1. JPNIC プライマリルート認証局の電子証明書の入手と確認の手順

概　要

一般社団法人日本ネットワークインフォメーションセンター（以下、当センター）では、インターネットのアドレス資源管理やネットワーク運用の安全性向上のため、認証局が運用しています。認証局とは、SSL/TLS などで通信相手の認証などに使われる、電子証明書を発行する仕組みです。

電子証明書は、偽造することや改変することが技術的に難しいものですが、適切に利用しなければ、偽造されたものが、あたかも正しいものであるかのように表示されてしまうことがあります。例えばhttpsを使ってアクセスしている Web サーバが、実は悪意のある別の Web サーバであっても、https の認証の結果が良好であるような表示（鍵マーク等）がされてしまうことがあります。これを防ぐためには、電子証明書を利用する前に認証局の電子証明書（以下、認証局証明書と呼びます）を適切に入手し、設定することが重要です。

ここでは、JPNIC プライマリルート認証局の認証局証明書を適切に設定する手順を説明します。

1.1. JPNIC プライマリルート認証局の認証局証明書について

JPNIC プライマリルート認証局は、資源管理者証明書を発行している「JPNIC 資源管理認証局」の認証局の上位に位置する認証局です。JPNIC プライマリルート認証局の認証局証明書は、JPNIC で運用されている認証局の認証局証明書を正しいものであるかどうかを確認するために使われます。従って JPNIC から発行されたユーザやサーバの電子証明書を検証するには、JPNIC プライマリルート認証局の証明書を「適切に」入手する必要があります。ここで言う適切さとは下記の二点を意味します。

a. **フィンガープリントが正しいこと**
当センターが配布している認証局証明書のデータと同一であること

b. **認証局証明書としての有効性**
認証局証明書の有効性を確認した結果、問題がないこと

正しさが確認できていない認証局証明書を使うと、当センターから発行されていない電子証明書が、あたかも当センターから発行されたかのように表示されてしまうことがあります。これは、Web サーバのなりすましや利用者のなりすましの原因になります。

1.2. JPNIC プライマリルート証明書とフィンガープリントの入手方法

1.2.1. JPNIC プライマリルート証明書の入手と確認

認証局証明書は、下記の Web ページから入手できます。

JPNIC 認証局のページ
http://jpnic-ca.nic.ad.jp/

この Web ページでは、個人情報や認証に関わる情報入力を促されることはありません。異なる場合には、本書末尾にあるご連絡先までお知らせ下さい。

1.2.2. 利用規約とフィンガープリント

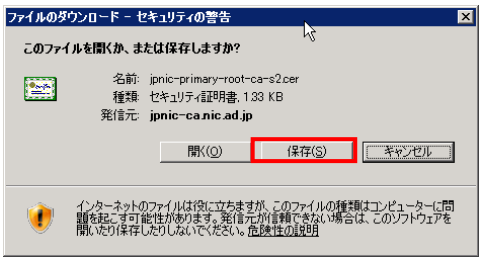
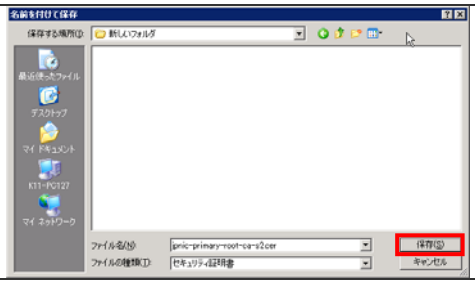
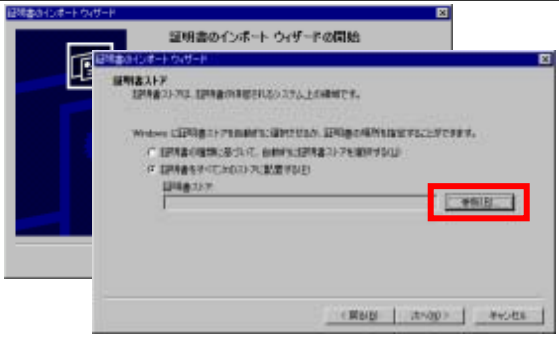
当センターで別途申請者に配布している「JPNIC 認証局証明書 利用規約」をご覧下さい。JPNIC 認証局証明書を利用された場合、この規約に書かれた事項に同意されたものとみなされます。

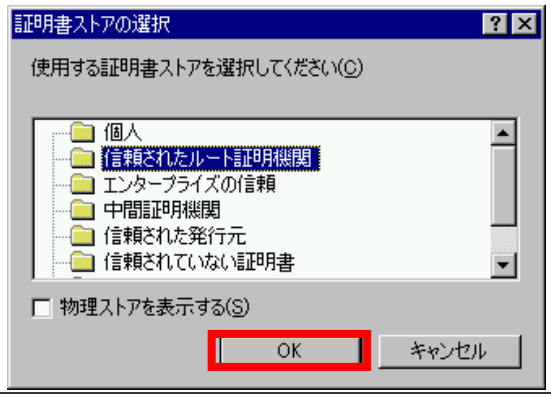
便宜上、下記の Web ページにて、本規約に記載されている「JPNIC プライマリルート認証局のフィンガープリント」を提供しています。

JPNIC 認証局 fingerprint のページ
https://serv.nic.ad.jp/capub/fingerprint.html

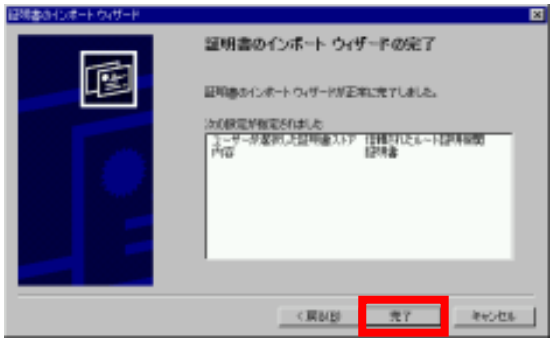
★ 2012 年 8 月 14 日以前に発行された資源管理カードをご利用の場合
「JPNIC プライマリルート認証局 S2」に加えて、従来の「JPNIC プライマリルート認証局 S1」をインストールしておく必要があります。インストール方法につきましては、資源管理カードと共に郵送されました「資源管理者証明書 セットアップマニュアル」をご覧下さい。

1.2.3. JPNIC プライマリルート証明書の設定手順（Internet Explorer）

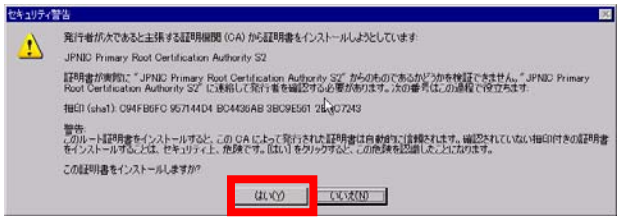
1. JPNIC プライマリルート証明書を入手します。	JPNIC 認証局のページ(http://jpnic-ca.nic.ad.jp/) の「JPNIC プライマリルート認証局証明書」jpnic-primary-root-ca-S2.cer をダウンロードします。
2. 「ファイルのダウンロード」画面が表示されますので、“保存”ボタンをクリックします。	
3. 保存する場所をデスクトップなどに選択し、“保存”ボタンをクリックします。 ⇒ ファイルのダウンロードが始まります。	
4. 保存した JPNIC プライマリルート証明書ファイルをダブルクリックします。(ファイル名は「jpnic-primary-root-ca-s2.cer」又は「jpnic-primary-root-ca-s2」となります)	
5. 入手した証明書は、発行先と発行者と同一になっている「自己署名証明書」です。「証明書は信頼されていません」と表示されます。内容を確認するため、“証明書のインストール”ボタンをクリックしてください。 ⇒ 「証明書のインポートウィザード」の画面が表示されます。	
6. インポートウィザードでは、「証明書をすべて次のストアに配置する(P)」をクリックし、証明書ストアとして「信頼されたルート証明機関」を選択します。	



7. 「証明書のインポートウィザードの完了」で、“完了”ボタンをクリックしてください。



8. まだ信頼していない証明書をインストールしようとしているため、「セキュリティ警告」ダイアログボックスが表示されます。



拇印(sha1)の値と、「JPNIC 認証局利用規約」（色のついた紙）や JPNIC NewsLetter の最後のページなどに載せられている「JPNIC プライマリルート証明書のフィンガープリント」の値と等しいことを確認します。

確認後は、“はい”ボタンをクリックしていください。

⇒正しくインポートされたことが表示されます。これで a. フィンガープリントが正しいこと の確認ができました。JPNIC プライマリルート証明書の設定は完了です。

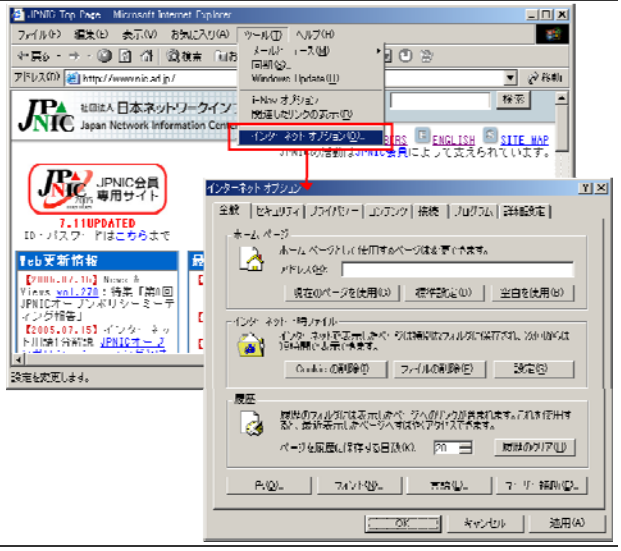
【保存したファイル】
「4.」で保存した JPNIC プライマリルート証明書ファイルは必要ありませんので、削除しても問題ありません。

⚠注意
証明書の拇印と JPNIC プライマリルート証明書のフィンガープリントの値が異なる場合には証明書の安全性を確認できません。”いいえ”ボタンをクリックして設定作業を中止してください。

※SHA-1 により算出した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、フィンガープリントを表示するソフトウェアの種類又はバージョンにより、大文字又は小文字の相違等表示方法が異なることがあります。

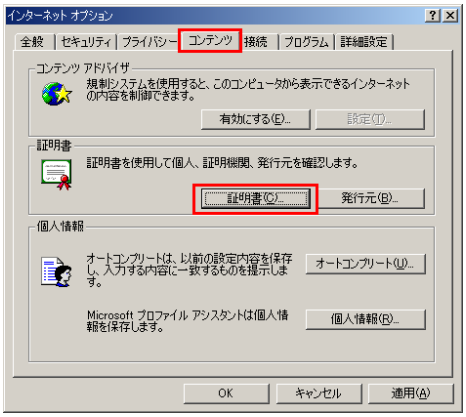
9. ブラウザの“ツール”メニューの“インターネットオプション”を選択してください。

⇒「インターネットオプション」画面が表示されます。



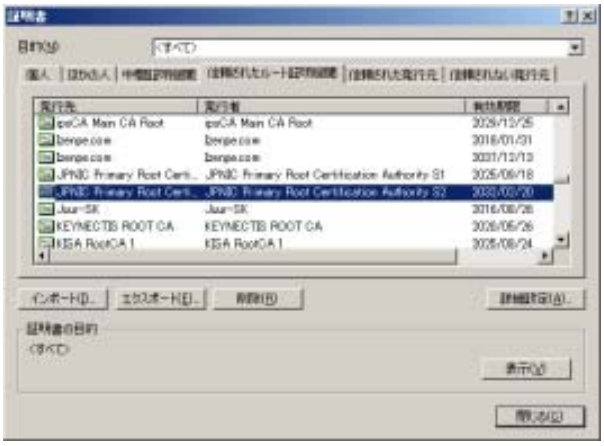
10. 「インターネットオプション」画面の“コンテンツ”タブを選択し、“証明書”ボタンをクリックしてください。

⇒「証明書」画面が表示されます。



11. 「信頼されたルート証明機関」タブを選択し、発行先の「JPNIC Primary Root Certification Authority S2」をクリックし、画面下部の“表示”ボタンをクリックしてください。

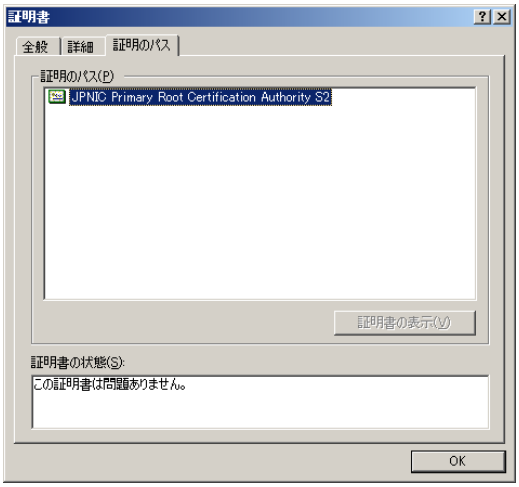
⇒JPNIC Primary Root Certification Authority S2 の「証明書」画面が表示されます。



12. “証明のパス”タブを選択すると、証明のパスが最上位に記載されます。

「この証明書は問題ありません。」というメッセージが確認できれば b. 認証局証明書としての有効性の確認ができていることになります。

これで JPNIC プライマリルート証明書が正しく Web ブラウザにインストールされていることが確認できました。

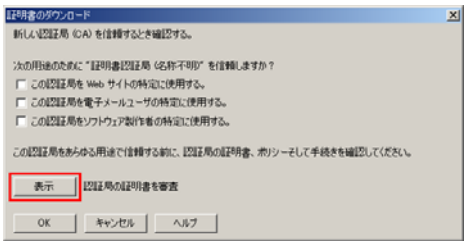


1.2.4. JPNIC プライマリルート証明書の設定手順（Firefox）

1. 認証局証明書を入手します。

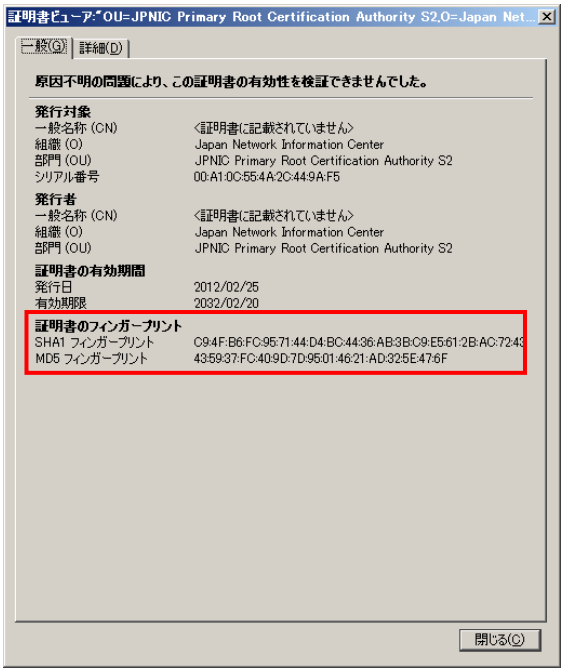
JPNIC 認証局のページ(http://jpnic-ca.nic.ad.jp/)にリンクがあります。「JPNIC プライマリルート認証局証明書」jpnic-primary-root-ca-S2.cer をダウンロードします。

2. 「証明書のダウンロード」画面が表示されますので、入手した証明書が正しいことを確認するために“表示”ボタンをクリックします。



3. 証明書ビューアが表示されたら、画面下部の「フィンガープリント」が表示されますので、これらが等しいことを確認します。SHA-1 Fingerprint と MD5 Fingerprint の両方を確認して下さい。

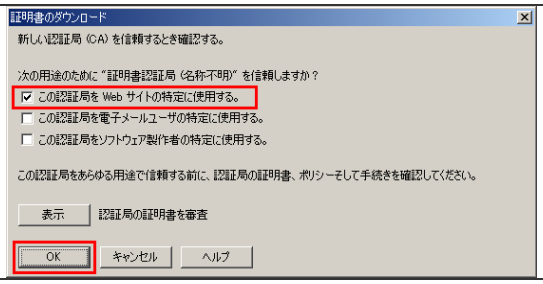
注意
証明書の拇印と JPNIC プライマリルート証明書のフィンガープリントの値が異なる場合には証明書の安全性を確認できません。"閉じる"ボタンをクリックして設定作業を中止してください。
※SHA-1 により算出したフィンガープリントは、40 桁の 16 進数であり、「0」～「9」及び「A」～「F」の文字の組合せで示されます。ただし、フィンガープリントを表示するソフトウェアの種類又はバージョンにより、大文字又は小文字の相違等表示方法が異なることがあります。



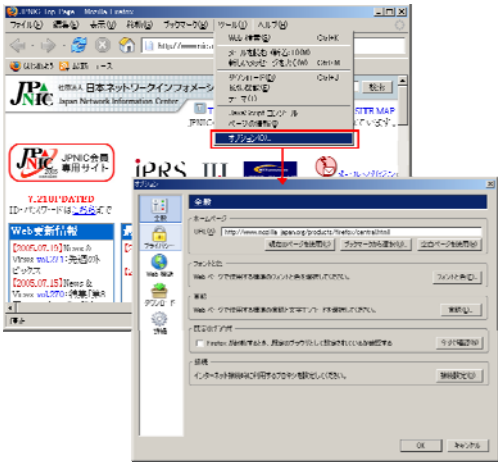
確認後は “閉じる”ボタンをクリックしてください。これで a.フィンガープリントが正しいこと の確認ができました。

⇒「証明書のダウンロード」画面に戻ります。

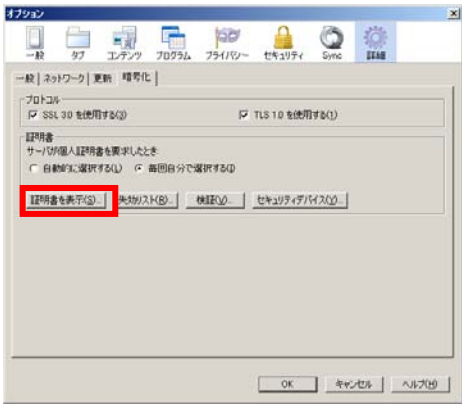
4.「Web サイトを特定するとき、この認証局を信頼する。」、「この認証局による Web サイトの識別を信頼する。」または「この認証局を Web サイトの特定に使用する。」にチェックをして“OK“ボタンをクリックしてください。何も表示されませんが、これで設定は完了です。次に進みます。



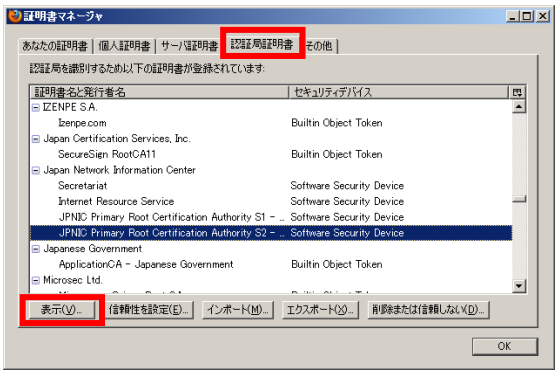
5. ブラウザの“編集”メニューの“設定”もしくは“ツール”メニューの“オプション”を選択してください。
⇒「設定」または「オプション」画面が表示されます。



6. メニューの「詳細」画面を選択し（Firefox のみ）、「証明書」より“証明書マネージャ”ボタンをクリックしてください。
⇒「証明書マネージャ」画面が表示されます。

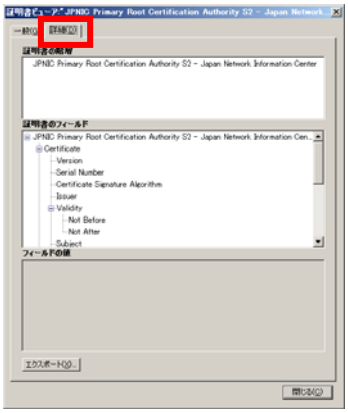


7. “認証局証明書”タブを選択後、証明書名の「JPNIC Primary Root Certification Authority S2 – Japan Network Information Center」を選択し、“表示”ボタンをクリックしてください。
⇒ JPNIC Primary Root Certification Authority の「証明書」画面が表示されます。



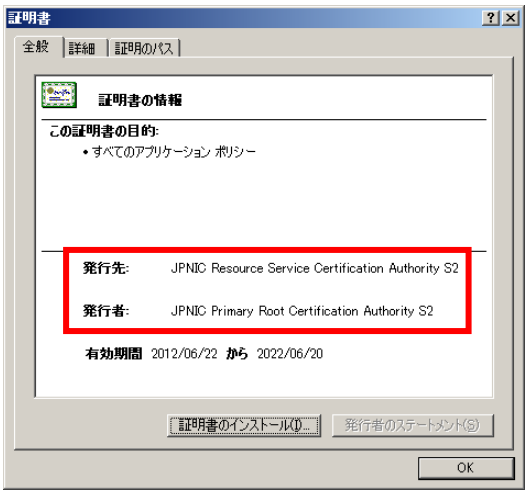
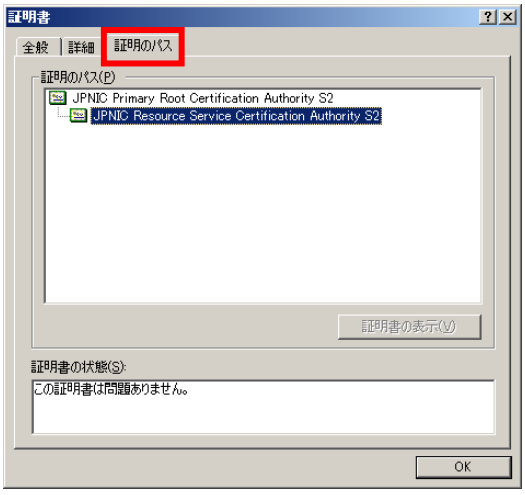
8. “詳細”タブを選択すると、証明書の階層が最上位に記載されることが確認できます。特に警告が表示されていなければ b. 認証局証明書としての有効性 の確認ができています。

これで JPNIC プライマリルート証明書が正しく Web ブラウザにインストールされていることが確認できました。

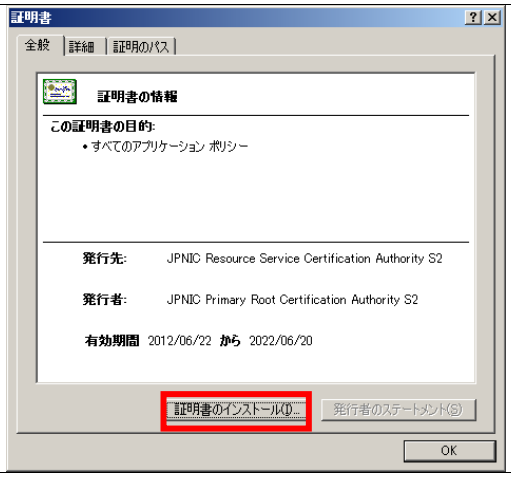


2. JPNIC 資源管理認証局証明書の入手と確認の手順

2.1. Internet Explorer での設定手順

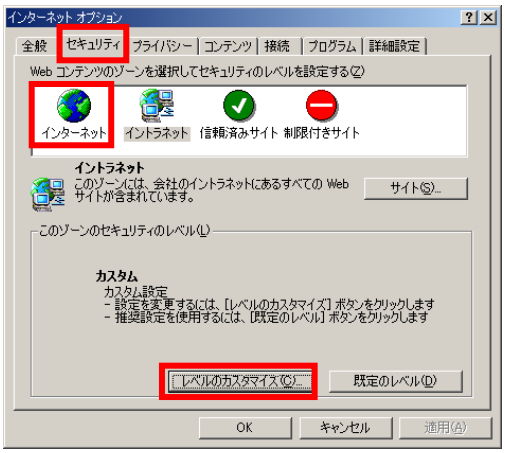
1. JPNIC 資源管理認証局証明書の入手 JPNIC 資源管理認証局証明書（JPNIC-Resource-Service-CA-S2.cer）をダウンロードします。	JPNIC 認証局のページ（http://jpnic-ca.nic.ad.jp/）にリンクがあります。
2. JPNIC 資源管理認証局証明書の表示 入手した証明書ファイルをダブルクリックすると右のダイアログが表示されます。 発行先が 「JPNIC Resource Service Certification Authority S2」 発行者が 「JPNIC Primary Root Certification Authority S2」 であることを確認してください。	
3. 証明のパスの確認 証明のパスが 「JPNIC Primary Root Certification Authority S2」 で始まっていることを確認して下さい。	

“証明書のインストール”ボタンを押下し、ウィザードに従ってインストールを行います。



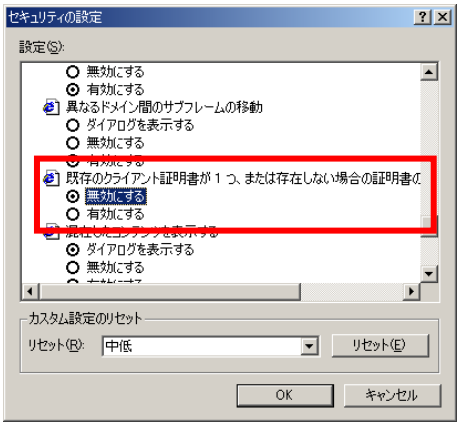
4. 証明書選択の設定

インターネットエクスプローラーのツール→［インターネットオプション（O)］をクリックし、表示される「セキュリティ」タブより“レベルのカスタマイズ”ボタンを押下します。



5.「既存のクライアント証明書が一つ、または存在しない場合の証明書の選択」を、“無効にする”を選択してください。

この設定により、クライアント証明書を使う際に必ず確認のダイアログボックスが表示され、Web 申請システム以外のサーバなどに不用意に証明書を提示することを避けることができます。



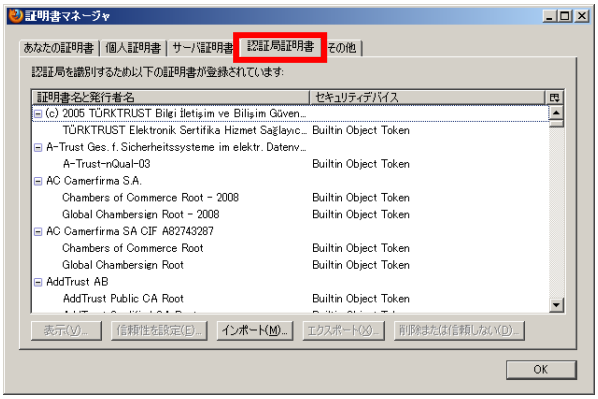
2.2. Firefox での設定手順

1. JPNIC 資源管理認証局証明書の入手

JPNIC 資源管理認証局証明書（JPNIC-Resource-Service-CA-S2.cer）をダウンロードします。

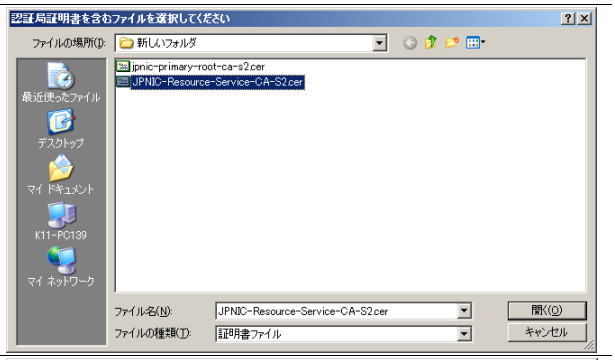
JPNIC 認証局のページ（http://jpnic-ca.nic.ad.jp/）にリンクがあります。

ツール(T) → オプション(O) → 証明書を表示(S)... から「認証局証明書」タブを開きます。



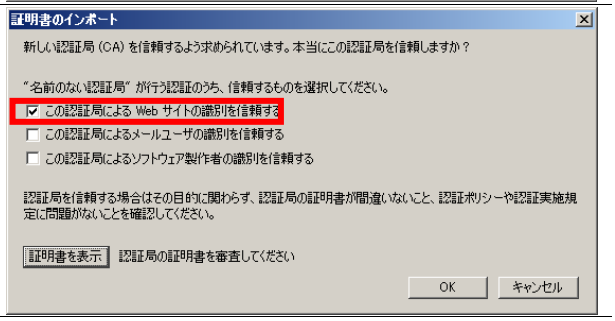
2. インポート

インポート(M)...をクリックし、ダウンロードしたファイルを選択します。



3. 証明書のインストール

「この認証局による Web サイトの識別を信頼する。」にチェックをし、証明書を表示をクリックします。



4. 証明書選択の設定

ツール(T) → オプション(O) →詳細で、“毎回自分で選択する”を選びます。

この設定により、クライアント証明書を使う際に必ず確認のダイアログボックスが表示され、Web 申請システム以外のサーバに不用意に証明書を提示することを避けることができます。