ので、これが今後の課題となった。

ファイヤーウォールが入っていると、繋がらない場合があった。しかし、多くの施設ではＷｅｂの閲覧が自由にできる場合がほとんどであるので、ポートを８０番に設定したり、接続に失敗した場合でも幾つかのポートをスキャンして、変更するようにすると接続できるようになった。

E　結論

非常に簡便に安全なネットワーク構築が可能になった。また、P2Pでなく、複数の施設の接続も可能になり、利用の幅が広がった。今後、ＶＧＮの医療応用をさらに深く検討するためには、全国規模のネットワーク構築の実験と、IPv6を活かした医療アプリケーションの開発が望まれる。

研究発表

(1) 論文発表

1. 戸倉　一，明石浩史，大西浩文，　西城一翼，山口徳蔵，新見隆彦，木村眞司，西陰研治，今井浩三，辰巳治之　　NORTH 活動報告　ホームヘルスケアのための高性能健康測定機器開発＆戦略的情報通信研究開発推進制度（SCOPE）．Proceedings of NORTH Internet Symposium 2006, Vol. 12, 12-13
2. 戸倉　一，明石浩史，藤川　賢，中村正弘，石田　朗，新見隆彦，辰巳治之，田中　博．ユビキタス医療実現のためのインフラ技術の開発．第 2 回ユビキタス医療シンポジウム p67 (2006.9)
3. 戸倉　一，明石浩史，新見隆彦，榊　房子，石田　朗，西城一翼，山口徳蔵，西陰研治，松本　尚，辰巳治之．次世代オペレーティングシステム SSS-PC による三次元再構築システムの開発．医療情報学 26 (Suppl.) : 206-207, 2006
4. 石田　朗，明石浩史，戸倉　一，新見隆彦，辰巳治之．「情報薬」の開発：ヘルスケア・システムの統合化の可能性と諸問題．医療情報．26(Suppl.) : 299-300,2006
5. 5．戸倉　一，明石浩史，藤川賢二，中村正弘，石田　朗，新見隆彦，辰巳治之，　田中　博．情報薬開発基盤としてのネットワークインフラの開発．医療情報学．26 (Suppl.) :106-107,2006
6. 6．石田　朗，明石浩史，戸倉　一，新見隆彦，榊　房子，中村正弘，辰巳治之　情報薬作成のためのサーバの統合．医療情報学 26(Suppl.):108-109,2006
7. 戸倉　一、石田　朗、明石浩史、新見隆彦、大石憲且、藤川賢治、馬場　聡、中山正志、林　祥介、高井昌彰、辰巳治之．NORTH 活動報告　地域及び医療ネットワークの問題解決型のために．Proceedings of NORTH Internet Symposium 2007,Vol.13 : 8-16 (2007) ISSN1345-0247
8. 石田　朗、明石浩史、戸倉　一、新見隆彦、辰巳治之．ネットワークを活用したヘルスケアシステムの統合化．Proceedings of NORTH Internet Symposium 2007, Vol.13:36-39(2007) ISSN1345-0247
9. 辰巳治之、新見隆彦、中村正弘、高橋正昇、明石浩史、戸倉　一、石田　朗、榊　房子、大石憲且、村井　純、南　政樹、三谷博明、木内貴弘、田中　博．医療系の利用を目指した日米通信実験 - Virtual Global Network の可能性．Proceedings of NORTH Internet Symposium2007, Vol.13:101-115(2007) ISSN1345-0247

（2）その他:講演など

1. 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．辰巳治之．2006年２月３日　感性工学会　in 北海道大学：パネルディスカッション「北海道感性産

業開発のアプローチ」

2. 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. 辰巳治之. H18年3月11日 山形県臨床整形外科医会春季総会
3. A challenge to three-dimensional reconstruction system development. H. Tatsumi, T. Shimmi, M. Nakamura, T. Ninomiya, R. Ichikawa, S. Kikuchi, H. Akashi, H. Tokura, E. Takaoki, T. Matsumoto. 2006/3/21 第１４１回日本獣医解剖学会・シンポジウム　つくば国際会議場
4. SSS-PCの形態学研究への応用
その２．辰巳治之、新見隆彦、中村正弘、市川量一、二宮孝文、菊池　真、明石浩史、大西浩文、戸倉一、松本尚. 日本解剖学会 北里大学　2006/3/31
5. ホームヘルスケアfシステムを用いたIT健康術：戦略的防衛医療構想の第一歩. 辰巳治之. H18年4月9日　二子玉川高島屋アレーナホール. NPOナチュラビオティック推進協議会
6. 「ＩＴ新改革戦略と医療改革」ネットワーク利活用で医療が変わる. 辰巳治之. 平成１８年５月１７日 JGNIIシンポジウム. ｅーとぴあ・かがわ
7. ITを用いた戦略的防衛医療構想の実現
情報薬の開発とその応用：「ゼロクリック」と「どこでも逆ナースコール」. 辰巳治之.　H18年5月30日帝国ホテル. 国際システム健康科学学会
8. センサーネットワークへの期待
戦略的防衛医療構想のための情報薬の開発:「ゼロクリック」と「どこでも逆ナースコール」 辰巳治之. H18年6月1日 秋葉原コンベンションホール. LonUsers' Japan 2006
9. 情報薬の開発とその処方：戦略的防衛医療構想実現に向けて. 辰巳治之. PML研究会　第14回定例会　2006年7月12日 恵比寿
10. NORTHの歩みとICTフル利活用による健康サービスの可能性. 辰巳治之. NORTH 総会記念フォーラム. 2006年7月19日
11. 周産期医療システムの現状と課題「産科の在宅モニターシステム」. 辰巳治之. 第四回北海道周産期談話会 2006年7月22日（土曜）　札幌医科大学　臨床講堂
12. ヘルス・サービス・プロバイダーとしての究極のサービス. 辰巳治之. Netone Service Provider セミナー. 2006年9月8日 貿易センタービル
13. 高性能健康測定機器群とホームヘルスケア支援システムの開発
フィールドテストの成果について. 辰巳治之.　第四回生活支援工学系学会連合大会. 第22回ライフサポート学会大会・第6回生活支援工学会大会. 2006年9月11日. 東京理科大学　野田キャンパス
14. ホームケアへのユビキタス技術の応用戦略的防衛医療構想実現に向けて:ユビキタス技術と情報薬の医療応用. 辰巳治之. 第2回ユビキタス医療シンポジウム 2006年9月12日 学術総合センター（一橋記念講堂），東京
15. 感性工学から感性産業へ:ITによる生活習慣病克服への挑戦. 辰巳治之. 2006年10月24日　札幌市立大学サテライト開設記念：産学連携推進事業.「北海道感性産業開発ネットワーク」 キックオフ・シンポジウム
16. IT新改革戦略における遠隔医療と電子カルテネットワークの現状と将来展望. 辰巳治之. 2006年10月25日　九州テクノフェア & 北九州医療IT研究：ワークショップ2 & 日本遠隔医療学会によるセミナー
17. 戦略的防衛医療構想実現に向けて:「情報薬」開発の基礎研究から応用まで. 辰巳

治之. 第26回医療情報学連合大会　2006年11月3日. 札幌コンベンションセンター

18. IT医療の未来と課題. 辰巳治之. H18年11月22日　「JIMAインターネット医療フォーラム2006」東京・国立成育医療センター
19. JGNⅡの現状と医学系応用:戦略的防衛医療構想実現に向けて. 辰巳治之. JGNII 活用プロジェクトX（札幌医科大学）& JGNIIアクセスポイント移設記念（香川大学）, 2006年11月27日
20. 健康モニタリングネットワーク実証実験:生活習慣病克服の為の情報薬開発と処方による超予防医学. 辰巳治之. 計測自動制御学会　システムインテグレーションフォーラム/市民公開講座　2006年12月16. 「生活習慣病予防に役立つ計測・情報処理技術」. 札幌コンベンションセンター.
21. 医療情報ネットワーク相互接続分科会（JAMINA）活動報告. 辰巳治之. 2007年1月16日　ITRC総会: シンポジウム in 広島.
22. ヘルス・サービス・プロバイダーとしての究極のサービス:戦略的防衛医療構想実現に向けて. 辰巳治之. Netone Service Provider セミナー. 2007年1月26日.　旭川天人閣.
23. 道内における医療、健康ビジネスの展開状況、動向. ICTを活用した医療・健康セミナー：戦略的防衛医療構想のバックグランドとその応用. 辰巳治之.　2007年3月1日岩見沢市雇用対策協議会.
24. 医療系の利用を目指した日米通信実験. 辰巳治之. 第１３回 NORTH Internet Symposium 2007. 2007/3/7 札幌
25. Strategic Defensive Medical-Care Initiative with Advanced IT Utilization. H. Tatsumi. Ubiquitous Medical IT Seminar. 8 March 2007. Tokyo
26. 戦略的防衛医療構想:情報薬の開発とその処方. 辰巳治之. 2007年3月8日 無名会3月例会.　札幌グランドホテル.
27. 医療分野への利活用を交えたネットワーク技術. 辰巳治之. 2007/3/14　ICTネットワークセミナー: e-とぴあ・かがわ BB

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CAの構築と運用

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と接続された三重遠隔画像診断ネットワーク内において、プライベートCA（認証局）を構築し、電子メールの暗号化および読影依頼書、読影レポートの暗号化通信と読影レポートへの電子署名を行った。これにより各医療機関との情報交換において、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真正性確保ができた。このような医療情報の機密性・正当性・真正性を保証しながら、地域医療情報の共有化と安全なアクセスの提供を図ることで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討を行った。

A．研究目的

医療VPNと接続された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三重遠隔画像診断ネットワーク上に地域医療専用プライベート認証局（CA）を構築し、電子メールの暗号化を行うととも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時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の１４病院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。各病院の通信回線はインターネットを使用しないクローズドネットワークであるフレッツグループ回線を利用している。読影依頼については依頼病院からFAXまたは専用Webページを利用するために、FAXサーバおよびWWW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、専用Webページを使用している（図１）。

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いる。また、業務連絡や医療情報共有のため、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。

地域医療専用の認証局として、LinuxをOSとしオープンソースであるOpenCAソフトウェアを使用してプライベート認証局（CA）を構築した。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。この認証局はプライベート設置であり、アクセスするクライアント側に何も設定をしなければ、証明書が無効であるとメッセージが表示される。この場合でも暗号化などについては有効に機能するが、アクセスするたびに警告メッセージが表示されないように認証局が発行する証明書を地域医療機関で利用する端末にインストールを行った。

この認証局で認証を行い、読影レポートを作成する医師個人の電子署名により、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を行った。また、電子メールはS/MIMEによる暗号化及び電子署名を使用し、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、認証局によるデジタルIDの発行は最初の本人確認を確実にするために文書で登録受付を行い、それを認証局に登録することにより、webでのオンライン発行をした。

C．研究結果及び考察

本研究で構築した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。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、情報漏洩に対しても有効であった。暗号化したメールの送受信だけであれば、WebメールとSSLによる通信で自己署名により認証局を利用しなくても可能であるが、メールの内容が改ざんされていないか、また、送信したのが本人であるかどうかの検証には本研究のような認証局を利用した認証が必要である。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た。

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。

病院内で発生するデータには1)院内だけで扱う患者情報、2)地域医療ネットワーク内の利用者で共有する医療情報、3)インターネットなどで地域住民をはじめとする広く一般に開示する情報などの区別が考えられるが、認証サーバと認証局により、これらの情報の種類に応じて、本人認証を行い特定の情報参照や電子署名による情報の真正性を保障することが可能であると考える。

本研究のようなプライベート認証局の設置自体は比較的簡単に行えるが、重要なのは認証局の管理であり、認証局が何らかのトラブルで停止した場合は、何も証明できなくなってしまう。また、セキュリティ管理、バックアップ機器、認証局の秘密鍵の管理、利用者の秘密鍵紛失に対する対策のためには秘密鍵の保管等が必要となる。また、ネットワークによる通信のセキュリティの確保は現実に可能であるが、それ以外の人的なものも含めて、総合的な地域医療ネットワークの情報セキュリティポリシーの策定が必要になると考える。なお、本研究では認証は限られた利用者、端末によるものであり、第３者による不特定多数のための認証ではないためプライベートな（専用的な）認証局が適していると考えるが、管理コストとの兼ね合いで、第３者による認証かもしくはプライベート認証局のアウトソーシングのほうがよい場合があると思われる。

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。今後は複数の地域で多数の人が電子署名、暗号化通信のため利用する場合は、オーソライズされた医療専用の認証局、あるいは他の認証局との相互認証が必要になるであろうと考える。また、電子カルテなど医療文書は長期保存する必要があるが、電子署名の証明書は有効期限が２年間ほどであり、正しく署名されていても、有効期限が切れたり、失効したりした証明書では、その時点で有効性を証明できない。しかし、医療情報は時間が経過し、証明書が失効していても作成時点の日時と作成者が正しく、内容も改ざんされていないということがわかればよく、作成時点で有効であると証明できるような機能が必要となり、今後はこのような電子署名の長期保存に対する署名有効性の検証が必要であると考える。

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，佐久間肇，永岡宏朋，山本晧二、セキュリティの確保された地域医療情報ネットワーク上に構築した画像検査予約システム、医療情報学23回連合大会論文集 Page700-701(2003.

11)
３．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)
４．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

１）高田孝広、佐久間肇、小林茂樹、竹田寛、山本晧二、大学とNPOによる遠隔画像ネットワークの構築と管理の実際、Rad Fan、５巻１号　Page20-22(2007.01)
２）高田孝広、小林茂樹、永澤直樹、山本晧二、安価な導入と運営を実現した遠隔画像診断ネットワーク、第34回日本放射線技術学会秋季学術大会
３）高田孝広、シンポジウム「遠隔画像診断の現状と課題」大学とNPOによる遠隔画像ネットワークの構築と管理の実際、第43回医学放射線学会秋季臨床大会

G．知的財産権の出願・登録状況

なし

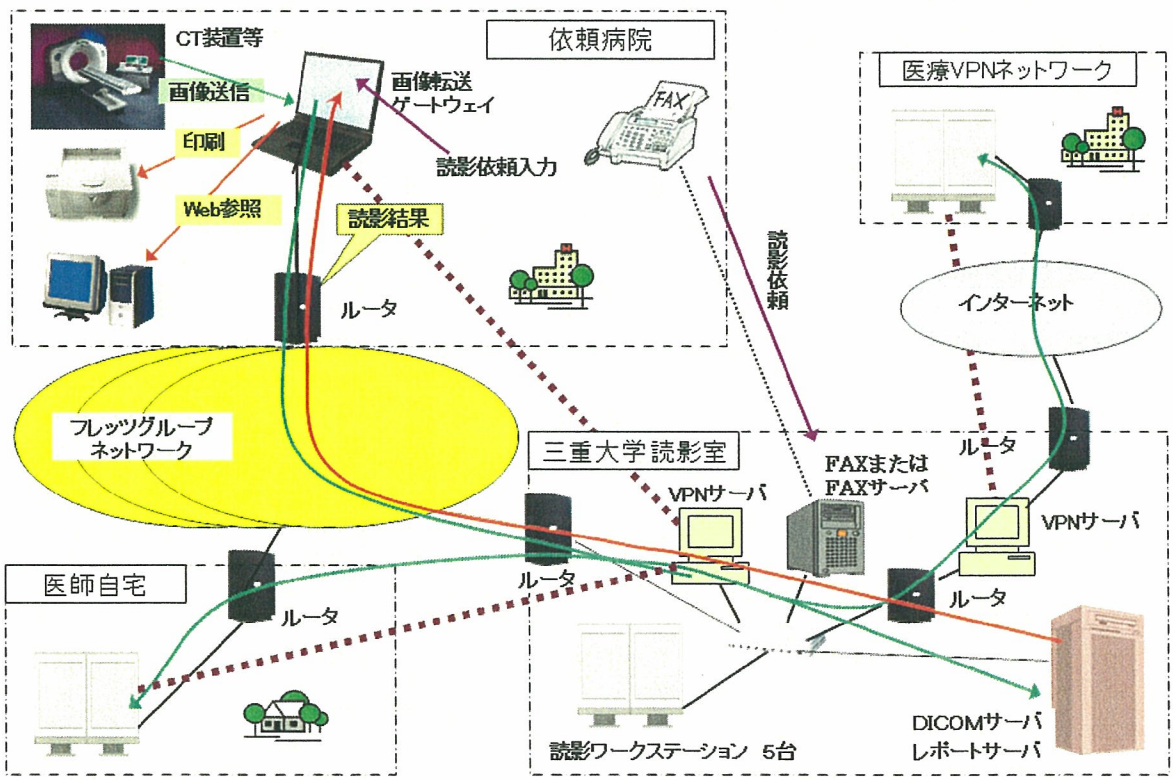


図１　三重遠隔画像診断ネットワーク構成図

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
—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ロジェクト等におけるCAの構築と運用

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

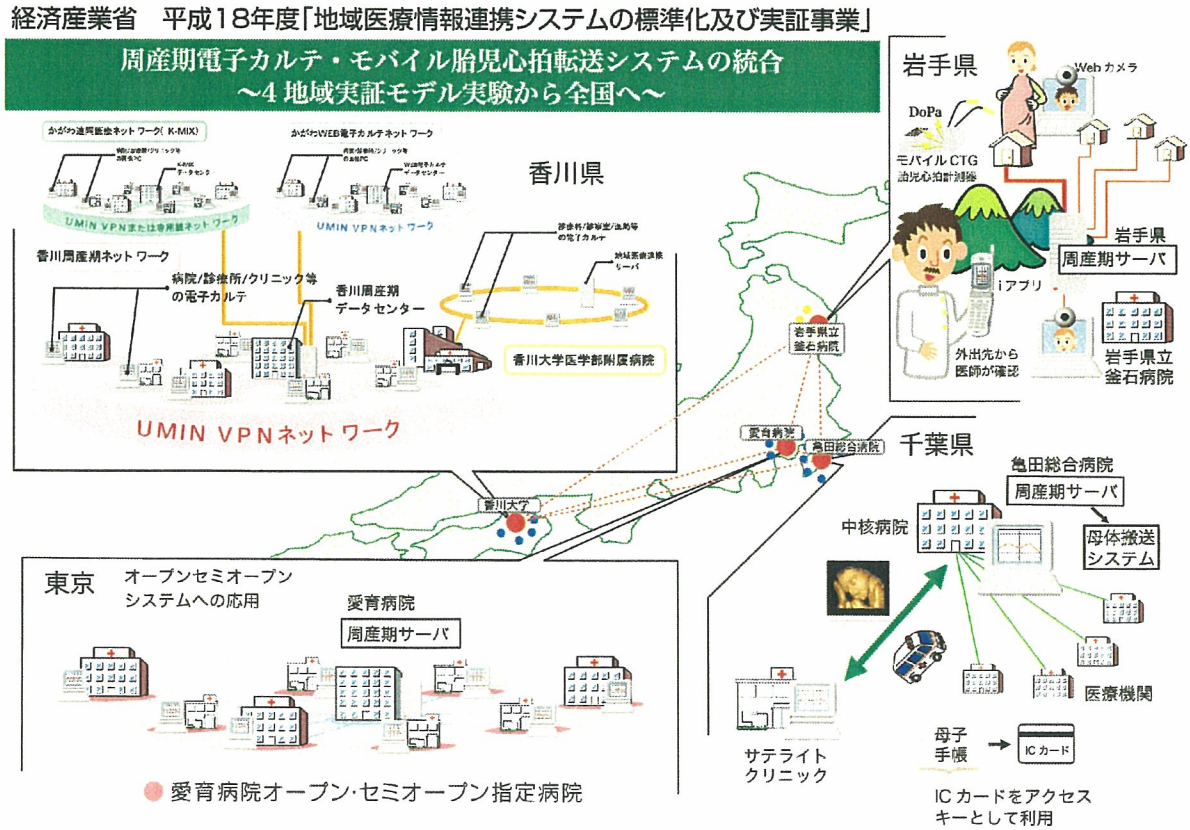
研究要旨　医療VPNとHPKIを併用した安全な医療情報交換基盤の構築に向け、香川大学医学部附属病院とかがわ遠隔医療ネットワークにUMIN-VPNを実装する。また、経済産業省の進める周産期電子カルテネットワークプロジェクトにおいても、UMIN-VPNならびに厚生労働省の進めるHPKIを実装する予定で、今後遠隔医療、並びに電子カルテネットワークが全国に展開することが期待される。

A　研究目的

昨年１月、内閣は「e-Japan戦略」に続く「IT新改革戦略」を新たにスタートさせた。「IT新改革戦略」では、時間と距離を超越するITの力を生かして、日本が世界のIT革命のフロントランナーとして、国民が夢をもてる社会を実現することをめざしている。ITによる構造改革の対象として、医療のIT化が第一に取り上げられ、なかでも遠隔医療と電子カルテによる医療機関相互の連携が最重要課題とされている。

香川県においては、すでに1998年度から妊娠管理を目的とした電子カルテのネットワーク化（周産期ネットワーク）に、2001年度には経済産業省の事業による「四国４県電子カルテネットワーク連携プロジェクト」に取り組んできた。その成果に基づき、2003年度には香川県による画像センター構想「かがわ遠隔医療ネットワーク（略称：Ｋ－ＭＩＸ）」がスタートし、現在すでに60の医療機関が参加している。

本年よりＫ－ＭＩＸは全国の医療機関が参加可能となっており、さらなる発展が期待されている。また本年度から経済産業省により３年間



（図１）４地域実証モデル実験の概要

の予定で、地域医療情報連携システムの標準化及び実証実験事業ー「周産期電子カルテネットワーク連携プロジェクト」ーがスタートし、岩手県、千葉県、東京都、香川県をフィールドとして実証実験が行われている（図１）。

本稿では、本研究班の主要テーマである医療用UMIN-VPNとHPKIを、これら４地域のサーバ相互、ならびに関連医療機関を実際に連携する上での、技術的、維持管理上の課題を明確にする。

A.1　「周産期電子カルテネットワーク連携プロジェクト」

今回の経済産業省によるプロジェクトでは、Web版周産期電子カルテワークと、モバイルによる在宅妊婦管理システムの機能を統合し、医療機関相互、そして医療機関と在宅妊婦を結ぶネットワークを全国に普及させることが大きな目標である。まず全国の中で周産期医療を実施する上で特徴のある４地域、すなわち東京都（愛育病院）、千葉県（亀田総合病院）、岩手県（遠野市、県立釜石病院）、香川県（香川大学医学部附属病院）において、それぞれの地域特性にあった周産期電子カルテネットワークを構築するとともに、４地域のシステムをVPNを介して相互に接続し、最終的には全国の周産期医療機関と在宅妊婦を連携することを視野にいれている。

B　研究方法

実際には、東京都と千葉県の総合周産期母子医療センターである愛育病院と亀田総合病院を中心として、オープン・セミオープンシステムへの応用、ならびに遠野市と県立釜石病院をフィールドとして、過疎地における診療所、家庭や助産院を連携する医療体制をモデル化することにより、他地域へ適用を拡大する。

その場合、４地域で開発したモデルを全国の地域ごとの特性に応じて最適化したシステムを提供できるようにする。

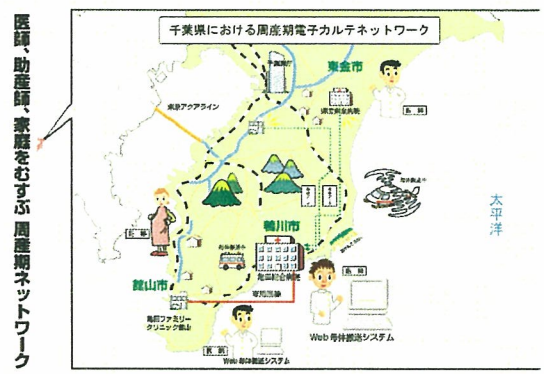
本事業で開発された技術は、他の領域でも容易に応用可能なことが大きな特徴であり、妊娠管理にくわえ、新生児医療、小児医療に関して、また医療機関だけでなく、保健所など行政まで、そして母親などが直接データにアクセスできるようにするなど、いわゆるユビキタス医療の実現に役立つ。

B.1　東京都での取り組み

愛育病院では、昨年度よりオープン・セミオープンシステムを導入しているが、今回のプロジェクトでは、Web版周産期電子カルテシステムを愛育病院に導入し、周囲の診療所（約10か所を予定）と電子カルテネットワークで連携する。電子カルテネットワークにより、医師、ならびに妊婦が医療機関を移動しても、紹介状だけでなくすべての周産期データをどこからでも入力、参照が可能となり、オープン・セミオープンシステムの運用に威力を発揮する。

B.2　千葉県での取り組み

亀田総合病院の電子カルテと周産期電子カルテを機能的に連携し、周産期データを一元管する。また新たに館山に開設されたサテライトクリニックと電子カルテネットワークで連携し、安房夷隅地域全体での妊娠管理に取り組む。電子カルテと直接データ連携するWeb母体搬送提供書やWeb母子手帳を開発するとともに、ＴＶ会議システムを用いた遠隔診療や超音波画像の転送による遠隔診断に取り組む。

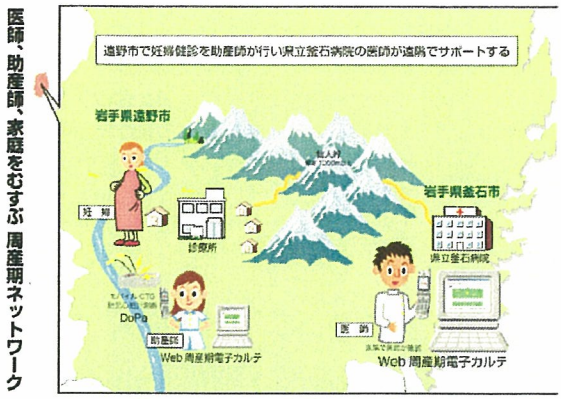


（図２）千葉県での取り組み

B.3　岩手県での取り組み

岩手県の自然環境は広大であり、隣接する医療機関への移動距離が50kmをこえるところが少なくない。また冬季の気象条件は過酷であり妊婦は分娩時の移動のみならず、日常の妊婦健診を受診する際においても大変な困難をともなう。今回のプロジェクトでは、自然環境が厳しく、しかも産婦人科医のいない遠野市をフィールドとして、在宅妊婦管理システムと電子カルテネットワーク、Web母子手帳、Webテレビ会議システムを利用した遠隔での妊婦管理に取り組む。

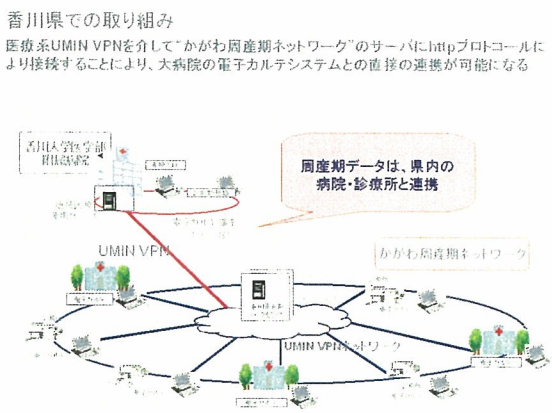
宅妊婦管理システムは小型軽量のモバイル胎児心拍数検出装置と受信側の装置からなる。家庭で検出された胎児心拍数情報は通信ネットワーク、DoPa網を介してサーバに送られ、医師はインターネット網を介して常時データを受け取ることができる。映像コミュニケーションは送信側・受信側ともに光ファイバーやADSL回線でインターネットブラウザを利用し、30万画素Webカメラとヘッドセットで通信を行う。セキュリティに関しては映像と音声は独自プロトコルで通信しており、テキストやファイル共有などはSSLで通信する。



（図３）岩手県での取り組み

B.4　香川県での取り組み

香川県においては、「かがわ周産期ネットワーク」と「かがわ遠隔医療ネットワーク」両者の機能統合を行うとともに、他の３地域をVPVを介して相互に接続するサーバを構築する。



（図４）香川県での取り組み

C　研究結果

C.1　セキュリティに関して

セキュリティに関しては医療用ＶＰＮネットワーク（ＵＭＩＮ－ＶＰＮ）、経済産業省、厚生労働省の推進する電子証明書ポリシー（ＨＰＫＩ）による電子署名を周産期電子カルテ上で実現させ、その有効性や利便性を検証する。連携プロセスの抽出とアルゴリズム化は、日本産婦人科医会の全面的な協力により産婦人科専門医等から構成される委員会を組織し、実施する。

通信プロトコルの作成等は当該分野の専門家等から構成される委員会を組織して行うとともに、有効性や利便性の検証は机上の検討の後、香川県、東京都、千葉県、岩手県の実フィールドにおいて実証する。

C.2　本プロジェクトへのＶＰＮとＨＰＫＩ導入

周産期の連携は従来顔の見えたスタッフで行われているので、相互信頼が成り立っているのでセキュリティの問題は顕在化してこない面がある。今後、日常接していないスタッフとの連携や長期保存データの活用が行われてくるとそのセキュリティ問題がクリアされていないことによる、活用の阻害要因になる可能性がある。

本年度の実証試験を踏まえ、次年度以降問題点を整理し、重点的に技術開発を行い実証する。

本プロジェクトでは、地域間のデータ連携サーバを構築することで4地域に分散された患者カルテ情報を、地域を越え、妊婦が全国どこへ移動しても、必要な時に医療データが利用することが可能である。今までは患者ＩＤが地域ごとに異なって登録されているために、地域を越えたデータの検索が困難だったがその紐付けも可能となる。

本プロジェクトへのＶＰＮとＨＰＫＩの利用は以下のものを想定している。

（１）診断書の電子化
（２）紹介状の電子化
（３）周産期連携情報の真正性（証拠性）
（４）母子手帳の電子化
（５）他科医療データの真正性
（６）オンデマンドＶＰＮ使用時の施設確認

C.3　「かがわ周産期ネットワーク」と「かがわ遠隔医療ネットワーク」の機能統合

本プロジェクトにより周産期電子カルテネットワーク周産期の医療情報と医療画像をシームレスに扱うことを可能になった。産婦人科医だけでは判断の難しい検査でも、放射線科医などの専門医に診断を依頼することにより、患者へ適切な診断治療を行うことができる。これにより、難しい病気は高次医療施設へ、普段の通院は身近な診療所へ、と医療施設の役割分担化を進めることができる。これはオープン・セミオープンシステムの考えと共通のものである。

また今回の連携で使用したJ-MIXは診療情報の電子的な相互交換のための公開された規格であり、HL7など標準的な構造を持ったデータを含めること可能で、将来的にはHL7 CDAR2など他システムとの連携の使用にも期待することができる。

C.4　ＶＰＮによる４地域のサーバの相互連携

４県で導入している周産期サーバ同士を概念的に接続しデータ連携が行えるようにＶＰＮを

介して周産期サーバをネットワークで結ぶ香川県の周産期サーバは他の地域（現時点で３カ所）のサーバを結ぶネットワークのハブとしての役割を果たす。ネットワークの接続にはインターネットVPNを用いる。インターネットVPN接続の暗号化プロトコルはIPsecを利用する。これにより安全な通信を確保することができる。

本プロジェクトで用いるVPNルータはハブ・アンド・スポーク型で接続されており、周産期ネットワークのハブとして動作する。すなわち、VPNネットワークを一元的に管理できる。ただしVPNハブとなるシステムには、全てのVPNトラフィックに対して暗号化／複合化処理が求められるため、高可用性・高信頼性が求められる。

この様に、香川県サーバを中心として各地域のサーバを連携することにより、今後全国へ普及しやすい形を形成することができる。

C.5　本研究班によるOpenCAを使った認証局（CA）の構築

2007年2月15日に厚生労働省はHPKIをスタートさせた。本プロジェクトでは2007年度にHPKIを実装する予定であるが、その前段階として、本研究班によるOpenCAによるPKIの構築を試験的に行った。以下にOpenCA実装に用いたシステム環境を示す（表１）。

Server：Dell PowerEdge 800
CPU: Intel Pentium 4
Memory: 1GB
Hard Disk: 40GB
OS: Redhat Enterprise Linux ES 4

（表１）OpenCAを実装したシステム環境

実際の手順として、①OpenSSL、Apache-SSLをインストール、②サーバ証明書を作成、③OpenCAのインストールと必要なモジュールの追加、④管理者として証明書を発行と証明書のインポート（この作業によりCAが信頼される機関として登録される）、⑥署名付きメールの送受信、⑤暗号メールの送受信、の順に行った。アドレス帳より送信相手を選び、送信する。

実際に使っての感想として、OpenCA を使って構築したサーバにアクセスすることでGUIを使って簡単に登録、証明書の発行が出来ることは、限られた範囲での運用には大変有用であると思われた。今回は実際利用したネットワーク環境が限定されており、医療の実際のフィールドで充分な検証は出来なかったが、厚生労働省によるHPKIの実装の前段階としては大変有意義であった。

D　考察

本事業で導入されたＶＰＮによる周産期ネットワークは、他の領域でも容易に応用可能なことが大きな特徴である。

今後、ＨＰＫＩを実装することにより、妊娠管理にくわえ、新生児医療、小児医療に関して、医療機関だけでなく、保健所ならびに行政まで、そして母親などが直接データにアクセスできるようにするなど、いわゆるユビキタス医療の実現に役立つ。

以上報告した様にセキュリティを確保した医療用VPNネットワーク（UMIN－VPN）とＨＰＫＩはあらゆる医療系のネットワークに応用可能である。

（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、文部科学省科学研究費No.15300185、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、日母胎児心拍数情報ファアイルデータフォーマット規格に関して電気通信学会　信技報MBE99-38 p1-7、1999

[2] 原　量宏、岡田宏基ほか、周産期医療情報の標準化"日母標準フォーマット"とネットワークを用いた周産期管理システムの開発と運用、医療情報学、20(2)p143-148、2000

[3] 原　量宏、岡田宏基、木村敏章、千田彰一、医療ネットワークにおけるモバイル機器の活用、臨床外科、vol 57、No9、1241-1249、2002

[4] 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

[5] 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

[6] 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.

[7] 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

[8] 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.

[9] 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

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
―やまぐち情報スーパーネットワークにおけるCAの構築と運用

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．このVPNにより山口大学病院を含む県内の医療機関は相互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。この地域医療ネット内には限定したメール機能が稼動しているが、PKIとCA実装することにより高い安全保障を維持したメールによる広域連携が可能になった

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）を敷設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、運用と管理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を中心にした研究グループや地域医師会が共同して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。また、地域医療ネットを利用する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．

４）認証局：試験的に山口大学内に認証局を立ち上げ、導入、運用方法について検討した。

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医療機関（萩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うもので、医療機関内の診療業務LAN（萩市民病院）、ATM専用線（メガデータネット、NTT）、やまぐち情報スーパーネットワーク（山口県）、学内LAN（山口大学）および山口大学病院遠隔医療LANを一貫させることで実現した。

C.研究結果

非営利法人（NPO）と協力して大学病院が支援することの意味は、

①患者データのプライバシー保護に配慮した医療ネットが安心して利用できること

②地域の医療機関が特別な技術者を持たなくても変化の激しい情報技術に対応できること

③営利企業でない運営組織であることが産学官連携の場として信頼がえられること

である。

２）安全保障された通信環境：地域ＩＸに加入したインターネットサービス事業者を接続回線ネットワークとしたので、インターネットに出ることなくＹＳＮを介する途中経路が明確になった．山口県を超えた情報連携は、ＵＭＩＮセンターを介した医療ＶＰＮにより、国立大学病院あるいは国立病院との安全保障された診療連携の情報基盤を確立できた．（図１）

３）認証局：山口大学内にOSがFreeBSD5.5のサーバ、及びその他の関連ソフトウェアを用意し、OpenCAの認証局用サーバソフトウェアを導入した。また、証明書の要求発行を行った。

D.考察

やまぐち健康福祉ネットワークにおける地域医療ネットワーク構造の概念は、患者に身近な地域医療圏を単位として診療所や病院をネットワーク化し、それを仮想(バーチャル)の一つの病院と見立てることである。かかりつけ医が中心となって地域の専門医と連携して患者の問題解決にあたり、必要となれば医療圏を飛び越えて全県域で、さらには、UMINの医療VPNが実現したことで全国の専門医へのコンサルテーションも可能となる。

山口県では、大学病院が主導してきた運用管理の機能を県当局から活動を委託された非営利法人に移管し、同時に、広域ネットワークのボトルネックとなるlast one mileの安全保障の強化を進めてきた。地域医療連携にもとめられるのは、医師からは安全保障であり、患者からは個人情報のプライバシー保護である。その際に、VPNに加えて、日常のコミュニケーションの手段として定着した電子メールの安全保障と手軽な取り扱いが求められており、来年度は本研究プロジェクトで実装することになる。

実際に認証局を立ち上げたが、これまでの認証局のシステムより容易に導入できた。それでもやはり専門的知識が必要であった。個別にサーバのハードウェア、サーバソフト、証明書を導入して立ち上げるのではなく、認証局専用機器があると導入が容易になると考えられる。

また、証明書を要求、利用に関して操作画面のメニューが複雑であった。これでは、一般の利用者が利用するには、敷居が高い用に思われる。これらは情報セキュリティーのためには、必要なこではあるが、医療情報ネットワークでPKI環境を広めるためには、運用・操作を簡略化する必要がある。

利用状況に応じたセキュリティーレベルが存在しているので、遠隔医療ネットワークに関するセキュリティーレベルを検討し、それに適したPKIの機能を整理することが必要である。

E.結論

医療VPNとPKIは安全・安心の医療連携の基本技術である。山口県下の医療機関を高速回線で結ぶネットワーク基盤を構築し、接続回線ネットワークの安全保障を進めてきたが、PKIを利用する情報連携を実装することにより利用者の利便性と安心はいっそう高まるものと期待できる。

F．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ITを利用した地域医療形態-山口トライアルを通してみる情報化の実際-　日本臨床検査医学会誌 56(7)：980-986，2007

２．学会発表

井上裕二、石田博：やまぐち型IHN(統合地域医療ネットワーク)プロジェクト　中四国医療情報学研究会、2007、徳島

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

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
—カルナ事業におけるCA構築と運用

分担研究者　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　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、九州大学が展開する疾病管理事業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、疾病管理事業がより効率的に推進されることが期待される。

A　研究目的

九州大学が展開している生活習慣病に対する疾病管理事業「カルナ」（以下、カルナ事業という）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行い、今年度はPKIを構築する。

Bカルナ事業の提供サービスと必要な情報流通

九州大学では2003年度からJST研究の一環として、九州電力系列企業と発電所制御技術を応用した患者個別性に対応する電子化クリティカルパスの産学連携共同研究を行った。さらに2005年度からは、経済産業省・健康サービス産業創生支援事業によって、地域連携クリティカルパスを中核技術として用いるアウトバウンド・コールセンタ型の糖尿病予防（2、3次予防）プログラムをサービスする疾病管理事業を開発してきた[1)]。これは、コールセンタからかかりつけ医と患者の両方に働きかけて、糖尿病合併症（網膜症、腎症、神経障害）、動脈硬化症（心筋梗塞、脳卒中）などの発症を予防し、患者QOLを上げるとともに医療費増加抑制を視野に入れたものである。さらに2008年度から開始される「特定健康診査制度」を保険者から受注するための生活習慣予防（1次予防）プログラムをサービスする体制を2006年度にやはり経済産業省・サービス産業創生支援事業により開発した[2)]。これらによりカルナ事業では糖尿病においては1次から3次までをシームレスに運営することが可能となった

1次予防プログラムでは、カルナ・コールセンタは①患者と②保険者との間で情報流通を行う。①に関しては、個人の情報がメールで取り交わされるが、生活習慣病の前段階者が対象であり、罹患に至っていないことから内容は一般のメールに順ずる程度で、本人の了承の元、メールでのコミュニケーションを用いている。なお、本人が了承しない場合は、郵便、電話を用いる。一方、保険者との間では、被保険者リストや複数人の健康状態一覧、検査結果、生活習慣およびその改善努力などがやり取りされる。これに関しては、メールを用いることが簡便ではあるが、高度の認証性を有することが求められる。その他、インターネットデータセンタから健康診断結果のWeb参照や、被保険者への面談時にASPを用いた面談ナビゲーションおよび保健指導内容入力システムを開発している。

2次、3次予防プログラムでは、コールセンタと①患者との間、および②かかりつけ医療機関との間で、情報の流通が発生する。患者については、個人診療情報が多く含まれるため、現在は電話と郵便で行っている。またかかりつけ医に対しても、患者診療情報や患者への生活習慣病教材（かかりつけ医経由による教育）、患者へのアドバイス（コールセンタ経由で行う）などセンシティブな情報が流通するため、郵便を利用しており、コスト、時間ともに事業運営には不利に働いている。従って高度の認証システムを有したセキュアな広域ネットワーク上でメールを用いた情報流通をおこなうことが望ましい。

C 研究方法

本研究のテストベッドには、2005年度に構築したコールセンタとかかりつけ医との間のネットワーク、および2006年度に構築したコールセンタと保険者との間のネットワークを用いる。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。

本研究には以下の情報機器群を用いた。

CA Server
Maker： Dell
機器名： Power Edge 860
OS：　CentOS

Mail Server

Maker：Sun Micro
機器名：Sun Fire T-2000
OS：　Solaris 10

DNS Server
Maker：Sun Micro
機器名：Sun Fire V20
OS：　Solaris 8

D 研究結果

D.1 ネットワーク構成

九州大学病院にCAおよびメールサーバを設置し、インターネット接続にはKyushu university Integrated information Transmission Environment (KITE) - SuperSINETを用いた。カルナ事務局の接続はKITEの配下にある。

D.2 サービス対象アプリケーション

[1]　同一CAドメイン内

現在、2次、3次予防プログラムの実証実験を行っているかかりつけ医療機関は7機関、患者30人であり、患者の通院に合わせて月に1度程度郵送にて診察支援用・教育支援用の資料を送っている。また、患者の通院後にかかりつけ医療機関から、患者の診察結果、および血液検査結果などを提供している返信用封筒でコールセンタ事務局に送る運用になっている。更に、1次予防プログラムにおいては、現在4企業健康保険組合、300人との間で実証実験中であり、その事務局や産業医などとの連携（対象者登録や健康診断結果の送付など）は郵便で行っている。これらにはsensitiveな複数対象者の個人診療・健康情報が多数含まれており、電子メールを用いた情報流通は行ってこなかった。

これらの情報コミュニケーション手段として当システム上での電子メールの利用を希望するかかりつけ医療機関や健康保険組合については、PKIを用いた認証システムの利用が可能となった（図１）。

[2]　他共同研究大学CAドメインとの通信

UMINのブリッジCAを介した共同研究の各大学設置のCA同士の相互信頼が成立していると考えると、全国規模で利用できる通信基盤としての利用も可能である。カルナ事業では2007年度には東京都、静岡県の健康保険組合や疾病管理事業者と連携して九州支社の被保険者に対するサービスや遠隔地へのコールセンタサービスを実証実験と登録して行うが、やはり複数対象者の個人健康情報の受け渡しなどが頻繁に必要となる。ブリッジ CA を介した署名検証を行うためには証明書パス構築・検証が複雑となるので今後の検証が必要ではあるが、これらについても通信基盤は完成した（図２）。

E 考察

PKIに対応したインフラがカルナ事業に出来たことで、カルナ事業の目指す高セキュリティな通信ネットワーク基盤整備が前進した。

各種のVPN通信との併用により、sensitiveな個人情報がセキュアに流通可能であるが、本事業のように固定された通信相手と常にsensitiveな個人健康・診療情報の流通を行っているような場合には医療VPNの利用が合目的でもあり、また意識せずにVPNを用いることが出来るためVPN利用忘れなどを避ける上で有効である。

特定健康診査制度では、40歳以上の被保険者の健康診断・保健指導データは「生涯健康情報」として標準的な形で保存することを義務付けられている。検査コードはJLAC10を用いて通信プロトコルはHL7CDAを使用するなどが定められている。例えば転職などにより、保険者が変わる際には旧保険者が責任を持って新保険者へデータ移行せねばならない。カルナ事業と連携している保険者同士であれば本研究のCAを用いた相互認証が可能となる。またコールセンタ-事務局と患者間の通信、地域医療連携の際のかかりつけ医―専門医間の通信、糖尿病発症の際の保険者からかかりつけ医への連携通信、カルナ事業で使用するインターネットデータセンタからの個人健康データのWeb閲覧などの際の個人認証など、認証面で様々な展開が期待される。

PKIのもう一つの大きな機能は真正性の担保である。疾病管理事業では個人健康・診療情報を長期間電子的に蓄積するため、医療機関で用いる電子カルテと同様な真正性の担保が要求されることになる。この目的への応用もこの基盤で可能であり、今後の課題と考える。

F 結論

九州大学が展開している疾病管理事業「カルナ」に於いて、PKI基盤を整備した。広域に応用できるセキュアな通信インフラが実装されることにより、疾病管理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]　中島直樹、小林邦久、井口登與志、西田大介、副島秀久、高柳涼一、名和田新．２、３次予防としての「カルナ」事例－日本型疾病管理事業－．医療情報学　(supple)72-75，2006.

[2]　中島直樹．特定健康診査制度によって　　変わる健診．新医療、34：90-93　2007.

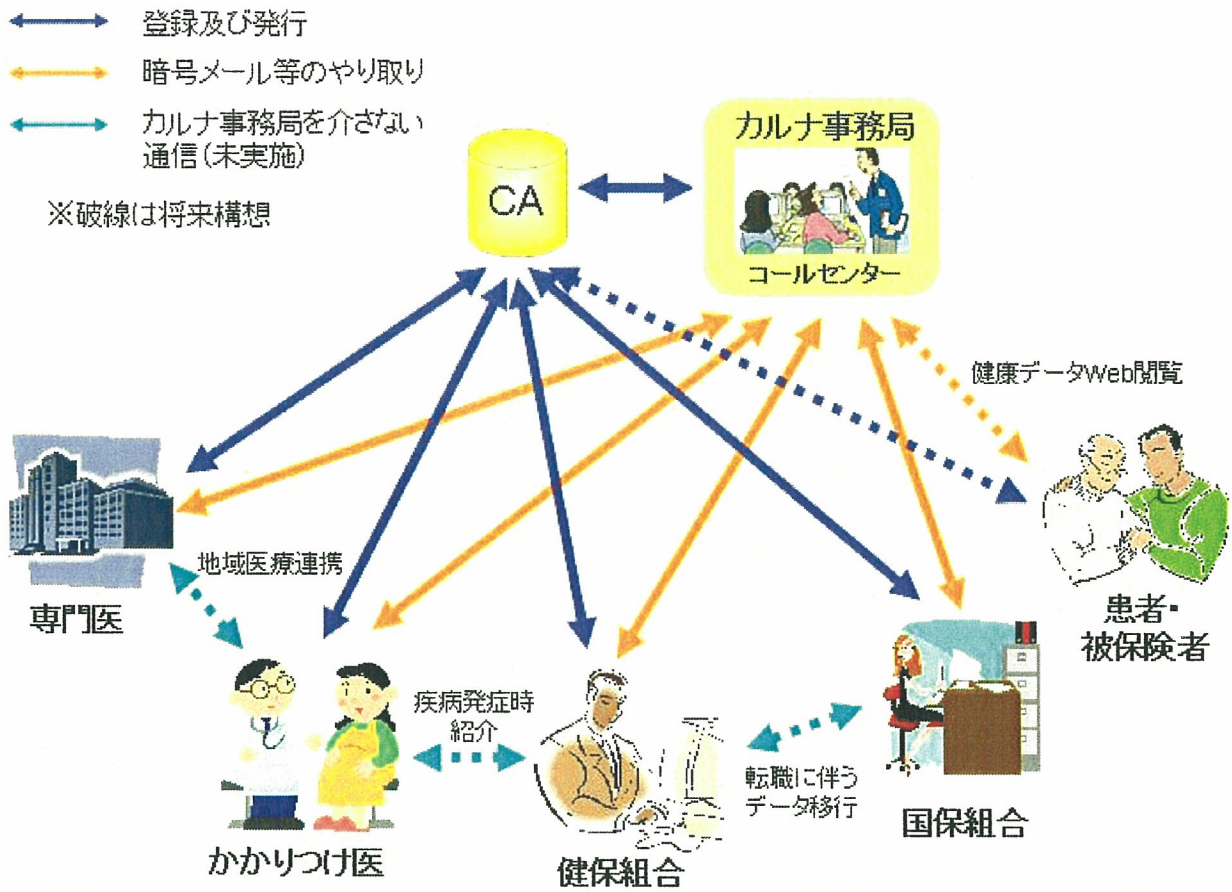


図１　CAを用いた疾病管理事業「カルナ」のコミュニケーションシステム

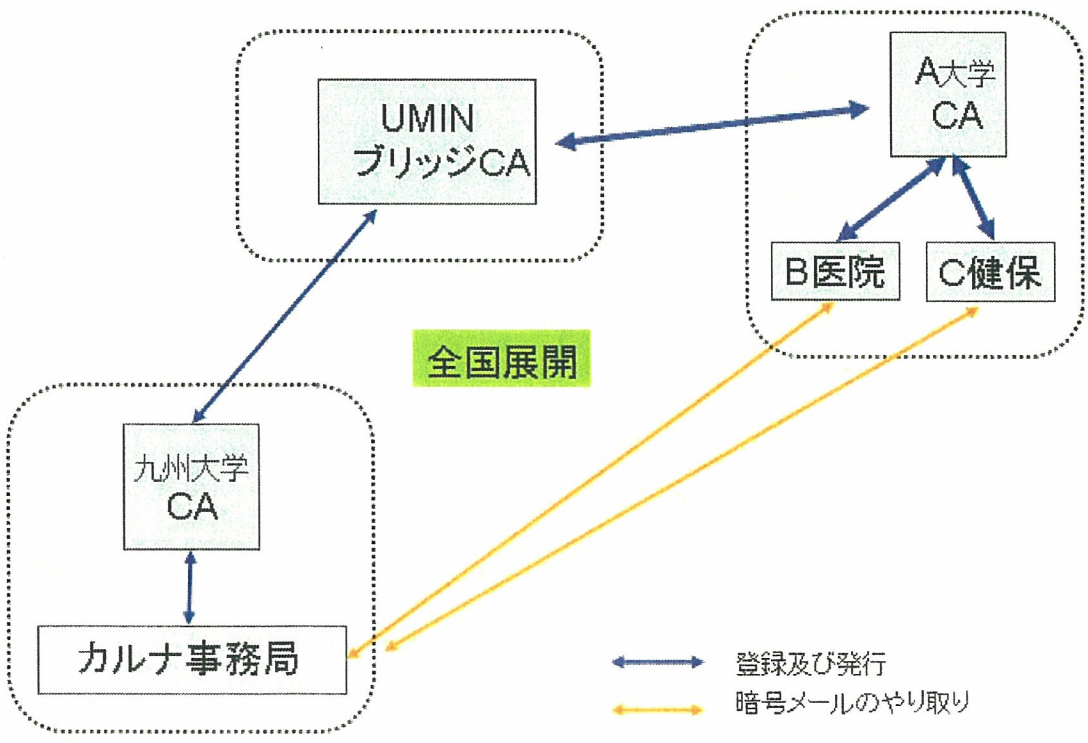


図２　ブリッジCAを介した遠隔地域での相互認証とコミュニケーション

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
—熊本大学医学部附属病院におけるCAの構築と運用

分担研究者　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

研究要旨　本研究では、システム利用者の利便性と既存システムとの連携を考慮しつつ、安全に医療情報を交換可能なネットワーク基盤を提案する。本システムでは、一般に普及しているプロトコルを用いることでシステム間連携を容易にするとともに、階層化した暗号化処理を行うことで、ユーザの利便性を大きく損なわずに安全な情報交換を行う手法を提案する。

A　研究目的

熊本大学医学部附属病院には31の診療科と28の中央診療部門があり、様々な部門システムが4種類のネットワーク（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[1]。しかし、現在の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ため、電文やユーザアカウント情報などを全て平文で取り扱っていることが多い。そのため、地域連携などで外部機関との情報交換が必要な場合には、拠点間の暗号化通信を行うだけでなく、院内システムにおいても部門間・ネットワーク間で不要な情報が流通しないようにネットワークインフラ側で対策を行う必要がある。

そこで、本研究では一般に普及しているプロトコルを用いることでシステム間連携を容易にするとともに、階層化した暗号化処理を行うことで、ユーザの利便性を大きく損なわずに安全に医療情報交換を行う手法を提案する。

本報告書では、本院で構築した暗号化基盤と情報交換基盤について説明する。

B　研究方法

本研究では、医療機関同士だけでなく院内の部門システム同士でも安全な情報交換を実現するための仕組みとして、暗号化技術を導入した情報交換基盤を構築した。また、災害時等の場面でも情報システムを利用可能にする手段として、無線ネットワークを用いた情報インフラの構築を行った(図1)。

B.1　暗号化基盤の構築

暗号化通信やクライアント認証などを行う仕組みとして、電子証明書を管理・運用するための認証サーバを構築した。認証サーバは、OpenCA[2]とOpenMicroServer[3]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。一度環境構築を完了すれば、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。

B.2　情報交換基盤の構築

本研究では、情報交換基盤としてwebメールシステムの導入を行った。

メールサーバは、メッセージ交換の手段として利用するだけでなく、文書管理を行うデータベースサーバとしても有用であり、以下のような利点がある[4]。

1. テキストに変換できれば、あらゆるデータをメッセージとして扱うことができ、S/MIME[5]による暗号化が行える。
2. 長い歴史を持つシンプルなプロトコルであるため、実装が容易である。
   → 他システムと容易にデータ交換できる。
3. 時系列でメッセージを一元管理できる。
4. 送信元アドレスやクライアントPCのIP情報などのヘッダ情報をメッセージと一緒に管理できる。
5. メッセージの変更処理などを行う際にメールの返信機能を利用することで、Message-ID: と References:、In-Reply-To:ヘッダの内容から作業履歴を追うことができる。
6. メーリングリストなどを用いることで、複数人で作業を行うことが可能になる。

また、webサーバを利用すれば、SOAP[6]やREST[7]などのプロトコルを使うことで、より多くのシステムとの連携が可能となる。メールシステムを応用した例では、webメールサービス「GMail」を利用したファイルサーバ「GSpace[8]」や、カレンダーベースのコラボレーションソフト「c2talk[9]」がある。どちらも、アプリケーション同士の情報交換手段としてメールを利用しているだけである。

また、本システムでは、メールシステムの認証・暗号化機能とは独立したwebサーバでのクライアント認証を行うことで、より強固なセキュリティ対策を施した。通常、メールの暗号化を行う場合には、ユーザごとに公開鍵と秘密鍵を作成し、公開鍵暗号方式でメールの暗号化を行う。しかし、コンピュータの盗難などにより秘密鍵が外部に漏洩した場合、速やかに当該鍵を失効させる必要があるが、一度鍵を失効させてしまうと、それまでに受信したメールを復号することが不可能になる。コンピュータが破損した場合も同様で、メールサーバ内に情報が残っていたとしても、復号することは困難な状況に陥る可能性がある。

そこで、本サーバでは、利用者にはクライアント認証用の電子証明書のみを配布し、S/MIME用の公開鍵・秘密鍵はwebメールサーバ内のみで所有・利用する方式を考案した。この場合、クライアント認証とS/MIME処理では、それぞれ異なる電子証明書を用いることになる。したがって、コンピュータの盗難・破損で電子証明書を失っても、単にwebメールシステムへのアクセスが不能になるだけで、電子証明書を再発行すれば従来どおりにwebメールシステムにアクセスし、従前どおりにメールを読むことが可能となる。

今回導入したwebメールサーバでは、OpenSSL、 HTTP (apache)、SMTP (postfix)、POP3 (qpopper)の各サービスとwebメール用のCGIを稼動している。代表的なwebメールシステムにはSquirrelMail[10]やIMP[11]があるが、今回はクライアント認証部分のみを実装し、検証を行うためにシンプルなウェブメーラー[12]を使用した。webメールシステム内での公開鍵・秘密鍵の管理と暗号化・復号処理機能については、来年度以降に実装する予定である。

B.3 災害用病院内情報交換基盤の構築

医療行為を迅速かつ適切に遂行するためには、スタッフ同士が円滑に情報交換を行う必要があるが、ネットワーク障害や災害発生時には既存の通信インフラが利用できない場合が多いため、従来はトランシーバや紙伝票を用いて情報交換・収集を行うことになる。しかし、大学病院のように敷地が広く、建物が入り組んでいる場合には、人手による伝票配送の手間がかかり、情報交換が滞るという問題があった。この問題に対処するためには、企業などで取り組んでいる事業継続計画 (Business Continuity Plan: BCP)と同様の対応が大学病院でも必要であると考える。そこで、病院内で円滑に情報交換をしながら医療行為を遂行可能な環境を実現するため、既設の院内ネットワーク網とは異なる独自のネットワーク網と、情報共有環境の構築と評価を行った[13]。

B.3.1 方法

無線ネットワーク網の構築 広範囲に設置された各診療拠点をネットワーク接続する手段として、無線LANアクセスポイントを複数台用意し、Wireless Distribution System(WDS)機能を用いてアクセスポイント同士を接続した(図2)。WDSはアクセスポイント同士を無線で接続する技術で、IEEE802.11で規定されている[14]。このWDSネットワーク網は院内の既存ネットワークや外部回線とは完全に独立したネットワークである。

今回使用したアクセスポイントはIO-DATA社製「WN-WAPG/R」で、電波の到達距離は見通しで300m、建物内で100mという仕様である[15]。WDSを用いた場合、最大8台のアクセスポイントを接続可能である。

情報共有システム 職員同士が情報交換を行う仕組みとして、webベースの情報共有システムを試作した。図2に示す通り、WDSネットワーク網に情報共有サーバと各拠点へ設置するクライアントPCでハードウェアを構成してある。各拠点では、クライアントPCを用いて各種情報を入力し、情報共有サーバへ送信する。クライアント側では、本院が作成した「災害対策マニュアル」で規定している災害時チェックリスト(図3)に沿って必要事項を入力・送信する。万が一、本システムが使用不能になった場合にも備え、速やかに紙の運用に移行できるよう、紙と同様の入力画面を用意した。情報共有サーバは災害対策本部に設置するものとし、各拠点から集めた情報を集約・表示するとともに、本部からの通知等を各拠点へ配信する機能を有する。情報共有システムは、一般職員でも扱いやすいように全てWindows OSで構成してあり、Apache2, PHP, MySQLなどのwebアプリケーション開発環境をパッケージ化したXAMPP[16]を用いて開発した。

B.3.2 結果

本システムで構築したWDSネットワーク網の有効範囲を調査するため、院内で無線LANの有効範囲について調査実験を行った。本実験では、無線LANアクセスポイントを2台とノートPCを2台(クライアント、サーバ各1台)用いて行った。図

4 に示す△がアクセスポイントの位置、○がノートPCの位置で、各機器の接続関係を太線で示した。実験の結果、良好な通信状態(ping応答1ms以内、パケットロス無し)を維持したまま、見通しで総距離約264mのPC間で通信可能なことを確認した。建物内の遮蔽物による影響を考慮する必要はあるが、アクセスポイントを5台程度用意すれば、本院の建物周辺をカバーするネットワーク網の構築が可能になると考える。

C　考察

C.1　メールプロトコルによるシステム連携

本報告書では、認証サーバとwebメールシステムを用いた安全な医療情報交換基盤の提案と、災害時などでも情報システムによる業務を継続可能な無線ネットワーク基盤について報告した。

昨年の報告書で紹介したカルテラベルオーダシステムでも、メールによるメッセージ配信機能を実装したが、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アラームやメッセージ配信に利用されている、安定した情報交換方式である。現状、平文で通信を行っている既存システムでも、メールプロトコルを利用することで比較的容易に暗号化機能を実装することが可能であると考える。

また、メールサーバに格納される医療情報へのアクセスは、クライアント認証とS/MIMEのセキュリティ対策を施している。電子証明書の紛失・盗難等を考慮すると、一般的に行われているS/MIMEのみの共通鍵暗号方式だけを用いる場合に比べ、より強固なセキュリティを利用者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。この点については、来年度にメールサーバ内での証明書管理と暗号化処理について更に深く検討を行い、より使いやすい仕組みを提案したいと考える。

C.2　災害用病院内情報交換基盤の構築

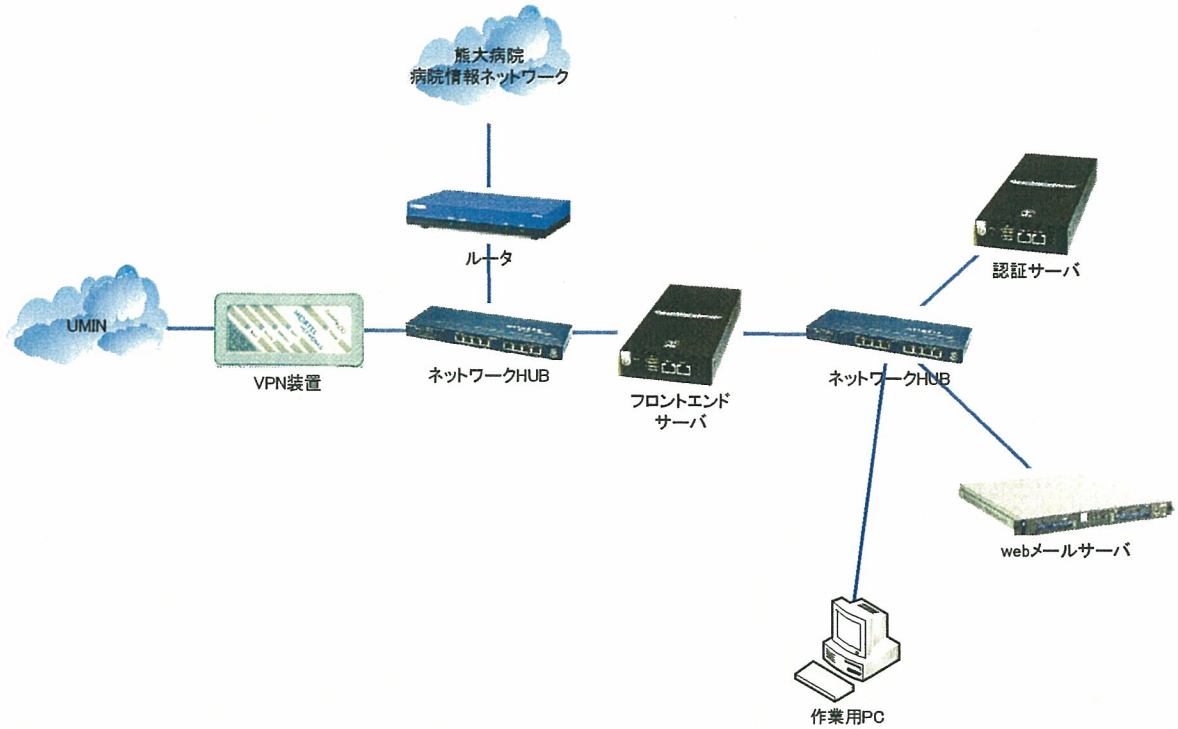
災害時に円滑な情報交換を行うためのネットワーク網と、情報共有システムを提案した。実際には電源確保の問題や、建物・遮蔽物による無線LANへの影響も考慮する必要があるが、各機器の配置を柔軟に設定できる利点は災害時以外にも応用可能であると考える。今後は、実証実験を重ね、提案手法の安定度を確認するとともに、前述の認証サーバとwebメールシステムを稼動することも検討していきたいと考える。

D　結論

本報告では、システム利用者の利便性と既存システムとの連携を考慮しつつ、安全に医療情報を交換可能なネットワーク基盤を提案した。本システムでは、一般に普及しているプロトコルを用いることでシステム間連携を容易にするとともに、階層化した暗号化処理を行うことで、ユーザの利便性を大きく損なわずに安全な情報交換を実現できると考えているが、今後も検討と改良を重ね、より使いやすい仕組みにしていきたいと考える。

参考文献

[1] 熊本大学医学部附属病院:
http://www.kuh.kumamoto-u.ac.jp
[2] OpenCA: http://www.openca.org
[3] OpenMicroServer:
http://www.plathome.co.jp/products/microserver/
[4] RFC2822(Internet Message Format):
http://www.emaillab.org/emailref/RFC/rfc2822.txt
[5] S/MIME:
http://www.ipa.go.jp/security/rfc/RFC2311-01JA.html
[6] SOAP:
http://www.w3.org/TR/soap12-part0/
[7] REST:
http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm
[8] Gspace: http://www.getgspace.com/
[9] c2talk:
http://www.c2talk.net/jp/index.php
[10] IMP Webmail Client:
http://horde.org/imp/
[11] SquirrelMail:
http://www.squirrelmail.jp/
[12] ウェブメーラー:
http://www.ai.is.saga-u.ac.jp/~takeda/
[13] 末永貴俊, 菊池 健, 高田 彰, 宇宿功市郎:
災害用病院内情報共有システムの構築, 生体医工学シンポジウム2006, 講演予稿集CD-ROM
[14] IEEE 802.11, The Working Group Setting the Standards for Wireless LANs, http://www.ieee802.org/11/
[15] WN-WAPG/R, IO-DATA社製,
http://www.iodata.jp/prod/network/wnlan/2005/wn-wapgr/
[16] XAMPP for Windows,
http://www.apachefriends.org/en/xampp-windows.html


熊大病院
病院情報ネットワーク
ルータ
認証サーバ
UMIN
VPN装置
ネットワークHUB
フロントエンド
サーバ
ネットワークHUB
webメールサーバ
作業用PC