VPN(virtual private network)を使った仮想専用線で接続され、収集されたACCおよびブロック拠点病院や拠点病院の診療情報は統合的に管理され、治療・研究開発に利用される。その他、国際医療センター研究所における患者検体サンプルの保存状況に関するデータベースであるエイズ研究支援システムや、収集された患者情報等を分析し、患者情報にもとづく最新情報を拠点病院に提供するシステムもある。更に、システムのハードウェアおよびソフトウェアは、業界標準への準拠等、今後のシステムの拡張性を十分に確保されており、また将来的に拠点病院の院内システムとも連携できるように考慮している。したがって、標準化されたオーダエントリーシステムが導入された病院では、このシステムからオーダを出すことが可能になる。

2)A-netのセキュリティ対策

セキュリティを維持する目的から、当初、A-netの通信の基礎となるネットワークは、国立病院・療養所（現独立行政法人国立病院機構）のみで試行開始し、国立病院等総合診療ネットワーク（HOSPnet）を使用した。このHOSPnetは、専用ネットワークであり、いわゆるイントラネットである。さらに、国立病院以外を接続するためインターネットを介したが、その際暗号化等のセキュリティ技術であるVPNを使用した。さらに、運用面でもセキュリティを維持するため、エイズ治療に関わる医療従事者で当システムを利用出来るのは、システム部会が認定したユーザＩＤを持つ人に限ることとした。医療従事者は患者のデータを保護するため、パスワードによる厳密なシステム保護運用を前提としている。登録記録される情報項目は、項目単位にアクセス権限を定義されており、患者情報はその患者の治療に関わった医療従事者のみが参照利用出来る仕組みとしている。その他、部外者からの不正侵入を防御するために、ファイアウォールを設定して、利用は必要性を認めたユーザのみに制限している。

3)A-netの運用

A-netにおける情報ネットワークの最大の意義は情報の共有である。エイズ治療の高度化と前進のために、患者のデータを治療中の病院内にとどめず、データベースとして共有し、診療を受けたことのある過去のすべての病院の情報も併せて参照することにより、経過情報の推移や投薬歴、ウイルス量の治療行為に伴う変遷が体系的に参照することが可能になる。これは一病院一カルテから全国的に一患者一カルテへの道を拓くもので、治療の前進の為には大いに有用と判断されるが、病院カルテが一病院から他の施設へ出て行くとも判断されるので、守秘義務や患者のプライバシー保護の観点から厳正な運用を確保する仕組作りが必要となった。これらの問題に対応する為、運営に関する委員会(システム部会)を設置すると共に、運用管理要綱、管理細則を定め、組織化された管理体制により遵守することとした。そのうえで、適切な説明に基づく説明と同意を取っている。ここでは、エイズ治療に関わる自分の診療記録データをA-netに記録利用する事に患者が同意することを前提とした。診療上発生したデータを有効に活用し患者の治療や研究に役立てるのである。その同意書の概略は、以下のようなものである。

１．患者は自身のエイズ治療に関わる診療経過の中で発生した医学情報を自身及び将来のエイズ患者への治療の向上と発展の為にA-net上のデータベースに記録する事に同意する。

２．A-net上の患者データは、当該患者を診察治療する立場にある病院及び医療従事者に限って利用される。

３．A-net上の他のエイズ診療専門医のコンサルテーションを受ける旨患者が同意した場合、ACC等の専門機関の医師等による当該患者の参照コンサルテーションを実施することが出来る。

４．エイズ治療の向上等の研究における個人が特定されないデータ利用に関し、その利用目的や方法等が適切であるかどうか運営委員会に図り、それが了承された場合、患者は診療のために登録されたデータを利用される事に同意する。

4)データの共有理念

A-netの診療支援電子カルテシステムは個人の診療記録を複数の医療機関で共有することが基本である。これにより、地方の診療機関であっても、ACCと同じ診療レベルの実現が可能になるであろう。さらに、このシステムが有効活用され、蓄積されたデータを統計解析して、新規の診断法や治療法を開発し、予後の改善が図られることが期待されている。しかし、個人名を抜いた程度では、患者が類推されてしまう危険性もあり、プライバシー保護堅持とデータの有効利用（治療開発研究）という相反する面を調整するための運営組織やガイドラインも作成した。このような観点の検討はまだ少なく、他の分野では名前を抜いた程度でデータベース化され、臨床研究が行われている状態である。プライバシー保護とデータの有効利用に関し、さらに検討が必要と考えられた。

さらに、近年急速に顕在化した要求として、患者自身による診療情報管理である。特に、検査データの結果を患者に手渡しすることは、A-netを利用する多くの患者に対し行われており、当初無

かった検査結果印刷仕様を機能追加した。ここ1～2年ではそれを電子情報として受け取りたいという患者が増加している。デジタル情報として受け取ることにより、自身のパソコンに情報を蓄積し、自己管理に用いたいというニーズである。

D. 考察

A-net の診療支援電子カルテシステムは個人の診療記録を複数の医療機関で共有することが基本である。これにより、地方の診療機関であっても、ACC と同じ診療レベルの実現が可能になるであろう。さらに、このシステムが有効活用されるため、蓄積されたデータを統計解析して、新規の診断法や治療法を開発し、予後の改善が図られることが望ましい。しかし、個人名を抜いた程度では、患者が類推されてしまう危険性もあり、プライバシー保護とデータの有効利用による治療開発というトレードオフの点を調整するための運営組織やガイドラインも作成した。しかし、個人情報保護法施行を迎え課題は多く、このような観点の検討はまだ十分ではなく、他の分野では名前を抜いた程度でデータベース化され、臨床研究が行われている状態である。今後、プライバシー保護とデータのアクセス制御、有効利用に関し、さらに検討が必要である。

A-net 運用開始の1998年時点ではインターネットを介してセキュリティを保った状態で施設同士をつなぐ技術である仮想専用線網の研究報告も医療分野においては、ほとんど行われていなかったが、現在ではさらに安全な技術が開発されており、A-net におけるセキュリティ技術水準は過去のものになりつつある。一般に、利便性とセキュリティは相反する性格を持つといわれており、昨年4月施行の「個人情報の保護に関する法律」を踏まえ、プライバシー保護に役立つ最新のセキュリティ技術と臨床現場で利用可能な利便性がいかなるレベルで運用・維持できるかを調査検討した。

まず、診療時での利用に関しては、A-net の電子カルテは、診療機会毎の症状のみならず、治療行為、ウイルス量などの検査結果等いわゆる臨床試験に必要なデータが、1患者1カルテとして、複数の病院を統一してすべて記録されているシステムである。一方、研究など二次利用に関し、他の分野で広く普及している癌登録や脳卒中登録、透析患者登録といった患者登録は、年に一度程度のサマリ情報であり、受診毎のデータなど詳細なデータを集計できている訳ではない。したがってネットワーク型電子カルテを使った臨床研究応用の方策は、病院間の診療連携のみならず多施設診療研究にも応用できると考えられる。近年急速に医療情報の電子化が推進されてきたが、未だ A-net 以外に大規模な臨床データが蓄積されていないのが現状である。それには、いくつかの問題点があると予想されるが、大きく分けて、技術的側面と患者の心理的側面に分けられると考えられる。情報技術の進歩は急速であるが、ハッカーやクラッカーの技術進歩も速く、両者は鼬ごっこの状況であり、情報技術の進歩に伴いながら継続して個人情報保護法を踏まえた技術開発を研究する必要がある。

また、A-net 利用促進を図るための、各病院のオーダリングシステムより A-net への自動取り込みシステムに関する、これらのデータの自動転送のルール作りが肝要であろう。また、鍵のかからない部屋での端末の安全性を担保するためのソフトによるセキュリティ担保と物理的なセキュリティ担保のレベル検討必要と思われる。

さらに、近年インフォームドコンセントが当たり前のこととなり、診療情報の患者への開示が進んできた。その結果、診療は医師任せにするのではなく、患者も治療に参加するという姿勢に変わりつつあるようである。HIV 疾患では特にウイルス量や肝機能などの検査情報が重要とされているが、それらを患者にもデジタル情報として渡して欲しいという要求が生まれてきた。これは、従来の「お任せ医療」から「患者参加型医療」への大きな転換といえる。したがって、今後の医療機関内部における個人情報管理に関する考え方は、医療機関内部のみでなく連携医療機関、さらに患者との情報共有まで考慮した管理モデル構築が望まれる。

E. 結論

A-net におけるセキュリティ確保は、ネットワークのセキュリティ確保以外に医療従事者が患者のデータを保護するため、パスワードによる厳密なシステム保護運用が前提で、登録記録される情報項目は、項目単位にアクセス権限を定義されており、診療時にその患者の治療に関わった医療従事者のみが患者情報を参照利用出来る仕組みとしていた。A-net における情報ネットワークの最大の意義は情報の共有である。エイズ治療に関わる自分の診療記録データを A-net に記録利用する事に患者が同意することを前提としていた。

一方、二次利用に関し、研究用に無名化されたデータを、患者の同意を条件にその利用目的や方法等が適切であるかどうか運営委員会に図った上で利用していた。また、A-net 利用促進を図るためには、病院オーダリングシステムや電子カル

テ等の病院情報システムに集積されている検査データの自動連携が有効であるが、A-net と別メーカのシステムとを接続することは技術的に困難であり、標準化の技術的検討のみでなく、標準技術の実装が望まれる。

インフォームドコンセントが普及し、診療情報の患者への開示が進んだ結果、患者参加型医療に変化している。検査情報を患者にもデジタル情報として渡して欲しいという要求が生まれてきており、今後の医療機関内部における個人情報管理に関する考え方は、医療機関内部のみでなく連携医療機関、さらに患者との情報共有まで考慮した管理モデル構築が望まれる。

F. 健康危険情報

なし。

G. 研究発表

1. 論文発表

秋山昌範：不正行為を調査するデジタル・フォレンジック医療分野における重要性. COMPUTER & NETWORK LAN23(3)：27-32、2005.

H. 知的財産権の出願・登録状況

なし。

厚生労働科学研究費補助金（厚生労働科学特別研究事業）

（分担）研究報告書

# 大学病院における医療情報システム管理に関する検討

## —アンケート調査—

（分担）研究者　石垣武男　名古屋大学教授

研究要旨：医療情報システムの導入は大学病院においても進んでいるが各大学の導入状況およびその管理に関してアンケートによる調査を行い医療情報システム管理に関する検討を行った。病院医療情報システムは大学病院にほとんど設置され電子カルテもかなり普及してきている。その管理運用に関しては個人情報保護法の関係からもより厳しい対応を迫られるわけである。大学病院としての特殊性から臨床研究上患者情報の取得は必要不可欠であるがその対応に関しては早急に全国レベルでの指針を作成する必要がある。

A．研究目的

医療情報システムの導入は大学病院においても進んでいるが各大学の導入状況およびその管理に関してアンケートによる調査を行い医療情報システム管理に関する検討を行った

B．研究方法

全国の医学部付属病院を有する大学を対象に旧国立系大学４２施設および公・私立大学（一部分院も）３８施設の放射線科教授宛にアンケートを依頼した。アンケートの内容は資料①のごとくである。

C．研究結果

アンケートの回答は旧国立系大学４２施設中３５施設、公・私立大学（一部分院も）３８施設中３０施設、合計６５施設から得られた（資料②）。資料③にその集計を示す。

１）医療情報システムの導入状況では病院情報システムはその規模はともかく、旧国立大学病院ではすべて導入されている（図１）。大学病院全体でみてもほとんど導入されている。ＰＡＣＳに関しては旧国立大学病院では８割の施設では導入されており、大学全体でも８割弱に導入されている（図２）。電子カルテになるとまだ導入実数は少なく、旧国立大学病院、公・私立大学ともそれぞれ 11 施設に導入され大学全体で三分の一の導入実績である。しかし、

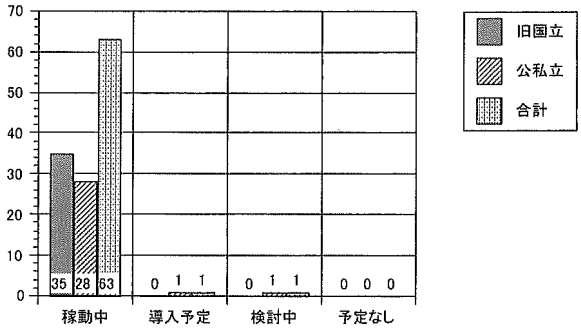


図１．大学病院における HIS 導入の現状

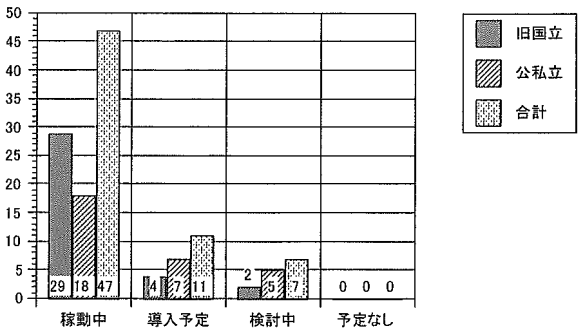


図２．大学病院における PACS 導入の現状

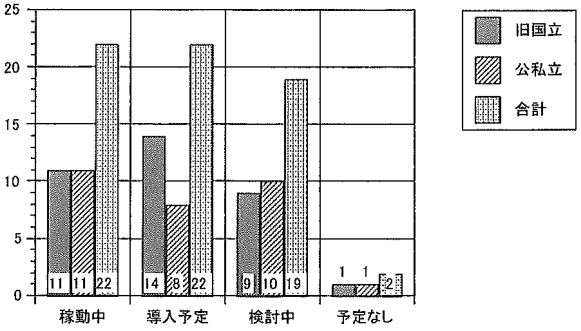


図３．大学病院における電子カルテ導入の現状

近々導入が決定している施設も多く2年以内で3分の2の施設には導入される予定である（図3）。

2）病院情報システム又は電子カルテの管理

システムへのアクセスに関してはパスワード管理が多いが、IDカードとの併用を導入している施設もある（図4）。アクセス方法で「その他」とした11施設中10施設では指紋照合単独もしくはパスワードやIDカードとの併用であった。1施設ではPKI（公開鍵暗号方式によるセキュリティインフラ）方式とICカードとの併用であった。アクセス権の職制別規制はすべての施設で対応していた。

教育上医学部学生のシステムへのアクセスに関しては三分の一の施設で可能としている（図5）。ただし、その内容は様々である。学生用に臨時のIDを発行している施設もあるが学生がシステムを利用できるのは特定の患者に限られている場合がほとんどである。また操作に関しては閲覧のみとするものがほとんどである。

アクセス履歴の記録はほとんどの施設で行われておりIDなどから個人の特定ができる（図6）。

不正アクセス防止策は三分の二の施設で対応しているという回答であったが、その内容は単にアクセス時点でのパスワードによる対応というものから、情報管理室でのログイン状況のチェックと警告など様々であった（図7）。

放置画面に対する対応では半数の施設では一定時間後に自動的にログアウトされるというものであった（図8）。

情報システムのデータが取得できるかどうかについては、可能としているのが8割を超える（図9）。その場合取得に関しての制限を設けている施設もかなりある（図10）。申請方式や管理規定で定めているものが多く病理組織結果は主治医のみに公開という場合もある。データ取得の手段はプリントアウトはもちろん他の記録媒体にコピー可能である（図11）。

外部と情報システムとの接続に関してはほとんどの施設では出来ないが、少数可能と回答した施設がある(図12)。内容はインターネットとの接続しているものであった。

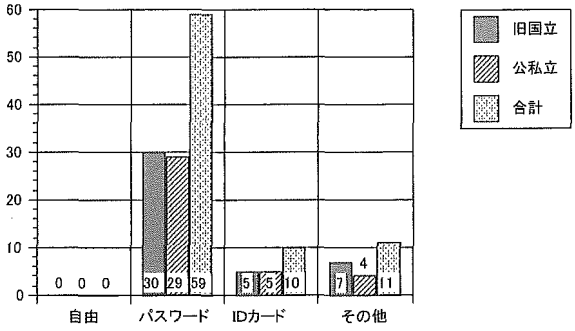


図4．システムへのアクセス方法

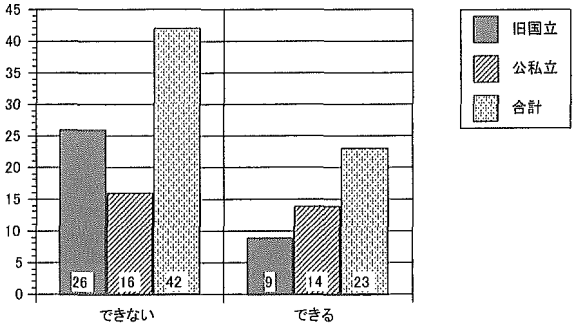


図5．学生のアクセス

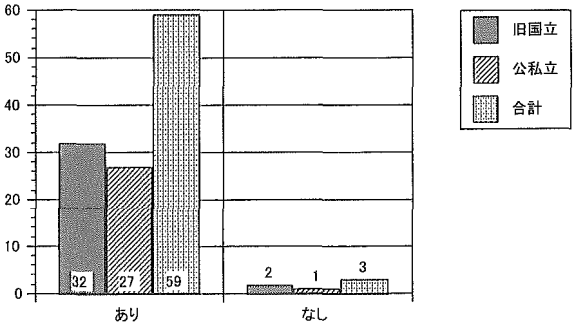


図6．アクセス履歴の記録

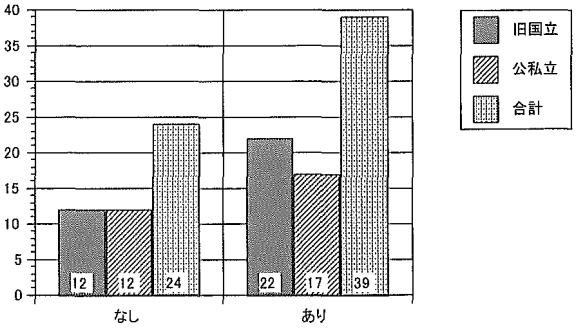


図7．不正アクセスの防止対策

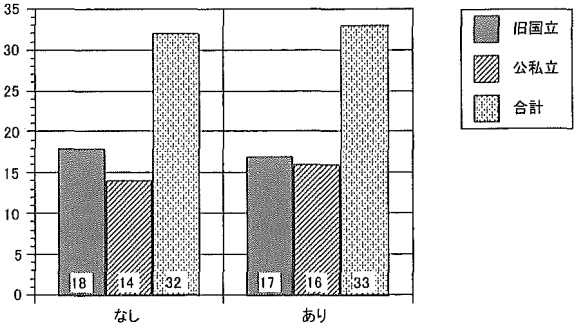


図8．放置画面対策

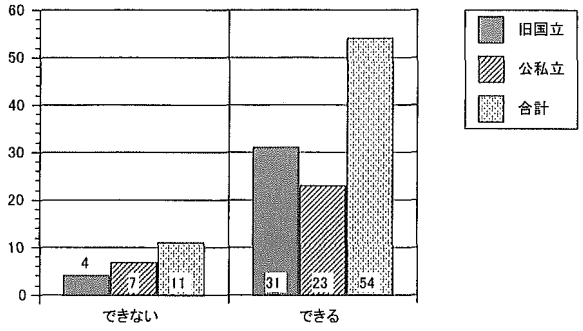


図９．データの取得

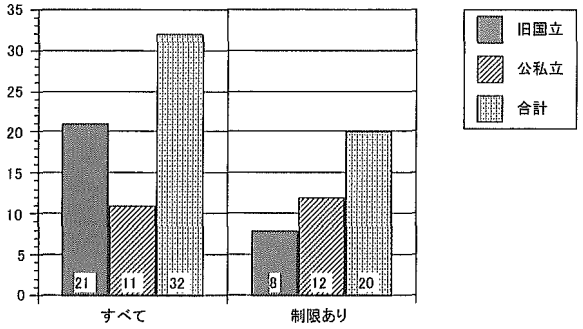


図１０．データの取得範囲

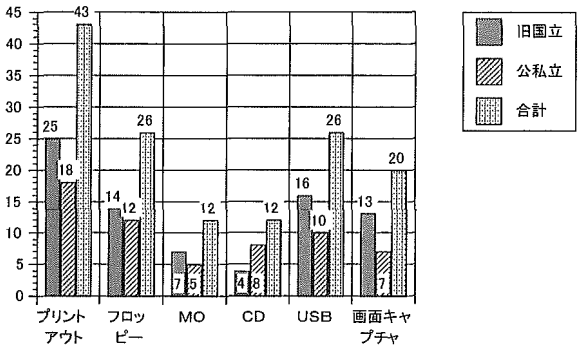


図１１．データの取得手段

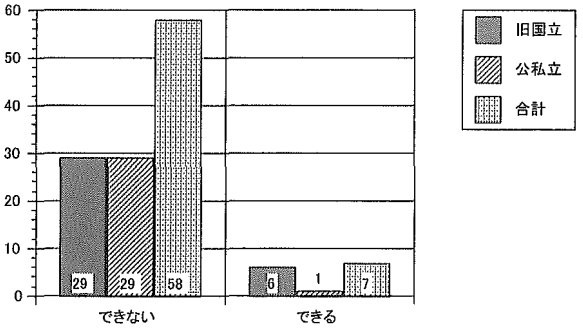


図１２．外部との接続

患者データをシステムから取得できないと臨床研究上影響が大であることに関して記述方式で回答を求めた。施設によっては、医療情報部が公式には許可していないところもあるが、電子データとして取得することに関しては個人情報保護法との関係を重視しつつ何らかの規定（申請式、取得内容履歴の記録、端末限定）を全国的な統一指針として出すのが急務という意見が大半である。これとは別に患者に渡す電子データに関しての指針も必要との意見もあった。

D．考察

電子カルテの導入に関しては厚生労働省が平成13年12月に打ち出した保健医療分野の情報化グランドデザインによると平成18年までに、全診療所の6割以上、全国の400床以上の病院の6割以上に普及させるとした。今回の調査からは大学病院に限ってみるとこの数値目標はなんとか達成されそうである。

電子カルテの運用に関してはその技術的なシステム上の課題と人的運用面での課題があり、病院自体が規定を儲け、情報の漏洩・改ざんなどの防止に努めているところである。電子カルテのセキュリティ対策としては大量のデータをいちどに盗まれるような事態は別として一般的には診療現場レベルにおいて、各論的な問題が生じる危険性が大きい。加えて。大学病院という特殊性から研究・教育面で患者個々のカルテ情報の特定の内容を基礎データとして特定の人間の手元において解析をすることは紙カルテのころから日常茶飯事のことであった。したがって、電子カルテが保有する患者データをプリントアウト、もしくは別の記録媒体に保存して、個人的に利用するということもしごく当然という判断が現況であろう。しかしながら、個人情報保護法の施行された現在医療という特殊な環境下であっても法との関連で対応していく必要がある。従来の紙カルテでは臨床データの整理にあたって紙カルテを大量にカルテ部から借り出して、個人的な管理のもとにデータの取得が行われていることが多かった。この場合、データ整理のために医師以外の第三者がその作業を手伝うといった事例も多くみられ患者情報に対する明らかな守秘義務違反と指摘せざるを得ない状況が発生していた。電子情報になってもこういったずさんな運用がなされるのは許されることではなしのは当然といえる。しかしながら、データをまったく取得することができず、画面から書き写すのみというのでは臨床研究上大いに支障がある。したがってこの問題に関しては早急

に全国レベルでの指針の作成が必要と考えられる。

一方、情報システムからの情報漏えいという点ではアクセス時点での対応がまず必要である。まだ普及はこれからであるが PKI 方式の認証システムの導入が必要であろう。情報システムと外部との接続、すなわちイオンターネットとの接続が可能でる施設が少数ではあるが存在することは、外部からの不正アクセス、データ改ざん、ウィルスによる攻撃などが想定され利便性以上に取り返しのつかない事態が生じる危険もあるので慎重に対処すべきである。

E．結論

病院医療情報システムは大学病院にほとんど設置され電子カルテもかなり普及してきている。その管理運用に関しては個人情報保護法の関係からもより厳しい対応を迫られるわけである。大学病院としての特殊性から臨床研究上患者情報の取得は必要不可欠であるがその対応に関しては早急に全国レベルでの指針を作成する必要がある。

G．研究発表

なし

H．知的財産権の出願・登録状況

なし

# 資料①　アンケート内容

１．貴施設における医療情報システムの現状(該当する箇所に○を付けてください)

A)ＰＡＣＳ　　イ．稼動中　ロ．導入予定（　年）　ハ．検討中　ニ．予定なし

B)病院情報システム　イ．稼動中　ロ．導入予定（　年）　ハ．検討中　ニ．予定なし

C)電子カルテ　　イ．稼動中　ロ．導入予定（　年）　ハ．検討中　ニ．予定なし

２．病院情報システム又は電子カルテについて

Ａ）アクセスの方法

イ．自由　ロ．パスワード入力　ハ．ＩＤカード　ニ．その他（具体に：　　）

Ｂ）アクセス権の職制別規制

イ．あり　ロ．なし

Ｃ）医学部学生のアクセス

イ．できない　　ロ．できる（どのように：　　）

Ｄ）アクセスの履歴の記録（誰？がアクセスしたか）＊複数回答してください

イ．あり　　ロ．なし　ハ．個人が特定できる　ニ．個人までは特定できない

Ｅ）不正アクセス防止策

イ．なし　ロ．あり（具体的に：　　）

Ｆ）放置画面（いわゆるつけっぱなし）への対応

イ．なし　ロ．あり（①一定時間後に自動的にログアウト②その他：　　）

Ｇ）データの取得

イ．できない　ロ．できる

Ｈ）設問Ｇでできると答えた場合その範囲は（医師の場合）

イ．すべて　ロ．制限あり（具体的に：　　）

Ｉ）設問Ｇでできると答えた場合その方法は（複数回答可）

イ．プリントアウト　ロ．フロッピー　ハ．ＭＯ　ニ．ＣＤ　ホ．ＵＳＢ　ヘ．画面キャプチャト．その他（　　）

Ｊ）情報システムと外部との接続

イ．できない　ロ．できる

Ｋ）設問Ｊでできると答えた場合具体的にその方法など記述してください

Ｌ）患者個別の臨床データを紙にせよ電子的にせよ医療情報システムから取得できないとなると臨床研究上影響が大きいと思いますがそれに対してのお考えをお聞かせください。

## 資料② アンケート回答施設

旧国立大学:42中35施設

北海道大学医学部、旭川医科大学医学部、弘前大学医学部、東北大学医学部、秋田大学医学部、山形大学医学部、新潟大学医学部、信州大学医学部、金沢大学医学部、筑波大学医学専門学群、群馬大学医学部、千葉大学医学部、東京大学医学部、東京医科歯科大学医学部、防衛医科大学校、岐阜大学医学部、浜松医科大学医学部、名古屋大学医学部、三重大学医学部、滋賀医科大学医学部、京都大学医学部、大阪大学医学部、神戸大学医学部、鳥取大学医学部、岡山大学医学部、広島大学医学部、山口大学医学部、徳島大学医学部、高知大学医学部、佐賀大学医学部、長崎大学医学部、熊本大学医学部、大分大学医学部、宮崎大学医学部、鹿児島大学医学部

公・私立大学:38施設中31施設

札幌医科大学医学部、岩手医科大学医学部、福島県立医科大学医学部、自治医科大学医学部、埼玉医科大学医学部、日本大学医学部、昭和大学医学部、昭和大学医学部横浜市北部病院、東邦大学医学部、順天堂大学医学部、東京慈恵会医科大学医学部、日本医科大学医学部、慶応義塾大学医学部、東京女子医科大学医学部、東海大学医学部、聖マリアンナ医科大学医学部、横浜市立大学医学部、金沢医科大学医学部、藤田保健衛生大学医学部、愛知医科大学、名古屋市立大学医学部、京都府立医科大学医学部、大阪市立大学医学部、近畿大学医学部、関西医科大学医学部、大阪医科大学医学部、奈良県立医科大学医学部、和歌山県立医科大学医学部、久留米大学医学部、産業医科大学医学部

# 資料③ アンケート結果

| | | 旧国立 | 公私立 | 合計 |
|---|---|---|---|---|
| PACS | イ. 稼動中 | 29 | 18 | 47 |
| | ロ. 導入予定 | 4 | 7 | 11 |
| | ハ. 検討中 | 2 | 5 | 7 |
| | ニ. 予定なし | 0 | 0 | 0 |
| 病院情報システム | イ. 稼動中 | 35 | 28 | 63 |
| | ロ. 導入予定 | 0 | 1 | 1 |
| | ハ. 検討中 | 0 | 1 | 1 |
| | ニ. 予定なし | 0 | 0 | 0 |
| 電子カルテ | イ. 稼動中 | 11 | 11 | 22 |
| | ロ. 導入予定 | 14 | 8 | 22 |
| | ハ. 検討中 | 9 | 10 | 19 |
| | ニ. 予定なし | 1 | 1 | 2 |
| アクセスの方法 | イ. 自由 | 0 | 0 | 0 |
| | ロ. パスワード | 30 | 29 | 59 |
| | ハ. IDカード | 5 | 5 | 10 |
| | ニ. その他 | 7 | 4 | 11 |
| アクセス権の職制別規制 | イ. あり | 35 | 30 | 65 |
| | ロ. なし | 0 | 0 | 0 |
| 医学部学生のアクセス | イ. できない | 26 | 16 | 42 |
| | ロ. できる | 9 | 14 | 23 |
| アクセス履歴の記録 | イ. あり | 32 | 27 | 59 |
| | ロ. なし | 2 | 1 | 3 |
| | ハ. 個人特定できる | 20 | 24 | 44 |
| | ニ. 個人特定できない | 1 | 1 | 2 |
| 不正アクセス防止策 | イ. なし | 12 | 12 | 24 |
| | ロ. あり | 22 | 17 | 39 |
| 放置画面対策 | イ. なし | 18 | 14 | 32 |
| | ロ. あり①自動ログアウト | 17 | 16 | 33 |
| | ロ. あり②その他ト | | | 0 |
| データの取得 | イ. できない | 4 | 7 | 11 |
| | ロ. できる | 31 | 23 | 54 |
| データ取得の範囲 | イ. すべて | 21 | 11 | 32 |
| | ロ. 制限あり | 8 | 12 | 20 |
| データ取得方法 | イ. プリントアウト | 25 | 18 | 43 |
| | ロ. フロッピー | 14 | 12 | 26 |
| | ハ. MO | 7 | 5 | 12 |
| | ニ. CD | 4 | 8 | 12 |
| | ホ. USB | 16 | 10 | 26 |
| | ヘ. 画面キャプチャ | 13 | 7 | 20 |
| | ト. その他 | 1 | | 1 |
| 外部との接続 | イ. できない | 29 | 29 | 58 |
| | ロ. できる | 6 | 1 | 7 |

# 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。本研究では現時点でもっとも容易に実現できる可搬媒体での診療情報提供書や患者への情報提供を実現するにあたっての安全確保の手段として、暗号化および電子署名の標準的な適応方法を確立した。

## 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、この指針はあくまでも医療機関内での医療情報の安全管理を中心に記載されたものであり、施設間の情報交換や患者等の利用者への情報提供に関しては部分的に触れられているにすぎない。本研究の目的は電子化診療情報が医療機関の合理化だけでなく、わが国の医療の質に貢献する使われ方のひとつとして、電子化診療情報提供書と患者への情報提供書をとりあげ、その安全管理の手段として電子署名と暗号化の手法の標準を示すことにある。電子化診療情報提供書は従来の紙ベースの診療情報提供書に比べて格段に大量の情報を提供可能であり、重複検査や重複投薬を防ぐだけでなく、提供元の医療機関で注目されなかったデータを含むことで、病状の変化に伴う新たな関心点に関しても対応可能な情報提供になる可能性があり、適切に運用されれば、連携医療を大きく進展させることができる。また患者等

への情報提供を電子化することによって、客観的な情報をすべて提供することが可能で、提供を受けた個人が適切に管理することができれば生涯健康データベースを構築する基礎となる。政府が 2006 年 1 月に公表した IT 新改革戦略に謳われている生涯健康データベースの実現にも資するものである。

## B．研究方法

電子カルテには様々な情報が格納されるが、その中には記載する医師等が自らの考えを整理するための事項や、病院内での事務処理のための事項、さらには電子カルテシステム自体の運用のための情報も含まれる。本研究が対象としている提供書はこれらの情報を含まない、患者に関する情報のみからなる。紙ベースの場合は記載量の制限から、取捨選別が必要であったが、電子情報では記載量の制限は緩く、多くの場合取捨選抜は必要ない。また医療機関間での情報提供と患者への情報提供の間に、若干の差はあるが、主に情報の受け手の理解力や受容性を考慮したものであり、検体検査、処方履歴、画像検査などの客観的事実はほぼ同じものと考えてよい。そこで、まず可搬媒体を用いた提供書のモデルを検討した。ネットワークではなく可搬媒体をモデルを検討したのは本研究班の全体の成果として期待されるセキュアなネットワークがわが国の基盤として確立するのは本年度中には期待できず、その一方で CD-R や DVD-R などの可搬媒体は安価で書き込みに用いる機器も用意に入手可能であるためである。つぎに責任の所在を明らかにし、改ざんを防止するための電子署名のあり方について考察し、その標準を提案した。さらに可搬媒体へ格納する際の暗号化について標準を提案した。なおこれらの標準案の作成にあたっては日本 HL7 協会の SIG の活動の一部としておこなったが、経費はすべて本研究班の研究補助金を使用し、混同はない。

## C．研究結果

### （1）可搬媒体での提供書モデルの検討。

診療情報提供書や患者等への情報提供書の電子化モデルはこれまで、いくつか試作されている。代表的なものは a.）吉原らが中心となって作成し、現在 MedXML コンソーシアムが保守・管理を行っている MML3.0 に基づくもの、b.）日本医療情報学会が作成した MERIT-9 診療情報提供書 ver. 2、c.）また静岡県で木村らが提案している MERIT-9 診療情報提供書 ver. 3 がある。これらはいずれも事実上の国際標準である HL7 CDA に準拠しているという共通点がある。前 2 者は CDA Release 1 に準拠し、最後の MERIT-9 診療情報提供書 ver 3 は CDA Release 2 に準拠している。これらはいずれの実証実験としての実装例があり、継続的に使用され、有用であることが証明されている。そこでこれらのすべてを本研究の対象とした。これはいずれも HL7 CDA に準拠しているために共通の特徴がある。本文は XML インスタンスであり、放射線画像のような非 XML インスタンスは外部参照ファイルとして結びつけることができる。

### （2）電子署名規格の作成

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、医師等の医療従事者の公的資格を確認可能な電子署名基盤の整備を進めている。診療情報提供書には作成者である医師等の記名押印が求められ、また患者等に提供する情報提供書も責任の所在を明確にし、改ざんのないことを保障するために電子署名を施すことが望ましい。一方で XML インスタンスに対する電子署名は国際的に RFC 3275 として標準案が作成されており、またタイムスタンプを含めた署名技術も W3C で XAdES として提案されている。本研究で行うことはこれらの標準の適応方法を規定し、またこれらで不十分な点があれば追加することである。

まず不十分な点があるか、であるが、RFC3275 や W3C XAdES は基本的には XML インスタンスのみを対象としている。XML インスタンス内に非 XML オブジェクトを埋め込む技術は存在するが、先にあげた診療情報提供書のモデルはいずれば本分である XML インスタンスの外側に外部参照ファイルとして置くことを認めている。さらに診療情報の提供書では放射線画像や検体検査結果などの客観情報の多くは外部ファイルとして格納される可能性が高く、電子署名の影響が外部ファイルに及ばなければならない。前述の提供書モデルはいずれも外部ファイルを URI で指定しているために、URI の指定と同時に外部ファイルのハッシュ値とその計算に用いたハッシュ関数を本文である XML インスタンス内に格納すれば、本文に電子署名を施すことによって、外部ファイルを含めて責任の所在を明確にし、改ざんを検出可能とすることができる。そこで本研究で提案する規格にはこの仕組みを追加した。また XAdES は大きな規格で、署名延長も対応可能となっているが、本研究ではタイムスタンプまで、つまり XAdES-T までの実装を必須とし、多はオプションとした。また前述した厚生労働省が公表した保健医療福祉分野認証局ポシリに準拠した証明書、すなわち ISO 17090 に準拠した HPKI による電子署名を使用可能とし、署名アルゴリズムは RSAEncryptionWithSHA として、SHA は 128 ビットの SHA-1 の脆弱性が問題になっていることから、SHA-2（256 – 512 ビット）も含めた。

**（3）暗号化規格の作成**

医療機関間の診療情報提供書といえども可搬媒体に格納する場合は一時的にせよ患者等が所持することになる。紙ベースの診療情報提供書でも同様で、この場合、管理責任は患者等が所持している間は患者等にある。つまり紛失して中身が他人に見られても本人の責任である。これとアナロジーを考えるなら、可搬媒体の格納された電子化診療情報も患者等が所持している間は患者等に管理責任があることになる。しかし、格納されている情報は大量で、第三者に暴露した場合の危険性について、すべての患者が十分認識していると仮定することが合理的と言い切ることは難しい。可能であれば何らかの防御策を講じておくことが望ましい。解決策として暗号化が考えられるが、暗号化には副作用もある。暗号化された情報は復号できなくなる可能性があり、診療に関わる情報の場合、復号できない、つまり可用性が損なわれることは時には重要な問題になりうる。また暗号アルゴリズムやどのファイルを暗号化するかなどの暗号化

の方法は様々であるが、これらをあらかじめ合わせておかないと復号はできない。また同じアルゴリズムでも鍵の選び方で暗号強度が異なる。一般に暗号強度を上げることは鍵長が大きくなることを意味し、鍵の管理を複雑にする。

対象となる提供書は第三者に見られてもそう大きな問題にならないような内容もありうるし、知られることによって本人に重大な損害を与えかねない情報が含まれる場合もある。

以上のような観点から、本研究で提案した規格は、暗号アルゴリズムを 128 ビットの最大鍵長を持つブロック暗号のうち、ISO 18033 の Part 3 に記載されているものに限定し、また鍵長を 128 ビットまでの任意の長さに設定できるようにした。具体的には鍵のパディングルールを明確にし、例えば 4 桁の数字のような短い鍵長でも利用可能とした。また媒体に格納するファイルの中に、暗号化をおこなったファイルが何かを示す情報ファイルを置くことを義務付け、このファイルを暗号化しないように規定した。

**D．考察**

診療情報の IT 化には目的があり、医療機関によって様々な目的で IT 化を行う。しかし、医療サービスという面から見れば共通の目的もあり、医療の向上につながらなければならない。それゆえに情報が医療機関を超えてもセマンティックに相互運用性があることが重要視される。現状はかならずしも情報学的にセマンティックな相互運用性が確保されているとは言えないが、検体検査や処方、放射線画像などの客観情報の多くはほぼ達成されているといえる。したがってこれらの情報を医療機関を超えて提供または共有することによって実質的な効果を期待できるようになってきたといえる。提供または共有する方法は将来的にはネットワークを介することが理想であるが、基盤整備の状況を考えると当面は可搬媒体を用いることも現実的な解として考慮する必要がある。そしてその際の安全対策も十分に準備する必要がある。

本研究で提案した電子署名と暗号化の 2 つの標準案はこれを満たすことを目指したものである。

電子署名は方法論的には確立されて久しくまた、わが国では制度的にも整備が進んでいる。しかしまだ実際の普及という点では十分とは言えない。これはわが国においては行政手続きと密接に関係した電子署名のみが先行整備されたためで、国民から見ればもともとあまり使われない用途から整備されたためかも知れない。これに対して保健医療福祉分野の公的資格を確認できる HPKI 電子署名はかなり頻繁に生成される診断書や診療情報提供書に用いられるもので、これが整備されることによって初めての広く用いられる電子署名基盤になる可能性がある。

しかし、診療情報提供書で見てもわかるように、署名対象となる文書は単純な構造ではない。診療情報は様々な形式の情報を含む、いわゆるマルチメディア情報であり、電子署名もそのことに十分配慮したものである必要がある。本研究で提案した規格はマルチメディア外部ファイルを URI およびファイル自体のハッシュ値および計算に用いたハッシュ関数を基本情報である XML インスタンス中に埋め込むことで、形式的

には単純な XML 署名でありながら、複数のファイルからなるマルチメディア情報全体に電子署名の効果である責任の所在の明確化と改ざんの検出可能性を及ぼすものである。添付の規格書でわかるように対象をHL7 CDA に準拠した文書全体とし、外部ファイルの扱いは CDA の Release 1 と Release 2 で使い分けている。Release 1 では外部ファイルの参照に拡張を許しているために、Local Markup としてハッシュ値およびハッシュ関数種別を含む XML エレメントを定義することができる。しかし Release 2 は External Act として定義されるために独自の拡張は使うべきではない。そこで、HL7 RIM で定義済みで、ハッシュ値およびハッシュ関数種別を格納可能な ED (Encapsulated Data)データタイプの使用を必須とした。本来の CDA Release 2 では External Act では ED データタイプの属性はオプショナルではあるが、必須とすることで実装上の問題は生じない。

また暗号化は暗号強度の最大値を現時点で一般に利用されるブロック暗号の十分なものとし、その上で鍵長を短くして運用する場合のパディングルールを定義した。短い鍵長で運用することは暗号強度を下げることになるが、結果の項で述べたように、診療情報の提供書は常に高度な機密性を必要とするわけではない。ノートＰＣや携帯電話のプライバシーシートのような、他者からは見えにくい程度でよい場合もある。その一方で暗号強度を上げれば鍵の管理等の運用面での対策もそれなりに強化する必要があり、患者にも医療機関にも負担が増加する。例えば社会的差別につながるような疾患に関する情報が含まれるといった場合は運用上の負荷が高くても鍵長を最長で類推困難なものとし暗号強度を上げなければならない場合もあるだろう。逆にほとんど機密性が必要ない場合もあり、このような場合は電車の中で置き忘れた場合でも PC に挿入するだけで、すべての情報がすぐに見えることはない、程度で十分である。例えば誕生日を鍵にした４桁の数字でもことたりる。このような大きな差のある状況でも本研究で提案した規格は容易に対応することができるし実装の一通りでよい。

なお本規格の作成段階で、最終案とほぼ同じ内容で実証実験をおこなった。この実験は本研究費ではなく、経済産業省の補助事業である相互運用性実証事業の一環として医療情報システム開発センターが主体となって、高岡公立病院を中心に複数の医療機関と 10 数名の患者さんの協力でおこなったもので、電子署名、暗号化ともに実装が可能で十分効果があることが確認できた。

## E．結論

診療情報の IT 化の効果が現れやすい医療機関間の診療情報提供書および患者等への情報提供を対象に可搬媒体を利用する場合の電子署名と暗号化の標準規格を作成し提案した。本研究の成果は日本 HL7 協会の規格として採用され、また HELICS 標準に申請している。

## F．健康危険情報

特になし。

## G．発表

論文

１．山本隆一、海外の医療現場での個人情報保護の動き、INR インターナショナルナーシングレビュー、28 (5)、42-45、日本看護協会出版会、東京、2005

２．山本隆一、診療情報システムと個人情報保護、医学のあゆみ、215 (4)、231-234、医歯薬出版株式会社、東京、2005
３．山本隆一、プライバシーの考え方と個人情報保護、看護展望、30 (5)、17-20、メヂカルフレンド社、東京、2005
４．山本隆一、医療における個人情報保護とセキュリティ、日本病院会雑誌、52 (1)、106-124、(社) 日本病院会、東京、2005

**H．知的財産権の登録・出願状況**

現在のところなし。

**I．謝辞**

本研究の成果は日本 HL7 協会の CDA 作業班ならびに医療情報システム開発センターの多大な貢献による。深謝したい。

付録 1


# CDA 文書電子署名規格

ver. 1.01

日本 HL7 協会

目次

## まえがき

昨今、患者あるいは家族から診療の把握、あるいはセカンドオピニオンを得たいという要求が高まってきている。また、医療・介護機関の機能分化と施設間連携を高度化し、医療・介護の率向上が求められている。このような要求を満たすためには、医療・介護機関間および医療・介護機関と患者・利用者の間で流通する情報を電子化し、情報の密度や可用性を飛躍的に向上させることが有用よ考えられている。そしてこのような電子化文書の規格としてHL7 CDAが存在する。

医療・介護は様々な法律規則に則って行われるもので、さまざまな理由で作成される文書には作成者・責任者の署名または記名・押印が求められるものが存在する。電子化文書では電子署名法によって電子署名で署名または記名・押印に代えることができるが、本規格はCDA文書に電子署名を行い際の規格を記述するものである。また診療文書には添付情報が存在するものが数多くあり、電子署名の対象情報にこれらの添付情報を含めることがもとめられることも多い。そのため、本規格には外部参照情報も電子署名の対象とする場合についても規定する。

なお、本規格の目標は、以下のとおりである。

(1) 患者ケア情報の提供に重点をおく
(2) システムを低コストで実現できるようにする
(3) 記述された情報は、再利用の可能性があるものとする
(4) さまざまなドキュメント生成アプリケーションで互換性をもつようにする
(5) その文書の転送方式や格納のメカニズムとは独立である
(6) すみやかに設計書を提供する
(7) オープンな標準を使う

## 1. 適用

本規格は、さまざまな目的で作成される CDA 文書に電子署名を付与する際に適用する。電子署名が必要か否かは本規格では規定しない。

## 2. 引用規格

本規格は、以下の規格を引用する。日付の付いた引用規格については、その日付以降に発行された修正票または改訂版は参照しない。しかしながら、本仕様書を使用する場合は、各規格の最新版を調べて必要に応じて適用するよう努めなければならない。

RFC3275　XML-Signature Syntax and Processing

保健医療福祉分野 PKI 認証局 証明書ポリシ(厚生労働省　平成 17 年)

ISO TS17090-1:2002 Health informatics -- Public key infrastructure -- Part 1: Framework and overview

ISO/TS 17090-2:2002 Health informatics -- Public key infrastructure -- Part 2: Certificate profile

ISO/TS 17090-3:2002 Health informatics -- Public key infrastructure -- Part 3: Policy management of certification authority

「タイムスタンプビジネスに係る指針—ネットワークの安心な利用と電子データの安全な長期保存のために—」(総務省、平成 16 年)

RFC3161　Internet X.509 Public Key Infrastructure Time-Stamp Protocol

XML Advanced Electronic Signatures (XAdES), (W3C 2003)

患者診療情報提供書規格　V1.00　(日本 HL7 協会　2006)

CDA 文書暗号化規格　V1.00　(日本 HL7 協会　2006)

## 3. 用語と定義

### 3.1 XML 電子署名

RFC3275 に規定される XML 文書に添付して文書作成者の身元を証明し、またその文書が改竄されていないことを保証するデータ。XML 文書全体ではなくその一部にだけ署名を付けたり、また XML 文書の中に署名を含めたりといったことができる。

### 3.2 タイムスタンプサービス

データがある時刻に存在していたことを証明するサービス。データの作成者はタイムスタンプサービスを提供している第三者機関に依頼し、データの内容と現在時刻から作られたハッシュ値を用いるなどして電子署名を発行してもらう。データの受信者はその署