参考

アプリケーション認証局（第四世代）（Root）
自己署名証明書のインストール方法について
（ Internet Explorer、Google Chrome版）

はじめに

LGPKIアプリケーション認証局（第四世代）から発行するアプリケーション証明書の検証に当たっては、LGPKIアプリケーション認証局（第四世代）の最上位の認証局（以下「APCA G4（Root）」という。）の自己署名証明書が必要になります。

ブラウザソフトとしてInternet Explorerを利用する場合、APCA G4（Root）の自己署名証明書については、マイクロソフト株式会社から提供される Windows Update 機能を利用したルート証明書更新プログラムにより、自動でクライアントの証明書ストアへのインストールが実行されます。しかし、インターネットに接続していない環境（Windows Updateサーバに接続不可）など、クライアントの環境によっては、手動でAPCA G4（Root）の自己署名証明書のインストールが必要な場合があります。
手動インストールが必要な場合には、本資料を参考にインストール作業を実施してください（ただし、APCA G4(Root）の自己署名証明書の取得に当たっては、インターネット接続が必要です。）。

なお、本手順でインストールした自己署名証明書は、ブラウザベンダによって管理されないため、APCA G4(Root)が危殆化した場合には、手動で自己署名証明書の削除が必要となりますので留意してください。

また、本資料は、Internet Explorerの場合の手動インストール手順となります。ブラウザソフトとしてGoogle Chromeを利用する場合のインストール手順については、スライド１１を参照してください。

1　APCA G4（Root）自己署名証明書の入手

LGPKIホームページの「LGPKIにおける自己署名証明書」のページから、APCA G4（Root）の自己署名証明書（以下「自己署名証明書」という。）をデスクトップ等にダウンロードする。

インターネット側ページ：
https://www.lgpki.jp/CAInfo/install.htm

LGWAN側ページ：
http://center.lgwan.jp/use/third2_5.html

■ ダウンロードについて

LGPKIでは、次の自己署名証明書を公開しております。

LGPKIにおけるブリッジCAの自己署名証明書ダウンロード
LGPKIから発行された職責証明書のトラストアンカー(信頼点)であるブリッジCAの自己署名証明書です。
ブリッジCAは、平成26年9月13日にCA鍵ペアの更新を実施し、新暗号の新しいCA鍵ペアにより発行した自己署名証明書です。
CA鍵ペア更新前の自己署名証明書はこちら

LGPKIにおける組織CAへの中間CA証明書ダウンロード
中間CA証明書は、LGPKIから発行されたブリッジCAから組織CAへの相互認証証明書で、新暗号でのCA鍵ペアの更新に伴い、平成26年9月13日に新しく発行されました。
CA鍵ペア更新前の中間CA証明書はこちら

LGPKIにおけるアプリケーションCA G3 Rootの自己署名証明書ダウンロード
LGPKIにおける自己署名証明書及び下位CA証明書を発行するアプリケーションCA G3 Root(第三世代)の自己署名証明書です。

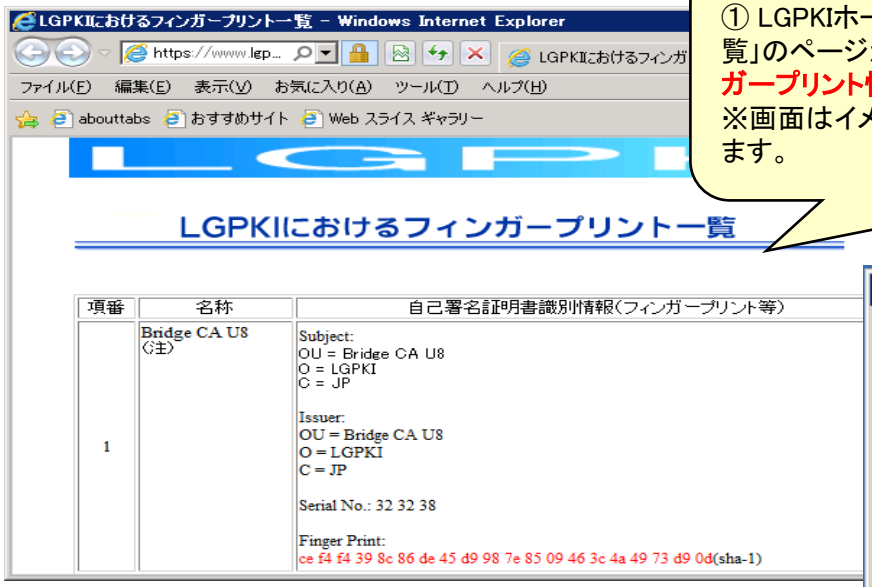
LGPKIにおけるアプリケーションCA G3 Subの下位CA証明書ダウンロード
LGPKIにおけるWEBサーバ証明書等を発行するアプリケーションCA G3 Sub(第三世代)の下位CA証明書です。

LGPKIにおけるアプリケーションCA G4 Rootの自己署名証明書ダウンロード
LGPKIにおける自己署名証明書及び下位CA証明書を発行するアプリケーションCA G4 Root(第四世代)の自己署名証明書です。

LGPKIにおけるアプリケーションCA G4 Subの下位CA証明書ダウンロード
LGPKIにおけるWEBサーバ証明書等を発行するアプリケーションCA G4 Sub(第四世代)の下位CA証明書です。

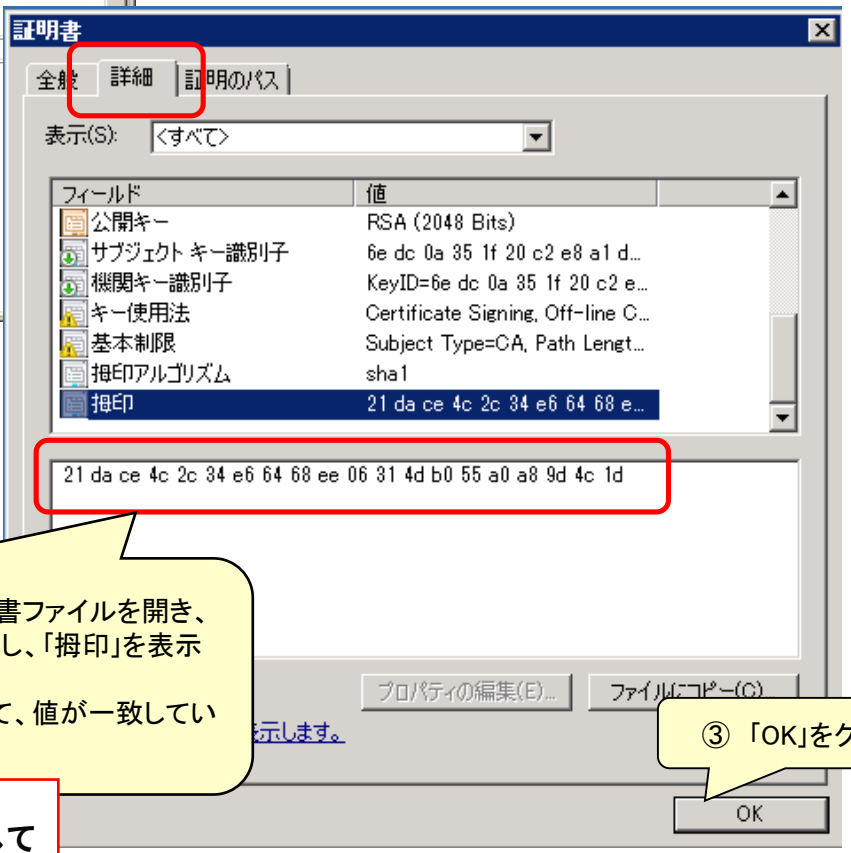
アプリケーションCA	CP/CPS	
	アプリケーションCA G3(Root)CP/CPS	2015.12.18付けでRFC3647準拠に伴う全面見直しを実施 CP/CPS改訂履歴
	アプリケーションCA G3(Sub)CP/CPS	2015.12.18付けでRFC3647準拠に伴う全面見直しを実施 CP/CPS改訂履歴
	アプリケーションCA G4(Root)CP/CPS	2017.7.3付けのAPCAG4立上げに伴う掲載 CP/CPS改訂履歴
	アプリケーションCA G4(Sub)CP/CPS	2017.7.3付けのAPCAG4立上げに伴う掲載 CP/CPS改訂履歴
	CA秘密鍵危殆化に関する情報	
	－(該当なし)	
	第3世代(APCA G3 新暗号)の自己署名証明書等	
	APCA G3(Root)の自己署名証明書のダウンロード	フィンガープリント
	APCA G3(Sub)の下位CA証明書のダウンロード	フィンガープリント
	第4世代(APCA G4 新暗号)の自己署名証明書等	
	APCA G4(Root)の自己署名証明書のダウンロード	フィンガープリント
	APCA G4(Sub)の下位CA証明書のダウンロード	フィンガープリント
	アプリケーション証明書の発行、更新及び失効(申請書類)	
	LGPKI 証明書利用者の手引 様式	
組織CA	CP/CPS	
	組織CA CP/CPS	2015.12.18付けでRFC3647準拠に伴う全面見直しを実施 CP/CPS改訂履歴
	相互認証	
	組織CAと相互認証したCAの名称	ブリッジCA
	組織CAと相互認証を取り消したCAの名称	－
	CA秘密鍵危殆化に関する情報	
	－(該当なし)	
	中間CA証明書(ブリッジCAから組織CAへの相互認証証明書)	
	中間CA証明書 のダウンロード	フィンガープリント
	エンドエンティティ証明書の発行、更新及び失効(申請書類)	

2　フィンガープリントの確認



① LGPKIホームページの「LGPKIにおけるフィンガープリント一覧」のページから、**Application CA G4 Root(第四世代)のフィンガープリント情報**をメモ等に控えておく。
※画面はイメージです。実際のフィンガープリントの値は異なります。

インターネット側ページ：https://www.lgpki.jp/CAInfo/fingerprint.htm
LGWAN側ページ：https://center.lgwan.jp/CAInfo/fingerprint.html



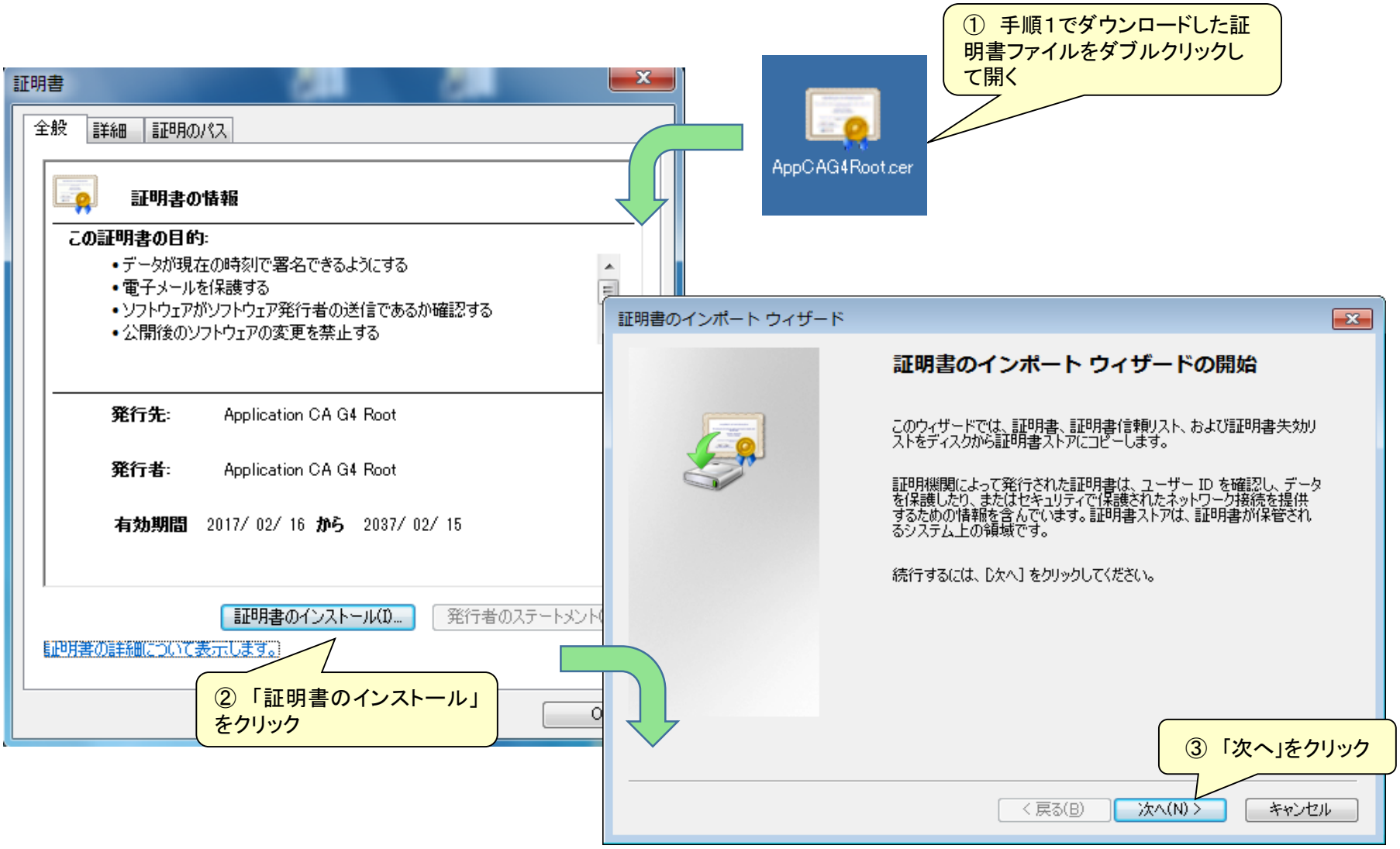
② 手順1でダウンロードした自己署名証明書ファイルを開き、「証明書」画面において「詳細」タブをクリックし、「拇印」を表示する。
①で控えたフィンガープリント情報と比較して、値が一致していることを確認する。

③ 「OK」をクリック

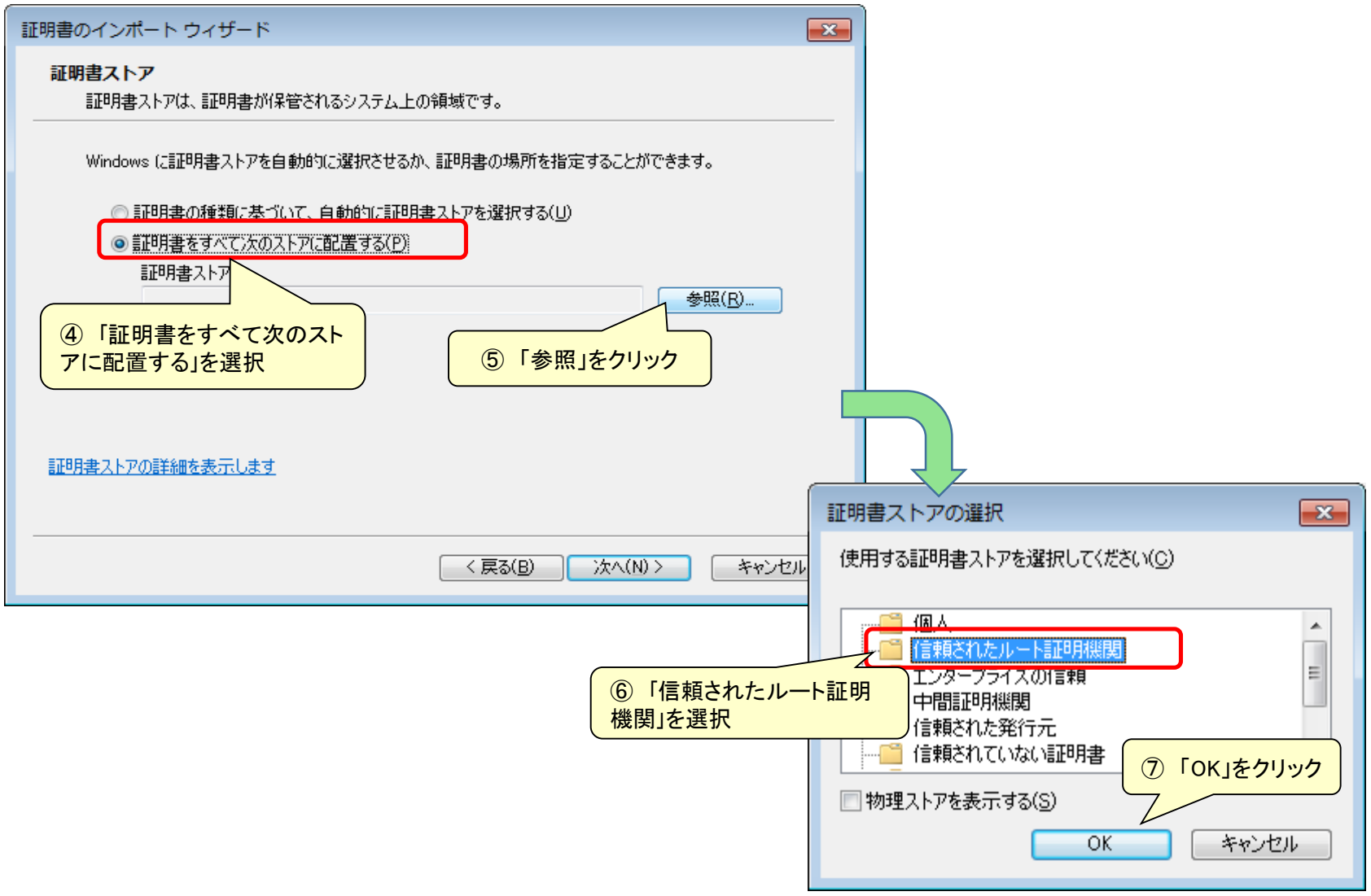
※県情報政策課注
LGWAN側ページのこのURLは誤っていますので，クリックしても表示されません。正しいURLは次のとおりです。
https://center.lgwan.jp/use/CAInfo/fingerprint.html

3　自己署名証明書のインストール

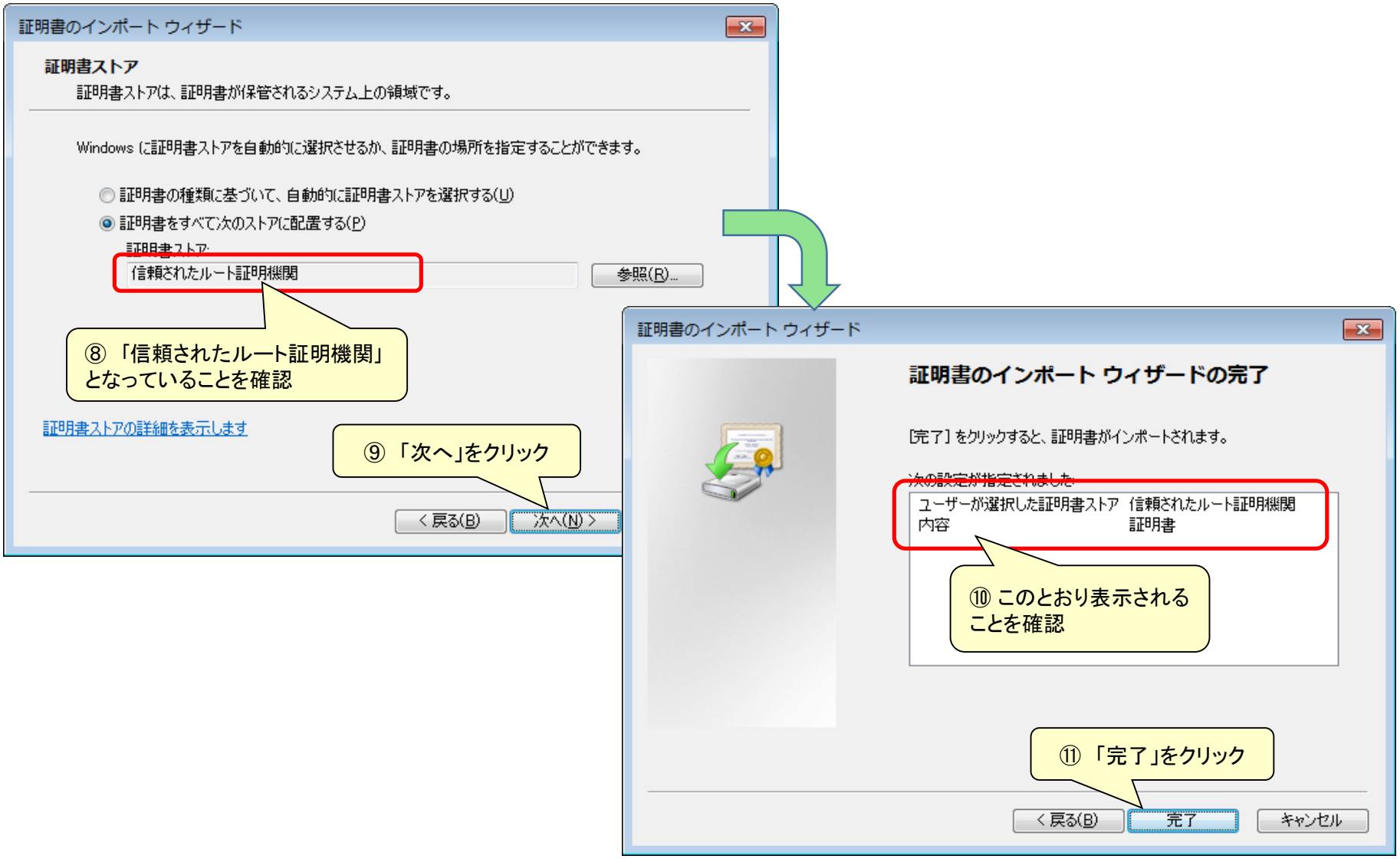
次の手順で自己署名証明書を証明書ストアにインストールする。



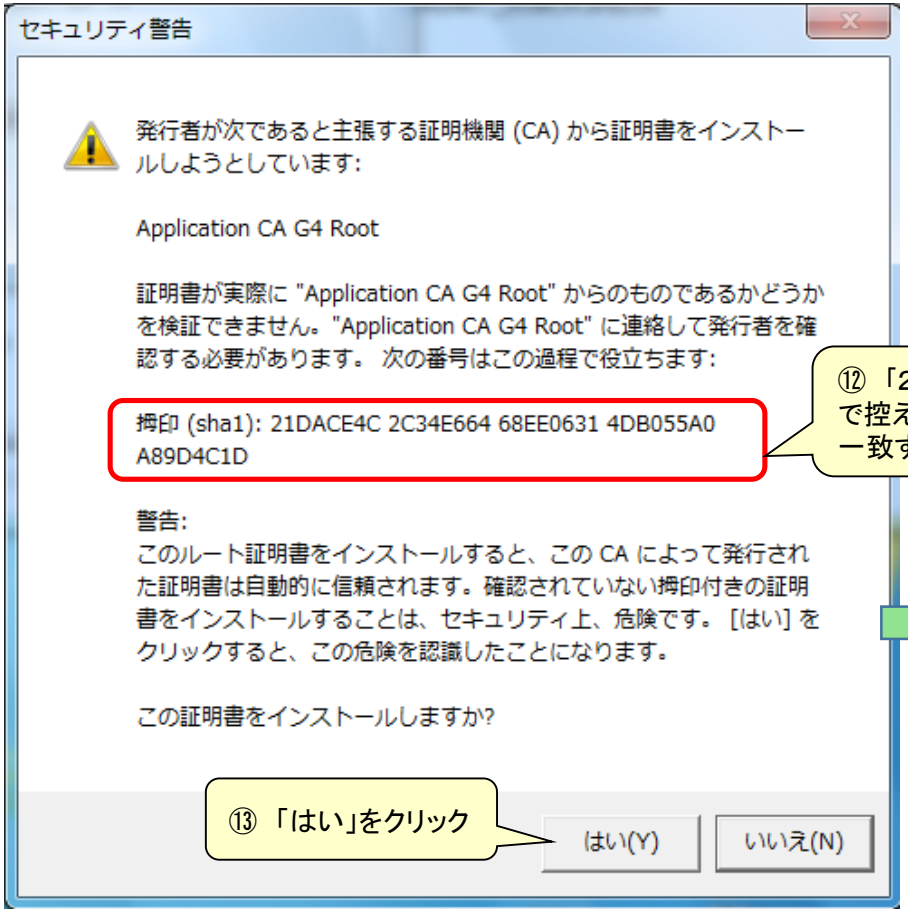
3　自己署名証明書のインストール



3　自己署名証明書のインストール

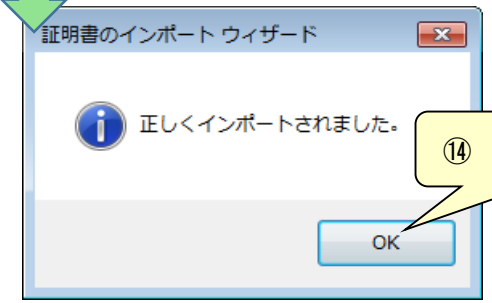


3　自己署名証明書のインストール



⑫ 「2　フィンガープリントの確認」の①で控えておいたフィンガープリントの値と一致することを確認する。

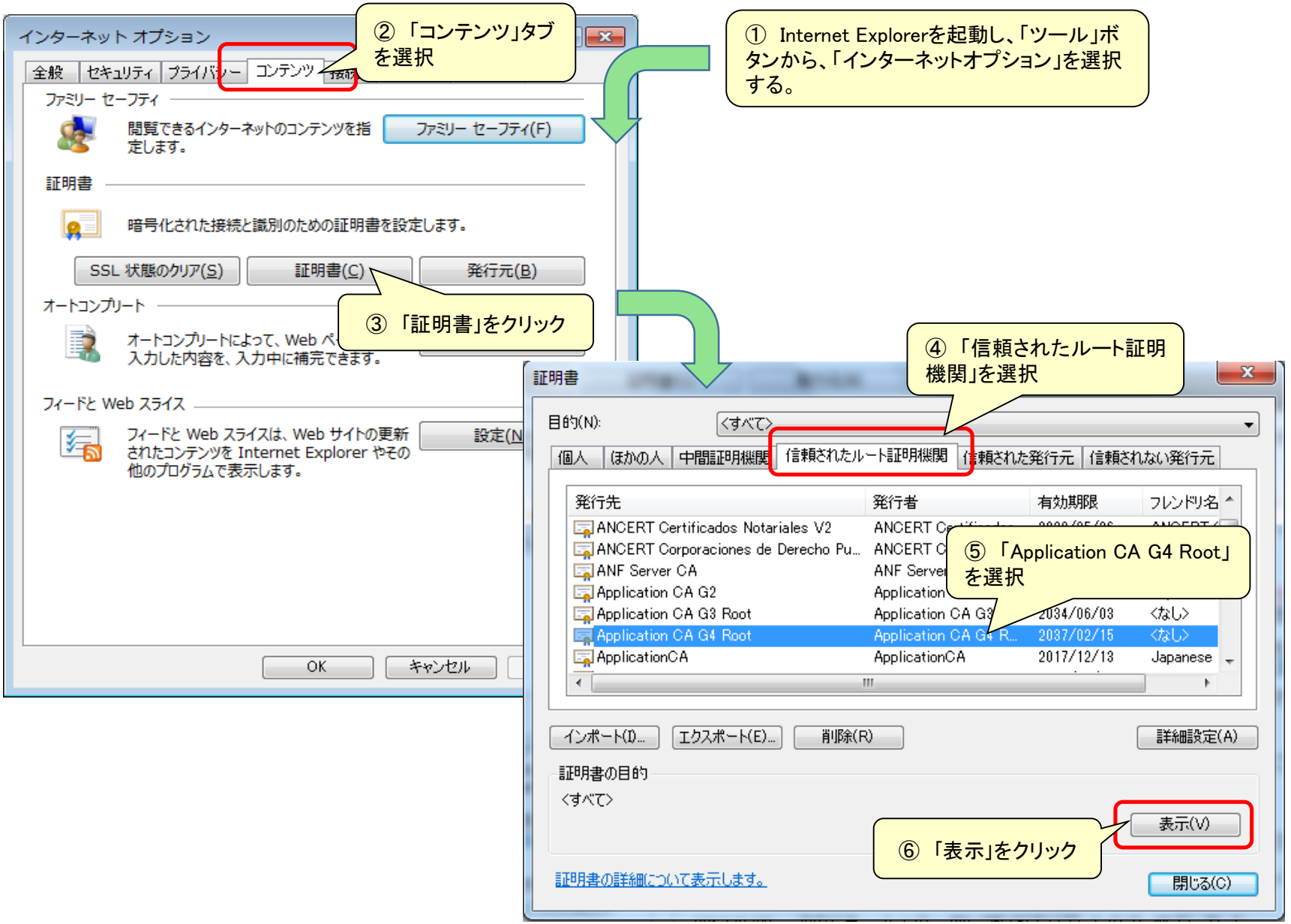
⑬ 「はい」をクリック



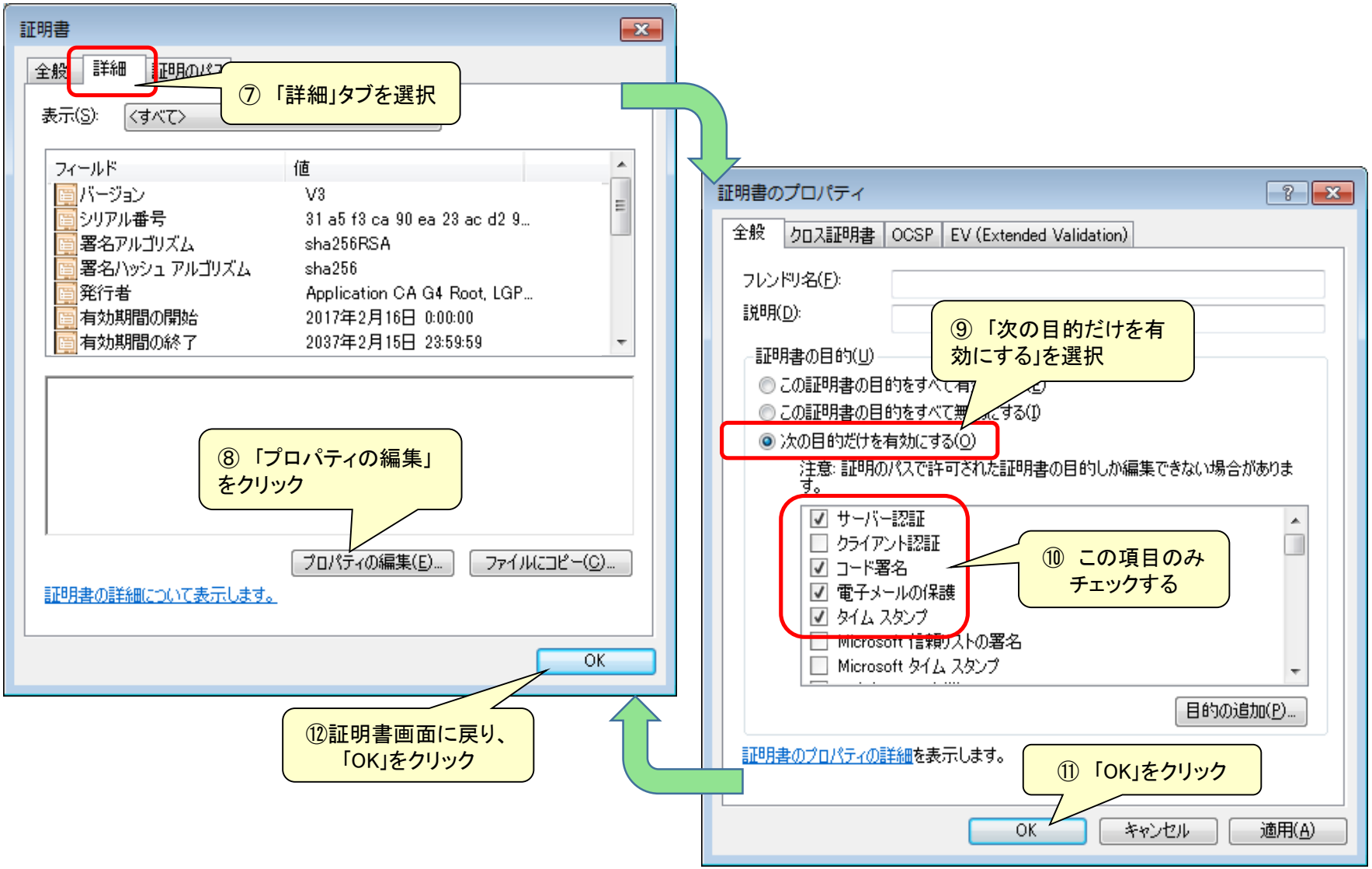
⑭ 「OK」をクリック

自己署名証明書のインストール完了後は、手順1でダウンロードした自己署名証明書ファイル（2ページ参照）を削除しても問題ありません。

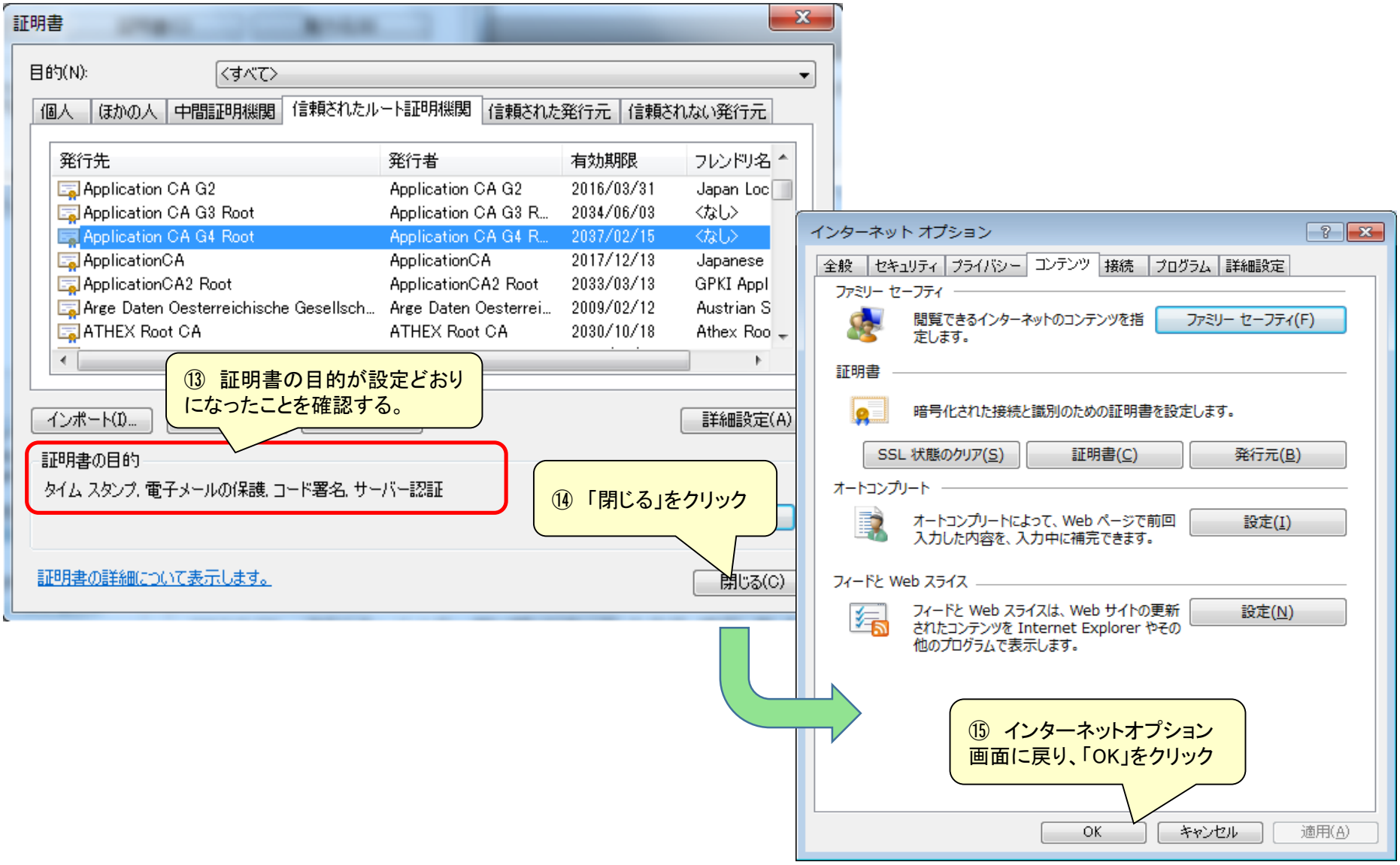
4　証明書の目的の設定


① Internet Explorerを起動し、「ツール」ボタンから、「インターネットオプション」を選択する。
② 「コンテンツ」タブを選択
③ 「証明書」をクリック
④ 「信頼されたルート証明機関」を選択
⑤ 「Application CA G4 Root」を選択
⑥ 「表示」をクリック
インターネット オプション
全般
セキュリティ
プライバシー
コンテンツ
ファミリー セーフティ
閲覧できるインターネットのコンテンツを指定します。
ファミリー セーフティ(F)
証明書
暗号化された接続と識別のための証明書を設定します。
SSL 状態のクリア(S)
証明書(C)
発行元(B)
オートコンプリート
フィードと Web スライス
フィードと Web スライスは、Web サイトの更新されたコンテンツを Internet Explorer やその他のプログラムで表示します。
設定(N
OK
キャンセル
証明書
目的(N):
<すべて>
個人
ほかの人
中間証明機関
信頼されたルート証明機関
信頼された発行元
信頼されない発行元
発行先
発行者
有効期限
フレンドリ名
ANCERT Certificados Notariales V2
ANCERT Corporaciones de Derecho Pu...
ANF Server CA
Application CA G2
Application CA G3 Root
Application CA G4 Root
ApplicationCA
2034/06/03
2037/02/15
2017/12/13
Japanese
インポート(I)...
エクスポート(E)...
削除(R)
詳細設定(A)
証明書の目的
<すべて>
表示(V)
証明書の詳細について表示します。
閉じる(C)

4　証明書の目的の設定


証明書
全般
詳細
⑦ 「詳細」タブを選択
表示(S):
<すべて>
フィールド
値
バージョン
V3
シリアル番号
31 a5 f3 ca 90 ea 23 ac d2 9...
署名アルゴリズム
sha256RSA
署名ハッシュ アルゴリズム
sha256
発行者
Application CA G4 Root, LGP...
有効期間の開始
2017年2月16日 0:00:00
有効期間の終了
2037年2月15日 23:59:59
⑧ 「プロパティの編集」をクリック
プロパティの編集(E)...
ファイルにコピー(C)...
証明書の詳細について表示します。
OK
⑫証明書画面に戻り、「OK」をクリック
証明書のプロパティ
全般
クロス証明書
OCSP
EV (Extended Validation)
フレンドリ名(F):
説明(D):
⑨ 「次の目的だけを有効にする」を選択
証明書の目的(U)
この証明書の目的をすべて有効にする(E)
この証明書の目的をすべて無効にする(I)
次の目的だけを有効にする(O)
注意: 証明のパスで許可された証明書の目的しか編集できない場合があります。
サーバー認証
クライアント認証
コード署名
電子メールの保護
タイム スタンプ
Microsoft 信頼リストの署名
Microsoft タイム スタンプ
⑩ この項目のみチェックする
目的の追加(P)...
証明書のプロパティの詳細を表示します。
⑪ 「OK」をクリック
OK
キャンセル
適用(A)

4　証明書の目的の設定


証明書
目的(N):
<すべて>
個人
ほかの人
中間証明機関
信頼されたルート証明機関
信頼された発行元
信頼されない発行元
発行先
発行者
有効期限
フレンドリ名
Application CA G2
Application CA G2
2016/03/31
Japan Loc
Application CA G3 Root
Application CA G3 R...
2034/06/03
<なし>
Application CA G4 Root
Application CA G4 R...
2037/02/15
<なし>
ApplicationCA
ApplicationCA
2017/12/13
Japanese
ApplicationCA2 Root
ApplicationCA2 Root
2033/03/13
GPKI Appl
Arge Daten Oesterreichische Gesellsch...
Arge Daten Oesterrei...
2009/02/12
Austrian S
ATHEX Root CA
ATHEX Root CA
2030/10/18
Athex Roo
⑬　証明書の目的が設定どおりになったことを確認する。
インポート(I)...
詳細設定(A)
証明書の目的
タイム スタンプ, 電子メールの保護, コード署名, サーバー認証
⑭　「閉じる」をクリック
証明書の詳細について表示します。
閉じる(C)
インターネット オプション
全般
セキュリティ
プライバシー
コンテンツ
接続
プログラム
詳細設定
ファミリー セーフティ
閲覧できるインターネットのコンテンツを指定します。
ファミリー セーフティ(F)
証明書
暗号化された接続と識別のための証明書を設定します。
SSL 状態のクリア(S)
証明書(C)
発行元(B)
オートコンプリート
オートコンプリートによって、Web ページで前回入力した内容を、入力中に補完できます。
設定(I)
フィードと Web スライス
フィードと Web スライスは、Web サイトの更新されたコンテンツを Internet Explorer やその他のプログラムで表示します。
設定(N)
⑮　インターネットオプション画面に戻り、「OK」をクリック
OK
キャンセル
適用(A)

5　Google Chrome（Windows版）の場合

「1　APCA G4（Root）自己署名証明書の入手」から「3　自己署名証明書のインストール」までの手順は、Internet Explorerの場合と同じです。「4　証明書の目的の設定」は次の手順で実施してください。