セコムIS研究所
Intelligent Systems Laboratory

PKIの展開状況の概観

松本　泰
セコム（株）IS研究所
2009年6月24日

セコムIS研究所
Intelligent Systems Laboratory

PKIの展開状況の概観

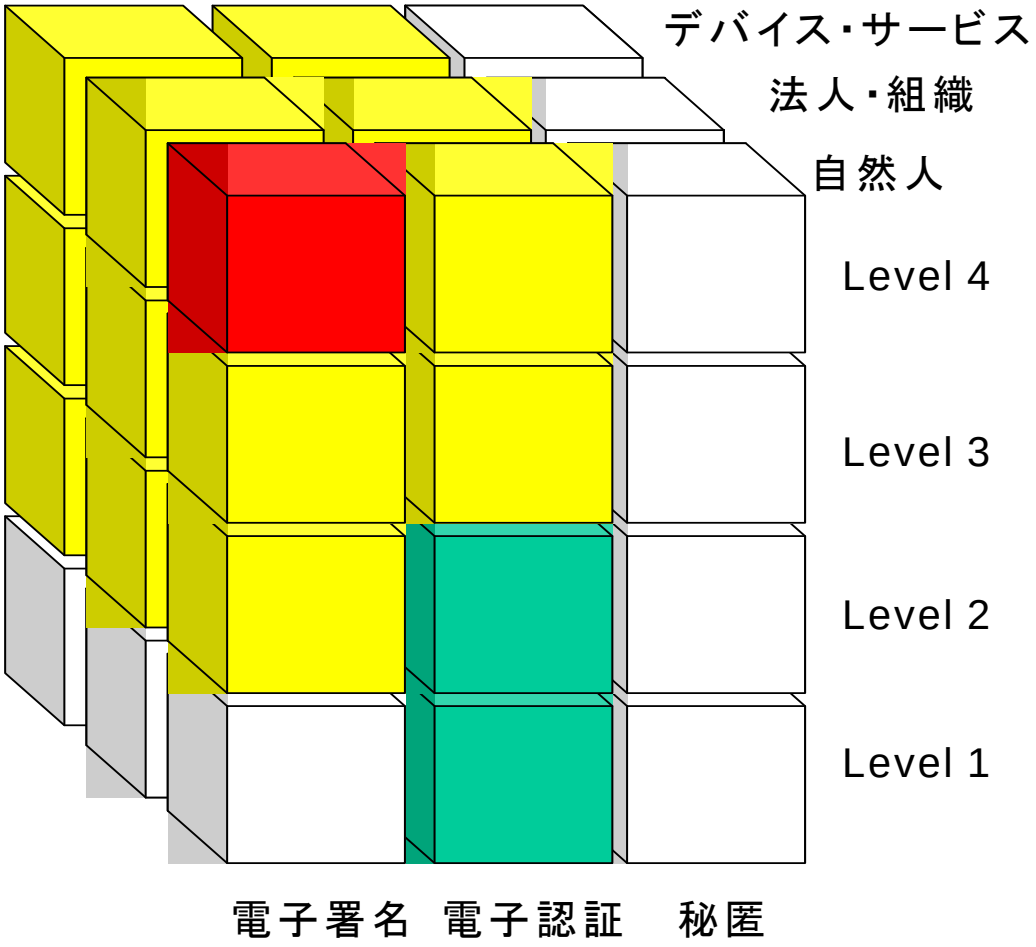
- 欧米におけるPKIの重要な動向を説明するとともに、インターネット、学術分野、医療分野、政府関係、企業内などで展開されるPKIの概況を説明します。

PKI day 2009のプログラム

1. 「PKIの標準化動向とリソースPKI」
2. 「長期署名フォーマットの欧州実証実験ETSI Remote XAdES/CAdES Plugtests について」
3. 「大学のサーバ証明書自動発行を目指して」
4. 「日本におけるヘルスケアPKI（HPKI）の最新動向」
5. 「欧州の政府系PKIとID管理」
6. 「政府機関及び金融機関のSSLサーバ暗号設定に関する調査結果について」
7. 「Windows 7とWindows 2008 R2で実現するPKI」

松本キューブ??

セコムIS研究所
Intelligent Systems Laboratory



・電子署名とユーザID・パスワードの関係（の誤解）

・何が世の中の基盤として整備されるべきなのか？

電子署名法（認定）の領域

現実に利用されているユーザID・パスワードの領域

（松本が考える）世の中の基盤として整備されるべき領域

PKIの展開状況の概観

セコムIS研究所
Intelligent Systems Laboratory

- 分野別のPKIの世界的動向
  - 電子政府のPKI
  - 医療分野のPKI
  - 米国の4BF
- 技術的観点のトピック？
  - 携帯PKI　モバイルID、モバイル署名
  - サーバサイド署名
  - 暗号アルゴリズムの移行

セコムIS研究所
Intelligent Systems Laboratory

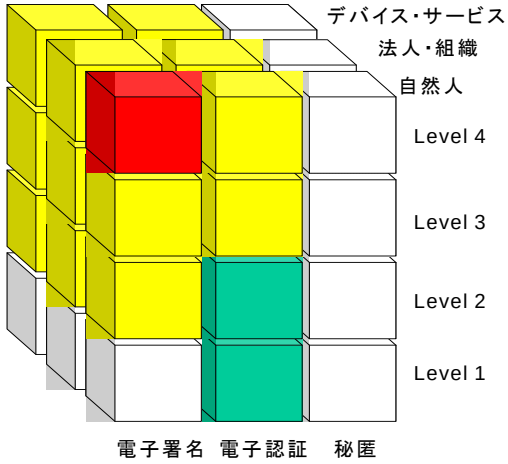
分野別のPKIの世界的動向

(1) 電子政府に関連するPKIの動向
(2) 医療分野に関連するPKIの動向
(3) 米国の4BF

電子政府に関連するPKIの動向
技術と制度を包括した相互運用性確保への取組

セコム IS研究所 Intelligent Systems Laboratory

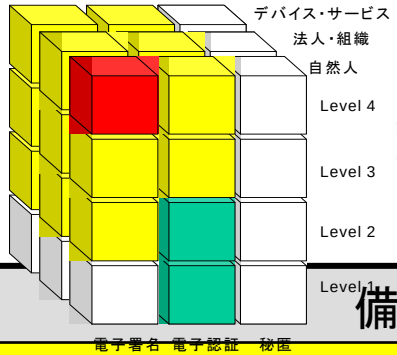
- LoA(Level-of-Assurance)という考え方の導入
  - 日本の「電子政府ガイドライン検討会・セキュリティ分科会」でも議論されている。
    - http://www.kantei.go.jp/jp/singi/it2/guide/index.html
- ID管理(社会基盤としてのID管理) → 「欧州の政府系PKIとID管理」



欧州では、国を越えたID管理、LoAの整合といった制度面も含めた相互運用性の課題を確保し、大規模なパイロット実験を行うSTORKプロジェクトがある。

http://www.eid-stork.eu/

電子政府に関連するPKIの動向
署名だけでなく認証にも対応



セコムIS研究所
Intelligent Systems Laboratory

事例	媒体	署名区分	認証LoA	備考
ベルギー eID	身分証明書 カード	Qualified signature	レベル4 *1	·ふたつの証明書が格納されたIDカード ·レベル4は、「認証用」証明書で実現 ·社会保障カード(SIS)もeIDに統合
オーストリア 市民カード	複数の媒体 が利用可能	Qualified signature	レベル4 *1	携帯電話、ATMカード、健康保険カード (e-card)で利用可能
スロベニアの Soft証明書	PCに 格納	Qualified Certificate	レベル3 *1	証明書により、個人と企業の双方で個別化(個人の)したサービスを提供している。
デンマーク OCES	PCに 格納	Advanced signature	レベル3 *1	·証明書は「署名」と「認証」の兼用。 ·「レベル3」は、この兼用証明書で実現 ・OCES Ⅱ は、サーバサイド署名
カナダ ePASS	利用時に ローミング	法的効力 は不明?	レベル 2or3 ??	ローミング鍵による「認証」と「署名」 (ライトウェイトなPKIの典型例)
米国 E-auth	LoAにより 異なる	署名は 範囲外	LoAにより 異なる	レベル3,4 は、現在のところ全てPKIベース

*1　「認証LoA」は、IDABCの調査報告書である「Proposal for a multi-level authentication mechanism and a mapping of existing　authentication mechanisms」での評価を記述している。

電子政府に関連するPKIの動向
国によって異なる普及の方針

セコムIS研究所
Intelligent Systems Laboratory

- 先行するエストニア、ベルギーのeID
  - 身分証明書として展開
  - 国民全てが持っていること前提の多目的な利用
  - 欧州の多くの国が追随？

- オーストリアの市民カード
  - 「市民カード」は、特定のデバイス（装置）に依存せずに実装
  - 「オーストリア電子政府法」において「市民カード」は、特定のデバイスではない「論理ユニット」であることが明記されている。
  - 携帯電話、ATMカード、健康保険カード(e-card)

- 簡易なPKIの普及をはかるデンマーク
  - ダウンロード可能なソフトウェアー証明書のOCES Ⅰ
  - ペーパトークンとサーバサイド署名を利用したOCES Ⅱ

- モバイル署名の普及をはかるトルコ
  - R/Wを必要としないモバイル署名

医療分野に関連するPKIの動向

- 高齢化を迎える先進各国は、その対応としてEHR(Electronic Health Record)/PHR(Personal Health Record)に積極的に取りくみつつある。このEHR/PHRを実現するためにHPKIを展開している。
- フランス、ドイツなどでの大規模なHPKIの展開
  - 医療従事者ためのPKI対応
  - 健康保険証カード等のPKI対応化

2007年から発行されている
ドイツの“健康カード”
(Gesundheitskarte)

「日本におけるヘルスケアPKI(HPKI)の最新動向」
講師:保健医療福祉情報システム工業会　セキュリティ委員会　委員長　茗原秀幸 氏

フランスのSESAM-Vitale2　健康保険証カード

セコムIS研究所
Intelligent Systems Laboratory

- 以前(2000年)からICカード化されていた健康保険証カード(SESAM-Vitale)
  - １６歳以上全国民
- SESAM-Vitale2
  - フランス版EHR(Electronic Health Record)に対応させるためのPKI対応
  - **フランス版EHR**　->2006年秋から開始
  - ３年で全てリプレース(年2000万枚??)
- NXP「SmartMX」、フランスの健康保険カード“Sesam-Vitale2”に採用
  - http://japan.internet.com/webtech/20061110/4.html
    - 保持者は請求書に**サイン**できるだけでなく、セキュアな電子環境で自分の**個人医療ファイルへアクセス**することが可能となる
    - 36K EEPROM PKI(公開鍵基盤)コンタクトマイクロコントローラ

http://www.sesam-vitale.fr/index.asp

http://www.sesam-vitale.fr/programme/programme_eng.asp

上がSESAM-Vitale2

下が医師のカード

「社会保障カード」等が、ちゃんと利用できるためには、医師カードとの連携が重要なのだが、医師カードが標準化できるかが鍵になる。

米国の4BF

- Four Bridges Forum (4BF)
  - ブリッジ認証局を持つ4つの分野
- Four Bridges
  - (1) FPKI　米国連邦政府
  - (2) SAFE-BioPharma
    - 製薬、医療
  - (3) HEBCA
    - 学術系
  - (4) Certipath
    - 航空宇宙産業

http://www.the4bf.com/

セコムIS研究所
Intelligent Systems Laboratory

技術的観点のトピック？

(1) モバイルID、モバイル署名
(2) サーバサイド署名
(3) 暗号アルゴリズムの移行

欧州のモバイル署名

セコムIS研究所
Intelligent Systems Laboratory

- 欧州のモバイル署名の標準化
  - ETSI(欧州通信規格協会)において標準化が進められている。
- 「モバイル署名サービス」が稼働している国
  - トルコ、フィンランド、スロベニア等
- トルコでの事例
  - 2007年2月のサービス開始
  - 「モバイル署名サービスプロバイダー」は、トルコの大手モバイルキャリア2社が提供
  - モバイル署名が利用できるサービスとしては、金融機関、電子政府、etc…
  - 電子申告を「 モバイル署名」で行うパイロットプロジェクトがある。

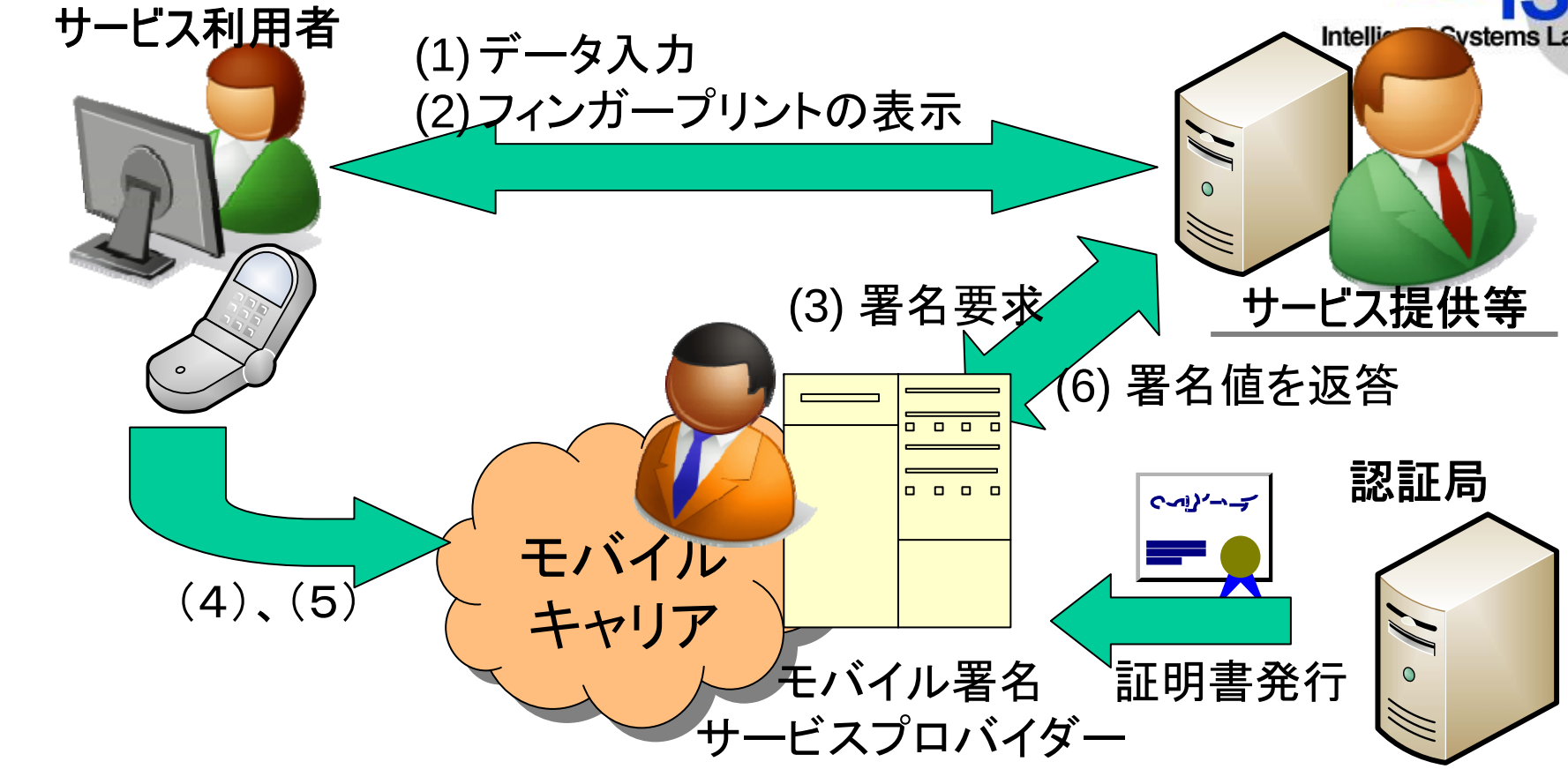
モバイルID、モバイル署名

ETSI(欧州通信規格協会)のモバイル署名に関する標準化文書

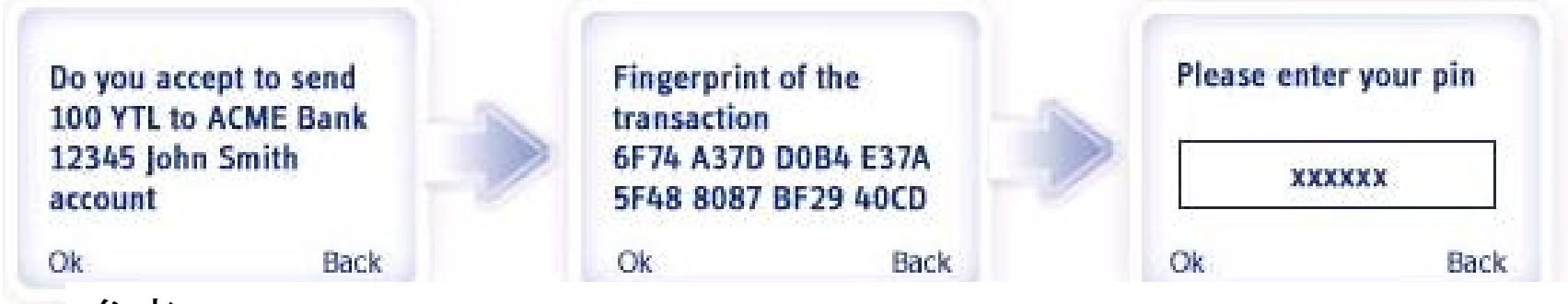
- ETSI 102
  - Mobile Commerce (M-COMM); Mobile Signature Service;
- ETSI TR 102 203
  - Business and Functional Requirements
- ETSI TS 102 204
  - Web Service Interface
- ETSI TR 102 206
  - Security Framework
- ETSI TS 102 207
  - Specifications for Roaming in Mobile Signature Services

・電子署名に関する標準化の多くは、ETSIを中心に進められている。
・「長期署名フォーマットの欧州実証実験ETSI Remote XAdES/CAdES Plugtests について」
欧州通信規格協会(ETSI) スペシャリストタスクフォース(STF)351 メンバー
次世代電子商取引推進協議会(ECOM) 客員研究員
エントラストジャパン株式会社　漆嶌 賢二 氏

欧州のモバイル署名



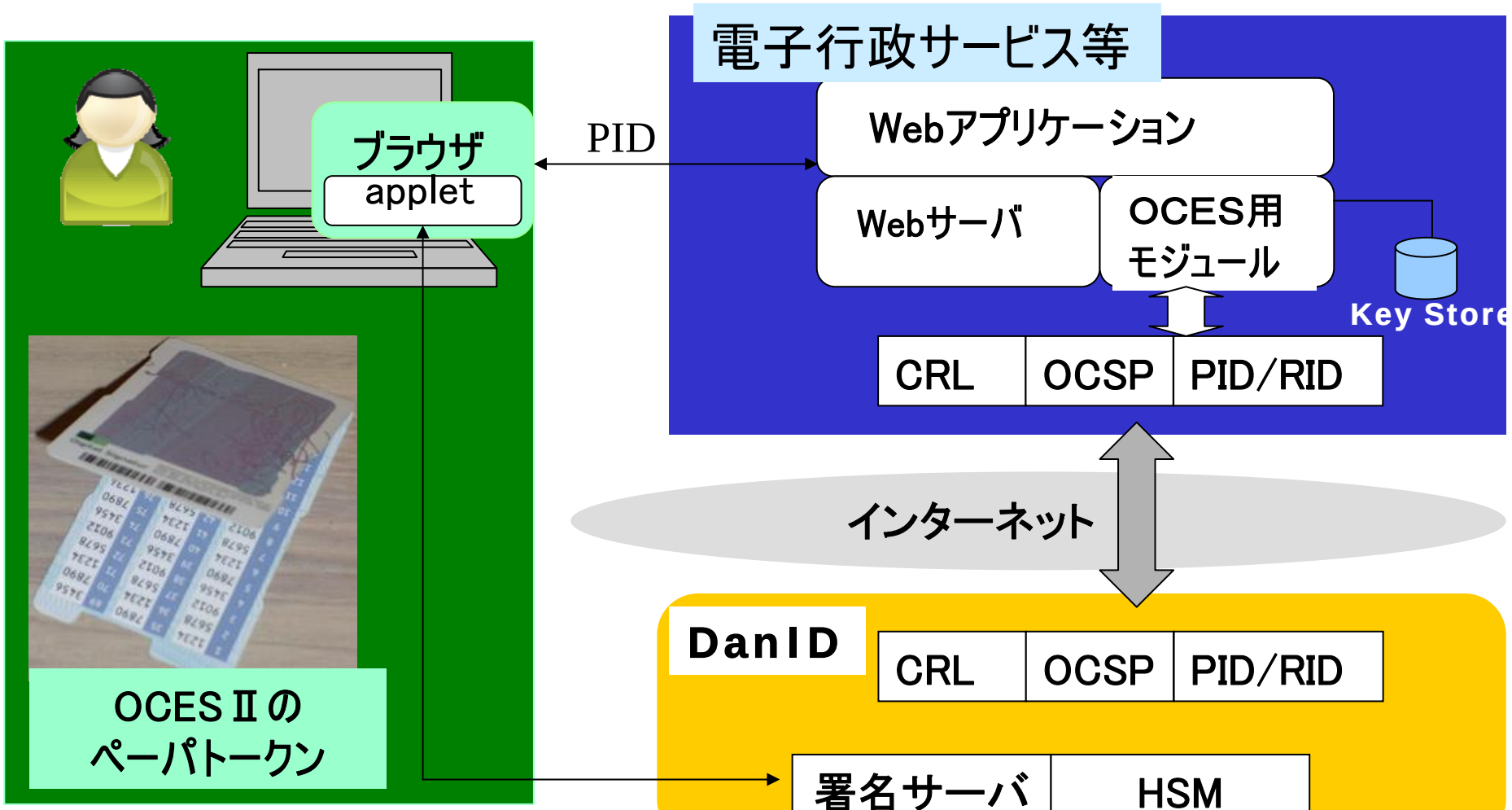
(4) フィンガープリントの表示　　(5) 署名のためのPIN入力



参考　http://www.turkcell.com.tr/en/services/Information/turkcellmobilimza

デンマークの
サーバサイド署名を利用した新しいOCES Ⅱ

セコム IS 研究所
Intelligent Systems Laboratory



PC上には、鍵、証明書も保持しない

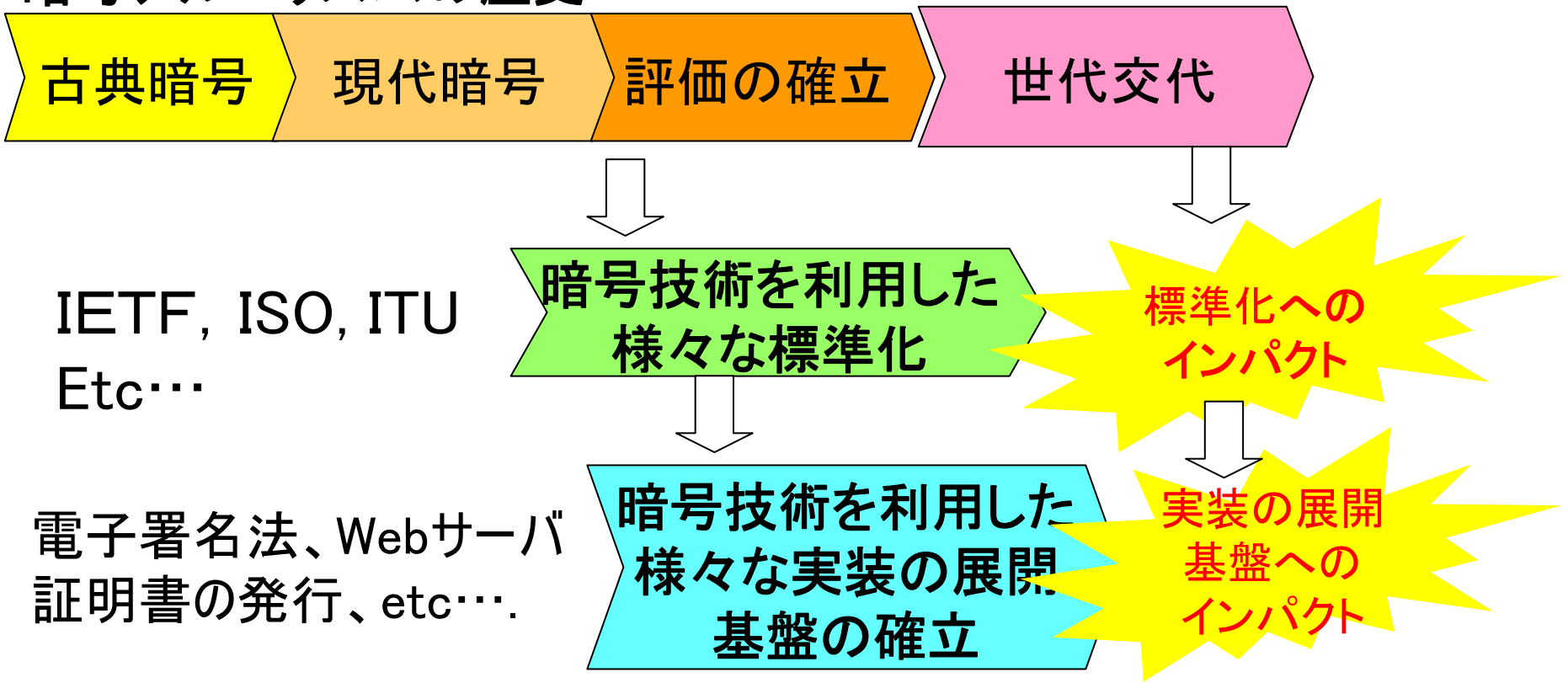
*** RIDは、企業ID

http://danid.dk/download/DanID-infomoede_250209.ppt

暗号アルゴリズムの移行

セコムIS研究所
Intelligent Systems Laboratory

暗号アルゴリズムの歴史



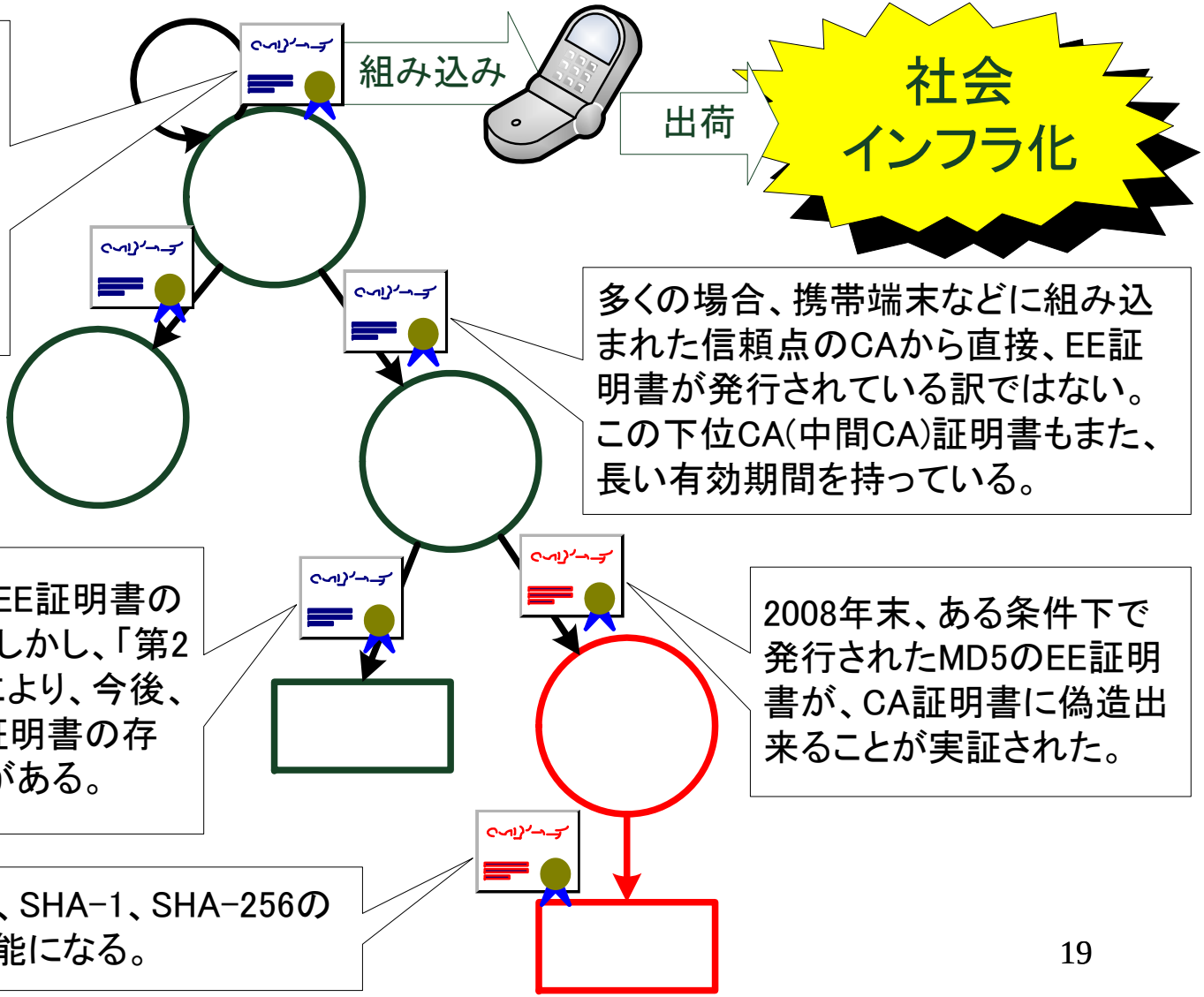
広く展開されているものほど移行が難しい

「政府機関及び金融機関のSSLサーバ暗号設定に関する調査結果について」
NTT情報流通プラットフォーム研究所　神田 雅透 氏

MD5 アルゴリズムへの攻撃を用いた X.509 証明書の偽造 移行の難しさ（暗号アルゴリズム脆弱化の本質）

セコム IS 研究所
Intelligent Systems Laboratory

「信頼点となる証明書」は、20年から30年の有効期限を持っている。しかしRSA 1024bitの証明書も多い。これらは、信頼点としての寿命であることが認識されるべき。



多くの場合、携帯端末などに組み込まれた信頼点のCAから直接、EE証明書が発行されている訳ではない。この下位CA(中間CA)証明書もまた、長い有効期間を持っている。

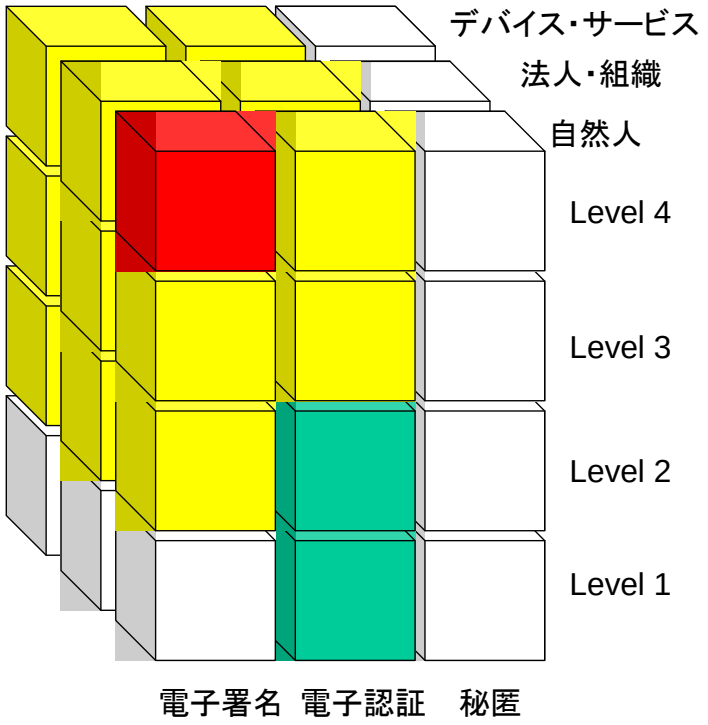
2009年1月以降、MD5のEE証明書の発行は停止されている。しかし、「第2原像探索攻撃」の成立により、今後、過去に発行されたMD5証明書の存在が脅威になる可能性がある。

2008年末、ある条件下で発行されたMD5のEE証明書が、CA証明書に偽造出来ることが実証された。

偽造CAからの証明書は、SHA-1、SHA-256の偽造証明書の発行が可能になる。

まとめ

- 標準化への努力
  - IETFやETSI等における活動
- 各分野における展開の努力
  - 電子政府や医療分野など
  - デジタル社会の基盤としての幅広い展開
  - 法制度との整合の努力
- 使いやすくする努力
  - モバイル署名、サーバサイド署名
  - リスクとのトレードオフ（サービスの要求レベルにあったPKI　LoAの導入）



参考

セコムIS研究所
Intelligent Systems Laboratory

- 「PKIをめぐる社会的動向」
  - プロフェッショナル・セキュリティ・レビュー
  - 出版社: アスキー (2008/1/24)
  - ISBN:978-4-7561-5103-2