表1　産業保健の管理形態の種類

従業員数	産業医の有無	産業保健部門の形態	組織区分
50名未満	無し	事務職の兼任	企業内事務所
50名以上1000名未満	嘱託	医療機関などから派遣	企業内事務所と医療機関
		労働衛生コンサルタント事務所	企業内および企業外の事務所
	専属	企業内診療所	企業内部医療機関
1000名以上	専属	健康管理室	企業内部事務所
		企業内診療所	企業内部医療機関

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。データ領域とデータ利用領域を論理的に分割したデータの保護を実現し、また、基幹ネットワークへの不要な通信が流入しないよう、ブロードキャストドメインごとにアクセス制御する方式設計も重要である。これはデータ領域を保護するだけではなく、ネットワークの安定化への貢献にもつながることである。

エンドポイント(有線、無線 LAN)のネットワークに対して、不正端末、不正利用者の脅威を軽減する対策や、セキュリティコンプライアンス機能（PC 端末のセキュリティポロシへの準拠度合いの監査)、ウィルスの感染、拡大を軽減するセキュリティ方式を検討、方式として適用し、エンドポイントだけではなく、エンドポイントのふるまい制御機能も併せて検討する必要がある。

これらセキュリティ機能の導入により､エンドポイントにおけるセキュリティを高めることができ、結果として、情報漏洩対策への大きな貢献が可能となる。

病院情報システム端末から安全にインターネットへ直接接続を行うためには､すべてのネットワークセキュリティ機能を有機的に結合し、2 重、3 重の防御体制を取ることで、より大きな効果を得ることができると判断する。

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、医療情報システムにおける安全なインターネット直接接続に関するデータベース作成を行うことを目的とする。

B. 研究方法

インターネットを利用して、医療機関相互に連携するために診療記録の外部保存、保険統計情報の分析および遠隔医療への取り組みは、近い将来にネットワーク型医療サービスの出現が推測されるものである。また、従来は院内で独立・隔離して管理されていた情報が関連組織間で共有化されていくことを意味している。こうした提供サービスの変化は情報保護（セキュリティ）面における詳細なセキュリティポリシーの策定と関連組織間での合意・順守体制が求められることになる。またサービス内容としてリアルタイム性が追求されることにもなり、患者情報の保護だけではなくネットワークシステム全体のセキュリティも検討していく必要があると考える。

実際の医療・介護・福祉の現場では、多職種の人材が働いており、守秘義務の規定があいまいな職種やボランティアも含まれてくる。そこで、医療機関において必要となる課題を明らかにする。研究方法として、文献調査ならびに実際のシステムのケースタディからセキュリティ上の観点から、医療情報システムにおける安全なインターネット直接接続に関するデータベースの有効性を検証する。

（倫理面への配慮）

本研究は、個人情報を扱うものではないので、問題はないと考えられる。

C. 研究結果

I） 事例調査

現在、インターネットを利用し、地域医療連携に広がりがある①Net4U（山形県鶴岡市)、②加古

川地域保健医療情報システム（兵庫県）、③あじさいネットワーク（長崎県）の３事例についての調査結果を以下にまとめる。

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検討する上で、これらの事例などを参考にすることも重要であると考えられる。

(1)Net4U（山形県鶴岡市）

①　ネットワークシステムの機能

患者が通院しているそれぞれの医療機関間でカルテ等の診療情報を共有する仕組みを利用し、他の医療機関で受けた検査、処方薬などを参考にした診察が行われている。受けた検査結果を経過順にグラフや図にする機能や、他の医療機関に患者を紹介するための補助機能も含まれている。

ア）　在宅患者情報共有システム

在宅医療では、主治医の指示書で訪問看護師が患者宅を訪問し、指示書に従って医師に報告する必要があるが、Net4U を使うことで、医師と訪問看護師間のコミュニケーションが向上し、緊密な連携下での、より質の高い在宅医療が可能になっている。

イ）　訪問看護介護システム

訪問看護指示書、訪問看護サマリーなどの看護情報や、サービス利用票等のケアプラン情報もNet4U と連携可能であり、かかりつけ医、専門医及び訪問看護師の間で情報共有することが可能。

ウ）　臨床検査オンラインシステム

荘内地区健康管理センターに検体の検査依頼をして、検査結果をオンラインにて参照することが可能。

エ）　医療情報の共有

医療機関間を相互につなぐことで、検査データやカルテ内容の共有、紹介等の省力化の実現が図られている。

②　ネットワークの通信技術及びセキュリティ対策

当初の通信手段は、INS64／INS1500（※1）での ISDN（※2）網を使用した閉じたイントラネットでの運用だったが、現在は、インターネットを使った VPN（※3）網へと移行している。利用者及びサーバ間の利用には SSL（※4）を採用する等のセキュリティ対策を講じている。また、診療情報を共有することについて、事前に患者に説明し、同意を確認した上で、患者の通院歴のある医療機関以外では参照できない仕組みになっている。

※1 INS64/INS1500：総合デジタル通信網サービス提供の商品名

※2 ISDN：電話や FAX、データ通信を統合して扱う総合サービスデジタル網

※3 VPN：インターネットなど公共のネットワークを利用して、専用線のような環境を実現した仮想閉域ネットワーク

※4 SSL：インターネット上で情報を暗号化して送受信するプロトコル

(2)加古川地域保健医療情報システム（兵庫県）

①　ネットワークシステムの機能

昭和 60 年から集積されている検査及び健康診断のデータベースを基に運用しているオンラインシステムと、可搬記録媒体として IC カードを用いたオフラインシステムを併用している点が、加古川地域保健医療情報システムの特徴となっている。

検査・健診オンラインシステムにより、①各医療施設に対する検査データの自動配信②検査及び健康診断のデータベースの照会③地域住民の健診受診状況の詳細把握が可能となっている。

また、IC カードにより、診療記録や検査・健康診断結果などの記録を個人が保持できるため、適切な保健指導や病診連携などを効率的に進めることが可能。

ア）　検査・健診オンラインシステム（平成６年度供用開始）

検査及び健康診断のデータベースに蓄積されたデータの照会を行うシステム。データ加工は、医療施設側の端末で行う。

イ）　IC カードシステム（平成６年度供用開始）

患者個人の基本データや診療データをカードに記録し、保持・管理することが可能なシステム。平成 18 年度から IC カードである KIND カードでの運用を始めており、安全性が向上している。

ウ）　診療所支援システム（平成６年度供用開始）

ネットワーク接続により、診療所の端末から、その他の医療施設に分散している個人の病歴や検査歴等の保健医療データを時系列的に参照することが可能。

エ）　画像情報システム（地域 PACS 平成 10 年

度供用開始)
地域PACS1により、各医療施設で撮影されたデジタル検査画像を地域内で共有・参照することが可能。

オ)　健康増進システム（平成10年度供用開始)
軽度の循環器系疾病を持つ患者への運動療法と食事指導、生活習慣病の対象者への運動療法や運動指導のための文書作成機能を有している。

②　ネットワークの通信技術及びセキュリティ対策
システムの運用が始まった当初は、ネットワーク基盤はINS64を採用していたが、現在は、トラフィック（※1）増や運用コスト削減のため、インターネット網を使ったNTTPCコミュニケーションズのサービスである「IP-Members」を採用している。
加古川地域保健医療情報システムで活用されているKINDカードは、患者の個人認証機能を備えるほか、個人の保健医療の情報を記録することが可能なカード式カルテとしての機能も有している。KINDカードには保有者の保健医療情報が記録されており、各医療施設において提示することで病気の治療・指導に活用することが可能。
KINDカードは、ICチップに秘密鍵（※2)、接続先のPKI（※3）証明書及びアクセス制御リストを格納しているため、鍵の管理や接続設定が容易であり、ネットワーク接続にはオンデマンドVPN（※4）の認証技術を用いています。加古川地域保健医療情報システムに加入を希望する患者は、「地域保健医療情報システム同意書」をシステム参加医療施設に提出します。同意書については、KINDカードの申込みも兼ねている。

※1 トラフィック：一定時間に特定のネットワーク上を移動する、音声、文書及び画像などのデジタルデー
タの量
※2 秘密鍵：暗号技術の一つである公開鍵暗号方式で使う、本人だけが持つ鍵
※3 PKI：公開鍵暗号方式を使って、暗号化通信やユーザー認証などを行うための仕組み
※4 オンデマンドVPN：IP-Membersにおいて提供される、セッション単位に通信相手とPKIを用いて機器
や機器の所有機関を相互認証するVPNサービス

(3)あじさいネットワーク（長崎県）

①　ネットワークシステムの機能
病院の画像、検査データなどの医療情報を診療所で参照することが可能で、インターネットVPNを用いた比較的安価なネットワーク。
あじさいネットワークで参照可能な医療情報は、市立大村市民病院の検査画像と国立病院機構長崎医療センターの画像を含む検査データ、処方、処置を含む診療録データとなっている。インターネット網を経由して、市立大村市民病院の画像サーバ、国立病院機構長崎医療センターの公開用サーバへ接続する仕組みとなっている。
診療所側はインターネットに接続できるパソコンを用意することで、複数の基幹病院の診療情報、検査情報や画像データを参照することが可能となる。

②　ネットワークの通信技術及びセキュリティ対策
インターネット網を使ったIPSec-VPN（※1）による暗号化通信網を採用している。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」を踏まえた安全なネットワークを構築するために、株式会社エスイーシーのサービスである「ID-LINK」を採用している。
ID-LINKにおいては、PKI証明書要求(PKCS7及びPKCS10（※2）)によるIPSec-VPNによる拠点間のデータ暗号化とファイアウォール機能を用いており、センター側の機器によるウイルス定義ファイルの管理、更新を行うことが可能である。
患者同意については、患者から「あじさいネット説明同意書」の提出を受け、「かかりつけ医」が、情報連携する基幹病院にFAXすることにより、基幹病院側で対象患者の医療情報の参照を許可する仕組みとなっている。

※1 IPsec-VPN：IPによる通信を暗号化するためのプロトコル群で、IPプロトコルのレベルでデータを暗号
化
※2 PKCS7及びPKCS10：公開鍵の認証を要求するために認証局へ送信されるメッセージのフォーマット

II) 分析
医療情報システムにおける安全なインターネット直接接続に関し、セキュリティ上の観点からの分析を行う。

1.　ネットワークセキュリティ

医療情報システムは医療サービスの業務過程にて、様々な情報を生み出し、保存し、利用する。これら情報は個人に密接に紐付く重要な情報資産であり、堅牢に保護しなければならない。この情報資産の漏洩、守備としてネットワークセキュリティ対策が非常に重要である。
ネットワークセキュリティを確保する箇所として、トラフィックの入り口、通信経路、サーバ（端末）のすべての位置で確保することは、2 重、3 重のセキュリティを得ることができるが、コストへの反動が大きい。その為、適材適所のサービスレベルの確保、費用対効果、および運用管理を考慮し、トラフィックの入り口、通信経路でのセキュリティを十分確保することが重要である。
ネットワークセキュリティを確保する為のポイントとして、次の３点を上げる。

①医療情報システムネットワークのすべてのトラフィックの入り口で不正端末の接続を防止する。
②医療情報システムネットワークのすべてのトラフィックの入り口で不正アクセスを防止する。
③医療情報システムネットワークのすべてのトラフィックの入り口で DoS 攻撃を防止する。

2.　ネットワークの脅威

人による意図的、計画的脅威には、以下の種類のものを想定することができる。

① 不正侵入
② ウイルス、ワーム、スパイウェア
③ 悪意のあるソフトウェア
④ なりすまし
⑤ 盗聴

想定すべき具体的な攻撃、攻撃者の行なうであろう行為とその対策について以下にまとめる。

(1)　不正接続、不正アクセス

ネットワークに対する攻撃の要因として、共通の要因として不正端末の接続、不正アクセスが考えられる。ネットワークセキュリティでは、不正端末を接続させない、不正アクセスをさせないことを大目標とすることで、攻撃の実現性を低くする。

表 3-2-1 不正接続対策

攻撃名称	攻撃者の行為	対策例
不正接続	未使用ポートに管理対象外の機器を接続する	●未使用ポートを無効にする ●未使用ポートに無効な VLAN をアサインする ●認証を行なわせる
	使用中のポートに管理対象外の機器を接続する（認証実行ポート）	●MAC アドレスフィルタをかける ●認証を行なわせる
	使用中のポートに管理対象外の機器を接続する（認証未実行ポート）	●MAC アドレスフィルタをかける
	上記の対策を越えてネットワーク機器を接続する	●ネットワーク機器を接続されることによる ●対策を行なう

表 3-2-2 不正アクセス対策

攻撃名称	攻撃者の行為	対策例
不正アクセス	外部からの不正アクセスを行なう	●インターネット上に公開している情報、サービス利用を目的としたインターネットへのアクセスは、行わない。 ●インターネットと医療情報システムネットワーク間は、セキュリティゲートウェイを導入し、対策を行なう ●サービス妨害(DoS)攻撃の対策を行なう ●内部向けに適切なアクセス制御をかける ●偽装アドレスに対するアクセス制御を行なう（RFC2827 フィルタ）
	セキュリティレベルの低いネットワークから不正アクセスを行なう	●セキュリティゲートウェイを導入し、対策を行なう ●DoS 攻撃の対策を行なう ●内部向けに適切なアクセス制御

		をかける ●偽装アドレスに対するアクセス制御を行なう（RFC2827 フィルタ）
	認証済みの端末を不正利用する （認証後、放置された端末を利用）	●端末とサーバ間の通信には、適切なアクセス制御をかけ、影響範囲を小さくする ●アプリケーションに、アクセス制限レベルをかける ●端末自身にふるまい監視機能を装備する（USB メモリなどを使ってプログラムなどをインストールされることを監視する。）

(2)パケットスニファ

ネットワークアダプタカードを無差別モードで使用して、特定のコリジョンドメイン内で送信されるすべてのネット ワークパケットを捕捉する行為

表 3-2-3 パケットスニファ対策

攻撃名称	攻撃者の行為	対策例
パケット盗聴 [関連する脅威] ・不正侵入 ・盗聴	機器の接続に成功し、盗聴を行なう	●スイッチ型インフラを採用し、影響範囲を小さくする ●ネットワーク機器へのログイン（侵入）を防止する（機器の設定を変更させない）
	上記の対策を回避し盗聴を行なう	●暗号化通信を行なう

(1) IP スプーフィング

偽の IP アドレスを送信元にセットしたパケットを送り込む攻撃手法。

表 3-2-4 IP スプーフィング対策

攻撃名称	攻撃者の行為	対策例
IP スプーフィング	ソースアドレスを偽装し、内部へアクセス（攻撃）を行なう	●ネットワークに対するアクセス制御をかける ●偽装アドレスに対するアクセス制御を行なう（RFC2827 フィルタ）
[関連する脅威] ・なりすまし		

(2) サービス妨害(DoS-Denial of Services)

ネットワークの特定の機器に対し、大量のパケットを送信することにより、サーバやネットワーク機器のサービスを停止させてしまう行為。または、ネットワーク内にトラフィックを増大させてネットワークを停止させる行為。

表 3-2-5 サービス妨害対策

攻撃名称	攻撃者の行為	対策例
サービス妨害 [関連する脅威] ・なりすまし ・不正侵入 ・ウイルス、ワーム、スパイウェア、悪意のあるソフトウェア	スプーフィングした上で、攻撃を行なう（医療情報システムネットワーク内から）	●ネットワークに対するアクセス制御をかける ●偽装アドレスに対するアクセス制御を行なう（RFC2827 フィルタ）
	サービス妨害(DoS)攻撃を行なう（医療情報システムネットワーク内から） TCP SYN Flood、Ping of Death、TFN、Trinoo 他	●DoS 攻撃対策を行なう

(3) パスワード攻撃

辞書攻撃やブルートフォース攻撃で、ユーザ情報を入手する行為。

表 3-2-6 パスワード攻撃対策

攻撃名称	攻撃者の行為	対策例
パスワード攻撃 [関連する脅威] ・不正侵入	内外部から不正侵入を行なった後、認証サーバに対し攻撃を行なう	●厳密なパスワードポリシを策定し、運用する（運用管理策）

(4) 中間者による偽装攻撃

通信経路上で、通過するパケットに対し、セッションのハイジャック、パケット内の情報の

改ざん、サービス妨害などを行なう行為。

表 3-2-7 中間者による偽装攻撃対策

攻撃名称	攻撃者の行為	対策例
中間者による偽装攻撃 [関連する脅威] ・不正侵入 ・盗聴 ・なりすまし	経路制御パケットをネットワーク上に流す	●ネットワーク機器を接続されることによる対策を行なう ●偽装アドレスに対するアクセス制御を行なう
	上記を越えて、セッションをハイジャックし、情報の参照、改ざんを行なう	●暗号化通信を行なう

(5) アプリケーションレイヤ攻撃

サーバで一般的に使用するプロトコルを利用して攻撃をする行為。

表 3-2-8 アプリケーションレイヤ攻撃対策

攻撃名称	攻撃者の行為	対策例
アプリケーションレイヤ攻撃 [関連する脅威] ・不正侵入 ・悪意のあるソフトウェア	セキュリティゲートウェイを通過可能なプロトコルを利用してサーバへアクセスする	●ネットワーク機器では、対策なし ●サーバに対するネットワークセキュリティ施策として『ふるまい監視』を導入する

(6) ネットワーク偵察攻撃

公開されている情報、およびアプリケーションを使用して、ターゲットのネットワークに関する情報(IP アドレス、DNS 名、使用ポート番号など)を得る行為。直接的な攻撃ではないが、ネットワークを把握されることで 2 次攻撃に結びつく可能性がある為、考慮する必要がある。

表 3-2-9 ネットワーク偵察攻撃対策

攻撃名称	攻撃者の行為	対策例
ネットワーク偵察攻撃 [関連する脅威] ・不正侵入 ・悪意のあるソフトウェア	不正アクセス用の裏口経路、インターネット経由で偵察を行なう	●セキュリティゲートウェイにより管理、監視パケットの侵入を防ぐ
	医療情報システムネットワーク内部より偵察を行なう	●管理、監視用パケットのやり取りに対し、適切なアクセス制御を行う (ICMP、SNMP、CDP 他)

(7) 信用詐欺攻撃

企業間などで信頼関係を構築したセグメント上のサーバ等から情報を入手する行為。または、同セグメント上で攻撃を受けたサーバの影響が他のサーバにも及ぶ状況。

表 3-2-10 信用詐欺攻撃対策

攻撃名称	攻撃者の行為	対策例
信用詐欺攻撃 [関連する脅威] ・不正侵入 ・悪意のあるソフトウェア	侵入したサーバを経由して、アクセス可能なサーバに攻撃を行なうこと。踏み台攻撃	●サーバのセキュリティレベルを上げる(サーバ) ●サーバに対するネットワークセキュリティ施策 として『ふるまい監視』を導入する。 ●同一セグメント内のサーバ間通信にて不要なものを制限する。

(8) ポート転送攻撃

公開サーバへのアクセスに成功し、セキュリティゲートウェイを通過可能な IP アドレス、ポート番号を使って内部ネットワークへの攻撃を行なう行為。

表 3-2-11 ポート転送攻撃対策

攻撃名称	攻撃者の行為	対策例
ポート転送攻撃 [関連する脅威] ・不正侵入 ・悪意のあるソフトウェア	アクセス制御で通信を許可されているサーバにアクセスし、内部への侵入を行なう	●サーバのセキュリティレベルを上げる ●サーバに対するネットワークセキュリティ施策として『ふるまい監視』を導入する

(9) ウイルスおよびトロイの木馬アプリケーション攻撃

ウイルスとは、他のプログラムに添付され、

ユーザ端末上で特定の望ましくない機能を実行する、悪意のあるソフトウェアをさす。トロイの木馬は、アプリケーション全体を別のプログラムのように見せて実行させる悪意のあるソフトウェアをさす。

表 3-2-12 ウイルスおよびトロイの木馬アプリケーション攻撃対策

攻撃名称	攻撃者の行為	対策例
ネットワーク偵察攻撃 [関連する脅威] ・不正侵入 ・悪意のあるソフトウェア	アクセス制御で通信を許可されているサーバにアクセスし、内部への侵入を行なう	●サーバ、端末でウイルスの検出、除去が行なえるようにする ●サーバ、クライアントに対するネットワークセキュリティ施策として『ふるまい監視』を導入する

1. エンドポイントセキュリティ

医療情報システムネットワークの終端に接続されるものとして、エンドポイントデバイスのセキュリティ対策についてまとめる。病院内に、「PC 端末利用手順」や「PC サーバ利用手順」に類する PC に関連するセキュリティポリシー(セキュリティ要件)が存在していることを前提とする。

2. 想定される脅威

医療情報システムネットワークのエンドポイントに配置される、PC 端末、PC サーバには、機密性、完全性を要する重要なデータがおかれ、システムの外側から内側に向かって見ると、システム管理者にとっては最後の防御点である。

また、反対にエンドポイントの観点でみると、入出力デバイスを経由した情報漏洩、および悪意のあるソフトウェアの侵入という別の観点での脅威も想定する必要がある。

これらの想定される脅威の概要を、表 3-4-1 にまとめる。

表 3-4-1 エンドポイントへの脅威と分類

脅威の分類	脅威
悪意のある動作	●オペレーティングシステムに対する不正な改ざん ●意図しないファイルの削除、新規ファイルの作成 ●意図しないプログラムのインストール ●バックドアを仕掛けるプログラムのインストール ●バッファオーバーフロー攻撃 ●DoS アタック ●メールソフト管理下のファイル(アドレス帳)への不自然、不合理なアクセス ●ネットワークリソースへの不自然、不合理なアクセス(ポートスキャン、DoS 攻撃など) ●P2P 関連のファイル交換ソフトウェアのインストール
ポリシー関連の動作 (悪意がない場合でも危険性がある。)	●ウェブブラウザなどからファイルをダウンロードさせるかどうか。ダウンロードしたファイルの危険性を考慮する。 ●ダウンロードしたファイルを実行させるかどうか。ダウンロードしたファイルの危険性を考慮する。 ●メールの添付ファイルを開封させるかどうか。添付ファイルの危険性を考慮する。 ●着脱可能な記憶装置を使用許可とするか。着脱可能な記憶装置(USB メモリなど)経由での悪意のあるファイルの侵入や情報漏洩。読み出しと書き込みの許可、不許可の区別。 ●PC に内蔵されている、記憶装置を使うか。読み出しと書き込みの許可、不許可の区別。読み出しを許可した場合は、ウィル

	スの混入、書き込みを許可した場合は、情報漏洩の危険性がある。 ●メッセンジャーソフトを使用する際、プログラムをダウンロードさせるか。 ●新規にプログラムをインストールさせるか。 ●既にインストールされている、特定のアプリケーションを利用させるか。

3. エンドポイントに対する脅威への対策

前項で述べた、想定される脅威への対策方法で、悪意のある動作に対する抑止機能はすべて有効(無条件で不許可)にすることを強く推奨する。

ポリシー関連の動作については、「PC端末利用手順」などのセキュリティポリシーをベースに業務内容に応じて動作の許可、不許可を決定する。

許可、不許可設定のレベルとログレベルについては次のようなものがある。

表 3-5-1 動作の許可、不許可とログレベルについて

許可／不許可	詳細とログレベル
1. 不許可 ログレベル	ポップアップウインドウなしに不許可となる。 ログレベル:Alert
2. 許可 ログレベル	許可。 ログレベル:information
3. 利用者が選択(許可前提) ログレベル	ポップアップウィンドウが現れ、利用者に選択させる。許可前提で、5分経過して選択されない場合、許可となる。 ログレベル:Warning
4. 利用者が選択(不許可前提) ログレベル	ポップアップウィンドウが現れ、利用者に選択させる。不許可前提で、5分経過して選択されない場合、不許可となる。 ログレベル:Warning
5. 不許可 ログレベル	ポップアップウインドウが表示されて不許可となる。 ログレベル:Alert

ポリシー関連の動作に対して、抑止するか、利用させるかの決定は、運用(利便性)に極めて密接に関わってくるため、運用時の動作を想定しながら決定する必要がある。

ログに関しては、ネットワークの帯域への影響や管理サーバの性能、記憶装置の容量を勘案した上でログを取るか取らないかを決定する必要がある。

D. 考察

現状、病院情報システムネットワークは、セキュリティ確保の観点からHTTPやE-Mailによる通信をインターネットやWANを経由して行なわないネットワークとしている。しかし、急速に進む高齢化社会において、地域医療連携(病診連携、病病連携等)のニーズは高まる一方であり、患者、病院、診療所側双方に有益なサービスを提供するためには、病院情報システムにおいても、WAN、インターネット接続を行なえる必要性がでてきている。

病院情報システムからインターネット接続を行う場合、既に述べてきたような障害やウィルス感染などによるネットワークシステム、サーバシステムの停止は、診療業務に影響を及ぼすだけでなく、関連病院が保持する患者情報に影響が及ぶ可能性があるため、十分なセキュリティを確保した上でサービスを行なわなくてはならない。

患者、病院、診療所側双方に有益である根拠を以下に示す。

・患者様への医療サービス、生涯1カルテ、重複の検査の回避が可能

・医療サービスの高度化への対応が可能

・健全な病院経営が可能

・法改正への迅速な対応が可能

1. ネットワークセキュリティのアーキテクチャ

医療情報システムのネットワーク方式設計で採用するアーキテクチャは、多層防御(Defence in Depth)の概念を採用すべきと考える。

医療情報システムネットワーク内では単一のソリューションに頼ってアクセス制御をした場合、その単一のソリューションに障害があった場合、ワークセキュリティの方式設計では、同様の機能を持つソリューションをネットワークトポロジの異あるいは、その単一のソリューションを攻撃者が突破した場合、セキュリティの脅威は増大する。そこで、シングルポイント(単一のソリューション)によるセキュリティ脅威を軽減するために、ネットなった場所で実装し、2 重、3 重の防御体制を取ることが重要であると考える。

次に、多層防御 (Defence in Depth)の概念図を示す。

表 4-1-1 多層防御 (Defence in Depth)の概念

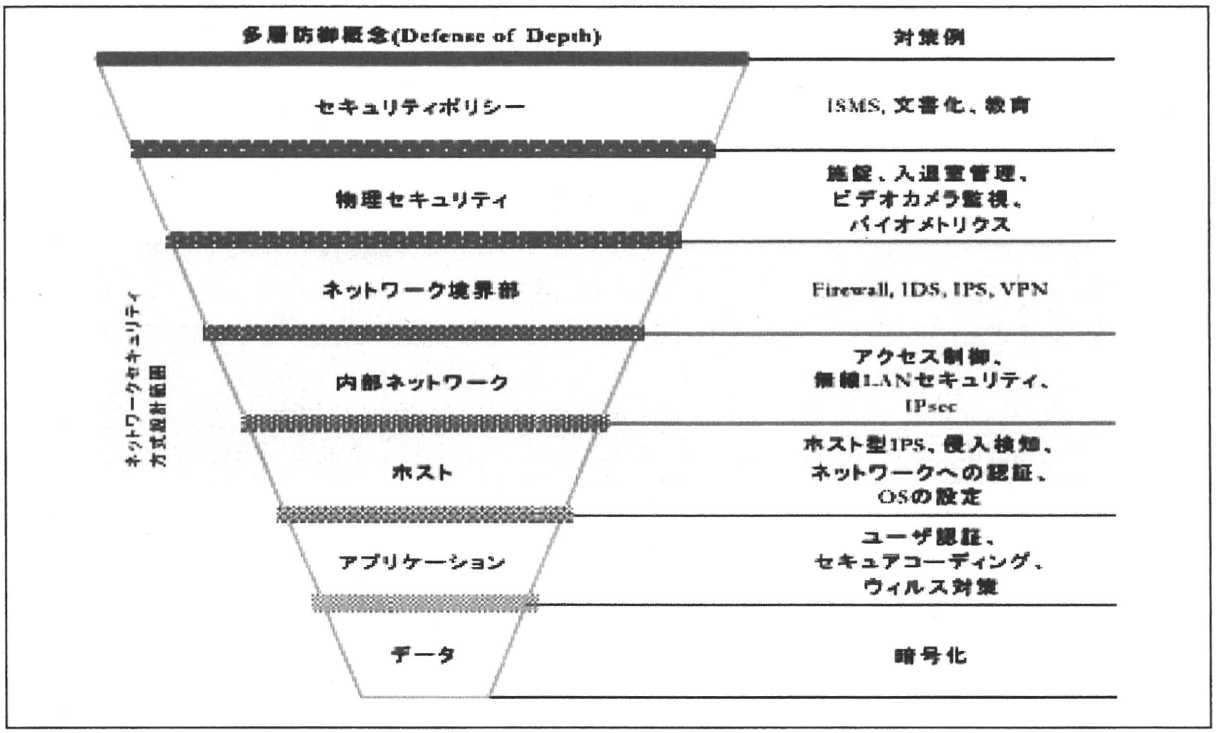
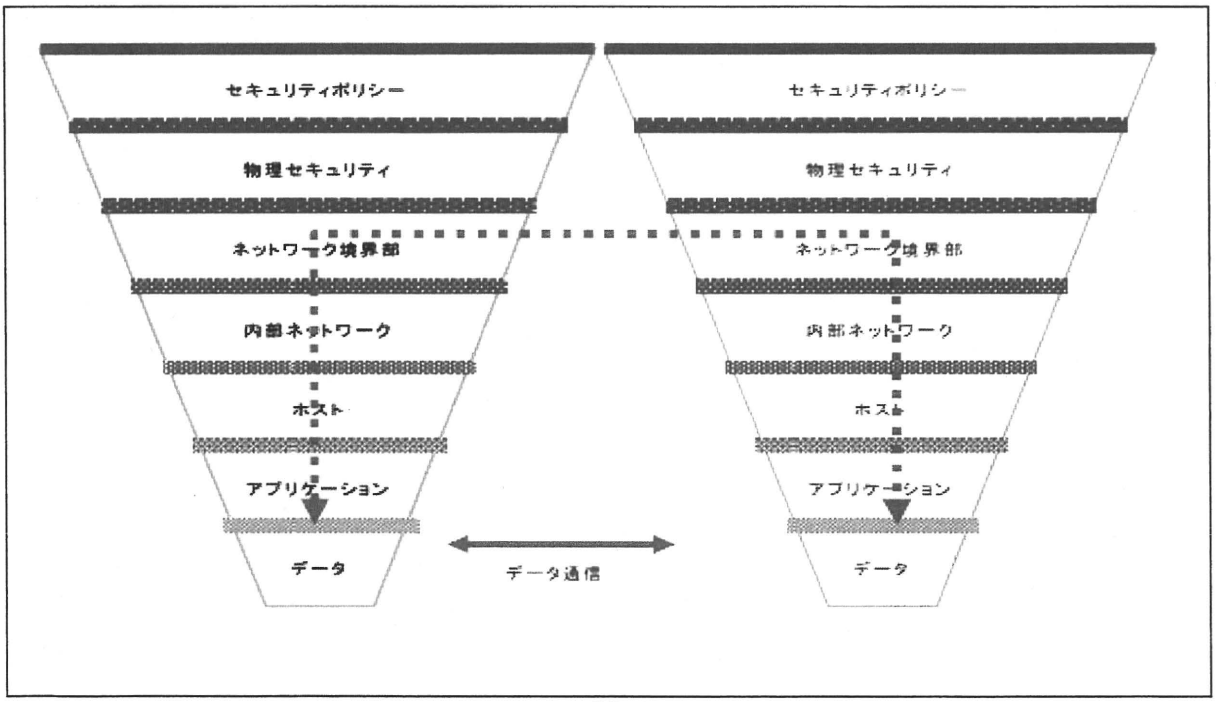


表 4-1-、多層防御 (Defence in Depth)の概念



2 重、3 重の防御体制を取るためには、ネットワークトポロジとセキュリティの脅威の軽減の観点でもっとも有効な設置場所を検討し、運用管理コストを含めた費用対効果を検討した上で実装する位置を決定することが重要である。

E. 結論

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。データ領域とデータ利用領域を論理的に分割したデータの保護を実現し、また、基幹ネットワークへの不要な通信が流入しないよう、ブロードキャストドメインごとにアクセス制御する方式設計も重要である。これはデータ領域を保護するだけではなく、ネットワークの安定化への貢献にもつながることである。

エンドポイント(有線、無線 LAN)のネットワークに対して、不正端末、不正利用者の脅威を軽減する対策や、セキュリティコンプライアンス機能 (PC 端末のセキュリティポロシへの準拠度合いの監査)、ウィルスの感染、拡大を軽減するセキュリティ方式を検討、方式として適用し、エンドポイントだけではなく、エンドポイントのふるまい制御機能も併せて検討する必要がある。

これらセキュリティ機能の導入により、エンドポイントにおけるセキュリティを高めることができ、結果として、情報漏洩対策への大きな貢献が可能となる。

病院情報システム端末から安全にインターネットへ直接接続を行うためには、すべてのネットワークセキュリティ機能を有機的に結合し、2 重、3 重の防御体制を取ることで、より大きな効果を得ることができると判断する。

F. 研究発表

1. 論文発表

1). Akiyama M, Koshio A, Kaihotsu N. Analysis on data captured by the barcode medication administration system with PDA for reducing medical error at point of care in Japanese Red Cross Kochi Hospital. Taked a H(Ed.): E-Health 2010, IFIP AICT 335, pp. 122-129, 2010.

2). Koshio A, Akiyama M. Capturing and analyzing injection processes with point of act system for improving quality and productivity of health service administration. Takeda H(Ed.): E-Health 2010, IFIP AICT 335, pp. 114-121, 2010.

3). Akiyama M, Koshio A.,Kaihotsu N. Analysis of data captured by barcode medication administration system using a PDA; aiming at reducing medication errors at point of care in Japanese Red Cross Kochi Hospital. Stud Health Technol Inform. 2010; 160(Pt 1):774-8.

4). 秋山昌範, 森川富昭, 清水佐知子, 小塩篤史, 長谷川友紀. 保健医療の最適化と医療情報学の役割. 医療情報学 30(Suppl.) 212-213, 2010.

5). 小塩篤史, 秋山昌範, 中村章一郎. 診療行為実施時点において入力されたデータを用いた看護業務分析. 医療情報学 30(Suppl.) 1082-1085, 2010.

.

2. 学会発表

1). Akiyama M., Koshio A, Kaihotsu N. Analysis of data captured by barcode medication administration system using a PDA; aiming at reducing medication errors at point of care in Japanese Red Cross Kochi Hospital. Medinfo 2010 - 13th World Congress on Medical and Health Informatics, Cape Town, South Africa. Sep., 2010.

2). Akiyama M Koshio A, Kaihotsu N. Analysis on data captured by the barcode medication administration system with PDA for reducing medical error at point of care in Japanese Red Cross Kochi Hospital. IFIP (International Federation for Information Processing) - IMIA (International Medical Informatics Association) First Joint Symposium on World Computer Congress 2010, Brisbane, Australia Sep 2010.

3). Koshio A, Akiyama M. Capturing and analyzing injection processes with point of .act system for improving quality and productivity of health server administration. IFIP (International Federation for Information Processing) - IMIA (International Medical Informatics Association) First Joint Symposium on World Computer Congress 2010, Brisbane, Australia, Sep., 2010.

4). Koshio A. Applying US physician demand projection model to Japan. International Conference on future healthcare workforce

supply and demand. Tokyo, Japan. March 2011.
5). 小塩篤史. ワークショップ；保健医療の最適化と医療情報学の役割（パネリスト), 第 30 回医療情報学連合大会（第 11 回日本医療情報学会学術大会）2010 年 11 月.
6). 小塩篤史,秋山昌範,中村章一郎. 診療行為実施時点において入力されたデータを用いた看護業務分析. 第 30 回医療情報学連合大会（第 11 回日本医療情報学会学術大会）2010 年 11 月.
7). 小塩篤史,秋山昌範. 診療行為実施時に捕捉されたデータの解析を通じた医療安全マネジメント. 第 14 回日本医療情報学会春季学術大会. 2010 年 5 月.

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

院内医療情報システムとの情報管理・連携方法の調査・検討

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、医療情報システムを導入し、医療の効率化や迅速化を行っている。さらに、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階層に分けている。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、業務システムを利用する。

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、部門システムなどの診療に必要なシステムが接続されている。

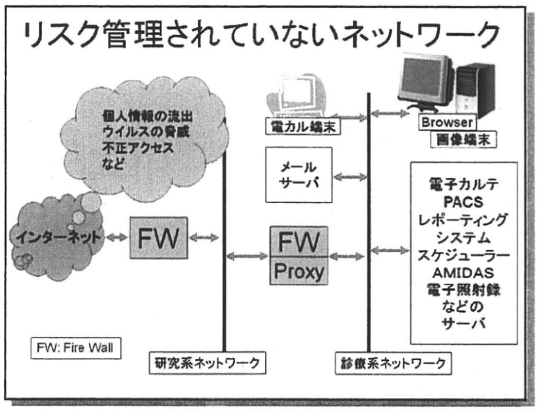


図１　リスク管理されていないネットワーク

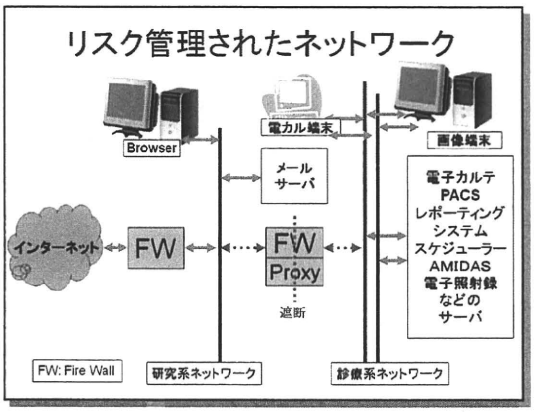


図２　リスク管理されたネットワーク

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、幸いまだ事故はないが、研究系のネットワークでは、ウイルス感染事故が数件起きていた。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＋件検出され、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。

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、以下のような者が考えられる。

(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など）へのアクセスの不備

(b) 病院内外に対する電子メールの連絡ができなくなり、迅速な情報伝達が不能となる

C.4 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、患者は紹介もと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、インターネットが必要となり、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

以下の表１のようなメリット・デメリットがある。

表１ 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	個人 ID	名寄せのコスト

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る。この場合に、暗号化技術やユーザの認証技術を用いて安全・安心な患者が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（図 3)。

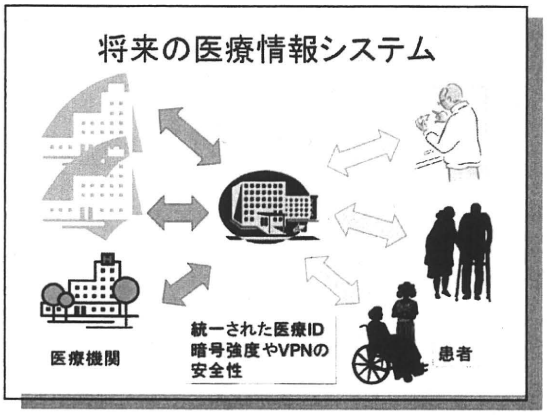


図３ 将来の医療情報システム（関連病院や患者との連携）

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。

また、患者や複数医療機関でシステムを共有する場合には、統一された患者 ID が必要となる。医療ＩＤについて、外国では、スエーデンやノルウエーなどでは、医療ＩＤが確立している。また、アメリカでもソーシャル・セキュリティー番号を名寄せに利用することが可能である。日本でも、早く医療関連の情報を一元的に扱えるような機構が必要と思われる。

日本でも社会保障ファイナンスを一元化し、社会保障番号で管理する案が提案された経緯があるが、税金や年金などの番号とは、共通にせず、医療だけに特化したＩＤ番号を創設するべきであろう。現在の情報技術を利用すれば、医療 ID 番号を税金の納税者番号や社会保障番号とリンクすることは、技術的に容易である。国民の医療福祉の推進のためにも、早急に医療ＩＤ

制度確立すべきと考える。

E．結論

インターネット接続による医療機関外部からのリスク、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の点から病院情報システムについて検討し、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コストが挙げられる。

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

病院における診療端末のインターネット接続に関する研究

分担研究者　山本　隆一　　東京大学大学院情報学環　助教授

研究要旨　従来、病院の情報システムはインターネットと隔離されていることが多い。しかし、外部ネットワークとの接続はレセプトオンラインをはじめ、電子署名の検証など必須となりつつある。本分担研究は病院における実態を明らかにすると同時に接続の方策を提言することにある。本年度は実態を３つの大学病院で調査した。

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への医療機関側からの要求は増大している。またブロードバンド等の普及により、市民のネットワークリテラシは確実に向上しており、患者が自らの診療情報へのインターネットを介したアクセスを希望する場合も今後増加するであろう。しかし、たとえレセコンであってもプライバシーに機微な電子化情報を大量に保有しており、安全管理には万全を期すことが求められている。厚生労働省は「医療情報システムの安全管理に関するガイドライン」公表し、版を重ね適切な安全管理指針を示している。この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、かなり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。本研究の目的は特に病院においてこのような事情に対し、特別な専門知識を持たない医療機関が、自らの情報資産の安全を確保した上で安全にインターネットと通信できる状態にすることで、現状を調査し、実現のための方策を提言することにある。

B．研究方法

３つの大学病院で医療情報システム管理者を中心にインタビュー調査をおこなった。インタビュー項目は以下の３点を中心に、実際の対策を聞き取った。

Ｑ１．診療端末とメール、Web など閲覧するインターネット端末が別ということで、安心だと思われる点（セキュリティ面）などありましたらお聞かせください。また、診療端末がインターネットに接続していないために不便な点などあればお聞かせください。

Ｑ２．診療の際にインターネットによる情報の閲覧、参照が必要と思われますか？

また、もし必要な場合どのような情報が必要もしくは便利だと思われますか。（例、医薬品の副作用情報、EBM など）

Ｑ３．もし病院内の診療端末を直接インターネットに接続することになった場合、不安な点がありましたらお聞かせください。

C．研究結果

３つの病院はそれぞれ特色があるので個別述べたい。

T 大学病院：

すでに診療端末はほぼ完全にインターネットに接続されている。したがって Q1 に対しては前提が異なっており、回答はなかった。Q2 においては例示した医薬品の副作用や EBM は重要性が低かったが、むしろ、初診患者の職業に関する検索など、患者の社会的背景の把握が重要という指摘があった。また診療業務外の利用（研究や教育など）も必要な時にすぐに出来る点は評価が高かった。Q3 についてはこの病院はウイルス侵入などの事案があったものの、実際には USB メモリを介した感染であり、インターネット接続によるアクシデント・インシデントはこれまでになく、現状の対策（ファイアウォール、ウィルススクリーニング等）で特に不安は感じていないとのことであった。

A 大学病院:

現状、診療端末はまったくインターネットに接続されていないが、Windows Server のターミナルサービスを用いて、DMZ にある Internet 接続 Windows Server を介して、診療情報端末上の仮想ターミナルでインターネットアクセスを許可する機構を完成させサービスイン直前であった。ターミナルサービスを拡張し、医局の PC やサーバとの情報転送などもサポートし、ユーザの要求にスペック上はほぼ完全に対応できるとのことであった。

Q1 に関しては診療情報システム管理部門としては特に不安は感じていないが、これまで厳重に制限していた経緯から、それなりの説得あるセキュリティ対策が必要という認識であった。Q2 については T 大学病院と同様。Q3 についてはサービスイン直前である仕組みは診療情報システムへの影響はなく、運用上の不安（不正サイトへのアクセスなど）以外は特に感じていないとのことであった。

K 大学病院:

現状はもっとも複雑で、診療部署には２種類の端末がある。一つは完全に診療情報システムと隔離されたインターネット接続端末で、もう一つは診療情報システムの専用端末である。さらにこの診療情報システム専用端末には２種類あり、ひとつは外部インターネット接続がまったく不可能な端末であるが、もう一つは非常に限定された WEB アクセスが許可された端末である。アクセスできるサイトは申請を行い許可されなければならない。Q1 については A 大学病院と同様で、特に不安は感じていないが、これまでの経緯で院内的には相当な説明責任を果たさなければ接続できない状況とのことである。Q2 に関しては T 大学病院と同様。Q3 に関しては情報システム管理者としては特段の不安はないが、ユーザは運用上の不安を覚えているとのことであった。

D．考察

今回の３つの大学病院のインタビューでは情報システムの管理者自体はファイアウォールによる外部からのアタックを防止し、適切に悪意のあるソフトウェアをスクリーニングできれば接続することに不安は感じていなかった。むしろ一つの病院を除いてこれまで厳しく制限していた経緯から接続するための説明を行うための対策に苦慮しているように思える。悪意のあるソフトウェアによる事故はあったものの、インター

ネットを介した事故はほとんどなく、可搬媒体によるものが主体で、そういう意味では接続自体の実際的な脅威は少ないかも知れない。しかし問題は間に人が介する運用上の事故であり、情報を安易にコピーできれば適切な安全処置なしにインターネット上に守秘性の高い情報を流してしまう恐れは否定できない。ちなみにK大学病院では診療情報システムを扱う端末ではすべての外部インターフェイスを物理的に使用不可としている。ただしT大学病院はそのような対策はとられていないが、特段の事故は経験していないとのことであった。

今回はいずれの大学病院であり、情報システムを管理するスタッフも豊富で、利用者もそれなりに意識が高い。ここで得られた知見をそのまま一般の医療機関に援用することは危険であろう。しかし外部との情報交換がかなりの高頻度である施設であることも事実で、過不足ない対策を論じる上での参考にはなると考えられる。

E. 結論

3つの大学病院における診療情報システム端末からのインターネット利用はそれぞれ特色のあるものであった。今後は一般の医療機関に調査を広げると同時に運用上の問題を解決するための、技術的、運用的な対策の検討を行う必要があると考えられる。

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。

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　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は、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が、その際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。本年度は、医療機関内に設置された情報端末の認証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技術的方法について検討した。

A．研究目的

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。

そこで、本研究では、情報端末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、医療機関内に設置された情報端末の認証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の整理と技術的実現方法の検討をおこなうことを目的とした。

B．研究方法

平成２２年度の研究では、まず保健医療の各分野における利用シーンの整理をおこない、それに基づき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整理する。そして、その結果に基づき、オンデマンドVPN技術を拡張して、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検討する。

C．研究結果および考察

厚生労働省が策定している「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、ネットワークを介して、外部と医療情報をやりとりする場合は、ネットワーク事業者・システム事業者と医療機関との間で責任分界点を明確にすることが必要とされて