ィ対策は一定以上の対策を採ろうとすると、その対策による安全性への効果に比してコストの上昇が大きい傾向にある。すなわち、セキュリティ対策を突き詰めていくと、最後は相当なコストをかけてもわずかしか安全性が向上しないことになりやすい。むろん医療情報の安全管理は医療機関等の責務であり、一定の達成度は求められるが、この達成度に対して明示的な基準はなく、社会的なコンセンサスも存在しなかった。つまり医療機関は自らの判断で達成度を定めて努力していきたわけであるが、ではその達成度が十分なものかどうかを判断する基準はなかった。さらに安全やプライバシーは結果的に守られたから十分とはいえない。医療機関としては説明責任を果たすことが求められており、事前に患者等に安心感を与えることも必要である。このような状況で安全管理 GL ができたことは大きな意味がある。もちろんこの安全管理 GL がプロテクションプロファイルとして完全なものではなく、じゅうぶん厳格な基準を定めているともいえない。しかし、厚生労働省としておおまかな基準を示したとは言える。

安全管理 GL ができたからといって一気に医療機関におけるセキュリティ目標が明確になるわけではないが、一定の基準には違いなく、何も存在しないこれまでにくらべればはるかに明確になったと言うことでき、今後のコンセンサス形成のきっかけになることが期待できる。

前章で述べたように安全管理はこれまでの電子保存や外部保存のガイドラインに比べて具体的で、理解しやすい。しかし情報セキュリティそのものが一般の医療機関勤務者にとって親しみのある事項ではなく、その中の情報システム担当とは言え、すべてが容易に理解できるものではないであろう。その意味で改善の余地はあり、今後の定期的な見直しの際に改善を求めることが必要であろう。

また厚生労働省の標準的電子カルテ WG で医療情報システムの品質に関する基準を含める必要があることを指摘されている。一般の医療機器等では薬事法によって一定の品質が検査されるが、情報システムの特質でソフトウエアのバージョンアップや診療報酬制度の改訂に伴う変更など、頻繁に改造が行われ、通常の薬事法のスキームでは無理があると考えられる。

C-4. 医療情報システムの安全管理のためのガイドラインの受け取られ方の調査

C-2 のアンケート調査で安全管理ガイド

ラインを知らない、内容を知らないと応えた機関以外に対して、ガイドラインを読んでどう感じたかを尋ねたところ、小規模、大規模いずれも「分りにくい」という返答が最も多かった。しかし、「難しすぎて自機関では運用が困難である」という返答も目立つが、これらの返答から、機関内の情報の安全管理について真剣に取り組み、より適切な対応を考えていると見受けられる。（図９）

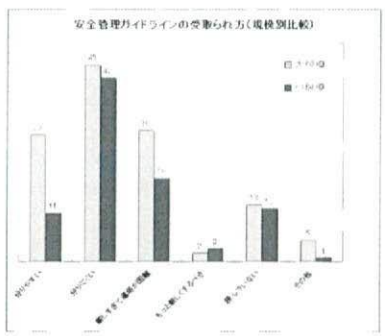

図９．安全管理ガイドラインの受取られ方（2006年３月）

C-5. 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-6. 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-7. 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

HPKI 署名検証ライブラリは本年度は作成したところまでで、実際に有用なものとするためには十分な検証が必要である。本研究班でも平成 18 年度に十分な検証と評価を予定している。また個人情報保護法への医療機関の対応はこの 1 年でかなり整備され、全体的には好ましい結果といえる。しかし、情報システムの安全管理に関しては、実際に事故が起こったかどうかは別として説明責任を果たすという意味では不十分といわざるを得ない。C-3 で述べたように厚労省が公表した医療情報システムの安全管理のためのガイドラインは全体としてみれば意義深いものであるが、いくつか問題がある。一つはやはり医療機関にとっては理解しくいことで、特に小規模医療機関にとっては課題である。この理由の一つは

一冊のガイドラインであらゆる規模の医療情報システムに対応しているためで、レセコン 1 台だけという医療機関にとっては大部分が自施設の関係のない記述になってしまう。また 2 つ目はかなりよく練られた内容ではあるが、文章自体がわかりにくい部分もあり、改訂が望まれる。さらに情報セキュリティは多少とも基礎知識のある者とまったく基礎知識のない者では理解力に大きな差がでる。医療従事者にも一定の基礎知識を持つ人もあり、大規模医療機関では専門職として従事する人さえいる場合がある。つまりガイドラインの読み手としての理解力を単純に想定することに無理がある。これは紙に印刷することを想定した平板な構造の文書では対応が難しい。読み手のレベル別にいくつかの版を用意するか、E-Learning を利用してインタラクティブに理解できるような仕組みを導入する必要がある。また情報システムの品質評価に関する事項がないと指摘され、確かにその点では不十分である。これに関しては本年度は十分には検討できなかったが、米国の医療情報システムのベンダー団体である HIMSS が規定している MDS2 が参考になる可能性がある。

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

HPKI 電子署名基盤が整備されることを前提に署名および検証ライブラリを作成した。今後の評価が期待される。また前研究班の成果とあわせ実施した個人情報保護に関するアンケートではこの1年間に医療機関の個人情報保護対策の整備は大幅に進んだことが明らかになった。しかし一方で医療情報システムの安全管理に関しては十分とはいえなかった。厚労省の公表した「医療情報システムの安全管理のためのガイドライン」の整備と普及が求められる。また情報システムの品質管理の一助として米国HIMSSが示しているMDS2が参考になる可能性があると考えられた。さらに診療情報の 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。

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