別紙２

厚生労働科学研究研究費補助金

医療技術評価総合研究事業

保健医療福祉分野における住基カードを用いた個人・組織・資格認証の在り方に関する研究

平成15年度　総括・分担研究報告書

主任研究者　大山　永昭

平成16（2004）年　4月

別紙３

研究報告書目次

目　　次

厚生労働科学研究費補助金（医療技術評価総合研究事業）
総括研究報告書

保健医療福祉分野における住基カードを用いた個人・組織・資格認証の在り方に関する研究

主任研究者　大山　永昭　東京工業大学フロンティア創造共同研究センター　教授

研究要旨：情報通信技術を利用して保健医療福祉サービスの効率化・高度化を図る際には、患者の個人情報保護、記名押印の電子化等の観点から、医療従事者や患者等の認証を行うことが必須となる。本研究では、今後配布が予定されている住民基本台帳 IC カードや公的個人認証サービスなどと連携して保健医療福祉分野の電子認証を実施する方策を検討し、実現に向けた課題を明らかにした。

分担研究者
公文　敦　（財）医療情報システム開発センター 課長
喜多　紘一　（財）医療情報システム開発センター 審議役
土屋　文人　東京医科歯科大学歯学部付属病院 薬剤部長
八幡　勝也　（財）九州ﾋｭｰﾏﾝﾒﾃﾞｨｱ創造ｾﾝﾀｰ 専任主任研究員
髙橋　紘士　立教大学コミュニティ福祉学部 教授
秋山　昌範　国立国際医療センター情報システム部 部長

A．研究目的

近年の情報基盤整備の進展に伴い、保健医療福祉分野の情報化推進が期待されている。電子的に保健医療福祉情報の流通を行う際には、個人情報の保護を図るための適切な措置を講じることが必要である。このためには、通信回線上の個人データの秘匿やデータを使用する者の正当性を認証することが必須となる。さらに、診療録や処方箋等を電子化する際には、記名押印等の扱いが問題になる。

現在、行政においても電子署名及び認証業務に関する法律（以下、電子署名法）の成立や住民基本台帳法の改正及び住民基本台帳カード（住基カード）の導入、GPKI（政府公開鍵基盤）等の検討が進められている。また、本年度から住基カードの配布や地方自治体による公的個人認証サービスが開始され、これらを保健医療福祉サービスにおいても活用することが期待されている。

本研究では、個人情報保護法、電子署名法、公的個人認証サービス、GPKI 等に関する状況を踏まえた上で、住基カードと連携した保健医療福祉分野における個人・組織・資格認証の実施方策を明らかにすることを目的とする。

これまでの研究で、法定資格を有する医師や薬剤師等の本人確認、保健医療福祉サービス提供機関の認証、提供される情報の真正性確保等を行うためには、医師免許等の資格登録情報に基づく認証の仕組みが必要であることを示し、技術面・運用面に関する問題点の検討を行ってきた。同時に資格名簿の整備等の課題を解決することの必要性及び、資格認証を実施するための具体的な方法を明らかにすることの重要性を示した。本年度は、平成 15 年度より配布が開始された住基カードや、同じく平成 15 年度末にサービスが開始された公的個人認証サービスと連携して、保健医療福祉分野における個人・組織・資格認証を実施する方法及び、それを利用した保健医療福祉サービスの今後の新たな展開を示す。

B．研究方法

工学者及び医師らの研究分担者からなる研究班として、保健、医療、福祉の各分野における情報化推進にあたっている専門家を中心として組織し、委員会を開催して各分野における認証に関する要件と、実現方法の検討を行った。また、IC カードや電子認証に関す

る実験などを行っている諸機関・グループとの情報交換・連携を行い、今後の社会共通基盤となると予想される電子認証の仕組みとの整合を図った。さらに、住基カードの仕様やサービスが開始された公的個人認証サービスの実施形態などに基づいて、住基カードを利用して個人・組織・資格認証を実現するための運用方策を考察し、組織・資格認証機構の具体化を図った。

C．研究結果

(1) 住基カード及び公的個人認証サービスの動向

平成15年8月に改正住基法の2次稼動として、希望者への住基カード配布が開始された。住基カードには個人を特定する住基コードが記録されるため、コードが記録される領域（住基アプリ）へのアクセスには極めて高度なセキュリティが要求されている。そのため、用いられるスマートICカードには、安全性を含めた機能が定義されており、第3者の専門家による評価・確認を行うことになっている。住基カードで特筆すべき機能は電子署名と広域・多目的利用であり、特に広域・多目的利用では、カードの空き領域に如何なるアプリケーションが相乗りしても、住基アプリの安全性に全く影響しないように作られている。また、カードの空き領域は、条例を作ることで利用することが可能であるため、地方自治体において条例を制定すれば、電子行政サービスや健康管理等に用いることも可能であり、住基カードを利用したサービスとしては、「電子署名に係る地方公共団体の認証業務に関する法律」(平成14年12月13日公布)が、平成16年1月29日に施行され、同日より自治体による公的個人認証サービスが開始された。

申請・届出等の行政手続きのオンライン化を実現するにあたっては、第三者による情報の改ざんを防止し、通信相手の正当性を確認するために、電子証明書の発行などを行う高度な個人認証サービスを、全国どこに住んでいる人に対しても安い費用で提供することが必要になる。公的個人認証サービスでは、住民基本台帳に記録されており、サービスを希望するものが、市町村の窓口において電子署名に使用する鍵ペアを自ら作成し、都道府県知事の発行する公開鍵証明書を受け取ることができる。また、署名検証者からの要請に対して、都道府県は発行された公開鍵証明書の失効情報を提供する。これによって、住所・氏名の変更または死亡の事実が生じた場合に証明書は失効する。

このため、この制度を利用すれば、住民基本台帳に記録されている医療従事者は、低廉な価格で電子署名を行うことが可能である。

(2) 保健医療福祉分野における電子認証

ここでは、保健医療分野における個人、資格、組織に関する電子認証の対象について、次のように整理した。

・個人認証

個人認証の対象は、患者としての個人、被保険者などの保健医療福祉サービス受給者としての個人と、保健医療福祉サービス従事者としての個人などが挙げられる。

・資格認証

医師、薬剤師などの国家資格については、法令に規定された行為を行うことに関する認証が必要である。また、その他の資格についても、患者情報の保護や情報の信頼性確保の観点から、情報を扱う者の資格を確認する必要が生じる。

・組織認証

医療機関等の組織を認証するべき例としては、オンラインで診療報酬請求などを行う場合や医療機関同士の連携などが考えられるが、一方、医療機関などの組織に属する医療従事者が患者情報を扱う際に、個人や資格の認証を代行することが現実的である場合が多い。

また、以上の認証対象を考慮し、整理すると電子認証を必要とする場面は以下の通りとなる。

・電子的に記名・押印を行う場合

－診療録への記載

－紹介状（診療情報提供書）の作成
－処方箋の作成
－照射録の作成
－診断書等の作成
・電子的に患者情報の交換・管理を行う場合
－患者紹介を受ける際
－患者の診療録や医療情報へのアクセス時
・電子申請・届出など
－オンラインによる診療報酬請求

(3) 資格認証の実施方策

紹介状や診療録の作成者を、電子署名によって記録する場合には、医師の資格に基づき署名を行ったことを記録する必要が生じる。医師等の法定資格者の認証については、税理士や行政書士などの他の職種でも必要となるため、これらとの整合性を確保して実施手段を構築することが重要であり、他の認証との整合性から、**PKI** をベースとして実施することが望まれる。また、住基カードと公的個人認証サービス用カードは共通の仕様であり、保健医療福祉分野での資格認証においても、このタイプのカードを利用することが有効と考えられる。

ここで、具体的な実施方法としては、①認定認証機関を立ち上げる方法、②属性証明書を用いる方法が考えられる。①②いずれの場合でも、先に述べた「公的個人認証サービス」を利用することで、登録時の本人確認（特定認証業務）の負担を低減できる。

具体的には、資格認証を希望する個人は、公的個人認証サービスの申し込みを行う。まず、居住している市町村の窓口に出向き、秘密鍵を本人のカードに記録する。市町村は、所属する都道府県に公開鍵を送付し、知事の署名付きの公開鍵証明書が本人に送付される。これにより電子署名が使えるようになる。さらに資格認証サービスを受けるときは、この電子署名を付した申請書を当該資格認証機関に申請する。資格認証機関は、受け付けた申請書の電子署名により本人確認を行い、同機関が管理する有資格者のデータベースと照合する。そして、申請者が有資格者である場合には、電子的な資格証明書を発行する。

このとき、本人の実在性を認証するための本人確認と、その本人が保有する資格の認証が必要になる。PKI において資格認証を実現する方法としては、以下の方法が考えられる。

・資格が書き込まれた公開鍵証明書（PKC）を用いる方法
・PKC に対してリンクを有する属性証明書（AC）を用いる方法

資格が書き込まれた PKC を用いて電子署名を行う場合には、電子文書に対してこの PKC を添付した上で、この PKC に記載された公開鍵に対応する秘密鍵を用いて署名する。このため、資格証明を行うためには、秘密鍵の生成と公開鍵の CA への登録が必要になる。

AC を用いる場合には、個人認証のための PKC へのリンク情報を持つ AC と、その PKC を電子文書に添付し、この PKC に記載された公開鍵に対応する秘密鍵を用いて署名する。このため、別途個人認証のための PKC を用意することが必要である。ここで、公的個人認証サービスでは、署名検証者が行政機関等及び認定認証事業者等に事業者に限定されており、この利用については今後の課題である。このため、医師等の公的な資格については公開鍵証明書に属性として資格などを記載することで運用し、その他の属性については属性証明書を併用する方法が考えられる。

(4) 資格認証の実証システム

（財）医療情報システム開発センターでは経済産業省の事業である「保健医療情報セキュリティ事業の一環としてヘルスケア **PKI** の実証試験をおこなっている。本研究では、この実証試験システムにおいて、資格認証の実現形態及び問題点などを検討した。その結果、公的個人認証サービスを利用することにより迅速性、簡便性、安全性、正確性を改善することが示された。一方で、サービス利用時に用いるソフトウエアの開発に必要となる署名のためのアプリケーション仕様が公開されておらず、容易に電子カルテシステム等

へ組み込めないことや医籍簿のデジタル化等の整備が必要であることが明らかになった。

(5) 多機能 IC チップへの応用

住基カードで用いられる広域・多目的ICカードと同等な仕様の多機能ICチップは、カードとして個人が携帯する用途だけでなく、ネットワークに接続された様々な機器の認証にも用いることが可能である。機器認証が必要となるのは、ネットワークを通じた様々なサービスで、対象とする機器を特定する必要がある場合であり、医療機器の保守などのリモートメンテナンスや医療機関同士の連携の際には必要不可欠である。この際、リモートサービスを提供する側あるいは遠隔地から機器を操作する側からすると、特定の機器との間に安全な通信経路を確保する必要があり、利用者からすると、安全なサービスのみを受け入れる仕組みが必要となるため、機器とサービスを特定するための相互認証が重要であり、認証で利用するための鍵を安全に機器に配送し、設定する必要がある。

ここで、多機能ICチップを利用した鍵配送モデルは、住基カードでも採用されているマルチアプリケーションカードのアプリケーション管理モデルであるNICSSフレームワークに基づいている。

ICチップには、チップ上のアプリケーションを管理するためのチップマネージャ（CM）が搭載されており、CMには、機器を管理する機器管理者及びサービス提供者を認証するための情報が格納されているものとする。また、アプリケーションは、サービス提供者によって搭載され、その中にはサービスを認証するための情報、サービスで利用する機器を認証するための認証鍵、その他サービスで利用する機器固有の情報が含まれている。

ここで、サービス提供者が、アプリケーションをICチップに搭載するためには、以下の手順に従う。

まず事前に必要なのは、機器を機器管理者に登録（機器登録）することである。製造者によって仮登録、つまり仮の認証鍵がCMに設定された機器を、機器管理者に登録する。機器登録の際には、機器管理者から認証鍵などの情報の設定を受けICチップ内のCMに設定する。次にサービスの登録に入る。まず、サービス提供者とICチップの間で相互認証を行う。たとえば機器管理者とサービス提供者が同じ認証局から証明書を受けていれば、サービス提供者とICチップの間で認証することが可能となる。サービス提供者はICチップに搭載しようとするアプリケーションに関し、機器管理者に依頼してアプリケーションに対する機器管理者の署名などアプリケー

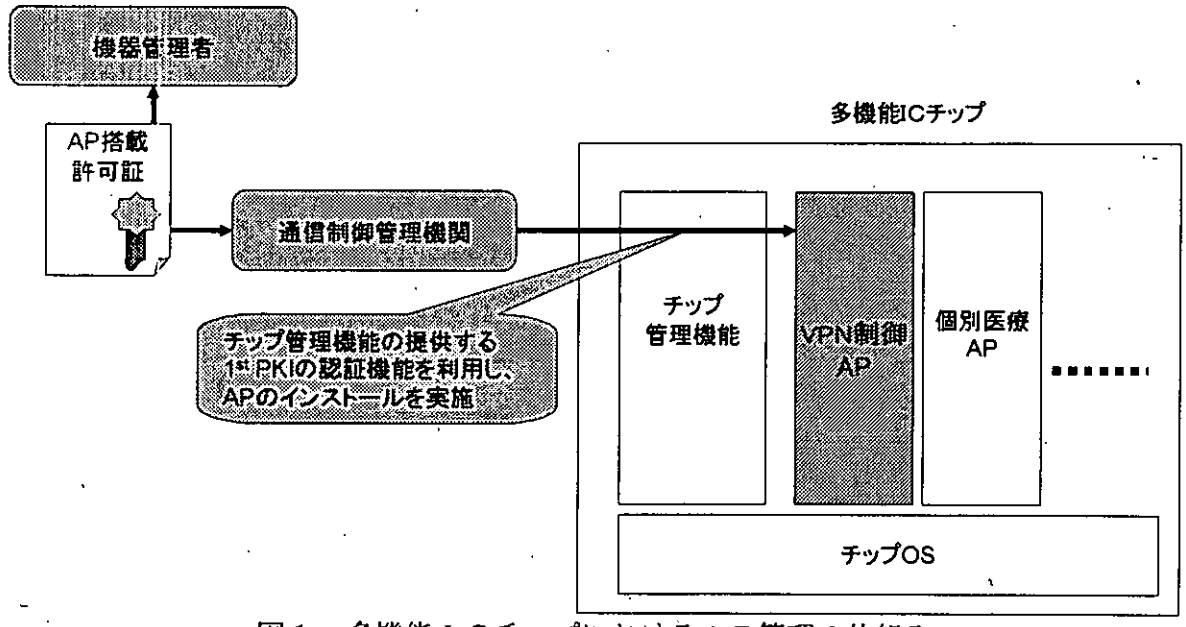


図１　多機能ＩＣチップにおけるＡＰ管理の仕組み

ションの正当性を保証するAP搭載許可証を取得する。ICチップに取得した搭載許可証を送り、ICチップは、AP搭載許可証の正当性を確認し、正しい場合にはアプリケーションを検証の後、チップ内に格納する。さらに、サービス実施に当たっては、サービス提供者とICチップ上の鍵で相互認証を行う。

ここで述べた鍵配送モデルでは、実際のサービスを含めるとIC チップにより実施される認証は２つのレイヤに分けられる。１層目は機器管理者によって正当であると許可された通信制御管理機関などのサービス提供者を認証し、ICチップのセキュリティ状態を変化させ、サービスに必要となる認証鍵を含むアプリケーションの管理を可能とする（図１）。２層目は、実際のサービスを提供するための認証である。第3者の正当性を確認するためには、各層の認証はPKIに基づくことが必要となるので、このモデルを２階層PKIと呼ぶ。

このように、多機能ICチップを利用することでオープンかつセキュアなネットワークにおいて、利用者や利用環境を迅速に確認し、誰もが安全、手軽に情報サービスを利用可能なインフラを実現することができる。

(6) 保健医療福祉分野における多機能ＩＣチップの活用

保健医療福祉分野においては、医療における情報セキュリティの確保、個人の医療情報の保護などが重要な課題として挙げられているが、多機能ICチップを利用した鍵配送モデルは、複数の情報機器間をセキュアなネットワークで繋ぐことを可能とする仕組みであるため、インターネットや無線LANなど、ネットワークの種類を問わずセキュリティが確保された状態で情報を流通させることができる。その結果、ネットワーク上を流通する個人の医療情報の保護が可能となる。また、セキュアなネットワークをオンデマンドで構築できる特徴もあることから、電子カルテ等、現在は特定の端末からしか利用できない情報も、旅先で急に病気になってしまったときに現地の端末から認証を経て自分のカルテをダウンロードするといったような利用法も考えられる。

さらに、通常、セキュアなネットワーク環境の構築には専用線等を利用する必要があり、ネットワーク環境の構築コストや通信コストは非常に高額となるが、多機能ICチップを利用することで、通常のインターネット上でセキュアなネットワーク環境を構築できるため、構築コスト、通信コストの低減を期待できる。

このように、保健医療福祉分野において多機能ICチップを利用した認証の仕組みは非常に有効であると考えられるが、全国に約20万箇所ある医療機関の医療情報機器やPC全てにICチップを据え付けるのは容易なことではなく、また、既存の医療情報機器を多機能ICチップ搭載機に置き換えるのも莫大な費用が必要となる。そのため、まずはセキュアなネットワーク環境の構築に必要となるルータ等に多機能ICチップを搭載し、ルータ単位でのセキュリティ確保を行う等、段階的な導入を推進する必要があると考えられる。

例えば、現在、VPN（Virtual Private Network）を用いて地域医療連携やオンライン保険請求の実証試験が行われているが、その実用展開・広域利用にあたっては、インターネットVPNでの認証・暗号化のための鍵の管理を行うことが必須になる。前述の仕組みを利用して機器に搭載された多機能ICチップにVPNアプリケーションをダウンロードすることにより、ネットワーク上にオンデマンドにVPNを構築することができる。これにより、ネットワークそのものへの外部からの不正なアクセスを防ぎ、セキュアなネットワーク環境でサービスを利用することができる。また、オンデマンドVPNは、従来のVPNのようにあらかじめ環境を構築することなく、その場で簡単にVPNの構築が実現する(図２)。

今後、図２に登場するプレイヤの具体的な役割、これらの機関が複数存在した場合における相互連携の具体的方法、通信プロトコル、運用手順などを検討し、実証システムの開発を行うことが課題である。

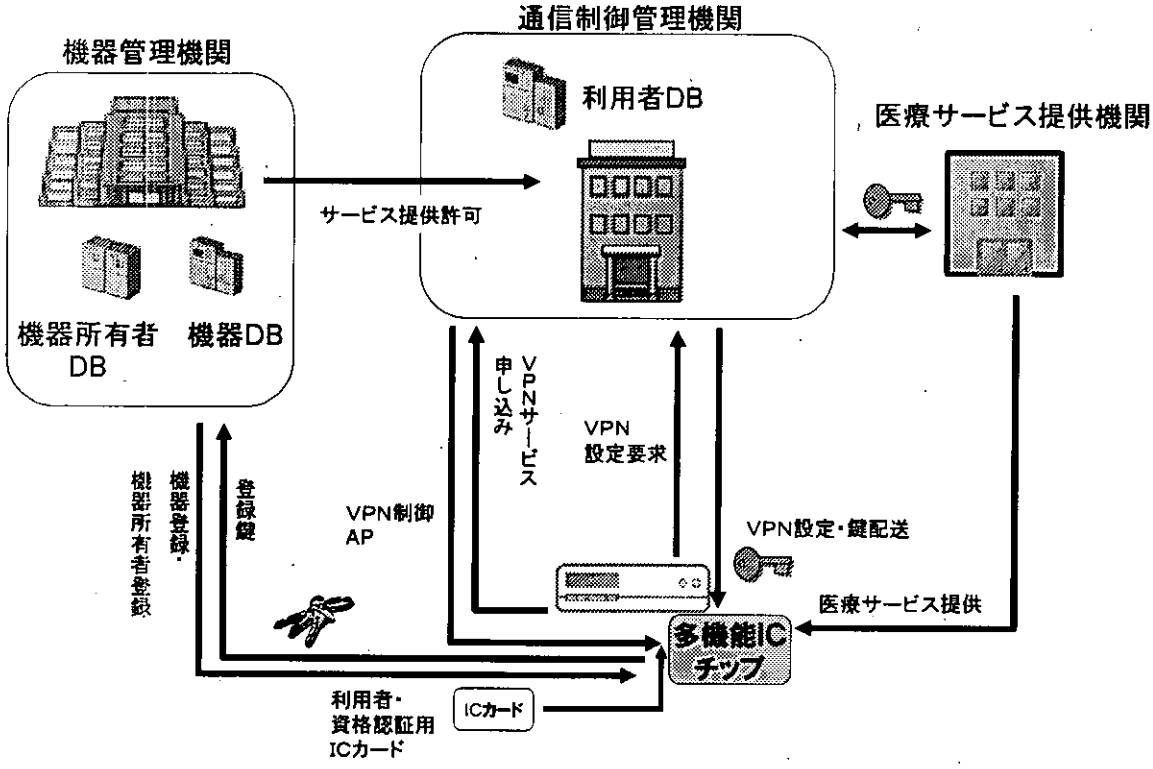


図２　オンデマンドVPNへの適用例

D．考察

医師等の認証を行うためには、まず認証の対象者が本人であること、そして医師等の資格や所属する医療機関等の情報を有するデータベースの情報を用いて資格を確認することが必要である。ここで、医籍は、医師免許の唯一の原簿であり、医師であることを証明する点について、信頼性が高いことから、資格認証を行うにあたっての資格の検証先として最適かつ欠かせないデータベースと考えられる。また、医師、歯科医師等の保健医療関連の資格にかかる証明書の発行を申請する場合の手続きとしては、概ね、各資格の免許証を再発行する場合と同様の手続き及び書類によってなしうると考えられる。しかし、現在の医籍に現住所が記載されていないため、基本４情報との照合ができないことも問題になる可能性がある。このため、医籍登録されている人物と、証明書発行申請を提出した人物の同一性を確認する方法については、今後更なる検討が必要である。

また電子的な資格認証の導入に付随する問題としては、従来の紙ベースの運用では行ってこなかった様々な課題を厳密化して実施することが必要であり、これが実務上極めて大きな障害となる可能性がある。このような問題の多くは、本来、電子化とはかかわりないものであるが、紙媒体中心の日常業務では通常、厳密な資格認証を求めていないため、顕在化していない状況にある。利便性が重要視される臨床の場において、厳格な資格認証を回避するシステムが構築された場合には、結果的に我が国の法が予定している内容とは異なったものになってしまう可能性がある。これを防止するために、早期に法の整備やその運用方法を含めて再検討を行う必要がある。

さらに、今後は認証基盤の整備とともに、それを活用した様々な保健医療福祉サービスの充実が求められており、資格・施設認証等と連動して多機能 IC チップを利用した安全なネットワーク基盤を構築していくことが、安全性、利便性、経済性などに優れた医療サービスの充実に役立つと考えられる。

E．結論

本研究では、保健医療福祉分野の電子認証を実施する方策を検討し、実現に向けた課題を明らかにした。住基カードの配布、公的個人認証サービスの開始など、実施に向けた環境は整いつつある。近年、電子カルテによる医療機関連携の運用も進んでいることから、PKIに基づく個人および資格認証の仕組みを早急に確立することが望まれる。

本研究で得られた成果は、保健医療福祉サービスにおける認証機構の研究開発に活用される予定となっている。具体的には（財）医療情報システム開発センターとの間で成果を共有することで、同センターで進めているヘルスケアPKIの実証実験や、多機能ICチップを利用した医療サービスの検討およびガイドライン等に反映する。また、住基カード、行政連携ICカード等に関連する研究開発や実証実験などに本研究の成果を提供し、実施に向けた具体的な課題の解決策を示していく予定である。

さらに、認証基盤の整備だけでなく、それを活用した様々なサービスの拡充が求められており、今後、本研究で得られた成果を活用して、新たな保健医療福祉サービスの創設に関する研究開発が行われることを期待する。

F．健康危険情報

該当なし

G．研究発表

1. 大山永昭, "次世代スマートカードの技術と応用," Interface, vol. 3, 2003.
2. 大山永昭, "電子政府の現状と課題," 情報処理, vol. 44, no. 5, pp.455-460, 2003.
3. 大山永昭, "e-Japan 戦略の見直しと電子行政に関する新たな課題," ITU ジャーナル, vol.33, no.6, pp. 42-46, 2003.
4. 大山永昭, "ユビキタスネットワークを支える技術(第2回)-電子認証基盤(PKI)-," 蔵前ジャーナル 6, 972, pp. 40-43, 2003.
5. 大山永昭, "スマートカードが先導する、e—JAPAN の行方と展望～スマートカードが変える、暮らしを変える、ビジネスを変える～," 財団法人ニューメディア開発協会 研究成果レポート, 10, 2003.

厚生科学研究補助金（医療技術評価総合研究事業）

分担研究報告書

資格認証の実証システムの構築

分担研究者　喜多紘一　（財）医療情報システム開発センター　審議役

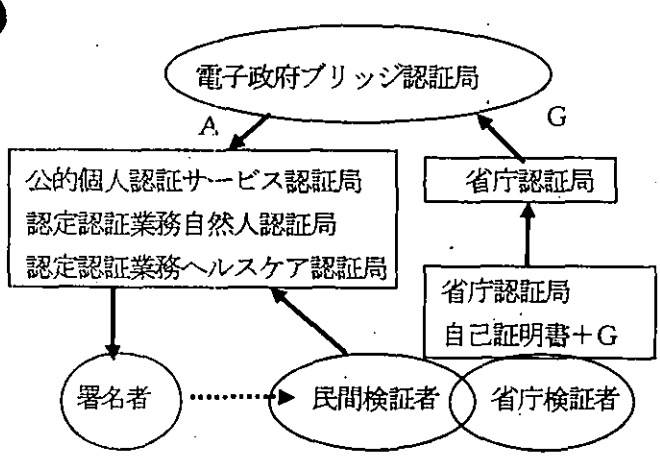
研究要旨　医療関連公的資格認証基盤を構築するに当たり、認証局を「電子政府用ブリッジ認証局へ接続する場合」とISO/TS17090に従った「電子政府用ブリッジ認証局とは独立したルート認証局へ接続する場合」の比較・検討を行った。その結果、「電子政府への電子申請」と「民間医療施設間の情報交換」を同一の医師用電子証明書で行うとすると、電子政府ブリッジとは接続しない独立したルート認証局による階構造をもった資格属性つきの証明書を発行できるヘルスケア認証局を構築することが望ましいとの結論となった。その為のルート認証局は必ずしも一つとは限らないので、証明書ポリシーをマッピング可能にするため、その標準化を早急に進める必要がある。また、電子政府側がこのルート証明書を組み込むためのルールと組み込み可能なルート認証局の条件を作成する必要がある。この場合、これらの仕組みを有効に活用するためには、電子署名法にもとづく署名を診療録等の記名、押印に変えても良いとの通知を出す必要がある。その際、認証局の条件は安易に特定認定認証業務取得認証局とせず、ISO/TS17090相当とする等の注意が必要である。

A．研究目的

現在、厚生労働省の「医療情報ネットワーク基盤検討会」で認証局のあり方を含め、検討が行われている。ここではその議論を踏まえ、医療関連公的資格認証基盤を構築するに当たり、認証局を図１に示す「電子政府用ブリッジ認証局へ接続する場合」と図２に示すISO/TS17090[1]に従い、「独立したルート認証局へ接続する場合」の比較・検討を行う。

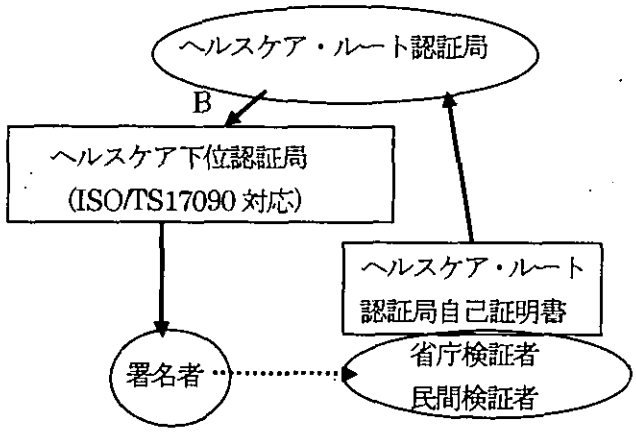
B．研究方法

資格認証システムの構築のために電子的な証明書、すなわち電子資格証明書を発行する認証局を「電子政府用ブリッジ認証局へ接続した場合」と「独立したルート認証局へ接続する場合」の比較・検討を「認証局の構築フェーズ」、「電子資格証明書発行フェーズ」と「電子資格証明書利用フェーズ」に分けて検討を行う。さらに、「電子資格証明書利用フェーズ」を「電子政府への電子申請」



申請書類＋署名者証明書＋相互認証証明書A

図１　電子政府用ブリッジ認証局へ接続する場合



申請書類＋署名者証明書＋下位認証局証明書B

図２　独立したルート認証局へ接続する場合

と「民間医療施設間の情報交換」に分けて比較する。この場合は、公的個人認証サービスや認定認証業務として自然人に発行される証明書を用いた場合も含め検討する。ここで言う「ヘルスケア認証局」とは自然人ではなく、ISO/TS17090に準拠した医師等の公的資格を記述した証明書を発行する認証局をさすこととする。

C．研究結果

1．認証局の構築フェーズ

a）電子政府用ブリッジ認証局へ接続した場合

ブリッジへ接続するためには民間の認証局の場合は「特定認証業務の認定」を受ける必要があり[2]、政府認証基盤相互運用性仕様書[3]に従う必要がある。電子署名法によれば、「「特定認証業務」とは、電子署名のうち、その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務」となっていて、現在は総務省、法務省、経済産業省が定めていて、医療行政を主管する厚生労働省は特に定めていないので、この業務が医師に対する「特定認証業務」として準用できるかは定かではない。

また、三省の特定認証業務は自然人に対するもので、属性は対象外となっているのでこの点も課題である。

特定認証業務の認定のためには初期設備費用や運用経費が年間数千万円かかり、認定費用も１億円近くかかる。特定認証業務はルート局に対して認定する制度はないので階層構造の認証ドメインを形成することはできない。

また、政府ブリッジに接続するには政府認証基盤相互運用性仕様書等に従う必要があり、相互認証証明書の交換手続きが必要になり、仕様的制約、時間的制約で自由度が阻害される。

b）独立したルート認証局へ接続する場合

ＧＰＫＩから独立して証明書ポリシーを決められるので、医療の世界で受け入れられやすいドメインを構築するための自由度が上がる。反面、ポリシーの妥当性等の管理、判定を行う組織化が必要となる。階層化した認証局ができるので、地域ごと、施設ごとでＣＰＳを作成し、ここの事情にあった認証局を構築できる。

又、特定認証業務の認定を取らなくても、何らかの監査基準、例えばISO/TS17090等に従っていれば、安全性が説明できるので、申請費用や設備費用が低いコストで認証局を構築できる。

2．電子資格証明書発行処理フェーズ

a）電子政府用ブリッジ認証局へ接続した場合

特定認証業務は電子署名用証明書のみであるので、認証用証明書が出せない。また、組織や機器証明書も出すことができない。階層化されていないので、１箇所の発行局から証明書を発行し、本人確認を1箇所または、登録端末のみをローカルに分散配置して行う方法になり、多様性に欠けたサービス提供となる。

b）独立したルート認証局へ接続する場合

ルート認証局の下に複数のＣＡ局をぶら下げることができるので、登録環境に合わせたＣＡ局が構築できる。反面、ルート認証局は下位ＣＡ局の証明書ポリシーおよび運用管理を何らかの形で監視し、認証局全体の証明書ポリシーの質の低下を防止する措置が必要である。

3．電子資格証明書の利用フェーズ

3．1　電子政府への電子申請

ここでは労災等給付申請の場合を想定する。申請書本紙は個人が直接申請する場合は公的個人認証サービスや民間の認定認証業務として発行された証明書を用い、又、社労士が代理申請する場合は社労士協会で発行された証明書を用いるものとする。これらはいずれも政府ブリッジへ接続された自然人の証明書である。この申請の際に添付される医師の診断書に対する電子署名を検討する。

3．1．1　電子署名の実施

a）公的個人認証サービス発行の証明書を用いる場合

図１に示すように、署名した診断書、署名者証明書、ブリッジ認証局からの相互認証証明書を添付して申請する。ただし、相互認証証明書は公的個人認証サービス利用者クライアントソフトには含まれていないので、入手する必要がある。電子政府へ申請するときは都道府県の相互認証証明書は検証側の電子政府がすでに用意してあれば、診断書につける必要はないので調査が必要である。

この場合、医師かどうかの判定は、診断書のコンテンツの、医療機関名、医療機関住所、医師氏名からわかり、

問題あれば確認できる現行の認印と同様の方式となる。

また、公的個人認証サービスの場合は氏名、性別、年齢、住所が出てしまい、実印の印鑑証明と同様であるが、単に診断結果を保証するのに実印を用いることは現状では行われないので、本方式が個人情報保護上、医師等から受け入れられるか問題である。

b）民間認定認証業務発行の自然人証明書を用いる場合

図1に示すように、署名した診断書、署名者証明書、ブリッジ認証局からの相互認証証明書を添付して申請する。この場合、医師かどうかの判定は、診断書のコンテンツとしての、医療機関名、医療機関住所、医師氏名からわかり、問題があれば確認できる現行の認印と同様の方式となる。

また、公的個人認証サービスの場合と異なり、通常、氏名以外の性別、年齢、住所は証明書には出てこない。

c）ブリッジ認証局へ接続したヘルスケア認証局の場合

図1に示すように、署名した診断書、署名者証明書、ブリッジ認証局からの相互認証証明書を添付して申請する。この場合、医師かどうかの判定は、証明書のhcRoleに記録されているので検証者は医師と確認しやすくなる。

また、公的個人認証サービスの場合と異なり、通常、氏名以外の性別、年齢、住所は証明書には出てこない。

d）独立したルート認証局へ接続した認証局の場合

図2に示すように、署名した診断書、署名者証明書、ルート認証局からの下位認証局証明書を添付して申請する。この場合、医師かどうかの判定は、証明書のhcRoleに記録されているので検証者は医師と確認しやすくなる。

また、公的個人認証サービスの場合と異なり、通常、氏名以外の性別、年齢、住所は証明書には出てこない。

3．1．2　電子署名の検証

検証側の一般的な処理ステップは以下のようである。

a）公開鍵証明書が正当か検証する。（証明書記述の正当性、証明書の有効期限、ＣＲＬ等による有効性、認証局の正当性の検証）

b）資格付電子証明書形式の場合は資格を証明書から抽出する。

c）本文のハッシュをとり、これと添付された電子署名としてのＭＡＣを公開鍵で復号したものと同じ値になれば公開鍵に対応する本人が正当に署名したものとみなす。

以下、認証局の違いによる検証のための処理を比較する。

a）公的個人認証サービス発行の証明書を用いる場合

電子政府機関は診断書に署名した公的個人認証サービス対応の電子証明書をブリッジ認証局経由、有効性を確認する。診断書が医師により発行されたものかどうかの確認は診断書の医療機関名等の記述内容により確認し、疑義があれば適切な方法で資格確認を行う。

b）民間認定認証業務発行の自然人証明書を用いる場合

電子政府機関は診断書に署名した認定認証業務発行の自然人電子証明書をブリッジ認証局経由、有効性を確認する。診断書が医師により発行されたものかどうかの確認は診断書の記述内容により確認し、疑義があれば適切な方法で資格確認を行う。

c）ブリッジ認証局へ接続したヘルスケア認証局の場合

電子政府機関は診断書に署名したヘルスケア認証局発行の医師資格つき電子証明書をブリッジ認証局経由、有効性を確認する。診断書が医師により発行されたものかどうかの確認は電子証明書より確認する。

d）独立したルート認証局へ接続した認証局の場合

電子政府機関は診断書に署名したヘルスケア認証局発行の医師資格つき電子証明書を独立したルート認証局を信頼点として、有効性を確認する。診断書が医師により発行されたものかどうかの確認は電子証明書より確認する。この場合、独立したルート認証局のルート証明書を検証システムにあらかじめ組み込んでおく必要がある。

3．2　民間医療施設間の情報交換

診療情報提供書を民間医療機関同士で交換する場合を検討する。公的個人認証サービスは民間同士の取引での使用は許可されてはいないのでその適用例は除いてある。

3．2．1　電子署名の実施

a）民間認定認証業務発行の自然人証明書を用いる場合

図1に示すように、署名した診断書、署名者証明書、ブリッジ認証局からの相互認証証明書を添付して情報交換する。この場合、医師かどうかの判定は、診療情報提供のコンテンツに記述された、医療機関名、住所、医師氏名からわかり、問題あれば確認できる現行の認印と同様の方式となる。

b）ブリッジ認証局へ接続したヘルスケア認証局の場合

この場合、医師かどうかは、証明書のhcRoleに記録されているので検証者は医師と確認しやすくなる。

また、公的個人認証サービスの場合と異なり、通常、氏名以外の性別、年齢、住所は、証明書には出てこない。

c）独立したルート認証局へ接続した認証局の場合

図2に示すように、署名した診療情報提供書、署名者証明書、ルート認証局からの下位認証局証明書を添付して申請する。この場合、医師かどうかは、証明書のhcRoleに記録されているので検証者は医師と確認しやすくなる。

また、公的個人認証サービスの場合と異なり、通常、氏名以外、性別、年齢、住所は証明書には出てこない。

3．2．2　電子署名の検証

a）民間認定認証業務発行の自然人証明書を用いる場合

民間医療機関は民間の取引でブリッジ認証局を利用できないので診断書に署名した認定認証業務発行の自然人電子証明書をブリッジ認証局経由、有効性を確認するわけにはいかない。同じ民間認定認証業務の認証局が発行した証明書であればその認証局を信頼点としてその証明書の正当性が確認できる。診断書が医師により発行されたものかどうかの確認は診断書の医療機関名等の記述内容により確認し、疑義があれば電話等で資格確認を行う。

b）ブリッジ認証局へ接続したヘルスケア認証局の場合

民間医療機関は民間の取引でブリッジ認証局を利用できないので診断書に署名したブリッジ認証局へ接続したヘルスケア認証局の電子証明書をブリッジ認証局経由、有効性を確認するわけにはいかない。同じヘルスケア認証局が発行した証明書であればその認証局を信頼点としてその証明書の正当性が確認できる。診断書が医師により発行されたかどうかの確認は電子証明書より確認する。

c）独立したルート認証局へ接続した認証局の場合

民間医療機関は診断書に署名したヘルスケア認証局発行の医師資格つき電子証明書を独立したルート認証局を信頼点として、有効性を確認する。診断書が医師により発行されたものかどうかの確認は電子証明書より確認する。この場合、独立したルート認証局のルート認証局証明書を検証システムにあらかじめ組み込んでおく必要があるが、一般に検証側も独立したルート認証局へ接続されたヘルスケア認証局からの証明書を保持していることが多いのですでに組み込まれていることが多い。ヘルスケア分野で複数のルートを設ける場合は、別途信頼できる方法で他のルート証明書も組み込む必要がある。将来的にはＯＳに組みこまれることが望ましい。

D．考察

1．医師の個人情報保護

公的個人認証サービス用の証明書を診断書の署名に用いると電子証明書には基本情報が記入されているので検証者等関係者に知らせることになる。

申請者本人であれば4情報を申請書に記入することが多いので、さほど問題にならないが、添付文書というレベルでそこまで医師を危険にさらすのは強制できない。

2．システム制限

2．1　階層構造が便利

電子政府ブリッジに接続させるためには特定認定業務の認定を取る必要があり、この認証局はエンドエンティティに対して証明書を出す必要があり、ルート認証局単体のみの構成では認定をとることができない。

医療の場合は資格確認の正確性が要求されるので、確認しやすく、責任を取りやすい、利用者の近くで登録業務を行うことが望ましいので、ルートの下に幾つかの認証局を構成し、その認証局をルートが認定する形が良い。その為には階層構造を認める構築が望ましい。

2．2　ソフトウエアの作成

診断書のインストール形態はＩＣカード、ＵＳＢスティック、ワークステーション等セキュリティ管理規定に

より自由に設計できることが望ましい。

公的個人認証サービスの場合、今のところカード仕様が民間で使用できるようにオープンになっていないので、活用に制限がでてくる。

3．使用制限

公的個人認証サービスは民間取引には使用できないとの制限があるので、電子政府に限った使用になる。
また、電子政府ブリッジも民間の取引には使用できないので、ブリッジに接続された異なった民間認証局から発行された電子証明書を民間取引のため、相互に検証することはできない。

従って民間取引を行うためにはブリッジに接続された認証局を使用する場合にはブリッジを経由せず、すべて一つの認証局より発行された証明書のみを用いる必要があり、医師用も薬剤師用も患者も、施設用証明書も同一の認証局から発行することになり、現実的ではない。

4．証明書の一元化

電子申請用証明書、民間医療機関情報交換用証明書を分離することは利用者にとって望ましいことではない。そのためには、電子政府のブリッジとは独立したるルート認証局より認証を受けた認証局より発行された電子証明書による診断書を電子政府側でも検証できるように、ヘルスケアのルート証明書を電子政府側でも組み込む必要があり、その為の基準が必要である。

4．認証局の費用

特定認証業務の認定を受けるためには1億円近くの費用が必要となり、運用コストも年間数千万円かかり、電子証明書の価格を引き上げることになり、ＰＫＩ市場が立ち上がっていない状況ではかえって立ち上がりを阻害することになる。

ルート認証局が下位認定局への証明書を発行する際に、証明書ポリシーとして、管理運用基準を審査し、利用にあった環境を自由に構築できるようにすることが、ＰＫＩの促進につながると考えられる。ただし、どこまで簡易化するかは全体のヘルスケアドメインに影響を与えるので、厳重に管理する必要があり、安易にコスト面の妥協をしないよう注意が必要である。

E．結論

電子申請用と民間医療施設間の情報交換を同一の医師用電子証明書で行うとすると、階層構造をもったブリッジと接続しない独立したヘルスケア認証局を構築することが望ましい。

その為のルートは必ずしも一つとは限らないので、証明書ポリシーのマッピング可能な標準化を早急に進める必要がある。

また、電子政府側はこのルート証明書を組み込む必要があり、組み込むためのルール作成と組み込み可能なルート認証局の条件を作成する必要がある。

この場合、これらの仕組みを有効に活用するためには、電子署名法にもとづく署名を医療関係の記名、押印に変えても良いとの通知を出す必要があり、通知発行の際、安易に特定認定認証業務取得を条件にしがちであるのを注意する必要があり、例えばISO/TS17090対応の認証局とする等の注意が必要である。

但し、将来、厚生労働省が医籍簿等を整備し、認証局を立ち上げ電子免許証として民間の取引への使用を認めるという解決策も残っており、もし予算的に可能であれば有望な方向であるので計画的に進めるべきである。

また、階層構造をもったルート認証局の接続が政府ブリッジでも認められ、民間取引にも開放されればこの方が、電子政府側でヘルスケア用のルート証明書を組み込む必要がなくなるので、望ましい姿である。しかし、接続条件がきびしくなり、自由度が阻害されるようであれば結局接続しないことになるであろう。

この場合、ヘルスケア認証局のルートが複数個、構築される場合はヘルスケアブリッジという構想も出てくると思われる。

F．参考文献

1）Health Informatics – Public Key Infrastructure (ISO/TS17090)

2）政府認証基盤におけるブリッジ認証局の相互認証基準について，行政情報化推進各省庁連絡会議，2001.4.15

3）政府認証基盤相互運用性仕様書，基本問題専門部会，2001.4.25

厚生労働科学研究費補助金(医療技術評価総合研究事業)
分担研究報告書

保健医療関連の資格認証の実施方策の調査·検討

分担研究者　公文敦　(財)医療情報システム開発センター研究開発部

研究要旨

医療の情報化をすすめるにあたって、医師の資格や所属する医療機関等の属性認証が必要となるケースが多くなると考えられる。その基盤となるデータベースには、厚生労働省の医籍登録や医師調査、都道府県における病院·診療所の開設にかかる許可申請または届出、医療施設調査などを活用することが、網羅性及び情報更新の管理から適切であると考えられる。これらのデータベースに基づき、医師の資格や所属する医療機関等の属性認証などの認証業務を行う属性認証機関に必要な要件や利点、課題等を検討した。

A. 研究目的

平成13年4月に施行された電子署名法では、利用者の肩書きや資格等の属性を証明することは、特定認証業務の対象には含まれていない。したがって、専門分野ごとにこれら属性認証に関する適切な方策を検討する必要がある。

保健医療分野においては、これまでに、ユースケースごとに認証が必要な医療資格を分類し、その資格の認証をおこなったり、属性証明書の発行に必要な手続きや申請書類を設定するとともに、申請書類を検証する方法などの検討を行ってきた。

本研究においては、医療従事者の本人確認及び、医療資格の認証を行う適切な機関を検討するための基礎資料を提供することを目的とする。

B. 研究方法

医師の資格や所属する医療機関等の属性認証を行う機関を検討するために、属性認証機関に必要な要件、及びその利点や課題を整理した。

(1)資格の確認等に活用できるデータベースの整理

医師の資格や所属する医療機関等の属性認証に利用できると考えられる既存データベースについて、その利点と課題を整理した。

(2)属性認証を行うために必要な手続きの

整理

医師の資格や所属する医療機関等の属性認証を行うには、属性(資格)証明書を発行することが必要であるが、発行に際しての申請手続きや申請に必要と考えられる書類を検討した。

(3)属性認証機関に必要な要件の整理

医師の資格や所属する医療機関等の属性認証を行う機関として必要な要件を整理した。

(4)医師の資格や所属する医療機関等の属性認証機関として考えられる認証機関

医師の資格や所属する医療機関等の属性認証を行うには、どのような認証機関が考えられるかについて、その特徴ごとに列挙した。

C. 研究結果

1. 資格の確認等に活用できるデータベースの整理

・医師の資格を確認するには、厚生労働省の医籍登録と隔年ごとに実施される医師調査を活用することが、網羅性及び情報更新の管理から適切であると考えられる

・医籍登録については、正確な電子データベース化が進んでおらず、またデータの更新等が十分ではない。

・医師調査は、ある程度電子的にデータベース化されており、データも隔年ごとに更新されている。また登録日現在の医師の所属機関等に関する属性情報なども付加されている。一方、届出漏れ、重複届出、医籍登録番号の転記ミス等を完全に検証する体制になっていないこと、また虚偽の届出があったとしても、完全に排除する仕組みができていない。

・したがって、これを活用するには、医籍と医師調査のデータを一致させる検証作業が必要であり、また医師調査の届出率をできる限り 100%に近づけること、医師調査を届出ない限り、オンライン等を通じた医師の資格認証を伴う医療サービスの提供を実施させない等の政策的誘導も必要と考えられる。

2. 属性認証を行うために必要な手続きの整理

(1)属性認証および属性証明書発行のための申請書類

医師の資格や所属する医療機関等の属性認証を行うために発行する属性証明書の申請に必要な書類を、医師免許証の再交付(毀損・亡失時)に必要な書類と同等とした場合、次のような書類が必要と考えられる。

○認証及び証明書発行申請書

○医師免許証、歯科医師免許証等の原本

または写し

○戸籍抄(謄)本、本籍地の記載された住民票、または、公的個人認証サービスで発行された電子証明書など、本人確認を行うための証明

○印鑑または電子署名

(2)書類の検証

① 想定される脅威(実社会とサイバー社会での脅威)

医師の免許証等の発行～再発行を虚偽により申請し、万一発行された場合には、次のような脅威が発生すると考えられる。

(虚偽申請に基づく医師の免許証発行で発生しうる実社会での脅威)

架空の医師により、診療所を開設したり、診療行為を行うことが可能となる。また診断書や死亡診断書の交付、処方箋の交付等が可能になる。一方、これらには実務的な技術力が必要と思われることから、医学を修得していないものには、ごく限られた活動しか行うことができず、社会への影響力は比較的小さいと思われる。

(虚偽申請に基づく医師の免許証発行で発生しうるオンライン社会での脅威)

先述の実社会での活動に加え、cyber 上(コンピュータネット上)での活動が可能となる。これは、インターネットや情報通信機器を介して遠隔地から診療や処方を行ったり、インターネット等を介して個人情報を含む患者情報にアクセスしたりすることが可能となり、これにより、医師でないものの医業が容易に行われる脅威が発生する。

②申請書類の検証の必要性

オンラインを介した医師の免許証等の発行や資格認証においては、従来に比べて社会への影響力が拡大する可能性があると考えられるため、これまで以上に慎重になるとともに、申請書類の真正性の検証を完全に行う必要があると考えられる。

③申請書類の検証方法

○検証先

厚生労働省医政局にて管理する医籍簿、歯科医籍簿

○厚生労働省医薬食品局総務課にて管理する薬剤師名簿

○検証に必要なデータの種類

別添(表1)参照

3. 属性認証機関に必要な要件の整理

医師の資格や所属する医療機関等を認証する(資格等の属性認証)ためには、次のような手順が考えられる。

まず、認証を行ったものが本人であることの確認を行い、次に、1. 2. で検討した、医

師の資格や所属する医療機関に関するデータベースの情報の提供を受け、医師の資格や所属する医療機関等を認証することである。

このためには、属性認証機関の要件としては、

①自らの認証によって、または他の認証機関との役割分担や、他の手法によって、本人認証が行えること。

②医師の資格を保持していることが確認できること。方法のひとつとして、厚生労働省の管理する医籍や医師調査のデータベースから情報の提供を受けることができることがある。

③②で厚生労働省の管理する医籍や医師調査のデータベースから情報の提供を受けるにあたっては、医師法や統計法等の関係が整理できること。

などが考えられる。

4. 医師の資格や所属する医療機関等の属性認証機関として考えられる認証機関

3. で検討した要件を満たす属性認証業務を行いうる機関としては、次のような機関が考えられる。

① 国等の公的機関

② 民間機関(特定認証業務を請負う認定機関)

③ 民間機関(特定認証業務以外の認定機関)

D. 考 察

研究方法3.で検討した要件に基づいて、研究方法4. で検討した機関ごとに、信頼性、利便性、経済性、脅威への対応等の観点から、利点と課題を検討したところ、別添(表2)のように考えられた。

E. 結 論

医療情報を交換したり、参照したり、診断書を発行したりする際には、医師等の医療従事者が作成した文書であること、また一定の条件のもとでアクセスが許された医療従事者であること等を確認する必要があり、その手順として、医師の資格や所属する医療機関等を認証すること(資格等の属性認証)が考えられる。

認証を行うためには、先ず認証を行う自然人が本人であること、次いで医師の資格や所属する医療機関に関するデータベースから情報の提供を受けて、資格を確認することが求められる。

これらの要件に基づいて考えると、公的な機関が本人認証する場合には、信用度が高いこと、安価に行えることなどの利点がある反面、住民基本台帳記載の個人4属性(氏名、生年月日、性別、住所)が公開され

ること、署名のためのアプリケーション仕様が公開されておらず、電子カルテや診断書作成ソフトに組み込めないことなどの課題がある。さらに資格認証を行う場合には、医籍簿等との連携が比較的容易であることなどがあげられる。

一方、民間の機関が本人認証する場合には、個人のプライバシーにかかる属性情報の公開等を管理できること、署名のためのアプリケーションの入手が容易であることなどの利点がある反面、信用度のレベルや費用がかかるという課題がある。さらに、資格認証を行う場合には、資格の要件の確認方法及びその正当性に課題が伴う。

今後は、これらの利点、課題にもとづく特性を踏まえたうえで、社会的なコンセンサスを形成し、安全性の確保とともに、利便性と経済性のバランスのとれた認証基盤の構築を検討するべきである。

（表1） 検証に必要なデータの種類

	属性認証及び属性証明書発行に必要な書類		医籍に登録されている事項 （医師法施行令第２条、施行規則第２条）
	書　　類	書類に記載されている事項	
資格認証	① 認証及び証明書発行申請書 （☆免許証再交付申請書）	登録番号	登録番号
		登録年月日	登録年月日
		本籍地都道府県名（日本国籍を有しないものについては、その国籍）	本籍地都道府県名（日本国籍を有しないものについては、その国籍）
		氏名	氏名
		性別	性別
		生年月日	生年月日
		合格試験名（第〇回〇〇試験）	（資格ごとに個別の名簿あり）
		試験合格年月	医師国家試験合格の年月
			免許の取消又は医業の停止の処分に関する事項
			再免許の場合はその旨
			免許証を書替え交付又は再交付した場合には、その旨並びにその事由及び年月日
			登録の抹消をした場合には、その旨及びその自由及び年月日
	② 医師免許証、歯科医師免許証等の原本または写し		
本人認証	③ 戸籍抄（謄）本、本籍地の記載された住民票 （☆または公的個人認証サービスで発行された電子証明書など、本人確認を行うための証明）		
	④ 印鑑 （☆または電子署名）		

☆ 属性認証及び属性証明書発行に必要な書類は、医師免許証の再交付（毀損・亡失時）に必要な書類と同等とした）