20031066

厚生労働科学研究研究費補助金
医療技術評価総合研究事業研究事業

電子カルテネットワーク等の相互接続法の標準化

平成１５年度　総括研究報告書

主任研究者　木内　貴弘

平成１６（２００４）年　４月

目　　次

Ⅰ．総括研究報告

厚生省科学研究費補助金（医療技術評価総合研究事業）

総括研究報告書

電子カルテネットワーク等の相互接続法の標準化

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　各地で構築されつつある電子カルテネットワーク等を、VPN (Virtual Private Network)を利用して、全国レベルで安全に相互接続するために必要な標準的な技術仕様の策定を行った。更に策定した標準仕様を利用して、既存の国立大学病院VPN(UMIN VPN)と６つの地域医療情報ネットワークの相互接続を実際に行い、その実用性を立証した（医療VPN)。本研究の成果により、全国レベルでの地域医療情報ネットワーク・医療機関の安全な閉域ネットワークの構築が技術的に可能となった。今後は、今回構築した医療VPNへの参加施設の拡大と有効活用が望まれる。

分担研究者

廣川博之	旭川医科大学附属病院経営企画部部教授
辰巳治之	札幌医科大学大学院医学研究科生態情報形態学教授
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
高田彰	熊本大学医学部附属病院医療情報経営企画部助教授

A．研究目的

地方自治体主導、医師会、大学等の主導によって、複数の地域で電子カルテネットワーク等を中心とした様々な地域医療情報ネットワークの構築が進んでいる[1-6]。これらを構築するためのインフラとしての通信回線には、ISDN、専用回線、インターネット上のVPN等の様々なものが用いられている。また地域医療ネットワークの機能・役割も地域単位で電子カルテセンターサーバを共有して用いるものから、遠隔医療や単純な患者情報のまで様々である。

これらのネットワークは、従来、将来お互いに相互接続することをまったく念頭におかずに独立して構築が行われてきた。今後、このような新たな地域医療情報ネットワークの構築は更に増えていくと予想される。またASP(Application Service Provider)方式による病院・診療所用の医療情報システムのネットワークでの提供が、ベンダー等によって進められていくことも予想される。今後、数百、数千もの地域医療ネットワークやベンダー等による医療情報システムのネットワークが、相互接続を考慮することなく、構築されつづけていった場合には、将来これらを相互接続することは技術的にもコスト的にも不可能となることが想定される。

本研究の第１の目的は、VPNを用いて、日本の全ての医療情報ネットワーク・医療機関が参加できる安全な閉域ネットワーク（医療VPN）を構築するための標準仕様を策定することにある[7]。そして、第２の目的は、この標準仕様を利用して、既存の電子カルテネットワーク等を実際に接続して、その実用性を検討することにある。

B.研究方法

標準仕様の策定にあたっては、ドメイン名・IPアドレス割当方針の策定（廣川)、IPv6との相互接続・運用の検討（辰巳)、VPNの各医療機関への接続形態の検討（山本)、専用線ネットワークとの相互接続法の策定（井上)、DNSの運用法の策定（原)、ルーティング運用法の検討（中島)、運用のセキュリティ保護指針の策定（高田）について、各々が原案の作成を行い、３回にわたって班会議を行い全員で仕様原案の議論を詳細に行った。

仕様策定のあたっては、下記のような方針を採用した。

１）インターネットと医療VPNの同時利用

医療VPNへの参加施設が、医療VPN経由で他の参加施設が提供するサーバ等へのアクセスが安全にできることは当然であるが、同時に各施設内から、インターネット上のサーバ等へのアクセスも可能であるようにするように配慮した。

２）医療VPNの自律・分散管理

医療機関等だけが参加する医療VPNにおいても、基本的にインターネットと同様に自律・分散管理の仕組みを採用する方針とした。

３）各施設自身の責任によるセキュリティ保護

医療VPN経由での各施設へのすべての通信は、各施設の責任で行う方針とした。このために各施設の医療VPN接続時におけるファイアウォールとVPN機器の安全な接続形態の検討を行った。

４）インターネット用DNSサーバとの共用化

DNSについては、医療VPN用のDNSルートサーバは医療VPN内におくとともに、各施設内の同一のDNSサーバで、通常のインターネットのサーバ等の名前解決と医療VPN内のサーバ等の名前

解決ができる方法の検討を行った[8]。

5）既存のUMIN VPNの機能の維持と独立運用

本研究開始の前から、国立大学病院だけが相互接続されたVPNネットワーク（UMIN VPN）が運用されてきた[9]。今回の医療VPNの接続にあたっては、現行のUMIN VPNについては、まったく従来通りに医療VPNとは独立した方式で使えるようにする方針とした。

6）UMIN VPNを介しての医療VPNへの参加

UMIN VPNを介して各国立大学病院が医療VPNの中の1施設として、参加できるように配慮した。ただし、このためには、各国立大学病院で設定変更の作業が必要となる。

上記の方針に基づいて策定された標準仕様案にもとづいて、既存のUMIN VPN及び分担研究者らが関係する6つの地域医療情報ネットワークとの実際の接続作業を行った。

C.研究結果

すべての国内の地域医療情報ネットワーク、医療機関等をすべてVPNで相互接続可能とするためには、お互いがユニークなIPアドレスを持つように見えるようにする必要がある。このため、プライベートアドレスの中に医療VPNのユニークなアドレス空間を予約することにした（図1）。医療VPNで使用するプライベートアドレスの領域は、10.255.0.0/16とした。また予備のプライベートアドレス領域として、10.254.0.0/16を予約した。また医療VPN系の情報資源であることを明確にするために、医療VPN内のサーバ等には、hvpn.netというドメイン名を使用することにした。例えば、旭川医科大学は、「asahikawa-med.hvpn.net」というドメイン名で、医療VPN内から見えるようになる。

医療VPN参加施設から、外部に出る場合には、グローバルアドレスの場合には、インターネット側に、上記で指定した医療VPNアドレスの場合には、医療VPN側にルーティングされるようにすれば、同一の施設から、インターネットと医療VPNの両方を同時に使用することが可能である（図2）。また医療VPNで提供されるWWWサービスやメールアドレスは、ドメイン名により、容易にインターネットのものと区別することが可能である。ファイアウォールとVPN機器の接続方法としては、インターネットを介した通信も医療VPNを介した通信も、施設内部に入る前に必ずファイアウォールを経由するような接続形態とする必要がある。またファイアウォールを介さないで、インターネット側からVPN側へ、または逆方向に通信できないような接続形態とする必要がある。このような接続形態として、資料「ファイアウォールとVPN機器の接続形態」のような接続方法を考案し、例示した。

医療VPNの運用のためには、基本的に医療VPNアドレスとドメイン名を重複しないように各参加施設に割り当てるだけでよい。ルーティング等は、インターネットと同様に行われるため、集中管理を行う必要はない。医療VPNのIPアドレスとドメイン名の割当を受けて、既存のVPN参加施設と接続し、両施設でルーティング等の設定を正しく行えば、直ちに通信が可能となる。医療VPN内に設置される医療VPN用ルートネームサーバ及び各施設内でのDNSサーバの運用については、以下の医療VPN構築の具体例の中で触れることにする。

今回実際に構築を行った医療VPNについて記述を行う前に、既存の国立大学病院VPN(UMIN VPN)について、概略を説明する。平成15年11月時点で、UMIN VPNは、図3のように構成されていた。各国立大学病院とUMINセンターのVPN系情報システムとの通信は、以下のような手順で行われる。

1）各国立大病院からUMIN VPN系サーバへの通信

まず通常のインターネットのDNSサーバでアクセス先のサーバ（例えば、s.umin.ac.jp=130.69.92.201）の名前解決を行う。UMIN VPNでは、サーバ用セグメントはグローバルIPアドレスが割当てられているため、通常のインターネット用のDNSで名前解決を行うことができる。名前解決が完了すると、そのアドレスに向けてセッションを張りに行くが、各国立大学病院ではサーバが設置されている130.69.92.192/26に対するルーティングをVPN装置に向けているため、自動的にVPN装置経由の通信となり、UMINセンターからのサービスをVPNを介して受けることができるようになっている。

2）UMIN VPN系サーバから各国立大病院への通信

UMINセンターから各国立大学病院に通信コネクションを張る場合は、UMINのVPN系システム内のサーバは、UMIN内のVPN用DNSサーバを参照して名前解決を行い、各国立大学病院のアドレス（10.xxx.xxx.xxx）に向けて通信を行う。現在、この方向のコネクションは、UMIN VPN系メールサーバから各国立大学病院のメールサーバにメールを送付する際にのみ使用されている。

本研究では、医療VPN用に、新しいネットワー

クを構築し、既存のUMIN VPNについては、ネットワーク構成などを変更することなく、この新しい医療VPNネットワークに、１つのネットワークとして参加する形をとった。医療VPNでは、アドレス空間としては、現在、国立大学病院VPN内で使われていないアドレス空間(10.255.0.0/16)を利用することになるため、医療VPN側から見ると、UMIN VPN内のサーバ等が医療VPNのアドレス空間に存在するように見えなくてはならない。このため、両者の接続部では、ＮＡＴによるアドレスの変換が必要となる他、UMIN VPNのセキュリティ確保のための対策が必要である。このために、ネットワークの境界上にファイアウォールを設置して、パケットのフィルタリングを行うとともに、NATを行うことで、相互に通信が可能となるようにした。図４はその概念図である。左側の「国立大学病院VPN(UMIN VPN)」は既存のものであり、右側の「医療VPN」は、本研究によって新設され、各地域医療情報ネットワークが接続されるものである。医療VPNの基本的な内部構成は、国立大学病院VPNとほぼ同等である。それをFirewallで相互接続し、医療VPN側から国立大学病院VPN側を見た場合には、「10.255.xxx.xxx」で見えるようにし、逆に国立大学病院VPN側から医療VPN側を見た場合には、「130.69.92.xxx」で見えるようにNATを行うようにした。

医療VPN用ルートDNSサーバは、図５に示す通り、医療VPN内に２台(予備用が１台)設置し、「hvpn.net」などの医療VPN用に確保したドメインを管理することにした。医療VPN用ルートDNSサーバは、(1)医療VPN参加各施設内のDNSサーバに医療VPN内のDNS情報をゾーン転送する他、(2)医療VPN内からの直接の名前解決要求に答え、(3)UMIN VPNからの名前問合せ要求(s.umin.ac.jp及びhvpn.net)にも回答するようにした。

UMIN VPNでは、これまでインターネット上のDNSを使用してアドレス解決を行ってきた。今後は、UMIN VPN参加施設内のDNSサーバが、医療VPN用ルートDNSサーバから、s.umin.ac.jp及びhvpn.netのゾーン転送を受けることによって、すべて医療VPN(UMIN VPNを含む)だけで、インターネットを利用せずにUMIN VPN及び医療VPNの名前解決が可能となる。ただし、このためには、UMIN VPN参加の各国立大学病院内のDNSサーバの設定変更が必要となる。また設定変更をしない国立大学病院に対応するために、従来とおり、インターネット上でs.umin.ac.jpの名前解決が可能であるようにs.umin.ac.jp用のDNSサーバの運用を維持しておく必要がある。この場合、設定変更しない国立大学病院は、医療VPN上のサーバの利用はできないことになる。

D.考察

木内（主任研究者）は、国際的に見ても最も早い時期から、医療機関のファイアウォール間の通信を暗号化することによって、医療機関専用の閉域網（当時は、Virtual Closed Networkと木内は呼ぶことを提唱していた）を作ることを構想していた[10]。木内の具体的な標準仕様の提案は、HTTPの多機能性と汎用性に着目して、この閉域網をHTTP専用に作ることであった。しかしながら、この提案は国際標準技術となることできなかった。様々な方式の提案が数多く出される中で、特定のアプリケーションレベルの通信プロトコールに依存しないIPsecを利用した暗号化技術が標準技術として認められるようになり、名称もVirtual Private Network（VPN）が定着していった。本研究は、この標準化されたVPNを利用して、木内の以前から抱いてきた医療機関等による暗号技術による閉域網を実現するものであると位置付けることができる。

医療VPNでは、医療機関等の間の通信はすべて暗号化され、医療VPN内のサーバ等へは、医療VPNの参加している医療機関等以外からは、アクセスができないために、安全性は非常に高い。しかしながら、セキュリティは常に「程度の問題」であり、完全に安全ということはありえない。特に１つの医療機関が外部から侵入された場合には、連鎖的に侵入や攻撃にさらされる危険がある。このため、我々が策定した医療VPNの仕様では、例え医療VPNを介した通信であっても、セキュリティポリシーとして、すべて各施設のファイアウォールによるチェックを行うことを前提としている。

医療VPNは、医療機関等の間の「インターネットに出ている部分」だけを暗号化するものであり、２つの通信を行っているコンピュータや機器等の間のすべての通信を暗号化する、いわゆるend-to-endのセキュリティ保護システムよりは、セキュリティが劣ると一般的に考えられている。例えば、各医療機関等のファイアウォールの内部や医療VPNのエクスチェンジでは、通信内容がVPNからでて、暗号が解かれるため、盗聴の危険が存在する。

一方、end-to-endの暗号化（暗号電子メール等）には、上記のような欠点はないものの、厳密な個人認証または個々のコンピュータや機器毎の認証が必要であり、このため、個人や個々のコンピュータ・機器等に公開鍵証明書発行が必要となる。この作業は、医療機関にとっては費用と手間がかかる煩雑な作業であり、また個人を対象にした場合にはそれ相当の利用者教育も必要となる。また医療機関等の職員の側にも負担が発生する。

これに対して、VPNは、施設対施設の通信だけを暗号化するので、認証は施設単位で行われ、１

施設に1枚の公開鍵証明書を発行すれば済む。このため、コストが安く、運用・管理も容易であり、利用者側の負担もほとんどない。運用上の労力とコスト上の理由から、end-to-endのセキュリティ保護法よりも、VPNの方がより早く普及し、その後にend-to-endのセキュリティ保護手段が普及していくものと考えている。

しかしながら、上記のことは、end-to-endのセキュリティ保護手段が、VPNに取って代わるということは必ずしも意味しないと考えている。より安全性を高めるためには、end-to-endのセキュリティ保護手段とVPNを併用するのが最も望ましい。両者の併用のメリットとして、下記が考えられる。

1)ファイルセーフ機能

医療VPNが普及しても、通常のインターネットでのメールのやりとりは行われるであろうし、暗号電子メールが普及しても、平文のメールのやりとりも行われていくと思われる。このような状況のもとでは、医療VPN、暗号電子メールを各々単独で使用した場合には、利用者のミスによって、医療VPN経由で送られるべきメールがインターネット経由で、暗号化されて送られるべきメールが平文で送られる危険性がある。このため、医療VPNと暗号電子メールの併用によって、単独利用のときに発生しがちな利用者によるミスを相互補完することが可能になる。

2)暗号の二重化による安全性の向上

暗号化が二重に行われることによって、解読の難しさが増すとともに、片方の暗号アルゴリズムにセキュリティホールが見つかった場合でも、2つの暗号の併用によって安全性が確保できる。また通信の安全性について患者等への説得力が増すという利点もある。

インターネットでは、IPアドレスとドメイン名の割当だけが集中管理され、それ以外の設定情報（ルーティング、マシン名等）は基本的に自律・分散管理されている。電話のように全体の通信の状況を監視・管理されていないために、通信の速度や確実性についての保証はない。一方で、この自律・分散管理の仕組みは、インターネットの運用の労力とコストを大幅に下げている。最近は、インターネットの普及と技術の成熟とともに、通信速度も向上し、信頼性も増してきている。医療VPNでも、インターネットとまったく同様の仕組みを採用しており、実質的に医療機関等だけが参加できる閉じた小さなインターネットのようなものと考えることができる。本研究班で行った実際の接続では、UMINセンターだけが医療VPNのエクスチェンジの役割を果たしているが、各施設からUMINセンターを介さずに直接相互接続することは容易であり、単に相互のVPN機器とルーティングの設定だけの問題となる。我々の策定した医療VPNの標準仕様は、インターネットを介したVPNによる接続が最もコストパフォーマンスがよいため、VPNによる接続を想定しているが、技術的には、専用回線を利用して接続してもまったく同じである。特に施設間が隣接している場合には、イーサーネット等を用いることも可能である。

一方、このような自律・分散型の医療VPNの管理・運用方式には、大きな欠点が存在する。複数の組織が共同で運用に関わっているため、どの組織も単独で通信全体セキュリティを保証することができない点である。即ち、医療VPNに参加する2つの施設の間の通信は、複数の第三者の施設を経由しうるが、経由するすべての施設が安全性を保証しなければ通信全体の安全性は保証されない、また経由する経路すら、通信時点で自動的に変更される可能性があるのである。つまり、自律・分散型の医療VPNでは、セキュリティを保証するようなポリシーは採用できない。このことは、医療VPNを利用した通信のセキュリティ保護の最終的な責任は、あくまでも通信する2施設で負う必要があることを意味する。このためにも、医療VPNと他の暗号化手段の併用が望ましいと考えられる。

医療VPN内では、参加する機関同士は医療VPNのグローバルアドレス（＝インターネットのプライベートアドレス）を持っているようにお互い見える。医療VPN用のIPアドレス空間として、インターネットグローバルアドレスを利用することも検討したが、実用上運用困難と判断した。すべての国内の医療機関等に割り当てられるような広大なまとまったグローバルなアドレス空間の新規確保は困難なため、小さな多数の領域のグローバルアドレスを医療VPN内で利用することになってしまうが、これにより、ルーティグの設定が非常に複雑となり、各施設での設定の変更が頻発する等の問題が生じるためである。

医療VPN用として、予約するインターネットプライベートアドレス空間の選択については、最も大きな連続したプライベートアドレス領域の一番後ろの部分を選ぶということを選択の根拠として考えた。どの領域を使ったとしても、既に医療機関内等で使われているプライベートアドレスがバッティングする可能性があることは同じであるが、上記のアドレス領域がバッティングの可能性が最も低いと考えたからである。

DNSについては、従来、UMIN VPNでは、インターネットのDNSサーバを利用して、UMIN VPN内のサーバの名前解決を行う方式をとっていたが、この方法は、DNSサーバが乗っ取られた

り、第三者が偽物のDNSサーバを用意した場合にセキュリティ上、大きな問題となりえる。今回の標準仕様の策定にあたっては、医療VPN内で、医療VPN用のDNSルートサーバを運用する方針を採用し、各医療VPN参加施設内のDNSサーバからゾーン転送の設定をすることによって、この問題を解決することができた。このため、従来のUMIN VPNに比較して、DNSに関するセキュリティ上の問題は大きく改善している。

本研究によって、全国立大学病院、全国立病院と６つの地域医療情報ネットワークがVPNで相互接続されることになった（ただし、国立病院については、HOSPNETの運用ポリシーの問題からメールのやりとりだけしかできない設定となっている）（図６－１、６－２、６－３）。今回構築した医療VPNは、既に巨大な医療専用閉域ネットワークと呼んでよいと思われる。このような巨大なインフラをどのように活用をするかは、今後の課題といえる。またこの医療VPNが、更に拡大していった場合には、アドレス・ドメイン名割当のための組織やもっと詳細なセキュリティポリシーの策定が必要となってくることが考えられる。

E.結論

本研究の成果によって、電子カルテネットワーク等の地域医療情報ネットワーク及びASPベンダー提供の電子カルテシステム等の全国レベルでの相互接続（医療VPN）のための標準仕様が策定された。またUMIN VPN、HOSPNET、６つの地域医療情報ネットワークが実際に相互接続され、安全な相互の通信が可能になった。今後は、更に参加施設を増やしていくとともに、構築された医療VPNを有効に活用する方法についての研究が行われていくことが期待される。

F．参考文献等

[1]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.

[2]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．医用画像情報学会雑誌 18(3):125-134, 2001.

[3]久長穣、八木英俊、奥田昌之、井上裕二：山口における地域遠隔医療ネットワークの構築 医療情報学 20:95-98, 2000.

[4] 原量宏、近藤博史、石原謙、瀬戸山元一．四国４県電子カルテネットワーク、病院 61(8):666-670、2002.

[5] Masuda G. Ishido Y, Nakashima N, Sakamoto N: An HL7 version 3 based regional diabetes patient record project developed in Japan. Journal of Korean Society of Medical Informatics 9(suppl. 2): s284-s288, 2003.

[6] 西尾大助，田中亨治，郭錦秋，佐藤純三，高田彰，吉原博幸：Dolphin Projectの現状，医療情報学23(Suppl.):153-154, 2003.

[7]木内貴弘．VPNの概念と今後の展望．INNERVISION 16(7):28-30、2001.

[8] ポール アルビッツ，クリケット リュウ．DNS&BIND（第4版）、オライリー・ジャパン、2002.

[9] 木内貴弘．インターネットにおけるセキュリティ保護技術 － VPNの概要と実例を中心に．医療とコンピュータ 12(9):15-19、2001.

[10] Kiuchi T, Kaihara S. C-HTTP - The development of a secure, closed HTTP-based network on the Internet. Proceedings of the Internet Society Symposium on Network and Distributed System Security, IEEE Computer Society Press, 64-75, 1996.

（注記）

医療VPNの標準技術仕様については、お互いに関係が深く分担研究報告書として別々の分担報告書で記述すると非常に分かりづらくなること、すべての項目は３回にわたる班会議で分担研究者全員（または代理人）によって、充分に議論されており、その過程で大きく内容が変更されているため、各々の研究者の貢献を区分することは必ずしも容易でない。このことから、技術的な接続の仕様については、すべて総括研究報告書でまとめて記述を行うことにした。

一方で、策定された標準仕様に基づいて、各地域ネットワークを実際に接続する際には様々な具体的な問題点が発生し、その解決が重要な研究課題となったこと、及び各々の運営する地域医療情報ネットワークの性格や構成によって、様々な視点から医療VPNによる相互接続の意義づけ・活用方法が可能であることから、分担研究報告書では、各地域ネットワークを接続する場合の問題や接続の意義・活用法について、記載する方式をとることにした。

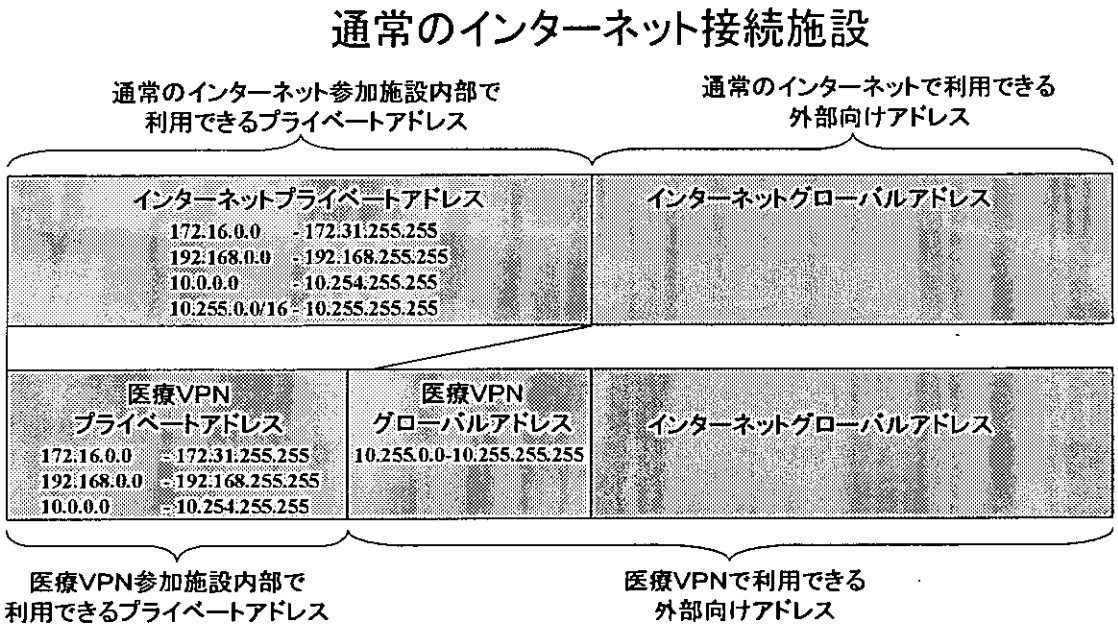


図１　インターネットプライベートアドレスと医療VPNグローバルアドレス・医療VPNプライベートアドレスの関係

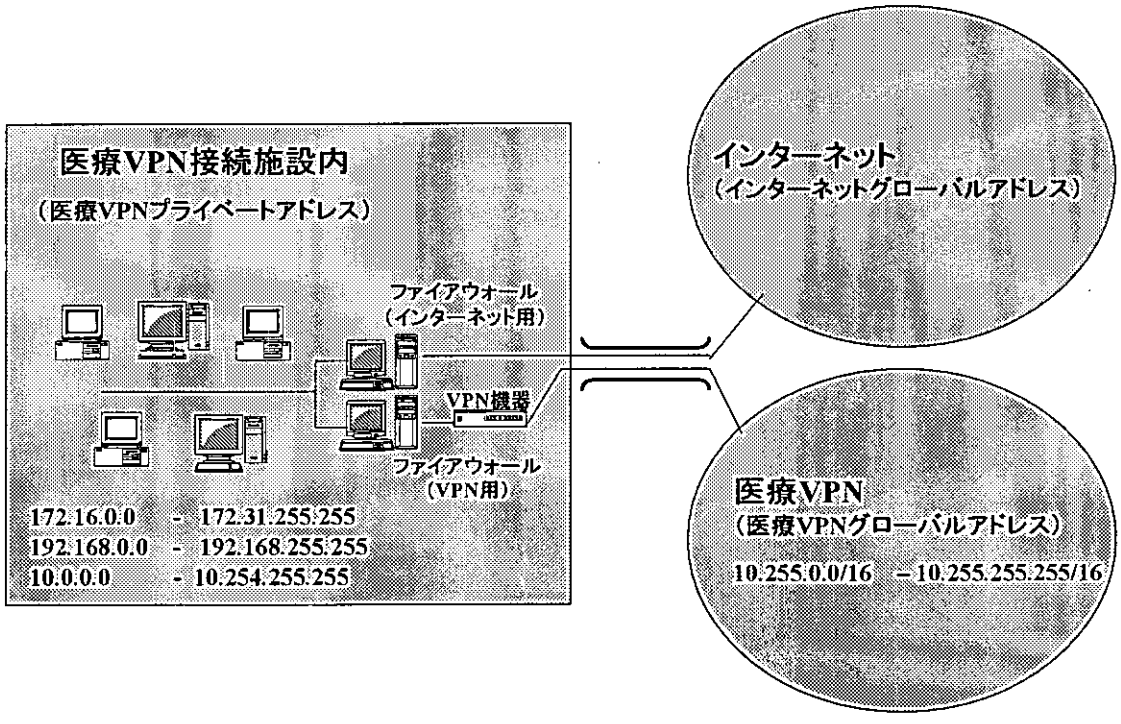


図２　医療VPN接続施設内からのインターネットと医療VPNのアクセス

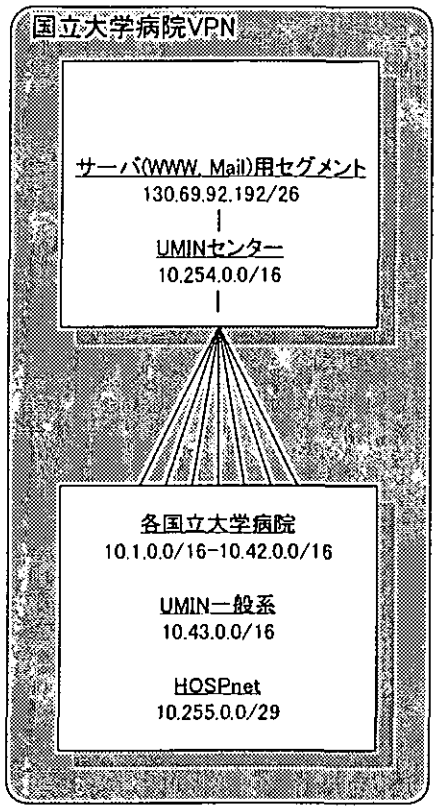


図３　国立大学病院VPN(UMIN VPN)

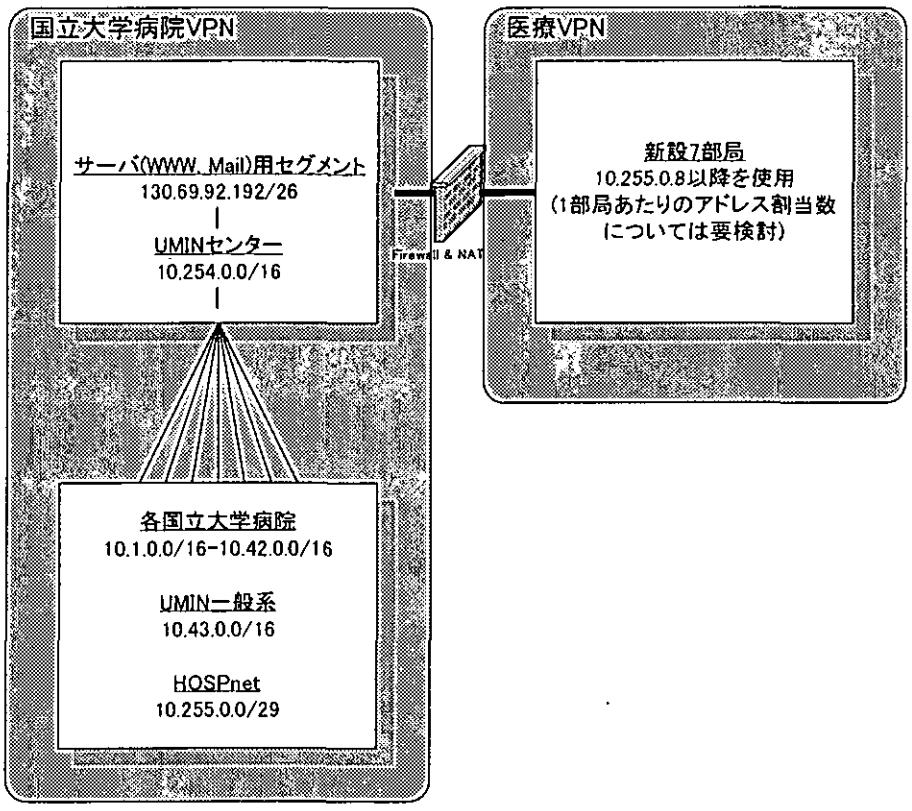


図４　国立大学病院VPN(UMIN VPN)と医療VPNの接続

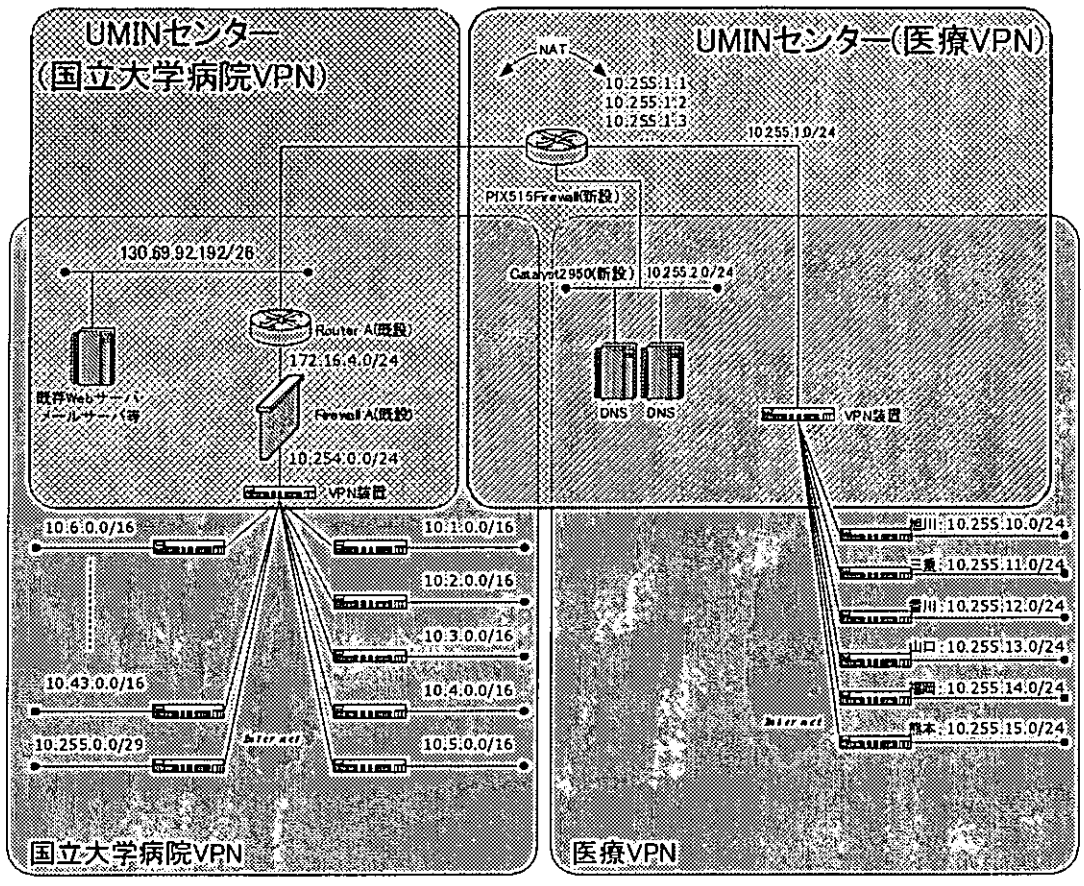


図５　国立大学病院VPN(UMIN VPN)と医療VPNのIPアドレスと名前解決

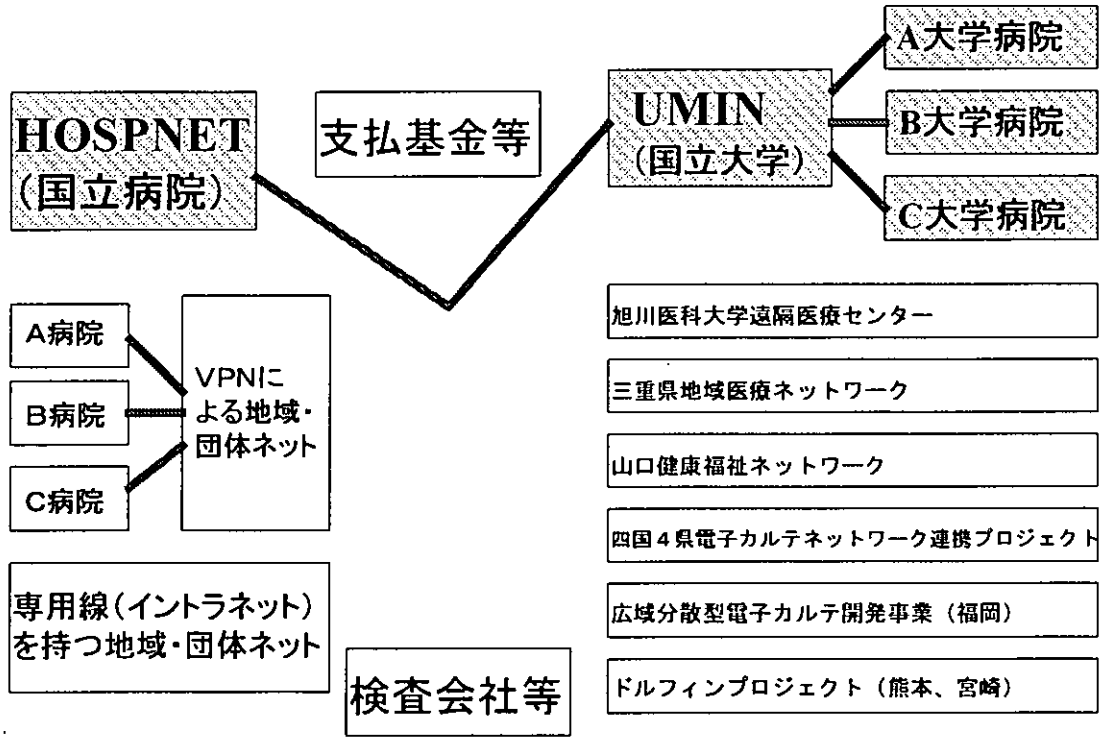


図６－１　本研究開始前（平成１５年３月）

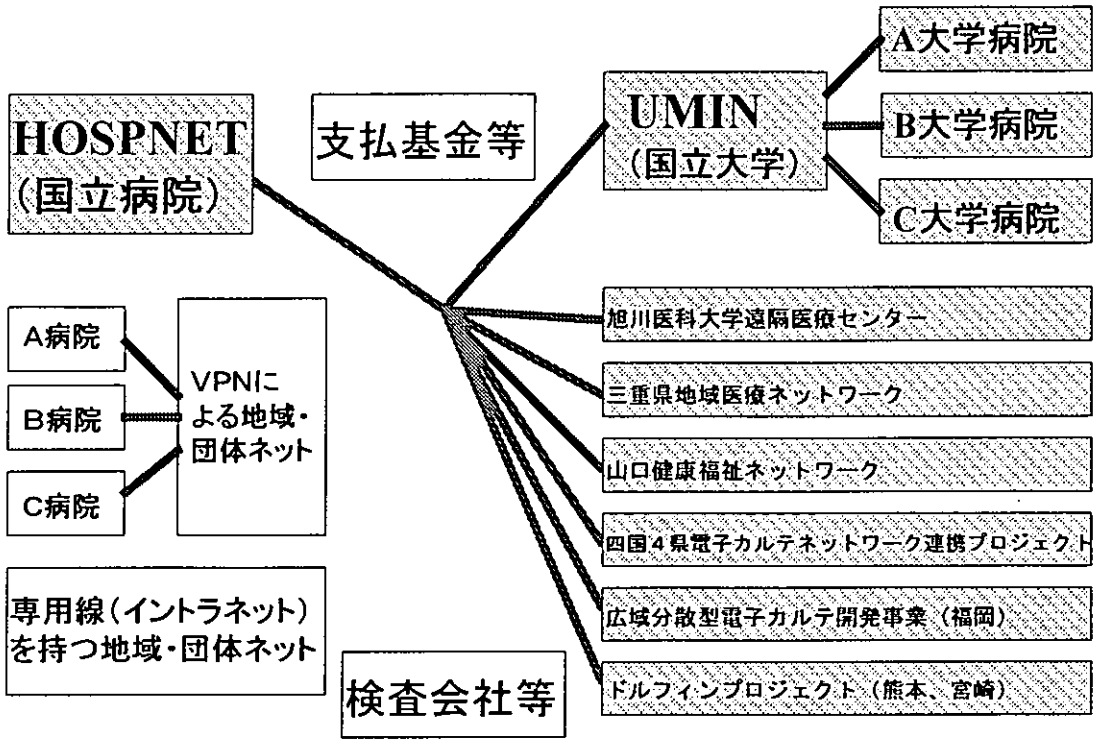


図６－２　本研究終了後（平成１６年３月）

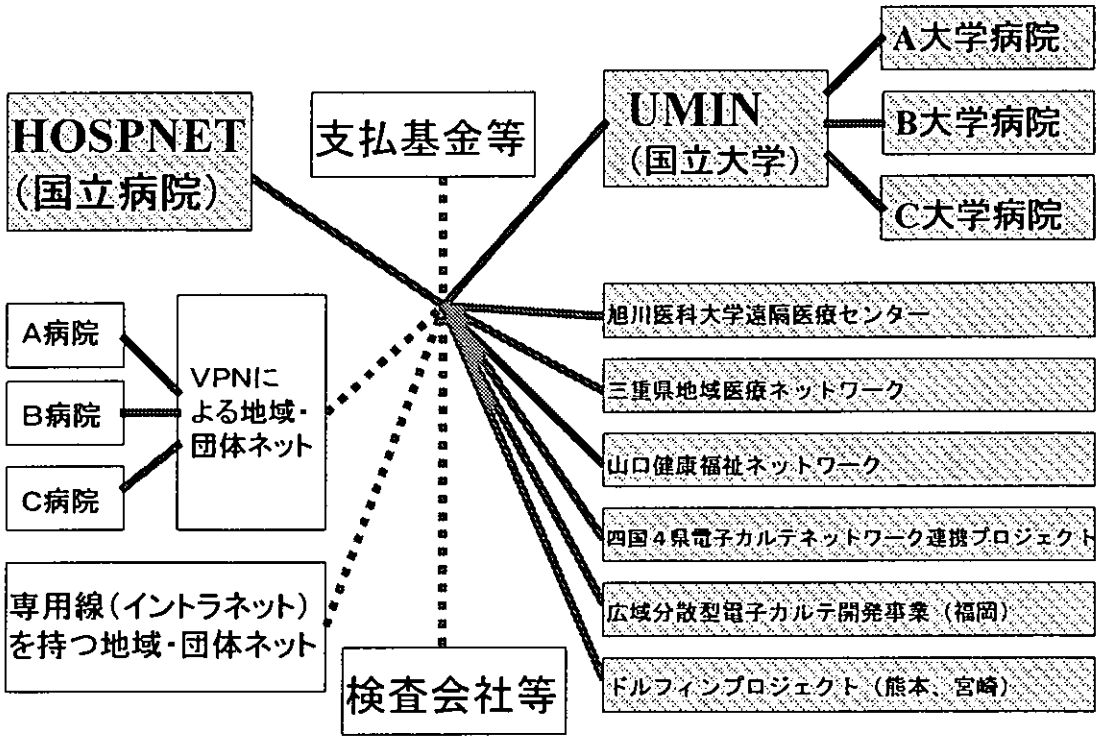


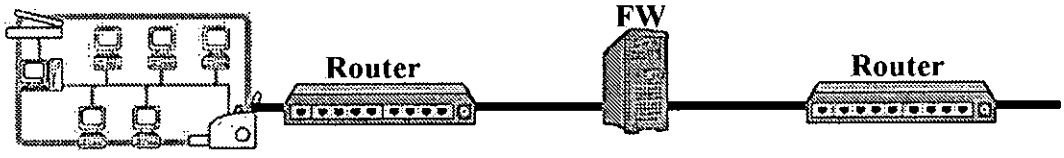
図６－３　平成１６年度以降の展望

資料：　ファイアウォールとVPN機器の接続形態の例

凡例　——　通常の通信　　FW：ファイアウォール

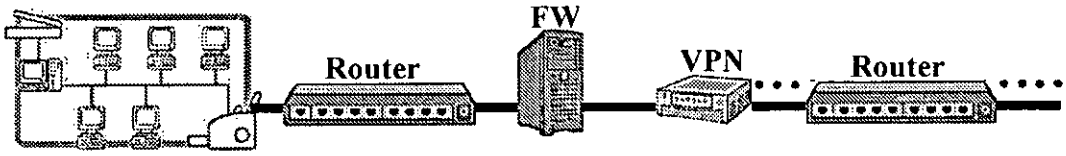
　　・・・・・　暗号化された通信　　VPN：VPN機器

1．VPN機器未設置状態



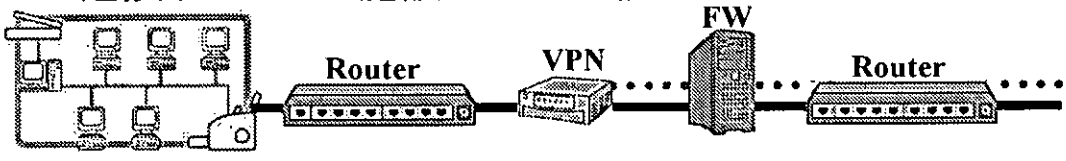
2．VPN機器の直列設置（1）

⇒　危険（VPN-インターネット間の通信にFWが介在しない）



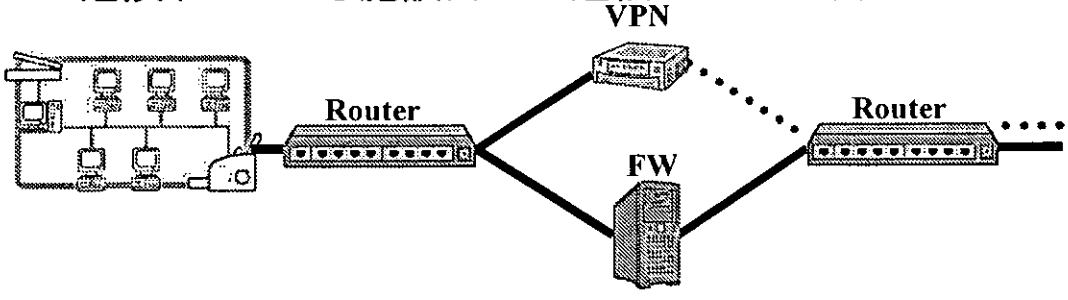
3．VPN機器の直列設置（2）

⇒　危険（VPNから施設内への通信にFWが介在しない）

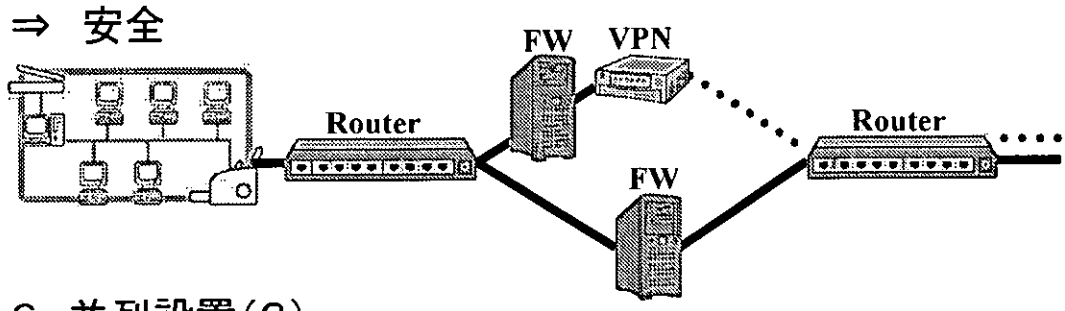


4．並列設置（1）

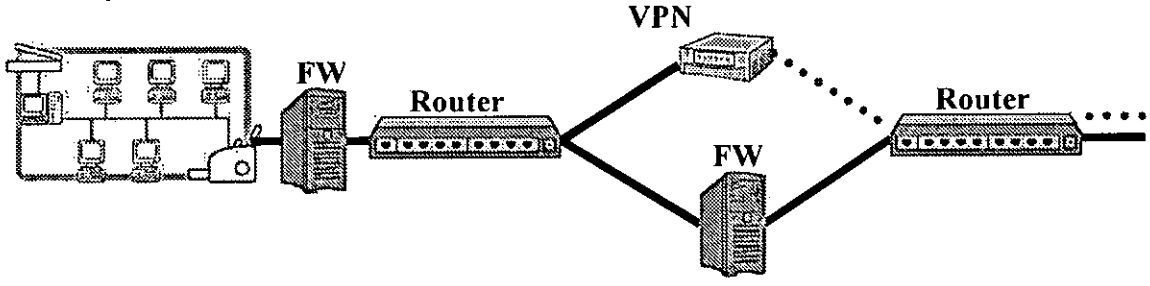
⇒　危険（VPNから施設内への通信にFWが介在しない）



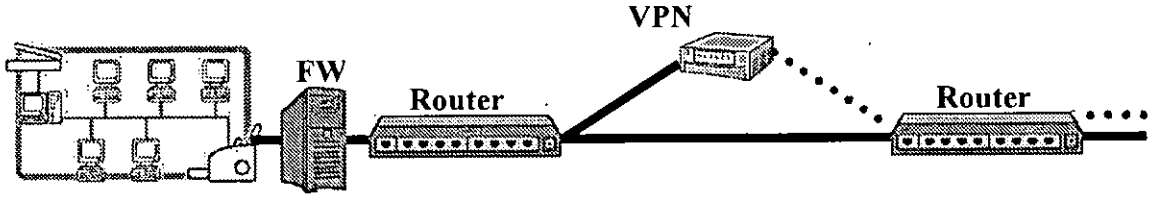
5. 並列設置(2)
⇒ 安全



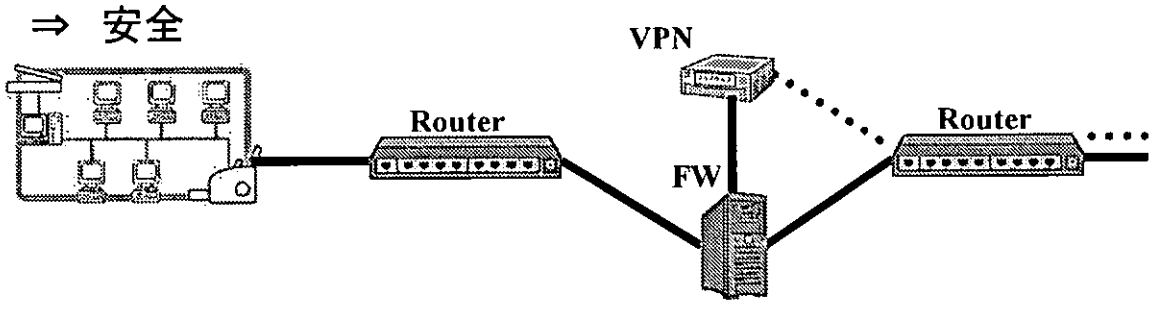
6. 並列設置(3)
⇒ 安全



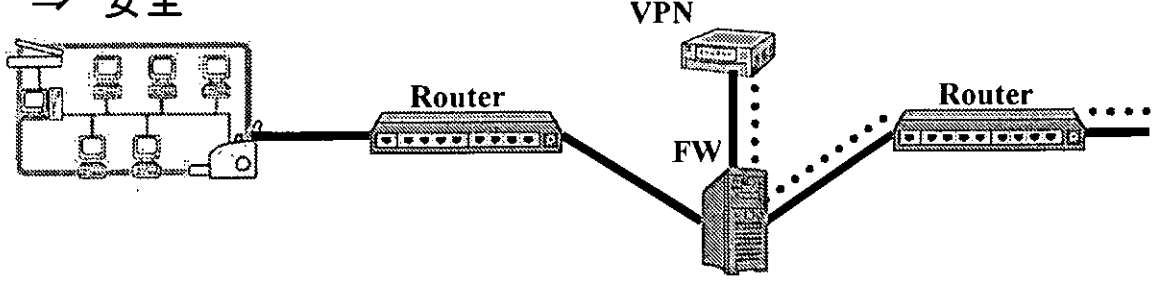
7. 並列設置(4)
⇒ 危険(VPN-インターネット間の通信にFWが介在しない)



8. 並列設置(5)
⇒ 安全



9. 並列設置(6)
⇒ 安全



II. 分担研究報告

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

電子カルテネットワーク等の相互接続法の標準化
ー旭川医大サイトの構築

分担研究者　廣川博之　旭川医科大学医学部附属病院経営企画部　教授
研究協力者　山上浩志　旭川医科大学医学部附属病院経営企画部　講師

研究要旨　旭川医科大学医学部附属病院遠隔医療センターに医療VPNサイト（ドメイン名：asahikawa-med.hvpn.net）を構築するための方法を検討し、実装を行った。IPベースのセキュアで広域な通信インフラが遠隔医療センターに備わることで、当院が進める遠隔医療サービスの形態にもコンテンツの幅が増し、道北地区から全国区へとサービス提供エリアの拡大が期待できる。

A　研究目的

旭川医科大学医学部附属病院遠隔医療センター（以下、単にセンターという）に医療VPN旭川医大サイト（ドメイン名：asahikawa-med.hvpn.net）を構築することを目的とする。

B　センターの情報インフラ

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]。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、施設間に対向でVPN装置を設置したセキュアなネットワーク内で運用している（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、NTSC動画像を外部入力として、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科で行われている。

又、これら直接的な医療支援とは目的を異にするが、2003年10月より「北海道メディカルミュージアム（以下、メディカルミュージアムという）」の構築を進めている。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るもので、旭川市及び近隣市町の住民を対象にテレビ会議システムを用いた遠隔講座が定期的に開催されている[7][8][9]。

センターより提供されるサービスは、ISDN回線（INS64×18回線，INS1500×3回線）、及びADSL回線（12M×1回線，24M×1回線，Bフレッツ×1回線）を利用して行われており、大学や附属病院の情報ネットワークとは独立したネットワークとなっている。

C　研究方法

C.1　医療VPNのためのインフラ選定

医療VPN旭川医大サイト構築に際しては、メディカルミュージアム構想を一層発展させたい考えから、それとリンクした形で構築を行う方針とした。図2にそのイメージを示すが、既契約中のADSL-Bフレッツ回線とOCN-IP8（ドメイン名：med-mm.jp）を共用して、且つテレビ会議システム系には変更を加えずに、データ系通信のためのVPN経路を新たに作成する。テレビ会議システム用ホストPCには、インターネットグローバルアドレスが割り当てられて運用されていること、テレビ会議の品質を優先するためにルータには複雑なセキュリティルールが設定されていないことから、既存のメディカルミュージアムサイトに医療VPNを結合して実装することは容易と考えられた。

C.2　医療VPNサイトでの必要機能

医療VPNサイトを構築する上で、ルータ装置、ファイアウォール装置、VPN装置（以下、装置を各々RT、FW、VPNと略す）が必須である。同時に、各々の装置には運用上必要な機能に留めて、アクセスリスト（フィルタリングルール）を適切に記述することが肝要である。

サイトの運営に必要不可欠なサーバとしては、DNSサーバ、MAILサーバ、SYSLOGサーバ、NTPサーバが挙げられる。SYSLOG及びNTPサーバについてはオプションではあるが、サイト内のセキュリティ管理、保守等の用途の為に用意することが望ましい。このほか、コンテンツ公開のために用意するWWWサーバ、Database（DB）サーバは、DMZ（De-Militarized Zone）に相当するセグメントに配置することが必要となる。

D　研究結果

D.1　ネットワーク構成

医療VPNサイトを図3に示すように構成した。

又、今回用いた機器の一覧を表1に示す。

図中の VLAN#A と VLAN#E（#F,#G,#H,#I も同様）は、遠隔医療センター内の既存ネットワークセグメントであり、この間に挟むように VLAN#B、#C、#D を新たに作成した。

VLAN#C は医療 VPN サイトの DMZ に位置付けられるセグメントとなっており、そこに DNS サーバ、NTP サーバ、WWW サーバ、MAIL サーバ、SYSLOG サーバ、DB サーバの機能を持たせた PC サーバ（OS：Mac OS X server 10.3.3，以下、SERVER という）を1台配置した。DB サーバを除くサーバソフトウエアは、OS に標準添付されているものを用いた。

D.2　セキュリティルール

FW(1)装置については、DMZ → Trusted ポート（VLAN#B → VLAN#C）では、SERVER に対して HTTP、HTTPS、IMAP、SMTP、DNS プロトコルのみ通過させるようルールを設定した。又、Trusted → Un-Trusted ポート（VLAN#C → VLAN#A）では、SERVER がインターネット上のタイムサーバと時刻同期するよう、NTP プロトコルが通過できるようにした。

VLAN#E からは FW(2)及び RT(2)を経由して SERVER にアクセスできるようにし、コンテンツのアップロードや動作確認、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行えるように HTTP、HTTPS、FTP、TELNET、SSH プロトコルを通過させている。

医療 VPN サイト内のフィルタリング動作が正しく機能しているかどうかの確認作業は、nmap（Version 3.0）ツールを用いて実施した（但し、VPN 通信路については後日検証を予定）。

E　考察

医療 VPN 旭川医大サイトより発信する医療コンテンツとしては、現時点ではデータベースサービス、メールサービスを考えているが、クライアントからは WWW ブラウザを通して利用させる方針である。その理由として、セキュリティ上の優位性に加え、SERVER コンテンツへのアクセスが VLAN#A より外側からと VLAN#C より内側からと同一の操作性であること等が挙げられる。

医療 VPN に対応したインフラが当遠隔医療センター内に出来たことで、当院が進める遠隔医療サービスの形態にもコンテンツの幅が増すことが期待できる。又、時期を同じくして、三重、香川、山口、福岡、熊本にも医療 VPN サイトが立ち上がっており、道北地区から全国区へとサービス提供エリアの拡大も期待できる。

VPN 通信では通信路がトンネル化され、流れるデータは隠蔽されるため、インターネット上では生データを伝送するのは危険と判断される情報についても、VPN 通信路であれば安心して流通可能である。現在、旭川薬剤師会（会員数：約 230）でインシデントレポート収集システムの構想があり、これを医療 VPN 内で実装しようと計画している。会員は、VPN クライアントソフトウエアを用いて医療 VPN にアクセスし、インシデント情報を共有することにより、地域住民への安全な医療サービスの提供が期待できる。

F　結論

旭川医科大学医学部附属病院遠隔医療センターに医療 VPN に参加するための必要なインフラ整備を行った。IP ベースのセキュアで広域な通信インフラは、今後当センターでの遠隔医療サービスを一層拡げてゆく足がかりとなるものと期待される。

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：テレパソ路地−の現状・課題・対策と当院における工夫．第7回遠隔医療研究会論文集：76-77，2003.

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

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

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

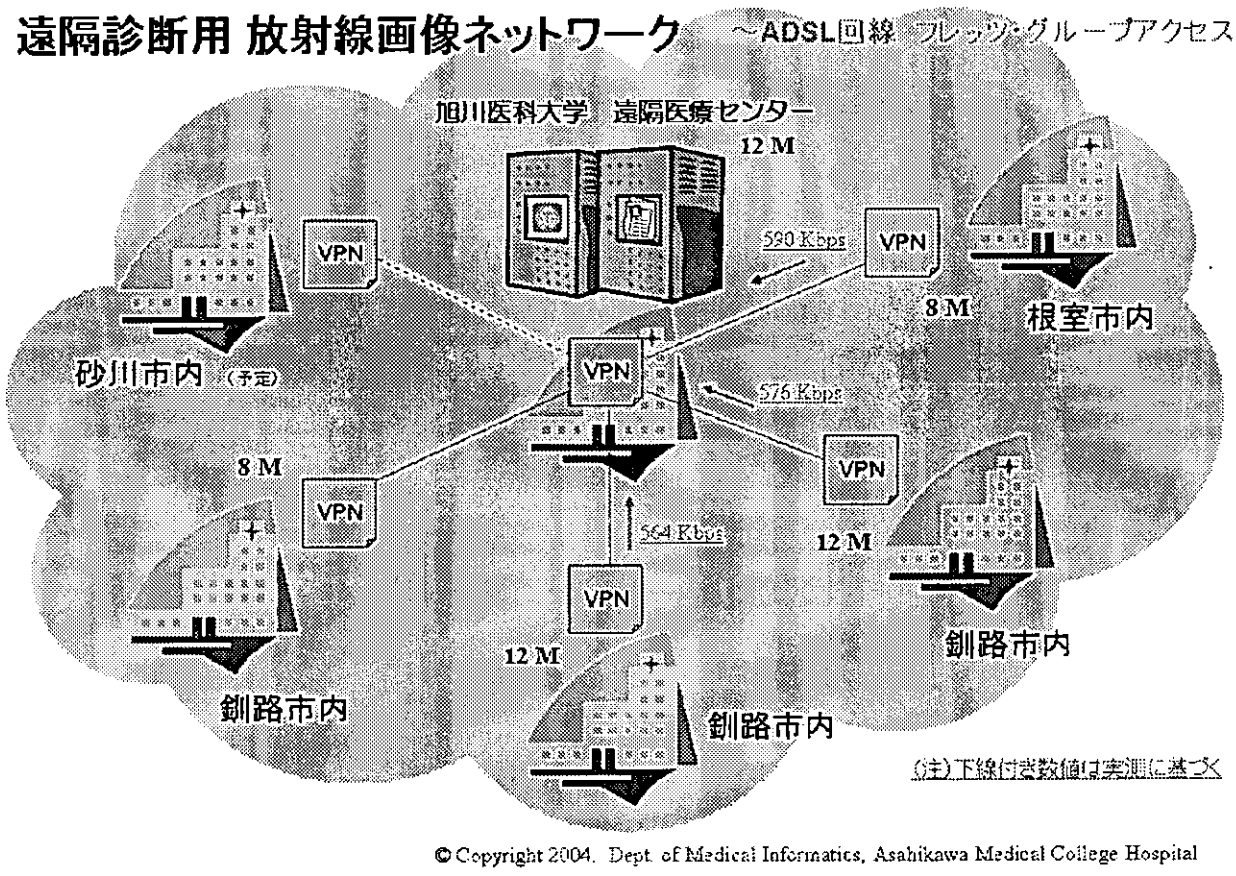


図 1 遠隔診断用放射線画像ネットワーク構成（2004 年 3 月）

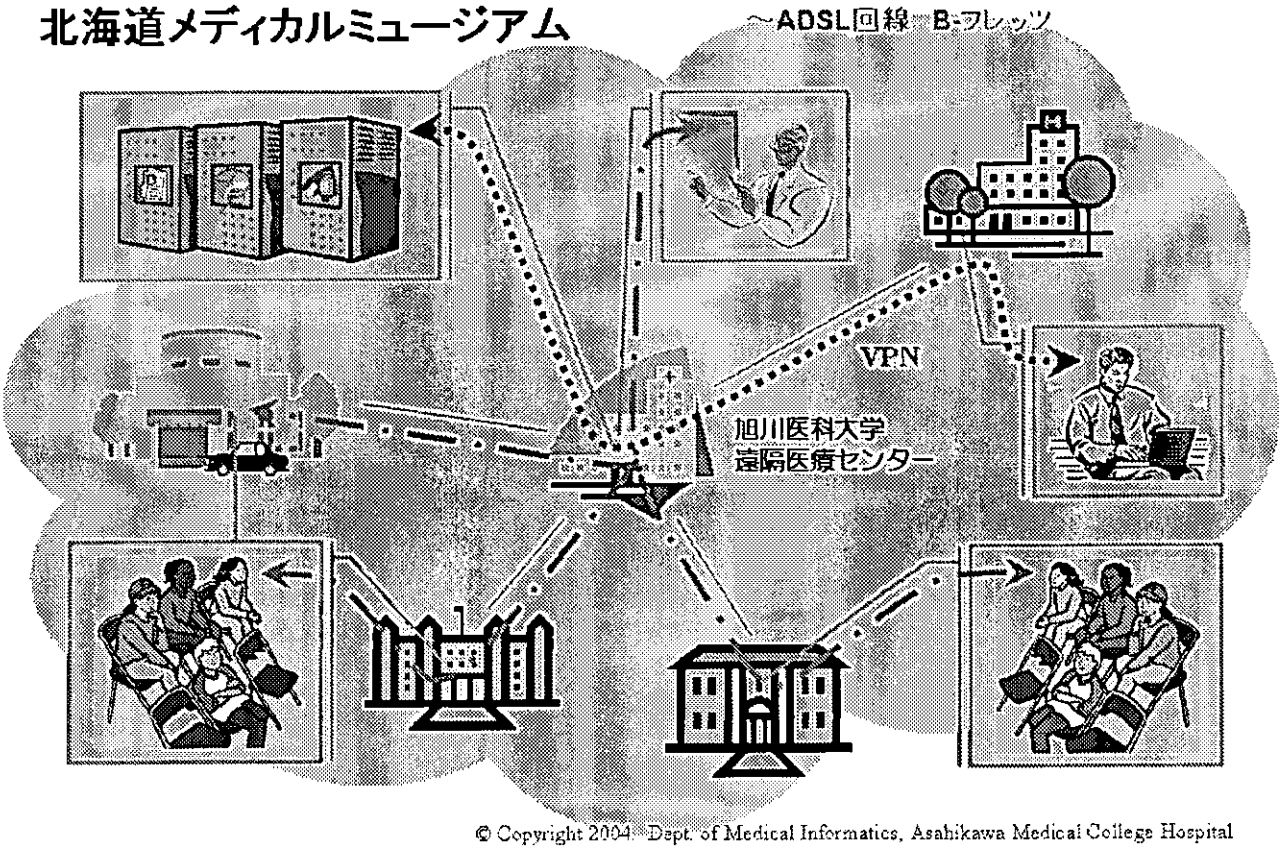


図 2 北海道メディカルミュージアム概念図

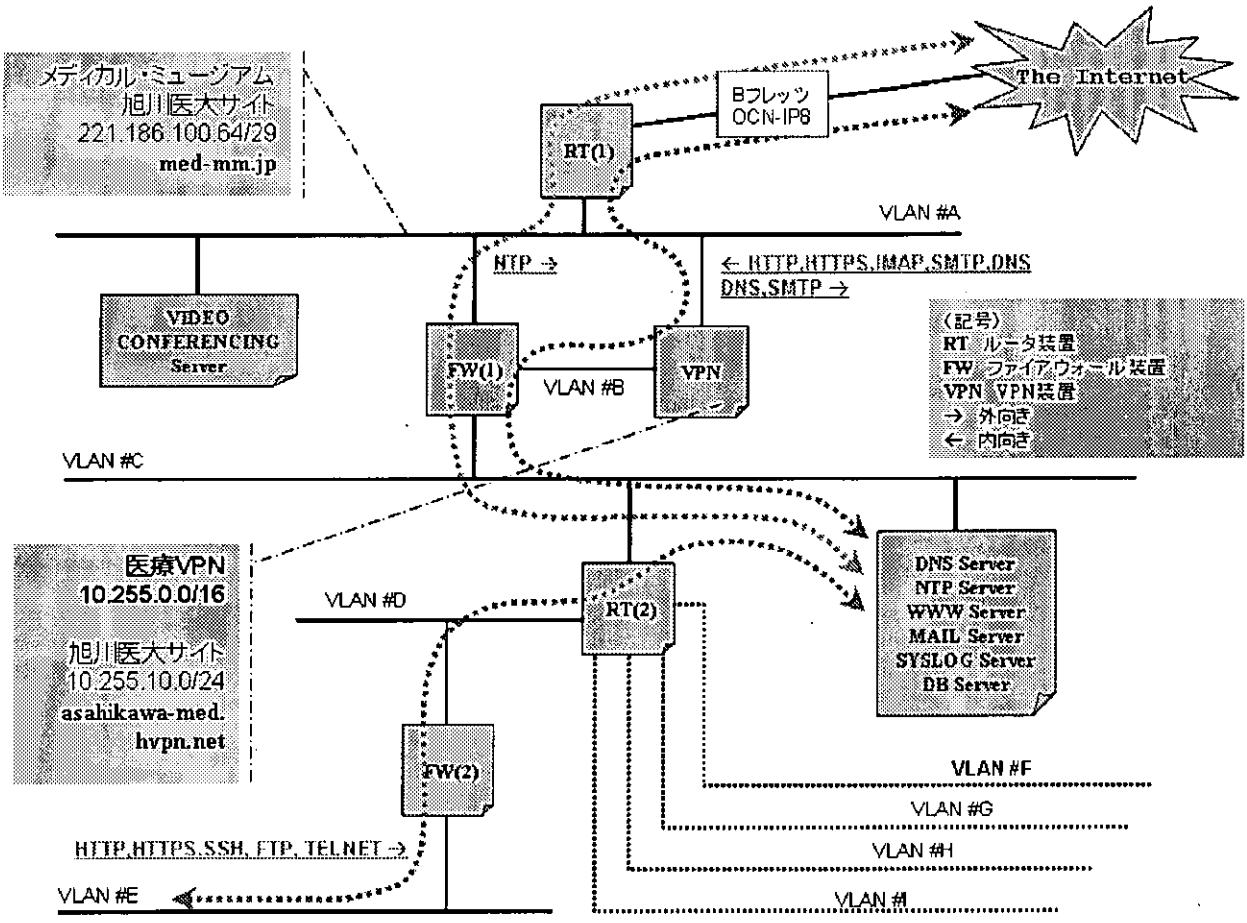


図 3 医療 VPN 旭川医大サイト構成図

表 1 構成機器

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 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