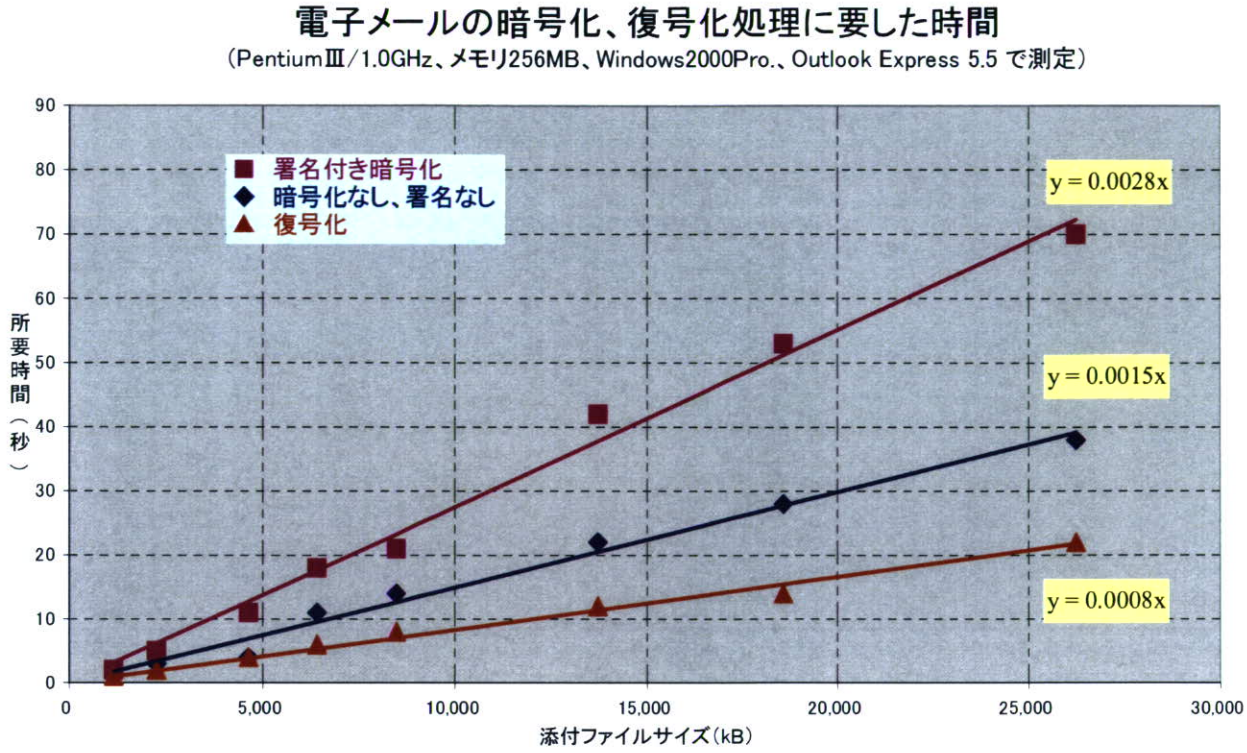


図12　電子メールの暗号化、復号化に要する時間

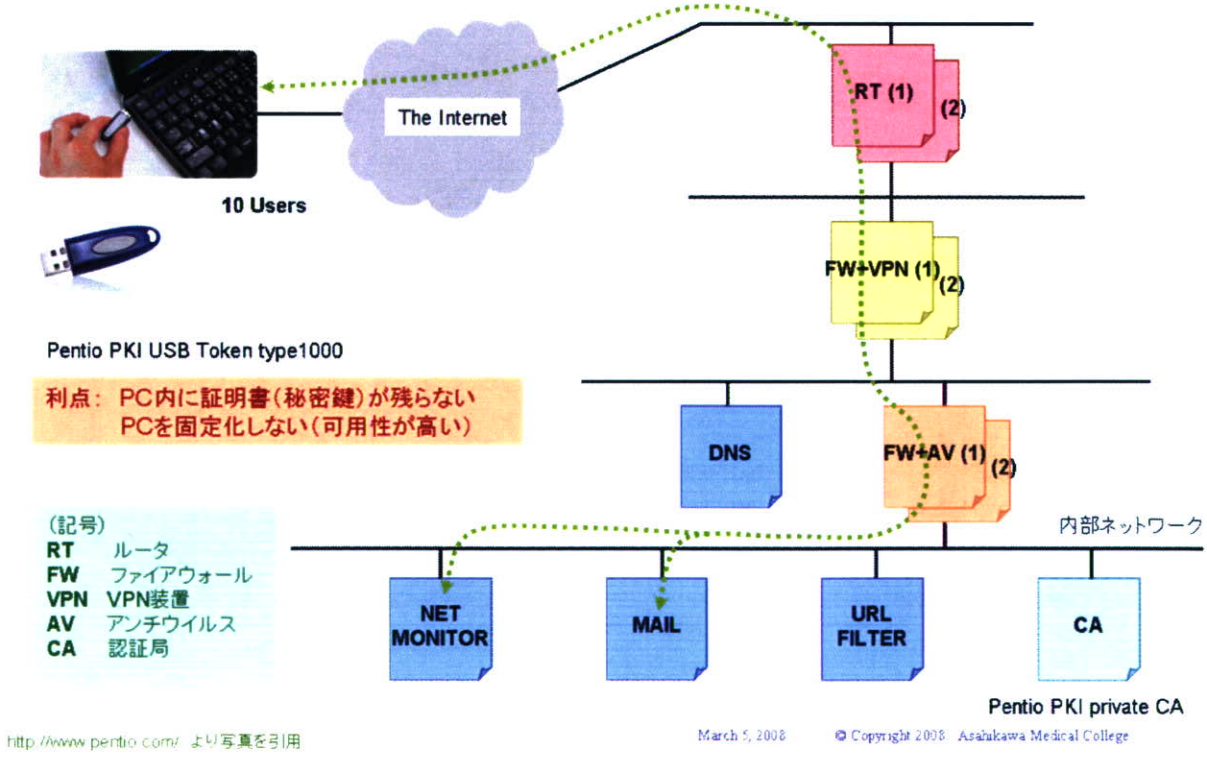


図13　PKI USBトークンを利用したVPN、CA運用

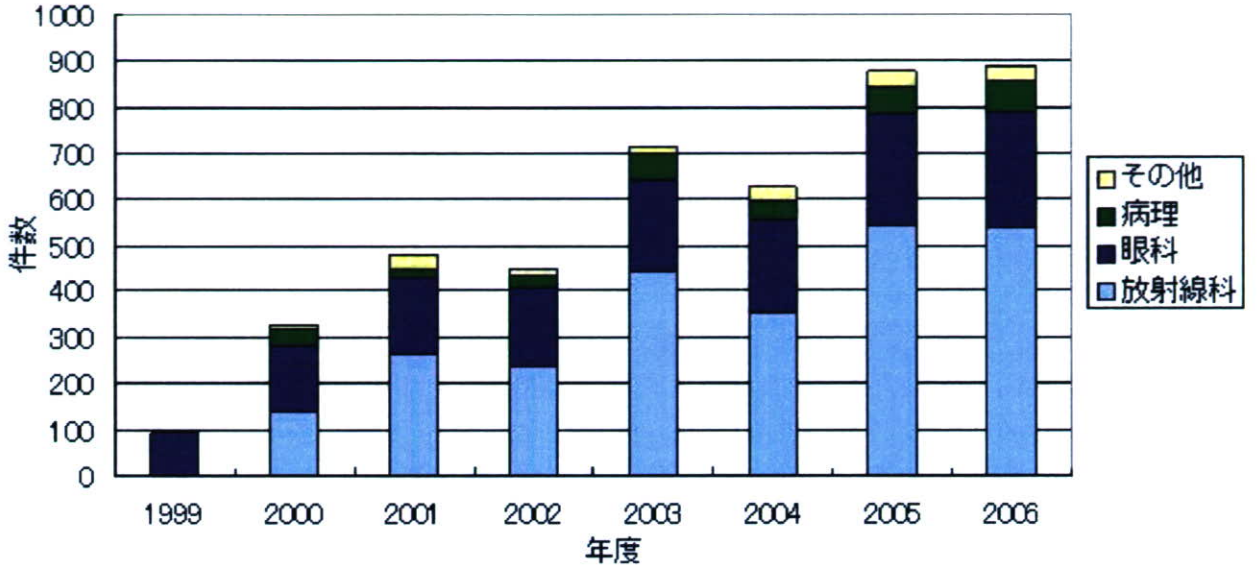


図14　旭川医科大学病院遠隔医療センターの利用実績

（参考文献　18より）

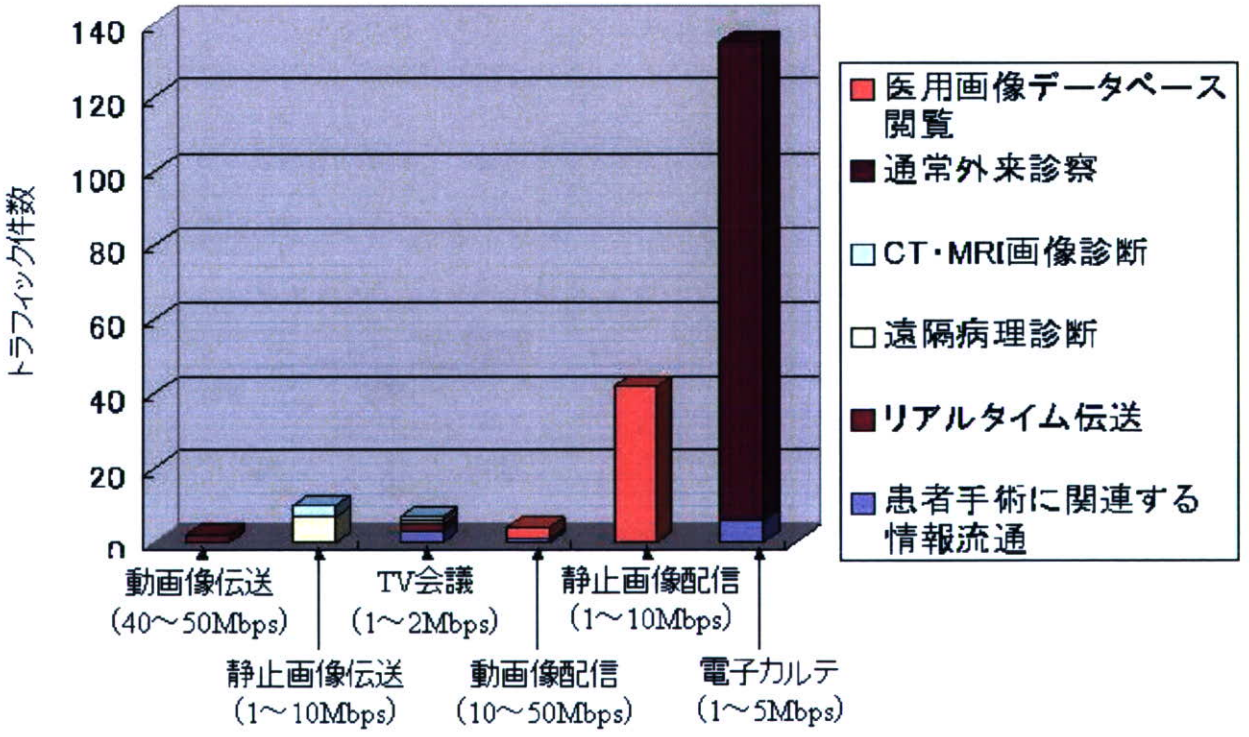


図15　一つの拠点病院で発生するコンテンツ別トラフィック件数（1日あたり）

（参考文献　18より）

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

三重遠隔画像診断ネットワークにおける運用実験

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
研究協力者　高田　孝広　三重大学医学部附属病院　医療情報部　講師

研究要旨
医療VPNとプライベートCA（認証局）に接続された三重遠隔画像診断ネットワーク内に設置されたプライベートCA（認証局）を利用して、VPN通信時の認証および電子メールの暗号化と電子署名を行った。これによりVPN通信の信頼性向上とPKIによる暗号化メールと画像読影レポートへの電子署名付与により各医療機関との情報交換において真正性確保ができた。この医療情報のインフラは、医療情報を安全に交換する事が可能となり、セキュリティを確保しての医療連携が可能となった。

A．研究目的

これからの地域医療は地域住民がどの地域医療機関に受診しても、最新の医療サービスが受けられたり、同一の医療情報が得られたりするように地域や医療機関のバリアフリーを実現する必要があり、医療情報の連携は必要不可欠なこととなってきている。しかし、医療情報をネットワーク上で共有・交換する場合、通信経路上のセキュリティを確保するとともに情報の発生元が正しいという保証と確かに本人であるという認証が必要になる。そこで、本研究では医療VPNと接続されたクローズドネットワークである三重遠隔画像診断ネットワーク上に設置した地域医療専用プライベート認証局（CA）を利用し、VPN通信時の認証及び電子メールの暗号化を行うと共に、認証局から証明を受けることにより医師個人の電子署名で遠隔画像診断の読影レポートの安全な提供および真正性の検証を行い、医療VPNとPKIを併用した安全な医療情報交換におけるセキュリティ確保の技術的な方法と問題点ならびに運用方法と管理体制等の検証を行う。

B．研究方法

三重遠隔画像診断ネットワークは三重県下で地域中核病院と放射線読影専門医をプライベートネットワークで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。依頼病院側には通信回線と接続するためのルータと画像転送のためのゲートウェイPCを依頼病院のネットワークに設置する。この画像転送ゲートウェイPCは通常のWindows PCにVPNクライアントソフトとDICOM転送ソフトおよびリモートコントロールソフトをインストールしたものである。この画像転送ゲートウェイPCのVPNクライアント機能とNPO読影センターのVPNサーバにより遠隔画像診断ネットワークを構築しており、各施設のモダリティやDICOMサーバはゲートウェイPCとだけ接続し、各施設のLANやモダリティは遠隔画像診断ネットワークには接続していない（図１）。

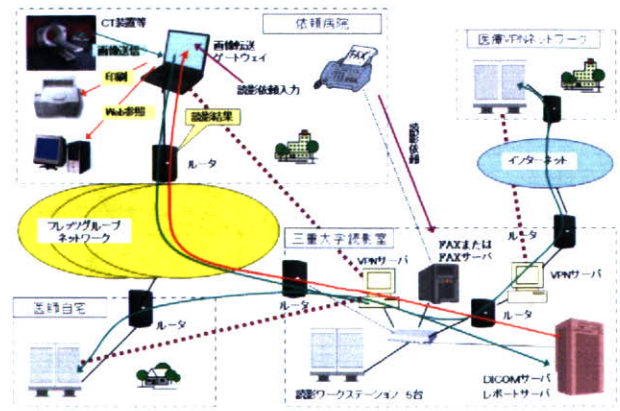


図1　VPNネットワーク接続

ネットワーク通信回線としてはインターネットを使用しない閉じたネットワークであるフレッ

ツグループ回線を使用するが、物理回線としては光回線を基本とし、利用できない場所はADSL回線を使用する。この回線を接続するルータは依頼病院側では通常の安価なブロードバンドルータを使用している。なお、フレッツグループ回線は安価でプライベートネットワークを利用できるが、10箇所までの制限がある。これについてはVPNサーバで各グループを接続することにより、3つのグループ23箇所を接続している。また、海外留学中の医師自宅との接続はインターネットを使用しているが、セキュリティ対策として、別VPNサーバで別セグメントとし、遠隔画像ネットワークとはルータで接続しアクセス制限を行っており、三重県内のフレッツグループ網と海外拠点へ転送する回線はそれぞれ独立し、混在することはない。画像は専用のDICOMゲートウェイ装置経由で自動配送しており、また、海外拠点からの画像を大学内海外拠点用サーバに逆転送することを不可としている。読影依頼については依頼病院からオーダ連携または専用Webページを利用するために、ゲートウェイサーバおよびWWWサーバを設置している。

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間接的に接続しており、地域医療専用の認証局として、Windows2003をOSとした既存のサービスであるWindowsの認証局サービスでプライベート認証局（CA）を構築した（図２）。

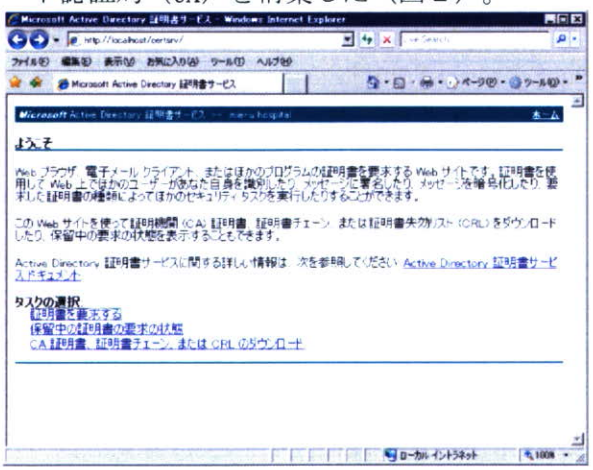


図２　プライベート認証局

この認証局で、電子メール及びWebブラウザの認証を行い、暗号化・なりすまし及び改ざん防止の検証を行った。電子メールはS/MIMEプロトコルを使用し、認証局から発行した証明書を使用することにより、セキュアなメールを簡便に送受信できるようにした。また、認証局から発行した証明書を使用することにより、HTTPSによるセキュアWebアクセス暗号化通信を行うことが可能である。

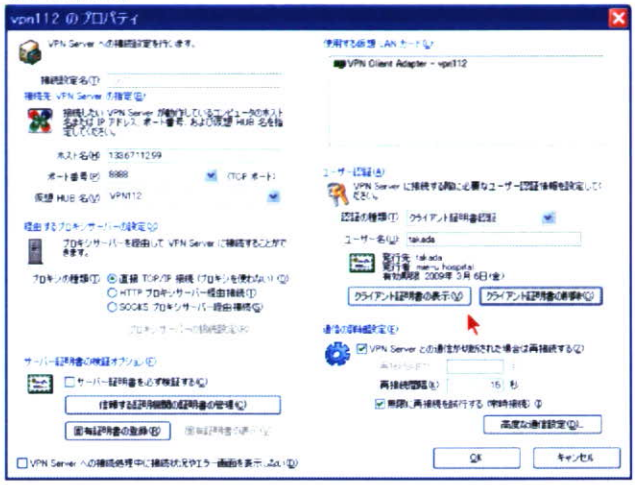


図３　VPN接続の認証

この認証局であらかじめ発行したユーザ証明書を使用することにより、VPN接続時のユーザ認証を行い、VPN接続の信頼度を向上させた（図３）。また、認証局で、読影レポートを作成する医師個人の電子署名を行い、読影医師本人であることの証明および医療情報の真正性を確保した。これら暗号化および認証技術により、情報の原本性・真正性を確保し、データの改ざんなどの不正アクセスから医療情報の保護の検証を行った。

C．研究結果及び考察

本研究で実証的に構築したソフトウェアVPNネットワークとプライベート認証局で、三重遠隔画像診断ネットワーク内で利用する電子メールは認証局から発行した証明書を使用することにより、セキュアなメールを送受信することができた。また、電子メールの添付ファイルも同時に暗号化された。この暗号化電子メールを利用できることにより、読影結果のレポートなど重要な医療情報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、平文で送信する場合に比べて情報漏洩に対しても有効である。また、認証局から発行した証明書を使用することにより、https暗号化通信によるセキュアWebアクセスや地域医療ネットワーク内のレポートサーバへの読影依頼書の送付、読影レポートの参照を安全に行うこと

ができる。

図４　レポート一覧画面

このように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ことが検証できた。認証局による証明及びVPN通信により、読影依頼書、読影レポートの送付を真正性を確保して安全に行うことができ、限定的ではあるが地域医療機関との医療データの安全な交換が可能となった。地域医療ネットワークにより、地域住民が地域のどこに住んでいても、最新の医療・福祉サービスが受けられる安心社会を実現させ、医療・福祉を包括し、地域や医療機関のバリアフリーを実現するためにもセキュリティ確保は重要なことであり、緊急時においては医療の専門家同士が連携して地域住民のヘルスケアを実現するネットワークが必要になると共に、今後ますます高度化、専門化する医療福祉に対し、セキュリティの確保された医療情報交換による医療連携により住民の健康管理に当たる体制を進めていく必要がある。地域医療ネットワークは医療情報を扱うことから信頼性のある安心して利用できるシステムでなければならないが、VPNネットワークと医療専用の認証局により、医療データの真正性の確保および通信経路の暗号化、情報の原本性・真正性を確保できることは実証できた。しかし、医療情報の連携を行う場合に、最も重要なことは情報に対する責任の明確化と内容の信頼性の保障の元にタイムリーに情報連携ができることであると考え、施設間連携のために共通のデータベース、共通のデータ構造、共通のアプリケーションインターフェースなどの標準化が必要であり、各施設のデータを施設間でシームレスに交換・利用できるシステムを目指して医療ネットワークを構築していきたいと考えている。

参考文献

１．高田孝広，山本晧二、医療情報の共有化とセキュリティ確保、新医療　31巻11号　Page128-131(2004.11)

２．高田孝広，永岡宏朋、永澤直樹、山本晧二、プライベート認証局とVPN通信によるセキュリティを確保した医療情報共有と提供、医療情報学22回連合大会論文集Page542-543(2002.11)

３．山本晧二，高田　孝広，永岡　宏朋，永澤　直樹、診療所・国立病院・大学病院の医療連携支援機構、医用画像情報学会誌　18巻3号　Page125-134(2001.09)

F．研究発表

なし

G．知的財産権の出願・登録状況

なし

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

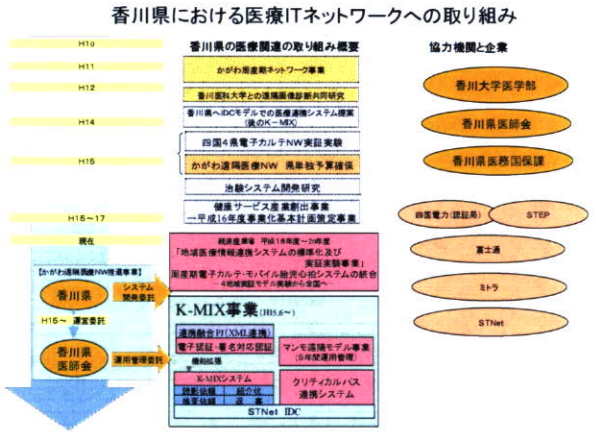
かがわ遠隔医療ネットワーク、周産期電子カルテネットワークプにおける運用実験

分担研究者　原　量宏　香川大学医学部附属病院医療情報部教授
研究協力者　横井英人　香川大学医学部附属病院医療情報部講師
　　河内一芳　香川大学医学部ネットワーク管理室

研究要旨　香川県では医療へのIT導入に積極的に取り組んでおり、妊娠管理を目的とした周産期電子カルテネットワーク、そして香川県と香川県医師会、香川大学医学部が一体となって運用する「かがわ遠隔医療ネットワーク」が稼働している。二つのネットワークの機能は年々増強されており、本年度新たにVPNを基本としたデジタルマンモグラフィの遠隔診断システムがスタートした。今後は糖尿病や肝炎の診断と治療に関して地域全体での管理など、生涯の情報を取り扱う、ＥＨＲの実現にむけて努力したい。

A 研究目的

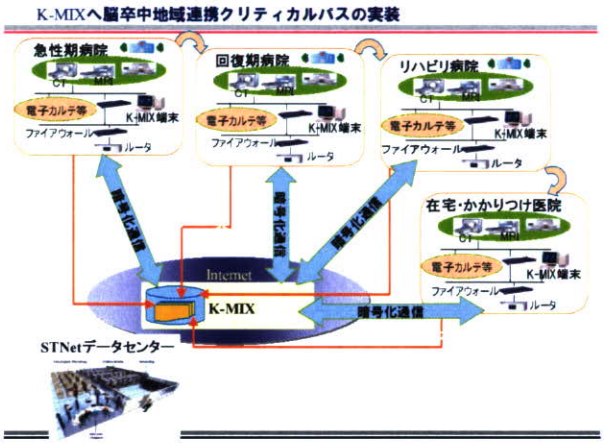
香川県においては、「e-Japan 戦略」が発表される以前から、医療へのIT導入に積極的に取り組んでおり、妊娠管理を目的とした周産期電子カルテネットワーク、そして香川県と香川県医師会、香川大学医学部が一体となって運用する「かがわ遠隔医療ネットワーク（略称：K-MIX、http://www.m-ix.jp/）」が稼働している（図１）。



（図１）香川県における遠隔医療ネットワーク構築の経緯

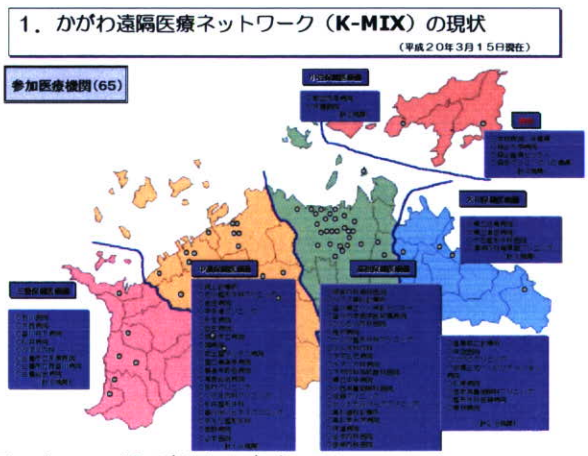
二つのネットワークの機能は年々増強されており、最近重要視されている、いわゆるシームレスな医療を目指した脳卒中地域連携クリティカルパスの機能も稼働しはじめている（図２）。

これらの医療ITネットワーク基盤の上に、あらたに厚生労働省による「マンモグラフィ検診遠隔診断支援モデル事業」がスタートすることは、香川県にとってはもちろん、今後全国規模で進む遠隔医療ネットワークの発展と普及にとって大変意義のあることである。



（図２）K-MIXへ脳卒中地域連携クリティカルパスの実装

K-MIXは07年度より日本全国の医療機関が利用できるようになっている。参加医療機関は08年3月時点ですでに65施設になり経営的にも自立できるまでに至っている（図３）。



（図３）かがわ遠隔医療ネットワーク
県外の医療機関も参加可能で現在65施設が参

加している。

B　研究方法

VPNを基本としたオリーブマンモネットワークの構成

今回開発したシステムでは、地域支援病院、予防協会、検診専門の施設、健診併用型施設など多様な施設が参加している事にくわえ、接続される機器に関しても、標準的な医療データの伝送、保存のフォーマット（DICOM規格）を利用するため、異なるメーカのマンモグラフィやＰＡＣＳであっても連携が容易で各施設が参加しやすいシステムとなっており今後全国の標準的なモデルになることをめざしている。

ちなみに今回のネットワークには、東芝メディカルシステムズ社、コニカミノルタメディカル社）、富士フィルムメディカル社、シーメンス社、ＧＥ社等５社の製品が接続されている。

B.1　要求される仕様への対応

今回構築した「オリーブマンモネットワーク」の設計にあたっては、厚生労働省補助事業としての要求条件（表１）をみたすとともに、県医師会ならびに医療機関側からの希望をできる限り反映し、さらにハード面、ソフト面でK-MIXとの連携（K-MIXユーザとの相互の読影依頼など）を考慮し、将来をみすえたシステム構成とした（表２）。

K-MIXとの連携部分に関しては、K-MIXの現状のシステムで対応可能であるが、マンモグラフィの画像は、従来のCTやMRに比較し大容量であることを考慮し、K-MIXのサーバの負荷軽減のためマンモグラフィ用に別途サーバを増強した。また将来の発展をみすえたシステム構成を考慮し、STNetのデータセンター（iDC）で医療情報の一元管理が可能な構成とし、DICOM画像にくわえ、JPEG、MPEG、波形データ、ワード文書等広範囲な情報管理に対応可能とした。

（表１）補助金交付にあたっての仕様

１．依頼側施設からマンモグラフィ画像を送信できること（必須）

２．送信画像はデータセンターにおかれたセンターサーバで保存・管理できること（必須）

３．管理ツールは、自動的に各ドクターにメール送信することにより，緊急対応が可能なこと

４．支援側施設にて、ＰＡＣＳ及びマンモグラフィビューワで読影し、専用のＷｅｂレポーティングシステムにて所見入力を実施できること（必須）

５．結果レポートは読影依頼元施設でＷｅｂ参照可能なこと（必須）

（表２）医療関係者からの要求事項

１．ハード面、ソフト面でK-MIX運営の補助となるように（県医師会）

２．K-MIXとの連携（K-MIXユーザとの相互の読影依頼など）を視野に入れること

３．将来を踏まえたシステム構成を考慮し、iDCで医療情報の一元管理が可能な構成であること

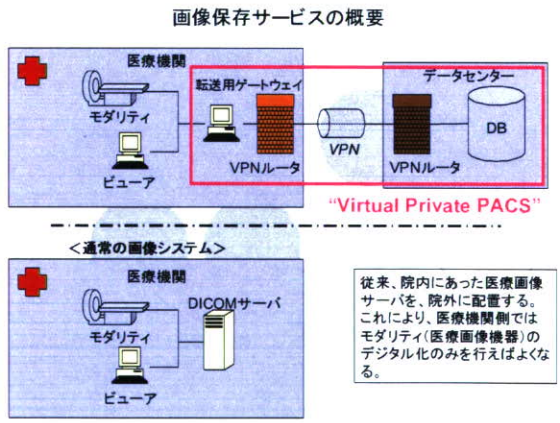
４．読影支援先を１ヶ所に固定しない仕組み（相互に補完しあう遠隔読影のシステム）とすること（厚生労働省）

B.2 VP-PACS（virtual private PACS）構想

画像情報の蓄積に関して、従来より香川大学医学部で提案しているVP-PACS（virtual private PACS）構想に対応可能とした。

本方式により、従来院内にあった医療画像サーバを院外に配置することができ、医療機関側では医療画像機器のデジタル化のみを行えばよくなる（図４）。

読影支援先を１ヶ所に固定しない仕組みに関しては、iDCで医療情報の一元管理することにより完全なn対nの相互連携が実現した。



（図４）画像保存サービスの概要、Virtual Private PACS

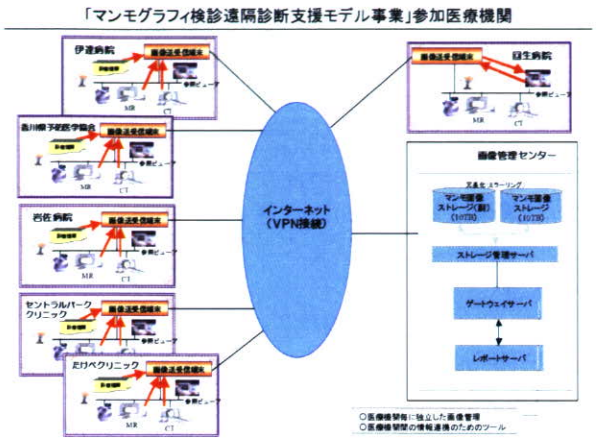
各医療機関はCTやMRなどのモダリティに簡単なゲートウエイを設置するだけでよく、高額なDICOMサーバを必要としなくなった。

B.3　オリーブマンモネットワークのシステムイメージ

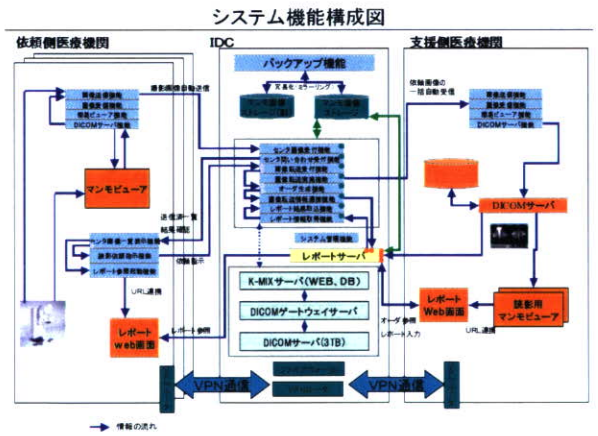
今回稼働したオリーブマンモネットワークは、支援側の施設として回生病院、依頼側施設の施設とし

ては５施設（伊達病院、香川県予防医学協会、岩佐病院、セントラルパーククリニック、たけべクリニック）から構成されている（図５）。

各医療機関とSTNetのデータセンター（iDC）との間は、インターネットとVPNにより接続されセキュリティーを確保しており、iDCを介してどの施設からでも相互に情報を送受信可能となっている（図６）。



（図５）「マンモグラフィ検診遠隔診断支援モデル事業」参加医療機関
各医療機関とSTNetのデータセンター（iDC）との間は、インターネットとVPNにより接続されセキュリティーを確保している。

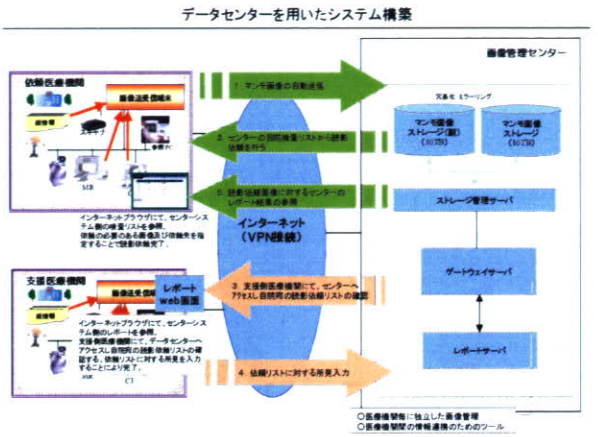


（図６）システム機能構成図

また各医療機関の機器構成に関しては、支援側に高精細のビューアが設置されていることをのぞき、支援側、依頼側とも基本的にはほぼ同じ構成である。データセンター側のシステムは、正副のマンモ画像ストレージ（各10TB）とストレージ管理サーバ、ゲートウェイサーバ、レポートサーバから構成されている。撮影されたマンモグラフィは原則として医療機関内には保存せず、直接データセンターに送信・保存する設定となっているため、医療機関側には高額なDICOMサーバを必要としないことが大きな特徴である（図７）。

B.4 オリーブマンモネットワークの運用の流れ

オリーブマンモネットワークの実際の運用の流れを説明すると、まず依頼側から撮影されたマンモグラフィのすべての画像がデータセンターに送信される。送信された画像はデータセンターに設置されたセンターサーバで保存・管



（図７）STNetデータセンターを用いたシステム構築

iDCを介してどの施設からでも相互に情報を送受信可能となっている。

理される。依頼側医療機関は、自施設のインターネットブラウザでセンターシステム側の検査リストを参照し、依頼の必要のある画像及び依頼先をブラウザから指定する（表３）。

（表３）オリーブマンモネットワークの運用の流れ

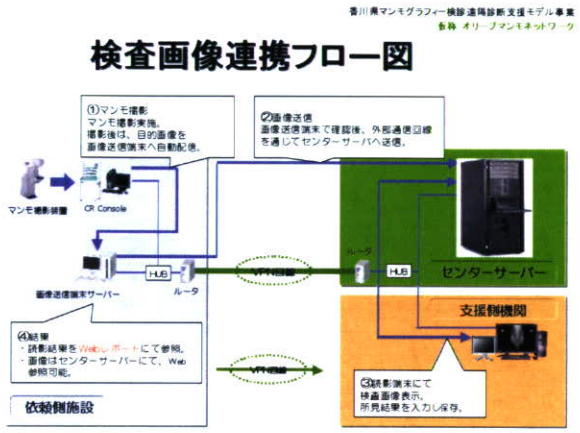
１．マンモ画像の自動送信
２．センターの自院検査リストから読影依頼を行う
３．支援側医療機関にて、センターへアクセス自院宛の読影依頼リストの確認
４．依頼リストに対する所見入力
５．読影依頼画像に対するセンターのレポート結果の参照
６．レポートシステムに関しても標準的な診断法の確立や地域全体のマンモグラフィに関するデータベースの構築実現を視野にいれる

支援側医療機関では、データセンターへアクセスし自施設宛の読影依頼リストを確認し、依頼リストにある個々の症例に対する所見を、ＰＡＣＳ及びマンモグラフィビューワで読影し、専用のWebレポーティングシステムを用いて所見入力を実施する（図８）。

B.5 オリーブマンモネットワークの拡張性と今後の展開

本システムでは、診療情報、画像情報を含め、基本的にすべてデータセンターに保存・管理される。そのため医療機関側に高額なDICOMサーバを必要と

せず、比較的安価な設備投資で本ネットワークに接続できるため、新規の医療機関が参加しやすい。マンモグラフィの読影診断についての専門医の確保が困難な地域においてもマンモグラフィによる乳がん健診を実施することができる。さらにかがわ遠隔医療ネットワークを含め、他地域の遠隔医療ネットワークとも連携は容易なため、今後全国規模でのマンモグラフィネットワークの構築が可能である。



（図８）オリーブマンモネットワークの運用の流れ

本ネットワークは、K-MIXと連繋しているため、例えば本システムで乳がんが疑われ大学病院や中核病院に転院した場合には、K-MIXを介してもとのマンモグラフィを参照することが可能である。また画像だけでなく、レポートシステムに関しても全国規模での標準化を考慮しており、今後は標準的な診断法の確立や、地域全体のマンモグラフィに関するデータベース構築実現も視野にいれている（図９）。

（図９）レポートシステム

標準的な診断法の確立や、地域全体のマンモグラフィに関するデータベース構築を視野にいれている。

C　研究結果

香川県で新たにスタートした厚生労働省の支援事業によるVPNを基本としたデジタルマンモグラフィの遠隔診断システム「オリーブマンモネットワーク」の概要に関して解説した。かがわ遠隔医療ネットワークでは、デジタルマンモグラフィの遠隔診断システムにくわえ、最近特に重要視されているシームレスな医療連繋をめざして、脳卒中地域連携クリティカルパスを実装するとともに、厚生労働省の推進する保健医療福祉分野における公的電子認証局（Healthcare PKI、HPKI）も稼働する予定である。今後は糖尿病や肝炎の診断と治療に関して地域全体での管理、電子処方箋を用いた院外処方箋薬局との連繋など、生涯の情報を取り扱う、真のＥＨＲの実現へむけて努力したい。

（本研究は、厚生労働省研究助成費、文部科学省連携融合事業経費、経済産業省研究開発助成費、香川県健康福祉部の援助による）

参考文献

[1] 原　量宏、 岡田宏基、秋山正史、千田彰一、DoPa技術を用いた在宅ハイリスク妊婦管理システムの開発　－携帯端末を用いた妊婦管理－、電気通信学会　信学技報、
MBE2003-31 p25-28、2003
[2] 原　量宏、携帯端末を用いた在宅ハイリスク妊婦管理システムの開発、月刊新医療、31, 12, 41-44、2004
[3] 原　量宏、横井英人、秋山　正史、岡田宏基、電子カルテと地域医療ネットワーク -医療連携の未来のために-, Digital Medicine、5(6) 、15-19、2005.
[4] 原　量宏、横井英人、岡田宏基、地域医療連携に向けた遠隔医療の現状と課題、ITvision、NO.10、21-23、2006
[5] 横井英人、IHE－医療機関の中と外での有用性－、Digital Medicine、6(6)、28-32、2007.
[6] 原　量宏、横井英人、小笠原敏浩、鈴木 真、中林正雄、周産期医療ネットワークの現状とこれから、-「周産期電子カルテネットワーク連携プロジェクト」-, Digital Medicine、
6(6) 、19-23、2007
[7] 原　量宏、横井英人、岡田宏基、他、かがわ遠隔医療ネットワークから日本版ＥＨＲの実現へ、月刊新医療　35(2)、48-53、2008

（以上）

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

山口県医療情報ネットワークにおける運用実験

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）を構築した。さらに、PKIとCAを利用するのに比較的容易な運用形態をとるプライベート認証局を構築することにより、イントラネットに限定してきたアプリケーションがインタネットから利用可能になった。医療VPNはネットワークのバックボーンを形成するためその存在を利用者が認識することはないが、デジタル署名と暗号化は一般の医療従事者に安全な医療情報連携を進める為の技術を啓蒙し認識させるののに重要な情報基盤となると考えられた。

A.　研究目的

地域遠隔医療ネットワークは安全な医療情報交換を可能にする情報基盤が前提であり、専用線等を用いて構築された閉じたネットワーク、インターネットや他のネットワーク上でVPNを構築したネットワーク、および公開鍵暗号基盤(Public Key Infrastructure: PKI)を用いた情報通信が用いられている。

ネットワーク上の脅威には、盗聴、改ざん、成りすまし、および、事実の否認、があげられる。PKIを用いることで、専用線接続やVPNルータのように特別なネットワークを構築することなく、通信したい機器間の安全な情報交換が実現できることにより、外部からの脅威だけでなく内部からの脅威に対しても対応可能になる。　しかし、医療連携の運用に応じたPKIの構築は技術的敷居が高く、独自に構築すること、また、それを運用することに困難を伴うため一般に利用されるにいたっていない。商用サービスを購入することで技術的な敷居を下げることはできるが、利用者の認証、秘密鍵や証明書を作成し正しく配布する、等の作業を厳密に行うには多大の人的コストおよび経費が発生する。

PKIは商用サーバの安全性を保つ方法として一般化しているが、利用者の立場から、特に医療現場での運用に即したアプローチは殆どない。そのためPKIを用いるためには、まず、参加者同士の利用をとおして、その活用方法および安全性を実感することが重要になる。一旦、利用方法及び安全性を実感できると、関係者の大きなネットワークでの活用、グローバル認証での利用への移行が容易になると考える。

そこで、証明書の発行と取得が比較的容易にできるプライベート認証局を構築し、地域医療連携の場で実際に証明書を発行し関係者間での利用を計った

B.　研究方法

図1　プライ

図２　プライベート認証局証明書をインストールした状態

プライベート認証局の簡易な運用体系：

証明書の発行、取得が比較的に容易に行うことができるプライベート認証局を構築するにあたり次の点を考慮した。

1) 証明書利用することの啓発を行うためには、まず利用してみることが重要
2) 導入時の障壁を下げるために、通常使用しないメニューやキーワードを削除
3) 一般利用者でも理解できる用語を使用
4) 遠隔医療情報ネットワークの関係者のみが利用することが前提
5) 取得した証明書を実際に利用
6) その後、本格的な導入を検討

これらを実現するために、プライベート認証局のトップページは、通常利用で用いるための最小単位となる4つのメニューを配置した（図１）

① プライベート認証局証明書取得
② 利用者用証明書の発行依頼
③ 利用者証明書の受け取り
④ 他の利用者の公開鍵検索

また、アイコンをクリックすることで、証明書のインストールが実行されるように配置している。図2に認証局証明書をインストールできた状態を示す。

まず、利用者に、3種類の証明書（認証局証明書、自分の証明書、相手の証明書）があること、それらの関係を理解してもらうことが重要である。これらの関係がわかるような配置に心がけた。

利用者の個人証明書を発行依頼のページにおいて、メールでの利用のために最低限必要な情報のみを入力するようにした。また、地域遠隔医療ネットワークの関係者（本研究ではやまめネット利用者）で利用することを前提とすると、すでに、お互いの認証は行えていることから、依頼から発行までの処理をシステム管理者(実際には運用担当者)が行うことを想定した（図３，４）。

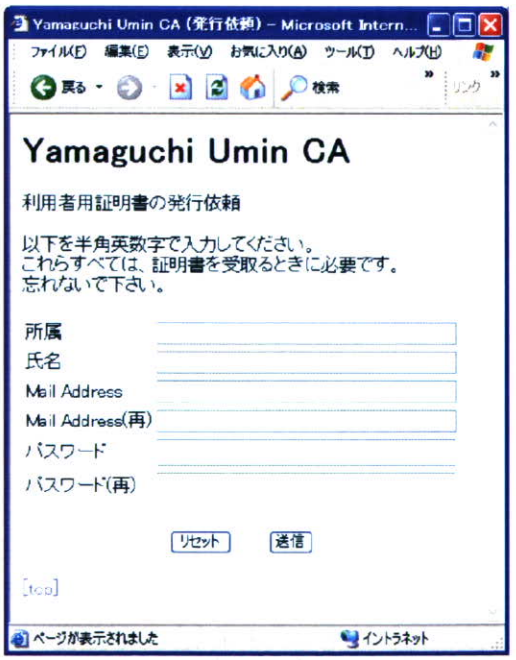


図３　利用者証明書の発行依頼

遠隔医療情報ネットワークの相手にメールを送るためには、相手の公開鍵を取得する必要がある。そのため、プライベート認証局で発行した公開鍵を取得できるページを用意した（図５）。

C.　研究結果

山口県医療情報ネットワーク（やまめネット）においてプライベート認証局の設置と運用を実現した。これまで、専用線によって分離したネットワークおよびVPNルータによって暗号化したネットワークの2種の方法で地域遠隔医療を構築してきた経緯から、ネットワークの運用管理規準が規定され利用者登録の手続きが正しく実施される状況をシステム運用の前提とした。登録者同士がお互い認識し合える人的範囲のネットワークであり、技術的に厳密な取扱い行わなくても、比較的に安全にPKIを導入することができた。また、限定された人的ネットワークにおいては、商用サービスを利用しなくても、独自に構築したプライベート認証局とそこから発行された証明書を用いることが可能となった。この点は、実際の診療業務に即した医療従事者の利用者登録、つまり、医師、看護師、医事職員、等の認証を登録申請する施設管理者の責任で行う、という現実的で適用可能な運用に繋がった。

遠隔医療ネットワークの関係者間で実際に電子メールの際に、自分の証明書を用いることでデジタル署名を添付することでなりすましおよび否認を防止し、メール送信の相手の公開鍵を用いて暗号化することにより盗聴および改ざん防止の措置を実施した。

図４　利用者証明書の取得

このデジタル証明書および暗号化によって、これまで、閉じたイントラネット上でしか利用できなかったメールがインターネットからの運用を実現した。

D. 考察

山口県医療情報ネットワーク（やまめネット）のWebアプリケーションの中からセキュリティー保護を必要としないものについては、診療所からの利用促進を図るために、トライアルとしてインターネットからの利用を可能した。認証局の実用化で、イントラネットで閉じていたWebアプリケーションがインターネット経由で利用可能になった。このことは、利用対象が一部の病院・診療所だけでなく、広範な診療所の医療連携の支援が可能となった。

これらの運用を通じて、地域遠隔医療ネットワークが、イントラネットワークで閉じているといった基本的な考え方の変更が検討できるようになった。例えば、電子メールやWebアプリケーションの利用においては、インターネットからの利用に供することができる可能性がある。これまでのイントラネットはより専門性に特化した医療用セキュリティネットワークとして扱うことが可能になる。例えば、PET検査を専門にする医療機関への検査オーダーの送信、検査報告書と診断画像の受信および全ての原画像のファイル転送、また、がん診療連携のためのバーチャルスライドカンファレンス、DICOMサーバを使った放射線画像診断コンサルテーションなどがある。

E. まとめ

PKIの利用範囲を、山口県医療情報ネットワークに登録された利用者に限定することで、比較的容易に利用可能なプライベート認証局が構築できた。また、この認証局を用いることで、イントラネットで限定されたアプリケーションの一部が、インタネットから利用できる可能性が見えてきており、より広範な医療連携が実現できる可能性がある。さらには、これまで利用してきたイントラネットはより専門的な利用に特化させる可能性が見えてきた。

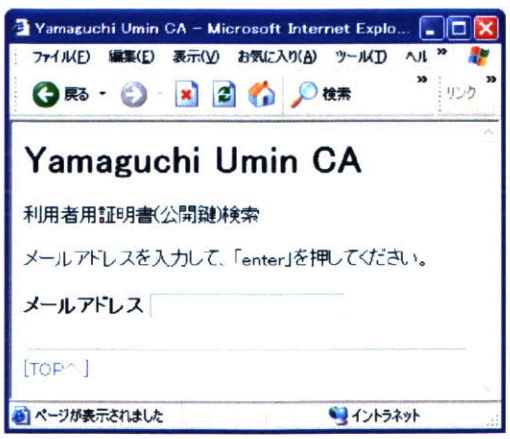


図５　利用者証明書の取得

PKIの利用することで、利用における閾値を下げることができ、全国で本格的なPKI活用への流れができると可能性が見えてきた。

F. 健康危険情報

なし

G. 研究発表

１．論文発表

1) Haku Ishida, Yuji Inoue, John B Wong, Kiwamu Okita : Cost-effectiveness of ribavirin plus interferon alpha-2b for either interferon relapsers or non-responders in Chronic Hepatitis C :A Japanese trial. Hepatology Research 28(3) : 125-136, 2004.

2) 奥田　昌之、久長　穣、小早川　節、国次　一郎、杉山　真一、石田　博、芳原　達也、井上　裕二　：　地域における医療・福祉情報共有システムの継続運用実現のための質的研究．医療情報学 24(1) ：177-185, 2004.

3) 石田　博、北村　聖、三宅　一徳、西堀　眞弘、松野　容子、井上　裕二　：　診断検査についてのEvidenceの収集を目指したWebベースシステムの構築．医療情報学 24(1) ：98-97, 2004.

4) 藤澤　博亮、野村　貞宏、梶原　浩司、加藤　洋一、藤井　正美、石田　博、井上　裕二、松永　尚文、真田　泰三、岡部　英洋、八木　英俊、原田　正治、鈴木　倫保　：　医療用業務サーバーからの全自動取り込みによる画像ライブラリ作成．EUROLOGICAL　SURGERY 33(9) ：932-937, 2005.

6) 井上　裕二、原田　正治、久長　穣、石田　博　：　集学医療システム：臨床研究、医療評価、教育活動のための診療情報の二次利用環境の再構築．医療情報学 25(Suppl) ：483-485, 2005.

7) 荒木　栄一、石田　博、高木　俊和、竹原　文子、正木　克典 原田　正治 井上　裕二　：　臨床研究支援システム：多施設共同研究を可能とす臨床研究プラットフォームの構築．医療情報学 25(Suppl) ：894-895, 2005.

8) 石田　博、井上　裕二　：　地域医療連携を図るためのシステム展開．日本臨床検査自動化学会会誌 30(2) ：119-123, 2005.

9) 石田博、井上裕二：大学病院が支援する地域医療連携。やまぐちトライアルをとおしてみる情報化の実際。臨床病理 54(9)：980-986, 2006

10) 石田博、井上裕二：アウトカム研究（医学判断学）を支援する病院情報システムのありかたについて。医療情報学　26(suppl)：10-11, 2006

11) 久長穣、杉井学、長篤志、三池秀敏：大学における迷惑メール対応のあり方～利用者毎のオンデマンド対策の効果～　学術情報処理研究 No. 11 pp. 5-13 2007

２．学会発表
なし

H. 知的財産権の出願・登録状況
なし

厚生労働科学研究費補助金(医療技術評価総合研究事業)

分担研究終了報告書

糖尿病疾病管理研究事業カルナにおける運用実験

研究分担者　中島　直樹　九州大学病院医療情報部講師
研究協力者　安徳　恭彰　九州大学病院医療情報部技官

研究要旨

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。

A．研究目的

我々が行っている糖尿病疾病管理研究事業では、多種のコミュニケーション方法を用いた情報流通が発生する。そのネットワーク上では、やはり多種の機微な個人情報を取り扱う。コミュニケーション方法を選定した上で、認証が強化された医療 VPN 上で PKI による認証・暗号化を用いて情報流通を行う可能性と意義について検討する。

B．研究方法

B－1　研究フィールド

九州大学では、九州電力グループとともに平成 16 年度より糖尿病疾病管理研究事業「カルナ」を行ってきた。平成 17・18 年度には、経済産業省公募事業「（健康）サービス産業創出支援事業」として採択され、クリティカルパスなどのアルゴリズム開発や IT 開発などの事業基盤整備を行った。また、平成 18 年度からは、特定領域研究「情報爆発」の福岡実験フィールドとして心拍計や運動量センサなどを用いたセンサネットワークの構築をすすめている（平成 22 年度までを予定）。平成 19 年度からは特定健診制度の実証実験を糖尿病 1 次予防プログラムと認識して行い、平成 20 年度からの制度実施に備えているところである。「カルナ」の研究フィールドにおいては、糖尿病 1 －3 次予防をシームレスに行うために、様々なアクター間（患者、かかりつけ医、専門者、保険者、保健指導者、カルナ事務局など）において、Web やメールを用いて、保険者・被保険者情報、診療録情報やレセプト情報、保健指導情報、センサ情報など、多種多様な個人情報の受け渡しを行っている。これを本研究の検討対象とした。

B－2　システム導入

・医療 VPN

福岡県医師会から文書で正式にカルナ研究事業への協力承認を得た。九州大学病院地区に設置したコールセンター機能を有するカルナ事務局とかかりつけ医の一つとして福岡市医師会成人病センタの間で医療VPNを設定した。

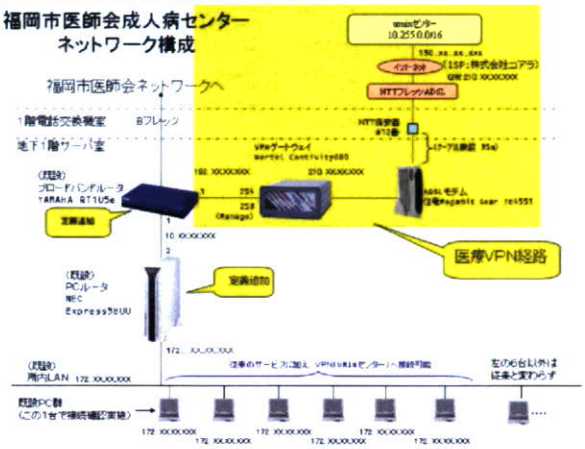


図１　福岡市医師会成人病センタへ導入した医療VPN構成図

・PKIの構築

CAサーバとして、DELL Power Edge680(Intel Xeonプロセッサー3040)を用意し、CentOS4.4 (kernel 2.6.9-42.0.10.Elsmp)を導入した。本サーバ上に Apache_2.0.52,mod_ssl,Perl5.8.5,openssl0.9.7dをインストールし、OpenCA-0.9.2.5を認証局として構築した。

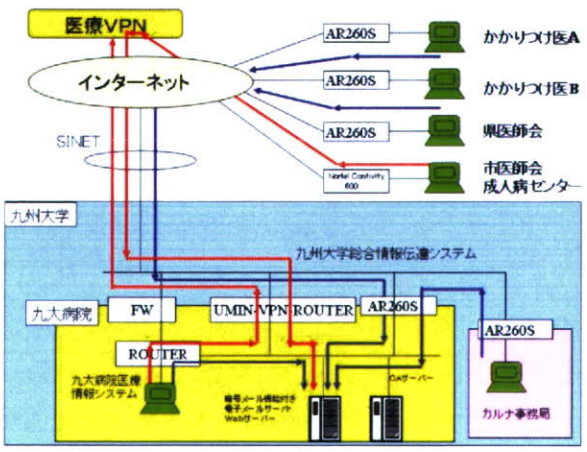


図２　医療VPNとPKIのハイブリッド・セキュリテ

ィシステム。赤線が医療VPN経由によるメール伝送。青線がインターネット経由（オンデマンドVPN）を用いたメール伝送。

C．実験および検討結果

C－1　通信結果

動作確認として、以下の３つの環境で暗号化されたメールの送受信テストを行った。

1）　WindowsXP SP2 + Microsoft Outlook 6

2）　MacOS X 10.5 + Thunderbird 2

3）　MacOS X 10.5 + Eudora 6.2

１、２の環境において適切に暗号化を行った結果、正しくメールの送受信が行えることを確認した。また、暗号キーを外せば、メールの本文自体の復号化が解かれ、判読できないことも確認した。１から１、２から２、１から２、２から１いずれの送信でも問題なく暗号化、復号化を行うことが可能であった。しかしながら、３の環境においては、メールソフト自体が暗号化に対応しておらず、暗号化されたメールを受信しても復号化できないことを確認した。

C－2　想定されるコミュニケーション

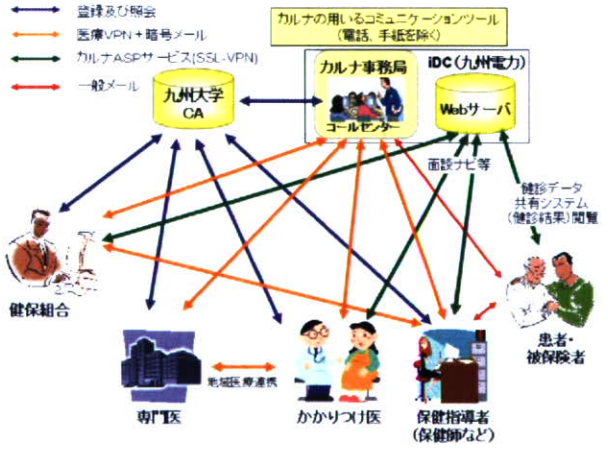


図３　カルナで想定される情報流通。ASPで提供されるアプリケーション群（緑色）、メール（赤および橙色）が考えられる。

D．考察

図３に示すように、メールもカルナ事務局を中心とした単中心型ではなく、多中心型に流通する。ASPにはSSL-VPNを用いれば良いが、施設間同士では、医療VPNの設置が可能である。課題は、患者との連携であり、個人情報は当然含まれているが、現状では暗号メールを用いないことが多い（図３の「一般メール」）。これに対しては、PKIによる認証・暗号化を用いることにより、最低限度の暗号化が担保される。しかしながら、各利用者のITリテラシは高いとは言えず、医療VPNやPKIの簡便なインストール方法の開発が不可欠である。また、一部のメールソフトでは対応不可であると判明した。

離れた地域間の情報連携も医療VPNおよび認証局連携により同じセキュリティレベで可能となる（図４）。

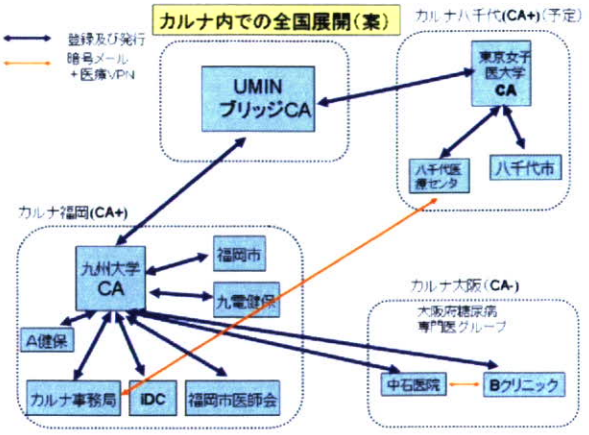


図４．医療VPNおよびブリッジCA(UMINあるいはHPKI-CA)を用いた全国展開。

E．結論

疾病管理事業におけるネットワークにおいても医療VPNとPKIのハイブリッドあるいは単独での使用により安価に、かつ効果的にセキュリティを向上させうる。

F．研究結果

・関連する論文発表

中島直樹：地域連携クリニカルパスを用いた糖尿病．日本クリニカルパス学会雑誌9:629-636，2007

中島直樹、小林邦久、井口登興志、他：特定健康診査/保健指導制度時代に対応する日本型Disease Management事業の開発．医療情報学会雑誌　27：47-55，2007

中島直樹：特定健診制度時代における糖尿病医療専門スタッフの役割とICTシステムの動向．第27回医療情報学連合大会論文集　46-51，2007

Nakashima N, Kobayashi K, Inoguchi T, et al.: Japanese Model of Disease. Management Medinfo 2007 Part2 1174-1178, 2007

Nakashima N, Shimizu S, Okamura K, et al.: Development of a Broadband Telemedical Network Based on Internet Protocol in the Asia-Pacific Region. Method in Information of Medicine　46: 709-715, 2007

Shimizu S, Nakashima N, Okamura K, et al.: Telesurgery system with original-quality moving images over high-speed internet: Expansion within the Asia-Pacific region. Journal of Laparoendoscopic & Advanced Surgical Techniques 17: 674-678, 2007

中島直樹、小林邦久、井口登興志、他：糖尿病のディジーズ・マネジメント ―カルナプロジェクト―Diabetes Journal

35: 161-165, 2008

G．知的財産権の出願・登録状況

1. 特許取得：なし

2. 実用新案登録：なし

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

熊本大学医学部附属病院における運用実験

分担研究者　末永貴俊　名古屋工業大学　プロジェクト研究員・プロジェクト助教

研究要旨　本研究では、病院内で用いられている様々な機器間で安全に医療情報を交換する手段として、一般に広く普及しているメールプロトコルを用いた情報交換基盤を提案する。提案手法では、階層化した暗号化処理を行うことで、異なる特性・仕様を備えたシステム・機器にも柔軟に対応可能な構造を備えている。また、ユーザは直接暗号化処理を意識する必要が無いため、ユーザの利便性を大きく損なわずに安全な情報交換基盤を構築・提供することが可能となる。提案手法の有効性を確認するため、本手法を用いた試作システムを構築し、検証を行った。

A.　はじめに

元来、医療情報は厳重に管理すべきものであり、医療従事者は守秘義務により患者の個人情報を保護する必要がある。近年のネットワーク普及に伴って病院情報システムが発展するとともに、病院や診療所、検診センターなどの情報交換にもネットワークを利用する機会が増えているため、情報漏洩防止や不正アクセス防止に努める必要がある。

すでにセキュリティ対策を施すためのネットワーク技術やアプライアンス製品が登場しているため、実現するセキュリティレベルに応じて容易に対策を行うことが可能となった。本研究班においても、VPN装置を介して大学病院を接続し、安全に医療情報を交換するとともに、我が国の医療水準の向上に貢献可能なコミュニケーション環境を構築・運用する研究を行ってきた。しかしながら、既存の製品群は一般企業等を対象としたシステムが多いため、大学病院と周辺地域での医療連携に適用する際には、より細かい部分まで配慮したセキュリティ対策を行う必要があると考える。大学病院同士を接続するだけであれば、おもに統一的な情報を交換するために一般企業と同様に施設間をVPN接続することで安全に情報交換を行うことが可能となる。しかし、将来的に大学病院が各々の地域で地域連携を開始する際には、各連携先に応じて不要な情報が流れないように十分配慮する必要がある。この状況に対応するためには、各大学病院が、各々の連携状況に応じて柔軟に対策する必要がある。

具体的な例として、熊本大学病院では病院情報システムをはじめとする様々な部門システムが複数のネットワーク（医療系・放射線画像系・研究系・事務系）上で連携し、業務を行っている。しかし、従来、医療情報システムはクローズドネットワークを前提として開発されていることが多く、暗号化などを施さずにデータやアカウント情報を通信したり、通信方式が独自方式であることも少なくない。そのため、地域がん登録事業をはじめとする医療連携などで外部機関と情報交換を行う必要がある場合には、通信内容の暗号化を施すだけではなく、拠点間および院内の各部門システム間で不要な情報が流通しないように適切に経路制御を行い、その上で暗号化通信などの対策を施す必要がある。

近年、ヘルスケア事業などで健康機器からのデータを家庭から収集するような試みも行われているが[1-2]、今後は一般家庭と医療機関との連携も考慮したセキュリティ対策を施す必要があると考える[3]。

B.　従来手法

従来、安全な情報交換を行うための手段としては、SSLによる暗号化通信やS/MIMEによるメールの暗号化と、公開鍵暗号基盤(PKI)を用いた暗号化通信・クライアント認証などが用いられている[4]。しかし、病院の規模によっては情報部門が無い場合もあるため、部門システム毎・診療科毎などの細かい管理を行うことを想定した場合には、ユーザ・システムごとの電子証明書や公開鍵・秘密鍵を管理することは煩雑であり、運用時の負担が大きい。また、訪問診療や施設間の医療従事者の交流を想定した場合には、移動に伴ってコンピュータの故障・盗難などで電子証明書・秘密鍵を紛失・失効してしまうと、クライアント認証が不能になるだけでなく、それまで蓄積してきたデータの復旧作業が非常に困難になる場合もあり、ユーザ側の管理責任・負担が大きくなる。一般的に、システムの導入作業と通常運用業務の煩雑さはシステムの普及を妨げる大きな要因になるため、医療情報の電子保存を実現するうえで大きな障害となってしまう可能性がある。

C. 提案手法

この問題を解決する手段として、本研究では各システムで独自の暗号化処理などを実装するのではなく、異種システム間に介在することで各システムの機能を補助し、安全な情報交換を実現する仕組みを提案する(図1)。本報告ではメールプロトコルと共通鍵暗号方式と公開鍵暗号方式を組み合わせることで運用の手間を軽減しつつ、安全に医療情報交換を行う手法を提案する。

本研究で提案する情報交換基盤は、様々なシステム・環境に対応するため、機能ごとに分割した階層構造を持たせている。次に各部について説明する。

C.1. 暗号化基盤

暗号化通信やクライアント認証などで用いる電子証明書を管理・運用するための認証サーバである。認証サーバはOpenCA[4]とOpenMicroServer[5]を用いて構築した。OpenCAは一般に広く用いられているオープンソースのソフトウェアであり、OpenCAで構築された他機関のサーバとも容易に連携することができ、運用に関する様々な情報をインターネット上から入手することが可能である。OpenMicroServerはファンやハードディスクなどの機械部品を使わずに構成することで高耐久性を実現した小型サーバである。一般のPCサーバと比べて処理性能は劣るものの、一度環境を構築すれば、ほとんどメンテナンスフリーで維持・運用を行うことができる。認証サーバはセキュアな情報基盤を運用する上で要になる重要な機器であり、最優先で機能を維持する必要がある。通常、医療機関に情報系技術者を常駐させることは困難な場合も多いが、OpenCAとOpenMicro Serverを組み合わせることで、導入・維持コストなどを軽減しつつ、信頼性の高いサーバを運用することが可能となる。

C.2. 情報交換基盤

情報交換基盤の概要を図2に示す。本研究ではメールサーバを中心とした情報交換基盤を提案する。この基盤は異種システム間の差異を吸収するため、３つの階層を持った構造となっている。連携するシステムの機能に応じて接続方法を選択し、データやプロトコルの変換を行った後に、メールサーバを介した安全な情報交換を実現する仕組みを提供する。ここでは、データの暗号化・復号処理は共通鍵暗号を用いて各システムで行い、データの交換は暗号化通信を用いたメールプロトコルで行う。

次に、各階層の詳細について説明する。

C.2.1. インタフェース層

メールサーバへ送信するデータを共通鍵暗号で暗号化し、各システム間での暗号化通信の準備を行う。健康機器や検査装置など、独自に暗号化処理の実装が困難な場合は、Crypt Gatewayを介して暗号化処理を行う。メールサーバから受信するデータについても、送信するときと同様に共通鍵を用いて復号する。

ユーザが情報を閲覧する場合には、webメールインタフェースを介して情報の送信・閲覧を行うことになるが、暗号化通信だけでなく、電子証明書を用いたクライアント認証も行う。データの暗号化は後述のプロトコル変換層が担当するため、ユーザが意識することは無い。

C.2.2. プロトコル変換層

インタフェース層とメールサーバを接続し、暗号化通信によるデータの送受信を行う。各システムが利用する通信プロトコルの差異を吸収するため、メールプロトコルを用いた円滑な情報交換を行う仕組みを提供する。本階層に位置するメールサーバはSMTPとPOP3の両機能を持ち、平文のデータを暗号化する機能も併せ持つ。将来的には、各階層の負荷分散を行うことも想定して、両者をSSL通信を併用したプロトコルに移行する予定である。

ユーザが利用するwebメールシステム本体もこの階層に位置する。この場合、データの暗号化・復号はwebサーバとメールサーバの中間に位置するCrypt moduleで行う。Crypt moduleでは、Blowfish[6]を用いた暗号化・復号化処理を採用している。BlowfishはOpenSSH[7]などにも含まれる方式で、計算コストが低いことから、処理能力が低い機器に実装することも比較的容易である。

C.2.3. データベース層

全てのデータは暗号化され、メッセージとしてMailboxに蓄積する。一般的なデータベースサーバと異なり、メールサーバを利用してメッセージ管理を行うが、メールサーバは時系列にメッセージを一元管理できるため、データベースサーバとして検索等の操作が可能である。データの暗号化には共通鍵暗号方式を用いており、共通鍵は本システム内でのみ管理・利用する。そのため、システム障害などにより暗号鍵の変更が必要になった場合には、本階層内で新たな共通鍵を用いた再暗号化処理を行うことも可能である。

D. 結果

提案システムの機能を確認するため、次の2点について検証を行った。

・webメールを用いたメッセージ交換

・電子証明書・電子鍵失効時のデータ復旧作業

これまで、ユーザ側で行ってきたメールの暗

号化処理などをシステム側で担当するため、システム構築に関する作業時間は通常のメールサーバ・webサーバの構築よりも長時間を要した。試作システムでは、ユーザはwebブラウザを用いてメールの送受信を行う。この場合、ユーザが意識することなく、メッセージを暗号化してメール送信する環境を構築することができた(図３)。メールは一般的なメーラでも取り込むことは可能であるが、暗号化メッセージの復号機能を持たないため、内容を解読することができないことを確認した(図４)。

提案システムでは、図５に示すように2段階の暗号化方式を採用している。ユーザは初めにブラウザを用いてクライアント認証を行い、サーバへアクセスする。ユーザ側ではクライアント認証用の電子証明書の管理が必要となるが、あらかじめ電子証明書を組み込んだブラウザを用意することにより、特別なインストール作業などを行わせずに提案システムを利用可能な環境構築を行うことができた。また、データ自体の暗号化はサーバ内でのみ、共通鍵を用いて行っているため、ユーザのクライアント認証用の電子証明書が失効したり、PCを紛失したりしても、サーバへの接続が不能になるだけで、データ自体は復号可能な状態で保持できるトラブル発生時の影響範囲を最小限に抑えることが可能となり、データの復旧も容易な環境を構築できたといえる。

E. 議論

本稿では、メールプロトコルと階層的な暗号化処理を用いた安全な医療情報交換インフラの提案と、運用方法の検討を行った。

メールプロトコルは長年世界中で用いられ、様々な情報システムでもメッセージ配信等に利用されている。また、データの暗号化についても、OpenSSLライブラリなどを用いれば暗号化強度の高い処理を容易に実装することができる。したがって、現在独自の通信方式で暗号化処理を行わずに通信している既存システムでも、提案システムと同様の通信方式への移行を比較的容易に進めることが可能であると考える。

また、暗号化通信とデータ暗号化処理を分離したため、メールサーバに蓄積された医療情報への通信処理は一見複雑な構造を持つようにも見える。しかし、ユーザや連携システム側での障害により電子証明書の紛失・盗難等が発生した場合のリスクを考慮すると、一般的に行われているS/MIMEのみの公開鍵暗号方式だけを用いる場合に比べ、より柔軟で強固なセキュリティをユーザへ提供するだけでなく、データの復旧に関する手間暇を大きく軽減することが可能になると考える。

最近では、ネットワークインタフェースを持つ小型デバイスが製品化されており（図６）、提案システムで用いているBlowfishの実装も容易であると考える。このようなデバイスを小型暗号化アプライアンスとして利用すれば、病院内で使用される計測機器類なども提案基盤に参加することができ、医療情報を扱うあらゆる場面においてセキュリティを確保することが可能になると考える。

参考文献

[1] IEEE eHealth.com: http://www.ehealthcom.org/
[2] uHealth.com: http://www.ehealthcom.org/uhealth.htm
[3] 厚生労働省, 「医療情報システムの安全管理に関するガイドライン　第2版」: http://www.mhlw.go.jp/shingi/2007/03/s0301-12.html
[4] OpenCA. : http://www.openca.org
[5] OpenMicroServer. : http://www.plathome.co.jp/products/microserver/
[6] Blowfish:
[7] OpenSSL: The Open Source toolkit for SSL/TLS. : http://www.openssl.org

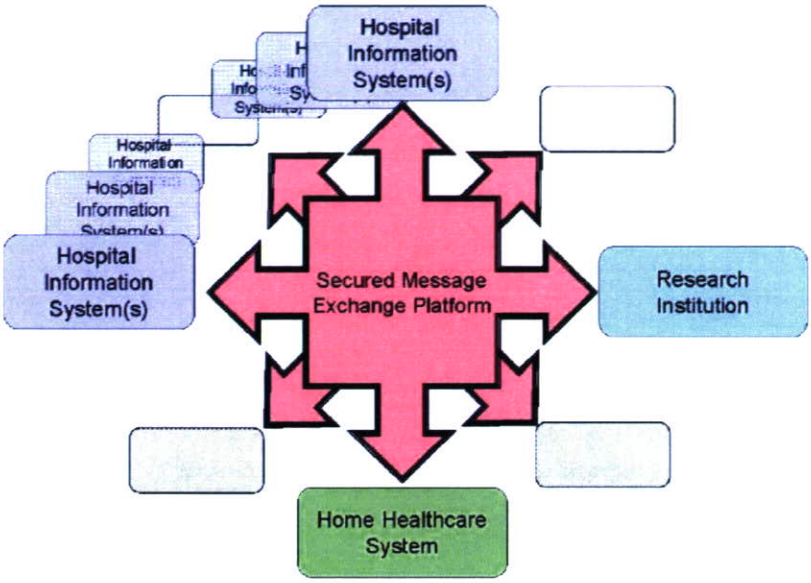


図１：Secured Message Exchange Overview

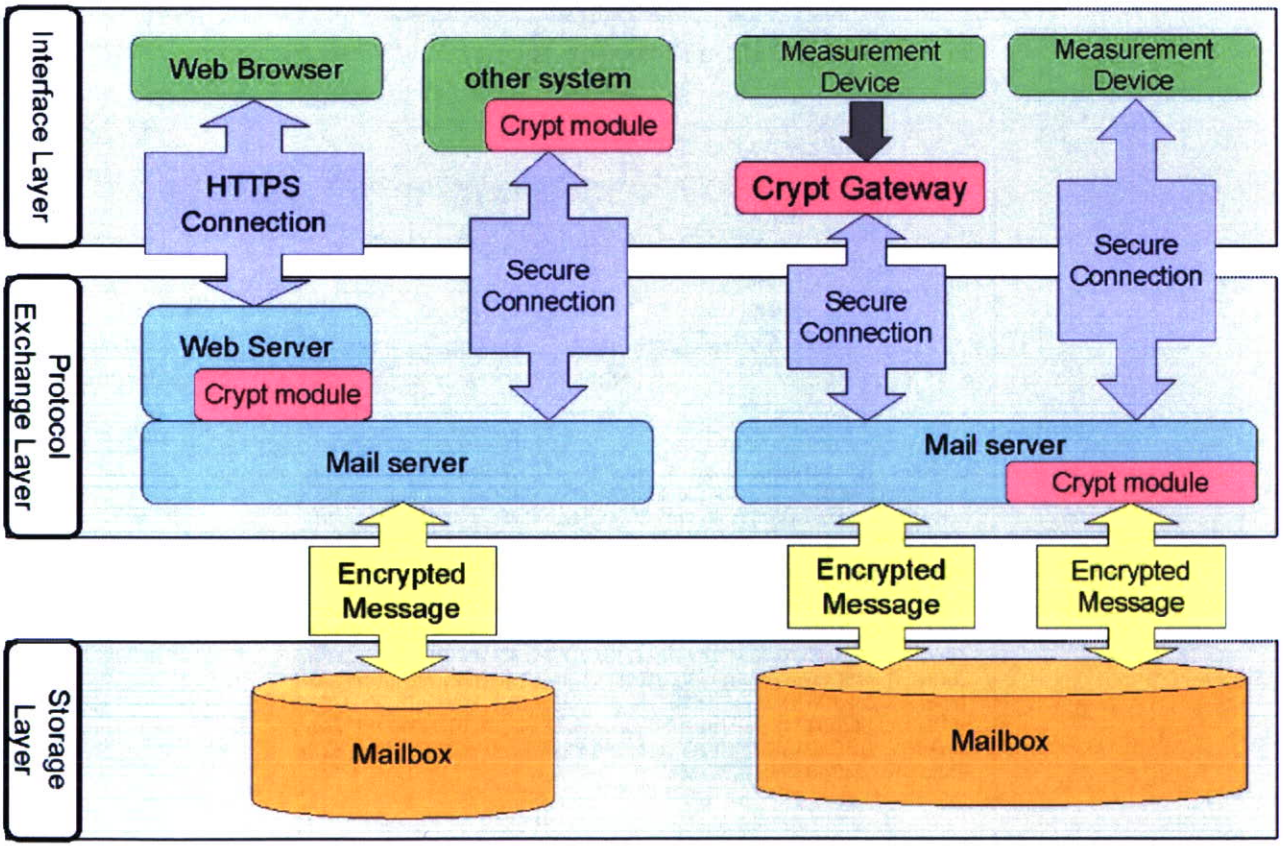


図２：Layered Architecture Overview