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）

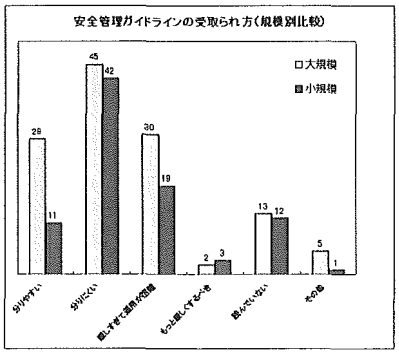

図９．安全管理ガイドラインの受取られ方（2006年３月）

C-5. 医療情報システムの安全管理のためのガイドライン普及のための E-Learning コンテンツの作成の準備

富士通株式会社の Internet Navigware を導入し、研究班で共同作業可能な環境を構築した。本年度は導入にとどまり、18 年とにコンテンツの試作と効果の評価を行う予定である。

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。本研究班では今年度準備を整えることができたので、18 年度にはインタラクティブコンテンツを開発し評価することを予定している。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り、18 年度には検討を行う予定にしている。

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。資料として MDS2 を添付する。

F．健康危険情報

特になし。

G．発表

書籍

１．　開原成允、樋口範夫編、「医療の個人情報保護とセキュリティ（改訂２版）」、有斐閣、東京、2005、330ページ

雑誌

１．　山本隆一、厚生労働省「医療情報システムの安全管理に関するガイドライン」について、医療情報学、vol. 24, pp507-515、2005

２．　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

３．　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

４．　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

５．　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。

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
山本隆一	厚生労働省「医療情報システムの安全管理に関するガイドライン」について	医療情報学	24巻5号	Pp507-515	2005

特集　医療および医療情報における個人情報保護法

厚生労働省「医療情報システムの安全管理に関するガイドライン」について

山本隆一
(東京大学大学院情報学環)

Introduction of "Security Guidelines for Medical Information Systems by Ministry of Health, Labor and Welfare of Japan 2005"：Ryuichi Yamamoto(Interfaculty Initiatives of Information Studies, Graduate School of The University of Tokyo)

In March 2005, the Ministry of Health, Labor and Welfare of Japan published "Security Guidelines for Medical Information Systems 2005". This guideline have some standpoints, the supplemental guidelines of "Guidelines for privacy protection in health field, a part of infrastructure for Information and Communication Technology Strategy of Japanese government, guidelines for applying Digital Documents Act in health field, and update version of guidelines for digital storage of medical records. Indeed we had some security guidelines for medical information systems, but those are only applied with limited situation and not for general information system security. This is the first attempt to make guideline for general security of various medical information systems and we hope this guideline will be baseline to build up social consensus for security and privacy protection of medical information systems.

Key words：Security guidelines, Medical information systems, Ministry of health labor and welfare, Privacy, Electronic health records

1. はじめに

医療情報システムに関係する者にとって安全管理は常に重大な関心事である．きわめてプライバシーに機微な情報を大量に扱う医療情報システムではセキュリティの確保は当然達成すべきことであるが，一方でセキュリティに完全ということはない．したがって自ら安全管理目標を定めて，社会通念上問題のないと考えられるレベルの安全管理を実施してきたわけであるが，では厳然とした社会通念が存在したかと言えば，そうとは言えない．情報システム自体の歴史が浅く，またプライバシーの概念自体も社会の情報化に伴って発展してきたもので，したがってその一部としてとらえることができる情報セキュリティも，いわば発展途上の概念であり，共通の理解を形成しているとは言いがたい．結局は医療機関の主体的な判断で安全管理レベルを定めてきたわけで，結果として情報の安全性に問題がないとしても，管理目標が不足なのか，過剰なのか，確たる自信がないというのが現状であろう．

医療情報システムが診療報酬に関係する事務処理の合理化を主目的としていて，プライバシーも努力目標であった時代では，医療情報システムの安全管理目標のもっとも重大な目標は診療に差し支えないことで，セキュリティの用語で言えば可用性の確保，それもその時点での可用性の確保であった．したがって目標も比較的明確で，対策も立てやすかった．守秘義務の観点からの情報セキュリティの機密性も重要ではあったが，基本的に

事務処理に使われた情報であったために，保持期間も短く，また利用も限定的で機密性に関する対策は比較的容易であった．

これに対して，電子カルテに象徴されるように，医療情報システムの目的が事務処理の合理化だけではなく，直接診療に利用されることを目的とするようになり，また，医療以外の分野も含めて国をあげてのIT化促進の当然の条件整備として個人情報保護法が成立したこともあり，安全管理目標は大きく変化し，しかも医療機関内だけの問題ではなくなり，患者等の利用者や社会に対して説明責任を求められるようになった．

一方で医療は社会的側面が強く，さまざまな法令に基づき運営されている．医療情報システムが単に医療機関内の作業の合理化だけに用いられている場合は情報セキュリティも医療機関内に閉じた問題であったが，直接医療に係り，また物理媒体だけではなし得ない高度な医療連携や患者等との情報共有が視野に入るにつれて，医療情報システムの情報セキュリティも医療機関内で閉じた問題とは言えなくなった．すなわち社会的な合意形成の一環として行政をはじめとする制度的な手当ても必須になってきたと言える．

平成17年3月に厚生労働省が本稿の主題である「医療情報システムにおける安全管理に関するガイドライン」(以下，安全管理GLと呼ぶ)を公表したが，前述の背景を考えれば極めて意味の大きい文書と言えるであろう．なお，著者は後述するようにこの安全管理GLの作成に深く関与してきたが，本稿執筆時点ではまだパブリックコメントを募集している状態であり，本稿内容と最終的な安全管理GLに齟齬がある可能性があることに留意していただきたい．

2. 安全管理GL作成の背景

この安全管理GLは平成17年4月から全面実施された個人情報保護に関する法律の情報の安全管理指針としての意味が大きいが，作成の背景はそれだけではない．これらの背景は安全管理GLの内容とも深く関係するので，簡単に触れておきたい．

平成15年に厚生労働省の医政局長の私的諮問検討会として「医療におけるネットワーク基盤検討会(座長：東京工業大学　大山永昭教授)」が組織され，平成16年9月の答申[1]を出した．安全管理GLは直接的にはこの答申に基づいて作成された．作成に携わった組織は「医療におけるネットワーク基盤検討会」(以下，基盤検討会と呼ぶ)の作業班で，著者はこの作業班の主査を勤めた．基盤検討会では医療情報の安全に関するさまざまなことが検討されたが，主要な論点は，1)公開鍵基盤の整備，2)医療に関する文書の電子化の促進，3)電子保存，外部保存のガイドラインの見直し，の3点である．さらに平成16年秋に「民間事業者が行う書面の保存等における情報通信の技術の利用に関する法律」(以下，e-文書法と呼ぶ)が成立したが，これに対応することも論点の一つであった．これらすべての論点が安全管理GLに取り入れられているが，さらに平成16年末に「医療・介護関係事業者における個人情報の適切な取扱いに関するガイドライン」[2](以下，厚労省個人情報保護指針と呼ぶ)が公表され，その中で，安全管理に関して医療情報システムを用いる場合は別に指針を示すこととなったが，その指針としての役割も果たすこととなった．最後に厚生労働省の医政局に医療の情報化を推進するための一つとして「標準的電子カルテ推進委員会(座長:東京大学　大江和彦教授)」が標準的な電子カルテの要件と普及の方策を検討しているが，その検討の過程で，電子カルテの個人情報保護を含めたセキュリティ基準を設けることが必要とされ，その検討を基盤検討会に委託した．安全管理GLはこの検討の結果としての意味も持つ．

つまり，個人情報保護に関する法律の安全管理に関する要請に応えるだけではなく，医療におけるe-文書法への対応や医療情報の電子化の促進も視野において作成されたものということができる．

なお，e-文書法とは民間事業者に対して法令で作成や保管が義務付けられた文書を一括して電子媒体上の電子文書に置き換えることを認める法律で，これまで，診療録等の個別の文書の電子化を容認してきたものを一気に一括で，しかも紙媒体などの物理媒体をスキャナやデジタイザで電子化して扱うことも容認する法律で，原則は全文書が対象であるが，実際には関係府省が省令で対象を

定めることになっている．医療で言えば電子保存通知が省令に格上げされ，さらに通知では保留または認められていなかった，記名・押印が必要な文書や，紙媒体やフィルムの情報も一定の条件を満たせば一部の例外を除き，電子的に扱うことが可能となる．

3. 安全管理GL概説

1) 概観と構成

安全管理GLは100ページを超える指針であり，図1のように10章と付表からなっている．

1章には安全管理GLの背景とスコープが書かれている．この指針は病院，診療所，薬局，助産所等の医療機関等における電子化の責任者を対象としており，介護事業者は直接の対象としていない．しかし医療機関を介護機関，患者等を利用者と読みかえれば指針の大部分は適応可能であると考えられるし，また適応することが求められるであろう．

また重要な点として，この指針自体を理解しやすいものとするために，現時点で利用可能な技術に関しても具体的に触れるとされている．これまで公表された電子保存のガイドラインや外部保存のガイドラインが徹底した技術的中立の立場で書かれたものであったが，確かにそのために表現が抽象的になり，具体的対策がわかりにくかった．この指針は大きく方針と転換したものと考えることができる．一方で，トレンドの技術に触れる以上は記載の陳腐化は避けられない．定期的な見直しが必要となり，そのことも明記されている．

2章はこの指針の読み方であり，各章の記載の原則と，付表の利用の仕方に言及している．この指針は日本情報処理開発協会が作成したプライバシーマーク認定制度の医療機関向け認定指針[3]と同様の構成をとっており，A.として制度上の要求事項を原文で挙げ，B.でその解説を述べ，C.で最低限必要な対策を列挙し，D.で必ずしも実施しなくてもA.の要求事項を満たすことはできるが，行ったほうが説明責任を果たしやすい，推奨される対策を列挙している．この指針も，前述の「医療機関向け認定指針」も著者が作成に携わったが，もともと，米国でHIPAA Privacy standardsに大学関連病院が対応するための指針が作成された際にとられた構成で，同じくこの指針の作成にも関与した著者らが導入したものである．

3章は対象システムおよび対象情報で，電子保存や外部保存の通知では文書が列挙されていたが，e-文書法の実施に伴って厚生省令が出されることから，その省令を参照する形になっている．注意しなければならないことは大部分の書類が電子的に運用し保存することが認められているが，依然として処方せんの電子化は容認されていないことである．

4章は医療機関等の責任のあり方について記載されている．医療情報の大部分は法令によって作成や保管が義務付けられているもので，それぞれの法令に従って医療機関等が自己責任で実施することを求められている．電子的に扱うからといってこのことに違いはないが，あらためて明示したと考えてよい．

5章は相互利用性と標準化に関して記載されている．電子保存通知や外部保存通知の要件はあくまでも行政から見た電子化による弊害を避けることが主体であったが，医療機関等や患者から見れば情報を継続して利用できることは極めて重要で，途中でシステムが入れ替わったからといって，利用性が阻害されることは避けなければならない．そのためには標準化は非常に重要な要素であり，

1．はじめに
2．本ガイドラインの読み方
3．本ガイドラインの対象システムおよび対象情報
4．自己責任について
5．情報の相互利用性と標準化について
6．医療情報システムの基本的な安全管理
7．電子保存の要求事項について
　　真正性，見読性，保存性，電子署名
8．診療録および診療諸記録を外部に保存する際の基準
9．診療諸記録をスキャナ等で電子化して保存する場合について
10．運用管理について
付表1．一般管理における運用管理の実施項目例
付表2．電子保存における運用管理の実施項目例
付表3．外部保存における運用管理の実施項目例

図1 医療情報システムの安全管理に関するガイドラインの構成

1章を設ける価値は十分あると考えられる.その中で中間法人日本医療情報学会も中心的役割を果たしている医療情報標準化推進協議会(HELICS協議会)が重要視されている点も注目したい.

以降,6～10章は**図1**に示すとおりで,内容は次節以降で概観したい.しかし重要な点は7～9章は必要に応じて利用すればよいという構成になっていることであろう.

この安全管理GLは個人情報保護法の安全管理に関して医療情報システムに係る指針としての面がある.したがって患者個人情報を扱うシステムはすべて対象となる.言い換えればレセコンや医事システム,保険薬局の調剤記録システム,服薬指導管理システムなども対象となる.個人情報保護法では個人データと一定期間保有する保有個人データは区別されるが,法の求めの内で,目的明確化と目的外使用の禁止や,安全管理,第三者提供の原則禁止などはすべての個人データに関して要求される.したがって,たとえ1カ月で情報を消去するレセコンシステムがあったとしても安全管理は同様に行わなければならない.つまり電子保存をしなくても,外部保存をしなくても,必要な安全管理は存在し,それに対して指針を示す必要がある.安全管理GLではこのような基本的な安全管理指針を6章に集約している.これによって,電子保存も外部保存もしないが,レセコン等の情報システムを導入している医療機関等は7～9章は読む必要はない.後述するが10章および付表もそのような配慮が為されている.

2) 情報システムの基本的な安全管理(6章)

医療において電子保存や外部保存を行わない場合の情報システムの安全管理に関する規定はこれまで存在しなかった.もちろん医療機関においてレセコンやオーダエントリシステムで情報の安全管理に配慮がされなかったわけではないが,刑法等で定められた守秘義務への対応の一環として医療機関が自主的に取り組んできたもので,情報システムを特定した明文化された安全管理の責務やその基準は存在しなかった.その意味で個人情報保護法および厚労省個人情報保護指針ははじめて医療情報システムを直接の対象として安全管理を責務としたと言える.したがって6章では「A.制度上の要求事項」は個人情報保護に関する法律の条文を挙げている.そしてB.以下は厚労省個人情報保護指針の内容を踏まえて**図2**のように9個の項目に分けて記載している.その中で「6.1方針の制定」と「6.2上方の取り扱いの把握とリスク分析」は厚労省個人情報保護指針で求められているもので,必須や推奨の区別はできず,また使うシステムや医療機関の状況で大きく変化するものであるために,B, C, Dを区別せずにフラットな記載となっている.

6．1　方針の制定と公表
6．2　情報の取り扱いの把握とリスク分析
6．3　組織的安全管理
6．4　物理的安全管理
6．5　技術的安全管理
6．6　人的安全管理
6．7　情報の破棄
6．8　情報システムの改造と保守
6．9　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

図2　医療情報システムの基本的な安全管理(6章)の項目

6.3～6.7は厚労省個人情報保護指針で具体的に記載されている項目で,それを実際的な観点から医療情報システムの要件と運用にブレークダウンして解説し,対策を述べている.この中で組織的対策はやや抽象的であるが,その他は比較的具体的に書かれており,特に技術的対策においては1章で述べられているように,利用可能な技術要素を列挙し,それぞれの特徴や運用上の注意を具体的に述べている.

6.8の「情報システムの改造と保守」は現場で遭遇する機会の多い事項で,契約を含めて具体的な対策が記載されている.

6.9の「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」は言うまでもなくオンラインで医療情報を交換する場合の安全管理であり,オンラインで外部保存する場合は8章で詳細に述べられるために割愛されている.つまりこの項では外部保存するわけではないが,オンラインで医療情報を交換する場合の安全管理について述べられている.地域連携システム等,実験的または実用的にすでに実装されているものもあり,これに対して安全管理基準を示した意義は大きい.

3) 電子保存の要求事項について(7章)

7章は従来の平成11年の「診療録等の電子媒体による保存について」の通知に基づく電子保存のガイドラインのリライトであり，保存義務のある文書を電子媒体で保存する医療機関だけに関係する．この章の記載にはひとつ形式上の問題がある．現在の版(パブリックコメント版)ではA.の制度上の要求事項は平成11年の電子保存通知の要求事項が書かれているが，本稿2章で述べたように，e-文書法の実施に伴って厚労省から省令が出されることになっており，この省令の要件に変更される必要がある．もっとも個人情報保護法が成立したことなどを除けば通知と省令で大きな要件の変更はないと考えられるので，内容は大差ないであろう．この章の特徴としては，記載が具体的になったことと，7.4に電子署名に関する要件が記載されたことである．

例えば真正性の確保に関しても具体的なユースケースに分けて詳解し，**図3**に示すように，イラストが添えられている．これまでの電子保存のガイドラインでは理解しがたかった部分もかなり容易に理解できるようになったと考えられる．

7.4の「法令で定められた記名・押印を電子署名で行うことについて」は，平成11年通知では保留にされた文書の内，処方せんを除く書類に関して電子署名で記名・押印に代えることができることがe-文書法および厚労省令で容認されたことに対応する部分で，Aの制度上の要求事項は電子署名および認証業務に関する法律からとられている．この項はDがなくCだけであるが，その要件は1)認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと，2)電子署名を含む文書全体にタイムスタンプを付与すること，3)上記タイムスタンプを付与する時点で有効な電子証明書を用いること，となっている．認定特定認証事業者等と，「等」がついているのは，将来保健医療福祉分野で公開鍵基盤が整備された場合のことを想定してのことであろう．2章で述べた基盤検討会の答申ではこのような公開鍵基盤の必要性が明記されている．また公的個人認証サービス[4]についても言及されている．公的個人認証サービスは住民基本台帳カードに付随するサービスで安価に電子署名法に適合する証明書が入手できるという意味は大きい．しかし，現時点ではこのサービスを利用して行った電子署名を検証できる組織は行政機関等に限られており，利用可能な組織は限定されている．タイムスタンプを必須とすることで，電子署名自体の有効性は署名時点，正確には署名後タイムスタンプを付与する時点で確保されていれば良い．これは各自が管理しなければならない署名用の電子証明書ではなく，一般に長期間有効性が保障されるタイムスタンプに有効性根拠をおいたことで，運用の負担を軽減したと考えられる．一方でこれに伴ってタイムスタンプの要件が厳格に

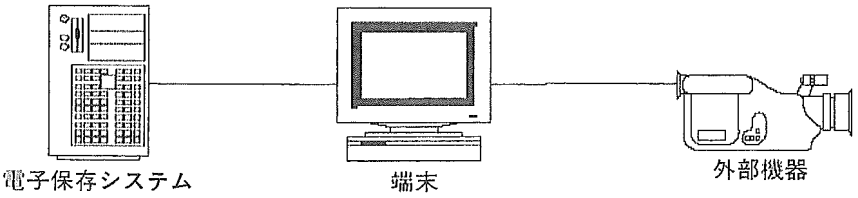

図3　電子保存の要求事項について(7章)の真正性の確保の記載例

【ケース概要】
外部機器を電子保存システムの認証機能が動作する端末を経由して電子保存システムへ患部の写真等を医療情報の一部として格納するケース．

【入力手順】
外部機器から送信される医療情報等を一旦電子保存システムの端末に格納し，受信情報の内容の確認と患者属性の付与(必要に応じて)，確認を行い，電子保存システムへ送信し格納する．

【記録の確定】
この際の記録の確定は，端末での内容確認時点であり，作成責任者が端末で内容を確認する必要がある．

なっているが，e-文書法の実施に伴い，他分野でもタイムスタンプの利用が進むために，医療機関でも十分対応可能と考えられる．

4）診療録および診療の諸記録を外部に保存する際の基準(8章)

8章は平成14年の通知「診療録等の保存を行う場所について」に伴って作成された外部保存のガイドラインのリライトであるが，基盤検討会の答申を踏まえ，オンライン外部保存の制限が緩和されている．平成14年の通知「診療録等の保存を行う場所について」には紙やフィルムの物理媒体で外部に保存する場合も含まれていることから，この章の一部に医療情報システムに無関係な指針が含まれている．はじめてこのような指針を見るものにとってはとまどう点かも知れないが，医療情報システムをまったく使わない医療機関はごく少数である現状を考えると医療機関が参照すべき指針をできるだけ単純にする意味で，やむを得ないであろう．また，7章は旧電子保存に関する指針を大幅に書き改めているが，8章は後述する数点を除いて全体としては旧外部保存に関する指針を踏襲している．これはオンラインで情報を伝達する部分を除くと，主に運用上の指針であり，旧指針からすでにかなり具体的であったためであろう．

安全管理GLとして外部保存に関する内容上の改定点はオンライン外部保存の対象の拡大であり，旧通知および指針では受託機関は「病院または診療所その他これに順ずるものとして医療法人等が適切に管理する場所」だけであったが，これに「行政機関等が開設したデータセンター」と「医療機関等が震災対策等の危機管理上の目的で確保した安全な場所」が追加された．もちろん，いずれも安全性と個人情報保護が確保されていることが条件である．「行政機関等が開設されたデータセンター等」は国の機関，独立行政法人，国立大学法人，地方公共団体等が開設したデータセンターで，政策医療の確保のために有機的な医療機関間連携が必要で電子保存を支援することで質の高い医療供給体制の構築を目指す場合に許される．受託者であるデータセンターの条件として，従業者に退職後を含めて罰則を伴う守秘義務が課せられていること，緊急対応を除き保存主体の医療機関のみがデータ内容を閲覧できることを技術的に担保していること，さらに受託に必要な技術的および運用的管理能力をシステム監査技術者[5]やCertified Information Systems Auditor[6]等の適切な能力を持つ監査人の外部監査を受け，定期的に確認されていることが挙げられている．「医療機関等が震災対策等の危機管理上の目的で確保した安全な場所」は，医療機関等が，保存に係る情報処理機器を自らの所有物として保持し，電気通信回線の確保や管理を保存主体である医療機関等の責任で行えること，また，診療録等の保存された情報に係る責任を自ら担保でき，外部に電源設備等を含めて保存場所を確保するか，または，適切な利用形態で借り受けて行う保存形態とされている．端的に言えば厳密なハウジングサービスの利用である．この場合ハウジングサービスの提供は一般的に民間企業であり，行政機関等と異なり法令による罰則を伴う守秘義務は期待できない．したがって，ペナルティを含めた厳格なルールを契約で定めることを求めている．さらに行政機関等と同様に，保存主体のみが保存情報にアクセスできることを技術的に担保すること，および安全管理能力をシステム監査技術者やCertified Information Systems Auditor等の適切な能力を持つ監査人の外部監査を受け，定期的に確認されていることが挙げられていて，民間事業者が受託する場合はプライバシーマーク制度等による第三者認定も求めている．なお，システム監査技術者は経済産業大臣が認定する監査資格である．Certified Information Systems AuditorはISACAが認定する監査資格であるが，国際的に評価が高い．

5）診療録等をスキャナ等により電子化して保存する場合について(9章)

本章はまったくの新設の指針である．平成11年の電子保存に関するガイドラインでは，スキャナやデジタイザによる電子化は真正性の確保が困難として法的義務を満たす電子保存としては認められていなかった．しかし，その後のスキャナやデジタイザの技術の進歩と電子署名による責任の所在の明確化の技術が進歩したことから平成16年秋にe-文書法が成立し，それに伴った新たに容認されたために加えられた指針である．

文字を主体とする文書の場合，一般にスキャナで取り込んだ情報は図形情報となり，その内容を計算機が意味のある情報として扱うことは難しい．医療情報の電子化の重要な目的は意味のある情報の医療機関内外での共有であり，その意味では発生時からの電子化を目指すべきで，画像情報として扱うスキャナでの取り込みが多用すべき方法でないことは明白である．もともと画像情報であるアナログ撮影されたX線写真をデジタイザで電子化した場合は，情報の意味としては大きな違いはない．しかし，いかにすぐれたデジタイザを使っても，もとのアナログ画像より情報量が落ちることも明白である．

一方で電子化情報は紙やフィルムに比べて操作性が向上する可能性が高く，また一旦電子化した後は劣化しない．フィルム等の変色を考えると，無視できない利点である．また，ペーパーレス，フィルムレスを基本として運用している医療機関でも，診療情報提供書やフィルム画像を患者等が持ち込むことはしばしばある．これらはいずれも重要な医療情報であり，診療に際して必要に応じて参照できなければならない．そのために紙やフィルムの保管や運用を考慮するのは施設にとって負担であるだけでなく，電子化情報と紙やフィルムの物理媒体の双方の存在を常に意識する必要があり，万が一にも一方を見落とすことになれば，医療安全上の問題にもなる．そのような意味ではe-文書法による規制緩和は今後当分続くと予想される新旧が混在する医療の電子化の過程で重要であろう．

安全管理GLではスキャナ等により電子化して保存する場合を2つに分けている．ひとつは診療等の都度スキャナ等で電子化して保存する場合で，典型的な例は前述のペーパーレス・フィルムレス運用の医療機関に外部から紙やフィルムで持ち込まれた情報を扱う場合であるが，これ以外にも保険薬局に持ち込まれた処方せんで処方済みとなったものなども考えられる．もう一つは過去に蓄積された紙媒体等をスキャナ等で電子化して保存する場合で，これはある時点からペーパーレス・フィルムレスに移行したが，その時点までの保存義務のある紙やフィルムの情報が存在し，それを一括してスキャナ等で電子化し保存する場合が考えられる．指針ではまず共通の要件として，通常の文書はRGB各色8ビット以上，300 dpi以上のスキャナを使用することを求め，放射線画像に関しては，日本医学放射線学会電子情報委員会が公表した「デジタル画像の取り扱いに関するガイドライン1.1版」[7]に準拠することを求めている．この日本医学放射線学会のガイドラインではマンモグラフィは対象とされていない．最近の検討でもマンモグラフィに関してはデジタイザの性能がいまだ不十分としていることから，マンモグラフィは対象外と考えなければならない．なお，放射線以外の画像情報に関してはこのような基準がなく，医療に関する業務に差し支えないことを尺度としてそれぞれの医療機関が判断しなければならない．また運用管理規程を定めて，責任者を置き，さらに電子化に際して電子署名とタイムスタンプの付与を求めている．このときの電子署名とタイムスタンプの要件は7.4の「法令で定められた記名・押印を電子署名で行うことについて」に記載された要件と同じである．また情報システムとしての安全管理はもちろんのこと，電子化した後の紙等の媒体の破棄についても個人情報保護に配慮した扱いを求めている．

診療等の都度スキャナ等で電子化して保存する場合では共通の要件に加えて情報が発生，または情報を入手してから，電子化までの期間を合理的な範囲にすることを求めている．通常は診療録の記載と同様に遅滞なく行わなければならない．

過去に蓄積された紙媒体等をスキャナ等で電子化して保存する場合は共通の要件に加えて，あらかじめ本人に通知し，計画の段階から倫理委員会等の公正性を確保した組織で妥当性・公正性の評価を受けた運用管理規程を作成し，システム監査技術者やCertified Information Systems Auditor等の適切な能力を持つ監査人の外部監査を受けることが必要とされている．また外部に委託する場合は少なくともプライバシーマークを取得しており，過去に安全管理や個人情報保護上の問題を起こしていない事業者を選定し，実施に際してはシステム監査技術者やCertified Information Systems Auditor等の適切な能力を持つ監査人の

外部監査を受けることを含めて，契約上に十分な安全管理を行うことを具体的に明記することを求めている．かなり厳しい要件ではあるが，情報の作成から電子化までの時間が長い場合，改ざん動機を生じる可能性は否定できず，当然であろう．

なお本章には補足として「運用の利便性のためにスキャナ等で電子化を行うが，紙等の媒体もそのまま保存を行う場合」の指針が記載されている．もとより保存義務も作成義務とも無関係な情報に関して指針が存在するのは，個人情報保護上はスキャン後のデータも原本と同様に安全管理をする必要があり，また，その目的から考えて診療等に用いるのはスキャナ等によって電子化された情報であり，診療に差し支えない精度の必要性は保存義務を果たすために用いるか否かと無関係に存在するからであろう．

6）運用管理について（10章）および付表

情報システムの安全管理が技術要素とそれに見合った運用規程で達成できることは当然であり，運用規程が重要であることは論を待たない．しかし運用規程はあくまでも技術要素との兼ね合いであり，一律に論じることは難しく，また医療機関等にあっても苦労するところであろう．安全管理GLでは10章では管理項目だけを挙げ，実際の運用規程の作成は付表を参照して作成するステップを記載するにとどめている．

1．運用管理項目
　安全管理上の要求事項で多少とも運用的対策が必要な項目
2．実施項目
　上記管理項目を実施レベルに細分化したもの
3．対象
　医療機関の規模の目安
4．技術的対策
　技術的に可能な対策，ひとつの実施項目に対して選択可能な対策を列挙した
5．運用的対策
　4．の技術的対策を行った場合に必要な運用的対策の要約
6．運用管理規程文例
　運用的対策を規程に記載する場合の文例

図4　付表の構成

付表は図4に示す6カラムからなる表で，10章で挙げた管理項目ごとに記載されている．さらに付表を3つにわけ，付表1ではすべての医療情報システムの安全管理の際に参照すべき管理項目を挙げ，付表2では電子保存を行う場合の管理項目，付表3では外部保存を行う場合の管理項目を挙げている．管理項目ごとに，自らの医療機関の規模を選び，複数の技術的対策がある場合は，導入したか導入予定の技術的対策を選択し，それに対応する運用的対策を理解し，運用規程を作成すればよいことになる．さらに6カラム目には運用規程文例もあり，ドラフトレベルであればこの文例を用いれば作成することができる．ただし，運用管理規程はきわめて重要なもので，作成する場合も十分理解し，その医療機関の事情に応じて調整することが必要で，十分吟味して作成することが求められる．

4. 安全管理GLの意義と問題点

この安全管理GLは医療情報システムを利用する医療機関等において，情報システムの安全管理の指針として用いることを目指して作られたことは当然であるが，このような一種の基準が示された意義はさまざまな意味を持つ．最初に述べたように，医療情報にとってセキュリティは極めて重要な問題で，これまでも管理者は細心の注意を払ってきた．しかしいかに技術的対策をとり，細心の運用を行っても安全管理は100％とはいえない．またセキュリテ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，充分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．医療と情報の両側に足場を持つ日本医療情報学会は中間法人として責任を取れる立場にあり，医療の情報化の普及にとって大きな意味を持つ安全管理GLの定期的な見直しの際には積極的に寄与していくことが求められると考えられる．

参考文献

1)「今後の医療情報ネットワーク基盤のあり方について－医療情報ネットワーク基盤検討会最終報告」,医療情報ネットワーク基盤検討会，2004年，http://www.mhlw.go.jp/shingi/2004/09/s0930-10a.html(2005年3月15日)

2)「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」，厚生労働省，2004年，http://www.mhlw.go.jp/houdou/2004/12/h1227-6.html（2005年3月15日）

3)「個人情報保護に関するコンプライアンス・プログラム(JIS Q 15001)医療機関の認定指針　V1．02」，(財)日本情報処理開発協会，2002年，http://privacy.medis.jp/file/shisin030917.pdf(2005年3月15日)

4)「公的個人認証サービスポータルサイト」,公的個人認証サービス都道府県協議会，2004，http://www.jpki.go.jp/(2005年3月15日)

5)「システム監査技術者試験」,独立行政法人情報処理機構，2004，http://www.jitec.jp/1_11seido/h13/au.html(2005年3月15日)

6)“CISA Certification”，Information Systems Audit and Control Association，2002，http://www.isaca.org/（2005年3月15日）

7)「デジタル画像の取り扱いに関するガイドライン1.1版」，日本医学放射線学会電子情報委員会，2002，http://www.radiology.or.jp/jrs_doc/archive/DigitalImageGuide.htm(2005年3月15日)

HPKI署名ライブラリ開発
仕様書

Version 1.0

更新履歴

更新日付	Version	説明	更新者

目次

仕様書

1. はじめに

1.1 目的

本文書の目的は、XML 署名ライブラリの機能及び満たすべき仕様を明らかにするとともに、XML 署名ライブラリ開発の入力となる設計書を提供し、開発者の作業指針を示すことである。

1.2 参考資料

下記の表は、この文書で参照している標準仕様及び研究報告書等の名称、バージョン、並びにその説明の一覧である。

仕様等の名称	Ver.	説明
XML-Signature Syntax and Processing	20020212	IETF が提供する、XML ドキュメントに電子書名を付加するための標準仕様。XML のフォーマットや参照する暗号技術を策定する。以下、XML Signature と呼ぶ。
ETSI TS 101 903 (XAdES)	1.3.2	ETSI が提供する、XML ドキュメントに長期署名を付加するための仕様。XML のフォーマットは XML Signature に準拠し、そこにタイムスタンプ及び長期署名を付加するための仕様を追加する。2006 年 4 月 1 日現在の最新使用である V1.3.2 を参照する。
XAdES 長期署名プロファイル[1]		ECOM が提供する、XAdES に準拠した XML 長期署名記述のためのフォーマットを策定した標準プロファイル。本プロファイルは XAdES V1.3.1 を参照し記述されているが、本文所では修正を含む最新使用である V1.3.2 を参照する。
保健医療福祉分野 PKI 認証局 証明書ポリシ[2]		
タイムスタンプ・プロトコルに関する技術調査　調査報告書[3]		
タイムスタンプサービスの利用ガイドライン[4]		
XML-Signature Core Syntax and Processing		
IAIK		
BouncyCastle		
Apache XML Security		

[1] http://www.ecom.jp/report/electronic_signatures/XAdESLong-TermSignatureFormatProfile_V0.6pub_.pdf

[2] http://www.mhlw.go.jp/shingi/2005/04/s0401-1.html

[3] http://www.ipa.go.jp/security/fy15/reports/tsp/

[4] http://www.ecom.jp/results/h14seika/17_タイムスタンプサービスの利用ガイドライン.pdf

2. XML 署名ライブラリの概要

本章では、開発する XML 署名ライブラリが満たすべき機能の概要を説明する。

2.1 XML 署名ライブラリの機能

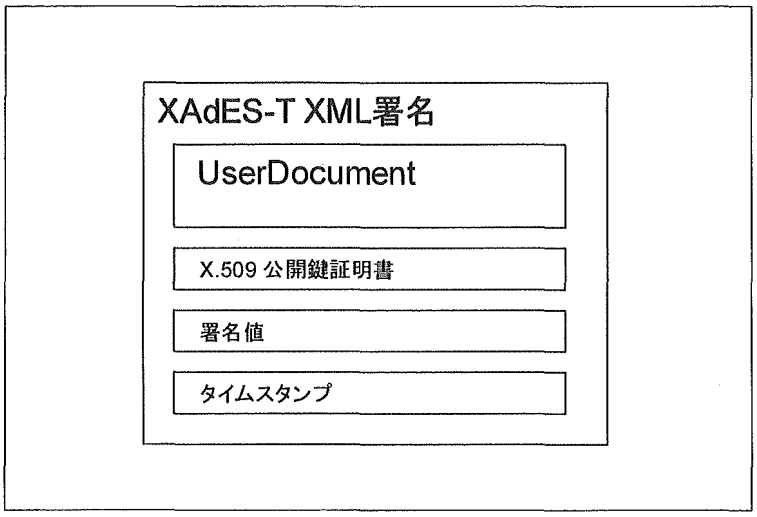

図 2-1 XAdES-T XML 署名の構成

XML 署名ライブラリの開発は XAdES-T に準拠した XML 署名（上図参照）の作成及びその検証機能をユーザに提供することが主な目的である。これらの機能をサポートするため、XML 署名ライブラリは下記の表に挙げた機能群を提供する。詳細については次章以降を参照。

表 2-1 XML 署名ライブラリの機能一覧

No	名前
1	XAdES-T XML 署名の作成
2	XAdES-T XML 署名の検証
3	X.509 証明書の検証
4	タイムスタンプトークンの取得及び検証

2.1.1 XAdES-T XML 署名の作成

ユーザが作成した XML ドキュメントへ、XAdES-T 準拠のフォーマットで XML 署名及びタイムスタンプを付加する。本機能は、以下の要件を満たす。

- XAdES-T に準拠した、タイムスタンプを含む XML 署名の作成
- Enveloping 型の XML 署名への対応
- 入れ子構造の多重署名の作成
- RSA 及び DSA のサポート
- SHA-1 及び SHA-256（またはそれ以上）のサポート

2.1.2 XAdES-T XML 署名の検証

XAdES-T 準拠に準拠した、タイムスタンプを含む XML 署名を検証する。本機能は、以下の要件を満たす。

- XAdES-T 仕様に準拠した、タイムスタンプを含む XML 署名の検証
- 多重署名された XML 署名の検証

2.1.3 *X.509 証明書の検証*

X509 公開鍵証明書の正当性を検証するため、証明書チェーンの構築、CRL の取得、ポリシ制約の確認といった機能を提供する。本機能は、以下の要件を満たす。

- HTTP プロトコルによるリポジトリからの公開鍵証明書及び CRL の取得
- 階層型の証明書チェーン構築及び検証
- 拡張領域を含む X.509 証明書プロパティの取得

2.1.4 *タイムスタンプトークンの取得及び検証*

TSP over HTTP プロトコルによるタイムスタンプトークンの取得、及びタイムスタンプトークンの検証をサポートする。本機能は、以下の要件を満たす。

- TSP over HTTP プロトコルによる TSA サーバからのタイムスタンプトークン取得
- タイムスタンプトークンの検証
- タイムスタンプトークンのプロパティの取得

2.2 PKI の構成

下記の図は、XML 署名ライブラリが公開鍵証明書の検証の際に想定する PKI の構成である。各要素のついては続く説を参照。

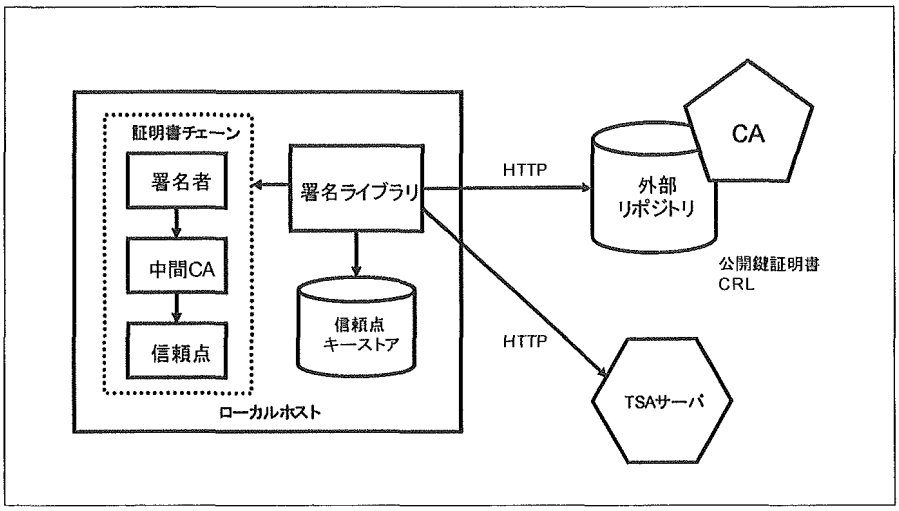

図 2-2 PKI の構成

2.2.1 *署名ライブラリ*

ユーザが作成した XML ドキュメントに XAdES に準拠した XML 署名及びタイムスタンプを付加する。また、XML 署名及びタイムスタンプの有効性を検証する。

公開鍵証明書の検証の際には、証明書チェーンや CRL を取得し、公開鍵証明書の正当性を検証する。また、外部の TSA サーバにアクセスしてタイムスタンプを取得する。

2.2.2 *証明書チェーン*

公開鍵証明書からその信頼点までの認証パスを構成する証明書のチェーン。

2.2.3 *CA*

公開鍵証明書の発行機関。公開鍵証明書や CRL を、リポジトリを通して公開する。

2.2.4 *外部リポジトリ*

CA が管理する、公開鍵証明書や CRL を格納するデータベース。HTTP プロトコルを使用してアクセスする。

2.2.5 *信頼点キーストア*

信頼点の証明書を保存するデータベース。署名ライブラリと同一ホスト上にセキュアに保管される。

2.2.6 *TSA サーバ*

タイムスタンプトークンを発行するサーバ。TSP over HTTP プロトコルを使用してアクセスする。