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１７年度　総括研究報告書

主任研究者　山本　隆一

平成１８（２００６）年４月

目　　次

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。本研究では HPKI の実現の技術的課題を研究するとともに高度な情報交換が可能になることを前提とした個人情報保護の在り方や医療機関における医療情報システムの安全管理に関して研究をおこなった。個人情報保護に関してはこの 1 年間で大幅に対応が強化されていることがアンケート調査で明らかになったが、その一方で安全管理に関しては少なくとも説明責任を果たすレベルでは不十分な状況が明らかになった。

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。平成 18 年 1 月に内閣府が示した IT 新改革戦略をひくまでもなく、医療の IT 化はさまざまな理由で推進されなければならず、また実際に推進されている。平成 16 年の医

療情報ネットワーク基盤検討会の最終報告を受け、平成17年には「医療情報システムの安全管理のためのガイドライン」、および「保健医療福祉分野認証局ポリシ」が厚生労働省から公表されたが、これらはいずれも安全で安心できる医療の IT 化の推進に非常に重要なものである。

本研究では保健医療福祉分野認証局ポリシ（以降 HPKI 標準ポリシと呼ぶ）の速やかな発展のための技術的課題を研究することを目的の一つとした。また高度な電子化診療情報の交換や共有が可能になることを前提に医療機関における個人情報保護への取り組みをアンケート調査によって明らかにすることも目的とした。さらに前述の「医療情報システムの安全管理のためのガイドライン」自体を分析するとともに、広く受け入れられるための方策をアンケート調査等で明らかにすることを目的とした。なお、本研究は分担研究者とメーリングリスト等で緊密に共同して行い、経費に主任に一括計上していることもあり本年度は分担研究報告書は総括研究書に一括して報告することとした。

B．研究方法

B-1. HPKI の円滑な普及のための技術的課題の研究

HPKI 標準ポリシが公表され、保健医療福祉分野認証局専門化会議が組織され、さらに平成 18 年度には実証的に厚労省が Root 認証局の運用を計画するなど、HPKI 電子署名基盤の整備は相当に具体化しつつある。本研究では HPKI 電子署名基盤が整備されることを前提に、署名や検証者が使用する証明アプリケーションおよび検証アプリケーションの基準を示すために、ライブラリを試作した。

B-2. 医療機関における個人情報保護対策の実施状況の調査

主任研究者が昨年度までおこなった個人情報保護に関する研究班で実施した内容とほぼ同様に、全国の医療機関から 2000 件を無作為に抽出し、アンケート調査を実施した。3 月 13 日にアンケートを発送し、締め切りは 3 月 25 日に設定したが 3 月 31 日到着分までを分析対象とした。調査表（回答集計を含む）および回答表を資料として添付する。

B-3. 医療情報システムの安全管理のためのガイドラインの調査

当該ガイドラインの研究の最初にガイドライン自体を詳細に分析し、今後の改善点等を抽出した。

B-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

B-2 のアンケート調査に際して当該ガイドラインの医療機関における受け取られ方を調査した。

B-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

当該ガイドラインはかなりのボリュームがあり、また内容も医療従事者にとっては理解しやすいものから理解しにくいものまで含まれる。理解の容易さは読む人のリテラシーに依存するために、一律に平易化をはかるといたずらに容量が増えることになり、好ましくない。そこで E-Learning の活用の可能性を検討するためにコンテンツの作成を行うこととした。ただし今年度はその準備として E-Learning System 自体の導入にとどまっている。

C. 研究結果

C-1. HPKI の円滑な普及のための技術的課題の研究

HPKI 電子署名基盤が整備されることを前提に、署名や検証者が使用する証明アプリケーションおよび検証アプリケーションの基準を示すために、ライブラリを試作した。資料として試作ライブラリの仕様の概要を示す。このライブラリは Microsoft .net2.0 および JAVA に対応するもので、今年度は開発にとどまっている。18 年度に主任・分担研究者で検証・評価を行い、また連続使用での異常の有無など feasible study を行うことを予定している。

C-2. 医療機関における個人情報保護対策の実施状況の調査

郵送した１９１０件のうち３月３０日までに返答があったものは３７０件で、回答率は１９．７％であった。また、３１件が廃院などを理由に宛先不明で戻ってきた。また、我々は全体の結果を分析した上で、前回と同様、病床数で病院の規模を小規模医療機関、大規模医療機関と分け、結果データを比較した。小規模医療機関とは、「病床なし」（４９．３％）「１９床以下」（４．４％）を併せた計５３．７％、大規模医療機関は「２０～９９床」（１８．４％）「１００～４９９床」（２５．２％）「５００床以上」（２．７％）の合計４６．３％である。

個人情報保護法についての質問では、有効回答数３６４のうち、全体の結果は、「既に対応を終了」１３２件（３６．３％）、「対応をはじめた」１２３件（３３．８％）、「対応を予定」３７件（１０．２％）、「未対応

で今後の対応を検討中」２３件（６．３％）、「対応は検討していない」３６件（９．９％）、「法律の内容を知らない」１２件（３．３％）「法律を聞いたことがない」１件（０．３％）という結果で、もっとも多かった回答が「既に対応終了で全体の４割近くであった。（図１）。また、前回の調査の結果は、調査時期が法律全面実施直前ということもあり、「既に対応終了」は２．５％、もっとも多かった回答が「現在は未対応だが、今後は対応を予定」で３２．９％であった。

今回と前回（図２）を比較すると、やはり法律全面実施前と実施後ということで、明らかに「対応済み」が増えたことと、「法律の内容を知らない」「法律をきいたことがない」が半分以下に減少したことが目についた。

既に対応終了	132 (36.3%)
既に対応をはじめた	123 (33.8%)
現在未対応、今後対応予定	37 (10.2%)
現在未対応、今後は検討中	23 (6.3%)
対応は検討していない	36 (9.9%)
法律の内容は知らない	12 (3.3%)
法律を聞いたことがない	1 (0.3%)

図１．　個人情報保護法への対応（2006 年 3 月）

既に対応終了	11 (2.5%)
既に対応をはじめた	136 (30.8%)
現在未対応、今後対応予定	145 (32.9%)
現在未対応、今後は検討中	59 (13.4%)
対応は検討していない	37 (8.4%)
法律の内容は知らない	48 (10.9%)

図２．　個人情報保護法への対応（2005 年 3 月）

個人情報保護法の厚労省ガイドラインへの対応についての質問では、小規模医療機関で「対応済み」が１７．６％、「対応中」は１８．７％である。「ガイドラインの存在を知らない」が７．８％で、「内容を知らない」が１８．７％という結果だった。

大規模医療機関では、「対応済み」は５７．９％、「対応中」は２９．２％で、大規模医療機関のほとんどが対応をおこなっているということになる。

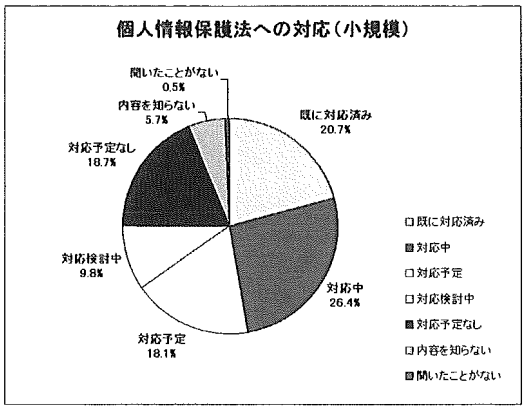

図３．　小規模機関の厚労省ガイドラインへの対応状況　（2006 年 3 月）

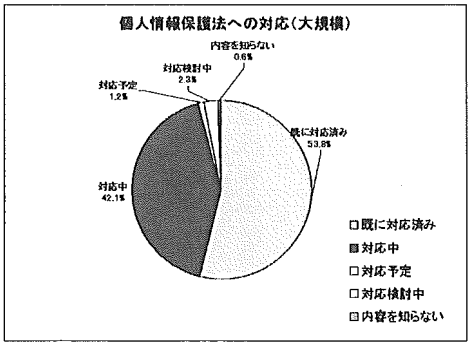

図４．大規模機関の厚労省ガイドラインへの対応

状況　（2006年3月）

なお、昨年度の結果は、次の図の通り、小規模機関では「対応済み」「対応中」が９．３％、「今後対応予定」を含めると５２．８％で、一方で「ガイドラインを知らない」が３５．９％であった。大規模機関では「対応済み」３．９％「対応中」が４９．５％、「今後対応予定」を併せると９４．６％であった。

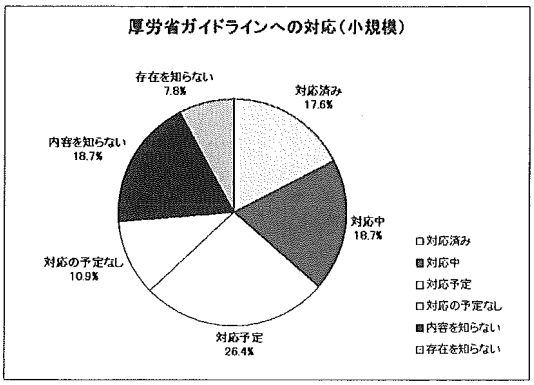

図５．小規模機関の厚労省ガイドラインへの対応状況（2005年3月）

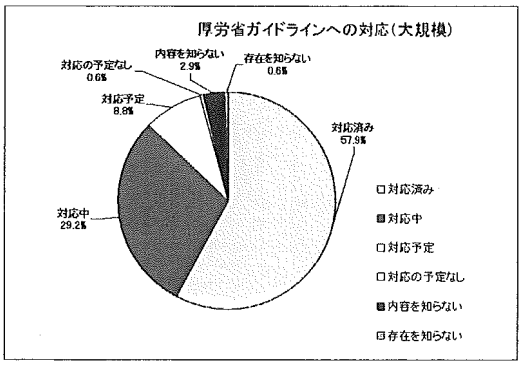

図６．大規模機関の厚労省ガイドラインへの対応

状況（2005年3月）

厚労省が昨年３月に出した安全管理ガイドラインへの対応についての質問は、小規模医療機関では「存在を知らない」「内容を知らない」が６３．６％、一方で「対応済み」は９．１％であった。

また、大規模医療機関では「存在を知らない」「内容は知らない」が３９．１％、「対応済み」は２２．５％であった。

このガイドラインは、何らかの情報システムを導入している医療機関はすべて対象となる。ここでの何らかの情報システムとは、オーダリングシステムや電子カルテシステムだけでなく、パソコンやワープロ、プリンタやスキャナを含んでおり、現在の医療機関で導入していない機関はないと思われるが、大規模医療機関でさえ、ガイドラインを知らない機関が１６％あり、小規模医療機関の過半数で、内容および存在をしらないと答えているのは、やはり周知不足ではないかと思われる。（図７、図８）

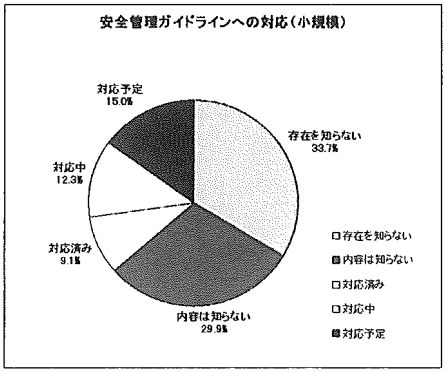

図７．小規模機関の安全管理ガイドラインへの対応状況　（2006 年 3 月）

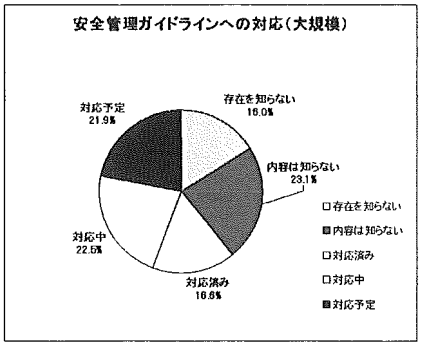

図８．大規模機関の安全管理ガイドラインへの対応状況　（2006 年 3 月）

個人情報保護の取り扱いに関する院内掲示物についての質問では、大規模機関の場合、

「自医療機関で作成」３３件（２１．４%）、「医師会などを作成したものを雛形に再作成」８９件（５７．８%）、「医師会などが作成したものをそのまま使用」が３１件（２０．１%）、「未作成」が１件（０．６%）。一方で小規模医療機関の場合は、自医療機関で作成が４件（２．８%）、「医師会などを作成したものを雛形に再作成」が１４件（９．９%）、「医師会などが作成したものをそのまま使用」は８７件（６１．７%）、「未作成」が３６件（２５．５%）となっている。

これらは昨年度の状況は、「未作成」が、大規模機関でも２６．５%で小規模機関では６２．５%であったため、例え医師会や病院団体が作成したものをそのまま利用しているとはいえ、かなりの機関が個人情報の取扱いに関しての院内掲示を実施していることは、１年経過した現在も対応が進んだといえると考える。

また、大規模機関の過半数が、医師会などが作成したものを雛形に自医療機関向けに再作成したということであり、この結果から、医師会や病院団体が雛形を作り公開したことは大変意味のあることだと考える

C-3. 医療情報システムの安全管理のためのガイドラインの調査

C-3-1 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、医療情報誌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。

C-3-2 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。

C-3-3 安全管理 GL 概説

C-3-3-1　概観と構成

安全管理 GL は 100 ページを超える指針であり、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あげ、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-文書法の実施にともな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、それぞれの法令にしたが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きわめて重要で、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章、7章、8章、9章、10章については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ヶ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。

C-3-3-1　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あげている。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 9 個の項目にわけて記載している。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。

6.3~6.7 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、実験的又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。

C-3-3-3　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-文書法の実施にともな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、イラストもそえられている。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（本稿執筆時点で予定）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及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と付与すること、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たおこな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。

C-3-3-4　診療録及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」にともな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 Auditor6)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 は民間団体である ISACA が認定する監査資格であるが、国際的に評価が高い。

C-3-3-5　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、それにともな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、300dpi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」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。

C-3-3-6　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あげ、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。

付表は 6 カラムからなる表で、10 章であ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あげ、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あげている。管理項目ごとに、みずか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。

C-3-4 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きわめて重要な問題で、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、細心の運用をおこなっても安全管理は 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。