図19

依頼施設からの画像伝送について
（複数回答可）

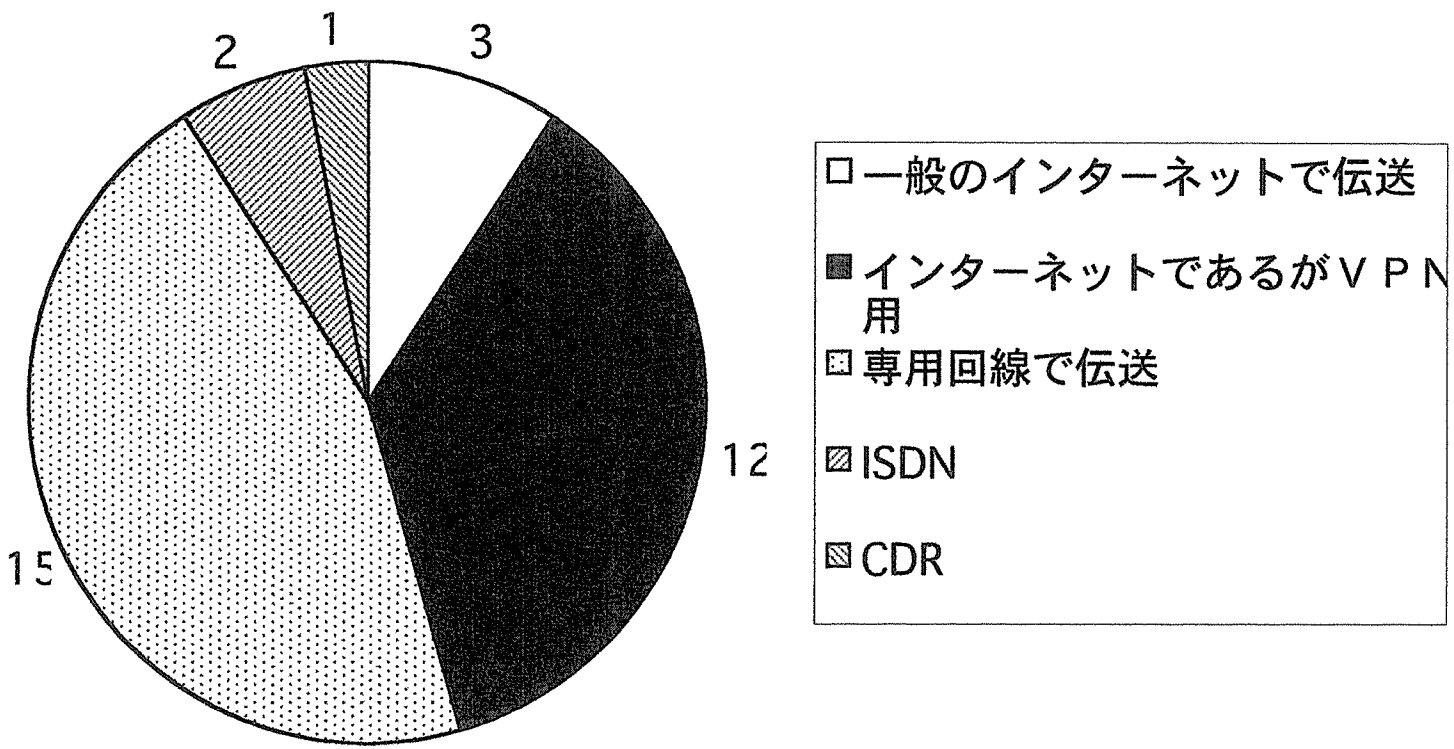


図20

依頼施設側のシステムの利用について実際に行っている項
（複数回答可）

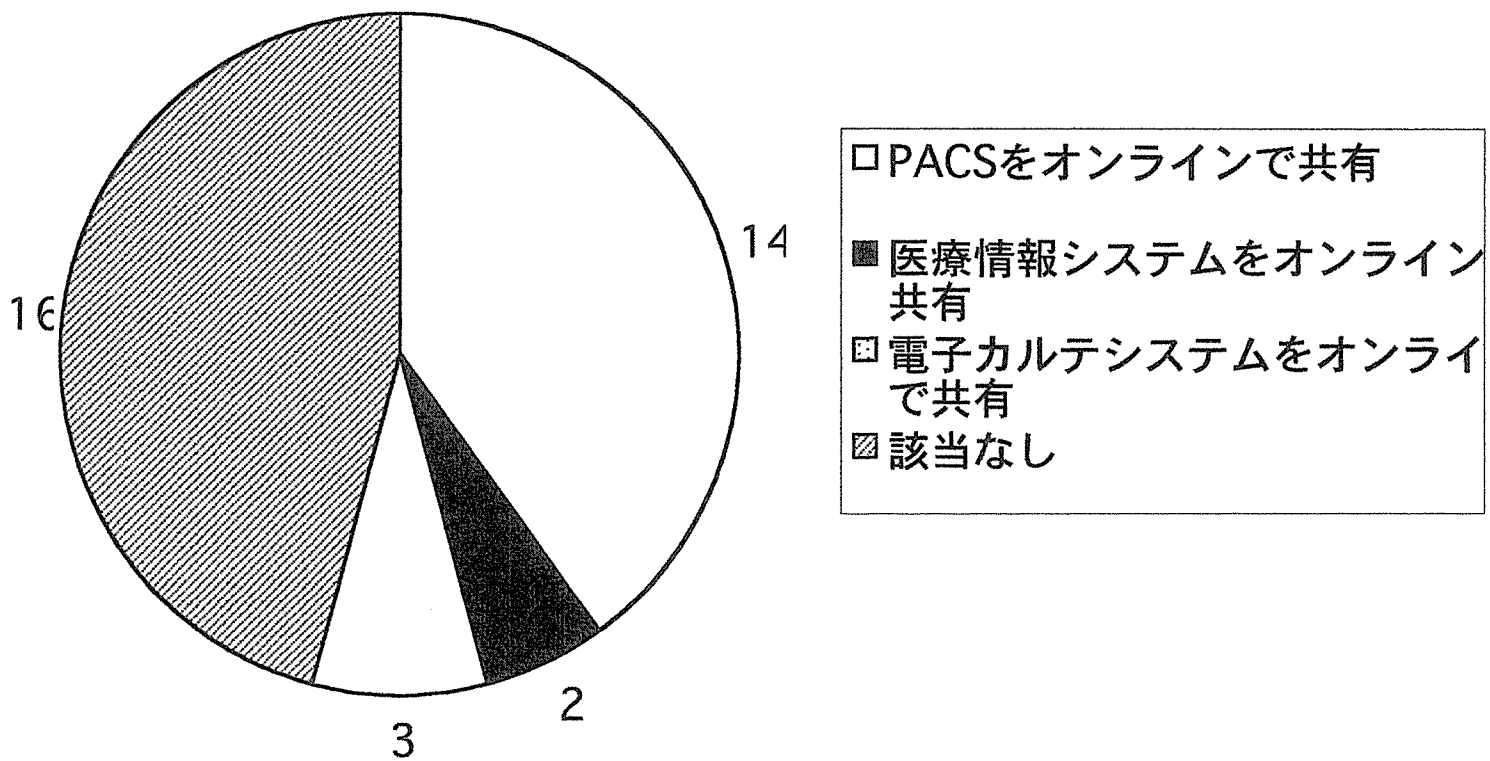


図21

今は行えていないが行えたら良いと考えられる項
（複数回答可）

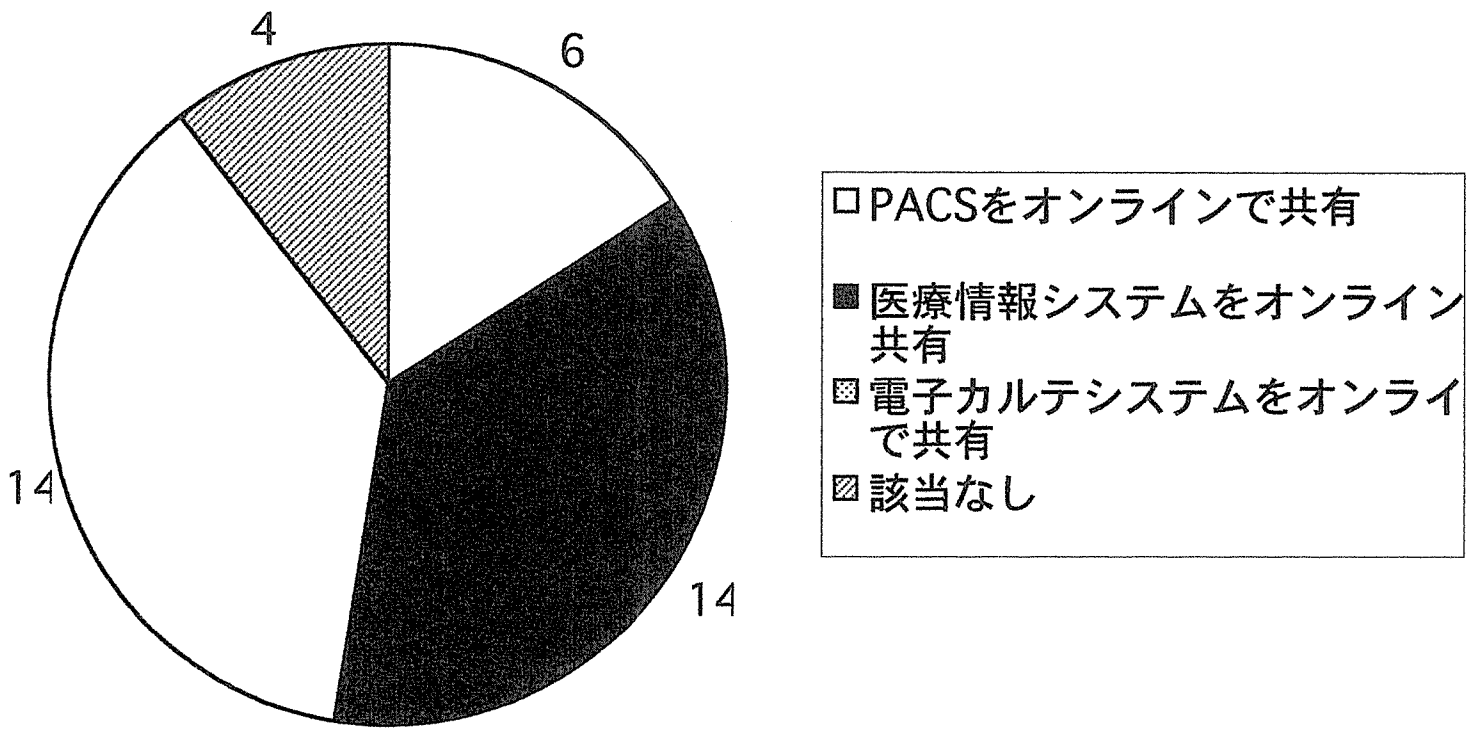


図22

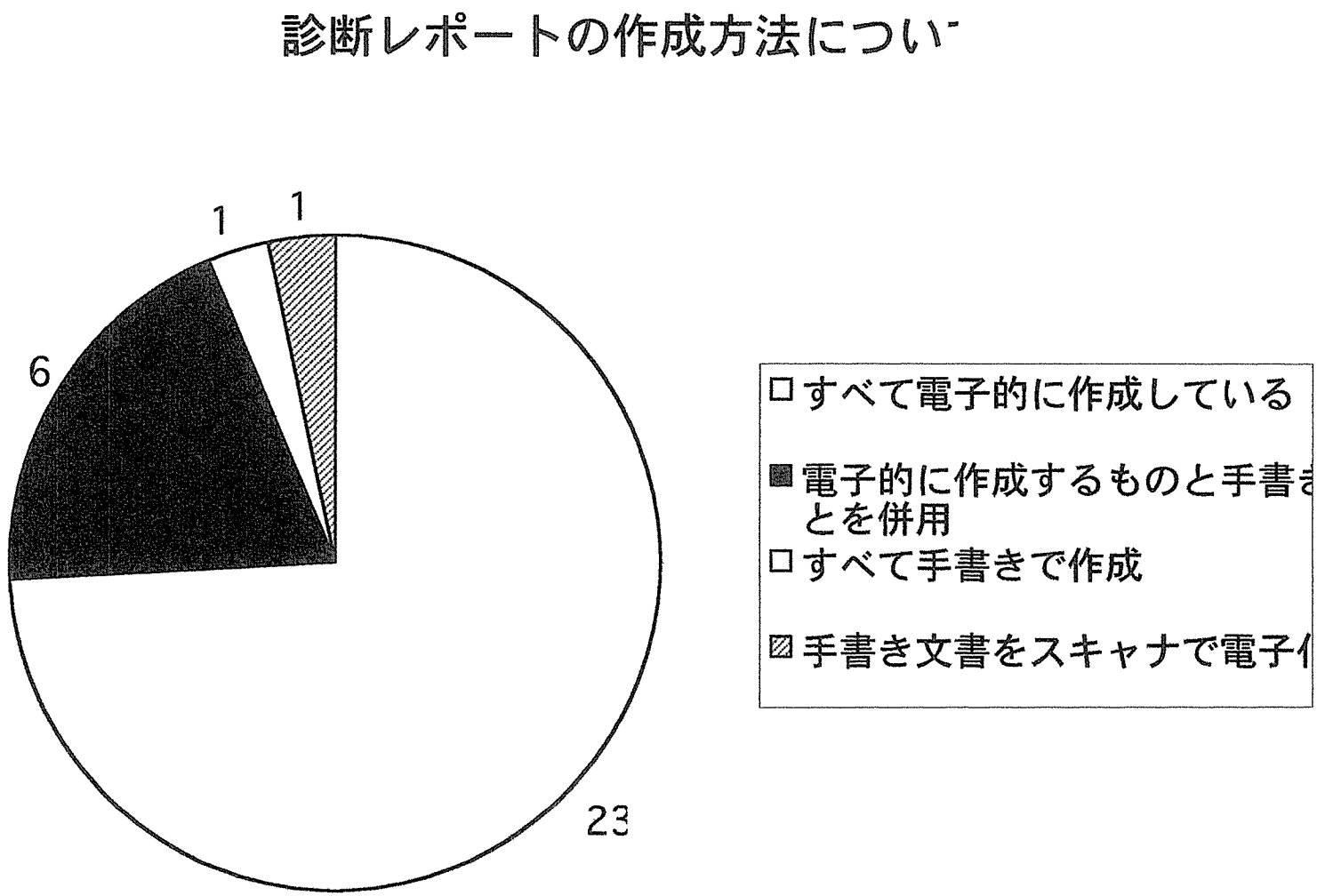

診断レポートの作成方法につい
1
1
6
23
すべて電子的に作成している
電子的に作成するものと手書き
とを併用
すべて手書きで作成
手書き文書をスキャナで電子化

図23

検査依頼情報（患者の基本情報および臨床情報の受け取りについて

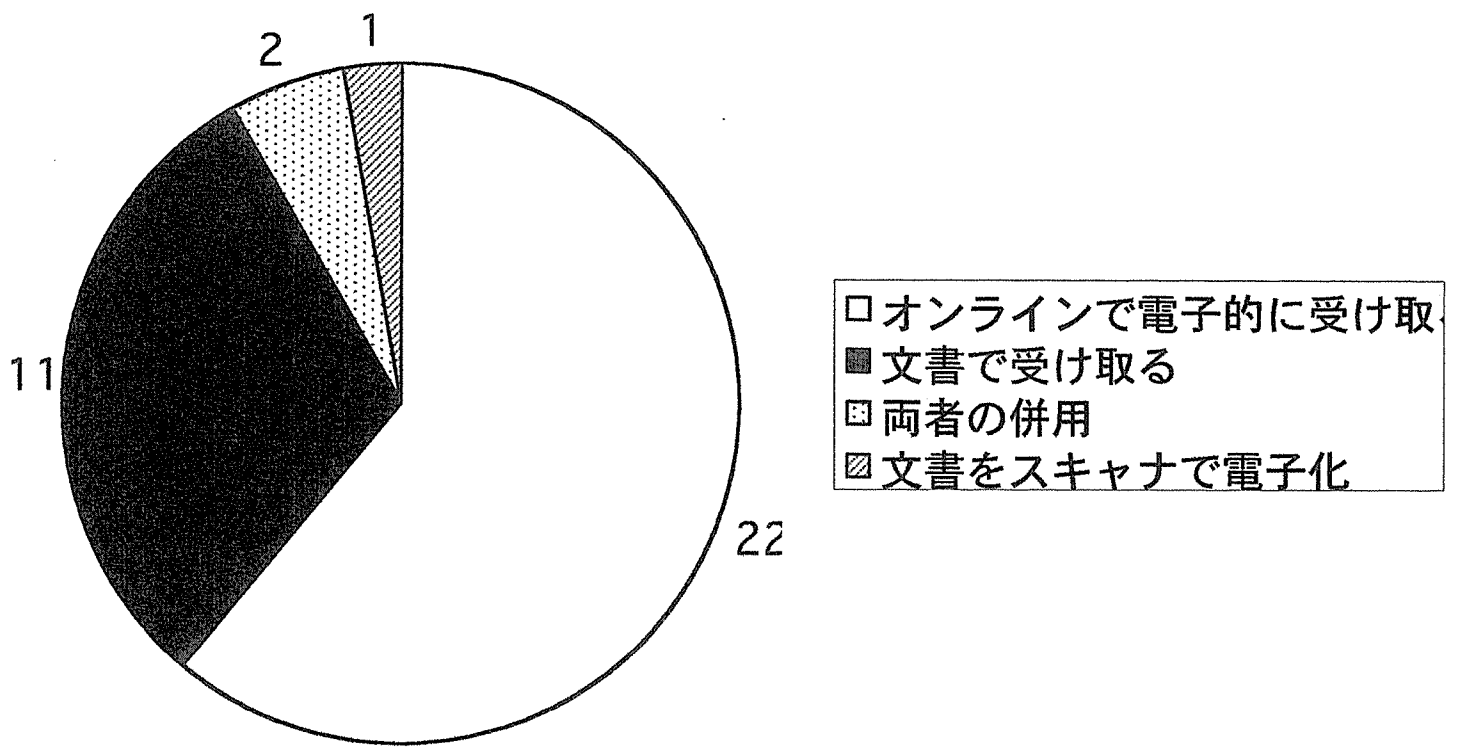


図24

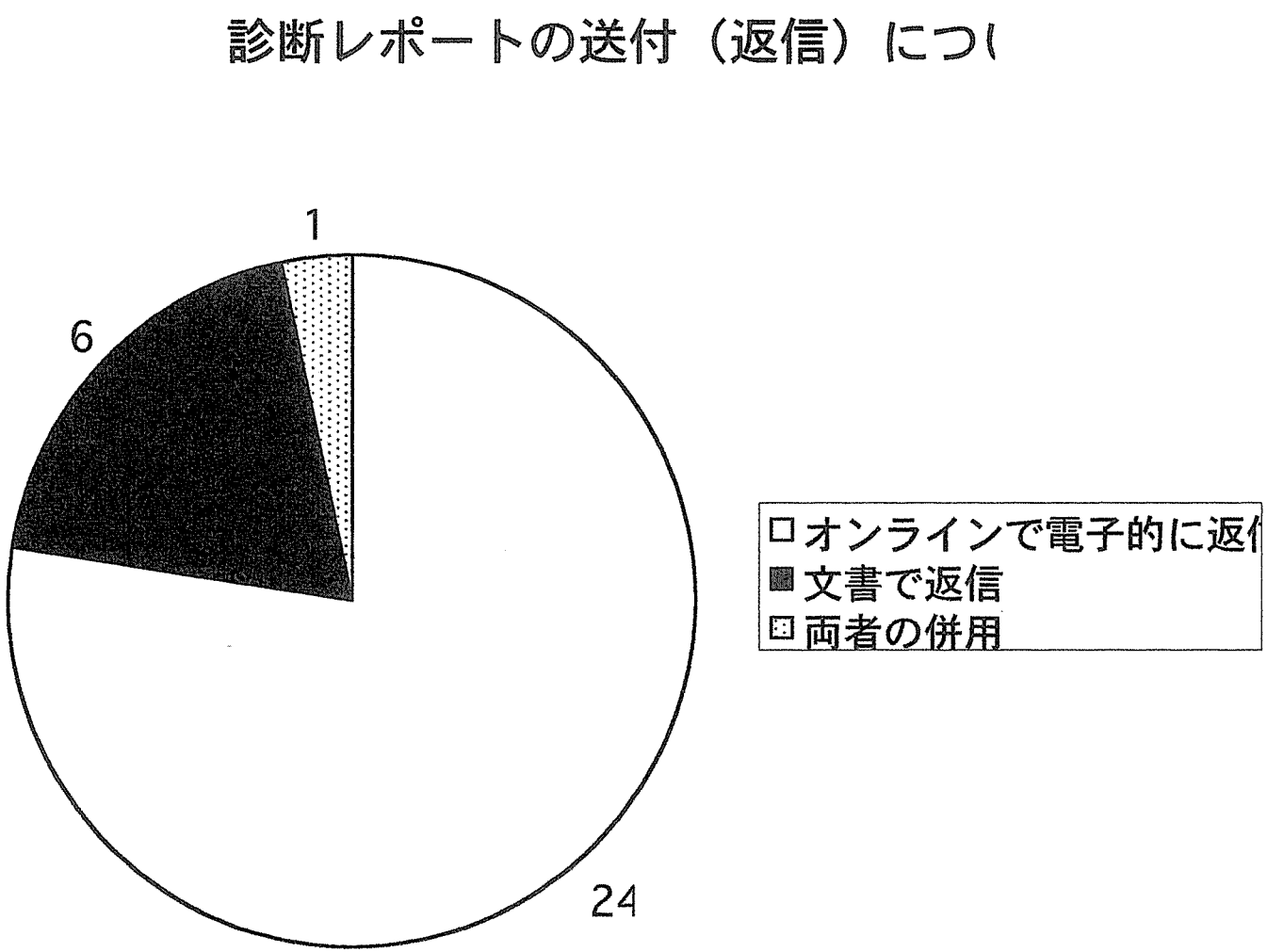


図25

電子的に検査依頼情報を受け取る場合，
依頼情報の読影後の保管状況

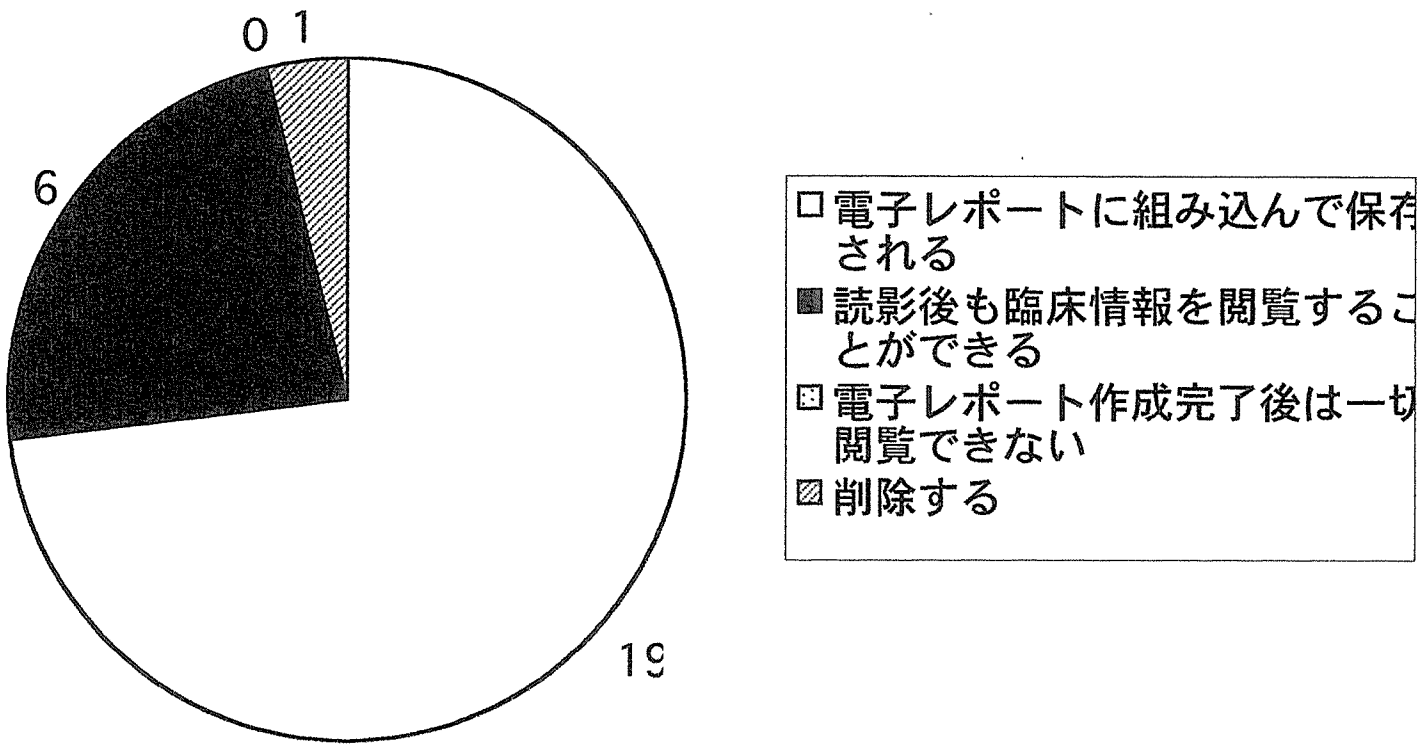


図26

手書き文書で依頼情報を受け取る場合，依頼情報
読影レポート完成直後の保管状況について

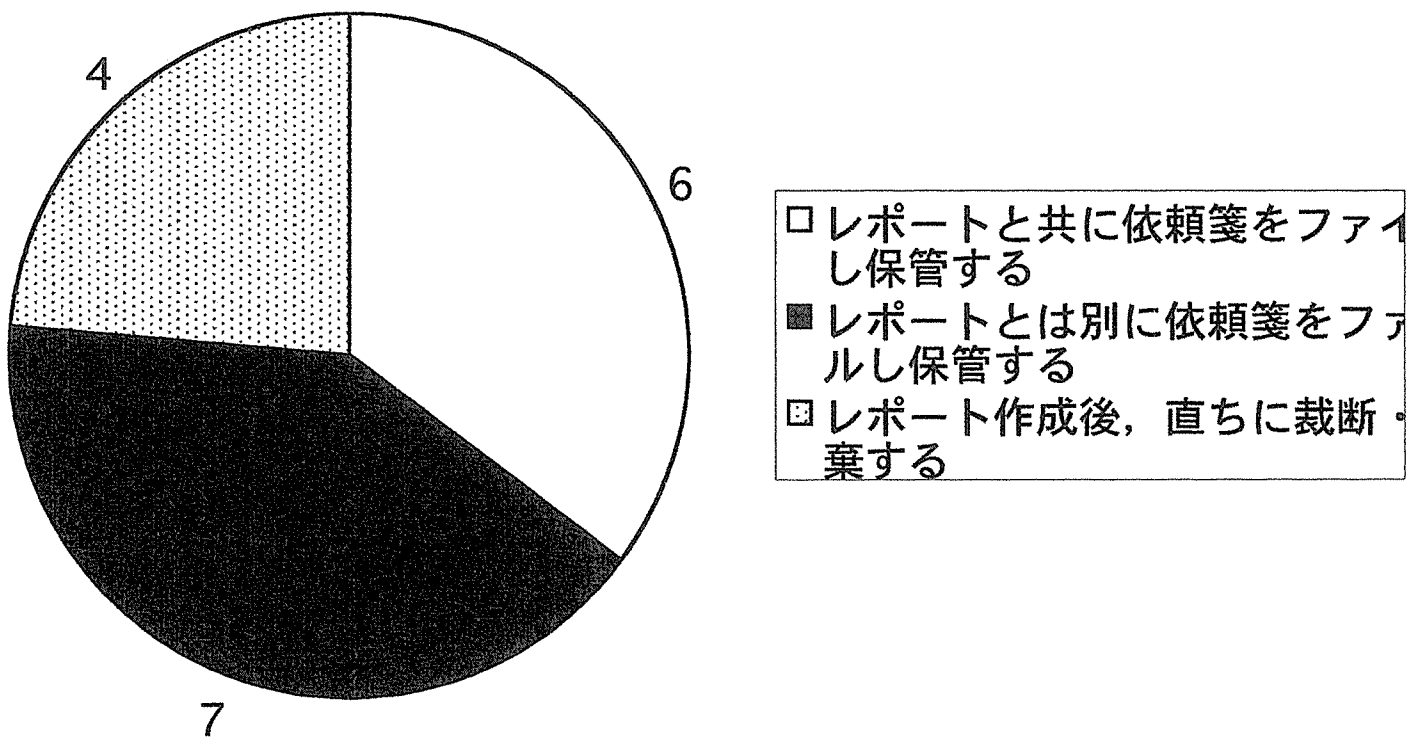


図27

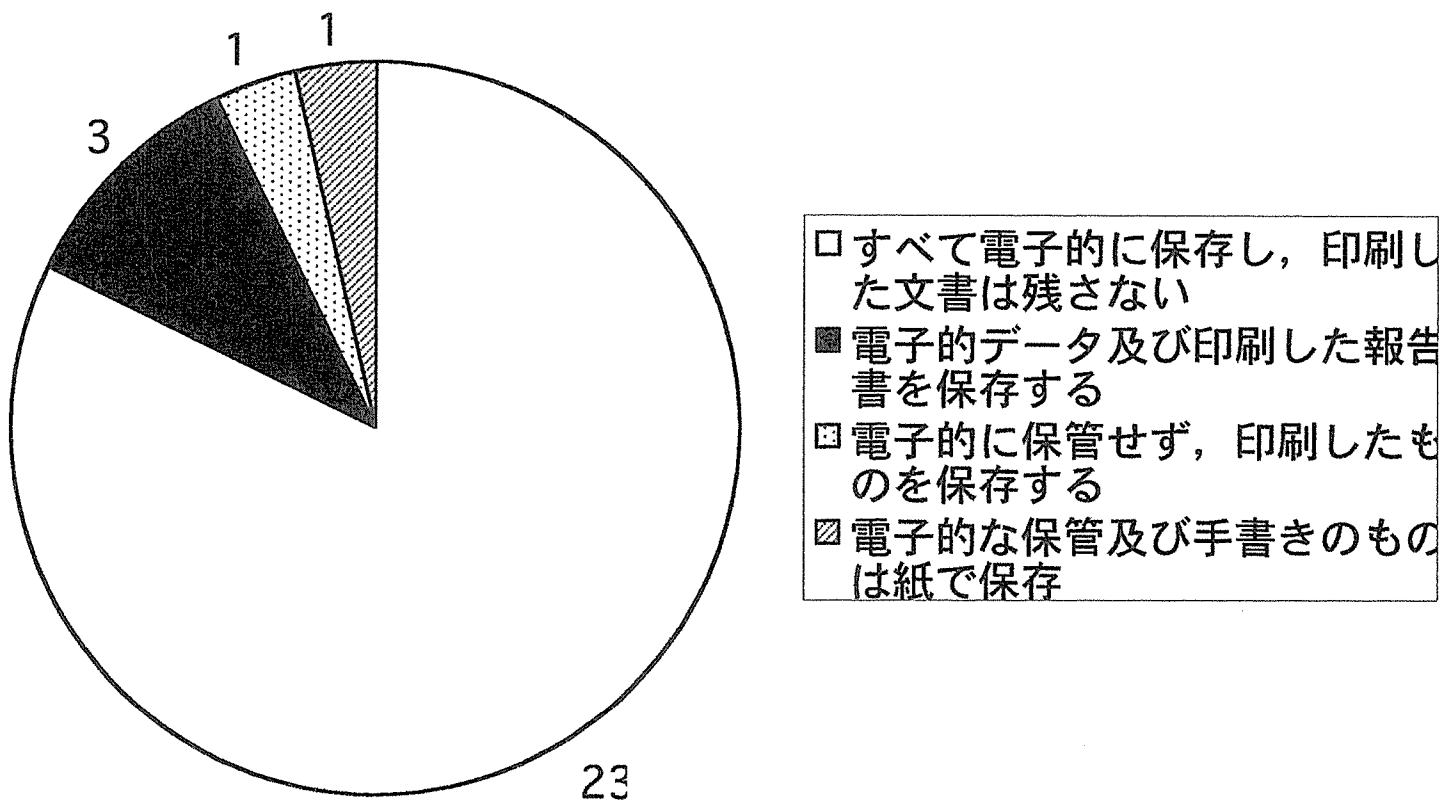
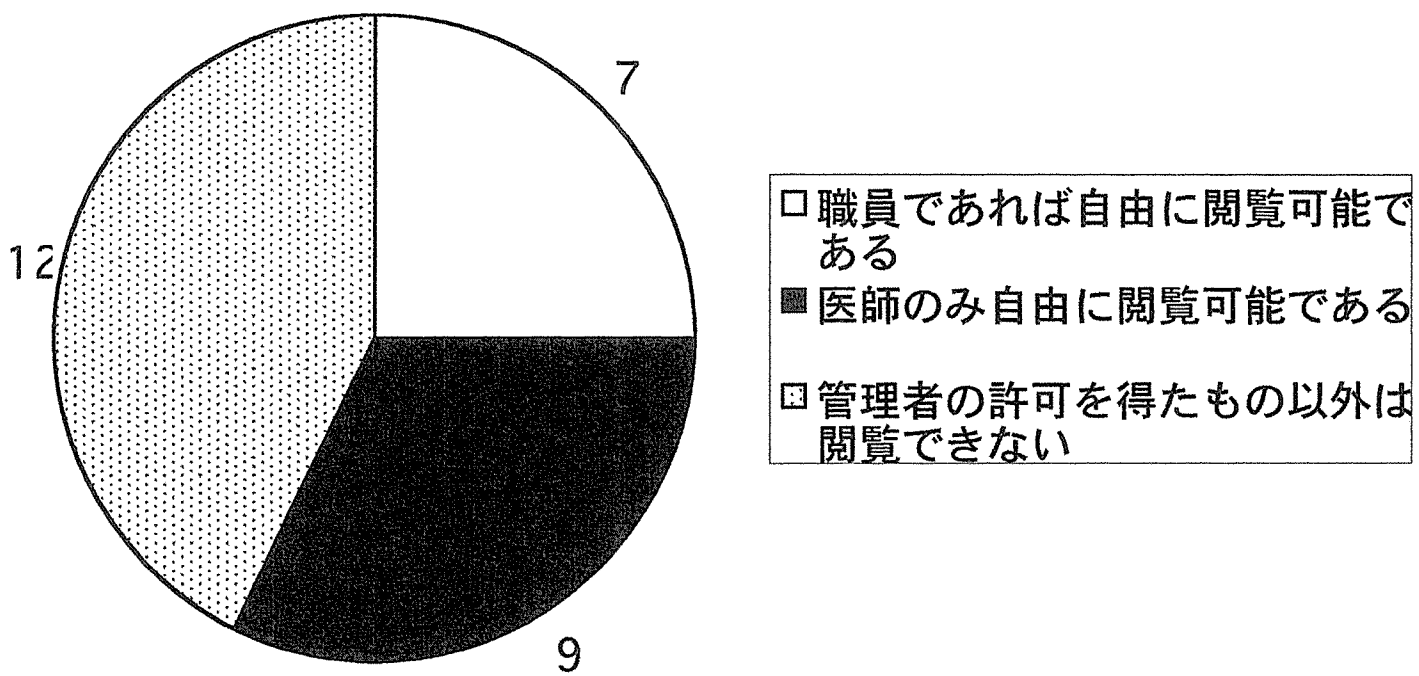

レポートの保存方法について
1
1
3
23
すべて電子的に保存し，印刷した文書は残さない
電子的データ及び印刷した報告書を保存する
電子的に保管せず，印刷したものを保存する
電子的な保管及び手書きのものは紙で保存

図28

依頼箋，レポートなど印刷された文書又は電子的な文書
施設内での閲覧状況について



電子カルテの安全性確保に関する調査研究

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　電子カルテをはじめとする医療のIT化は単に医療機関の事務の合理化のために行われるのではなく、国民の医療の向上に役立つものであるべきである。IT化によって大きく国民の医療の向上に寄与する電子化診療情報の用途の一部として、医療機関間の情報交換である診療情報提供書と利用者である患者への情報提供が挙げられる。しかしこれの用途も安全性確保が前提であることは言うまでもない。本研究では「医療情報システムの安全管理にかんするガイドライン」の主に広域ネットワークを利用する際の安全基準の改訂を調査・考察するとともに、医療情報の安全管理の基本要素である電子署名およびタイムスタンプの実施の上で問題となる外部ネットワークとの接続法について実証的に解決を行った。

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。その一方で、高度な経済効率を達成しているわが国の医療において、経済的に破綻をきたさずさらなる医療の質の向上にはIT技術の導入は避けられない。医療情報システム全般に対しての安全指針は平成15年3月に厚生労働省が安全管理に関するガイドラインを示したところであるが、この指針は当時の医療のIT化の程度に応じて、他施設とのオンラインの伝送に関しては限定的な記載にとどまっていた。また昨年度の本研究班の研究で電子署名およびタイムスタンプを施した電子診療情報提供書の運用にあたって多くの医療機関の業務システムがインターネットに接続されていないことが問題であることを指摘した。本年度は先にのべた「医療情報システムの安全管理のためのガイドライン」（以下、「安全管理GL」と呼ぶ）の改訂の作業班主査として参加する機会があったので、この改定内容について検討するとともに、昨年度指摘した問題点の解決を試みることが本年度の分担研究の目的である。

昨年1月に内閣から公表されたIT新改革戦略および6月に公表された重点計画2006では医療分野は重要な部分を占めており、またその内容の多くは医療機関が広域ネットワークを利用することが前提になっている。したがって本研究はこれらの方針を実現するにあたって重要な意味を持つと考えられる。

B．研究方法

「安全管理GL」の改訂は、本来理解を容易にするためにトレンドの技術にも触れていることから定期的に見直しが求められるものであるという理由からも検討されたが、もっとも大きな動機は前述のようにIT新

改革戦略や重点計画 2006 で初版当時の前提として IT 化から広域ネットワークを積極的利活用する IT 化にシフトすることが明確になったことと、サイバーテロや災害時の対策を明記する必要になったことによる。後者は一定の IT システムの普及とそれらに医療が依存する割合の増加によるものである。ただ本研究では後者は直接の対象ではないために、主に、広域ネットワークを利活用することを前提とするための改訂点を中心に考察する。具体的には制度的な要件を整理し、現行の技術を俯瞰したうえで、改訂結果を評価する。

また、昨年度示した、電子署名およびタイムスタンプを活用していくうえでの問題点に関してはプロキシシステムを実験的に構築し評価する。

C．研究結果

（1）安全管理 GL の改訂に関して。

旧版の安全管理 GL は外部の広域ネットワークの利用に関しては 6.9 章にきわめて基本的な記載があり、また診療録等の外部保存に関する場合に関しては８章に、これも概念的な記載があるにすぎなかった。

しかし 2006 年に内閣から IT 新改革戦略が公表され、重点計画 2006 を含めて医療機関等が外部の広域ネットワークへの接続を前提とする IT による構造改革が推進されることが明確になり、安全管理 GL に具体的な記載が求められるようになった。旧版の安全管理 GL は医療情報の専門化とシステムを提供するベンダーおよび利用者の立場を代表するものが作業班を形成して作成したが、今回の改訂にあたってはこれらのメンバーとともに、回線提供者やネットワークサービス提供者も参加し、また通信サービスを所轄する総務省からもオブザーバが参加した。現在作業班として望みうる参加者はすべて参加していると考えることができる。

改定は主に旧版の 6.9 章を全面改定する形で行われている。ただし災害対策等が追加され、章番号は 6.10 に変更されている。

安全管理 GL は A：制度的な要求事項、B：解説、C：最低限のガイドライン、D：推奨されるガイドラインという構成をとっているが、6 章全体の制度的な要求事項は個人情報保護法および関連ガイドラインであり、6.10 章に特別に加わった要求事項はない。したがってこの章も A はなく、B の解説から始まっている。B は３つのパートに分かれており、B-1 は総説、B-2 は具体的な要求事項、B-3 は採用する通信サービス別に考慮すべき点を述べている。総説からしだいに詳細な解説に移行していると言ってよい。B-1 は主に責任分界点について述べられているが、6 章全体の中で、この章でだけ、一つの医療機関等で完結しない事象を取り扱うことを考えると当然と言える。責任分界点には２つあり、一つは情報の管理責任の分界点、もう一つは安全管理の責任分界点である。

情報の管理責任は情報の主権者である患者等にとって開示・訂正・利用の停止を必用に応じて求めることができる対象がどの事業者であるのかを明確にすることと言い換えることができる。個人情報保護法には他の事業者に情報を提供する場合を「委託」と「第三者提供」に分けている。委託の場合、管理責任は提供元事業者にあり、提供先事業者が個人情報保護に関する適切な対処をおこなうように監督する責務は提供元事業者にある。つまり患者等に対する窓口は提供元事業者だけである。その一方で委託に際してはあらかじめ明らかにされた利用目的の範囲であれば通知や同意の必要はない。これに対して第三者提供は個人情報保護法等で例外として記載されている場合を除いて、患者等への通知と同意が必要である。その一方で管理責任は提供先事業者に移動する。つまり提供元事業者が提供先

事業者を監督する責務はない。

安全管理の責任分界点は前記の管理責任の分界点とはレイヤが異なる。患者等から見れば安全管理責任も情報の管理責任の一部であり、違いはない。しかし責任を負う側の観点で考えれば、要求されるのは所謂「善良なる管理者の注意義務」であり、この義務を果たすために通信にかかわるプレーヤの役割分担を明確にする必要がある。たとえばベストエフォートの接続サービスだけ提供する通信事業者と両端の事業者だけが存在する場合、相手の確認や経路上の守秘は両端の事業者の双方またはいずれかの責任であり、通信事業者にはこの責務はない。これに対して両端の事業者に設置された通信機器の認証と経路の暗号化を提供する通信事業者の場合、両端の事業者は通信事業者と正しく契約することで分担すべき役割を減らすことが可能になる。

B-2 は一般的な要求事項の解説であり、B-3 で専用線、ISDN、IP-VPN、インターネットなどに分けて詳細に得失および留意点を解説している。しかしその一方でどのような通信種別を選択する場合でも提供元事業者内で充分な情報セキュリティを確保することを求めている。これには２つの意味があり、一つは通信経路でいかに安全性を確保しても、起点・終点の事業者内でいい加減な情報の安全管理を行えば全体としての安全性を確保できないという、いわば当たり前の事実の指摘である。もう一つは通信経路に流す前に情報自体に一定の安全対策を求めている。通常は暗号化に相当する対策である。

C は B-1、B-2、B-3 から当然帰結する指針ばかりであり、6.10 章には D はない。

（２）タイムスタンプ PROXY の評価

電子署名はわが国には電子署名法があり、法律にしたがって電子署名であれば原則として記名押印に代えることができる。また厚生労働省は 2005 年 3 月に保健医療福祉分野認証局ポリシを公表し、2007 年 3 月には厚労省の Root CA 立ち上がった。保健医療福祉分野での電子署名基盤は着実に整備されつつある。本研究でも昨年度、CDA 文書の電子署名規格および暗号化規格について報告した。しかしその一方で昨年度の富岡総合病院を中心とする実証的な実験において問題点も明らかになっている。それは電子署名の検証とタイムスタンプの付与の２つの場合に原則としてインターネットへのアクセスが必要になることで、実証フィールドではほとんどの医療機関において業務システムはインターネットに接続していなかった。これはこの実証フィールドに特別なことではなく、わが国では 80%以上の医療機関は業務システムを外部のネットワークに接続していない。適切なファイアウォールを設定すれば外部のネットワークへ安全に接続することは可能で、現に大規模な医療機関ではそのようにしているところもある。しかし、多くの医療機関はネットワークの管理に専任者を置く経済的余裕はなく、現実的には困難である。そこで、ファイアウォールセンターのようなものを設置し、各医療機関はそのセンターに VPN 等で安全に接続すれば安全に必要なサービスを利用できるようにする必要がある。これは電子署名やタイムスタンプだけではなく、IT 新改革戦略で提案されている様々な IT による医療の構造改革のためには外部ネットワークへの安全な接続が必須で、応用性は高い。

今年度は現状でもっともニーズが高いと考えられる。タイムスタンプの取得と電子署名の検証に際して必要な CRL/ARL の確認をモデルシステムで検討した。モデルシステムは東大病院内の研究室内に構築されたファイアウォールの DMZ 内にプロ棋士サーバを設置し、ファイアウォールの内部セクションにインターネット VPN で接続した PC からタイムスタンプおよび

CRL/ARL のチェックが可能であることを検証した。タイムスタンププロキシは PFU 社の製品を用い、Windows2003 サーバ上で稼働させ、また CRL のチェックはファイアウォールの外部向け接続許可を CRL サーバだけ許可することで確認した。

結果はまったく問題なく、タイムスタンプが取得でき、また電子署名の検証もクライアントソフトウエアに特別な変更を行うことなく可能であった。

D．考察

安全管理 GL の改定に関しては、B-1 の責任分界点の記述に関して考察を加える。ここで記載されている委託と第三者提供の区別は個人情報保護法に一定の理解があれば当たり前のことであるが、保健医療福祉分野ではともすれば曖昧なままで情報提供が行われることもないとはいえない。たとえば遠隔画像診断を例に考えると、画像診断自体は検体検査と同様に委託業務と考えるのが自然である。しかし、もし、診断に用いた画像情報を後日の参照画像とするために、あるいは症例研究のために診断機関側で保存した場合は単純な委託とは言えない可能性がある。保存期間が限定されており、保存中期間中は提供元医療機関が監督を行っていれば委託であるが、そのような契約でない場合は第三者提供と考えざるとえない。

現実に病理検査や遺伝子検査などにも同様の場合が存在し、しかも現状では委託と第三者提供の区別がかならずしも明確でない場合もあると思われる。オンライン化した場合に限らないのではあるが、あらためて注意喚起が必要で、その意味で安全管理 GL の記載は重要と思われる。ただ、結果の項で述べたように、レイヤの異なる安全管理に関する責任分界点と連続して述べられており、ややわかりにくい印象があり、将来の改善点と考えられる。

タイムスタンププロキシのモデル実験は学術的には新規性はないものの、今後の医療の IT 化において IT 技術者の常駐が期待できない大多数の医療機関も含めた網羅的な IT による構造改革を進めていく上で必須の要件を実証的に解決できたことは意味が大きい。これまでの医療の IT 化はできるところが先進的に進めることを前提に行政的な支援や学術的な研究がなされてきたが、IT 新改革戦略はレセプトオンライン 100%に代表されるように網羅的な IT 化を前提としており、またそうでなければ国民に実感として体感できる構造改革は難しい。その一方で我が国では保健医療福祉事業者の大多数は民営であり、その事業形態や規模は多彩である。そのような状況で一律に IT 化を進めるためには基盤の整備が必須であり、今回実験的に示したファイアウォールのセンターなどもその一例と考えることができる。もっとも基盤といっても純粋な社会基盤というより付加価値サービスも可能な、社会基盤と個別のシステムの中間的なもので、ミドルウエア的とも言える。つまり純粋な公的サービスとして整備する必要はないが、一定の方式で整備される必要はある。今後、この方式や医師会等が整備する場合の公的な支援の在り方が検討される必要があるであろう。

E．結論

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定について調査と考察おこなった。妥当かつ必要な改定であるが、やや表現がわかりにくい点があった。また電子署名にかかわるタイムスタンプおよび CRL/ARL のチェックをプロキシサーバでファイアウォールの内に問題なく中継できることを示し、ファイアウォール内への VPN 接続で一般の医療機関に安全に利用できるものとなることができることを示した。

F．健康危険情報

特になし。

G．発表

論文

１．山本隆一、大江和彦、田中勝弥、「電子化診療情報の患者への提供の在り方に関する調査研究」、文部科学研究補助金特定領域情報爆発 IT 基盤成果報告書、2007

２．山本隆一、「医療施設における個人情報保護」、病院設備、48 巻・1 号，P.74-79，日本医療福祉設備協会，2006 年 1 月

３．山本隆一、「個人情報保護法の導入と診療現場の改革」、病院設備、48 巻・2 号，P.140，日本医療福祉設備学会，2006 年 3 月

３．山本隆一、「医療における個人情報保護」、（特別講演／５回糖尿病教育資源共有機構学術集会）、肥満と糖尿病（別冊）、5 巻・30 号，P.18-26，（株）丹水社，2006 年 7 月

４．山本隆一、「遠隔画像診断のセキュリティと個人情報保護」、Rad Fan、5 巻・1 号，P.18-19（株）メディカルアイ，2006 年 12 月

５．山本隆一、「電子カルテとプライバシー保護」、日本医師会雑誌、135 巻・9 号，P.1954-1954，日本医師会，2006 年 12 月

H．知的財産権の登録・出願状況

現在のところなし。

別紙３

厚生労働科学研究費補助金(医療技術評価総合研究事業)
(総括(分担)研究報告書

安全な保健医療情報流通を促進する保健医療認証基盤整備の技術的方策に関する研究

分担研究者　北里大学　医療衛生学部　梅田　徳男

研究要旨:

医療情報、特に画像情報の保管、伝送時おける秘匿性、安全性を確保する方法の検討を行う。

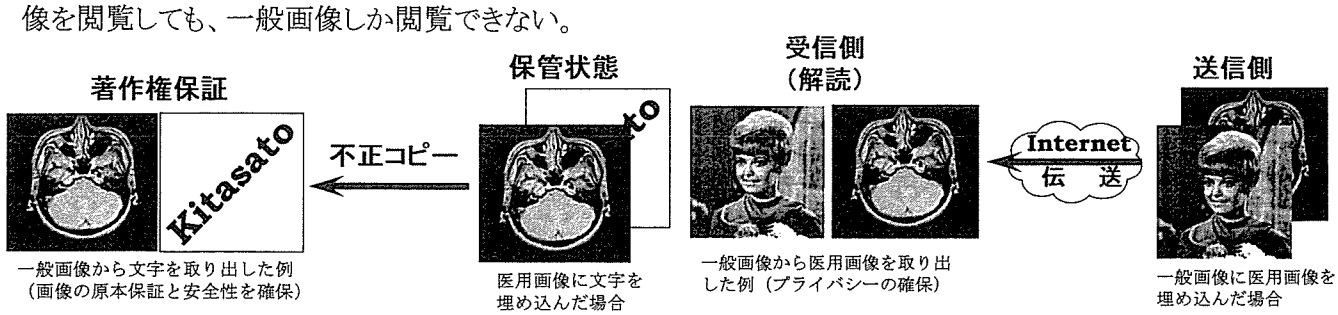
本研究では医用画像の著作権保証、安全性・秘匿性を確保するために、『Watermark(電子透かし)技術』を利用する。この電子透かし技術は透かし情報をノイズ成分に重畳するために、元の医療情報の容量が増えず、新規の大規模な設備も必要としない。まず、医用画像に文字情報を重畳するプログラムの作成を行い、伝送実験を行う。この情報の受信側と発信側とで画像データの欠損、付加の有無の確認を行い、秘匿性の確認確保の確認を行う。その後、文字情報に変えて、一般画像に医用画像を重畳するプログラムの作成し、伝送実験の後、伝送データの確認、安全性の確認を行う。

A. 研究目的:

昨今、個人情報流出が社会問題となり、より厳格な医療施設における医用情報の取扱いが求められている。医療施設でもセキュリティ対策として VPN やファイアウォールなどのネットワークに対するセキュリティは確立されつつあるが、画像情報に対するセキュリティは匿名化のみであるのが現状である。そこで、本研究では画像情報に対する、より高いセキュリティを確保するために、医用画像を一般画像に埋込む技術である Watermark 技術の医用画像への適用を検討する。

B. 研究方法:

画像埋込み用のソフトウエアを本研究で開発する。すなわち図1(a)に示すように、送信側で Kitasato の文字を重畳されて(図1(a)では説明のために少しKitasatoの文字を見せて示しているが、実際は完全に重畳されている。)保管・伝送された医用画像は、その著作権が保証される。ちょうど、住民票をコピーした際に、住民票用紙の地模様として『複写』あるいは『無効』などの文字が浮き出るのと同じように、保管施設や受信施設以外でこの医用画像を利用した場合には、 隠された Kitasato の文字を医療画像から抽出でき、不正コピーと断定できる。また、一般画像に医用画像を重畳させた場合(この場合も図1(b)で少し医用画像を見せて示しているが、実際は完全に重畳されている。)には、伝送時に不正進入してこの画像を閲覧しても、一般画像しか閲覧できない。



(a) 著作権保証　　(b) 安全性・秘匿性の確保

図1　Watermark 技術を利用した医用画像の著作権保証、安全性・秘匿性の例

C. 研究結果、D. 考察:

埋込み後の画像の視覚的な劣化が見られないことがまず、必要である。加えて、埋込み前後の画像の容量変化がないことが必要となる。これらによって、医用画像が隠されていることを隠すことができ、秘匿性をうち破る意欲が湧かないと予想できる。これにより、異なる施設間で医用画像の送受信時など、万が一、画像が流出した場合でも医用画像の秘匿性・安全性が確保できると考えられる。

図 2 に Watermark 技術を利用した医用画像の伝送・保管の運用例を示す。画像発生装置(モダリティ)から画像が生成された時点で、著作権を保証できる施設名等を電子透かしとして発生画像に埋め込む。伝送する場合には、別画像に医用画像を埋め込む。これによって著作権の保証、秘匿性の確保が行えると考えられる。

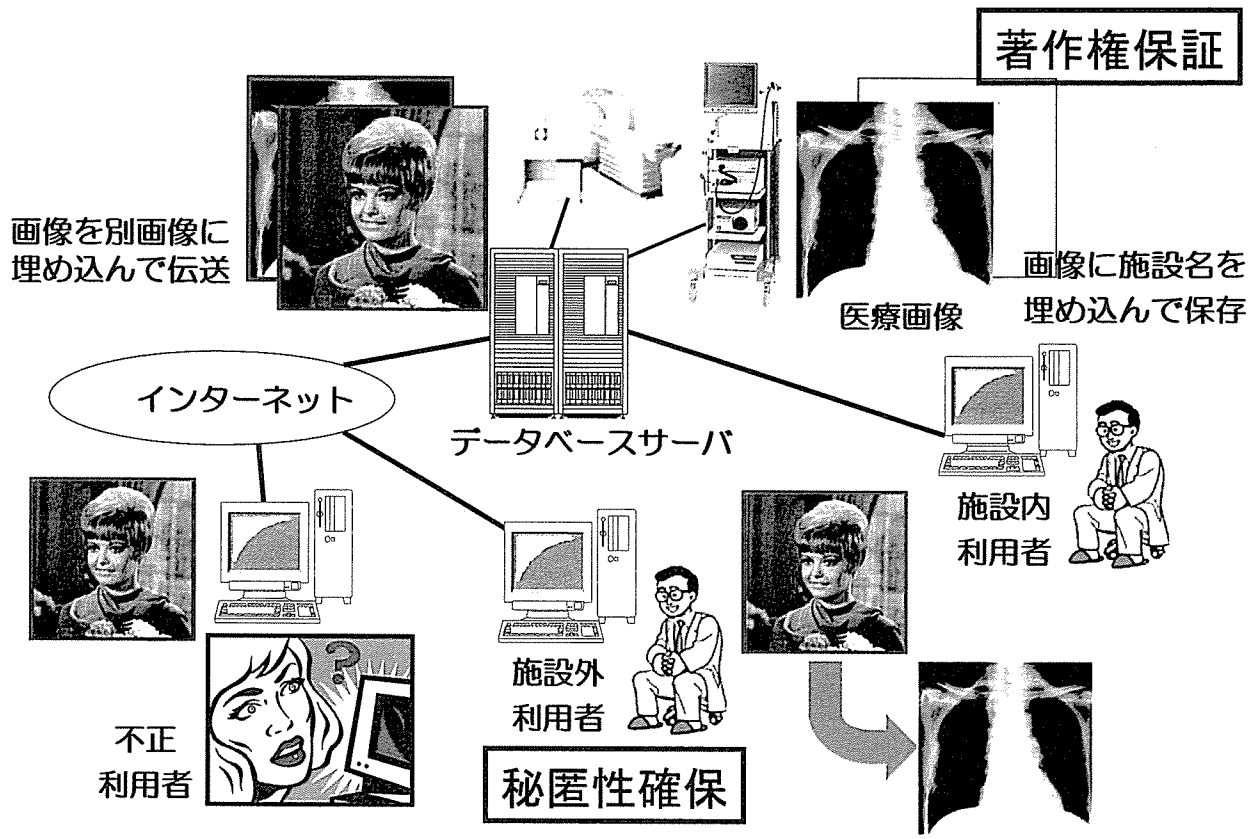


図 2 Watermark 技術を利用した医用画像の伝送・保管の運用例

E. 結論:

Watermark 技術を用いることにより、画像の伝送時の秘匿性の確保、画像保管時の著作権保証が行えると考えられる。

F. 健康危険情報

(分担研究報告書には記入せずに、総括研究報告書にまとめて記入)

G. 研究発表

1. 論文発表

Tachibana H., Omatsu M., Higuchi K. and Umeda T.: Design and development of a secure

DICOM-Network Attached Server:Computer Methods and Programs in Biomedicine 81(3): 197-202 2006

2. 学会発表

(発表誌名巻号・頁・発行年等も記入)

Umeda T., Okawa A., Ikeda T., Yamamoto H. and Harauchi H.:Visit Nursing Station System with Secured Internet Communication using Watermarking Technique : Tele-nursing System Experiments, 14th International Conference on Cancer Nursing, 2006 : 196-197 2006.9.27-10.1(in Toronto)

H. 知的財産権の出願・登録状況

なし

Ⅲ. 研究成果の刊行に関する一覧表

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
小尾高史 他4名	多機能ICチップを利用した任意多地点間VPNのための鍵交換手法	ワイヤレス・テクノロジーパーク2006講演予稿集		20-21	2006
大山永昭	IT新改革戦略における医療の情報化の概要	Japan Medical Society	5月号	53-54	2006
大山永昭	医療機関における個人情報保護とセキュリティシステム	日本病院会雑誌	53巻10号	118-136	2006
押田知己 他5名	多機能IC チップを利用したネットワークサービスにおける暗号技術の更新とサービスの継続利用の実現	電子情報通信学会2007年総合大会講演予稿集		225	2007
浦野雄平 他5名	多機能IC チップを利用した任意多地点間VPN における通信主体情報の秘匿	電子情報通信学会2007年総合大会講演予稿集		230	2007
山本隆一	遠隔画像診断のセキュリティと個人情報保護	Rad Fan	5巻1号	18-19	2006
山本隆一	電子カルテとプライバシー保護	日本医師会雑誌	135巻9号	1954	2006
八幡勝也 他6名	健康管理を支援する情報技術	第26回医療情報学連合大会論文集		150	2006
小林慎治 他5名	医療分野におけるOpen Source Software活用の現状と問題点	医療情報学	26, 5	341-350	2006
Tachibana H., Omatsu M., Higuchi K. and Umeda T.	Design and development of a secure DICOM-Network Attached Server	Computer Methods and Programs in Biomedicine	81, 3	197-202	2006
Umeda T., Okawa A., Ikeda T., Yamamoto H. and Harauchi H.	Visit Nursing Station System with Secured Internet Communication using Watermarking Technique: Tele-nursing System Experments	14th International Conference on Cancer Nursing		196-197	2006

多機能 IC チップを利用した任意多地点間 VPN のための鍵交換手法

New key exchange protocol for the On-Demand VPN using the smart IC chip

○小尾高史　鈴木裕之　谷内田益義　山口雅浩　大山永昭

(Takashi Obi　Hiroyuki Suzuki　Masuyoshi Yachida　Masahiro Yamaguchi　Nagaaki Ohyama)

東京工業大学大学院 (Tokyo Institute of Technology)・

総合理工学研究科 物理情報システム専攻 (Interdischiplinary Graduate School of Science and Engineering , Department of Information Processing)

〒226-8503・横浜市緑区長津田町 4259-G2-2・電話 045-924-5482／FAX 045-924-5482

Yokohama MidorikuNagatsutacho 4259-G2-2 226-8503
E-mail:obi@ip.titech.ac.jp

1. はじめに

近年、インターネットを専用線と同様に利用できる VPN サービスが大きな広がりを見せている。しかし、VPN の構築には利用者にネットワークの専門知識が必要なうえ、設定などを間違うと情報セキュリティ上多大な影響が発生する恐れがあるなど、誰もが容易に設置できる状況に至っていない。このような背景の下、VPN の状態管理を行う VPN 管理機関と 2 階層 PKI に対応した IC チップが搭載された通信機器を用いて、利用者の要求に応じて認証鍵などの VPN 構築に必要な設定情報を、ネットワークを介して安全に配送し[1]、任意多地点間で直ちに VPN を構築するオンデマンド VPN(OD-VPN)技術の研究開発[2]が進められている。

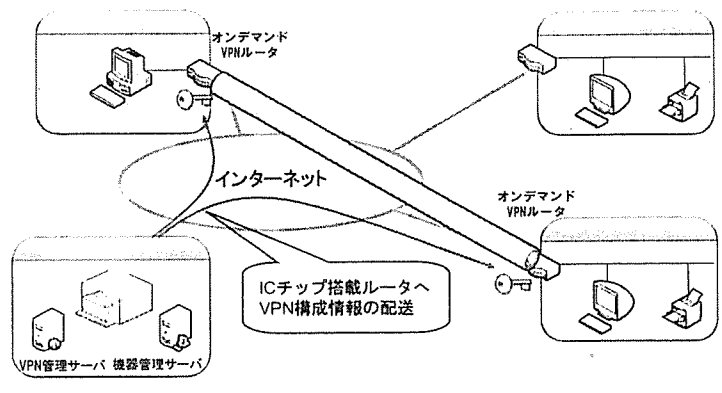


図 1. オンデマンド VPN

現在の OD-VPN（図１）は、IPsec を利用した暗号通信を行っており、そのための鍵交換手法としては、Pre-Shared Key を利用した IKE（Internet Key Exchange）を用いている。しかし、Pre-Shared Key を用いる場合、同じ通信機器においても VPN 通信路毎に異なる鍵を設定する必要があり VPN 管理機関における鍵管理が煩雑になることや、通信機器が異なる VPN 管理機関に属していた場合の鍵生成・情報共有を実現する手法が明確になっていない等の課題がある。本研究では、IKE プロトコルで用いられるデジタル署名認証方式をベースとし、機器に組み込まれた IC チップの利用と属性証明書を用いた接続権限管理とを組み合わせた鍵交換手法を提案する。さらに提案手法を用いて、異なる管理機関に属する機器間で容易に鍵交換が実現できることを示す。

2. 接続許可証を利用したデジタル署名認証ベースのオンデマンド VPN 鍵交換手法

OD-VPN では、ルータ間で IPsec による VPN を構築するために、機器相互の ID や鍵情報などを用いて IPsec-SA を確立する必要があり、現在は、IKE における Pre-Shared Key を利用した鍵交換を採用しているが、このために VPN 通信路毎に異なる鍵が必要となることや、複数の VPN 管理機関間で VPN 通信のローミングサービスを実施する場合の鍵漏洩の危険など、Pre-Shared Key をどのように管理、配送