（エ）保健指導情報

5. 個人健康

（ア）既往歴

（イ）治療状況

（ウ）メンタルヘルス

従業員個人を取り巻くこれらの情報は、管理組織も内容も全く関連が無い。また、何時、どこで、どのように利用されるか不明である。おそらくは、ほとんど利用される可能性はないと考えられる。しかし、アスベストやB型肝炎などのように、記録があることで利用されることもある。

生涯という数十年に渡って、これらの情報をすべての従業員個人に継続して利用できる状態にするには、最終的には企業から従業員個人に情報提供する以外にはない。

２，情報提供の方法

１，　各部署が定期的に発行する。

２，　人事や安全衛生が協力して、情報を取りまとめて定期的に発行する。

各部署が発行する方法は、情報に関する責任が明確だが、発行作業や配布作業上効率が悪い。

人事や安全衛生が取りまとめる方法は、情報の確認や業務内容の変化の反映が、配布時とずれる可能性が高い。

中小企業の場合には、各部署の発行の作業量の負担はあまり重くはない。しかし、大企業になると負担が増大するので、情報を管理しうる部署でまとめたほうが良い。

従来にない方法として、産業保健の現状をまとめて報告する方法が、望ましいと考える。

E. 結論

産業保健分野における、健康関連情報は多岐にわたる。今後数十年という長期に渡る健康情報の保護管理のためには、多様な変化に耐えうる情報提供の方法を検討する必要がある。

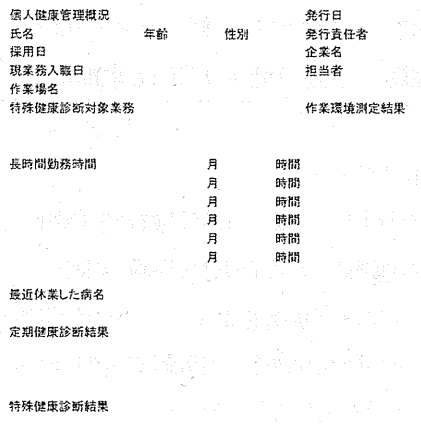
F．健康危険情報

特になし

G．研究発表

1. 論文発表

八幡勝也　他、病院情報システムにおける紙情報の現状と変化の方向性、医療情報学、34(Suppl.)、186-189、2014



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研究関する調査研究

－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－

研究分担者　齋田　幸久　東京医科歯科大学　画像診断・核医学分野　特任教授

研究要旨

医療・介護分野における公的認証サービスを用いた情報連携を行う際には、医療機関を対象とするだけではなく、個々人を対象とした肌理細やかな連携支援も視野に入れる必要がある。患者あるいは介護される側の利益を第一義として念頭においた構想を立案する必要があるのはもちろんであり、患者の living will としての意志確認にも踏み込んだ情報連携についても検討した。

A．研究目的

JPKI を利用した電子認証機能を利用したHPKI との連携による高度な保険・医療・と介護サービスの実現を目指し、その実用化に向けての具体的課題、問題点を明らかにし、進むべき方向性を示すこと。

B．研究方法

公的認証サービスを利用しての有効な医療情報連携モデルとしてのユースケースをとり上げ、実地調査を踏まえながら、問題点を検討する。

（倫理面への配慮）

患者個人情報に極力配慮する。

C．研究結果

医療において、開業医、地域基幹病院、がん拠点病院などのそれぞれの役割を十分生かすには、複数の医療施設が共同で医療を実践する方向を示さなければならない。分野別にみると、救急および一般医療においては、既往歴、手術歴、遺伝情報、アレルギー情報、などを共有することが患者個人の直接の利益に繋がる可能性が高い。但し、これらの情報を医療分野以外で利用することには厳しい制限を設ける必要がある。また、救急、および、介護の分野では、患者の意思表現としてのLiving willを積極的に取り込み、臨床内容に反映する仕組みが必要である。

D．考察

既往歴、手術歴、遺伝情報、アレルギー情報などの基本的な医療健康情報などを患者の過去を振り返る情報とすれば、Living willは患者の未来を展望する重要な医療情報である。患者本人の意志を無視した医療技術の応用は現実として多くの弊害を生じている。これらを医療情報として客観化し共有化することは、高い医療の質を追及する際に必須の要素となる。これら患者のための医療情報の保存、共有が可能となることで、新しい医療の在り方を展望し、新しい医療文化を導入する絶好の機会になり得

る。

E．結論

一般医療、救急、介護・訪問看護などで共有すべき医療情報は一患者単位とし、連携する際には、当該患者のためという一点のみで正当化される。患者本人の人間性尊重のための意志確認を情報として取り込むことが重要な課題である。

F．研究発表

なし

1. 論文発表

なし

2. 学会発表

なし

G．知的所有権の取得状況

1. 特許取得

なし

2. 実用新案登録

なし

3. その他

なし

H26 年度　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」
分担研究報告書

医療機関における患者個人への画像情報提供に関する研究

研究分担者　安藤　裕　放射線医学総合研究所　重粒子医科学センター 病院長

研究要旨　JPKI を利用して、多施設間で医療情報を連携して、有効に活用し、医療の効率化高度化を目指すことが期待されている。この場合に、Integrating the Healthcare Enterprise (IHE)のテクニカルフレームワークを使用して画像情報を扱うと仮定した場合に、JPKI や HPKI との整合性を図りつつ、どのような問題点があるかを検討した。

A．研究目的

患者の画像を含む医療情報を医療機関間で跨いで、あるいは、地域医療圏を跨いで医療情報を連携することは重要である。この場合に、予め登録された JPKI の患者の基本情報（氏名、生年月日、性別、住所）と患者のパスワードなどを組み合わせて、患者個人を認証する方法を検討した。さらに、医療機関でこのような個人認証が利用できるか検討を行った。

また、このような枠組みを Integrating the Healthcare Enterprise (IHE) [1][2]のテクニカルフレームワークを利用する場合の可能性について検討した。

B．研究方法

前提として以下のワークフローを用いる。図１に示すように、（１）個人番号カードによりパスワードなどで個人認証を行う。この結果、個人番号に付随する基本４情報（患者氏名、生年月日、性別、住所）を個人情報 DB に問い合わせる。（２）患者の４情報から Master Patient Index (MPI) のデータベースに患者検索を行う。（３）MPI を元に各医療機関の患者 ID を取得し、患者の同意の下に各医療機関へ必要な情報（診療情報や画像情報）を参照する。

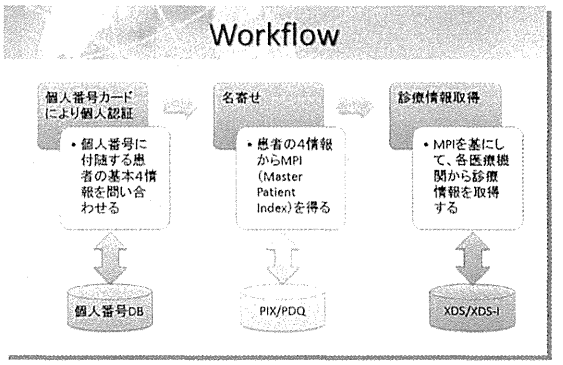


図１　ワークフロー

施設間連携や地域医療圏における連携に利用できそうな IHE のテクニカルフレームワーク (Technical Framework) として、ITI 領域と放射線領域から利用可能な統合プロファイル (Integration Profile) を抽出した。ワークフローの名寄せには、Patient Information Cross-referencing / (PIX/PDQ) を使用する。もし、複数のコミュニティーにまたがって名寄せを行う場合には、Cross-Community Patient Discovery (XCPD) も使用する。次に、診療情報の取得には、文書情報は Cross-Enterprise Document Sharing (XDS)、画像情報は Cross-Enterprise

Document Sharing for Imaging （XDS-I）を用いる。もし、情報がたのコミュニティーに保管されている場合は、文書用に Cross Community Access（XCA）、画像用に Cross Community Access for Imaging（XCA-I）を使用する。

個人情報保護には、 Basic Patient Privacy Consents （BPPC）使用することになる。

システムの監査証跡には、Consistent Time （CT）と Audit Trail and Node Authentication (ATNA)を使用する(表 1)。

C．研究結果

ここでは、平時に患者 ID を確認する場合を検討する。

C.1　患者 ID の確認

大規模災害が発生した時には、患者は診療機関の診察券や保険証を失ってしまう可能性がある。この場合、患者の個人を特定する手段として、個人番号カードを利用することにする。この場合、簡易的な認証方法を利用して可能性のある患者基本情報を検索し、患者に氏名や住所を申告してもらい、複数候補から患者を同定する方法が必要である。

患者の基本 4 情報が分かれば、IHE ITI のテクニカルフレームワークにある、PIX の機能を利用することにより、患者の Master Patient Index（MPI）を検索し、MPI より複数の医療機関の患者 ID が判明し、各医療機関での診療情報を閲覧することが可能となる（図２）。

また、患者の本人確認には、患者の氏名や生年月日の確認などが必要になり、この機能を実現するには、IHE の PDQ プロファイルが必要である。

PIX/PDQ を利用して、MPI より各医療機関の情報にアクセスすることが可能となる。この場合利用する統合プロファイルは、XDS.b または XDS-I.b である。このような枠組みでは、共通のデータ開示のポリシーを持っている医療機関の団体が一つの単位となる（図 3)。

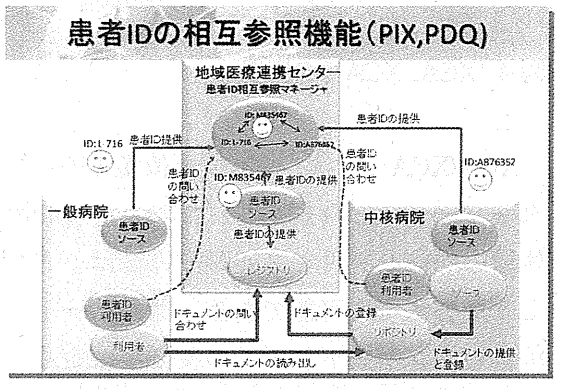


図２　PIX,PDQ による患者 ID 管理

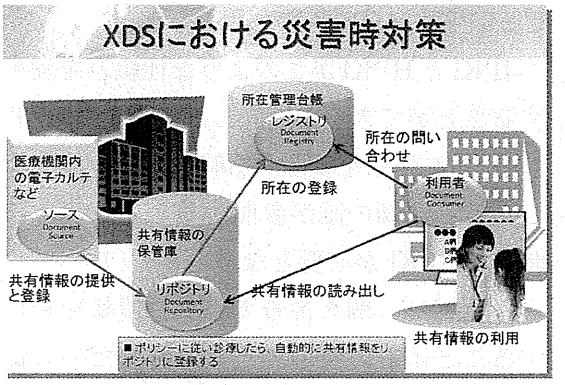


図３　XDS による情報共有

さらに、これらの医療団体を跨いで情報にアクセスすることが必要となる場合は、IHE の XCA（文字情報）と XCA-I（画像情報）が必要となる。概要を図４に示すが、同一ポリシーの団体内のアクセスは、完全に隠蔽化されており、団体間のデータやり取りの手順やフォーマットが規定されている。

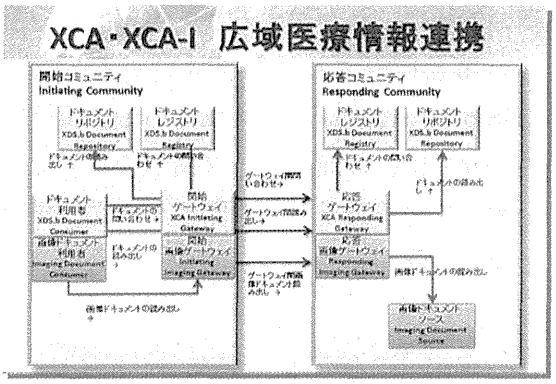


図４ XCA、XCA-I の概要

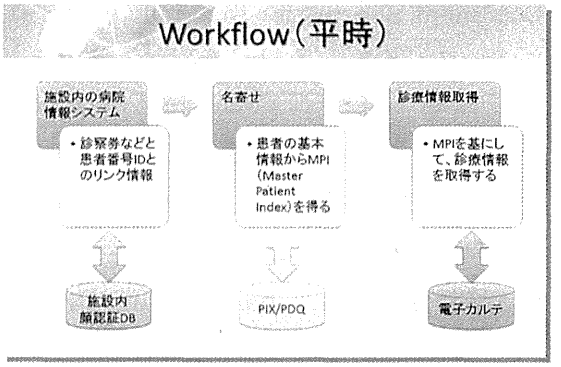


図５ 平時の時のワークフロー

XCA/XCA-I では、依頼元と依頼先のインターフェースのみ規定されており、その団体間の内部のアクセス手順や方法は、どのような方法でも可能である。開始ゲートウエイと応答ゲートウエイの役割が規定されており、非同期の応答も可能である。

C.2 JPKI と HPKI の利用

JPKI と HPKI がこのような仕組みを利用することができるか検討した。JPKI で患者の基本 4 情報を参照する時に、医療機関もしくは、医師の誰が参照するかを証明する時に、HPKI が必要となろう。

平時では、個人番号カードの情報を利用することは、困難と考える。そのため、個人番号カードとその利用の正当性を保証するために自分の身分を証明する機能として、HPKI を利用する必要がある。この場合、各患者のデータと患者基本情報とのリンク情報を整備する必要がある。各医療機関では、予め、患者の基本情報をリンクしておく必要がある（図５）。

この場合、多くの医療機関では、患者の顔写真を初診時に登録し、患者の取り違え防止に利用しているので、この患者写真を利用できれば、患者の基本情報とリンクすることは、手間が少ないと考えられる。

IHE の統合プロファイルでは、患者の顔写真から該当する患者の基本情報を取得して、病院内の患者 ID（カルテ番号）を導く方法が定義されていない。この機能を実現するために、統合プロファイルを拡張するか、または、IHE のスコープ外として、各医療機関に独自の方法で実装することにするか検討が必要であった。

D．考察

D.1 PIX/PDQ の拡張機能としての顔認証

図６に示すように、患者の MPI を管理しているデータベースがあり、これを Patient Identifier Cross-reference Manager（PICM）と呼ぶ。この PICM は、複数の医療機関に関する患者 ID を管理しており、ある患者は、A 病院のカルテ番号 X 番が B 病院のカルテ番号 Y 番であり、C 病院のカルテ番号 Z 番が同一であることを管理している。

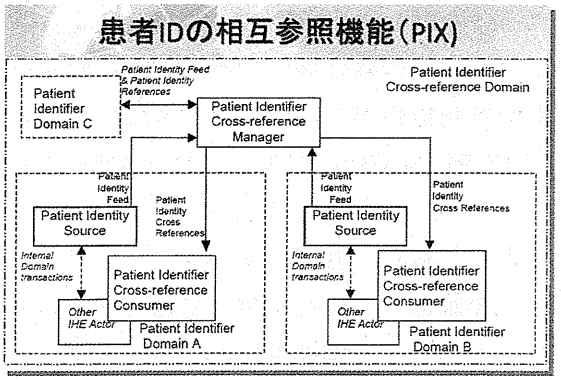


図6　患者 ID の相互参照機能（PIX）

PICM は、患者の ID を各施設の Patient Identity Source（PIS）から受け取り、自分のデータベースを update することになる。この場合、顔認証システムが各施設にあるとそのシステムからの新規 ID 登録を処理する必要がある。

図 7 には、PDQ の機能を示す。PDQ は、Patient Demographic Consumer（PDC）から対象とする患者の基本文字情報を登録し、また基本文字情報による検索に応答する機能である。この文字情報に患者の顔認証情報を含ませることは、困難があるので、PDQ の拡張は困難であろう。そのため、顔認証モジュールとして別に考えることが、IHE の考え方としては適していると考えられる。

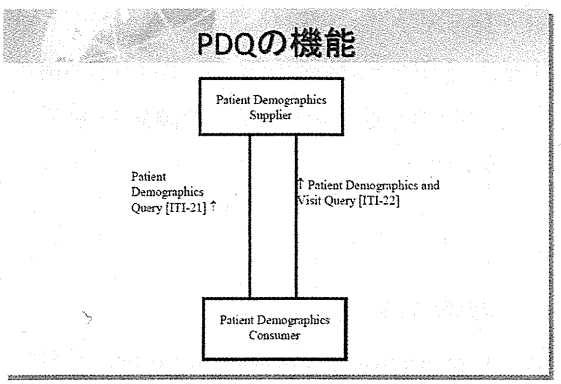


図7　PDQ の機能

D.2 プライバシー保護

患者の個人認証を行うことは、必要性が高く、また、場合によっては緊急性のある事項である。そのため、平時に比べて、患者のプライバシー保護のハードルが下がっている。このような場合でも適切にプライバシー保護を行うことが重要である。

患者が自分のデータを救命救急時にどのように使用するかをあらかじめ定めておく方法を提供するのが、BPPC (Basic Patient Privacy Consents)である。基本患者プライバシー同意プロフィールは、患者のプライバシー同意を記録するメカニズムを提供し、コンテンツ・コンシューマーが適切なプライバシー同意を使用できるような方法を提供する（図 8）。

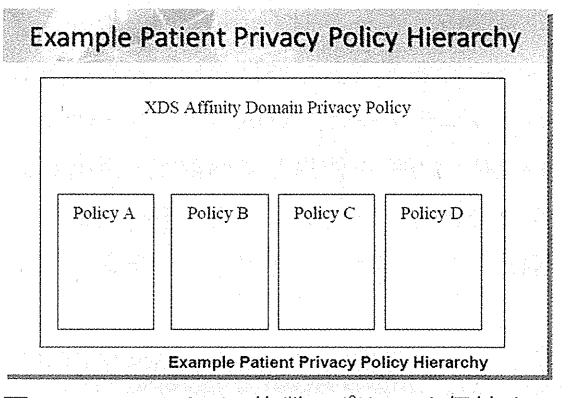


図8　BPPC における複数のポリシーを保持する機能

図 8 に示すように、BPPC を用いることにより医療情報の利用ポリシーを①平常時、②災害時、③意識消失時などと分類して定めることが可能となる。災害時に社会インフラがダウンしたときに、このポリシーをどのように管理し、アクセスするか課題は残る。このような複数の状況に対応したポリシーを管理でき、さらに、状況に応じてそのポリシーを確認して、アクセス等を切り替えることができる仕組みが大変有効と思われる。

D.3 Cross-Community Patient Discovery

(XCPD)

コミュニティー間の患者発見(XCPD)プロフィールは、患者の関連する健康データを保持するコミュニティーを見つける手段、および同じ患者のコミュニティーを横断する患者 ID の変換を提供する。コミュニティーは、確立しているメカニズムによってコミュニティー内の健康情報を共有する際に、共通のポリシーを用いた相互提供に合意した一群の医療機関として定義される (図 9)。

医療機関は、EHR、PHR などのような任意のタイプの医療サービスを提供する。コミュニティーは homeCommunityId と呼ばれるユニークな id によって識別可能である。1 つのコミュニティーの中の医療機関の会員資格は、それが別のコミュニティーのメンバーであることを妨げない。そのようなコミュニティーは、XDS プロフィールあるいは他の方法を使用して内部での共有構造が何であれ、ドキュメント共有を定義する XDS アフィニティードメインである。

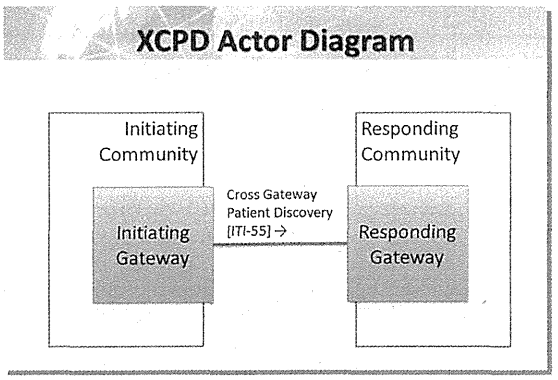


図 9　XCPD のダイアグラム

D.4　課題

XDS の大規模災害時の検討が必要となる。いかにリポジトリや画像ソースにデータを事前に準備して保管するかが鍵となる。

名寄せ機能は、PIX/PDQ で実現することは可能である。更に、コミュニティー間の場合は、XCPD を利用すれば可能と思われる。ただし、XCPD は、検索対象のコミュニティーの数が多くなると検索に時間がかかる可能性があるので、できれば、事前に XCPD を実行しておくことがベターである。

また、事前に BPPC を用いて、プライバシー保護のポリシーを定めておく必要もある。このような事前準備をどのように行うかは、費用や人手の面で大きな課題となる。

PIX/PDQ、XDS, XDS-I, XCPD, XCA, XCA-I の各システムは、CT+ATNA で監査証跡を行う必要があり、誰が責任を持って行うかポリシーを決める必要がある。

MPI として、マイナンバーからリンクした医療 ID (仮称) が利用できるようになることを予想すると、MPI は将来、この医療 ID とリンクすることが重要である。この医療 ID が実現してすぐに MPI に組み込まれることが可能なように今から準備しておくことが望まれる。

E．結論

地域医用連携に個人番号カードを利用して個人認証を行うことを検討した。この場合に期待されている IHE の機能として、XDS、XDS-I、PIX/PDQ、XCA、XCA-I、XCPD、ATNA、CT などがあり、JPKI と HPKI を同時に利用することが可能か検討した。その結果、いくつかの課題を解決する必要があった。

F．参考文献

[1] Integrating the Healthcare Enterprise (IHE), http://www.ihe.net/Technical_Framework/index.cfm

[2] 日本 IHE 協会、http://www.ihe-j.org/

なし

G．研究発表

1．論文発表

なし

2．学会発表

H．知的財産権の出願・登録状況

なし

表1　使用を検討するIHEの統合プロファイル

番号	機　能	IHE プロファイル
1	名寄せ機能（コミュニティ内）	・Patient Information Cross-referencing / (PIX/PDQ)
2	名寄せ機能（コミュニティ間）	・Cross-Community Patient Discovery (XCPD)
3	診療(文書)情報の共有機能 画像の共有機能	・Cross-Enterprise Document Sharing (XDS) ・Cross-Enterprise Document Sharing for Imaging (XDS-I)
4	コミュニティーを跨いだ診療(文書)情報の共有機能 画像の共有機能	・Cross Community Access (XCA) ・Cross Community Access for Imaging (XCA-I)
5	個人情報保護には、使用することになる。	Basic Patient Privacy Consents (BPPC)
6	時刻同期と監査証跡	・Consistent Time (CT) ・Audit Trail and Node Authentication (ATNA)

公的個人認証サービスをPINなしで使用する場合の安全確保に関する研究

研究分担者　山本　隆一　　東京大学大学院医学系研究科医療経営政策学講座　准教授

研究要旨　公的個人認証の本人確認サービスを医療介護分野で用いる場合、様々な場面でPIN無しで使用しなければならなくなることが予想される。公的個人認証の本人確認サービスでは外部認証によるPINなしのインターフェイスが用意されているが、その運用に関して考察を加えた。想定されるPINなしの本人確認は、証明書のシリアル番号だけ読み出し、その番号で本人確認を行うこと、ICカードリーダに外部認証機能を持たせ、リーダを信頼できる期間に配布する方法、サーバ側に外部認証機能を持たせ、ネットワーク越しに外部認証を行う方法の３つが考えられる。シリアル番号だけ読み出す場合は、証明書とICカードの関係の正当性を確認できないためにシリアル番号のなりすましの危険を排除できない。他の２つは証明書の正当性を確認できるために、シリアル番号のなりすましは防ぐことができる。外部認証機能を持つリーダを配布する場合は、外部認証のトランザクションはローカルに限定されるために、パフォーマンスは高いと思われるが、リーダ配布の労務コストが高い。また医療機関等におけるリーダの管理を確認する必要がある。サーバによる外部認証は特別なリーダを必要としないが、外部認証を要求している組織が信頼できる医療機関であることを何らかの方法で確認する必要があり、On Demand VPNとHPKI組織認証を組み合わせるか、SSLクライアント認証にHPKI組織認証用証明書を用いるなどの工夫が必要となる。いずれにしても早期のHPKI組織認証の整備が求められる。

A．研究目的

諸外国で、国民にかなりの割合でICカードを配布しているのは、ほぼすべてICカードに医療保険証機能を持たせている場合で、わが国でも個人番号カードを相当程度網羅的に配布することを目指すのであれば、保険証機能の不可は必須であろう。ICカードに様々な情報を付加する実証事業は数多くなされているが、いずれも負荷した情報の管理が複雑になり、運用コストの高騰を招いている。多くの実証事業の結論では、ICカードはキーとして用い、情報自体はサーバに格納し、キーで検索することが妥当とされている。個人番号カードは新たな公的

個人認証の仕組みが内臓されており、個人番号を用いることなく、アクセスキーとして使用できる。個人番号カードには署名用と本人確認用の２つの証明書と私有鍵が格納される。また本人確認サービスは外部認証の仕組みが用意され、条件を満たせばPINを入力しなくても本人確認用の証明書の正当性・有効性が確認できる。医療現場では短時間に大量の保険資格確認を行う場合や本人に意識がない場合、あるいは認知症が高度な場合など、本人にPINを入力させることが期待できない場合がある。本研究の目的は、公的個人認証の本人確認サービスをPINなしで用いる場合の安全性を評価し、最適な方法を提言することにある。

B．研究方法

公的個人認証の各サービスの仕様が研究時点で十分に公開されていないため、実証的研究が困難なため机上の考察によった。各種ガイドラインやOn Demand VPNのHEASNETの規格書、および、HPKIの組織認証のポリシを参考文献とした。PINなしの利用を以下の３つのパターンを想定し、安全性と運用コストを検討した。

1　本人確認用証明書のシリアル番号を直接読み出す方法
2　外部認証機能を持つICカードリーダを、医療機関等を確認して配布する方法
3　外部認証サーバを設定し、ネットワーク越しに外部認証を行う方法

C．研究結果

C-1　本人確認用の証明書のシリアル番号を直接読み出す方法

本人確認用証明書は本質的に公開情報であり、個人番号カードでも特段のアクセス権がなくても読み出せると考えられる。証明書自体は公的個人認証サービスの認証局の署名があり、偽造は困難であるが、個人番号カード内の私有鍵との関係を確認派できない。つまり、個人番号カードと同様の証明書読み出しインターフェイスを持つICカードを用意すればコピーの作成が可能であり、アクセスキーとしての最低要件を失う。

C-2 外部認証機能を持つICカードリーダを、医療機関等を確認して配布する方法

外部認証の関わるトランザクションはローカルに行われ、パフォーマンスは最も高いと思われる。ただし、安全性はリーダの配布の正当性と、医療機関等におけるリーダの管理に依存する。リーダを適切に配布するためにはPINなしで使用する権限のある組織にリーダを配布する必要があり、C-3と同様の確認コストがかかる上に、リーダの盗用に対して、十分な保護策がとられなければならない。また在宅医療のや在宅介護の現場までリーダが持ち込まないといけないことを考えると、安全管理の面から現実的な運用は相当困難であると考えられる。

C-3 外部認証サーバを設定し、ネットワーク越しに外部認証を行う方法

医療機関等では通常のリーダの設置でよく、管理面では負担は軽減される。ただし、外部認証サーバは信頼できる場所からの要求であることを確認する必要がある。中規模医療の医療機関等では複数のリーダが必要であり、ゲートウエイを設置し、ゲートウ

エイと外部認証サーバを場所の信頼性が確認できる VPN で接続されなければならない。Internet VPN を用いる場合は On Demand VPN を用い、ルータ（ゲートウエイ）認証には医療機関等であることを確認できる公開鍵基盤である、HPKI 組織認証を用いる必要がある。IP-VPN を用いる場合も、SSL 等のクライアント認証が可能な暗号化を使い、クライアント証明書に HPKI 組織認証を用いることが適切と考えられる。なお、HPKI 組織認証以外の確認方法も想定されるが、現在レセプトオンライン請求に使われている SSL クライアント証明書は代行請求が存在することや、発行時の組織の正当性確認がそれほどの厳密性を必要としないことを考えると、適切とは言えない。これ以外に現実に医療機関等の組織の正当性を確認できるのは、HPKI 個人認証で、施設の代表者の証明書を使う可能性が考えられるが、現在、発行はされておらず、また、あくまでも個人の認証であり、代表者の変更の際の手続きが複雑になることなどを考えると、ゲートウエイで自動認証する用途に用いることは適切とは言えない。

またこの方法を用いることの利点として、リーダが組織の外部にあっても、適切な VPN で組織のゲートウエイを通じて外部認証を行うように設定すれば、在宅などの現場でも利用可能になることが挙げられる。C-2 に比べて劣る点は外部認証に関わるトランザクションが VPN ネットワークを通じて行われるために、パフォーマンスの低下は否めない。

D．考察

３つの想定した方法の内、証明書のシリアル番号だけ読み出す方法は安全性の観点から採用すべきではなく、IC カードリーダに外部認証機能を持たせ、リーダを信頼できる期間に配布する方法、サーバ側に外部認証機能を持たせ、ネットワーク越しに外部認証を行う方法の２つは安全性の観点からは採用可能を考えられる。外部認証機能を持つリーダを配布する場合は、外部認証のトランザクションはローカルに限定されるために、パフォーマンスは高いと思われるが、リーダ配布の労務コストが高い。また医療機関等におけるリーダの管理を確認する必要があり、在宅などの院外での使用は困難である。サーバによる外部認証は特別なリーダを必要としないが、HPKI 組織認証を組み合わせるか必要があり、院外での使用も可能であるが、外来繁忙時の保険証の資格確認に用いる場合は、フィージビリティ・スタディが必要であろう。

HPKI 組織認証は CP の検討は厚生労働省の HPKI 専門家会議で検討はされているものの、実際に稼働している CA はない。早期の整備が望まれる。

E．結論

PIN なしの外部認証のもっとも優れた方法はサーバ側に外部認証機能を持たせ、ネットワーク越しに外部認証を行う方法に HPKI 組織認証を組み合わせた方法であり、HPKI 組織認証の基盤の早期の整備が望まれる

F．健康危険情報

特になし。

G．発表

なし

H．知的財産権の登録・出願状況

現在のところなし。

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にかかわる技術的検討
研究分担者　小尾高史　像情報工学研究所　准教授

研究要旨　社会保障・税に係る様々な手続きにおける国民の利便性向上を目的とし、行政手続における特定の個人を識別するための番号の利用等に関する法律（番号法）及び、番号法の施行に伴う関係法律の整備等に関する法律（整備法）が平成25年5月24日に成立した。これにより、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、平成28年1月からは個人番号カードの交付が開始される予定となっている。個人番号については、法施行後3年を目途にその利用範囲の拡大について検討を行うこととなっており、医療機関のような民間機関を含む分野での利用は、早くとも平成31年以降になると想定される。その一方で、個人番号カードに搭載される新たな公的個人認証サービスについては、カード交付時から行政機関での利用にとどまらず、一定の要件を満たす民間事業者の利用を認めることを予定しており、特に医療、金融分野での利用が検討されている。本研究では、この新たな公的個人認証サービスの医療分野での利用方法について検討を行った。

A．研究目的

社会保障・税に係る様々な手続きにおける国民の利便性向上を目的とし、行政手続における特定の個人を識別するための番号の利用等に関する法律[1]（番号法）及び、番号法の施行に伴う関係法律の整備等に関する法律[2]（整備法）が平成25年5月24日に成立した。これにより、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、平成28年1月からは個人番号カードの交付が開始される予定である。

個人番号については、法施行後3年を目途にその利用範囲の拡大について検討を行うこととなっており、民間分野の利用は、早くとも平成31年以降になると想定される。その一方で、個人番号カードに搭載される新たな公的個人認証サービスについては、カード交付時から行政機関での利用にとどまらず、一定の要件を満たす民間事業者の利用を認めることを予定しており、特に金融、医療分野での利用が検討されている。本研究では、この新たな公的個人認証サービスの医療分野での利用方法について検討する。

B．研究方法

厚生労働省は、平成20年度から21年度にかけて、健康保健証、介護保険証、年金手帳の役割を兼ね、医療機関受診時の健康保健の資格確認やインターネットを通じた自己の診療情報や年金受給額の閲覧等を可能とする社会保障カードの導入についての検討を進めていた。カード導入検討の理由の一つに、レセプト返戻の解消があり、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り、医療機

関等における事務負担軽減を図るものであった。また同時に、社会保障カードが導入されることで、保険者が変更となった場合でもカード返却の必要はなく、１枚のカードで様々な保険証などの役割を果たすため、利用者や保険者の負担軽減にもつながるとされており、平成 20 年の見積もりで、その経費削減効果は、保険者で年間約 120 億円、医療機関等で年間約 120 億円といわれていた。この際の検討では、社会保障カード導入に代わり公的個人認証サービスを利用する方法等も検討する必要があるとされていた。

また、現在、医療等分野における番号としては、健康保険証や介護保険証に記載されている保険者番号や記号番号があるが、これらは被保険者とその扶養者で同じ番号であり、転職や転居等により保険者が変わると変更が生じるため、本人を確実に特定するために使うことは難しい、また、医療分野では、年金分野における基礎年金番号のように本人特定が可能な生涯不変な番号は導入されておらず、一般的に医療機関等では、診察券番号などの独自の番号を利用して診療情報等を管理している。一方、近年の地域医療連携の推進にみられるように、医療等分野における情報連携へのニーズは高く、運用面、緊急性、さらにはコストの観点から、同一の番号を用いて患者を特定し、一次利用に限定した医療情報連携を可能とする基盤整備が求められている。このためには、社会保障・税分野の番号である個人番号を利用することも考えられるが、医療等分野において取り扱われる情報は極めて機微性の高い情報を含むものであり、かつ、情報連携に関わるプレイヤーも多いことから、個人番号とは異なる医療等分野に利用範囲を限定した別の番号を用いることが必要とされている。このような背景から、厚生労働省は平成 23 年から医療等 ID の検討を開始しており、平成 25 年 12 月に医療等分野における番号制度の活用等に関する研究会より中間とりまとめが出されている。

これらの実現に際しては、今後、本人確認のあり方やなどについて引き続き検討を進めることとされているが、その際マイナンバー法に基づくインフラについて、共用できる部分については二重投資を避ける観点から共用することが必要とされており、これらのサービスを利用する際の本人確認手段として個人番号カードに搭載される新たな公的個人認証サービス(JPKI) の利用が有力な候補であることは明らかである。

JPKI の電子利用者証明機能を利用して、健康保険等の資格確認を行うためには、まず電子利用者証明用証明書と利用者、さらに利用者の保険資格を紐づけるデータベースの構築が必要となる。現在の番号制度では、医療、介護等の保険料などの徴収及び、医療、介護保険等の給付に関する事務について個人番号を利用することが認められており、保険者は上記事務に利用するために、被保険者から個人番号の提供を受けることとなる。このため、保険者を経由して個人番号と保険資格情報の提供を求め、現在の審査支払機関（社会保険診療報酬支払基金及び国民健康保険団体連合会）もしくは、これらが共同で設置した組織（保険資格確認機関、以下保険資格確認ＰＦ）が電子利用者証明検証者として、電子利用者証明用証明書と利用者、さらに利用者の保険資格を紐づけるデータベースの構築を行うことが想定される。これにより、社会保障カードの検討と同様に、患者は医療機関の専用端末などで保険証の代わりに個人番号カードを挿入し、資格確認機関が患者の本人確認を行った後、利用者証明用証明書の発行番号に紐付けられた保険資格および被保険証番号を医療機関にリアルタイムで通知することが可能になる。

一方、患者が意識不明や危篤状態等の場合、もしくは高齢の場合などには PIN 入力を求めることができないことも想定されるため、この際には医療機関の医療従事者、職員などが患者の個人番号カードを資格確認用端末に挿入するとともに、別

途の手段で操作者が医療従事者であることや医療機関端末からの利用であることを確認することにより、PIN の入力なしで患者の資格確認を行えることが要求されており、医療等での利用を想定した場合、これらに対応できる機能をあらかじめ JPKI カードアプリケーションに搭載しておく必要がある。我々は、PIN の入力を求めない利用について、電子利用者証明の仕組みを用いてカード確認を行う仕組みを提案しており[1]、PIN 入力時と PIN 入力を求めない場合で、電子利用者証明機能の内部演算を変化させることによりどのような状況下で電子利用者証明機能が利用されているかを識別することを可能としている。この方法では、現在想定されている IC カードでサポートされる機能を利用するため、カードの仕様や運用に大きな変更を加えることなく実現が可能となっている。

本研究で提案する具体的な保険資格確認のフローを以下に述べるが、ここでは、まず、提案する手法を利用する場合の前提条件を示す。PIN 入力を求めない利用については、電子利用者証明機能の例外的利用であるため、その利用範囲については厳格に管理される必要がある。このため、この機能を利用できる保険資格確認機関は、JPKI の発行機関である地方公共団体情報システム機構から、機関コード、その機関コードを含む外部認証用公開鍵証明書及び秘密鍵を交付するものとする。ここで、保険資格確認機関に交付される秘密鍵は、耐タンパな HSM に保持され、厳格に管理される。また、個人番号カード内に格納される JPKI アプリケーションには、あらかじめ地方公共団体公共システム機構の公開鍵が格納されている。(図１) また、医療機関等におかれる保険資格確認用の端末については、正当な場所で管理・運用されていることを確認する必要があるため、保険資格確認サービスを利用するにあたり保健医療福祉 PKI などを利用した端末認証を行うことを想定する。

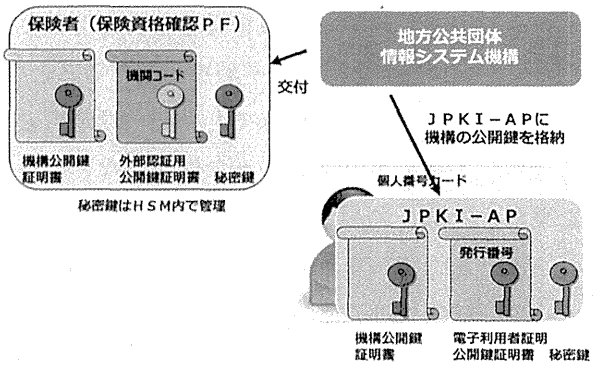


図１　保険資格確認に伴う前提

また、先に述べたように、保険資格確認ＰＦは、電子利用者証明用証明書と利用者、さらに利用者の保険資格を紐づけるデータベースの構築を行う必要がある。この構築については、可能な限り既存の仕組みを活用することを想定し、現在構築が進められているマイ・ポータルの個人アカウント開設の仕組みを利用することを提案する。

まず、被保険者は、現在の番号制度の下で、保険者に個人番号を通知する必要があるため、保険者は、各被保険者の個人番号及び保険資格を格納したデータベースを有しているものとする。ここで、保険資格確認プラットフォームにおいても、個人番号を管理できるものとし、情報提供ネットワークシステムに接続可能な組織とすることができれば、保険資格確認 PF は、個人番号よりそれに対応する機関別符号を入手し、これをデータベースに登録することができる。(図２)

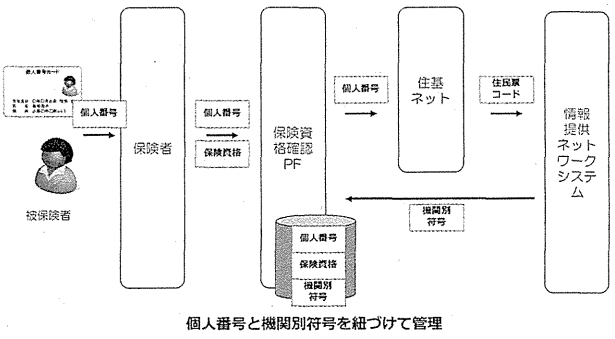


図２　初期登録　(PF への登録)

さらに、JPKI を利用するにあたっては、上記データベースに電子利用者証明用証明書の登録が必要となるが、この登録については、マイ・ポータルのために追加された電子証明書のシリアル番号から機関別符号を入手する機能を利用することが有効である。具体的には、被保険者が初めて医療機関から保険資格確認 PF への保険資格確認要求を発したとき、又は、保険資格確認 PF が用意する被保険者が JPKI と紐づけられた自己の保険資格を確認する Web サイトに初めてアクセスした際に、保険資格確認 PF が電子証明書のシリアル番号から機関別符号を入手し、上記データベースに格納されている機関別符号と照合することで、資格確認を要求した被保険者を特定し、当該被保険者と関連付けて電子利用者証明用電子証明書を登録する（図３）。これにより、次回からは医療機関からの保険資格確認要求に対して、電子利用者証明用電子証明書と紐づけられた保険資格を提供することが可能となる。

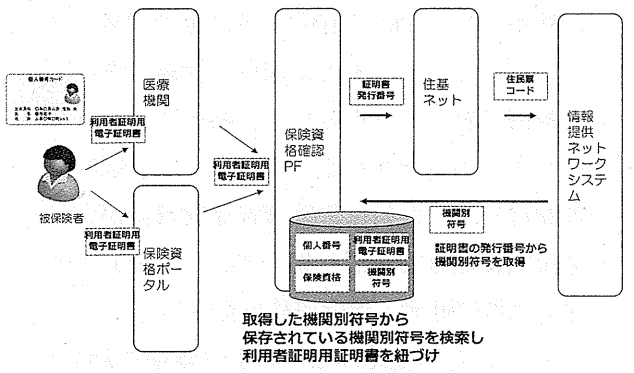


図３　初期登録　（証明書登録）

以上のようにして初期登録が終了した後の、医療機関において PIN 入力なしで保険確認を行う処理の流れを示す。

① 保険資格確認機関は、あらかじめ保健医療福祉 PKI を利用した医療機関端末の認証、もしくは医療機関の利用するネットワーク回線の確認などを利用して、保険資格確認の要求が医療機関からのものであることを確認する

② 医療機関の医療従事者は、患者の個人番号カードを端末に挿入し、PIN 入力なしでの保険資格確認を要求する

③ 保険資格確認機関は、保険資格確認機関に発行された外部認証用公開鍵証明書を医療機関端末を経由して JPKI アプリケーションに送付する

④ JPKI アプリケーションは、機構の公開鍵を利用し公開鍵証明書の検証を行い、検証に成功した場合には、その旨を医療機関端末を通して保険資格確認機関に返送する

⑤ 保険資格確認機関は、医療機関端末を経由してチャレンジコードを要求する

⑥ JPKI アプリケーションは、外部認証用の乱数を生成し、医療機関端末を通して保険資格確認機関に送付する

⑦ 保険資格確認機関は、乱数に対して自己の秘密鍵を用いて署名し、医療機関端末を経由して JPKI アプリケーションに返送する

⑧ JPKI アプリケーションは、保険資格確認機関の公開鍵を用いて、署名検証を行い、検証が成功した場合、保険資格確認機関の公開鍵証明書に含まれる機関コードを一時利用メモリに格納するとともに、外部認証が成功した旨、医療機関端末を通して保険資格確認機関に返送する（外部認証モードでの状態での利用に移行）

⑨ 保険資格確認機関は、患者の電子利用者証明用公開鍵証明書を医療機関端末を経由して JPKI アプリケーションに検証要求する

⑩ JPKI アプリケーションは、電子利用者証明用公開鍵証明書を医療機関端末を通して保険資格確認機関に送付する

⑪ 保険資格確認機関は、電子利用者証明用公開鍵証明書の検証と有効性の確認を行い、検証が成功した場合には、乱数を発生し、医療機

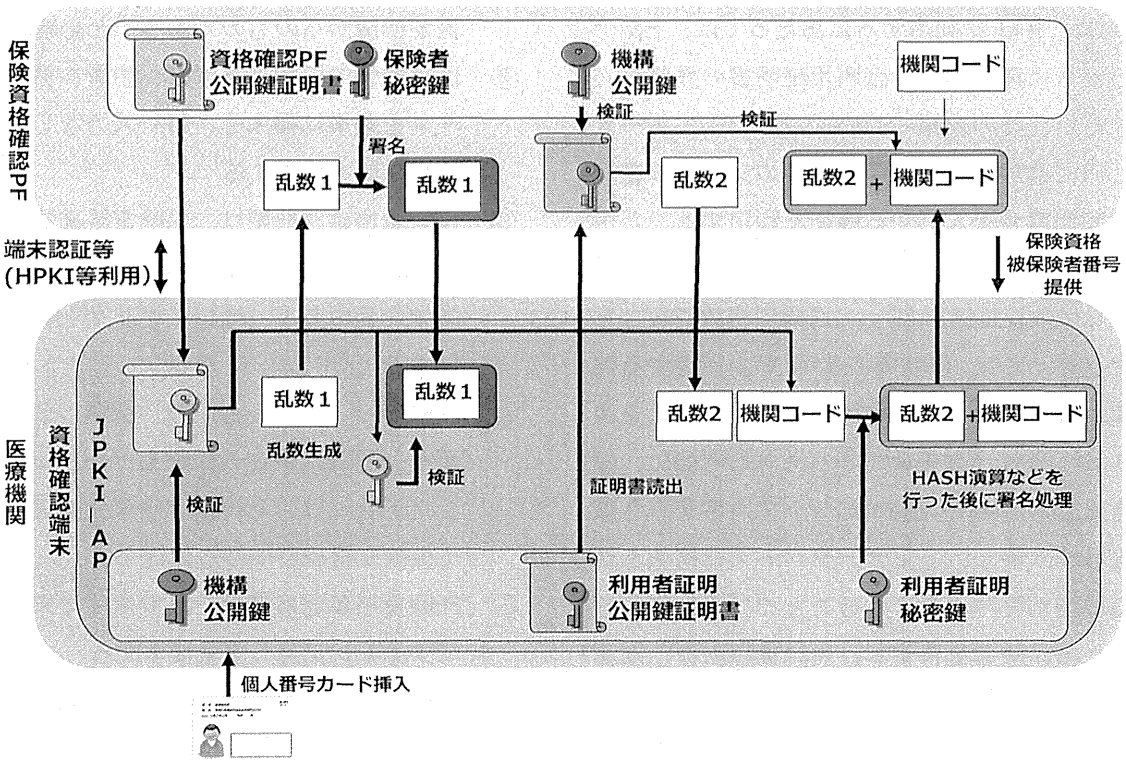


図４　保険資格確認のフロー概略

関端末を経由して JPKI アプリケーションに送付する

⑫　JPKI アプリケーションは、送付された乱数と一時利用領域に格納された機関コードから生成される署名用コードに、電子利用者証明用秘密鍵を用いて署名し、医療機関端末を通して保険資格確認機関に返送する

⑬　保険資格確認機関は、送付した乱数と自身の機関コードから署名用コードを生成し、返送された署名の検証を行う。

⑭　⑬の検証が成功した場合、医療機関端末に対して電子利用者証明用証明書の発行番号に紐づいた利用者の保険資格及び被保険者番号を送付する

⑮　医療機関は、医療機関端末に送られてきた保険資格の有無及び被保険者番号を確認する

C．研究結果

このように提案手法により、医療機関は患者の個人番号カードを利用して、PIN の入力を求めずに保険資格の確認を行うことが可能となる。この際、PIN 入力時とは異なり、機関コードと乱数から生成される署名コードが利用されるため、保険資格確認機関では、JPKI が動作する状態を明確に区別することができる。また、同様の仕組みを利用する別機関が存在する場合でも、機関ごとに異なる機関コードが発行されるため、万が一、別機関が外部認証を行った後に保険資格確認機関が電子利用者証明機能を利用した場合でも、上記⑬の処理が正常に終了せず、保険資格は提供されない。

また、この仕組みは、厚生労働省が平成 28 年度の導入をめざして検討を進めている電子処方箋の運用において、例えば、保護者が子供の個人番号カードを用いて薬を受け取るなどの際にも利用できると考えられる。

D．考察

電子認証機能を付加した公的個人認証サービスと類似する電子認証サービスは、フィンランドなど EU の一部の国でも、すでに金融分野な

ど身近な分野で利用されており、新たなJPKIで導入される電子利用者証明についても、署名用と比較して多くの場面で利用されることが想定される。このため、利用者証明用証明書については、証明書取得時に必要以上に個人情報を与えないよう証明書内に基本4情報など個人の特定が容易に可能な情報を記載しないこととなっており、また、新たな公的個人認証法で、“機構、署名検証者等、署名確認者又は利用者証明検証者以外の者は、何人も、業として、署名用電子証明書の発行の番号又は利用者証明用電子証明書の発行の番号の記録されたデータベースであって、当該データベースに記録された情報が他に提供されることが予定されているものを構成してはならない”と記載されるように、証明書に記載される発行番号をデータベース化することを禁じている。

しかしながら、今後多くの医療機関、薬局や介護機関などで利用されるようになった場合、患者のプライバシーを侵害するような誤った利用がされる可能性もある。また、JPKIの金融分野での検討も進められているため、JPKIの署名・電子利用者証明検証者の認定基準の明確化や、PINの入力を求めない利用を認める機関の認定方法、その機能の利用手順などの策定を、今後行っていく必要がある。

E．結論

本研究では、番号制度の下で導入される新たな公的個人認証サービスの実施にあたり、医療分野での利用について検討した。新たな公的個人認証サービスは、今後、医療での利用にとどまらず、金融分野など他の民間分野での利用も想定されており、今後は安全性やプライバシーに配慮しつつ、更なるユースケースの検討や、実際のサービス導入に際した費用対効果等の検証等を行っていることが必要である。

F．健康危険情報

特になし

G．研究発表

なし

参考文献

[1] 小尾高史，本間祐次，大山永昭，“公的ICカードを利用した医療機関からの保険資格確認方法の検討，”コンピュータセキュリティシンポジウム2010，2F22-1，2010年10月

研究成果の刊行に関する一覧表

書籍

著者氏名	論文タイトル名	書籍全体の編集者名	書　籍　名	出版社名	出版地	出版年	ページ
大山永昭	電子自治体推進のための体制・リーダーシップのあり方	大山永昭，木村恵太郎 編著，井堀幹夫，夏目哲也，御代川知加大共同執筆	番号制度導入時代の電子自治体加速　～その実績と展望～	自治日報社	東京	2014	1-8

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
大山永昭	中間サーバはデータ移行に有効　業務フロー可視化で調達改革を	日経ＢＰガバメントテクノロジー	第30号	35-38	2014
八幡 勝也、武田 裕 松村 泰志 中川 肇 木村 映善 村田 晃一郎 瀬戸 遼馬	病院情報システムにおける紙情報の現状と変化の方向性	医療情報学	34(Suppl.)	186-189	2014
小尾高史，鈴木裕之，李中淳，平良奈緒子，大山永昭	プライバシーを考慮した医療情報の活用とその実現に向けた課題	電子情報通信学会誌	Vol. 98, No. 3	14-15	2015
藤田和重，小尾高史，谷内田益義，李　中淳，平良奈緒子，奥　信人，庭野栄一，則武智，福田賢一，岩丸良明，大山永昭	金融・決済分野における公的個人認証サービスの活用に関する考察	信学技報	Vol.　114, No.　500	135-140	2015