○労働安全衛生法の施行について[1)]

(昭和四七年九月一八日)(発基第九一号)

第二　この法律の基本的事項

三　事業場の範囲

「しかし、同一場所にあつても、著しく労働の態様を異にする部門が存する場合に、その部門を主たる部門と切り離して別個の事業場としてとらえることによつてこの法律がより適切に運用できる場合には、その部門は別個の事業場としてとらえるものとする。たとえば、工場内の診療所、自動車販売会社に附属する自動車整備工場、学校に附置された給食場等はこれに該当する。」

つまり、企業内診療所は、診療を行う以上、本来企業から分離した事業場で無ければならず、企業内の健康情報の利用は、企業と医療機関の間の契約による医療情報の提供となる。

企業内の安全衛生部門の場合には、企業内の情報管理の対象となり、先ほどの事務部門での取り扱いと同じになる。これは、産業医の業務として、救急処置をのぞいて診療行為がない事にも通じる。[2)]

しかし、多くの場合には機密性の高い個人情報を外部医療機関と交わすことが求められるために、専用の電話などの設備を必要とする。これはインターネットも同様であるが、設備的に企業内であり、他の部署との情報連携も多いので、企業の管理に含まれる。

企業内診療所であれば、インターネットの接続のセキュリティは、診療所自身で担保しなければならない。しかし、ほとんどの場合、そのスキルが不十分である。

E. 結論

産業保健分野における、インターネット接続は、多くの場合には企業の管理下に置かれる。

F. 健康危険情報

特になし

参考文献

1) 厚生労働省、労働安全衛生法の施行について、http://wwwhourei.mhlw.go.jp/cgi-bin/t_docframe.cgi?MODE=tsuchi&DMODE=CONTENTS&SMODE=NORMAL&KEYWORD=&EFSNO=7485

2) 労働安全衛生規則14条「産業医及び産業歯科医の職務等」、http://law.e-gov.go.jp/htmldata/S47/S47F04101000032.html

厚生労働科学研究費補助金（地域医療基盤開発研究事業）
病院情報システム端末からの安全なインターネット直接接続に関する研究
分担研究報告書

医療機関内部における医療情報管理に関する調査･検討

研究分担者　秋山 昌範　（東京大学政策ビジョン研究センター）

研究要旨
病院情報システム端末からの安全なインターネット直接接続をおこなうためのネットワークセキュリティを検討する上では、多重防御の概念を適用した、ネットワークのセキュリティ方式の検討、方式設計を行う必要がある。また、近年比較的重症度の高い回復期の患者に対する在宅医療介護の需要が高まっている。そこでは、クラウドコンピューティングとスマートフォンを使ってリアルタイムに情報共有できる､在宅医療介護に対応した電子カルテが有用である。しかし、在宅医療介護は、病院のようにセキュリティ管理されていない居宅において行われるため､堅牢な情報セキュリティ技術によって患者のプライバシー情報を保護することが必要である。
したがって、在宅医療介護においては、ID 盗用等の不正アクセスを防ぐため、スマートフォンの SIM カード番号を用いた確な個人認証などによるセキュリティが適している。また､在宅医療介護においては複数の従事者が事業者ごとに散在しており､病院のように一カ所に集結していないため、情報基盤を共通化し SIM 認証を用いることが有用である。
今後、在宅医療介護に必要な情報連携機能について検討を進め、医療、介護、情報セキュリティなどの分野を横断し、学際的なアプローチを取り入れる視点が望ましい。

A. 研究目的

現状、導入されている医療情報システムは、セキュリティ上の問題により、インターネットへの直接接続が不可となっている。病院内以外の外部の医療機関との連携を行う際には、医療情報システムとは別の端末を使用し、接続が行われている。外部との医療機関とのシームレスな連携を行うためには、医療情報システム端末からのインターネット直接接続は不可欠である。

本研究では、セキュリティ上の観点から、特に在宅医療介護において、安全なインターネット直接接続に関する検討を行う。

B. 研究方法

愛媛県新居浜市の新居浜医療生活協同組合を中心に、愛媛県医師会、愛媛大学医学部付属病院の協力を得て３ヶ月間の効果検証を行った。調査対象として、居宅介護支援における患者（介護サービス利用者）を 30 名抽出した。家族構成や年齢、要介護度、疾患等の属性を幅広く選出し、網羅的な検証が行えるよう配慮した。

新居浜医療生協は１９７４年３月に設立された、在宅診療及び在宅介護サービスを提供する組合である。新居浜市内の３つの診療所を中心として、通所リハビリテーション・通所介護・訪問看護・訪問介護・指定居宅介護支援・グループホームなどの事業を運営している。

調査時、医師・看護師・理学療法士・作業療法士・介護スタッフ等３８０人程度が事業に従事していた。

大学病院の医師、地域の開業医、介護従事者などの関係者を集めた研究協議会を２回、有識者を集めた評価委員会を１回行い、効果等の検証・評価について検討を行った。

（倫理面への配慮）

今回調査にあたって収集した患者（在宅介護サービス利用者）30 名分の個人情報の取り扱いに関しては、細心の注意を払い厳重な管理の下で利用した。研究目的で利用する際は、個人が特定できないよう属性情報のみ公開とし、研究活動以外の二次利用は行わないことで合意し、患者及び従事者の同意を得ている。

C. 研究結果

I）対象

調査対象人数	30 名
調査対象性別内訳	男性 10 名 女性 20 名

調査対象 年齢範囲	70～101 歳
要支援 要介護内訳	①要支援 1… 0 名 ②要支援 2… 5 名 計 5 名 ①要介護 1… 5 名 ②要介護 2… 6 名 ③要介護 3… 8 名 ④要介護 4… 3 名 ⑤要介護 5… 3 名 計 25 名
家族構成 内訳	①独居 … 8 名 ②高齢者世帯（1 人が介護） … 10 名 ③家族同居（介護者あり） … 7 名 ④老老介護（両方介護） … 4 名 ※うち 2 名は⑤と重複 ⑤認認介護（共に認知症） … 2 名

(2) システムの概要

① スマートフォンによる入力

ケアマネージャー（7 名）、ヘルパー（7 名）が従来ノートに手書きで記録を行っていた介護記録を、携帯端末スマートフォンを使用して行っていた。今回は、特に食事と排泄行為に関して、携帯端末スマートフォンを用いて記録していた。

食前の画像データを写真で撮り、送信する。食後の画像データを写真で撮り、食事状況を入力して送信する。送信情報は入力時間のタイムスタンプとともにリアルタイムで記録される。入力した情報を写真と入力時間を併せて照会できていた。

排便と排尿の回数と状態を入力して送信する。送信情報は入力時間のタイムスタンプとともにリアルタイムで記録される。入力した情報を入力時間と併せて照会できる。

携帯端末スマートフォンは、基本的にはヘルパー、ケアマネージャーなどの介護従事者が使用する事を前提に設計したが、患者の家族や患者が携帯端末スマートフォンを問題なく操作できる場合には、家族や患者が使用することも想定して設計した。。

② スマートフォンに関する要件

1)SIM（Subscriber Identity Module Card カードに関する要件への対応

一般的に流通している携帯端末スマートフォンに搭載されている SIM カードを使用する。

2)認証に関する要件への対応

携帯端末スマートフォンで用いる認証を、以下の 3 段階の認証とすることにより、強固なセキュリティを担保する技術について検証した。

①VPN（Virtual Private Network）認証 ※ネットワークでの接続認証

②ログイン認証（システムでのユーザ認証）

③端末認証（携帯端末スマートフォンの SIM カード認証）

3)セキュリティに関する要件への対応

セキュリティと安全管理のため、携帯端末スマートフォンのハードディスク上に、一切のデータを記憶させず、全て RAM 上で展開する設計となっていた。

また、要求される 3 階層のセキュリティレベルを満たす、安全性に優れた共通基盤であった。

(3) システム要件

① 個人認証（SIM カード認証）

在宅医療介護に対応した電子カルテシステムには、端末としてスマートフォンを用いることが有用である。従来の PC 端末を中心としたシステムと大きく異なる点は、スマートフォンの SIM カードによる個人認証の機能である。スマートフォンの SIM カードによって個人認証を行い、他人による ID 盗用を防止可能である。SIM カード番号とは、製造番号と電話番号の組み合わせである。通常、SIM カード番号を認証するのは、通信業者である。日本においては、ドコモ、KDDI、ソフトバンク、等の通信業者が行っている。S IM カード番号は通信業者にとって顧客情報であるだけでなく、非常に精度の高い本人認証の仕組みである。携帯電話の契約を行う際、従来に比べて本人確認の書類手続きが厳しくなっており、他人がなりすましできない仕組みになっている。常識的には、個人に 1 台のスマートフォンを常時携帯し、スマートフォンの貸し借りは基本的にはしないことが一般的であり、個人を特定しやすい。

② 3 段階のセキュリティ

VPN 接続（仮想プライベートネットワーク）によって、データを暗号化する。インターネットに接続する際、VPN 接続で暗号化を行い、サーバーにアクセスできる仕組みになっている。サーバーに情報を転送される時に、既に情報そのものが暗号化されている。専用回線の中で、①SIM 番号（誰の携帯電話か認証する暗号）、②個人 ID、③パスワード管理のための暗号、3 つの暗号の仕組みを設定している。3 つ全て知らないと認証できない、簡単にはハッキングできない仕組みになっている。現在他の研究例で取り組まれているスマート

フォンを使った在宅医療介護システムとは圧倒的に異なる点がこのセキュリティレベルであり、他のシステムと比べて2段階セキュリティレベルの高いことが差別化できる点である。

③ プライバシー保護

端末には、全てのデータが残らない仕組みにする必要がある。具体的には、ヘルパーや介護士が取り扱う情報は、アップロードされた時点で即時に削除され、端末にはデータが残らない仕組みにすることが必要である。なぜならば、在宅医療介護においては、排泄の情報等の非常にプライバシーレベルが高い個人情報を取り扱う為である。
例えば、血尿や血便などが見られた場合に、介護士が便や尿の写真を撮影して画像をアップロードし、病院の医師と情報共有を行うことで、素早く医師の判断を仰ぐ等のケースが想定される。在宅医療介護において、排泄に関する記録は食事の摂取量と共に必要な情報であり、具体的には排便の色や柔らかさ、排尿の頻度等の傾向を記録している。

④ 通信ネットワーク環境

インターネットブラウザ経由で利用可能であるため、ソフトウェアを端末毎にインストールする必要はない。スマートフォンを利用することの利点は、通信回線が3G回線及びインターネット回線の双方を利用できる点である。従来の病院における電子カルテのようにPCを端末とするシステムの場合は、光ファイバーやADSL等のインターネット回線を利用するが、在宅医療介護の場合は患者の居宅の環境が病院のようにインフラが整備されていないケースが多い。スマートフォンを利用すれば、光ファイバーやADSLなどのインターネット回線の通信インフラが整備されていない地域においても利用できる。特に、病院までのアクセスが比較的良好な都市部よりも地方の地域の方が、在宅医療介護に対する需要が高い。都市部よりも地方の方が、インターネットのインフラ整備が低い傾向がある。（平成22年通信利用動向調査　総務省）在宅医療介護の需要が高い地方において、スマートフォンにより3G回線を利用することが有用であると考えられる。

D. 考察

日本は、平均寿命が長く、医療水準が高いため、複数の病気を持つ高齢者が多い世界一の超高齢化社会になった。現状では、年金・介護・医療のIDがそれぞれ異なり名寄せができないため、高齢者が年金、医療、介護をどれだけ受けているのか正確に把握できず、社会保障資源の最適化の議論ができていない。

20世紀の医療モデルでは、病院での治療の後、元気になってから退院していたが、2007年の第五次医療法改正等で、完全に回復していない患者も在宅通院するよう制度改正され、在宅医療や介護の重要性が高まった。しかし、健保を含む医療保険と介護保険はそれぞれ独立した制度であるため、制度間の狭間が生じている。病院のみならず、在宅介護データも極めて重要な医療データであるが、現在では、現場での看護・介護情報を記録した手書きの「ノート」が活用されているのが実態である。

21世紀の医療福祉モデルにおいては、在宅の介護情報も含め、複数の事業者間のデータの共有や連携ならびに複数の保険制度の組み合わせが重要になる。今後は、番号制度を導入するとともに、「ノート」のICT化を進め、さらに入力の必要がないセンサーの開発・活用等が求められる。センサーは、医療スタッフのいない被災地の医療にも役立つであろう。

米国とEUは、2010年12月にヘルスケアに関する情報およびアーキテクチャーの共有を目的としたeHealth協力協定を締結し、WHOも途上国にこの枠組みを提供しようとしているが、日本はこの枠組みに入っていない。欧米の「医療クラウド」モデルは、PHR（Personal Health Record）で、病院や診療所、患者の居宅、製薬会社などを一気通貫で捉えようとするものである。この連携を従来のICTシステムで行うと莫大な費用がかかるため、プライバシー、セキュリティ、課金等の課題を解決し、クラウドで仮想化・可視化していく必要がある。

昨今、回復期の患者に対する在宅医療介護の需要が高まっている。2007年の第5次医療法改正等の制度改正に伴い、平均在院日数の短縮が進んでおり、従来平均1ヶ月程度であった入院期間が、現在では一般病床では18日に短縮している。術後の退院期間も短縮されており、従来入院で治療を行っていた回復期の患者に対するケアが必要である。また医療技術の進歩に伴い、複数疾患を抱えた高齢者が増加している。従来の看取り中心の在宅医療よりも、比較的重症度の高い高齢患者に対する在宅医療の需要が発生していると考えられる。

在宅医療介護において必要な仕組みが従来の病院と異なる点は、以下の3点である。一点目に、病院のように関係者が物理的に一カ所に集結しておらず、複数の従事者が事業者ごとに散在しているため、情報を連携することが困難である。仮想的に情報を集約し、連携を行う仕組みが必要である。二点目に、在宅医療介護における情報は病院のカルテとは異なり、介護記録が介護士やヘルパーによって手書きでノートに記録されている。事業者毎に複数のノートが存在しており、共通フォーマットが無いため、転記する等の記録行為にヘルパーや介護士の業務負荷がかかっている。情報基盤を共通化し、複数事業者間でもリアルタイムに情報を共有できる仕組みが必要である。三点目に、在宅医療介護患者のプライバシー保護のために、情報漏洩を防ぐ強固なセキュリティレベルを維持する必要がある。具体的には、従来の病院における血圧や体温等の情報に加えて、排尿の量や排泄の頻度等の情報を記録するため、極めてプライバシーレベルの高い情報を取り扱う。また、在宅医療介護の患者の居宅においては、物理的なセキュリティ管理が十分ではないケースが多く、病院と比較すると情報セキュリティの対応が脆弱である。病院のようにアクセスが限定された環境ではないため、より厳密に個人を特定し、情報管理を行う仕組みが必要である。

E. 結論

在宅医療介護の現場となる一般の居宅は情報基盤のみならず物理的なセキュリティも低い場合が多く、在宅医療介護においては病院よりも高いセキュリティレベルを確保する必要がある。病院の職員証のような仕組みは居宅には無く、一人の患者に対して複数の事業者が関与するため個人認証が難しい。そのため、スマートフォンのSIMカード番号を用いた正確な個人認証が有用である。また、在宅医療介護と病院との違いは、病院のように一つの建物に集約されておらず、在宅医療介護の従事者が複数の事業者に渡り、物理的に散在していることである。情報基盤を共通化し、情報を一元管理することにより、複数に散在している事業者間での連携を円滑にする。医療の個人情報を有効活用するためには個人情報の仮名化が必要であり、適切な認証レベルを設定することが重要である。

F. 研究発表

1. 論文発表

1). 金安双葉、秋山昌範. 在宅医療対応電子カルテに必要な機能. 医療情報学 31(Suppl.):767-768, 2011.

2. 学会発表

1). 金安双葉、秋山昌範. 在宅医療対応電子カルテに必要な機能. 第 31 回医療情報学連合大会. 鹿児島県. 11 月. 2011.

2). 秋山昌範. 共同企画 7 デジタル・フォレンジック研究会 社会保障・税番号制度と医療情報保護法案の動向と医療情報の利活用. 第 31 回医療情報学連合大会. 鹿児島県. 11 月. 2011.

3). 秋山昌範. 医療情報システムによる新しい管理会計と医療の最適化. 第 31 回医療情報学連合大会. 鹿児島県. 11 月. 2011.

G. 知的所有権の取得状況

1. 特許取得 なし。
2. 実用新案登録 なし。
3. その他 なし。

厚生労働科学研究費補助金　（地域医療基盤開発推進研究事業）
分担研究報告書

病院情報システム端末からの安全なインターネット直接接続に関する研究

研究分担者　安藤　裕　放射線医学総合研究所　重粒子医科学センター 病院長

研究要旨　院内の医療情報システムと外部のインターネットとの接続には、十分な安全性が要求される。特に病院のような機微な情報を扱うシステムには、より慎重になる必要がある。そこで、当院の現状と今後のインターネット接続に関する必要性を検討し、今後の接続に関する安全な方策を模索した。

A．研究目的

一般の医療機関では、医療情報システム(オーダリングシステムや電子カルテなど)を導入し、医療の効率化や迅速化を行っている。このような医療情報システムは、独自の診療用のネットワークに接続しており、このネットワークは、外部のインターネットなどとは分離している使用形態が安全上望まれる。しかし、院内からインターネットを介して、様々な情報へアクセスする要望が生じている。具体的には、医薬品の安全情報、診療ガイドラインや紹介先医療機関に関する情報、さらに医療機器をメンテナンスするためのリモート回線などである。

また、患者自身による自分の診療情報に関する医療機関へのアクセスなどの要望も増大している。このような状況で、医療機関の外部へあるいは外部からインターネットを介したアクセスは、危険性があり多くの医療機関では制限する状況である。このような場合に、厚生労働省の「医療情報システムの安全管理に関するガイドライン」が参考になるが、実際に安全に安心して接続している医療機関は限られる状況である。

本研究の目的は、当院の現状と将来のインターネット接続の問題点とその解決策があれば、解決策の可否を検討することにより一般の医療機関が利用できる安全なインターネット接続方法を模索することである。

B．研究方法

当院のインターネット接続に関する経緯とリスク分析を行い、今後のインターネット接続の必要性を検討し、よりよいインターネット接続方法を検討調査した。

特に以下の点について検討を行う。（1）インターネット接続による医療機関外部からのリスク、（2）インターネット接続がない場合のデメリット、（3）患者による医療情報アクセスへの要望である。

C．研究結果

C.1　当院の医療情報システムの変遷とインターネット接続

従来のリスク管理されていないネットワーク構成を図１に示す。当院では、ネットワークを大きく２階層に分けていた。１階層は、研究系ネットワークであり、電子メールやWWWなどのアプリケーション、業務システムが接続されている。

一方、診療系ネットワークには、電子カ

ルテや画像管理システム（PACS）、臨床データベース（AMIDAS）、スケジュール管理システム、電子照射録システム、病院の部門システムなどの診療に直結したシステムが接続されている。

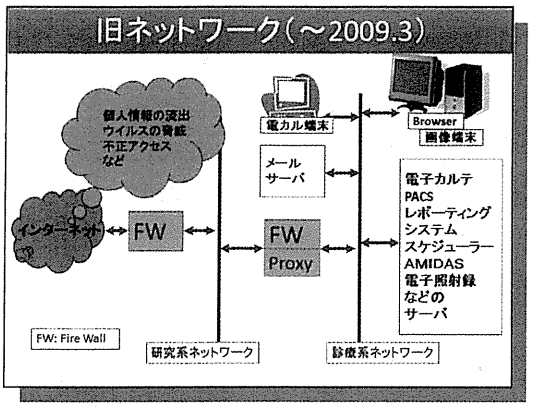

図１　リスク管理されていないネットワーク

図１に示す。ネットワークでは、インターネットから Firewall を 2 回経由して、診療系のネットワークに接続されている。診療系のネットワークでは、不正アクセスなどの事例はまだないが、研究系のネットワークでは、しばしばウイルス感染事故が起きていた。このような状況では、診療系ネットワークにもウイルスの侵入の可能性があり、感染すれば診療業務に影響が出る恐れがある。

また、メールに添付されるウイルスの件数は、年間数十件検出され、ウイルスによる感染リスクが高いと判断された。

図２に示すのが、現状のリスク管理されたネットワークである。研究系ネットワークは、Firewall を介してインターネットに接続している。しかし、診療系のネットワークは、研究系ネットワークとの物理的な接続を遮断した。遮断（Firewall と Proxy を停止）により外部からのリスクを取り除くことが可能となった。しかし、反面、インターネット接続による利便性が犠牲になった。

例えば、一般のメールが診療系では利用できない。また、インターネットを介して web 等の情報を利用することができない。などの問題がある。

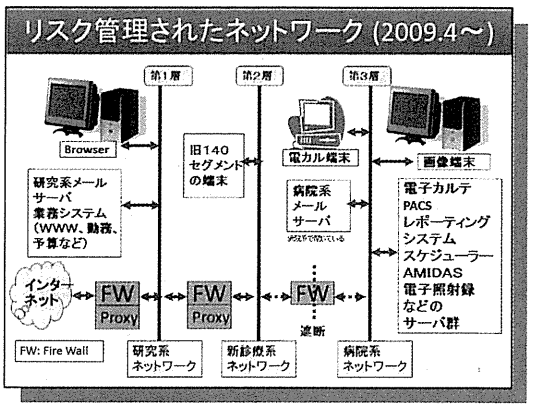

図２　リスク管理されたネットワーク

C.2 リスク

医療情報システムに格納されている電子データのリスクとしては、以下のような事項が考えられる。

(a) 権限のない者による不正アクセス、改ざん

(b) コンピュータウイルス等の不正なソフトウェアによるアクセス、改ざん

これらのリスクを減少させる方法の一つとして、インターネットとの接続を遮断することである。

C.3　インターネット接続がない場合のデメリット

逆に、インターネット接続ができなくなることにより生ずる欠点を検討した。

(a) オンライン情報（薬剤副作用情報、医療機関の受診案内、ウイルスの最新パターンファイル配信など）へのアクセスが困難

(b) 病院内外に対する電子メールの連絡ができなくなり、迅速な情報伝達

が阻害され影響を受ける業務がある

C.4 現状の接続

病院系のネットワークは、外部から切り離されているとはいえ、どうしても外部と接続しなければならない業務が存在する。表１に示す。

表１ 診療系からの外部接続の必要性

NO	内　　容	頻　　度
1	リモートメンテ用の回線 ・CT, MR、PET などの画像検査機器 ・電子カルテ、臨床データベース、スケジューラなどのデータベースサーバ	故障時やメンテナンス時（年数回）
2	ウイルスパターンファイルの更新	日１回
3	オンライン・レセプト請求	月１回

現状では、これら表１の接続は、図３に示すように、十分なリスク管理がされていない。このような状況を改善するために、図４に示すようなリスク管理された外部接続方法を検討している。ここで、VPN は、選択枝としてオンデマンド VPN も考えられる。

図４に示すように、外部に接続する回線は、一括してログ管理と認証管理を行い、2階層の Firewall を設置することを検討している。さらに外部に出てく出口には、オンデマンド VPN などを検討している。

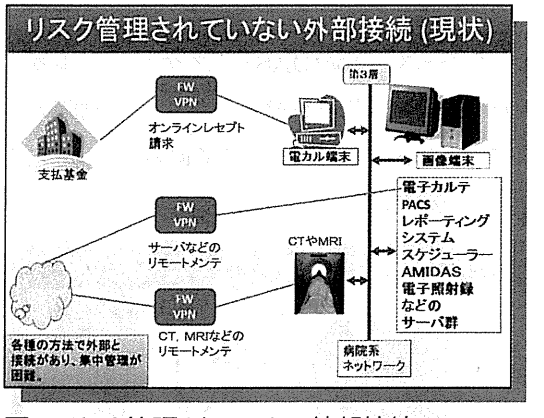

図３ リスク管理されていない外部接続

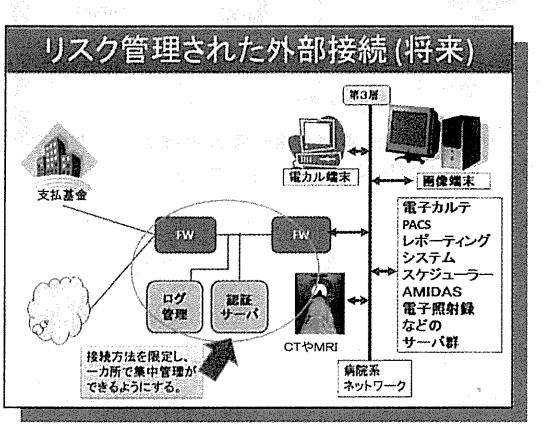

図４ リスク管理された外部接続（将来）

C.5 患者や医療機関による医療情報アクセスの要望

医療サービスが広く普及すると患者が直接自分の医療データにアクセスする要望が生じる。現状のネットワークトポロジーではこのような要望に応じることができない。将来の患者サービスの向上に備えて、安全なインターネットアクセスの方法も開発する必要がある。また、当院では、放射線治療の患者が全国各地から紹介されてくる。このような患者に放射線治療を行い、治療終了後は、患者は紹介元に戻っていくことになる。このような場合に、紹介状を依頼元から入手する手段として、インターネットが利用できると便利であり、また、治療後、治療サマリーや退院サマリーなど依頼元の医療機関へ伝達する必要

がある。この時にも、やはりインターネット接続が望まれる。

D．考察

さて、「病院情報システム端末からの安全なインターネット直接接続」について、表２のようなメリット・デメリットが考えられる。VPN を使用して、安全な通信路を確保するのは、必要だが、コストの面で患者個人が利用するには、困難であろう。また、暗号強度については、その時々に最適の暗号強度を使用する必要があり、技術の発達やコンピュータの速度が向上すると要求される強度が変化する。この場合に、もっとも問題になるのは、管理要員の人件費であろう。

患者を対象にしたり、紹介元の医師を対象としたり、また、CT や MRI あるいは電子カルテなどの Remote Maintenance のためのネットワーク接続では、それぞれに必要最小限のアクセス範囲を設定し、また、個人認証の方法を用意する必要がある。

表２ メリット・デメリット

NO	分野	メリット・デメリット
1	VPN	安全な接続の確保 コスト
2	暗号強度	ガイドライン 管理要員のコスト
3	公開データの管理	電子カルテシステムからの公開するデータの抽出やアクセス管理

インターネットに代表されるネットワークを利用して患者の個人情報をやり取りする時代になりつつあり、また、急速に必要性が増している（図５）。この場合に、暗号化技術やユーザの認証技術を用いて患者が安全・安心にアクセスできる病院情報システムを構築することが急務である。実際に、ネットワークを利用して、システムを構築する場合に、どのくらいの強度の暗号ならば良いのか、また、どのようなＶＰＮを使用するべきなのかを示す時期に来ていると考える。

医療機関が限られた資源（人材やコスト）で情報システムを構築する際に問題になるのは、そのシステムの管理や説明責任をクリアーすることが必要である。これらの要求に耐えるだけのシステムを開発し、そのコストが実現可能であるかどうかが問題となろう。このようなコストをいかに低減して、医療に活用するかが緊急の課題である。

インターネットを経由して個人情報を参照する場合には、多くの医療機関がその手間や事故などの場合のリスクにおびえて、尻込みしていると考えられる。また、医療機関といえどもコストを十分にかけることが困難である。このような問題を解決するためには、学会や省庁などが中心となってガイドラインを示すことが特に必要と考える。

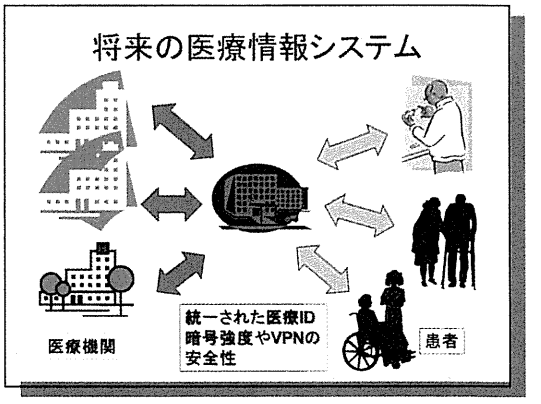

図５ 将来の医療情報システム（関連病院や患者との連携）

E．結論

インターネットを利用して、病院から外部への接続は、今後の医療サービスや医療情報システムの管理に必要な機能である。これらのリスク、インターネット接続がない場合のデメリット、患者による医療情報アクセスへの要望などの点から病院情報システムのネットワークについて検討した。今後の解決すべき問題点として、暗号化の強度やネットワークにかかる管理コストに問題点があり、十分な検討が必要である。

G．研究発表

1．論文発表

なし

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（地域医療基盤開発研究事業）
病院情報システム端末からの安全なインターネット直接接続に関する研究
分担研究報告書

医療機関のインターネット接続におけるリスク分析に関する研究

研究分担者　山本　隆一　　東京大学大学院情報学環　准教授

研究要旨　医療機関の大部分は何らかの情報システムを導入し、レセプトオンライン、緊急安全性情報へのアクセス、診療ガイドラインへのアクセスなど外部ネットワークへのアクセスに対する医療機関側からの要求は増大してきている。自らの情報資産の安全を確保した上で診療に必要なインターネット通信を行える状態を促進するためには、リスク分析および対応要件を詳細に定義し、接続の程度に応じた現実的に可能な方法や具体例を示す必要 がある。本研究では、要件定義のための検討材料の一つとして、 すでにインターネット接続を行っている大学病院における利用状況の分析を行った。

A．研究目的

医療機関の大部分は何らかの情報システムを導入し、レセプトオンライン、緊急安全性情報へのアクセス、診療ガイドラインへのアクセスなど外部ネットワークへのアクセスに対する医療機関側からの要求は増大してきている。厚生労働省による「医療情報システムの安全管理に関するガイドライン」では、インターネットへの接続を禁止はしていないが、厳重な対策を求めており、一般の医療機関が安易に接続できる状況ではない。

政府による「国民を守る情報セキュリティ戦略」においてもインターネットの安全・安心な利用は重要視されており、情報セキュリティへの政策として、サイバー攻撃・情報漏えいやデバイス・技術の多様化などを焦点として、政府関連組織のセキュリティ基盤強化や利用者への普及・啓蒙活動、人材育成に対する取り組みが行われている。なかでも、経済産業省では、民間企業を対象として、これまでにコンピュータウィルスや不正アクセスを対象とした情報システムの基本的な安全管理基準にくわえ、Web を含むソフトウェアの脆弱性に対する基準やフィッシング対策ガイドラインの作成なども行ってきており、とくに情報セキュリティに対して専門の人材確保が行えない中小企業への支援が重要課題のひとつとされている。

こうした状況において、医療機関においてインターネットに直接接続する場合に考えられるリスクとしては、

1)　マルウェア等の混入により、診療情

報システム に予期せぬ障害がもたらされること

2) 通信先が適切に認証されない状況での利用により、なりすまし等による情報漏洩が起こること
3) 通信内容が適切に秘匿されず、患者・医療者に関する機微な情報の漏洩が起こること
4) 利用者による公序良俗に反した利用がなされること

などが挙げられる。ブロードバンドの普及と上記のような啓蒙活動により一般市民のITリテラシーは向上してきてはいるが、中小企業の場合と同様に専門人員の確保が困難な医療機関が、こうしたリスクに対する自らの情報資産の安全を確保した上で診療に必要なインターネット通信を行える状態を促進するためには、リスク分析および対応要件を詳細に定義し、接続の程度に応じた現実的に可能な方法や具体例を示す必要がある。

本研究では、要件定義のための検討材料の一つとして、すでにインターネット接続を行っている大学病院における利用状況の分析を行った。

B. 研究方法

現在の利用状況の把握のため、パケット解析装置を用い、2 つの大学病院においてインターネット利用状 況の調査を行った。双方の大学病院ともに施設内からのインターネット接続を行っているが、A 大学病院は診療端末からのインターネットアクセスは禁止されており、個人ないしは診療科の端末からアクセスができる。一方で、B 大学病院はそれらに加えて、診療端末からのインターネットアクセスが可能である。

調査期間は平日の 1 週間程度とし、プロトコル・宛先サ イトの分類・利用帯域・セッション数などの統計情報を採取した。パケット解析装置として、Cisco Systems 社製の Service Control Engine を使用した。

C. 研究結果

C－1 サービス別の利用帯域

どちらの大学病院でも、インターネット利用のうち大部 分が HTTP や HTTPS といったブラウザ系の通信で帯域が使用されている (図 1～2)。また、メールの受信、IM、VoIP 通信、Facebook や Twitter による専用プロトコルなども観測される。

C－2 Web サイト利用

利用形態として帯域の大半をしめる Web 系の通信について、アクセス先サイトの内訳は、図 3～4 のとおりとなる。アクセスページ数として多いのは、情報検索目的と思われる検索エンジンや twitter、facebook などの利用のほか、文献検索サイトへのアクセスも上位に観測された。また、OS やウイルス対策ソフトウェアのアップデートによるアクセス数も上位に観測された。

C－3 外部からのアタック

外部からの不正アクセスとして、Web サーバへの攻撃と見られる 80 番ポートへのアクセスが多く観測された (図 5)。また、データベース接続やリモートアクセス用のサービスへのアクセスが検出されている。

D. 考察

D－1 利用状況

本研究の調査では、とくにWebを利用した情報検索エンジンの利用が圧倒的なアクセス数を有し、その他に、電子メールの送受信を含めると大半の利用数が力バーされる。利用者へのヒアリングでは、情報検索対象として、医薬品・診療ガイドライン・副作用・略語・学術文献・他医療機関やその担当医師名の情報などが挙げられた。したがって、Web・メールの利用に対する安全性の確保とこれら以外の通信を区別・制限できるか、といったことが大きな課題になると考えられる。Webアクセスに対するリスク軽減策の一つとして、不特定のサイトアクセスを回避するために、事前登録制によりアクセス先を限定することも考えられるが、維持管理にかかる人的負担は大きい。たとえば、外来診療システム端末からの Web によるアクセスサイト数は約14000サイトにのぼる（B大学病院、2011年6月分)。

D－2リスクと対策

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 4.1 版」に記載されているように、不正ソフトウェア対策、不正アクセスに対する技術的対策は行う必要がある。利用状況の調査にも見られる多くのWebアクセスやメールの受信など外部コンテンツを取得する場合には、個々の情報システム端末上でマルウェア対策ソフトを導入するのが効果的であると考えられる。たとえば、2011年8月の一か月間で、B大学病院では、全429件（Web経由：1件、USB経由:4件､その 他は受信メール経由）のウイルス検出があり、いずれも対策ソフトにより駆除あるいは隔離されている。一方で、こうした対策ソフトは、定義ファイルを常に最新のものに維持しておかなければ､新しいマルウェアに対応できないため、業務システムとしても対策ソフトの最新化を行える機能が求められる。同様に、こうしたマルウェアが標的とする基本 OS の脆弱性についても個々の情報システム端末で常に最新化されること、業務システムが基本 OS の最新化に対応していることが求められる。逆に、特殊な検査機器など、こうした技術的な対策が取れない機器は、医療機関内部でネットワークとしても区別される必要がある。

また、インターネット接続することにより、医療機関側のネットワーク機器やサーバコンピュータが外部からの攻撃対象となりうるため、ネットワーク機器･サーバ コンピュータにおいても同様に基本 OS やアプリケーションの脆弱性対策を行うことが求められる。大規模病院では多くの場合、外部からのアタックは対策がされており、ファイアウォール等により効果的にブロックされているが、特にアプリケーションサーバごとの脆弱性への対応など、情報収集段階から人的努力に依存する部分が大きい場合もあり、どのようなサイトにも期待できるとは限らない。

このような技術的な対策で一定の防御が可能なリスクのほかに、Webやメールによる人為的な情報漏洩もリスクとして考えられる。これに対しては、継続的な運 用ルールの周知やセキュリティ教育などを実施するといった人的対策が必要と考えられる。

D－3接続形態

現状で病院情報システム端末としては、

インターネット接続を禁止しているケース、アクセス可能な端末を別に設置するケース、直接アクセスが可能なケースがある。今回調査を行った大学病院のような大規模機関では、自身でインターネット接続を行い、一定の専門知識を持った管理要員が情報システムを管理している場合がほとんどであり、先に述べた技術的対策は自身で行っている。これに対し、一定の専門知識のある管理要員を確保できないケースでは、上述のような技術的対策を、外部サービス利用により実現することも考えられる。多くの商用サービスプロバイダでも、メール・Web利用時のウィルススキヤンやP2P通信対策などのサービスが提供されてきている。インターネット接続を行う際に、情報システム端末上での対策とあわせて、こうしたサービスを利用することにより、一定の安全性を確保できると考えられるが、公的機関等による接続サービスの運営も考慮し、さらに詳細に検討する必要がある。

E．結論

２つの大学病院においてインターネットアクセスにおけるリスク分析をおこなった。ネットワーク管理の専門知識を持つ管理者を置くことが可能な大病院では一定にリスク対策が可能であるが、一般の医療機関では外部サービスを活用するなどの対策が必要と考えられた。

F．健康危険情報

特になし。

G．発表

なし

H．知的財産権の登録・出願状況

現在のところなし。

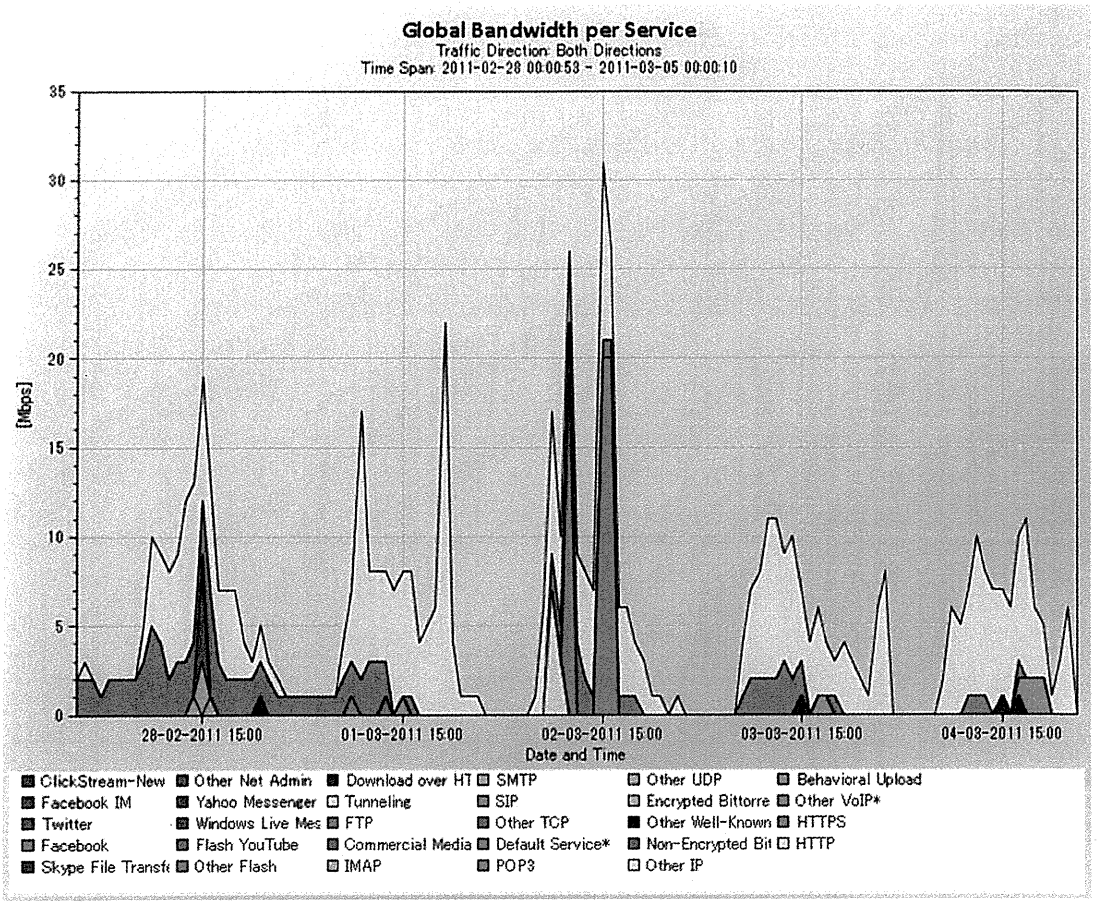

図１サービス別通信量（A大学病院）

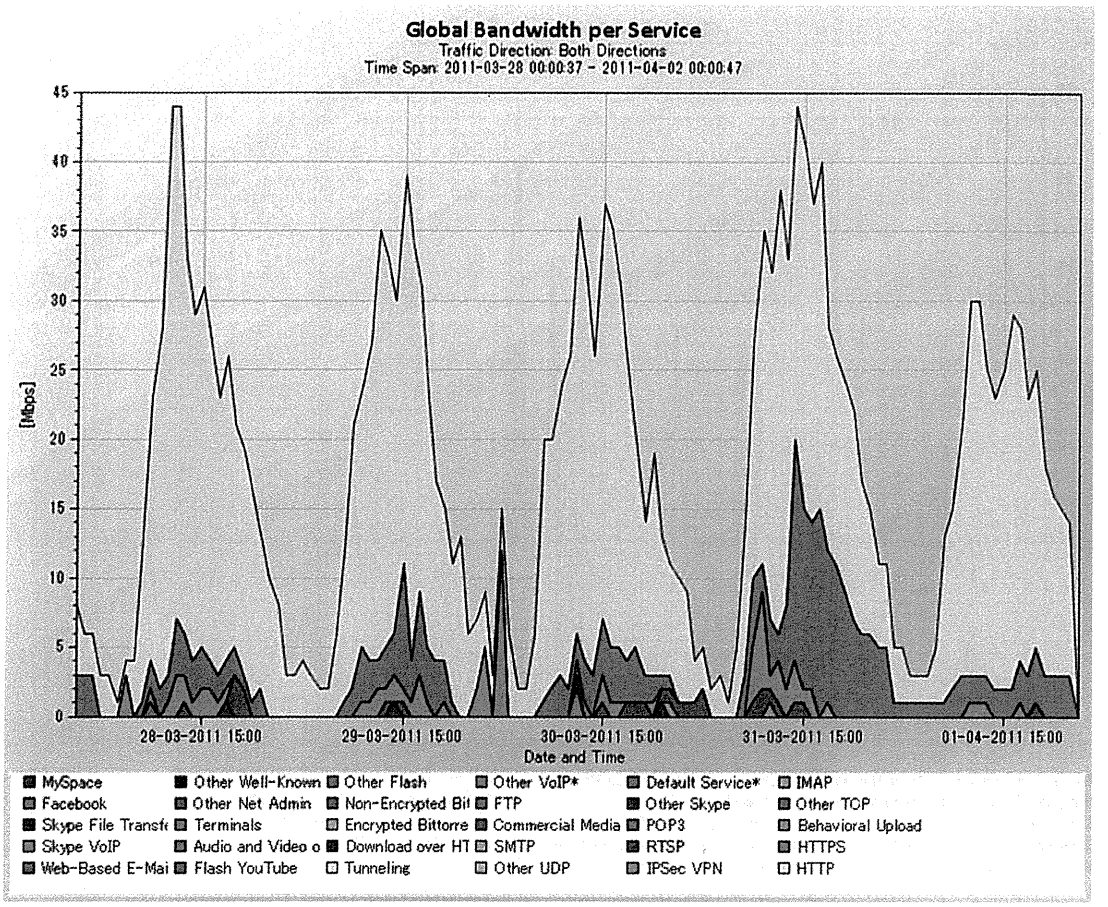

図２サービス別通信量（Ｂ大学病院）

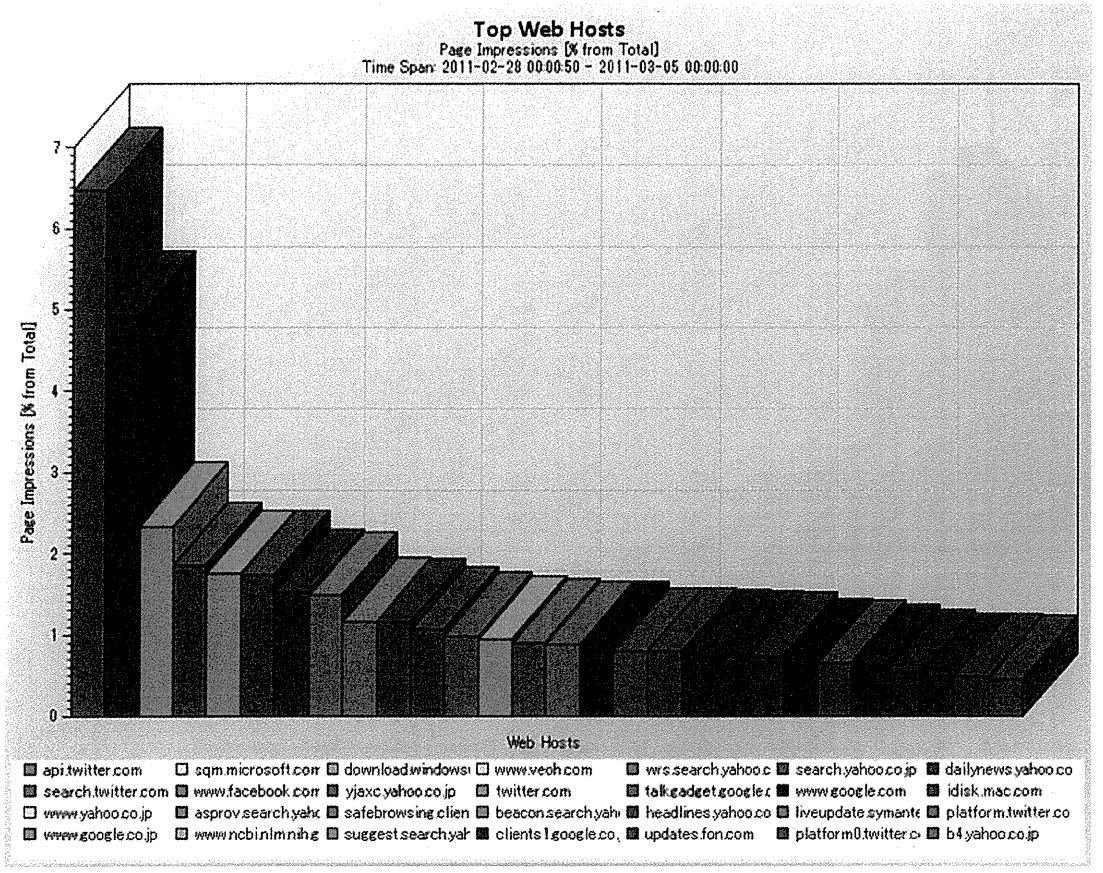

図３ＷＥＢサービスのアクセス状況（Ａ大学病院）

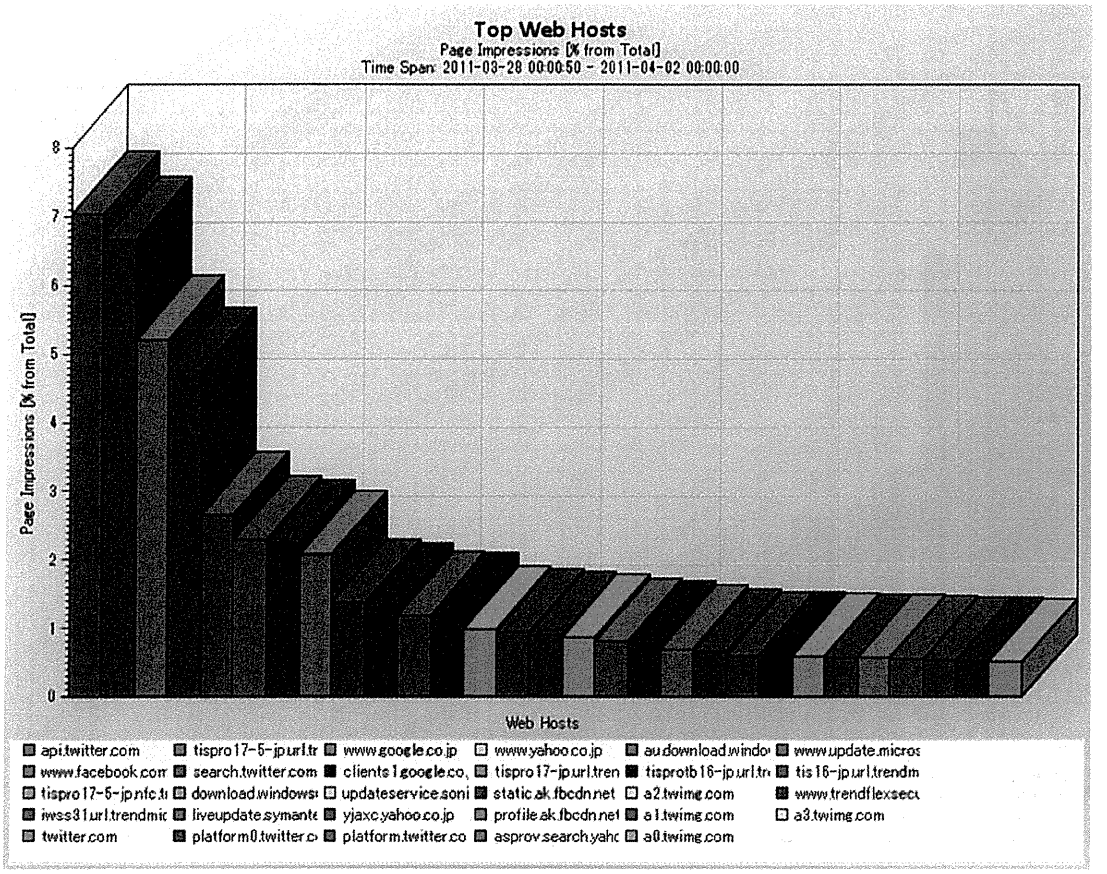

図４ＷＥＢサービスのアクセス状況（Ｂ大学病院）

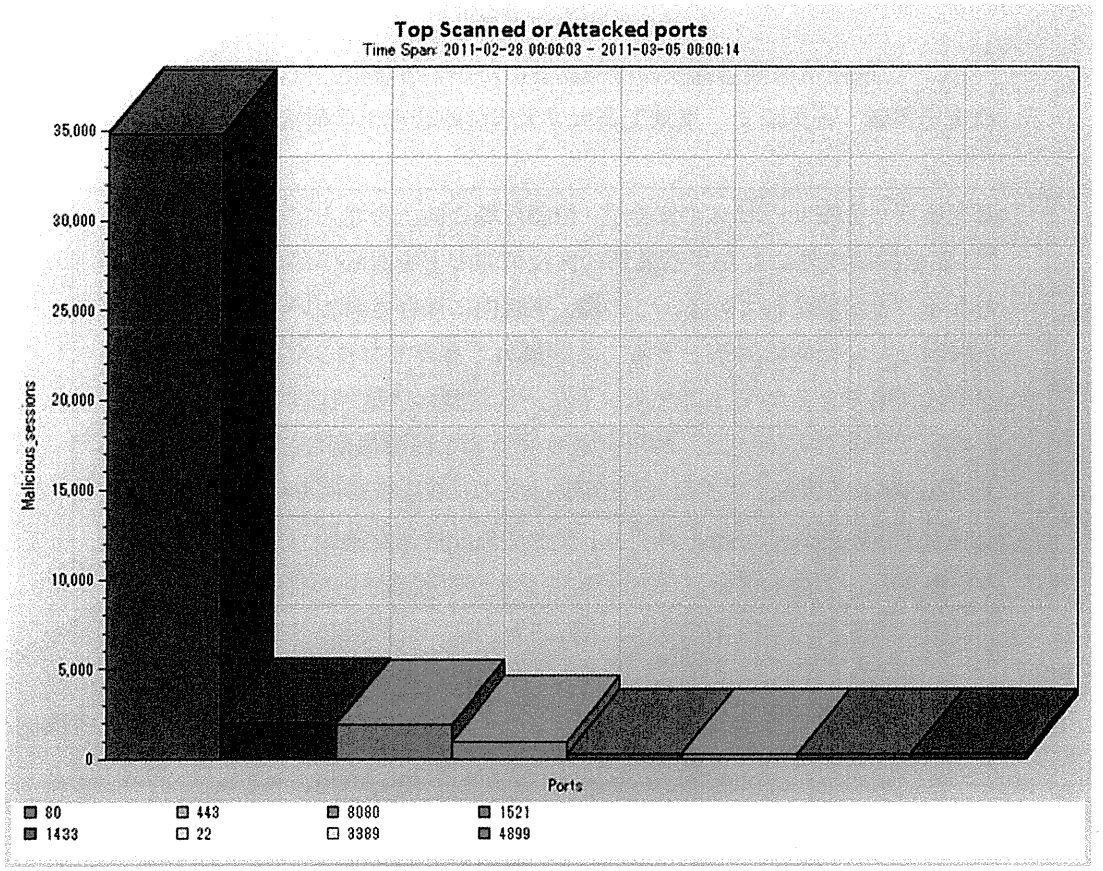

図５ポート別不正アクセス検出数（Ｂ大学病院）

厚生労働科学研究費補助金（地域医療基盤開発推進研究事業）
分担研究報告書
院内情報機器端末の機器認証にかかわる技術的検討
研究分担者　小尾高史　東京工業大学大学院総合理工学研究科　准教授

研究要旨　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、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。この際、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必要とされている。最終年度である本年度は、昨年度取りまとめた医療機関などがインターネット上で公開される情報にアクセスする際に求められる技術要件をもとに、適切な情報端末からのみ外部接続を許可し、安全に外部情報を参照可能とするシステムを提案し、プロトタイプシステムによりその有効性を検証した。

A．研究目的

現在、医療分野においても様々な場面において情報技術の活用が進められており、診療データの外部保存、レセプトのオンライン申請など、様々な場面でネットワーク技術が利用されている。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。

そこで、本研究では、情報端末や利用者を認証する仕組みを導入することで、適切な利用者・端末からのみ外部接続を可能とするシステムを検討している。外部との接続に際しては、オンデマンドVPNの機能を拡張することで、医療機関と情報提供機関間のインターネット接続を安全におこない、不正アクセスなどを防止可能な仕組みの実現を目指している。

今年度は、昨年度取りまとめた医療機関などがインターネット上で公開される情報にアクセスする際に求められる要件をもとに、医療機関内に設置された情報端末と端末利用者の認証と組み合わせることで、適切な情報端末に対してのみ外部接続を許可し、安全に情報を参照可能とするシステムを提案し、その有効性を示すことを目的とする。

B．研究方法

平成２３年度の研究では、平成２２年度に行った医療機関内で利用される端末の抽出、及び、適切な情報端末からのみ外部接続を許可し、安全に外部情報を参照可能とするシステムの要件を踏まえ、医療機関からの外部情報を参照するシステムの実現方法を具体的に検討する。そして、その結果をもとに、プロトタイプシステムを構築し、提案システムの有効性を検証する。

C．研究結果および考察

平成２２年度に行った研究で検討した、新たな