3. 情報技術選択の非技術的側面

情報技術の選択を行う上では、選択対象としての情報技術自体の分析／評価だけでなく、情報技術を取り巻く環境としての非技術的側面についても検討が必要である。非技術的側面とは、技術参照モデルで示される各種の情報技術自体及び情報技術の基盤となる情報工学、計算機科学や数学等の技術的側面とは対照を為す、情報技術及び情報システムが存在する為に必要な環境に関する事項である。具体的には、情報技術が活用される情報産業の社会的経済的な構造、情報システムを導入する組織の構造や性質、それらに関連する行政や法規等である。この様な非技術的側面を無視／軽視した情報技術の選択は学術的なものでしかなく、実際の情報システムの開発／導入を誤った方向に導きかねない。

例えば、優れた能力をもった開発チームが顧客の要請で最先端の情報技術に基づいて電子カルテを開発したとする。しかし、保守チームがその技術を理解できず、かつ、その技術に対応した各種のツールが用意されていなければ、運用時に保守を受けることはできない。そのような電子カルテは車輪の無い飛行機のようなものであり、一度稼働して問題がなければ良いが、保守ができないため最後には墜落するしかない。対策として、開発チーム自らが保守まで行うようにすると、開発チームは保守に忙殺されて新製品や新たな技術の開発ができなくなり、開発チームはその製品と運命を供にすることになる。これは優秀な技術者の潜在的な成果を失うという意味で開発企業にとってだけではなく社会全体としても損失となる。

情報技術にはそれ自身の特性としてのメリット／デメリットがあるだけでなく、それを活用する環境においてのメリット／デメリットもあるということである。情報技術の選択に際してはそれが活用される環境との関係について、具体的に考慮せねばならない。この章では電子カルテに関わる非技術的側面についての関心を喚起するため、医療機関における電子カルテの導入における各種の問題点について検討を行う。

3.1. 資材調達型の導入方式の問題

既に多くの電子カルテやオーダー・エントリー・システムが医療機関に導入されているが、運用現場において少なからずクレームを聞く。この問題が情報システムの開発工程の質が低いことだけに起因するとは考えにくい。実際、日本の情報システム開発技術は世界的に高いレベルにあると評価されているのである。したがって開発工程以外にも何らかの原因があるのではないかと考えられる。

一般に情報システムの調達は、請負契約あるいは売買契約または両者の混合契約である製作物供給契約に基づく取引で行われていると見なされる。請負契約は厳密には、請負人が注文者から何らかの「仕事の完成」を請け負うものであって、完成された物の所有権が

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 Architecture. 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～16 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」
総合研究報告書

(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

本研究における昨年度の活動として、「標準的電子カルテシステム」におけるセキュリティ機能要件の定義に取り組んだ。ここではアプローチの手段として、厚生労働省から平成 11 年に発行されている「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ガイドライン」(以下、「電子保存のガイドライン」と省略する)の記述からセキュリティ機能要件に該当する項目を抽出し、そこからさらに機能実装上の要件と考えられる項目だけを抜き出すことを行った。抽出の対象に「電子保存ガイドライン」を選んだのは、非常に独自性が強くバリエーションの豊富な電子カルテシステムにおけるセキュリティを包括的に取り扱っている代表的な例であり、かつ政府主導で編纂された経緯から内容的にもよく吟味されたものとの認識があったからである。

「電子保存のガイドライン」はその名が示すように、診療録(カルテ)の保存だけに対象を絞っており、参照や保存情報の活用に関しては原則的に言及されていない。したがって、これを元に機能要件を導出しても参照に関する項目は含まれないので、この機能要件の欠落部分を補うことが次年度の課題となった。

このような状況の中、厚生労働省が主催する「医療情報ネットワーク基盤検討会」が招集され、その作業班によって「診療情報システムの安全管理に関するガイドライン」(以下、「安全管理のガイドライン」と省略する)が、従来の「電子保存」の刷新版として発行された。[1] この「安全管理のガイドライン」においては、「電子保存のガイドライン」では留意事項の扱いであった「患者の個人情報保護(プライバシ保護)」が最重要の要件として定義されており、この対策としてのアクセス制御と監査証跡が機能要件に挙げられた。そこで本年度の研究では、この「安全管理のガイドライン」を対象として、「電子保存のガイドライン」に行ったのと同様のアプローチで機能要件抽出を行うことにした。

「安全管理のガイドライン」を対象とすることで、「標準的電子カルテシステム」で言及されるべき多くの範囲がカバーされることになるが、「標準的電子カルテシステム」の機能モデルを明確に定義した上でのリスクアセスメントを実施しないと網羅的なアプローチとはならず、これは平成 15 年度の結論と変わらない。それでも、「安全管理」自体が医療機関で利用される情報システムを大掴みに想定して記述されているのでアプローチとしては近く、対象が増えた分だけより求めるものに近くなったと考えられる。

2. 基本的な考え方

一般にセキュリティ要件定義のアプローチとして、2 つの ISO 標準が参考になる。1 つはシステム製品自体が有するセキュリティ機能を管理するための「ISO/IEC 15408」(CC: Common Criteria

---

[1] 平成 17 年 3 月現時点ではまだ正式文書とはなっておらず、ドラフトとして公開意見募集中の状況である。

として知られ、以下 CC と省略する)、もう 1 つは情報システムを運用する組織における管理(情報セキュリティマネジメント)を対象とした「ISO/IEC 17799」(日本国内では ISMS:Information Security Management System として制度化されており、以下 ISMS と称する)がある。

ここではこれら 2 つの ISO について要点を説明する。これにより、「安全管理のガイドライン」から機能要件を抽出することの持つ意味が、より明瞭になると考える。

2.1. ISO/IEC 15408 の手法

情報システムの業務モデルを明確に定義した上で厳密なリスクアセスメントを行い、その結果から機能要件と保証要件を導出する手法である。具体的な手順は下記による。

(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

これは機能製品(システムも含む)の備えるべきセキュリティ機能を実装する上で、現存する最も洗練された網羅的なアプローチであると言えるが、業務モデルが明確に定義されないと、ここから導出されるセキュリティ要件にも曖昧さが生じる。CC は非常に強力な手法であるが、システムを対象とした場合に、その業務モデルを明確に定義することは一般に困難で、今後の課題とされている。現状では、「標準的電子カルテ」に明確な業務モデルを設定することは困難であり、この手法を完全に実践することはできない。[2] したがって、下記の ISMS に基づいて検討した場合でも、「網羅的でない」ことを前提としていることを最初に意識しなければならない。

2.2. ISMS の手法

ISMS は CC と異なり、情報システムを運用する組織の管理を中心に考える手法である。これはリスクアセスメントの結果から論理的に導き出された対応策を実施するというよりは、これまでの「うまくいった」組織の経験をもとにした「ベストプラクティス」に倣うことで、抜けがなく、過剰、重複もない管理策を策定し、実施することを求めている。ISMS で定義された管理策[3]だけで必要十分であることが論理的に証明されているわけではないが、これにしたがって「うまくいく」ことは経験上十分に説得力がある。

---

[2] 医療情報システムにおける CC に基づくセキュリティ仕様(Protection Profile と呼ばれる)を策定しようという試みが、日本医療情報福祉システム工業会(JAHIS)を中心に進められている。

[3] ISMS が参照する ISO?IEC 17799 の 2002 年度版では、10 の管理対象、36 の管理目的、127 の詳細管理策が定義されている。

「安全管理のガイドライン」は ISMS をベースとしたものではないが、医療分野の情報システムに関する有識者の知見を集約することで構築されているので、「ベストプラクティス」に近い。

3. 電子保存から導出されるセキュリティ機能要件

ここでは平成 15 年度と同様の手法で、「安全管理のガイドライン」から機能要件を別紙「電子カルテシステムにおけるセキュリティ機能要件.xls」)に抽出した。

「安全管理のガイドライン」における機能要件は、「システム機能」と「運用管理」のいずれで担保してもよいことになっており、その担保割合(0～100%)は運用する組織の自由裁量に任されている。要件の抽出については、下記に留意した。

- 本文の文章から機能要件を抜き出し、アトムレベルに細分化した。
- 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した。
- 明らかに運用で担保すべき要件については除外した。
- 通常は「運用管理」で担保することが効率的であるが、「システム機能」で全部または一部を担保可能な要件は残した。
- 「外部保存」は現状では実施する医療機関をほとんど想定できないため、これに関する要件は除外した。

4. 標準的電子カルテシステムとしての留意事項

上記のアプローチにより、少しでも「システム機能」で担保する余地のある要件がリストアップされた。「標準的電子カルテシステム」を実装する場合、下記に留意すべきである。

- これら「すべて」の実装が必須であると考える必要はない。
- 運用は「業務モデル」と深い関係があり、運用管理を含む「業務モデル」を明確に定義することが先決である。
- 運用によっては実装される必要のない「システム機能」が生じる。
- これらすべてを「システム機能」で実装した「電子カルテシステム」を仮定すると、おそらく情報セキュリティ的にはあらゆる種類の運用に耐えるものとなるだろうが、非常に実装の難しい機能もあるし、実装されたとしても利用するには細かい運用ルールの設定が必要な機能もある。
- セキュリティ実装において、「システム機能」と「運用管理」は不可分であり、運用を想定しない機能実装はありえない。

以上

付図-1. 電子カルテシステムにおけるセキュリティ機能要件

カテゴリ	機能要件
利用者認証	診療録データへのアクセスにおける識別と認証を行うこと。
	メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、作業記録を残すこと。これはシステム利用者を模して操作確認を行うための識別・認証についても同様である。
	利用者にID、パスワード等の本人認証、識別に用いる識別情報を発行し、本人しか持ち得ない、または知り得ないように運用を定めること。システムは発行されたID、パスワード等による本人認証、識別機能を有すること。ただし、運用により確実に担保される場合は除く。
	本人認証、識別にICカード等のセキュリティ・デバイスを利用する場合は、そのデバイス単独で有効にならないようにし、必ずユーザIDやパスワードと組み合わせた識別、認証を行うこと。
	本人認証、識別に指紋、虹彩等のバイオメトリクスを利用する場合は、1対1の照合となるよう、必ずユーザIDやパスワードと組み合わせた識別、認証を行うこと。
	記録の作成入力に関与する利用者識別・認証用に電子証明書を発行し、本人しか持ち得ないよう私有鍵をICカード等のセキュリティ・デバイスに格納する。
	本人が私有鍵を活性化する際にはパスワードや生体認証等の認証情報を用い、その認証情報が暗号化されずにネットワークへ流れることのないような手段を用いること。また、電子証明書をシステムへの認証用に用いる際は少なくとも端末へのログオン毎に、電子署名用に用いる際には署名毎に私有鍵の活性化を求めること
アクセス管理	情報の区分管理を実施し、区分単位でアクセス管理を実施すること。
	医療施設内の医療従事者、関係職員ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行うこと。
	業務アプリケーションが稼動可能な端末を管理し、権限を持たない者からのアクセスを防止すること。
	操作者の役割(ロール)を定義し、上記で定義したプロシジャに対して適用可否を判断できること
監査証跡	電子的に保存された診療録等の情報に対するアクセス履歴を残し、管理すること。
	アクセスの記録として、誰が、何時、誰の情報にアクセスしたかを記録し、定期的な記録の確認を行うこと。
	アクセスの記録および定期的なログの確認を行うこと。
	詳細なオペレーション記録を保守操作ログとして記録すること。
	保守作業にかかわるログの確認手段として、アクセスした診療録等の識別情報を時系列順に並べで表示し、かつ指定時間内でどの患者に何回のアクセスが行われたかが確認できる仕組みが備わっていること。
	アクセスログの記録を残し、そのログが改ざんされない対策を講じ、万が一、記録情報の改ざん・削除が起こった場合にはその事実を検証可能とすること。
	ワークフローに沿ったログが記録されること。
代行操作	代行操作を運用上認めるケースがあれば、具体的にどの医療行為（プロシジャ）に適用するか、また誰が誰を代行してよいかを定義すること
	代行操作を認める医療行為がある場合は、その代行操作者自身も予め電子保存システムの運用操作に携わる者として当該システムに識別管理情報を登録すること。
	代行操作が行われた場合には、誰の代行が誰によっていつ行われたかの管理情報が、その代行操作の都度記録されること。
	代行操作により記録された診療録等は、できるだけ速やかに作成責任者による「確定操作（承認）」が行われること。このため、代行入力により記録された情報およびその管理情報は必要な都度参照ができるとともに、一定の期間内に確定操作が行われるように督促機能が組織のルールとして整備されていること
	それぞれの役割者による記述を代行するケースがあれば、それを分担する役割者を医療行為ごとに定義すること。
	代行操作を認めるかどうかを医療行為(プロシジャ)ごとに定義しうること。
	代行操作が行われたプロシジャに対し、その承認者(作成責任者)による承認操作が行えること。また、その承認操作が督促されること。

カテゴリ	機能要件
記録の確定	診療録等の作成・保存を行おうとする場合、システムは確定された情報が登録できる仕組みを備えること。その際、作成責任者の氏名等の識別情報、信頼できる時刻源を用いた作成日時が含まれること。
	「記録の確定」を行うにあたり、作成責任者による内容の十分な確認が実施できるようにすること。
	確定された記録が、不正に追記、改ざん、消去されることを運用も含めて防止でき、それらが検知された場合はバックアップ等を用いて原状回復できるようになっていること。
	外部から入力された情報を「参照」する場合、その情報は本ガイドラインに従って正しく保存された確定記録でなければならない。参照元の情報が「保存された記録」でない場合は、コピー等の移動手段を経て取り込み操作を行った後に、その情報も含めた「記録の確定」が行
	運用管理規程等に当該装置により作成された記録の確定ルールが定義されていること。その際、作成責任者の氏名等の識別情報（または装置の識別情報）、信頼できる時間源を用いた作成日時が記録に含まれること。
	確定された記録が、不正に追記、改ざん、消去されることを運用も含めて防止でき、それらが検知された場合はバックアップ等を用いて原状回復できるようになっていること。
	一旦確定した診療録等を更新した場合、更新履歴を保管し、必要に応じて更新前と更新後の内容を照らし合せることができること。
	更新履歴の参照（照らし合せ）は、更新前後の情報が各々物理的に独立して保存されているものの様に更新の順序に沿って参照する方法か、更新時の変更点を明示するような方法（消し込み線を表示するように）で参照できること。
	同じ診療録等に対して更新が複数回行われた場合にも、更新の順序性が識別できるように参照できること。
	一定時間後に記録が自動確定するような運用の場合は、作成責任者を特定する明確なルールを策定し運用規程に明記すること。
	診療記録を共同して作成するケースが運用上あれば、具体的にどの医療行為に適用するか定義すること。また、それぞれを分担する役割者（ロール）を具体的な職種や所属部署等を用いて定義すること。
	記述の分担単位に確定操作が行えるようになっており、それぞれの記述者の識別管理情報が記録されること。
	「記録の確定」に際し、作成者責任者の電子署名を行うこと。また、確定操作がいつ行われたかを担保するために、確定操作後速やかに信頼できる時刻源を用いたタイムスタンプ署名を行うこと。
	「記録の確定」に際し、その作成責任者の識別情報が電子署名により記録情報に関連付けられること。この際、署名はICカード等のセキュアなトークン内で行われるか、利用者の端末内で行われる場合は署名後に私有鍵の情報が一切残らない方式を用いること。
	「確定操作」を行うにあたり、責任者による内容の十分な確認が行われたことを確認する手続きを義務づけること。
	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。追記・書き換え・消去時の確定操作を行う際には当該部分の変更履歴を含んだ電子署名をおこなうこと。
	1つの診療記録に対し、複数の入力者による署名をサポートすること。この場合、1つの情報単位に対して複数の署名を付与する実装でもよいし、情報を分担ごとの複数のセクションに分けて、それぞれを独立した情報として別々に署名を付与してもよい。しかし、後者の場合には情報間の関連性が失われないように配慮すること。
	共同作業における情報入力のワークフローが管理でき、そのワークフローに沿った制御が可能であること。
保存性	電子署名は保存が義務づけられた期間より長期にわたり署名時点での証明書および署名の有効性が確認できること。
	システムの永久ないし長時間障害対策として、日々バックアップデータを採取すること。
	システムが情報を保存する場所（内部、可搬媒体）を明示し、その場所ごとの保存可能用量（サイズ、期間）、リスク、レスポンス、バックアップ頻度、バックアップ方法などを明示すること。これらを運用管理規程としてまとめて、その運用を関係者全員に周知徹底すること。
	各保存場所における原本（データ）が破損した時に、バックアップされたデータを用いて破損前の状態に戻せること。もし、破損前と同じ状態に戻せない場合は、失われた範囲が容易にわかること。
	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。システム導入時に、システム導入業者にデータ移行に関する情報開示条件を明確にし、旧システムから新システムに移行する場合に、システム内のデータ構造が分からないことに起因するデータ移行の不能を防止すること。
	システム更新の際の移行を迅速に行えるように、診療録等のデータを標準的なデータ形式にて出力および入力できる機能を備えること。

カテゴリ	機能要件
	マスタDBの変更の際に、過去の診療録等の情報に対する内容の変更が起こらないようにすること。
	診療録等のデータのバックアップを定期的に取得し、その内容に対して改ざん等による情報の破壊が行われていないことを検査する機能を備えること。なお、改ざん等による情報の破壊が行われていないことが証明された場合は、原本が破壊された場合にその複製を原本として扱うことと
	記録媒体に関しては、あるレベル以上の品質が保証された媒体に保存すること。
	診療録等の情報をハードディスク等の記録機器に保存する場合は、RAID-1もしくはRAID-5相当のディスク障害に対する対策を取ること。
	マスタDBの変更の際に、過去の診療録等の情報に対する内容の変更が起こらないような機能を備えていること。
見読性	電子媒体に保存された全ての診療情報等が見読目的に支障のない応答時間やスループットと操作方法で見読可能であることと、システム障害においてもバップアップシステム等により診療に致命的な支障が起きない水準で見読出来ることが必要である。
	紙管理された情報を含め、各種媒体に分散管理された情報であっても、患者毎の情報の全ての所在が日常的に管理されていること。
	電子媒体に保存された全ての情報とそれらの見読化手段は対応づけて管理されていること。また、見読手段である機器、ソフトウェア、関連情報等は常に整備されていること。
	外来診療部門においては、患者の前回の診療録等が当日の診療に支障のない時間内に検索表示もしくは書面に表示できること。
	入院診療部門においては、入院中の患者の診療録等が当日の診療に支障のない時間内に検索表示もしくは書面に表示できこと。
	患者への説明が生じた時点で速やかに検索表示もしくは書面に表示できること。なお、この場合の"速やかに"とは、数分以内である。
	監査当日に指定された患者の診療録等を監査に支障のない時間内に検索表示もしくは書面に表示できること
	所定の期間より指定された日までに、患者の診療録等を書面に表示できること。
	保存場所が複数ある場合、各保存場所毎に見読手段を用意し、その操作方法を明示すること。
	システムの一系統に障害が発生した場合でも、通常の診療に差し支えない範囲で診療記録等を見読可能とするために、システムの冗長化や代替え的な見読手段を用意すること。
	システムが停止した場合でも、バップアップサーバと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読することができ
	システムが停止した場合でも、見読目的に該当する患者の一連の診療記録を汎用のブラウザ等で見読ができるように見読性を確保した形式で外部ファイルへ出力することができること。
	大規模火災等の災害対策として、遠隔地に電子保存記録をバックアップし、そのバックアップデータと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読することができること。
	緊急に必要になることが予測される診療情報は、内部に保存するか、外部に保存しても複製または同等の内容を施設内に保持すること
	緊急に必要になるとまではいえない情報についても、ネットワークや施設の障害等に対応できるような措置を行っておくことが望ましい。
	診療上緊急に閲覧が必要になったときに迅速に対応できるよう、停電時の補助電源の確保、システムトラブルに備えたミラーサーバーの確保などの必要な体制を構築すること
ウィルス対策	ウィルスなどの不正なソフトウェアの混入を防ぐ適切な措置をとること。
	ウィルスなどの不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持(たとえばパターンファイルの更新の確認・維持)をとること。
	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に、システムで利用するソフトウェア、機器および媒体の管理を行うこと。
	電子的に保存された診療録等の情報にアクセスするシステムでは、ウィルス対策ソフト等を導入し、定期的にウィルスの検出を行い、ウィルスが発見された場合には直ちに駆除すること。また、ウィルス定義ファイルは常に最新の状態に保つように、端末の運用管理を徹底すること。
	アンチウィルスゲートウェイ等を導入し、院内のシステムにウィルスが侵入することを防止すること。また、ウィルス定義ファイル更新用のサーバを導入し、各端末に導入したウィルス対策ソフトの定義ファイルおよびバージョンが、常に最新の状態に保たれるようにシステム的な対策を施す
構成管理	システムを構成するソフトウェアの構成管理を行い、不正な変更が検知できること。また検知された場合は、バックアップ等を用いて原状回復で
リモート保守	情報システムに施設外からリモート接続する場合は、暗号化、ネットワーク接続端末のアクセス制限等のセキュリティ対策を実施するこ

カテゴリ	機能要件
	情報システムにリモートアクセスする場合には、VPN等、通信経路の暗号化を実施するとともにICカード、電子証明書とパスワード等、2つ以上の要素からなる認証方式により利用者の識別、認証を求めること。
	リモート保守によるシステムの改造や保守が行なわれる場合には、必ずメッセージログを採取し、当該作業の終了後速やかにメッセージログの内容を医療機関側責任者が確認すること。
スキャナによる保存	診療に支障が生じることのないよう、スキャンによる情報量の低下を防ぎ、原本として必要な情報量を確保するため、光学解像度、センサなどの一定の規格・基準を満たすスキャナを用いること。
	診療情報提供書等の紙媒体の場合、300dpi、RGB各色8ビット(24ビット)の，カラースキャナを用いること。
	放射線フィルムなど高精細な情報に関しては日本医学放射線学会電子情報委員会が「デジタル画像の取り扱いに関するガイドライン1.1版(平成14年6月)」を公表しており、参考にされたい。なお、このガイドラインではマンモグラフィーは対象とされていないが、同委員会で検討される予
	このほか心電図などの波形情報やポラロイド撮影した情報など、さまざまな対象が考えられる。一般的に極めて精細な精度が必要なもの以外は300dpi、24ビットのカラースキャナで十分と考えられるが、あくまでも診療に差し支えない精度が必要であり、その点に十分配慮すること。
	スキャンした画像情報はTIFF形式またはPDF形式で保存することが望ましい。また非可逆的な圧縮は画像の精度を低下させるために、非可逆圧縮をおこなう場合は診療に支障がない精度であること、およびオリジナルの紙などの破損や汚れなどの状況も判定可能な範囲であることを念頭におこなう必要がある。
	スキャナで読み取った際は、作業責任者(実施者または管理者)が電子署名及び認証業務に関する法律(電子署名法)に適合した電子署名等を行い、責任を明確にすること
	スキャナで読み取る際は、タイムスタンプの利用または運用上システムの時刻の正確性を確保することにより、読み取り時刻が明示され、かつ、信頼できること
	情報作成管理者は、上記運用管理規程に基づき、スキャナによる読み取り作業が、適正な手続で確実に実施される措置を講じること。
	診療に支障が生じることのないよう、スキャンによる情報量の低下を防ぎ、原本として必要な情報量を確保するため、光学解像度、センサなどの一定の規格・基準を満たすスキャナを用いること。
	診療情報提供書等の紙媒体の場合、300dpi、RGB各色8ビット(24ビット)の，カラースキャナを用いること。
	放射線フィルムなど高精細な情報に関しては日本医学放射線学会電子情報委員会が「デジタル画像の取り扱いに関するガイドライン1.1版(平成14年6月)」を公表しており、参考にされたい。なお、このガイドラインではマンモグラフィーは対象とされていないが、同委員会で検討される予
	このほか心電図などの波形情報やポラロイド撮影した情報など、さまざまな対象が考えられる。一般的に極めて精細な精度が必要なもの以外は300dpi、24ビットのカラースキャナで十分と考えられるが、あくまでも診療に差し支えない精度が必要であり、その点に十分配慮すること。
	スキャンした画像情報はTIFF形式またはPDF形式で保存することが望ましい。また非可逆的な圧縮は画像の精度を低下させるために、非可逆圧縮をおこなう場合は診療に支障がない精度であること、およびオリジナルの紙などの破損や汚れなどの状況も判定可能な範囲であることを念頭におこなう必要がある。

平成15年度～16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」
総合研究報告書

(資料9)

電子カルテの個人情報保護対応要件

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、第 9 条により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し立てること、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。

2.4. 医療機関等における個人情報の保護に係る当面の取組について

「医療機関等における個人情報の保護に係る当面の取組について」という文章が平成 16 年 12 月 24 日付で医療機関等における個人情報保護のあり方に関する検討会より発表された。その中で、医療分野における個人情報は以下のように位置づけられている。

「医療分野については、「個人情報の保護に関する基本方針(平成 16 年 4 月 2 日閣議決定)」(以下「基本方針」という。)において、金融・信用や情報通信等と並んで、「個人情報の性質や利用方法等から特に適正な取扱いの厳格な実施を確保する必要がある分野」の一つと位置付けられている。」

そして、医療機関等における個人情報の取扱いに係る課題として以下の三つの問題をとりあげている。

(1)　安全管理に関する問題

医療分野に関する個人情報の漏えいや不当な利用などにより、個人の権利利益が侵害された場合には、他の分野の情報に比べ、被害者の苦痛や権利回復の困難さが大きいことから、安全管理のための格別の措置が必要と考えられること。

(2)　自己情報のコントロールに関する問題

患者の自己決定権のもと、患者自らが主体となって判断し、医療を受けることができるようにしていくためには、患者の医療に関する個人情報の自己情報コントロールについて、格別の措置が必要と考えられること。一方で、医療分野の情報は、公衆衛生などその利用の意義が大きい点や、患者への配慮のない開示により逆に患者に不利益になる場合もありうるなど、他の分野にない特性を有することから、特別な配慮を必要とする場合があると考えられること。

(3)　死者の情報

個人情報保護法は、生存する個人に関する情報について適用されるものであるが、医療分野においては、医療は死と向き合う分野であり、死者の情報についても安全管理や開示に配慮する必要があるため、死者の情報について他の分野の情報とは異なる格別の措置が必要と考えられること。

医療機関等における個人情報保護のあり方に関する検討会では、これらの問題に対応するために「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」を策定し、同日公表した。

2.5. 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

(1)　ガイドラインの趣旨

ガイドラインではまず本ガイドラインの趣旨を明確に定義している。

「本ガイドラインは、「個人情報の保護に関する法律」(平成15年法律第57号。以下「法」という。)第6条第3項及び第8条の規定に基づき、法の対象となる病院、診療所、薬局、介護保険法に規定する