セコムIS研究所
Intelligent Systems Laboratory

「PKI対応IDカードの相互運用とHPKI対応ICカードガイドライン」

2008年7月3日

セコム㈱IS研究所　松本　泰

「PKI対応IDカードの相互運用とHPKI対応ICカードガイドライン」

セコムIS研究所
Intelligent Systems Laboratory

- 現在、様々な分野においてPKIに対応したIDカードが検討されています。こうしたIDカードの多くは、様々な環境で利用することを想定した幅広い相互運用性が要求されています。
- このような、PKI対応IDカードは、相互運用性を確保するために広くその仕様が公開される必要もあります。
- こうした動向に対応したものとして、2008年6月に公開されたJAHIS(保健医療福祉情報システム工業会)が策定した「HPKI対応ICカードガイドライン」があります。
- 本講演では、PKI対応IDカードの相互運用性に関する技術動向と、「HPKI対応ICカードガイドライン」についての紹介を行います。

仕様が広く公開されたPKI対応IDカードが大量に発行されつつある。。。。

セコムIS研究所
Intelligent Systems Laboratory

IDカード	発行予定枚数	仕様 *1	ミドルウェアのソースコード	テスト仕様	備考
米国 PIV	数百万枚 (*3)	公開	レファレンス実装のソースコードが公開	公開	連邦政府職員と契約業者が保持する。 *2
ベルギー BELPIC	1000万枚	公開	ソースコードが公開	不明	2008年6月現在800万枚発行済み。*2
ドイツ 健康カード	8200万枚	公開	不明	不明	「健康カード」と連携して動作する「医療従事者向けICカード（HPC）」も同様に仕様が公開されている。

*1 ここでの仕様は、主にカードエッジI/F、データモデルの仕様
*2 IPAの「IC・ID カードの相互運用可能性の向上に係る基礎調査」で仕様の詳細を解説している。
*3 TWICS,FRAC,CAC,ACISといった連邦政府職員向け以外も含めると2000万枚程度の計画がある

セコムIS研究所
Intelligent Systems Laboratory

PKI対応IDカードの相互運用と HPKI対応ICカードガイドライン

- PKI ICカードWorkShop
- PKI対応IDカードの相互運用性
- HPKI対応ICカードガイドライン
- まとめ
- 参考
- おまけ(Global Platform)

セコムIS研究所
Intelligent Systems Laboratory

PKI ICカードWorkShop

2007年11月27日(火)
JNSA PKI相互運用技術WGが行った
「PKI ICカードWorkShop」の報告

PKI ICカードWorkShop
目的

セコムIS研究所
Intelligent Systems Laboratory

- PKI ICカードWorkShopでは、仕様が明確なカードや、オープンソースのソフトウェアを使うことにより、ICカードからミドルウェアまでの理解を深めることを目標にします。
- 標準的なGlobal Platform対応のJavaCard、オープンソースのPKI対応JavaCardアプレットのMuscle Card Applet、オープンソースのマルチプラットフォーム対応ミドルウェアのOpenSCを教材として使います。
- WorkShopでは、各参加者のPC(Windows, Mac OS X, LINUX)にOpenSCをインストールし、複数のICカードを扱います。実際に動作させ、講義も並行して行います。
- ICカードとミドルウェアの共通の理解と深めた上で、今後のPKI ICカードの方向性を議論していきます。

PKI ICカードWorkShop 開催概要

セコムIS研究所 Intelligent Systems Laboratory

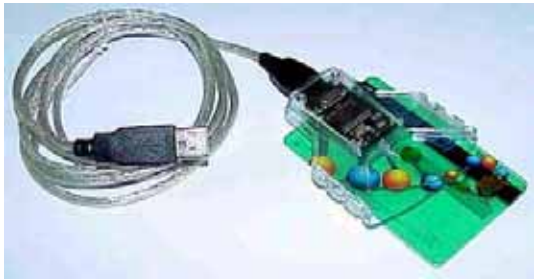
- 参加者
  - 今回は、「PKI相互運用技術WGのメーリングリストメンバー」と「PKI相互運用技術WGのメンバーの紹介者」
  - 当日の参加者は、14名
- 日時
  - 2007年11月27日(火)　10:00 -　終わるまで？？
  - その後、別日程で、2,3時間のディスカッション
- 場所
  - 工学院大学　新宿校舎（中層棟）6階　665号室
- 参加者の感想
  - 1日ではしんどい。。。etc..

PKI ICカードWorkShop
使用したICカードとR/Wなど（１５名分）

セコム IS 研究所
Intelligent Systems Laboratory

- Axalto Cryptoflex E-Gate and Reflex 531
  - $27　15 set
- NXP (Philips) JCOP 20 V2.1/16K
  - $8.00　$40.00　5枚
- GemPC Twin Reader/Writer
  - $22.00　$110.00　R/Wとのセット　5 set 分
- NXP (Philips) JCOP 31 V2.2/36K
  - $15.00　$45.00　3枚
- NXP (Philips) JCOP 41 V2.2.1/72K
  - $19.00　$57.0　3枚
- Oberthur Cosmo Card Dual-Interface
  - $19.00　$38.00　2枚
- Oberthur Cosmo Token (R)
  - $27.00　$54.00　2個
- 購入　http://www.usasmartcard.com/shop/

Cryptoflex E-Gate



GemPC Twin R/W

Oberthur Cosmo Token

PKI ICカードWorkShop
使用したJavaカードと仕様

セコムIS研究所
Intelligent Systems Laboratory

製品	GP バージョン	JC API	容量	価格 *1	その他
NXP JCOP 20	2.0.1	2.2.1	16K	$8	RSA1024bitまで
NXP JCOP 31	2.0.1	2.2.1	36K	$15	Dual-Interface
NXP JCOP 41	2.1.1	2.2.1	72K	$19	Dual-Interface
Oberthur Cosmo Card Dual-Interface	2.1.1	2.2	66K	$19	Dual-Interface
Oberthur Cosmo Token	2.1.1	2.2	66K	$27	USB token
Axalto Cyberflex E-Gate	2.01	2.1.1	32K	-	*2

*1 価格は、http://www.usasmartcard.com/shop/での購入当時の価格

*2 Workshopでは使用せず。事前調査。

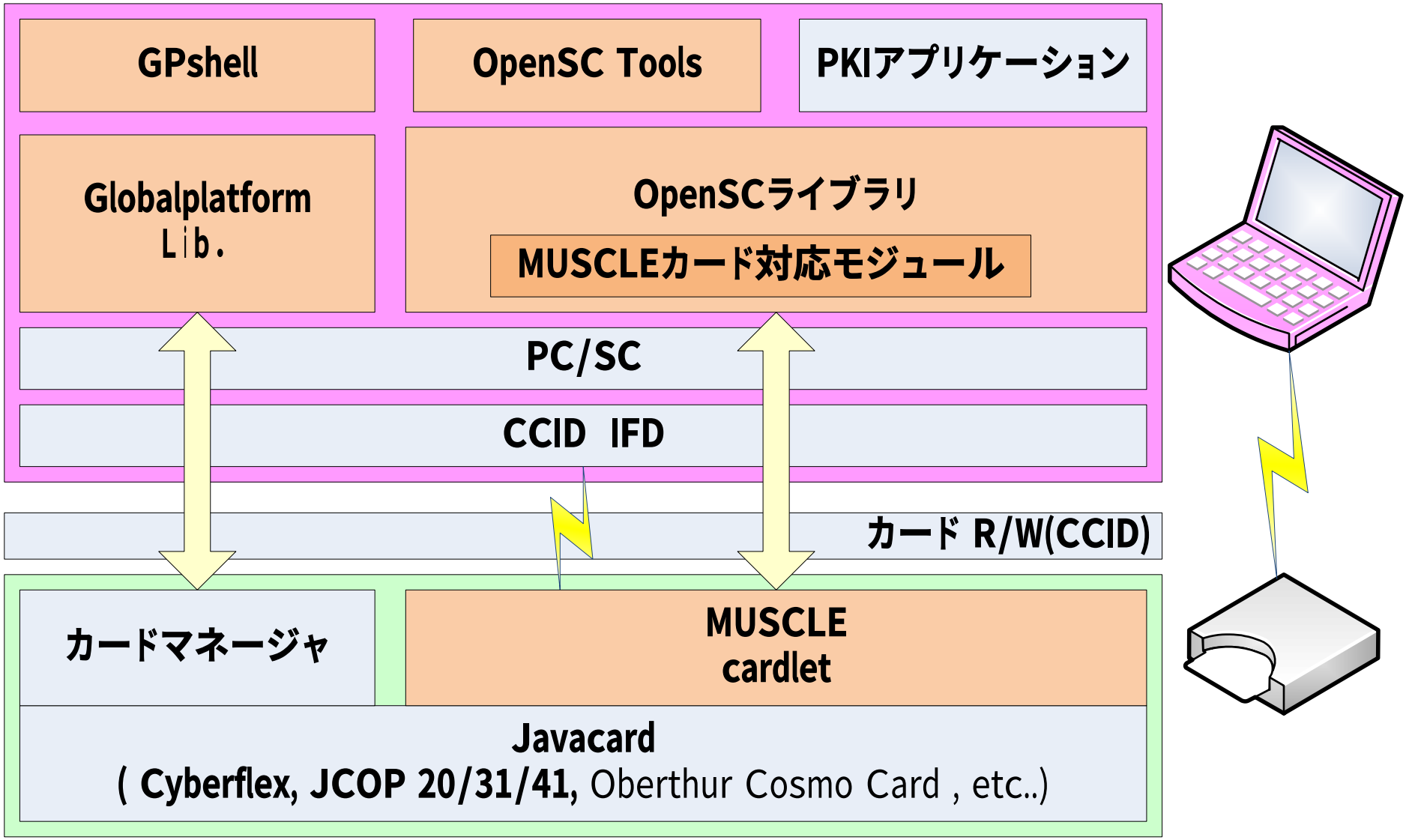
PKI ICカードWorkShop
使用した（主な）ソフトウェア

セコム IS 研究所
Intelligent Systems Laboratory

- OpenSC
  - http://www.opensc-project.org/
  - 色々なICカード、色々なIDカード(BELPIC,FINEID,etc)、色々なプラットフォーム(Windows,Linux,Mac)をサポートしたでオープンソースのPKCS#11, PKCS#15対応ミドルウェア
  - 9万ステップ
- MUSCLEカードアプレット
  - http://www.linuxnet.com/musclecard/index.html
  - オープンソースのPKIx対応のJavaCardアプレット
  - 5000ステップ
- GlobalPlatform 、GPShell
  - http://sourceforge.net/projects/globalplatform
  - オープンソースのGlobalPlatform対応ライブラリ＆ユーティリティ

PKI ICカードWorkShop　Javacardの環境
Javacard,OpenSC,Musclecard,GPShellの関係

セコム IS 研究所
Intelligent Systems Laboratory



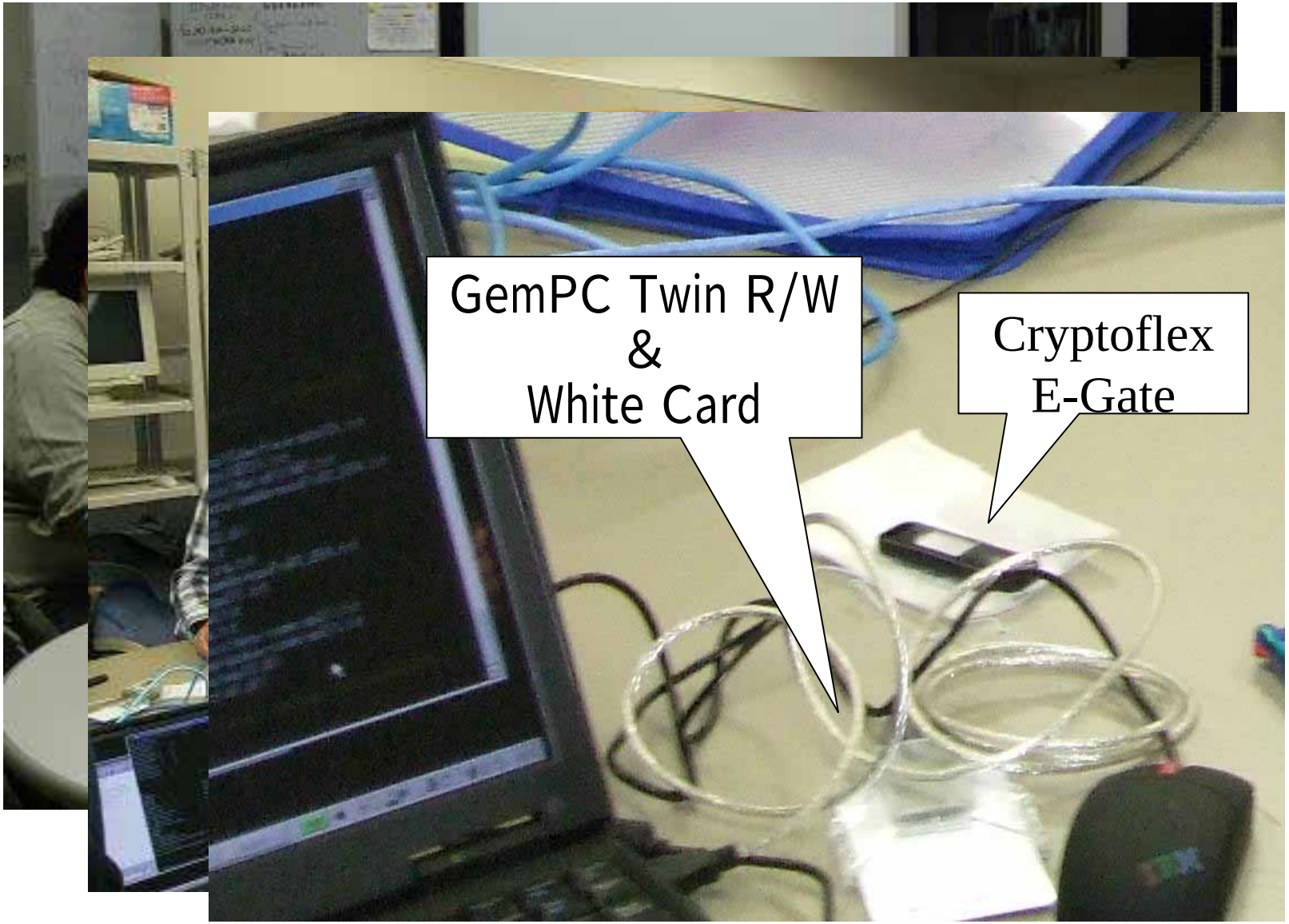
PKI ICカードWorkShopのスケジュール

セコムIS研究所
Intelligent Systems Laboratory

項目	時間	内容
PKI ICカードWorkShopの概要	0.5	概要、スケジュールの説明
ICカードについての講義	1	PKIに利用するICカードの概要
環境の説明+設定	0.5	カード類の配布、プログラム類のInstallと環境設定
Cryptoflexの初期化	1	OpenSCを使ったカードの初期化
OpenSCの使い方	1	OpenSCを使い方とカードの説明
javacarcの初期化	1	GpshellをつかったJavaCardアプレットのダウンロード
GlobalPlatform	0.5	GlobalPlatformの説明
色々なプラットフォーム	0.5	Windows,Linux,Macの環境でのOpenSCの利用など
ICカード(Cryptoflex, javacard)の利用	1	Windows,Linux,MacでOpenSCを使った ICカードアプリケーションの実行
OpenSCの説明	1	OpenSCのアーキテクチャの説明
Javacardのアプレットの開発	1	MUSCLEカードアプレットを題材とした開発方法
まとめ	0.5	まとめ

PKI ICカードWorkShop
WorkShopの様子

セコムIS研究所
Intelligent Systems Laboratory

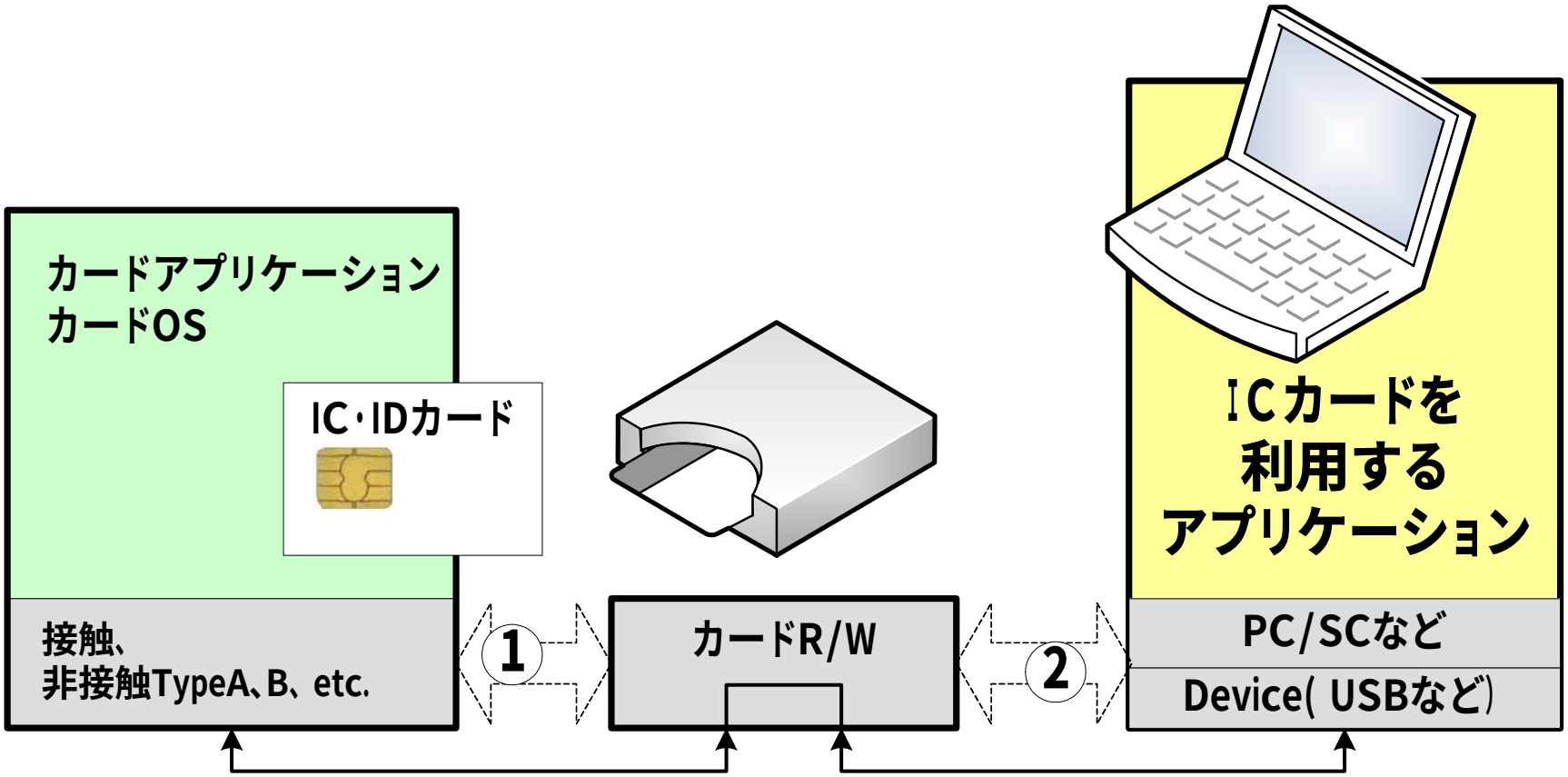


セコムIS研究所
Intelligent Systems Laboratory

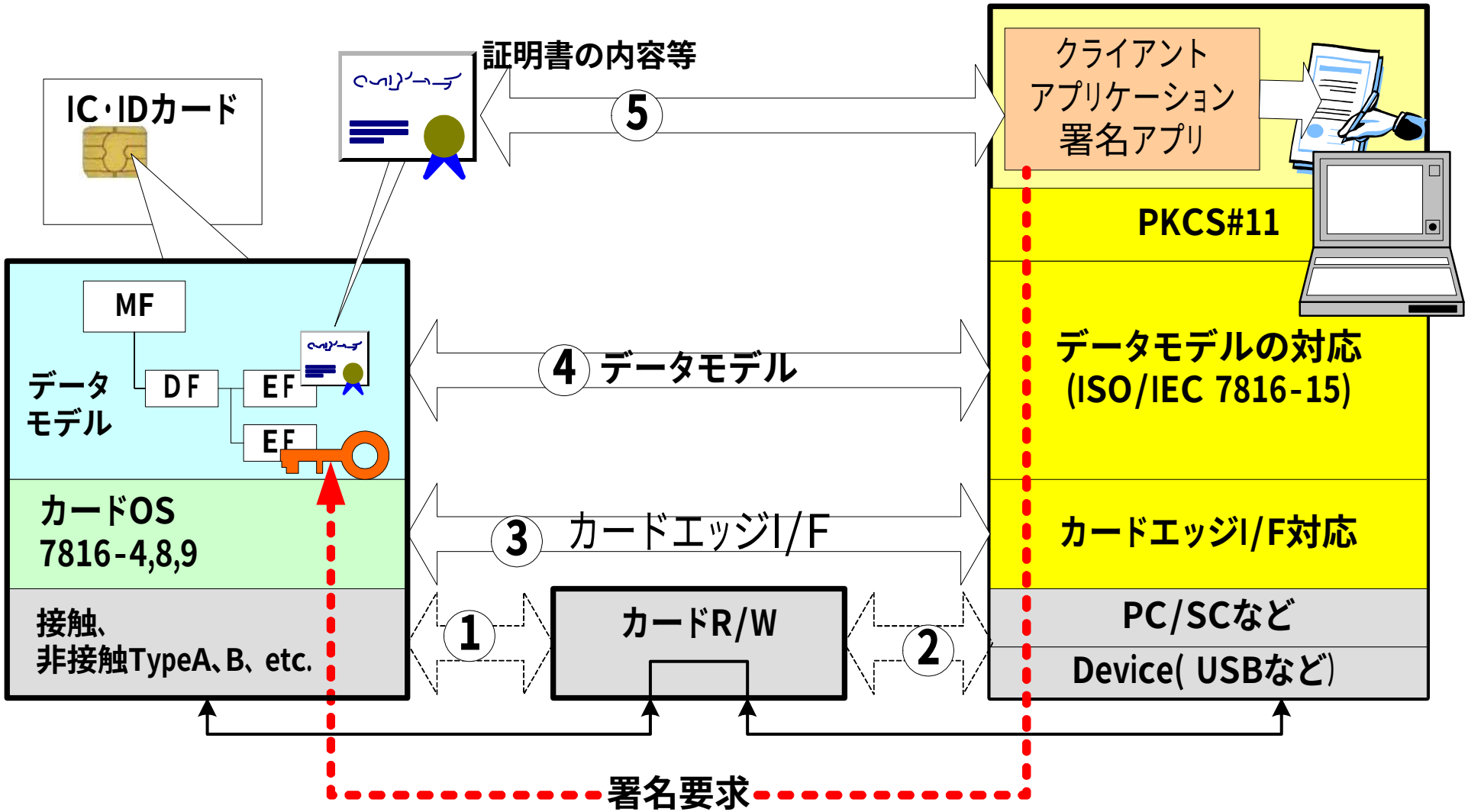
PKI対応IDカードの相互運用性

IPAの「IC・ID カードの相互運用可能性の向上に係る基礎調査」より

PKI対応IDカードの相互運用性
物理的に理解できるインターフェースと相互運用性



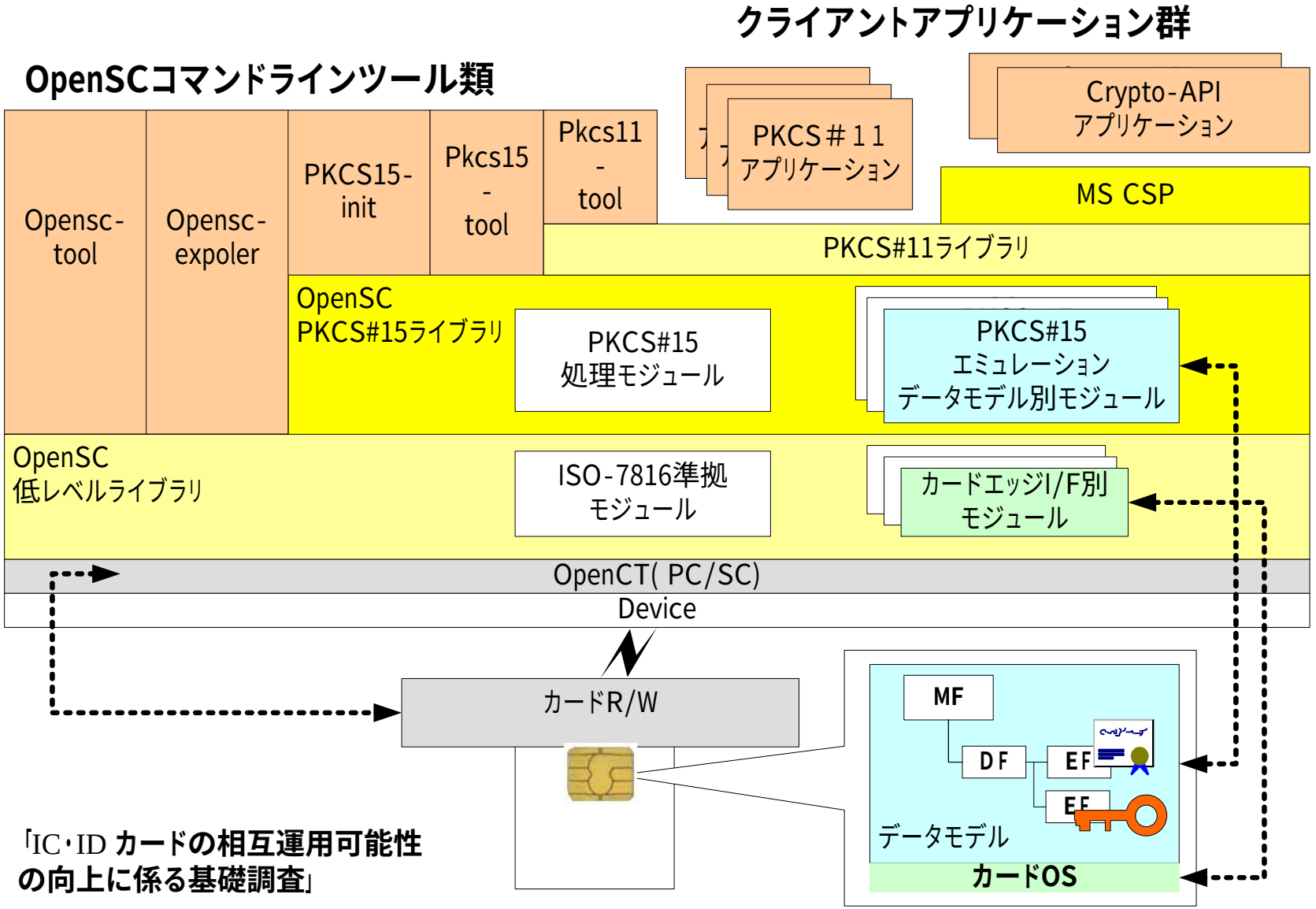
PKI対応IDカードの相互運用性
相互運用性の分類



「IC・ID カードの相互運用可能性の向上に係る基礎調査」

PKI対応IDカードの相互運用性
OpenSCの全体のアーキテクチャ

セコムIS研究所
Intelligent Systems Laboratory



「IC・ID カードの相互運用可能性の向上に係る基礎調査」

セコムIS研究所
Intelligent Systems Laboratory

HPKI対応ICカードガイドライン

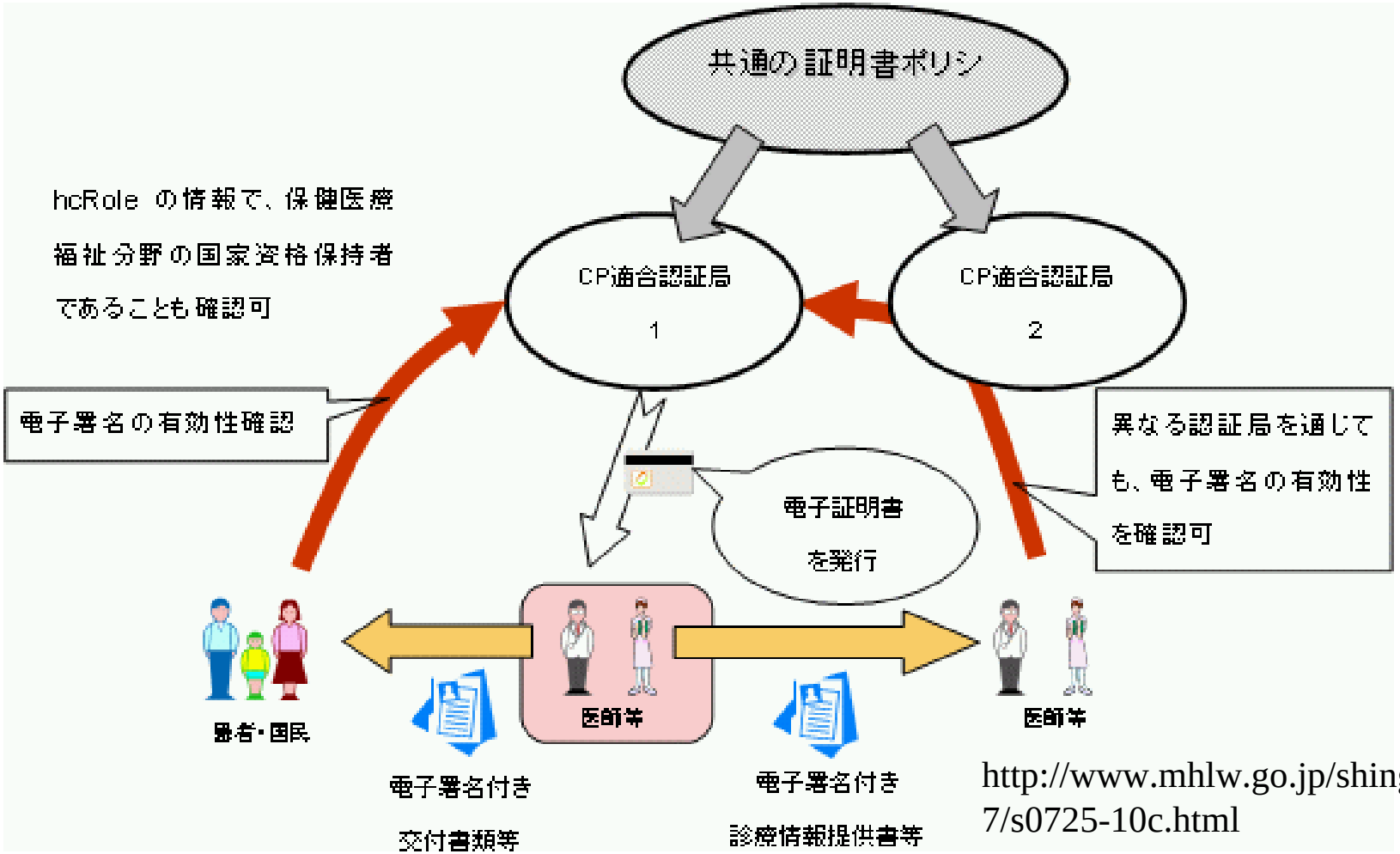
JAHIS(**保健医療福祉情報システム工業会**)で作成したHPKI**対応ICカードガイドラインの説明**

HPKI対応ICカードガイドライン
HPKI　- 日本の医療分野共通のPKI

セコム IS 研究所
Intelligent Systems Laboratory

- 厚生労働省、医療情報ネットワーク基盤検討会
  - 医療における公開鍵基盤（HPKI）のあり方などの提言
  - 最終報告：2004.9
    - http://www.mhlw.go.jp/shingi/2004/09/s0930-10.html
  - 「医療情報システムの安全管理に関するガイドライン策定」へ
    - 医療情報システムの安全管理に関するガイドライン（2005年3月）
    - http://www.mhlw.go.jp/shingi/2005/03/s0331-8.html
  - 「医療界共通の証明書ポリシーの策定」へ
- 保健医療福祉分野PKI認証局　証明書ポリシ（2005年４月）
  - http://www.mhlw.go.jp/shingi/2005/04/s0401-1.html
  - 全国で共通の信頼性と検証可能性を確保して認証局を運営を行なうためのポリシー
  - 各認証局はHPKI CP(Certificate Policy)に従いCPS(Certification Practice Statement）を作る
    - CP/CPSフレームワークRFC3647に従う
  - ISO TS 17090に準拠　　ｈｃRole　など

HPKI対応ICカードガイドライン
HPKI　- 証明書ポリシ（CP）



http://www.mhlw.go.jp/shingi/2005/07/s0725-10c.html

公開鍵証明書レベルにおいては、相互運用性の確保が可能な状況にある。
ところがICカードを利用すると。。。利用環境が制限される。。。

HPKI対応ICカードガイドライン
ガイドラインの目的

セコム IS 研究所
Intelligent Systems Laboratory

- （1）安全なPKIの鍵の保存媒体として、ICカードが注目を浴びているため、厚生労働省保健医療福祉分野PKI認証局証明書ポリシに準拠したHPKIの要求仕様を満たすICカードのガイドラインを策定する。
- （2）「HPKIを利用した医療文書に対する電子署名規格」と共に利用することを前提に、電子署名を目的としたHPKI で使用されるIC カード、及びIC カードの利用環境に対する要求事項を定める。
  - IC カード機能・仕様
  - IC カードのセキュリティ要件
  - 相互運用性を確保するためのIC カード内のPKI アプリケーションの仕様
  - 相互運用性を確保するためのIC カードを利用する際のインタフェースの仕様

HPKI対応ICカードガイドライン
内容：目次

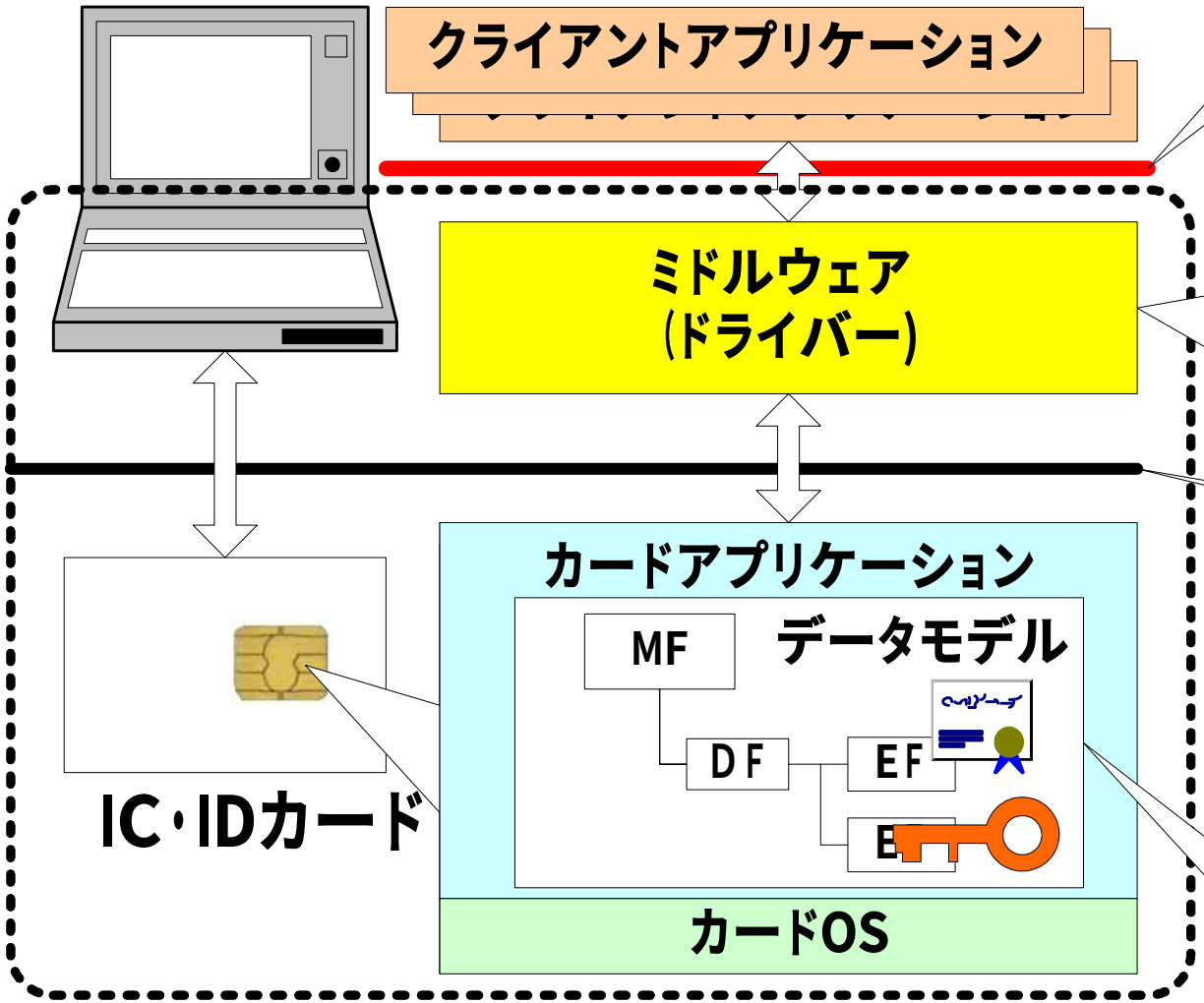
- 第1章　適応範囲
- 第2章　引用規格・引用文献
- 第3章　用語の定期
- 第4章　HPKI用ICカードの機能
- **第5章　相互運用性のための仕様**
- 付属書A　PKIアプリケーション利用のシーケンス
- 付属書B　PKIアプリケーションの構造例
- 付属書C　PKIアプリケーション利用のコマンド
- 付属書D　ICカードリーダライタとのインタフェース

HPKI対応ICカードガイドライン
内容：概要

セコム IS 研究所
Intelligent Systems Laboratory

- 第4章　HPKI用ICカードの機能
  - ICカードの機能について説明
    - 一般的なICカードの機能
    - PKIを用いるために必要となる機能
  - 私有鍵・公開鍵証明書保存機能、私有鍵生成機能、私有鍵インポート機能、私有鍵活性化機能、署名機能
- 第5章　相互運用性確保のための仕様
  - HPKI実証実験での問題点の1つであった認証事業が発行するカード及びPKIアプリケーションの違いに起因するトラブルの解消を目的に、相互運用性を確保することを課題とした複数の認証事業を行うことが想定されているので、実際のシステムでは、カードが混在することを前提とするソフトウェア側の対応を検討し、デファクトであるCrypto API及びPKCS#11の最小限の仕様、利用シーケンスを示すICカード

HPKI対応ICカードガイドライン
現状のICカードの提供形態



PKCS#11などのデファクトスタンダードなAPI

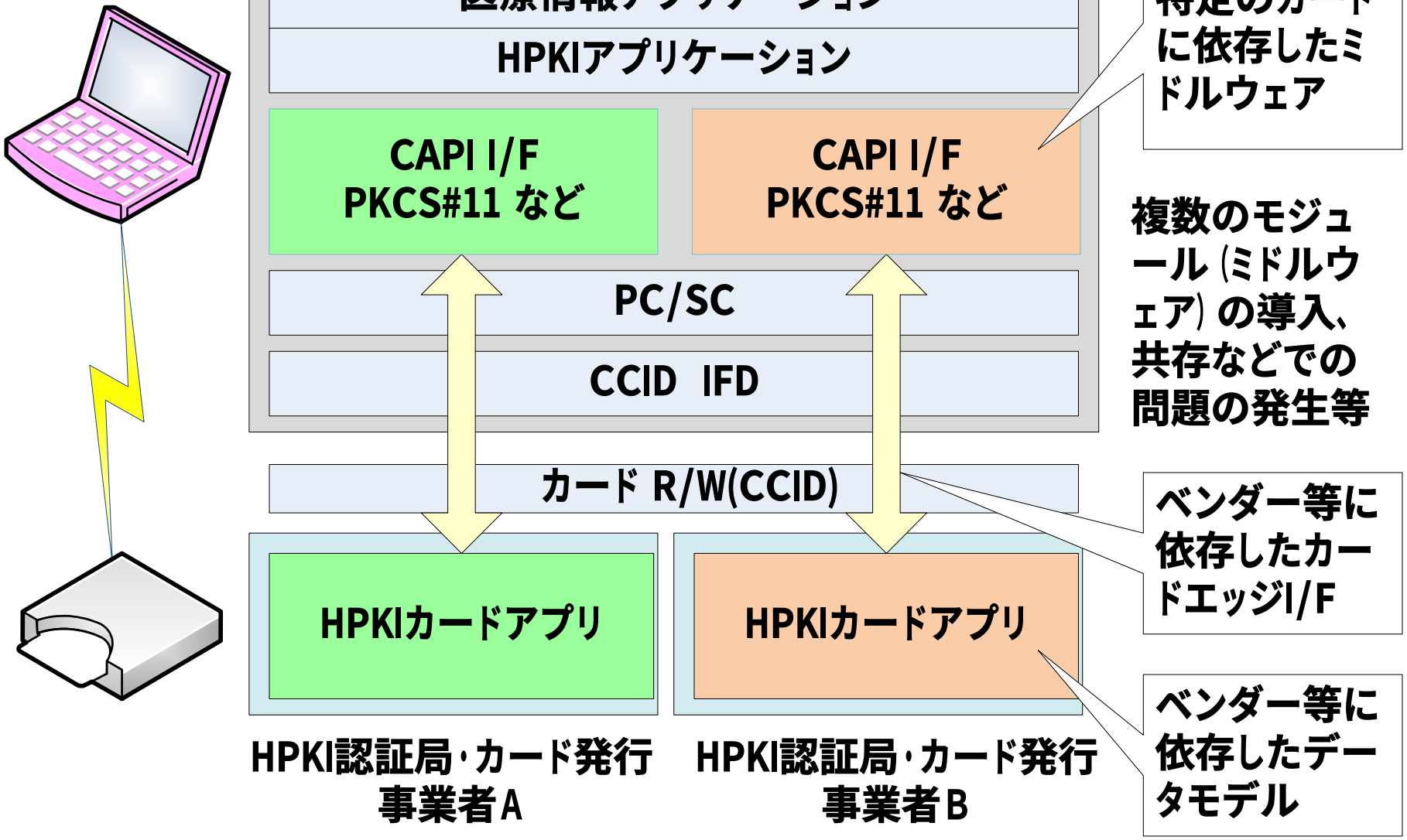
ベンダー独自のデータモデルのカードエッジI/Fをサポートするためのミドルウェア (IC・IDカードに依存したドライバー)

ベンダー等に依存したカードエッジI/F。非公開の場合もある。

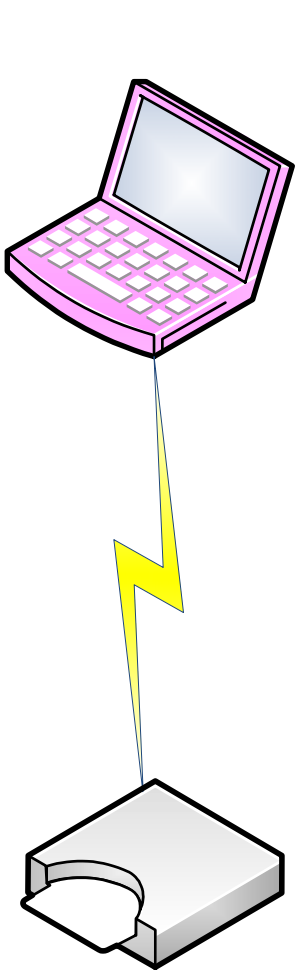
ベンダー等に依存したデータモデル。多くの場合、非公開。

HPKI対応ICカードガイドライン
従来のPKIソフトウェアの構成

セコムIS研究所
Intelligent Systems Laboratory



HPKI対応ICカードガイドライン
相互運用性を考慮したソフトウエア構成



医療情報アプリケーション

HPKIアプリケーション

CAPI I/F, PKCS#11

ISO/IEC 7816-15,4,8 等に準拠した実装

PC/SC

CCID　IFD

カード R/W(CCID)

HPKIカードアプリ

HPKIカードアプリ

HPKI認証局･カード発行事業者A

HPKI認証局･カード発行事業者B

インタフェースの最小限の機能と利用シーケンスを例示

国際標準に準拠したアプリケーション構造例とコマンド･シーケンスを例示

異なる事業者が発行したHPKIカード

HPKI対応ICカードガイドライン 仕様のポイント（第5章　相互運用性のための仕様）

セコム IS 研究所 Intelligent Systems Laboratory

- ISO/IEC 7816-15（JIS X 6320-15:2006 IC カード－ 第15 部 暗号情報アプリケーション)のプロファイルを定義
  - カード内のデータモデルを定義、また、ISO/IEC 7816-15を利用し、そのプロファイル定義
  - このことにより、「ベンダー等に依存したデータモデル」の問題を解消
- ISO/IEC 7816-8
  - 署名機能などで使用するISO/IEC 7816-8 のプロファイルを定義
    - PERFORM SECURITY OPERATION(PSO)の利用範囲を明確にした。
  - このことにより「ベンダー等に依存したカードエッジI/F」の問題を解消
- HPKI対応ICカードの識別とカードアプリケーションの選択
  - ”ISO/IEC 7816-15”を示すAIDを使用
    - “E8 28 BD 08 0F XX XX XX XX“

HPKI対応ICカードガイドライン
相互運用性を確保するための条件（制約）

セコム IS 研究所
Intelligent Systems Laboratory

- 相互運用性の範囲：電子署名の部分（カード管理は含まない）
- 証明書の適用範囲：HPKI認証局発行の証明書（否認防止）のみ
- 複数の証明書保持（厚労省HPKIルート認証局、事業者のルート認証局）
- 複数の資格への対応：１証明書には１つのｈｃRole（資格）、将来は、1枚のカードに複数の証明書の可能性
- hcRole(資格）の確認は、ミドルウェアでは行わず、上位の医療アプリケーションで行う。
- 管理された医療施設内の情報システム・端末での利用が前提
- 既存の国内外の標準に準拠した仕様
- 証明書の読み出しにはアクセス権をかけない。私有鍵の利用には、毎回利用者認証（PINの確認）を行う。

HPKI対応ICカードガイドライン 活用のメリットと今後の課題

セコムIS研究所 Intelligent Systems Laboratory

- 活用のメリット
  - (1) 認証事業者
    - 標準に従った仕様になっているので、継続的に同じ仕様の調達・利用が可能
  - (2) ICカード、モジュール提供者
    - 固有の仕様の開発負担・維持の軽減
  - (3) システム開発者
    - 認証事業者毎の違いやカードが混在することを意識することなく開発・導入が可能
  - (4) 利用者 (医療施設・医療従事者)
    - 導入コストが下げられる可能性
- 今後の課題
  - 認証用証明書を含めた仕様 (今年度策定??)
  - 実際の実装
  - コンフォーマンステスト

セコムIS研究所
Intelligent Systems Laboratory

まとめ

- プラットフォーム環境に依存しないポータビリティのあるPKI対応IDカードは、「特定のベンダー等に依存しないデータモデル」「特定のベンダー等に依存しないカードエッジI/F」の仕様が必要になる。
- 「HPKI対応ICカードガイドライン」は、こうした仕様を策定している。
- #ただし、実際の実装は、今後の課題。
- ＨＰＫＩと同様の問題と要求は、様々な分野で潜在的に存在する。「 PKI対応IDカードの相互運用」の課題が正しく理解され、標準化、仕様策定、テストフレームワーク、実装が促進されるべきである。

セコムIS研究所
Intelligent Systems Laboratory

参考

参考

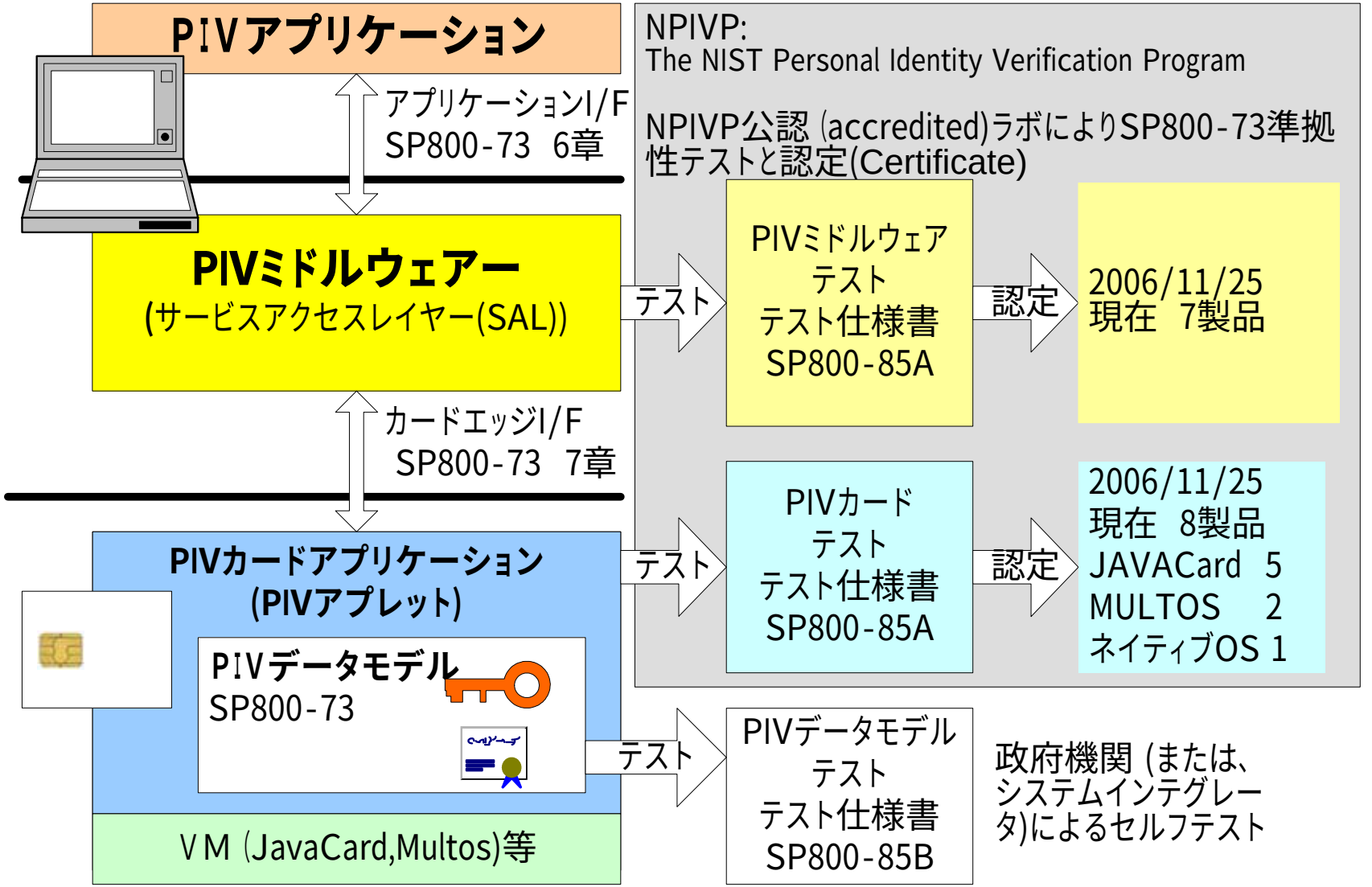
セコムIS研究所
Intelligent Systems Laboratory

- IC・ID カードの相互運用可能性の向上に係る基礎調査
  - http://www.ipa.go.jp/security/fy18/reports/ICID/index.html
  - シーズ編
    - http://www.ipa.go.jp/security/fy18/reports/ICID/seeds_rep.pdf
- セキュリティAPIに関する技術調査
  - http://www.ipa.go.jp/security/fy15/reports/sec_api/
  - 2003年度にJNSAが受託した調査報告書
  - http://www.jnsa.org/seminar/2004/seminar_20040826.html
- 「IC・ID カードの相互運用可能性」技術セミナー
  - http://www.jnsa.org/seminar/2006/20070328/index.html
- 情報セキュリティと仕様のオープン性に関する課題
  - http://www.jnsa.org/jnsapress/vol19/19-3_tokusyu1.pdf
- JAHIS標準　HPKI 対応IC カードガイドライン
  - http://www.jahis.jp/standard/seitei/st08-002/st08-002.htm
- HPKI対応ICカードガイドライン　　2008年6月公開
  - http://www.jahis.jp/sisuiryo/houkoku/h19gyoumuhoukokukai/gyoudata/04iccard.pdf

参考
仕様が広く公開されたPKI対応IDカードの例

- 米国のPIV
  - http://csrc.nist.gov/piv-program/
- ベルギーのBELPIC
  - http://www.snelbalie.be/content/content/record.php?ID=131
- ドイツの健康保険カード(The Specification of the German Electronic Health)
  - Part 1 Specification of the German Electronic Health Card eHC Part 1: Commands, Algorithms and Functions of the COS Platform
    - http://www.gematik.de/(S(sm2ihl55dyakedvnoaymsg45))/upload/gematik_eGK_Specification_Part1_e_V1_1_0_518.pdf
  - Part 2: Applications and application-related structures
    - http://www.gematik.de/(S(xvnpoweqs03nttfeb2m5w3bu))/upload/gematik_eGK_Specification_Part2e_V1_2_1_1392.pdf
  - Part3 Specification of the German Electronic Health Card eHC Part 3: Layout and visual design of the eHC
    - http://www.gematik.de/(S(wplpvpnkk20opu45tbolaj45))/upload/gematik_eGK_Specification_Part3_e_V1_3_1_1794.pdf

PIV　－　PIVのテスト方法論と仕様



「IC・ID カードの相互運用可能性の向上に係る基礎調査」より

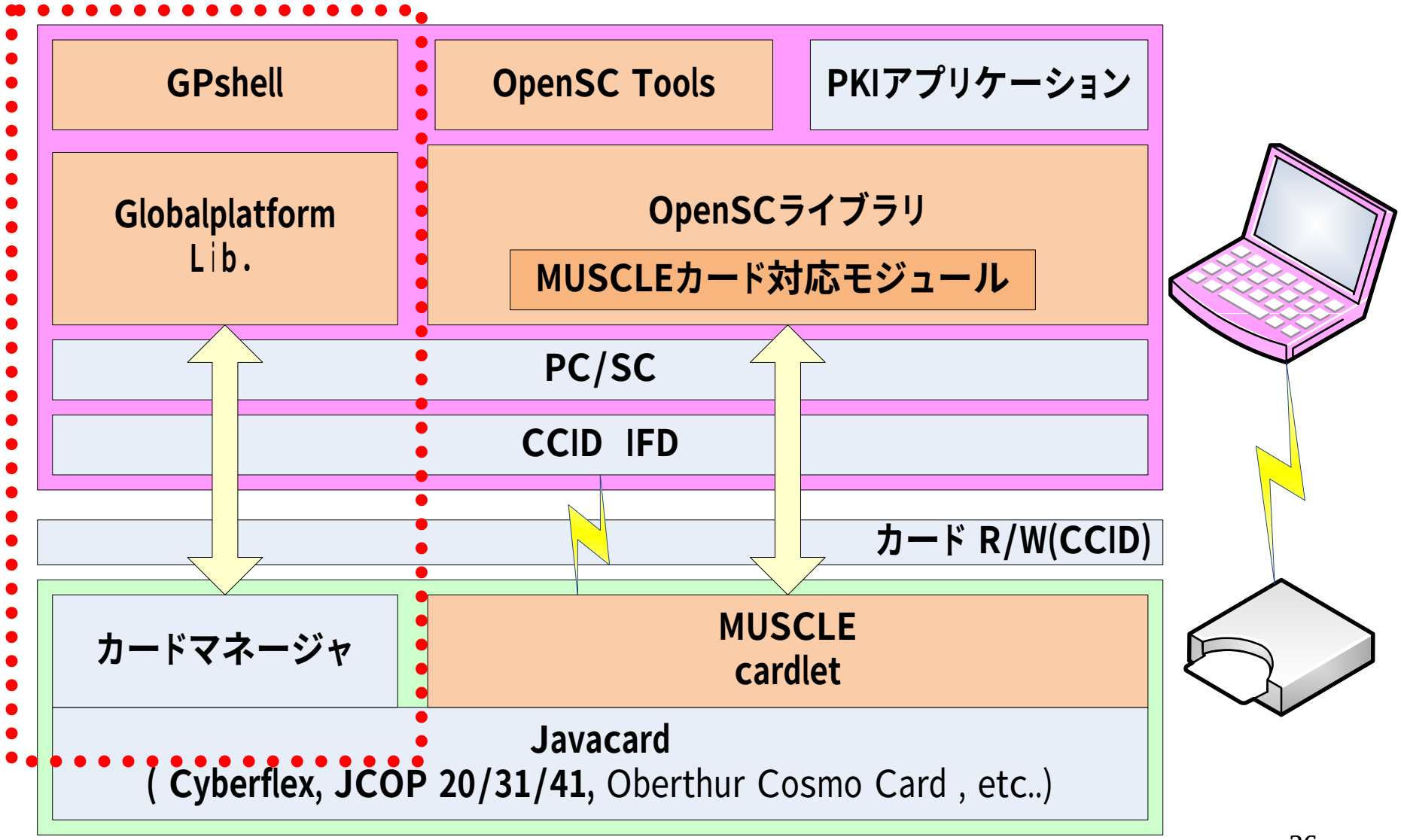
セコムIS研究所
Intelligent Systems Laboratory

Global Platform

おまけ

Global Platform
Javacard,OpenSC,Musclecard,GPShellの関係

セコムIS研究所
Intelligent Systems Laboratory



Global Platform
Global Platformのバージョン

バージョン	発行日	SCP	製品 (Workshopで使用)	その他備考
Ver.2.0.1	2000.7	共通鍵 SCP01	NXP JCOP 20 NXP JCOP 31 Cyberflex E-Gate	GPShellは、”mode_201”を使用
Ver.2.1.1 237Page	2003.5	共通鍵 SCP01 SCP02	NXP JCOP 41 Oberthur Cosmo Card	GPShellは、”mode_211”を使用
Ver.2.2 375Page	2006.5	共通鍵 SCP02 公開鍵 SCP10	未確認	GPShellは、現在(2008.6)未サポート

Global Platform
セキュアチャネルプロトコル (SCP)

セコム IS 研究所
Intelligent Systems Laboratory

- セキュアチャネルプロトコル (SCP)
  - Global Platformの仕様で定義された「カード」と「端末」間の「認証」「暗号化」等を行なうためのプロトコル
- Openplatfoem Ver.2.0.1
  - 共通鍵ベースの「SCP 01」
  - 現在の製品では、このSCP 01がよく使用されている
    - 多くの製品が、SCP01しかサポートしていないため
- Global Platform Ver.2.1.1
  - 共通鍵ベースの「SCP 02」
  - 2008年現在、新製品の多くがサポートしている
- Global Platform Ver2.2
  - 公開鍵ベースの「SCP 10」

Global Platform
セキュアチャネルプロトコルと外部認証、内部認証

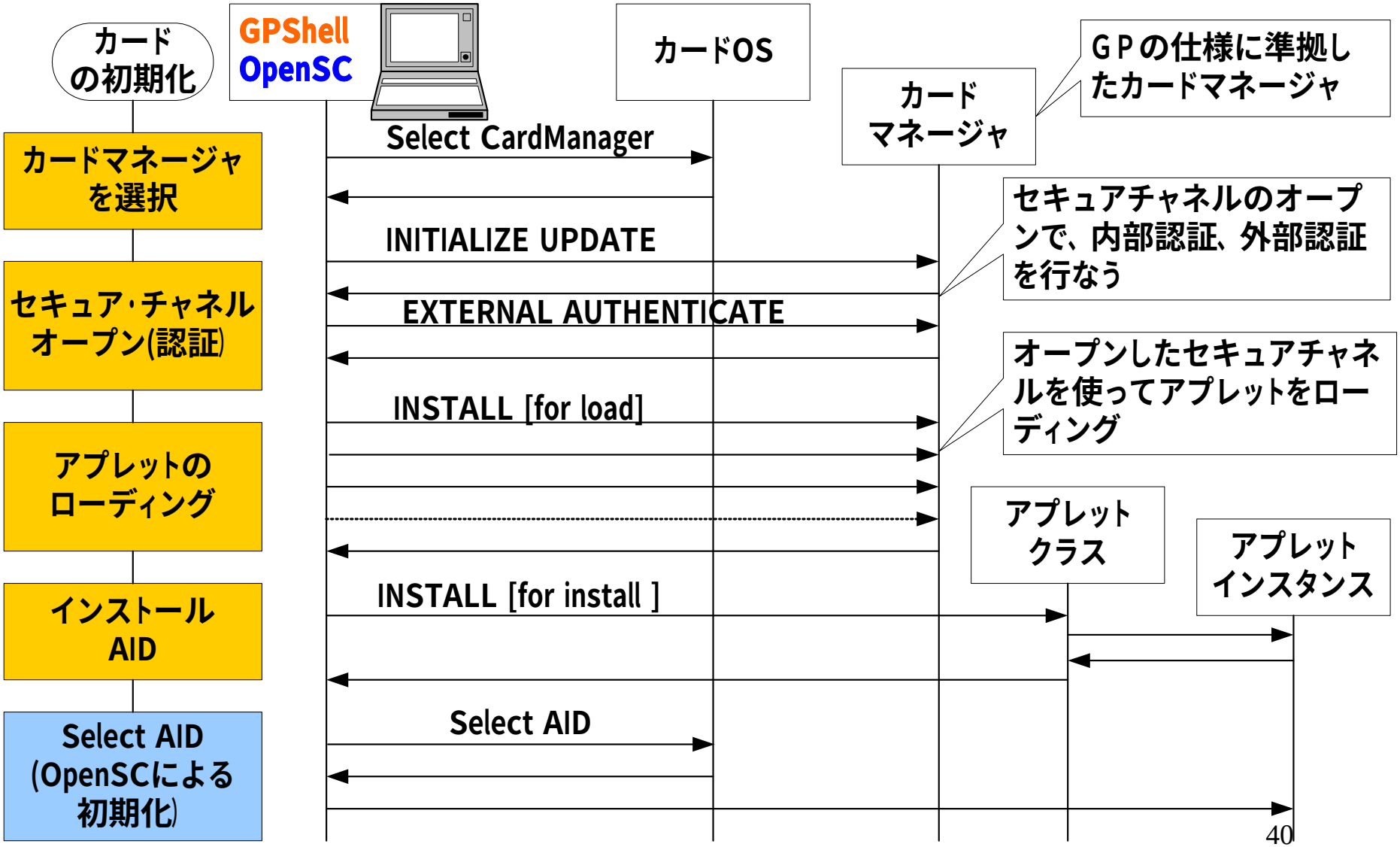
セコム IS 研究所
Intelligent Systems Laboratory

認証	認証を行うエンティティ	認証の対象となるエンティティ	認証の方法の例
外部認証 External Authentication	ICカード	外部端末	外部端末のプライベート鍵を使って、カード内の公開鍵で検証（または共通鍵（秘密鍵））
内部認証 Internal Authentication	外部端末	ICカード	ICカード内のプライベート鍵を使って、外部端末の公開鍵で検証（または共通鍵（秘密鍵））

- 「カード」と「端末」間の「認証」
  - 「カード」と「カード発行システム」
  - 「カード」と「利用者端末」　　これが問題。。。
- PKI ICカードWorkShopでは。。。
  - Workshopでは、GPShellを利用し「カード」とGPShellを動作させているPC間をSCPにより認証を行いカードアプレット(MUSCLE)をダウンロード

Global Platform
カードアプレットのローディング

セコム IS 研究所
Intelligent Systems Laboratory



セコムIS研究所
Intelligent Systems Laboratory

参考

- GlobalPlatform
  - http://www.globalplatform.org/
- A Comparison of Java Cards: State-of-Affairs 2006
  - http://alexandria.tue.nl/repository/books/627238.pdf