

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

公的個人認証サービスを活用した医療従事者認証手法に関する研究

公的個人認証サービスを医療従事者認証用の本人確認に利用する際の技術的検討

研究分担者 小尾高史 科学技術創成研究院 准教授

研究要旨 平成28年1月よりマイナンバーカード(個人番号カード)の交付が開始され、交付枚数の総計はすでに1100万件を超えている。マイナンバーカードに搭載された新たな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は極めて信頼性が高く、HPKI発行・運用時の本人確認手段として利用することで、HPKIを利用する医療従事者本人の存在の信頼性が高まるだけでなく、将来的なHPKIの発行・運用費用等を大幅に削減できる可能性がある。本研究では、JPKI利用に関する制度・技術を調査し、JPKIとHPKIを連携させるための仕組みについて検討を行った。

A. 研究目的

平成28年1月よりマイナンバーカード(個人番号カード)の交付が開始され、交付枚数の総計はすでに1100万件を超えている。マイナンバーカードに搭載された新たな公的個人認証サービス(JPKI)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られており、特に医療分野での利用が検討されている。

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は極めて信頼性が高く、HPKI発行・運用時の本人確認手段として利用できれば、HPKIを利用する医療従事者本人の存在の信頼性が高まるだけでなく、将来的なHPKIの発行・運用費用等を大幅に削減できる可能性があり、今後のHPKIの普及に大きく貢献するものと期待される。そこで本研究では、JPKIをHPKIのための認証ツール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

マイナンバーカードに搭載されているICチップ内には、交付時に表1に示す4種類のアプリケーションが搭載されており、券面事項入力補助アプリ、券面事項確認アプリの2つについては、雇用主や民間事業者が、従業員等の住所などの情報を入手する際や、個人番号の確認、本人確認などを行う際に利用することが想定されている。券面事項入力補助アプリに記録されている情報には、4情報や個人番号の偽造・改竄(かいざん)の防止のために個人番号カードの発行元である地方公共団体情報システム機構(J-LIS)の電子署名データが付されているため、番号法施行規則第4条に記載されているように、カード内に保存された個人番号等の電子データのオンラインでの提供を受けることにより、個人番号等の取得・確認を行うことも可能である。

また、従来から進められてきたコンビニエンスストアにおける住民票や印鑑登録証明書など

の各種証明書交付サービスについても、マイナンバーカードの発行開始に伴って、現在のところ、400 を超える自治体が参加している。加えて、現在のコンビニ交付サービスでは、戸籍の証明書の交付を受けられるのは、住所地と本籍地が同一の住民に限られているが、平成 28 年 5 月以降は、住所地と本籍地が異なる住民でも本籍地に利用登録申請をすることで、戸籍の証明書の交付を受けられるようになるなど、より一層のサービス充実がなされている。

さらに、マイナンバーカードには、オンライン上で本人を厳格に確認できる手段として公的個人認証サービス（JPKI）が搭載されている。総務省は、民間分野からの希望状況などを考慮しつつ、JPKI を必要とする民間機関を順次“総務大臣が認定するもの”としておりすでに、民間 10 団体が初の総務大臣認定を取得している。

表 1 マイナンバーカードに搭載されたアプリケーション

カード AP 名	記録される情報と利用目的	セキュリティ機能
券面事項 確認アプリ	（アプリ内記録情報） 表面情報：4 情報+顔 画像の画像データ 裏面情報：個人番号の 画像データ （利用目的） 対面時の券面記載情報の改ざん検知 対面における本人確認の証跡として保存	個人番号を利用できる者は、表面、裏面情報を取得時に、照合番号 A（個人番号 12 桁）を入力 個人番号を利用できない者は、表面情報のみを取得であり、総合番号 B（生年月日 6 桁+有効期限西暦部分 4 桁+セキュリティコード 4 桁）を入力して読み出し
券面事項 入力補助ア	（アプリ内記録情報） ① 個人番号及び 4	①については、利用者が設定する暗証番

アプリ	情報並びにその電子署名データ ② 個人番号及びその電子署名データ ③ 4 情報並びにこれらの電子署名データ （利用目的） 個人番号や 4 情報を確認（対面・非対面）し、テキストデータとして利用することが可能	号（4 桁の数字）を入力して読み出し ②については、上記照合番号 A を入力して読み出し ③については、上記照合番号 B を入力して読み出し
JPKI アプリ	電子署名機能	署名時に利用者が設定した暗証番号（6～16 桁の英数字）を入力
	電子利用者証明機能	利用時に利用者が設定した暗証番号（4 桁の数字）を入力
住基アプリ	（アプリ内記録情報） 住民票コード （利用目的） 住基ネット事務のために住民票コードをデータとして利用	情報読み出し時に利用者が設定した暗証番号（4 桁の数字）を入力

ここで、JPKI は住基ネットと連携して管理・運営されている、利用者本人との対応付けは極めて信頼性が高く、HPKI の発行・運用時の本人確認手段として利用すれば、HPKI を利用する医療従事者本人の存在を確実に保証することができると考えられる。また、HPKI の発行機関である一般財団法人医療情報システム開発センター、日本医師会、日本歯科医師会、日本薬剤師会の各民間団体が総務大臣の認定を受け、JPKI の署名検証者及び

利用者証明検証者として認められると、本人確認手段としてのJPKIの利用が認められるだけでなく、医師等のJPKI証明書の発行番号をデータベース化することが認められるため、これら発行番号をもとに住所変更を把握することが可能となる。

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、HPKI発行機関である医師会は、申請者である医師から

- ・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

を郵送で受け付け、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をもって出向き、

- ・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）

対面での本人確認、医師資格の確認が行われたのちに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）
- ・マイナンバーカード

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2 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 2 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 時間以内を知ることができる。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。

C. 研究結果

本研究で提案するシステムを利用することで、HPKI 発行機関は、HPKI 発行時の本人確認を電子的かつ厳格に行うことができるだけでなく、発行後の医師等の異動情報についても把握することが可能になり、従来は医師等や遺族からの届け出がなければ把握が困難だった住所変更や脂肪情報についても迅速に把握することが可能になる。これは、医師等の負担軽減だけでなく、HPKI 自体の信頼性を向上させることにつながる。

D. 考察

HPKI 発行における本人確認については、JPKI を HPKI 発行・運用時の本人確認手段として利用することで、医療従事者本人の存在の信頼性が高可能である。

現在の HPKI は、自然人としての認証に加え、当該自然人を紐づけられた医師などの属性を有することを証明することにあるが、本来は、これらが一つの公開鍵証明書ではなく、論理的に紐づけられた 2 つの仕組みを融合して証明されてもよい。このため、電子認証については、医師の自然人としての認証は JPKI を利用し、属性認証のみを別途行う仕組みを考えることも可能であり、具体的には、JPKI と連携する HPKI 機能を一枚の IC カード内に搭載するカード搭載方式や、HPKI 機能を ASP サーバ等へ実装し、個人番号カードに搭載される 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が考えられる。現状の HPKI カードによる HPKI 運用に加え、これら方式が実現可能かについては、リモート署名の検討、電子委任状の制度化、JPKI 専用 IC カードの検討などを踏まえ、来年度に検討祖薄める必要がある

E. 結論

本年度の研究では、公的個人認証サービスを HPKI を発行する際の本人確認手段として利用する仕組みについて検討を行い、その実現モデルを示した。来年度は、本年成立を予定している“電子委任状の普及の促進に関する法律”の内容と、本年度検討した HPKI 発行時の JPKI 利用法を踏まえ、HPKI を運用・利用する際の JPKI の利用方法について検討を行う。

F. 健康危険情報

特になし

Stage, ” World e-ID and Cybersecurity 2016, Sep.
2016

G. 研究発表

[1] Takashi Obi, “Japan e-ID Card go to the next