とめるのは非常に難しいと言うことができる。

従って、本節においては、「医療情報システムの安全管理に関するガイドライン」を直接PP化するための検討ではなく、一般論としてCCにおいて作成するST（あるいはSTが参照するPP）が、「TOEセキュリティ環境」、「セキュリティ対策方針」、「ITセキュリティ要件」（いわゆるST(PP)の3章から5章まで）の3つ組でTOEのセキュリティの実現を記述しているように、本ガイドラインからST(あるいはPP)を導きだすためにはこの3つ組をどう抽出するかに向けた検討をすることとする。ただし、4．3．3項においてガイドラインの一要件である7章1節の「真正性」をモデルにして模擬的なPP化の試みをおこなう。

4．3．2　ガイドラインのCC類似の運用について

（a）ガイドラインの運用

本ガイドラインをCC類似の位置付けで利用するためには、CCがST（PP）に規定しているITセキュリティ実現の枠組みを把握する必要がある。

CCでは

I.　対象となる製品・システムに対して想定されている「TOEセキュリティ環境」（これは、「前提条件」、「脅威」、および「組織のセキュリティ方針」の3つから構成される）

に対処する

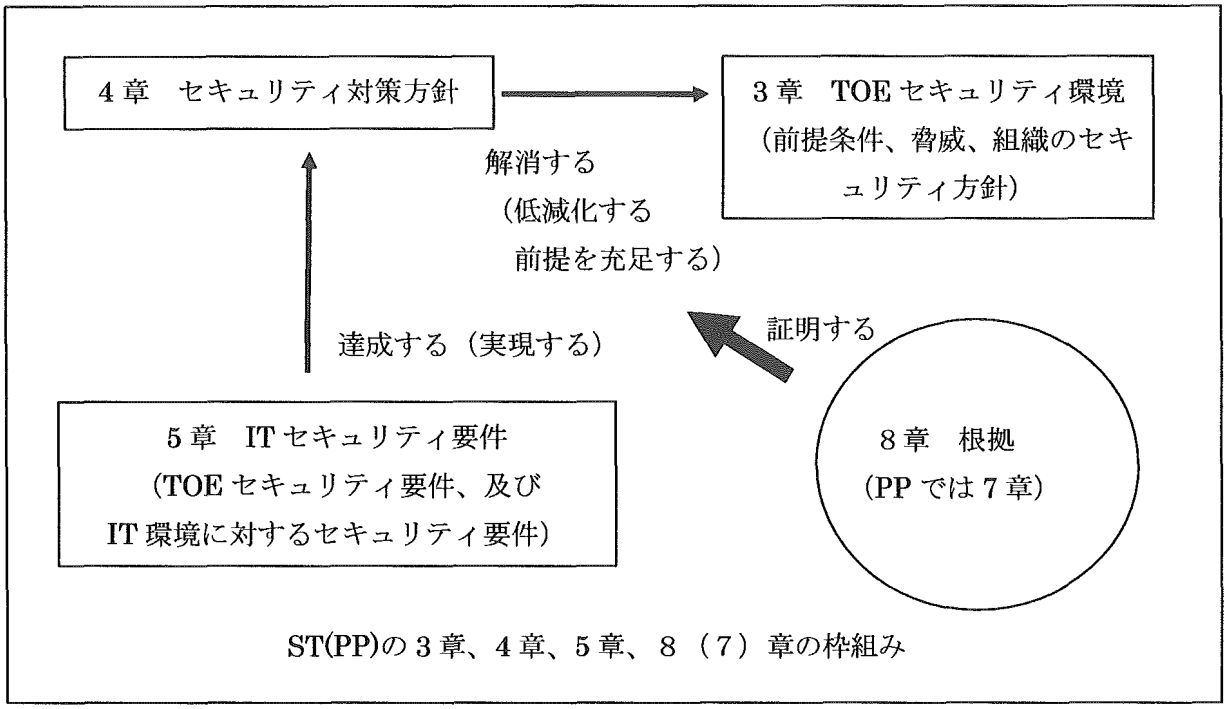
II.　「セキュリティ対策方針」

を

III.　「TOEセキュリティ要件」（これは、「TOEセキュリティ機能要件」と「TOEセキュリティ保証要件」の2つから構成される）

によって実現する枠組みを構築している（下図参照）。

これと同様に、本ガイドラインを用いて「医療情報システムの安全管理」の実現の枠組みを構築するためには、ガイドラインの記述から「TOEセキュリティ環境」、「ITセキュリティ要件」および「セキュリティ対策方針」類似の概念相当物を抽出し、その中で「TOEセキュリティ環境」に対処する仕方を構築することになる。ただし、本ガイドラインの記述にはCCでいう保証の概念は明示的には記述されていない。



ST(PP)の3章、4章、5章、8（7）章の枠組み

この枠組みで「安全管理に関するガイドライン」の第6章7章をあらためて整理すると、次表のようになる。

項番	名称	意味するところ	対応するPP(ST)内の章	
6.1	方針の制定と公表	セキュリティ方針	2章 3章 4章	TOE記述、及び組織のセキュリティ方針 ITセキュリティ要件
6.2.1	取扱情報の把握	情報資産管理	3章	前提条件
6.2.2.	リスク分析	脅威の摘出と分析	3章	脅威
6.3	組織的安全管理対策	運用、環境の整備	3章 4章 5章	前提条件 セキュリティ対策方針 ITセキュリティ要件
6.4	物理的安全対策	運用、環境の整備	3章 4章 5章	前提条件、脅威 セキュリティ対策方針 ITセキュリティ要件
6.5	技術的安全対策	ITによる対応	3章 4章 5章	前提条件、脅威 セキュリティ対策方針 ITセキュリティ要件
6.6	人的安全対策	運用	3章 4章 5章	前提条件、脅威 セキュリティ対策方針 ITセキュリティ要件

6.7	情報の破棄	IT による対応、一部運用を含む	3 章 4 章 5 章	前提条件、脅威 セキュリティ対策方針 IT セキュリティ要件
6.8	情報システムの改造と保守	IT による対応、一部運用を含む	3 章 4 章 5 章	前提条件、脅威 セキュリティ対策方針 IT セキュリティ要件
6.9	外部との情報交換	運用、方針、一部 IT による対応策を含む	3 章 4 章	前提条件、脅威 セキュリティ対策方針
7.1	真正性の確保について	脅威、運用、方針、一部 IT による対応策を含む	3 章 4 章 5 章	前提条件、脅威 セキュリティ対策方針 IT セキュリティ要件
7.2	見読性の確保について	脅威、運用、方針、一部 IT による対応策を含む	3 章 4 章 5 章	前提条件、脅威 セキュリティ対策方針 IT セキュリティ要件
7.3	保存性の確保について	脅威、運用、方針、一部 IT による対応策を含む	3 章 4 章 5 章	前提条件、脅威 セキュリティ対策方針 IT セキュリティ要件
7.4	法令で定められた記名・押印を伝署名で行うことについて	脅威、運用、方針、一部 IT による対応策を含む	3 章 4 章 5 章	前提条件、脅威 セキュリティ対策方針 IT セキュリティ要件

6．3以降のいずれもの節で対応する PP の章に3章が出現するのは、各節の B：考え方に、その節で取り扱うガイドラインが対処する脅威や前提が提示されているからである。本ガイドラインの PP（ST）化においては、B 節の記述から漏れなく脅威と前提を抜き出す必要がある。また記述の一部には、根拠（PP7 章、ST8 章）に書いても良い部分が含まれる。

（b）ガイドライン各節のC：、D：について

各項のC：最低限のガイドライン、D：推奨されるガイドラインは、ＳＴの「セキュリティ対策方針」に相当する記述とみることができる。

ＣＣ的には、「最低限」と「推奨」の差は、ＳＴを作成するに当たって参照するＰＰの差とみることができる。アメリカの例では、同一の製品カテゴリーに要件の厳格さに差のある複数のＰＰが用意され、どのＰＰを参照するかはＳＴ作成者（あるいは発注者の指示）にまかされるというような使い方がある。

5 章に記述する内容のうち、TOE セキュリティ機能要件は CC の場合には、CC 規格書パート２に記載された１１のクラス－ファミリー－コンポーネントの中から取捨選択して記述するものであるが、本ガイドラインの場合には現時点では直接参照する文献・資料は存在しない。

（c）ガイドラインを利用した脅威の抜き出し例

上記記述に「B節の記述から漏れなく脅威と前提を抜き出す」と書いたが、そのような例として、6．7「情報の破棄」のB節の解釈例を下記に示す。解釈にあたっては、他の章で取り扱う事項も生じる可能性はあるが、一応6．7単独で見ていくことにする。

6．7のB節は以下の通りである。

> 医療に係る電子情報は運用、保存する場合だけでなく破棄に関しても安全性を確保する必要がある。またデータベースのように情報がお互いに関連して存在する場合は、一部の情報を不適切に破棄したために、その他の情報が利用不可能になる場合もある。
>
> 実際の廃棄に備えて、事前に廃棄プログラム等の手順を明確化したものを作成しておくべきである。
>
> 外部の委託機関等に保存を委託している診療録等について、その委託の終了により診療録等を破棄する場合には、速やかに破棄を行い、処理が厳正に執り行われたかを監査する義務（または 監督する責任）を果たさなくてはならない。また、受託先の機関等も、委託元の医療機関等の求めに応じて、保存されている診療録等を厳正に取り扱い、処理を行った旨を明確に示す必要がある。

本節のキーワードは「破棄に際しての安全性の確保」である。分析にあたって、まず「破棄」の対象は何かを明らかにする必要がある。情報それ自体は単独で存在するわけではないから、「情報の破棄」とは情報を収めるメディアから情報を破棄（削除）することと同時に情報を収めるメディアの破棄の２つを考えることになる。また、「破棄」は人間の行為であるから、「意図した破棄」と「意図していない破棄」の２面があることに注意する。つまり、「意図した破棄」のすべてを分析したあとで、それらが「意図していない破棄」という状況の下で、であったらどうかを更に分析する、ということである。次に「安全性」であるが、これは情報セキュリティが担保されている、ということであるから、「秘匿性」、「完全性」、「可用性」、「真正性」、「責任追跡性」、「信頼性」の６要素について、破棄の対象となった情報・メディアでの確保の状況を考えるだけではなく、破棄に際して、残された方の情報システム・情報の安全性（６要素）も考える必要がある。また、「破棄の行為」が組織内部の行為か、外部委託の行為かによっても脅威の貌は変化する。

従って、下表の各枡一つ一つについて脅威を考察することになる。

内部の破棄の場合

	秘匿性	完全性	可用性	真正性	責任性	信頼性
メディアからの破棄（削除）	A1	B1	C1	D1	E1	F1

メディアの破棄	G1	H1	I1	J1	K1	L1

外部委託破棄の場合

	秘匿性	完全性	可用性	真正性	責任性	信頼性
メディアからの破棄（削除）	A2	B2	C2	D2	E2	F2
メディアの破棄	G2	H2	I2	J2	K2	L2

以下脅威の例

（A1）破棄（削除）が不完全で復元できてしまう

（A1）論理上破棄されただけで実態が残っている

（A1）システムの作業ファイルにコピーが残っている

（A1）キャッシュメモリーに情報が残っている

（B1）リンク先との整合性が取れなくなり、マッチング処理でエラーがおこって処理が進まない

（C1）（B1）と似たような状況であるが、そもそものアプリソフトが起動できなくなった

（D1）真正性の証拠データを含むファイルを削除したためにリンク先データの真正性が確認できなくなってしまった

（E1）旧システムの関連ファイルを消去したら、実は新システムも参照していたため、正しくログイン処理ができなくなってしまった

（F1）旧システムのコンフィギュレーションファイルを消したら、新システムもそこを参照していたので、勝手なテンポラリーコンフィギュレーションファイルが生成され望んだ動作をしなくなってしまった

（G1）メディアの中に情報が残ったままで拾得した者に情報が漏れた

（G1）情報の印刷された紙が裁断されることなく捨てられ情報が漏れた

＜H1～L1は割愛＞

（A2）作業者がミスを恐れるあまり不正にバックアップをとっていた

（A2）二次委託業者に破棄の指示が伝わってなかった

（G2）廃棄・破壊される筈だったＰＣが情報を残したまま転売されてしまっていた

＜H2～L2は割愛＞

前提の例としては、

(A2) 情報の委託先とは処理完了したときは速やかに消去する契約を結んでいる
(G2) 廃棄委託業者とは復元できない状態でメディアを破棄する契約を結んでいる

等々がある。明示的に記されていなくても、記述の一行一行に脅威あるいは前提が書き込まれていることに注意して分析を進める必要がある。

4．3．3　例示：真正性について

本節では、ガイドライン記述のPP化の検討をガイドライン7章「電子保存の要求事項について」の7．1節「真正性の確保について」を例として行う。医療情報を取り扱うIT機器・システム全体としたときはTOE記述も膨大な内容になると思われるが、本節の例示では、TOEとして、以下のような真正性の確保にのみ特化した抽象的な情報処理機器（或いはシステム）とする。

以下の記述で＜・＞で囲まれた部分は注釈である。

4．3．3．1　PP概説

＜CCが定めるPPではPP概説には、PP登録を行うのに必要なPP識別とPP概要からなる、とされている。本説では、例示であるので簡単な記述にとどめる＞

（1）PP識別

PP名称：情報の真正性を確保して保存する装置SE1のプロテクションプロファイル
バージョン：0．01
作成日：平成18年3月28日
作成者：MEDIS-DC
＜以下、CC識別（PPの記述に用いたCCのバージョン）、PPの評価者、PPを検索する場合に利用可能なキーワード等を記載する。＞

（2）PP概要

＜PP概要では、PP記述の対象となるTOEについて、PPの潜在的利用者が対象とするTOEのST記述に有用か否かを判断するための内容を記述する。本節で言えば、対象がDBMSなのか、HDDなのか、医療情報システムなのか対象は定まっていないので、仮にもっとも抽象的なレベルで「真正性を確保して情報を保存するシステム」とする。実際上は、TOEはDBMSのカテゴリー、HDDのカテゴリー、システムのカテゴリー等、抽象度を大幅に落として、利用者が

まさに開発しようとしている製品・システムのカテゴリーに正確に合致する範囲で記述しなければ有用性は低いものと思われる。＞

（本文は略）

（3）その他

＜PP 概要には、その他「CC 適合」、「参照資料」、「PP 記述の規約（ローカルな規約である）」、「PP 記述で使用する略語」、「専門用語」などを記述する。略語にしろ専門用語にしろ一般的通用性は特に要求されない。技術的常識の用語の範囲で定義が明確であればよい。＞

4．3．3．2　TOE 記述

本節では TOE 記述を展開する。

＜TOE 記述では、そのセキュリティ要件の理解を助けるものとして記述される筈のものなので、製品種別やその製品の一般的な IT 機器としての機能も示さなければならない。具体的には、「TOE の概要」（TOE 種別、TOE の機能および利用方法など）、「TOE 構成」（物理的構成や論理的構成など）、「TOE の保護資産」を書き下すことになる。TOE のセキュリティ面での特質を打ち出すためにも TOE 記述では、イラストなども使って、利用環境や、他の IT 機器との関係、設置場所に関するトポロジーなど、以下の TOE セキュリティ環境を活写するものである必要がある。＞

4．3．3．2．1　TOE 概要

＜TOE 概要では、TOE のセキュリティ要件の理解を助けるものとして記述する。TOE の製品種別や一般的な IT 機器としての機能などを記述する。＞

（本文は略）

4．3．3．2．2　TOE 保護資産

＜本例示で重要なのは「TOE 保護資産」である。PP3 章の TOE セキュリティ環境における脅威の記述においては、「何に対する脅威なのか」の「何」に当てはまるのが「TOE 保護資産」であるからである。

TOE 保護資産としては例えば「医療行為の中で生成された真正性が確保された状態で保存義務のある＜情報＞」というようなものになる。当然ながら、TOE が使われる種々の状況の中で、「画像処理装置」、「検査装置」の特徴に合わせて＜情報＞の記述は変更されてよい。＞

本 TOE における保護資産は次の通りである。

・ 医療行為の中で生成された真正性が確保された状態で保存義務のある“情報”を本 TOE の保護資産とする。

ここで「真正性」は、次の意味とする。

(a) 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、同時に

(b) 作成の責任の所在が明確である

ような情報を真正性が確保された情報であるという。ここに、「混同」とは、情報の対象（患者）を取り違えた記録がなされたり、記録された情報間での関連性を誤ったりすることをいう。

4．3．3．3 TOE セキュリティ環境

本節では TOE セキュリティ環境を記述する。

＜本項以下が PP の中心的記述になる。本例示では、ガイドラインの記述がすべてであるから、記述に用いる概念はすべてガイドラインから引き出すことになる。本項では、前提条件、脅威、セキュリティ方針はすべて識別されなければならないので、記述を表形式で行うのが見やすいと思われる＞

（a）前提条件

TOE の使用、運用時には、下表で詳述する環境が必要になる。

識別子	定義
A.EQUIPMENT	TOE を構成する機械は正常な環境下において意図した入力を正確に保存装置に出力する
A.SOFTWARE	TOE を構成するソフトウェアは正常にインストールされた状態においては意図した入力を正確に保存装置のドライバーに伝達する。
A.REPLACE	TOE を構成する機械やソフトウェアは正常に設置されインストールされた状態を維持している。
A.LOCATION	TOE が設置された場所には正当な権利を有しない操作者は立ち入ることができない。
A.REVIEW	TOE に対して正当なアクセス権を有する者は、正常業務においては、正しい操作・処理を行なったかどうかを常に心にとめ確認を行う。

A. は Assumption の意

（b）脅威

TOE に対する脅威を下表に詳述する。TOE に対する攻撃者については、IT 機器、ネットワーク、医療情報装置の動作について一般的知識を有し、TOE 保護資産の所在やそのアクセス方法を知悉し、院内のネットワークに物理的に接続して任意のサーバマシンに対するログイン・プロシジャまでは正常に進む技量を有してい

るものとする。また、TOE 保護資産にアクセスする正当な権利を有する者であっても、過失行為の瞬間には不正な攻撃者と同等の存在とみなすこととする。

識別子	定義
T.SPOOF	攻撃者は悪意をもって虚偽入力により偽の保護資産を生成するか、正常な保護資産を書換えるか、消去するかあるいは正常な保護資産に混同を生じせしめる。
T.MISSTEP	保護資産に対して正当なアクセス権を有する者が、過失により結果として虚偽入力を行い偽の保護資産を生成するか、正常な保護資産を書換えるか、消去するかあるいは正常な保護資産に混同を生じせしめる。
T.ACCOUNT	蓄えられている保護資産の生成責任者が不明になる。

T.は Threat の意

＜本節における「脅威」は、真正性の阻害の一点に焦点を当てている。＞

（c）組織のセキュリティ方針

本 PP が想定する組織のセキュリティ方針は不明である。

4．3．3．4　セキュリティ対策方針

本節ではセキュリティ対策方針における施策について述べる。

（a）TOE のセキュリティ対策方針

TOE のセキュリティ対策方針を下表に示す。

識別子	定義
O.LOGIN	TOE のログイン処理においては、IT 面での性格の異なる 2 種以上の識別情報を用いて操作者の識別を行う。
O.ROLE	データの入力においては、ログイン処理時に識別された操作者のロールを認識し、保護資産のレコード単位でアクセス権限を検査する。
O.TERMINAL	保護資産の入出力を許す端末は特定され、正当な端末以外の端末からの操作においてはたとえ正常な権限者によるものであってもアクセスを拒否する。
O.REMOTE	内外のネットワーク経由で保護資産の管理サーバにリモートアクセスをしてきた場合には、アクセス端末が正当な権限を有し、かつ接続回線のセキュリティ対策が整っている場合にのみ許可する。
O.DOUBLECHK	保護資産の重要度に応じて、入力操作は 2 度入力とし、2 回とも同一の情報であるときのみ入力を許可する。
O.CHKBOX	入力操作領域にはチェックボックスを設定し、全項目に対する入力操作者の確認チェックが無ければ保存を拒否するようにする。
O.RECOVER	過去の任意の更新の時点にさかのぼって確定済みの保護資産を

	再現することができる。
O.AUTHENT	確定された保護資産は、そのロケーションに依らず確定済みであることを示す作成者による署名が付随して、必要の都度、参照確認することができる。
O.UPDATE	すべての保護資産は識別され、確定された内容変更が発生した場合には変更前と変更後の状態の参照が常に可能であるようにする。

O.は Objective の意

（b）環境のセキュリティ対策方針

TOE 環境に対するセキュリティ対策方針を下表に示す。

識別子	定義
OE.DEPUTY	保護資産に対する正当なアクセス者に代わって代理を行う手続きが制定されている。
OE.WHODEPUTY	代行処理の記録は正当な代行者を識別できる。
OE.DOBLECAST	同一の保護資産に 2 人以上の正当なアクセス権限者を設定する規則が定められている。
OE.LECTURE	TOE に対する従業員教育体制が整えられている。
OE.COMPLIANCE	従業者に対する院内規則に関するルール遵守教育が定められていて実施されている。
OE.BIOKEY	TOE 設置室の扉には生体認証式の施錠処理がなされている。

OE.は Objective Environment の意

4．3．3．5　IT セキュリティ要件

＜本項に関しては、ガイドラインに対応する明確な定めはない。本項では TOE セキュリティ要件として TOE セキュリティ機能要件および TOE セキュリティ保証要件、並びに IT 環境に対するセキュリティ要件を記述することになるが、これらは CC パート 2 から機能コンポーネントを、及び CC パート 3 から EAL を選択して記述する。＞

4．3．3．6　適用上の注釈

＜必要に応じて任意に記載することができる＞

4．3．3．7　根拠

本章では本書の完全性と一貫性を検証する。

4．3．3．7．1　セキュリティ対策方針根拠

＜本項では、前提条件：A.***と脅威：T.***に対する対策方針：O.***と環境：OE.***の寄与を証明することになる。また、IT セキュリティ要件が定められた上では、その各セキュリティ要件と各セキュリティ対策方針との間の関係を詳述し、セキュリテ

ィ対策方針が確かに要件によって達成されていることを証明することになる。

前提条件・脅威と対策方針・「環境の対策方針」の間の関係については、例えば下表のような対照表を構成し、縦横の交叉する場所に証明（あるいは証明を記述した節番号）を書くことになる。以下、項番は例示のため仮想のものである。＞

	A.EQUIPMENT	A.SOFTWARE	A.REPLACE	A.LOCATION	A.REVIEW
OE.LECTURE					4.3.3.7.a
OE.BIOKEY				4.3.3.7.b	

「前提」とそれを充足する「環境のセキュリティ対策」の組の関係を記述する項番などを記入する。

前提条件に対する充足表

4.3.3.7.a　A.REVIEW に対する充足

CHKBOX の機能を実装することで、正当な利用者が正当な業務の遂行の過程でデータの入力確定を行う前に確認をおこなったことが証明される。

4.3.3.7.b　A.LOCATION に対する充足

OE.BIOKEY により非権限者は TOE 設置室に入ることは出来ないことが証明される。

・	T.SPOOF	T. MISSTEP	T.ACCOUNT
O.LOGIN			4.3.3.7.d
			4.3.3.7.d
O.DOUBLECHK		4.3.3.7.c	
O.CHKBOX		4.3.3.7.c	
O.AUTHENT			4.3.3.7.d
O.UPDATE			4.3.3.7.d

「脅威」に対抗するすべての「対策方針」の組と根拠を記述する項番などを記入する。

脅威に対する対抗表

4.3.3.7.c　T.MISSTEP

- O.DOUBLECHK により重要情報については 2 度入力装置により過失の虚偽入力を避けることができる。
- O.CHKBOX によりチェックボックスにチェックを入れる都度、データの確認を行うことで過失の虚偽入力を避けることができる。

（本例では、一つの識別子で複数列挙した脅威を示しているが、対策と対抗の関係を明らかにするために、本来はすべて別識別子にする。たとえば、T.MISSTEP.1、T.MISSTEP.2、等）

4.3.3.7.d　T.ACCOUNT

- O.LOGIN により正当な権限を持った人間以外はログインできない。

・ O.ROLE により正当な役割を持った人間以外は保護資産にアクセスできない
・ O.AUTHENT により処理結果には作成者の署名が添付される
・ O.UPDATE により更新データにたいしては、常に更新前の状態が参照できることから作成者・変更者の履歴を初期生成の段階からすべて確認することができる。

以上の 4 対策方針の実装により、保護資産の作成（変更）責任者が不明になることはないことが証明された。

４．３．３．７．２　セキュリティ要件根拠

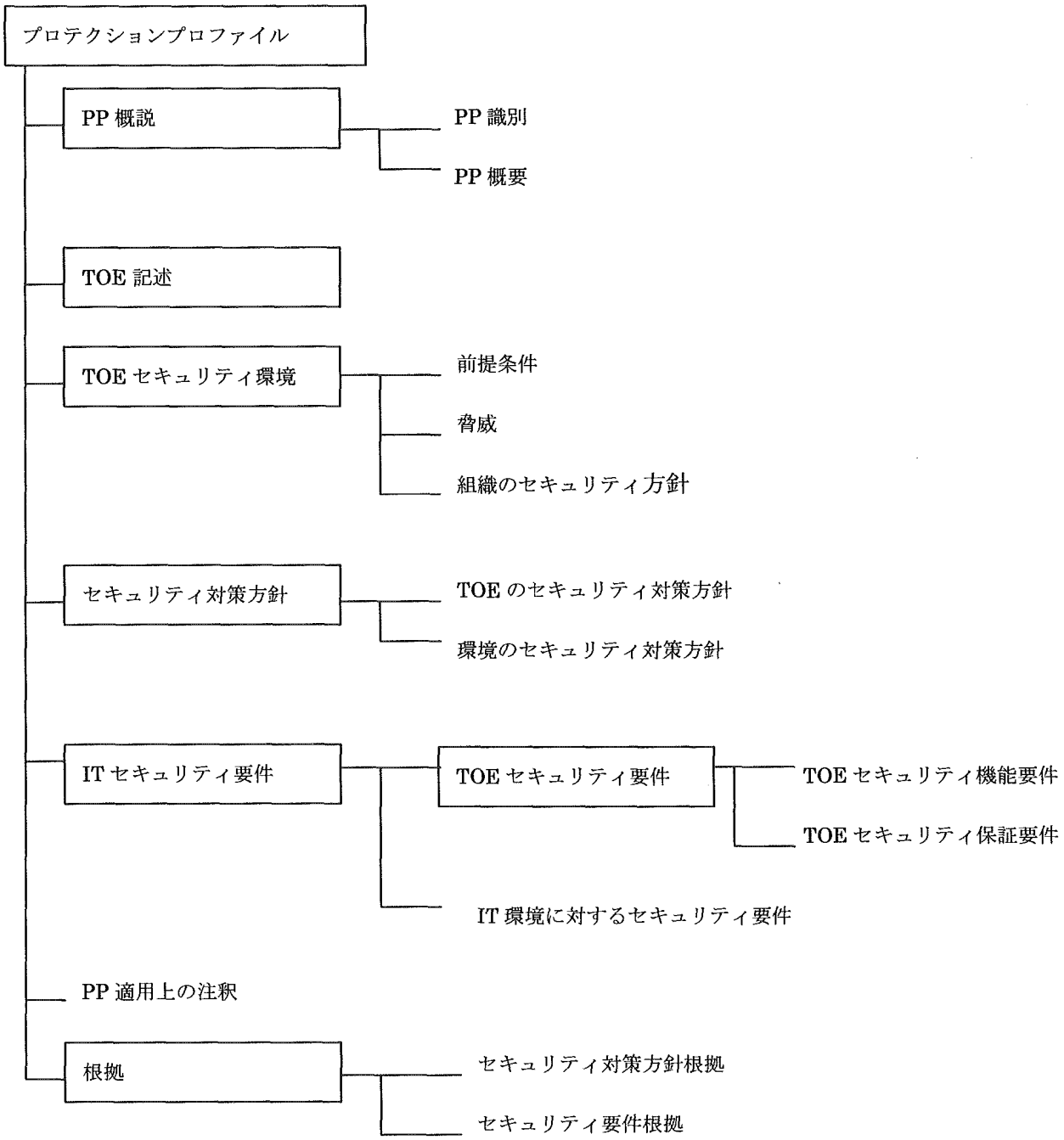
＜本節では、セキュリティ対策方針をどのようなセキュリティ機能要件で実現するかを記述することになる。＞

（本文略）

4．4　プロテクションプロファイルとセキュリティターゲット（資料）

4．4．1　プロテクションプロファイル（PP）

PP の構成は、「情報技術セキュリティ評価のためのコモンクライテリア」パート１付属書Ｂに記載されている。構成は以下の通りである。



PPは、TOEのカテゴリーに属する実装に依存しないITセキュリティ要件のセットを定義するものであり、そのようなTOEは、ITセキュリティに対する消費者ニーズを満たすことを目的とすることから、消費者はPPの作成または参照を行うことにより、特定のTOEを参照せずにITセキュリティのニーズを表現することができる、とされている。

4．4．1．1　内容と提示

PPは、当該付属書に記述されている内容要件に従っていなければならない、とされており、上記形式をアウトラインとして構成されていることが要請されている。

4．4．1．2　PP概説

PP概説は、PP登録を行うのに必要な、PP識別（PPを識別、カタログ化、登録、及び相互参照を行うために必要なラベル情報及び記述的情報からなる）とPP概要（PPについて叙述的形式で要約したものであり、PPが関心の対象となるかどうかをPPの潜在的利用者が判断するに十分な詳細度をもったもの）からなる。

4．4．1．3　TOE記述

TOE記述はTOEについてそのセキュリティ要件の理解を助けるものとして記述され、またTOEの製品種別および一般的IT機能についても示すこととされている。

TOE記述では、評価の範囲を規定する、とある。また、PPは実装については言及しないので、記述するTOE機能は想定でよい。さらに、PPのこの部分に、TOEの適用範囲を記述することが出来るとある。

4．4．1．4　TOEセキュリティ環境

ここでは、TOEが意図する使用環境セキュリティの側面、および期待される使用方法を記述するものとされており、記述には、前提条件、脅威、組織のセキュリティ方針を含めることになっている。

（ア）　前提条件は、TOEが使用される（あるいは意図される）環境についてのセキュリティの側面を記述し、その記述の中には、使用目的に関する情報と使用環境の情報を含める。

（イ）　脅威は、TOEまたはその環境において固有の保護を必要とする資産に対する脅威をすべて含むものとされている。資産に対するすべての脅威とは、その環境で直面するすべての脅威、ということではなく、TOEのセキュアな運用に関連するもののみとしたときの「すべて」である。脅威は、脅威エージェント（技能、利用可能資源、動機をもって記述）、攻撃（攻撃方法、つけこまれる脆弱性、機会をもって記述）、および攻撃対象の資産の観点から記述する。組織のセキュリティ方針および前提条件のみからセキュリティ対策方針を導き出す場合は脅

威の記述は省略できる。

（ウ） 組織のセキュリティ方針では、TOE が従わなければならない組織のセキュリティ方針の記述または規則を識別し、必要なら説明を加えることになっている。

TOE が物理的に分離している場合は、その個別領域ごとに TOE 環境のセキュリティ環境を考察することとされている。

4．4．1．5　セキュリティ対策方針

TOE およびその環境に対するセキュリティ対策方針を定義しなければならない。セキュリティ対策方針では、識別されたセキュリティ環境の側面にすべて対処したものでなければならない。セキュリティ対策方針は、記述された意図を反映したものでなければならず、また識別されたすべての脅威に対抗し、識別されたすべての組織のセキュリティ方針および前提条件をカバーするのに適したものでなければならない。

（ア） TOE のセキュリティ対策方針では、TOE が対抗すべき識別された脅威、及び（または）TOE が満たすべき組織のセキュリティ方針の側面にまでさかのぼれなければならない、とされている。

（イ） 環境のセキュリティ対策方針では、TOE が完全に対抗できない識別された脅威、及び（または）TOE が完全には満たしていない組織のセキュリティ方針または前提条件の側面にまでさかのぼれなければならない、とされている。

4．4．1．6　IT セキュリティ要件

ここでは、TOE またはその環境が満たしていなければならない詳細な IT セキュリティ要件を定義する。記述は、TOE セキュリティ要件（TOE セキュリティ機能要件と TOE セキュリティ保証要件から構成される）、および IT 環境に対するセキュリティ要件の２要件から構成される。また、その表現が従うべき一般条件が規定されている。

（ア） TOE セキュリティ機能要件の記述はパート２から該当する機能コンポーネントを抜き出して TOE に対する機能要件を定義する。

（イ） TOE セキュリティ保証要件の記述はパート３の保証コンポーネントにて用意された EAL のうちから１つを選んで記述する。

（ウ） IT 環境に対するセキュリティ要件は TOE の IT 環境が満たすべき IT セキュリティ要件を識別しなければならない。

4．4．1．7　適用上の注釈

この部分は任意選択部分である。TOE の構築、評価、または使用に関連する（有用であると考えられる）追加の補足情報を記述する。

４．４．１．８　根拠

ここではPP評価に用いる証拠を提示する。根拠は、PPが完全で理路整然とした要求のセットであることと、適合したTOEがセキュリティ環境において有効なITセキュリティ対抗策のセットを提供することの主張の裏づけとなる。根拠には、セキュリティ対策方針根拠とセキュリティ要件根拠からなる。

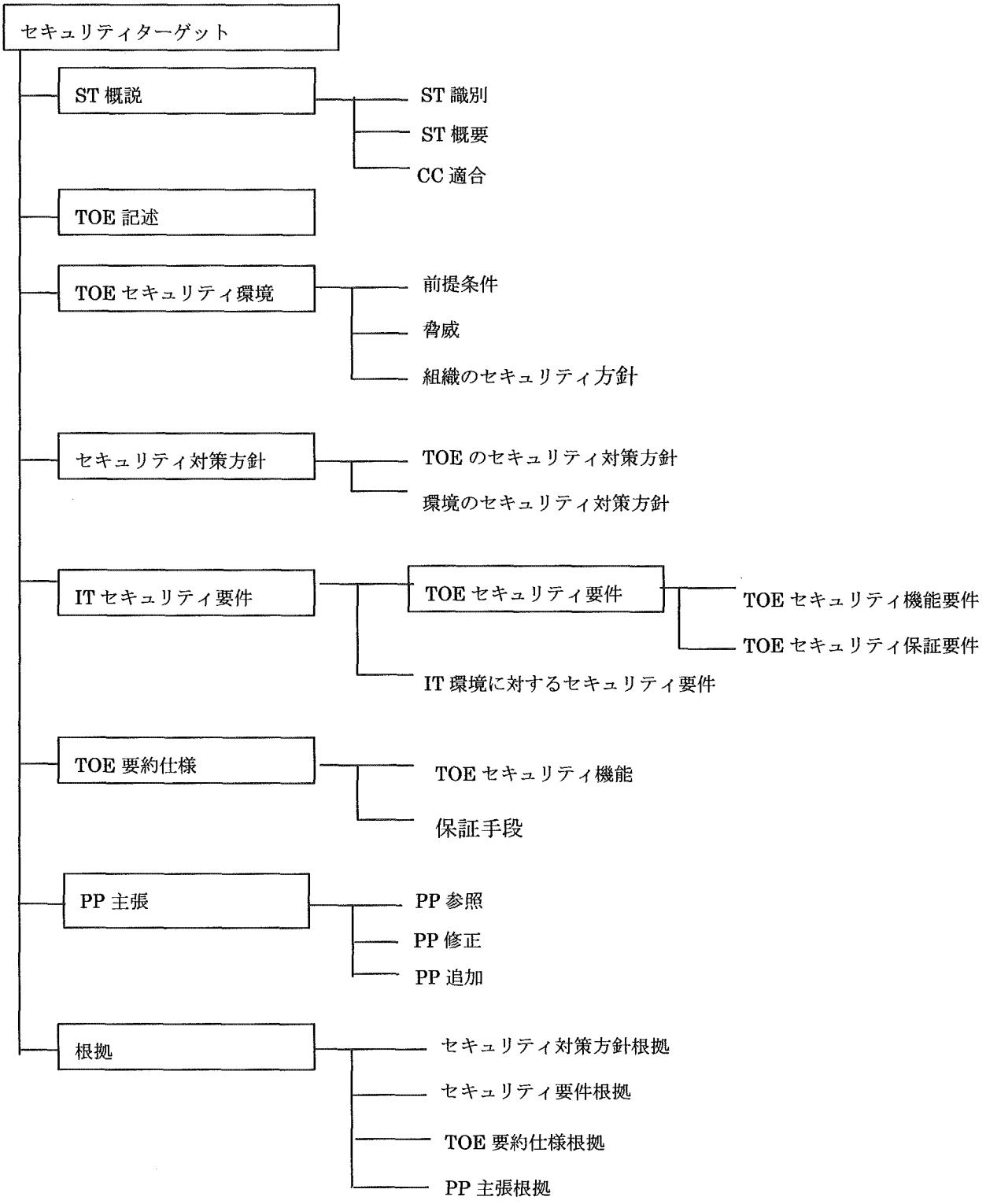
（ア）　セキュリティ対策方針根拠では、記述されたセキュリティ対策方針がTOEセキュリティ環境において識別されたすべての側面にまでたどれることができ、かつそれらをカバーするのに適していることを実証する。

（イ）　セキュリティ要件根拠では、セキュリティ要件（TOE及び環境）のセットがセキュリティ対策方針を満たすのに適し、かつセキュリティ対策方針にまでたどれることを実証しなければならない。

内容・量が膨大になる可能性がある根拠を裏づけることになる資料は別々に分割することができる。

4．4．2　セキュリティターゲット（ST）

STは、識別されたTOEのITセキュリティ要件を記載するものであり、記述された要件を満たすためにそのTOEが提供する機能及び保証のセキュリティ手段を明記するものである、とされている。構成は以下の通りである。



4．4．2．1　内容と提示

STは、当該付属書に記述されている内容要件に従っていなければならない、とされており、上記形式をアウトラインとして構成されていることが要請されている。

4．4．2．2　ST概説

ST概説は、ST識別（STおよびその対象となるTOEの管理及び識別に必要なラベル情報及び記述的情報からなる）、ST概要（STについて叙述的形式で要約したものであり、TOEが関心の対象となるかどうかをTOEの潜在的利用者が判断するに十分な詳細度をもったもの）、およびCC適合（TOEのCC適合についてあらゆる評価可能な主張を記述）からなる。

4．4．2．3　TOE記述

TOEについてそのセキュリティ要件の理解を助けるものとして記述される。また製品またはシステムの種別についても示す。TOEの範囲および境界は、物理面（ハードウェア、及び（または）ソフトウェアコンポーネント（モジュール）と論理面（TOEが提供するIT及びセキュリティ機能）の両方について一般的な表現で記述するものとされている。TOE記述では、評価の範囲を規定する、とある。さらに、STのこの部分に、TOEの適用範囲を記述することが出来るとある。

4．4．2．4　TOEセキュリティ環境

ここでは、TOEが意図する使用環境セキュリティの側面、および期待される使用方法を記述するものとされており、記述には、前提条件、脅威、組織のセキュリティ方針を含めることになっている。

（ア）　提条件は、TOEが使用される（あるいは意図される）環境についてのセキュリティの側面を記述し、その記述の中には、使用目的に関する情報と使用環境の情報を含める。

（イ）　脅威は、TOEまたはその環境において固有の保護を必要とする資産に対する脅威をすべて含むものとされている。資産に対するすべての脅威とは、その環境で直面するすべての脅威、ということではなく、TOEのセキュアな運用に関連するもののみとしたときの「すべて」である。脅威は、脅威エージェント（技能、利用可能資源、動機をもって記述）、攻撃（攻撃方法、つけこまれる脆弱性、機会をもって記述）、および攻撃対象の資産の観点から記述する。組織のセキュリティ方針および前提条件のみからセキュリティ対策方針を導き出す場合は脅威の記述は省略できる。

（ウ）　組織のセキュリティ方針では、TOEが従わなければならない組織のセキュリティ方針の記述または規則を識別し、必要なら説明を加えることになっている。

TOEが物理的に分離している場合は、その個別領域ごとにTOE環境のセキュリティ環

境を考察することとされている。

４．４．２．５　セキュリティ対策方針

TOE およびその環境に対するセキュリティ対策方針を定義しなければならない。セキュリティ対策方針では、識別されたセキュリティ環境の側面にすべて対処したものでなければならない。セキュリティ対策方針は、記述された意図を反映したものでなければならず、また識別されたすべての脅威に対抗し、識別されたすべての組織のセキュリティ方針および前提条件をカバーするのに適したものでなければならない。

（ア）　OE のセキュリティ対策方針では、TOE が対抗すべき識別された脅威、及び（または）TOE が満たすべき組織のセキュリティ方針の側面にまでさかのぼれなければならない、とされている。

（イ）　環境のセキュリティ対策方針では、TOE が完全に対抗できない識別された脅威、及び（または）TOE が完全には満たしていない組織のセキュリティ方針または前提条件の側面にまでさかのぼれなければならない、とされている。

４．４．２．６　IT セキュリティ要件

ここでは、TOE またはその環境が満たしていなければならない詳細な IT セキュリティ要件を定義する。記述は、TOE セキュリティ要件（TOE セキュリティ機能要件と TOE セキュリティ保証要件から構成される）、および IT 環境に対するセキュリティ要件の２要件から構成される。また、その表現が従うべき一般条件が規定されている。

（ア）　OE セキュリティ機能要件の記述はパート２から該当する機能コンポーネントを抜き出して TOE に対する機能要件を定義する。

（イ）　OE セキュリティ保証要件の記述はパート３の保証コンポーネントにて用意された EAL のうちから１つを選んで記述する。

（ウ）　IT 環境に対するセキュリティ要件は TOE の IT 環境が満たすべき IT セキュリティ要件を識別しなければならない。

４．４．２．７　TOE 要約仕様

ここでは、TOE に対するセキュリティ要件を具体的に定義する。すなわち、TOE セキュリティ要件を満たす TOE のセキュリティ機能、及び保証手段を記述することになる。

（ア）　TOE セキュリティ機能では、IT セキュリティ機能をカバーしていなければならず、その機能が TOE セキュリティ機能要件をどのように満たしているかを明示していなければならない。機能と要件の双方向の対応関係を記述することで、どの機能がどの要件を満たしているか、及びすべての要件は満たされているかが明らかになる。各セキュリティ要件は、少なくとも一つの TOE セキュリティ要件に寄与していなければならない。

（イ） 保証手段では、記述された保証要件を満たしていると主張する TOE の保証手段を明示する。

4．4．2．8 PP 主張

ST は TOE が 1 つ（または複数）の PP の要件に適合していることを任意に主張することができるが、その主張を実証するのに必要な説明、根拠、及び裏づけとなるその他の主張を、PP 主張に記述することになる。

4．4．2．9 根拠

ここでは ST 評価に用いる証拠を提示する。根拠は、ST が完全で理路整然とした要求のセットであることと、適合した TOE がセキュリティ環境において有効な IT セキュリティ対抗策のセットを提供すること、ならびに TOE 要約仕様がその要件に対処したものであることの主張の裏づけになる。根拠は、セキュリティ対策方針根拠、セキュリティ要件根拠、TOE 要約仕様根拠と PP 主張根拠からなる。

（ア） セキュリティ対策方針根拠では、記述されたセキュリティ対策方針が TOE セキュリティ環境において識別されたすべての側面にまでたどれることができ、かつそれらをカバーするのに適していることを実証する。

（イ） セキュリティ要件根拠では、セキュリティ要件（TOE 及び環境）のセットがセキュリティ対策方針を満たすのに適し、かつセキュリティ対策方針にまでたどれることを実証しなければならない。

（ウ） TOE 要約仕様根拠では、TOE のセキュリティ機能および保証手段が TOE セキュリティ要件を満たしていることを示す。

（エ） PP 主張根拠では、ST と適合を主張する PP との間のセキュリティ対策方針及び要件の相違をすべて説明しなければならない。

内容・量が膨大になる可能性がある根拠を裏づけることになる資料は別々に分割することができる。