

**公的個人認証サービス**

**利用者クライアントソフト  
機能概要説明書  
(Android 版)**

**第 1.7 版**

**地方公共団体情報システム機構**

## 変更履歴

版数	変更日付	変更内容
1.0 版	平成 28 年 8 月 31 日	新規作成
1.1 版	平成 29 年 7 月 31 日	Java9 対応に伴い、以下を修正。 <ul style="list-style-type: none"> <li>第 2 章 ドキュメント体系図を改訂。</li> <li>第 3 章 第 1 節 表 3 - 1 の【PC 接続の場合】に Android 6.0.1、7.0 を追加。</li> <li>第 3 章 第 1 節 表 3 - 1 の【Android 単体で利用する場合】に Android 6.0.1、7.0 を追加。</li> </ul>
1.2 版	平成 30 年 8 月 31 日	Android SDK(26)対応に伴い、以下を修正。 <ul style="list-style-type: none"> <li>第 3 章 第 1 節 表 3 - 1 の【PC 接続の場合】に Android 8.0 を追加。</li> <li>第 3 章 第 1 節 表 3 - 1 の【Android 単体で利用する場合】に Android 8.0 を追加。</li> </ul>
1.3 版	令和元年 5 月 1 日	新元号対応に伴い、以下を修正。 <ul style="list-style-type: none"> <li>第 3 章 第 1 節 動作環境の Android 版利用者ソフトウェアバージョンを 1.1 に変更。</li> <li>第 3 章 第 2 節 前提条件の Android 版利用者ソフトウェアバージョンを 1.1 に変更。</li> <li>第 4 章 第 3 節 の表 4-2 における 2 生年月日の設定ルールに新元号を追加。</li> <li>第 4 章 第 5 節 の機能仕様における 生年月日の設定ルールに新元号を追加。</li> </ul> 旧氏対応に伴い、以下を修正。 <ul style="list-style-type: none"> <li>第 4 章 第 3 節 図 4 - 9 および表 4 - 2 に旧氏に関する記述を追加。</li> <li>第 4 章 第 5 節 2 機能仕様に旧氏に関する記述を追加。</li> </ul>

版数	変更日付	変更内容
1.4 版	令和 2 年 3 月 31 日	<p>MacOS 版における住基カードサポート廃止に伴い、以下を修正。</p> <ul style="list-style-type: none"> <li>・第 2 章 ドキュメント体系図から「API 仕様書 Mac OS X C 言語インターフェース編」を削除。</li> </ul> <p>ブラウザ対応版、iOS 版のリリースに伴い、以下を修正。</p> <ul style="list-style-type: none"> <li>・第 2 章 ドキュメント体系 「利用者クライアントソフト機能概要説明書 ブラウザ対応編」を追加。</li> <li>・第 2 章 ドキュメント体系 「API 仕様書 カード AP ライブラリ ブラウザインターフェース編」を追加。</li> <li>・第 2 章 ドキュメント体系 「利用者クライアントソフト機能概要説明書(iOS 版)」を追加。</li> <li>・第 2 章 ドキュメント体系 「API 仕様書 iOS Framework 編」を追加。</li> <li>・第 3 章 第 1 節 動作環境に Android9.0、10.0 を追加。</li> </ul>
1.5 版	令和 3 年 3 月 31 日	<p>ブラウザ対応 Android 版のリリースに伴い、以下を修正</p> <ul style="list-style-type: none"> <li>・第 2 章 ドキュメント体系 「利用者クライアントソフト機能概要説明書(Android 版) ブラウザ対応編」を追加。</li> <li>・第 2 章 ドキュメント体系 「API 仕様書 Android インテント ブラウザインターフェース編」を追加。</li> </ul> <p>Android のバージョンの更新に伴い、以下を修正</p> <ul style="list-style-type: none"> <li>・第 3 章 システム概要 第 1 節 動作環境の Android バージョンを修正、ブラウザ項目の追加</li> </ul> <p>OSS ライセンス情報表示画面追加に伴い、以下を修正</p> <ul style="list-style-type: none"> <li>・第 4 章 機能概要(Android 編) 第 1 節 メニュー画面表示機能 3 画面仕様 図 4 - 1 を修正</li> </ul>
1.5.1 版	令和 5 年 1 月 31 日	<p>Android SDK31 対応に伴い、以下を修正</p> <ul style="list-style-type: none"> <li>・第 3 章 システム概要 第 1 節 動作環境の Android 版利用者ソフトバージョンを 2.0.2 に変更</li> <li>・第 3 章 システム概要 第 1 節 動作環境の OS に Android12.0 を追加</li> <li>・第 3 章 システム概要 第 2 節 前提条件の Android 版利用者ソフトバージョンを 2.0.2 に変更</li> <li>・第 5 章 機能概要(PC 接続編)第 3 節 PC 接続機能の画面仕様を Android11 以前と Android12 以降に分け、Android12 以降の場合は Bluetooth 利用許可に関する画面が表示されることを追加</li> </ul>

版数	変更日付	変更内容
1.6 版	令和 5 年 3 月 31 日	利用者同意状況確認機能の追加に伴い、以下を修正 <ul style="list-style-type: none"> <li>・ 第 1 章 利用者同意状況確認機能を追加</li> <li>・ 第 1 章 表 1 - 1 用語の定義 利用者証明書、認証局の自己署名証明書の説明を変更</li> <li>・ 第 3 章 第 1 節 動作環境の Android 版利用者ソフトウェアバージョンを 2.1 に変更</li> <li>・ 第 3 章 第 1 節 表 3 - 1 動作環境の OS から Android7.0 を削除</li> <li>・ 第 3 章 第 2 節 動作環境の Android 版利用者ソフトウェアバージョンを 2.1 に変更</li> <li>・ 第 4 章 第 1 節 利用者同意状況確認機能を追加</li> <li>・ 第 4 章 第 1 6 節 利用者同意状況確認機能を追加</li> </ul>
1.6.1 版	令和 5 年 3 月 31 日	以下を修正 <ul style="list-style-type: none"> <li>・ 第 3 章 第 1 節 動作環境の記載を修正</li> </ul>
1.7 版	令和 6 年 7 月 31 日	Android SDK34 対応に伴い、以下を修正 <ul style="list-style-type: none"> <li>・ 第 2 章 ドキュメント体系 図 2 - 3 ドキュメント体系図(iOS 版)に API 仕様書 iOS XCFramework 編を追加</li> <li>・ 第 3 章 システム概要 第 1 節 動作環境の Android 版利用者ソフトウェアバージョンを 2.2 に変更</li> <li>・ 第 3 章 システム概要 第 1 節 動作環境の OS に Android13.0、14.0 を追加</li> <li>・ 第 3 章 システム概要 第 2 節 前提条件の Android 版利用者ソフトウェアバージョンを 2.2 に変更</li> <li>・ 巻末 注意事項欄の商標表記を Google LLC に変更</li> </ul>

## - 目次 -

<b>第 1 章 はじめに</b> .....	<b><u>1-1</u></b>
第 1 節 用語の定義.....	2
<b>第 2 章 ドキュメント体系</b> .....	<b><u>3-3</u></b>
<b>第 3 章 システム概要</b> .....	<b><u>5-5</u></b>
第 1 節 動作環境 .....	<u>6-6</u>
第 2 節 前提条件 .....	<u>8-7</u>
<b>第 4 章 機能概要 (Android 編)</b> .....	<b><u>9-8</u></b>
第 1 節 メニュー画面表示機能 .....	<u>9-8</u>
第 2 節 ポータルサイト閲覧機能.....	<u>11-10</u>
第 3 節 電子証明書表示機能 .....	<u>12-11</u>
第 4 節 電子証明書出力機能 .....	<u>29-28</u>
第 5 節 基本 4 情報取得機能 .....	<u>32-31</u>
第 6 節 電子署名作成機能 .....	<u>33-32</u>
第 7 節 電子証明書取得機能 .....	<u>34-33</u>
第 8 節 電子署名検証機能 .....	<u>35-34</u>
第 9 節 官職証明書検証機能 .....	<u>36-35</u>
第 10 節 自分の電子証明書の有効性確認機能 .....	<u>38-37</u>
第 11 節 自分の電子証明書のオンライン失効申請機能 .....	<u>40-39</u>
第 12 節 ソフトウェア動作確認機能 .....	<u>47-46</u>
第 13 節 パスワード変更機能 .....	<u>49-48</u>
第 14 節 プロキシ設定機能 .....	<u>57-56</u>
第 15 節 電子証明書の更新通知機能 .....	<u>59-58</u>
第 16 節 利用者同意状況確認機能 .....	<u>63-62</u>
<b>第 5 章 機能概要 (PC 接続編)</b> .....	<b><u>69-68</u></b>
第 1 節 メニュー画面表示機能 .....	<u>69-68</u>
第 2 節 PC 接続動作確認機能.....	<u>71-70</u>
第 3 節 PC 接続機能 .....	<u>74-73</u>

## 第1章 はじめに

公的個人認証サービス利用者クライアントソフト(以下、JPKI 利用者ソフト)は、利用者が Android 端末や、自宅のパソコンでオンライン申請などを利用する際に必要となる以下の機能を提供する。

- メニュー画面表示機能
- ポータルサイト閲覧機能
- 電子証明書表示機能
- 電子証明書出力機能
- 基本4情報取得機能
- 電子署名作成機能
- 電子証明書取得機能
- 電子署名検証機能
- 官職証明書検証機能
- 自分の電子証明書の有効性確認機能
- 自分の電子証明書のオンライン失効申請機能
- ソフトウェア動作確認機能
- パスワード変更機能
- プロキシ設定機能
- 電子証明書の更新通知機能
- 利用者同意状況確認機能
- PC 接続機能

以降、本書では Android 版 JPKI 利用者ソフトの機能概要について説明する。

## 第1節 用語の定義

表 1-1 用語の定義

項番	用語・略号	説明
1	ICカード	以下のカードを指す総称 ・個人番号カード
2	電子証明書	公開鍵及び発行対象を識別する情報を含むデータに、認証局が発行対象の正当性を保証する電子署名を付与し、発行されるデータを示す。データは、ISO/IEC 8825-1の識別符号化規則により符号化された形式で利用される。
3	証明書	電子証明書と同義
4	利用者証明書	公的個人認証サービスで発行した利用者の証明書 本書では以下の電子証明書を示す。 ・個人番号カードに格納された署名用電子証明書 ・個人番号カードに格納された利用者証明用電子証明書 ・移動端末設備に格納された署名用電子証明書 ・移動端末設備に格納された利用者証明用電子証明書
5	認証局の自己署名証明書	自認証局の公開鍵に対して、自認証局の秘密鍵で署名した証明書。 本書では以下の電子証明書を示す。 ・個人番号カードに格納された署名用認証局の自己署名証明書 ・個人番号カードに格納された利用者証明用認証局の自己署名証明書 ・移動端末設備に格納された署名用認証局の自己署名証明書 ・移動端末設備に格納された利用者証明用認証局の自己署名証明書
6	NFC	Near Field Communication (近距離無線通信)の略。
7	Bluetooth	機器間の近距離無線通信 IEEE 802.15.1の規格名称。
8	インテント	Androidの機能の一つ。アプリケーション間やアプリケーション内の機能間において、情報を連携するための機能。

## 第2章 ドキュメント体系

JPKI 利用者ソフトのドキュメント体系図を以下に示す。本書は以下の体系図の網掛け部分に該当する。

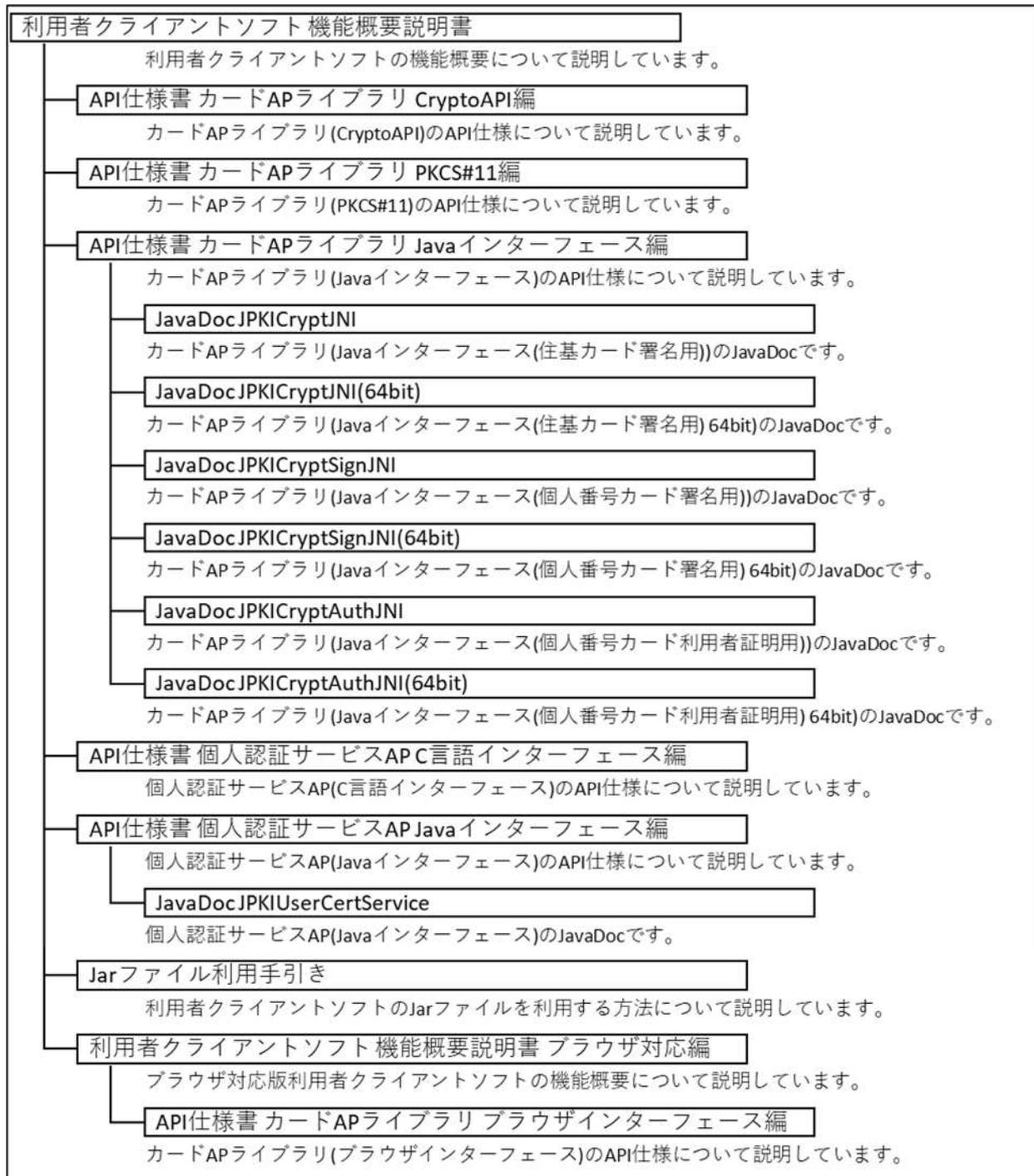


図 2-1 ドキュメント体系図(PC版)

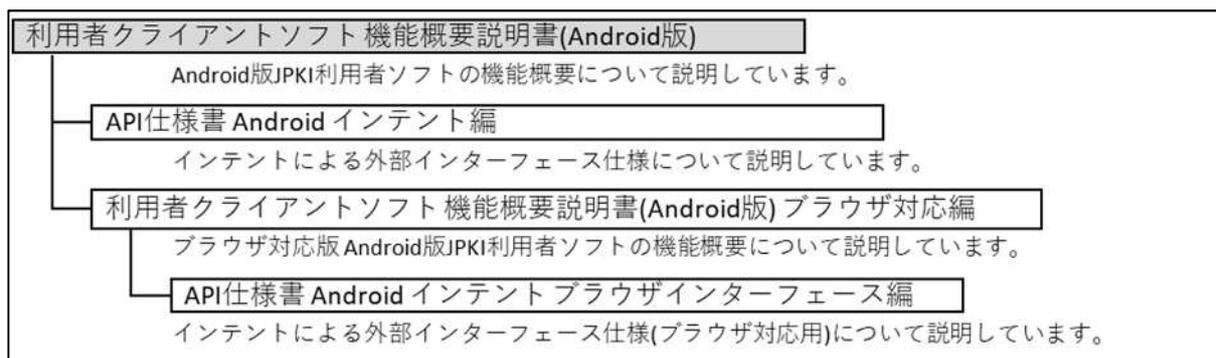


図 2-2 ドキュメント体系図(Android版)

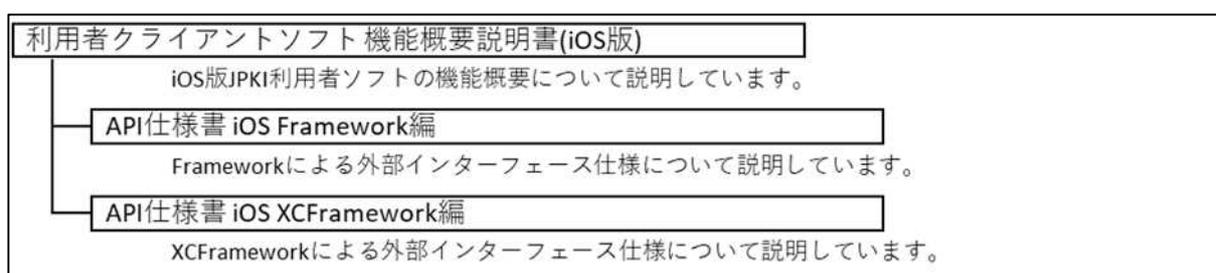


図 2-3 ドキュメント体系図(iOS版)

### 第3章 システム概要

以下の2方式を対象とする。

#### 【方式1】

Android 端末を IC カードリーダーとして使用し、Android 端末と PC を接続し活用する。



図 3-1 方式1イメージ

「第5章 [機能概要 \(PC 接続編\)](#) [機能概要 \(PC 接続編\)](#)」を参照。

#### 【方式2】

Android 端末の NFC 機能を使用し、Android 端末にて IC カードの電子証明書等の情報を読み込み、Android 端末で読み込んだ情報を使用する。



図 3-2 方式2イメージ

「第4章 [機能概要 \(Android 編\)](#) [機能概要 \(Android 編\)](#)」を参照。

## 第1節 動作環境

Android版 JPKI 利用者ソフト Ver2.2 の動作環境は以下の通りとする。

表 3-1 動作環境

項目	条件
OS	下記の Android のいずれかを搭載していること。 ・ 8.0、9.0、10.0、11.0、12.0、13.0、14.0
Bluetooth	Bluetooth 4.2 を搭載していること。
NFC	以下の条件を満たす Android 端末とする。(「個人番号カード対応適合性検証済み Android 端末一覧」 1 を参照のこと。) ・ ISO/IEC 14443 Type B に対応している NFC を搭載していること。
IC カード	個人番号カードであること。(住基カードは対象外)

1 最新の「個人番号カード対応適合性検証済み Android 端末一覧」の情報は、JPKI ポータルサイトに掲載するものとする。

また、最新の「個人番号カード対応適合性検証済み Android 端末」以外を使用した場合の不具合等に関するお問い合わせは、サポート対象外とする。

表示画面については以下の通りとする。

表 3-2 表示画面

項目	仕様
解像度	フルHD または HD
画面比	16:9
画面の向き	縦画面固定とする。

Android版 JPKI 利用者ソフトにおける Android 端末のボタン操作について以下の通りとする。

表 3-3 ボタン操作

ボタン名	動作
ホームボタン	使用しない。
履歴ボタン	使用しない。
戻るボタン	1つ前の画面に戻る。

PC版 JPKI 利用者ソフトの動作環境

「利用者クライアントソフト機能概要説明書」を参照。

## 第2節 前提条件

Android版 JPKI 利用者ソフト Ver2.2 の前提条件は以下の通りとする。

表 3-4 前提条件

前提条件
Android版 JPKI 利用者ソフトで設定、登録した情報は機種変更等による Android 端末間の移行には対応しない。
Android のマルチユーザ機能には対応しない。

## 第4章 機能概要 (Android 編)

### 第1節 メニュー画面表示機能

#### 1 概要

Android版 JPKI 利用者ソフトのポータルサイト閲覧機能、電子証明書表示機能、動作確認機能、電子証明書失効申請機能、パスワード変更機能、プロキシ設定機能、更新通知機能、利用者同意状況確認機能、PC 接続機能の起動ボタンを表示する。

#### 2 機能仕様

Android版 JPKI 利用者ソフトを起動することで、以下のボタンを含むメニュー画面を表示する。

- JPKI ポータルサイト閲覧ボタン
- 自分の電子証明書表示ボタン
- 認証局の自己署名証明書表示ボタン
- その他の電子証明書表示ボタン
- 動作確認ボタン
- 電子証明書失効申請ボタン
- パスワード変更ボタン
- プロキシ設定ボタン
- 更新通知設定ボタン
- 住所等提供同意状況の照会・取消ボタン
- PC 接続ボタン
- ヘルプボタン

メニュー画面では、上記のボタンが画面上にすべて表示されないため、上下にスクロールすることで、ボタンを表示する。

### 3 画面仕様

メニュー画面の仕様は以下の通りである。

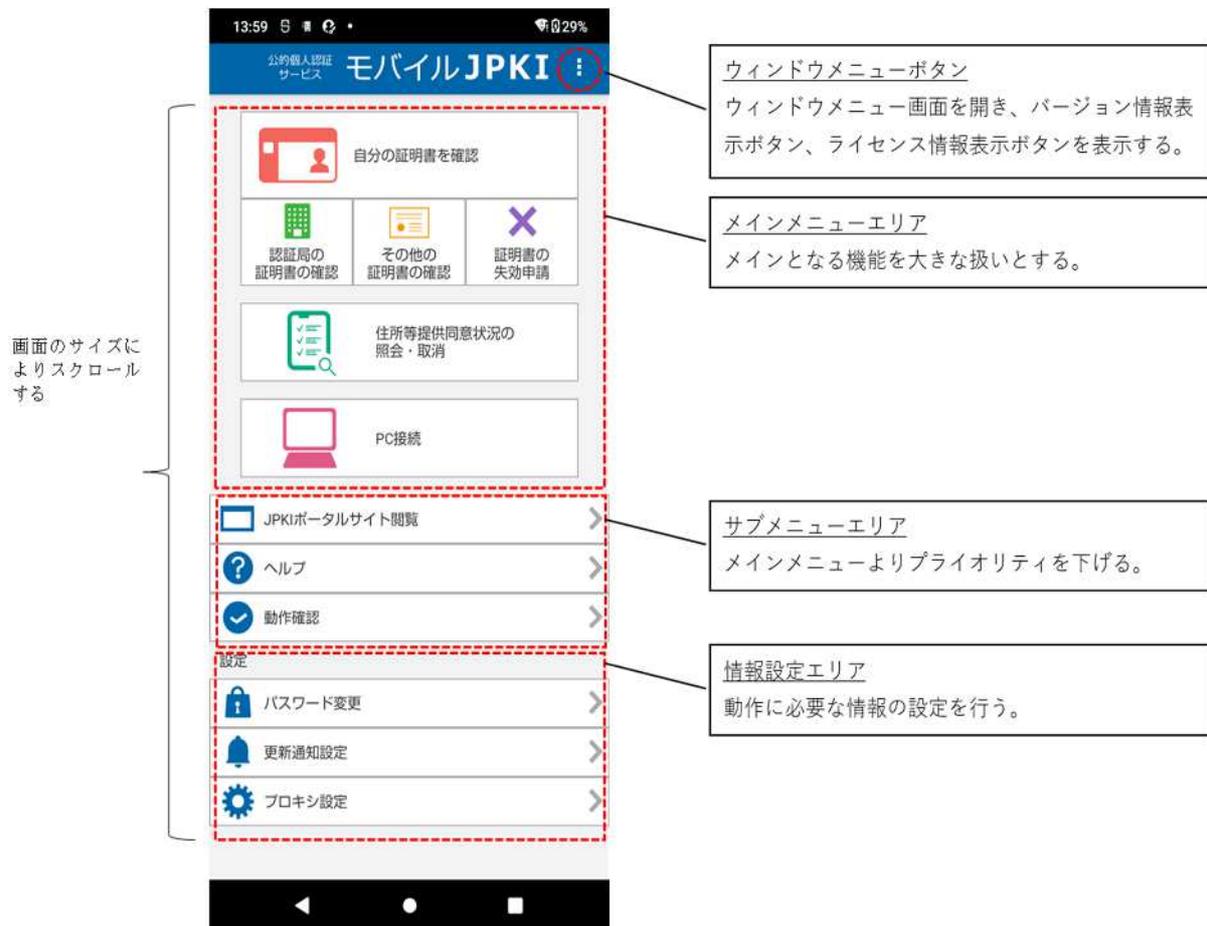


図 4-1 メニュー画面イメージ

## 第2節 ポータルサイト閲覧機能

### 1 概要

Android版 JPKI 利用者ソフトの最新情報や利用できる電子申請の情報等を閲覧するために、ウェブブラウザを起動し、公的個人認証サービスポータルサイトを表示する。

### 2 機能仕様

通常使用するウェブブラウザとして設定されているウェブブラウザを起動し、公的個人認証サービスポータルサイトを表示する。

### 3 画面仕様

メニュー画面の「JPKI ポータルサイト閲覧」ボタンを押下することで、通常使用するウェブブラウザとして設定されているウェブブラウザを起動し、公的個人認証サービスポータルサイトを表示する。



図 4-2 JPKI ポータルサイト閲覧ボタン

## 第3節 電子証明書表示機能

### 1 概要

- (1) ICカードに格納された利用者証明書および認証局の自己署名証明書の内容を表示する。
- (2) 電子公文書等に添付された官職証明書(GPKI)または職責証明書(LGPKI)、その他の電子証明書を表示する。

### 2 機能仕様

- (1) 上位アプリケーションからの外部インターフェースによる要求に基づいて、ICカード(個人認証カード AP)等から取得した電子証明書を受け取り、受け取った電子証明書を GUI(Graphical User Interface)画面に表示する。
- (2) 以下の電子証明書を表示対象とする。

#### 公的個人認証サービス(JPKI)

- ◇ ICカードに格納された署名用電子証明書
- ◇ ICカードに格納された署名用認証局の自己署名証明書
- ◇ ICカードに格納された利用者証明用電子証明書
- ◇ ICカードに格納された利用者証明用認証局の自己署名証明書

#### 政府認証基盤(GPKI)

- ◇ 電子公文書等に添付された官職証明書
- ◇ 電子公文書等に添付された CA の自己署名証明書

#### 地方公共団体における組織認証基盤(LGPKI)

- ◇ 電子公文書等に添付された職責証明書
- ◇ 電子公文書等に添付された CA の自己署名証明書

#### その他

- ◇ その他の認証基盤および CA で発行された電子証明書(日本工業規格 X560-1 の識別符号化規則により符号化された形式の電子証明書)

- (3) 上位アプリケーションから受け取る電子証明書のデータ形式は、日本工業規格 X560-1 の識別符号化規則により符号化された形式(以下、DER(Distinguished Encoding Rules)形式)とする。
- (4) 「自分の証明書を確認する」ボタンまたは「認証局の証明書の確認」ボタンを押下すると、署名用、利用者証明用を選択する画面を表示し、選択後、ICカードを Android 端末にかざした状態から、選択された電子証明書を GUI 画面に表示する。
- (5) GUI 画面に利用者証明書を表示する際は、次の2種類のボタンを配置する。
  - ◇ 自分の電子証明書の有効性確認機能により電子証明書の有効性を確認するための有効性確認ボタン
  - ◇ 電子証明書出力機能により DER 形式またはテキスト形式にファイル出力するためのファイル出力ボタン
- (6) GUI 画面に認証局の自己署名証明書を表示する際は、次のボタンを配置する。
  - ◇ 電子証明書出力機能により DER 形式またはテキスト形式にファイル出力するためのファイル出力ボタン

(7) GUI画面に官職証明書、職責証明書、その他の電子証明書を表示する際は、次の2種類のボタンを配置する。

- ◇ 官職証明書検証機能により電子証明書の有効性を確認するための証明書検証ボタン
- ◇ 電子証明書出力機能により DER形式またはテキスト形式にファイル出力するためのファイル出力ボタン

### 3 電子証明書表示手順

本機能を使用する場合、電子証明書の取得は上位アプリケーションで行う。電子証明書の取得方法としては以下の通りとなる。

- ◇ ICカードからの電子証明書の取得
- ◇ ファイルからの電子証明書の取得

### 4 画面仕様

電子証明書の記載事項の表示については、基本情報を表示する画面(以下、基本画面)と全ての記載事項を表示する画面(以下、詳細画面)を設ける。

以下に、電子証明書表示画面の画面仕様を記述する。

## 画面共通仕様

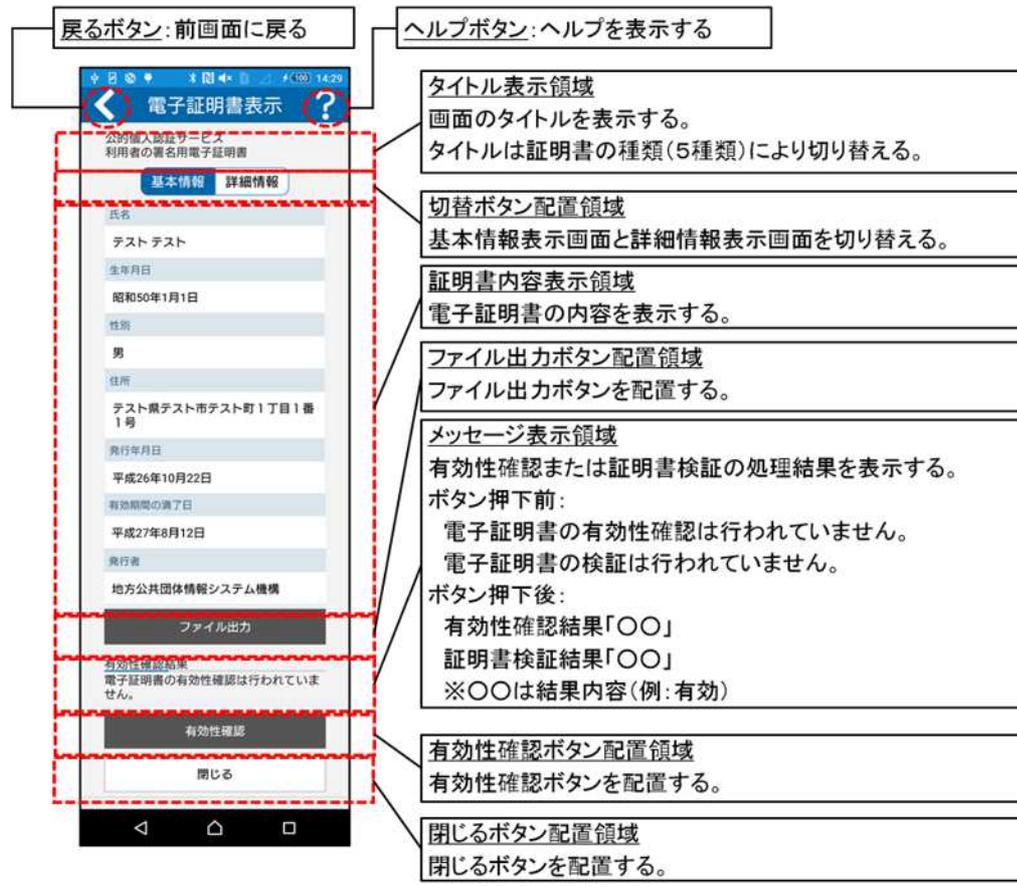


図 4-3 画面共通仕様イメージ

- フォントの種類およびサイズは視認性を考慮し、以下の通りとする。  
Android 端末に標準搭載されている「モトヤL マルベリ3」を使用する。フォントサイズは「14sp」とする。
- GUI 画面に文字を表示する際、以下の文字についても正しい表示を可能とする。
  - 「¥」(半角円サイン)
  - 「~」(半角チルド)
  - 「\」(全角バックスラッシュ)
  - 「~」(全角チルド)
  - 「」」(全角2重縦線)
  - 「-」(全角ハイフン)
  - 「」」(全角セントサイン)
  - 「」」(全角ポンドサイン)
  - 「」」(全角ノットサイン)

## 基本画面

基本画面は、電子証明書の種類に応じて、以下の3種類の表示方式に分類される。

認証局の自己署名証明書

自己署名証明書、ルート認証局の自己署名証明書、リンク証明書、下位認証局の自己署名証明書、相互認証証明書

利用者証明書

公的個人認証サービスで発行した利用者の証明書

官職証明書、職責証明書、その他の証明書

上記以外の電子証明書

電子証明書を分類するための処理フローは図 4-4 図 4-4 の通り。

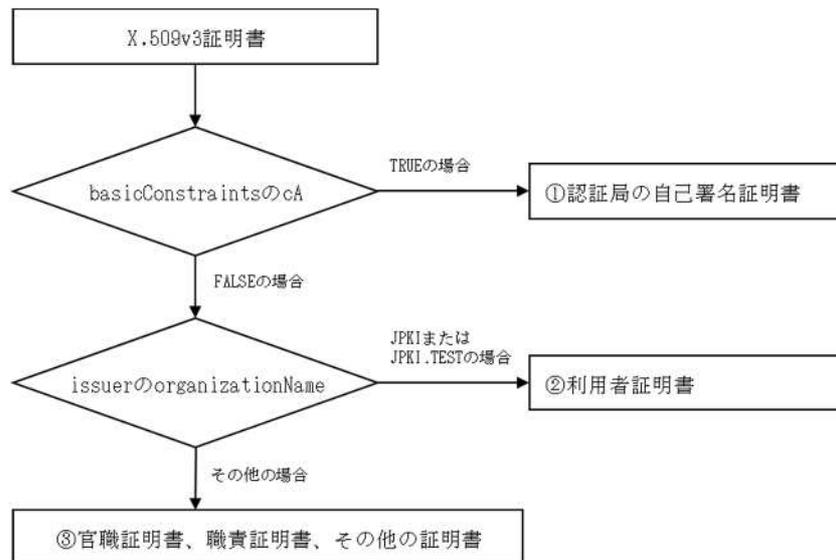


図 4-4 電子証明書分類処理フロー

次頁以降、各画面の画面仕様について記述する。

## 認証局の自己署名証明書

メニュー画面の「認証局の証明書の確認」ボタンを押下することで、ICカードに格納されている認証局の自己署名証明書を選択する画面を表示する。



図 4 - 5 電子証明書表示ボタン(認証局の自己署名証明書)

電子証明書選択画面で表示する認証局の自己署名証明書を選択し、「OK」ボタンを押下することで、選択された認証局の自己署名証明書を表示する。



図 4 - 6 電子証明書選択画面イメージ

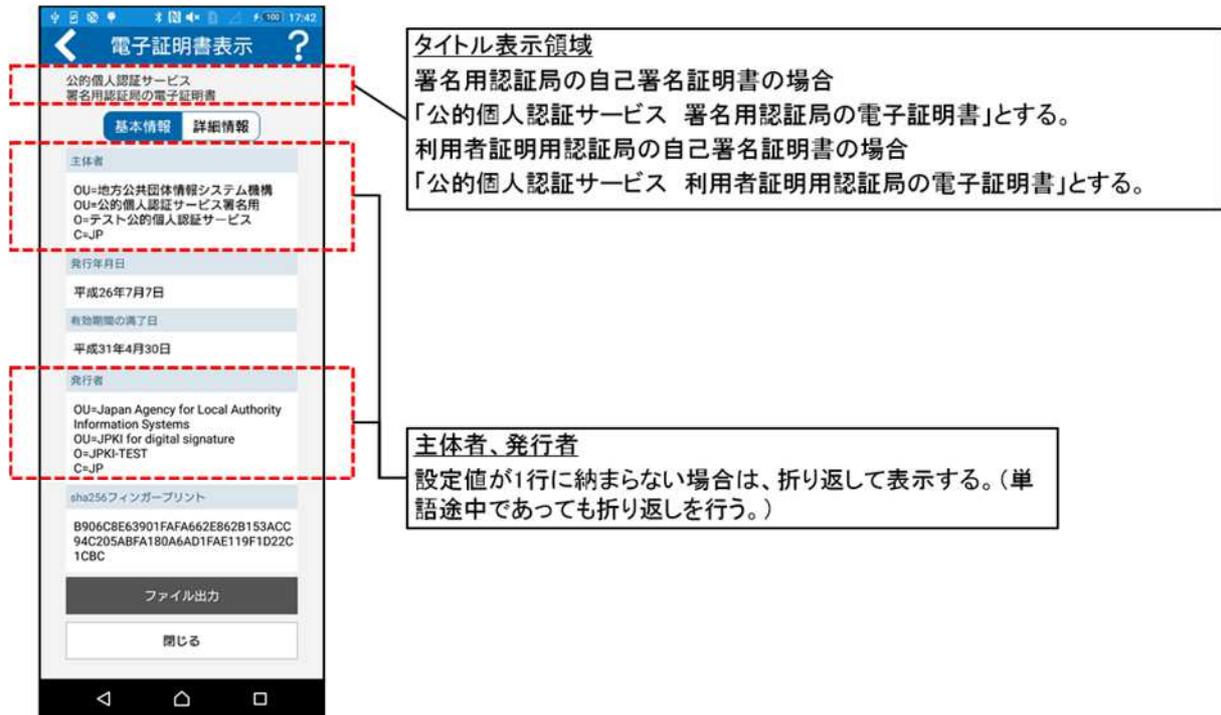


図 4-7 基本画面イメージ(認証局の自己署名証明書)

表 4-1 表示項目と証明書領域の対応(認証局の自己署名証明書)

項番	項目名	証明書の項目名		表示方法
		上位項目名	項目名	
1	主体者	SubjectAltName または Subject	CountryName OrganizationName OrganizationalUnitName OrganizationalUnitName	SubjectAltName の DN を全て表示。 DN は属性毎に改行して表示し、「(属性名の略語) = (設定値)」にて表記。 subjectAltName に記述がない場合は subject を表示。
2	発行年月日	Validity	notBefore	設定値を和暦(日本標準時)に変換して表示。書式は「GGYY年MM月DD日」(GGは元号、時分秒は表示せず。)
3	有効期間の満了日		notAfter	
4	発行者	IssuerAltName または Issuer	CountryName OrganizationName OrganizationalUnitName OrganizationalUnitName	IssuerAltName の DN を全て表示。 DN は属性毎に改行して表示し、「(属性名の略語) = (設定値)」にて表記。 issuerAltName に記述がない場合は issuer を表示。
5	フィンガープリント	-	-	電子証明書のハッシュ値を計算して表示。ハッシュ関数は「sha256」を使用する。

## 利用者証明書

メニュー画面の「自分の証明書を確認する」ボタンを押下することで、ICカードに格納されている利用者の電子証明書を表示する。



図 4 - 8 電子証明書表示ボタン(利用者証明書)

電子証明書選択画面で表示する利用者証明書を選択し、「OK」ボタンを押下することで、選択された利用者証明書を表示する。

電子証明書選択画面の画面イメージは「[図 4 - 6 電子証明書選択画面イメージ](#)」を参照。

## (1) 署名用電子証明書の場合

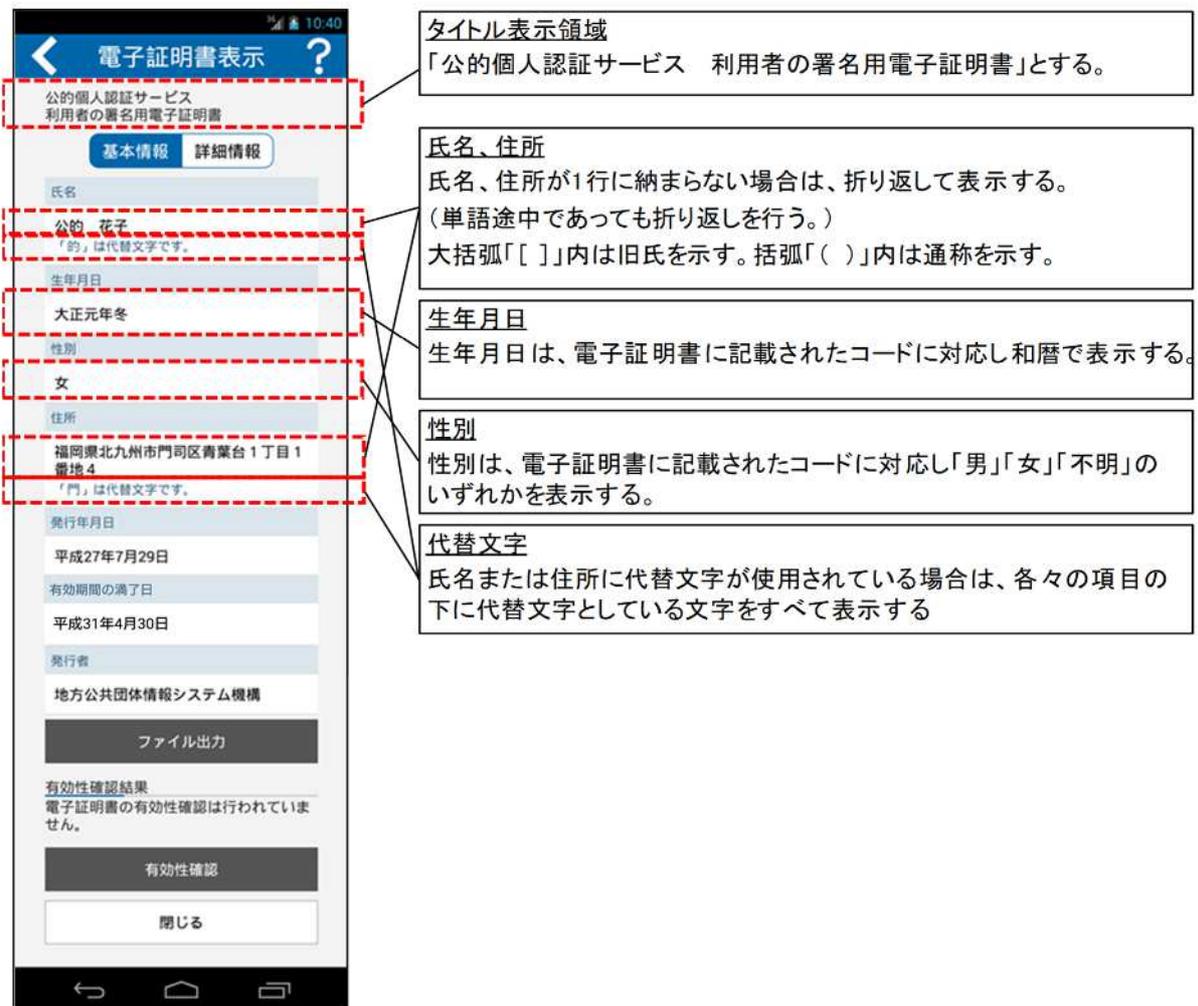


図 4-9 基本画面イメージ(署名用電子証明書)

表 4-2 表示項目と証明書領域の対応(利用者証明書)

項番	項目名	証明書の項目名		表示方法	
		上位項目名	項目名		
1	氏名	SubjectAltName	commonName	設定値をそのまま表示。 大括弧「[ ]」内は旧氏を示す。 括弧「( )」内は通称を示す。	
2	代替文字の使用(氏名)		substituteCharacterOf-CommonName <sup>1</sup>	・代替文字を「鍵括弧」付で表示。 ・代替文字が複数ある場合は代替文字を続けて表示。 例)「吉」「郎」は代替文字です。	
3	生年月日		dateOfBirth <sup>2</sup>	設定値を和暦に変換して表示。	
4	性別		gender <sup>3</sup>	設定値を日本語表記に変換して表示。	
5	住所		Address	設定値をそのまま表示。	
6	代替文字の使用(住所)		substituteCharacterOf-Address <sup>1</sup>	・代替文字を「鍵括弧」付で表示。 ・代替文字が複数ある場合は代替文字を続けて表示。 例)「葛」「飾」は代替文字です。	
7	発行年月日		Validity	notBefore	設定値を和暦(日本標準時)に変換して表示。書式は「GGYY年MM月DD日」(GGは元号、時分秒は表示せず。)
8	有効期間の満了日			notAfter	
9	発行者		IssuerAltName	organizationalUnitName	設定値をそのまま表示。

## 1 代替文字の設定ルール

## ( ) 表記ルール

1. 代替文字を"1"、それ以外を"0"で表現する。
2. スペースも1文字として捉え、ルール1を適用する。

## ( )表記例

項目名	設定値	代替文字使用位置の値	説明
氏名	吉田 太郎	10000	氏名の長さは5文字 1文字目の「吉」が代替文字
住所	東京都葛飾区 x x x	000100000	住所の長さは9文字 4文字目の「葛」が代替文字

は全角スペース

## 2 生年月日の設定ルール

## ( ) コード体系

英数字型 9桁 EYYYYMMDD

E : 年号コード 1桁 (1:明治 2:大正 3:昭和 4:平成 5:令和)

YYYY : 西暦年 4桁

MM : 月 2桁(01~12:1月~12月 00:不明 A1:春 A2:夏 A3:秋 A4:冬)

DD : 日 2桁(01~31:1日~31日 00:不明 A1:上旬 A2:中旬 A3:下旬)

## ( ) 表記例

例	生年月日の値	表 記
通常	420030401	平成 15 年 4 月 1 日
年号のはざまの日	219261225	大正 15 年 12 月 25 日
	319261225	昭和元年 12 月 25 日
年月日不明	000000000	
月日不明	319260000	昭和元年
	31926A100	昭和元年春
日不明	319261200	昭和元年 12 月
	3192612A2	昭和元年 12 月中旬

## 3 性別の設定ルール

## ( ) コード体系

英数字型 1桁 X

X : 性別コード1桁 (1:男 2:女 3:不明)

## (2) 利用者証明用電子証明書の場合

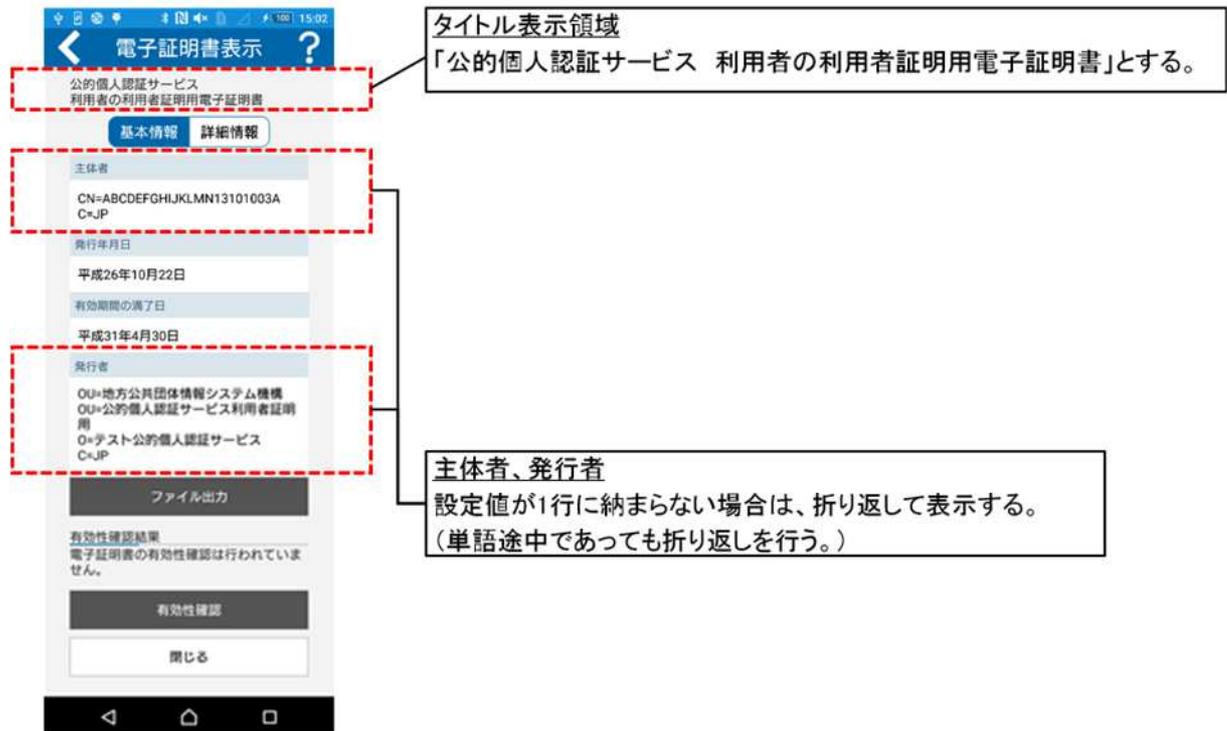


図 4 - 1 0 利用者証明用電子証明書

表 4 - 3 表示項目と証明書領域の対応(利用者証明用電子証明書)

項番	項目名	証明書の項目名		表示方法
		上位項目名	項目名	
1	主体者	SubjectAltName または Subject	CountryName CommonName 例)利用者証明用電子証明書の場合	SubjectAltName の DN を全て表示。 DN は属性毎に改行して表示し、「(属性名の略語) = (設定値)」にて表記。 subjectAltName に記述がない場合は subject を表示。
2	発行年月日	Validity	notBefore	設定値を和暦(日本標準時)に変換して表示。書式は「GGYY年MM月DD日」(GGは元号、時分秒は表示せず。)
3	有効期間の満了日		notAfter	
4	発行者	IssuerAltName または Issuer	CountryName OrganizationName OrganizationalUnitName OrganizationalUnitName 例)利用者証明用電子証明書の場合	IssuerAltName の DN を全て表示。 DN は属性毎に改行して表示し、「(属性名の略語) = (設定値)」にて表記。issuerAltName に記述がない場合は issuer を表示。

官職証明書、職責証明書、その他の証明書  
 メニュー画面の「その他の証明書の確認」ボタンを押下することで、官職証明書、職責証明書、その他の証明書ファイルを開いて表示する。



図 4 - 1 1 電子証明書表示ボタン(官職証明書、職責証明書、その他の証明書)

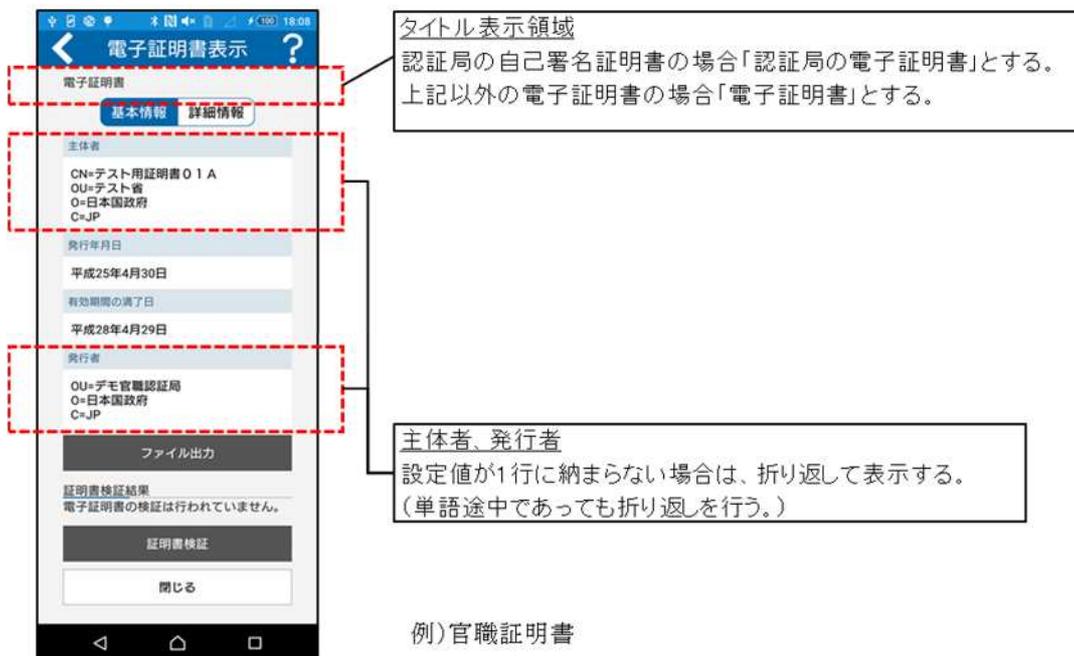
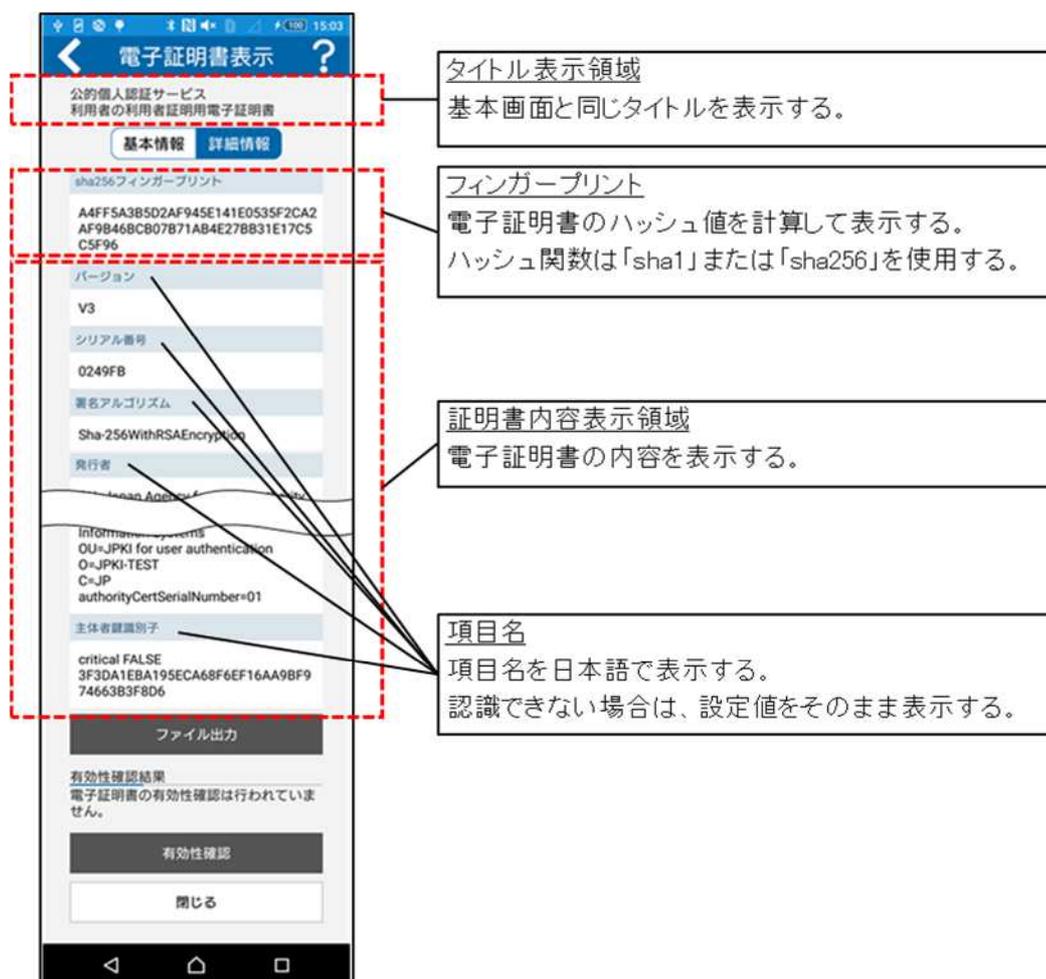


図 4 - 1 2 基本画面イメージ(官職証明書、職責証明書、その他の証明書)

表 4-4 表示項目と証明書領域の対応(官職証明書、職責証明書、その他の証明書)

項番	項目名	証明書の項目名		表示方法
		上位項目名	項目名	
1	主体者	SubjectAltName または Subject	CountryName OrganizationName OrganizationalUnitName CommonName 例)官職証明書の場合	SubjectAltName の DN を全て表示。 DN は属性毎に改行して表示し、「(属性名の略語) = (設定値)」にて表記。 subjectAltName に記述がない場合は subject を表示。
2	発行年月日	Validity	notBefore	設定値を和暦(日本標準時)に変換して表示。書式は「GGYY年MM月DD日」(GGは元号、時分秒は表示せず。)
3	有効期間の満了日		notAfter	
4	発行者	IssuerAltName または Issuer	CountryName OrganizationName OrganizationalUnitName OrganizationalUnitName 例)官職証明書の場合	IssuerAltName の DN を全て表示。 DN は属性毎に改行して表示し、「(属性名の略語) = (設定値)」にて表記。 issuerAltName に記述がない場合は issuer を表示。
5	フィンガープリント	-	-	認証局の自己署名証明書の場合のみ表示。 電子証明書のハッシュ値を計算して表示。ハッシュ関数は「sha1」または「sha256」を使用する。

## 詳細画面



詳細画面は、X.509 証明書における全ての記載事項を表示する画面である。尚、詳細画面は証明書の種類によらず、同様の画面仕様とする。

図 4-13 詳細画面イメージ

以下に、詳細画面の設定値表示に関する共通ルールを示す。

- ◇ 項目名、表示内容は、証明書プロファイルにおける最上位項目毎に表示する。ただし、有効期間については、「発行年月日」と「有効期間の満了日」を個別に表示する。
- ◇ 日付は設定値を西暦(日本標準時)で表示する。ただし、利用者証明書における利用者の生年月日については和暦(日本標準時)で表示する。
- ◇ オブジェクト識別子(OID: Object Identifier)については、対応する値に変換して表示する。対応する値がない場合は、OID をそのまま表示する。
- ◇ 鍵使用目的(KeyUsage)については、bit 列のうち、値が“1”の項目のみを名称で表示する。

例) 110000000 digitalSignature , nonRepudiation

次に、証明書基本領域と証明書拡張領域の表記ルールを示す。

< 証明書基本領域 >

- ◇ 発行者(issuer)と主体者(subject)については、DNの属性毎に改行して表示する。但し、利用者証明書の主体者については、一般名(CN: commonName)のみを以下のように分け、個別に表示する。

署名用電子証明書の場合

「発行申請送信時刻」「シーケンス番号」「受付端末識別記号」

([図 4-1-4 詳細画面イメージ\(署名用電子証明書\)](#)~~図 4-1-4 詳細画面イメージ(署名用電子証明書)~~参照)

利用者証明用電子証明書の場合

「ランダム文字列」「受付端末識別記号」

([図 4-1-5 詳細画面イメージ\(利用者証明用電子証明書\)](#)~~図 4-1-5 詳細画面イメージ(利用者証明用電子証明書)~~参照)

- ◇ 主体者公開鍵情報(subjectPublicKeyInfo)については、公開鍵値(subjectPublicKey)を16進数で表示する。

< 証明書拡張領域 >

- ◇ 最上位項目以下の情報を項目毎に階層表示とする。

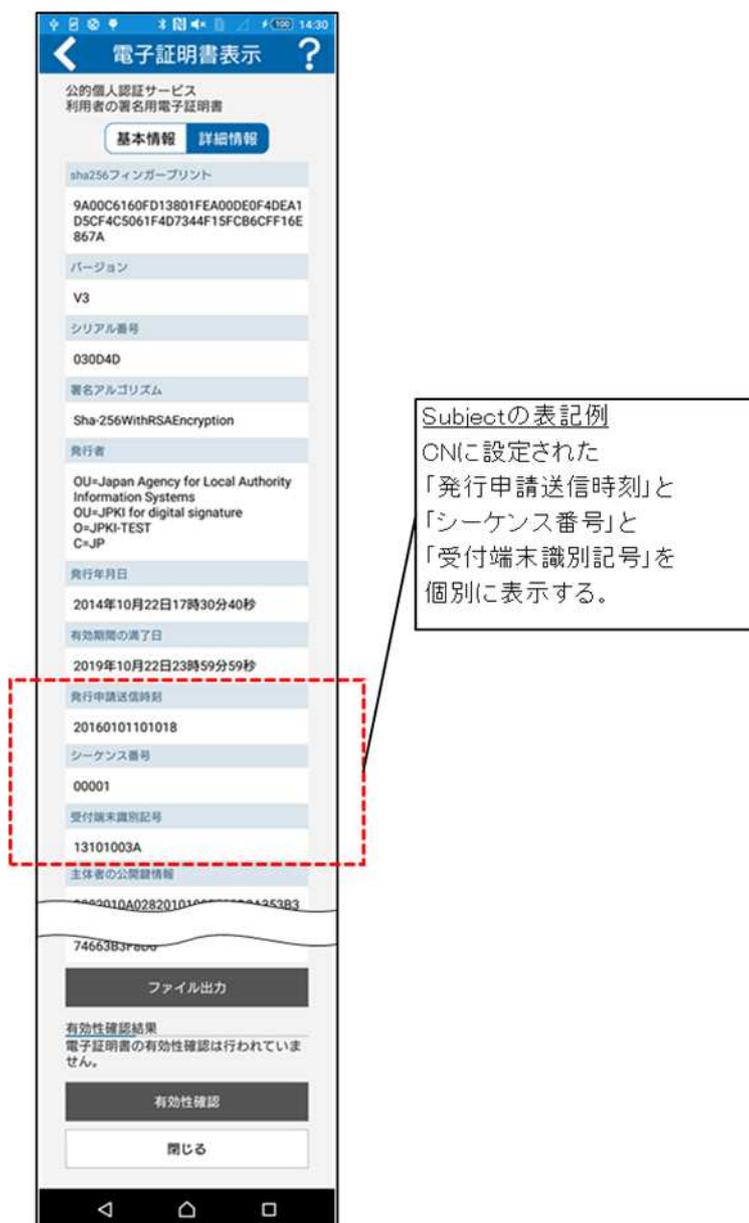


図 4 - 1 4 詳細画面イメージ(署名用電子証明書)

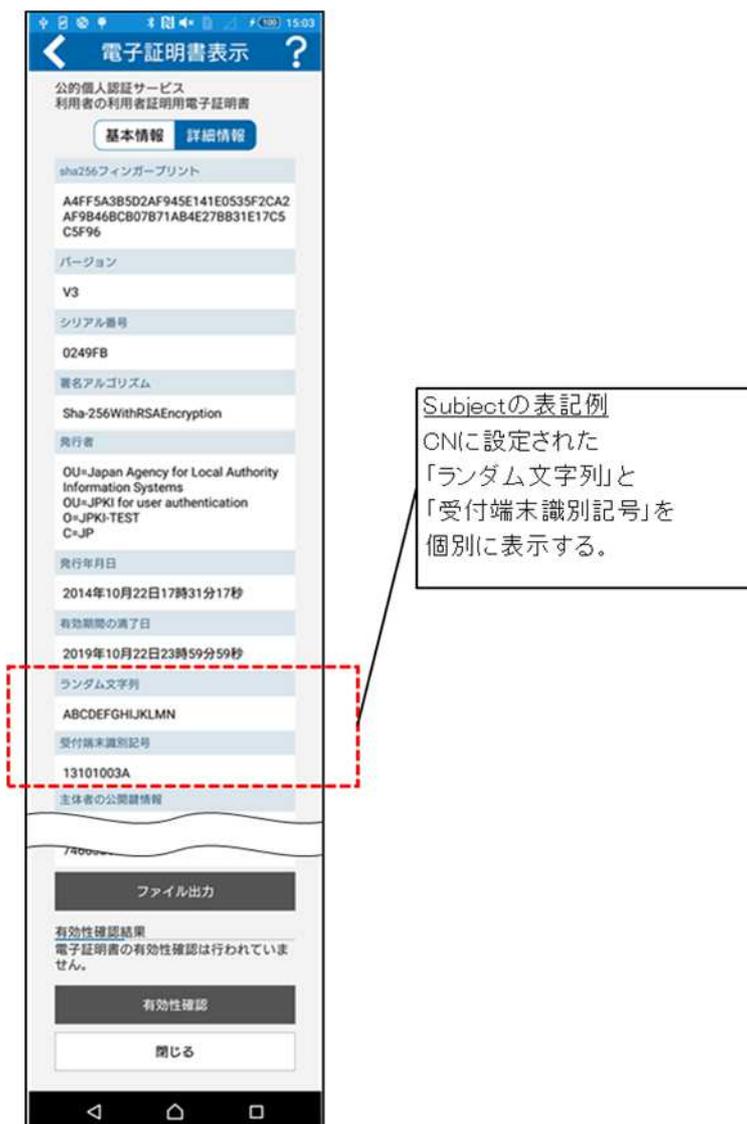


図 4-15 詳細画面イメージ(利用者証明用電子証明書)

## 第4節 電子証明書出力機能

### 1 概要

電子証明書表示機能にて表示した電子証明書をファイルに出力する。

### 2 機能仕様

(1) 電子証明書表示機能の画面に配置されたファイル出力ボタンを押下することで、電子証明書を DER 形式のファイルまたはテキスト形式 (ASCII 形式) のファイルとして出力する。

(2) 本機能では、次の2つの機能を持つ。

- 電子証明書を DER 形式のファイルとして出力する。
- 電子証明書表示機能の画面表示内容をテキスト形式のファイルとして出力する。  
ファイル名と拡張子については(4)を参照。

(3) 電子証明書表示機能の表示対象となる以下の電子証明書を、ファイル出力の対象とする。

#### 公的個人認証サービス(JPKI)

- ◇ ICカードに格納された署名用電子証明書
- ◇ ICカードに格納された署名用認証局の自己署名証明書
- ◇ ICカードに格納された利用者証明用電子証明書
- ◇ ICカードに格納された利用者証明用認証局の自己署名証明書

#### 政府認証基盤(GPKI)

- ◇ 電子公文書等に添付された官職証明書
- ◇ 電子公文書等に添付された CA の自己署名証明書

#### 地方公共団体における組織認証基盤(LGPKI)

- ◇ 電子公文書等に添付された職責証明書
- ◇ 電子公文書等に添付された CA の自己署名証明書

#### その他

- ◇ その他の認証基盤および CA で発行された電子証明書

(4) ファイル名は以下の通りとする。

表 4-5 ファイル出力時のファイル名称

#	形式	表示内容	ファイル名称 <sup>1</sup>
1	DER 形式	-	証明書の種類 <sup>2</sup> YYYYMMDDhhmmss.cer
2	テキスト	基本情報	証明書の種類 <sup>2</sup> BasicYYYYMMDDhhmmss.txt
3	形式	詳細情報	証明書の種類 <sup>2</sup> DetailYYYYMMDDhhmmss.txt

1 ファイル名の "YYYYMMDDhhmmss" は以下の通り。

"YYYY": 年、"MM": 月、"DD": 日、"hh": 時、"mm": 分、"ss": 秒

- 2 “証明書の種類”に設定する文字列は、[表 4 - 6 “証明書の種類”に設定する文字列表 4 - 6 “証明書の種類”に設定する文字列](#)参照。

表 4 - 6 “証明書の種類”に設定する文字列

#	認証基盤	電子証明書	文字列
1	公的個人認証サービス (JPKI)	署名用電子証明書	CertUserAuth
2		利用者証明用電子証明書	CertUserSign
3		署名用認証局の自己署名 証明書	CertCAAuth
4		利用者証明用認証局の自 己署名証明書	CertCASign
5	上記以外	-	CertOther

### 3 画面仕様

電子証明書表示画面の「ファイル出力」ボタンを押下することで、表示している電子証明書を DER 形式またはテキスト形式で出力する。



図 4-16 電子証明書出力ボタン

## 第5節 基本4情報取得機能

### 1 概要

電子申請を行う際に、ICカードに格納された署名用電子証明書から申請者の氏名、性別、生年月日、住所を取得する。

### 2 機能仕様

(1) 本機能は、以下のAPIで対応する。

➤ Android インテント

(2) 上位アプリケーションからICカードに格納された署名用電子証明書を受け取り、受け取った署名用電子証明書から基本4情報を取得して、上位アプリケーションに返す。

(3) 上位アプリケーションから受け取る電子証明書のデータ形式はDER形式とする。

(4) 基本4情報取得の際は、電子証明書内のsubjectAltNameのOtherNameから以下の情報を取得する。

◇ 氏名(代替文字の使用の有無、大括弧「[ ]」内は旧氏を示す、  
括弧「( )」内は通称を示す。)

◇ 住所(代替文字の使用の有無)

◇ 性別

◇ 生年月日(9桁のコード(EYYYYMMDD))

E : 年号コード(1:明治 2:大正 3:昭和 4:平成 5:令和)

YYYY : 西暦年

MM : 月(01~12:1月~12月 00:不明 A1:春 A2:夏 A3:秋 A4:冬)

DD : 日(01~31:1日~31日 00:不明 A1:上旬 A2:中旬 A3:下旬)

## 第6節 電子署名作成機能

### 1 概要

電子申請を行う際に、ICカードに格納された利用者の秘密鍵を使用して電子署名を作成する。

### 2 機能仕様

(1) 本機能は、以下のAPIで対応する。

➤ Android インテント

(2) 本機能では、次の5つの機能を実現する。

- 上位アプリケーションから署名対象データまたは署名対象データのハッシュ値（ハッシュ関数はSHA-1またはSHA-256に限る）を受け取る。
- ハッシュ値の場合は、受け取ったハッシュ値をそのままICカードに引き渡す。
- ICカード内で作成された電子署名を受け取り、上位アプリケーションに返す。
- 利用者の秘密鍵による暗号演算（電子署名生成）については、ICカード内の個人認証カードAPが行う。

(3) 署名アルゴリズムは「Sha-1WithRSAEncryption」、「Sha-256WithRSAEncryption」とする。

## 第7節 電子証明書取得機能

### 1 概要

ICカードに格納された利用者証明書または認証局の自己署名証明書を取得する。

### 2 機能仕様

(1) 本機能は、以下のAPIで対応する。

➤ Android インテント

(2) 取得対象とする電子証明書は以下の通りとする。

公的個人認証サービス(JPKI)

- ◇ ICカードに格納された署名用電子証明書
- ◇ ICカードに格納された署名用認証局の自己署名証明書
- ◇ ICカードに格納された利用者証明用電子証明書
- ◇ ICカードに格納された利用者証明用認証局の自己署名証明書

(3) 上位アプリケーションにおいて利用者証明書または認証局の自己署名証明書を指定することで、ICカードから対象の電子証明書を取得し、上位アプリケーションに返す。

(4) 上位アプリケーションに返す電子証明書のデータ形式はDER形式とする。

## 第8節 電子署名検証機能

### 1 概要

利用者が行政機関等から受け取った電子公文書等の電子署名を検証する。

### 2 機能仕様

(1) 本機能は、以下のAPIで対応する。

➤ Android インテント

(2) 本機能では、次の3つの機能を実現する。

➤ 上位アプリケーションから以下の情報を受け取る。

- ・ 署名対象データのハッシュ値（ハッシュ関数はSHA-1またはSHA-256に限る）
- ・ 電子署名
- ・ 電子署名の作成で使用した秘密鍵に対応する公開鍵

➤ 受け取った情報を使用して電子署名の検証を行う。

➤ 電子署名の検証結果を上位アプリケーションに返す。

(3) 署名アルゴリズムは「Sha-1WithRSAEncryption」、「Sha-256WithRSAEncryption」とする。

## 第9節 官職証明書検証機能

### 1 概要

- (1) 行政機関からの結果通知等に添付されている官職証明書または職責証明書を検証するために、公的個人認証サービスに問合せを行う。
- (2) 電子証明書表示機能から官職証明書または職責証明書の検証を行う。

### 2 機能仕様

- (1) 電子証明書表示機能における官職証明書または職責証明書の検証機能については、本機能を適用して実装する。
- (2) 検証対象とする電子証明書の種類は以下の通り。
  - 政府認証基盤(GPKI)
    - ◇ 電子公文書等に添付された官職証明書
  - 地方公共団体における組織認証基盤(LGPKI)
    - ◇ 電子公文書等に添付された職責証明書
- (3) 本機能では、次の2つの機能を実現する。
  - 上位アプリケーションから官職証明書あるいは職責証明書を受け取り、検証要求電文を作成し、公的個人認証サービスセンターのCVSに対して証明書検証要求を発行する。
  - CVSから受け取った証明書検証結果電文から検証結果を取り出し、上位アプリケーションに返す。
- (4) 証明書検証要求電文で必要となる認証局の自己署名証明書と利用者証明書については、電子証明書取得機能を用いてICカードより取得する。
- (5) CVSへの証明書検証要求電文には、電子署名作成機能を用いて利用者の電子署名を付与する。この際、電子署名の付与には、利用者の署名用電子証明書に対する秘密鍵を利用する。このため、本機能を利用する際は、ICカード内に利用者の署名用電子証明書および署名用電子証明書に対する秘密鍵が格納されている事が前提となる。
- (6) 上位アプリケーションから受け取る電子証明書のデータ形式はDER形式とする。
- (7) 公的個人認証サービスセンターとの通信機能を有する。

### 3 画面仕様

電子証明書表示画面(官職証明書、職責証明書、その他の証明書)の「証明書検証」ボタンを押下することで、証明書検証を行う。

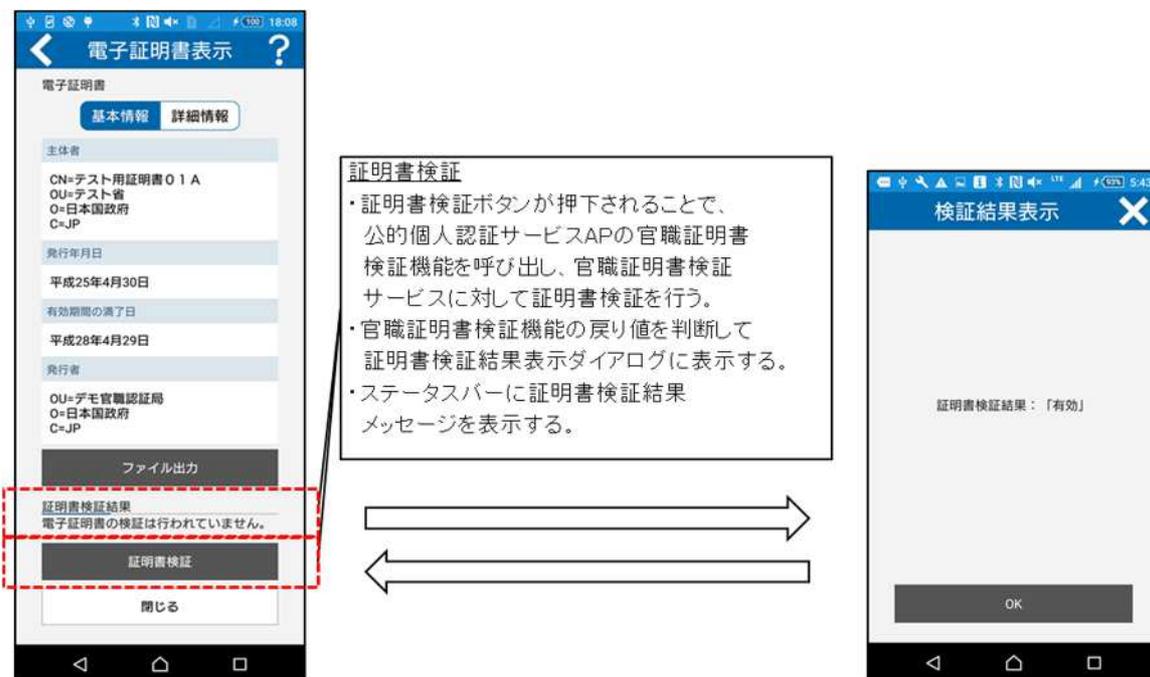


図 4 - 1 7 証明書検証画面イメージ

## 第10節 自分の電子証明書の有効性確認機能

### 1 概要

- (1) ICカード内の自分の電子証明書(利用者証明書)の有効性を確認するために、公的個人認証サービスに問合せを行う。
- (2) 電子証明書表示機能から利用者証明書の有効性確認を行う。

### 2 機能仕様

- (1) 電子証明書表示機能における利用者証明書の有効性確認機能については、本機能を適用して実装する。
- (2) 有効性確認の対象となる電子証明書の種類は以下の通り。  
公的個人認証サービス(JPKI)
  - ◇ ICカードに格納された利用者証明書
- (3) 本機能では、次の2つの機能を実現する。
  - ICカードから利用者証明書を取り出し、有効性確認電文を作成し、公的個人認証サービスセンターのオンライン窓口サーバに対して電子証明書の有効性確認要求を発行する。
  - オンライン窓口サーバから受け取った有効性確認結果電文から確認結果を取り出し、上位アプリケーションに返す。
- (4) 有効性確認電文で必要となる認証局の自己署名証明書と利用者証明書については、電子証明書表示機能を用いてICカードより取得する。
- (5) オンライン窓口サーバへの有効性確認電文には、電子署名作成機能を用いて利用者の電子署名を付与する。
- (6) 上位アプリケーションから受け取る電子証明書のデータ形式はDER形式とする。
- (7) 公的個人認証サービスセンターとの通信機能を有する。

### 3 画面仕様

電子証明書表示画面(利用者証明書)の「有効性確認」ボタンを押下することで、利用者証明書の有効性確認を行う。

有効性確認が完了すると、画面下部のメッセージは以下通りとなる。



図 4 - 1 8 有効性確認画面イメージ

## 第11節 自分の電子証明書のオンライン失効申請機能

### 1 概要

利用者がインターネットを通じて IC カード内の自分の電子証明書(利用者証明書)の失効申請を行う。

### 2 機能仕様

- (1) 失効申請対象とする電子証明書の種類は以下の通り。  
公的個人認証サービス(JPKI)
  - ◇ IC カードに格納された利用者証明書
- (2) 失効申請対象とする電子証明書の種別は、証明書選択画面の選択によって決定される。
- (3) 本機能では、次の2つの機能を実現する。
  - IC カードから利用者証明書を取り出し、失効申請電文を作成し、公的個人認証サービスのオンライン窓口サーバに対して電子証明書の失効申請を行う。
  - オンライン窓口サーバから受け取った失効申請結果電文から申請結果を取り出し、GUI 画面に表示する。
- (4) 失効申請電文で必要となる認証局の自己署名証明書と利用者証明書については、電子証明書取得機能を用いて IC カードより取得する。
- (5) オンライン窓口サーバへの失効申請電文には、電子署名作成機能を用いて利用者の電子署名を付与する。この際、電子署名の付与には、利用者の署名用電子証明書に対する秘密鍵を利用する。このため、本機能を利用する際は、IC カード内に利用者の署名用電子証明書および署名用電子証明書に対する秘密鍵が格納されている事が前提となる。
- (6) 署名用電子証明書が失効している場合、利用者証明用電子証明書の失効申請を行うことはできない。このため署名用電子証明書、利用者署名用電子証明書の両方を失効申請する場合は、以下の順番で失効申請を行う必要がある。

順番	利用者証明用電子証明書の失効申請
順番	署名用電子証明書の失効申請
- (7) 公的個人認証サービスセンターとの通信機能を有する。

### 3 画面仕様

メニュー画面の「証明書の失効申請」ボタンを押下することで、オンライン失効申請画面を表示する。



図 4 - 1 9 証明書の失効申請ボタン

#### 画面共通仕様

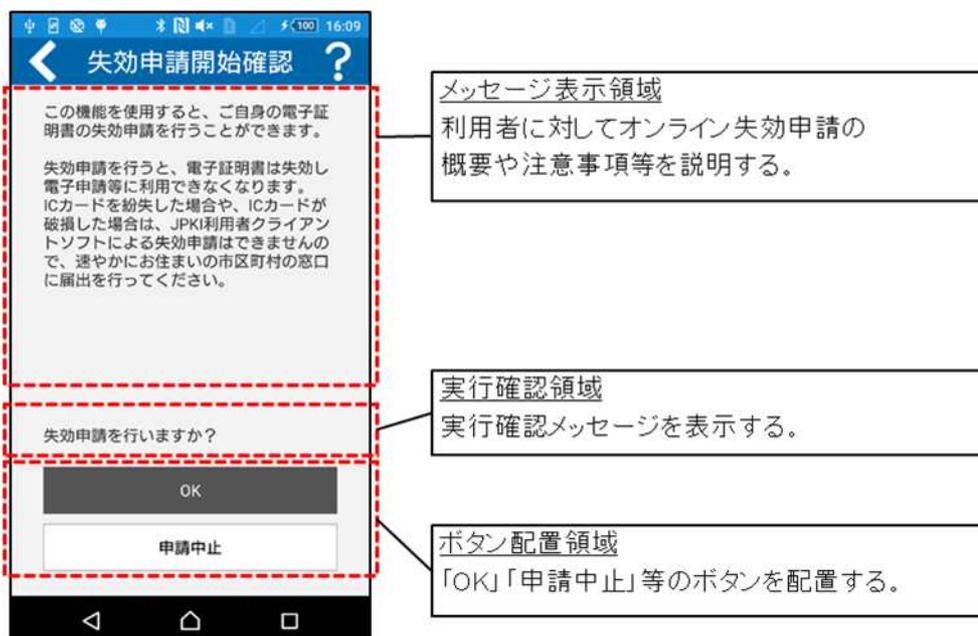


図 4 - 2 0 画面共通仕様イメージ

- フォントは、Android に標準搭載されている「モトヤ L マルベリ 3」を使用する。
- フォントサイズは視認性を考慮し「14sp」とする。
- 生年月日を画面に表示する際、電子証明書表示機能と同一の設定ルールに従い、書式は「G G Y Y 年 MM 月 DD 日」(G G は元号、時分秒は表示せず)で表示する。
- 性別を画面に表示する際、電子証明書表示機能と同一の設定ルールに従い、「男」、「女」、「不明」のいずれかで表示する。

## 署名用電子証明書の場合 画面遷移



図 4-2 1 オンライン失効申請機能の画面遷移 (署名用電子証明書) (1/2)

OK 押下後に IC カードセット案内画面を表示し、IC カードをセットします。



図 4-2-2 オンライン失効申請機能の画面遷移(署名用電子証明書)(2/2)  
電子署名の実施前に IC カードセット案内画面を表示し、IC カードをセットします。

## 利用者証明用電子証明書の場合 画面遷移

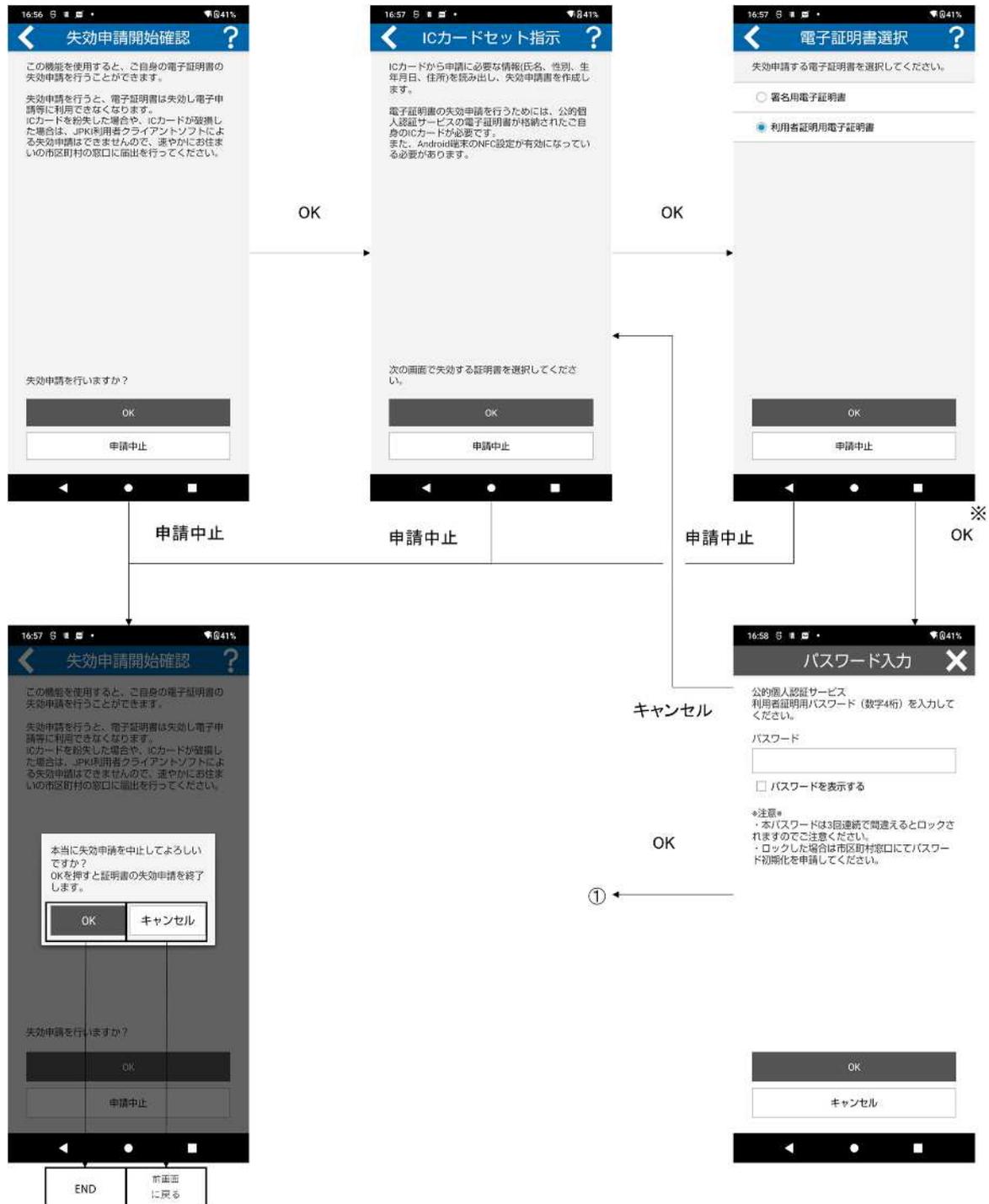


図 4-23 オンライン失効申請機能の画面遷移(利用者証明用電子証明書)(1/2)  
OK 押下後に IC カードセット案内画面を表示し、IC カードをセットします。



図 4-2-4 オンライン失効申請機能の画面遷移(利用者証明用電子証明書)(2/2)  
電子署名の実施前に IC カードセット案内画面を表示し、IC カードをセットします。

## 第12節 ソフトウェア動作確認機能

### 1 概要

Android版 JPKI 利用者ソフトから NFC と IC カード間の疎通を確認する。

### 2 機能仕様

(1) 本機能では、次の機能を実現する。

- Android 版 JPKI 利用者ソフトから NFC と IC カードが認識できるかを確認する。PC 版 JPKI 利用者ソフトと同様、IC カードが個人番号カードか否かについての判別は行わない。

### 3 画面仕様

メニュー画面の「動作確認」ボタンを押下する。



図 4 - 2 5 動作確認ボタン

ICカードを認識すると以下の画面が表示される。



図 4 - 2 6 動作確認完了画面イメージ

## 第13節 パスワード変更機能

### 1 概要

利用者の IC カードに設定されたパスワードの変更を行う。

### 2 機能仕様

- (1) メニュー画面の「パスワード変更」ボタンを押下することで、個別パスワードまたは統合パスワードを選択する画面を表示する。
- (2) 変更パスワード選択画面から「個別パスワード変更」を選択することにより、IC カードに設定された以下のパスワードから選択されたパスワードを個別に変更する。
  - ◇ 公的個人認証 署名用パスワード
  - ◇ 公的個人認証 利用者証明用パスワード
  - ◇ 券面事項入力補助用パスワード
  - ◇ 個人番号カード用パスワード
- (3) 変更パスワード選択画面から「統合パスワード変更」を選択することにより、IC カードに設定された以下のパスワードを一括して変更する。
  - ◇ 公的個人認証 利用者証明用パスワード
  - ◇ 券面事項入力補助用パスワード
  - ◇ 個人番号カード用パスワード
- (4) パスワード変更の際に入力誤りが発生しないように、パスワード確認用の入力欄を別途設ける。
- (5) パスワードは伏せ字として表示する。(「パスワードを表示する」にチェックを入れると、入力されたパスワードが表示される。)
- (6) 各パスワードに入力する文字数および文字種を以下に示す。

表 4-7 パスワードに入力する文字数および文字種

項番	パスワードの種別	文字数	文字種	備考
1	公的個人認証 署名用パスワード	6~16	半角英数字	・数字と英字両方の入力が必要 ・英小文字が入力された場合は、英大文字に変換して IC カードに設定する
2	公的個人認証 利用者証明用パスワード	4	半角数字	
3	券面事項入力補助用パスワード	4	半角数字	
4	個人番号カード用パスワード	4	半角数字	

- (7) パスワード変更機能で入力されたパスワードを、利用者の Android 端末に残さない方式とする。

- (8) パスワードがロックされている場合には、その旨の表示をする。統合パスワード変更で、いずれかのパスワードがロックされていた場合には、その旨の表示をする。
- (9) 統合パスワード変更は、以下の順番でパスワードの変更を行う。
  - ◇ 「公的個人認証 利用者証明用パスワード」
  - ◇ 「券面事項入力補助用パスワード」
  - ◇ 「個人番号カード用パスワード」
- (10) 統合パスワード変更において、いずれかのパスワードの変更に失敗した場合、その時点で処理を中止し、以降のパスワード変更は行われぬ。
- (11) 「個人番号カード用パスワード」の変更は、以下の順番で2つのパスワードの変更を行う。
  - ◇ 「個人番号カード用パスワード(住基 AP)」
  - ◇ 「個人番号カード用パスワード(本人確認業務用領域)」
- (12) 「個人番号カード用パスワード」の変更において、「個人番号カード用パスワード(住基 AP)」が成功、「個人番号カード用パスワード(本人確認業務用領域)」が失敗した場合、「個人番号カード用パスワード(本人確認業務用領域)」を含むエラーメッセージを表示する( )。

上記のケースが発生した場合、「個人番号カード用パスワード(住基 AP)」と「個人番号カード用パスワード(本人確認業務用領域)」は不一致の状態となる。Android版 JPKI 利用者ソフトで「個人番号カード用パスワード」の変更を行うためには、上記2つのパスワードが一致している必要があるため、上記のケースにおいてはAndroid版 JPKI 利用者ソフトではパスワード変更は行えない。

### 3 画面仕様

メニュー画面の「パスワード変更」ボタンを押下することで、変更パスワード選択画面を表示する。



図 4-27 パスワード変更ボタン



図 4-28 変更パスワード選択画面イメージ

## 個別パスワード変更

変更パスワード選択画面の「個別パスワード変更」ボタンを押下することで、個別パスワード選択画面を表示する。



図 4-29 個別パスワード選択画面イメージ

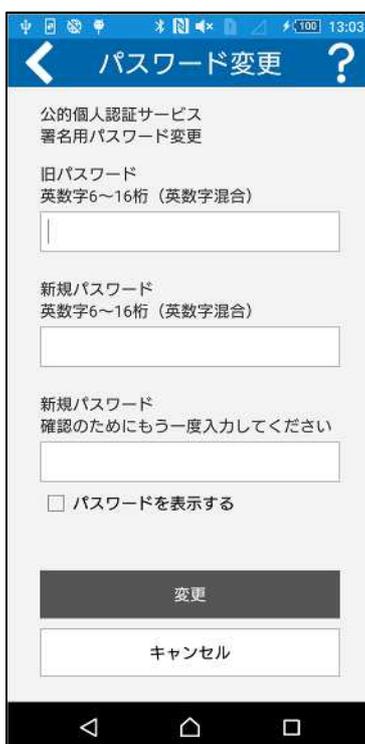


図 4-30 署名用パスワード変更画面イメージ



図 4 - 3 1 利用者証明用パスワード変更画面イメージ



図 4 - 3 2 券面事項入力補助用パスワード変更画面イメージ



図 4-3-3 個人番号カード用パスワード変更画面イメージ

パスワードの変更に成功した場合、以下の画面を表示する。



図 4-3-4 個別パスワード変更結果画面イメージ

## 統合パスワード変更

変更パスワード選択画面の「統合パスワード変更」ボタンを押下することで、統合パスワード変更画面を表示する。

公的個人認証サービス  
統合パスワード変更

旧パスワード  
数字4桁

新規パスワード  
数字4桁

新規パスワード  
確認のためにもう一度入力してください

パスワードを表示する

変更

キャンセル

図 4-35 統合パスワード変更画面イメージ

全てのパスワードの変更に成功した場合、以下の画面を表示する。

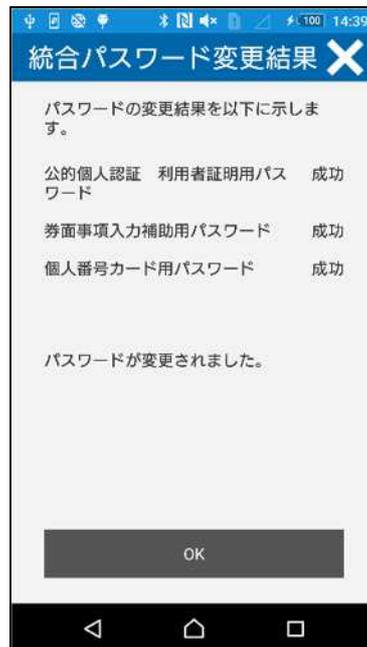


図 4 - 3 6 統合パスワード変更結果画面イメージ

## 第14節 プロキシ設定機能

### 1 概要

プロキシサーバを利用する場合の設定を行う。

### 2 機能仕様

(1) プロキシ設定画面から設定する。

(2) ポートの値は1～65535の範囲とする。

(3) パスワードは伏せ字として表示する。(「パスワードを表示する」にチェックを入れると、入力されたパスワードが表示される。)

### 3 画面仕様

メニュー画面の「プロキシ設定」ボタンを押下することで、プロキシ設定画面を表示する



図 4-37 プロキシ設定ボタン



図 4-38 プロキシ設定画面イメージ



図 4-39 プロキシ設定完了通知画面イメージ

## 第15節 電子証明書の更新通知機能

### 1 概要

ICカード内の署名用電子証明書および利用者証明用電子証明書の有効期間の満了日が過ぎる前に、電子証明書の更新を促す通知を行う。

### 2 機能仕様

(1) 本機能は、次の2つの機能を実現する。

- 電子証明書更新通知
- 更新通知設定

(2) 電子証明書更新通知は以下の仕様とする。

- 以下の方法で電子証明書表示履歴を保持する。
  - ・ 「第4章 第3節 電子証明書表示機能」でICカードに格納された署名用電子証明書または利用者証明用電子証明書を表示した際、電子証明書表示履歴（電子証明書の種別、シリアル番号、有効期間の満了日、自分の証明書表示日時）を保持する。
  - ・ 保持している電子証明書表示履歴に「第4章 第3節 電子証明書表示機能」で表示した電子証明書の種別、シリアル番号と一致する情報がすでに存在する場合は、自分の証明書表示日時のみを更新する。
  - ・ 保持している電子証明書表示履歴に「第4章 第3節 電子証明書表示機能」で表示した電子証明書の種別、シリアル番号と一致する情報が存在しない場合は、新規に保持する。
  - ・ 署名用電子証明書および利用者証明用電子証明書の電子証明書表示履歴をそれぞれ最大10件まで保持する。
  - ・ 署名用電子証明書の電子証明書表示履歴が10件を超えた場合、自分の証明書表示日時が最も古い署名用電子証明書の電子証明書表示履歴を破棄する。
  - ・ 利用者証明用電子証明書の電子証明書表示履歴が10件を超えた場合、自分の証明書表示日時が最も古い利用者証明用電子証明書の電子証明書表示履歴を破棄する。
  - ・ 「第4章 第3節 電子証明書表示機能」で表示していない電子証明書の電子証明書表示履歴は保持しない。
  - ・ 有効期間の満了日が過ぎている電子証明書の電子証明書表示履歴は保持しない。
- 以下の方法で電子証明書の更新を促す通知をする。
  - ・ Android版JPKI利用者ソフト起動時、電子証明書表示履歴を参照し、有効期間満了日が迫っている電子証明書が存在する場合は更新通知を行う。
  - ・ 有効期間満了日が迫っている電子証明書が存在しない場合は更新通知を行わない。
  - ・ 移動端末設備用電子証明書の有効期限情報は保持しない。

- ・ 移動端末設備用電子証明書に関して、電子証明書に伴い更新対象となる旨を更新通知画面のメッセージに記載する。
- ・ 以下の条件を満たす場合「有効期間満了日が迫っている電子証明書」と判断する。
  - ・ OSのシステム日付が電子証明書の有効期間満了日の3カ月前～有効期間満了日の間
- ・ 更新通知を行った電子証明書の電子証明書表示履歴は破棄され、以降は更新通知されない。ただし、更新通知を行った電子証明書が再び「第4章 第3節 電子証明書表示機能」で表示された場合は、再度、更新通知の対象となる。
- ・ 電子証明書表示機能で表示していない電子証明書は電子証明書表示履歴が保持されないため、更新通知の対象外となる。

(3) 更新通知設定は以下の仕様とする。

- Android版 JPKI 利用者ソフト起動時の電子証明書更新通知の有効、無効化を設定可能にする。
- 本機能は以下の方法で実行可能とする。
  - ・ メニュー画面に登録される「更新通知設定」の実行
- 「更新通知設定」を実行していない場合は、更新通知機能「無効」とみなす。

### 3 画面仕様

有効期間満了日が迫っている電子証明書が存在する場合、更新通知画面を表示する。



図 4-40 更新通知画面イメージ

メニュー画面の「更新通知設定」ボタンを押下することによって、更新通知設定画面を表示する。

「はい」が選択された場合、更新通知機能を有効とし、メニュー画面に戻る。

「いいえ」が選択された場合、更新通知機能を無効とし、メニュー画面に戻る。

戻るボタンを押下した場合、現在の設定内容を変更しない。

(Android版 JPKI 利用者ソフトインストール時の場合は未設定となることにより、更新通知機能「無効」とみなされる。)



図 4-4-1 更新通知設定ボタン

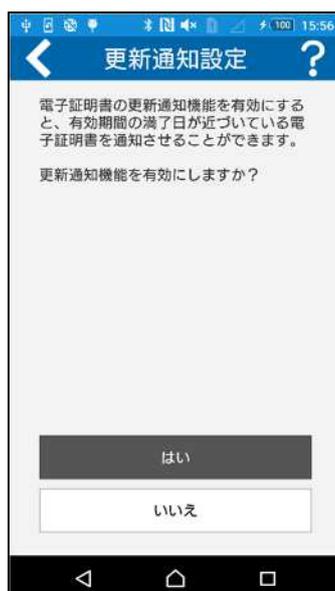


図 4-4-2 更新通知設定画面イメージ

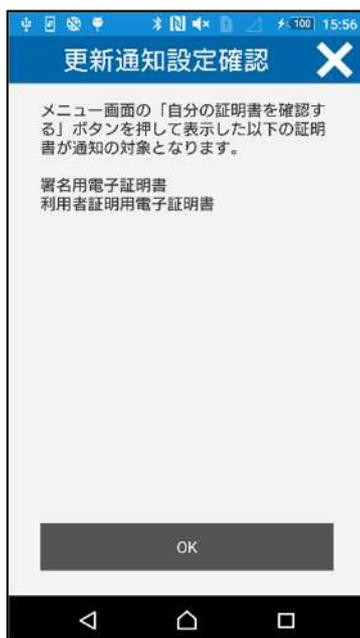


図 4 - 4 3 更新通知設定確認画面イメージ

## 第16節 利用者同意状況確認機能

### 1 概要

利用者がインターネットを通じて、ICカード内および移動端末設備内の利用者証明用電子証明書に紐づく基本4情報提供のサービス事業者の各サービスへの利用者同意状況確認および利用者同意取消申請を行う。

### 2 機能仕様

(1) 利用者同意状況確認申請および利用者同意取消申請で使用する電子証明書の種類は以下の通り。

公的個人認証サービス(JPKI)

- ◇ ICカードに格納された利用者証明用電子証明書
- ◇ ICカードに格納された署名用電子証明書
- ◇ 移動端末設備内に格納された利用者証明用電子証明書
- ◇ 移動端末設備内に格納された署名用電子証明書

(2) 利用者同意状況確認申請で使用する電子証明書の種別は、証明書選択ダイアログの選択によって決定される。証明書選択ダイアログの表示タイミングについては「[図 4-46](#) [図-4-46](#)」を参照。

(3) 本機能では、次の4つの機能を実現する。

- ICカードまたは移動端末設備に格納された利用者証明用電子証明書を取り出し、利用者同意状況確認申請電文を作成し、公的個人認証サービスの利用者同意管理サーバに対して利用者同意状況確認申請を行う。
- 利用者同意管理サーバから受け取った利用者同意状況確認申請結果電文から申請結果(4情報提供に対する同意状況一覧)を取り出し、GUI画面に表示する。  
なお、申請結果はシリアル番号に紐づく個人番号カード用署名用証明書および移動端末設備用署名用証明書の結果が含まれ、単一利用者・全サービス分が応答される。
- ICカードまたは移動端末設備に格納された署名用電子証明書を取り出し、ユーザが選択したサービスを元に利用者同意取消申請電文を作成し、公的個人認証サービスの利用者同意管理サーバに対して利用者同意取消申請を行う。
- 利用者同意管理サーバから受け取った利用者同意取消申請結果電文から申請結果を取り出し、GUI画面に表示する。

(4) 利用者同意状況確認申請電文で必要となる利用者証明用電子証明書、および利用者同意取消申請電文で必要となる署名用電子証明書については、電子証明書取得機能( )を用いてICカードまたは移動端末設備内より取得する。

(5) 利用者同意管理サーバへの利用者同意状況確認申請電文には、電子署名作成機能( )を用いて利用者の電子署名を付与する。この際、電子署名の付与には利用者証明用電子証明書に対する秘密鍵を利用する。このため、本機能を利用する際は、ICカード内または移動端末設備内に利用者の利用者証明用電子証明書、利用者証明用電子証明書に対する秘密鍵が格納されている事が前提となる。

- (6) 利用者同意管理サーバへの利用者同意取消申請電文には、電子署名作成機能( )を用いて利用者の電子署名を付与する。この際、電子署名の付与には署名用電子証明書に対する秘密鍵を利用する。このため、本機能を利用する際は、ICカード内または移動端末設備内に署名用電子証明書および署名用電子証明書に対する秘密鍵が格納されている事が前提となる。
- (7) 電子証明書が「失効」「有効期限切れ」「一時保留」の場合、利用者同意状況確認申請および利用者同意取消申請を行うことはできない。なお、有効性確認の結果が「有効」の状態には、署名用電子証明書および利用者証明用電子証明書の状態が失効申請受理済みの場合も含まれる。
- (8) 公的個人認証サービスセンターとの通信機能を有する。

( )個人番号カード用の電子証明書に係る電子証明書取得機能及び電子署名作成機能は利用者クライアントソフトのみで提供する機能である。また、移動端末設備用の電子証明書に係る電子証明書取得機能及び電子署名作成機能はマイナポータルアプリを介して利用者クライアントソフトから提供される機能である。

### 3 画面仕様

メニュー画面の「住所等提供同意状況の照会・取消」ボタンを押下することで、提供同意状況の照会画面を表示する。



図 4 - 4 4 住所等提供同意状況の照会・取消ボタン

「住所等提供同意状況の照会・取消」ボタン押下後の画面遷移については、「[図 4 - 4 6](#) [図 4 - 4 6](#)、[図 4 - 4 7](#) [図 4 - 4 7](#)」を参照。

## 画面共通仕様

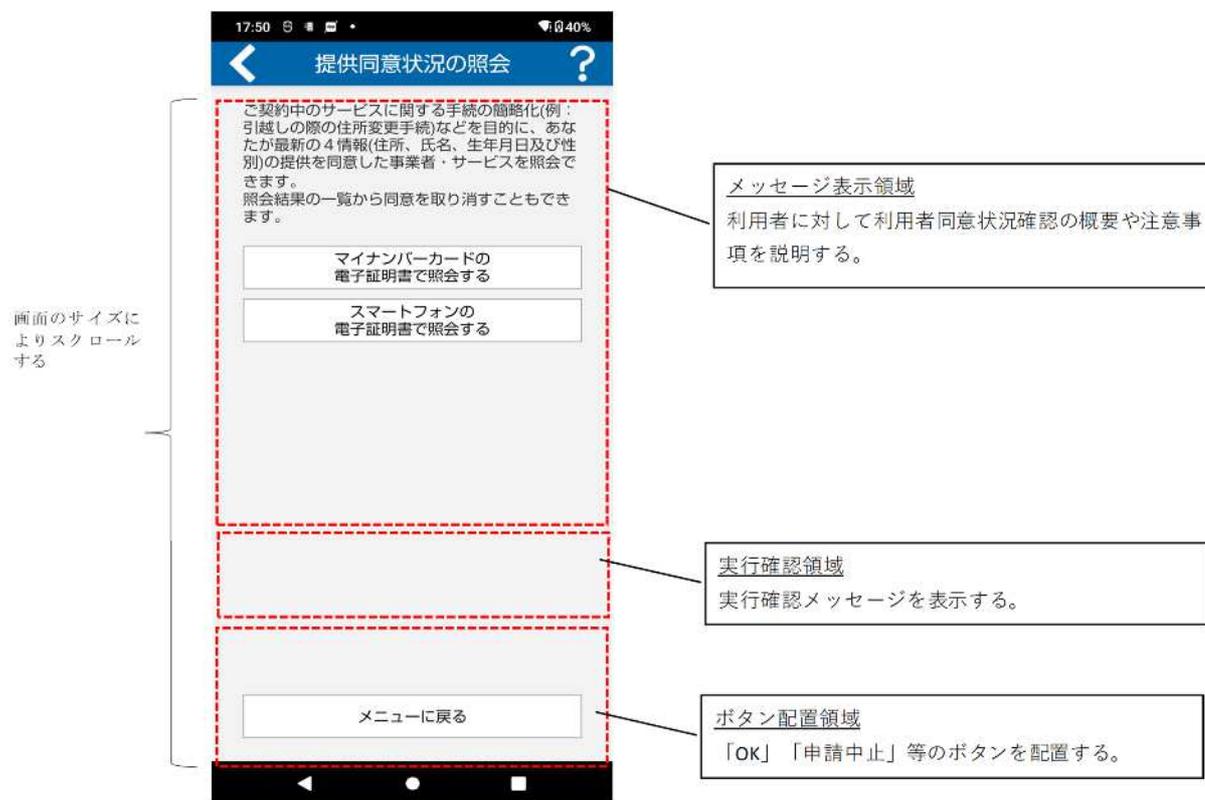


図 4-45 画面共通仕様イメージ

- フォントは、Android に標準搭載されている「モトヤ L マルベリ 3」を使用する。
- フォントサイズは視認性を考慮し「14sp」とする。
- 日付を画面に表示する場合、書式は「YYYY/MM/DD」(時分秒は表示せず)で表示する。

## 利用者同意状況確認 画面遷移



図 4 - 4 6 利用者同意状況確認機能の画面遷移 (利用者同意状況確認)

## 利用者同意取消 画面遷移



図 4-4-7 利用者同意状況確認機能の画面遷移（利用者同意取消）

## 第5章 機能概要 (PC接続編)

### 第1節 メニュー画面表示機能

#### 1 概要

PC接続動作確認機能、PC接続機能の選択ボタンを表示する。

#### 2 機能仕様

「PC接続」を選択することで、以下のボタンを含むPC接続メニュー画面を表示する。

- PC接続の開始ボタン
- PC接続状態の確認ボタン
- ヘルプボタン
- 戻るボタン

#### 3 画面仕様

メニュー画面の「PC接続」ボタンを押下し、PC接続メニュー画面を表示する。



図 5 - 1 PC 接続ボタン



図 5 - 2 PC 接続メニュー画面イメージ

## 第2節 PC 接続動作確認機能

### 1 概要

PC と Android 端末が接続できる設定になっているか確認を行う。

### 2 機能仕様

Android 端末で以下の設定を確認する。

- Bluetooth が有効になっていること
- NFC が有効になっていること

### 3 画面仕様

PC 接続メニュー画面の「PC 接続状態の確認」ボタンを押下することで、動作確認画面を表示する。



図 5 - 3 PC 接続状態の確認ボタン

Android 端末の設定で Bluetooth、NFC の両方が有効の場合は以下の画面を表示する。



図 5 - 4 動作確認結果の画面イメージ(正常動作)

Android 端末の設定で Bluetooth が無効の場合は以下の画面を表示する。



図 5 - 5 動作確認結果画面のイメージ(Bluetooth が無効の場合)

Android 端末の設定で NFC が無効の場合は以下の画面を表示する。



図 5 - 6 動作確認結果画面のイメージ(NFCが無効の場合)

### 第3節 PC接続機能

#### 1 概要

PCとAndroid端末をBluetoothで接続し、ICカードアクセスを行う。

#### 2 機能仕様

PCからBluetoothを経由して、ICカードのコマンドを受け付ける。

ICカードのコマンドはNFCでICカードへ中継する。

前提として、以下が完了していることとする。

- PCとAndroid端末がBluetoothのペアリングが完了していること。
- PC版JPKI利用者ソフトのICカードリーダーライタ設定でBluetooth対応を設定していること。詳細は、「利用者クライアントソフト 機能概要説明書」を参照。

#### 3 画面仕様

(1) Android11.0以前の場合

PC接続メニュー画面の「PC接続の開始」ボタンを押下し、PCとの接続を開始する。



図 5 - 7 PC 接続の開始ボタン

ICカードセット案内画面が表示される。



図 5 - 8 ICカードセット案内画面イメージ

ICカードセット後、PCと接続できる状態の場合は以下の画面が表示される。



図 5 - 9 接続待機中画面イメージ

## (2) Android12以降の場合

PC接続メニュー画面の「PC接続の開始」ボタンを押下し、PCとの接続を開始する。



図 5 - 1 0 PC 接続の開始ボタン

Bluetooth 利用案内画面で「OK」ボタンを押下する。(Bluetooth の利用を一回拒否している場合のみ)

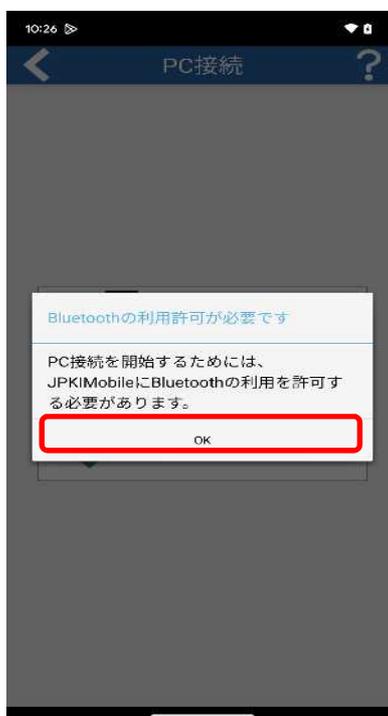


図 5 - 1 1 Bluetooth 利用案内画面イメージ

Bluetooth 利用許可要求画面の「許可」ボタンを押下する。



図 5 - 1 2 Bluetooth 利用許可要求画面イメージ

IC カードセット案内画面が表示される。



図 5 - 1 3 IC カードセット案内画面イメージ

ICカードセット後、PCと接続できる状態の場合は以下の画面が表示される。



図 5 - 1 4 接続待機中画面イメージ

### 補足事項

Bluetooth 利用許可要求画面で「許可しない」ボタンを押下した場合、Bluetooth 利用不可画面が表示される。

「閉じる」ボタンを押下すると PC 接続メニュー画面に戻る。

「設定を開く」ボタンを押下すると JPKIMobile のアプリ情報画面に遷移し、付近のデバイスをアクセスする権限を付与することで PC 接続を開始することが可能となる。

なお、Bluetooth の利用を複数回拒否している場合は完全拒否とみなされ、PC 接続メニュー画面から本画面に直接遷移する。

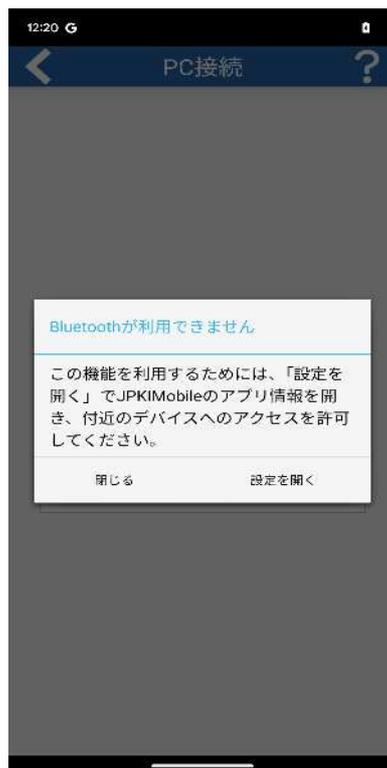


図 5 - 1 5 Bluetooth 利用不可画面イメージ

禁・無断転載

公的個人認証サービス

利用者クライアントソフト

機能概要説明書

(Android 版)

第 1.7 版

(注意事項)

利用者クライアントソフトの著作権は、総務省、地方公共団体情報システム機構が保有しており、国際著作権条約及び日本国の著作権関連法令によって保護されています。

利用者クライアントソフトの利用に当たっては、次に掲げる行為を禁止します。

- (1) 利用者クライアントソフトを電子署名に係る地方公共団体情報システム機構の認証業務に関する法律において制限されている電子証明書の用途で利用すること。
- (2) 利用者クライアントソフトに対し、総務省、地方公共団体情報システム機構に許可なく改造等を行うこと。

総務省、地方公共団体情報システム機構は、利用者が利用者クライアントソフトを利用したことにより発生した利用者の損害及び利用者が第三者に与えた損害について、一切の責任を負いません。

商標については次の通りです。

- (1) Android は、Google LLC の米国およびその他の国における登録商標です。
- (2) その他、記載されている会社名、製品名等は、各社の登録商標または商標です。