医療用ネットワークシステム構成(図1)に必要となる要件は、以下の通りであった。

医療機関内のネットワーク利用については、

1. 医療機関等の院内LANに接続される端末の正当性を確保し、正当な機器（登録機器）からのみ外部接続を許可すること
2. 医療機関内部の通信の安全性を確保すること
3. 外部接続時の機器利用者を特定し、許可された利用者のみの外部接続を許可すること
4. 院外でモバイル機器を利用する際には、外部モバイル機器は院内LANに対してVPNを利用して接続されること
5. モバイル機器が院内LANに接続される際には機器及び利用者の認証をおこなうこと

が必要となる。また、新たに導入した外部接続管理機関についての要件は、

6. 複数の医療機関からのパケットを分離し処理すること
7. 許可されたWebサイト（ページ）にのみ接続を許可すること
8. 院内LANに接続された機器に対して、名前解決の仕組みを提供すること
9. 証跡管理をおこなうこと

となる。

以上の要件と、昨年度整理した技術的要件の概要を、技術的動向や実現可能性を踏まえて以下の通り再整理した。まず、要件１の院内ＬＡＮで利用する端末の正当性確保を実現する技術的要件として、

1. PCの個別認識をハードウェアで保証するために、機器に組み込まれているチップ、特定ID等を利用した認証の実施すること（例えば、vPro搭載PCの利用、イーサネットボード、CPUやチップセットの中に特定のコードを利用）
2. 不正PC接続検知防止システムを導入すること（登録外のＰＣ等が接続されたことの検知とネットワーク接続の妨害など）

を、要件２のPCなどの機器、ルータ間の通信など医療機関内部の通信の安全性を確保には、

3. 機器とルータ間の通信にはIPAHを利用し

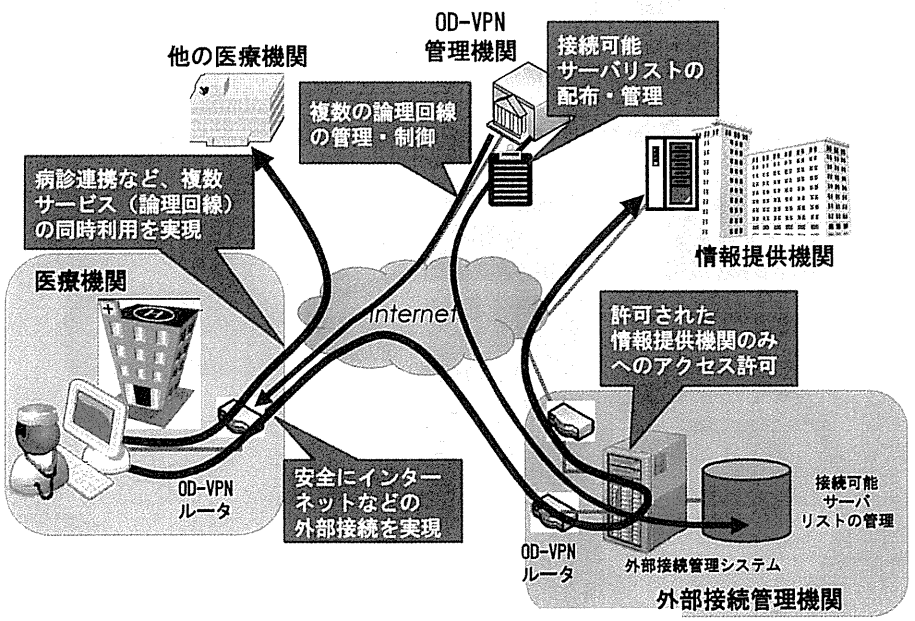


図１　提案システムの全体像

たパケット改ざん防止、VLANによる通信路の仮想化をおこなうこと

を定めた。要件５のモバイル機器の接続については、

4. IEEE 802.1x (EAP-TLS, PEAP)を利用して、無線LAN利用機器の安全性確保を行うこと

が必要であるとした。

また、要件３の機器利用者の識別及びそれに基づく特定機器からの外部接続については、

5. 外部接続利用時の利用者認証を行うこと。利用者認証方法はID, Passwordの利用も可能とするが、ICカード利用を奨励する（但し院内で特定の利用者のみが使用するモバイル端末の場合には、利用者認証だけでなく、機器認証のみでの利用も可能）
6. 利用者がどの機器を利用しているかを確認する必要があるため、認証はOD-VPNルータに対して実施すること
7. OD-VPNルータ又はそれと連携する機器は、機器・利用者情報を紐づけて管理すること
8. 機器認証及び機器利用者の認証が行われている場合のみ外部接続を許可すること

を技術的要件とした。

また、要件６から９の外部接続管理機関の要件を満たす技術的要件として、

9. 医療機関との間はOD-VPNなどVPN技術を利用して接続すること
10. 外部接続機関内では、VLAN技術を利用して複数の医療機関からのパケットを分離し処理すること
11. アプリケーション制御型FWを設置し、アプリケーションレベルで、医療機関から外部接続機関に対する接続ポリシー制御を実施すること
12. ホワイトリスト方式によるWebフィルタリングを実施すること
13. ホワイトリスト対象サイトの管理を行う

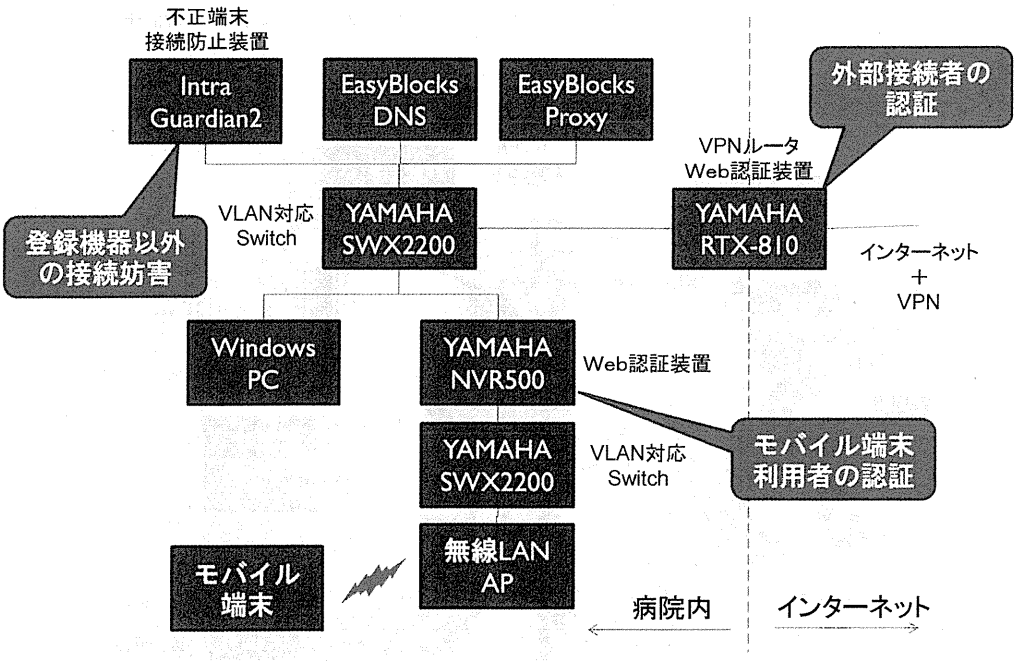


図２　プロトタイプシステムの機器構成（医療機関内）

こと

14. 院内のネットワーク機器に対して名前解決サービスを提供するための DNS 機能を有すること
15. 接続ログを保存すること

を定めた。

そして、これら技術的要件を満たすためのシステムを、図２，３に示す構成のプロトタイプシステムを構築した。プロトタイプシステムでおこなう実験的検証においては、技術的有効性を確認するための装置構成を用いているため、OD-VPN ルータの代替として、既存の VPN ルータを利用（接続先の変更管理は実施しない）している。

以下に技術的要件の実現方法を具体的に記載する。

- 技術要件１については、MAC アドレスを利用し、利用する機器は、すべて MAC アドレスを登録
- 技術要件２については、不正アクセス防止装置として IntraGuardian2 を導入し、MAC アドレスが登録されていない機器のネットワーク利用を防止
- 技術要件３は、外部接続時には、WindowsPC が接続された YAMAHA SWX2200 と YAMAHA RTX810 間で VLAN 接続をおこない、他の機器からの接続を禁止することで実現
- 技術要件 4 は、モバイル機器と無線 LAN アクセスポイント間で WPA2-AES を利用するとともに、YAMAHA NVR500 の Web 認証機能を利用し、モバイル機器利用者の認証をおこなうことで実現。認証が成功した場合のみ院内 LAN への接続を許可
- 技術要件 5-8 は、外部接続用の YAMAHA NVR500 の Web 認証機能を利用し、外部接続利用者の認証を実施することで実現。認証が成功した場合のみ外部接続機関への接続を許可
- 技術要件 9 は、YAMAHA NVR500、YAMAHA RTX-1200 間を IPsec/IKE で接続することで実現
- 技術要件 10 は、YAMAHA RTX-1200、YAMAHA SWX2200 間を VLAN 接続することで、異なる医療機関から RTX-1200 へ接続された通信経路を論理的に分離することで実現

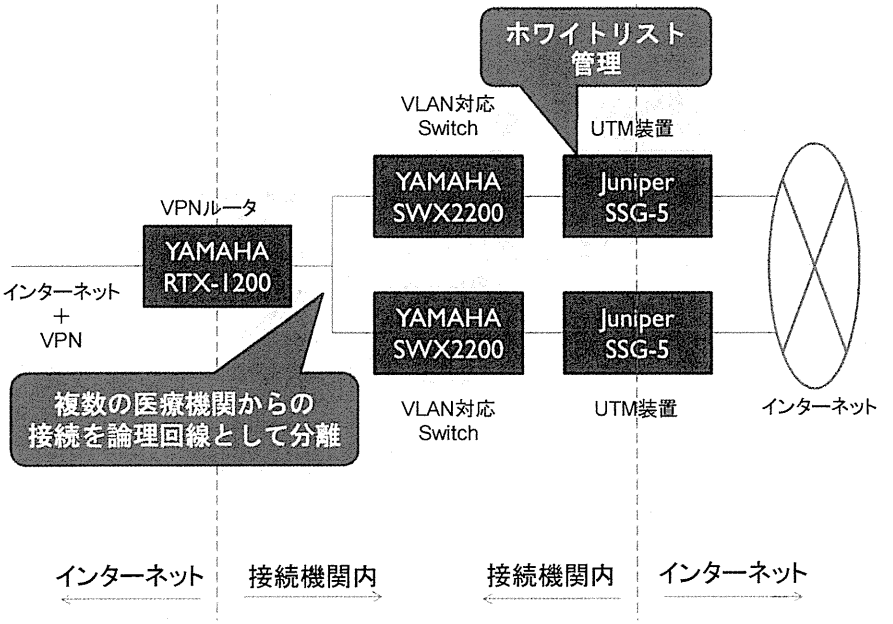


図３　プロトタイプシステムの機器構成（外部接続機関内）

- 技術要件 11-13 は、UTM(Unified Threat Management 、 統 合 脅 威 管 理) 装 置 JuniperSSG-5 を利用し、外部接続時の通信ポート制御と外部接続先 Web サーバのホワイトリスト管理を実施
- 技術要件 14 は、外部接続管理機関内に設置された JuniperSSG-5 の DNS 機能と医療機関内に設置された EasyBlockDNS の DNS サーバ機能を連携さ節ことで実現
- 技術要件 15 については、下記機器のログ機能を利用して実現

以上のプロトタイプシステムを利用して、施設内における機器等の安全性向上に関する機能の検証として、

- 登録外機器を医療機関内 LAN に接続し、通信がおこなえないこと
- 外部接続時の院内機器、ルータ間の通信が、他の院内機器から傍受できないこと
- 登録された利用者のみが外部接続許を行えること
- 正当な手順を実施した場合、医療機関内の PC に対してから医療情報提供サーバの URL を入力することで、接続が可能なこと
- 外部接続機関内で複数の医療機関からの回線が論理的に分離できていること
- 容易に接続可能リストの管理と接続制御が行えること

を確認し、これらが正しく行えることを確認した。

E. 結論

本研究により、医療機関内から外部医療等情報を参照する際に必要となる要件及び技術的実現性を明らかにすることができた。

我々が行った実験では、機器等の設定をオフラインで実施し、接続管理機関内でのネットワークの論理的分離について L2 スイッチを用いた VLAN を利用しているため、これらの設定を OD-VPN の管理者等が実施できる仕組みを整えることが必要となるが、これについては今後、OpenFlow[1] 技術を利用することが考えられる。OpenFlow 技術とは、2009 年 12 月に Stanford 大学により v1.0 が策定したものであり、現在は主なネットワーク機器メーカにより設立された Open Networking Foundation により標準化作業が実施されている。

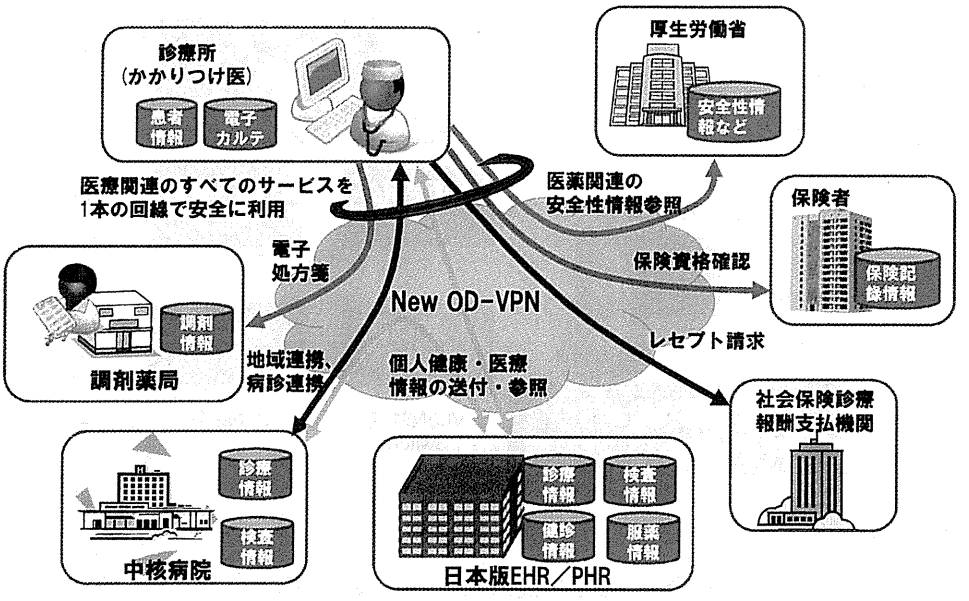


図４　次世代 OD-VPN の将来像

OpenFlow は、L1-L4 の要素を利用してフローを制御するものであり、今回手動で設定を行った、VLAN 対応 Switching HUB などの設定を自動化することが可能になると考えられるが、OpenFlow は、ルータ管理手法ではないため、OpenFlow に対して OD-VPN 技術で培ったルータ管理手法を融合させることで、安全安心な医療情報の連携・流通を可能とするネットワーク基盤である次世代 OD-VPN（図 4）を構築していくことが今後の課題である。

現在、医療機関などではレセプトのオンライン請求を実現するための手段として OD-VPN が利用されており、今後様々なサービスへの応用が期待されていることからも、本研究の成果は、医用機関の内部・外部を問わず統一的なネットワーク管理・運用に必要な仕組みを提供するための標準技術として電子的な医療情報の流通促進に大いに寄与することになると考えている。

Ｆ．健康危険情報

特になし

参考文献

[1] OpenFlow Switch Specification, Version 1.1.0 Implemented, http://www.openflow.org/documents/openflow-spec-v1.1.0.pdf, February 28, 2011

研究成果の刊行に関する一覧表

雑誌

発表者氏名	論文タイトル名	発表誌名	巻号	ページ	出版年
大山永昭	年金業務の改善とマイポータル	年金時代	40巻14号	13	2011
小尾高史、大山永昭	シームレスなサービス利用を可能とするセキュアネットワーク基盤の実現に向けて	月刊基金	52巻5号	2-4	2011
安藤　裕	画像ネットワークの基礎知識	臨床画像	27巻5号	556-570	2011
安藤　裕，向井まさみ，奥田保男	電子カルテと他システムの連携	映像情報MEDICAL	44巻2号	168-176	2012
安藤　裕	放射線治療専門病院における放射線治療情報システム	Rad Fan	10巻3号	39-42	2012

随筆

年金業務の改善とマイポータル

大山　永昭

我が国の公的年金制度には、国民年金、厚生年金等があり、我々の老後の生活を支える重要な基盤になっている。これらの年金制度は、世代間扶養を基本とする賦課方式であることから、財源不足を補う等のために、これまでしばしば制度変更が行われてきた。そして制度変更や移行時の特例措置等に加えて、婚姻や職種変更等にともなって年金の資格や種別が変わることがあり、結果として、年金の納付記録の管理や給付額決定等の事務作業を極めて複雑かつ煩雑にしている。特に、年金記録の管理に用いられる加入者の氏名、住所、生年月日等に何らかの不備や間違いがあると、当該記録の持ち主の特定ができなくなり、宙に浮いた五、〇〇〇万件の年金記録問題に繋がった。

年金記録を個人別に管理するため、基礎年金番号が一九九七年に導入された。この番号の導入により、年金加入者の特定は可能になったが、年金手帳を基に発番されたため、例えば複数の年金手帳を持っている方には、複数の番号が払い出された。この問題解決には、住民基本台帳との突合が有効なため、二〇〇六年から現況確認の廃止等を目的として、住基ネットの利用を開始した。その後、未統合記録問題に住基ネットが利用され、これまでに住所情報等の判明により四五〇万件以上の未統合記録が解消されてきた。

二〇一一年一月末に社会保障・税の共通番号に関する基本方針が策定・公表された。その後、同年七月には社会保障・税番号大綱が公表され、現在、同法案が準備されている。これまでに公表された大綱等には、新たな番号は、住民票コードに基づいて発番されること、個人情報の連携に関するログの確認を可能とするマイポータルが用意されること等が記されている。従来、年金加入者に住所や氏名の変更等が生じた際には、本人または雇用主等からの届出が必要であったが、これらの新たな基盤が整備されれば、連携基盤経由で移動等の変更が生じたことを通知することが可能になる。また、既存のねんきんネットの機能に加えて、年金の種別や資格変更、登録された住所の確認、変更請求等もマイポータルから可能になる。さらに、自治体や健康保険組合、金融機関や各種の保険会社等のサービス提供機関と本人との相互連絡も、順次、マイポータル経由で行える。マイポータルは個人情報のログ確認に加えて、官民連携を含めた様々なサービスの利用を可能にすることから、その利便性は飛躍的に高まると思われる。マイポータルの利用者が増えれば増えるほど、年金関連の事務手続きに要する手間と時間を大幅に縮減できるとともに、うっかりミスや重要な手続きの失念も無くなると期待される。

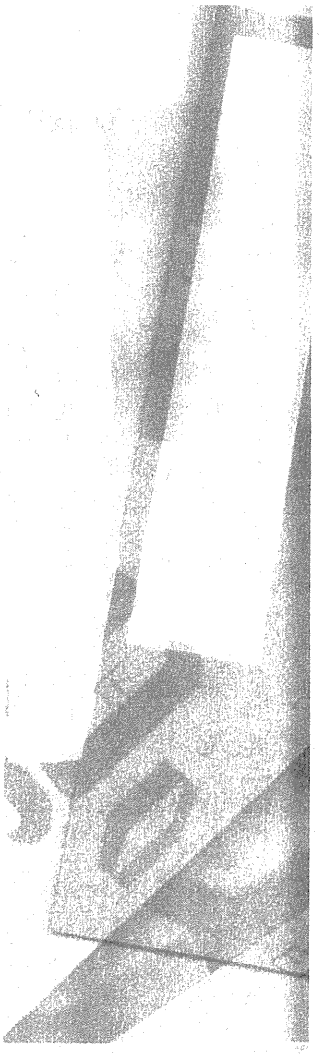
年金記録を正確かつ確実に管理するには、基礎年金番号の重複付番を解消しなければならない。そのためには、個々の基礎年金番号を住民票コードに紐付けることが効果的である。この作業は正確かつ迅速に行うことが望まれるが、住民票と異なる住所を登録している方の紐付けには、多くの手間と費用を要すると危惧されている。効率的な作業を進めるためには、加入者も参加して年金の登録住所を確認することが必要である。

（おおやま・ながあき）
1954年生まれ。82年東京工業大学総合理工学研究科物理情報工学専攻博士課程修了。88年同大学助教授、93年同教授を経て2010年4月より同研究所教授。専門分野は医用画像工学、社会情報流通システム工学等。工学博士。厚生労働省の検討会等でも要職を歴任。

特別寄稿

シームレスなサービス利用を可能とするセキュアネットワーク基盤の実現に向けて

東京工業大学　大学院総合理工学研究科　物理情報システム専攻　准教授　小尾　高史
東京工業大学　像情報工学研究所　教授　大山　永昭



はじめに

近年の情報技術の進展に伴い、医療分野においても診療データの外部保存、レセプトのオンライン申請など、ネットワーク技術が様々な場面で利用されている。このような状況の下、今後、医療サービスの安全性・信頼性等の向上をさらに推し進めるために、患者情報の一元管理、共有等を通した医療関連機関間の連携強化や、医療機関内外に存在する最新の医療情報などを医師等が容易に参照可能となることが望まれている。

これらを実現するには、病院内に保存されている個人情報などが漏洩しないための対策をとることが極めて重要であり、全ての医療機関が安全に利用できるセキュアなネットワーク基盤の構築が求められている。

本稿では、医療分野の情報連携に必要となるセキュアなネットワーク基盤の構築を目的として開発されたオンデマンドVPN（Virtual Private Network）をあらためて紹介し、オンデマンドVPNが持つ課題とその解決策について解説する。

医療分野で必要なネットワーク基盤の要件

医療機関等が外部の組織と医療情報の交換を行う際に必要となる、個人情報保護およびネットワークのセキュリティに関する留意事項は、2010年2月に改訂された「医療情報システムの安全管理に関するガイドライン第4.1版」[1]に記述されている。このガイドラインでは、ネットワークを利用して医療情報を外部と交換する際には、「送付すべき相手に」、「正しい内容を」、「内

小尾（おび） 高史（たかし）氏

【略歴】
1967年 東京都生まれ
1995年 東京工業大学大学院総合理工学研究科物理情報専攻博士後期課程満期退学
同年　同大工学部附属像情報工学研究施設教務職員
1997年 同助手
2003年 東京工業大学総合理工学研究科物理情報システム専攻助教授
2008年 現職
【専門分野】
医療画像処理、情報セキュリティ　博士（工学）

大山（おおやま） 永昭（ながあき）氏

【略歴】
1954年 神奈川県生まれ
1982年 東京工業大学大学院総合理工学研究科物理情報工学専攻博士課程修了
1983年 東京工業大学工学部附属像情報工学研究施設助手
1986～1987年 アリゾナ大学放射線科研究員（画像再構成についての研究）
1988年 東京工業大学工学部附属像情報工学研究施設助教授
1993年 現職
【専門分野】
医用画像工学、光情報処理　工学博士

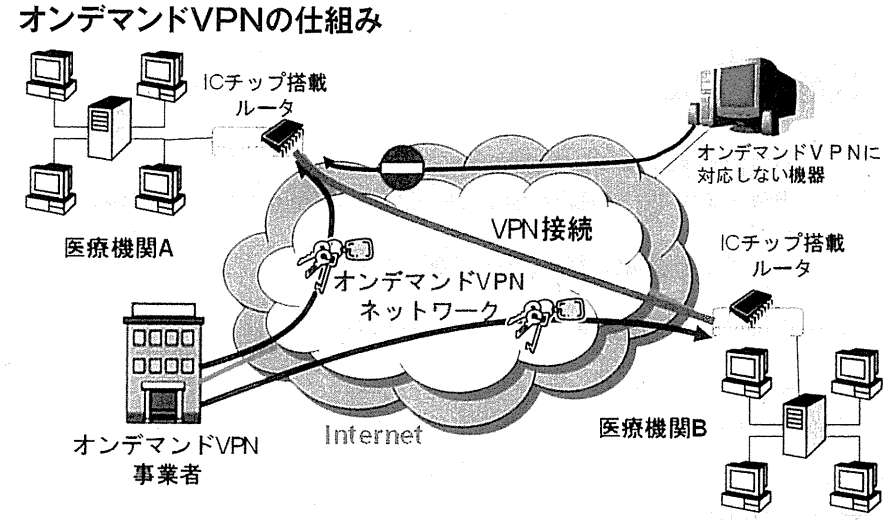
容を覗き見されない方法で」送付しなければならないとされており、送信元から送信先へのネットワーク経路において、送信元や送信先を偽装する「なりすまし」や送受信データに対する「盗聴」および「改ざん」、通信経路への「侵入」および「妨害」などの脅威から送受信する情報を守ることが必要であるとされている。

そのため、医療分野で利用されるネットワーク基盤には、①ネットワーク経路における安全性の確保、②データ送受信時における相手確認の実施、③正規利用者、許可機器などへのなりすましの防止、④送信する情報に対する暗号化などのセキュリティ対策の実施、⑤情報通信に関連する組織間における責任分界点、責任の所在の明確化、⑥安全性の確認できるネットワーク機器の利用および設定された経路以外での通信が不可能となる経路設定の実施、などが要求されている。

オンデマンドVPNとは

現在のブロードバンドの普及状況や導入コストなどを踏まえると、任意の組み合わせで必要な医療情報の連携を可能とするネットワーク基盤を構築するには、インターネットのようにオープンなネットワークをベースにすることが、効果的かつ効率的であると考えられる。しかしながら、オープンなネットワーク上には、「盗聴」、「侵入」、「改ざん」などのさまざまな脅威が存在することから、十分なセキュリティ対策を実施することが必須であり、そのための有効な対策としてVPN技術が広く利用されている。一般的にVPNは、インターネット等のオープンなネットワーク上に、暗号化技術を用いて仮想的な専用回線を実現する技術の総称であり、インターネット上を流れるデータの暗号化を行う「IPsec（IP security protocol）」と、暗号化通信に必要な鍵交換を行う「IKE（Internet Key Exchange）」と呼ばれる技術を組み合わせたものが広く普及している。しかし、このような技術を利用するには、VPNルータに対してさまざまな設定を行うことが必要であり、従来は専門のネットワーク技術者が手作業で実施していたため、VPN開設や接続機関の設定・変更等に多くの費用と時間を要するという課題が残っていた。また、鍵の設定ミスなどによりルータの管理・運用が正しく行われない場合には、設定情報の漏洩等の危険性が生じることから、セキュリティ面での不安などが指摘されていた。

これらの課題を解決し、誰もが安全かつ手軽にセキュアなネットワークを利用可能とするために開発された技術が、オンデマンドVPNである。オンデマンドVPNで使用されるルータには、2階層PKI技術が実装された耐タンパー性を有するICチップが搭載されており、この技術により、情報漏洩や盗聴の可能性があるインターネット環境においても、安全にVPN構成情報を配送し、任意の多地点間で安全なネットワークを構築することが可能になった（図参照）。また、オンデマンドVPNを利用することで、医療機関は、通信経路上の管理責任の大部分をオンデマンドVPN事業者に委託することが可能になるため、医療機関側の負担を大幅に減じることが可能になった。現在、オンデマンドVPNは、レセプトのオンライン請求、一部地域における病診連携等に利用されており、特にレセプト請求については現在4社よりVPNサービスが提供され、すでに多くの医療機関がインターネットを利用して外部機関と接続可能なネットワーク環境が構築されている。



シームレスなサービス利用を可能とするオンデマンドVPNを目指して

オンデマンドVPNの登場により、インターネットを通信路として使用した安全な医療情報の共有・交換・利用が可能となり、医療サービスの質向上に加えて、医療従事者、患者双方にとってメリットのあるさまざまな医療サービスの実現が可能になると期待されている。

しかし現状のオンデマンドVPNでは、医療機関内に置かれる端末等を経由する回り込みなどの問題から、一本のVPN回線を利用して複数のサービスをシームレスに利用することは難しい。そのため、たとえばレセプトのオンライン請求で利用する回線においては、現時点で他のサービスと共用して利用することができない状況となっている。

この問題を解決するには、端末認証の仕組みや内部データの流出を防止する技術、複数のサービスで利用する回線を論理的に分離する技術などの組み合わせが有効と考えられる。この新しい技術の導入による効果は、具体的には、たとえばレセプトのオンライン申請や病診連携等の医療用サービスと、一般的なインターネットを経由するサービスを、一つのVPN回線で利用できることであり、利用者にとっての利便性が大幅に向上すると期待されている。

また、複数事業者から提供されているオンデマンドVPNサービスは、その実装方式に若干の差異があるため、異なる事業者が提供するオンデマンドVPNネットワーク間の接続が困難であることや、通常インターネットで利用されているような名前解決の仕組みを持たないため接続先の特定が容易ではないなどの課題がある。前者については、実装方式の標準化や異なる事業者が管理するネットワークを接続するIX（Internet eXchange）と呼ばれる接続機能の実現が有効な解決策と考えられている。後者については、安全性の観点から医療分野でのみ共通に利用できる独自のDNS（Domain Name System、IPアドレスとホスト名を関連付けて管理する仕組み）の構築が必要であると考えられる。そして、これらの課題を解決するための具体的な取組みも開始されている。

おわりに

オンデマンドVPNは、さまざまな分野であらゆる利用者がシームレスにサービスを利用できる安全なネットワーク環境の実現を目指して開発が進められてきた。今後、オンデマンドVPNが医療分野における各種サービスの連携を支える基盤へと発展することが期待される。

参考資料　[1] 医療情報システムの安全管理に関するガイドライン第4．1版，厚生労働省
http://www.mhlw.go.jp/shingi/2010/02/dl/s0202-4a.pdf

画像ネットワークの基礎知識

安藤　裕

ネットワークを利用して画像システムを構築する場合に必要となる基礎知識について解説する。ネットワークは，PACSを構成する重要なインフラストラクチャーであり，図1に示すように画像検査機器(モダリティ)，画像サーバ，表示装置を結ぶ重要な装置である。またネットワーク上において画像を伝送する場合の伝送手順(プロトコル)やデータの安全性なども必要となる。そこで，以下のようなネットワークに必要な技術について述べる。

・標準化はなぜ必要か？
・ネットワークに関する常識
・伝送手順はDICOMそれともHTTP？
・電子署名・暗号化技術を使用すれば安全に伝送できるか？

標準化はなぜ必要か？

標準化とは，「標準を設定して，これを活用する組織的行為」(JIS[1])と定義されている。病院など医療機関で，あらかじめ使う器具/道具などを決めたり，医療の手順を一定に決めておくことが標準化*1である。

ネットワークで標準化が行われていないと大変なことが起こる。表1に示すような問題が生じる可能性がある。このような問題点を解決するためには，標準化を推進する必要がある。

画像システムの場合，あらかじめ使う情報システムやデータフォーマットなどを決めておいたり，業務の手順を一定に決めておいたりすることが標準化である。また，標準化することにより，システムの構築や更新が容易になり，ワークフローも均一となる。

標準化により，一定の枠にはめるので自分の好きなシステムや業者の独特の装置をつくったり使用したりすることはできなくなる反面，標準化された画像システムでは，システムの統合や連携において，システムの定義やインターフェース部分などの膨大な労力を省いてくれる便利な手法である。

用語アラカルト

＊1 標準化(standardization)とは？

標準化することにより，教育が簡単になり，誰がしても，迅速な処理ができ，かつ処理の結果も均一となる。

・自由に放置すれば，多様化，複雑化，無秩序化する事柄を少数化，単純化，秩序化すること。
・また，標準(＝規格：Standards)は，標準化によって制定される「取り決め」。標準には，強制的なものと任意のものがあり，一般的には任意なものを「標準(＝規格)」とよんでいる。メートル法は，強制される例。

画像診断医に必要なネットワークに関する常識

LANとWAN

LAN(Local Area Network；構内情報通信網)[2]は病院内など比較的小さい敷地をカバーするネットワークをさす。一施設の建物間などをつないで，高速かつ大容量の通信を行うことが可能である。

Ando Y：放射線医学総合研究所重粒子医科学センター病院

　0911-1069/11/¥400/論文/JCOPY

図1　画像システム(PACS)の構成

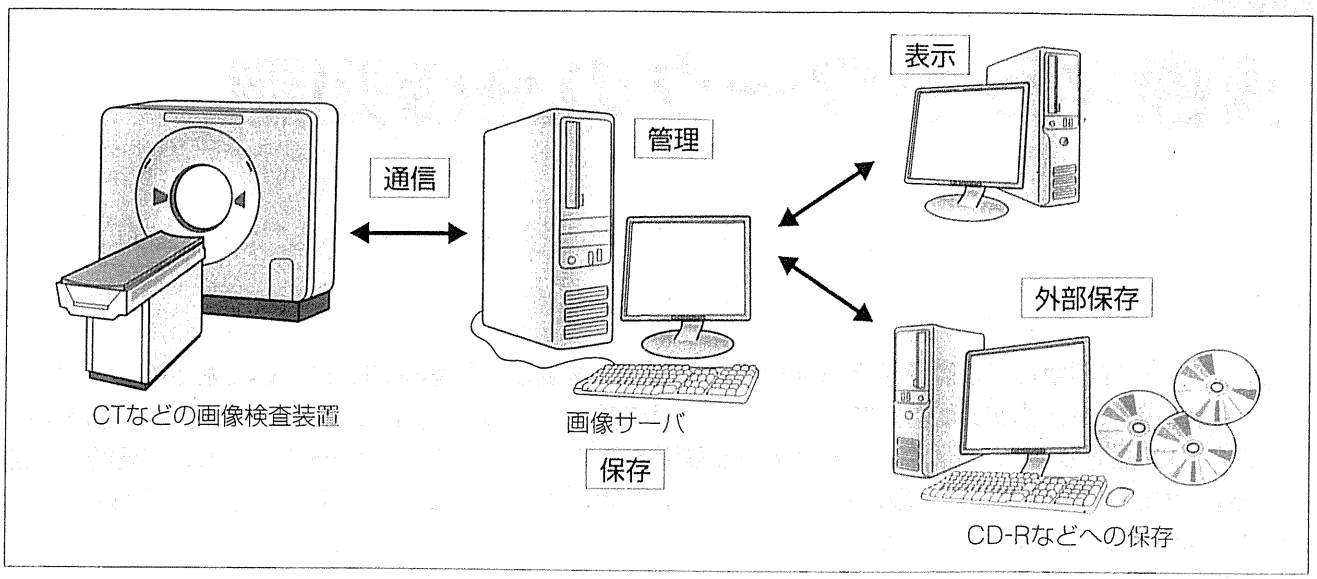


表1　標準化されていないことにより起こる問題

番号	項目
1	CT装置を入れ替えたら，ネットワーク機器を交換しなければならない
2	ネットワークのスピードを速くするために，非常に高額なネットワーク機器が必要となった
3	自由に機器の選択ができない
4	モダリティと更新したら，HISやRISとの連携がうまくできなくなった

一方，WAN(Wide Area Network；広域ネットワーク)は，遠隔地の複数のLANを相互に接続するネットワークをさし，スピードはLANに比べて遅い。

これらは相対的な概念であり，カバーする広さ，通信方法，通信媒体などでLANとWANの区別が明確に定義されているわけではない。一般的には，会社や病院が独自に用意しているネットワークがLANであり，通信事業者が提供している回線がWANとなる(**図2**)。

ネットワークとサブネット(図3)

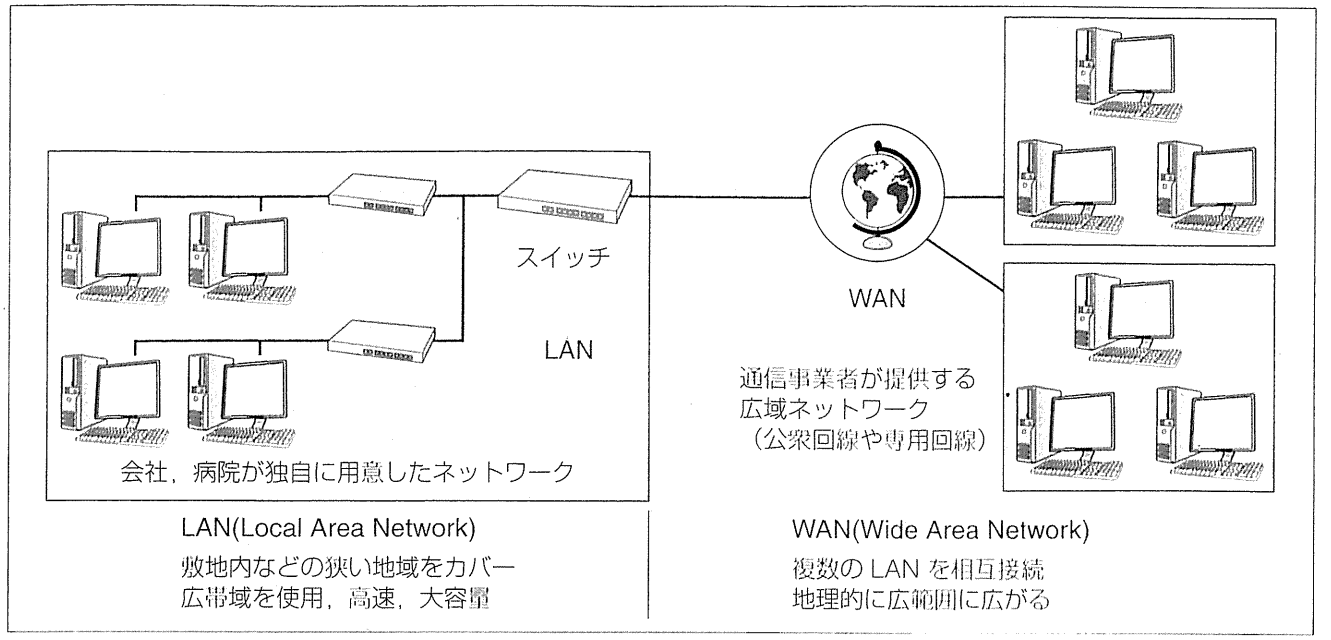
ネットワークは相互に通信を行う機器単位であり，明確な構成単位は決まっていない。ネットワーク層の中継機器(ルータやレイヤ3スイッチ)で分割されたネットワーク単位をさす。

ネットワークは1つまたは複数のセグメントから構成され，ネットワーク内で送受信する通信は，直接外部に送信されることはない。サブネットはネットワークを構成している分割されたネットワ

Pitfall　標準化のメリット

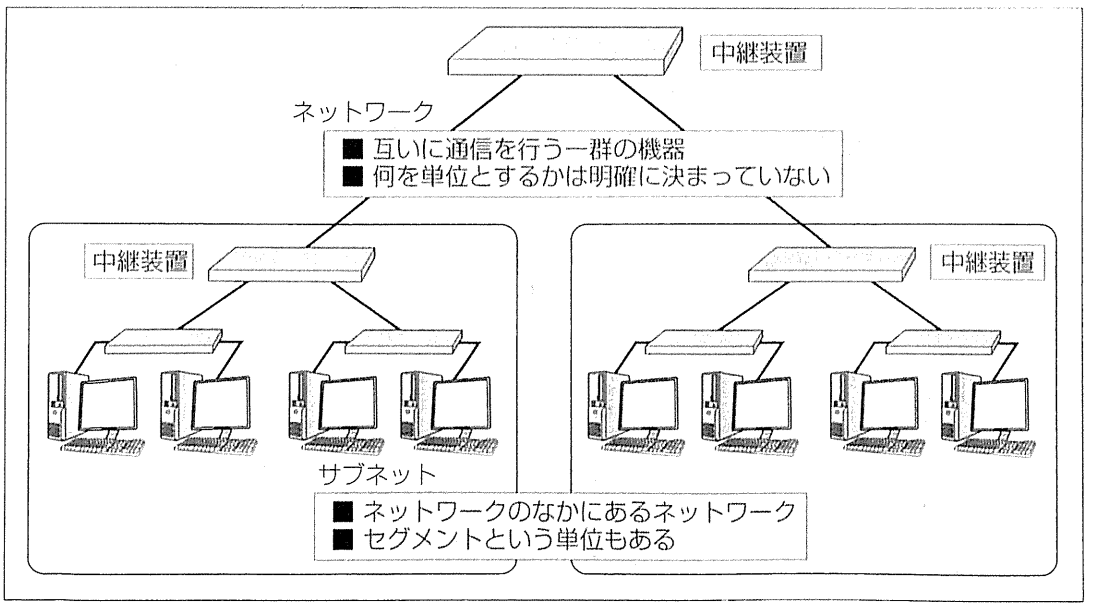
- 標準化のメリットとしては，以下に示すような特長がある。
  ①マルチベンダーの実現
  ②ネットワークによるシステム(リソース)の効率的な利用
  ③放射線情報システムや病院情報システムとの連携が可能となる。

図2　LANとWAN



LAN(Local Area Network：構内情報通信網)は敷地内など比較的小さい地域をカバーするネットワークをさす。一般に比較的広い帯域幅を使用していることが多く，高速かつ大容量の通信を行うことが可能である。
一方，WAN(Wide Area Network：広域ネットワーク)は，地理的に離れている複数のLANを相互に接続するネットワークをさし，一般的に狭い帯域幅で通信を行う。
これらは相対的な概念であり，地理的な広さ，通信方法，通信媒体などで LANとWANの区別が明確に定義されているわけではない。
現実的には，会社や病院が独自に用意しているネットワークがLAN，通信事業者が提供している回線がWANに相当する。

図3　ネットワークとサブネットの関係



ネットワークは，サブネットで構成され，各サブネットは，中継装置で接続されている。
ネットワークは互いに通信を行う機器群であり，明確な構成単位は決まっていない。一般的にはネットワーク層の中継機器(ルータ・レイヤ3スイッチ)で分割されたネットワークグループのことをいう。ネットワークは1つまたは複数のセグメントから構成され，ネットワーク内のノード管で送受信するパケットは，直接外部に送信されることはない。サブネットはネットワーク中にあるネットワークである。IPアドレスのネットマスクの設定においてネットワークアドレス長を変えることにより，ネットワークの構成を変化させることができる。セグメントは，ネットワークを拡張する場合にデータ・リンク層の中継機器(ブリッジやレイヤ2スイッチ)で分割されたネットワークグループをいう。このネットワークグループ内に送信したデータはグループ内のすべての端末に伝えられる。

図4　ネットワークの構成機器(ファイアウォール，ルータ，スイッチングハブやハブ，無線アクセスポイントと無線ネットワーク子機など)

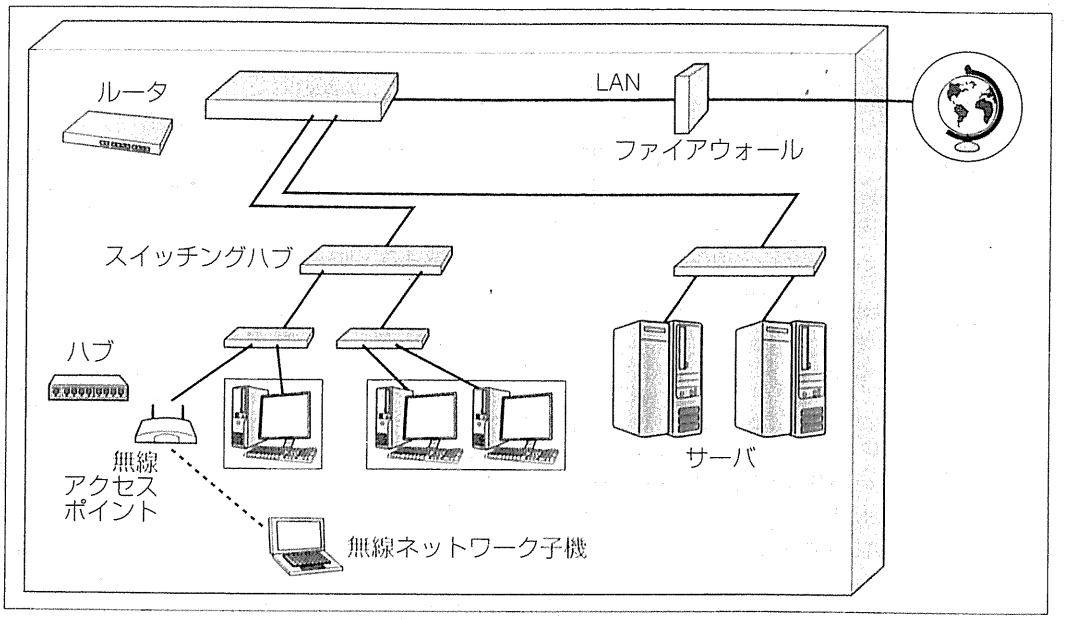
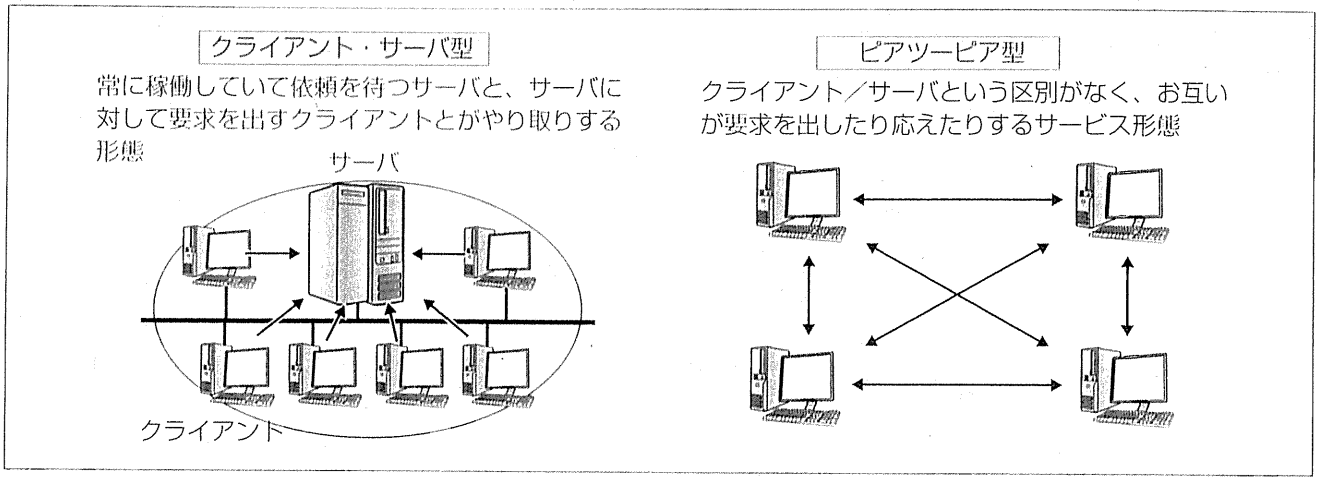


図5　ネットワーク上のサービス形態



ークである。サブネット内は，自由に通信できるが，1つのネットワークの内部にある複数のサブネット間の通信は，設定により通信の自由度が変化する。

ネットワーク構成機器

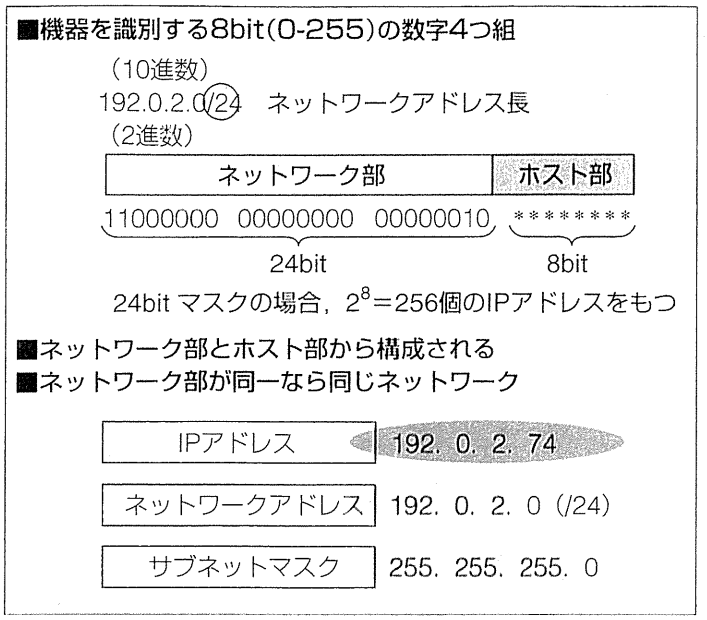
ネットワークを構成する機器は，**図4**に示すように，ネットワークを中継する中継装置であるルータ，ネットワークの通信を伝達するスイッチングハブやハブなどの構成機器からなる。また，無線ネットワークを使用する場合は，無線アクセスポイントと無線ネットワーク子機などが必要となる。

また，構内のネットワークを外部と接続するためには，ファイアウォールとよばれる通信の関所を設けて，必要な通信だけ許可し，不要な通信を遮断する機器が必要となる。

ネットワークのサービス形態(クライアント・サーバ型，ピアツーピア型)

ネットワーク上のサービス形態を**図5**に示す。病院で使用されているPACSは，クライアント・サーバ型[3]になる。クライアント・サーバ型は，サービス提供のために常に稼働して依頼を待ち受けるサーバ(画像サーバ)と，必要時にサーバに対して要求を出してサービスを受ける画像表示端末(クライアント)が情報をやり取りする形態である。ほかにも，電子カルテ，オーダリングシステム，

図6　IPアドレス



IPアドレスは32ビットの2進数であり，8ビットごとに4つのオクテットに分けて扱うことが多い。IPアドレスを記述するときもオクテットごとに10進表記するのが普通である。IPで通信するためには，それぞれの機器にIPアドレスを割り当てる必要がある。

IPアドレスの先頭寄りの何ビットかは，インターネット上のどのネットワークかを表す「ネットワーク部」で，それより後ろの部分は，ネットワーク中で機器を特定するための「ホスト部」である。ネットワーク部とホスト部がそれぞれ何ビット長かはネットワークによって異なるが，ネットワーク部の長さを記述するのがサブネットマスクである。サブネットマスクは，ネットワーク部に相当するビットが1，その他のビットが0という値をもち，例えばネットワーク部が16ビット長の場合のサブネットマスクは，11111111.11111111.00000000.00000000つまり255.255.0.0となる。

PACSなどの病院情報システムや，World Wide Web(WWW)をはじめとするインターネット上のサービスの多くは，クライアント・サーバ型で提供されている。

一方，ピアツーピア型[4]では，サービスを提供する/される側という役割が動的に変化し，多数のコンピュータがサービスを提供したりされたりしながら通信する構成をさす。ピアツーピア型の構成は，拡張が簡単でコストを抑えられるが，安定した稼働や通信速度を確保するのは難しい。

ネットワークのアドレス

ネットワークに接続する機器には，必ずアドレスが付いている。このアドレスをIPアドレス[5]とよび，IPアドレスでネットワーク内の通信が可能になる。IPアドレスは現在の第4版では32ビットの2進数からなり，8ビットごとに4つに分けて扱う。IPアドレスを記述するときは，xxx.xxx.xxx.xxxと10進表記するのが普通である。

IPアドレスは，先頭からnビットが，インターネット上のどのネットワークかを表す「ネットワーク部」で，それより後ろの32-nビットは，ネットワーク中で機器を特定するための「ホスト部」となっている。ネットワーク部とホスト部がそれぞれ何ビット長かはネットワークで定義され，ネットワーク部の長さを表すのがサブネットマスクである。サブネットマスクは，ネットワーク部に相当するビットが1，その他のビットが0という値をもち，例えばネットワーク部が16ビット長の場合のサブネットマスクは，11111111.11111111.00000000.00000000，つまり255.255.0.0となる(**図6**)。

通信のための設定(図7)

実際にネットワークで通信する機器には，その機器自身のIPアドレス，接続されているネットワークに対応したサブネットマスク，そのネットワークの出入り口となる中継機器(ルータ)のアドレスであるデフォルトゲートウェイなどを設定する必要がある。

あるIPアドレスに対して通信をする場合には，最初に宛先が自分の属しているネットワーク内にあるかネットワーク外かを判定する。これはIPアドレスとサブネットマスクとを比較し，宛先がネットワーク内なら直接そのアドレスに送信するが，ネットワーク外ならデフォルトゲートウェイ宛(中継機器)に送信し，宛先アドレスがあるネットワークに向けて転送してもらう。

ネットワークの回線種類とスピード

ネットワーク上で通信を行う場合，通信スピードが問題になる。一般には，スピードが速ければそれだけ業務の効率が向上するが，逆に高速になると不安定になる可能性もある。ネットワークの回線の種類と伝送スピードを**表2**に示す。UTP(Unshielded Twist Pair cable)[6]とは，ネットワーク・ケーブルの種類の1つで，銅でできた線材を2

図7　ネットワーク通信のための設定
①IPアドレス，②サブネットマスク，③デフォルトゲートウェイ，④DNSサーバを設定する。

■ IP アドレス
□ 自分が使うアドレス

■ サブネットマスク
□ サブネットの広さを表す
□ サブネット内外を判定する根拠となる

■ デフォルトゲートウェイ
□ サブネット外への経路になっているルータ

■ DNS サーバ
□ ドメイン名を問い合わせる相手

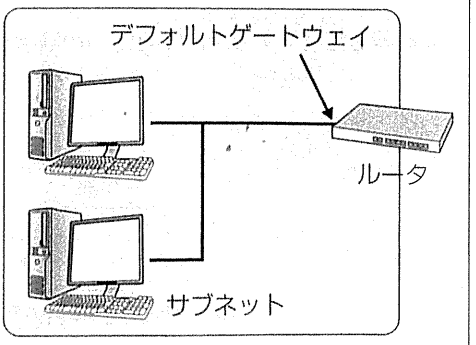


表2　ネットワーク回線とスピード
伝送媒体別の代表的な通信規格と，それぞれの伝送速度をまとめておく。全体的な傾向として，光ファイバを使用する場合は伝送速度が速く，次にUTP，無線という順序になっている。
表の最後にある ATM(Asynchronous Transfer Mode)は物理層とデータリンク層にまたがる規格で，長距離通信で主に使われていたプロトコルである。しかしWANにおける Ethernetの普及により，最近では音声通信などの限られた用途で使われている。

種類	規格名	伝達速度
Ethernet (UTP)	10Base-T	10Mbps
	100Base-TX	100Mbps
	1,000Base-T	1Gbps
Ethernet (光ファイバ)	100Base-FX	100Mbps
	1,000Base-SX(-LX)	1Gbps
	10GBase-SR(-LR)	10Gbps
Ethernet (無線)	802.11b	11Mbps
	802.11a，802.11g	54Mbps
	802.11n(*draft2.0)	540Mbps
ATM		155～1,250Mbps

本ずつより合わせたケーブルで，シールドしていないもの，「非シールドより対線」の意味である。UTPは電線を使用し，光ファイバはファイバ線を利用し，光ファイバを使用するほうが伝送速度が速い。また，最近は無線を使用するネットワークも広く使用されている。

伝送スピードは，MbpsやGbpsで表現される。Mbpsは，106bit per secondを表し，1秒間に106ビットの情報を転送することができる。同様にGbpsは，1秒間に109ビットの情報を転送することができる。

Pitfall

- インターネットなどのサービスを扱う場合は，ネットワークのIPアドレスを指定して通信することはしない。
- 人間が記憶しやすいアルファベットのネットワークアドレスを使用するほうが便利だからである。例えば，192.163.0.16というような数字を覚えるよりも，www.abc.co.jpのようなアルファベット表記のほうが理解しやすい。
- アルファベット表記のアドレスをIPアドレスに変換するためには，問合せ先のDNS（Domain Name System）[a]のサーバアドレスも設定する必要がある。

a) DNS. http://ja.wikipedia.org/wiki/Domain_Name_System

ネットワークの危険性

図8に示すように，ネットワークを道路にたとえると，交通事故が起きて情報がなくなったり，劣化したりする。また，盗聴やデータの改ざんなどが起こる可能性もある。また，雨・風によりデータの消失なども起こる。このようなリスクに対してしっかりした対策を立てることが，ネットワークを利用する場合に要求される。

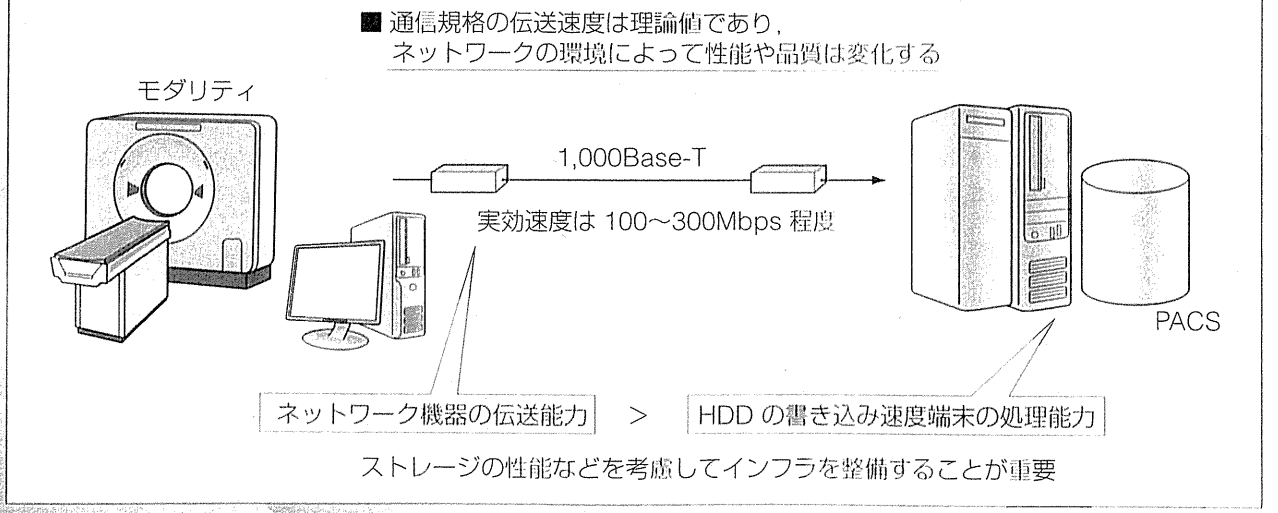
ネットワークを利用する通信(プロトコル)

国際規格(ISO)で定義されているネットワークのモデルは，7階層からなる「OSI参照モデル」[7]といわれている。これは，各種の通信プロトコル間

Pitfall 回線スピード

- ネットワークにおける転送スピードは，表2に示したが，この数値は，理想的な状態の転送スピードであり，普通のネットワークでは，この転送スピードは実現できない。
- その理由は，ネットワークには，複数の機器が接続されており，通信が複数の機器から同時に発生すると衝突を起こし，通信路が空くまで待たされる場合が生じるからである。
- 一般的なスループット(throughput：通信回線の単位時間当たりの実効転送量)は，図Aに示すように規格上のスピードの1／3～1／10である。

図A　ネットワークのスループット



実効転送量は，規格値の1／3～1／10である。

Pitfall 通信規格の伝送速度

- あくまでも理論上の最高値である。実際にはネットワーク機器や端末の性能や，機器が置かれている環境によって性能は変化する。
- 特に伝送速度は，情報を送信する機器，伝送する経路，受信する機器の処理能力に大きく依存し，最も処理が遅い機器の処理速度を超えることはない。
- したがって，大量の画像情報を伝送するなど大容量で高速な通信が要求される場合は，ネットワーク機器だけでなく高性能な端末などもバランスよく整備する必要がある。
- またネットワーク技術発展速度は非常に速いため，設備を整備する際には将来の需要拡大や機能拡張も意識しておく必要がある。特にケーブル敷設は大規模な工事になりやすいので，計画的な整備が必要である。

図8　ネットワークとセキュリティ
インターネットに代表されるネットワークは，治外法権的な環境であり，ネットワークを利用する情報伝達は，その内容が保証されない。

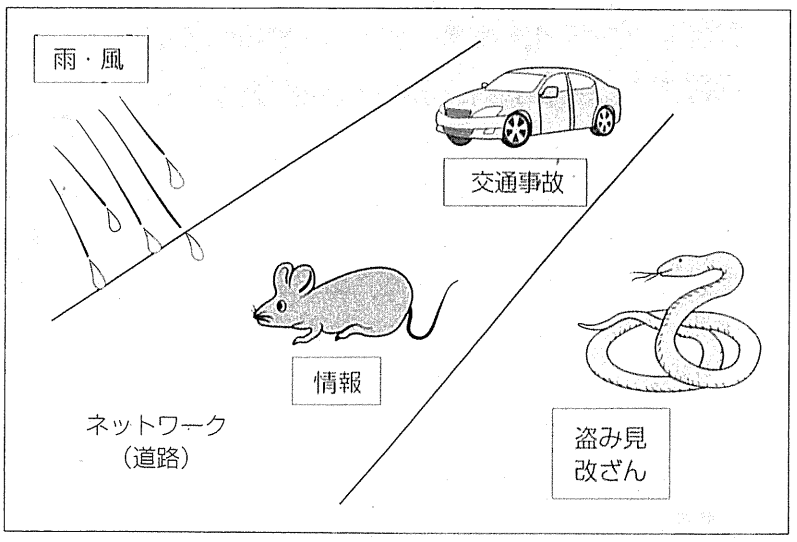


表3　OSI参照モデルとプロトコル

OSI参考モデル	TCP/IP 4層モデル	プロトコル	
Layer 7　アプリケーション層	アプリケーション層	HTTP, FTP, SMTP, POP3 telnet, ssh, DICOM	
Layer 6　プレゼンテーション層			
Layer 5　セッション層			
Layer 4　トランスポート層	トランスポート層	TCP	UDP
Layer 3　ネットワーク層	ネットワーク層	IP	
Layer 2　データリンク層	データリンク層	Ethernet	
Layer 1　物理層			

7階層からなる「OSI参照モデル」は国際的な規格ISOで定義されており，各種の通信プロトコル間の関係を階層化して整理するものである。プロトコルを階層化して役割分担を明確にすることにより，ほかの階層のプロトコルの内容に変更が生じた際の影響を最小化することを目的としている。
OSI参照モデルの上位層全体は，TCP/IP 4層モデルのアプリケーション層に該当する。また下位層のうち4層と3層は，TCP/IPモデルにおいてもトランスポート層，ネットワーク層と，同じ名前が付いている。またOSI参照モデルにおけるデータリンク層物理層は，TCP/IP 4層モデルではデータリンク層としてまとめられている。

の関係を階層化して整理するものである。プロトコルを階層化して役割分担を明確にすることにより，ほかの階層のプロトコルの内容に変更が生じた際の影響を最小化することを目的としている。OSI参照モデルでは，最もユーザに近い処理を行っている層(layer)が最も高いところにあり，上位層として7層(アプリケーション層)，6層(プレゼンテーション層)，5層(セッション層)がある。残りは下位層で，4層(トランスポート層)，3層(ネットワーク層)，2層(データリンク層)，1層(物理層)とよばれる。

OSI参照モデルとは別に，全体を4階層に簡略化した「TCP/IP 4層モデル」もある。**表3**に示すようにOSI参照モデルの上位層全体は，TCP/IP 4層モデルのアプリケーション層に該当する。ネットワーク利用者に関係するのは，アプリケーション層におけるプロトコルであり，ここで動作しているソフトウエアには，WWWのHTTP，ファイル転送のFTP，画像表示のDICOMなどがある。

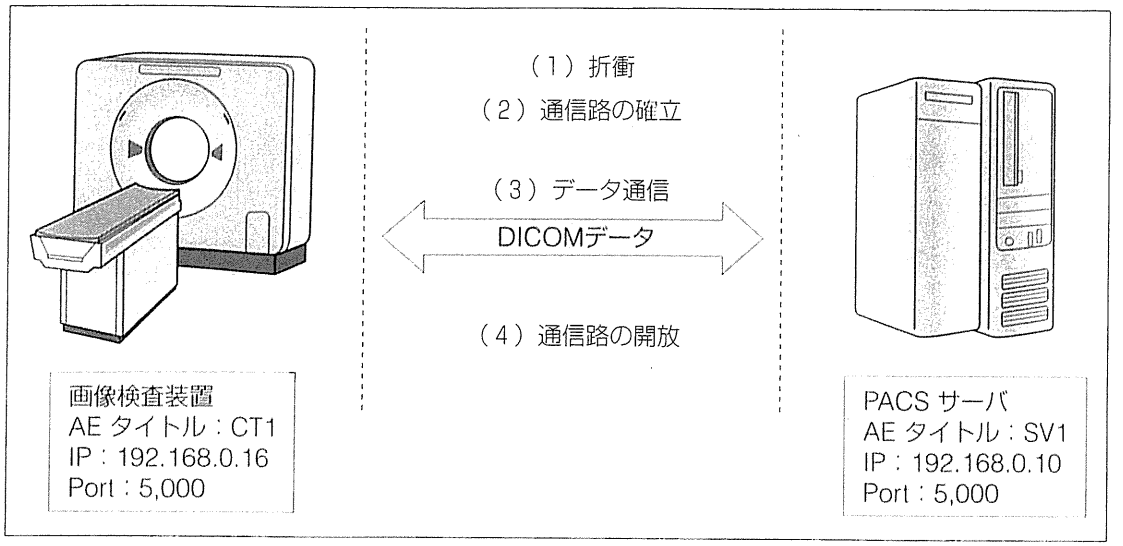
画像の伝送

DICOM規格による画像伝送

DICOM規格[8]の特徴は，ネットワーク対応，オブジェクト指向(医療の複雑な内容を詳細に表現可能)，媒体による情報交換(通信の規格から，媒体による保存まで拡張された)の3点である。DICOM規格は，画像情報のデータフォーマット，データ転送プロトコルとサービスクラスの三者が定義されている。

画像データを転送する場合について説明する。

図9　DICOMの転送手順



CT画像をネットワーク上で送信する際には，事前に発信元と送信先の情報が必要である。アプリケーション層での発信元と発信先の識別として「Application Entity（AE）タイトル」という名前が用いられる。これに加えて，IPアドレスとポート番号が指定される（**図9**）。

まず通信に先立って折衝が行われる。折衝では，要求するサービス，転送するデータなどが事前に送信元と送信先で合意が行われる。要求するサービスは，例えば，CT画像をサーバに転送して保存するというようなものである。この要求するサービスをSOPクラスといい，この場合はCT画像保存サービスクラスとなる。

DICOMオブジェクト（データ）の符号化方法を定めたものが，「転送構文」とよばれる。転送元から利用できる転送構文が転送先に送られ，転送先が自分に適した転送構文を選択することになる。転送構文には，送信元と送信先がその機能をサポートしていれば，非圧縮の画像データ，可逆圧縮の画像データ，非可逆圧縮の画像データ，リトル・エンディアン，ビッグ・エンディアンなどの種々の符号化方法で転送が可能である。

折衝が終了して，双方が同意すると通信路が確立され，実際に画像データの転送がはじまる。CT画像保存サービスクラスであれば，サーバ側に画像が保存される。通信が終了すると，通信路が開放される。

DICOM画像をWeb Browserで −WADO−

WADOとは，DICOM規格のPart 18で規定されているWeb Access to DICOM Persistent Object[9]である。一般にDICOM規格では，画像のネットワーク上の転送には，前述したDICOM規格固有の通信手順を使用している。この通信手順をWebで使用されているHyper Text Transfer Protocol（HTTP）を利用してDICOM画像情報を転送するのがWADOである（**図10**）。Web技術を利用して画像情報をやり取りするには，DICOM固有の通信手順はそぐわないので，新しく定義された。

WADOに対応したDICOMサーバは，Web browserなどからHTTPの転送手続きで画像を検索し，DICOM画像を画像データ（JPEG）や読影レポートならば文書表示フォーマットとしてPDFなどのフォーマットでWeb browserへHTTPの転送手続きで転送することができる。そのため，Webによるアプリケーションにとって便利な規格である。

Web技術では，インターネット上に存在するデータの指示方法として，URI（Uniform Resource Identifier）[10]が使用される。データの種類や変換方法は，Multipurpose Internet Mail Extensions（MIME）Typeとして表現される（**表4**）。DICOMフォーマットは，IETF RFC3240[11]で規定されているようにapplication/dicomで示される。

図10　WADOで使用されるHTTP通信
Web browserは，サーバに対してHTTPの手順で取得コマンド(GET)を送ると，サーバにそれに答えて要求された情報(画像やレポートなど)を返す。

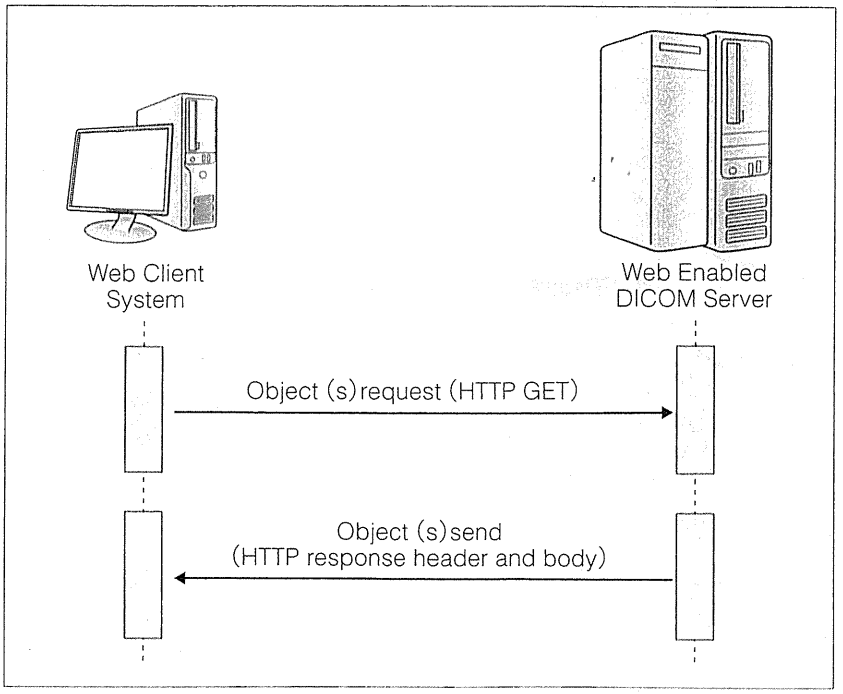


表4　WADOで利用できるMIMEタイプ
WADOでは，URIで示されるネットワーク上のサーバにおける，検査や画像を識別する固有識別子(Unique Identifier；UID)を組み合わせて画像をユニークに指定できる。例えば，パソコンからWADOを利用してPACSサーバ上にあるCT画像を指定して，その画像をDICOMフォーマットのまま，あるいは，JPEG画像に変換して，画像を転送することができる。パソコンでは，この転送されたデータをDICOMフォーマットであれば，DICOMビューアーで表示したり，JPEG画像であればWeb browserで画像を表示したりすることが可能となる。

番号	MIME/Type	説明
1	application/dicom	DICOMフォーマット
2	image/jpeg	JPEG画像フォーマット
3	image/gif	GIF画像フォーマット
4	image/png	PING画像フォーマット
5	image/jp2	JPEGの後継規格であるJPEG2,000画像フォーマット
6	video/mpeg	MPEG動画フォーマット
7	text/plain	テキスト
8	text/html	HTMLフォーマット
9	text/xml	XMLフォーマット
10	application/pdf	Portable data format(PDF)フォーマット
11	text/rtf	Rich Text Fileフォーマット
12	application/x-hl7-cda-level-one+xml	HL7で定義されているCDA(Clinical Data Architecture)レベル1のフォーマット。患者情報などの医療情報(文字)フォーマット

医療画像のデータベース

病院などの医療機関で画像を管理する場合は，必ず画像の管理用のデータベースが必要となる。DICOMサーバには，管理用の画像データベースが組み込まれており，画像の検索に対して迅速に返答を返すようになっている。PACSのサーバが画像を保存する場合は，DICOMヘッダーから付帯情報である患者情報(患者名，患者ID，性別，年齢)や検査情報(検査日，検査時刻，検査種別)などが読み出されて，PACSサーバ内のデータベースに検索用のキー情報として格納される。

病院などの医療機関では，規模が大きくなると検査部門ごとに画像サーバを管理するほうが，管理の利便性が上がったり，管理コストを節約した