JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

「ＰＫＩに利用するICカードの課題」

「IC・ID カードの相互運用可能性の向上に係る基礎調査」から

セコム株式会社 IS研究所/
JNSA PKI相互運用技術WGリーダー
松本　泰

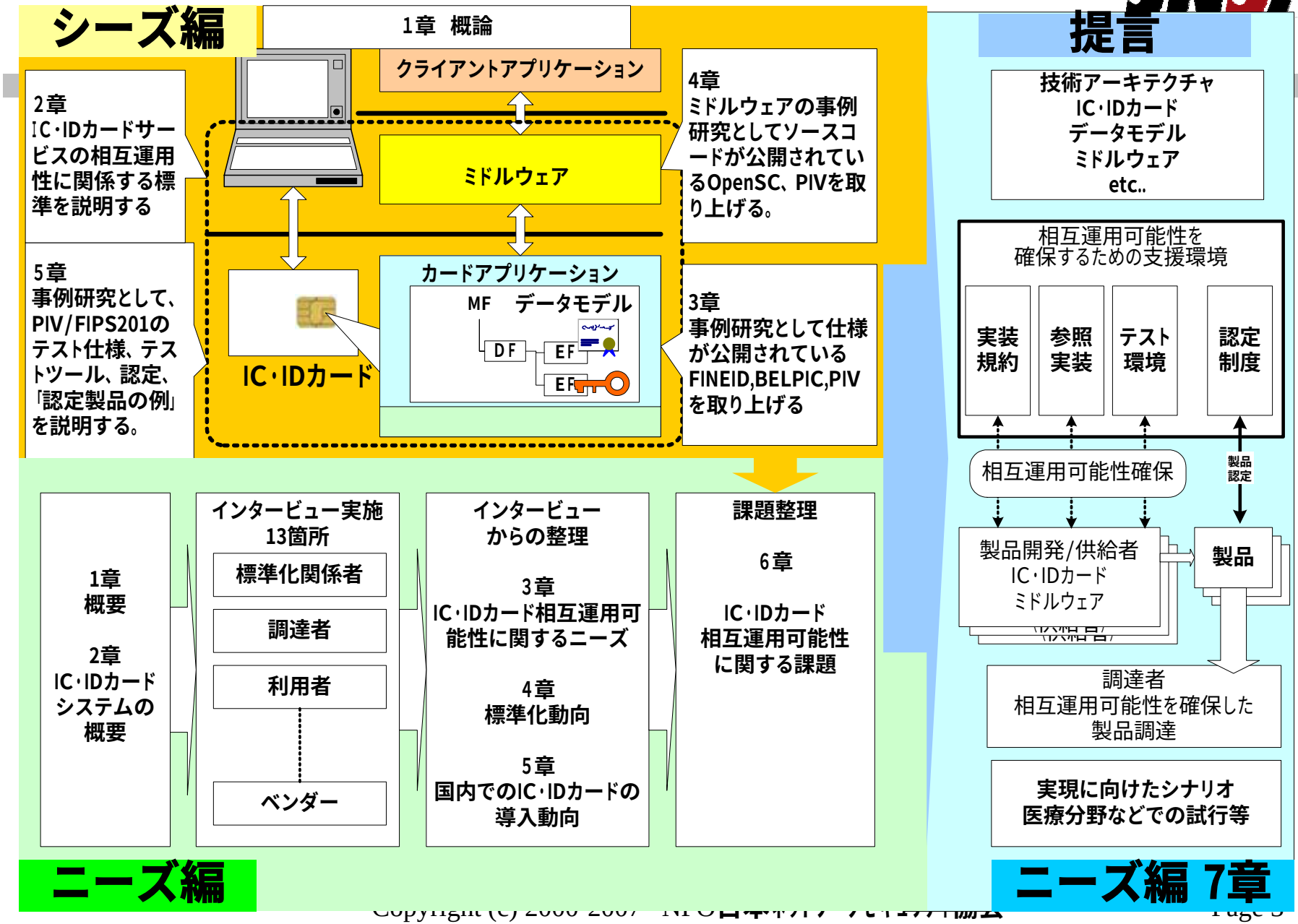
2007 年 6 月6日

「ＰＫＩに利用するICカードの課題」

「IC・ID カードの相互運用可能性の向上に係る基礎調査」から

- 独立行政法人 情報処理推進機構 セキュリティセンター(IPA/ISEC)の公募に、NPO JNSAの応募が採択された「IC・IDカードの相互運用可能性向上に係る基礎調査」の「調査報告書」が、2007年1月にIPAのサイトで公開されています。この調査で明らかになった「ＰＫＩに利用するICカードの課題」について説明します。

調査の全体概要

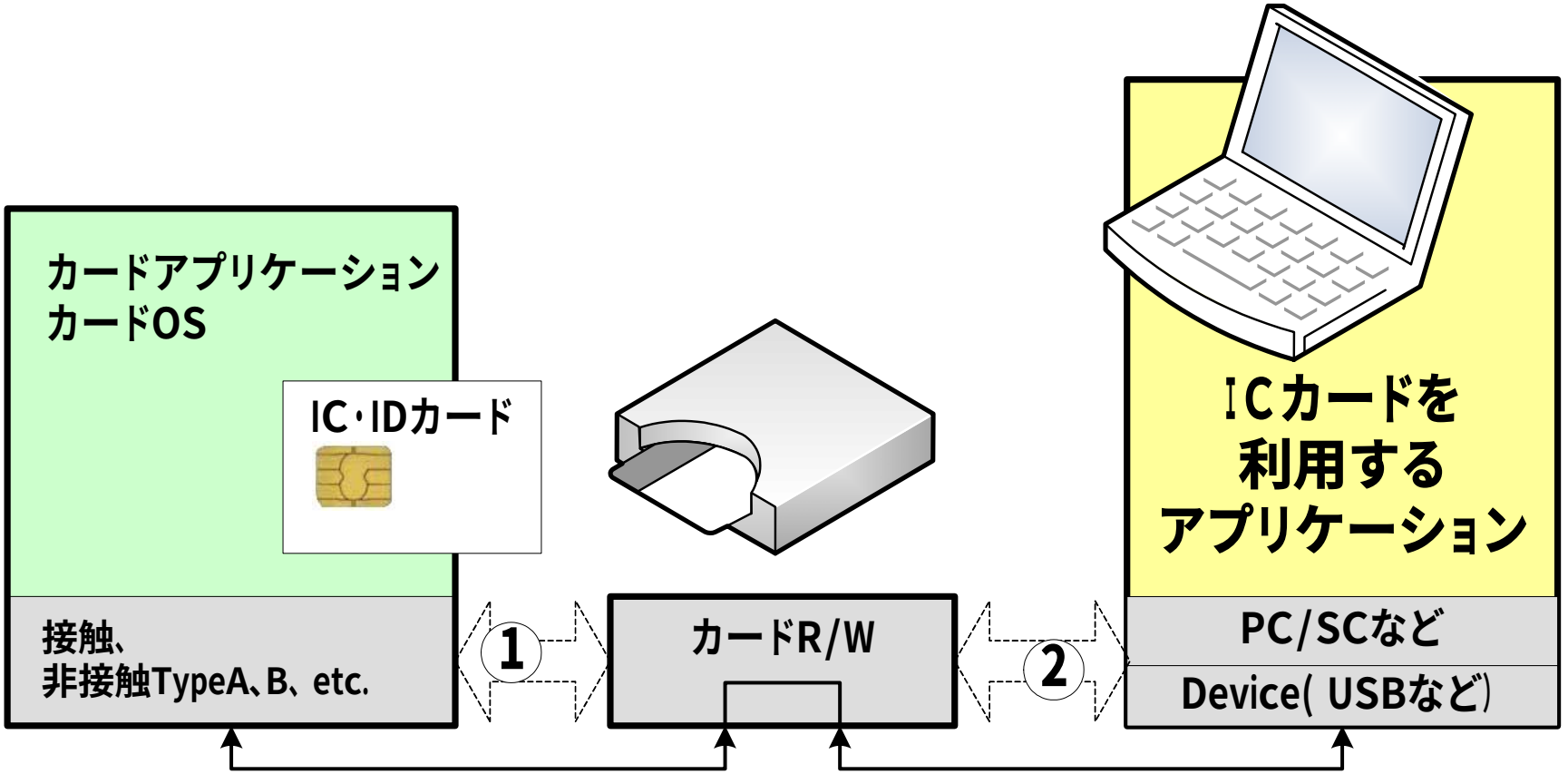


ニーズ調査からの結論

- IC・IDカードの相互運用ニーズは顕在化しつつある
  - 個別の「PKI用カード」からネットワーク上の「IDカード」へ
  - 「どこからでもつながる」「何にでも使える」
- 国内ではIC・IDカードの相互運用が進む環境にない
  - 個別に仕様を策定し、非公開で運営
  - ミドルウェア、リーダライタ、IC・IDカードをセットで提供
  - 国際標準だけでは相互運用できない
- このままでは「IC・ID」カードは普及しない
  - 個別サービスだけ見れば、標準化・公開されなくても短期的には困らない
  - 長期的には利用者ニーズを削ぎ普及を阻害する

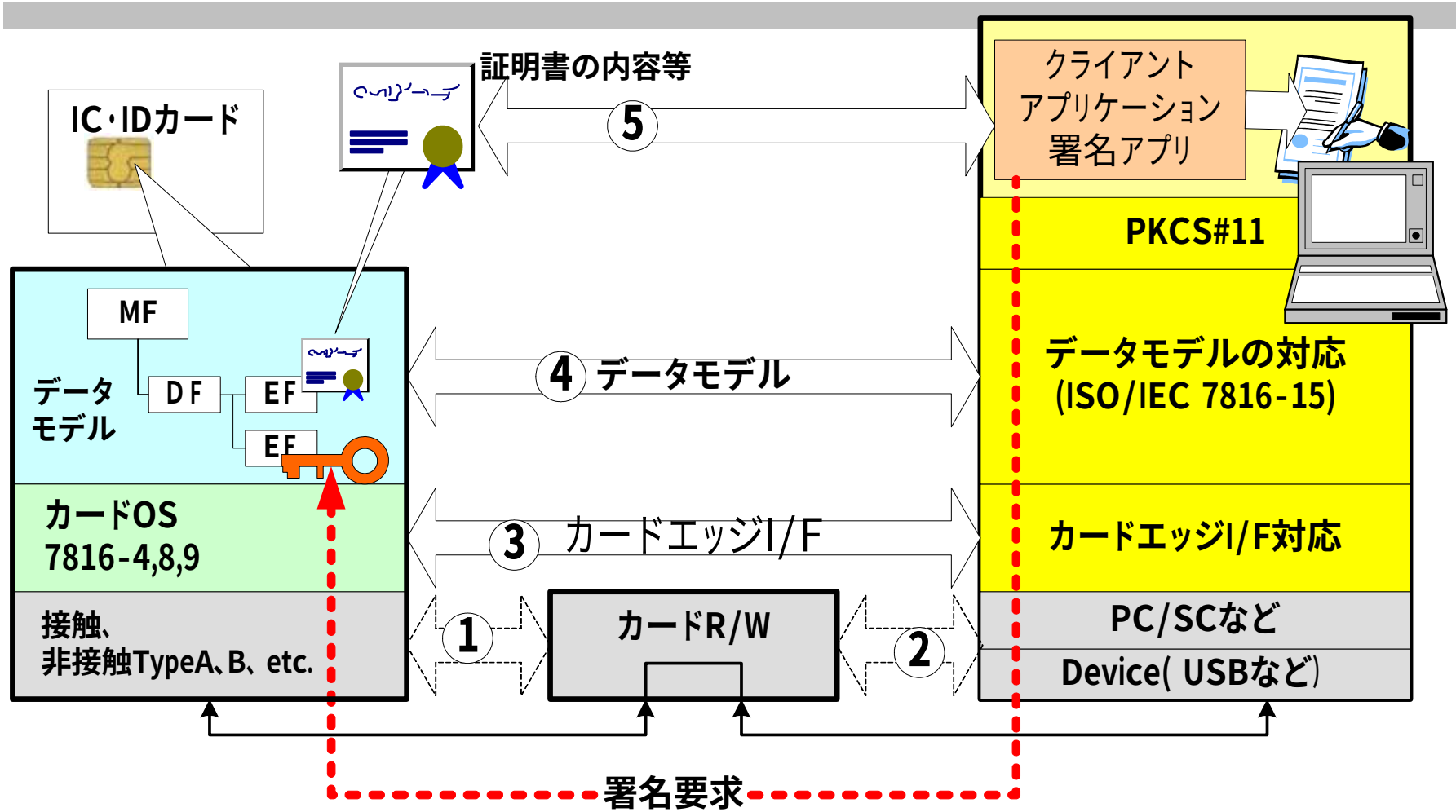
http://www.ipa.go.jp/security/fy18/reports/ICID/needs_rep.pdf

シーズ調査　相互運用可能性の分類



物理的に理解できるインターフェースと相互運用可能性。。。

シーズ調査　相互運用可能性の分類



相互運用可能性が問題になる部分は、5つに分類し、主に（3）、（4）をこの調査報告書で取り上げた。

相互運用可能性の課題

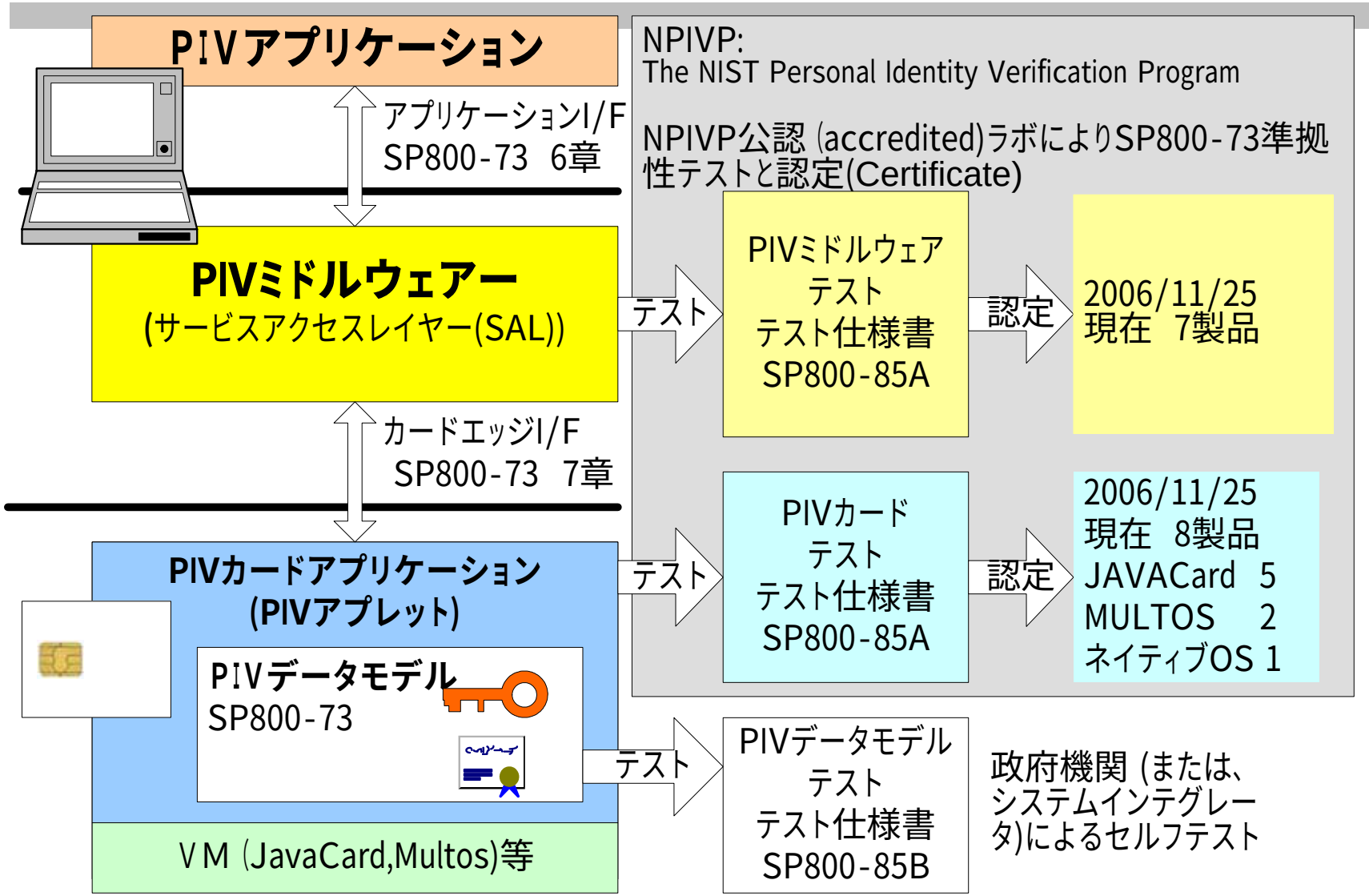
Q.　相互運用可能性の確保は？

A.　世界標準のISO/IEC 14443 TypeB、ISO/IEC7816準拠ですから大丈夫

Q.　データモデルは？？？

A.　（え？？）決まっていません。だけど、ポストイシューでどんなアプリケーションでも入れられるので大丈夫です。

シーズ調査
米国のPIVの例ーPIVのテスト方法論と仕様



事例研究
ベルギーのＢＥＬＰＩＣ

Q.

なぜ、身近に使えない海外の事例なの？

A.

それはね、国内で技術仕様が公開されたよい事例がないからなんだよ。。。。。

シーズ調査
米国PIVと国家公務員身分証明書ICカードの比較

比較項目	PIV	国家公務員身分証明書 ICカード
配布対象	連邦政府職員と契約業者	国家公務員
配布枚数	2000万枚が予定されている	不明
プラットフォーム対応	規定なし	規定なし
IC・IDカードをサポートするミドルウェア	仕様、テスト仕様が公開されており認定制度(NPIVP)がある。 ミドルウェアのレファレンス実装のソースコードなども公開されている	不明
カードエッジI/F	NIST SP800-73	非公開
カード内のデータモデル	NIST SP800-73	非公開
格納されるEE(End Entity)証明書	認証用の証明書 署名用の証明書(Option) 暗号用の証明書(Option)	規定なし

シーズ調査
相互運用可能性の課題

- なぜ仕様が十分に開示されないか？
  - 実力以上にICカードのセキュリティの高さが喧伝されている？
  - 実際には、様々なリスクがある。仕様が開示される（理解される）と、その「様々なリスク」が浮上する？
  - セキュリティに完全は無いにも係わらず、完全で無いことを脆弱性があるとか、プライバシー上の問題があるとか呼ばれることのリスク??
- 「情報セキュリティ vs. 相互運用可能性の確保」なのか??
  - BELPIC、米国のPIV
    - 「仕様をオープンにすることで、安全・安心なIC・IDカードの普及を図る」
  - 公的個人認証サービス、国家公務員身分証ICカード
    - 「仕様をオープンにしないことで、安全・安心なIC・IDカードを実現する」（と考えている??)
- IC・IDカードの仕様の閉鎖性は、相互運用可能性の問題解決を阻害し、それが、安全、安心を提供するとされているIC・IDカードの普及の阻害要因となっている??
- また、技術の不透明さは、セキュリティ上の不毛な議論を助長する。

IC・IDカードに限らず課題と思うこと。。。。

- 情報セキュリティ技術、特に情報セキュリティに関連した（相互運用）技術は、進歩しておらず停滞している。
- 情報セキュリティへの関心が高まるほどに、逆に情報セキュリティに関連する相互運用の問題の解決へのインセンティブは下がっている。
  - 情報の非公開、囲い込みなど、相互運用性を確保とは反対の方向へ向かっている。
- また、複雑さ（技術だけでなく、運用、マネージメント、さらに制度との関係）を克服できていない。
- #放って置くと、技術の形骸化を生む。既に、優秀な技術者が情報セキュリティ分野から逃げ出しているように感じられる。
- 結果。。 PKI相互運用技術WG。。終われない。。

参考

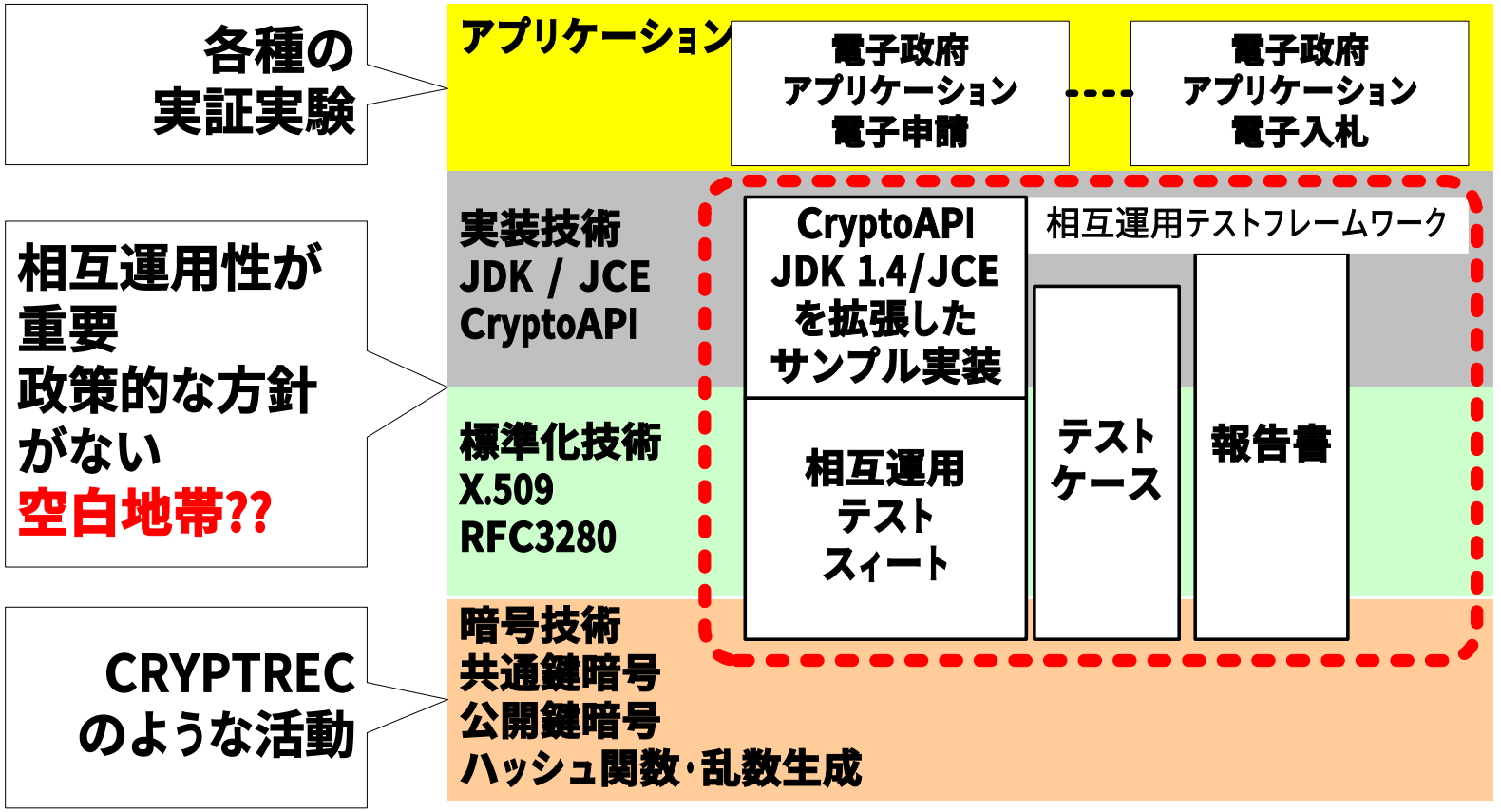
- IC・ID カードの相互運用可能性の向上に係る基礎調査
  - http://www.ipa.go.jp/security/fy18/reports/ICID/index.html
- 「IC・ID カードの相互運用可能性」技術セミナー
  - http://www.jnsa.org/seminar/2006/20070328/index.html
- 情報セキュリティと仕様のオープン性に関する課題
  - http://www.jnsa.org/jnsapress/vol19/19-3_tokusyu1.pdf

JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

NPO JNSAのChallenge PKIプロジェクト

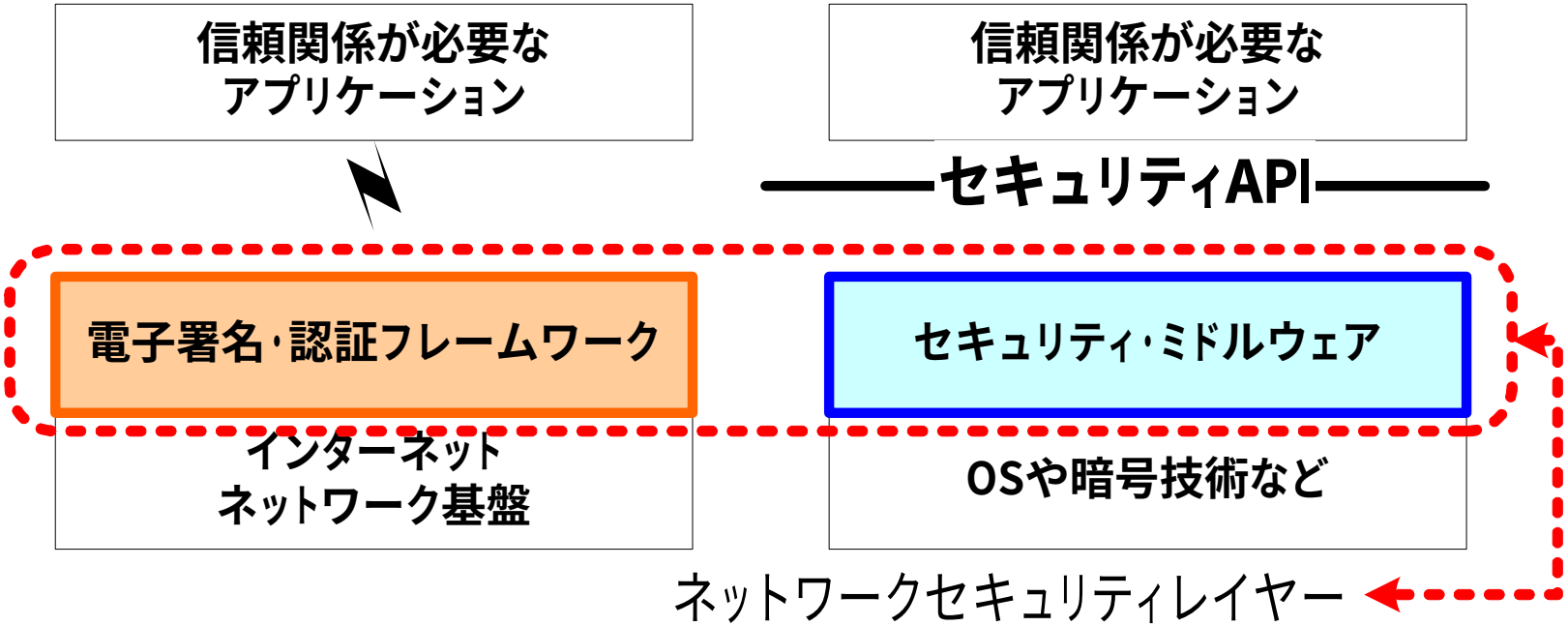
Challenge PKIプロジェクトの活動
プロジェクトの目標と課題 – *Challenge PKI 2002*



複雑さを隠蔽するためどんどん階層化されていく。。
このことが、問題の本質を分かり辛くしている！！

Challenge PKIプロジェクトの活動

セキュリティフレームワークやミドルウェア重要性 *Challenge PKI 2003*



- 何処でも、何時でも、誰にでもつながるユビキタスネットワークにおいて信頼の拠りどころが求められる。。。。
- ネットワーク上の信頼を実現するセキュリティ・レイヤーの必然性
  - これらは、古典的なOSI参照モデルなどでは説明がつかない。。。

Challenge PKIプロジェクトの活動

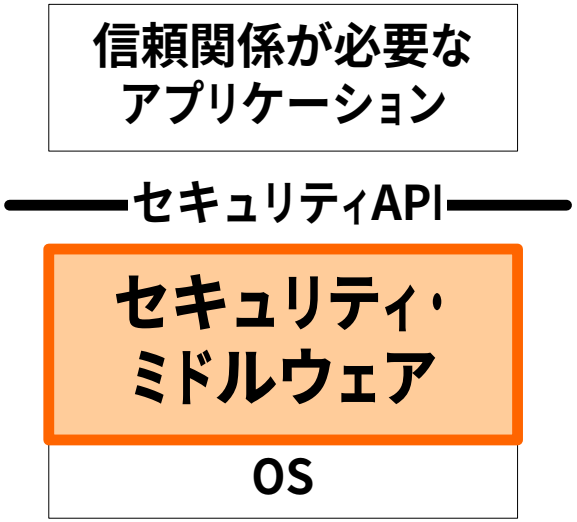
セキュリティフレームワークやミドルウェア重要性 *Challenge PKI 2003*

標準化、相互運用の課題

非常に複雑なセキュリティプロトコルの要求

セキュリティに対応し切れていない標準化＆標準化組織

テスト環境、テストケース、相互運用テストが非常に重要だが、整備ができていない



実装上の課題

暗号技術等、基礎技術が、セキュリティ・フレームワーク＆ミドルウェアに組み込まれていかない
（日本の話し。。。。）

多くのバグが内在する可能性
(OpenSSLなどは典型的)

標準と実装のギャップ。何がどこまで正しく実装されているのか分からない。

複雑さを隠蔽するために、どんどん階層化されていく。そのことにより本質的な問題点も隠蔽されていく??

複雑さと問題点が集約されていく