

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

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1300万件を超えている。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、確実に本人を確認したうえでの医療情報の連携等が実施できると考えられる。本研究では、広域での医療情報の連携をユースケースとして取り上げ、JPKIとHPKIを連携させるための仕組みについて具体的に検討を行った。

A．研究目的

我が国政府は 2018 年度から医療保険のオンライン資格確認を段階的に運用開始し、2020 年から本格運用を目指すとしており、現在、そのためのシステム開発が進められている。当該システムではマイナンバーカードに搭載された公的個人認証サービス(JPKI)を用いることが想定されているが、オンライン資格確認においては、利用者の利便性等を考慮し、PIN 入力を求めない JPKI の特定機関認証を用いた利用者証明が利用される。この仕組みの特徴はマイナンバーカードに搭載された JPKI のアプリケーションプログラムと特定機関認証を行うサーバがそれぞれデジタル署名を施すことにあり、この情報を有効に利用すれば、だれが、いつ、どの医療機関において診察を受けたかの情報を証跡として残すことが可能である。ここで、日本再興戦略 2016 には、「2018 年度までを目標とした地域医療情報連携ネットワークの全国各地へ普及に向けて」とあり、個々の医療圏に閉じず医療圏を跨いで医療情報を共有する方向性が示されている。地域医療情報連携ネットワークは、2015 年までに全国 271 箇所が展開されており、これら既存の仕組みを活用しつつ、全国共通の医療サービスを構築していくことが望まれているが、そのための仕組みの検討

が議論されているが、現時点では、患者本人のプライバシーに配慮しつつ、医療情報の連携を図る具体的な方法は明らかになっていない。それに対して、本研究では、医療保険の資格確認により生じる証跡情報を活用して、JPKIとHPKIの連携のもと必要な時に必要な医療情報を患者本人の同意のもとで参照可能とする仕組みを検討し、提案する仕組みを実現する簡易デモシステムを開発した。

B．研究方法

日本の医療保険制度では、海外でもあまり例の無い患者のフリーアクセスが認められている。このため、大病院・中小病院・診療所など医療機関の規模や、内科・外科などの診療科を問わず、いつでも患者が受診したいときに自由に受診先を選ぶことができる。この制度は、様々な面で医療の質の向上に寄与しているとの意見がある一方、患者の医療情報の集積という面においては、非常に困難を伴う状況を作り出しており、生涯の健康管理に必要と考えられている様々な場面を横断した一貫性のある健診情報、治療情報などを含む医療情報データベースの構築が実現できない状況にある(図1)。一方、特定の地域においては、その地域内での医療情報

連携を目的として地域医療情報連携ネットワークが整備されており、生涯にわたるデータベース構築とはいかないまでも、長期にわたる医療情報データベースの構築が進んでおり、2015年までにその数は全国271箇所にものぼっている。このため、このような地域医療情報連携ネットワークをベースとして、全国規模での医療情報連携を可能とする基盤整備を進めていくことが計画されている。

ここで、全国規模での医療情報連携を行うにあたっては、患者のプライバシーに配慮する必要がある、そのためには適切な患者同意による情報連携の仕組みを導入する必要がある。地域医療情報連携ネットワークに患者が参加する際の同意の取り方としては、“地域医療情報連携ネットワークに参加する医療施設すべてが情報連携をすることに一括して同意”、“参加する医療施設ごとに個別に同意する”、“参加する医師ごとに個別に同意する”などがあり、これら同意を事前に取得する方法がとられている。しかしながら、例えば、旅行先で病気にかかり、医療機関を受診する場合などでは、事前に情報を開示する医療機関を指定して同意をとることは困難であり、情報要求時に旅行先の医療機関から医療情報を提供する医療情報連携ネットワーク等へ患者の同意情報を送る必要がある。改正個人情報保護法においても、病歴などは要配慮情報とされ機微性が高い個人情報として明記されたため、事前同意なしに、いわゆるオプトアウトによる情報の取得は原則認められない。

システム的には、医療情報連携ネットワークにおいて患者同意による情報へのアクセス制御を行うには、患者同意情報を含む電子的な認可チケットを用いる必要がある。しかし、一般的に認可チケットの発行には、サーバが必要であり、そのサーバをだれがどのように運用するかは明らかでない。また、患者の同意情報を扱う

ための仕組みは、医療情報システムの相互接続性を推進する国際的なプロジェクトである IHE (Integrating the Healthcare Enterprise) において検討が進められている途上であり、現時点で標準となるべき仕組みが存在していない。

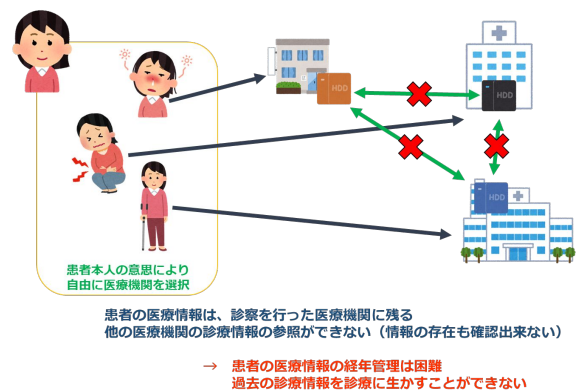


図1 日本の医療制度（フリーアクセスの保証）と医療情報連携の課題

そのため、我々は、医療保険の資格確認により生じる証跡情報を活用することで、必要な時に必要な医療情報を患者本人の同意のもとで参照可能とする仕組みを検討し、できるだけ患者、医療機関双方に負担の無い情報連携の仕組みを構築した。

ここでは、提案する仕組みを、ある患者が情報提供側医療機関において、オンライン保険資格確認を行った上で診察を受け、その受診記録が登録される場面と、別の日に、同じ患者が情報参照側医療機関に来院し、情報提供側医療機関で生成された医療情報を参照しながら診察を受ける場面を例にとり示す。

図2のように、受診記録の登録は、患者が慢性疾患に罹患して自宅近くの医療機関（情報提供側医療機関とする）を受診するところから始まる。患者は医療機関で、医療保険の資格確認端末にマイナンバーカードを挿入すると、まず保険資格確認 PF（以下、PF）は、自らがマイナ

ナンバーカードの発行元である地方公共団体情報システム機構（以下、J-LIS）から認められたものであることを証明する証明書をカードに送付し、カード内の JPKI アプリケーションプログラム（以下、JPKI アプリ）は、この証明書を検証する。検証が成功すると、通信相手先が PF であることを確認するために、乱数を生成して PF に送付し、PF は乱数に PF の秘密鍵を用いてデジタル署名をし、JPKI アプリに返送する。JPKI アプリでの署名の検証が成功すれば PIN の入力を求めない認証処理に進むこととなる。次に PF は、誰のマイナンバーカードが端末に挿入されているかを確認するため、先ほどとは逆に、PF から JPKI アプリに乱数を送る。JPKI アプリは、送られた乱数と PF の機関コードを組み合わせたものを患者の秘密鍵でデジタル署名して PF に返送する。PF は、この署名を検証し、検証に成功すれば、資格確認端末に患者やの保険資格情報を送信する（図 2）。この一連の処理を実行する際にやり取りされるトランザクションデータには、保険資格確認 PF と患者のマイナンバーカードに搭載された JPKI 利用者証明機能の双方のデジタル署名が含まれているため、患者本人が来院したことを保証する証跡とすることが可能であり、トランザクションデータに、医療機関の情報と時間情報を加えて受診記録とする（図 2）ことで、誰が、いつ、どの医療機関を受診したかを確認するための記録として利用可能である。

生成された受診記録は、資格確認端末から直接受信履歴管理サービスへと登録され（図 2）、診察後に地域医療情報連携ネットワークなどが保有する医療情報連携システムに他の医療機関との連携に必要な検査データや画像データなどの医療情報が記録される（図 2）。ここで検討している仕組みのポイントは、医療保険の資格確認を実現するための仕組みや端末をその

まま用いる点であり、受診記録の登録に関しては、病院内の情報システムへの影響はほとんどない。また、受診記録が登録される受信履歴管理サービスの提供機関は、現時点で存在するものではないが、例えば保険資格確認 PF などがサービス提供することも考えられる。

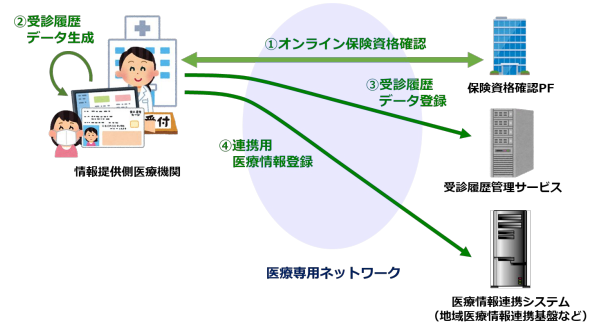


図 2 保険資格確認時の受診記録の登録

次に、患者が旅行先で、慢性疾患の症状が悪化し、旅行先の医療機関を受診することを想定する。旅行先医療機関の医師は、患者に適切な治療を行うにあたり、最近の検査等の状況はどうか、現在どのような治療を受けているのかなどを、確認することが望ましいが、患者の情報が保存されている医療情報連携システムでは、患者が事前に同意した地域内の医療機関や医師との間でのみ情報共有が許可されるよう設定されており、そのままでは、地域外の医療機関である旅行先の医療機関から保存されている情報を参照することはできない。

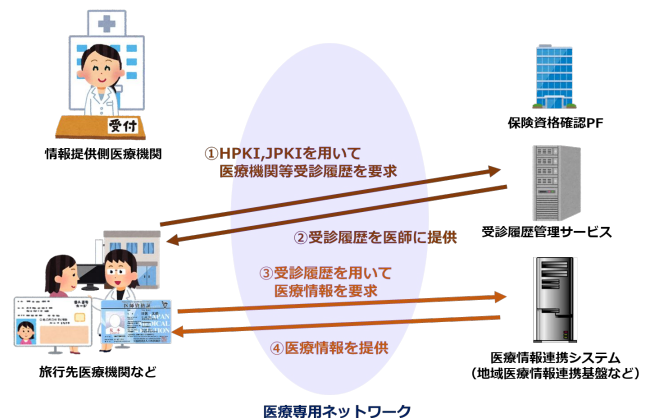


図 3 受診履歴をもとにした医療情報の参照

そこで、患者は自身のマイナンバーカード（JPKI）を利用して、受診履歴管理サービスから、情報を提供してほしい医療機関の受診記録をとりだし医師に提供する（図3）。この際、患者の意思を明確にするためにPIN入力を求める電子利用者証明機能を利用することが望ましいが、医師の資格を電子的に証明するためのICカードであるHPKIカードと特定機関認証を用いた利用者証明を組み合わせることも可能である（図3）。

先に述べたように、受診記録には、「だれ・いつ・どの医療機関」の情報が含まれており、患者の直接的な関与でしか入手できない状況であることから、この記録を、患者の医療情報を参照するための認可チケットとして医療情報連携システムに患者情報の提供を求めることができる（図3）。医療情報連携システムでは、受診記録から、「だれ・いつ・どの医療機関」を特定し、旅行先医療機関の医師等の資格をHPKIにより確認した後、医療情報を提供することとなる（図3）。

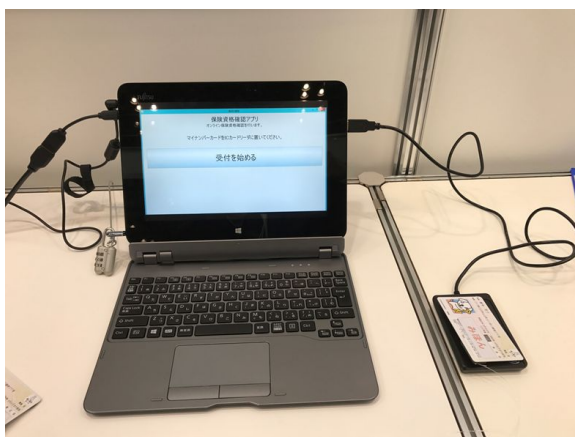


図4 簡易デモシステム

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4）。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。

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、マイナンバーカードを用いた医療保険の資格確認により生じる証跡情報を活用して、必要な時に必要な医療情報を患者本人の同意のもとで参照可能とすることが可能となる。

D．考察

受診記録生成に必要となる特定機関認証用の秘密鍵を医療機関側に移した場合の課題として、秘密鍵の漏洩の危険性が挙げられる。秘密鍵が漏洩した場合には、悪意ある者が正規の医療機関になりすまして患者の認証を行う恐れが生じるので、特定機関認証用秘密鍵のセキュアな管理は重要となる。より、安全性が高く、使いやすいシステムにするために、資格確認用端末もしくは端末と連携して特定機関認証を行う安全性の高い認証用機器において秘密鍵をセキュアに管理する必要がある。また、ここでは受診記録の患者による利用を中心に検討したが、保険者からみると、受診履歴は、被保険者がいつ、どの医療機関を利用したかを確実に把握するための情報として利用することも可能であり、診療報酬の架空請求の防止などを実現するために利用することも期待できる。

E．結論

本年度は、マイナンバーカードを用いた医療保険の資格確認により生じる証跡情報を活用して、

必要な時に必要な医療情報を患者本人の同意のもとで参照可能とする仕組みを検討した。さらに、簡易デモシステムを開発し、オフラインでの医療保険の資格確認の実現可能性を示した。特定機関認証を用いたオフラインでの医療保険の資格確認は、医療保険資格確認システムにおけるネットワーク起因の不安定要素を軽減するものであり、同システムの安定運用に大いに資することが期待される。

F．健康危険情報

特になし

G．研究発表

[1] 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-OP11-4，Nov.2017