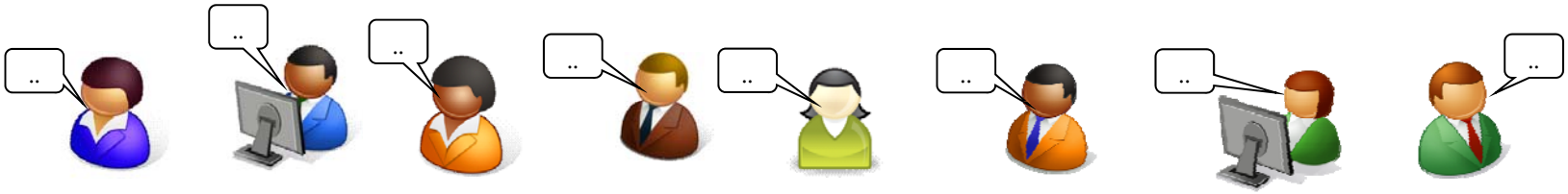
セコムIS研究所
Intelligent Systems Laboratory

我が国における信頼基盤の連携に向けて

2012年12月13日

セコム(株)IS研究所　松本　泰



【午前の部】
「我が国における信頼基盤の連携に向けて」

セコムIS研究所
Intelligent Systems Laboratory

- PKIは現在、様々な情報通信基盤の信頼の要として利用されています。例えば、インターネット上の通信におけるTLS/SSLや、電子政府の電子申請等で利用される電子署名法に準拠した証明書による電子署名、e文書法等で要求される時刻証明のためのタイムスタンプ等があります。我が国において、これらのPKIは、それぞれ別々の目的や成り立ちがあり、現在は、似て非なるフレームワークで、構築、運用されています。
- しかし、今後は様々な分野において情報連携が求められており、この情報連携を実現するうえで整合性の取れた信頼基盤構築のフレームワークが重要になると考えられます。そのため、これらのPKIにおいても制度的に整合性をもったフレームワーク作りが望まれます。
- 本セッションでは、PKIに関連した団体の活動を紹介すると共に、パネルディスカションでは日本社会における信頼基盤の連携を確立するため、各団体でどのような連携をはかっていくか議論します。

【午前の部】のプログラム
「我が国における信頼基盤の連携に向けて」

- 我が国における信頼基盤の連携に向けて
  - 松本泰　セコム（株）IS研究所
- 電子認証局会議の活動
  - 高橋 章氏　日本電子認証（株）
- タイムビジネス協議会の活動
  - 市川 桂介氏　アマノビジネスソリューションズ（株）
- 電子記録応用基盤フォーラム（eRAP）の活動
  - 宮崎一哉氏　三菱電機(株)
- パネルディスカション

セコムIS研究所
Intelligent Systems Laboratory

（見直されつつある）
電子政府と個人情報保護法の話

・2001年頃の目標 「世界最先端電子政府を目指し、既存の手続きを100%電子化する」

・＃ボタンの掛け違いのまま、進んでいった？？？

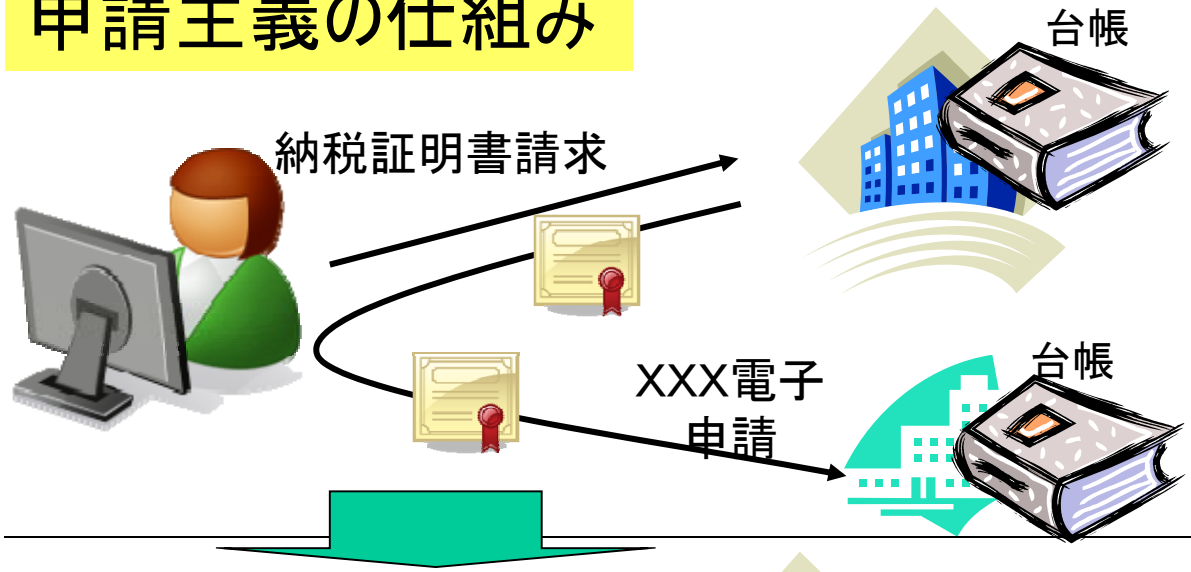
・＃そもそも目標を間違えていた？？？

・＃紙台帳の延長上の発想を、そのまま電子化した？？？

申請主義からプッシュ型のサービスへ

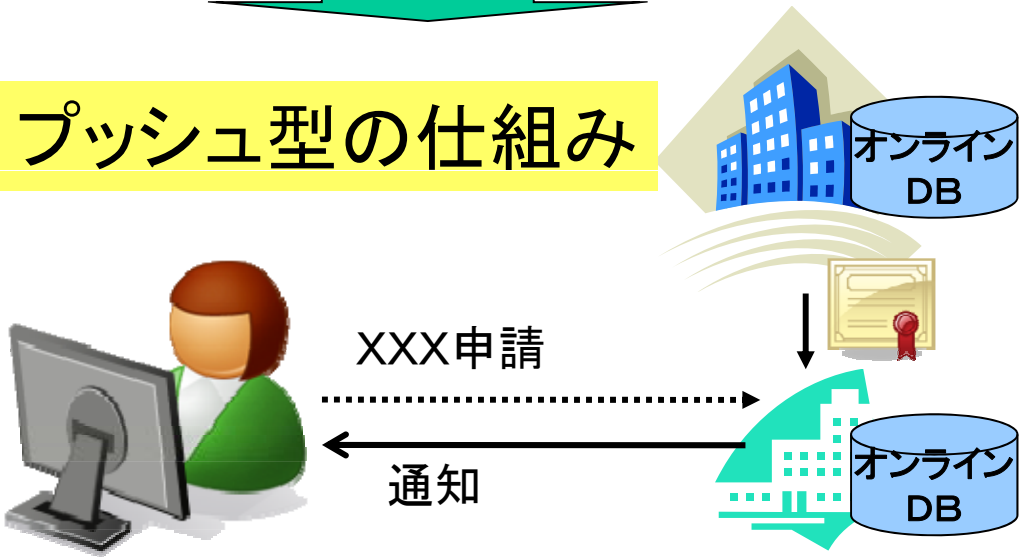
セコムIS研究所
Intelligent Systems Laboratory

申請主義の仕組み



- 「紙台帳」の延長上にある（その電子化）
- 明治（江戸）以来からの基本的な仕組み***
- 「識別」「認証」も個別組織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）

プッシュ型の仕組み



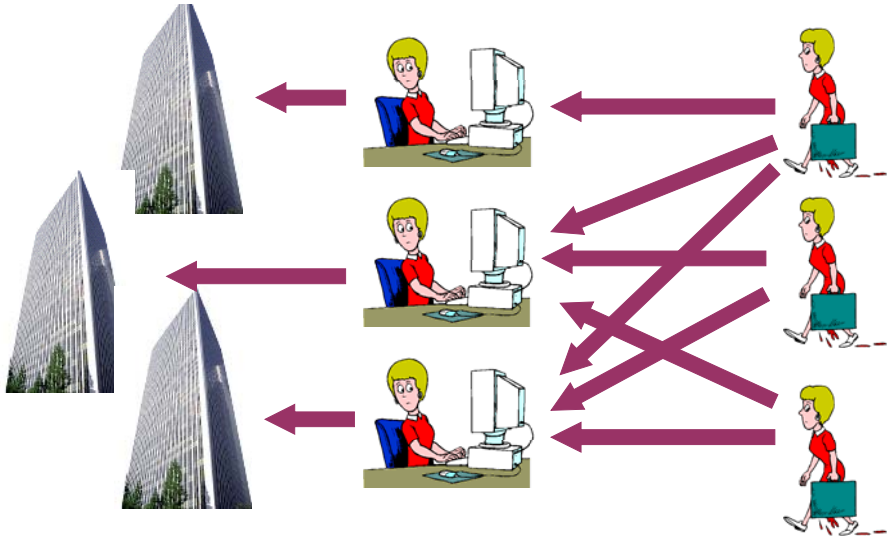
- 欧州の電子政府等では、行政のバックオフィスの連携ができなくてはならないというのが現在のトレンド
- 組織を超えた「一意識別」と「認証」

***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？

2001年頃の日本の電子政府の方針
（同時期のエストニアの電子政府の方針）

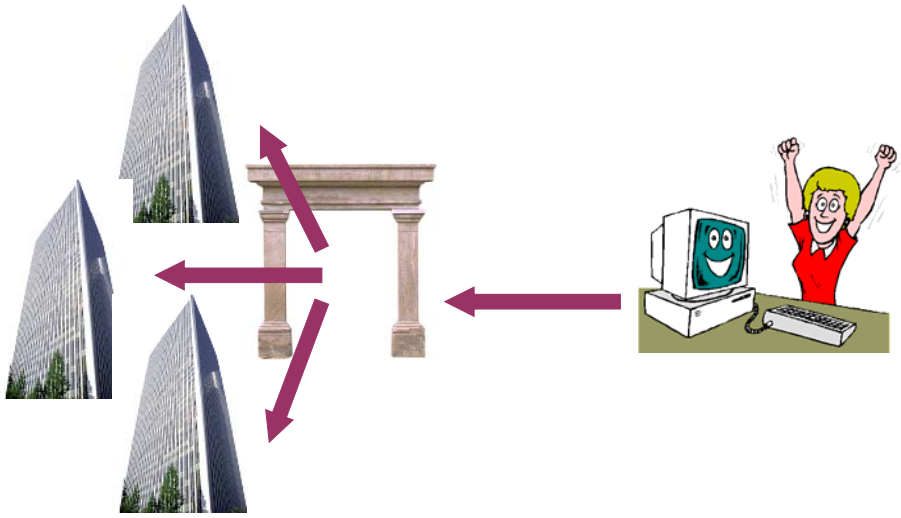
セコムIS研究所
Intelligent Systems Laboratory

日本



世界最先端電子政府を目指し、既存の手続きを100%電子化する

エストニア



制度と情報連携基盤を整備した上で電子政府のサービスを展開する

出典: **e-Government as customer http://cs.ioc.ee/excs/kickoff/heidelberg-slides.ppt**

マイナンバー法で必要とされている第3者機関についての1999年頃の議論

セコムIS研究所
Intelligent Systems Laboratory

- 我が国における個人情報保護システムの在り方について（中間報告）
- 平成11年11月
- 高度情報通信社会推進本部
- 個人情報保護検討部会
- http://www.kantei.go.jp/jp/it/privacy/991119tyukan.html
- ※1　監督機関について
- EUにおける「データ保護庁」のようなあらゆる分野を通じた規制権限を有する監督機関の創設は、一般多数の事業者に対する規制措置によって本来自由であるべき事業活動を大幅に制約することとなるなど、我が国の現状にかんがみると適切ではなく、また、**行政改革や規制緩和の流れにも反するところである**。
- また、EU各国においても、データ保護庁は、まだ十分に機能、定着していないとの指摘もあり、このようなことから、我が国においては、基本的方向として、これを代替し得る全体として実効性ある事後救済システムの構築等を目指すことがむしろ適切であると考えられる。

・2012年現在では、情報連携を円滑に進めるために「第3者機関」が必要という議論になっている。

個人情報保護法2000個問題：医療関連分野と適用法（例）

個人情報を取り扱う主体	適用法	監督官庁
厚生労働省	行政機関個人情報保護法	総務省
国立がん研究センター	独立行政法人等個人情報保護法	総務省
岩手県立○○病院	岩手県個人情報保護条例	岩手県
宮城県立△△病院	宮城県個人情報保護条例	宮城県
陸前高田市立□□病院	陸前高田市個人情報保護条例	陸前高田市
大船渡市立△△病院	大船渡市個人情報保護条例	大船渡市
医療福祉法人済生会	個人情報保護法	厚生労働省
鈴木内科医院	個人情報保護法	厚生労働省

マイナンバーシンポジウム資料 「プライバシーの権利と個人情報保護法」
新潟大学 大学院実務法学研究科・法学部 教授 鈴木 正朝
http://www.cas.go.jp/jp/seisaku/mynumber/symposium/iwate/siryou5.pdf

医療等分野の個人情報の「利活用（連携）」と「保護」を阻害するポリシ、制度の不整合？？

セコムIS研究所
Intelligent Systems Laboratory

日本の信頼基盤の現状

レガシーな紙台帳の延長上の発想を、
そのまま電子化した？？

2012年現在の状況？

？？？

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。。」

技術標準

ギャップ
噛み合わない会話
共有されないビジョン

・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

現実の実務からの乖離という問題

「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」、etc…

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

信頼基盤に関連する(連携が出来ない？)法制度

セコムIS研究所

信頼基盤、認証局	所管、制度等、法的根拠、備考	信頼点・信頼モデル
政府認証基盤	総務省行政管理局、官職証明書	GPKI
地方公共団体 組織認証基盤	総務省自治行政局、職責証明書	GPKI相互認証
公的個人認証サービス	総務省自治行政局 マイナンバー法案での認証用証明書	GPKI相互認証
電子認証登記所	法務省、法人向けの証明書	GPKI相互認証
電子署名法の認定認証局	経済産業省、総務省、法務省 自然人向けの証明書、印鑑登録 民事訴訟法228条2項	GPKI相互認証
電子公証人	法務省、電子公証制度 確定日付	GPKI相互認証
保険医療福祉分野の公開鍵基盤(ＨＰＫＩ)	厚生労働省 タイムスタンプへの要求 認証用証明書	GPKI、電子署名法認定認証局と無関係
時刻証明(のためのPKI)	データ通信協会（総務省） e文書法のガイドライン等	-規定なし？
ＳＳＬ証明書、EV証明書、コード署名等	（世界的な）民間の枠組み Web Trust for CA, ETSI	民間,ブラウザの証明書リスト等

「信頼基盤」と「個人情報保護法」の共通点？？

セコムIS研究所
Intelligent Systems Laboratory

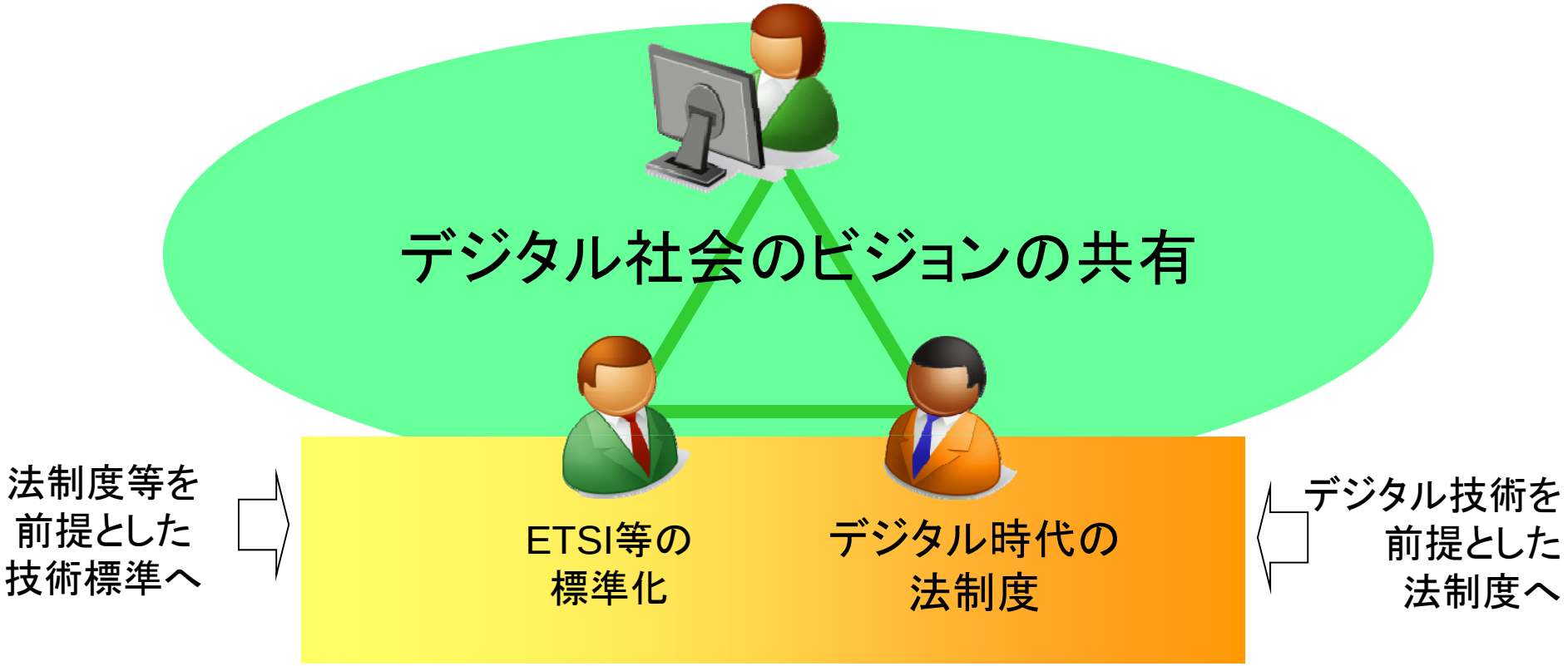
- 現在の法律の成立時期
  - （目標を間違えていた？？）世界最先端電子政府が検討されていた2000年前後に検討された頃に、法律（個人情報保護法、電子署名法）が成立
- 現在の制度は、欧州の制度と米国の制度の折衷案？
  - 欧州 vs. 米国
  - 日本における制度の立ち位置は？
- 現時点での状況　– 連携のためのポリシ不整合？？
  - 制度間、管轄官庁間の不整合？？
  - 制度と技術の成り立たない会話？？
  - 日本と世界の不整合？？
    - 個人情報保護法であれば、データの越境問題

セコムIS研究所
Intelligent Systems Laboratory

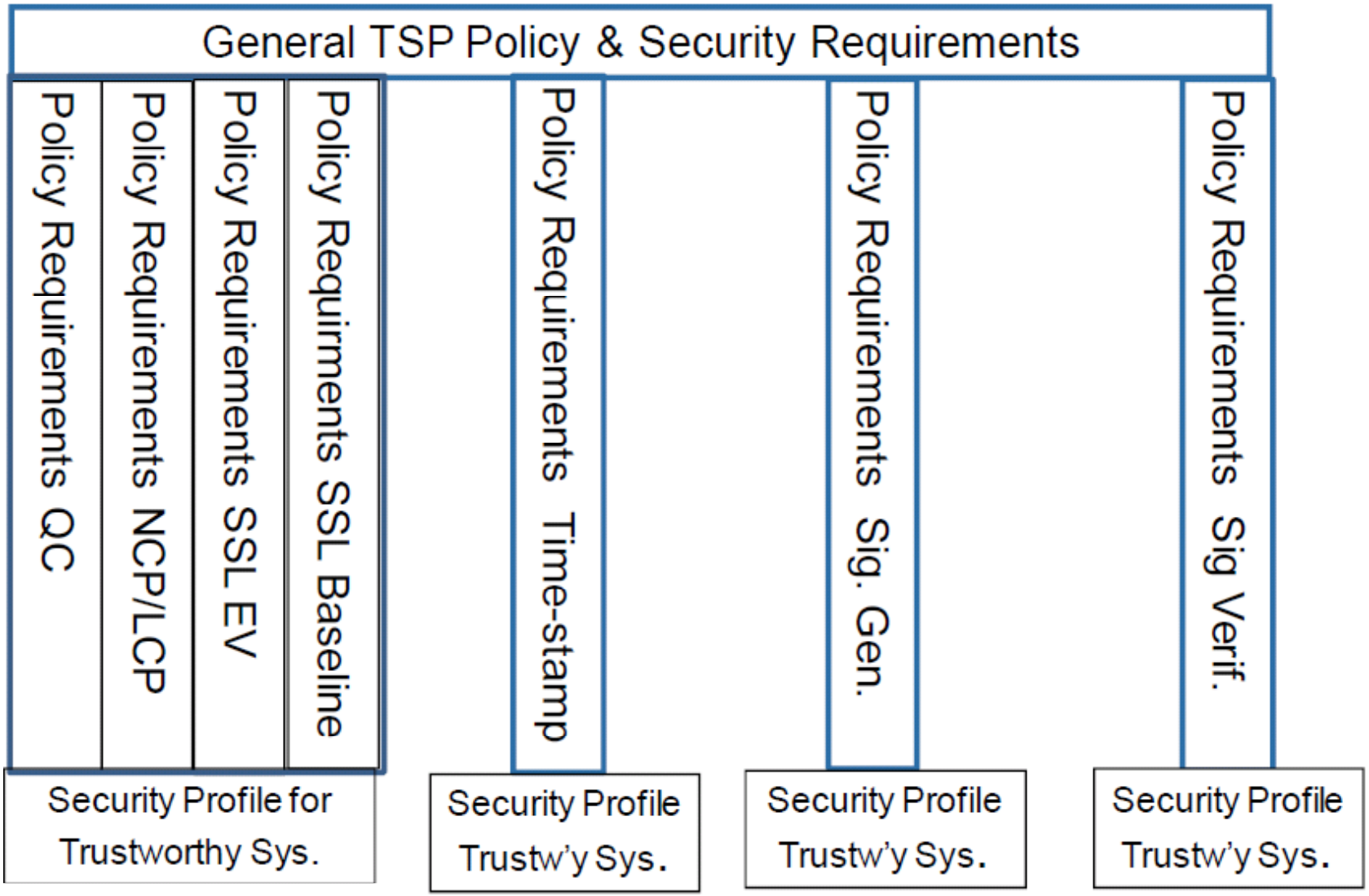
欧州における方向性

欧州におけるプライバシ保護指令の見直しと同じく、欧州各国の不整合、制度間の不整合を解消する方向で議論がなされている。

標準化と法制度の関係
欧州のアプローチ?



欧州（ETSI)における信頼基盤の標準化動向
ポリシーの整合へ – これは欧州のデータ保護法も同様



出展 : http://docbox.etsi.org/workshop/2012/201201_CA_DAY/3_POPE__ETSi-CA-Day24Jan2012-TSP-Conf-Ass-NickPope.pdf

TSP: Trusted Services Provider

エストニアの信頼基盤の信頼関係モデル

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

EE Certification Centre Root CA

・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-2011
エストニア
IDカード向け

EID-2011
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

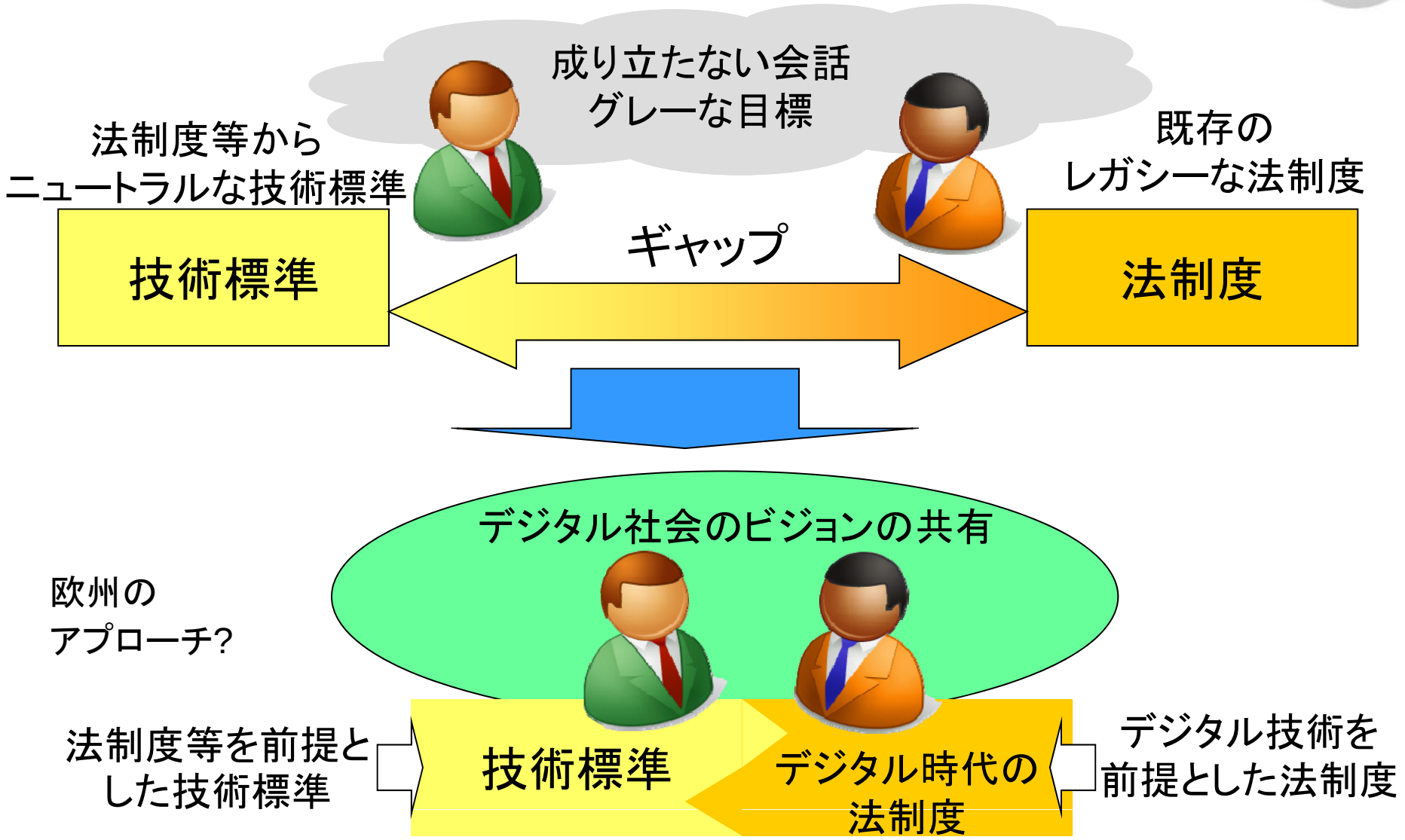
セコムIS研究所
Intelligent Systems Laboratory

議論したいこと

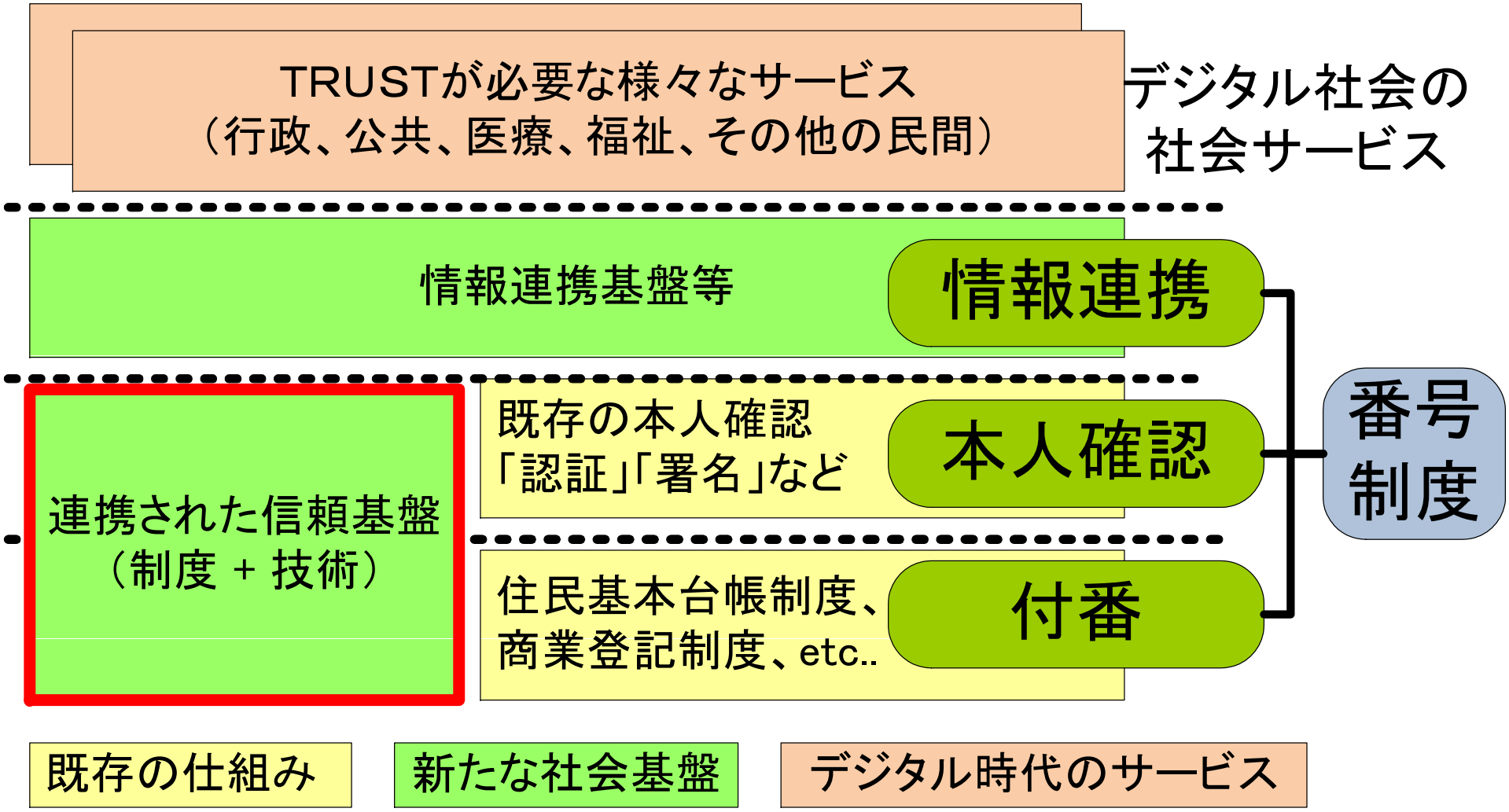
- 制度と技術の不整合
- 制度間の不整合
- 日本と海外の不整合
- これらの解消へのアプローチ

技術と制度をかみ合わせるためには

セコム IS 研究所
Intelligent Systems Laboratory



番号制度との関係は、どうあるべきか
番号制度の理解・松本の理解（拡大解釈？



デジタル時代のビジョンの共有は可能か？

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 が必要な様々なサービス（行政、民間）

デジタル時代の
社会基盤

連携された様々な信頼基盤

デジタル時代の
（信頼のための）
フレームワーク

デジタル社会を
支える技術

デジタル時代の
法制度

デジタル時代のビジョンの共有

セコムIS研究所
Intelligent Systems Laboratory

パネルディスカション

我が国における信頼基盤の連携に向けて

セコムIS研究所
Intelligent Systems Laboratory

【午前の部】
「我が国における信頼基盤の連携に向けて」

- モデレータ
  - 松本泰　セコム（株）IS研究所
- パネリスト
  - 高橋 章氏　日本電子認証（株）
  - 市川 桂介氏　アマノビジネスソリューションズ（株）
  - 宮崎一哉氏　三菱電機(株)
  - 秋山卓司　クロストラスト（株）
  - 宮内宏　宮内宏法律事務所

セコムIS研究所
Intelligent Systems Laboratory

論点案

- 論点1
  - 「電子署名法」「タイムスタンプ」「認証」
- 論点2
  - 信頼点、信頼リストの在り方

論点1
「電子署名」「タイムスタンプ」「認証」

セコム IS 研究所
Intelligent Systems Laboratory

- 欧州では、「タイムスタンプ」と「電子署名法」の関係が同一内の法律である国が多い。また、認証も統合される方向で議論されている。
- 技術的観点からは、電子署名」「タイムスタンプ」「認証」は、一貫性を保ち、連携、統合、されるべきだが、、
- 日本においては、紙前提の従来からの制度上の延長上以上の発想はない。また、管轄官庁の壁がある？？？
- 関連して　技術では決められない様々な不整合？
  - 証明する内容（名前）等の問題
    - 外字、英字表記　－ これらが、制度毎の個別対応
  - 世界との整合　　英表記、法人の証明
  - 「確定日付」とタイムスタンプ
- 番号制度の影響　　マイナンバー、法人番号

セコムIS研究所
Intelligent Systems Laboratory

論点2
信頼点、信頼リストの在り方

- 「相互運用性」だけでなく「相互信頼性」？？
- 監査の在り方
  - 制度毎？？
- CA/BF等での議論
- 欧州のTSL（Trust-service Status List）
- 日本と世界

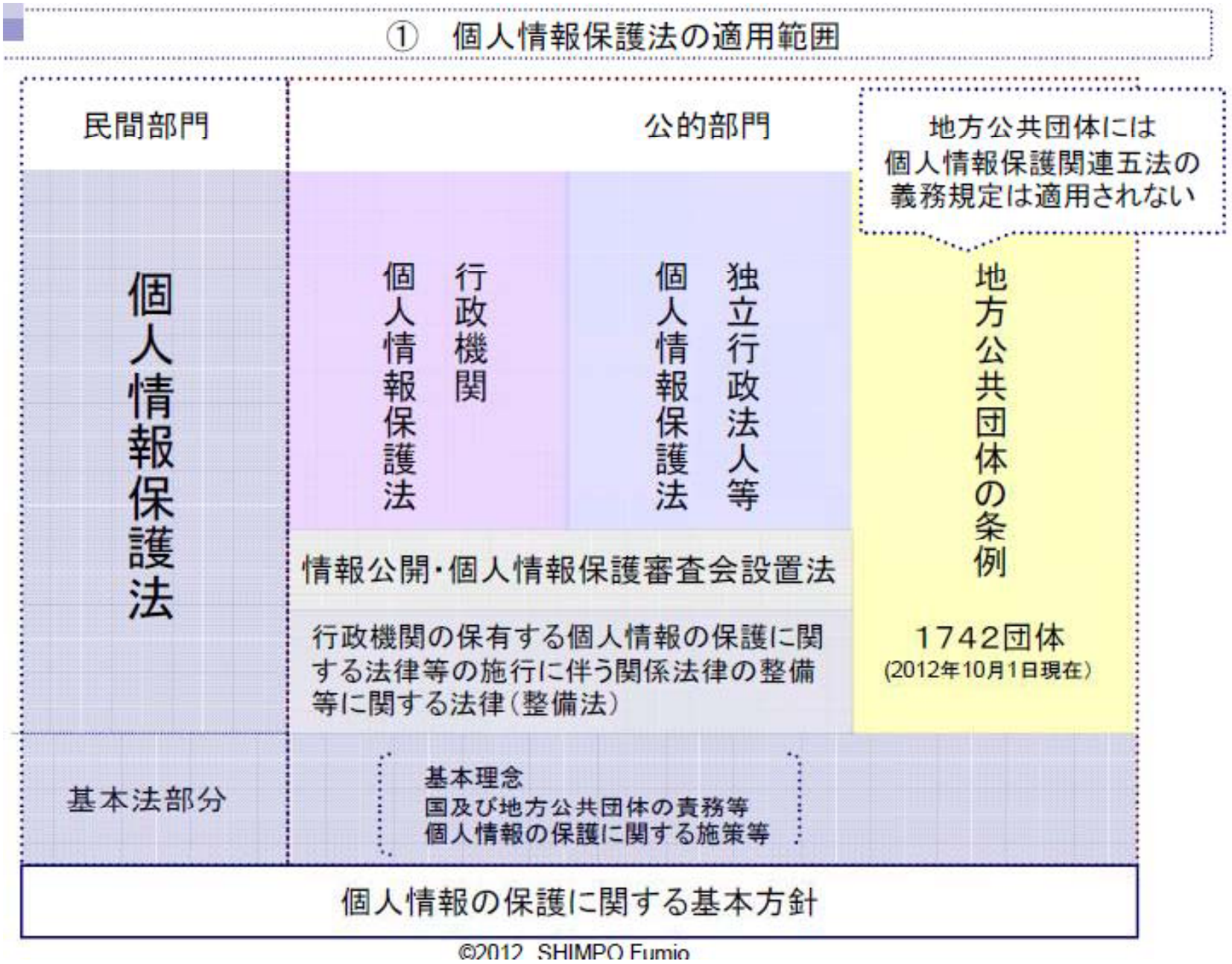
セコムIS研究所
Intelligent Systems Laboratory

Backup Slide

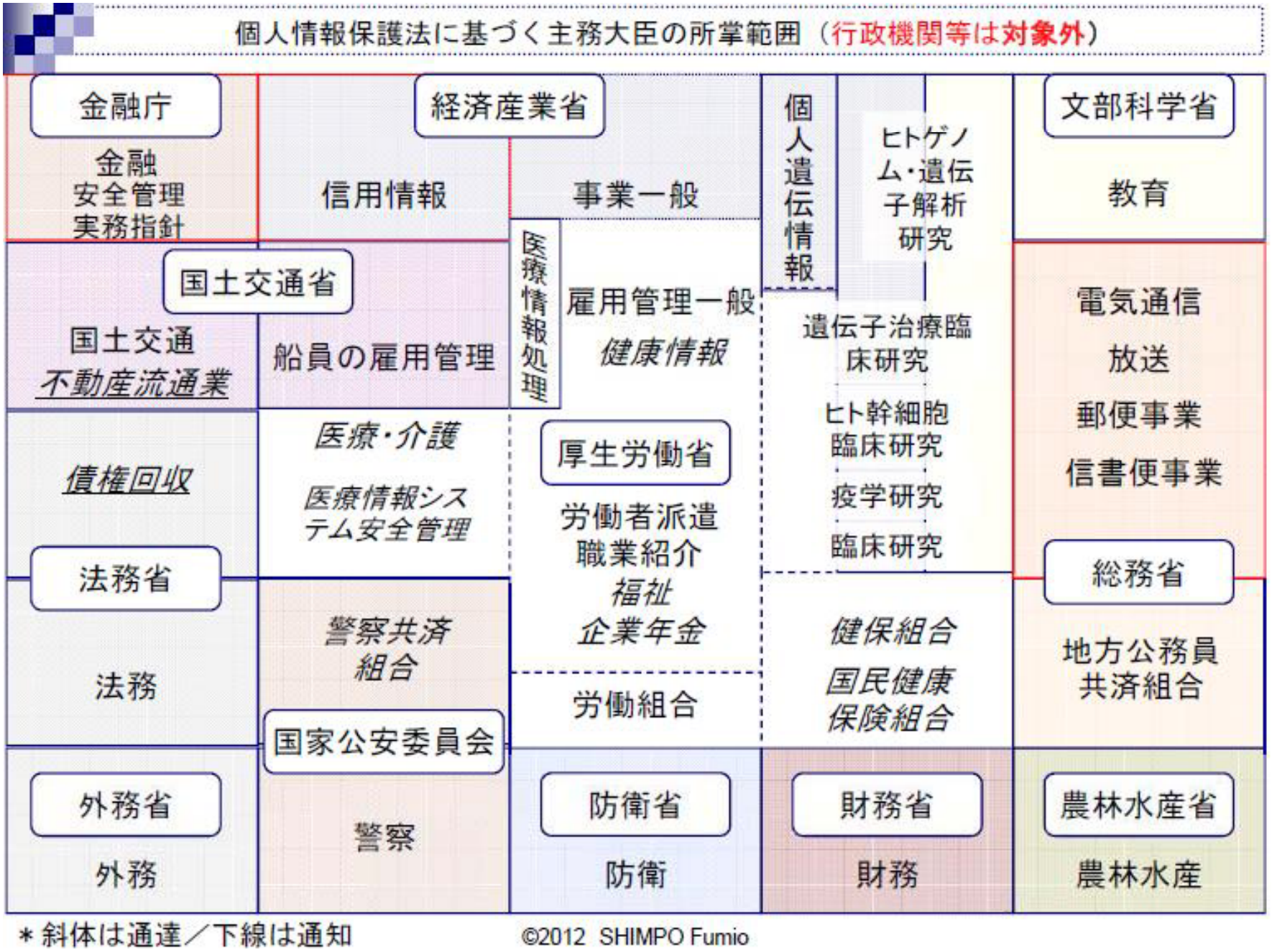
セコムIS研究所
Intelligent Systems Laboratory

個人情報保護法の話

個人情報の「利活用（連携）」と「保護」を
阻害するポリシ、制度の不整合？？



「日本の個人情報保護法は世界に通用するか？」慶応義塾大学総合政策学部 准教授　新保 史生
http://www.horibemasao.org/horibe_07/5.Prof.Sinpo_07.pdf



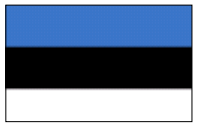
「日本の個人情報保護法は世界に通用するか？」慶応義塾大学総合政策学部 准教授　新保 史生
http://www.horibemasao.org/horibe_07/5.Prof.Sinpo_07.pdf

セコムIS研究所
Intelligent Systems Laboratory

「電子政府の話」参考

海外におけるプッシュ型の行政サービスへの流れ

セコムIS研究所
Intelligent Systems Laboratory



エストニアのX-Road（データ交換システム）

•エストニアでは、電子データ交換レイヤーX－roadで出産時に病院が出生届を行政に送付して、母親（父親）が何もしなくても児童手当や出産給付金が銀行口座に振り込まれる。

出展　特別テーマ評価検討委員会（平成20年度 第2回）　井堀構成員提出資料「井堀構成員メモ」より

http://www.kantei.go.jp/jp/singi/it2/tokubetu/kaisai_h20/dai2/siryou3-1.pdf

エストニアにおいて、X－roadの整備は2001年頃に決定されたらしい。

韓国の電子政府法

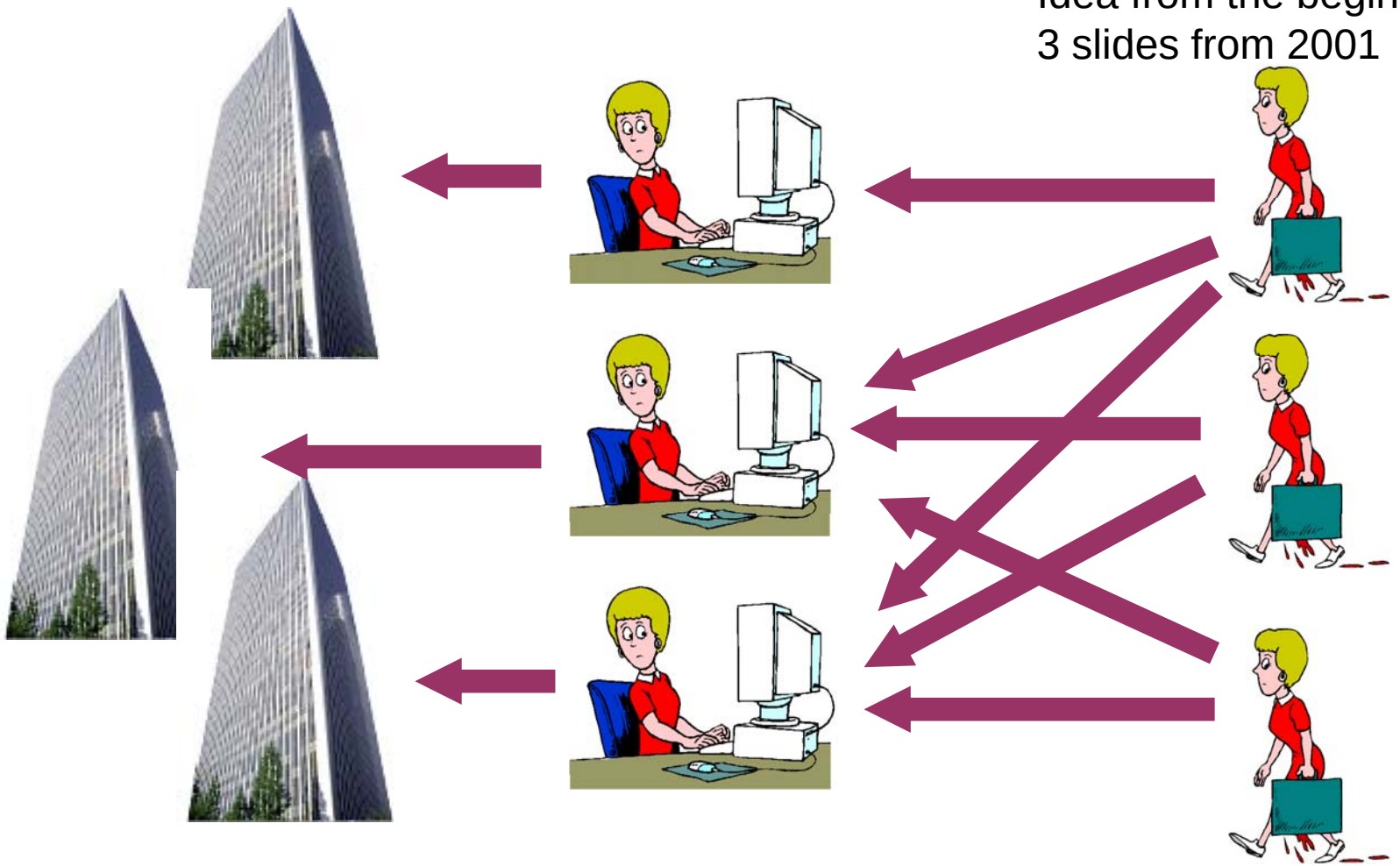
・「行政機関は特別な理由がある場合を除き、行政機関の間で電子的に確認できる事項を国民に証明書など提出させることをさせてはならない（電子政府法2条）」

似た主旨の法制度は、欧州の多くの国々で制定されつつある

エストニアの電子政府

Complexity transformations 1.

Idea from the beginning
3 slides from 2001



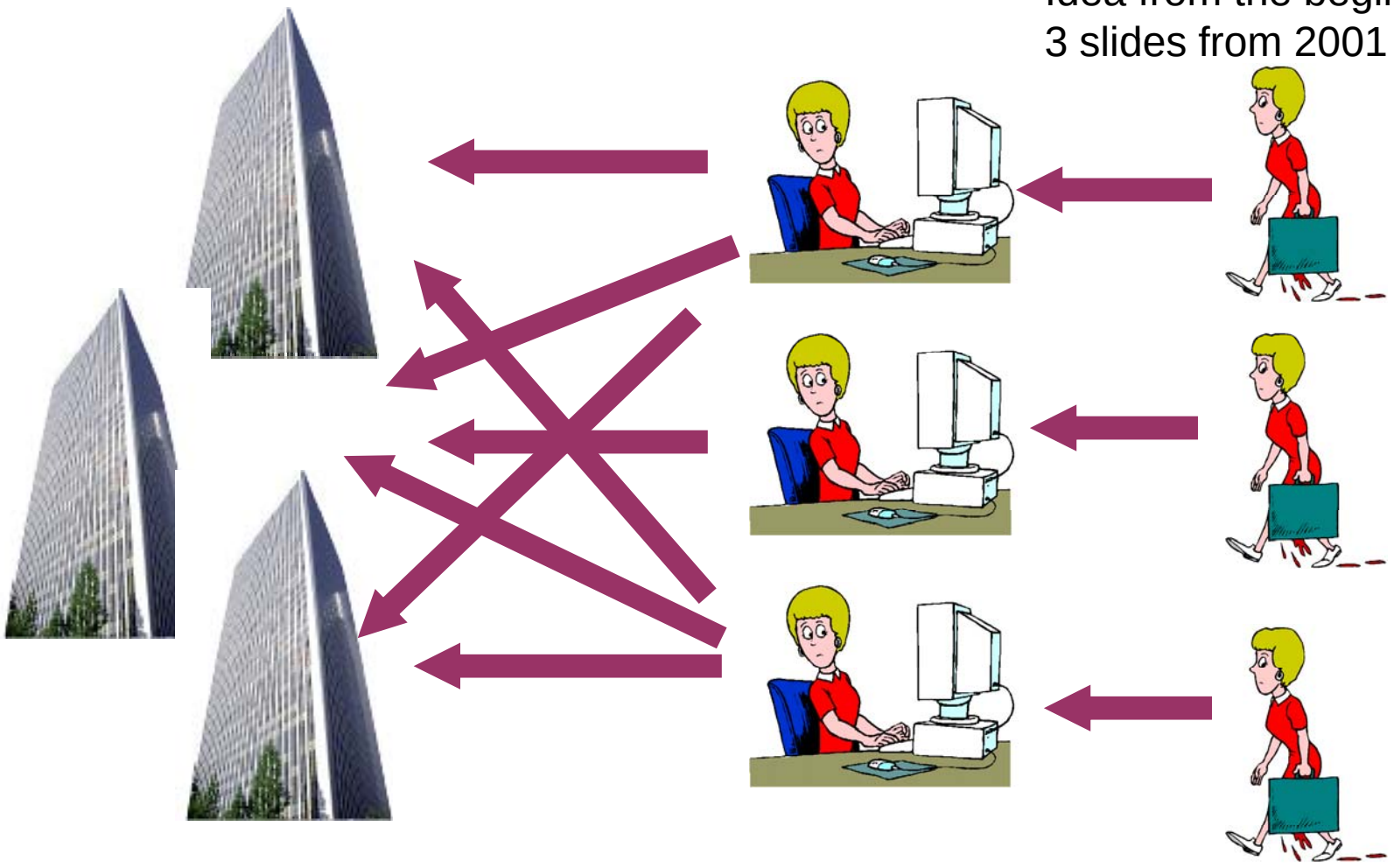
出典: **e-Government as customer http://cs.ioc.ee/excs/kickoff/heidelberg-slides.ppt**

エストニアの電子政府

Complexity transformations 2.

セコムIS研究所
Intelligent Systems Laboratory

Idea from the beginning
3 slides from 2001

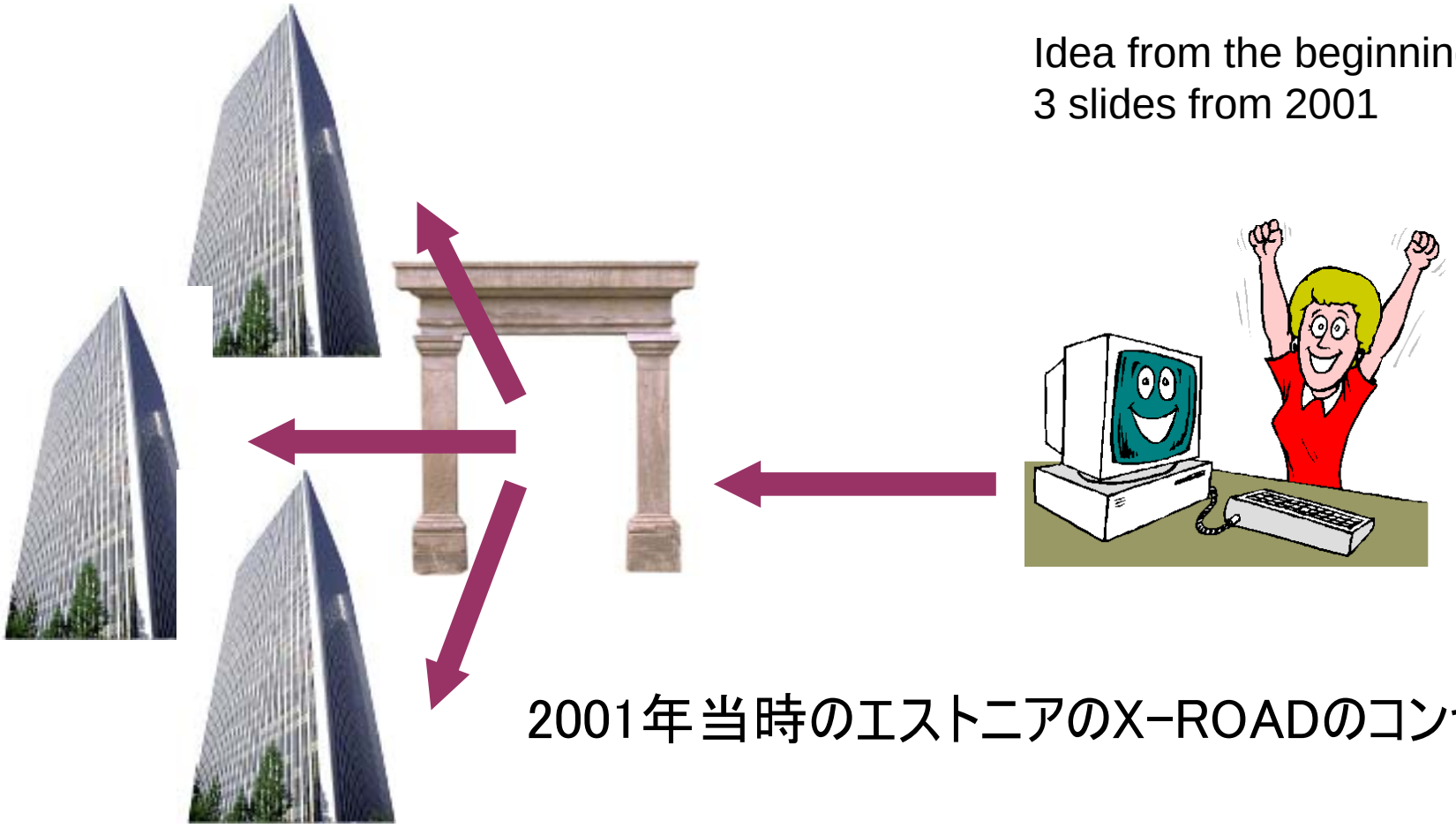


出典: **e-Government as customer http://cs.ioc.ee/excs/kickoff/heidelberg-slides.ppt**

エストニアの電子政府
Complexity transformations 3.

セコムIS研究所
Intelligent Systems Laboratory

Idea from the beginning
3 slides from 2001



2001年当時のエストニアのX-ROADのコンセプト

「行政中心のサービスではない国民中心の行政サービス」

出典: **e-Government as customer http://cs.ioc.ee/excs/kickoff/heidelberg-slides.ppt**

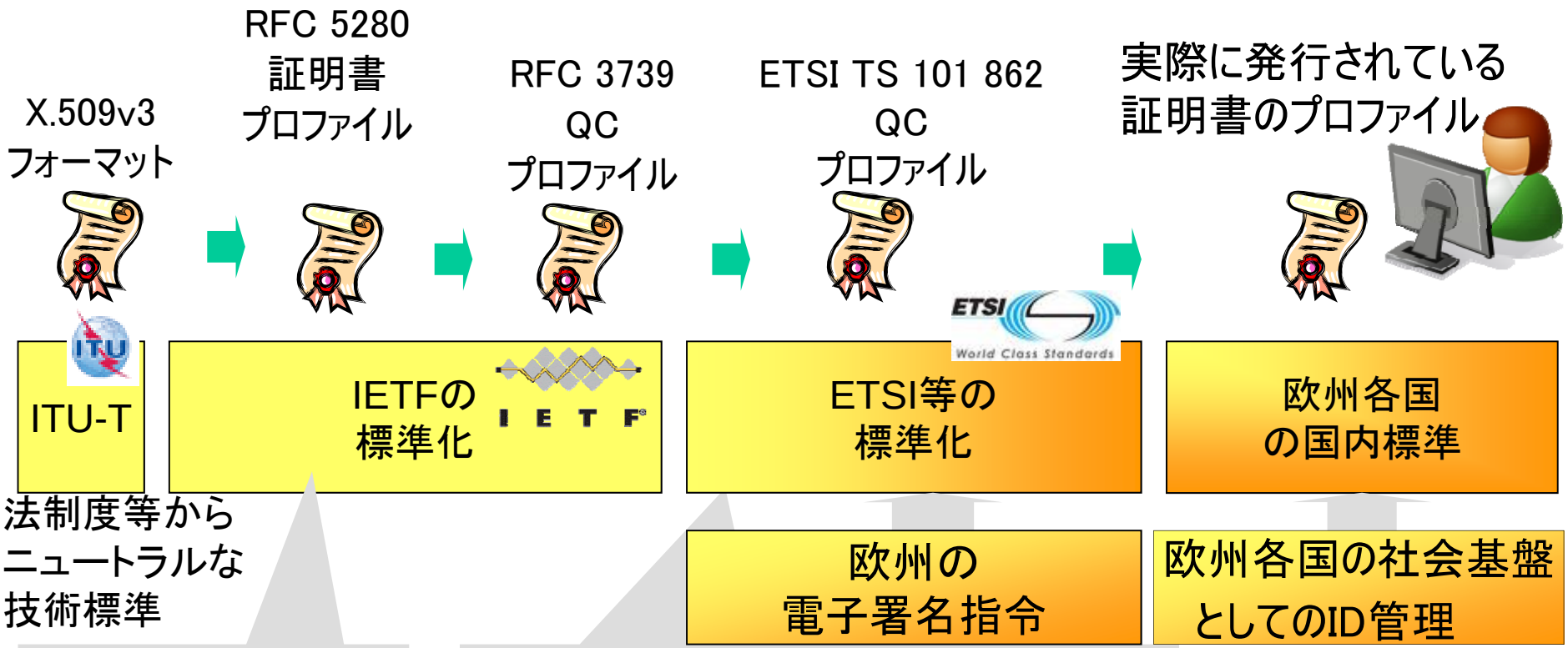
セコムIS研究所
Intelligent Systems Laboratory

その他の参考スライド

番号制度とPKI – 標準化と法制度の関係

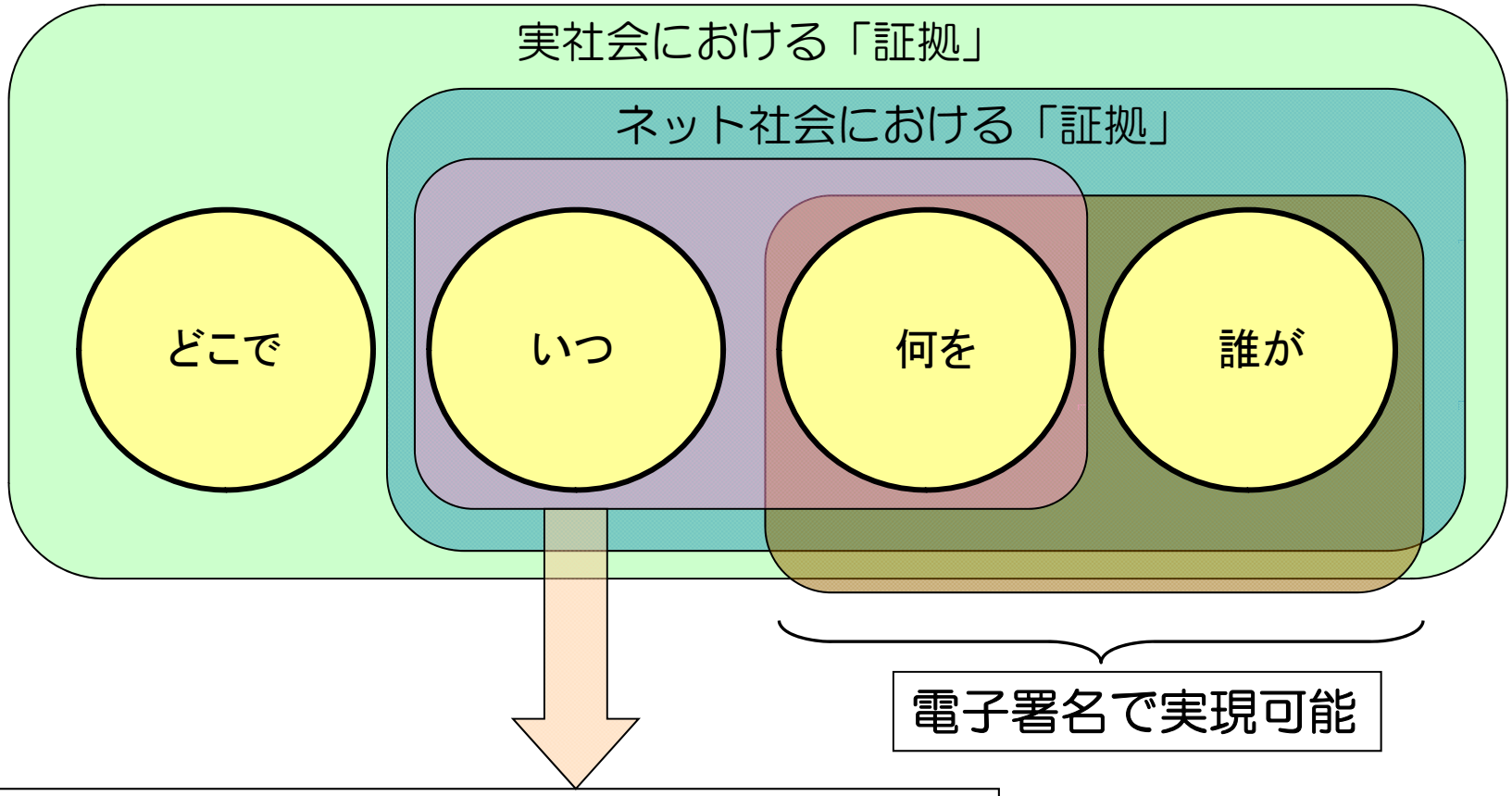
クォリファイされたアイデンティティを証明するための証明書

セコム IS 研究所
Intelligent Systems Laboratory



Trustのためのフレームワーク

タイムスタンプと電子署名



■これらを実現するのが「タイムスタンプ」
- ーある時刻にその文書が存在していた（存在証明）
- ーその文書は改ざんされていない（完全性証明）

「署名」「認証」の課題

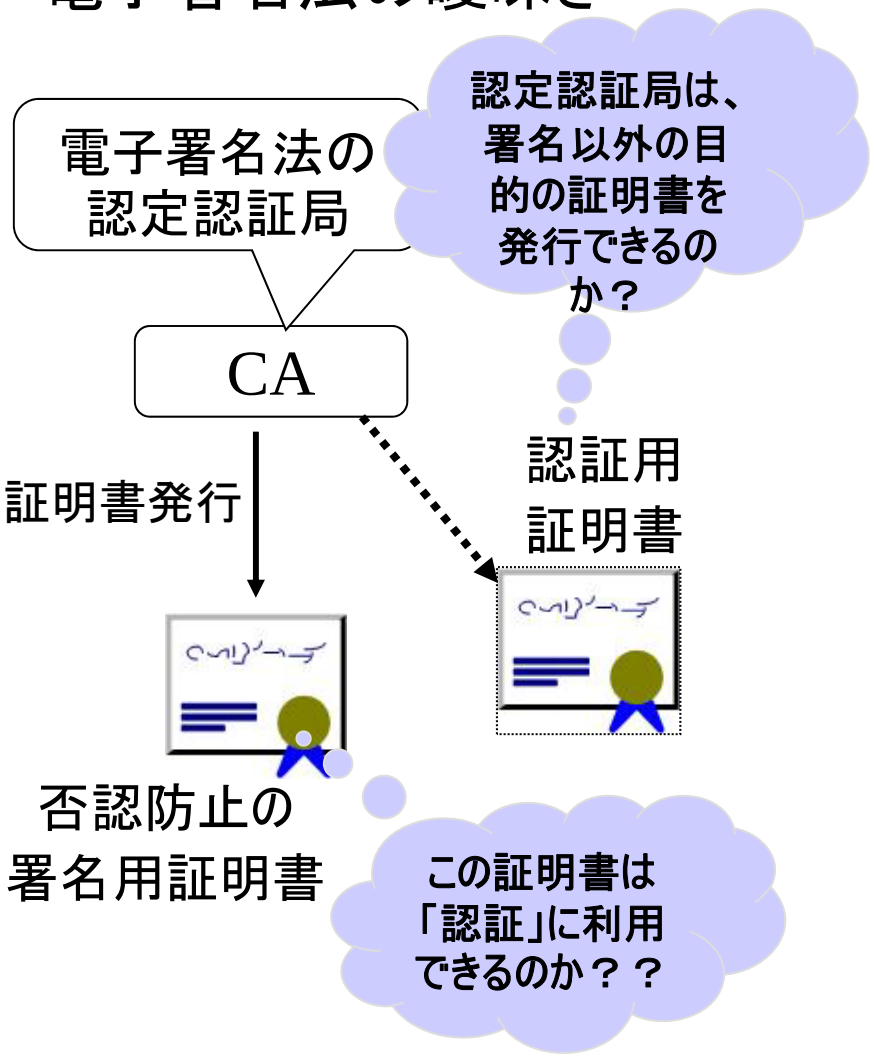
セコムIS研究所
Intelligent Systems Laboratory

- 「電子署名」に対する理解のギャップ
  - 法的な効力を持った「電子署名」のネイミング
    - 欧州では「クォリファイド署名」
    - 韓国では「公認署名」
    - 日本では？
      - 「電子署名法の特定認証業務認定認証局が発行する証明書を利用した電子署名」
- 行政手続きと電子署名に関連した法制度との関係の整理
  - 申請に関しては、「電子文書の法的根拠」と「適切な手段」との関係は、再度整理される必要がある（と思う）。
- 「認証」
  - 「認証」であっても、行政サービスに利用されるためには、「（自然人の）法的なアイデンティティ」と、この「法的なアイデンティティ」と結び付いた「オンラインで利用できるクレデンシャル」が必要
    - 行政サービスは、お金さえ払えば、匿名で受けられる民間サービスとは違う
  - これには、制度的なフレームワークも必要かもしれないが、現状何もないし、議論もされていない。

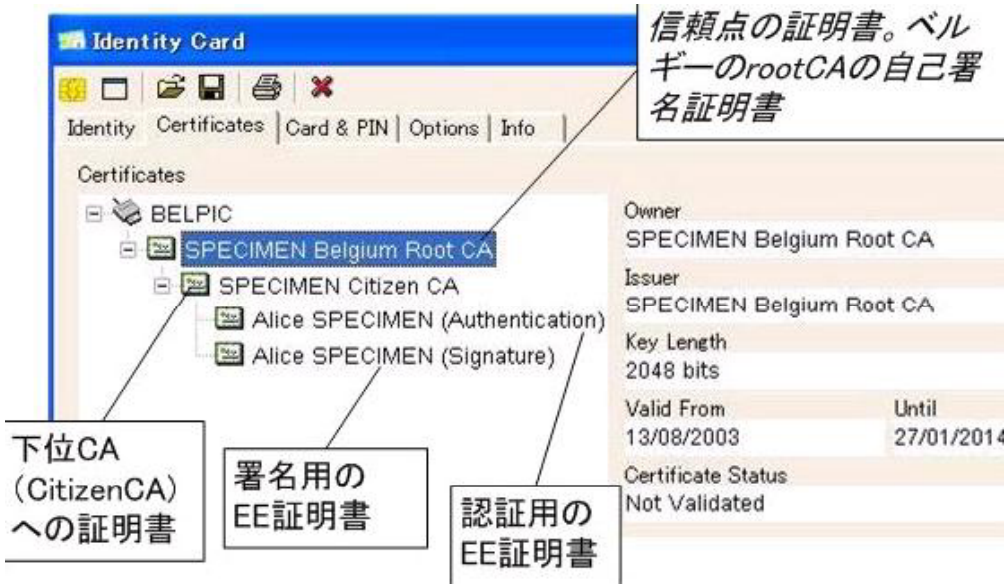
「認証」と「署名」に関する証明書の問題

セコムIS研究所
Intelligent Systems Laboratory

電子署名法の曖昧さ



欧州の典型例



- 「署名用」と「認証用」の証明書を分けている。
- 同じ認証局から「署名用」と「認証用」の証明書を発行している。

「電子署名法」と「認証」の関係
電子政府で利用する証明書(署名方式)の制約

セコムIS研究所 Intelligent Systems Laboratory

- 電子署名法の**特定認証業務の認定**からくる制約(GPKIの相互接続基準からくる制約)
  - (1) 技術基準(暗号アルゴリズムなど)
    - RSA 1024bit with SHA-1 など　今後、RSA 2048bit SHA-256へ
    - 署名方式の制約(　サーバ署名、ローミング鍵等が使えないなどの制約　)
  - (2) 運用基準(　たとえば、「本人確認」「発行管理」など　)
    - 証明書取得などにおけるユーザ負担(ユーザビリティとの関係)
  - (3)「誤認防止」条項からくる証明書発行の制約　-> 曖昧？？
    - 署名用証明書が「認証」「暗号」で利用できるのか？
      - 利用出来るとすると「否認防止」の意味が曖昧になる
    - 認証用証明書、暗号用証明書が発行できるのか？
      - 発行できるとすると「誤認防止」の考え方を明確にする必要がある。
- GPKIとの相互接続からくる制約　(　相互運用性を確保するための制約　)
  - 電子政府全体の相互運用性を確保するための「証明書プロファイル」が存在する。この仕様による制約がある。
  - GPKIでは、基本的に「否認防止用の証明書」のプロファイルしか規定していない。 -> 証明書を「認証Authentication」で使うことの問題

目指すべきセキュリティ基盤の考え

セコムIS研究所
Intelligent Systems Laboratory

- セキュリティの視点だけ追及してきたこと自体が、逆にセキュリティの高い電子署名・電子認証が基盤として機能しない原因を作っている？
- 広く展開され、そして利用されて初めてセキュリティの「基盤」としての意味をなす。
- 電子政府は、効率的で競争力のあるデジタル社会全体のために適切なセキュリティレベルの電子署名・電子認証の定着を牽引する必要がある。