

2016年01月28日

PKI プラットフォーム ルート証明書インストール手順書 v6.5.1 (PC、スマートフォン版)

ソフトバンク株式会社

バージョン	改訂日	改訂内容
1.0	2011/09/12	初版作成
5.0	2012/06/25	システム更新に伴う表示内容の改訂
6.0	2013/6/30	Windows8、InternetExplore10 およびスマートフォン(Android 端末)のサポートに伴う改訂
6.1	2013/12/19	iPhone5C/5S および Windows8.1、InternetExplore11 のサポートに伴う改訂
6.2	2014/05/14	Windows XP/ InternetExplore6 サポート終了に伴う記載削除 MAC OS サポートに伴う手順追加
6.3	2014/06/25	認証局延長前のルート証明書インストール削除
6.4	2015/04/01	社名変更に伴う改訂及び対応機種追加
6.5	2015/08/03	SHA-256 対応に伴う改訂
6.5.1	2016/01/28	Microsoft 社 InternetExplorer サポートポリシー変更に伴うサポート OS/ブラウザ改訂

目次

1. はじめに	3
2. 利用端末環境	4
3. ルート証明書のインストール手順	5
3-1. インストール手順 【Windows Vista & Windows 7】	5
3-2. インストール手順 【Windows 8.1】	9
3-3. インストール手順 【iPhone & iPad】	14
3-4. インストール手順 【Android Ver.4.0】	17
3.4.1 事前にルート証明書をインポートする場合	17
3.4.2 証明書取得時にルート証明書をインポートする場合	18
3.4.3 インポートしたルート証明書の内容	19
3-5. インストール手順 【MAC OS】	20

※本マニュアルはサービス仕様の追加・修正等により、お客様へ予告なく改訂する場合がございます。
最新マニュアルは申請受付ウェブサーバにございますのでそちらをご覧ください。

1. はじめに

まず、ルート証明書とは証明書を発行する認証局が正当性を証明するため自ら署名して発行する証明書です。本サービスのルート証明書はオペレーティングシステムにあらかじめ組み込まれていませんので、証明書を利用するデバイスには信頼された証明機関として事前にルート証明書をインストールしていただく必要があります。

表. インストールするルート証明書

	名称	有効期間	取得先 URL
1	ルート証明書 (SHA-1)	2011/6/6 ~ 2036/1/1	https://pki-platform.softbanktelecom.co.jp/PKI/pages/NewJTPKI_RootCA.crt
2	ルート証明書 (SHA-256)	2015/3/9 ~ 2036/6/15	https://pki-platform.softbanktelecom.co.jp/PKI/pages/doc/PKIPlatformCAG2_Root.crt

証明書をご利用いただく機器には、発行元となるルート証明書を必ずインストールして下さい。また、本サービスのサーバ証明書とクライアント証明書をご利用のお客様で SHA-1 証明書と SHA-256 証明書が混在する場合は、お互いを信頼し合えるようにサーバ機器およびクライアント機器に 2 種類のルート証明書をインストールする必要があります。

2. 利用端末環境

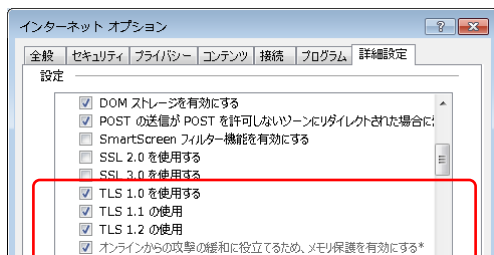
ルート証明書をインストールするクライアント端末は下記の条件を満たす必要があります。

表. クライアント端末の要件

項目	対応
対応機種	PC SoftBank iPhone 端末 4/4S/5/5S/5C/6/6Plus/6s/6s Plus,iPad シリーズ SoftBank Android 端末 104SH,107SH,302SH,303SH,305SH,Nexus5,XPERIA Z3,403HW,404KC
OS	Windows Vista Ultimate/Business/Enterprise SP2 以上 " 7 Ultimate/Professional/Enterprise SP1 以上 " 8.1/Pro/Enterprise " 10 /Pro/Enterprise iOS(最新バージョン、一世代前のメジャーバージョン) Android 4～(対応機種のみ) MAC OS X 10.9.2(ファイルダウンロード型のみ) ※OS メーカーのサポート終了後は、当社でもサポートできません ※動作確認は初期販売時の OS バージョンで実施しています ※USB トークンは非対応となります
ブラウザ	Internet Explorer 9.0 (Windows Vista) Internet Explorer 11(Windows 7/8.1/10) Android や iPhone・iPad OS に初期バンドルされているブラウザ Safari 7.0.2(MAC OS のみ) ※OS メーカーのサポート終了後は、当社でもサポートできません ※InternetExplorer は Microsoft 社でのサポート対象ブラウザの利用を前提としますが、記載されていないバージョンのブラウザについては弊社ナレッジベースとなりますので対応できない場合もあります。

以下の手順にて InternetExplorer の設定確認をお願い致します。

- (1) InternetExplorer のメニューの[ツール]より[インターネットオプション]を開きます。
- (2) [詳細設定]タブを選択し、[設定]の中の[セキュリティ]の項目にて、[TLS1.0を使用する]、[TLS1.1を使用する]、[TLS1.2を使用する]の何れかのチェックボックスがオンになっていることを確認します。
※全てオフになっていたら、いずれかのチェックボックスをオンにします。
- (3) [適用 (A)] [OK] (A)の順にてインターネットオプションを閉じます。
- (4) 設定を反映させるために、InternetExplorer を終了させ、ブラウザの再起動をしてください。



3. ルート証明書のインストール手順

3-1. インストール手順 【Windows Vista & Windows 7】

ルート証明書を PC にダウンロードし、以下の作業を実施してください。

(SHA-256)

https://pki-platform.softbanktelecom.co.jp/PKI/pages/doc/PKIPlatformCAG2_Root.crt

(SHA-1)

https://pki-platform.softbanktelecom.co.jp/PKI/pages/NewJTPKI_RootCA.crt

※管理者より特に指示がない場合は上記 2 種類ともにインポートしてください。

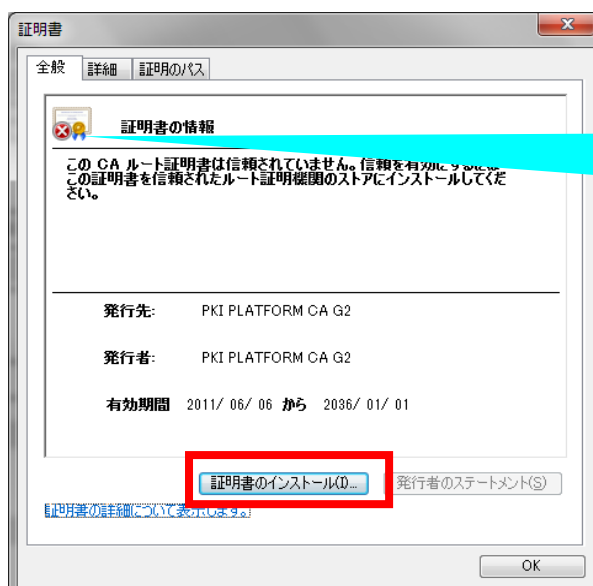
(1) ルート証明書のファイルをダブルクリックしてください。

下記画面が表示される場合は「開く」をクリックしてください。

※Windows Vista の画面にて説明します。Windows 7 も同様となります。



(2) 下記画面が表示されたら「証明書のインストール」をクリックしてください。

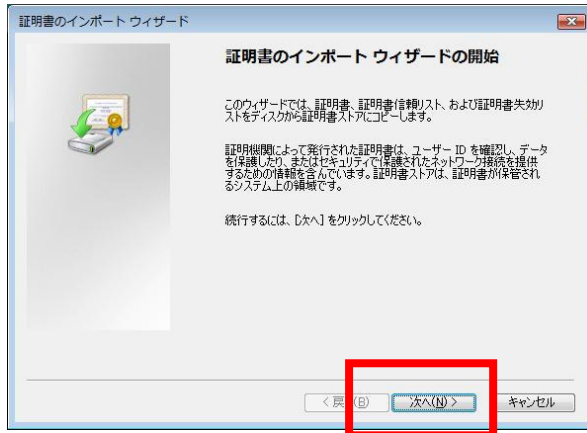


すでにインストールされていると

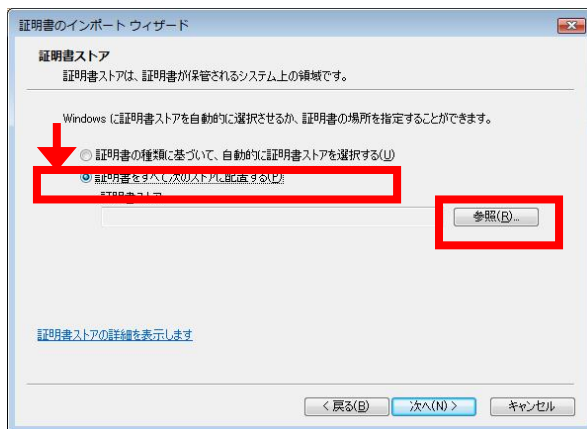
✖ マークが表示されません。

その場合、「OK」ボタンにて終了ください。

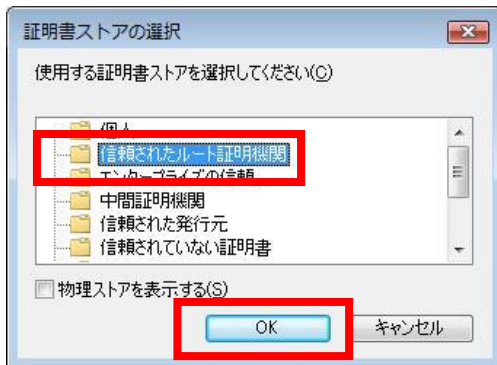
(3) 下記画面が表示されます。「次へ」をクリックしてください。



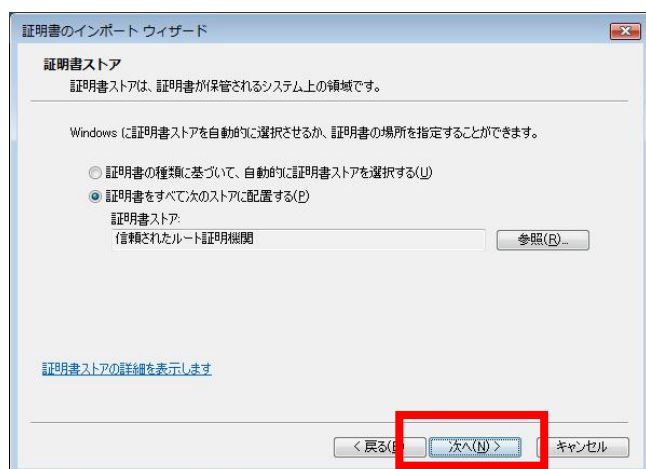
(4) 下記画面が表示されます。下記画面のように、下のラジオボタンを選択し、「参照」ボタンをクリックしてください。



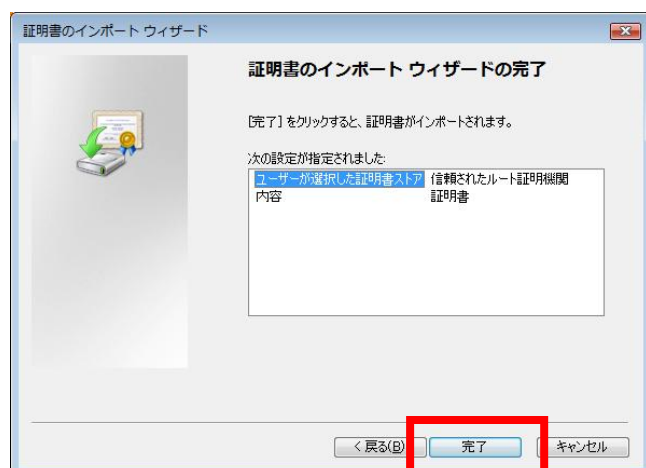
(5) 下記画面のように、「信頼されたルート認証機関」を選択し、「OK」をクリックしてください。



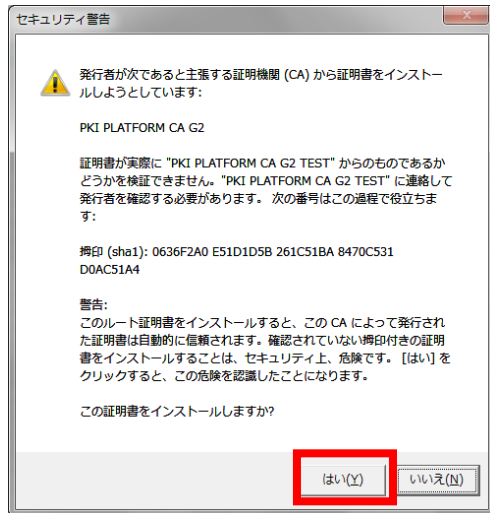
(6) 下記画面に戻ります。「次へ」をクリックしてください。



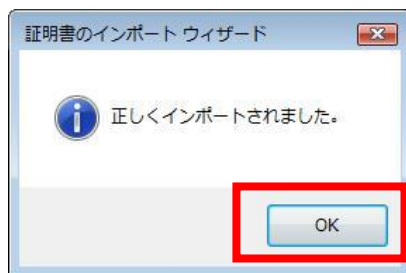
(7) 下記画面が表示されます。「完了」をクリックしてください。



※下記画面が表示される場合は、「はい」をクリックしてください。表示されない場合は特に問題ありません。



(8) 下記画面が表示されれば終了です。OK をクリックしてください。



※注意: 電子証明書は PC アカウントに紐づきます。つまりインストールを実行した PC アカウント以外では電子証明書利用不可となります。

3-2. インストール手順 【Windows 8.1】

ルート証明書を PC にダウンロードし、以下の作業を実施してください。

(SHA-256)

https://pki-platform.softbanktelecom.co.jp/PKI/pages/doc/PKIPlatformCAG2_Root.crt

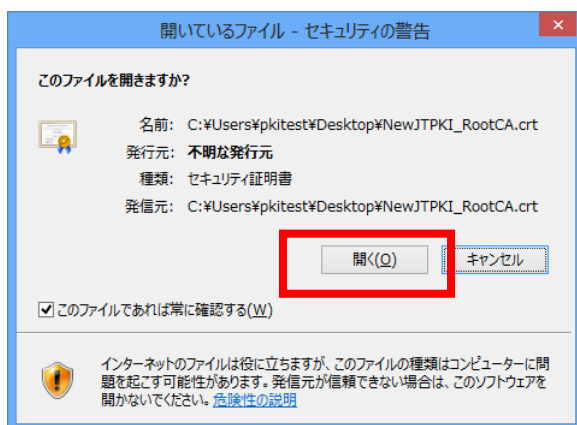
(SHA-1)

https://pki-platform.softbanktelecom.co.jp/PKI/pages/NewJTPKI_RootCA.crt

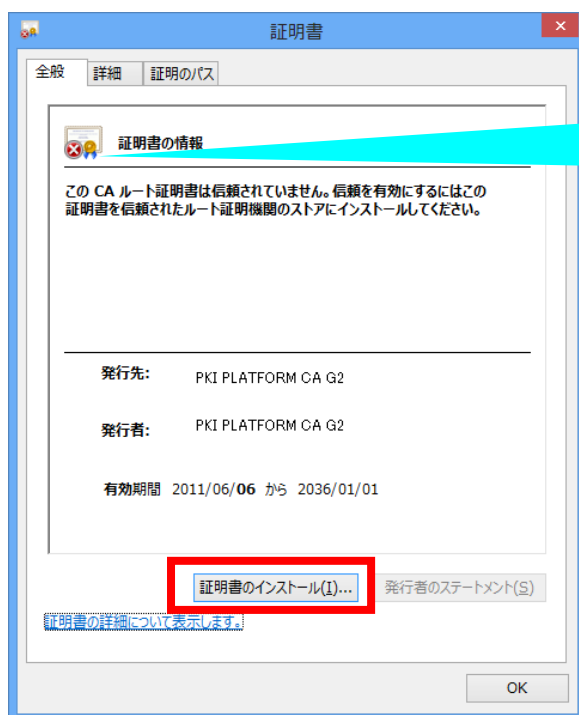
※管理者より特に指示がない場合は上記 2 種類ともにインポートしてください。

(1) ルート証明書のファイルをダブルクリックしてください。

下記画面が表示される場合は「開く」をクリックしてください。



(2) 下記画面が表示されたら「証明書のインストール」をクリックしてください。

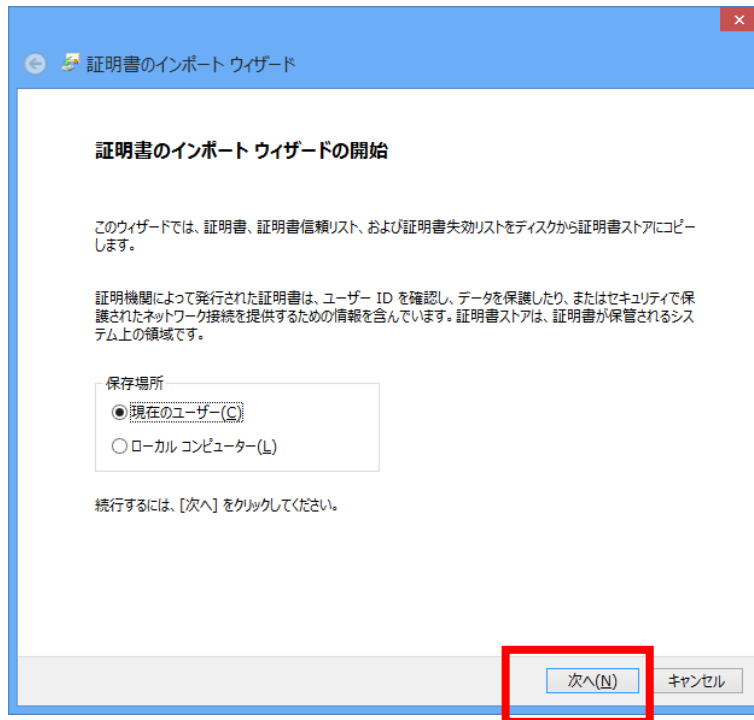


すでにインストールされていると

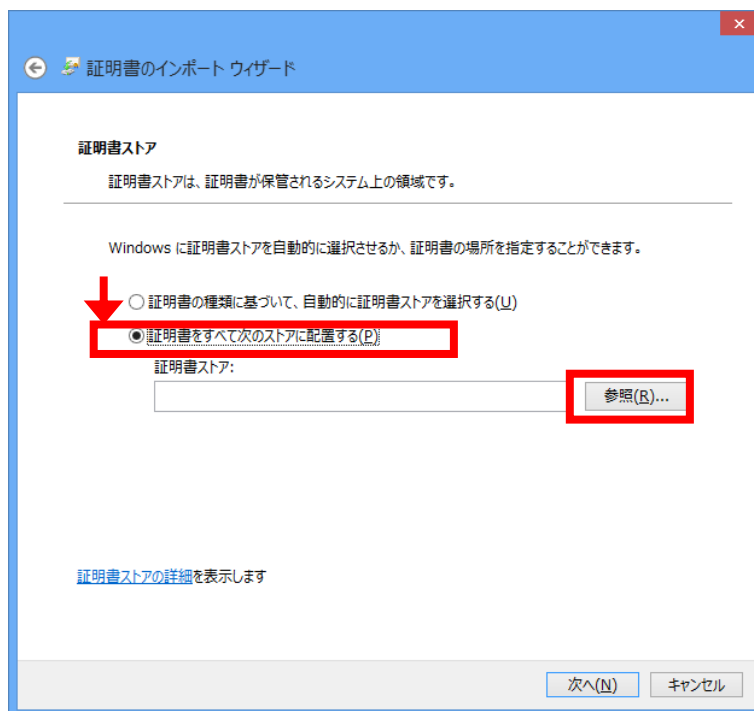
✗ マークが表示されません。

その場合、「OK」ボタンにて終了ください。

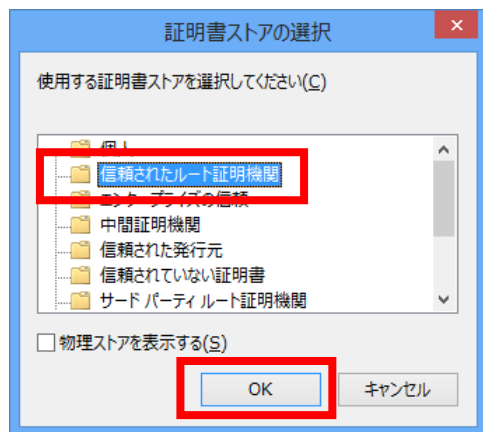
(3) 下記画面が表示されます。「次へ」をクリックしてください。



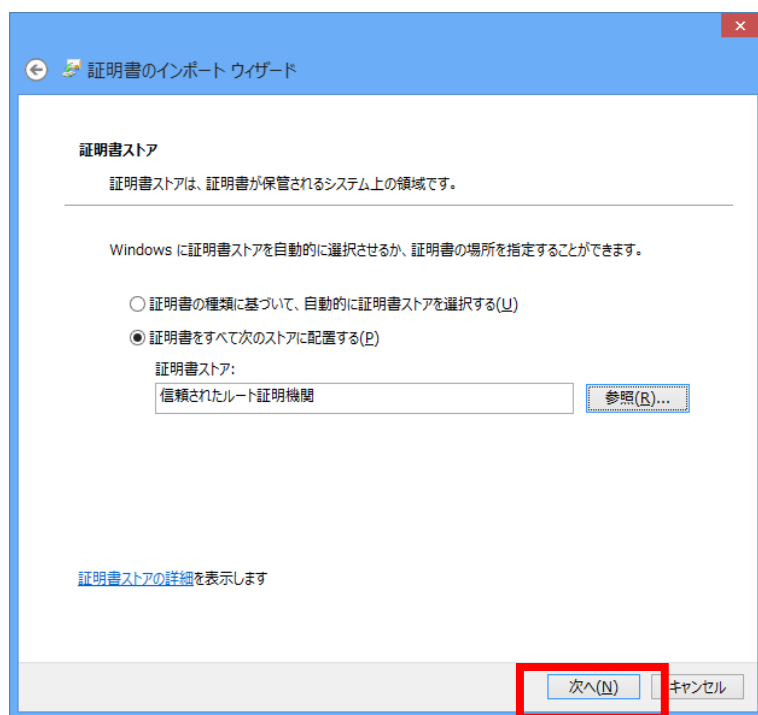
(4) 下記画面が表示されます。下記画面のように、下のラジオボタンを選択し、「参照」ボタンをクリックしてください。



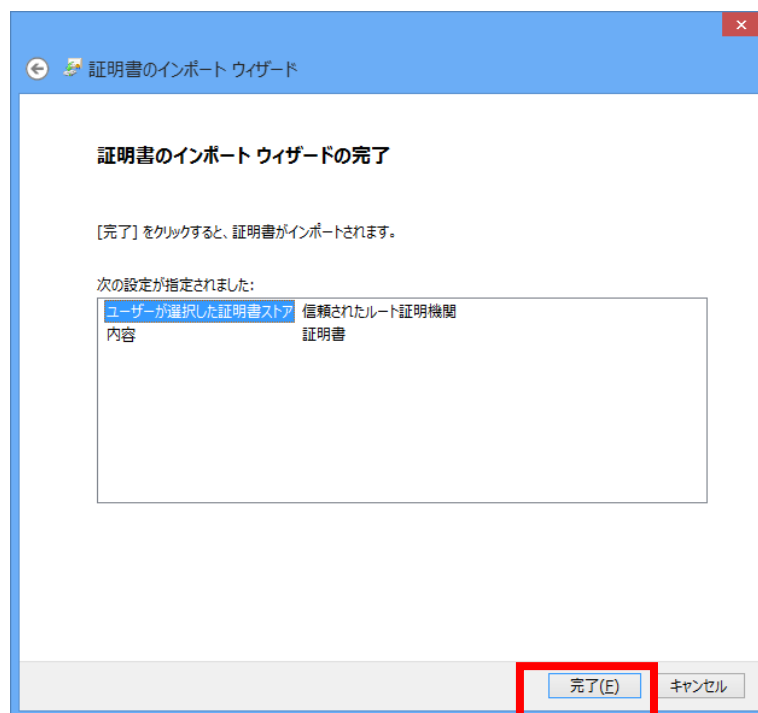
(5) 下記画面のように、「信頼されたルート認証機関」を選択し、「OK」をクリックしてください。



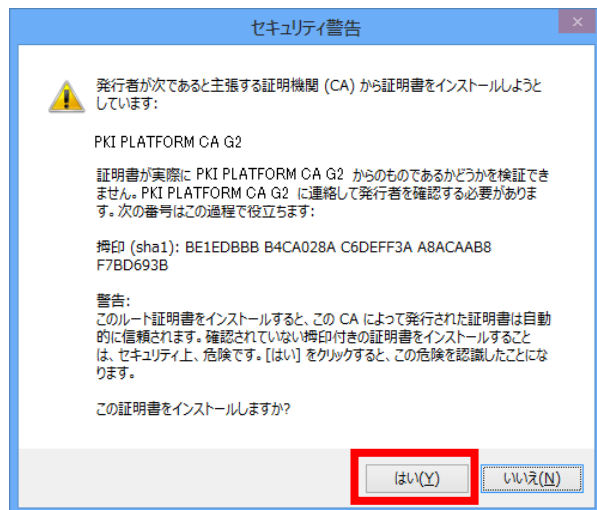
(6) 下記画面に戻ります。「次へ」をクリックしてください。



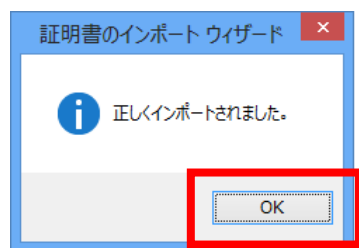
(7) 下記画面が表示されます。「完了」をクリックしてください。



※下記画面が表示される場合は、「はい」をクリックしてください。表示されない場合は特に問題ありません。



(8) 下記画面が表示されれば終了です。OK をクリックしてください。



※注意: 電子証明書は PC アカウントに紐づきます。つまりインストールを実行した PC アカウント以外では電子証明書利用不可となります。

3-3. インストール手順 【iPhone & iPad】

(1) Safari より以下 URL にアクセスしてください。

(SHA-256)

https://pki-platform.softbanktelecom.co.jp/PKI/pages/doc/PKIPlatformCAG2_Root.crt

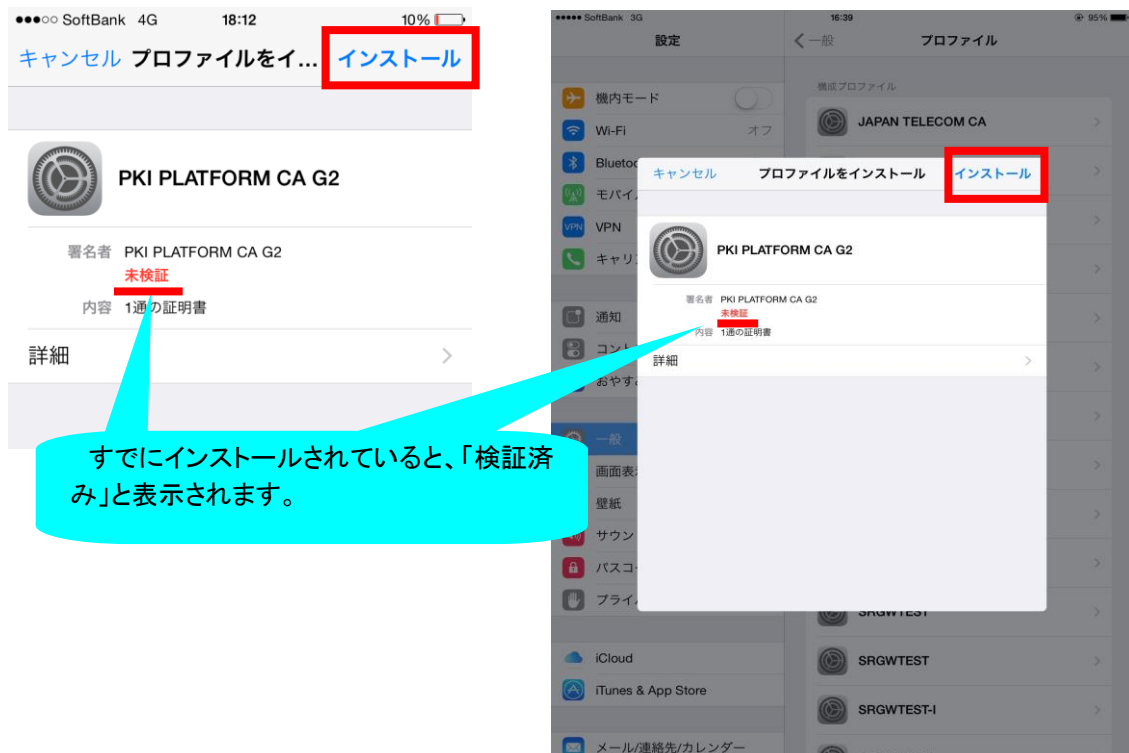
(SHA-1)

https://pki-platform.softbanktelecom.co.jp/PKI/pages/NewJTPKI_RootCA.crt

※管理者より特に指示がない場合は上記 2 種類ともにインポートしてください。

(2) 下記画面が表示されます。「インストール」をタップしてください。

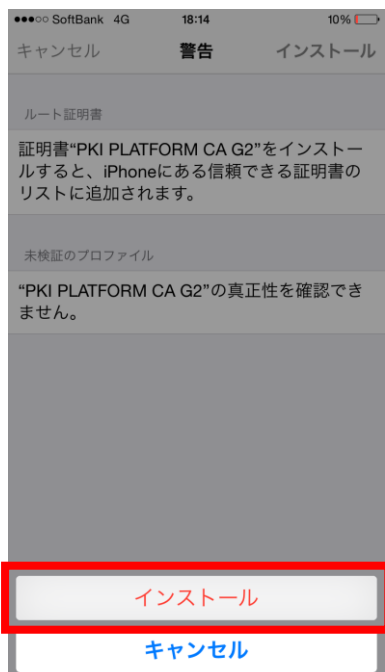
※左画面は iPhone 8.3、右画面 iPad 8.3 となります



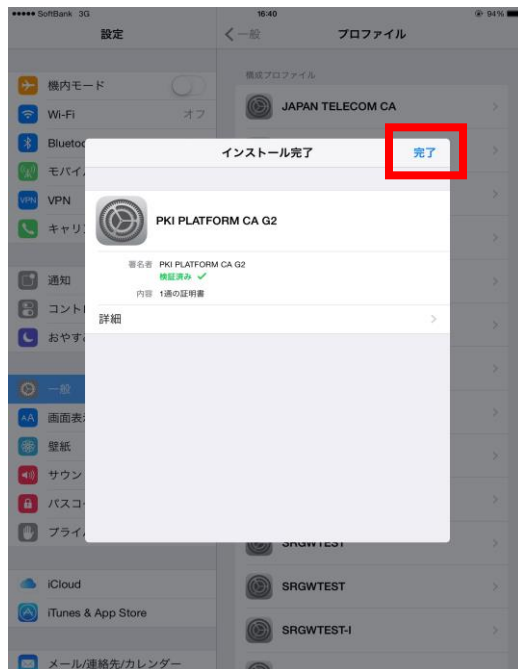
(3) パスコード入力の設定を行っている場合は、下記画面が表示されます。パスコードを入力後、「完了」をタップしてください。表示されなかった場合は(4)を確認ください。



(4) 下記画面が表示されます。「インストール」をタップしてください。



(5) 下記画面が表示されれば終了です。右上の「完了」をタップしてください。



3-4. インストール手順 【Android Ver.4.0】

ルート証明書のインポートは事前に実施するか証明書の取得時に実施するかのいずれかのタイミングで行ってください。

3.4.1 事前にルート証明書をインポートする場合

- (1) 標準ブラウザよりルート証明書が公開されている以下の URL にアクセスしてください。

(SHA-256)

https://pki-platform.softbanktelecom.co.jp/PKI/pages/doc/PKIPlatformCAG2_Root.crt

(SHA-1)

https://pki-platform.softbanktelecom.co.jp/PKI/pages/NewJTPKI_RootCA.crt

※管理者より特に指示がない場合は上記 2 種類ともにインポートしてください。

- (2) 下記画面が表示されますので、「パッケージの内容」欄が「CA 証明書 1 件」であることを確認し、証明書名には任意の文字列(インポート時にのみ利用)を入力して[OK]をタップしてください。



(図中の証明書名は例です)

- (3) ルート証明書のインストールに関するメッセージが画面下側に一時的に表示され、証明書のインポートが行われます。このメッセージが消えてからホームアイコンをタップしてメイン画面に戻ってください。

SBTMrootcert1がインストールされています。

- (4) インポートしたルート証明書はホーム画面から以下の手順で確認できます。

[設定] ⇒ [その他の設定] ⇒ [ロックとセキュリティ] ⇒ [安全な認証情報の使用]

“PKI PLATFORM CA G2”と記載された証明書情報のタイトルが表示され、詳細表示において有効期限が 2036 年 1 月 1 日と表示されれば、ルート証明書の取得は完了しています。

インポートしたルート証明書の情報は「3.5.3 インポートしたルート証明書の内容」をご覧ください。

3.4.2 証明書取得時にルート証明書をインポートする場合

- (1) 企業管理者様にて申請が行われたメールアドレス宛に当サービスから電子メールを送付します。メール件名は“電子証明書ファイルダウンロード準備完了について”になります。
- (2) メール記載の URL にアクセスするとブラウザが起動し、ユーザ認証画面が表示されます。
 - (2-1) 「ステップ 1: ルート証明書インストール」にて各ルート証明書の「こちら」をタップしてください。
 - (2-2) 各ルート証明書のインストールにおいて証明書の名前を指定する画面が表示されますので任意の名前を入力してください(図中の証明書名は例です)
 - (2-3) 「注意」画面として、ロック解除 PIN またはパスワード設定が要求される画面が表示される場合があります。このときは機器のロック解除 PIN もしくはパスワードを入力してください。



- (3) 証明書名の入力(ロック解除設定)の後、ルート証明書のインストールに関するメッセージが一時的に表示されます。

SBTM PKI-PF cert2がインストールされています。

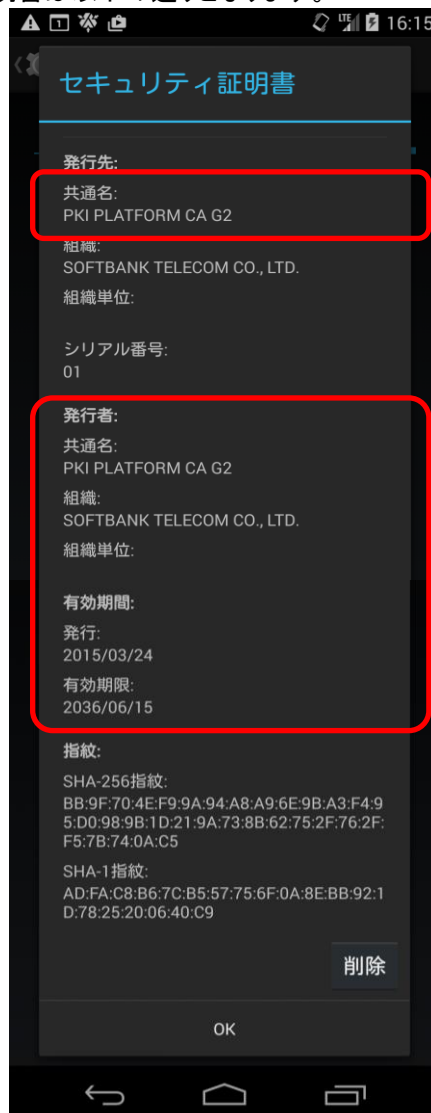
- (4) インポートしたルート証明書については以下の手順で確認できます。
[設定] ⇒ [その他の設定] ⇒ [ロックとセキュリティ] ⇒ [安全な認証情報の使用]
“PKI PLATFORM CA G2”と記載された証明書情報のタイトルが表示され、詳細表示において有効期限が 2036 年 1 月 1 日と表示されれば、ルート証明書の取得は完了しています。
インポートしたルート証明書の情報は「3.5.3 インポートしたルート証明書の内容」をご覧ください。

3.4.3 インポートしたルート証明書の内容

「安全な認証情報の使用」画面の「ユーザ」欄において[ユーザ]をタップしてください。



インポートしたルート証明書は以下の通りとなります。



3-5. インストール手順 【MAC OS】

(1) Safari より以下 URL にアクセスしてください。ルート証明書がダウンロードされます。

(管理者証明書の有効開始日が 2015/9/7 以降)

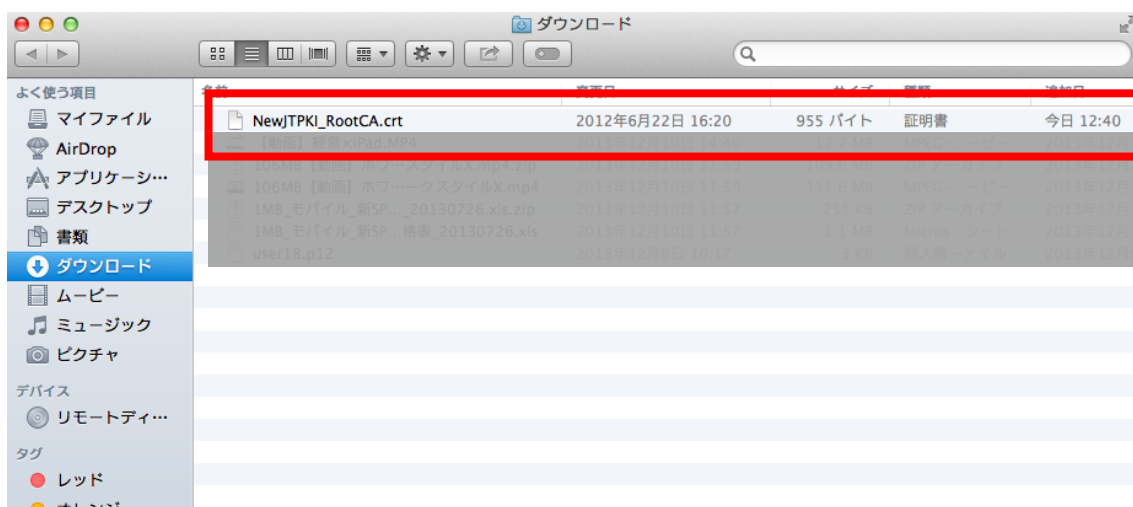
https://pki-platform.softbanktelecom.co.jp/PKI/pages/doc/PKIPlatformCAG2_Root.crt

(管理者証明書の有効開始日が 2015/9/6 以前)

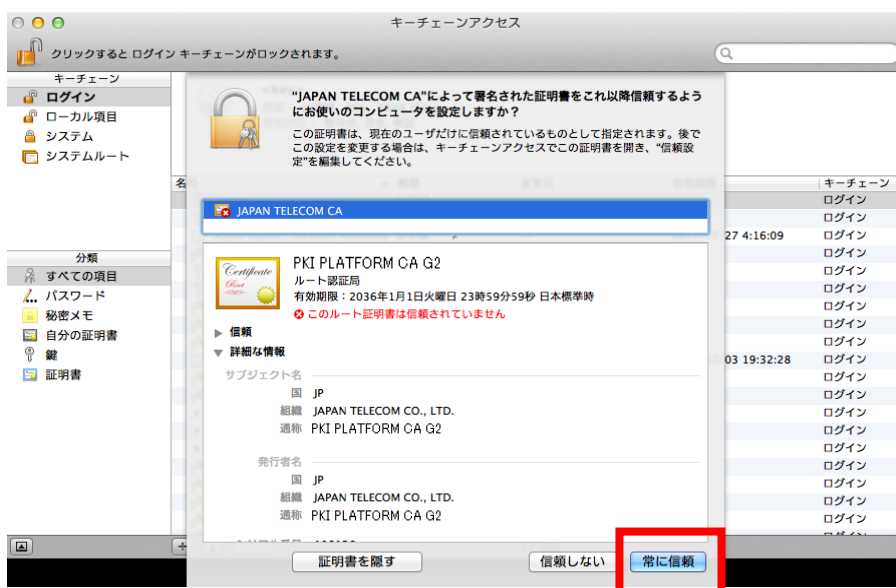
https://pki-platform.softbanktelecom.co.jp/PKI/pages/NewJTPKI_RootCA.crt

(2) ルート証明書のファイルをダブルクリックしてください。

※インストール手順で利用している画像は「MAC OS 10.9.2, Safari7.0.2」となります。



(3) 「キーチェーンアクセス」が表示されますので、「常に信頼」をクリックしてください。



(4) 下記ダイアログが表示されます。MAC OS の現在ログインしているユーザアカウント及びパスワードを入力し、「設定をアップデート」をクリックしてください。



※「設定をアップデート」をクリックすると証明書がインストールされます。

(5) インポートした証明書を確認します。

「Finder」 - 「アプリケーション」 - 「アプリケーション」 - 「ユーティリティ」 - 「キーチェーンアクセス」をクリックしてください。

「PKI PLATFORM CA G2」が表示されるので証明書をダブルクリックしてください。



※左フレームの「ログイン」、「証明書」が選択されていることを確認してください。

(6)「この証明書はこのアカウントにとって信頼されているものとして指定されています」と表示されていることを確認してください。また、ルート証明書の有効期限、詳細な情報は下記のとおりとなります。



PKI PLATFORM CA G2
ルート認証局
有効期限：2036年1月1日火曜日 23時59分59秒 日本標準時
この証明書はこのアカウントにとって信頼されているものとして指定されています

▶ 信頼
▼ 詳細な情報

サブジェクト名 _____
国 JP
組織 JAPAN TELECOM CO., LTD.
通称 PKI PLATFORM CA G2

発行者名 _____
国 JP
組織 JAPAN TELECOM CO., LTD.
通称 PKI PLATFORM CA G2

シリアル番号 108128
バージョン 3

署名アルゴリズム RSA 暗号化を使用する SHA-1 (1.2.840.113549.1.1.5)
パラメータ なし

以上