日本医師会における認証局の設立および運営に向けての研究

矢野 一博

１．はじめに

日本医師会（以下、日医）は、2001 年 11 月、医療現場の IT 化を自ら先頭に立って推進するとの観点に立って、「日医 IT 化宣言」を発表した。こうして医療現場における IT 化を進める活動で、当初から避けて通ることのできない重要な課題として、直面してきたのがセキュリティの確保という命題である。日医では「日医 IT 化宣言」の発表と同時に、安全で安心して使える IT 基盤を実現するための検討を重ねてきた。その答えの一つが、公開鍵認証基盤（Public Key Infrastructure：PKI）の枠組みを使った日医による認証局（日医認証局）の設立である。日医認証局は、2003 年度からシステムの設計・開発、運用構築の検討などの具体的な取り組みを開始し、2005 年 11 月に基本的な機能の開発を完了した。この年、2005 年 4 月には個人情報保護法が全面施行されている。

この日医認証局開発の完了を受けて、日医では実際に認証局から発行される電子証明書を用いた実証実験を 2005 年 12 月より実施している。この実証実験の目的は、開発された認証局の機能を確認することとあわせて、電子文書の作成責任者の明確化、および改ざんを行ったことが検出可能であることの検証を行うことである。

日医のこのような取り組みの一方で、行政施策においても保健医療福祉分野における認証基盤の構築が徐々に進んでいる。政府の高度情報通信ネットワーク社会推進戦略本部（IT 戦略本部）が発表した、2004 年の「e-Japan 重点計画-2004」から 2005 年の「IT 政策パッケージ-2005」、そして 2006 年 1 月の「IT 新改革戦略」において、保健医療福祉分野における認証基盤の整備が重要項目としてあげられている。

厚生労働省でも、2003 年に「医療情報ネットワーク基盤検討会」（座長：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）を設置し、2004 年の最終報告書の中で認証基盤の整備を答申し、2005 年 4 月に保健医療福祉分野における認証局の設置基準等を定めた「保健医療福祉分野 PKI 認証局　証明書ポリシ[1]」を通達した。

このように、保健医療福祉分野における認証基盤構築の動きは、日医の活動を先導として、国全体の IT 化を見据えた、行政も巻き込んだ大きな流れとして存在している。

今般、日医認証局の基本機能の開発が完成し、現場での活用を実現するための実証実験を開始したこともあり、医療現場における認証基盤構築の作業は、現在、きわめて重要な段階を迎えているということができる。本研究は、そのような動向を受けて、これまでの日医認証局開発の活動について総括を行い、今後のあり方の方向を明らかにすることを目的に実施したものである。

２．事業・活動の経過

日医総研における日医認証局の取り組みは、日医総研ワーキングペーパー「医療分野情報ネットワーク構築に向けての基礎研究　－日本医師会認証局の提言[2]」（2002 年 5 月、No68）から始まる。この研究は 2001 年 4 月の第 104 回日医代議員会での質問を受け、日医総研の研究として立ち上がり、2003 年には第Ⅰ期開発に着手した。

認証局の機能は、様々な要素を組み合わせて構築されている。これを大きく区分すると

「発行局」（Issuance Authority：IA）といわれる機能と、「登録局」（Registration Authority：RA）といわれる機能に分けられる。

発行局は、実際に電子署名をするための電子証明書を発行するシステムと、発行した証明書が有効か、無効か、を管理するシステムで構成される。

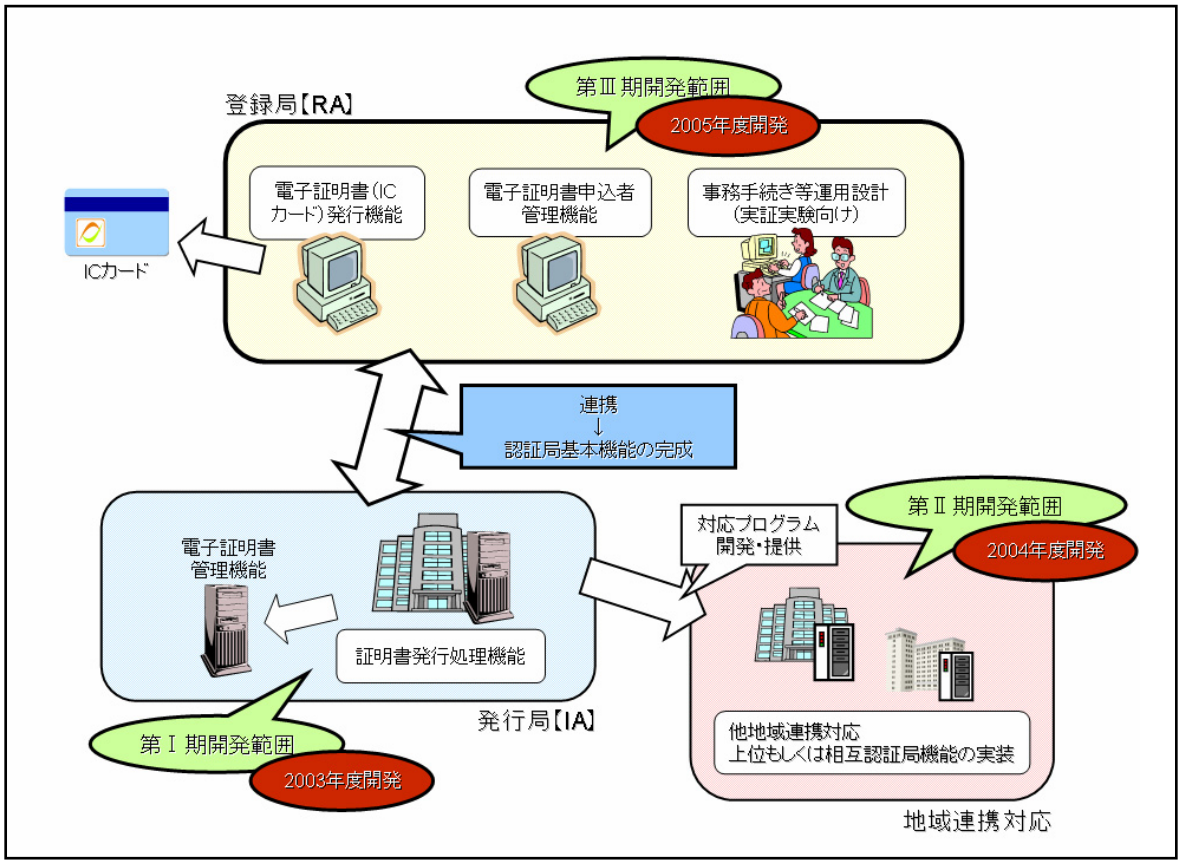
登録局は、電子証明書の申込者本人の確認や実在性を確認するなどの、人による実務を行う事務局の機能と、電子証明書の申込者の情報を登録して発行局に証明書の発行を依頼するシステムで構成される。

発行局はコンピュータやネットワークなどシステムで構成されるのに対して、登録局は人員なども含めた、部署、部門という色合いが濃い。従って、日医認証局の検討においては、コンピュータシステムやネットワーク設計などの検討と平行して、事務局機能などの組織体のあり方もあわせて検討を進めている。

最終の第Ⅲ期の開発段階まで完成したとしている認証局の基本機能は、このうちの機械的な認証システムであり、今後、本格的に日医認証局を展開する場合は、さらに登録局業務を実施する事務局機能のあり方について、詳細に検討をする必要がある。

こうして 2003 年から 3 期に分けて開発してきた認証局は、下図に示すような開発区分により開発を進め、2005 年 11 月に第Ⅲ期開発が完了した。

図 1　日医認証局の各フェーズにおける開発区分



日医認証局システムの開発完了によって提供できる機能は、表 1 のとおりである。この開発完成を受け、現在、実証実験を実施している。

表 1　認証局システムで提供可能な機能

開発フェーズ	開発機能等	提供可能な機能
第Ⅰ期開発 【2003 年度】	・ネットワークシステム ・電子証明書発行機能 電子証明書規定書など	・電子証明書発行（サーバシステム向け） ・失効リスト（無効証明書情報）発行
第Ⅱ期開発 【2004 年度】	・副認証局向け電子証明書発行システム ・副認証局向け電子証明書管理システム	・副認証局用電子証明書発行
第Ⅲ期開発 【2005 年度】	・登録局機能 －　証明書発行依頼業務端末 －　証明書情報管理端末 －　署名、認証、暗号鍵管理端末など ・個人向け証明書発行運用設計 ・個人電子証明書用認証局運用規定 ・個人電子証明書発行用事務取扱要領	・電子証明書発行（個人向け） ・電子証明書発行管理機能 ・IC カード格納用個人鍵発行機能

今回完成した認証局は、例えば印鑑登録証明書を発行する役所の役割であって、認証局から発行される電子証明書は印鑑登録証である。例えば「車を購入する」際には実印が必要であり、実印であることを証明するためには印鑑登録証明証が必要である。これを認証局に当てはめると、単に認証局システムが完成し、電子証明書（印鑑登録証明証）が発行できても意味がない。「車を購入する」という目的と同様に、電子証明書を用いた電子署名（実印）が、何のために必要であるかという、目的が必要である。

今回の認証局による電子証明書の発行は、「紹介状の作成」を目的として作業を行ってきた。現場の医師の紹介状には、当の医師による署名、もしくは押印が必要である。電子的に紹介状が作成されるならば、その紹介状が確かに当の医師により作成されたことを証明する電子的な署名押印が必要となる。この電子的な署名押印が電子署名であり、電子的に作成された紹介状に電子署名をすることで、電子医療情報の信頼性の確保を図ることができる。日医認証局から発行する電子証明書は、各種の国際規格等に準拠[4-13]するとともに、保健医療福祉分野独自に定められた国際規格にも準拠[14-16]している。さらに、電子署名の利用方法は、厚生労働省の「保健医療福祉分野 PKI 認証局　証明書ポリシ」に準拠している。

３．実証実験の実施

岐阜県岐阜市医師会、京都府山科医師会の協力を得て、岐阜県で 30 名、京都府で 84 名、合計 114 名の参加を得て、日医認証局の実証実験を実施している。電子証明書を格納する媒体としては IC カードを用い、これを読み込むための IC カードリーダーとともに参加医師会員に配布した。

電子署名を付与する電子紹介状については、ファイル形式を PDF（Portable Document Format）とした。これは、現行医療制度上、診療情報提供料などの加算を算定するためには、原本として紙が必要になる場合が多く見受けられるため、印刷時に親和性の高いファイル形式を選択したからである。

電子紹介状を作成する機能については、山科医師会では既に地域医療連携システムの中で紹介状を作成する機能を活用していたため、この機能の中に電子署名を付与する仕組みを組み込んだ。岐阜市医師会については、各医師がそれぞれ独自に紹介状を作成しているため、簡易な紹介状作成アプリケーションを開発した。また、PDF に付与される電子署名は、電子署名後、紹介状の指定した欄に印影のイメージを貼り付けるようにした。さらに、電子署名は署名押印に当たるため、実験に参加する 114 名の医師のみに可能としたが、実際に署名された電子ファイルは誰でも署名確認できることとした。

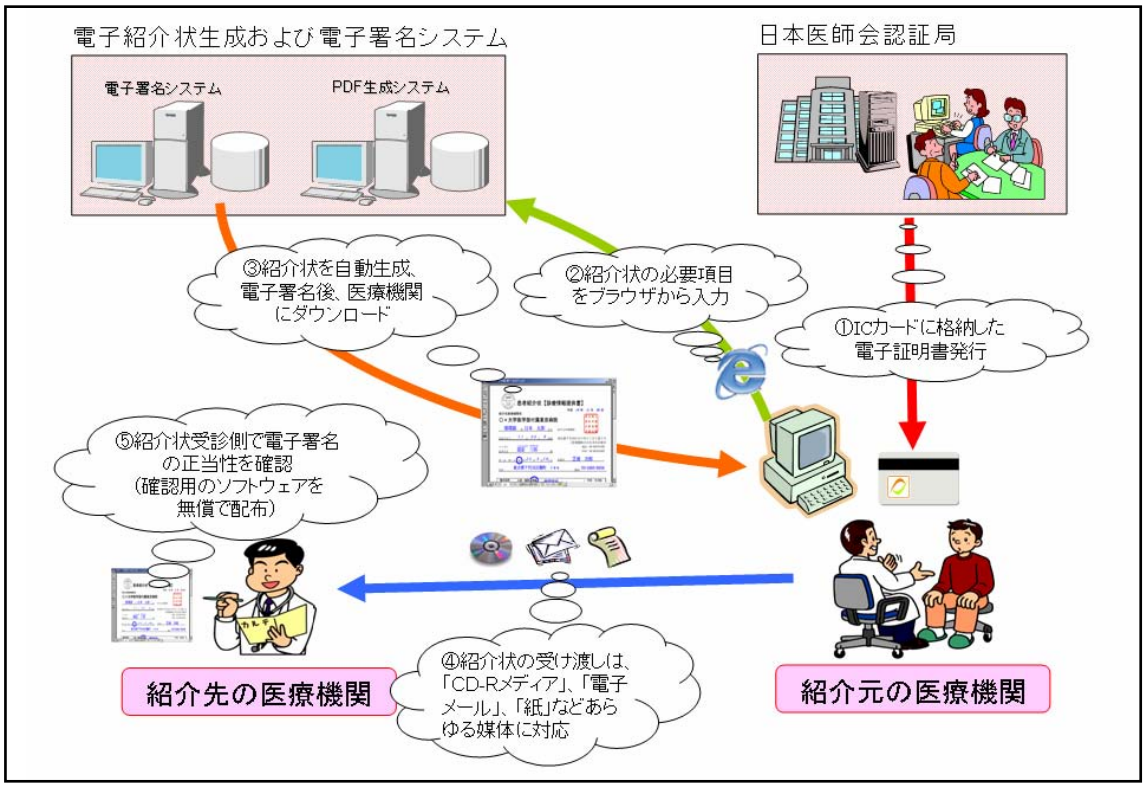
このような準備を経て、参加医師の協力のもと、日医認証局の実証実験を開始し、作成された電子紹介状のやり取りを実施する。

紹介状を受け取った医師は、イメージとして PDF に貼り付けられた印影をクリックすることで電子署名を検証し、電子紹介状の作成者を確認することができる。この作業を通して、電子署名に対する認識、また電子署名が付与された文書の信頼性について検証を行うこととした。

表 2　実験参加地域プロファイル

	岐阜県岐阜市医師会	京都府山科医師会
参加人数	30 名	84 名
紹介状作成機能	日医提供アプリケーション	地域独自アプリケーション
紹介状ファイル形式	PDF	
証明書格納媒体	IC カード	
	ELWISE（NTT 東日本製）	Standard-9M（三菱電機製）
署名検証方法	日医提供検証ソフト 日医 HPKI<SignedPDF Verifier> Ver.1.0.0 を利用	

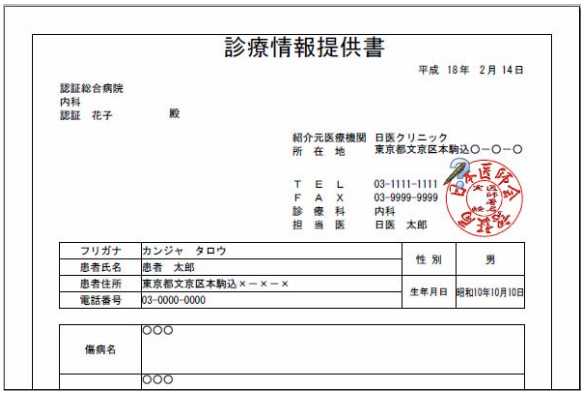
図 2　実証実験のイメージ



今回の電子署名は PDF ファイルに印影のイメージとして再現されている。従って、送られてきた紹介状にある印影をクリックすると電子署名の検証が行われ、正しく署名されていれば「医師が署名した文書です」と表示される。これによって利用者は、当該紹介状が確かに医師により作成され、かつ、作成後改ざんされていないことが確認でき、電子的に作成された紹介状を信頼することが可能となっている。

受け取った時の紹介状の状態が図 3 である。この時点では、まだ電子署名が正しいか否か、確認をしていないので、イメージとして付与された印影上にクエスチョンマークが表示されている。

図 3　紹介状を受け取った時の表示


診療情報提供書

平成 18年 2月 14日

認証総合病院
内科
認証　花子　　殿

紹介元医療機関　日医クリニック
所在地　東京都文京区本駒込〇－〇－〇

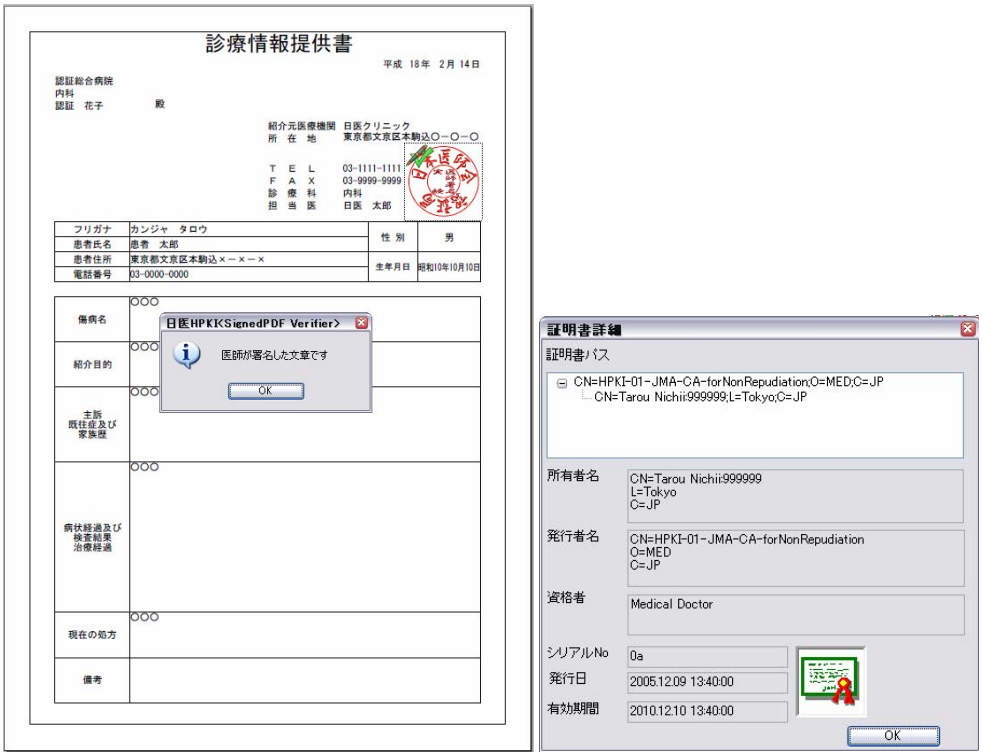
TEL　03-1111-1111
FAX　03-9999-9999
診療科　内科
担当医　日医　太郎

フリガナ	カンジャ　タロウ	性別	男
患者氏名	患者　太郎		
患者住所	東京都文京区本駒込×－×－×	生年月日	昭和10年10月10日
電話番号	03-0000-0000		

傷病名	○○○
	○○○

印影をクリックすることで電子署名の検証が実行される。この時、医師が当該紹介状に署名を施し、その後、改ざんされていない場合は正しい紹介状として「医師が署名した文書です」と表示されると同時に、印影上に確認済みというチェックが入る。その様子を示したのが図 4 左である。また、印影では表現されていない電子署名の詳細については、電子署名のプロパティを表示することでその詳細を見ることができ、その様子を示したのが図 4 右である。

図 4　電子署名を検証した時の表示と電子署名の詳細表示



この検証の時に、医師による署名がされなかったり、署名後文書が改ざんされていたような場合は、図 5 に示すように印影上にバツ印が付き、文書が正当なものではないと警告される。

図 5　正当に電子署名がされなかった場合の表示

これらの印影上に表示されるイメージを確認することで、電子署名の正当性をコンピュータ画面上で確認できる。

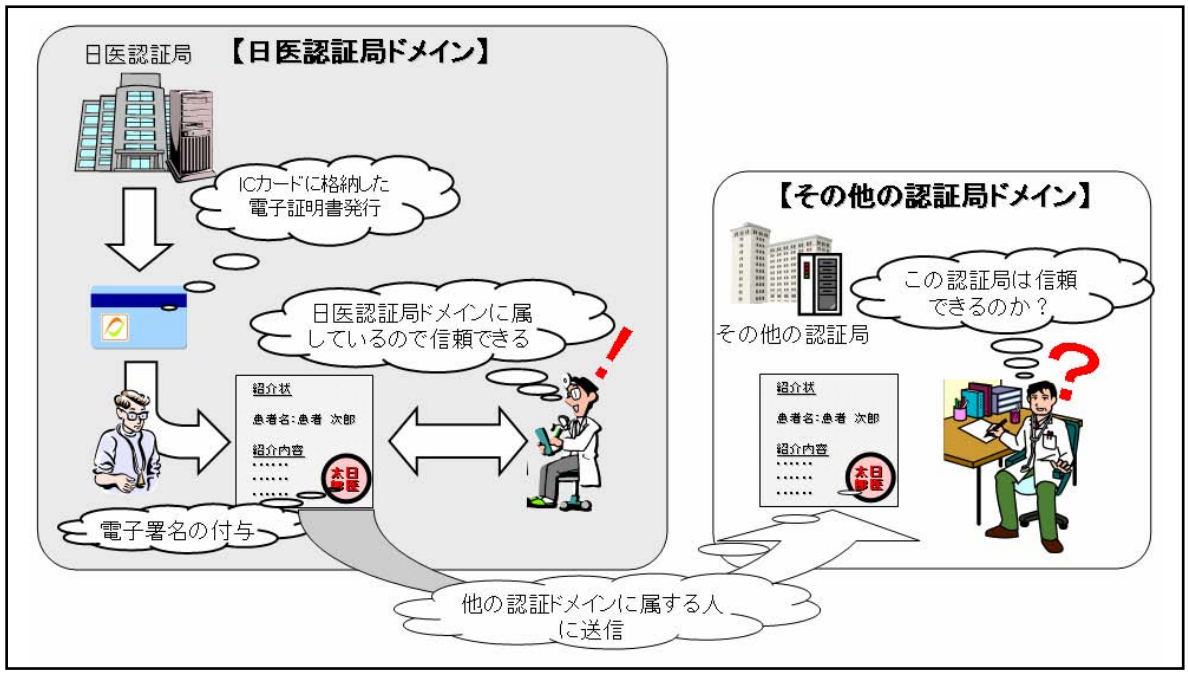
４．考 察

１）認証局のあり方

認証局は、単に電子証明書を発行するだけでは成り立たない。「信頼の輪」ともいうべきものが必要となる。例えば、日医認証局から発行した電子証明書による電子署名を、日医認証局以外の利用者が受け取ったときに正しいと確認できる必要がある。

日医認証局の電子署名を受け取る人たちを、仮に「日医認証局ドメイン」に属する人たちと呼ぶ。日医以外の認証局のドメインに属する人たちが、日医認証局ドメインの電子署名を確認できるようにするというのが問題解決の主題となる。

図 6　異なるドメインでの電子署名確認時の問題点



この問題を解決するには、それぞれのドメインに属する認証局が相互に接続され、相互の認証局がお互いに信頼できる基盤が必要である。この信頼基盤の構築こそが、日本全体における認証基盤構築の要となる。

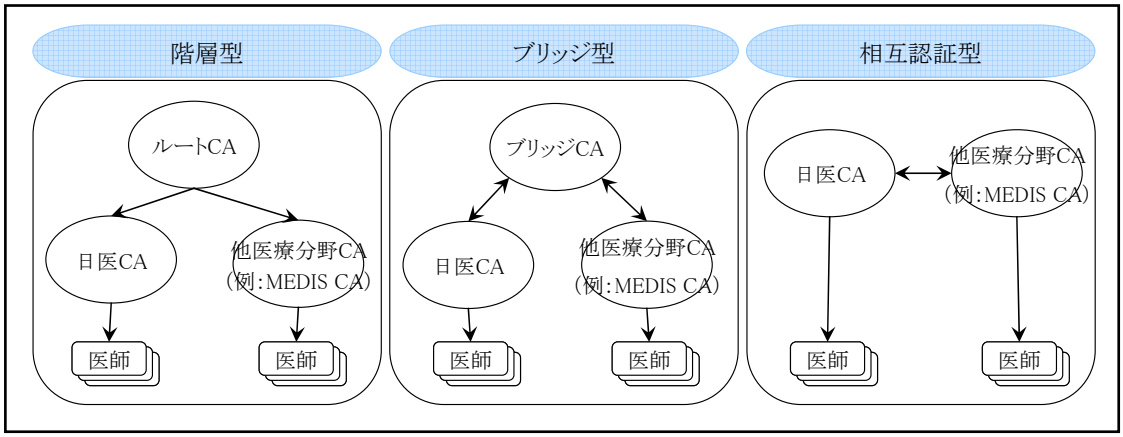
この相互信頼の輪の構築の仕方には幾つかのパターンが存在する。そこで 2005 年 5 月、日医総研において、それらの「信頼の輪」のあり方について検討を重ね、将来的な展望として取りまとめたのが、日医総研報告書「保健医療福祉分野における公開鍵認証基盤のあり方について－日医認証局の現状報告および公開鍵認証基盤の将来展望－[3]」である。

報告書の中では、保健医療福祉分野における認証基盤のあり方を「短期実現モデル」「中期実現モデル」「長期実現モデル」の段階に区切り、それぞれの段階における認証局同士の信頼基盤のあり方を類型化して整理している。

短期実現モデルでは、日医認証局単体で認証基盤を構築することを目指しており、今回開発した認証局はこのモデルに沿ったものとなっている。このモデルでは、仮に他のドメインに属する認証局が存在したとしても、その数は少数という仮定を設け、お互いが直接接続することで信頼基盤の確立を可能としている。

これに続く中期実現モデルでは、様々な認証局が保健医療福祉分野の認証基盤に参加するとの前提で、その信頼基盤のあり方について「階層型」「ブリッジ型」「相互認証型」と分類して、それぞれに対して整理を行った。

図 7　中期実現モデルにおける認証局の信頼基盤のあり方



最後の長期実現モデルでは、電子政府など行政系の認証基盤との接続についての検討をしており、現状では具体的な実現モデルの提言が困難であったため、課題の整理に留めている。

今後、わが国全体を網羅する保健医療福祉分野の認証基盤を構築するには認証局の相互信頼基盤の検討を進める必要がある。

日医は現在に至るまで、この保健医療福祉分野の認証基盤を担うために日医認証局の検討を進めてきている。従って、今後、厚生労働省で具体化してくると予測される保健医療福祉分野の認証基盤のあり方について、十分なフォローアップを行う必要がある。場合によっては、日医が主導権を持って保健医療福祉分野の認証基盤のあり方の提言をすることも必要である。

その際には、中期実現モデルに従って「階層型」「ブリッジ型」「相互認証型」など様々な形態が考えられる認証基盤モデルを、医療機関の現場からも検証する必要があると考えられる。現場からの検証がなければ、現場で使えないモデルが出来上がり、結局は基盤として成り立たなくなる可能性が高い。そのため、実際に認証局を必要とする臨床現場での業務を洗い出し、それを IT に適したモデルに落とし込む作業が必要と思われる。

本作業は相当の困難が伴うと思われるが、IT 化を行うには避けて通れない事項として、今後、研究を進めたい。

２）電子署名検証のあり方

実証実験では、PDF で作成された紹介状に電子署名を付与し、その印影を確認することで電子署名の正当性を実証することができた。

実験で用いた電子署名は、各種の国際規格や保健医療福祉分野における規格に準拠したものであり、今回の実験により正当性が実証できた意味合いは大きい。

今後、日医としてもこの取り組みを継続していくことで、行政でも検討されている保健医療福祉分野の認証基盤構築にも、日医認証局という実態を持って連携や交渉に当たることができる。しかし、そのためにはクリアしなくてはならない課題もある。

今回の実験は、岐阜県および京都府の日医会員に日医から依頼し、日医で開発した電子署名検証ソフトを用いていることに着目する必要がある。

実験では、日医の実験で日医会員に協力を依頼しているため、参加した医師は全て日医認証局のドメインに属している。したがって、電子署名の正当性については実証することができた。しかし、日医会員以外の医師や患者がこの紹介状を受け取った場合は、先ほどの「認証基盤のあり方」の中の図 6 に示した問題を解決しなくてはならない。言い換えれば、認証局の「信頼の輪」を確認するのが電子署名検証ソフトの役割でもある。

つまり、日医認証局ドメインに属する医師が作成した紹介状を、それ以外の認証局ドメインに属する医師等が確認できるようにするには、電子署名検証ソフトも「信頼の輪」の中に組み込む必要がある。

電子署名を検証する行為は、あくまでソフトウェアが実施するものである。そこで、この電子署名検証ソフトを他の認証局のドメインでも利用できる手続きを構築しなくてはならない。電子署名の検証が正当になされなければ、電子署名の信頼自体が揺らぐことになる。従って、まず、この電子署名検証ソフトの設計図を含めた、署名の検証ルールを作成しなくてはならない。しかも、そのルールは保健医療福祉分野で電子署名を検証しようとする人達全員が信頼できるルールでなくてはならない。

今回、日医認証局から発行された電子証明書による電子署名を確認するためのソフトウェアを日医から提供している。しかし、今後、このソフトウェアや別の業者が作成する電子署名検証ソフトは、ある一定のルールに基づいて作成され提供されるという仕組みが必要となる。その仕組みをつくり、認証局同士の信頼基盤を構築して初めて日本における保健医療福祉分野での安全、安心な認証基盤ができあがる。

３）電子紹介状の記載項目様式に関する互換性確保

今回の実験では、紹介状の作成に目的を絞って電子署名を付与し、その正当性を確認する実験を実施している。紹介状の作成を目的にしたのは、署名押印のいる文書であること、また、医療情報交換のために最もよく活用されている文書であるからである。

実験を開始するに当たり、紹介状作成アプリケーションを開発するために、実際の紹介状のサンプルを幾つか収集した。その結果、書式や記載項目に相当の多様性が見られた。そのため、実験ではサンプルとして簡易な紹介状を作成するアプリケーションを提供するに留まった。今回の実験では趣旨が異なるため、この点において何ら問題や課題となることはなかったが、紹介状の記載項目に係わる様式だけでも、このような多様性があることが判明した。

今後、医療の IT 化を進め、各種の医療情報を電子化して行くにあたり、このような様式に多様性があることにより、正確なデータ交換が不可能となったり、記載事項の読み間違いなどによる医療の情報の安全性に影響が及ぶことも十分考えられる。

４）電子署名目的の拡張

今回の実験では、電子署名を付与する目的を紹介状の作成に絞り込んでいる。これは、署名押印の必要な文書であったこともあるが、紹介状を使えば医療機関同士での電子化された医療情報交換が実施できるからである。現場で実際に使えるものでなければ、IT 化の意味合いが実感できない可能性があることを考慮した。

しかし、医療の世界を見ると、医師の署名押印の必要な書類は、それ以外にも多く存在する。労災申請時に用いる診断書や死亡診断書、出生証明書などが、その例である。これら多くの文書は、行政機関に対して提出する文書である。

今回の実験では医療機関同士の情報交換であったが、将来的には国による電子政府の普及促進策も見据えながら、診断書などの電子化にも取り組む必要がある。その際、日医認証局の電子署名があれば正当な書類であると行政機関が認めるような実績を構築することも必要になってくると思われる。

５．まとめ

本研究では、本年度の日医認証局の取り組みを中心に取りまとめた。本年度は 3 年にわたる認証局の開発が完了し、実際に認証局を用いた実証実験を開始した。今までのシステム開発の段階から、実用に向けて動き出した年といえる。

実用に向けて動き出したことにより、新たに解決しなくてはならない問題が浮き彫りになってきた。それが認証基盤の「信頼の輪」の構築、電子署名検証ソフトのあり方、紹介状の様式に関する課題である。

今回の認証局の完成、実験の結果をもって、ただちに日医認証局の本格運用とはならないが、実用に向けた動きを契機として、今後も様々な課題が明らかになってくると想定される。それらの課題についても、仮説や目的を明らかにし、解決を図っていきたいと考えている。

文 献

1 厚生労働省:保健医療福祉分野 PKI 認証局証明書ポリシ、2005

2 矢野一博：医療分野情報ネットワーク構築に向けての基礎研究－日本医師会認証局の提言、日医総研ワーキングペーパーNo68、2002

3 矢野一博・増子厚：保健医療福祉分野における公開鍵認証基盤のあり方について－日医認証局の現状報告および公開鍵認証基盤の将来展望－、日医総研報告書第 73 号、2005

4 IETF/RFC3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework, 2003

5 ISO 17799-1:2000 Information technology - Code of practice for information security management、2000

6 IETF/RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols、1999
7 IETF/RFC 2560 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP、1999
8 IETF/RFC 3280 Internet X.509 Public Key Infrastructure: Certificate and CRL Profile、2002
9 US FIPS140-2(Federal Information Processing Standard) : Security Requirements for Cryptographic Modules (http://csrc.nist.gov/cryptval/)、2002
10 JIS X 5080:2002：情報技術－情報セキュリティマネジメントの実践のための規範(ISO/IEC17799:2000)、2002
11 電子署名および認証業務に関する法律（平成 12 年 5 月 31 日　法律第 102 号）
12 電子署名および認証業務に関する法律施行規則（平成 13 年 3 月 27 日　総務省・法務省・経済産業省令第 2 号）
13 電子署名および認証業務に関する法律に基づく特定認証業務の認定に係る指針（平成 13 年 4 月 27 日　総務省・法務省・経済産業省告示第 2 号）
14 ISO/TS 17090-1:2002 Health informatics - Public key infrastructure Part 1 : Framework and overview、2002
15 ISO/TS 17090-2:2002 Health informatics - Public key infrastructure Part 2 : Certificate profile、2002
16 ISO/TS 17090-3:2002 Health informatics - Public key infrastructure Part 3 : Policy management of certification authority、2002