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１.1版

公的個人認証サービス　指定認証機関

財団法人　自治体衛星通信機構

変更履歴

版数	変更内容
1.0 版	新規作成
1.1 版	Windows XP SP2 対応に伴い表 1(2 頁)のプラットホームを追加

－ 目次 －

第１章　はじめに

利用者クライアント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２章　ドキュメント体系

利用者クライアント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。

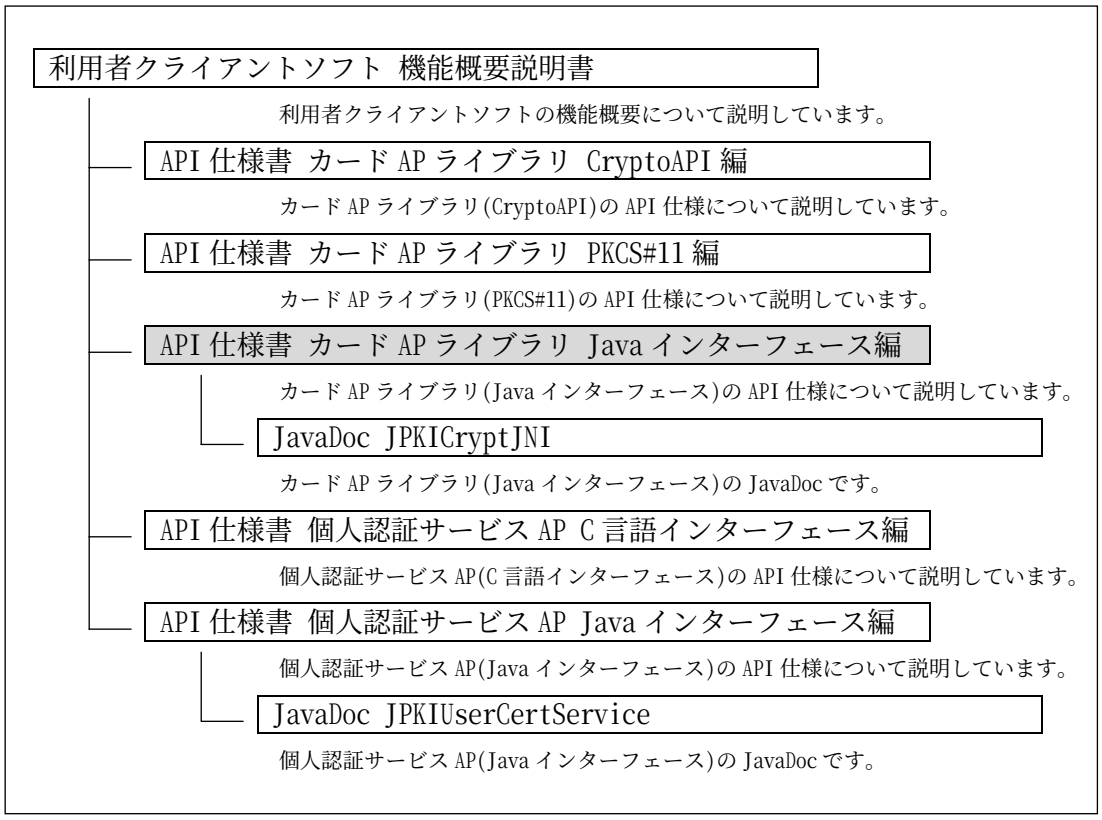

図 1 ドキュメント体系図

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 1 動作環境

項目	条件
プラットフォーム	Windows98 Second Edition(※1) Windows Millennium Edition(※1) WindowsNT4.0 ServicePack6a(※1) Windows2000 ServicePack2 Windows2000 ServicePack3 Windows2000 ServicePack4 WindowsXP ServicePack1 WindowsXP ServicePack2
Web ブラウザ(※2)	Internet Explorer5.5 ServicePack2(※3) Internet Explorer6 ServicePack1(※3) Netscape6.1 Netscape6.2.3 Netscape7.02 Netscape7.1
JavaVM(※4)	JRE 1.3.1 JRE 1.4.0 JRE 1.4.1 JRE 1.4.2
IC カード	公的個人認証サービスカードアプリケーションを搭載し、公的個人認証サービスの電子証明書が格納されたICカードとする。
IC カードリーダライタ	以下の条件を満たす IC カードリーダライタとする。(「適合性検証済み IC カードリーダライター覧」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 ・ USB や RS-232C 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 ・ 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 IC カードの利用のため、Microsoft Smart Card Base Components が必要になる。

※2 Java アプレットから利用者クライアントソフトを利用する場合にいずれかが必要。

※3 暗号機能等の利用のために Microsoft Internet Explorer5.5 ServicePack2 もしくは Microsoft Internet Explorer6 ServicePack1 が必要。

※4 Java アプリケーション(アプレット含む)から利用者クライアントソフトを利用する場合にいずれかが必要。利用者クライアントソフトでは Microsoft JavaVM はサポートしない。

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、利用者クライアントソフトのうち、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。

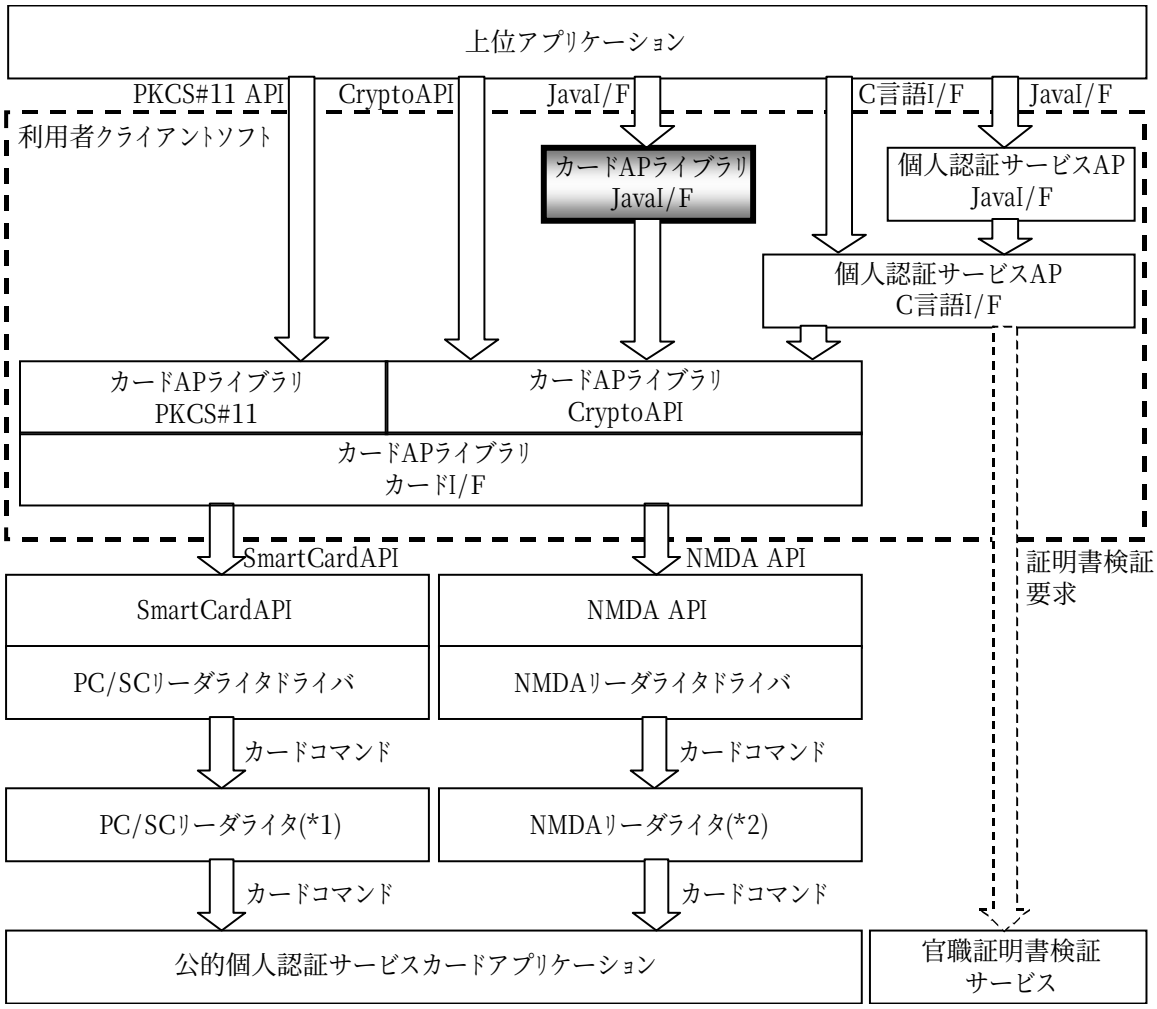

図 1 ソフトウェア構成図

*1 Personal Computer/Smart Cardの略。Microsoft社等のワーキンググループが推進する、Windows環境におけるICカード利用のための統一規格(PC/SC規格)に対応したICカードリーダライタのことを指す。

*2 New Media Development Associationの略。(財)ニューメディア開発協会「IT装備都市研究事業 リーダライタ共通インターフェース仕様書 1.1 版[平成 14 年 5 月 29 日]」に対応したICカードリーダライタのことを指す。

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 2 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	都道府県知事の自己署名証明書取得	IC カードに格納された都道府県知事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、JavaDoc (JPKICryptJNI)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
【カード AP ライブラリ Java インターフェース編】

第１．１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。

※総務省は、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。

※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申請・届出等の行政手続等以外の目的で利用すること。

（2） 利用者クライアントソフトに対し、総務省に許可なく改造等を行うこと。