200634076A

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

公開鍵基盤技術を活用した診療情報共有における個人情報保護と情報セキュリティに関する研究

平成１８年度　総括研究報告書

主任研究者　山本　隆一

平成１９（２００７）年４月

目　　次

Ⅰ．　総括研究報告書

公開鍵基盤技術を活用した診療情報共有における

個人情報保護と情報セキュリティに関する研究　－－－－－－－－　1

山本　隆一

Ⅱ．　分担研究報告書

厚生労働省ＨＰＫＩ認証局に関する研究　－－－－－－－－　9

喜多　紘一

公開鍵基盤技術を活用した診療情報共有における

個人情報保護と情報　－－－－－－－－－　１２

大江　和彦

Ⅲ．　研究成果の刊行に関する一覧表　－－－－－－－－－－－　１６

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

公開鍵基盤技術を活用した診療情報共有における個人情報保護と情報セキュリティに関する研究　総括研究報告書

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　保健医療福祉分野認証局ポリシが公表され、厚生労働省として HPKI の実現に向けて動き出し、高度の信頼性と安全性の元に診療情報が交換することが可能になりつつある。しかし、一方で医療における個人情報保護や医療機関内の医療情報システムの安全管理の重要性も増している。本研究で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。

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
喜多　紘一　　東京工業大学　像情報研究施設　ＩＴ都市創造工学　特任教授
矢野　一博　　日本医師会総合政策研究機構　主任研究員
田中　勝弥　　東京大学医学部附属病院企画情報運営部　助手

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。

また昨年度試作した HPKI ライブラリをより実用に耐えるものとするために、XML 署名に完全に対応し、若干の改良を加えた。

C．研究結果

C-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。

C-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。

C-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。

C－4　HPKI ライブラリの改良

昨年度作成した HPKI ライブラリを XML 署名に完全に対応し、若干の改良を施したのでＣＤ－ＲＯＭで添付する。

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

雑誌

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。

厚生労働科学研究費補助金（医療技術評価総合研究事業）

分担研究報告書

厚生労働省ＨＰＫＩ認証局に関する研究

分担研究者　喜多紘一　東京工業大学　像情報工学研究施設　特任教授

研究要旨　厚生労働省で設置したＨＰＫＩルート認証局が稼動を始めた。その経緯をまとめるとともに、ＨＰＫＩ専門化会議が個別認証局を審査し、ルート認証局からＣＡ証明書を発行する際の監査報告書についてふれた。さらに、基盤運用にあたりＨＰＫＩポータルサイトの必要性、ＨＰＫＩ証明書利用促進およびＨＰＫＩ証明書の検証について考察をおこなった。今後、ＨＰＫＩ証明書の普及の為には施設間での診療情報の授受や電子申請の場面に活用し、便利さを体験していくべきである。その為の電子署名やタイムスタンプのＧＵＩやワークフローも検討すべきである。

A．研究目的

平成 17 年 3 月には「保健医療福祉分野 PKI 認証局証明書ポリシ」（以下共通ポリシ）が策定され、HPKI の共通基盤の一部が整備された。平成 18 年度には、これらの基盤の一層の充実を目的として、厚生労働省は個別認証局が共通ポリシに準拠した形で電子署名を発行することが可能となるよう、厚生労働省に HPKI 認証局（ルート認証局）を構築し、個別の HPKI 認証局に対して、共通ポリシへの準拠を示すＣＡ証明書を発行する事業をおこなった。

本研究ではこの動向を踏まえ、HPKI 認証局の今後の進め方をまとめることを目的とする。

B．研究方法

平成１８年３月３０日に開催された「保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議」（以降ＨＰＫＩ専門家会議）において配布された資料およびその後の動きを踏まえて考察する。

C．研究結果

１．厚生労働省HPKI 認証局の構築・運営事業

ＨＰＫＩ専門家会議の配布資料、「厚生労働省HPKI 認証局の構築・運営事業について（案）」を以下に転載し、事業内容を説明する。

１．１ 趣旨

ネットワーク上の情報の改ざん、なりすまし等を防止するために、医師等の個人が電子署名を活用できるよう、公的資格等の確認機能を有する保健医療福祉分野の公開鍵基盤（ヘルスケアPKI：HPKI）が整備される必要がある。既に平成17 年3 月には「保健医療福祉分野PKI 認証局証明書ポリシ（以下、共通ポリシ）」が策定され、HPKI の共通基盤の一部が整備された。平成18 年度には、これらの基盤の一層の充実を目的として、個別認証局が共通ポリシに準拠した形で電子署名を発行することが可能となるよう、厚生労働省にHPKI 認証局（仮称）を構築し、個別のHPKI 認証局に対して、共通ポリシへの準拠を示す証明書を発行する事業を開始する。

２．２ 事業の概要

① 平成18 年度に共通ポリシに準拠した「厚生労働省HPKI 認証局（以下、厚労省HPKI CA）」を構築する。

② 「保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議」（専門家会議）は本事業の実施にあたり専門的な見地から意見、助言を行う。

③ 厚労省HPKI CA は共通ポリシに準拠した個別認証局あるいはその中間認証局に対し、相互認証を可能とする仕組みを提供する。

④ その他に厚労省HPKI CA は、自身の公開鍵証明書、CRL/ARL、CP/CPS 等の文書を公開する。

厚労省HPKI CA を介して個別認証局が相互認証するにあたっては、あらかじめ共通ポリシへの準拠について書面・実地調査等により確認する。当該調査は、専門家会議の要請に基づき、専門作業班が主体となって行う。専門家会議は専門作業班の報告に基づき、準拠性の確認を行い、厚生労働省ホームページに公表する。

１．３ 実施スケジュール

① 平成18 年度は実証フェーズとし、個別認証局の共通ポリシ準拠性の審査手続及び厚労省HPKI CA による認証業務についてのフィージビリティ検証を主な目標とする。

② 平成18 年度前半に「共通ポリシ」「準拠性監査報告書様式」に基づく準拠性の審査手続を検証し、個別認証局に対する一般的な審査手続規則の策定を目指す。

③ 平成18 年度後半に、厚労省HPKI CA の個別認証局に対する認証業務について検証し、共通ポリシへの準拠を示す証明書の発行が可能となることを目指す。

④ 平成19 年度は運用フェーズとし、厚労省HPKI CA 構築・運営事業に参画することを希望する個別認証局からの専門家会議に対する審査申請の受け付け開始を目指す。専門家会議により準拠性が確認された場合、HPKI 個別認証局として本事業に参画する。

１．４ 実施体制

平成18 年度当初の実証フェーズにおける個別認証局として、日本医師会CA、MEDIS CA への協力を依頼する。

１．５ 留意点

・ 本事業に参画する個別認証局は独自事業として認証局の運営を行うものとする。また電子署名法の定める認定認証事業者であることは要件としない。

・ 専門家会議による確認は、個別認証局が共通ポリシに準拠し本事業に参画していることを表示する以外に、何らの権利義務等を生じせしめない。

・ 認証業務上の責任については、共通ポリシ「9.7 無保証」、「9.8 責任制限」、「9.9 補償」に従い、個別認証局が負う。

・ 厚労省HPKI CA のCP/CPS を策定する際には、厚生労働省の法的な責任範囲等についても留意しつつ検討を進める。

・ 平成18 年度の本事業に係る予算は、厚生労働省が担当するHPKI CA の構築及び専門家会議による個別認証局の準拠性審査に係る経費である。

２．共通ポリシーについて

厚生労働省の発行した共通ポリシに関しても、同配布資料に判りやすく説明してあるので転載する。

２．１ 共通ポリシの特徴

共通ポリシに則って発行された電子証明書内には、保健医療福祉分野の国家資格（医師、歯科医師等）と医療施設等の管理者の属性を格納できる。

通常の電子証明書では、そこから読み取れる情報は、氏名・住所・年齢等の個人に関する情報に限られているが、共通ポリシでは資格専用の領域を確保して、そこに国家資格等の属性を格納するようにした。

この専用の領域を「hcRole」と呼び、国際標準化機構（ISO：International Organization for Standardization）の技術委員会（TC）215／WG4 にて協議されており、hcRole を含む規格名「ISO TS 17090」は、2005 年中に正式な国際標準規格（ＩＳ）となる予定。

２．２ 保健医療福祉分野PKI 認証局として共通ポリシを定めることの意義

共通ポリシに準拠した認証局が発行した電子証明書による電子署名であれば、どの認証局が発行した電子証明書による電子署名であっても、その有効性を確認（検証という）することが可能。

このような基盤が整備された場合、医師等の作成する電子的な医療関係書類に署名が付されていれば、その書類を受け取った医療従事者や患者等は、日本全国で有効性の検証が可能。また、保健医療福祉分野の資格保持者が作成した書類であるということも直接確認できるようになる。

信頼できる電子情報を取り扱えることから、医療分野における電子紹介状や電子カルテなど様々な具体的な用途への展開が考えられる。

３．証明書ポリシ準拠性監査報告書様式

同会議で配布された中に「証明書ポリシ準拠性監査報告書様式」がある。これは、個別認証局が共通ポリシへ準拠しているかの「準拠性審査」を受ける際に、個別認証局側で自己監査結果を報告するための様式である。

「共通ポリシ（証明書ポリシ）」に対する「措置状況」を「監査目標」に従って監査し厚生労働省に報告する。

通常２段階の提出になる。一段階目は個別認証局のキーセレモニー前の段階で、認証局の名称が過去に審査した

認証局とだぶりがないか、あるいはポリシに問題ないかをチェックし、問題なければＣＡ証明書を発行する。２段階目は個別認証局が証明書を発行後の稼働状況を監査して報告を受ける段階である。その２段階の報告の結果をＨＰＫＩ専門員会で確認し、問題なければ共通ポリシに準拠していることを公表する。これによりＣＡ証明書が正式なものとなるので、ＨＰＫＩ証明書利用者は厚生省ルートを信頼点として証明書の正当性を確認することができる。

４．ＨＰＫＩルート認証局の稼動

以上のべた趣旨に基づき、平成１９年２月に厚生労働省のＨＰＫＩルート認証局のキーセレモニーが行われ、３月に(財)医療情報システム開発センター（MEDIS-DC）に対してＣＡ証明書が発行された。

これにより、MEDIS-DC では医師等公的資格保有者に対して公開鍵証明書を出せるようになり日本において新たなステップが始まった。

Ｄ．考察

１．ＨＰＫＩポータルサイト

今後の運用のために厚生労働省ではＨＰＫＩ用のポータルサイトを公開していく予定にしている。

このサイトではＨＰＫＩルート証明書のフィンガープリントの公開やダウンロードを計画している。

また、普及の為の個別認証局の情報、ＨＰＫＩ証明書検証の為のサンプルプログラムの提供等が期待される。

２．ＨＰＫＩ証明書の利用

ＨＰＫＩ証明書の利用として、施設間の診療情報の提供と電子申請に分かれる。

前者はオンライン請求システムの医療機関の認証に積極的に導入すべきである。また健診データを健康指導の際に他施設で利用する場合の真正性の確保に有効であるので特定健診の保存の実施時をにらんで浸透を図るべきである。さらに、「地域医療情報連携システム」において複数の施設がかかわる場合にその記録の責任の所在確認に有効である。例えば経済産業省で進めている「地域医療連携システムの標準化および実証事業」での脳卒中連携医療あるいは周産期医療を例に電子署名の導入例を示していくべきである。

後者に関しては、労災での給付の例で社労士と連携して電子申請するシステムを推進してはいかがであろう。

また、医療保険の給付において診断書が必要になる。現在、退院後に申請を行っているのが通常であるが、電子化することにより迅速に給付を受けることが可能になり、場合によっては入院した時点で支給額が決定されている保険もあるので、入院中に申請可能である。こうした診断書の分野を開拓して普及を図るべきである。

３．ＨＰＫＩ証明書の検証

公開鍵証明書の検証はＣＡ局署名のチェック、証明書の有効期間、失効リストによる非該当のチェックおよび、証明書パスのチェックが通常である。

ＨＰＫＩではさらに、発行局のＣＮ名称のチェック、ＯＩＤのチェック、hcRoleのチェックおよび管理責任者の場合は組織名称の読取が追加される。

こうしたソフトウエアは個々に作成すると抜けが出るのでサンプルプログラムが提供されることが望ましい。

検証に関しては利用者に対して安心感を与えるＧＵＩも必要でこれからの課題である。

Ｅ．結論

2007年は厚生省ルート認証局が稼動を始め、医療の電子化として歴史的な一瞬である。産声をあげた出生の一瞬である。アダムとイブの誕生に匹敵する時期である。今後、これを育てる為には組織的な動きと伝道者のような強力なリーダシップが必要である。

考察でふれたように施設間での診療情報の授受や電子申請の場面を活用して便利さを体験していくべきである。

その為の電子署名やタイムスタンプのＧＵＩやワークフローも検討すべきである。

Ｆ．参考文献

１） 保健医療福祉分野PKI 認証局 証明書ポリシ，平成18 年3 月，厚生労働省，2006

２） 厚生労働省HPKI 認証局の構築・運営事業について（案），平成18 年3 月，厚生労働省，2006

３）保健医療福祉分野PKI 認証局 証明書ポリシ準拠性監査報告書様式，平成18 年3 月，厚生労働省，2006

平成 18 年度厚生労働科学研究補助金(医療安全・医療技術評価総合研究事業)分担研究報告書

公開鍵基盤技術を活用した診療情報共有における個人情報保護と情報

分担研究者
大江和彦　東京大学大学院医学系研究科・医療情報経済学分野・教授

研究要旨
電子カルテシステムにおける診療情報管理と共有・利活用では個人情報保護に配慮した安全な情報共有が必須である。そのためには、これらのシステムに必要とされる機能をモデル化し達成すべき目標と機能の具備用件について把握できることが重要である。本分担研究では、同システムに必要となる機能を分析し可視化することを目的とした。可視化にあたっては、溝口らによるオントロジー構築ツール「法造」を使用した。法造を使用して、機能単位をクラスとして記述し、その機能を構成する必須の機能要素を PartOf (p/o)として記述した。また、各機能クラス間の上限関係は is-a 関係を表す super-sub リンクを用いて表現した。オントロジー構築ツールを使用して、電子カルテシステムが備えるべき情報保護およびセキュリティ関連機能の分析と可視化を試みた。電子カルテ機能をこのような方法で可視化することは、機能と情報との関係、機能と機能との関係を把握する上で極めて有効であると考えられた。

A. 目的

オーダリングシステムを中核とした病院情報システムや電子カルテシステムにおける診療情報管理と共有・利活用では個人情報保護に配慮した安全な情報共有が必須である。そのためには、これらのシステムに必要とされる機能をモデル化し達成すべき目標と機能の具備用件について把握できることが重要である。本分担研究では、同システムに必要となる機能を分析し可視化する。

B. 研究の方法

平成15－16年度に分担研究者により実施された「標準的電子カルテに要求される基本機能の情報モデルの開発(H15－医療－046)」の研究成果のひとつであるユーザ視点から見たシステム機能リストから、本研究課題に直接関連する個人情報保護とセキュリティーに関連する機能項目をとりあげ、保護すべき対象、保護を実現するための行為、行為の補助手段などについて分析を行い可視化する。

可視化にあたっては、溝口らによるオントロジー構築ツール「法造」を使用した。法造を使用して、機能単位をクラスとして記述し、その機能を構成する必須の機能要素をPartOf (p/o)として記述した。また、各機能クラス間の上限関係は is-a 関係を表す super-sub リンクを用いて表現した。Super-sub リンクで結合される2つのクラス間では、上位クラスの p/o 要素のうちひとつ以上の要素について、その要素が下位クラスではより限定的(制約が強い)になるように記述した。

C. 結果

電子カルテシステムにおける個人情報保護とセキュリティーに関連する機能としては、

1) ユーザ認証機能
2) 情報操作権限適用・管理機能
3) 情報操作ログ記録・管理機能
4) 真正性確保機能
5) 個人識別情報削除機能
6) データ暗号化出力機能

の6つがあげられると考えられた。

1)ユーザ認証

ユーザ認証は情報システムを利用しようとするユーザを特定し、情報システムにアクセスすることが許可されているかをチェックし、許可されていれば利用可能状態とする一連の機能である。システムにアクセスする権限があるかどうかをチェックして了承するプロセスはログインプロセスと呼ばれる。図1はユーザ識別情報(顔や指紋などの生体情報、カードなどの物理メディアに記録された情報、ユーザ自身の記憶によるIDやパスワード)とあらかじめシステムが保持するユーザに関する情報とを照合することがユーザを特定する機能であることを示している。

2) 情報操作権限適用機能は、図2のようにモデル化できる。ログインプロセスは現在ユーザが確定しない状態での操作権限チェックのひとつであるとここではみなしている。患者にとって、HIVなど通常の診療情報よりは秘匿性を高めたい情報(センシティブ情報)の出力にはそれ専用の権限があるかをチェックする必要である。

この他、医学部学生やコメディカルなど実習生に対するアクセス制限機能は通常の利用者権限チェック機能とは別に用意される必要がある。

3)情報操作ログ記録・管理機能は、電子カルテシステムのすべての操作機能に対して、その実施日時、実施時利用者、実施場所、実施端末、操作対象情報種別に関するデータを統一的なフォーマットで記録し、あとで分析可能とするものである。機能的には単純であるが、実装のためには、システム全体のパーフォーマンス、ログ格納のための記憶領域確保、保存期間、具体的な解析方法など課題は多い。また患者へのアクセスログ開示の機能をどのように提供するかについても検討課題がある。

4)真正性確保機能は、下図(図3)のような機能要素から構成されると考えられる。ここでMDはメッセージダイジェストである。署名は、現在の利用者が誰であるかを同定することがもっとも重要であることと、現在の利用者が本来その記録を署名保存すべき運用上正当な利用者であるかどうかが重要である。運用上正当な利用者の存在は、たとえば研修医が指導医の監督下でしか認められていない医療行為を記録する場合には、記録し署名保存するのは研修医であるが、運用上正当な利用者は指導医であるので、指導医の署名保存も必要であるといった場合を想定している。こうしたケースは実習者が診療記録を代行記載する場合などにも発生する。

5)個人識別情報削除機能は、患者の氏名や住所などの情報を必要としない利用場面において、データのダウンロードやデータ表示・出力時にそれらの情報を削除する機能である。利用ケースとしては、臨床研究、学会発表等や専門医認定申請の資料作成、システムのデモなどが想定される。6)データ暗号化出力機能は、個人識別情報を含んだままデータを外部出力する必要がある場合に使用されるものである。

D. 考察

電子カルテシステムにおける個人情報保護、セキュリティーに関連する機能の分析と理解のために、法造のようなオントロジー構築ツールを使用することはきわめて有効である。ただ、電子カルテ機能の多くがどの取り扱うデータの性質と密接に関連するとともに、使用されるデバイスの機能とも密接に関連する。またその機能が何を実現するために用意されている機能であるかという情報(実現目標)と直結しているので、これらの関係をオントロジーとして記述することは、今後の検討が必要である。

E. 結論

オントロジー構築ツールを使用して、電子カルテシステムが備えるべき情報保護およびセキュリティ関連機能の分析と可視化を試みた。電子カルテ機能をこのような方法で可視化することは、機能と情報との関係、機能と機能との関係を把握する上で極めて有効であると考えられた。

F.研究発表

Yuki Sumita, Mami Takataa, Keiju Ishitsukab, Yasuyuki Tominaga and Kazuhiko OHE: Building a reference functional model for EHR systems. International Journal of Medical Informatics,URL:http://dx.doi.org/10.1016/j.ijmedinf.2006.06.008、2006(Epub Ahead)

G.知的所有権の取得状況

該当なし

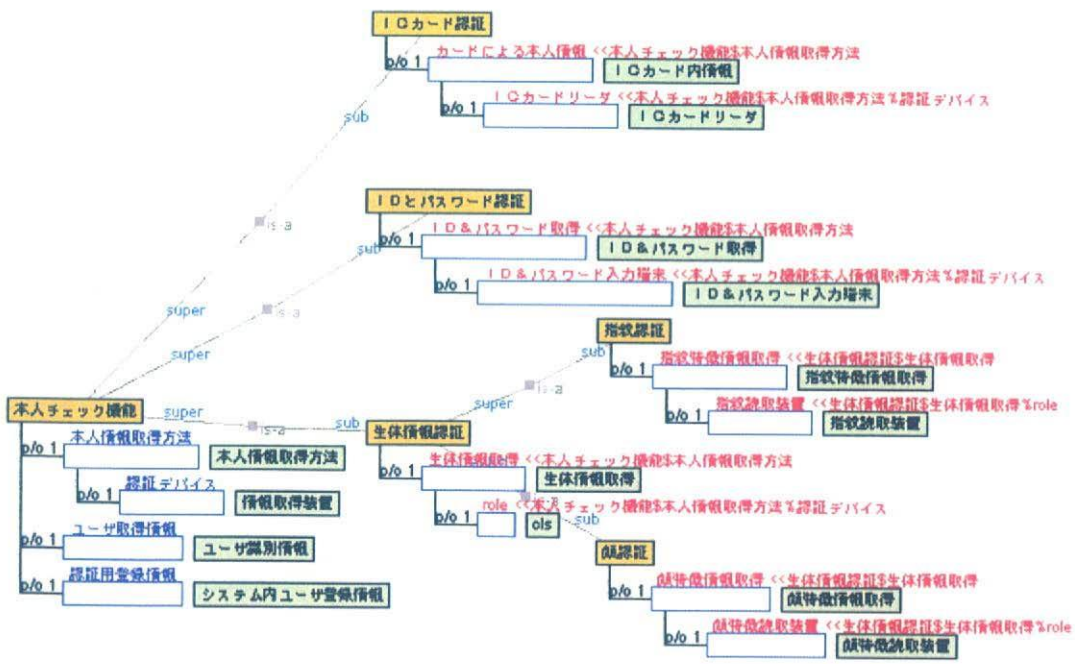


図１．認証に必要な本人チェック機能のモデル

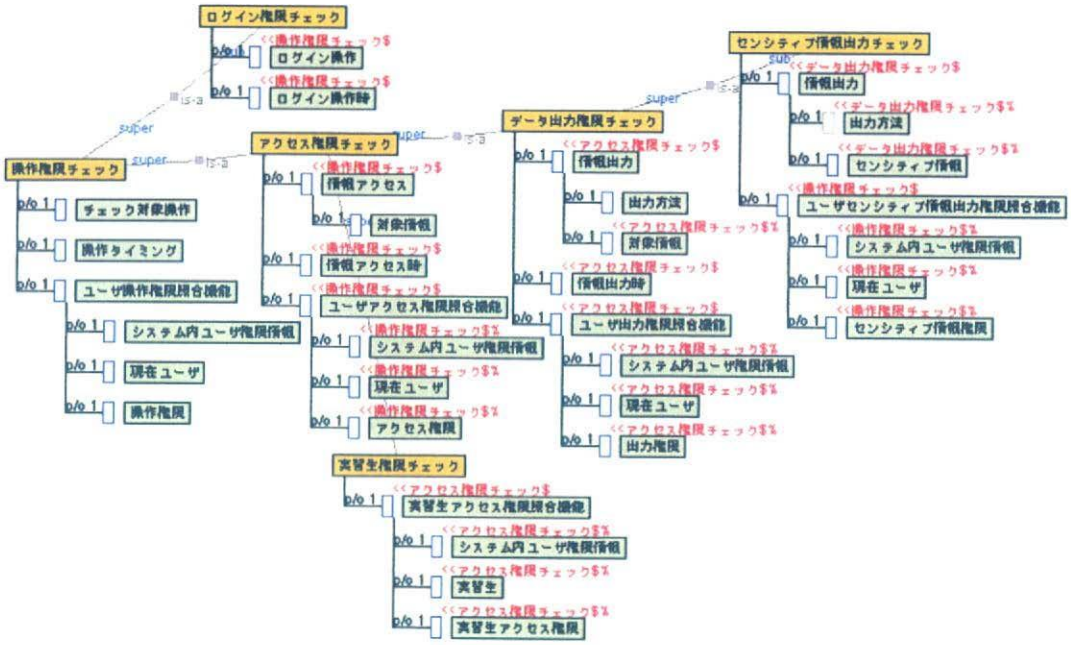
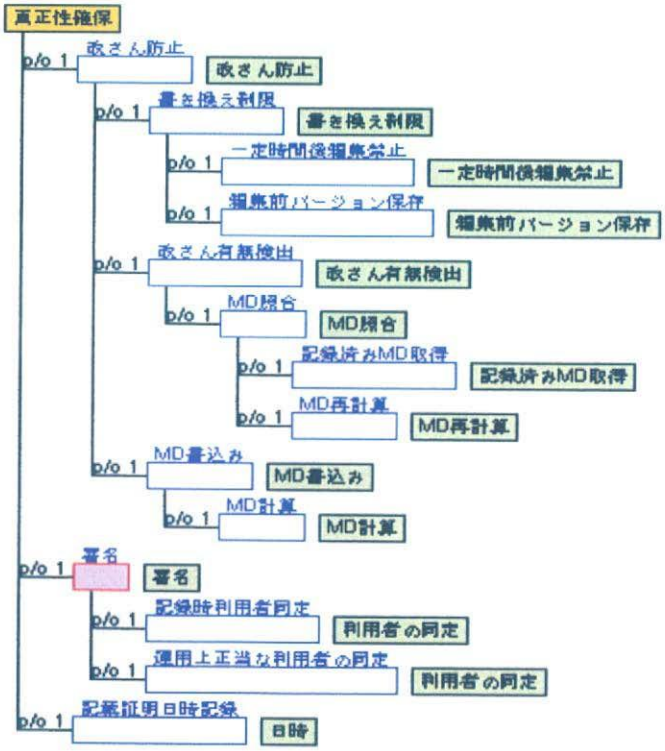


図２　権限のチェック機能モデル

図3. 真正性確保に関する機能の構成要素



書籍

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