厚生科学研究費補助金（医療技術評価総合研究事業）
総括研究報告書

保健医療福祉分野における住基カードを用いた個人・組織・資格認証の在り方に関する研究

主任研究者　大山　永昭　東京工業大学フロンティア創造共同研究センター教授

研究要旨：情報通信技術を利用して保健医療福祉サービスの効率化・高度化を図る際には、患者の個人情報保護、記名押印の電子化等の観点から、医療従事者や患者等の認証を行うことが必須となる。本研究では、今後配布が予定されている住民基本台帳 IC カードや公的個人認証サービスなどと連携して保健医療福祉分野の電子認証を実施する方策を検討し、実現に向けた課題を明らかにした。

分担研究者　公文　敦　（財）医療情報システム開発センター研究開発部
研究開発２課　課長
喜多　紘一　東京工業大学理工学研究科客員教授
土屋　文人　日本病院薬剤師会常務理事
八幡　勝也　産業医科大学産業生態科学研究所講師
高橋　紘士　立教大学コミュニティ福祉学部教授
秋山　昌範　国立国際医療センター第５内科医長

A．研究目的

近年の情報基盤整備の進展に伴い、保健医療福祉分野の情報化推進が期待されている。電子的に保健医療福祉情報の流通を行う際には、個人情報の保護を図るための適切な措置を講じることが必要である。このためには、通信回線上の個人データの秘匿やデータを使用する者の正当性を認証することが必須となる。さらに、診療録や処方箋等を電子化する際には、記名押印等の扱いが問題になる。

現在、行政においても電子署名及び認証業務に関する法律（以下、電子署名法）の成立や住民基本台帳法の改正及び住民基本台帳カード（住基カード）の導入、GPKI（政府公開鍵基盤）等の検討が進められている。平成15 年度には住基カードの配布や地方自治体による公的個人認証サービスの開始が予定されていることから、これらを保健医療福祉サービスにおいても活用することが期待される。

本研究課題では、個人情報保護法、電子署名法、公的個人認証サービス、GPKI 等に関する検討状況を踏まえた上で、住基カードと連携した保健医療福祉分野における個人・組織・資格認証を実施する具体的な方法を明らかにすることを目的とする。

本年度は、住基カードとして導入が予定されている広域・多目的利用可能なＩＣカードを利用した医師・薬剤師等、保健医療福祉分野における法定資格の認証方法、資格・組織認証に必要となる登録情報データベースの整備方法の検討を行った。また、患者や被保険者などの個人、医療機関などの組織の認証方法と、資格認証などを連携する方法についても検討した。

B．研究方法

保健、医療、福祉の各分野における情報化推進にあたっている工学者及び医師らの研究分担者を中心として研究委員会を組織し、各分野における認証の実現方法について調査・検討を行った。また、住基カード、先進的 IC カード、公的個人認証サービスなどの動向を調査し、これらの結果を基にして電子

的な認証の実施方策を整理した。

C．研究結果

(1) 保健医療福祉分野における個人・組織・資格認証

(1.1) 保健医療福祉分野における電子認証のユースケース

まず、個人、組織、資格に関する電子認証の対象について、以下の通り整理した。

・個人認証

個人認証の対象としては、患者としての個人、被保険者などの保健医療福祉サービス受給者としての個人と、保健医療福祉サービス従事者としての個人などが考えられる。

・資格認証

医師、薬剤師などの国家資格については、法令に規定された行為を行うことに関する認証が必要である。また、その他の資格についても、患者情報の保護や情報の信頼性確保の観点から、情報を扱う者の資格を確認する必要が生じる。

・組織認証

組織を認証するべきケースは、今後オンラインで診療報酬請求などを行う場合などが考えられるが、一方、医療機関などの組織に属する医療従事者が患者情報を扱う際に、個人や資格の認証を代行することが現実的である場合が多い。

以上の認証対象を考慮し、ユースケースを整理すると以下の通りとなる。

・電子的に記名・押印を行う場合
　－紹介状（診療情報提供書）の作成
　－処方箋の作成
　－診療録への記載
　－照射録の作成
　－診断書等の作成
・電子的に患者情報の交換・管理を行う場合
　－患者紹介を受ける際
　－患者の診療録や医療情報へのアクセス時
・電子申請・届出など
　－オンラインによる診療報酬請求

(1.2) 本人確認と資格認証

紹介状や診療録の作成者を、電子署名によって記録する場合には、医師の資格に基づき署名を行ったことを記録する必要が生じる。このとき、本人の実在性を認証するための本人確認と、その本人が保有する資格の認証が必要になる。

PKI において資格認証を実現する方法としては、以下の方法が考えられる。

・資格が書き込まれた公開鍵証明書（PKC）を用いる方法
・PKC に対してリンクを有する属性証明書（AC）を用いる方法

例えば、資格が書き込まれた PKC を用いて電子署名を行う場合には、電子文書に対してこの PKC を添付した上で、この PKC に記載された公開鍵に対応する秘密鍵を用いて署名する。このため、資格証明を行うためには、秘密鍵の生成と公開鍵の CA への登録が必要になる。

AC を用いる場合には、個人認証のための PKC へのリンク情報を持つ AC と、その PKC を電子文書に添付し、この PKC に記載された公開鍵に対応する秘密鍵を用いて署名する。このため、別途個人認証のための PKC を用意することが必要である。公的個人認証サービスの PKC は、現在のところ署名検証者が行政機関等と特定認証業務を行う事業者に限定されており、これを利用可能か否かについては今後検討が必要である。

PKI においては、多くの場合 AC は有効期間を短くし、オンデマンドで発行することが考えられている。しかし、ここで対象とする資格認証に用いる際には、長期間有効な AC が望ましい。このため、AC に関する失効リストの管理も必要になる。

(1.3) 関連動向

・電子署名及び認証業務に関する法律（電子署名法）

電子署名法では、規定された要件を満たす公開鍵暗号方式に基づく認証局（CA）を特定

認証業務として規定しており、これに基づく電子署名を手書きの記名・押印と同等な効力を認めるものとしている。また、特定認証業務の認定を受けるための要件も規定しており、認定に関する指針も省令として出されている。このことから、保健医療福祉分野において電子署名を使用する場合にも、同等の要件を満たすことに留意しなければならない。

・個人情報保護法案

現在公開されている個人情報保護法案では、個人情報の範囲を広く捕らえ、また個人情報を取り扱う事業者に対する責務を規定している。医師や保健医療福祉施設も個人情報取扱事業者としての義務が発生することから、個人情報保護法案の趣旨に則り患者情報を取り扱う必要がある。

・公的個人認証サービス

電子政府・電子自治体を推進することを目的として、平成15年度までに申請・届出等の電子化に必要とされる地方自治体による公的個人認証サービス等のシステムの整備が行われる予定とされている。公的個人認証サービスでは、地方自治体による厳密な本人確認のもとに、PKIに基づく公開鍵証明書を発行し、電子申請・届出や民間での特定認証業務における本人確認への利用を可能とするものである。保健医療福祉分野でも公的個人認証サービスと連携した電子認証の仕組みを採用することは有効と考えられ、これについては以下(3)項に述べる。

・行政連携ICカード

ICカードの利便性の向上、行政コストの削減を実現するため、国民等の関係府省等が発行するICカードについては、1枚化を図ることが可能になるよう、行政連携ICカードとして仕様を共通化する検討が進められている。これによって、導入・普及時における二重投資を防ぐ観点や、異なる性質のアプリケーションの相乗りが容易になると予想される。したがって、住基カードや公的個人認証サービスで使用されるICカードを保健医療福祉分野における電子認証に活用する環境は整いつつあるといえる。

・GPKI（政府公開鍵基盤）

現在、電子申請・届出や結果の通知等における作成者の確認、申請書や通知文書の内容が改ざん検知を可能とするため、GPKIの構築が進められている。GPKIの一部をなす省庁認証局は、処分権者の官職を認証するための証明書を発行する。医師や薬剤師等の法定資格にかかわる証明書を電子的に発行する場合には、GPKIの仕組みに基づき、処分権者である厚生労働大臣の電子署名が付与される必要がある。

(2) 住基カードの保健医療福祉分野における利用について

(2.1) 住基カード

住基カードは、平成15年度から配布開始が予定されており、カードの仕様についても固まりつつある。住基の基本4情報の利用は法律により規定されているが、ICカード内で住基アプリケーションが使用する領域以外の空き領域は自治体の条例において独自利用が可能となっている。空き領域の有効利用は、利用者の利便性向上、重複投資の防止などの効果が期待される。

(2.2) 先進的ICカード

住基カードとして導入が予定されるICカードの独自利用領域については、住民の希望に基づいて各種のサービスを搭載可能である。従来のICカードにおいては、ROM上に制御コマンドを搭載していたため、クレジット、保健医療、銀行などアプリケーション毎に異なる仕様のカードが用いられてきたが、近年開発された先進的なICカードは、制御コマンドをアプリケーション毎に後から設定することができるため、汎用性が高い。このようなICカードは、プラットフォーム型と呼

ばれている。また、非接触インタフェースの採用によって、信頼性向上、使い勝手の改善、インタフェース高速化などが図られている。

先進的 IC カードの大きな特徴は、IC カードの広域多目的利用を可能にするマルチアプリケーションフレームワークに基づくシステムを実現できる点にある。

従来の IC カードにおけるサービス提供においては、ほとんどの場合カード発行者とサービス提供者は同一であった。また、IC カードの多目的利用を行う場合にも、IC カード配布時に予め利用するサービスの設定を行う必要があることや、IC カード仕様が異なる業界を超えた多目的化は不可能であったため、オープンなマルチアプリケーションの利用環境が整っていなかった。マルチアプリケーションフレームワーク（図１）においては、カード発行者とサービス提供者の役割を分離し、両者間の統一的なオペレーションを規定することによりカード発行者に依存しないサービス提供者のシステム構築を可能にする。これによって、地域やシステム実装によらず任意のカードアプリケーションを動化すことができるほか、カード発行者とサービス提供者の間でのコストシェアを可能にしている。［参考文献１］

上述の住基カード及び行政連携カードは、このマルチアプリケーションフレームワークに則り運用されると想定できることから、保健医療福祉サービスにおいても有効活用を図ることが期待される。

マルチアプリケーションフレームワークにおけるサービス提供者とは、IC カードを用いるサービスを提供する主体であり、保健医療サービスの提供・受給の関係とは異なる場合がある。例として、医師等の資格認証に基づく電子署名を IC カードに格納した秘密鍵を用いて行う場合には、PKI・電子署名機能を提供する機関がサービス提供者となる。一方、患者の健康保険受給資格確認を行う場合を考えると、例えば保険者がそのようなサービスを提供するケースなども考えられる。これらは、マルチアプリケーションフレームワーク上で運用可能であり、利用者の要求に合わせて最適なカードに電子認証機能を搭載して利用することが可能である。

今後、先進的 IC カードを利用した資格認証の仕組みについてさらに具体的な検討を行うことが必要である。

(3) 公的個人認証サービスとの連携

認証局を運用するにあたっては、認証書発行対象者の本人確認を厳密に行うことがきわめて重要である。電子署名法における認定認証業務の要件では、本人を確認できる証明書の提示、本人の出頭もしくは本人限定郵便の利用などが必要とされており、実施にあたってはその確認が煩雑になる恐れがある。ただしこれによって、公的個人認証サービスは住民基本台帳を基にした信頼性の高い本人確認サービスを提供する。

そこで、公的個人認証サービスによる本人確認に基づいて資格証明書を発行することが考えられる[図２]。この場合、資格認証の対象者は、資格証明申請書＋公的個人認証サービスに登録された PKC＋※資格認証用公開鍵＋電子署名（同 PKC に対応する秘密鍵による署名）を登録機関（RA）に提出する（※は PKC により資格認証を行う場合）。このような方法をとることにより、公的個人認証サービスにおける厳密な本人確認のもとで資格証明書を発行でき、RA における本人確認の負担を低減できる。

(4) 資格登録の現状と課題

分担研究報告書に示されているように、医籍登録については、データベース化整備がなされていない。しかし、資格登録の確認は、原簿である医籍登録との同一性が確保されたリストに基づいて行われる必要がある。今後、法定資格の電子認証を実現するには、資格登録名簿のデータベース化を図るとともに、逐次情報の更新を行える体制を整備する必要がある。

(5) 組織・資格認証の連携

医療機関等に所属する医療従事者の認証は、外部に対する責任を医療機関が代表することにより、組織の認証と連携することが可能である。組織の認証と連携した医療従事者の認証を可能にすることによって、現行に近い形態での運用が可能になること、資格登録で網羅されない医療従事者やコメディカルに対する認証が容易になることなどの効果が期待される。

D．考察

電子署名法の特定認証業務の認定に関する要件はCAに対するものであり、ACを用いた資格認証を行う属性認証局（AA）に対しての要件は存在しない。しかし、法定資格認証のように高い信頼性が要求される属性認証においては、CAに対するものと同様な要件を満たすことが望まれる。したがって、今後法定資格認証などのためのAAに対する運用の基準を明確にする必要がある。

資格証明書を発行する際に、書面により本人確認書類を提出する場合にはその信頼性を確保するために本人の出頭を要するものと考えられる。公的個人認証サービスを利用した本人確認を行うことで、本人確認の信頼性確保、負担低減が可能であり、その場合には、本人の出頭が無くても信頼性を保つことができると考えられる。

一方で、鍵の信頼性を確保する観点から、公的個人認証サービスでは市町村の窓口に配備する鍵ペア生成装置を用いて、申請者自らが生成する方法に当面限定することとしている。これと同様の方法を採用すると、資格証明書としてPKCを用いる場合には本人の出頭を要することになる。ACを用いる場合には、鍵を生成する必要が無いので本人の出頭は不要である。したがって、PKCを用いる場合には、利用者が自らの端末などにおいて実行可能な、暗号の強度が確保され、改変される可能性のない鍵ペア生成及びICカードへの格納方法を確立することが望まれる。

また、医籍登録については、データベース化に向けた課題に加え、現住所が記載されていないため、基本4情報との照合ができないことも問題になる可能性がある。このため、医籍登録されている人物と、資格証明書発行申請を提出した人物の同一性を確認する方法については、さらに検討する必要がある。さらに異動等失効情報などを逐次反映する仕組みが必要である。

E．結論

本研究では、まず、保健医療福祉分野における電子認証のユースケースと関連する制度・技術の動向を整理し、住基カードとして導入が予定されている先進的ICカードを用いることが、保健医療福祉分野における個人・資格認証に有効であることを示した。また、公的個人認証サービスと連携した資格認証基盤の実現方法を明らかにした。さらに、資格認証を行うためには、資格登録名簿のデータベース整備が必須であることがわかった。現在、電子カルテ、ネットワークを利用した診療情報の交換、診療録の外部保存などが開始されつつある状況であり、保健医療福祉分野における個人・組織・資格の認証が可能な電子認証基盤を早急に整備するべきである。

本研究では、次年度以降、住基カードを利用して個人・組織・資格認証を実現するための運用モデルを確立するとともに、保健医療福祉分野において住基カードの利用に関連する各種の問題とその解決策を提示する。そして、ＩＣカードを用いて実証プロトタイプシステムの基本設計を行う予定である。

F．参考文献

1）次世代ＩＣカードシステム研究会平成12年度活動報告書、(2001)

G．研究発表

１．論文発表

１）大山 永昭:“個人認証の考え方と制度的な対応”、映像情報メディア学会誌, 55, [2], 168-171 (2001)

２）大山永昭:“電子政府と行政 IC カードの方向性”、ＩＣカード総覧 2001, 16-26 (2001)

３）大山永昭:“電子政府の構築と個人認証の考え方”、ハイパーフラッシュ２月号, 2-7 (2001)

４）大山永昭:“電子政府とＩＣカード”、月刊 Keidanren2 月号, 24-25 (2001)

５）大山永昭:“サイバーパスポートの実現”、edit 21, [2], 12-15 (2001)

６）大山永昭:“次世代 IC カードが拓く IT 社会”、蔵前ジャーナル４月号, 13-18 (2001)

７）大山永昭:“次世代 IC カード元年”、雑誌エレクトロニクス６月号, (2001)

８）大山永昭:“電子政府の展開と電子カルテ”、INNERVISION, ７月号, 74-77 (2001)

９）大山永昭:“住民基本台帳ネットワークシステムの構築と IC カードの利用”、フォト８月号, 40-41 (2001)

２．学会発表

１）大山永昭：“(4)医療情報システムを取り巻く社会情勢の変化”、日本放射線技術学会第 56 回総会学術大会予稿集, 77 (2001)

２）高橋裕樹・鈴木裕之・小尾高史・山口雅浩・大山永昭・角田　貢・喜多紘一：“属性証明書を利用した保健医療分野における資格認証システム”、2002 年電子情報通信学会大会予稿集, (2002)

保健医療福祉分野における住基カードを用いた個人・組織・資格認証のあり方に関する研究

東京工業大学
フロンティア創造共同研究センター
大 山 永 昭

保健医療福祉分野の電子認証について

- 必要性
  - 情報化される保健医療福祉分野の安全性の確保
  - 電子署名技術の実用化による記名・捺印の電子化
- 研究目的
  - 個人・組織・資格認証の実施方策の提示
  - 住基カードとの連携方策の提示　　等
- 検討課題
  - PKIを用いた本人、ライセンス、施設等の認証
  - スマートカードを用いた認証手法の開発
  - 住基カードシステムの開発状況の調査
  - 環境変化の調査　　等

認証について

- なぜ必要
  - インターネット等のオープンなネットワークでは、他人や架空の人物への成りすましが起こり得る
  - 行為に対する正当性の確認が必要なことがある
- どうやる？
  - 相手特定と正当性の確認 ： 2ステップになる

<u>誰が、何を、何のためにかを明らかにする</u>

保健医療分野での認証の必要性は明らか

次世代スマートカードとは

1. 機能
   - マルチアプリケーションをサポート
   - 非対称暗号方式(PKI対応)をサポート
   - 非接触インターフェイスを有する
     - 公共端末は非接触、個人用は接触も可能
   - 国際標準準拠
2. 運用 ⇒ NICSS-Fと呼ばれる ⇒ 世界最先端の技術
   - カード発行者、利用者、サービス提供者の3者モデルを利用
   - サービス提供者の登録システムを利用
   - サービスの追加削除は、PKIを用いた相互認証により実施
     ⇒ On siteで可能 ⇒ チップ間でも可能

<u>行政系カードの発行によりチップの大量生産が開始される</u>

電子行政の構築に関して

1. 課題：行政区域を越えたサービスの提供
2. 条件：行政手続には、本人確認と意思確認が必須

2-1. 窓口等(On site)での本人確認と意思確認

- 本人確認 ⇒ 公的な証明書等の利用 ⇒ 住基カードの券面
- 意思確認 ⇒ 既存サービスおよび手続きの特定

– 居住している自治体への通知

- <u>個人を特定して通知しなければならない</u>
  ⇒ <u>既存の住民番号に市区町村コードを付加する、</u>
  または外字利用の制限
- 11桁の乱数の利用と変更申請の受付 ⇒ 住基コード

電子行政の構築に関して

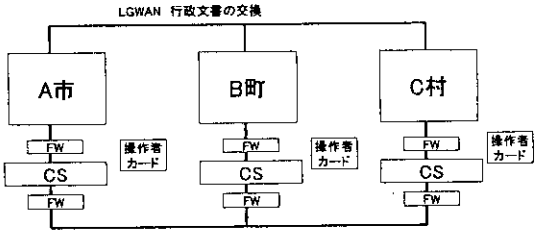
2-2. サイバー空間での本人確認と意思確認

– インターネット等を用いたオンライン申請・申告

- 記名捺印の電子化が必須
- <u>住基コードでは不十分</u>
  ⇒ 本人特定は可能であるが認証は不可能
- 法人認証と公的個人認証サービスの実施(準備中)

住基ネットとLGWAN

- どちらも、地方自治体間を結ぶネットワーク
  - より高い安全性を確保するために両者を切り分ける



住基ネットの安全性に関して

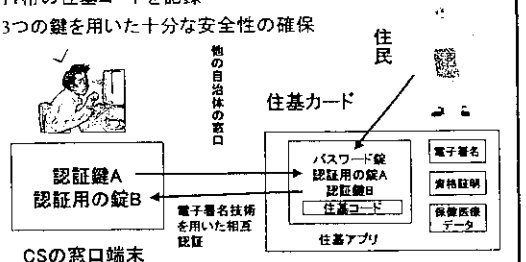
1. 技術的な対応
   - ネットワークの専用回線化
   - データの暗号化
   - ファイアーウォール(FW)の設置
   - コミュニケーションサーバー(CS)の専用化
     ⇒ 改変やソフトの追加付加
   - 操作者用カードの利用と管理
   - ログの記録 ⇒ 操作内容の追跡を可能とする
   - ネットワーク全体のモニタリング ⇒ 利用監視

住基ネットの安全性に関して

2. 組織的な(運用面での)対応
   - 管理・運用規定の制定
   - 職員の研修
   - システムの安全性の第3者評価(参考:ISO15408)
     ⇒ 自治体の既存システムを含めるべき
3. 制度的な対応
   - 法律の改正 ⇒ 罰則規定の強化
   - 新法の実施 ⇒ 個人情報保護法(主として対民間)

住民基本台帳カードについて

- CPU付のICカードでスマートカードと呼ばれる
- 11桁の住基コードを記録
- 3つの鍵を用いた十分な安全性の確保



住基カードの多目的利用

- 基本
  - 住基カードの空きエリアの多目的利用は、条例により可能(改正住基法)
- 条例の例示
  - 平成14年9月24日 都道府県の住基ネットワーク担当者に総務省から素案の提示
  - 公共料金等の支払いサービス
  - 公共交通機関等での利用
  - 商店街のショッピングポイントサービス
  - 保健・医療・福祉・介護等のサービス

等

住基カードの調達

- CSとカード発行管理システムとのI/F仕様提示
- 調達プロセスの明確化(一部提示済み)
  1. カードの機能要求定義の提示(PPを含む)
  2. 納入メーカとの秘密開示契約(住基アプリについて)
  3. カードの機能確認(住基アプリの相互運用に関して)
  4. カードの安全性確認(STの第3者評価)
  5. すべてのテストに合格したカードのリストアップ
- 調達対象カードのリストを提供
  ⇒ 平成14年度末まで

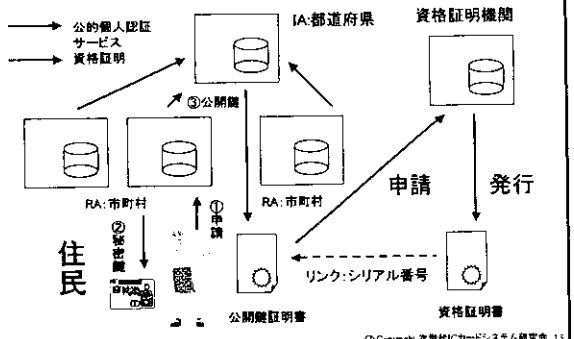
住基カードの券面表記について

- 基本認識
  - 住基カードは、身分証明書としても機能する
  - 券面表記の偽造変造等を防止するため、一般的に微細文字やホログラム等の特殊印刷が使われている
  - クレジットカードなどでは、安全性向上のためにスマートカードが使われている
  - インターネット経由の電子政府サービスでは、券面表記は役に立たない
- 住基カードの場合
  - 身分証明書としての機能を持つ場合には、券面表記を統一。安全性をさらに向上させるために、端末との相互認証および特殊印刷が使われる
  - 電子空間での本人確認には、電子署名とスマートカードが用いられる。券面表記は自由。

公的個人認証サービスについて

- 印鑑登録制度の電子化 ⇒ 公開鍵の自治体登録
- 条例から法令へ （法案提出済み）
- 電子署名技術の利用 ⇒ 本人の意思確認
- ICカードの利用；住基アプリとの相乗りも可能
  ⇒ 秘密鍵の安全性の確保
- 電子政府サービスの基盤
- H15に実施予定
- 法定資格属性証明の発行 ⇒ 関連府省

個人および資格認証の実現手段

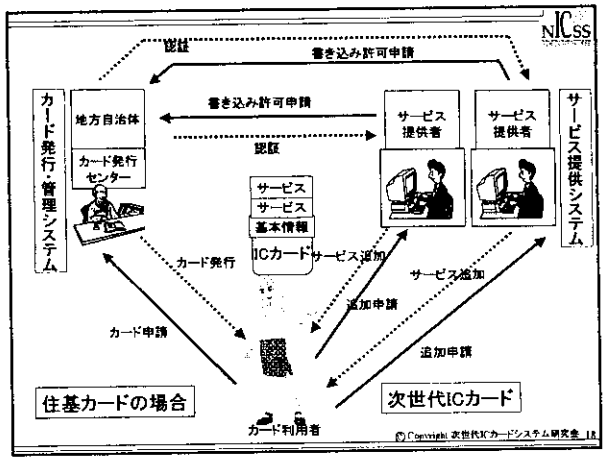


行政連携カードについて

- 内閣府IT室担当
- 目的
  - カードの2重、3重投資を避ける
  - 相乗りによる利用者の利便性の向上　　等
- 合意事項
  - 住民基本台帳カードを基本とする原案が提示される
    ⇒ NICSS-Fの採用
  - 各省庁は、カードを自由に発行する
  - カード発行省庁は、他の省庁の相乗りを拒否しない
  - 発行するカードは、共通仕様を満たすものとする

スマートカードのインフラ化

- 共通認識
  - インフラは専用システムではない
    ⇒ 多目的カードシステムの必要性
    ⇒ 道路、電力、ガス、水道等と同じ
  - インフラは、利用者、サービス提供者、ベンダー等の皆に有益である
  - 大量生産により、製造コストを大幅に減じる
  - サービス提供者による初期投資の大幅減



保険証のカード化について

- 「e-Japan戦略」において、スマートカードは電子政府サービスを受けるための官民のインターフェイスと位置づけられている
- 公的分野におけるカード導入計画
  - 住民基本台帳（平成15年8月から）
  - 公的個人認証サービス（カード利用を前提）
  - 健康保険証
- 上記3つのサービスを国民が選ぶ
- 一枚目のスマートカードは政府による支援を実施する
- 関連省庁の協力により、相乗り前提のスマートカードの配布は、別財源で行えるよう努力すべきである

まとめ

- 医療機関の完全なペーパーレス・フィルムレスは、まもなく制度的に可能になる
- サイバー空間でのセキュリティ確保は、登録・認証とアクセスコントロールが基本
- 医療分野の認証サービスの実施が不可欠
- 住基カードあるいは行政連携カードとの相乗りにより、認証は可能となる