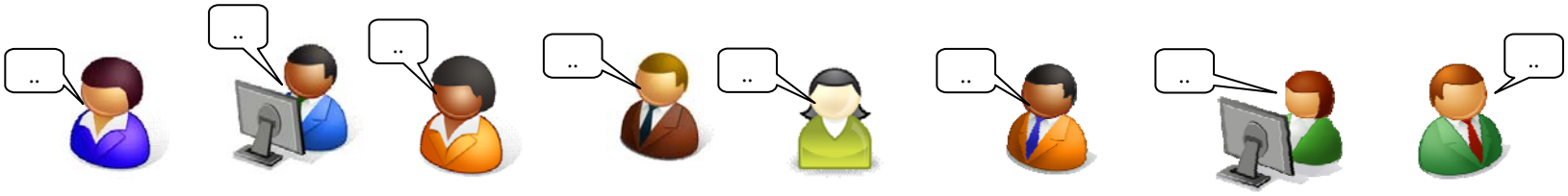
セコムIS研究所
Intelligent Systems Laboratory

社会基盤としてのPKI / PKIの10年

2010年6月29日

セコム(株)IS研究所　松本　泰



「社会基盤としてのPKI ／ PKIの10年」

セコム IS 研究所
Intelligent Systems Laboratory

- インターネットが急激に普及し社会基盤となったと言われ久しいものがあります。その中で、ネット社会における信頼（TRUST）の仕組み、すなわち信頼のおけるリモート認証や、電子署名、これらがネット社会の基盤として必要だと思われてきました。しかし、現実には、「ネット社会における信頼（TRUST）の仕組み」が定着し、社会基盤化していると感じている人は少ないでしょう。
- パネルディスカッションでは、過去からの現在までの取り組みや社会の変化も議論した上で、「ネット社会における信頼（TRUST）」を担うべき社会基盤としてのPKIの方向性を議論します。

セコムIS研究所
Intelligent Systems Laboratory

「社会基盤としてのPKI ／ PKIの10年」

- （1）「PKIの標準と相互運用性の課題」
  - 標準から実装、そして法制度との整合
- （2）「暗号アルゴリズムの移行問題」
  - SSL、電子署名法、電子政府。。。様々な課題
- （3）「電子署名法等の課題」
  - 認証(Authentication)も含めた認証、署名基盤へ
- （4）「番号制度とPKI」
  - そもそも、なぜ。。。電子証明書なのか。

パネリスト

セコムIS研究所
Intelligent Systems Laboratory

- 木村 泰司 氏
  - 社団法人 日本ネットワークインフォメーションセンター(JPNIC)技術部/インターネット基盤企画部 セキュリティ事業担当
- 稲田 龍 氏
  - 富士ゼロックス株式会社
- 秋山卓司 氏
  - クロストラスト株式会社 代表取締役／日本電子認証協議会 代表理事
- 佐藤　直之　氏
  - 日本ベリサイン株式会社　主席研究員
- 満塩 尚史　氏
  - 株式会社イマーディオ　パートナー
- 手塚 悟 氏
  - 東京工科大学 教授

セコムIS研究所
Intelligent Systems Laboratory

デジタル時代の
日本の社会？

効率的で、透明性があり
競争力のある社会？

目的

デジタル時代の
社会サービス

Trust が必要な様々な社会サービス

デジタル時代の
社会基盤

社会基盤としてのPKI　etc…

デジタル時代の
（信頼のための）
フレームワーク

標準化

実装

法制度

デジタル時代の
要素技術

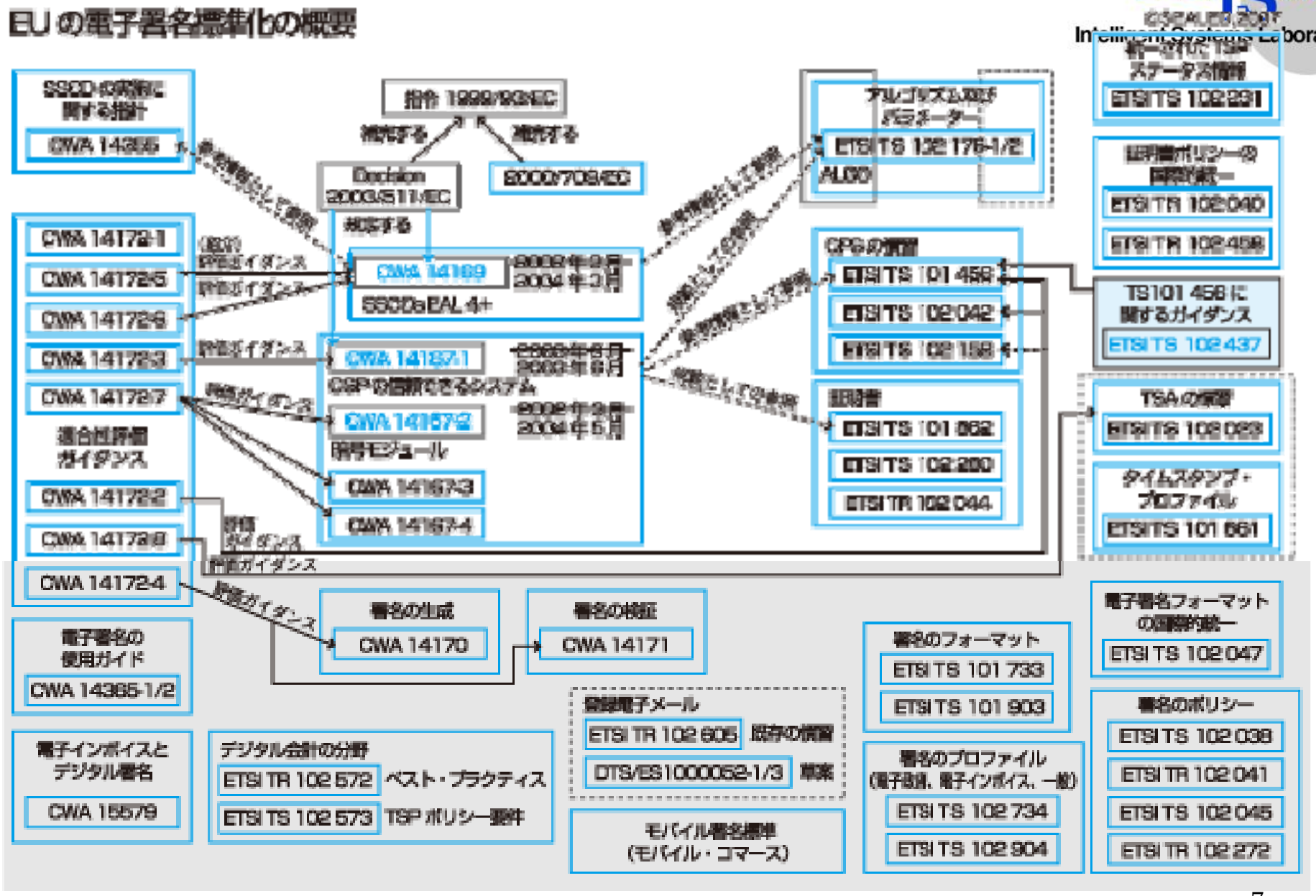
暗号技術　etc..

セコムIS研究所
Intelligent Systems Laboratory

「PKIの標準と相互運用性の課題」

標準から実装、そして法制度との整合

欧州における電子署名の標準化マップ



出展： http://www.jipdec.or.jp/archives/ecom/journal/2009/ecom_activity_report/safety/saf2.html

セコムIS研究所
Intelligent Systems Laboratory

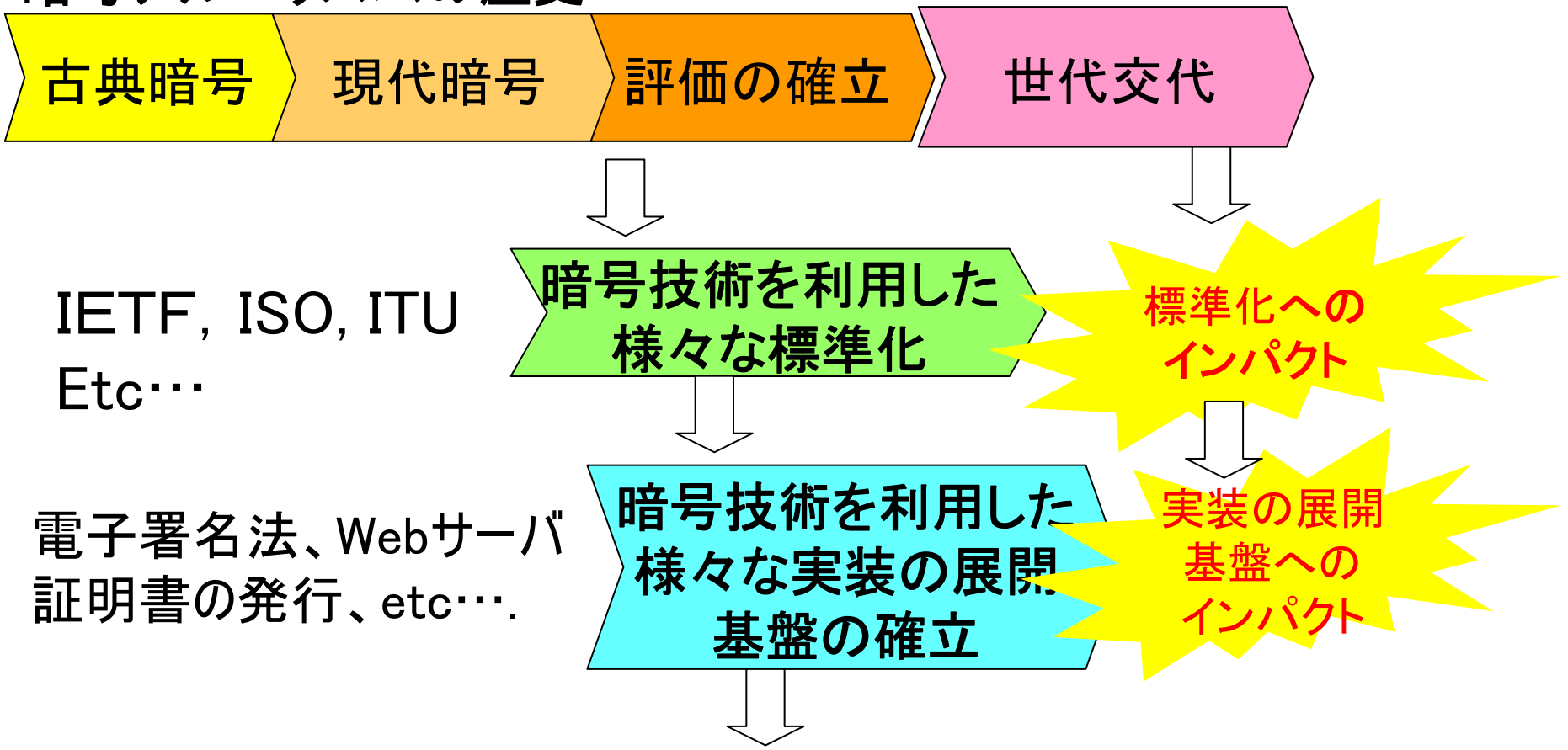
暗号アルゴリズムの移行問題

SSL証明書、電子署名法、電子政府、etc..
様々なステークホルダー間の調整

暗号の2010年問題？？
暗号アルゴリズムの移行の議論

セコムIS研究所
Intelligent Systems Laboratory

暗号アルゴリズムの歴史



暗号は、ITソリューションの「米」じゃなくて「小麦」状態??
ありとあらゆるITソリューションに組み込まれている

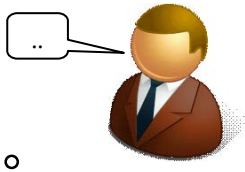
移行の問題

SHA-1からの移行の問題 – デッドロック状態になるかも

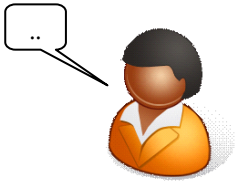
セコムIS研究所
Intelligent Systems Laboratory

- 暗号関係者 – CRYPTREC等
  - SHA2ファミリーに移行してね。。。

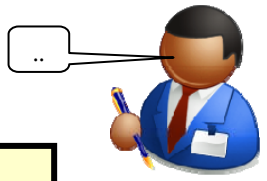
- (PKIなどの)標準仕様の策定者の悩み – IETFでの議論
  - 現実として展開されているプロトコルやフォーマットとの整合やマイグレーションの方法



- PKIミドルウェア(セキュリティ・ミドルウェア)開発者の悩み
  - 標準が曖昧でマイグレーションを考えると複雑な実装になってしまう。
  - #最新のバージョンのOS対応だけでいいよね？。。。。。



- アプリケーションベンダーの悩み
  - PKIミドルウェア頼み。悩みがないわけでもないが分からない。。。
  - #そもそも、そんな費用誰が負担するの??
- CA(認証局)運営者の悩み
  - CAは、アプリケーションが対応しない限り、SHA2ファミリに対応した証明書を発行できない。。。移行できない。



- (電子政府などの)??の悩み
  - ???

PKI day 2006 の松本のプレゼンから
http://www.jnsa.org/seminar/2006/20060607/matsumoto_02.pdf

暗号の2010年問題？？
2010年になったけど。。。。

セコムIS研究所
Intelligent Systems Laboratory

- 日本銀行・金融研究所・ディスカッションペーパーシリーズ
  - 「暗号アルゴリズムにおける2010年問題について」
    - 2005年11月
    - 宇根 正志・神田 雅透
  - 「SSL証明書における暗号アルゴリズム移行の現状と対応」
    - **2010年4月15日**公開
    - 宇根 正志・松本　泰

「暗号アルゴリズムにおける2010年問題」は
「暗号アルゴリズムの移行問題」

SSL証明書の暗号アルゴリズムの移行問題
ステークホルダーの声？？

セコム IS 研究所
Intelligent Systems Laboratory

モバイル
キャリア

メモリの関係から、よく使われるルート証明書だけを格納したい。

認証局

「全ての端末をサポート」して欲しいというお客様がいる限り古いルート証明書を使うしかない。

ブラウザベンダ

基準を満たしている限り、証明書リストに入れていくけど、暗号のことはどうしましょーね。
後、古いOSは、勘弁してね？

ともかくPCも携帯も全ての端末をサポートして欲しい

信頼できる証明書なんて分らないからブラウザを信頼するしかない

利用者

SSL

サーバ運営者

電子署名ってどうして
こんなに面倒なの？

セコムIS研究所
Intelligent Systems Laboratory

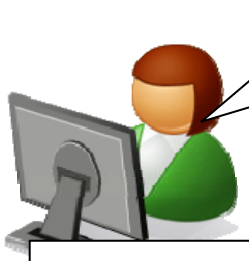
「電子署名法等の課題」

（標準）技術
はあります

法律は
こうなってます

ギャップ

標準化と法制度の関係



？？？

セコムIS研究所
Intelligent Systems Laboratory

"Rough consensus and running code"

法制度等から
ニュートラルな
技術標準

民事訴訟法は228条4項 「私文書は、本人又はその代理人の署名又は押印があるときは、真正に成立。。」

ギャップ
噛み合わない会話
共有されないビジョン

IETF等の
標準化

・既存のレガシーな法制度
・様々な管轄官庁の様々な業法

デファクト標準
としての実装

対極の実装

紙前提の制度
（の電子化）

強い影響

「電子署名法」、「e文書法」、「電子公証人制度」、「商業登記に基づく電子認証制度」、「住民基本台帳制度」、「タイムビジネス信頼・安心認定制度」、etc….

現実の実務からの乖離という問題

既存の慣習、権益が強すぎる問題

「光の道」で医療問題も教育問題も解決する？

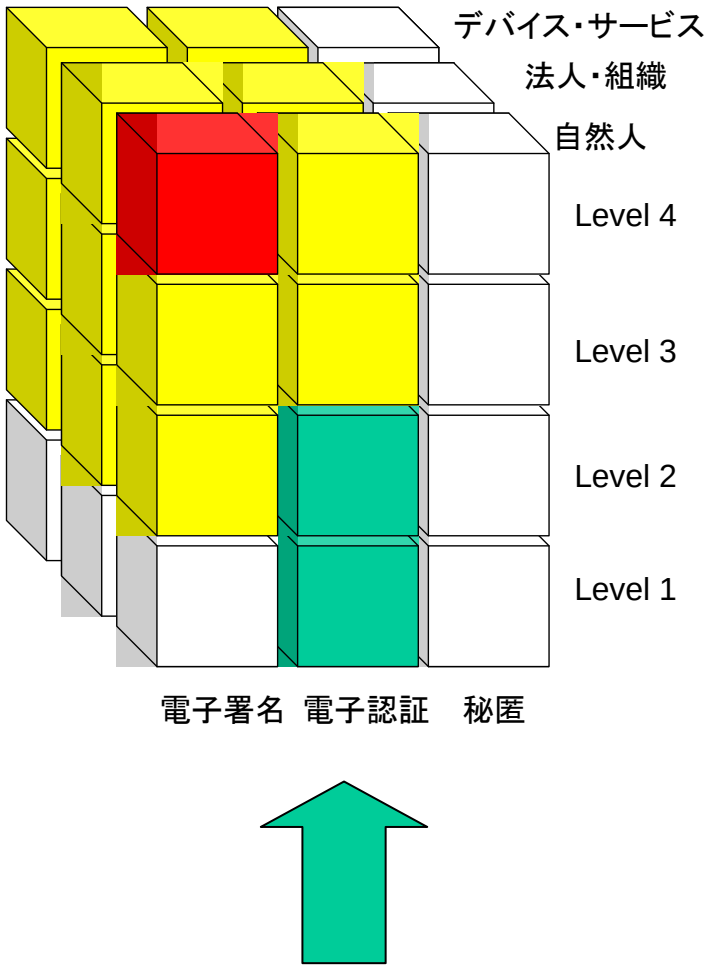
番外編

現在の医療の問題点は、デジタル化以前の問題

情報セキュリティに関連する制度の課題
電子署名法の功罪

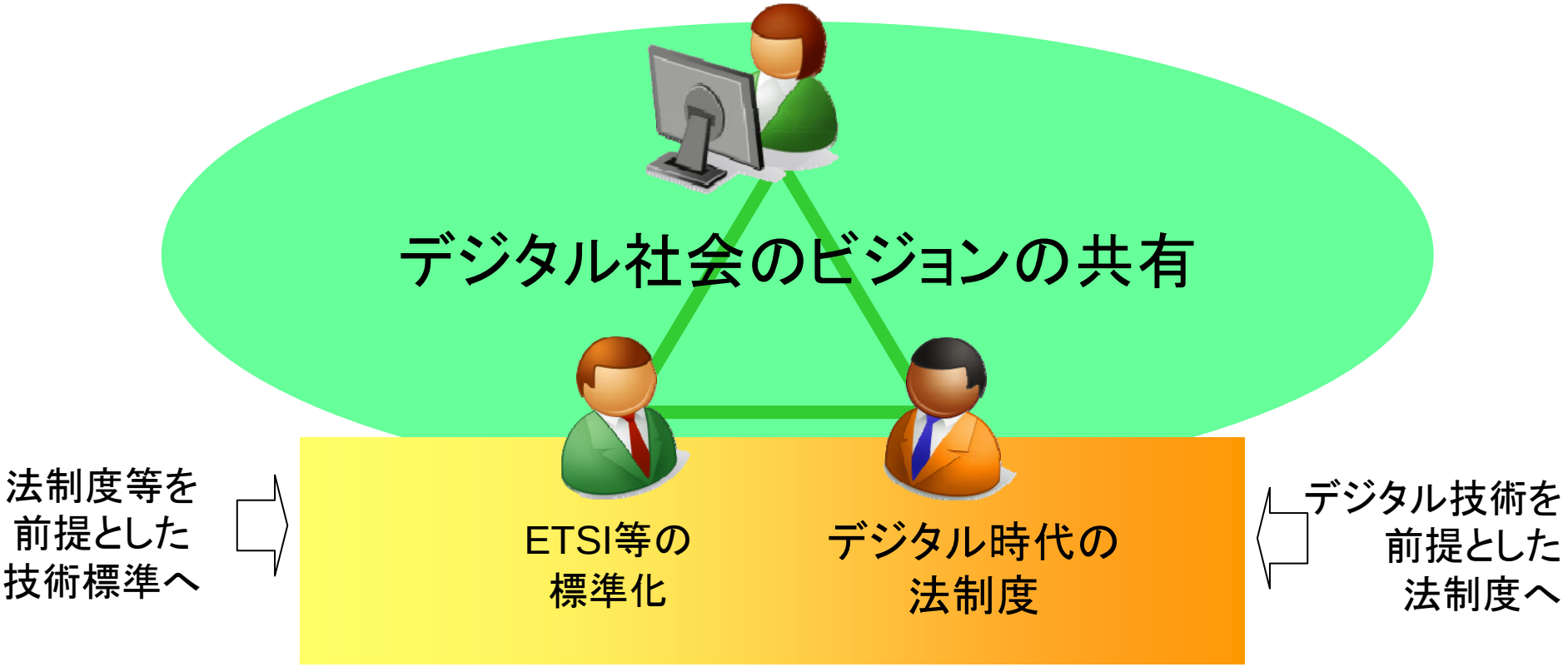
セコム IS 研究所
Intelligent Systems Laboratory

- 「電子署名法」の認定制度は、「**推定効**」の呪縛（および、無謬性を求める電子政府のサービス）等からリスクを許容しない非常に厳しい基準を課している。そのため、電子署名法の認定基準自体は、世の中で署名が使われるべき全ての領域に対してベストプラクティスを提供している訳ではない。
- 現状の電子署名法のカバーしている領域は、非常に狭く、各種の厳しい基準が、電子署名は使いにくい、高価、運用が難しいというイメージを与えている面がある。
  - 非常にニッチなビジネス領域の社会的なインパクトがない分野にしてしまっている。。。。
- セキュリティの視点だけ追及してきたこと自体が、逆に「TRUSTの確立」を妨げている可能性がある。



無謬性的な要求がなされた電子署名法の世界と
混沌としたビジネスのレモン市場の世界の同居？？

標準化と法制度の関係
欧州のアプローチ?



セキュリティの観点だけで「TRUSTが確立」するわけではない

2000年頃のアプローチ？

セキュリティ → X →「ネット社会における信頼（TRUST）の仕組み」の確立

トレードオフの正しい理解

コスト・効率　　利便性

（認証基盤等）社会基盤化

- 「セキュリティ」「コスト・効率」「利便性」のトレートオフに対する正しい理解
- 認証基盤なども、他の基盤（インフラ）と同様にエコシステムとして成立する必要がある

エストニアの政府系PKI

セコムIS研究所
Intelligent Systems Laboratory

Web trust for CAではなく、
ETSI TS 101 456　Policy requirements for certification authorities issuing qualified certificates
よる監査

Juur-SK
ルート認証局

・マイクロソフトルート証明書プログラムメンバー、
・Mozilla認証局証明書ストア
・iPhone OS 3.x: List of available trusted root certificates

ESTEID-2007
エストニア
IDカード向け

EID-2007
モバイルID向け

KLASS3 2010
法人、デバイス、
サーバ向け

認証用
証明書

署名用
証明書

認証用
証明書

署名用
証明書

SSL
証明書

エストニアの政府系PKI　その2

セコム IS 研究所
Intelligent Systems Laboratory

- エストニアの電子政府　　（日本の電子政府と真逆な？）
  - 既存の「インフラ、法制度、慣習、権益」等のしがらみが少ない
  - デジタル社会を前提にした法制度？　（そのための政府系PKI?）
  - PKIを利用したインターネット投票なども「柔軟な法制度」の典型
    - #エストニアにおけるインターネット投票の割合は、選挙毎に倍増
- エストニアの政府系PKIの特徴　－　実際には、公共と民間の差違はない
  - 同一の認証局から「署名用」と「認証用」の証明書を発行している
    - 欧州では、「署名用」と「認証用」の証明書を分けて発行するのが一般的
    - 欧州でも厳密な「電子署名法」を実施しているドイツなどでは、「署名用」の証明書を発行する認証局を分けている
  - 同一のルート認証局配下からからSSL証明書等も発行している
  - ETSIの標準による監査
    - 認証局の「監査」は、「Web trust for CA」 ベースではなく、「ETSIの標準」に基づいた監査を受けている
    - これを根拠に、MS、Mozilia、etcにルート証明書が組み込まれている。
    - 電子署名法の要求からくる認証局の監査と、ルート証明書をWebブラウザ等に組み込むための認証局の監査が同一？

セコムIS研究所
Intelligent Systems Laboratory

番号制度とPKI

そもそも証明書はなぜ必要か？

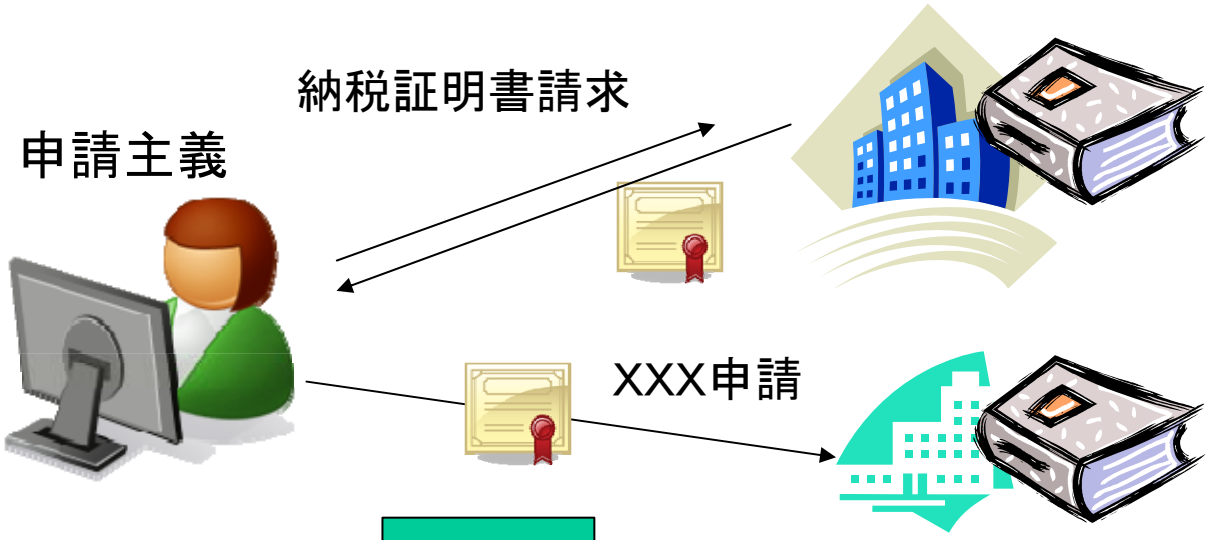
番号制度とPKI
アイデンティティの認証とか証明とかに関して

セコムIS研究所
Intelligent Systems Laboratory

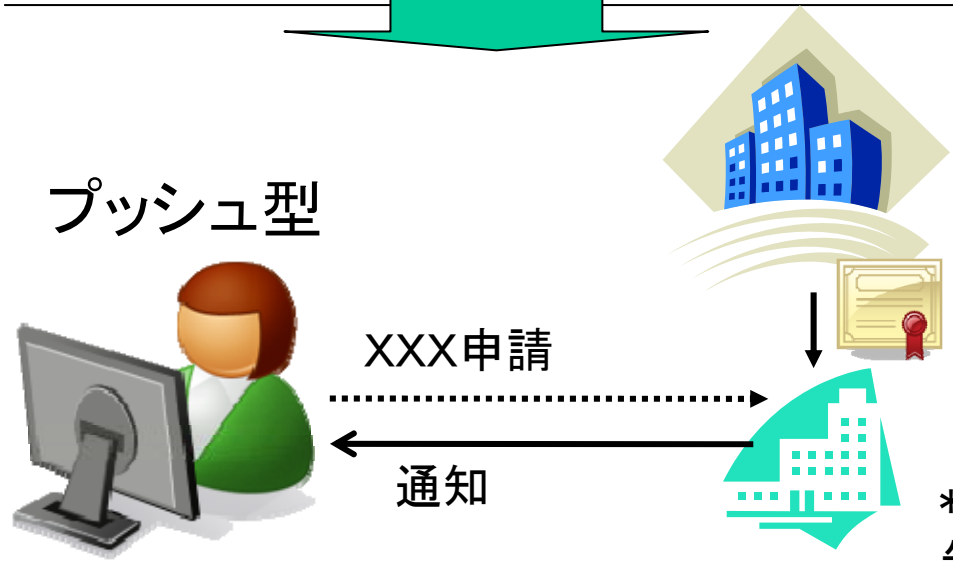
- How　ー　この話をずっと（10年間）やっている
  - 暗号の強度、電子政府推奨暗号リスト
  - 暗号の2010年問題
  - 電子署名法の認定認証局などの「認定制度」
  - 様々な標準化、複雑な相互運用技術。。。これの解決
  - Etc……
- What　ー　この観点は、ほとんど議論されていない。。。
  - 何を（電子的に）証明できれば社会の発展とか効率化に寄与できるのか？
    - もう少し具体的な例としては、
      - 「PKIの証明書の内容」や「ID連携のアサーションの内容」
  - 社会基盤としての「認証基盤」が必要だとすると、「社会基盤」としての「ID管理基盤」が必要になる（と思うけど。。。）

番号制度とPKI
電子政府のバックオフィス連携＆プッシュ型への流れ

セコム IS 研究所
Intelligent Systems Laboratory



- 「紙台帳」の延長上にある（その電子化）
- 明治以来からの基本的な仕組み＊＊＊
- 「認証」も個別対応でも可能だった（ex. 税金を払った人に納税証明書を発行する）



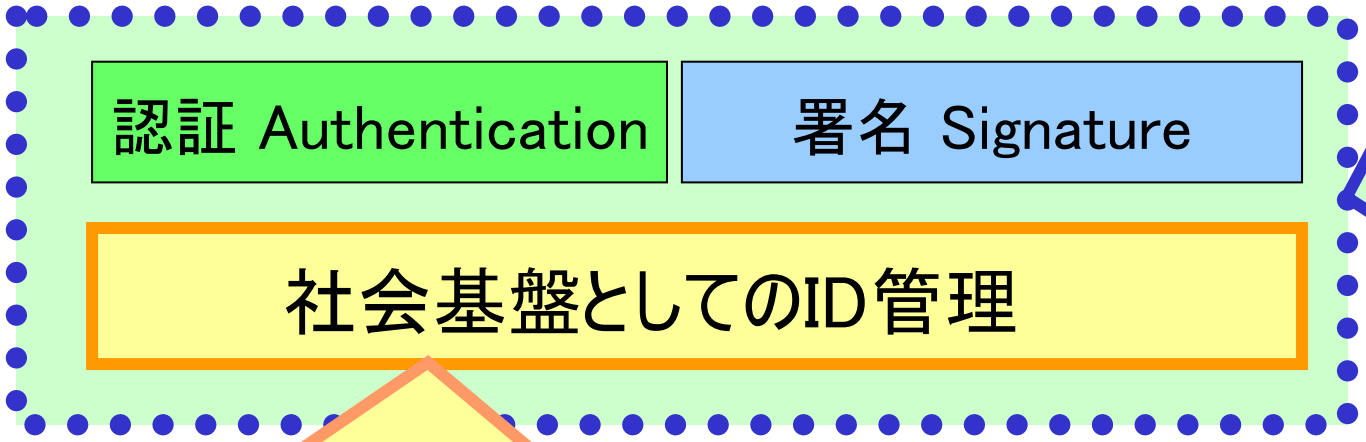
- 欧州の電子政府では、行政のバックオフィスの連携ができなくてはならないという方向性がある。
- 個人情報を転送するという「壁」もある（この議論は別途）

＊＊＊結局のところ、2001年頃に目指した世界最先端電子政府は、100年前からのシステムの電子化だったのでは？

番号制度とPKI
「認証基盤」と「社会基盤としてのID管理」

セコムIS研究所
Intelligent Systems Laboratory

- デジタル社会における識別（認証）や責任の明示（署名）には電子証明書が大きな意味を持つ
- 電子証明書は、個人や企業のアイデンティティを証明するもの（Certification）。
- このIDと人や企業を結びつけるID管理モデルは、行政サービスのフロントエンドだけでなく、バックオフィスの連携も含めて考える必要がある。
- よく考慮されたシステム（法制度、官民連携の情報システム）が構築できれば、社会全体としての、人や企業に対するサービスの効率性の向上と、透明性の確保が実現される。



広義の
「認証基盤」
電子的な認証
(Authentication)&
署名（Signature）
の基盤

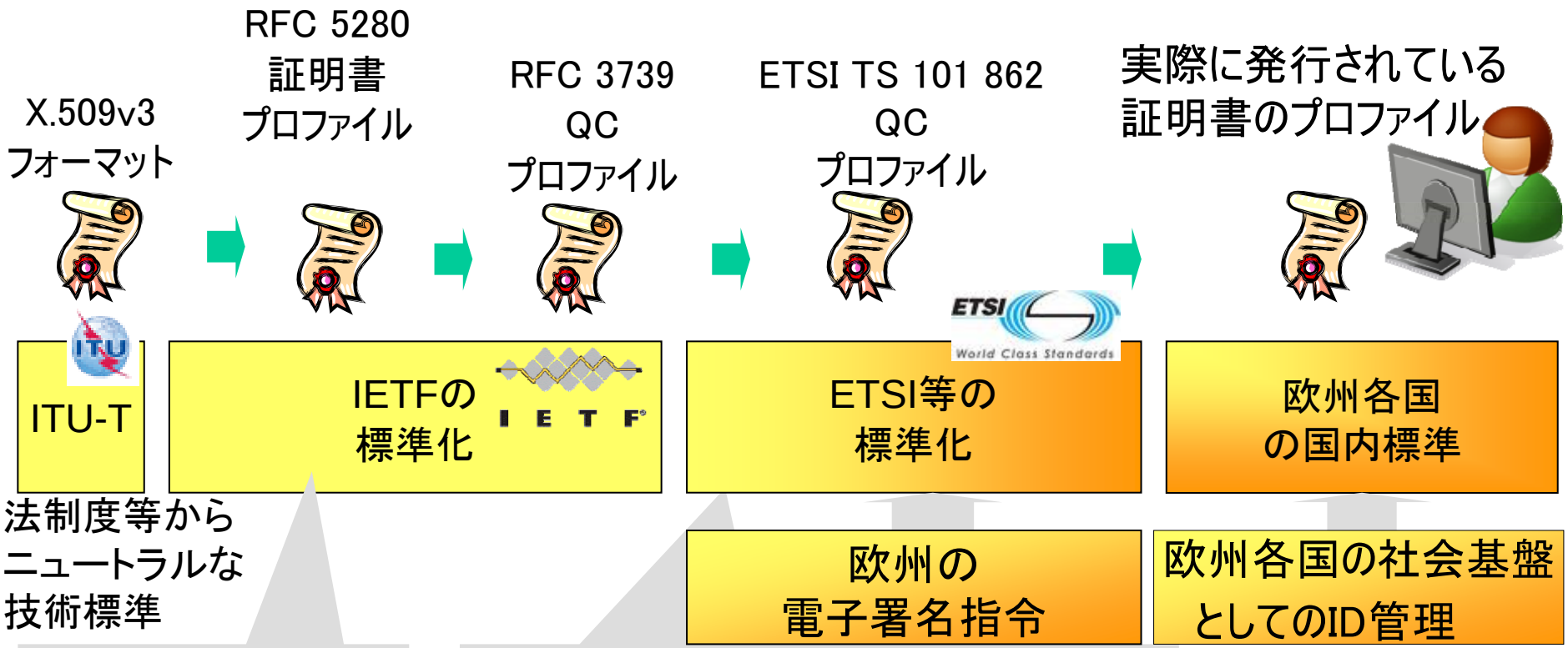
狭義の「認証基盤」
電子的にIdentityをCertifyし管理するための基盤

- PKI day 2009（JNSA）「欧州の政府系PKIとID管理」をアレンジ

番号制度とPKI – 標準化と法制度の関係

クォリファイされたアイデンティティを証明するための証明書

セコム IS 研究所
Intelligent Systems Laboratory



Trustのためのフレームワーク

韓国の場合

セコム IS 研究所
Intelligent Systems Laboratory

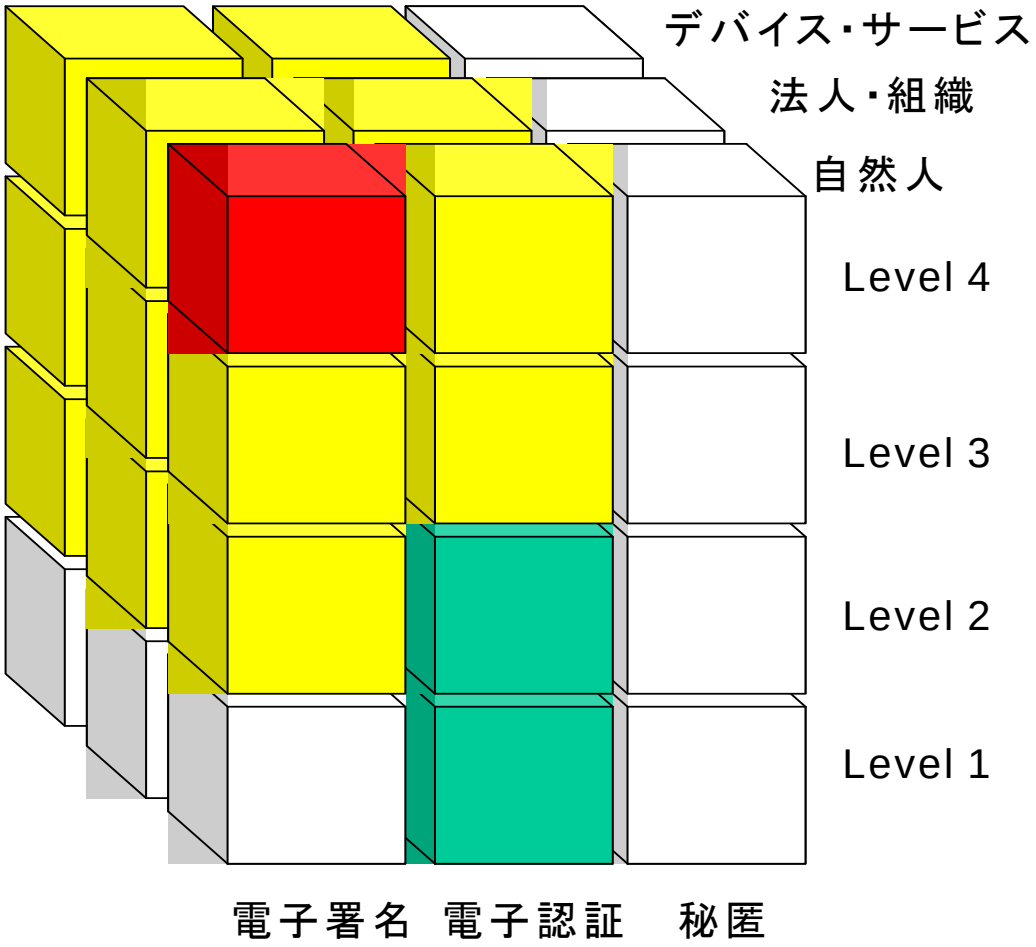
- 韓国の電子署名法
  - 「公認認証局」、「公認証明書」、「公認署名」
  - 「公認証明書」は、accredit certificate
  - ＃日本の電子署名法のネーミングの問題の問題
  - 2000万枚以上の公認証明書の発行
  - 市民レベルでの実際の利用の多くは「署名」ではなく「認証」
- 公認証明書により証明される内容
  - 名前と仮想識別番号(VID)
    - ＃VIDは、住民登録番号等から生成
  - ＃住所は入らない
- IETF/PKIXでの標準化　– KISAのメンバーによる標準化活動
  - RFC 4683 Subject Identification Method (SIM)
    - 韓国の「公認証明書」で実際に使われている
    - ＃VIDから住民登録番号を証明など
  - RFC 5636　Traceable Anonymous Certificate (TAC)
    - インターネット投票で利用することが念頭にあるらしい

セコムIS研究所
Intelligent Systems Laboratory

Backup

松本キューブ?? ー 2004年頃

セコムIS研究所
Intelligent Systems Laboratory



LoA(Level of Assurance)と言う考え方

・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？

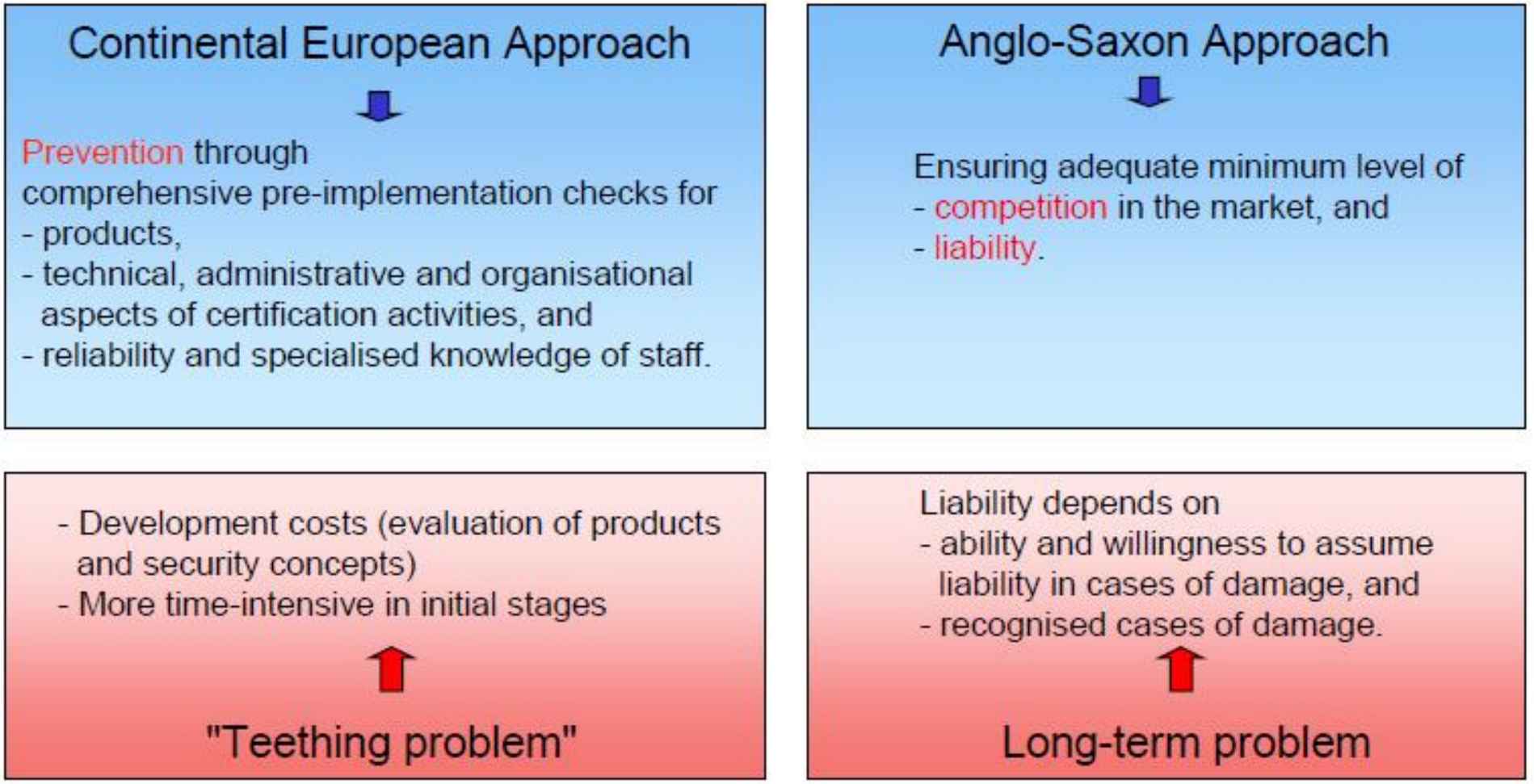
電子署名法(認定)の領域

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

電子署名法の”Teething problem”？？
この認識がないと将来は”long-term problem”に苦しむ？

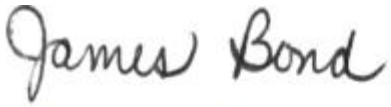
セコムIS研究所
Intelligent Systems Laboratory



http://www.efpe.eu/upload_module/downloads/efpe/2006/prezentacje/2/06_JSchwemmer_BNetzA.pdf

米国の電子署名法

セコム IS 研究所
Intelligent Systems Laboratory

	[*Digitized image of handwritten signature*]
/s/ James Bond	[*Typed name*]
007	[*Number or PIN*]
X	[*"X" or other random letter*]
☺	[*Smiley face or other picture*]
I Agree to these terms	[*Words typed in box*]
	[*Button clicked with mouse*]

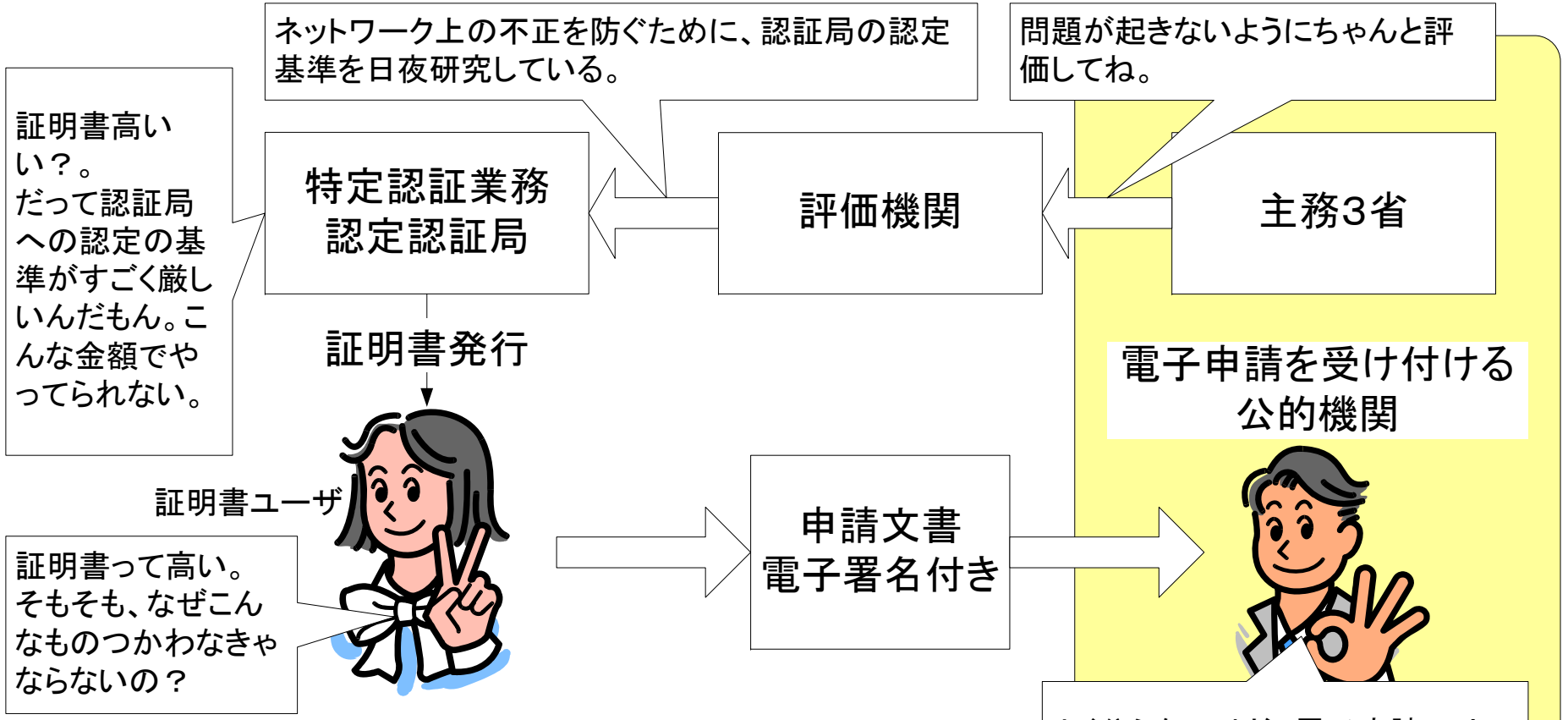
-----BEGIN SIGNATURE-----
iQCVAwUBMARo7vgyLN8bw6ZVAQF6ygP/fDnuvdAhGlDWsSMXUIR
MuNHYzdZ00cqkDb/Tc2+DuhuEa6GU03AgZY8K9t5r9iua34E68pCxo
gUz009b1OcjNt6+o+704Z3j1YY9ijYM8BWNaSp9L2W4nUuWBdlylWy
ol/2PjjRVNZEtqtSRQnPEpJ2IHtz9iGovHf0Sqh
-----END SIGNATURE-----

[*Digital signature*]

http://www.fips201.com/resources/audio/iab_0210/iab_022410_smedinghoff.pdf

電子署名法の認定認証局の認定の問題
非常に認定基準が厳しい － 結果、高コスト

セコム IS 研究所
Intelligent Systems Laboratory

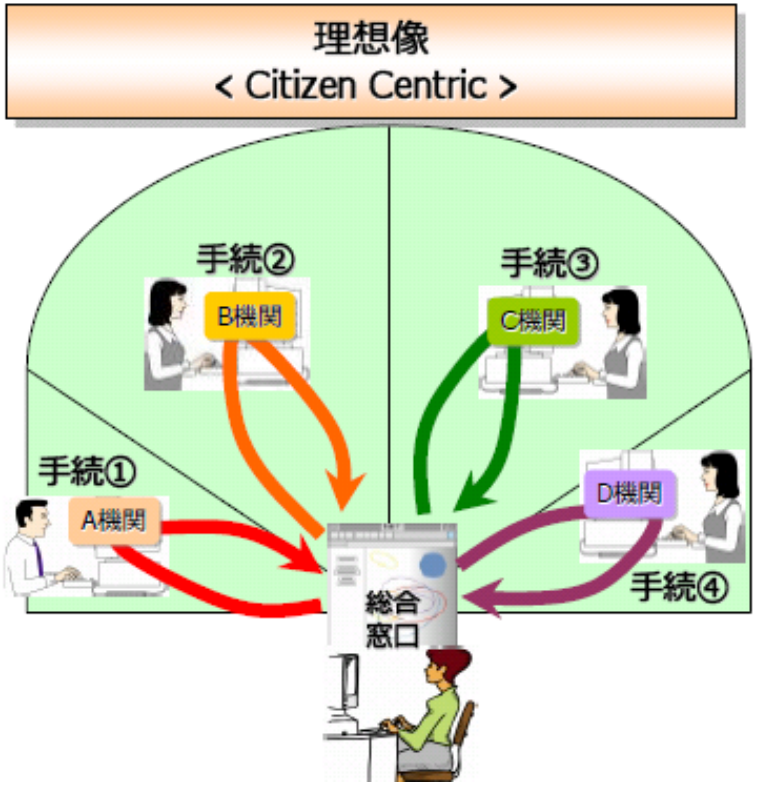


- *セキュリティとコストがバランスする構造になってない*
- *セキュリティ基準が高くてうれしいのは、本来電子申請を受け付ける府省などであるはず。ところが、府省からは料金を徴収できない。*

**公的個人認証サービスは、証明書検証者

2005年の松本のプレゼンから
http://www.jnsa.org/seminar/2005/seminar_20051028/6matsumoto.pdf

行政サービスのパラダイムシフト
次世代電子行政サービス基盤のコンセプト



出展： 次世代電子行政サービス基盤等検討プロジェクトチーム中間報告（案）
http://www.kantei.go.jp/jp/singi/it2/nextg/meeting/dai9/siryou4.pdf

エストニアの電子政府の概観

セコムIS研究所
Intelligent Systems Laboratory

法的な枠組み

個人情報保護法
Personal Data Protection Act

Public Information Act
（旧データベース法?）

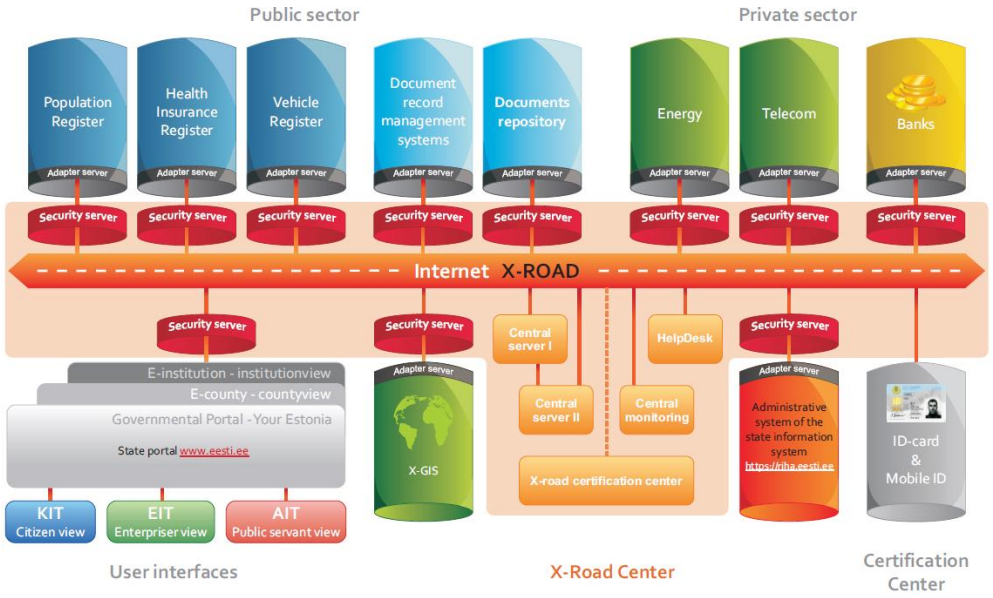
電子署名法
Digital Signatures Act

Etc…

監視

情報保護監察局（個人情報保護法に基づく第3者機関）

X－ROAD　バックオフィスの連携



フロントオフィス

エストニアのeID

識別、認証、署名のための
フロントエンドツール

サービス対象者

アイデンティティの考え方

Conseils Oy

Claimed Identity, Legal Identity

Identityの使い分けがある。公共性の強いサービスほどLegal Identity が求められる。

- Relational / Claimed identity:
  What is your relation to...
- Legal / Given identity:
  Who you are

出典： http://www.brreg.no/porvoo13/documents/european_eidmanagement_teemu_rissanen.pdf

「オーストリア電子政府法」 2004年
「オーストリア電子政府法」における識別

セコムIS研究所 Intelligent Systems Laboratory

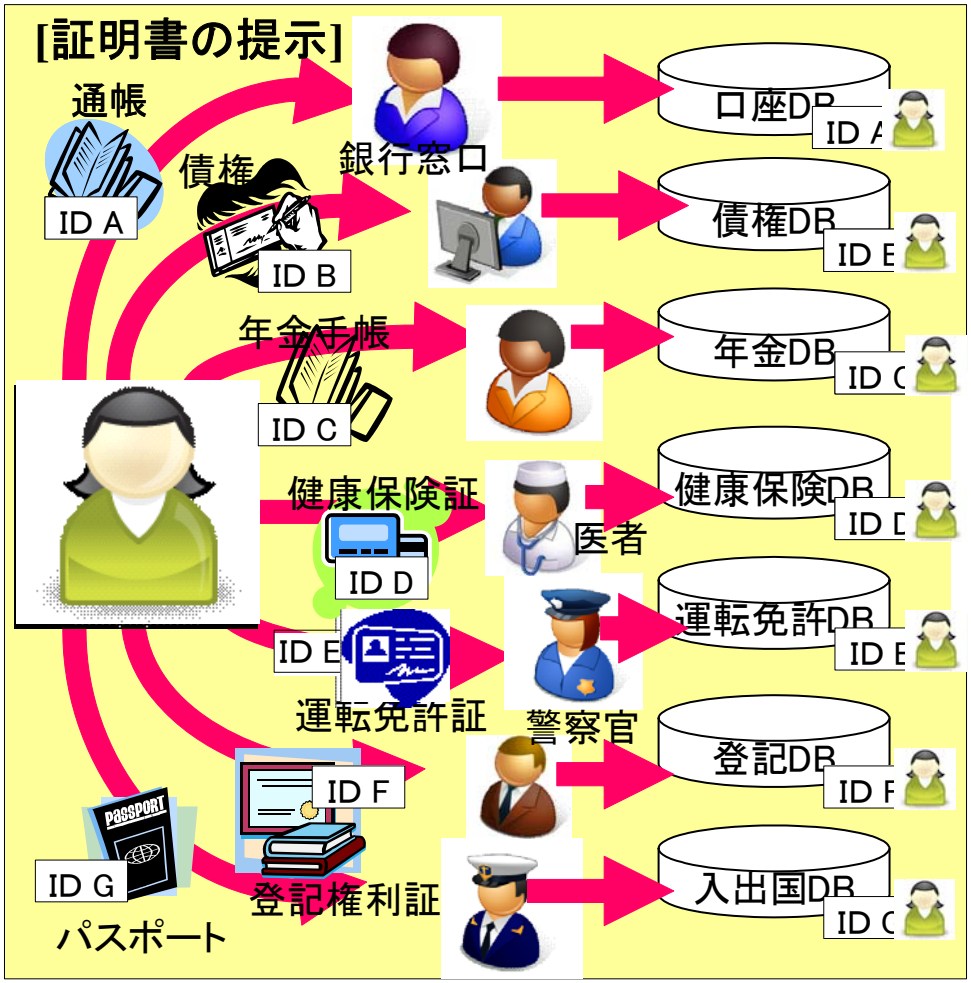
- 「一意識別(Unique identity)」
  - データ主体者が他のすべてのデータ主体者から誤りなく識別されることを可能にする、一つまたは複数の特徴による特定人(データ主体者、本条7号)の指定。
- 「履歴識別(Recurring identity)」
  - 一意識別(Unique identity)によらずに、以前の出来事(以前の提出行為など)の参照により人の認識を可能にする方法での特定人(データ主体者、本条7号)の指定。
- 一意識別と履歴識別
  - 「2000年データ保護法」(中略)秘密性に保護権益が存在する個人データへのアクセス権(「2000年データ保護法」第4条1号)が付与されるのは、アクセス要求者が一意識別(Unique identity)され、その要求の真正性(Authenticity)が確認された場合に限る。かかる確認は、電子的に証明されうる形態で提供されなければならない。
  - 履歴識別(Recurring identity)のみが可能な場合、アクセスが許可されるのは、アクセス要求者が当該識別を使用して自ら提供した個人データに関するものに限る。

＊＊2008年の改正で「履歴識別」の記述は削除された。

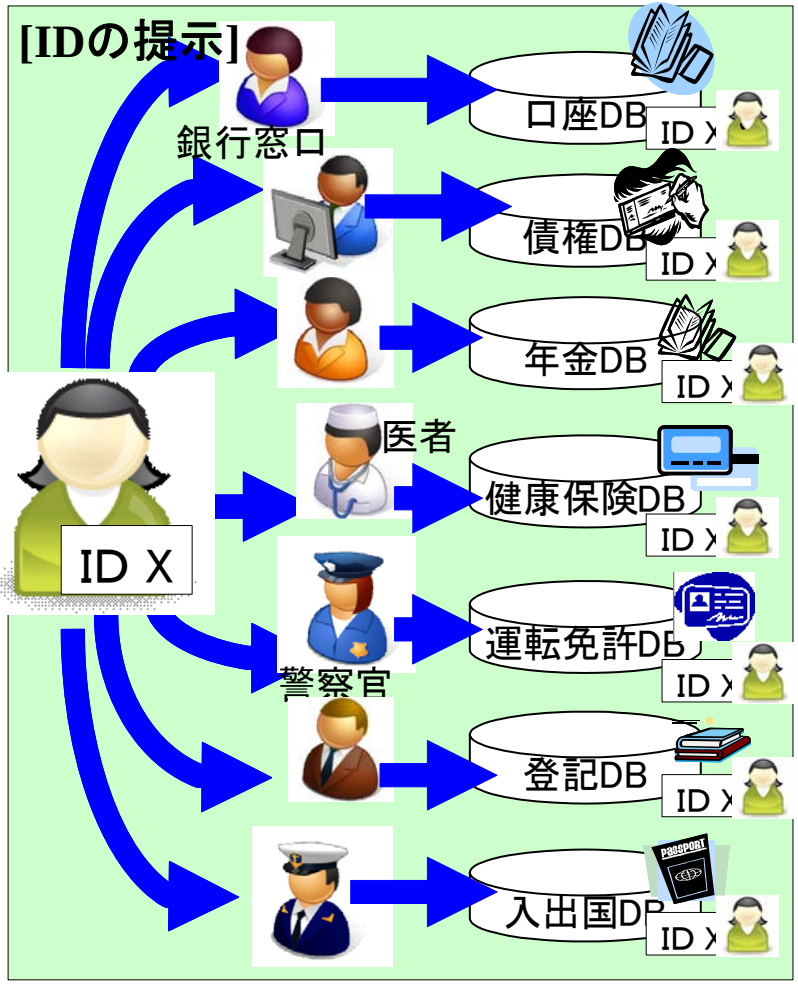
The Austrian E-Government Act
http://www.stammzahlenregister.gv.at/documents/e-government-. act_federal_law_gazette_part_i_no_10_2004.pdf

社会基盤としてのID管理
「識別された個人の属性」への移行

セコム IS 研究所
Intelligent Systems Laboratory



権利などの属性が所持により示される
オフライン指向



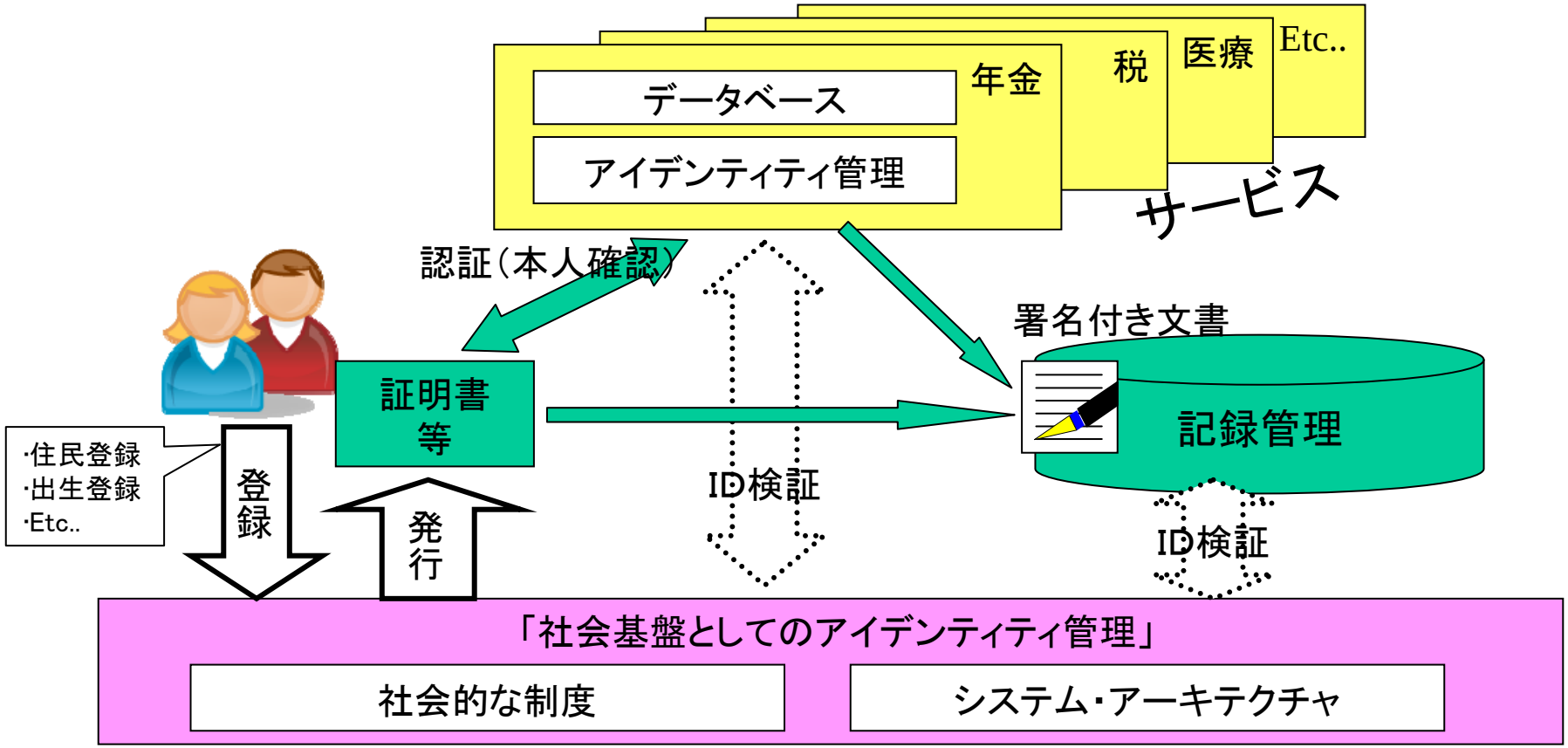
識別された個人と個人の属性
オンライン指向

「社会基盤としてのID管理」のあるべき姿

セコム IS 研究所
Intelligent Systems Laboratory

- 適切な**個人情報保護**、**プライバシー保護**
- IT化による**社会的コスト低減**、**全体最適化**
- 適切な**コンプライアンス**と長期的**アカウンタビリティ**の達成

これらがバランス良く実現されること



IPAの「情報セキュリティ白書 2008」「IT 社会を支える基盤としてのアイデンティティ管理」より作図した
PKI day 2009（JNSA）「欧州の政府系PKIとID管理」をアレンジ

ID管理と証明書の内容
各国の事例の比較

セコムIS研究所
Intelligent Systems Laboratory

国	ID管理モデル	IDとID管理の主体	認証局	証明書に記載されるID情報
エストニア 	フラットモデル	内務省の管轄にあるエストニア市民権・移民委員会（CMB）が**11桁の国民ID**を発行している。	エストニアの2つの主要な銀行および2つの通信会社によって設立された「証明書発行センター」	**11桁の国民ID** KAART
デンマーク 	フラットモデル	福祉省管轄のCPR Bureauという機関が、10桁の国民番号（CPR番号）を約40年前に導入している。	科学技術革新省と契約したTDC（旧国営電信電話会社：Tele Denmark）が運用している。	**CPR番号に変換可能なPerson-specific Identification Numbers (PID)**
スロベニア 	セパレートモデル	・個人登録番号(PRN)は、スロベニア内務省 ・納税者番号(Tax Number) は、国税庁(Tax Administration) ・健康保険番号(Health Insurance Number)は、スロベニア健康保険協会(HIIS)	総務省が運営する公務員に証明書を発行するSIGOV-CAと、自然人、法人に証明書を発行するSIGEN-CA その他民間認証局も存在する。	認証局(SIGEN)が管理する「シリアル番号」。この「シリアル番号は、個人登録番号(PRN)、納税者番号(Tax Number)と関係付けられている。
オーストリア 	セクトラルモデル	国民登録機関（CRR：Central Register of Residents）発行する国民登録番号（ZMR-Zahl）がある。ただし「国民登録番号（ZMR-Zahl）」の利用には法的な制約があり、そのまま利用する訳ではない。	民間の認証局であるA-TRUST または、 社会保険本部	「名前」のみ。 公開鍵証明書の「公開鍵」とSourcePINの関係を証明したIdentity.linkというXML署名ファイルが利用される。

参考資料

セコム IS 研究所
Intelligent Systems Laboratory

- Internet Week 2009　3時間でわかるこれからの電子認証
  - http://www.nic.ad.jp/ja/materials/iw/2009/proceedings/h9/
  - https://internetweek.jp/program/h9/
- PKI day 2008 パネルディスカッション／「暗号アルゴリズム移行問題」
  - http://www.jnsa.org/seminar/2008/0703/
- SecurityDay2009
  - 「電子認証のあり方」これまでの10年と今後の方向性
  - http://securityday.jp/?program
  - http://securityday.jp/?materials
- 国民ID時代の電子認証のあり方 ――Security Day 2009
  - http://codezine.jp/article/detail/4744
- Internet Week 2008　次世代暗号アルゴリズムへの移行 ～暗号の2010年問題にどう対応すべきか～
  - http://www.nic.ad.jp/ja/materials/iw/2008/proceedings/H10/
  - https://internetweek.smartseminar.jp/public/session/view/40
- SSL証明書における暗号アルゴリズム移行の現状と今後の対応
  - http://www.imes.boj.or.jp/japanese/jdps/2010/yoyaku/10-J-11.html
- 社会保障・税に関わる番号制度と情報セキュリティの１０年
  - http://www.jnsa.org/jnsapress/vol28/2_tokusyu1.pdf
- EV SSLを議論するCA/Browserフォーラム、日本で初開催
  - 非ラテン語圏の課題は欧米に伝わるか？
  - http://enterprise.watch.impress.co.jp/docs/news/20100513_366607.html