

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 Java インターフェース編】

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 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"> • JavaDoc に JPKIConfirmResult クラスを追加 • JavaDoc の JPKIUserCertService クラスに confirm メソッドを追加 • 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、ソフトウェア構成図を変更
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"> • 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
2.3 版	平成 19 年 4 月 10 日	表 3 - 1 動作環境を変更
2.4 版	平成 19 年 10 月 4 日	<ul style="list-style-type: none"> • 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 • 表 3 - 1 動作環境 JavaVM(Windows)に JRE6.0_2, JRE5.0_12, JRE1.4.2_13, JRE1.4.2_15 を追加 • 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
2.5 版	平成 20 年 10 月 10 日	<ul style="list-style-type: none"> • 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。 • 表 3 - 1 動作環境 JavaVM(Windows)に JRE5.0_15, JRE5.0_13, JRE1.4.2_17, JRE6.0_7, JRE6.0_6, JRE6.0_5, JRE6.0_4 を追加。 • 表 3 - 1 動作環境 Java for Mac OS X 10.5, Java for Mac OS X 10.4 Release6 を追加。

版数	変更日付	変更内容
2.6 版	平成 23 年 04 月 01 日	<ul style="list-style-type: none"> ・ 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
2.7 版	平成 25 年 12 月 01 日	<ul style="list-style-type: none"> ・ 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 6 章 画面仕様を追加。
3.0 版	平成 26 年 04 月 01 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。
3.1 版	平成 26 年 07 月 01 日	<ul style="list-style-type: none"> ・ 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 Safari 6.1 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	<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 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 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	<ul style="list-style-type: none"> ・ 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 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 接続機能追加対応に伴い、以下を修正。</p> <ul style="list-style-type: none"> ・ 第 1 章 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ー ➤ 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 カードリーダーライター、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。
4.2 版	平成 29 年 07 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 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	平成 31 年 03 月 31 日	<ul style="list-style-type: none"> ・ 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。

- 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 動作環境	5
第 1 節 PC/SC 対応 IC カードリーダーライター	7
第 2 節 Android 端末	8
第 4 章 機能仕様	9
第 1 節 ソフトウェア構成図	9
第 2 節 実現可能な機能の一覧	11
第 5 章 API 仕様	11
第 6 章 画面仕様	11

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、Java 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、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	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。

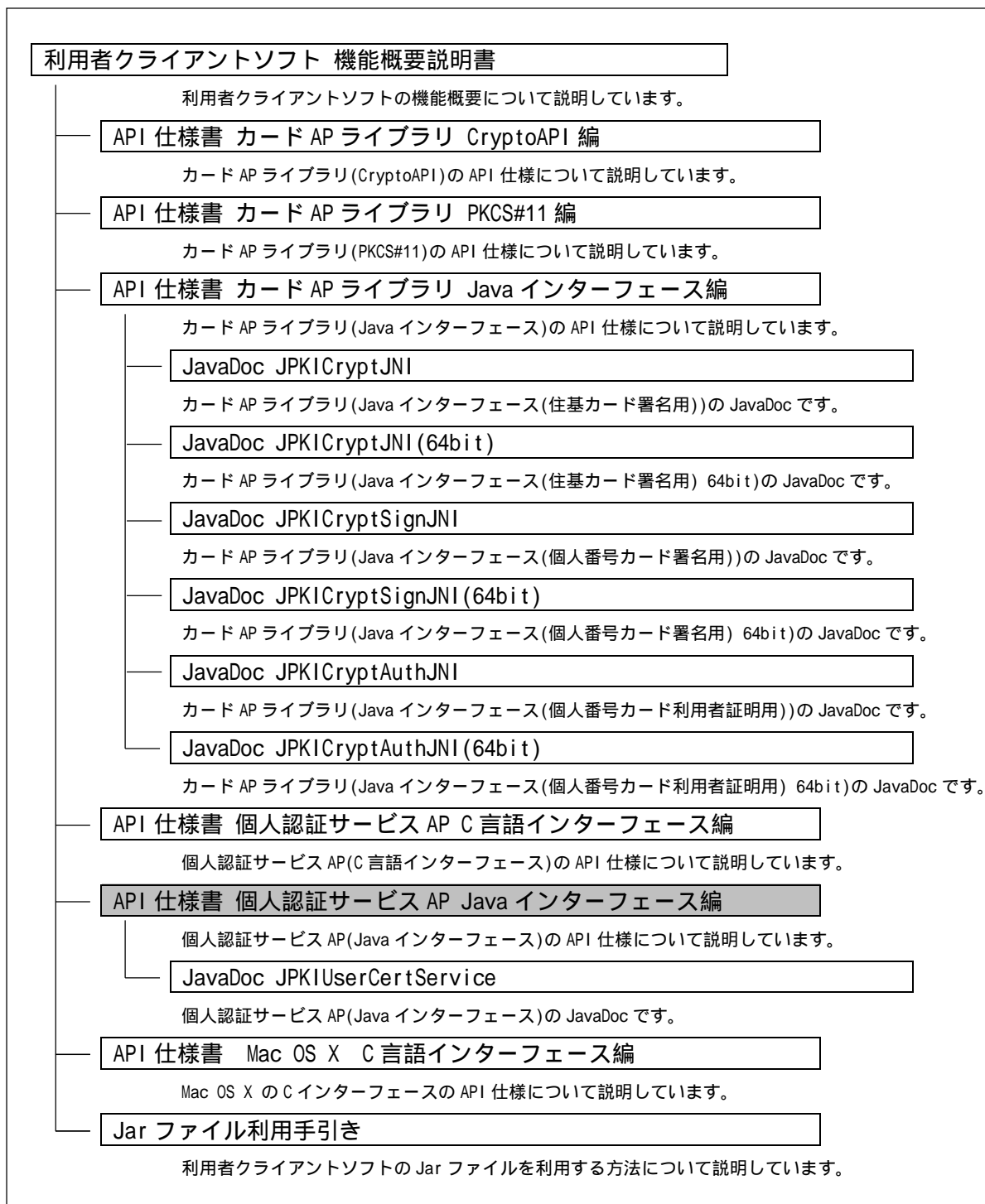


図 2-1 ドキュメント体系図

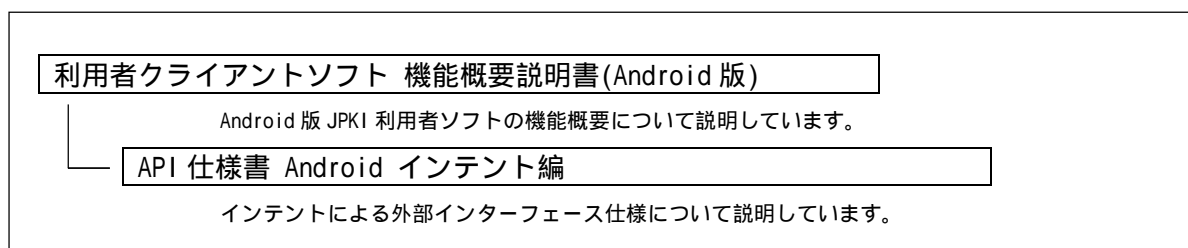


図 2-2 ドキュメント体系図(Android 版)

第 3 章 動作環境

個人認証サービス AP(Java 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, 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 版)	IE11.0		×	
Windows 10(64bit 版)	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「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。
- 6 JRE9.0 の 32bit 版は Oracle 社より提供されていないため非対応。

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 住基カードを使用する場合、または、住基カードと個人番号カードを両方使用する場合、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「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。

第 1 節 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 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。

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。) <ul style="list-style-type: none">・【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。

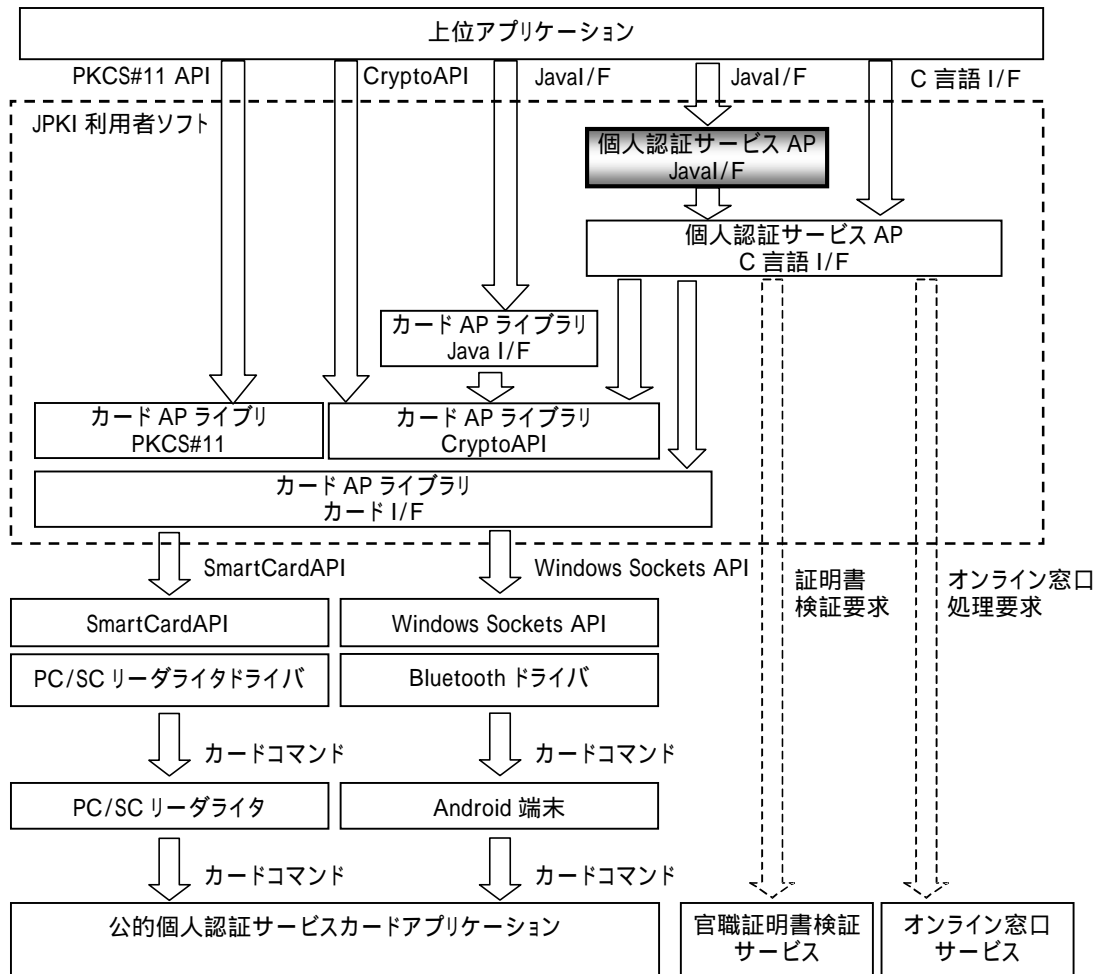
最新の「個人番号カード対応適合性検証済み Android 端末一覧」の情報は、JPKI ポータルサイトに掲載するものとする。

第 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(Java 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 >

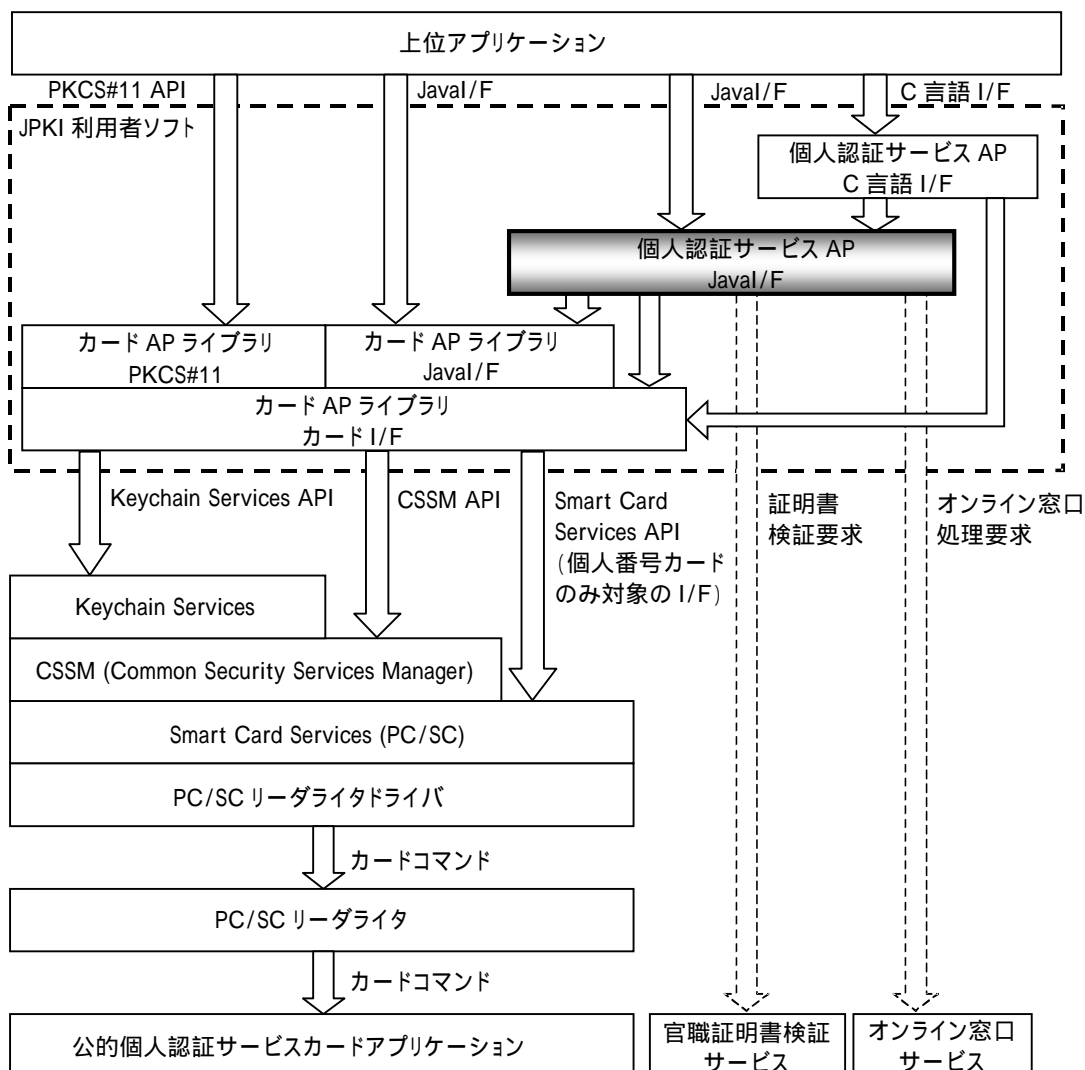


図 4-2 ソフトウェア構成図 (Mac OS 対応版)

第 2 節 実現可能な機能の一覧

個人認証サービス AP (Java インターフェース) で実現可能な機能の一覧を表 2 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	利用者証明書から基本 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の都道府県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の都道府県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 カードリーダーライターに挿入されている IC カードの種別を取得する。

第 5 章 API 仕様

個人認証サービス AP (Java インターフェース) の API 仕様については、JavaDoc(JPKIUserCertService)を参照のこと。

第 6 章 画面仕様

個人認証サービス AP (Java インターフェース) の画面仕様については、個人認証サービス AP (C 言語インターフェース) を参照のこと。

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 Java インターフェース編】

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。