

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

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

平成28～29年度 総合研究報告書

研究代表者 大山 永昭

平成30(2018)年 5月

目 次

I．総合研究報告

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	-----	1
大山 永昭		

II．研究成果の刊行に関する一覧表	-----	14
-------------------	-------	----

III．研究成果の刊行物・別刷	-----	16
-----------------	-------	----

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）

総合研究報告書

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

研究代表者 大山 永昭 東京工業大学科学技術創成研究院 教授

研究要旨： 我が国では、保健医療福祉分野向けの公開鍵基盤（HPKI）が運用されているが、カードの発行、管理、運用等に要する過大な費用やカード発行時の本人確認及び公的資格確認のために複雑な手続きが必要などの課題がある。一方、個人番号カード及びそこに搭載される公的個人認証サービス（JPKI）は住基ネットと連携して管理されるため、利用者本人との対応付けの信頼性は極めて高く、個人番号カード及びJPKIを利用した医療従事者資格の認証・電子署名の実現が可能となれば、医療従事者本人の存在の信頼性が高まるだけでなく、医療従事者資格の認証・電子署名に必要なシステムの設備投資や運用コストが削減できる可能性があり、今後の医療情報化の推進に大きく貢献すると期待される。そこで本研究では、医療従事者の資格確認や有資格者の電子署名の手段として、個人番号カード及びJPKIを利用することを検討し、その具体的な実現モデルを示すことを目的とする。個人番号カードおよびJPKIを利用して医療従事者資格を確認する方法として、HPKIの機能を個人番号カードに搭載する「個人番号カード搭載方式」、医療従事者資格の認証や電子署名の機能をASPサーバ等へ実装し、JPKIをASPサーバへのアクセス手段として利用する「サーバ連携方式」、JPKIによる電子署名及び利用者証明と、HPKI認証局による電子署名の検証や医療従事者資格確認の代行処理を組み合わせた「JPKI+検証代行方式」の各実現モデルを示し、それぞれの特徴について整理した。一方、HPKIカードの新規発行申請時における本人確認にJPKIの利用者証明を利用する手法についても検討を行い、この仕組みによってHPKI用カード発行時の手間や発行・管理に用いるシステムの設備投資が削減できるとともに、極めて高い信頼性で医療従事者の本人性および実在性を確認できることを示した。また、HPKIが重要な役割を果たすサービスへの応用として、受診記録を利用した医療情報連携や、薬歴管理について提案技術を適用したサービスモデルを検討し、提案技術の効果を示すとともに、実用化へ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
	大神 明	産業医科大学産業生態科学研究所	教授
	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	慶應義塾大学医学部	大学訪問准教授
	山本 隆一	医療情報システム開発センター	理事長
	小尾 高史	東京工業大学科学技術創成研究院	准教授

A．研究目的

近年医療分野では、レセプトオンライン申請や地域医療における情報の共有化など、従来の機関内に閉じた情報化から外部機関との情報連携へと発展しつつある。このような外部連携を実現するためには、通信相手の正当性を確認することや、情報提供者の正当性を保証することが重要であり、そのための公開鍵基盤の整備は必須である。我が国では、医療用のPKIとしてHPKIが運用されており、HPKIを利用した電子署名や電子利用者証明は、本人の存在だけでなく、その医療従事者の公的資格の正当性を確認することが可能である。

我々が実施した平成13から18年度の厚生労働科学研究では、HPKIを利用する際の技術要件や応用システムについて検討を行い、HPKIが医療の情報化にとって極めて重要であることを明らかにした。しかし、現在実運用されているHPKIを広く普及させるためには、カードの発行・運用にかかるコストの削減や、HPKI用カード発行時の本人及び公的資格確認のために不可欠な複雑な手続きの簡略化などの課題を解決することが重要である。一方、2016年1月より個人番号カードの交付が始まり、個人番号カードに搭載された公的個人認証サービス(JPKI)は、オンラインでの医療保険資格確認など様々なサービスでの利用が想定されており、近い将来多くの国民に利活用される社会インフラとなることが期待されている。またJPKIは住基ネットと連動して管理されるため、JPKIとその本人との対応は極めて高い信頼性を有する。よって個人番号カード及びJPKIをHPKIの発行・運用時の本人確認手段として利用すれば、HPKI用カード発行時の手間や発行・

管理に用いるシステムの設備投資が削減できるとともに、HPKIの利用時に必須となる医療従事者の本人性および実在性の確認を個人番号カード及びJPKIが担うことから、HPKIサービスに要するトータルコストを大幅に減じることが可能になり、結果としてHPKIの普及に大きく資すると期待される。本研究では、個人番号カード及びJPKIを医療従事者資格の認証、電子署名手段として利用する仕組みについて検討を行い、その具体的な実現モデルを示すことを目的とする。

B．研究方法

本研究で提案する個人番号カード及びJPKIを利用した医療従事者資格確認の実現方式に関し、以下の観点については、それぞれ二つの候補が存在する。

利用するICカード

- 個人番号カード or 別のカード
医療従事者資格確認機能の実装方法
- ICカード上に搭載 or ASPとして提供

上記において、の個人番号カードを利用する方法としては、個人番号カードの中にHPKIの機能を搭載する「個人番号カード搭載方式」、HPKIの資格認証に関わる機能をASPサーバ内に実装する「サーバ連携方式」JPKIによる電子署名及び利用者証明と、HPKI認証局による電子署名の検証や医療従事者資格確認の代行処理を組み合わせた「JPKI+検証代行方式」の3方式が考えられる。いずれの場合も、JPKIとHPKIを連携させるための仕組みが必要になり、そのための技術を検討する。

研究方法としては、まず現状の各種医療従事者用公的資格における HPKI の利用状況について調査を行い、HPKI を普及させる上での課題を整理する。また個人番号カードや JPKI の利用に関する制度を調査し、提案する仕組みを実現する上での制度的な課題について整理する。さらに、個人番号カードで署名する際に基本 4 情報が閲覧されてしまう問題など、現行の個人番号カード及び JPKI を HPKI と連携させる際の技術的課題についても整理する。そしてこれらの実情を踏まえ、提案する手法に求められる技術的要件を整理し、上記に述べた実現方式について、それぞれの実現モデルを提示する。また、提案技術の応用として、オンライン保険資格確認を利用した受診履歴管理や、電子処方箋の運用を前提とした薬歴管理への応用例を示すとともに、提案技術の実現のための課題を提言としてまとめる。

C . 研究結果

(1) 個人番号カードおよび JPKI を利用した医療従事者資格の確認

(ア) 個人番号カード搭載方式

まずは、前節で挙げた医療従事者資格確認の実現方式のうち、個人番号カード搭載方式について議論する。

個人番号搭載方式は、HPKI 署名および利用者証明を利用するための仕組みを個人番号カードに追加し、個人番号カード一枚で、JPKI だけでなく HPKI も利用可能にする方式である。個人番号カードに HPKI の機能を格

納する方式として、以下の二つが考えられる。

HPKI 証明書に医療従事者属性を確認できる機能を加える

個人番号カードに HPKI 用のアプリおよび証明書を追加する。

の方式では、HPKI 証明書で用いられている属性項目 (HcRole) を JPKI 証明書に追加し、HPKI 証明書と同等の機能を JPKI 証明書に持たせる方法である。この方式では、従来の HPKI 用カードに格納していたアプリおよび証明書を、個人番号カード内に格納する方法である。これら方式において想定される HPKI を新規登録するフローを図 1 に示す。このフローでは、医療従事者が自身の個人番号カードを持参して HPKI 発行を行う窓口へ赴き、まず窓口担当者に医療従事者資格を確認するための書類 (医師免許証等) を提示することで、医療従事者資格の正当性を確認する。その後、HPKI 発行を行う端末上で必要事項を記入した HPKI 発行申請書を電子的に作成し、この申請書に JPKI による電子署名を付与した上で申請書を HPKI 発行用サーバに送付する。申請書を受け取った HPKI 発行用サーバは、申請者の JPKI 署名の検証を行い、正しいことが確認できた場合には、基本 4 情報と医籍簿情報との対応を確認する。この対応に問題ないことが確認できた場合には、HPKI 機能を個人番号カードにインストールする。

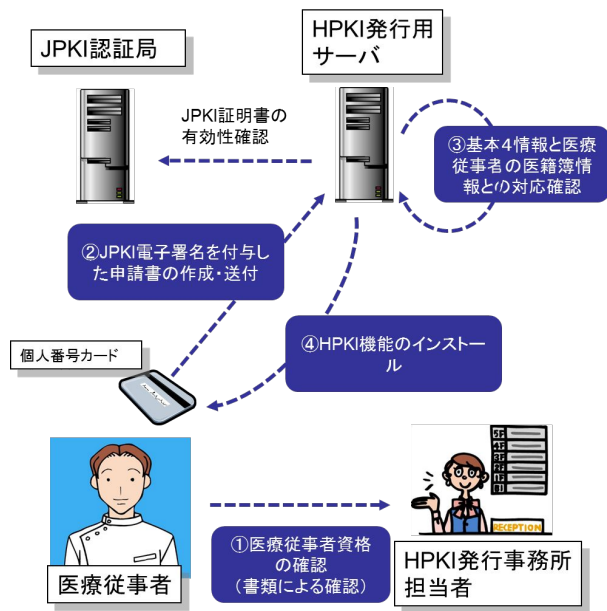


図1. 個人番号カード搭載方式におけるHPKI新規登録のフロー

それぞれの方式において、現行のJPKIや個人番号カードから変更が必要な点としては、ではJPKIの証明書の仕様変更を行う必要があり、またでは個人番号カードの仕様を変更する必要がある。よって、これらの方式は、技術的には実現可能と言えるが、現行制度では両方式ともに認められておらず、実現のためには制度変更が必要になる。

(イ) サーバ連携方式

サーバ連携方式は、HPKI署名や利用者証明の機能をインターネット上の連携用サーバに持たせ、JPKIは連携用サーバへのアクセスのために利用し、HPKIの署名や利用者証明は連携用サーバが提供するASPとして実現する方式である。この方式は、総務省において検討が進められているJPKIを利用した電子委任状を実現する仕組み[1]を応用し、医療従事者資格を一つの属性として認証するシステムを構築することで実現できると考

えられる。具体的な実現モデルの例を図2に示す。ここではある電子文書へHPKI署名を付与する場面を想定する。医療従事者は、電子文書の作成が完了した段階で、自身のJPKI利用者証明を利用してHPKI用連携サーバにアクセスし、本人であることが確認できた場合には、HPKI連携サーバが提供するASPによって電子文書に署名が付与される。

この仕組みの実現性について考えると、現在のHPKIカードは、オフライン時における医療従事者の身分・資格証明書としての利用が想定されていることや、本方式のベースとなるリモート署名の実施基準等の検討が未了であることから、短期的な実用化検討の対象からは除外するが、電子委任状に関する新たな法整備の動きもあること等の理由により、引き続きその実現可能性について検討を行うべきと考える。

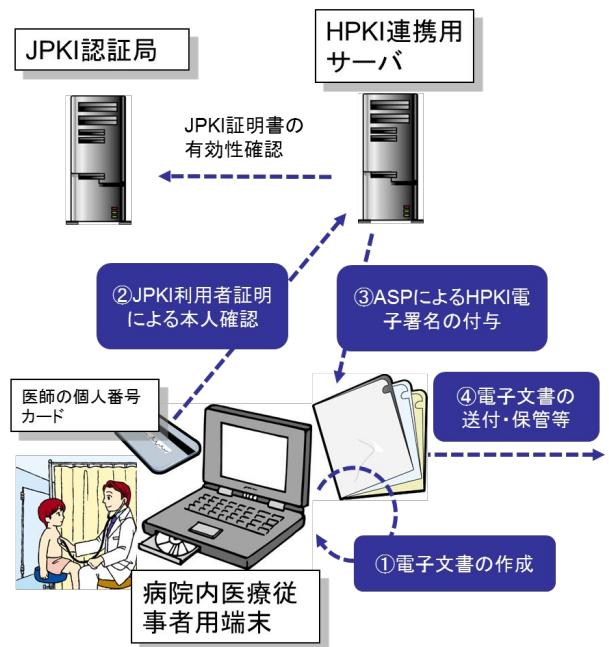


図2. サーバ連携方式における電子署名付与のフロー

(ウ) JPKI + 検証代行方式

この「JPKI + 検証代行方式」は、医師の電

子署名もしくは利用者証明には JPKI の公開鍵・秘密鍵を利用するが、電子証明書の検証、電子署名の検証、医療従事者の資格確認には、JPKI の電子証明書を直接利用するのではなく、HPKI 認証局が処理を代行する手法である。この仕組みを実現するにあたり、HPKI 認証局は、従来の HPKI 証明書及び公開鍵・秘密鍵ペアの発行や HPKI 証明書の有効性確認を行う代わりに、医療従事者の JPKI 証明書の有効性の確認、医療従事者が作成した電子署名の検証、医療従事者の医療従事者資格を確認し回答する機能を具備するものと想定する（図 3、図 4）。また、医療従事者と JPKI ユーザーとを対応付けさせるための ID 連携情報としては、例えば JPKI 証明書のシリアル番号を利用する方法が考えられる。ただし、この情報連携のための個人識別情報は、プライバシーや法的な取り扱い等を考慮して慎重に検討する必要がある。

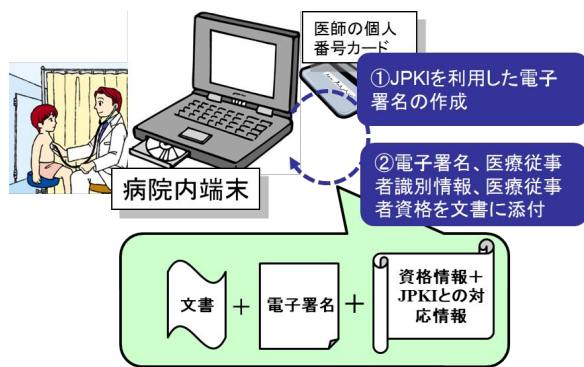


図 3 . 「JPKI + 検証代行方式」における署名作成の流れ

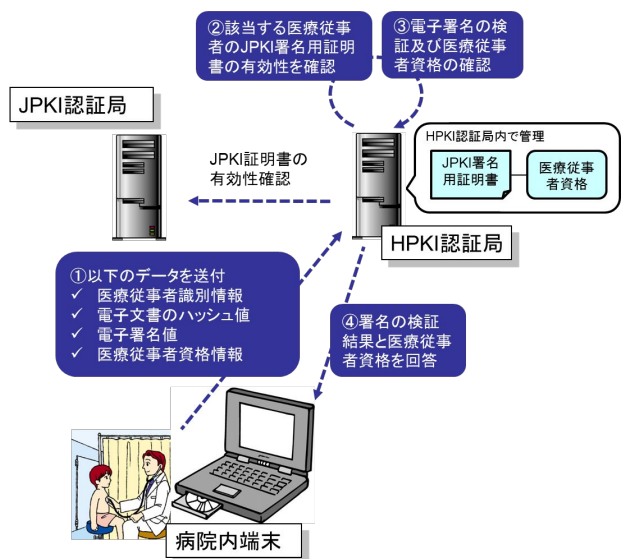


図 4 . 「JPKI + 検証代行方式」における署名検証の流れ

図 5 に、「JPKI + 検証代行方式」を利用したサービスの具体例として、電子紹介状における電子署名付与及び検証の実現例を示す。この処理の流れは以下の通りである。

【事前準備】

HPKI 利用登録時に、医療従事者の JPKI 署名用証明書を HPKI 認証局に送付し、医療従事者資格とあわせて登録する。

JPKI を利用可能な個人番号カードで電子署名を付与した電子紹介状を作成する。電子紹介状には、電子署名、資格情報、医療従事者識別情報が記載された文書を添付する。

媒体を紹介先病院に提出する。

受け取った医療機関は、医療従事者識別情報、電子紹介状本文のハッシュ値、電子署名、医療従事者資格情報を HPKI 認証局に送付し、署名検証と医療従事者資格の確認を依頼する。

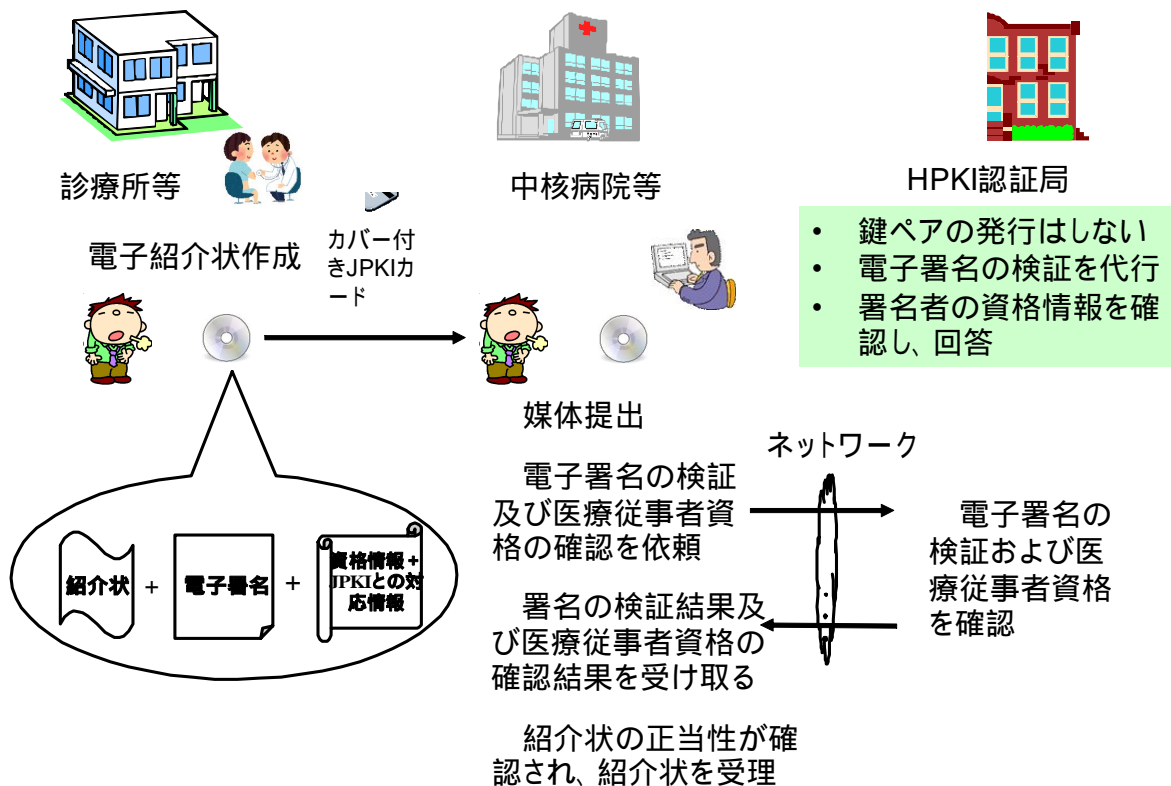


図5. 電子紹介状における「JPKE + 検証代行方式」を利用したサービス実現例

HPKE 認証局は、該当する医療従事者の JPKE 署名用証明書の有効性を確認し、有効性が確認できた場合には、JPKE 署名用証明書の公開鍵を利用して電子署名の検証を行う。また、送付された医療従事者資格と登録されている医療従事者資格が一致されていることを確認する。これら結果を医療機関に送付する。

署名の検証結果と医療従事者資格の確認結果を受け取る。

紹介状の正当性が確認され、紹介状が受理される。

この「JPKE + 資格情報提供方式」は、新たに HPKE カードを発行せず、またすでに利用されている個人番号カードや JPKE にも手を加える必要がないため、導入コストや運用コ

ストの大幅な削減が期待できる。また、現在の JPKE 署名用電子証明書には所有者の住所が記載されているが、この方式では HPKE 認証局以外に署名用証明書を受け渡すことはないため、医療従事者のプライバシーにも配慮された仕組みといえる。ただし、個人番号カードにはマイナンバーが記載されていることから、マイナンバー部分を秘匿するためのカバーをつけるなどの配慮が必要と思われる。

(2) HPKE カードの新規登録時における本人確認

現在行われている HPKE カードの新規発行においては、発行手続きが複雑であることや、カード発行のための環境整備に膨大な費用や時間を要するなど、これから HPKE カードの普及を進めるには解決すべき課題が存在

する。これに対し個人番号カード及び JPKI は、2017 年 5 月時点ですでに一千万枚以上の交付が行われており、社会インフラとしての確立が進みつつある。また JPKI は住基ネットと連動して管理されるため、JPKI とその本人との対応は極めて高い信頼性を有する。よって個人番号カード及び JPKI を HPKI の新規発行時の本人確認手段として利用すれば、HPKI 用カード発行時の手間や発行・管理に用いるシステムの設備投資が削減できるとともに、HPKI の利用時に必須となる医療従事者の本人性および実在性の確認を、極めて高い信頼性で実現できるようになると考えられる。ここでは、HPKI の新規発行を行う具体的な手順について検討を行う。

現在、医師会は HPKI カードの発行を以下のように行っている。まず、申請者の医師は、HPKI 発行機関である医師会へ、以下の書類を郵送することで申請を行う。

- 発行申請書
- 医師免許証のコピー
- 住民票の写し
- 身分証のコピー

カード発行完了後、発行完了通知書を申請者である医師へ送付する。医師は都道府県・郡市区医師会に以下の書類を持参して出向き、対面での本人確認及び医師資格の確認が行われる。

- 発行完了通知書
- 医師免許証（原本）または、医師免許証のコピーに実印押印及び印鑑登録証明書（発行から 3 ヶ月以内）
- 身分証（原本）

この確認の後、HPKI カードが渡される。

このように、従来は、医師免許証による医籍確認と、住民票による個人（自然人）の確認の両方を書面により行っている。これに対

して、個人認証は JPKI を利用し、医籍情報という属性の確認を別途行う仕組みを考える。

HPKI カードの発行を申請する医師等は、Web 等から医籍登録番号と医籍登録年月日、本籍地を含む申請情報を入力し、JPKI の電子署名機能を用いて電子署名を作成したのち、申請情報とその電子署名を HPKI 発行機関にオンラインで提出する。HPKI 発行機関は、申請を行った医師の JPKI による電子署名の検証及び署名用電子証明書の検証・有効性確認を行い、申請者の登録を行う。JPKI 署名用電子証明書には、申請を行った医師の基本 4 情報（氏名、住所、性別、生年月日）が記載されているため、これら情報を申請書の情報と照合し、正しければ署名用電子証明書（電子証明書発行番号）と共に HPKI 発行管理データベースに登録し、HPKI 証明書及びカードを発行する。また、署名検証者は、公的個人認証法第 18 条第 3 項により、署名用電子証明書の発行番号を J-LIS に通知することで、署名利用者に係る利用者証明用証明書の発行番号を受け取ることができるため、医師会等が申込者に対して HPKI カードの発行状況等を Web 経由で提供することも可能となる。カード発行完了後には、書面での申請時と同様に、医師は都道府県・郡市区医師会に出向くことになるが、その際に所持するものは、

- 発行完了通知書
- 医師免許証（原本）または、医師免許証のコピーに実印押印及び印鑑登録証明書（発行から 3 ヶ月以内）
- 個人番号カード

となり、窓口において、医師資格という属性と自然人としての情報を確実に紐づけることとなる。

表1. 失効理由コードの組み合わせによる失効原因の推測

失効原因	電子署名用証明書失効理由コード	電子利用者証明用証明書失効理由コード
異動	affiliationChanged	失効しない
住民票からの削除	affiliationChanged	affiliationChanged
カード紛失	certificateHold	certificateHold
更新	Superseded	Superseded
カード廃止	cessationOfOperation	cessationOfOperation

ここで、医師等が転居した場合には、住所が記載されている署名用電子証明書が失効するが、HPKI 発行機関は失効情報の提供をその失効理由コードとともに受けることができるため、表1に示すように失効理由コードの組み合わせにより医師等の基本4情報などに変更があったことを24時間以内に行うことができる。J-LIS が民間企業に変更後の4情報を提供することはできないため、HPKI 発行機関は変更後の新たな情報を知ることができないが、一般的に転居後1年以内であれば郵便は転送されることや、勤務先等の情報を合わせて管理することができれば、様々な手段を利用して修正情報の取得が可能となる。利用者証明用証明書には、個人を容易に特定できる情報は記載されておらず、転居などでは失効しないため、オンラインサービ

ス利用時に情報の変更届を提出させることも可能である。

また、証明書の更新等により発行番号が変更された場合においても、新旧の発行番号の対応情報が J-LIS から提供されることとなっており、一度 JPKI による利用登録を行えば、5年ごとの証明書更新や10年ごとのマイナンバーカードの更新などが生じた場合でも、医師等は特別の手続きなしに継続して HPKI カードの継続利用が可能となる。

(3) 提案技術の応用

(ア) 受診記録を利用した医療情報連携

2018年からの段階的な導入が予定されているオンライン保険資格確認[2]では、PIN入力不要な JPKI の利用者証明 (PIN 無し認証) の利用が想定されているが、この PIN 無し認証に基づくオンライン保険資格確認では、保険資格確認 PF と個人番号カードの両者がデジタル署名を行っており、このトランザクションデータを利用することで、証跡性を持った受診記録を生成することが可能となる。我々はこのトランザクションデータを利用した受診記録生成手法およびこの受診履歴を利用した医療情報連携の仕組みを提案している[3]。この仕組みにおける医療情報参照の際には、医師の HPKI 署名を付した参照要求を行っており、医師の有資格者のみが医療情報を参照できる仕組みとなっている。

提案手法における受診記録生成の流れを
図6に示す。受診に来た患者は、自身の個人
番号カードを受付端末に提示し、PIN 無し認
証によってオンライン保険資格確認を行う。
その際に生成するトランザクションデータ
に時間情報や病院の情報などを加えて受診

記録データを生成し、受診履歴管理サービ
スに送付する。この手法で生成する受診記録デ
ータは、「いつ・どこ・だれ」の情報のみと
する。またこの登録処理は、オンライン保険
資格確認を行う端末上ですべてを完了する
ため、病院内情報システムとのやり取りは生

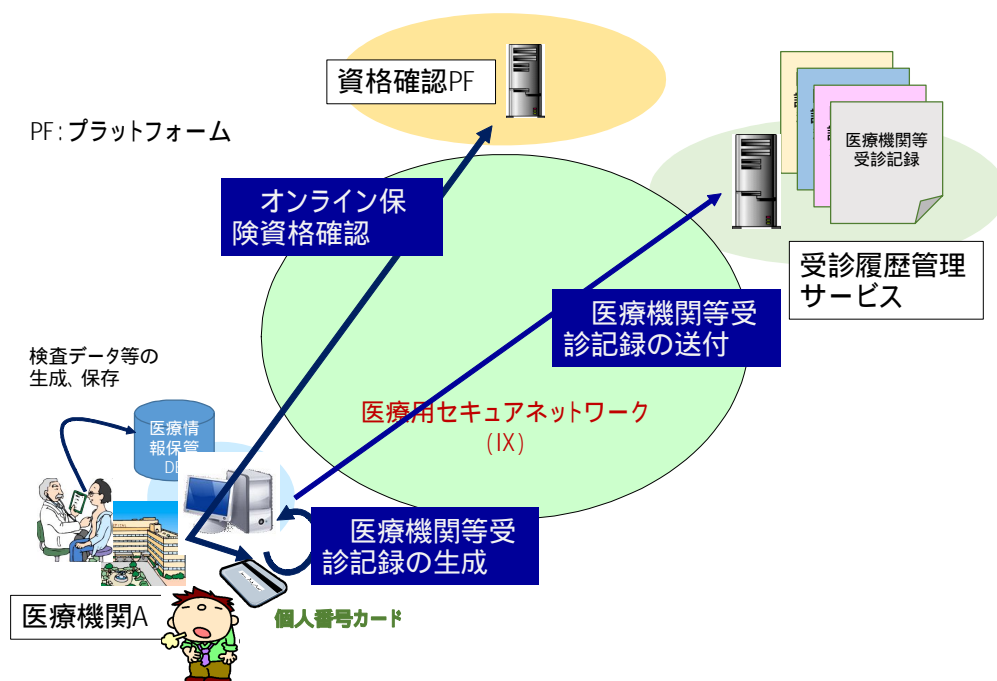


図6. オンライン保険資格確認を応用した受診記録登録処理フロー

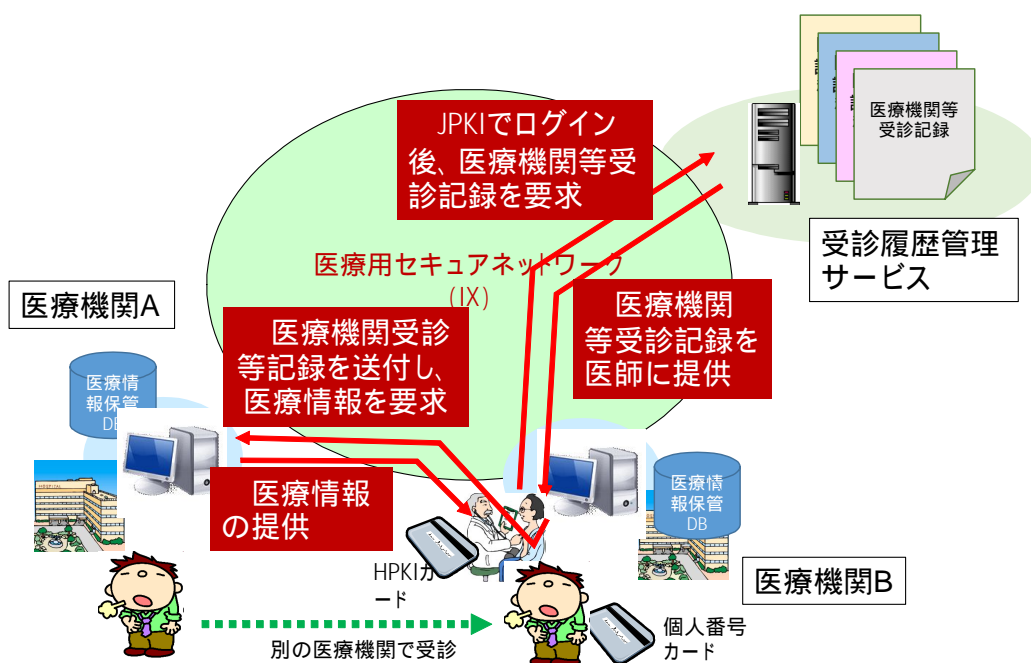


図7. 受診記録を利用した医療情報参照フロー

しない。なお、医療機関 A には、他の医療機関へ医療データ提供を可能とするためのデータベースが設置されているものとし、受診の際に生じた検査データ等の医療情報は、この医療情報連携用のデータベースに保存される。

この受診記録を利用した医療情報参照の流れは図 7 のようになる。この図では、医療機関 A で受診したある患者が、別の日に医療機関 B へ訪問し、医療機関 A で生成された医療データを参照しながら診察を受ける場面を想定する。なお、医療機関 B は、医療機関 A とは異なる地域医療圏に存在し、医療機関 A の医療データ提供に対する包括同意の対象外とする。まず患者は、医療機関 B の病院内端末から受診履歴管理サービスへ JPKI 利用者証明（ここでは PIN を入力）を利用してログインを行い、受診履歴管理サービスから患者の受診記録データを取得する。医療機関 B の医師は、患者の受診記録を見ながら、診察に必要な医療情報を保有していると思われる医療機関を選定し（ここでは医療機関 A）、その医療機関に対して医療情報提供を要求する。その際、医師の HPKI カードで、要求コードに署名を付す。要求コードを受け取った医療機関 A では、医師の HPKI カードの有効性を確認し、要求された医療情報を保有していた場合には、その情報を医療機関 B に提供する。

この医療機関 B の端末では、JPKI と HPKI の両方が扱える端末が必要になるが、このようなケースでは、(1)で提案した方式を適用することで、一つの端末での環境構築が可能となり、コストやスペースの削減が期待できる。

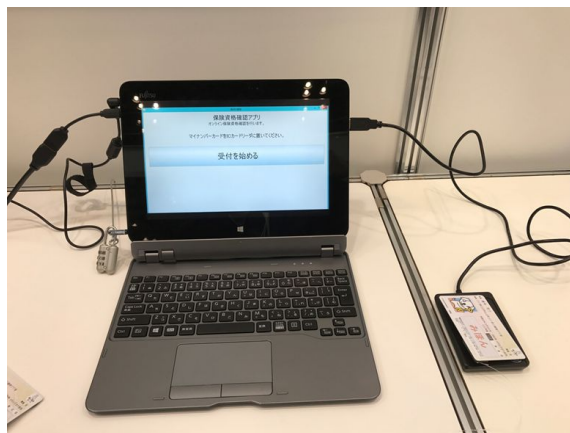


図 8 . 簡易デモシステム

ここで、受診記録生成の際の特定機関認証利用には、J-LIS から特定機関認証用公開鍵証明書及び秘密鍵の発行を受け、これらを用いて自らが特定機関認証の利用を認められた機関であることを電子的に証明する必要があるが、本研究ではそのために必要な機能を医療機関等の窓口を設置する資格確認用端末に実装する簡易デモシステムを開発した（図 8）。この簡易デモシステムでは、特定機関認証用秘密鍵を端末側に格納し、端末内で特定機関認証を行うとともに、受診記録の生成を行っている。

(イ) 電子処方箋及び薬歴管理

現在厚労省を中心に検討が進められている電子処方箋の運用モデルでは、医師が HPKI カードを利用して電子処方箋に電子署名を付与することが想定されている。よって電子処方箋の普及のためには、HPKI 電子署名を利用するための環境整備が極めて重要であり、本研究成果が大きく貢献しうる応用例といえる。

一方、現在の日本の医療分野では、重複処方方や残薬の問題が指摘されているが、これらの問題に対し、薬剤師の介入等により削減可能な薬剤費は、推計 100～6500 億円程度と報告されている[4]。重複処方の防止や残

薬を解消するためには、過去の調剤歴や自宅にある残薬の情報を把握した上で、適正に処方を行う仕組みが必要である。これに対し、電子処方箋が普及した将来を考えると、少なくとも処方情報及び調剤情報については電子的な情報が流通することになるため、処方情報、調剤情報を管理する仕組みについては整備しやすい環境になると言える。この状況を踏まえ本研究では、電子処方箋の運用から得られる情報を基に調剤歴や残薬を適切に管理する仕組みについて検討を行った。

今回の検討では、医療機関、診療所において処方情報、また調剤薬局において調剤情報の作成が行なわれ、これら情報は医療等分野専用ネットワーク(Inter-network Exchange:IX)を介して情報管理サーバへ蓄積される仕組みが存在する環境を想定する。これら情報は現在検討されている電子処方箋の運用モデルの中で蓄積が可能な情報であると考えられるが、残薬情報については、入力する仕組みは検討されていない。そこで残薬情報については在宅医療患者を対象を絞り、訪問看護師等が残薬情報を登録するシステムを検討する(図9)。訪問看護師は在宅患者の服薬状況を把握しているため、訪問看護師が情報管理サーバへ情報を登録する仕組みが実現できれば、在宅医療患者の残薬管理は実現可能と考えられる。

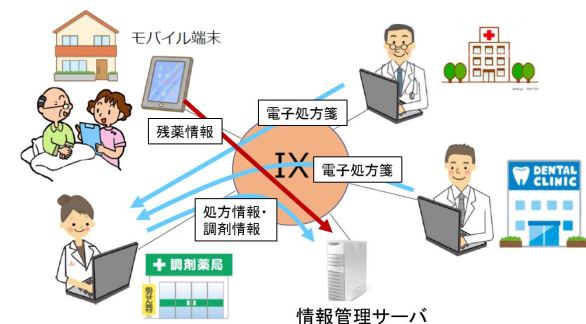


図9. 想定する薬歴管理の概念図

この管理情報システムを利活用する具体例を以下に示す。調剤時において、薬剤師は電子処方箋の監査、調剤、服薬指導、及び電子調剤情報の作成を行うが、電子処方箋監査では、薬剤師は患者同意を得た上で、情報管理サーバに蓄積された電子調剤情報、電子残薬情報を参照し、重複処方、残薬の有無を確認した上で、必要に応じて疑義照会を行う。調剤情報には、先発薬から後発薬への変更、服薬指導の内容を含めることで、次の診察時の医師等の情報収集の支援、また適正処方の支援につながると考えられる。

この仕組みの実現のためには、訪問看護師が情報管理サーバへアクセスするためのアクセス管理技術や、患者の自宅から医療等分野専用ネットワークへアクセスするためのネットワーク接続技術が必要になるが、いずれも訪問看護師用 HPKI による医療従事者資格の確認によって対応可能と考えられる。しかし現在の HPKI は、医師、歯科医師、薬剤師に対して発行されているが、今後は看護師に対しても HPKI が発行されることが望まれる。

(4) 実用化へ向けての課題

上記の検討を踏まえ、今後提案技術を実用化するための課題を整理する。

(ア) 端末に関する課題

HPKI や JPKI を利用するためには、IC カードを扱うことが可能な端末が必要になるが、現在の医療機関では IC カードを利用した環境整備は十分に進んでおらず、その環境整備は急務である。この端末については、省スペースやコスト面でのメリットを考えると、スマートフォン・タブレット端末での実装が望ま

しい。これに対し、(一財)ニューメディア開発協会が開発した医療用保険資格端末は、NFCによる非接触カード読み取りと、セキュアゲートウェイによる安全な鍵管理を実現する仕組みが実装されており、この端末を利用することで、JPKIやHPKIを安全かつ簡便に利用する環境を、安価に整備することが可能になると考えられる。

(イ) 医療等分野専用ネットワークに関する課題

HPKIの普及が進むと、在宅医療など医療機関以外での情報提供や参照の必要性が出てくるため、医療機関以外から無線のモバイル端末等を用いて医療等分野専用ネットワークへ接続することが想定される。そのため、IKE/IPsec等を用いて、無線回線の十分な安全性を確保する技術開発が必要になる。

(ウ) 医師・薬剤師以外のHPKIに関する課題
前述の通り、現在のHPKIは、医師、歯科医師、薬剤師に発行されているが、看護師、技師、療法士、事務員等、医療情報を取り扱うすべての医療従事者への普及を検討する必要がある。

D. 結論

平成28年度は、HPKIおよびJPKIの制度および技術的な位置付けを再整理した上で、個人番号カードおよびJPKIを利用した医療従事者資格の確認手法について検討を行った。その結果、「個人番号カード搭載方式」、「サーバ連方式」、「JPKI+検証代行方式」の3つの方式について実現例を示した。特に「JPKI+検証代行方式」は、個人番号カードやJPKIに手を加える必要がないため、導入コストや運用コストの削減が可能になると期

待され、また、現在のJPKI署名用電子証明書に所有者の住所が記載されている課題に対し、この方式ではHPKI認証局以外に署名用証明書を受け渡すことはないため、医療従事者のプライバシー保護の点でも有利である。一方、HPKIカードの新規発行申請時における本人確認にJPKIの利用者証明を利用する手法についても検討を行い、この仕組みによってHPKI用カード発行時の手間や発行・管理に用いるシステムの設備投資が削減できるとともに、極めて高い信頼性で医療従事者の本人性および実在性を確認できることを示した。また提案技術の応用検討として、受診記録を利用した医療情報連携や、薬歴管理への応用例を検討した。これらの応用例ではHPKIの利用が必須であるため、本研究の成果によってHPKIが簡便かつ安全に利用できるようになれば、このような応用サービスの実現が加速するものと期待される。

E. 健康危険情報

該当なし

F. 参考文献

- [1] 個人番号カード・公的個人認証サービス等の利活用推進の在り方に関する懇談会、属性認証検討SWG資料,
http://www.soumu.go.jp/main_content/000398182.pdf.
- [2] 小尾高史,第5回社会情報流基盤研究センターシンポジウム講演資料,
http://assist.ssr.titech.ac.jp/wp-content/uploads/text27_6.pdf.
- [3] 鈴木裕之,第7回社会情報流基盤研究センターシンポジウム,
<http://assist.ssr.titech.ac.jp/wp-content/uploads/e9a3be97c8924c08cd7ab17de4742cc2.pdf>.

[4] 益山光一, 医療保険財政への残葉の影響と その解消方策に関する研究 (中間報告), 平成 27 年度厚生労働科学特別研究 .

G . 研究発表

- 福田賢一, 小尾高史, 永田和之, 鈴木裕之, 平良奈緒子, 大山永昭, “医療保険の資格確認における公的個人認証サービスの活用に関する考察”, ライフインテリジェンスとオフィス情報システム研究会 (LOIS), 信学技報, Vol. 116, No. 23, pp. 1-6 (2016).
- 永田和之, 李中淳, 福田賢一, 岩丸良明, 庭野栄一, 谷内田益義, 平良奈緒子, 鈴木裕之, 小尾高史, 大山永昭, “ブロックチェーンにおける本人性確認の方法に関する考察”, 第 170 回マルチメディア通信と分散処理・第 76 回コンピュータセキュリティ合同研究発表会, 研究報告マルチメディア通信と分散処理 (DPS), 情報処理学会, 2017-DPS-170, 19, pp.1-6 (2017).
- 山根 拓人, 鈴木裕之, 大山永昭, 小尾高史, “トラステッド実行環境を用いた公的個人認証サービス利用時の 安全性向上に関する研究”, 電子情報通信学会総合大会, D-9-31, p.121 (2017).
- 下條拓未, 小尾高史, 大山永昭, 鈴木裕之, “個人番号カードを用いた病院の初診受付において必要な基本情報取得システムの提案”, 電子情報通信学会総合大会学生ポスターセッション, ISS-SP-219, p.219 (2017).
- 平良奈緒子, 小尾高史, 福田賢一, 岩丸良明, 鈴木裕之, 大山永昭, “医療保険のオンライン資格確認を活用した個人医療情報管理の実現手法について”, 第 37 回医療情報学会連合大会, 2-H-3-OP11-4 (2017).
- 福田賢一, 小尾高史, 岩丸良明, 鈴木裕之, 平良奈緒子, 中嶋秀樹, 長澤潔, 石原聰, 大山永昭, “医療保険オンライン資格確認及び医療機関受診記録生成システムの開発”, 第 37 回医療情報学会連合大会, 2-K-1-HD2-2 (2017).
- 小尾高史, “公的個人認証サービスの利用拡大に向けた取り組み”, 住民行政の窓, Vol.452, pp. 4-15 (2018).
- 大山永昭, “医療等分野におけるマイナンバーカードの利活用について”, 住民行政の窓, Vol.453, pp. 4-15 (2018).
- 應治沙織, 鈴木裕之, 小尾高史, 大山永昭, “健康保険の資格確認手順を用いた受診履歴データ作成・利活用に関する研究”, ライフインテリジェンスとオフィス情報システム研究会 (LOIS), (2018).
- 中島綾音, 平良奈緒子, 鈴木裕之, 小尾高史, 大山永昭, “健診データを含めた個人健康管理システムの実現方法”, メディカルイメージング連合フォーラム, 信学技報, Vol. 117, No. 518, pp. 63-64 (2018).
- 鈴木亮平, 鈴木裕之, 大山永昭, 小尾高史, “公的個人認証サービスを用いたオンラインバンキングの安全性向上に関する研究”, 電子情報通信学会総合大会, D-9-15, p.104 (2018).

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
福田賢一, 小尾高史, 永田和之, 鈴木裕之, 平良奈緒子, 大山永昭	医療保険の資格確認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. 116, No. 23	1-6	2016
Takashi Obi	Japan e-ID Card go to the next Stage	World e-ID and Cybersecurity 2016			2016
永田和之, 李中淳, 福田賢一, 岩丸良明, 庭野栄一, 谷内田益義, 平良奈緒子, 鈴木裕之, 小尾高史, 大山永昭	ブロックチェーンにおける本人性確認の方法に関する考察	第170回マルチメディア通信と分散処理・第76回コンピュータセキュリティ合同研究発表会	2017-DPS-170, 19	1-6	2017
山根拓人, 鈴木裕之, 大山永昭, 小尾高史	トラステッド実行環境を用いた公的個人認証サービス利用時の安全性向上に関する研究	電子情報通信学会総合大会講演論文集	D-9-31	121	2017
下條拓未, 小尾高史, 大山永昭, 鈴木裕之	個人番号カードを用いた病院の初診受付において必要な基本情報取得システムの提案	電子情報通信学会総合大会学生ポスターセッション論文集	ISS-SP-219	219	2017
平良奈緒子, 小尾高史, 福田賢一, 岩丸良明, 鈴木裕之, 大山永昭	医療保険のオンライン資格確認を活用した個人医療情報管理の実現手法について	第37回医療情報学会連合大会講演論文集	2-H-3-OP1-4		2017
福田賢一, 小尾高史, 岩丸良明, 鈴木裕之, 平良奈緒子, 中嶋秀樹, 長澤潔, 石原聰, 大山永昭	医療保険オンライン資格確認及び医療機関受診記録生成システムの開発	第37回医療情報学会連合大会講演論文集	2-K-1-HD2-2		2017

小尾高史	公的個人認証サービスの利用拡大に向けた取り組み	住民行政の窓	Vol.452	4-15	2018
大山永昭	医療等分野におけるマイナンバーカードの活用について	住民行政の窓	Vol.453	4-15	2018
中島綾音, 平良奈緒子, 鈴木裕之, 小尾高史, 大山永昭	健診データを含めた個人健康管理システムの実現方法	信学技報	Vol. 117, No. 518	63-64	2018
鈴木亮平, 鈴木裕之, 大山永昭, 小尾高史	公的個人認証サービスを用いたオンラインバンキングの安全性向上に関する研究	2017年電子情報通信学会総合大会講演論文集	D-9-15	104	2018