

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**

第 4.3 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 16 年 1 月 16 日	新規作成
1.1 版	平成 16 年 10 月 14 日	Windows XP SP2 対応に伴い、表 3 - 1 (5 頁)のプラットフォームを追加
2.0 版	平成 18 年 5 月 2 日	<ul style="list-style-type: none"> ・ 公的個人認証サービス利用者クライアントソフト Ver2.0 のリリースに伴い、動作環境を変更 ・ メニュー画面表示機能、ポータルサイト閲覧機能、電子証明書出力機能、自己の電子証明書の有効性確認機能、自己の電子証明書のオンライン失効申請機能、Java ライブラリ登録機能 を追加 ・ 表 4 - 2 表示項目と証明書領域の対応(利用者証明書)から Windows98/ME に関する記述を削除 ・ 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) から MD5 に関する記述を削除 ・ 電子証明書表示機能に有効性確認ボタンとファイル出力ボタンを配置する旨を追加 ・ 第 6 章 アクセシビリティ対応 を追加 ・ CA 証明書登録機能、CA 証明書取得機能を削除
2.1 版	平成 18 年 7 月 27 日	表 3 - 1 動作環境 JavaVM に JRE5.0 Update7 を追加
2.2 版	平成 18 年 11 月 1 日	<ul style="list-style-type: none"> ・ 第 2 章 ドキュメント体系、第 3 章 第 1 節 動作環境、第 3 章 第 2 節 上位アプリケーションとのインターフェース に MacOS に関する記述を追加 ・ 第 5 章 第 3 節 電子証明書表示機能 4 画面仕様に MacOS のフォントに関する記述を追加 ・ 第 5 章 第 1 3 節 1 概要、第 5 章 第 1 4 節 1 概要、第 5 章 第 1 5 節 1 概要 に MacOS に関する記述を追加 ・ 第 6 章 第 2 節 アクセシビリティ対応範囲 の IC カードリーダー設定機能、パスワード変更機能に文言を追加 ・ 第 7 章 第 2 節 IC カードに対するアクセス制御 に MacOS に関する記述を追加
2.3 版	平成 19 年 4 月 10 日	<ul style="list-style-type: none"> ・ 表 3 - 1 動作環境 を変更 ・ プロキシ設定機能を追加、 ・ メニュー画面を変更、

版数	変更日付	変更内容
2.4 版	平成 19 年 10 月 4 日	<ul style="list-style-type: none"> ・ 表 3 - 1 動作環境 注意書き 6 に Mac OS X 10.4.10, 10.4.9 を追加 ・ 全体 メニュー画面を Ver2.2 のものに変更
2.5 版	平成 20 年 10 月 10 日	<ul style="list-style-type: none"> ・ 表 3 - 1 動作環境を変更 ・ 第 5 章 第 1 5 節 1 MacOS に関する記述を削除 ・ 第 6 章 第 2 節 パスワード変更機能が Windows 版のみであるという記述を削除 ・ 全体 メニュー画面を Ver2.3 のものに変更 ・ エラー! 参照元が見つかりません。メニュー画面から署名付与機能を実行するためには、Java 実行環境が必要であることを追加。画面遷移に「Java 実行環境確認画面」を追加 ・ エラー! 参照元が見つかりません。メニュー画面から署名検証機能を実行するためには、Java 実行環境が必要であることを追加。画面遷移に「Java 実行環境確認画面」を追加 ・ 第 5 章 第 1 1 節 1 Java 実行環境が必要であることを追加 ・ 第 5 章 第 1 1 節 4 画面遷移に「Java 実行環境確認画面」を追加 ・ 第 5 章 第 1 3 節 2 IC リーダライタ設定に「自動検出機能」を追加 ・ 第 5 章 第 1 3 節 3 画面仕様に「自動検出」を追加 ・ 第 5 章 第 1 6 節 1 Java 実行環境が必要であることを追加

版数	変更日付	変更内容
2.6 版	平成 23 年 4 月 1 日	<ul style="list-style-type: none"> ・ 全体 メニュー画面を Ver2.4 のものに変更。 ・ 本文全体(1 章以降) 「JPKI 利用者ソフト」に記載を統一。 ・ 図 2 - 1 ドキュメント体系図に「JavaDoc JPKICryptJNI(64bit)」を追加。 ・ 表 3 - 1 動作環境を表 3 - 1 動作環境(Windows)、表 3 - 2 動作環境(MacOS)、表 3 - 3 動作環境(IC カード)に分割しマトリックス形式の記述に変更。 ・ 表 3 - 1 動作環境(Windows)の OS に WindowsVista ServicePack2, Windows7(32/64 bit)を追加、Web ブラウザに Internet Explorer8.0 を追加。 ・ 表 3 - 2 動作環境(MacOS)の OS に MacOS X 10.6.4 , MacOS X 10.5.6 , MacOS X 10.5.5 を追加、Web ブラウザに Safari 3.2, Safari 5.0 を追加。 ・ エラー! 参照元が見つかりません。エラー! 参照元が見つかりません。 の画面遷移の Java インストールチェックに関する画面を削除。 ・ エラー! 参照元が見つかりません。エラー! 参照元が見つかりません。 の画面遷移の Java インストールチェックに関する画面を削除。 ・ 第 5 章 第 1 1 節 1 概要の Java 実行環境が必要な環境を MacOS 版のみに変更。 ・ 第 5 章 第 1 1 節 4 画面仕様の画面遷移の Java インストールチェックに関する画面を削除。 ・ 第 5 章 第 1 4 節 1 概要および第 5 章 第 1 4 節 2 機能仕様の JPKI/BCA の自己署名証明書登録は、MacOS 版のみに変更。 ・ 第 5 章 第 1 4 節 3 画面仕様「Java ライブラリ登録画面イメージ」、「JPKI/BCA の自己署名証明書登録画面イメージ」を削除。 ・ 第 5 章 第 1 6 節 1 Java 実行環境が必要な環境を MacOS 版のみに変更。 ・ 第 5 章 第 1 6 節 2 機能仕様を Windows 版と MacOS 版に分割。 ・ 第 5 章 第 1 6 節 3 画面仕様の画面遷移を Windows 版と MacOS 版に分割。 ・ 第 5 章 第 1 7 節 自動更新機能を追加。 ・ 第 7 章 第 1 節 JPKI 利用者ソフトのインストール機能に 32bit 環境/64bit 環境に関する記述を追加。

版数	変更日付	変更内容
2.7 版	平成 25 年 12 月 1 日	<ul style="list-style-type: none"> ・全体 メニュー画面を Ver2.5 のものに変更。 ・第 3 章 第 1 節 表 3 - 1 動作環境の Windows 版、Mac 版の利用者ソフトバージョンを 2.5 に変更。 ・表 3 - 1 動作環境(Windows)の OS より Windows2000 を削除、Windows 7(32/64 bit)ServicePack1, Windows8(32/64 bit), Windows8.1(32/64 bit)を追加、Web ブラウザに Internet Explorer9.0, 10.0, 11.0 を追加。 ・表 3 - 2 動作環境(MacOS)の OS より MacOS X 10.4.X ,MacOS X 10.5.X , MacOS X 10.6.X を削除、MacOS X 10.7.5, OS X 10.8.4 を追加、Web ブラウザに Safari 6.0 を追加。 ・第 5 章 第 8 節 2 機能仕様 (2)署名アルゴリズムに「SHA256WithEncryption」を追加。 ・第 5 章 第 1 4 節 1 (2)Java 実行環境のキーストアに JPKI/BCA の自己署名証明書の登録を削除。 ・第 5 章 第 1 4 節 2 (4)BCA 自己署名証明書のキーストアに登録を削除。 ・第 6 章 第 1 節 (2)インストール時の公的個人認証サービスブリッジ証明書の登録を削除。
3.0 版	平成 26 年 4 月 1 日	<ul style="list-style-type: none"> ・全体 「地方公共団体情報システム機構」への事業承継により、組織名称を変更 ・全体 「公的個人認証サービス共通基盤事業運用会議」への事業承継により、「公的個人認証サービス都道府県協議会」の組織名称を変更する。

版数	変更日付	変更内容
3.1 版	平成 26 年 7 月 1 日	<ul style="list-style-type: none"> ・全体 メニュー画面を Ver2.6 のものに変更。 ・第 3 章 第 1 節 動作環境の Windows 版、Mac 版の利用者ソフトウェアバージョンを 2.6 に変更。 ・表 3 - 1 動作環境(Windows)から Windows XP/ Windows 8(32/64bit)を削除。Windows8.1 を Windows8.1 update に変更。Windows7(32/64bit)の Web ブラウザを IE11.0 に変更。 ・表 3 - 2 動作環境(MacOS) OS X v10.7.5 の Web ブラウザを Safari6.1 に変更。OS X v10.8.4 を削除。OS X v10.8.5、OS X v10.9.3 を追加。 ・第 4 章 第 6 節 2 (2)使用するハッシュ関数に SHA-256 を追加 ・第 4 章 第 6 節 2 (3)署名アルゴリズムに「SHA256WithEncryption」を追加し、カード AP ライブラリのみ対応であることの注釈を追加 ・エラー! 参照元が見つかりません。メニュー画面の「電子署名の付与/検証」機能については SHA1 のみに対応していることの注釈を追加
4.0 版	平成 27 年 6 月 30 日	<p>番号制度対応に伴い、以下を修正。</p> <ul style="list-style-type: none"> ・第 1 章 第 1 節に用語の定義を追加。 ・第 2 章のドキュメント体系を修正。 ・第 3 章 第 1 節の動作環境を修正。 ・機能概要として第 4 章 機能概要（住基カード編）、第 5 章 機能概要（個人番号カード編）を記載。 ・第 1 章、第 6 章、第 7 章に電子証明書の更新通知機能について記述を追加。 ・第 3 章 第 2 節、第 5 章 第 6 節、第 5 章 第 8 節、第 7 章 第 2 節の「CSSM および Keychain Service」についての記述を修正。
4.0.1 版	平成 28 年 10 月 26 日	<ul style="list-style-type: none"> ・第 3 章システム概要 第 1 節動作環境 更新プログラムに係る注釈 3、4 の追加 ・第 7 章 第 2 節 IC カードに対するアクセス制御 MacOS 版（個人番号カード用）に関する記述を追加 ・文末 注意事項の利用用途の文言修正 その他、図の整形及び誤記等の文言修正

版数	変更日付	変更内容
4.1 版	平成 28 年 11 月 30 日	<p>PC 接続機能追加に伴い、以下を修正</p> <ul style="list-style-type: none"> ・ 第 1 節の「用語の定義」に以下を追加。 <ul style="list-style-type: none"> ➤ PC/SC ➤ IC カードリーダーライタ ➤ 挿入 ➤ NFC ➤ Bluetooth ・ 第 2 章 ドキュメント体系図に Android 版を追加。 ・ 第 3 章 第 1 節の表 3-1 および表 3-2 に PC 接続機能を追加。 ・ 第 3 章 第 1 節の表 3-1 に Windows 10(32/64bit)を追加。 ・ 第 3 章 第 1 節の表 3-3 動作環境(共通)を表 3-3 動作環境(IC カード)、1.PC/SC 対応 IC カードリーダーライタ、2.Android 端末に分割。 ・ 第 3 章 第 3 節「PC 接続機能について」を追加。 ・ 第 5 章 第 1 2 節の動作仕様を修正。 ・ 第 5 章 第 1 3 節の機能仕様および画面仕様を修正。

版数	変更日付	変更内容
4.2 版	平成 29 年 7 月 31 日	<p>Java9 対応に伴い、以下を修正。</p> <ul style="list-style-type: none"> ・ 第 2 章 ドキュメント体系図を改訂。 ・ 第 3 章 第 1 節の表 3-1 から Windows Vista(32bit)(Service Pack 2)、Windows8(32bit)および Windows8(64bit)を削除。 ・ 第 3 章 第 1 節の表 3-2 から OS X v10.8(64bit)および OS X v10.9(64bit)を削除、OS X v10.11(64bit)および macOS v10.12(64bit)を追加。 ・ 第 3 章 第 1 節の表 3-5 の【PC 接続の場合】に Android 6.0.1、7.0 を追加。 ・ 第 3 章 第 1 節の表 3-5 の【Android 単体で利用する場合】に Android 6.0.1、7.0 を追加。 ・ 第 3 章 第 1 節の表 3-1 および表 3-2 に JRE9.0 を追加。 ・ 第 5 章 第 1 4 節 Java ライブラリ登録機能の記載を JRE9.0 向けに修正。 ・ 第 5 章 第 1 4 節に、MacOS 版の画像を追加。 ・ 第 5 章 第 1 5 節に、「パスワード変更」を起動した際の説明文言を追加。 ・ 第 5 章 第 1 6 節に、「JRE8u111 以降または JRE9 の場合は、プロキシ機能を使用できない」ことを記述。 ・ 第 5 章 第 1 6 節に、MacOS 版でプロキシを使用する場合の JRE バージョンについて記載を追加。

版数	変更日付	変更内容
4.3 版	令和元年 5 月 1 日	<p>新元号対応 / 閉局対応に伴い、以下を修正。</p> <ul style="list-style-type: none"> ・ 第 3 章 第 1 節 動作環境の利用者ソフトウェアバージョンを 3.3 に変更。 ・ 第 3 章 第 1 節 表 3-2 の OS X v10.11 を削除し、macOS v10.13 を追加。 ・ 第 3 章 第 1 節 表 3-5 の【PC 接続の場合】【Android 単体で利用する場合】に Android 8.0 を追加。 ・ 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。 ・ 第 5 章 第 3 節 の表 5-2 における 2 生年月日の設定ルールに新元号を追加。 ・ 第 5 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。 <p>旧署名用認証局の閉局対応に伴い、以下を修正。</p> <ul style="list-style-type: none"> ・ 全体 メニュー画面を「電子署名の付与 / 検証(V)」を削除した Ver3.3 のものに変更。 ・ 第 4 章 第 6 節 から電子署名作成機能をメニュー画面から利用する場合の記載を削除。 ・ 第 4 章 第 8 節 から電子署名検証機能をメニュー画面から利用する場合の記載を削除。 ・ 第 4 章 第 8 節 図 4-19、20 における「電子署名作成機能」を「電子署名検証機能」に修正。 ・ 第 5 章 第 1 節 のメニュー画面表示機能から電子署名付与機能、電子署名検証機能の記載を削除。 ・ 第 5 章 第 6 節 から電子署名作成機能をメニュー画面から利用できない旨の記載を削除。 ・ 第 5 章 第 8 節 から電子署名検証機能をメニュー画面から利用できない旨の記載を削除。 ・ 第 5 章 第 8 節 図 5-25、26 における「電子署名作成機能」を「電子署名検証機能」に修正。 ・ 第 6 章 第 2 節 から電子署名検証機能を削除。 <p>旧氏対応に伴い、以下を修正。</p> <ul style="list-style-type: none"> ・ 第 5 章 第 3 節の図 5-11 および表 5-2 に旧氏に関する記述を追加。 ・ 第 5 章 第 5 節の機能仕様に旧氏に関する記述を追加。

- 目次 -

第1章 はじめに	1
第1節 用語の定義.....	2
第2章 ドキュメント体系	3
第3章 システム概要	5
第1節 動作環境.....	5
第2節 上位アプリケーションとのインターフェース.....	9
第3節 PC 接続機能について.....	9
第4章 機能概要（住基カード編）	10
第1節 メニュー画面表示機能	10
第2節 ポータルサイト閲覧機能.....	10
第3節 電子証明書表示機能	10
第4節 電子証明書出力機能	25
第5節 基本4情報取得機能.....	25
第6節 電子署名作成機能.....	25
第7節 電子証明書取得機能	27
第8節 電子署名検証機能.....	28
第9節 官職証明書検証機能	30
第10節 自分の電子証明書の有効性確認機能.....	33
第11節 自分の電子証明書のオンライン失効申請機能	33
第12節 ソフトウェア動作確認機能	37
第13節 IC カードリーダーライター設定機能.....	37
第14節 JAVA ライブラリ登録機能.....	37
第15節 パスワード変更機能	37
第16節 プロキシ設定機能	38
第17節 自動更新機能	38
第18節 電子証明書の更新通知機能	38
第5章 機能概要（個人番号カード編）	39
第1節 メニュー画面表示機能	39
第2節 ポータルサイト閲覧機能.....	41
第3節 電子証明書表示機能	42
第4節 電子証明書出力機能	61
第5節 基本4情報取得機能.....	63
第6節 電子署名作成機能.....	64
第7節 電子証明書取得機能	66
第8節 電子署名検証機能.....	67
第9節 官職証明書検証機能	69
第10節 自分の電子証明書の有効性確認機能.....	72
第11節 自分の電子証明書のオンライン失効申請機能	75

第12節 ソフトウェア動作確認機能	82
第13節 ICカードリーダーライター設定機能.....	83
第14節 JAVAライブラリ登録機能.....	85
第15節 パスワード変更機能	87
第16節 プロキシ設定機能	93
第17節 自動更新機能	94
第18節 電子証明書の更新通知機能	97
第6章 アクセシビリティ対応.....	100
第1節 アクセシビリティ対応項目	100
第2節 アクセシビリティ対応範囲	102
第7章 その他	103
第1節 JPKI利用者ソフトのインストール機能	103
第2節 ICカードに対するアクセス制御	103

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、利用者が自宅のパソコン等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
- IC カードリーダライタ設定機能
- Java ライブラリ登録機能
- パスワード変更機能
- プロキシ設定機能
- 自動更新機能
- 電子証明書の更新通知機能

以降、本書では 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 ・住基カード ・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て、発行されるデータをいう。データは、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 具体的には以下の電子証明書を指す ・住基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 第 4 章に記述された利用者証明書は住基カードに格納された署名用電子証明書のみを指す。
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指す。 ・住基カードに格納された都道府県知事の自己署名証明書 ・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 第 4 章に記述された認証局の自己署名証明書は住基カードに格納された都道府県知事の自己署名証明書のみを指す。
6	PC/SC	Personal Computer/Smart Card の略。
7	IC カードリーダーライター	以下の機器を指す総称 ・PC/SC 対応 IC カードリーダーライター ・Android 端末
8	挿入	IC カードリーダーライターが IC カードを読み込める状態にすること。具体的には以下の状態にすることを指す。 ・PC/SC 対応 IC カードリーダーライターに IC カードをセットすること ・Android 端末に IC カードをセットすること
9	NFC	Near Field Communication (近距離無線通信)の略。
10	Bluetooth	機器間の近距離無線通信 IEEE 802.15.1 の規格名称。

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。

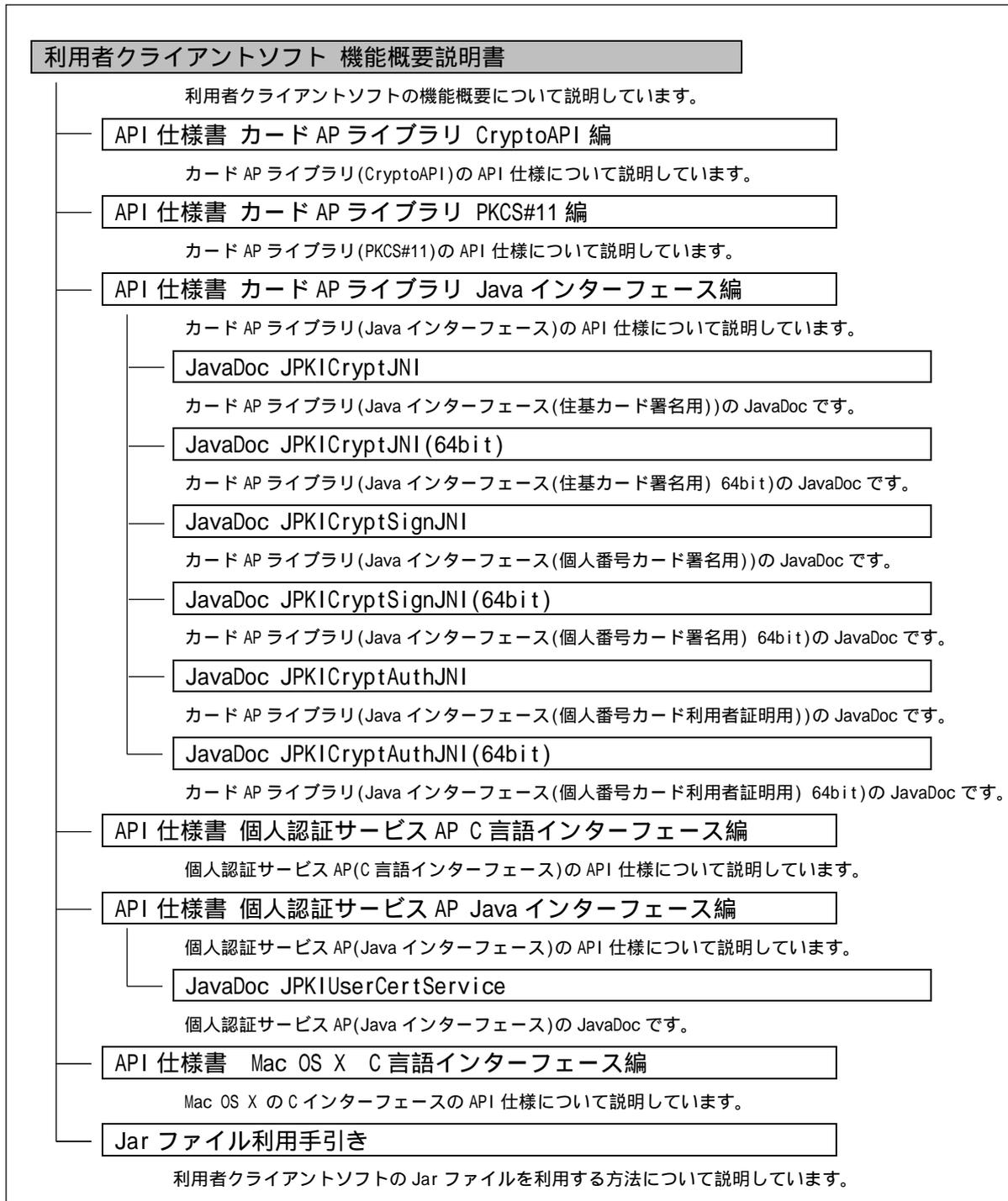


図 2-1 ドキュメント体系図(PC版)

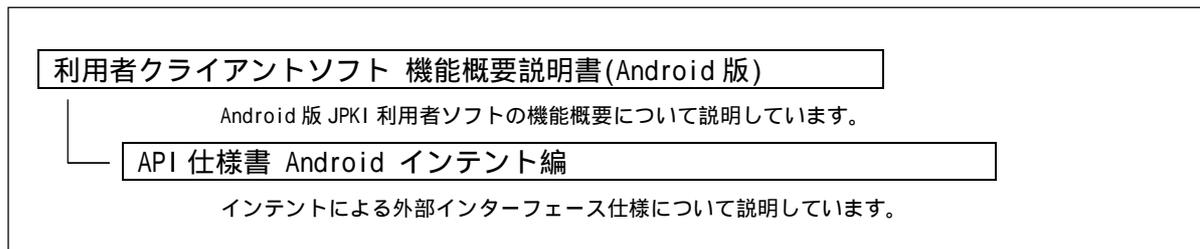


図 2-2 ドキュメント体系図(Android 版)

第3章 システム概要

第1節 動作環境

Windows 版 JPKI 利用者ソフト Ver3.3 の動作環境は以下の通りとする。

表 3 - 1 動作環境(Windows)

OS(1)	Web ブラウザ (1, 2)	JavaVM(1, 6)		PC 接続機能対応可否 (5)
		JRE8.0	JRE9.0	
Windows 7(32bit) (Service Pack 1) (3)	IE11.0		×	
Windows 7(64bit) (Service Pack 1) (3)	IE11.0			
Windows 8.1 update (32bit) (4)	IE11.0		×	
Windows 8.1 update (64bit) (4)	IE11.0			
Windows 10(32bit)	IE11.0		×	
Windows 10(64bit)	IE11.0			

1 本仕様書で定めるバージョンの開発時点の環境。最新の動作環境の情報は、JPKI ポータルサイトに掲載するものとする。

2 プラットフォームがWindowsの場合、暗号機能等の利用のために Internet Explorer が必要。

3 Windows の更新プログラム(KB3033929)をインストールする必要がある。

(なお、更新プログラム(KB3033929)のインストール前に、

関連する更新プログラム(KB3035131)が必要になる為、注意すること。)

4 Windows の更新プログラム(KB2919355)をインストールする必要がある。

5 PC 接続機能については『第3章 第3節 PC 接続機能について』を参照。

6 JRE9.0 の 32bit 版は Oracle 社より提供されていないため非対応。

MacOS 版 JPKI 利用者ソフト Ver3.3 の動作環境は以下の通りとする。

表 3 - 2 動作環境(MacOS)

OS(1, 2)	Web ブラウザ(1)	JavaVM(1)		PC 接続機能対応可否 (3)
		JRE8.0	JRE9.0	
macOS v10.12 (64bit)	Safari 10			×
macOS v10.13 (64bit)	Safari 11			×

- 1 本仕様書で定めるバージョンの開発時点の環境。最新の動作環境の情報は、JPKI ポータルサイトに掲載するものとする。
- 2 住基カードを利用する場合の動作前提条件として、Mac OS Forge が提供する「Smart Card Services」をそれぞれの OS に合ったものをダウンロードし、インストールする必要がある。
- 3 PC 接続機能については「第3章 第3節 PC 接続機能について」を参照。

IC カードの動作環境は以下の通りとする。

表 3 - 3 動作環境(ICカード)

項目	条件
IC カード	住基カードまたは個人番号カードであること。 PC 接続機能を使用する場合は個人番号カードのみ対応。

1 PC/SC 対応 IC カードリーダーライター

PC/SC 対応 IC カードリーダーライターの動作環境は以下の通りとする。

表 3-4 動作環境(PC/SC 対応 IC カードリーダーライター)

項目	条件
PC/SC 対応 IC カードリーダーライター	<p>以下の条件を満たす PC/SC 対応 IC カードリーダーライターとする。(「個人番号カード対応適合性検証済み IC カードリーダーライター一覧」「住基カード対応適合性検証済み PC/SC 対応 IC カードリーダーライター一覧」(1)を参照のこと。)</p> <ul style="list-style-type: none"> ・ IC カードのインターフェース(非接触型、接触非接触両対応型)に対応していること。 ・ PC/SC 対応 IC カードリーダーライターであること。 ・ USB など、パソコンに接続するためのインターフェースを有すること。 ・ PC/SC 対応 IC カードリーダーライターと通信するためのドライバソフトウェアが提供されていること。 ・ IC カードの搬送方式が手動挿入/手動排出タイプまたは自動挿入/自動排出タイプであること。 ・ IC カードを挿入するスロットの数は1つとし、1度に挿入できる IC カードは1枚であること。

1 最新の「個人番号カード対応適合性検証済み IC カードリーダーライター一覧」「住基カード対応適合性検証済み IC カードリーダーライター一覧」の情報は、JPKI ポータルサイトに掲載するものとする。

2 Android 端末

Android 端末の動作環境は以下の通りとする。

表 3 - 5 動作環境(Android 端末)

項目	条件
Android 端末	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」()を参照のこと。) ・【PC 接続の場合】Android 4.3、5.1、6.0.1、7.0 または 8.0 を搭載し ていること。 ・【Android 単体で利用する場合】Android 5.1、6.0.1、7.0 または 8.0 を搭載していること。 ・Bluetooth 4.0 を搭載していること。 ・ISO/IEC 14443 Type B に対応している NFC を搭載していること。

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。

第 2 節 上位アプリケーションとのインターフェース

上位アプリケーションの実装形態としては、以下のパターンが想定される。

- ・ クライアントアプリケーション（C 言語等で開発）
- ・ クライアントアプリケーション（Java 言語で開発）
- ・ Web アプリケーション（Java アプレット）

上記のパターンに対応するため、以下の Application Program Interface(以下、API)を提供する。

- ・ C 言語インターフェース
 - ◇ CryptoAPI 2.0
 - ◇ PKCS#11 Ver2.2
 - ◇ CSSM(CDSA Ver2.0 準拠)および Keychain Service
- ・ Java 言語インターフェース
 - ◇ Java Native Interface (C 言語インターフェースをラッピング)

プラットフォームに対する各インターフェースの対応は以下の通りである。

表 3-6 インターフェースの対応

API 種別		OS 種別	
		Windows	MacOS
C	CryptoAPI	対応	
	PKCS#11	対応	対応
	CSSM および Keychain Service		
Java	Java Native Interface	対応	対応

住基カードのみ対応。個人番号カードは非対応。

本ソフトウェアでは、上記のインターフェース群のうち、次章以降の機能を実現するインターフェースのみをサポートする。

なお、「証明書取得機能」「電子署名生成機能」「電子署名検証機能」を実現する API として、CryptoAPI、PKCS#11、Java インターフェースがあり、これらをカード AP ライブラリと呼ぶ。

「証明書表示機能」「基本 4 情報取得機能」「官職証明書検証機能」「自己の電子証明書の有効性確認機能」「IC カード種別取得機能」を実現する API として、C 言語インターフェースと Java インターフェースがあり、これらを個人認証サービス AP と呼ぶ。

各 API の詳細については、それぞれの API 仕様書を参照のこと。

第 3 節 PC 接続機能について

PC 接続機能とは、PC が Android 端末の NFC と Bluetooth を使用し、IC カードにアクセスする機能。住基カードの場合、本機能は提供しない。

詳細は「利用者クライアントソフト 機能概要説明書(Android 版) 第 5 章 第 3 節 PC 接続機能」を参照。

第 4 章 機能概要（住基カード編）

第 1 節 メニュー画面表示機能

「第 5 章 機能概要（個人番号カード編）」「第 1 節 メニュー画面表示機能」を参照。

第 2 節 ポータルサイト閲覧機能

「第 5 章 機能概要（個人番号カード編）」「第 2 節 ポータルサイト閲覧機能」を参照。

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都道府県知事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 API 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利用者証明書
- ◇ IC カードに格納された都道府県知事の自己署名証明書

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) 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
- (5) GUI 画面に都道府県知事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
- (6) 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(シーケンス)

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。

- ◇ 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

本機能を使用した、それぞれの証明書表示シーケンスを図 4-1、図 4-2 に示す。

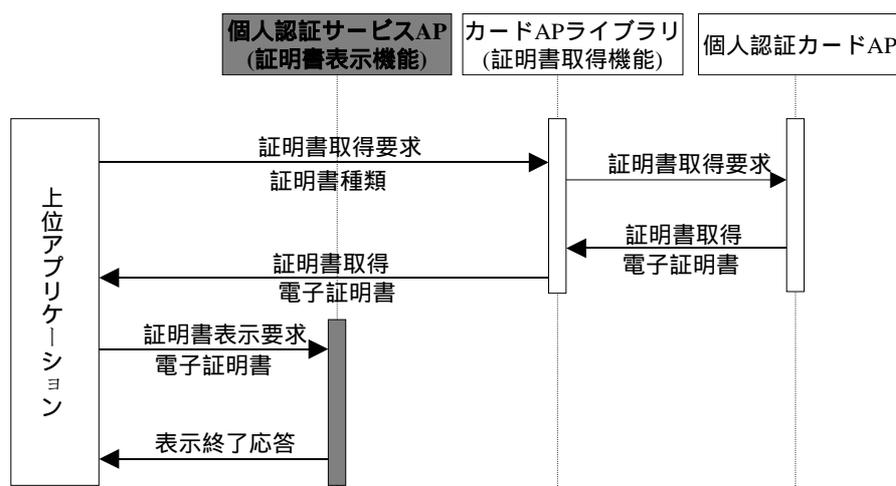


図 4-1 ICカード内の電子証明書を表示する場合

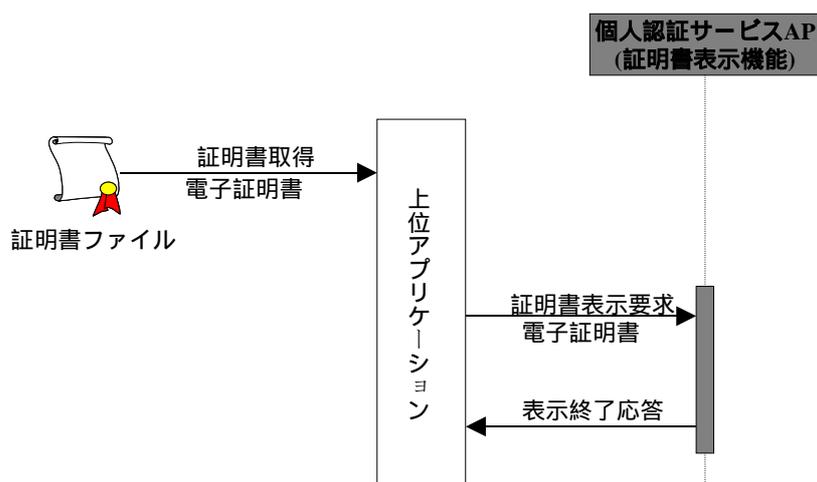


図 4-2 ファイルから電子証明書を表示する場合

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。

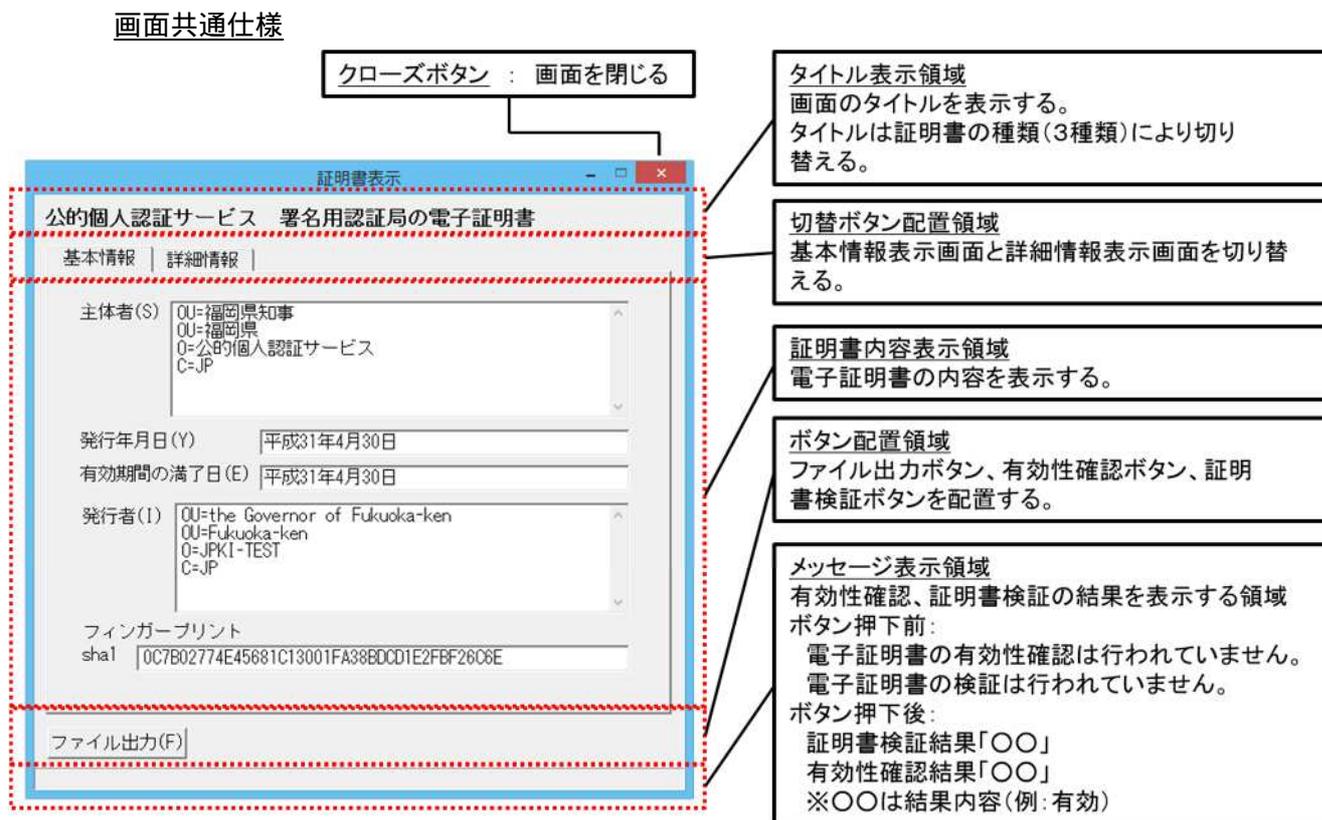


図 4-3 画面共通仕様イメージ

- 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。
Windows 版 : Windows に標準搭載されている「MS ゴシック」を使用する。フォントサイズは「12pt」とする。
MacOS 版 : Java に標準搭載されている「monospaced」を使用する。フォントサイズは「15pt」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 の通り。

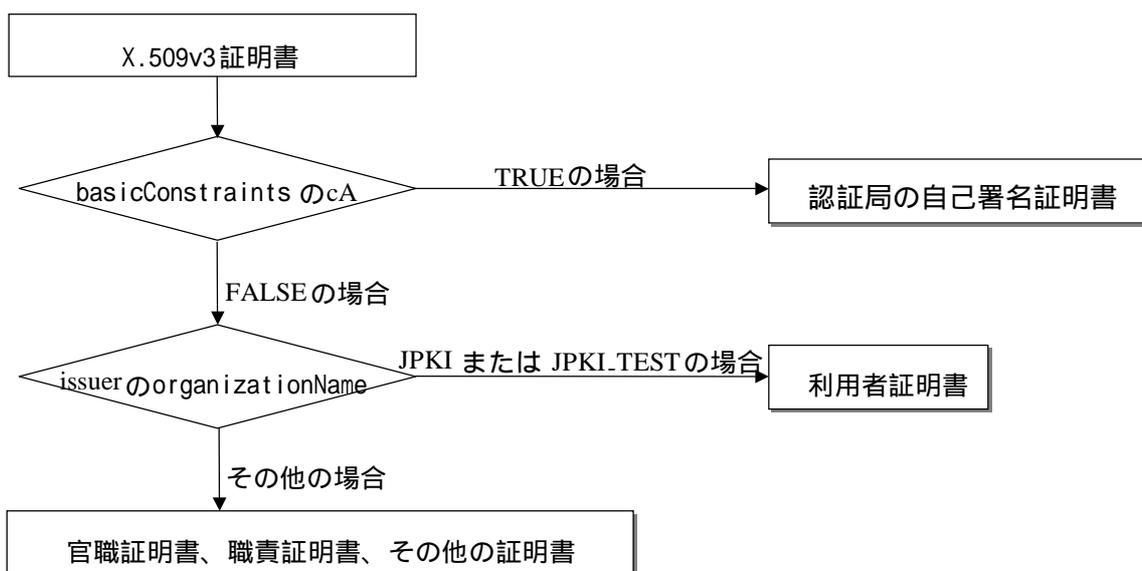


図 4-4 電子証明書分類処理フロー

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」ボタンを押下することで、ICカードに格納されている都道府県知事の自己署名証明書を表示する。

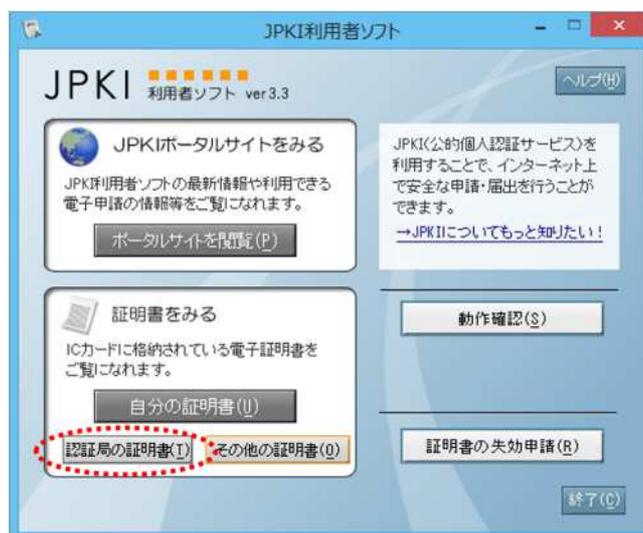
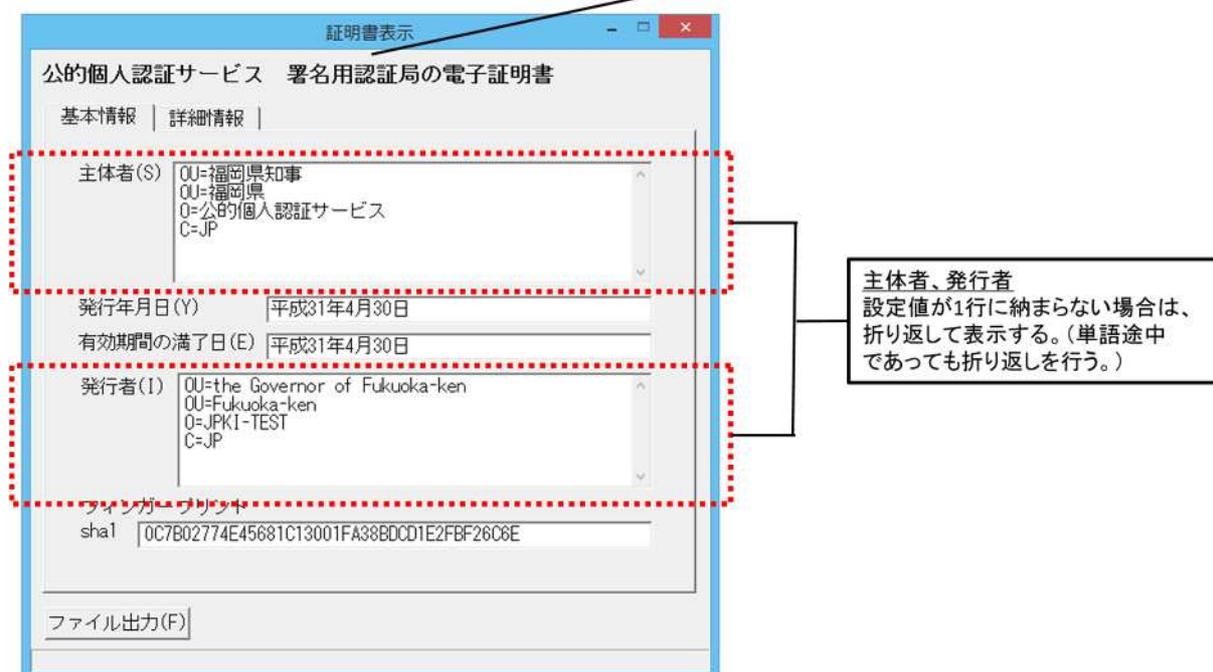


図 4-5 電子証明書表示ボタン(認証局の自己署名証明書)

タイトル表示領域
「公的個人認証サービス 署名用認証局の電子証明書」とする。



例)都道府県知事の自己証明書

図 4-6 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 例) 都道府県知事の自己署名証明書の場合	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) 都道府県知事の自己署名証明書の場合	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	-	-	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」を使用する。

利用者証明書

メニュー画面の「自分の証明書」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。

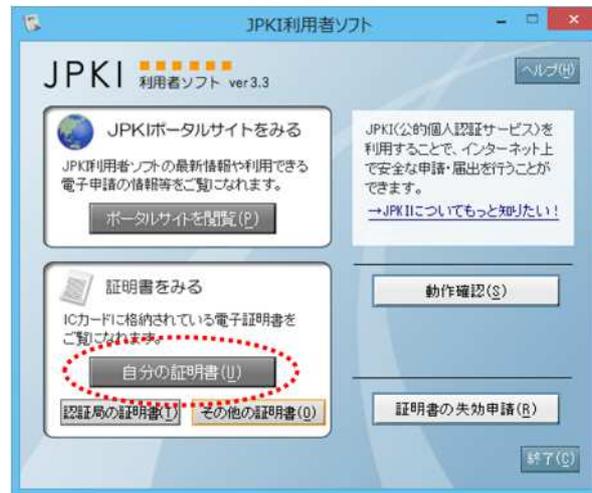


図 4 - 7 電子証明書表示ボタン(利用者証明書)

タイトル表示領域
「公的個人認証サービス 利用者の署名用電子証明書」とする。

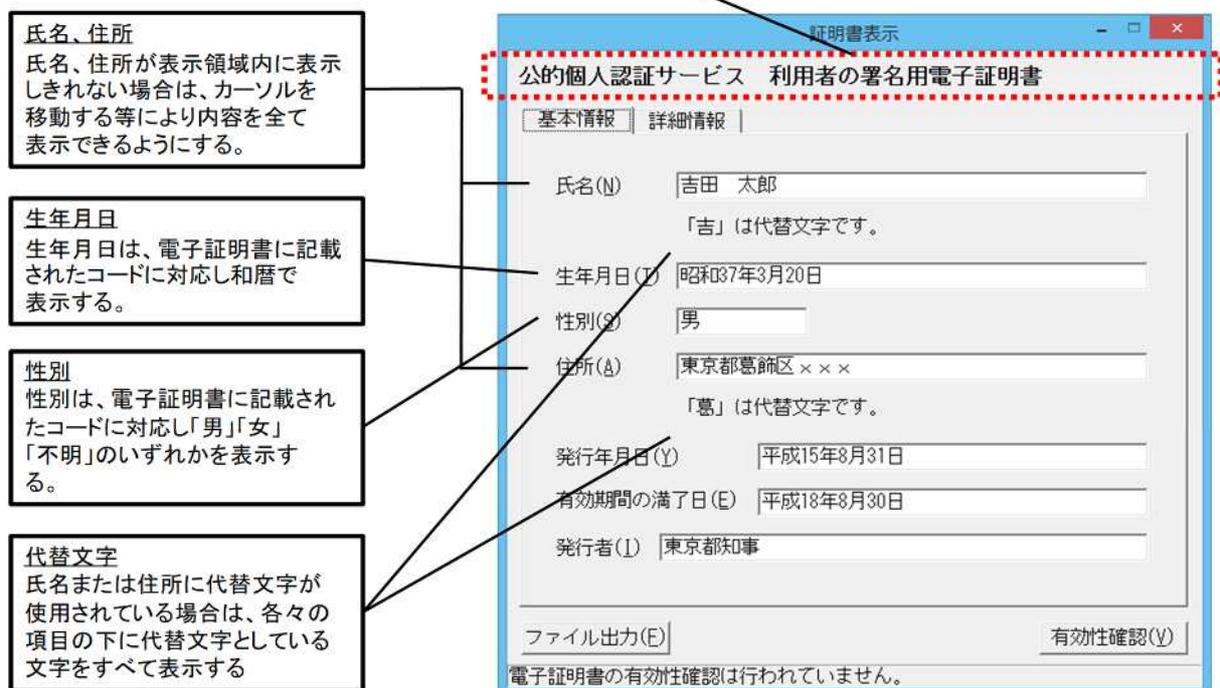


図 4 - 8 基本画面イメージ(利用者証明書)

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。
2	代替文字の使用(氏名)		substituteCharacterOf-CommonName ¹	<ul style="list-style-type: none"> ・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 ²	設定値を和暦に変換して表示。
4	性別		gender ³	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 ¹	<ul style="list-style-type: none"> ・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)

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」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。

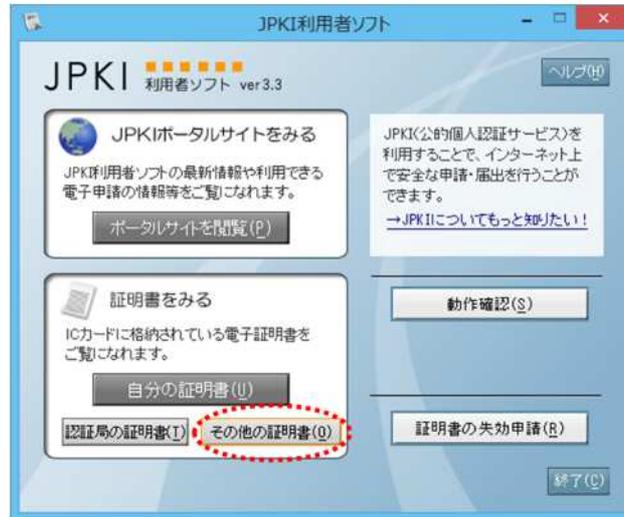


図 4 - 9 電子証明書表示ボタン(官職証明書、職責証明書、その他の証明書)

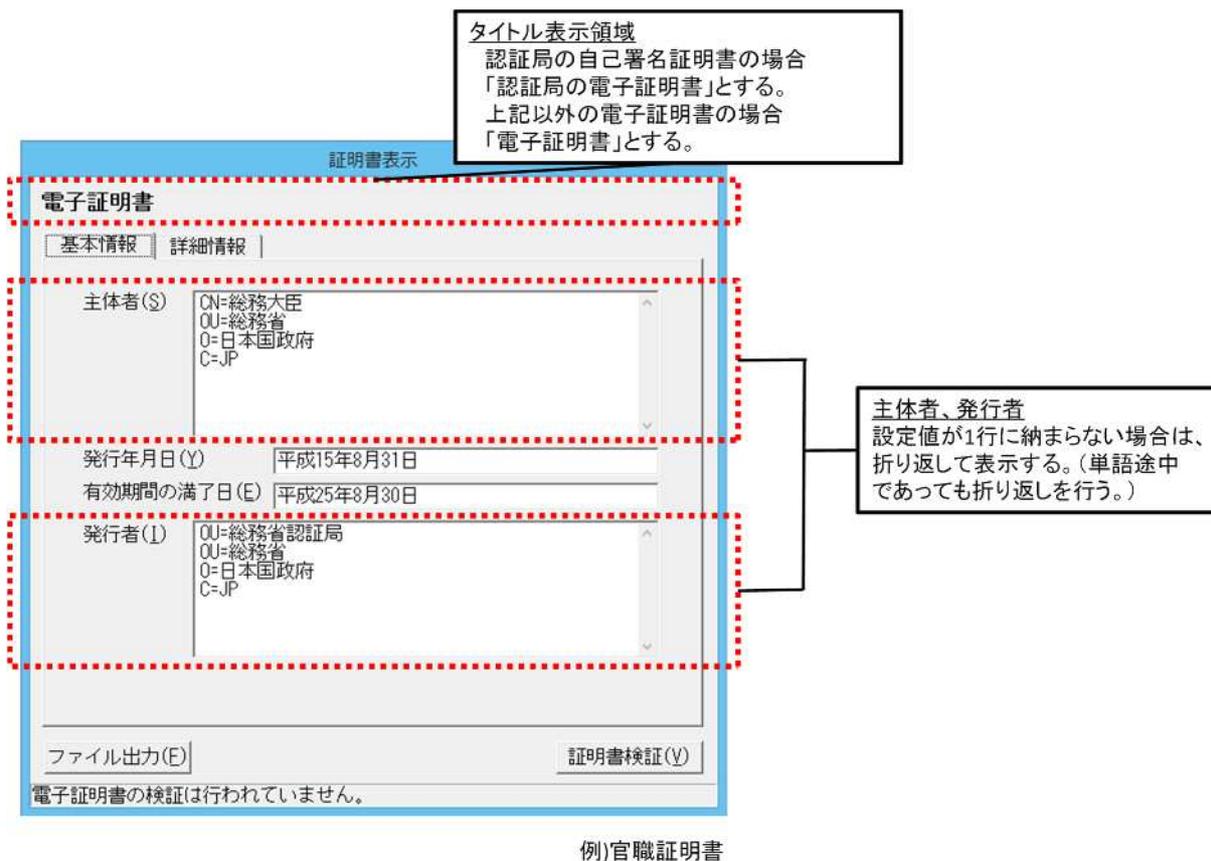


図 4 - 10 基本画面イメージ(官職証明書、職責証明書、その他の証明書)

表 4-3 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。

証明書表示
 公的個人認証サービス 利用者の署名用電子証明書

基本情報 | 詳細情報

項目名	値
バージョン	V3
シリアル番号	030D45
署名アルゴリズム	Sha-256WithRSAEncryp...
発行者	Japan Agency for Loc...
発行年月日	2014年7月17日00時00分...
有効期間の満了日	2019年7月16日23時59...
発行申請送信時刻	20160101101018

20160101101018

フィンガープリント
 sha256 | CD2C6C4E42CCE239965D2BEE129B46B770F13C8264758F8D3E41B0
 | C48ED3E84C

ファイル出力(F) | 有効性確認(V)

電子証明書の有効性確認は行われていません。

タイトル表示領域
 基本画面と同じタイトルを表示する。

項目名
 項目名を日本語で表示する認識できない場合は、設定値をそのまま表示する。

設定値の簡易表記
 設定値の簡易表記を表示する。認識できない場合は、設定値をそのまま表示する。

設定値の詳細表記
 選択した項目の設定値を表示する

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する。ハッシュ関数は「sha1」または「sha256」を使用する。

図 4 - 1 1 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。

- ◇ 項目名表示欄、簡易表記欄、詳細表記欄の各表示項目は、証明書プロフィー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、簡易表記と詳細表記で表記ルールが異なる項目を以下に示す。

< 簡易表記 >

証明書基本領域

- ◇ 発行者(issuer)と主体者(subject)については、識別名(DN: Distinguished Name)の属性毎にカンマ区切りで表示する。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「発行申請送信時刻」と「受付端末識別記号」の2つに分けて表示する。(図 4-12 参照)
- ◇ 主体者公開鍵情報(subjectPublicKeyInfo)については、暗号アルゴリズムと鍵長を表示する。表記方式は「(algorithm の OID に対応する値)+(鍵長)bits」

証明書拡張領域

- ◇ 最上位項目以下の情報を項目毎にカンマ区切りで表示する。

< 詳細表記 >

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、CN のみを「発行申請送信時刻」と「受付端末識別記号」の2つに分けて表示する。(図 4-12 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。

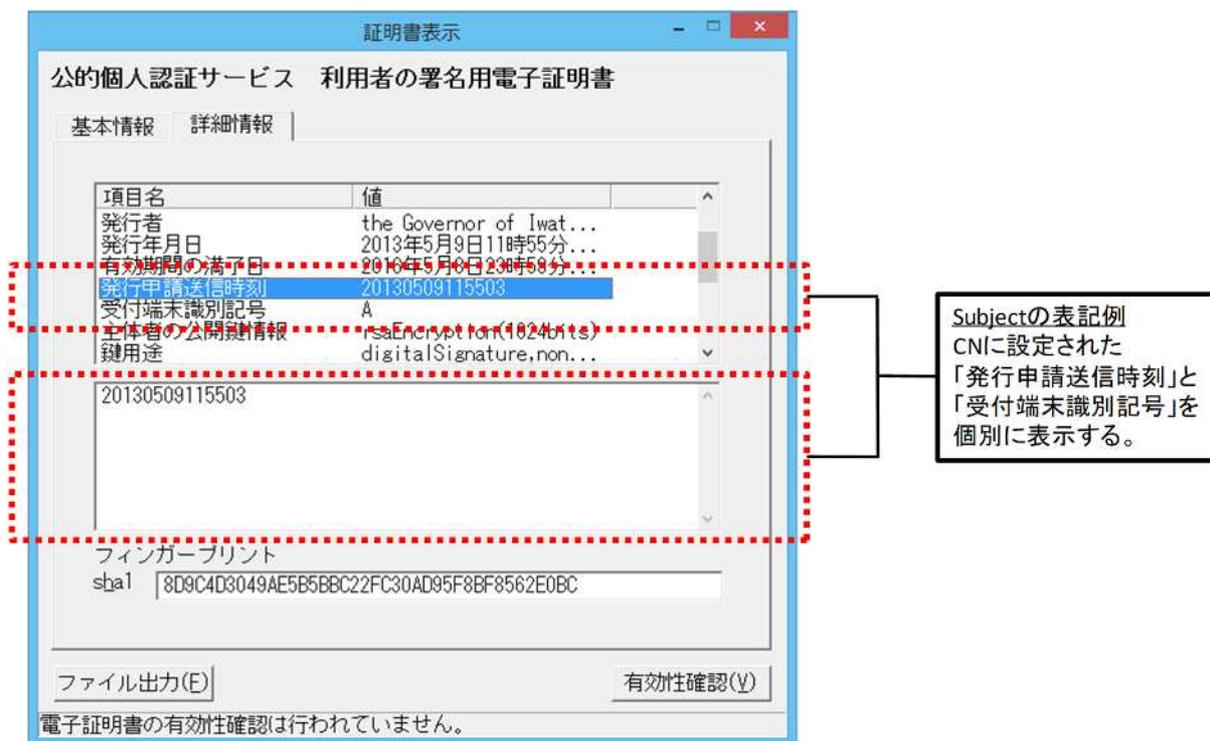


図 4 - 1 2 詳細画面イメージ(利用者証明書)

第 4 節 電子証明書出力機能

「第 5 章 機能概要 (個人番号カード編)」「第 4 節 電子証明書出力機能」を参照。
住基カードの場合は、出力対象とする公的個人認証サービスの電子証明書は以下の通り。

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
- ◇ IC カードに格納された都道府県知事の自己署名証明書

公的個人認証サービス以外の電子証明書については、「第 5 章 機能概要 (個人番号カード編)」「第 4 節 電子証明書出力機能」の通りとする。

第 5 節 基本 4 情報取得機能

「第 5 章 機能概要 (個人番号カード編)」「第 5 節 基本 4 情報取得機能」を参照。

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。

以下では、カード AP ライブラリからの本機能の利用方法を説明する。

2 機能仕様

(1) 本機能は以下のカード AP ライブラリで提供する。

- CryptoAPI
- PKCS#11
- CSSM および Keychain Service
- Java Native Interface

(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。
- 署名対象データの場合は、受け取った署名対象データからハッシュ値を計算して IC カードに引き渡す。
- 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。

3 電子署名作成手順(シーケンス)

本機能を使用した、電子署名作成シーケンスを図 4-13、図 4-14 に示す。

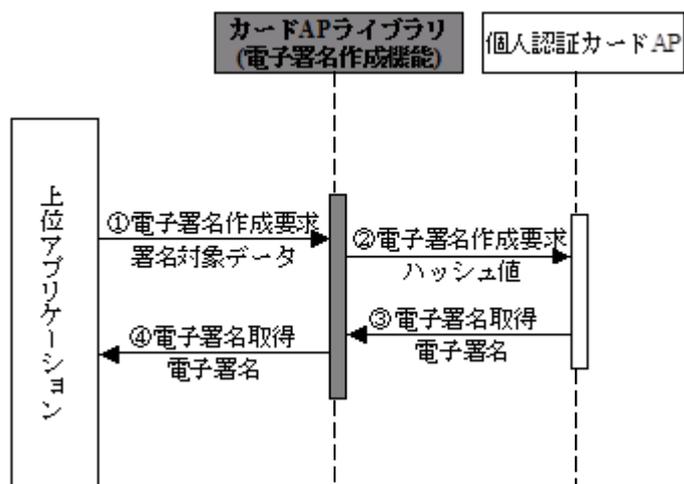


図 4-13 署名対象データからの電子署名作成

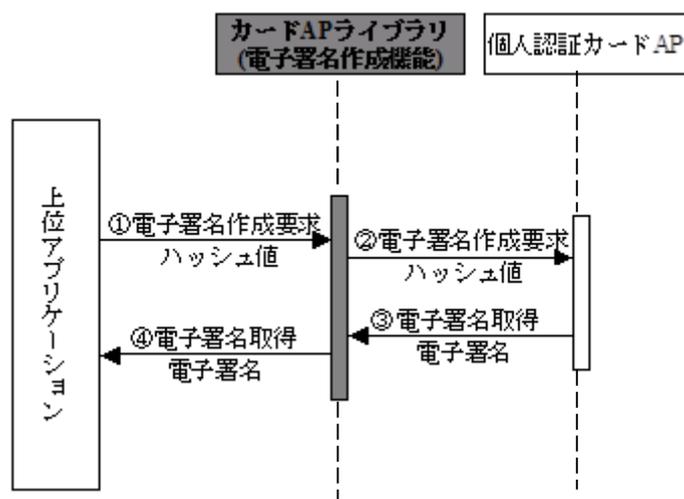


図 4-14 ハッシュ値からの電子署名作成

第 7 節 電子証明書取得機能

「第 5 章 機能概要（個人番号カード編）」「第 7 節 電子証明書取得機能」を参照。
住基カードの場合は、取得対象とする電子証明書は以下の通り。

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
- ◇ IC カードに格納された都道府県知事の自己署名証明書

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。

以下では、カード AP ライブラリからの本機能の利用方法を説明する。

2 機能仕様

(1) 本機能は以下のカード AP ライブラリで提供する。

- CryptoAPI
- PKCS#11
- CSSM および Keychain Service
- Java Native Interface

(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)
 - ・ 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。

3 電子署名検証手順(シーケンス)

本機能を使用した、電子署名検証シーケンスを図 4-15、図 4-16 に示す。

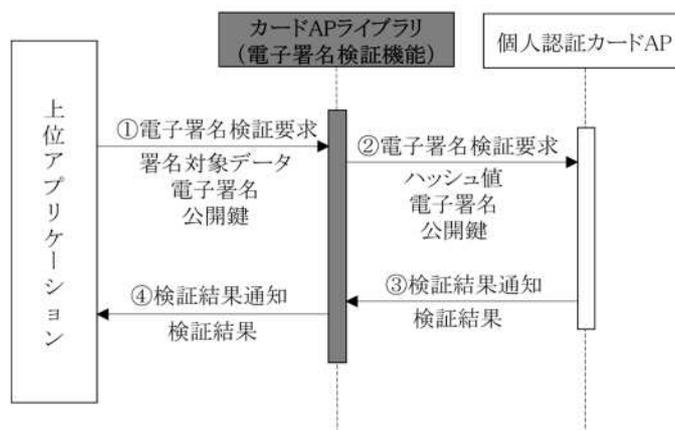


図 4-15 署名対象データ、電子署名、公開鍵からの電子署名検証

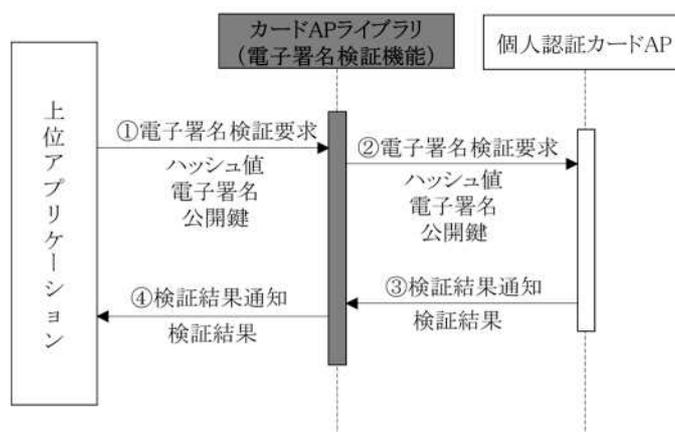


図 4-16 ハッシュ値、電子署名、公開鍵からの電子署名検証

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官職証明書検証サーバ(以下、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都道府県知事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。
- (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 官職証明書検証手順(シーケンス)

本機能を使用した、官職証明書検証シーケンスを図 4-17 に示す。

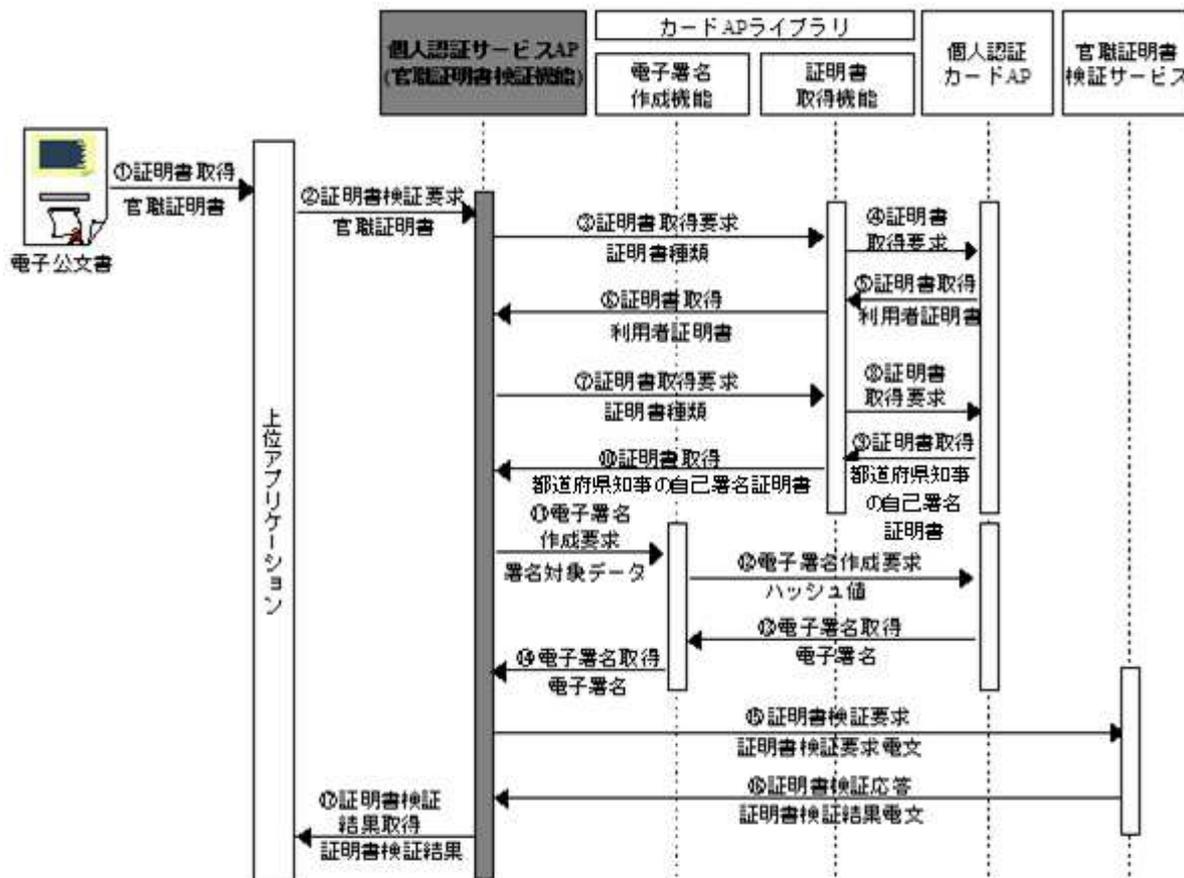


図 4-17 電子公文書の官職証明書を検証する場合

4 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。

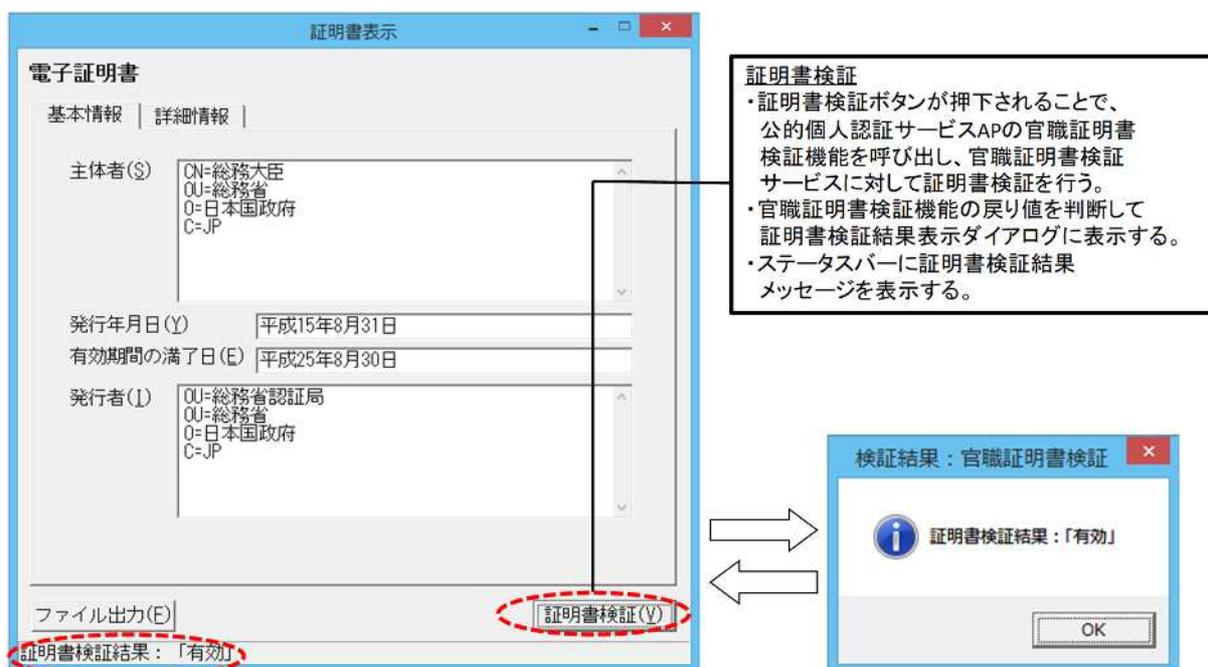


図 4 - 1 8 証明書検証ボタン

第 10 節 自分の電子証明書の有効性確認機能

「第 5 章 機能概要(個人番号カード編)」第 10 節 自分の電子証明書の有効性確認機能」を参照。

住基カードの場合は、取得対象とする電子証明書は以下の通り。

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

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。尚、MacOS 版では、この機能を実行するためには、Java 実行環境が必要となる。

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) 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。

(3) 失効申請電文で必要となる都道府県知事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。

(4) 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。

(5) 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 オンライン失効申請手順(シーケンス)

本機能を使用した、オンライン失効申請シーケンスを図 4-19 に示す。

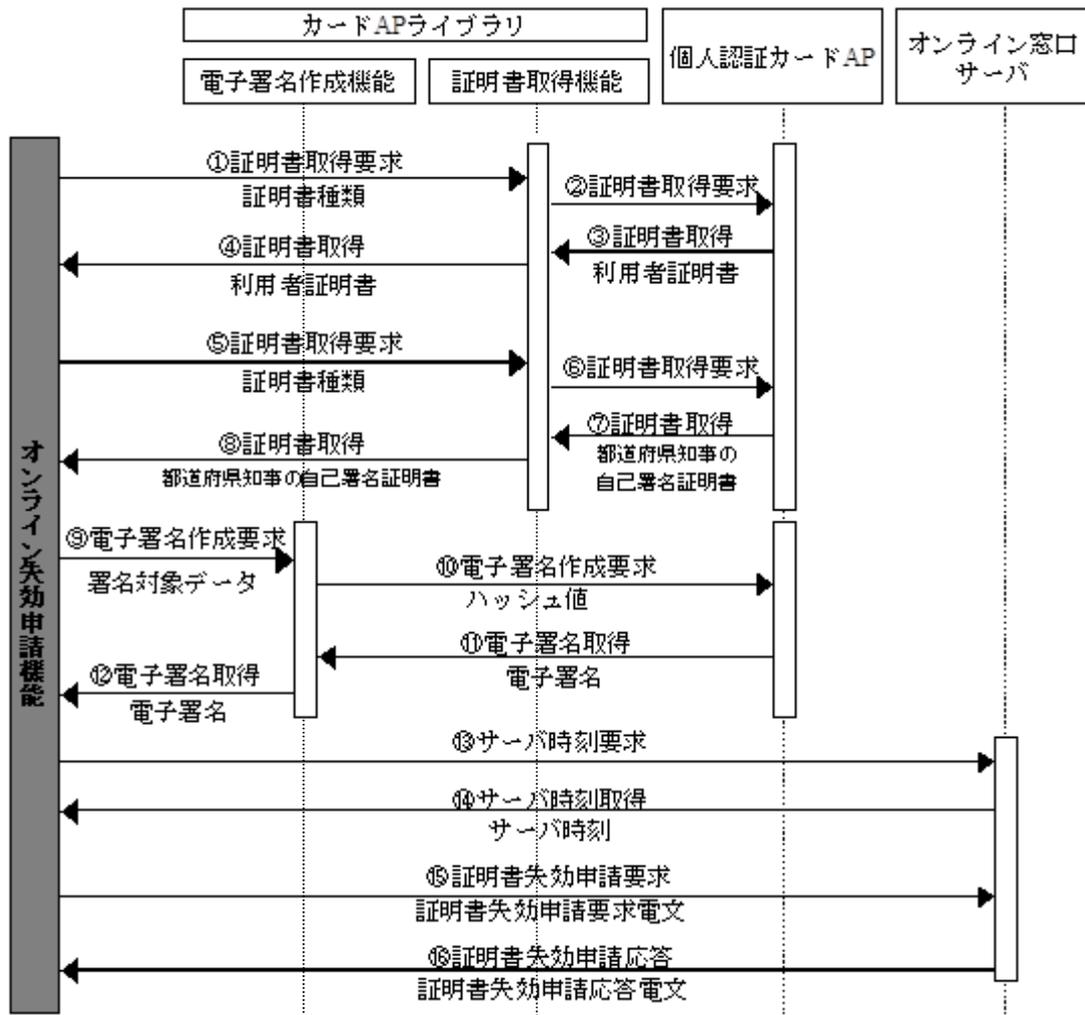


図 4-19 自分の電子証明書を失効申請する場合

4 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 - 2 0 証明書の失効申請ボタン

画面共通仕様

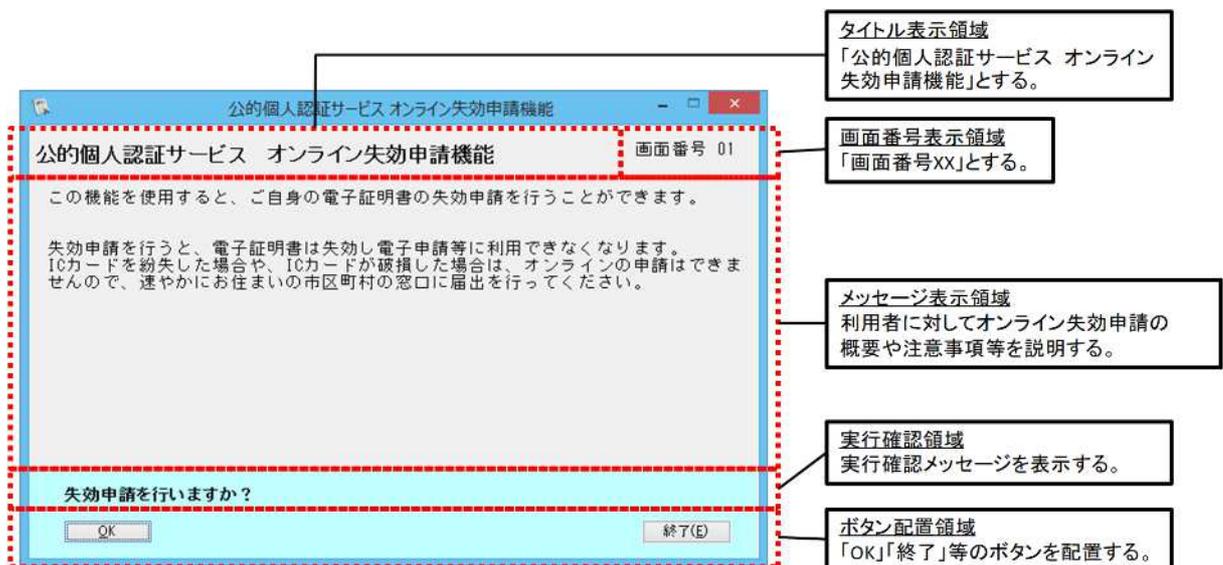


図 4 - 2 1 画面共通仕様イメージ

- フォントは、Java に標準搭載されている「Dialog」を使用する。(MacOS 版のみ)
- フォントサイズは視認性を考慮し「15pt」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 GYY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」、

第 1 2 節 ソフトウェア動作確認機能

「第 5 章 機能概要(個人番号カード編)」「第 1 2 節 ソフトウェア動作確認機能」を参照。

第 1 3 節 IC カードリーダライタ設定機能

「第 5 章 機能概要(個人番号カード編)」「第 1 3 節 IC カードリーダライタ設定機能」を参照。

第 1 4 節 Java ライブラリ登録機能

「第 5 章 機能概要(個人番号カード編)」「第 1 4 節 Java ライブラリ登録機能」を参照。

第 1 5 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公的個人認証サービスのパスワードを変更する機能。

2 機能仕様

- (1) メニュー画面から独立したユーティリティツールとして機能を実現する。
- (2) 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。
- (3) パスワードは伏せ字として表示し、4 文字以上 16 文字以下とする。
- (4) パスワードで使用する文字の種類は半角英数とすること。英小文字で入力された場合は、英大文字に変換して IC カードに設定する。
- (5) パスワード変更機能で入力されたパスワードを、利用者のパソコンに残さない方式とする。
- (6) IC カードがロックされている場合には、その旨の表示をする。

3 画面仕様

「パスワード変更」を起動することで、パスワード変更画面を表示する。

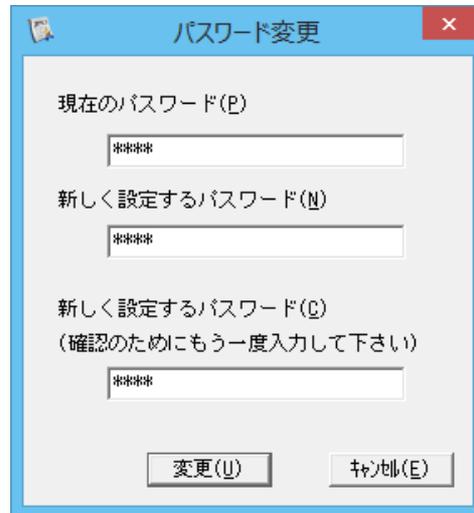


図 4-23 パスワード変更画面イメージ

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 4-24 パスワード変更結果画面イメージ

第16節 プロキシ設定機能

「第5章 機能概要（個人番号カード編）」「第16節 プロキシ設定機能」を参照。

第17節 自動更新機能

「第5章 機能概要（個人番号カード編）」「第17節 自動更新機能」を参照。

第18節 電子証明書の更新通知機能

住基カードの場合は、電子証明書の更新通知機能は提供しない。

第5章 機能概要（個人番号カード編）

第1節 メニュー画面表示機能

1 概要

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の起動ボタンを表示する。

メニュー画面起動時に、自動更新機能を実行する。

2 機能仕様

「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。

- 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
- ヘルプボタン
- 終了ボタン

3 画面仕様

メニュー画面の仕様は以下の通りである。

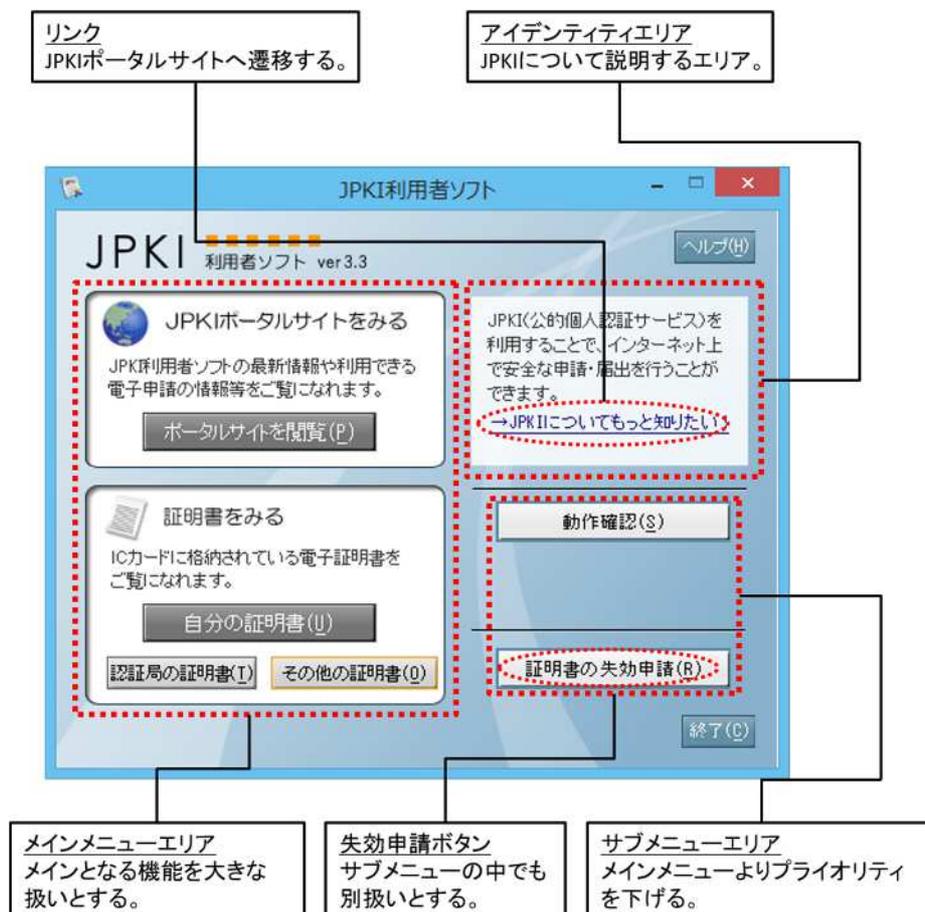


図 5-1 メニュー画面イメージ

第2節 ポータルサイト閲覧機能

1 概要

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

(1) 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「ポータルサイトを閲覧」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。

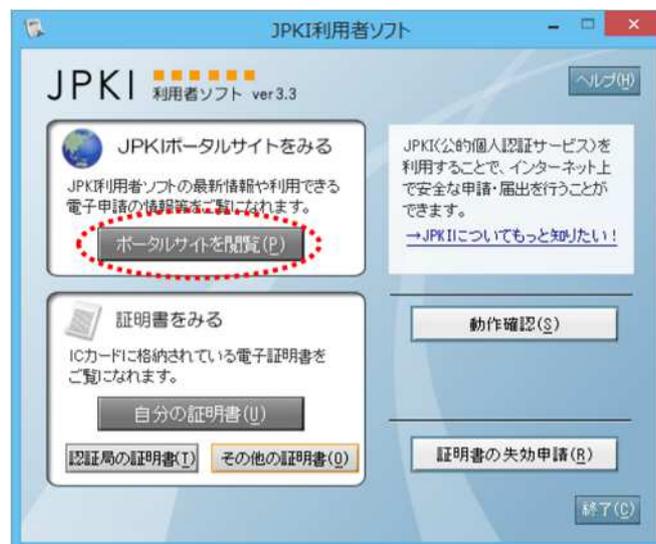


図 5-2 ポータルサイト閲覧ボタン

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 API 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) 個人番号カードが IC カードリーダーに挿入された状態で「自分の証明書」ボタンまたは「認証局の証明書」ボタンを押下した際、署名用、利用者証明用を選択するダイアログを表示し、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(シーケンス)

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。

- ◇ 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

本機能を使用した、それぞれの証明書表示シーケンスを図 5-3、図 5-4 に示す。

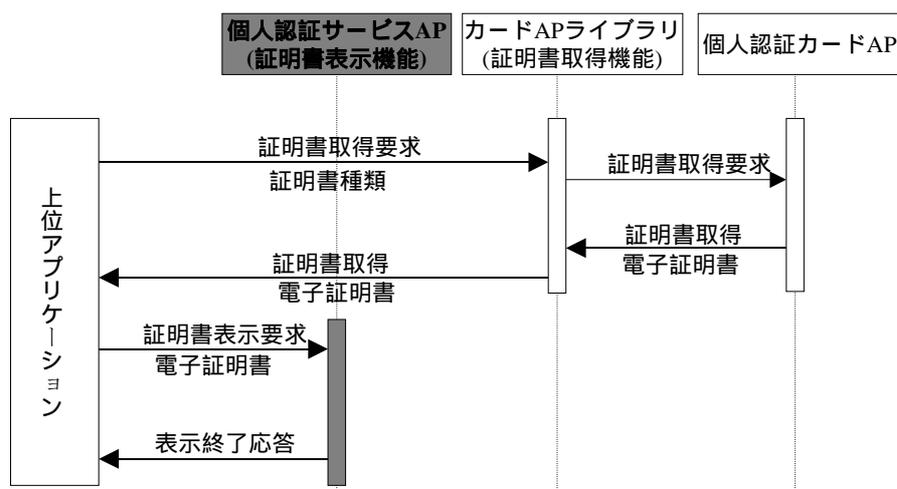


図 5-3 ICカード内の電子証明書を表示する場合

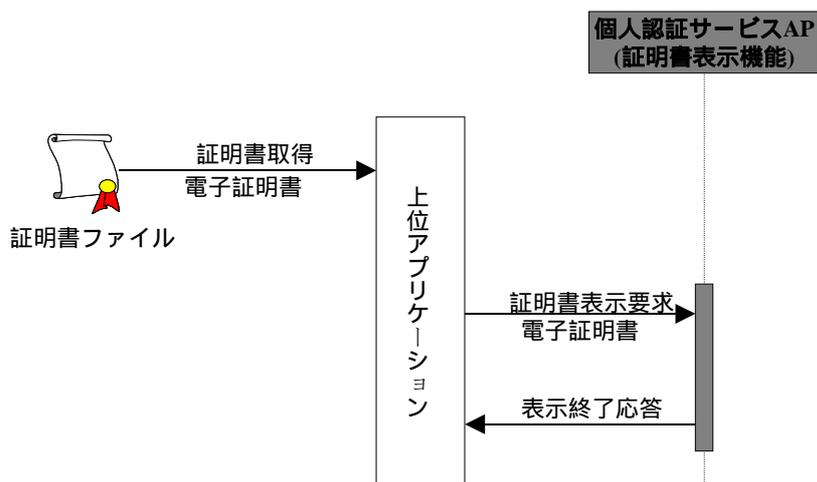


図 5-4 ファイルから電子証明書を表示する場合

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

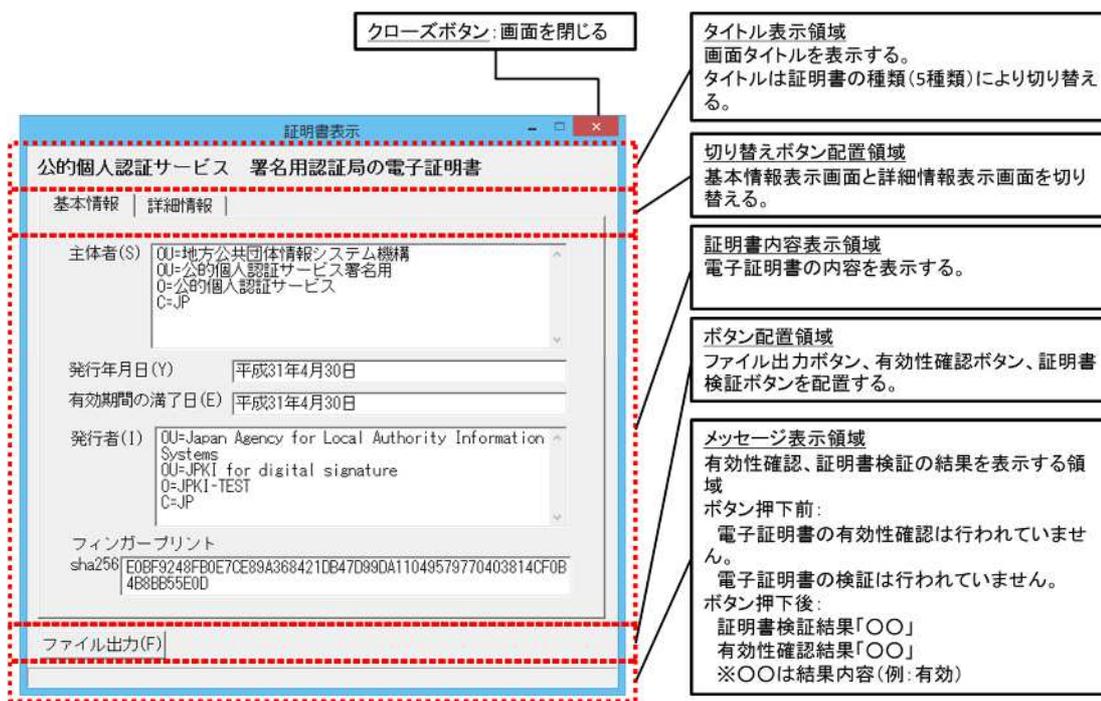


図 5-5 画面共通仕様イメージ

- 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。
Windows 版：Windows に標準搭載されている「MS ゴシック」を使用する。フォントサイズは「12pt」とする。
MacOS 版：Java に標準搭載されている「monospaced」を使用する。フォントサイズは「15pt」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電子証明書

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 5 - 6 の通り。

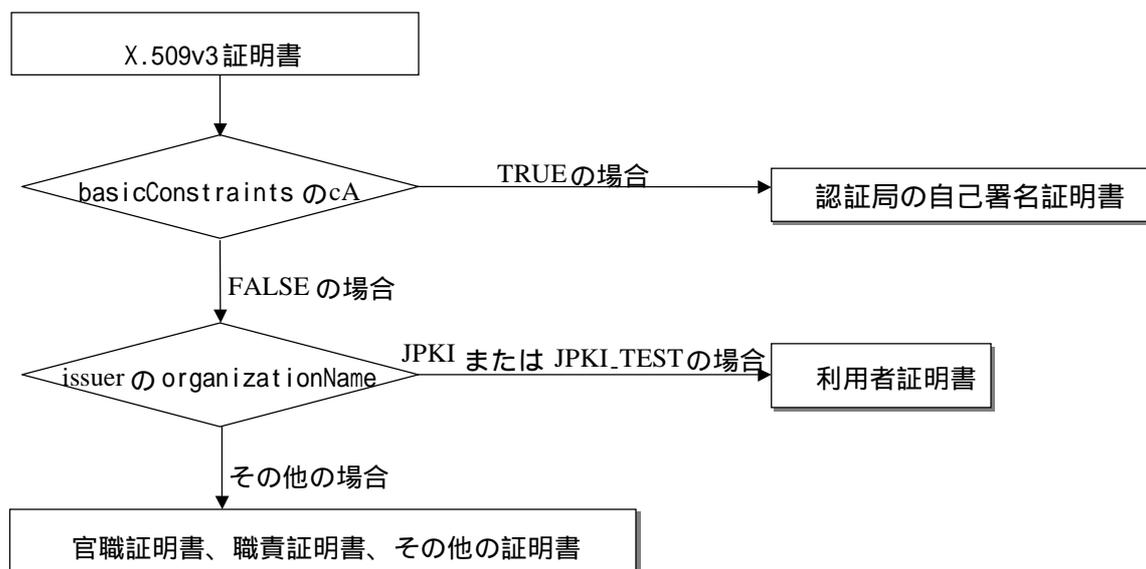


図 5 - 6 電子証明書分類処理フロー

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」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ダイアログを表示する。

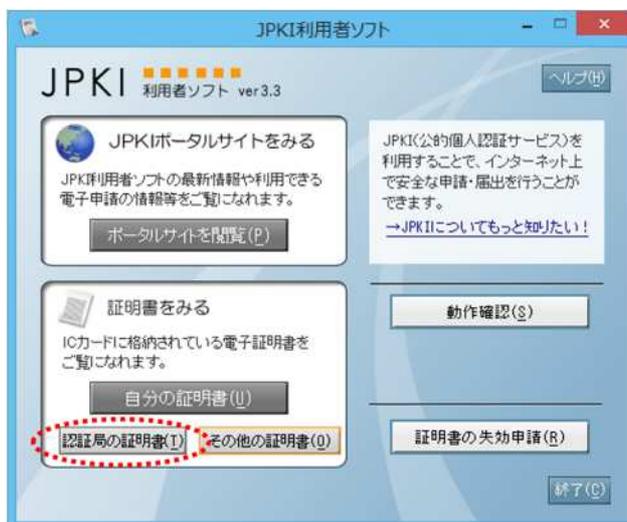


図 5 - 7 電子証明書表示ボタン(認証局の自己署名証明書)

電子証明書選択ダイアログ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。

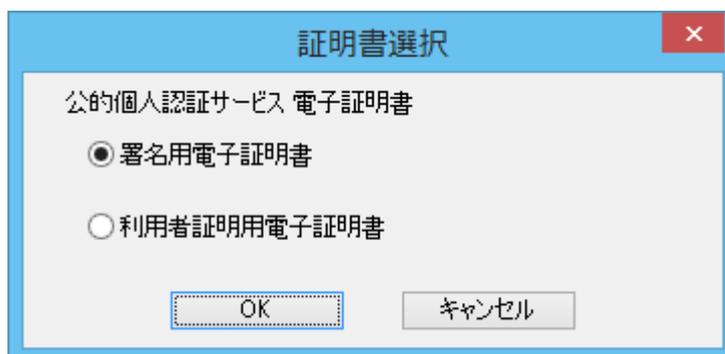


図 5 - 8 電子証明書選択ダイアログ

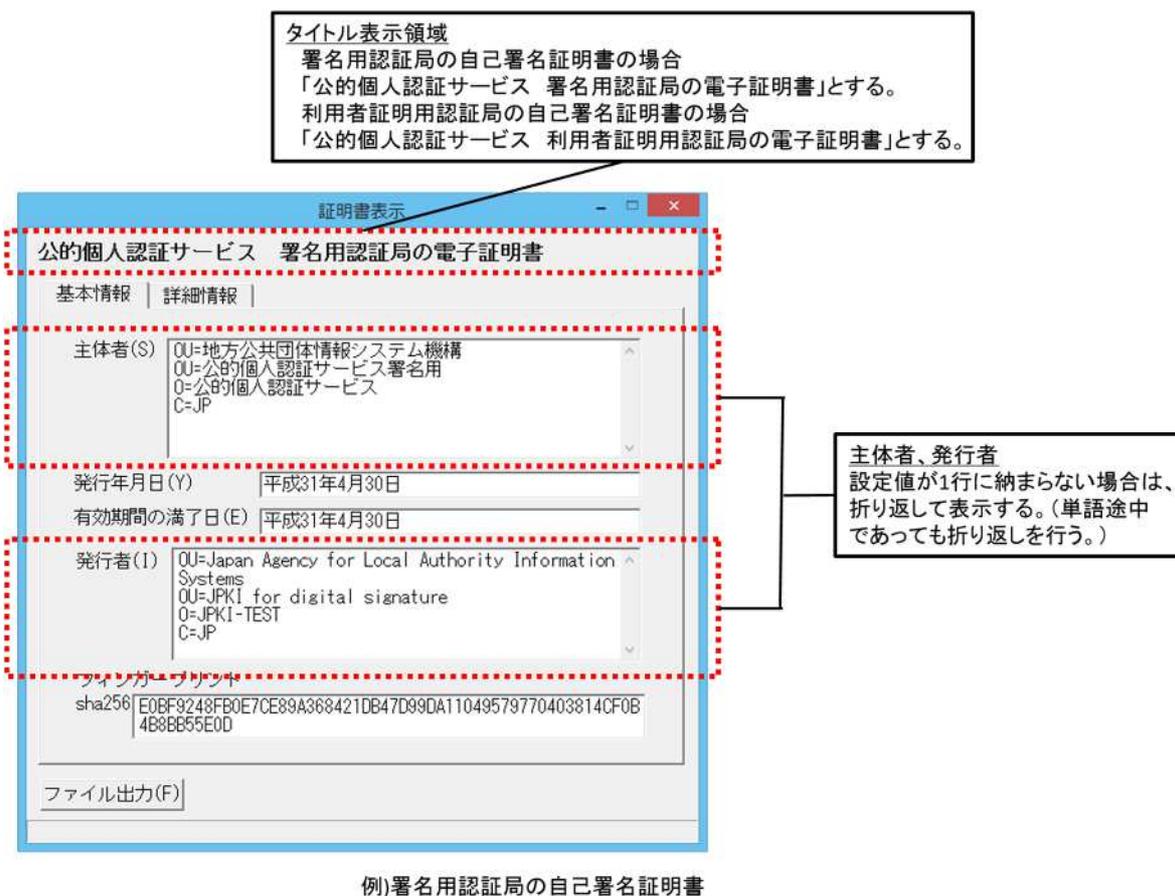


図 5 - 9 基本画面イメージ(認証局の自己署名証明書)

表 5 - 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 例) 認証局の自己署名証明書の場合	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「G G Y Y 年 MM 月 DD 日」(G G 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) 認証局の自己署名証明書の場合	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	-	-	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」ボタンを押下することで、個人番号カードに格納されている利用者の電子証明書を選択するダイアログを表示する。

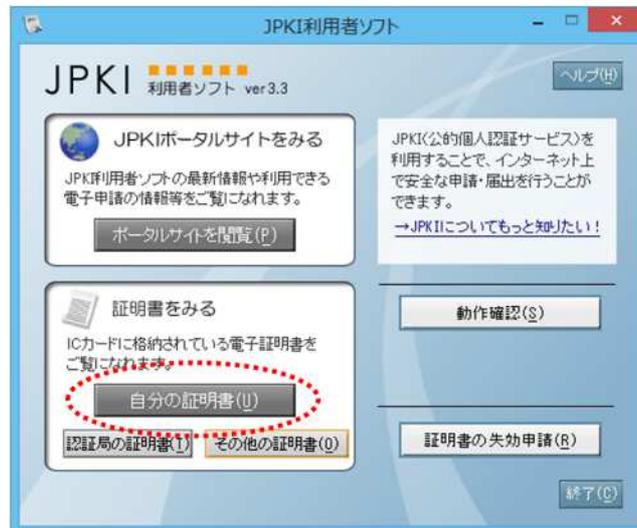


図 5 - 1 0 電子証明書表示ボタン(利用者証明書)

電子証明書選択ダイアログ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。

電子証明書選択ダイアログの画面イメージは「図 5 - 8 電子証明書選択ダイアログ」を参照。

(1) 署名用電子証明書の場合

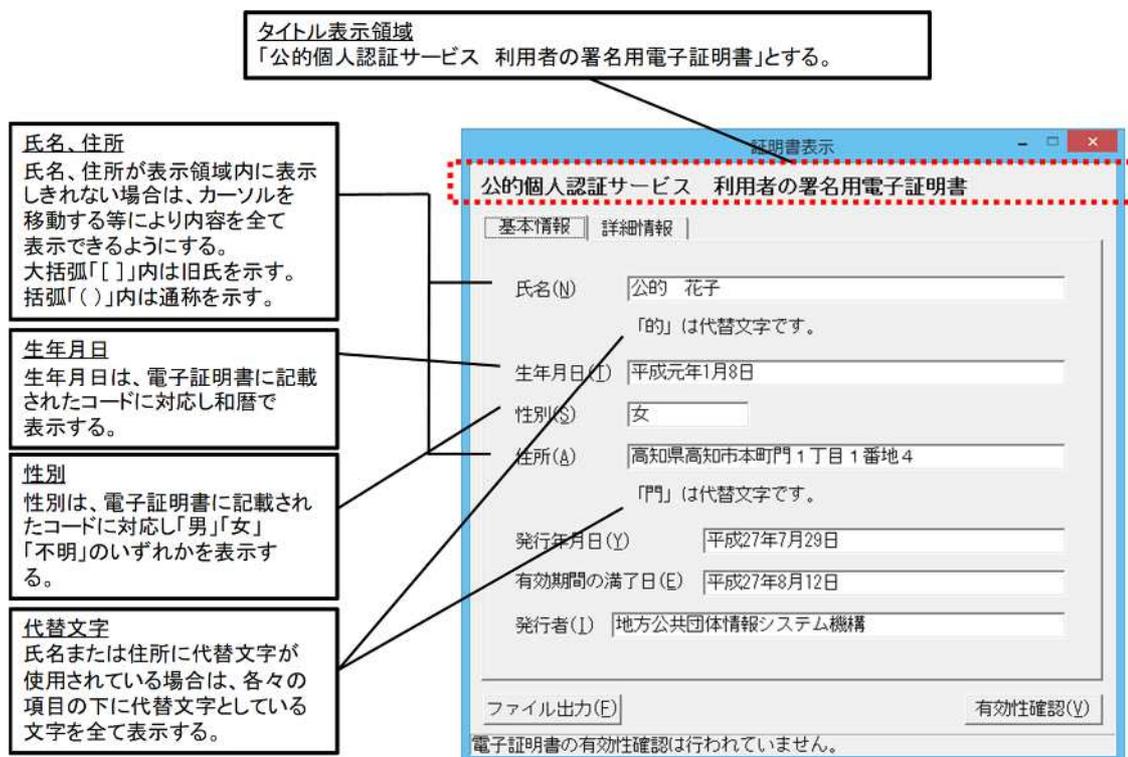


図 5 - 1 1 基本画面イメージ(署名用電子証明書)

表 5 - 2 表示項目と証明書領域の対応(署名用電子証明書)

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	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 ¹	・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 ²	設定値を和暦に変換して表示。
4	性別		gender ³	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 ¹	・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「G GYY年 MM 月 DD 日」(G G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

- 代替文字を「1」、それ以外を「0」で表現する。
- 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

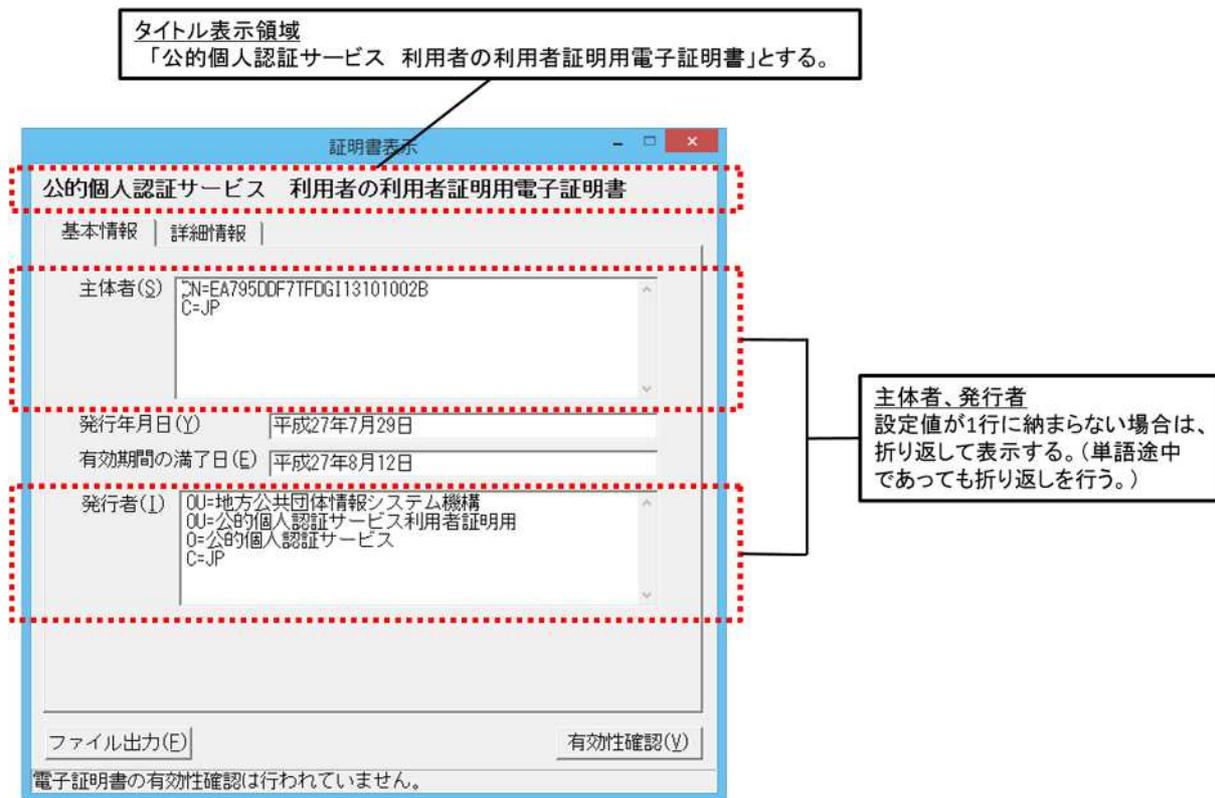


図 5 - 1 2 基本画面イメージ(利用者証明用電子証明書)

表 5 - 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」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。

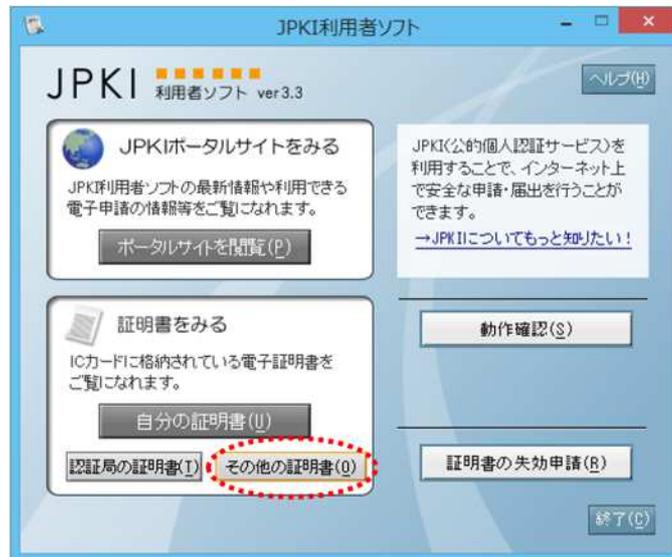
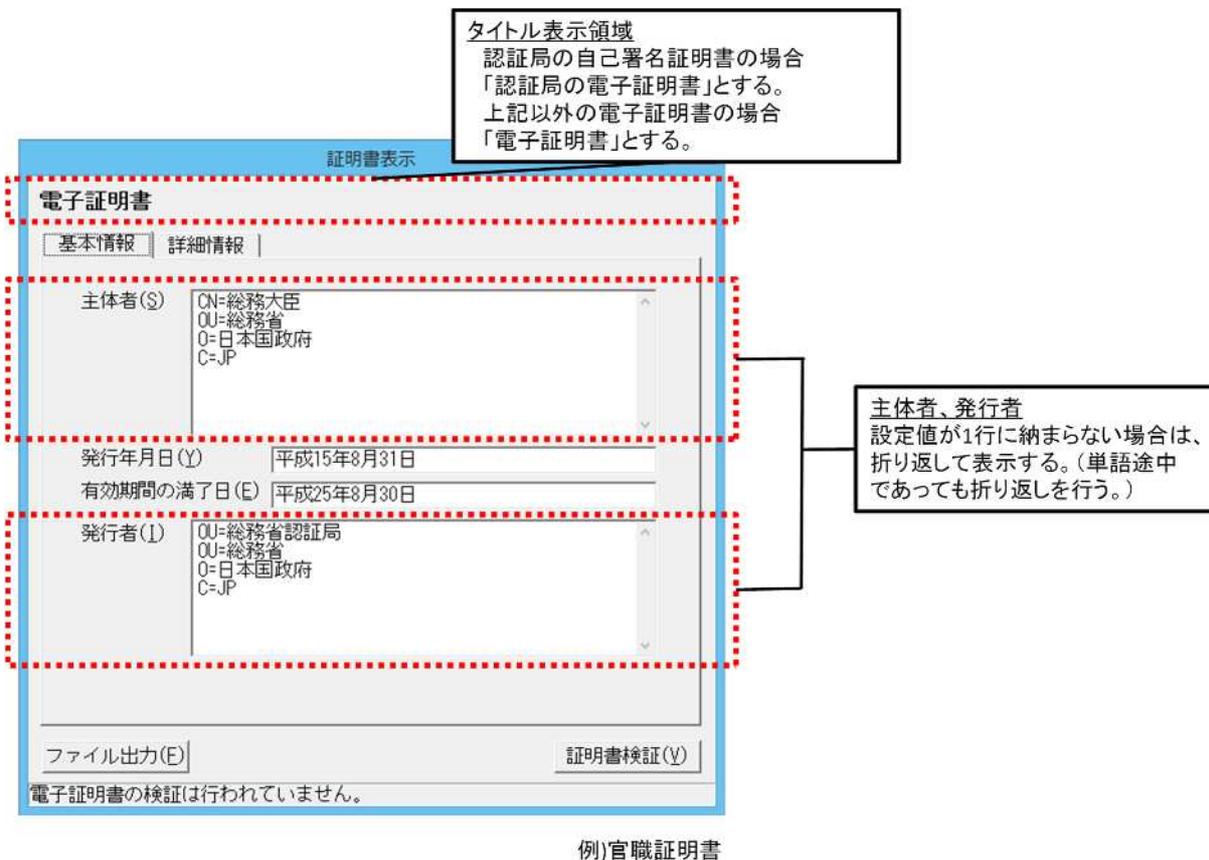


図 5 - 1 3 電子証明書表示ボタン(官職証明書、職責証明書、その他の証明書)



例)官職証明書

図 5 - 1 4 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 5 - 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「G GYY年 MM 月 DD 日」(G G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。

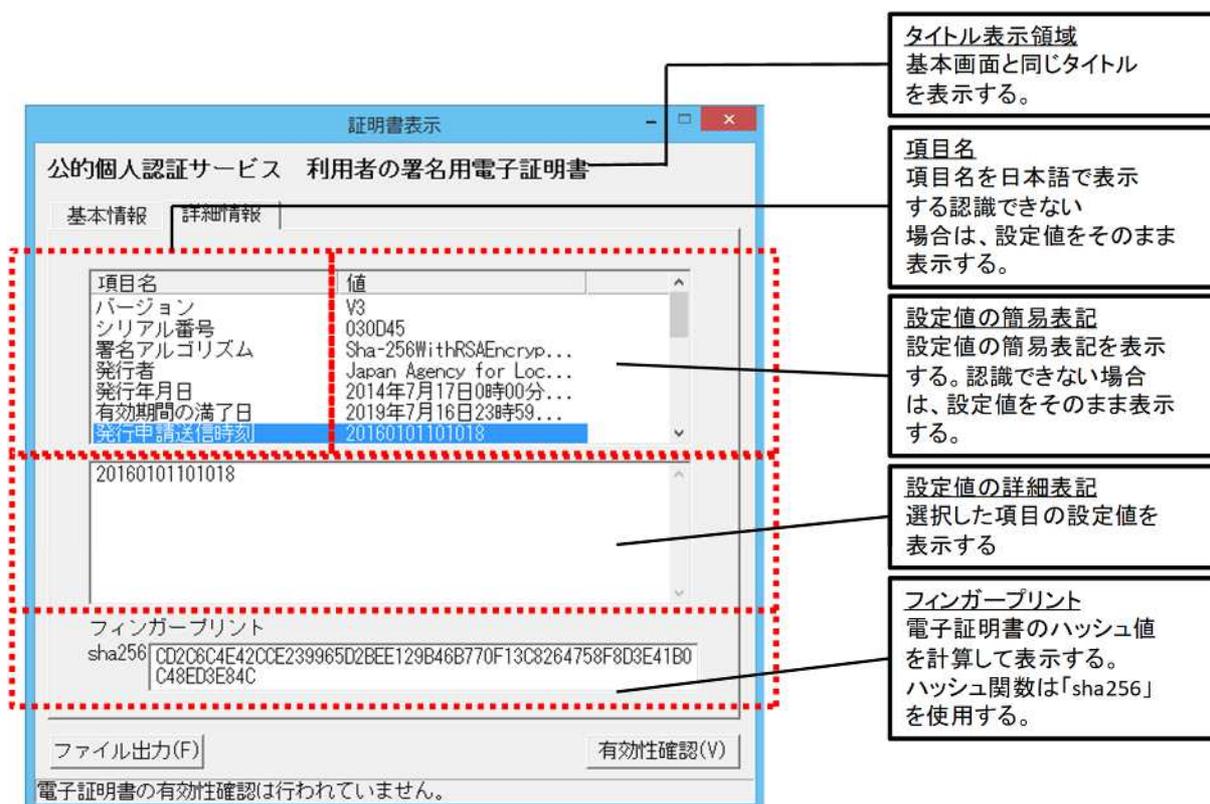


図 5 - 1 5 詳細画面イメージ

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。

- ◇ 項目名表示欄、簡易表記欄、詳細表記欄の各表示項目は、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)

署名用電子証明書の場合

110000000 digitalSignature , nonRepudiation

利用者証明用電子証明書の場合

100000000 digitalSignature

次に、簡易表記と詳細表記で表記ルールが異なる項目を以下に示す。

< 簡易表記 >

証明書基本領域

- ◇ 発行者(issuer)と主体者(subject)については、識別名(DN: Distinguished Name)の属性毎にカンマ区切りで表示する。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て表示する。

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 5 - 1 6 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 5 - 1 7 参照)

- ◇ 主体者公開鍵情報(subjectPublicKeyInfo)については、暗号アルゴリズムと鍵長を表示する。表記方式は「(algorithmのOIDに対応する値)+(鍵長)bits」

証明書拡張領域

- ◇ 最上位項目以下の情報を項目毎にカンマ区切りで表示する。

< 詳細表記 >

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 5 - 1 6 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 5 - 1 7 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。

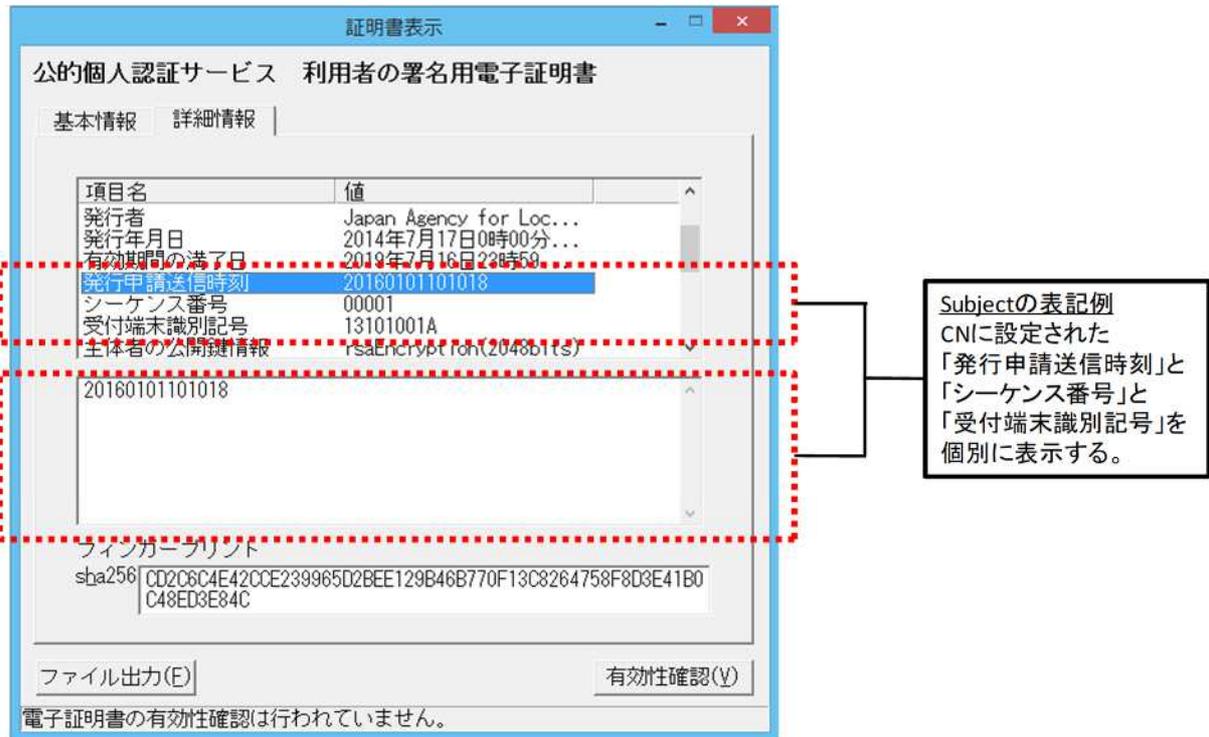


図 5 - 1 6 詳細画面イメージ(署名用電子証明書)

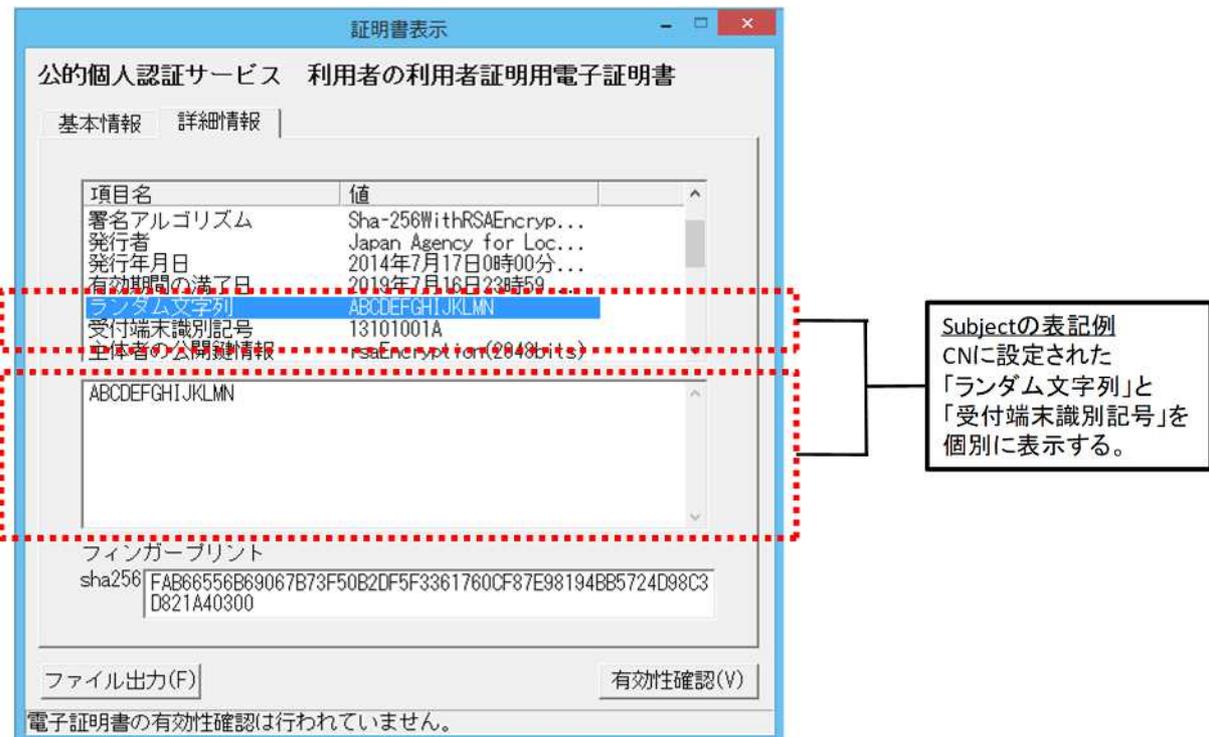


図 5 - 1 7 詳細画面イメージ(利用者証明用電子証明書)

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し、その際のファイル名は任意、拡張子は「.cer」とする。
- 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し、その際のファイル名は任意、拡張子は「.txt」とする。

(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) 電子証明書をファイルに出力する際に、任意の出力先を選択可能とする。

3 電子証明書出力手順(シーケンス)

本機能を使用した、電子証明書出力シーケンスを図 5 - 1 8 に示す。

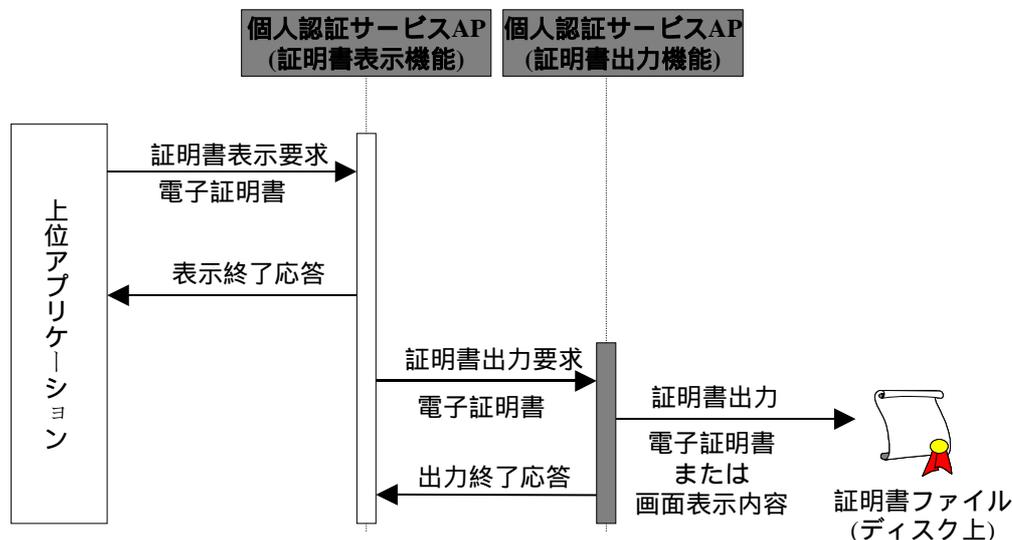


図 5 - 1 8 電子証明書表示機能から電子証明書を出力する場合

4 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。

ファイル出力

- ・ファイル出力ボタンの押下により、ファイル出力ダイアログを表示する。
- ・サポートするファイルのデータ形式は以下の2通りとする。
 - ① 基本情報ファイル (*.txt)
画面に表示されている情報をテキスト形式にて出力
 - ② 証明書ファイル (*.cer)
証明書データをDER形式にて出力

証明書表示

公的個人認証サービス 利用者の署名用電子証明書

基本情報 | 詳細情報

氏名(N)
「的」は代替文字です。

生年月日(I)

性別(S)

住所(A)
「門」は代替文字です。

発行年月日(Y)

有効期間の満了日(E)

発行者(I)

電子証明書の有効性確認は行われていません。

図 5 - 1 9 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) 上位アプリケーションから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。
- (2) 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。
- (3) 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)

3 基本 4 情報取得手順(シーケンス)

本機能を使用した、基本 4 情報取得シーケンスを図 5 - 2 0 に示す。

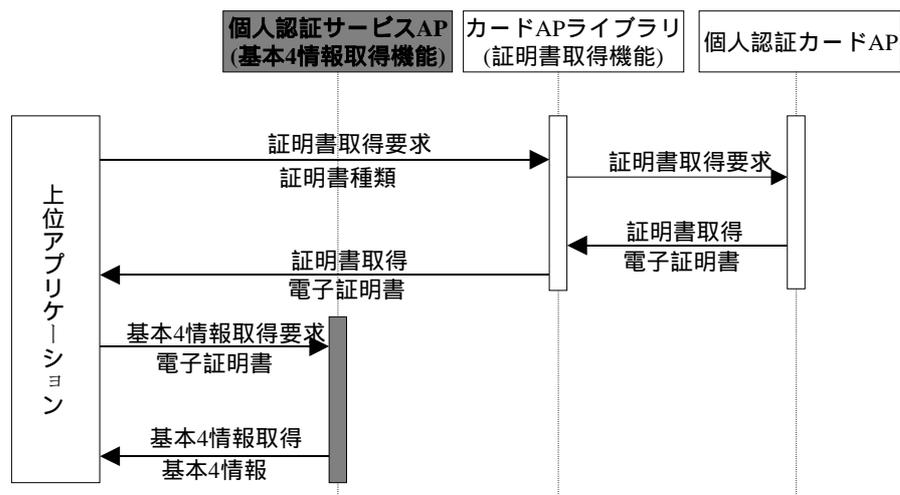


図 5 - 2 0 利用者の基本 4 情報を取得する場合

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。

以下では、カード AP ライブラリからの本機能の利用方法を説明する。

2 機能仕様

(1) 本機能は以下のカード AP ライブラリで対応する。

- CryptoAPI
- PKCS#11
- Java Native Interface

(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。
- 署名対象データの場合は、受け取った署名対象データからハッシュ値を計算して IC カードに引き渡す。
- 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。

機能上「Sha-1WithRSAEncryption」の電子署名作成機能があるが、将来的に削除予定。

3 電子署名作成手順(シーケンス)

本機能を使用した、電子署名作成シーケンスを図 5-2 1、図 5-2 2 に示す。

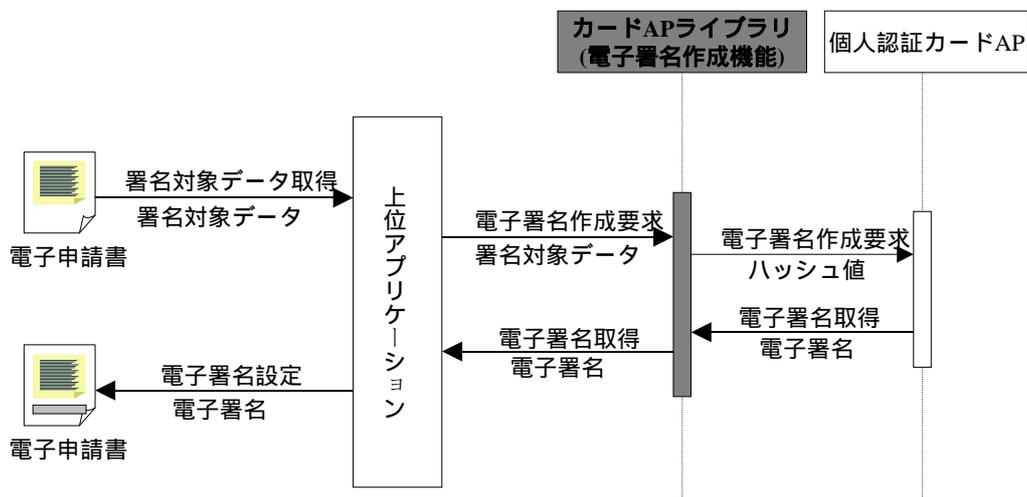


図 5-2 1 署名対象データからの電子署名作成

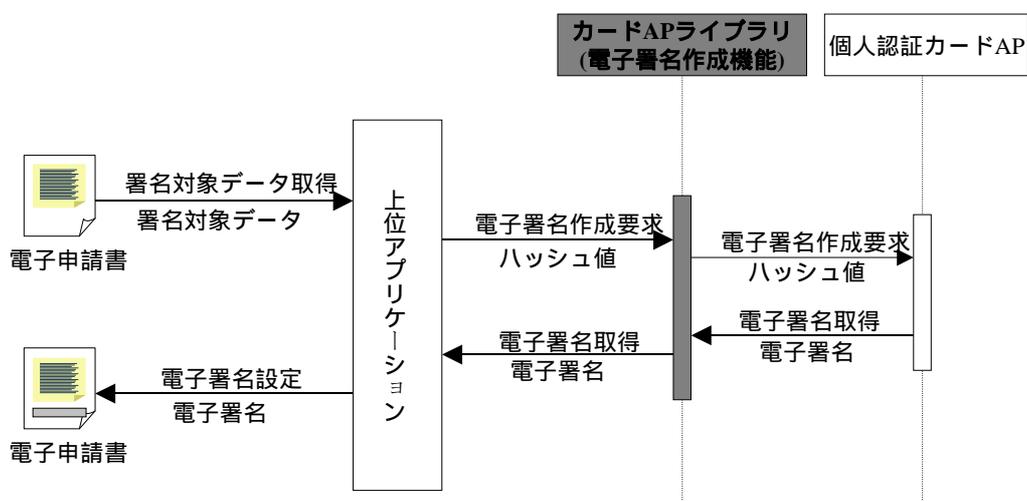


図 5-2 2 ハッシュ値からの電子署名作成

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) 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

(2) 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。

(3) 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。

3 証明書取得手順(シーケンス)

本機能を使用した、証明書取得シーケンスを図 5-23 に示す。

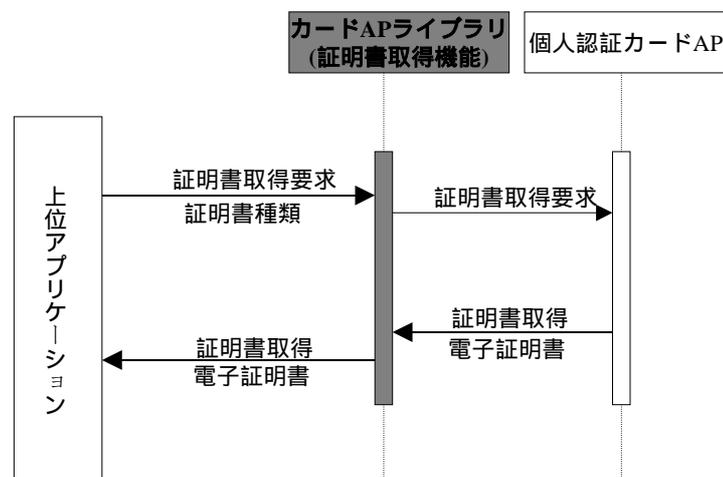


図 5-23 ICカード内の電子証明書を取得する場合

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。

以下では、カード AP ライブラリからの本機能の利用方法を説明する。

2 機能仕様

(1) 本機能は以下のカード AP ライブラリで提供する。

- CryptoAPI
- PKCS#11
- Java Native Interface

(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)
 - ・ 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。

機能上「Sha-1WithRSAEncryption」の電子署名検証機能があるが、将来的に削除予定。

3 電子署名検証手順(シーケンス)

本機能を使用した、電子署名検証シーケンスを図 5-24、図 5-25 に示す。

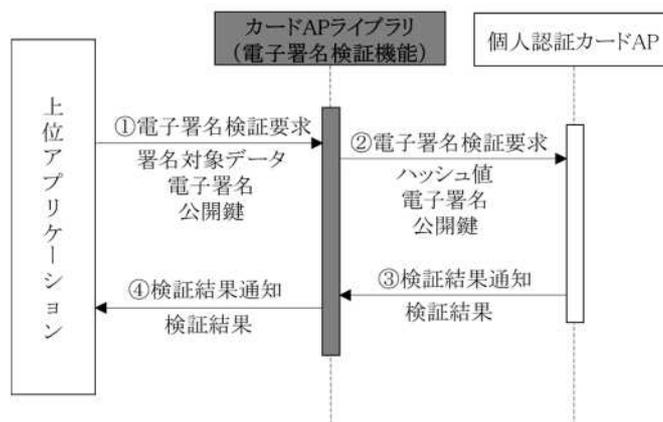


図 5-24 署名対象データ、電子署名、公開鍵からの電子署名検証

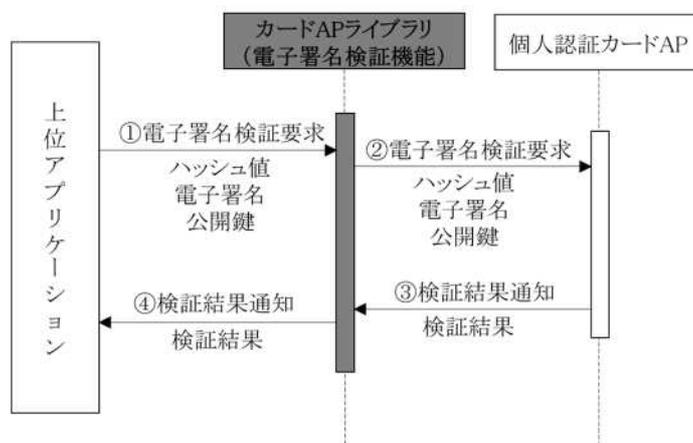


図 5-25 ハッシュ値、電子署名、公開鍵からの電子署名検証

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 官職証明書検証手順(シーケンス)

本機能を使用した、官職証明書検証シーケンスを図 5 - 2 6 に示す。

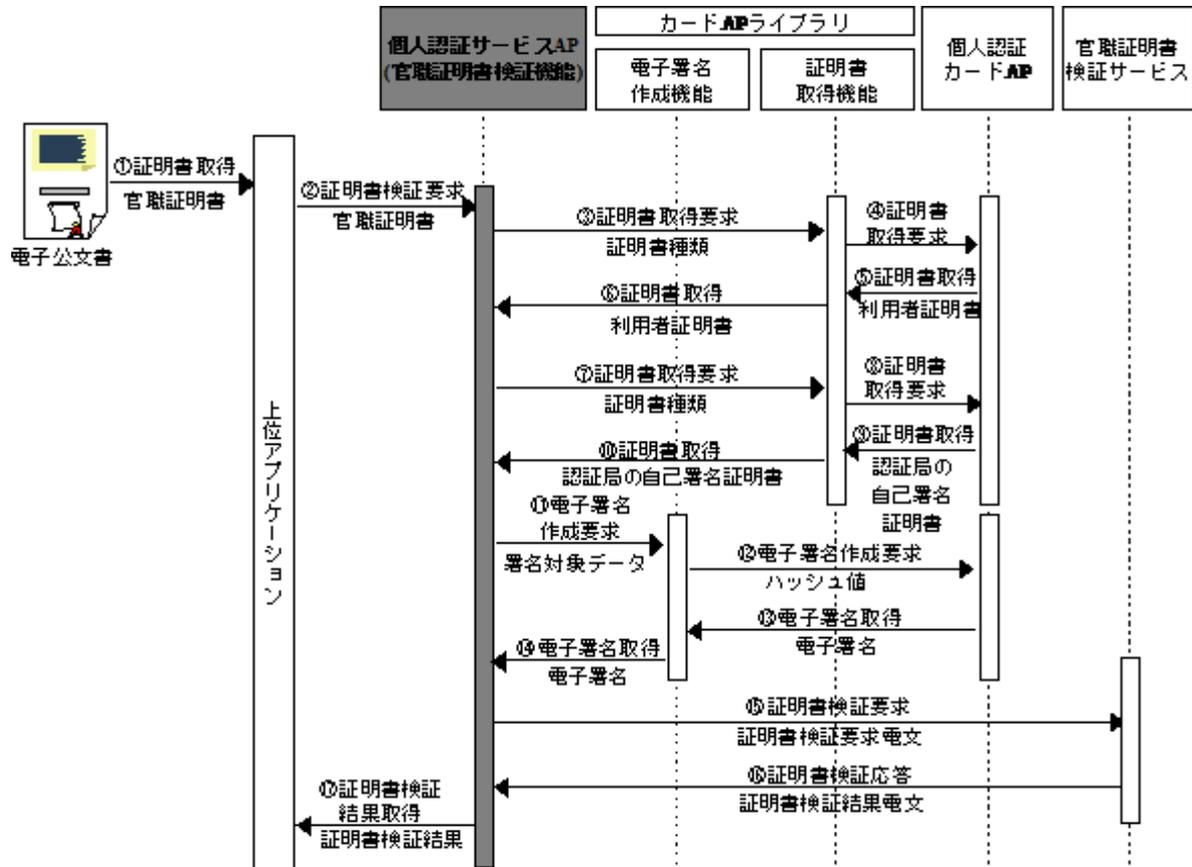


図 5 - 2 6 電子公文書の官職証明書を検証する場合

4 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。

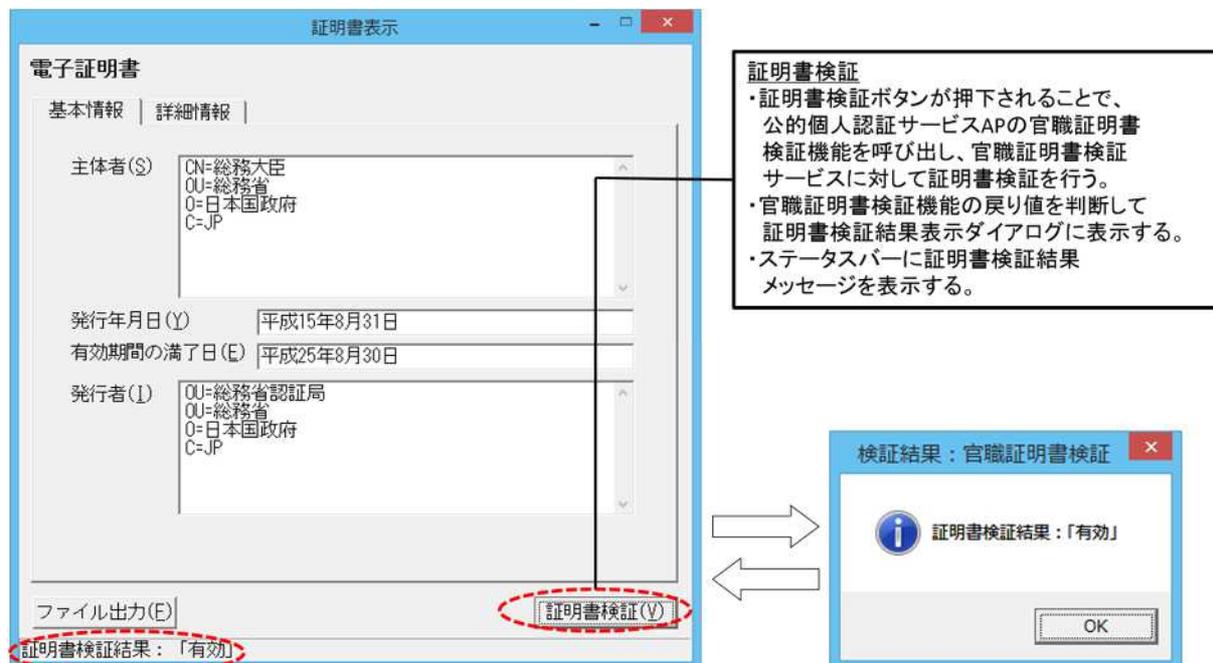


図 5 - 2 7 証明書検証ボタン

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 有効性確認手順(シーケンス)

本機能を使用した、有効性確認シーケンスを図 5 - 2 8 に示す。

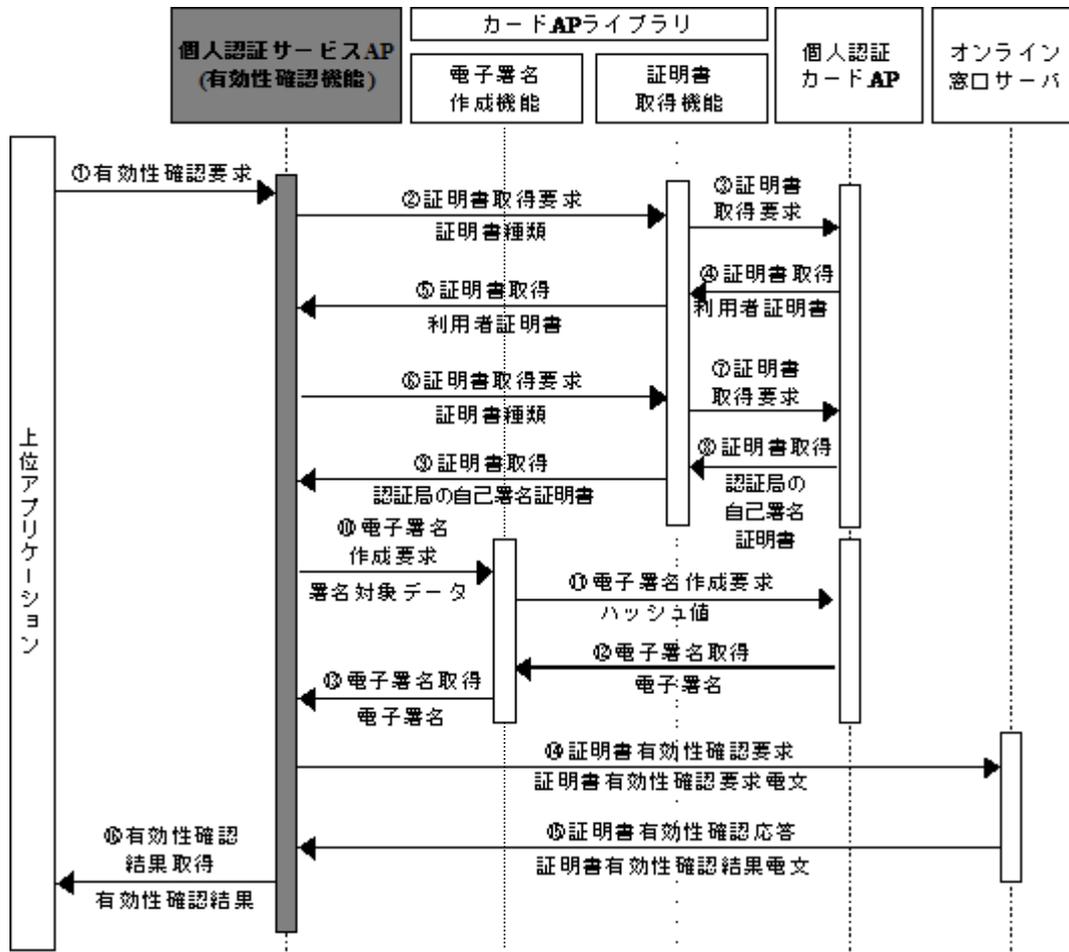
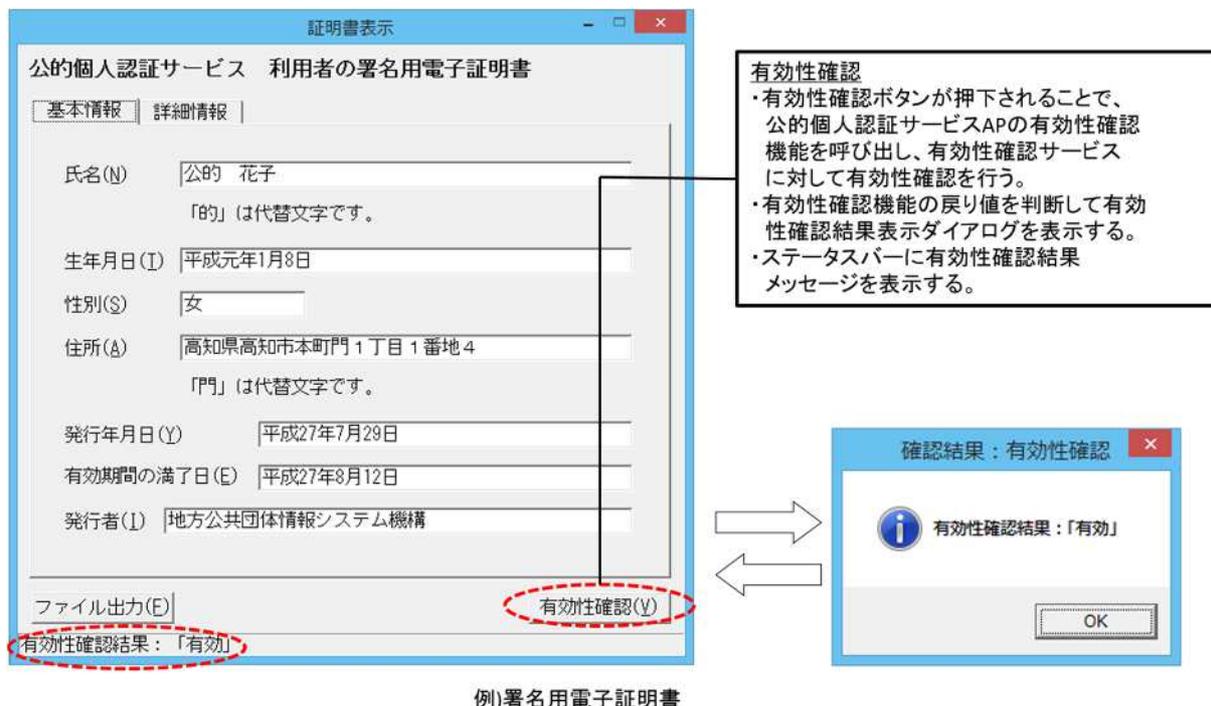


図 5 - 2 8 自分の電子証明書の有効性を確認する場合

4 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。



例)署名用電子証明書

図 5 - 2 9 有効性確認ボタン

第 1 1 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。尚、MacOS 版では、この機能を実行するためには、Java 実行環境が必要となる。

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 5-34、図 5-35」を参照。

(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 オンライン失効申請手順(シーケンス)

本機能を使用した、オンライン失効申請シーケンスを図 5-30、図 5-31 に示す。

署名用電子証明書の場合

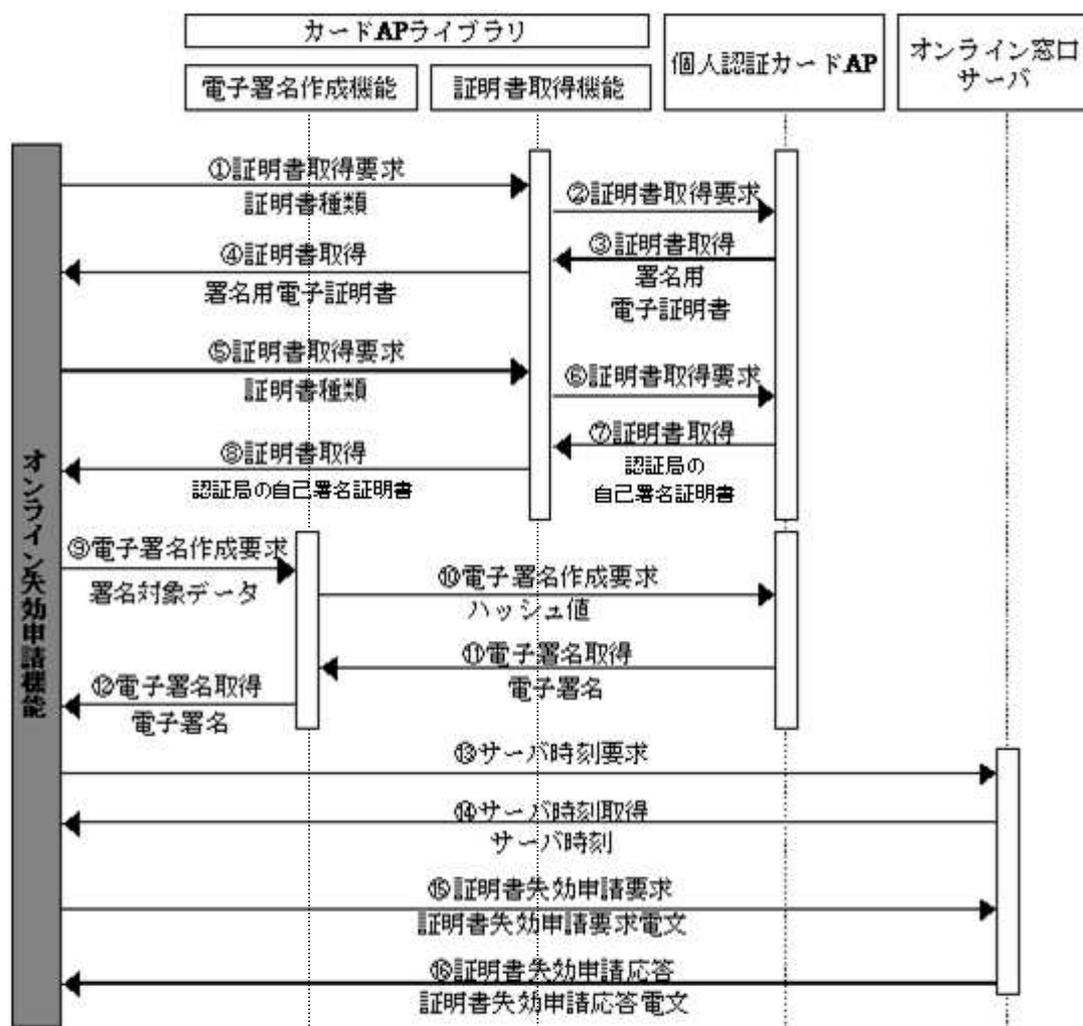


図 5-30 署名用電子証明書を失効申請する場合

利用者証明用電子証明書の場合

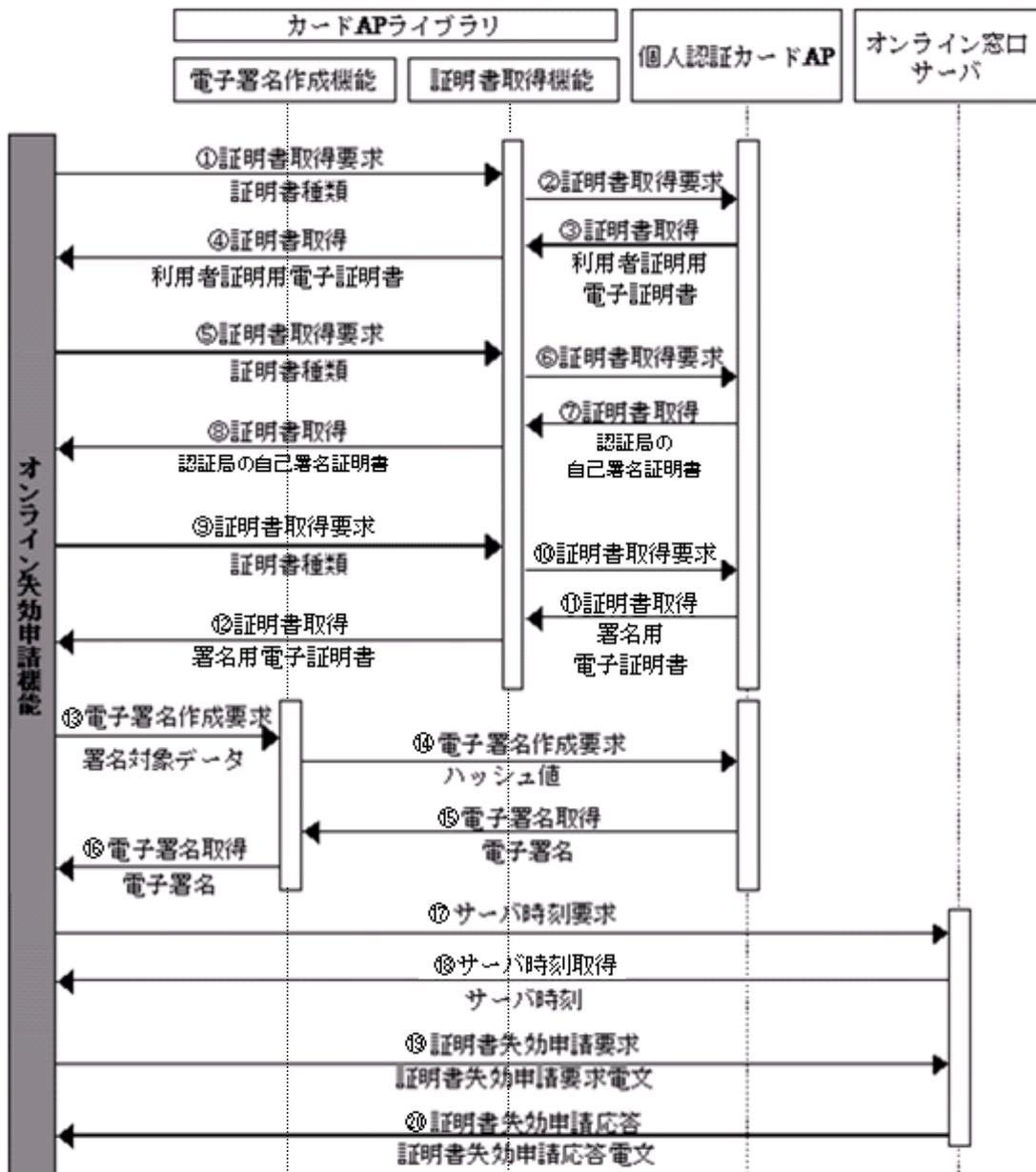


図 5 - 3 1 利用者証明用電子証明書を失効申請する場合

4 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。

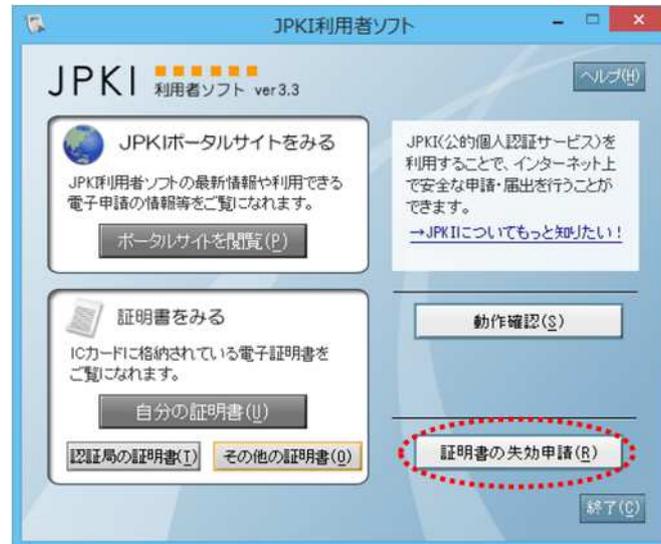


図 5 - 3 2 証明書の失効申請ボタン

「証明書の失効申請」ボタン押下後の画面遷移については、「図 5 - 3 4、図 5 - 3 5」を参照。

画面共通仕様

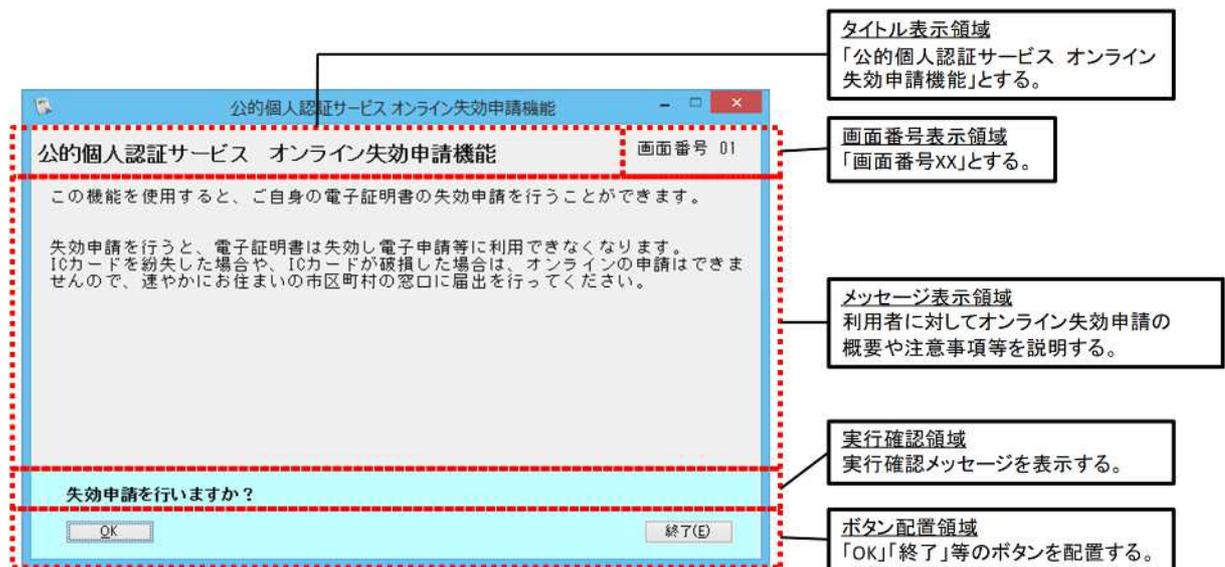


図 5 - 3 3 画面共通仕様イメージ

- フォントは、Java に標準搭載されている「Dialog」を使用する。(MacOS 版のみ)
- フォントサイズは視認性を考慮し「15pt」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。

第 1 2 節 ソフトウェア動作確認機能

1 概要

JPKI 利用者ソフトの前提となるソフトウェアやサービスの動作を確認する。

2 機能仕様

- (1) 前提となるソフトウェアやサービスの動作を確認し、実行結果を GUI 画面に表示する。
- (2) Windows の場合は Smart Card API または Windows Sockets API、MacOS の場合は Smart Card Services API を呼び出して、IC カードリーダーおよびドライバソフトウェアの動作を確認する。

3 画面仕様

メニュー画面の「動作確認」ボタンを押下することで、動作確認画面を表示する。

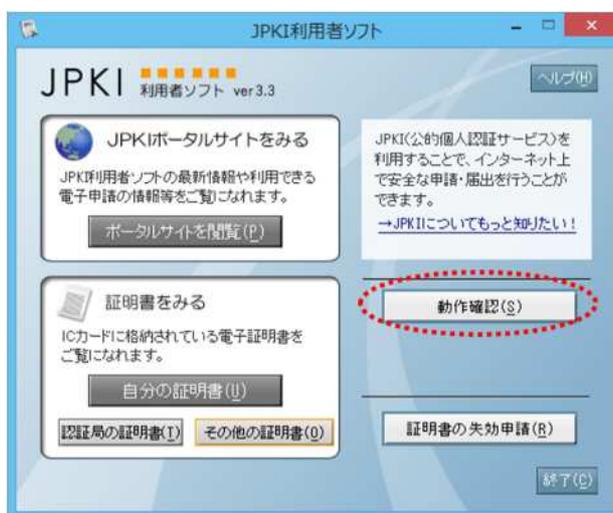


図 5-36 動作確認ボタン

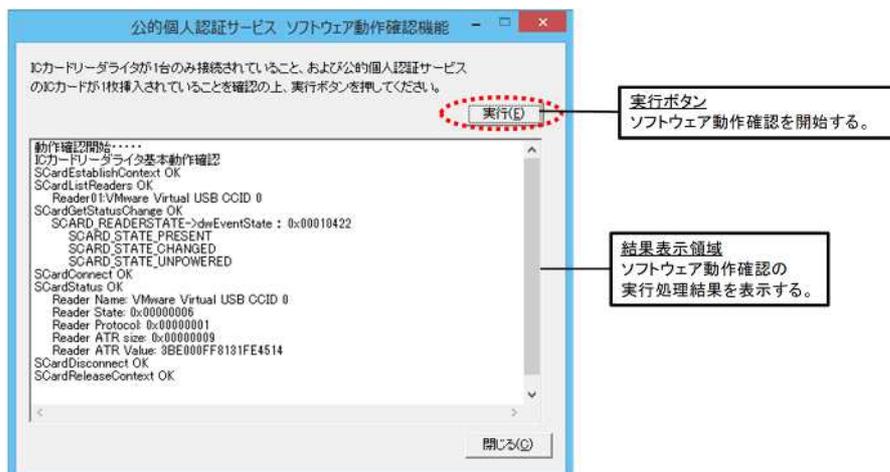


図 5-37 動作確認機能の画面イメージ

第13節 ICカードリーダーライター設定機能

1 概要

利用者がICカードを使用するためにICカードリーダーライターの種類や機種を設定する（Windows版のみ）。MacOSでは、ICカードをICカードリーダーライターにセットすることにより使用可能となるため、本機能は不要となる。

2 機能仕様

- (1) メニュー画面から独立したユーティリティツールとして機能を実現する。
- (2) 設定対象とするICカードリーダーライターの種類は以下の通り。
 - ◇ PC/SC対応ICカードリーダーライター
 - ◇ Android端末
- (3) PC/SC対応ICカードリーダーライターの設定では、パソコンに接続されたPC/SC対応ICカードリーダーライターの一覧から選択可能とする。
- (4) Bluetooth対応の設定では、Bluetooth機器(1)の一覧から選択可能とする。
Android端末以外のBluetooth機器も一覧に表示される為、利用者がデバイス名称を基に接続先のAndroid端末を選択するものとする。なお、Bluetooth機器のデバイス名称は「デバイス名 (MACアドレス)」(2)(3)と表示される。
 - 1Bluetooth機器とはパソコンにペアリング済みのBluetooth通信が行える機器を指す。
 - 2デバイス名は20文字までとし、Bluetooth機器に設定されている名称を表示する。デバイス名が20文字を超える場合、デバイス名称が全て表示されない可能性があるため、利用者がBluetooth機器に設定するデバイス名は20文字以内であるものとする。
 - 3デバイス名はShift_JISコードで表示可能な文字のみ使用できるものとする。
- (5) メニューで「ICカードリーダーライターを自動検出する」を設定した場合、ICカードにアクセスするタイミングで、接続されているPC/SC対応ICカードリーダーライターの接続を試みる仕様とする。Bluetooth機器は自動検出の対象外とする。

3 画面仕様

「ICカードリーダーダライタ設定」を起動することで、ICカードリーダーダライタ設定画面を表示する。



図 5-38 ICカードリーダーダライタ設定画面イメージ

第 1 4 節 Java ライブラリ登録機能

1 概要

JPKI 利用者ソフトの Java ライブラリを Java 実行環境に登録する機能であり、Java 実行環境の再インストールやバージョンアップを行った際に本機能を使用する。本機能により以下の機能が実行される。

◇ JPKI 利用者ソフトの Java ライブラリを Java 実行環境に登録する。

2 機能仕様

- (1) メニュー画面から独立したユーティリティツールとして機能を実現する。
- (2) 処理を実行する際は、GUI 画面を表示して登録確認を行う。
- (3) JPKI 利用者ソフトの各機能を実行するために必要な Java ライブラリを、表 5 - 5 に示すディレクトリにコピーする。

表 5 - 5 Java ライブラリのコピー先ディレクトリ

OS	コピー先ディレクトリ	備考
Windows	Java の拡張ディレクトリ	Java8 がインストールされている場合にコピーする。
	[%ProgramFiles%]¥JPKILib¥Javalib32 [%ProgramFiles%]¥JPKILib¥Javalib64	Java のバージョンに依存せずコピーする。(2)
Mac OS	/Library/Java/Extensions /usr/local/lib/JPKI(1)	Java のバージョンに依存せずコピーする。(2)

1 Java9 以降では、このディレクトリを利用すること。

2 Windows では異なるバージョンの Java の併存が可能であるが、Mac OS では併存不可である。

3 画面仕様

「Java 実行環境への登録」を起動することで、Java ライブラリ登録画面を表示する。

MacOS 版の場合、パスワードの入力ダイアログが表示されます。名前の欄に管理者権限のユーザ名が表示されていることを確認し、パスワードを入力後【OK】ボタンをクリックしてください。

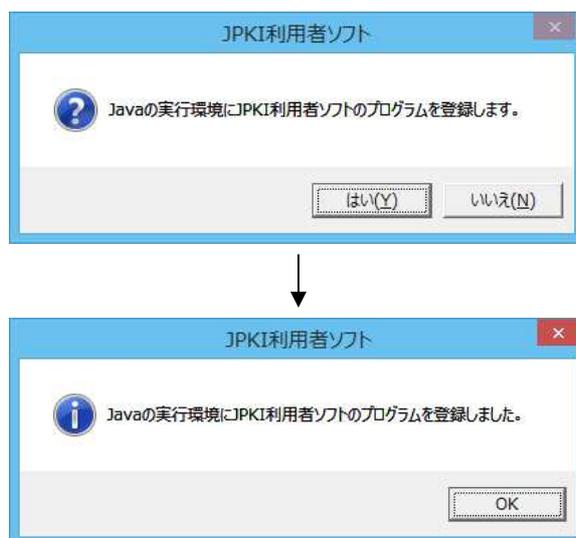


図 5 - 3 9 Java 実行環境への登録画面イメージ (Windows 版)



図 5 - 4 0 Java 実行環境への登録画面イメージ (MacOS 版)

第 15 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を変更する機能。

2 機能仕様

- (1) メニュー画面から独立したユーティリティツールとして機能を実現する。
- (2) スタートメニューから「パスワード変更」を起動することにより、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) スタートメニューから「統合パスワード変更」を起動することにより、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。
- (6) 各パスワードに入力する文字数および文字種を「表 5-6」に示す。

表 5-6 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、利用者のパソコン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ない。
 - (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。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 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

パスワード変更

「パスワード変更」を起動することで、個別変更のためのパスワード選択画面を表示する。

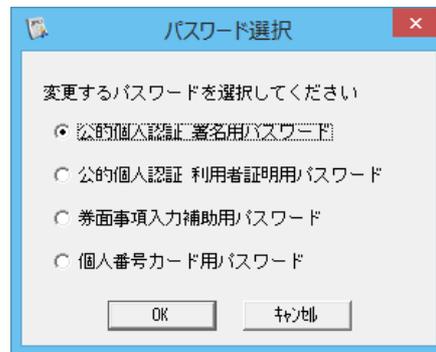


図 5-4 1 パスワード選択画面イメージ

選択したパスワードのパスワード変更画面を表示する。

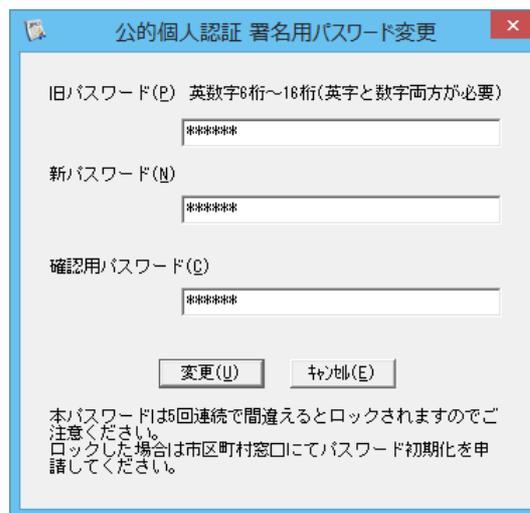


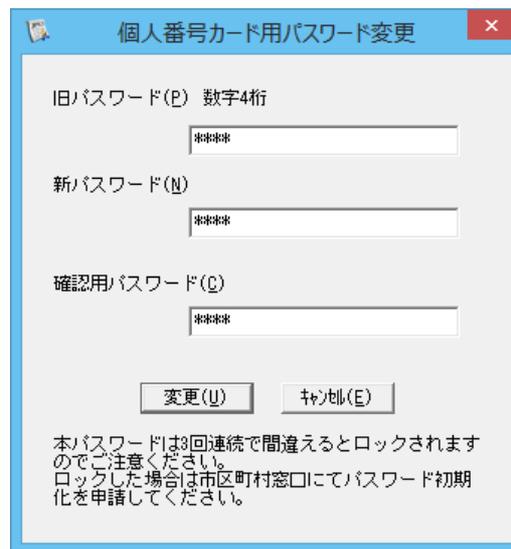
図 5-4 2 公的個人認証 署名用パスワード変更画面イメージ

The screenshot shows a dialog box titled "公的個人認証 利用者証明用パスワード変更" (Public Personal Authentication User Proof Password Change). It contains three input fields for "旧パスワード(P) 数字4桁" (Old Password (P) 4 digits), "新パスワード(N)" (New Password (N)), and "確認用パスワード(C)" (Confirmation Password (C)), each with "****" as a placeholder. Below the fields are two buttons: "変更(U)" (Change) and "キャンセル(E)" (Cancel). At the bottom, there is a warning message: "本パスワードは3回連続で間違えるとロックされますのでご注意ください。ロックした場合は市区町村窓口にてパスワード初期化を申請してください。" (This password will be locked if it is entered incorrectly 3 times in a row, so please be careful. If locked, please apply for password initialization at the city/town/village office.)

図 5 - 4 3 公的個人認証 利用者証明用パスワード変更画面イメージ

The screenshot shows a dialog box titled "券面事項入力補助用パスワード変更" (Coupon Item Input Support Password Change). It contains three input fields for "旧パスワード(P) 数字4桁" (Old Password (P) 4 digits), "新パスワード(N)" (New Password (N)), and "確認用パスワード(C)" (Confirmation Password (C)), each with "****" as a placeholder. Below the fields are two buttons: "変更(U)" (Change) and "キャンセル(E)" (Cancel). At the bottom, there is a warning message: "本パスワードは3回連続で間違えるとロックされますのでご注意ください。ロックした場合は市区町村窓口にてパスワード初期化を申請してください。" (This password will be locked if it is entered incorrectly 3 times in a row, so please be careful. If locked, please apply for password initialization at the city/town/village office.)

図 5 - 4 4 券面事項入力補助用パスワード変更画面イメージ



The screenshot shows a Windows-style dialog box titled "個人番号カード用パスワード変更" (Personal Number Card Password Change). It contains three input fields for passwords, each with "****" as a placeholder. The fields are labeled "旧パスワード(P) 数字4桁" (Old Password (P) 4 digits), "新パスワード(N)" (New Password), and "確認用パスワード(Q)" (Confirmation Password). Below the fields are two buttons: "変更(U)" (Change) and "キャンセル(E)" (Cancel). At the bottom, there is a warning message: "本パスワードは3回連続で間違えるとロックされますのでご注意ください。ロックした場合は市区町村窓口にてパスワード初期化を申請してください。" (This password will be locked if you enter it incorrectly 3 times in a row. Please be careful. If locked, please apply for password initialization at the city/town/village office.)

図 5 - 4 5 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 5 - 4 6 パスワード変更成功画面イメージ

統合パスワード変更

「統合パスワード変更」を起動することで、統合パスワード変更画面を表示する。

統合パスワード変更

旧パスワード(P) 数字4桁

新パスワード(N)

確認用パスワード(C)

変更(U) キャンセル(E)

交付時に統合パスワードで設定した方は、利用者証明用、券面事項入力補助用、個人番号カード用の3種類のパスワードを一括して変更できます。

注意：個別にパスワード変更を設定している方は、それぞれについてパスワード変更を使ってください。
統合パスワードで変更するとエラーになり、3回間違えるとロックします。
ロックした場合は市区町村窓口にてパスワード初期化を申請してください。

図 5-47 統合パスワード変更画面イメージ

全てのパスワード変更に成功した場合、以下の画面を表示する。

統合パスワード変更

パスワード変更の結果を以下に示します。

公的個人認証 利用者証明用パスワード 成功
券面事項入力補助用パスワード 成功
個人番号カード用パスワード 成功

OK

図 5-48 統合パスワード変更結果画面イメージ

第 16 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機能。

尚、MacOS 版では、この機能を実行するためには、Java 実行環境が必要となる。

ただし、MacOS 版で Java 実行環境が JRE8u111 以降または JRE9 の場合、この機能は使用できない。(Java のサポートから外れたため)

2 機能仕様

Windows 版の場合：

- (1) ブラウザに設定されているプロキシ設定から自動取得する。

MacOS 版の場合：

- (1) メニュー画面から独立したユーティリティツールとして機能を実現する。
- (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。

MacOS 版でプロキシ設定を行うためには JRE8u102 以前のバージョンを使用すること。

3 画面仕様

自動取得のため、画面は有さない。(Windows 版のみ)

「プロキシ設定」を起動することで、プロキシ設定画面を表示する。(MacOS 版のみ)

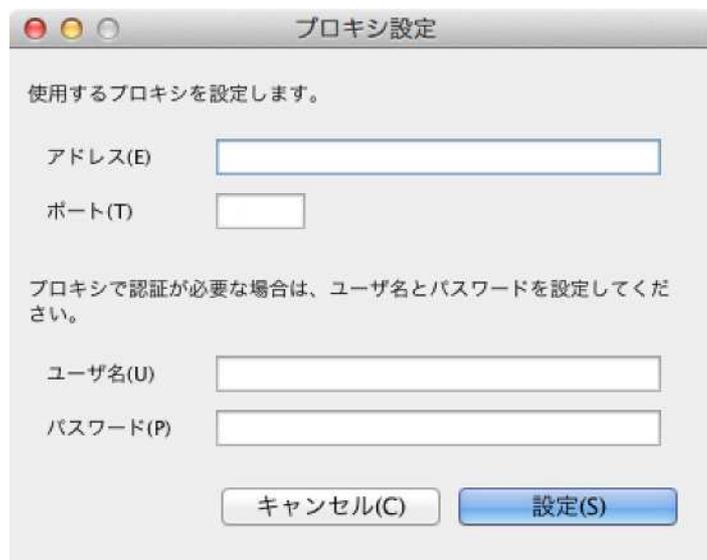


図 5-49 プロキシ設定画面イメージ

第17節 自動更新機能

1 概要

JPKI 利用者ソフトの最新バージョンの有無を確認し、より新しいバージョンがあればダイアログ表示する機能。

尚、この機能を実行するためには、オンライン窓口サーバと接続できる環境が必要となる。

2 機能仕様

- (1) メニュー画面の起動時に自動更新機能を実行する。
- (2) 最新バージョンのリリース情報は、オンライン窓口サーバにアクセスし取得する。
- (3) プロキシベーシック認証が必要な環境でオンライン窓口サーバにアクセスする場合は、プロキシサーバへ送信するユーザ名とパスワードの入力を確認するダイアログを表示する。
- (4) 最新バージョンの有無を確認し、より新しいバージョンがあればダイアログ表示する。

3 画面仕様

メニュー画面の起動時に自動更新機能を実行する。その際、プロキシベーシック認証が必要な環境では JPKI 利用者ソフト バージョン確認画面を表示する。

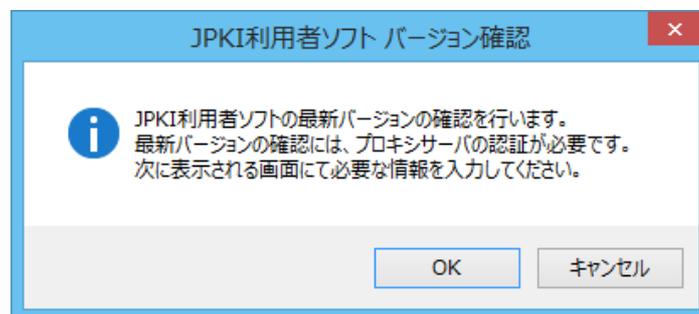


図 5-50 プロキシベーシック認証 確認画面イメージ

新しいバージョンを確認し、より新しいJPKI 利用者ソフトがリリースされている場合は、その旨を通知する画面を表示する。

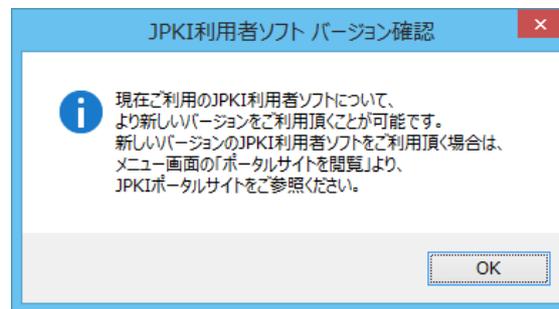


図 5 - 5 1 最新バージョン通知画面イメージ

オンライン窓口サーバに接続できない場合等、新しいバージョンのリリース確認が行えなかった場合は、JPKI 利用者ソフトバージョン確認画面を表示しない。

画面遷移

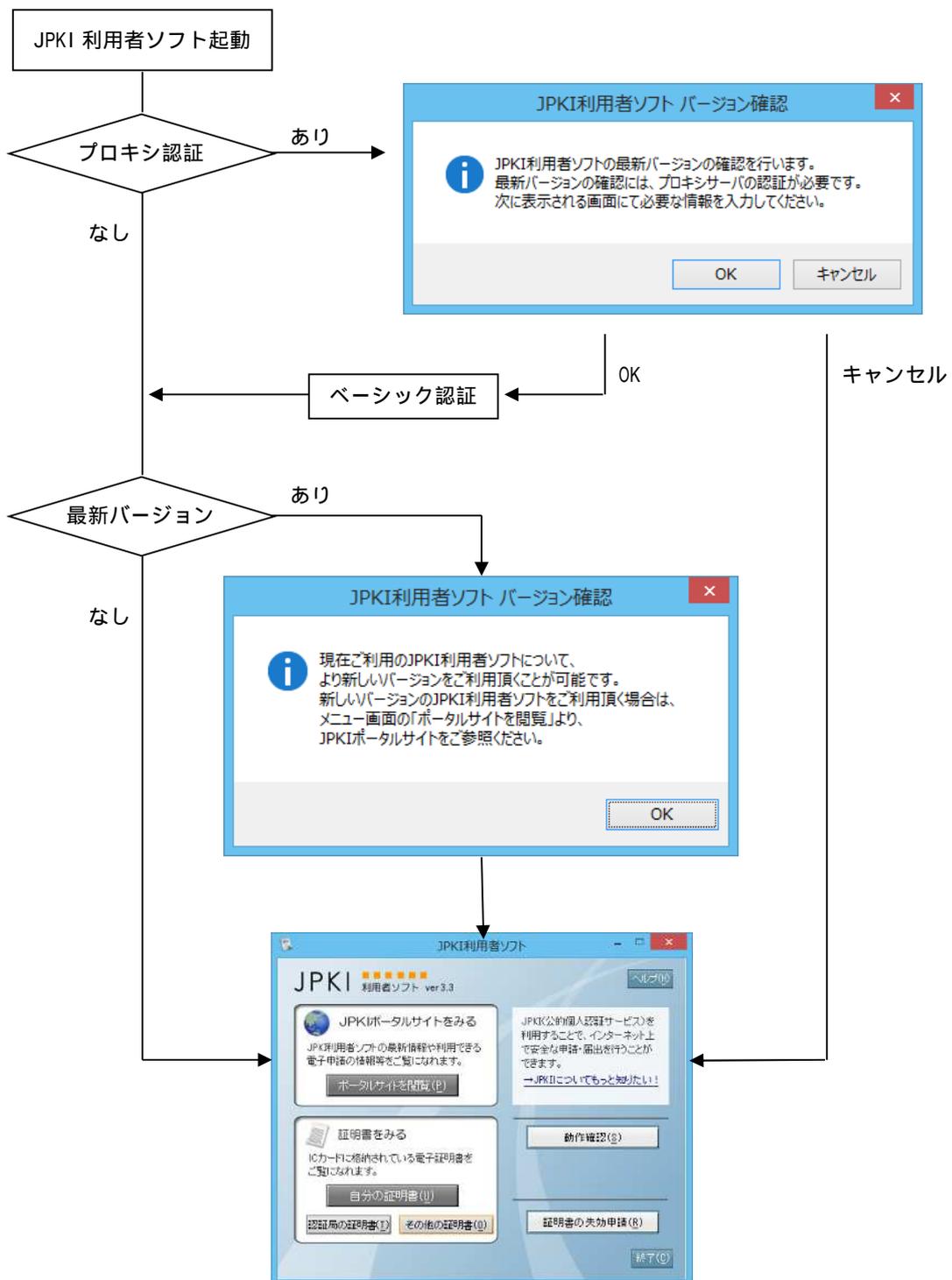


図 5 - 5 2 自動更新機能の画面遷移

第 18 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限切れ前に、電子証明書の更新を促す通知を行う機能。

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。

- 以下の方法でログインユーザごとに電子証明書表示履歴を保持する。
 - ・ 「第 5 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 5 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 5 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。
 - ・ ログインユーザごとに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 5 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。
 - ・ 有効期限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。
- 以下の方法でログインユーザごとに電子証明書の更新を促す通知をする。
 - ・ OS ログイン時、ログインユーザごとに保持されている電子証明書表示履歴を参照し、有効期限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。
 - ・ 有効期限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。
 - ・ 以下の条件を満たす場合「有効期限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 5 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。
- ・ 「第 5 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。

- メニュー画面から独立したユーティリティとして機能を実現する。
- ログインユーザごとに OS ログイン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。
 - ・ JPKI 利用者ソフトインストール時
 - ・ JPKI 利用者ソフトインストール後、スタートメニューに登録される「更新通知設定」の実行
- 本機能の実行方法と必要なユーザ権限および設定が反映されるユーザについて「表 5-7」に示す。

表 5-7 更新通知設定の実行方法と必要なユーザ権限および設定が反映されるユーザ

項番	更新通知設定の実行方法	必要なユーザ権限	更新通知設定が反映されるユーザ	備考
1	JPKI 利用者ソフトインストール時	管理者	インストールを実行したユーザ	インストールを実行したユーザ以外のユーザに対して更新通知設定を行う場合は、当該ユーザで OS にログイン後、スタートメニューから更新通知設定を実行する必要がある。
2	スタートメニューからの実行	標準ユーザ以上	更新通知設定を実行したユーザ	

- 「更新通知設定」を実行していないユーザは、更新通知機能「無効」とみなす。

3 画面仕様

有効期限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。

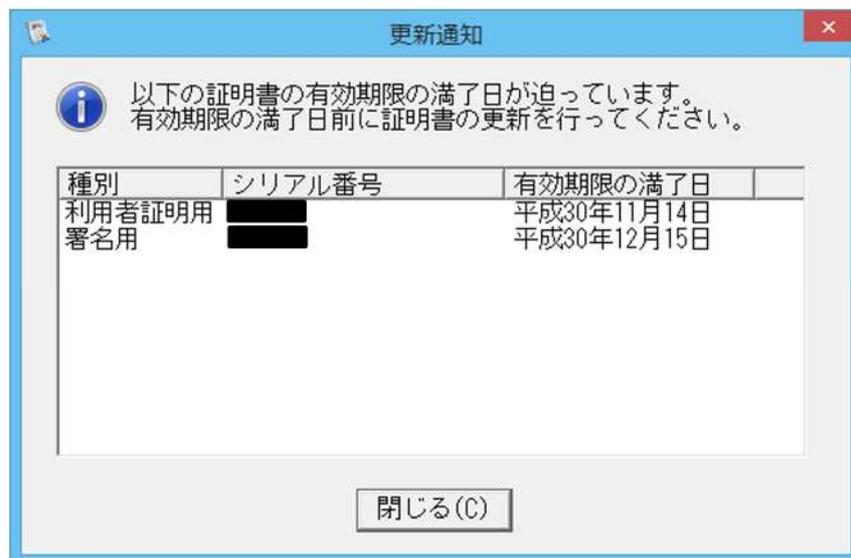


図 5 - 5 3 更新通知画面イメージ

JPKI 利用者ソフトインストール時およびスタートメニューの更新通知設定を起動することによって、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する。

「いいえ」が選択された場合、更新通知機能を無効とする。

「×」によって画面を閉じた場合、現在の設定内容を変更しない。

(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。)

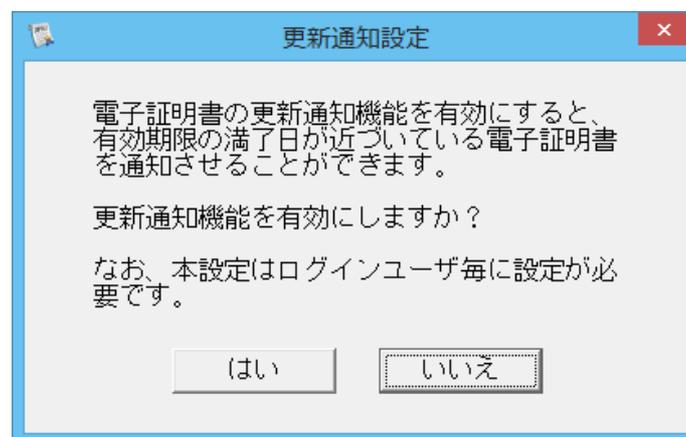


図 5 - 5 4 更新通知設定画面

第 6 章 アクセシビリティ対応

第 1 節 アクセシビリティ対応項目

1 概要

JPKI 利用者ソフトのアクセシビリティ対応項目を以下に示す。

表 6-1 アクセシビリティ対応項目

項番	アクセシビリティ対応項目
	初期フォーカス設定
	フォーカス順
	主要コンポーネントに対するニーモニック
	コンポーネントに対するツールチップ
	コンポーネントに対するユーザ補助の名称
	コンポーネントに対するユーザ補助の説明

2 画面イメージ

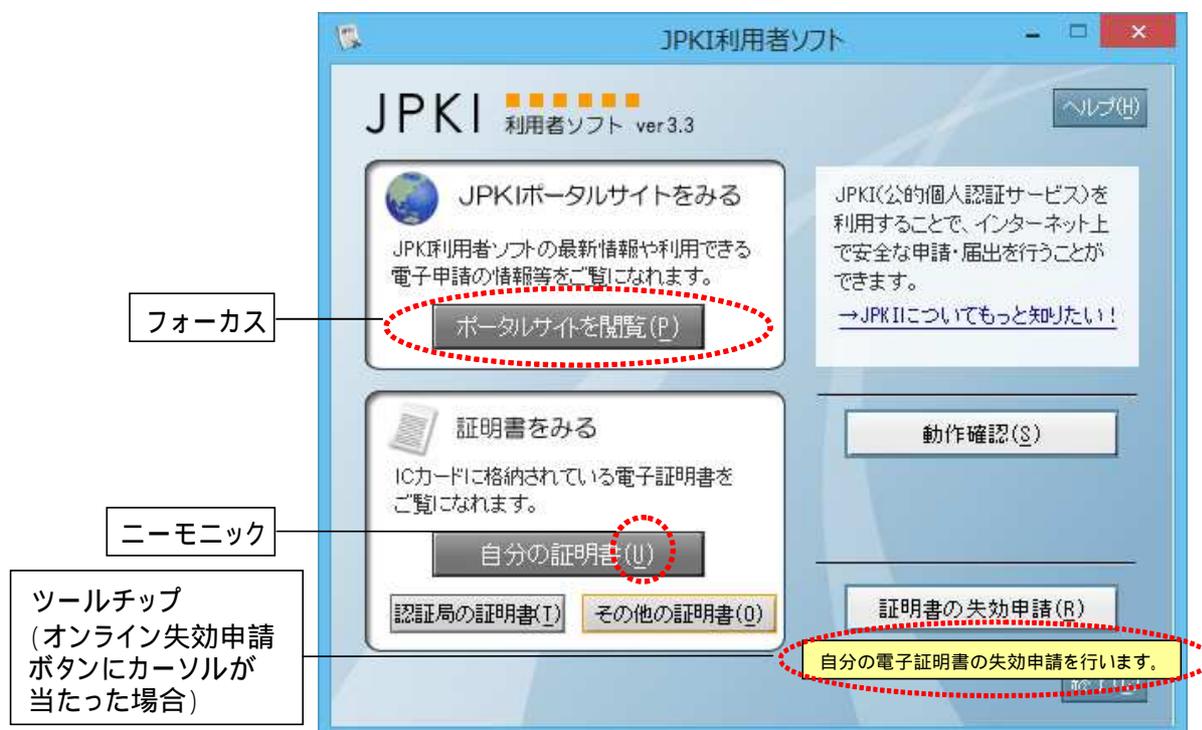


図 6-1 アクセシビリティ画面イメージ

3 詳細

初期フォーカスの設定

画面を表示した際に、フォーカス（ボタン等が選択されている状態）が設定されているコンポーネントの位置を設定する。

フォーカス順の設定

Tab ボタン押下時のフォーカスの順序を設定する。

主要コンポーネントに対するニーモニックの設定

主要コンポーネントに対してニーモニックを設定する。ニーモニックとは、メニューの中やボタンの中にある下線のついた（または括弧中の）文字のことである。ニーモニックは Alt キーを押しながらその文字を押すことで起動する。

コンポーネントに対するツールチップの設定

コンポーネントに対してツールチップを設定する。ツールチップとは、メニューやボタン等にカーソルを当てた際に一定時間表示される補助テキストのことである。

コンポーネントに対するユーザ補助の名称の設定

ボタンやテキストエディット等のコンポーネントに対してユーザ補助の名称を設定する。ユーザ補助の名称を設定することで、スクリーンリーダー（読み上げソフト）によってコンポーネントの名称を読み上げることが可能（スクリーンリーダーの設定に依存）となる。

コンポーネントに対するユーザ補助の説明の設定

ボタンやテキストエディット等のコンポーネントに対してユーザ補助の説明を設定する。Java モジュールの場合、ユーザ補助の説明（`accessibleDescription`）を設定することで、スクリーンリーダーによってコンポーネントに関する説明を読み上げることが可能（スクリーンリーダーの設定に依存）となる。

第2節 アクセシビリティ対応範囲

アクセシビリティ対応の対象となる画面を表示する機能は以下の通りである。なお、ファイル選択画面、ファイル保存画面等の OS 提供の標準部品や Java の標準部品を使用している画面については対象外とする（OS や Java のアクセシビリティ対応に依存する）。

- メニュー画面表示機能
- 電子証明書表示機能
- 官職証明書検証機能
- 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
- IC カードリーダーライタ設定機能（Windows 版のみ）
- Java ライブラリ登録機能
- 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

第 7 章 その他

第 1 節 JPKI 利用者ソフトのインストール機能

- (1) 利用者が設定する項目は必要最小限に留め、インストール時の利用者の負担を軽減させる。
- (2) アンインストール機能を設け、インストール時にコピーしたライブラリやユーティリティツールを全て削除する。
- (3) Windows 版の JPKI 利用者ソフトのインストーラは、32bit 環境 PC/64bit 環境 PC で共通のものとし、インストール実施後は 64bit 版、32bit 版両方のモジュールがインストールフォルダに展開される。
- (4) Windows 版の JPKI 利用者ソフトは、PC の 64bit 環境/32bit 環境を自動的に判別し、動的に適切なモジュールを選択するため、利用者は bit 環境の違いを意識することなく操作可能である。
- (5) MacOS 版(Ver2.5 以降)の JPKI 利用者ソフトは 64bit 環境対応版となり、対象環境において、利用者は bit 環境を意識することなく操作可能である。
- (6) インストール時、電子証明書の更新通知機能の有効、無効を選択可能とする。

第 2 節 IC カードに対するアクセス制御

JPKI 利用者ソフトは、上位アプリケーションが競合する環境下での利用が想定される。したがって、本ソフトウェアではパスワード認証無しでの IC カード利用を防止するため、以下のアクセス制御を行う。

<Windows 版>

- (1) IC カードに対するアクセス方法を排他モードとすることで、複数の上位アプリケーションからの同時アクセスを抑止する。
- (2) IC カードに対するログアウト処理をセッション単位で実装することで、不必要なログイン状態を防止する。

<MacOS 版(住基カード用)>

- (1) CSSM および Keychain Service を通じてのみ IC カードにアクセス可能とすることで、IC カードの不正利用等を防止する。

<MacOS 版(個人番号カード用)>

- (1) IC カードに対するアクセス方法を排他モードとすることで、複数の上位アプリケーションからの同時アクセスを抑止する。ただし、他のアプリケーションがすでに IC カードにアクセスしている場合は IC カードに対するアクセス方法を共有モードに切り替える。
- (2) IC カードに対するログアウト処理をセッション単位で実装することで、不必要なログイン状態を防止する。

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

第 4.3 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) Microsoft Windows および Internet Explorer は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- (2) Macintosh、Mac、MacOS、OS X および Safari は、米国およびその他の国で登録されている Apple Inc. の登録商標です。
- (3) Android は、Google Inc. の米国およびその他の国における登録商標です。
- (4) 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。