

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、やむを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、やむを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て表示し、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ー

経営者による組織横断的なセキュリティポリシーの発行、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ー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)

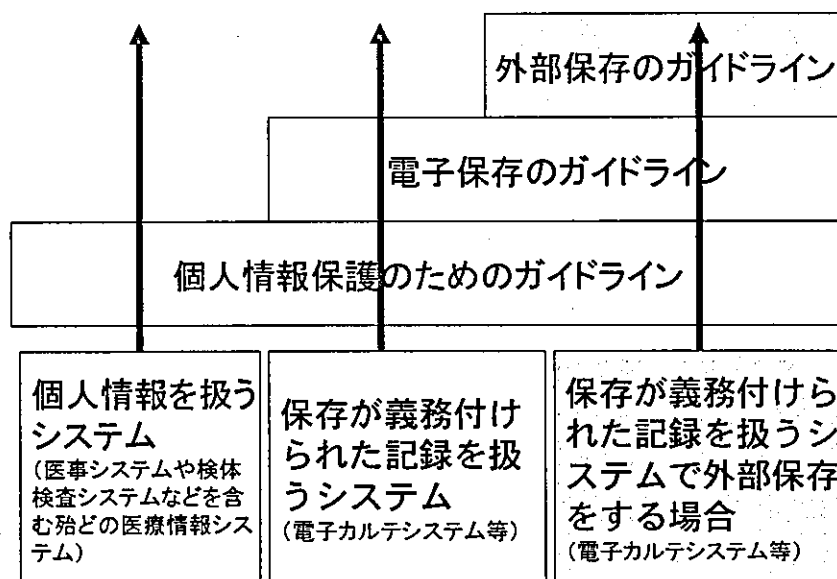
## 医療情報システムの安全管理に関するガイドラインの概要(2)

- 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 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 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.....	2
1.1 背景.....	2
1.2 目的.....	2
1.3 用語の定義.....	3
2. 診療プロセスにおけるユニット化.....	4
2.1 診療プロセスにおける主要な業務.....	4
2.2 業務プロセスにおける登場人物と場所.....	4
2.3 ユニット定義の考え方.....	5
2.4 ユニットと情報の流れ.....	5
2.5 ユニットの妥当性検証.....	10
3. 医事請求プロセスにおけるユニット化.....	11
3.1 医事請求プロセスにおける主要な業務.....	11
3.2 業務プロセスにおける登場人物と場所.....	11
3.3 ユニット定義の考え方.....	12
3.4 ユニットと情報の流れ.....	12
3.5 ユニットの妥当性検証.....	14
4. 病棟看護プロセスのユニット化.....	15
4.1 病棟看護プロセスにおける主要な業務.....	15
4.2 業務プロセスにおける登場人物と場所.....	16
4.3 ユニット定義の考え方.....	16
4.4 ユニットと情報の流れ.....	19
4.5 ユニットの妥当性検証.....	24
5. まとめと今後の課題.....	25

## 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。

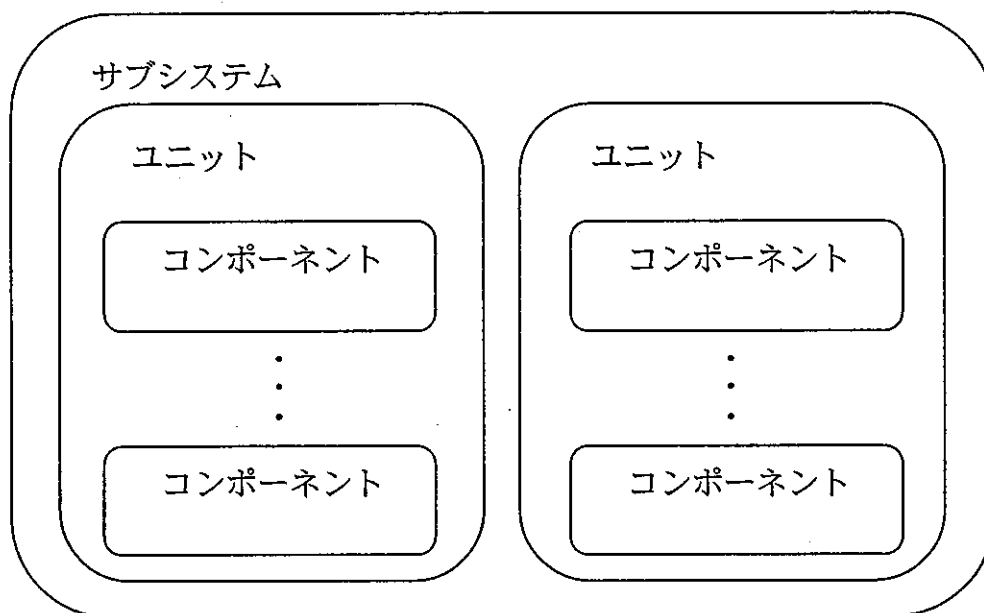


図1-1 コンポーネント、ユニット、サブシステムの構成概念図

## 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
- データ参照履歴管理

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。

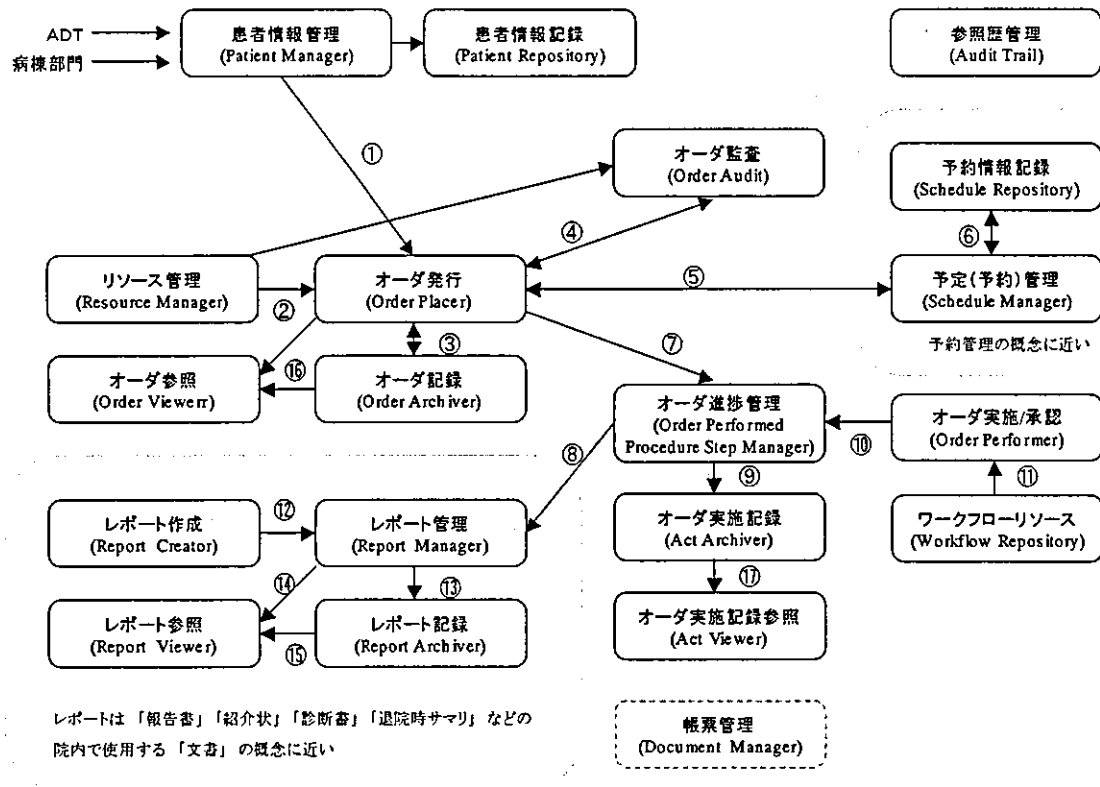


図2-1 診療プロセス ユニット構成案

図2-1では、診療システムを構成する5つのサブシステムと、関連する2つの外部システムを表している。5つのサブシステムは、以下の通りである。

■ 患者情報管理

患者情報を管理する。患者情報として氏名、年齢などの基本的な情報と、患者の属性情報(既往歴、アレルギー等)を保持する。ユニットとして患者情報管理、患者情報記録が存在する。

■ オーダー発行

オーダー(診療指示)を発行するための機能であり、発行したオーダーの記録やオーダー発行に必要なリソース(マスタ、ロール等)の管理を行う。ユニットとしてオーダー発行、リソース管理、オーダー記録、オーダー参照が存在する。

■ 予定(予約)管理

患者に依存しない院内の予定(予約)情報を管理する。ここで扱う予定情報とは例えば医師の予約枠や、医療機器の空きを意図している。ユニットとして予定(予約)管理と予約情報記録が存在する。

### ■ ワークフロー管理

オーダーに基づく各種医療行為の進捗状況や、医療行為の実施記録、実施に対する承認などのワークフローを管理する。ここでは明示的なオーダー入力を伴わない実施（必要時指示に伴う行為の実施等）もワークフローとして捉えている。ユニットにはオーダー進捗管理、オーダー実施/承認、オーダー実施記録、ワークフローリソース、オーダー実施記録参照が存在する。

### ■ レポート管理

院内における文書を管理する機能であるが、ここでは文書を診療記録、所見、アナムネ、サマリ、各種レポート、報告書などを含む広い概念で捉えている。ユニットとしてレポート管理、レポート作成、レポート記録、レポート参照が存在する。

なお、2つの外部システムは以下の通りである。

### ■ オーダ内容監査

### ■ データ参照履歴管理 (Audit Trail)

ユニットの一覧とその概要を表2-3に、トランザクションの説明を表2-4に、また業務プロセスと関連するユニットを表2-5に示す。なお表2-4のトランザクション番号は図2-1の丸囲みのトランザクション番号と対応づけられている。

表2-3 ユニットの説明

項番	ユニット名	英語表記	説明
1	患者情報管理	Patient Manager	患者の属性、プロフィールを管理する
2	患者情報記録	Patient Repository	患者属性、プロフィールの記録情報
3	オーダー発行	Order Placer	オーダー発行機能
4	オーダー記録	Order Archiver	発行されたオーダーの記録情報
5	オーダー参照	Order Viewer	記録されたオーダー内容参照のビューア
6	リソース管理	Resource Manager	オーダー発行するための諸リソース(マスタ情報など)の管理
7	オーダー監査	Order Audit	発行されるオーダー内容が適正であるかを監査する
8	予定(予約)管理	Schedule Manager	オーダーに関連する予約情報を管理する。患者の予定情報は OPPSM が管理するため、このユニットは予約枠管理を意味する
9	予約情報記録	Schedule Repository	予約枠情報



10	オーダー進捗管理	Order Performed Procedure Manager	Step OPPSM オーダーの進捗状況を管理する。
11	オーダー実施記録	Act Archiver	オーダー進捗記録
12	オーダー実施/承認	Order Performer	オーダーの実施、ならびに承認を行う。 (実施に対する承認もあり得る)
13	オーダー実施記録参照	Act Viewer	記録されたオーダー実施記録参照のビューア
14	ワークフローリソース	Workflow Repository	承認を行うためのワークフローを管理する。 (例 承認者は誰か)
15	レポート管理	Report Manager	レポートの管理を行う。ここでレポートは院内に存在する文書の概念に近い。
16	レポート記録	Report Archiver	レポートの記録情報
17	レポート参照	Report Viewer	レポートを参照するためのビューア
18	レポート作成	Report Creator	レポート作成を行う
19	参照履歴管理	Audit Trail	オーダー発行、実施、承認、レポート作成、参照の履歴を管理する。レポート参照の履歴管理を行うためにOPPSMから独立したユニットとする
20	帳票管理	Document Manager	帳票の定義によってはレポート管理とは別に必要になることが予測されるが、診療プロセスのユニットとしては対象にしない

表2-4 トランザクションの説明

トランザクション番号	トランザクションの説明
1	患者情報管理ユニットからオーダー発行に必要な患者情報を取得するトランザクション
2	オーダー発行のために必要なリソース(マスタ)やロールをリソース管理ユニットから取得するトランザクション
3	発行したオーダー情報をオーダー記録ユニットに通知するトランザクション
4	オーダー発行に際してオーダー内容監査のためにオーダー内容を通知し監査結果を受け取るトランザクション

5	オーダー発行に際して患者とは独立した予定(予約)情報(例えば検査機器の空き情報)を予約管理ユニットから取得し、決定した予約情報を返すトランザクション
6	予定(予約)管理情報を記録する予約情報記録ユニットから情報を取得、登録するためのトランザクション
7	発行されたオーダーの進捗状況(ワークフロー)を管理するオーダー進捗管理ユニット(OPPSM)にオーダーの発行を通知するトランザクション
8	オーダーの結果としてレポート、文書が発生する場合、それらのレポートを管理するユニットにオーダーの発生や進捗の変更を通知するトランザクション
9	オーダー実施記録ユニットにオーダーの発生、進捗の変更を通知するトランザクション
10	オーダーによって発生した診療行為の実施を OPPSM に通知するトランザクション。ならびに実施内容をオーダー実施記録ユニットに通知するトランザクション。(オーダーがなく発生した診療行為の通知もあり得る)
11	診療行為の実施や承認に関わるリソース、ロールを取得するトランザクション
12	レポート作成ユニットからレポート作成情報を受け取るトランザクション
13	レポート記録ユニットにレポート作成ユニットから受け取った情報を受け渡すトランザクション
14	レポート参照のためにレポートに関する情報をレポート管理ユニットから取得するトランザクション
15	レポート情報をレポート記録ユニットから取得するトランザクション
16	オーダー内容、履歴を取得するトランザクション
17	オーダー実施記録や履歴を取得するトランザクション

表2-5 業務プロセスと関連するユニット

項番	業務プロセス シナリオ	関連するユニット
1	紹介状を受け取り登録する	レポート作成
2	予備問診の登録	レポート作成
3	紹介状、予備問診の参照	レポート参照
4	診療録の記載	レポート作成
5	検査依頼、検査予約	オーダー発行、予定(予約)管理
6	検査実施	オーダー実施/承認
7	検査結果の登録	オーダー実施/承認

8	総合検査所見の登録	レポート作成
9	検査結果、検査所見の参照	レポート参照、オーダー実施記録参照
10	診療録の記載	レポート参照
11	入院の決定	スコープ外
12	適用クリティカルパスの決定	リソース管理、オーダー発行
13	入院予約	スコープ外
14	追加検査の依頼	オーダー発行
15	予約患者で受診予定患者を確認する	予定(予約)管理
16	予備問診内容の不足事項を追加	レポート作成
17	予約患者リストからの患者選択	予定(予約)管理、オーダー進捗管理
18	検査内容の確認	オーダー参照、オーダー実施記録参照
19	検査準備(採血、採尿)	オーダー実施/記録
20	手術予定の登録	オーダー発行、予定(予約)管理
21	入院時オーダー登録	オーダー発行

## 2.5 ユニットの妥当性検証

今回のユニット案の試作においてプロブレム(病名、看護問題など)はスコープに入っていない。これはユニット化に当たってベースとした業務プロセスモデルにこれらの情報が含まれていないためであるが、今後の検討においてはプロブレムをはじめとする複数のユニットをまたがるクラスについても、業務プロセスの分析、コンポーネント化、ユニット化の作業が必要になるものと考えられる。

### 3. 医事請求プロセスにおけるユニット化

#### 3.1 医事請求プロセスにおける主要な業務

通常、医事会計部門では、診療部門にて発生する患者のカルテや医療従事者の指示・実施などの伝票を見て、患者が受けた医療行為に対する会計計算を行う。医事請求プロセスとは、会計計算に必要となる診療行為の情報を、診療部門から医事会計部門に対して受け渡す事である。

医事請求プロセスは、診療行為の情報の電子的な受け渡しを主要な業務とするため、ユーザからは直接見えない業務プロセスとなっている。そのため、以下ではユーザから見える診療業務プロセスに沿って、医事請求プロセスにおけるユニット化について説明する。

表3-1には、医事請求プロセスにおけるユニット化を検討する際に用いた典型的な診療業務プロセスを示す。これは、典型的な診療業務プロセスを想定し、その業務プロセスの中から医事請求に関連するものを抜き出し、業務内容について例示したものである。

表3-1 典型的な診療業務プロセス

業務プロセス	業務の流れ
外来患者診察	診療録の記載 血液検査(動脈血液ガス分析)の指示 処方(PL 顆粒 1g/包 3包 分3 朝昼夕食後 5日分)の指示
検査の実施	血液検査の実施
会計	会計計算

#### 3.2 業務プロセスにおける登場人物と場所

医事請求プロセスは、上述の通り、ユーザからは直接見えない業務プロセスとなっている。このため、ここでは、医事請求プロセスにおけるユニット化を検討する際に用いた典型的な診療業務プロセス(表3-1)における登場人物と場所を表3-2として整理した。