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－

No. 68

平成１４年５月８日

日医総研　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　矢野　一博

キーワード

◆セキュアなネットワーク　◆PKI　◆認証局

◆認証と認定　◆日本医師会認証局

ポイント

◆ 医療分野の IT 化・ネットワーク化の流れは加速して行く。

◆ 医療で扱うデータは主に患者情報であり機密性が非常に高い。

◆ 機密を守るにはセキュリティを確保したネットワークを構築する必要がある。

◆ セキュリティを確保したネットワーク環境として PKI と言われるものがある。PKI で中心的役割を果たすのが認証局と呼ばれる機関である。

◆ 日医が主導権を持ってセキュリティが保たれたネットワークを構築して行くべきである。そのため、日医で認証局を立ち上げる必要がある。

目次

はじめに

近年、ネットワークを通して様々な情報をやり取りすることが一般的な行為として行なわれるようになってきた。銀行によるネットバンキング、インターネットを使ったショッピング、企業間の電子決算などが挙げられる。

ネットワークを使えば、家にいながらにして銀行に振り込みができ、欲しいものはインターネットで探して購入ができる。また、遠方から業者が集合することなく電子的に入札が可能となる。従来のネットワークを使わない方法に比べれば、格段に便利になったように思える。しかし、それとは裏腹に、ネットワークを使うことで新たな危険が発生してきた。その代表例が、「盗聴」「改ざん」「なりすまし」「否認」である。

そのような危険性があるにもかかわらずネットワーク化は勢いを増し続けている。この流れはどこか特定の分野に限らず、産業、医療、行政などあらゆる分野において言えることである。折しも、行政においては「e-Japan 戦略」によって、IT 化・ネットワーク化を IT 国家戦略として位置付け、その推進を図っているところである。

当然、医療分野においても各方面でネットワーク化や IT の活用が声高に言われるようになってきた。中でも、医療分野で扱うデータの守秘性や真正性の問題から、認証のあり方などについて言及されているところである。しかしながら、「具体的に医療分野においてどのように認証を行なうか？」という問題については、まだ具体的な方法や方向性は明確になっていない。それは認証システムの複雑さもあるが、医療に携わる人々・団体などの認証の範囲を明確にしにくいことも要因に挙げることができるだろう。誰をどこまで認証するのか、官・民混在した医療関係団体をどのように認証するか、患者までも含めた認証システムが必要になるのかなど考察すべき問題が山積みである。

また、医療分野においては情報化そのものの遅れが指摘されていることも事実である。統一化されたコード体系が整備されていない。医療情報交換の標準化が遅れている。法律による規制が存在する。そのような状況から、まだまだ医療自体がコンピュータ化しにくいと言う側面もある。医療事務処理については、比較的コンピュータ化が進んでいる分野であるが、各メーカ間で互換性もネットワーク化もされていない。

それでも、時代の流れとして医療分野もネットワーク化はその勢いを増して行くであろう。また、ネットワーク化することは今後の医療を考える時の重要なファクターであることも確かである。ただし、そこにはセキュリティの確保と言う重要な要素を組み込んでおかなくてはならない。

セキュリティを確保したネットワークを構築する技術は各種考えられている。それを医療分野で実現するにはどのような方法があるだろうか。本ペーパでは、セキュリティを確保した医療分野ネットワークの構築に向けてその手法を具体的に考えてみたいと思う。

まず第１章でネットワーク上でのセキュリティ確保のための技術を紹介する。第２章で現在のセキュリティネットワーク構築についての動向と予測を行う。第３章で医療分野におけるセキュリティネットワーク構築についてスキームを組み立てる。最後に、第４章でまとめを行うこととする。

第１章　セキュアなネットワークの概要

ネットワーク上に潜む危険

ネットワークを通じて情報をやり取りする時に、なぜセキュリティを考慮したネットワーク（以下、セキュアなネットワーク）を構築する必要があるだろうか。

ネットワークの特徴の１つにその秘匿性がある。情報は相手の顔を見ることなく、顔の見えないもの同士でやり取りされる。そのため、「盗聴」「改ざん」「なりすまし」「否認」といわれる危険が潜んでいる。

■ 盗聴

その名の通り、通信の内容を盗み取ることである。盗聴は電話回線で行われてきたが、ネットワークの通信でも同じである。ただし、ネットワークになると、電話の時のように単純に会話を盗み聴くだけではなく、通信している内容そのものを奪い取ることができる。例えば、Ａさんから Ｂさんに送信している文章を盗聴されると、内容全体が容易に外部に漏洩する。

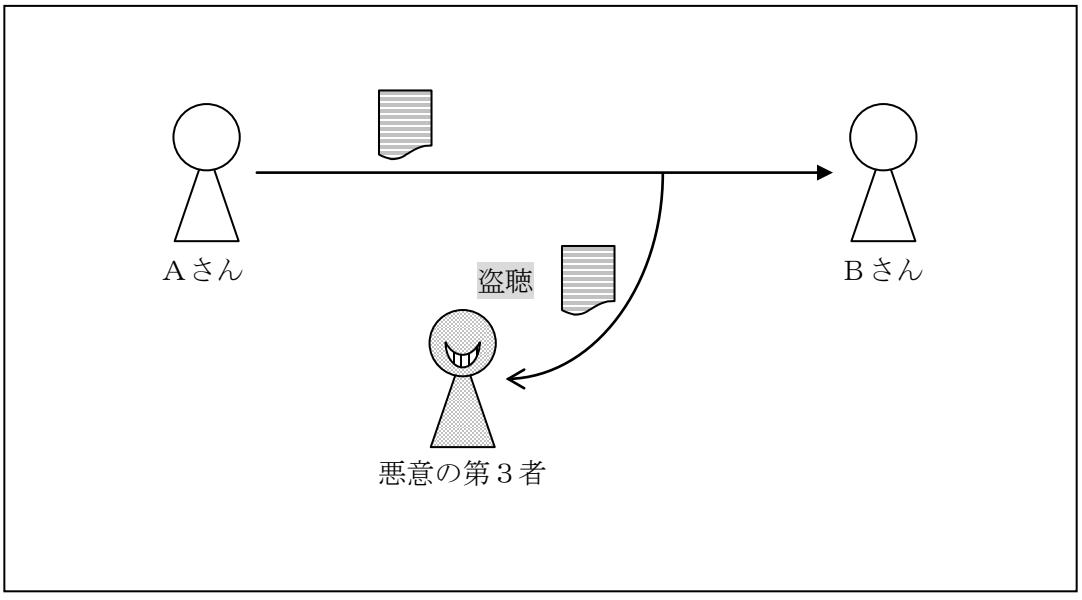


図１－１　盗聴

■ 改ざん

ネットワーク上でやり取りされる情報の内容を変更してしまうことである。例えば、ネットワークを介して銀行に振り込みをしている時に、振り込み金額を１桁改ざんするだけでも大変な損害を受ける可能性がある。

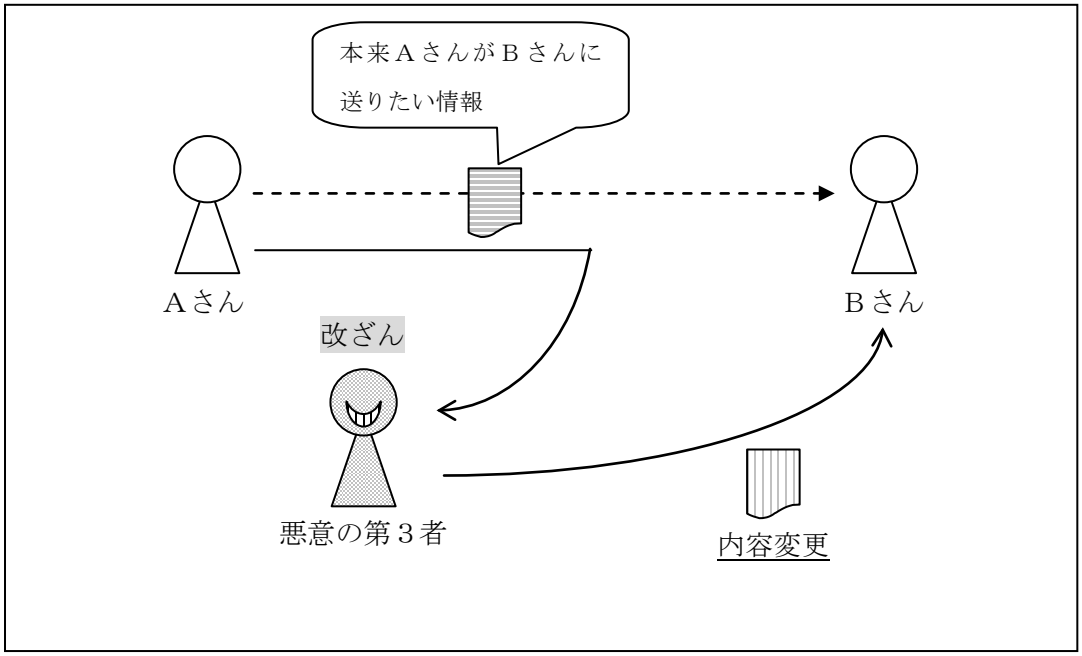


図１－２　改ざん

■ なりすまし

本人ではない別人が、その本人のふりをしてネットワーク上で振る舞うことである。本人になりすまし、インターネット上で買い物をして、代金の支払を本人にさせることもできる。また、どこかのホームページになりすまして、情報を盗み取ることも可能である。

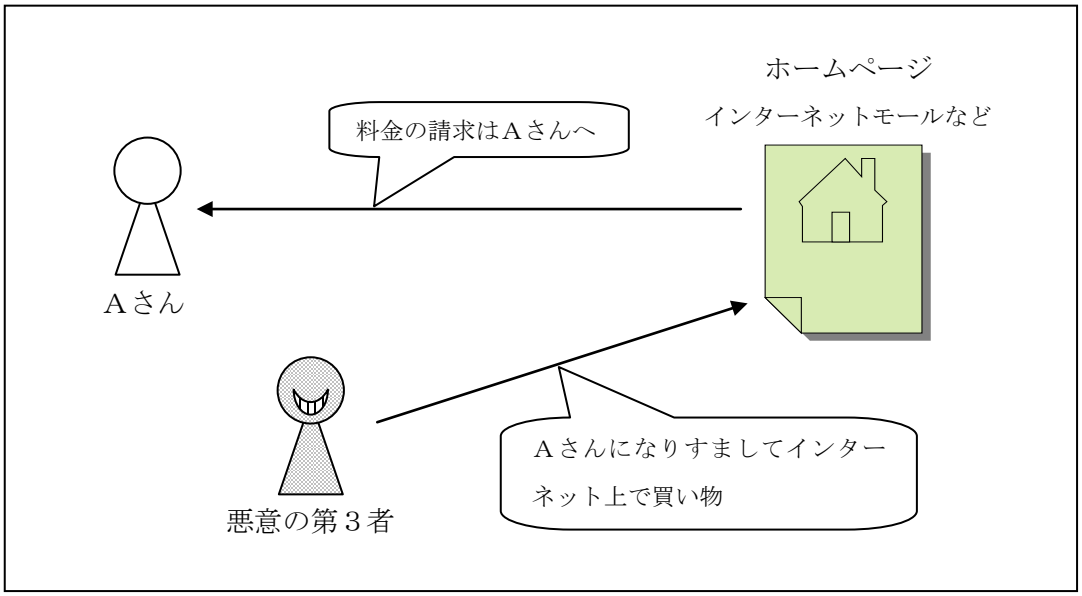


図１－３　なりすまし

■ 否認

「盗聴」「改ざん」「なりすまし」とは違い、本人が本人であることを認めないことである。例えば、インターネット上で買い物をした人に対して、その代金を請求したにも関わらず、そのような品物は購入していないと否認をするというようなことが想定される。

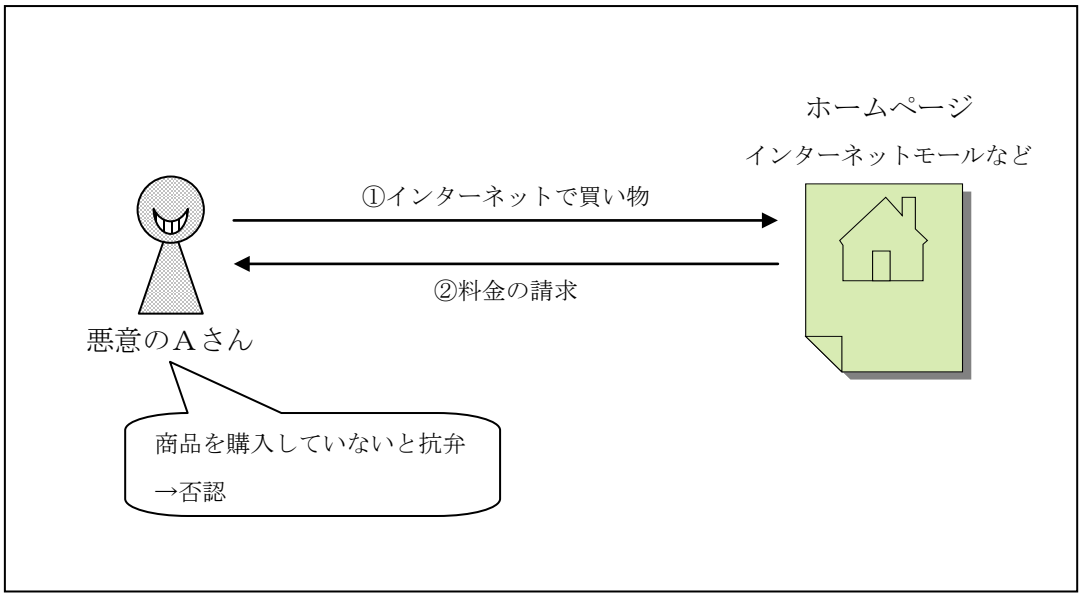


図１－４　否認

ネットワークを介して非対面で情報をやり取りする時には、上記のような危険が潜んでいる。また、「盗聴」「改ざん」「なりすまし」「否認」はそれぞれが単独に成り立っている訳ではない。ネットワーク上で「なりすまし」をして、他人の通信を「盗聴」するなどということが行なわれる。盗聴されていることが分かったとしても、誰かになりすまされていたら、盗聴をした個人を特定することは難しい。

医療従事者同士がネットワークで繋がれれば、当然、ネットワーク上を患者情報が飛び交う。また、個人同士の接続に限らず、医療機関同士、医療機関と検査施設など、組織同士で接続される場合も考えられる。この時、流れる情報が他人に盗聴されたり、改ざんされたりしたらどうなるだろうか。ネットワークを通じて、医療機関が他の医療機関に紹介状を送る。その紹介状が盗聴されれば患者のプライバシー情報は第３者に漏洩してしまう。ネットワークを通じて薬の処方を送る時に改ざんされた場合は、その患者の命に危険が及ぶ可能性もある。さらに、悪意の第３者が患者になりすまして医師に症状を問い合わせ、医師がそれに答えてしまうというようなことも想定される。それらは全て深刻な事態をもたらすことは容易に想像がつく。

このように、医療の分野ではセキュリティを確保した、セキュアなネットワークが非常に重要であると言える。

それでは、具体的にどのようにすればよいのであろうか。セキュリティに気を使って通信することは、個人レベルでも実現が可能である。ただ、いくら個人でセキュリティに配慮して通信をしたとしても、あくまでも個人のレベルでしかない。自分が信頼のおける人物と特定の通信をする場合のみに通じる話である。もっと大きな規模のネットワークで、それぞれが相互に通信相手を信頼できるネットワークの仕組みが必要になる。その仕組みが PKI である。

PKI とは何か？

PKI とは Public Key Infrastructure の略であり、日本では公開鍵暗号基盤（もしくは公開鍵基盤）と呼んでいる。これは、暗号化技術と電子署名技術を組み合わせ、ネットワーク上で安全な通信ができるようにするための環境のことを言う。

暗号化は文字通り情報を暗号にして送信する方法である。暗号方法は大きく分けて２通りある。従来からある暗号化と同じ考え方をコンピュータの世界に持ち込んだものと、従

来とは異なった考え方の暗号化の方法である。後者の「従来とは異なった考え方の暗号化の方法」は、ネットワークの世界だからこそ実現が可能な暗号化の方法である。その新しい暗号化の方法が「公開鍵暗号」と言う方法である。

通常、暗号といえば通信をするお互いが共通の鍵を持ち、その鍵を使って双方が暗号をかけたり解読をしたりする。例えば、ある文章を３文字ずらして暗号化するという暗号の場合、「３文字ずらす」という鍵[1]を双方が共有しておかなくてはならない。ネットワークの世界で暗号化する場合は、この鍵の受け渡しもネットワーク上で行われる。ネットワーク上で鍵を受け渡す途中で鍵を盗まれてしまうと、暗号をかけた情報も解読されてしまう。さらに、通信をする相手毎に鍵を保持しなくてはならないため、１００人と通信しようとすれば１００個の鍵を厳重に管理しなくてはならなくなる。インターネットでは、不特定多数の人と通信をするため、この方法は現実的ではなくなってしまった。そこで、この問題を解決する技術として、「従来とは異なった考え方の暗号化の方法」である「公開鍵暗号方式」といわれるものが考え出された。ちなみに、従来のように通信する双方が共通の鍵を持って暗号化をする方法を「共通鍵暗号方式」と呼んで区別している。

公開鍵暗号方式は、２つ一組の非対称の鍵を作成し、その片方を誰もが入手できるように公開してしまう方法である。公開する鍵を「公開鍵」と呼び、個人が保有する鍵を「秘密鍵」と呼ぶ。厳重に管理する必要があるのは、公開鍵と対になった秘密鍵のみである。情報を送る側（Ａさん）は、情報を受け取る側（Ｂさん）が公開している「公開鍵」を使って文章を暗号化する。Aさんが送った文章は情報を受け取ったBさんの「秘密鍵」でしか元に戻す（復号化[2]）ことはできない。ＡさんはＢさんの公開鍵を使って暗号化し、Ｂさんは自分しか所持していない秘密鍵で復号化を行うので、AさんとBさんの間で鍵のやり取りは発生しない。公開鍵暗号方式を使えば、鍵のやり取りを行わない通信を実現できる。

[1] 正確に言えば「３文字」が鍵で、「ずらす」はアルゴリズムと呼ばれ鍵ではない。説明の簡略のため鍵とアルゴリズムを同一とみなす。

[2] 「暗号化」に対し、暗号化された文章を元に戻すことを「復号化」と言う。

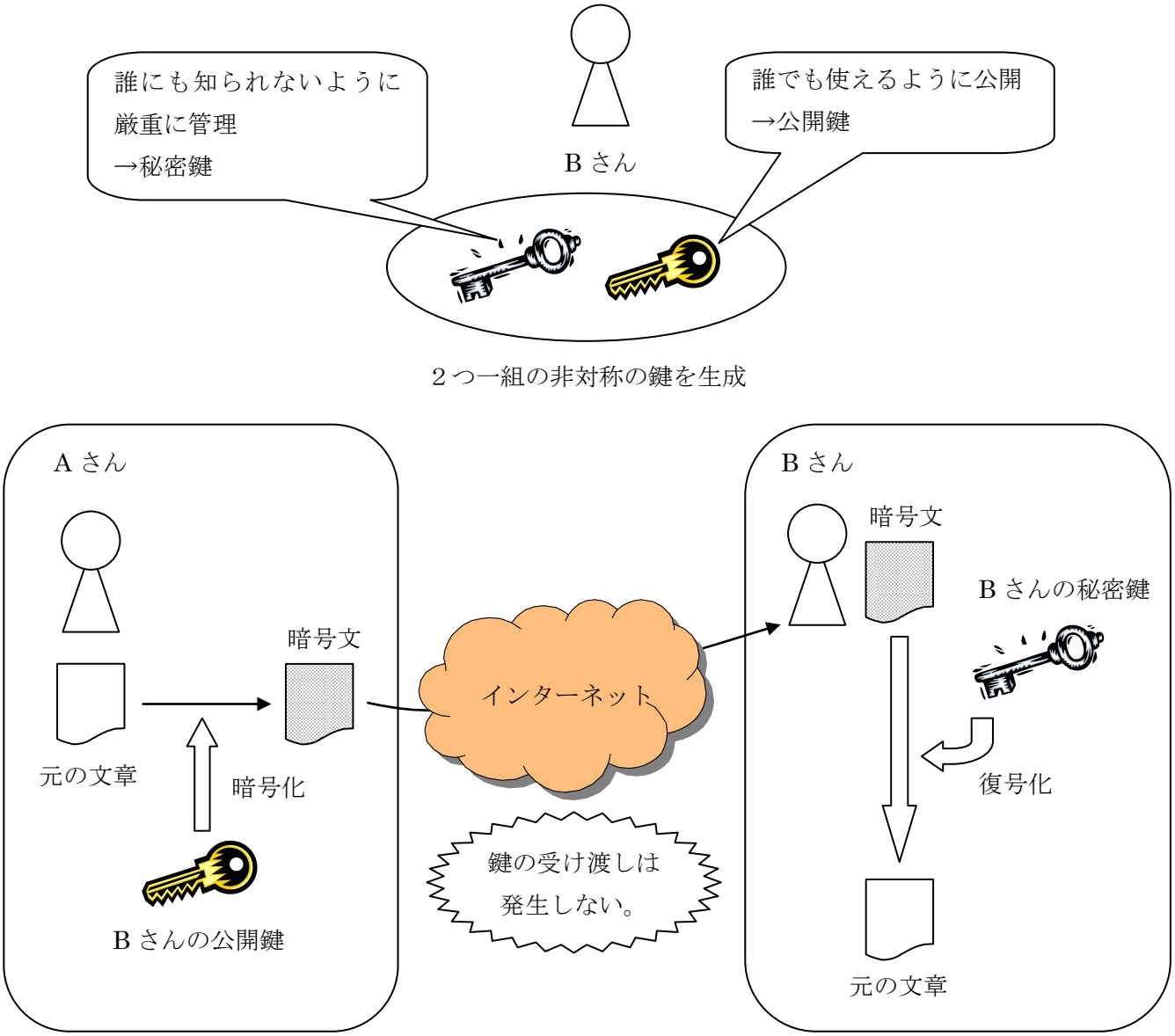


図１－５　公開鍵暗号方式による文章の受け渡し方法

逆に、Ａさんが自分の「秘密鍵」を使ってＢさんに文章を送ったとする。この時、Ａさんが送って来た文章はＡさんが公開している「公開鍵」でしか復号化することができない。これは、Ａさんの「公開鍵」を使えば、誰でもＡさんが送った文章の内容を確認することができるということである。このため、自分の秘密鍵を使って文章を暗号化しても暗号としては意味をなさない。しかし、Ａさんの秘密鍵で暗号化された文章はＡさんの公開鍵で

しか復号化できないという特性は利用価値がある。つまり、文章を復号化できたのは、文章が確かにＡさんの所持する秘密鍵で暗号化されたということの証明になるのである。

そこで、Ａさんの公開鍵を確かにＡさんのものであると証明する機関が存在すればその身元を保証することができる。Ａさんは秘密鍵で暗号化した名刺などを付けてＢさんに送れる。Ａさんの公開鍵で名刺を復号できれば、身元の保証されたＡさんだということが分かる。これが電子署名と言われる仕組みの基本である。Ａさんの公開鍵を確かにＡさんのものであると証明する機関は認証局と言われている[3]。

このように、公開暗号方式や電子署名、認証局などを組み合わせてセキュアなネットワークの基盤を形成する仕組みのことを PKI と呼んでいる。

PKI については、現在、政府も e-Japan 戦略の中で電子政府計画を立ち上げ、政府認証基盤（GPKI（Government Public Key Infrastructure））の構築を目指している。

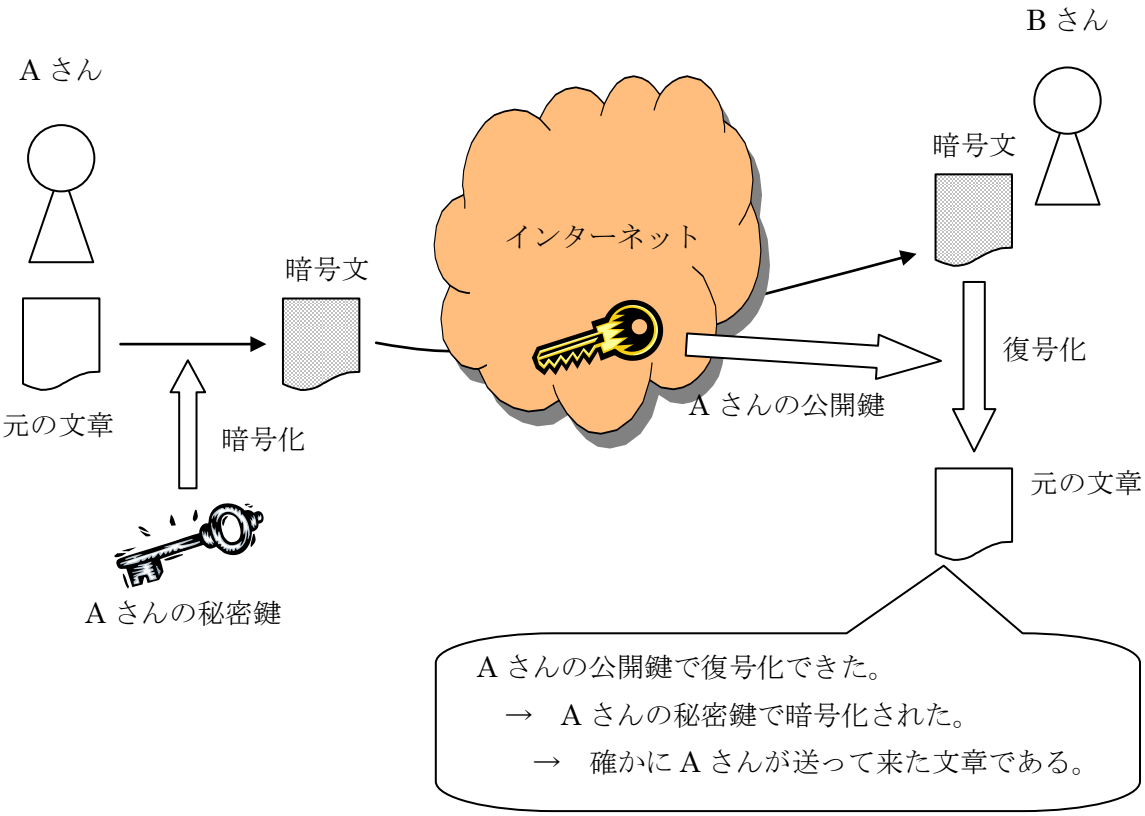


図１－６　電子署名の基本的仕組み

[3]実際の、電子署名は、その中に認証局の証明書が含まれていたり、暗号化した名刺も処理をしたものを確認するなど、上記のように単純ではないが、ここではその説明は割愛する。

認証局とはなにか

ＰＫＩの中で中核の役割を果たすのが認証局である。

簡単に言ってしまえば、認証局とはネットワーク上に存在する人間の身元や資格、組織を保証する機関である。現実の世界でいえば、印鑑証明を発行する役所であり、書類などの真正性を保証する公証役場と同じである。

認証局は身分保証のために電子証明書を発行している。同時に、証明書の発行申請の受付け、申請者の審査、証明書の有効性の管理なども行う。認証局で電子的な証明書を発行する業務を行なう機関を発行局（IA：Issuing Authority)、申請者の審査や登録の業務を行なう機関を登録局（RA：Registration Authority）と呼ぶ。登録局と発行局を合わせて認証局（CA：Certification Authority）と呼ぶ。

認証局が認証をするものは大きく分けて２つある。１つは一対一のやり取りで、本人保証をするもの。例えば、電子メールで電子署名をすることがこれに当てはまる。もう１つは複数に向けて自分の存在の確かさを証明するものである。ホームページを認証するのがこれに当てはまる。

第２章　認証の現状

政府と民間の動き

政府は行政関係の申請や各種届出の手続きをオンライン化する取り組みを行なっているところである。1997 年 12 月に「行政情報化推進基本計画の改定について」が閣議決定された。1999 年 12 月の「ミレニアムプロジェクト」では民間と政府の相互の行政手続きをインターネット経由で行なえる電子政府の基盤を構築することが決定された。2000 年 3 月の「申請・届出等手続きの電子化推進のための基本的枠組み」の中では、各省庁の中で、総務省・経済産業省・国土交通省については先行して府省認証局を整備することとされた。総務省ではこれらを相互に接続するブリッジ認証局を2000年度までに整備することとしている。

さらに、2001 年に入り、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）は、高度情報通信ネットワーク社会形成基本法（IT 基本法）に基づいて、1 月に「e-Japan 戦略」を決定した。3 月の「e-Japan 重点計画」では具体的な行動計画を定めている。この中で、2002 年度までに全府省において府省認証局を整備、立ち上げることとしている。また、6 月には「e-Japan 2002 プログラム」を策定している。

この中で認証について注目すべき点は、「公的個人認証基盤の構築」である。これは、2003 年から個人認証の実験を開始するというものである。認証は住民基本台帳のデータを元にして地方公共団体が行う。公的な個人認証システムの運用に備え、実証実験を実施し、法制面も含めた制度の整備、システム構築を行なうとされている。ちなみに、この個人認証は、現在、国会で審議中の個人情報保護法の成立後、実施に移される。

民間の場合、「日本ベリサイン株式会社」「ボルチモアテクノロジーズ株式会社」などが認証ビジネスを行っている。

上記に挙げた認証局などは国際的な信用があり、世界中で認証機関としてのシェアを拡大している。いわゆるデファクトスタンダードである。ただし、認証機関は信用のみで成り立っているため、認証をしたからといって法的に何らかの保証がされるというものではない。従って、利用者から民間の認証局に何らかの公的保証を与える必要性があるとの要望も高まってきていた。そのため政府は 2000 年に「電子署名及び認証業務に関する法律」（通称：電子署名法）を国会に提出・可決し、2001 年 4 月から施行している。これにより電子署名が手書きの署名や押印と同等に通用するものとされ、同時に、認証業務において

一定の水準を充たすものは国の認定を受けることが可能となった。認定を受けた企業は2002年3月29日現在5社となっている。(経済産業省ホームページ　認定認証業務一覧より[4])

また、それに先立って、法務省では「商業登記法等の一部を改正する法律[5]」の一部（商業登記法の一部改正関係）の施行に伴い、2000年10月から「商業登記に基礎を置く電子認証制度」の運用を開始している。これにより、法人代表者に対し電子証明書が発行できるようになった。

最後は企業内での認証の仕組みである。企業内では、本店と支店のような同一組織内でやり取りをすることが多い。例えば、物流産業ではネットワーク化が進み、品物の管理をネットワークを通じて的確に配置するということが行われている。その多くはネットワーク上の情報保護のためにセキュリティに最大の注意を払っている。企業はその企業内でのみ通用する電子証明書を作り、独自の認証局を立ち上げて運用している場合が多い。これは、外部に接続する場合は通用しないが、企業の中で閉じた仕組みであるのでセキュリティも高く、外部からの不正進入のリスクも少なくできるために有用な方法であると言える。しかし、一旦外部と接続を試みようとすると、互換性の問題などでシステムを全てゼロから再構築しなくてはならない場合があるなど必ずしも良い面ばかりとは言えない。

医療での認証

政府や民間では、認証に対する考え方がある程度浸透している。完全とは言えないまでも、その制度や基盤が整いつつある。では、医療での認証の現状はどうなっているのであろうか。残念ながら、医療における認証は非常に遅れを取っている。

医療分野のIT化は、世間に比べて20年遅れていると言われる。医療機関にはレセプトコンピュータと言われる医事会計専用のコンピュータが約80%もの割合で普及している。その他にも、病院であればオーダリングシステムに見られるように、コンピュータの導入は比較的進んでいる。しかし、これらは大抵ネットワーク接続されず単独で動作している。その意味では、このような状況でネットワーク上で自分自身を保証するという認証そのものを論じる場がなかった。しかし、ここ近年、医療のIT化は着実に進められようとしてい

[4] http://www.meti.go.jp/policy/netsecurity/digisign_ninteiitiran.htm
[5] 2000年4月　公布

る。

まず、2001 年 6 月 26 日に医療機関経営の近代化・効率化を目指し、医療サービスの IT 化の促進、電子カルテ、電子レセプトの推進が閣議決定された。経済財政諮問会議によるいわゆる、「骨太方針」の中である。続く 9 月 14 日の IT 戦略本部の中で、先に策定された、「e-Japan 重点計画」および「e-Japan2002 プログラム」の加速、前倒しが了承されている。その中で電子カルテ、レセプトの電算化等のための具体的な普及目標、期限、普及方策を明示した医療情報化のためのグランドデザインを年内に策定する方針が決められた。それを受けて、9 月 25 日に厚生労働省から「厚生労働省医療制度改革試案」が公表された。これは、2002 年度から 5 年間の保健医療の情報化計画・目標達成のための道筋と方策を示したものである。11 月 29 日には「医療制度改革大綱」が政府・与党改革協議会で取りまとめられた。この大綱の中では、電子カルテ等について目標と達成年次を年内に策定し、その実現に向けた支援措置を講じることとされている。

上記の流れを受け、2001 年 12 月 26 日、「保健医療分野の情報化にむけてのグランドデザイン」が策定、公表された。グランドデザインは、2002 年から 5 年間の情報化計画と具体的戦略を盛り込んだものとされている。その中心に位置付けられているのが、電子カルテとレセプト電算処理システムの普及であり、それぞれについて目標と達成年次を設定している。電子カルテは、2004 年度までに 2 次医療圏毎に最低 1 施設に導入、2006 年度には全国 400 床以上の病院と全診療所それぞれに 6 割以上の普及を目指すとされている。レセプト電算処理システムについては、2004 年度までに全国の病院の 5 割以上、2006 年度までには 7 割以上の病院に普及させるものとしている。また、それぞれの目標達成のために、達成目標等を明示したアクションプランを策定している。

このグランドデザインの中でも、認証について触れられていた。8 ページ目に以下のように紹介されている。

個人・資格認証システム 医療情報システムを用いて検査や処方などを行う際に、医師等の資格確認を電子的に行うシステム。今後は被保険者証をＩＣカード化し、医療施設を受診した際にオンラインで被保険者の資格を確認したり、住所・氏名などの個人情報をカルテ、レセプトへ自動的に転記をしたりすることへの応用が検討されている。

また、アクションプランの中では、その 4 ページ目に、医療公開鍵インフラストラクチャを整備するとし、以下のように述べている。

> 個人認証ならびに資格認証
> 診療に関連した情報がインターネット等によって安全に交換できるためには、公開鍵インフラストラクチャ（PKI）などの認証に関する社会的基盤が必要である。現在、政府機関の間にはこのような社会的インフラストラクチャが整備されつつあるが、医療は、公的機関と私的機関が混在する世界であり、医療の世界で用いる「医療公開鍵インフラストラクチャ」が必要である。そのため平成 15 年度までに、認証に関する社会基盤をどのように整備していくか、その方向性と計画を明らかにすることとする。

つまり、電子カルテ、レセプト電算処理などに関しては具体的な達成目標を掲げているが、認証に関しては社会的基盤を整備するための方向性と計画を策定すると目標を掲げたのみである。具体的にどのようにするというところまでは言及されていない。

今後の医療ネットワークの予測

ここまで述べてきたように、官・民問わず IT 化は加速していると言える。数年前であれば、一般家庭でインターネットをするために、複雑なコンピュータの設定が必要であった。接続できたとしても、その回線速度は画像を表示するのに耐えうるようなものではなく、文字による通信がメインであった。

それが、近年になりインターネットを利用する人々が急速に増加している。2001 年 2 月の時点で日本におけるインターネットの利用者数は 3263.6 万人に達し、前年比で 168.43%の伸びを示している。この中には、最近出てきたインターネット接続可能な携帯電話や PHS の利用者も含まれるが、利用数は着実に増加しており、2001 年末では 3628 万人に達すると予測されていた。これは、全人口の 1/3 近い数になる。接続形態も常時接続を導入する家庭が増えつつあり、通信速度もより高速なものが普及してきた。いわゆるブロードバンド化が確実に進んでいるのである。さらに、従来に比べ、接続料金もより安価になってきている。インターネットの利用者数は増加を続け、今後もこの傾向が続くことは確実であると言える。

その反面、セキュリティに対する不安意識も高く、インターネットを利用する約 7 割の人達が「不安や問題、危険を感じる」としている。不安や危険を感じる分野として「ウェッブ上での情報の取り扱い」（64.3%）、「ウェッブ上で取り扱われている製品／サービス」（35.6%）、「ウェッブサイトの情報内容」（35.0%）が挙げられている。つまり、インターネットへの個人情報の流出や濫用を懸念する傾向が最も強い。この傾向は、そのまま医療情報をネットワークで提供する場合も当てはめることができる[6]。

ネットワークを活用した医療ビジネスでは、「eヘルス」と言われる医療情報や医療機関情報の提供を目的としたサービスが開始されている。ホームページを使って情報を提供するWebサービスの幾つかを挙げておく。WebMD[7]と言うホームページでは、2001 年から医師向けの会員サービスを開始した。MEDWEB[8]は全国で 20 万件にのぼる医療機関のデータベースを検索したり、インターネットで医療相談を受けられるホームページを紹介するサービスを提供している。WebDoctor[9]では、医療機関の検索、インターネットでの医療相談、薬剤情報の提供なども行っている。

最近では、商用サービスとして ASP（Application Service Provider）方式で、ネットワークに接続した端末へ電子カルテを提供するというサービスまで登場してきた。しかし、ASP を利用した電子カルテの商業サービスについては、実際に患者の情報を保持するのが企業側であり、個人情報保護の観点からも議論が必要であると言う声も高い。

医療における広告については医療法で広告規制があり、その広告の仕方については規定・制限がされている。しかし、インターネットを通じての広告については、規制そのものが曖昧であり独自に情報提供サービスが行われている。行政でも問題視はしているようである。最近、インターネット上での医療関係の広告について、そのあり方を検討し、ガイドラインを作成しようとする動きがみられる。

民間の方が対応が早く、1998 年に日本インターネット医療協議会（JIMA：Japan Internet Medical Association）と言われる組織が設立された。これはインターネット医療の適正な利用を普及し、ひいては国民の医療・福祉の向上に貢献することをうたっている。この組織では、トラストプログラムと言われるものを開始している。ウェブサイトのコンテンツや個人情報保護に関する自己評価情報を開示し、所定の審査を受け許可された場合にホー

6 データは「インターネット白書 2001」（インターネット協会監修）を参照
7 http://www.webmed.ne.jp
8 http://www.medweb.ne.jp
9 http://www.webdoctor.ne.jp

ムページに掲載する JIMA 指定のトラストマーク（認定マーク）を発行している。上記に挙げた MEDWEB や WebDoctor などは、このプログラムに参加している。

以上のような例は、多くが個人情報を扱うものであり、その扱い方、セキュリティに対する問題について細心の注意を必要とする。現在、2003 年から施行される個人情報保護法が国会で審議中であるが、医療における個人情報保護法の適用についても様々な議論がされているところである。この議論については、実際に医療機関が持つ紙ベースのデータだけではなく、ネットワークを通じての医療情報の扱いについても注意深く検討して行く必要があると思われる。

いずれにせよ、今後もこのような流れはとどまることはなく医療における IT 化も他の分野と同様に進んで行くことは確実である。ネットワークを通じて様々な情報を収集・配信する限り、そのセキュリティ確保が重要な要素であることは間違いない。

第３章　医療分野における認証局の提言

認証の必要な場面と認証の種類

医療分野でネットワークを構築する上で、セキュリティの確保が重要である。では、実際に行われる情報のやり取りの中で、どこに認証が必要になるのか例を図で示してみる。図３－１中で実線の矢印が認証の必要な行為である。

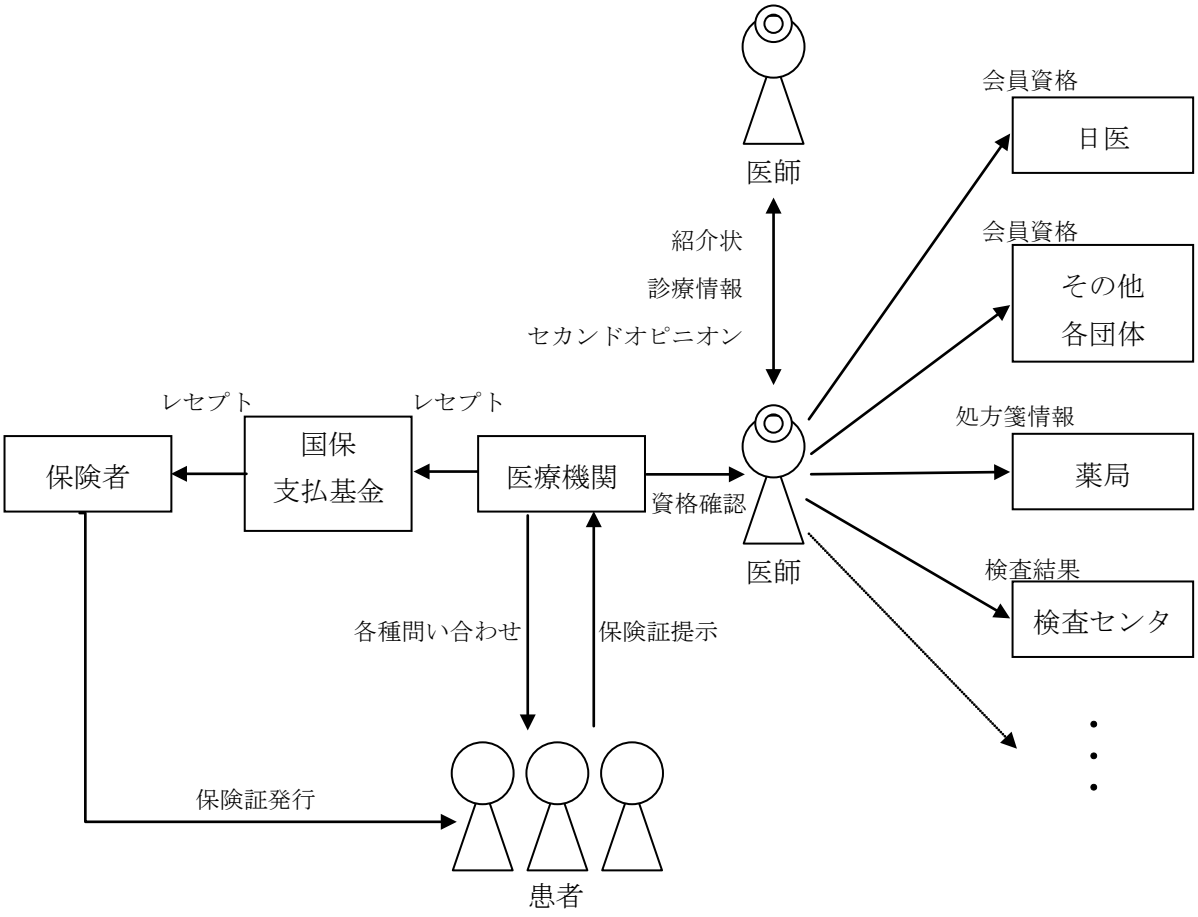


図３－１　認証の必要なやり取りの例

例１　レセプト電算処理

レセプトを提出する場合、レセプト用紙とは別に医療機関と管理者（院長など）の印鑑を押した用紙を同時に提出する。厚生労働省が推進しようとしているレセプト電算処理（レセ電算）を行う場合、この印鑑に相当する証明が必要になる。証明をするために電子署名が必要となり、その署名の確かさを証明す

るために認証局による認証が必要になる。

例２　紹介状の送付

ネットワークを通じて医療機関から他の医療機関に患者を紹介する場合、紹介状を受け取った医師は、紹介状の送り主が確かに本人であり、医師であるということを確認する必要がある。医師による電子署名が必要になり認証局による認証が必要になる。

例３　検査データの閲覧

ある検査会社がネットワークを通じて検査結果を医師に対して開示する場合、検査会社は開示する相手が確かに検査を依頼して来た医師であることを確認しなくてはならない。この時、医師による電子署名の認証が必要になる。検査会社にアクセスする医師も、検査会社が確かにその検査会社であると確認を取らなくてはならない。ここでも認証が必要になる。

このように医療で情報をやり取りする場合、そのほとんどの場面で認証が必要になる。しかし、上記の例でも分かる通り認証をする対象は複数存在する。

情報を発信する個人を認証する「個人認証」、資格を認証する「資格認証」、会社や団体などの組織を認証する「組織認証」である。これを医療分野に当てはめると、個人認証は医療に携わる個人を認証する。資格認証であれば、医師・看護婦・各種検査技師・薬剤師などが挙げられる。組織認証であれば、診療所・病院・臨床検査施設・保険者などである。医師会であれば資格認証として医師会員も含まれる。ただし、ここに挙げた例以外にも様々な資格や組織が存在する。

個人認証は本人確認をすればよい。ただし、その個人を認証するための情報がどこに存在するかが問題になる。国民であれば市町村長が作成する住民基本台帳に必ず登録されている。e-Japan 計画の中で検討されている個人認証がこれを元にして作成されようとしている。ただし、この計画はその是非はともかく、以前から議論されている国民総背番号制を導入することに等しいもので、今後まだまだ国民的な議論が必要であると思われる。

そうなると他に個人情報を所有しているところを考える必要がある。この場合、個人認

証は資格認証と密接に絡み合う。つまり、医師であれば医師の資格と共に医師個人の情報を厚生労働省が保有している。看護婦も同様である。各資格についても、その資格の認定機関が存在し、資格と共に個人の情報を保有している。医師会であれば、医師会員の資格と共に医師の個人情報を保有している。現実の世界では、個人情報は様々な場所に重複して保有されているのである。医師で医師会員になっていれば、厚生労働省と医師会に個人情報が存在する。従って、個人認証と資格認証は切り分けることが難しい。

組織認証はどうであろうか。組織の場合は、例えば厚生労働省と日本医師会が通信をする時に、厚生労働省から見れば確かに相手は日本医師会であり、日本医師会からみれば確かに相手は厚生労働省であると確認できれば問題ない。

ただ、厚生労働省に所属する人が日本医師会に所属する医師に情報を伝達する場合は話しが変わってくる。情報を受け取る医師は厚生労働省に所属する人から情報を受け取った時、その人が確かに厚生労働省に所属し（組織認証）、厚生労働省の役人の資格を持ち（資格認証）、確かにその人である（個人認証）ことが確認できなくてはならない。

単純に個人・資格・組織と認証を切り分けたとしても、現実世界ではそれぞれが密接に関連しており単純に分離して考えることは不可能である。

民間の認証局であれば、自分を認証してもらいたければ個人で申請をして認証を受けることができ、組織であれば商業登記簿などを提出して組織の認証をしてもらうことができる。当然、個人情報も組織情報も民間の認証局に一元的に保有されている。一番理解しやすい認証の形態にはこのスキームを使えばよい。医療分野としての認証を一認証局で一元的に管理し、個人情報、資格情報、組織情報をその認証局で保有することである。しかし、その認証局を構築するとなると、どこが認証局になるかと言う問題がある。また、認証をするには保有するデータが正確なものでなければならない。そうなると莫大な量のデータを、常に最新で正確なものにしておくための仕組みをどうするかなどの問題も生じる。さらに一元的に全ての情報を保有することは権威の象徴となり、政治的な問題も解決して行かなくてはならない。そのため大規模な一元管理をする認証局はあまり現実的とは言えない。

その問題を解決するには各組織が認証局を構築する必要がある。しかし、闇雲に各組織が認証局を構築したとしても、各組織が立ち上げた認証局の中では認証ができるが、それ以外の組織に所属する人が認証されなければ意味がない。

医療分野で認証局を立ち上げるならば、このような非常に複雑な要因を整理して解決する必要がある。それをどのようにすればよいか、考えを述べていく。

認証と認定

今までは認証するということに焦点を絞って話を進めて来た。ただし、単純に認証と言う一言でまとめてしまうと複雑な要因の切り分けが難しい。そこで、これ以降は認証と一言でまとめるのではなく、認証（Authentication）と認定（Authorization）と言う切り分けを考える。

■ 認証

認証とは、ネットワーク上でその人に間違いないと証明することである。

■ 認定

認定とは、ネットワーク上でその人がどのような資格があるのか、どのような組織にいるのか、何を実行することができるのかを定めることである。認定は認証をした上で初めて意味を持つものになる。

これはパスポートとビザの関係に似ている。パスポートはあくまで個人を同定する手段であり、個人に関する必要最低限の情報しか所有していない。パスポートを提示することで身分証明をすることができる。一方、ビザはパスポートに付随しており、パスポートを所持している人が観光用ビザを持っていれば、観光はできるがビジネスをすることはできない。ビザはその人が何をすることができて、何をすることが規制されているのかを定めたものである。これをふまえた上で再度話を整理する。

認証対象は認証と認定と考える。認証は本人確認であり個人認証のことだけとなる。資格認証や組織認証は認定となる。そこで、資格認定と組織認定と言いかえる。これを医療分野に当てはめると、個人認証は医療に携わる個人を認証するものである。資格認定は、医師・看護婦・各種検査技師・薬剤師などが挙げられる。組織認定は診療所・病院・臨床検査施設・保険者などである。医師会であれば、資格認定として医師会員も含まれる。

診療所から病院に紹介状を送る場合を考える。この場合、病院は診療所の医師から紹介

状を受け取った時、その人が確かに診療所に勤務している医師であり、確かにその人であることを確認する。これを紹介状を例にとって認証と認定から整理すると以下のようになる。

1. 病院は受け取った紹介状が、確かに情報発信者からであるか個人認証をする。
2. 個人が認証できたら、医師の資格と勤務する診療所が、その個人に付随した情報として認定されているか確認する。

このように、認証と認定を明確に切り分けることにより認証のスキームをはっきりとさせることができる。

次に、認証と認定を行う認証局をどのような構成にし、どのようにおこなって行けば良いかを考える。

認証局の構成

まず、認証局の構成を考える。認証局の構成としては「単純階層モデル」「メッシュ型モデル」「ブリッジ型モデル」の 3 タイプが考えられる。それぞれの構成は以下のようになる。

■ 単純階層モデル

全てのデータを一元的に保持管理する方法である。全てのデータを管理し、個人・資格・組織の認証と認定を一元的に扱える。ユーザは常に一ヵ所にアクセスすれば良く管理が容易になる。

ただし、全てを一元的に管理するためデータの量が莫大になり、医師が病院を移った、新たな医師が加わったなどのトリガがあった場合、常にデータを最新の状態に保つための保守管理の手間が非常に大きい。また、規模が大きくなればなるほどデータ更新の頻度も増し、常にデータを更新しているような状態にもなりかねない。さらに、一元集中しているので大元の機能がダウンした場合は全てのユーザに影響が及ぶ。

■ メッシュ型モデル

それぞれ組織や役割ごとに認証局を立ち上げ、それぞれの認証局同士で認証を行う仕

組みである。

この場合、日本医師会であれば日医会員のための認証局を立ち上げればよい。他の機関が認証局を立ち上げた場合は、認証局同士で相互に認証をすればよい。日医会員のＡさんの身元は、相互認証している認証局の中であればどこでも保証される。

ただし、この場合、認証をする仕組み（データの持ち方）を予め共通のものにしておかないといけない。

ある認証局では、「氏名」「住所」「電話番号」だけで認証するが、別の認証局では、「性別」まで加えないと認証できないとなっていた場合、相互に信頼関係があったとしてもＡさんの身元は完全には保証されない。

■ ブリッジ型モデル

ブリッジ型モデルは、相互に認証可能な認証局を中間に１つ立ち上げる。この場合、相互にそれぞれ認証をするのではなく、ブリッジ認証局とそれぞれの認証局が認証を行う。政府で立ち上げている GPKI は、各省庁間の認証にブリッジ認証局を利用している。

ブリッジ認証では、それぞれの認証局は相互に認証をせず、ブリッジ認証局と相互認証を行う。

しかし、ブリッジ認証でも保持するデータが大きくなるため、トップダウン認証と同じような問題が生じる可能性がある。

表３－１で構成をまとめておく。また、表３－２ではそれぞれのメリット・デメリットをまとめておく。

表３－１　認証局の構成のまとめ

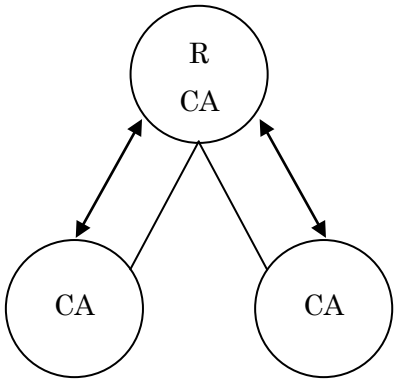
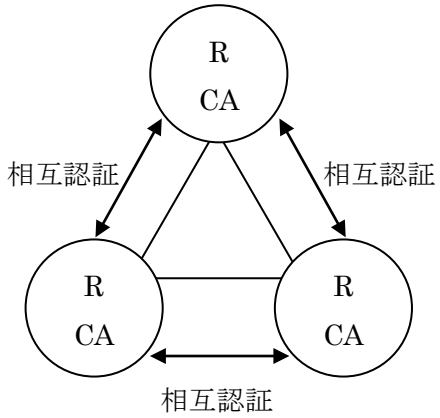
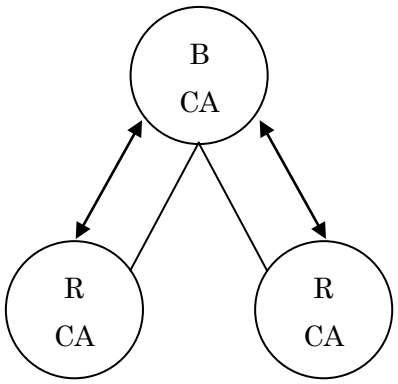
	認証タイプ	概要
単純階層モデル		全ての情報を保持するトップ認証局（Root CA）を立ち上げ、それぞれの CA が従属する形。 ※R CA＝Root CA
メッシュ型モデル		それぞれが Root CA を立ち上げ、Root CA 間で相互に認証を行う。
ブリッジ型モデル		ブリッジ CA が、それぞれに立ち上がった Root CA を認証する。 ※B CA=Bridge CA

表３－２　それぞれの構成のメリット・デメリット

	医療分野への適用	セキュリティ	拡張性
単純階層モデル	各種関係団体・資格が多く、最初からこの構造を作ることは困難。	閉じた認証のモデルであるので、セキュリティ上は安全性が高い。	当初から規定された認証ヒエラルキーの中で動作するため、拡張性は低い。
メッシュ型モデル	各種団体が独自に立ち上げたルートCA間で相互に認証を取り合うため調整が困難な場合がある。	認証体系が複数に渡るため、運用時のミスによるセキュリティホールの可能性はある。	新たにルートCAが立ち上がった場合、それぞれのルートCAとの相互認証さえ行えば拡張可能。
ブリッジ型モデル	各種団体のルートCA間にブリッジというクッションを設置する。それぞれのルートCAは独自に運用・管理しブリッジCAに接続することにより相互に認証する。	認証体系が複数に渡るため、運用時のミスによるセキュリティホールの可能性はある。	新たにルートCAを立ち上げた場合、ブリッジCAから認証を受けるだけで拡張できる。

認定の権限分散

認証局の構成には３タイプあった。認証は、これらのどの構成にしたとしても最終的にどこかが個人を特定して身元を保証する仕組みが必要となる。

認定に関しては、これらの仕組みの中に含めても、別なところに認定権限を委譲しても構わないだろう。

認定と言うのは、それぞれ各組織が独自に行うものであると考える。医師資格などの国家資格については、独自に行うという性質のものではないので、厚生労働省や医師会が医師資格を一元的に認定しておけばよい。ここで問題になるのは、さらに細分化された認定権である。例えばある医療機関で医師を雇用して患者を担当させた時、医師は担当患者の

カルテに自由に閲覧書き込みができなくてはならない。ところが、別の医師によって自由に書き込みができたならば問題になる場合もある。この場合、医療機関の責任者はＡ医師とＢ医師の行動を規定して認定しておく必要がある。この認定を一元的にまとめて、どこか大きな組織が管理するということは難しい。そこで責任者が権限者になって、自分の管理する組織内の認定権限を設定する。これが認定権限を委譲すると言う意味である。

つまり、セキュアなネットワークを支える根幹の認証はできる限り集中させて、それぞれの権限については権限を持つ機関に任せるというスキームを構築する。図３－２はそのイメージ図である。図３－３は認証と認定の構成を示した図である。

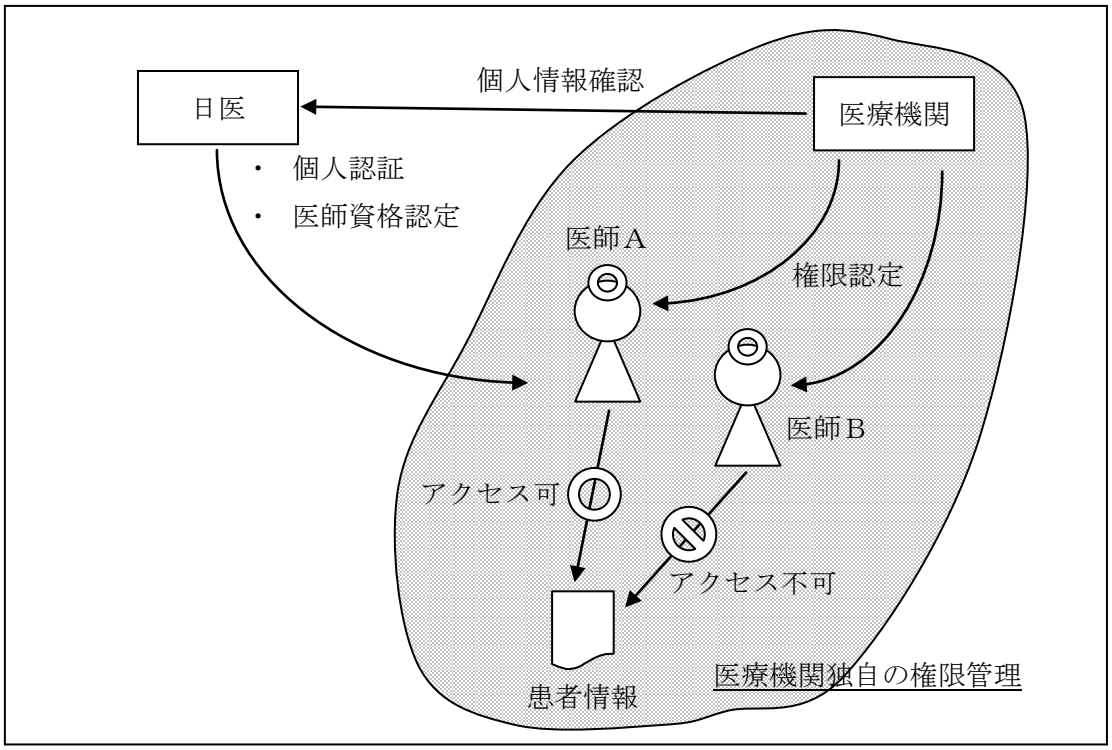
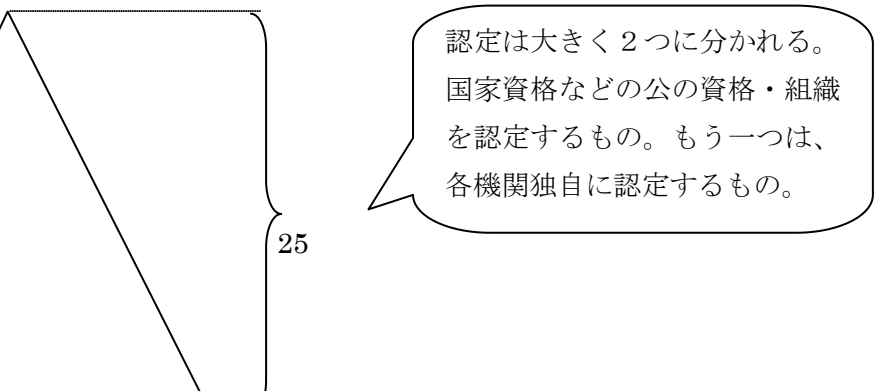


図３－２　認定委譲イメージ



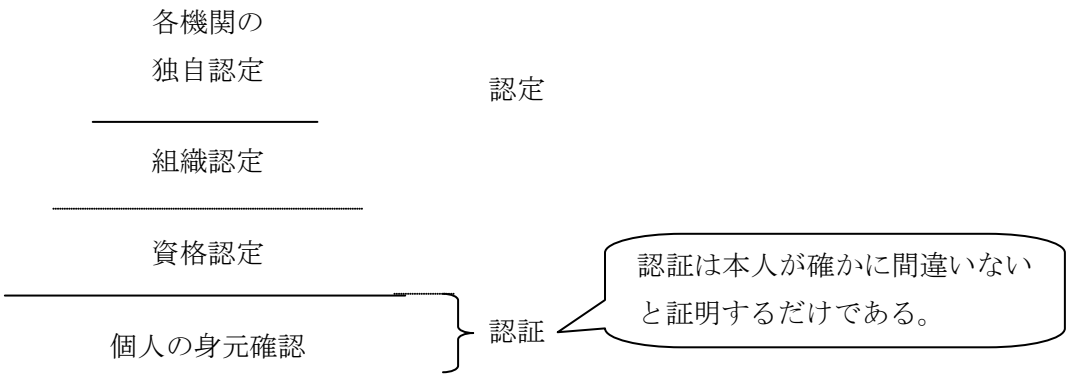


図３－３　認証と認定の構成

医療分野認証局のスキーム

認証と認定を切り分けた上で、医療分野認証局のスキームを提案する。

1. 認証はできる限り集約する

個人情報を所有し、個人を審査しうるだけの機能が必要になる。つまり、認証局の中の登録局を運営していけるだけの組織が認証を行うべきである。当然、日本医師会であれば十分に登録局の運営は可能である。

発行局については、適用範囲や証明書の認知度、汎用性を十分考慮した上で独自に構築するか、外部に委託するかを検討する必要がある。

2. 認定は分散して管理する

誰がどこまで権限を付与するのかを検討し、権限を決定する機関が認定権を持つ。医師資格や看護婦資格など国家資格またはそれに準じる資格についてはある程度集約する必要があるが、それ以外の認定権限については分散して保有することが望ましい。

3. ルート認証局の形態

ルート認証局は認証を行う機関が運営する。相互の認証に関しては、以下の２通りのいずれかにする。

1. 認証の共通規格を定め、それに則った形で認証局を立ち上げるルールを決める。ルールに則って相互に認証を行うメッシュ型認証とする。

2. 政府のブリッジ認証局に相互接続をするか、医療分野ブリッジ認証局を立ち上げることによって相互の認証をする。

このようにして認証をヒエラルキー型、認定を分散型とすることで現実世界に即した認証基盤を構築することができると考える。

日医における認証局の構築例

日医で認証局を立ち上げる場合、どのような形態にするか一例を挙げておく。まず、日医は既に会員情報を保有しているので、これを元にして日医会員の認証ができる。日医会員は医師であるので医師資格の認定ができる。これに追加して、日医会員資格の認定も行う。ただし、各都道府県医師会などの会員資格については日医で行うのではなく、各都道府県医師会に権限を委譲する。権限を委譲することにより、各医師会の独自性が確保できる。

例えば、医師は日医が提供する情報を取得したい場合、日医の情報提供先にアクセスをし、日医が発行した証明書により認証を受け、会員資格の認定を受ける。それをパスすれば医師は日医の提供する情報へとアクセスが可能になる。

また、A 医師会が独自に A 医師会の会員に向けて情報を提供する場合、A 医師会の会員は日医発行の証明書から個人の認証と医師資格を認定してもらう。A 医師会は認証と認定をパスした医師に対し、A 医師会へのアクセス権限の認定を行い、A 医師会の会員にのみ情報を提供するようにする。A 医師会が医師の認証を行うには、日医の認証局に問い合わせを行えばよい。

医師が紹介状を送るケースも考えてみる。A 医師が B 医師に紹介状を送る。受け取った B 医師は、A 医師の身元と資格を確認する。これだけであれば、A 医師が予め日医から証明書を発行してもらっておけばよい。ここで A 医師の勤務する医療機関の確認が必要になるとする。この場合、A 医師の勤務する医療機関が A 医師を認定する。B 医師は A 医師の勤務する医療機関に A 医師が確かに医療機関に勤務しているか確認をする。もし、医療機関で A 医師を認証する仕組みを持てなかった場合、認定の権限をどこかに委託することも可能である。医療機関のある地域医師会が各医療機関をまとめて認定権を持つことも可能で

ある。つまり、認定権は地域で閉じることもできる。

このように、認証を日医で行い、認定を分散させることにより認証方法の自由度が高められる。

第４章　まとめ

これまでの話を以下にまとめておく。

1. 「盗聴」「改ざん」「なりすまし」「否認」の危険性がある以上、ネットワークはセキュリティを十分に考慮して構築する必要がある。医療分野のネットワークでは、患者情報を中心に扱う。従って、セキュリティは通常のネットワーク以上に強固なものでなくてはならない。セキュリティを確保する１つの方法として医療分野 PKI を構築する必要がある。

2. PKI の中で中心的な役割を果たす機関が認証局である。認証局はネットワーク上に存在する人間の身元や資格、組織を認証する。医療分野で医師や他の医療従事者を認証する認証局を立ち上げるべきである。

3. 医療分野には様々な資格が存在している。この切り分けを十分に考察しておく必要がある。従来のように単純に認証という一言でくくってしまうと役職や組織の切り分けが難しい。そこで、認証と認定を明確に切り分けて考えた。

4. 官・民が混在し、様々な組織が存在する。個人情報も各組織に分散して保有されている。そこで、一元的な認証局で個人を認証することは現実的でない。各組織間で相互に認証をするメッシュ型認証か政府認証基盤で導入しているブリッジ型認証を導入するのが適切であろう。

5. 資格の認定権限は各組織に帰属している。この権限を集中させることは難しい。そこで、認定権限は分散させることにする。

6. 日医は医師の個人認証と医師資格認定、会員資格の認定が可能である。登録局の役割は既に果たしている。医師のための認証局を立ち上げることは難しくない。

7. 各地域医師会は各地域の医師の情報を保有している。また、地域毎に独自のコンテンツを提供している。地域医師会は、それぞれの地域の特性に応じた認定権限を持つことが望ましい。

医療分野のセキュアなネットワークを構築するには、医療分野認証局とでも呼ぶべき機関を構築し、その構成は各組織の認証局をつなぐものにする。個人の認証は医療分野認証局にできる限り集約する。それぞれの資格については、資格認定機関が責任を持って認定をする。

日医はその医療分野認証局の主導的立場に立ち、医師を認証するための認証局を構築するべきである。また、各地域医師会はそれぞれの独自色を発揮できるようにする。そのため、各種の認定権限を持つ仕組みにする。

医師はどこかの組織に一元的にまとめられるのではなく、自分の所属する機関から適正な権限を付与される。医師の認証がどこか一個所に固定されることで情報へのアクセスの自由を奪われてはならない。

最後に、まとめとして図４で全体像を示しておく。

図４　医療分野認証局の全体図

おわりに

医療情報ネットワークを構築する上で、なぜセキュリティを考慮し情報を守らなくてはならないかということは今更ながら述べることではないと思う。また、これから将来にかけて医療分野でも IT 化が進み、ネットワークを通じて医療情報がやり取りされる時代が到来することも当然であると思う。

医療という人の生命を扱う分野において、情報の守秘性の高さは媒体が紙であろうとネットワークであろうと変わることはない。しかし、情報の扱いは、媒体が紙からネットワークへ移ると格段に難しくなる。

大げさな言い方かもしれないが、ネットワークは世界につながっている。ネットワークを使えば、世界中の情報を収集することが可能になる。ネットワークであるので、それは当然のことである。ネットワークはオープンな環境であり、情報の発信者を一般の個人にしたと言う点で画期的なものである。

しかし、オープンな環境であるがゆえに情報を隠すことは難しい。何も進んで隠せという意味ではない。隠さなくてはならない情報も存在するという意味である。医療情報と言う人の生命に関わる情報であれば、その被害も取り返しのつかないものになる可能性がある。また、残念なことではあるが、世界に張り巡らされたネットワークの上には、情報を不正に取得して負の効果をもたらすように操作しようとする人間も存在する。

情報は公開するものであると同時に守るものでもあると考える。公開するものであると言う考え方があるからネットワークは発展して来たとも言える。逆に、隠す必要もあると言う考え方があるから暗号化、認証局に代表される PKI がこれだけ注目されるのである。医療分野で情報を扱う時も考え方は同じだと思う。

HIV や C 型肝炎の問題でも分かる通り、これらの情報は広く一般に公開され、迅速に対応をすべきものである。しかし、HIV 患者や C 型肝炎の患者の個人情報が漏洩した場合どうなるであろうか。個人の DNA 情報が巷でやり取りされたらどうなるであろうか。誰もが問題だと思うのではないだろうか。

医療で扱う情報が特殊な扱いをするものであるとは言わない。しかし、情報が漏洩した時に被る被害の大きさは他の一般産業界での情報漏洩とは質が違う。医療分野でセキュアなネットワークを構築する目的はそのような守るべき情報を守るためにある。

今回、セキュアなネットワークを構築する１つの手段として医療分野 PKI の構築、中でも認証局に焦点を絞ってまとめてみた。

ただし、これが全てではない。IT 化、コンピュータ化する時には他にも様々な要因を考える必要がある。コンピュータに蓄積される個人情報をどう取り扱うか。ネットワークをつなぐコンピュータであるサーバの安全性をどう確保するか。そして、何より情報を扱う当事者の意識改革が必要になる。

IT 革命という言葉が言われ出して久しく経つ。それに追従するかのように IT を支える技術は急速に発展してきている。しかし、その急速発展の流れの中で、IT 機器や情報を扱う人達の意識は変わっただろうか。IT 革命とは IT 化を進めるだけではなく個人個人の意識の改革も含めて IT 革命ではないだろうか。

アメリカの医療分野ネットワークの現状

アメリカの政府とヘルスケア分野におけるネットワーク化の動向について簡単に紹介する。

政府の動向

アメリカ政府のネットワーク化の動きは早かった。1998 年に制定された政府文章事務排除法（Government Paperwork Elimination Act）が制定されている。これ以前にも各種の動きがあったが、この法律制定から具体的な動きが始まる。これは、政府の全ての行政手続きを電子的に提供すると定めたものである。アメリカでは 2003 年 10 月まで電子政府設立を目標としている。

例えば、税務申告書をインターネットからダウンロードし、内国歳入庁へ電子申告が可能な仕組みが提供されている。

2000 年 9 月から提供が始まったアメリカ政府のオフィシャルポータルサイト[10]では、連邦政府内の情報を総合的に検索ができるようになった。さらに、2001 年 6 月からは機能を拡張し、全州政府の情報検索が可能となっている。

アメリカの政府認証局は、各省庁で独自に設立されている。これらを統合的に認証するために連邦公開鍵認証基盤（FPKI：Federal Public Key Infrastructure）が構築されている。これは日本の GPKI と同じくブリッジ型認証である。

ヘルスケア分野のネットワーク化の動向

アメリカのヘルスケア分野でのネットワーク化も発展が著しい。それでも、アメリカのヘルスケア分野の IT 化は一般産業界と比べて 5 年遅れているといわれているようである。その一例を紹介する。

アメリカは日本と違い皆保険制度ではない。個人が民間の保険会社に加入している。患者は診察を受ける際に保険の有無を確認し、保険会社に確認の電話や FAX を入れている。アメリカではこの処理のことをクレイム処理と呼んでいる。患者が病院で診察を受ける場合、必ずクレイム処理が起こるのでその処理量ははかり知れない。そのため、この部分をオンライン化して行こうという動きが始まった。

---

10 http://www.firstgov.gov/

IT 化が進んでいると言われるアメリカでも、ヘルスケア分野については進んでいる部分とそうでない部分が混在しているようである。

アメリカ医師会の取り組み

アメリカ医師会のネットワーク化のへの取り組みとして 4 月にインタビューをした。その時の内容をまとめておく。

アメリカ医師会は、「AMA Internet ID[11]」というサービス名で全ての医師へ電子署名を配布する仕組みを構築している。2002 年 4 月末で 2000 人が電子署名を受け取っている。

電子署名を配る背景は、やはりアメリカでの IT 化の流れが一番大きな要因だったようである。アメリカ医師会はヘルスケアネットワークを今後のビジネスに必須の要素と捉えていた。そこで、1997 年から 1999 年まで 3 年をかけて実態調査を進めている。その結果、単純にユーザに ID とパスワードを配布するだけではセキュリティの確保が難しく応用範囲も狭いと判断がなされた。そこで電子署名の配布が決定されている。

電子署名を配布するには、医師の情報が必要となる。アメリカ医師会は、設立当初からアメリカ全土の医師の情報を保持し、データベース化している。また、その管理・保守を業務の一つとして長年運用していた。そのため、電子署名を配布する条件が元々備わっていた。

システム構築時に一番の課題となったのは、医師からの要求とセキュリティのバランスをどう処理するかということだった。医師からの要望はセキュリティと反比例するものが多かったそうである。しかし、説明を繰り返しセキュリティについて理解をしてもらうことで納得してもらったそうである。

また、アメリカ医師会の職員の教育もセキュリティを確保する上で重要な要素であると説明された。今までのシステムに加えて、新たなシステムが導入されるため、操作方法や機密保持のための教育が大変だったそうである。

それでも、AMA Internet ID を導入した効果は少しずつ現れているようである。今まで機密情報の漏洩を恐れてインターネットを使わなかった医師が AMA の電子証明書を使ってアクセスをするようになっているそうである。ただ、まだ患者の理解を得るところまで

[11] http://www.ama-assn.org/internetid

は進んでいないようである。AMA では今後、患者にも適用範囲を拡大することを目標としてリサーチをしているとのことであった。

最後に、アメリカ医師会で AMA Internet ID を使って、どのような将来ビジョンがえがけるかと質問してみた。担当者曰く「あまりにも応用があって、はっきりとこれというものをえがけない。技術も日々進化している。」と言われた。例として、ネットワークを通じて患者の緊急対応を行うヘルスアラートシステム、医師と患者がセキュアに遠隔診断できるような仕組みができると言うことであった。

日本でも同様の仕組みが模索されているようである。アメリカでの仕組みを日本で使うかどうかは別として、日本より先を行くアメリカの動向は今後も注目しておく必要があると思う。