H20501335A

別紙1

厚生労働科学研究研究費補助金

医療技術評価総合研究事業

医療VPNとPKIを併用した安全な医療情報交換インフラの構築と運用に関する研究

平成17年度　総括研究報告書

主任研究者　木内　貴弘

平成18(2006)年　4月

別紙2

目　次

別紙3

厚生労働科学研究費補助金(医療技術評価総合研究事業)
総括研究報告書

医療VPNとPKIを併用した安全な医療情報交換インフラの構築と運用に関する研究

主任研究者　木内貴弘　東京大学医学部附属病院大学病院医療情報ネットワーク研究センター教授

研究要旨　本研究の目的は、施設の認証に基づき医療機関等をVPNで相互接続する医療VPNと、個人認証をもとにしたPKIを併用することによって、安価で運用のしやすい、安全な医療情報交換基盤の構築と検証を行うことにある。平成17年度は、システムの設計・開発および各地域医療ネットワークにおける運用形態と対象アプリケーションの検討を行った。PKIについては、参加研究者のサイトにWebベースで使えるCA、及び1台で多数の端末から使用でき、汎用性も高く、柔軟な利用が可能な暗号電子メール対応のWebメールシステムを開発した。またこれまでに構築してきた医療VPNインフラを活用し、やりとりされる情報のハッシュ値を電子署名付きで記録するシステムをこれに追加した。これによって、やりとりされる情報の追跡可能性が向上し、医療VPNの安全性が高まることが期待される。実験予定のアプリケーションについては、各地域医療ネットワークの実情にもとづき、病診連携、遠隔医療等が検討された。

分担研究者

廣川博之
(旭川医科大学付属病院企画経営部)
辰巳治之
(札幌医科大学附属情報処理センター教授)
山本晧二
(三重大学医学部附属病院医療情報部教授)
井上裕二
(山口大学医学部附属病院医療情報部教授)
原　量宏
(香川大学医学部附属病院医療情報部教授)
中島直樹
(九州大学病院医療情報部講師)

末永貴俊
(熊本大学医学部附属病院医療情報経営企画部助手)

A. 目的

医療分野におけるIT化の推進のためには、ネットワークを介して、遠隔地の医療情報を安価に安全に交換するための技術と運用管理法の確立が絶対に必要である。本研究の目的は、「施設認証にもとづく医療VPN」と「個人認証にもとづくPKI」の併用方式による、運用が容易で安全な医療情報交換基盤の構築と運用管理法の提案にある。

B. 方法

本研究で開発・運用するシステム、及び各地域ネットワークでの運用形態について、各主任・分担研究者が事前作成した資料を元に全員で検討を行った。また将来的な発展性も考慮して、IPv6の併用による医療VPNの運用等についても技術的な検討・応用分野の検討を行った。更にメーリングリスト等を通じて、開発・運用するソフトウエアの詳細設計、必要な修正、及び各地域ネットワークでの運用形態・実験に利用する具体的なアプリケーションについての検討を行った。

C. 結果

C.1 システム仕様策定・開発

下記のシステムの仕様策定・開発を行った。システムの構築には、オープンソースのソフトウエアを基本的なツールやライブラリーとして用いた。

(1)PKIを利用した通信ツールの開発

医療VPNと併用して用いるPKIを利用した通信ツールとして、暗号メール対応のWebメールシステムの開発を行った。ベースとなるWebメールとしてIMP、SqWeb、UMIN Webメール等についての再度調査、比較検討を行い、日本語対応(日本語を利用した場合に、IMP、SqWebメールで文字化けや動作不良が見つかった)信頼性、負荷の軽さの観点からUMIN Webメールをベースにして、開発を行うことにした。暗号化のためのライブラリーとして、当初OpenSSLだけ想定していたが、運用のしやすさや個人利用者の利用しやすさを考慮し、OpenSSLと両方が使えるような形を想定して、システムの開発を行うこととした。

(2)公開鍵認証局(CA)の構築

暗号メール対応のWebメールシステム等で利用する公開鍵認証局及びこれとWebメールシステムとのインターフェイスについて、PERLを用いて、独自に開発する方針とし、必要な仕様の策定を行った。この際、GNUPGとOpenSSLの両方の利用を考慮した仕様とした。

(3)医療VPN内交信記録システムの構築

QMAILをベースにして、医療VPN内で交換される情報のハッシュ値を電子署名付きで記録するソフトウエアの仕様策定を行った。ハッシュ関数として、SHA-256を採用することとした。

C.2 地域医療医療ネットワークにおける構築と運用等

具体的な各地域医療ネットワークにおける医療VPN、PKIの運用形態・アプリケーションの内容については、各々の分担研究報告書で詳しく記述されている。ここではそのアプリケーションの内容をごく簡単に一覧として示す。

(1)旭川医科大学遠隔医療センター
(分担研究者:廣川博之)
遠隔医療に関するデータ通信全般

(2)三重遠隔画像診断ネットワーク
(分担研究者:山本晧二)
画像診断読影レポートの送受信

(3)やまぐち健康福祉ネットワーク
(分担研究者:井上裕二)
遠隔医療と医療機関連携全般

(4)周産期ネットワーク
(分担研究者:原　量宏)

周産期医療ネットワークにおける情報交換

(5)カルナ事業(九州大学、福岡市医師会等)
(分担研究者:中島直樹)
カルナ事業事務局とかかりつけ医療機関との情報交換

(6)熊本大学医学部附属病院
(分担研究者:末永貴俊)
「ひごメド」電子カルテにおける各種の情報交換

C.3 IPv6による医療VPNの検討

IPv6の活用した将来的な医療VPNの運用形態についての検討と考察が「IPv6の活用」(分担研究者:辰巳治之)にまとめられている。現行の医療VPNのようにprivate addressを活用することなく、IPv6の利点である膨大なアドレス空間を活用したVirtual Global Network(VGN)の提唱である。特にモバイル環境の場合に医療VPNの接続が非常に簡便になり、遠隔患者モニターリング、救急車と医療機関の情報交換に役立つものと思われる。現行では、IPv6の普及が不十分なため活用基盤がないが、今後の普及と活用が期待される。

D. 考察

インターネットを利用して安全に情報交換を行うための方策として、厳密な個人認証を利用したPKIを活用するのが一般的であり、様々な試みが数多く行われてきている。PKIは特定の企業内等での運用実績はあるもの、運営主体を異にする多数の事業体が存在するような分野で、大きな国家レベルで広く普及して使われている例はほとんど存在しない。それは、個人認証をベースとしたPKIは、暗号鍵発行のための個人確認の方法、公開鍵認証局による公開鍵の署名、鍵の発行管理等の手続きが煩雑で高コストであるという難点があるためである。特に大規模な運用になるとこの難点は一層顕著となる。

VPNを利用して、特定の企業内、もしくは複数の関連企業間を相互接続して、安全に情報をやり取りする試みは数多く行われている。しかしながら、医療VPNのように、標準を規定することによって、運営主体を異にする事業体を相互接続する試みは国際的にも他に類例がない医療VPNは、低コストで運用が容易であるという利点があるが、PKIと比較してセキュリティ保護の厳密さに劣っている。

本研究の特色は、医療VPNとPKIの併用によって、低コストで運用が簡便な医療情報基盤の実現を図ろうという点にあり、このようなアプローチ法は医療分野以外の分野でも他に類例がないユニークな試みである。医療VPNとPKIを併用することによって、1)通信先の追跡可能性の向上、2)複数の暗号方式の組み合わせによるセキュリティ強化、3)相互のフェイルセーフ機能等の実現が可能であり、セキュリティの一層の向上が期待できる。従って、両者を併用することによって、PKI運用上の煩雑さを軽減しつつ、一定レベルの安全性を確保することが可能であり、全体としての運用のコストと労力の削減が期待できる(図)。本研究の成果により、安価で安全な医療情報交換のための新しい技術・方法が構築され、医療分野でのe-Japanの実現のための基幹技術に発展していくことが期待される。

E. 結論

医療VPNとPKIの併用によって、安いコストで、安全性の高い医療情報交換が可能になると考

えられる。平成17年度は、上記の運用実験をするための、(1)PKIを利用した通信ツール、(2)公開鍵認証局(CA)、(3)医療VPN内交信記録システムの開発と、各地域医療ネットワークにおける運用法とアプリケーションの検討を行った。

F. 研究発表

(1)木内貴弘. インターネットで変わる臨床研究. 医療白書. 日本医療企画(東京)、417-421、2005

(2)大塚健一、門川英男、村井伸昭、吉田元、松葉尚子、木内貴弘. 次期UMIN電子メールサービスの概要. 第25回医療情報学連合大会論文集 (CD-ROM)、日本医療情報学、2005

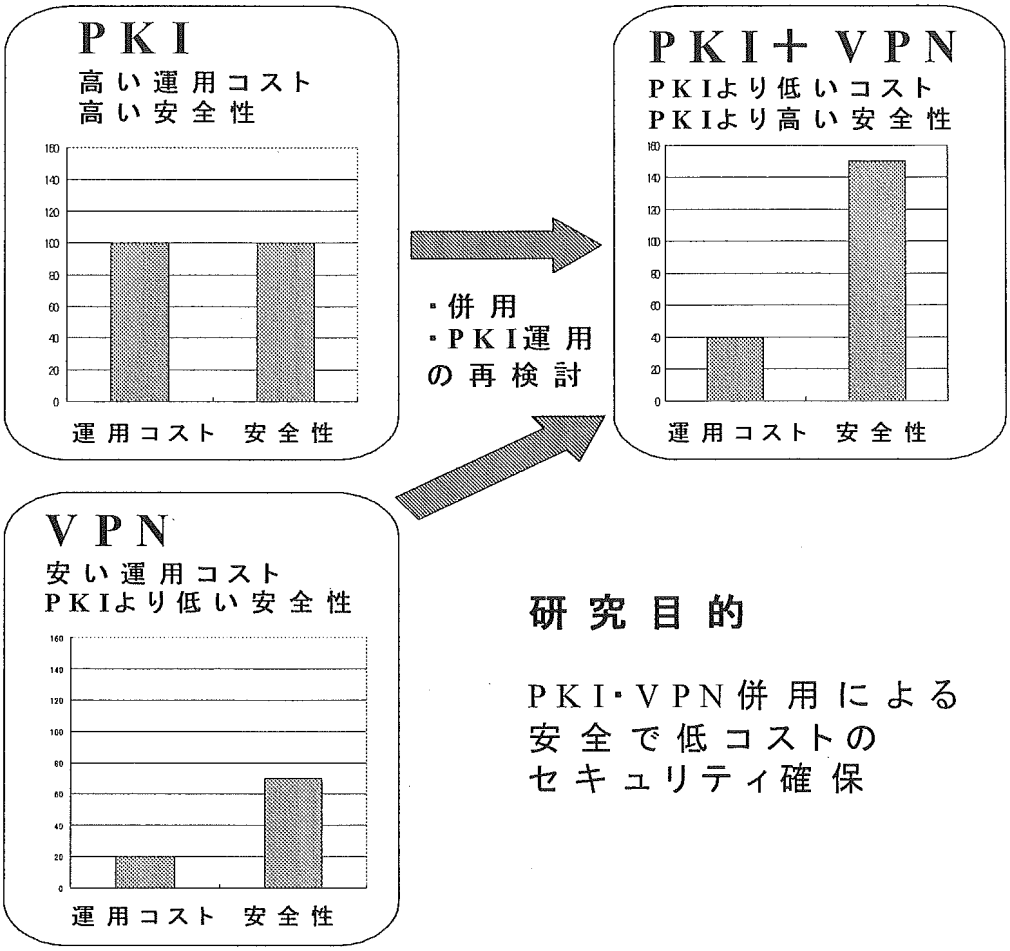

図. VPNとPKIの併用によるメリット

厚生労働科学研究費補助金(医療技術評価総合研究事業)
分担研究報告書

医療VPNとPKIを併用した安全な医療情報交換インフラの構築と運用に関する研究
― 旭川医科大学遠隔医療センターにおける構築と運用の方法

分担研究者　廣川博之　旭川医科大学病院　経営企画部　教授
研究協力者　山上浩志　旭川医科大学病院　経営企画部　講師

研究要旨　医療VPNとPKIを併用した安全な医療情報交換基盤の構築に向け、旭川医科大学病院遠隔医療センターに於けるネットワーク設計を行なう。IPベースのセキュアで広域な通信インフラが整備されることで、遠隔医療サービスに新しい拡がりの生じることが期待される。

A　研究目的

旭川医科大学病院遠隔医療センター(以下、単にセンターという)に於いて、医療VPNとPKIを併用した安全な医療情報交換インフラを構築する上で、必要なネットワーク設計を行なう。

B　センターの提供サービスと情報インフラ

旭川医科大学では、附属病院に隣接した遠隔医療センター施設を中心に、全科で遠隔医療を日常的に実践している[1][2][3][4][5][6]。例えば、放射線部門では、遠隔地の病院より伝送を受けたCT・MRI画像に対し診断所見レポートをオンラインで返すシステムを、施設間にVPN装置を対向で設置したセキュアなネットワークインフラを用いて運用している(図1)。又、病理部門では、相手施設内の顕微鏡をセンター側から遠隔操作しながら精度の高い迅速診断を可能とするシステムが導入されている。そのほか、テレビ会議システムを利用したコンサルテーションやカンファレンスが眼科をはじめとする全診療科でNTSCやHD画像を外部入力に併用しながら行われている。

又、これら直接的な医療支援とは目的を異にするが、2003年10月より「北海道メディカルミュージアム(以下、メディカルミュージアムという)」を実践している。これは旭川医科大学が行う地域貢献事業の一環として位置付けられているもので、旭川市及び近隣市町の住民を対象にIPテレビ会議システムを用いた遠隔講座であり、一回当たり60分～90分の双方向な番組編成としている。これまで全6回、内科、整形外科、眼科領域よりテーマが選定され、8～21ヶ所より参加があった[7][8][9][10]。

このようなセンターが提供するサービスは、大学や病院側の情報ネットワークとは独立した網内で行なわれている。現在、ISDN回線(INS64×15回線, INS1500×3回線)、及びADSL回線(12M×1回線, 24M×1回線, Bフレッツ×1回線)を利用して行なっているが、2005年度にセンター側装置の更新によりIP対応化が図られ、契約回線の見直しについても近く行なう予定である。装置のIP化によって、様々なメディアで蓄積されている医療情報を統一的に扱うことが可能になり、相手側に必要な設備として専用装置、専用回線を必要とせず、PCベースな装置と安価な通信回線サービスが利用できるため、遠隔医療がより日常的な医療形態に近づくと考えられる。

そのほかセンターには、独立行政法人情報通信研究機構(以下NICT)が管理する次世代超高速・高機能研究開発テストベッド・ネットワーク(JGN2)が時限付きながら用意されている。アジア地域との遠隔医療・遠隔教育等の各種アプリケーションに関する実証実験を目的としたもので、2006年2月には、シンガポールナショナルアイセンターとの間で、眼科手術を題材にハイビジョン-3D動画像を用いた国際遠隔医療カンファレンスが行なわれた[11]。

更に、安定した地上回線の確保が難しい地域への対応として、衛星回線を用いた遠隔医療インフラも用意されており、センターと稚内市内及び利尻島の医療機関に衛星機器一式を設置して、衛星インターネット回線を通じた遠隔医療実証実験をJSAT(株)の協力を得て進行中である。

B　研究方法

本研究のテストベッドには、2004年度に構築された医療VPN旭川医大サイト(ドメイン名:asahikawa-med.hvpn.net)を用いる。そこに、新たに認証局(CA)サーバ及びセキュアなメールサーバを組み入れることにより、PKIによる一層安全な医療情報交換を行うためのネットワーク基盤が整う。

同時に、医療VPN旭川医大サイトについても、構築当時と比べてセンター提供サービスが変容してきていることから、この機会にあらためて機能や構成を再検討を加え、必要な見直しを実施する。

C　研究結果

C.1　外部通信回線・サービス

インターネット接続にはBフレッツ(ベーシックタイ

ブ)サービスを利用し、グローバルIPアドレスはOCN-IP8(サブネットマスク:29ビット、使用可能なIPアドレス:6個)により取得済みである。医療VPNサイト構築に必要となるIPアドレスは、これらプールされたアドレスの中から用いている。

又、これとは別に、NTT東日本が提供するフレッツグループアクセスライトサービス(最大参加拠点数:10箇所)によりプライベートグループ内で運用するネットワークがある。それは、図1に示した放射線領域での画像伝送と、函館及び帯広市内の医療機関間で行なわれているハイビジョン動画像伝送用途で利用されているもので、これまでフレッツ・ADSL-8Mタイプ、ADSL-24Mタイプで各々契約していたものを、経済性と運用性に照らして、Bフレッツ(ベーシックタイプ)サービス一本に集約することとした。

C.2 遠隔医療ネットワークの概構成

遠隔医療センターネットワークの内、医療VPNサイトが属するOCN-IP8を利用するネットワーク系での全体構成図を図2に示した。

外部ネットワークとの通信経路には次の四つがあるが、図中の番号と対応付けて各々多少の説明を加える。

[1] 医療VPN(非VPN系)

ユーザサービスとして用いる経路ではないが、医療VPNセグメント(VLAN#B)から、例えばサーバがインターネット上のタイムサーバと時刻同期を行なう、ウイルス定義ファイルの更新を行うといった用途に用いる。

[2] 医療VPN(VPN系)

医療VPNサービスにおいて利用される経路である。対向に配置したVPN装置、若しくはVPNクライアントソフトウエアを用いることで、VPN通信路が確立される。

[3] メディカルミュージアム

メディカルミュージアムではインターネット画像会議システム(onsori.com製)を用いており、そのサーバはセンターに配置されている。聴講対象者が固定されないこと、動画像データ通信なため、最大限のパフォーマンスを確保したいために、ファイアウォール装置を介さずにインターネットに接続する。

[4] 遠隔医療実践系

この経路で日常的な遠隔医療業務が実践される。VPN通信機能を併備したファイアウォール装置をインターネットとの間に挟むと共に、IPS(侵入検知、防御ソフトウエア)により不正なアクセスを監視する。VLAN#Cの下位にはサーバ系、クライアント系、ネットワーク管理系、部門業務系(救急系、病理系、手術系、放射線系)等、用途別にVLANを分離して構成しており、原則的にレイヤ2動作での運用がなされている。

C.3 医療VPNセグメント構成

医療VPNセグメントは、図3に示すように、ルータ装置(RT(1))下にファイアウォール装置(FW(1))、VPN装置(VPN)を組み合わせて実装されており、各装置には運用上必要となる最小限のパケット通過ルールを定義している。

医療VPNサイトの運営に不可欠なサーバ機能としては、DNSサーバ、MAILサーバ、SYSLOGサーバ、NTPサーバが挙げられる。SYSLOG及びNTPサーバについてはオプションであるが、サイト内のセキュリティ管理、保守等の用途の為に用意することが望ましい。このほか、コンテンツ公開のためにWWWサーバ、Database(DB)サーバを用意している。

本研究では、この医療VPNセグメント上にCAサーバ及びセキュアなメールサーバを追配置することとした。

CAサーバ並びにメールサーバは、セキュリティ上の理由からこれらサーバは二台に物理的に分離された形態としている。又、アプリケーションソフトウエアの動作条件に基づき、OSにはLinuxを採用している。これらサーバのハードウエア故障は実質的にネットワークダウンを意味することから、ハードディスクをミラーリング(RAID-1)した耐障害性を高めた仕様としている。今回用意した機器の一覧を表1に示した。

医療VPNセグメント(VLAN#B)に配置された装置に対して、コンテンツのアップロードやWWWブラウザを介したメールの読み書き、ログ参照等のサーバ管理が内部ネットワーク側から行なえるように 通信経路[5]を用意している。内側ネットワークに向かう脅威を低減するために、ファイアウォール装置(FW(2))とルータ装置(RT(2))を組み合わせた構成を採っている。

D 考察

医療VPN、PKIに対応したインフラが当遠隔医療センター内に出来たことで、当院が進める遠隔医療サービスの形態にもコンテンツの幅が増すものと考えられる。

VPN通信では通信路がトンネル化され、流れるデータは隠蔽されるため、インターネット上では生データを伝送するのは危険と判断される情報についても、VPN通信路であれば安心して流通可能であり、且つPKIによる個人認証が行なわれることで、セキュリティの一層の向上が期待できる。

D.1 PKIを用いた他構築事例

旭川医科大学病院情報システムに於いては、ファイアウォール機能の一部として、PKIプライベートCAが実装され運用が行なわれている(Pentio PKI PrivateCA)。秘密鍵と電子証明書はPKI-USBトークンに格納され、このUSBトークンがPCのUSBポートに接続されていない限り、そのPCから病院情

報ネットワークにアクセスすることは出来ない。このUSBトークン方式はPC内部に証明書(秘密鍵)が残らない点で安全でもある。

このCAとVPN装置とを組み合わせることにより、インターネット側にセキュアなメンテナンス環境が構築できる。実際、限られたシステム管理者のみが利用するユースケースにおいて、この方式は特別な不都合もなく運用が行なえている。

D.2 医療 VPN アプリケーションの検討

筆者らは平成14年度から16年度にかけて、P2Pネットワーク上で医療情報を安全に流通させるために必要なシステム要素技術の研究開発とアプリケーションソフトウエア(眼科用広域版電子カルテシステム)の開発を行なってきた[12][13]。今後、医療VPN上でその動作検証を行なう予定である。

E 結論

旭川医科大学病院遠隔医療センターに於いて、医療VPN、PKI基盤を用意する上で必要なネットワークインフラの設計を行った。セキュアで広域な通信インフラが実装されることにより、遠隔医療サービスの質的向上に資することが期待される。

参考文献

[1] 廣川博之, 山上浩志, 吉田晃敏: 旭川医大附属病院での眼科遠隔医療. 医療情報学20 (Suppl.2): 652-655, 2000.

[2] 廣川博之, 山上浩志: 旭川医科大学病院を中心とした遠隔医療システムの現状と将来. Digital Medicine 2(4): 59-62, 2001.

[3] 廣川博之, 山上浩志: 遠隔診断とカンファレンス. 現代医療 34(3): 125-129, 2002.

[4] 廣川博之, 山上浩志, 吉田晃敏: 旭川医科大学附属病院での遠隔医療の現状と将来. 医学物理 23(1): 16-23, 2003.

[5] 峯田昌之, 高橋康二, 山田有則, 長沢研一, 稲岡努, 山本和香子, 油野民雄: 旭川医大付属病院遠隔医療センターにおける放射線科画像診断の運営状況. 第7回遠隔医療研究会論文集: 72-73, 2003.

[6] 三代川斉之, 加藤志津夫, 徳差良彦, 佐渡正敏, 平沼法義: テレパソロジーの現状・課題・対策と当院における工夫. 第7回遠隔医療研究会論文集: 76-77, 2003.

[7] 「旭医大 ネットで講義配信 旭川などの4施設へ」. 北海道新聞, 平成15年10月10日.

[8] 「旭川医大 ネット講演会で医療相談 地域貢献へ 4会場結ぶ」. 読売新聞, 平成15年10月10日.

[9] 「ネット活用し医療公開講座 旭医大が2回目」. 北海道新聞, 平成16年3月17日.

[10] 北海道メディカルミュージアム. http://www.u-p.co.jp/hmm/.

[11] NICT報道発表「世界初の国際間3次元高精細画像伝送実験の実施」. http://www2.nict.go.jp/pub/whatsnew/press/h17/060215/060215.html.

[12] P2P 型高信頼情報流通に関する研究開発プロジェクト研究開発最終報告書. 独立行政法人情報通信研究機構, 平成 17 年 3 月.

[13] 山上浩志, 浪岡智朗, 林弘樹, 山本明仁, 続木雄磨, 乗越雅光, 坂井豪, 廣川博之, 吉田晃敏, 三田村好矩, 下野哲雄, 橋本真幸, 田中卓也, 清本晋作, 山田明, 松本修一, 小池淳:遠隔医療とP2P型医療情報ネットワーク. 日本遠隔医療学会雑誌 1(1): 100-101, 2005.

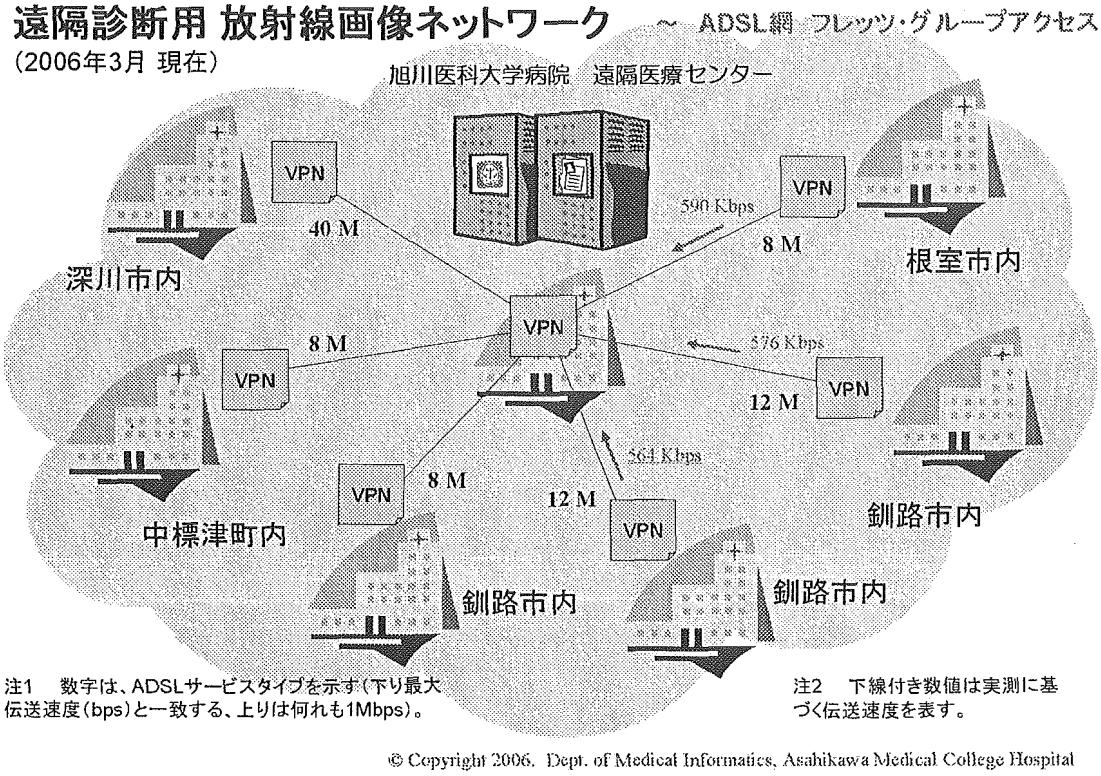

図1 遠隔医療ネットワーク(放射線画像の遠隔診断用途)

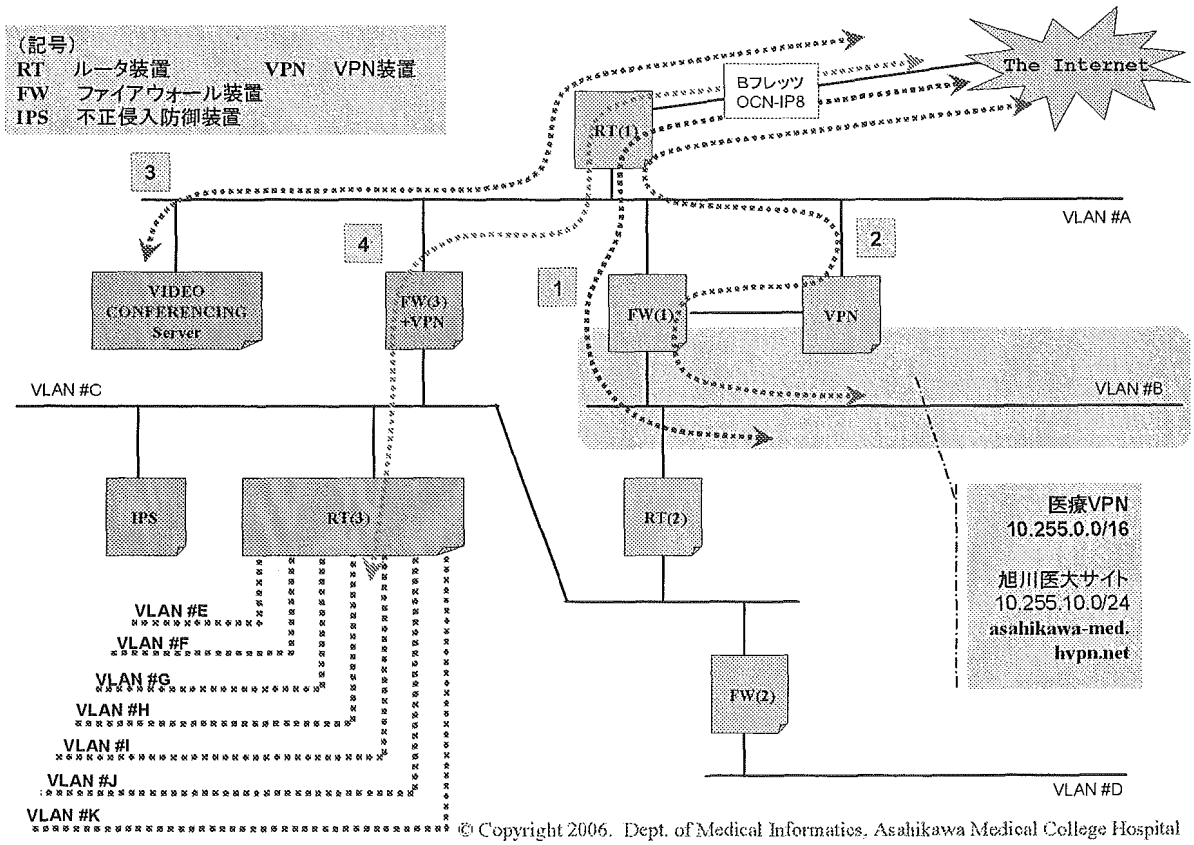

図2 遠隔医療ネットワーク全体構成図

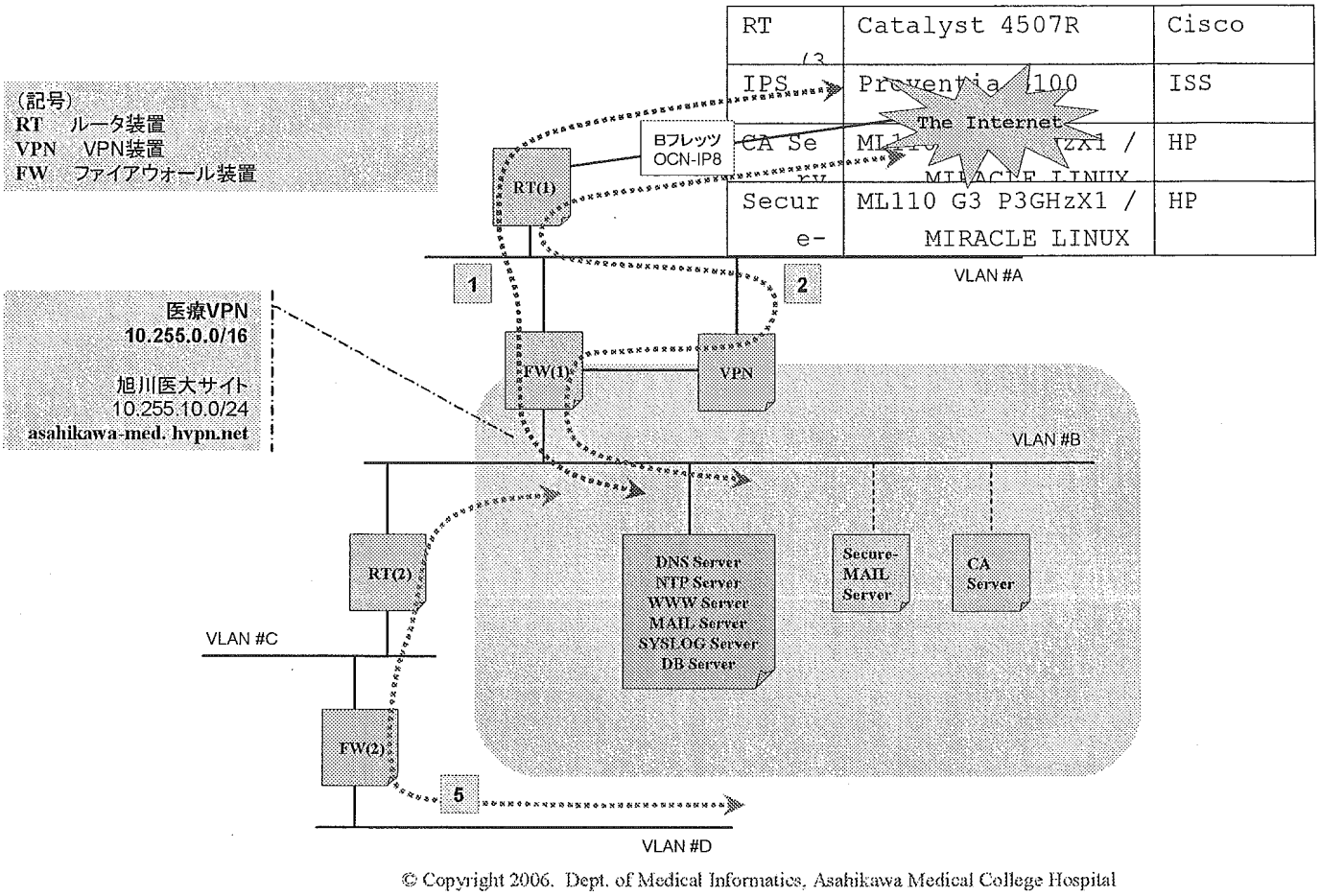

図3 医療VPN旭川医大サイト構成図

表1 構成機器一覧

表中、SERVERはDNS Server、NTP Server、WWW Server、MAIL Server、SYSLOG Server、DB Serverの総称として用いている。そのほかは、図2、図3の表記と対応する。

名称	型式等	メーカ
RT (1)	RTX-1000	Yamaha
FW (1)	Netscreen-25	Netscreen
VPN	CES-600	Nortel Networ
FW (2)	Pix-515	Cisco
RT (2)	Cisco-2651	Cisco
SERVER	Power Mac G5 / Mac OS X server 1	Apple
FW (3)	Netscreen-50	Netscreen
RT (3)	Catalyst 4507R	Cisco
IPS	Proventia 1100	ISS
CA Server	ML110 G3 P3GHzX1 / MIRACLE LINUX	HP
Secure-MAIL Server	ML110 G3 P3GHzX1 / MIRACLE LINUX	HP

厚生労働科学研究費補助金(医療技術評価総合研究事業)
分担研究報告書

医療VPNとPKIを併用した安全な医療情報交換インフラの構築と運用に関する研究
— IPv6の活用

分担研究者　辰巳治之　札幌医科大学大学院医学研究科　生態情報形態学教授
研究協力者　親身隆彦　札幌医科大学大学院医学研究科　生体情報形態学　助手
明石浩史　札幌医科大学附属情報センター　講師
大西浩文　札幌医科大学附属情報センター　助手
戸倉　一　札幌医科大学附属情報センター　訪問研究員
西城一翼　札幌医科大学附属情報センター　研究生
山口徳蔵　札幌医科大学附属情報センター　研究生

研究要旨　医療分野におけるIT化の推進のためには、医療情報を安価に安全に交換するための技術と運用管理法の確立が絶対に必要である。そこで医療情報ネットワークの具体的な利用を念頭に置き、種々のアプリケーションを動かした際の問題点を明らかにし、その利用促進の方策を考える。そこで、安全性を確保しながら、出来るだけ簡単に利用できる方法を検討し、医療系ネットワークにおいての様々な利用シーン(ホームヘルスケア、健康管理システム、遠隔医療、遠隔講義等)を想定し実証実験を行った。我々の開発しつつあるシステムはVGN(Virtual Global Network)というもので、アドレスに関しては、PrivateではなくGlobal IPv6 Addressを利用しようというものである。もちろんIPv4アドレスも利用できる。また、アドレス体系に関してはIPv6 Topological Addressing Policyに従ったものを利用している。モバイルパソコンでVPNを実現しようとすると、どうしてもインターネットにさらされてしまうため、このことによる危険性は避けられない。一方、我々のシステムのVGNboxはインターネットにさらされるが、モバイルパソコンのアドレスは、医療系VGNのもので、まったく外のインターネットに触れることがない。この点が、今後のインターネット脅威を考えたときには、大きな利点になりうると考えている。医療系における情報化を推進するにあたり、目に見えない障害となる色々なファクターがあり、それらがある程度クリアーされないと医療系における情報化の推進は難しい。我々の分担では、安全、簡単、安価を目標に研究開発を進めている。今回の研究では、まずは、安全にかつ簡単にVGNネットワークを構築することが可能であることを示すことができた。

A. 研究目的

医療分野におけるIT化の推進のためには、医療情報を安価に安全に交換するための技術と運用管理法の確立が絶対に必要である。医療VPNは、低コストで運用が容易であるという利点があるが、PKIと比較してセキュリティ保護の厳密さに劣っている。一方、PKIは厳密な個人認証によるセキュリティ保護が可能であるが、運用法が煩雑で高コストになりがちであるという欠点があり、急速な普及は当面困難な状況にある。そこで、低コストによる安全な医療専用ネットワーク形成のために必要な医療VPNの可能性とその問題点を明らかにし、今後の発展性を検討し、安全な医療情報交換インフラの構築と運用に関する研究を行うのが目的である。

B. 研究方法

医療情報ネットワークの具体的な利用を念頭に置き、種々のアプリケーションを動かした際の問題点を明らかにし、その利用促進の方策を考える。そこで、医療情報ネットワークに必要な要件として、安全・安価に加え容易に利用できるということが医療ネットワークに置いては非常に重要になってくる。そこで、VPNにおける便利さをもちながら、簡単にセットアップして利用できるところに力点を置き、さらに次世代のネットワークプロトコールであるIPv6(Internet Protocol Version 6)の利用の可能性を検討し、実験ネットワークを構築し、その実験から得られた経験から、次の解決策を模索する。

C. 研究結果

医療情報交換のインフラとして、大きく分けて2種類が考えられる。
1. インターネット環境であればどこでも使えるもの、2. インターネット環境以外に、特別なものが必要で十分に準備された環境で利用できるもの。

我々の目指している安全な情報交換インフラを構築しようとする場合にはどうしても後者になってしまう。そこで、安全性を確保しながら、出来るだけ前者に近

づける為の方法を検討した。また、その際には医療系ネットワークにおいての様々な利用シーン(ホームヘルスケア、健康管理システム、遠隔医療、遠隔講義等)を想定し、実証実験を行った。

実証実験を行う中で、コスト・パーフォーマンス及び利用のしやすさを考え、近年急激に普及しているskypeに注目した。その利点は、なんといっても安価(IP同士は無料)でインストールが簡単なこと。必要なものはコンピュータ、マイク、スピーカ、USBカメラである。IP同士なら、無料で、固定電話や移動体電話に通信するときには有料になるが、非常に安い。一分0.266円ほどである(携帯へは一分17.5円)。また、IP同士ならTV電話にもなり、複数の接続ができ会議も可能でファイルの転送なども行える。また特筆すべきことは、エコーキャンセラーの性能がよく音声が非常によい。ノートパソコンに標準装備のスピーカ、マイクでも十分に使用に耐える。さらに、ファイアーウォールを越えることが出来る。唯一の欠点は、音質を良くするためにCPUを使うために、遅いノートパソコンではかなり粘ついたり、音質がわるくなる。

医療系でIT化を推進するときにはskypeに学ぶべきところは非常に多い。そこで医療系VPNの場合で各施設ごとを繋げるときには、VPN機器を対向で設置する。また、施設とモバイルパソコンを繋げるときには、施設側はVPN機器で、モバイルパソコンはソフトでVPNを実現する。いずれの場合も、名前の通りPrivate Networkなので、予めアドレスを決めてネットワーク構築をしておく必要がある。

実際の利用シーンを考えると、VPNソフトの場合、実際にはそのソフトのインストール、接続相手の設定、そしてパスワード入力などの操作が必要である。

我々の開発しつつあるシステムはVGN(Virtual Global Network)というもので、アドレスに関しては、PrivateではなくGlobal IPv6 Addressを利用しようというものである。もちろんIPv4アドレスも利用できる。また、アドレス体系に関してはIPv6 Topological Addressing Policyに従ったものを利用している。

このシステムは、Skypeの便利さまでは行かないが、従来のVPNシステムよりも簡便になっている。VGNのserverとVGN clientのBOXが必要ではあるが、VPNのソフトを起動しパスワードを入れなくてもよいという点がある。VGN clientのBOXは持ち運びできるぐらいのサイズである。この箱を、インターネットコンセントとPCの間に接続するだけで、医療系IPv6ネットワークに接続することが可能となる。

施設とモバイルパソコンとの間にVPNを張る場合、モバイルパソコンをまずインターネットに接続して、医療系VPNと接続するときのみ、VPNとなる。即ち、このノートパソコンがインターネットにさらされてしまうため、このことによる危険性は避けられない。一方、我々のシステムのVGNboxはインターネットにさらされるが、モバイルパソコンのアドレスは、医療系VGNのもので、まったく外のインターネットに触れることがない。この点が、今後のインターネット脅威を考えたときには、大きな利点になりうると考えている。

D. 考察

VGN boxを利用した利点は、VPNの場合、パスワードを盗まれアクセスされると侵入される危険性がある。パスワード紛失に関しては、その実体があいまいなので管理が非常に難しい。すなわちパスワードが漏れていても、それが漏れたのかどうかも全くわからない。

一方我々のシステムは、BOXで実現しているので、この箱がなくなればすぐに分かり、VGN serverの方ですぐにブロックすることができる。このようにセキュリティーの管理という点では非常に判りやすく優れている。

Skypeに比べ劣るところは、FireWallである。Server側のセキュリティ監視を高めどこからでもアクセスすることを可能にはできるが、一方で、各施設、各インターネット環境で、手前にFireWallがある場合、そこをすり抜けないと通信ができない。不思議なことに、どういう工夫をしてあるのか、Skypeでは、ほとんどの場合通信が可能となっている。おそらく、汎用のポートをいくつか使い、工夫をしているものと考えられる。そこで、今後我々のBOXでも汎用のポートに切り替え、自動選択が行えるようにしたいと考えている。

Skypeでは、非常にパーフォーマンスがよく、通信経路をオプティマイズしていいる可能性がある。そこで、われわれは、まずは、安定性確保のためにMulti-Homeの導入を考えると共に、Multi-Pathをはり効率のよい経路選択が可能かが今後の検討課題である。

E. 結論

医療系における情報化を推進するにあたり、目に見えない障害となる色々なファクターがあり、それらがある程度クリアーされないと医療系における情報化の推進は難しい。我々の分担では、安全、簡単、安価を目標に研究開発を進めている。今回の研究では、まずは、安全にかつ簡単にVGNネットワークを構築することが可能であることを示すことができた。これらの利用価値も実際のいろいろな利用シーンにおいて実証実験をくりかえし普及可能なものにブラッシュアップする必要があると考える。今後の普及を考えると、すべて完璧なレベルを達成できなくてもある程度のレベルを満足できれば、普及に拍車がかかるものと考えている。最高のものを目指し研究開発を推進する一方で、具体的に安全・安価・簡単に使える利用シーンを提供することも必要であろうと考えている。

F. 研究発表

1. 論文発表

(1) 辰巳治之、新見隆彦、中村正弘、高橋正昇、明石浩史、戸倉一、大西浩文、村井純、南政樹、三谷博明、田中博. ITとATを活用した情報薬の開発. 医療情報学 25.Suppl, 2005, 766-767

(2) 戸倉一, 明石浩史, 大西浩文, 新見隆彦, 西城一翼, 山口徳蔵, 西陰研治, 辰巳治之, 今井浩三. End to End Multihome 解説. Proceedings of NORTH Internet Symposium 2005 (ISSN 1345-0247), Pp19-20 (2005)

(3) 辰巳治之, 新見隆彦, 中村正弘, 高橋正昇, 明石浩史, 戸倉一, 村井 純, 南政樹, 三谷博明, 田中博. 情報薬とゼロクリック-戦略的防衛医療構想を支えるもの:ITとATのフル利活用. Proceedings of NORTH Internet Symposium 2005 (ISSN 1345-0247), Pp33-42 (2005)

(4) Akashi H, Tokura H, Ohnishi H, Nishikage K, Yamaguchi T, Saijo K, Shimmi T, Nakamura M, Nakayama M, Tatsumi H. Establishment and Assessment of Wide Area Medical Information Network System in Hokkaido. Lecture Notes in Computer Science. 2005, 3597:179-189.

(5) 明石浩史、中村正弘、戸倉 一、大西浩文、西城一翼、山口徳蔵、新見隆彦、西陰研治、木村眞司、佐々木茂、澤田いずみ、今野美紀、片寄正樹、仙石泰仁、相馬 仁、小海康夫、丸山知子、辰巳治之、今井浩三. 各種ビデオ会議システムによる遠隔地教育支援の実際と評価. 医療情報学 25.Suppl, 2005, 1046-1047.

(6) 戸倉一、藤川健二、明石浩史、大西浩文、西城一翼、山口徳蔵、新見隆彦、西陰研治、中山正志、辰巳治之、今井浩三. エンドツーエンドマルチホーミング技術を使用した医療施設間通信. 医療情報学 25.Suppl, 2005, 877-878

(7) 明石浩史、竹原孝治、河合修吾、中村正弘、重田光雄、戸倉一、大西浩文、西城一翼、山口徳蔵、新見隆彦、西陰研治、馬場啓好、山口千寿、木村眞司、佐々木茂、澤田いずみ、今野美紀、片寄正樹、仙石泰仁、相馬仁、丸山知子、辰巳治之、今井浩三. 札幌医科大学附属情報センターにおける教育支援のとりくみ. Proceedings of NORTH Internet Symposium 2005 (ISSN1345-0247), 2005, 11:106-113.

2. 講演・学会発表

(1) 辰巳治之.「ユビキタス健康管理と情報薬-戦略的防衛医療構想を支えるもの-ICTとATのフル利活用」H17年4月23日 第一回ユビキタス医療シンポジウム (一橋記念講堂)

(2) 辰巳治之,「楽しみながらやる生活習慣病予防:ICTとATのフル利活用」総務省:情報通信月間 H17年5月10日NORTH健康セミナー

(3) 辰巳治之, ユビキタス健康管理と情報薬「戦略的防衛医療構想」H17年5月20日 新社会システム総合研究所 セミナー(虎ノ門パストラル)

(4) 辰巳治之, 究極の代替医療 情報薬による戦略的防衛医療構想. H17年5月25日 第12回PML研究会(大阪薬業年金会館)

(5) 辰巳治之. ICTとATによるユビキタス健康管理情報薬を実現する:戦略的防衛医療構想を支えるもの: H17年5月26日 ITRC研究会 (名古屋)

(6) 辰巳治之 IPv6ユビキタス医療ネットワーク戦略的防衛医療構想実現に向けて. H17年6月11日 和歌山地域医療ネットワーク協議会 (アバローム紀の国)

(7) 辰巳治之. ICTとATによるユビキタス健康管理情報薬による代替医療の可能性:戦略的防衛医療構想を支えるもの. H17年6月30日 JIMAシンポジウム(市ヶ谷アルカディア)

(8) 辰巳治之. NORTHの歴史を振り返って21世紀を考える. 平成17年度 NORTH定期総会 記念フォーラム札幌医科大学50周年記念ホール (H17.7.6)

(9) 辰巳治之. 生命科学からの発想による情報科学の医療応用:戦略的防衛医療構想. H17年9月8日 FIT2005 中央大学.

(10) 辰巳治之. 知(先)見性の科学を解剖学する. H17年9月10-12日 (伊豆 大仁ホテル) JST異

分野融合ワークショップ「知見性の科学ー経験、類推、発見と適応」

(11) 辰巳治之．生命科学からの発想によるシステム(社会)安全についての考察．H17年10月6日 JAXAシステム安全研修（東京）

(12) 辰巳治之．ITで変わる！地域医療？戦略的防衛医療構想，ICTフル利活用による情報薬の開発．H17年10月21日 鶴岡医師会

(13) 辰巳治之．End Userから見た医療ネットワークの理想．HEASNET 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 第5回利用促進部会．H17年10月28日 （東京）

(14) 辰巳治之．IPv6-VGNへの期待と医療応用：情報薬の開発応用．ITRC研究会．H17年10月24日(天人閣)

(15) 辰巳治之．高度情報化社会における形而上学的諸問題の解明：個人情報保護・セキュリティ．H17年11月2日第5回 個人情報保護対策セミナー，主催:JAMINA，共催:NORTH（札幌）

(16) 辰巳治之．生活習慣病克服への挑戦．H17年11月5日 京都きづ川病院文化月間行事＆創立25周年（文化パルク城陽）

(17) 辰巳治之．NORTHについて．H17年11月8日 JPNIC セキュリティセミナー in 札幌

(18) 辰巳治之．CTとATによるユビキタス健康管理情報薬による代替医療の可能性：戦略的防衛医療構想を支えるもの．H17年11月9日 BB-Consortium Japan（東京）

(19) 辰巳治之．ITの医療応用としての戦略的防衛医療構想ゼロクリックによる逆ナースコールと情報薬の開発．H17年11月12日 よくわかるIPv6セミナー・CSIインターネット利用研究会 広島県情報プラザ

(20) 辰巳治之．u-Japanに向けて全国へのフィールドの拡大と情報端末の多様化を行う工業系高等学校等に於けるIPv6を用いたユビキタス社会実験研究の展開．H17年11月26日 uJapan研究会

(21) 辰巳治之．ITとATを活用した情報薬の開発．H17年11月26日 日本医療情報学会（横浜）

(22) 辰巳治之．ネットワーク社会における医療情報とは．H17年12月14日 JIMAフォーラム（東京）

(23) 辰巳治之．ITの医療応用と感性工学への期待：生活習慣病克服への挑戦．2006年2月3日 感性工学会（北海道大学）

(24) 辰巳治之．ICTフル利活用による戦略的防衛医療構想：情報薬の開発とリハビリへの応用．H18年3月11日山形県臨床整形外科医会春季総会

(25) 辰巳治之．戦略的防衛医療構想の第一歩：生体情報収集による超予防医療実現を目指して．H18年3月17日 NORTH Internet Symposium 2006

G．知的財産権の出願・登録状況
(予定を含む)

1．特許取得
なし。

2．実用新案取得
なし。

3．その他
なし。

厚生省科学研究費補助金(医療技術評価総合研究事業)
分担研究報告書

医療VPNとPKIを併用した安全な医療情報交換インフラの構築と運用に関する研究
― 三重遠隔画像診断ネットワークにおける構築と運用の方法

分担研究者　山本　晧二　三重大学医学部附属病院医療情報部教授

研究要旨
既存の三重遠隔画像診断ネットワークと医療VPNを接続し、電子メールサーバ及びWWWサーバを設置した。これにより、画像読影結果のレポート配信およびWWWホームページ・電子メールによる各医療機関・医師との情報共有を行うとともに、PKIによる暗号化メールと読影レポートへの電子署名付与による真正性確保の利用可能な環境を整えた。

A. 研究目的

三重遠隔画像診断ネットワークはインターネットを利用しないクローズドネットワークであるが、医療VPNとの接続により、UMINネットワークのサービスを利用可能にするとともに既存遠隔画像診断時の読影レポートの安全な送受信および読影レポートの真正性を確保を検証する。

B. 研究方法

三重遠隔画像診断ネットワークは三重県下病院11病院および医師個人宅12箇所を接続しているネットワークであり、CT、MRIなどの画像を大学病院あるいは医師個人宅へ配信することにより、画像読影を行いその読影レポートを各病院へ配信するネットワークシステムである。

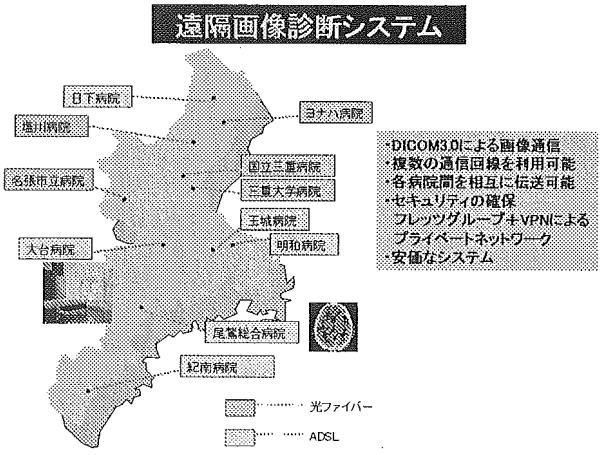

図1　三重遠隔画像診断ネットワーク関連病院

各病院の通信回線はインターネットではない、閉じたネットワークである地域IP網(フレッツグループ)を利用している。フレッツグループは安価なネットワークで、同一グループのみが通信可能でありセキュリティの確保をしやすいが、同一グループでは10箇所しか接続できない制約がある、しかし、三重遠隔画像診断ネットワークではVPNソフトウェアを使用し、三重大学内の読影室に複数のフレッツグループネットワークを集約し、ここに設置したVPNサーバによりフレッツグループネットワーク上に別のVPNネットワークを構築し、このVPNネットワークに参加する施設が相互にデータの送受信を行えるようにした。また、読影依頼については依頼病院からFAXまたはメールを利用することにしたが、依頼を受けるために、FAXサーバ及びメールサーバを設置している。また、転送した画像のレポート結果として、FAXまたはメールを使用した。

医療VPNとの接続には三重遠隔画像診断ネットワークを直接接続するのではなく、VPNソフトウェアを設定した端末をVPNゲートウェイとして稼動させ、必要なときに間接的に接続できるようにした。また、業務連絡や医療情報共有のため、

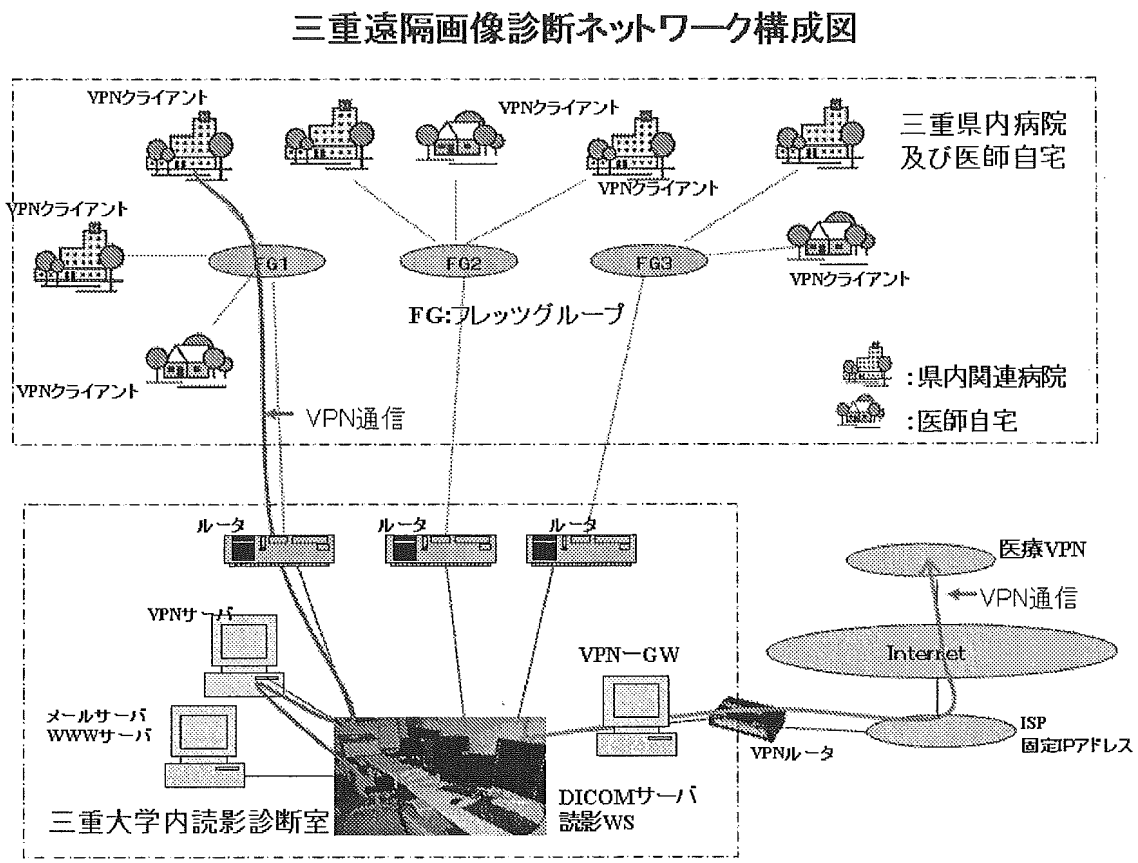

図2　三重遠隔画像診断ネットワーク構成図

WWWサーバおよび電子メールサーバを設置し、画像読影結果のレポート配信およびWWWホームページ・電子メールによる各医療機関・医師との情報共有および業務連絡を暗号化通信で行った。

C. 研究結果及び考察

三重県は南北に長く、地域病院での画像読影に実際に行く場合は、三重大学病院から南の紀南病院へは車で3時間以上かかるが、遠隔読影ネットワークを利用することにより、時間に拘束されることなく、空いた時間で行えるため、画像転送による遠隔画像診断は非常に有用であり、不足している放射線科専門医の有効時間を増やすことが可能となっている。三重遠隔画像診断ネットワークは専用のネットワークであり、画像転送だけに使用していたが、本年度行った医療VPNとの接続により、セキュリティを確保しつつ、UMINネットワークのデータベースや様々なネットワークサービスの利用が可能になった。このことにより、各地域の病院からも画像転送用のネットワーク回線からUMINの様々な情報を利用することが各病院の負担を増やすことなく可能になり、地域病院での情報活用に有効となった。また、今後の医療VPN内の暗号化電子メールおよびCAサーバを利用できることにより、読影結果のレポートについても暗号化したメールで配信することが可能となり、情報漏洩に対しても有効であるとともに、PKIによる本人認証およびレポート内容の電子署名を行うことにより、読影レポートを書いた医師が間違いなく本人であること、および内容が改ざんされていないことが各病院で確認でき、読影レポートの信頼性確保に有効であると期待している。

G. 知的財産権の出願・登録状況

なし

厚生省科学研究費補助金(医療技術評価総合研究事業)

分担研究報告書

医療VPNとPKIを併用した安全な医療情報交換インフラの構築と運用に関する研究
―やまぐち健康福祉ネットワークのおける構築と運用の方法

分担研究者　井上裕二　山口大学医学部附属病院医療情報部教授

研究要旨　山口県が提供する情報スーパーネットワーク(YSN)に山口県内のインターネットサービス事業者(ISP)が接続する地域IXを構成し、その上に仮想私設ネットワーク(VPN)を構築して安全の保障された医療ネットワークとした．県内の医療機関はこのVPNにより山口大学病院との医療情報交換が可能になり、さらには、大学病院医療情報ネットワーク(UMIN)と接続することにより、全国レベルの医療VPNと連携を実現した。地域医療ネット内に限定したメール機能は稼動しており、PKIとCA実装する準備は整った。

A．研究目的

地域の医療機関が診療情報の連携を実現しようとするとき、それぞれの医療機関を結ぶ広域の情報通信網を構築し、同時に、患者の情報保護に配慮した安心して利用できる情報環境が求められる．これまで、山口県が提供する情報スーパーネットワーク(YSN)および県内のインターネットサービス事業者(ISP)を利用してYSN上に地域IXを構成し、その上に仮想私設ネットワーク(VPN)を構築して安全の保障された医療ネットワークを構築してきた．本研究の目的は、この地域医療ネットをさらに発展させ、大学病院医療情報ネットワーク(UMIN)と接続することによって全国レベルの医療VPNを実現し、同時に地域医療ネット上でPKIとCAを実装することによって運用が容易で安全な医療情報交換基盤とすることにある。

B．研究方法

1．情報センター(NPOやまぐち健康福祉ネットワーク機構)の機能

遠隔医療と地域の医療連携を円滑に運用するために、これまで山口大学病院で管理運用してきたセンター機能をNPOやまぐち健康福祉ネットワーク機構に統合し、同時に、サーバーネットワークと機器全てを山口県の管理下に移管した。大学病院主導ですすめてきた地域連携を、山口県、医師会、保健センター、等の関連団体が協力する運用体制に移行するためである。

このセンターでは、遠隔医療の基盤についての広報と遠隔医療を希望する病院と病院、あるいは、診療科間の仲立ちをする。地域医療ネットを利用した医療サービス産業の参入を促し、医療連携をキャッシュフローをともなうビジネスとして配慮し、依頼先と依頼元の間の取り決めの仲介も行う。また、実運用の中で指摘される情報システムの不備および改善の要望を県当局と協議して具体的対応に結びつける、という役割を担っている。

2．地域遠隔医療ネットワークの構成

1)　幹線ネットワーク:医療圏の拠点間を結ぶネットワークで、山口県が敷設した光ケーブル通信網(やまぐち情報スーパーネットワーク:YSN)の利用を基本とした。

2)　接続回線ネットワーク:幹線ネットワークのアクセスポイントと医療機関の間を接続する回線で、NTTの地域IP網やATM専用線、また、やまぐち情報スーパーネットワーク(YSN)に接続する県内のインターネットサービス事業者を用いた．

3)　サーバーネットワーク:遠隔医療および地域医療連携を実現するための各種サーバ群を設置したネットワークであり、山口県の管理下にある情報センターに全てを再構築した．

3．医療ネットワークの安全保障(図1、2)

①　YSN地域IX:県内のインターネットサービス事業者がやまぐち情報スーパーネットワーク(YSN)に接続することにより、山口県の地域IXを構成し、その上に仮想私設ネットワーク(VPN)を論理ネットワークとして構築した．これに伴い、ケーブルインターネット網を利用する医療機関もPPTPにより接続可能になった。

②　NTTの地域IP網:BフレッツやADSLを利用する医療機関には、2セッションの選択が可能なルータ利用を支援することにより、地域医療ネットとインターネットの選択的な接続を可能にした。また、ISDN等によってISPを利用する場合はNTT系のMEON(ISP)が利用者認証により地域医療ネットの選択接続を可能にするサービスを提供した。

③　ATM専用線接続:県内の広域ネットワークにおいて複数の管理区域をまたがった仮想私設ネットワーク(VPN)を構築した。100キロメートル離れた市民病院放射線科と山口大学病院放射線部の間で画像診断をおこな