別添1

厚生労働科学研究研究費補助金
医療安全・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18年度　総括研究報告書

主任研究者　木内　貴弘

平成19(2007)年　4月

別添2

目　　次

別添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18年度は、各地域ネットワークの実情に合わせて、システムの導入と動作の検証を行った。公開鍵認証局については、参加研究者のサイトにWebベースで使えるCAを導入し、電子メール用公開鍵証明書の発行、廃止及び実際にメールをやり取りしての動作確認を行った。本年度の研究成果により、次年度の検証実験を実施するための体制が整った。

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

本年度は、主としてCA等のソフトウエア等を実際に各地域ネットワーク内のサーバ上に構築して、動作確認及び運用実験を行った。システム構築のための必要な資料について、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、構築・運用の状況・必要なソフトウエアやマニュアルの修正を行った。

C. 結果

C. 1 地域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システムの構築、運用形態、動作確認等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。一部機能利用時の若干の不安定性はみられたものの、すべての地域医療ネットワークで、概ね正常に稼動した。

(1)旭川医科大学遠隔医療センター
(分担研究者:廣川博之)

(2)三重遠隔画像診断ネットワーク
(分担研究者:山本晧二)

(3)やまぐち健康福祉ネットワーク
(分担研究者:井上裕二)

(4)周産期ネットワーク
(分担研究者:原　量宏)

(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)

(6)熊本大学医学部附属病院
(分担研究者:末永貴俊)

C.2 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。

平成18年度には、システム構築と動作確認がほぼ完了した。一部に不安定な部分もあり、今後も動作の検証と改良は継続するが、次年度の実証実験の実施に大きな支障とはならない程度のものと考えている。

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18年度は、上記の運用実験をするための、システムの各地域医療ネットワークにおける構築と動作検証等を行った。

F. 研究発表

(1)木内貴弘　情報システムの活用とセキュリティ　大橋靖雄、荒川義弘　臨床試験の進め方 南江堂　東京　2006　118-121

(2)Matsuba H, Kiuchi T, Tsutani K, Uchida E, Ohashi Y　The Japanese perspective on registries and a review of clinical trial process in Japan　Mary ann Foote　Clinical Trial Registries - Practical Guide for Sponsors and Researchers of Medicinal Products　Birkhäuser Verlag Basel　2006　83-106 (1)

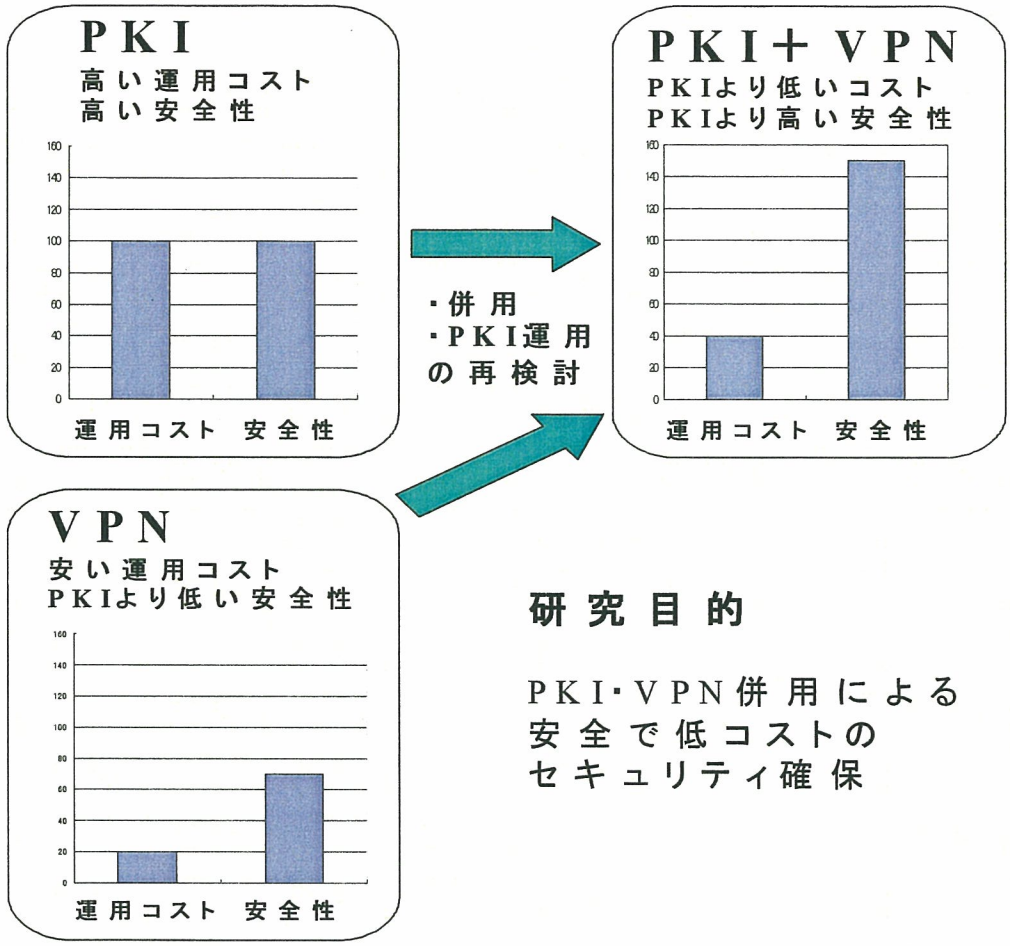


図. VPNとPKIの併用によるメリット

別添4　分担研究報告書

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）研究年度終了報告書

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CAの構築と運用

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　旭川医科大学病院遠隔医療センターに医療VPNとPKIを併用した安全な医療情報交換基盤の構築を行なう。OpenCAを用いてCA、RA、REPOSI- TORY機能を実装し、S/MIMEでの運用性評価を行なった。セキュアで広域な通信基盤が整備されることにより、当院が推進する遠隔医療サービスの形態にもコンテンツの幅が増すことが期待される。

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）に於ける医療VPN旭川医大サイト（以下、単にサイトという）に、PKI基盤を構築し、その運用性について考察する。

B　センターの提供サービスと情報インフラの概要

旭川医科大学では、附属病院に隣接され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][7]。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、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）」を継続して実践している。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8回、内科、整形外科、眼科、脳神経外科領域よりテーマが選定され、各回7～21ヶ所より参加があった[8][9][10][11]。

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もので、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×2回線）が用いられている。

2005年度には、センター設備機器のIP対応化が実行され、様々なメディアで蓄積されていた医療情報を統一的に扱うことが可能になっている。このことは、通信の相手側にとっても専用装置や専用回線を設備する必要がなく、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ことが期待できる。

そのほかセンターには、独立行政法人情報通信研究機構（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、シンガポールやタイとの間で、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2006年2月より実践されている[12][13]。

更に、安定した地上回線の確保が難しい地域への医療支援のために、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進めている[14]。

C　医療 VPN 旭川医大サイトのネットワーク構成

本研究のテストベッドには、2004年度来構築してきた医療VPN旭川医大サイト（ドメイン名：asahikawa-med.hvpn.net）を利用するため、そのネットワーク構成について概説する。

C.1　外部との通信に用いる回線サービス

インターネット接続にはBフレッツ（ベーシ

ックタイプ）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）により取得している。医療VPNサイト構築に必要な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。

尚、前述した放射線領域での遠隔画像診断サービスはこれとは別に、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している（図1）。

C.2　遠隔医療ネットワークの構成

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ながら各々若干の説明を加える。

[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、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セグメント（VLAN#B）上には、医療VPNサイトの運営に不可欠なサーバ機能として、DNSサーバ、MAILサーバ、SYSLOGサーバ、NTPサーバ、コンテンツ公開のためにWWWサーバ、Database（DB）サーバ機能が実装済みであり、今回構築を目的とするPKI基盤もこのセグメントを利用する。

医療VPNセグメントに配置された装置に対しては、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（VLAN#D）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　研究方法

安全な医療情報交換を行うためのPKI基盤をVPN旭川医大サイトに構築する。認証局（Certification Authority；CA）サーバ及びセキュアなメールサーバを実装することにより、各利用者に電子証明書（以下、証明書）を配布し、暗号化メールの交換が可能となる。

E　研究結果

E.1　ソフトウエア実装

今回はPKI信用モデルを「単独CAモデル」として構築した。CA構築に用いた主なソフトウエアの名称とヴァージョン情報を列挙する。

主なソフトウエアの名称、版数

Miracle Linux	4.0
(kernel	2.6.9)
OpenCA	0.9.2.5
PostgreSQL	8.0.3
OpenSSL	0.9.7a
Apache	2.0.52
Sendmail	8.13.1
Dovecot	0.99.11
Perl	5.8.5

セキュアメールサーバにはF-Secure Linuxサーバセキュリティ（日本エフ・セキュア株式会社）をインストールし、ウイルスやワームからサーバをリアルタイムに保護している。

又、サイト内での情報共有の用途にグループ

ウエアソフトウエアAIPO3（株式会社エイムラック）を導入した。

E.2　CAの運用手順

証明書の発行プロセスでは、ユーザ（証明書の被発行者）が鍵ペアを作成した上で登録局（Registration Authority；RA）に申請する方式（ユーザ鍵生成モデル）のではなく、RAが鍵ペアを一括して生成する方式（センター一括鍵生成モデル）を採っている[15]。

以下、構築したCAサイトにおける証明書の申請及び失効に際しての一連の運用手順を示すが、これらは全てWEBブラウザ（HTTPS通信）上の操作により処理が進行する（但し、実際の操作上ではRA、CA、リポジトリ（Repository）の明確な区別は付きにくい）。

E.2.1 証明書発行手順

(A1) ユーザは氏名、メールアドレス、PINコードを入力して証明書申請を行なう。

(A2) (A1)の申請を受け付けたRAでは、本人性の確認を行なった上で鍵ペア（秘密鍵と公開鍵）を生成し、CAに対して証明書発行を要求する。

(A3) CAは公開鍵に署名を施し、証明書の発行処理を行なう。この証明書は、PKIユーザが利用できるようにRepositoryにて公開される。

(A4) RAは証明書の配布を申請ユーザに宛ててメールで通知する（図4）。

(A5) (A4)のメールを受信したユーザは、証明書とキーペア（PKCS#12ファイル）を自らダウンロードする。この際に、申請時に指定したPINコードが要求される。

(A6) PKIユーザ（証明書利用者）は証明書をRepository上の証明書一覧より随時ダウンロードして利用する。

E.2.2 証明書失効手順

(B1) ユーザは氏名、メールアドレス、PINコードを入力して証明書申請を行なう。この時、(A4)で受信したメール内に書かれた証明書破棄用のPINコードが要求される。

(B2) (B1)の申請を受け付けたRAでは、CAに対して証明書の失効を要求する。

(B3) CAは、失効処理を行ない、CRL（Certificate Revocation List）を発行する。PKIユーザが利用できるようにリポジトリにて公開される。

(B4) PKIユーザ（証明書利用者）はCRL情報をRepositoryより随時ダウンロードして利用する。

E.3　S/MIMEでの試運用

PKIアプリケーションとして最も利用が期待されるS/MIMEを利用した暗号メールの運用を通じて、CA機能の動作検証を行なった。

今回はメールクライアント（MUA）にOutlook系（Expressを含む）を用いて検証を行なった。作成したメールに対し、署名、暗号化操作を行なう（図5）。この時、送信先ユーザの証明書（公開鍵）を事前に準備しておく必要がある。この時、送信された暗号メールのMIMEヘッダ部が、application/x-pkcs7-mime、smime-type =enveloped-dataであることを確認した（図7）。

受信者側では、秘密鍵をインストールしてあった場合にはメールを正しく復号することができる（図8,図9）が、未所持の場合には復号することができない（図10）。

E.4　性能評価

運用性に対する評価の一環として、メールを平文で作成した場合と暗号化した場合との処理待ち時間を比較計測した。併せて、メールの復号に要する時間も計測した。

暗号化に要する時間は、メールクライアントソフトウエア（Mail User Agent；MUA）で署名、暗号化したメールを作成（図5）し、送信ボタンを押下してから送信トレイに格納される（図6）迄と定義した。一方の復号化に要する時間とは、暗号メールの復号を指示（図8）してから復号結果が表れる（図9）迄とした。

サイズの異なる8種のファイルを用意し、各々を添付した単名宛てのメールを生成しながらこれら時間を計測した。尚、測定では次の仕様のPCを用いた。

性能評価に用いたPC
Pentium Ⅲ/1.0GHz、メモリ256MB、
Windows 2000 Professional、
Outlook Express 5.5

結果を図11に示す。メールに添付するファイルサイズ：X（kB）と、暗号化、復号化に要するオーダヘッド時間：Y（s）は、各々次の関係式で示される結果であった。

暗号過程 → Y = 0.0013・X
復号過程 → Y = 0.0008・X

F　考察

構築システムの試運用を通じた評価結果とそれを踏まえた今後の展開について考察する。

F.1　RAの運用ポリシー

利用者から証明書発行申請を受けて、RAがど

のように本人確認を行なうか？ CAサイトの運用ポリシーを決定する必要がある。本人が直接窓口に出向く方法が確認レベルとしては最も高いが凡そ現実的ではない。

本運用に先立ち、想定されるPKIアプリケーションやユーザ規模を勘案しながら、無理ない現実的な運用ポリシーを見定めることが重要である。

F.2 CRL情報の適時通知

CRL情報をクライアントに定期的に反映させるためにはどうするか？ 例えば、宛先ユーザの証明書の失効・更新に気づかずに暗号メールを送信した場合には、そのメールを復号できない事態を招くことが起こり得る（尤もこの例では実害に至ることは少ないと考えられるが）。

証明書の失効情報の通知方式には二方式、CRLモデルとOCSP（Online certificate Status Protocol）モデルとがある[15]。CRLモデルがCRL情報をRepositoryから定期的にダウンロード処理する必要があるのに対し、OCSPモデルは失効情報をリアルタイムに照会する。後者モデルは証券、金融、株取引等のリアルタイム性の要求されるシステムに使われているが、常時オンライン接続されている必要がある。

医療系システムではCRLモデルの方が適していると考えられるが、利用者が主体的にCRL情報をダウンロードしてもらうことが必要である。そこで、短周期で確実に参照すると考えられるグループウエアページを利用してCRL更新を案内していくことを計画中である。

F.3 他のPKI運用方式との比較

当院の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（Pentio PKI PrivateCA）を運用している。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を構築している。

秘密鍵と電子証明書はPKI-USBトークンに格納されており、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はアクセス出来ない。

このPKIトークン方式は、トークン自体から秘密鍵を読み出せないために秘密鍵が漏洩する危険が小さいこと、秘密鍵の持ち運びが可能なため可用性が高く、PC内部に証明書（秘密鍵）が残らない点で安全性が高い。

今回構築したPKI基盤とはそのユースケースを全く異にするが、システム管理者のみが利用するような場面においてこのPKI運用方式は有利である。

F.4 暗号メールでの応答性

メールの暗号化処理が遅くストレスでないか？ 測定結果からは、メールサイズが3MB程度の場合、暗号化処理に約4秒の余分な時間がかかる。

この時間は、遠隔医療を想定した場合には、実用上も問題になることはないと思われる。例えば、放射線や病理領域での画像診断ではセキュリティを含めて専用システムとして構築されていて、大容量データを効率的に伝送できる機能を備えている。電子メールに添付して医療画像を伝送する情報交換方法は極めて汎用性が高いが、それが画像伝送における定型的な業務スタイルにはなりにくいと考えられる。

F.5 システムの安定性

構築したCA環境はライセンス料金が不要なパブリックドメインソフトウエアを組み合わせて実装している。試運用中には、ログアウト操作後に証明書発行サイトにアクセス出来なくなった、証明書失効リストが参照出来ない、失効手続きをした直後に新規登録が出来なくなった、等の不具合を経験した。

運用モデルとしては高信頼性が絶対的な必要要件であり、自作システムだからという言い訳は通用しない。今後試運用評価を通して、安定性を十分に確保していくことが肝要である。

G 結論

旭川医科大学病院遠隔医療センターに於ける医療VPNネットワークの上にPKI基盤を構築し、S/MIMEでの運用性評価を行なった。

システム運用面での課題点は幾つかあるものの、セキュアで広域な通信基盤が整備されたことにより当院が推進する遠隔医療サービスの形態にもコンテンツの幅が増すことが期待される。

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] 吉田晃敏，廣川博之，山上浩志，林弘樹，高橋康二，峯田昌之，三代川斉之，佐々木春光，上田淳大，近藤照仁：旭川医科大学が推進している遠隔医療（1）ー過去・現在ー．日本遠隔医療学会雑誌，Vol.1(1)：96-97，2005．

[8] 「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．

[9] 「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．

[10] 「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．

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

[12] 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．

[13] 吉田晃敏，笹沼宏，鈴木康之，花房廣安，高橋淳一，高橋淳士，籠川浩幸，加藤祐司，石子智士，佐々木春光：アジア・ブロードバンドネットワークを活用した眼科遠隔医療．日本遠隔医療学会雑誌，Vol.2(2)：160-161，2006．

[14] 吉田晃敏，伊達貴彦，佐々木春光，山口亨，高野了滋，石子智士，加藤祐司，籠川浩幸，亀山大希，山上浩志，廣川博之：衛星インターネットを用いた過疎地・離島遠隔医療．日本遠隔医療学会雑誌，Vol.2(2)：162-163，2006．

[15] 独立行政法人情報処理推進機構セキュリティセンター．PKI 関連技術解説．http://www.ipa.go.jp/security/pki/．

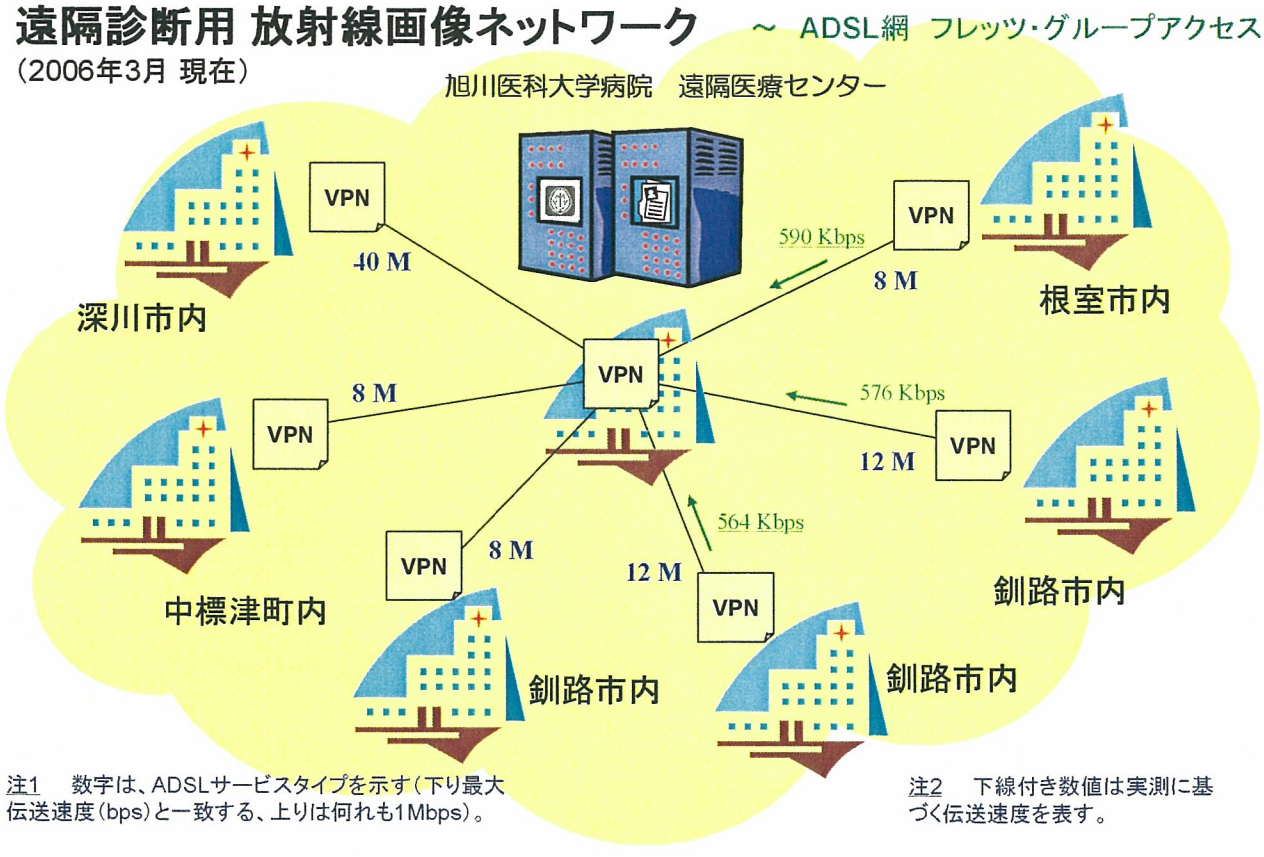


図1 遠隔医療ネットワーク(放射線画像の遠隔診断用途)

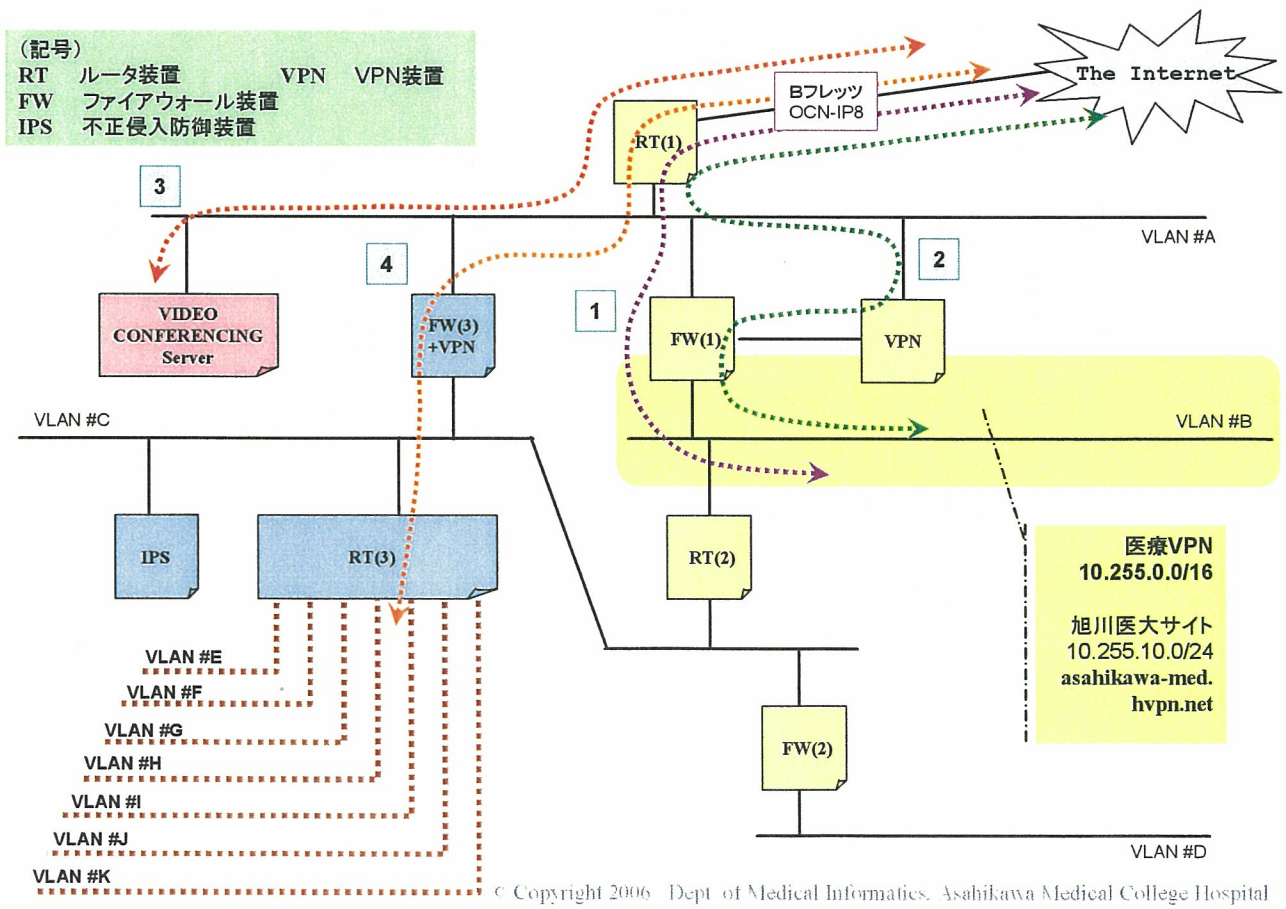


図2 遠隔医療ネットワーク全体構成図

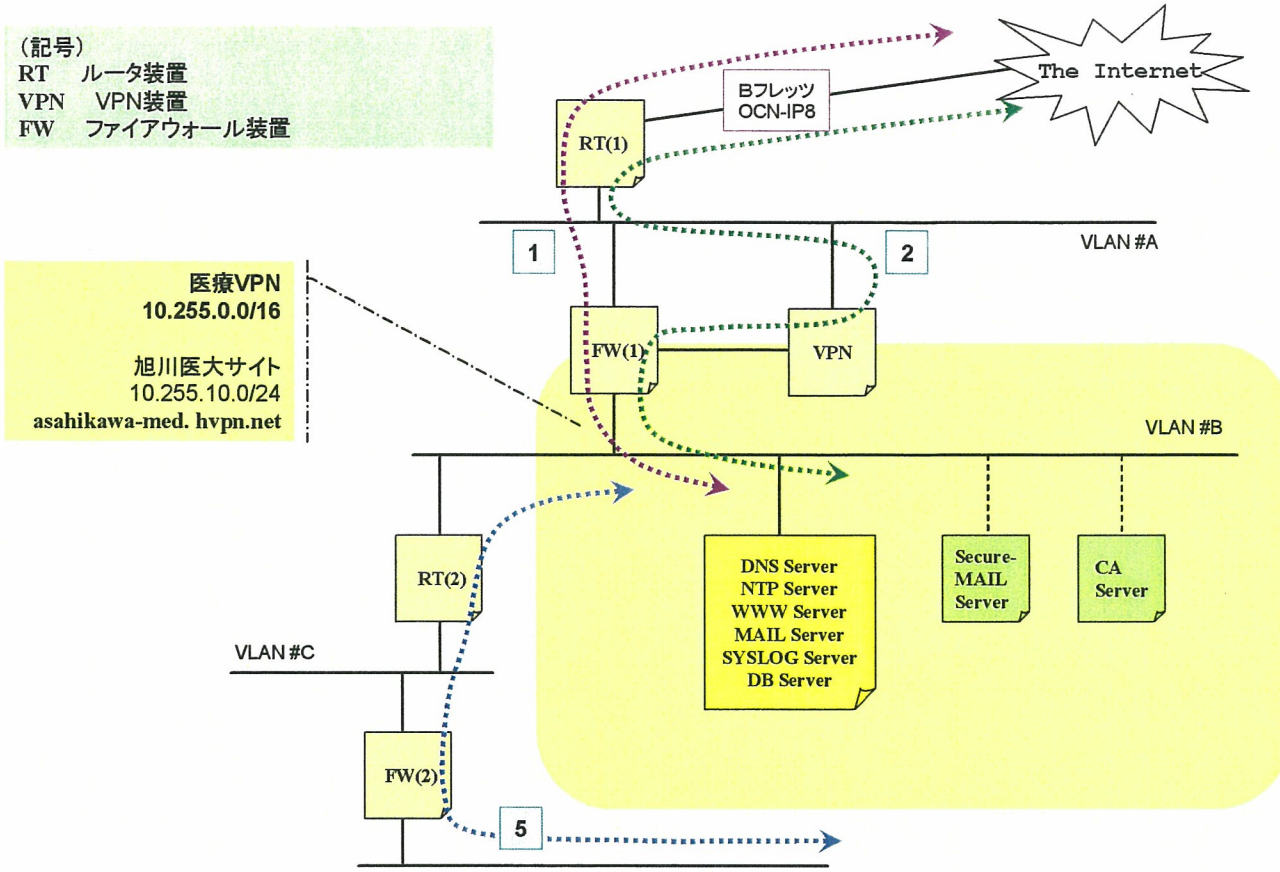
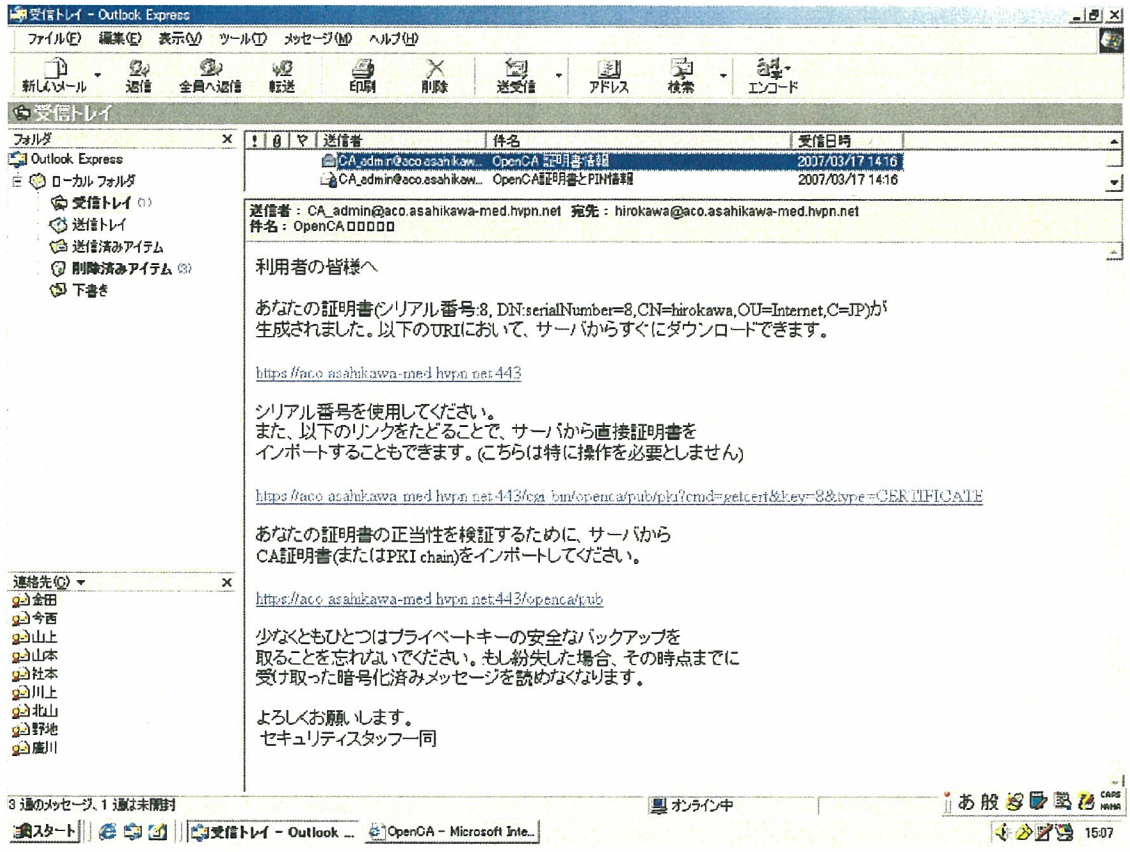


図3　医療VPN旭川医大サイト構成図

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 Networks
FW (2)	Pix-515	Cisco
RT (2)	Cisco-2651	Cisco
SERVER	Power Mac G5 / Mac OS X server 10.3.3	Apple
FW (3)	Netscreen-50	Netscreen
RT (3)	Catalyst 4507R	Cisco
IPS	Proventia G100	ISS
CA Server	ML110 G3 P3GHzX1 / MIRACLE LINUX V4.0	HP
Secure-Mail Server	ML110 G3 P3GHzX1 / MIRACLE LINUX V4.0	HP



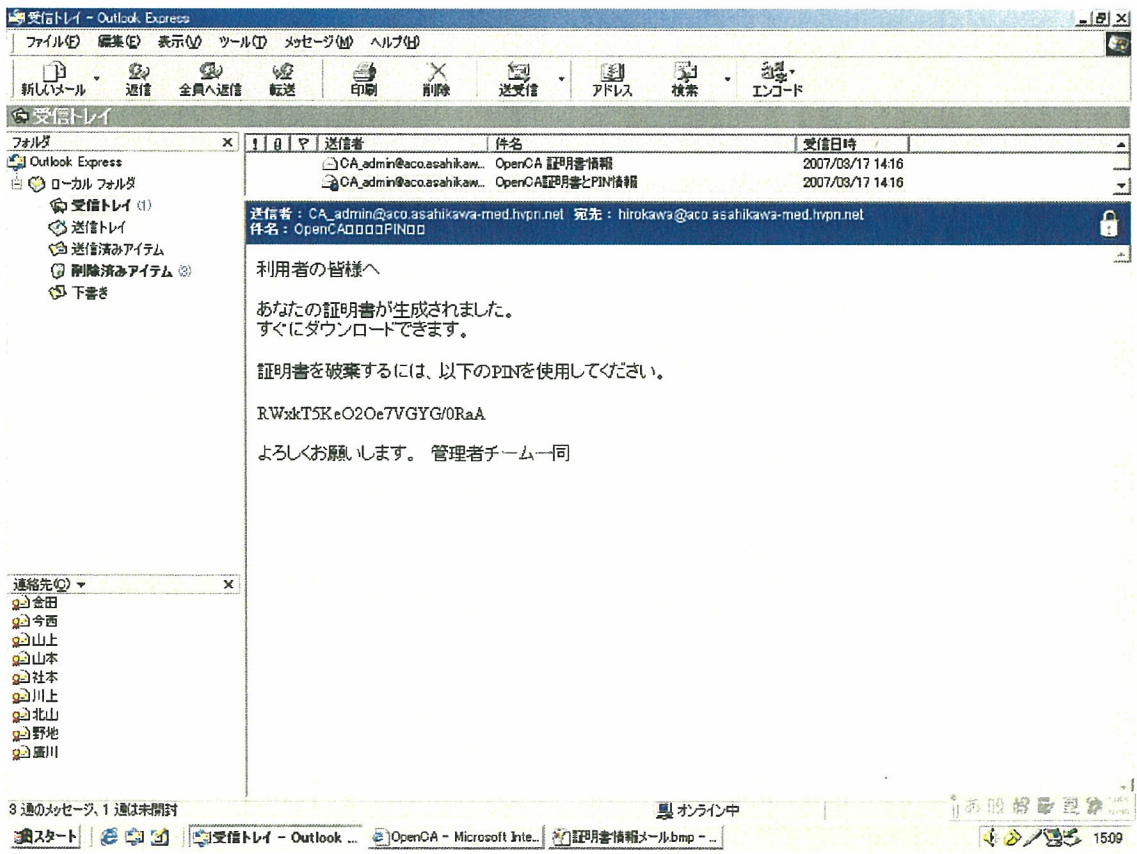


図4 証明書発行時に送付されてくるメール （二通）

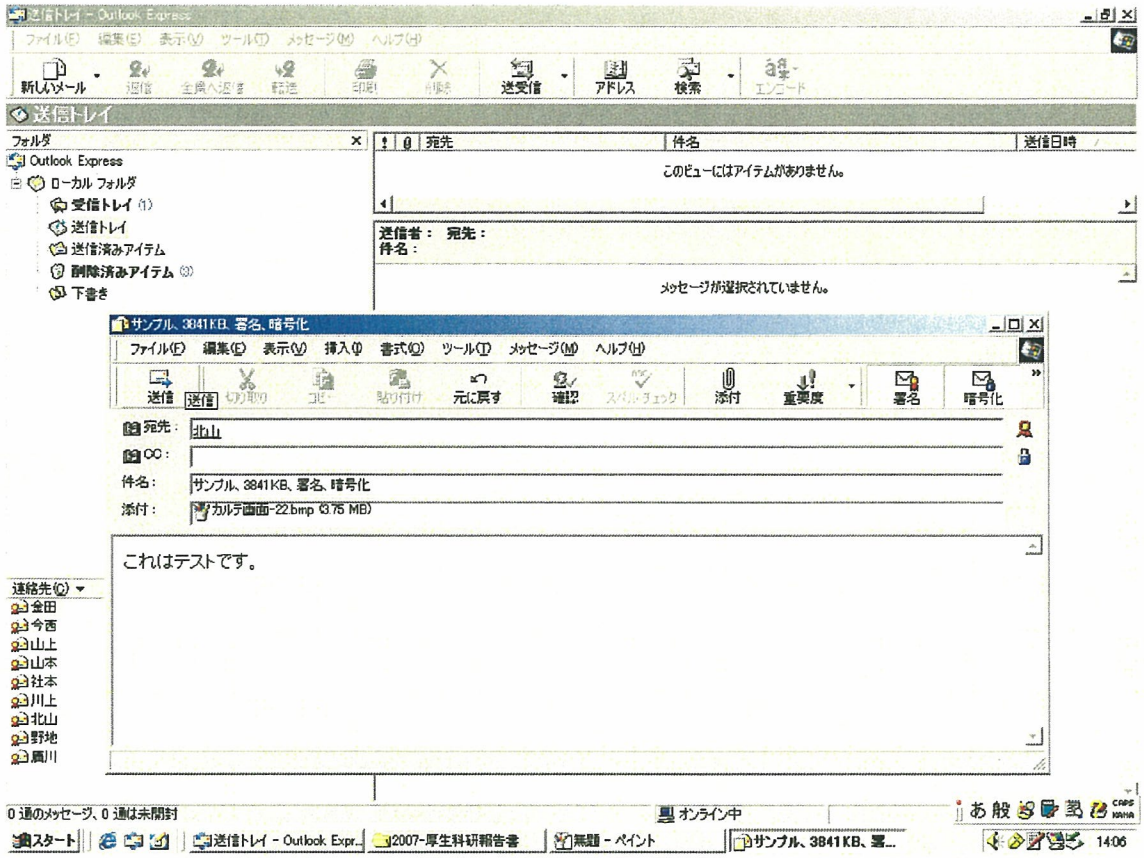


図5　MUA画面(送信側；1)　暗号化メールを作成した状態

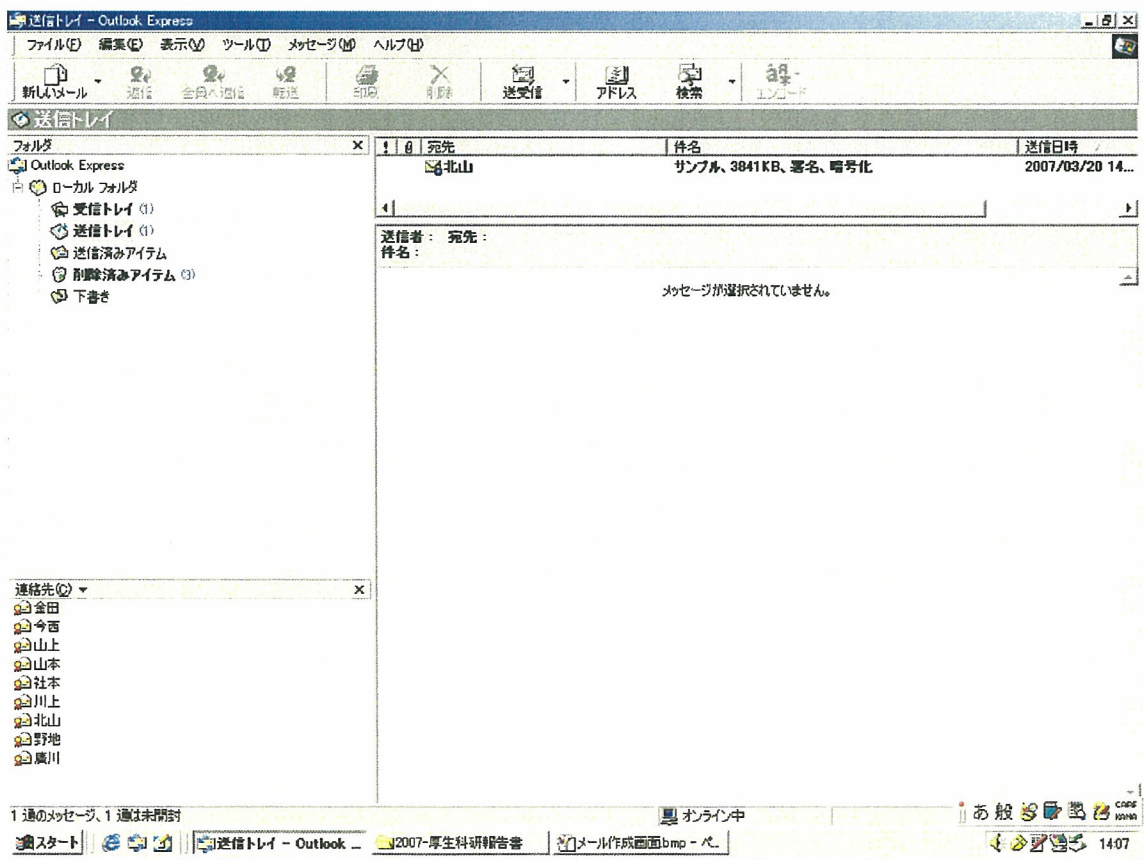


図6　MUA画面(送信側；1)　図4で「送信」ボタンを押した後に、送信トレイにおかれた状態

（ 途中省略 ）

図7 暗号化メール　メールサーバ上のmailboxを表示したところ

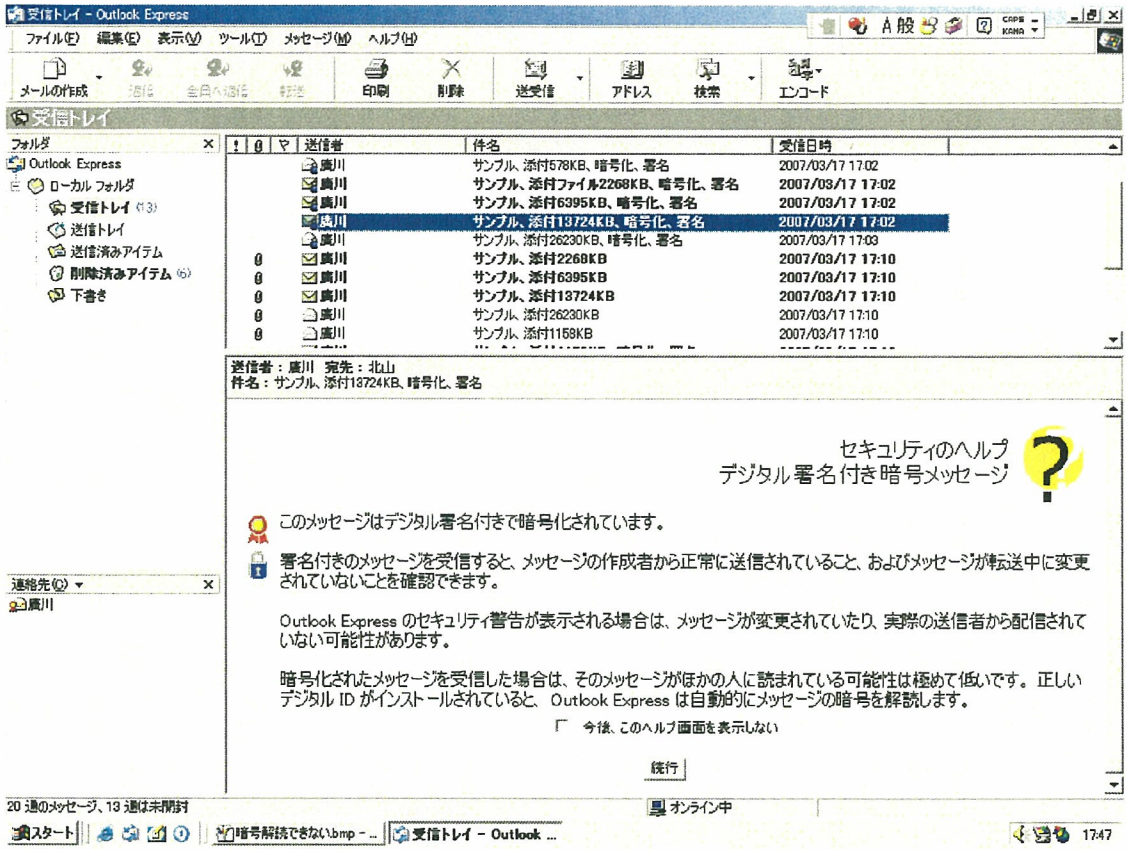


図8　MUA画面(受信側；1)　暗号メールを受信した状態

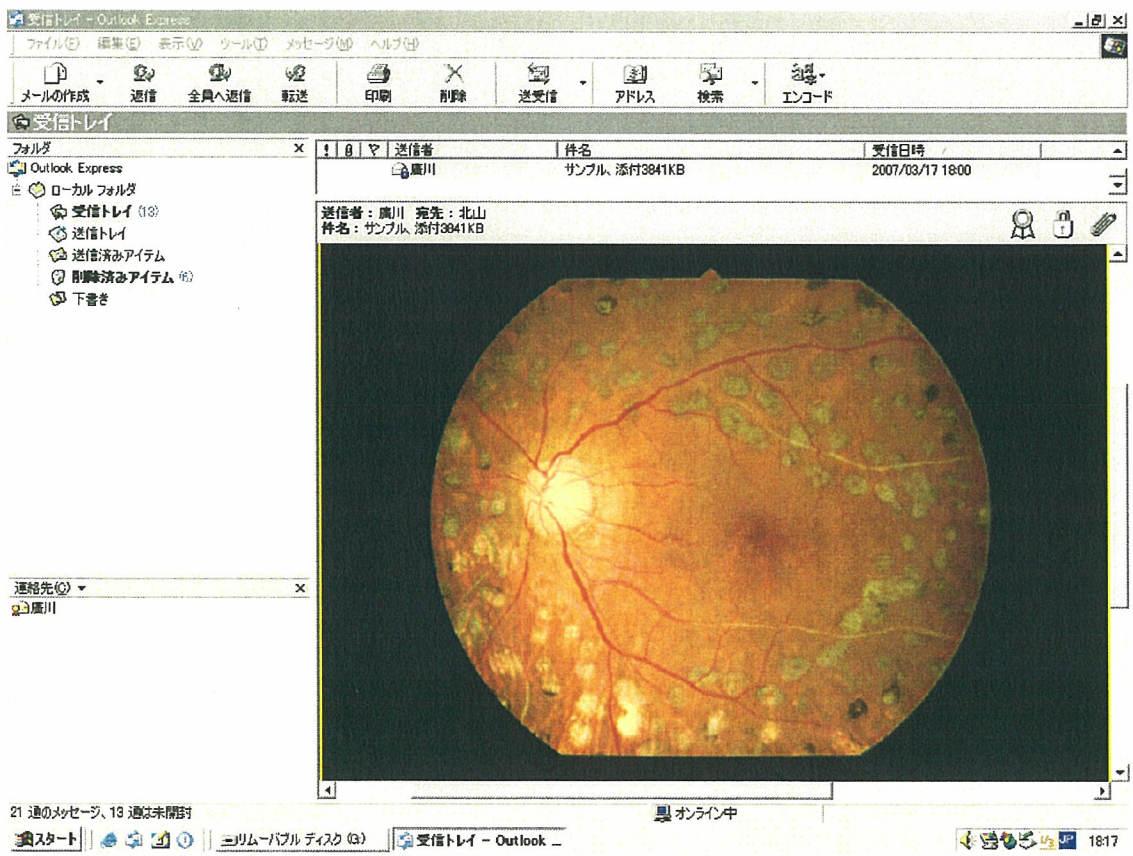


図9　MUA画面（受信側；2）　図9でボタン「続行」を押下して、メールに添付されていた画像を復号したところ

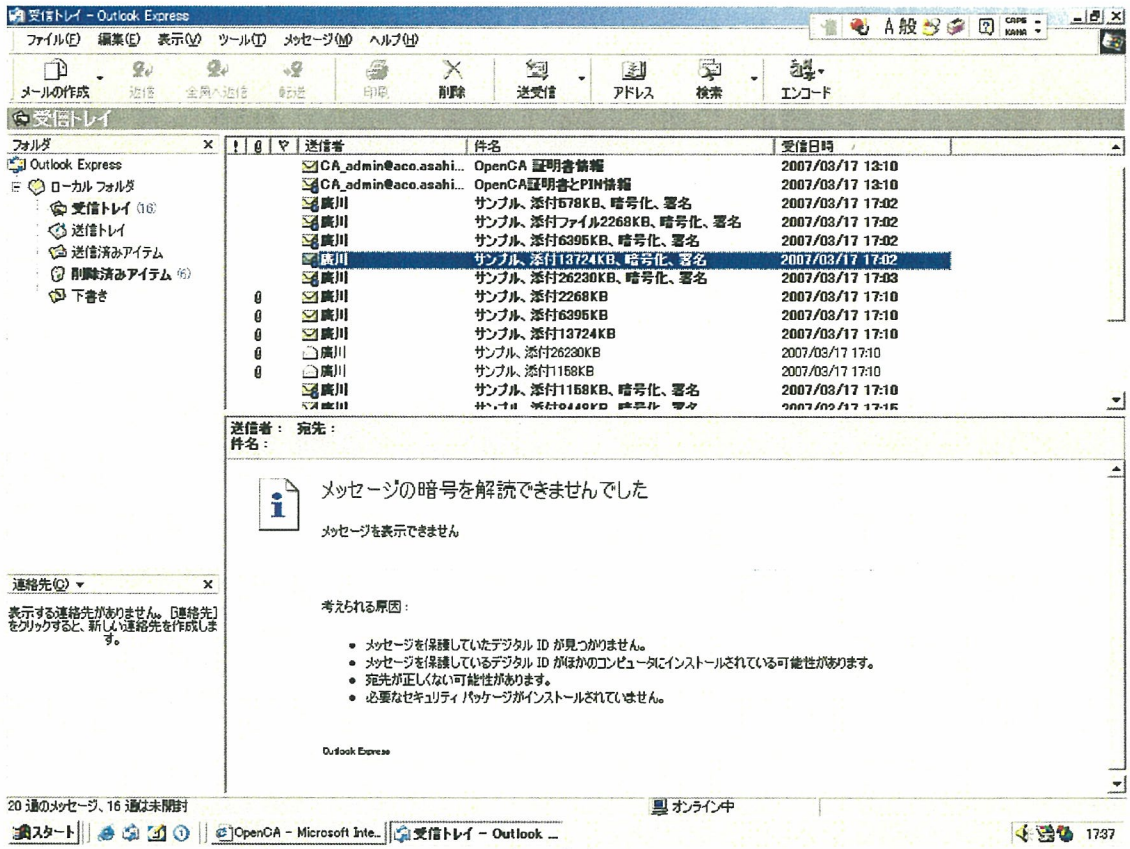


図10　MUA画面（受信側；3）　受信者が秘密鍵を持たない（インストールしていない）場合

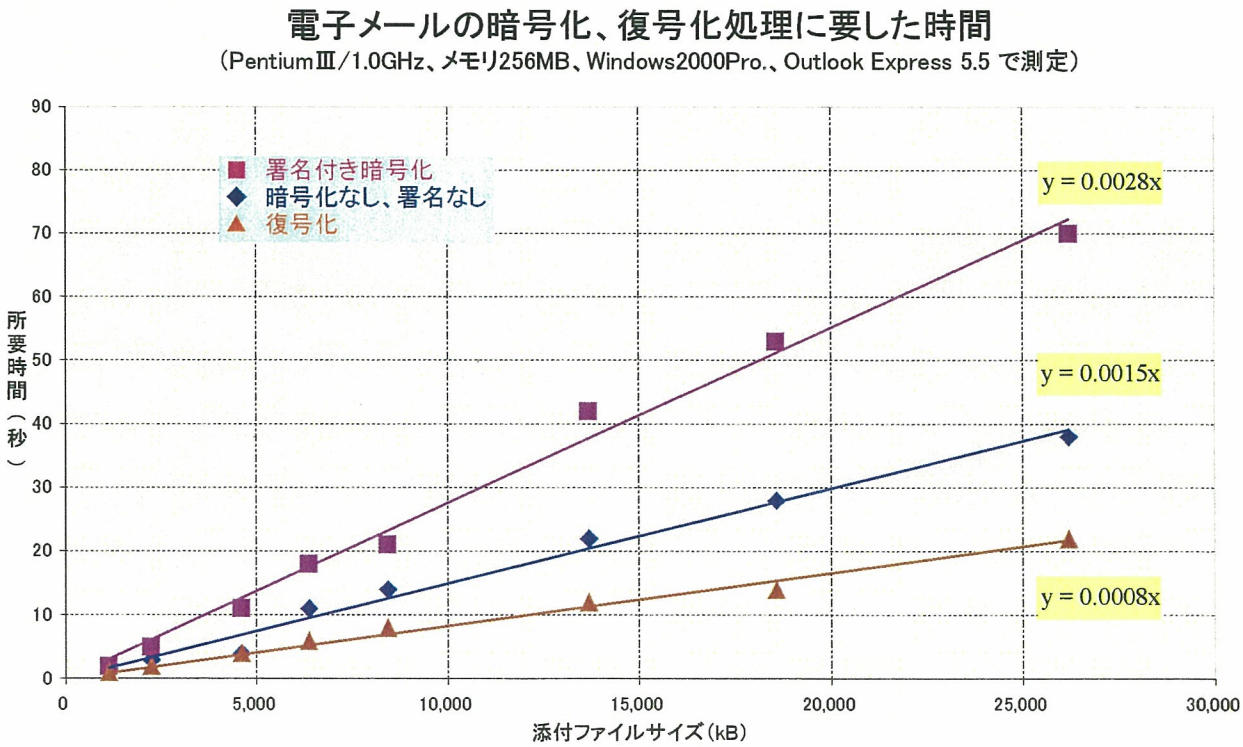


図11　電子メールの暗号化、復号化に要する時間

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

分担研究者　辰巳　治之　札幌医科大学大学院医学研究科　生体情報形態学教授
研究協力者
新見隆彦　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　札幌医科大学附属総合情報センター　講師
戸倉　一　札幌医科大学附属総合情報センター　訪問研究員
西城一翼　札幌医科大学附属総合情報センター　研究生
山口徳蔵　札幌医科大学附属総合情報センター　研究生

研究要旨　安全な医療情報交換のインフラ構築の為には、セキュリティや認証システムが重要になってくる。そこで、この研究班では医療ＶＰＮの構築とCAなどをつかったPKIの運用に関する研究をする一方で、我々は分担研究として新たなる解決方法について検討を行った。医療系における情報化を推し進めるためには、安価な費用にて実現でき、運用が簡便であることが重要である。そこで将来の発展性をも勘案し、IPv6のグローバルアドレスを使った実証実験を行った。

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の確立が必要である。専用回線による医療ネットワークの実現は、費用の点で実現的ではない。そこで医療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、医療情報ネットワークの具体的な利用シーンを念頭に置き、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。まず、VPNにおける安全性を確保し、且つ、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、通信運用実験を行う。

C　研究結果

ブロードバンド世界一となった日本において、広域性及び経費の点においてインターネットは無視できず、また、医療情報ネットワーク実現の為には、それを安全に使えることが必須となってくる。そこでＶＰＮ(Virtual Global Ne

twork)の利用が推進されるべきと考える。しかし、まったく問題が無いわけではない。この名前の通り、Private Networkということは、どこかに管理組織がないと、同じアドレスを使ってしまう可能性がある。また、関連病院だけのネットワークで、相互接続性がないとインターネットの真価が発揮されない。急患の患者の情報を得るために、連携していない医療施設との接続も必要になる。そこで、我々は、Global Addressでセキュアーネットワークを実現するＶＧＮ(Virtual Global Network)を開発し、医療系ネットワークへの応用実験を行った。

VGNとは（図1）、IPv4の従来のインターネットの上に、Point To Pointで、トンネルを掘り、Layer 2にて通信ができるシステムである。このトンネルの中をTopological Addressing Policyに従ってIPv6のグローバルのアドレスを配布するものである。今までは、Ｐ２Ｐによるネットワーク構築であったが、今回はP2Nの構築を行った。即ち、VGNのサーバーに対して複数のトンネルを掘れるようにした。また、認証に関してはVGN Box同士で行い、複雑な操作なく、接続すれば即、VGNが設定される仕組みになっている。

これでは、IPv6の環境がない施設でも、IPv6が利用できるようになっている。IPv4のネットワークも従来通り使えるが、IPv6では、その通路はセキュリティを確保した形で通信が可能となる。

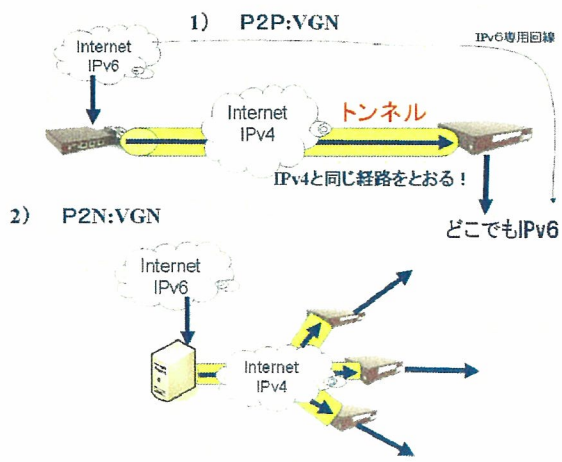


図1．VGNの実現（P2PとP2N）

このシステムの将来利用として、図2.に示すように、専用回線で実現していた医療ネットワークを、このＶＧＮで、インターネットを使って実現することができる。今後、２０１１年までにオンラインでレセプト収集するという計画がされているなか、このような安全なネットワークの形成が必要とされ、その実現によって医療機関同士のネットワーク形成も可能になる。

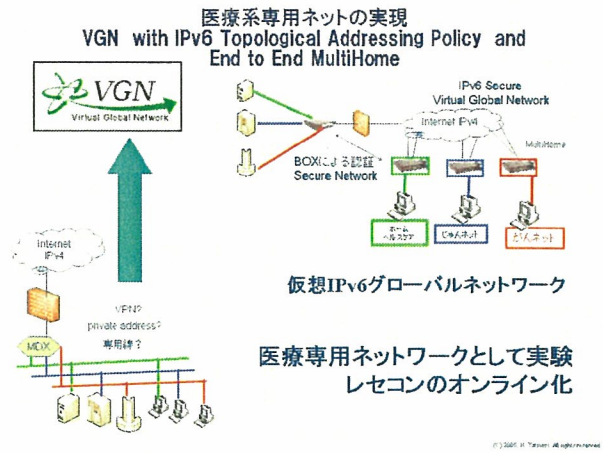


図2．VGNによる医療専用ネットの実現

D　考察

いろいろな具体的な利用シーンにおいて種々の問題が生じた。 このVGN Boxは、煩雑な操作なく接続できることが利点ではあるが、モバイル用に利用できるようにこのＶＧＮ boxを小さくしたところ、大容量通信を必要とするDVTSでは、暗号化などＣＰＵに負荷がかかり過ぎ、実用に耐えなかった。これは地域医療支援などに行くときを想定しモバイルを重視したためで、施設に設置する場合は通常のＰＣレベルの性能で問題はない。今後、種々の負荷テストや小型BOXのＣＰＵの性能向上などを検討する必要がある。

いろいろな現場での利用を実験したところ、アドレスを取得するために認証がかかるような場合は、Interactiveなインターフェースが無いために接続できないことがあった。また、最近では無線のホットスポットがポピュラーになってきているが、今のシステムでは無線や携帯電話のデータ通信カードにも対応できていない