FIPS PUB 140-1 Test Result Details

Results of FIPS 140-1 Specified Tests on sample2

data: c4s(2Mbyte)

//1-20000

The monobit test	X=	9973	pass	(pass if 9654 <X <10346)
The poker test	X=	12.884	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2455	2579	pass	(pass if 2267 <X <2733)
2	1279	1158	pass	(pass if 1079 <X <1421)
3	636	621	pass	(pass if 502 <X <748)
4	326	306	pass	(pass if 223 <X <402)
5	166	186	pass	(pass if 90 <X <223)
6+	139	151	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//2000001-2020000

The monobit test	X=	9987	pass	(pass if 9654 <X <10346)
The poker test	X=	20.5952	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2501	2509	pass	(pass if 2267 <X <2733)
2	1239	1216	pass	(pass if 1079 <X <1421)
3	615	640	pass	(pass if 502 <X <748)
4	336	337	pass	(pass if 223 <X <402)
5	160	165	pass	(pass if 90 <X <223)
6+	151	135	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//4000001-4020000

The monobit test	X=	10048	pass	(pass if 9654 <X <10346)
The poker test	X=	17.0176	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2511	2462	pass	(pass if 2267 <X <2733)
2	1219	1242	pass	(pass if 1079 <X <1421)
3	612	624	pass	(pass if 502 <X <748)
4	316	335	pass	(pass if 223 <X <402)
5	172	143	pass	(pass if 90 <X <223)
6+	150	173	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//6000001-6020000

The monobit test	X=	10025	pass	(pass if 9654 <X <10346)
The poker test	X=	18.8864	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2497	2426	pass	(pass if 2267 <X <2733)
2	1278	1294	pass	(pass if 1079 <X <1421)
3	584	641	pass	(pass if 502 <X <748)
4	315	340	pass	(pass if 223 <X <402)
5	160	161	pass	(pass if 90 <X <223)
6+	161	132	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//8000001-8020000

The monobit test	X=	10045	pass	(pass if 9654 <X <10346)
The poker test	X=	19.8912	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2489	2499	pass	(pass if 2267 <X <2733)
2	1252	1221	pass	(pass if 1079 <X <1421)
3	601	604	pass	(pass if 502 <X <748)
4	313	303	pass	(pass if 223 <X <402)
5	161	157	pass	(pass if 90 <X <223)
6+	157	189	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

Ⅱ. 分 担 研 究 報 告 書

医療情報のセキュリティに関する研究

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　個人情報保護関連 5 法案が成立し、わが国も法律の裏づけを持って個人情報保護を考える時期に入った。本研究は扱う情報が高度なプライバシー情報であり、利用目的が複雑で公益利用も重要な HIV ネットでの個人情報保護の取り扱いを研究することが目的で、現状調査、諸外国（特に米国の HIPAA Privacy standards）の調査などを通して最適な指針のあり方を求めた。

A．研究目的

高度情報通信社会の急速な進展、個人情報保護への関心の高まり、データ保護に関するＥＵ指令や HIPAA 法に関連した米国規則など、諸外国のプライバシー保護、セキュリティの規制の変化等から、我が国においても保健医療分野での個人情報保護のあり方に関して、国際動向や現在のセキュリティ技術水準を踏まえた一定の方向性を示すことが緊急かつ重大な課題となっている。また国会においては、平成 15 年 5 月に個人情報保護関連 5 法案が成立し、平成 17 年 4 月の実施が決定されており、ガイドラインの作成が一層重要性をおびている。

本研究は、HIV ネットにおける個人情報の取扱い上の課題を整理し、ガイドラインを研究することにより、個人情報保護対策の推進に資するものである。

B．研究方法

（1）個人情報保護関連法に関する現状及び問題点に関する調査

個人情報保護関連 5 法について、論点を整理し、医療分野、特に臨床現場及び診療報酬請求過程における個人情報の取扱いに関し、運用及び技術面での対応や課題の解決策について検討した。

（2）個人情報保護対策例として米国 HIPAA Privacy Standards とわが国の JIS Q 15001 「プライバシー保護のためのコンプライアンスプログラム作成指針」を取り上げ、比較検討を行った。

（3）個人情報保護のための基本的な技術的課題の調査

利用者識別、権限管理、ネットワークセキュリティといった技術要素は運用のいかんに関わらず情報システムでの個人情報保護を考える上で必須の要素であり、保健医療福祉分野での課題や要件を整理する必要がある。本研究では経済産業省の事業として東大病院で実施される予定の保健医療福祉分野における PKI の実証実験を利用し、それの技術的要件を整理する。

C．研究結果

（1）個人情報保護関連法に関する現状及び問題点に関する調査

現時点での医療における個人情報保護のあり方について「医療の個人情報保護とセキュリティ（有斐閣 2003)」を上梓した以下に目次を示す。

第 1 章　医療における個人情報保護の歴史と背景

第 2 章　保護されるべき医療個人情報

第 3 章　アメリカにおける医療情報保護：HIPAA 法と日本への示唆

第 4 章　個人情報保護法が医療に与える影響

第 5 章　電子情報のセキュリティ対策

第 6 章　医療機関は具体的にどうすればよいか？

第 7 章　今後の課題

資料　個人情報保護に関する法律

個人情報保護に関する法律案に対する附帯決議

アメリカの医療のプライバシールール（HIPAA 法のプライバシールール）

（2）個人情報保護のための既存基準や指針の調査

個人情報保護のための基準や指針がわが国をはじめ諸外国、および国際団体に存在する。その代表的なものとして、JIS Q 15001 とそれに基づくプライバシーマーク認定制度および米国の HIPAA Privacy Standards に関して調査を行った。

イ．JIS Q 15001 とプライバシーマーク

日本において OECD の個人情報保護に関するガイドラインと同時に作成された勧告、つまりガイドラインに従った制度整備を行うために導入された基準および認定制度で、財団法人日本情報処理開発協会（JIPDEC）が管理と運用を行っている。JIS Q 15001 自体は汎用的な基準であるが、同協会が医療関連機関向けのガイドラインを作成し、それにしたがった認定も開始している。

基準の内容は一般論としては充実してお

り、個人情報保護関連法の要求を満たすものと考えることができる。一方で基準自体には例えばプライバシーに機微な情報として思想や信条とともに医療に関する情報があげられ、原則収集禁止とするなど、保健医療福祉分野にはそのまま適用することが難しい項目が含まれている。主任研究者の山本および分担研究者の清谷が参加してJIPDEC が作成した医療関連機関向けの指針にはこのような問題点が一応は解決されている。ただし次項で述べる米国の HIPAA Privacy Standards に比べると、具体性と詳細性の程度はやや低いと考えられる。

この指針はA．JIS Q 15001 の要求事項、B．医療機関としての解釈、C．最低限のガイドライン、D．推奨されるガイドラインの４つの項目に構造化されており、これは主任研究者の山本も参加して作成した後述する米国大学関連病院の HIPAA Privacy Standards 適合のための指針と同じ構造をとっている。

たとえばJIS Q 15001 4.4.2.3の情報収集禁止の項では以下のようになっている。

A．JIS Q 15001 の要求事項

次に示す内容を含む個人情報の収集、利用又は提供は行ってはならない。ただし、これらの収集、利用又は提供について、明示的な情報主体の同意、法令に特別の規定がある場合、及び司法手続き上必要不可欠である場合は、この限りでない。

a）思想、信条、及び宗教に関する事項。

b）人種、民族、門地、本籍地、身体・精神障害、犯罪歴、その他社会的差別の原因となる事項。

c）勤労者の団結権、団体交渉及びその他団体行動の行為に関する事項。

d）集団示威行為への参加、請願権の行使、及びその他の政治的権利の行使に関する事項。

e）保健医療及び性生活。

B．医療機関としての解釈

４．４．２．３の項目は一般的な情報収集と保健医療福祉分野での情報収集でもっとも大きな違いが見られる事項である。人種、民族、身体・精神障害および保健医療に関する情報収集は診療の遂行に関して必須であり、保健医療福祉分野では特別に扱う必要はないと考えられる。また思想、信条、犯罪歴でさえも精神疾患などでは収集目的の達成のために必要な場合がある。したがってこれらの禁止項目は保健医療福祉分野の場合、取得目的の範囲を超えた場合のみに適用されると考えるべきである。ただしこれらは特にプライバシーに敏感な項

目であるために挙げられたことに十分留意するべきで、これらの項目を収集する場合は特に利用範囲が診療の遂行のための限度内であることを確認する必要がある。

プライバシーに敏感で医療の遂行上必要な情報は少なからず存在する。これらの情報収集には慎重でなければならないが、複雑な手続きを規定すると診療の遂行が困難になることもあり得る。このような情報は診療の専門性によってもことなるために一概に判断することは困難である。その医療機関の実態をよく把握し、日常的な情報収集で少しでも曖昧さがある場合はあらかじめ倫理委員会で方針を決めるなどの、説明可能な対策が求められる。

特殊な例として、宗教法人が運営する医療機関などで信者か否かを受診時に確認する場合がある。これも宗教に関する情報収集にあたる。医療面からの必要性は乏しく、安易に収集すればプライバシーの侵害にあたる。このような場合は、初診申し込み前に宗教に関する質問があることを通知し、回答を拒否できるようにするべきである。またホスピス等で本人の宗教によってケアが異なる場合ために情報を収集する場合がある。診療上の必要性はあると考えられるが、止むを得ないかどうかは判断が困難である。このような場合にも、事前に通知し、回答を拒否できるようにしておくべきある。

C. 最低限のガイドライン

以下のａ～ｅの項目については、原則として情報を収集してはいけない。ただし診療の遂行上情報の収集を避けられない場合はその理由が自明でない限り、その理由を診療録等に明記した上で収集することができる。その場合も利用は診療上必要な範囲内にあることに特に注意しなければならない。診療上の理由が自明とは性生活そのものが健康上の問題である場合の性生活に関する情報や、思想、宗教、犯罪歴などが妄想などの精神症状に強く関連している場合であって、安易に自明と判断してはいけない。

ａ） 勤労者の団結権、団体交渉及びその他団体行動の行為に関する事項。

ｂ） 集団示威行為への参加、請願権の行使、及びその他の政治的権利の行使に関する事項。

ｃ） 思想、信条、及び宗教に関する事項。

ｄ） 門地、本籍地、犯罪歴、その他社会的差別の原因となる事項。

ｅ） 性生活。

D. 推奨されるガイドライン

C. に加えてこれらの項目の情報収集を行う場合、診療上の必要性が自明でない場合、

可能な限り事前に倫理委員会の了承を得る。事前に倫理委員会に諮ることが出来なかった場合は事後に倫理委員会に報告し、その際、不適と判断された場合は当該情報を抹消する。

例えば不妊外来での性生活に関する情報収集のように診療上の必要性があって、かつ日常的に収集されることが予想される場合は、あらかじめ一括して倫理委員会等で検討を行い、必要性を明確にし、個人情報保護上の配慮を具体的に定めておく。このような過程を経た情報収集はその必要性と配慮がある前提で、個々に特別な手続きを経ずに収集することができる。

ロ. 米国 HIPAA 法 Privacy Standards

米国 HIPAA 法の Privacy Standards（以後 Privacy Standards）は 2001 年に一度制定され実施が決まったが、米国連邦政府の政権交代にともなって見直されたもので、最終版は 2002 年 12 月に改定され、大規模医療機関では 2003 年 4 月から実施されている。2001 年版は診療に関わるすべての情報の取得段階で診療をはじめとするすべての利用目的を本人に提示し、文書による同意を義務付けていたが、2002 年版は診療自体、診療報酬請求、および医療機関の組織の維持運営管理の 3 つの利用目的に限って同意は必須ではなくなったことが主な変更点である。Privacy Standards 自体は前文を合わせると3段組で400ページ程度あり、条文だけでも 30 ページを越える。以下に主な項目の邦訳をあげる。

1．プライバシールールの規制機関・対象機関・提携事業者

1-1 規制機関

1-2 対象事業者

1-3 提携事業者

2．プライバシールールで保護される情報・保護されない情報

2-1 個人識別医療情報と保護対象医療情報

2-2 個人匿名化情報

3．医療情報の利用および提供

3-1 基本原則

3-2 診療、支払、または医療機関業務での利用・提供

3-3 同意または異議申し立ての機会を伴う（簡易な許可でよい）利用および提供

3-4 公益目的での医療および提供

3-5 限定されたデータセット

Privacy Standards の特徴は極めて詳細かつ具体的であることで、医療分野に特化して作成されているために、現場が遭遇す

る場面を網羅することを目指している。ただし、詳細かつ具体的である反面、微妙な例外事態が起こることが予想され、かえって現場が判断に迷う可能性もある。米国では大学関連病院がさらに詳細に起こりうる事象を検討し、対策をまとめた指針を作成しているが、このような可能性に配慮したものであろう。ただし、この指針は 1000 ページを越える大部である。

（4）個人情報保護のための基本的な技術的課題の調査

利用者識別、権限管理、ネットワークセキュリティといった技術要素は運用のいかんに関わらず情報システムでの個人情報保護を考える上で必須の要素であり、保健医療福祉分野での課題や要件を整理する必要がある。本研究では経済産業省の事業として東大病院で実施される予定の保健医療福祉分野における PKI の実証実験を利用し、それの技術的要件の整理を試みた。現時点では解析が十分ではなく、16 年度研究の中でさらに整理を進める予定であるが、概要を示す。

イ．実証実験システムの背景

医療の分極化が進むにつれて、大学病院のような高度医療機関では入院期間を圧縮し短期間で密度の高い医療を提供することが求められている。このため加療スケジュール密度は高く、担当医師や看護師は 24 時間体制で患者の状況を把握する必要がある。看護師は一応のシフト制があるが、医師は当直医が存在するものの、十分なシフト制とは言えない。現状では診療情報は病院内だけからアクセス可能で、担当医が昼夜の別なく病棟で状況把握に努め、院外から院内のスタッフに電話で状況を聞かなければならない状況にある。このような状況は院内にいるスタッフの仕事量を増加させ、また院外からの状況把握を抑制することにもなり、望ましいとは言えない状態である。院外から診療情報システムのアクセスを許す場合、経路の安全性はＶＰＮやＳＳＬなどのセキュリティ技術で確保可能であるが、厳密な利用者認証と権限管理が必要で、また病院の管理が十分に及ばないＰＣを用いてアクセスするために、そのＰＣに不正ソフトウエアが仕組まれて情報がリレーされる危険があり、これまで実現されていなかった。

ロ．実証実験システムの概要

本システムは東京大学医学部附属病院の医師が自宅や出張先などの院外から、自己が閲覧権を有する診療情報を安全に閲覧することを目的としている。また同様の問題

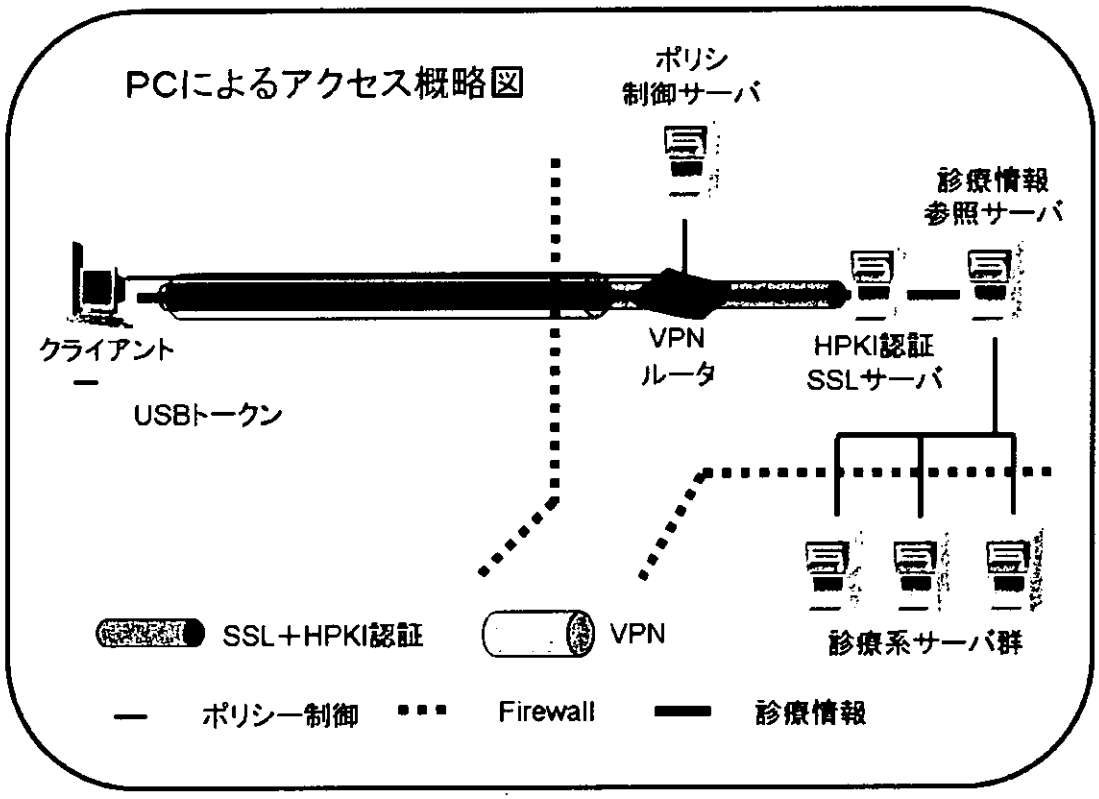
があるために広く実用化されていない患者が自己の診療情報を自宅等からアクセスするシステムに拡張することも視野に入れている。技術的にはすでに開発され効果が実証されているＶＰＮやＳＳＬと言った一般的なネットワークセキュリティ技術に加えて利用者の本人確認と権限管理のためにISO TS17090 に基づいた公開鍵基盤技術を用い、さらにアクセスするＰＣを介した不正な情報リレーや機器なりすましによる病院情報システムへの不正アクセスを確実に防止するためにアクセス中のＰＣのポリシーを厳密に管理している。具体的には接続時にＯＳの版をチェックし、本システムで使用する以外のアプリケーションやＤＬＬの起動を抑制している。さらに病院内に実施体制を確立した上で運用上のポリシーおよび利用規則と実施マニュアルを作成し、運用体制を整えることができた。

ハ．システムの詳細

本システムのポイントは３つある。一点目はSSL と VPN という広く用いられている安全技術でインターネット上の通信を秘匿化したこと。二点目はISO TS 17090 で規定された保健医療福祉分野でのPKI を用いた職種認証機能を実装し、職種によるアクセス制限を既存の利用者ごとのアクセス制限機能に付加したこと。3 点目はVPN 接続と連携してクライアントとなる利用者管理の PC のセキュリティポリシーを本システムに接続する間だけに限定して厳しく制限したことである。

SSL は富士通株式会社のセキュリティディレクターを用い、サーバ認証は通常のX.509 V3 の証明書形式に SSL サーバ認証用の keyUsage, Extended keyUsage フィールドをセットしたものを用い、SSL クライアント認証として利用者識別と職種識別のためにISO TS 17090 準拠の公開鍵証明書と対応する私有鍵を新たに作成した SD メモリカードアダプタを装備した USB トークンを使用し、SD メモリカード内に格納して使用した。この USB トークンはそれ自体で暗号化機能を持ち、同一の USB トークンでなければ SD メモリカード内の証明書や私有鍵にアクセスできない構造をとっている。また私有鍵は PKCS #12 の形式で格納されており、利用者だけが知っているパスフレーズを入力しないと使用することはできない。

さらに利用者はクライアントに装備した専用アプリケーションによるソフトウエアVPN 接続を行わないと利用できない機構とし、さらにこの VPN アプリケーションと



連動して動作する、米国 ZoneLabs 社のサーバクライアント型のファイアウォールソフトウエアを用い、VPN 接続している間はクライアントＰＣの動作をきびしく制限し、たとえウイルスやワームが感染していてもその動作を止め、サーバへの影響やクライアントＰＣでの情報流出を防止している。図１はその概略を示している。

ニ．実証実験の評価

医師を中心に役 30 名の利用者で実証実験をおこない、利用者にはアンケート調査、管理者にはヒアリング調査をおこなった。本研究課題と関係の深い点だけ述べれば、個人情報保護の観点から情報の安全管理という点では十分な成果が得られた。しかし利用者の管理するＰＣへのソフトウエアのセットアップがやや煩雑であり、また予想はされていたものの、利用者管理ＰＣはＯＳの版や細かなソフトウエア構成まで含めると著しく多彩であり、管理者側の利用者への支援も相当な負荷であり、ソフトウエアのブラッシュアップが必要と考えられた。

ホ．実証実験の考察

おおむね良好な実証実験結果と考えられ、本実証実験の仕組みが個人情報保護の情報の安全管理の要件として適切と考えられるが、管理の手間はかなり大きく、広く利用されるためには、ポリシーも含めた運用の

再考とソフトウエアの改善が必要であると思われた。

またポリシーとも関連するが、保健医療福祉分野の公的資格確認が必ずしも容易ではない、現状では、ISO TS 17090 準拠の資格証明書発行機能の内、少なくとも利用者登録機能は証明書所有を希望する有資格者の近傍にあることが求められる。そのため、多くのＲＡまたはＣＡの構築が必要になる。コンパクトでシステム自体の安全管理が容易な証明書発行局または登録局が望まれる。さらに当然のことながら情報の安全管理が達成されただけでは個人情報保護は達成できない。個人情報の利用のあり方について情報主権者である患者に説明の上で同意を得ることが望まれる。このような説明と同意のあり方についても含めたポリシーの策定が必須である。

D．考察

平成15年5月に個人情報保護関連5法案が成立し、17 年 4 月の実施が決定された。保健医療福祉分野では何らかの具体的指針を至急に検討する必要がある。2003 年 4 月から米国では HIPAA Privacy Standards が発効し、実際の運用が始まっている。本年度の研究でこの状況を調査したが、現時点では大規模医療機関に限定されているとは言え、先進的な少数の医療機関を除いて対応にかなり苦慮している状況があきらかになった。経費も数億という推定もあり、が国でも十分な配慮のもとに個人情報保護対策の指針等を作成しなければ、混乱を来たす可能性は否定できない。

実際に指針を作成するにあたってはある程度は具体的なものでなければ現場が対応に苦慮することは明白であるが、どの程度詳細で具体的にするかは慎重に検討する必要がある。

また当初より高度な確実性を求めるか、漸進的な手法をとるかも重要な判断となる。米国の Privacy Standards は具体的な条件や対策を詳細に記述しているが、罰則を背景とする規則である以上は確実性を求めている。つまり Privacy Standards が実施された時点で、そこに記載されている要件は確実に満たさなければならない。したがって米国政府は Privacy Standards を Minimal standards と捕らえている。これに対して JIS Q 15001 は詳細な実施計画（コンプライアンスプログラム）の作成とその実施が主体であり、コンプライアンスプログラムには「計画→実施→監査→計画の見直し→実施・・」といった見直しを含

む繰り返し（PDCA サイクル）を基本にしている。つまり、継続的に改善することを保障する体制に主体が置かれている。このような手法は ISO 9000 シリーズにおける品質管理や、BS 7799 における情報セキュリティマネージメントと基本的に同様な手法で、確実性は保障されない反面、新たな事態に容易に対応できる利点がある。わが国の保健医療福祉分野では理論的な個人情報保護の状況は前述の先行研究を見ても十分とは言えないが、実際に患者との間で深刻な問題になっている事例は極めて少なく、また一方で多くの保健医療福祉機関は経済的にも人的にもそれほど多くの余力はない。このような状況でのさらなるプライバシー保護の達成のための戦略は保障レベルの設定と対策体制のバランスに十分考慮したものにする必要がある。

基本的な技術要素もスムーズな対応を期待するためには技術的な中立性にこだわっていては現場の混乱を来たす可能性があり、ある程度の具体的な提言が必要であろう。この点も含めて 16 年度もさらに検討を行いたい。

E．結論

個人情報保護とセキュリティに関する書籍を刊行し、多くの保健医療福祉関連機関で利用されている。また今後個人情報保護法の実施にあわせ保健医療福祉分野の指針が必要となるが、そのあり方を検討するために米国 HIPAA 法 Privacy Standards の実施状況と医療機関の対応状況を調査し、現状を把握することができた。また指針を考える材料として、この Privacy Standards とわが国の JIS Q 15001 およびプライバシーマーク制度を比較検討しその差を明らかにした。また東大病院における経済産業省補助金による外部からの診療情報にアクセスするシステムを調査し、個人情報保護のための技術的要件の整理を試み一定の成果を挙げた。

F．健康危険情報

特になし。

G．発表

書籍

1．　開原成允、樋口範夫編、「医療の個人情報保護とセキュリティ」、有斐閣、東京、2003、224 ページ

雑誌

1．　山本隆一、医療情報のセキュリティとプライバシー保護、映像情報 Medical、

Vol.35、No.14、2003

２．　山本隆一、個人情報保護の観点からの診療情報開示と記録整備のあり方、看護展望、Vol.29、No.2、2004s

H．知的財産権の登録・出願状況

現在のところなし。

汎用医療 VPN ネットワークを活用した HIV 診療支援ネットワークの運用について

厚生労働科学研究費補助金（HIV診療支援ネットワークを活用した診療連携に関する研究）

分担研究報告書

汎用医療VPNネットワークを活用したHIV診療支援ネットワークの運用について

分担研究者　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助教授

研究要旨　HIV診療支援ネットワーク(A-net)は、現在独自のVPNネットワークを構築して運用を行っているが、より効率的な運用を行うためには、汎用の医療VPNネットワークを活用し、これにA-Net独自のセキュリティ保護手段(128ビットSSL等)を併用する方法が有効である。本研究では、汎用の医療VPNネットワーク基盤構築のための技術仕様と、これを活用してA-Netを構築するための方法の検討を行い、汎用医療VPNを活用したA-netの運用方法とメリットを示した。

A. 研究目的

HIV診療支援ネットワーク（A-Net）は、現在独自のVPNネットワークを構築して運用を行っている。安全性への配慮は充分なされているが、より安価なシステム構築・運用を行うためには、すべての医療機関をVPNで相互接続することができる汎用の暗号化医療ネットワーク（医療VPN）を実現し、これにA-Net独自のセキュリティ保護手段(128ビットSSLの利用等)を併用する方法が考えられる。本研究の目的は、医療VPN構築のための技術仕様の検討と、これを活用したA-Netの新たな運用形態を検討することにある。

B. 研究方法

医療VPN実現のために必要なアドレスの割当、ルーティングの方法、VPN機器接続形態、DNS運用形態等についての技術仕様の検討を行った。更にこれを活用してA-Netを運用するための運用形態の検討を行った。

C. 結果

インターネットのプライベートアドレスの一定の領域（一般的に利用されていない確率の高い10.255.0.0/16）を、医療VPN内で使用する予約アドレスとした。各医療機関からは、グローバルアドレスと上記予約アドレスを利用したルーティングにより、インターネット側にも、医療VPN側にもアクセスすることができる。医療VPN内においては、各医療機関は、インターネット接続時と同様に必ずファイアウォールを介して相互接続する仕様とした。DNSについては、各施設内のDNSサーバに医療VPN専用DNSからのゾーン転送を受け付けるように設定することにより、インターネットと医療VPNの両方のサーバの名前解決を可能とする方式を採用した。

D. 考察

医療機関だけの閉鎖的な医療VPN内でも、相互接続に必ずファイアウォールを介すようにしたのは、最終的なセキュリティ管理の責任を各医療機関が持つ必要があると考えたからである。医療VPNは、医療機関間の通信のセキュリティを格段に高めるが、A-netは、通常の診療支援ネットワーク、臨床・疫学研究よりも、一層高度のセキュリティを要求されるため、医療VPNだけではとても充分とはいえない。このため、SSL等の別のセキュリティ保護手段の併用が必須である。VPNは、汎用に様々なプロトコールが利用できるように設計されているため、A-Net独自のセキュリティ対策を追加することは非常に容易である。

A-Netは、現在、独自のVPNネットワークを利用して構築、運営されているが、もし医療VPNが普及して、一般化した場合には、医療VPN上で、新たなセキュリティ対策を追加して、A-Netを運用した方がはるかにコスト的に有利と思われる。ただし、医療VPNの普及・一般化には、まだ相当の時間がかかると思われる。このため、当面A-Netでの全面採用は困難であるが、一部施設での試験運用は可能であり、今後医療VPN活用の可能性について検討を進めるべきであると考える。

HIV診療支援ネットワークのための医療VPNネットワーク情報基盤

－第２回目－

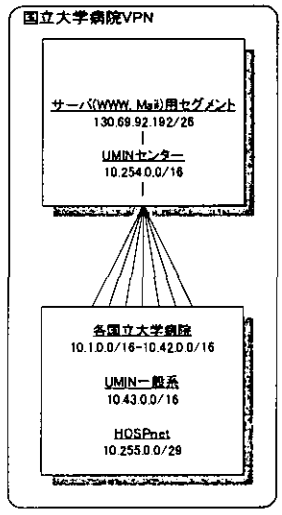
1

１．現況のUMIN VPN

(1)各国立大学病院
10.1.0.0/16-10.43.0.0/16を使用

(2)UMINセンター
10.254.0.0/16を使用

(3)DNSの運用はインターネットを利用
UMINセンターVPNの後背に、サーバ(WWW, Mail)用セグメントをグローバルIPアドレスの空間として用意(130.69.92.192/26)
⇒ これにより、UMINセンターが提供するサービスを受けるためにサーバに接続する際には、通常のインターネット上のDNSで名前解決が可能となる



2

2．新たな医療VPNのネットワーク構成

2.1 基本的な考え方

(1)既存UMIN VPN

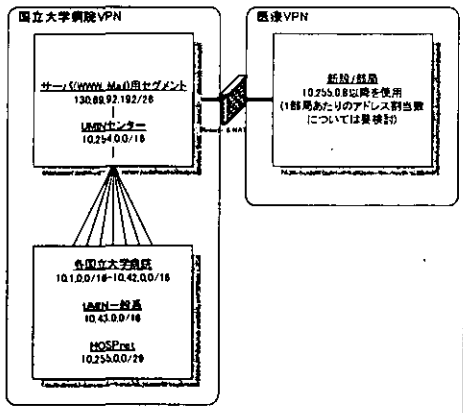
従来とまったく同様に使えるようにする

(2)医療VPN新規参加施設等

新たに予約したアドレス空間を用いる
(10.255.0.0/16)

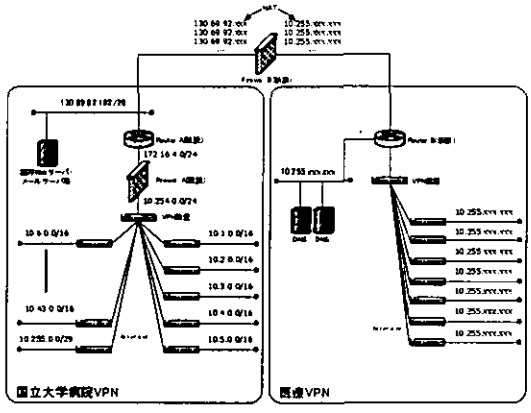
(3)既存UMIN VPNと医療VPNの接続

セキュリティ確保と既存UMIN VPNの運用方式維持のために、Firewall設置し、NATにより相互通信可能とする。



3

2.2 ネットワーク構成



注意：医療VPNの基本的な内部構成は、国立大学病院VPNと同等である。それをFirewall B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。

4

2.3 ＤＮＳの運用　ー医療VPN専用DNSサーバ

(1)医療VPN専用DNSサーバを医療VPN内に設置

(2)医療VPN専用DNSサーバで、「hvpn.net」等の医療VPN専用ドメインを管理

yamaguchi-u.hvpn.net等

(3)医療VPN専用DNSサーバは、医療VPN内からの直接の名前解決要求に返答

(4)医療VPN専用DNSサーバは、各施設内のDNSサーバに医療VPN用DNS情報のゾーン転送を実施

5

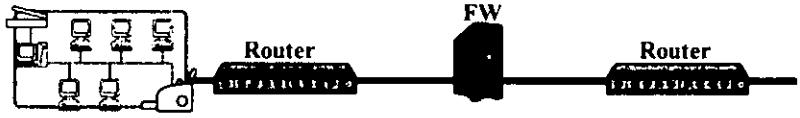
参考資料

安全なFWとVPN機器の接続形態

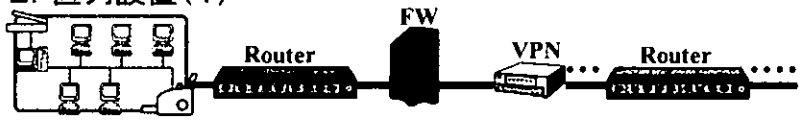
6

FWとVPN機器の接続方法(1)

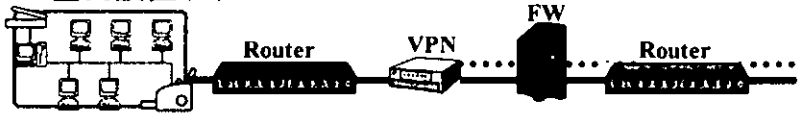
1. VPN機器未設置 ×



2. 直列設置(1) ×



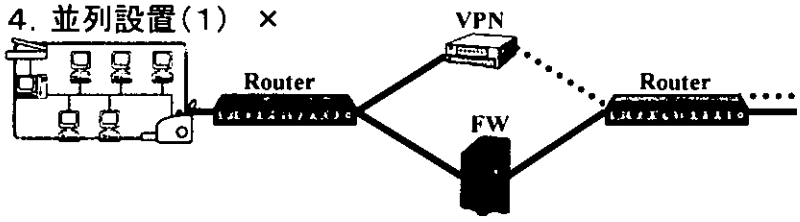
3. 直列設置(2) ×



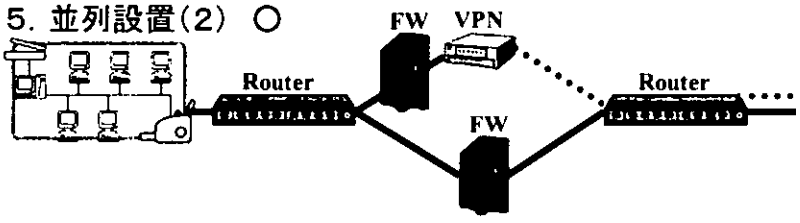
7

FWとVPN機器の接続方法(2)

4. 並列設置(1) ×



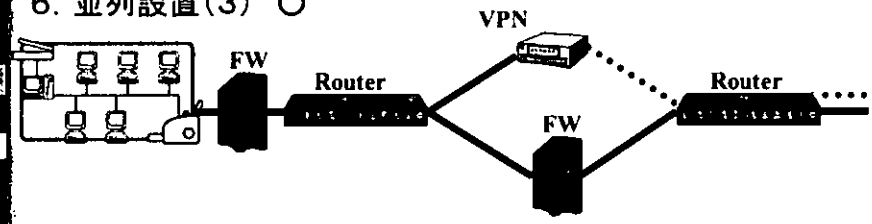
5. 並列設置(2) ○



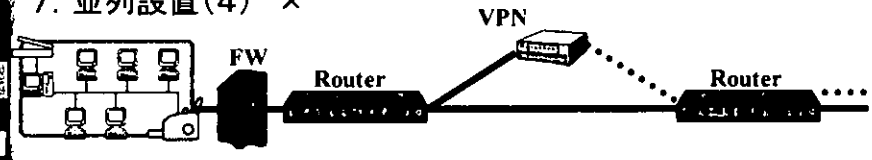
8

FWとVPN機器の接続方法(3)

6. 並列設置(3) ○



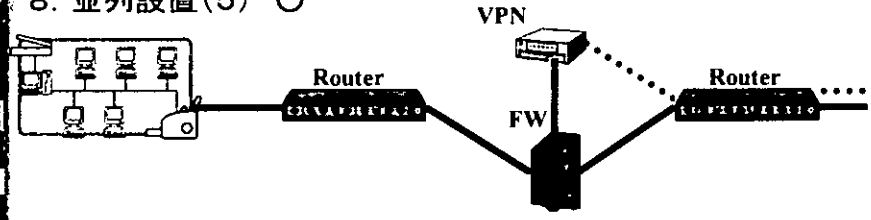
7. 並列設置(4) ×



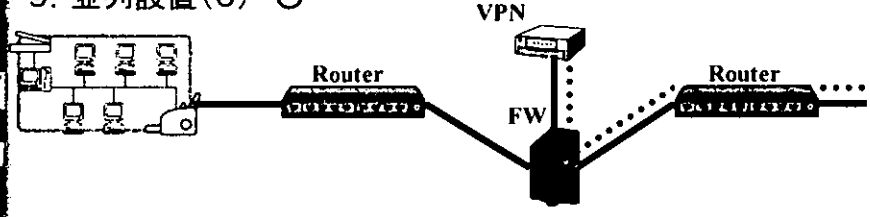
9

FWとVPN機器の接続方法(4)

8. 並列設置(5) ○



9. 並列設置(6) ○



10