

アプリケーション認証局(第四世代)(Root)
自己署名証明書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鍵ベアの更新を実施し、**新暗号**の新しいCA鍵ベアにより発行した自己署名証明書です。
CA鍵ベ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鍵ベアの更新に伴い、平成26年9月13日に新しく発行されました。
CA鍵ベア更新前の中間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
組織CA	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	
	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)		
LGPKI 証明書利用者の手引 様式		

2 フィンガープリントの確認

項番	名称	自己署名証明書識別情報(フィンガープリント等)
1	Bridge CA US (注)	Subject: OU = Bridge CA U8 O = LGPKI C = JP Issuer: OU = Bridge CA U8 O = LGPKI C = JP Serial No.: 32 32 38 Finger Print: ce f4 f4 39 8c 86 de 45 d9 98 7e 85 09 46 3c 4a 49 73 d9 0d(sha-1)

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.lgpkj.jp/CAInfo/fingerprint.htm>
LGWAN側ページ: <https://center.lgwan.jp/CAInfo/fingerprint.html>

証明書

全般 詳細 証明のパス

表示(S): <すべて>

フィールド	値
公開キー	RSA (2048 Bits)
サブジェクト キー識別子	6e dc 0a 35 1f 20 c2 e8 a1 d...
機関キー識別子	KeyID=6e dc 0a 35 1f 20 c2 e...
キー使用法	Certificate Signing, Off-line C...
基本制限	Subject Type=CA, Path Lengt...
指印アルゴリズム	sha1
指印	21 da ce 4c 2c 34 e6 64 68 e...

21 da ce 4c 2c 34 e6 64 68 ee 06 31 4d b0 55 a0 a8 9d 4c 1d

プロパティの編集(E)... ファイルにコピー(C)...

OK

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、「指印」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。

① 手順1でダウンロードした証明書ファイルをダブルクリックして開く

証明書

全般 詳細 証明のパス

証明書の情報

この証明書の目的:

- データが現在の時刻で署名できるようにする
- 電子メールを保護する
- ソフトウェアがソフトウェア発行者の送信であるか確認する
- 公開後のソフトウェアの変更を禁止する

発行先: Application CA G4 Root

発行者: Application CA G4 Root

有効期間 2017/ 02/ 16 から 2037/ 02/ 15

証明書のインストール(I)... 発行者のステートメント

証明書の詳細について表示します。

証明書のインポート ウィザード

証明書のインポート ウィザードの開始

このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピーします。

証明機関によって発行された証明書は、ユーザー ID を確認し、データを保護したり、またはセキュリティで保護されたネットワーク接続を提供するための情報を含んでいます。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。

続行するには、[次へ] をクリックしてください。

< 戻る(B) 次へ(N) > キャンセル

② 「証明書のインストール」をクリック

③ 「次へ」をクリック

3 自己署名証明書のインストール

The image shows two windows from a Windows operating system. The first window is titled '証明書のインポート ウィザード' (Certificate Import Wizard) and is on the '証明書ストア' (Certificate Store) step. It contains two radio button options: '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(U)' and '証明書をすべて次のストアに配置する(P)'. The second option is selected and circled in red. Below the options is a text box for '証明書ストア' and a '参照(B)...' button. A callout box labeled '④ 「証明書をすべて次のストアに配置する」を選択' points to the selected radio button. Another callout box labeled '⑤ 「参照」をクリック' points to the '参照(B)...' button. The second window is titled '証明書ストアの選択' (Select Certificate Store) and prompts the user to '使用する証明書ストアを選択してください(C)'. It shows a tree view of certificate stores under '個人' (Personal), with '信頼されたルート証明機関' (Trusted Root Certification Authorities) selected and circled in red. Other visible stores include 'エンタープライズの信頼' (Enterprise Trust), '中間証明機関' (Intermediate Certification Authorities), '信頼された発行元' (Trusted Issuers), and '信頼されていない証明書' (Untrusted Certificates). There is also a checkbox for '物理ストアを表示する(S)'. A callout box labeled '⑥ 「信頼されたルート証明機関」を選択' points to the selected store. Another callout box labeled '⑦ 「OK」をクリック' points to the 'OK' button.

証明書のインポート ウィザード

証明書ストア

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。

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。

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(U)

証明書をすべて次のストアに配置する(P)

証明書ストア

参照(B)...

④ 「証明書をすべて次のストアに配置する」を選択

⑤ 「参照」をクリック

証明書ストアの詳細を表示します

< 戻る(B) 次へ(N) > キャンセル

証明書ストアの選択

使用する証明書ストアを選択してください(C)

個人

信頼されたルート証明機関

エンタープライズの信頼

中間証明機関

信頼された発行元

信頼されていない証明書

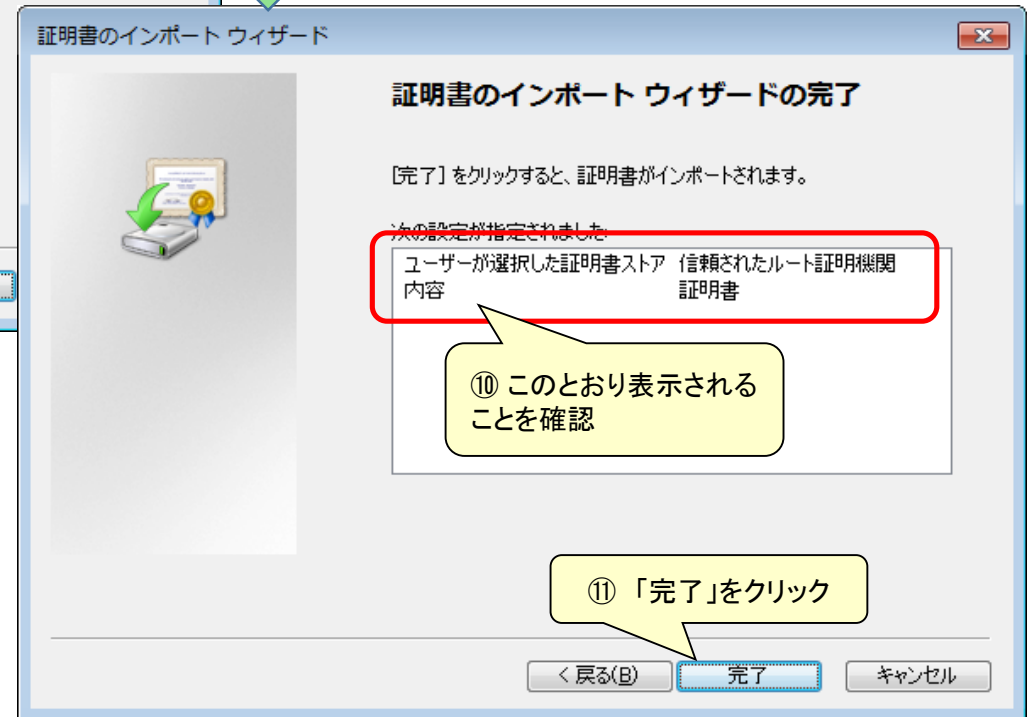
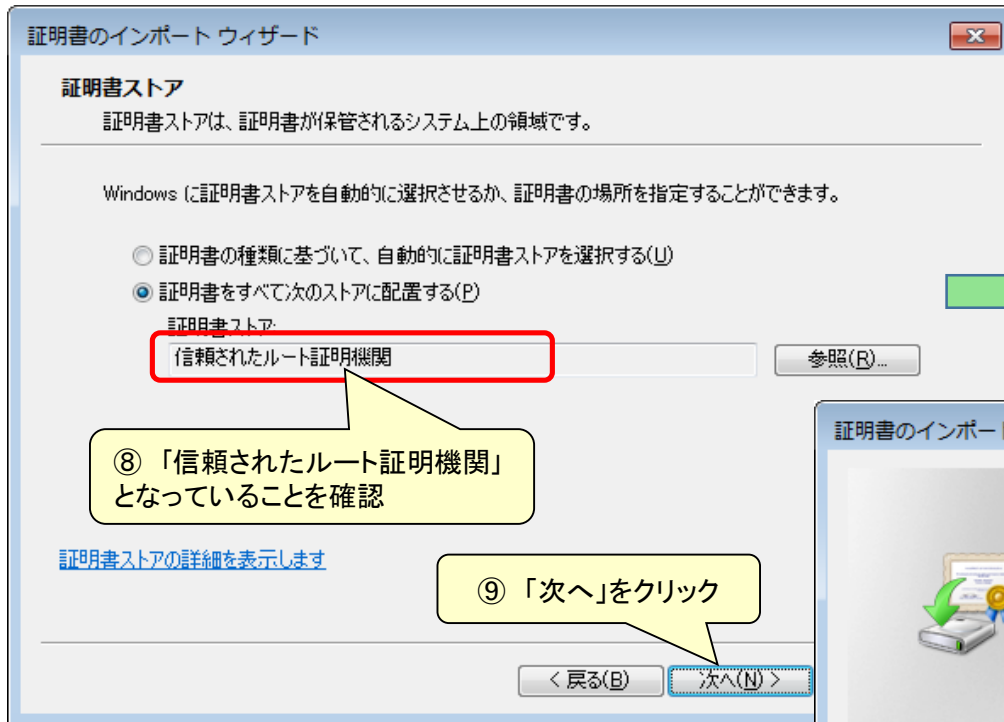
物理ストアを表示する(S)

OK キャンセル

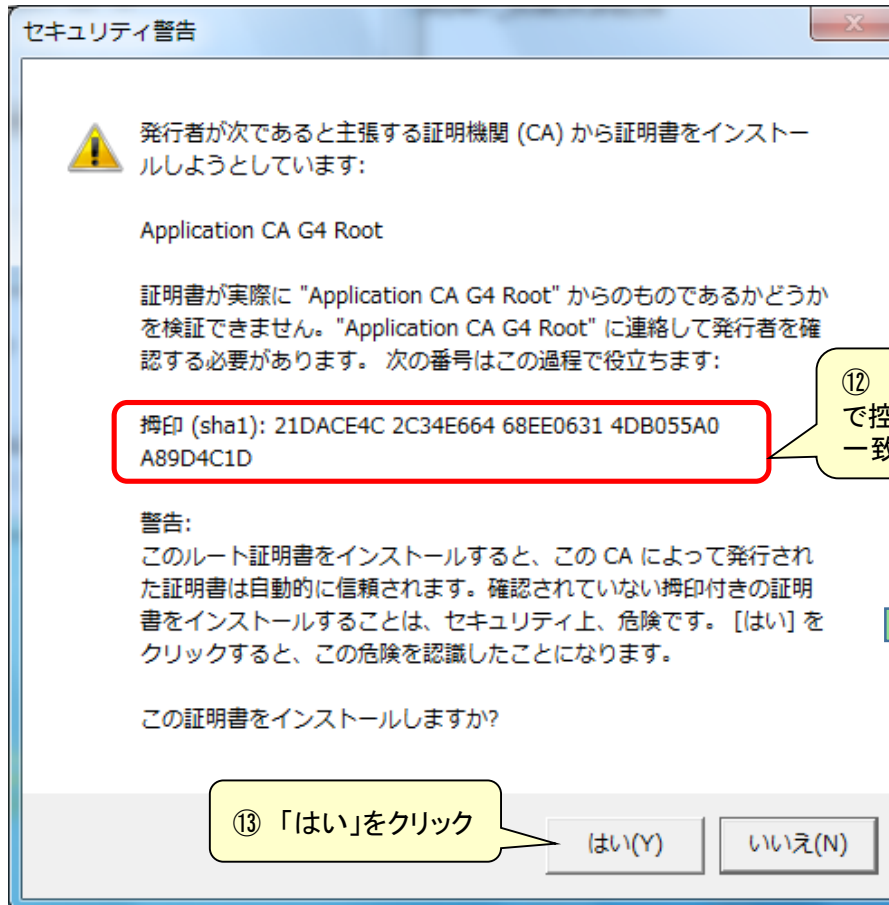
⑥ 「信頼されたルート証明機関」を選択

⑦ 「OK」をクリック

3 自己署名証明書のインストール

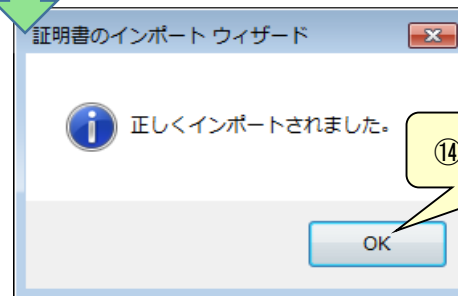


3 自己署名証明書のインストール



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

発行先	発行者	有効期限	フレンドリ名
ANCERT Certificados Notariales V2	ANCERT Certificados Notariales V2	0000/05/06	ANCERT (I)
ANCERT Corporaciones de Derecho Pu...	ANCERT Corporaciones de Derecho Pu...		
ANF Server CA	ANF Server CA		
Application CA G2	Application CA G2		
Application CA G3 Root	Application CA G3 Root	2034/06/03	<なし>
Application CA G4 Root	Application CA G4 Root	2037/02/15	<なし>
ApplicationCA	ApplicationCA	2017/12/13	Japanese

⑤ 「Application CA G4 Root」を選択

⑥ 「表示」をクリック

表示(V)

閉じる(C)

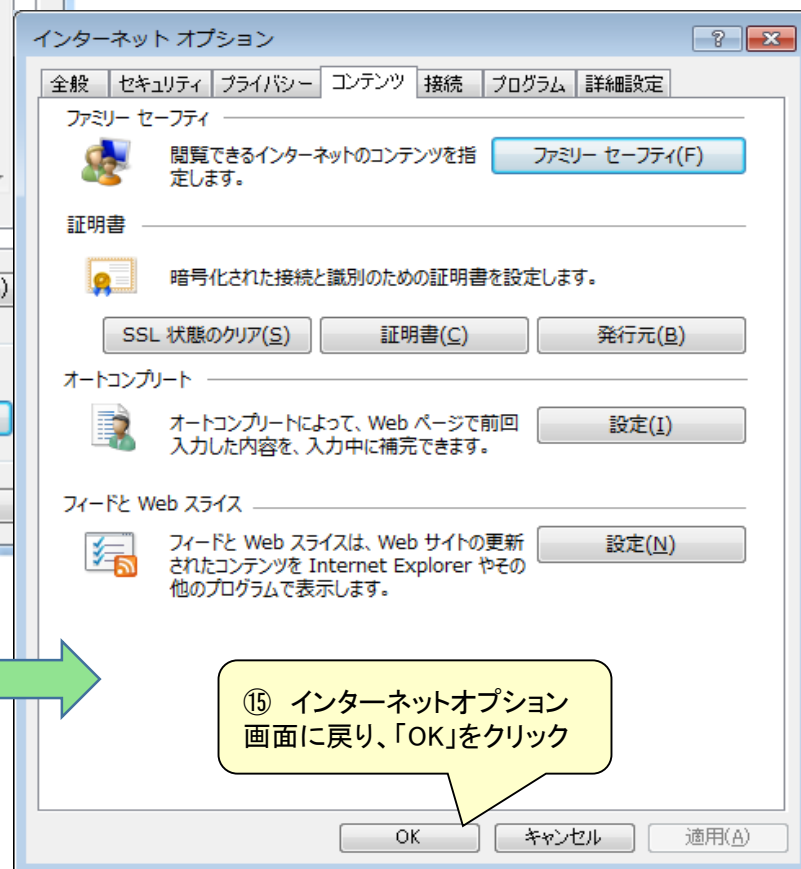
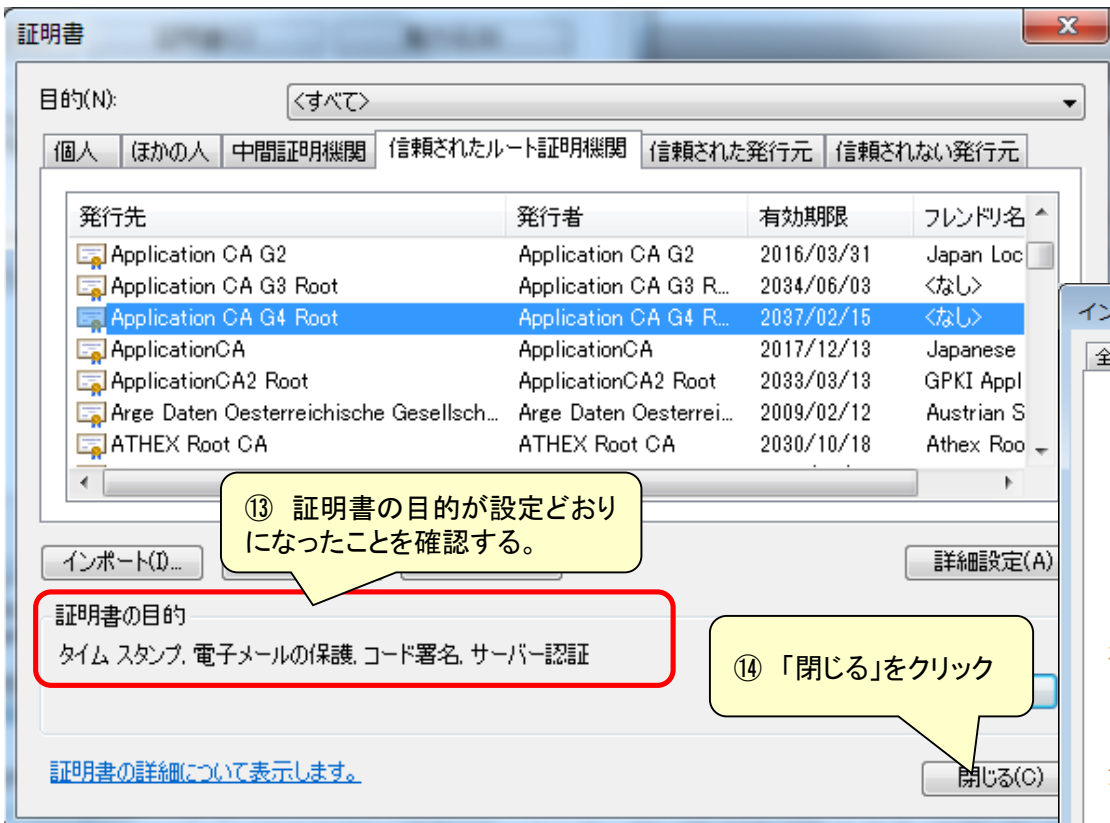
4 証明書の目的の設定

The image shows two windows from a certificate management application. The left window is titled '証明書' (Certificate) and has three tabs: '全般' (General), '詳細' (Details), and '証明のパス' (Certificate Paths). The '詳細' tab is selected, showing a table of certificate fields and their values. A callout box points to the '詳細' tab with the text '⑦ 「詳細」タブを選択' (Select the 'Details' tab). Below the table, there are buttons for 'プロパティの編集(E)...' (Edit Properties...) and 'ファイルにコピー(C)...' (Copy to File...). A callout box points to the 'プロパティの編集(E)...' button with the text '⑧ 「プロパティの編集」をクリック' (Click 'Edit Properties'). At the bottom of the window is an 'OK' button, with a callout box pointing to it that says '⑫ 証明書画面に戻り、「OK」をクリック' (Return to the certificate screen and click 'OK').

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

The right window is titled '証明書のプロパティ' (Certificate Properties) and has three tabs: '全般' (General), 'クロス証明書' (Cross-Certificate), 'OCSP', and 'EV (Extended Validation)'. The '全般' tab is selected. It contains fields for 'フレンドリ名(E):' (Friendly Name) and '説明(D):' (Description). Below these is the '証明書の目的(U)' (Certificate Purposes) section, which has three radio button options: 'この証明書の目的をすべて有効にする(O)' (Enable all purposes of this certificate), 'この証明書の目的をすべて無効にする(O)' (Disable all purposes of this certificate), and '次の目的だけを有効にする(O)' (Enable only the following purposes). The third option is selected and highlighted with a red box. A callout box points to it with the text '⑨ 「次の目的だけを有効にする」を選択' (Select 'Enable only the following purposes'). Below the radio buttons is a note: '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。' (Note: You may not be able to edit certificate purposes that are permitted by the certificate path). Below the note is a list of purposes with checkboxes: 'サーバー認証' (checked), 'クライアント認証' (unchecked), 'コード署名' (checked), '電子メールの保護' (checked), 'タイム スタンプ' (checked), 'Microsoft 信頼リストの署名' (unchecked), and 'Microsoft タイム スタンプ' (unchecked). A callout box points to the checked items with the text '⑩ この項目のみチェックする' (Check only these items). At the bottom of the window are 'OK', 'キャンセル' (Cancel), and '適用(A)' (Apply) buttons. A callout box points to the 'OK' button with the text '⑪ 「OK」をクリック' (Click 'OK').

4 証明書の目的の設定



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。

The image consists of three screenshots of the Google Chrome interface, illustrating the steps to reach the certificate management settings.

- Top Left Screenshot:** Shows the Chrome menu. The '設定(S)' (Settings) option is highlighted with a red box. A callout bubble points to it with the text: **① Google Chromeの設定をクリック** (Click Google Chrome settings).
- Top Right Screenshot:** Shows the Chrome Settings page (chrome://settings). The '詳細設定を表示...' (Show advanced settings) link is highlighted with a red box. A callout bubble points to it with the text: **② 設定画面で詳細設定を表示** (Show advanced settings on the settings screen).
- Bottom Screenshot:** Shows the 'HTTPS/SSL' section of the settings. The '証明書の管理...' (Manage certificates...) button is highlighted with a red box. A callout bubble points to it with the text: **③ 詳細設定内のHTTPS/SSLの「証明書の管理」をクリック** (Click 'Manage certificates' in the HTTPS/SSL section of the advanced settings). Below this, it says: **→ 証明書ストアの画面が表示されるので、これ以降は、Internet Explorerの場合における「4 証明書の目的の設定」の④(スライド8参照)からの手順に沿って設定を行ってください。** (Since the certificate store screen is displayed, from here onwards, follow the procedure from step ④ (see slide 8) of '4 Certificate Purpose Settings' in the case of Internet Explorer).

Green arrows indicate the flow from the menu to the settings page, and then to the advanced settings section.