

1. 電子証明書の新規発行手順の流れ

電子証明書の新規発行手続きの流れについて説明します。

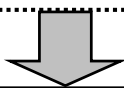
登録申請・更新申請手続き

e-Rad システム運用担当へ申請書等の様式、必要書類を郵送する。



電子証明書発行通知メール

e-Rad システム運用担当から電子証明書発行通知メールが送信されます。



1

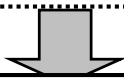
電子証明書を取得（ダウンロード）

電子証明書の新規発行サイトから電子証明書を取得（ダウンロード）します。



電子証明書の配付、電子証明書をインポートするためのパスワードを通知

事務分担者・配分機関担当者に取得（ダウンロード）した電子証明書及び、電子証明書をインポートするためのパスワードを配付します。



2

ご利用のパソコンへの電子証明書のインポート

電子証明書をご利用のパソコンにインポートします。

操作方法⇒「2.2 新しい電子証明書のインポート」参照

- (A) Internet Explorer に電子証明書をインポートする
- (B) FireFox に電子証明書をインポートする
- (C) Safari (Macintosh) に電子証明書をインポートする

メモ

- ・ 電子証明書のインポートは、事務代表者・分担者、配分機関管理者・担当者のそれぞれ個別に行ってください。

2. 操作説明

2.1 電子証明書の取得（ダウンロード）

電子証明書の新規発行ページにアクセスし、電子証明書をダウンロードするまでの操作について説明します。

(A) 電子証明書ダウンロードサイトへアクセスする

- (1) 電子証明書ダウンロードサイトのURLが記載された「e-Rad 電子証明書発行完了のお知らせ」メールがお手元に届きましたら、メールに記載された電子証明書ダウンロードサイトを開く。

【受信されるメールの内容】

いつも e-Rad の運用にご協力いただき、ありがとうございます。
e-Rad で使用する電子証明書について、発行手続きが完了しました。
e-Rad 運用担当より送付した所属研究機関通知書（※1）に記載の
ログイン ID・パスワードを用意いただき、以下リンクより電子証明
書をダウンロード願います。

（※1 新規に機関登録を申請された場合、お手元に通知書が届く
まで2週間程度かかります。）

なお、ダウンロードは本メール送信日から30日以内のみ行えます。
30日を越えるとダウンロードが出来ませんので、ご注意願います。

—【電子証明書ダウンロードサイト】—

<http://www.e-rad.go.jp/certificate/registration.html>

- (2) 「電子証明書は新規発行ページ」ボタンをクリックして電子証明書ダウンロードサイトへアクセスする。



「電子証明書の新規発行について」画面

メモ

- ・ ダウンロードの際、e-Rad 運用担当より送付した所属研究機関通知書または、ログイン情報通知書のログイン ID、パスワードが必要ですので、お手元に準備ください。(新規に機関登録を申請された場合、到着まで2週間程度かかります)。
- ・ セキュリティ上、ダウンロード可能な期間は発行通知メール送信日から30日以内となっておりますので、必ず期限までに行ってください。
- ・ 電子証明書のダウンロードサイトは、毎月第2水曜日の22:00～翌8:00まではメンテナンス作業のため新規発行できません。

(B) 発行済みの電子証明書の取得（ダウンロード）

(1) 「ログイン ID」と「パスワード」を入力してから「Login」ボタンをクリックする。



「ユーザ認証」画面

メモ

- ・ 所属研究機関の場合は、「所属研究機関通知書」に記載された「ログイン ID」と「パスワード」を入力してください。新規に機関登録を申請された場合、「所属研究機関通知書」、「ログイン情報通知書」の到着まで2週間程度かかります。配分機関管理者の場合は、「ログイン情報通知書」に記載された「ログイン ID」と「パスワード」を入力してください。
- ・ 「ログイン ID」と「パスワード」を入力する際は、半角文字にしてください。
- ・ 「ログイン ID」と「パスワード」を入力する際は、大文字と小文字の使い分けにご注意ください。Caps Lock が有効になっていることにより、小文字の代わりに大文字、大文字の代わりに小文字が入力されていないか注意してください。
- ・ 毎月第2水曜日の22:00～翌8:00まではメンテナンス作業のため新規発行できません。

(2) 「電子証明書のダウンロード」リンクをクリックする。



「電子証明書の新規発行」画面

(3) 「発行した電子証明書のダウンロード」ボタンをクリックする。

電子用証明書は1ファイルずつダウンロードします。

Common Name には、機関名称と連番が登録されています。複数ファイルの電子証明書をダウンロードする場合は、Common Name を確認しながらダウンロードしてください。

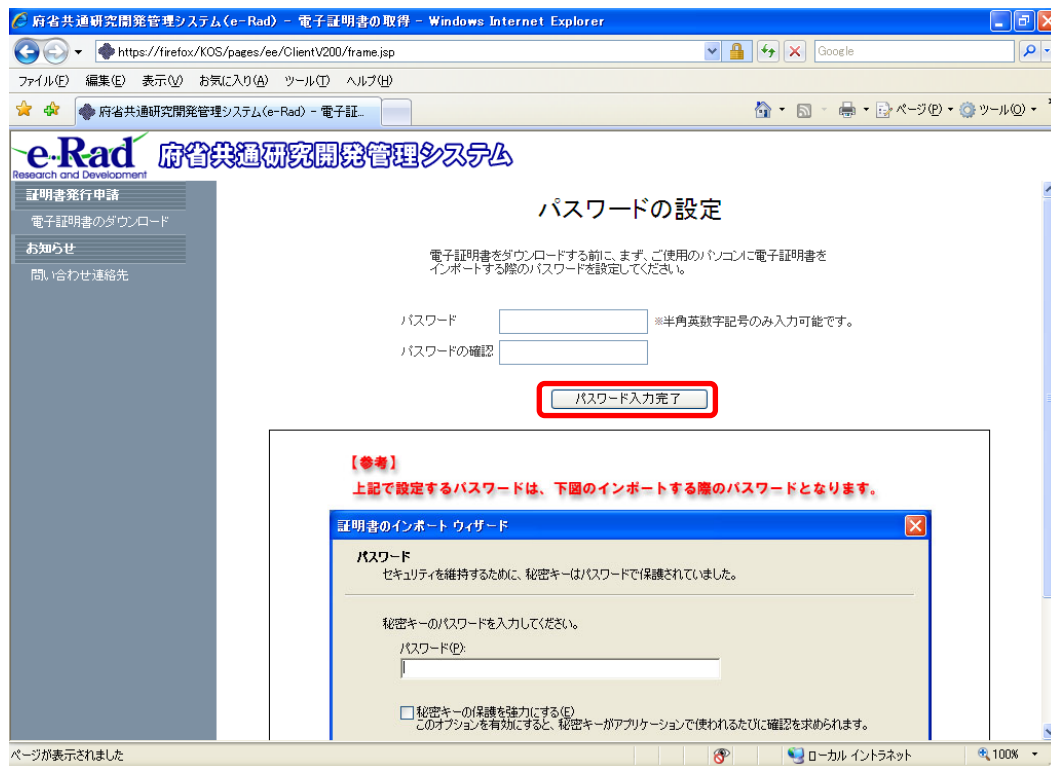


「発行した電子証明書の一覧」画面

メモ

- 発行した電子証明書の一覧は申請順（降順）に表示されます。
- 電子証明書の発行が20件を超える場合は、一覧表示が複数のページに表示されます。その場合、「次ページへ」ボタン、「前ページへ」ボタンが表示されます。
「次ページへ」ボタンをクリックすると次のページに移動することができます。
「前ページへ」ボタンをクリックすると1つ前のページに移動することができます。
- セキュリティ上、ダウンロード可能な期間は証明書発行申請日時から30日以内です。30日を超えると「発行した電子証明書のダウンロード」ボタンは非表示となりダウンロードできません。

- (4) パスワード設定画面が表示されるので、「パスワード」、「パスワードの確認」を入力してから「パスワード入力完了」ボタンをクリックする。

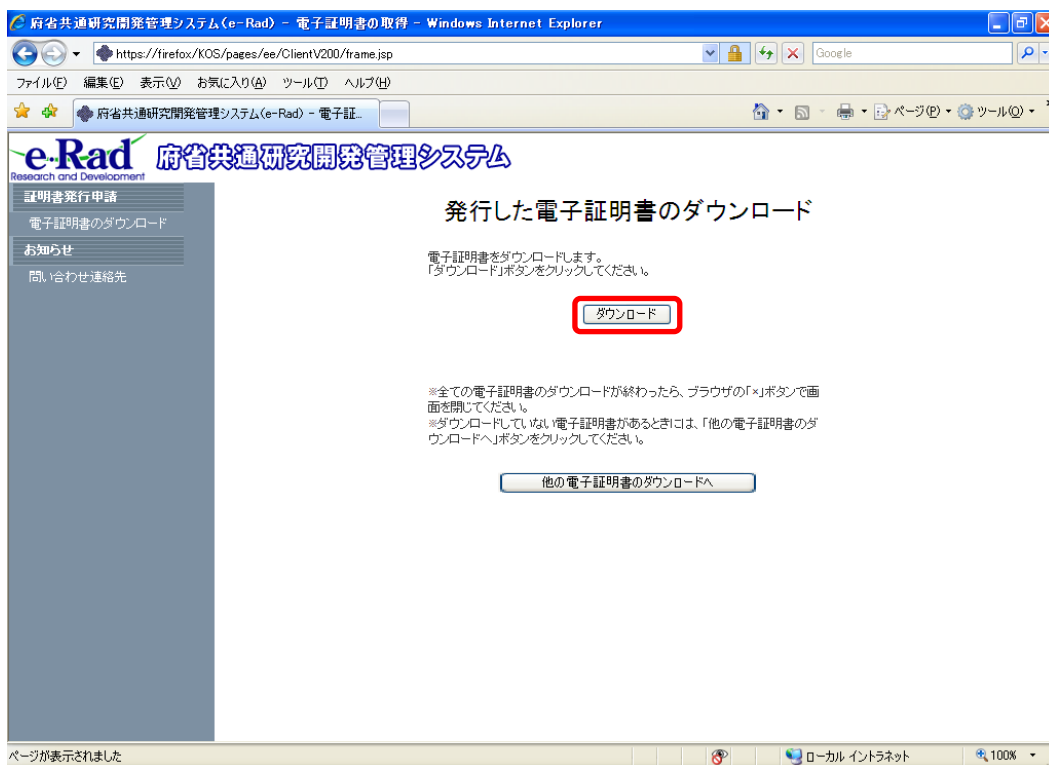


「パスワードの設定」画面

メモ

- ・ 「パスワード」と「パスワードの確認」には、同じパスワードを入力してください。
- ・ パスワードとして入力した英字の大文字と小文字は区別されます。
- ・ 入力したパスワードは電子証明書をインポートする際のパスワードとなりますので、大切に保管し、事務分担者・配分機関担当者へのパスワードの通知は安全・確実に行ってください。
- ・ パスワードは半角英数記号のみ、入力できます。

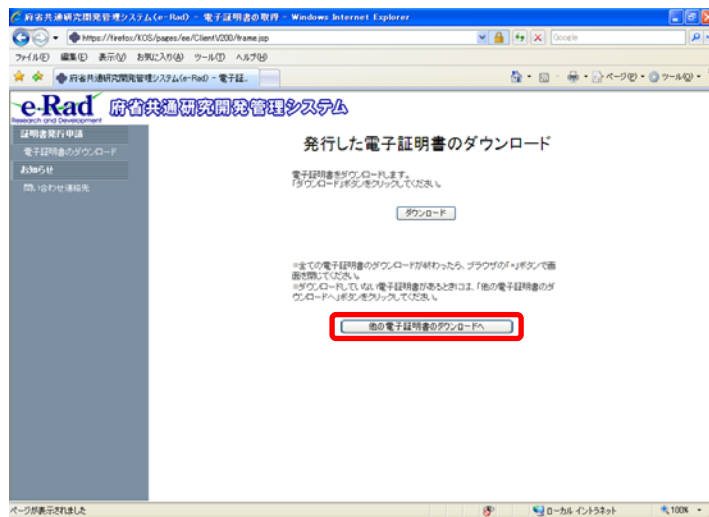
(5) 「ダウンロード」ボタンをクリックして電子証明書をダウンロードする。



「更新した電子証明書のダウンロード」画面

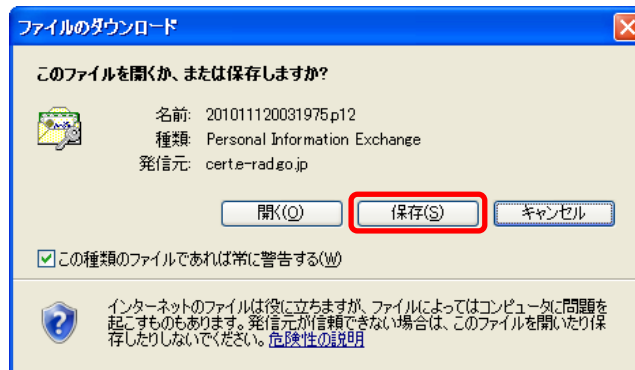
メモ

- ・ 続けて電子証明書ファイルをダウンロードする場合は、「他の電子証明書のダウンロードへ」ボタンをクリックしてください。「発行した電子証明書の一覧」画面が表示されます。

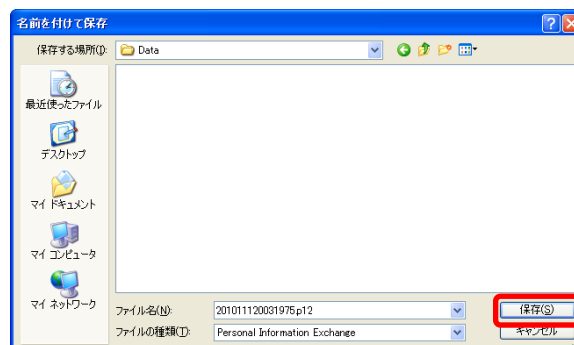


「発行した電子証明書のダウンロード」画面

(6) 電子証明書のダウンロードが開始するので、「保存ボタン」をクリックする。



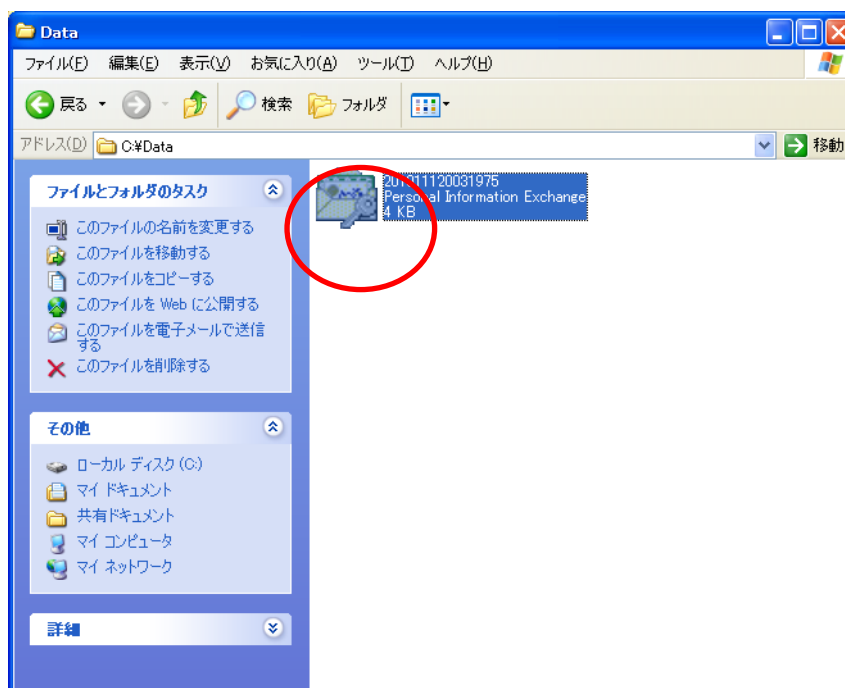
(7) ファイルを保存するフォルダを選択してから「保存」ボタンをクリックする。



メモ

- ・ ダウンロードした電子証明書ファイルの取り扱いには、十分ご注意ください。

(8) 指定したフォルダを開き、正常に保存されているかを確認する。ファイルがあればダウンロードは完了です。



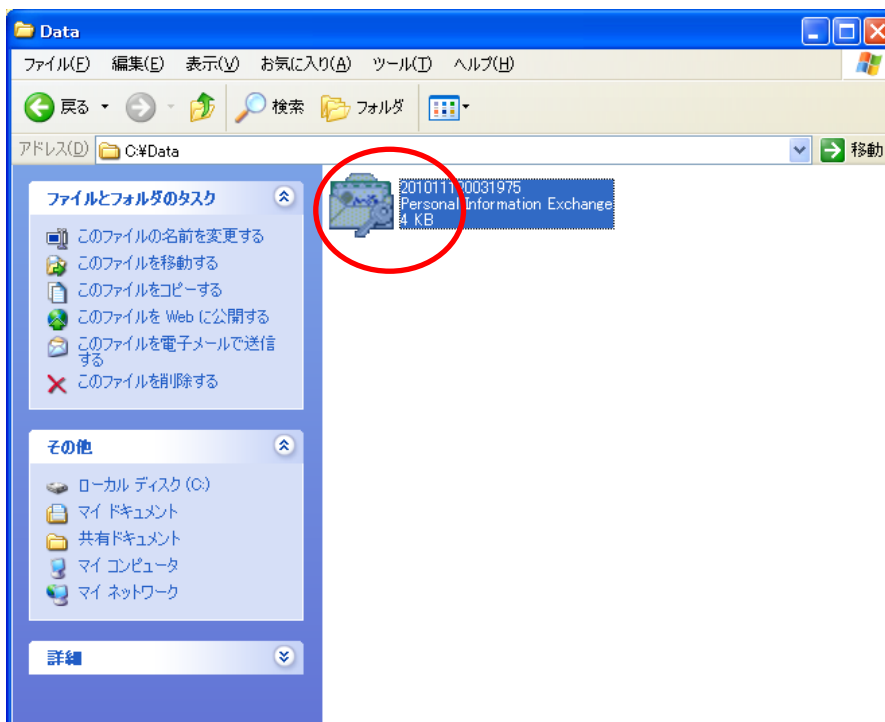
2.2 電子証明書のインポート

メモ

- ・ ダウンロードした電子証明書は大切に保管してください。
- ・ 電子証明書のファイルにはパスワードが設定されています。インポートには電子証明書ファイルと電子証明書ダウンロード時に設定した「パスワード」の入力が必要です。
- ・ パスワードが分からない場合は、事務代表者または、配分機関管理者へお問い合わせください。

(A) Internet Explorerに電子証明書をインポートする

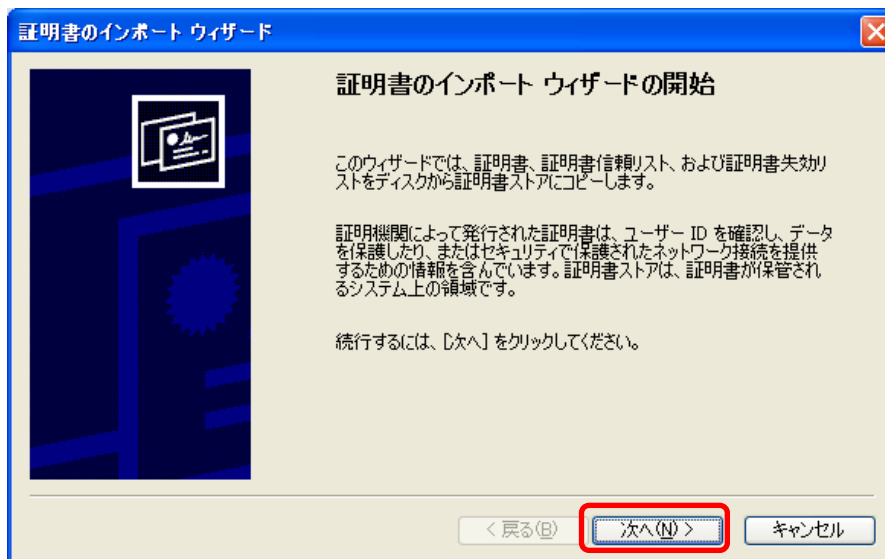
(1) ダウンロードした電子証明書ファイルをダブルクリックする。



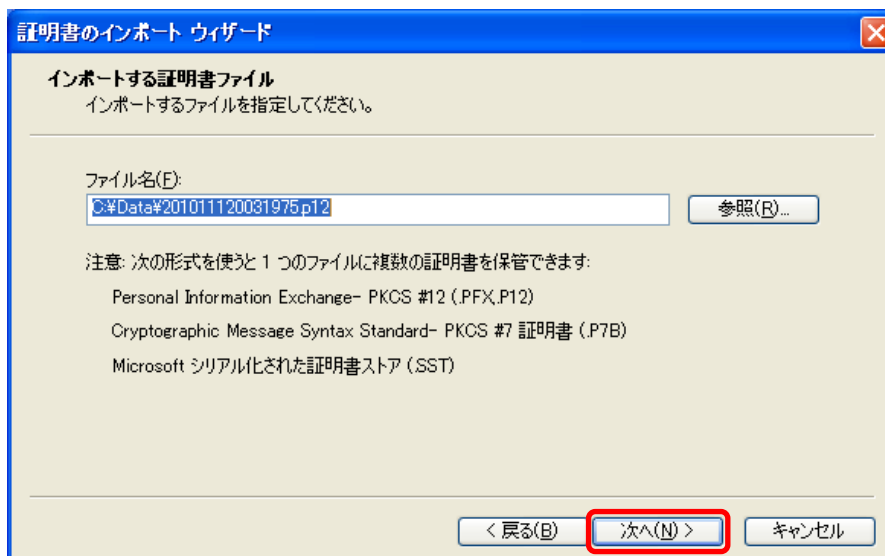
メモ

- ・ 画面は Windows XP、Internet Explorer 7 の例です。OS や Web ブラウザのバージョンにより表示される画面が異なる場合があります。
OS や Web ブラウザのバージョンが異なる場合の操作については、ご利用の Web ブラウザのヘルプや、Web ブラウザのメーカーのホームページ等をご確認ください。

(2) 証明書インポートウィザードが開始するので、「次へ」ボタンをクリックする。



(3) インポートする電子証明書ファイルが選択されていることを確認してから、「次へ」ボタンをクリックする。



- (4) パスワードの入力を求められるので、電子証明書のダウンロード画面で設定したパスワードを秘密キーのパスワードとして入力してから、「次へ」ボタンをクリックする。

The screenshot shows the 'Certificate Import Wizard' dialog box with the title '証明書のインポート ウィザード'. The current step is 'パスワード' (Password). The text reads: 'セキュリティを維持するために、秘密キーはパスワードで保護されていました。' (To maintain security, the private key is protected with a password.) Below this, it says '秘密キーのパスワードを入力してください。' (Enter the password for the private key.) There is a text input field for the password, which contains a series of asterisks. Below the input field are two checkboxes: the first is '秘密キーの保護を強力にする(E)' (Strengthen protection of the private key) with the subtext 'このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。' (If this option is enabled, you will be prompted for confirmation every time the private key is used by an application.); the second is 'このキーをエクスポート可能にする(M)' (Allow this key to be exported) with the subtext 'キーのバックアップやトランスポートを可能にします。' (Allows backup and transport of the key.). At the bottom of the dialog are three buttons: '< 戻る(B)' (Back), '次へ(N) >' (Next), and 'キャンセル' (Cancel). The '次へ(N) >' button is highlighted with a red rectangle.

メモ

- ・ 秘密キーのパスワードは、電子証明書のダウンロード時に設定したパスワードになります。パスワードが分からない場合は、事務代表者または、配分機関管理者へお問い合わせください。

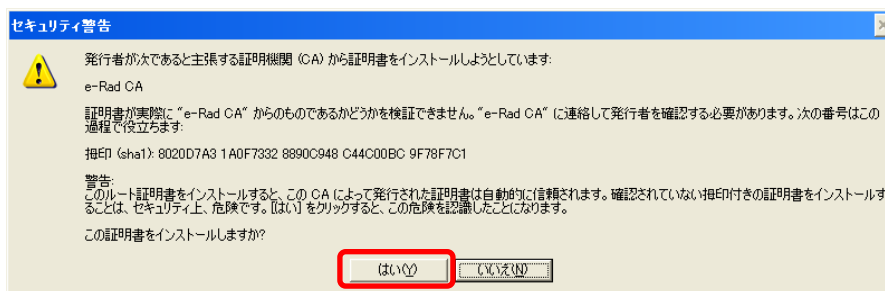
- (5) 「証明書の種類に基づいて、自動的に証明書ストアを選択する」を選択してから、「次へ」ボタンをクリックする。

The screenshot shows the 'Certificate Import Wizard' dialog box with the title '証明書のインポート ウィザード'. The current step is '証明書ストア' (Certificate Store). The text reads: '証明書ストアは、証明書が保管されるシステム上の領域です。' (The certificate store is a system area where certificates are stored.) Below this, it says 'Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。' (You can either let Windows automatically select a certificate store or specify the location of the certificate.) There are two radio button options: the first is '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(O)' (Automatically select a certificate store based on the certificate type), which is selected and highlighted with a red rectangle; the second is '証明書をすべて次のストアに配置する(P)' (Place all certificates in the following store). Below the radio buttons is a text input field for the certificate store name, with a '参照(R)...' (Browse...) button to its right. At the bottom of the dialog are three buttons: '< 戻る(B)' (Back), '次へ(N) >' (Next), and 'キャンセル' (Cancel). The '次へ(N) >' button is highlighted with a red rectangle.

(6) 以下の画面が表示されたら、「完了」ボタンをクリックする。



(7) セキュリティ警告画面に拇印番号が表示され、正しければ「はい」ボタンをクリックする。



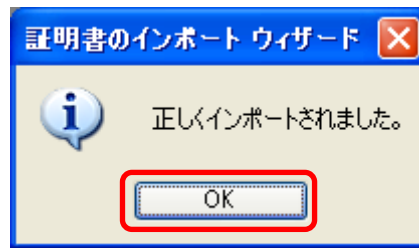
メモ

- ・本システムの正式な電子証明書は、拇印(フィンガープリント)に次のように表示されます。

拇印アルゴリズム	sha1
拇印(フィンガープリント)	80 20 D7 A3 1A 0F 73 32 88 90 C9 48 C4 4C 00 BC 9F 78 F7 C1

- ・拇印(フィンガープリント)は、40桁の16進数であり、「0」～「9」及び「A」～「F」の文字の組合せで示されます。ただし、拇印(フィンガープリント)を表示するソフトウェア(Webブラウザ)により、大文字又は小文字の相違、「:」又はスペースの付加等表示方法が異なることがあります。

(8) 以下の画面が表示されるとインポートは終了です。「OK」ボタンをクリックする。



メモ

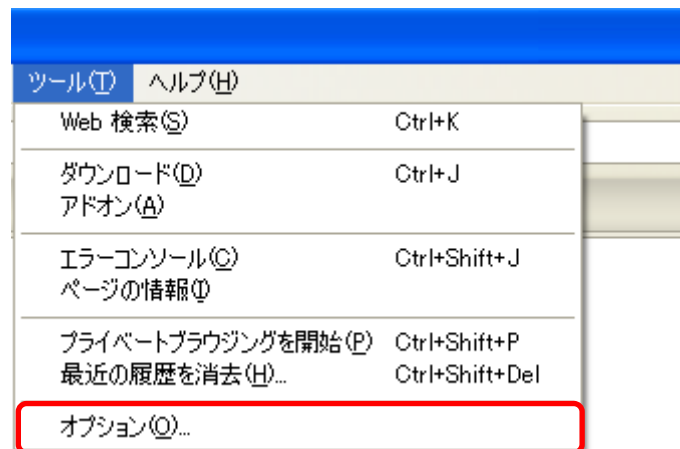
- ・ 電子証明書をインポートできない場合は、ヘルプデスクにご連絡ください。
- ・ セキュリティ警告に文字列が表示されない場合、以下の①又は②の要因が考えられます。
 - ① PC のアカウントに管理者権限が存在しない（対応：管理者権限を付与して下さい）
 - ② 特定の動作環境で特定のセキュリティパッチが適用されている（対応：修正プログラムを適用して下さい※）

※修正プログラムを適用する際は、以下のURLに記載されている内容について、各機関のシステム部門に確認の上、修正プログラムの適用を行って頂く必要があります。

（参考）<http://support.microsoft.com/kb/940275/ja>

(B) FireFoxに電子証明書をインポートする

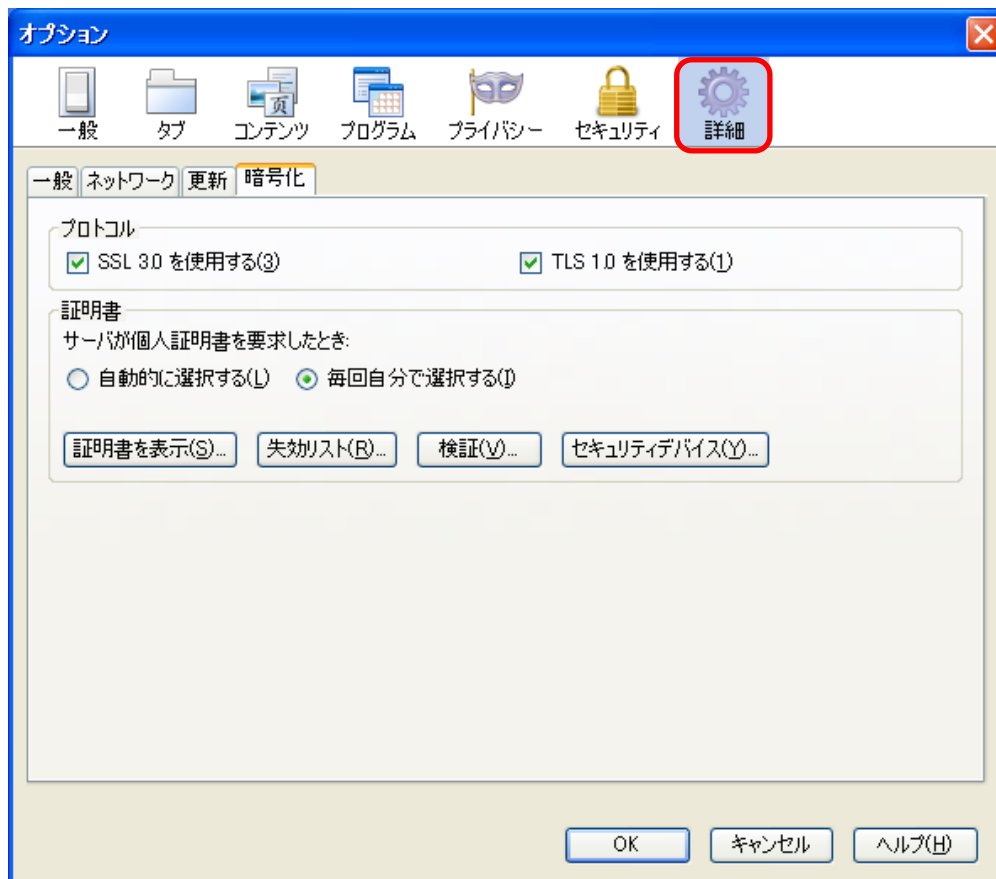
(1) FireFox を起動してから、「ツール」 - 「オプション」を選択する。



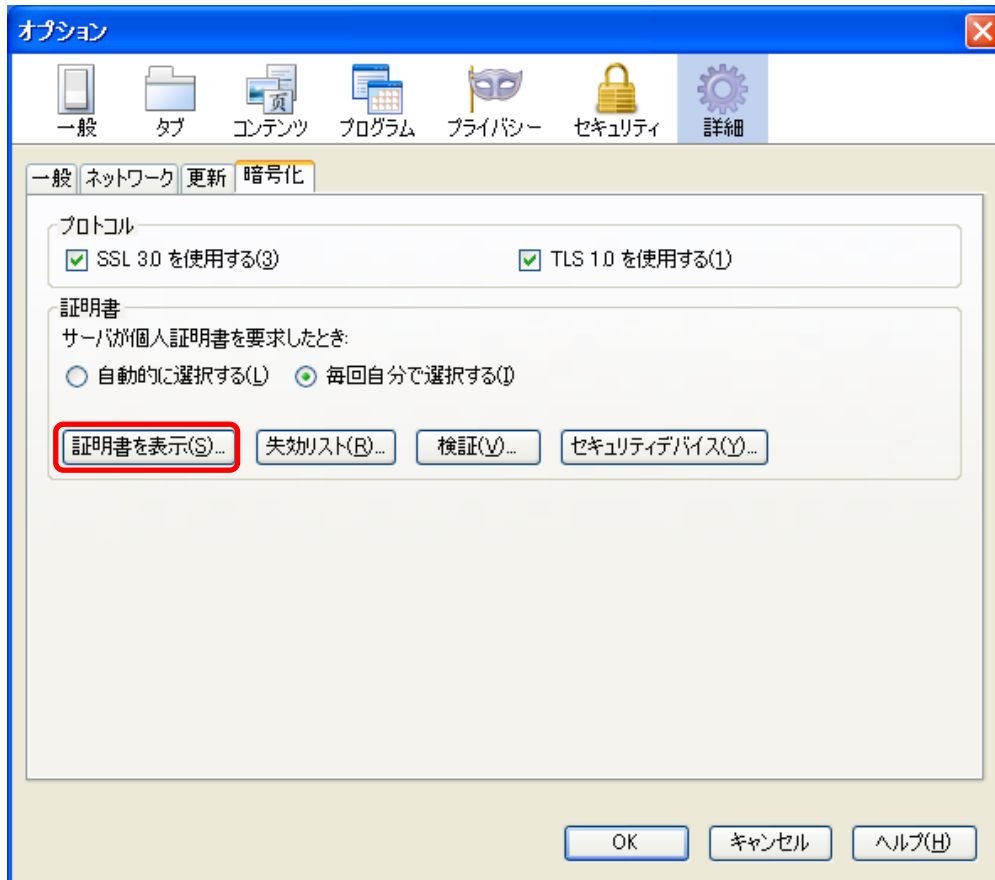
メモ

- ・画面は Windows XP、Firefox 3.6 の例です。OS や Web ブラウザのバージョンにより表示される画面が異なる場合もあります。
- OS や Web ブラウザのバージョンが異なる場合の操作については、ご利用の Web ブラウザのヘルプや、Web ブラウザのメーカーのホームページ等をご確認ください。

(2) 上部のアイコンで「詳細」を選択する。



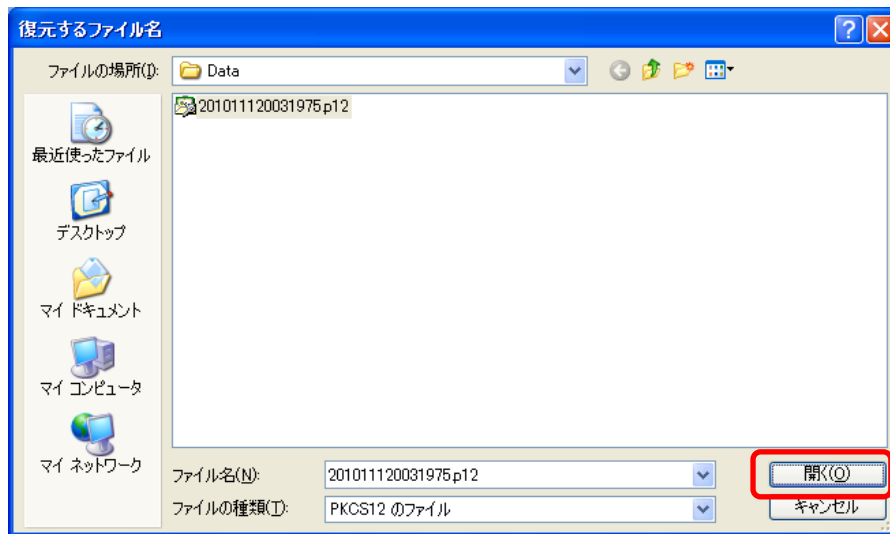
(3) 「証明書を表示」ボタンをクリックする。



(4) 「インポート」ボタンをクリックする。



(5) 電子証明書ファイルを選択してから、「開く」ボタンをクリックする。

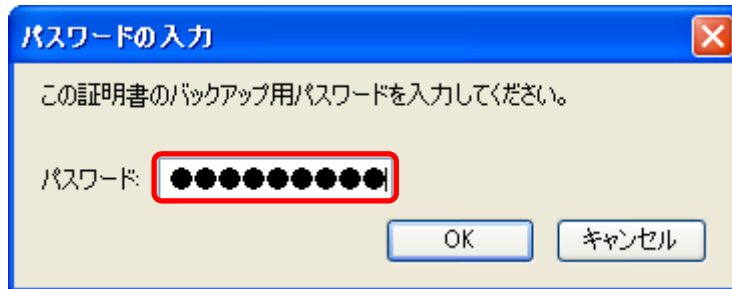


メモ

・「パスワードを入力してください」画面が表示された場合は、Firefox のマスターパスワードが設定されています。設定済みのマスターパスワードを入力してから「OK」ボタンをクリックしてください。



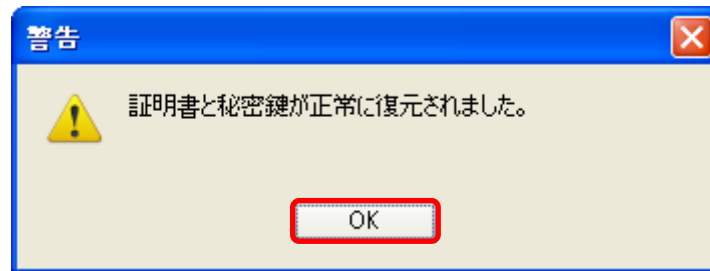
- (6) パスワードの入力を求められるので、電子証明書のダウンロード画面で設定したパスワードを入力してから、「OK」ボタンをクリックする。



メモ

- 電子証明書のダウンロード時に設定したパスワードになります。
パスワードが分からない場合は、事務代表者または、配分機関管理者へお問い合わせください。

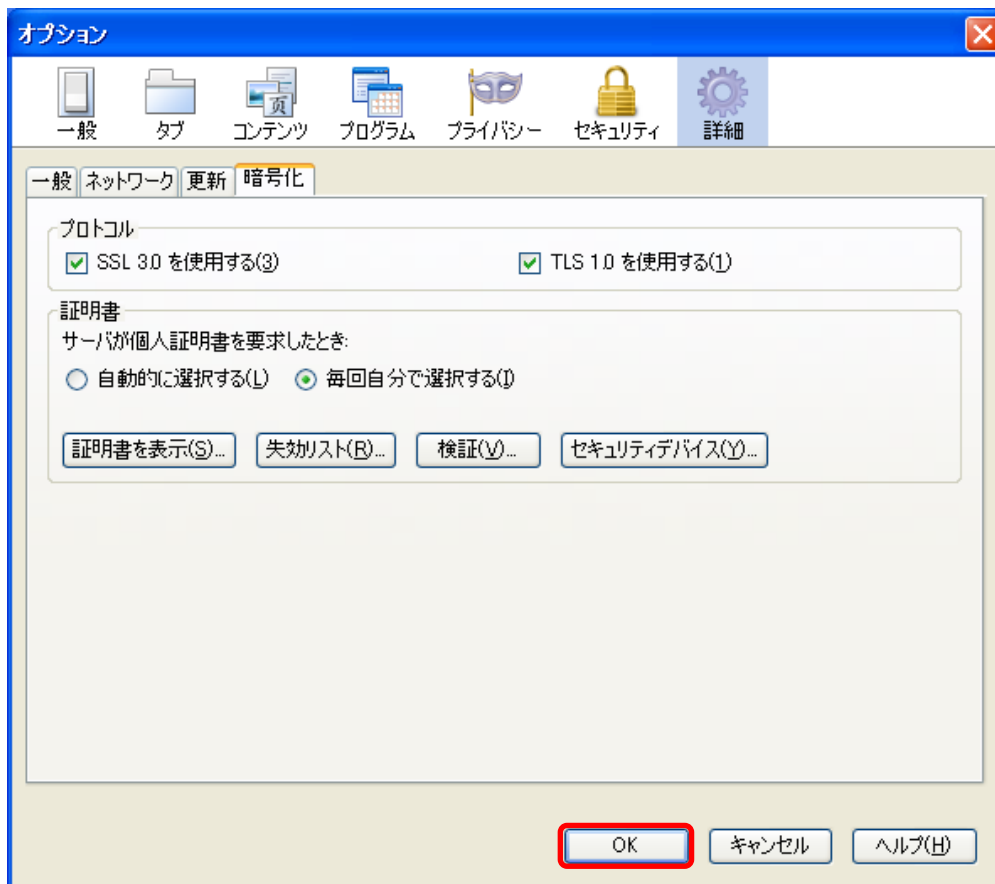
- (7) 「警告」のメッセージが表示されたら「OK」ボタンをクリックする。



- (8) 電子証明書がインポートされていることを確認してから、「OK」ボタンをクリックする。



(9) 「OK」 ボタンをクリックしてオプション画面を閉じる。これで手順は完了です。

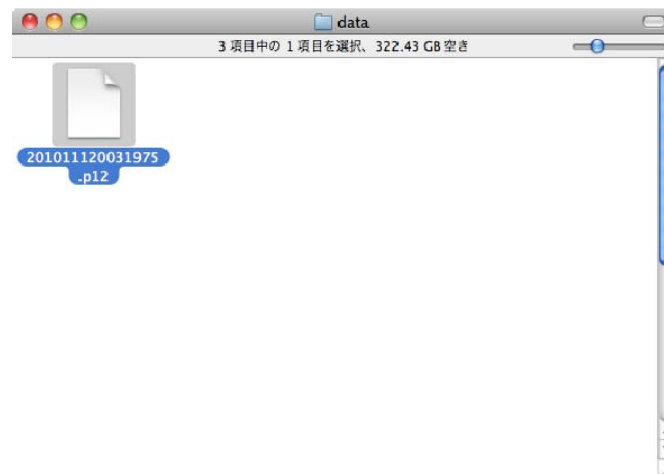


メモ

・電子証明書をインポートできない場合は、ヘルプデスクにご連絡ください。

(C) Safari (Macintosh)に電子証明書をインポートする

(1) 電子証明書ファイルをダブルクリックする。



メモ

- ・画面は Mac OS X Snow Leopard の例です。OS や Web ブラウザのバージョンにより表示される画面が異なる場合もあります。
- OS や Web ブラウザのバージョンが異なる場合の操作については、ご利用の Web ブラウザのヘルプや、Web ブラウザのメーカーのホームページ等をご確認ください。

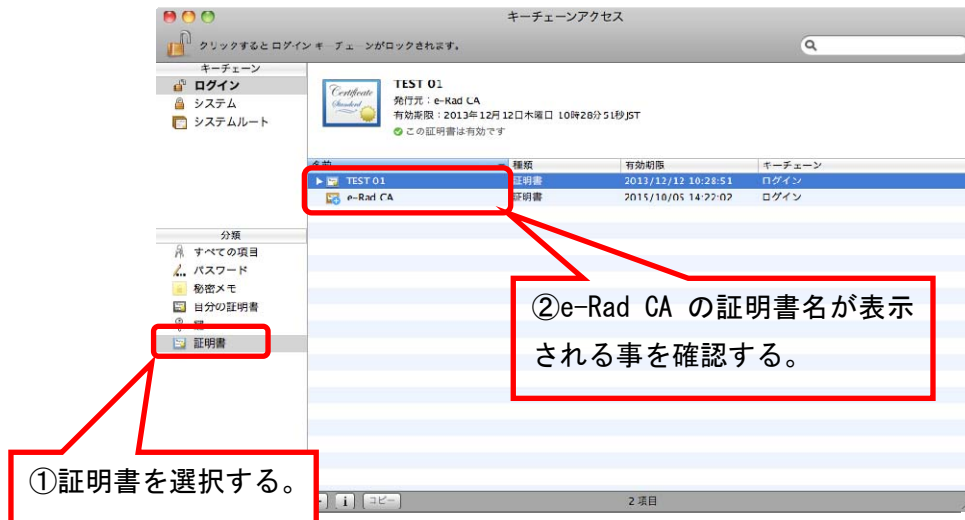
(2) パスワードを入力する。



メモ

- ・電子証明書のダウンロード時に設定したパスワードになります。
- パスワードが分からない場合は、事務代表者または、配分機関管理者へお問い合わせください。
- ・キーチェーンアクセスをロックしている場合は、(3)の後に「キーチェーンのロック解除」画面が表示されますので、MacOS のログインパスワードを入力してロックを解除してください。

(3) 電子証明書がキーチェーンアクセスに追加されていることを確認する。



メモ

- ・ 電子証明書をインポートできない場合は、ヘルプデスクにご連絡ください。

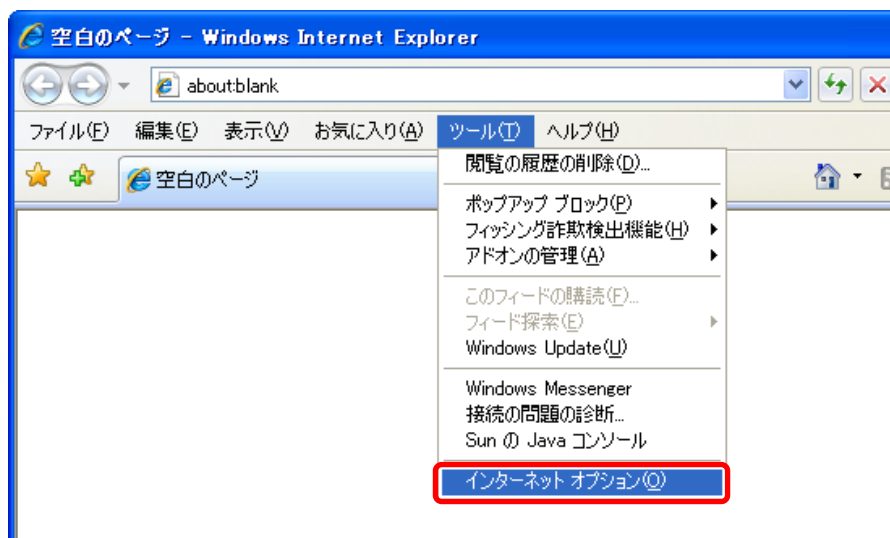
(D) インポートした電子証明書を確認する

インポートした電子証明書が確かに本システムの電子証明書であることを確認する操作について、Internet Explorer を例に説明します。

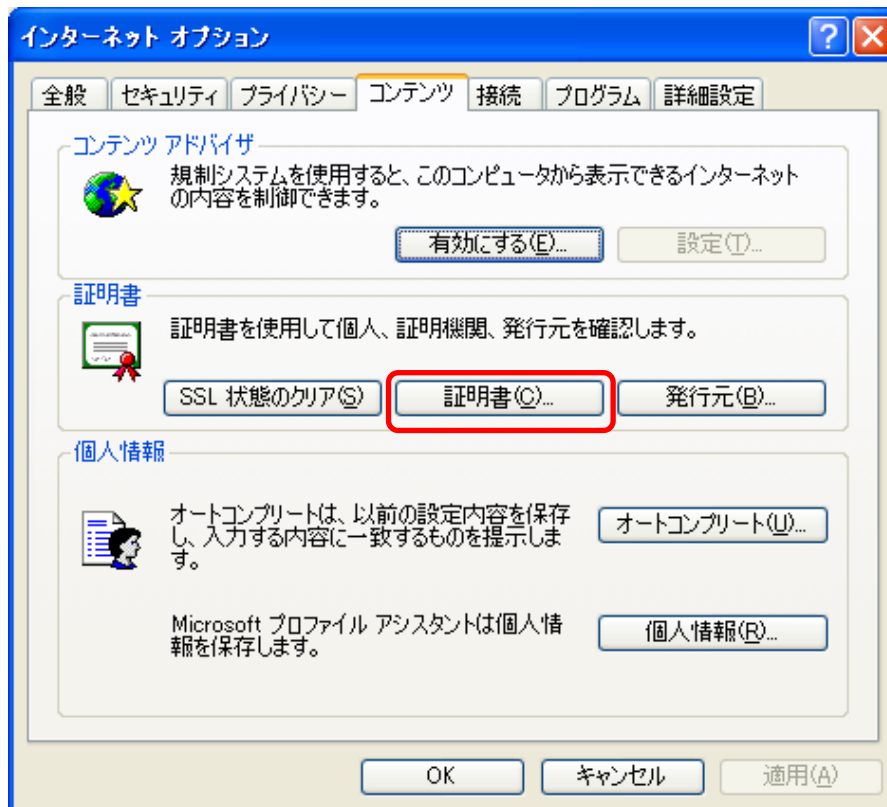
- (1) Internet Explorer を起動してから、「ツール」-「インターネットオプション」を選択する。

メモ

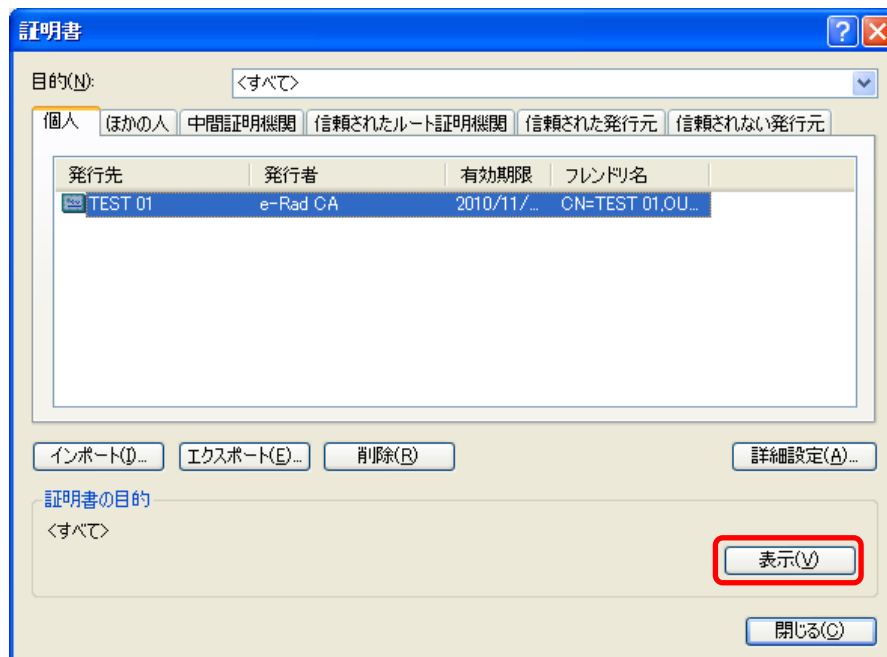
- 画面は Windows XP、Internet Explorer 7 の例です。OS や Web ブラウザのバージョンにより表示される画面が異なる場合があります。
OS や Web ブラウザのバージョンが異なる場合の操作については、ご利用の Web ブラウザのヘルプや、Web ブラウザのメーカーのホームページ等をご確認ください。



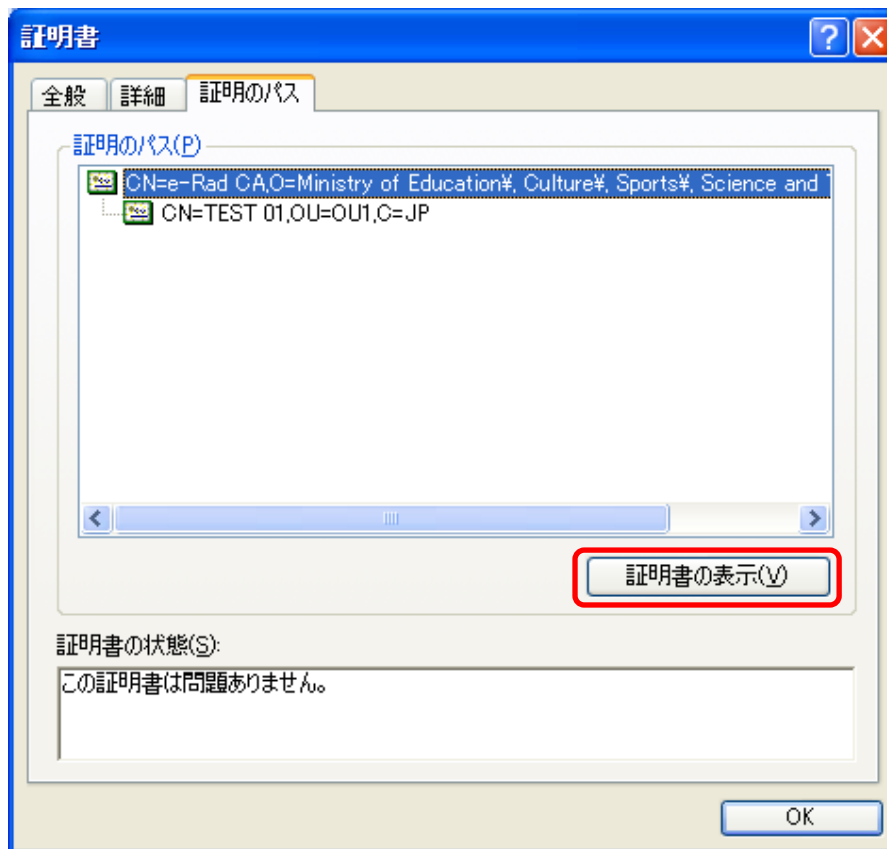
- (2) 「コンテンツ」タブを選択し、「証明書」ボタンをクリックする。



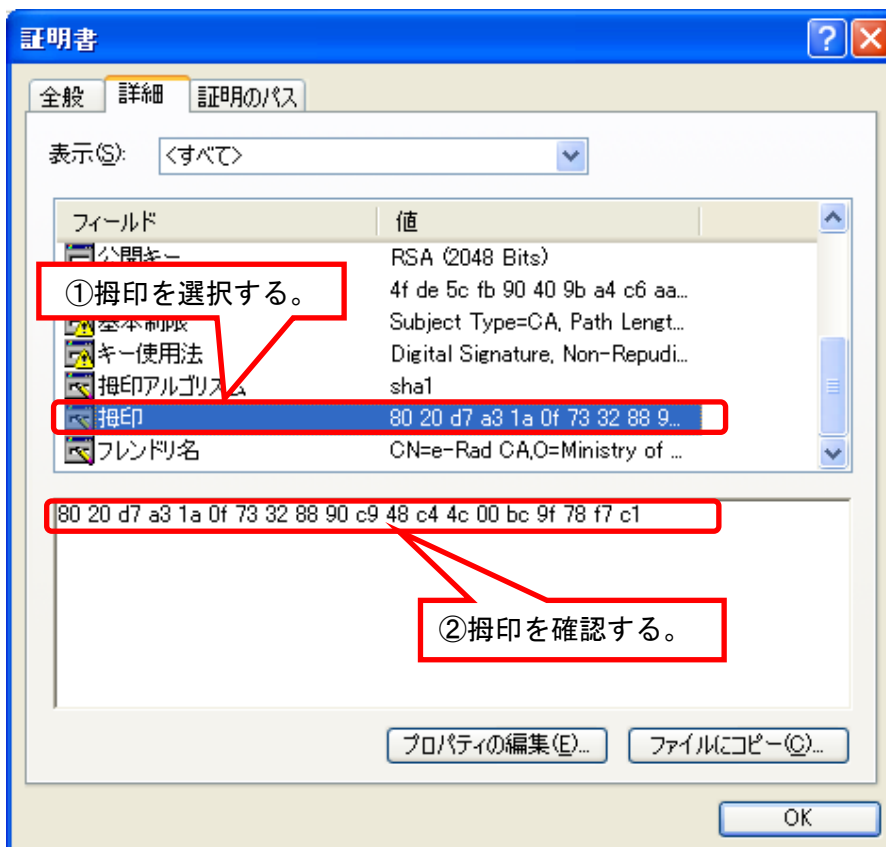
- (3) 「個人」タブを選択し、確認する証明書を選択してから「表示」ボタンをクリックする。



- (4) 「証明のパス」タブを選択し、「CN=e-Rad CA」で始まる証明書のパスを選択してから「証明書の表示」ボタンをクリックする。



(5) 「詳細設定」タブの「拇印(フィンガープリント)」を確認する。



メモ

- ・本システムの正式な電子証明書は、拇印(フィンガープリント)に次のように表示されます。

拇印アルゴリズム	sha1
拇印(フィンガープリント)	80 20 d7 a3 1a 0f 73 32 88 90 c9 48 c4 4c 00 bc 9f 78 f7 c1

- ・拇印(フィンガープリント)は、40桁の16進数であり、「0」～「9」及び「A」～「F」の文字の組合せで示されます。ただし、拇印(フィンガープリント)を表示するソフトウェア(Webブラウザ)により、大文字又は小文字の相違、「:」又はスペースの付加等表示方法が異なることがあります。

メモ

- ・「拇印(フィンガープリント)」の数字が異なる場合は、システム運用担当にご連絡ください。