資料. 5

平成１５年度厚生労働科学研究費補助金医療技術評価総合研究事業
「電子カルテネットワーク等の相互接続法の標準化」

主任研究者：木内貴弘（東京大学医学部附属病院）
分担研究者：廣川博之（旭川医科大学附属病院），辰巳治之（札幌医科大学），山本晧二（三重大学医学部附属病院），井上裕二（三重大学医学部附属病院），原量宏（香川大学医学部附属病院），中島直樹（九州大学病院），高田彰（熊本大学医学部附属病院）

１．はじめに

全国の複数の地域で電子カルテネットワーク等を中心とした様々な地域医療情報ネットワークの構築が進んでいる。これらのネットワークは、従来、お互いに相互接続することをまったく念頭におかずに独立して構築が行われてきている。このままの状況が続くと、各地域医療ネットワークを全国レベルで相互に接続することが不可能になっていくと思われる。本研究の目的は、VPNを用いて、全ての地域医療情報ネットワーク・医療機関が参加できる安全な閉域ネットワーク（医療VPN）を構築するための標準仕様を策定し、この仕様を利用して、既存の電子カルテネットワーク等を実際に接続し、その実用性を検証することにある。

２．方法

標準仕様の策定のために、ドメイン名・IPアドレス割当方針の策定（廣川）、IPv6との相互接続・運用の検討（辰巳）、VPNの各医療機関への接続形態の検討（山本）、専用線ネットワークとの相互接続法の策定（井上）、DNSの運用法の策定（原）、ルーティング運用法の検討（中島）、運用のセキュリティ保護指針の策定（高田）について各々が分担して原案の策定を行い、３回にわたって班会議を行い全員で策定した仕様原案の検討を行った。仕様策定のあたっては、１）各参加施設がインターネットと医療VPNを同時に利用できるようにすること、２）医療VPNをインターネットのように自律・分散管理できるものにすること、３）医療VPNからの通信についても、各施設自身の責任による侵入対策を行うことを前提とすること、４）医療VPN用のルートDNSサーバを医療VPN内に設置する一方で、各参加施設内の同一のDNSサーバでインターネットと医療VPNの名前解決ができるようにすること、５）既存の国立大学病院VPN(UMIN VPN)の機能の維持と独立した運用が従来とおりできるようにすること、６）国立大学病院がUMIN VPNを介しての医療VPNへの参加できるようにすることを基本方針とした。この方針に基づいて標準仕様を策定し、既存のUMIN VPN及び分担研究者らが関係する６つの地域医療情報ネットワークとの実際の接続作業を行った。

３．結果

相互接続に必要な医療VPNのユニークなアドレス空間として、インターネットプライベートアドレス領域の10.255.0.0/16を利用することにした。また医療VPN内で利用するドメイン名としては、医療VPN系の情報資源であることを明確にするために、hvpn.netというドメイン名を使用することにした。ファイアウォールとVPN機器の接続方法としては、インターネットを介した通信も医療VPNを介した通信も、施設内部に入る前に必ずファイアウォールを経由するような接続形態とし、またファイアウォールを介さないで、インターネット側からVPN側へ、または逆方向に通信できないような接続形態を検討して、接続例として例示した。医療VPN用ルートDNSサーバは、(1)医療VPN参加各施設内のDNSサーバに医療VPN内のDNS情報をゾーン転送する他、(2)医療VPN内からの直接の名前解決要求に答え、(3)既存UMIN VPNとの互換性維持のために、UMIN VPNの名前問合せ要求(s.umin.ac.jp)にも対応することとした。上記の仕様をもとに実際に相互接続を行い、実際に運用が可能であることを確認した。

４．考察

医療VPNでは、医療機関等の間の通信はすべて暗号化され、医療VPN内のサーバ等へは、医療VPNの参加機関以外からは、アクセスができないために、安全性は非常に高いと考えてよい。しかし、１つの医療機関等が外部から侵入された場合には、連鎖的に侵入や攻撃にさらされる危険がある。このため、例え医療VPNを介した通信であっても、セキュリティポリシーとして、すべて各施設のファイアウォールによるチェックを行うことを前提とした。

医療VPNは、施設対施設の通信を全体として暗号化するので、認証も施設単位で行うことができ、１施設に１枚の公開鍵証明書を発行すれば済むため、コストが安く、運用・管理も楽である。一方、２つ

の通信を行っているコンピュータや機器等の間の通信を暗号化するいわゆるend-to-endの暗号化は、VPNよりもセキュリティ上は優位にあると考えられているが、厳密な個人認証または個々のコンピュータや機器毎の認証が必要であるため、個人や個々のコンピュータ・機器等に公開鍵証明書発行が必要となる。この作業は、医療機関等にとっては費用と手間がかかる煩雑な作業であり、また個人対象の場合にはそれ相当の利用者教育も必要となる。また医療機関等の職員の側にも負担が発生する。このため、VPNの普及が先に進んでいくと予想しているが、VPNとend-to-endのセキュリティ暗号化は互いを排除するものではなく、より安全性を高めるためには、両者を併用するのが最も望ましいと考えている。併用のメリットとして、（1）ファイルセーフ機能（例えばメールの暗号化をし忘れて送付してしまったり、誤って医療VPNでなくインターネット経由でメールを出してしまう場合等の対策）及び（2）暗号の二重化による安全性の向上（解読の難しさが増すともに、暗号アルゴリズムのセキュリティホールを相互補完できる）が考えられる。

インターネットの自律・分散管理の仕組みは、インターネットの運用の労力とコストを大幅に下げている。医療VPNでも、インターネットとまったく同様の仕組みを採用しており、実質的に医療機関等だけが参加できる閉じた小さなインターネットのようなものと考えることができる。一方、このような自律・分散型の医療VPNの管理・運用方式では、複数の組織が共同で運用に関わっているため、どの組織も単独で通信全体セキュリティを保証することができない点が問題である。このことは、医療VPN側を利用した通信のセキュリティ保護の責任は、あくまでも通信する２施設の責任で行う必要があることを意味する。このためにも、医療VPNと他の暗号化手段の併用が望ましいと考えられる。

医療VPN内では、インターネットプライベートアドレスの一部を医療VPN用のグローバルアドレスとしてお互い見えるようにする仕様となっている。医療VPN用のIPアドレス空間として、インターネットグローバルアドレスを利用することも検討したが、実用上運用困難と判断した。すべての国内の医療機関等に割り当てられるような広大なまとまったグローバルなアドレス空間の新規確保は困難であるため、小さな多数の領域のグローバルアドレスを医療VPN内で利用することになるが、これによりルーティグの設定が非常に複雑となり、各施設での設定変更が頻繁に発生する等の問題が生じるためである。

医療VPN用として、予約するインターネットプライベートアドレス空間の選択については、最も大きな連続したプライベートアドレス領域の一番後ろの部分を選ぶということを選択の根拠として考えた。どの領域を使ったとしても、既に医療機関内等で使われているプライベートアドレスがバッティングする可能性があることは同じであるが、上記のアドレス領域がバッティングの可能性が最も低いと考えたからである。

DNSについては、従来、UMIN VPNでは、インターネットのDNSサーバを利用して、UMIN VPN内のサーバの名前解決を行う方式をとっていたが、DNSサーバが乗っ取られたり、第三者が偽物のDNSサーバを用意した場合に大きな問題となりえるため、今回の標準仕様の策定にあたっては、医療VPN内で、医療VPN用のDNSルートサーバを運用する方針を採用し、各医療VPN参加施設内のDNSサーバからゾーン転送の設定をすることによって、この問題を解決することができた。

本研究によって、全国立大学病院、全国立病院(HOSPNETは、UMIN VPNと既接続でメール交換のみ可能)と６つの地域医療情報ネットワークがVPNで相互接続されることになった。今回構築した医療VPNは、既に巨大な医療専用閉域ネットワークと呼んでよいと思われる。このような巨大なインフラをどのように活用をするかは、今後の課題といえる。またこの医療VPNが、更に拡大していった場合には、アドレス・ドメイン名割当のための組織やもっと詳細なセキュリティポリシーの策定が必要となってくることが考えられる。

## ５．結論

本研究の成果によって、電子カルテネットワーク等の地域医療情報ネットワーク及びAPSベンダー提供の電子カルテシステム等の全国レベルでの相互接続（医療VPN）のための標準仕様が策定された。またUMIN VPN、HOSPNET、６つの地域医療情報ネットワークが実際に相互接続され、安全な相互の通信が可能になった。今後は、更に参加施設を増やしていくとともに、構築された医療VPNを有効に活用する方法についての研究が行われていくことが期待される。

資料. 6

第５回標準的電子カルテ関連研究報告会
研究発表資料

# 保健医療分野における電子署名の実用化に関する研究

主任研究者　坂本　憲広　神戸大学医学部附属病院　教授

研究要旨
電子政府の実現に向けて個人認証、電子署名は非常に重要な課題である。また、平成13年度「保健医療分野の情報化にむけてのグランドデザイン」および平成16年8月の医療情報ネットワーク基盤検討会最終報告（案）「今後の医療情報ネットワーク基盤のあり方について」においても、公開鍵基盤を用いた電子署名の必要性が基盤整備の促進の1つの課題として認識されている。公開鍵基盤の中核技術である電子署名とは、発信者本人しか使えない暗号化処理を電子文書に施すことにより、その電子文書が発信者のものであり、通信路の途中で改竄されていないことを証明するものである。保健医療文書の中にも法的に署名もしくは記名捺印が必要なものがあるが、平成13年度より電子署名法が施行されており、この電子署名が利用できれば、電子カルテの応用範囲が広がり、より高品質の医療の実現に繋がることが期待される。逆に、電子署名を施さない限り、電子化した保健医療文書を保健医療施設間で交換し、その情報に基づいて診療を行うことは困難である。また、電子カルテの真正性、証拠能力を担保するためには、長期間に渡り有効な電子署名を電子カルテに付加する必要がある。既に医療訴訟において電子カルテが証拠能力を有しなかった事例が発生している。しかしながら、医療文書の電子化、あるいはその電子署名の付加に際しては、法的、技術的に様々な問題を解決しなければならない。本研究は、保健医療分野において電子署名を実用化するための様々な問題を明らかにし、それに対する技術な解法を与えるものである。
平成13年度では、処方箋や診療情報提供書など、保健医療施設間で頻繁に交換される保健医療文書を対象として、電子署名を付加するための情報モデルおよびプロトコルを研究開発した。平成14年度は平成13年度の成果を活用し、医療施設間で実際に電子署名付きデータを交換する実証実験を行った。処方箋そのものについては、未だ法的に電子化することが認められていないため、今回の実証実験では処方情報、調剤情報、遺伝子情報、安全管理情報などを主体として行った。また、実際に電子署名付きデータを交換し、それをお互いに信頼するためには、各医療機関のセキュリティポリシおよび証明書ポリシの交換が必要である。そこで、平成14年度はこれらの実装を一部行った。平成15年度は、この電子署名ライブラリーとHL7メッセージングライブラリの統合を行っ

ている。また、この統合ライブラリーを用いた実システムの構築も行っており、実システムでの検証後、この統合ライブラリーを公開し、国際標準に準拠した医療情報メッセージが電子署名を付加して安全に交換できる環境整備の促進に寄与する予定である。

分担研究者：
山本隆一
東京大学大学院情報学環　助教授
石戸是亘
財団法人先端医療振興財団　研究員

## A. 研究目的

本研究の目的は、これからの電子政府に向けて、法的に署名もしくは記名、押印が要求されている診療録に対して、その電子化診療録に電子署名を行うことができるよう、電子署名の保健医療分野での実用化のための基礎研究を行うことにある。特に平成14年度はその実証実験を行い、実用化の可能性およびその際の問題点を明らかにすることを主たる研究目的としている。本研究は、この電子署名を保健医療分野において実用化するための技術を研究、開発しようとするものであり、電子カルテの普及、患者サービスの向上を実現する上においての基盤を提供しようとするものである。電子署名の実用化に関する研究は様々な分野において行われているが、他分野の電子署名技術をそのまま保健医療分野に応用することはできない。他の分野で実用化され、あるいは実運用されている技術に関しては、安全性や問題点が既に明らかにされているものが多い。しかしながら、保健医療分野において独自に開発し、あるいは実用化しなければならない場合、その実用化に関する問題点は保健医療分野において明らかにしなければならない。そこで本研究では平成13年度に提案したプロトコルについて、平成14年度はその実証実験を行い、その実用性および安全性を明らかにするための研究を行う。この研究により、電子カルテの利便性、安全性が大きく向上すると期待される。

## B．研究方法

平成13年度は、研究全体を概観するために、保健医療分野におけるPKI利用のトップユースケース分析と紹介状、処方箋等の医療情報のインタラクション分析を行った。PKIの利用目的は、主として暗号化通信による秘匿性の担保と電子署名による情報源の確認である。ここでは、保健医療において電子署名付き文書交換を主目的としたPKI利用が要求される場面を包括的に特定し、そのトップユースケースを分析、生成することを試みた。

平成14年度は、このユースケースおよびそれに基づいて作成したプロトコルモデルと元に、三菱社製の暗号化ライブラリMistyCertを用いて、JAVA、Webでプロトタイプシステムを作成し、その実用性および安全性、コストなどについて評価する。同時に、医療機関間での電子署名付き医療

文書の交換に際して必要となる、情報セキュリティポリシ、プライバシポリシ、認証局実施規程を開発し、また、個人認証を行うためのICカードについても調査を行う。

## C．研究結果

平成 14 年度は以下のプロトタイプシステムを開発し、神戸大学医学部附属病院の病院情報システムとの間で連携テストを行い、実証実験を行った。

本実証実験で開発または構築されたシステム、機能は以下の通りである。(1)LRA システム、(2)Sub CA システム、(3)利用者認証機能、(4)アクセス権限管理機能、(5)電子署名機能、(6)タイムスタンプ機能、(7)PKI 対応クライアントシステム

さらに、情報セキュリティポリシのテンプレート開発を行った。情報セキュリティポリシ策定の目的は、情報システムを構築する期間が、その情報セキュリティに対する考え方や取り組みを明確にすることにある。

本研究で開発した情報セキュリティポリシには、保健医療機関が保有する情報資産と、それを保護する理由を明示している。本年度の研究では、情報セキュリティ基本方針、および個人情報保護基本方針についてそのテンプレートを開発し、実証実験において使用した。さらに、証明書ポリシ、認証局実施規程のテンプレート開発を行った。最近、保健医療分野においては認証局を階層化し、1 つあるいは少数の保健医療機関がルート認証局を運営し、その他の医療機関はそのサブ CA とする方向性が打ち出されている。そして、その際には、証明書ポリシはそれぞれのルート認証局の証明書ポリシを用い、その他のサブ CA はその証明書ポリシに従って、認証実施規程のみを独自に作成することとなっている。従って、今後は医療機関でこの認証実施規程を作成する必要が出てくる。当然、今回のプロトタイプを用いて実証実験においてもこの認証局実施規程が必要であり、本研究においてこれを開発した。認証局実施規程(Certification Practice Statement)は、認証局が行う証明書発行、失効、及び証明書を基礎とする公開鍵基盤(PKI：Public Key Infrastructure)の運用維持に関する諸手続きおよび証明書発行、利用にかかわる主体の責任を記述したものである。認証局実施規程には、認証局で用いる、証明書所有者の私有鍵や証明書の格納媒体を指定する。また、認証局は、CA 証明書の発行を受けるルート認証局を明らかにし、その下位認証局として活動することを宣言する。認証局実施規程は、医療従事者用公開鍵証明書、患者・保健医療福祉サービス利用者用公開鍵証明書および医療機関・保健医療福祉サービス供給組織用公開鍵証明書を発行する「ヘルスケア PKI 認証局」証明書ポリシ(以下 CP という)に従い、認証局が発行するすべての証明書に適用される。ヘルスケア PKI とは、保健医療福祉分野において医療情報を地域で連携して利用するための PKI である。

本研究で開発したこれらの規程類はまだまだ不完全で十分なものではないが、作成には非常に大きな労力を要した。

今後、これらの規程類を各保健医療機関で制定しなければならないとすると、そのコストは大変大きいとされると考えられる。しかしながら、本研究の成果を次年度以降

利用することにより、それらのコストを下げながら、確実に電子署名を用いた安全な情報交換が実現できる環境整備が可能であると考えられる。

## D．考察

平成13年度の研究成果では、保健医療分野において、処方箋等を電子的に交換する際のシナリオ、ユースケース、プロトコルが明確となり、電子署名の付加方法が同定された。平成14年度はその成果の実用性、安全性を検証するために、プロトタイプシステムを開発し、その実証実験を行うことを目的とした。しかしながら、実際に電子署名付き保健医療情報を作成し、それを交換しようとすると、それを利用する保健医療機関におけるセキュリティ環境整備が非常に大きな課題であることが判明した。これはなぜならば、如何に厳密なセキュリティ技術を応用して、安全なシステムを開発したとしても、それを利用する、あるいは運用する環境のセキュリティがおざなりであれば、結局は交換される保健医療情報の信頼性が低下するからである。

しかしながら、平成15年度に厚生労働省に医療情報ネットワーク基盤検討会が設置され、平成15年8月にはその最終報告（案）として「今後の医療情報ネットワーク基盤のあり方について」において、公開鍵基盤、書類の電子化及び診療録等の電子保存について、技術的側面及び運用管理上の課題解決や推進のための制度基盤の検討を行っている。今後、この検討会によるガイドライン作成や監査制度の提案により、安全で正確な医療記録の電子保存が推進することが期待される。

## E．結語

平成14年度の研究は、平成13年度に行った基礎的な事項の調査研究の成果の実用性、安全性を検証することが目的であった。

そのため、昨年度提案したユースケース、およびプロトコルに基づくプロトタイプシステムを開発し、その実証実験を行い、昨年度の提案が妥当であったことを証明した。

以上の研究結果を基に、来年度はより詳細な実用化研究とその検証を行うと共に、情報セキュリティポリシテンプレート、認証局実施規程テンプレートなど、これから各保健医療機関で必要となるリソースについて更に整備を行っている。また、本研究の電子署名ライブラリーと厚生科学研究「電子カルテの相互運用のための HL7 メッセージの流通および管理に関する研究」で開発中の HL7 メッセージングライブラリの統合を行っている。この統合ライブラリーを用いて、神戸大学病院では処方オーダリングシステムや電子カルテシステムを実装しており、2005年1月より順次稼動予定である。これらの実システムでの検証後、この統合ライブラリーを公開する予定であり、その結果、国際標準に基づいた医療情報メッセージが電子署名を付加して安全に交換できる環境が整備されるものと期待される。

資料. 7

# 保険証認証のためのデータ交換基準に関する研究 （H 15-医療-072）

里村 洋一 （千葉大学）

研究の目的：本研究は、保険者の持つ被保険者データのデータベースと医療機関等を通信回線を介して結び、保険証の有効性を即時的に認証を行うシステムの開発である

方法：研究方法=本研究は主として次の４ステップについて行った。

1．センターと全保険者との接続を想定した方式の確立。

2．センターと全医療機関との接続を想定した方式の確立

3．課金方式の確立

4．上記の成果を踏まえて構築した実験システムによる構内通信実験

結果１．検証に必要なデータ項目の整理：ＨＬ７、ＭＭＬ、ＪＭＩＸなどで定義されている既存のデータ項目では不十分であることがわかり、新たに認証用データセットを定義することとした。

結果２．既存の医療用通信規格を比較し、オバーヘッドの軽いことと、比較的限定された当事者間（医療機関と保険者）の通信であることを理由に、Ｊ－ＭＩＸを採用することとした。

結果３．通信はインターネットを利用し、通信の安全のために、ＶＰＮを採用することとした。そのために、利用者登録やユーザー認証のシステムを盛り込んだ。

結果４．システムを試作し、構内回線を利用した認証実験をおこなった。その結果、いくつかのシステム上の問題解決を必要としたが、最終的には、１件１５０msec以下の速度で、正確な認証結果を回答することに成功した。

結果５．課金システムについては、基本構築の設計におわった。

結語：本システムの稼動に必要な技術要件をほぼ満たしたシステムを完成した。今後は、実際の医療機関と保険者を結んだ実証実験を必要とする。