

200501346A

厚生労働科学研究研究費補助金

医療技術評価総合研究事業

医籍データベースと医師資格 I Cカードの応用と評価に関する研究

平成17年度 総括研究報告書

主任研究者 山本 隆一

平成18（2006）年4月

目 次

I.	総括研究報告書		
	医籍データベースと医師資格 I Cカードの応用と 評価に関する研究	-----	1
	山本 隆一		
II.	研究成果の刊行に関する一覧表	-----	1 2
III.	研究成果の刊行物別冊	-----	1 3

医籍データベースと医師資格 IC カードの応用と評価に関する研究総括研究報告書

主任研究者 山本 隆一 東京大学大学院情報学環 助教授

研究要旨 医籍登録情報の電子化およびその高度利用は医療の IT 化を進め、実効あるものとするためにきわめて重要といえる。本研究では医籍等の資格データベースを活用する際に必須である IC カードの利用を保健医療福祉分野 PKI との連携や他の施策との関連の観点からデータベースのあり方および IC カードの要件の抽出を行い、住民基本台帳ネットワークとの連携を行う場合および行わない場合の運用、ISO 14442 Type B の IC カードの優位性、および利用指針の必要性を示した。

分担研究者

喜多 紘一 東京工業大学 像情報研究施設 IT 都市創造工学 特任教授
山下 芳範 福井大学医学部 医療情報部 助教授
田中 勝弥 東京大学医学部附属病院企画情報運営部 助手

A. 研究目的

わが国では国家的な目標として IT の活用による構造改革を推進している。2000 年以降 IT 戦略を作成し、各分野での IT 化を促進しているところである。医療はその中でも常に重要分野にあげられており、IT 加速化パッケージ 2003 では医師等の資格が電子的に確認できることを目指すことが求められている。また 2006 年 1 月に公表された IT 新改革戦略でも医師等の国家資格を確認できる電子署名基盤である HPKI

の推進が具体的にあげられている。医師等の国家資格は医療という社会サービスを担う公的資格であり、診療現場だけでなくさまざまな場面で確認できることが必要であるが、現状は本人の資格確認を随時おこなっているわけではない。診療所等の設立時には免許証を確認することで、また病院等では医療従事者の雇用時に免許証を確認することで、一応の確認はなされ、その後は 2 年に一度の 3 師調査、医療監視などで確認はされるが、その他の、診療場面や診断

書の確認などの、いわば日常の場面では実質的には確認されていない。もちろん確認は状況に応じて行うことは可能であるが、手間がかかることは事実であり、多くの場合はなされていない。この状態で現状大きな問題が生じていないのは、もっとも重要な診療や投薬において対面の原則が厳しく維持されており、医療従事者の職業的倫理意識が高いことに依存していると考えられる。対面診療の原則が、遠隔診療のような特例を除いて変わることはないと思われるが、今後の医療現場の IT 化によって、医療連携が高度化するにしたがって、同時に複数の医療従事者が診療に参加することも想定される。また現状では医療機関のレターヘッドや封筒の印字が一種の根拠になっている診断書や診療情報提供書の記載者の資格確認であるが、これらが電子化され電子的に送付される場合は、これまでの慣習的な確認方法は機能しない。したがって医療従事者の資格の電子的な確認は医療の IT 化を進めていく上で必須の事項と考えられる。厚生労働省はすでに医籍登録台帳の電子化に取り組んでおり、昨年度の特別研究の結果を受け、医籍台帳の電子化を前提として医籍データベースと前述の HPKI 電子署名基盤との連携を、主に IC カードの使用

を前提にして、高度利用のあり方を提言することにある。なお、本研究の実施にあたっては分担研究者に多くの研究を分担していただいたが、常に研究グループとして連携して行い、また経費も一括処理したことから総括報告書に一括して報告する。

B. 方法

B-1. HPKI との連携に関する問題点の調査

厚生労働省が平成 17 年 3 月に医療情報ネットワーク基盤検討会の成果として公表した保健医療福祉分野認証局ポリシおよびそのベースとなった IS IS17090 を精査し、HPKI 電子署名基盤と医籍データベースの連携の問題点を調査した。

B-2. 他の施策との関係

医療の IT 化は国家的要請であり、2000 年にしめされたグランドデザインにもさまざまな施策を組み込んだアクションプランが示されている。その中で特に医籍データベースの利活用と関係が深いのは医師等の資格を含めた電子署名であり、現状を俯瞰し医籍データベースとの関連を考察した。

B-3. 医療分野でのスマートカード（IC カード）利用に関する研究

医籍データベースの高度利用には資格情報を格納したいり、資格確認のアクセスキ

一としての IC カードのようなトークンの存在は必須である。わが国では住民基本台帳カードに代表されるように IC カードをこのような目的のトークンとしてもちいることが一般的であり、これは世界的に見ても主流である。そこで IC カードの現状を調査した。これには国際標準化機構 (ISO) で進められている医療分野での IC カードに関する標準化の動向も含めた。

C. 結果

C-1. HPKI との連携に関する問題点の調査

連携の検討を述べるために厚生労働省が公表した保健医療福祉分野認証局ポリシー (以降 HPKI 標準ポリシーと呼ぶ) の目次を掲載する。

HPKI 標準ポリシー目次

1 はじめに

1.1 概要

1.2 文書の名前と識別

1.3 PKI の関係者

1.4 証明書の使用方法

1.5 ポリシ管理

1.6 定義と略語

2 公開及びリポジトリの責任

2.1 リポジトリ

2.2 証明書情報の公開

2.3 公開の時期又はその頻度

2.4 リポジトリへのアクセス管理

3 識別及び認証

3.1 名称決定

3.2 初回の本人性確認

3.2.1 私有鍵の所持を証明する方法

3.2.2 組織の認証

3.2.3 個人の認証

3.2.4 確認しない加入者の情報

3.2.5 機関の正当性確認

3.2.6 相互運用の基準

3.3 鍵更新申請時の本人性確認及び認証

3.3.1 通常の鍵更新時の本人性確認及び認証

3.3.2 証明書失効後の鍵更新の本人性確認及び認証

3.4 失効申請時の本人性確認及び認証

4 証明書のライフサイクルに対する運用上の要件

4.1 証明書申請

4.1.1 証明書の申請者

4.1.2 申請手続及び責任

4.2 証明書申請手続

4.2.1 本人性及び資格確認

4.2.2 証明書申請の承認又は却下

4.2.3 証明書申請手続期間

4.3 証明書発行

- 4.3.1 証明書発行時の認証局の機能
- 4.3.2 証明書発行後の通知
- 4.4 証明書の受理
 - 4.4.1 証明書の受理
 - 4.4.2 認証局による証明書の公開
 - 4.4.3 他のエンティティに対する認証局による証明書発行通知
- 4.5 鍵ペアと証明書の利用目的
 - 4.5.1 加入者の私有鍵と証明書の利用目的
 - 4.5.2 検証者の公開鍵と証明書の利用目的
- 4.6 証明書更新
 - 4.6.1 証明書更新の要件
 - 4.6.2 証明書の更新申請者
 - 4.6.3 証明書更新の処理手順
 - 4.6.4 加入者への新証明書発行通知
 - 4.6.5 更新された証明書の受理
 - 4.6.6 認証局による更新証明書の公開
 - 4.6.7 他のエンティティへの証明書発行通知
- 4.7 証明書の鍵更新（鍵更新を伴う証明書更新）
 - 4.7.1 証明書鍵更新の要件
 - 4.7.2 鍵更新申請者
 - 4.7.3 鍵更新申請の処理手順
 - 4.7.4 加入者への新証明書発行通知
 - 4.7.5 鍵更新された証明書の受理
 - 4.7.6 認証局による鍵更新証明書の公開
 - 4.7.7 他のエンティティへの証明書発行通知
- 4.8 証明書変更
- 4.9 証明書の失効と一時停止
 - 4.9.1 証明書失効の要件
 - 4.9.2 失効申請者
 - 4.9.3 失効申請の処理手順
 - 4.9.4 失効における猶予期間
 - 4.9.5 認証局による失効申請の処理期間
 - 4.9.6 検証者の失効情報確認の要件
 - 4.9.7 CRL 発行頻度
 - 4.9.8 CRL が公開されない最大期間
 - 4.9.9 オンラインでの失効／ステータス情報の入手方法
 - 4.9.10 オンラインでの失効確認要件
 - 4.9.11 その他利用可能な失効情報確認手段
 - 4.9.12 鍵の危殆化に関する特別な要件
 - 4.9.13 証明書一時停止の要件
 - 4.9.14 一時停止申請者
 - 4.9.15 一時停止申請の処理手順
 - 4.9.16 一時停止期間の制限
- 4.10 証明書ステータスの確認サービス

4.11	加入の終了	6.2.10	私有鍵の廃棄方法
4.12	私有鍵預託と鍵回復	6.2.11	暗号モジュールの評価
5	建物・関連設備、運用のセキュリティ管理	6.3	鍵ペア管理に関するその他の面
5.1	建物及び物理的管理	6.3.1	公開鍵のアーカイブ
5.2	手続的管理	6.3.2	公開鍵証明書の有効期間と鍵ペアの使用期間
5.3	要員管理	6.4	活性化用データ 43
5.4	監査ログの取扱い	6.5	コンピュータのセキュリティ管理
5.5	記録の保管	6.6	ライフサイクルの技術的管理
5.6	鍵の切り替え	6.7	ネットワークのセキュリティ管理
5.7	危殆化及び災害からの復旧	6.8	タイムスタンプ
5.8	認証局又は登録局の終了	7	証明書及び失効リスト及び OCSP のプロファイル
6	技術的なセキュリティ管理	7.1	証明書のプロファイル
6.1	鍵ペアの生成と実装	7.1.10	保健医療福祉分野の属性 (hcRole)
6.2	私有鍵の保護及び暗号モジュール技術的管理	7.2	証明書失効リストのプロファイル
6.2.1	暗号モジュールの標準及び管理	7.3	OCSP プロファイル 55
6.2.2	私有鍵の複数人によるコントロール	8	準拠性監査とその他の評価 56
6.2.3	私有鍵のエスクロウ	8.1	監査頻度
6.2.4	私有鍵のバックアップ	8.2	監査者の身元・資格
6.2.5	私有鍵のアーカイブ	8.3	監査者と被監査者の関係
6.2.6	暗号モジュールへの私有鍵の格納と取り出し	8.4	監査テーマ
6.2.7	暗号モジュールへの私有鍵の格納	8.5	監査指摘事項への対応
6.2.8	私有鍵の活性化方法	8.6	監査結果の通知
6.2.9	私有鍵の非活性化方法	9	その他の業務上及び法務上の事項
		9.1	料金

- 9.2 財務上の責任
- 9.3 業務情報の秘密保護
- 9.4 個人情報のプライバシー保護
- 9.5 知的財産権
- 9.6 表明保証
- 9.7 無保証
- 9.8 責任制限
- 9.9 補償
- 9.10 本ポリシーの有効期間と終了
- 9.11 関係者間の個々の通知と連絡
- 9.12 改訂
- 9.13 紛争解決手続
- 9.14 準拠法
- 9.15 適用法の遵守
- 9.16 雑則
- 9.17 その他の条項

なお、本研究と無関係を考えられる部分の詳細は割愛した。またこの HPKI 標準ポリシーは 17 年に厚労省が公表したものを HPKI 専門家会議で小改訂してものである。

まず 3 章の認証および、4 章の証明書ライフサイクルの部分で医籍データベースとの連携が検討される。この 2 つの章の関係は PKI を専門としないものにとってはわかりにくい、3 章は証明書を申請する側、すなわち医療従事者等の準備する要件であり、4 章は証明書を発行する側が確認する

要件である。現状の HPKI ポリシは利用できる医籍データベースがない、という前提で書かれており、対面による医師等の免許証の確認または免許証のコピーに実印を捺印し、印鑑証明書を添付して郵送することで、資格を確認している。対面や郵送の場合はこれでよいが、HPKI 標準ポリシーはオンラインによる申請についても記載されていて、このときの本人性、実在性確認は公的個人認証サービスを用い、資格確認は資格データベースが整備され利用できることを前提にしている。つまりオンラインによる申請を可能にするためには、HPKI 認証局が公的個人サービスにおける署名検証者になり、さらに申請情報をキーに資格データベースを検索できる必要がある。公的個人認証サービスの利用は現状では HPKI 標準ポリシーに準拠することで直接検証者になれるわけではないが、認定特定認証事業者として認定されれば可能になる。また今後は HPKI 標準ポリシーに準拠するだけで、検証者となるように制度改正される可能性もある。

したがって医籍をはじめとする医療従事者の国家資格のデータベースを整備する場合、HPKI 認証局に対して、住民登録情報をキーに検索を許す必要がある。元来、国

家資格取得情報は官報に掲載され、公開情報と考えられるが、官報に掲載される情報は氏名（カタカナ表記）のみで、住民登録情報は含まれていない。また医籍登録台帳でも現住所や住民基本台帳番号は含まれていない。これは言い換えれば登録台帳やそれを単純に電子化した資格データベースだけの情報では資格者を一意に特定することは困難な場合があることを意味している。言い換えれば HPKI 認証局が仮に資格データベースにアクセスを許されても、申請者の資格確認が十分にはできないことを意味している。現状の登録項目では、やはり本人が持っている免許証を確認しなければならない。しかしながらこの紙の免許証は特別な識別模様などを持っているわけではなく、容易に複製できる。

次に HPKI 標準ポリシーの中で医籍等のデータベースと関連する部分は、6 章の私有鍵の格納モジュールであり、エンドエンティティ、すなわち国家資格を持つ医療従事者等は FIPS 140-2 Level1 以上に相当するモジュールに格納しなければならない。単に IC カードであればこれに相当するわけではなく、それなりの強度を持った IC カードを用いる必要があるが、IC カード以外で携帯可能な安価なデバイスは現状はほとん

どない。したがって銀実には HPKI 署名基盤を用いて署名するためには適切な IC カードに私有鍵を格納する必要がある。逆に言えばこのような IC カードを持つことによって、最低限、電子署名を行えば資格を電子的に確認できることになる。医籍等をデータベース化する大きな目的の一つが医師等の国家資格を電子的に確認することであり、その意味で、医籍データベースと HPKI はエンドエンティティの所有する IC カードを介して相補的であり、相互依存しているといえる。

C-2. 他の施策との関係

平成 18 年 1 月に公表された IT 新改革戦略の医療の項の具体的目標の「医療情報化インフラの整備」に以下の項目があげられている。

1. 医療機関の機能、規模、特性等を考慮して、目的に応じた情報化の必要性と活用度を適切に評価するための指標を 2007 年度までに開発する。
2. 統合系医療情報システム（オーダリングシステム、統合的電子カルテ等）を 200 床以上の医療機関のほとんどに導入し、業務の効率化、医療安全および診療情報の提供を実現する（400 床以上は 2008 年度まで、400 床未満は 2010 年度まで）。

3. 統合系医療情報システム導入の費用対効果に乏しい小規模な医療機関に対しては、低コストで診療情報連携に適した電子カルテ等を用いて、2010年度までに面的な医療連携を図る。

4. 医療機関間の診療情報連携、マルチベンダー化によるシステム導入コストの低減を実現するため、システムベンダーは標準的なデータフォーマット及びデータ交換規約の医療情報システムへの標準搭載を2006年度より開始する。

5. 医療機関等におけるより高度な医療安全や業務の効率化を実現するため、2010年度までに電子タグ等のユビキタスネット関連技術の活用を推進する。

6. 厳格な本人確認を行いつつ診療情報等の安全な交換や参照を実現するため、HPKI (Healthcare Public Key Infrastructure: 保健医療福祉分野の公開鍵基盤)、安全で安心なネットワーク基盤等を2008年度までに整備する。

7. 円滑な情報化を支援する助言・指導等を通じて医療情報化インフラの利用価値を高める医療機関CIOの在り方について検討し、2008年度までに人材育成の体制を整備する。上記の中で6は直接的にHPKIの整備を示したもので、先に触れた。3の統合系医療

情報システムの導入に関して「面的な医療連携を図る」とあるが、これは従来の簡単な診療情報提供書による直線的な連携、すなわち、患者を紹介したという事実が中心で、それぞれの医療機関が並行的に連携して医療にあたるという要素のない連携から、情報を高度に共有し、同時並行的に複数の医療機関が同一の患者の医療にあたる体制と考えることができる。現状で、先進的な試みとして診療情報提供書や患者への情報提供を電子化し、高度化に取り組んでいるプロジェクトがいくつか存在する。しかしいわゆる面的な連携は過去に試みられたことはあったが持続して実施しているところは皆無である。これには様々な理由が考えられるが、安価で確実な資格認証を維持することが難しいことも原因の一つであることは確実である。資格認証は技術的には電子署名と同様であり、HPKIのような認証基盤を作ればよいが、やはり資格の確認が大変な手間になり、継続した実運用が難しい。この点でも現場での資格確認の一助のなる形での資格データベースの整備は必須と考えることができる。

C-3. 医療分野でのスマートカード (IC カード) 利用に関する研究

このテーマに関しては2つの側面から研

究を開始した。一つは実際に利用可能な IC カードを用いて仮想的な医籍データベースを構築し、運用実験を行うことで、本年度は、ISO 14443 の 3 つの規格 Type A, B, C をそれぞれ代表するものとして、Mifare、eLWISSE、Felica の各仕様と適合性を検討した。検討には DENSO-Wave 社の Reader-Writer およびカードアクセスライブラリを用い、分担研究者を含めた全員で異なる環境で評価をおこなった。実験環境が整ったのが遅れたために、評価は一部にとどまっているが、HPKI 署名基盤を用いて医師等の公的資格を示して記名押印に代わる電子署名を行う場合、デバイス内で署名を行う、すなわち私有鍵を外部に露出しないことが推奨され、その意味では CPU 機能の搭載が保障される Type B が適切と考えられた。今後実験を継続し、主に Type B のスマートカードの利用を前提に利用の指針をまとめる予定である。

またこれとは別に IC カード利用のガイドラインをまとめる予定である。現時点では目次案を作成できているのでこれを示す。

1. 適用範囲

HPKI で使用される IC カードに対する要求事項を定める。

2. 用語の定義

3. 機能

私有鍵保存機能

公開鍵証明書保存機能

私有鍵生成機能（オプション、公開鍵エクスポート機能を含む）

私有鍵インポート機能（オプション）

公開鍵証明書インポート機能

公開鍵証明書エクスポート機能

署名機能

私有鍵活性化機能

4. アプリケーションの独立性

4.1 組み込みタイプ

4.2 ダウンロードタイプ

4.3 シングルアプリケーション

4.4 マルチアプリケーション

5. カード内フォーマット

6. インターフェイス

6.1 PC/SC

6.2 クリプト API

6.3 NICSS フレームワーク

7. セキュリティ要求事項

7.1 公開鍵の送付と公開鍵証明書

7.2 公開鍵のインポート

7.3 私有鍵をインポートする場合

7.4 NICSS フレームワーク

8. その他の要求事項

8.1 認証用鍵、暗号化用鍵との混同禁止

8.2 署名を行う場合の注意事項

D. 考察

医籍データベースを高度利用するためには HPKI との連携が非常に重要である。しかし C-1 に示したように、現状の登録項目をベースにデータベースを作成した場合、HPKI の要求する厳密さに応えることは難しい。これには2つの方法が考えられる。一つは医籍等の国家資格データベースに実在性、本人性を結び付けるための情報を付加する方法で、簡単に言えば住民基本台帳ネットワークとのリンクを実現するものである。この方法を用いれば死亡による資格データベースからの消去も自動化されうる。もう一つは資格獲得時、つまり国家試験合格後の申請時に HPKI 署名用証明書を発行し、その際に公的個人認証サービスを用いる方法である。PKI による署名用公開鍵証明書は有効期限があり一般には1～5年程度である。常識的には3年に一度程度は更新する必要がある。これは公的個人認証サービスも同様である。更新はその時点で有効な旧の証明書および私有鍵を用いることで電子申請可能であるが、その際に公的個人認証サービスによる署名を要求することにすればその都度、実在性、本人性は公的

個人認証サービスにまかせることができ、医籍等の資格データベースに、住民基本台帳ネットワークとのリンク機能は必要ない。またその都度現住所等を確認できるので、3師調査の一助として利用することも可能である。しかしこの方法は初めて申請するときに必ず公的個人認証サービスを利用しなければならない。新規資格獲得者は合格後に交付申請をするので、これを電子申請にすることを義務付ければ問題はないが、すでに資格を獲得している者にも強制しなければならない。もともと HPKI 証明書の取得は原則として義務ではないので、実現は不可能ではない。

いずれにしても IC カードの利用は必須であるが、米国 NIST の FIPS140 規格も 140-1 から 140-2 への改訂の際に Level 1 の例として掲載されていたスマートカード (IC カード) が削除された。つまり単に IC カードというだけでは医籍データベースを活用するためのデバイスとしては不十分である。適切な指針の作成が必要と考えられ、今後本研究で作成を試みる予定である。

E. 結論

医籍情報の電子化と高度利用に関して以下の項目の研究をおこない成果を得た。

(1)HPKI との連携に関しての問題点の調査し、現状の医籍等の収載項目を単純データベース化するだけでは問題あることを示した。解決策としては資格データベース自体が住民基本台帳ネットワークにリンクする方法と、リンクせずに運用上関係付ける方法を示した。(2)IT 新改革戦略に記載されている統合系診療情報システムの導入による面的な連携医療の実現のためには HPKI 電子署名基盤以外に資格確認が可能な認証基盤の作成を手助けするような機能が医籍等の資格データベースに必要であることを示した。(3)IC カードとしては ISO14443 に規定されている Type B のスマートカードがもっとも適切であることを実験的に明らかにした。また IC カードを使用するためのガイドラインが必要と考え、その作成に着手した。

F. 健康危険情報

特になし。

G. 発表

論文

1. 山本隆一、医療従事者資格 IC カード導入のコストモデルの検討、医療情報学連合大会論文集 2005、pp898-901、2005
2. 山本隆一、海外の医療現場での個人

情報保護の動き、INR インターナショナルナーシングレビュー、28 (5)、42-45、日本看護協会出版会、東京、2005

3. 山本隆一、診療情報システムと個人情報保護、医学のあゆみ、215 (4)、231-234、医歯薬出版株式会社、東京、2005

4. 山本隆一、プライバシーの考え方と個人情報保護、看護展望、30 (5)、17-20、メヂカルフレンド社、東京、2005

5. 山本隆一、医療における個人情報保護とセキュリティ、日本病院会雑誌、52 (1)、106-124、(社) 日本病院会、東京、2005

H. 知的財産権の登録・出願状況

現在のところなし。

研究成果の刊行に関する一覧表

雑誌

発表者氏名	論文タイトル名	発表誌名	巻号	ページ	出版年
山本隆一	医療従事者資格 I C カード導入のコストモデルの検討	医療情報学会雑誌 (別冊)	第25回医療情報学連合大会論文集	Pp898-901	2005

医療従事者資格ICカード導入のコストモデルの検討

山本 隆一¹⁾ 喜多 紘一²⁾ 清谷 哲朗³⁾ 公文 敦⁴⁾ 田中 勝弥⁵⁾ 山下 芳範⁶⁾ 吉田 真弓¹⁾
東京大学 大学院 情報学環¹⁾ 東京工業大学 像情報研究施設 IT都市創造工学²⁾
関西労災病院 医療情報部³⁾ 適寿リハビリテーション病院⁴⁾
東京大学 医学部付属病院 企画情報運営部⁵⁾ 福井大学医学部 医療情報部⁶⁾

Cost Model for Applying Healthcare Professional Smart Card

YAMAMOTO RYUICHI¹⁾ KITA KOUICHI²⁾ KIYOTANI TETSUROU³⁾ KUMON ATSUSHI¹⁾
TANAKA KATSUYA³⁾ YAMASHITA YOSHINORI⁶⁾ YOSHIDA MAYUMI¹⁾

Interfaculty Initiative In Information Studies, Graduate School of the University of Tokyo, Tokyo, Japan¹⁾

Tokyo Institute of Technology Imaging Science and Engineering Laboratory, Yokohama, Japan²⁾

Department of Hospital Information Systems, Kansai Rousai Hospital, Amagasaki, Japan³⁾

Tekiju Rehabilitation Hospital, Kobe, Japan⁴⁾

Department of Planning, Information and Management, The University of Tokyo Hospital, Tokyo, Japan⁵⁾

Department of Medical Informatics, University of Fukui Hospital, Fukui, Japan⁶⁾

Abstract: In Japan, Ministry of Health, Labor and Welfare (MHLW) published the suggestion for network security and the standard policy of Healthcare PKI certification. For compliance to them, using security tokens, such as smart cards, for identification and certification as regulated healthcare professionals will be indispensable in the near future. We studied the cost models of healthcare smart cards distribution in French and Chinese Taipei where smart cards are distributed to all people as health care insurance identifier and to all physicians as healthcare professional identifier. In France, health plans are responsible for almost all cost for distributing tokens otherwise in Chinese Taipei, the government is responsible for all cost. We discussed that the difference is mainly due to difference of health plan payment system. And the health plan payment system in Japan is different from French system and Chinese Taipei. So we should employ another cost model, such as payment incentive to the product of computerized healthcare information systems.

Keywords: Security token, Smart card, Public key infrastructure, Cost model

1. はじめに

わが国では各分野でのIT化を促進しており、医療はその中でも常に重要分野にあげられている。さまざまな解決すべき課題があるが、セキュリティの確保とプライバシーの保護が重要な課題であることは2004年9月に厚生労働省の医療情報ネットワーク基盤検討会の最終報告¹⁾にも明記されているように異論はない。セキュリティやプライバシー保護は技術的な対策だけで達成されるものではなく、組織的、制度的、倫理的側面が重要ではあるが、IT加の中で最低限の技術的対策は避けられない。技術的対策のもっとも基礎となるのが、認証および責任の所在を明確にするための電子署名である。厚生労働省も先の医療情報ネットワーク基盤検討会の成果物として保健医療福祉分野PKI認証局証明書ポリシー²⁾を公表している。認証はパスワードのような記憶に依存する方法や生体計測認証のように生体だけで実施することも不可能ではないが、いずれも明確な欠点を持ち、また電子署名を実施するためには公開鍵暗号の私有鍵を本人しか使用できない状態で管理しなければならない。つまり認証情報や署名用の私有鍵を格納するセキュリティアークの導入は現状では避けられない。セキュリティアーク

ンにはUSBトークンや生体埋め込みチップなどさまざまなものが考えられるが、コストやトークン自体の安全性を考慮すればICカード(スマートカード)が最適であることにも異論がないであろう。ICカードは安価とは言え、リーダやライタまで含めればそれなりのコストは必要で、わが国の医療ドメイン全体で導入を図るためにはコストモデルの検討も重要である。我々は平成16年度厚生労働科学研究補助金特別研究事業を実施する機会を得、ICカード導入のコストモデルをすでに導入が進められているフランス、台湾の調査を含めた検討の行なうことができたので、結果を報告する。

2. 方法

医籍情報・資格情報を電子的に利活用することに先進的に取り組んでいるフランスを調査した。患者への医療用ICカードの開発と配布を担当しているGIE SesamVitale³⁾および医師等の医療従事者に配布するICカードの開発と配布と担当しているGIP CPS⁴⁾を訪問し、GIE SesamVitaleでは開発および国際担当のNoel Nader氏、GIP CPSでは副所長のRichard Decottignies氏とそれぞれ数時間の会見をおこない、現状と将来像、および問題点を明らかにし、わが国での取り組み参考になる点を明らかに

した。また最近取り組みをはじめた台湾についても現状を調査した。

医療のIT化は国家的要請であり、2000年にしめされたグランドデザインにもさまざまな施策を組み込んだアクションプランが示されている。その中で特に医籍データベースの利活用と関係が深いのは医師等の資格を含めた電子署名であり、現状を俯瞰し医籍データベースとの関連を考察した。

3. 結果

3.1 フランスの診療報酬請求

フランスで診療を受けた場合、診療報酬の支払いには二つのパターンがある。一つはほぼわが国と同様で、医療機関は総請求額から強制健康保険および任意健康保険の負担分を差し引いて患者に請求し、残額を医療機関から保険者に請求する方法で、もう一つは医療機関は患者に一括して請求し、診療明細を患者に交付する。患者は診療明細書をまず強制保険の保険者に送付し、保険給付を受領する。さらに任意保険に加入している場合は、診療明細を任意保険の保険者に送付し、保険給付を受ける。前者の医療機関から保険者に請求する方法は、医療機関の不正が相次いだために、実質的にはほとんど行われておらず、ほとんどの場合、患者は一旦全額を支払い、事後に保険者から保険給付を受け取ることになる。ここで問題になるのは立替期間で、医療の高度化にともなって次第に長くなり、1990年ごろには強制保険で2~3週間を要するようになっていた。任意保険まで含めると1ヶ月を超えることもあり、医療機関を利用する市民にとって大きな負担となっていた。

3.2 Sesam-Vitale プロジェクト

このような背景で、患者および医師、薬剤師等にICカードを配布し、保険資格と医療従事者資格をオンラインで確認し、保険者における事務処理を簡素化し、患者の立替期間を短縮化することを目的にSesam-Vitaleプロジェクトが開始された。93年以降、さまざまな問題を克服しながら進められており、2004年には診療所における診療の90%以上でこの仕組みが利用されている。患者にとっては患者カード(Sesam-Vitaleカード)を取得し、定期的に更新するという手間が生じるが、ほとんどの場合、強制保険加入時に配布され、保険者から更新等の通知もなされるためにそれほど大きな負担はなく、フランス全国のほぼすべての診療所と薬局が対応しているために、このカードを利用すれば立替期間が極めて短くなり、利用のインセンティブは高い。

3.3 GIE Sesam-Vitale

この患者カード(Sesam-Vitaleカード)の開発から配布までを担当しているのがGIE Sesam-Vitaleである。GIEはフランスの法人の種別で、政府が予算を含む活動を監督するが、経費を負担しない法人である。わが国の財団法人に近いと考えられる。GIEは出資額に応じて理事会で発言権が認めら

ず、主な出資者は保険者である。また患者等へのカードの配布費用(一人あたり約5ユーロ)はすべて保険者が負担している。

3.4 Sesam-Vitale カード

カードは接触型のスマートカードで患者のID情報およびカード自体を識別する情報だけが格納されている。PINが設定されており、患者は医療機関でカードをリーダーにセットしPINを入力する必要がある。

Sesam-Vitaleカードは現時点では診療報酬請求にのみ利用されているが、2002年に医療情報が患者に所属することが法的に明記され、2004年には16才以上の診療情報を政府が管理するサーバに保存することになっており、これに対応するために、現在Sesam-Vitale2カードが準備されている。2005年からは16才以上のすべての国民にSesam-Vitale2カードが配布される予定で、このカードは従来のSesam-Vitaleカードと異なり、サーバに存在する診療情報のアクセスをコントロールするためのアプリケーションも存在するマルチアプリケーションカードである。

3.5 Sesam-Vitale の経済的背景

GIE Sesam-Vitaleの経費の大部分(後述のGIP CPSでもそうであるが)は保険者が負担している。保険者はSesam-Vitaleの仕組みにより、診療報酬請求はほぼ100%電子化され、事務経費が大幅に削減できるためにむしろ積極的に経費負担をしていることであった。カード発行の費用だけでなく、診療者や薬局が必要な設備投資も限度はあるものの実質的には大部分保険者からの補助金でまかなっている。

3.6 医療従事者カード

診療所、薬局、助産所の医療従事者のほぼすべてにCPSと呼ばれる医療従事者カードが配布されている。CPSは現行のSesam-Vitaleカードに比べてかなり多くの情報を格納している。とは言ってもデータとして保持しているのは、基本的には医療従事者のIDおよび電子署名に用いる署名鍵および証明書データをデータとして保持し、さらに伝送経路の暗号化に用いるための鍵等も共通エリアとして持っている。このカードは言わばネットワークセキュリティを確保する装置および医療従事者の認証カードとしての機能を持つと言ってよい。Sesam-Vitaleカードより高機能であるために一枚あたりの発行コストは20ユーロである。

3.7 GIP CPS

CPSカードの開発や発行・配布を担当しているのはGIP CPSである。GIPはやはりフランスの法人の種別で、政府が予算を含む活動を監督し、経費も一部負担している。日本でいえば独立行政法人に近いと考えられる。政府の出資比率は低く、最大の出資者は保険者である。それ以外に医師会等の医療従事者団体も出資をしている。GIPでは理事

会の発言権は出資額に比例せず、GIP CPS の場合は医師会等の医療従事者団体の発言権が強い。また開発、発行・配布を担当していると言ってもいずれも実務は入札による外注で、GIP CPS はシンクタンク的な機能を果たしている。

3.8 CPS の経済的背景

GIP CPS には政府も医師会等の職能団体も出資はしているが、診療所や薬局に対する CPS のカード発行のコストはすべて保険者が負担している。CPS カードは3年に一度更新しているため、毎年ほぼ一定数の更新発行があり、年間関係費はほぼ1300万ユーロで、漸増しているがすべて保険者が負担している。現在使われているアプリケーションは Sesam-Vitale だけであり、前述のように Sesam-Vitale は保険者に多大な事務経費の節減をもたらすためにこのような経費負担が可能になっていると考えられる。ただし病院の勤務者に対する CPS カードの発行経費は病院負担となっている。病院とは言えほかのアプリケーションが存在するわけではなく、そのために病院勤務者への CPS カードの普及は低い。

3.9 CPS の今後

Sesam-Vitale の項でも触れたが2002年に医療情報に関する患者の権利法が成立し、2004年には16歳以上のすべての国民の診療情報を一元的にデータベース管理する法律が成立し、2007年の実施に向けて計画が進められている。これが実施されればデータベースへのアクセスキーとしての CPS カードの意義が付加されるために、CPS は病院勤務者も含めて拡大するであろう。

3.10 台湾における医療ICカードの状況

台湾では患者カードのIC化とともに、医師資格カードが発行されている。医師資格カードの発行主体は、台湾衛生署(日本の厚生労働省に相当)で、患者カードの内容アクセスを目的として利用されている。患者カードには重大な疾患の履歴およびCT・MR・PETなどの高額検査の実施状況が記録されており、医療機関はこれらのチェックが義務付けられている。例えば高額検査が月別実施回数制限を上回った場合は診療報酬が支払われない。このため、診察室で確認を行う必要があり、患者カードと医師資格カードを同時に挿して利用するための専用ハードウェア及びドライバが提供されており、それぞれの病院情報システムの診療用端末として利用しているパソコン上で利用できるように整備されている。

この医師資格カードには、電子署名及び暗号化を想定した証明書および私有鍵が格納されており、一部の高度医療機関ではあるが、電子カルテや地域医療応用についても試行が行われている。

なお、医師資格カードの利用について、衛生署としては特に制限を設けておらず、また、仕様にも公開しており、医療機関等は独自に応用を試みる事が可能である。既に、病歴管理を行うシステ

ム、糖尿病在宅フォローアップのシステム、病診連携のシステムなどの医師資格カードが活用されているプロジェクトが実験的に始められている。

4. 考察

セキュリティトークンとしてのICカードの重要性は最初に述べたが、ICカードの配布および保守には相応の経費が必要で、継続して全国で使用するためには安定した財源が必要である。この面で一日の長があるフランスでは診療報酬のオンライン化による保険者の事務経費の節減によってこの問題を解決している。これは非常に現実的ですぐれた方法であるが、フランスでは背景に患者の一時的な立替払い制度があり、その事務処理の遅れが直接市民の負担となることからコンセンサスを得やすいという特質があったことは無視できない。

ではわが国ではどうであろうか。レセプトの電子化は保険薬局ではかなり浸透しているが、医療機関ではまだ普及率はそれほど高くなく、オンラインではない。これはフランスと異なり、提出が一月ごとであり、随時請求ではないために、そもそもリアルタイム性が利点であるオンライン請求の必要性が低いことによると考えられる。

保険者から見ても診療報酬請求の審査制度は2段階で第一段階は支払い基金等が審査で診療費は医療機関にいったん支払われ、第二段階での審査で問題があった場合、医療機関は返還を要求されることになる。つまり第一段階の事務処理の遅れがもし生じたとしても困るのは医療機関で保険者ではない。オンライン化は第一段階の審査のみに影響を与え、その診療報酬請求の事務手続きに及ぼす効果は第一段階の審査機関だけに限定的である。

以上の点からフランスのように保険者または第一段階の審査機関が経費を負担して資格カードを実用レベルでほぼ全員に配布することは現状では容易とはいえない。

台湾ではカード配布の費用は国費で負担しているが、そもそも保険が国営保険一つしかなく、きわめてシンプルなモデルと考えることができる。少なくとも経費負担の面ではわが国にあまり参考になるとはいえない。

次に医療従事者が経費を負担するモデルを考える。新規の国家試験合格者は現状でも資格登録の際に手数料を必要とする。この手数料は資格カードの発行に要する経費と比べれば高額であり、ここに資格カード発行経費を上乗せしても大きな障害はないと思われる。問題はその後保守経費であろう。カード自体の物理的な劣化や電子証明書の有効期限等の理由で2~3年に一度は更新する必要がある。一枚あたりの経費はフランスの20ユーロとあまり大きくは変わらないことが予想される。つまり経費としては決して高額ではないが、まったくインセンティブなしには維持が難しい。インセンティブとして政府の補助では継続性に問題が生じる可能性がある。

2-H-1-3 セキュリティ/一般口演: セキュリティ

少し視点を変えて診療への応用を考えてみたい。診療情報提供書は現状は紙ベースであり、書くための労力もスペースも連携医療をさらに高度化するためには問題がある。医療のIT化が十分進めば診療情報の中で重要なものは電子化されていることになり、電子的に診療情報提供書を作成することは容易である。情報量の制限はゆるやかになり、例えば初診時から紹介時までの処方履歴、画像検査、検体検査などの客観情報をすべて含めることも容易である。現状の紙ベースの診療情報提供書よりはるかに情報密度の高いものを作成することはそれほど困難ではない。また同様のことが患者等への情報提供でも言える。パソコンの普及率は十分高く、患者等の要望も大きい。さらにはセカンドオピニオンの普及にも有用であり、電子化診療情報提供書にインセンティブをつけることには大きな問題はないと考えられる。

しかしこのような診療情報が改ざんされてはならないし、作成の責任の所在は明確でなくてはならず、電子署名は必須である。したがって医療ドメインで

活用可能な公開鍵基盤が整備されれば、私有鍵の格納先としてICカードは考えやすい。

このようなインセンティブがあれば2～3年に一度の数千円の経費負担を医師等にもとめることも十分可能と考える。

参考文献

- [1] 今後の医療情報ネットワーク基盤のあり方について: 「<http://www.mhlw.go.jp/shingi/2004/09/s0930-10a.html> (2005年9月1日確認)」厚生労働省医療情報ネットワーク基盤検討会最終報告
- [2] 保健医療福祉分野PKI認証局証明書ポリン: 「<http://www.mhlw.go.jp/shingi/2005/04/s0401-1.html> (2005年9月1日確認)」厚生労働省医療情報ネットワーク基盤検討会
- [3] GIE Sesam-Vitale: 「<http://www.sesam-vitale.fr/index.asp> (2005年9月1日確認)」Groupement d'Interet Economique Sasam-Vitale
- [4] GIP CPS: 「<http://www.gip-cps.fr/> (2005年9月1日確認)」Groupement d'Interet Public - Carte de Professionnelle de Sante