平成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」
総括研究報告書

(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

居宅サービス事業を行う者等の事業者等が行う個人情報の適正な取扱いの確保に関する活動を支援するためのガイドラインとして定めるものであり、厚生労働大臣が法を執行する際の基準となるものである。」

ここで「法を失効するための基準」と定義していることからこのガイドラインが国の個人情報保護対応要件を構成していると理解して差し支えないと考えることができる。

(2)　医療・介護関係事業者が講ずるべき安全管理措置

電子カルテの個人情報保護対応要件として考えなければならないのは「医療・介護関係事業者が講ずるべき安全管理措置」の部分である。ここでは以下のように記載されている。

> 「医療・介護関係事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のため、組織的、人的、物理的、及び技術的安全管理措置を講じなければならない。その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱い状況等に起因するリスクに応じ、必要かつ適切な措置を講ずるものとする。なお、その際には、個人データを記録した媒体の性質に応じた安全管理措置を講ずる。」

その上で、医療情報システムの導入及びそれに伴う情報の外部保存を行う場合の取り扱いとして、

> 「医療機関等において、医療情報システムを導入したり、診療情報の外部保存を行う場合には、厚生労働省が別途定める指針によることとし、各医療機関等において運営及び委託等の取扱いについて安全性が確保されるよう規程を定め、実施するものとする。」

と規定されており、実際の要件については別途定める指針を参照することとなっている。この指針については、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の座長である樋口教授より、医療情報ネットワーク基盤検討会において医療情報ネットワーク基盤検討会における検討結果を参照したいとの表明があり、医療情報ネットワーク基盤検討会において「医療情報システムの安全管理に関するガイドライン」の検討がなされることとなった。

2.6.　医療情報システムの安全管理に関するガイドライン

当初、医療情報ネットワーク基盤検討会においては「保存が義務付けられた診療録等の電子保存、外部保存のためのガイドライン」として検討が進められていたが、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の決定を受け、医療情報システム全般の個人情報保護についても記載することとなり、タイトルも上記のように変更された。

本ガイドラインでは 6 章において、「個人情報保護に関する法律」の要求事項を受けて考え方の解説と対応すべきガイドラインを記載している。ガイドラインは「C.最低限のガイドライン」と「D.推奨されるガイドライン」の二つのレベルで規定されている。ガイドラインの概要と電子保存、外部保存の関係は図表のとおりとなっている。

(1)　リスク分析

本ガイドラインではリスク分析の必要性について特に運用面の配慮を中心に説明が行われており、

> 「安全管理や個人情報保護関連各法で原則禁止されている目的外利用の防止はシステ

ム機能だけでは決して達成できないことに留意しなければならない。システムとして 可能なことは人が正しく操作すれば誰が操作したかを明確に記録しつつ安全に稼動することを保障するのが限界である。したがって人の行為も含めた脅威を想定 し、運用規程を含めた対策を講じることが重要である。診療情報システムとして上記の観点で留意すべき点は、システムに格納されている電子データに関してだけでなく、入出力の際に露見等の脅威にさらされる恐れのある個人情報を保護するための方策を考える必要がある。」

としている。電子カルテシステムの個人情報保護要件を検討する場合、運用的対策などのシステムとしての技術的対策以外の部分も考慮しなければならない。

(2)　組織的安全対策

組織的安全対策の要件は以下のようになっている。

C. 最低限のガイドライン

① 情報システム運用責任者の設置及び担当者(システム管理者を含む)の限定を行うこと。ただし小規模医療機関等において役割が自明の場合は、明確な規程を定めなくとも良い。

② 個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定めること。

③ 情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。

④ 個人情報の取り扱いを委託する場合、委託契約において安全管理に関する条項を含めること。

⑤ 運用管理規程等において下記の内容を定めること。

(a) 個人情報の記録媒体の管理(保管・授受等)の方法

(b) リスクに対する予防、発生時の対応の方法

(3)　物理的安全対策

物理的安全対策の要件は以下のようになっている。

C. 最低限のガイドライン

① 個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。

② 個人情報を入力、参照できる端末が設置されている区画は、業務時間帯以外は施錠等、権限者以外立ち入ることが出来ない対策を講じること。

③ 個人情報の物理的保存を行っている区画への入退管理を実施すること。

・ 入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録すること。

・ 入退者の記録を定期的にチェックし、妥当性を確認すること。

④ 個人情報が存在するPC等の重要な機器に盗難防止用チェーンを設置すること。

⑤ 離席時にも端末等での正当な権限者以外の者による窃視防止の対策を実施すること。

D. 推奨されるガイドライン

① 防犯カメラ、自動侵入監視装置等を設置すること。

(4)　技術的安全対策

技術的安全対策の要件は以下のようになっている。

C. 最低限のガイドライン

① ID、パスワード等により、情報システムへのアクセスにおける識別と認証を行うこと。
② 動作確認等で個人情報を含むデータを使用するときは、漏洩等に十分留意すること。
③ 医療従事者、関係職種ごとに、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。
④ アクセスの記録及び定期的なログの確認を行うこと。
情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録(操作者及び操作内容)を必ず行うこと。
⑤ アクセスの記録に用いる時刻情報は信頼できるものであること。医療機関等の内部で利用する時刻情報は同期している必要があり、また標準時刻と定期的に一致させる等の手段で標準時と診療事実の記録として問題のない範囲の精度を保つ必要がある。
⑥ ウィルス等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。

D. 推奨されるガイドライン

① 情報システムへのアクセスにおける識別と認証を行うこと。
② 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。
③ 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。
④ 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。
⑤ ウィルス等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。
⑥ 離席の場合のクローズ処理を施すこと(クリアスクリーン)。

(5)　人的安全対策

従業者に対する人的安全管理措置の要件は以下のようになっている。

C. 最低限のガイドライン

医療機関等の管理者は、個人情報に関する施策が適切に実施されるよう措置するとともにその実施状況を監督する必要があり、以下の措置をとること。

① 法令上の守秘義務のある者以外を事務職員等として採用するにあたっては、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。
② 定期的に従業者に対し教育訓練を行うこと。
③ 従業者の退職後の個人情報保護規程を定めること。

D. 推奨されるガイドライン

サーバ室等の管理上重要な場所では、モニタリング等により従業者に対する行動の管理を行うこと。

また、託業者の監督及び守秘義務契約の要件は以下のようになっている。

C. 最低限のガイドライン

① プログラムの異常等で、保存データを救済する必要があるとき等、やむをえない事情で病院事務、運用等で、外部受託業者を採用する場合は、医療機関等の内部における適切な個人情報保護が行われるように、以下のような措置を行うこと。

・ 包括的な委託先の罰則を定めた就業規則等で裏づけられた守秘契約を締結すること
・ 保守作業等の医療情報システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認をおこなうこと。
・ 清掃等の直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。
・ 委託先事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託先と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること。

② プログラムの異常等で、保存データを救済する必要があるとき等、やむをえない事情で外部の保守要員が診療録等の個人情報にアクセスする場合は、罰則のある就業規則等で裏づけられた守秘契約等の秘密保持の対策を行うこと。

(6)　情報の破棄

情報の破棄については特別二節が設けられており、特に注意を促している。その要件は以下のようになっている。

C. 最低限のガイドライン

① 「6.1　方針の制定と公表」で把握した情報種別ごとに破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる従業者の特定、具体的な破棄の方法を含めること。

② 情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこととし、残存し、読み出し可能な情報がないことを確認すること。

③ 破棄を外部事業者に委託した場合は、「6.6　人的安全対策　(2)事務取扱委託業者の監督及び守秘義務契約」に準じ、さらに委託者が確実に情報の破棄が行なわれたことを確認すること。

④ 運用管理規程において下記の内容を定めること。

(a) 不要になった個人情報を含む媒体の廃棄を定める規程の作成の方法

(7)　情報システムの改造と保守

情報システムの改造と保守についても特別な節が設けられており、特に注意を促している。その要件は以下のようになっている。

C. 最低限のガイドライン

① 動作確認で個人情報を含むデータを使用するときは、明確な守秘義務の設定を行うともに、終了後は確実にデータを消去する等の処理を行うことを求めること。

② 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。
③ そのアカウント情報は外部流出等による不正使用の防止の観点から適切に管理することを求めること。
④ 保守要員の離職や担当変え等に対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付けまた、それに応じるアカウント管理体制を整えておくこと。
⑤ 保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を求めること。それらの書類は医療機関等の責任者が逐一承認すること。
⑥ 保守会社と守秘義務契約を締結し、これを遵守させること。
⑦ 保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむ得ない状況で組織外に持ち出さなければならない場合には、置き忘れ等に対する十分な対策を含む取り扱いについて運用管理規程を定めることを求め、医療機関等の責任者が逐一承認すること。
⑧ 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等の責任者が確認すること。
⑨ 再委託が行なわれる場合は再委託先にも保守会社と同等の義務を課すこと。

D. 推奨されるガイドライン
① 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。
② 保守作業時には病院関係者立会いのもとで行うこと。
③ 作業員各人と保守会社との守秘義務契約を求めること。
④ 保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむ得ない状況で組織外に持ち出さなければならない場合には、詳細な作業記録を残すことを求めること。また必要に応じて医療機関等の監査に応じることを求めること。
⑤ 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。

3. 電子カルテシステムとしての機能要件の抽出の考え方

2 章で述べたことは、個人情報取扱事業者としての医療機関が遵守すべき要件であり、電子カルテシステムとしてのシステム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。しかし、標準的な要件をまとめるという観点からは 2 章で規定されたガイドラインの要件を唯

一の共通要件として捕らえることは可能である。そこで、以下では個別の医療機関において、更なる要件を定義しようとする場合に必要なアプローチについて解説する。

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、不正ソフトウェア対策、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。2 章にて紹介した医療情報システムの安全管理のガイドラインにおいても ISMS のアプローチを推奨しており、医療機関自らがリスクアセスメントを行うことを要求している。

4. おわりに

「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」と「医療情報システムの安全管理のガイドライン」という二つのガイドラインが公表されたことにより、国としての個人情報保護要件が明確になった。標準的電子カルテとして遵守すべき要件としてはこれを遵守することと定義して問題ないと考えられるが、個々の医療機関における業務モデルや運用形態に応じた要件の追加は発生する可能性がある。これについては医療機関のリスクアセスメントによって導出されるものであるから汎用的な要件とはならないと考えられる。

以上

医療情報システムの安全管理に関するガイドラインの概要(1)

【1章～6章】：個人情報を含むデータを扱うすべての医療機関で参照されるべき内容を含んでいる。
【7章】：保存義務のある診療録等を電子的に保存する場合の指針を含んでいる。
【8章】：保存義務のある診療録等を医療機関の外部に保存する場合の指針を含んでいる。
【9章】：e－文書法に基づいてスキャナ等で電子保存する場合の指針を含んでいる。
【10章】：運用管理規程に関する事項について記載されている。主に電子保存や外部保存を行う場合の運用管理規程の作成に関する指針であるが、電子保存や外部保存を行わない場合でも参考になる。

付図. 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概要（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概要(2)

A　制度上の要求事項
法律、通知、他の指針などの要求事項をそのまま掲載している。

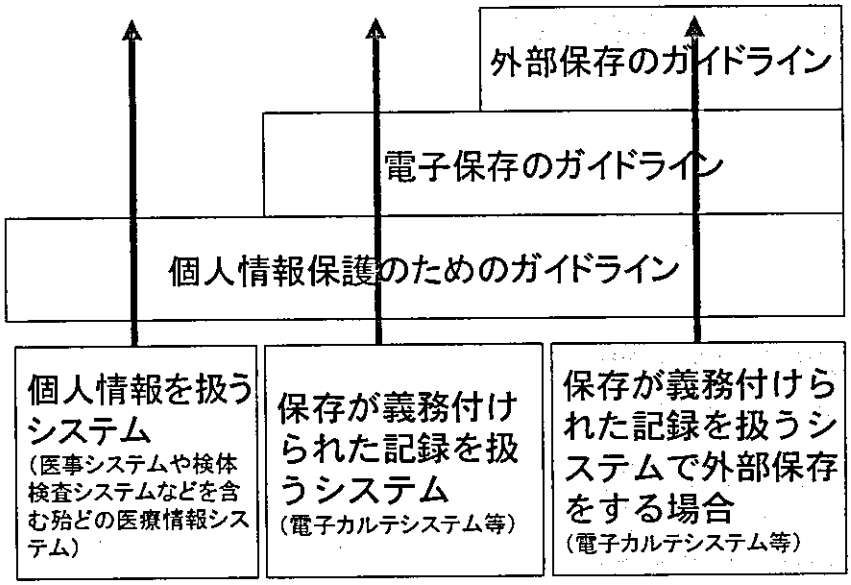
B　考え方
要求事項の解説および原則的な対策について記載している。

C　最低限のガイドライン
Aの要求事項を満たすためにかならず実施しなければならない事項を記載している。
この項にはいくつかの対策の中の一つを選択する場合もあるが、選択を明記している場合以外はすべて実施しなければならない対策である。
なお、この項の対策にあっては医療機関等の規模により実際の対策が異なる可能性がある。後述するように付表の運用管理表を活用し、適切な具体的対策を採用されたい。

D　推奨されるガイドライン
実施しなくても要求事項を満たすことは可能であるが、説明責任の観点から実施したほうが理解が得やすい対策を記載している。

付図. 2　医療情報システムの安全管理に関するガイドラインの概要（2）

個人情報保護と電子保存と外部保存の関係



付図. 3　個人情報保護と電子保存と外部保存の関係

平成 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
総括研究報告書

(資料 10)

電子カルテシステムのユニット化の検討

目次

1. はじめに

1.1 背景

標準的電子カルテシステム開発において、MDA(Model Driven Architecture)を実現するための手法の一つであるUML Profile for EDOCに従い、処理モデルの開発を進めてきた。処理モデルは、UML Profile for EDOCにおいてComputational Viewpoint(部品定義)として位置づけられるものであり、業務フローモデル(To-Be モデル)と情報モデルから導出される。具体的には、システムが実現すべき論理的な機能を表すコンポーネントとコンポーネント間の関連を示したものである。

標準的電子カルテシステムが目指すベンダに依存しない電子カルテシステムの構築を可能とするためには、コンポーネントの標準化ならびにその組み合わせによって、これらのコンポーネントを適切な粒度を持った「ユニット」としてまとめて、複数のベンダがユニット単位に独立して開発できるようにすることが必要と考えられる。ここでいうユニットとは、いくつかのコンポーネントをトランザクションが発生する機能構成単位に集約したものである。

また、近年IHE(Integrating the Healthcare Enterprise)的なシステム統合手法への理解が深まるにつれて、ユニット(IHE でいうアクタ)を定義し、業務フロー毎にユニット間の関連を整理する手法も定着してきている。このため、標準的電子カルテシステムを構成するユニットを定義し、業務フロー毎にユニット間のトランザクションを定義する、IHE 的なアプローチを採用することは、多くのベンダにとっても理解しやすいと考えられる。また、ユニットやユニット間のトランザクションを定義していくことは、マルチベンダによる標準的電子カルテシステム構築の実現性、妥当性を検討していくうえで重要な位置づけを持つものと考えられる。

1.2 目的

コンポーネントをまとめたユニットの粒度の妥当性ならびに、これまでに得られたコンポーネントモデルとの整合検証のために以下の3つの業務プロセスにおけるユニットおよびトランザクションを定義するとともに今後の課題について検討を加える。

■診療プロセス

■医事請求プロセス
■病棟看護プロセス

1．3 用語の定義

図1－1に、本報告で用いるサブシステム、ユニット、コンポーネントの構成概念を掲げる。マルチベンダでシステムを相互供給および相互利用する単位としてサブシステムがある。サブシステムの相互運用性を保証するには、サブシステムを構成するユニットについて、ワークフローごとにユニット間の通信手順および通信方式を規定するプロファイルを策定し、そのプロファイルに準拠していることを接続試験により検証する。ユニットも、複数のコンポーネントから構成される。

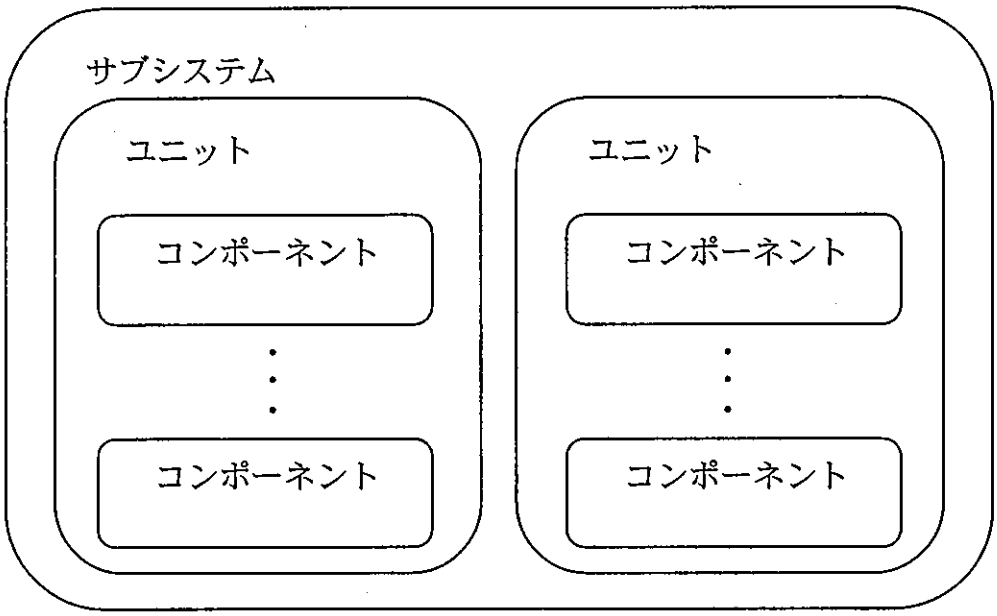


図1－1 コンポーネント、ユニット、サブシステムの構成概念図

2. 診療プロセスにおけるユニット化

2. 1 診療プロセスにおける主要な業務

診療プロセスにおけるユニット化を検討するにあたり対象業務を明確にし、その業務に含まれるコンポーネントを抽出する必要があったが、先行して実施された平成14年度厚生労働科学特別研究事業、研究課題名『コンポーネントの標準化による電子カルテ開発』にて対象業務ならびに業務プロセスを抽出していたため、今回の検討の土台として利用した。なお、今回のユニット化検討に当たっては、上記研究報告の中でモデル化対象外とした診療シナリオも含めている。

表2－1『コンポーネントの標準化による電子カルテ開発』の業務プロセス

業務プロセス	業務の流れ
外来患者診察前受付	紹介状を受け取り登録する 予備問診の登録
外来診察前	予約患者で受診予定患者を確認する 予備問診内容の不足事項を追加
外来患者診察	予約患者リストからの患者選択 紹介状、予備問診の参照 診療録の記載 検査依頼、検査予約
検査の実施	検査内容の確認 検査準備(採血、採尿) 検査実施 検査結果の登録 総合検査所見の登録
検査後の診察	手術予定の登録 入院時オーダ登録

2. 2 業務プロセスにおける登場人物と場所

前節で述べた業務プロセスにおける登場人物と場所を以下に整理する。

表2－2 業務プロセスにおける登場人物と場所

登場人物	場所
患者	診察前受付 外来診察室 検査受付 検査室
受付職員	診察前受付
医師	外来診察室
検査技師(検査実施者)	検査受付 検査室

2. 3 ユニット定義の考え方

ユニット検討に当たって最初に業務プロセスから必要なサブシステムを検討し、以下のサブシステムを導いた。この検討は、IHEで行われている放射線部門統合プロファイルの一つであるSWF(Scheduled Workflow)を参考にした。

- ■ 患者情報管理
- ■ オーダ発行
- ■ 予定(予約)管理
- ■ ワークフロー管理(オーダ進捗管理)
- ■ レポート管理(レポート作成、レポート参照、所見作成、所見参照)
- ■ オーダ内容監査
- ■ データ参照歴管理

次にこれらのサブシステムをユニットに分解し、ユニット間の関連をトランザクションとして記述した。

2. 4 ユニットと情報の流れ

今回検討した診療プロセスにおけるユニット化案を図2－1に示す。