厚生労働科学研究費補助金

地域医療基盤開発推進研究事業

医療・介護分野における公的個人認証サービスを利用した情報連携に関する研究

平成２７年度　総括・分担研究報告書

研究代表者　大山　永昭

平成２８（２０１６）年　５月

目　　次

Ⅰ．総括研究報告

医療・介護分野における公的個人認証サービスを利用した情報連携に関する研究-- 1
大山　永昭

II. 分担研究報告

公的個人認証サービス利用提供事業者、医療機関における運用方法の検討、国際的な医療情報保護の取り組みとの整合性の調査・検討---- 10
喜多　紘一

２．薬務関連に関わる公的個人認証サービス利用例の調査・検討 ---------- 17
土屋　文人

３．産業保健医療に関わる情報連携に関する調査・検討 ---------- 22
八幡　勝也

４．在宅医療における公的個人認証サービス利用例に関する調査･検討 ----- 24
齋田　幸久

５．個人電子健康手帳 Personal Health Record への応用 ---------- 25
安藤　裕

６．医療における公的個人認証サービスの活用において Counter Part となる HPKI 医師認証をめぐる問題に関する研究 ---------- 29
山本　隆一

７．公的個人認証サービス利用にかかわる技術的 ---------- 36
小尾　高史

III. 研究成果の刊行に関する一覧表 ---------- 44

Ⅳ．研究成果の刊行物･別刷 ---------- 45

厚生労働科学研究費補助金（地域医療基盤開発推進研究事業）

総括研究報告書

医療・介護分野における公的個人認証サービスを利用した情報連携に関する研究

研究代表者　　大山　永昭　　東京工業大学像情報工学研究所　教授

研究要旨：　平成 25 年 5 月に改正された公的個人認証法により、番号制度導入時に発行される個人番号カードには、既存の電子署名機能に加えて電子利用者証明（電子認証サービス）機能が利用可能な新たな公的個人認証サービス（JPKI）が搭載される。また、新たな JPKI は、民間事業者であっても政令で定める基準に適合すればその利用が認められることとなる。今後ネットワーク技術の活用が想定される医療介護サービスの実現には、サービス提供時の医師・薬剤師等の法定資格の確認や医療データの提供・利用に関わる責任所在を明確化できる仕組みの構築が必要であり、本研究では、JPKI と医療従事者の資格確認を可能とする認証基盤（HPKI）を連携させることで、その仕組みを利用した新たな医療・介護分野における情報サービスの実現方法について検討する。今年度は医療や介護分野における JPKI や HPKI の利用が求められる情報サービスについて、前年度提示した具体的なサービス例のより詳細な検討を行い、JPKI と HPKI を連携させた医療情報システムの有効性及び実現可能性を示した。また、これら検討を元に、実用化に向けての課題を整理した。

研究分担者　喜多　紘一　保健医療福祉情報安全管理適合性評価協会　理事長
土屋　文人　国際医療福祉大学薬学部 特任教授
八幡　勝也　産業医科大学産業生態科学研究所 非常勤講師
齋田　幸久　東京医科歯科大学大学院医歯学総合研究科　特任教授
安藤　裕　放射線医学総合研究所重粒子医科学センター病院　病院長
山本　隆一　東京大学大学院医学系研究科　特任准教授
小尾　高史　東京工業大学像情報工学研究所　准教授

A．研究目的

平成 25 年 5 月、番号関連法案の成立によって「社会保障・税番号制度」が導入されることとなり，平成 27 年 10 月から国民に対する個人番号の通知が開始されるとともに，平成 28 年 1 月から個人番号カードの交付が開始される．同制度の導入に関連し，e-Tax 等のオンライン申請の安全性確保のために利用されている「公的個人認証サービス（JPKI）」について，従来の「電子署名」の機能に加えて，国民が自己の個人番号に係る個人情報を自宅のパソコン等から確認できる仕組み（マイ・ポータル）への安全なログイン手段として「電子利用者証明」の機能が追加される．また，従来は「電子署名」の検証は行政機関等に限定されていたが，今後は「電子署名」及び「電子利用者証明」の検証は，総務大臣が認定する民間事業者も可能となる．そして，JPKI の機能は現在，住民基本台帳カードに（国民の選択に基づき）搭載されているが，上述の新しい JPKI の機能は平成 28 年 1 月より配布が開始された個人番号カードに標準

搭載されている．この個人番号カードに搭載されている JPKI は、医療分野においても多くの場面で有用であると考えられ、特にネットワークを介して行われる医療情報の連携や在宅診療時の患者情報の提供・参照などにおいては、JPKI による厳格な本人確認が、これらサービスの実現に大きく寄与すると期待されている。また、上記のような医療・介護における情報サービスを利用する際には、多くの場面で医師等の法定資格の確認や医療データの提供・利用に関する責任所在を明確化できる仕組みが求められている。この要求に対しては、医療従事者の資格を確認するための認証基盤（HPKI）の利用が有効である。HPKI では、医師、薬剤師、看護師など保険医療福祉分野の 24 種類の国家資格と病院長、管理薬剤師など医療機関等の 5 種類の管理者資格を電子的に認証することが可能であり、その認証の正当性は、厚生労働省が運用する認証局が保証している。よって、JPKI による本人確認を利用した医療・介護に関する情報サービスを実現するためには、JPKI のみを利用したシステムだけではなく、JPKI と HPKI とを組み合わせたシステムの構築についても検討が必要である。そこで本研究では、JPKI を利用した電子認証機能の利用及び HPKI との連携により、患者および医師等の認証を組み合わせ、保健医療介護サービスの実現に不可欠な認証基盤を構築する方法について、その運用方法も含めた技術的方策を明らかにする。

B．研究方法

本研究では、保健医療介護分野における JPKI の利用方法、JPKI と HPKI の連携方法を技術的に検討するとともに、これらを利用した医療や介護分野における新しいサービスを検討する。そして、これを実現するために必要となる技術的要件を明らかにする。また、最終年度には検討結果を厚生労働省ネットワーク基盤検討会における“医療情報システムの安全管理に関するガイドライン”に反映させることを目標とする。

平成 26 年度は、医療分野における JPKI 及び HPKI の利用が求められるサービスの例として、保険資格のオンライン確認及び在宅医療でのデータ参照における本人確認の仕組みについて検討を行い、具体的な実現例を示した。平成 27 年度は、前年度に検討したサービスについて、詳細なサービスモデルの検討を行い、具体的なシステムの実現案を示すとともに、電子処方箋の運用などの他のサービスについても検討を加え、JPKI や HPKI の連携方法の検討及び、これら電子認証を利用した医療情報システムの有効性及び実現可能性を示す。

C．研究結果

(1) 医療分野における JPKI を利用したシステムの具体例の検討

(ア) 健康保険のオンライン資格確認

現行の医療保険制度では、レセプトの返戻が大きな問題となっており、平成 21 年度のレセプト返戻件数は、約 420 万件（金額ベースでは 4800 億円）、このうち、被保険者証の転記ミスが約 4 割、被保険資格確認の不足が約 5 割あるとされる。これらは、オンラインでの医療保険資格確認やレセプト等への被保険者番号自動転記が実現されれば解消できる問題であると考えられる。このオンライン保険資格確認の実現のためには、個人番号カードに搭載される JPKI の電子利用者証明機能が有用であると考えられ、政府の方針としても、個人番号カードを保険証として利用し、オンラインでの保険資格確認を行う仕組みを導入する方向で検討が進められている。このような背景から、本研究では、JPKI

の電子利用者証明によってオンラインの保険資格確認を行う方法について、具体的なシステムの実現モデルについて検討を行っている。昨年度はPINを入力しない形式での保険資格確認を行う仕組みの提案等を行ったが、今年度は、この仕組みをより詳細に検討し、より高速かつバッチでも保険資格確認を行えるシステムの検討を行った。

昨年度の本研究において、PINの入力を求めない個人番号カードの電子利用者証明（以下機関認証JPKI）を利用してオンライン保険資格確認を行う手法を提示しているが、この手法はサービスを提供している保険資格確認プラットフォーム（PF）の正当性を確認す

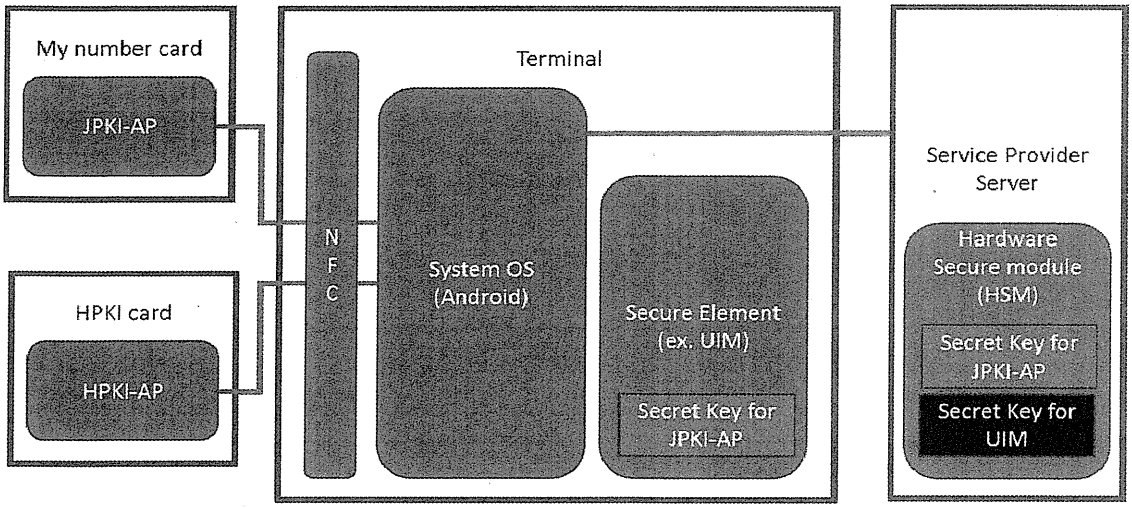

図1　端末のシステム構成案

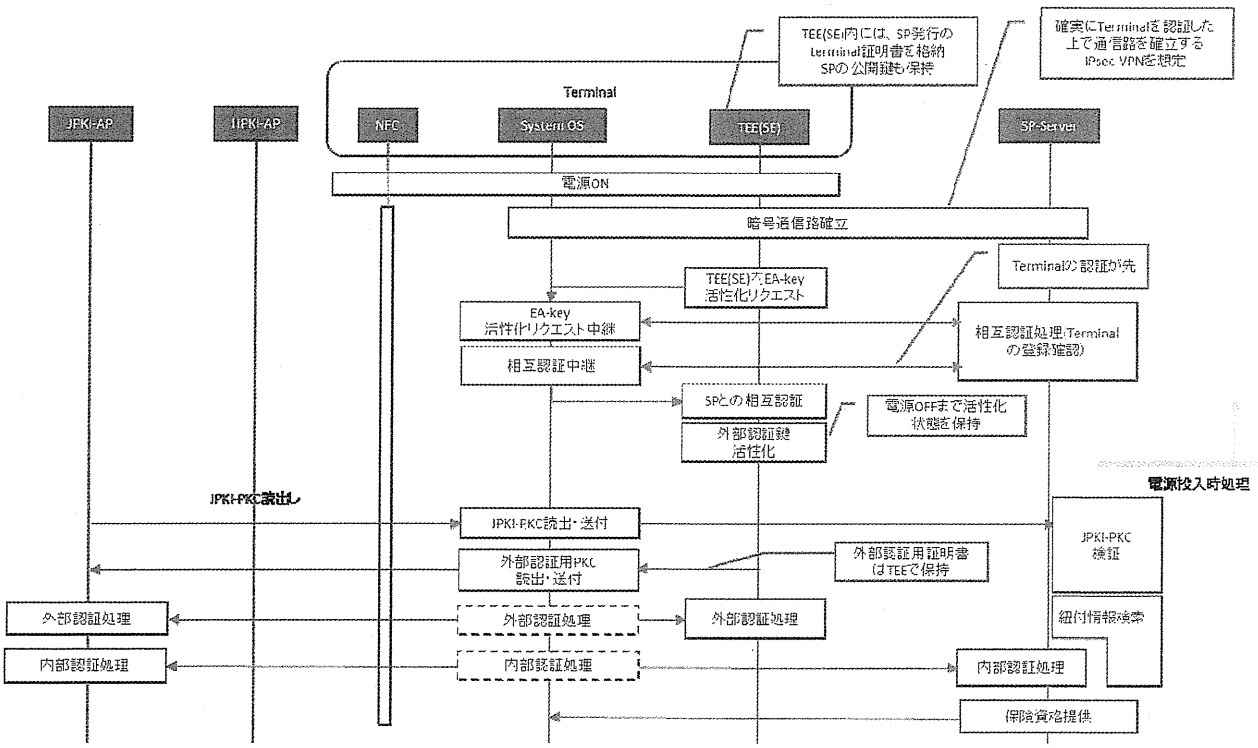

図2　機関認証鍵を端末で保持する場合の想定処理フロー

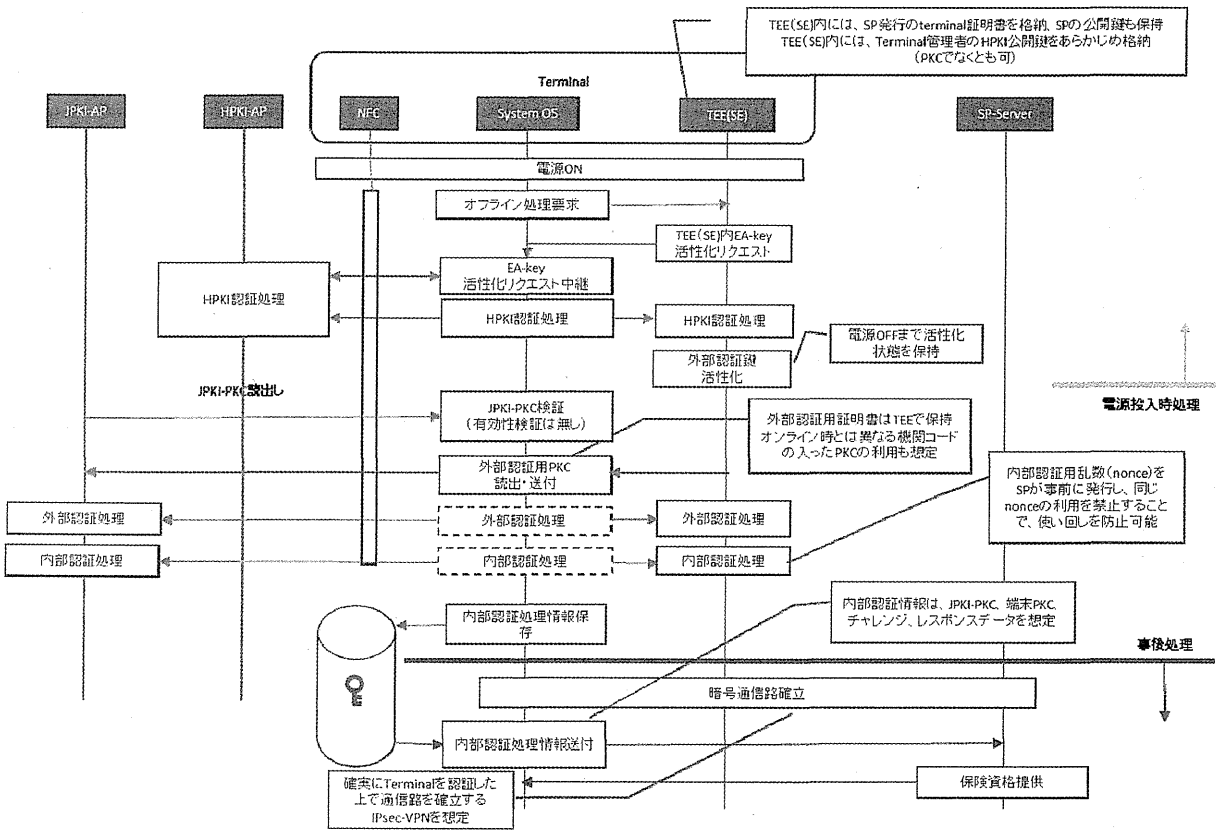

図３　機関認証鍵を端末で保持する場合のオフライン処理時想定フロー

るための外部認証をネットワーク経由で行う必要がある。そのため、通常の PIN 入力での保険資格確認に比べて処理に時間がかかること、またネットワーク障害等が発生した場合には対応できない等が課題であった。そこで今回は、外部認証用秘密鍵と証明書を医療機関内のレセコンや電子カルテシステムあるいは保険資格確認用端末に格納しておき、保険資格確認時には、保険資格確認 PF とのネットワーク経由での外部認証を行わなくとも、医療機関内の処理のみで機器認証 JPKI の外部認証を実現するシステムを提案する。この手法によって、保険資格確認に有効な PIN 無し認証に要する処理時間を短縮することが可能になる。また後述のネットワーク障害時の対応を行うことにより、ネットワーク障害時でも受付業務を停滞させないシステムを実現できると予測される。

図１に提案するシステム構成案を示す。このシステムでは、保険資格確認 PF の外部認証のための秘密鍵を、医療機関内端末内の User Identity Module （UIM） や Trusted Execution Environment（TEE）など耐タンパな Secure Element に格納しておき、この秘密鍵を利用して外部認証を行う。ただし、この機能を利用する端末の電源投入時には、保険資格確認 PF との相互認証をオンラインで行い、医療機関内の端末の正当性を確認できた場合のみ、この医療機関内端末に格納された秘密鍵での外部認証機能を有効とする機構を組み込む。この具体的な処理シーケンスを、図２に示す。

また、医療機関と保険資格確認機関間のネットワーク障害等が発生した場合には、オン

ラインでの保険資格確認や、前述の機関認証用秘密鍵を利用可能な状態にするための電源投入時の相互認証処理を行うことができない。よって、ネットワーク障害が発生した場合には、電源投入時の保険資格確認 PF との相互認証を行う代わりに、医師等の HPKI カードを利用した HPKI 認証を行うことで電源投入時における秘密鍵の活性化を行う（図３）。さらに、保険資格確認のための IC カード認証（個人番号カードの内部認証）の代わりに、医療機関端末が発生させた乱数（NONCE）を利用した内部認証を行うこととする。この仕組みにより、ネットワーク障害が発生している間の個人番号カードの使い回しは防止可能である。そしてネットワーク障害が復旧した後、NONCE を用いた医療機関内での内部認証結果を保険資格確認 PF に送付し、これら患者についての保険資格情報を入手する。この仕組みによって、ネットワーク障害が発生した場合でも、停滞なく受付業務が実施可能である。

(イ) 在宅医療・介護におけるデータ参照

昨年度は、在宅医療・介護における情報システムとして、共有化された患者情報を患者の自宅からオンラインで登録及び参照するシーンを想定し、HPKI による医師の資格確認と患者本人の JPKI による本人確認を組み合わせた認証行うことでアクセス制御を行う仕組みを提案した。JPKI 及び HPKI を利用した認証では、それぞれの IC カードを所持している人物を特定する意味での認証としては高い信頼性を有するが、その人がどのような環境でアクセスしているかを確認することはできない。今回想定する家庭内から外部サーバへのデータアクセスでは、情報を取り扱う端末にマルウェア等の不正プログラ

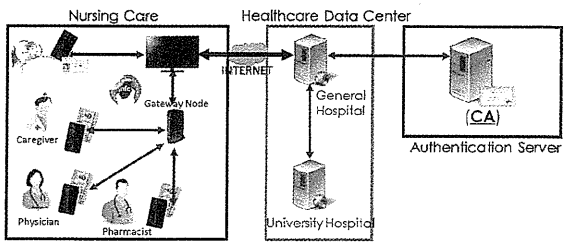

図４　提案システムの構成図

ムが動作しないための対策や、外部からの不正アクセス対策は重要である。このような場合、時間や場所などの環境を限定することで、JPKI の電子利用者証明を利用したサービスの信頼性を向上させることが可能になると考えられる。そこで今年度は、昨年度提案した JPKI 及び HPKI を利用した本人認証、資格認証に加えて、場所や時間等の複数要素を認証に加えることで、より安全に情報管理を行うシステムについて検討する。

想定する環境としては、自宅で医療・介護を受けている患者の情報が病院内の情報システムや医療情報連携サーバ等に管理されており、この情報を患者自身もしくは医療従事者が患者の自宅から参照する場面を想定する。データ管理用の情報端末としては、患者はケーブルテレビの利用を想定し、医療従事者はタブレットなどの携帯端末の利用を想定する。これらの情報端末において IC カードを読む手段として、テレビでは、IC カードリーダーが備わっているセットトップボックス（STB）を利用し、タブレットでは NFC でのコネクションを利用する。

このシステムにおいて、医療従事者がデータ参照を行う場合に、患者の自宅以外ではデータ参照させないような場所の限定や、勤務時間のみ参照可能とする時間の限定を行うことで、より安全なアクセス制御が実現できると考えられる。そこで、昨年度提案したシステムにコンテキスト情報（デバイスが使わ

れる時間や場所等）を管理する仕組みを追加する。その実現手法として、コンテキスト情報を管理するためのホームゲートウェイを患者の家庭に設置する。ゲートウェイでは、患者のデータサーバへアクセスしようとしている端末の時間、場所、デバイス情報を取得し、これら情報を認証サーバへ送付し、アクセスポリシー（データ参照が可能な条件）に適合するかどうかをチェックする。適合した場合には、昨年度提案したHPKI認証、JPKI認証へと手順を進める。コンテキスト情報の取得方法は様々考えられるが、一例として、時間情報はタイムスタンプ、場所情報及びデバイス情報は医師のタブレット端末のGPS及びMACアドレスをそれぞれ利用することが考えられる。この仕組みにより、医療従事者であっても、正しい環境でのみ情報参照が可能になり、より安全性の高い情報管理が行えると考えられる。

一方、在宅医療・介護現場でのデータ参照において、初めて対応する患者のデータを参照する際には、データベースへのリンク情報を入手する方法も簡便であることが望ましい。このような場合、従来は検索システムを利用して患者を検索する方法や、QRコード等を利用してリンク情報を取得する方法が一般的であるが、提案システムでは、NFCを利用可能なデバイスを利用することを想定しているため、NFCタグの利用が有効であると考えられる。NFCタグは、QRコードよりもより高速かつ簡便な操作が可能であり、またより多くの情報を扱うことができる。現状、NFCタグの利用は一般的とは言えないが、将来の高度な情報管理のためには、各家庭にNFCタグを容易に設置できる環境整備が期待される。

以上の検討を踏まえた提案システムのシステム構成図および処理の流れを図4および図5に示す。

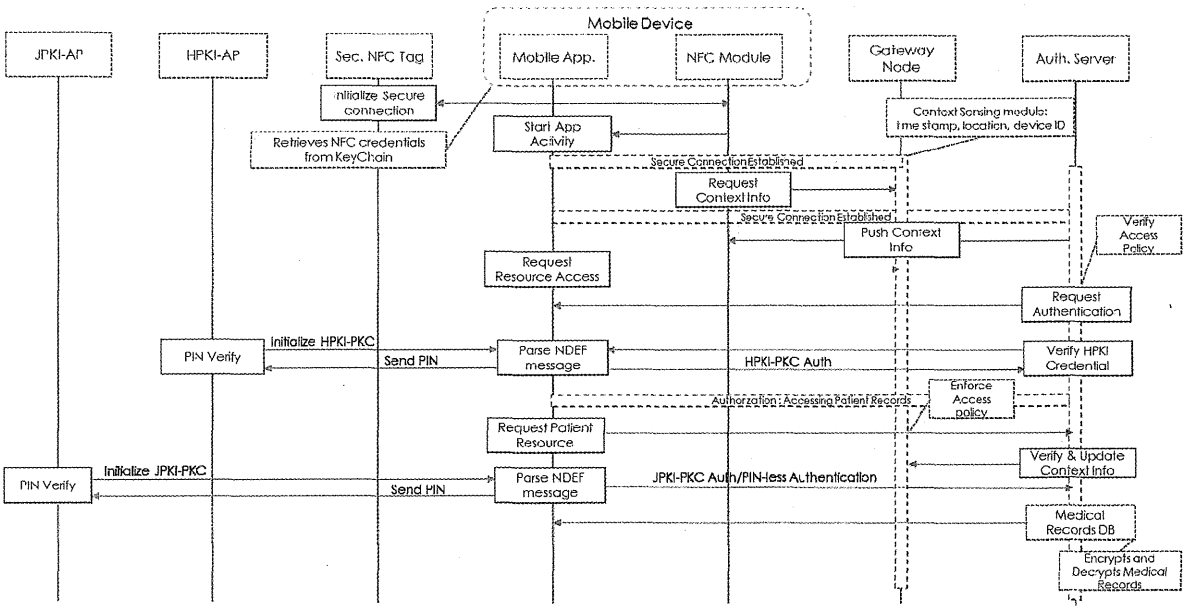

図5　提案システムにおける認証処理フロー

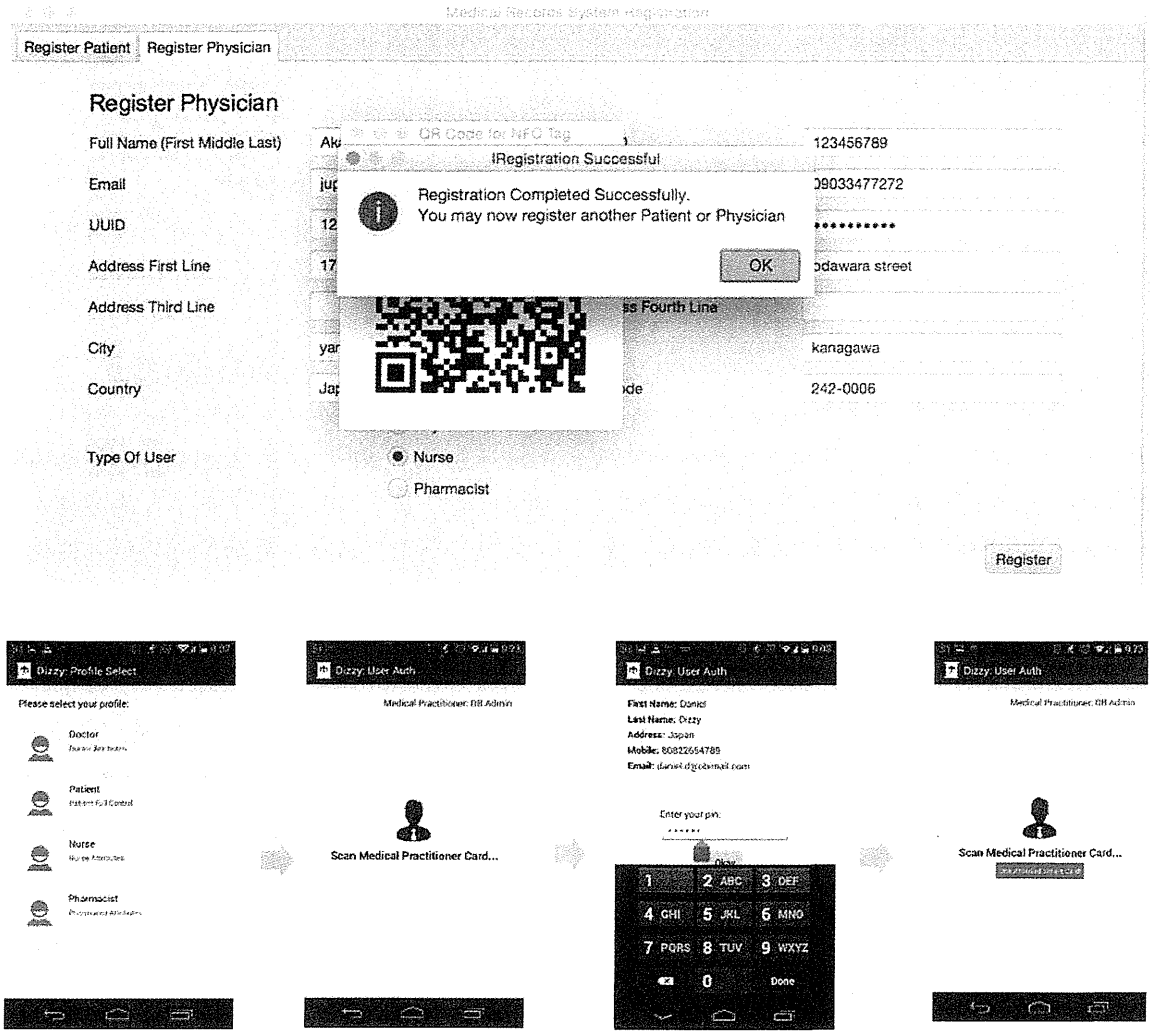

図６　開発したプロトタイプシステムの画面例
（上：ユーザー登録画面、下：タブレットでの認証の様子）

また、このシステムのプロトタイプシステムを構築し、動作確認実験を行った。タブレットはNFCを利用可能なAndroid端末を用いた。このシステムの動作画面の一例を図８に示す。このシステムによって、コンテキスト情報を確認し、HPKI 認証、JPKI 認証を経た上で、患者の情報を参照できることを確認した。なお、このプロトタイプシステムでは、NFC タグからのリンク情報取得は実装していない。

(ウ) 電子処方せん

これまで厚生労働省で検討されてきた電子処方せんについては、2016 年 4 月からはその実施が認められることとなった。厚生労働省のガイドラインでは、電子処方せんシステムでは、本人確認のための認証インフラのために JPKI を利用すべきとの明記はないが、国民全員が利用可能なサービスにするためには、JPKI の利用は実現手段の有力候補である。また、電子処方せんを導入する際に、オンライン保険資格確認や電子お薬手帳との

連携を行うことは重要であり、個人番号カードや JPKI を利用すれば、これらサービスを一枚のカードで実現できることから、個人番号カード及び JPKI を電子処方せんの本人確認手段として活用することは理想的であると言える。

図７に個人番号カード（JPKI）の利用を前提とする電子処方せんシステムの概略図を示す。このシステムでは、医師が発行した電子処方せん ASP サーバに登録し、薬局でその電子処方せんを取得することで、紙と同様の処方せん運用を行うことができる。また、電子お薬手帳運用サーバでは、処方情報や調剤情報が記録され、患者が日ごろの健康管理のために参照できるだけでなく、処方せん発行時や調剤時に飲み合わせ、重複処方のチェックを行うことができる。このシステムにおいて、患者本人を確認する際には、どのシーンにおいても JPKI によって本人確認することが可能であり、また電子処方せんや電子お薬手帳に記録する情報には、医師や薬剤師の HPKI を利用した電子署名を付与することで、その情報の生成者を確認することが可能になる。このシステムを実現するためには、医療等 ID の整備や、病院及び薬局と各サーバを安全に接続するネットワークの確立が課題として挙げられる。

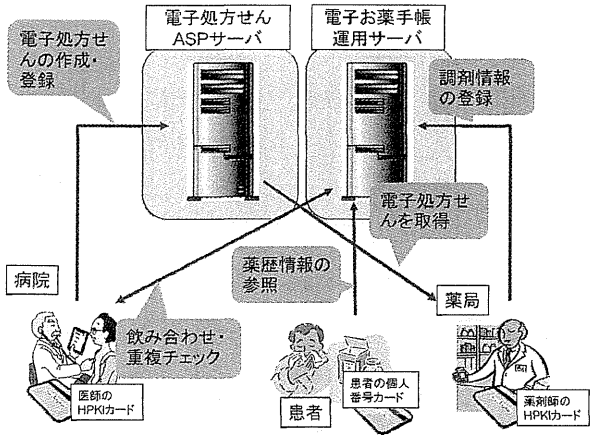

図７　JPK を利用した電子処方せんシステムの概念図

(2) 実用化へ向けての課題

本研究で挙げた JPKI と HPKI を連携させた医療情報システムの実用化へ向けての課題を以下に挙げる。

①　JPKI を利用するための環境整備

提案技術を実用化するためには、いつでもどこでも日常的に JPKI を利用可能な環境整備が重要である。2016 年 1 月より個人番号カードの交付が始まり、希望者は無料で取得できることから、これまでの住基カードに比べて大きく普及が進むものと期待されている。さらに、現在政府によってスマートフォンで JPKI を利用可能な仕組み作りが検討されており、これによってより利便性の高い JPKI 利用が可能になる。以上のように、JPKI を利用するための環境整備は積極的に行われている。

②　HPKI の普及

現在の HPKI は、医師会および MEDIS-DC より提供されているが、その普及は十分とは言えない。そこで普及が進みつつある個人番号カードを HPKI のための認証デバイスとして利用することができれば、HPKI の普及は加速するものと考えられる。そのためには、個人番号カードと HPKI の属性証明書を連携させることで、HPKI カードと同等の機能を提供できると考えられ、今後はこの仕組みについての検討が重要である。

③　医療等 ID の整備

JPKI を利用した医療サービスでは、電子処方せんのように複数の医療機関が関わるサービスが多くなると考えられ、別々の医療機関で管理しているユーザー情報を連携させることは必須であると考えられる。とくに

各人の保健・医療情報を生涯にわたって管理することは重要であり、そのための医療等 ID の整備は極めて重要な課題であると考えられる。その解決策としては、保険資格確認の仕組みを元に医療等 ID を発行する手法等が考えられる。

D．結論

本研究では、JPKIと医療従事者の資格確認を可能とする認証基盤（HPKI）とを連携させた新たな医療・介護分野における情報サービスの実現方法について検討し、前年度に検討したサービスについて、より詳細なサービスモデルの検討を行い、具体的なシステムの実現案を示すとともに、電子処方せんの運用などの他のサービスに関する検討を加え、JPKIとHPKIを連携させた医療情報システムの有効性及び実現可能性を示した。また、これらの検討を元に、実用化に向けての課題を整理した。

E．健康危険情報

該当なし

F．研究発表

- T. Obi, "New Japan e-ID Card toward Infrastructure of e-Health and e-Business," World e-ID and Cybersecurity 2015, Sep. 2015.
- D. A. Dzissah, H. Suzuki, Lee Joong-Sun, T. Obi, N. Ohyama, "An Access Control System for Home Based Healthcare Information Sharing using Smart Gateway," The 2016 IEICE General Conference, A-15-10, p. 220, Mar. 2016.

厚生労働科学研究費補助金（地域医療基盤開発推進研究事業）
分担研究報告書
公的個人認証サービス利用提供事業者、医療機関における運用方法の検討、
国際的な医療情報保護の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「医療・介護分野における公的個人認証サービスを利用した情報連携に関する研究」の中の分担研究として「公的個人認証利サービス利用提供事業者、医療機関における運用方法の検討」を行うものである。その為に電子生涯健康手帳システムを例に検討した。
「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）をどのように利用していくか、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。
先ず、電子生涯健康手帳サービス提供者地方自治体等の公的機関が成るメリットを提案した。利用者証明書の有効性確認やシステム導入のしやすさとして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、その場合、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モチベーションになっている組織化か検討の余地がある。
また、マイナンバーカードには利用者証明機能をＰＩＮ無しで利用できる機能があり、救急の場面でアクセスカードとして利用価値があるが、アクセス者の区別として使用される機関コードの体系化とその公開方法およびこれに対応して健康情報の分類が必要になる。さらに、マイナンバーのポータルサイトを医療情報の公的受信ボックスとして活用できるかは、今後のポータルサイトの運用次第であるが、早急な活用を期待したい。
個人収集データの真正性を確保し、有効活用性を高めるにはスマートフォンで公的認証サービスを用いて電子署名を行うアプリケーションが、まだ一般的に普及していないので、今後の課題である。

A．研究目的

本研究では「医療・介護分野における公的個人認証サービスを利用した情報連携に関する研究」の中の分担研究として「公的個人認証利サービス利用提供事業者、医療機関における運用方法の検討、国際的な医療情報保護の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）をどのように利用していくか、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、自治体が「電子生涯健康手帳」サービスを運用した場合のメリット、デメリットの検討、利用者が意識不明等でマイナンバーカードを携帯しているがカードを活性化するためのピン入力ができない場合のJPKIの特長を活かした対応方法および利用者が日常データをウエアラブルセンサーにより、スマートフォン等を経由して「電子生涯健康手帳」へデータを登録する場合の課題と解決方法を検討する。

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）利用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）自治体は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）経由で行えること。

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。

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．ＪＰＫＩカード活性化方式の検討

ＪＰＫＩのカード利用の基本動作は小尾高史准教授の東京工業での講演会資料集[1]を参考に検討する。

すなわち、ＰＩＮを用いてカードの活性化を行う場合は図１の機能図を検討対象とする。

また、ＰＩＮを用いずに機関認証によりカードの活性化を行う場合は図２の機能図を対象とする。

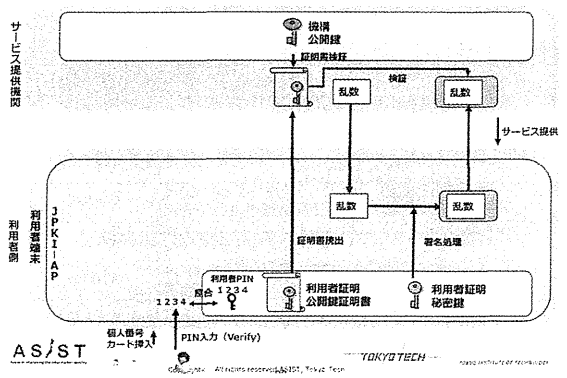

図１　ＰＩＮ入力による利用者証明機能の活用

ＰＩＮを用いる場合はカードの使用の最初に端末側からＰＩＮ入力し利用者が正当なカードの保有者であることの認証（外部認証）を行ったあと、カードが誰の

使用であるかサービスを提供するシステムが確認する為にカード内の秘密鍵とその保持者が誰であるか、チャレンジ＆レスポンス方式により確認する。

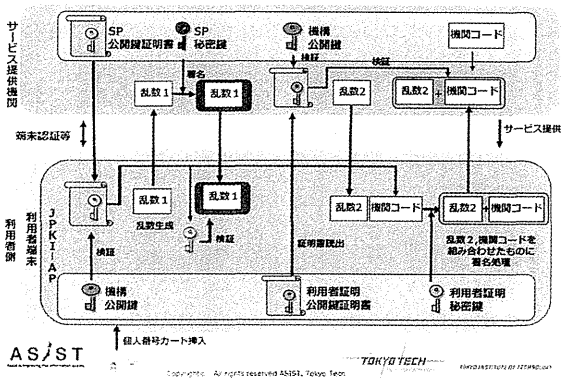

図２　機関認証による利用者証明機能の利用

ＰＩＮ無しで行うためには、端末のアクセス者がＪ－ＬＩＳの発行した公開鍵を保有した機関であるかカードが認証する為に、カード側から端末に対してチャレンジ＆レスポンスを行い確認する。(カードによる外部認証機能)

次にカードが誰の使用であるかサービスを提供するシステムが確認する為にカード内の秘密鍵とその保持者が誰であるか、チャレンジ＆レスポンス方式により確認する。

この時、アクセスしている機関コードも同時に確認する。

３．ウエアラブルセンサーの活用検討

ウエアラブルセンサーの例として、Ｆｉｔｂｉｔ製ＣｈａｒｇｅHRを用い、中継ゲートウエイとしてＡｎｄｏｒｏｉｄ系のスマートフォンを用いて、電子生涯健康手帳サーバへアップロードした。

ＣｈａｒｇｅHRはリアルタイム心拍数、安静時心拍数、歩数、睡眠時間等を測定する。アップロードしたデータは他の情報と比較して閲覧、提示出来る。

スマートフォンはｄｏｃｏｍｏ　Ｆ－０２Ｇ　Ａｒｒｏｗｓ　ＮＸを用いた。

４．国際的な医療情報保護の取り組みとの整合性の調査・検討

国際的な取り組みとの整合性調査としてＩＳＯ／ＴＣ２１５のPublic Key infrastructure規格化状況を調査する。

Ｃ．研究結果

１．電子生涯健康手帳へのアクセスカードとしてのＪＰＫＩ（利用者等がＰＩＮ入力でカードを活性化出来る場合）

電子生涯健康手帳はＪＰＫＩの利用者認証機能を利用して、アクセス制御することが出来る。この場合利用者証明書の有効性を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３にその場合のアクセス制御の機能を示す。ＪＰＫＩカードのアクセス動作は図１と同様である。

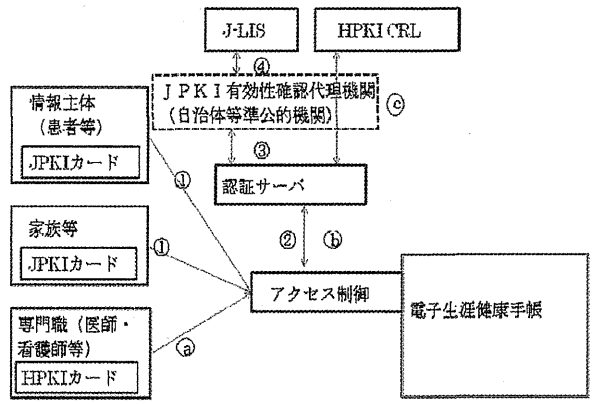

図３　アクセス制御

動作の流れの概要は以下である。

1）利用者および家族のアクセス

① 利用者または家族（以下利用者）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。

② 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公開鍵証明書が有効であることを確認する為に、Ｊ－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。

② 認証サーバは公開鍵証明書が有効であれば、アクセス制御部へ公開鍵証明書の本人がアクセスしていることを返す。

2）専門職（医師・看護師等）のアクセス

a）専門職が利用者または家族（以下利用者）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コントロールリストと比較してアクセス対象へのアクセスを認可する

2．電子生涯健康手帳へのアクセスカードとしてのＪＰＫＩ（利用者等がＰＩＮ入力でカードを活性化出来ない場合）

ＪＰＫＩサービスは図２に示すようにＪ―ＬＩＳが発行した公開鍵を持つ機関が利用者のカードを活性化することが出来る。この機能により、救急関連機関に公開鍵を発行しておけば、端末の操作者が救急関連機関に認証されている操作者であれば、公開鍵を持つ救急関連機関によりカードを活性化してもらい、電子生涯健康手帳の認証サーバにアクセスすることが出来る。この場合、救急関連機関であることを示す機関コードを認証サーバに通知するので、電子生涯健康手帳サービスはこれに応じた情報を提供することが出来る。

3．診療・介護データの収集

診療･介護からデータの収集場合の概要を図４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。

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で署名を行い､個人の場合はＪＰＫＩの署名機能を使用する。

データはマイナンバーでサービスされる利用者ポータルサイトを経由して電子生涯健康手帳サーバへ送付する場合と利用者へ提供して利用者がアップロードする場合が考えられる。

前者の場合、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。

後者の場合は電子生涯健康手帳サーバのアクセスにＪＰＫＩの利用者証明書を用いる。

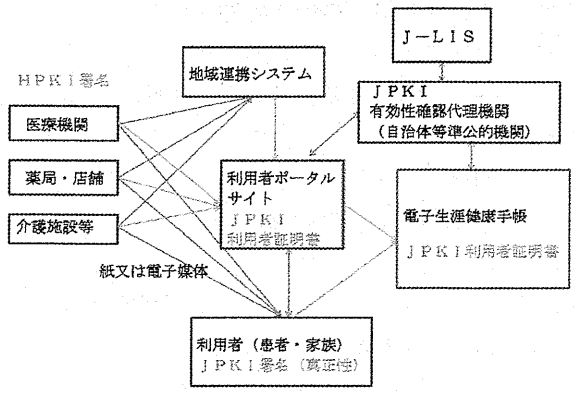

図４ 診療・介護データの収集

いずれの場合も証明書の有効性確認の為、Ｊ－ＬＩＳへ有効性確認代理機関経由Ｊ－ＬＩＳに問い合わせる。

４．健康管理機器データの収集

ウエアラブルな健康管理機器からのデータ収集は図５のように考えられる。ウエアラブルセンサーからＰＣやスマートフォン経由で電子生涯健康手帳サーバへ送る場合と、スマートフォンから、ウエアラブルサービスのホームサーバ経由マイナンバー制度で構築される利用者ポータルサイトの場合がある。

この場合、データの真正性を確保が必要な場合は、スマートフォンでＪＰＫＩにより電子署名を行うことが、解決策の一つとなる。

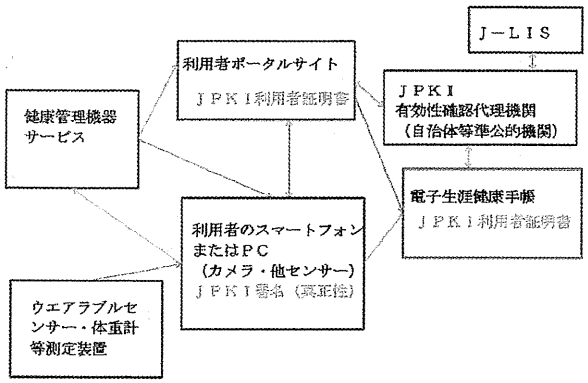

図５　健康管理機器からのデータ収集

本年度はウエアラブルセンサーとしてＦｉｔｂｉｔ製のＣｈａｒｇｅＨＲ用いて動作確認を行った。

ＣｈａｒｇｅＨＲはスマートフォンでＢｌｕｅＴｏｏｔｈインターフェイスを経由してデータを取り込み、日々のデータ、１週間、１か月間、３ケ月間、１年間のスケールでグラフ化することが出来る。本年度はこの生データを直接電子生涯健康手帳サーバへ送るソフトウエアは作成できなかったので、スクリーン画像として取り込み、スマートフォン上で電子生涯健康手帳サービスを起動し、閲覧・提示の為のメタデータを付与してアップロードした。

スマートフォンの表示画面はＳｃｒｅｅｎ　ｓｈｏｔｓ機能により電源スイッチと音量キーの下を同時に１秒以上押すことにより保存される。取り込み確認は「ギャラリー」フォルダーの中にある「Ｓｃｒｅｅｎｓｈｏｔｓ」をアクセスすることにより可能である。

５．電子生涯健康手帳サービスでの機能確認

ウエアラブルセンサーのデータを収集し、１か月分の安静時心拍数サマリーを電子生涯健康手帳サーバに取り込んだデータとＵＳＢで結合可能な OMRON 手首式自動血圧計 HEM-637IT からＰＣへ取り込んだ１か月分のサマリー画像データを同一画面に並行してならべ、表示し、その相互関係の有無を比較・評価できることを確認した。

また、電子生涯健康手帳サーバソフトウエアを構成する「健康情報の保管・提示マネージメントプログラム」の改良として、本年度は主に複数利用者の実使用を考慮し、パスワードを失念した時に再発行できる機能等、電子生涯健康手帳サービス管理者の為の機能等を追加作成・評価し、計画通りに機能することを確認した。

６．医療機関等から提供された資料のＰＤＦ化

医療機関等から紙情報として提供される資料を電子生涯健康手帳サービスに保存して提示することが可能である。この場合ＰＤＦ化して保存する。

ＰＤＦ化機能としてはコピー機と同様にシートをスキャンして行うのが一般的であるが、カメラ機能を用いて機械的にスキャンせずに全体を撮影して、歪み補正を行う装置もでてきている。

本年度は、スタンドスキャナーとして、A.M.T. piQx スキャネックスを評価した。

スタンドとして自由度が高いので、初期設定が難しく、少ない枚数を偶にデジタル化するには使いこなし、再現性の良い最適値を求めておく必要がある

７．国際的な取り組みとの整合性調査

ＩＳＯ／ＴＣ２１５の Public Key infrastructure 規格化の状況は以下のように５つのパートからなっている。

Health informatics — Public key infrastructure
Part 1: Overview of digital certificate services
Part 2: Certificate profile

Part3: Policy management of certification authority
Part 4: Digital Signatures for healthcare documents
Part 5: Authentication using Healthcare PKI credentials
Part 5の３月末の状況はＤＩＳ投票の準備中である。他は発行済みである。

Ｄ．考察

１．　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

電子生涯健康手帳サービスへのアクセス制御としてパスワード方式とアクセスカードを用いる方式があるが、カード方式の方が、安全性が高い。この場合、個々の電子生涯健康手帳サービス提供者がカードを発行する場合と他の一般的なカードを流用する場合が考えられるが、一般的に流通するカードがあればこれを利用する方が電子生涯健康手帳サービス提供者のカードに対する発行コストが低くなる。一般的に流通するカードとしてマイナンバーカードが有り、その中の公的個人認証サービス（ＪＰＫＩ）の電子利用者証明を用いることが考えられる。

この場合、証明書の有効性を確認する必要があり、法律で定められた主に公的機関がＪ－ＬＩＳにアクセスして確認することが可能である。

法律では、総務大臣が認定した民間事業者も有効性確認の実施が可能で、２０１６年２月現在民間３団体が認定済みである。[1)]

電子生涯健康手帳サービス提供者が個々に認定を受けることが考えられるが、法律上確認可能な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なれば既存の手順で有効性確認を行うことが出来る。

電子生涯健康手帳サービス提供者にならない場合でも、電子生涯健康手帳サービス提供者を地方自治体ごとに評価して有効性確認情報を提供することも考えられる。

地方自治体単位の医療ネットワークサービスとしては地域連携システムが構築されつつあり、診療報酬制度もそれを推進すべく改定されつつあるので、地域連携システムの付加機能としての検討も有効と考えている。

しかし、この場合は、自治体や医療機関等の管理しやすい運用形態や情報が中心になるので、生涯にわたり健康情報の保管に対するモチベーションが下がり、必ずしも個人健康管理に適しない運用になる可能性がある。

２．利用者証明機能のＰＩＮ無しによる利用

ＰＩＮなしでカードを利用する場合はＪ－ＬＩＳの認証局が発行した機関保証する公開鍵との外部認証を実施する必要がある。この場合、機関コードがアクセス者を区別することに成るので、電子生涯健康手帳サービス提供者はこれに応じて健康情報を提供することに成るので、機関コードの体系化と公開方法およびこれに対応して健康情報の分類が必要になる。

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安全性が高い事が期待される。

医療機関や地域連携サービス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。

今後のポータルサイトの運用次第であるが、早急な活用を期待したい。

４．提供情報の真正性確保

診療時真正性が必要な電子化された医療情報はＨＰＫＩで署名することが求められている。

ウエアラブル等個人が収集した情報もものによっては真正性が保証された方が受け取る方の評価としても高くなる。その場合、ウエアラブルセンサーが中継器と

してスマートフォンを用いることが多い。
個人が電子署名をする場合、公的個人認証サービスの署名機能を用いることが考えられるが、スマートフォンで公的認証サービスを用いて電子署名を行うアプリケーションは一般的に普及していないので、今後の課題である。

５．電子生涯健康手帳サービスでの機能確認
スマートフォンは一度に表示出来る画面が通常１つであるが、ＰＣ上では１つのスクリーン上で複数画面を表示出来るので、時系列サマリーデータの異なったモダリティのもの同じ部位で異なったモダリティのもの、部位の異なった画像が並べられる。
また、シナリオのエピソードごとの関連データを①画像にして提示することもできる。

６．医療機関等から提供された資料のＰＤＦ化
コピー機方式はシートごとに行うので一般的に変換時間が長い。
カメラ方式のスタンドスキャナーとして、A.M.T. piQx スキャネックスを主に評価したが、
スマートフォンのアプリケーションとして「ＰＤＦスキャナー」と称するものが有り、１回の紙面の撮影でひずみ補正をして、ＰＤＦ化するものであるが、歪み補正や撮影位置の再現性慣れが必要である。

７．ＩＳＯ／ＴＣ２１５のPublic Key infrastructure規格化の状況
ＰＡＲＴ１～３の改定は日本で国家資格を示す為に使用している項目のhcRoleがオプションになったが、特に運用上は問題が無い。
ＰＡＲＴ４はＪＡＨＩＳ（保健医療服情報システム工業会）がＩＳＯ規格化したもので国内の動向とは整合性が取れている。
ＰＡＲＴ５はＴＣ２１５　ＷＧ４（セキュリティWG）とＪＡＨＩＳのセキュリティ委員会が共同して議論に参加し、国内との整合性を進めている。

Ｅ．結論
１）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。
２）利用者証明機能のＰＩＮ無しによる利用
機関コードの体系化と公開方法およびこれに対応して健康情報の分類が必要になる。
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、早急な活用を期待したい。
４）提供情報の真正性確保
スマートフォンで公的認証サービスを用いて電子署名を行うアプリケーションは一般的に普及していないので、今後の課題である。
５）電子生涯健康手帳サービスでの機能確認
スマートフォン、ＰＣまたタブレットの機能を生かして、場面に応じて使い分ける必要がある。
６）医療機関等から提供された資料のＰＤＦ化
紙で提供されたものの個人によるデジタル化は簡易な機器開発が望まれる。
７）Public Key infrastructure 規格化の状況
日本として今後ともＴＣ２１５　ＷＧ４等を通じて参画していく必要がある。

文献
１）小尾高史、公的個人認証サービスのあらたなり用シーンへの展開、東京工業大学科学技術創造研究院未来産業研究所　第６回　社会情報流通基盤研究センター・シンポジウム講演資料集、２０１６年４月２２日

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

厚生労働科学研究費補助金（地域医療基盤開発研究事業）
分担研究報告書

医療・介護分野における公的個人認証サービスを利用した情報連携に関する調査研究

－薬務関連に関わる公的個人認証サービス利用例の調査・検討－

研究分担者　土屋　文人　　国際医療福祉大学薬学部　特任教授

研究要旨

今般電子処方せんが違法でなくなったことに伴い、薬剤師に関連する記録を電子的にどのようにすべきかについて検討を行った。薬剤師の業務は対物業務から対人業務への転換が行われている最中であるが、医師・歯科医師に比べて身分法における法的規定が存在していないことから、この面でも整備が必要と思われる。患者が服用した医薬品を記録するお薬手帳については、現在電子化が進展しつつあるが、患者のＰＨＲとして原点に戻った検討が必要と思われる。また、我が国において流通している全ての医薬品を記録可能ならしめるコードは存在していない。医療用医薬品以外の医薬品を含めた形でジード体系を検討すべき時期にきていると考えられる。

Ａ．研究目的

本研究期間において薬務関連に関わる公的個人認証サービス利用が普及・実用化しているケースは存在していない。しかしながら、電子処方せんについては平成 28 年 2 月に開催された第 29 回医療情報ネットワーク基盤検討会を経て、3 月 31 日付けで省令改正が行われ、「電子処方せんの運用ガイドラインの策定について」なる通知が発出されたことから、次年度において電子処方せんが実用化する可能性が出てきた。また、将来的には電子処方せんとの連携が必須となる電子版お薬手帳については、平成 27 年に「電子版お薬手帳の適切な推進に向けた調査検討会」が開催され、電子版お薬手帳に関する諸課題について検討がなされた。しかし本検討会は、現在日本薬剤師会やチェーン薬局によって現実に実用化されている電子版のお薬手帳について一定の方向性を持たせる事及び、診療報酬や調剤報酬において電子版のお薬手帳においても、算定を可能にする（電子版のお薬手帳の紙版お薬手帳との同等性を確保する）こと等の課題も含まれていたことから、電子処方せんにおいて検討されたような原点に戻って厳格な規定を定める事よりは、先行して実用化されてしまった電子版お薬手帳について実務的な面からの運用について検討が行われた側面が強い。そのため、本来なら患者個人のＰＨＲそのものであるお薬手帳であるが、現実の運用としては、公的個人認証サービスを利用することは全く要件とされていないのが実情である。

そこで本研究においては、将来的に電子処方せんが普及し、かつ電子版お薬手帳との連携が図られることを前提とした場合に、

薬務関連、特に処方せん調剤に関連して公的個人認証サービスとして実行される可能性があるものを含めて考えた場合に、そこに生じると思われる課題の検討を行うとともに、将来的に克服すべき課題等について検討を行うこととする。

薬剤師法第25条の２は、以前は情報提供義務のみを定めていたが、平成26年施行された改正により、「薬剤師は、調剤した薬剤の適正な使用のため、販売又は授与の目的で調剤したときは、患者又は現にその看護に当たっている者に対し、必要な情報を提供し、及び必要な薬学的知見に基づく指導を行わなければならない。」と変わり、薬剤師に医師同様の指導義務が課せられることになった。従来薬剤師の業務は対物業務的なものが多かったが、この指導義務が与えられたことにより、薬剤師の業務は対人業務へと移行し、それ故、指導内容等を記録する義務も課せられたことになる。

また、薬剤師は薬剤師法第24条により「薬剤師は、処方せん中に疑わしい点があるときは、その処方せんを交付した医師、歯科医師又は獣医師に問い合わせて、その疑わしい点を確かめた後でなければ、これによって調剤してはならない。」と定められている。即ち、医師から患者に処方せんが交付されるが、その内容について疑義が無い場合には、交付された処方せんの内容がそのまま確定するが、疑義照会が行われて内容に変更が生じた場合には、薬剤師により変更された内容が処方せん記載内容の最終確定となる。従ってこの疑義照会の内容の記録は最終的な処方情報を決定するという極めて重要な記録に位置づけられるのである。我が国は医薬分業を原則としていることから、通常疑義照会を行う薬剤師は保険薬局の薬剤師ということになる。その場合、本来なら薬剤師の個人認証のみでよいと思われるが、保険診療においては、保険薬剤師の資格を有していることも求められることになる。しかしながら、薬剤師は国家資格であるが、保険薬剤師は都道府県知事の許可によるものである。処方権を有する医師の場合に求められる資格としては、国家資格である医師資格と都道府県知事の許可による保険医と麻薬施用者免許が存在する。

医師、薬剤師の資格認証については、日本医師会、日本薬剤師会において、少数ではあるが、資格証の発行等が行われていることから、それに委ねることとする。

一方、千葉県においてテレビ電話を利用した医療用医薬品の服薬指導を行うことが最近特区申請されたことから、本研究においては、改正薬剤師法による薬剤師の指導義務を中心とした情報連携について検討を行うこととする。

Ｂ．研究方法

改正薬剤師法は、ＯＴＣ医薬品のインターネット販売の是非を巡る論議を経て、薬事法（現医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律；医機法）が改正され、ＯＴＣ医薬品の分類が要指導医薬品と一般用医薬品、薬局医薬品という分類に変更になったこと、また要指導医薬品及び薬局医薬品に関しては対面販売が義務づけられ、同時に薬剤師に対して、「薬学的知見に基づく指導」が義務づけられたものである。前述のように、指導内容については指導したことの証としての記録が求められる事になる。そこで本研究では、今後医