セコムIS研究所
Intelligent Systems Laboratory

PKI Day 2016
マイナンバー時代のPKI

2015年　4月　22日

松本　泰　　セコム（株）ＩＳ研究所

PKI Day 2016
マイナンバー時代のPKI

セコム IS研究所
Intelligent Systems Laboratory

- マイナンバー制度が、施行され、その社会的インパクトの大きさが徐々に認識され始めています。
- しかし「マイナンバー法」自体が、本来の目的のために機能し、また、その社会的意義が広く認識されるまでには、まだ、紆余曲折があるかもしれません。
- こうした中、公的個人認証サービスにおける「利用者用電子証明書」の発行と、その民間開放が行われようとしています。また、法人番号とPKIとの関わりも重要になるかもしれません。
- PKI day 2016では、以上のことを踏まえ、「マイナンバー時代のPKI」をテーマに、今後の社会におけるPKIの在り方を議論します。

PKI day 2016 までの歩み

セコム IS 研究所
Intelligent Systems Laboratory

回	年	PKI day テーマ
1	2005	PKI技術最新事情
2	2006	PKIの展開と最新技術動向
3	2007	PKIの過去・現在・未来
4	2008	PKIの標準から実装まで 最新動向
5	2009	さまざまな分野に展開されるPKIの最新動向
6	2010	社会基盤としてのPKI／PKIの10年
7	2011	番号制度時代のPKI
8	2012	・我が国における信頼基盤の連携に向けて ・PKIへの攻撃とその対応
9	2014	・公開鍵暗号に関連する周辺技術動向の共有 ・デジタル社会のための「電子署名を見直す」
10	2015	サイバーセキュリティの要となるPKIを見直す
11	2016	マイナンバー時代のPKI

PKI Day 2016　マイナンバー時代のPKI
背景について　その1

セコム IS研究所 Intelligent Systems Laboratory

- 社会基盤としての「トラスト」の世界的動向
  - 市場モデルとして成立してきたトラスト　　Web証明書（等）
  - 規制モデル型として成立してきたトラスト　　電子署名法等
- 市場モデルとして成立してきたトラスト　（ボトムアップに成長）
  - PKI Day 2015「第2部　SSL/TLS実装の今とこれから」
    - 「SSL/TLS生誕20年、脆弱性と対策を振返る」　by 富士ゼロックスの漆島さん
  - 現状のトラストサービス(SSL/TLS関連等）の様々なほころび
  - トラストを構成する様々なステークホルダー
    - 競争の中でのトラスト、エコシステムによるトラストの難しさ
- 規制モデル型として成立してきたトラスト　（トップダウン）
  - 欧州においては、1999年のEU電子署名指令(Directive)からより広範囲（ Web証明書も含む）で強制力のあるeIDAS規則（Regulation)へ
- 欧州の規制モデル型　vs. 米国の市場モデル型
  - では、日本の立ち位置は？

PKI Day 2016　マイナンバー時代のPKI　背景について　その2

セコム IS研究所 Intelligent Systems Laboratory

- トラストサービスの難しさ
  - 法制度と同じで、一般の方には空気のような存在
    - 「SSL/TLS生誕20年」
    - 小人さんが考えていると思われている？
  - 制度、技術、ビジネスのかみ合わせが難しい
- トラストサービスの追い風？
  - デジタル社会のための国レベルのアイデンティティ管理基盤が整備されてきた
    - マイナンバー法
      - マイナンバー
      - JPKI証明書のシリアル番号
      - 法人番号
- 更に今後の課題
  - 人口よりもはるかに多い、数百億のデバイスのIoT時代のトラストの在り方

PKI Day 2016

セコム IS研究所
Intelligent Systems Laboratory

- 10:10-10:50 【基調講演】「我が国における安全安心な環境の実現　―マイナンバー、電子署名電子認証等― 」
  - 慶應義塾大学大学院政策・メディア研究科　特任教授　手塚悟　氏
- 11:00-11:40【講　演】「サイバー攻撃とPKI」
  - トレンドマイクロ株式会社　木村 仁美 氏
- 11:40-12:20 【講　演】「Certificate Transparencyを知ろう ～証明書の透明性とは何か～」
  - 講師：NTTデータ先端技術株式会社　大角 祐介 氏
- 12:20-13:00 【講　演】「TLS1.3とは何か？」
  - 講師：株式会社インターネットイニシアティブ　大津 繁樹 氏
- 14:00-14:40【講　演】「エストニアIDカードのPKIマニアック解析」
  - 講師：有限会社ラング・エッジ　宮地　直人 氏
- 14:40-15:20【講　演】「電子署名標準化動向から今後の方向性を探る」
  - 講師：セコム株式会社 IS研究所　佐藤　雅史 氏
- 15:20-16:00【講　演】「デジタルwatashiアプリ」
  - 講師：経済産業省　CIO補佐官　満塩　尚史 氏
- 16:20-17:40 【パネルディスカション】「マイナンバー時代のPKI」

セコムIS研究所
Intelligent Systems Laboratory

パネルディスカション
マイナンバー時代のPKI

＜パネリスト＞

手塚 悟　氏　　慶應義塾大学大学院 政策・メディア研究科　特任教授

満塩 尚史　氏　　経済産業省　CIO補佐官

宮内 宏　氏　　五番町法律事務所　弁護士

宮崎 一哉　氏　　三菱電機株式会社 生産システム本部/電子署名WGリーダー

パネルディスカション
マイナンバー時代のPKI

- JPKIの民間開放
- 法人番号、e-seal、電子契約等
- 欧州のeIDAS
  - 欧州における指令から規則への移行

JPKIの民間開放

セコム IS研究所
Intelligent Systems Laboratory

- 「電子署名に係る地方公共団体の認証業務に関する法律」の改正
  - 利用者証明用電子証明書の発行
  - 署名検証者等に係る届出等
- 利用者証明用電子証明書
  - 証明書の記載された「シリアル番号」の利用
- ディスカション
  - JPKI民間開放のインパクト
  - マイナバーと証明書のシリアル番号
  - 犯罪収益防止法等の本人確認との関係
  - JPKI利活用に向けた総務省の二つのWGの活動
    - スマートフォンへの利用者証明機能ダウンロード検討サブワーキンググループ
    - 属性認証検討サブワーキンググループ　→　「法人確認」？
  - 経済産業省「デジタルwatashiアプリ」

法人番号、e-seal、電子契約等

セコムIS研究所
Intelligent Systems Laboratory

- 番号制度の3つの仕組み（マイナンバーの場合）
  - 法人おける「番号」、「法人確認」、「情報連携」のあり方
- 「法人確認」　法人が使う証明書のあり方
  - 電子契約などのB2Bのための証明書
  - 法人番号を記載した証明書のプロファイル
  - 法人における属性の証明
    - 「特定認証業務の範囲外」を証明することの課題
    - 電子証明書に格納された属性情報の 信頼性と利用に関するガイドラインVer1.10
      - 平成28年3月25日 電子認証局会議 属性ガイドライン検討会
      - http://c-a-c.jp/pdf/report/guideline_ver1.1.pdf
- その他？
  - 欧州のe-sealのコンセプト
  - IoTデバイス等による署名？？

欧州のeIDAS
日本と欧州における
「個人情報保護法」と「電子署名法」

セコム IS研究所
Intelligent Systems Laboratory

年	日欧	
1995	欧州	データ保護**指令**採択
1999	欧州	電子署名**指令**採択
2001	日本	電子署名法施行
2005	日本	個人情報保護法の完全施行
2014	欧州	eIDAS**規則**発効
2015	日本	改正個人情報保護法の成立
2016	欧州	一般データ保護**規則**の可決（2016年4月14日）

- 一般データ保護規則：General Data Protection Regulation(GDPR)
- eIDAS規則： eIDAS Regulation

欧州のeIDAS
欧州における「指令」から「規則」への流れ

セコムIS研究所
Intelligent Systems Laboratory

- 欧州の成長戦略
  - 2010年 「欧州デジタル・アジェンダ」(Digital Agenda for Europe)」
  - 2011年 「単一市場法」(Single Market Act)
  - 2015年 「デジタル単一市場戦略」(A Digital Single Market Strategy for Europe)
- 「一般データ保護規則」
  - 地域や業界を横断する「デジタル単一市場構築」のために、パーソナルデータに関する扱いについて欧州における統一の基準と、その強制力を持った一般データ保護規則へ
- 「eIDAS規則」
  - 地域や業界を横断する「デジタル単一市場構築」のためのトラストサービスを確立するために、1999年の電子署名指令から、その範囲を大幅に拡張し強制力ももたせたeIDAS規則へ

欧州・米国・日本

セコム IS研究所
Intelligent Systems Laboratory

欧州
規制モデル

米国
市場モデル

社会サービス（行政、社会保障、税等）

一般データ
保護規則

個人情報の連携・個人情報の利活用と保護

eIDAS規則

トラストサービス・レイヤー

アイデンティティ管理（自然人、法人）
日本におけるマイナンバー制度等

日本の立ち位置は？？

セコムIS研究所
Intelligent Systems Laboratory

「番号制度とPKI」

2011年9月26日

セコム(株)IS研究所　松本　泰

番号制度とPKI

セコムIS研究所
Intelligent Systems Laboratory

- 番号制度は、国の根幹を成す制度と理解されつつあります。番号制度には、法人番号も含まれていますが、自然人、法人も含め、本格的なデジタル社会に相応しい「社会基盤としてのアイデンティティ管理」の整備への動きと捉えられるのではないでしょうか。そしてPKIの証明書は、本来「社会基盤としてのアイデンティティ管理」に基づき発行されるべきものと言えます。
- パネルディスカッション「番号制度とPKI」では、「番号制度」にPKIや電子署名法等の制度が、どのように対応していくべきか等を議論します。

＃昨年の「PKI day 2010」のプレゼンから
番号制度とPKI
アイデン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
  - 数々の脆弱性の対処
  - 電子署名法の認定認証局などの制度
  - 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？
    - PKIの証明書の内容やID連携のアサーションの内容等について
  - 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。。。）

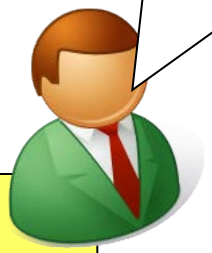
2011年現在の状況？

セコム IS 研究所
Intelligent Systems Laboratory

"Rough consensus and running code"

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。。」

法制度等から
ニュートラルな
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

技術標準

・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」、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

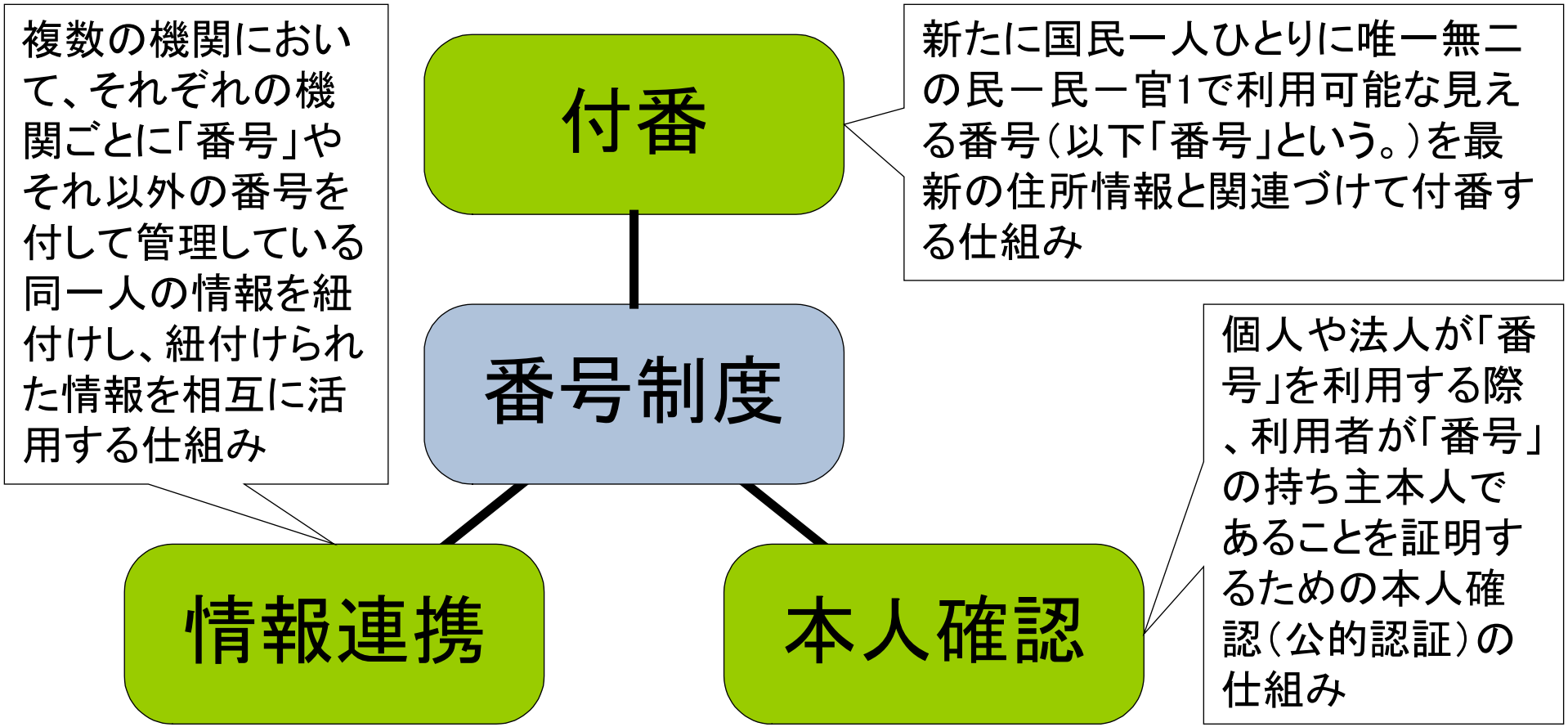
「光の道」で医療問題も教育問題も解決する？

番外編

現在の医療の問題点は、デジタル化以前の問題

番号制度に必要な3つの仕組み

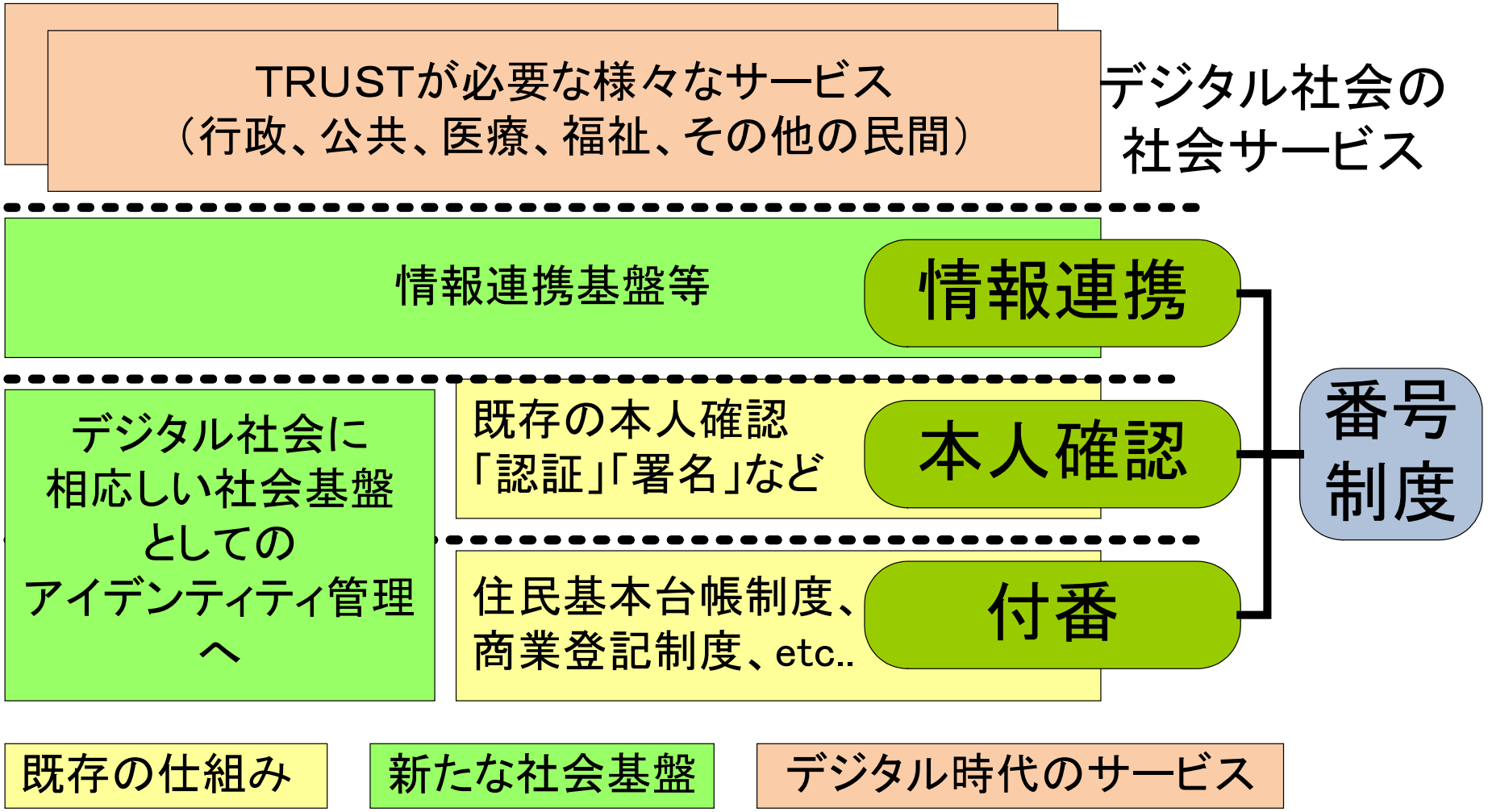
社会保障・税に関わる番号制度についての基本方針
2011年1月28日から



出典：http://www.cas.go.jp/jp/seisaku/jouhouwg/renkei/dai1/siryou1_1.pdf より作図

番号制度に必要な3つの仕組み
松本の理解 （拡大解釈？？）

セコム IS研究所
Intelligent Systems Laboratory

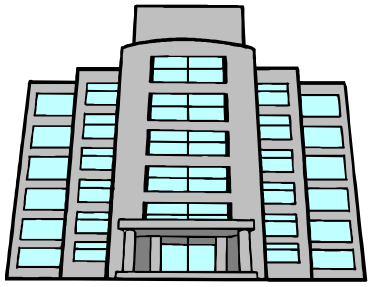


「番号」と「情報連携基盤」のイメージ

セコム IS研究所
Intelligent Systems Laboratory

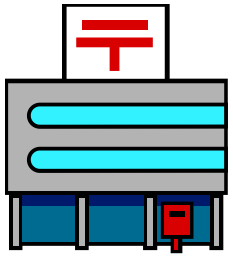
情報連携基盤

情報保有機関



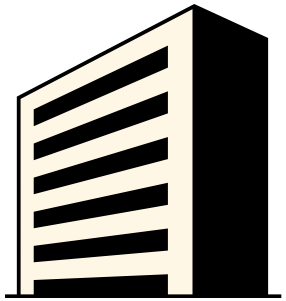
「番号」に係る個人情報

「番号」を取り扱い得る事業者



「番号」に係る個人情報

1234567890



情報保有機関

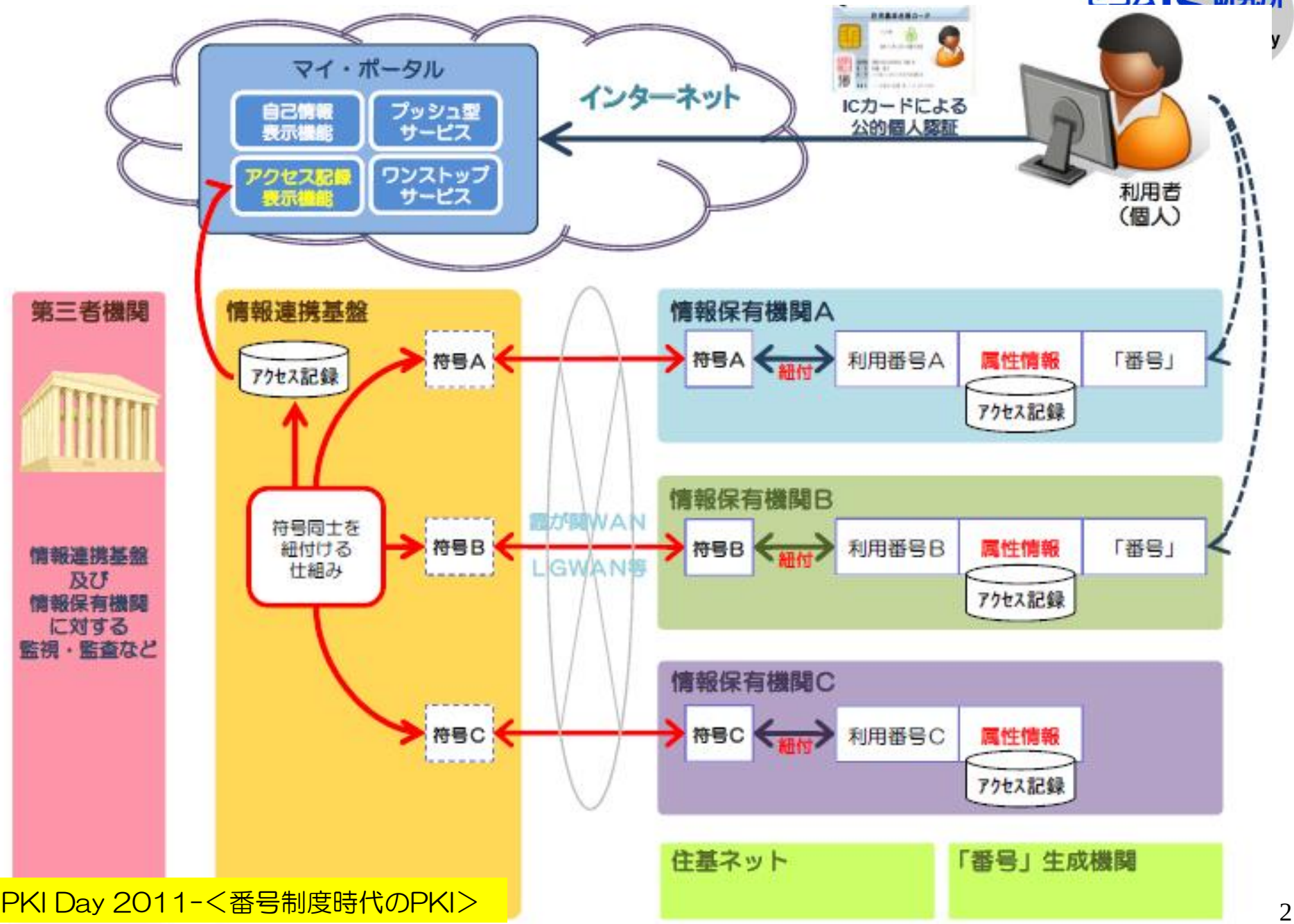
「番号」に係る個人情報

「番号」=マイナンバー

第3者機関

「番号」を取り扱い得る事業者

番号制度における符号連携のイメージ



オンラインでの本人確認

セコム IS研究所
Intelligent Systems Laboratory

- 番号制度「大綱」
  - （53page）

    ３．公的個人認証サービスの改良

    （１）現在の署名用電子証明書の発行に加え、マイ・ポータルにログインする等、文書を伴わないアクセスにおける本人確認を行うため、電磁的記録に記録することができる情報について行われる措置であって、当該措置を行った者が本人であることを示すために用いる認証用電子証明書の発行を行う。

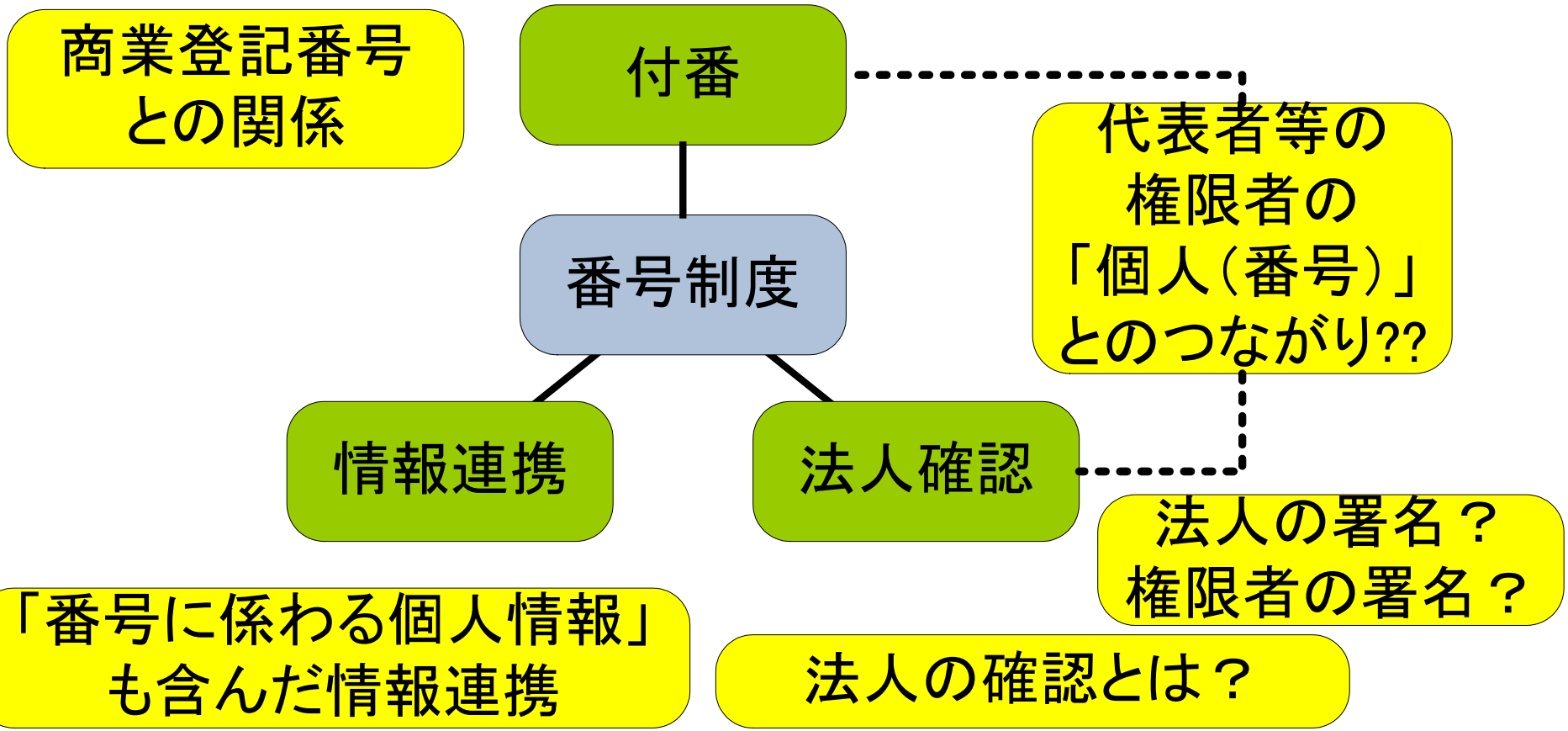
情報連携基盤技術ワーキンググループ　中間とりまとめ

法人に対する付番等

（23page）

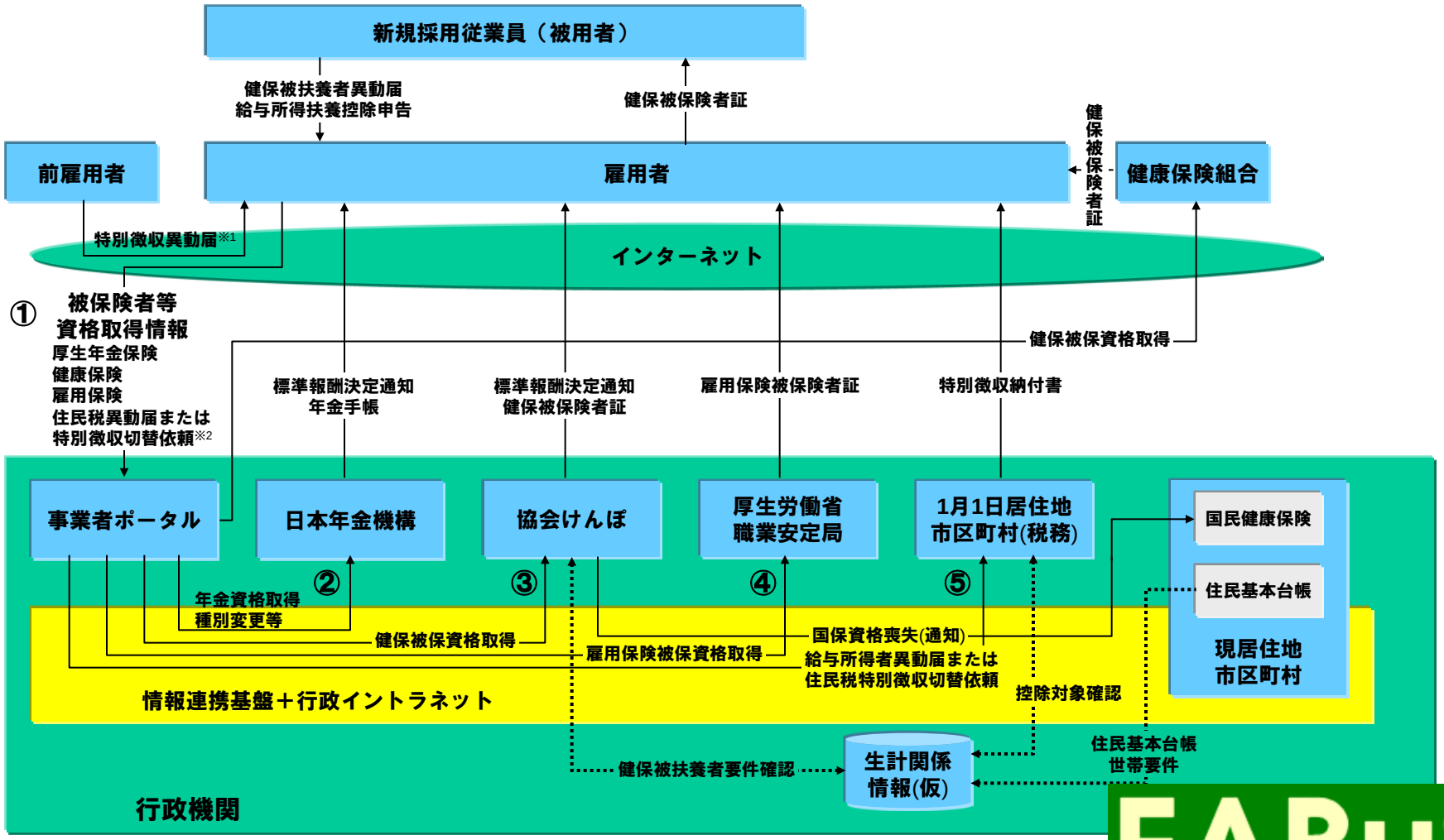
今後の検討の方向性としては、ニーズの把握、費用対効果の検証を前提として、例えば、番号制度により付番される法人番号と他の行政分野や民間分野で使用されている法人の識別番号との紐付け・置換の推進、行政機関間での企業情報の相互参照による行政手続における公的添付書類の削減、民間の電子商取引等においても**信頼性が保たれた企業のアイデンティティを表す属性情報の参照の充実、用途・利用者・利用場所等を考慮した企業認証の整備、企業コードに関連した企業ポータルの整備等が考えられる**。なお、企業認証については、電子署名及び認証業務に関する法律に基づく認定認証業務の活用を含めて検討することが考えられる。

法人番号の場合？？



EABUSの被用者の社会保障・税に関るケース(入社）

- 雇用者は事業者ポータルサイト（仮称）により被用者のイベント単位にワンクリックで行政手続を行う。
- 被用者の扶養関係等手続に必要な証憑は生計関係登録（仮称）で確認し、添付書類を求めない。
- 健康保険組合や国民健康保険間の被保険者資格得喪は被保険者の手続によらず保険者間の情報連携によって完結する。



※1転職等により住民税特別徴収を転職先で継続する場合

情報連携基盤

事業者ポータル

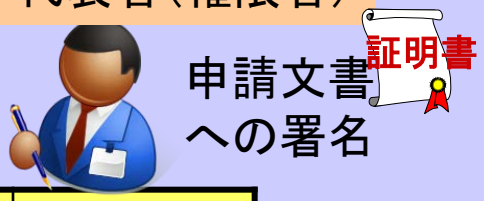
PKI(株)「番号」を取り扱い得る事業者

セコム IS研究所 Intelligent Systems Laboratory

作業者？

代表者（権限者）

ポータルへのログイン



申請文書への署名

申請

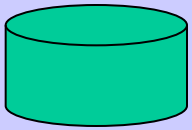
通知、参照・問い合せ？

法人名	PKI(株)	法人番号	887298

「番号」	名前	届出内容
998987	松本　泰	2011.9.26 入社
887692	手塚　悟	2011.9.26 入社
209987	満塩尚史	2011.9.26 入社
887628	宮内　宏	2011.9.26 入社

社員　松本泰

「番号」に係わる個人情報



法人番号
887298
の情報

情報保有機関

税理士

社会保険労務士

代理署名の場合、「法人番号」も含めた法人確認を行いたい（行ったことを証明したい）。

セコムIS研究所
Intelligent Systems Laboratory

パネリスト

- 手塚　悟　氏　　東京工科大学　教授
- 満塩　尚史 氏　経済産業省CIO補佐官
- 佐藤　直之 氏　日本ベリサイン株式会社　主席研究員
- 宮内　宏　氏　　宮内宏法律事務所　弁護士

セコムIS研究所
Intelligent Systems Laboratory

過去のPKI dayの関連スライド

社会基盤としてのPKI　Big Picture

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

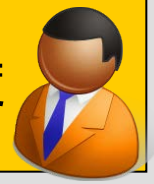
デジタル時代の社会基盤

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..

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？

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

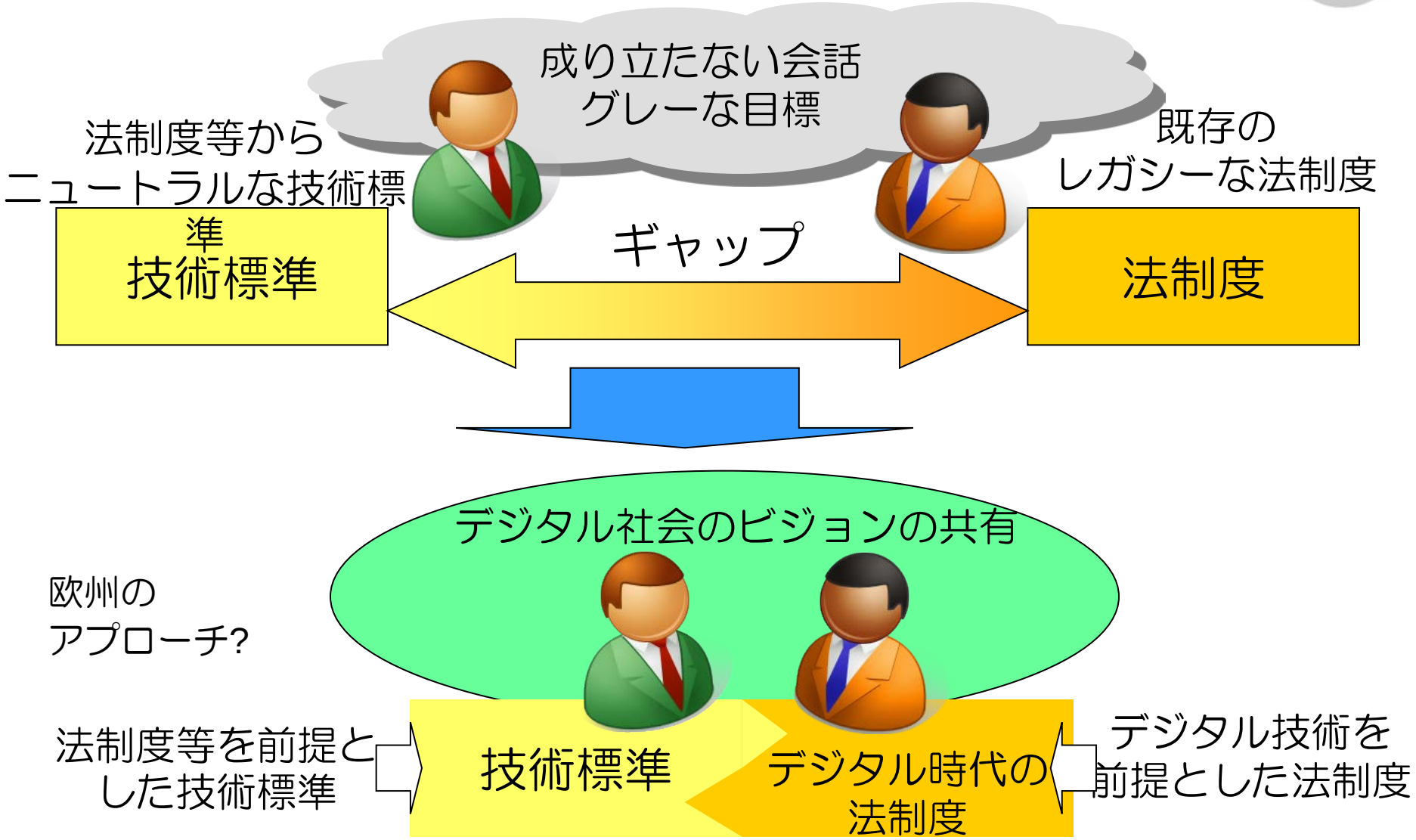
SSL

サーバ運営者

ともかくPCも携帯も全ての端末をサポートして欲しい

技術と制度をかみ合わせるためには

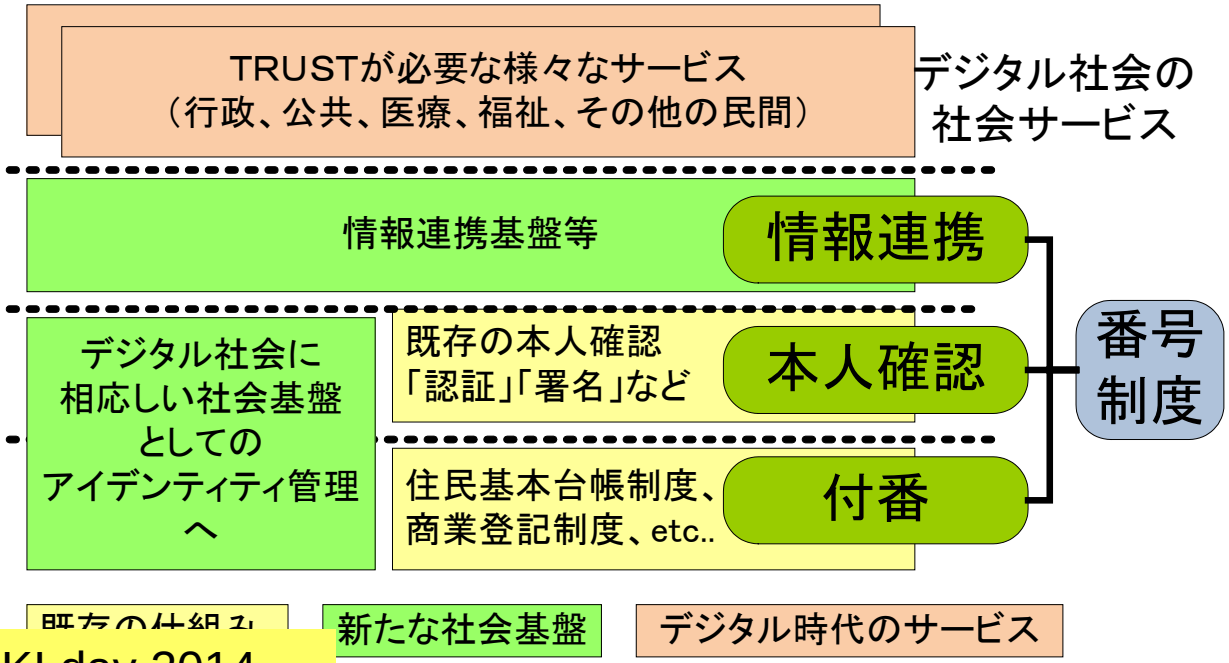
セコム IS研究所
Intelligent Systems Laboratory



2013年に成立した番号法

セコム IS研究所 Intelligent Systems Laboratory

- 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

PKI day 2015のオーバビュー

セコムIS研究所

3部　広がるサイバー空間に対応するPKIの新しい応用領域

時代の要請

マイナンバー制度の時代

ビッグデータ時代

IoT時代

サービスレイヤー

行政サービス
医療サービス
金融サービス
Webサービス

電子契約書
医療記録
電子領収書
プログラム（コード署名）

オープン化する制御システム
医療機器
ITS
車の車載器
IPルーティング

信頼が必要な情報連携サービス

信頼が必要なデジタルコンテンツ

数百億個のデバイスの多様な信頼関係

トラストレイヤー

eIDAS
電子署名
タイムスタンプ
電子シール
電子配布
Webサイト認証

Web trust for CA
Webサイト認証
DNSSEC
RPKI

（広義の）トラストサービス

トラストを構成する要素

デジタル社会のための法制度
法制度と整合性のある標準化
信頼のおける運用
セキュアな実装技術
暗号技術等のコア技術

1部 新しい時代の電子署名

2部 SSL/TLS実装の今とこれから

PKI day 2015