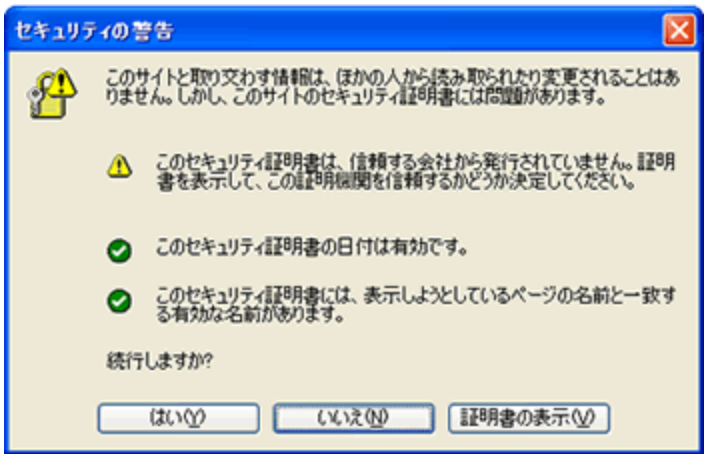
「安全な通信を行うための証明書（第二世代）」の入手と設定

（平成 18 年 9 月 22 日）

はじめに

電子登録システム・電子調達システムを利用した際に、次の警告が表示される場合は、下記手順に沿って、「安全な通信を行うための証明書（第二世代）」の入手と設定を行ってください。



警告が表示されない場合は、そのままご利用いただけます。

「安全な通信を行うための証明書（第二世代）」の入手と設定について

堺市の電子登録システム・電子調達システムを利用するためには、「安全な通信を行うための証明書（第二世代）（以下、証明書）」をブラウザに組み込むことが必要です。

以下に記載された作業手順により、必要なデータを入手して、ブラウザに組み込むことができます。

なお、OS 及びブラウザのバージョンにより、画面及び操作が若干異なることがあります。（以下に記載の例は、WindowsXP、Internet Explorer6 の画面イメージです。）

堺市の電子登録システム・電子調達システムでは、認証局として地方公共団体組織認証局（LGPKI）を利用しています。

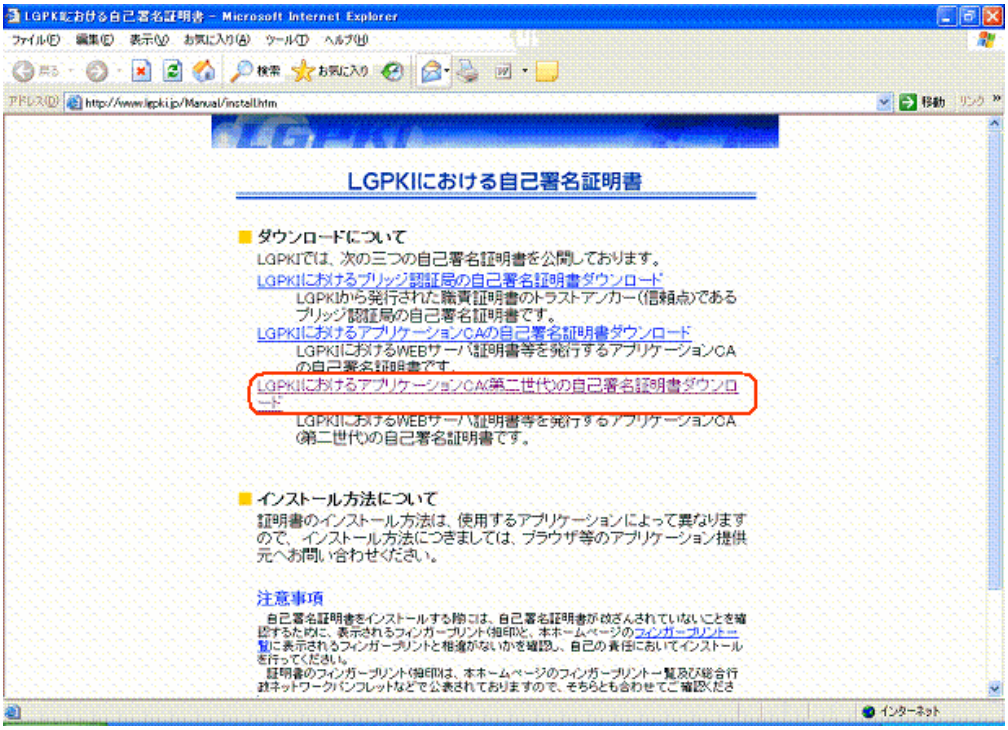
設定作業の概要

- 証明書をダウンロードし、パソコン上に保存する。
- 証明書が正しいか、フィンガープリント(拇印)を照合して確認する。
- 証明書をブラウザに取り込む。
- ブラウザの設定をする。

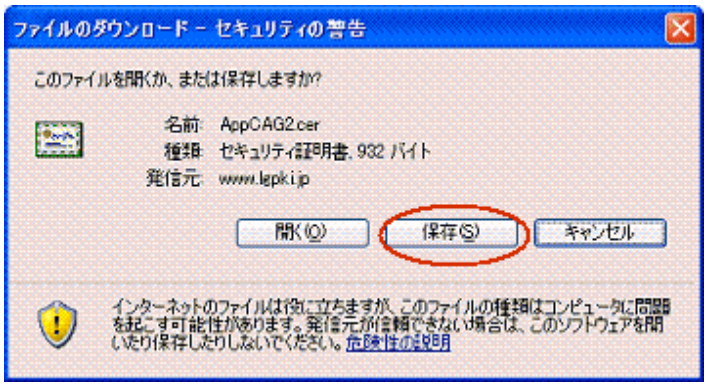
証明書をダウンロードし、パソコン上に保存する。

1. LGPKI（地方公共団体組織認証基盤）の「LGPKI　における自己署名証明書」のページを開きます。

［LGPKI におけるアプリケーション CA（第二世代）の自己署名証明書ダウンロード］をクリックします。

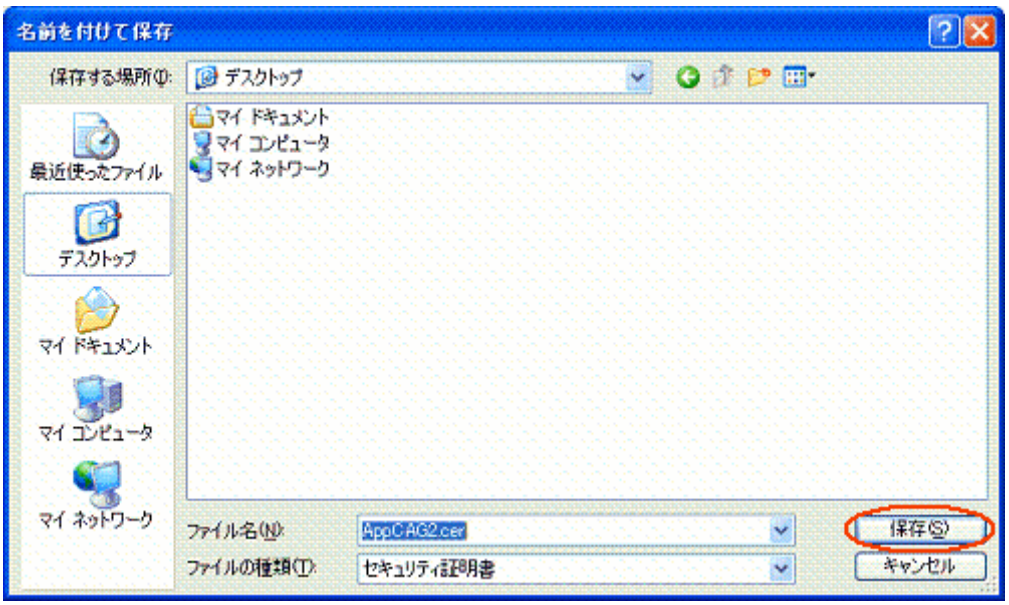


2. ファイルのダウンロード画面が表示されます。『保存』ボタンをクリックします。



3. 名前を付けて保存画面が表示されます。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。

※ファイル名は「AppCAG2.cer」のままで保存してください。なお、このファイルは証明書の組み込みが完了した後に削除しても問題ありません。

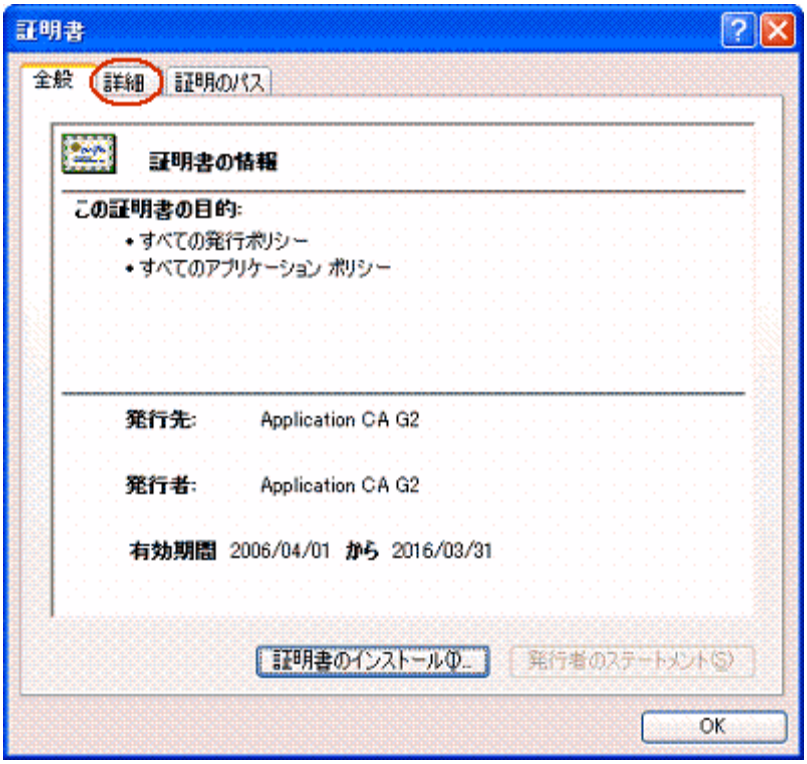


4. 3 で指定した場所に、「AppCAG2.cer」ファイルが保存されます。

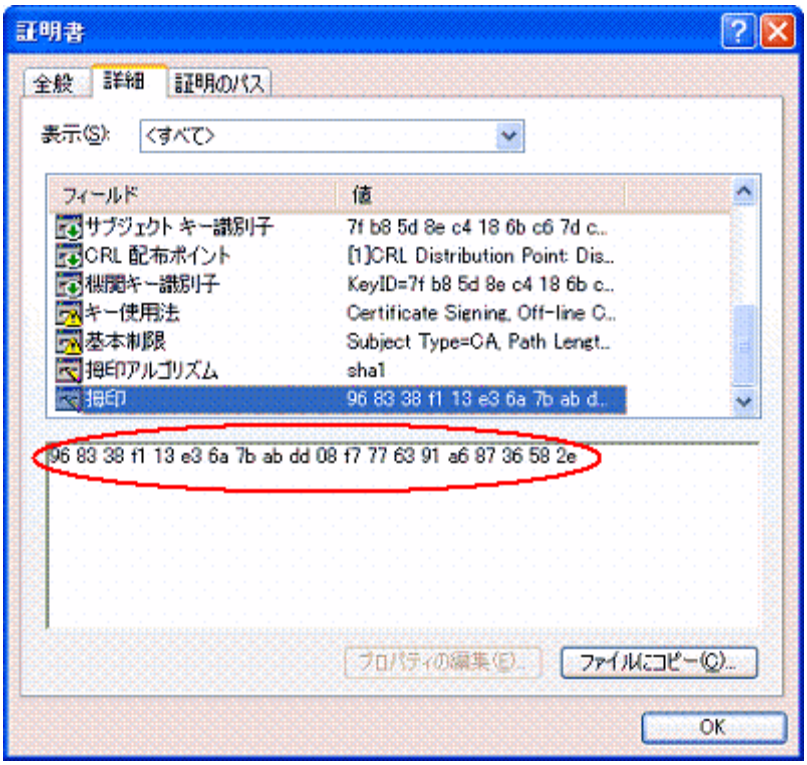
証明書が正しいか、フィンガープリント(拇印)を照合して確認する。

1. 保存した「AppCAG2.cer」ファイルをダブルクリックします。

2. 証明書画面が表示されます。「詳細」タブをクリックします。



3. 証明書の詳細画面が表示されたら下にスクロールし、「拇印」をクリックします。



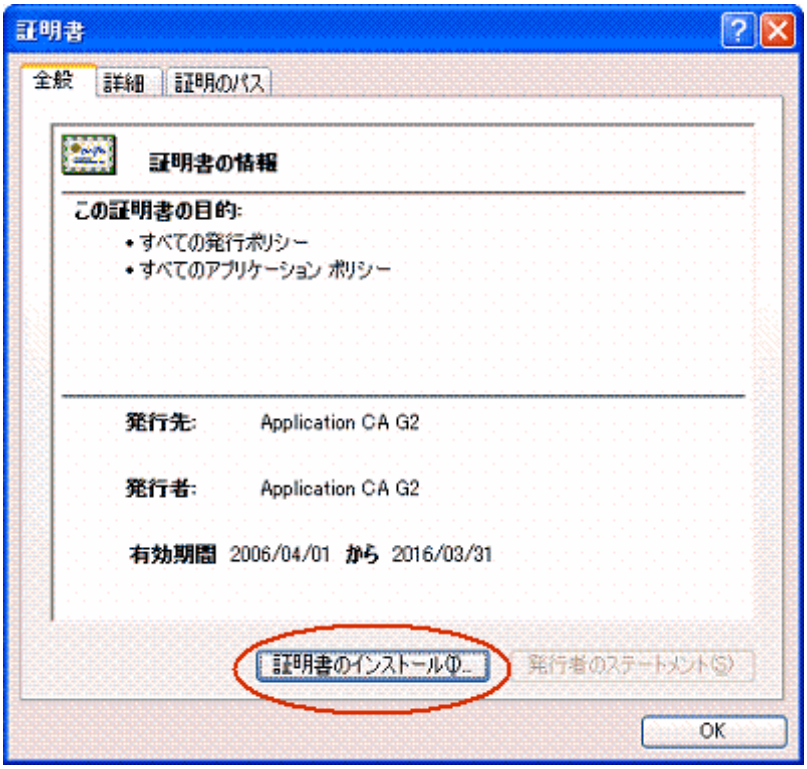
4. 証明書の拇印（以下、フィンガープリント）が表示されますので、この数値とLGPKIApplicationCAG2(第二世代)の自己署名証明書のフィンガープリントの数値とが一致していることを確認してください。

ハッシュ関数の種類	フィンガープリント
S H A – 1	96 83 38 F1 13 E3 6A 7B AB DD 08 F7 77 63 91 A6 87 36 58 2E

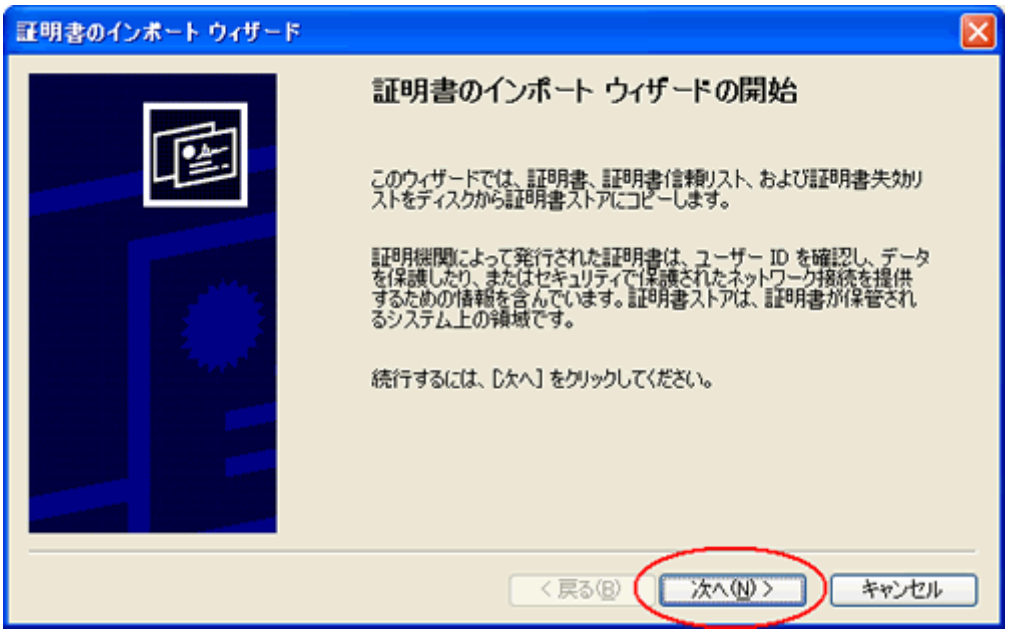
※SHA-1 により算出したフィンガープリントは、40 けたの 16 進数であり、0 から 9 まで及び A から F までの文字の組合せで示されます。表示するブラウザの種類またはバージョンにより、大文字又は小文字の相違、コロン（：）又はスペースの付加等表示方法が異なることがあります。

証明書をブラウザに取り込む。

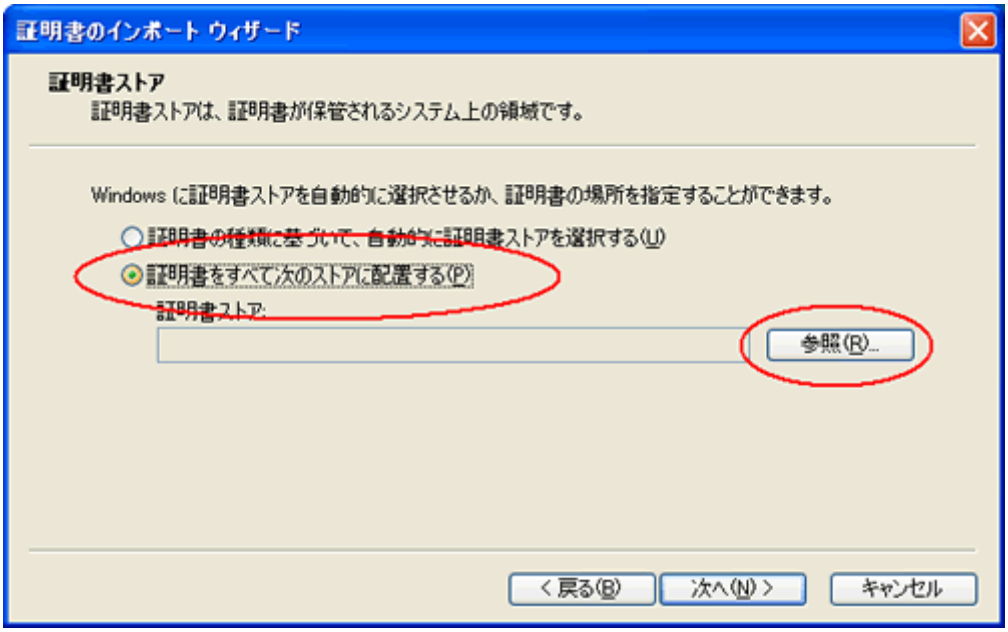
1 .証明書画面で「全般」タグをクリックします。証明書の全般画面が表示されたら、『証明書のインストール』ボタンをクリックします。



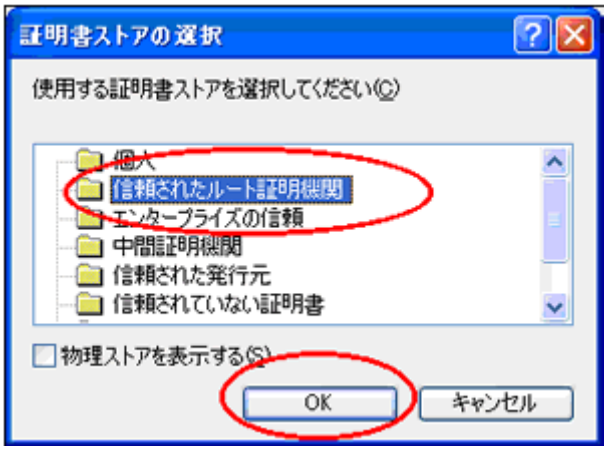
2. 証明書のインポートウィザード画面が表示されます。『次へ』ボタンをクリックします。



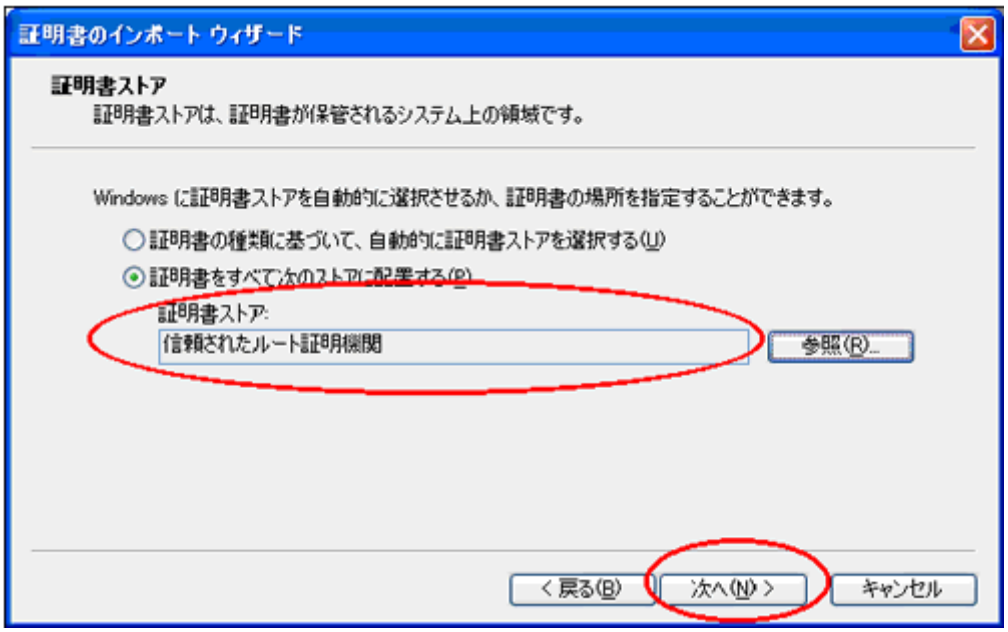
3. 「証明書をすべて次のストアに配置する」にチェックを入れて、『参照』ボタンをクリックします。



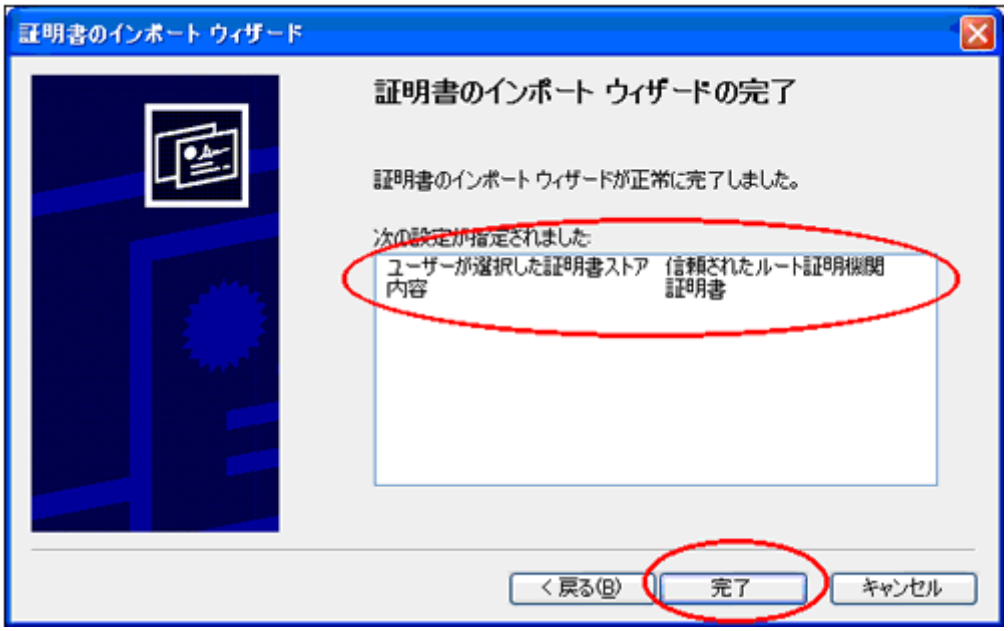
4. 証明書ストアの選択画面が表示されます。「信頼されたルート証明機関」を選択し、『OK』ボタンをクリックします。



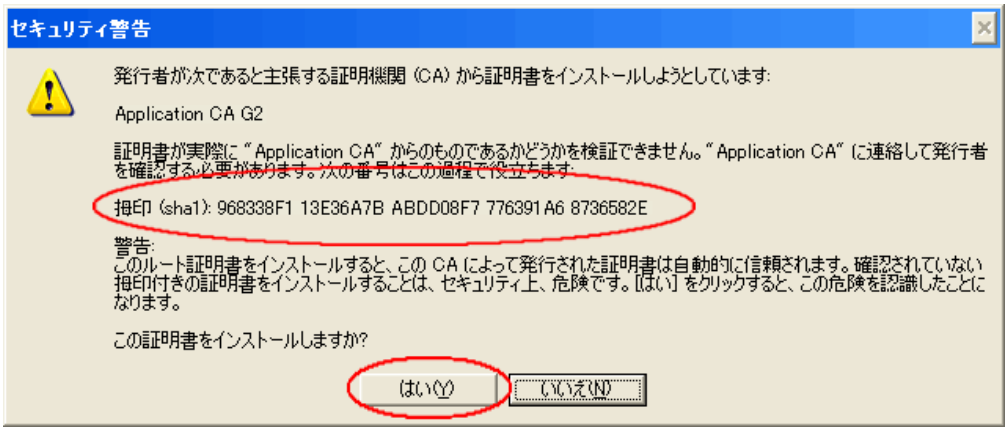
5. 「証明書ストア」欄に「信頼されたルート証明機関」が表示されていることを確認し、『次へ』ボタンをクリックします。



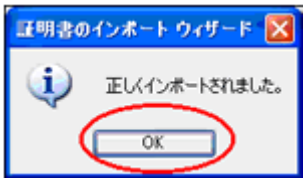
6. 「ユーザが選択した証明書ストア」の横に「信頼されたルート証明機関」と表示されていることを確認し、『完了』ボタンをクリックします。



7. セキュリティ警告画面が表示されます。拇印（sha1）の値が、LGPKIApplicationCAG2(第二世代)の自己署名証明書の拇印と一致することを確認し、『はい』ボタンをクリックします。

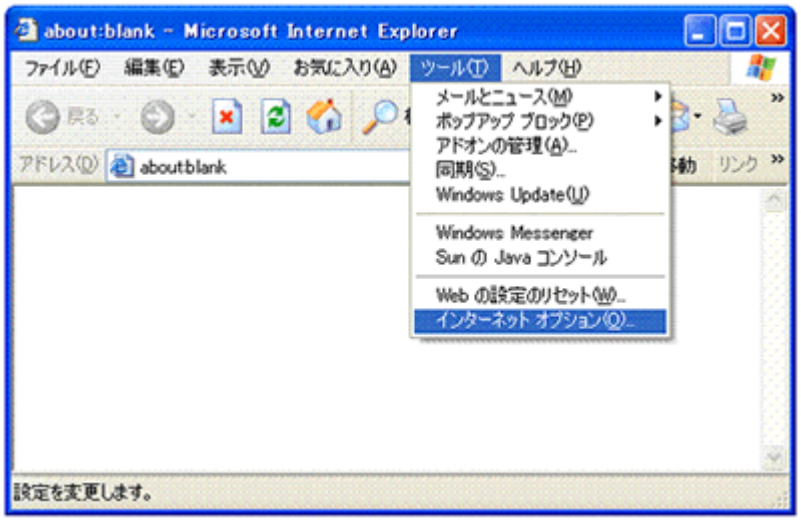


8. 以下の画面が表示されれば、処理は終了です。『OK』ボタンをクリックします。

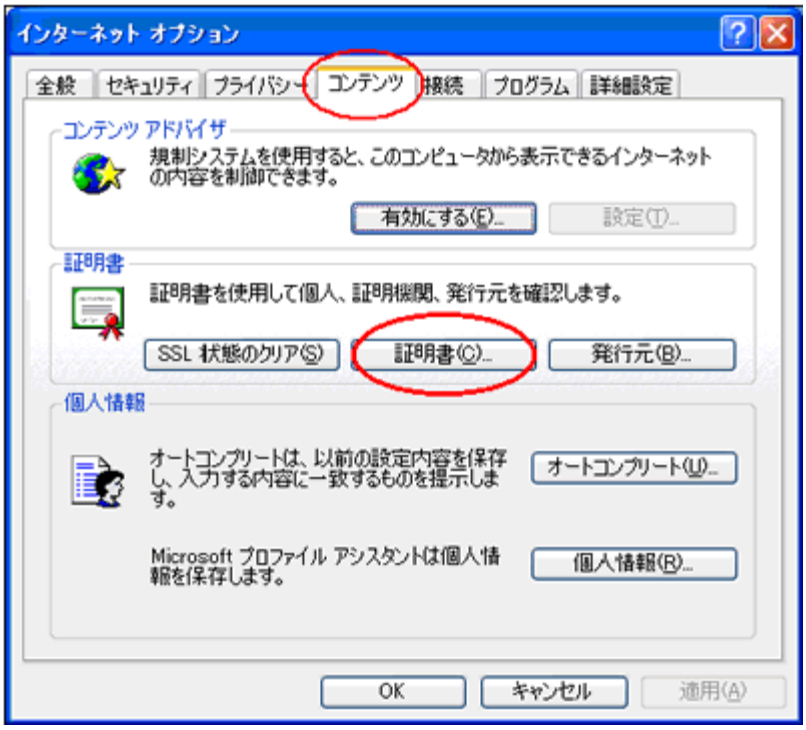


ブラウザの設定をする。

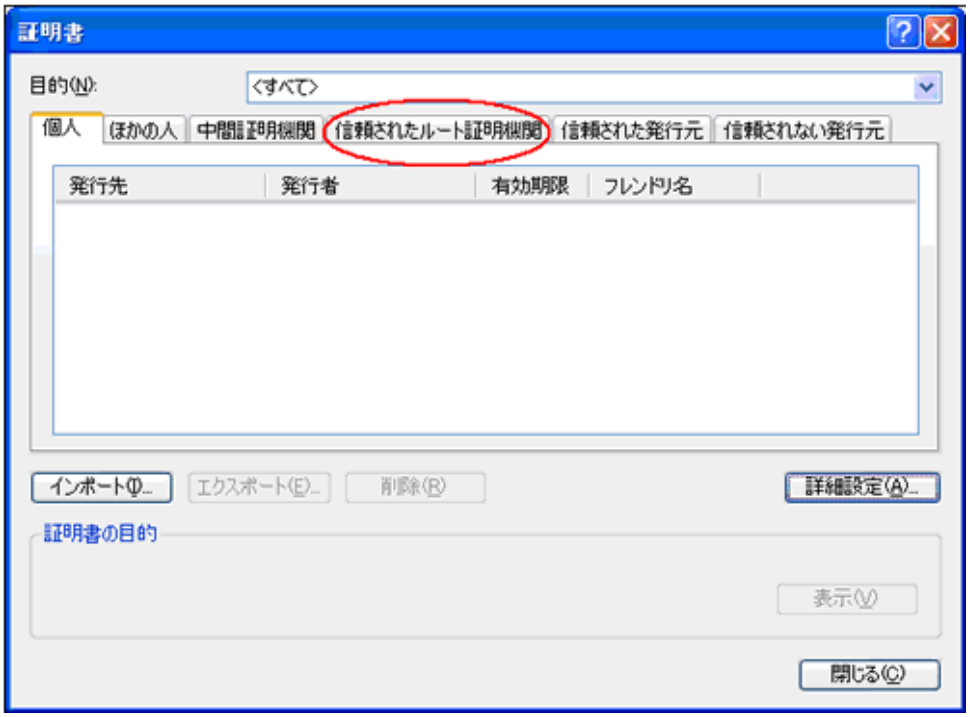
1. ブラウザのツールバーで「ツール」→「インターネットオプション(O)」をクリックします。



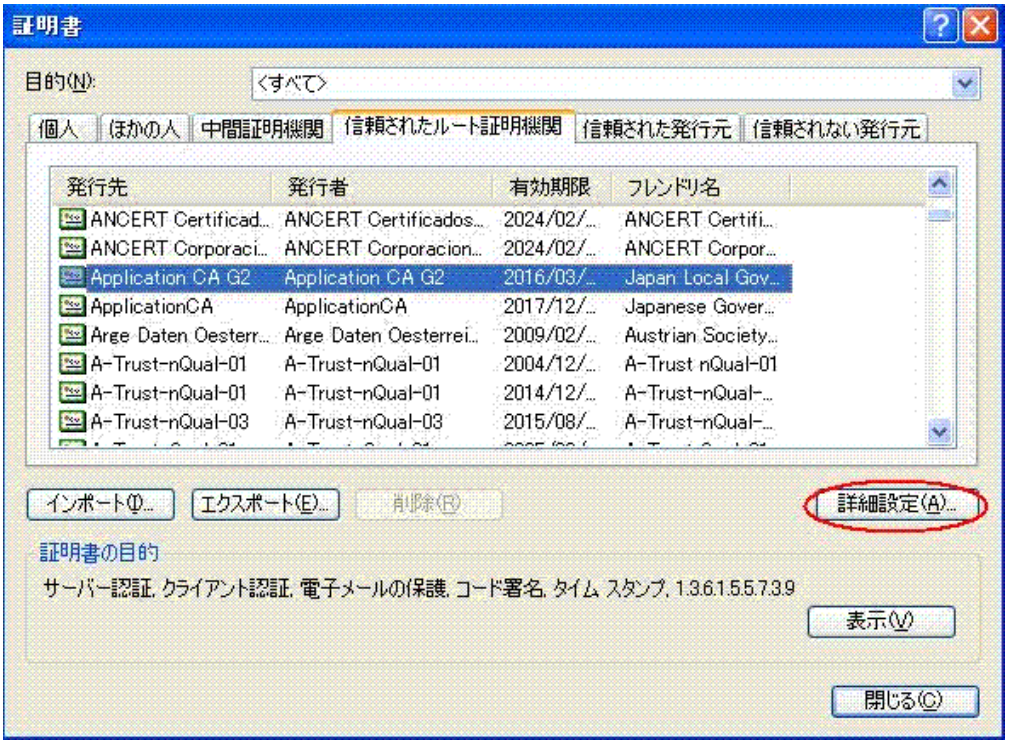
2. インターネットオプション画面で「コンテンツ」タブをクリックし、『証明書』ボタンをクリックします。



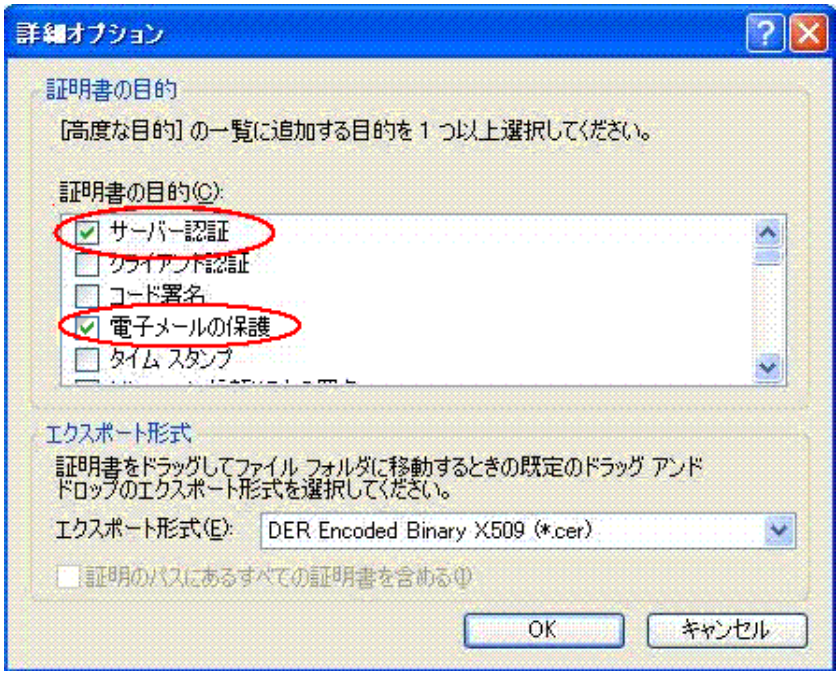
3. 証明書画面で「信頼されたルート証明機関」タブをクリックします。



4. 証明書の信頼されたルート証明機関画面が開いたら、「ApplicationCAG2」を選択し、『詳細設定』ボタンをクリックします。



5. 「証明書の目的」で「サーバー認証」と「電子メールの保護」のみチェックを入れ、その他はすべて外して『OK』ボタンをクリックします。



6. 以上でブラウザの設定作業は終了です。「証明書」画面を閉じて、「インターネットオプション」画面の『OK』ボタンをクリックして閉じます。