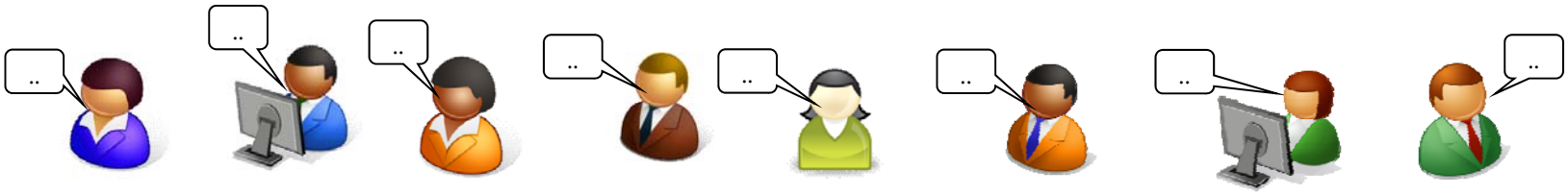
デジタル社会のための電子署名を見直す

2014年3月13日

セコム（株）ＩＳ研究所　松本　泰



Copyright © 2014 SECOM Co., Ltd. All rights reserved.

デジタル社会のための電子署名を見直す

セコムIS研究所
Intelligent Systems Laboratory

- デジタル社会のための制度見直し
  - 個人情報法の改正に向けた動向
    - 「パーソナルデータの利活用に関する制度見直し方針」
  - 欧州における「電子署名指令(1999年）」の見直し
    - 「指令(Directive)」から「規則(Regulation)」へ
    - 「信頼サービス」全般のための制度へ
  - 成立した「番号法」
    - 紙前提の制度からの脱却等？？
    - 「識別」の見直し
- それでは、日本の「電子署名法」は？
- 論点（パネルのお題目）
- 参考（過去のPKI day でのスライド）

Copyright © 2014 SECOM Co., Ltd. All rights reserved.

デジタル社会のための制度の見直し

紙文書の（延長上の）電子化のための制度から脱却

・個人情報法の改正に向けた動向
・欧州における電子署名指令(1999年)見直し
・成立した「番号法」
・＃それでは、「電子署名法」は？

Copyright © 2014 SECOM Co., Ltd. All rights reserved.

個人情報法の改正に向けた動向
改正を示唆している理由

セコムIS研究所
Intelligent Systems Laboratory

- 日本の成長戦略のため
  - パーソナルデータの利活用等
- インターネット等の環境の大きな変化に対応
  - ネット上の情報等を介した意図せぬ名寄せ等
- グローバル対応（国際間の整合等）
  - 欧州のデータ保護法の（指令から規則への）影響が大きい
  - データ移転に関する国際的な整合へ
- 国内の分野別のガイドライン、自治体毎の個人保護条例の違い等による情報連携の阻害
  - 個別最適から全体最適への流れ？
  - 欧州における指令(Directive ）（データ保護指令、電子署名指令）から加盟各国への拘束力のある「規則(Regulation)」への動きに近い
    - 拘束力のない法制度は、相互運用性を確保の阻害要因になる

それでは、日本の「電子署名法」は？

ECOM Co., Ltd. All rights reserved.

欧州における電子署名指令（1999年）見直し

- 見直しのトリガーないし理由？？
  - 欧州デジタル・アジェンダ－欧州における成長戦略
    - Key Action 3
      - Propose a revision of the eSignature Directive with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems
    - Key Action 16
      - Propose a Council and Parliament Decision to ensure mutual recognition of e-identification and e-authentication across the EU based on online 'authentication services' to be offered in all Member States

本当は、欧州の成長戦略と、このKey Action の関係、理由、背景等の理解が必要

Copyright © 2014 SECOM Co., Ltd. All rights reserved.

欧州における電子署名指令（1999年）見直し

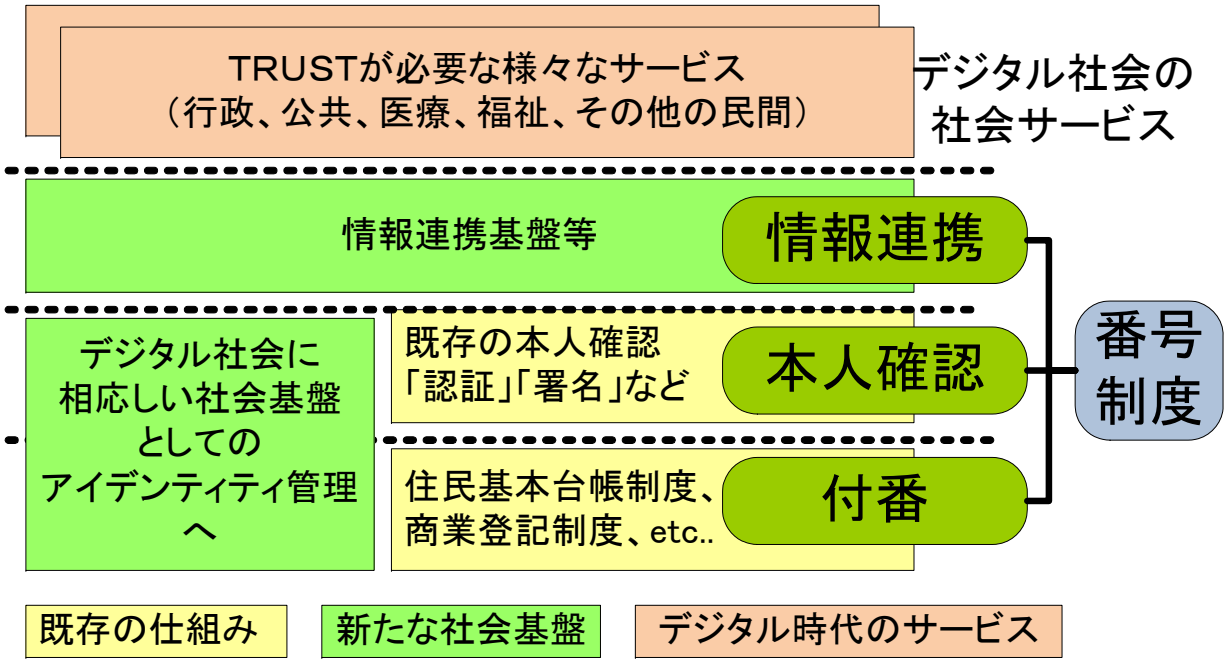
- 見直しの案
  - Proposal for a regulation on electronic identification and trust services for electronic transactions in the internal market.
  - 2012年6月 EU 委員会がアクセプト
- 「指令(Directive)」から「規則(Regulation)」へ
  - 加盟各国への拘束力を強め、相互運用性の確保、信頼レベルの整合を図る？？
  - ＃これは、欧州のデータ保護法も同じ（指令->規則）
- 「電子署名」だけでなく、様々な「信頼サービス」における信頼の確立ための制度へ
  - (1) Electronic Signature、(2) Electronic Seals 、(3) Electronic time stamp 、(4) Electronic documents 、(5) Qualified Electronic delivery 、(6) Website authentication

それでは、日本の「電子署名法」は？

ECOM Co., Ltd. All rights reserved.

2013年に成立した番号法

- 番号制度を構成する３つの仕組み
  - 「付番」「本人確認」「情報連携」
  - 申請主義の行政サービスからプッシュ型の行政サービスへ
    - ・紙台帳の仕組みを引きずった制度からの脱却
      - 紙台帳の電子化の発想からの脱却
    - ・そのための識別の見直しを行った制度？



e-Signature
以前に
e-identification
が必要

Copyright © 2014 SECOM Co., Ltd. All rights reserved.

それでは、日本の「電子署名法」は？

・日本の成長戦略？？
・インターネット等の環境の大きな変化？？
・グローバル対応（国際間の整合等）？？
・分野別の弊害？？
・これらと現状の「電子署名法」との関係は？？

Copyright © 2014 SECOM Co., Ltd. All rights reserved.

それでは、日本の「電子署名法」は？ これまでの経緯等

セコムIS研究所 Intelligent Systems Laboratory

- 2001年4月１日施行
- 「電子署名及び認証業務に関する法律」
- 「特定認証業務の認定」制度を含んでいる
  - 欧州における適格サービスプロバイダー（ qualified service provider）の認定に近いが。。
    - 欧州では、適格サービスプロバイダー（信頼サービスプロバイダー）の範囲が拡大している。
- 影響を受けた海外の制度
  - やはり欧州の「電子署名指令(1999年）」
    - 現在、この大きな影響を受けた欧州の「電子署名指令」自体が大きく改正（指令から規則へ）されようとしている。
- 国内の既存の法律との関係
  - 民事訴訟法228条の電子データへの拡大
  - 物理的な印鑑証明の代替以上のことは何も考えられていない？？

Copyright © 2014 SECOM Co., Ltd. All rights reserved.

それでは、日本の「電子署名法」は？番号制度との関係

セコムIS研究所
Intelligent Systems Laboratory

- 個人番号、個人番号カード、法人番号
- 電子署名法とは別の（電子署名に関する）法律の改正
  - 行政手続における特定の個人を識別するための番号の利用等に関する法律の 施行に伴う関係法律の整備等に関する法律
    - 電子署名に係る地方公共団体の認証業務に関する法律の一 部を改正
  - 個人番号カードに格納する証明書
    - 従来からの「電子署名用証明書」
    - 追加された「利用者証明用電子証明書」

・「電子署名法」以外は、世の中の要求に従って法律も改正されつつある。
・しかし分野毎の改正は、将来、全体最適を阻害する可能性がある。こうした動きは、欧州における指令から規則へとは逆の流れになってはいないか？？

Copyright © 2014 SECOM Co., Ltd. All rights reserved.

日本の「電子署名法」　現状の疑問

セコムIS研究所
Intelligent Systems Laboratory

- 非常にニッチなビジネス領域
  - 2001年当時、高いセキュリティレベルのみを目指した
    - 高いセキュリティレベルを目指す程にニッチなビジネスになっていくという罠にはまった？？
  - ＃結果「日本の成長戦略」に寄与しているとはとても言えない状況を作り出している
- –トラストサービスに関連する（連携が出来ない？）法制度
  - トラストサービスの範囲が狭義の電子署名に閉じている
  - 官民別々の法制度（現状の個人情報保護法と似ている）
  - 拘束力がないため分野毎にバラける傾向にある？
- 既存のレガシーな法制度の延長上
  - 民事訴訟法228条からの紙前提の制度の電子化？
    - 既存の紙前提の様々な法制度の延長が、デジタルデータのためのトラストの「連携」「統合」を阻害している？？
- 「識別」の考え方が、紙台帳の延長上にあり曖昧性を含んでいる
  - 番号制度以前の紙台帳の延長上の名前、住所等、法人の扱い。そのために横断的な連携を困難にしている？

Copyright © 2014 SECOM Co., Ltd. All rights reserved.

論点？

Copyright © 2014 SECOM Co., Ltd. All rights reserved.

論点

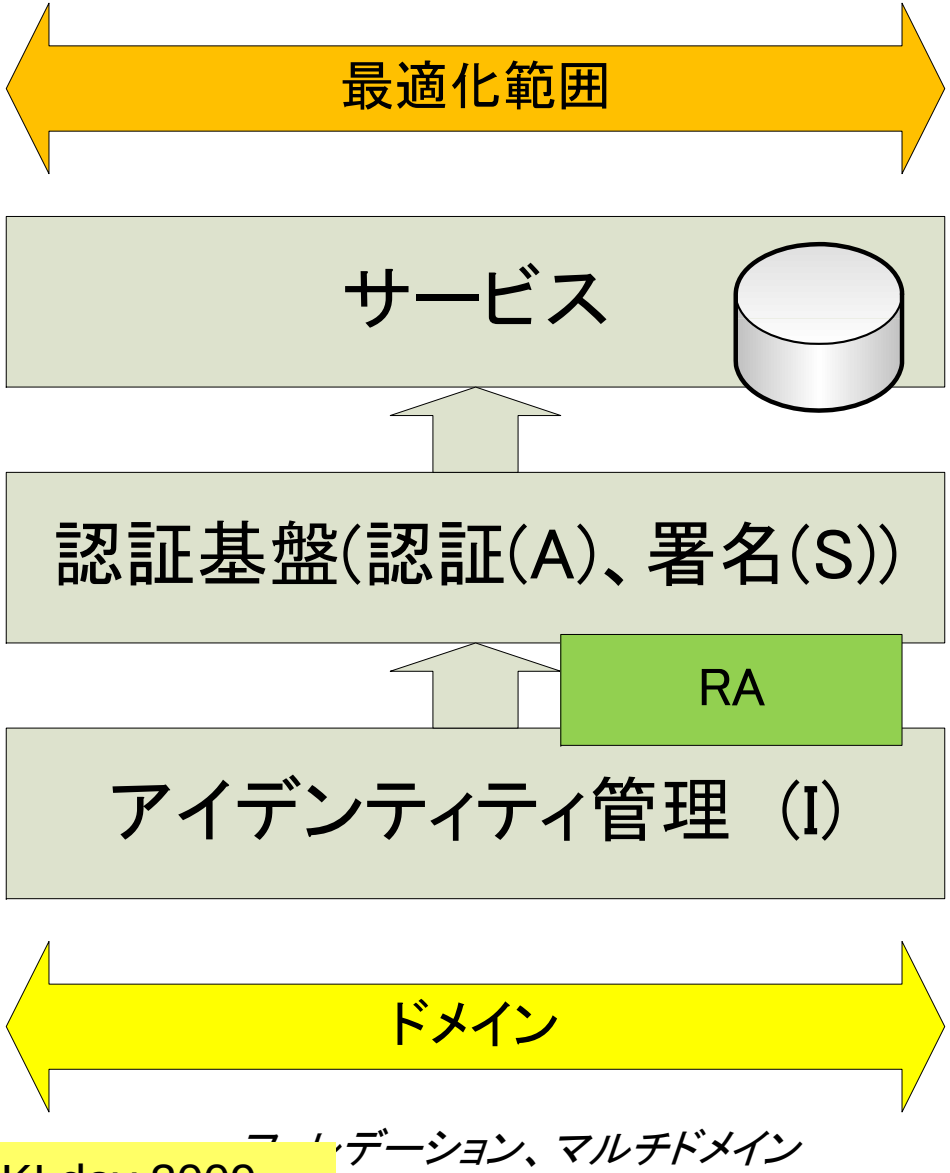
- 法人署名
  - 欧州では e-Seal
  - GPKIの官職証明書
  - 日本における法制度との関係
- 識別・署名・認証の関係
  - 電子署名と識別の関係
  - 番号制度、法人番号との関係
  - 仮名の扱い
- トラストサービスの統合
  - タイムスタンプ、Webサイト証明書等との関係
  - JPKI、HPKI等との関係

Copyright © 2014 SECOM Co., Ltd. All rights reserved.

過去のPKI day の関連スライド

Copyright © 2014 SECOM Co., Ltd. All rights reserved.

社会基盤としてのID管理
全体最適化と社会的コスト低減



全体最適の範囲を意識してID管理が検討されるべき

- 世の中の動きとして、効率を上げるために最適化の範囲が、広がっている
- 全体最適を検討する上でID管理の原則がベースになるべき。

組織を越えたID管理をどう達成するかが大きな課題

- 医療、介護、看護とか。
- 官民連携を行うID管理をとうやって達成するか？
- G2B2C
- プライバシー保護

Copyright © 2014 SECOM Co., Ltd. All rights reserved.

社会基盤としてのPKI　Big Picture

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

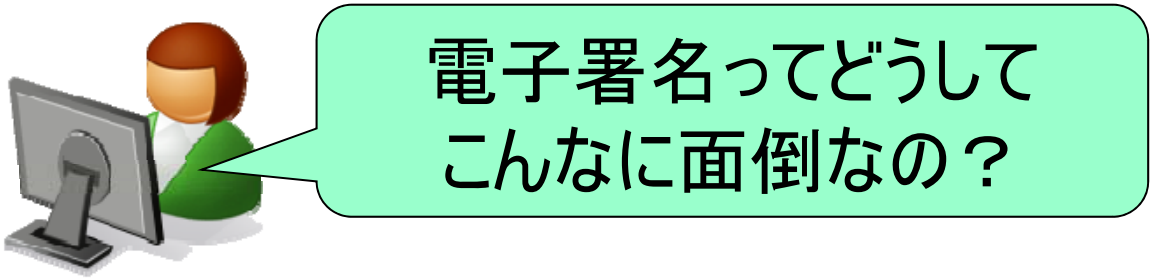
実装

法制度

デジタル時代の要素技術

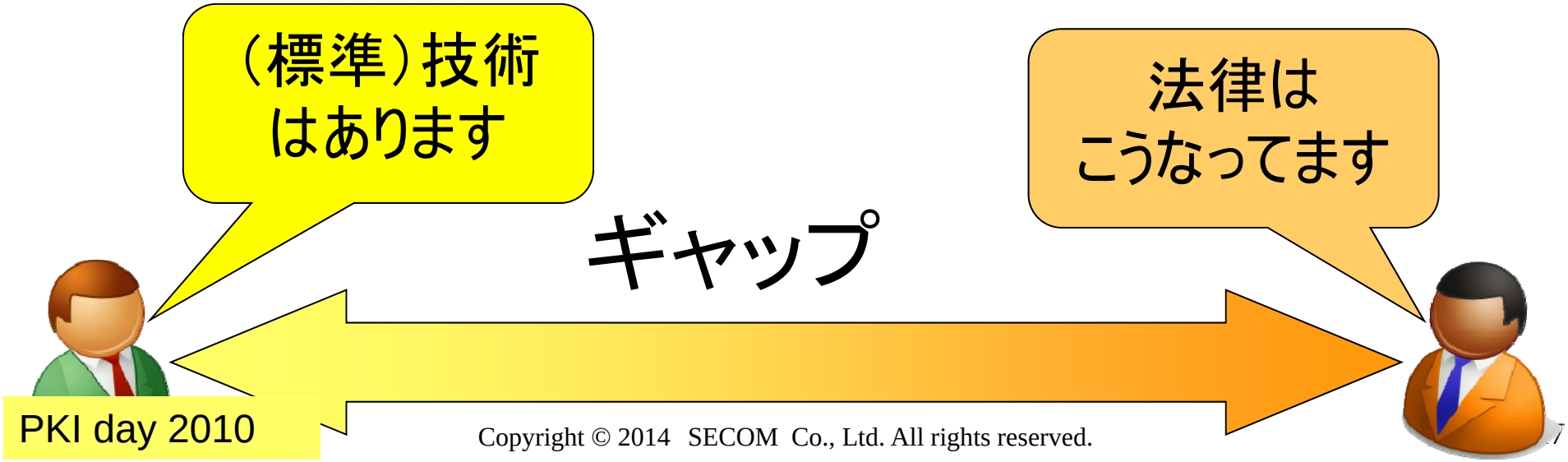
暗号技術　etc..

Copyright © 2014　SECOM　Co., Ltd. All rights reserved.



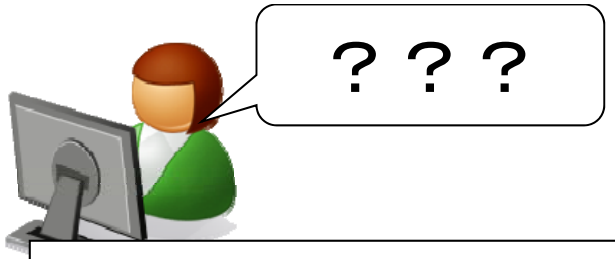
セコムIS研究所
Intelligent Systems Laboratory

「電子署名法等の課題」



Copyright © 2014 SECOM Co., Ltd. All rights reserved.

標準化と法制度の関係

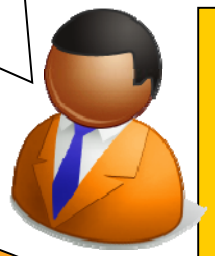


セコムIS研究所
Intelligent Systems Laboratory

"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。。」



IETF等の
標準化

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

「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
決する？

番外編

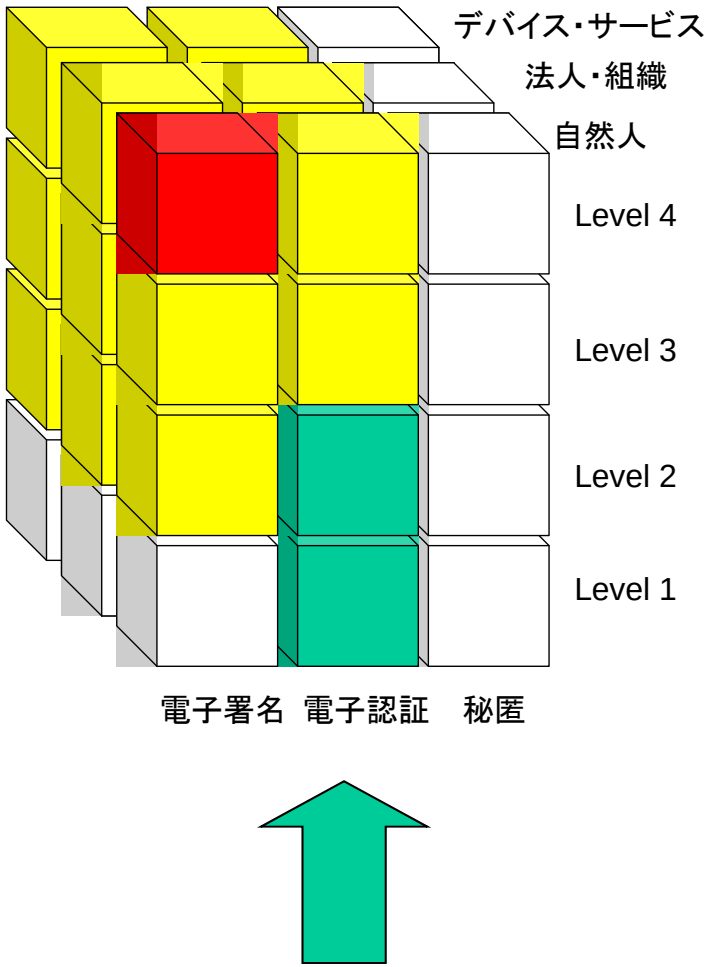
現在の医療の問題点は、
デジタル化以前の問題

Copyright © 2014 SECOM Co., Ltd. All rights reserved.

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

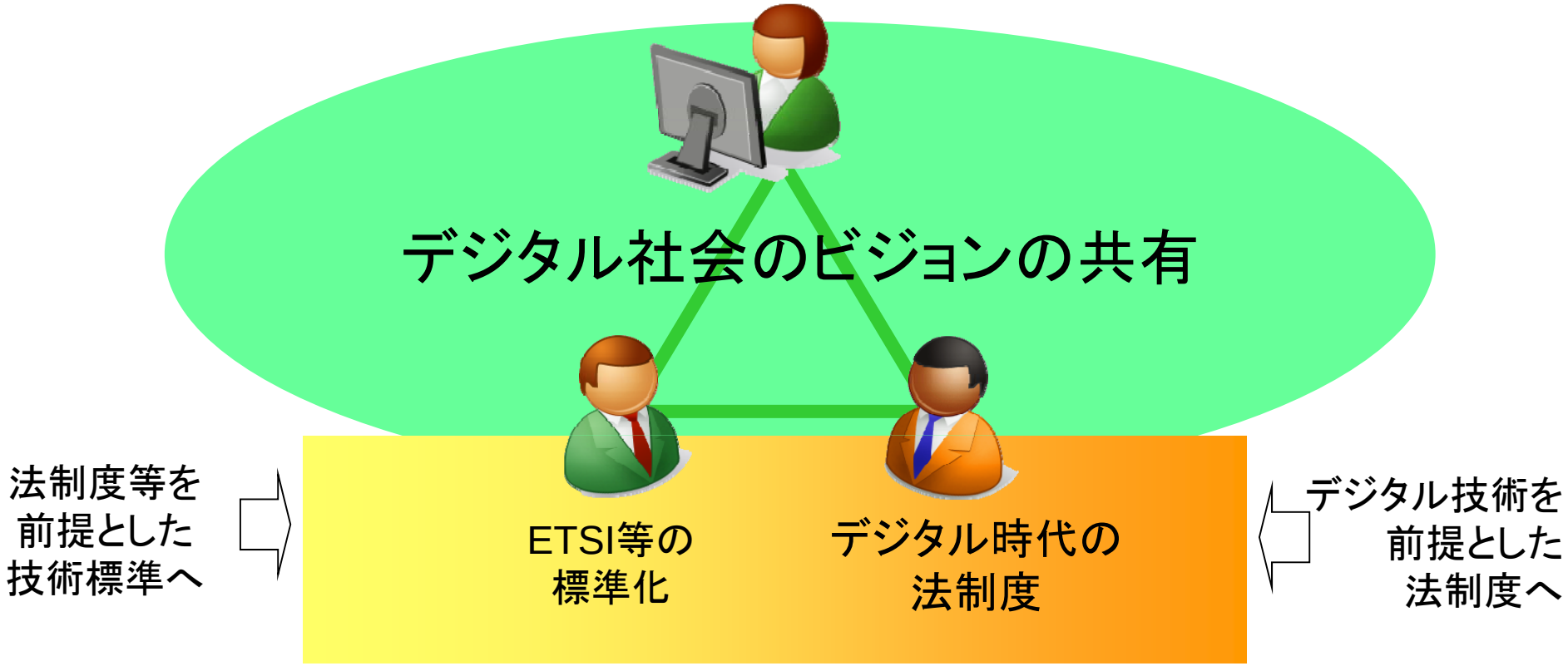
セコムIS研究所
Intelligent Systems Laboratory

- 「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。



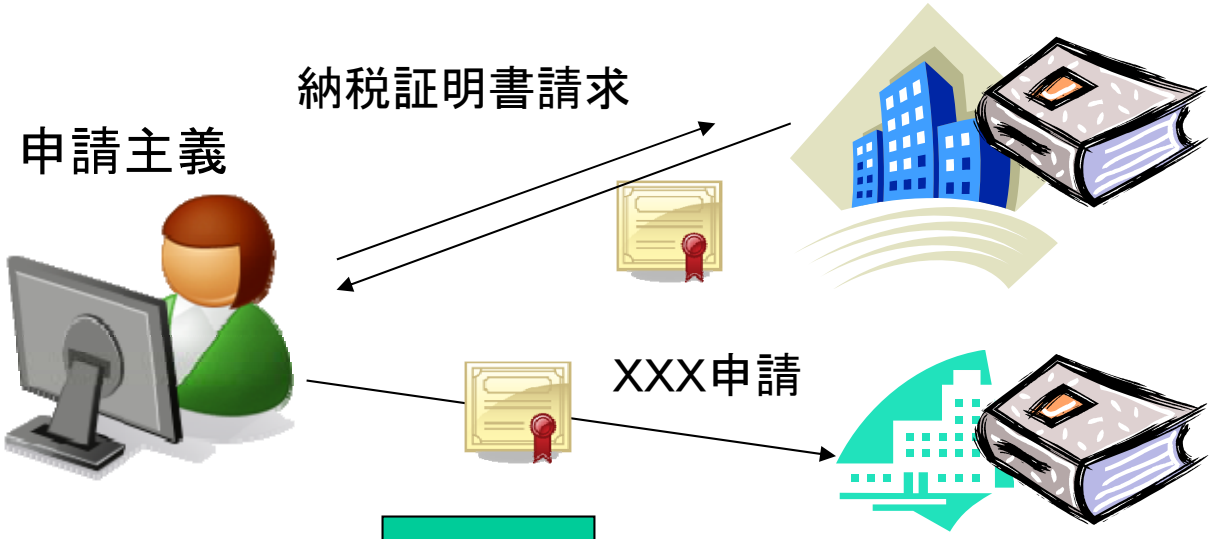
無謬性的な要求がなされた電子署名法の世界と
混沌としたビジネスのレモン市場の世界の同居？？

標準化と法制度の関係
欧州のアプローチ?

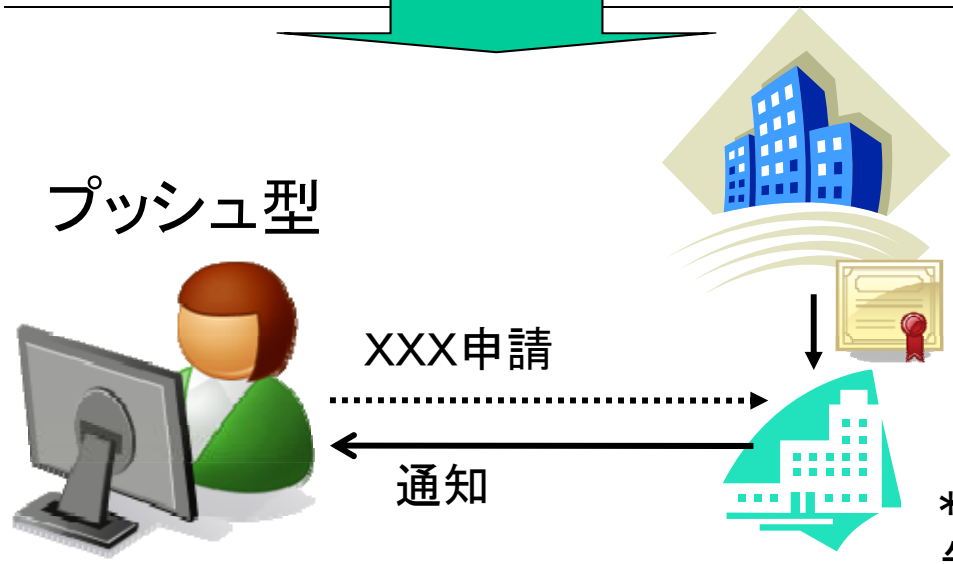


Copyright © 2014 SECOM Co., Ltd. All rights reserved.

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



- 「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？

Copyright © 2014 SECOM Co., Ltd. All rights reserved.

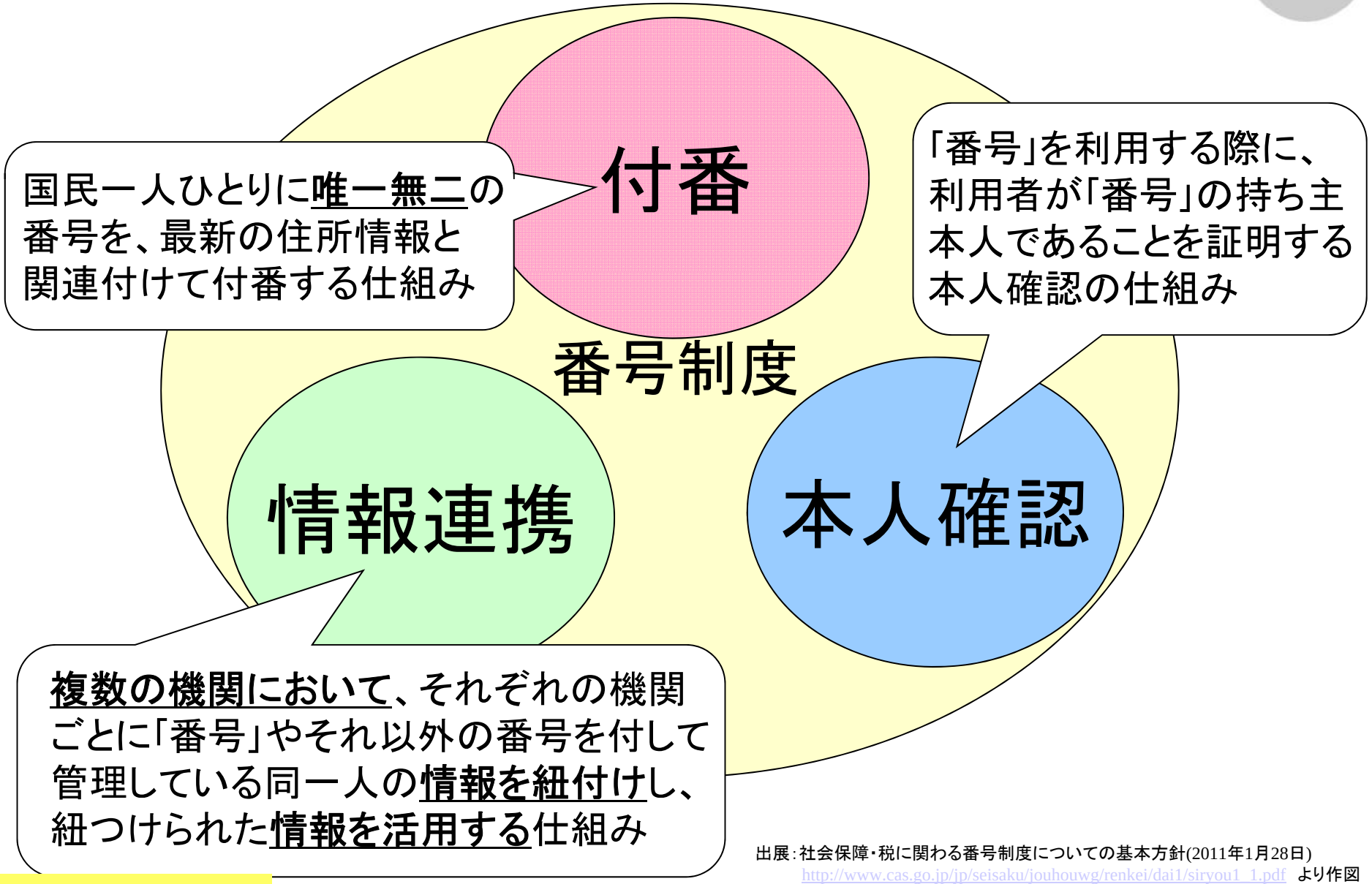
韓国の場合

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
  - 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

Copyright © 2014 SECOM Co., Ltd. All rights reserved.

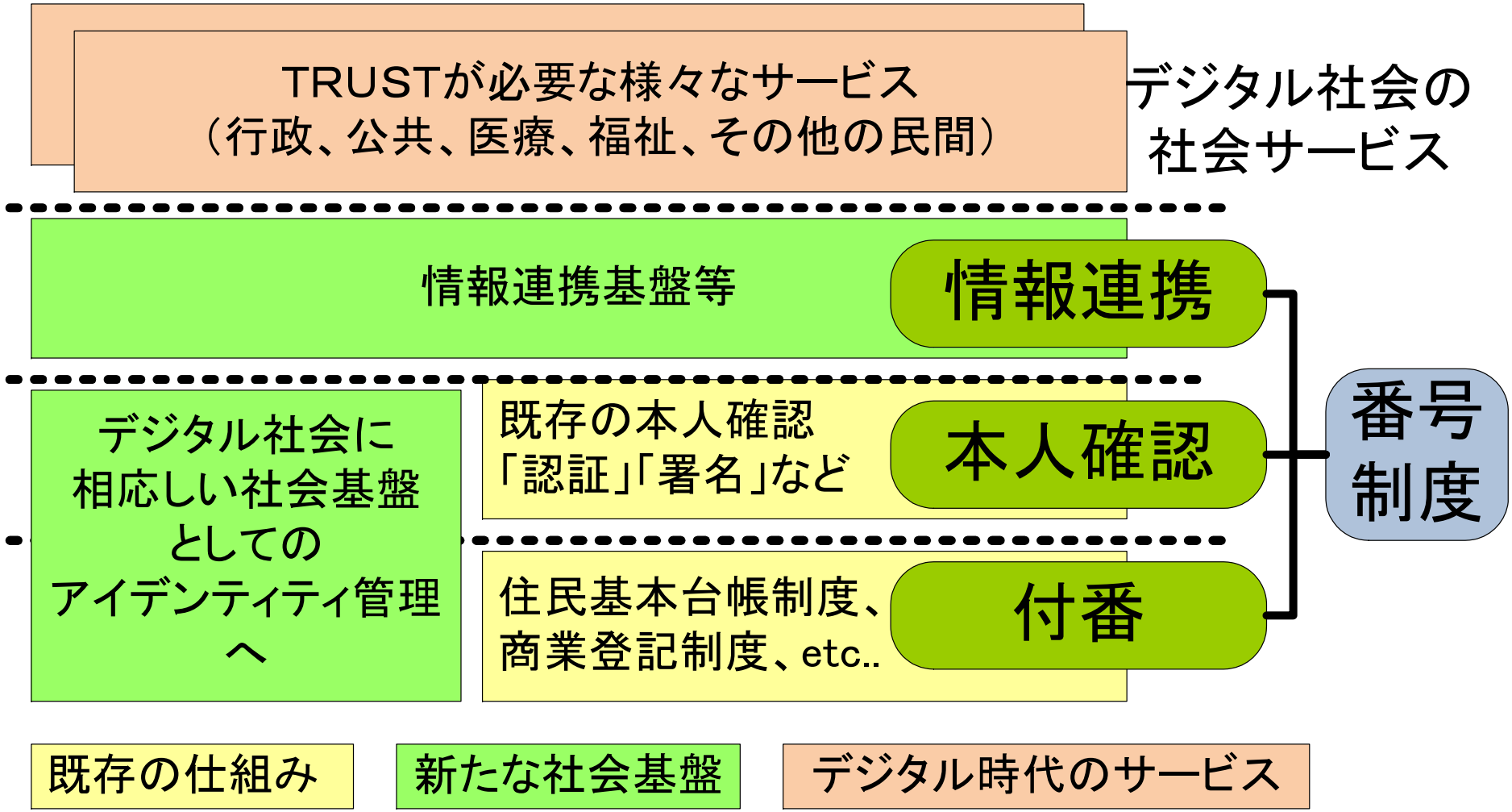
番号制度を構成する３つの仕組み



出展：社会保障・税に関わる番号制度についての基本方針(2011年1月28日)
http://www.cas.go.jp/jp/seisaku/jouhouwg/renkei/dai1/siryou1_1.pdf より作図

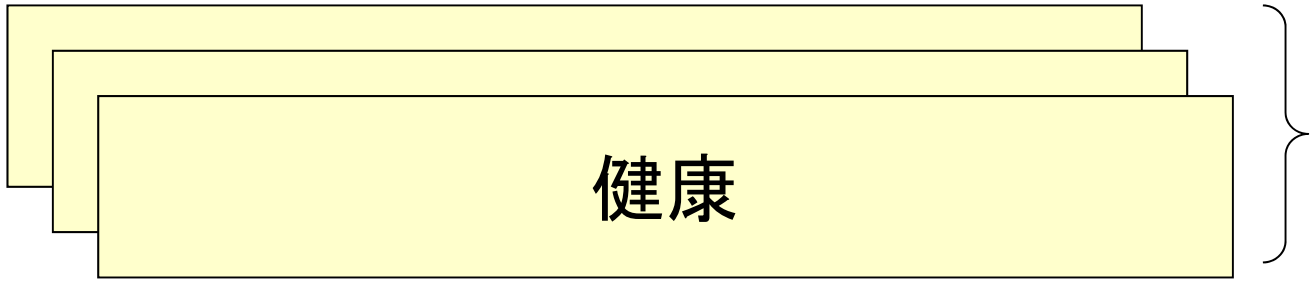
Copyright © 2014 SECOM Co., Ltd. All rights reserved.

番号制度に必要な3つの仕組み
松本の理解 （拡大解釈？？）



Copyright © 2014 SECOM Co., Ltd. All rights reserved.

「認証基盤」と「社会基盤としてのID管理」



社会を支える様々なサービス

認証 Authentication

署名 Signature

社会基盤としてのID管理

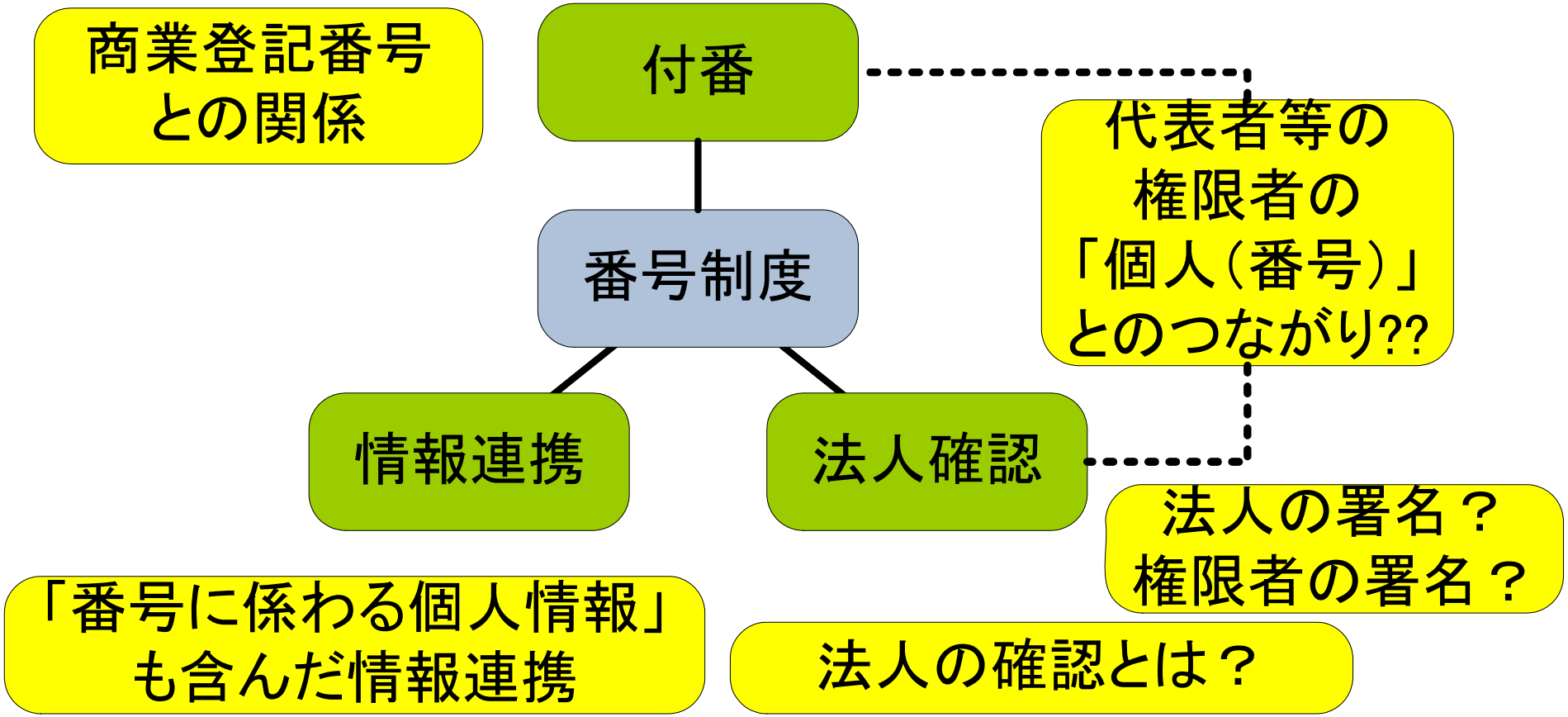
広義の「認証基盤」
電子的な認証(Authentication)&署名(Signature)の基盤

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

電子証明書の本質は、個人や企業のアイデンティティを電子データとして証明(Certify)することに大きな意味がある。

Copyright © 2014 SECOM Co., Ltd. All rights reserved.

法人番号の場合？？



Copyright © 2014 SECOM Co., Ltd. All rights reserved.

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

PKI day 2012

Copyright © 2014 SECOM Co., Ltd. All rights reserved.

「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

Copyright © 2014 SECOM Co., Ltd. All rights reserved.