図13. 診療記録に関連する項目が評点2以下となる割合

(2004年度受審病院／Ver4:n=603;)

4.3.1	診療録管理部門の体制が整備されている	14.4%
4.3.2	診療録が適切に管理されている	27.7%
4.3.3	診療情報が適切に管理され活用されている	14.3%
4.20.3	医師の指示が確実に伝達され実施されている	13.7%
5.10.4	医師の指示に基づいて医療行為を行い、その反応を観察している	11.9%

(注)

Ver4の「4.3.1」「4.3.2」「4.3.3」は、Ver5の「4.16.1」「4.16.2」「4.16.3」に対応

Ver4の「4.20.3」「5.10.4」は、Ver5の「5.3.2」に対応

図14. 医療安全に関連する評価項目

- 第1領域:病院組織の運営と地域における役割
  - 病院の理念における医療安全の位置づけ、適切な組織管理体制、医療安全に関する教育体制、リーダーシップなど
- 第2領域:患者の権利と安全確保の体制
- 第3領域:療養環境と患者サービス
  - 患者の安全に対する日常的な配慮
- 第4領域:医療提供の組織と運営
  - 各部門における、安全に配慮した手順の遵守
- 第5領域:医療の質と安全のためのケアプロセス
  - 診療・看護の責任体制、正確な指示の伝達、安全に配慮した手順の遵守など
- 第6領域:病院運営管理の合理性
  - 医療機器の管理、保安管理など

4.「医療情報システムの安全管理に関するガイドライン」に関する

ISO/IEC15408(Common Criteria)の視点から見た概要設計

喜多　紘一

東京工業大学像情報工学研究施設

４．１　ISO/IEC15408：IT セキュリティの国際評価標準のポイントと動向

４．１．１　ISO/IEC15408 が謳う IT セキュリティを高めるコンセプト

ISO/IEC15408 は IT 機器、情報システムのセキュリティを高めるコンセプトを次のように捉えている。

> **「セキュリティの枠組を明確に定義し、その上で、セキュリティ機能が確かに設計され実装されたことの信頼性を「保証」する」**

ここで、「明確な定義」とは、保護資産、脅威、対抗策、セキュリティ要件、セキュリティ機能の関係を明らかにしその正当性の根拠を与えることである。また、この「保証」は評価対象機器や、情報システムの開発のライフサイクル全般を対象としている。このとき、ISO/IEC15408 が定める情報セキュリティは「保証と評価」のセットで把握することになる。ここで「保証」とは、CC 特有の概念である。ISO/IEC15408 が定める保証とは、国や第三者機関による保証ではなく

> **「セキュリティ機能がきちんと設計実装されていることを開発者が保証する」**

ということである。さらに、評価とは

> **「セキュリティ機能が開発者の主張のとおりきちんと設計実装されていることを評価する」**

ということになる。セキュリティ機能の強度の診断ではないことに注意する必要がある。

４．１．２　ISO/IEC15408の歴史的背景

欧米では約20年前から軍・政府調達を主対象とした情報セキュリティに関する規格・制度が運用されてきた。具体的には、欧州では欧州各国の評価基準を統合したITSECが制度化され、米国ではTCSEC（俗にいうOrange Book）が運用されてきた。この2つの制度を中核としたCC（Common Criteria：情報セキュリティ評価のための共通（Common）基準（Criteria））がVer1.0（1996年）、Ver2.0（1998年）、Ver2.1（1999）と順次定められ、1999年6月、ISO/IEC15408として国際規格として承認を受け同年12月に発効した（この歴史的経緯から、ISO/IEC15408をCCと呼ぶことが規格で認められている）。

日本ではJIS／X5070：2000としてJIS化され2001年に運用が開始されているが、評価基準としては、本家のCCや国際規格としてのISO/IEC15408など、複数の「基準」の使用が認められおり、これらを総称して、ISO/IEC15408と呼称している。またCCの解釈に関する補正事項をまとめたものとしてCCIMB Interpretation-0407　があり、CCと併せて使用することになっている。更に、評価方法としては通称CEM（セム）と呼ばれる、Common Methodology for Information Security Evaluation Ver 1.0がある（同格の方法として、JIS TR X 0049:2001　や　CCIMB Interpretation-0407がある）。

現時点での最新版は、2005年に発効したISO/IEC15408:2005（同時にCCVer2.3、CEM2.3、CCIMBInterpretation0512）である。

４．１．３　規格の構成

ISO/IEC15408は、情報セキュリティに関する「機能要件」、「保証要件」がカタログ化された３つのパートから構成される「要件集」である、ということができる。

パート１は、「概説と一般モデル」と題され、ISO/IEC15408の考え方や開発評価モデルが記述されている。この付属書としてプロテクションプロファイル（PP）やセキュリティターゲット（ST）の仕様が定義されている。

パート２は、「セキュリティ機能要件」と題され、製品やシステムが備えるべきセキュリティ機能に関する種々の要件が定義されている。機能要件はクラス－ファミリー－コンポーネントと３層で階層化され現在１１のクラスでセキュリティ機能が記述されている。

パート３は、「セキュリティ保証要件」と題され、設計から製品化に至る過程で、機能要件が確実に実装されているかどうかを評価で確認する（保証する）ための要件が定義されている。保証要件も機能要件と同様３階層で構成され、現在９つのクラスで保証要件が記述されている。

４．１．４　機能要件の内容と依存性について

機能要件を定める１１のクラスとは、下記の通りである。

・セキュリティ監査（FAU）

・通信（FCO）
・暗号サポート（FCS）
・利用者データ保護（FDP）
・識別と認証（FIA）
・セキュリティ管理（FMT）
・プライバシー（FPR）
・TOE セキュリティ機能（TSF）の保護（FPT）
・資源利用（FRU）
・TOE アクセス（FTA）
・高信頼パス/チャネル（FTP）

これらは、あくまでも「機能の要件」であり「実装方式」は規定されていない。また、これらの機能要件には「依存性」と称する要件間の関係が規定されており、これによって各機能要件が適用されるときに併せて適用することが求められる機能要件が指定されている。依存性は、機能コンポーネントが自己完結型でないときその機能が適切に働くために他のコンポーネントの機能を必要とする場合や、セキュリティ機能設計時に機能の「漏れ」を防ぐために定められている。逆に、この依存性を適用しない場合には、設計時に適用しなかった合理的な理由を明示することが求められる。

４．１．５　保証要件の内容と保証できること

保証要件を定める９つのクラスとは以下の通りである。

・PP 評価（APE）
・ST 評価（ASE）
・構成管理（ACM）
・配布と運用（ADO）
・開発（ADV）
・ガイダンス文書（AGD）
・ライフサイクルサポート（ALC）
・テスト（ATE）
・脆弱性評定（AVA）

これらを使って保証できることは、次の通りである。

- セキュリティ基本設計（セキュリティ構造の定義・宣言）が適切であること《ST 評価》
- セキュリティ機能に関係する開発成果物の構成管理として求められる管理レベルを満たすこと《構成管理》

- 対象製品のセキュリティ機能が、製造、検査、搬送、サービスを経て間違いなく利用者が使用できること《配付と運用》
- セキュリティ機能が適切に設計、開発され、設計文書（機能、サブシステム、インタフェースなど）の論理的整合が完全にとれていること《開発》
- 対象製品やシステムを使用する際に利用者が認識すべき事項をもれなくマニュアルに示していること《ガイダンス文書》
- 開発拠点で実施すべきセキュリティ対策として求められる管理レベルを満たすこと《ライフサイクルサポート》
- 対象製品やシステムが正しく実装されたことをテストによって適切に確認していること《テスト》
- 顕在化する脆弱性がないことが分析・確認されていること《脆弱性評定》

PP 評価のみは位置付けが異なり、目標とするところは、PP が完全で一貫性があり、技術的に信頼性があることを実証することである。評価・認証された PP は ST の開発に利用することが可能となり、また登録機関へ登録するに相応しいものとみなされることになる。

４．１．６　評価保証レベル

『評価保証レベル』（EAL : Evaluation Assurance Level）は ISO/IEC15408 の特徴的な手法であり、意図するところは、**開発者が**、製品・システムのセキュリティ機能の実装を「**どれだけ確認したか**」という「レベル」を表すことである。設計、生産、流通、利用（ガイダンスの記述）の各フェーズにおいて、どのフェーズをどれくらい深く評価するか、という組み合わせによって、保証レベルを提示する。このレベルは、CC パート３の「保証要件」から選ばれた要件のパッケージとして EAL１から EAL７までの７段階で示される。

１．１で ISO/IEC15408 に基づく情報セキュリティ評価が“**セキュリティ機能の強度の診断ではない**”と述べたのと同様に、この評価保証レベルも、“**製品がもつセキュリティ機能の差やセキュリティ強度レベルを表すものではない**”ことに注意する必要がある。

次表で、保証レベルと保証要件（各クラスのコンポーネント）のパッケージの組み合わせを提示する。

保証クラス	保証ファミリ	省略名	評価保証レベル(EAL)/保証コンポーネント						
			EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ACMクラス 構成管理	CM自動化	ACM_AUT				1	1	2	2
	CM能力	ACM_CAP	1	2	3	4	4	5	5
	CM範囲	ACM_SCP			1	2	3	3	3
ADOクラス 配付と運用	配付	ADO_DEL		1	1	2	2	2	3
	設置、生成、及び立上げ	ADO_IGS	1	1	1	1	1	1	1
ADVクラス 開発	機能仕様	ADV_FSP	1	1	1	2	3	3	4
	上位レベル設計	ADV_HLD		1	2	2	3	4	5
	実装表現	ADV_IMP				1	2	3	3
	TSF内部構造	ADV_INT					1	2	3
	下位レベル設計	ADV_LLD				1	1	2	2
	表現対応	ADV_RCR	1	1	1	1	2	2	3
	セキュリティ方針モデル化	ADV_SPM				1	3	3	3
AGDクラス ガイダンス文書	管理者ガイダンス	ADG_ADM	1	1	1	1	1	1	1
	利用者ガイダンス	ADG_USR	1	1	1	1	1	1	1
ALCクラス ライフサイクル サポート	開発セキュリティ	ALC_DVS			1	1	1	2	2
	欠陥修正	ALC_FLR							
	ライフサイクル定義	ALC_LCD				1	2	2	3
	ツールと技法	ALC_TAT				1	2	3	3
ATEクラス テスト	カバレージ	ATE_COV		1	2	2	2	3	3
	深さ	ATE_DPT			1	1	2	2	3
	機能テスト	ATE_FUN		1	1	1	1	2	2
	独立テスト	ATE_IND	1	2	2	2	2	2	3
AVAクラス 脆弱性評定	隠れチャネル分析	AVA_CCA					1	2	2
	誤使用	AVA_MSU			1	2	2	3	3
	TOEセキュリティ機能強度	AVA_SOF		1	1	1	1	1	1
	脆弱性分析	AVA_VLA		1	1	2	3	4	4

4．1．7　評価保証レベルと保証度合い、および適用例の関連について

評価保証レベルと保証の度合いについて概略は次の通りである。

（1）　EAL1：セキュリティ機能が正しく利用できることを保証
運用システムやセキュリティが重視されない一般 IT 製品等に適用

（2）　EAL2：設計情報と開発者によるテストが正しいことを保証
セキュリティ機能が要求される一般 OA 製品等に適用

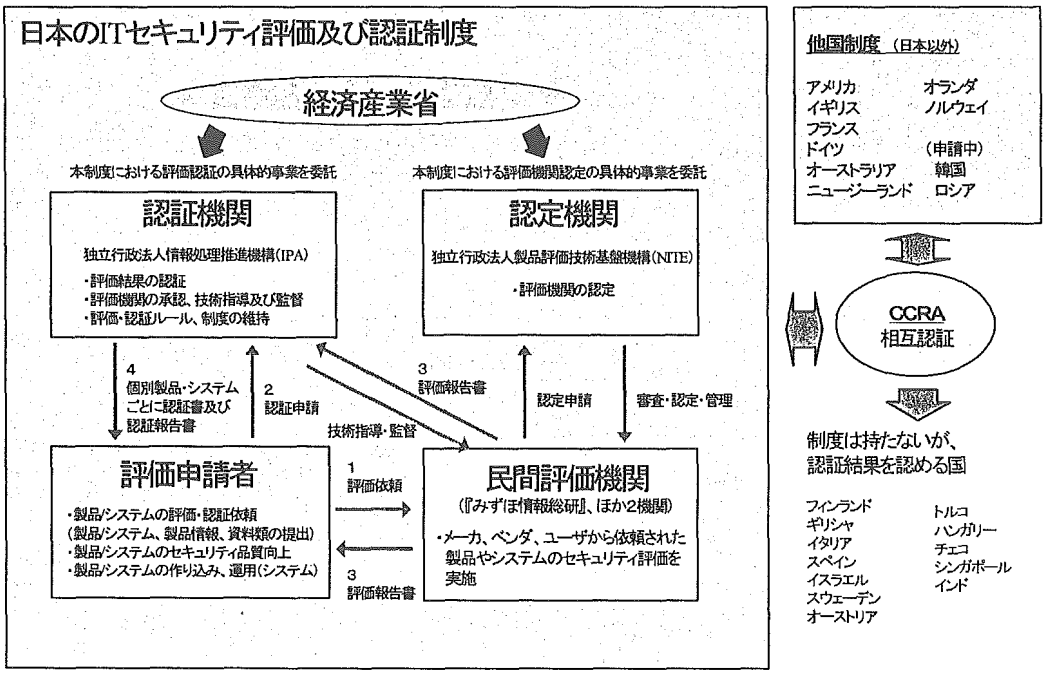
（3）　EAL3：設計、開発が方式的に適切に行われたことを保証
セキュリティ品質が要求されるネットワーク接続製品等に適用

（4）　EAL4：設計、テスト、レビューが系統的に行われたことを保証
高度なセキュリティ品質が要求されるセキュリティ機器・部品、セキュリティソフトウェア等に適用

（5）　EAL5 以上：セキュリティ品質が最優先されるような製品を対象
これはより高品質なセキュリティが求められる製品（IC チップ、セキュリティコンポーネントなど）や軍事目的など、一部の種類の製品で実績がある程度である。

4．1．8　国内制度と政府の動き

わが国では平成13年4月にITセキュリティ評価及び認証制度が発足し、平成14年度より本格的な運用が開始されている。



本評価認証の制度は、評価申請者（SIer、ベンダー等）、民間評価機関（みずほ情報総研、JEITA、ECSEC の3機関が活動）、認証機関（独立行政法人　情報処理推進機構：IPA）の3主体の間の活動として運用されている。（民間評価機関を認定するのは、独立行政法人製品評価技術基盤機構：NITE である）制度の発足・運用の前には、平成12年3月に、行政情報化推進各省庁連絡会議了承事項として、

「各省庁は、セキュリティに関する信頼度の高い情報システムの構築を図る観点から、今後の情報システムの構築に当たっては、可能な限り次の方法等により、ISO/IEC15408 に基づいて評価または認証を図ること

- 調達仕様書にて、セキュリティ機能の全部又は一部が ISO/IEC15408 にもとづいて評価・認証された製品等で実現されることを入札要件とする
- 調達仕様書にて、落札者が提案した製品等について ISO/IEC15408 にもとづくセキュリティ設計仕様書（Security Target）を作成し、納品までに評価機関による評価を受け合格を取得することを契約事項とする旨を明示する」

が決定されている。また、平成17年12月には、政府機関の情報セキュリティ対策のための統一基準が公表され、そこでは

・ 情報システムで使用する機器やソフトウェアについて、要求仕様に基づく認証取得を強化遵守事項とする

という内容が含まれている。

2005年12月現在、日本で認証取得した製品は47件（IPA公表）、2006年3月17日現在評価中の案件は12件と発表されている。

4．1．9　評価認証取得に当たって開発者に求められるもの

評価認証取得を目標とする場合、その対応は商品・製品企画段階から始めることが求められる。「ISO認証」というと「膨大なドキュメントの整備」がセットして語られる場合が多いようだが、それは結果に過ぎない。目指すところは、情報セキュリティ機能要件の設計実装の保証に際して取る保証手段に適応した開発の実施、が本質である。常に、保証要件で要求されることを意識しておくことが重要である。そうであれば、当然のことながら、保証要件に則った開発がなされたことを示す証拠・ドキュメントを残して（整備して）提示することになる。要求される証拠、文書類は以下のようなものである。

・ ISO/IEC15408特有のもの（セキュリティターゲット、脆弱性分析書など）
・ ISO/IEC15408の観点に則って記述された仕様書類（ガイダンス文書、上位レベル設計、テスト分析など通常のドキュメントを評価用にしたもの
・ 構成管理や開発環境に関わるもの（構成要素一覧、開発セキュリティに関する文書など）

4．1．10　評価・認証に対応する留意点

CC評価・認証を取得するには製品企画の段階から最終的な販売・サービスのフェーズに至るまでを考慮した長期にわたる継続的な活動が求められる。そのために、以下に列挙するような種々の留意点に気を配ってプロジェクトを遂行する必要がある。

① 多部門にまたがる活動を推進する体制

・プロジェクトをとりまとめ推進する責任、推進体制の構築
・長期にわたる評価・認証対応を通じた一貫した推進体制の維持

② 開発・リリーススケジュールとの調整

・製品の開発、ISO/IEC15408の両方を理解した評価証拠資料の作成

・要員・工数の確保（評価証拠資料の品質が評価を左右する）
・評価で出される所見事項への対応など手戻り工程の確保
・評価途中での仕様変更への対応

③ 評価に耐えられる証拠の準備

・セキュリティ設計が適切に行われたか（製品設計全体との整合）
・証拠作成の入力源となる社内ドキュメントは十分か、また証拠資料の内容との整合は取れるか

④ 関係者の ISO/IEC15408 に関する理解

⑤ 評価・認証への対応に伴う既存の開発工程への影響

・機能修正・追加、マニュアル変更
・仕様修正、機能修正が発生した場合のテストや脆弱性分析の見直し

⑥実際の開発時点で実施しておくべきこと（後付け困難なので要注意）

・開発プロセスは付け焼刃では「ぼろが出る」
・開発拠点でのセキュリティ確保、構成管理など、事前にセキュリティポリシーを明確化し、適切な手段を講じる必要がある（後からでは取り返しがつかないケースもある）
・確実にコントロールできる自動化手段を適用（構成管理の記録など）

４．２「医療情報システムの安全管理に関するガイドライン」の CC 的位置付け

４．２．１　本節の目的

本節の目的は、厚生労働省（平成 17 年 3 月）より発表された「医療情報システムの安全管理に関するガイドライン」（以下、「ガイドライン」）6 章：「情報システムの基本的な安全管理」および 7 章：「電子保存の要求事項について」に関して、個々の情報システムの開発検討、開発、導入、運用の場面において考慮すべき課題を明らかにし、CC 的観点からコメントを加えるものである。利用にあたっては、「ガイドライン」本編と照らし合わせて、ガイドライン本文記述を参照しつつ利用していただきたい。

４．２．２　構成と使い方

以下では、「ガイドライン」6 章、7 章の各分節それぞれについて、「医療機関等の責任者、

情報システム管理者」および「システム導入業者、システム開発業者」が留意すべき点を指摘し、「ガイドライン」の理解を助ける構成となっている。利用者は、「ガイドライン」本編6章、7章の各項番について、当該項番の記述を合わせ読むことでガイドラインの指摘する事項の詳細をどのように具体化するかについて情報を得ることができる。

4．2．3　第6章の分節詳論

ガイドライン項番	医療機関等の責任者、情報システム管理者のなすべきこと	システム導入業者、システム開発業者のなすべきこと
6．1 方針の制定と公表	当該医療機関が扱う医療情報、情報システムの安全管理に関する方針として、取り扱う情報の範囲、取扱や保存の方法と期間、利用者識別を確実に行い不要・不法なアクセスを防止していること、安全管理の責任者、苦情・質問の窓口、を明らかにし、公表しなければならない。 　情報システムの開発、導入にあたっては、「ガイドライン」に従って定めた方針、規程等を導入業者、開発業者に提示し、当該医療機関が取り扱う医療情報および医療情報システムの安全管理に関する考え方を伝える必要がある。 PPの2章「TOE記述」、3章「TOEセキュリティ環境」、4章「セキュリティ対策方針」に記述される内容の一部が含まれる。	「ガイドライン」本編をよく理解し、医療情報システムの安全管理に関するユーザ、開発者の共通認識の基盤と捉えることで、対象医療機関等から提示される医療情報システムの安全管理に関する方針を受け止め、導入提供あるいは開発を目指す医療情報システムについて方針との齟齬の無いように努める必要がある。 STの2章「TOE記述」、3章「TOEセキュリティ環境」、4章「セキュリティ対策方針」に記述される内容の一部が含まれる。
6．2．1 取扱情報の把握	まず当該医療機関が取り扱う医療情報のすべてを洗い出し、台帳の形で整理する必要がある。個々の情報は、多くの場合、それら一つ一つが単独で保管されていることはなく、あるまとまりとして一枚あるいは複数枚の紙に印刷された形で、あるいは、データベースのレコードとして存在しているのが普通であるから、洗い出しの単位は、その「まとまり」を一単位として行う。洗い出された一単位の情報の重要度分類は、そこに含まれる情報の中の最重要な情報の重要度分類に従う。 情報管理者はこの台帳を常に最新のものになっているように維持管理し、更新があったときはその事実を	提示された情報のリストを検討し、場合によっては提示された一単位の情報のまとまりを分解し、安全管理の観点からシステム開発に最も馴染むような形で情報の組合せを再構成する必要があるかもしれない。個々の情報の一つ一つについてそれが使われる状況や頻度、環境を調査し、医療の現場担当者に対するヒアリングや打ち合わせを念入りに進める必要がある。 対象医療機関等より提示された台帳と実装データとの対照表を常に最新のものに保ち、台帳の更新が伝えられたときには、速やかに実装方式との整合性を分析し、情報システムの健全性を保つことが必要である。 CC的にはここで把握した情報は「保

	速やかに情報システム管理者、導入業者に伝え既存システムへの影響を吸収できるように努めなければならない。 CC 的には、ここで把握された情報は「保護すべき資産」を構成し、PP の３章で記述する脅威の対象になる。次の６．２．２と併せて PP の３章「TOE セキュリティ環境」に記述される内容の一部が含まれる。	護すべき資産」を構成する。情報セキュリティ対策で対処する脅威は「保護すべき資産」に対する脅威として捉えられるから、資産の把握が不十分だと連鎖的に脅威の把握が不十分になり、それは対策の不十分さに繋がる。次の６．２．２と併せて ST の３章「TOE セキュリティ環境」に記述される内容の一部が含まれる。
６．２．２ リスク分析	リスク分析は、あるレベルまでは、全く形式的な行為であると割り切る必要がある。まず保護すべき資産を明らかにし、次に資産に対する脅威の芽は全て可能性として取り上げる。情緒の入り込む余地はないことを理解しなければならない。保護すべき資産は、６．３以降の各節の B:「考え方」の記述の中からとらえることができる。６．３以降の種々の方策は、ここで分析された脅威の存在に応じてとられるものであり、この分析が不十分であった場合には、情報システムは不意の脅威に晒されることになる。逆に、分析の結果、例えば世間一般には存在するのが普通と思われているある脅威が存在しないことが確かめられた場合には、その種の脅威に対して世間一般では必要と認識されている情報セキュリティ対策であっても、当該システムに対しては全く必要ないということもありえる。 本ガイドラインの６．２節と CC の PP 開発の関係として、PP の３章「TOE セキュリティ環境」に記述される脅威の一部が含まれる。PP (ST) に脅威を記載する場合は、ガイドラインにある脅威の現象面的記述だけでは不十分であり、脅威の発生源（犯人、技量、使用設備（HW、SW)、動機)、攻撃対象となる情報材、攻撃（攻撃を受ける情報材ごとに攻撃方法、脆弱性、攻撃の機会）等を詳細に記述する必要がある。 PP の開発においては、更に、４章「セキュリティ対策方針」に記述する脅威と TOE が満たすべきすべての目	システム開発業者は情報システム一般に対する脅威と医療情報について広い知識と深い経験を持った分析技術者を動員しなければならない。その上で、対象医療機関等の個別の状況を知悉してリスク分析を進める必要がある。この段階での分析は、なによりも網羅性が要求さる。次に、情報資産とそれに対する脅威の組のおのおのに対し、情報システムの対策として対応可能な組と、情報システム単独では対応が困難であると思われる組に分類し、以降の運用まで含めたシステム設計における情報セキュリティ面での分析の資料とする。この分析の中には、当然ながら、入出力装置の病院内での物理的な配置などに代表される環境から生じる脅威も含まれていなければならない。 ST の３章「TOE セキュリティ環境」に記述される脅威の一部が含まれる。 PP（ST）に脅威を記載する場合は、ガイドラインにある脅威の現象面的記述だけでは不十分であり、脅威の発生源（犯人、技量、使用設備（HW、SW)、動機)、攻撃対象となる情報材、攻撃（攻撃を受ける情報材ごとに攻撃方法、脆弱性、攻撃の機会）等を詳細に記述する必要がある。 ST の設計においては、更に、４章「セキュリティ対策方針」に記述する脅威と TOE が満たすべきすべての目標を定義する必要がある。 また、本節の内容は、ST の８章「根拠」（通常膨大なドキュメントになる）に直接に繋がることを認識しておく必要がある。

	標を定義する必要がある。 また、本節の内容は、PPの7章「根拠」（通常膨大なドキュメントになる）に直接に繋がることを認識しておく必要がある。	
6．3 組織的安全管理対策(体制､運用管理規定)	組織的安全管理対策の目的は、ややもすると従業者の個人的な努力や資質に依存して達成される安全管理対策の種々の要素から、個人依存性を排除し、従業者の責任と権限の範囲を明確に定めることで抜けのない安全管理対策を実現しようとするものである。従って、組織的安全管理対策には、組織体制、オーソライズされた組織活動の証として必須の規定類の整備と運用、安全管理の対象である情報の全体を明らかにする台帳、管理対策の評価、見直しおよび改善、事故や違反への対処法を含ませることが必須のこととなる。 PPの3章「TOEセキュリティ環境」及び4章「セキュリティ対策方針」に記述される内容の一部が含まれる。	この段階で開発者が考慮するのは、安全管理対策が定める組織体制から導かれる情報システムの利用対象者と利用者の情報システムへのアクセス権限の関係、利用対象者と情報の台帳から得られる個々の情報へのアクセス権限の関係、システムの異常やデータの不整合を事故または違反の現れの指標として使うことができるかもしれない可能性の認識である。 STの3章「TOEのセキュリティ環境」及び4章の「セキュリティ対策方針」に記述される内容の一部が含まれる。
6．4 物理的安全対策	物理的安全対策の目的は、情報システムの機器、デバイス、に対する脅威と情報システムの利用時に想定される脅威を物理的な方法で保護することにある。 PPの3章「TOEセキュリティ環境」に記述される内容の一部を構成する。本節の内容もPPの7章「根拠」の要素に繋がる。	物理的安全対策の目的は、情報システムの機器、デバイス、に対する脅威と情報システムの利用時に想定される脅威を物理的な方法で保護することにある。 STの3章「TOEセキュリティ環境」に記述される内容の一部を構成する。本節の内容もSTの8章「根拠」の要素に繋がる。セキュリティ環境の如何に応じて、情報システム自体のセキュリティ機能の一部を実装する必要がなくなる場合がある。

6．5（1）技術的安全対策:利用者の識別及び認証	医療機関という閉じた情報システムの世界であっても、その世界のなかでネットワークが構築されている限り、また、ネットワーク接続の PC にしろあるいはスタンドアロンの PC にしろ、ほんの僅かでも部外者による PC 操作の可能性が残っているなら、情報システムのアクセス管理は必須の処理となる。 リスク分析の結果、非アクセス権限者の存在の可能性が予想される場合、情報システム管理者は、情報システム導入業者、開発業者に対してリスク分析の結果を伝え、分析に基づく脅威の軽減に効果のあるアクセス管理方式の採用を指示しなければならない。その場合、運用の不備、情報セキュリティ規程・手順の不遵守によるアクセス管理の破綻を防ぐために、情報システムの機能として規程遵守の監視が可能であればその機能の採用を求める必要がある。 6．5節（1）の内容は PP の第 4 章「セキュリティ対策方針」及び第 5 章「IT セキュリティ要件」とりわけ「TOE セキュリティ機能要件」ならびに「TOE セキュリティ保証要件」に記述されるべき内容を含む。またこの第 4 章と第 5 章の関係は第 7 章「根拠」に展開される必要がある。 続く各節（2）～（5）についても同様である。	情報システム導入業者、開発業者は、情報システムのアクセス管理が情報セキュリティの重要な一歩であることを認識していなければならない。利用者の real name と ID 文字列の連関、ID 文字数、ID と role の関係、パスワードの文字列、文字数、更新期限、世代管理、複数の認証システムの併用、ID もしくはパスワードの不正によるログイン失敗時の制御、等々、システム開発者は開発検討時点での最新の知見に基づくアクセス管理方式の全てを調査検討の上、それらを当該医療機関等の情報システム管理者に提示し、開発費用と脅威軽減のバランスの上で最適な手法の選択を提案する（推奨する）必要がある。 6．5節の内容は ST の第 4 章「セキュリティ対策方針」及び第 5 章「IT セキュリティ要件」とりわけ「TOE セキュリティ機能要件」ならびに「TOE セキュリティ保証要件」に記述されるべき内容を含む。またこの第 4 章と第 5 章の関係は第 8 章「根拠」に展開される必要がある。 続く各節（2）～（5）についても同様である。
6．5（2）技術的安全対策:情報の区別管理とアクセス権限の管理	責任者(管理者)は、6．2．1で作成した医療情報台帳の重要度分類に基づき、当該医療機関職員の職責と権限に応じたアクセスポリシーを定めそのポリシーに基づく運用に努めなければならない（システム開発の場合には、そのポリシーを情報システム導入業者に提示する必要がある)。 「ガイドライン」本文にある「必要と権限の関係」の原則はアクセスポリシー策定の重要な要素であることを理解しなければならない。往々にして、実社会の権限に呼応するようなアクセス権限の付与が見受けられるが、その方式は情報セキュリティの保持を必要以上に困難にするもの	対象医療機関等の情報台帳の重要度分類と実装データの対照、及びアクセスポリシーとから、各 ID の role に基づくデータへのアクセス可否の仕組を構築しなければならない。 運用の煩雑さを軽減するためには、最新の人事情報との連携を考慮にいれたアクセス管理や、日々の臨時的な役割定義リストから権限を演繹する仕組などの検討構築も必要になるかも知れない。堅牢確実なだけでなく柔軟なアクセス管理方式を実装しなければ、利用者レベルでの単純な運用に走ってしまい、結果として情報セキュリティの低下を招いてしまう危険を避ける必要がある。

	であることを理解する必要がある。 例えば、実社会での権限の低い層が参照できる領域に対する高権限者の書込み不可制限は、高権限者のみが知りうる情報を誤って低権限者に伝えてしまう脅威を防いでいる。	
6．5（3）技術的安全対策:アクセスの記録(アクセスログ)	アクセスログに留まらずログ一般は、事故・過失・不正等による情報システムの破綻について、破綻の事実を記録し、直接的な破綻の原因や責任の所在を明らかにし、場合によっては破綻の程度を示し、破綻の再発防止策の検討に資する重要な情報である。またログは監査証跡や刑事・民事訴訟における重要証拠にもなりうる公的な性質を持つ記録である。従ってログの記録、保全は、医療情報と同等以上の重要な性格を有する情報であることを理解しなければならない。	ログの記録・保全システムは情報セキュリティの CIA（秘匿性、完全性、可用性）の全てを満たすように構築される必要がある。ログとして残すべき情報の取捨選択と保管情報量・保管システムの入念な検討と同時に、ログの信頼性の基本として、ログ対象となる全システムの同期性の確保が重要である。標準時間の定期的な取り込みによる内部時計の校正とシステム時間の集中管理による医療機関内時間の精度の維持を実現しなければならない。
6．5（4）技術的安全対策:不正ソフトウェア対策	製品、あるいは情報システムの導入検討においては、不正ソフトウェアの混入、侵入、過失によるインストール（善意の第三者を装った者からの送付等）から病院システムを保護する手段の検討が必須である。現在広く使われている手法は、コードスキャニングによる不正コードの特徴的パターンの発見・摘出ですがそのためには不正コードパターン DB を常に最新のものに保つと同時に、運用する情報システムの基本ソフトウェアについてもセキュリティホールに関する最新情報の収集と最新パッチの充当が求められる。これらの対応は、PP においては第 4 章「セキュリティ対策方針」に記述することになる。 対策の中には、不正ソフトの侵入・発症が現実のものとなってもそれによる内部データの破壊や漏出は許さないような機能が検討されている例もあるので、常に最新の対策ソフトの動向に注目することも重要である。	ウィルス対策ソフトやスパイウェア対抗ソフトそれ自体を開発する場合を除いて、一般的な医療ソフトウェアや院内システムの開発においてそれらの機能として対ウィルス、対スパイウェア機能を盛り込むことはまれかもしれないが、リスク分析の中では、それらによる脅威とそれらに対する対策を施した環境のもとでの運用を前提とする場合は多いかもしれない。その場合は、ST の第 4 章「セキュリティ対策方針」に記述することになる。

6．5（5）技術的安全対策:ネットワーク上からの不正アクセス	ネットワーク接続に際してのファイアウォールの設置も、6．5（4）と同様にセキュリティ対策方針としてPPの第4章に記述することになる。 ネットワーク製品では対策の方式がいろいろ検討されているので、特質を検討し、自病院（診療所）の情報環境に応じた複数の対策ソフトを導入するのが望ましい。	本節も前節同様システムの運用の前提としてST第4章セキュリティ対策方針の中に記述することになる。
6．6（1）人的安全対策:従業者に対する人的安全対策	従業者の雇用については、ガイドラインに記載の通りであるが、情報システムへの脅威の面では、ガイドライン記載の(a)～(e)の種々のロールを演じる登場人物の全体的管理が必要になる。管理の実態は、6．5節における（1）～（3）の項で記載したとおり、医療情報種別とロールとの対応を整理し権限の付与を検討することになる。6．5と同様、PP第4章、第5章、にセキュリティ対策方針と要件を記述しそれらの関係を第7章で展開することになる。 次の（2）についても同様である。	開発サイドからみた本節の内容は、6．5（1）～（3）の再掲になる。
6．6（2）人的安全対策:事務取扱委託業者の監督及び守秘義務契約	事務取扱委託業者の監督及び守秘義務契約の措置についてはガイドライン記載の通りです。本節の内容は、運用面での対応（ISMS的側面）になります。情報システム面での検討は、6．8を参照してください。	開発サイドから見た本節の内容は、6．8を参照してください。
6．7 情報の破棄	多数の複数の情報が関連しあう情報システムにおいては廃棄、破棄について予め検討する必要があることをガイドラインは述べている。これは、情報システムの可用性の破綻が往々にして日常の定常的な作業の情報破棄の局面で出現するからである。破棄行為に伴う秘匿性担保の面での検討は当然のこととして、可用性の維持についても、取り扱う情報の設計段階から情報廃棄時のリスク分析を行い、対抗策（機能要件）の検討を含めPPの第3章～第7章に展開する。	情報を破棄する際の秘匿性、完全性、可用性の破綻はCC面における脅威として十分な検討が必要である。大域的なデータ破棄とともに、局所的なデータ破棄の際のセキュリティ破綻も等しく分析の対象としなければならない。検討結果は、ST 第3章～第8章に展開する。

６．８ 情報システムの改造と保守	本節も６．７節と同様、情報システムの可用性の維持に大きな影響を及ぼす事象であるが、本節で問題にしているのは、メンテナンスに伴う、個人情報保護の破綻、真正性、見読性、保存性（診療録等の電子媒体による保存についての三基準）の破綻に対する対応である。 メンテナンス時は、通常の運用モードとは明らかに異なるモードで情報システムが稼動している、という認識が重要である。従って、メンテナンスを統御する規程では、メンテナンス作業を行う業者、作業者の識別、業者側管理者、メンテナンスの日時、メンテナンスの範囲、作業内容、作業に利用するIT機器の種別、院内ネットワークへの作業機器接続の有無、記憶媒体の利用の有無、アクセスを許す情報の種別とアクセス種別（及びその深さ）、作業開始前のバックアップの範囲、等の管理が必須になる。特に最近の情報システム事故の事例に鑑み、メンテナンス請負業者の従業員に対するPCコントロールの有無の確認は必須である。従業員のPCコントロールを行っていない業者にメンテナンスを任せてはいけない。 メンテナンス管理の機能は可能であれば情報システムに組み込まれるべきであり、それらはPPの第3章～第7章に展開される内容になる。	メンテナンスは情報システムの完全性、可用性、および信頼性の維持にとって不可欠の作業である。従って、開発者はメンテナンス機能に組み込むメンテナンスコマンドの機能、メンテナンス機器、メンテナンス作業者に付与する権限、メンナンス作業者がアクセスすることになる情報等を十分に分析し、メンテナンス時に特有のリスク分析を行わなければならない。それらは、ST3章の脅威の項に詳細に展開されるべきであり、それらに対する対抗策、セキュリティ機能要件、保証要件以下を、第4章~第8章に展開することになる。
６．９ 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	本節は、特に個人情報を外部機関に委託する場合、電気通信回線を用いて送信する際の注意事項を指摘している（保存の委託は、ガイドライン8.1.3で詳述されている）。個人情報保護法では、その第20条で情報の取扱において安全管理を要求しているのでそれに応える節になる。ガイドラインは個人情報の秘匿を組織情報秘匿の枠組より一層限られた範囲の枠組で捉えることを要求している。 ①の記述はそのことを言っている。 ②は、情報伝達の送受エンティティが情報送信の前に相互認証することを要求しています。通常のSSL（イ	電気通信回線を利用したアプリケーションの開発において、組織間ではなく端末間秘密通信の採用を求めている。企画段階では、流れるデータに個人情報が含まれることがあるかどうかの確認が重要である。一般ユーザは、よく、「殆ど流れないから大丈夫」という言い方をするが、1件でも可能性があるなら、それなりの対応が必要である。セキュリティが問題になっている場合、件数は判断の基準にならない。STの設計における脅威の分析が重要である。本節の記述はすべてSTの第3章で展開・考察される内容である。

	ンターネットのショッピングサイト等）では一般ユーザを対象としているため片側認証で運用されているが、本節は、SSL を利用するのであれば、送受ともに、信頼できる認証局により発行されたサーティフィケーションを使った利用であること、あるいは VPN を利用したエンティティ間の仮想専用線通信であること、あるいは ISCL を用いた共有鍵方式による秘密通信であること、等を要求している。また、③は情報保存リモートサーバーへのログイン・プロシジャにおいて送受する情報が平文（暗号化無し）で運用する危険を指摘している。この節の記述は総体的に PP の第 3 章(とくに前提と脅威）に展開される。	

４．２．４　第７章の分節詳論

本節ではガイドライン７章各節について、医療機関等の責任者、情報システム管理者のなすべきことと、システム導入業者、システム開発業者のなすべきことを対応して記述する。７章は法令あるいは厚生労働省の施行通知が要求する機能を実現するためのガイドラインであるため、特に IT 技術的に出来ること出来ないことを明確に切り分けた上で実装の検討に進む必要がある。とくに、７．２の見読性ではシステムのスループットやパフォーマンスが制約としてあり、７．３の保存性においては IT 技術の歴史的時間軸の単位での議論が求められていることは、可用性の範囲が非常に広く捉えられていることとして注目すべきことである。どこまで IT で対応可能か十分な検討が必要である。

ガイドライン項番	医療機関等の責任者、情報システム管理者のなすべきこと	システム導入業者、システム開発業者のなすべきこと
７．１ 真正性の確保について	施行通知では、「故意または過失による虚偽入力、書換え、消去及び混同が防止され、かつ作成の責任の所在が明確である」ことをもって真正性が確保されている、と定義している。本節の趣旨は、一貫してこの真正性の確保に向けた指針の記述である。真正性に対する脅威は、上記定義の 2 条件の少なくとも一方を阻害する行為・動作であるから、CC 的には、その脅威に対抗する対処方針の実装を如何に実現するかを記述することになる。７．１節本文はガイ	真正性の定義に基づき、開発の対象となるシステムが取り扱う全ての情報に対する脅威の出現可能性と出現の様相を検討しなければならない。ガイドラインには医療の現場における種々の状況が説明されているが、それに対する対処療法的な対応ではなく、真正性を阻害する要件に対する本質的な対応を各状況に敷衍する意識で対応する必要がある。ST で言えば 4 章の検討が非常に重要になる。７．１の C 項、D 項には、多くの状況下での対応が記述されているので、それら

	ドラインの全記述中最長の１つであるが、脅威が明快であるから、対応に紛れは少ないといえるであろう。IT 技術的対応あるいは運用による対応のいずれの検討にあっても、2条件の担保を中心に作業をすすめることになる。ただし、真正性が要求される対象情報の入出力の種類や情報生成の機器の種類は多種に及ぶので、実際の現場で使われる手法・機器の全体を漏れなく押さえる緻密さが要求される。本節の記述は、PP の 3 章、4 章、5 章のすべてに影響を及ぼす（直接利用できる）内容である。	をセキュリティ対策方針に変換することから作業は始まるであろう。また、5 章の IT セキュリティ機能要件では、まず、CC パート２にカタログ化された１１のクラスに拘ることなく IT 技術の展開を検討することが重要である。
７．２ 見読性の確保について	施行通知では、「情報の内容を必要に応じて肉眼で見読可能な状態に容易にでき、かつ、情報の内容を必要に応じて直ちに書面にできること」をもって、見読性が確保されている、としている。B 項の「考え方」には、「必要に応じて」の意味として、「診療」、「患者への説明」、「監査」、「訴訟」の４つが例示されている。この４つの場合のそれぞれに対応できること、と明示されているので、CC 的対応はある意味、非常に直接的である（その要件は C 項に記述されている）。重要なことは、「必要に応じて」「肉眼で」「容易に」以外のいかなる制約条件も添えられていないことである。これは、人間の活動が可能な状況ならどんな場合であっても達成されることが要求されているということである。本節においても、B 項でもとめられていることが前提条件あるいは脅威に直結する。CC 的には、B 項から 3 章の内容を抜きだし、C 項、D 項から対処方針を作成することになるが、秘匿性の要素は殆どないので CC 的には、完全性の保持以外、やや馴染まない条件かもしれない。	本要請では、情報セキュリティ的には、可用性と信頼性が非常に重要な要求である。しかもこの可用性には「肉眼で」「容易に」の時間的、視覚的な条件が厳しく付加されている。ST 的には、第 5 章の IT セキュリティ機能要件以上に、IT それ自体の能力を強調した書き方になるであろう（CC パート２では可用性にあまり比重がおかれていない）。ガイドライン C 項に在るとおり、システムの冗長性や、バックアップ体系など、IT 技術と運用の双方を効果的に組合せた検討が必要になるであろう。
７．３ 保存性の確保について	施行通知では「法令に定める保存期間内、復元可能な状態で保存する」ことをもって保存性が確保されている、としている。B の考え方では、更に敷衍して、「法令等で定められ	IT 機器・メディアの耐時間変化性が強く求められる条項である。真正性、見読性を維持したまま、如何に格納情報の完全性を保ち続けるかが重要である。保存装置、メディアの進化に即

	た期間に渡って真正性を保ち、見読可能にできる状態で」保存されること、としている。従って、見読性、真正性の、「法令の定める期間内」の維持が中心課題になる。７．２と同様、B 項から前提と脅威を取り出して第３章を構成し、C 項、D 項から対処方針を抜き出すことになる。	応可能なシステム構成と運用の工夫が必要になる。
７．４ 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	電子署名については、IT 技術としては署名方式、確認方式が実用的に十分な機能をもって運用されていることから、署名の有効範囲（署名がカバーする情報の範囲、及び時間的範囲）をどのように決めるかが課題になるであろう。CC 的には署名の確認方式の部分に若干の検討項目が存在する。	病院システムとしては、署名につけるサーティフィケーションの有効性の確認や、院内の時間システムの整合性、タイムスタンプ取得の手法などが問題になるであろう。ガイドラインは制度としての電子署名方式に対する検討に意が注がれているが、院内システムとして運用面での検討を深める必要があるであろう。

４．３　ガイドラインの規範化について

４．３．１　ガイドラインと PP

ISO/IEC15408 における PP では、TOE（Target of Evaluation）と称される評価対象に関して、個別具体的な製品・システムではなく、1 つのカテゴリーとみてそこに属する製品に共通の“実装には依存しない IT セキュリティ要件”を定義する。しかしそれは抽象的な要件ではなく、病院・診療所等で稼動する製品・システムで言えば、受付システム（初診、再診、入退院）、患者データベース、電子カルテシステム、画像処理システム、検査情報システム、医事会計システム、ネットワーク制御機器、等々の製品・システムカテゴリーとしてまとめることのできるものに対して共通に或いは単独のカテゴリーごとに利用可能な要件を規定するものであり、通常は、あるひとつのカテゴリーにおいて複数のメーカー・ベンダーから種々の製品・システムが出揃ってきたところで、それらに共通の要件を抽出して出来上がるものとしてよい。逆にいえば、そのような具体的な商品が出揃ってからでなければ、本来の PP の目的（すなわち利用者側の要求）と提供者側の実現可能性とのギャップを埋めるのは難しいということでもある。つまり、情報セキュリティが求められるある分野において情報セキュリティに関する環境や機能について一定の類型化が達成できたときに初めてその分野で意味をもつ PP をつくることができる、ということである。

一方、本ガイドラインは、これまで連綿と継続している医療の現場において主として紙ベース（および銀塩フィルムに代表される画像処理装置）で運用されてきた情報処理の現場で利用可能な IT 技術の利用・運用について、従来通りの（あるいはそれ以上の）信頼性、安全性、確実性をもたせるための指針として作られている。従って、対象分野や情報セキュリティに関する要請は十分に具体的ではあるが、IT 製品・IT システムとしては機能面においてもあるいは運用面においても多方面にわたるため、「医療情報システム」として PP にま