公的個人認証サービス

利用者クライアントソフト API 仕様書

【個人認証サービス AP C 言語インターフェース編】

第 4.6 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 のプラットフォームを追加
2.0 版	平成 18 年 5 月 2 日	・ 公的個人認証サービス利用者ソフト Ver2.0 のリリースに伴い、動作環境、ソフトウェア構成図を変更 ・ 表 4-1 実現可能な処理の一覧に自分の電子証明書の有効性確認機能を追加 ・ 第５章 第１節 サポート API 一覧の表 5-1 サポート API 一覧に JPKIConfirm を追加 ・ 第５章 第２節 サポート API 仕様詳細に（５）JPKIConfirm を追加 ・ 第５章 第４節 コーリングシーケンスに（４）有効性確認処理 を追加 ・ 表 6-1 画面一覧に[有効性確認]ボタンおよび[ファイル出力]ボタンを押下した場合の動作を追加 ・ 第６章 第２節 画面仕様詳細の画面レイアウトを変更 ・ 表 6-4 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
2.1 版	平成 18 年 11 月 1 日	・ MacOS 対応に伴い、第２章 ドキュメント体系、第３章 動作環境、第４章 第１節 ソフトウェア構成図を変更
2.2 版	平成 19 年 4 月 10 日	・ 表 3-1 動作環境を変更
2.3 版	平成 19 年 10 月 4 日	・ 表 3-1 動作環境 プラットフォームに WindowsVista, MacOS X 10.4.10, MacOS X 10.4.9 を追加 ・ 表 3-1 動作環境 Web ブラウザに Internet Explorer7.0 を追加
2.4 版	平成 20 年 10 月 10 日	・ 表 3-1 動作環境 プラットフォームに WindowsVista ServicePack1, WindowsXP ServicePack3, MacOS X 10.5.4, MacOS X 10.5.3, MacOS X 10.5.2, MacOS X 10.5.1, MacOS X 10.5, MacOS X 10.4.11 を追加。 ・ 表 3-1 動作環境 Web ブラウザに Internet Explorer6.0 ServicePack3 を追加。

版数	変更日付	変更内容
2.5 版	平成 23 年 04 月 01 日	・ 図 2-1 ドキュメント体系図**エラー! 参照元が見つかりません。**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、マトリクス形式の記述に変更。 ・ 表 3-1 動作環境(Windows)の OS に Windows 7(32/64 bit), WindowsVista ServicePack2 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。 ・ 図 4-1 ソフトウェア構成図(Windows 対応版)を変更。 ・ 第４章 第２節 実現可能な機能の一覧に使用するライブラリ名を追加。 ・ 第５章 第２節 サポート API 仕様詳細（５）JPKIConfirm の誤記を修正。
2.6 版	平成 25 年 12 月 01 日	第３章 動作環境 表 3-1 動作環境(Windows) Windows2000 を削除、Windows8(32/64bit)、Windows8.1(32/64bit)を追加 表 3-2 動作環境(MacOS) MacOS X 10.4.X, 10.5.X, 10.6.X を削除、MacOS X 10.7.5, OS X 10.8.4 を追加 ・ 第４章 第２節 実現可能な機能の一覧に MacOSX を追加。 ・ 第５章 第１節 サポート API 一覧に sha-356 対応する API の記載を追加 ・ 表 5-3 検証結果コード（certPathStatus）にアルゴリズム拒否のコードを追加。 ・ 第６章 第２節 （２）画面項目説明 ⑧に sha256 の表示を追加。 ・ 第６章 第２節 （４）画面項目説明 ⑥に sha256 の表示を追加。 ・ 表 6-8 証明書検証結果「無効」の場合のエラーコード一覧にアルゴリズム拒否のコードを追加。
3.0 版	平成 26 年 04 月 01 日	・ 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、組織名称を変更する。 ・ 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 07 月 01 日	・ 第３章　動作環境 表 ３-１ 動作環境(Windows) Windows XP を削除、Windows7(32/64bit)の Web ブラウザを IE10.0 から IE11.0 に変更、Windows 8(32/64bit)を削除、Windows 8.1 を Windows 8.1 update に変更 表 ３-２ 動作環境(MacOS) OS X 10.7.5 の Web ブラウザを Safari6.0 から Safari6.1 に変更、OS X 10.8.4 を OS X 10.8.5 に変更し、Web ブラウザを Safari6.0 から Safari6.1 に変更、OS X 10.9.3(64bit)、Web ブラウザに Safari7.0 を追加
4.0 版	平成 27 年 6 月 30 日	番号制度対応に伴い、以下を修正。 ・第１章　第１節　用語の定義を追加。 ・第２章　ドキュメント体系を修正。 ・第３章　動作環境を修正。 ・第４章　機能仕様を修正。 ・第５章　API 仕様を修正。 ・第６章　画面仕様を修正。 ・第４章　第１節　ソフトウェア構成図(MacOS 対応版)を修正。
4.0.1 版	平成 28 年 10 月 26 日	・第３章システム概要 動作環境　更新プログラムに係る注釈※3、4 の追加 ・第６章　第２節　画面仕様詳細　表 6-10　エラーコード一覧　No11-17 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
4.1 版	平成 28 年 11 月 30 日	PC 接続機能追加対応に伴い、以下を修正。 ・第１章　第１節の「用語の定義」に以下を追加。 ➢ PC/SC ➢ IC カードリーダライタ ➢ 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 表 3-1 および表 3-2 に PC 接続機能対応可否追加。 ・第３章 表 3-1 に Windows 10(32/64bit)を追加。 ・第３章 表 3-3 動作環境(共通)を表 3-3 動作環境(IC カード)、第１節 PC/SC 対応 IC カードリーダライタ、第 2 節 Android 端末に分割。 ・第４章 第１節 ソフトウェア構成図に Bluetooth 通信を追加。

版数	変更日付	変更内容
4.2 版	平成 29 年 07 月 31 日	Java9 対応に伴い、以下を修正。 ・第２章 ドキュメント体系図を改訂。 ・第３章 表 ３-１の OS から Windows Vista(32bit)を削除。 ・第３章 表 ３-１の OS から Windows 8(32bit)を削除。 ・第３章 表 ３-１の OS から Windows 8(64bit)を削除。 ・第３章 表 ３-１の JavaVM に JRE9 を追加。 ・第３章 表 ３-２の OS から OS X 10.8, 10.9 を削除。 ・第３章 表 ３-２の OS に OS X 10.11, macOS v10.12 を追加。 ・第３章 表 ３-２の JavaVM に JRE9 を追加。 ・※２に説明文を追記。 ・第３章 表 ３-５の【PC 接続の場合】に Android 6.0.1、7.0 を追加。 ・第３章 表 ３-５の【Android 単体で利用する場合】に Android 6.0.1、7.0 を追加。
4.3 版	令和元年 5 月 1 日	・第３章 表 ３-２の OS から OS X 10.11 を削除。 ・第３章 表 ３-２の OS に macOS v10.13 を追加。 ・第３章 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。 新元号対応に伴い、以下を修正。 ・第５章　第３節　構造体仕様の生年月日の設定ルールに新元号を追加。 ・第６章　第２節　画面仕様詳細の※2 生年月日の設定ルールに新元号を追加。 旧氏対応に伴い、以下を修正。 ・第５章　第３節　構造体仕様に旧氏に関する記述を追加。 ・第６章　第２節　画面仕様詳細に旧氏に関する記述を追加。

版数	変更日付	変更内容
4.4 版	令和 2 年 3 月 31 日	MacOS 版における開発言語(Java)変更対応に伴い、以下を修正。 ・第３章 表３-２を修正。 macOS v10.12、v10.13 を削除。 macOS v10.14、macOS v10.15(Web ブラウザは Safari 13)を追加。 ・第４章 第１節 図４-２ ソフトウェア構成図(MacOS 対応版)から個人認証サービス AP C 言語 I/F から個人認証サービス AP JavaI/F の呼び出しを削除。 ・第６章 第２節（６） 表６-９エラーコード 300100 の「環境設定ファイルのプロキシ情報の指定」を「システムのプロキシ情報の指定」に修正。 Mac 版における住基カードサポート廃止に伴い、以下を修正。 ・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。 ・第３章 表３-２ ※２の注釈を削除。 ・第３章 表３-３ MacOS 版を使用する場合は個人番号カードのみ対応である旨を追加。 ・第４章 第１節 図４-２ ソフトウェア構成図(MacOS 対応版)から Keychain Services 及び CSSM を削除。 ・第５章 第２節（３）表５-２ JPKI_CVS_FALSE_CL_GETCERT に MacOS 版の場合は住基カードが利用されている場合に本エラーが発生する旨の注釈を追加。 ・第５章 第２節（５）表５-５ JPKI_CLIENT_ICCARD_NOT_READY に MacOS 版の場合は住基カードが利用されている場合に本エラーが発生する旨の注釈を追加。 ・第６章 第２節（６） 表６-９エラーコード 300400 に MacOS 版の場合は IC カードリーダライタに住基カードが設定されている場合に本エラーが発生する旨の注釈を追加。 ・第６章 第２節（７）表６-１０エラーコード 300704 に MacOS 版の場合は住基カードが利用されている場合に本エラーが発生する旨の注釈を追加。 ブラウザ対応版、iOS 版のリリースに伴い、以下を修正。 ・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。 ・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。 ・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。 ・第２章 ドキュメント体系 「API 仕様書 iOS Framework 編」を追加。 ・第３章 第２節 動作環境に Android9.0、10.0 を追加。 Windows 7 サポート終了に伴い、以下を修正。 ・第３章 表３-１を修正。 Windows 7(32bit)、Windows 7(64bit)および※3 を削除。

版数	変更日付	変更内容
4.5 版	令和 3 年 3 月 31 日	ブラウザ対応版(Android)のリリースに伴い、以下を修正 ・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。 ・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。
4.5.1 版	令和 3 年 3 月 31 日	InstallShield2022 対応に伴い、第３章　動作環境の記載を修正。
4.6 版	令和 6 年 4 月 15 日	Mac OS 版 Ver3.7 のリリースに伴い、以下を修正 ・第１章　第１節　用語の定義の記載を修正。 ・第３章　動作環境の記載を修正。

－ 目次 －

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)における個人認証サービス AP は、以下の機能を実現するための Application Program Interface(以下、API)を提供する。

- 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
- 自分の電子証明書の有効性確認機能
- IC カード種別取得機能

以降、本書では個人認証サービス AP のうち、C 言語インターフェースの API 仕様について説明する。

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、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	署名用電子証明書	公的個人認証サービスで発行した署名用途の利用者の電子証明書。 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
5	利用者証明用電子証明書	公的個人認証サービスで発行した利用者証明用途の利用者の電子証明書。 本書では以下の電子証明書を指す。 ・個人番号カードに格納された利用者証明用電子証明書
6	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
7	利用者秘密鍵	公開鍵暗号方式において用いられる鍵ペアの一方。公開鍵に対する、利用者のみが保有する鍵。 本書では以下の秘密鍵を指す。 ・住基カードに格納された署名用利用者秘密鍵 ・個人番号カードに格納された署名用利用者秘密鍵 ・個人番号カードに格納された利用者証明用利用者秘密鍵
8	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
9	PC/SC	Personal Computer/Smart Card の略。
10	IC カードリーダライタ	以下の機器を指す総称 ・PC/SC 対応 IC カードリーダライタ ・Android 端末
11	挿入	IC カードリーダライタが 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 カードリーダライタに 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
12	NFC	Near Field Communication　(近距離無線通信)の略。
13	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。

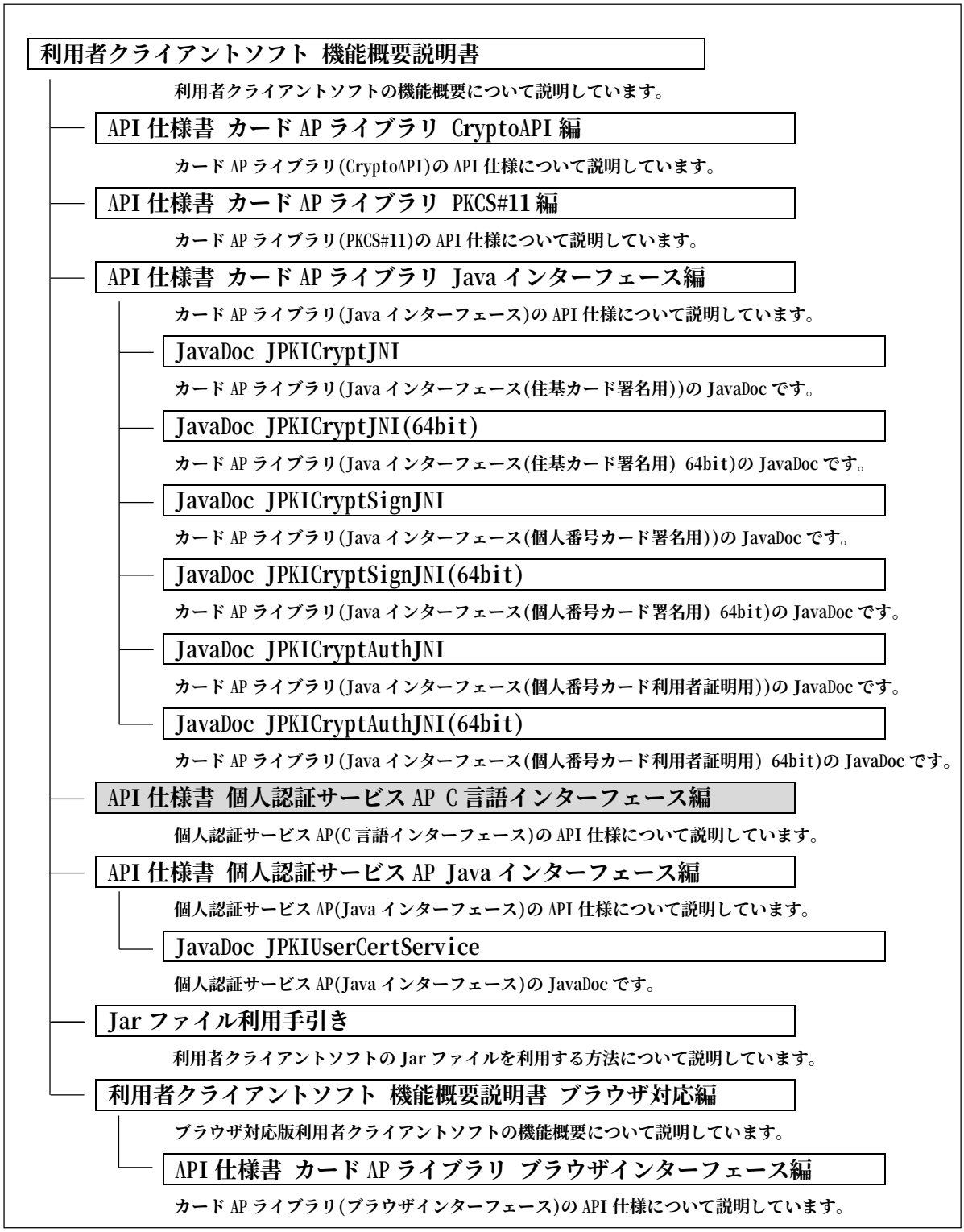


図 2-1 ドキュメント体系図(PC 版)

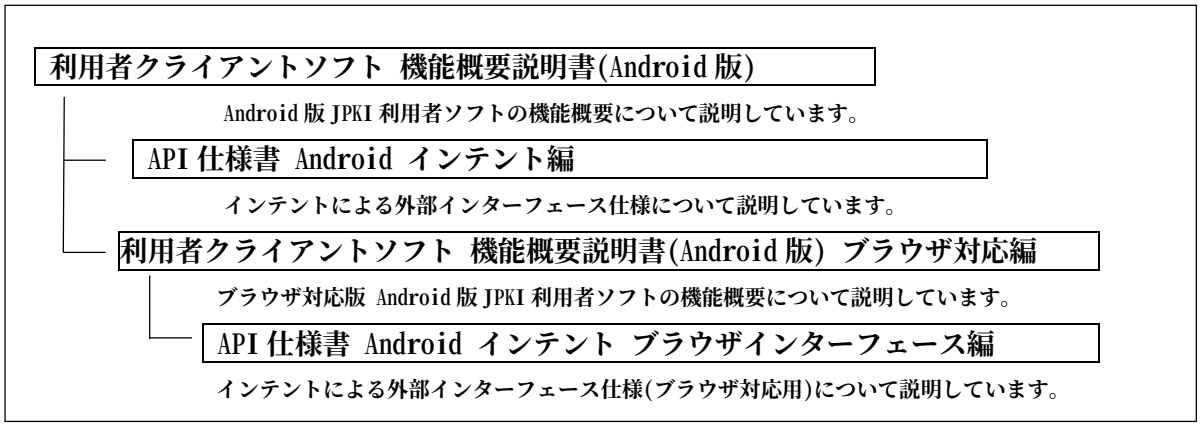


図 2-1 ドキュメント体系図(Android 版)

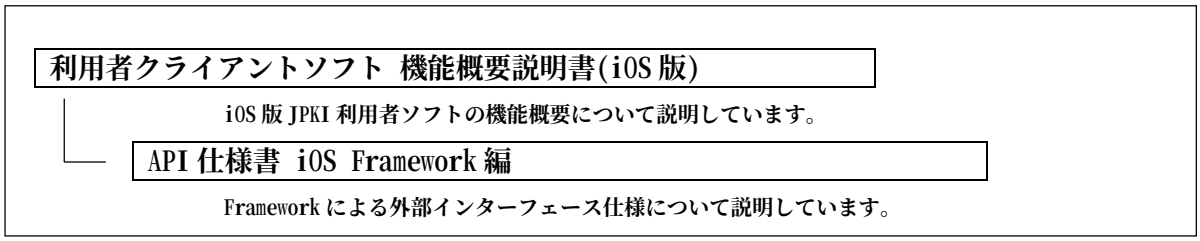


図 2-2 ドキュメント体系図(iOS 版)

第３章　動作環境

個人認証サービス AP(C 言語インターフェース)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) JRE8.0	PC 接続機能対応可否(※3)
Windows 10 Home/Pro (32bit/64bit)	Edge	○	○
Windows 11 Home/Pro	Edge	○	○

※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。
また、最新の動作環境に掲載された OS、Web ブラウザ、JavaVM 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。

※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 Microsoft Edge(カード AP ライブラリ（Java インタフェース編）の場合、IE モード)が必要。

※3 PC 接続機能については「利用者クライアントソフト 機能概要説明書 第３章 第３節 PC 接続機能について」を参照。

表 3-2 動作環境(MacOS)

OS(※1)	Web ブラウザ (※1)	JavaVM(※1) JRE8.0	PC 接続機能対応可否 (※2)
macOS 13 Ventura	Safari 16	○	×
macOS 14 Sonoma	Safari 17	○	×

※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。
また、最新の動作環境に掲載された OS、Web ブラウザ、JavaVM 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。

※2 PC 接続機能については「利用者クライアントソフト 機能概要説明書 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。 ※MacOS 版を使用する場合は個人番号カードのみ対応。

第１節　PC/SC 対応 IC カードリーダライタ

PC/SC 対応 IC カードリーダライタ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 カードリーダライタ)

項目	条件
PC/SC 対応 IC カードリーダライタ	以下の条件を満たす PC/SC 対応 IC カードリーダライタとする。(「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一覧」(※1)を参照のこと。) ・ 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 カードリーダライタであること。 ・ 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 カードリーダライタ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　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。) ・Android　8.0、9.0、10.0、11.0 または 12.0 を搭載していること。 ・Bluetooth 4.2 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。

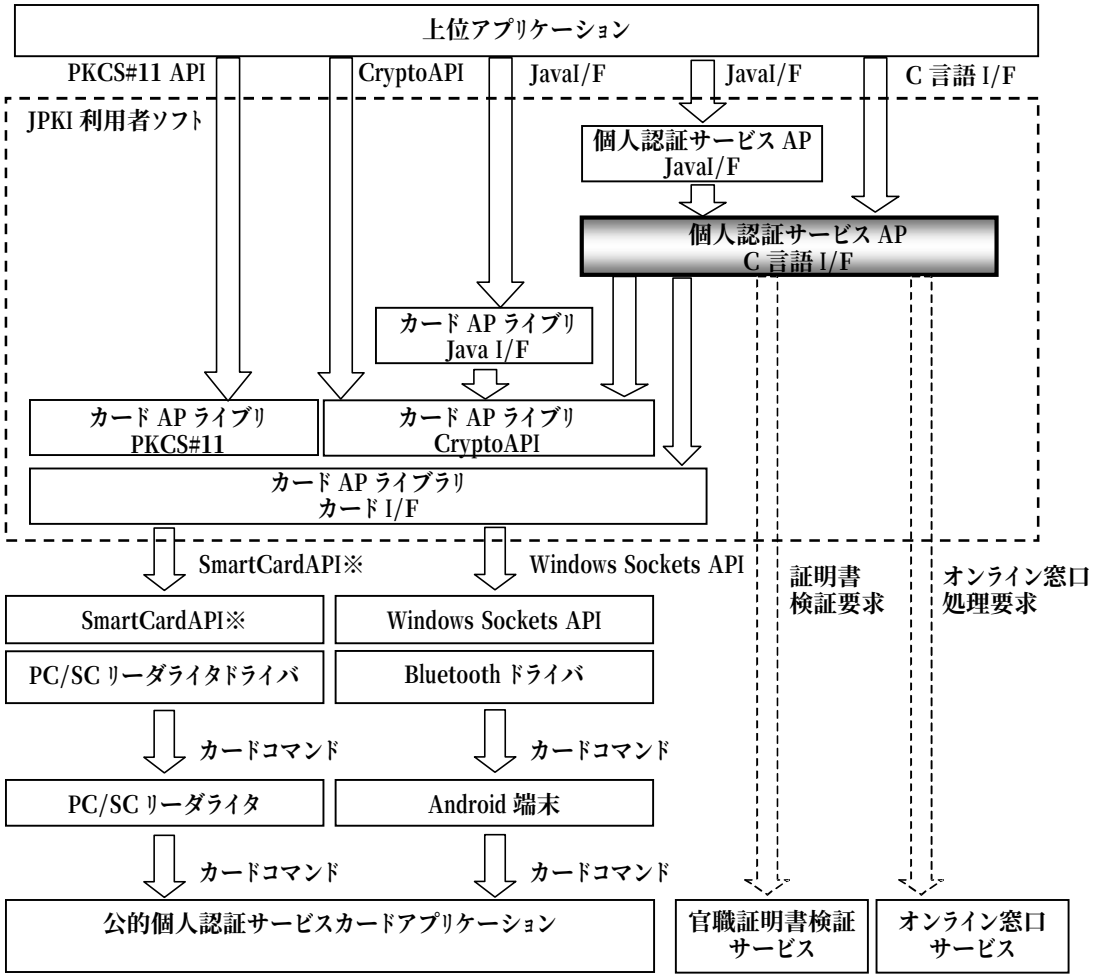
※　最新の「個人番号カード対応適合性検証済み Android 端末一覧」の情報は、JPKI ポータルサイトに掲載するものとする。
また、最新の動作環境に掲載された OS 以外を使用した場合の不具合等に関するお問い合わせは、サポート対象外とする。

第４章　機能仕様

第１節　ソフトウェア構成図

本仕様書では、JPKI 利用者ソフトのうち、下図の太枠に示す個人認証サービス AP(C 言語インターフェース)の仕様をまとめる。

＜Windows 対応版＞



※ Smart Card Resource Manager API の略

図 4-1 ソフトウェア構成図(Windows 対応版)

＜MacOS 対応版＞

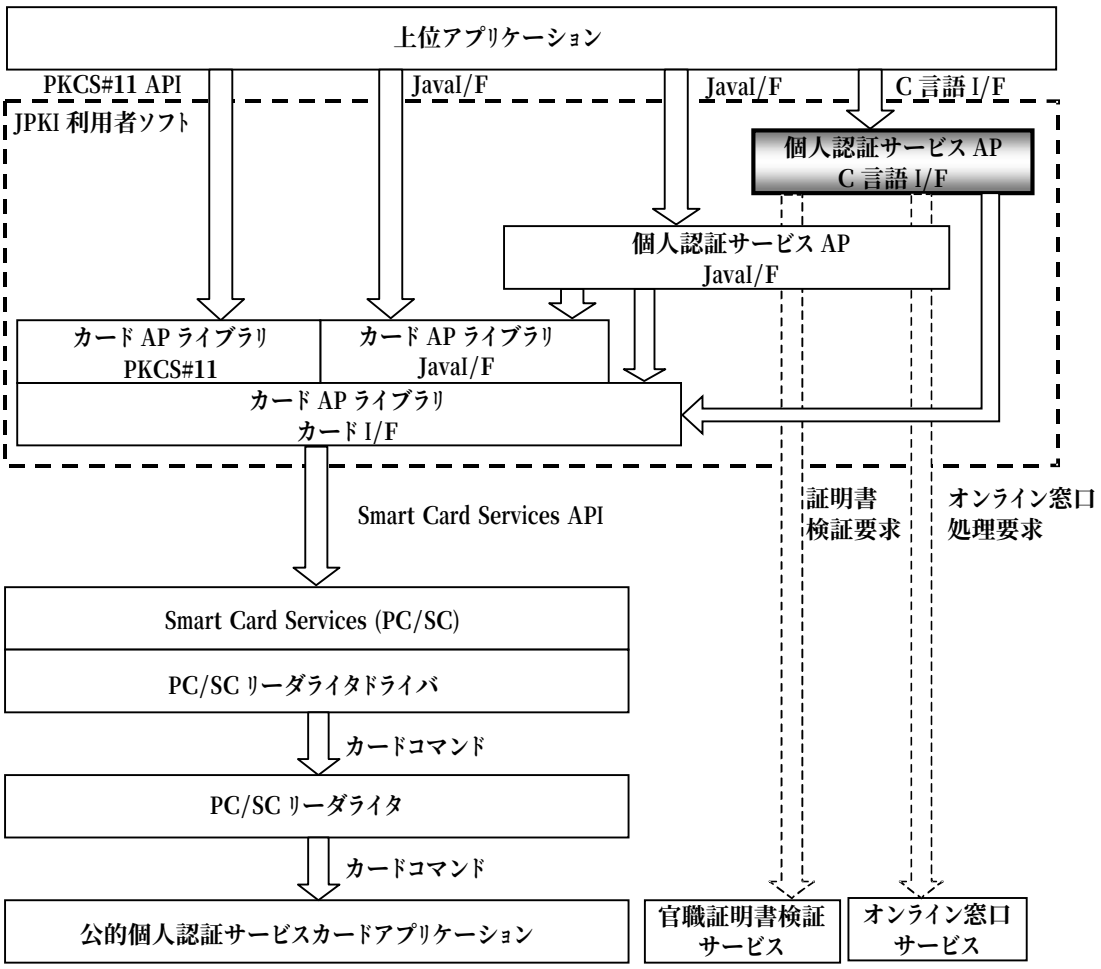


図 4-2 ソフトウェア構成図（MacOS 対応版）

第２節　実現可能な機能の一覧

個人認証サービス AP(C 言語インターフェース)で実現可能な機能の一覧を表 ４-１に示す。

表 ４-１ 実現可能な処理の一覧

NO	機能	概要
1	証明書表示	電子証明書を証明書 Viewer で表示する。
2	基本 4 情報取得	署名用電子証明書から基本 4 情報(氏名、住所、性別、生年月日)を取得する。
3	官職証明書検証	官職証明書や職責証明書の証明書検証を行うため、公的個人認証サービスセンターにある官職証明書検証サービスに対して証明書検証要求を発行する。
4	自分の電子証明書の有効性確認	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センターにあるオンライン窓口サービスに対して有効性確認要求を発行する。
5	IC カード種別取得	IC カードリーダライタに挿入されている IC カードの種別を取得する。

個人認証サービス AP(C 言語インターフェース)の機能は、以下のライブラリで提供する。

＜Windows 対応版＞

32bit 版：(インストールフォルダ)¥JPKIServiceAPI.dll

64bit 版：(インストールフォルダ)¥JPKIServiceAPI64.dll

＜Mac OS 対応版＞

64bit 版：/usr/local/lib/JPKIServiceAPI.dylib

第５章　API 仕様

第１節　サポート API 一覧

サポート API 一覧を表 ５-１に示す。

表 ５-１ サポート API 一覧

NO	API 名	概要
1	JPKICertViewDialog	電子証明書を表示する。
2	JPKIGetBasicData	署名用電子証明書から基本 4 情報を取得する。
3	JPKICertValid	官職証明書の証明書検証を行う。
4	JPKIFreeBasicData	基本 4 情報の格納領域を解放する。
5	JPKIConfirm	自分の電子証明書(利用者証明書)の有効性確認を行う。
6	JPKIGetCardType	IC カードリーダライタに挿入されている IC カードの種別を取得する。

※住基カード利用時は NO.1,3 について sha-256 の官職証明書・職責証明書の表示・検証に対応済み。

※個人番号カード利用時は NO.1,3,5 について sha-256 の官職証明書・職責証明書の表示・検証、sha256 の利用者証明書の有効性確認に対応済み。

第２節　サポート API 仕様詳細

（1）JPKICertViewDialog

API 名	JPKICertViewDialog		
概要	電子証明書を表示する。		
関数インターフェース	int JPKICertViewDialog (　　JPKI_CertBinaryData　　*certData);		
	値		内容
戻り値	JPKI_USER_TRUE		正常終了。
	JPKI_USER_FALSE_INVALID_PARAM		引数に不正な値が設定されていた。
	JPKI_USER_FALSE_MEMORY		メモリが不足している。
	JPKI_USER_FALSE_DECODE_CERT		証明書のデータの解析に失敗した。
	JPKI_USER_FALSE_SHOW_VIEWER		ダイアログの表示に失敗した。
	JPKI_USER_FALSE_OTHER		その他システムエラーが発生した。
	型	I/O	内容
引数	JPKI_CertBinaryData *	IN	電子証明書データ(DER 形式)

（2）JPKIGetBasicData

API 名	JPKIGetBasicData		
概要	署名用電子証明書から基本 4 情報を取得する。		
関数インターフェース	int JPKIGetBasicData (　　JPKI_CertBinaryData　　*certData, 　　JPKI_BasicData　　*basicData);		
	値		内容
戻り値	JPKI_USER_TRUE		正常終了。
	JPKI_USER_FALSE_INVALID_PARAM		引数に不正な値が設定されていた。
	JPKI_USER_FALSE_MEMORY		メモリが不足している。
	JPKI_USER_FALSE_DECODE_CERT		証明書のデータの解析に失敗した。
	JPKI_USER_FALSE_OTHER		その他システムエラーが発生した。
	型	I/O	内容
引数	JPKI_CertBinaryData *	IN	署名用電子証明書データ(DER 形式)
	JPKI_BasicData *	OUT	基本 4 情報

（3）JPKICertValid

API 名	JPKICertValid		
概要	官職証明書の証明書検証を行う。		
関数インターフェース	int JPKICertValid (JPKI_CertBinaryData *certData, int *certPathStatus, int *responseStatus);		
戻り値	int（表 5-2 検証結果コード（戻り値）参照）		
	型	I/O	内容
引数	JPKI_CertBinaryData *	IN	検証対象証明書データ(DER 形式)
	int *	OUT	証明書検証（認証パスの構築および検証）の結果コード (表 5-3 検証結果コード（certPathStatus）参照)
	int *	OUT	OCSP レスポンスステータス (表 5-4 検証結果コード（responseStatus）参照)

表 5-2 検証結果コード（戻り値）

#	Define シンボル(定義名)	区分※1	意味
1	JPKI_CVS_OK	-	証明書検証に成功した。 この戻り値を返却する場合、以下の値が設定される。 certPathStatus … 0（有効） responseStatus … 0（OCSP Request が正しく処理された）
2	JPKI_CVS_NG	-	証明書検証に失敗した。 この戻り値が返却された場合、certPathStatus に官職証明書検証サーバ(CVS)が返却した検証結果コードが設定される。
3	JPKI_CVS_FALSE_CL_MEMORY	C	メモリの確保に失敗した。
4	JPKI_CVS_FALSE_CL_INVALID_PARAM	C	引数に設定した値が間違っている。
5	JPKI_CVS_FALSE_CL_OTHER	C	システム関数起因によるエラーが発生。
6	JPKI_CVS_FALSE_CL_CREATE_REQUEST	C	OCSP Request および拡張情報の生成に失敗した。または、リクエスト署名の生成に失敗した。
7	JPKI_CVS_FALSE_CL_HTTP	C	HTTP または HTTPS 通信で失敗した。
8	JPKI_CVS_FALSE_SV_DECODE	S	OCSP Response(ASN.1 エンコード形式)のデコードに失敗した。
9	JPKI_CVS_FALSE_SV_RESPONSE_EXCEPTION	S	官職証明書検証サーバ(CVS)で例外が発生した。 この戻り値が返却された場合、responseStatus に官職証明書検証サーバ(CVS)が返却したステータスが設定される。

#	Define シンボル(定義名)	区分※1	意味
10	JPKI_CVS_FALSE_SV_SIGN_VERIFY_SIGNATURE	S	官職証明書検証サーバ(CVS)から受信した OCSP Response(ASN.1 エンコード形式)の署名検証に失敗した。
11	JPKI_CVS_FALSE_SV_NONCE	S	Request 送信時に付与した nonce と Response に含まれる nonce※2 が一致しない場合に返却する。
12	JPKI_CVS_FALSE_SV_CERT_VERYFY	S	CVS 証明書の証明書検証に失敗した。
13	JPKI_CVS_FALSE_SV_ANALYZE	S	証明書検証結果の解析に失敗した。
14	JPKI_CVS_FALSE_CL_CVSURL	C	官職証明書検証サーバ(CVS)の URL が不正の場合に返却する。
15	JPKI_CVS_FALSE_CL_GETCERT	C	IC カードから証明書(利用者証明書または認証局の自己署名証明書)の取得に失敗した。※3

(※1) 区分　C:クライアント側エラー　S:サーバ側エラー

（※2）nonce

官職証明書検証サーバ(CVS)に検証を依頼するために送信した Request とその結果として返ってきた Response が真に対応しているかどうかを確認する為に、送信時に Request に付与する 1 から 33 バイトの乱数。Request に付与した nonce と、Response に含まれる nonce が一致すれば送信した Request に対する Response であると確認される。

（※3）MacOS 版の場合、住基カードが利用されている場合にも本エラーが発生する。

表 5-3 検証結果コード（certPathStatus）

#	Define シンボル(定義名)	値	内容	解説
1	JPKI_CVS_GOOD	0	有効	認証パスの構築が成功し検証結果が正しい
2	JPKI_CVS_INTERNAL_PATH_CONSTRUCTION_ERROR	101	認証パス構築不可	認証パス構築ができない
3	JPKI_CVS_SIGNATURE_VERIFICATION_FAILURE	202	署名不正	認証パスに署名が不正である証明書が含まれる
4	JPKI_CVS_ONE_OR_MORE_CERTIFICATES_ARE_REVOKED	203	失効証明書を含む	認証パスに失効した証明書が含まれる
5	JPKI_CVS_POLICY_MAPPING_ERROR	204	ポリシー不一致	認証パスにポリシーが一致しない証明書が含まれる
6	JPKI_CVS_CONSTRAINTS_ERROR	205	制約違反	認証パスに制約に違反している証明書が含まれる
7	JPKI_CVS_CERTSTATUS_OF_OCSP_RESPONSE_IS_UNKNOWN	206	OCSP での証明書検証確認不正	認証パスに OCSP での certStatus が unknown と応答される証明書が含まれる
8	JPKI_CVS_REJECTED_BY_ALGORITHM_EE	301	アルゴリズム拒否	官職証明書検証サーバ(CVS)側で検証対象証明書の受け付けを拒否した

#	Define シンボル(定義名)	値	内容	解説
9	JPKI_CVS_REJECTED_BY_ALGORITHM_CA	302	アルゴリズム拒否	官職証明書検証サーバ(CVS)側で中間証明書または認証局の自己署名証明書の受け付けを拒否した
10	JPKI_CVS_REJECTED_A_REQUEST	901	要求受付け拒否	官職証明書検証サーバ(CVS)側で要求の受け付けを拒否した
11	JPKI_CVS_VALIDATION_TIMEOUT	902	タイムアウト	要求がタイムアウトとなった

表 5-4 検証結果コード（responseStatus）

#	Define シンボル(定義名)	値	内容	解説
1	JPKI_CVS_RESSTATUS_SUCCESSFUL	0	成功	OCSP Request が正しく処理された
2	JPKI_CVS_RESSTATUS_MALFORMEDREQUEST	1	エラー	OCSP Request のフォーマットエラー
3	JPKI_CVS_RESSTATUS_INTERNALERROR	2	エラー	内部エラー
4	JPKI_CVS_RESSTATUS_TRYLATER	3	エラー	一時的な解答不能
5	JPKI_CVS_RESSTATUS_SIGREQUIRED	5	エラー	OCSP Request への署名が必要
6	JPKI_CVS_RESSTATUS_UNAUTHORIZED	6	エラー	クライアントが認証されていない

（4）JPKIFreeBasicData

API 名	JPKIFreeBasicData		
概要	基本 4 情報の格納領域を解放する。		
関数インターフェース	int JPKIFreeBasicData (JPKI_BasicData *basicData);		
	値		内容
戻り値	JPKI_USER_TRUE		正常終了。
	JPKI_USER_FALSE_INVALID_PARAM		引数に不正な値が設定されていた。
	型	I/O	内容
引数	JPKI_BasicData *	IN	基本 4 情報

（5）JPKIConfirm

API 名	JPKIConfirm		
概要	自分の電子証明書(利用者証明書)の有効性確認を行う。		
関数インターフェース	int JPKIConfirm (JPKI_CertBinaryData *certData);		
	値		内容
戻り値	JPKI_USER_FALSE_INVALID_PARAM		引数に不正な値が設定されていた。
	JPKI_USER_FALSE_MEMORY		メモリが不足している。
	JPKI_USER_FALSE_OTHER		その他システムエラーが発生した。
	int(表 5-5 有効性確認結果コード(戻り値)参照)		
	型	I/O	内容
引数	JPKI_CertBinaryData *	IN	利用者証明書データ(DER 形式)

表 5-5 有効性確認結果コード(戻り値)

#	Define シンボル(定義名)	値	解説
1	JPKI_CONFIRM_OK	200	有効性確認結果が有効である。
2	JPKI_SERVER_VERIFY_ERROR	600	申請書の電子証明書検証エラーが発生した。
3	JPKI_SERVER_APPLY_ERROR	601	オンライン窓口サーバで「申請情報取込エラー」が発生した。
4	JPKI_SERVER_EXPIRED_ERROR	602	オンライン窓口サーバで「対象とする証明書の有効期限切れエラー」が発生した。
5	JPKI_SERVER_DATA_ERROR	603	オンライン窓口サーバで「受信データ形式エラー」が発生した。
6	JPKI_SERVER_ISSUER_ERROR	604	オンライン窓口サーバで「対象とする証明書の認証局の電子署名検証エラー」が発生した。
7	JPKI_SERVER_VALIDITY_ERROR	605	オンライン窓口サーバで「対象とする証明書の有効性確認エラー」が発生した。
8	JPKI_SERVER_OCSP_ERROR	606	オンライン窓口サーバで「対象とする証明書のオンライン窓口エラー(OCSP)」が発生した。
9	JPKI_SERVER_REVOKED_ERROR	607	対象とする証明書が失効済みである。
10	JPKI_SERVER_APPLYED_ERROR	608	対象とする証明書が失効申請済みである。
11	JPKI_SERVER_DB_ERROR	609	オンライン窓口サーバで「オンライン窓口エラー(DB)」が発生した。
12	JPKI_SERVER_JAM_ERROR	611	オンライン窓口サーバが混雑している。
13	JPKI_SERVER_OTHER_ERROR	612	オンライン窓口サーバでエラーが発生した。

#	Define シンボル(定義名)	値	解説
14	JPKI_SERVER_HOLD_ERROR	613	対象とする証明書が一時保留状態である。
15	JPKI_SERVER_CERT_UNMATCH_ERROR	622	オンライン窓口サーバで「対象とする証明書と署名実施証明書の不一致エラー」が発生した。
16	JPKI_CLIENT_LOGIN_CANCEL	700	ログインのキャンセル。
17	JPKI_CLIENT_NOMEMORY	701	メモリ不足が発生した。
18	JPKI_CLIENT_UNEXPECTED_ERR	702	予期せぬエラーが発生した。
19	JPKI_CLIENT_ICCARD_BLOCKED	703	IC カードがロックされている。
20	JPKI_CLIENT_ICCARD_NOT_READY	704	IC カードに接続できない。※1
21	JPKI_CLIENT_FALSE_DECODE_CERT	705	対象とする証明書の解析失敗。
22	JPKI_CLIENT_ONLINE_TIME	706	サーバ時刻の取得に失敗。
23	JPKI_CLIENT_HTTP_NOT_ACCESS	707	オンライン窓口サーバへのアクセスに失敗。
24	JPKI_CLIENT_EXPIRED_ERROR	708	対象とする証明書の有効期限切れ。
25	JPKI_CLIENT_NOT_YET_VALID	709	対象とする証明書の有効期限開始の日付が未来の日時。
26	その他	100～500 (200 を除く)	HTTP1.1 ステータスコード(100～500 番台)。

（※1）MacOS 版の場合、住基カードが利用されている場合にも本エラーが発生する。

（6）JPKIGetCardType

API 名	JPKIGetCardType		
概要	IC カードリーダライタに挿入されている IC カードの種別を取得する。		
関数インターフェース	int JPKIGetCardType(JPKI_CardType *cardType);		
	値		内容
戻り値	JPKI_USER_TRUE		正常終了
	JPKI_USER_FALSE_INVALID_PARAM		引数に不正な値が設定されていた。
	JPKI_USER_FALSE_ICCARD_NOT_READY		R/W 接続不備、IC カード未挿入等のため IC カードに接続できない。
	JPKI_USER_FALSE_OTHER		その他システムエラーが発生した。
	型	I/O	内容
引数	JPKI_CardType *	OUT	カード種別

第３節　構造体仕様

（1）JPKI_CertBinaryData

構造体名		JPKI_CertBinaryData		
概要		電子証明書情報を格納する構造体。		
NO	変数名	型	値	備考
1	len	unsigned long	電子証明書データ長	
2	data	unsigned char *	電子証明書データの格納先ポインタ	DER 形式とする。

（2）JPKI_BasicData

構造体名		JPKI_BasicData		
概要		基本 4 情報を格納する構造体。		
NO	変数名	型	値	備考
1	name	wchar_t *	氏名	UNICODE 大括弧「［］」内は旧氏を示す。 括弧「( )」内は通称を示す。
2	address	wchar_t *	住所	UNICODE
3	gender	char *	性別	性別コード。 1:男　2:女　3:不明
4	dateOfBirth	char *	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)
5	substituteCharacterOfName	char *	代替文字の使用（氏名）	name と同じ文字数の文字列。代替文字と同じ位置に 1、その他に 0 が入る。
6	substituteCharacterOfAddress	char *	代替文字の使用（住所）	address と同じ文字数の文字列。代替文字と同じ位置に 1、その他に 0 が入る。

（3）JPKI_CardType

構造体名		JPKI_CardType		
概要		IC カード種別情報を格納する構造体。		
NO	変数名	型	値	備考
1	id	int	カード種別	カード種別コード 0:不明 1:住基カード 2:個人番号カード
2	tokenInfo	unsigned char[32]	TOKEN 情報	TOKEN 情報 (サイズ 32byte、null 終端無し) 住基カードの場合： "JPKIAPICCTOKEN△△△△△△△△△△△△△△△△" 個人番号カードの場合： "JPKIAPICCTOKEN2△△△△△△△△△△△△△△△△" ※△は半角スペースを表す

第４節　コーリングシーケンス

「第４章　第２節　実現可能な機能の一覧」を実現するためのコーリングシーケンスを以下に示す。上位アプリケーションは、このコーリングシーケンスに沿って実装すること。

（1）証明書表示処理

電子証明書を DER 形式で取得	
↓	
JPKICertViewDialog	電子証明書の表示 certData: 電子証明書格納領域アドレス

（2）基本 4 情報取得処理

署名用電子証明書を DER 形式で取得	
↓	
JPKIGetBasicData	基本 4 情報の取得 certData: 署名用電子証明書格納領域アドレス basicData: 基本 4 情報格納領域アドレス
↓	
basicData から必要情報の取得	
↓	
JPKIFreeBasicData	基本 4 情報格納領域の解放 basicData: 基本 4 情報格納領域アドレス

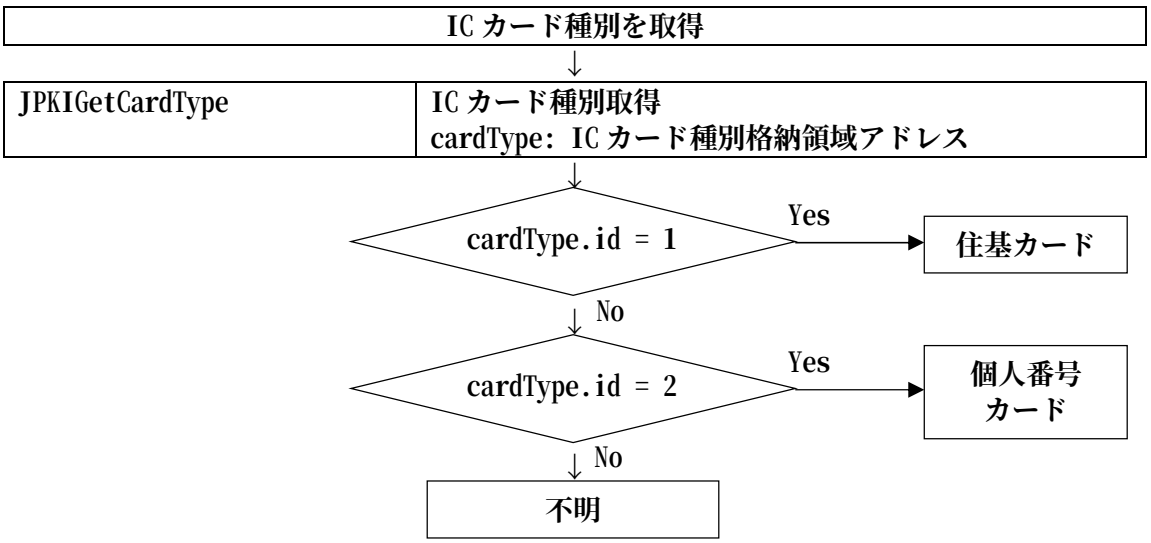
（3）官職証明書検証処理

官職証明書や職責証明書を DER 形式で取得	
↓	
JPKICertValid	官職証明書や職責証明書の証明書検証 certData: 電子証明書格納領域アドレス certPathStatus: 証明書検証（認証パスの構築および検証）の結果コード格納領域アドレス responseStatus: OCSP レスポンスステータス格納領域アドレス
↓	
結果コードの解析	

（4）有効性確認処理

利用者証明書を DER 形式で取得	
↓	
JPKIConfirm	自分の電子証明書(利用者証明書)の有効性確認 certData: 利用者証明書格納領域アドレス
↓	
結果コードの解析	

（5）IC カード種別取得処理



第６章　画面仕様
第１節　画面一覧

表 6-1 画面一覧

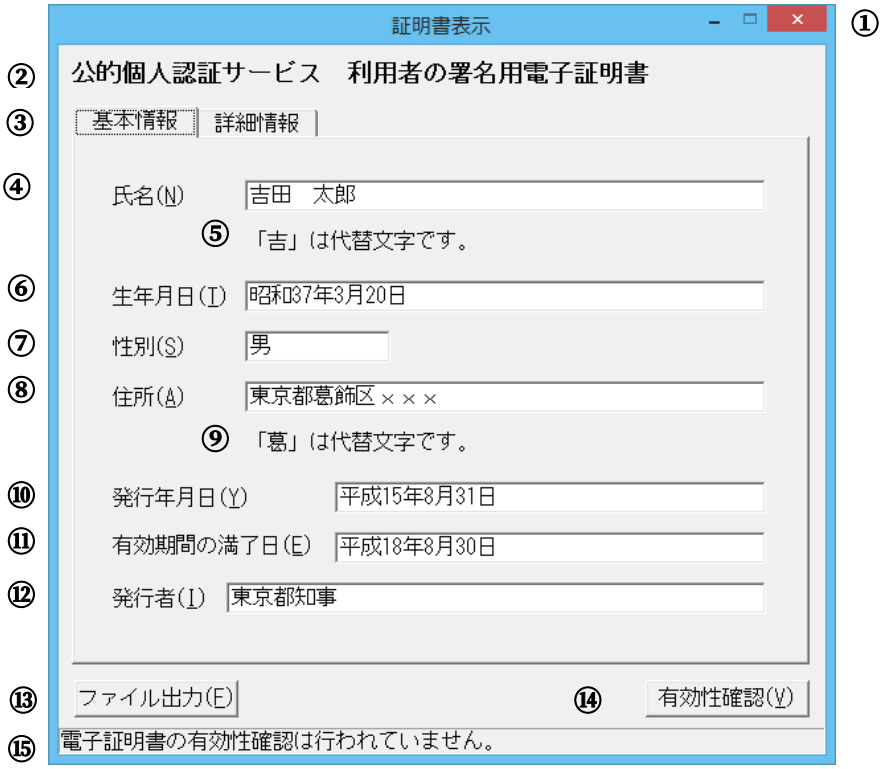
NO	機能名	画面名		概要
1	証明書表示機能	基本画面	署名用電子証明書	署名用電子証明書の基本情報を表示する。 [有効性確認]ボタンの押下により、自分の電子証明書の有効性確認を行う。 [ファイル出力]ボタンの押下により、電子証明書の内容をファイルに出力する。
2			利用者証明用電子証明書	利用者証明用電子証明書の基本情報を表示する。 [有効性確認]ボタンの押下により、自分の電子証明書の有効性確認を行う。 [ファイル出力]ボタンの押下により、電子証明書の内容をファイルに出力する。
3			認証局の自己署名証明書	認証局の自己署名証明書(ルート認証局の自己署名証明書,リンク証明書,下位認証局の自己署名証明書,相互認証証明書,自己署名証明書等)の基本情報を表示する。 [ファイル出力]ボタンの押下により、電子証明書の内容をファイルに出力する。
4			その他の電子証明書	上記以外の証明書(官職証明書,職責証明書,その他の証明書）の基本情報を表示する。 [証明書検証]ボタン押下により、証明書の検証を行う。 [ファイル出力]ボタンの押下により、電子証明書の内容をファイルに出力する。
5		詳細画面		電子証明書内の全ての記載事項を表示する。 署名用電子証明書または利用者証明用電子証明書の場合、[有効性確認]ボタンの押下により、自分の電子証明書の有効性確認を行う。 その他の電子証明書の場合、[証明書検証]ボタン押下により、証明書の検証を行う。 [ファイル出力]ボタンの押下により、電子証明書の内容をファイルに出力する。
6		官職証明書・職責証明書検証画面		その他の電子証明書（基本／詳細）画面にて、[証明書検証]ボタンを押下し、証明書検証を行い、証明書検証結果を表示する。
7		利用者証明書有効性確認画面		署名用電子証明書（基本／詳細）画面または利用者証明用電子証明書（基本／詳細）画面にて、[有効性確認]ボタンを押下して有効性確認を行い、有効性確認結果を表示する。

第２節　画面仕様詳細

（1）署名用電子証明書基本画面

画面名	署名用電子証明書基本画面
概要	署名用電子証明書の基本情報を表示する。

画面レイアウト



表示項目と証明書領域の対応は、**表　6-2** を参照。

画面項目説明

NO	項目名	概要
①	終了ボタン	証明書 Viewer を閉じる。
②	タイトル	表示する電子証明書の種類を表示する。 表示テキストは以下の通りとする。 「公的個人認証サービス 利用者の署名用電子証明書」
③	タブ	基本画面と詳細画面を切り替える。
④	氏名*1	利用者の氏名を表示する。大括弧「［ ］」内は旧氏を示す。括弧「（ ）」内は通称を示す。最大 100 文字まで表示可能。画面上に表示しきれない場合は、カーソルを移動することにより、表示欄のスクロールを可能とする。
⑤	代替文字の使用（氏名）*1	氏名の代替文字を表示する。最大 100 文字まで表示可能。代替文字がない場合は、表示しない。
⑥	生年月日	利用者の生年月日を和暦で表示する。
⑦	性別	利用者の性別（男/女/不明）を表示する。

NO	項目名	概要
⑧	住所[*1]	利用者の住所を表示する。最大 200 文字まで表示可能。画面上に表示しきれない場合は、カーソルを移動することにより、表示欄のスクロールを可能とする。
⑨	代替文字の使用（住所）[*1]	住所の代替文字を表示する。最大 200 文字まで表示可能。代替文字がない場合は、表示しない。
⑩	発行年月日	電子証明書の発行年月日を和暦で表示する。
⑪	有効期間の満了日	電子証明書の有効期間の満了日を和暦で表示する。
⑫	発行者	電子証明書の発行者を表示する。
⑬	ファイル出力ボタン	[ファイル出力]ボタンを押下することによって電子証明書の内容をファイルに出力する。出力様式は以下の 2 通り。 ・電子証明書を DER 形式のファイルとして出力する。拡張子は *.cer とする。 ・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。拡張子は*.txt とする。
⑭	有効性確認ボタン	[有効性確認]ボタンを押下することによって、公的個人認証サービス AP の自分の電子証明書の有効性確認機能を呼び出し、オンライン窓口サービスに有効性確認の問い合わせを行う。 自分の電子証明書の有効性確認機能の戻り値を判断して有効性確認結果ダイアログを表示する。
⑮	ステータスバー	有効性確認状態を以下のように表示する。 確認前：電子証明書の有効性確認は行われていません。 確認後：有効性確認結果：「有効」 有効性確認結果：「有効期限切れ」 有効性確認結果：「失効済み」 有効性確認結果：「失効申請受理済み」 有効性確認結果：「一時保留」 有効性確認結果：「確認失敗(xxxxxx)」 「xxxxxx」は原因を示すエラーコード。詳細は、表 ６-１０を参照。

表 6-2 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	SubjectAlt-Name	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)		Substitute-CharacterOf-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。 ・同じ代替文字が続いた場合は、繰り返し表示。 例）「吉」「吉」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)		Substitute-CharacterOf-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。 ・代替文字が続いた場合は、繰り返し表示。 例）「葛」「葛」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「ＧＧ YY 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	IssuerAlt-Name	Organizational-UnitName	設定値をそのまま表示。

※1 代替文字の設定ルール

（ｉ） 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。

(ⅱ)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ｘｘｘ	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

（ｉ） 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）

（ⅱ） 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

（ｉ） コード体系

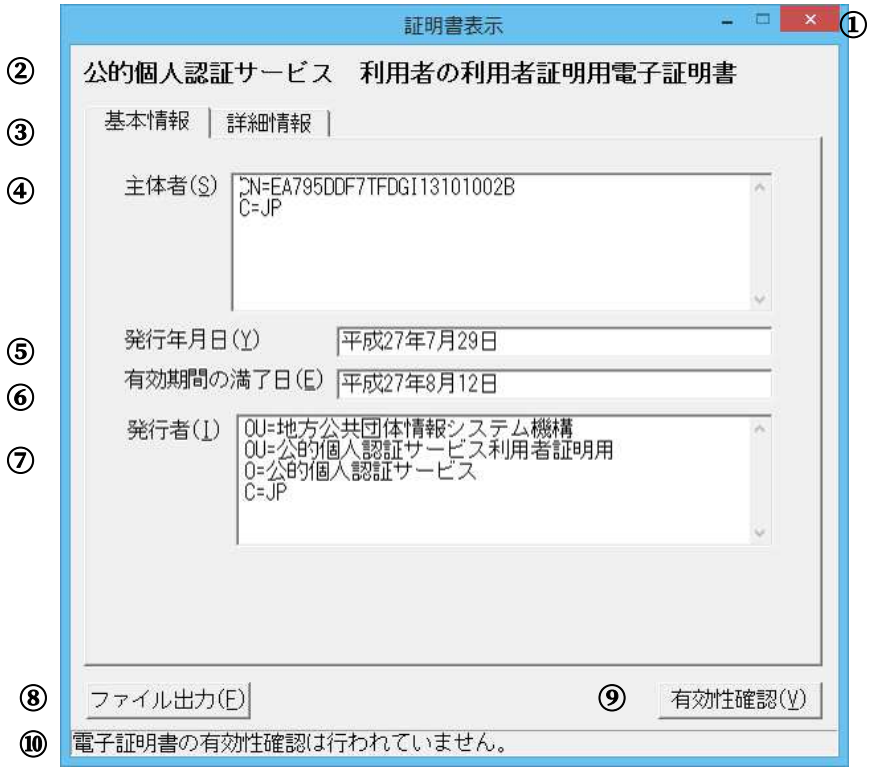
英数字型　1 桁　X

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基本画面

画面名	利用者証明用電子証明書基本画面
概要	利用者証明用電子証明書の基本情報を表示する。

画面レイアウト



表示項目証明書領域の対応は、表 6 - 3 を参照。

画面項目説明

NO	項目名	概要
①	終了ボタン	証明書 Viewer を閉じる。
②	タイトル	表示する電子証明書の種類を表示する。 表示テキストは以下の通りとする。 「公的個人認証サービス　利用者の利用者証明用電子証明書」
③	タブ	基本画面と詳細画面を切り替える。
④	主体者	主体者を表示する。 設定値が 1 行で収まらない場合は、折り返して表示する。
⑤	発行年月日	電子証明書の発行年月日を和暦で表示する。
⑥	有効期間の満了日	電子証明書の有効期間の満了日を和暦で表示する。
⑦	発行者	電子証明書の発行者を表示する。 設定値が 1 行で収まらない場合は、折り返して表示する。

NO	項目名	概要
⑧	ファイル出力ボタン	[ファイル出力]ボタンを押下することによって電子証明書の内容をファイルに出力する。出力様式は以下の 2 通り。 ・電子証明書を DER 形式のファイルとして出力する。拡張子は*.cer とする。 ・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。拡張子は*.txt とする。
⑨	有効性確認ボタン	[有効性確認]ボタンを押下することによって、公的個人認証サービス AP の自分の電子証明書の有効性確認機能を呼び出し、オンライン窓口サービスに有効性確認の問い合わせを行う。 自分の電子証明書の有効性確認機能の戻り値を判断して有効性確認結果ダイアログを表示する。
⑩	ステータスバー	有効性確認状態を以下のように表示する。 確認前：電子証明書の有効性確認は行われていません。 確認後：有効性確認結果：「有効」 有効性確認結果：「有効期限切れ」 有効性確認結果：「失効済み」 有効性確認結果：「失効申請受理済み」 有効性確認結果：「一時保留」 有効性確認結果：「確認失敗(xxxxxx)」 「xxxxxx」は原因を示すエラーコード。詳細は、表 6-10 を参照。

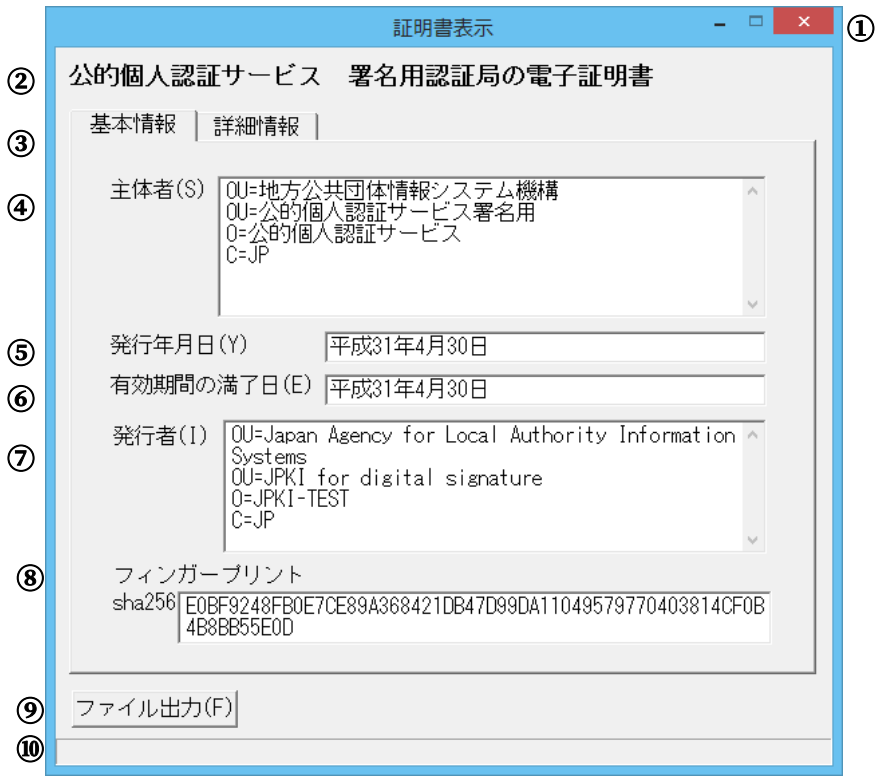
表 6-3 表示項目と証明書領域の対応（利用者証明用電子証明書）

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	SubjectAlt-Name または Subject	CountryName OrganizationalUnitName 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「GG YY 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	IssuerAlt-Name 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。

（3）認証局の自己署名証明書基本画面

画面名	認証局の自己署名証明書基本画面
概要	認証局の自己署名証明書の基本情報を表示する。

画面レイアウト



表示項目証明書領域の対応は、表　6 - 4 を参照。

画面項目説明

NO	項目名	概要
①	終了ボタン	証明書 Viewer を閉じる。
②	タイトル	表示する電子証明書の種類を表示する。 表示テキストは以下の通りとする。 ・都道府県知事の自己署名証明書および署名用認証局の自己署名証明書の場合 「公的個人認証サービス　署名用認証局の電子証明書」 ・利用者証明用認証局の自己署名証明書の場合 「公的個人認証サービス　利用者証明用認証局の電子証明書」 ・上記以外の認証局の自己署名証明書の場合 「認証局の電子証明書」
③	タブ	基本画面と詳細画面を切り替える。
④	主体者	主体者を表示する。 設定値が 1 行で収まらない場合は、折り返して表示する。
⑤	発行年月日	電子証明書の発行年月日を和暦で表示する。
⑥	有効期間の満了日	電子証明書の有効期間の満了日を和暦で表示する。

NO	項目名	概要
⑦	発行者	電子証明書の発行者を表示する。 設定値が 1 行で収まらない場合は、折り返して表示する。
⑧	sha1 または、sha256	電子証明書の署名アルゴリズムによって「sha1」または、「sha256」ハッシュ値を表示する。
⑨	ファイル出力ボタン	[ファイル出力]ボタンを押下することによって電子証明書の内容をファイルに出力する。出力様式は以下の 2 通り。 ・電子証明書を DER 形式のファイルとして出力する。拡張子は *.cer とする。 ・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。拡張子は*.txt とする。
⑩	ステータスバー	使用せず。

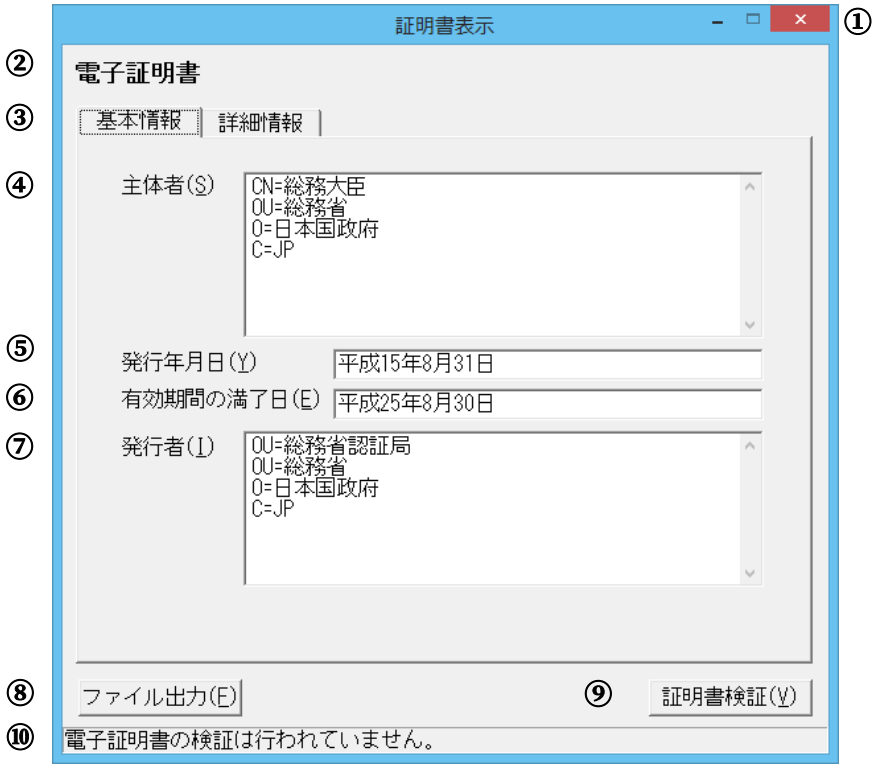
表 6-4 表示項目と証明書領域の対応（認証局の自己署名証明書）

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	SubjectAlt-Name または Subject	CountryName OrganizationName OrganizationalUnitName OrganizationalUnitName 例) 署名用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「ＧＧ YY 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	IssuerAlt-Name または Issuer	CountryName OrganizationName OrganizationalUnitName OrganizationalUnitName 例) 署名用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。ハッシュ関数は電子証明書の署名アルゴリズムによって「sha1」または「sha256」を使用する。

（4）その他の電子証明書基本画面

画面名	その他の電子証明書基本画面
概要	利用者証明書、認証局の自己署名証明書以外の電子証明書の基本情報を表示する。

画面レイアウト



表示項目と証明書領域の対応は、表 6 - 5 を参照。

画面項目説明

NO	項目名	概要
①	終了ボタン	証明書 Viewer を閉じる。
②	タイトル	表示する電子証明書の種類を表示する。 表示テキストは以下の通りとする。 「電子証明書」
③	タブ	基本画面と詳細画面を切り替える。
④	主体者	主体者を表示する。 設定値が 1 行で収まらない場合は、折り返して表示する。(単語途中であっても折り返しを行う仕様とする。)
⑤	発行年月日	電子証明書の発行年月日を和暦で表示する。
⑥	有効期間の満了日	電子証明書の有効期間の満了日を和暦で表示する。
⑦	発行者	電子証明書の発行者を表示する。 設定値が 1 行で収まらない場合は、折り返して表示する。(単語途中であっても折り返しを行う仕様とする。)

NO	項目名	概要
⑧	ファイル出力ボタン	[ファイル出力]ボタンを押下することによって電子証明書の内容をファイルに出力する。出力様式は以下の 2 通り。 ・電子証明書を DER 形式のファイルとして出力する。拡張子は *.cer とする。 ・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。拡張子は*.txt とする。
⑨	証明書検証ボタン	[証明書検証]ボタンを押下することによって、公的個人認証サービス AP の官職証明書検証機能を呼び出し、官職証明書検証サービスに証明書検証の問い合わせを行う。 官職証明書検証機能の戻り値を判断して官職証明書・職責証明書検証ダイアログを表示する。
⑩	ステータスバー	証明書検証状態を以下のように表示する。 検証前：電子証明書の検証は行われていません。 検証後：証明書検証結果「有効」 証明書検証結果「無効（xxxxxx)」 証明書検証結果「検証失敗（xxxxxx)」 「xxxxxx」は原因を示すエラーコード。詳細は、表 6-8、表 6-9 を参照。

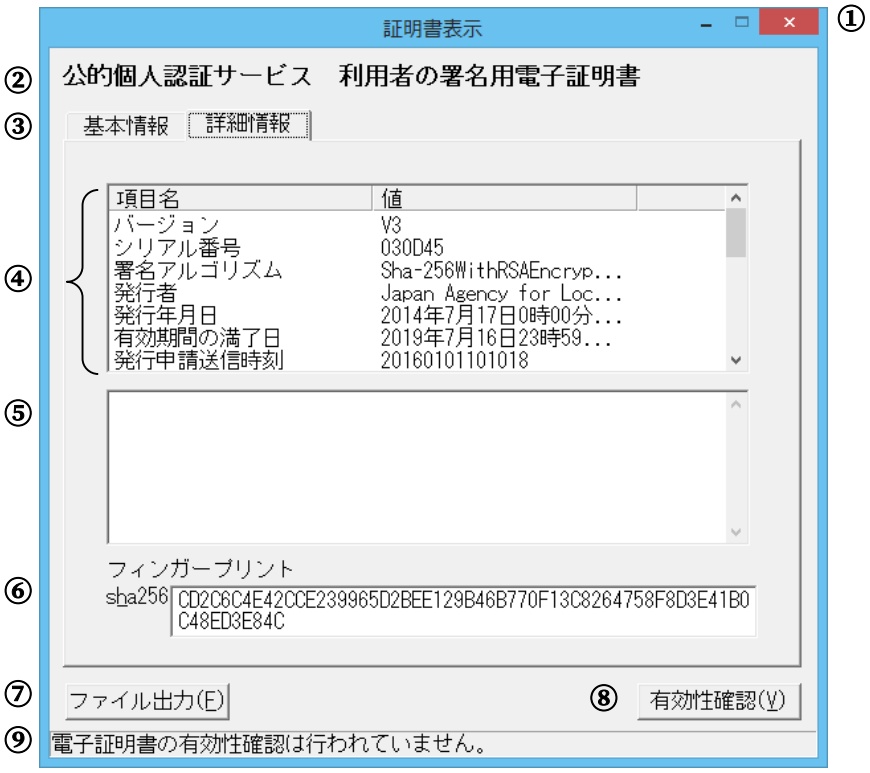
表 6-5 表示項目と証明書領域の対応（官職証明書／職責証明書／その他の証明書）

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	SubjectAlt-Name 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「ＧＧ YY 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	IssuerAlt-Name 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。ハッシュ関数は電子証明書の署名アルゴリズムによって「sha1」または「sha256」を使用する。

（5）詳細画面

画面名	詳細画面
概要	電子証明書内の全ての記載事項を表示する。

画面レイアウト



表示項目と証明書領域の対応は、表 6-6、表 6-7 を参照。

画面項目説明

NO	項目名	概要
①	終了ボタン	証明書 Viewer を閉じる。

NO	項目名	概要
②	タイトルバー	表示する電子証明書の種類を表示する。 表示テキストは以下の通りとする。 ・住基カードに格納された署名用電子証明書および個人番号カードに格納された署名用電子証明書の場合 「公的個人認証サービス　利用者の署名用電子証明書」 ・個人番号カードに格納された利用者証明用電子証明書の場合 「公的個人認証サービス　利用者の利用者証明用電子証明書」 ・都道府県知事の自己署名証明書および署名用認証局の自己署名証明書の場合 「公的個人認証サービス　署名用認証局の電子証明書」 ・利用者証明用認証局の自己署名証明書の場合 「公的個人認証サービス　利用者証明用認証局の電子証明書」 ・上記以外の認証局の自己署名証明書の場合 「認証局の電子証明書」 ・上記以外の証明書の場合 「電子証明書」
③	タブ	基本画面と詳細画面を切り替える。
④	設定値の簡易表記	電子証明書内の記載事項を表示する。 フィールドにて、表示しきれないものは、縦スクロールバー、横スクロールバーを移動することによって表示する。 フィールド名と値の詳細は、「表 6-6 項目名と証明書基本領域との対応」と「表 6-7 項目名と証明書標準拡張領域との対応」の簡易表記を参照。
⑤	設定値の詳細表記	選択したフィールドの設定値を表示する。 折り返し表示とし、横スクロールバーは表示しない。 フィールド名と値の詳細は、「表 6-6 項目名と証明書基本領域との対応」と「表 6-7 項目名と証明書標準拡張領域との対応」の詳細表記を参照。
⑥	sha1 または、sha256	電子証明書の署名アルゴリズムによって「sha1」または、「sha256」ハッシュ値を表示する。
⑦	ファイル出力ボタン	[ファイル出力]ボタンを押下することによって電子証明書の内容をファイルに出力する。出力様式は以下の 2 通り。 ・電子証明書を DER 形式のファイルとして出力する。拡張子は *.cer とする。 ・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。拡張子は*.txt とする。
⑧	有効性確認ボタン／証明書検証ボタン	利用者証明書の場合は有効性確認ボタンを表示する。(有効性確認機能については、(１) 署名用電子証明書の画面項目説明を参照。) 官職証明書／職責証明書の場合は証明書検証ボタンを表示する。(証明書検証機能については、(４) その他の電子証明書の画面項目説明を参照。)

NO	項目名	概要
⑨	ステータスバー	利用者証明書の場合は有効性確認結果を表示する。(ステータスバーの概要については、(１) 署名用電子証明書の画面項目説明を参照。) 官職証明書／職責証明書の場合は証明書確認結果を表示する。(ステータスバーの概要については、(４) その他の電子証明書の画面項目説明を参照。)

表 6-6 項目名と証明書基本領域との対応

NO	項目名	証明書の項目名		表示方法	
		上位項目名	項目名	簡易表記	詳細表記
1	バージョン	version		Version 表記。Version3 は“V3”とする。	
2	シリアル番号	serialNumber		設定値をそのまま表示。	
3	署名アルゴリズム	signature	algorithm parameters	algorithm の OID を RFC の規定値に変換した値。	
4	発行者	issuer	countryName organizationName organizationalUnitName 等	DN をカンマ区切り表示。「(設定値),(設定値),･･･」。	DN を属性毎に改行。各行は「(属性の略語)=(設定値)」にて表記。 <属性の略語> 「countryName」 →C 「organizationName」 →O 「organizationalUnitName」 →OU
5	発行年月日	Validity	notBefore	設定値を西暦（日本標準時）で表示。書式は「YYYY 年 MM 月 DD 日 hh 時 mm 分 ss 秒」。	
6	有効期間の満了日		notAfter		
7	主体者[*1]	subject	countryName localityName commonName 等	DN をカンマ区切り表示。「(設定値),(設定値),･･･」。 commonName が発行要求発生時刻の場合は、設定値をそのまま表示。	DN を属性毎に改行。各行は「(属性の略語)=(設定値)」にて表記。 <属性の略語> 「countryName」 →C 「localityName」 →L 「commonName」 →CN commonName が発行要求発生時刻の場合は、設定値をそのまま表示。

NO	項目名	証明書の項目名		表示方法	
		上位項目名	項目名	簡易表記	詳細表記
8	発行申請送信時刻*2	subject	commonName のみが表示対象	commonName から発行申請送信時刻を抜き出して表示。	
9	受付端末識別記号*2			commonName から受付端末識別記号を抜き出して表示。	
10	発行申請送信時刻*3	subject	commonName のみが表示対象	commonName から発行申請送信時刻を抜き出して表示。	
11	シーケンス番号*3			commonName からシーケンス番号を抜き出して表示。	
12	受付端末識別記号*3			commonName から受付端末識別記号を抜き出して表示。	
13	ランダム文字列*4	subject	commonName のみが表示対象	commonName からランダム文字列を抜き出して表示。	
14	受付端末識別記号*4			commonName から受付端末識別記号を抜き出して表示。	
15	主体者の公開鍵情報	subjectPublicKeyInfo	algorithm	暗号アルゴリズムと鍵長を表示。書式は「(algorithm の OID を RFC の規定値に変換した値)＋(鍵長)Bits」。	SubjectPublicKey の設定値（１６進数）をそのまま表示。
			subjectPublicKey		
16	発行者ユニーク識別子	issuerUniqueID		設定値をそのまま表示。	
17	主体者ユニーク識別子	subjectUniqueID		設定値をそのまま表示。	

*1：利用者証明書以外の場合

*2：住基カードに格納された署名用電子証明書の場合

*3：個人番号カードに格納された署名用電子証明書の場合

*4：個人番号カードに格納された利用者証明用電子証明書の場合

表 6-7 項目名と証明書標準拡張領域との対応

NO	項目名	証明書の項目名		表示方法	
		上位項目名	項目名	簡易表記	詳細表記
1	認証局鍵識別子	AuthorityKeyIdentifier	keyIdentifier authorityCertIssuer authorityCertSerialNumber	AuthorityKeyIdentifier の情報を項目毎にカンマ区切り表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。	AuthorityKeyIdentifier の情報を項目毎に階層表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。 ・DN は属性毎に改行。
2	鍵用途	KeyUsage	digitalSignature nonRepudiation keyEncipherment dataEncipherment keyAgreement keyCertSign cRLSign encipherOnly decipherOnly	KeyUsage の情報を項目毎にカンマ区切り表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。 ・KeyUsage のビット列は、鍵用途の英語名に変換してカンマ区切り表示。	KeyUsage の情報を項目毎に階層表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。 ・KeyUsage のビット列は、鍵用途の英語名に変換してカンマ区切り表示。
3	主体者代替名	SubjectAltName	countryName organizationName organizationalUnitName 等	SubjectAltName の情報を項目毎にカンマ区切り表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。	SubjectAltName の情報を項目毎に階層表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。
4	発行者代替名	issuerAltName	countryName organizationName organizationalUnitName 等	issuerAltName の情報を項目毎にカンマ区切り表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。	issuerAltName の情報を項目毎に階層表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。

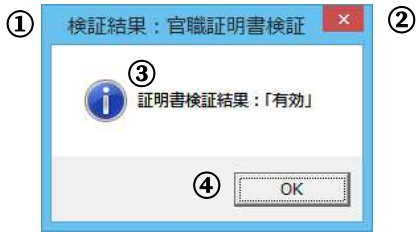
NO	項目名	証明書の項目名		表示方法	
		上位項目名	項目名	簡易表記	詳細表記
5	基本制約	BasicConstrains	cA pathLenConstraint	BasicConstrains の情報を項目毎にカンマ区切り表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。	BasicConstrains の情報を項目毎に階層表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。
6	CRL 分配点	CRLDistributionPoints	countryName organizationName organizationalUnitName 等	CRLDistributionPoints の情報を項目毎にカンマ区切り表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。	CRLDistributionPoints の情報を項目毎に階層表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。 ・DN は属性毎に改行。
7	証明書ポリシー	CertificatePolicies	policyIdentifier policyQualifiers	CertificatePolicies の情報を項目毎にカンマ区切り表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。	CertificatePolicies の情報を項目毎に階層表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。
8	主体者鍵識別子	SubjectKeyIdentifier	keyIdentifier	SubjectKeyIdentifier の情報を項目毎にカンマ区切り表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。	SubjectKeyIdentifier の情報を項目毎に階層表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。

NO	項目名	証明書の項目名		表示方法	
		上位項目名	項目名	簡易表記	詳細表記
9	拡張鍵用途	ExtKeyUsage	serverAuth clientAuth codeSigning emailProtection ipsecEndSystem ipsecTunnel ipsecUser timeStamping	ExtKeyUsage の情報を項目毎にカンマ区切り表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。	ExtKeyUsage の情報を項目毎に階層表示。なお、表示の際は以下のルールを適用する。 ・項目名は英語のまま。 ・OID は RFC の規定値に変換。

（6）官職証明書・職責証明書検証画面

画面名	官職証明書・職責証明書検証画面
概要	その他の電子証明書（基本／詳細）画面にて、[証明書検証]ボタンを押下し、証明書検証を行い、証明書検証結果を表示する。

画面レイアウト



画面項目説明

NO	項目名	概要
①	タイトルバー	表示テキストは「検証結果：官職証明書検証」とする。
②	終了ボタン	官職証明書・職責証明書検証画面を閉じる。
③	証明書検証結果	証明書検証が終了した場合、以下のメッセージを表示する。 証明書が有効の場合：証明書検証結果「有効」 証明書が無効の場合：証明書検証結果「無効（xxxxxx）」 （無効の場合とは、証明書検証結果が失敗した場合を示す。） 証明書検証処理が失敗した場合 ：証明書検証結果「検証失敗（xxxxxx）」 （検証失敗とは、証明書検証が行えなかった場合を示す。） 「xxxxxx」は原因を示すエラーコード。詳細は、表 6-8、表 6-9を参照。
④	ＯＫボタン	官職証明書・職責証明書検証画面を閉じる。

＜メッセージの詳細＞

表 6-8 証明書検証結果「無効」の場合のエラーコード一覧

NO	エラーコード	内容	意味
1	100101	認証パス構築不可(101)	認証パス構築ができないこと。
2	100202	署名不正(202)	認証パスに署名が不正である証明書が含まれていること。
3	100203	失効証明書を含む(203)	認証パスに失効した証明書が含まれていること。
4	100204	ポリシー不一致(204)	認証パスにポリシーが一致しない証明書が含まれていること。
5	100205	制約違反(205)	認証パスに制約に違反している証明書が含まれていること。
6	100206	OCSP での証明書検証確認不正(206)	認証パスに OCSP での certStatus が unknown と応答される証明書が含まれていること。
7	100301	アルゴリズム拒否(301)	官職証明書検証サーバ(CVS)側で検証対象証明書の受け付けを拒否されたこと。
8	100302	アルゴリズム拒否(302)	官職証明書検証サーバ(CVS)側で中間証明書または都道府県知事の自己署名証明書の受け付けを拒否されたこと。
9	100901	要求受付け拒否(901)	官職証明書検証サーバ(CVS)側で要求の受け付が拒否されたこと。

注：( )中のコードは certPathStatus を示す。

表 6-9 証明書検証結果「検証失敗」の場合のエラーコード一覧

NO	エラーコード	内容	意味
1	100902	タイムアウト(902)	要求がタイムアウトとなったこと。( )中のコードは certPathStatus を示す。
2	200100	署名検証失敗	受信した OCSP レスポンスデータが改竄されていること。
3	200200	証明書が改竄または、有効期限切れ	OCSP レスポンスに付与されている電子証明書が改竄または有効期限切れである。
4	300100	接続失敗	ネットワークの問題で通信できなかった。 LAN 環境からプロキシサーバを使用している場合は、Internet Explorer の LAN の設定又は、システムのプロキシ情報の指定に誤りがある。
5	300200	拡張領域の解析に失敗	官職証明書検証サーバ(CVS)に接続していない。環境設定ファイルの CVS 接続先 URL をもう一度見直してください。
6	300300	その他のエラー発生のため証明書検証の確認不可	・ 環境設定ファイルに CVS 接続先 URL が指定されていない又は、環境設定ファイルが存在しない。 ・ その他の内部エラーが発生。

NO	エラーコード	内容	意味
7	300400	証明書の取得失敗	・ IC カードの PIN 入力でキャンセルされた場合。 ・ IC カードリーダライタに IC カードがセットされていない場合。 ・ IC カードリーダライタが PC に接続されていない場合。※1
8	400001	OCSP Request のフォーマットエラー(1)	官職証明書検証サーバ(CVS）で例外が発生 ・ 検証要求を行う官職証明書検証サーバ(CVS）の検証依頼者認証が必要であるか確認してください。 ・ 署名に使用した電子証明書が X.509 バージョン 3 の電子証明書であるかを確認してください。
9	400002	内部エラー (2)	
10	400003	一時的な解答不能(3)	
11	400005	OCSP Request への署名が必要(5)	
12	400006	クライアントが認証されていない(6)	

注：( )中のコードは responseStatus を示す。

（※1）MacOS 版の場合、住基カードが利用されている場合にも本エラーが発生する。

（7）利用者証明書有効性確認画面

画面名	利用者証明書有効性確認画面
概要	電子証明書（基本／詳細）画面にて、[有効性確認]ボタンを押下し、有効性確認を行い、有効性確認結果を表示する。

画面レイアウト

画面項目説明

NO	項目名	概要
①	タイトルバー	表示テキストは「確認結果：有効性確認」とする。
②	終了ボタン	利用者証明書有効性確認画面を閉じる。
③	有効性確認結果	有効性確認結果が終了した場合､以下のメッセージを表示する。 対象とする証明書が有効の場合 ：有効性確認結果「有効」 対象とする証明書の有効期限が切れている場合 ：有効性確認結果「有効期限切れ」 対象とする証明書が失効済みの場合 ：有効性確認結果「失効済み」 対象とする証明書のオンライン失効申請を行った場合 ：有効性確認結果「失効申請受理済み」 対象とする証明書が一時保留状態の場合 ：有効性確認結果「一時保留」 有効性確認処理が失敗した場合 ：有効性確認結果「確認失敗（xxxxxx）」 （確認失敗とは、有効性確認が行えなかった場合を示す。） 「xxxxxx」は原因を示すエラーコード。詳細は、表 ６-１０を参照。
④	ＯＫボタン	利用者証明書有効性確認画面を閉じる。

＜メッセージの詳細＞

表 6-10 有効性確認結果「確認失敗」のエラーコード一覧

NO	エラーコード	内容	意味
1	100600	申請書の電子署名検証エラー	オンライン窓口サーバで「申請書の電子署名検証エラー」が発生した。
2	100604	対象とする証明書の認証局の電子署名検証エラー	オンライン窓口サーバで「対象とする証明書の認証局の電子署名検証エラー」が発生した。
3	100605	対象とする証明書の有効性確認エラー	オンライン窓口サーバで「対象とする証明書の有効性確認エラー」が発生した。
4	200601	申請情報取込エラー	オンライン窓口サーバで「申請情報取込エラー」が発生した。
5	200602	対象とする証明書の有効期限切れエラー	オンライン窓口サーバで「対象とする証明書の有効期限切れエラー」が発生した。
6	200603	受信データ形式エラー	オンライン窓口サーバで「受信データ形式エラー」が発生した。
7	200609	オンライン窓口エラー（DB）	オンライン窓口サーバで「オンライン窓口エラー(DB)」が発生した。
8	200611	オンライン窓口混雑	オンライン窓口サーバが混雑している。
9	200612	オンライン窓口エラー	オンライン窓口サーバでエラーが発生した。
10	200622	対象とする証明書と署名実施証明書の不一致エラー	オンライン窓口サーバで「対象とする証明書と署名実施証明書の不一致エラー」が発生した。
11	200652	署名実施証明書の有効期間外エラー	オンライン窓口サーバで「署名実施証明書の有効期間外エラー」が発生した。
12	200654	署名実施証明書の認証局の電子署名検証エラー	オンライン窓口サーバで「署名実施証明書の認証局の電子署名検証エラー」が発生した。
13	200655	署名実施証明書の有効性確認エラー	オンライン窓口サーバで「署名実施証明書の有効性確認エラー」が発生した。
14	200656	オンライン窓口エラー(OCSP)	オンライン窓口サーバで「オンライン窓口エラー(OCSP)」が発生した。
15	200657	署名実施証明書の失効済みエラー	オンライン窓口サーバで「署名実施証明書の失効済みエラー」が発生した。
16	200658	署名実施証明書の失効申請受理済みエラー	オンライン窓口サーバで「署名実施証明書の失効申請受理済みエラー」が発生した。
17	200663	署名実施証明書の一時保留状態エラー	オンライン窓口サーバで「署名実施証明書の一時保留状態エラー」が発生した。

NO	エラーコード	内容	意味
18	2001xx	HTTP 通信エラー	HTTP 通信中にエラーが発生した。 1xx～5xx は HTTP1.1 ステータスコード。
19	2002xx		
20	2003xx		
21	2005xx		
22	3004xx		
23	300703	IC カードがロックされている	IC カードは現在使用中。
24	300704	IC カードに接続できない	カードリーダ接続不備、またはカードが接続されていない。※1
25	300705	対象とする証明書の解析失敗	対象とする証明書の解析に失敗した。
26	300706	サーバ時刻の取得に失敗	サーバ時刻の取得に失敗した。
27	300707	オンライン窓口サーバへのアクセスエラー	オンライン窓口サーバでアクセスに失敗した。
28	300709	対象とする証明書の有効期間になっていない	対象とする証明書の有効期限開始の日付が未来の日時である。
29	400606	対象とする証明書のオンライン窓口エラー（OCSP）	オンライン窓口サーバで「対象とする証明書のオンライン窓口エラー(OCSP)」が発生した。

（※1）MacOS 版の場合、住基カードが利用されている場合にも本エラーが発生する。

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 API 仕様書
【個人認証サービス AP C 言語インターフェース編】

第 4.6 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。