200401004B

厚生労働科学研究研究費補助金

医療技術評価総合研究事業

保健医療福祉分野における個人情報保護の取り扱いに関する研究

平成１５年度～１６年度　総合研究報告書

主任研究者　山本　隆一

平成１７（２００５）年４月

目　　次

厚生労働科学研究研究費補助金　医療技術評価総合研究事業

保健医療福祉分野における個人情報保護の取り扱いに関する研究　総合研究報告書

主任研究者　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ほぼすべて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保健医療福祉分野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保健医療福祉分野での個人情報の適切な取り扱いのための施策等を検討した。

分担研究者：
大江　和彦　東京大学付属病院企画運営情報部　教授
開原　成允　(財)医療情報システム開発センター　理事長
清谷　哲朗　関西労災病院医療情報部　部長
公文　　敦　(財)医療情報システム開発センター　課長

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、各分野ごとにガイドラインを作成する等の対策が求められている。

本研究は、保健医療福祉分野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、保健医療分野の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

平成 15 年度

B-1-1. 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する。

B-1-2. 米国 HIPAA 法施行後の状況に関する調査

平成 15 年 4 月より、米国 HIPAA 法に関連したプライバシー保護基準が施行されるにともない、政府側の広報や普及策を調査する。また、医療機関、保険会社、代行機関における実施状況や今後の課題を調査する。必要に応じて、米国内での研究成果を取り入れるとともに、米国で調査を行う。

B-1-3. 米国以外の国おいて、OECD のプライバシーガイドラインやセキュリティガイドライン、EU のデータ保護に関する指令などの対応についてインターネットでの情報収集を中心に調査を行う。さらに ISO TC215 で作成が検討されている国際間の診療情報交換におけるデータ保護指針についても ISO 国内対策委員会等を通じて調査を行う。

B-1-4. 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、それの技術的要件を整理する。

平成 16 年度

B-2-1. 出版等による知識普及活動

昨年度に引き続き、医療における個人情報保護のあり方に関する出版を行い、また医療機関、医療関連職能団体、医療機器業界団体などで積極的講演会を開催し、医療における個人情報保護への関心の鼓舞と知識の普及に努めた。

B-2-2. 医療機関における個人情報保護対策の実施状況の調査

全国の医療機関から 2000 件を無作為に抽出し、アンケート調査を実施した。3 月 15 日にアンケートを発送し、締め切りは 3 月 25 日に設定したが 3 月 31 日到着分までを分析対象とした。調査表および回答表を資料として添付する。

B-2-3. 米国 HIPAA Privacy Standards 実施状況の調査

米国会計監査院によって、保健医療情報を保護するための医療機関、保険者等の責務について規定している HIPAA 法 Privacy 規則について、①医療機関と保険者における Privacy 規則遵守の実績、②公衆衛生関連機関、研究者、患者の代理人が患者の医療情報にアクセスする際の実績、③患者が自らの権利について理解する限界　等について調査しており、この結果を分析した。

医療情報管理システム協会(HIMSS)によって、医療機関及び保険者等を対象に HIPAA 法準拠の状況について調査しており、この結果を分析した。

米国の医療機関及び保険者においては HIPAA 準拠のために弁護士等の資格を有するコンサルタントと契約する傾向にある。フロリダ州にある法律事務所で HIPAA 法専門の医療コンサルタントを行っている弁護士に、現在の医療機関等における HIPAA 法 Privacy 規則の遵守の状況や医療機関の負担と課題、実情について聴取した。

B-2-4. 医療情報システムの安全管理に関するガイドラインの検討

個人情報保護法（関連３法）は対象分野を限定しないために、きわめて抽象的で、情報セキュリティのように、あくまでも相対的な評価しかなしえない対策においては基準を定めることが難しい。そのために、関係省府は指針を定めている。本研究では経済産業省の指針と厚生労働省の医療・介護関係事業者における個人情報の適切な取り扱いに関するガイドラインを精査し、要件を抽出した。

平成６年に医用画像の電子保存を容認する通知が出され、その際に基準と指針が作成されている。また平成１１年にいわゆる電子保存の容認通知が出され、基準と指針が作成された。また海外では HIPAA 法の実施にあたって、米国厚生省が security standards を省令として定めている。これらを精査し、要件を抽出した。

以上で抽出した要件の中で、電子保存等の特別な行為に依存しない一般的な安全管理対策を基礎として、厚労省、経産省の２指針の要件を加味し、安全管理指針を作成した。

C．研究結果

平成 15 年度

（１）継続研究

今年度の新規採用課題ではあるが、厚生科学研究（医療技術評価総合研究）「医療情

報技術の総合的評価と推進に関する研究」（平成 10-12 年、主任研究者：開原成允）により、「診療情報利用の現状と個人情報保護法大綱案を踏まえた診療情報保護のあり方について」を作成した。また、厚生科学研究（医療技術評価総合研究）「医療分野における個人情報保護対策に関する研究」（平成 13-14 年、主任研究者：開原成允）により、全国の医療機関等にアンケート調査を実施し、臨床現場における個人情報の取扱いの現状について調査・研究した。また、米国 HIPAA 法等海外の個人情報保護対策の動向を調査・研究した。本研究班はこれらの研究活動の継続ととらえられため、それぞれの成果については研究報告を参照されたい。また継続研究の一環として、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）米国における HIPAA 法の施行状況の調査

分担研究者の清谷と公文が 2003 年 9 月に Baltimore で開催された National HIPAA SUMMIT に参加し、米国の HIPAA 法および関連規則の制定に中心的役割を果たしている Braithwaite 博士、the Centers for Medicare & Medicaid Services (CMS) の Dr. Stanley Nachimson, HIPAA Privacy Standards の米国大学関連病院での対策ガイドライン作りに中心的役割を果たした Duke University の Dr. J. David Kirby にインタビュー調査を行った。これらのインタビュー結果には個人情報保護面だけではなく、電子請求や標準化に関するものを多く含まれるが、ここでは個人情報保護に関連する結果を以下に示す。

A. Privacy Standards について (Dr. Kirby)

○HIPAA Standards では診療基本３目的（Treatment, Payment, Operation）に関する患者の了承がオプショナルになったが、州によっては書面での了承を求めている。

○患者の関心は高い人と低い人に分かれる。高い人には芸能人や社会的地位の高い人が含まれる。

○UCLA の研究によれば、電子カルテを扱う職員のうちの半分は、スクリーニングサービスを行うためにアクセス権を利用しているという結果が出ている。

○HIPAA 法では、法違反に対する罰則が極めて厳しくできている。(意識の低い覗き見－innocent record reviewer も対象となっている)

○ハーバード大の実験（システム）では、患者は、誰が自分の記録にアクセスしたのかを確認することができるようになっている。米国では医療機関内で、一人の医療記録にアクセスするヒトは平均して 50 人ほどいるといわれているが、ハーバードの場合は、上記のシステムを導入して 2-3 か月でアクセス数が減少する結果がみられた。とはいえ、1 年に 2-3 回は、患者のいとこ、前夫といった資格の人間が患者の状態を確認しようとする現象がおこっている。

○以前は、(患者の知名度高い場合や事件性がある場合などの）場合によって、患者の容態について記者発表することがあったが、HIPAA 法施行後は全くなくなった。ただし、公衆衛生上のプライオリティが高いときなどは例外である。

○HIPAA 法 Privacy Standards 施行の準備期間の目安と予測については、200 床未満の小規模医療機関では約 1 年間、大学病院クラスでは 3-4 年間と考えられる。

○大学病院クラスの場合、システムの変更や研修など、直接的な投資が 100 万ドル、間接的な投資は 20-40 ドル×全従業員数／年と考えられている。

○Privacy 保護に関する有能なコンサルタントは極めて少ない。

B. Medicare, Medicaid から見た医療機関の準備状況（Dr. Nachimson）

○多くの医療機関が HIPAA 法全体への準備不足の状態にあると考えられるが、そのなかでは Privacy Standards への対応に対する努力が優先されているようだ。

○準備は、ソフトの組込みやシステムの変更等が困難で、予測を上回る作業量となっている。また医師が医療機関に Social Security Number を知らせることを拒んでいる。これらの理由により、医師や医療機関における実証テストの導入そのものが難

しかったり、テスト期間が長引いている状況にある。

（3）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。

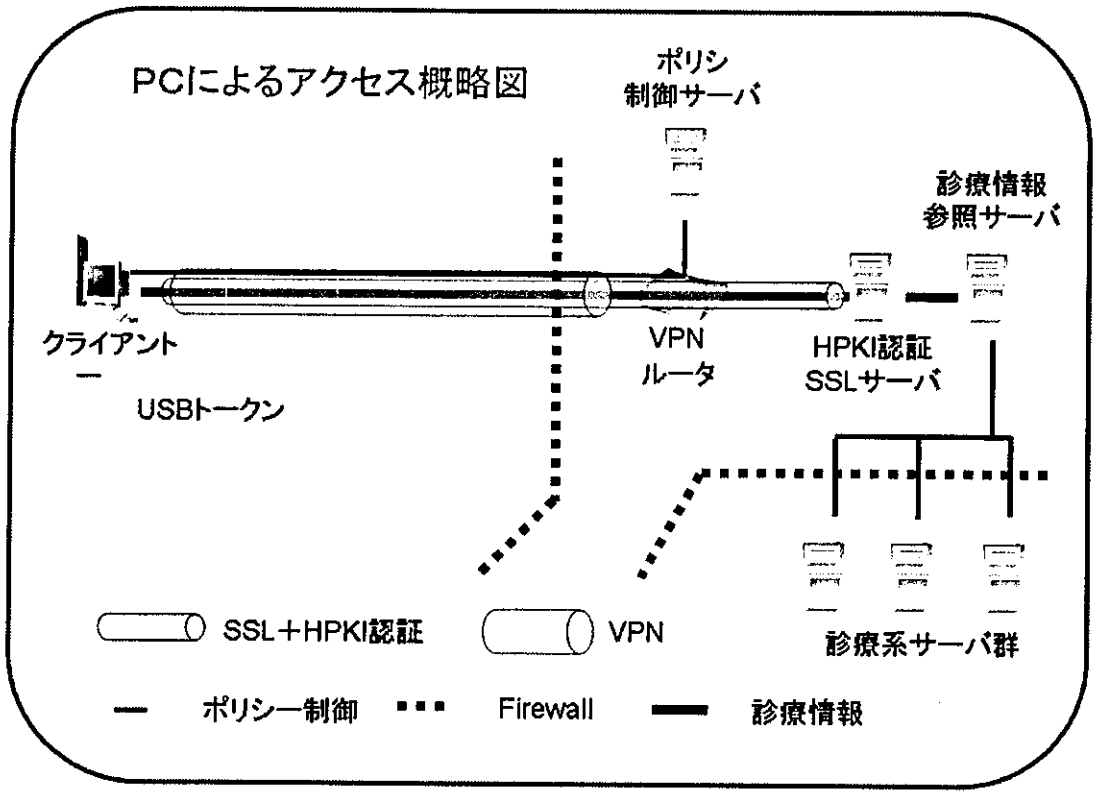

図１　実験システムの概要

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。

平成 16 年

（1） 出版等

昨年度上梓した「医療の個人情報保護とセキュリティ（有斐閣 2003)」の改定を行った。改定版は現在校正がほぼ終了し、出版準備中で 2005 年 4 月中に出版予定である。また主任研究者が「個人情報保護法対応マニュアル（日経メディカル編、日経 BP 社)」の第３章「医療情報システムの安全管理に関するガイドラインとは何か」を監修した。

（2）米国 HIPAA Privacy Standards 実施状況の調査

分担研究者の清谷と公文が昨年に引き続き米国の HIPAA Privacy Standards の施行状況の調査をおこなった。具体的な問題点はいまでも存在するが、昨年の調査にくらべて医療機関の対応は進んでおり、いわば落ち着いた状況に移行しつつあると言える。

（3）．医療情報システムの安全管理に関するガイドラインの検討

1. 個人情報保護法に関する指針等の安全管理義務にあたる部分の要件抽出。

厚労省、経産省のいずれの指針も組織的、人的、技術的、物理的対策を求めており、リスク分析を基礎に体系的な対策をとることを求めている。また、やや具体的なレベルとしてはアクセス制限、アクセス記録の採取と保存を求めている。その一方でアクセス制限やアクセス記録の基礎となる利用者の識別に関しては言及されていない。また平成１７年３月末時点で公表されているＱアンドＡでは個人情報をコンピュータシステムへ入力する際に、入力やの記録は必ずしも必要でないとするなど、矛盾した対

応も見られる。

2. これまでに公表されている医療情報システムの安全管理に係る指針の調査

平成６年の医用画像の電子保存の指針は、基準自体がほぼ技術的対策に限定して述べられていることもあって、技術仕様書といっても良いものであった。情報の完全性や可用性に関しては技術のみでも対策は不可能ではないが、機密性や情報主権の勘案など個人情報保護の観点からの安全管理対策は情報の利活用の場面でも保障される必要があり、技術だけでは達成できない。その意味ではこの指針は現時点では著しく不十分といわざるを得ない。

平成１１年の電子保存通知の際に作成された指針は技術と運用のバランスで安全管理を達成することを求めており、現実的な指針となっている。また組織的、人的、物理的対策にも言及はされている。しかしながら、技術面ではかなり厳格に中立的立場で書かれており、著しく具体性に欠ける。そのために、技術的対策と相補的に講じられるべき組織的、人的対策も、歯切れの悪い記載になっており、電子保存のように、ある程度技術力のある組織が実施する、いわば特殊な状況での指針としては機能するが、個人情報保護法への対応のように、医療情報システムを導入しているすべての医療機関が対応しなければならない状況では不適切と考えざるをえない。

米国の HIPAA Security Standards も国際的に見れば重要な安全管理基準ではあるが、Privacy Standards が医療情報全般を対象にして作成された汎用的なものであるのに比べて、Security Standards は HIPAA 法の一部である、オンライン診療報酬請求にかなり限定して定められたもので、また、内容は主にシステムのベンダー向けであり、抽象的である。米国では HIPAA 法の施行前はわが国ほどレセコン等の情報機器の導入は進んではなく、HIPAA 法のオンライン診療報酬請求の義務化に対して導入を行う医療機関が多いために、このような基準で機能するのであろうが、わが国のようにすでに７０％以上の医療機関に医療情報システムが導入している状況では、やはり具体性に欠けるといわざるを得ない。

なお、平成１４年にわが国では外部保存に関する通知が出され、基準と指針が作成されているが、安全管理に関しては、平成１１年の指針と大きく異なる点はないために、ここでは割愛する。

3. 個人情報保護法に対応する情報システムの安全管理指針の作成

２の結果から、平成１１年の電子保存に関する指針から電子保存を行うか否かにかかわらず安全管理上必要な項目を抽出し、1の２つの指針の要件と和をとり、指針を作成した。概要を以下に示す。

１．方針の制定と公表

電子保存の指針では透明性の確保は触れられていなかったが、個人情報保護の指針で、特に厚労省指針では透明性の確保は重視されており、追加した。

２．情報の取り扱いの把握とリスク分析

リスク分析は安全管理上もっとも重要な初期ステップであるが、医療機関はスタッフの信頼関係を基礎に医療業務を行っている関係からか、リスク分析が不得意な傾向にある。したがってリスクを例示し、取り組み易さを目指した。以下の亜項目にわけて示している。

２．１　取り扱い情報の把握

２．２　リスク分析

３．組織的安全管理対策（体制、運用管理規程）

体制は適応する組織の形態に大きく依存するし、運用管理規程も物理的な対策や技術的対策と相補的であり、具体的な記述が困難な部分であった。運用管理規程は物理的対策や技術的対策に応じて具体化されるべきもので、対応表形式で整備することが望まれる。

４．物理的安全対策

情報システムの物理的安全対策は建物の立地条件から考慮されるべきであるが、すでに大多数の医療機関に導入されている医療情報システムの安全管理を扱う指針であることから、管理区分の設定と施錠、入退管理のみを記載した。

５．技術的安全対策

平成１１年の電子保存に関する指針が技術的中立性を基本としたために全体として理解しがたいものであったことを踏まえ、具体的な技術要素にできるだけ触れることとした。利用者の識別及び認証、情報の区分管理とアクセス権限の管理、アクセスの記録（アクセスログ)、不正ソフトウェア対策の４項に分けて指針を示した。もっとも重要な利用者の識別および認証においては、パスワード認証、生体計測認証、IC カード等の所持情報のそれぞれ技術的な特徴と採用する際の運用上の留意点を示した。また技術要素は現時点でのコストも勘案して記載したために、精度は高いものの高額のために、一般的な医療機関では採用が困難なものは除いて指針を示している。

６．人的安全対策

医療機関の職員に対する対策と、第三者、特に情報システムの保守等の委託契約に対して言及している。

７．情報の破棄

個人情報保護法が存在しなくても医療従事者の守秘義務の観点から重要な項目であるが、これまで存在する医療分野の指針では積極的に触れられていなかった項目である。内容は単純であるが、指針として明記した。

８．情報システムの改造と保守

医療情報システムにとっては重要な項目であり、６の人的安全対策の委託契約と一部重複するが、しばしば実施される点数改定や制度の変更による情報システムの改造は、いわば日常茶飯事であり、それだけに指針として明示する必要がある。あくまでも医療機関が責務を全うするという観点から監督責任に重点をおいた指針とした。

９．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

オンラインメインテナンスやネットワークを利用した医療連携が相当する。現時点でそれほど普及しているわけではないが、維持コストや連携密度を上げる観点から今後急速に普及すると思われるために、特に指針を示した。ただし、ＡＳＰ型のレセコンや電子カルテに代表されるオンラインの外部保存に関しては、単なる安全管理だけではなく、情報の二次利用の制限や責任分担などさまざまな問題があるために、安全管理の指針としては対象外としている。

なお、本指針案の作成は厚生労働省医療情報ネットワーク基盤検討会合同作業班の班員の多大な貢献があった。

（４） 医療機関における個人情報保護対策の実施状況の調査

アンケート送付数は 2000 件であったが、あて先不明等で送付できなかったものが 84 件あり、送付対象は 1916 件で、うち、回答が返送されたものは 450 件（回答率 23.5%）であった。

対象の規模は病床数１９床以下の診療所が 54.6%、病院が 45.6%であった。また特定機能病院が３施設、地域医療支援病院が７施設含まれていたが、98%は一般病院または診療所であった。

個人情報保護法は医療機関の開設者によって適用される法律が異なるために、開設者の種別を聞いたが、独立行政法人が 1.2%、地方公共団体が 6.3%で、他は民間立であった。

個人情報保護法への対応に関する回答を図２に示す。少なくとも対応を始めている施設が 32.5%に過ぎない。また内容をまったく知らない施設が 10%以上ある。

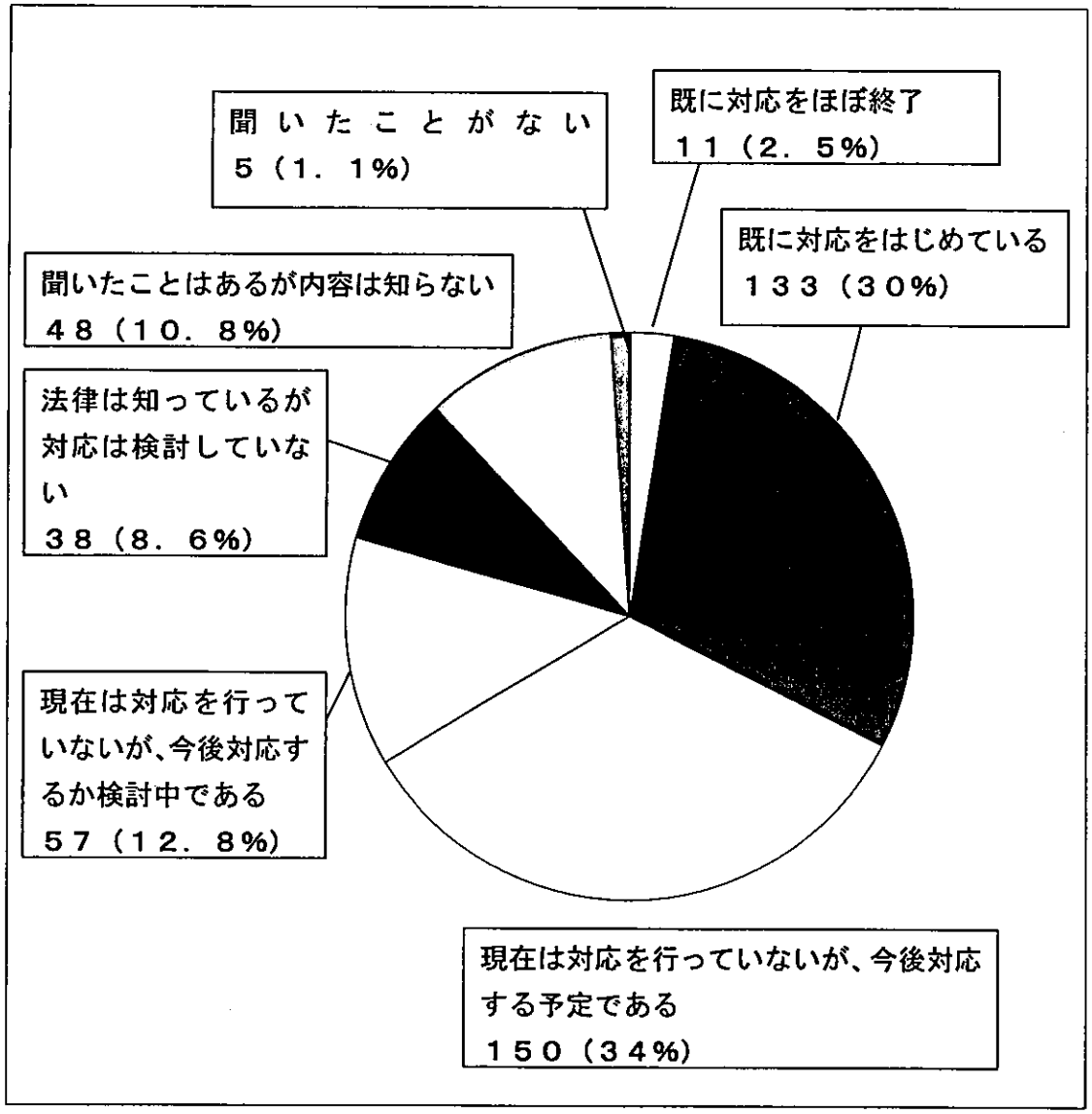

図２　個人情報保護法への対応について

また厚生労働省の「医療・介護関係事業者における個人情報保護の適切な取り扱いのためのガイドライン」の活用状況についての回答を図３に示す。ガイドラインを参考にした、またはするつもりの施設が72.3%でガイドラインを知らない施設が20.5%あった。

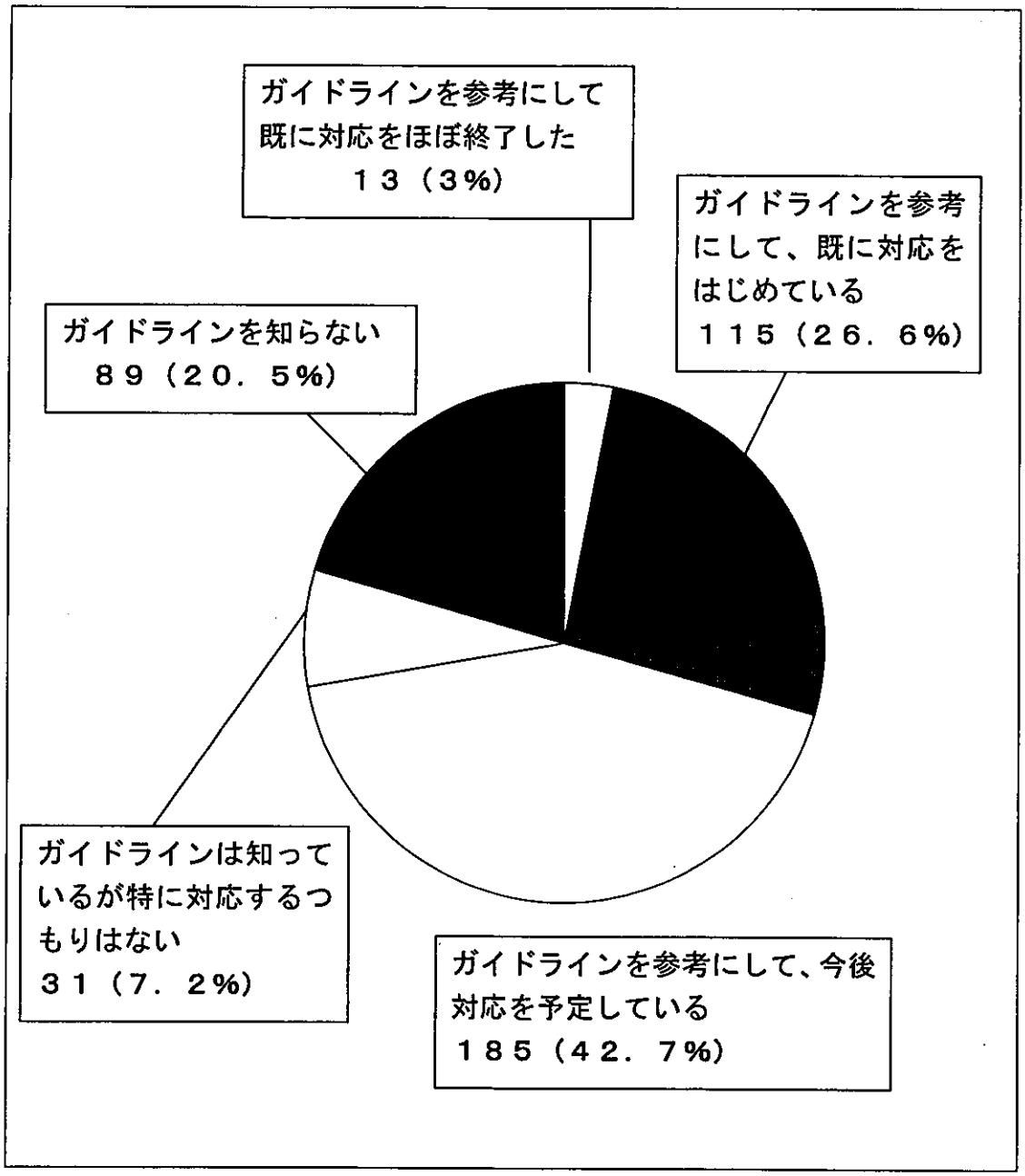

図３　「医療・介護関係事業者における個人情報保護の適切な取り扱いのためのガイドライン」について

対策の個別の項目についてはプライバシーポリシーの作成についての回答を図４に、利用目的の通知等に用いる院内掲示物に関しては図５に、患者向けの配布物に関して