どちらにあるかは定めていない。もし、全ての材料を請負人が用意したのであれば、完成された物の所有権は請負人にある。実際に完成した物の注文者への引き渡しは売買と見なされる。請負契約であれ売買契約であれ、引き渡しの際に瑕疵(不具合、バグ、故障)が有れば注文者は補償を求める事ができる。また、引き渡し後の一定期間(一般的には１年)も同様に瑕疵についての補償を求められる。

瑕疵有無の判断の基準となるのは、契約時に何らかの形で行われた合意(仕様書や検査証など)である。この合意を満たしているのであれば、完成された物が注文者の意図に沿っていなかったり、何らかの問題が有ったりしても瑕疵とは認定されない。実際、民法６３６条は請負契約において注文者の指図に原因があって瑕疵が生じた場合、請負人は担保責任を負わないことが書かれている。ただし、請負人が専門家として注文者の指図の不適当なことを知っていてこれを注文者に告げなかった場合は請負人が担保責任を負うとも書かれている。しかし、医療情報システムにおいては医療の特殊性／専門性が極めて高いため、情報技術の専門家に対して仕様書の医療の面から見た不適当さの指摘を求めるには限界があると考えざるを得ない。

売買契約として購入する場合においても、販売者が提示する仕様書に基づいて購入するか否かを決めるわけであり、購入者が自らの目的を達成可能かどうか判断するのは購入者の責任である。メーカの書いた仕様書を理解し判断するのは、自らの要求を仕様書に記述する以上に高度の知識と洞察力が必要であろう。

仮に、非常に複雑な情報システムである電子カルテの仕様を厳密に記述するとなれば、それこそ百科辞典か長編小説になってしまうだろう。一方、曖昧な仕様書で無理やりに合意する事で、注文者が納入後に気づいた不満な点を瑕疵と認定し、それへの補償であるとしてシステムの修正を要求するというやりかたも事実上は不可能ではない。この場合は「○×業務支援機能を有すること」と仕様書に一筆入っていればよいのである。○×機能支援機能が厳密に定義されていないのであれば、○×業務を行う上での不満の解消は全て瑕疵であると主張することができる。このやりかたは、仮に請負人が不服を申立てて裁判となれば、機能の認定や仕様書の合意の過程等が論点となるが、簡単に決着がつくことはないだろう。実際、このような裁判が行われることは稀である。

実際に行われている電子カルテやオーダー・エントリー・システムの調達では個々の機能が一筆で記述された仕様書が取り交わされていると考えられる。一筆型の仕様書に基づいた導入は電子カルテメーカ、医療機関の双方に問題をもたらす。電子カルテメーカは、納入後の(瑕疵の補修としての)改造要求に応える為の費用をあらかじめの納入価格に保険として上乗せしておかなければならない。このため、電子カルテの価格は高騰することになる。一方、医療機関側は納入された時点では、要求を完全に満たすものを手にする事ができない。その上、稼働後のシステムの改造は一般的にはシステムを複雑かつ不安定なものにしてしまう。高い電子カルテを導入したにも関わらず、思った通りの動きはしないしバグだらけだ、という声の原因ではないかと考えられる。

３．２　医療機関における情報システム部門の不在

有る程度の規模の企業には専任スタッフによる情報システム部門があり、電子カルテやオーダー・エントリー・システムのような組織の根幹業務を支援する大規模な情報システムの導入において、開発やプロジェクトの指揮／管理、そして導入後の保守を行うのが普通である。しかし、大学病院や大規模な医療法人を除けば医療機関に情報システム部門は存在しない。また、大学病院の医療情報部にしても研究組織という側面もあり純粋に情報システム部門とは言い切れない。

通常、情報システム部門を持たない医療機関における電子カルテやオーダー・エントリー・システムを導入する場合、診療科や診療部門から担当者を集めワーキング・グループや委員会等の形で１年から３年程度の期間をかけて仕様の検討が行われる。

このような体制では、電子カルテの要件について科や部門からの個別の要求はあがるが組織全体としての戦略的な視点で仕様をまとめることは困難である。また特に医師などは頻繁に医療機関を異動するため、長期的な戦略に責任を負うことができない。例えば、ある部門の責任者が「部門体制の編成が間に合わないので今回は部分的な電子化にとどめ、全面的なシステム化は次回の調達に見送る」といったような戦略的な判断をすることができない。

前節の仕様書についての議論からもわかるように、情報技術に関する知識だけでなく企画力や交渉力をもった専任スタッフをもたない医療機関にとって、電子カルテの導入はまさにギャンブルである。

３．３　エンタープライズ・アーキテクチャ＋医療情報技師＋IT アウトシーシング＝プロセスとしての電子カルテ導入

現状の資材調達型の導入方式と医療機関の情報システム部門不在という問題が残される限り、どんなに優れた仕様や実装の電子カルテが開発されたとしても、導入の過程は難航し導入後も十分な効果を引き出すのは困難であると考えられる。なぜなら、これらは非技術的側面の問題であって、技術的側面である情報技術はこれらを解決することができない。

この問題を解決する一つの方法は、電子カルテの導入を一過性の「イベント」としてとらえるのではなく「プロセス(工程、過程)」ととらえる事である。プロセスには、それを導く枠組が必要であり、また、プロセスを実行する人的資源が継続的に必要である。そこで、枠組としてエンタープライズ・アーキテクチャ、人的資源として医療情報技師と IT アウトソーシングを活用することを提案する。

３．３．１　エンタープライズ・アーキテクチャ(再訪)

エンタープライズ・アーキテクチャは資材調達型の情報システム導入の弊害に対応することが出来ることから、米国連邦政府の電子政府化政策における枠組の核となったものであり、医療機関にとっても有効と考えられる。ただし、エンタープライズ・アーキテクチャを策定するにはかなりの人的資源が必要となる。その一つの例が米国連邦政府エンタープライズ・アーキテクチャの中で配布されているガイドライン[5]に示されている。少なくとも情報責任者(Chief Information Officer, CIO)が必要であり、その他にも業務の分析やプランニングをするアーキテクトが必要となる。通常、医療機関は医師やコメディカル等の医療従事者と事務職員と施設管理職員だけで構成され、常勤の情報管理職員が置かれることはまずない。電子カルテやオーダー・エントリー・システム 等の大規模な情報システムの導入費用を考えると、情報システムを効果的に導入／運用ができるのであれば、そういった情報管理職員の人件費は決して無駄では無いと考えられる。

３．３．２　医療情報技師

今まで、医療機関に情報技術や情報システムあるいは情報の管理を担当する専任かつ常勤の職員が置かれなかった理由は、大規模な情報システムの導入が一般的ではなかったためそのようなスタッフの必要性が無いと考えられていたこともあるが、それだけでなく一体どのようなスキルをもった人間を雇用すれば良いのか基準が無かったことも考えられる。とりわけ、医療機関は資格を持った人間によって構成されている非常に特異な組織であり、情報技術者という資格の無い専門家を雇用するという考え方自体が馴染まない。

日本医療情報学会では、平成１５年より医療情報技師の育成事業を始めた。これは厚生労働省による「保健医療分野の情報化に向けてのグランドデザイン」を達成する為には必要な技術者を育成する事が急務とされたからである。医療情報技師とは「保健医療福祉専門職の一員として、医療の特質をふまえ、最適な情報処理技術にもとづき、医療情報を安全かつ有効に活用・提供することができる知識・技術および資質を有する者」であり、そのような専門家を能力認定しようとういう制度である。「技師」とはついているが臨床放射線技師や臨床検査技師のような「資格」ではないが、雇用時の一つの明確な基準とすることができる。

医療情報技師の育成は始まったばかりの事業であるため、講習や検定の内容はこれから更に検討が加えられていくものであるが、エンタープライズ・アーキテクチャを行うために必要な能力として企画力や交渉力の養成が加えられることを期待する。医療情報技師はコンピュータオタクであってはならない。

３．３．３　ITアウトソーシング

エンタープライズ・アーキテクチャは継続的に行うものではあるが、電子カルテ導入時のような大人数のスタッフが常時必要なわけではない。したがって、何人ものスタッフを抱える情報システム部門を維持する必要は無くアウトソーシングを行うべきである。

アウトソーシングは業務の外注や要員の派遣とは異なったものである。業務の外注は請負契約((民法 632 条)であり仕事の結果について代価を支払うものであって、作業の過程について指揮することはできない。一方、要員の派遣については作業の過程について指揮する権利(義務)が得られるが結果については保証されない。どちらも依頼する側に大きなリスクがある。アウトソーシングは言うならばこれらの中間的なものであり依頼側が一方的にリスクを負うことが無く、受注側もスケールメリットや専門性による利益が得られるように留意した形態での業務委託の契約をするものである。業務の外注という見地からみれば、小さな単位の仕事(サービス)を継続的反復的に外注している状態であり、大きな単位での請負にある仕様書のリスクが負わなくて良い。要員の派遣という見地からみると、指揮の責任を負わなくて良いが、細かい指示をすることができる。

医療機関では小数の医療情報技師による情報システム部門を CIO として機能させ、高度な情報技術を要する分析や設計などの業務、或は、情報システムの保守などをアウトソーシングするのが効率的と考えられる。アウトソーシング・ベンダは情報システムの納入業者とは中立的であることが望ましい。

３．３．４　情報技術選択との関係

エンタープライズ・アーキテクチャにおける情報技術選択は戦術的ではなく戦略的なものになる。従来型の情報システムの開発／導入では「情報システムのこの機能を実現するにはこういう情報技術が必要である」が選択の基準であり短期的かつ局所的(即ち戦術的)判断であった。したがって、個々の情報システム開発時の判断によって情報技術が選択され、同じ組織内の情報システム間で互換性や接続性の問題を引き起こしていた。しかし、エンタープライズ・アーキテクチャでは情報技術は組織の資産と見なされるため長期的かつ組織横断的(即ち戦略的)判断により選択され、個々の情報システムの要求によって左右されるものではない。

医療機関における情報技術の選択は、外来重視の経営か入院患者重視の経営か、特定疾患専門か総合診療、検査や給食、医療事務等の外注化を進めるか否かなどの病院運営の方針から導き出されるべきであって、システム開発に用いるツールや開発者の判断によってなされるべきではない。今後の課題として、医療施設運営(経営)の各種の特性と情報技術との関係についての分析が必要となる。これはまさに医療機関におけるエンタープライズ・アーキテクチャの枠組と各種参照モデルを開発する作業である。

４．まとめ

情報技術選択について、選択のもととなる分類のモデルについて検討を行った。また、医療機関における情報システムの導入の問題について検討を行った。この二つは直接的には関連の無い事項の考察において、どちらもエンタープライズ・アーキテクチャがキーとなることが示された。エンタープライズ・アーキテクチャは情報技術技術者だけでなく医療機関の運営を改善していく上で重要と考えられる。エンタープライズ・アーキテクチャはまだ新しい考え方であり今後の研究成果が期待される。特に医療分野への適用についての研究が進められることが期待される。

Bibliography

[1] John A Zachman. A Framework for Information Systems Architecuter. IBM Systems Journal. VOL. 26. NO. 3. 276-286. 1987.

[2] John F Sowa and John A Zachman. Extending and formalizing the framework for information systems architecture. IBM Systems Journal. VOL. 31. NO. 3. 590-616. 1992.

[3] CIO Council. Federal Enterprise Architecture Framework Version 1.1. September 1999. http://www.cio.gov/archive/fedarch1.pdf

[4] Federal Enterprise Architecture Program Management Office. The Technical Reference Model (TRM) Version 1.1. August 2003. http://www.feapmo.gov/resources/fea_trm_release_document_rev_1.1.pdf

[5] CIO Council. A Practical Guide to Federal Enterprise Architecture Version 1.0. February 2001. http://www.cio.gov/archive/bpeaguide.pdf

平成 15 年度厚生労働科学研究
標準的電子カルテシステムのアーキテクチャ（フレームワーク）に関する研究
総括研究報告書

(資料８)

電子カルテシステムの電子保存対応要件の検討

————目次————

１．はじめに

JAHIS セキュリティ委員会において、「標準的電子カルテにおけるセキュリティ機能要件」について検討した結果について紹介する。

２．基本的な考え方

Common Criteria（ISO/IEC15408）の考え方に従えば、セキュリティの機能要件は下記の手順によって導出されるべきものである。

(1) 業務モデル策定
(2) 保護対象資産の決定
(3) 脅威分析
(4) セキュリティポリシーの策定
(5) セキュリティ対策の立案（機能要件の抽出）
(6) 保証要件の抽出

今回の厚生科学研究標準的電子カルテ関連研究班からの要望に関しては、まずは具体的なモデル策定がされないと厳密な意味でのセキュリティ機能要件の抽出はできない。したがって、依頼元に対しては、「まず業務モデルを確定してください。セキュリティ機能要件の抽出はそれを元に行います。」とお願いすることになる。しかし、医療情報システム（主に電子カルテ）においては、「電子保存」という必須要件が厳然と存在するので、セキュリティに関する最低限の要件は、ここから導出されるはずであると考えた。以降にそれを示す。

３．電子保存から導出されるセキュリティ機能要件

MEDIS-DC によるガイドラインは、電子保存を行う際の機能要件と管理要件をまとめたものと考えられる。このうち、機能要件については「システムが備えるべき機能」と「システムの機能とは明記せず運用も含めて実現すればよい機能」の２種類が混在して読み取れるが、これらをまとめて機能要件と考える。また、機能実装と実運用の観点から見ると、各機能要件は複数の機能要件から構成されていると読み取れる。

そこで、この電子保存からセキュリティ観点での機能要件を抽出するため、下記の作業を行うことを考えた。

１）MEDIS-DC ガイドラインの機能要件をアトムレベルに細分化する
２）細分化した機能要件のうち、セキュリティに特化されるものを識別する

この結果を参考資料にまとめた。

この資料においては、機能要件として言及している元の文章を「原文」とし、それをアトムレベルの機能要件に分解した。これらのうち、セキュリティに該当すると考えられる項目に色（水色）をつけて識別した。この水色をつけた項目が、電子保存を行うための最低限の機能要件であると考えらる。

４．今後の課題

「電子保存」は診療録の保存について言及したものであり、そこに蓄えられた情報の活用についての言及はない。元より電子カルテを行う重要な目的の１つに「情報の活用」があるから、これが抜けていることは問題である。ただ、これを考慮するためには「電子カルテ」の業務モデル策定が先決であり、これを行った後で、上記の手順を踏んで機能要件を抽出していきたいと考える。

今後、本件の基本的な考え方の吟味をしていき、さらには参考資料の機能要件のリストアップとセキュリティ要件の選択について検討していく必要がある。

以上

原文	3.3-1(1) 作成責任者（入力者と作成責任者が異なる場合は入力者も）の識別及び認証（ID・パスワード等）が行われるこ
1	システムの利用者を登録し、それを識別子（ユーザID）で管理すること
2	システムの利用者の識別子（ユーザID）に対して、本人を認証すること
3	利用者本人を認証するための情報が、利用者以外に不正に使用されることのないように対策されていること
4	正当な利用者以外が不正にシステムを利用した場合、それを検知または追及すること

原文	3.3-1(2) 作成責任者による入力の完了、代行入力の場合は作成責任者による確認の完了、及び一旦確定した情報の作成責任者本人及び作成共同責任者による情報の追記、書き換え及び消去等の責任を明確にするために「確定」操作が
1	直接入力と代行入力を区別して管理すること
2	代行入力の場合は作成責任者による確認を行えること
3	作成責任者と作成共同責任者を区別して管理すること
4	一旦確定した情報への追記、書き換え及び消去等の操作を行えること
5	情報入力（新規、追記、書き換え、消去等）の際に確定操作が行われること

原文	3.3-1(3)「確定」操作に際し、その作成責任者の識別情報が記録情報に関連付けられること。
1	確定操作毎に作成責任者の識別情報が記録されること
2	確定操作毎に情報入力者の識別情報が記録されること

原文	3.3-1(4) 一旦確定された情報は、後からの追記・書き換え・消去の事実を正しく確認できるよう、当該事項の履歴が保存され、その内容を容易に確認できること。
1	情報の記録に際し、履歴を保存すること
2	履歴の内容が容易に確認できること

原文	3.3-2 過失による誤入力、書き換え、消去及び混同は、単純な入力ミス、誤った思い込み、情報の取り違えによって生じるが、内容的に明らかな過失であっても技術的に過失と認識することが困難な場合が多い。したがって、確定操作を行う前に十分に内容の確認を行うことを運用規定等に定めることが望ましい。
1	確定操作の際に情報の記載内容を容易に確認できること

原文	3.3-3 虚偽入力、書き換え・消去・混同は、不適切な機器・ソフトウェアの使用によって発生する可能性がある。従って、機器やソフトウェアの導入及び更新に際して、医療機関が自らその品質管理を行うこと。
1	システムの機能定義と動作保証がなされていること（Common Criteriaにおける保証要件に該当）

原文	3.3-4 第三者の責任ある人への成りすましによる虚偽入力、書き換え、消去及び混同に対しては、少なくとも責任者の識別・認証等により防止すること。なお、責任ある人の不正の意を持った虚偽入力及び改竄（確定された情報に対する書き換え、消去、混同）は、もとより違法行為である。
1	該当なし

原文	4.(1) 分散された情報であっても、患者別等の情報の所在が可搬型媒体を含めて管理されていること。
1	情報の所在が可搬型媒体を含め管理されていること

原文	4.(2) 保存情報を見読するための手段が対応付けられて管理されていること。そのために保存情報に対応した、機器、ソフトウェア、関連情報等が整備されていること。
1	保存情報を見読するための手段が対応付けられて管理されていること

原文	4.(3) 情報の確定状態、利用範囲、更新履歴、機密度等に応じた管理区分を設定し、アクセス権等を管理すること。
1	管理区分（情報の確定状態、利用範囲、更新履歴、機密度等）を設定できること
2	管理区分に応じたアクセス権を設定し、管理できること

原文	4.(4) 運用手順を明確にし適切で安全なシステムの利用を保証すること
1	該当なし

原文	4.(5) システムに対するアクセス権限の割り当てを制御するため、利用者管理の手順を明確にすること。利用者の管理手順では、利用者の登録から抹消までの利用者の状況の変化に応じたアクセス権限の変更を可及的速やかに行うこと。
1	アクセス権限の変更を可及的速やかに行う手立てが用意されていること

原文	5.(1) 記録媒体の劣化する以前に情報を新たな記録媒体に複写すること。
1	情報を新たな記憶媒体に複写できること
2	任意のタイミングにおいて複写操作を実施できること

原文	5.(2) いわゆるコンピュータウィルスを含む不適切なソフトウェアによる情報の破壊・混同が起こらないようシステムで利用するソフトウェア、機器及び媒体の管理を行うこと。
1	コンピュータウィルス等による攻撃に対処可能なシステム構成（例：メーカがサポートを打ち切ったバージョンでない）であること

原文	5.(3) システムの変更に際して、以前のシステムで蓄積した情報の継続的利用を図るための対策を実施すること。なお、システム導入時にデータ移行に関する情報開示条件を明確にすること。
1	情報の蓄積方法が隠蔽化されていないこと

原文	5.(4) 故意又は過失による情報の破壊が起こらないよう情報保護機能を備えること。また、万一破壊が起こった場合に備えて、必要に応じて回復できる機能を備えること。
1	情報のバックアップを定期的に行いうること
2	人為的、もしくはプログラムの暴走等による情報の広範囲の破壊を検知し、防止できること

原文	6. 電子保存された情報の効率的な相互利用を可能とするために、システム間のデータ互換性が確保されることが望ましい。効率的な相互利用とは、同一施設内又は異なる施設間で複数のシステムが存在する場合、それぞれのシステム内の情報を交換して、より効率的な情報の利用を行うことをいう。なお、異なる施設間で情報の交換を行う場合には、契約等により責任範囲を明確にし、管理の責任の所在を明らかにする必要がある。
1	他システムとデータ交換を行うためのインタフェース機能を備えること
2	情報のコード等の体系が外部に公開可能な形式となっていること

原文	7. 各施設にあった運用管理規程を作成し、遵守すること。なお、運用管理規程にはシステム導入に際して、「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関する基準」を満足するために技術的に対応するか、運用によって対応するかを判定し、その内容を公開可能な状態で保存する旨の規定を盛り込むこと。
1	システムの機能仕様が明確に定義されていること

原文	8. 管理者は利用者にプライバシー保護意識の徹底を図り、運用上のアクセス権を設定し、プライバシー侵害の恐れがある場合には、調査し適切な対応を行わなければならない。
1	アクセス権侵害に関する監査証跡を保存する機能を備えること

原文	（参考）① 電子データの存在自体を立証する場合は、非供述証拠であり、刑事訴訟法上の伝聞法則　の適用はなく、したがって、要証事実との関連性が立証できれば証拠能力が認められる。通常、プリントアウトした書面を証拠として提出することになるため、電子データの内容　が正確に出力されていることの立証が必要とされている。また、電子データの内容の真実性を立証する場合は、供述証拠であり、文書に準ずるも　のと考えられることから、証拠能力が認められるためには、要証事実との関連性に加え、　刑事訴訟法上の伝聞法則の例外が認められるための要件の具備が必要とされている。この場合、商業帳簿等業務の通常の過程において作成された書面については、一般に業務の遂行に際して規則的、機械的かつ継続的に作成されるもので、作為の入り込む余地が少なく、正確に記載されるものと一般に期待されていることから、証拠能力が認められている。これ以外の書面についても特に信用すべき状況の下に作成されていることが認められれば、証拠能力が認められるが、商業帳簿等と同様に信用性の高い書面であることが必要とされている。さらに、証明力については裁判官の自由な判断に委ねられているが、その判断は電子データの正確性等の評価に依存するものとされている。以上から、電子データの証拠能力及び証明力の確保については、データの入力及び出力の正確性を確保するとともに、データの改変の可能性を減殺することなどにより電子データの信頼性を高め、かつこれに対する責任の所在を明かにする必要がある。そのためには、書類の内容、性格に応じた電子データの真正性、見読性及び保存性の確保措置を構ずる必要がある。なお、紙で作成又は受領した証ひょう類の電子化については、紙に記録される紙質、筆跡等の情報が電子データには記録されないため、犯罪捜査・立証上問題が多いと指摘されており、電子データによる保存を認めるに当たっては、その点に十分配意する必要がある。
1	電子データの内容を正確にプリントアウトする機能を備えること
2	データ改変の可能性を減殺する機能を備えること

原文	（参考）② 民事訴訟においては、証拠能力についての制限はなく、また、証明力については裁判官の自由な判断に委ねられている。電子データによって保存された書類を証拠とする場合、その証明力の判断においては、データの入力及び出力の正確性、データの改変の可能性が問題となり、電子データの信頼性を高め、かつこれに対する責任の所在を明らかにすることが必要であるが、この点については、書類の内容、性格に応じた電子データの真正性、見読性及び保存性の確保措置を講ずる必要がある。なお、書類の電子データによる保存の認容をどの程度とするかは、そのデータにより証明しようとする事柄についての検証責任を官と民のいずれが負担するかについても関係するので、その点も踏まえ、検討することが必要である。
1	電子データの責任の所在を明らかにする機能（署名等）を備えること

平成 15 年度厚生労働科学研究
標準的電子カルテシステムのアーキテクチャ（フレームワーク）に関する研究
総括研究報告書

(資料９)

電子カルテシステムの個人情報保護対応要件の検討

――――目次――――

１．OECD の個人情報保護 8 原則

1980 年、OECD は「プライバシー保護と個人データの流通についてのガイドラインに関する理事会勧告」を採択した。以下に勧告された８原則を示す。訳は外務省の web ページの訳をベースにしている。

(1)収集制限の原則
個人データの収集には制限を設けるべきであり、いかなる個人データも、適法かつ公正な手段によって、かつ適当な場合には、データ主体に知らしめ又は同意を得た上で、収集されるべきである。

(2)データ内容の原則
個人データは、その利用目的に沿ったものであるべきであり、かつ利用目的に必要な範囲内で正確、完全であり最新なものに保たれなければならない。

(3)目的明確化の原則
個人データの収集目的は、収集時よりも遅くない時点において明確化されなければならず、その後のデータの利用は、当該収集目的の達成又は当該収集目的に矛盾しないでかつ、目的の変更毎に明確化された他の目的の達成に限定されるべきである。

(4)利用制限の原則
個人データは、明確化された目的以外の目的のために開示利用その他の使用に供されるべきではないが、次の場合はこの限りではない。
(a)　データ主体の同意がある場合、又は、
(b)　法律の規定による場合

(5)安全保護の原則
個人データは、その紛失もしくは不当なアクセス、破壊、使用、修正、開示等の危険に対し、合理的な安全保護措置により保護されなければならない。

(6)公開の原則
個人データに係わる開発、運用及び政策については、一般的な公開の政策が取られなければならない。個人データの存在、性質及びその主要な利用目的とともにデータ管理者の識別、通常の住所をはっきりさせるための手段が容易に利用できなければならない。

(7)個人参加の原則
個人は次の権利を有する。

(a) データ管理者が自己に関するデータを有しているか否かについて、データ管理者又はその他の者から確認を得ること
(b) 自己に関するデータを、
(i) 合理的な期間内に、
(ii) もし必要なら、過度にならない費用で、
(iii) 合理的な方法で、かつ、
(iv) 自己に分かりやすい形で、
自己に知らしめられること。
(c) 上記 (a) 及び (b) の要求が拒否された場合には、その理由が与えられること及びそのような拒否に対して異議を申立てることができること。
(d) 自己に関するデータに対して異議を申立てること、及びその異議が認められた場合には、そのデータを消去、修正、完全化、補正させること。

(8)責任の原則
データ管理者は、上記の諸原則を実施するための措置に従う責任を有する。

現在、世界各国で制定される個人情報保護に関する法令等は、このOECDのガイドラインに示された基本原則に基づいたものとなっており、日本の「個人情報の保護に関する法律」においても同様である。

２．日本における個人情報保護

２．１　個人情報の保護に関する法律

日本においては平成15年5月30日に「個人情報の保護に関する法律」が公布された。第４章から第６章までの規定は、公布後２年以内に施行されることとなっていたが、平成17年4月より施行されることが決定した。この法律は「個人情報の有用性に配慮しつつ、個人の権利利益を保護」することを目的にしており、個人情報を有効活用するための法律という位置付けになっている。その上で、個人情報を取り扱う上での基本理念として「個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものであり、その適正な取扱いが図られなければならない。」とうたっている。

「個人情報の保護に関する法律」における言葉の定義は以下のようになっている。

「個人情報」…生存する個人に関する情報（識別可能情報）

「個人情報データベース等」…個人情報を含む情報の集合物（検索が可能なもの。一定のマニュアル処理情報を含む）

「個人情報取扱事業者」…個人情報データベース等を事業の用に供している者（国、地方公共団体等のほか、取り扱う個人情報が少ない等の一定の者を除く）

「個人データ」…個人情報データベース等を構成する個人情報

「保有個人データ」…個人情報取扱事業者が開示、訂正等の権限を有する個人データ

医療機関の殆どは上記の「個人情報取扱事業者」に該当することになると思われるため、「個人情報取扱事業者の義務」が課せられることとなる。
（個人情報取扱事業者の義務については次節で詳細に記述する）

また、適用除外についても定められており、学術研究に利用する場合の学術研究機関等の利用においては「安全管理、苦情処理等のために必要な措置を自ら講じ、その内容を公表するよう努力」することを前提に適用が除外されることとなっている。（なお、適用除外は他に報道、著述、宗教活動、政治活動にも認められているが、対象は報道機関、著述業、宗教団体、政治団体を対象としているため本節では言及しない）

罰則規定については、個人情報取扱事業者が主務大臣の命令に違反した場合等における罰則が定められており、六ヶ月以下の懲役または30万円以下の罰金となっ

ている。これは違反行為をした行為者を罰するのみならず、法人に対しても罰金刑が課されることとなっている。

２．２　個人情報取扱事業者の義務規定

「個人情報の保護に関する法律」の第４章第１節には個人情報取扱事業者の義務等に関する規定が盛り込まれている。これらの項目はOECDの個人情報保護８原則と対応付けがなされており、「個人情報の保護に関する法律」がOECDの個人情報保護８原則に則っていることを示している。

(1)　利用目的の特定、利用目的による制限（15条、16条）
・個人情報を取り扱うに当たり、その利用目的をできる限り特定
・特定された利用目的の達成に必要な範囲を超えた個人情報の取扱いの原則禁止

(2)　適正な取得、取得に際しての利用目的の通知等（17条、18条）
・偽りその他不正の手段による個人情報の取得の禁止
・個人情報を取得した際の利用目的の通知又は公表
・本人から直接個人情報を取得する場合の利用目的の明示

(3)　データ内容の正確性の確保（19条）
・利用目的の達成に必要な範囲内で個人データの正確性、最新性を確保

(4)　安全管理措置、従業者・委託先の監督（20条～22条）
・個人データの安全管理のために必要かつ適切な措置、従業者・委託先に対する　必要かつ適切な監督

(5)　第三者提供の制限（23条）
・本人の同意を得ない個人データの第三者提供の原則禁止
・本人の求めに応じて第三者提供を停止することとしており、その旨その他一定の事項を通知等しているときは、第三者提供が可能
・委託の場合、合併等の場合、特定の者との共同利用の場合（共同利用する旨その他一定の事項を通知等している場合）は第三者提供とみなさない

(6)　公表等、開示、訂正等、利用停止等（24条～27条）
・保有個人データの利用目的、開示等に必要な手続等についての公表等
・保有個人データの本人からの求めに応じ、開示、訂正等、利用停止等

(7)　苦情の処理（31条）
・個人情報の取扱いに関する苦情の適切かつ迅速な処理

(8)　主務大臣の関与（32 条～35 条）
・この節の規定の施行に必要な限度における報告の徴収、必要な助言
・個人情報取扱事業者が義務規定（努力義務を除く）に違反し、個人の権利利益保護のため必要がある場合における勧告、勧告に従わない一定の場合の命令等
・主務大臣の権限の行使の制限（表現、学問、信教、政治活動の自由）

(9)　主務大臣（36 条）
・個人情報取扱事業者が行う事業等の所管大臣。規定の円滑な実施のために必要があるときは、内閣総理大臣が指定

２．３　本人の関与について

保有個人データに関する本人の関与については第 24 条から第 27 条において規定されている。特に開示ルールについては医療分野において適用除外にあたるケースが救急医療現場などにおいて頻繁に発生すると考えられる。

(1)利用目的の通知（第24条第2項）
保有個人データがどのような目的で利用されているのかについて、原則として、本人に通知しなければならない。

(2)開示（第25条第1項）
保有個人データについて、原則として、本人に開示しなければならない。
（開示しないことができる場合の例）
① 本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
② 個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合など

(3)訂正等（第26条第1項）
保有個人データの内容が事実でないときは、利用目的の達成に必要な範囲内において、訂正等を行わなければならない

(4)利用停止等（第27条第1項、第2項）
①利用目的による制限、②適正な取得、③第三者提供の制限に違反していることが判明したときは、違反を是正するために必要な限度で、原則として、利用停止等を行わなければならない。

３．電子カルテシステムとしての機能要件抽出の考え方

２章で述べたことは、個人情報取扱事業者としての要件であり、電子カルテシステムとしての要件にはなっていない。実際には個人情報取扱事業者の経営者が情報セキュリティマネジメントの観点から適切なリスクアセスメントを実施し、それを受けた総合的な対策のなかの一部として電子カルテシステムにおける技術的対策が実施されることとなる。そのため電子カルテシステムの機能要件は厳密にはリスクアセスメントを実施してその詳細管理策を策定しなければ導出されない。

３．１　情報セキュリティマネジメント

情報セキュリティマネジメントとは事業リスクに対するアプローチに基づいて情報セキュリティの確立、導入、運用、監視、見直し、維持、改善をおこなうことである。対象は情報システムだけではなく、組織の構造および方針、事業計画、責任の所在、運用手順などが含まれる。情報セキュリティマネジメントの目標は情報セキュリティを確保することである。情報セキュリティを確保するためのアプローチとして情報セキュリティマネジメントシステム（ISMS）がある。ISMS は ISO/IEC17799 として国際規格化されている。ISMS はプロセスアプローチを使用しており、品質管理の規格である ISO/IEC9001 と同様に PDCA モデルが採用されている。その計画フェーズにおける手順は以下のようになっている。

STEP1　ISMS 適用範囲の決定
STEP2　ISMS 基本方針の策定
STEP3　リスクアセスメントの体系的な取り組み方法の策定
STEP4　リスク因子の特定、情報資産の洗い出し
STEP5　リスクアセスメントの実施
STEP6　リスク対応の決定
STEP7　管理目的と管理策の選択
STEP8　適用宣言書の作成
STEP9　残留リスクの承認と ISMS 実施の許可

この中で、電子カルテシステムの機能要件は STEP7 の管理目的と管理策の選択において明確化される。

３．２　管理目的と管理策の選択

ISMS では 10 のマネジメント領域を定めている。これらのマネジメント領域は大別すると組織的・管理的領域と技術的領域の二つに整理することが出来る。

（１）組織的・管理的領域

①セキュリティポリシ

経営者による組織横断的なセキュリティポリシの発行、及び支援について規定

②セキュリティ組織
セキュリティを確保するための組織作り（セキュリティフォーラムの設置など）について規定

③資産の分類および管理
組織の資産を保護するための資産目録や資産分類（極秘、部外秘など）について規定

④人的セキュリティ
人的な問題によるリスクを軽減するため、業務責任、採用時の審査、採用条件、教育などについて規定

⑤事業継続管理
各種障害（事故、災害などを含む）における回復対策、予防対策による事業継続管理（影響分析、継続計画など）について規定

⑥適合性
知的所有権、記録の保管、プライバシー保護など法的要求事項への準拠について規定やセキュリティポリシと技術準拠のレビュー（内部監査）について規定

（２）技術的領域

①物理的および環境的セキュリティ
入退出管理、施設(事務所、居室など)、装置の設置などのセキュリティについて規定

②通信および運用管理
情報処理システムの管理・運用を健全に実施するため、操作手順書の整備、運用の変更管理、セキュリティ問題管理、不正ソフトウエア対策、バックアップなどについて規定

③アクセス制御
情報へのアクセス制御、利用者のアクセス管理、特権管理、ネットワークにおけるアクセス制御などについて規定

④システム開発およびメンテナンス

健全な開発・運用のため、システムへのセキュリティ要件、アプリケーションプログラムに対するセキュリティ要件情報の秘匿・認証、暗号鍵の管理などについて規定

電子カルテシステムにおける機能要件はこの技術的領域の部分における管理目的を実現することになる。ここに至るまでには前節にて示したとおり、個人情報に関する情報資産を定義した上で、リスクアセスメントを実施しそこから導き出されたリスクに対する管理策を策定するという一連の作業が実施されていることが前提である。

４．来年度以降の課題

電子カルテシステムにおける個人情報保護要件を明確にするには、前述した個人情報取扱事業者としての義務規定を遵守しつつ、医療機関におけるセキュリティマネジメントシステムに適合する技術的対策を明確にする必要がある。勿論、個々の医療機関における要件は完全には一致しないものの、義務規定が明確であることから、各医療機関に共通の要件を洗い出して汎用的な技術的対策を導出することは不可能ではないと考えられる。厚生労働省による個別法もしくはガイドラインの策定などの個人情報保護に関する制度整備の進捗状況をみながら、対応を行っていく必要がある。情報資産の定義、医療機関の標準的な運用モデル（ベストプラクティス）などを明確に定義したうえで、リスクアセスメントを実施し、電子カルテシステムとしての技術的要件を明確化していくことが重要である。