厚生労働科学研究費補助金

医療技術評価総合研究事業

安全な保健医療情報流通を促進する保健医療認証基盤整備の技術的方策に関する研究

平成１７年度　総括研究報告書

主任研究者　大山　永昭

平成１８（２００６）年　４月

目　　次

厚生労働科学研究費補助金（厚生労働科学特別研究事業）

総括研究報告書

安全な保健医療情報流通を促進する保健医療認証基盤整備の技術的方策に関する研究

主任研究者　　大山　永昭　　東京工業大学像情報工学研究施設　教授

研究要旨：　今後の医療の高度化やそれに伴う機能分化の促進が想定される状況下で、患者主体の診療が実施されるためには、関連する施設等の間で、電子カルテや医療情報の伝送を安全かつ動的に行っていくためのネットワーク基盤が必要である。本研究では、多機能 IC チップを利用し、オープンなネットワーク上で、誰もが安全・手軽に情報サービスを利用可能なネットワーク基盤を医療分野に適用する方法を提案した。さらに、オンデマンド VPN がネットワーク上を流通する医療情報の保護に有効であることを実験的に明らかにし、実用化に向けた課題を明らかにした。

分担研究者　　喜多　紘一　東京工業大学像情報工学研究施設 特任教授
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 専任主席研究員
高橋　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
石垣　武男　名古屋大学大学院医学研究科　教授
山本　隆一　東京大学大学院情報学環　助教授

A．研究目的

近年の情報基盤整備の進展に伴い、保健医療分野における情報化の推進が期待されているが、電子的に保健医療情報の流通を行う場合には、個人情報の保護が極めて重要であり、そのために必要となる適切な措置を講じることが急務とされている。

ここで、個人情報の安全性を確保するためには、医療データ等を使用する者の正当性を認証すること及び、通信回線上や医療機関内での医療データ等の保護を実現することが重要である。我々は、これまでに保健医療福祉分野の情報化において必須となる電子的な認証、特に医師･看護婦等の資格認証の必要性を示し、電子認証の実施方法や問題点の調査・検討を行ってきており、本研究では、これら研究成果を踏まえ、もう１つの重要な課題である通信回線上や医療機関内部における個人情報・医療情報等の安全性を確保する技術について研究開発を進めるとともに、保健医療分野における情報の安全な流通を保証するネットワーク基盤を構築・運用する方策について検討した。さらに、保健医療福祉分野でのネットワーク基盤整備を進めるとともに、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いることから、ネットワーク基盤を利用した安全性、利便性、経済性などに優れた医療サービスの実施方法を取りまとめ、さらに保健医療福祉サービスの今後の新たな展開の可能性等を示した。

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電子化の状況や情報保護に対する取り組みを調査し、安全に医療情報を取り扱うための課題の抽出と実現方法の検討を行った。さらに、安全なネットワーク基盤構築に関する検討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、医療分野における共通ネットワーク基盤にするための方策を検討した。

C．研究結果

(1) 多機能ＩＣチップを利用した安全なネットワーク基盤（オンデマンドVPN）

外出先などからインターネットを使って安全に社内へアクセスすることや、特定の相手に対して安全に情報提供したりするニーズが急速に高まっており、以前は、このようなニーズに対して情報を流通する際のセキュアな通信路の確保手段として、専用線を用いた通信を行っていたが、最近ではコスト面で優れたインターネットなどの公衆回線を利用したVPN(Virtual Private Network)を用いることが多くなってきている。しかし、VPNの構築には、利用者にネットワークの専門知識が必要なうえ、設定などを誤ると情報セキュリティ上多大な影響が発生する恐れがあるなど、誰もが容易に設置できる状況に至っていない。このような背景の下、VPNの状態管理を行うVPN管理機関と2階層PKIに対応したICチップが搭載された通信機器を用いて、利用者の要求に応じて鍵情報などのVPN構築に必要な情報を、ネットワークを介して配送し、即座にVPNが構築可能な環境を構築する多機能ＩＣチップを利用した安全なネットワーク基盤（オンデマンドVPN）の研究開発が進められている。

オンデマンドVPNで利用される多機能ICチップは、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を持ち、ネットワークに接続された様々な機器の認証に用いることができる。このため、複数の機器間や、異なる組織間で動的に安全なネットワークを構築することができ、ネットワーク上を流通する様々な情報の保護に有効であると考えられる。

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、オンデマンドVPNで利用されている鍵配送方式は、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り、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様々な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必要な認証を経て、自分のカルテ情報等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。

現在までに開発され実証実験に供されているオンデマンド VPN は、それぞれ独立した管理機関での運用となっているが、異なる管理機関に属する VPN ルータ同士で接続を行うためには、様々な課題を解決しなければならない。オンデマンド VPN では、ルータ間で IPsec による VPN を構築するために、機器相互の ID や鍵情報などを用いて IPsec-SA を確立する必要があり、現在は、IKE における Pre-Shared Key を利用した鍵交換を採用しているが、このために VPN 通信路毎に異なる鍵が必要となることや、複数の VPN 管理機関間で VPN 通信のローミングサービスを実施する場合の鍵漏洩の危険など、Pre-Shared Key をどのように管理、配送するかが新たな課題となる。このような課題に対して、接続許可証を用いることにより、異なる管理機関同士の接続においても安全な鍵交換を実現する手法が考えられる。まず、証明書ベースの鍵交換を行うためには、現在の Pre-Shared Key による鍵交換ではなくデジタル署名認証方式を導入する。そのためには、秘密鍵およびそれに対応する VPN 管理機関が発行した公開鍵証明書が必要となる。オンデマンド VPN においては、VPN 接続の可否を VPN 管理機関が制御することになるため、IKE 時に必要となる公開鍵証明書の配送を VPN 管理機関が行う。同時に、ルータを管理

する VPN 管理機関（機関 A）は、ルータ A への接続許可証を発行し、これを VPN 管理機関 B へ送付する。その後、接続許可証は VPN 管理機関 B から管理下にあるルータ B へ送付される（図 1 参照）。この接続許可証により接続許可の判断や異なる VPN 管理機関へのアクセス権限などを制御する。鍵交換時には、ルータ間でさきほどの接続許可証を交換し、接続許可証の内容のチェック及び署名検証を行う。仮に、ルータ A 及び B で VPN 管理機関が異なる場合でも、接続許可証の署名検証は自己が属する VPN 管理機関の公開鍵により行うため、IC チップ上で複数の CA の存在を意識する必要はない。この手法では、接続許可証として公開鍵証明書に対応する属性証明書を用いることを想定している。これは、VPN 管理機関発行の属性証明書の送付要求及び証明書送付を Certificate Request ペイロードを利用して送付することが可能なため、従来の ISAKMP パケットの構成と機能をそのまま利用可能であり、既存の鍵交換プロトコルを変更することなく、実現が可能なためである。

今後、これらを医療分野の共通のネットワークインフラとして活用するためには、ネットワーク基盤を管理・運用する認証機構のあり方や、登場するプレイヤの具体的な役割などを検討し、実証システムの開発を行うことが必要である。

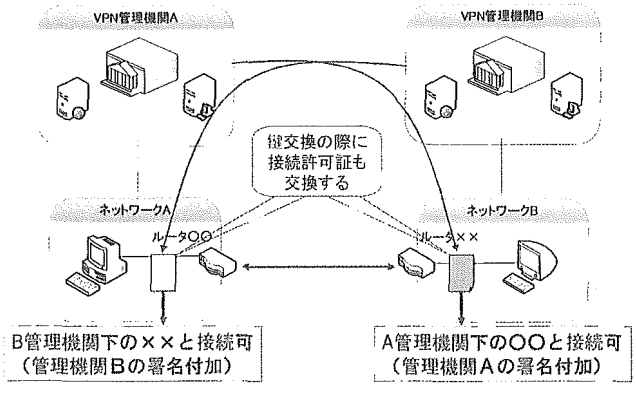

図１．接続許可証を利用した鍵交換

(2) 多機能ＩＣチップに関する標準化技術動向

ここでは、多機能 IC チップの標準動向について述べる。CPU を持った多機能 IC チップの代表は IC カードであり、その標準は、JTC1 の下部組織である SC17 が担当し、国際的な活動を行っている。又、これとは別に、PC に搭載するセキュリティチップと、安全な計算機環境を構築するための活動が行われている。

（ア）PC 組み込み型セキュリティチップ

PCのセキュリティ機能を高めるために、マザーボード上にセキュリティチップと呼ばれるICチップを搭載したものが出始めている。代表的なものがIBM、Intel、HPなどの企業が中心となって設立されたTrusted Computing Group(TPG)と呼ばれる団体が行っている標準化活動である。

TPGでは、PC上のアプリケーション、OS、ハードウェアを含めた安全性を確保することを目指している。その中で、重要な要素となるのがTrusted Platform Module(TPM)と呼ばれるICチップである。このICチップは、

- 情報（鍵、証明書、パスワード等）を安全に格納する場所の提供
- 暗号処理を行う機能（上記の情報を用いた演算を含む）、特に認証機能、電子署名機能の提供
- インテグリティの確認するための情報の格納と、確認機能の提供

等の機能を提供しており、下記の標準インタフェースが提供される。

- アプリケーションレベルでのインタフェース
- TPMドライバのインタフェース

TPMのチップ自体は、Atmel, STMicron, など複数の企業が製造を行っており、既にIBM、東芝、DELLなどからTPMを標準搭載したノートPC、デスクトップPCが発売されている。チップは製造メーカにより仕様が一部異なるが、TPMドライバの層でその違いの吸収を図っている。

TCGの活動範囲は、当初PCに限られていたが、その範囲を他のネットワーク接続機器に広げてきたのが今年の特徴である。接続形態は、有線・無線両方を想定しており、携帯端末なども範疇に入れることを想定している。

TCGには米国の企業だけでなく日本の企業も参加しており、今後の活動が注目される。;

（イ）ISO/IEC7816-13：多機能 IC カードにおけるマルチアプリケーションアプリケーション管理

1 枚の IC カードに複数のアプリケーションを搭載し、複数の業務を 1 枚のカードでこなすことを可能とすることでカードホルダーの利便性が向上することが期待される。この機能の実用化については、日本が世界をリードしているため、日本から IC カードのアプリケーションを管理する機能を国際標準とすべく JTC1/SC17/WG4 に提案を行っている。先に述べた TPM は、固定された認証機能を利用可能とする点で、従来の IC カードを PC 上に搭載したものと考えることができる。これに対して、7816-13 は、任意のサービスを提供するためのオブジェクトを機器内のチップに配送することを可能とするための機能を規定している。標準に従った IC カードのインフラの普及が始まると、機器に内蔵させる多機能 IC チップの普及に大きな影響を与えるものと予想され、今後の多機能 IC チップのアプリケーション管理にとって、非常に重要なものとなると考えられる。

平成18年4月現在での7816-13の審議は、2005 年に 2 回の CD 投票（Committee Draft）が行われ、次のステップである FCD（Final CD）投票に進むことが決定した。技術的な課題は解決したことから、2006 年中に最後の投票である FDIS（Final Draft International Standard)の投票に入り、新しい国際標準が成立するものと予想される。審議には、海外でカード管理に大きな影響を持つ Global Platform（GP）や MULTOS などの団体からも専門家が参加しており、国際規格を反映した製品を開発する準備が進んでいる。

(3) 医療施設間における医療情報アクセス制御

現在、多くの医療施設において電子カルテシステム等の電子医療情報システムの導入が進められている。それらの多くは個々の医療施設内での閉じたネットワークにおける利用に留まっており、インターネットのようなオープンなネットワークを経由した情報交換はほとんど行われていない。その理由としては、現状のシステムはベンダー毎に仕様が異なり相互運用に困難性があることに加え、データの安全性を確保するセキュリティの問題が大きい。ここでは、オープンネットワークを経由して医療施設間で安全に情報を交換するために、オンデマンドVPNを利用したアクセス制御方法を検討する。

（ア）医療情報交換に必要な電子的な認証

医療施設間で情報をやり取りする際の最も重要な課題として、情報交換を行う主体（利用者や機器）の正当性の確認が挙げられる。主体の正当性を確認する方法としては、主体が医療施設に属していることを認証し、また情報によっては医療従事者であることを電子的に認証する必要がある。さらに患者の個人情報となる医療情報については、患者の同意の認証も必要になるケースもある。

（イ）オンデマンドVPNを利用した施設認証

医療施設の認証方法としては、オンデマンドVPNの利用が有効である。医療施設内のネットワークに接続された機器をオンデマンドVPN経由でのみアクセスを可能とすることにより、オンデマンドVPNが設置された医療施設間のみの情報交換が可能になる。また、オンデマンドVPNは、VPN構築のための複雑な設定が不要なため、大学病院のような大規模な医療施設から診療所のような小規模な医療施設まで容易に設置可能であり、高いスケーラビリティを実現できる。

（ウ）HPKIによる資格認証

医師や看護師等の資格を有する者のみがアクセスできる情報の場合には、アクセス者の資格を認証する必要がある。現在（財）医療情報システム開発センター（MEDIS-DC）や日本医師会によって、医療用の認証基盤（ヘルスケアPKI：HPKI）の運用が進められており、資格認証を行うインフラは整備されつつあり、その実用化が期待される。

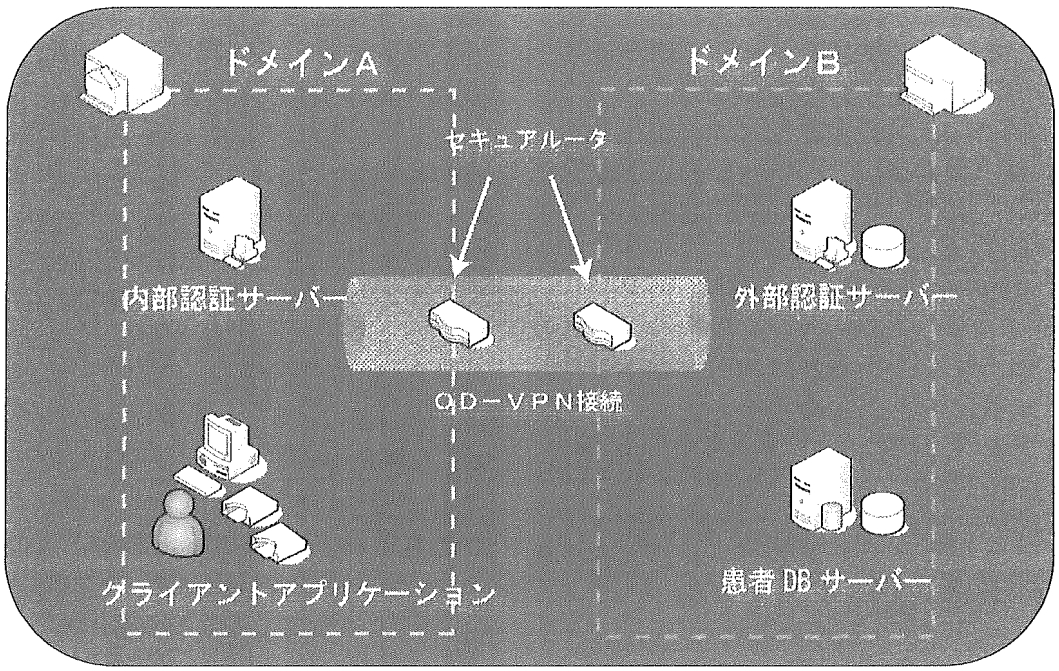

図２．実験システムの構成

（エ）患者の同意

患者の同意が必要な情報については、患者のICカードで電子署名することにより同意を得る手法が有効である。

（オ）実験システム

以上の検討に基づき、安全に医療施設間で情報をやり取りするための実験システムを構築した。実験システムでは、ある医療従事者が、本人が所属する医療ドメインとは異なるドメインで管理された患者データに対してアクセスするシーンを想定する。システム構成を図２に示す。医療従事者の所属する医療施設のドメイン（ドメインA）と患者データの存在する医療施設のドメイン（ドメインB）にはそれぞれオンデマンドVPNルータを設置し、VPN接続のみのアクセスを可能とする。医療従事者は、HPKIに対応したICカードを所持しており、内部認証サーバー、外部認証サーバーによって資格認証を行う。また患者データは、患者の同意がある場合とない場合で医療従事者が閲覧できる内容が異なる。患者の同意には、公的個人認証サービスを利用した患者の電子署名で意志確認を表すものとする。アクセス制御の結果は認可チケットとして発行され、患者データを保持するデータベース（DB）に対してチケットを提示することでアクセスが許可または拒否される。チケットはXML形式（SAML Assertion）で記述する。

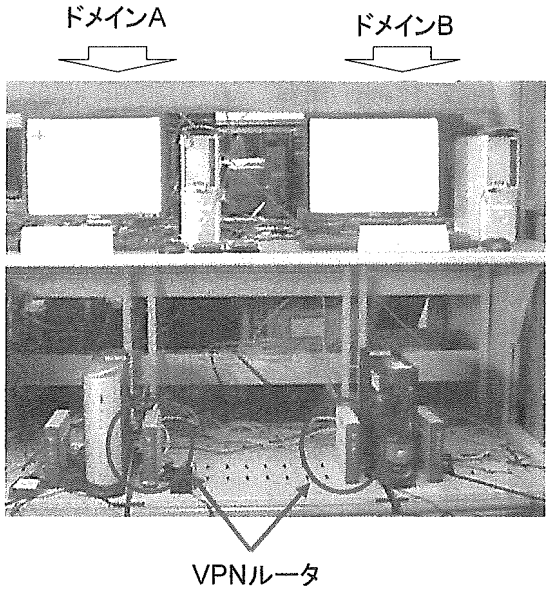

図３．実験システムの外観

実験システムにおけるデータ提供までの流れは、以下の通りとなる。

① ドメインAとドメインBをオンデマンドVPN接続する。
② 医療従事者がドメインBの患者データへのアクセスを要求すると、内部認証サーバーは医療従事者の資格を認証する。

③ 内部サーバーは医療従事者の要求と認証情報を外部認証サーバーへ提供するとともに、チケット要求を行う。
④ 外部サーバーは医療従事者の資格を確認後、外部認証サーバーから内部認証サーバーに対して、患者の意志確認を要求する。
⑤ 内部サーバーはクライアントアプリに患者ICカードの挿入を要求する。患者の意志確認がある場合は、患者署名を検証し、正当なものであればチケットに反映する。その後、認証結果をDBに記録し、医療従事者へチケットを発行する。
⑥ 医療従事者はチケットを患者DBへ提示し、条件に応じた患者データを医療従事者へ提供する。

各パターンに関して検証した結果、アクセス制御はすべて正常に行われた。資格や患者の同意などの条件によって適切な情報提供が行われることを確認した。

D．考察

近年、様々な診療情報を医療施設や患者等の間でネットワークを介して電子的に交換・共有する試みが行われているが、個人情報保護のために専用回線等を通じ、あらかじめ固定された施設間における限定的な運用がなされていることが多い。しかしながら、今後、更なる医療の高度化やそれに伴う機能分化の促進が想定され、このような状況下で患者主体の診療が実施されるためには、関連する施設等の間で、医療情報の伝送を安全かつダイナミックに行っていくためのネットワーク基盤が必要である。

また、医療情報の伝送を行う際には、電子署名法やe-文書法等などの新たな制度への対応や情報セキュリティの確保及び個人情報保護の実現を必須要件とし、医療施設におけるセキュリティ対策、ネットワーク上の安全な情報伝達、情報の真正性保証等を実現する保健・医療・福祉分野における共通的な技術的基盤を構築すべきである。ここで、オンデマンドVPNは、利用者や利用環境をネットワーク経由で迅速に確認し、複数の情報機器で動的にセキュアなネットワークを構築することができることから、医療分野における共通的なネットワーク基盤の候補として有効である。また、オンデマンドVPNを利用した機器等の認証機構とこれらを利用する医師等の認証機構を用いることで、医療施設に設置された情報機器を用いた医療従事者であることを保障した上で医療情報へのアクセスコントロールを実現できるため、保健医療福祉分野においては、オンデマンドVPNを利用したネットワーク化を促進することにより、医療にかかわる多くの機関が相互に情報交換可能な環境下で電子カルテに代表される医療情報の電子化を進めることが可能になり、個人情報保護を実現しつつ必要な情報の授受を実現する基盤が構築可能となると考えられる。例えば、患者が他の医療施設へ紹介される際の負担軽減や、医師が患者の診断・治療に関するアドバイスを他施設の専門医から得られる、他の医療機関を受診する際に過去の情報を参照して適切な治療に役立てるなど、患者や医療従事者に対する明確なメリットがもたらされるため、共通基盤の早期構築を進めることが望ましい。

さらに、今後はネットワーク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、ネットワーク基盤を利用した安全性、利便性、経済性などに優れた医療サービスの具体的検討が必要である。

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、安全なネットワーク基盤を利用した保健医療福祉サービスの研究開発に活用される予定となっている。具体的には、保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム

や現在オンデマンドVPN技術の研究開発を行っている研究グループとの間で成果を共有することで、これら研究グループが進めている医療機関相互における情報連携の実証実験や医療サービスの検討等への反映や、オンデマンドVPNを構成する技術仕様へフィードバックすることを予定している。

さらに、ネットワーク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．論文発表

- 大山永昭：次期「e-Japan 戦略」における医療分野関連の重要課題（案）について；行政&ADP，<41>，4-8(2005)
- 高橋成文，東川淳紀，山本修一郎，小尾高史，谷内田益義，大山永昭：2 階層 PKI を用いたオンデマンド VPN システム；情報処理学会論文誌，<46>，1129-1136(2004)

2．学会発表

- 佐藤茜，小尾高史，鈴木裕之，谷内田益義，大山永昭：通信ネットワーク利用放送のためのコンテンツ暗号鍵管理；第 7 回 YRP 移動体通信産学官交流シンポジウム 2005 講演予稿集，74-75(2005)
- 佐藤守，谷内田益義，鈴木裕之，小尾高史，山口雅浩，大山永昭，喜多紘一：医療情報ネットワークにおける安全な相互運用の実現に関する研究；第 7 回 YRP 移動体通信産学官交流シンポジウム 2005 講演予稿集，86-87(2005)
- 兵庫友一郎，鈴木裕之，小尾高史，谷内田益義，大山永昭：IC チップを用いた任意多地点間 VPN 構築における鍵管理手法の提案；第 7 回 YRP 移動体通信産学官交流シンポジウム 2005 講演予稿集，116-117(2005)
- 佐藤守，谷内田益義，鈴木裕之，小尾高史，山口雅浩，大山永昭，喜多紘一：異なる医療情報ネットワークドメイン 間に属する機器の接続方法に関する研究；FIT2005 第 4 回情報科学技術フォーラム講演論文集，249-250(2005)
- 佐藤茜，小尾高史，鈴木裕之，谷内田益義，大山永昭：マルチキャスト映像配信のためのスケーラブル映像暗号鍵管理；FIT2005 第 4 回情報科学技術フォーラム講演論文集，219-220(2005)
- 兵庫友一郎，鈴木裕之，小尾高史，谷内田益義，山口雅浩，大山永昭：多機能 IC チップを利用した任意多地点間 VPN のための鍵管理手法に関する研究；情報処理学会第 68 回全国大会講演予稿集，3-683-3-684(2006)
- 佐藤守，谷内田益義，鈴木裕之，小尾高史，山口雅浩，大山永昭，喜多紘一：異なる医療情報ネットワークドメインにおけるアクセス制御と権限付与に関する研究；情報処理学会第 68 回全国大会講演予稿集，3-695-3-696 (2005)

厚生労働科学研究費補助金（厚生労働科学特別研究事業）
分担研究報告書
認証業務等提供事業者、医療機関における運用方法の検討
分担研究者　喜多紘一
東京工業大学　像情報工学研究施設　特任教授

研究要旨　「医療情報ネットワーク基盤検討会　最終報告」、「医療情報システムの安全管理に関するガイドライン」および「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」から、医療情報流通実現に必要とされる認証基盤等の技術的要件をまとめた。これを実現する一つとして多機能ICチップを利用したセキュアネットワークおよび厚生労働省の証明書ポリシに準拠した認証局を検討した。さらに、海外の動向を調査し、整合をとる為の技術的要件を追加した。これらの要件を実現する為にセキュアネットワークを運用する為の公開鍵証明書としては、機器証明書、ルータ開設者の公開鍵証明書、VPNサービスセンターに対する証明書、registry 等の支援サーバに対する公開鍵証明書が必要である。HPKI（保険医療福祉分野公開鍵基盤）は接続先を個別に指定する場合、医療機関や棟医師や薬剤師等を包括的に指定する場合にも友好である。各認証局は公開鍵証明書の正当性を検証できる手段を必要なドメインに対して提供する必要がある。医療機関は運用に当たり、セキュアネットワークVPNを確実に経由しているか、想定している相手と接続しているかを監視する必要がある。保険医療情報の流通を促進するにはセキュアネットワークの他にデータを共有する場合のRepositoryとしてのデータベース、その登録内容を管理するRegistryおよびID管理機能が別途必要である。さらに患者の同意の確認や、アクセスポリシーに基づいたエマージェンシー時、主治医団、一般医療スタッフおよび事務関係者によるアクセスの区別もそれぞれの医療機関で別途行う必要がある。

A．研究目的

「安全な保健医療情報流通を促進するための保健医療認証基盤を整備するための技術的方策の研究」として、HIPPA法など欧米等で進められている医療情報保護の取り組みとの関係を考慮して「保健医療分野の公開鍵認証基盤の実用化に向けた検討」、「認証業務等提供者や医療機関における運用方法や、導入・維持コストについての調査・試算」および「認証機構を用いて医療機関内部や医療機関相互に個人情報・医療情報等の安全性の確保」を研究することがうたわれている。

分担研究として「認証業務等提供事業者、医療機関における運用方法の検討」を行う。本研究では、医療に関する施設の間で電子化された診療情報を交換又は共有する場合などに、安全な医療情報の流通を推進する際に必要となる、「保健医療福祉分野に適した公開鍵基盤の構築」及び、医療機関内外において個人情報・医療情報等の安全性を確保するために必要となる「様々な権限管理に対して公開鍵基盤を活用するための技術的方策」を明らかにすることを目的とする。

その為には、「個人情報保護のありかたについて技術的側面からの具体的実現方策」、「医師・薬剤師等の法定資格の確認」、「個人データの提供と使用に関わる責任所在の明確化」および「認証基盤を利用し、医療情報を安全かつ円滑に取り扱うための技術的方策」の検討が必要となる。

特に、本研究では、現在住民基本台帳カード等で利用されているICカードと同等の機能を持ち、暗号鍵の記録や暗号演算等を安全に行うデバイスである多機能ICチップを利用することで、医療施設の間で電子化された診療情報を交換又は共有する場合において安全性を確保する技術を開発すると同時に、そこで利用される保健医療分野の公開鍵認証基盤の実用化に向けた方策について具体

的に検討することを目的とする。

B．研究方法

1）医療情報ネットワーク基盤検討会での検討結果を踏まえ安全な医療情報流通実現に必要とされる認証基盤等の技術的要件を明らかにする。

2）多機能ICチップを利用した機器等の認証機構とこれらを利用する医療従事者等の認証機構を組み合わせて、医療情報へのセキュアネットワークを構成するシステムを検討する。

3）情報の安全な流通を保証する医療情報ネットワーク基盤を実用化するために必要となる認証システムを実施・管理・運用するための要件をまとめ、システムの基本設計を行う。

4）米国 HIPPA 法など欧米等で進められている国際的な医療情報保護の取り組みを調査し、本研究で実現する医療情報ネットワーク基盤との整合性を取るために必要な要件をまとめる。

C. 研究結果

1．「医療情報ネットワーク基盤検討会」の最終報告書にみる要求事項[1]

「医療情報ネットワーク基盤検討会」は平成15年6月より医政局長の私的検討会として設置された。近年の情報通信技術に基づく医療施設間のネットワーク化への関心の高まりを踏まえ、国民の医療を受ける際の利便性の向上や医療の質の向上の観点から、その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について検討を行っている。報告書では「公開鍵基盤」、「書類の電子化」及び「診療録等の電子保存」の主要課題を中心に、取りまとめている。その中で特に本研究に直接関係する公開鍵基盤に対する要求事項を中心に抜粋する。

1．1　医療における公開鍵基盤

電子署名法に適合した電子署名の技術を適切に用いることで、署名または記名押印が義務づけられている書類については、紙媒体の書類上に署名または記名押印したことと同等に安定的に取り扱うことができ、医療に係る関係書類等の電子化及び電子保存をさらに推進することができる。

また、ネットワーク上で電子的に交換される情報の改ざん、なりすまし等を防止することにも大きく寄与できると考えられる。

医療関連の諸施設等が、患者等の診療の継続に必要なネットワーク環境を構築していくためには、以下の項目を対応する必要がある。

1）書類の電子的な様式や電子的メッセージ交換の規格等の標準化を行う

2）関係者・関係機関の合意の下に、医療分野に適した公開鍵基盤の構築を進める。

3）署名自体に公的資格の確認機能を有する保健医療福祉分野の公開鍵基盤（ヘルスケアPKI；HPKI: Health Public Key Infrastructure）の整備を目指していくことが必要である。

4）ヘルスケアPKI認証局開設は、国際的標準との整合性も念頭に置き、ISO/TS 17090（国家資格の記載はhcRole）を参酌標準として位置づけるべきである[2]。

5）ヘルスケアPKI認証局は階層構造（上位のルート認証局とその下位に位置する認証局の体系）となることを想定し、一つ又は限定された数のルート認証局の設置を準備する

6）ヘルスケアPKI全体として整合性を確保するために、各ヘルスケアPKI認証局が準拠すべき証明書共通ポリシを早期に作成し公表すべきである。

7）併せて、ヘルスケアPKI認証局が共通ポリシに準拠することを担保するための審査を行う仕組みを設けることが必要である。

8） 医療の公的資格保有の確認を効果的かつ効率的に実施するためには、免許（国家資格）に関する電子化された台帳（電子化された医籍登録情報データベースなど）の整備は将来的には不可欠となるものと考えられ、並行して準備を進める必要がある。

9）免許取得時の台帳への電子的な登録と同時に、取得者本人に対して、ＩＣカードに格納する等により秘密鍵付きの電子証明書を発行することも考慮されるべきである。

１０）電子政府及び電子自治体を構成する行政機関に対して、国民等が電子的に申請等（公的制度に基づく給付の申請等）を行う場合には、電子署名が可能な基盤の整備だけではなく、申請書本体に添付する診断書等も含め

て総合的に電子化を図る必要がある。

１１） ヘルスケアPKIが整備されるまでの対応として、当面は、「公的個人認証サービス」および「認定特定認証業務を行う認証局」の発行する証明書の適切な利用により、電子化された書類等へ医師や薬剤師等が電子署名を附与することで、医師や薬剤師等の自然人としての個人認証を行うことができる。しかし、資格や属性の確認は、電子的手段ではなく、情報の受け手の機関が当該医師や薬剤師等の所属する機関に照会するなどの方法によることとなり、現在の紙媒体による運用と同様の負担が必要である。

１２） 医療機関等を組織として認証することについては、当該組織を代表する者を自然人として認証することと併せて、開設者や管理者（病院長等）としての役割を、例えば、hcRoleに位置づけること等により、結果として組織の認証が可能となるという方法が考えられる。

１３）医療機関内での電子的個人認証や電子カルテシステムへのアクセス制限を行う等、電子署名以外の役割に基づく権限管理について、地域医療等で幅広く公開鍵基盤を活用すること等については、今後の医療分野の標準化の進展を踏まえつつ、具体的な運用の局面を想定しながら進めていくことが望ましい。

１．２　医療に係る文書の電子化および電子保存

１）患者等の情報が瞬時に大量に漏洩する危険性がある一方で、漏洩した場所や責任者の特定の困難性が増し、常にリスク分析を行いつつ万全の対策を講じなければならない。

２）一層の情報改ざん防止等の措置の必要性の高まり（責任の所在明確化、経路のセキュリティ確保、真正性保証など）により、医療施設等の責任が相対的に大きくなる。

３）蓄積された情報を外部保存を受託する機関等が独自に利活用することへの国民等の危惧が存在する。

４）診療録等は、本来、患者への診療の用に供するものであることから、法令上の保存義務を有する医療機関等においては、個人情報保護に留意しながら、電子保存された情報を必要時に直ちに利用できる体制が求められる。

５）オンラインによる医療機関等以外の場所での外部保存についても、保存主体の医療機関等が、電子保存された診療情報等を適切かつ安全に管理し、患者に対する保健医療サービス等の提供に当該情報を利活用するための責任を果たせる体制の確保を前提とするべきである。

２．「医療情報システムの安全管理に関するガイドライン」による要求事項[3]

本ガイドラインは２００５年３月に厚生労働省から出され、各施設の情報システムのポリシに合わせて、必要な章をあてはめられる章立てになっている。

すなわち、診療情報をペーパレスやフィルムレス化しない医療機関は６章まで対応すれば良く、診療情報をペーパレスやフィルムレス化して、その情報を外部保存しない機関は７章まで対応する。外部保存するところは８章まで対応する必要がある。さらに、紙やフィルムで発生した診療情報をスキャナで読み取り、原本を破棄する場合は９章に従う必要がある。

７章の「電子保存の要求事項について」では記名押印に替わって、タイムスタンプと電子署名にかえることが明記され、診療情報提供書や診断書の電子化が可能となった。処方箋は疑義照会等のシステム上の問題もあり今回は見送られた。

８章の「外部に保存する際の基準」では従来から可能であった「病院、診療所および医療法人等が適切に管理する場所」だけではなく、「行政機関等が開設したデータセンター等」および「医療機関等が震災対策等の危機管理上の目的で確保した安全な場所」も可能となっている。

９章では「診療等の都度スキャナ等で電子化して保存する場合」は電子署名とタイムスタンプを使用することにより、比較的楽に原本を破棄できる。しかし、「過去に蓄積された紙媒体等をスキャナ等で電子化保存する場合」は「対象となる患者等への周知」、「実施前の実施計画書を作成」、「電子化をおこなう場合の監査」、「委託する場合は少なくともプライバシーマークを取得しており、過去に情報の安全管理や個人情報保護上の問題を起こしていない事業者であること」等厳しい条件を課している。

前述の個人情報保護のガイドラインも安全管理に関してはこのガイドラインを引用している。

２．１　アクセスログ

６．５章の「技術的安全対策」(3) アクセスの記録（ア

クセスログ）の項目がある。

1）個人情報を含む資源については、全てのアクセスの記録（アクセスログ）を収集し、定期的にその内容をチェックして不正利用がないことを確認しなければならない。

2）アクセスログは、それ自体に個人情報が含まれている可能性があること、さらにはセキュリティ事故が発生した際の調査に非常に有効な情報であるため、その保護は必須である。

3）アクセスログへのアクセス制限を行い、削除／改ざん／追加等を防止する対策を講じなければならない。

4）アクセスログの証拠性確保のためには、記録する時刻は重要である。精度の高いものを使用し、組織内の全てのシステムで同期をとらねばならない。

2．2　外部との情報交換

6．9章に「外部と個人情報を含む医療情報を交換する場合の安全管理」の項がありそれに付いて検討する。

1）医療機関等が法令による義務の有無に係らず、外部と個人情報を含む医療情報を交換し、外部に保存を委託する場合は、情報の不適切な二次利用を防止する等、特段の個人情報保護に関する配慮が必要である。

2）個人情報を電気通信回線により伝送する場合は以下の対策が必要である。

① 秘匿性の確保のための適切な暗号化

電気通信回線を通過する際の個人情報保護は、通信手段の種類によって、個別に考える必要がある。秘匿性に関しては専用線であっても施設の出入り口等で回線を物理的にモニタすることで破られる可能性があり配慮が必要である。したがって電気通信回線を通過する際の個人情報の保護を担保するためには、適切な暗号化は不可欠である。

② 通信の起点・終点識別のための認証

通信手段によって、起点・終点の識別方法は異なる。例えば、インターネットを用いる場合は起点・終点の識別はIPパケットを見るだけでは確実にはできない。起点・終点の識別が確実でない場合は、公開鍵方式や共有鍵方式等の確立された認証機構を用いてネットワークに入る前と出た後で委託元の機関と受託先の機関を確実に相互に認証しなければならない。たとえば、認証付きのVPN、SSL/TLS やISCL を適切に利用することにより実現できる。なお、当然のことではあるが、用いる公開鍵暗号や共有鍵暗号の強度には十分配慮しなければならない。

③ リモートログイン制限機能

個人情報を含む医療情報の保存業務を受託先の機関や委託元の機関のサーバへのリモートログイン機能に制限を設けないで容認すると、ログインのためのパスワードが平文でLAN 回線上を流れたり、ファイル転送プログラム中にパスワードがそのままの形でとりこまれたりすることにより、これが漏洩する可能性がある。

また、認証や改ざん検知の機能をソフトウェアで行っている場合には、関連する暗号鍵が盗まれたり、認証や改ざん検知の機構そのものが破壊されたりするおそれもある。また、一時保存しているディスク上の個人情報を含む医療情報の不正な読み取りや改ざんが行われる可能性もある。他方、システムメンテナンスを目的とした遠隔保守のためのアクセスも考えられる。

3．「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」による要求事項[4]

本ガイドラインは「医療・介護関係事業者の義務」として、「利用目的の特定」、「利用目的の通知」、「個人情報の適正な取得」、「個人データ内容の正確性の確保」、「安全管理措置」、「従業者の監督及び委託先の監督」および「個人データの第三者提供」等に留意する必要があることを説明している。

医療施設の間で電子化された診療情報を交換又は共有する場合においては特に個人情報の利用目的および第三者提供への患者の同意が重要である。

4．上記3要求事項を踏まえた安全な医療情報流通実現に必要とされる認証基盤等の技術的要件

以上のガイドラインを総合すると医療情報流通実現に必要とされる認証基盤等の技術的要件として以下のような項目にまとめられる。

1）電子化された書類等へ医師や薬剤師等が電子署名を附与する場合は公的資格の確認機能を有する保健医療福祉分野の公開鍵基盤（ヘルスケアPKI；HPKI）を用いる（国家資格の記載はhcRole）。

2）医療機関等を組織として認証する場合は、当該組織を代表する者を自然人として認証することと併せて、開設者や管理者(病院長等)としての役割を、例えば、hcRoleに位置づけることにより、組織の認証が可能となる方法をとる。
3）蓄積された情報の外部保存を受託する機関等が独自に利活用することへの国民等の危惧を除く必要がある。
4）保存主体の医療機関等が、電子保存された診療情報等を適切かつ安全に管理し、患者に対する保健医療サービス等の提供に当該情報を利活用するための責任を果たせる体制の確保を前提とする。
5）アクセスログの収集および監視をおこなう。
6）伝送する場合は秘匿性の確保のための適切な暗号化が必要。
7）伝送する場合は通信の起点・終点識別のための認証が必要
8）伝送する場合はリモートログイン制限機能が必要。
9）医療施設の間で電子化された診療情報を交換又は共有する場合においては特に個人情報の利用目的および第三者提供への患者の同意が重要である。

5．多機能ICチップを利用して医療情報へのアクセスコントロールを実施するシステムの検討

以上の要求事項に対応する一つとして、多機能ICチップを利用した機器等の認証機構とこれらを利用する医療従事者等の認証機構を組み合わせて、医療情報へのアクセスコントロールを実施するシステムを検討する。

多機能ICチップの応用として機器に組み込みセキュアな機器を実現、あるいは、その機器同士でセキュアな通信を行うことができる。勿論、カードに組み込んで本人確認に使用することができる。ここでは、本研究の主題であるネットワークに組み込んだ場合のシステムを検討する。

多機能ICチップは２階層PKIを基本とし１階層目のPKIを利用して２階層目のソフトウエアをダウンロードできることを特徴とする。通常のVPNのパラメータ設定はオフラインで設定されるが、多機能ICチップをVPNルータに使用し、これとVPNサービスセンターを利用することにより、パラメータをダウンロード適宜設定することができる。これをセキュアネットワークVPNと称し、以下に条件を説明する。

5．1　セキュアネットワーク VPN

1）セキュアネットワークVPN Routerは、耐タンパ性を有する多機能ICチップを内蔵し、インターネット上で厳格な機器認証や利用者認証を実施し、VPNの構成情報や鍵情報をセンタからセキュアに配信する。
2）利用者がインターネットを利用してVPNの開設をVPNセンタに依頼すると、認証後直ちにVPN構成情報や鍵情報をセキュアにセキュアネットワークVPN Router　に配信しVPNの開設を完了する。
3）利用者がVPNの接続先を変更したい場合にも、センタで変更依頼を受付けてインターネットを通してセキュアに接続先を変更することも出来る。
4）設定する情報は、ICチップ内に保存されるため不正にコピーや改竄されることは無い。
5）高いセキュリティを確保し、VPN開設の手間やコストを大幅に削減することが可能になる。利用者は必要なときにVPNを即座に開設可能となり、インターネットを介した機密情報の授受を効率良く実行出来る。

5．2　２階層PKIの概念について

1）ルータの認証や構成情報、鍵情報の配信には、NICSS(the Next generation IC Card System Study group：次世代ICカードシステム研究会）で提唱する２階層PKI技術を応用し、様々なサービスを利用する機器自体の認証とその機器に様々なサービス・アプリケーションをインターネット経由でセキュアに配信・設定することが可能となる。
2）搭載されるアプリケーションや認証のための電子証明書もそれぞれ独立に多機能ICチップに配信可能となり、複数のアプリケーション間でのセキュリティも保たれる。
3）この時、１階層目の証明書は多機能ICチップによるVPN routerであることを示す機器証明書が必要である。この証明書の認証局は多機能チップ全体に一つでも良いが、VPN用、あるいは医療用など区別が付く形が望ましい。インストールもルータや機器の製造時点でインストールするのが分かり易い。

5．3　VPN接続要求とパラメータ設定

1）VPN接続をVPNセンターへ依頼する時は、接続申請書、あるいは接続許可証をVPNサービスセンターへ送り、サービスセンターより設定パラメータをダウンロードする。
2）この時、依頼者の署名用の私有鍵で署名するのが通常のオフラインの登録との整合性がとれる。相手先の指定は公開鍵証明書の提示により相手先を固定する場合や医師や薬剤師等、医療施設を特定の個人や施設を指定せずに行うことも可能である。

たとえば、オンラインレセの支払い側は相手が保険施設であればどこでも接続要求があれば許可することが考えられる。

3）また、指定する場合も前もって許可をしておけば、その相手が接続を要求してくれば、こちらの許可はその都度なくても接続を設定することtが出来る。
4）接続は施設、機器、個人の３段階があり対にすると９通りの組合せになる。
5）申請時接続の相手を確認するには別途相手側から情報を入手sするか、電話帳のようなDirectoryが必要である。
6）接続時要求する相手と正しく接続されたか野表示と公開鍵証明書を検証する等の目視による確認ができるGUIの作成がのぞましい。

6．認証システムを実施・管理・運用するための要件とシステムの基本設計

保健医療福祉分野PKI認証局は複数あっても良いが、その証明書のポリシが異なっていては、他の認証局で発行した証明書を信用するのに証明書ポリシを確認する必要が出てくる。

そのために厚生労働省は証明書ポリシを作成し、準拠することを推奨した。[5]

2005年度は準拠性を審査する為の方法をまとめ[6]、2006年はその実証を行う予定にしている。準拠していると公表された認証局は当面、自己証明書をルートとして公開鍵証明書を正当なものと検証する。

2006年の後半には厚生労働省のルート認証局を立ち上げる実証試験を行うことを予定していて、2007年度からは準拠している認証局にCA証明書を発行することとしているので、2007年度からは厚生労働省のルート認証局をルートとする証明書パスの検証を行うことができる。

電子申請の際に検証が便利なように、このルートをブリッジ認証局に接続できる要件をそなえるかは今後のブリッジのあり方を見て検討されるであろう。

さらに、公開鍵証明書が正当化、署名が正当化を検証するプログラムが適切かどうかの審査および公表もいるのではないかと思われる。

7．米国 HIPPA 法など欧米等で進められている国際的な医療情報保護の取り組みの調査

7．1　米国 EHR の例

米国は 2014 年までに全国民にＥＨＲを普及するとして、NHII(National Health Information Infrastructure)(国家医療情報基盤)計画を立ち上げるための大統領命令を発し、National Health Information Technology Coordinator という役職を設定した。

この指令に基づき National Coordinator となったブレーラ（Brailer）博士が 2004 年 7 月 21 日に計画立案し以下の提案をおこなった。

7．1．1　「4 つの目標　と　12 の戦略への細分化」

1）臨床の情報化（臨床プラクティス）
インセンティブをつけたＥＨＲの適用、ＥＨＲ投資リスク削減、地方や普及の遅れた地域へのＥＨＲ普及
2）臨床の接続（医師の相互連携）
地域相互協調の促進、国の医療情報ネットワークの開発、連邦情報システムの調整
3）医療の個人化（個人レベルのケア）
個人病歴サマリと病院への検索を持つＰＨＲの利用奨励、同意のもとでの消費者の選択拡大、遠隔医療の利用促進
4）国民健康状態の増進（地域住民医療の改善）
公衆衛生調査方式の統一、一貫した品質および健康状態監視、研究の加速と証拠に基づく実践

7．1．2　「8 つの行動計画」

機能的市場の創設(2006 年迄)，診療運営能力の拡大(2009 年迄)，効率競争の強化（其後）
1）ＨＩＴ指導パネルの創設
１０社のＣＥＯから構成され、他産業のＩＴ化の技術移転を受ける
2）ＨＩＴ製品の民間側での認定促進

ＥＨＲの投資リスク削減の為、機能、相互運用性、セキュリティ・信頼性などの評価を行う諮問委員会を設置

３）医療情報交換の拠点地域の設置

ＥＨＲの適用や活用を行い、患者安全、サービス品質向上や効率向上でのコスト低減となる地域医療情報組織（RHIO: Regional Health Information Organization）の設置

４）民間相互運用コンソーシアム創設計画

NHIN(National Health Information Network) などの計画促進を図る為、広く提案を求める為のRFI(Request for Information)を発行し、提案された内容を政府内関連の省庁で作る 100 名ほどのタスクフォースで審議し結果を発表

５）電子処方箋促進の為の標準化

2006 年のＣＭＳ近代化法に対応するために RHIO の中で薬局初め関連者が検討し、ＨＬ７なども協力し標準化をはかる。

６）ＣＭＳ近代化法に対応するポータルの確立

ＣＭＳ（Center for Medicare and Medicaid Service）近代化法に対応し予防情報の利用などを無料で行えるようにする。

７）安全なインフラストラクチャ上での研究データの共用

FDA, NIH や CDISC や製薬会社などが治験情報交換などを交換し、研究の加速を図る

８）標準の採用

HHS(The Department of Health and Human Services), DoD (the Depart of Defence) や FDA が積極的に標準の適用を行うとともに CHI（Consolidated Health Information Initiative）が２０の標準団体を選定し情報の利用を容易にし、公衆衛生の情報ネットワークへも積極的に標準の適用を進める。

(平成 16 年度経済産業省先導的戦略情報化事業（医療情報システムにおける相互運用性の実証事業報告書）事業成果報告書より抜粋補足)

７．２　HIPAA に基づく SPC の動向

売国の NEMA（National Electrical Manufacturers Association)、ヨーロッパの COCIR（European Coordination Committee of the Radiological and Electromedical Industry)および　日本の JIRA（Japan Industries Association of Radiological Systems)は共同して HIPPA　(The Health Insurance Portability and Accountability Act of 1996) を含めた「Security and Privacy」に対応する為に、「the Joint NEMA/COCIR/JIRA Security and Privacy　Committee」(SPC) を形成し、ガイドラインを発行している。現在発行されている主なものは以下である。

１）Break-Glass - An Approach to Granting Emergency Access to Healthcare Systems

２）Patching Off-the-Shelf Software Used in Medical Information Systems

３）Defending Medical Information Systems Against Malicious Software

４）Identification and Allocation of Basic Security Rules In Healthcare Imaging Systems

５）Security and Privacy Requirements for Remote Servicing

６）Security And Privacy Auditing In Health Care Information Technology

７）Security and Privacy: An Introduction to HIPAA Security and Privacy Committee (SPC)

特に５）は今回検討のセキュアネットワークに関係するもので、リモートメンテナンスに対して次の要求をしている。

１）病院のアクセス点は一つに絞る。

２）病院の入口で認証、院内外の Network で経路保証

３）システムアクセスの権限認証

４）作業監視と非常時の切断

５）VPN 等の信頼性の高いデータ転送

６）ログ収集及び監査によるトレーサビリティの向上

７）病院、RSC(Remote Service Center)のセキュリティーポリシーの策定と管理

７．３　IHE における XDS

IHE（Integrating the Healthcare Enterprise）は、1999 年にアメリカにおいて始められた。その目指すところは電子カルテを構成するために、病院内で利用される

システム間での情報の交換を標準に基づいて行うことにある。ここで遵守される標準はHL7 とDICOM を中心とするメッセージ標準である。

IHE は基本的に標準開発作業ではない。HL7 や DICOM は国際標準であるがために解釈や定義に曖昧さを残している。そこで、それぞれの国や地域ごとに標準に基づいて情報の共有、交換を行い、情報システムが診療支援を可能とする。

ためには具体的に利用される情報を定義する必要がある。この情報を定義するための活動が IHE である。そのため診療上、既存の標準が不適当であれば、それぞれの母体となる標準化機関に是正や新規標準の提案は行う。

その中で、XDS (Cross Enterprise Data Sharing) という統合プロファイルがあり、地域で医療情報を共有する場合に参考になる。セキュリティに関するITインフラストラクチャもある。米国の HER はこれを元に進められとのことである。

アクター（機能要素）としては、Document source, Document consumer, Document registry, Document Repository ～構成される。実際はさらに Patient Identity source が必要となる。

7．4 Health-ID management

EU 内を旅行などで移動した場合、本国にいるような診療を受けられるためには、EU 内でいつでも、どこでも、保険情報、処方箋、退院サマリおよびエマージェンシーデータがアクセスできる必要がある。

その為には医師や薬剤師等のプロフェッショナルや市民を識別するための”Identifier”が必要である。

その為の問題点に対する意見交換と各国の窓口の登録を行うための会議が３月２０日―２１日、オランダの厚生労働省のスポンサーにより Amsterdam で行われた。

「医師の業務は国により異なるので、ポリシーブリッジが必要である」との議論があった。

ソーシャルセキュリティ番号とは切り離した方が良いとの意見もあった。

データは一元化しないで分散させた方がよい。それを連結するものとして、オランダはスイッチボックスを導入するプロジェクトを始めるとのこと。

今後、「i2-Health」が eTEN/Euro commission の Fund を受けて検討を続けていくとのこと。

“The best is a enemy of better”, “for future children”を合言葉に各国の多様性を失わずに進めていくとのことであった。

7．5 その他の欧州の動向

カナダでは「Infoway」, イギリスでは「the Spine」としてHER が進められている。

また、オランダでは患者情報は患者のものであるとの法律を通そうとしている。さらにHER のために患者情報がどこにあるかを示すスイッチボックスを構築しようとしている。

スウエーデンではPKI をはじめている。ドイツでは検討中とのこと。

また、フランスでは2002 年に医療情報に関する患者の権利法が成立し、2004 年には16 歳以上のすべての国民の診療情報を一元的にデータベース管理する法律が成立し、2007 年の実施に向けて計画が進められている。これに対応するために、現在Sesam-Vitale2 カードが準備されている。

2005 年から16 才以上のすべての国民にSesam-Vitale2 カードが配布される予定で、このカードは従来のSesam-Vitale カードと異なり、サーバに存在する診療情報のアクセスをコントロールするためのアプリケーションも存在するマルチアプリケーションカードである。

また、医師や薬剤師等などのHealth professional に対してはGIP-CPS (Groupment d’Interêt Publique Carte de Professionnel de Santé)から発行されている。現在は保険請求に使用されているが、医療データのアクセスなどの応用が考えられている。

8．本研究で実現する医療情報ネットワーク基盤と海外動向の整合性を取るために必要な要件

４章でまとめた、技術要件に対して、海外動向との整合性を図る為には、以下のような観点の追加が必要である。

1）リモートメンテナンスに対しては「病院のアクセス点は一つに絞る」等SPC のガイドラインへの対応が必要である。

2）アクセスコントロールは「structure role」と「functional role」のポリシーマッピングをとることが必要がある。
3）Repository とリンクするために何らかのRegistryが必要である。
4）IDを管理する為のhealth-ID managementが必要である。

D．考察

安全な保健医療情報流通が必要な場面は以下が考えられる。
1）オンラインレセ請求のように特定の多数から支払機関のような特定少数機関にデータを伝送する場合
2）遠隔読影のように、契約している読影者に伝送する場合。
3）紹介状のように都度必要な医療施設にデータを送る場合。
4）紹介された患者のデータを紹介先の医療機関に見に行く場合
5）共有データベースに患者データを見に行く場合
6）医療機関が共有データベースに患者データを登録する場合
7）患者が共有データベースに患者データを登録する場合
7）患者にデータを提供する場合
8）医師が外部から主治医として患者のデータにアクセスする場合
9）医師が外部から読影等の支援を行う場合

以上をまとめると、契約により、アクセスする施設があらかじめ決まっている場合、と医療施設あるいは医師や薬剤師等という属性で包括的にアクセスを許可する場合がある事が分かる。

HPKIは個人の特定と属性としての国家資格および医療施設の管理責任者を示すのでこうした、包括的接続要求の対象の確認手段として有効である。

また、患者情報へのアクセスは原則として患者の同意が必要であるので、こうした同意を機械的に確認する仕組みも必要であるが、今後の課題である。

5章で検討したセキュアネットワークVPNを使用する際、本提案によるVPNを経由していること、ユーザとして現在接続している相手がユーザの許可したあるいは望んでいる相手に間違いないか確認できる必要がある。

その為には6章によるHPKI認証局による国家資格付および管理責任者の公開鍵証明書の内容が相手側に伝わり、有効な公開鍵証明書であることが検証できる必要がある。

このためにVPNサービス提供者はそのような検証手段とGUIを提供する必要がある。また、期待しているVPNサービスかどうかはVPN提供者およびVPNモードの確認を行う必要がある。

これは、サービスの各フェーズのVPNサービス用ルータ開設要求、接続設定要求、通信開始要求の各時点で確認できることが望まれる。そのためにVPNサービスセンターの認証も必要になる。

医療機関の運用としてはこうした確認を行う必要がある。又、提案したVPNはセキュアなチャンネルを作るだけなので、患者の同意の確認や、アクセスポリシーに基づいたエマージェンシー時、主治医団、一般医療スタッフおよび事務関係者によるアクセス管理の区別はそれぞれの医療機関で別途行う必要がある。

データを共有する場合のRepositoryとしてのデータベース、そこの登録内容を管理するRegistryやID管理は別途必要である。こうしたエンティティの管理はそのドメインでの共通、もしくは個人による管理があり、暗号化やアクセス方法等、そのシステム設計はこれからの課題である。

こうしたエンティティに対する公開鍵証明書の発行は実在性や責任の所在を示す為に必要である。

認証局は多機能ICチップの1階層目に発行して、機器の種類あるいはサービスを特定する証明書、医療機関や医師や薬剤師等などサービスを受ける人に出す証明書、VPNサービスセンターに出す証明書、アクセスをサポートする為のエンティティに出す証明書がある。認証局としては証明書の有効性を確認する為の手法の公開や認証パスの検証をおこなえる手段の提供を行う必要がある。

E．結論

機器証明書とルータ開設申請書と結びけたものにより、そのルータノードをユニークにする為の管理体制が必要

である。これはちょうど機器を購入して機器登録をするのと同じである。

VPNサービスセンターの機能としてルータ開設要求、接続設定要求、通信開始要求、接続拒否機能、強制切断要求および接続監視機能が必要である。

多機能ICチップが安全なチップであることを認定する機関あるいはルータのメーカが自己責任で認定する必要がある。

ルータメーカは１階層目の機器証明書を入手して秘密鍵とともにルータに組み込む。この時の認証局は製造メーカとVPNサービスセンターがその正当性を検証できる必要がある。

機器証明書は多機能ICチップのセキュアルータや機器等への用途を証明するもので、その認証局はメーカとの間で、私有鍵の発生と公開鍵の認証局への送付手段を取り決める。パス検証のためのルートは自己認証か更に公表された上位の認証局からのCA証明書を利用する。

ルータ開設要求、接続設定要求はHPKI証明書を用い申請書に署名を行う。申請書には接続可能な相手先を個別指定又は属性による包括指定を行う。接続相手の公開鍵証明書はあらかじめ接続あいてから入手するか、Directory から入手する必要がある。相手先は医療施設、医療機器、個人の場合がありうる。送信、受信どちらかの選択の場合もありうる。

申請に対して、受理等の返信やダウンロードの為にVPNサービスセンターに対する認証も必要となる。

通信の開始時又は設定時にダウンロードする公開鍵証明書の有効性はルータおよびVPNサービスセンターで検証できる必要がある。

セキュアネットワーク以外にRepository、Registry、ID管理およびDirectoryが必要である。これらのエンティティの安全管理に対してもセキュアネットワークは有効で、そのための秘密鍵と公開鍵証明書が必要となる。医療関係機関の場合はHPKIによる証明書を用いて開設を申請することができる。他の機関の場合はVPNサービスセンターが検証できる認証局を用いる必要がある。

さらに、その秘密鍵はエンティティが提供するデータの責任の所在および正確性を示す為の署名としても使用される。

まとめると、公開鍵証明書としては、機器証明書、ルータ開設者の公開鍵証明書。VPNサービスセンターに対する証明書、registry 等の支援サーバに対する公開鍵証明書がある。

これらの認証局は検証パスを示すともに、検証方法も周知させる必要がある。

医療機関側はVPN接続されてりか、想定している相手であるかの検証を行わなくてはならない。又、セキュアネット以外に個人情報保護を勘案したアクセス制御を行わなくてはならない。

VPNサービスセンターは医療機関に対して、接続相手先のマッチングを行い、安全にVPN経由接続である事、相手先が意図する相手である事を確認できる手段を持つ必要がある。

F．参考文献

[1] 今後の医療情報ネットワーク基盤のあり方について(医療情報ネットワーク基盤検討会　最終報告)，厚生労働省，2004,
http://www.mhlw.go.jp/shingi/2004/09/s0930-10a.html

[2]ISO/TS 17090-2 Health informatics - Public key Infrastructure Part 2: Certificate profile,(2002)

[3] “医療情報システムの安全管理に関するガイドライン”、厚生労働省，2005,
http://www.mhlw.go.jp/shingi/2005/03/dl/s0331-8a.pdf

[4]“医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン”，厚生労働省，(2004)
http://www.mhlw.go.jp/shingi/2004/12/dl/s1224-11a.pdf

[5] “保健医療福祉分野PKI認証局　証明書ポリシV1.1”，厚生労働省，2006
http://www.mhlw.go.jp/shingi/2006/03/dl/s0330-8a.pdf

[6]“保健医療福祉分野PKI認証局 証明書ポリシ準拠性審査報告書様式”，厚生労働省，2006
http://www.mhlw.go.jp/shingi/2006/03/dl/s0330-8b.pdf

[7]“厚生労働省HPKI認証局の構築・運営事業について”，厚生労働省，2006
http://www.mhlw.go.jp/shingi/2006/03/dl/s0330-8c.pdf

平成１６年度　厚生科学研究報告書

薬務関連における個人情報管理の実施方策の調査・検討

分担研究者　土屋　文人（東京医科歯科大学歯学部附属病院薬剤部）

（研究要旨）　薬務関連における個人情報管理について、その基本となる処方情報（医療用医薬品情報）及び販売規制緩和により新しい局面を迎えることとなった一般用医薬品を対象に個人情報管理の実施方法についての課題について検討を行った。国民が服用する医薬品に関する情報の一元管理は重要であるが、これらは一律にすべきではなく、国民個人個人の意思を尊重しつつ、国民が専門家のアドバイス等を受けられるべくシステム構築を行う必要がある。

A　研究目的

我が国においては電子処方せんが承認されていないことから、患者（国民）が服用あるいは使用している医薬品に関する情報を電子的に把握することは現実的には殆どされていないのが現状である。

一方、政府の「ＩＴ新改革戦略」において医療分野は「ＩＴ政策の重点項目」として位置づけられた。このため、今後医療分野において情報化が急激に進展すると思われる。

そこで　、本研究においては患者（国民）と医薬品に関する情報をどのように管理するのかについて検討を行う。

B　研究方法

研究は以下の２つの観点に分けて、薬剤師の個人認証との兼ね合いについて、医療機関及び薬局における現状分析を行うとともに、これらの情報が電子化された場合を想定し、克服すべき課題を顕在化させる。

（１）　医療用医薬品に関する処方情報と患者情報の管理

（２）　一般用医薬品に関する情報と患者情報の管理

ここで、一般用医薬品に関しては、医薬品の販売規制緩和に関する検討会が厚生労働省に設置され、種々の検討が行われ、その結果リスクに応じて販売する資格が決定された。この検討結果は平成１８年の通常国会において薬事法等の改正によって実施されると思われることから、本研究においては検討会の最終報告が実施されるという前提に立って検討を行った。

C　研究結果及び考察

（１）　医療用医薬品に関する処方情報と患者情報の管理

処方せんの電子化はいわゆる「ｅ－文書法」においても例外とされたことにあらわれているように、電子化については克服すべき課題は多い。処方情報を一元管理する方法についてはデーターデンターの設置を行い、そこで一元管理を行う方法が経産省関係のプロジェクトで示されることが多い。