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

## 【カード AP ライブラリ Java 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 | ・ 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 | 表 3-1 動作環境<br>・ プラットフォームに WindowsVista、MacOS X 10.4.9、MacOS X 10.4.10 を追加<br>・ Web ブラウザに Internet Explorer7.0 を追加<br>・ JavaVM に JRE5.0_12、JRE1.4.2_15、JRE6.0_2 を追加 |
| 2.5 版 | 平成 20 年 10 月 10 日 | 表 3-1 動作環境<br>・ 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<br>・ Web ブラウザに Internet Explorer6.0 ServicePack3 を追加<br>・ 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<br>・ JavaVM（MacOS）に 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 | 図 2-1 ドキュメント体系図に「JavaDoc JPKICryptJNI(64bit)」を追加。<br>表 3-1 動作環境<br>・表 3-1 動作環境(Windows)、 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。<br>表 3-1 動作環境(Windows)<br>・ OS に Windows 7(32/64 bit) , WindowsVista ServicePack2 を追加。<br>・ Web ブラウザに Internet Explorer8.0 を追加。<br>動作環境(MacOS)<br>・ OS に MacOS X 10.6.4, MacOS X 10.5.6, MacOS X 10.5.5 を追加。<br>・ Web ブラウザに Safari 3.2, Safari 5.0 を追加。<br>図 4-1 ソフトウェア構成図 (Windows 対応版)を変更。<br>第５章 API 仕様に 64bit に関する記載を追加。 |
| 2.7 版 | 平成 25 年 12 月 01 日 | 第３章 動作環境<br>・表 3-1 動作環境(Windows)<br>Windows2000 を削除、Windows8(32/64bit)、Windows8.1(32/64bit)を追加<br>・ 動作環境(MacOS)<br>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 |
| 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<br>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 | ・第３章 表 3-1 動作環境(Windows)で WindowsXP を削除、Windows 7(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<br>・第３章 動作環境(MacOS)で OS X 10.7.5 の Web ブラウザを Safari 6.0 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 Safari 6.0 から Safari 6.1 に変更、OS X 10.9.3、Web ブラウザに Safari7.0 を追加 |

| 版数 | 変更日付 | 変更内容 |
|---|---|---|
| 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。<br>・第１章 第１節に用語の定義を追加。<br>・第２章のドキュメント体系を修正。<br>・第３章の動作環境を修正。<br>・第４章の機能仕様を修正。<br>・第４章 第１節の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<br>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。<br>・第１章　第１節の「用語の定義」に以下を追加。<br>➢ PC/SC<br>➢ IC カードリーダライタ<br>➢ 挿入<br>➢ NFC<br>➢ Bluetooth<br>・第２章　ドキュメント体系図に Android 版を追加。<br>・第３章 表 3-1 および表 3-2 に PC 接続機能対応可否追加。<br>・第３章 表 3-1 に Windows 10(32/64bit)を追加。<br>・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。<br>・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。<br>・第２章 ドキュメント体系図を改訂。<br>・第３章 表 ３-１の OS から Windows Vista(32bit)を削除。<br>・第３章 表 ３-１の OS から Windows 8(32bit)を削除。<br>・第３章 表 ３-１の OS から Windows 8(64bit)を削除。<br>・第３章 表 ３-１の JavaVM に JRE9 を追加。<br>・第３章 表 ３-２の OS から OS X 10.8, 10.9 を削除。<br>・第３章 表 ３-２の OS に OS X 10.11, macOS v10.12 を追加。<br>・第３章 表 ３-２の JavaVM に JRE9 を追加。<br>・※２に説明文を追記。<br>・第３章 表 ３-５の【PC 接続の場合】に Android 6.0.1、7.0 を追加。<br>・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 | ・第３章 表 ３-２の OS から OS X 10.11 を削除。<br>・第３章 表 ３-２の OS に macOS v10.13 を追加。<br>・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。 |

| 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。<br>・第３章　表３-２を修正。<br>macOS v10.12、macOS v10.13 を削除。<br>macOS v10.14、macOS v10.15（Web ブラウザは Safari 13）を追加。<br>・第３章　カード AP ライブラリ(Java インターフェース)を利用する場合、Java 実行環境のインストールおよび Java 実行環境への登録を実行するよう利用者に通知する旨を追加。<br>・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。<br><br>MacOS 版における住基カードサポート廃止に伴い、以下を修正。<br>・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。<br>・第３章 表３-２ ※２の注釈を削除。<br>・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。<br>・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。<br>・第５章 表５－１ の住基カードは Windows 版のみ使用可能である旨の注釈を追加。<br><br>ブラウザ対応版、iOS 版のリリースに伴い、以下を修正。<br>・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。<br>・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。<br>・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。<br>・第２章　ドキュメント体系　「API 仕様書 iOS Framework 編」を追加。<br>・第３章　第２節　動作環境に Android9.0、10.0 を追加。<br><br>Windows 7 サポート終了に伴い、以下を修正。<br>・第３章　表３-１を修正。<br>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<br>・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。<br>・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<br>・第１章　第１節　用語の定義の記載を修正。<br>・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)におけるカード AP ライブラリは、以下の機能を実現するための Application Program Interface(以下、API)を提供する。

- 証明書取得機能
- 電子署名生成機能
- 電子署名検証機能

以降、本書ではカード AP ライブラリのうち、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。<br>・住基カード<br>・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。<br>データは、ISO/IEC 8825-1 の識別符号化規則により符号化された形式で利用される。 |
| 3 | 証明書 | 電子証明書と同義。 |
| 4 | 利用者証明書 | 公的個人認証サービスで発行した利用者の証明書。<br>本書では以下の電子証明書を指す。<br>・住基カードに格納された署名用電子証明書<br>・個人番号カードに格納された署名用電子証明書<br>・個人番号カードに格納された利用者証明用電子証明書 |
| 5 | 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。<br>本書では以下の秘密鍵を指す。<br>・住基カードに格納された署名用利用者秘密鍵<br>・個人番号カードに格納された署名用利用者秘密鍵<br>・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 |
| 6 | 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。<br>本書では以下の電子証明書を指す。<br>・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<br>・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<br>・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 |
| 7 | PC/SC | Personal Computer/Smart Card の略。 |
| 8 | IC カードリーダライタ | 以下の機器を指す総称<br>・PC/SC 対応 IC カードリーダライタ<br>・Android 端末 |
| 9 | 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。<br>具体的には以下の状態にすることを指す。<br>・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<br>・Android 端末に IC カードをセットすること |

| 項番 | 用語・略号 | 説明 |
|---|---|---|
| 10 | NFC | Near Field Communication (近距離無線通信)の略。 |
| 11 | 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。

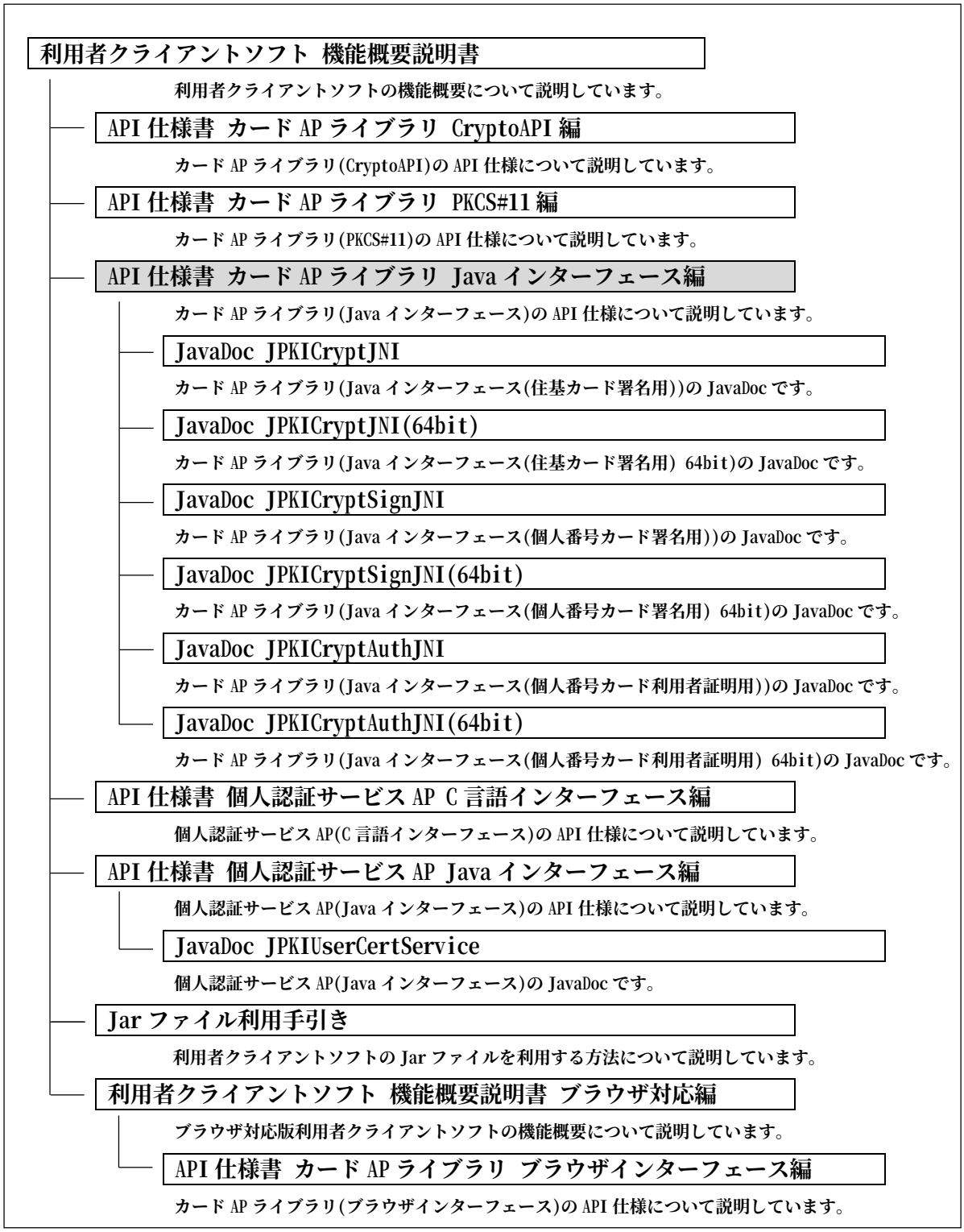



**図 2-1 ドキュメント体系図(PC 版)**

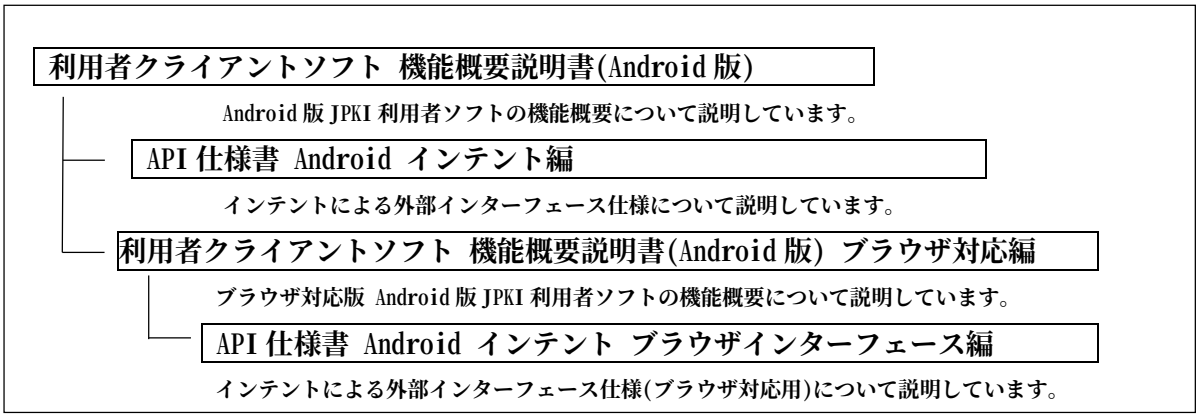



**図 2-1 ドキュメント体系図(Android 版)**

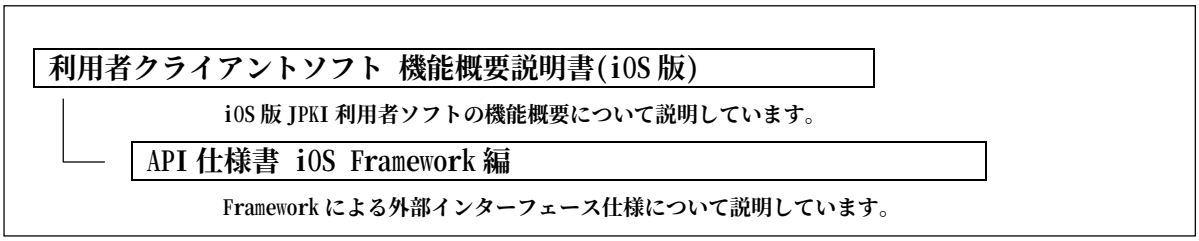



**図 2-2 ドキュメント体系図(iOS 版)**

# 第３章　動作環境

カード AP ライブラリ(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) 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。

なお、カード AP ライブラリ(Java インターフェース)を利用するアプリケーションの場合、Java 実行環境をインストールした上で「Java 実行環境への登録」を実行するよう、アプリケーションを利用するユーザへ通知する必要がある。

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。<br>※PC 接続機能を使用する場合は個人番号カードのみ対応。<br>※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。)<br>・ 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。<br>・ PC/SC 対応 IC カードリーダライタであること。<br>・ 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。<br>・ 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。<br>・ 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。<br>・ 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。)<br>・Android 8.0、9.0、10.0、11.0 または 12.0 を搭載していること。<br>・Bluetooth 4.2 を搭載していること。<br>・ISO/IEC 14443 Type B に対応している NFC を搭載していること。 |

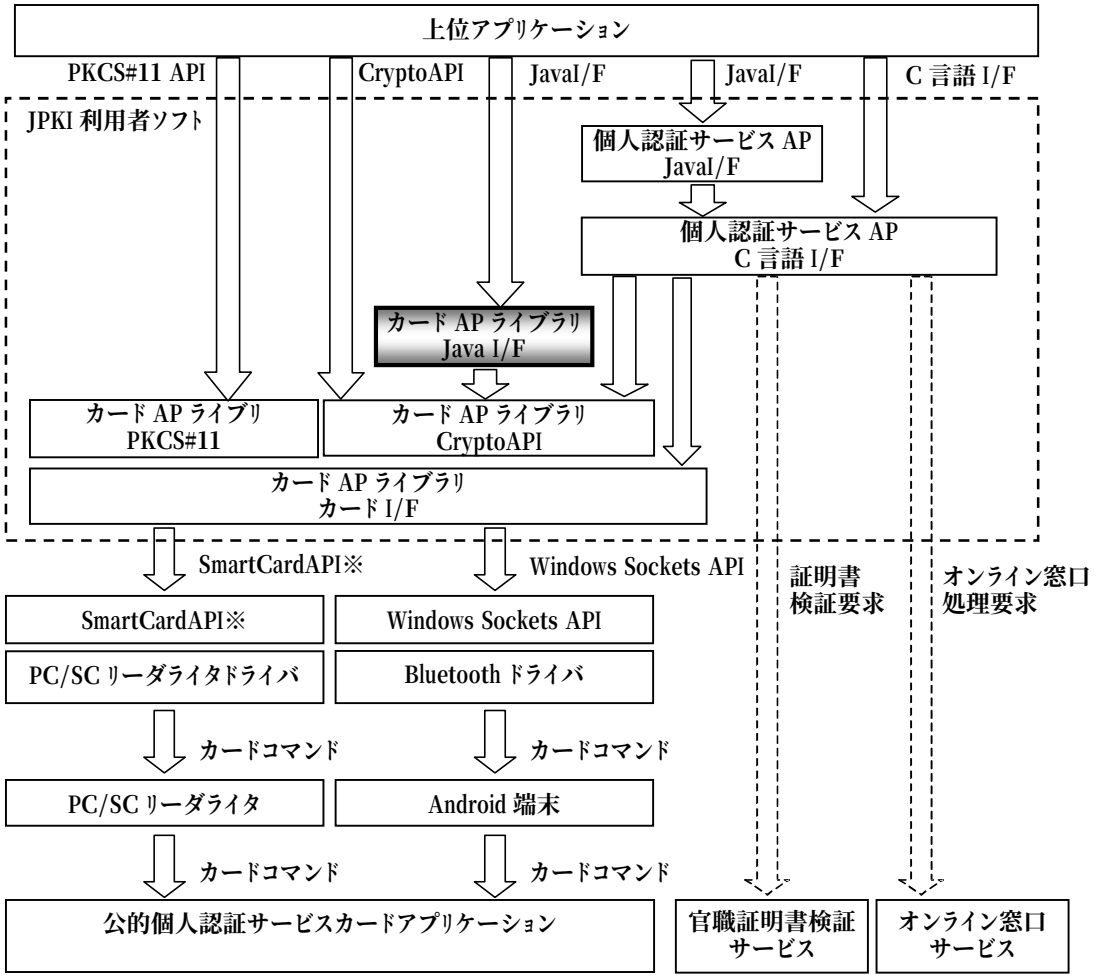
※ 最新の「個人番号カード対応適合性検証済み Android 端末一覧」の情報は、JPKI ポータルサイトに掲載するものとする。
また、最新の動作環境に掲載された OS 以外を使用した場合の不具合等に関するお問い合わせは、サポート対象外とする。

# 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、下図の太枠に示すカード AP ライブラリ(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＞

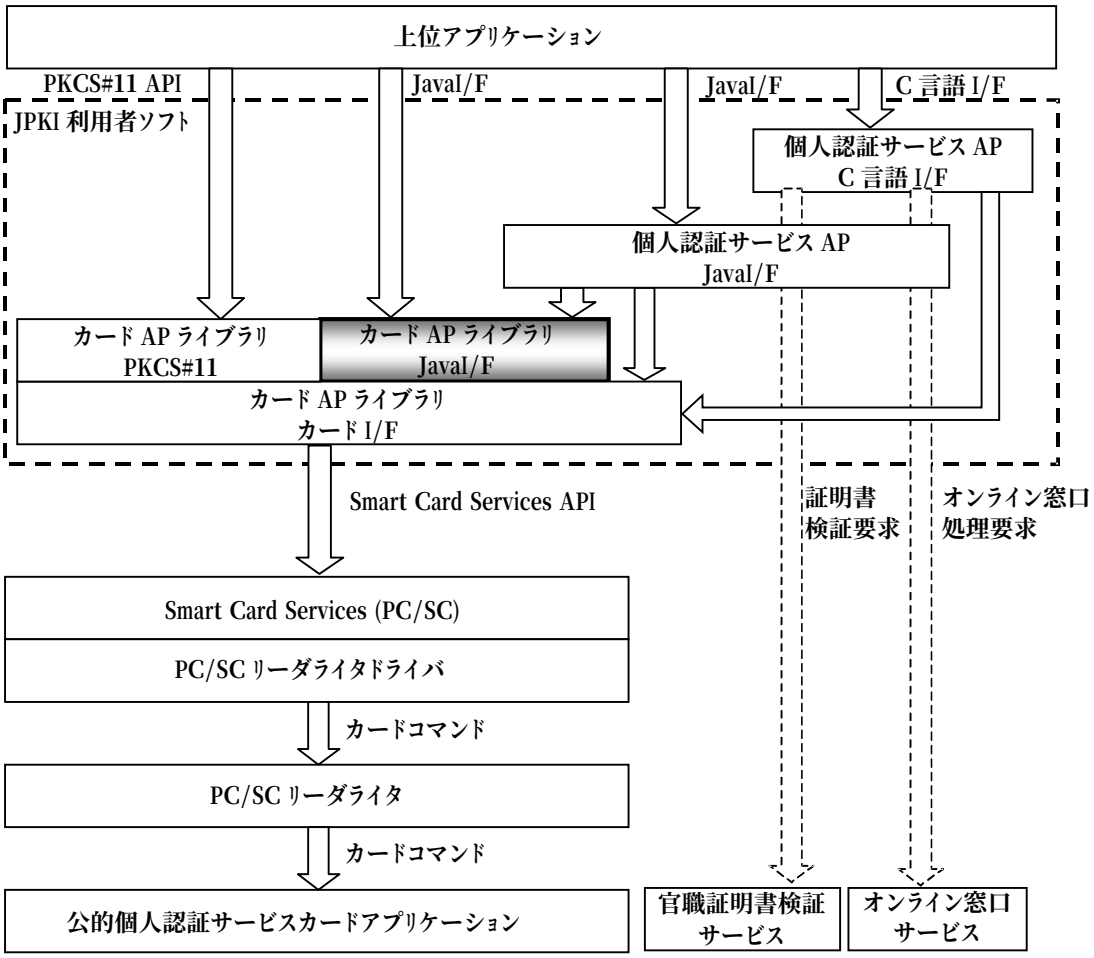



**図 4-2 ソフトウェア構成図 (MacOS 対応版)**

## 第２節　実現可能な機能の一覧

カード AP ライブラリ(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 実現可能な機能の一覧**

| NO | 機能 | 概要 |
|---|---|---|
| 1 | 利用者証明書取得 | IC カードに格納された利用者証明書を取得する。 |
| 2 | 認証局の自己署名証明書取得 | IC カードに格納された認証局の自己署名証明書を取得する。 |
| 3 | 署名生成(署名対象データを渡すパターン) | 署名対象データからハッシュ値を計算し、IC カードに格納された利用者秘密鍵を使用して電子署名を生成する。 |
| 4 | 署名生成(ハッシュ値を渡すパターン) | ハッシュ値に対して、IC カードに格納された利用者秘密鍵を使用して電子署名を生成する。 |
| 5 | 署名検証(検証対象データを渡すパターン) | 検証対象データからハッシュ値を計算し、ハッシュ値、電子署名、公開鍵を使用して電子署名を検証する。 |
| 6 | 署名検証(ハッシュ値を渡すパターン) | ハッシュ値、電子署名、公開鍵を使用して電子署名を検証する。 |
| 7 | 繰り返し署名生成(署名対象データを渡すパターン) | NO3 の処理を繰り返し実行し、複数の署名対象データに対する電子署名を生成する。 |
| 8 | 繰り返し署名生成(ハッシュ値を渡すパターン) | NO4 の処理を繰り返し実行し、複数のハッシュ値に対する電子署名を生成する。 |
| 9 | 繰り返し署名検証(検証対象データを渡すパターン) | NO5 の処理を繰り返し実行し、複数の電子署名を検証する。 |
| 10 | 繰り返し署名検証(ハッシュ値を渡すパターン) | NO6 の処理を繰り返し実行し、複数の電子署名を検証する。 |

# 第５章　API 仕様

カード AP ライブラリ(Java インターフェース)の API 仕様については、表 ５-１を参照のこと。

**表 ５-１ 対応 JavaDoc**

| NO | OS | 証明書種別 | | JavaDoc |
|---|---|---|---|---|
| | | IC カード | 証明書 | |
| 1 | Windows(32bit) | 住基カード | 署名用電子証明書 | JPKICryptJNI javadoc(32bit) |
| 2 | | 個人番号カード | 署名用電子証明書 | JPKICryptSignJNI javadoc(32bit) |
| 3 | | 個人番号カード | 利用者証明用電子証明書 | JPKICryptAuthJNI javadoc(32bit) |
| 4 | Windows(64bit) | 住基カード（※） | 署名用電子証明書 | JPKICryptJNI javadoc(64bit) |
| 5 | MacOS | 個人番号カード | 署名用電子証明書 | JPKICryptSignJNI javadoc(64bit) |
| 6 | | 個人番号カード | 利用者証明用電子証明書 | JPKICryptAuthJNI javadoc(64bit) |

※住基カードは Windows 版のみ使用可能。

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
# 【カード AP ライブラリ Java 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。