

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 科学技術創成研究院
社会情報流通基盤研究センター

大 山 永 昭

JPKIの愛称決定

- 公的個人認証サービス
⇒ JPKI (Japan Public Key Infrastructure)
- マイナンバーは、マイナちゃん ⇒ ウサギ
- JPKIは、マイキー (私の鍵) くん ⇒ 犬
- コピーができるマイナちゃん、コピーができないマイキーくん



マイナンバーカードの現状

- 社会保障・税番号制度の実施に伴い、H28 (2016) ,1 から希望者にマイナンバーカードの交付を開始
- H28,1からH29,3までの15ヵ月間、3000万枚分の予算確保
- 本予算では、マイナンバーカードは無料
- 月平均200万枚の発行が必要
- 最新資料では、1000万人を超える方からの申請あり
- 申請数は減少気味 ⇒ 普及促進 ⇒ 民間応用

マイナンバーカードの機能

- ① 身分証明書機能 ⇒ 住基カードの代替えとして
- ② マイナンバーの確認 ⇒ 金銭の受け渡し時における番号確認
- ③ マイナポータル経由での本人情報提供の履歴確認
- ④ 自動化ゲート ⇒ アプリケーションの追加（公務員証の機能）
- ⑤ JPKIを用いた官・民サービスの利用 等

官民連携の実現手段

- マイナンバーカードがサポートするJPKI (電子署名、利用者証明) の利用 ⇒ マイナンバーは使わない
 - マイナンバーカードは、電子身分証明書 (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
 - 属性情報の例
 - 健康保険証、資格、各種権限
- 等

個人番号カードの様式



【おもて面】



【うら面】

総務省の説明文より

JPKI (公的個人認証サービス) とは

- 旧法

- 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

- 改正された現行法 (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、仮名 ⇒ ログインの安全性向上

JPKIの民間利用

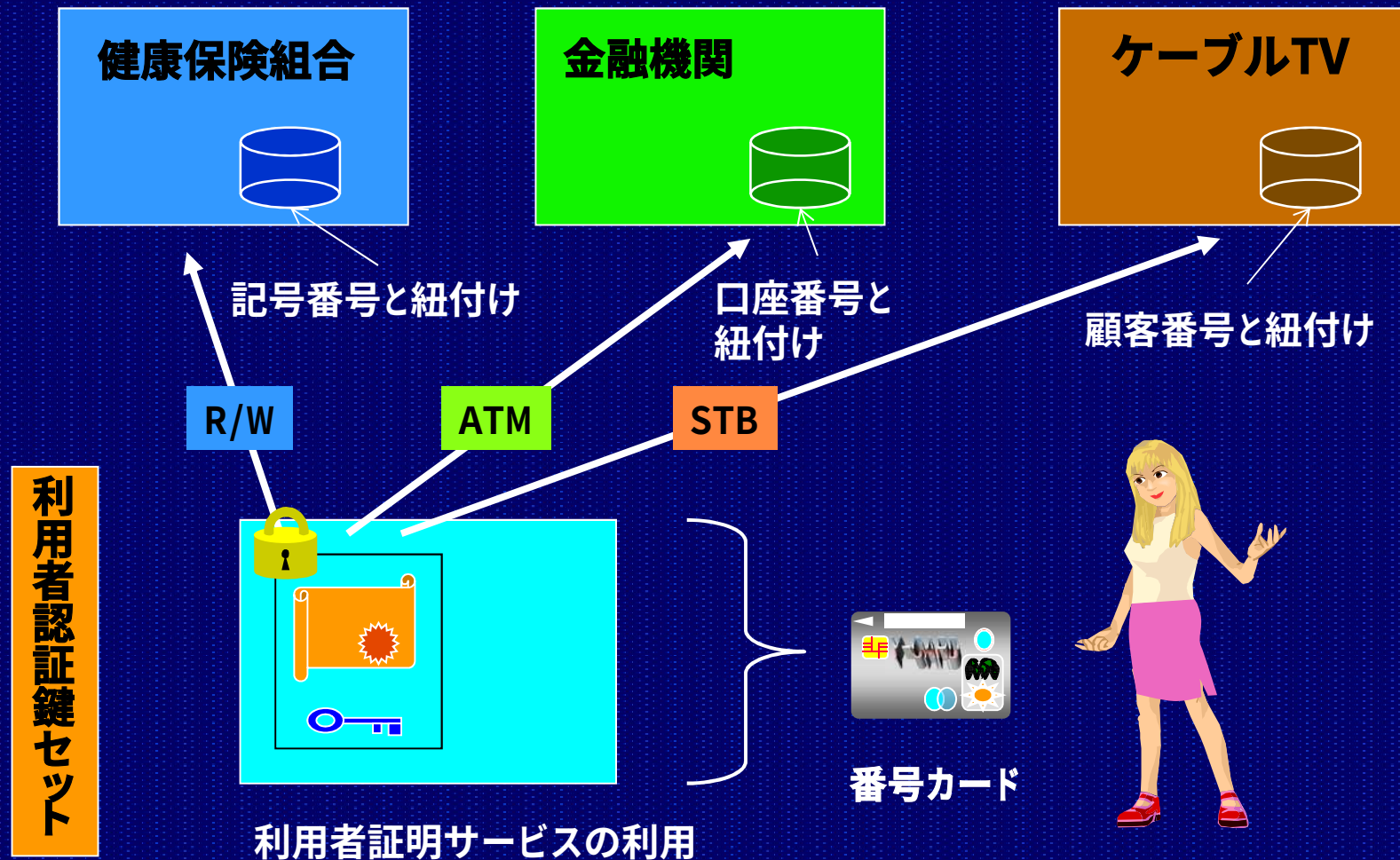
- 電子証明書の署名検証者になる民間事業者は、総務大臣の認定が必要
- H28,5末までに民間5団体が認定を受ける
 - 日本デジタル配信株式会社
 - 一般社団法人 スマートテレビ連携・地域防災等対応システム普及高度化機構
 - 一般社団法人 ICTまちづくり共通プラットフォーム推進機構
 - NTTコミュニケーションズ株式会社
 - GMOグローバルサイン株式会社
- 認定団体は今後増加すると予想されている

総務省の実証事業の例

- 酒田市日本海総合病院 (H26) 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
- 豊田市の一般家庭 (H27)
 - ケーブルテレビを使った手続き
- 横浜スタジアム (H27) にて
 - サーバー上に紐づけた電子チケット
- マイナンバーカードは、H26年は模擬版、H27は本番
- PIN無し認証を実装
- VTRをご覧ください 

番号カードの多目的利用の例

条例は必要ない



利用者から見た特徴

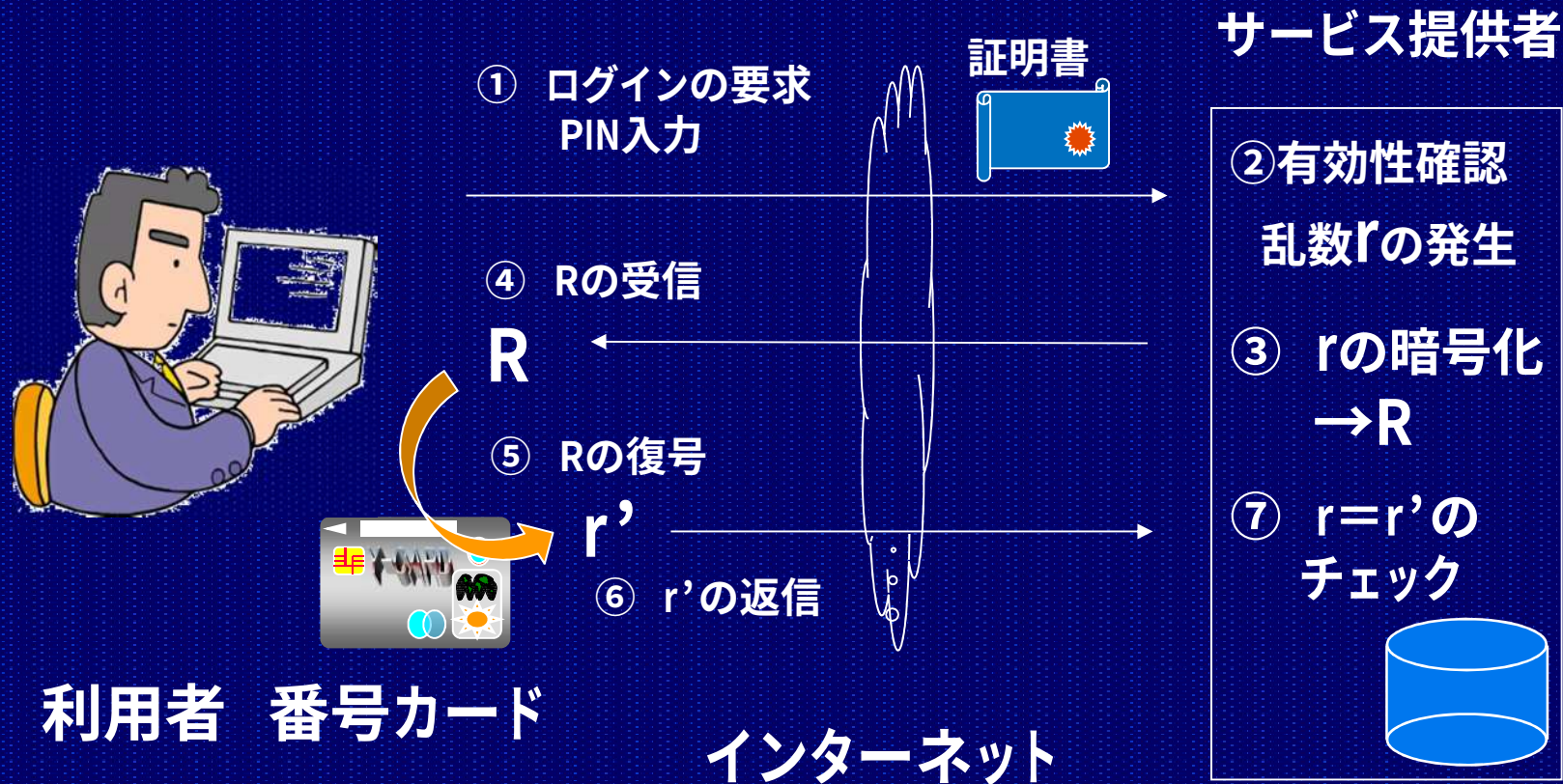
- 多数のID、パスワード (PW) の利用は面倒
 - IDは証明書番号、PW (PIN; Personal Identification Number) はカードに記録される2つのみ
 - 利用者は、署名と利用者証明の2つのPWを利用
- 便利なカードほど紛失、故障時等が心配
 - 番号カードを子カードにする
 - 親カード (各種保険証等) は自宅等に保管
 - 再発行されるまで、親カードを利用

財布の中に番号カード、親カードは一緒に持ち歩かない

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) 等を利用
 - その後は、仮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 ⇒ 認証連携の利用
- 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

利用者証明の利用手順



PIN (パスワード) を入力する必要あり

利用者証明の利便性向上

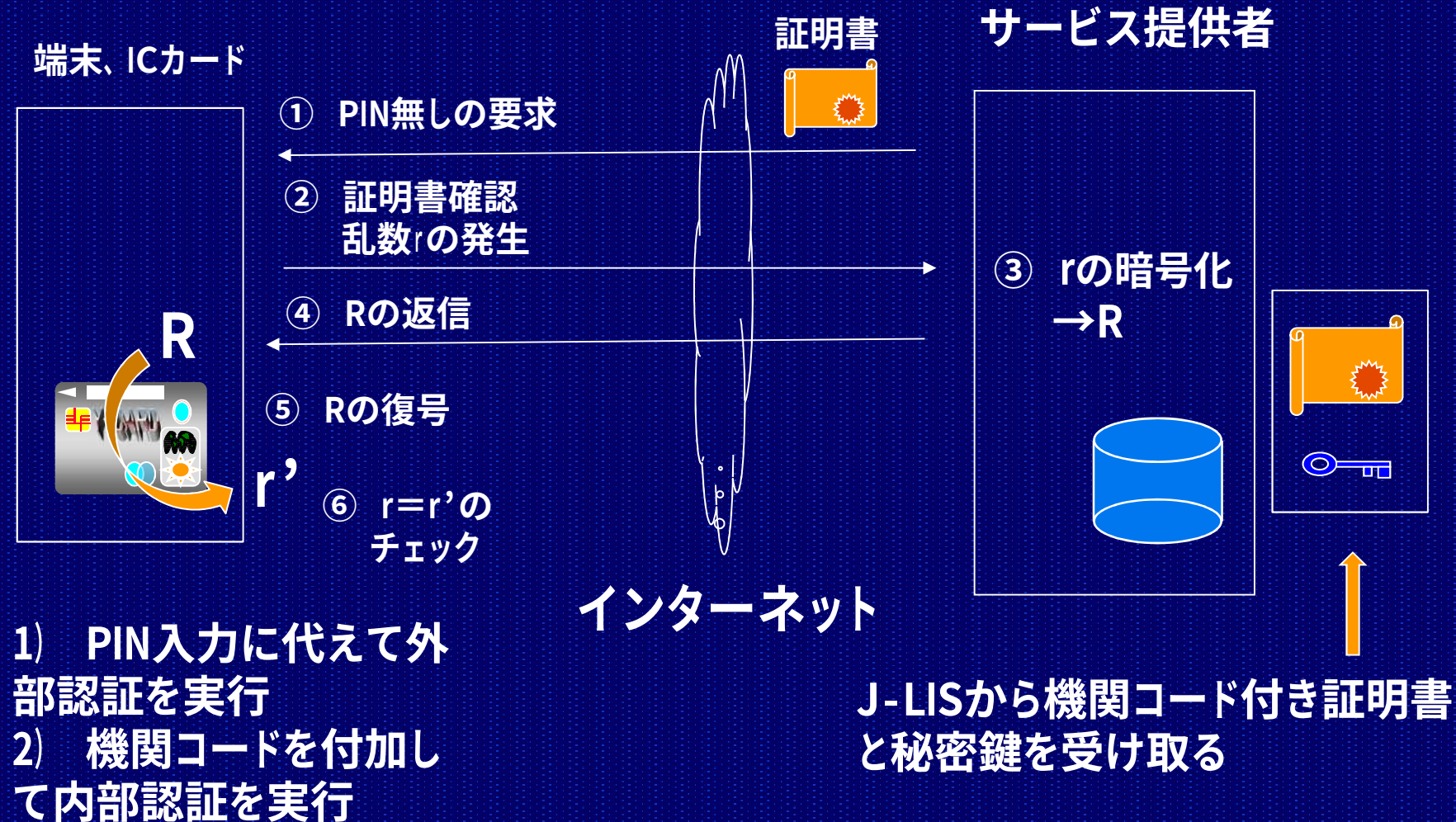
- 課題

- クレジットのサインレス決済、救急情報へのアクセス、健康保険の資格確認等のアプリでは、PIN入力を省略したいとの要望がある
- PIN入力の有無をサーバが検知するとともに、その結果が証明力を持つこと

- 対応策

- カードからサーバを認証 (外部認証) を行う
- PIN入力の有無により、PKIのレスポンスを変える

PIN入力に代る外部認証の概念



マイナンバーカードのメリット

- 確実な本人確認ができるから
 - 個人情報に対する安全なアクセスが可能に
 - 各種証明書（保険証、免許証等）は、サーバで管理可能に ⇒ 迅速な変更が可能に
 - 社会保障関連のサービスを確実に提供
 - 健康情報等も本人の属性情報として確実に紐づけ
 - PIN無し機能により、救急対応も可能に

個人の権利を守る電子身分証明書

マイナンバーカードのメリット

- 本質的な価値
 - 対面での本人確認を経て、識別子を提供
 - 手間、時間、費用のかかる膨大な作業を自治体の実施
 - コピーができる個人番号、コピーができない秘密鍵を配布
- 現実、電子空間での本人確認を確実に実施
 - ⇒ 電子身分証明書 (最高レベル)

コンビニ等での証明書の発行について

- 番号カードは、JPKIによる電子利用者証明サービスが追加されている
- 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
- そのため、JPKIの利用者認証を代行するサーバーをJ-LISに設置
- 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
- 対人口比で50%を超える。店舗数は6万強 ⇒ 導入推進へ

コンビニ等での証明書発行の有用性は、極めて大きい

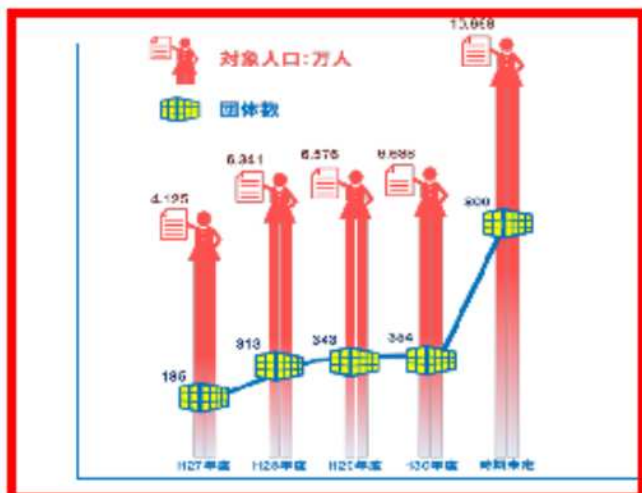
コンビニ交付サービス(未導入団体の導入推進)

20

■ 未導入団体における留意点

- 昨年末：概ね6人に一人がコンビニ交付サービスを享受できる状況
- 3月末：概ね3人に一人が享受できる状況
- 今後：1.1億人が享受できることとなる見込み

⇒大きなメリットを小さなコストで実現できるコンビニ交付サービスを、他に遅れることなく、導入することが期待される



※ J-LISが平成26年度末に実施したアンケート調査結果による。H27年度の団体数は実施済み。

■ 既導入団体における留意点

- 取得できる証明書の追加など、サービスの向上が期待される。
- 特に、新たに可能となった本籍地と住所地が異なる場合でも戸籍証明書が取得できるサービスは、住民の利便性の高いものであり、既導入団体が取得できる証明書に追加することが期待される。
- なお、特別交付税措置(右参照)は、導入当初3年間が対象であるが、この間に取得できる証明書を追加した場合に生じる経費についても措置の対象となる。その積極的な活用が期待される。

導入のための経費と特別交付税措置

- コンビニ交付サービスの導入コストは、標準的な団体の実績平均で約2,100万円※。

- 既存システムの改修費
- 証明書発行サーバの構築費
- 証明書交付センターへの接続費

約2,100万円

※住民票の写し、印鑑登録証明書を対象とする場合、平成22年度～24年度に導入した59団体の事業費を基に算出。

特別交付税措置

対象経費に対し、

2分の1、上限5,000万円の措置

条件：自治体クラウドの推進に資するものであること。

■ ランニングコスト

- ◆ 証明書発行サーバの保守費
- ◆ 証明書交付センターの運営負担金
 - ・町村100万円～指定都市(100万人以上)1,000万円
 - ・一定の時期には、参加団体の増加に伴い、見直しを予定。
- ◆ コンビニ事業者等への委託手数料(1通当たり)123円

以上についても、当初3年間は上記特別交付税の対象となる。

総務省第4回個人番号カード・公的個人認証サービス等の利活用推進の在り方に関する懇談会資料より

◎住所地と本籍地が異なる場合における戸籍証明書等の交付方法

Before(郵送請求による場合)

＜交付を受けるために必要な物＞

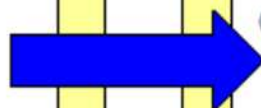
本人確認書類の写し、交付手数料、
請求書、送付用封筒、返信用封筒、切手など

- ① 請求書の記入
- ② 請求書等の送付
記入した請求書等を本籍地あてに郵送する。
- ③ 請求書の審査
本籍地の戸籍担当者は請求書の内容を確認する。
問題なければ、戸籍証明書等を交付する。
- ④ 戸籍証明書等の発送
本籍地の戸籍担当者は交付した戸籍証明書等を
請求者に発送する。

ここまでの手続きが**毎回必要**

負担大

- ⑤ 戸籍証明書等の受取り



After(コンビニ交付による場合)

＜交付を受けるために必要な物＞

マイナンバーカード、交付手数料

- ① 利用登録申請
キオスク端末申請とインターネット申請の両方に対応。
- ② 利用者登録
本籍地の戸籍担当者は申請情報を確認する。
問題なければ、利用者登録を行う。

ここまでの手続きは**初回のみ**

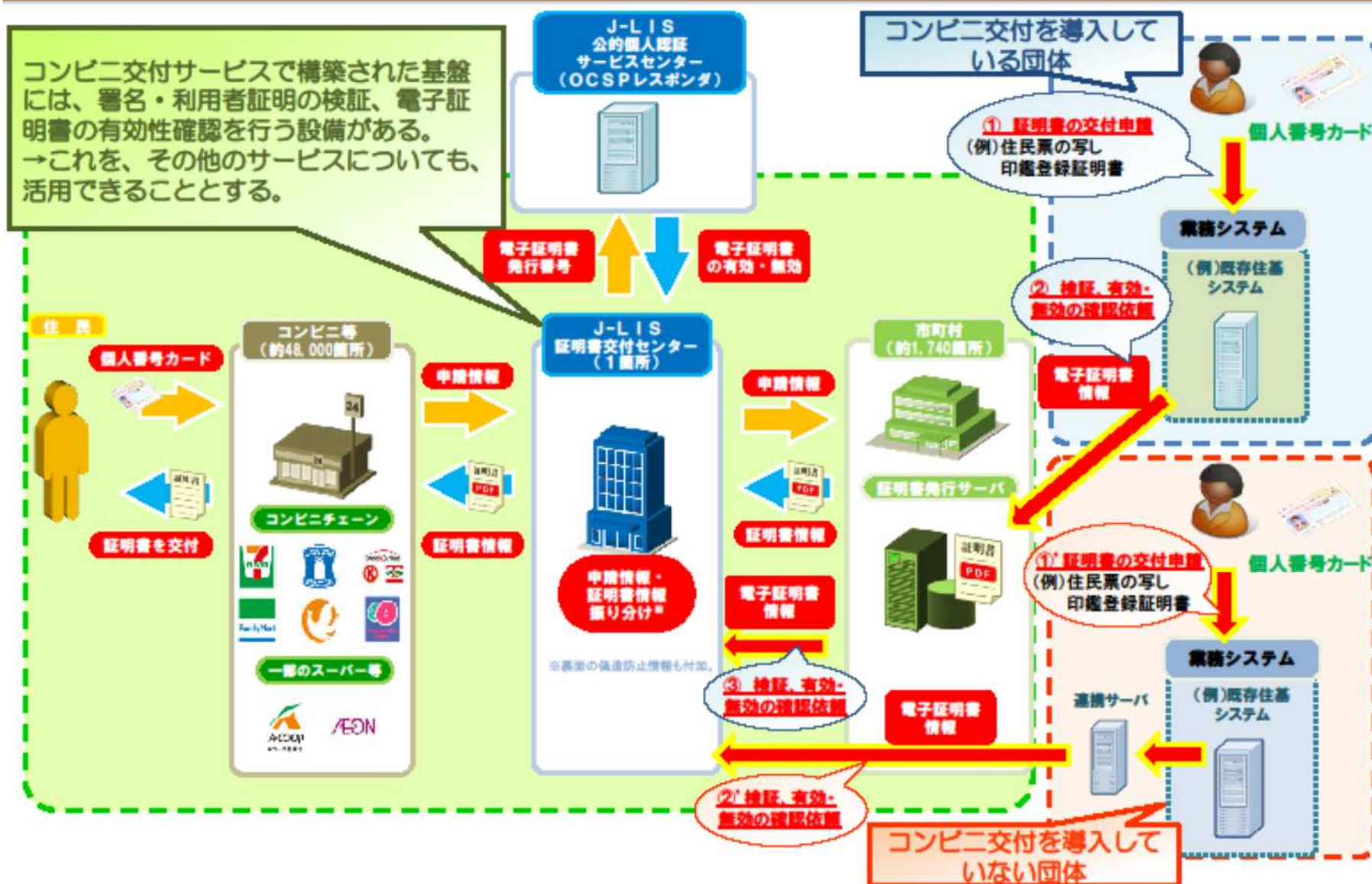
負担小

- ③ 戸籍証明書等の交付(2回目以降はここから)
コンビニに設置されている端末を操作して、
交付した戸籍証明書等を受取る。



導入のメリット

- ・初回のみ利用登録申請が必要だが、以降は不要となるため、請求者の負担が大幅に軽減される。
 - ・郵送請求に比べて、戸籍証明書等の受取りまでに要する期間が大幅に短縮される。
- ＜参考＞ 郵送請求: 1～2週間 コンビニ交付: 初回のみ利用者登録のため数日(2回目以降は随時)



総務省第4回個人番号カード・公的個人認証サービス等の利活用推進の在り方に関する懇談会資料より

マイキーIDと登録の方向性（素案）

マイキープラットフォームを用いたマイキーIDの設定、登録に関して、以下の方向で検討。

・マイキーIDとは

マイキーIDは、交付済のマイナンバーカードに格納されている利用者証明用電子証明書の既定のランダム文字列（14ケタ）を活用することが可能。この場合、受付端末識別記号（9ケタ）とあわせて一意性を担保する。

また、マイキープラットフォームを通じて、利用者が他者と重複しない任意のID（14ケタ）を設定・仮登録したうえで、市区町村窓口にて、マイナンバーカードに格納されている交付済みの利用者証明用電子証明書のランダム文字列を上書することでマイキーIDとして活用することが可能。

・マイキーIDの継続性

既定のランダム文字列をマイキーIDとして活用する場合、利用者証明用電子証明書の失効（5回目の誕生日等）にともない、マイキーIDは新たなランダム文字列に切り替わり、サービスID等との連携は、新たなマイキーIDに引き継がれる。

また、本人が設定したマイキーIDを活用する場合、利用者証明用電子証明書が失効（5回目の誕生日等）されても、設定したマイキーIDおよびサービスID等との連携は、そのまま引き継がれる。

マイキーIDと利用者証明用電子証明書（素案）

公的個人認証サービスから提供される利用者クライアントソフトウェアでは、「自分の証明書」の「詳細情報」において、利用者証明用電子証明書内容を確認できる。

マイキーIDのマイナンバーカードへの搭載内容の確認は、この機能を利用することを想定する。

証明書表示
公的個人認証サービス 利用者の利用者証明用電子証明書

基本情報 | 詳細情報

主体者(S) CN=1C2410DF79DGEL07202002B
C=JP

発行年月日(Y) 平成27年7月9日
有効期間の満了日(E) 平成32年6月1日

発行者(I) OU=地方公共団体情報システム機構
OU=公的個人認証サービス利用者証明用
O=公的個人認証サービス
C=JP

ファイル出力(E)

電子証明書の有効性確認は行われていません。

証明書表示
公的個人認証サービス 利用者の利用者証明用電子証明書

基本情報 | 詳細情報

項目名	値
署名アルゴリズム	sha256WithRSASignature
発行者	Japan Agency for Loc...
発行年月日	2015年7月9日 19時33分...
有効期間の満了日	2020年6月1日 23時59分...
ランダム文字列	1C2410DF79DGEL
受付端末識別記号	07202002B
生成者の公開鍵情報	rsaEncryption(2048bits)

07202002B

フィンガープリント
sha256 077C0927083C1E9096873F038B04929BE276E28E1AC223B01C6C0A
5D9B0F0672

ファイル出力(E)

有効性確認(Y)

電子証明書の有効性確認は行われていません。

マイキーIDにあたる情報(※)
※英字A-Z、
数字0-9の
36種類、14ケタ

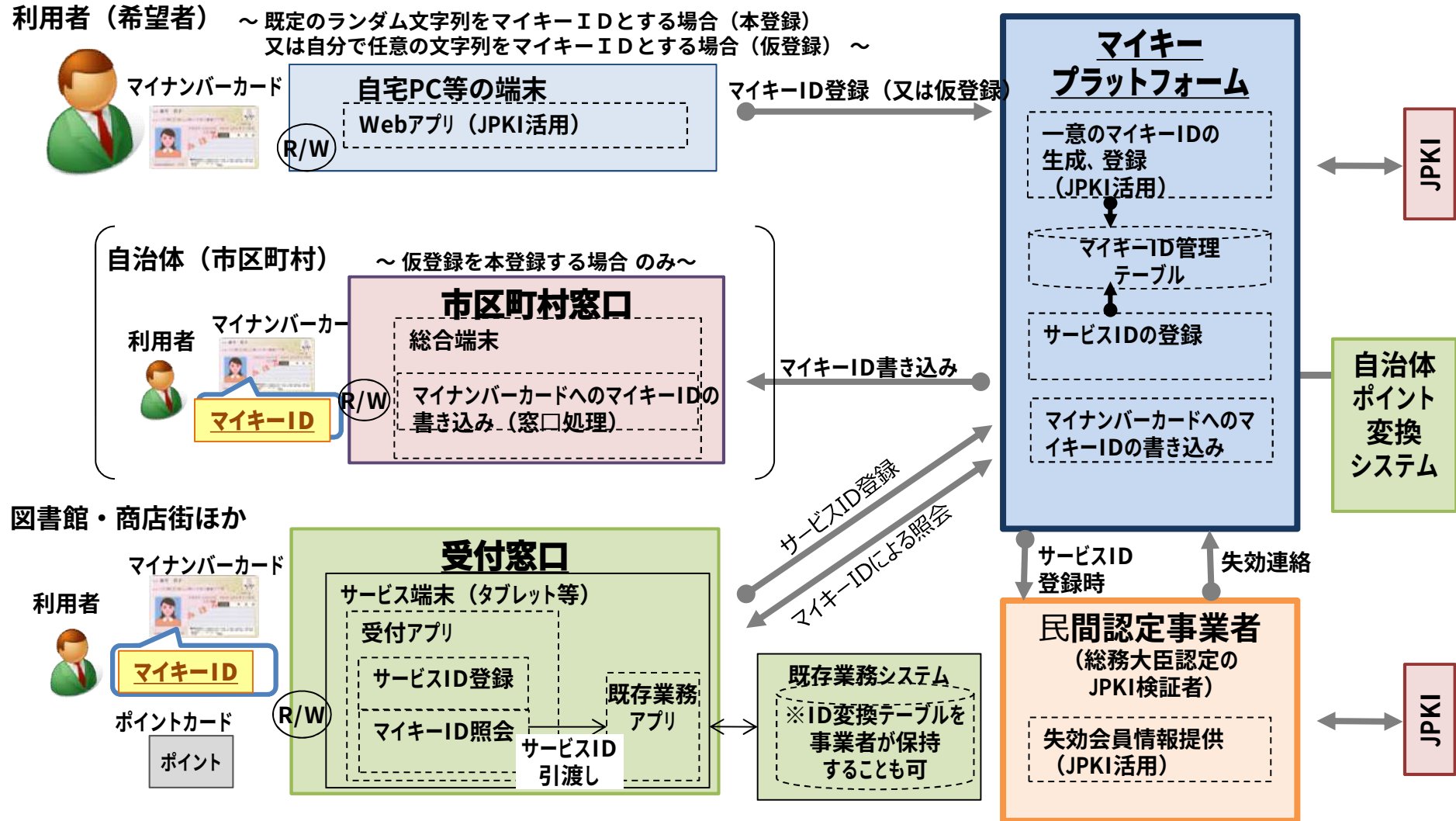
**既定のランダム文字列を
一意にするための補足情報**

出力ファイル(抜粋)

[ランダム文字列]
1C2410DF79DGEL

[受付端末識別記号]
07202002B

マイキー利用イメージ（素案）



マイナンバーカードを活用した利活用将来像

2

母子健康情報・おしらせ

- ✓ 母子健康情報をいつでもどこでも閲覧
- ✓ 電子私書箱あてに自治体からの予防接種のおしらせ通知により、受診漏れ防止



地域経済を応援

- ✓ マイナンバーカード1枚で自治体ポイントなど様々なサービス利用が可能。
- ✓ 民間ポイントを自治体ポイントに交換し、商店街等で活用



インターネットバンキング

- インターネットバンキングのログイン時にマイナンバーカードをスマートフォンで読み取って認証



行政サービスの利便性向上

- コンビニ交付サービスの基盤について、地方公共団体の窓口など他の場面で活用



ワンストップサービス

- 年金支給の生存確認をケーブルテレビから簡便に実施（現況届）
- 保育所の利用申請手続（雇用証明書取得を含む）を在宅から実施



チケットレスサービス

- コンサート会場への入場時にマイナンバーカードを使ってスムーズに入場



災害時の避難指示・見守り

- ✓ 迅速な個人への避難の呼びかけ
- ✓ 健康状況を確認、遠隔サポート



避難所での適切な住民支援

- ✓ 迅速な避難状況の把握により、避難状況にあわせた支援物資の準備



官民様々なサービス基盤との連携



住民の利便性向上、生産性向上等

地域経済活性化、好循環拡大

地域活性化、1億総活躍社会の実現

総務省第4回個人番号カード・公的個人認証サービス等の利活用推進の在り方に関する懇談会資料より

利用者証明書の利用方法の整理

- 共通認識
 - 利用者証明書は、4情報の記載はないが、仮名になっている
 - 仮名に当たるものには、Common Name (マイキーIDと呼ぶ) となる
- セキュリティレベルからの整理
 - 高; PINを用いる (PINあり) 利用者認証
 - 中; PIN入力を省略した (PIN無し) 利用者証明
 - 低; 利用者証明書のみ利用 (秘密鍵の利用無し)

注意; 利用者証明書は、コピー可能

アプリケーションが求めるセキュリティレベルで、上記3つの手法を適切に選択

H27年度の実証事業等のまとめ

- 実証項目（試行的な本番実施を含む）
 - コンビニのキオスク端末からの戸籍取得
 - イベント会場チケットレスサービス
 - ケーブルテレビにおけるマイナンバーカードの読み取り
 - スマートテレビにおけるマイナンバーカードの読み取り
 - 電子私書箱における属性証明 等
- 実証を終え、実現に向けて詳細検討中
 - 健康保険の資格確認（H30,4から実施予定）
 - クレジットカード 等

JPKIの特徴と次の論点

- 利便性向上から、スマホ等への利用者証明書搭載の要望があり、総務省において検討を開始
 - 個人番号カードを持っている人向けのサービス
 - 3枚目の証明書を発行 ⇒ 要法改正
- スマホに搭載するなら、他の媒体（カード含む）、機器もありか？ ⇒ 2枚目のカード、HPKI（資格付き電子署名）の普及促進へ
- HPKIの電子署名は、電子処方箋、紹介状等で利用 ⇒ 住所の記載のない電子署名用証明書が望まれている

属性証明の法制化

- “電子委任状の普及及び電子委任状取扱業務の認定等に関する法律案（仮称）”を総務省、経産省、法務省で検討開始
- 法人の代表者からの委任状 ⇒ 例えば、政府調達における応札が対面・書面なく電子的に可能にする
- GPKIを使った委任状 ⇒ 例えば、医師資格の証明を代行する者を指定。 注意；書面の証明書は従来通り
- 卒業証明書の電子版も同じ方式で可能に
- 委任手続きを行うケースはすべてカバーされる

社会的な背景 (リマインド)

- 少子高齢化の進展による、歳入の低下と歳出の増大 ⇒ バランス、景気の改善等が必須
- 共通番号制度の実施 ⇒ バランス改善
 - 現状制度の確実な実施で、制度変更とは別
 - 法人・個人番号を導入 ⇒ 歳入増加に資する！
 - 社会保障分野の歳出削減に資するか？？
 - 効果が期待できる施策を考えるべき！

医療等分野における情報化の目的 (1)

- 事務処理等の手間、コストの削減
 - レセプトコンピュータの導入
 - レセプトのオンライン化 ⇒ 2005年から本格実施
 - 医療保険の資格確認 ⇒ 2017年から実施予定
- 医療情報の電子化 (医療機関内)
 - 病院情報システムの導入
 - 電子カルテの導入 ⇒ 1995年から国プロとして取り組み開始

医療等分野における情報化の目的 (2)

- 医療情報連携
 - 地域医療ネットワークの構築による病診連携等
 - 地域をまたがる医療情報の参照等
 - 遠隔医療の実現
- 医療情報の高度利用
 - 予防医療の実現
 - 疾病構造の変化に対する迅速な対応

個人健康管理システムの実現

⇒ 医療等IDの導入、究極の目的

個人健康管理システムとは

- 目的
 - 個人別の健康情報を時系列で管理・活用
 - マクロ・ミクロでの情報分析 (天気予報を参考) を実現
 - ⇒ 健康予測、新たな感染症等への対策
- 効果予測 (多くの先進国が取り組むが未だ実証されていない)
 - 健康予測を可能とすることで、健康寿命を延長
 - 衛星によるマクロ、雨量計等によるミクロ、スパコンによるモデル解析
 - ⇒ 天気予報の精度が大幅に向上
 - 生活習慣病等の減少による医療費の削減
 - 新たな疾病等に対する対応の迅速化

個人健康管理システム

- アプローチ
 - 健康・医療・介護情報を組織、疾病別管理に加えて個人別に時系列管理
 - 各人の情報の所在場所をデータベース化 (分散管理)
- 現実的な手段
 - 健康保険の資格確認をトリガーとする (医療情報の保存義務あり) ⇒ クラウドの利用等
 - 希望者による参加 ⇒ 紐づけミスを無くするため、番号カード (JPKI) の利用を必須とする

資格確認をトリガーとして

- 個人健康管理や医療情報連携には、正確な紐付けが必須
 - ⇒ 不正確な紐付けには、年金記録で懲りている
 - ⇒ 正確な資格確認により生成される（保険診療）
 - ⇒ 責任の明確化 ⇒ だからエビデンス化
- 実現手段
 - 共通番号の導入 ⇒ 転記ミス無くすることは、極めて困難
 - 2次元バーコード ⇒ 転記ミスは大幅に削減できる
 - JPKIの利用 ⇒ 電子署名と同じ技術の利用
 - ⇒ 資格確認の手続きがエビデンスになる

保険資格確認の本格実施 (案)

- JPKIのシリアル#と保険証の記号番号を紐付け
- いつ、誰が、どこから医療サービスを受けたかを確実に
捕捉 ⇒ トランザクションのエビデンス化 ⇒ 責任分
解点の明確化
- これにより、レセプトの返戻や未収金の問題解決に資す
ると期待
- 専用端末とHIS、レセコン等とは、別回線 (有線、無線を
問わず) で接続 ⇒ システムの責任分界点と取り扱う
情報の明確化 ⇒ 受付処理番号を発行

専用端末の機能概要 (案)

- NFCのR/Wを兼ねる資格DBへのアクセス端末
- PIN無し処理のスピードアップのために、セキュアチップをサポート
- 電池駆動、WiFi接続、タイムスタンプ、GPS、ホワイトリストのキャッシュ等の機能を持つ ⇒ 携帯電話をベースとするか
- 設定済み端末 ⇒ 保健医療機関を特定 ⇒ 機器を特定
- 起動時には、HPKI等による認証を要求 ⇒ 不正利用や盗難等の対策

医療等IDに関する検討状況

- 社会保障分野における現物給付については、マイナンバーとは別の医療等IDの導入を検討
- 厚労省、3師会のそれぞれにおいて検討会を開催
- 厚労省については、11月18日の検討会で報告書の原案が示され、年内に最終報告を公開
- 3師会の検討会で示された方向性が、厚労省の報告書に盛り込まれている

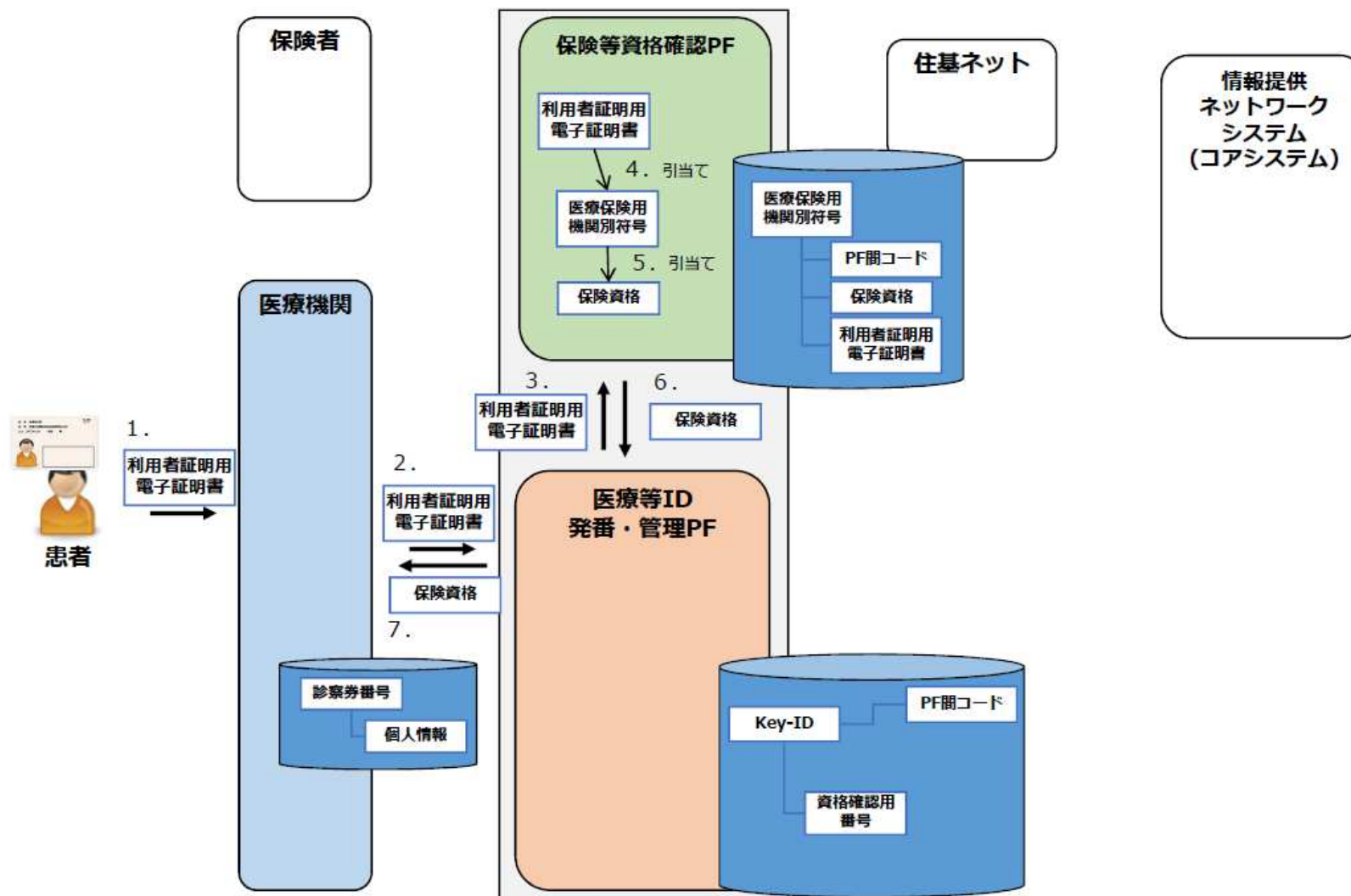
医療等IDの基本的な考え方

- 医療等IDは、用途別（保険資格確認、疾患別DB、地域を跨る情報連携等）に異なる番号を用いる
- そのため、KeyID（コアシステムのIDコードに当たる）を機関別符合から生成
- 機関別符合（リンクコード）はマイナンバー法により、審査支払機関に払い出される
- リンクコードは悉皆性と唯一無二性を有している
- KeyIDを用いて用途別に異なるIDを生成

用途別IDの例

- KeyIDを用いて用途別のID-X、ID-Y等を生成
- 医療情報の連携に用いるIDは見えない番号とする
- 一方、医療保険においては、保険者に依らない被保険者番号（資格確認番号）を見える番号として導入
 - ⇒ オプトアウト無しの番号であれば、十分な保護策が必須
 - ⇒ 個人情報保護法は本人同意で利用可能
 - ⇒ マイナンバーは、できる法 ⇒ 導入、利用禁止、例外規定
- 医療保険と介護保険、地域を跨る情報提供等を可能とするための紐づけ用IDも必要に応じて発番
- 疾患別DBや疫学等の研究には、それぞれ独自のIDをKeyIDから生成

医療等ID発番・管理PFで個人番号カードを利用し、保険資格確認



3 師会検討会の参考資料

おわりに

- マイナンバーカードとコンビニ証明書発行基盤は新たなインフラになると期待
- マイナンバーカードで資格確認、決済等が可能に (本人の選択)
⇒ 健康保険証、クレジット等の機能を1枚で
- 多機能端末は、他分野にも有効
⇒ 保険資格確認、クレジット、電子チケット等
- スマートフォン、HPKIカード等へのJPKIの追加搭載を検討
- 属性証明の法制化を本格的に開始
- 保険証をはじめとした社会保障分野での利用を推進