20112902 8A

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

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

平成２３年度　総括・分担研究報告書

主任研究者　山本　隆一

平成２４（２０１２年）年５月

目　　次

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
総括研究報告書

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

主任研究者　山本　隆一　東京大学大学院情報学環・准教授
分担研究者　中島直樹　九州大学医学部付属病院医療情報部・准教授
分担研究者　田中勝弥　東京大学付属病院企画情報運営部・助教
分担研究者　矢野一博　日本医師会総合政策研究所・主任研究員

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、扱いは不明瞭で、一般の医療機関が安易に接続できる状況ではない。本研究の目的はこのような事情に対し、ニーズとリスクおよび、その対策と結果として残る残余リスクを実証的院明確にし、ガイドラインのあり方やゲートウエイセンタの必要性などの、今後の施策に資する提言をまとめた。

最初に本研究は目的が政策提言であり、また班員の所属するフィールドで調査を行うなど、主任研究者、分担研究者が班として一体的に研究を進めたために、総括研究報告書にまとめて記載をする。

A．研究目的

医療機関にとって、診療情報システムの管理運用においては二つの意味で安全性が確保されなければならない。一つは守秘義務と保存義務のある患者情報が含まれているために、法的責務として漏洩があってはならないし、保存期間中の遺失も許されない。もう一つは業務の継続性の確保で、診療情報システムで動作異常や可用性の低下のために、診療行為を阻害することは許されないし、直接の診療行為ではなくても、例えば受診料の徴収ができないなど、組織の運営に支障が生じることも避けなければならない。その一方で、医療情報のIT化の進展は、組織内だけで情報が閉じることを許さなくなっていることも事実である。多くの医療機関等は早晩、診療情報システムと外部のネットワークを一定の制限下であるにしても接続しなければならなくなることが予想される。本研究は医療機関等が外部のネットワークに接続した場合のリスクを分析し、適切な対応を提言として示すことにある。

B．研究方法

昨年度実施した事例調査と医療機関へのインタビュー調査を元に研究班全員および研究協力者でブレインストーミングを行い、ニーズ分析と接続によるリスク分析を行った。またすでに診療情報システムをインターネット接続している大学病院と診療情報システム直接ではないが、診療現場にインターネット接続をしているＰＣを設置している大学病院の２病院でパケット解析装置（Cisco Systems社 Service Control Engine）を用い現状分析をおこなった。その上でリスクに対して対応を検討し、指針案としてまとめた。

C．研究結果

C－１　２大学病院における現状分析

C－１－１　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－１－２　Webサイト利用状況

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エ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－１－３　外部からの攻撃

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。

C－２　リスク分析

C－２－１　インターネット接続のニーズ

ニーズとしては診療業務上のニーズと情報システムの保守上のニーズに分けて考えることができた。

診療業務上のニーズ

1. 地域医療連携・地域連携パス：
   現状は紙ベースあるいは CD-R などの媒体による情報連携が主体であるが、地域における共同診療やその進化形である地域連携パスの試みが諸地域で行われている。このような有機的な情報連携にＩＴを用いる個とは内閣官房がまとめた新たな情報通信技術政策の工程表でも「シームレスな地域医療連携」として促進を図っており、また地域医療再生基金を用いた計画の中にも多く見られている。これまでは病院の地域連携室等にインターネット接続端末を置き、媒体等でエアギャップを超えて情報を移動させるような間接的な連携が主体であったが、一般的になればなるほど、このような間接的な手法は非効率となり、今後は診療情報システム自体が直接的に連携できるニーズが生じることは確実である。
2. 医療計画支援:
   地域での医療計画の策定は医療法で定められているが、合理的な計画を策定するためにはエビデンスとなる事実の収集を迅速に行う必要がある。

慢性疾患の場合はオンラインでなくとも収集可能であるが、感染症のOutbreakやPandemicに効果的に対応するためには持続的で迅速な情報収集と分析が必要であり、オンライン接続のニーズが存在する。

3. 診療報酬請求:
診療報酬請求のオンライン化は2006年のIT新改革戦略で導入が謳われ、かなり普及している。導入期に作られた接続のための指針ではオンライン請求用の端末は独立したＰＣを用い、他の用途に用いてはいけないとされている。診療情報システムの大部分が外部ネットワークに接続されていない状況ではやむを得ないルールとも言えるが、セキュリティ上の必要条件とは言えない。リソースとしてもコストとしても無駄があり、安全に外部ネットワークに接続できるのであれば、より合理的なルールに変更することも可能である。

4. 従業員による外部からの診療情報システムへのアクセス:
医療崩壊が言われて久しく、地域医療再生基金による改善をはじめとするいくつかの試みがされているが、根本的な解決にはいたっていない。過酷な労働を強いられている医師等にとっては病院外からの院内の診療情報へのアクセスはニーズとして存在する。自宅や出張先ではオープンネットワークを利用してアクセスする以外は現実的ではなく、適切なセキュリティ確保は前提ではあるが、診療情報システム側の受け口として外部ネットワークへの接続ニーズが存在する。

5. 臨床治験における EDC (Electronic Data Capture):
我が国の臨床治験は数多くの問題を抱えているが、診療現場のいわゆる二度手間も大きな障害となっている。データ収集にITを導入する試みが行われているが、あくまでも収集する側の利便性のためであり、診療医あるいは治験支援員が手入力で転記していることが大部分である。複数の治験を平行して実施している場合、診療現場に複数の EDC 端末が持ち込まれていることもある。臨床治験に対応した診療情報システムから直接CRFを出力・送信できることが望ましいことは明白でニーズとして存在する。

6. ASP, SaaS による診療情報サービスの導入:
中小の医療機関で診療情報システムを時前ですべて整備することは管理コストが高く、このことが診療情報の電子化や標準化の妨げとなる。2010年2月の厚労省通知で適切な契約を行えば民間事業者に診療情報の保存を委託することが可能になり、ASPやSaaSによる診療情報システムの運用が可能になった。経費の管理労力の両面から改善される可能性があり、また標準化への対応も容易になる。さらに診療報酬改定に対応するコストも軽減される可能性が高く、推進されるべきと考えられる。このためには導入する医療機関は外部ネットワークへの接続は必須である。

7. 電子署名の検証:
診療情報の電子化が進むにつれて、情報の責任の所在を明確にするための電子署名が使われる機会が増加する。電子署名を検証するためにはCRLへのアクセスが必須であり、こ

れは外部ネットワークへの接続なしには行えない。

8. 院外の患者データの閲覧:
長崎県のアジザイネットプロジェクトのような開示型の情報連携やPHR、どこでもマイ病院に医療機関がアクセスするためには外部ネットワークへの接続は避けられない。現状は独立した端末をそのために使用している場合もあるが、オンライン診療報酬請求と同様にリソースやコストの無駄が生じている。さらに情報の転記が困難など、致命的な欠陥もあり、診療情報システム自体からのアクセスがニーズとして存在する。

9. その他の診療に必要な情報収集:
緊急安全性情報、診療ガイドライン、患者の勤務先の状況等プロファイルの検索、紹介先医療機関等の検索、
災害情報、文献等の検索などが昨年度実施したインタビューから抽出することができたニーズである。

診療情報システムの保守上のニーズ

1. OSのアップデート:
OS の脆弱性に対応するためのアップデートは、少なくとも重要なものは迅速に実施する必要がある。ただし、外部ネットワークに接続するだけで、これが可能になる訳ではなく、診療情報システムのアプリケーション自体がアップデートにより、誤動作を起こす可能もあるために、遅れている場合も少なくはない。OSの提供している機能を適切に使っていれば問題は少ないはずであるが、そうではないアプリケーションも多く、また仮に適切な設計であっても、動作の確認が必要である。ただ、媒体等でアップデートファイルを導入することで十分という訳ではない。

2. ウイルス等の不正ソフト対策のための定義ファイル等の更新:
OS アップデートに比べればアプリケーションへの影響は少ないと考えられ、コンピュータウイルス感染事故が散見される現状を考慮すれば、適切な更新は必須である。

3. マスターファイルの保守:
通常マスターファイルは組織内でメインテナンスするものであるが、薬剤マスターに関しては、2つの理由で全薬マスターが望ましい。一つはDPC 対応医療機関では持参薬を服薬することがあり、組織ごとのマスターでは対応できない。2つめは後発薬への変更が調剤薬局でされたことを記録する場合で、この場合も全薬に対応したマスターが必要になる。全薬マスターは組織内でメインテナンスすることは不可能で、日々、ダウンロードして更新しなければならない。

4. リモートメインテナンス:
診療情報システムそのものや放射線診断機器、検査機器などはオンサイトの保守は費用が嵩む上に即時性に欠けることがある。そのため、ベンダーまたは保守担当会社がリモートで保守を行うことが一般的である。その目的のために ISDN 回線を用意する場合もあるが、保守対象システムや機器が増加すれば合理的とは言えないし、医療機関側の管理負担も増加する。IP-VPN や Internet VPN で対応することが求められている。

5. バックアップ:
東日本大震災やそれに伴う電力不足はバックアップの重要性を再認識させた。それもオンサイトのバックア

ップでは不十分で、遠隔地バックアップが求められる。媒体で都度輸送することも考えられるが、コストの点を考えても合理的とは思われない。オンラインの遠隔地バックアップが求められる。

これらのニーズのいくつかはオープンネットワークではなく、専用線やIP-VPNでも要求を満たすことは可能であるが、複数のニーズに対応する場合や、要求に応じて接続先を変更する場合などはInternet（要求によってはその上でのVPN）を使うことが合理的である。

C－2－2　具体的なリスク分析

前節で列挙したニーズへの対応としてInternetに診療情報システムを接続した場合のリスクを分析した。

1. コンピュータウイルス等の悪意のあるソフトウエアの侵入:
   悪意のあるソフトウエアが外部ネットワークから侵入した場合、まず、診療情報システム自体の動作に影響を与える可能性がある。最悪の場合、機能停止に陥る可能性がある。さらに、悪意のあるソフトウエアによって情報が外部に漏出する可能性がある。さらに外部ネットワークへ増殖した悪意のあるソフトウエアを再配布したり、不正な通信を大量に行い、DOS攻撃をしかけたり、SPAMメールを大量に送信する可能性もある。
2. 外部からの不正アクセス:
   外部に開いた口があればかならずポートスキャンや、特定のポートに対する不正アクセスがありうる。通常はOS自体で防御可能であるが、前項の悪意のあるソフトウエアによって、特定のポートをオープンな状態にされる可能性があり、またOS自体を改変される可能性がある。
3. DoS攻撃（Denial of Service Attack）:
   外部に対して何らかのネットワークサービスを提供している場合、そのサービスに大量のリクエストを出すことで、サービス提供を不能にする攻撃。WEBサービスがもっとも標的にされやすい。
4. 通信に対する攻撃:
   パケットやセッション自体になりすましたり、盗聴、改ざんを行う攻撃が存在する。
5. 内部からの不正または迷惑行為:
   外部に対する不正アクセスや大量の通信による帯域占拠がありうる。組織内の利用者が故意に行う場合だけではなく、悪意のあるソフトウエアに感染したＰＣから外部に攻撃する場合もある。
6. 不適切な業務外使用:
   業務と無関係な株式取引や、SNSの利用などが考えられる。またP2Pソフトを不適切に用いた著作権侵害事件も一般には数多く見られる。

C－2－3　対策

リスクに対して対策を検討した。

1. コンピュータウイルス等の悪意のあるソフトウエアの侵入:
   悪意のあるソフトウエアの大部分は汎用的なOSの脆弱性を利用するもので、OSのセキュリティアップデートを確実におこなっていれば防止できるものが多い。ただOS提供者のアップデートが間に合わない場合もあり、いわゆるワクチンソフトや悪意のあるソフトウエアを除去する能力のあるファイアウォールの設置は必須である。さらに診療情報システム

に OS の機能に大きく依存する通信機能を使うことは控えたほうが良い。例えば Microsoft Windows 系の OS における NetBIOS は悪意のあるソフトウエの標的になり、また拡散の手段となることが多く、組織内の被害の拡大につながる。したがって、NetBIOS を用いた通信を小さなセグメントに閉じ込める等の対策は被害の拡散の防止に有用である。ただ、我が国の診療情報システムで経験された悪意のあるソフトウエアに関する事故の大部分はネットワーク経由の感染ではなく、USB メモリなどの可搬媒体からの感染であり、この対策はネットワーク接続の有無にかかわらず行う必要がある。また外部の WEB サービスを用いること許可する場合は、相当な注意が必要で、可能であれば、アプリケーション・ファイアウォールを用いて、危険なサイトをブロックすることが望ましい。

2. 外部からの不正アクセス:
OS 自体のアップデートが重要なことは言うまでもないが、それだけでは不十分で、ファイアウォールの設置と適切な設定は不可欠である。基本的には直接診療情報システムに外部からパケットが流れ込むことは禁止すべきで、DMZ（DeMilitarized Zone）の設置は必須である。DMZ に設置したアプリケーションゲートウエイを介して WEB でああれ、SMTP であれ通信しなければならない。WEB サーバのソフトウエアの脆弱性にも最新の注意が必要で、多くの WEB ページ書き換え攻撃はサーバソフトウエアの脆弱性を利用している。PHP スクリプトを利用することがもっとも多く、PHP 自体のバージョン管理や脆弱性のあるスクリプトの使用が起こらないようにチェックする必要がある。
3. DoS 攻撃（Denial of Service Attack）:
早期に検出し、悪意のある攻撃サイトからの要求を無視する必要がある。踏み台を用意したり、多数のサイトから同時に攻撃されることもあるので、注意深い監視が必要である。
4. 通信に対する攻撃:
盗聴・改ざんが許されない通信はかならず適切な強度の暗号化を行う必要がある。一般的には SSL/TLS が使われることが多いが、RC4 や 1024 ビット未満の RSA 公開鍵暗号は使うべきではない。Triple DES や AES を使った SSL/TLS でもセッションを乗っ取られる可能性はわずかではあるが、存在する。単純な SSL/TLS ではリスクはきわめて小さいが、SSL-VPN ではやや増大する。多種のプロトコルが大量に使われる場合には SSL-VPN は避けることが望ましい。また IP-VPN や専用線には暗号化を行う機能はない。どちらも物理的に完全に保護することは困難であり、これらを用いる場合にはコンテンツを暗号化する必要がある。
5. 内部からの不正または迷惑行為:
運用規程を整備すると同時に教育を十分に行う。さらに 1 の対策を徹底的に行う必要がある。また定期的にチェックを行うことも重要である。
6. 不適切な業務外使用:
5 と同様に運用規程の整備と教育を十分に行う。P2P を完全にモニタすることは難しいが、業務で用いる端末を定期的に検査するなどチェックが必要である。

C－2－4 残余リスク

上記の対策を合理的な範囲で実施したとしても以下に示すリスクは残存する。

1. コンピュータウイルス等の悪意のあるソフトウエアの侵入:
   Zero Day Attack は前述の対策では防止できない。Zero Day Attack とは開発された悪意のあるソフトウエアが、OS のアップデートやワクチンソフトの定義ファイルが対応する前に感染することであり、事前に阻止することは原則として不可能である。一部のワクチンソフトはソフトウエアの振る舞いをチェックしているが、確実に検出できるとは言えない。現在、多くの悪意のあるソフトウエアが東アジアで作られていることを考えると、ネットワーク的に近い我が国で Zero Day Attack による被害の出る可能性はある。
2. 利用者を含む内部の不正な振る舞いによるリスク:
   一定の規模以上の医療機関等では利用者も多く、また常に常勤の職員とは限らない。さらに施設内には多くの外来者が存在し、そのすべてに運用規程の徹底や教育が可能とは限らない。医療機関等では建物内の構成が変更されることが多く、情報コンセントの管理さえ用意ではない。また無線ＬＡＮの使用もあり、ネットワーク自体へのアクセスを管理することは不可能ではないにしても、容易ではない。内部からの不正な振る舞いを事前に完全に防ぐことは相当困難と言わざるを得ない。ただし、このリスクは外部ネットワークへの接続とは一次的には無関係であり、むしろ外部ネットワークに接続していた場合、被害を外部に拡散させる可能があるということになる。

C－2－5 残余リスクへの対策

上記の残余リスクへの事前に防止する対策はきわめて難しく、事故が起こった場合の対策を十分に行うしかない。その医療機関等のBCPに含めておくべきであろう。その場合にもっとも重要なことは事故の早期発見であり、効果的なモニタリングを行う必要がある。

D．考察と提言

D－1 考察

D－1－1 ニーズの確認

診療情報システムをInternetに接続するニーズは確実に存在する。その中には今後の診療の継続や、診療情報システムを真に役立つものにするために避けられないニーズもあり、現時点はともかく、近い将来には何らかの接続は避けられない。本研究では管理されない接続を対象にはしなかったが、現在は携帯電話網を通じたインターネット接続や公衆無線ＬＡＮも普及しており、妥当なニーズに対して適切な管理下に接続を行わない場合、管理されない接続が行われる可能性もある。管理されない接続は極めて危険なことを考えれば、適切に管理された接続は必須と考えて良い。

D－1－2 リスク・対応と残余リスク

Internetに接続した場合、リスクは確かに存在する。その多くは適切に管理することで、対応可能であるが、Zero Day Attackのように事前の予防としては対応不可能な残余リスクも存在する。ただし、残余リスクとしてあげたZero Day Attackと内部からの不正行為は、Internetに接続しない場合にもリスクとして存在するもので、Internetに接続することで改め

て生じるリスクではない。つまり、Internetに接続していなくても何らかの情報システムを用いる以上は対応をしなければならない。

そのようなリスクを除けば適切に管理された接続であれば、対応可能である。問題は適切な管理のためのコストである。運用規定の制定や教育はともかく、適切なファイアウォールの設定や、不正アタック、不正使用の監視はネットワーク管理に関する一定の知識が必要で、また経済的にもコストが生じる。大学病院のような大規模医療機関では対応可能な場合もあるが、小規模医療機関では困難であることが推測される。一般には組織内の人員で対応できない場合は、外部事業者に管理を委託するが、常時監視であり、委託費用もそれなりの価格になるであろう。これを解決にするには、高度のネットワーク知識を持たない場合でも十分な管理ができるような、マニュアルや指針を整備するか、委託先を大規模化したコストを下げることが考えられる。ASP・SaaSによる診療情報システムの場合はサービス提供者と医療機関等の間のネットワーク管理はサービス提供者が行うことが普通であろうし、さらに外部との接続もサービス提供者の管理下に行われれば、医療機関等としてのコストはサービス利用料の含まれることになる。ただASP・SaaSを利用する場合でも、ハイブリッド型のシステムである場合が考えられる。つまり一部の診療情報システム機能は医療機関等内に存在し、一部をASP・SaaSで利用する場合である。この場合、外部接続の管理の責任主体は複雑になる。外部への接続はASP・SaaSのサービス提供者に委託することも考えられるが、その場合、サービス提供者は自らの管理するシステム以外からの通信も管理することになり、一体的なサービス対価にはならない可能性がある。また双方で外部接続を行う可能性もあるが、この場合は責任の所在が複雑になり、事故があった場合の対応等を契約で明確にしなければならない。この場合で単独で医療機関等が外部接続する場合より運用コストが増加する可能性もある。

本研究のとりまとめの議論の中で、望ましいと考えたことは外部接続に関するゲートウエイセンタを設置することである。ゲートウエイセンタはファイアウォール機能を含む適切な外部接続管理を集中して行い、利用する医療機関等はこのセンタにVPN接続する。医療機関等は自らの診療情報システムの異常の監視は行う必要があるが、それはネットワークに接続しない場合でも同様であり、追加の労力なく、必要な外部アクセスが可能になる。またこのゲートウエイセンタがDMZとして機能し、共同利用型のサーバを設置すれば外部への情報発信も行うことができる。

D－2　提言

D－1で述べたようにInternet接続は近い将来には必須であり、適切な対応を行わない場合、管理されない接続によって危機的状況が起こりえない状況と言える。行政からの情報発信もInternetを利用していることを考えれば、行政的・制度的な手当も必要と考えら得る。研究班では2点の提言を行いたい。

1点目はゲートウエイセンタの誘導である。行政が直接ゲートウエイセンタを設置する必要性はないが、一定の信頼が必要であり、関与はすべきものと考えられる。可能性としては現在レセプトオンラインの受け口となっている支払基金や国保連合中央会もこのような機能を持つ

主体としては有望と思われるが、レセプトオンラインより、トラフィックは飛躍的に増大する可能性があり、もう少し分散することが必要と思われる。管轄の公益法人を活用するか、一定の基準と定期的な監視を行う仕組を整備することで、民間事業者の参入を誘導する等の対策をとることが望ましいと考えられる。

２点目は「医療情報システムの安全管理に関するガイドライン」の改訂である。当該ガイドラインは2010年の外部保存用件の緩和通知に際して4.1版が発出され以下のような目次で構成されている。

1　はじめに
2　本指針の読み方
3　本ガイドラインの対象システム及び対象情報
　3.1　7章及び9章の対象となる文書について
　3.2　8章の対象となる文書等について
　3.3　取扱いに注意を要する文書等

4 電子的な医療情報を扱う際の責任のあり方
　4.1　医療機関等の管理者の情報保護責任について
　4.2　委託と第三者提供における責任分界
　　4.2.1　委託における責任分界
　　4.2.2　第三者提供における責任分界
　4.3　例示による責任分界点の考え方の整理
　4.4　技術的対策と運用による対策における責任分界点

5　情報の相互運用性と標準化について
　5.1　基本データセットや標準的な用語集、コードセットの利用
　　5.1.1　基本データセット
　　5.1.2　用語集・コードセット
　5.2　データ交換のための国際的な標準規格への準拠
　5.3　標準規格の適用に関わるその他の事項

6　情報システムの基本的な安全管理
　6.1　方針の制定と公表
　6.2　医療機関における情報セキュリティマネジメントシステムISMS）の実践
　　6.2.1　ISMS構築の手順
　　6.2.2　取扱い情報の把握
　　6.2.3　リスク分析
　6.3　組織的安全管理対策（体制、運用管理規程）
　6.4　物理的安全対策
　6.5　技術的安全対策
　6.6　人的安全対策
　6.7　情報の破棄
　6.8　情報システムの改造と保守
　6.9　情報及び情報機器の持ち出しについて
　6.10　災害等の非常時の対応
　6.11　外部と個人情報を含む医療情報を交換する場合の安全管理
　6.12　法令で定められた記名・押印を電子署名で行うことについて

7　電子保存の要求事項について
　7.1　真正性の確保について
　7.2　見読性の確保について
　7.3　保存性の確保について

8　診療録及び診療諸記録を外部に保存する際の基準
　8.1　電子媒体による外部保存をネットワークを通じて行う場合
　　8.1.1　電子保存の3基準の遵守
　　8.1.2　外部保存を受託する機関の

選定基準及び情報の取り扱いに関する基準

8.1.3　個人情報の保護

8.1.4　責任の明確化

8.1.5　留意事項

8.2　電子媒体による外部保存を可搬媒体を用いて行う場合

8.3　紙媒体のままで外部保存を行う場合

8.4　外部保存全般の留意事項について

8.4.1　運用管理規程

8.4.2　外部保存契約終了時の処理について

8.4.3　保存義務のない診療録等の外部保存について

9　診療録等をスキャナ等により電子化して保存する場合について

9.1　共通の要件

9.2　診療等の都度スキャナ等で電子化して保存する場合

9.3　過去に蓄積された紙媒体等をスキャナ等で電子化保存する場合

9.4（補足）　運用の利便性のためにスキャナ等で電子化を行うが、紙等の媒体もそのまま保存を行う場合

10　運用管理について

付則1　電子媒体による外部保存を可搬媒体を用いて行う場合

付則2　紙媒体のままで外部保存を行う場合

付表1　一般管理における運用管理の実施項目例

付表2　電子保存における運用管理の実施項目例

付表3　外部保存における運用管理の例

付録　（参考）外部機関と診療情報等を連携する場合に取り決めるべき内容

この中でInternetに接続する場合の用件については6.5の技術的安全対策のB項のとして以下のように記載されている。

（4）不正ソフトウエア対策

ウイルス、ワーム等と呼ばれる様々な形態を持つ不正なソフトウエアは、電子メール、ネットワーク、可搬媒体等を通して情報システム内に入る可能性がある。これら不正ソフトウエアの侵入に際して適切な保護対策がとられていなければ、セキュリティ機構の破壊、システムダウン、情報の暴露や改ざん、情報の破壊、資源の不正使用等の重大な問題を引き起こされる。そして、何らかの問題が発生して初めて、不正ソフトウエアの侵入に気づくことになる。

対策としては不正ソフトウエアのスキャン用ソフトウエアの導入が最も効果的であると考えられ、このソフトウエアを情報システム内の端末装置、サーバ、ネットワーク機器等に常駐させることにより、不正ソフトウエアの検出と除去が期待できる。また、このことは医療機関等の外部で利用する情報端末やPC等についても同様であるが、その考え方と対策については、「6.9　情報及び情報端末の持ち出しについて」を参照されたい。

ただし、これらのコンピュータウイルス等も常に変化しており、検出のためにはパターンファイルを常に最新のものに更新することが必須である。

たとえ優れたスキャン用ソフトウエアを導入し、適切に運用したとしても、全ての不正ソフトウエアが検出できるわけではない。このためには、情報システム側の脆弱性を可能な限り小さくしておくことが重要であり、オペレーティング・システム等でセキュリティ・ホールの報告

されているものについては、対応版（セキュリティ・パッチと呼ばれるもの）への逐次更新、さらには利用していないサービスや通信ポートの非活性化、マクロ実行の抑制等も効果が大きい。

(5) ネットワーク上からの不正アクセス
ネットワークからのセキュリティでは、クラッカーやコンピュータウイルスや不正アクセスを目的とするソフトウエアの攻撃から保護するための一つ手段としてファイアウォールの導入がある。
ファイアウォールは「パケットフィルタリング」、「アプリケーションゲートウエイ」、「ステートフルインスペクション」等の各種方式がある。またその設定によっても動作機能が異なるので、単にファイアウォールを入れれば安心ということにはならない。単純なパケットフィルタリングで十分と考えるのではなく、それ以外の手法も組み合わせて、外部からの攻撃に対処することが望ましい。システム管理者はその方式が何をどのように守っているかを認識するべきである。
このことは、医療機関等の外部から医療機関等の情報システムに接続されるPC等の情報端末に対しても同様であるが、その考え方と対策については、「6.9　情報及び情報端末の持ち出しについて」を参照されたい。
不正な攻撃を検知するシステム（IDS：Intrusion Detection System）もあり、医療情報システムと外部ネットワークとの関係に応じて、IDSの採用も検討すべきである。また、システムのネットワーク環境におけるセキュリティホール（脆弱性等）に対する診断（セキュリティ診断）を定期的に実施し、パッチ等の対策を講じておくことも重要である。
無線LANや情報コンセントが部外者により、物理的にネットワークに接続できる可能性がある場合、不正なコンピュータを接続し、ウイルス等を感染させたり、サーバやネットワーク機器に対して攻撃（サービス不能攻撃DoS：Denial of Service等）を行ったり、不正にネットワーク上のデータを傍受したり改ざんする等が可能となる。不正なPCに対する対策を行う場合、一般的にMACアドレスを用いてPCを識別する場合が多いが、MACアドレスは改ざん可能であるため、そのことを念頭に置いた上で対策を行う必要がある。
不正アクセスの防止は、いかにアクセス先の識別を確実に担保するかが重要であり、特に、“なりすまし“の防止は確実に行わなければならない。また、ネットワーク上を流れる情報の窃視を防止するために、暗号化等による”情報漏えい“への対策も必要となる。

またC項で、
9. システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時にはウイルス等の不正なソフトウエアが混入していないか確認すること。適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等の不正なソフトウエアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（たとえばパターンファイルの更新の確認・維持）を行うこと。

と記載され、D項で、
3. 外部のネットワークとの接続点やDBサーバ等の安全管理上の重要部分にはファイアウォール（ステートフルインスペクションやそれと同等の機能を含む）を設置し、ACL(アクセス制御リスト)等を適切

に設定すること。

と記載れているに過ぎない。項目は系統的でなく、理解しにくいという問題はあるが、さらに、2010年の外部保存用件の緩和により、今後普及することが予想されるASP・SaaSの活用に関する指針や、Zero Day Attackや内部からの不正行為のための障害に対する対応には記載が見られない。本来BCP (Business Continuing Plan)として考慮すべきことであるが、現状のBCPは6.10章で主に災害や、システム異常について完結に書かれているのみで、外部接続や、外部接続を行わない場合でも起こりうる障害に十分対応できているとは言い難い。さらに本研究とは無関係であるが、東日本大震災のような大規模災害やそれにともなう電力事情の悪化にも対応できているとは言い難い。改訂が必要である。これらの改訂が適切になされれば、８章は原則として不要と考えられる。

E．結論

昨年度行ったインタビューおよびゲートウエイセンタの構成要素の基礎的な評価に加えて、２大学病院で実際の通信状況を定性的に評価するとともに、ニーズ分析、リスク分析をおこなった上で、対策と残余リスクを整理し、提言をまとめた。提言では人員に余力のない医療機関等が安心して診療情報システムをInternetに接続するためには、ASP・SaaSによる診療情報システムを用いるか、ゲートウエイセンタの利用が強く求められるために、その誘導策をとることと、「医療情報システムの安全管理に関するガイドライン」の改訂が必要であることを示した。

F．研究発表

1.　論文発表

K. Tanaka, H. Atarashi, I. Yamaguchi, H. Watanabe, R. Yamamoto, K. ohe, “Wireless LAN Security Management with Location Detection Capability in Hospitals”, Methods of Information in Medicine, vol. 51, pp 221-228, 2012

2.　学会発表

田中勝弥、山本隆一、大江和彦、”病院情報システム端末からの安全なインターネット接続に関する検討”，第31回医療情報学連合大会（鹿児島），2011年11月21-23日，論文集（医療情報学別冊），pp 713-716

G．知的財産権の出願・登録状況
（予定を含む。）

1. 特許取得

なし

2. 実用新案登録

なし

3. その他

なし

図１　A病院でのサービス別帯域

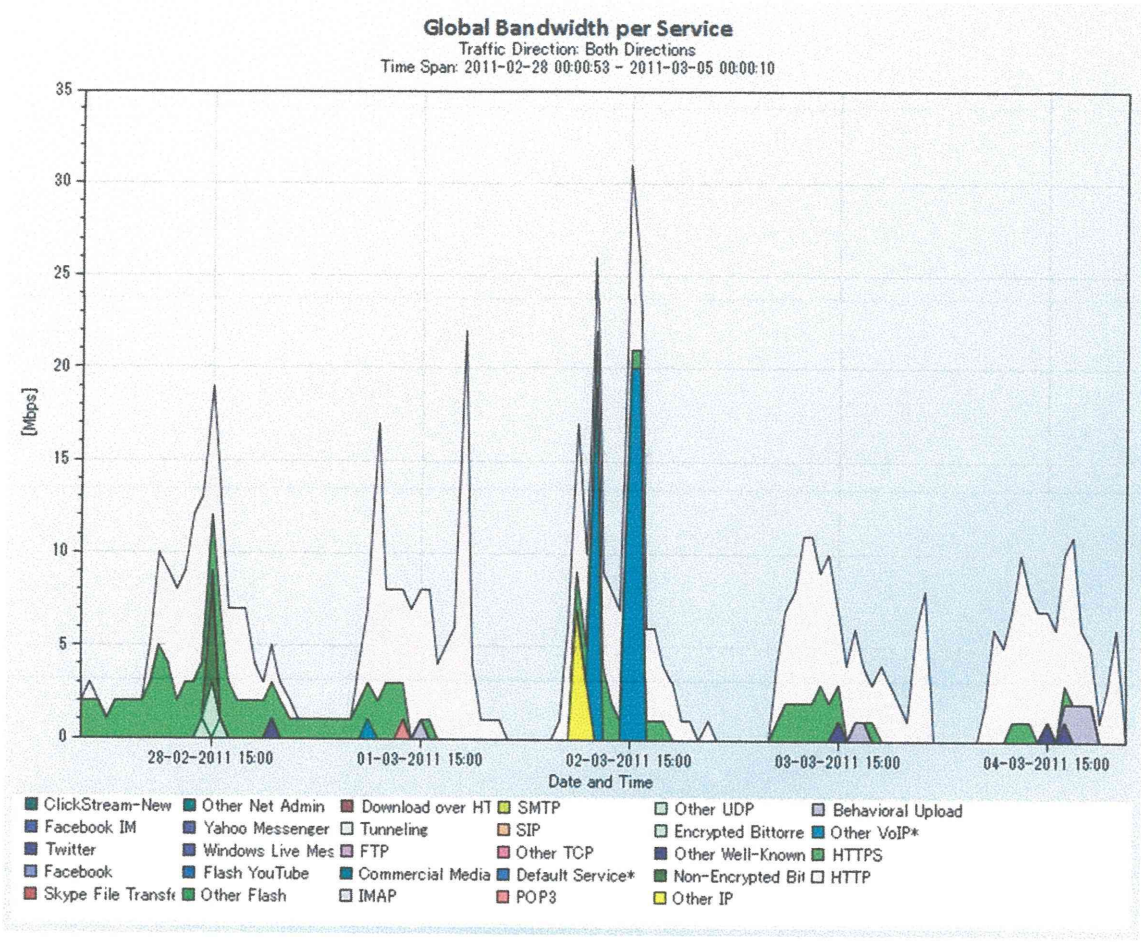


図２　Ｂ病院でのサービス別帯域

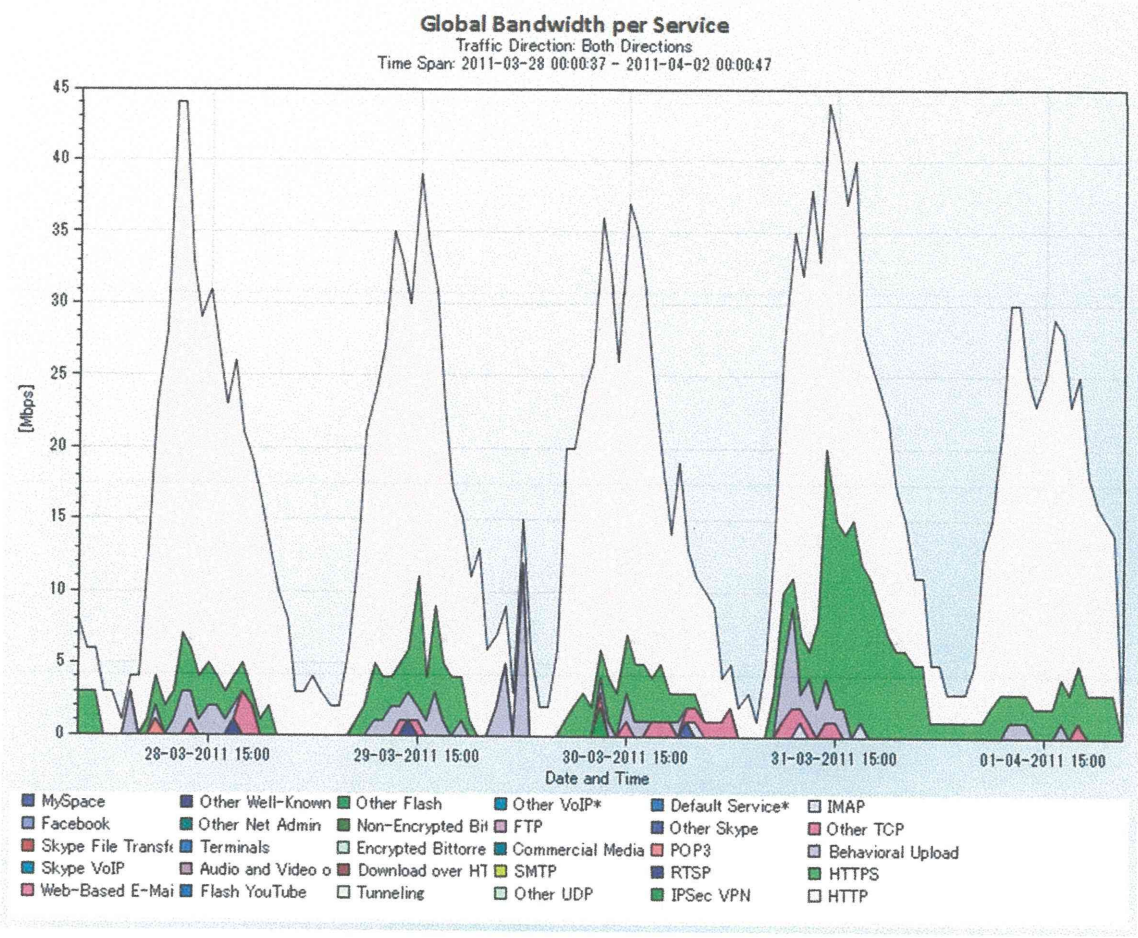
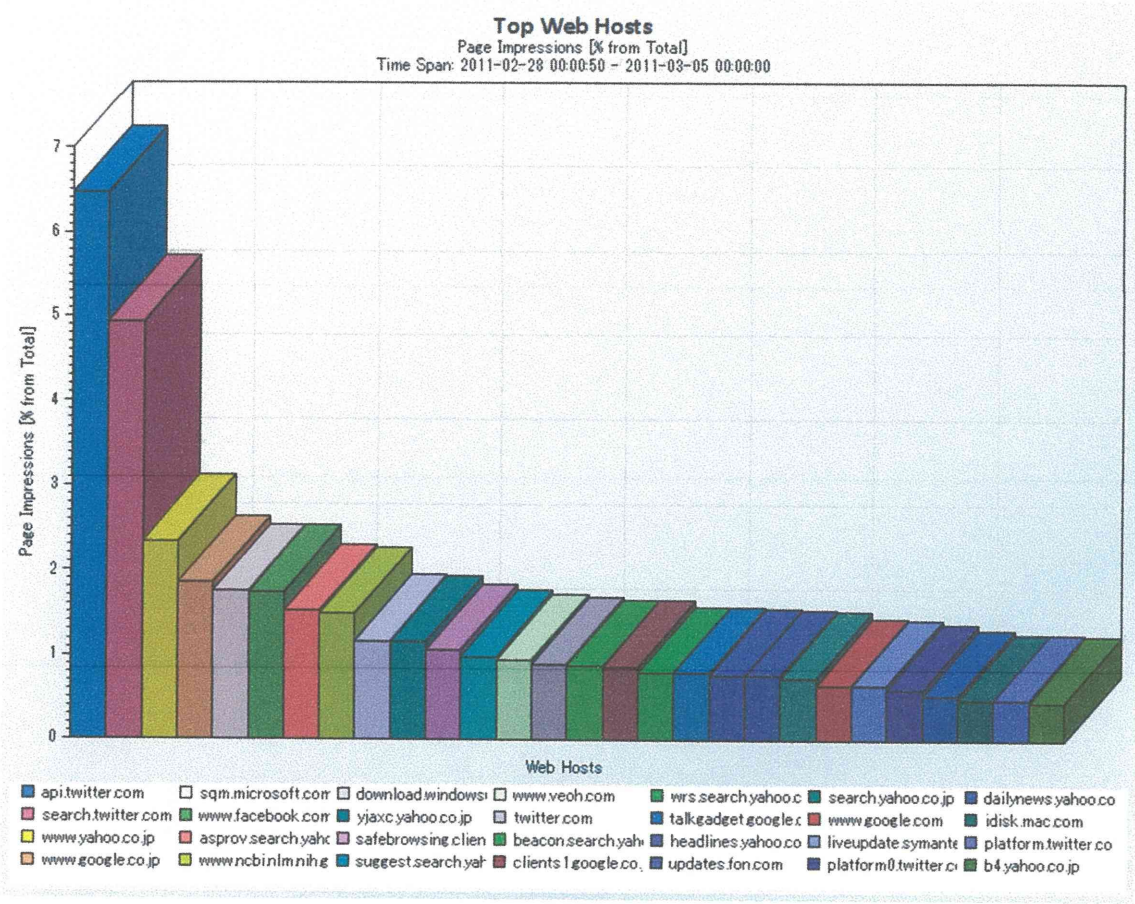


図３　　A病院WEBアクセスの状況



B病院でのWEBアクセスの状況

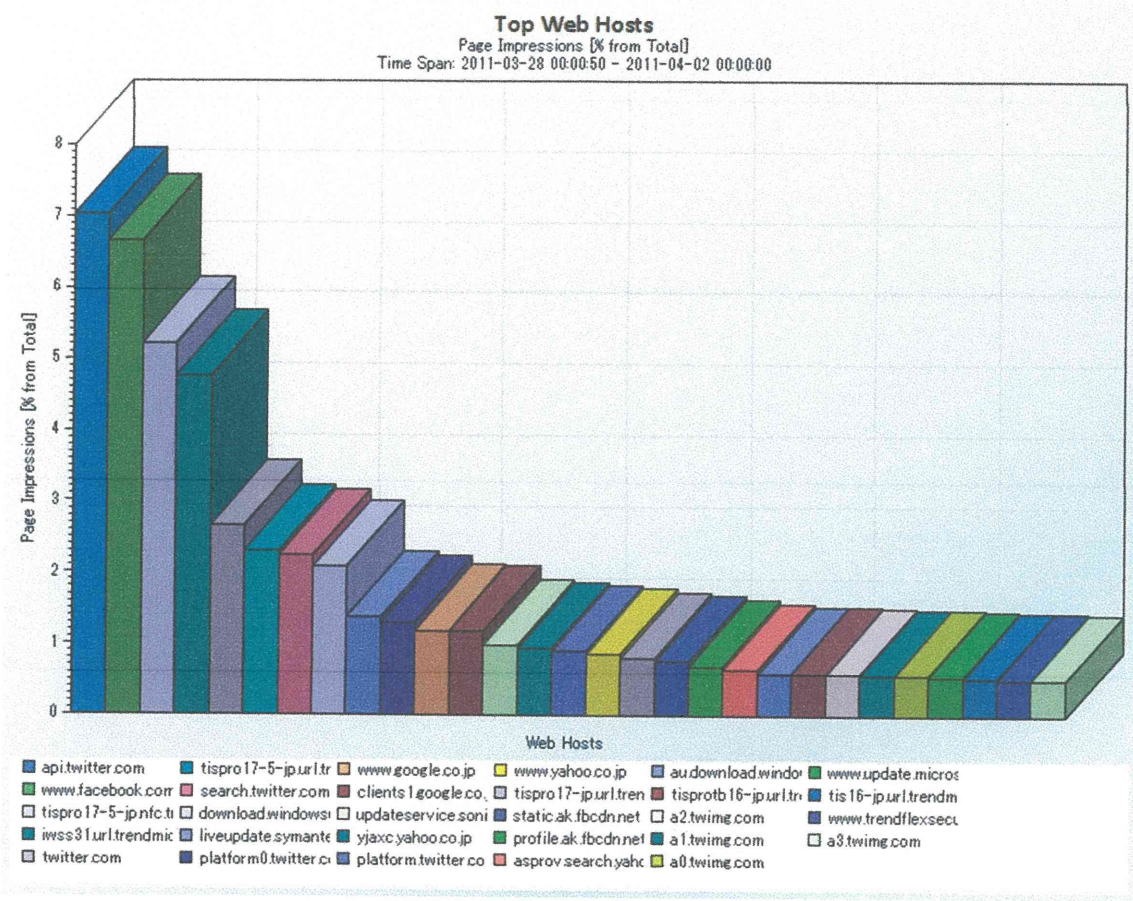
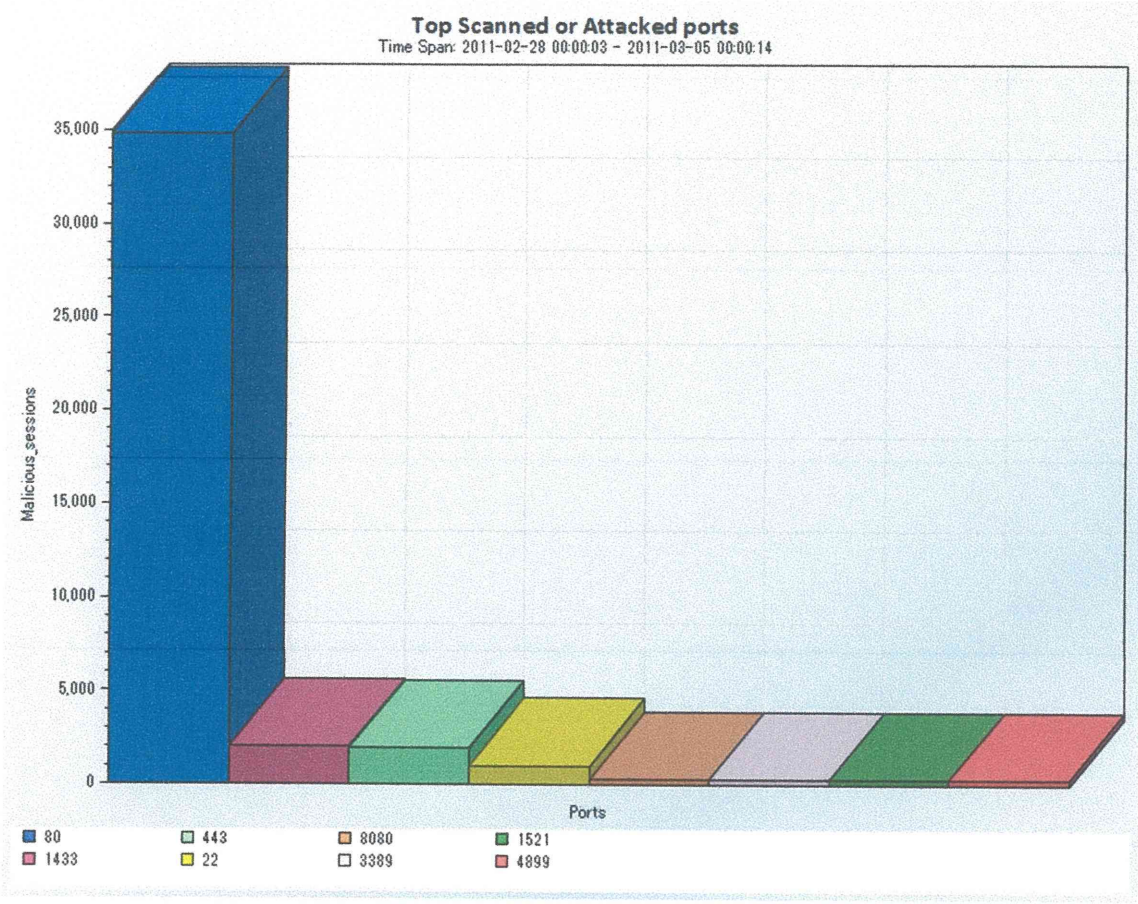


図５　A病院での外部からの攻撃の状況



刊行物

書籍　なし

著者氏名	論文タイトル名	書籍全体の編集者名	書　籍　名	出版社名	出版地	出版年	ページ

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
田中勝弥、山本隆一、大江和彦	病院情報システム端末からの安全なインターネット接続に関する検討	医療情報学別冊第31回医療情報学連合大会論文集	31	713 - 716	2011
K. Tanaka, H. Atarashi, I. Yamaguchi, H. Watanabe, R. Yamamoto, K. ohe	Wireless LAN Security Management with Location Detection Capability in Hospitals	Methods of Information in Medicine	51	221 - 228	2012