200732020B

厚生労働科学研究費補助金

医療安全・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１９年度　総合研究報告書

主任研究者　大山　永昭

平成２０（２００８）年　４月

目　　次

厚生労働科学研究費補助金（医療安全・医療技術評価総合研究事業）
総合研究報告書

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、オープンなネットワーク上において誰でも安全・手軽に保健医療情報を流通可能なネットワーク基盤として、オンデマンドVPNが有効であることを示した。またオンデマンドVPNを利用した具体的なサービスへの適用モデルとして、個人が自己の保健医療情報を主体的に管理できるシステムを提案し、個人情報を管理する「電子私書箱」と連携させる方法やその効果の検討を通して、ネットワーク基盤の有効性や実現可能性を明らかにした。

分担研究者
喜多　紘一　東京工業大学統合研究院 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　産業医科大学産業生態科学研究所 准教授
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　名誉教授
山本　隆一　東京大学大学院情報学環　准教授
高橋　紘士　立教大学ｺﾐｭﾆﾃｨ福祉学部 教授
梅田　徳男　北里大学医療衛生学部　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する。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) 医療情報管理のための認証基盤における技術的要件

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の技術的要件を整理する。

（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。上記について、（イ）～（エ）にそれぞれの具体的な対策について述べる。

（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。

（エ） 患者の同意

患者の同意が必要な情報へのアクセスについては、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。

(2) 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。

(3) 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(TCG)と呼ばれる団体が行っている標準化活動である。

TCG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いる。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。

(4) オンデマンドVPNを利用した医療情報交換の実施例

オンデマンドVPNを利用した医療情報の実験システムが、加古川市（検査・検診オンラインシステム）と秋田大学病院（遠隔医療診断システム）で稼動している。

（ア） 加古川地域保健医療情報システム

本システムは、疾病の早期発見・早期治療、健診の受診率向上を目的とし、各医療機関における個人の健康に関する情報の共有機能やネットワークを介した病診連携機能を提供している。

総合保健センターでは、診療所や小規模病院から検査依頼された検体を検査し、その結果を報告書（紙ベース）にて依頼元の医療機関に報告する。また、オンラインにて、検査結果を加古川地域保健医療情報センタ（以下情報センタと略記）に送付し、管理を委託された情報センターは、検査健診データベースに情報を登録・保存する。

一方、中核病院では、独自で検体の検査を実施し、検査結果を院内の地域医療データベースに登録・保存すると共に、情報センタにオンラインにて送付し、情報センタが検査健診データベースに登録・保存する。

診療所や小規模病院では、総合保健センターより、患者や受診者の検査報告書を紙ベースで受け取ると共に、情報センターの検査健診データベースに登録された医療情報を、オンラインにて検索・参照することができる。

オープンなネットワークに接続されているため、2点間の通信はオンデマンドVPNを利用して接続されている。またそれ以外にも以下の対策を施している。

- 検査情報などの情報資産を保管するサーバの安全な場所での管理・運用とアクセス制限
- 公開情報のDMZへの配置と、通信の限定
- 外部からDMZ以外へのアクセス禁止
- サービス利用者の認証・限定
- 接続先拠点との合意
- 接続先・接続元のアドレスによるアクセス制限
- 不正な中継禁止
- HTTP、メールアクセスの制限
- ウィルスチェック

これらの対策をオンデマンドVPNと組み合わせることによって、安全なシステム運用を確保している。

（イ） 秋田大学付属病院での遠隔診断

秋田大学付属病院を中心とした遠隔診断の取り組みでは、遠隔画像読影ネットワーク及び医療画像読影依頼・レポート（ASP）システムが構築されている。本システムは、地域の小規模病院や診療所で撮影されたCTやMRIの画像の読影を、専門医のいる大規模・中核病院や大学病院に依頼し、専門医が読影を行って、その結果をレポートとして返送することで、専門医不足の解消や地域医療の向上を図ろうとするものである。

上記のシステムでは、遠隔診断システムのネットワークサービスとして、オンライン・

インターネットVPNサービスが利用されている。また、情報の暗号化やファイルへのパスワードの付与を行うと共に、オンラインサービス提供者、回線業者、医療機関などの関係者、関係機関等が、その責任範囲を明確にし、役割を果たして行くことにより、十分な安全性を確保できている。

現在、秋田大学付属病院と大森市民病院間で実施されているが、H19年度には、専門医のいる５病院とも連携を行えるよう、拡張される予定である。

(5) オンデマンドVPNを実運用する上での課題

（1）でも述べたように、医療情報を安全に交換するためには、オンデマンドVPNによる接続が極めて有効である。しかしオンデマンドVPNを実運用することを考えた場合、技術的な課題もいくつか残っている。ここではオンデマンドVPNを実運用する際の技術的課題とその解決策について検討する。

（ア） VPN管理機関が異なる場合の相互接続

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、登場するプレイヤーの具体的な役割な

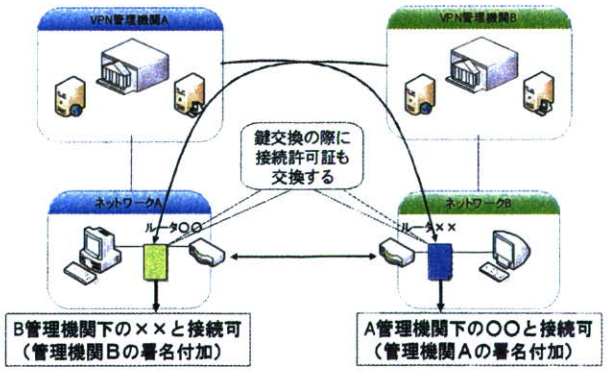

図１．接続許可証を利用した鍵交換

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。

（イ） 暗号手法の危殆化に対する対策

現在、様々なシステムで用いられている暗号の強度が近い将来危殆化するという予測がなされており、その場合に使用している暗号を安全性の高いものに更新する必要性が議論されている。しかし現在利用されている殆どのシステムでは、使用している暗号方式の更新を想定して構築されておらず、オンデマンドVPNにおいても、その対策について検討することが必要になると考えられる。ここではオンデマンドVPNの暗号方式を移行する方法について議論する。

オンデマンドVPNに用いられているICチップ内の暗号機能を更新するためには、拡張用ライブラリの追加やあらかじめ移行用の暗号ライブラリを予備として備えておく等の機能がIC チップに必要となる。しかし、製造コストの面からこういった機能を有していないチップを搭載した機器が流通することも考えられる。

そこで、更新可能なチップと不可能なチップ混在した場合でも対応可能な暗号機能移行スケジュールを検討した結果、図2のような方式が妥当であると考えられる。このスケジュールは、情報処理推進機構による「暗号の危殆化に関する調査報告書」に基づいた暗号の危殆化レベルに合わせて、レベルごとにサービス提供者及びICチップ内蔵機器がどのような対策をすべきかを示しており、レベル３で暗号の移行が勧告されると想定している。サービス提供者は、レベル３の移行期において更新可能なICチップを搭載した機器とそうでない機器の両方にサービスを提

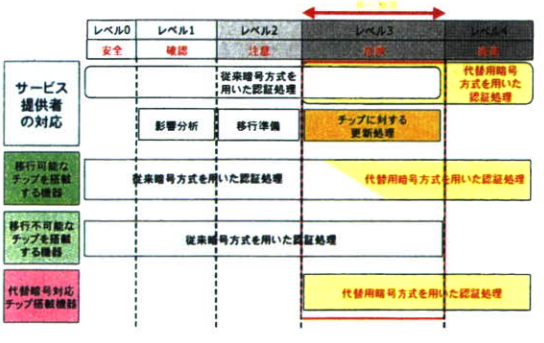

図 2. 移行スケジュールの例

供可能な体制を整えておく必要があり、また暗号機能を更新した場合にも、暗号や認証の信頼関係を維持してサービスを継続的に提供できるような仕組みが必要になる。

（ウ） 通信主体の秘匿

医療情報交換におけるVPN接続では、希少な病気を取り扱う病院との通信など通信相手の匿名性が要求されるシーンがいくつか考えられる。現状のオンデマンドVPNは、一般的なVPNと同様に通信主体の匿名性を有していないため、通信そのもの（どこからどこへ通信しているか）の秘匿を必要とする用途に用いることができない。ここでは、現状のオンデマンドVPNに対し、通信主体の匿名性を確保する技術について述べる。

一般的に通信主体を秘匿する方法としては、通信主体間の間に第三者を中継ノードとして用いることで間接的な通信を行い、特定を防ぐ方法がとられることが多い。しかし、中継ノードを置くだけでは、通信パケットの盗み見によるトラフィック解析の脅威には対応できない。よって通信主体の特定を困難にするためには、中継ノードを多数用意し、その中から使用する中継ノードをランダムに選択する中継方法が有効である。また、中継ノードを利用して通信パケットのあて先を秘匿できた場合でも、選ばれた中継ノード前後でパケットを見張られた場合、パケットの関連付けによって通信主体が特定される危険性がある。これを防ぐ為には、通信を行う２者と中継ノード間で異なる鍵で暗号化されたセッションを構築し、さらにセッションごとにパケット長をランダムに変えるなどの対策が必要になる。また、中継ノードを用いたシステムでは、中継ノードに対してパケット内容の機密性を守る為に、中継ノード前後のセッションの中を更に暗号化されたパケットを通し、二重のVPNを構築することにより中継ノードにおいても平文が見えないようにする必要がある。

以上の要件に基づき、匿名通信可能なオンデマンドVPN接続システムの一例を図3に示す。このシステムでは、匿名通信を管理する機関（匿名通信管理局）を設置し、匿名通信拠点登録情報の管理、中継ノード群の管理、セキュアルータへの匿名通信のネットワー

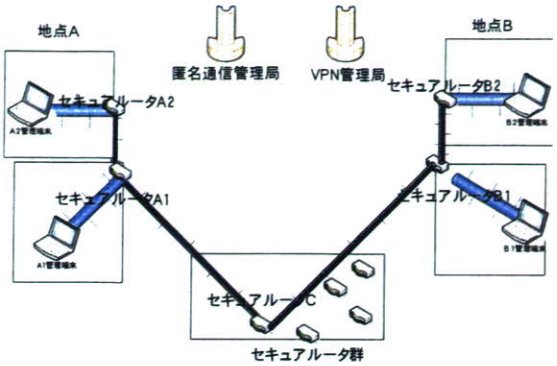

図3. 匿名通信可能なオンデマンドVPNシステムの実現例

ク構築指示という３つの機能をオンラインで実行させる。これにより、煩雑な設定をユーザは意識することなく自動的にＶＰＮ接続を構築可能である。図3のシステムの接続処理の流れを以下に記す。

① 地点Aのセキュアルータ A２が匿名通信管理局に地点Bとの匿名通信開設要求（A２の署名付与）
② 匿名通信管理局において、A２の署名検証。地点Aと地点Bが匿名通信サービスを受けられるかを照合。中継ノードとしてCを選択
③ 匿名通信管理局がセキュアルータA１、B１、B２、Cと相互認証
④ 匿名通信管理局とVPN管理局で相互認証
⑤ 匿名通信管理局からVPN管理局にA１、A２、B１、B２、C匿名通信用SPD、ルーティングテーブル構成情報、パケット長ランダム化要請配信要求
⑥ VPN管理局がセキュアルータA１、A２、B１、B２、Cと相互認証
⑦ VPN管理局がセキュアルータA１、A２、B１、B２、Cに構成情報を配信
⑧ 匿名通信管理局からセキュアルータA１、B１にCのアドレスとオンデマンドVPN開設要求を送信
⑨ A１―C間でのオンデマンドVPN設立（A１－C間でのトンネル成立）
⑩ C―B１間でのオンデマンドVPN設立（C－B１間でのトンネル成立）
⑪ A１、B１から匿名管理局にVPN開設完了通知
⑫ 匿名通信管理局からセキュアルータA２、B２にオンデマンドVPN開設要求
⑬ A２―B２間でオンデマンドVPN設立（A１－C間、C－B１間のトンネルを通す）

(6) 保健医療情報を取り扱う具体的なサービス例とセキュリティ要件

保健医療情報の流通を促進する試みとしては、地域ごとに地域医療情報管理センターなどを設置し、患者の保健医療情報を集中的に管理・利用する方法と、個人自らが自己の保健医療情報を管理し、その情報を健康増進や診察に役立てる方法がある。従来、我が国においては、前者の方法による様々な試みがなされてきたが、安全性の問題やセンター運営の費用などの問題から、必ずしも目的を達しているとは言い難い。

これに対し本研究では、平成19年4月に発表された「ＩＴ新改革戦略 政策パッケージ」に記載された“社会保障に関する国民個々の情報を国民が自らのものとして簡単に収集管理可能な仕組みである「電子私書箱（仮称）（電子情報アカウント）」”を利用することで、個人が保健医療情報を主体的に管理できる仕組みを提案し、後者の立場からの保健医療情報の流通促進を実現する。

具体的には、まず日本における個人保健医療情報管理の実現に必要なセキュリティ要件を整理し、これまでの研究で我々が提案した認証基盤を応用した実現モデルを検討する。

（ア） 個人による保健医療情報管理の現状

個人が主体的に保健医療情報を管理・運用する代表的な仕組みとして、Personal Health Record (PHR)がある。欧州では、医療情報を一元化・統合化する、EHR(Electronic Health Record)システムの整備が進んでおり、その拡張機能として、PHR機能を提供する仕組みの整備が進んでいる。また米国においては、民間中心の医療制度の下で様々なタイプのPHRの構築が進められている。PHRでは、「医療情報をどこから、どのように集めるか」という点が重要であるが、近年欧米で利用され始めているシステムでは、「外部接続性の確保」を重要機能として実装することで、「情報の入出力」という課題に対して対処することを目指している。

一方我が国では、欧米と比べ個人により保

健医療情報管理を行うシステムへの取り組みは遅れているが、IT戦略本部で2007年7月に決定された「重点計画-2007」において、「世界最先端の国民健康情報基盤を目指し、健診結果等の健康情報を個人が活用する仕組みを2011年度当初までに構築する」こと及び「国民の社会保障に関する情報を希望する国民が自ら入手・管理できる『電子私書箱(仮称)』を検討し、2010 年頃のサービス開始を目指す」ことが盛り込まれ、個人に対する健康医療情報の提供手段としての電子私書箱への期待が高まっている。

本節では、保健医療情報の流通を促進する仕組みとして、個人保健医療情報管理に必要となる「情報の入出力」に電子私書箱を利用し、本研究で明らかにした保健医療情報を取り扱う際に必要な認証基盤を組み合わせることで、個人が安全に保健医療情報を主体的に管理・運用できる仕組みを提案する。

（イ） 個人保健医療情報管理で要求されるセキュリティ技術

個人保健医療情報管理で取り扱う保健医療情報は個人情報であるため、送信された情報を本人のみが開封可能とし、同意がある場合に限り情報の閲覧を他人に許可する仕組みなどが必要になる。ここでは、そのための要件として以下の2点を挙げる。

① 個人のアカウントへアクセスするための厳格な個人認証
② 本人のみに情報が開示される仕組み（親展通信）

①については、ICカードを用いた電子認証が有効である。特に、全国どこでも質の高い保健医療サービスを受けられる“医療のフリーアクセス”を考慮すると、ICカードは、公的な公開鍵基盤(PKI)に対応し、それを利用した電子認証を用いることが望ましい。②については、サーバに保存する保健医療情報をICカード内の公開鍵証明書(PKC)に含まれる公開鍵で暗号化し、復号化には対応する秘密鍵を用いることで実現できる。このとき、秘密鍵はICカードに格納されるため、本人以外が情報を復号化することはできない。

保健医療情報のディペンダビリティの観点からは、保健医療情報を提供する医療機関と電子私書箱や個人保健医療情報を管理する機関との間の通信路は暗号化されるべきであり、スパムやDOS攻撃を防止するためには医療機関以外からのアクセスは避けるべきである。また取り扱う保健医療情報は、正当な保健医療業務従事者から提供された情報であることを保証したい。よって以下の３点を要件として挙げる。

③ 情報提供者とデータサーバ間の通信路を暗号化すること
④ 医療施設からの通信のみアクセス可能とすること
⑤ 医療従事者の提供したデータであることが確認できること

③及び④についてはオンデマンドＶＰＮが有効である。平成19年3月に厚生労働省より発行された「医療情報システムの安全管理に関するガイドライン（第二版）」では、オープンなネットワーク上で医療情報を伝送する場合の安全な通信方法の一つとしてIPsec-VPNが推奨されているが、オンデマンドVPNは、専用ルータを設置することでIPsec-VPNを容易に利用可能である。また専用ルータに組み込まれたICチップを利用して機器認証を行えるため、特定の施設からのアクセスのみに制限することが可能である。⑤についてはヘルスケアPKI（HPKI）を利用した電子署名が有効である。HPKIでは、証明書に「hcRole」という医療従事者の資格情報を記述する項目があり、HPKIの署名が付与されたデータは、どのような資格を有する人に提供されたものであるかを確認することができる。

以上の要件とその対策を表１にまとめる。

表１．保健医療情報管理に要求される技術

要件	手段
厳格な個人認証	公的なＰＫＩによるＩＣカード認証
親展通信	ＰＫＣ及びＩＣカードでの鍵管理
通信路の暗号化 医療機関の施設認証	オンデマンドＶＰＮ
保健医療情報の信頼性の確認	ＨＰＫＩによる電子署名

(7) 個人の医療情報を一元的に扱う情報管理システムの検討

（ア） システム仕様設計

前節の検討を踏まえ、個人への情報提供、管理サーバへの登録、データの参照を行うPHRシステムを設計する。

PHRシステムとして想定するプレイヤーは、個人（ユーザ）、健診センター、健診データサーバ、病院、外部連携サービスとする。特に健診データサーバは、データを個人に提供する機能をもつ部分をInBox、登録・参照する機能有する部分をViewBoxと呼ぶことにし、InBoxは将来実現される電子私書箱の機能を利用することを想定している。プロトタイプシステムにおいて想定されるシナリオの概念図を図4に示す。

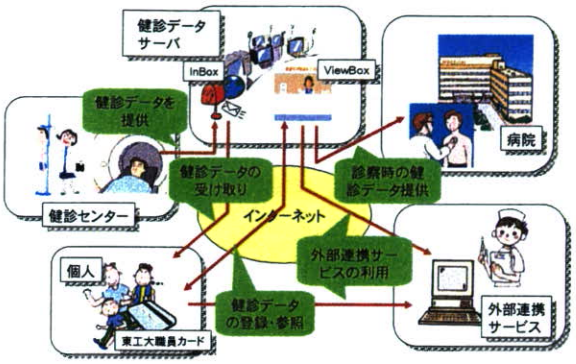

図 4. 想定する PHR システム

以下に機能ごとの仕様詳細を述べる。

(1) 保健医療データの個人への提供

健診データは特定健診のXMLベースの標準フォーマットに準拠させ、提供する健診データを作成する際にはデータ作成者（健診センターの医師など）の電子署名およびタイムスタンプを付与する。健診データは圧縮された上で共通鍵によって暗号化され、共通鍵はユーザのRSA公開鍵で暗号化される。健診センターから健診データサーバ（InBox）への送信はオンデマンドVPN接続で行う。ユーザが健診データサーバへアクセスする際にはICカードに格納されたPKIを用いた認証を行う。健診データは、ICカードに格納されたRSA秘密鍵を用いて復号化された共有鍵により、ユーザのPC上で復号化・解凍される。ユーザは、復号化された健診データに含まれる、検体検査、DICOM画像、心電図波形を専用ビューワーで参照でき、またデータに付与された電子署名及びタイムスタンプの検証が可能である。

(2) 保健医療データ管理サーバへの登録

ユーザが健診データベースサーバ（ViewBox）へアクセスする際にはICカードを用いた認証を行う。健診データはICカードに格納されたRSA秘密鍵を用いたXML暗号処理を施され、暗号化された状態でViewBoxへ登録されるため、ユーザ本人以外は登録された健診データを閲覧することはできない。登録時には健診データに付与された電子署名及びタイムスタンプの検証を行う。

(3) 保健医療データのオンライン参照

ユーザが健診データサーバ（ViewBox）へアクセスする際にはICカードを用いた認証を行う。健診データサーバとユーザPCの通信はSSLとするが、病院に設置されたPCより参照する場合にはオンデマンドVPN接続とし、その場合健診データのダウンロードを可能としている。健診データの参照時には、ICカードに格納されたRSA秘密鍵を用いてユーザPC側で共有鍵を復号化した後、それをサーバに送付してXML復号処理を行い、検体検査、画像、波形などのデータはWebブラウザを利用して参照する。またサーバ側には、健診データに付与されている電子署名及びタイムスタンプを検証できる機能を付与している。参照が終わったら、データを再暗号化して健診データサーバに保存するため、ユーザ本人が健診データサーバに接続している時以外は、他の者が登録された健診データを閲覧することはできない。さらに、ユーザが同意した健診データは外部連携サービス用サーバへ転送し、そのサービスを利用することができる。

(4) 医療機関間のオンデマンドVPN接続

VPN接続許可のためのポリシーマッピングを行う際に、医療機関であることを確認する。医療機関であることを確認する方法には、HPKIによる電子署名を利用する。ポリシーマッピングによって接続先が医療機関であることが確認された場合のみ、VPN接続を許可する。

（イ） プロトタイプシステムの構築及び動作実験

前節の仕様検討に基づき実験システムを構築した。個人認証用のＩＣカードとしては、

ＰＫＩ機能を有する東工大の職員証を利用し、またオンデマンド VPN は、㈱ＮＴＴＰＣコミュニケーションズの IP-members を利用した。システム図および外観を図 5 および図 6 に示す。

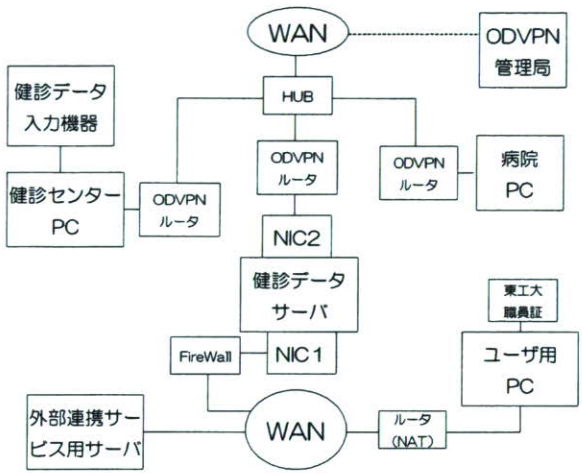

図 5. プロトタイプシステムの構成図

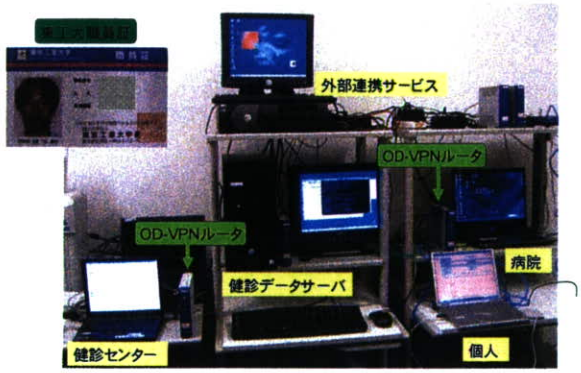

図 6. プロトタイプシステムの外観

以下にそれぞれの動作結果について述べる。

(1)　健診データ入力

健診センター用 PC にインストールされた専用 AP を利用し、ユーザ情報に関する情報や健康診断に関する情報を登録した上で、検体検査、問診、画像、波形等の結果を入力する。また、検索等に必要な情報をメタデータとして入力する。ユーザ登録の際には、健診データを暗号するためのユーザの公開鍵証明書を登録する。

(2)　健診センター・健診データサーバ間のオンデマンド VPN 接続

オンデマンド VPN 用管理 AP を利用して、健診データサーバへ接続要求する。接続要求する前には、サーバ条件、クライアント条件を登録し、接続合意を取っておく。

(3)　健診センターから InBox へのデータ送付

オンデマンド VPN の接続完了後、健診センターの専用 AP を利用して健診データサーバの Inbox へデータを送付する。この際、標準フォーマットへの変換、データの圧縮、電子署名、タイムスタンプの付与が行われる。

(4)　InBox から個人用 PC へのダウンロード

ユーザ PC の専用 AP を利用して健診データをダウンロードする。ユーザは InBox へアクセスすると認証要求が来るので、IC カードを利用してユーザ認証を行う。認証成功後、InBox 上のデータ一覧が表示されるので、必要なデータを選択し、ダウンロードする。ダウンロードしたデータは、メタデータは表示されるが、データの本体は暗号化された状態なので見ることはできない。

(5)　個人用 PC でのデータ復号化および閲覧

ユーザ PC の専用 AP を利用して健診データの復号化を行う。復号化されたデータには参照用 Viewer ソフトが含まれているので、これを利用して健診結果のデータを閲覧する。また、参照用 Viewer を利用して電子署名およびタイムスタンプの検証を行うことができる。

(6)　個人用 PC へダウンロードしたデータの ViewBox への登録

ユーザ PC の専用 AP を利用して InBox からダウンロードしたデータを ViewBox へ登録するためのデータフォーマットへ変換する。Web ブラウザから ViewBox へアクセスし、職員証を利用したユーザ認証を行う。ViewBox へ登録するデータを選択し、登録を行う。

(7)　InBox に保存されているデータの ViewBox への登録

ユーザ PC の専用 AP を利用して InBox 上のデータを ViewBox へ直接登録する。登録が完了すると Web ブラウザが立ち上がり、健診結果を参照できる。

(8)　個人用 PC から ViewBox へ登録されている健診データの参照

ViewBox へアクセスし、ユーザ認証を行う。メニューの中から、一覧もしくは検索によって参照するデータを選択し、健診結果を参照する(図 7)。画像や波形も Web ブラウザ上で閲覧可能である(図 8)。また、電子署名およびタイムスタンプの検証結果を確認することができる(図 9)。

(9)　外部連携サービスへ提供、利用

ViewBox での参照画面で、健診結果内に表示されている外部連携ボタンを押すと、その検体検査の結果が外部連携サービスに送付され、外部連携サービス(ヘルスアップ WEB)が別の Web ブラウザ上で起動する(図 10)。このサービスでは、送付した検体検査結果に基づき健康チェックを行うサービスである。

(10)　病院内 PC でのデータ参照及びダウンロード

病院内の PC で参照する場合には、まず病院と健診情報管理サーバとの間をオンデマンド VPN 接続する。その後ユーザの PC と同様に ViewBox へアクセスし、健診結果を参照する。また病院の場合にはデータのダウンロードも可能であり、ダウンロードしたデータはユーザ PC で復号化したデータと同様に専用 Viewer を用いてデータを閲覧可能である。

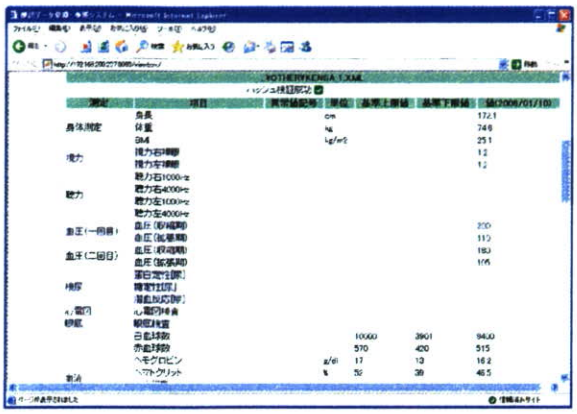

図 7.　ViewBox での参照（検体検査結果）

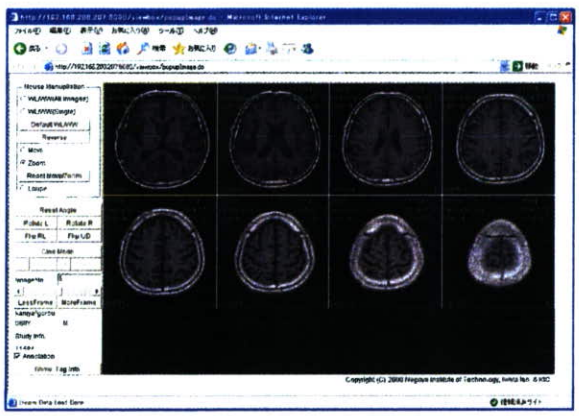

図 8.　ViewBox での参照（画像検査結果）

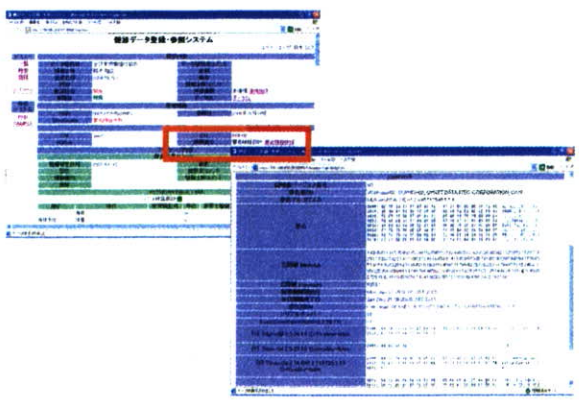

図 9.　ViewBox での署名検証結果

図 10.　外部連携サービスの利用

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。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、また個人情報保護を実現しつつ必要な保健医療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。このような基盤の整備により、患者が他の医療施設へ紹介される際の負担軽減、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、個人が自己の健康管理に役立てる等、国民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。

また、検討した認証基盤を具体的なサービスへ適用した実験結果より、システムの運用に関する考察を以下のように整理した。

（ア） システムの安全性について

今回構築した PHR のプロトタイプシステムでは、我々の設定したセキュリティ要件を満たしているが、暗号アルゴリズムの危殆化や悪意の第三者のよる様々な攻撃方法に対する対策についは今後検討の必要がある。

（イ） システムの利便性について

システムを利用するためには、専用ソフトウエアやICカードを利用する環境をインストールする必要があり、誰でも容易に利用可能な状況になっていない。PCを利用する場合には、プラットフォームに依存しないWebブラウザでの実装が望ましい。また、より汎用的な端末を考えた場合、地上波デジタルテレビや携帯電話のような機器での実現が望まれる。

（ウ） 実現可能性について

提案するシステムでは、我々が研究を進めてきたオンデマンド VPN を利用することで保健医療情報を提供する提供者を医療機関のみに限定することができるが、このためには専用ルータを設置する必要があり、すべての医療機関がオンデマンド VPN を利用できる環境を整えることが大きな課題となる。しかし、これについては、2010 年度までにレセプト提出及び受領の完全オンライン化がすべての医療機関に義務付けられており、オンラインレセプトを行うためには、ISDN、IP-VPN といった専用回線を利用するか、もしくは IP-sec と IKE を利用したインターネットでの VPN が必要とされている。ここで、回線速度や運用のコストを考えると、オンライン請求を行う医療機関の多くはオンデマンド VPN を利用すると予想され、提案システム導入の課題である情報流通基盤整備は、一気に進むものと考えられる。

電子認証を行う IC カードについては、すべての国民が利用可能な認証基盤が必要になるが、住民基本台帳カードと公的個人認証サービスがすでに運用されており、今後公的個人認証サービスの電子認証への拡張が実施されれば、これを利用する方法が考えられる。また、「重点計画-2007」には、健康保険証などとしての役割を果たす『社会保障カード(仮称)』 を 2011 年度中を目途に導入することも明記されており、有力な候補である。

また、「情報の入出力」としての電子私書箱が公的な機関によって設置され、ユニバーサルサービスとしての提供が開始されれば、希望する国民はだれもが医療機関との間で安全に保健医療情報をやり取りできるようになり、保健医療情報の流通が促進されるこ

とで、新たな保健医療産業の発展が期待できる。

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、オンデマンドVPNやHPKI等のセキュリティ技術が有効であることを示した。またこれらの技術を実際のサービスへ適用する際の検討として、個人健康医療情報の安全な流通を促進するシステムモデルを提案し、現在政府で検討が進められている電子私書箱や社会保障カードと連携することで、安全・安心な保健医療情報の流通が可能であることを示した。

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(2005)
- 大山永昭：医療機関における個人情報保護とセキュリティシステム；日本病院会雑誌，53(10)，118-136(2006)
- 丸山剛，喜多紘一，鈴木裕之，小尾高史，谷内田益義，山口雅浩，大山永昭：医療分野における自己情報コントロールを目的としたアクセス制御方法に関する研究；電子情報通信学会論文誌，J90-D(12)，3170-3180(2007)

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 (2006)
- 小尾高史，鈴木裕之，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 のための鍵交換手法；ワイヤレス・テクノロジーパーク 2006 講演予稿集，20-21(2006)
- 押田知己，谷内田益義，鈴木裕之，小尾高史，山口雅浩，大山永昭：多機能 IC チップを利用したネットワークサービスにおける暗号技術の更新とサービスの継続利用の実現；電子情報通信学会 2007 年総合大会講演予稿集，225(2007)
- 浦野雄平，小尾高史，大山永昭，谷内田益義，鈴木裕之：多機能 IC チップを利用した任意多地点間 VPN における通信主体情報の秘匿；電子情報通信学会 2007 年総合大会講演予稿集，230(2007)
- 鈴木裕之，喜多紘一，谷内田益義，小尾高史，山口雅浩，大山永昭：ＨＰＫＩによる電子署名を利用した健康管理データ提供・参照システム；ワイヤレス・テクノロジーパーク 2007 講演予稿集，56-57(2007)
- 喜多紘一，平井正明，鈴木裕之，谷内田益義，山口雅浩，小尾高史，大山永昭：CDA R2 に準拠した個人提供用健康診断結果報告書を利用した個人健康情報管理システム；第 27 回医療情報学連合大会 （第 8 回日本医療情報学会学術大会）予稿集，P7-4 (2007)
- 喜多紘一，鈴木裕之，竹田忠雄，猪俣彰浩，島田宏，有馬一閣：HPKI とダイナミック・オンデマンド VPN との連携によるセキュアな医療ドメインネットワーク；第 27 回医療情報学連合大会 （第 8 回日本医療情報学会学術大会）予稿集，1-H-3-2 (2007)
- 喜多紘一，鈴木裕之，竹田忠雄，猪俣彰浩，島田宏，有馬一閣：VPN 接続許可をポリシー制御可能なダイナミック・オンデマンドＶＰＮ；SCIS2008(暗号と情報セキュリティシンポジウム)予稿集，4C2-2 (2008)
- 岡野　翔，鈴木裕之，小尾高史，山口雅浩，谷内田益義，大山永昭，喜多紘一：個人情報の利活用を可能とするサービス基盤に関する研究；電子情報通信学会 2008 年総合大会講演予稿集，520(2008)

Ⅲ. 研究成果の刊行に関する一覧表

雑誌

発表者氏名	論文タイトル名	発表誌名	巻号	ページ	出版年
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 (5)	1129-1136	2005
秋山昌範	不正行為を調査するデジタル・フォレンジック医療分野における重要性	COMPUTER & NETWORK LAN	23 (3)	27-32	2005
山本隆一	海外の医療現場での個人情報保護の動き	INR インターナショナルナーシングレビュー	28 (5)	42-45	2005
山本隆一	診療情報システムと個人情報保護	医学のあゆみ	215 (4)	231-234	2005
山本隆一	プライバシーの考え方と個人情報保護	看護展望	30 (5)	17-20	2005
山本隆一	医療における個人情報保護とセキュリティ	日本病院会雑誌	52 (1)	106-124	2005
小尾高史 他４名	多機能ICチップを利用した任意多地点間VPNのための鍵交換手法	ワイヤレス・テクノロジーパーク2006講演予稿集		20-21	2006
大山永昭	IT新改革戦略における医療の情報化の概要	Japan Medical Society	5月号	53-54	2006
大山永昭	医療機関における個人情報保護とセキュリティシステム	日本病院会雑誌	53巻10号	118-136	2006
押田知己 他5名	多機能ICチップを利用したネットワークサービスにおける暗号技術の更新とサービスの継続利用の実現	電子情報通信学会2007年総合大会講演予稿集		225	2007
浦野雄平 他5名	多機能ICチップを利用した任意多地点VPNにおける通信主体情報の秘匿	電子情報通信学会2007年総合大会講演予稿集		230	2007

山本隆一	遠隔画像診断のセキュリティと個人情報保護	Rad Fan	5巻1号	18-19	2006
山本隆一	電子カルテとプライバシー保護	日本医師会雑誌	135巻9号	1954	2006
八幡勝也 他6名	健康管理を支援する情報技術	第26回医療情報学連合大会論文集		150	2006
小林慎治 他5名	医療分野における Open Source Software 活用の現状と問題点	医療情報学	26,5	341-350	2006
Tachibana H., Omatsu M., Higuchi K. and Umeda T.	Design and development of a secure DICOM-Network Attached Server	Computer Methods and Programs in Biomedicine	81,3	197-202	2006
Umeda T., Okawa A., Ikeda T., Yamamoto H. and Harauchi H.	Visit Nursing Station System with Secured Internet Communication using Watermarking Technique: Tele-nursing System Experments	14th International Conference on Cancer Nursing		196-197	2006
丸山剛,喜多紘一,鈴木裕之,小尾高史,谷内田益義,山口雅浩,大山永昭	医療分野における自己情報コントロールを目的としたアクセス制御方法に関する研究	電子情報通信学会論文誌	J90-D(12)	3170-3180	2007
鈴木裕之,喜多紘一,谷内田益義,小尾高史,山口雅浩,大山永昭	HPKI による電子署名を利用した健康管理データ提供・参照システム	ワイヤレス・テクノロジーパーク2007講演予稿集		56-57	2007
喜多紘一,平井正明,鈴木裕之,谷内田益義,山口雅浩,小尾高史	CDA R2 に準拠した個人提供用健康診断結果報告書を利用した個人健康診断結果	第27回医療情報学連合大会(第8回日本医療		P7-4	2007

,大山永昭	管理システム	情報学連合大会)予稿集			
喜多紘一,鈴木裕之,竹田忠雄,猪俣彰浩,島田宏,有馬一閣	HPKI とダイナミック・オンデマンドVPNとの連携によるセキュアな医療ドメインネットワーク	第 27 回医療情報学連合大会(第 8 回日本医療情報学連合大会)予稿集		1-H-3-2	2007
喜多紘一,鈴木裕之,竹田忠雄,猪俣彰浩,島田宏,有馬一閣	VPN 接続許可をポリシー制御可能なダイナミック・オンデマンドVPN	SCI2008(暗号と情報セキュリティシンポジウム)予稿集		4C2-2	2008
岡野翔,鈴木裕之,小尾高史,山口雅浩,谷内田益義,大山永昭,喜多紘一	個人情報の利活用を可能とするサービス基盤に関する研究	電子情報通信学会 2008 年総合大会講演予稿集		520	2008
大山永昭	電子政府・電子自治体の実現について	月刊 日本行政	412	10-18	2007
大山永昭	政府が掲げる IT 戦略は、“正しい方向”を向いているか “国家 IT 戦略”から“変化の時代”を正しく読み解く	CIO Magazine	83	20-28	2007
大山永昭	医療情報システムのネットワーク環境と基盤の整備を推進します	月刊 新医療	Vol.34 No.390	152-155	2007
大山永昭	住基カードの今後の展開～利便性を実感できるカードとして活用の幅が広がる～	月刊 LASDEC	Vol.37 No.8	6-7	2007
八幡勝也 他	産業保健が抱える問題点と解決策	特定健診制度に対して産業保健が		233-247	2007

		抱える問題点と解決策、これでわかる特定健診制度			
八幡勝也	3.特集 1『健康情報シリーズ第２回』生涯健康管理の重要な要件となる健康情報システムについて	Report of the Society of HDS	Vol.11 No.2	18-22	2007
八幡勝也	特定健診制度と産業保健の問題点と解決策	第 27 回医療情報学連合大会	S11-2-C	140-141	2007
山本隆一	医療情報の安全管理	医学のあゆみ	Vol.222 No.8	571-575	2007
Katsuya Tanaka,Mayumi Yoshida, Ryuichi Yamamoto	Secure Remote Access for Web Based Clinical Information System Using Policy Control of PCs and Healthcare PKI Authentication	MEDINFO 2007		1480	2007
Omatsu M., Umeda T., Tachibana H., Okawa A.	Development of Narratine Based Medicine(NBM) Automatic Medical Comminication System	The Kitasato Medical Journal	Vol.37 No.2	65-75	2007
Kenta Miwa, Tokuo Umeda, Nao Fukuchi, Shuji Yamamoto, Akio Okawa, Hidenobu	A Novel Security Model for Hiding in Medical images using High-Capacity Digital Watermark And Steganography	93th Scientific Assembly and Annual Meeting Rediologi-		841	2007