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）
総括研究報告書

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について検討した結果、技術的には実現可能なモデルを示すことはできたが、現状の制度としては認められておらず、短期的な実現は難しいことを明らかにした。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ことは現行の制度でも可能であり、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。

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　　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。

① 利用する IC カード
- 個人番号カード or 別のカード

② 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、①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」と 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」が考えられる。また別カードを利用する方式としては、現行の HPKI カードの応用が妥当であると考えられるが、HPKI カードにはもともと医療従事者医療資格機能が実装されているため、資格確認機能を ASP で提供する方式は想定せず、HPKI カードの中に JPKI の機能を搭載する「HPKI カード搭載方式」を検討する。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、そのための技術として、属性証明書を利用する仕組みを検討する。

研究方法としては、平成 28 年度は、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の仕組みへの適用を検討し、その効果や実現可能性について検討を行う。

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。

① JPKI 証明書に医療従事者属性を確認できる機能を加える
② 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。

①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。②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 発行を行う窓口に赴き、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。

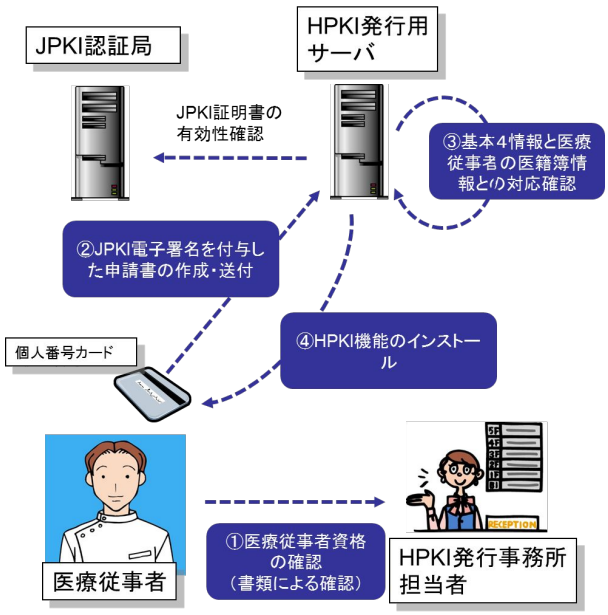

図 1. 個人番号カード搭載方式における HPKI 新規登録のフロー

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、①では JPKI の証明書の仕様変更を行う必要

があり、また②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。

なお、HPKI カードに JPKI 機能を搭載する「HPKI カード搭載方式」については、HPKI カードを先に発行した後、後日 JPKI 機能を追加することになるが、先に行うべき HPKI カードの発行に現時点で多くの課題を有していることや、個人番号カードの交付がすでに開始され、発行枚数が順調に増えていることを鑑みると、「個人番号カード搭載方式」が現実的な実現手段と言えるため、今回の検討では個人番号カード搭載方式のみ実現モデルを示した。

(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。

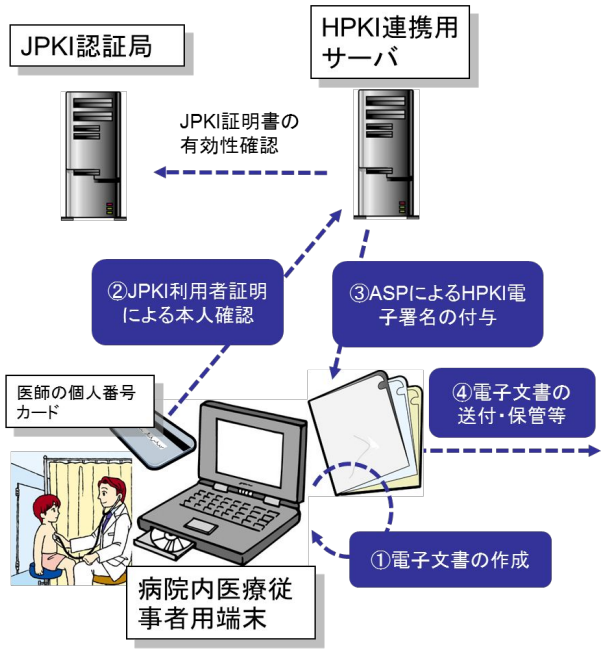

図 2. サーバ連携方式における電子署名付与のフロー

(2) HPKI 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 HPKI 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 HPKI 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ﾄﾞ
異動	affiliationChanged	失効しない
住民票からの消除	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 時間以内に知ることができる。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はできないが、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

ここでは、HPKI 署名や HPKI 利用者証明を利用するユースケースについて議論する。HPKI の利用が想定されている代表的なサービスとしては、電子的診療情報提供書や電子処方せんが挙げられるが、提案技術が導入されることで、HPKI カードの発行手続きが単純化することや、発行や運用にかかる費用が抑えられるといった利点を享受できることから、提案技術はこれらサービスの普及に大きく貢献できると考えられる。

一方、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 3 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じない。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

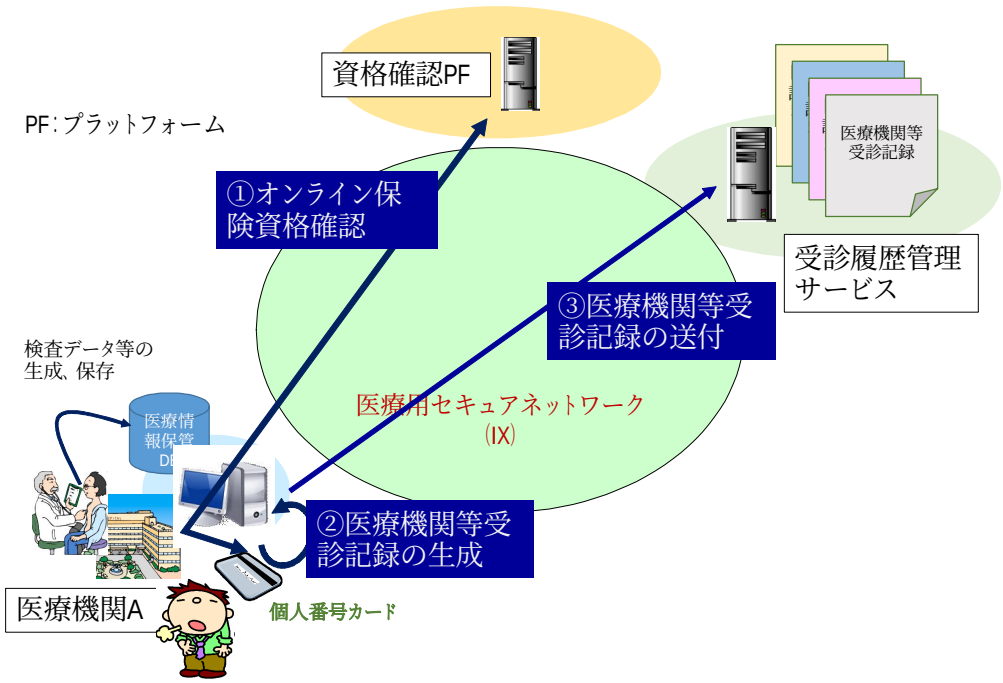

図 3. オンライン保険資格確認を応用した受診記録登録処理フロー

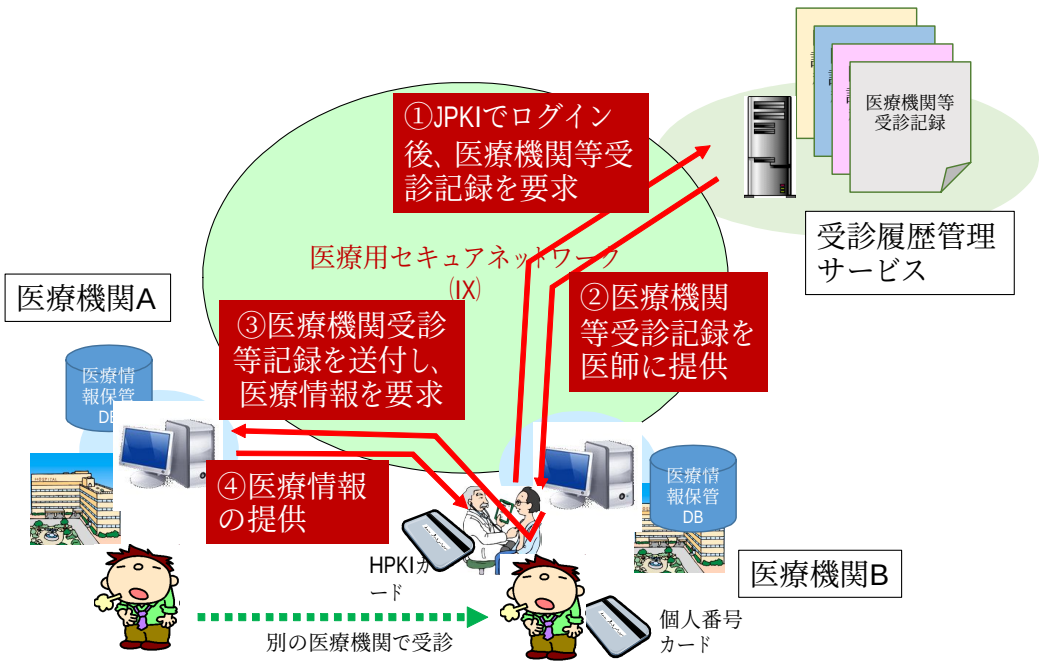

図 4. 受診記録を利用した医療情報参照フロー

れる。

この受診記録を利用した医療情報参照の流れは図 4 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「個人番号カード搭載方式」及び「サーバ連携方式」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。

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及びサーバ連方式の2つの手法について実現例を示し、これら方式は、いずれも技術的には実現可能であると考えられるが、現状の制度等の問題により、短期的な実現は難しいことを明らかにした。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ことは現行の制度でも可能であり、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。

平成29年度は、医療情報連携など具体的なユースケースを想定した総務省の実証実験等を通して、予測される提案手法の効果を検証し、改善すべき技術課題を明らかにし、具体的な実現指針を提言としてまとめる予定である。

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://asist.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://asist.ssr.titech.ac.jp/wp-content/uploads/e9a3be97c8924c08cd7ab17de4742cc2.pdf.

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).