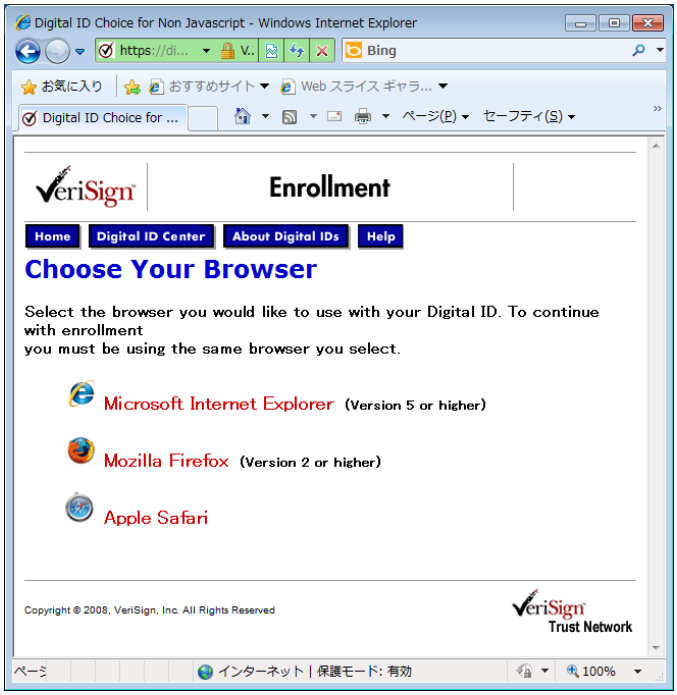


図 25 Web ブラウザ選択ページ

4. Microsoft Internet Explorer を選択した後、下記のような画面が表示された場合は、「はい」ボタンをクリックして続行してください。

図 26 証明書の代理要求確認画面

5. Web ブラウザを選択すると、下記のような申請書式ページが表示されます。画面中の設問に従い書式を埋めていきます。

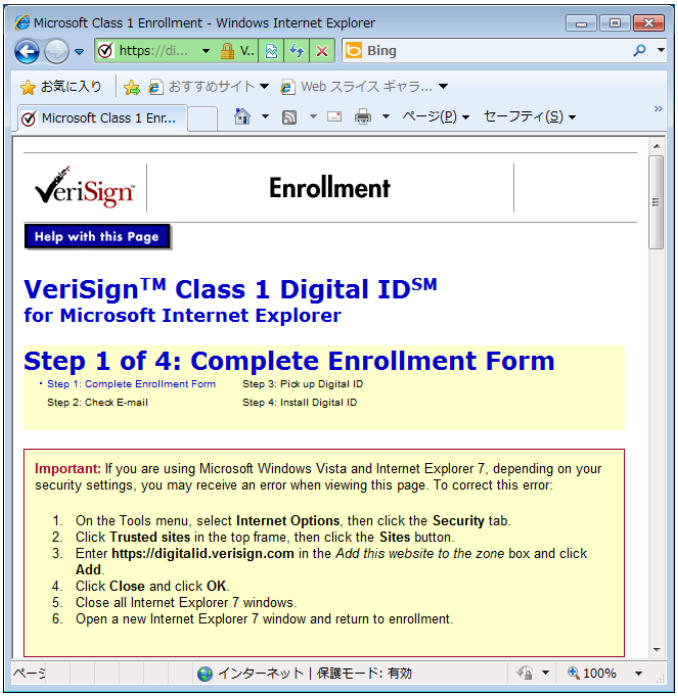


図 27 電子証明書申請書式ページ

6. 先ず初めに、電子証明書に含める名、姓、電子メールアドレスを夫々入力します。

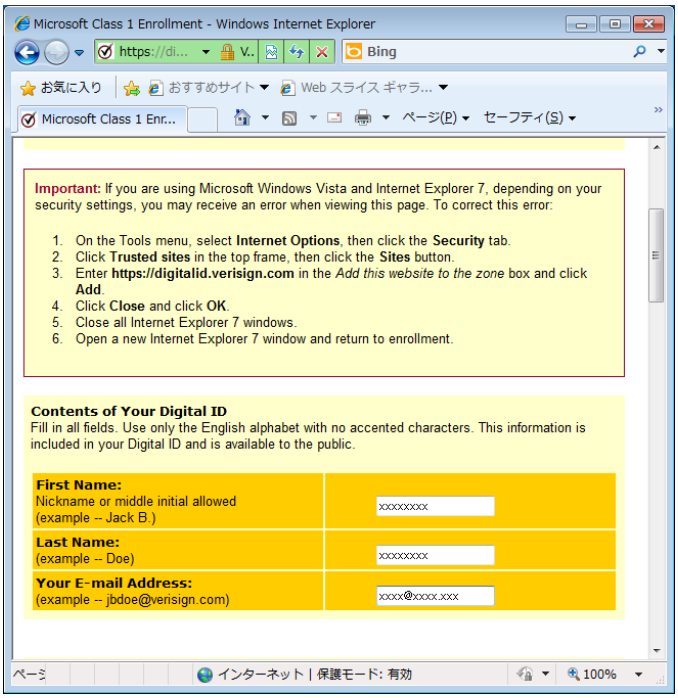


図 28 電子証明書に含める内容の入力

7. 次に、電子証明書の再発行などの認証時に利用する、チャレンジフレーズを入力します。

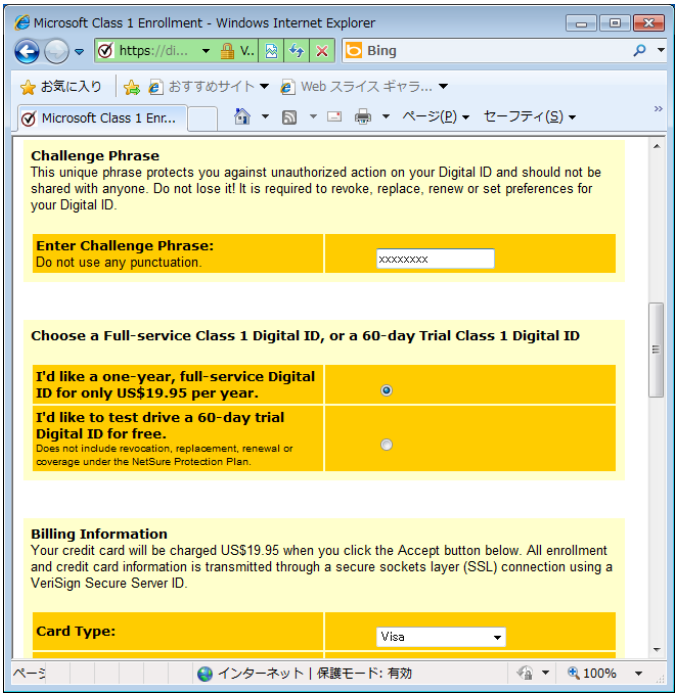


図 29 チャレンジフレーズの入力

8. 次に、取得する電子証明書の種類を選択します。1 年間有効な有償の電子証明書か 60 日間有効な無償の評価用電子証明書の何れかを選択できます。初めて電子証明書を利用する場合は、評価用電子証明書を取得して試されることをお勧めします。

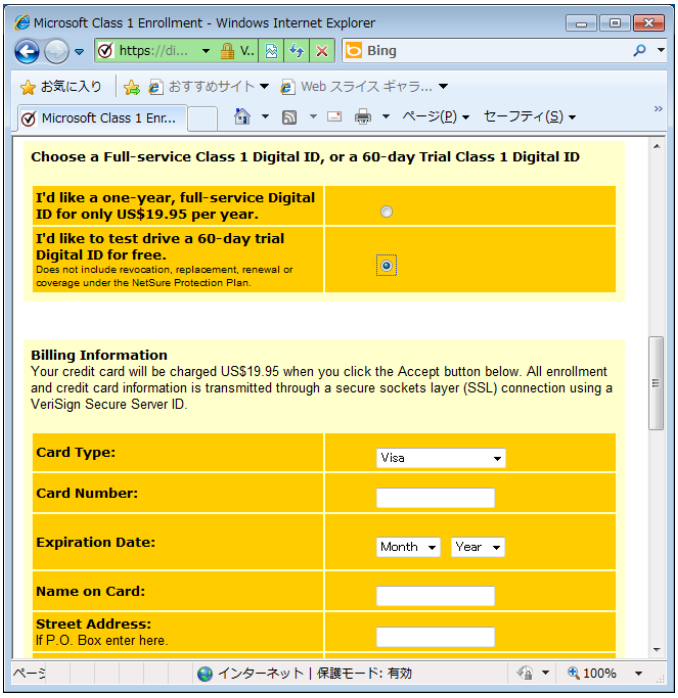


図 30 電子証明書の選択

9. 次に、前述の電子証明書の選択で有償の電子証明書を選択した場合のクレジットカード支払い情報を入力します。前述の選択時に無償の評価用電子証明書を選択した場合、この項目の入力は不要です。

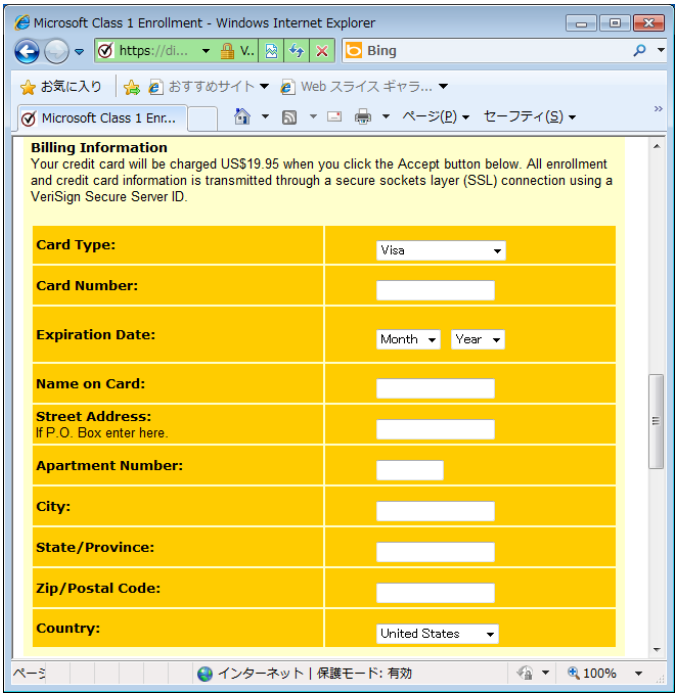


図 31 クレジットカード支払い情報の入力

10. 次に、利用する暗号サービスプロバイダーの選択画面に移行したら、ドロップダウンリストから「TruStack Cryptographic Provider v1.0」を選択してください。

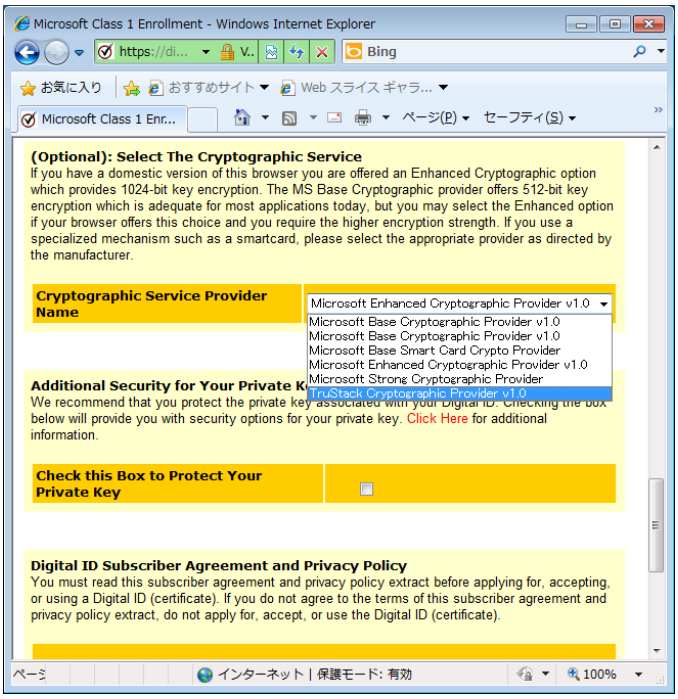


図 32 暗号サービスプロバイダーの選択

11. 次に、「秘密キーを保護する」チェックボックスをチェックしてください。
注）本例では「キーの長さ」の設定項目がありませんが、他社の CA サービス等で「キーの長さ」を設定する項目がありましたら、必ず 1024 以下を設定してください。

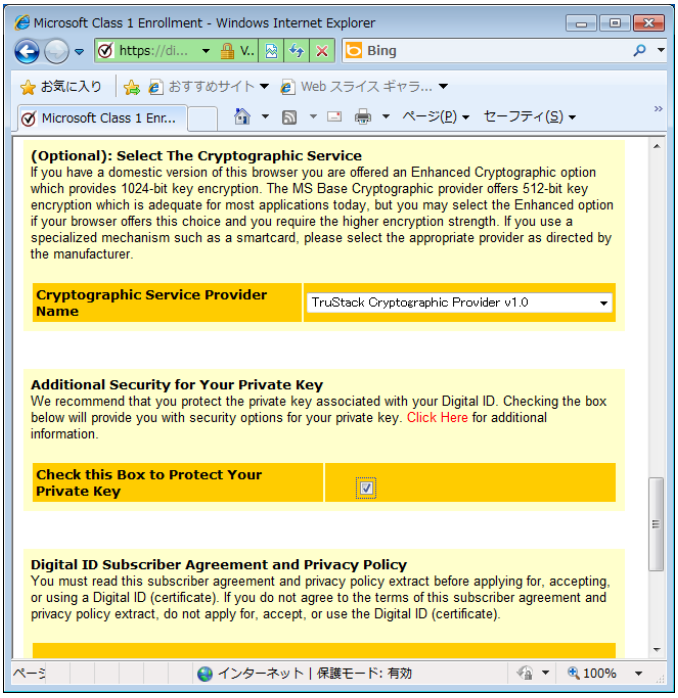


図 33 秘密キーを保護する

12. 申請書式ページの最後に Digital ID Subscriber Agreement and Privacy Policy が記載されていますので、内容をよく読み、同意できる場合は「Accept」ボタンをクリックします。

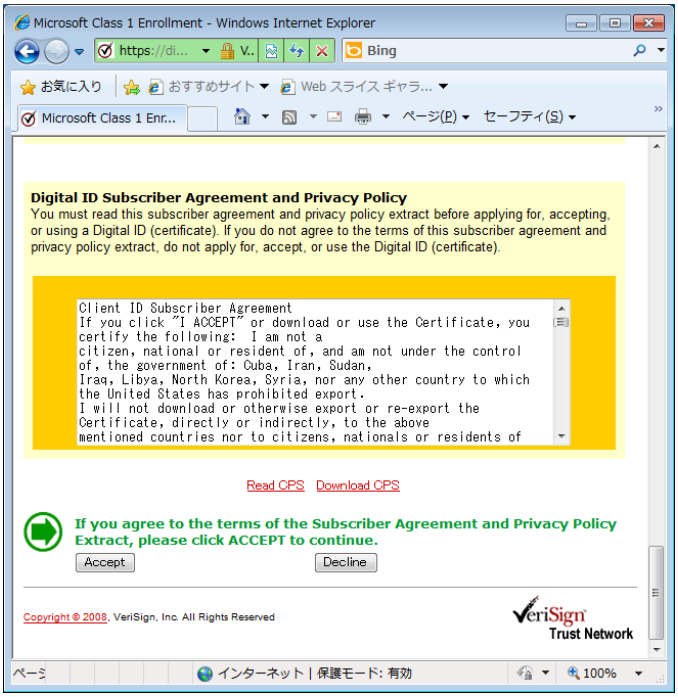


図 34 Digital ID Subscriber Agreement and Privacy Policy

13. 「Accept」ボタンをクリックすると、下記に示すような電子メールの確認画面が表示されます。電子メールが正しい場合は、「OK」ボタンをクリックしてください。正しくない場合は「キャンセル」ボタンをクリックし、申請書式ページに戻って訂正してください。

図 35 電子証明書の電子メールアドレス確認画面

14. もし、認証デバイスが利用できない状態だったり、認証デバイスの格納域に既に別の証明書及び公開/秘密鍵ペアが登録されていた場合、下記のようなエラー画面が表示されます。

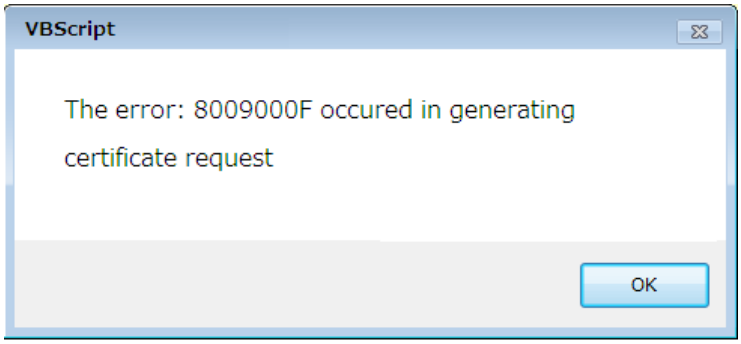


図 36 電子証明書申請エラー画面

15. 上記の様なエラーが発生した場合、「OK」ボタンをクリックすると、下記のようなエラーの原因例ページが表示されます。

注）エラーが発生した場合は、認証デバイスの状態を確認し、認証デバイスの接続や格納域の初期化などの作業（証明書要求エラー/インポートエラー発生時の対処方法を参照）を行った上で、再度、電子証明書の申請を行ってください。

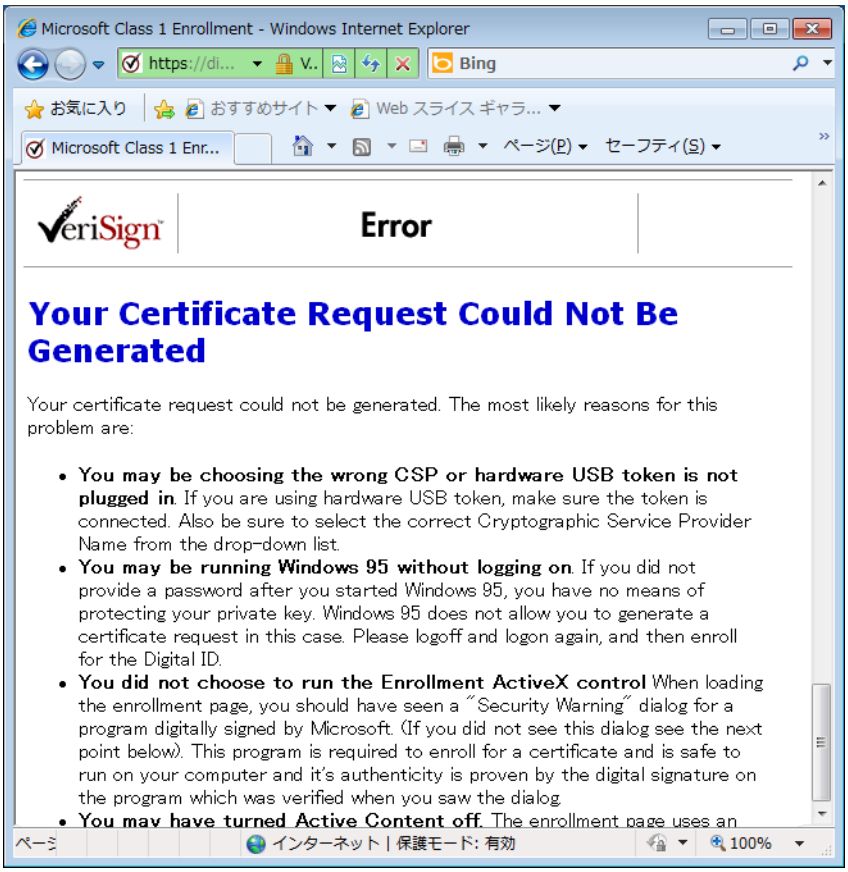


図 37 電子証明書申請エラーの原因例ページ

16. 電子証明書の申請が正常に行われた場合、下記のような電子メールの確認ページに移行します。

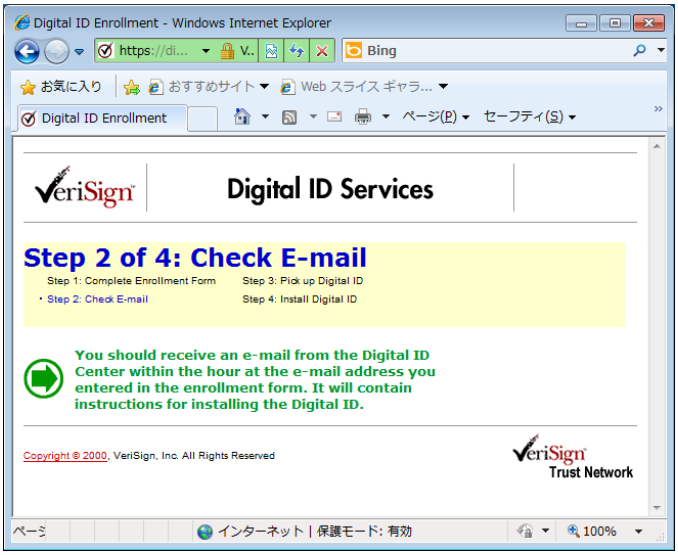
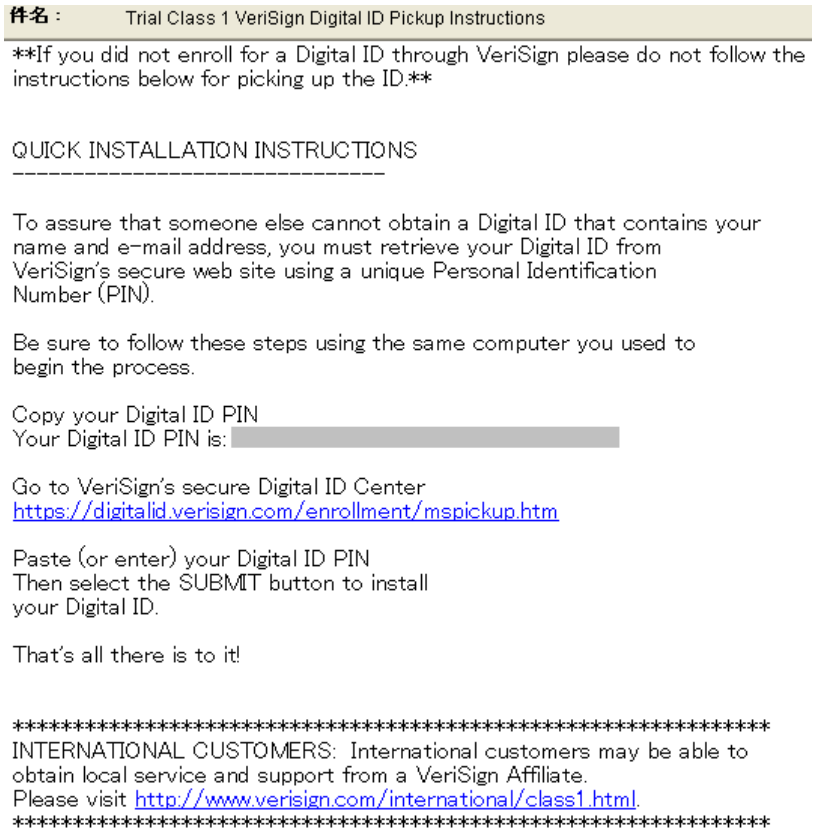


図 38 電子メールの確認を促すページ

17. 上記画面が表示されたら、暫く経ってからメーラーを起動し、VeriSign からの電子メ

ールを確認します。電子証明書の申請が正常に受理されると、下記に示すようなメールが VeriSign から送付されてきます。



件名： Trial Class 1 VeriSign Digital ID Pickup Instructions

If you did not enroll for a Digital ID through VeriSign please do not follow the instructions below for picking up the ID.

QUICK INSTALLATION INSTRUCTIONS

To assure that someone else cannot obtain a Digital ID that contains your name and e-mail address, you must retrieve your Digital ID from VeriSign's secure web site using a unique Personal Identification Number (PIN).

Be sure to follow these steps using the same computer you used to begin the process.

Copy your Digital ID PIN
Your Digital ID PIN is:

Go to VeriSign's secure Digital ID Center
https://digitalid.verisign.com/enrollment/mspickup.htm

Paste (or enter) your Digital ID PIN
Then select the SUBMIT button to install
your Digital ID.

That's all there is to it!

****
INTERNATIONAL CUSTOMERS: International customers may be able to obtain local service and support from a VeriSign Affiliate.
Please visit http://www.verisign.com/international/class1.html.
****

図 39 VeriSign からの電子証明書申請受理メール

18. 次に、上記メール中に示される Digital ID Center へのリンクをクリックします。下記に示す Pick up Digital ID ページが表示されたら、メール中の Digital ID PIN を、ページ中の「Digital ID Personal Identification Number（PIN）:」にコピー&ペーストし、「Submit」ボタンをクリックしてください。

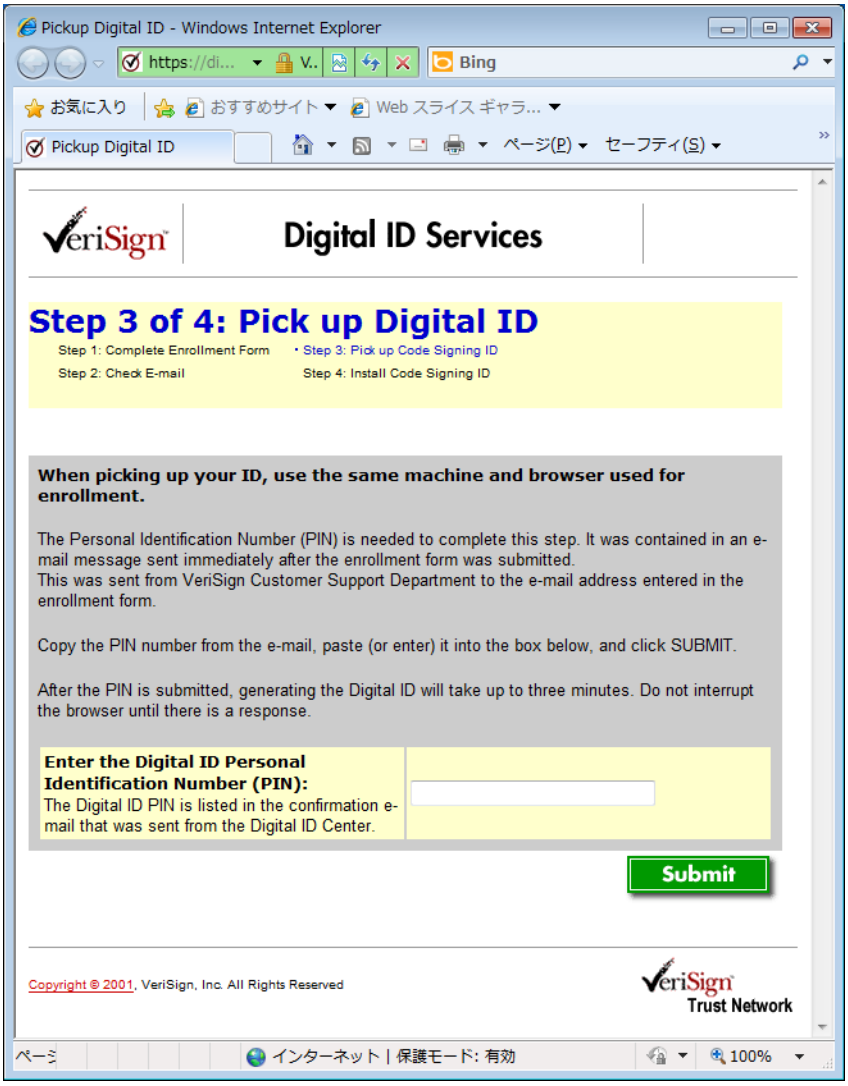


図 40 Digital ID Personal Identification Number（PIN）の入力

19. Digital ID が正常に生成されると、下記に示す Install Digital ID ページが表示されます。表示内容を確認し、正しければ「Install」ボタンをクリックしてインストールします。

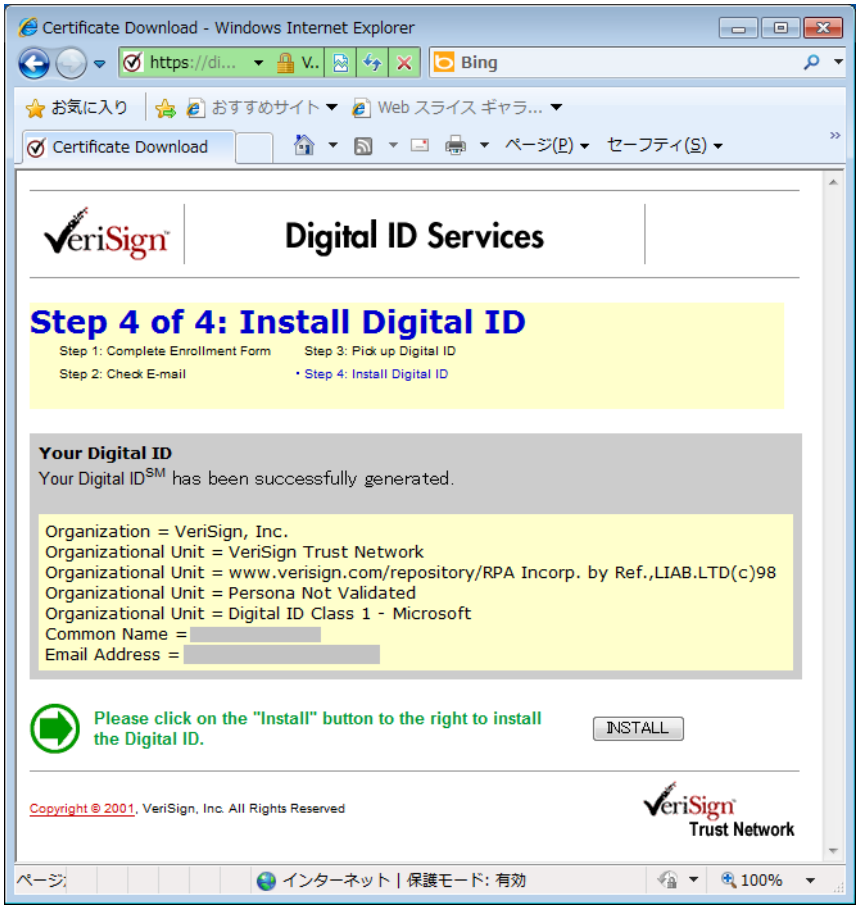


図 41 Install Digital ID ページ

20. 「Install」ボタンをクリックした後、下記のような画面が表示された場合は、「はい」ボタンをクリックして続行してください。

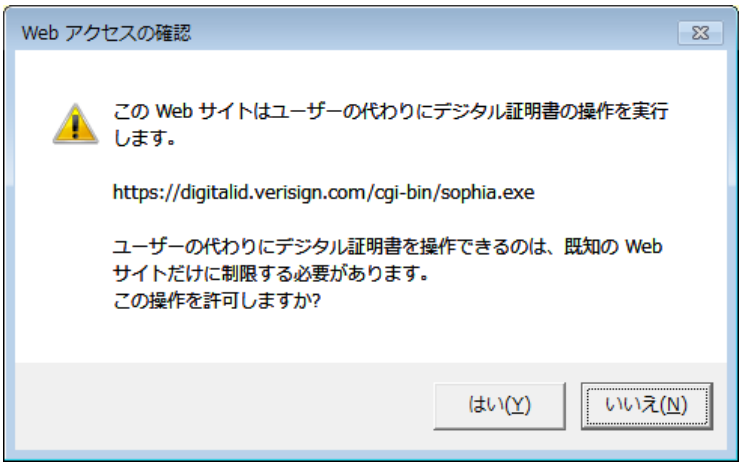


図 42 証明書の追加確認画面

21. デバイス認証画面が表示された場合は、デバイス認証を行ってください。
22. 電子証明書のインストールが正常に行われると、下記に示す電子証明書の利用設

定ページが表示されます。

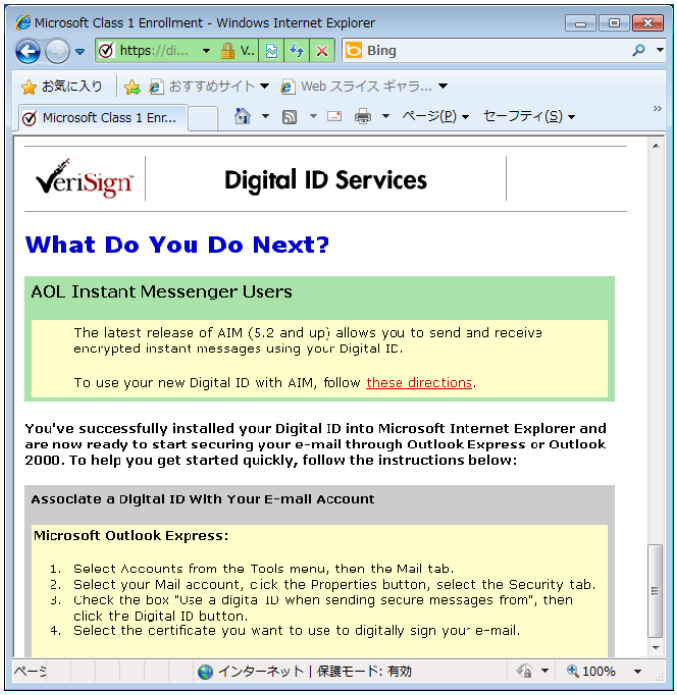


図 43 電子証明書利用設定ページ

23. インストールされた電子証明書を確認するため、Internet Explorer のメニューバーから「ツール」ー「インターネット オプション」を選択します。

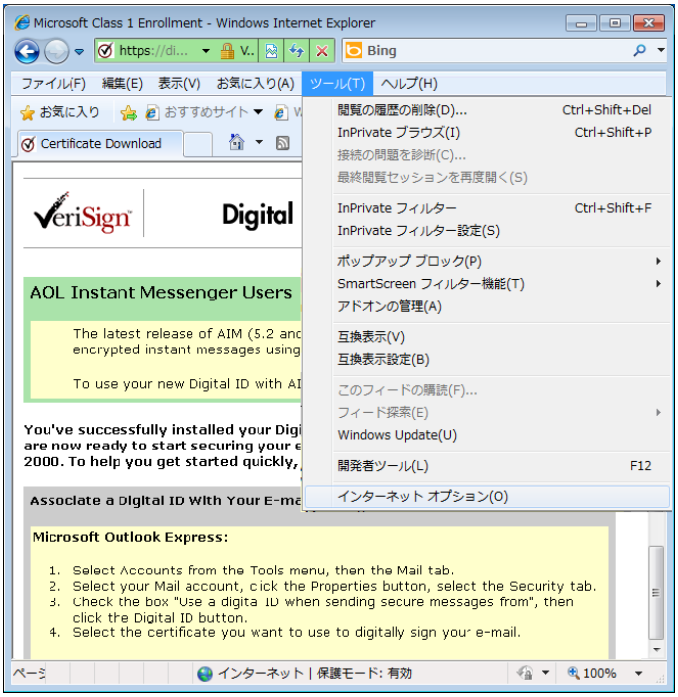


図 44 インターネットオプションの起動

24. インターネットオプション画面が表示されたら、「コンテンツ」タブを選択してください。

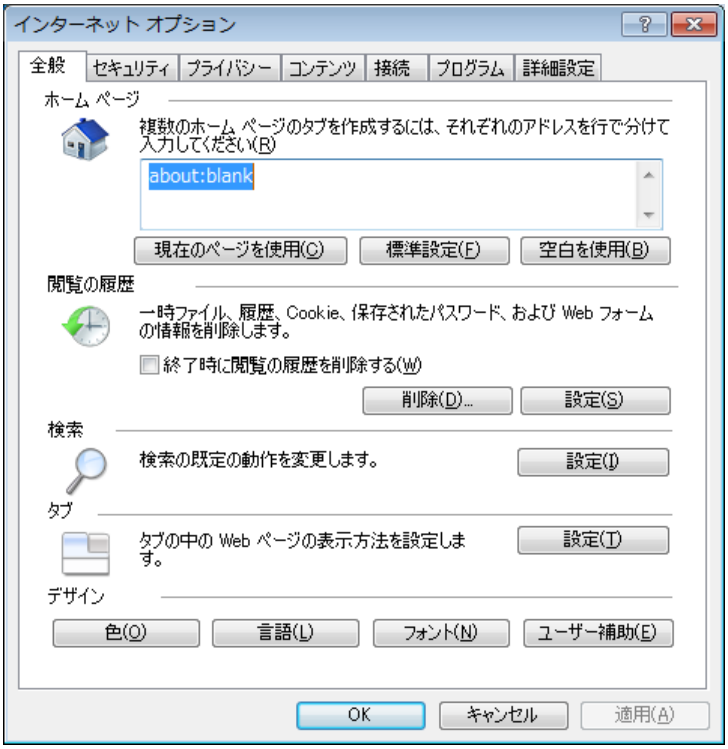


図 45 インターネットオプション起動画面

25. インターネットオプションの表示がコンテンツに切り替わったら、「証明書」ボタンをクリックします。

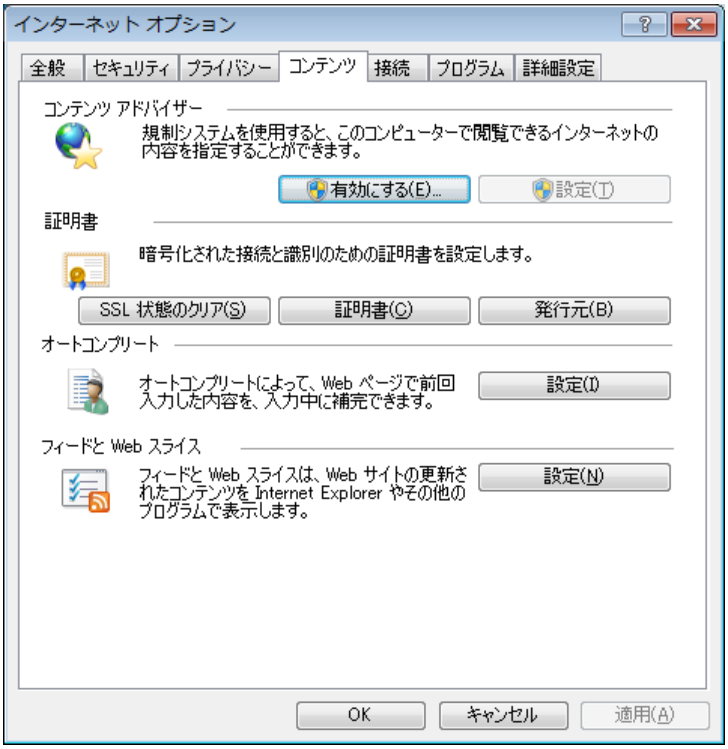


図 46 コンテンツの表示

26. 証明書画面が表示されたら、先ほどインストールした証明書を選択し、「表示」ボタンをクリックします。

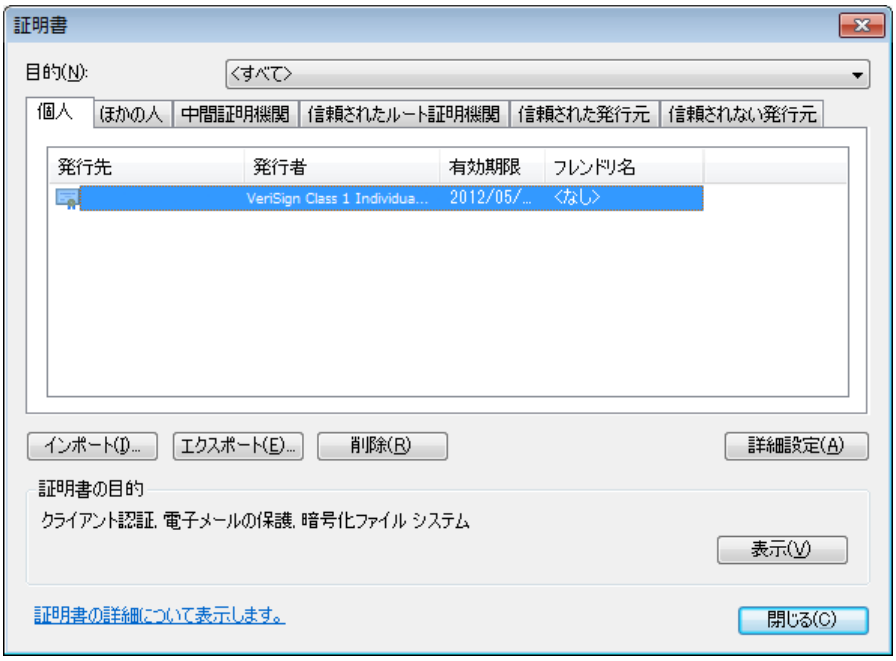


図 47 証明書確認画面

27. 下記に示す証明書の情報画面が表示されたら、申請した内容と合致しているか確認

してください。

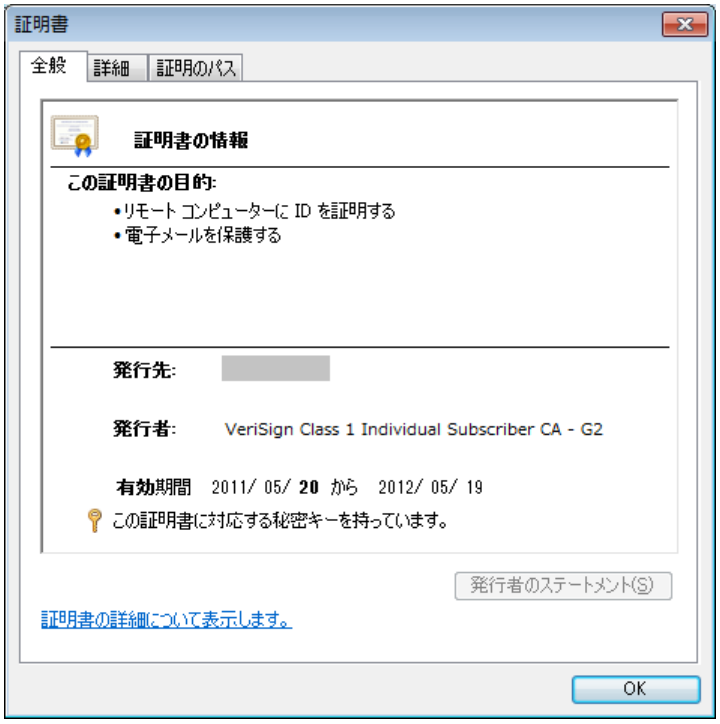


図 48 証明書の情報画面

28. 確認が終了したら、夫々の画面をクローズして終了します。

ii. Windows CA からの取得例

以下に、Active Directory 内に設定した CA から個人用電子証明書を TruCSP に格納する例を示します。

クライアント PC の証明書コンソールから、Active Directory 内の CA に証明書を要求するには、サーバーPC の OS でエンタプライズ CA が設定されている必要があります。

注）既存の CA が、スタンドアロン CA である場合、クライアント PC の証明書コンソールから、Active Directory 内の CA に証明書を直接要求する事は出来ません。その場合は、Windows CA の証明書サービス Web ページ（http://＜サーバー名＞/certsrv）を介して、商用 CA からの取得と同様に、証明書を要求してください。

1) CA の設定

1. サーバーPC にエンタプライズ管理者としてログオンしてください。
2. 「スタート」－「サーバーマネージャー」を選択します。

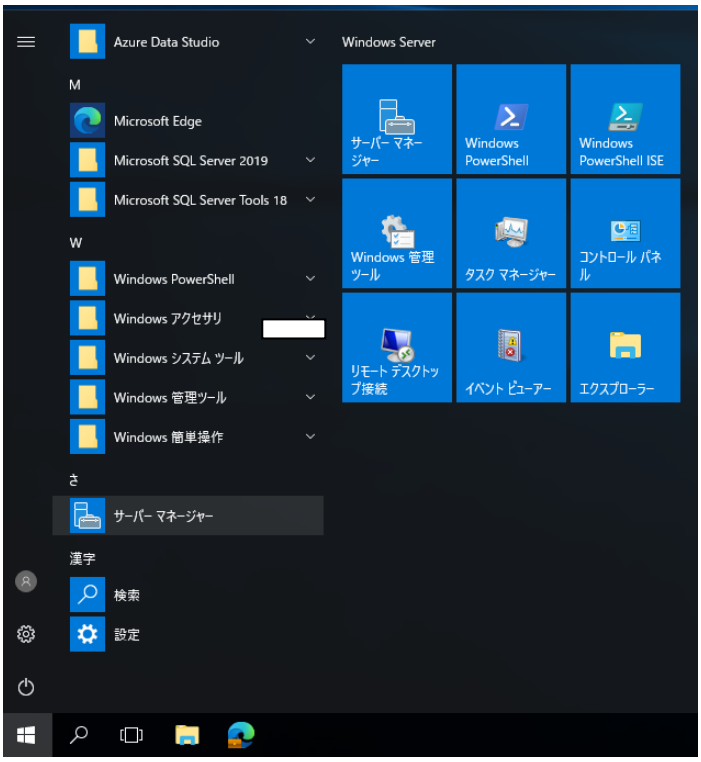


図 49 サーバーマネージャーの起動

3. サーバーマネージャー画面が表示されたら、「役割の追加」をクリックします。

図 50 サーバーマネージャー起動画面

4. 下記のような役割と機能の追加ウィザード画面が表示されたら、「開始する前に」の事項を確認し、問題が無ければ「次へ」ボタンをクリックします。

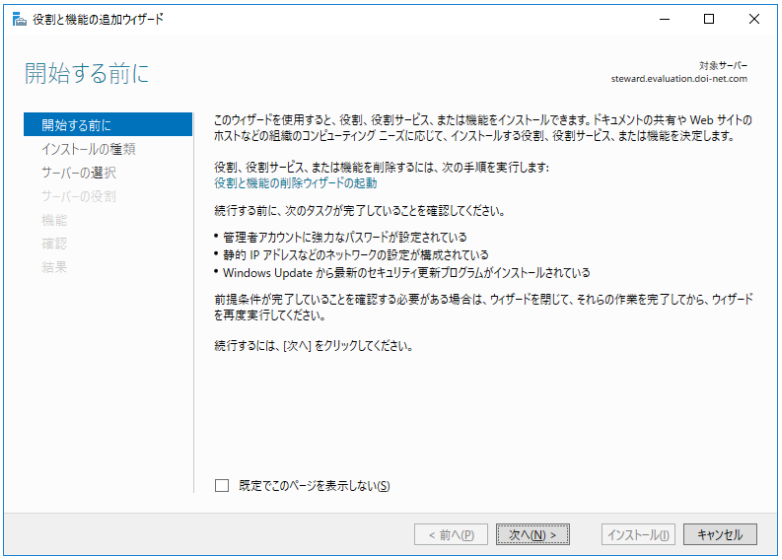


図 51 役割と機能の追加ウィザード起動画面

5. 「インストールの種類の選択」ページが表示されたら、「役割ベースまたは機能ベースのインストール」ラジオボタンをチェックし、「次へ」ボタンをクリックします。

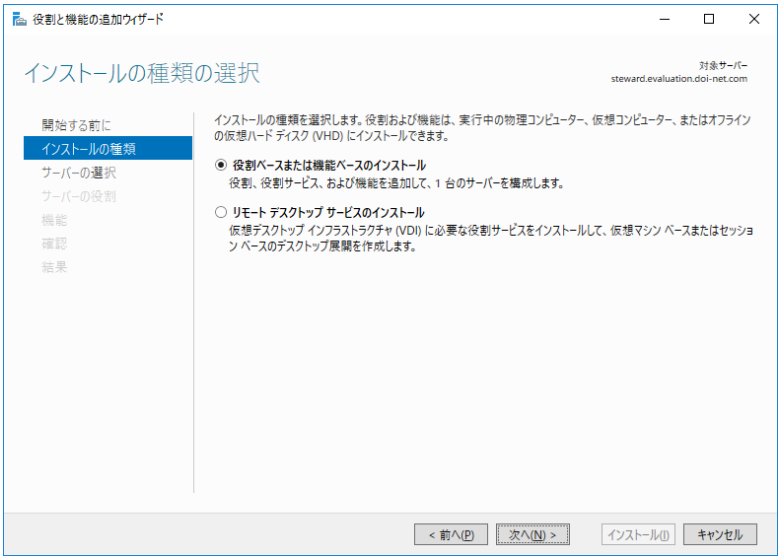


図 52 インストールの種類の選択画面

6. 「対象サーバーの選択」ページが表示されたら、サーバープールから対象のサーバーを選択し、「次へ」ボタンをクリックします。

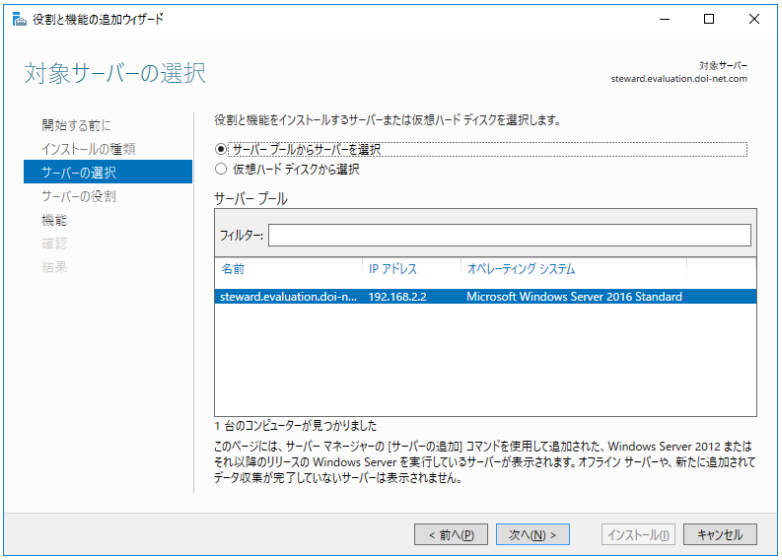


図 53 対象サーバーの選択画面

7. 「サーバーの役割の選択」ページが表示されたら、「Active Directory 証明書サービス」チェックボックスをチェックし、「次へ」ボタンをクリックします。

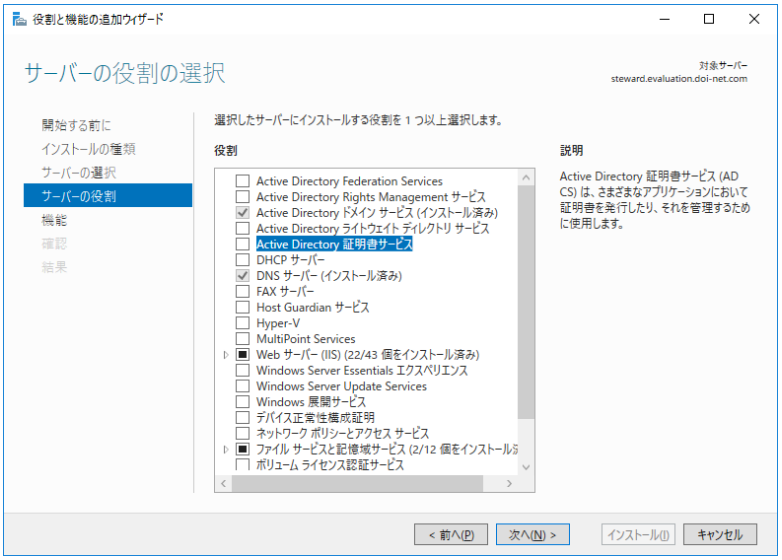


図 54 サーバーの役割の選択画面

8. 「Active Directory 証明書サービス」チェックボックスをチェックすると、下記に示す機能の追加の確認画面が表示されます。問題がなければ、「機能の追加」ボタンをクリックして続行します。

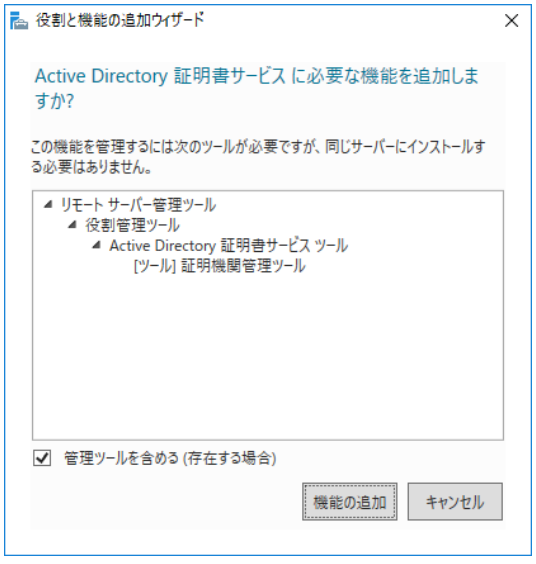


図 55 機能の追加の確認画面

9. 機能の選択画面が表示されたら項目を確認し、問題がなければ、「次へ」ボタンをクリックして続行します。

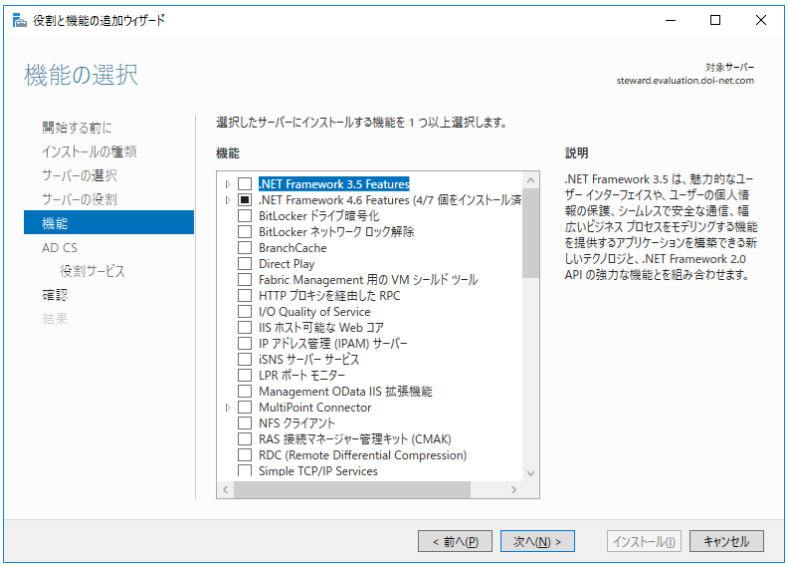


図 56 機能の選択画面

10. 「Active Directory 証明書サービス」チェックボックスをチェックすると、下記に示すコンピューター名とドメインメンバシップの確認画面が表示されます。問題がなければ、「次へ」ボタンをクリックして続行します。

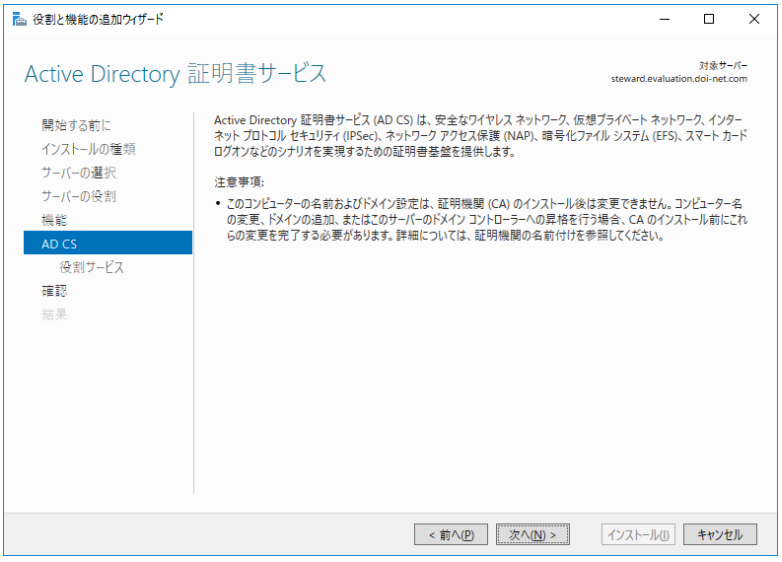


図 57 Active Directory 証明書サービス画面

11. 「役割サービスの選択」ページが表示されたら、証明書サービス Web ページを利用するため、「証明機関 Web 登録」チェックボックスをチェックし、「次へ」ボタンをクリックします。

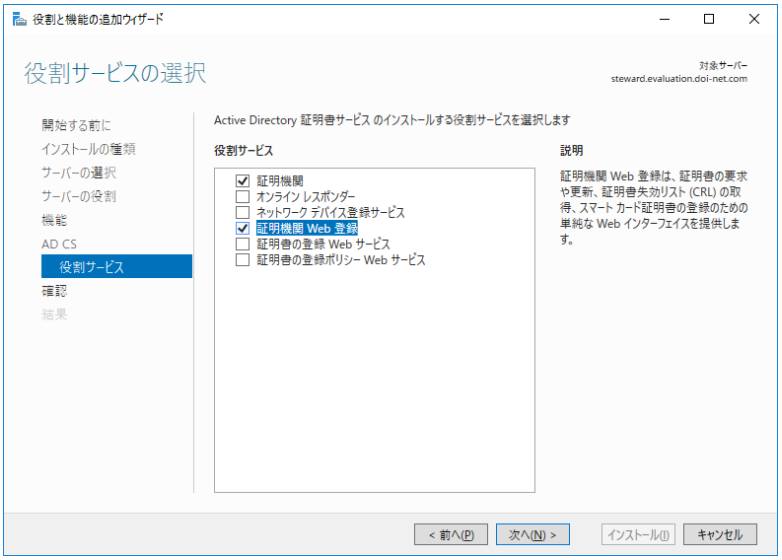


図 58 役割サービスの選択画面

12. 事前にオプションの機能がインストールされていない場合、「証明機関 Web 登録」がチェックされると、下記に示す画面が表示されます。問題がなければ、「インストール」ボタンをクリックして続行します。

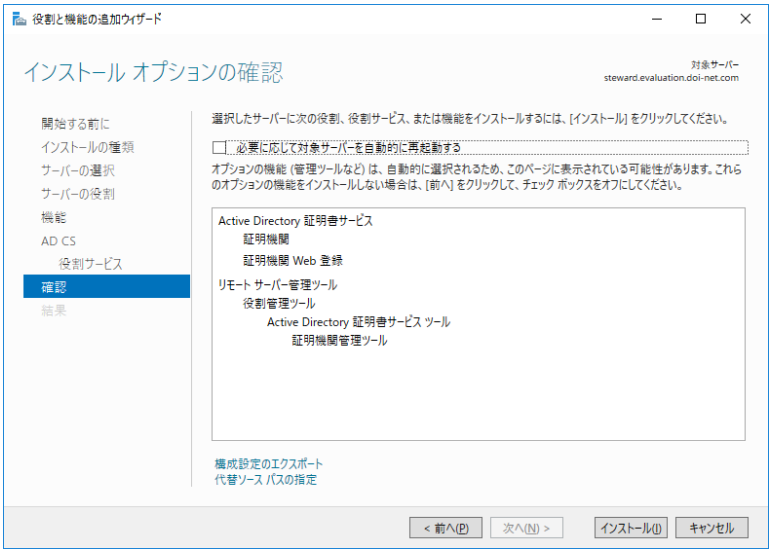


図 59 インストールオプションの確認画面

13. 次に、「セットアップの種類」ページが表示されたら、ネットワーク構成に応じてセットアップ種類を選択し、「次へ」ボタンをクリックします。

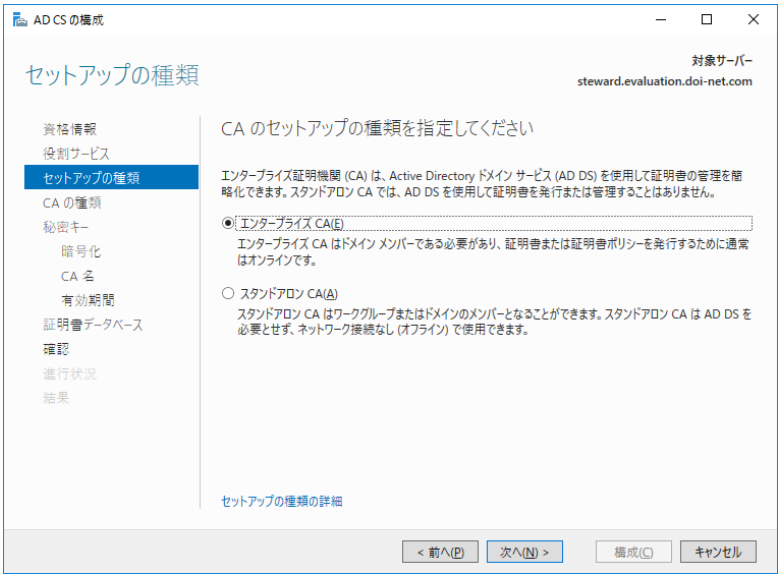


図 60 セットアップの種類の指定画面

14. 「CA の種類」ページが表示されたら、セットアップしたい CA 種類を選択し、「次へ」ボタンをクリックします。

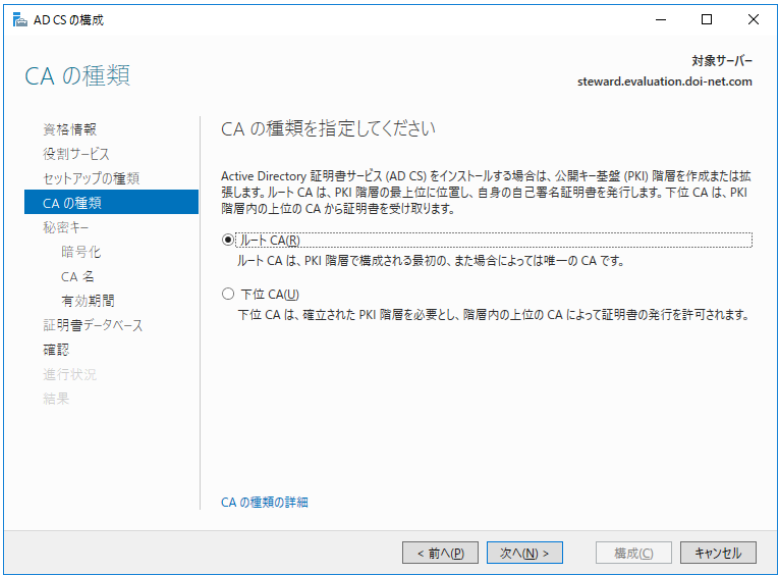


図 61 CA の種類の指定画面

15. 「秘密キー」画面が表示されたら、「新しい秘密キーを作成する」ラジオボタンを選択し、「次へ」ボタンをクリックします。

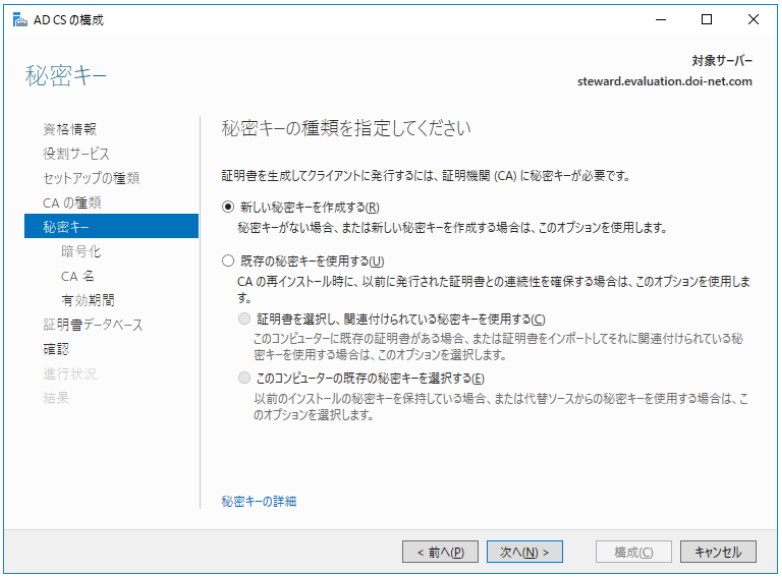


図 62 秘密キーの設定画面

16. 次に、「CA の暗号化」ページが表示されます。使用したい CSP、ハッシュアルゴリズム、キーの長さ等を設定し、「次へ」ボタンをクリックします。

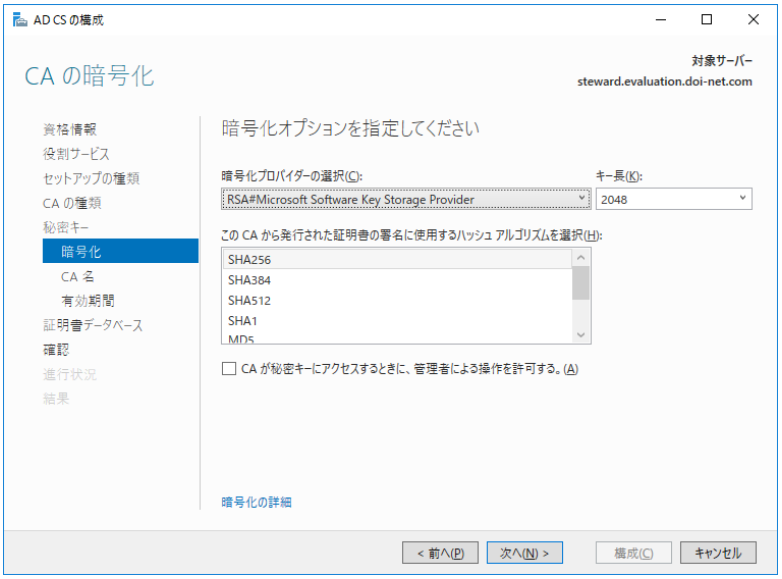


図 63 CA の暗号化構成画面

17. 「CA の名前」ページが表示されたら、必要に応じて「この CA の共通名」エディットボックスに生成する一意の CA 名をタイプし、「次へ」ボタンをクリックします。

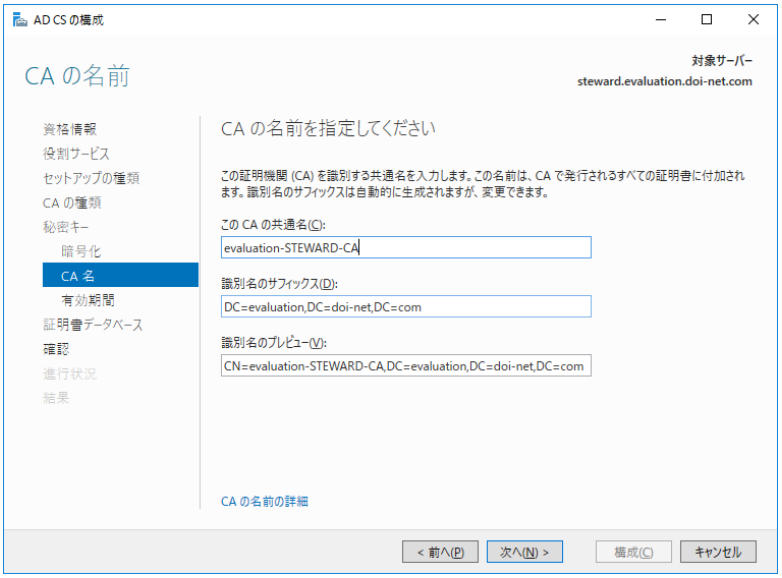


図 64 CA の名前構成画面

18. 「有効期間」ページが表示されたら、必要に応じて有効期間を選択し、「次へ」ボタンをクリックします。

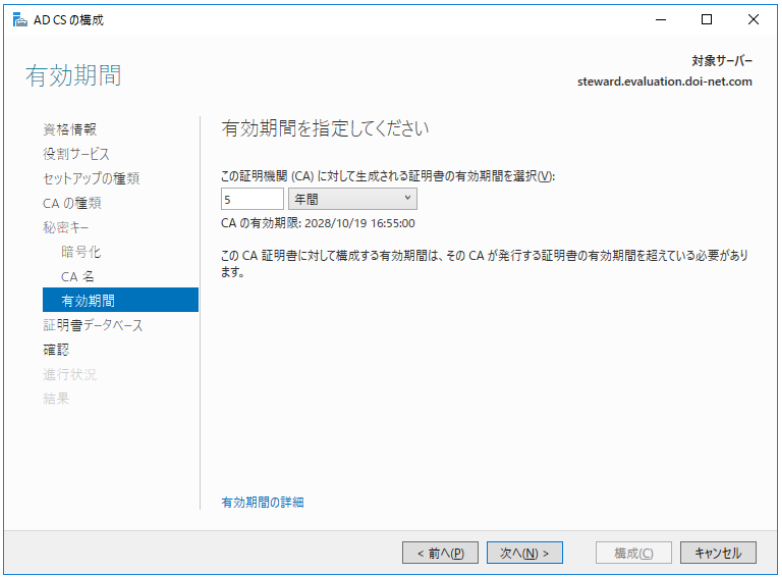


図 65 有効期間の設定画面

19. 「CA データベース」画面が表示されたら、必要に応じて場所を変更してください。

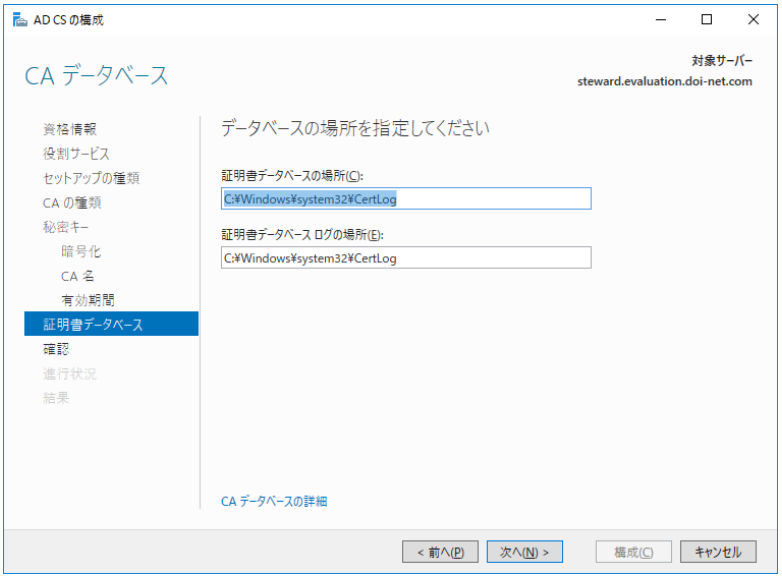


図 66 証明書データベースの構成画面

20. 「確認」ページが表示されたら、問題が無いことを確認し、「構成」ボタンをクリックして続行してください。

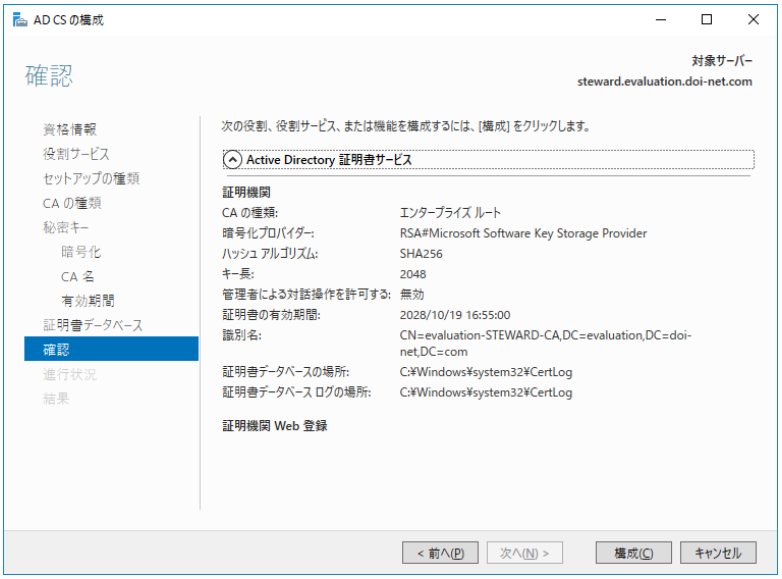


図 67 インストールオプションの確認画面

21. インストールが終了すると、「インストールの結果」ページが表示されます。問題が発生した場合は、原因を排除し、再度インストールしてください。

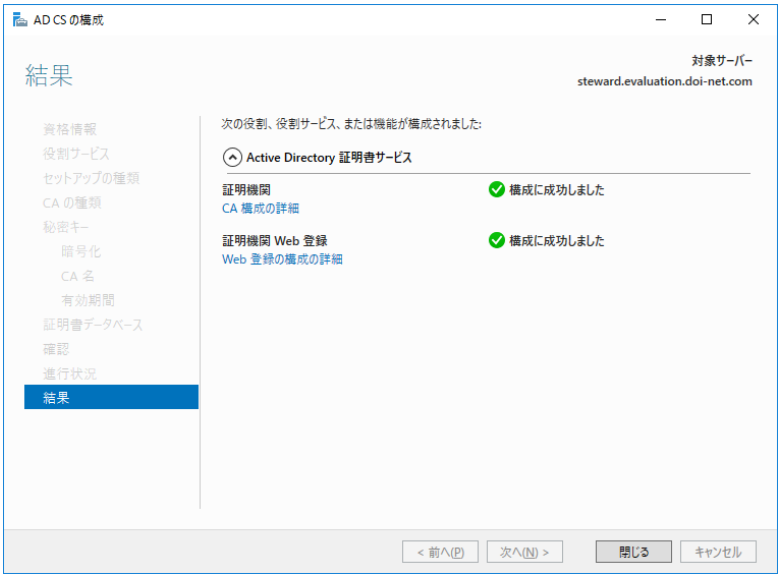


図 68 インストールの結果画面

22. 「閉じる」ボタンをクリックしてサーバーマネージャーに戻ったら、「役割」に「Active Directory 証明書サービス」が追加されていることを確認し、終了します。

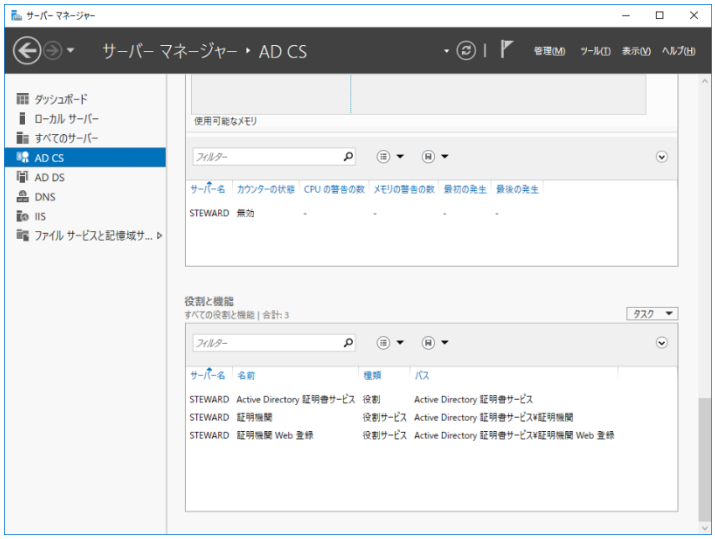


図 69 サーバーマネージャー終了画面

23. 次に、「スタート」－「Windows 管理ツール」－「証明機関」を選択します。

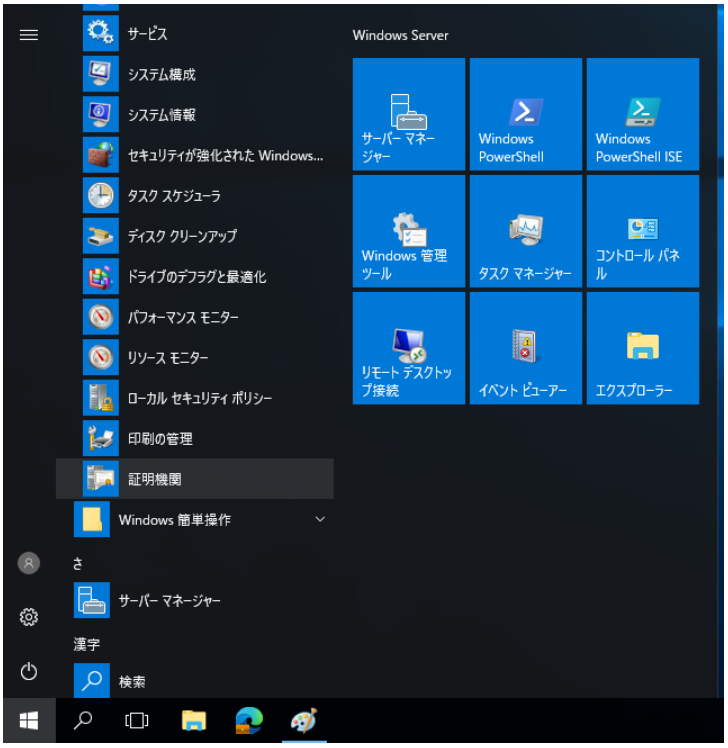


図 70 証明機関コンソールの起動

24. 証明機関コンソール画面が表示されたら、左側ペインから「証明書テンプレート」を選択します。

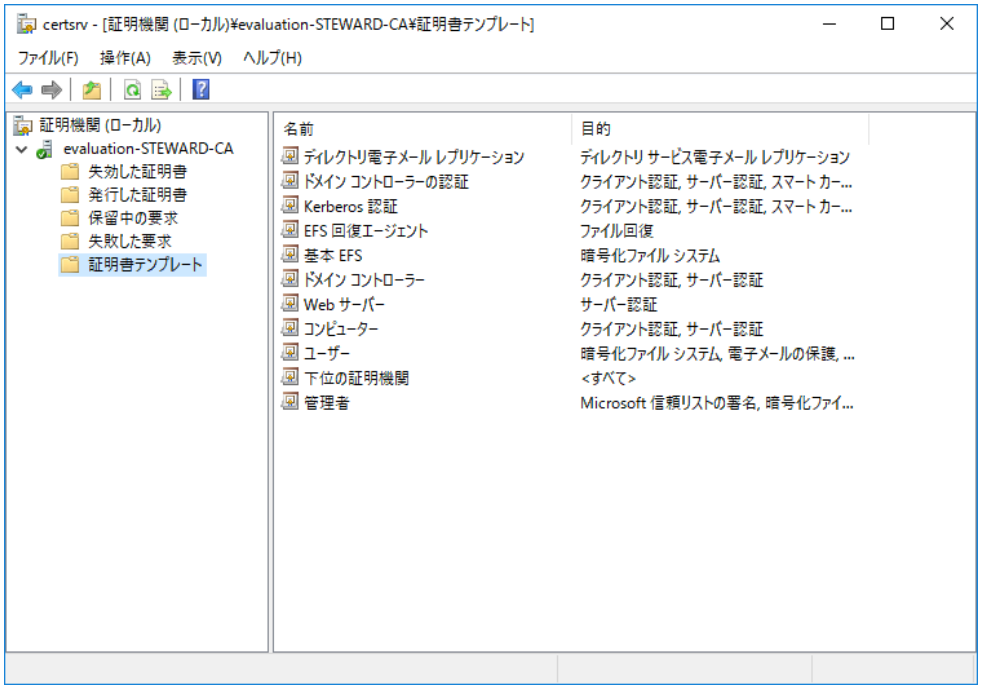


図 71 証明機関コンソール起動画面

25. 右側ペインに、発行済みの証明書テンプレートの一覧が表示されたら、「証明書テンプレート」上で、マウスの右ボタンをクリックします。ポップアップメニューが表示されたら、「管理」を選択します。

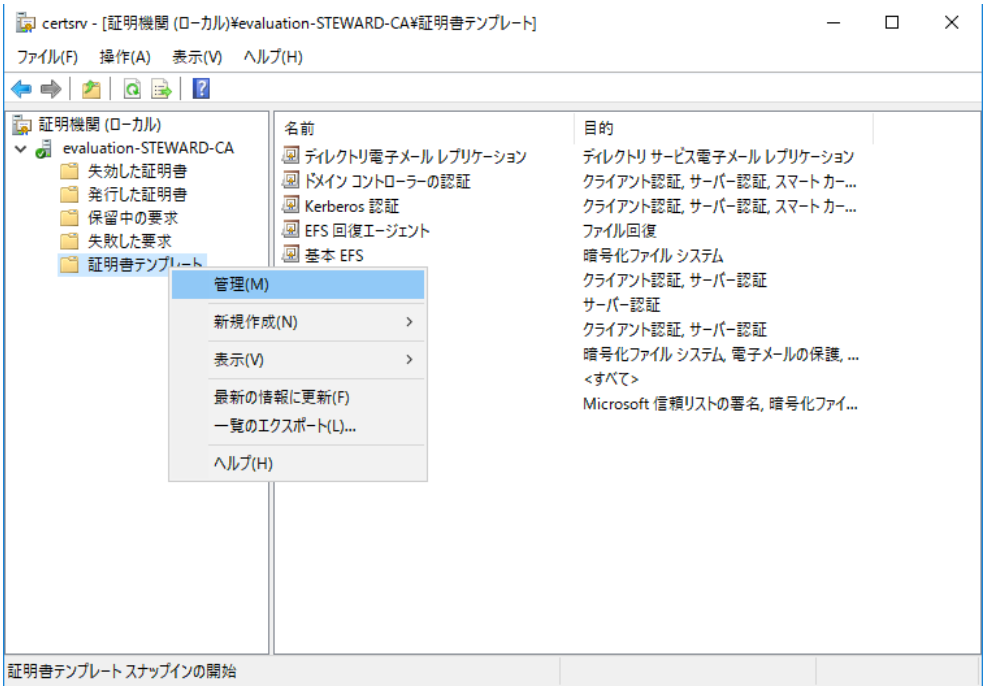


図 72 証明機関コンソールから証明書テンプレートの呼出し

26. 「管理」が選択されると、下記に示す証明書テンプレートコンソール画面が表示されます。

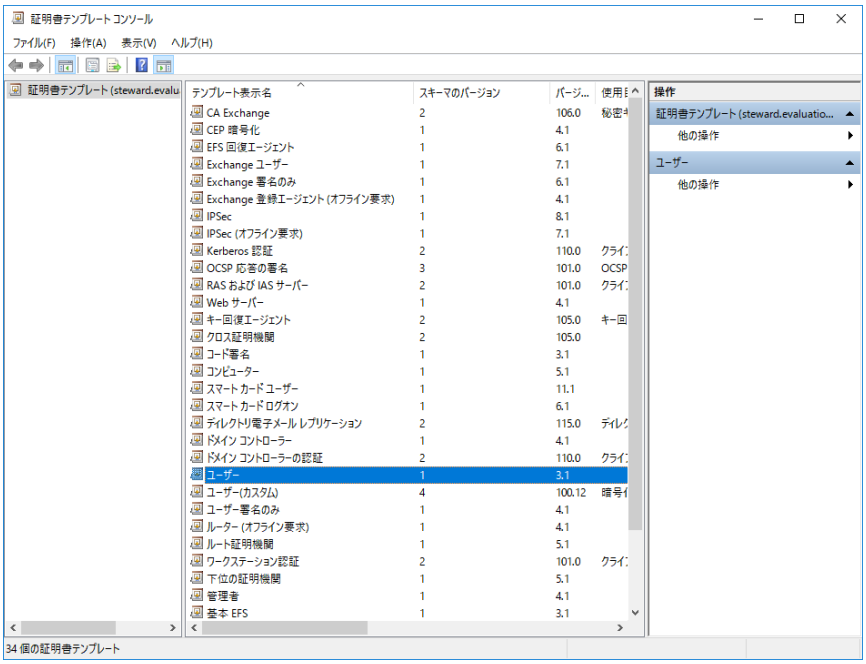


図 73 証明書テンプレートコンソール起動画面

27. 証明書テンプレートコンソール画面が表示されたら、右側ペイン中の「ユーザー」上で、マウスの右ボタンをクリックします。ポップアップメニューが表示されたら、「テンプレートの複製」を選択します。

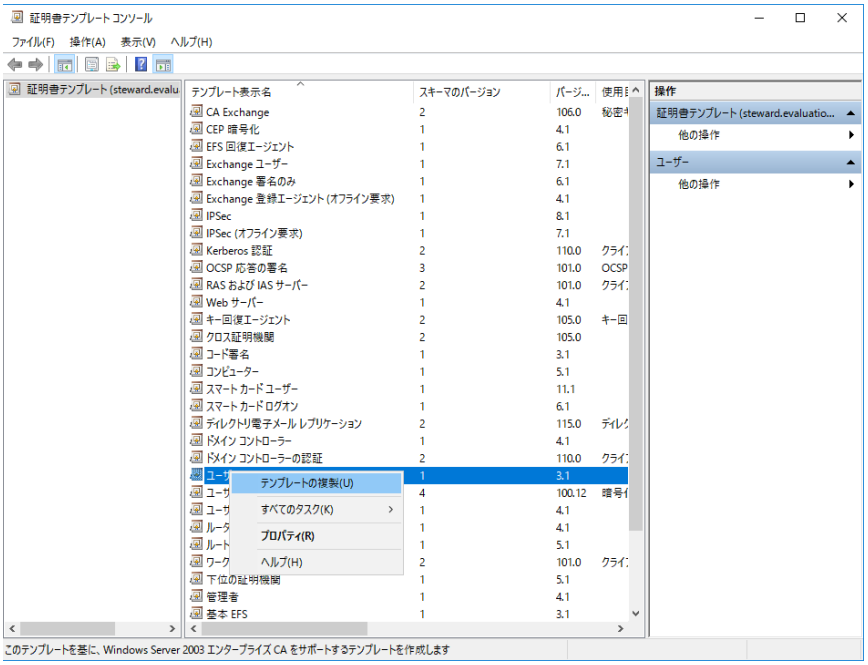


図 74 証明書テンプレートの複製

28. 「テンプレートの複製」が選択されると、下記に示すようなテンプレートの複製画面が表示されます。利用環境に応じて、必要なテンプレートのバージョンを選択

し、「OK」ボタンをクリックしてください。

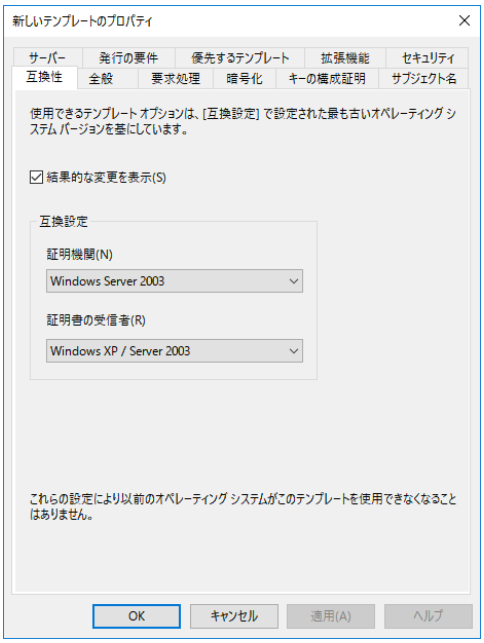


図 75 テンプレートの複製画面

29. 次に、下記に示すような証明書テンプレートのプロパティ画面が表示されます。「テンプレート表示名」と「テンプレート名」に夫々任意の名称（本例では、ユーザー（カスタム）と UserCustom）をタイプします。必要に応じて、有効期間と更新期間も変更してください。

図 76 証明書テンプレートのプロパティ起動画面

30. 次に、「暗号化」タブを選択した後、「最小キーサイズ」を 1024 以下にするとともに、「サブジェクトのコンピューターで利用可能な任意のプロバイダー」ラジオボタンを選択し、「適用」ボタンをクリックした後、「OK」ボタンをクリックしてください。

注）エンドユーザで利用可能な CSP の選択肢を制限したい場合は、「以下のプロバイダーのうちどれか 1 つ」ラジオボタンをクリックします。その際は、サーバーPC に事前に TruCSP がインストールされている必要があります。このような利用形態をご希望の場合は、弊社にご相談ください。

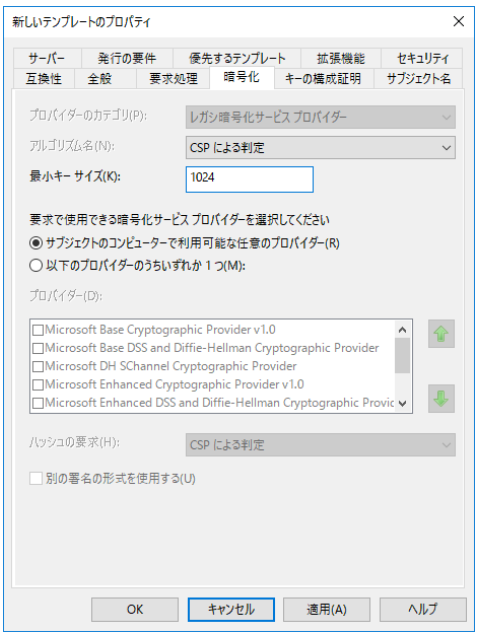


図 77 証明書テンプレートプロパティの暗号化設定画面

31. 証明書テンプレートコンソール画面に戻ったら、メニューバーから「ファイル」ー「終了」を選択し、証明書テンプレートの作成を終了します。

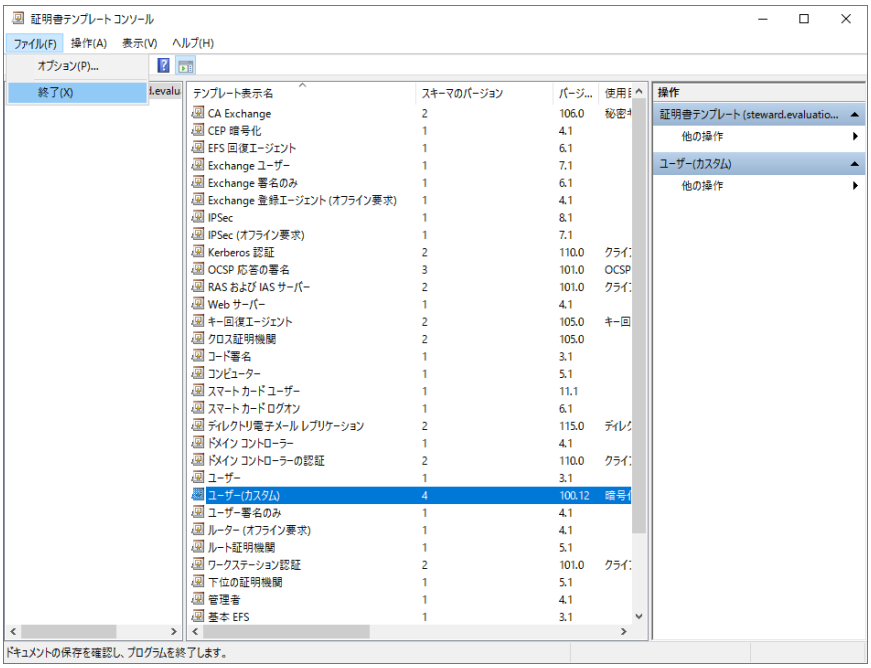


図 78 証明書テンプレートコンソール終了画面

32. 証明機関コンソール画面に戻ったら、「証明書テンプレート」上でマウスの右ボタンをクリックします。ポップアップメニューが表示されたら、「新規作成」ー「発行する証明書テンプレート」を選択します。

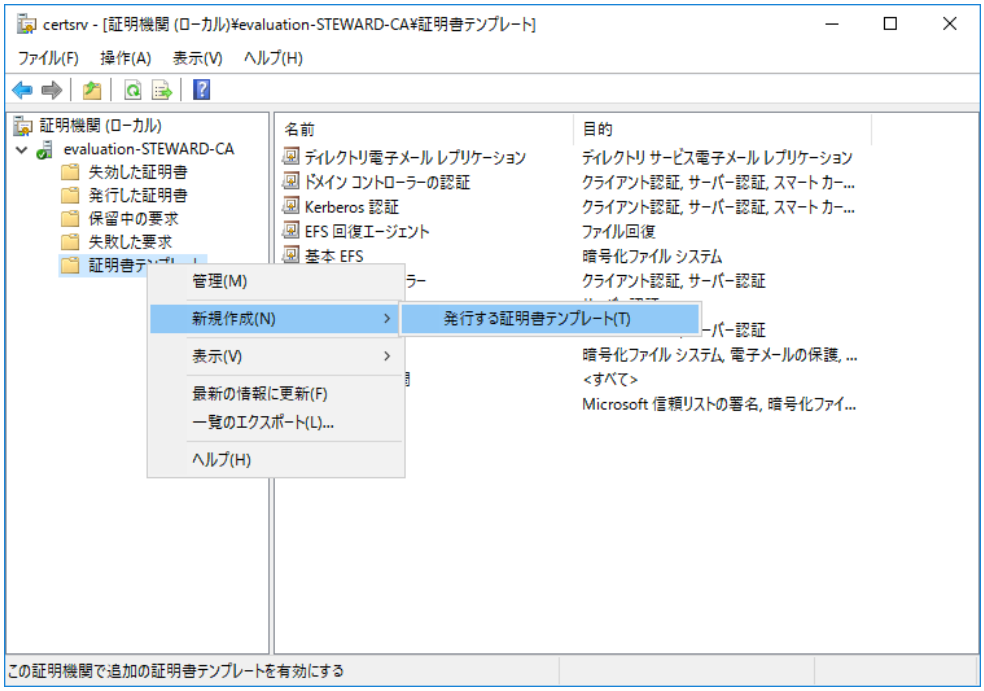


図 79 証明書テンプレートの発行

33. 証明書テンプレートの選択画面が表示されたら、先に作成した証明書テンプレ

ート（本例ではユーザー（カスタム））を選択し、「OK」ボタンをクリックします。

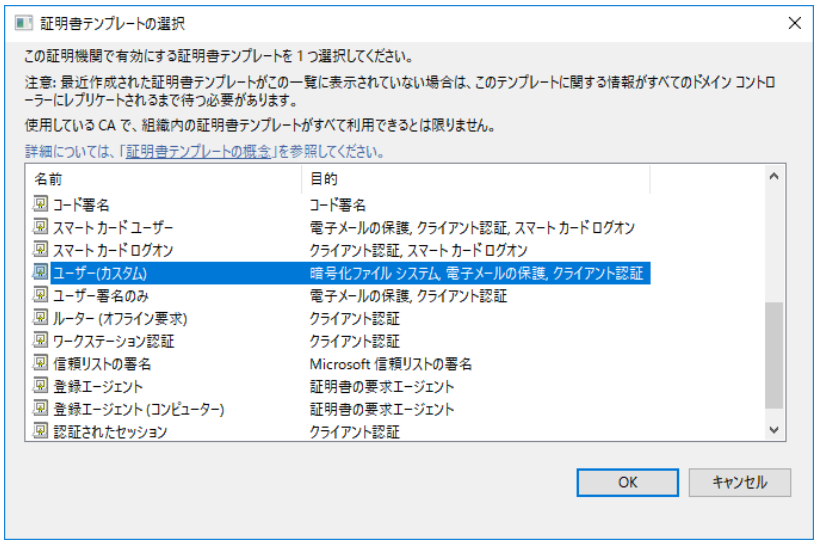


図 80 証明書テンプレートの選択画面

34. 証明機関コンソール画面に戻ったら、発行済みの証明書テンプレートの一覧に、前項で選択した証明書テンプレート（本例ではユーザー（カスタム））が追加されていることを確認し、メニューバーから「ファイル」－「終了」を選択して、設定を終了します。

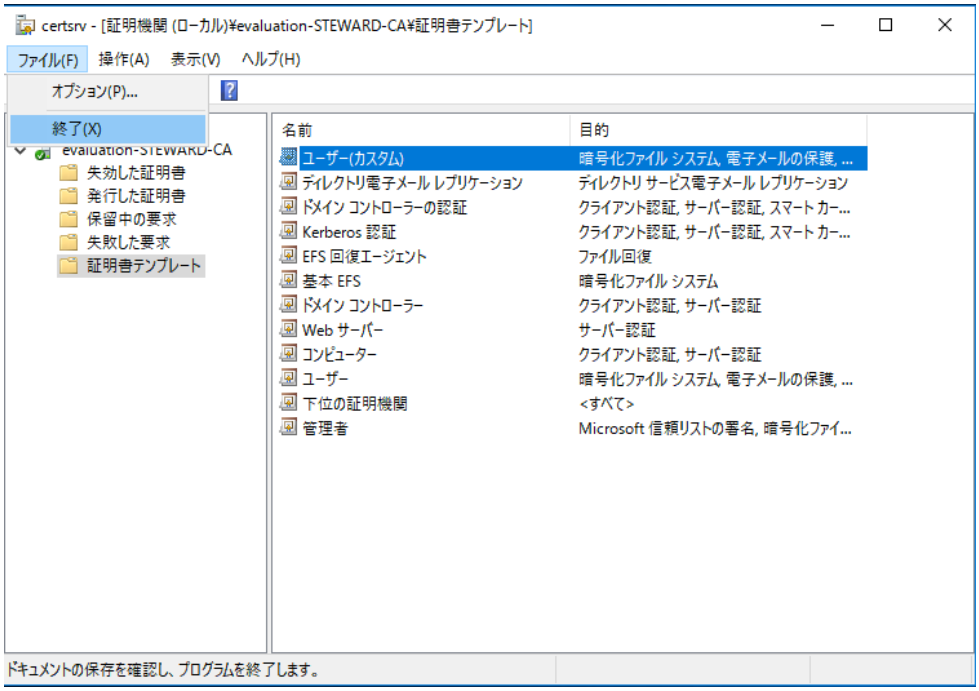


図 81 証明機関コンソールの終了

2) 証明書の要求

1. クライアント PC に TruGate にてログインするか、TruStack Gina を有効化していない場合は認証デバイスを利用可能にしてください。
2. MMC を起動し、先に作成した証明書コンソールファイルを開き、証明書コンソールを起動します。

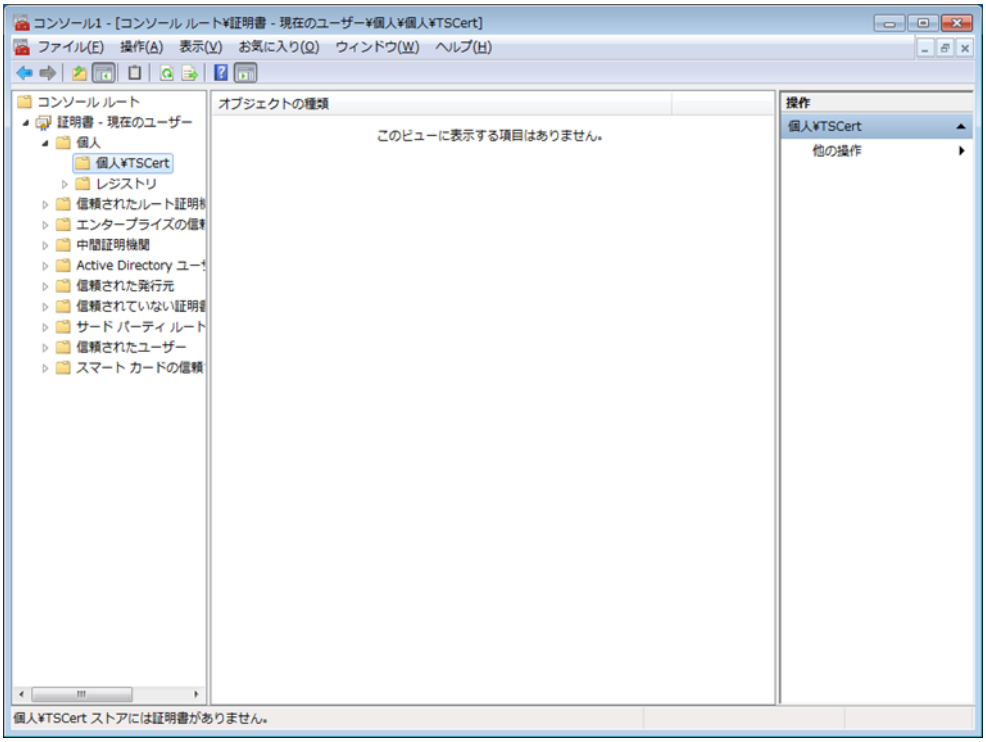


図 82 証明書コンソールの起動

3. 証明書コンソールが起動されたら、左側ペイン中の「TSCert」上で右クリックし、ポップアップメニューが表示されたら、「すべてのタスク」ー「新しい証明書の要求」を選択します。

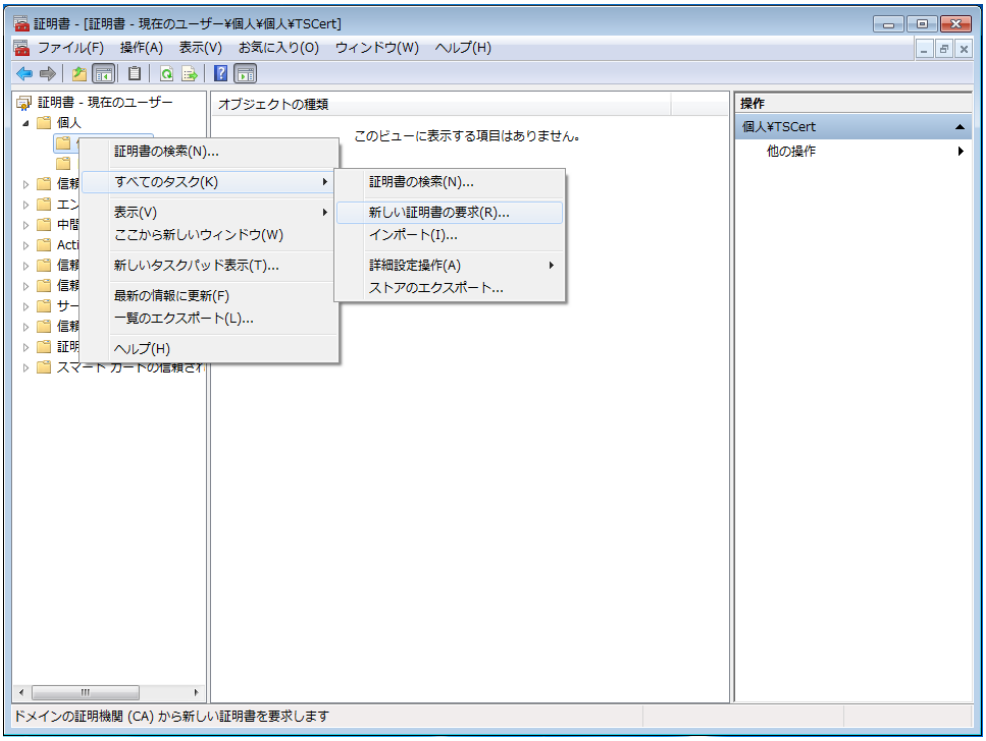


図 83 証明書コンソール – 新しい証明書の要求

4. 以下、証明書の登録ウィザードに従って操作します。

(ア)「開始する前に」ページが表示されたら、内容を確認し「次へ」ボタンをクリックしてください。

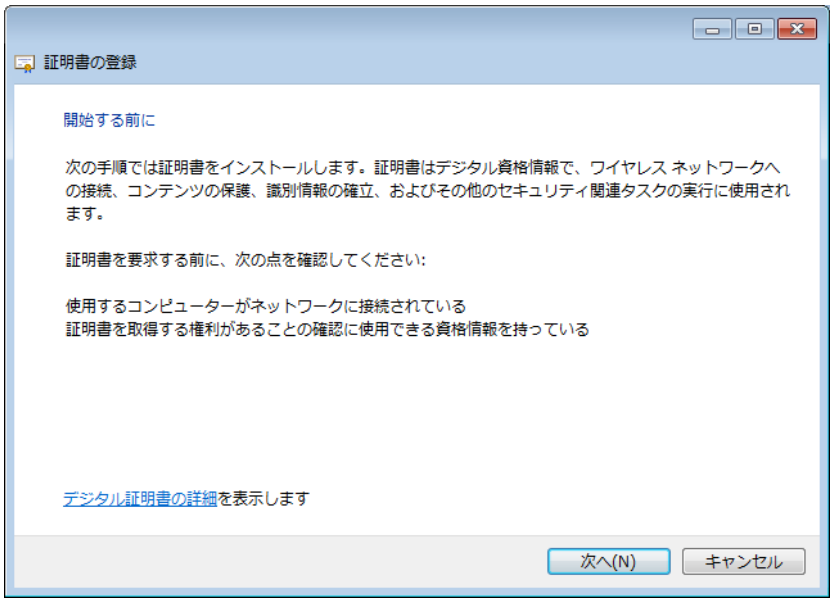


図 84 証明書の登録ウィザード起動画面

(イ)「証明書の登録ポリシーの選択」ページが表示されたら、「次へ」ボタンをク

リックしてください。

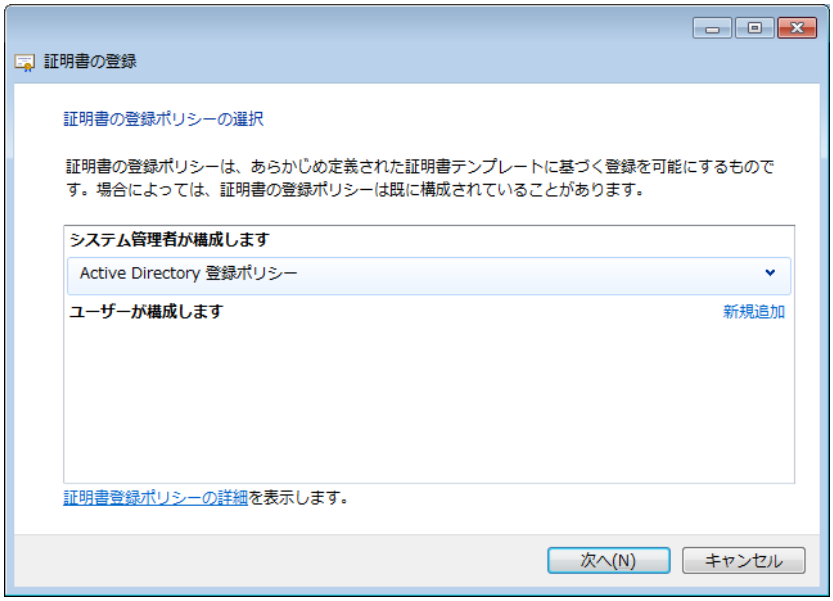


図 85 証明書の登録ポリシーの選択画面

(ウ) 次に、「証明書の要求」ページが表示されたら、先に CA で新規に発行した証明書テンプレート（本例では「ユーザー（カスタム）」）を選択した後、「詳細」ボタンをクリックします。

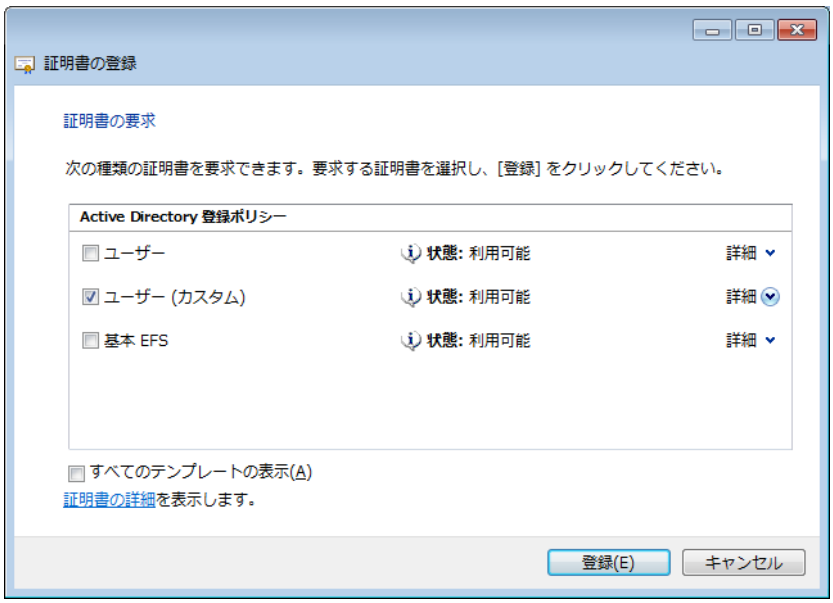


図 86 証明書の要求画面

(エ) 「ユーザー（カスタム）」の詳細内容が展開表示されたら、「プロパティ」ボタンをクリックします。

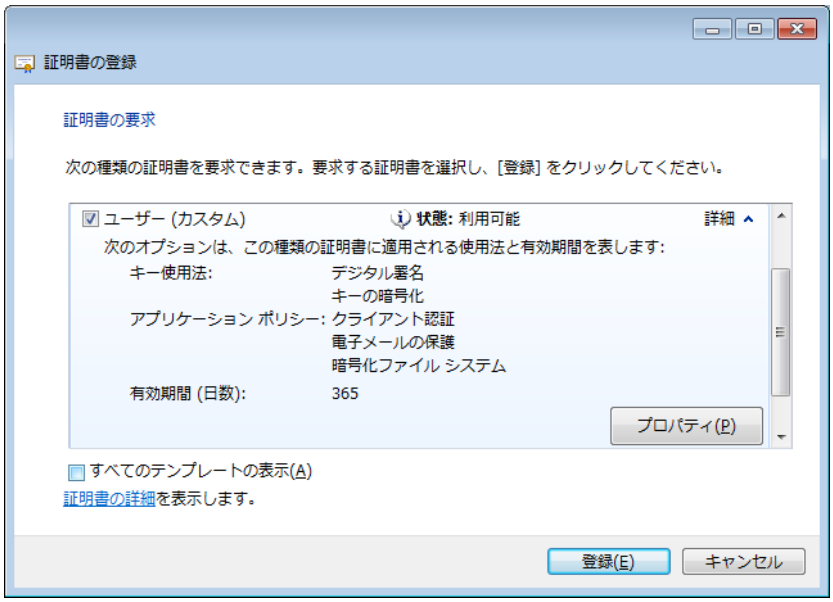


図 87 ユーザー(カスタム)のテンプレート画面

(オ) 証明書のプロパティ画面が表示されたら、「秘密キー」タブをクリックします。

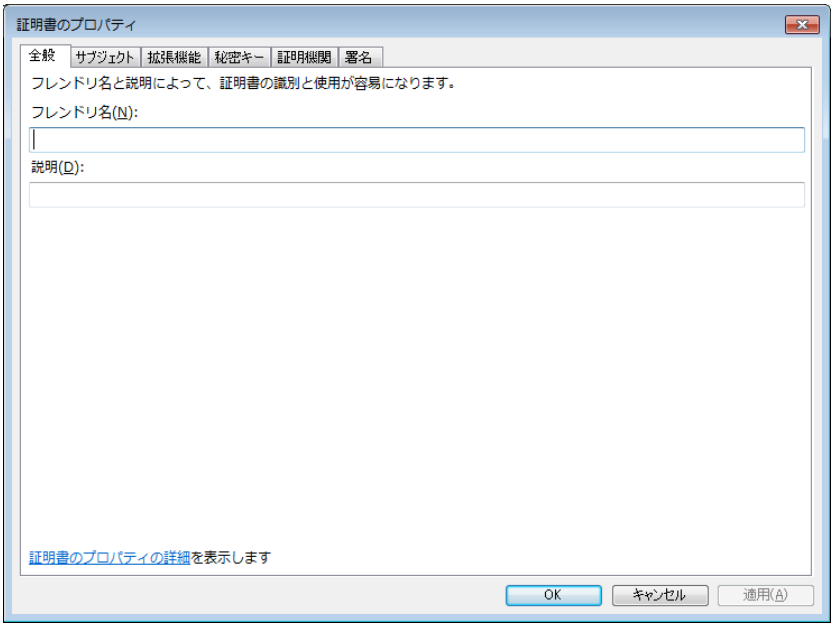


図 88 証明書のプロパティ画面

(カ) 秘密キーページが表示されたら、「暗号化サービスプロバイダー」バーをクリックし、暗号化サービスプロバイダーの選択画面を表示させます。「TruStack Cryptographic Provider v1.0」のチェックボックスをチェックし、他の暗号化サービスプロバイダーのチェックボックスを全てアンチェックします。

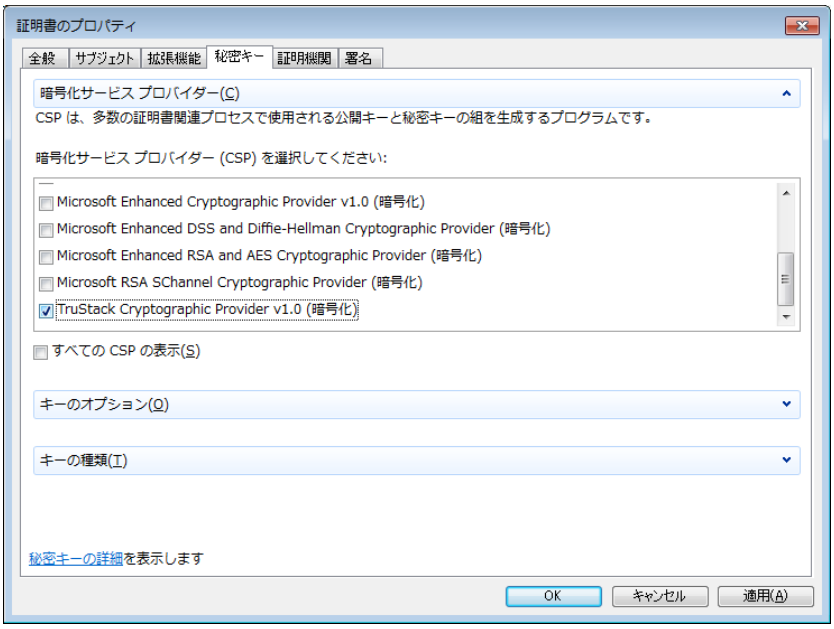


図 89 暗号化サービスプロバイダー選択画面

(キ) 次に、「キーのオプション」バーをクリックしてオプションを表示した後、「キーのサイズ」を 1024 以下にし、「秘密キーをエクスポート可能にする」、「秘密キーのアーカイブを許可する」、「強力な秘密キーの保護」チェックボックスを夫々チェックして、「OK」ボタンをクリックします。

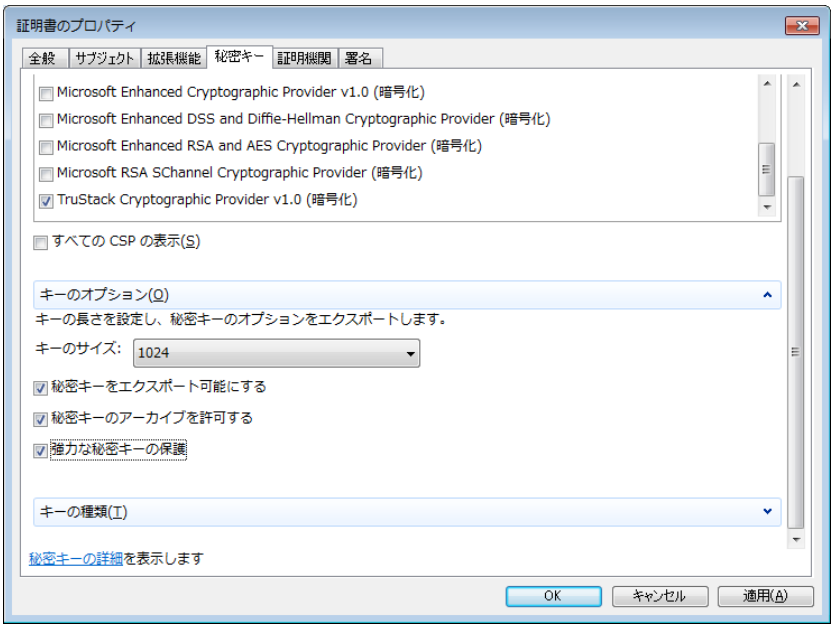


図 90 キーのオプション設定画面

(ク) 証明書の要求ページに戻ったら、「登録」ボタンをクリックします。

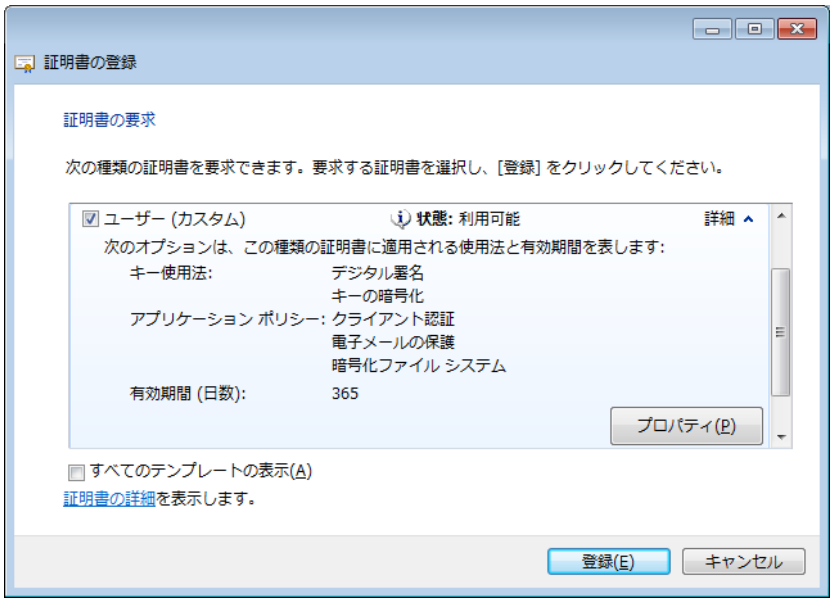


図 91 証明書の登録要求画面

(ケ) 登録が実行されると、証明書インストールの結果ページ確認画面が表示されます。証明書の登録が正常に終了すると、下図に示すように「状態」に成功の表示が現れます。最後に、「完了」ボタンをクリックして終了します。

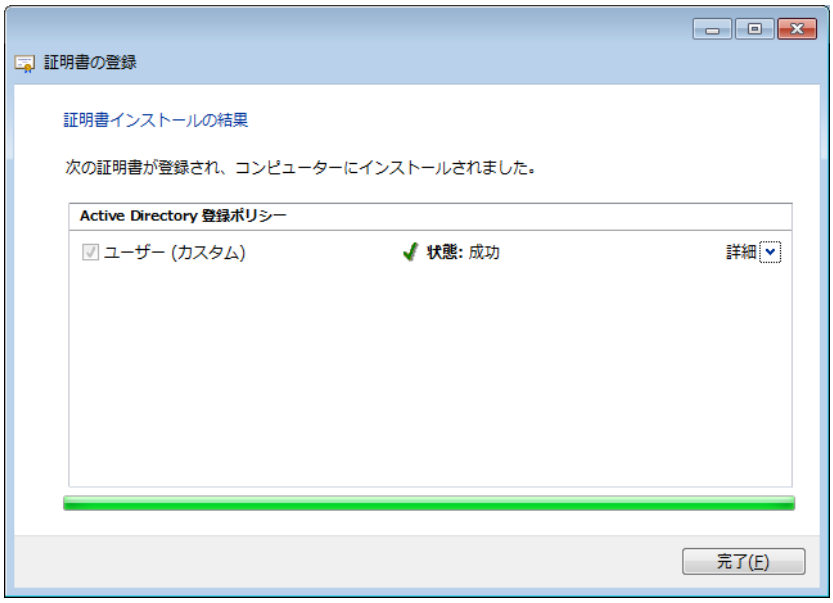


図 92 証明書インストールの結果画面

注）エラーが発生した場合は、認証デバイスの状態を確認し、認証デバイスの接続や格納域の初期化などの作業（証明書要求エラー/インポートエラー発生時の対処方法を参照）を行った上で、再度、証明書の要求を行ってください。

5. 証明書コンソールに戻ったら、「Active Directory ユーザーオブジェクト」－「ユー

ザー証明書」ー「証明書」フォルダに、要求した証明書が生成されていることを確認します。

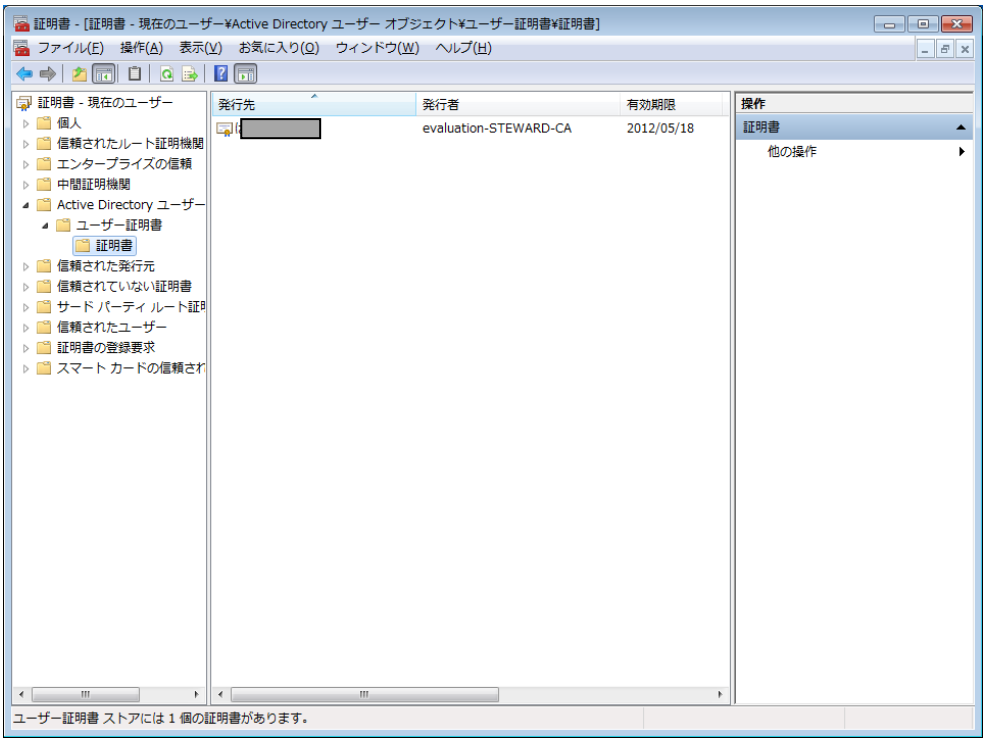


図 93 ユーザー証明書の生成確認

6. 同様に、「個人」ー「TSCert」ー「証明書」フォルダに証明書が表示されることを確認します。

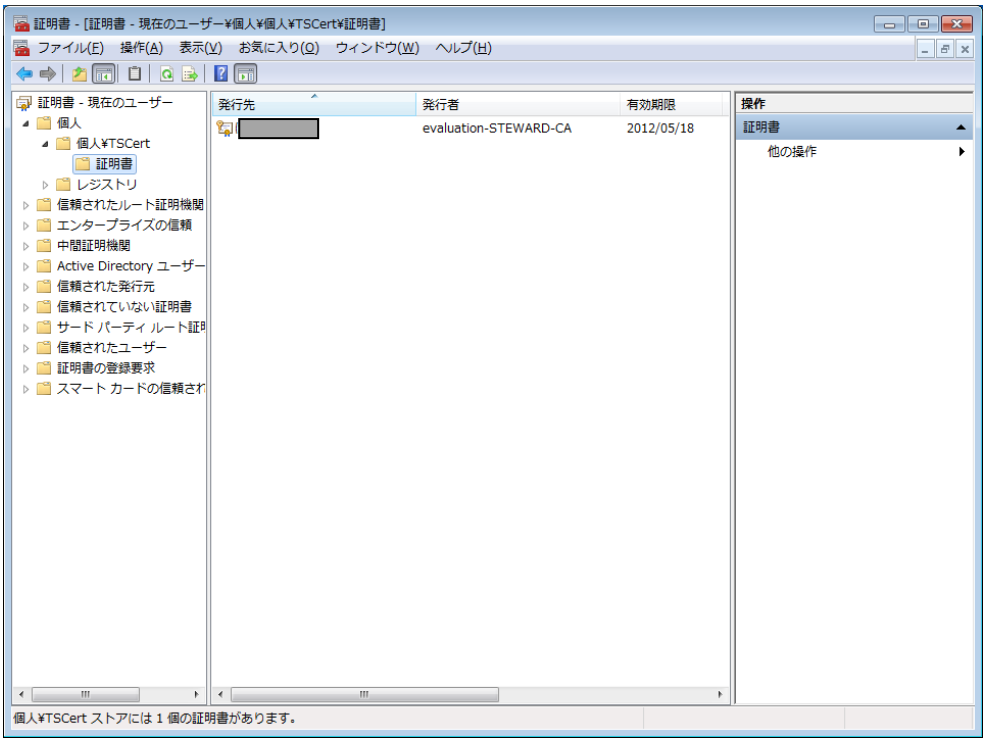


図 94 証明書コンソール画面 ― 証明書の確認

7. 確認できたら、証明書コンソール画面から「ファイル」ー「終了」を選択して終了します。

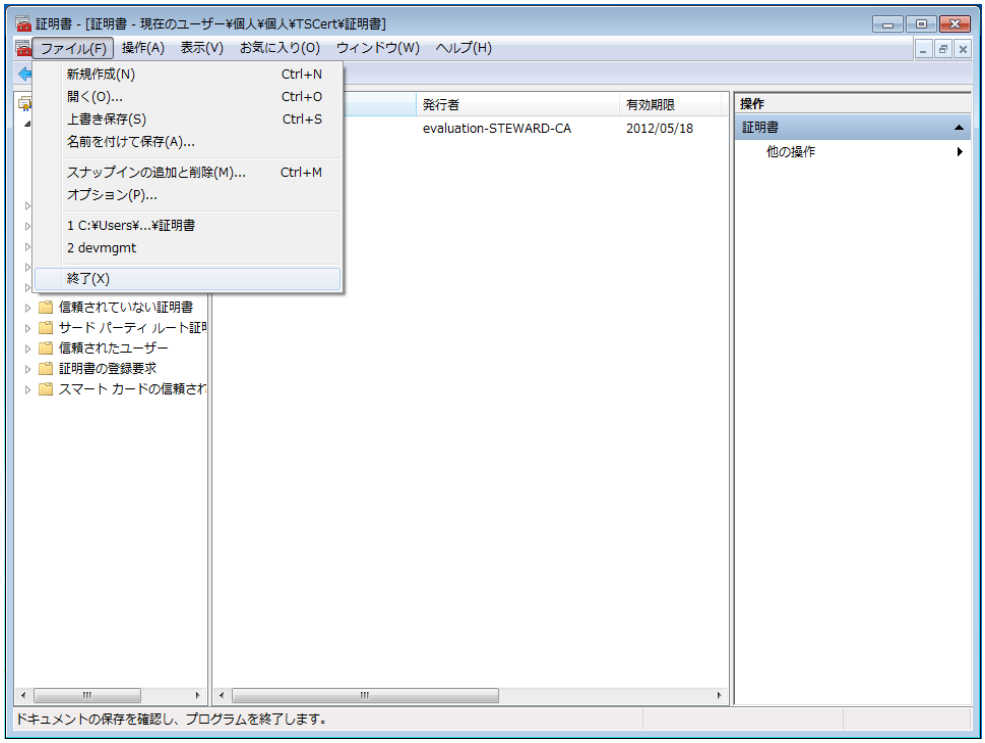


図 95 証明書コンソール画面 ― 終了

d. TruCSP をアプリケーションで利用する為の設定例

CSP タイプとして TruCSP を指定して取得した証明書を、アプリケーションで利用する際の設定例として、Outlook Express での設定方法を以下に示します。

1. TruGate にてログオンしてください。
2. Outlook Express を起動し、メニューバーから「ツール」ー「アカウント」を選択します。

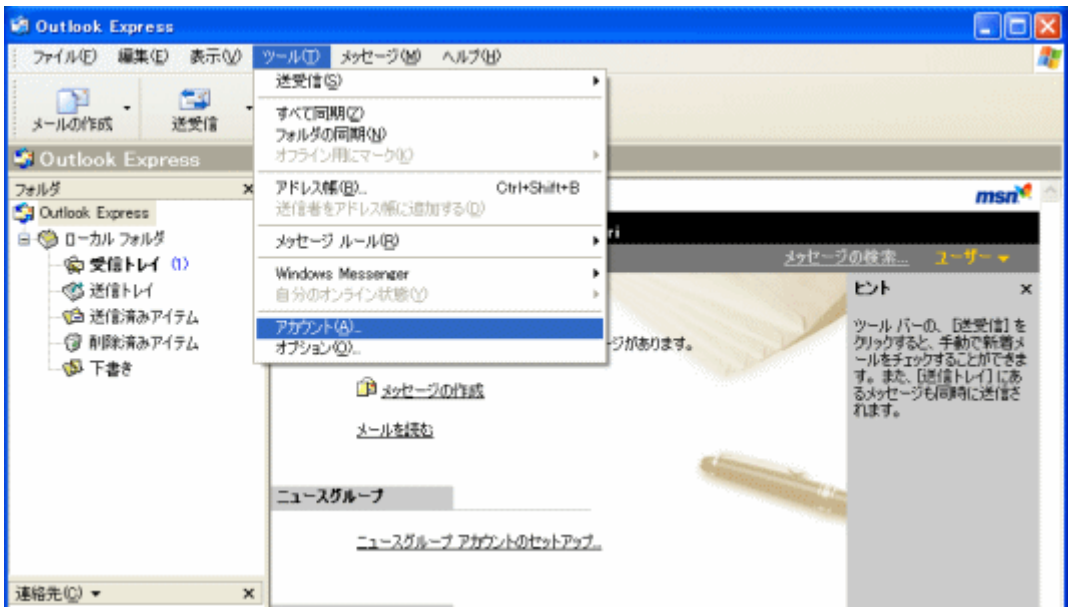


図 96 Outlook Express の起動

3. 下記に示すインターネットアカウント画面が表示されたら、「メール」タブを選択します。

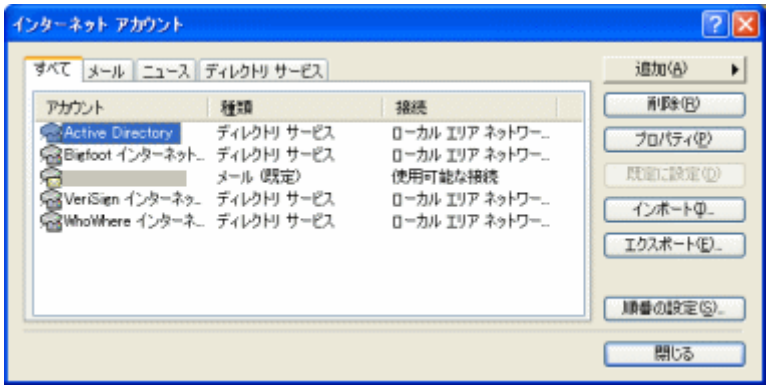


図 97 インターネット アカウント起動画面

4. インターネットアカウント画面の内容がメールに切り替わったら、電子証明書を利用するアカウントを選択し、「プロパティ」ボタンをクリックします。

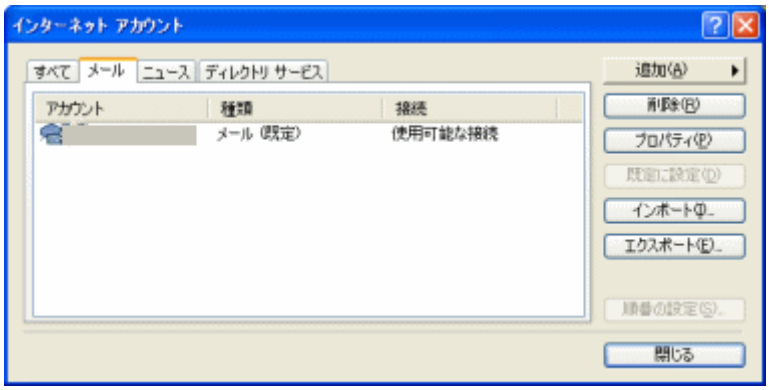


図 98 メールアカウントの表示

5. 次に、メールアカウントのプロパティ画面が表示されたら、「セキュリティ」タブを選択します。

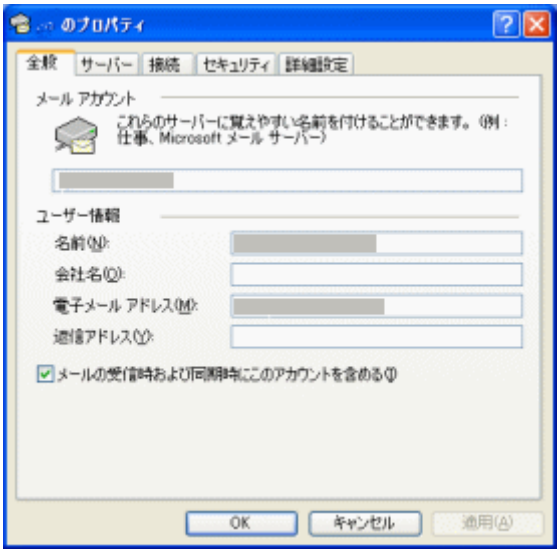


図 99 メールアカウントのプロパティ起動画面

6. メールアカウントのプロパティ画面の内容がセキュリティに切り替わったら、「署名の証明書」の「選択」ボタンをクリックします。

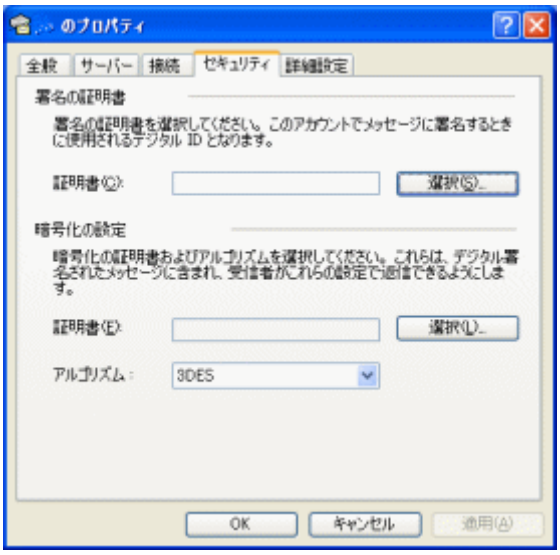


図 100 セキュリティ – 署名の証明書

7. 次に、下記に示す証明書の選択画面が表示されたら、CSP タイプに TruCSP を指定して取得した電子証明書を選択し、「証明書の表示」ボタンをクリックします。

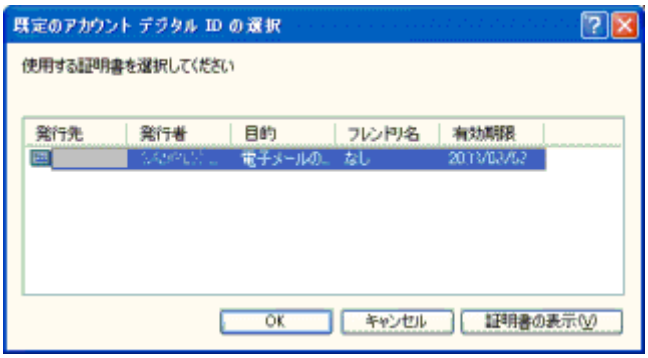


図 101 証明書の選択画面

8. 下記に示す証明書の情報画面が表示されたら、正しい証明書であることを確認し、「OK」ボタンをクリックしてください。複数の証明書がインストールされている場合は、十分に確認してください。

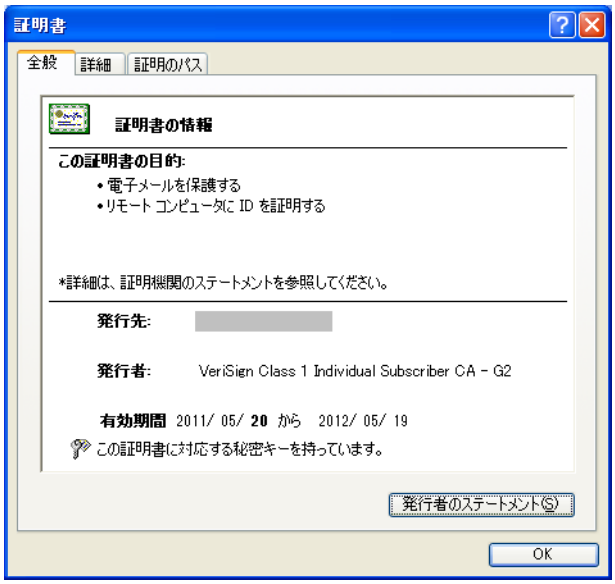


図 102 証明書の情報画面

9. 下記に示すメールアカウントのプロパティ画面に戻ったら、「暗号化の設定」の「選択」ボタンをクリックします。

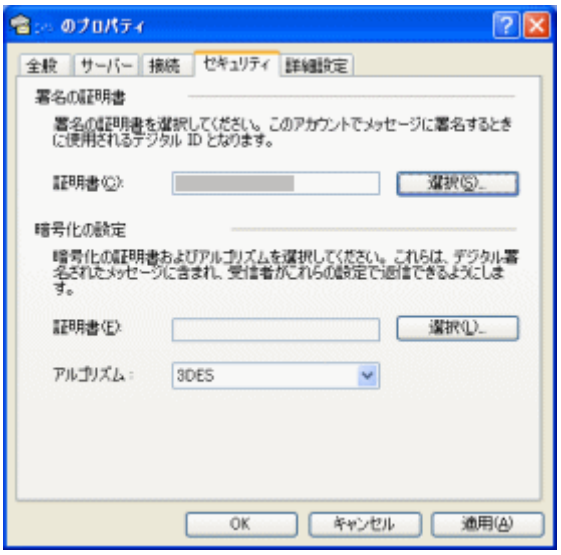


図 103 セキュリティ – 暗号化の設定

10. 次に、下記に示す証明書の選択画面が表示されたら、CSP タイプに TSCSP を指定して取得した電子証明書を選択し、「OK」ボタンをクリックします。

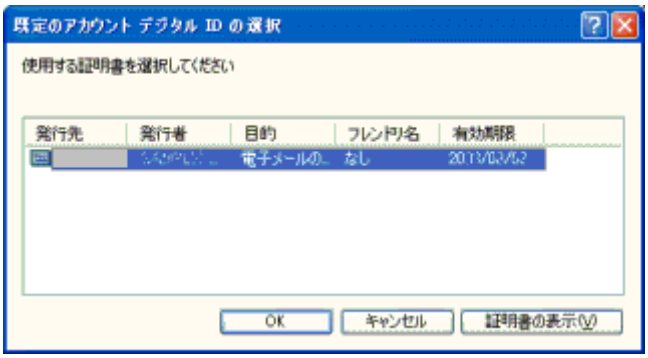


図 104 証明書の選択画面

11. 下記に示すメールアカウントのプロパティ画面に戻ったら、「OK」ボタンをクリックします。

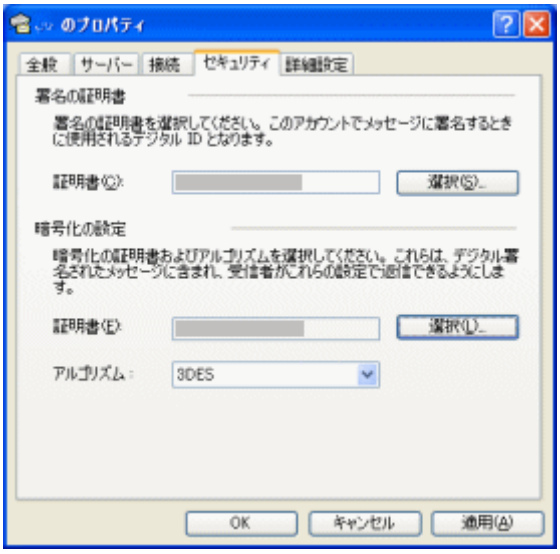


図 105 メールアカウントのプロパティ終了画面

12. 下記に示すインターネットアカウント画面に戻ったら、「閉じる」ボタンをクリックして終了します。

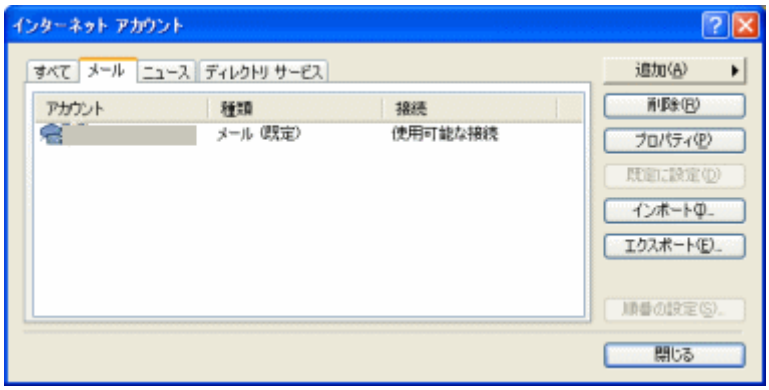


図 106 インターネットアカウント終了画面

e. 証明書ならびに公開/秘密鍵ペアのインポート方法

予め登録したい証明書ファイル（PFX ファイル等）をご用意ください。下記手順に従って、証明書ファイルから証明書ストアにインポートします。

1. TruGate にてログオンするか、TruStack Gina を有効化していない場合は認証デバイスを利用可能にしてください。
2. MMC を起動し、先に作成した証明書コンソールファイルを開き、証明書コンソールを起動します。

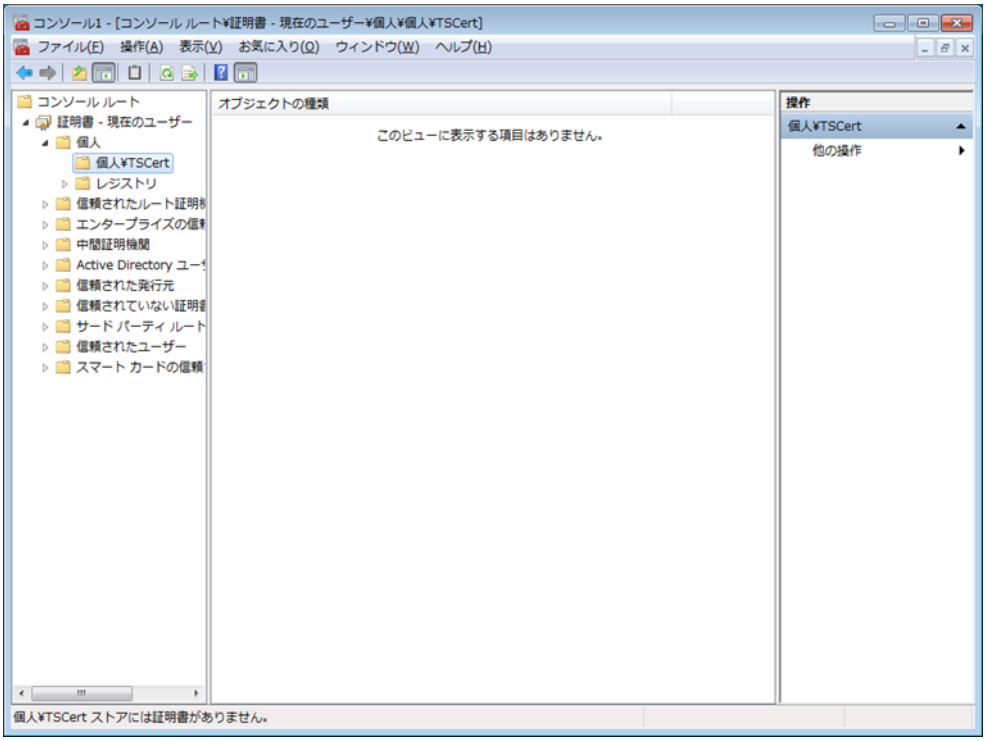


図 107 証明書コンソールの起動

3. 証明書コンソール左側ペインの「個人」–「TSCert」を展開し、右側ペインに証明書が何も表示されないことを確認します。

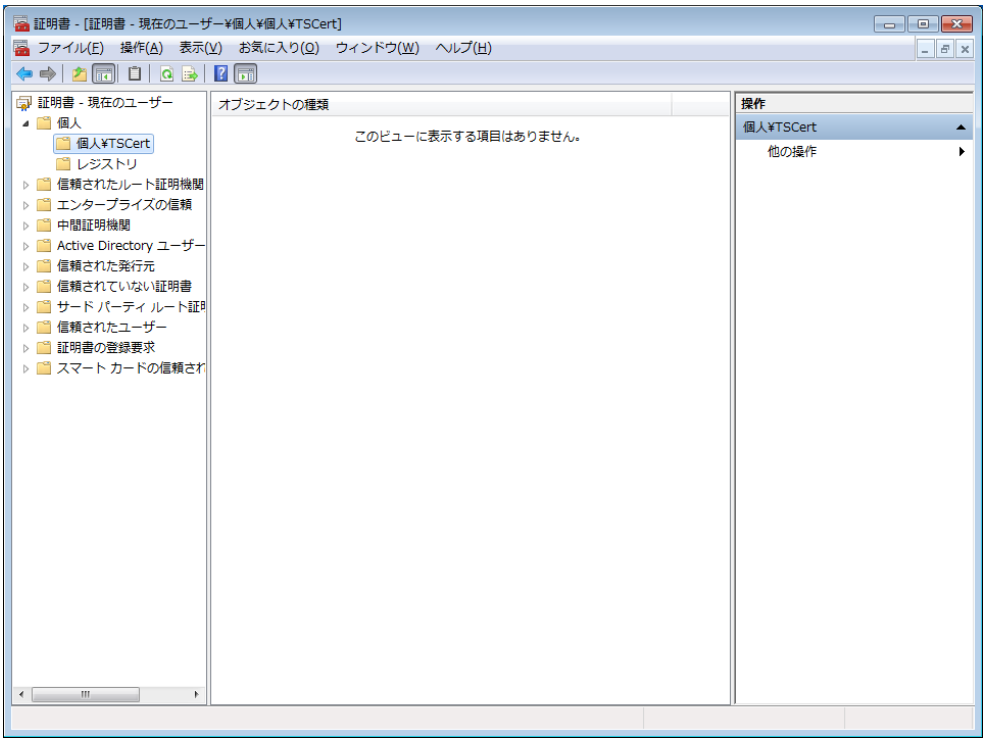


図 108 証明書コンソール画面 ー 証明書未登録

4. 左側ペイン「TSCert」上でマウスを右クリックしてポップアップメニューを表示させ、「すべてのタスク」ー「インポート」を選択します。

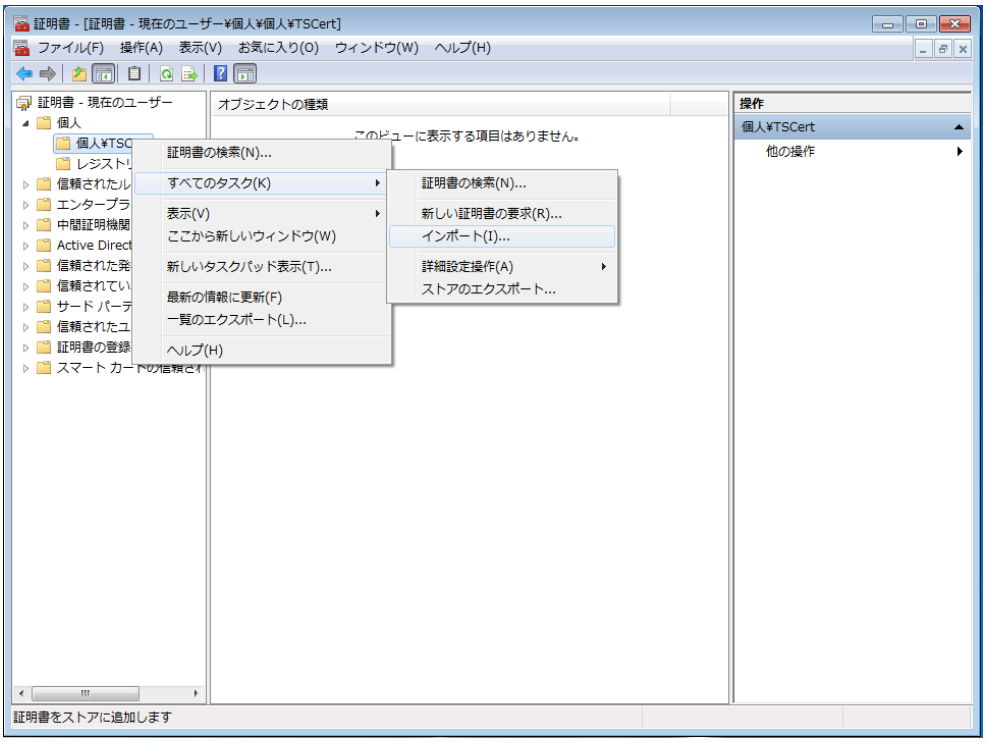


図 109 証明書インポート選択画面

5. 以下、証明書のインポートウィザードに従って操作します。

(ア) 証明書のインポートウィザード画面が表示されたら、「次へ」ボタンをクリックします。

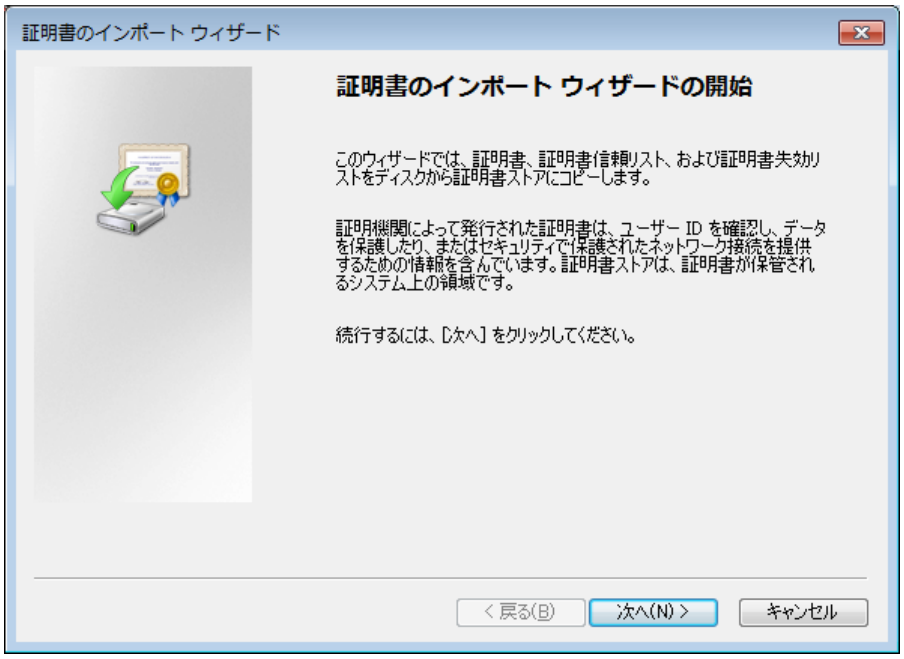


図 110 証明書のインポートウィザード起動画面

(イ) インポートする証明書ファイルの指定画面が表示されたら、「参照」ボタンをクリックし

ます。

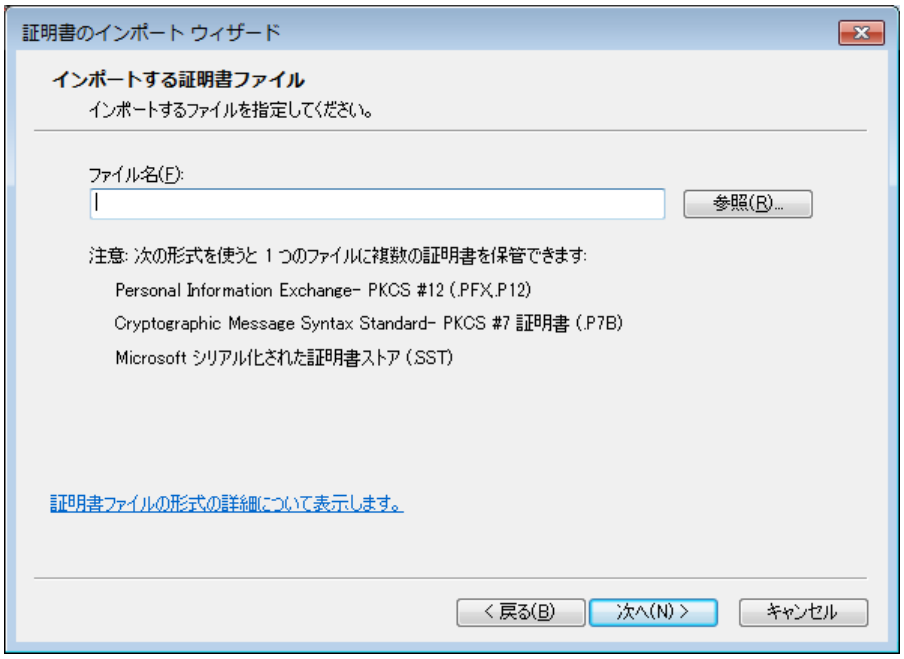


図 111 インポートする証明書ファイル指定画面

(ウ) 保存されている pfx ファイルを指定した後、「開く」ボタンをクリックします

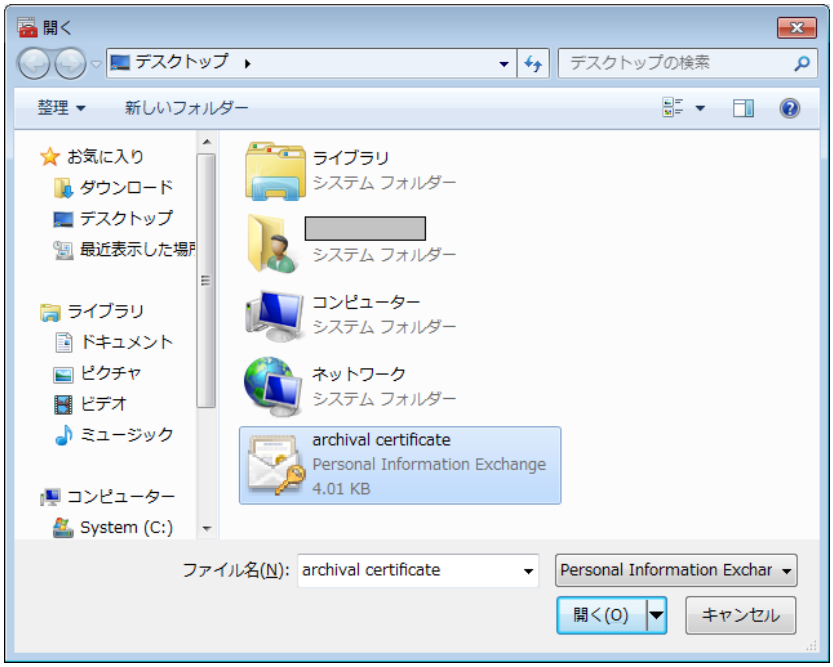


図 112 証明書ファイル選択画面

(エ) インポートする証明書ファイルの指定画面に戻ったら、「次へ」ボタンをクリックします。

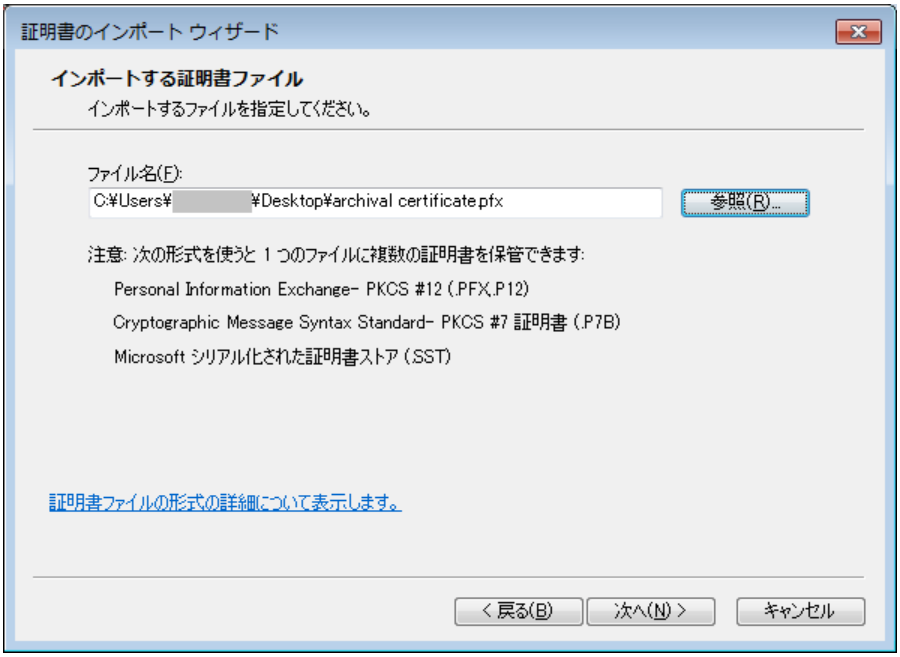


図 113 インポートする証明書ファイル指定画面 ― 指定後

(オ) パスワード入力画面が表示されたら、エクスポート時に設定したパスワードを入力し、「秘密キーの保護を強力にする」、「このキーをエクスポート可能にする」チェックボックスに夫々チェックを入れ、「次へ」ボタンをクリックします。

注）証明書取得時に TruStack Crypt Service Provider 以外の CSP タイプを指定して取得した証明書を TSCert にインポートすると、公開/秘密鍵ペアは TSCSP に格納されません。

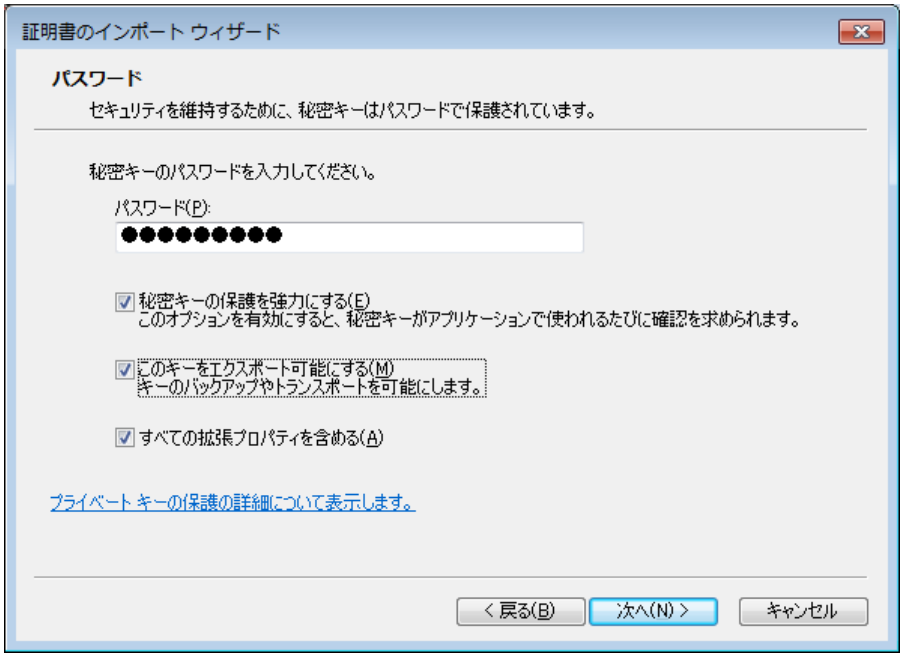


図 114 パスワード入力画面

(カ) 証明書ストア選択画面が表示されたら、「証明書の種類に基づいて、自動的に証明書ストアを選択する」ラジオボタンを選択し、「次へ」ボタンをクリックします。

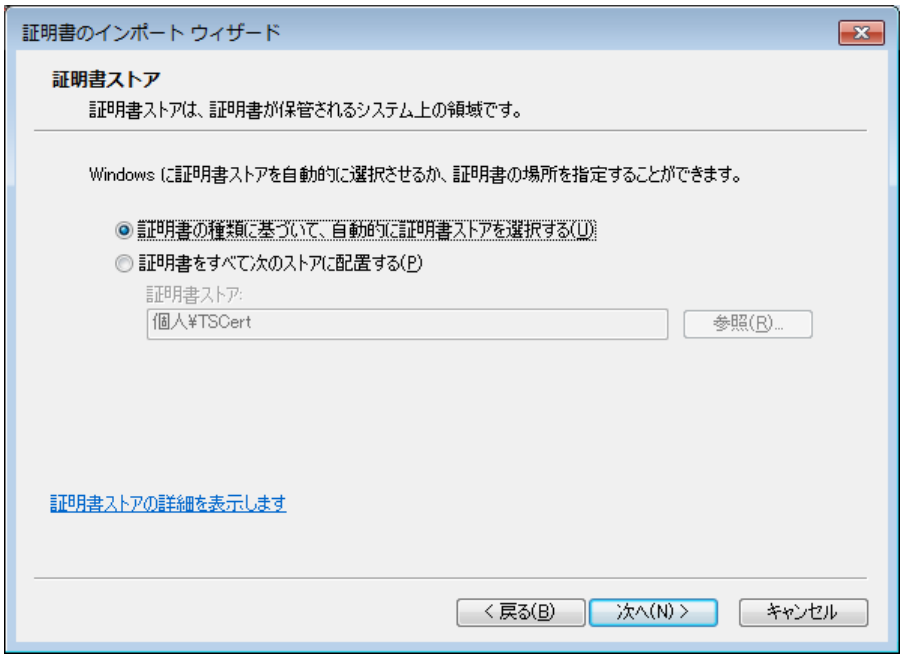


図 115 証明書ストア選択画面

(キ) 証明書のインポート ウィザードの完了画面が表示されたら、「完了」ボタンをクリックします。

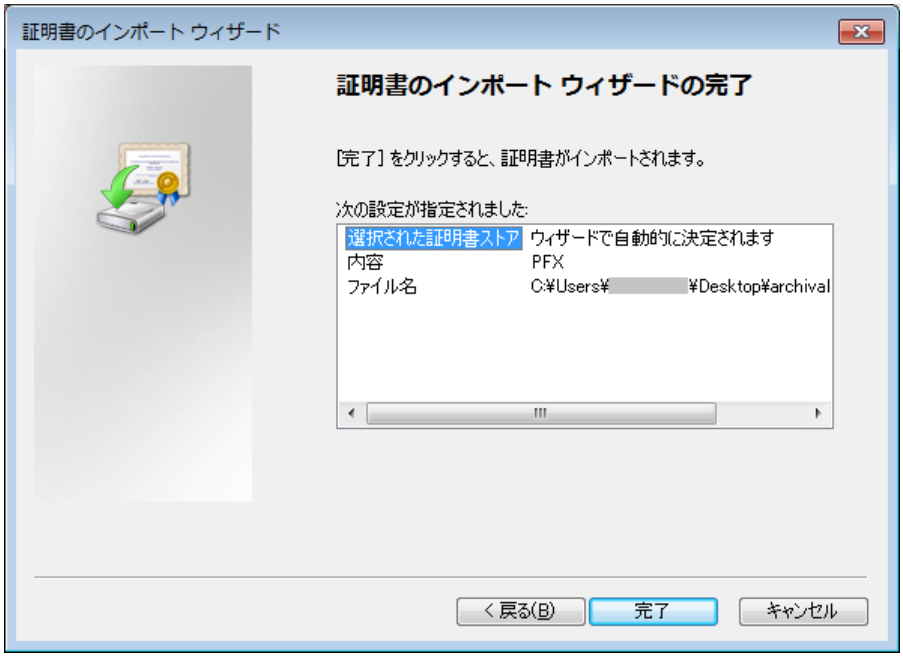


図 116 証明書のインポートウィザード完了画面

(ク) デバイス認証画面が表示された場合は、デバイス認証を行ってください。

(ケ) 正常にインポートされると、下記画面が表示されます。「OK」ボタンをクリックします。

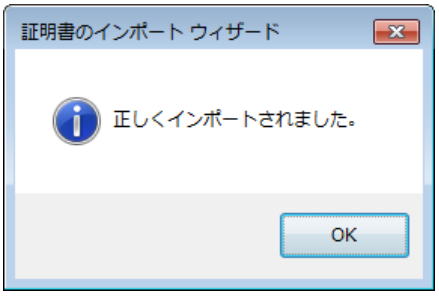


図 117 インポート正常終了確認画面

証明書の格納先として利用される認証デバイスの格納域が空白でなかった場合、下記のようなエラーメッセージが表示されます。

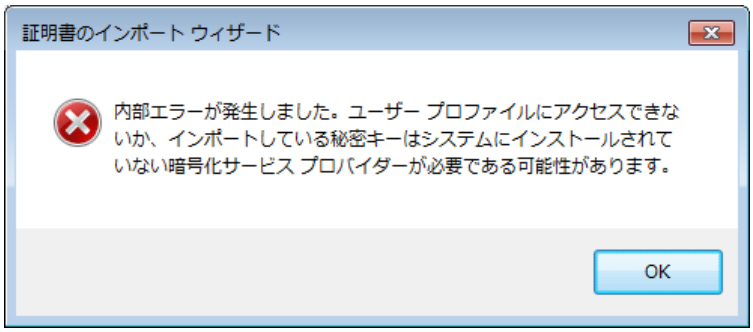


図 118 インポートエラー画面

注）エラーメッセージが表示された際は、認証デバイスの状態を確認し、認証デバイスの接続や格納域の初期化などの作業（証明書要求エラー/インポートエラー発生時の対処方法を参照）を行った上で、再度、証明書のインポートを行ってください。

6. 証明書のインポートが終了し、コンソール画面に戻ったら、証明書コンソール左側ペインの「TSCert」を右クリックしてポップアップメニューを表示させ、「最新の情報に更新」をクリックし、右側ペインに証明書が表示されることを確認します。

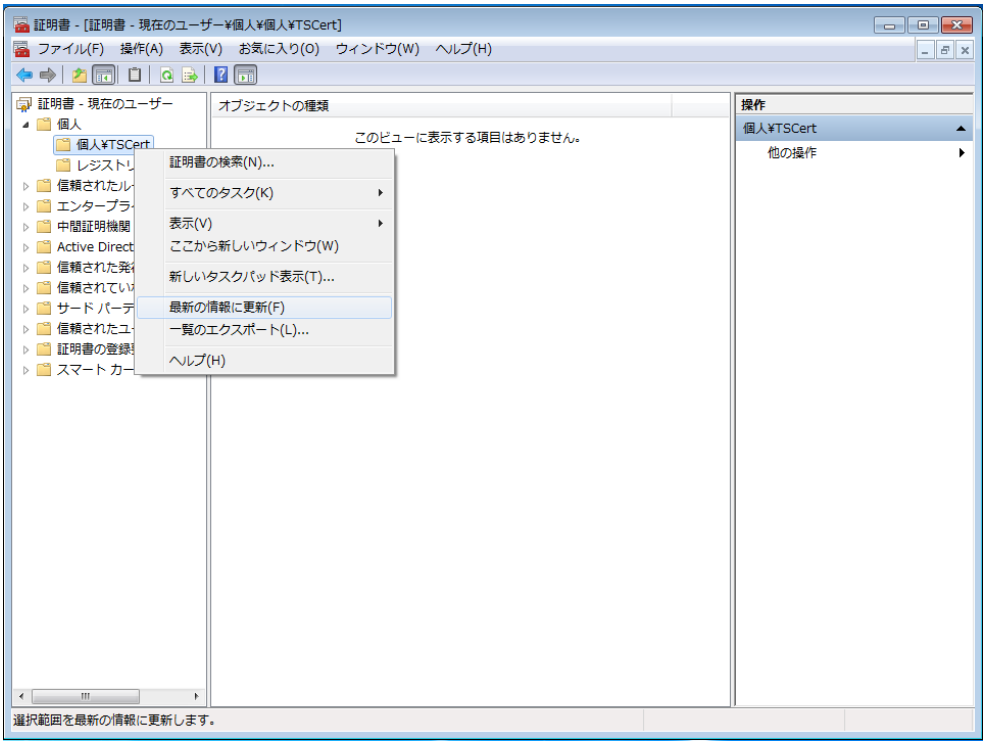


図 119 証明書コンソール画面 ― 最新の情報に更新

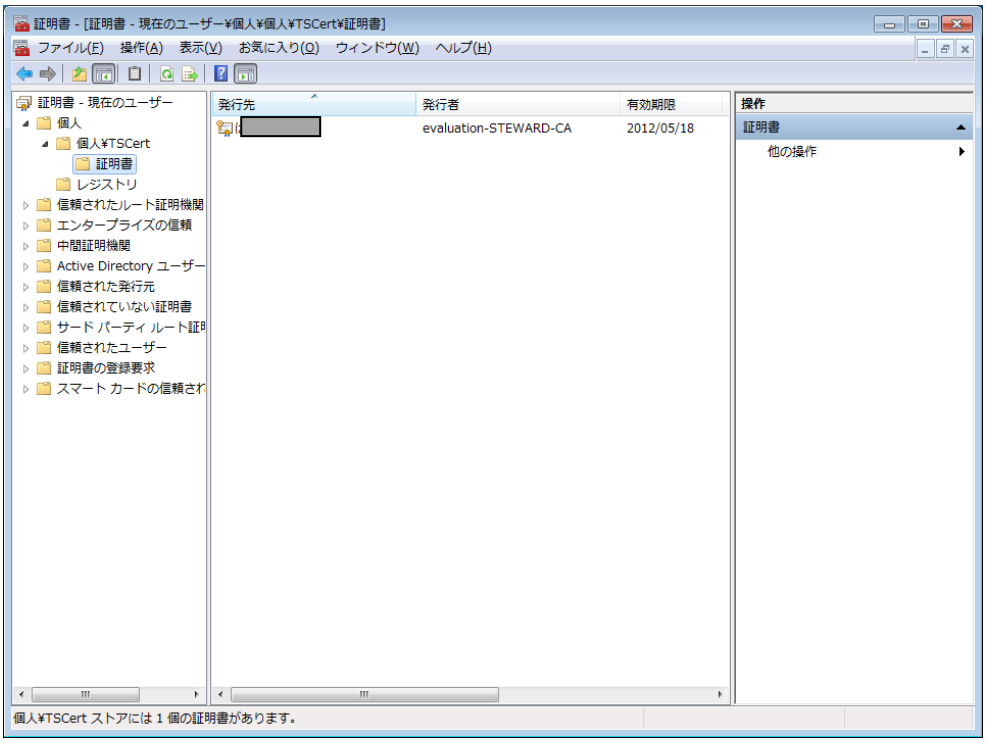


図 120 証明書コンソール画面 ― 証明書の確認

7. 確認できたら、証明書コンソール画面から「ファイル」ー「終了」を選択して終了します。

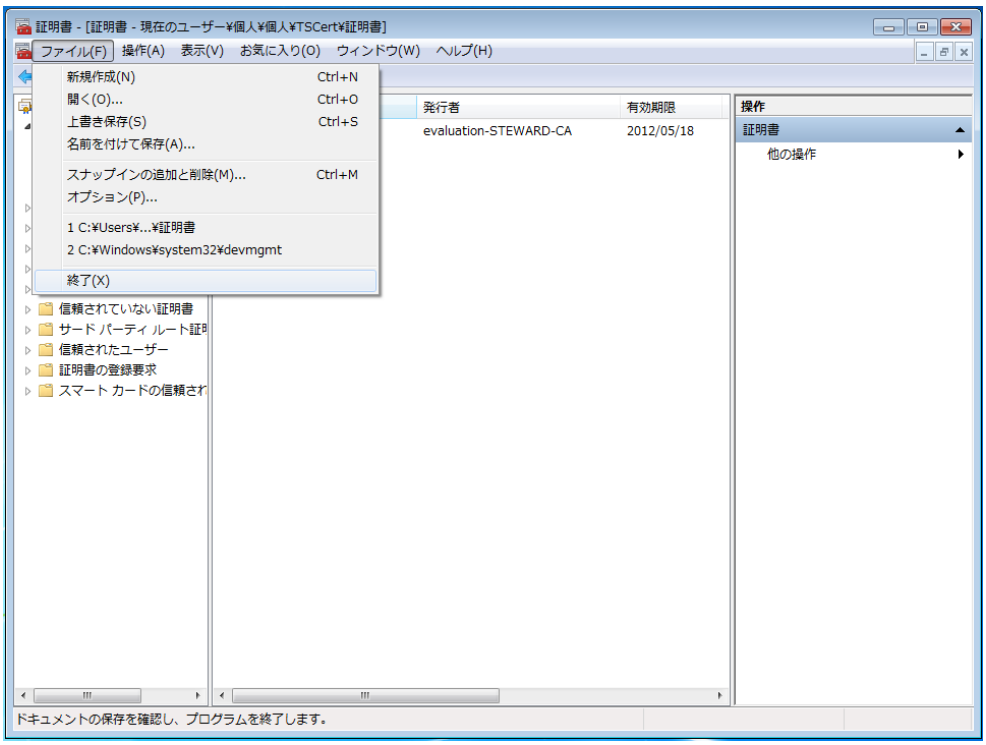


図 121 証明書コンソール画面 ― 終了

f. 証明書ならびに公開/秘密鍵ペアのエクスポートと削除方法

TSCSP で TSCSP の格納域に登録した公開/秘密鍵ペアを削除する場合、下記手順に従って、登録した証明書をエクスポートする際に秘密キーを削除するようにします。

1. TruGate にてログオンするか、TruStack Gina を有効化していない場合は認証デバイスを利用可能にしてください。
2. MMC を起動し、先に作成した証明書コンソールファイルを開き、証明書コンソールを起動します。

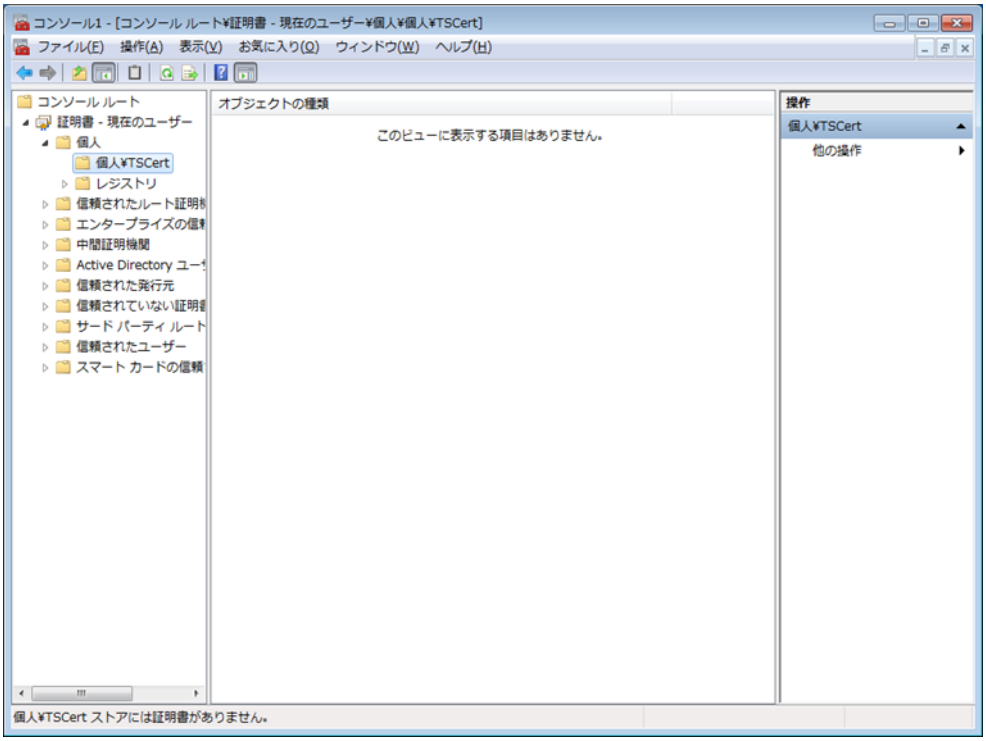


図 122 証明書コンソールの起動

3. 証明書コンソール左側ペインを展開し、右側ペインに削除するキーを含む証明書を表示させます。

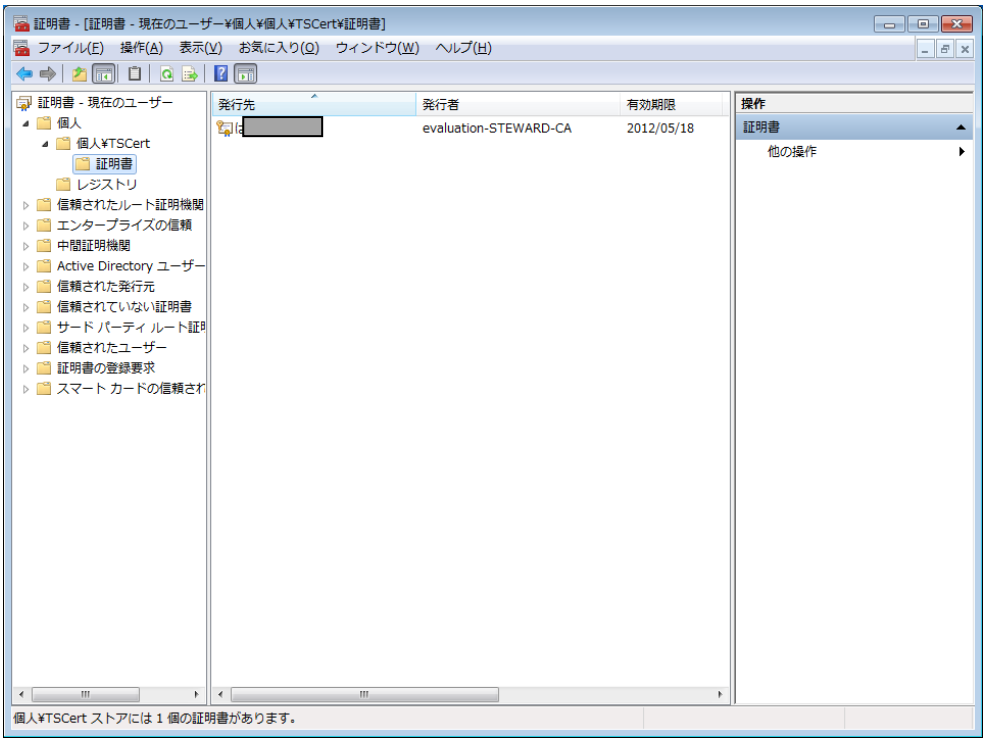


図 123 証明書コンソール画面 ー 証明書の表示

4. 証明書を右クリックし、ポップアップメニューを表示させ、「すべてのタスク」–「エクスポート」を左クリックします。

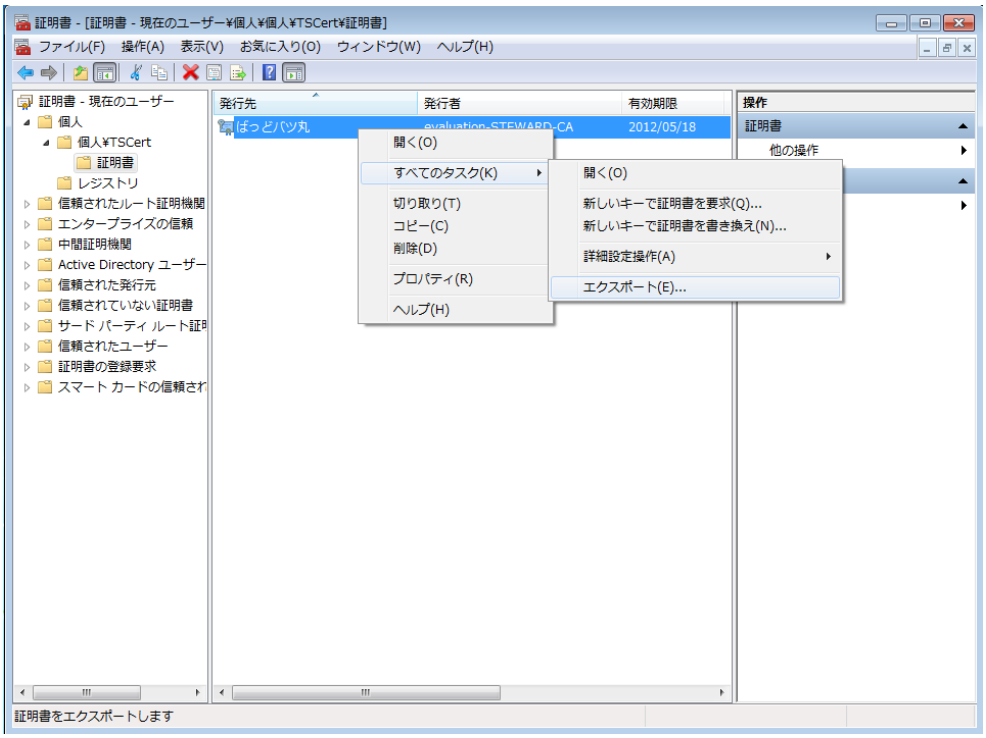


図 124 証明書インポート選択画面

5. 以下、証明書のエクスポートウィザードに従って操作します。

(ア) 証明書のエクスポートウィザード画面が表示されたら、「次へ」ボタンをクリックします。

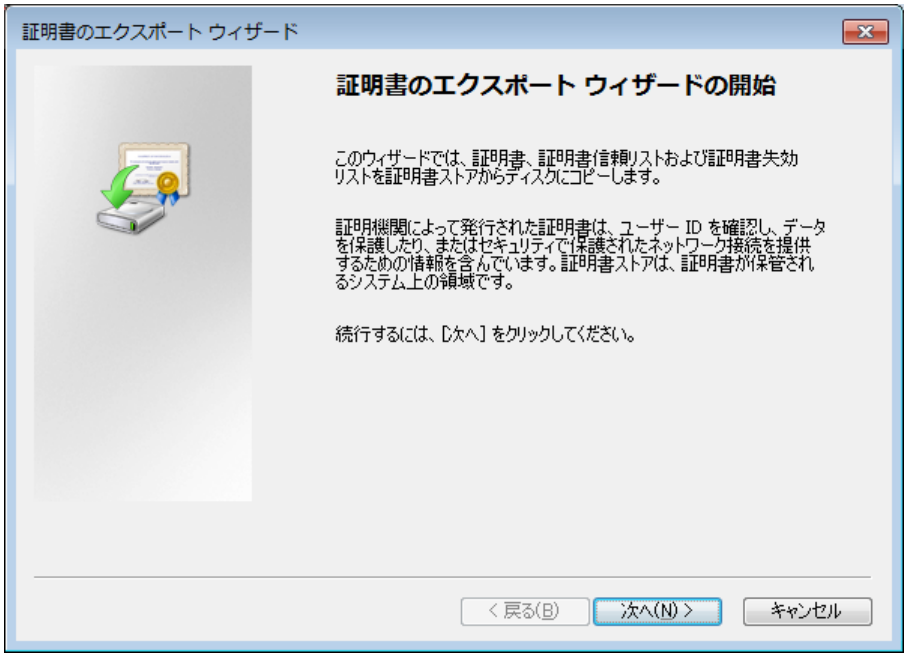


図 125 証明書のエクスポートウィザード起動画面

(イ) 秘密キーのエクスポート指定において、「はい、秘密キーをエクスポートします」ラジオボタンを選択します。

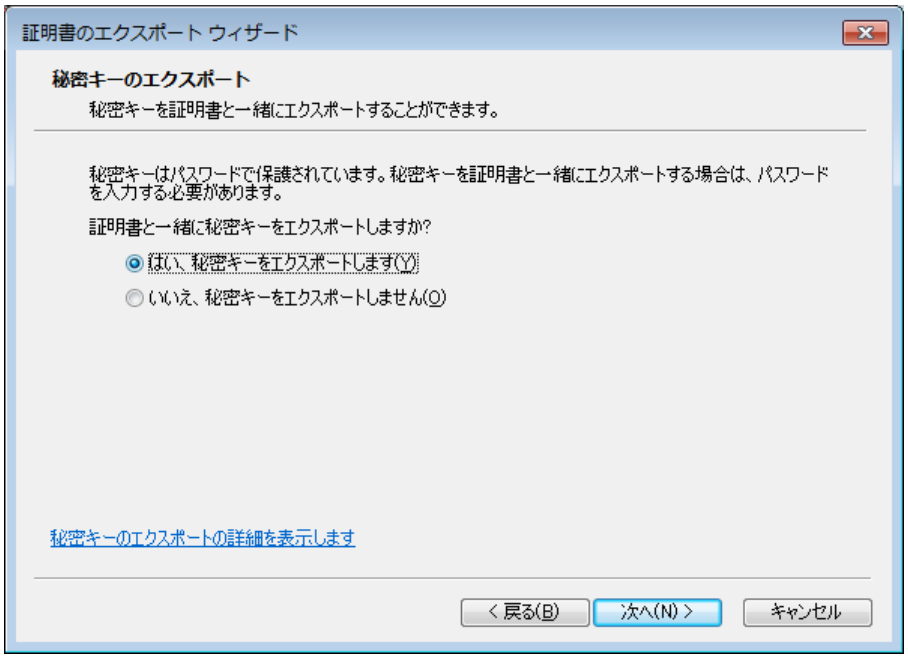


図 126 秘密キーのエクスポート指定画面

(ウ) 引き続くエクスポートファイルの形式指定において、「正しくエクスポートされた時は秘密キーを削除する」チェックボックスをチェックします。

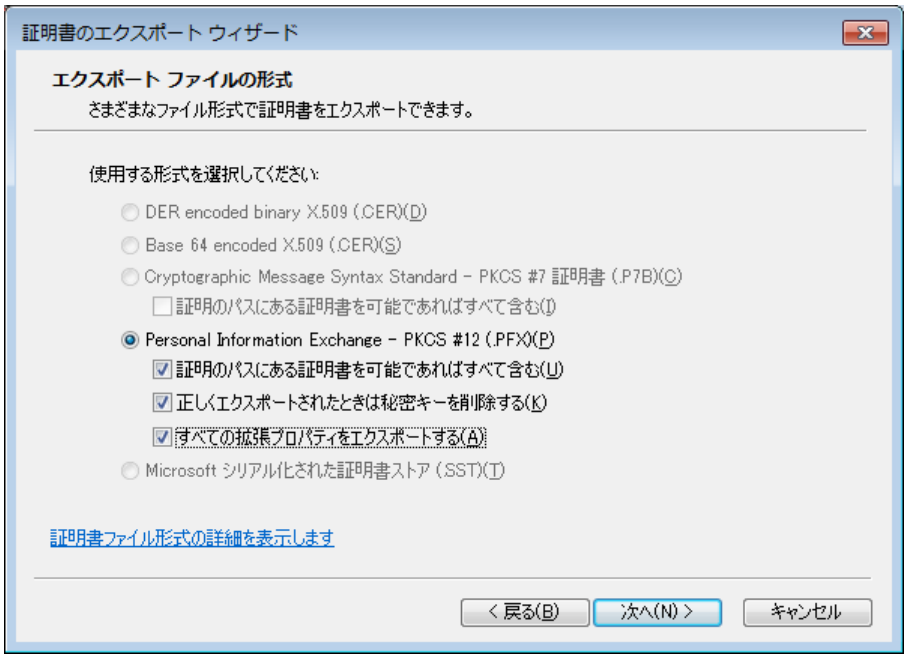


図 127 エクスポートファイルの形式指定画面

(エ) 次に、パスワード入力画面が表示されたら、エクスポートする証明書の秘密キーを保

護するためのパスワードをタイプします。

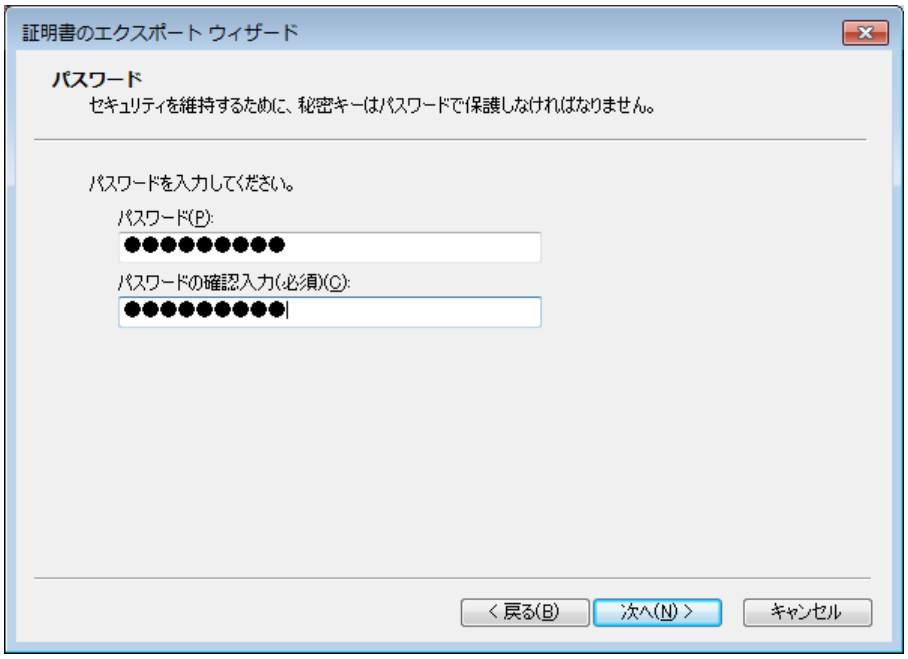


図 128 パスワードの入力画面

(オ) 次に、エクスポートするファイル名の入力画面が表示されたら、「参照」ボタンをクリックします。

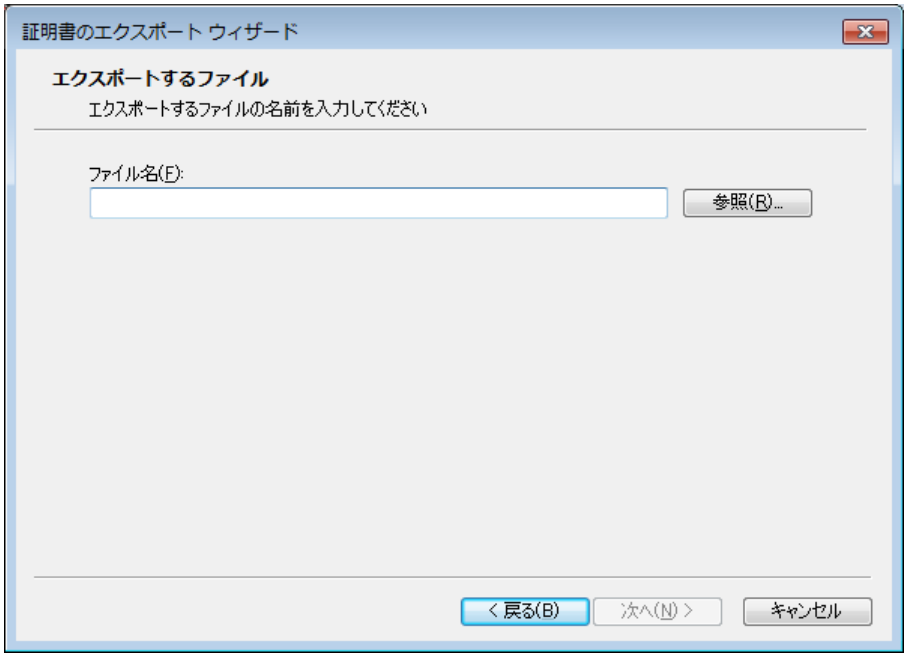


図 129 エクスポートするファイル名入力画面

(カ) 次に、名前を付けて保存画面が表示されたら、ファイル名にエクスポートするファイル名をタイプします。

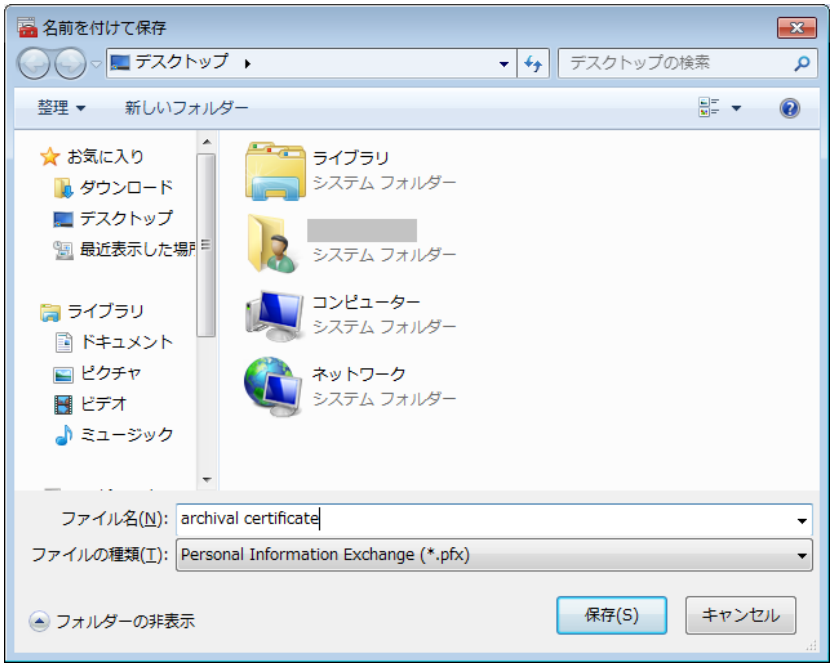


図 130 名前を付けて保存画面

(キ) エクスポートするファイル名の入力画面に戻ったら、「次へ」ボタンをクリックします。

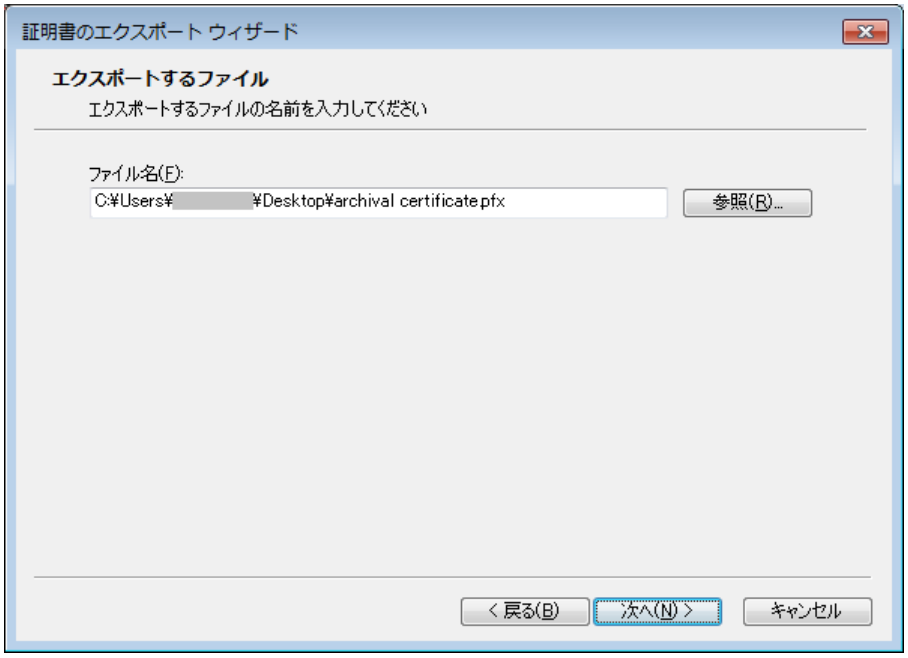


図 131 エクスポートするファイル名指定画面

(ク) 証明書のエクスポート ウィザードの完了画面が表示されたら、「完了」ボタンをクリックします。

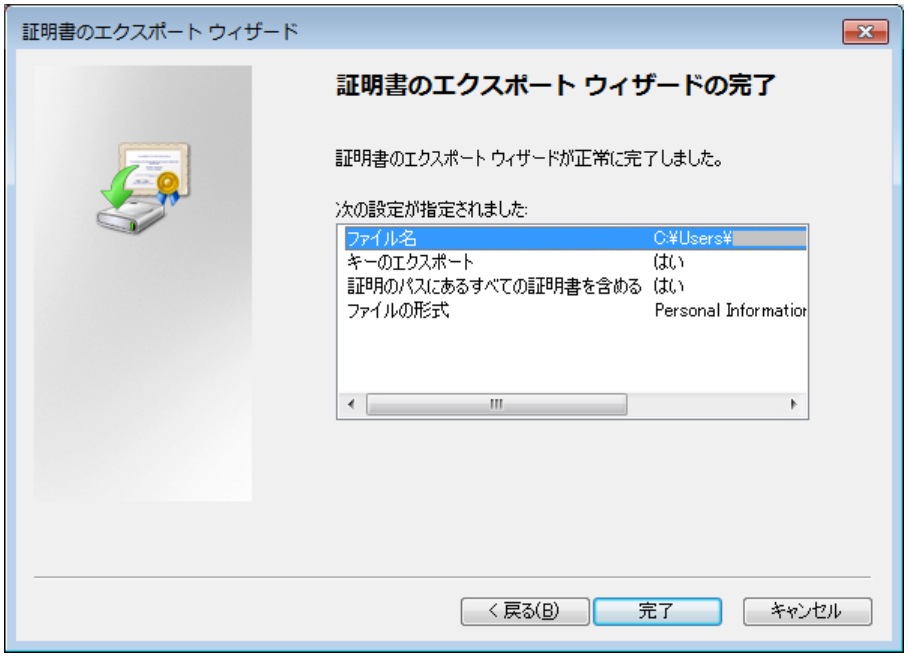


図 132 エクスポートウィザード完了画面

(ケ) デバイス認証画面が表示された場合は、デバイス認証を行ってください。

(コ) 正常にエクスポートされると、下記画面が表示されます。「OK」ボタンをクリックします。

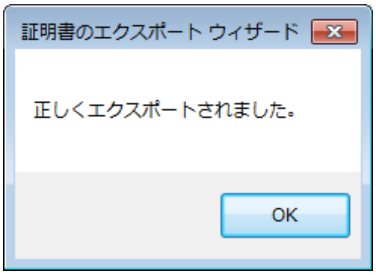


図 133 エクスポート正常終了確認画面

6. 証明書のエクスポートが終了し、証明書コンソールに戻ったら、再度証明書を右クリックしてポップアップメニューを表示させ、「削除」を左クリックして証明書ストアから証明書を削除します。

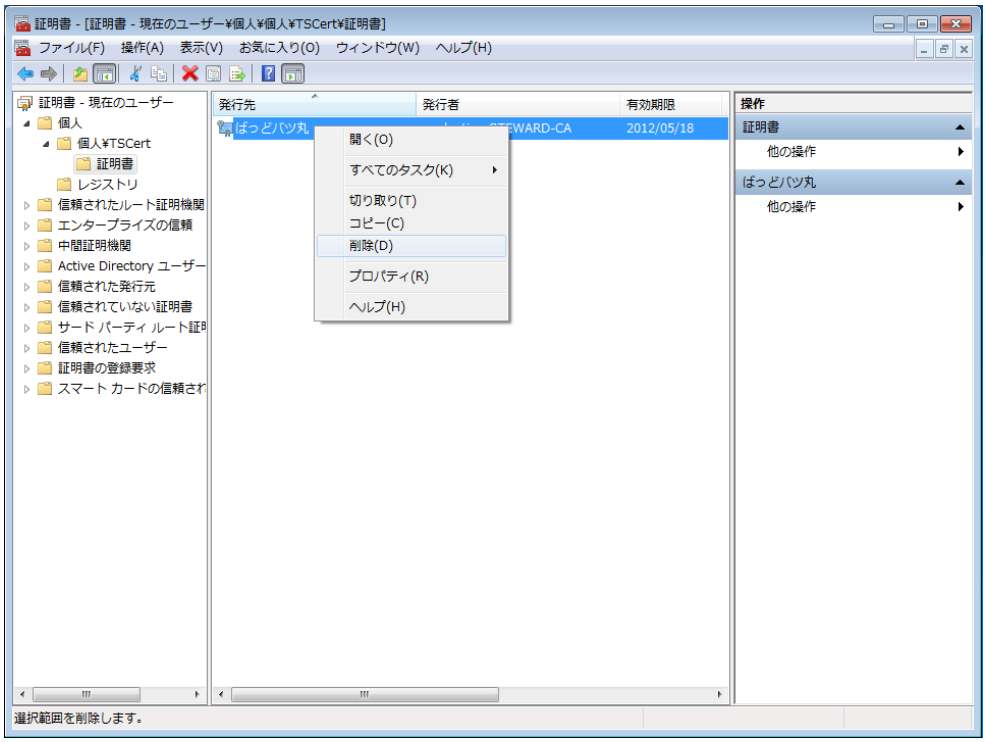


図 134 証明書の削除選択画面

7. 証明書の削除の確認画面が表示されたら、削除する証明書を用いて暗号化されたデータがないことを十分に確認し、ない場合にのみ「はい」ボタンをクリックします。

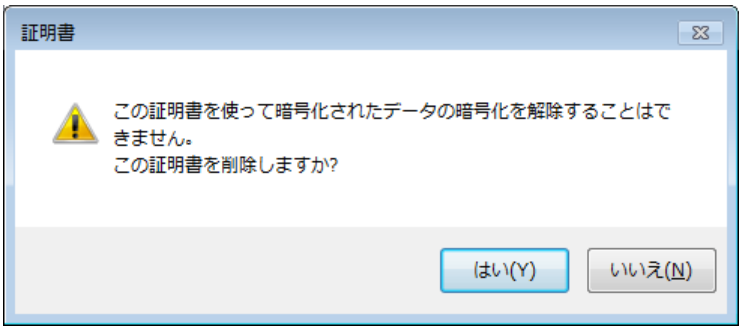


図 135 証明書の削除の確認画面

8. 証明書の削除が終了したら、証明書コンソール左側ペインの「TSCert」を右クリックしてポップアップメニューを表示させ、「最新の情報に更新」をクリックして右側ペインに証明書が何も表示されないことを確認します。

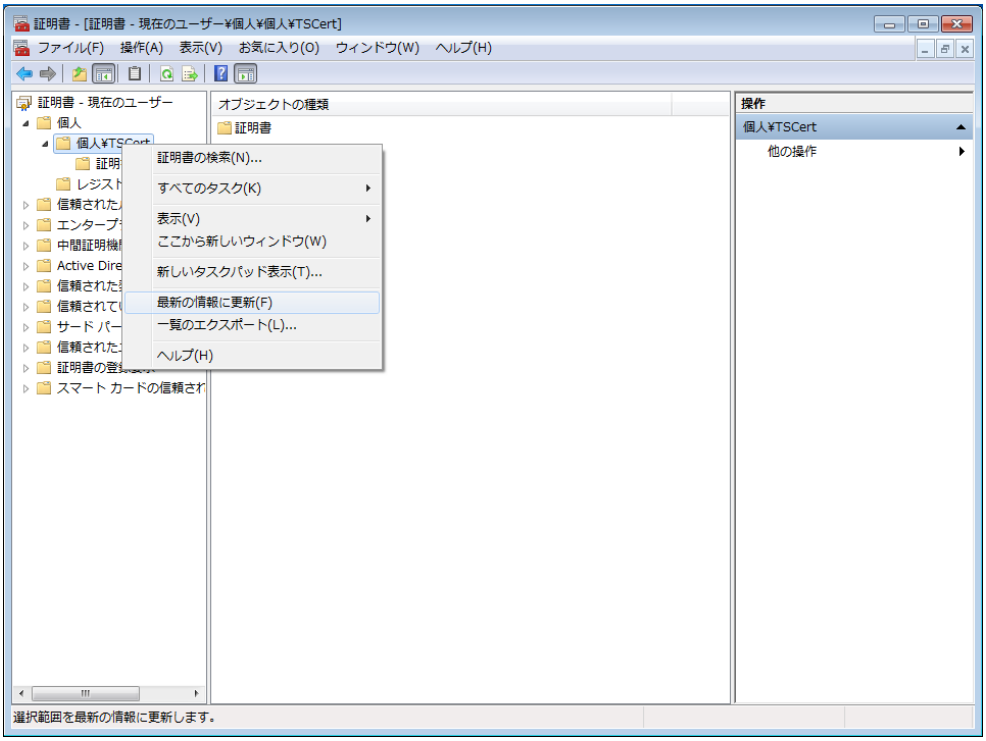


図 136 証明書コンソール画面 ー 最新の情報に更新

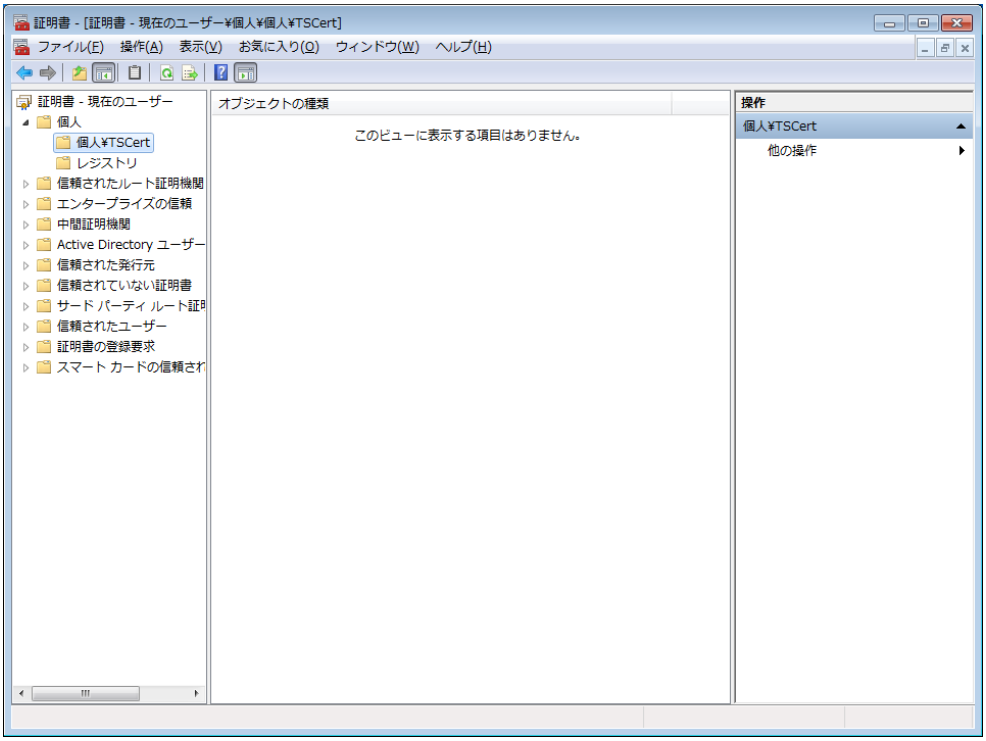


図 137 証明書コンソール画面 ー 証明書削除

9. 確認できたら、証明書コンソール画面から「ファイル」ー「終了」を選択して終了します。

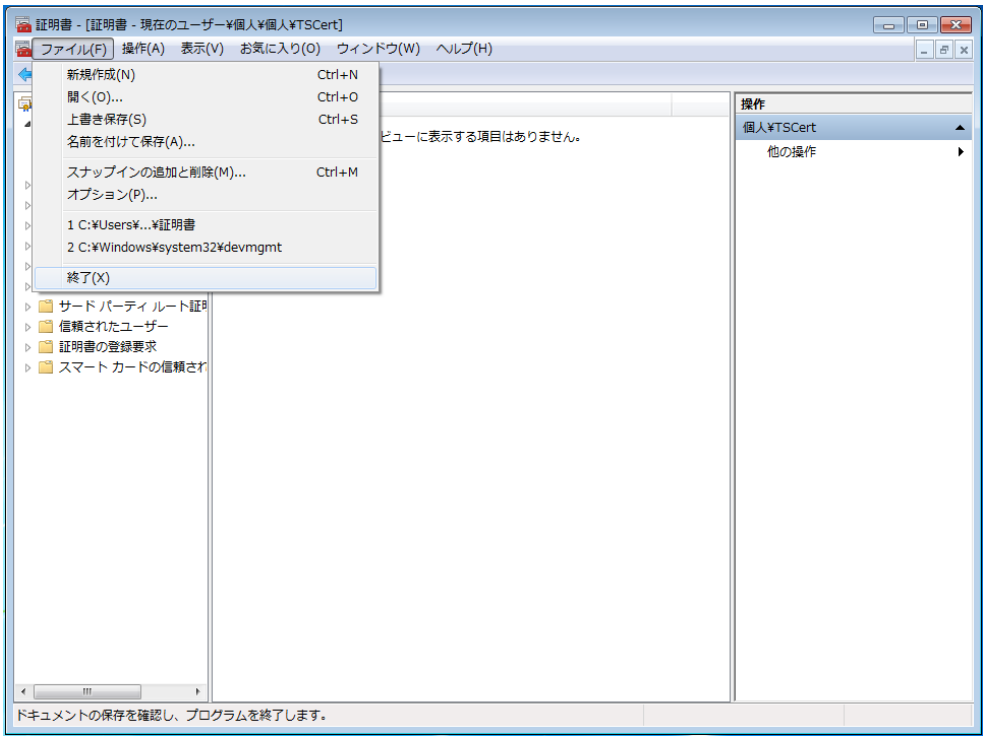


図 138 証明書コンソール画面 ― 終了

g. TruCSP 利用時の認証について

証明書の取得時に CSP タイプとして TruStack Cryptographic Provider を指定し、且つ、秘密キーの強力な保護を指定すると、以降、その証明書がアプリケーションで最初に利用される時に、各認証デバイスに依存したデバイス認証画面が表示されます。
デバイス認証画面が表示されましたら、デバイス認証を行ってください。
デバイス認証に成功すると、証明書の利用が可能となります。デバイス認証に失敗した場合、証明書は利用できません。

注）Administrator などの OS で予め予約されているユーザー名（Well Known Users）で Windows ログオンした場合、認証画面は表示されません。また、利用する認証デバイスによっては、デバイス認証画面が表示されないものがあります。

h. 証明書要求エラー/インポートエラー発生時の対処方法

証明書の要求やインポート時にエラーメッセージが表示された際は、メッセージ画面をクローズし、一旦、証明書の要求やインポート作業を中断した後、下記手順に従ってデータを初期化した上で、証明書の要求やインポートを再度行ってください。
各ユーティリティの使用方法は、TruGate のユーザーズガイドをご参照ください。

1. TruGate に同梱されているクライアント設定ユーティリティを起動します。
2. エラーが発生したユーザーの登録解除を実行します。
3. テンプレートを再度登録します。
4. パスワードを再度設定します。
5. クライアント設定ユーティリティを終了します。

TruGate 管理ユーティリティをご利用の方は、上記ユーティリティの代わりに、TruGate 管理ユーティリティをご使用ください。
ユーティリティの使用方法は、TruGate 管理ユーティリティのユーザーズガイドをご参照ください。

i. 製品登録

i. 製品登録ユーティリティの起動

注） 製品登録ユーティリティの操作は、ローカルコンピュータの管理者権限でログオンして行ってください。

Windows 11 の場合、「スタート」－「すべてのアプリ」－「TruStack」－「TruCSP ライセンス登録」の順にクリックします。

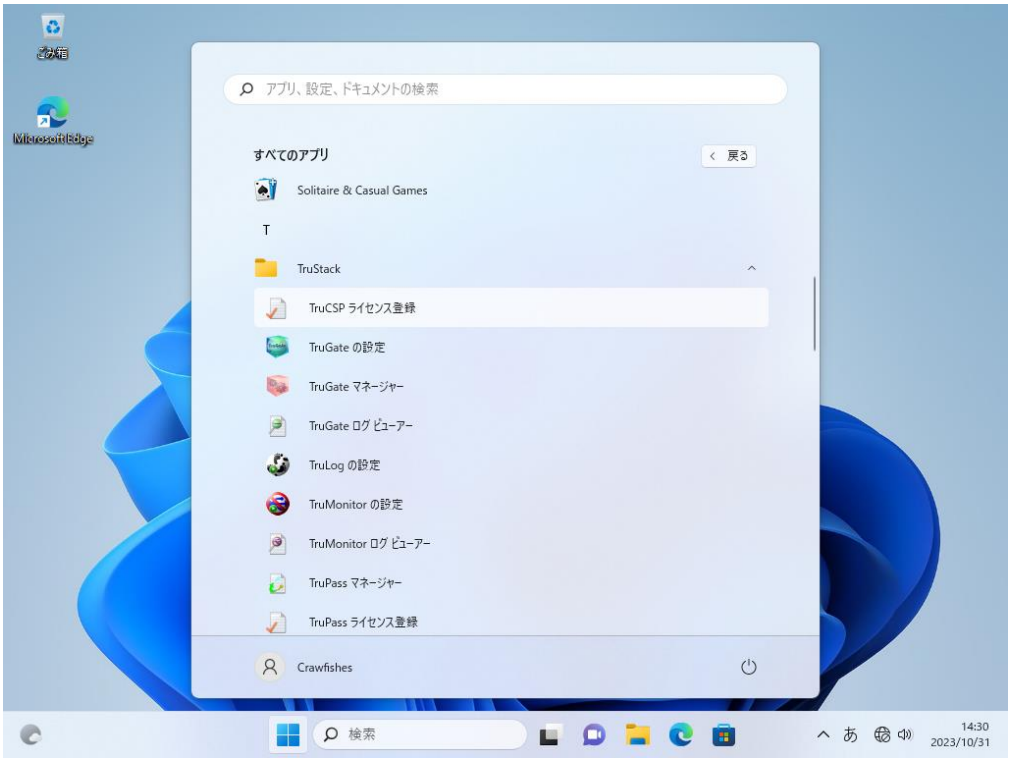


図 139 製品登録ユーティリティの起動

「製品登録」ダイアログが表示されたら、別途入手したプロダクトキーをエディットボックスに入力した後、「OK」ボタンをクリックしてください。「キャンセル」ボタンをクリックすると、製品登録を中止します。

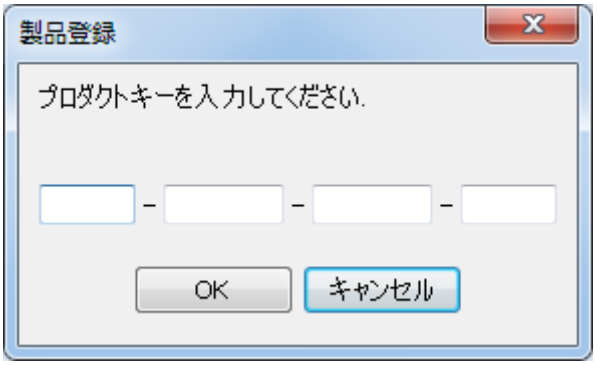


図 140 製品登録画面

製品登録が正常に終了すると下記に示す画面が表示されます。

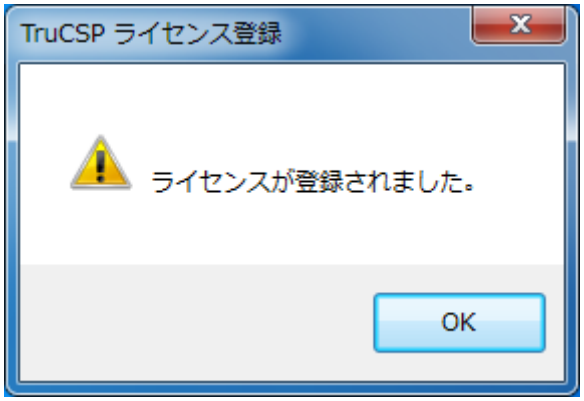


図 141 製品登録終了画面

以上

Trusted Stackware シリーズ製品に関するお問い合わせ
有限会社ディーオーアイネット
〒190-0011
東京都立川市高松町 2-25-23
E-Mail: info@doi-net.com
URL: http://www.doi-net.com/