厚生労働行政推進調査事業費補助金（地域医療基盤開発推進研究事業）
分担研究報告書

個人番号カードを活用した医療従事者認証手法に関する研究

医療従事者認証サービスの運用方法の検討、国際的な取り組みとの整合性の調査・検討

研究分担者　喜多紘一
一般社団法人保健医療福祉情報安全管理適合性評価協会　理事長

研究要旨　本研究では「個人番号カードを活用した医療従事者認証手法に関する研究」の中の分担研究として「医療従事者認証サービスの運用方法の検討、国際的な取り組みとの整合性の調査・検討」を行うものである。その為に電子生涯健康手帳を例に検討した。「電子生涯健康手帳」とは利用者が医療機関や健康管理施設等から得た医療情報や利用者等が記録した情報をサーバ上に登録し、利用場面に合わせて健康情報を選択し、診療等の場面に応じて適切に診療を受ける為に必要とされる健康情報を医療機関等やサービス提供者等に提示、あるいは自己の健康管理の為に閲覧できるシステムである。そのサービスの運用あるいはシステム設計に於いて「公的個人認証利用サービス」（ＪＰＫＩ）とヘルスケアＰＫＩ（ＨＰＫＩ）をどのように利用していくか、特に医療従事者認証モデルを作成し、実際の診療場面や健康管理の場面等を想定して評価を行った。
その結果、国家資格はＨＰＫＩの方が扱いやすいが、国家資格以外はＪＰＫＩ＋属性証明書の利用が考えられる。その場合ＪＰＫＩでは４情報が明確になってしまうので、業務に使用するには抵抗がある。３枚目のＪＰＫＩ証明書が検討されているので、その際、住所、生年月日、性別のない証明書も検討する必要がある。また、ＪＰＫＩの有効性確認は機関が制限されているので、社会システムとして工夫が必要である。
電子生涯健康手帳のプロトタイプの意義は、まだ少ないサンプルの調査であるが、理解いただけたとの印象である。実際の使用を配慮し患者や医療従事者の立場での必要な情報、見やすさの追及を始めるべき時期である。
ISO17090 Part2 規格は次回見直し時、属性証明部分は hcRole が absent に成っていることを含め検討が必要である。

A. 研究目的

本研究では「個人番号カードを活用した医療従事者認証手法に関する研究」の中の分担研究として「医療従事者認証サービスの運用方法の検討、国際的な取り組みとの整合性の調査・検討」を行う。

その為にサービスの一例として生まれてから死ぬまでの「電子生涯健康手帳」サービスを例にして検討を行う。「電子生涯健康手帳」サービスとは利用者が医療機関や健康管理施設等から得た医療情報や利用者等が記録した情報をサーバ上に登録し、利用場面に合わせて蓄積された健康情報を選択し、① 診療等の場面に応じて適切に診療を受ける為に必要とされる健康情報を医療機関等やサービス提供者等に提示、あるいは② 自己の健康管理の為に閲覧できるシステムである。そのサービスを運用あるいはシステム設計に於いて「公的個人認証利用サービス」（ＪＰＫＩ）とヘルス

ケアＰＫＩ（ＨＰＫＩ）とをどのように利用していくか、特に医療従事者認証サービスとして、公的個人認証利用サービス」（ＪＰＫＩ）と属性認証あるいは電子委任状の組合せをどのように利用していくのか実際の診療場面や健康管理の場面等で評価を行う。

本年度は特に、医療従事者が「電子生涯健康手帳」サービス参照する場合のアクセス制御および健康手帳情報の真正性確保の為に電子署名を利用した場合について検討をおこなう。

また、本検討に使用した「電子生涯健康手帳」のプロトタイプは検索機能およびダウンロード機能の改善を行い、医療従事者等からの評価をいただく。

進めるに当たり国際的な取り組みとの整合性を調査し、検討を行う。

Ｂ．研究方法

１．研究の前提条件

ＪＰＫＩおよびＨＰＫＩの運用の為の環境が以下のように整備されることを前提に研究を進める。

１）医療従事者のマイナンバーカードには搭載可能な公的個人認証サービスとして署名用証明書および利用者証明用電子証明書が発行されていること。

２）ＪＰＫＩの利用者の両証明書の有効性確認をＪ―ＬＩＳ（地方公共団体情報システム機構：(Japan Agency for Local Authority Information Systems)に対して行える機関が存在すること。

３）ＨＰＫＩの認証局を運用している日本医師会あるいは医療情報システム開発センターより署名用および認証用の証明書が発行されていること。

４）マイナンバー制度で利用される個人ごとのポータルサイトへヘルスケアデータを送付できるようになること。

５）地域連携システム及び医療情報匿名加工・提供機関の付帯サービスとして患者情報をマイナンバー制度で利用される個人ごとのポータルサイトへ送付可能になること。

６）ＪＰＫＩの両証明書に対して医療従事者の属性証明または電子委任状を発行する機関が存在すること。

７）電子委任状を保管する事業者が存在すること。

２．電子生涯健康手帳プロトタイプによる検討

本プロトタイプは患者が医療機関等から得た医療情報や利用者等が記録した情報をサーバ上に登録し、単に時間軸に並べて表示するばかりではなく、診療シナリオに応じて適切に診療を受ける為の判断として要求される健康情報を医療機関等に提示、あるいは自己の健康管理の為に必要な健康情報を閲覧できるシステムである。診療場面ごとに予め想定される健康情報を検索し、診療シナリオにそって医師が判断するための健康情報を提示できることを目的にしている。

プロトタイプの機能は以下を想定する。

１）ＩＤ申請・利用者用登録機能

２）ユーザログイン機能

（利用者、家族、ヘルスケアサービスプロバイダーごとにログイン可能）

３）パスワード管理機能

４）ユーザ基本情報参照・登録・更新機能

５）健康情報登録保管機能

６）健康情報一覧表示機能（時系列情報種別表示）

７）提示リスト作成・修正機能

（エピソードごとに健康情報をまとめる機能）

８）特定場面提示情報リスト一覧編集機能

（閲覧・提示場面（特定場面）のシナリオごとに提示リストを選択・整理する機能）

９）特定場面一覧表示機能

１０）表示用語マスター登録機能

３．HPKIカード（保健医療福祉分野公開鍵基盤カード）

HPKI （Healthcare Public Key Infrastructure）カードはISO17090に準拠して厚生労働省がとりまとめた「保健医療福祉分野 PKI 認証局　証明書ポリシ」に従って発行されたカードである。電子署名用と認証用の証明書を発行することができる。

保健医療福祉分野の国家資格と、院長・管理薬剤師などの管理者資格を認証することができる。

日本医師会からは医師資格証、日本薬剤師会からは薬剤師資格証として、医療情報システム開発センターからは保健医療福祉分野PKI（HPKI）電子証明書として発行されている。

４．ＪＰＫＩと属性認証の併用

公的個人認証（ＪＰＫI）を用いる場合はそれだけでは医療従事者であるか判らないので属性証明書の利用が考えられる。

属性証明として以下の２方式を検討する。

４．１　電子委任状による方法

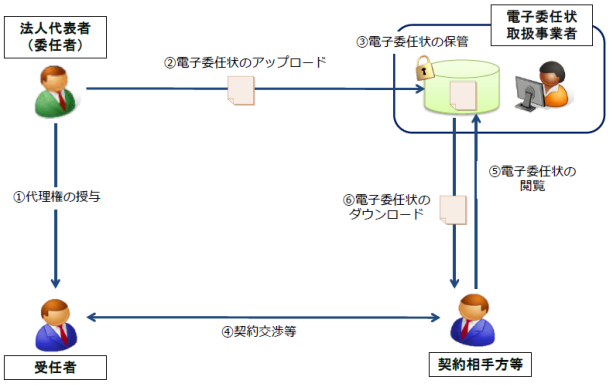

図１　電子委任状取扱業務のイメージ
（総務省情報通信国際戦略局資料[1]）

電子委任状取扱事業者が電子委任状を保管・提供するサービスを「電子委任状の普及の促進に関する法律」に基づいて行う。

電子委任状は担当者に権限を与える為に組織の長が発行する。自治体あるいは病院長等が考えられる。電子委任状取扱事業者のサービスのイメージを図１に示す。

４．２　RFC5755準拠属性証明書を用いる方法

IETF PKIX Working Group が規定したRFC5755（An Internet Attribute Certificate Profile for Authorization）を検討対象とする。

属性証明書を利用したシステム例を図２に示す。又、属性証明書のフォーマットを図３に示す。公開鍵を持たず、公開鍵証明書とのリンクを持っている。

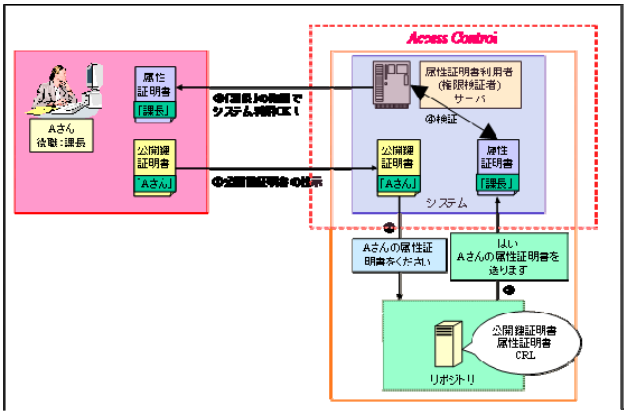

図２　属性証明書を利用したシステム例
（独立行政法人情報処理推進機構資料[2]）

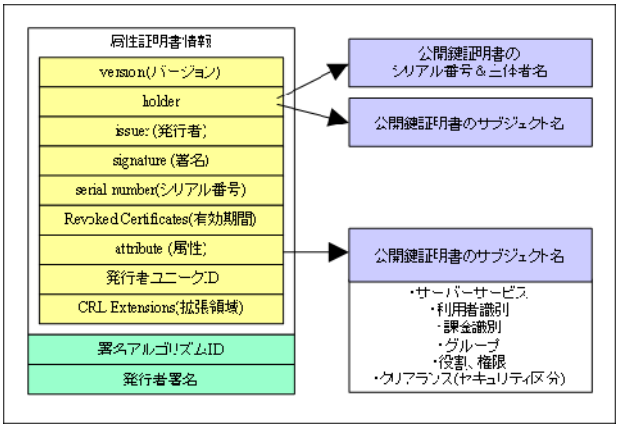

図３　属性証明書のフォーマット
（独立行政法人情報処理推進機構資料[2]）

５．本人認証と認可

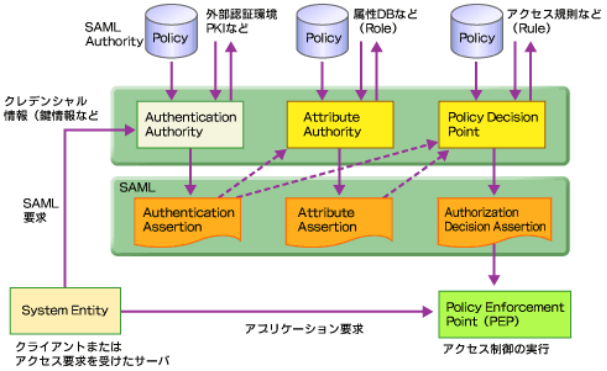

図４　SAML 概念モデル
（@IT ＞ Security & Trust 資料[4]）

本人認証と認可は図４に示すＳＡＭＬ概念モデルを参考にする。

本人認証を行い、属性を確認してアクセスポリシーと比較して、満足していればアクセスを認可する。

６．認定匿名加工医療情報作成事業者の利用

医療分野の研究開発に資するための匿名加工医療情報に関する法律（次世代医療基盤法案）で構築が期待される認定匿名加工医療情報作成事業者が個人の医療情報の提供を受けるので、その際、個人に医療情報を保存するサービスを行うことが考えられ、そのデータを個人へ提供することも考えられる。それが可能になった場合を想定してシステム提案を行う。

認定匿名加工医療情報作成事業者は当初は「代理機関」と呼ばれ、法律のパブコメ段階では「医療情報匿名加工・提供機関」と称されていたものである。

７．その他機関の利用

地方再生基金等で構築されている地域医療連携システムや今後利用が拡大される個人番号の利用チェックをおこなう個人用ポータルサイトの利用も合わせて配慮する。

７．ユーザ調査

大学病院勤務医師、内科開業医、患者団体事務局に電子生涯県区手帳に関してプロトタイプを見せヒヤリングを行った。

（倫理面への配慮）

今回の研究内容は属性認証によるアクセス制御や真正性の確保はシステム構想の提案であり、またその評価の為の電子生涯健康手帳はプロトタイプで、実際の臨床場面では使用しないので、倫理面の問題がないと判断した。

Ｃ．研究結果

１．医療従事者の電子生涯健康手帳へのアクセス制御

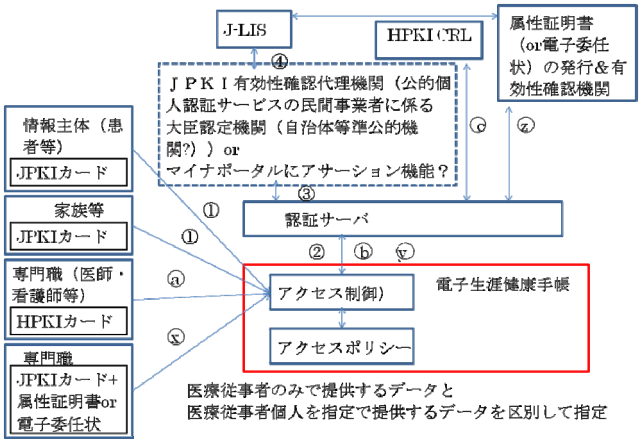

図５　属性証明書 or 電子委任状によるアクセス制御

電子生涯健康手帳は利用者、家族、ヘルスケアサービスプロバイダーごとにログインして、参照および情報の登録が可能である。今回はヘルスケアプロバイダーのアクセス機能を医療従事者の権限として利用することとした。

１．１　ＪＰＫＩと属性証明によるアクセス制御

証明書の有効性をＪ―ＬＩＳを通じて確認することが必要となる。Ｊ―ＬＩＳと有効性の確認が出来るのは官公庁等法律で定められた機関であるが、民間も許可を受ければ可能となる。

各電子生涯健康手帳サービス提供者が許可を申請することも考えられるが、地方自治体等の公的機関がサービス提供者になれば、手続きが簡素化される。

自治体等公的機関が直接サービスを実施しない場合でも、電子生涯健康手帳サービスを何らかの形で実施を民間に委託または　認定して、Ｊ―ＬＩＳとの有効性の確認のみ公的機関が行い、結果を電子生涯健康手帳サービスへ通知するシステムも考えられる。

図５にその場合のアクセス制御の機能を示す。

動作の流れの概要は以下である。

（ｘ）医療従事者（専門職）がＪＰＫＩカードを利用者端末にセットし、カードを活性化する為にＰＩＮ入力を行い、カードを活性化する。電子生涯健康手帳のアクセス制御部にアクセスする。

（ｙ）アクセス制御部は認証サーバに認証を委託する。認証サーバはＪＰＫＩ の利用者証明書の公開鍵を用い

て、チャレンジ＆レスポンス方式等により現在のアクセス者が利用者証明書の本人であることを確認する。
③　④　認証サーバはさらに利用者証明書が有効であることを確認する為に、ＪーＬＩＳへ自治体等の実施する有効性確認代理機関が問い合わせ、結果を電子生涯健康手帳サービス提供者に通知する。自治体等が電子生涯健康手帳サービスを実施している場合は有効性確認代理機関と電子生涯健康手帳サービスは一体のサービスとなる。
（Ｚ）認証サーバは利用者証明書が有効であれば、属性証明書が有効であるか発行機関に確認するか４．１で示した電子委任状取扱事業者に属性証明書と考えられる電子委任状を受信する。
②　属性がポロシーにあっていれば、電子生涯健康手帳へのアクセスを許可する。

１．２　ＨＰＫＩカードによるアクセス制御
（ａ）医療従事者（専門職）がHPKI カードをクライアントにセットし、電子生涯健康手帳のアクセス制御部にアクセスする。
（b）アクセス制御部は認証サーバに認証を委託する。認証サーバはＨＰＫＩの公開鍵証明書の公開鍵を用いて、チャレンジアンドレスポンス方式等により現在のアクセス者が公開鍵証明書の本人であることを確認する。
（ｃ）認証サーバはさらに公開鍵証明書が有効であることを確認する為にＨＰＫＩ　ＣＲＬへアクセスして、ＨＰＫＩ証明書の有効性を確認する。
認証サーバは公開鍵証明書が有効であれば、アクセス制御部へＨＰＫＩの公開鍵証明書の本人がアクセスしていることを返す。
アクセス制御部はアクセスポリシーと比較してアクセス対象へのアクセスを認可する。

２．電子署名による真正性の確保
診療・介護からデータの収集場合の概要を図６に示す。
診療・介護データの発生源は医療機関、薬局・市販薬販売店舗（薬店）、介護施設等および利用者・家族である。

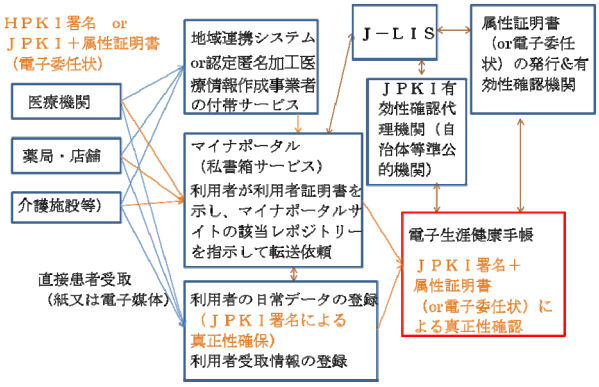

図６　属性証明書等での電子署名による真正性確保

収集経路を図６に示す。地域連携システムあるいは認定匿名加工情報作成事業者の付帯サービスからマイナポータルの私書箱機能を利用して電子生涯健康手帳へ送信するルートが準公的機関を経由するのが、管理しやすく安全性が高い。
この場合、ポータルサイトへのデータ送付の為に利用者証明書をデータの提供者に予め通知しておかなければならない。
これ以外に個人が提供を受けて情報を登録するルートもある。
情報の真正性を確保する為に電子署名を行うがその方式を以下に検討する。

２．１　ＪＰＫＩと属性証明による電子署名
ＪＰＫＩの電子署名用証明書で電子署名を行う。医療従事者であることを確認する場合には属性あるいは電子委任状を確認する。
Ｊ－ＬＩＳへ有効性確認代理機関経由Ｊ－ＬＩＳに問い合わせる。

２．２　ＨＰＫＩによる電子署名
真正性を確保する為に国家資格を有する専門職の場合はＨＰＫＩで署名を行う。この場合は医療従事者であることはＨＰＫＩ証明書のhcRoleを参照することにより確認出来る。

３．生涯電子健康手帳の機能改善
３．１　検索機能改善
これまではメタデータの項目ごとの一致で該当する

情報を検索していたが、全メタ項目を全項目検索できる機能を追加した。

これにより、情報登録時に厳密にメタ項目を選択しなくても、目的の情報が検索できるようになった。

３．２　ダウンロード機能改善

電子生涯健康手帳に登録した情報と登録時に入力したメタデータをＰＣへダウンロードできるようにした。これにより、サーバやブラウザーに表示機能が無い情報もＰＣ側にダウンロードして表示することが可能となった。

４．ユーザ調査

４．１　大学病院勤務医師

最初の画面が複雑なので最初に見える画面をすっきりさせた方が良い。

リビングウイルや臓器提供は分かりやすいところに表示して欲しい。

４．２　内科開業医

色々な機能が有るので機能を抜き出して単純化する方が良い。

過去の履歴は現在の疾患にも関係するので、自院の電子カルテでも一番見える所に表示している。

自院の電子カルテではＳＡＯＰが分かるように表示している。

４．３　患者団体事務局

目的を絞って透析患者の生涯フォローやフェニルケトン尿症に利用してみるとかはどうだろうか。

前者は色々な合併症を気にしている。後者は特殊ミルクの供給サイドとその利用者との情報共有が欠けている現状が見られるのを改善できないだろうか。

Ｄ．考察

１．ＨＰＫＩとＪＰＫＩ＋属性証明書の比較

ＨＰＫＩカードは証明書が１枚に成るので扱いやすい。ただし、国家資格だけなのでそれ以外の場合は属性証明書が考えられる。

RFC5755は認証用属性証明書であり、電子委任状は署名用のスキームなので厳密には使い分ける必要がある。

ＪＰＫＩを業務用に使用することは住所、年齢がオープンに成るので抵抗がある。

スマホＳＩＭでの発行が検討されているので、こうした証明書では住所、年齢の記述されない証明書を発行しても良いのではないだろうか。

２．ＩＳＯ　１７０９０（医療用の属性証明書規格）

医療用ＰＫＩとしてＩＳＯ１７０９０があり、ＨＰＫＩはこれに準拠している。

属性証明書に関してはＰａｒｔ２に記述されているが、ほとんどがoptionalになっていて、hcRoleはabsentになっていて、標準規格としては利用価値がない。次回見直しの時期に配慮が必要である。

３．マイナンバーのポータルサイトの利用

我々は私書箱と称して公的アカウントによる医療情報等の受発信可能なサイトの必要性を提案してきている。

マイナンバーが計画しているポータルサイトの初期はアクセスログの監視が目的であるが、個人への広報としての活用も計画されている。

更に進んだ場合は個人の医療情報の受取サイトとしての活用も原理的には可能である。

この場合、公的個人認証サービスの利用者証明のナンバーをキーにして郵便の番地のようにおくりつけてくることが可能になる。

公的な番号なのでメールよりは本人確認のレベルが高い事が期待される。

医療機関や地域連携サービスや認定匿名加工医療情報作成事業者はこの番号に送りつけるほうが、個々の電子生涯健康手帳サービス提供者の個人ごとのアカウントへ送るよりは簡易で安全性が高くなる。

４．ユーザ調査

電子生涯健康手帳の意義は理解いただけたとの印象である。医療従事者の立場での必要な情報、見やすさの追及が必要である。

Ｅ．結論

１．ＪＰＫＩ＋属性証明書による利用

国家資格はＨＰＫＩの方が扱いやすい。

国家資格以外はＪＰＫＩ＋属性証明書の利用が考えられる。

その場合ＪＰＫＩでは４情報が明確になってしまうので、業務に使用するには抵抗がある。

３枚目の証明書が検討されているので、その際、住所､生年月日､性別のない証明書を考える必要がある。また、ＪＰＫＩの有効性確認は制限されているので、社会システムとして工夫が必要である。

２　地方自治体等の公的機関が電子生涯健康手帳サービス提供者に成るメリット

利用者証明書の有効性確認には王六時地域連携システムの付加機能として実施するのが良いと考えられるが、個人の生涯健康データ保管のニーズの実現にふさわしいか検討の余地がある。

３　マイナンバーのポータルサイトの利用

活用できるかは、今後のポータルサイトの運用次第であるが、早急に活用出来るようになることを期待したい。

４．電子生涯健康手帳サービスでの機能確認

電子生涯健康手帳は患者自身の治療管理や健康管理のツールばかりでなく、医療従事者や家族との情報交換のツールであるのでそれぞれの立場での見やすさ、使いやすさを追求する必要がある。

５．次年度以降の改善項目

・ランチャー画面を作成し、ログインした時利用しやすくする。
・今回可能としたダウンロードされたメタデータと情報ファイルとをアップロードできるようにする。
・別に作成された同様の形式のセットもアップロードできるようにする。
・メタデータと情報ファイルを一括ダウンロードし他のシステムに一括アップロードする。

５　ISO17090 Part2 規格

次回見直し時、属性証明部分はhcRoleがabsentに成っていることを含め検討が必要である。

文献

１）総務省情報通信国際戦略局情報通信政策課、マイナンバーカード・公的個人認証サービス等の利活用推進について、ICT街づくり推進会議（第13回会合）（平成29年2月10日)配付資料、
http://www.soumu.go.jp/main_content/000467135.pdf

２）独立行政法人情報処理推進機構, PKI 関連技術情報 9.1 属性証明書,
http://www.ipa.go.jp/security/pki/091.html,
IPA>情報セキュリティ>PKI 関連技術情報, 2012年 7月

３）IETF PKIX Working Group ,An Internet Attribute Certificate Profile for Authorization,
http://www.ietf.org/rfc/rfc5755.txt, 2010年

４）鈴木優一, 強力なSSOを実現するXML認証・認可サービス（SAML）、
http://www.atmarkit.co.jp/ait/articles/0210/02/news002.html, @IT > Security & Trust > Webサービスのセキュリティ（4）, 2002年10月,

Ｇ．研究発表

特になし

Ｈ．知的財産権の出願・登録状況

特になし