

番号制度で広がる社会基盤と 多様なサービス

東京工業大学 像情報工学研究所

大山 永 昭

実現すべき社会

- より公平・公正な社会
- 社会保障がきめ細やか、かつ的確に行われる社会
- 行政に過誤や無駄のない社会
- 国民にとって利便性の高い社会
- 国民の権利を守り、国民が自己情報をコントロールできる社会

番号制度の実施による変化

- (1) 個人、法人等の番号導入
- (2) 情報提供ネットワークシステムの構築
- (3) 番号通知カードの送付
- (4) マイナポータルの実現
- (5) 希望者に対する番号カードの交付

個人情報保護について

- 課題認識

- 知られたくないからコントロール権へ(OECD8原則)
- 個人情報の利用は、利便性や便益を提供する
- 一方、個人情報の漏洩は防ぐべきである

- 個人情報保護法の役割

- 個人情報の利用を妨げるのではなく、安全・確実な利用を可能にするためのルール作りが必要 道交法と基本的に似ている
- 個別の個人情報の重要性は人により異なる

民事訴訟が原則 刑事罰ではない

個人情報保護について

- 自主規制と法規制
 - 自主規制が有効に機能する対象
 - 社会的な信用を重要視する個人組織には有効
 - 罰金よりも大きな被害を被る
 - 法規制が有効に機能する対象
 - 社会的な信用を重要視しない個人組織に対して有効
 - 民事訴訟における心象を変える 努力義務違反
- 個人情報を大量に扱う事業者には、行政罰を適用

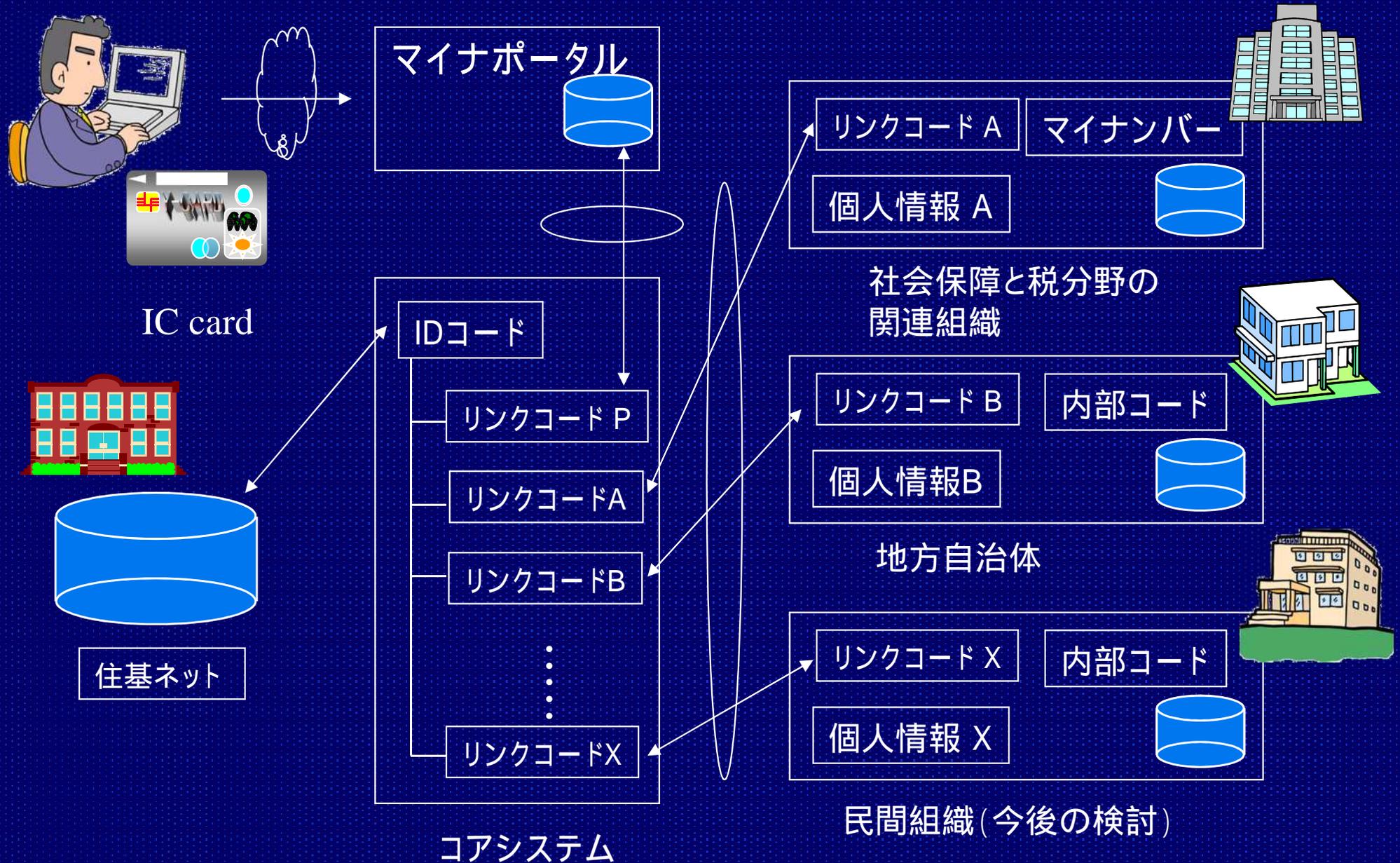
(1) 個人、法人等の番号導入

- 正確なマネーフローを補足するため、個人、法人等に番号を導入
- 個人番号の導入に起因するプライバシー侵害を防止するため、保護策を強化
特定個人情報(番号付個人情報)の定義、第3者機関の設置、直接罰の導入 等
- 個人番号の利用範囲を法律で限定

(2) 情報提供ネットワークシステムの構築

- 番号法で許可されている法定業務に係る個人情報、バックオフィス連携で取得可能とするために構築 住民の手間を削減
- 個人情報の漏洩等による被害の拡大(情報提供ネットワークの構築による脅威の増加を避ける)と、コアシステム運用に係る内部犯罪等を防止するため、リンクコードを導入
- 法定業務をホワイトリスト化し、それ以外の情報提供を技術的に防止
- 全ての情報提供を記録し、マイナポータル経由で確認可能に

情報提供ネットワークシステムの概念図



(3) 番号通知カードの送付

- 平成27年10月から、全ての住民に送付
- 氏名、住所、番号等が記載された紙カード
- 源泉徴収業務等において正しい個人番号を記録するため、通知カードは単独ではなく他の顔写真付き公的書類等と組み合わせて確認することと規定

留意点：誤配送が無いよう十分な注意が必要

(4) マイナポータルの実現

- コアシステムに記録される情報提供履歴を本人が確認できるための個人向けポータル
- 中間サーバに保持される個人情報の内容確認機能の提供
- 機微な個人情報含むため、マイナポータルへのアクセスには番号カード(ICカード)の利用を想定
- 利用者に合わせて極め細やかな情報提供を実現

(5) 番号カードの交付

- 平成28年1月から希望者に交付
- 住基カードの発展版として位置付け
- 拡張されたJPKI(電子署名と利用者証明)を標準サポート 2組のPKIを利用
- 自治体による条例利用領域をサポート
- 発行日から10回目の誕生日まで有効(20歳以上)
- 現実、及び電子空間の公的身分証明書になる

税分野での利用

- 正確なマネーフローを補足するため、源泉徴収票等に個人、法人等の番号を記載
- 番号の正確性の確保
 - 法人等の番号は、公開された手段により確認
 - 個人番号は、番号通知カードと顔写真付き公的証明書
の組み合わせ等で確認
顔写真付きの身分
証明書に番号を記載
番号カードを交付

社会保障分野での利用

- 所得に応じた給付を確実に行うため、社会保障分野での現金給付事務で利用
- 健康保険の被扶養者認定等に要する所得情報等をバックオフィス連携で入手 情報提供ネットワークの利用
- 身体に係る機微性の高い医療情報(現物給付)分野では、個人番号の利用を禁止 医療等番号の導入は、別途検討

個人番号の利用範囲と留意点

- 利用範囲

A: 納税

B-1: 税+社会保障分野における現金給付

B-2: 上記に加えて、現物給付 医療等IDの導入

C: 官民連携 平成30年を目途に検討

} 本法による

- 留意点

- 本人同意を不要とするため、情報提供ネットワークシステム等を実現
- 個人情報保護法の改正準備が進められている

原則、本人同意が不可欠

カード発行の手順(案)

1. 希望者は、申込用紙に顔写真を貼付して自治体に申請
2. 申込者の取りまとめを地方公共団体情報システム機構が実施
3. 4情報を付して、発行を民間に委託
4. 工場で、パーソナル化まで実施
5. カードをロックして、自治体に送付
6. ハガキによる本人への通知を実施
7. 申請者は本人確認書類を持参して自治体窓口へ
8. 対面での本人確認後、ロック解除、PIN入力等を行ってカードを交付

注意点：顔写真のデジタル化は、多くの手間がかかる

電子申請によるカード発行の手順(一案)

1. 希望者は、申込用紙(番号通知カードに貼付)を持って証明写真ボックスへ
2. 申込用紙に印刷されている処理番号を読ませて、写真撮影 電子申請完了
3. 以下同様

留意点: 顔写真はデジタルデータのまま暗号化されて送信、氏名等の個人情報には送信されない

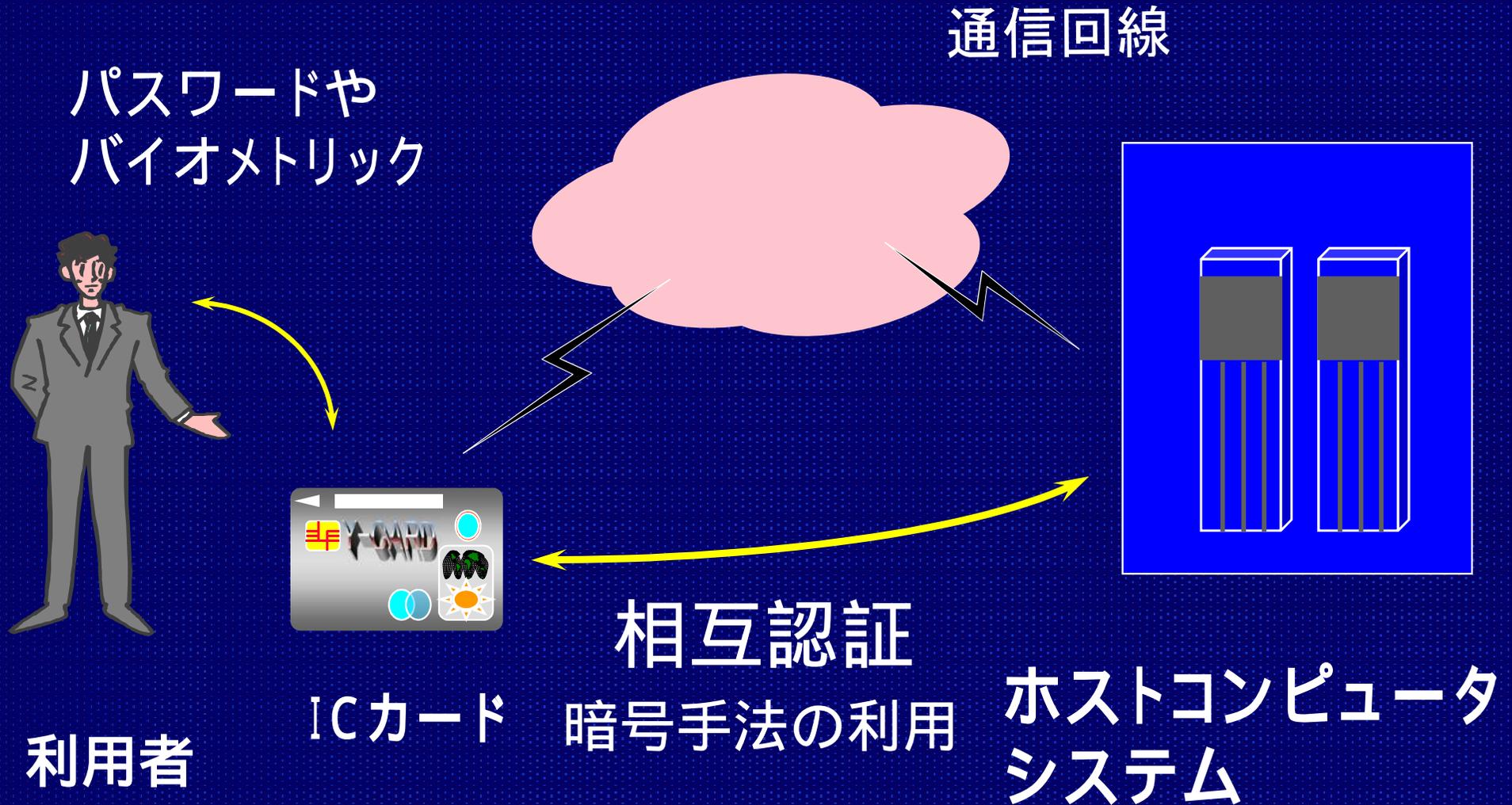
H26年度の実証事業 (総務省)

- 酒田市日本海総合病院にて
 - 国民健康保険の資格確認
 - クレジットカードとの紐付け
- 京都市ケーブルTV
 - ポケットカルテ
- 番号カードは、模擬版 (機能は、ほぼ同じ)
- PIN無し認証を実装
- VTRをご覧ください 

セキュリティ技術の基本

- 現実空間も電子空間も鍵の管理が不可欠
- 電子の鍵の特徴
 - パスワードは4～12桁、暗号鍵は数十から数百桁
 - 金属の鍵と違って、簡単にコピーできる
 - 磁気カードは、コピー防止に無力
 - だから、ICカードに鍵を記録し、読み出せなくする
- 鍵をどう盗るか(破るか)が犯罪者の関心事
- 多数のID, パスワードの安全な管理は大変

本人確認の考え方(オンライン)



暗号手法について

暗号化鍵: K1

おはよう

平文

暗号化处理

&%'?

暗号文

復号化鍵: K2

&%'?

暗号文

復号化处理

おはよう

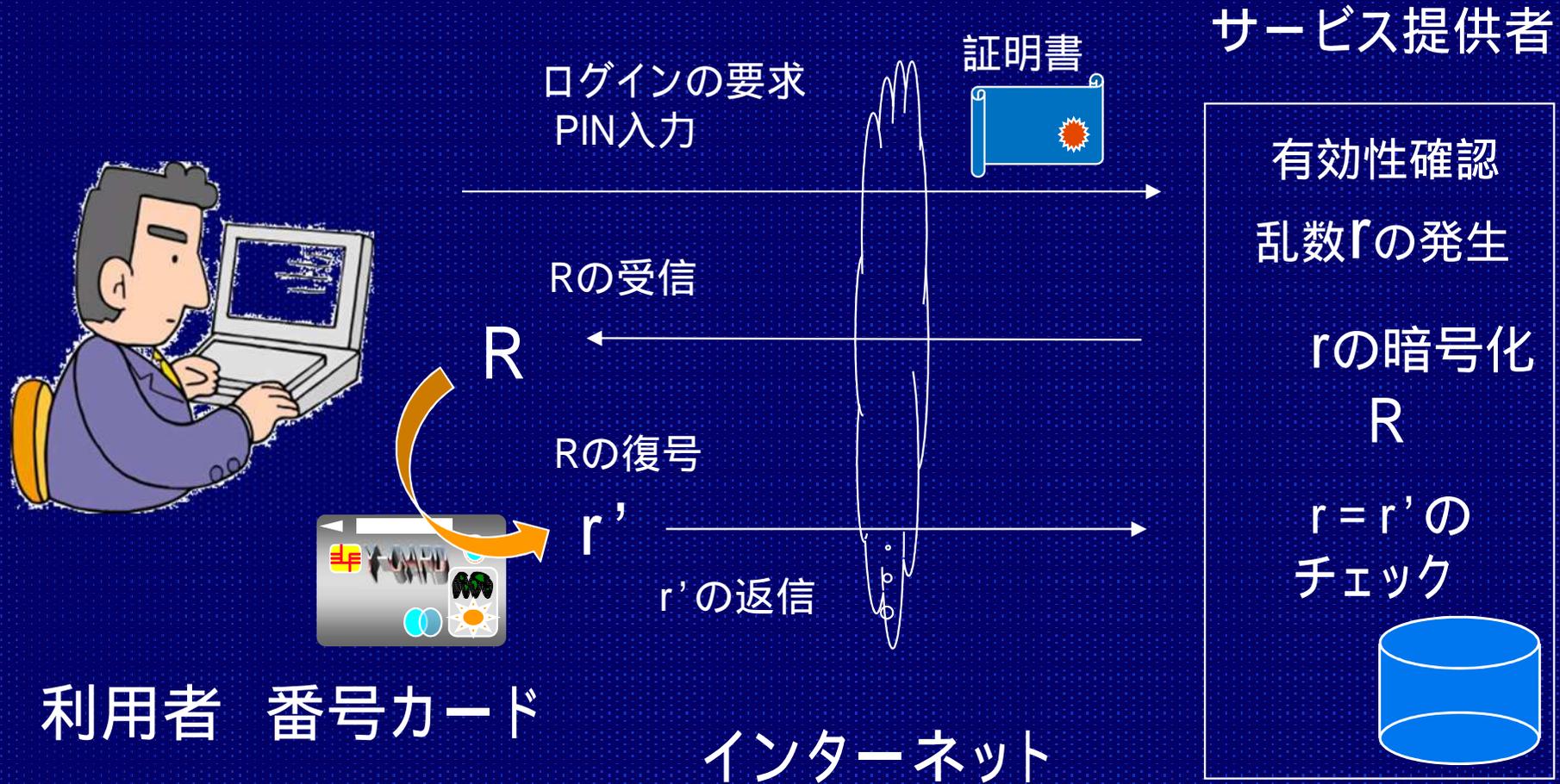
平文

$K1 = K2$; 秘密鍵共有 (対称鍵) 暗号方式

$K1 \neq K2$; 公開鍵 (非対称鍵) 暗号方式

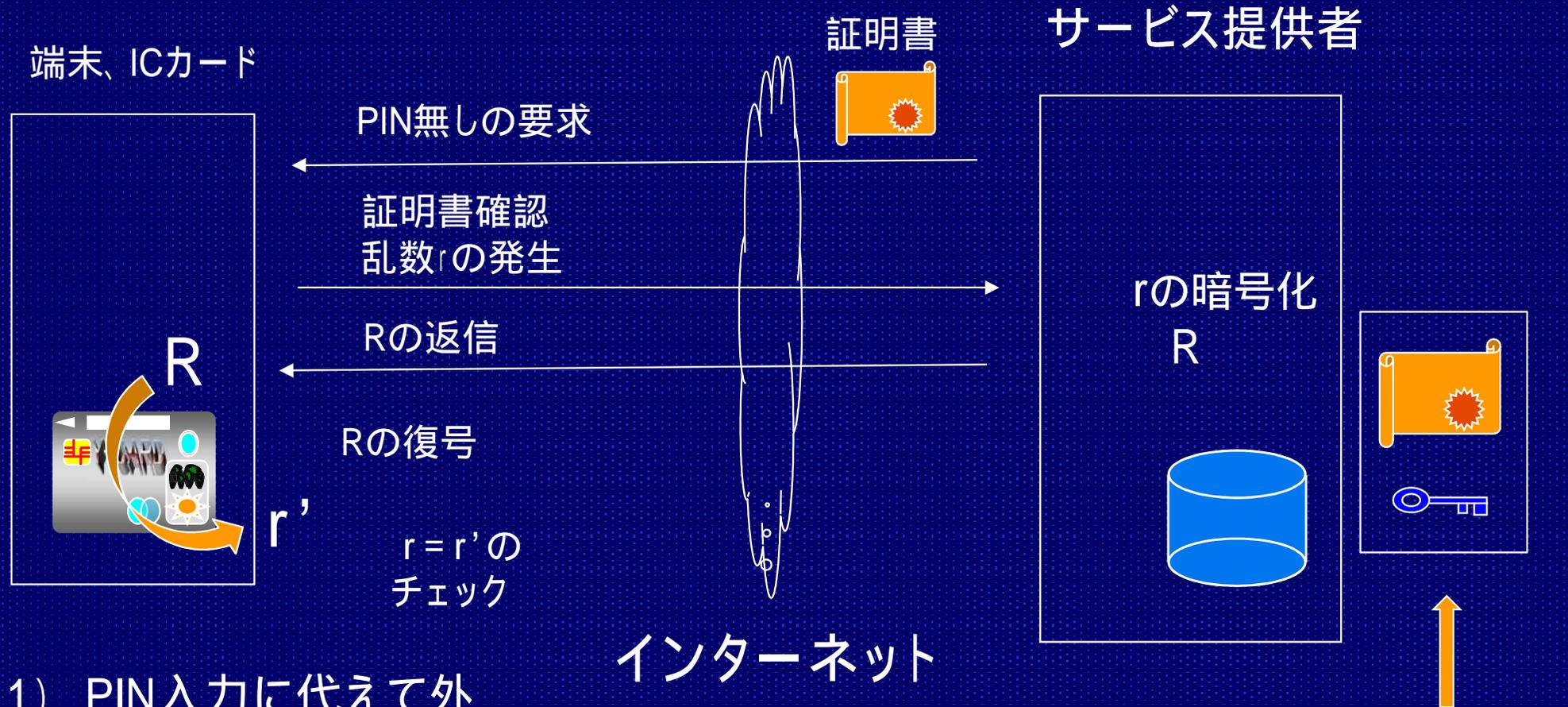
電子署名

利用者証明の利用手順



PIN(パスワード)を入力する必要あり

PIN入力に代る外部認証の概念



- 1) PIN入力に代えて外部認証を実行
- 2) 機関コードを付加して内部認証を実行

J-LISから機関コード付き証明書と秘密鍵を受け取る

番号カードに関する社会的背景

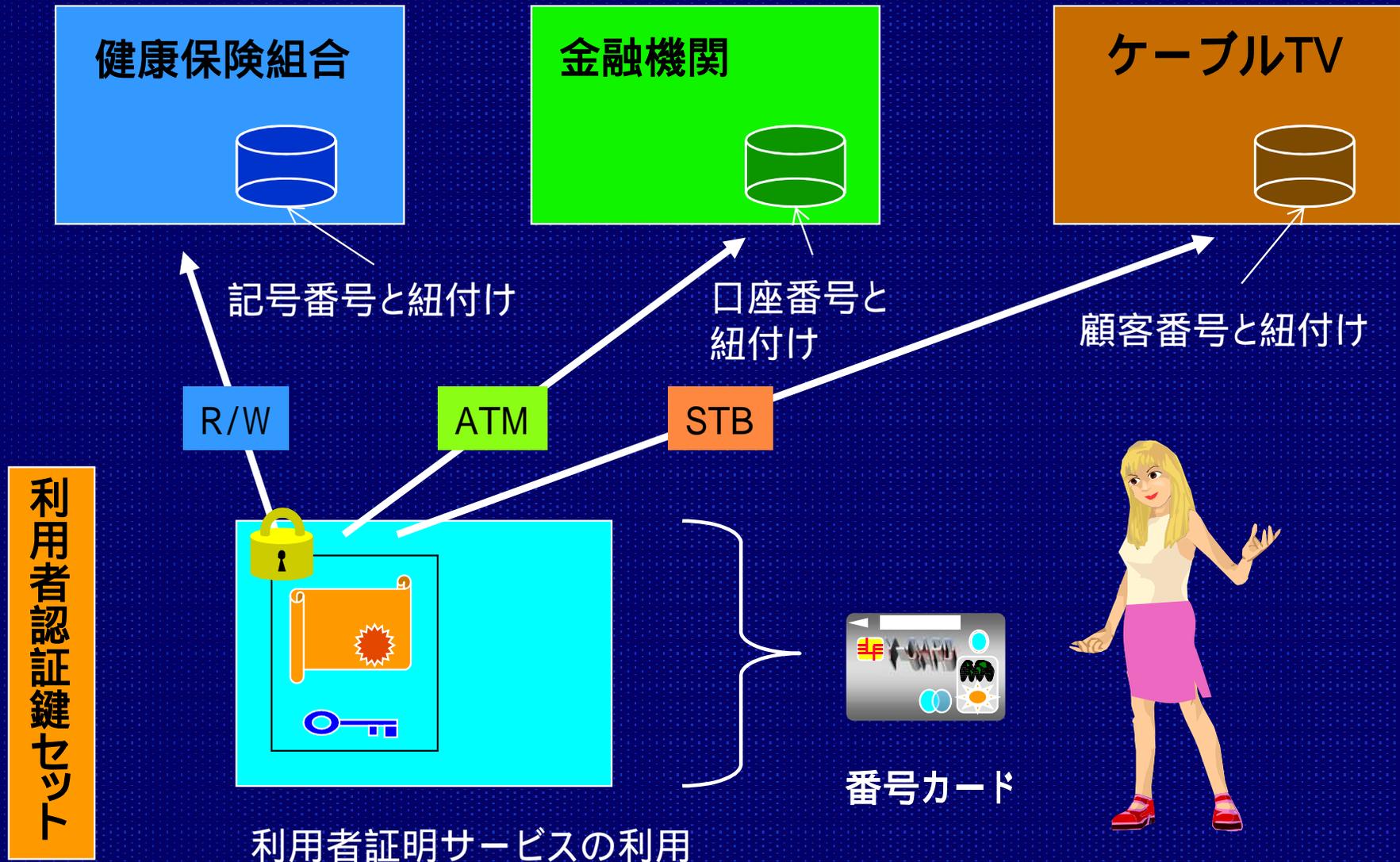
- 社会保障・税番号制度の実施に伴い、H28,1から希望者に個人番号カードの交付が開始される
- 政府与党から、H31年度末(2020年、3月末)までに8700万枚(全住民の2/3)の発行を目指すべきとの提言あり
- H28,1からの15ヶ月で、1500万枚分の予算を確保
- 普及には、官民連携が不可欠 便利な社会を実現

番号カードによる官民連携

- 実現手段
 - 番号カードがサポートするJPKI(電子署名、利用者証明)の利用 マイナンバーの利用ではない
 - 番号カードは身分証明書(現実空間および電子空間)
 - 個人を確実に認証 属性情報を紐付け
- 課題の例
 - 総務大臣による認定手順の決定
 - 想定されるユースケースの明確化

番号カードの多目的利用の例

条例は必要ない



JPKI(公的個人認証サービス)とは

- 現行法
 - Japan Public Key Infrastructure の略で、“電子署名に係る地方公共団体の認証業務に関する法律”に依拠
 - 2004年1月29日にサービスイン
 - 電子証明書の発行枚数累計は255万強(H25年11月)
- 改正法(H28,1~)
 - 個人番号カード向けに改正、民間利用も可能に
 - 既存の電子署名に、利用者証明サービスを追加
 - 署名用証明書には4情報が記載される
 - 利用者証明書は、匿名 ログインの安全性向上

JPKIが提供する主な機能

1. 本人確認

- 写真付きカード券面は対面での身分証明
- 4情報付きの署名用電子証明書は、サイバー空間での本人確認
- 加えて本人の意思確認 否認防止

2. 資格確認

- 電子署名や対面で、初期の紐付けを実施
- 利用者証明用電子証明書のシリアル#がIDに、カード内のPINがPWに対応
- PKIベースの安全なログインが可能に
- 本人の属性情報に応じたサービス提供が可能

番号カードはサイバー・スペース・パスポート

JPKIが提供する主な機能

3. 変更確認 ; 新規機能

- 氏名、住所等に変更があると、電子署名用証明書は失効する
- CRL(失効リスト)から、事象発生を知ることが可能
- 死亡時は、利用者証明書、署名用証明書が同時に失効
- 変更情報の取得
 - 本人に連絡して、変更後の情報を確認する
 - 本人同意の下で、変更情報を提供

例)引っ越しのワンストップ

コンビニ等での証明書の発行について

- 新たな番号カードは、JPKIによる電子署名に加えて認証(電子利用者証明)サービスが追加される
- これにより、ICカードに専用アプリを追加する必要はなくなる
- しかし、この手法では、証明書の有効性確認を行うことが必要になる
- この課題を解決するには、JPKIの利用者認証を代行するサーバーをJ-LISに設置することが有効
- これにより、従来の専用アプリを使っているケースでも、システムの変更を最小限にすることが可能
住基カードによるサービスは継続可能になる
戸籍抄本も取得可能になる予定

コンビニ等での証明書発行の有用性は、極めて大きい

サービス提供者から見た特徴(例)

- 安全性の向上
 - 初期の紐付けには、電子署名(4情報を記載)を利用
 - その後は、匿名の利用者証明書を利用 インターネット利用もより安全に 2つの証明書番号は論理的にリンク
- サービス開始のハードルを下げる
 - ID、パスワードの発行・管理等を必ずしも必要としない
 - システム経費等を削減できる可能性大 実証が必要
- 変更確認が可能に
 - 利用者の氏名等に変更があると、証明書失効リストに載る

利用者から見た特徴

- 多数のID、パスワード(PW)の利用は面倒
 - IDは証明書番号、PWはカードに記録される2つのみ
 - 利用者は、署名と利用者証明の2つのPWを利用
- 便利なカードほど紛失、故障時等が心配
 - 番号カードを子カードにする
 - 親カード(各種保険証等)は自宅等に保管
 - 再発行されるまで、親カードを利用

財布の中に番号カード、親カードは一緒に持ち歩かない

期待される大きな変化

家のTVからマイナポータル等へログインして

- 情報提供に関するログの内容確認
- 自治体からの各種お知らせ(健康診断等)の確認・申込み
- 民間提供の各種ネットサービス(ネットスーパー、医療機関の予約等)の利用

番号カードを持って外出

- 役所、銀行等での本人確認と各種料金の支払い等
- コンビニ等での各種証明書(住民票、印鑑登録証等)の取得等
- 医療機関等での利用 例えば保険証や決済の機能を追加

国民にとって利便性の高い社会

- さらなる可能性
 - 番号カードによるデビット、クレジット、健康保険、介護保険等のサービス 一枚のカードで
- **官民連携**の実現が重要
 - 官による環境整備(インフラを含む)
 - 民間主導による新たなサービス、ビジネスの創出(イノベーション)

更なる展開の例

- 健康保険等の資格確認
- 本人経由の情報提供 電子私書箱等
- 医療等分野での個人番号の導入

医療等ID

健康保険の資格確認

- 年間約200億円の医療費未収金がある
- 保険資格の失効や転記ミスに起因するレセプト返戻が存在 手間と費用回収の遅れが医療機関の負担になっている
- いつ、誰が、どここの医療サービスを受けたかの記録が必要 JPKIが有効
- 番号カードはJPKI付き身分証明書

電子私書箱について

- G2Gの情報提供は、別表の改正により可能
- B2G、B2Bは、本人経由の情報提供が原則
 - 診断書、卒業証明書、住民票等
- 本人から提供されるこれらの情報は、その真正性の確保が不可欠になる
- 真正性を確保するには、電子署名付きの証明文書の利用が有効

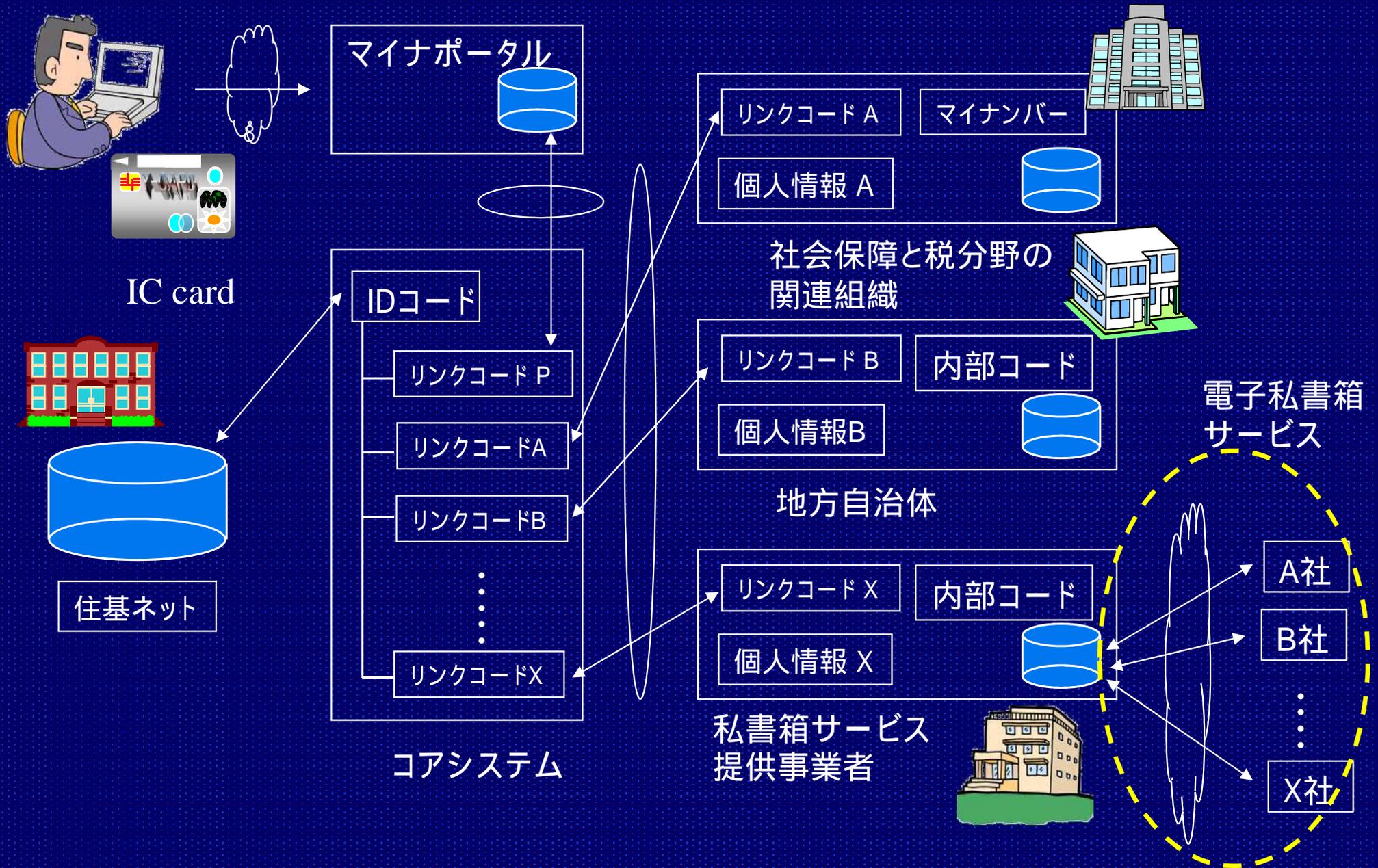
電子私書箱について

- 法人等の電子署名およびその検証手法の普及が不可欠

電子文書の証明力の確保

- さらに郵便と同じように、到達を保証する手段が必要
- 電子化された領収書等の電子文書の確実な受け渡し、
整理が必要 確定申告の完全電子化が可能に
- これらの背景から、電子私書箱の実用化が強く望まれる

情報提供NSと私書箱サービス(私案)



医療等分野における情報連携

- 生涯にわたる健康情報の一元管理の必要性が指摘されている
- 欧米等の先進国では、EHRに関する取り組みが開始されている
- 我が国においても、地域医療の再生等を目的として、地域における医療コミュニティが創生され、コミュニティ内での共通診察券番号等を導入する事例が報告されている
- これらのことから、個人の健康医療情報を時間軸、空間軸を超えて、論理的に紐付けることの必要性は明らか
- この紐付けの正確性の確保は、必須要件
- 医療等情報のセキュリティを考えると、マイナンバー以外の番号の利用が望まれる

医療等IDの在るべき姿

- マイナンバーの利用形態と利用制限等を参考にして、医療等IDのあるべき姿を検討すべき
- 多重付番を避けるためには、悉皆性と唯一無二性を満たした完備なDB等が不可欠
- この条件を満たすものとしては、住民票コード、マイナンバー、リンクコード(コアから新たに発番)があげられる
- 費用対効果を勘案して、医療等IDの現実的な導入策を策定すべき
健康保険の資格確認が先か？！

おわりに

- マイナンバー制度の概要と今後の展開を紹介
- 住民にとっては、番号カードの利便性を高くするが重要
- そのためには、官民連携の実現が不可欠

官による環境整備、民間主導のイノベーション

- 番号カードで資格確認、決済等を可能にすることが強く望まれる

健康保険証、デビット、クレジット等の機能を1枚で

- 医療等分野の情報化の推進

健康保険の資格確認、医療等IDの導入