第３４回 ISSスクエア水平ワークショップ
「マイナンバーとオープンデータ 」

セコムIS研究所
Intelligent Systems Laboratory

番号制度に係わる情報セキュリティの課題

2013年10月18日

セコム（株）ＩＳ研究所　松本　泰

松本の自己紹介

セコム IS研究所 Intelligent Systems Laboratory

- 所属　セコム(株) IS研究所　コミュニケーションプラットフォームサービスマネージャ
- 1984年 UNIX上のビデオテックス・パソコン通信システムの開発に従事
- 1994年 各種インターネットサービスの設計、開発、運用に従事
- 1999年 サイバーセキュリティ事業の立ち上げに従事（不正侵入検知サービス等）
- 2003年-2007年
  - 工学院大学「セキュアシステム設計技術者の育成」プログラム客員教授
- 2005年　金融庁 偽造カード問題に関するスタディーグループ・メンバー
- 2007年　経済産業省商務情報政策局長表彰「情報セキュリティ促進部門」受賞
- 2007年-2012年　IPA 情報セキュリティ分析ラボラトリー非常勤研究員
- 2011年-2012年
  - 社会保障・税に関わる番号制度　　情報連携基盤技術WG　構成員
  - 社会保障・税に関わる番号制度　　社会保障分野サブWG　構成員
- 2013年10月現在
  - NPO 日本ネットワークセキュリティ協会 PKI相互運用技術WGリーダ
  - 暗号技術検討会（CRYPTREC）構成員
  - 暗号技術検討会（CRYPTREC）暗号技術評価委員会委員
  - 内閣官房　パーソナルデータに関する検討委員会・技術検討ワーキンググループ構成員
  - IEC/AAL（Ambient Assisted Living）　国内委員会　委員
  - 日本データセンター協会　セキュリティWGリーダ
  - 警察庁　官民ボード・行動計画策定WGメンバー

セコムIS研究所
Intelligent Systems Laboratory

番号制度に係わる情報セキュリティの課題

- 2013年5月24日、番号法（正式名称「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」）案及び関連法案が参議院本会議で可決され成立しました。この法律の成立により、番号制度の導入のスケジュールが確定し、その導入に向けた様々な動きが活発化しています。
- 番号制度の導入における大きな課題は、情報セキュリティの対応だとされてきました。この情報セキュリティに関しては番号法の成立までにも様々な議論がなされ、番号法自体にもその対応が盛り込まれています。
- しかし社会への実装という意味において情報セキュリティの課題は、番号法の成立を課題解決への終わりととらえるのではなく、始まりと捉えるべきです。
- 本講演では、番号制度と番号制度が社会へ及ぼす変化に対して、情報セキュリティ関係者は何を考えるべきか等を念頭に置き、番号制度に係わる情報セキュリティの課題、論点等を概説します。

セコムIS研究所
Intelligent Systems Laboratory

番号制度に係わる情報セキュリティの課題

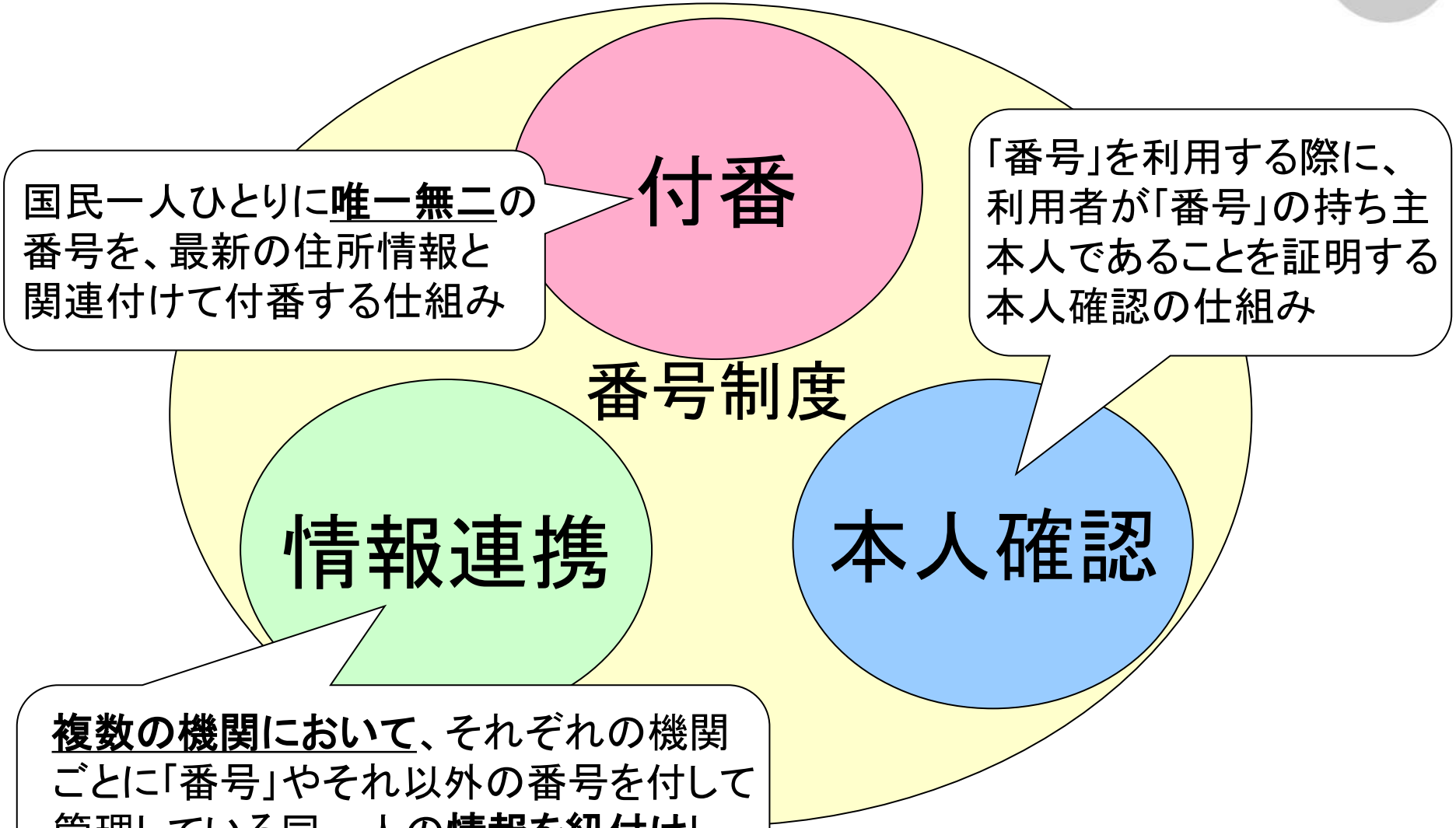
- 番号制度の概要
- セキュリティの課題の分類
- 第３者機関に関する論点
- 本人確認に関する論点
- 医療等分野に関する論点
- パーソナルデータに関する論点（おまけ？）
- まとめ

セコムIS研究所
Intelligent Systems Laboratory

（セキュリティを考察する上での）
番号制度の概要

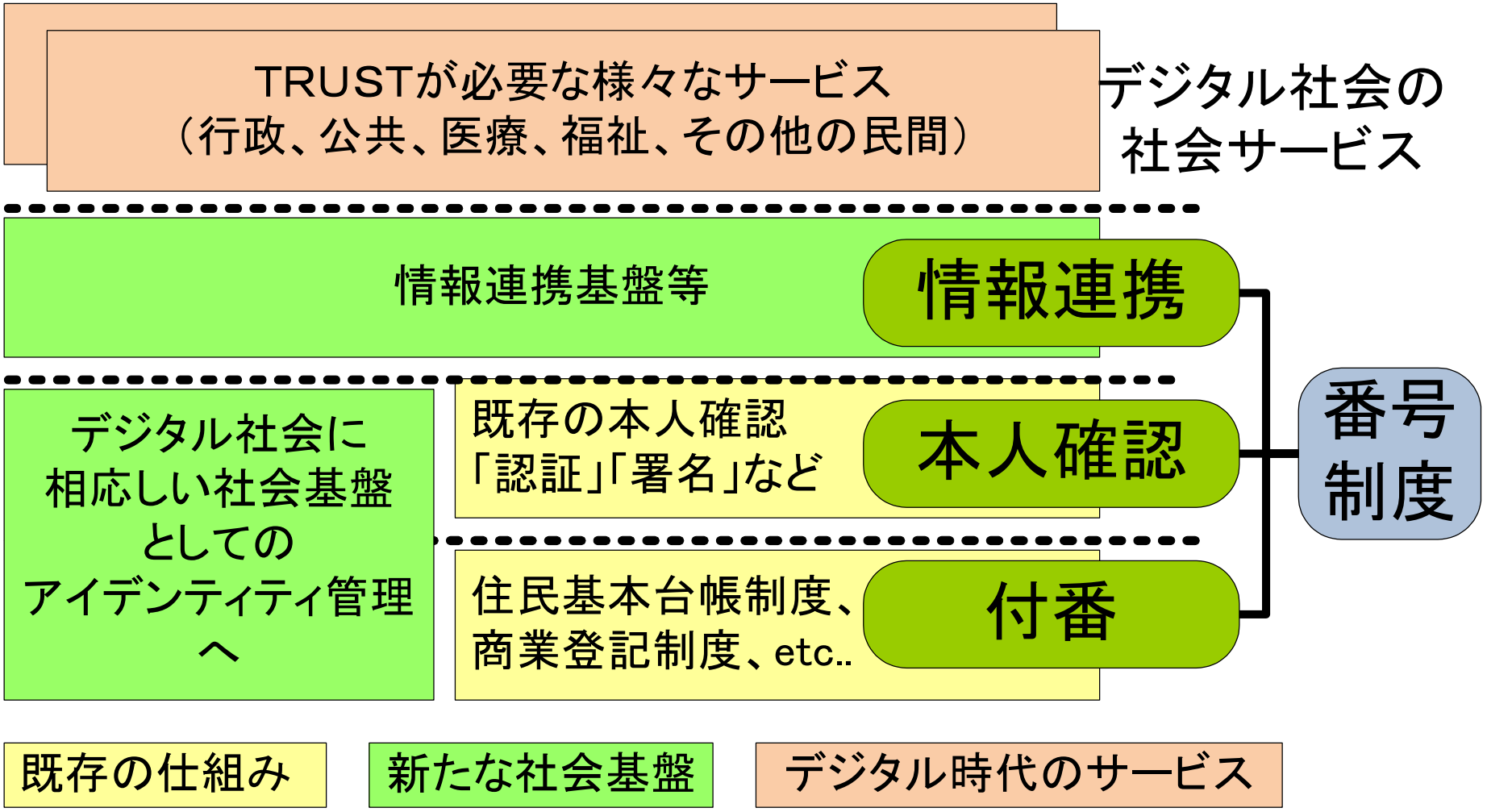
番号制度を構成する３つの仕組み

セコムIS研究所
Intelligent Systems Laboratory



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

番号制度に必要な３つの仕組み
松本の理解　（拡大解釈？？）



番号制度で何ができるのか（大綱での記述）

セコムIS研究所 Intelligent Systems Laboratory

	「番号制度で何ができるのか」（大綱の記述）	背景（松本の理解）
1	きめ細やかな社会保障給付の実現	「歳入庁」構想、総合合算制度等からの流れ 消費税率アップの対応。再配分の仕組み
2	所得把握の精度の向上等	納税者番号等、昔からの議論 税収アップと公正な社会。
3	災害時の活用	3.11以降の議論
4	自分に関する情報や必要なお知らせ等の情報を自宅のパソコンなどから簡単に入手	「電子行政」等の議論 自己情報コントロール権等の議論 エストニアの情報連携基盤等からの影響
5	各種事務・手続の簡素化、負担軽減	「電子行政」等の議論 行政サービスを中心とした効率的な社会
6	医療・介護等のサービスの質の向上	「健康ITカード」等の頃からの議論 少子高齢化、増大する社会保障費等の問題 （民間を含む）社会保障分野関係の効率化

社会保障・税番号大綱　http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/110630/honbun.pdf　より

番号法での用語

セコムIS研究所
Intelligent Systems Laboratory

- 個人番号（マイナンバー）
- 特定個人情報
- 個人番号カード　　任意取得
- 通知カード　　全員に配布
- 特定個人情報保護委員会 （第３者委員会）
- 特定個人情報保護評価 （ＰＩＡ）
- 情報提供ネットワークシステム（情報連携基盤）
- 情報提供記録開示システム（マイポータル）
- 個人番号利用事務（実施者）　自治体等
- 個人番号関係事務（実施者）
  - 一般の企業（従業員の源泉徴収等）も含まれる

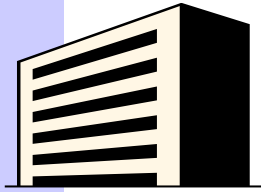
「個人番号」と「情報提供ネットワークシステム」のイメージ

セコムIS研究所
Intelligent Systems Laboratory

情報提供
ネットワークシステム

個人番号利用事務実施者A

個人番号利用事務実施者B



個人番号利用事務実施者C

特定個人情報

個人番号関係事務実施者D

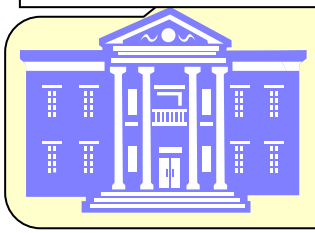
個人番号関係事務実施者E

個人番号

個人番号カード

個人番号

監視、監査、評価



特定個人情報保護
委員会

セコムIS研究所
Intelligent Systems Laboratory

セキュリティの課題の分類

・（１）国家管理への懸念
・（２）個人情報の追跡・突合に対する懸念
・（３）財産的被害への懸念

国民の懸念の類型

懸念の類型	制度上の保護措置	システム上の安全措置	松本メモ
①国家管理への懸念	・第三者機関による監視 ・自己情報へのアクセス記録の確認	・個人情報の分散管理 ・「番号」を用いない情報連携	・第３者機関以前に全体のガバナスが重要 ・個人の意思に関係なく個人情報が蓄積される行政機関、公共機関はより透明性が求められる。
②個人情報の追跡・突合に対する懸念	・法令上の規制等措置 ・第三者機関による監視 ・罰則強化	・「番号」を用いない情報連携 ・アクセス制御 ・個人情報及び通信の暗号化	・番号に係わる個人情報の不正な扱い ・不正なブラックリストの作成 ・個人の意思に反するトラッキング
③財産的被害への懸念	・法令上の規制等措置 ・罰則強化	・アクセス制御 ・公的個人認証等	・ID詐称（典型的には米国のSSNの被害） ・番号による本人確認の禁止

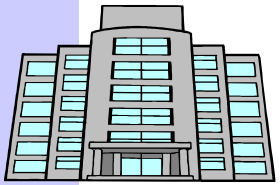
出展：番号制度の大綱

国民の懸念の類型

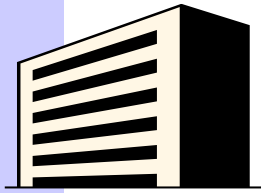
セコムIS研究所
Intelligent Systems Laboratory

情報提供
ネットワークシステム

個人番号利用事務実施者A



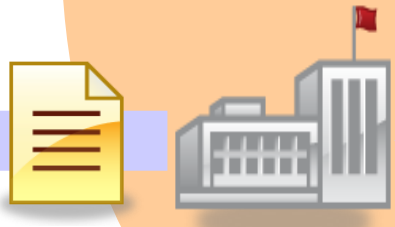
個人番号利用事務実施者B



個人番号利用事務実施者C

特定個人情報

個人番号関係事務実施者D



個人番号関係事務実施者E

個人番号

個人番号カード

個人番号

①国家管理への懸念

②個人情報の
追跡・突合に対する懸念

③財産的被害
に関する懸念

なかなか噛み合わない（かった）議論
国民の懸念（プライバシ＆セキュリティ）への対応

セコム IS研究所 Intelligent Systems Laboratory

技術は解らないけどともかく第3者機関は必要。ついでにPIA（情報保護評価）も

セキュリティ＆プライバシー

住基ネット訴訟の最高裁判決に従った設計、訴訟リスクを極力避ける設計にしなければならない。

よく分からんが。。情報連携基盤は、ITゼネコンの策略じゃないのか？

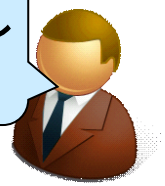
トレードオフ・バランスが見えない

ICカードは使いにくい。利用率をあげるため、利便性の高いユーザID、パスワードに変更すべき。

コスト

利便性

番号は広く民間でも利用可能にして利便性の高いものにすべき。



- 制度と技術の噛み合わない議論
- 様々な誤解、様々な思惑、技術的に対する不理解、Etc…

成立した番号法とセキュリティ

セコムIS研究所
Intelligent Systems Laboratory

- (1) 本人確認 (16条)
- (2) 特定個人情報保護委員会の設置 (6章)
- (3) 特定個人情報保護評価の実施 (26条から28条)
- (4) 特定個人情報等の取り扱いについての罰則（67条から77条）

セコムIS研究所
Intelligent Systems Laboratory

第３者機関に関する論点

- 特定個人情報保護委員会
- 特定個人情報保護評価

番号法の特定個人情報保護委員会 の役割

セコム IS研究所 Intelligent Systems Laboratory

- 第六章　特定個人情報保護委員会
  - (任務)
  - 第三十七条
    - 委員会は、国民生活にとっての個人番号その他の特定個人情報の有用性に配慮しつつ、その適正な取扱いを確保するために必要な個人番号利用事務等実施者に対する指導及び助言その他の措置を講ずることを任務とする。
  - (所掌事務)
  - 第三十八条
    - 委員会は、前条の任務を達成するため、次に掲げる事務をつかさどる。
    - 一 特定個人情報の取扱いに関する監視又は監督及び苦情の申出についての必要なあっせんに関すること。
    - 二 特定個人情報保護評価に関すること。
    - 三 特定個人情報の保護についての広報及び啓発に関すること。
    - 四 前三号に掲げる事務を行うために必要な調査及び研究に関すること。
    - 五 所掌事務に係る国際協力に関すること。
    - 六 前各号に掲げるもののほか、法律(法律に基づく命令を含む。)に基づき委員会に属させられた事務

番号法で必要とされた第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。

・２０１３年成立の番号法では、情報連携を円滑に進めるために、（また行政改革のため？）「第３者機関」が必要という結論になった。

特定個人情報保護評価 （制度）

セコムIS研究所 Intelligent Systems Laboratory

- 類似の制度は「環境影響評価制度」
- 個人情報の扱いのパラダイムシフト
  - 現状
    - 人が「曖昧な情報」（曖昧な識別情報、紙イメージの情報等）を目で見て判断
    - 人をコントロールするための現状の個人情報保護法関連の制度
  - 今後？　（　松本の理解　）
    - 情報システムが、ルール（制度）に従って、曖昧性の無い「特定個人情報ファイル」を自動処理する。
    - この「情報処理システム」の事前評価のための制度
    - 「プライバシー・バイ・デザイン」で設計された情報システム
    - 技術的な基準等も制度に組み入れらことが重要になる

番号法の付則（附則第6条）と関連する動向

セコム IS 研究所 Intelligent Systems Laboratory

- 番号法の付則（附則第6条）
  - 「政府は、この法律の施行後一年を目途として、この法律の施行の状況、個人情報の保護に関する国際 的動向等を勘案し、特定個人情報以外の個人情報の取扱いに関する監視又は監督に関する事務を委員会 の所掌事務とすることについて検討を加え、その結果に基づいて所要の措置を講ずるものとする」

- 「世界最先端ＩＴ国家想像宣言」（平成25 年6 月14 日 閣議決定）
  - （１）オープンデータ・ビッグデータの活用の推進
  - ② ビッグデータ利活用による新事業・新サービス創出の促進
  - IT 総合戦略本部の下に新たな検討組織を設置し、個人情報やプライバシー保護に配慮したパーソナルデータの利活用のルールを明確化した上で、個人情報保護ガイドラインの見直し、同意取得手続の標準化等の取組を年内できるだけ早期に着手するほか、新たな検討組織が、第三者機関の設置を含む、新たな法的措置も視野に入れた制度見直し方針（ロードマップを含む）を年内に策定

セコムIS研究所
Intelligent Systems Laboratory

本人確認に関する論点

先送りにされた課題の多い本人確認

「本人確認」の難しさ

セコム IS 研究所
Intelligent Systems Laboratory

- 「国民の懸念」との関係
  - 財産的被害への懸念　　―　　なりすましの防止
    - 「個人番号」と「本人」の関係を確実に証明したい。
  - 個人情報の追跡・突合に対する懸念
    - 「個人番号」を拡散させたくない
- 様々なトレードオフ
  - セキュリティ、利便性、コスト
- 本人確認を行う側の問題
  - マルチステークホルダーの世界？？での本人確認を行う側のインセンティブ
  - 本人確認の責任や証跡
- 様々な場面での「本人確認」
  - 対面
  - 非対面
    - 郵送
    - オンライン
      - マイ・ポータル（情報提供記録開示システム）
      - マイ・ポータル以外

個人番号カード、通知カード、本人確認

セコムIS研究所 Intelligent Systems Laboratory

- 個人番号カード　－　任意取得
  - 個人番号の記載＋現状の住基カード（顔写真付き）＋ＪＰＫＩ＋α
- 通知カード　－　全員配布
  - 個人番号の記載＋住基４情報
- 対面での本人確認
  - ＃「個人番号」のみで本人確認してはいけない！！
  - (1)「個人番号カード」
  - (2)「通知カード」と運転免許書等の**写真付きの本人確認書類**
- マイ・ポータル（情報提供記録開示システム）での本人確認
  - 「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」（整備法）の中の「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改正」
  - 公的個人認証サービスの従来からの「署名用電子証明書」以外に「利用者証明用電子証明書」を番号カードに格納して利用することが示されている。
  - 公的なＩＤカードに二つの証明書（認証用、署名用）を格納するのは、欧州の事例（eID）では良く見かける

本人確認関係の課題等

セコムIS研究所 Intelligent Systems Laboratory

- 非対面の郵送の本人確認
- 非対面でオンラインの本人確認
  - 「個人番号」をオンラインで伝える手段が用意されていない。
  - 欧州の事例（eID）では、電子証明書に「番号」が格納されている事例が多い
  - 韓国の「公認証明書　（accredit certificate）などの事例が参考になるかもしれない
- 対面での本人確認の責任や証跡
  - 「非対面でオンラインの本人確認」と同じにしてしまえばよい？
- 失効等の課題
  - 個人番号カード、通知カード等の盗難や紛失時の失効処理
    - 番号を失効される or クレデンシャルを失効される
      - 番号を失効させ新たな番号を割り振った場合の全体（社会全体）のコストが分からない
  - 失効状況を本人確認の検証者にどうのように知らせるのか
    - 現在のＪＰＫＩは、（失効情報を）民間に開放していない

番号法の付則（附則第6条4項）

セコムIS研究所
Intelligent Systems Laboratory

- 政府は、第十四条第一項の規定により本人から個人番号の提供を受ける者が、当該提供をする者が本人であることを確認するための措置として選択することができる措置の内容を拡充するため、適時に必要な 技術的事項について検討を加え、必要があると認めるときは、その結果に基づいて所要の措置を講ずるものとする

第十四条　個人番号利用事務等実施者は、個人番号利用事務等を処理するために必要があるときは、本人又は他の個人番号利用事務等実施者に対し個人番号の提供を求めることができる。

セコムIS研究所
Intelligent Systems Laboratory

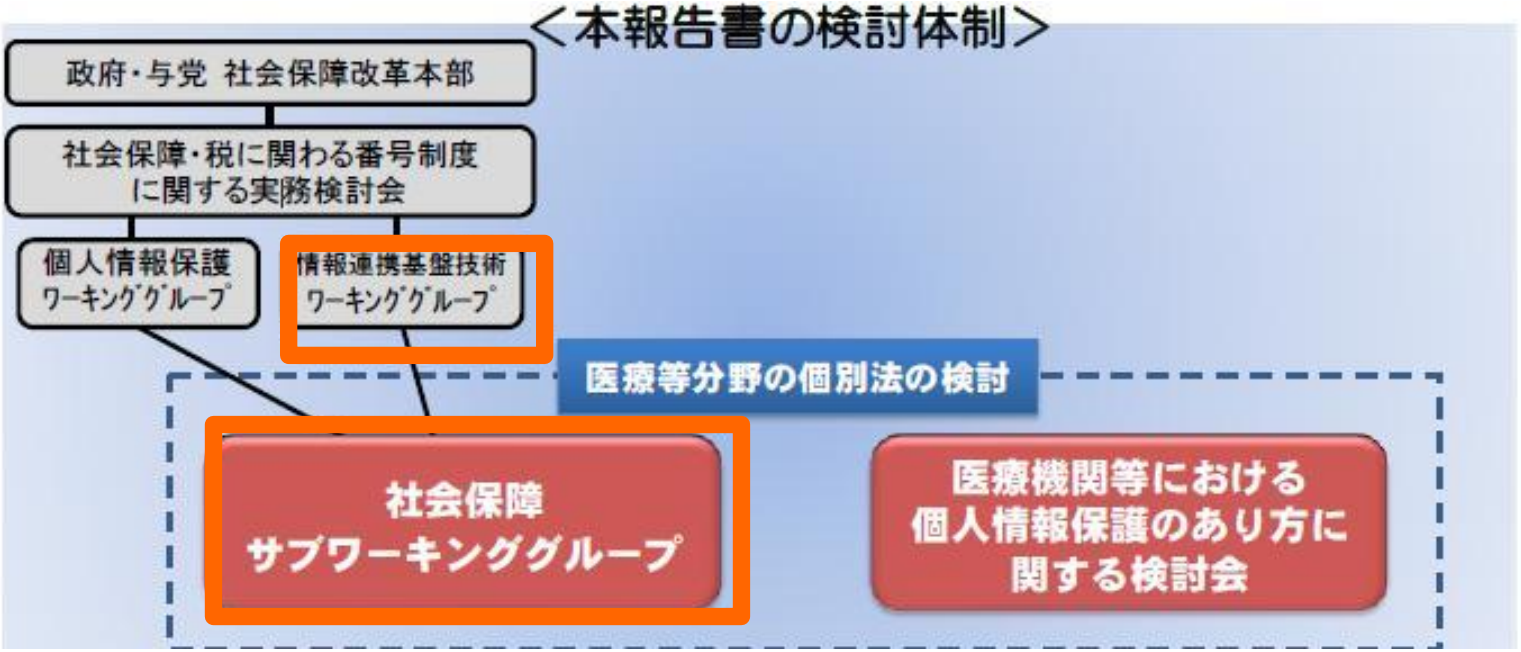
医療等分野に関する論点

厚労省の長い名前の検討会での議論

「社会保障分野サブワーキンググループ及び医療機関等における個人情報保護のあり方に関する検討会合同開催」

医療等分野における情報の利活用と保護のための環境整備のあり方に関する報告書

- 2012年9月12日に発行された「社会保障分野サブワーキンググループ及び医療機関等における個人情報保護のあり方に関する検討会合同開催」の報告書



検討会での議論された特別法の位置付・論点
現在の状況

セコムIS研究所 Intelligent Systems Laboratory

- 医療等分野の特別法の位置づけ
  - 「番号法」に対する医療等分野としての特別法
    - 「医療等ID」の議論
    - 健康保険の資格確認、地域医療連携、PHR
    - 医療等情報の個人情報の連携
    - 個人のための利活用に関する同意
  - 「個人情報保護法」の医療等分野としての特別法
    - 医療情報の２次利用、同意の在り方
    - 匿名化、連結可能匿名化、連結不可能匿名化など扱い
    - 個人情報保護法の不整合？
  - 医療等分野の範囲（特別法の範囲）
    - 範囲（連携の範囲、刑事罰の範囲）
- 2013年10月時点の状況
  - 番号制度のロードマップから「医療等分野の特別法」のスケジュールは削除
  - その一方　―「日本再興戦略-JAPAN is BACK」 2013年６月14日
    - 「個人一人ひとりが自分の医療・健康でータを利活用できる環境を整備・促進し、 適正な情報の活用により適切な健康産業の振興につなげるべく検討を進め、国民的理解 を得た上で、医療情報の番号制度の導入を図る」

番号法と医療等分野の特別法の違い

セコムIS研究所

	番号法	医療等分野の特別法
情報保有機関（個人番号利用事務実施者）	自治体等の公的機関が多い。 民間利用は想定していない（修正議論はある？）	病院、介護事業者等など民間の事業者が多く含まれる。 **
情報連携に対する同意	明示的な同意を必要としない法令で示された範囲	基本的には同意が必要
付番	個人番号	医療等分野ＩＤ（仮称）
情報連携基盤	番号法の「情報提供ネットワークシステム」	医療等分野に閉じた情報連携基盤***
本人確認	個人番号カード等	（議論なし）

*** 検討会のメンバーが、医療等分野のステークホルダーが多いこともあり、他の分野と分離した医療等分野に閉じた議論が多くなる傾向にある。

医療等分野の特別法は、番号法に比べ、通常の民間ビジネスの話に近い？？

検討会のメンバーとその視点

セコムIS研究所 Intelligent Systems Laboratory

- 医療等分野のステークホルダー
  - ３師会（医師会、歯科医師会、薬剤師会）
  - 看護、介護、福祉関係者
  - 健康保険組合
  - 医療情報（山本隆一先生*２）
  - 法学者　　（宇賀克也先生*１、鈴木正朝先生*２）
  - 自治体関係者
  - 情報セキュリティ分野（ＨＰ佐藤慶浩氏*3、松本*3）
- 検討会の委員に足りない観点
  - 医療等分野を越えた範囲、国全体の最適化の観点
  - コスト的、ビジネス的な観点？？
    - ＃「医療等分野」は、国民皆保険制度、診療報酬制度等の影響が大きい

＊1　パーソナルデータに関する検討会座長代理
＊2　パーソナルデータに関する検討会構成員
＊3　パーソナルデータに関する検討会・技術検討WG構成員

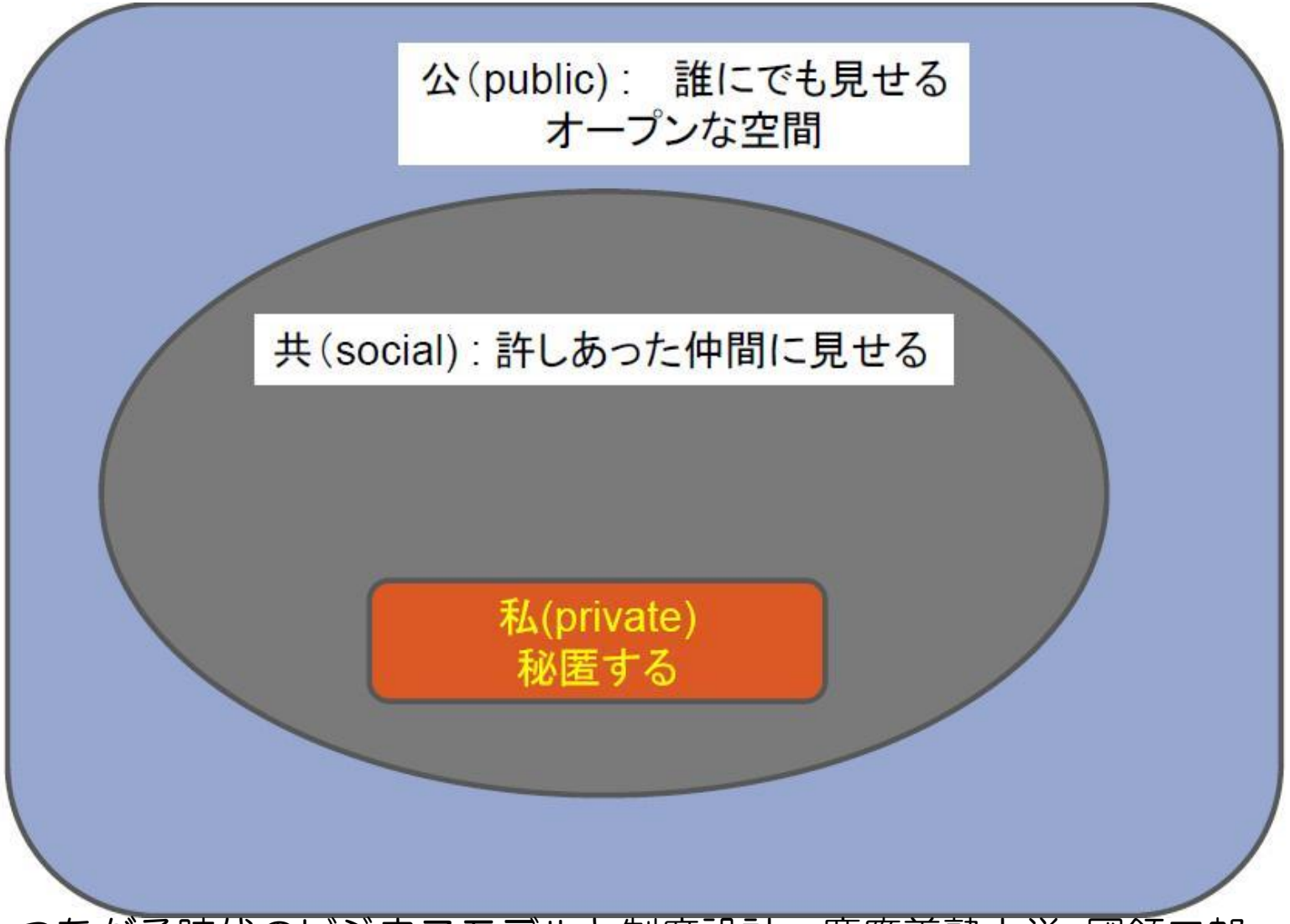
制度的の大枠的な議論

セコムIS研究所 Intelligent Systems Laboratory

- 医療等分野の範囲
  - 狭い　-- 医師会、歯科医師会等
  - 広い　-- 介護・福祉分野の関係者
  - 医療等ＩＤを利用する範囲？ or 刑事罰等の適用範囲？
- 刑事罰等　- 議論が交錯しており整理されてない。
  - 必要vs.必要ではない（直罰規定vs.間接罰）
  - 刑事罰による保護の促進
    - 米国のHIPPA/HITECH法等の事例
  - 萎縮を防ぐ　-- 多分ルールの明確化以外にない？
- 刑事罰などの対象者
  - 「現在の刑法にある医療従事者等の守秘義務」等に対して
  - 「有資格者（医師等）」 から「情報取扱い者」へ
  - 医療->介護->福祉　範囲が広まる程に責任が曖昧になる
- 課題？
  - 医療等分野と医療等分野外の分断or架け橋？

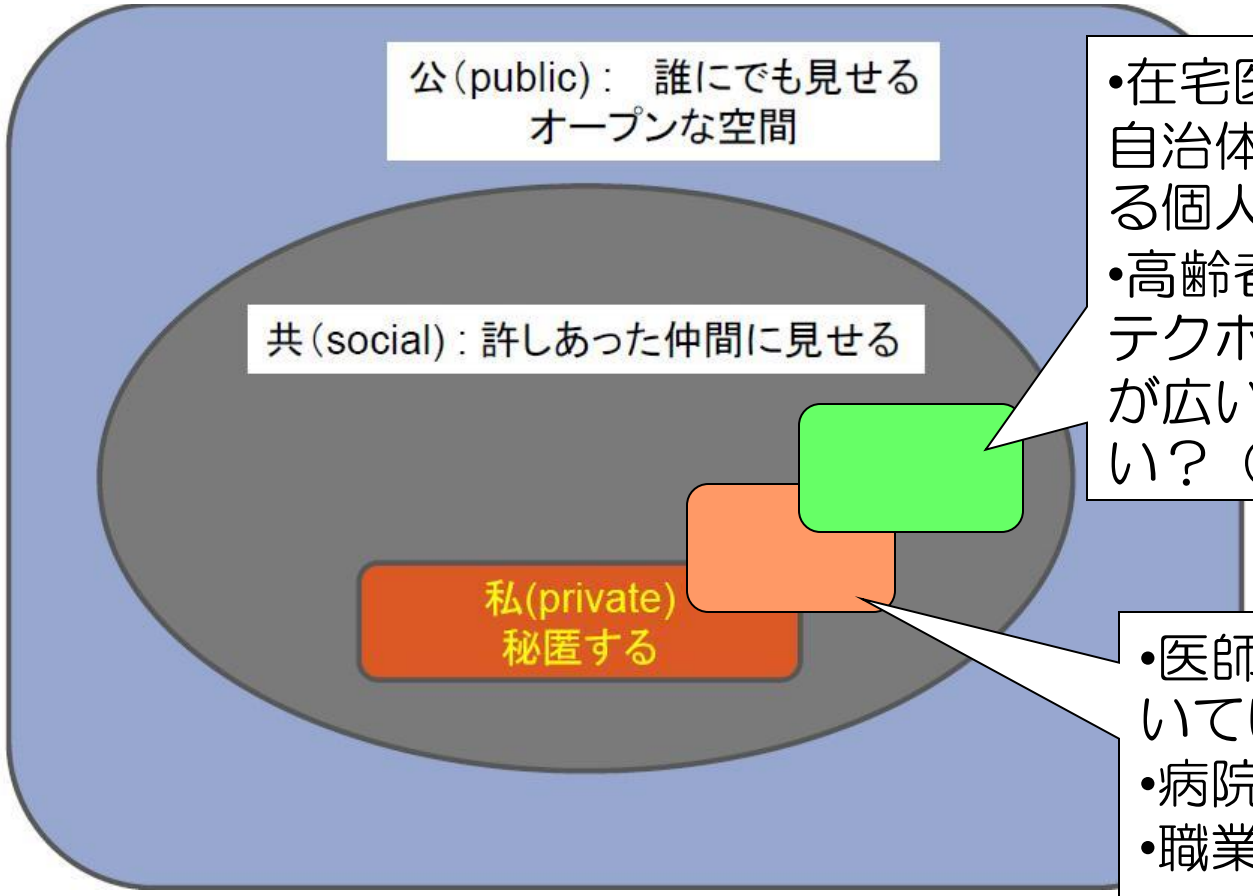
特別法の「範囲」？？

セコムIS研究所
Intelligent Systems Laboratory



つながる時代のビジネスモデルと制度設計　慶應義塾大学. 國領二郎
http://www.it-yugo.jp/program/PDF/4-2_kokuryo.pdf

噛み合わない議論？？？



•在宅医療、看護、介護、福祉、自治体関係者が念頭においてる個人情報連携？？
•高齢者等を支える幅広いステークホルダー（職業的な範囲が広い）が、地理的範囲は狭い？（地域コミュニティ）

•医師会等の関係者が念頭に置いている個人情報連携？？
•病院間連系等
•職業的な範囲は狭い

在宅医療、看護、介護、福祉、自治体関係者の思い？？？

- （広い）情報連携は必要、
- （狭い）医療分野の厳しい刑事罰まで含めた範囲に中に入ると現場が回らない？

同意に関する議論

セコムIS研究所
Intelligent Systems Laboratory

- ２次利用に対する同意
  - 公益と個益のバランス
  - 公益のために、同意を如何に現場の負担のないようにするかと言う観点
- 病院間連携、PHR等における同意
  - PHRに関しては、そもそもPHRに否定的な立場の人もいて議論は少ない。
  - （松本の意見としては）個人の「同意」「意思」により、より多くのステークホルダーに第３者提供可能なスキーム、フレームワークが重要
- 代諾
  - 代理、家族、etc…　社会の変化
  - 現状においても、現場は、すごく困っている。

後、、議論はなかったが「同意」の扱いが曖昧だと「故意」と「過失」の区分も曖昧になる（刑事罰等に関して）

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？？

日医ニュース　2012/10/20　石川常任理事に聞く
–個人情報保護のため医療分野に関する個別法の早期の制定を–

私ども医師には，ヒポクラテスの時代から，患者の秘密を守るという職業倫理の順守が求められていますが，この職業倫理は現在でも，刑法や医療関係法規に反映されています．

「患者の秘密が漏示されない」点を重視しなければならず，医療情報を扱う全ての者に対し罰則を科すこと等も検討しなければなりません．また，診療目的以外で患者の医療情報を扱う場合は，原則として，患者自身の同意を得るべきだと主張しています．

医療者側としては，まず個人情報の保護のルールをきちんと確立してから、次に利活用を検討すべきと考えています．

出展：　http://www.med.or.jp/nichinews/n241020b.html

松本の発言と意見

セコムIS研究所 Intelligent Systems Laboratory

- 情報連携基盤に同意の扱いを取り込む - 松本の提出した意見書より
  - 現在の「合同開催」では、「医療等の提供のために必要な場合における本人同意」の議論があり、この「同意」の扱いが様々な課題に結びついている。
  - 「医療等分野情報連携基盤」のあるべき方向性としては、同意されたものが同意された範囲にしか転送されないといったシステムであるべきである。また、オンラインでの同意確認、同意の状態管理を積極的に行うことにより、情報連携の制御も「同意」に基づいて行えるような仕組みが望ましいと考える。その他、医療等分野においては、代理、委任の仕組みなども重要になる。
- 特別法の範囲　- 検討会での松本の発言（議事録より）
  - 医療・介護等のサービスの質の向上に寄与できるステークホルダー全般をなるべく取り込む。ただし、ここで何の制約も働かないというのはまずいというのは勿論ありまして、それを何らかの形で特別法の枠組みで制御する。特にこれから制度が明確になれば出てくるであろうPHR事業者等、そういったところの参入はやはり促すべきだと考えておりますが、そういったところに対しての許認可制度、認定制度、そういったものをセットでやると良いのではないかと個人的には思っております。
- 通知義務（情報漏えい、データ侵害）
  - 検討会における、法制度の議論は、刑事罰の扱いのみ。情報漏えいに関する「通知義務」の扱いを明確にするべき。その際、何が「情報漏えい」なのかを明確にすべき。

セコムIS研究所
Intelligent Systems Laboratory

（おまけ）
パーソナルデータに関する論点

・番号制度の議論ではないのですが、番号制度の議論とも関係が深いパーソナルデータの保護と利活用の議論
・「識別性」と「匿名性」の関係
・セキュリティ、プライバシーに関する制度と技術の関係
・オープンデータにとっても大きな課題？？？

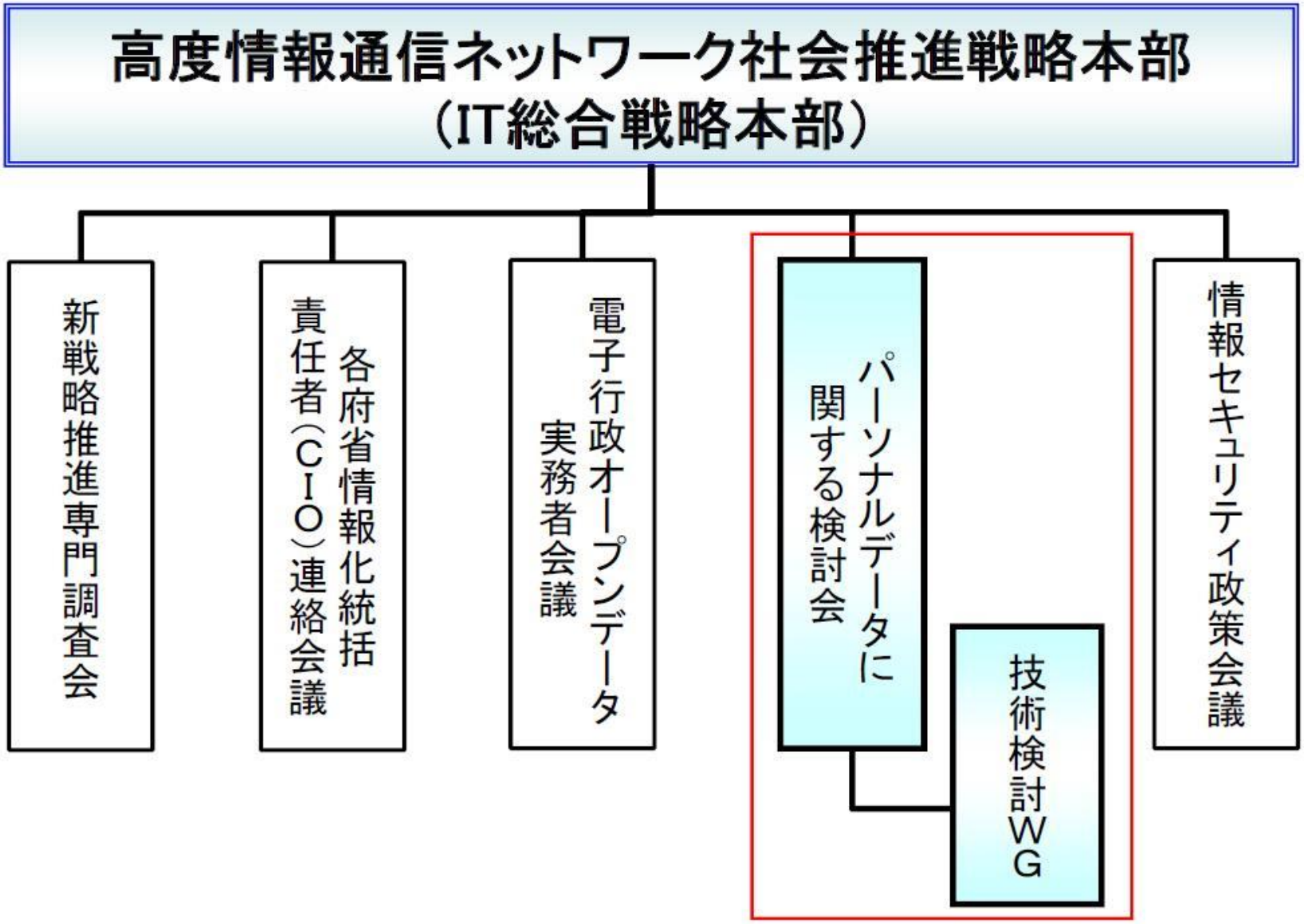
「世界最先端ＩＴ国家創造宣言」（平成25 年6 月14 日 閣議決定）

セコムIS研究所 Intelligent Systems Laboratory

- Ⅲ.目指すべき社会・姿を実現するための取組
- １．革新的な新産業・新サービスの創出と全産業の成長を促進する社会の実現
- （１）オープンデータ・ビッグデータの活用の推進
- ② ビッグデータ利活用による新事業・新サービス創出の促進
- （中略）
- 個人や機器・インフラの行動・状態等が日々刻々とIT により流通・蓄積されており、この「ビッグデータ」の利活用による、付加価値を生み出す新事業・新サービス創出を強力に推進する。
- （中略）
- また、速やかにIT 総合戦略本部の下に新たな検討組織を設置し、個人情報やプライバシー保護に配慮したパーソナルデータの利活用のルールを明確化した上で、個人情報保護ガイドラインの見直し、同意取得手続の標準化等の取組を年内できるだけ早期に着手するほか、新たな検討組織が、第三者機関の設置を含む、新たな法的措置も視野に入れた制度見直し方針（ロードマップを含む）を年内に策定する。
- （中略）

パーソナルデータに関する検討会

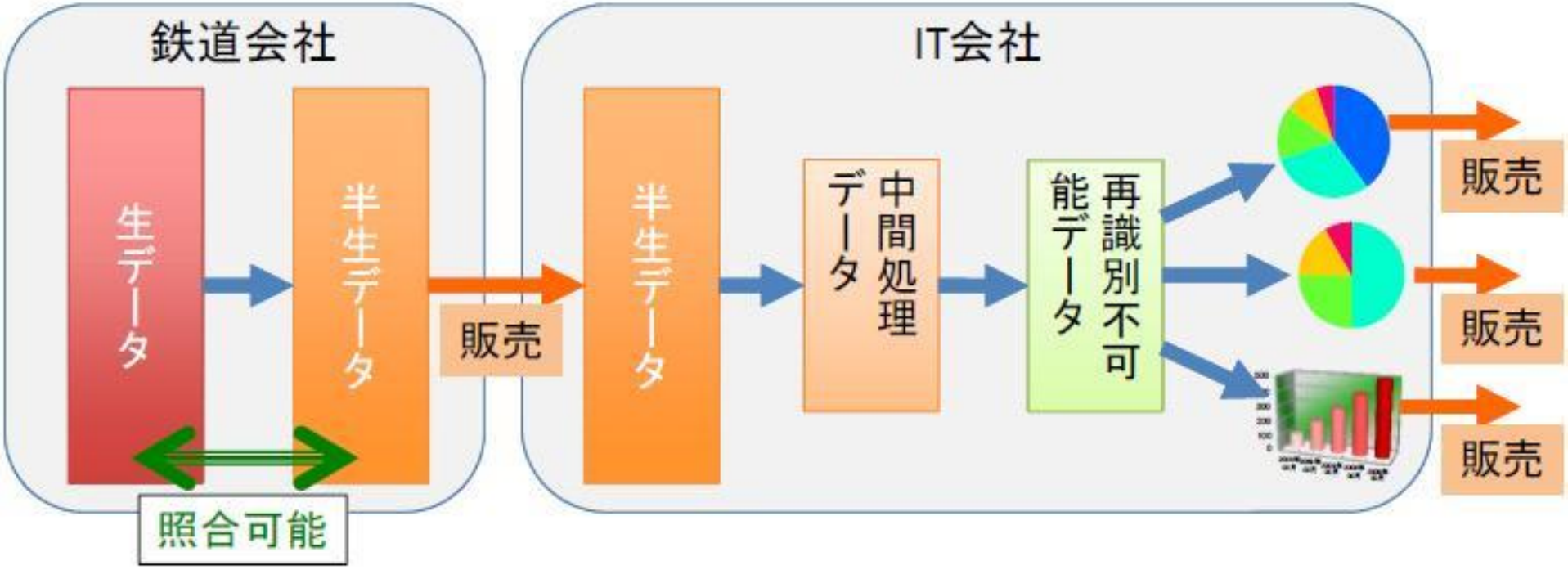
セコムIS研究所
Intelligent Systems Laboratory



パーソナルデータに関する検討会
第２回検討会での鈴木正朝構成員の提出資料

セコム IS研究所 Intelligent Systems Laboratory

モデル1： ガイドライン対応
モデル2： 立法措置で実現

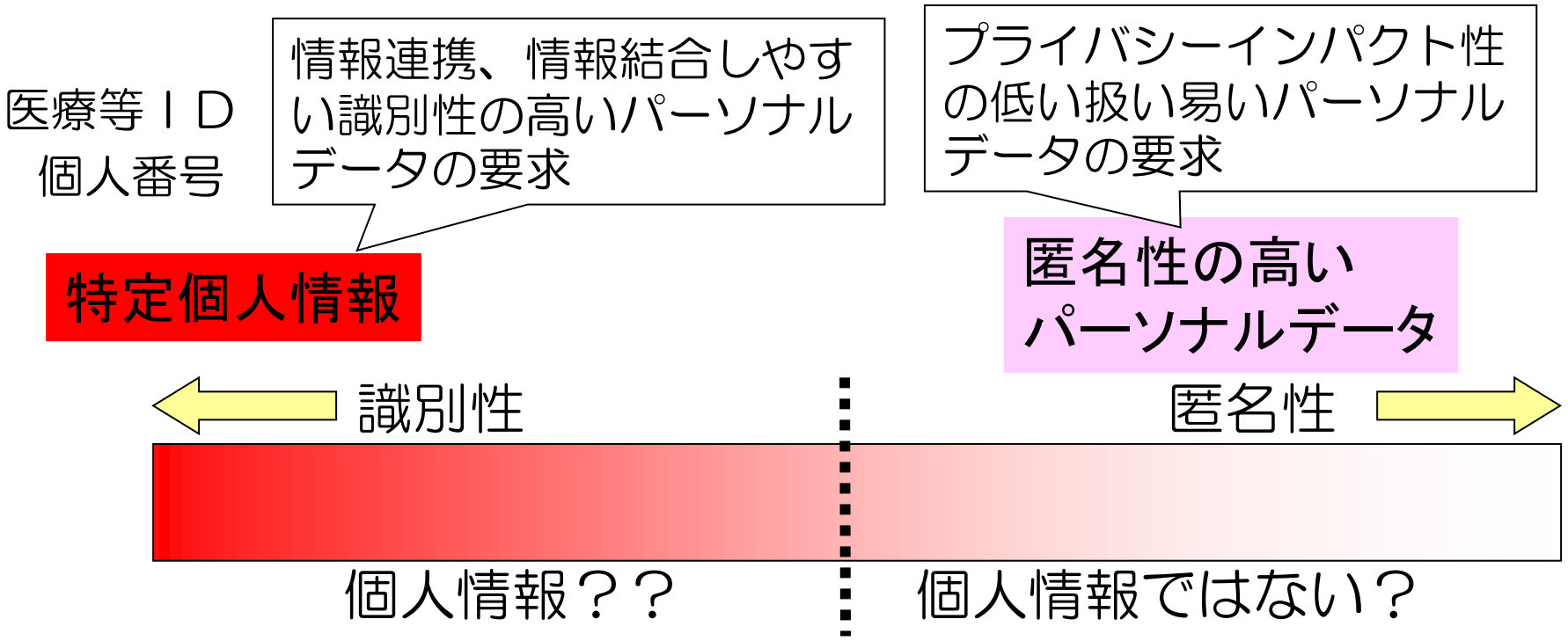


＊ 某交通カードの乗車履歴データ提供事案 （現行法制下で違法）

匿名化の議論 – 匿名化は定義できるのか？

セコムIS研究所 Intelligent Systems Laboratory

- 第３者提供時の同意を不要にしたい？という「匿名情報」の要求？？？
- 現実は、
  - 匿名性は、グラデーション
  - 背景知識等による再識別化の問題
  - ビッグデータ時代 ＝ 多くの背景知識が容易に入手可能な時代へ？



医療等分野のパーソナルデータの利活用の特性

セコム IS研究所 Intelligent Systems Laboratory

- 利活用は公益性の性格が非常に強い（社会的合意性？）
- 有益な２次利用のためのパーソナルデータの要求
  - 医療情報の２次利用の必要な情報の粒度（　高い匿名性との相反する要求？）
    - 個人の連結可能(匿名）性が重要
    - 追跡性、トレーサビリティ（不正防止性）、状況特定性、地域性等の要求
  - データ集積・結合の要求（集積・結合後の２次利用？）
    - 集積：　医療機関等の1次パーソナルデータホルダーの規模が小さい
    - 結合：　健康診断票とレセプトの結合等。個人番号、医療等ID(仮称）等によるデータ結合の要求
- データ利活用のための条件　（ 匿名化の意味も多様に解釈されている ）
  - 倫理委員会や第三者機関による審査等を持つものが多い
    - 無秩序なデータの利活用を防ぐため、利用する情報や公開の方法は、倫理委員会等で評価される（こうした組織では、技術的評価は難しい？）
  - 個人情報と匿名情報の境界線は曖昧であり「個人情報保護法」の適用範囲も曖昧だが、これはユースケース毎のガイドライン、指針等でカバーしている
  - 医療等分野全体としては、医療等分野の特別法（特例法）の検討がある
- 同意との関係（　同意だけに頼らないことも要求されている？　）
  - 本人同意の原則をそのまま適用することが困難な場合も多い

利活用の特性を踏まえた第３者提供の考察

セコムIS研究所 Intelligent Systems Laboratory

- 「公表物」、「制約のないデータ販売」（コントロールの利かないパーソナルデータ）
  - 高い匿名性の基準があるべき
- データの利活用のための処理を行う組織等（コントロールの利く組織でのパーソナルデータ）への第３者提供（？）
  - 利活用ができないほどの匿名化されたパーソナルデータしか扱えなくなるのでは意味がない（成果物の有用性とのトレードオフがある）
  - ある程度の匿名性を高めたパーソナルデータ（例えば、連結可能匿名化）は、リスクインパクトを減らすために有効
    - そのための匿名性のレベルを測る「ものさし」は重要（匿名化ではなく）
  - 匿名性のレベルを含め、その他の要素（機微性、組織の信頼性（ガバナンス等）、技術的信頼性（情報セキュリティ）、再識別化禁止等の契約での縛り）等の総合的なリスク評価（の指標）が重要なのではないか（ＰＩＡのガイドライン等？？）。
    - 第３者提供先の技術的な要件としては、医療情報（匿名化情報ではなく）の医療機関から委託先への要件になる「医療情報システムの安全管理に関するガイドライン」が参考になる。

利活用の特性を踏まえた第３者提供の考察

セコムIS研究所 Intelligent Systems Laboratory

主体者

同意等

１次データホルダー

第3者提供

第３者提供を受ける組織

第3者提供

第３者提供を受ける組織（３次利用）

公開物

•高い匿名性の基準
•（機微性のレベル）
•（同意のレベル）

•成果物の目的の公益性等
•同意のレベル
•再識別化禁止などの制約のレベル
•データの機微性のレベル
•データ量？
•組織の信頼性のレベル
•組織内でのデータの技術的安全性のレベル
•データの匿名性のレベル
•＃（匿名化以外の）プライバシー保護技術の利用？

非技術的課題
（非技術的評価）

技術的課題
（技術的評価）

セコムIS研究所
Intelligent Systems Laboratory

まとめ？？

まとめ

セコムIS研究所
Intelligent Systems Laboratory

- 番号制度は、紙文書、紙台帳前提の制度の時代から、デジタル技術、デジタルデータ前提の時代の制度への流れになる
  - 「パーソナルデータに関する検討会」での議論も同じ
- 個人情報の保護のための情報セキュリティではなく、個人情報の保護と利活用のための情報セキュリティへ

セコムIS研究所
Intelligent Systems Laboratory

参考

2010年10月22日
第18回 ISSスクエア水平ワークショップ
「国民ID時代の個人識別とプライバシー保護の課題 」

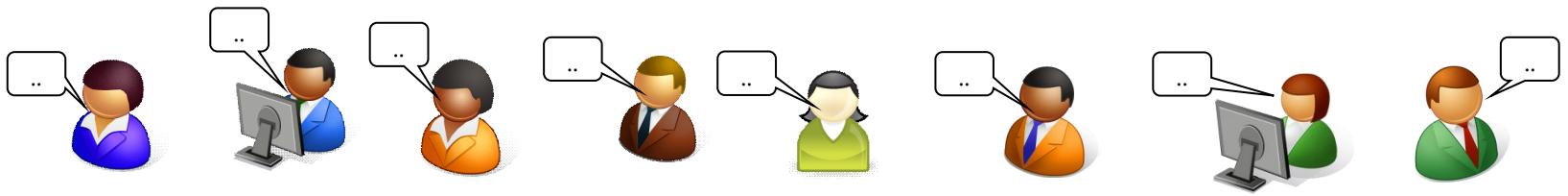
番号制度等における
セキュリティとプライバシーの課題と対応

第18回 ISSスクエア水平ワークショップ
「国民ID時代の個人識別とプライバシー保護の課題 」

番号制度等における
セキュリティとプライバシーの課題と対応

2010年10月22日

セコム(株)IS研究所　松本　泰



49

番号制度等におけるセキュリティとプライバシーの課題と対応

- 番号制度等の導入が急がれている。こうした番号制度等の導入は、行政機関間等において電子化された個人情報を転送により、個人にとっての個人情報の利活用や、行政機関にとっての業務の効率化等といった狙いがある。
- これは、更に効率的で透明性の高い社会の構築へとつながる。その一方、行政機関による個人の不正な監視や、恣意的な個人情報の名寄せを防ぐ必要がある。ここでは、番号制度等の導入に伴う、こうしたセキュリティとプライバシーの課題を整理し、その対応について考察する。

住民票をオンライン取得したい.

国民総背番号制、絶対反対！！

セコムIS研究所 Intelligent Systems Laboratory

「番号制度」「国民ID制度」等に関する様々な議論
セキュリティとプライバシの課題の解決以前に
そもそも何を目指しているのか分からないという問題？

財務省

税の公平性のために納税者番号が必須

どこでもMyカルテの実現で国民ID制度との関係は？

電子私書は？

社会保障カードの実証実験では。。

厚生労働省

国家戦略室

社会保障・税に関わる番号制度

国民ID制度と国民IDコード

内閣官房　IT室

電子行政に関するタスクフォース

行政の効率化には、共通番号が必要

次世代電子行政サービス基盤は？

総務省

原口5原則

民間IDを活用すべき

電子政府推進対応WG

第3者機関を設立すべき

個人情報保護専門調査会

韓国の国民ID制度－公認証明書

セコムIS研究所 Intelligent Systems Laboratory

- 公認証明書 （ accredit certificate ）
  - 韓国の電子署名法に基づく**民間が発行**する「公認証明書」
    - 「公認認証局」が発行する「公認証明書」による「公認署名」
  - 毎年2000万枚以上の公認証明書の発行（有効期間１年）
- 記載内容
  - 氏名と仮想識別番号(VID)が記載
  - 仮想識別番号(VID)　　RFC 4696
    - VIDは、住民登録番号等から生成
  - #やはり住所等は記載されない
- RFC 4696　Subject Identification Method (SIM)
  - PEPSI = H(H(P || R || SIItype || SII))
  - PEPSI – Privacy-Enhanced Protected Subject Information
  - SII　– Sensitive Identification Information (e.g., Social Security Number).

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

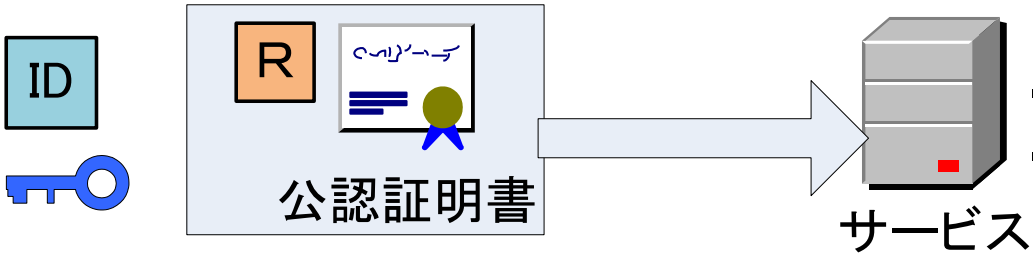
RFC 5636　Traceable Anonymous Certificate (TAC)

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

韓国の国民ID制度　公認証明書の利用

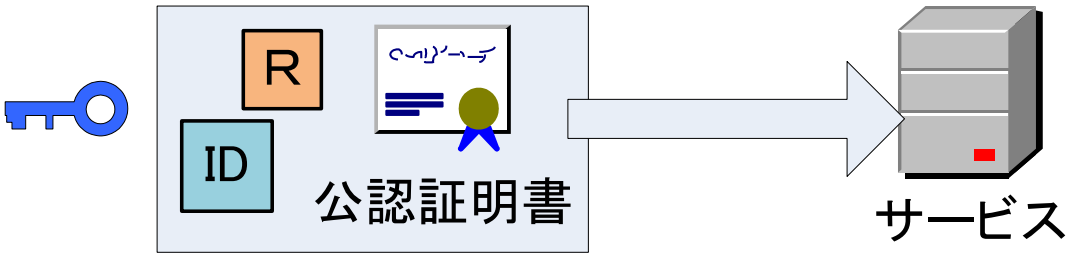
セコム IS研究所 Intelligent Systems Laboratory

(1) サービス側が「住民登録番号(ID)を知っている場合」 一般の行政サービス：



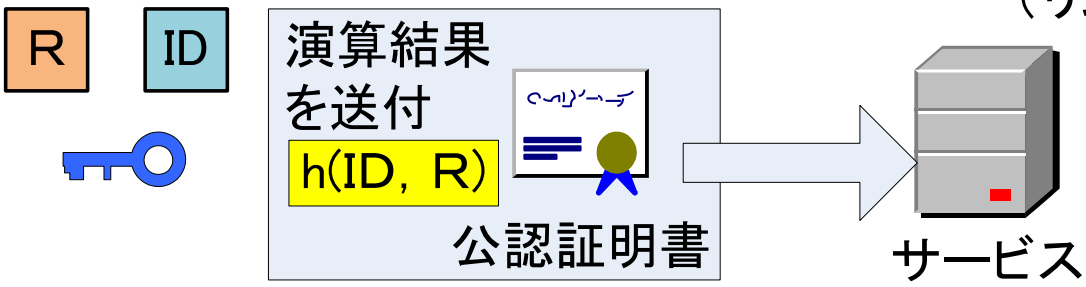
・公認証明書からVIDを取得
・VID=h(h(ID，R))を検証

(2) サービス側が「住民登録番号(ID)を必要とする場合」



・公認証明書からVIDを取得
・VID=h(h(ID，R))を検証

(3) サービス側が「住民登録番号(ID)」必要としない場合
（リンカビリティは証明できる）



・公認証明書からVIDを取得
・VID=h(h(ID，R))を検証

ID 住民登録番号　R 公認証明書発行時に生成する乱数　署名鍵 プライベート鍵

各国の制度の比較

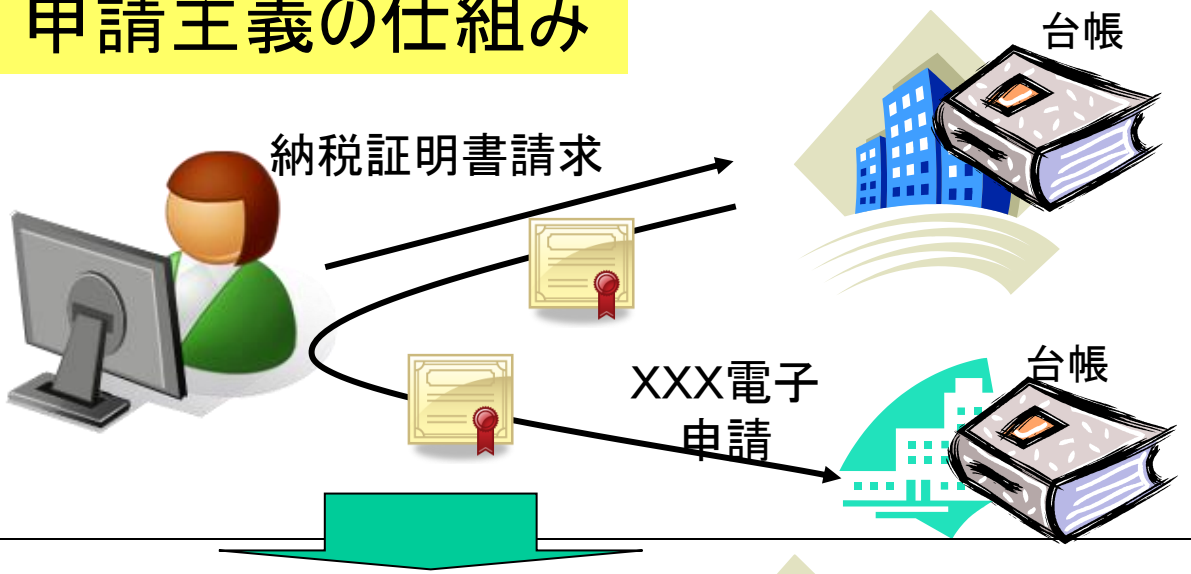
セコムIS研究所
Intelligent Systems Laboratory

	エストニア	デンマーク	韓国	日本
制度を横断する識別子等	PIC: Personal Identification Code	中央住民登録番号（ CPR番号）	住民登録番号	基本4情報を利用？
対面としてのクレデンシャル	・国民IDカード ・名前、PICを証明	・医療保障カード ・名前、CPR番号を証明	・住民登録証 ・名前、住民登録番号を証明	・運転免許証、印鑑登録証他 ・住基4情報等を証明
オンラインとしてのクレデンシャル	・国民IDカード ・PICを証明 ・（その他　バンクID，モバイルID）	・ DanID/NemID ・ PIDを証明 ・間接的にCPR番号を証明	・公認証明書 ・ VIDを証明 ・間接的に住民登録番号を証明	・JPKI等 ・住基4情報を証明
個人情報保護法	・ EU準拠 オムニバス方式 ・第3者機関あり	・ EU準拠 オムニバス方式 ・第3者機関あり	・(要調査) ＃行政安全部が大きな役割を果たしている？	・セグメント方式 ・第3者機関なし
制度を横断する情報交換基盤 情報交換方法 同意確認？	・ X-ROAD ・オンラインデータ交換	・（要調査）	・行政情報共同利用センター ・オンラインデータ交換	・なし？ ・書面、電話？

申請主義からプッシュ型の行政サービスへ

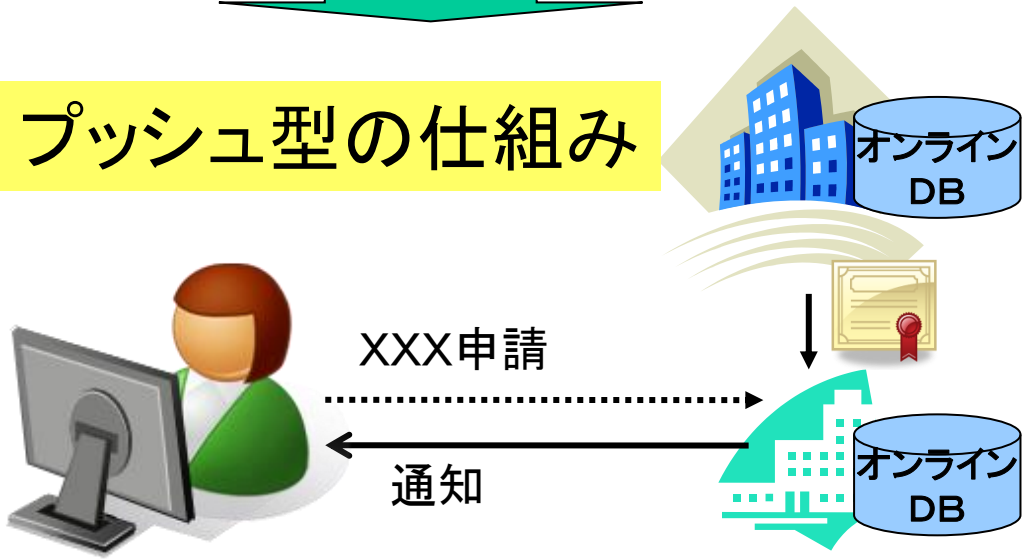
セコム IS 研究所
Intelligent Systems Laboratory

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



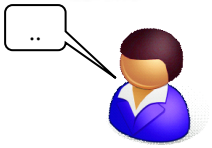
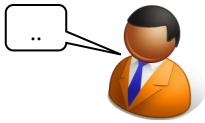
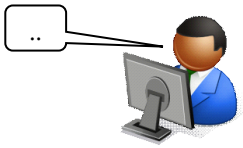
- 欧州の電子政府等では、行政のバックオフィスの連携ができなくてはならないというのが現在のトレンド
- 複数の組織における一意識別と認証 → 番号制度、国民IDの議論
- 個人情報の転送のフレームワーク → 番号制度、個人情報保護法等の議論

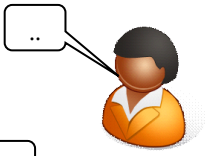
***結局のところ、2001年頃に目指した世界最先端電子政府は、100年前からのシステムの電子化だったのでは？

プッシュ型の行政サービスのための制度と基盤？

セコム IS研究所 Intelligent Systems Laboratory

- (1) 個人情報連携のための個人の一意識別等 － **番号制度**？？
  - 「制度」を超えた識別子
  - 番号、識別子（identifier）だけでなく、基本的な属性の管理
  - 識別子自体の分散や利用範囲の議論
- (2) 個人の身元証明、本人確認 － **国民ID制度**？？
  - オンライン、オフラインでの本人確認のための「ID=クレデンシャル?」
  - **国民IDの在り方**、**民間IDの活用**などの議論
  - 「**番号制度?**」との関係？
- (3) 個人情報を移動する際の原則の確立
  - 個人情報保護法などの制度的なフレームワーク
    - 第3者機関の設立？などの議論
    - **同意確認のフレームワーク**等？
- (4) 個人情報を連携させるための情報交換基盤
  - データ連携を可能とする電子行政の共通基盤？？
  - エストニアのX-ROAD,ベルギーのクロスロードバンク、韓国の行政情報共同利用センターなど



オンライン・オフライン利用する「クレデンシャル」の課題

セコム IS研究所 Intelligent Systems Laboratory

- 行政サービスにおける「識別・番号」との関係の整理
  - アサーションや証明書で何を証明するのか？または何を関連付けるのか？
    - 現状の行政サービスの一般的な識別子は「基本4情報」
    - → 番号制度、国民ID制度の課題
- 認証のための保証レベルの確立（ Level of Assurance for Authentication ）
  - サービスのリスクに応じた認証レベルの提供
  - （米国の)OMB M04-04 連邦政府機関向けの電子認証にかかわるガイダンス
    - 4つのレベルを定義（2003年12月）
  - 電子政府検討会の「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」 これが重要
- 身分確認基準の確立 – Evidence of Identity Standard
  - ニュージーランド、カナダ・ブリティッシュコロンビア州などの事例がある
  - オンライン、オフラインの整合
    - 現状の対面の行政サービスにおいてもバラバラ
  - 民間に対する制度である「犯罪収益移転防止法」、「電子署名法」等での本人確認などとの整合
- 行政の基本的な登録情報（戸籍、住民基本台帳等）が、社会のトラストアンカーとして機能し、クレデンシャルの発行に有効に利用できること。。

番号制度等における
セキュリティとプライバシーの課題と対応

セコム IS研究所
Intelligent Systems Laboratory

- 番号制度等（番号制度、国民ID制度）の目標は「国民の利便性」「行政サービスの効率化」など（更に社会保障分野、公共分野への展開？）
- こうした目標を達成するための「セキュリティとプライバシーの課題と対応」を考えていく必要がある。
- 全体として
  - （コストや利便性も考慮した）適切な情報セキュリティ
  - （個人情報の利活用を前提とした）適切なプレイバシー保護
- クレデンシャルとしての課題と対応
  - オンライン・オフライン利用する公的なアイデンティティを証明する「クレデンシャル」このクレデンシャルの適切な情報セキュリティの確保
  - 証明する「識別子」の扱いや範囲についての社会的な合意？
- バックオフィス連携の課題と対応
  - 個人情報の処理に関する制度的なフレームワーク
  - （個人）情報交換基盤における情報セキュリティ

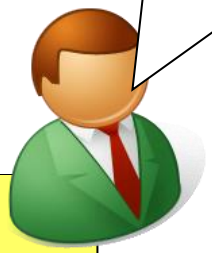
2010年現在の状況？

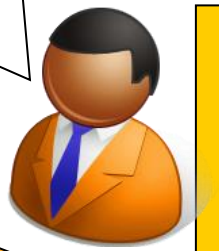
セコム IS 研究所
Intelligent Systems Laboratory

"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

•今後の社会？

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？

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

認証基盤、アイデンティティ管理基盤（行政、民間）

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