

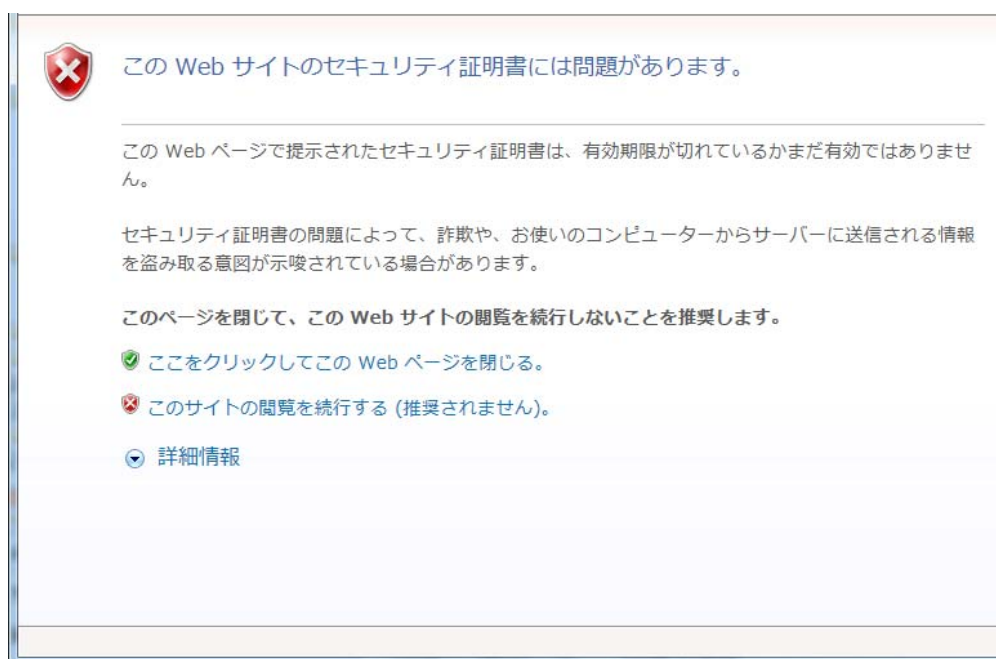
在留カード等番号失効情報照会へ接続した際のエラー画面について

平成28年12月28日
法務省入国管理局

在留カード等番号失効情報照会においては、政府認証基盤（GPKI）が発行するセキュリティ証明書を使用しておりますところ、今般、証明書の更新が行われました。

これにより、御利用の環境によっては、在留カード等番号失効情報照会へ接続した際に、下記のとおりエラー画面が表示される場合がありますが、この場合、「**政府認証基盤（GPKI）のホームページ**」から、最新の証明書ファイルをインストールしていただくことで正常に使用可能となりますので、対応手順について添付のとおり御案内いたします。

皆様には、御不便、御迷惑をお掛けしますが、御理解と御協力をお願いいたします。



「政府認証基盤（GPKI）のホームページ」 <http://www.gpki.go.jp/>
(セキュリティ証明書に関するホームページ)

お問い合わせ先 <http://www.gpki.go.jp/sendto.html>

※「在留カード等番号失効情報照会」に関する内容につきましては、
法務省入国管理局出入国管理情報官付システム管理第二係まで御確認願います。

TEL：03-3580-4111（内線：5688）

<対応手順>

(1) 以下のURLにアクセスし、「政府認証基盤(GPKI)のホームページ」を開く。
<http://www.gpki.go.jp/>

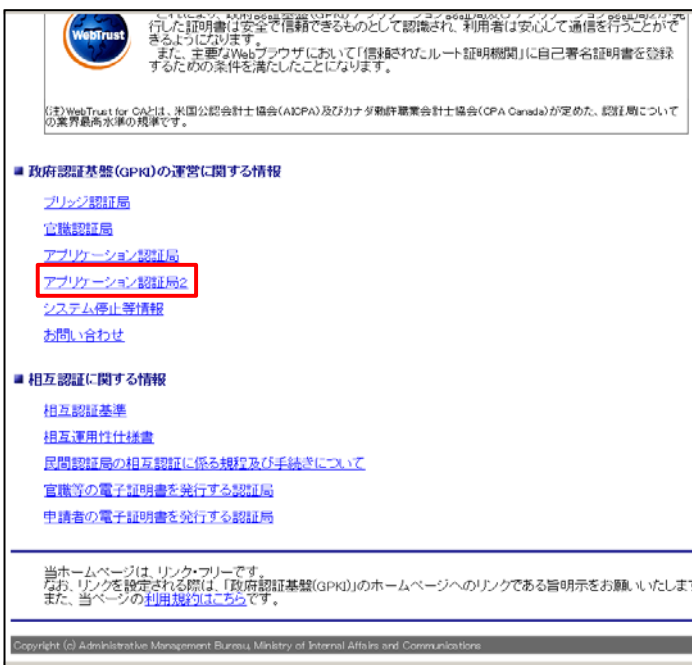


The screenshot shows the homepage of the Government Public Key Infrastructure (GPKI). At the top, there is a logo for GPKI and the text "政府認証基盤(GPKI) 電子政府の認証基盤に関する情報を案内するホームページです。" (Government Public Key Infrastructure (GPKI) Home page providing information on the authentication infrastructure of the electronic government.) Below this, there are several sections:

- 重要なお知らせ** (Important Notice): "政府認証基盤(GPKI)のサービス停止について" (Regarding the suspension of GPKI services).
- お知らせ** (Notice): Information about the suspension of services and the need to update certificates.
- 政府認証基盤(GPKI)についてのご案内** (Introduction to GPKI): A link to "政府認証基盤(GPKI)について" (About GPKI) and "政府における取組み" (Government initiatives).
- 政府認証基盤(GPKI)の運用に関する情報** (Information on GPKI operations): A link to "プリンツ認証局" (Prinzip Certification Authority).

A central box contains a WebTrust logo and text: "政府認証基盤(GPKI)アプリケーション認証局及びアプリケーション認証局2では、「WebTrust for CA® (Certification Authority)」の規準に基づき検証報告書を取得しました。これにより、政府認証基盤(GPKI)アプリケーション認証局及びアプリケーション認証局2が発行した証明書は安全で信頼できるものとして認識され、利用者は安心して通信を行うことができます。また、主要なWebブラウザにおいて「信頼されたルート証明機関」に自己署名証明書を登録するための条件を満たしたことになります。" (The GPKI Application Certification Authority and Application Certification Authority 2 have obtained a WebTrust for CA® (Certification Authority) compliance report. This means that certificates issued by the GPKI Application Certification Authority and Application Certification Authority 2 are recognized as safe and reliable, allowing users to communicate with confidence. Additionally, the self-signed certificates are registered as trusted root certification authorities in major web browsers, meeting the conditions for this recognition.)

(2) 「政府認証基盤(GPKI)の運用に関する情報」の「アプリケーション認証局2」をクリックする。



The screenshot shows the "政府認証基盤(GPKI)の運用に関する情報" (Information on GPKI operations) page. It features a list of links under the heading "■ 政府認証基盤(GPKI)の運用に関する情報":

- プリンツ認証局
- 官機認証局
- アプリケーション認証局
- アプリケーション認証局2** (highlighted with a red box)
- システム停止等情報
- お問い合わせ

Below this list, there is another section "■ 相互認証に関する情報" (Information on mutual authentication) with links to "相互認証基準", "相互運用性仕様書", "民間認証局の相互認証に係る規程及び手続書について", "官機等の電子証明書を発行する認証局", and "申請者の電子証明書を発行する認証局".

At the bottom, there is a footer: "Copyright (c) Administrative Management Bureau, Ministry of Internal Affairs and Communications".

- (3) 切り替わったページ「アプリケーション認証局2」において、「アプリケーション認証局2の証明書」の「アプリケーション認証局2(Root)の自己署名証明書」をクリックし、**ファイル「APCA2Root.cer」をデスクトップ上に保存する。**

アプリケーション認証局2は、平成25年3月からの運営を開始しました。

■ アプリケーション認証局2の運営に関する情報
[アプリケーション認証局2のCP/CPS](#)

■ アプリケーション認証局2の証明書について

◆ アプリケーション認証局2(Root)自己署名証明書のインストール方法について

- Windows Vista、Windows 7、Windows 8 かつ Internet Explorer、Safari、Google Chrome をご利用の方
 ※Firefoxをご利用で「安全な接続ではありません」が表示される方は[こちら](#)
- Mac OS X Mountain Lion (v10.8.5) かつ Safari をご利用の方
- Androidで標準ブラウザをご利用の方

◆ アプリケーション認証局2の証明書

- アプリケーション認証局2(Root)の自己署名証明書 (DER)**

証明書のダウンロード時に、ブラウザによっては拡張子が「CER」となる場合があります。
[アプリケーション認証局2\(Sub\)の下位CA証明書が必要な方はこちら](#)

※注意事項
 ダウンロードした証明書が改ざんされていないことを確認するために、ダウンロードした証明書のフィンガープリント(指印)と本ウェブサイトで公開している[フィンガープリント一覧](#)にあるフィンガープリントとを比較して、相違がないことを必ず確認してください。
 なお、各証明書のフィンガープリントは、以下の方法での提供も行っていきます。
 ・官報(平成25年9月10日第6128号)での公示
 ・電子政府の総合窓口(https://www.e-gov.go.jp/fingerprint/gpkihtml)での公開
 ・Mozillaでの公開(APCA2ルートのみ)

証明書に関する問題を発見し緊急連絡される場合は、平日日中(10~17時)であれば[お問い合わせ](#)に記載の電話番号に、夜間・休日であれば下記メールアドレスへご連絡ください。
 kinkyu-renraku-apca@gpki.go.jp

Copyright (c) Administrative Management Bureau, Ministry of Internal Affairs and Communications

注：
 スマートフォンの場合は、そのままインストールして下さい。

- (4) 手順(3)のリンク直下にある「アプリケーション認証局2(Sub)の下位CA証明書が必要な方はこちら」をクリックする。

アプリケーション認証局2は、平成25年3月からの運営を開始しました。

■ アプリケーション認証局2の運営に関する情報
[アプリケーション認証局2のCP/CPS](#)

■ アプリケーション認証局2の証明書について

◆ アプリケーション認証局2(Root)自己署名証明書のインストール方法について

- Windows Vista、Windows 7、Windows 8 かつ Internet Explorer、Safari、Google Chrome をご利用の方
 ※Firefoxをご利用で「安全な接続ではありません」が表示される方は[こちら](#)
- Mac OS X Mountain Lion (v10.8.5) かつ Safari をご利用の方
- Androidで標準ブラウザをご利用の方

◆ アプリケーション認証局2の証明書

- アプリケーション認証局2(Root)の自己署名証明書 (DER)
- アプリケーション認証局2(Sub)の下位CA証明書 (DER)**

証明書のダウンロード時に、ブラウザによっては拡張子が「CER」となる場合があります。
[アプリケーション認証局2\(Sub\)の下位CA証明書が必要な方はこちら](#)

※注意事項
 ダウンロードした証明書が改ざんされていないことを確認するために、ダウンロードした証明書のフィンガープリント(指印)と本ウェブサイトで公開している[フィンガープリント一覧](#)にあるフィンガープリントとを比較して、相違がないことを必ず確認してください。
 なお、各証明書のフィンガープリントは、以下の方法での提供も行っていきます。
 ・官報(平成25年9月10日第6128号)での公示
 ・電子政府の総合窓口(https://www.e-gov.go.jp/fingerprint/gpkihtml)での公開
 ・Mozillaでの公開(APCA2ルートのみ)

証明書に関する問題を発見し緊急連絡される場合は、平日日中(10~17時)であれば[お問い合わせ](#)に記載の電話番号に、夜間・休日であれば下記メールアドレスへご連絡ください。
 kinkyu-renraku-apca@gpki.go.jp

Copyright (c) Administrative Management Bureau, Ministry of Internal Affairs and Communications

- (5) 切り替わったページ「アプリケーション認証局2(Sub)」において、「アプリケーション認証局2(Sub)の証明書」の「アプリケーション認証局2(Sub)の下位CA証明書」をクリックし、**ファイル「APCA2Sub.cer」をデスクトップ上に保存する。**

■ アプリケーション認証局2(Sub)

■ アプリケーション認証局2(Sub)の証明書について

◆ アプリケーション認証局2(Sub)の証明書

- アプリケーション認証局2(Sub)の下位CA証明書 (DER)**
- アプリケーション認証局2(Sub)の下位CA証明書(CSP対応) (DER)

証明書のダウンロード時に、ブラウザによっては拡張子が「CER」となる場合があります。

※注意事項
 ダウンロードした証明書が改ざんされていないことを確認するために、ダウンロードした証明書のフィンガープリント(指印)と本ウェブサイトで公開している[フィンガープリント一覧](#)にあるフィンガープリントとを比較して、相違がないことを必ず確認してください。

Copyright (c) Administrative Management Bureau, Ministry of Internal Affairs and Communications

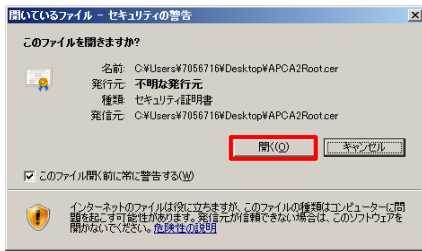
注：
 スマートフォンの場合は、そのままインストールして下さい。

- (6) 御利用の環境がスマートフォンの場合は、これで対応完了です。

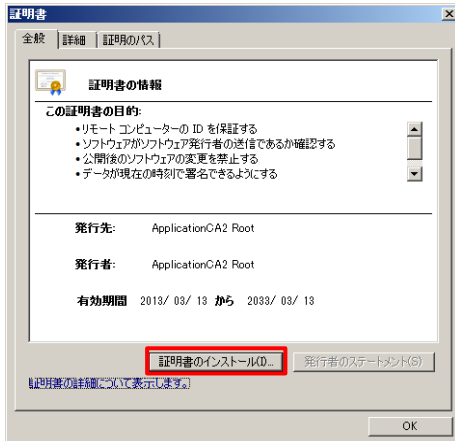
<証明書インストール手順>

※スマートフォンについては、以下の手順は不要です。

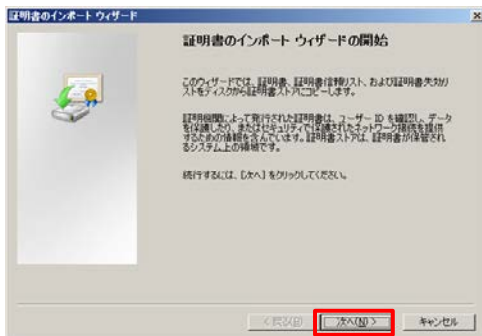
(7) 手順(3)においてデスクトップ上に保存した「APCA2Root.cer」をダブルクリックし、「開く」をクリックする。



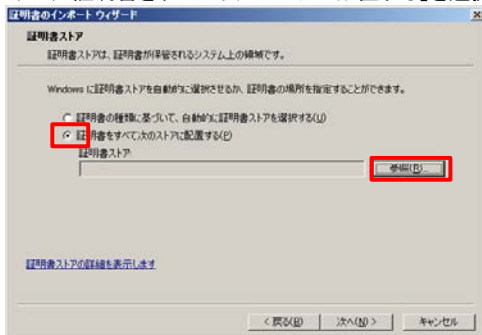
(8) 「証明書のインストール」をクリックする。



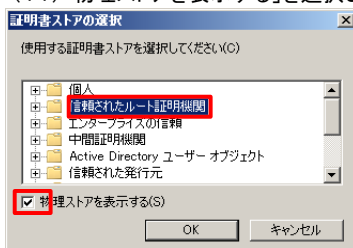
(9) 「次へ」をクリックする。



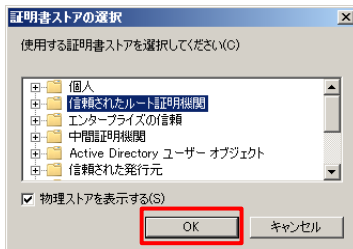
(10) 「証明書をすべて次のストアに配置する」を選択し、「参照」をクリックする。



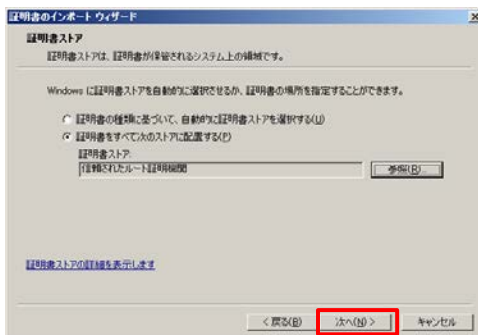
(11) 「物理ストアを表示する」を選択し、「信頼されたルート証明書機関」を選択する。



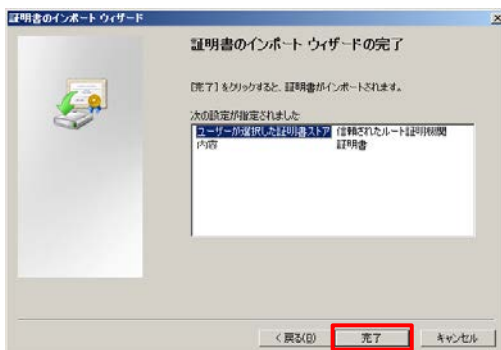
(12)「OK」をクリックする。



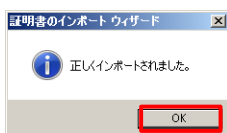
(13)「次へ」をクリックする。



(14)「完了」をクリックする。

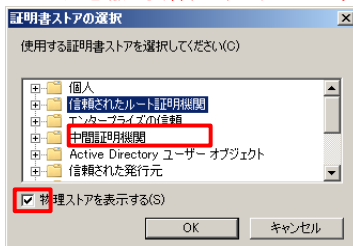


(15)「OK」をクリックする。



(16) 手順(5)においてデスクトップ上に保存した「APCA2Sub.cer」についても、手順(7)～(15)と同様の流れでインストールする。

※ 注意点: 手順(11)においては、「中間証明書機関」を選択すること。



(17)これで、全ての対応が完了です。