200732021A

別添１

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

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１９年度　総括・分担研究報告書

主任研究者　木内貴弘

平成２０（２００８）年４月

別添２

目　次

別添３

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(UMIN)研究センター教授

研究要旨　過去の２年間に構築した医療VPNとPKIを併用した安全な医療情報交換基盤を用いて、各地域ネットワークにおいて、各種の医療情報交換の運用実験を実施した。一部に運用の安定性の問題が見られたものの、暗号化によるオーバヘッドも少なく、各種の医療情報交換に活用可能なことが立証された。また地域での実践利用に際して、利用者の立場からの更なる利用法の簡略化・わかりやすさを目指して、簡略化されたユーザインターフェイスの追加、Webメールでの利用等の工夫が見られたことは注目される。今後は、本研究の実用化に向けて、更に詳細な運用方針を詰めていくことが必要であると考えられた。

Ａ　研究目的

本年度の研究目的は、平成１７年度、１８年度にかけて、UMIN及び各地域ネットワーク等で構築した医療VPNとPKIのインフラを活用して、各種の医療情報交換の実証実験を行い、その実用性と課題を検討することにある。

Ｂ　研究方法

北岡、辰巳分担研究者以外は、各分担研究者の運用する地域ネットワーク等において、過去の２年間に構築した医療VPNとPKIを併用した安全な医療情報交換基盤を用いて、各種の医療情報交換の運用実験を実施した。具体的な交換する情報の内容、運用方法等について、各分担研究者に依頼して、各地域ネットワーク等の実情や必要性に応じた形態で実施した。

辰巳分担研究者は、将来のIP v6の導入を視野に入れた医療VPNの運用形態等についての調査研究を実施し、今後の将来像についての提言を行った。

木内主任研究者と北岡分担研究者は、国立大学病院VPN(UMIN VPN)と国立病院専用閉域ネットワーク(HospNet)の相互接続方法について、技術的検討を実施した。

Ｃ　研究結果

UMIN VPNとHospNetの相互接続法ついては、その結果を本総括研究報告書に記述した。その他の研究については、詳細は、分担研究者にまとめられているので、総括研究報告書では、各分担研究報告書の内容の概略について記述することにした。

C-1 UMIN VPNとHospNetの相互接続

相互通信はSMTPを用いた電子メールの交換のみを実施する方針とした。この方法によれば、データの中継が非常に容易であり、簡単なメールサーバ、ネットワーク機器の設定変更のみで実施可能である。本年度中に具体的な機器の接続作業を実施する予定であったが、国立病院機構による最終承認・確認が遅れたため、実際の接続にはいたっていない。

C-2　旭川医科大学遠隔医療センターにおける運用実験

旭川医科大学では、過疎地域の多い北海道の所在していることから、遠隔医療が盛んに実施されている。今回は、本研究で構築した医療VPNとCAを活用して、電子メールによる遠隔医療情報交換実験が実施された。電子メールは汎用性が高く、その利便性は大きいが、一方でデータの量の医療画像の送受信には使いづらい現状が明らかになった。

C-3　三重遠隔画像診断ネットワークにおける運用実験

三重遠隔画像診断ネットワークでは、画像診断読影の通知に電子メールを利用している。本研究で構築した医療VPNとCAを活用して、画像診断読影通知の暗号化・真正性の証明に実証実験を行い、実用性を確認した。

C-4　かがわ遠隔医療ネットワーク、周産期電子カルテネットワークプにおける運用実験

かがわ遠隔医療ネットワーク、周産期電子カルテネットワークにおける各種の電子メール通知について、実用性の確認が行われた。

C-5　山口県医療情報ネットワークにおける運用実験

山口県医療情報ネットワークは、専用線、VPN等によって構築された山口県域での医療機関等の間の閉域網である。本ネットワークでの活用にあたり、CAのユーザインターフェイスをより簡便にするためにツールの開発が行われ、同ネットワークの参加者がより一層容易に電子メール用の秘密鍵・公開鍵を得られる工夫がなされ、その実用性が実証された。

C-6　糖尿病疾病管理研究事業カルナにおける運用実験

カルナでは、医療VPNとの接続の他、電話回線による開業医からの接続を受け付けている。カルナプロジェクト内で、汎用の診療情報交換目的で、CAの運用・情報交換実験が行われ、その実用性が立証された。

C-7　熊本大学医学部附属病院における運用実験

本研究で構築した医療VPNとCAを活用して、Webメールによる各種医療情報交換の実験が行われた。Webメールによる利用に限定することによって、利用者は秘密鍵・公開鍵証

明書等の発行を意識することなく、安全な通信が可能となった。

C-8　IPv6技術を活用した医療VPNについての検討

アドレス空間の広いIP v6の場合には、本研究の医療VPNのようにプライベート領域の一部を割り当てる運用ではなく、医療VPN専用のアドレスを予約してしまうことが可能であり、IP v6普及時の医療VPNの運用形態として、医療VPN専用の領域の確保を提案した。

D　考察

D-1 UMIN VPNとHospNet相互接続について

UMIN VPNとHospNetは、運用主体を異にしており、お互いのセキュリティが低下しないように考慮する必要がある。特にHospNetは、規模の小さい参加病院も多いため、セキュリティ保護の基準はより厳しい。しかしながら、HospNetでは、インターネット電子メールを現状でも受け入れており、UMIN VPNから電子メールを受け入れてもセキュリティ低下は見られない。その一方で、メールのやり取りさえできれば、大きなデータ場合のデータ分割の必要性やデータ送受信のリアルタイム性の欠如という問題はあるものの、どのようなデータでも送受信可能であり、応用範囲は非常に広い。

D-2　地域医療ネットワーク等での運用実験について

一部に運用の安定性の問題が見られたものの、暗号化によるオーバヘッドも少なく、各種の医療情報交換に活用可能なことが立証された。今後、更に詳細な運用指針の策定を実施することよって、本研究の成果を実際の医療情報交換に活用することが臨まれる。

本研究で構築した医療VPNとCAに加えて、CAへの簡易なインターフェイスの追加による秘密鍵・公開鍵証明書発行の簡略化（山口県医療情報ネットワーク）、Webメール専用で運用することによる利用簡便化（熊本大学附属病院）等の工夫が見られたことは本年度の研究成果として大きな意義を持っていると思われる。いずれも利用者にとっても簡便化・わかりやすさの方向で工夫が行われたことは興味深い。

D-3　IPv6技術を活用した将来の医療VPNについて

IP v6技術については普及が遅れているが、インタネットアドレスが枯渇する中でアドレス空間の大きい、IP v6への移行が今後必要になる。医療VPNの研究を進めるにあたっても、IP v6への展開を常に視野に入れて進めていくことが重要と考えられた。

F　結論

各地域ネットワーク等において、医療VPNとPKIを併用した安全な医療情報交換基盤の実用性をいくつかの複数の用途で実証した。地域での実践利用に際して、利用者の立場からの更なる利用法の簡略化・わかりやすさを目指して、簡略化されたユーザインターフェイスの追加、Webメ

ールでの利用等の工夫が見られたことは注目される。今後、更に詳細な運用指針の策定を実施することよって、本研究の成果をHospNetも含めた実際の医療情報交換に活用することが望まれる。

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

旭川医科大学遠隔医療センターにおける運用実験

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おいて、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った。OpenCAによるCA、RA、REPOSITORY機能を実装し、S/MIMEアプリケーションによる動作検証を行った。構築システムの運用性を評価すると共に他のPKI方式との運用性の比較、北海道における遠隔医療の需要予測を踏まえて本インフラの展開について論じる。

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の上で運用している（図1）。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が可能なシステムを導入している。

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）を実践してきている。これは旭川医科大学が地域貢献事業の一環として位置付けて行っている、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。これまでに内科、整形外科、眼科、脳神経外科、皮膚科、生理学領域よりテーマが選定されて全11回開催されており、当初は旭川市及び近隣市町の住民を対象にスタートしたが、今では参加サイトが21ヶ所にも拡大している[8][9][10][11]。この取り組みは、全日本社会貢献団体機構より平成19年度「命を大切にする研究・事業」として支援を受けた[12]。

センターが提供するこのような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おり、現在は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。

センター設備機器のIP対応化を2005年度に実行したことにより、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。同時に、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、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[13][14][15]。

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いる。稚内市内及び利尻島の医療機関に衛星通信機器を設置して、衛星インターネット回線における遠隔医療実証実験を行い[16]、平成19年度からは衛星回線と地上無線回線とを融合したネットワークシステムを構築して、離島を含む6地点を結んだ実証実験へと拡大している（図2）。

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3に示した。

外部ネットワークとの通信経路には四つ（<1>～<4>）があり、各々について若干の説明を加える（<数字>は図中の番号と対応している）。

<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4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導入することにより、電子証明書（以下、証明書）を利用者に配布した上で、S/MIMEによる暗号化メールの交換を可能にする。

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。

クライアント側におけるメール添付ファイルの作成用にはPDF作成ソフトウエアAcrobat 8 Professional（アドビシステムズ株式会社）を用いたほか、紙類のデジタル化にはカラーイメージスキャナScanSnap S300（株式会社PFU）を用いた。

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[17]。

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5）。

(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動作検証

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う。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6）。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。

送信された暗号メールのMIMEヘッダ部は、application/x-pkcs7-mime、smime-type = enveloped-dataとなっており、正しく暗号化されていることを確認した（図8）。

一方の受信者側では、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9,図10）が、未所持の場合には復号することができない（図11）。

これら一連の動作確認を通して、S/MIMEアプリケーションの正常動作を検証できた。

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6）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7）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9）してから復号結果が表れる（図10）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、測定には次の仕様の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

測定結果を図12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バヘッド時間：Y（s）は、各々次の関係式で示された。

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　システムの運用性評価

F.1.1 暗号メールでの応答性

測定結果によれば、3MB程度のメールサイズの場合、それを暗号化するのには約4秒の余分な時間を要するが、この暗号化に係る処理時間が実用的に許容範囲であるかにつき考察する。

放射線や病理領域のような画像診断を主とした遠隔医療においては、大容量データを効率的に伝送できる性能、機能を有した専用システムとして構築され、セキュリティにも配慮されているのが一般的である。電子メールに医療画像を添付して伝送する情報交換手段は汎用性が高いが、画像伝送を定型的な業務スタイルとするような場面で用いるには煩雑であり、この手段が専用システムに代替されることは考えにくい。

暗号化メールを頻度の少ない非定型的な情報交換手段として用いるとするならば、遠隔医療を想定した場合に、暗号化処理のオーバヘッドが実用上問題になることはないと考えられる。

F.1.2 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について、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。

本運用に至る上で、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.1.3 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について考慮が必要である。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等の工夫が必要と考える。

F.1.4 CA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。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、各々対処が必要であった。

運用モデルとしては高信頼性が絶対的な必要要件であるため、実運用に向けては信頼性評価を繰り返し十分な安定性を確保する必要がある。

F.2　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、インターネット側からのセキュアなメンテナンス環境を用意している（図13）。

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、保守用途のように利用者が限定されるような運用場面においてこの方式は運用コストが小さく有利である。

F.3　遠隔医療におけるPKIの可能性

旭川医科大学病院では遠隔医療を積極的に行っており、実施件数が増加傾向にある（図14）。独立行政法人情報通信機構、北海道リサーチセンターでは「オンデマンド型ネットワーク制御技術の研究開発」プロジェクトの中で、旭川医

科大学病院の診療実績と遠隔医療実績を基に北海道での遠隔医療需要予測を行った[18]。そこでは関連する他の医療機関の電子カルテ閲覧件数が最も多くなると推測している（図15）。電子カルテには図10の様な静止画像や文字情報が含まれており、安全に送信するためにPKIがきわめて有用であると考えられる。

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。又、他のPKI方式との比較、北海道における遠隔医療の需要予測をする中でPKIの適用可能性について論じた。

PKIによる基盤整備が進むことにより、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の増すことが期待できる。

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）－過去・現在－．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]　全日本社会貢献団体機構．http://www.ajosc.org/subsidy/2007presently/subsidy02.html

[13] 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．

[14]　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.

[15]　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，廣川博之，佐々木春光，林弘樹：アジア・ブロードバンドネットワークを用いた眼科遠隔医療実験－3カ国同時開催3D-HDバーチャル眼科シンポジウムの実施－．日本遠隔医療学会雑誌，Vol.3(2)：195-196,2007.

[16]　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.

[17]　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/．

[18] 独立行政法人情報通信機構．　オンデマンド型ネットワーク制御技術の研究開発プロジェクト研究開発最終報告書．　(印刷中)

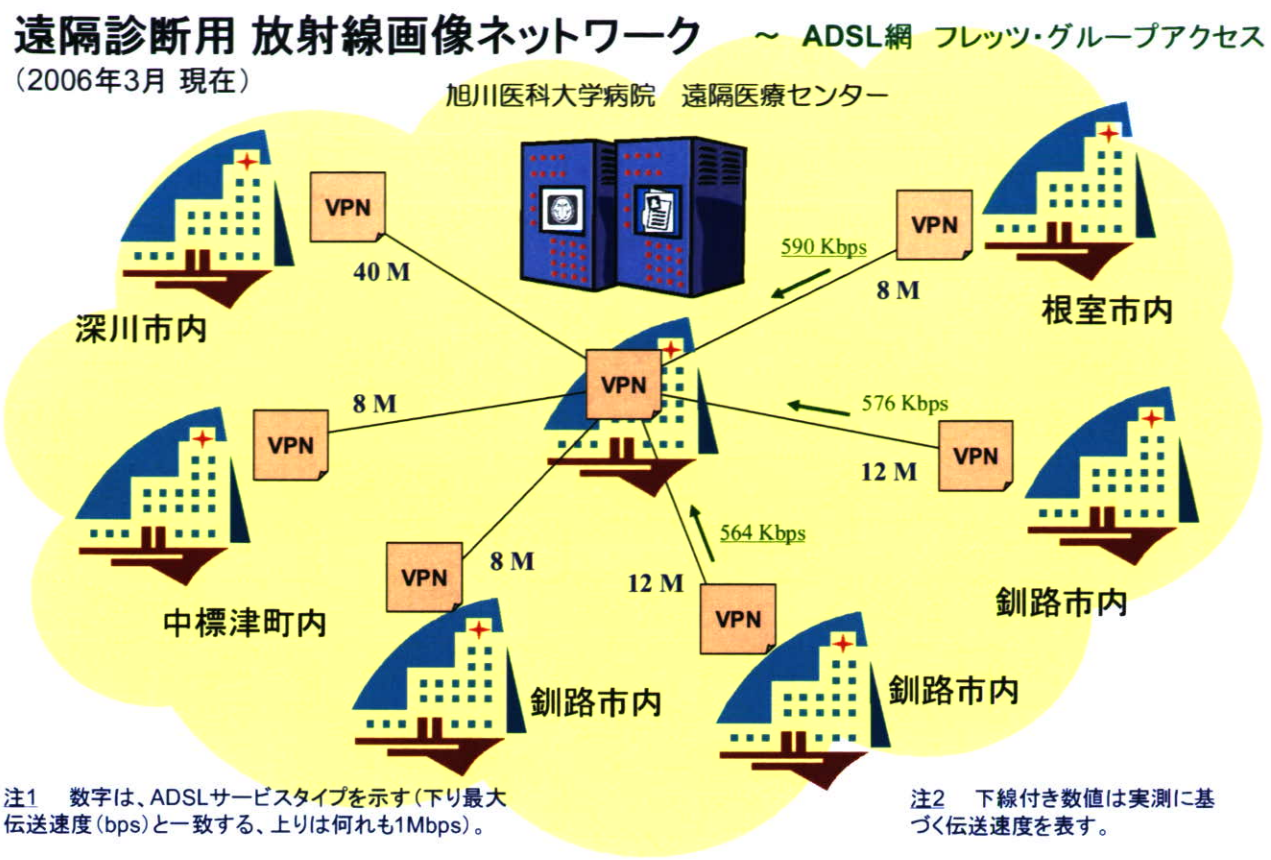

図1 遠隔医療ネットワーク（放射線画像の遠隔診断用途）

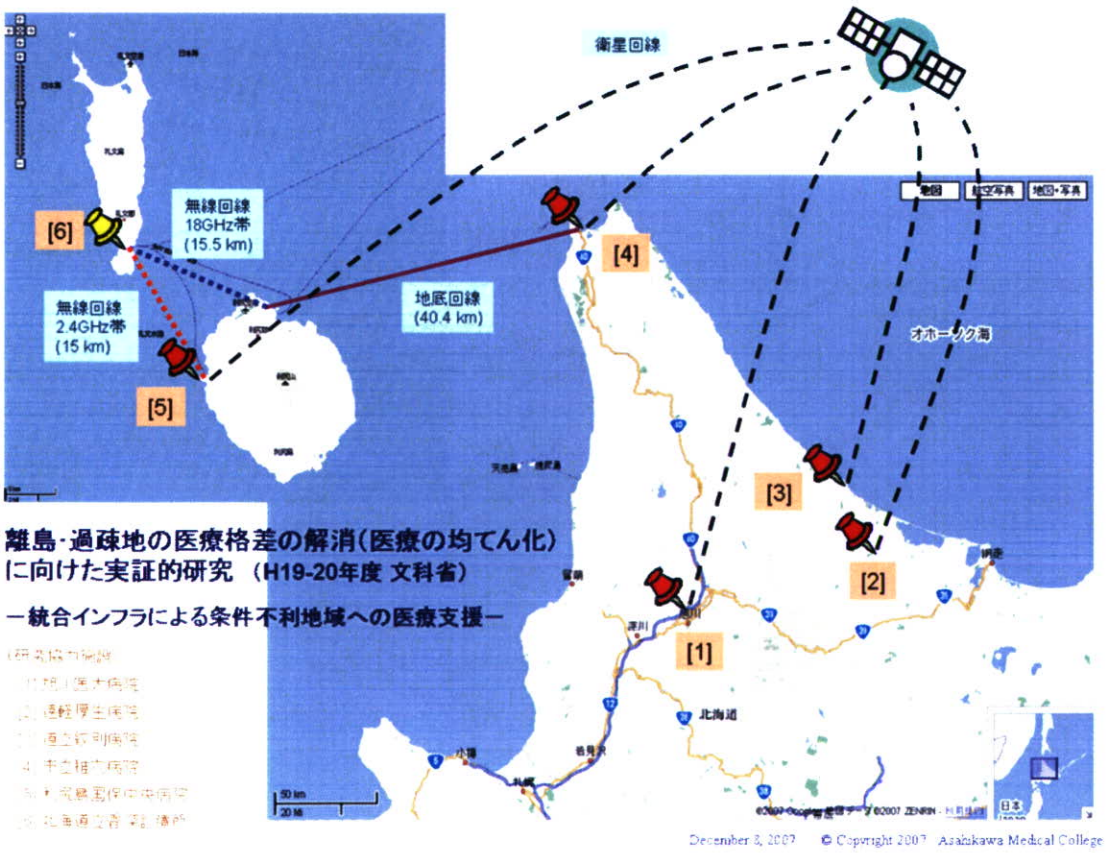

図2 統合インフラによる条件不利地域への医療支援

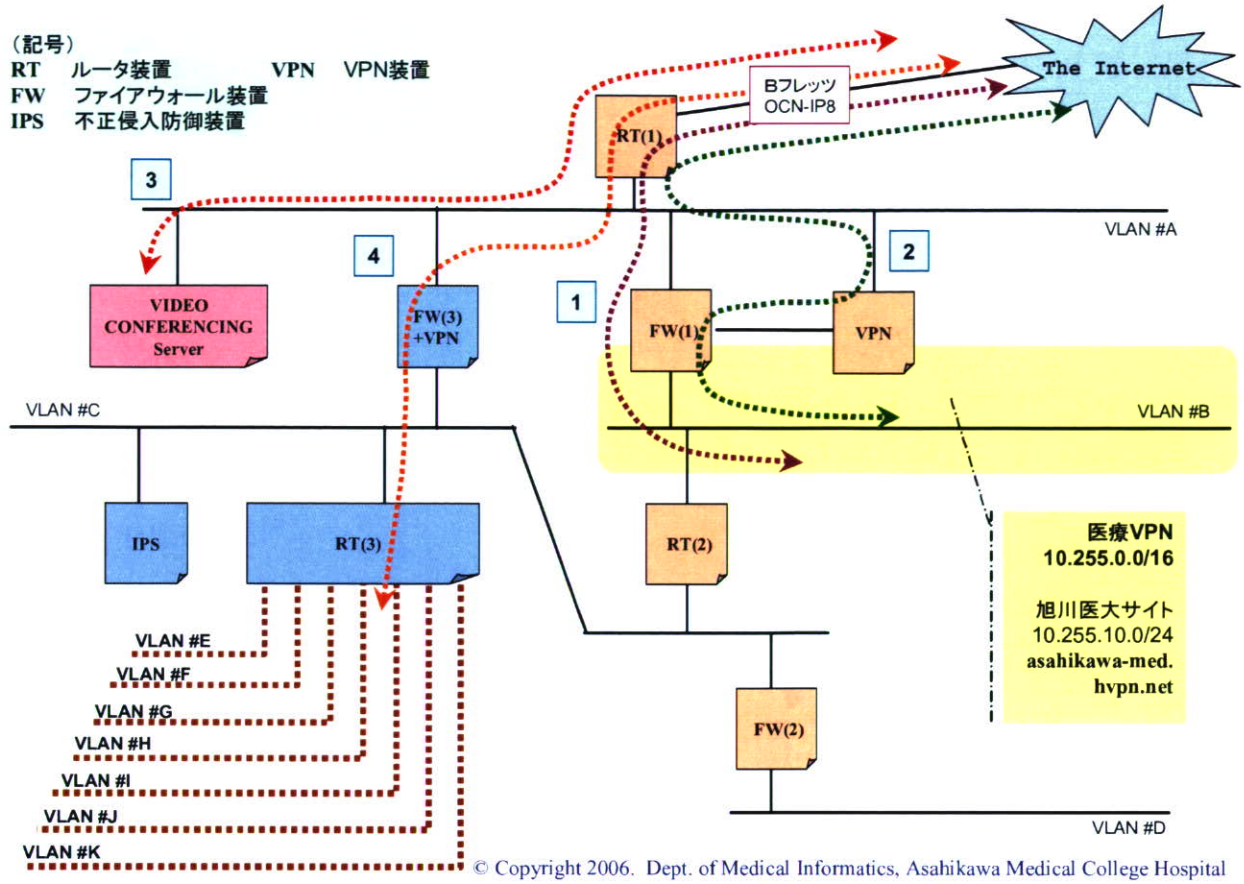

図3　遠隔医療ネットワーク全体構成図

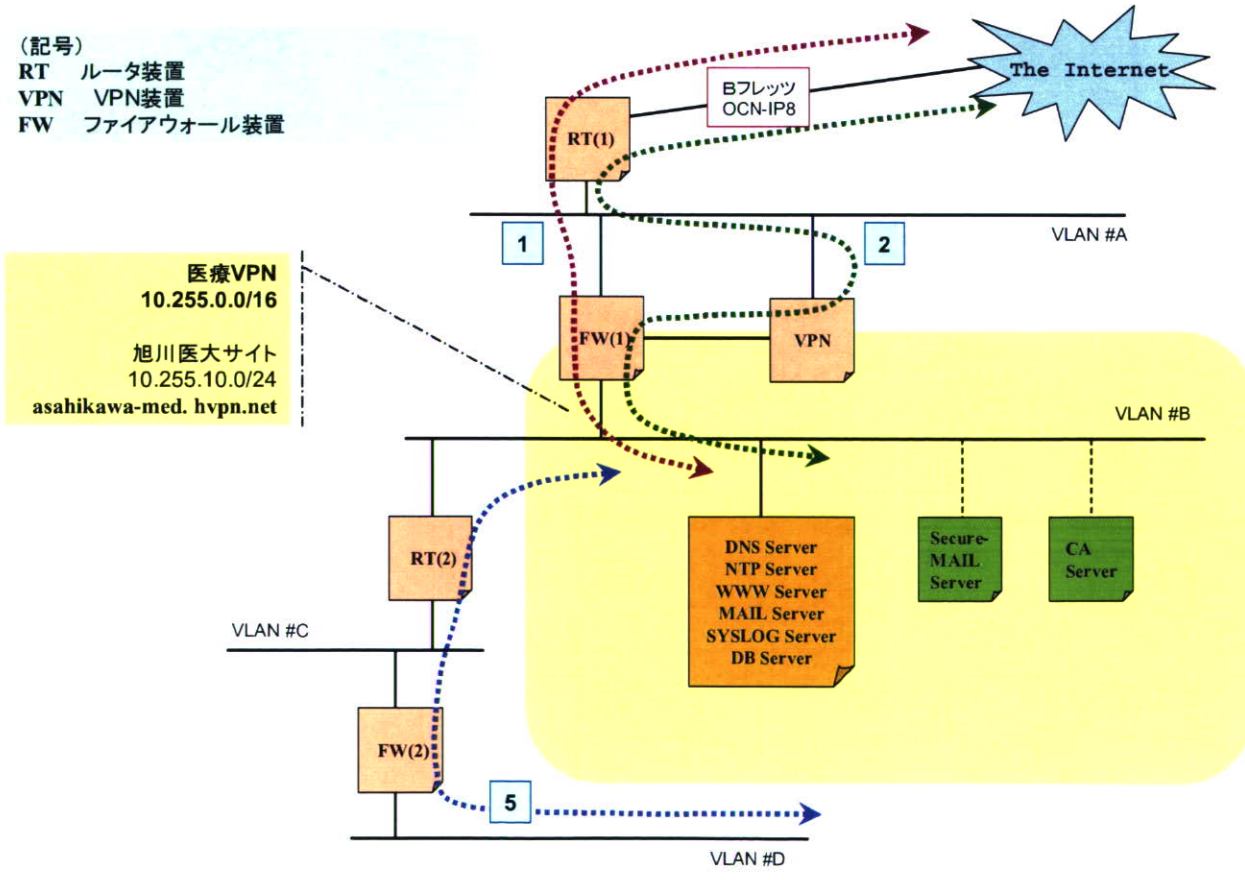

図4 医療VPN旭川医大サイト構成図

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

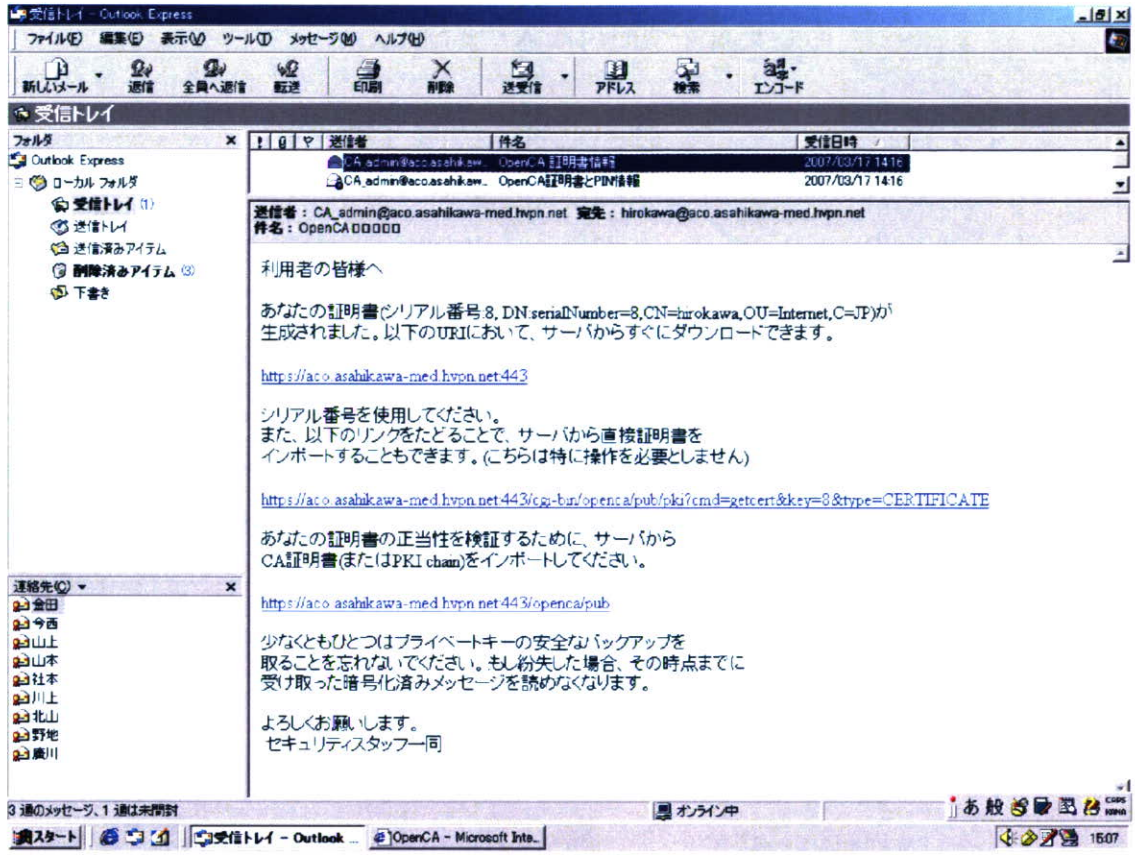

図5　証明書発行時に送付されてくるメール　（二通）

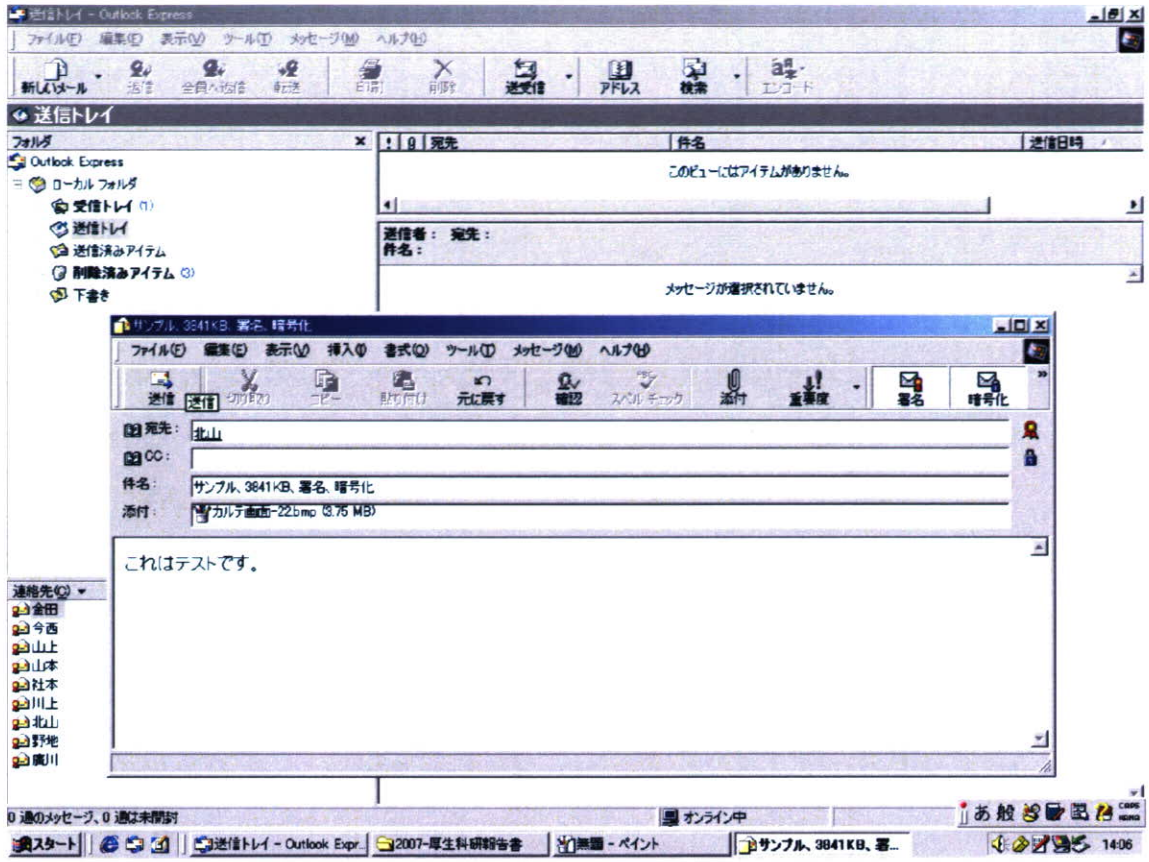

図6 MUA画面(送信側; 1) 暗号化メールを作成した状態

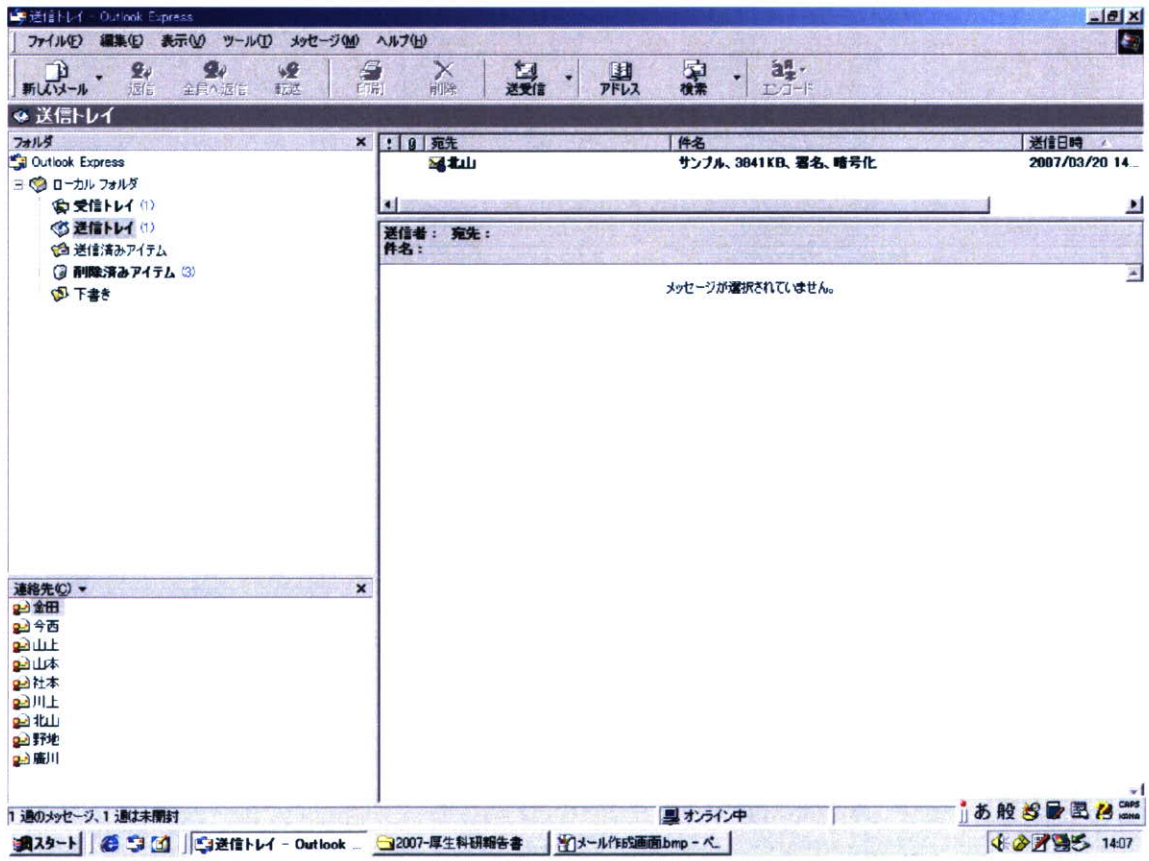

図7 MUA画面(送信側; 1) 図4で「送信」ボタンを押した後に、送信トレイにおかれた状態


root@aco:/var/spool/mail - シェル - Konsole
セッション 編集 表示 ブックマーク 設定 ヘルプ
From hirokawa@aco.asahikawa-med.hvpn.net Sat Mar 17 21:41:11 2007
Return-Path: <hirokawa@aco.asahikawa-med.hvpn.net>
Received: from NAVCES3 ([172.16.51.203])
by aco.asahikawa-med.hvpn.net (8.13.1/8.13.1) with SMTP id l2HCfBMf006450
for <kitayama@aco.asahikawa-med.hvpn.net>; Sat, 17 Mar 2007 21:41:11 +0900
Message-ID: <000b01c76891$b19706c0$cb3310ac@asahikawamed.hvpn.net>
From: "=?iso-2022-jp?B?GyRCVyJAbhsoQg==?=" <hirokawa@aco.asahikawa-med.hvpn.net>
To: "=?iso-2022-jp?B?GyRCS0w7MxsoQg==?=" <kitayama@aco.asahikawa-med.hvpn.net>
Subject: =?iso-2022-jp?B?GyRCJTUlcyVXJWshIkU6SVUbKEI1NzhLQhskQiEiPXBMPkIVMEUbKEI=?=
=?iso-2022-jp?B?GyRCOWYyPRsoQg==?=
Date: Sat, 17 Mar 2007 21:41:47 +0900
MIME-Version: 1.0
Content-Type: application/x-pkcs7-mime;
smime-type=enveloped-data;
boundary="----=_NextPart_000_0007_01C768DD.11844250";
name="smime.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="smime.p7m"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.50.4807.1700
X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4910.0300
X-IMAPbase: 1174114815 27
Status: O
X-UID: 27
Content-Length: 1511057
X-Keywords:
MIAGCSqGSIb3DQEHA6CAMIACAQAxggJYMIIBKAIBADCBkDCBijELMAkGA1UEBhMCSlAxEzARBgNV
BAoUCk9wZW5DQV9hY28xDTALBgNVBAsTBEpvaG8xIzAhBgNVBAMTGmFjby5hc2FoaWthd2EtbWVk
Lmh2cG4ubmV0MTIwMAYJKoZIhvcNAQkBFiN5YW1ha2FtaUBhY28uYXNhaGlrYXdhLW1ZC5odnBu
Lm5ldAIBBzANBgkqhkiG9w0BAQEFAASBgIVSEOTXxKFAG7FmPw1+eIdwY8IBujVp/0LLTJpOr/SW
CoiQ5IJBLz0CPLqRWFus7y+qHqDMWaVGdGKWhz9R0JB+r368u2kYNVCZC/Xkvy7Bj3d2tLmVOgJI
OZqz9YVUJOIgWqDOnEpQehPSYKemO5d2phNSyUiuKeL7v5HIfbhVMIIBKAIBADCBkDCBijELMAkG
A1UEBhMCSlAxEzARBgNVBAoUCk9wZW5DQV9hY28xDTALBgNVBAsTBEpvaG8xIzAhBgNVBAMTGmFj
by5hc2FoaWthd2EtbWVkLmh2cG4ubmV0MTIwMAYJKoZIhvcNAQkBFiN5YW1ha2FtaUBhY28uYXNh
aGlrYXdhLW1ZC5odnBuLm5ldAIBCDANBgkqhkiG9w0BAQEFAASBgIu1vaXDGdIvYxOpEy/iJ1O/
I8RclJKYSIj6Vp6VONE6IWSR8EnqZqRf00AmgYgi8zTo8J9fMcPCQgSpu3edAuAwComvNEaIDg3w
Mf8w8I7SDX6KBECeqwHZ1SFbw8kdltLYoithTJxFSMvrKwvpMs5vJwK1Htzu9Sg+dE0Wzf4FMIAG
CSqGSIb3DQEHATAaBggqhkiG9w0DAjAOAgIAoAQI2VDXr7p1QSCggASCBADvz4QCidA7SX4ttc5R
p36N3ZeTu5Ix7zZ0W+ImFChdPpiaGf3W3+SCxyTzTNEVtR30py7pd1zcUWsP36ZtnZH20mE9/MWb
GjdRQNECaG+9YU7C5U4uCFXmSArvBNuqDOJ1WT3bkISTdG1sRhAMbCN+WYndPFVzSDf7+58XB24m
CvKS6kTujmCBKGELJbXVSShxwAasjSoE8pwLvIAhI7onkZocfTjUeouPS084zPNhtEhUt+AF/Os9i
RcQxJjyc6gG68TAOdw3t1E3erDBfJX1FeGSGNn+AqJ6TQO1LjwItIdf26TRI+tgvtp3w4z/VdX8j
Y6GerkgFhX/VlyJW/xNMrH7Z/TpIITg1igM9DaNgp6EChMgulASzEUTuzS061++epmuBUgAAAAAA
AAAAAAA=
シェル
シェル No. 2

（ 途中省略 ）

図8　暗号化メール　メールサーバ上のmailboxを表示したところ

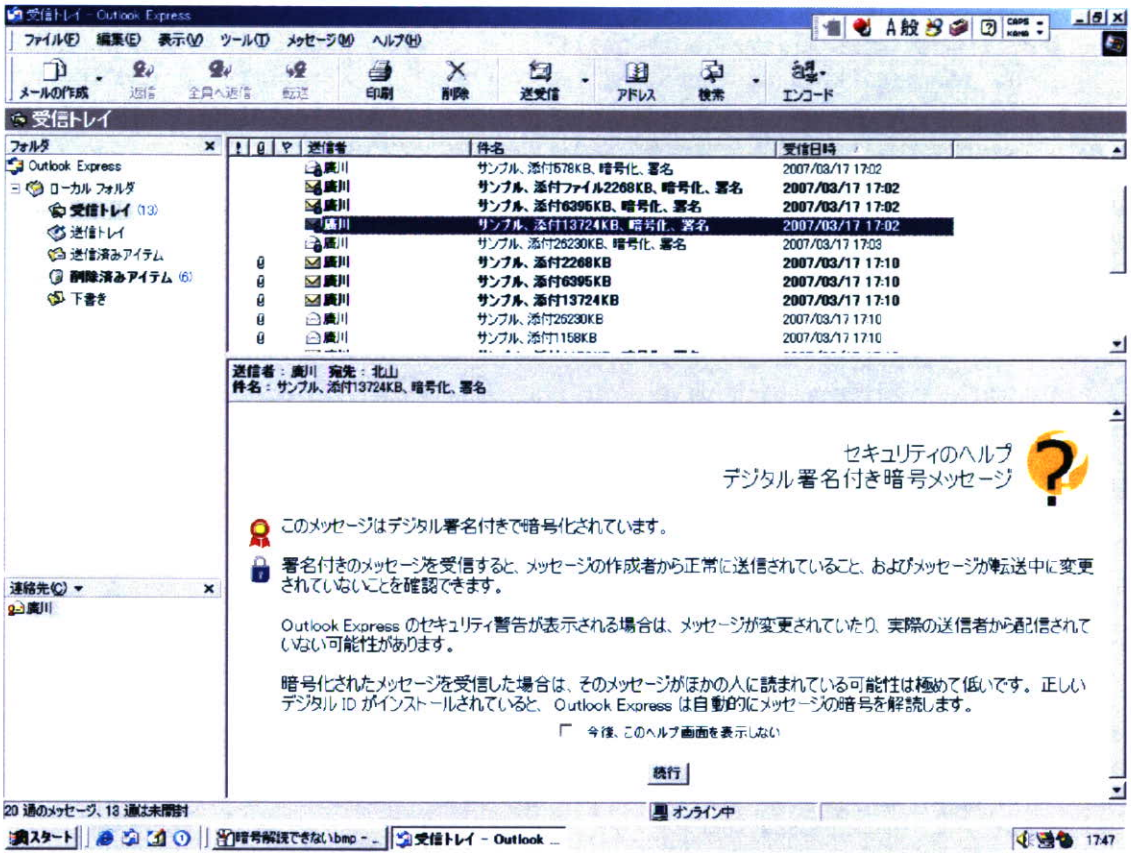

図9　MUA画面(受信側；1)　暗号メールを受信した状態

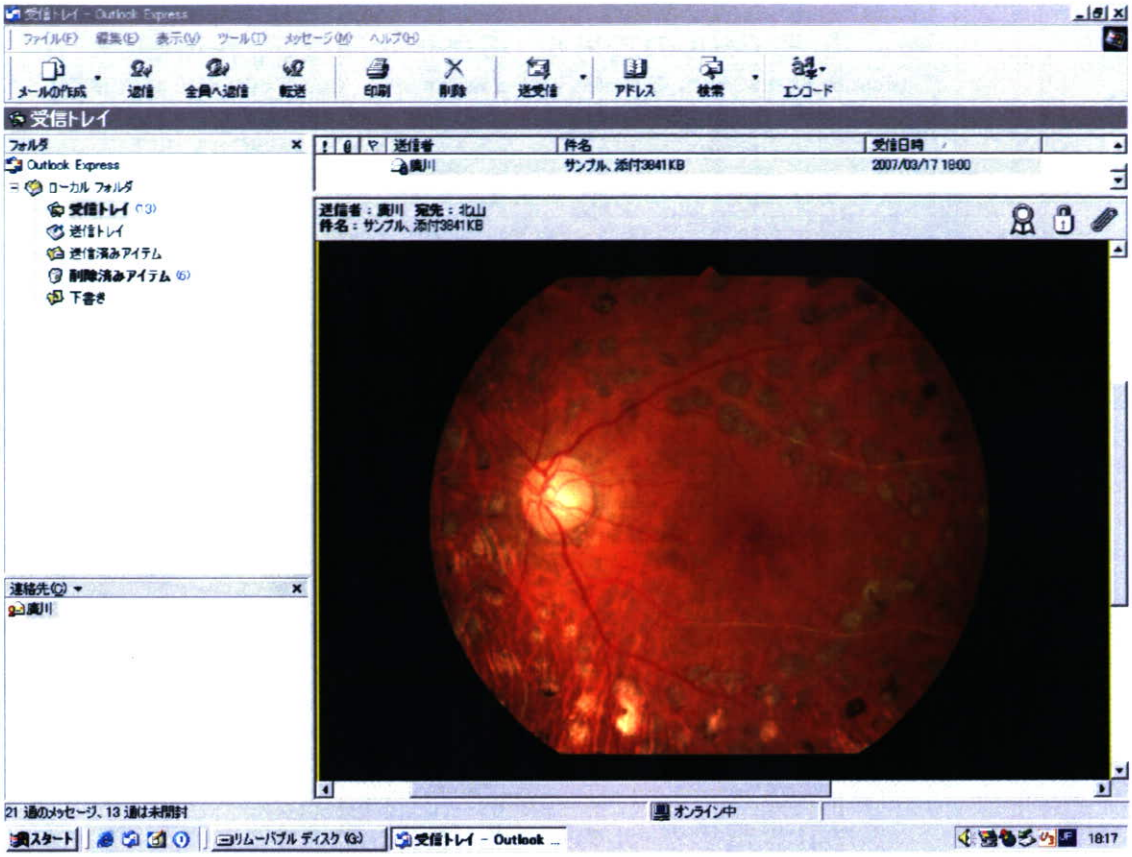

図10　MUA画面（受信側；2）　図9でボタン「続行」を押下して、メールに添付されていた画像を復号したところ

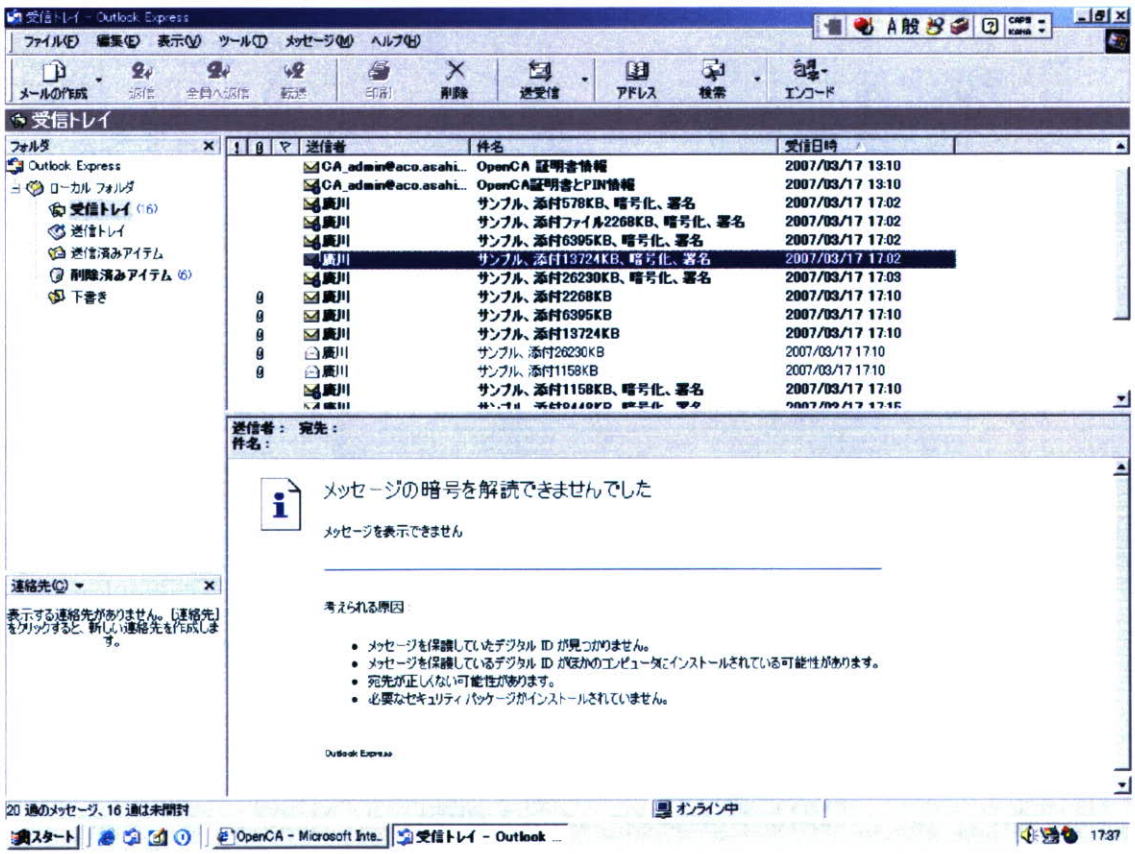

図11　MUA画面（受信側；3）　受信者が秘密鍵を持たない（インストールしていない）場合