JAHIS

セキュリティ委員会報告書

Japanese

Association of

Healthcare

Information

Systems Industry

ＪＡＨＩＳ
ＨＰＫＩ　マルチプラットフォーム対応ガイド

２０２０年３月

一般社団法人 保健医療福祉情報システム工業会

医療システム部会　セキュリティ委員会

HPKI 電子署名規格作成 WG

ＪＡＨＩＳ　ＨＰＫＩマルチプラットフォーム対応ガイド

ま　え　が　き

JAHIS セキュリティ委員会としては厚生労働省の推進するヘルスケア PKI（以下 HPKI）に対応する JAHIS 標準として「JAHIS ヘルスケア PKI を利用した医療文書に対する電子署名規格 Ver.2.0」、「JAHIS HPKI 電子認証ガイドライン V1.1 」、「JAHIS HPKI 対応 IC カードガイドライン Ver.3.0」等を策定してきた。現在まで様々なユースケースで利用されているが、HPKI 認証局にて動作保証を行っているモジュールについて動作保証範囲が特定のプラットフォームにとどまっていることから、他のプラットフォームでの利用について会員各社より対応方法の問い合わせを受けている状況である。

上記を鑑み、JAHIS セキュリティ委員会としては HPKI 電子保存規格作成 WG を中心に関係委員会の協力のもと HPKI マルチプラットフォーム対応ガイドを作成した。

本書は現時点の各種プラットフォームにおける対応方法について調査した結果をとりまとめたものであり、プラットフォーム提供各社のプラットフォームの改定などにより陳腐化する可能性があることから JAHIS 標準類としてではなく、報告書として取りまとめることとした。

本書はあくまで調査時点での公開情報を基に取りまとめたものであるので、利用にあたっては利用者の責任においてプラットフォーム提供各社の最新情報を確認の上利用いただきたい。

２０２０年３月

一般社団法人 保健医療福祉情報システム工業会
医療システム部会 セキュリティ委員会
HPKI 電子署名規格作成 WG

<<　告知事項　>>

本規約は関連団体の所属の有無に関わらず、規約の引用を明示することで自由に使用することができるものとします。ただし一部の改変を伴う場合は個々の責任において行い、本規約に準拠する旨を表現することは厳禁するものとします。

本規約ならびに本規約に基づいたシステムの導入・運用についてのあらゆる障害や損害について、本規約作成者は何らの責任を負わないものとします。ただし、関連団体所属の正規の資格者は本規約についての疑義を作成者に申し入れることができ、作成者はこれに誠意をもって協議するものとします。

目　　次

1. はじめに

JAHIS セキュリティ委員会としてはHPKI 電子署名規格作成WG を中心に関係委員会の協力のもとHPKI マルチプラットフォーム対応ガイドを作成した。

本書は現時点の各種プラットフォームにおける対応方法について調査した結果をとりまとめたものであり、プラットフォーム提供各社のプラットフォームの改定などにより陳腐化する可能性があることからJAHIS 標準類としてではなく、報告書として取りまとめることとした。

本書はあくまで調査時点での公開情報を基に取りまとめたものであるので、利用にあたっては利用者の責任においてプラットフォーム提供各社の最新情報を確認の上利用いただきたい。

また、本書はシステム実装について詳細な解説は行っていない。あくまで参考資料の位置づけであるので、不足する情報については各プラットフォームの他の公開資料などを参照願う。

2. 概要

本書はJAHIS 標準類に準拠したHPKI カードを利用して署名や認証を行う際のプラットフォームについて調査した結果をとりまとめたものである。調査対象としては、OS ごとの対応状況や仮想 OS での対応状況、ブラウザの対応状況、カードドライバの最新状況などを調査している。特にGoogle Chrome における署名と認証の実装方法については、普及率や現場のニーズを踏まえて集中的な調査を行い現状の実装方法を取りまとめた。

3. 主な用語

MEDIS
一般財団法人 医療情報システム開発センター

NFC 機能
NFC(Near Field Communication)
近距離無線通信規格の一つで、国際標準となっております。かざすだけで周辺機器と通信できるため IC カードやスマートフォンなどで利用されています。

NFC ポート（旧 FeliCa ポート）
FeliCa の規格を用いたIC カード上のデータを読み書きするためのカードリーダの総称です。

OpenSC
OpenSC は、認証、暗号化、デジタル署名などのセキュリティの機能が、IC カードで動作するソフトウェアツールとライブラリのセットになったミドルウェアです。

PC/SC (Personal Computer/Smart Card)
Windows 環境でIC カードやリーダ/ライタ（R/W）を相互利用するための標準規格です。

PC/SC Lite
Linux 環境でIC カードやリーダ/ライタ（R/W）を相互利用するための標準規格です。

PKCS#11
RSA セキュリティにより考案された公開鍵暗号技術を標準化するための規格です。電子証明書をIC カードに格納するAPI 等を定義しています。

4. HPKI を用いた認証：TLS1.2 をベースに認証機能を実装する上での構成要素

図 4.1 はクライアント PC（Windows）のウェブブラウザを用いて行う例を記載している。
各 OS で稼働するウェブブラウザは様々な種類が存在するが、医療分野に於いては TLS1.2 に対応したクライアント認証機能が実装されている必要がある。HPKI に於いてはクライアント証明書と秘密鍵はロクライアント PC に接続された IC カード RW 経由、もしくは端末に実装された RW で HPKI カードにアクセスして TLS クライアント認証を行えることが必要である。
ウェブブラウザは HPKI カードドライバが提供する PKCS#11 もしくは CryptoAPI のいずれかを使用する。
動作可能な IC カード RW については、動作する物、しない物が存在するので個別に検証が必要である。

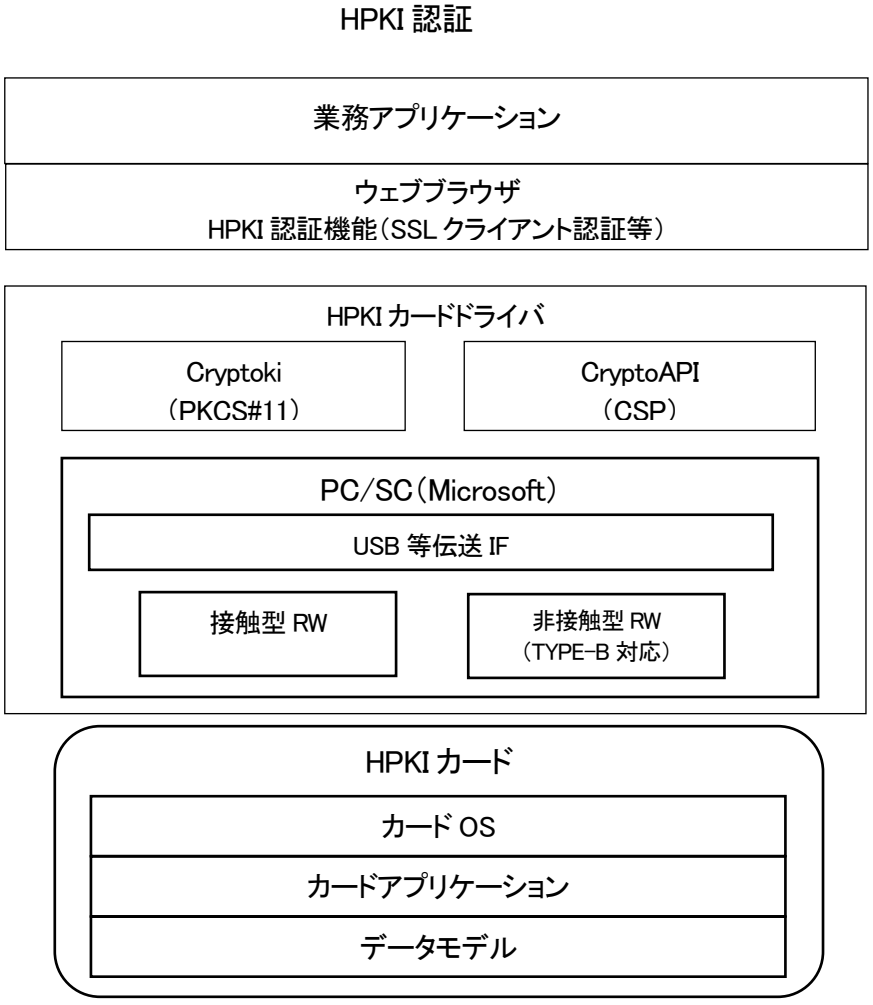

図 4.1　ウェブブラウザを用いて HPKI 認証を行う例

5. HPKI を用いた署名：文書に対する署名機能を実装する上での構成要素

図 5.1 はクライアント PC（Windows）のローカルアプリケーションで署名を行う例を記載している。
署名機能はクライアント PC に接続された IC カード RW 経由、もしくは端末に実装された RW を介して HPKI カードの証明書と秘密鍵にて暗号演算する必要がある。
署名を行う業務アプリケーションは署名フォーマット（CAdES/XAdES/PAdES）に応じた署名アプリケーション（署名ライブラリ）を利用する場合が多い。
署名ライブラリは HPKI カードドライバが提供する PKCS#11 もしくは CryptoAPI のいずれかを使用する。
動作可能な IC カード RW については、動作する物、しない物が存在するので個別に検証が必要である。

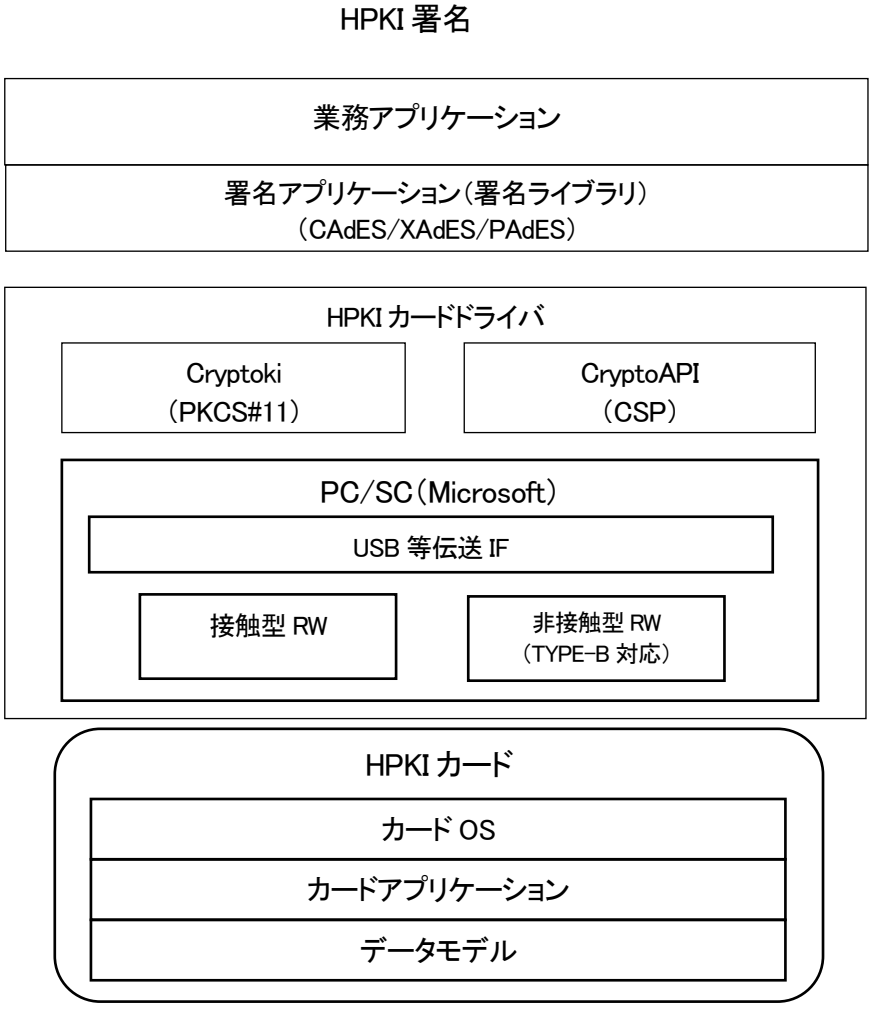

図 5.1　ローカルアプリケーションで HPKI 署名を行う例

6. HPKI の署名検証と証明書検証

HPKI における署名検証と証明書検証については、「JAHIS 標準 18-006 : JAHIS ヘルスケア PKI を利用した医療文書に対する電子署名規格 Ver.2.0」を参照すること。概要が同規格の「５.１ 電子署名の基本要件（p.13-14）」に、詳細が「６.２ 電子署名の検証（共通事項）（p.20-29）」に示されている。

基本的な処理は一般の PKI と同等であるが、医師等の資格要件によって検証の成否を判断する必要がある場合には、署名者証明書の hcRole 属性の値を参照すべき点が HPKI 特有の要件である。

7. OS ごとの HPKI カード対応状況

7.1. OS ごとのサポート状況

HPKI カードを利用する場合には、IC カードを読み取る IC カード R/W と IC カードにアクセスする API を OS がサポートしている必要がある。

以下は各 OS の IC カードへアクセスする対応と、IC カードにカード R/W の状況を示す。

表 7.1 各 OS の IC カードへのアクセス対応およびカード R/W 対応状況

OS	OS 対応状況	IC カード R/W
Windows	PCSC 経由でアクセスが可能。 なお、日医、日薬、MEDIS からドライバ（PKCS#11、CSP ライブラリ）提供中	PaSoRi、ACR39、SCR3310 等
Linux	PCSC lite 経由でアクセスが可能。	ACR39、SCR3310 等
Android	Android9 から拡張 APDU をサポート。	内蔵 NFC ポート （搭載しない機種あり）
OSX (Mac OS)	MacOS 10.12 から CryptoTokenKit による IC カードアクセスをサポート。	ACR39、SCR3310 等
iOS (iPhone)	iOS13 から内蔵 NFC で APDU コマンドをサポート。	内蔵 NFC ポート (iPad に NFC ポートはなし)

表 7.1 のうち、Windows については、「４．HPKI を用いた認証 : TLS1.2 をベースに認証機能を実装する上での構成要素 HPKI カードを利用する場合」(以下第 4 章)、「５．HPKI を用いた署名 : 文書に対する署名機能を実装する上での構成要素」(以下第 5 章)にて説明されている通りである。Windows 以外の OS については、第 4 章の図 4.1 および第 5 章の図 5.1 の「PC/SC（Microsoft）」の部分が、それぞれ表 7.1 の「OS 対応状況」の内容に差し代わる形となる。同図での「接触型 RW」、「非接触 TYPE-B」にあたる箇所に実際に使用できるものが存在するかどうかについては、表 7.1 の「IC カード R/W」に現在の状況を示してある。

ドライバが提供されているのはWindowsのみという場合もあるので、Windows以外のOSを使用する場合は事前に確認が必要である。

7.2. ICカードR/Wが動作対応していないOSでの対応方法

7.2.1. 仮想OSによる対応

ICカードR/Wが動作するOSについては各メーカのドライバの提供状況に依存する。ドライバが提供されているのはWindowsのみという場合もある。このような場合の対応方法の一つに、仮想OSを利用した方法がある。ICカードR/Wのドライバが提供されていないOSをホストOSとし、ICカードR/Wが提供されているOSをゲストOSとして、ゲストOSのICカードR/Wのドライバを利用する方式が存在する。以下の動作条件での例をいくつか提示する。

・ホストOS：Linux
・ゲストOS：Windows10等

7.2.2. VMWare

VMware, Inc.が提供している製品を利用しゲストOSを動作させる。デバイスの設定は2種類ある。

・仮想モード
　接続されているICカードR/W等USBデバイスを仮想的にゲストOSに接続した状態とし、ホストOSからもデバイスが利用できるようにする。
・USBパススルーモード
　接続されているICカードR/W等USBデバイスを、ホストOSではスルーさせて、ゲストOSから直接制御できるようにする。ホストOSからは利用できなくなる。

7.2.3. Oracle VM VirturlBOX

Oracle社が提供している仮想環境を利用し、ゲストOSを動作させる。VMWareと同様に、仮想モード以外にパススルーモードも利用可能である。パススルーモードの場合、認識さえしていればLinuxで利用できないデバイスでも動作できるとのこと。

7.2.4. KVM(Kernel-based Virtual Machine)

Linuxに組み込まれている仮想化基盤を利用してゲストOSを動作させる。別途製品を導入しなくても済む。設定等にはvirt-managerを使用する。virt-managerにて使用するデバイスに対してリダイレクトの設定にてゲストOSで利用可能となる。この場合ホストOSでは使用不可となる。

8. ブラウザ毎の HPKI カード対応状況

HPKI カードをブラウザで使用する場合には、TLS 認証と、Web アプリケーションでの認証/署名の２つのケースが有る。

（1）TLS 認証の場合
ブラウザが HPKI カード内の証明書を TLS で使用する機能を実装している必要がある。

（2）Web アプリケーションでの認証/署名
ブラウザ上で動作する JavaScript 等の Web アプリケーションは、セキュリティの問題からローカルリソース（IC カードへのアクセス）へのアクセスは制限されている。ただし、ブラウザではローカルリソースへアクセスするために拡張機能などをサポートしており、この機能を利用することで、Web アプリケーションから HPKI カードへアクセスすることが可能となる。

以下に各ブラウザの対応状況を示す。

表 8.1 ブラウザ毎のサポート状況

ブラウザ	TLS 認証（カッコ内は I/F）	Web アプリケーションからの署名
IE	OS 証明書ストア (CSP/KSP 等)	ActiveX
Edge	OS 証明書ストア (CSP/KSP 等)	拡張機能(Native Messaging)※
Firefox	NSS Database (PKCS#11)	拡張機能(Native Messaging) ※
Google Chrome	OS 証明書ストア (CSP/KSP、CryptoTokenKit、PKCS#11 等)	拡張機能(Native Messaging) ※
Safari	OS 証明書ストア (CryptoTokenKit)	Safari アプリ拡張機能 (macOS 10.12 以降、および Safari 10)

※：モバイル版は未サポート

9. Google Chrome における署名と認証の実装方法

Google Chrome(以下 Chrome)で HPKI カードを使用する場合には OS に応じた実装が必要となる。以下に OS 毎のサポート状況と実現方法を示す。なお、動作確認例がある場合においても実装者が自らの責任において確認することが推奨される。

表 9.1 OS 毎のサポート状況

項目	TLS 認証	Web アプリケーションからの署名		備考
		拡張機能 (Native Messaging)	WebUSB API	
Windows	◎ HPKI カードの動作確認例有	◎ HPKI カードの動作確認情報有	△ Felica アクセス動作確認情報有	TLS 認証は OS 証明書ストア(CSP/KSP)
Linux	○ IC カード動作確認情報有	△ Chrome 開発者向けに設定情報有	△ Felica アクセス動作確認情報有	TLS 認証は NSS Database (PKCS#11)
Android	要調査（※）	× 拡張機能未サポート	△ Felica アクセス動作確認情報有	
OSX (Mac OS)	○ IC カード動作確認情報有	△ Chrome 開発者向けに設定情報有	△ Felica アクセス動作確認情報有	TLS 認証は OS 証明書ストア(CryptoTokenKit)
iOS (iPhone)	要調査（※）	× 拡張機能未サポート	要調査（※）	

◎：HPKI カードの動作確認情報有
○：IC カードの動作確認情報有
△：何らかの動作確認情報有
×：未サポート
（※）JAHIS として調査を行ったが適切な資料を検索できなかった。

9.1. TLS 認証について

TLS 認証は Chrome が TLS クライアント認証で使用する証明書は OS 標準の証明書ストアを使用している。したがって、証明書ストアから HPKI カードにアクセスする API は OS がサポートしている必要がある。

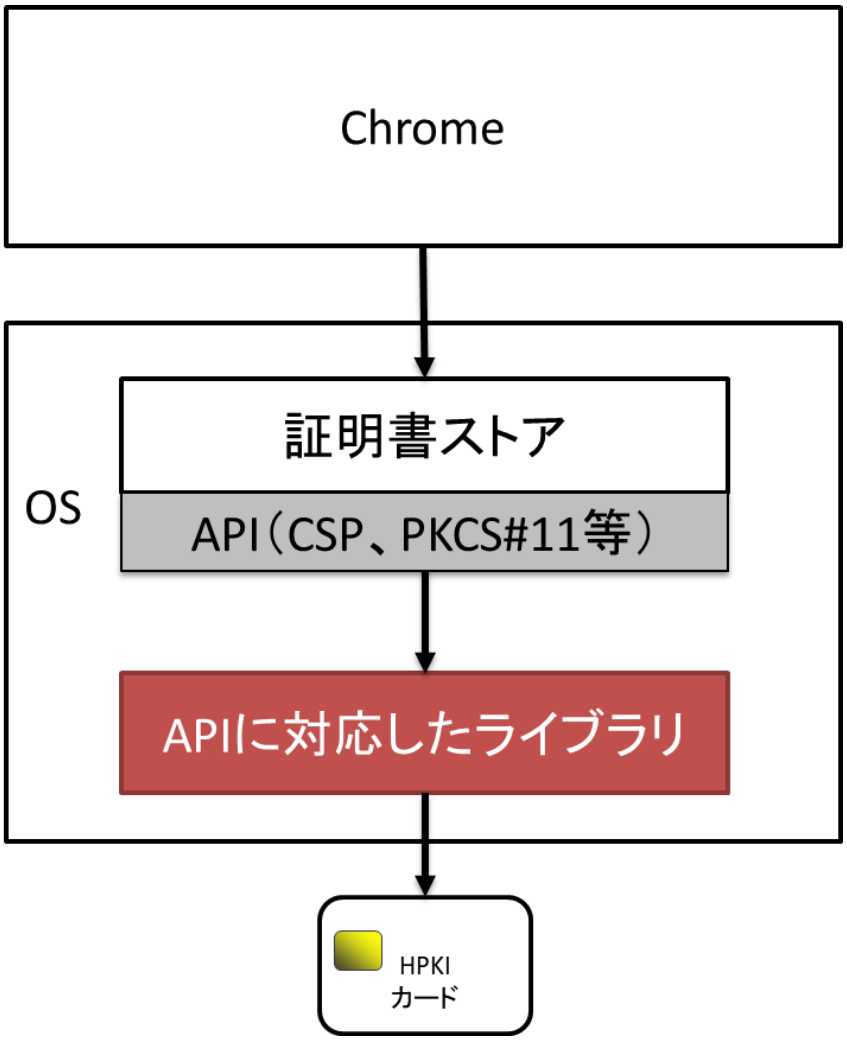

図 9.1 TLS 認証の概要図

9.2. 拡張機能 (Native Messaging) について

Chrome 上の Web アプリケーションからの署名するために必要となる拡張機能(Native Messaging)は、拡張機能と Native Host から構成される。

Web アプリケーションから、“拡張機能”と“Native Host”を経由して、HPKI カードにアクセスする。

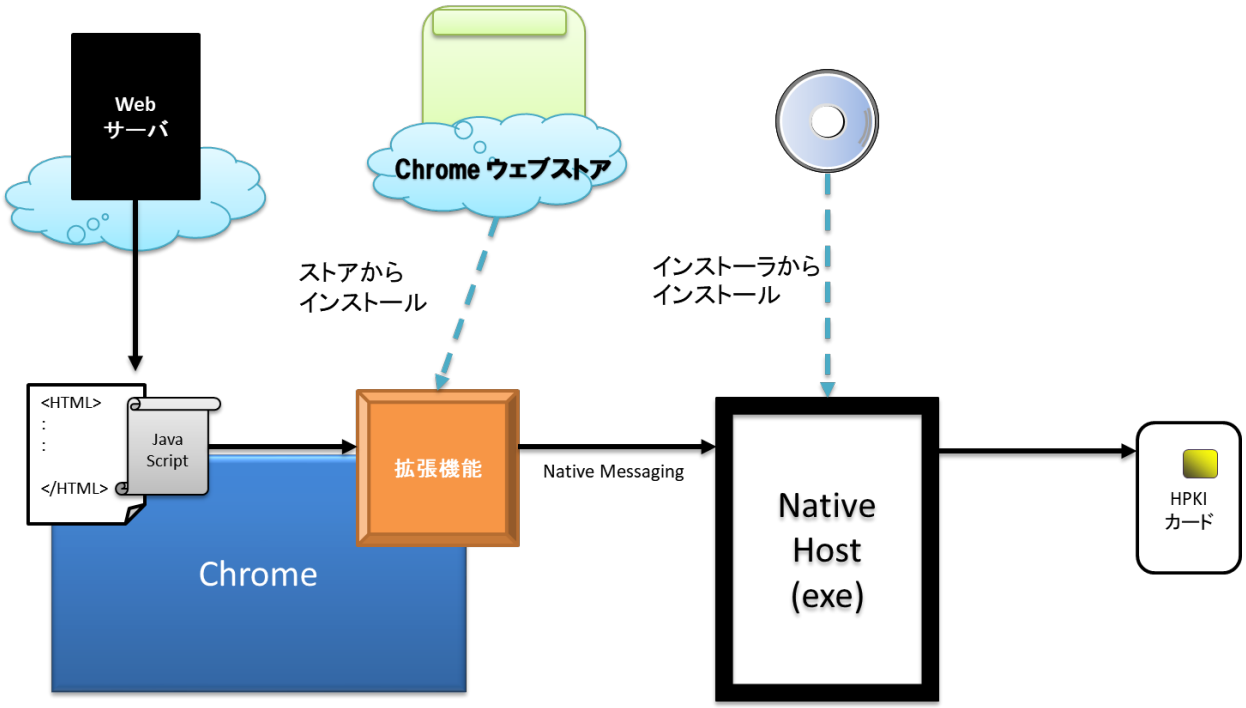

図 9.2 拡張機能（Native Messaging）の概要図

9.2.1. 拡張機能について

拡張機能は、Chrome の Web アプリケーションから呼び出すことができ、Javascript で実装される。
なお、v71 から Chrome ストア以外からの拡張機能がインストールできなくなった。

9.2.2. NativeHost について

NativeHost は拡張機能から起動するアプリケーションで、通常のアプリケーションと同様にローカルリソースへ自由にアクセスが可能となる。
なお、NativeHost は事前に作成の上、インストールしておく必要がある。

9.2.3. 拡張機能（セキュリティ）

Chrome では Web アプリケーションからローカルリソースにアクセスすることからセキュリティ機能として利用できるリソースや URL などを制限することができるようになっている。セキュリティ設定は、ユーザと拡張機能開発者がそれぞれで設定を行う機能が用意されている。

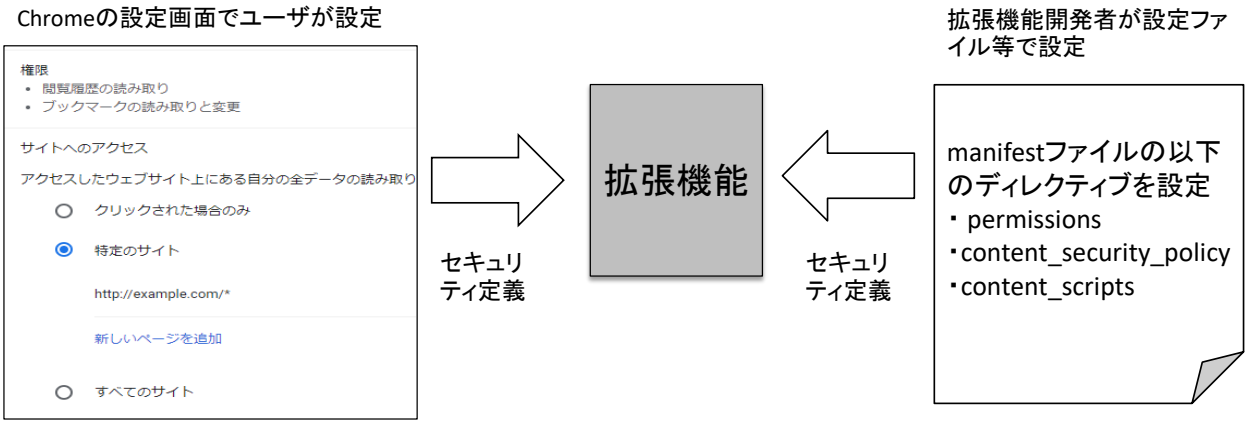

図 9.3 拡張機能セキュリティの構成イメージ

以下に設定できる機能詳細を示す。

表 9.2 拡張機能セキュリティ項目

セキュリティ項目	内容	設定者	設定方法	備考
拡張機能を利用できるサイト制限	拡張機能が使用できる Web サイトを制限する	利用者	Chrome の設定画面で設定	
		拡張機能開発者	manifest ファイルの content_scripts に利用可能なサイトの URL を記載	
拡張へのリソースの利用制限	Chrome の API（ファイル、位置情報等）の利用および、拡張機能からアクセスする URL がある場合に指定する	拡張機能開発者	manifest ファイルの permission を設定（導入時に利用者が許可する。）	Chrome の設定画面で拡張機能に設定されたアクセス権を確認できる。
拡張機能への外部サイトの利用制限	拡張機能のコンテンツセキュリティポリシー（外部サイトのアクセス先制限等）	拡張機能開発者	manifest ファイルの content_security_policy を設定	Permission でアクセスするドメインの許可設定が必要。

9.3. WebUSB API について

WebUSB API は Google Chrome に実装されており、PC に接続された USB デバイスにウェブから直接アクセスすることができるものである。ブラウザが Google Chrome に限定されるが、ドライバが提供されていない OS にて USB デバイスを使用する手段として利用できる。専用ドライバにて動作している USB デバイスは認識できないため、ドライバが提供されていないものを利用するための場合に限定して利用することが望ましい。

デフォルト設定の場合、ユーザが Web ページと USB デバイスの相互通信を明示的に許可することで開始されるため、その操作を手順に入れる必要がある。接続デバイスはベンダ ID、プロダクト ID で指定可能である。Google Chrome のデフォルト設定では WEBUSB が有効になっているが、無効にすることができる。

10.その他の環境における実装上の情報

これまで HPKI での実装上の情報を述べてきたが、本章ではその他の類似した環境における実装上の情報を示すことで、HPKI の実装に関する一助となれば幸いである。

10.1. JPKI における Android での実装例

HPKI と HPKI カードと類似した例として、公的個人認証サービス(以下、JPKI)とマイナンバーカードがある。JPKI に関する情報は、地方公共団体情報システム機構(以下、J-LIS)より JPKI が提供する電子証明書を取り扱うソフトウェアを開発するためのライブラリである JPKI 利用者クライアントソフトが提供されており、その技術仕様が公開されている。その中で Android 用の利用者クライアントソフトでは、インテントと呼ばれる Android 上のアプリケーションとアプリケーションの間やソフト内の機能間を繋ぎ合わせる仕組みを利用して、JPKI 利用者クライアントソフトの機能を利用できるように、インテントインターフェースを提供しており、その API 仕様書を公開している。

利用者クライアントソフトに係る技術仕様について
https://www.j-lis.go.jp/jpki/procedure/procedure1_2_3.html

利用者クライアントソフト仕様書（Android 版） － 利用者クライアントソフト機能概要説明書_1.3 版
https://www.j-lis.go.jp/file/11_Android_gaiyou.pdf

利用者クライアントソフト_API 仕様書 － Android インテント編_1.3 版
https://www.j-lis.go.jp/file/12_Android_siyou_intent.pdf

このインテントインターフェースを利用することで、Android 端末の NFC 機能を使用し、マイナンバーカードの IC チップに格納された情報を読み込み、Android 端末で読み込んだ情報を利用することが可能となる。

Android 版の JPKI 利用者クライアントソフト(Ver.1.1)の動作環境は、下記の通り。

表 10.1 Android 版の JPKI 利用者クライアントソフトの動作環境

項目	条件
OS	Android 5.1、6.0.1、7.0 または 8.0 を搭載していること。
NFC	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」※1 を参照。） ・ISO/IEC 14443 Type B に対応している NFC を搭載していること
IC カード	個人番号カードであること。（住基カードは対象外）

※1 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されている。

Android 版の JPKI 利用者クライアントソフトにおけるインテントインターフェースで提供されている機能は下記となる。

表 10.2 インテントインターフェースで提供されている機能

NO	カテゴリ	機能	概要
1	カードAPライブラリ	証明書取得	IC カードに格納された電子証明書(利用者証明書、認証局の自己署名証明書)を取得する。
2		電子署名生成	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。
3		電子署名検証	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。
4	個人認証サービス AP	証明書表示	電子証明書を表示する。
5		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。
6		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。
7		自己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。
8		IC カード種別取得	端末にセットされている IC カードの種別を取得する。

Android 用の JPKI 利用者クライアントソフトのカード AP ライブラリのインテントインターフェースを利用する際のソフトウェア構成図は図 10.1 のようになっている。

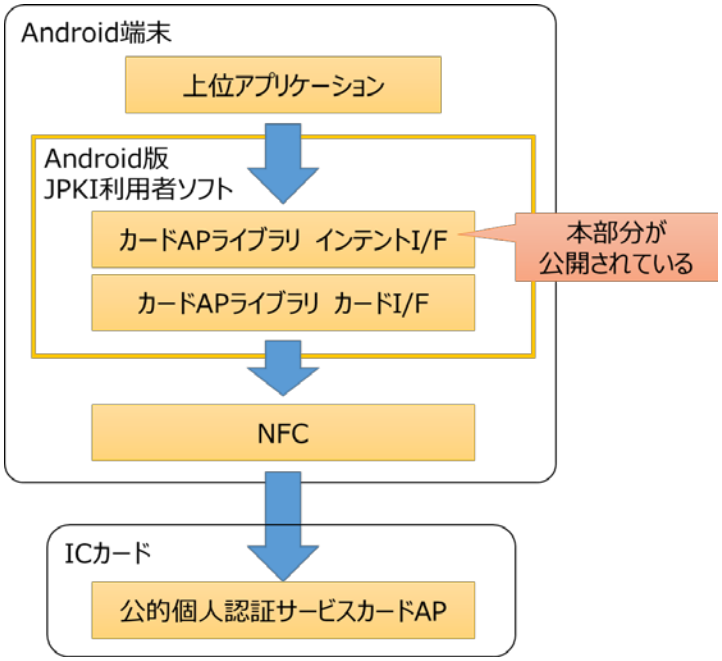

図 10.1 ソフトウェア構成図

Android 版の JPKI 利用者クライアントソフトのインテントインターフェースを利用する際のデータの流れに関する概念図は図 10.2 のようになっており、JPKI 利用者ソフトを利用するための初期処理を行い（図 10.2 中①）、各機能に対応したリクエストコードとリクエストコードに対応した引数を送信し（図 10.2 中②）、IC カードからの結果を処理した結果についてインテントインターフェースを通じ受信（図 10.2 中③）、JPKI 利用者ソフトの利用終了を行うための処理を行い（図 10.2 中④）、上位アプリケーションからマイナンバーカードに格納されている電子証明書にアクセスする等の機能を提供することになる。

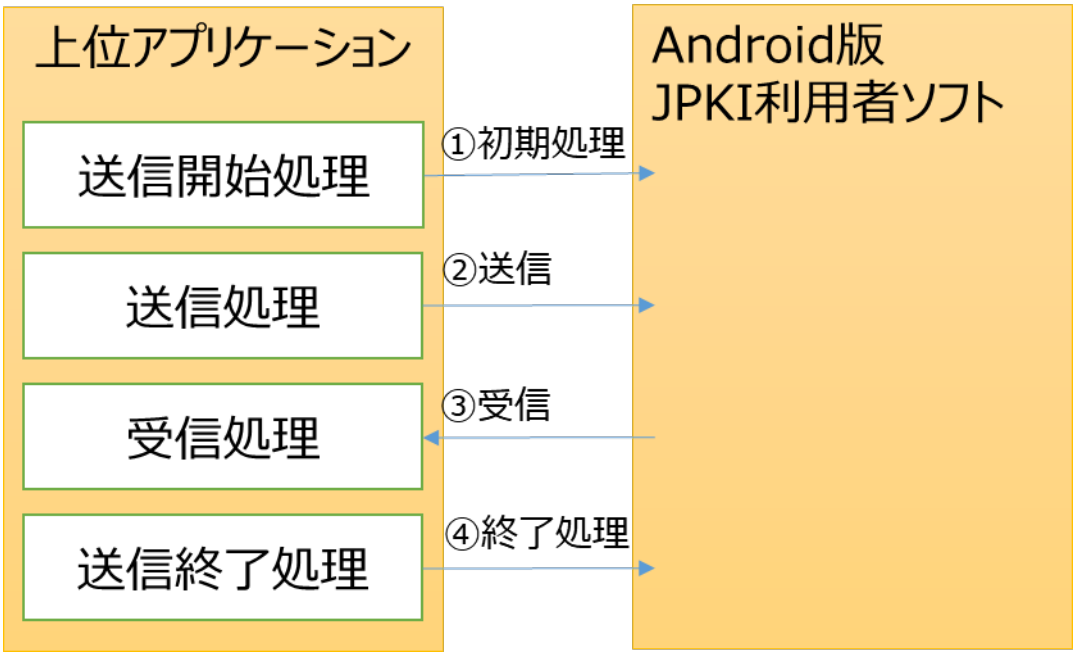

図 10.2 インテント I/F を利用する際のデータの流れに関する概念図

“利用者クライアントソフト_API 仕様書 － Android インテント編_1.3 版”では、各コマンドの詳細なデータ項目が示されているだけでなく、実際の上位アプリケーションからインテントインターフェースを利用しアクセスする際の、コーリングシーケンスが記載されているため参考となる。

付録―１．拡張機能で設定できるセキュリティ項目

（1）拡張機能を利用できるサイト制限

表 11.1 拡張機能を利用できるサイト制限

設定値	内容
クリックされた場合のみ	サイト表示後に対象の拡張機能アイコンをクリックしたときのみ有効となる。
特定のサイト	登録した URL のみ有効となる。
すべてのサイト	すべてのサイトで有効となる。

（2）拡張へのリソースの利用制限

拡張機能に “nativeMessaging”へのアクセスを許可することで、nativeMessaging 経由で HPKI カードへアクセスが可能となる。

表 11.2 拡張へのリソースの利用制限

許可	説明
nativeMessaging	アプリにネイティブメッセージング API へのアクセスを許可

（3）拡張機能への外部サイトの利用制限（content_security_policy）

表 11.3 拡張機能への外部サイトの利用制限

項目	内容
base-uri	ページの <base> 要素に表示できる URL を制限
child-src	ワーカーと組み込みのフレーム コンテンツの URL を列挙。たとえば、child-src https://youtube.com は YouTube の動画を埋め込むことができるが、他のオリジンの動画は埋め込むことができない。廃止された frame-src ディレクティブの代わりに、このディレクティブを使用してください。
connect-src	（XHR、WebSockets、EventSource を経由して）接続できるオリジンを制限
default-src	デフォルトでは、ディレクティブに制限はなし。ディレクティブに特定のポリシーを設定しない場合、たとえば font-src は、有効な参照元として * を指定しても、そのディレクティブがデフォルトで動作する（たとえば、制限なしでどこからでもフォントを読み込むことができる）。このデフォルトの動作は、default-src ディレクティブを指定することで上書きできる。 このディレクティブは、未指定のディレクティブの大半に対してデフォルトを定義。
font-src	ウェブフォントを配信できるオリジンを指定する。Google のウェブフォントは font-src https://themes.googleusercontent.com で有効化できる。
form-action	<form> タグからの送信の有効なエンドポイントを列挙する。
frame-ancestors	現在のページに組み込める参照元を指定する。このディレクティブは、<frame>、<iframe>、<embed>、<applet> タグに適用される。<meta> タグには使用できず、非 HTML リソースのみに適用される。

img-src	画像を読み込み可能なオリジンを定義する。
media-src	動画と音声を配信できるオリジンを制限する。
object-src	Flash などのプラグインを制御できる。
plugin-types	ページで起動できるプラグインの種類を制限する。
report-uri	コンテンツ セキュリティ ポリシーが違反されたときにレポートを送信する URL を指定する。 このディレクティブは、<meta> タグで使用できない。
sandbox	ページが読み込めるリソースにではなく、ページで実行できるアクションに制限を加える。 sandbox ディレクティブが存在すると、ページは sandbox 属性を指定した <iframe> 内に読み込まれるように処理される。 このディレクティブは、ページを一意のオリジンに限定したり、フォームの送信を禁止したり、ページに幅広い効果をもたらす。
script-src	特定のページでスクリプト関連の権限を制御するディレクティブ。スクリプトの有効な参照元として 'self' ともう 1 つ、https://apis.google.com を指定する。 ブラウザは HTTPS を介して、オリジンが現在のページおよび apis.google.com の JavaScript を従順にダウンロードし、実行する。
style-src	スタイルシートの script-src に相当する。
upgrade-insecure-requests	ユーザ エージェントに指示して URL スキーマを書き直し、HTTP を HTTPS に変更する。 このディレクティブは、書き直しが必要な古い URL が多数存在するウェブサイトに使用する。

参照 URL：https://developers.google.com/web/fundamentals/security/csp/?hl=ja

付録―２．カードドライバ周辺情報

1. カードドライバとのインタフェース

カードリーダとのインタフェースは、OS に依存している。

⑴ PC/SC (Windows)

PC/SC ワークグループによって仕様が定められている。最新のバージョンは 2.01（2005 年）である。Microsoft 社の OS で採用されており、WinSCard API を通じてカードリーダとの通信を可能としている。

各カードリーダ固有の部分に関してはカードリーダ製造者から提供されるが、ソフトウェア開発者は個別の IC カードリーダのドライバを直接ハンドリングせずに利用可能となっている。

Microsoft 社の認定が行われており、比較的安定した動作を行うカードリーダが数多く販売されている。

⑵ PCSC Lite

LINUX 等の UNIX 系の OS で、OS/SC と同様の目的のための仕様として作成された。
オープンソースウェアとして提供されている。基本は PC/SC のサブセットである。

⑶ CCID　(Chip/Smart Card Interface Devices)

USB で接続される IC カードリーダのインタフェース仕様で、USB working group により策定されている。2005 年 4 月に Rev 1.1 がリリースされている 。

PCSC Lite に準拠した CCID のドライバは、オープンソースウェアとして提供されている。そのため、USB CCID に準拠した ID カードリーダは、固有のドライバを必要としない。

⑷ LINUX への移植

・PCSC-Lite
　　1.8.26 が最新
　　debian (MacOSX への移植を含む)
　　CCID ドライバとして提供されている
　　パッケージ: libccid (1.4.31-1)が最新　(2019 年 8 月)

・ubuntu
　　PCSC-Lite のライブラリとして提供されている
　　1.8.25-2 が最新（2019 年 8 月）

・Arch
　　Pcsclite　1.8.26-1 がリリースされている。
　　2020 年 1 月リリース

⑸ PCSC-Lite 使用に際しての注意

必ずしも動作が保証されているわけではないので、利用する各システムベンダーが対象となるカードリーダで動作確認を行うこと。

2. Open SC

(1) PKCS#11 に加えて、ISO/IEC 7816-15（JIS X 6320-15)も実装されている。
(2) Windows , Mac OS X, LINUX 等で動作する。
Windows は、PC/SC 上で動作する。
Mac OS は、PC/SC（PCSC Lite）で動作する。
LINUX は、OpenCT で動作する。
(3) Open SC は、CCID に準拠するカードリーダをサポート。
(4) Windows , Mac OS X, LINUX 等で動作する。
(5) 最新版は OpenSC 0.20.0 で、2019 年 12 月に登録されている。
(6) 必ずしも動作が保証されているわけではないので、利用する各システムベンダーが対象となるカードおよびカードリーダで動作確認を行うこと。

付録―３．作成者名簿

作成者（社名五十音順）

有馬　一閣	(株)NTT データ
長谷川　英重	JAHIS 特別委員
平田　泰三	JIRA
佐藤　雅史	セコム(株)
瀧　勝也	(株)テクノウェア
佐藤　恵一	日本光電工業(株)
梶山　孝治	(株)日立製作所
宮崎　一哉	三菱電機(株)
茗原　秀幸	三菱電機(株)
酒巻　一紀	三菱電機インフォメーションシステムズ(株)
岩佐　直樹	(株)メドレー
谷内田　益義	(株)リコー

改定履歴		
日付	バージョン	内容
2020/03/19	Ver. 1.0	初版

（ＪＡＨＩＳセキュリティ委員会報告書）
２０２０年3月発行

ＪＡＨＩＳ　ＨＰＫＩマルチプラットフォーム対応ガイド

発行元　一般社団法人　保健医療福祉情報システム工業会
〒１０５－０００４　東京都港区新橋２丁目５番５号
（新橋２丁目ＭＴビル５階）

電話　03-3506-8010　　FAX　03-3506-8070