

参考資料

ISO/IEC TR 15446

WD N3374

PP/ST作成のためのガイド

バージョン 0.93

2002-10-01

平成 16 年 1 月仮訳
独立行政法人 情報処理推進機構
セキュリティセンター

IPAまえがき

本書の目的

本書は、ISO/IEC TR 15446 「Guide for the Production of PPs and STs, Version0.93 2002-10-20 (Working Draft)」を日本語訳(付録の一部を除く)したもので、独立行政法人 情報処理推進機構セキュリティセンターにてPP/ST作成の注意点、評価方法等の調査を行うための補助資料として作成したものです。

使用上の注意

本書の原書のステータスは、“ For study and comment by ISO/IEC JTC 1/SC 27 ” として ISO/IEC SC27 WG3において審議中のものです。2003年11月現在、既にN3816の更新版が発行されている。

N3816は、ISO文書への書式合わせが主な変更であるが、本書において技術的変更点については、[【ISO/IEC JTC 1/SC 27 N3816改訂情報】](#)と明示し翻訳を追加している。N3816に関連するすべての変更は、青色の斜体文字で示される：追加されたテキストは下線が引かれ、削除されたテキストは抹消線が引かれている。

また、本書は、用語及び体裁の統一、記述内容などに不備がある可能性がある。疑問点については 原書または参考資料で確認していただきたい。本書の改変、及び他への転載は禁止する。

原書

ISO/IEC TR 15446: WD N3374

TITLE: Guide for the Production of PPs and STs, Version 0.93

SOURCE: Project editor (Murray G. Donaldson)

DATE: 2002-10-01

PROJECT: ISO/IEC JTC 1.27.22

STATUS: For study and comment by ISO/IEC JTC 1/SC 27

参考資料

ISO/IEC TR 15446: DTR N3816

DOC. TYPE: Text for DTR

TITLE: Text for ISO/IEC DTR 15446 - Information technology - Security techniques.
Guide on the production of protection profiles and security targets

SOURCE: Project Editor (M. Nash)

DATE: 2003-11-10

PROJECT: 1.27.22 (TR 15446)

STATUS: In accordance with document SC 27 N3815 "Editor's report on DTR ballot text, ISO/IEC 15446" and based on Warsaw resolution 7 (reference document SC 27 N3411) of the 14th SC 27 Plenary meeting, October 2002, this document has been sent to the JTC 1 Secretariat for a 3-month letter ballot. It is being circulated within SC 27 for information.

目次

1 序説	1
1.1 目的及び意図される読者	1
1.2 本ガイドの目的及び範囲	1
1.3 ガイドの概要	1
1.4 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 - 序説	3
1.5 用語集	5
1.6 参照文献	5
2 PPとSTの概要	8
2.1 序説	8
2.2 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の内容	8
2.3 PPとSTの関係	10
2.4 PPまたはSTの対象読者への狙い	11
2.5 PP及びST開発プロセス	12
2.6 PPファミリ	13
3 PP及びSTの記述的な部分	14
3.1 序説	14
3.2 PPまたはSTの記述的な部分	14
4 TOEセキュリティ環境	17
4.1 序説	17
4.2 前提条件の識別と特定のしかた	18
4.3 脅威の識別と特定のしかた	19
4.4 いかにより組織のセキュリティ方針を識別し特定するか	25
5 セキュリティ対策方針	27
5.1 序説	27
5.2 TOEのセキュリティ対策方針の特定のしかた	28
5.3 環境のセキュリティ対策方針の特定のしかた	30
6 セキュリティ要件	34
6.1 序説	34
6.2 PPまたはSTにおいてセキュリティ機能要件の特定のしかた	37
6.3 PPまたはSTにおける保証要件の特定のしかた	50
6.4 環境のセキュリティ要件	53
7 TOE要約仕様	55

7.1 序説	55
7.2 ITセキュリティ機能の特定のみかた	56
7.3 セキュリティメカニズムの特定のみかた	57
7.4 保証手段の特定のみかた	57
8 PP及びST根拠.....	61
8.1 序説	61
8.2 PPまたはSTにセキュリティ対策方針の根拠の提示のみかた	62
8.3 PPまたはSTにセキュリティ要件の根拠の提示のみかた	64
9 コンポジット及びコンポーネントTOEのPPとST.....	73
9.1 序説	73
9.2 コンポジットTOE	74
9.3 コンポーネントTOE.....	77
10 機能及び保証パッケージ.....	80
10.1 背景	80
10.2 機能パッケージの特定のみかた	80
10.3 保証パッケージの特定のみかた	82
附属書A ガイダンスチェックリスト	84
A.1 PP/ST概説	84
A.2 TOE記述.....	84
A.3 TOEセキュリティ環境のステートメントの定義.....	84
A.4 セキュリティ対策方針の定義	85
A.5 ITセキュリティ要件の指定	86
A.6 TOE要約仕様の作成.....	87
A.7 PP根拠の構成.....	88
A.8 ST根拠の構成.....	89
附属書B 一般的な例	90
B.1 脅威の例.....	91
B.2 組織のセキュリティ方針の例	92
B.3 前提条件の例	93
B.4 TOEのセキュリティ対策方針の例	94
B.5 環境のセキュリティ対策方針の例	95
B.6 セキュリティ対策方針から脅威へのマッピングの例.....	96
B.7 セキュリティ機能要件の例.....	104
附属書C 暗号機能性の特定	111
C.1 序説.....	111

C.2 暗号の概説.....	114
C.3 セキュリティ要件の抽出.....	116
C.4 ITセキュリティ要件の表現	122
C.5 保証要件適用のガイダンス.....	141
附属書D 作業例：ファイアウォールのPPとST	143
D.1 PP/ST概説.....	143
D.2 TOE記述	143
D.3 セキュリティ環境.....	143
D.4 セキュリティ対策方針.....	145
D.5 ITセキュリティ要件.....	146
D.6 TOE要約仕様.....	148
D.7 PP根拠	150
D.8 ST根拠	152
附属書E 作業例：データベースPP	153
E.1 TOEセキュリティ環境.....	153
E.2 セキュリティ対策方針.....	155
E.3 ITセキュリティ要件.....	156
E.4 PP根拠.....	158
附属書F 作業例：信頼できる第三者機関のPP	161
F.1 TOEセキュリティ環境.....	162
F.2 セキュリティ対策方針.....	164
F.3 ITセキュリティ要件.....	165
F.4 PP根拠	168

1 序説

1.1 目的及び意図される読者

本文書は、ISO/IEC 15408(「コモンクライテリア」)に準拠して作成されることを意図されるプロテクションプロファイル(PP)及びセキュリティターゲット(ST)を作成することに関するガイダンスを提供するものである。 (1)

本文書はPP及びSTの開発に携る者を主な対象としている。しかしながら、PP及びSTの評価者、PP及びSTの評価を監視する責任をもつ者に対してもまた有用であるように思われる。PP/STの作成者がどのガイダンスを使用しているか、PP及びSTのどの部分が最も重要であるかを理解することを望むST及びPPの消費者及び利用者に対してもまた、興味の対象であろう。 (2)

本ガイドの読者は、ISO/IEC 15408[15408-1]のパート1、とりわけPP及びSTについて記述している附属書B及びCについて精通していると仮定される。PP及びSTの作成者は(もちろん)本ガイドで述べられているように、[15408-2] 1.3副項の機能要件のパラダイムのような導入的な題材を含むISO/IEC 15408の他の部分にも精通する必要が生じるだろう。 (3)

1.2 本ガイドの目的及び範囲

本文書は、ガイダンスのためだけに提供される参考的ISOテクニカルレポートである。本ガイドはPP及びSTの評価のために、内容や構造に対して権威のあるものとして引用すべきではない。本ガイドは、ISO/IEC 15408に十分一貫性をもつことを意図されている；ただし、本ガイドとISO/IEC 15408の間にはいかなる矛盾があった場合も、後者の方が優先される。 (4)

本ガイドは、PP登録のタスクやPP中の知的所有権(例えば特許)の保護の扱いのような関連のタスクについては取り扱わない。PP登録手続きの定義を提案している[WD-15292]を参照。 (5)

1.3 ガイドの概要

本ガイドは、PPまたはSTの個々のパート、及びそれらがどのように相互に関連するかに関わる詳細なガイダンスを提供する。本文書に含まれるガイダンスのキーポイントの概要が、チェックリストの形で提示されているので、興味ある読者は附属書Aを参考にするべきである。 (6)

PP及びSTの作成者へのガイダンスが本ガイドの本文(すなわち、個々の章)に提示され、その要約が上記のように附属書Aに提示されるように、本ガイドは構成されている。それ以降の附属書で、本ガイドの適用を説明するための様々な例を提示する。 (7)

2章はPP及びSTの概要を提供するものであり、目次の例を提示し、PPまたはSTについて、個々のパートの期待される内容及び対象読者を明らかにする。また、この章はPPとSTの関係、及び

PP/ST開発過程に関する問題について論じている。3章はより深くPP及びSTの記述パートについて吟味し、PP及びSTの概説とTOE記述(これは、どちらかといえば消費者や利用者を対象としている)と同様にPPアプリケーションノート(これはどちらかといえばST作成者とTOE開発者を対象としている)をカバーしている。 (8)

本ガイドの次の5つの章はISO/IEC 15408([15408-1] 図B.1及びC.1)にアウトラインが示されている、PP及びSTの内容の順番を追ったものである。 (9)

4章はPPまたはSTのTOEセキュリティ環境の定義についてのガイダンスを与え、TOEで満たされるべき「セキュリティ関連事項(security concerns)」の様々な局面をカバーする。そして5章は、PPまたはSTのセキュリティ対策方針の特定で与えられるような、TOEとその環境によるセキュリティ関連事項の別の局面に対する意図された対応の定義についてのガイダンスを提供する。そのため、この両方の章はPP/ST作成者だけでなくPPとSTの消費者及び利用者に対しても、一般的な興味の対象となる。 (10)

6章はPPのITセキュリティ要件を選択及び特定することについてのガイダンスを提供する。ISO/IEC 15408で機能及び保証コンポーネントがどのように定義されているか、これと同様にISO/IEC 15408定義外のコンポーネントも、ITセキュリティ要件の明確な定義を提供するにすべきであるといった、いくぶん詳細な記述もこの章に含まれる。7章はSTに関連する特有のガイダンスを提供し、ITセキュリティ要件の特定(そして、これがPPの場合とどう異なるか)及びTOE要約仕様についてカバーする。このため、これらの2つの章は主にPP/STの作成者と評価者の興味の対象になるだろう。 (11)

[【ISO/IEC JTC 1/SC 27 N3816改訂情報】：段落11は「12 PP主張」の追加に伴い以下に示すとおり修正される。](#)

[10章^{訳注}はPPまたはSTのITセキュリティ要件を選択及び特定することについてのガイダンスを提供する。ISO/IEC 15408で機能及び保証コンポーネントがどのように定義されているか、これと同様にISO/IEC 15408定義外のコンポーネントも、ITセキュリティ要件の明確な定義を提供するにすべきであるといった、いくぶん詳細な記述もこの章に含まれる。11章^{訳注}と12章はSTに関連する特有のガイダンスを提供し、TOE要約仕様とPP準拠の主張それぞれについてカバーする。これらの3つの章は主にPP/STの作成者と評価者の興味の対象になるだろう。](#)

[訳注：10章は本書の6章に該当し、11章は本書の7章に該当する。](#)

8章はPP及びSTの根拠セクションの構成と表現についてのガイダンスを提供する。 (12)

9章はコンポジット(複合)TOE、すなわち各々がそれ自身のPPまたはSTを持つ2つ以上のコンポーネントTOEにより構成されるTOEのPP及びSTに特有の問題を吟味する。 (13)

10章は別のSTやPPで利用できるように定義される、機能及び保証パッケージの作成についてのガイダンスを提供する。パッケージはPP及びSTの費用効果の高い作成を促進し容易にすることを意図された潜在的に非常に有用なツールであることが理解できる。 (14)

前述のように、附属書Aはチェックリストの形でガイダンスを要約するものである。 (15)

附属書Bは、脅威、組織のセキュリティ方針、前提条件、セキュリティ対策方針の例を提示し、そして共通的なまたは一般的なセキュリティ機能要件を特定するために、[15408-2]機能コンポーネントの適切なものを識別している。これらの例は広範囲なものであることを意図されているが、決して網羅的であることを主張するものではない。 (16)

附属書Cは特に暗号機能性を実装するTOEのPP及びSTに関連するガイダンスを提供する。このようなガイダンスは広い範囲のそのようなTOEをカバーするために含まれてきたもので、そして暗号機能性の仕様に関する特殊な問題を扱っている。(本ガイドの将来のバージョンはその他のタイプのTOEのための類似した附属書を含むだろう。) (17)

附属書DからFは異なるタイプのTOEについての作業例を使用して、様々な状況でこのガイダンスの適用を説明する。各々の例は(本ガイドとは関係なく)開発された実際のPPとSTに基づいている。附属書DではファイアウォールのPP及びSTの作成へのガイダンスの適用を見る。附属書Eはデータベース管理システムのPPについて論じ、ここではIT環境への依存の問題が非常に重要であることを見ることができる。最後に、附属書Fは信頼できる第三者機関(TTP: Trusted Third Party)のPPの開発を取り巻く問題について吟味する。 (18)

1.4 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 - 序説

1.4.1 PPの目的

PPの目的はシステムや製品の集まり - 評価対象(TOE)として認識される - のセキュリティの問題を厳密に述べ、そのセキュリティの問題に対応するためのセキュリティ要件を、その要件がどのように実装されるかに言及することなく特定することである。(この理由のために、PPは実装から独立したセキュリティの記述を提供すると言われる。) PPは以下のように、いくつかの関連する種類のセキュリティの情報を含んでいる： (19)

- a) PP概説とTOE記述： 情報技術の利用者にとって適切な用語で、対応されるべき要求またはセキュリティの問題のステートメントを識別する。
- b) TOEセキュリティ環境の記述： 対応されるべき脅威と特定の前提条件の見地から満たされるべき組織のセキュリティ方針が導き出され、意図される使用環境に関する要求のステートメントを詳細化する。
- c) セキュリティ対策方針： どのように、またどの範囲でセキュリティ関連事項が満たされるべきかについての情報を与え、TOEセキュリティ環境の記述に基づくTOE評価の範囲を決める。セキュリティ対策方針の目的は、リスクを軽減し、PPスポンサーのセキュリティ方針をサポートすることである。
- d) セキュリティ機能要件及び保証要件： TOE及びIT環境のセキュリティ対策方

針の範囲で、要求のステートメントから引き起こされるセキュリティ問題に対応する。セキュリティ機能要件は、セキュリティ対策方針を満足するために、何がTOEによってなされなければならないか、そして何がそのIT環境によってなされなければならないかを説明する。保証要件は、TOE及びIT環境のセキュリティ機能に見込まれる確信の度合いを説明する。

- e) 根拠： セキュリティの機能要件と保証要件が、要求のステートメントを満たすために十分であることを実証する。セキュリティ対策方針は、TOEセキュリティ環境の記述で発見されるセキュリティ関連事項について何がなされなければならないかを説明しなければならない。セキュリティの機能要件及び保証要件はセキュリティ対策方針を満たしていなければならない。

1.4.2 STの目的

特定の製品やシステムでセキュリティ要件がどのように実現されるかを詳述した追加的な実装特有の情報を除けば、STはPPに類似している。したがってSTはPPには見られない次のような追加の情報が含まれる。 (20)

- a) TOE特有のセキュリティの機能と保証手段を提示するTOE要約仕様。
- b) STがどのPPへの適合を主張するかを説明する、オプションのPP主張部(該当する場合)。
- c) 最後に、TOE要約仕様が実装から独立した要件を満足すること保証すること、及びどのPP適合の主張も満足されることを確認する、追加の証拠を含む、根拠。

1.4.3 PPとSTの使用法

1つまたはそれ以上の製品が準拠を主張する、または組織の中で特定の目的のために使用されるシステムが準拠しなければならない、セキュリティ要件の「標準」セットを定義するために、PPを使用することができる。(用語 製品とシステムの定義は[15408-1]2.3副項を、同様に両者の区別についての一般的な解説は[15408-1] 4.1.2副項を参照)。PPは特定のタイプのTOE(例：オペレーティングシステム、データベース管理システム、スマートカード、ファイアウォールなど)に適用してもよいし、またはコンポジット(複合)TOE(システムまたは製品)の形でグループ化された製品のセットに適用できる。 (21)

製品ベンダは、彼らの製品がどのようにセキュリティ関連事項に対応しているかを実証するSTを作成することで、PPに定義されているセキュリティ関連事項に応じる。しかしながら、STがPPへの適合を主張する義務はない。製品ベンダはセキュリティ関連事項のセットについて、市場に対して責任を負い、彼らの製品によって主張されるセキュリティ機能が、どのようにそれらの関連事項を満たすかを特定するSTを作成することができ、そしてこれは製品評価の際の基準になる。 (22)

PPはまた、特定のITシステムで満足されるべきセキュリティ要件を定義することができる。この

場合、STはPPに対応して提案され、例えば、STはそのPPを参照するRFP(提案要求)に対応して書くことができる。このようにPPとSTはシステムの開発を管理することに責任をもつ組織、システムの調達者、及びシステムを作成することに責任を持つ組織(以下、開発者として参照される)との間のコミュニケーション手段として使用することもできる。PPとSTの内容は主要関係者によって交渉される。実際のシステムをST(PPに適合することが確認されている)に対して評価することは、受け入れプロセスの一部になりうる。(もちろん、PPを参照しないRFPへの対応の一部として、STが書かれてもよいことは、認識されるべきである。) (23)

1.5 用語集

本ガイドで使用される述語は別途指定されない限りは[15408-1]の2.3副項で定義されている。 (24)

以下の略語は[15408-1]の2.1副項にリストされる略語に追加して本ガイドで使用されるものである。 (25)

DBMS	データベース管理システム(Database Management System)
OSP	組織のセキュリティ方針(Organisational Security Policy)
RFP	提案要求(Request for Proposal)
SAR	セキュリティ保証要件(Security Assurance Requirement)
SFR	セキュリティ機能要件(Security Functional Requirement)
TSS	TOE要約仕様(TOE Summary Specification)
TTP	信頼できる第三者機関(Trusted Third Party)

1.6 参照文献

- [15408-1] Evaluation Criteria for IT Security
Part 1: Introduction and general model
ISO/IEC 15408-1: 1999(E), December 1998
- [15408-2] Evaluation Criteria for IT Security
Part 2: Security functional requirements
ISO/IEC 15408-2: 1999(E), December 1998
- [15408-3] Evaluation Criteria for IT Security
Part 3: Security assurance requirements
ISO/IEC 15408-3: 1999(E), December 1998

[13335] Guidelines for the Management of IT Security (GMITS)
Part 1: Concepts and models of IT Security
Part 2: Managing and planning IT Security
Part 3: Techniques for the management of IT Security
Part 4: Selection of Safeguards
Part 5: Safeguards for external connection

[ISO-2382] Information Technology - Vocabulary
Part 8: Security (Revision of ISO 2382-9:1986)
ISO/IEC DIS 2382-8, Edition 2.

[WD-15292] Information Technology - Security techniques -
Protection Profile registration procedures
ISO/IEC 15292, 1999-06-11

訳注：ISO/IEC 15292, 2001-12-15が発行されている。

【ISO/IEC JTC 1/SC 27 N3816改訂情報】：参考文献は以下に示すとおり修正される。

Bibliography

[1] ISO/IEC 15292, Protection Profile registration procedures

[2] ISO/IEC 13335, Information technology — Security Techniques — Management of information and communications technology security

[3] ISO/IEC 14516, Information technology — Security Techniques — Guidelines on the use and management of Trusted Third Parties services

[4] ISO/IEC 9798-1, Information technology — Security Techniques — Entity authentication — Part 1: General

[5] ISO/IEC 10118-1, Information technology — Security Techniques — Hash functions — Part 1: General

[6] ISO/IEC 11770-1, Information technology — Security Techniques — Key management — Part 1: Framework

[7] ISO/IEC 13888-1, Information technology — Security Techniques — Non-repudiation — Part 1: General

[8] ISO/IEC 14888-1, Information technology — Security Techniques — Digital signature

with appendix — Part 1: General

[9] ISO/IEC 18031, Information technology — Security Techniques — Random number generation

[10] ISO/IEC 18032, Information technology — Security Techniques — Prime number generation

2 PPとSTの概要

2.1 序説

この章では、PPとST両文書の内容を要約し、PPとSTとの関係を論じながらPPとSTの概要を規定する。また、開発される文書のプロセスも規定する。[15408-1]附属書B及びC参照。 (26)

2.2 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の内容

PPが要求される内容は、[15408-1]附属書B、図B.1、38ページに図示されている。下の表1は、これを内容のリストの例として転載したものである。 (27)

1	PP概説 1.1 識別 1.2 概要
2	TOE記述
3	TOEセキュリティ環境 3.1 前提条件 3.2 脅威 3.3 組織のセキュリティ方針
4	セキュリティ対策方針 4.1 TOEのセキュリティ対策方針 4.2 環境のセキュリティ対策方針
5	ITセキュリティ要件 5.1 TOEセキュリティ機能要件 5.2 TOEセキュリティ保証要件 5.3 IT環境に対するセキュリティ要件
6	PPアプリケーションノート
7	根拠 7.1 セキュリティ対策方針根拠 7.2 セキュリティ要件根拠

表1 – プロテクションプロファイル内容リストの例

STが要求される内容は、[15408-1]附属書C、図C.1、44ページに図示されている。下の表2は、STの内容リストの例として、表1に付加内容を加えたものである。 (28)

1	ST概説 1.3 ISO/IEC 15408適合
6 ^a	TOE要約仕様 6.1 TOEセキュリティ機能 6.2 保証手段
7	PP主張 7.1 PP参照 7.2 PP修整 7.3 PP追加
8	根拠 8.3 TOE要約仕様根拠 8.4 PP主張根拠

表2 - セキュリティターゲットの内容リストの例

a. PPアプリケーションノートはセキュリティターゲットには含まれない。

PPまたはSTの読者は、その他の文章と同様に必要とする内容がPPまたはSTのどこにあるかを簡単に見つけ出せるべきである。 (29)

*概説*は、PPまたはSTとTOE(そのバージョン番号を含む)を識別し、またPPまたはSTの要約を叙述的な形式で提供する。PPの要約は、PPカタログやPP登録に含まれるものとして用いることができる。STでは、例えば評価済み製品のリストに含めるものとして適している。この節については、本ガイドの3章でより詳細に論じる。 (30)

*TOE記述*は、TOE(またはTOE種別)についての全般的な情報を提供し、そのセキュリティ要件と意図される使用方法の理解の助力として役立つ。また、STのTOE記述では、TOEが評価されるべき構成についての定義も含まれていなければならない。この節については、本ガイドの3章でより詳細に論じる。 (31)

*TOEセキュリティ環境*は、TOEが存在する背景の定義を提供し、特にTOEが対応しようとしている「セキュリティ関連事項」を明らかにしている。この記述では、セキュリティ関連事項の範囲を定義するあらゆる前提条件、意図された使用の範囲、保護を必要とする資産(それらの資産の記述とともに)に対する識別された脅威、そしてTOEが従うべきあらゆる組織のセキュリティ方針について詳しく述べている。この節については、本ガイドの4章で詳細に論じる。 (32)

*セキュリティ対策方針*は、TOEによって満たされるべきセキュリティ対策方針及びTOE環境内でITと非IT手段によって満たされるべきセキュリティ対策方針の双方の観点で、セキュリティ事項

に対する意図された対応の簡潔なステートメントを提供している。この節については、本ガイドの5章で詳細に論じる。 (33)

*ITセキュリティ要件*は、TOEにおけるセキュリティ機能要件、セキュリティ保証要件そしてTOEのIT環境のソフトウェア、ファームウェアまたはハードウェアにおけるあらゆるセキュリティ要件を定義する。ITセキュリティ要件は、適切であればパート2 [15408-2]及びパート3 [15408-3]の中の機能コンポーネントと保証コンポーネントを用いて定義される。この節については、本ガイドの6章で詳細に論じる。 (34)

*PPアプリケーションノート*は、PP作成者によって有益と考えられたあらゆる付加的なサポート情報を提供するPPのオプション的な節である。アプリケーションノートは、独立した節として提供される代わりに、PP中のそれぞれ関連する節に分散させてもよいことに注意が必要である。このことは本ガイドの3章でより詳細に論じる。 (35)

*TOE要約仕様*は、特定されたセキュリティ機能要件を満たすためにTOEによって提供されるITセキュリティ機能と、特定されたセキュリティ保証要件を満たすために主張されたあらゆる保証手段とを定義したST中の節である。このことは本ガイドの7章で詳細に論じる。 (36)

*PP主張*は、そのSTが適合を主張するあらゆるPPと、PP目的または要件のあらゆる追加または修整を識別するSTのオプション的な節である。このことは本ガイドの8章で詳細に論じる。 (37)

*根拠*は、PPまたはSTが完全かつ一貫したITセキュリティ要件の集合を特定し、適合TOEは定義されたセキュリティ関連事項に対し効果的に対応するものであり、ITセキュリティ機能及び保証手段はTOEセキュリティ要件を満たすものとして適していることの実証を提供している。根拠は、独立した節として提供される代わりに、PPまたはST中のそれぞれの関連する節に分散させてもよいことに注意が必要である。このことは本ガイドの8章で詳細に論じる。 (38)

また根拠の節は、[15408-1]、B.2.8副項、42ページに述べられているように、独立した文書としてまとめることもできることに注意すること。 (39)

2.3 PPとSTの関係

表1と表2の内容リストの例を比較すると明らかであるように、PPとSTはきわめて共有性が高い。特に*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*の節と、これらの側面に対応している*根拠*の節の部分は共有性が高い。実際、STがまったく追加の機能要件または保証要件を含まないPPへの適合を単に主張した場合、STのこれらの節の内容は、PP中のそれらに相当する節とまったく一致するであろう。そのような場合、STは単にPPの内容を参照し、PPとの違いのみの詳細を提供することが推奨される。 (40)

ST中の次に述べる節は、ST特有の本質が反映されていてPP中では取り上げられない詳細、すなわち定義されたセキュリティ関連事項に対しTOEがどのように解決策をもたらすかについての定

義を規定している：

(41)

- a) ITセキュリティ機能、セキュリティメカニズムまたは技法、保証手段をカバーする *TOE要約仕様*。
- b) 参照されたPPへの準拠のあらゆる主張を詳述し正当化する、オプションである *PP主張*。
- c) ITセキュリティ機能と保証手段がTOEセキュリティ要件を満足することの妥当性を実証するST中の *根拠*のそれらの部分。

2.4 PPまたはSTの対象読者への狙い

PPまたはSTを書くにあたっての重要な努力目標のひとつは、すべての意図した読者が適切に利用できるような説明を織り込んでおくことである。

(42)

- a) 消費者（すなわち調達者や上層部の意思決定者）は、適合したTOEが、セキュリティの点で何を提供するのかという全般的な理解を必要とする。よくできたPPは、このクラスがもっとも大きい読者となるであろう。
- b) 開発者（STの場合は実装者も含む）は、適合したTOEを組み立てるための曖昧さのないセキュリティ要件の定義を必要とする。
- c) TOE利用者（導入者、管理者、保守者を含む）は、要求されるTOEセキュリティ環境についての情報を必要とする。
- d) 評価者は、PPまたはSTの技術上の確実な根拠及び有効性を正当化するような情報を必要とする。

PP及びSTは、それぞれの節をそれぞれの読者が利用できるように設計されており、またそのように書かれるべきである。

(43)

PP/ST概説、*TOE記述*、*TOEセキュリティ環境*の節は、主として消費者向けに書かれるべきである。*セキュリティ対策方針*の節もまた消費者向けに書かれるであろう。しかしながら、TOE開発者もまた*TOEセキュリティ環境*及び*セキュリティ対策方針*の節にある情報に注意する必要があるということをおぼわすはならない。

(44)

PPの*ITセキュリティ要件*の節は、主としてTOE開発者向けに書かれるべきであるが、それらが含む情報はTOE消費者にとっても関心のあるものと思われる。反対に、STの*TOE要約仕様*の節は、主として評価者と消費者に向けて書かれるべきである。もし、これらの節が自己完結していない場合には、他のPPの節や他の文書（例えば、参照している暗号標準）のどれが、提示されたITセキュリティ要件の完全かつ正確な理解に必要なかを明示的に示さなければならない。特に、*TOE要約仕様*が、それ自体の意義が*ITセキュリティ要件*の節に依存している場合、その事実を明示的に指摘しなければならない。

(45)

評価者はPPまたはSTのすべての節に精通している必要がある。しかしながら、*根拠*の節は、PPまたはSTのそれぞれの利用者の関心であると同時に、一般的には評価情報であり、主として評価

者向けである。

(46)

2.5 PP及びST開発プロセス

[15408-1]附属書BとC、及び[15408-3]3から5項に示したPP及びSTに対する要件の説明は、PP及びSTはいつも論理上「トップダウン」のやり方で開発されることを期待されていることを示唆しているかもしれない。例えば、(PPの場合において)は、

(47)

- a) 最初にセキュリティ関連事項が定義される。
- b) 次にそのセキュリティ関連事項に対応するためのセキュリティ対策方針が識別される。
- c) さらにTOEのセキュリティ対策方針を満たすためのITセキュリティ要件が定義される。

このような可能性は除外されるものではないが、反復的なプロセスがより要求されることであろう。例えば、ITセキュリティ要件の定義は、セキュリティ対策方針の定義またはセキュリティ関連事項までも必要とする説明をハイライトするかもしれない。一般に、脅威、組織のセキュリティ方針、セキュリティ対策方針、ITセキュリティ要件間の関係において多くの反復が要求されるであろうし、機能も密接に検査される。PPまたはST根拠を構築しているときなど特にそうである。根拠におけるすべての識別された欠落が満たされたときのみ、PPまたはSTが完全であると見なすことができる。

(48)

PPまたはST開発の反復的なプロセスの間、現在のセキュリティ関連事項の範囲内の新しい情報が明るみになるかもしれない。それは外部環境の変化を反映する文書への変更をもたらすかもしれない。例えば、

(49)

- a) 新たな脅威が識別されるかもしれない。
- b) 組織のセキュリティ方針が変更されるかもしれない。
- c) 経費や時間的制約が、TOEがすべきこととTOE環境に期待すべきこととの責務の境界線の変更を強いるかもしれない。
- d) 意図すべき攻撃能力の変更は、TOEセキュリティ環境に影響を与えるかもしれない。

(例えば、TOEが既に開発されている製品であるような場合) PPまたはST作成者が(たとえ、それらが今のところISO/IEC 15408が要求するやり方に示されていないとしても) TOEが満足するであろうSFRの明確な考えをすでにもっていることもあり得る。そのような場合、セキュリティ関連事項及びセキュリティ対策方針の定義は、そのTOEが提供するセキュリティソリューション

の形の知識によって否応なしに左右されるであろう。PP/ST開発プロセスはこの場合ある程度は「ボトムアップ」となるだろう。(50)

2.6 PPファミリ

「PPファミリ」は(その名の示唆するとおり)、通常同じ製品やシステムタイプ(例えば、オペレーティングシステム、ファイアウォールなど)に適用する密接に関連するPPの集合である。よってPPは、PPのファミリの開発のより広範囲なプロセスの一部として開発される。可能性としては次の開発を含む：(51)

- a) 同じタイプのTOEの階層的に関連するPPのシリーズ(あるPPが他のPP中に明記されているすべてのITセキュリティ要件を含んでいるような場合、そのPPはもう一方のPPに対し上位階層的であるといえる)。
- b) 異なるITシステムのコンポーネントに適用するPPの集合。例えばスマートカードファミリは集積回路カード、オペレーティングシステム、アプリケーション、スマートカードリーダー、その他のPPを含んでいるであろう。

PPファミリをTOEの特定の種別に適用する場合、ファミリの異なるメンバー間では明白な区別があることは重要なことである。すなわち、TOEセキュリティ要件が明らかに異なる必要がある。このことからPPは、TOEセキュリティ環境のステートメントの違いがない場合、少なくとも(ITセキュリティ要件の選択を決める)それらのセキュリティ対策方針は異なる必要があることになる。例えば、ふたつのPPが同じSFRの集合と、異なるSARの集合を特定していた場合を考える。環境のセキュリティを拡大することで、より低位の保証要件を正当化することはできるかもしれない。このような差異は、セキュリティ対策方針に反映されるべきである。(52)

PPのファミリが(仕様にしても、または想定された環境にしても)ITシステムの異なるコンポーネントに適用される場合、PP間の関係は明らかにすべきである。ITシステムのコンポーネントのPPの定義に関する問題を論じている本ガイドの9章も参照。(53)

3 PP及びSTの記述的な部分

3.1 序説

この章では、PP及びSTの純粋に記述的な部分の構造のガイダンスを提供する。

すなわち：

(54)

- a) PP及びST概説；
- b) PPまたはSTにおけるTOE記述；
- c) PPアプリケーションノート。

3.2 PPまたはSTの記述的な部分

3.2.1 概説

識別

この節の趣旨は、PPまたはSTを一意に識別する十分な識別情報(PPの登録目的のためであり、評価された製品のリストに含めることができるSTのため)を提供することである。最低限、これはPPまたはSTのバージョンを一意に決める識別子を含んだPPまたはSTの名称、及びTOEの識別子(例えば、名称とバージョン番号)を含めるだろう。次に示す情報もまた有効である。(またはPP登録や評価製品のリストに要求されるかもしれない)：

(55)

- a) キーワード(例えば、識別、または登録または製品リストの検索のためのセキュリティ特徴(feature)または機能性(functionality)；
- b) 保証パッケージも特定されるかもしれない(例えば、適用できるならEALなど)；

ISO/IEC 15408は、*概説*においてEAL(もしあれば)を含めるべきであると押し付けるのではなく、保証パッケージまたは使用されたEALがここに配置されることを推奨する。それは国際相互承認において重要な役割を演じる。

(56)

~~ISO/IEC 15408のバージョンは、バージョン管理のために含められる必要がある。とはいえ、ISO/IEC 15408はそれを明示的には要求しない。それは識別においてバージョンを強調することは役に立つかもしれない。~~

(57)

[【ISO/IEC JTC 1/SC 27 N3816改訂情報】：段落57は以下に示すとおり修正される。](#)

[PPまたはSTを開発するために使用されたISO/IEC 15408のバージョンの日付は、バージョン管理のための識別として含められる必要がある。とはいえ、ISO/IEC 15408はそれを明示的には要求しない。PPまたはSTによって必要とされるあらゆる最近のクライテリアの解釈または補足の詳細](#)

も同様である。

STにおいて、CC適合主張の包含は、国際相互承認で重要な役割を演じる概説に配置されなければならない。これは[15408-1]、5.4副項、31ページに列挙されている。(58)

概要

ISO/IEC 15408によれば、*概要*はPPまたはSTの叙述形式の要約であるべきであり、PPカタログ及び登録または評価済み製品リストのSTで用いる抄録として単独に利用可能であるべきである。PPまたはSTが解決するセキュリティ問題のトップレベルの概要が含まれているかもしれず、そして潜在的消費者にとってPPまたはSTが関心の対象となるかどうか決定するために十分であるかもしれない。この概要はPPまたはSTの技術的内容と一貫していなければならない。(59)

3.2.2 TOE記述

TOE記述は、次に示す情報の種類を含めるべきである。(始めの2つはISO/IEC 15408による必須、最後は示唆される)：(60)

- a) 製品またはシステムの種別；
- b) 一般的TOE機能性；
- c) TOE境界(PPではオプション)。

一般的なTOE機能の記述は、まさにそのものである。TOEが特定の目的のセキュリティ製品である場合を除いて、単純にTOEセキュリティ特徴を記述するものではない。(61)

PPでは、TOE境界のオプション記述は、TOEの中に何が含まれて何が含まれないのかを読者に伝える。STでは、TOE境界の定義は、物理的方法(ハードウェア及び/またはソフトウェアのコンポーネント/モジュール)、及び論理的方法(TOEで提供されるIT及びセキュリティ特徴)で提供されなければならない。(62)

TOEやそのセキュリティ機能性の意図された扱い方の不確かさや誤解を招く恐れのある説明(例えば、TOEの評価予定の範囲にないセキュリティ特徴や構成を記述する)を、TOE記述が提示しないことを保証しなければならない。(63)

3.2.3 アプリケーションノート

アプリケーションノートは、PPではオプションであり、独立した節に含めた方が良い。または、それらを文書全体に点在させても良い。例えば、個々のTOEセキュリティ要件に付け加える。アプリケーションノートは、TOEの使用、評価、構築に関係のある、または有用な検討をするいくつかのサポート情報を提供するのに使われなければならない。アプリケーションノートの代表的な使われ方は、個別のセキュリティ要件がTOEという状況下でどのように解釈されるかの説明の提供、または機能コンポーネントの操作がSTでどのように完成されるかのST作成者へのアドバイスの提供である。(64)

もし、アプリケーションノートがPPの至る所の文章にまとめられたならば、その文章が参考であるかないか(例えばSFRやSARの詳細化)を読者が明確に理解するために、個々のアプリケーションノートとして明確に識別されることが推奨される。 (65)

4 TOEセキュリティ環境

4.1 序説

この章では、PPまたはSTのTOEセキュリティ環境の特定についてのガイダンスを提供する。ISO/IEC 15408では、PPまたはSTのこのパートの内容に対する要件を、[15408-1]のB.2.4及びC.2.4副項で定義している。これら二つの節での言い回しについてはまったく同じものであり、これはTOEセキュリティ環境の節の期待される内容がPPとSTとでは大きく変わらないことを示すものととることができる。(66)

TOEセキュリティ環境の節の目的は、TOEが意図する使用環境の定義の特質と範囲、及び使用されることが期待される方法、すなわちTOEが対応する「セキュリティ関連事項」である。このことを以下図1に示す。(67)

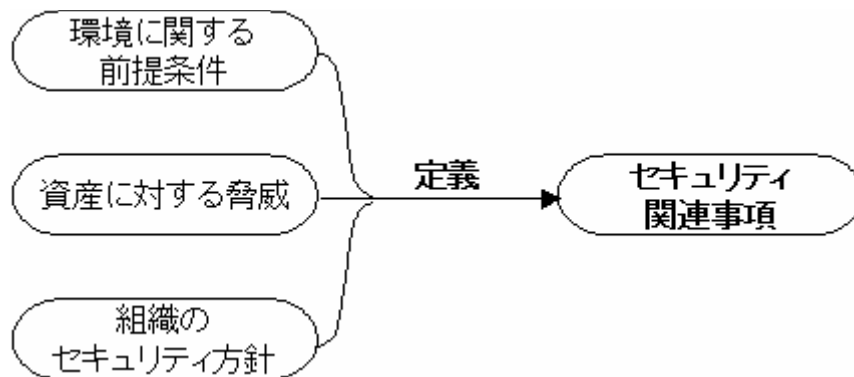


図1 - セキュリティ関連事項の定義

したがって、この節は以下の解説を含むこととなる。(68)

- a) TOEセキュリティ環境に関して作成された前提条件。それによりセキュリティ関連事項の範囲を定義する。
- b) 保護を必要とする資産(通常、IT環境またはTOE自身の情報または資源)、識別された脅威エージェント、それらが資産にもたらす脅威。
- c) セキュリティ関連事項への対応の中で、TOEが従わなければならないあらゆる組織のセキュリティ方針や規則。

PPとSTのその後の節では、TOEがその動作環境とともにどのようにセキュリティ関連事項に対応するかを示す。したがって、セキュリティ関連事項が明白かつ簡潔に定義されていることを保証することが重要となる。さもなければ、間違った関連事項に対応したPPやSTに終わるかもしれない。(69)

一般的原則として、可能であれば、セキュリティ関連事項の定義は、例えばTOEセキュリティ機

能に関する詳細のような、セキュリティ関連事項を満たすためのTOEの対応の形態についてのいかなる解説をも避けるべきである。この原則に従うことで、読者の注意を何がセキュリティ関連事項の重要な側面であるかに焦点をあてることができる。セキュリティ関連事項がいかにTOEにより満足されるかについての解説は、PPまたはSTの後のパートに任せるものとしよう。(70)

4.2 前提条件の識別と特定のしかた

ISO/IEC 15408は、PPまたはSTの *TOEセキュリティ環境*の節がTOEセキュリティ環境またはTOEの意図される使用法に関する前提条件のリストを含むことを要求する。そのようなリストを列挙するには、まず次のような疑問が浮かんでくる。(71)

TOEセキュリティ環境やセキュリティ関連事項の範囲に関し、どのような前提条件を設ければよいのか？

例えば、資産に対する潜在的脅威が、実際にはTOEセキュリティ環境内で問題とならないことを保証するため、いくつかの前提条件を作る必要があるだろう。(72)

前提条件では次の種別を含めるべきである。(73)

- a) TOEの意図した使用法に関する側面
- b) TOEのあらゆる部分の環境的な(例えば物理的な)保護
- c) 接続性の側面(例えば、プライベートネットワークと敵意のあるネットワーク間のネットワーク接続のみを想定して構成されたファイアウォール)
- d) 人的側面(例えば、望むべき利用者役割の種別、彼らの全般的な責任、これらの利用者に置くことのできる信頼の度合い)。

その他の前提条件としては、例えば保証要件の選択を導く前提条件のような、PPまたはSTの内容に重大な影響を与えるものも含まれるであろう。しかしながら、ISO/IEC 15408では、正式に識別された前提条件はセキュリティ対策方針によって対処されることを示さなければならないことを要求していることを覚えておく必要がある。とはいうものの、セキュリティ対策方針までたどれない一般的な前提条件も、PPまたはST中の記述的(参考としての)テキストに有用なものとして含まれるであろう。(74)

すべての前提条件を一度の試みで完全に識別することはできそうもない。むしろ、PPまたはSTの開発を通して更なる前提条件を識別することになるはずである。特に、PPまたはST根拠を構築(例えば、セキュリティ対策方針が識別された脅威に対抗するのに適していることの実証)する場合、PPまたはSTに述べられていないような前提条件を作り出していないかを考慮すべきである。(75)

前提条件を識別するこの反復的なアプローチを用いる際、(先に述べた一般的原則に従い)根拠の構築のプロセスにおいて識別した特定のTOEセキュリティ機能の効果的な使用に関するいかなる「前提条件」を含めることは注意深く考慮することが重要である。そのような詳細は非IT環境のセキュリティ要件により適切に含められるだろう(6.4.2節参照)。しかしながら、(例えば)適切に

TOEセキュリティ機能が構築、及び使用されていることを保証する責任を割当てられている責任者をTOEが一人またはそれ以上有するといったことを「人的」前提条件として述べることは理にかなっている。 (76)

参照を容易にするため、それぞれの前提条件は番号付けか、さもなければ一意にラベル付けされることが推奨される。 (77)

前提条件の例は本ガイドの附属書Bに提示されている。 (78)

4.3 脅威の識別と特定のしかた

ISO/IEC 15408は、PPまたはSTが脅威からの保護を必要とする資産へのあらゆる脅威の記述を含むことを要求する([15408-1]、B.2.4副項、39ページ)。しかしながらISO/IEC 15408では、もしセキュリティ対策方針が単に組織のセキュリティ方針(OSP)や前提条件から引き出されたものであるならば、言い換えれば「セキュリティ関連事項」がOSPや前提条件によって完全に定義されるのであれば、脅威のステートメントは省略できると謳っている。これは、例えばSTがこれらのOSPを定義しているRFPに応じて書かれているような場合かもしれない。 (79)

実際には、脅威のステートメントはOSPの集合の対応よりも、よりセキュリティ関連事項の理解を一般的に提供するものとして、PPまたはST中に含まれることが推奨される。さらに、OSPだけを当てにすることは危険なことである。なぜならば、OSPは最新のものとなっていないであろうし、現在の脅威を正確に反映したものにはなっていないであろう。もし、すでに包括的なOSP一式を有していても、それでもセキュリティ関連事項のより徹底した理解を伝えるのと同様に、PPの最大限の再利用を容易にするために対応する脅威を推定することが望ましい。 (80)

リスク分析の重要性、資産及び資産に対する脅威を正確に識別するために軽視すべきではない。なぜならば、それが適切になされなければ、 (81)

- a) TOEは不十分な保護を提供するかもしれない、その結果組織の資産は、容認できないレベルのリスクにさらされることになるかもしれない。
- b) 脅威が過大に見積もられ、実装や実装において必要とされる保証のコストを上昇させ、潜在的な解決策を制限するかもしれない。

しかしながら、ISO/IEC 15408はリスク分析のためのフレームワークや組織的レベルでの脅威の特定については規定しないことに注意しなければならない。同様に、資産に対する脅威を識別するためのプロセス(これは組織のリスク分析のなかでの難しい部分のひとつである)についての詳細な解説は、本ガイドの範囲の外にある。しかしながら、このガイドを完全とするため、これらに伴う一般的な原則を以下に示す。また[15408-1] 4項も参照。この話題のより詳細なガイダンスについては、[13335]^(訳注)のような標準を読者は参照することになる。 (82)

(訳注：原文では、「GMITS」となっているが、「13335」への修正漏れである。訳では「13335」とした。)

4.3.1 脅威をどのように識別すべきか

「脅威」は([15408-1]、4.1.1副項、13ページに述べられているように)、ただ望ましくない事象であり、それは脅威エージェント、推定される攻撃方法、攻撃の土台となるあらゆる脆弱性、そして攻撃を受ける資産の識別といった観点により特徴付けられている([15408-1]、4.3.1副項、21ページ)。(83)

なにが脅威かを識別するために、次の問いに答える必要がある。(84)

- a) 保護を必要とする資産はなにか？
- b) 誰または何が脅威エージェントか？
- c) どんな攻撃方法または望ましくない事象から資産の保護が必要となるか？

資産を識別する

ISO/IEC 15408は資産を、TOEの対抗策によって保護されるべき情報または資源として定義している([15408-1]、2.3副項、4ページ)。資産とは、それらの所有者たち(個人であれ、組織であれ)にとって、そのもの本来の価値を持つことから、資産と名付けられた。さらに、所有者の要望や利益に反して、例えば資産の機密性、完全性、信頼性、真正性、責任追跡性または可用性の低下を生じさせることによってこれらの資産の価値を危険にさらそうとするかもしれない脅威エージェントにとって、資産はしばしば価値がある。(85)

PPまたはST作成者にとって重要な資産は、組織の一次資産(例えば、貨幣的価値、または組織の職員、顧客、または世評)の表現であろう。[15408-1] 4.1.1副項に規定されている記述によると、資産の所有者は(TOEが配置された)ITシステム内の資産の保護を講じる責任がある人々として照会されるものと見なされるべきである。実際、彼らが提示した一次資産は、TOEの所有者やTOEが含む情報の所有者と異なる多数の所有者を持つかもしれない。PPやSTの読者にとって、資産を記述する際、そのような一次所有者を識別することは有益かもしれない。例えば、(86)

[【ISO/IEC JTC 1/SC 27 N3816改訂情報】：段落86、a\)は以下に示すとおり\[3\]への参照に関する記述が追加される。](#)

- a) 信頼できる第三者機関(TTP)において、異なる鍵を異なる所有者、すなわちTTPそれ自身の所有者に加え、TTP加入者も持つ(附属書Fの作業例 [及び追加情報として\[3\]も参照](#))。
- b) 医療システムでは、一般的にはその使用と管理のガイドの複雑な規則と配慮により、TOEの情報はただの一人の所有者が持つのではなく、むしろ関与するすべての人から構成されることになっている。

ISO/IEC 15408では、資産は大抵、ITシステムによって格納され、処理され、伝達される情報というかたちを持つと示唆している([15408-1]、4.1.2副項、15ページ)。ファイアウォールや侵入検出システムにより保護されている情報や資源の場合のように、資産はTOEの外部(しかしIT環境

内)であってもよいことは強調されるべきである。 (87)

ISO/IEC 15408は、識別された資産が公認の証明書やIT実装のような間接的にセキュリティ要件の対象となるものを含んでもよいと示唆する([15408-1]、4.3.1副項、21ページ)。そのような「資産」は、一次資産(またはそれらの表現)を保護するのに必要となる対抗策の識別のプロセスの一部として識別されるであろう。ISO/IEC 15408では認められてはいるものの、TOEそれ自身の存在により導かれ、また単に一次資産に間接的に関係のあるような情報や資源を、資産として明示的に識別することは(一般には)推奨できない。なぜならば、そのような詳細を含むことは、 (88)

- a) (IT環境内の一次資産またはそれらの表現を保護する)TOEの第一目標が不明瞭となる。
- b) PPまたはSTのあまりに早い段階で、実装詳細(すなわち定義されたセキュリティ関連事項の解決策)を導入することとなる。それらは、脅威やセキュリティ対策方針を通して明らかにされるものである。

脅威エージェントを識別する

上に述べたように、脅威エージェントは人間か非人間かであるが、([15408-1]、4.1.1副項、13ページで指摘しているように)セキュリティの分野で、悪意またはその他の人間のアクティビティに関連するこれらの脅威に対し、より多くの注意がいつも払われている。 (89)

誰が人間脅威エージェントかを識別するにおいて、次のことを考慮すべきである、 (90)

- a) 誰が、識別された資産を危険にさらそうとすることに、どのような理由であれ価値があるか考えるか。
- b) 誰が、これらの資産を危険にさらそうと企てる立場にいるであろうか。 - 言い換えれば、資産を格納、処理、伝送するITシステムへのアクセスを手に入れることができるか。
- c) 推定される彼らの専門技術のレベル、機会、利用できる資源(例えばネットワークのハッキングやプロービングの自動ツール)と動機。

脅威の非人間の原因もまた、人間の原因から故意でなく生じた脅威(例えばアクシデントによる)と同様に資産を危険にさらすことへ至らしむことがあるということは検討されるべきである。 (91)

攻撃方法を識別する

保護されるべき資産と脅威エージェントを識別したならば、次の段階は資産を危険にさらすことへ至らしむかもしれない可能性のある攻撃方法を識別することである。これはTOEセキュリティ環境に関し、何が分かっているかに基づくであろう。例えば、 (92)

- a) 脅威エージェントが悪用するかもしれない資産の潜在的脆弱性。
- b) TOEセキュリティ環境へのアクセスを持つ攻撃者の能力。

組織の資産に対する潜在的脆弱性は、識別された環境の前提条件を考慮することで、TOEセキュリティ環境の脆弱性分析によって識別されるかもしれない(しかしながら、そのような分析はISO/IEC 15408の範囲内ではないことに注意)。しかしながら、そのような分析はすべての脆弱性を識別しないであろうことに注意をし、それゆえに新しくかつ未発見の脅威の可能性を小さく見積もるべきではない。(93)

脅威識別でのリスク分析の役割

リスク分析方法は脅威識別のプロセスで役に立つであろうが、そのような方法はISO/IEC 15408では定義されていない。リスク分析プロセスはまた、TOEとその環境のセキュリティ対策方針の識別(4章参照)や脅威に対応するために提案された対抗策の保証の要求されるレベル(5章参照)に関連すると思われる。そのような方法は次のことを考慮するであろう。(94)

- a) 以下のことを考慮した資産を危険にさらす公算と結果。
 - 識別された、可能性のある攻撃方法
 - 成功したことを判明できる攻撃の公算
 - (攻撃の成功により生じる明確な損失の予期された規模を含む)起こり得るあらゆる損害の結果
- b) 法的要件やコストなどその他の制約

4.3.2 脅威をどのように特定すべきか？

TOEまたはその環境により対応する脅威を識別したならば、次の段階はPPまたはSTの中でそれらを特定することである。先に書き留めたように、*TOEセキュリティ環境*の節はセキュリティ関連事項の明確かつ簡潔なステートメントでなくてはならず、また脅威の明確かつ簡潔な特定がこの主要な部分である。(95)

脅威の*明確な(clear)*特定を規定するために、以下の(上記の4.3.1節で述べたように、識別された)詳細を含めるべきである。(96)

- a) 脅威エージェント(例えば、TOEの許可された利用者)、
- b) 攻撃にさらされる資産(例えば、秘匿データ)、
- c) 用いられる攻撃方法(例えば、TOEの許可された利用者を装う)。

例えば、(97)

攻撃者は、TOEの許可された利用者を装うことで、情報または資源への不当なアクセスをもたらすかもしれない。

TOEの許可された利用者は、他の許可された利用者を装うことで、情報または資源への不当なアクセスをもたらすかもしれない。

脅威の記述に、その脅威の記述の中で用いられるあらゆる用語の解説を付けたり、危険にさらされる資産や脅威エージェントが用いるかもしれない特定の攻撃方法に基づく脅威の範囲を付け加えることは、読者が脅威を理解するのに役立つであろう。例えば、上記の脅威の場合、危険にさらされた資産が、(成りすまされた)利用者がアクセス権を持つ情報であり、資源であること；または(多くの異なる手法から)どのように成りすましが達成されるだろうかということを明確にするのに有効であろう。(98)

脅威の簡潔な(*concise*)ステートメントを持つことを保証するのを助けるために、できる限り脅威の記述はそれぞれをばらばらにするべきである。言い換えれば、異なる脅威間の重複は最小限にとどめるべきである。このことは不必要な復唱を避けることでPPまたはST根拠を単純化するのを助けるだけでなく、PPまたはSTの読者による混同の恐れを避けるためにも役立つであろう。(99)

もし同じ詳細レベルですべての脅威を特定するのであれば、脅威間の重複はより簡単に避けることができる。例えば、その脅威がもしPPまたはSTのどこかで述べられている、より一般的な脅威とすでに関連している特定の攻撃のシナリオであるような場合、特定の資産に対する詳細な攻撃方法を記述する脅威を特定しないこと。(100)

参照を容易にするため、それぞれの脅威は一意にラベル付けられるべきである(例えば、特定されたセキュリティ対策方針が脅威にどのように対応しているかを示すPP根拠のこれらの部分)。可能なオプションは、(101)

- a) 脅威のシーケンシャル番号(例えば、T1、T2、T3など)；
- b) 脅威に対して短くしかも意味のある「名前」を一意のラベルとして与える(例えば、附属書Bで示した脅威の例に用いられているようなもの)。

最初のオプションの利点は、単純な番号は、参照目的に使用するのに概して短く容易である。2番目のオプションの利点は、ラベルは独立した識別子としても、より意味があり覚えやすい。しかしながら、2番目のオプションを使用した場合、(ラベルでの文字の数の制限という現実的制約のため)すべての場合において、しかもその意図を正確に反映させるように完全に定義されたラベルを割当ててすることは不可能であろう。(102)

脅威の記述は、保護を必要とする直接的に資産を危険にさらすような潜在的な事象の言及のみすべきである。したがって、それらはTOEにおけるセキュリティ欠陥かもしれないような「脅威」を含めないことが推奨される。そのような「脅威」は、とりわけ、それはいかなるTOEにも当てはまるため、読者がセキュリティニーズがなんであるかを理解する助けとはならない。さらに言えば、それはTOEまたはTOEセキュリティ環境において用いられる非技術的手段によって実際に対応できる事象ではない。むしろ、それはTOEを開発または評価する人々による対処によってのみ対応可能である。(103)

脅威に対する対抗策の序説では、間接的に資産を危険にさらすことになるであろう攻撃の詳細、例えばTOEセキュリティ機能に対するバイパスや改ざん攻撃について紹介してもよい。このような資産に対する間接的な脅威を考慮する場合、慎重であることを勧める。特に、そのような脅威

を保証すべきである。 (104)

- a) *TOEセキュリティ環境*の節にそれらを含めた結果、TOE実装の詳細を先に述べることで読者が混同することはない。
- b) 既存の脅威の範囲に、すでに収まってはいない。

例えば、もし脅威Xが、資産Yを危険にさらすのであれば、すべての脅威Xに対する対抗策をバイパスする試みは、資産Yを危険にさらすことへと至らしめる。それゆえに、脅威Xに対する対抗策のバイパスは、事実上すでに脅威Xの範囲にある攻撃方法といえるであろう。ゆえに、(*TOEセキュリティ環境*のステートメントを簡略にするために)独立した脅威として明示的に述べる必要はない。 (105)

(相互サポートを要求するISO/IEC 15408のITセキュリティ要件を選択することになった場合、バイパスや改ざんなどTOEの対抗策に対する攻撃の考慮が必要となることもまた注意すべきである。8.3.4節参照。TOEセキュリティ機能に対し可能ないかなる攻撃もまた、TOEの評価の間に見つけ出されなければならない。) (106)

脅威の例は、本ガイドの附属書Bに提示されている。 (107)

4.3.3 脅威のステートメントを完了させる

ISO/IEC 15408は*TOEセキュリティ環境*の節が、セキュアなTOE操作に関連するような資産に対するすべての脅威を含めることを要求している([15408-1]、B.2.4副項、39ページ)。脅威の第一の関心事項は、それらがTOEによって対抗されるということである(それらはしばしば手続き上または非技術的対抗策に関連していることもある)。しかしながら、完全なものにするには、例えば、TOEがそれに対しての保護を提供しない攻撃方法や脅威エージェントなどのため、TOEによってまったく対応されないいくつかの脅威をPPやSTに含める必要があるだろう。 (108)

TOEのセキュアな運用に関連する脅威の例で、しかしTOEによって対応されないであろうものとして次のようなものが含まれるであろう。 (109)

- a) TOEに対する物理的攻撃。
- b) 高い特権利用者による信用の悪用。
- c) 不用意なまたは適切でない訓練を受けた管理者によるTOEの不適切な管理や運用。

どの脅威がTOEによって対応されて、(もしあれば)どの脅威が環境によってのみ対応されるのかに関する決断は、(もちろん)セキュリティ対策方針が決着するまではなされないであろう。 (110)

識別された環境の前提条件は、それがなければTOEのセキュアな操作に関連して考慮されるであろう脅威を排除できることに注意すべきである。このことからすると、PPやSTの作成者は、そのような側面を環境の前提条件のなかで扱うか、運用環境によって対抗すべき脅威のステートメン

トのなかで扱うかの決断においてある程度の自由をもつ。どちらのアプローチも、前提条件や脅威どちらもそれらを支持または対応するセキュリティ対策方針にマッピングされなければならないので、容認できる。したがって、これら二つの選択肢の選択は、読者がセキュリティ関連事項を理解するのを助けるのにどちらが最良なアプローチかに基づいて行われるべきである。通例として特定できる攻撃は脅威として扱うべきで、一方より一般的な性格をもつ攻撃は前提条件として扱うのが最良であろう。どちらのアプローチを採用するにせよ、その問題についてはただ一度だけ述べられることが重要である。(111)

4.4 いかに関連組織のセキュリティ方針を識別し特定するか

ISO/IEC 15408はTOEセキュリティ環境の節が、TOEが従わなければならないすべてのOSPの記述を含めることを要求している([15408-1]、B.2.4副項、39ページ)。しかしながら、ISO/IEC 15408は次のようにも言っている。もし、セキュリティ対策方針がただ脅威と前提条件から引き出されたのであれば、言い換えればセキュリティ関連事項が完全に脅威と前提条件で定義されているのであれば、OSPのステートメントは省略することができる。(112)

先の4.3節に示したように、PPやSTの作成者は、資産に対して現存し関連する脅威に対するいかなるOSPも、それらをPPまたはSTに含める前にレビューすべきである。(113)

OSPは、組織によって課されるひとつまたはそれ以上の規則、手続きまたは慣行として定義される([15408-1]、2.3副項、5ページ)。OSPはTOEまたはその環境、またはそれらふたつのいくつかの組合せを用いる必要があるかもしれない。(114)

PPまたはSTが脅威だけでなくOSPを特定している場合、TOEセキュリティ環境の節でセキュリティ関連事項の簡潔なステートメントを提供する要件を思い出すべきである。脅威を異なる表し方で言い直しているだけのOSPを含むことは、ほとんど有用な主旨を提供するものではない(もちろん、既存の脅威の言い換えであるOSPを、関連する組織が命じているために選択権がない場合を除いてである)。(115)

例えば、次に述べる脅威を識別したとする。(116)

許可されない人間がTOEに論理的なアクセスを得るかもしれない。

すると、次に述べるOSPを含めることはあまり得るところがない。

TOEの正当な利用者は、TOEアクセスが認められる前に識別されなければならない。

このOSPは(実際には)脅威を異なる言い方で言い換えているだけではない。それはまた、セキュリティ関連事項に対する期待される応答をもたらすセキュリティ対策方針の定義をも先取りしてしまっている。問題を一度だけ述べておけば、そのPPまたはSTはフォローするのがより容易となるであろう。(117)

一般に、TOEが特定の組織や組織のタイプにより用いられることを意図されている場合、または脅威の記述の中に明確に含めたり、それによって暗示できないような規則のセットをTOEが実装する必要がある場合には、OSPを特定することは適切であろう。例としては、 (118)

- a) 適用される情報フロー制御規則の識別
- b) 適用されるアクセス制御規則の識別
- c) セキュリティ監査に関する組織のセキュリティ方針の定義
- d) 組織が命じる解決策の技法。例えば、特定され承認された暗号アルゴリズムの使用や識別された標準への適合

脅威と同様、それぞれのOSPは参照が容易なように一意にラベル付けされなければならない。 (119)

OSPの例は、本ガイドの附属書Bに提示されている。 (120)

5 セキュリティ対策方針

5.1 序説

この章はPPまたはSTのセキュリティ対策方針の識別と特定についてのガイダンスを提供するものであり、これに関する要件は[15408-1]B.2.5及びC.2.5節に記述されている。 (121)

セキュリティ対策方針はセキュリティ問題への意図した対応の簡潔なステートメントを規定する ([15408-3]、4.4副項、31ページ)。言い換えれば、何がセキュリティ関連事項かを(TOEセキュリティ環境の節に)記述し、TOE及びその環境によって対応される範囲の提示をセキュリティ対策方針のステートメントの形で与える必要がある。これは、下記の図2に図解されている。 (122)

【ISO/IEC JTC 1/SC 27 N3816改訂情報】：図2は以下に示すとおり非IT環境のセキュリティ要件にオプションという記述が追加される。

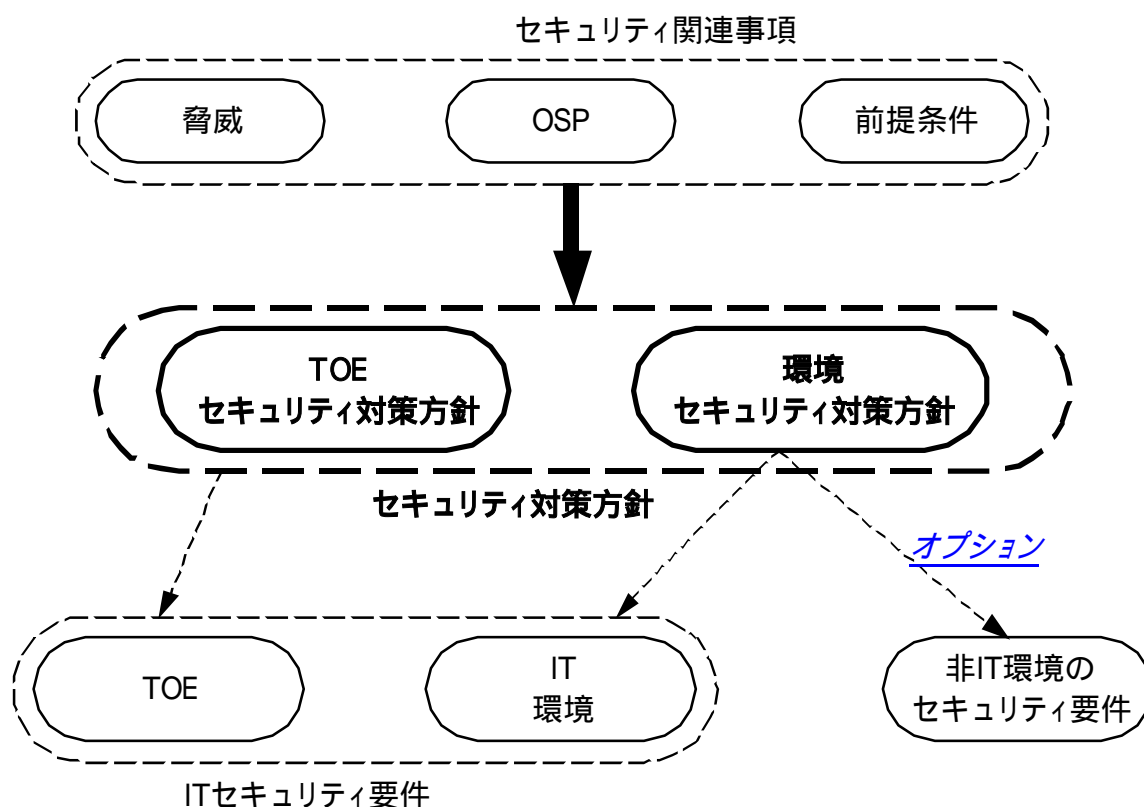


図2 - セキュリティ対策方針の役割

図2はISO/IEC 15408がPPまたはSTにおいて明確に区別することを要求する2つのタイプのセキュリティ対策方針を図解している： (123)

- a) TOEに実装される技術的(IT)対策により満足されるべき、TOEのセキュリティ対策方針；
- b) IT環境に実装される技術的手段か、非IT(例えば、手続き)手段のどちらかにより満足されるべき、環境のセキュリティ対策方針。

このように、セキュリティ対策方針のステートメントはTOEセキュリティ環境の状況の中で、TOEが何をやり何をやらないかを概述するために役立つ。TOEとその環境の間でセキュリティ関連事項を満足するための責任を明確に区別することにより、保護を必要とする資産に対する脅威を軽減することができる。さらに、責任の区別を定義する中で、セキュリティ対策方針はTOEの評価の範囲を決めるだろう。これは、TOEのセキュリティ対策方針が、セキュリティ関連事項を満足するためのTOEの責任を実行するために必要なセキュリティ機能要件の選択と、TOEに要求されるセキュリティ機能に必要な保証レベルの決定の両方を推し進めるからである。 (124)

5.2 TOEのセキュリティ対策方針の特定のみかた

TOEのセキュリティ対策方針は、脅威に対抗することにおいて、及びOSPをサポートすることにおいて、何がTOEの責任であるかを記述する。上記の図2に示すように、TOEのセキュリティ対策方針はセキュリティ関連事項からITセキュリティ要件への「踏み石」(または橋渡し)を読者に対して提供するものであり、このことは、TOEのセキュリティ対策方針を特定する際に、常に心に留めておくべきである。 (125)

PPまたはST中でセキュリティ対策方針により果たされる中核の役割のため、セキュリティ対策方針のステートメントにおいてどのレベルの詳細さが適切かという疑問は重要なものである。ISO/IEC 15408は、セキュリティ対策方針は簡潔(*concise*)であることを意図されていると述べる(上記で指摘したように)ことで、有力なヒントを与えている。実際のところ、次の2つの考慮されるべき事柄のバランスを取る必要がある： (126)

- a) セキュリティ関連事項がTOEによって対応される範囲を、実装までの詳細を探索することなく理解することを助けるべきである；理想的には、TOEのセキュリティ対策方針は実装から独立しているべきである。よって、解決策がどのように(*how*)達成されるかよりむしろ何を(*what*)達成しようと意図するかに焦点が置かれる。
- b) それと同時に、定義されるセキュリティ対策方針が単に脅威やOSPの情報を繰り返すだけにはならないことを保証すべきである(たとえ、僅かに異なる形式であったとしても)。

セキュリティ対策方針が適切なレベルの詳細度で表現されるかどうかの検査は結局、セキュリティ対策方針及びセキュリティ要件の根拠を構成する際に訪れる。もし一方の根拠のステップが簡単すぎるものであり、片やもう一方のステップがかなり困難である場合、どちらのステップが簡

単かによるが、セキュリティ対策方針が詳細すぎるか抽象的すぎるかのどちらかである。 (127)

本ガイドの次の章で明らかになるように、明確に定義されたTOEのセキュリティ対策方針は、それを満足するために選択されたITセキュリティ要件に対して、セキュリティ機能要件(6.2.1節参照)とセキュリティ保証要件(6.3.1節参照)の両方の観点から、過剰ではないことを保証することを助ける。これは、さらにTOE評価の費用と時間を最小にすることに役立つ。 (128)

大まかに言って、識別された脅威に対応するために、3つのタイプのセキュリティ対策方針を識別することができる： (129)

- a) *防止の対策方針* 脅威が遂行されることを妨げる、または脅威が遂行できる手段を制限する；
- b) *検出の対策方針* TOEのセキュアな動作に関連する事象の発生を検出及び監視する手段を提供する
- c) *回復の対策方針* 起こりうる可能性のあるセキュリティ侵害または他の望ましくない事象への対応として、セキュアな状態への回復及び/または起こったいかなる損害も抑制するために、TOEがアクションを起こすことを要求する。

*防止の対策方針*の例は以下のものであり、これは、TOEの利用者の識別と認証に対する要求を識別したものである。 (130)

TOEは利用者がTOE設備にアクセスすることを許可する前に、各々の利用者が一意に識別されること、及び主張された識別情報が認証されることを保証しなければならない。

アクセス制御と情報フロー制御のセキュリティ対策方針もまた、*防止*の категорияに区分される。セキュリティ関連事項が、TOEが1つ以上のアクセス制御方針または情報フロー制御方針を実施することを示唆している場合、各々の方針に対して区別されたセキュリティ対策方針を識別することが推奨される。 (131)

*検出のセキュリティ対策方針*の例は下記のものであり、TOEが発信の否認不可の能力を提供することに対する要求を識別する。 (132)

TOEは情報の受信者が情報の発信の証明に使用できる証拠を生成できる手段を提供する。

*回復のセキュリティ対策方針*の例は下記のものであり、TOEが検出された侵入に対して対応することに対する要求を識別する。 (133)

TOEは切迫したセキュリティ侵害を示唆するイベントを検出した場合すぐさま、他のTOE利用者に提供するサービスへの混乱を最小限にしつつ、攻撃に対して適切な手順を取る。

可能な場合、セキュリティ対策方針は、最小限の期待される効果を非形式的に定量化することを志すべきであり、これにより、PPまたはSTの根拠においてどのレベルの効果が正当化されるべきかといった小さな疑問を取り除く。定量は以下のように記述されるであろう： (134)

- a) (例えば環境条件に対しての、直前の状態に対しての)相対的な条件で；
- b) 絶対的な数値条件で。

明確に、絶対的な数値を特定することは最も正確な選択肢であるが、有効性を評価することは最も困難なことである。 (135)

SFRが既知である状況で、PPまたはSTが書かれる場合、有用な出発点は、PPまたはSTで特定されているセキュリティ機能要件の主要なグループ分けの各々に対応させて、1つのTOEのセキュリティ対策方針を定義することである。この手法の1つの利点はセキュリティ要件の根拠を構成することが簡単になることであろう。この手法が採用されれば、定義されたセキュリティ対策方針がこの章のガイダンスに従うことを一層確信させるものになるだろう。とりわけ、セキュリティ対策方針が不必要な実装上の詳細を含まないことを保証すべきである。 (136)

セキュリティ対策方針の例は、本ガイドの附属書 Bに提供される。 (137)

ISO/IEC 15408はTOEのセキュリティ対策方針が関連する脅威やOSPにまで明確にたどることができることを要求する([15408-1]、B.2.5副項、39ページ)。よって、下記のことを保証する必要がある： (138)

- a) TOEにより一部または全部が對抗されるべき識別された脅威の各々が、少なくとも1つ以上のTOEのセキュリティ対策方針によって対応される；
- b) TOEにより一部または全部が満足されるべき、識別されたOSPの各々が、少なくとも1つのTOEのセキュリティ対策方針によって対応される。

この追跡性は文章の相互参照の方法で、または表形式のマッピングで提供される。ここで要求される情報は根拠の中で提供されるであろうが(8章参照)、セキュリティ対策方針の節でマッピングが提供されれば、PPまたはSTの読者にとってより助けになるものになるであろう。セキュリティ対策方針がOSPに従うために含まれる場合、実施されるべきすべてのルールを繰り返すよりむしろ、OSPを参照することが適切である(例えば、附属書 Bの例のO.DACについてのよう)。 (139)

脅威とOSPについてと同様に、TOEのセキュリティ対策方針は参照の簡単化のために一意にラベル付けされるべきである。また、ラベル付けの規約は通し番号(例えば、O1、O2、O3など)や短い意味のある名前(例えば、附属書 Bに提示される例のような)に基づいてもよい。 (140)

5.3 環境のセキュリティ対策方針の特定のしかた

環境のセキュリティ対策方針は、IT環境により、また同様にTOEの運用環境で実施されるべき手

続的または非技術的手段により、満足されるべきいかなるセキュリティ対策方針も含むべきである。言い換えると、環境のセキュリティ対策方針はITまたは非ITどちらでもありうる。(141)

環境のセキュリティ対策方針は、TOEが対応しない(またはできない)ことが予測されるセキュリティ関連事項の局面に対応するために識別されなければならない。とりわけ、環境のセキュリティ対策方針は以下を行うことが必要となる：(142)

- a) TOEによって対抗されない脅威(または脅威の局面)に対抗する；
- b) TOEによって完全には満足されないOSPをサポートする；
- c) 脅威への対抗を助けるまたはOSPを満足することを助けることにより、識別されたTOEのセキュリティ対策方針をサポートする；
- d) 識別された環境の前提条件が満足されることを保証する。

識別プロセスの適切な出発点は、TOEによって完全には対応されない脅威、OSP、前提条件を各々順に取り上げることによりセキュリティ対策方針のリストを編集し、そしてそのようなTOEのセキュリティ対策方針の各々に対して、下記のどちらかを行う：(143)

- a) その局面に対応するために新たなセキュリティ対策方針をリストに付加する；
または
- b) 適切なものが既に識別されていれば(恐らく、範囲を広げるためにセキュリティ対策方針を書き換えて)、既存のセキュリティ対策方針にマッピングする。

このリストは、セキュリティ対策方針根拠を系統立てて述べる際に改良されるべきである。なぜならこれは、セキュリティ関連事項が適切に(脅威が対抗されOSPと前提条件がカバーされているという観点から)満足されることを保証するために必要な追加のセキュリティ対策方針の識別を導くからである。(144)

この識別プロセスはTOEのセキュリティ対策方針の識別と同時進行で遂行されるべきである。セキュリティ対策方針のステートメントは全体として、TOEとその環境との間の責任の区分が適切であることを保証するためにレビューされるべきである。例えば下記のように：(145)

- a) TOEのセキュリティ対策方針が、実装及び評価のコストが保護される資産の価値に対して不釣り合いであるITセキュリティ要件のセットを導くことがない；
- b) 環境のセキュリティ対策方針が、実施することが実際的ではない、またはTOE利用者に対して過度に制限的である手続きのセットまたは非ITセキュリティ要件を導くことがない。

環境の(非IT)セキュリティ対策方針の典型例には下記のようなものがある：(146)

- a) TOEがセキュアなやり方で(特に環境の前提条件に従って)、使用されることを保証する手続きの確立と実行

b) 十分なセキュリティの実施のもとでの、管理者及び利用者の教育と養成の対策方針

そこで、環境のセキュリティ対策方針のステートメントは、TOEによって提供されるべきセキュリティのサービスが効果的であることを保証するために必要とされる管理アクティビティに関連する、いかなる対策方針も含むべきである。いくつかのケースでは、要求される管理アクティビティが明示的であり、都合よく(非IT)環境のセキュリティ対策方針の形で表現することができる(例えば、監査機能の適切な管理の必要性に関して)。別のケースでは、要求される管理アクティビティがTOEセキュリティ対策方針を実施するために使用される詳細なセキュリティ要件に依存するだろう。例えば、前述の段落130で与えられる「識別」と「認証」のセキュリティ対策方針は利用者パスワードで実装されるかもしれない。これは、利用者が他人に対してパスワードが露見しないことを保証する要件を暗に含んでおり、環境のセキュリティ対策方針を詳細化した非IT環境のセキュリティ要件(6.4.2節参照)として適切に表現されるだろう。(147)

脅威またはOSPが一部はTOEで一部は環境でカバーされる場合、関連するセキュリティ対策方針はそれぞれのカテゴリーで繰り返されるべきであるとISO/IEC 15408は記述している([15408-1]、B.2.5副項、39ページ)。このことは、上記で識別された識別と認証のセキュリティ対策方針のケースに当てはまるであろう。この場合は、関連する脅威はTOEと環境内の管理アクティビティ(例えば、パスワードのような認証データの管理)の適切なサポートによってのみ対抗できる。このようにしてセキュリティ対策方針は下記のような書き方で記述されるであろう：(148)

TOEは、その環境からのサポートとともに、TOE設備に対するアクセスが許可される前に、利用者が一意に識別されること、主張された識別情報が認証されることを保証する。

TOEとその環境の間で責任を明確に区別することが可能であるようなケースでは、両方のカテゴリーでのセキュリティ対策方針のこのような繰り返しは明らかに不要だろう。一つの例が監査のためのセキュリティ対策方針の識別であろう。この場合、TOEはデータを生成し収集することに対して責任を割り当てられ、そして環境はそれをサポートする管理アクティビティ(例えば、生成されたデータの解析)に対して責任を割り当てられる。(149)

環境のITセキュリティ対策方針の典型例は、TOE利用者の識別と認証を行う下層のオペレーティングシステムに対するセキュリティ対策方針である。(IT環境に対するこのような依存性は環境のITセキュリティ要件として詳細化されるであろう：6.4.1節参照)。(150)

TOEのセキュリティ対策方針と同様に、環境のセキュリティ対策方針は参照の簡単化のために一意にラベル付けされることが推奨される。環境のセキュリティ対策方針をTOEのセキュリティ対策方針と明確に区別するようなラベル付けの規約を適用するならば、それは役に立つものになるであろう。番号付けの規約が使用される場合、2つのタイプのセキュリティ対策方針に対して区別された番号付けがあるべきである(例えば、環境のセキュリティ対策方針はOE1、OE2、OE3などのように番号付けできる)。(151)

環境のセキュリティ対策方針の例は、本ガイドの附属書Bに提示されている。

(152)

6 セキュリティ要件

6.1 序説

この章では、PPまたはSTにおけるITセキュリティ要件を特定するためのガイダンスを提供する。このガイダンスは、TOEセキュリティ要件とIT環境に対するセキュリティ要件の両方に適用する。非IT環境に対するセキュリティ要件(PPまたはSTの正式な部分では要求されない)についても簡潔に論じる。 (153)

PPまたはSTで特定されるITセキュリティ要件の種類を次に示す： (154)

- a) TOEのセキュリティ機能要件(SFR)。これらは、TOEに対するセキュリティ対策方針が達成される保証をTOEが与えなければならないという、セキュリティ機能に対する要件を識別する。
- b) TOEのセキュリティ保証要件(SAR)。これらは、SFRの実装表現において要求される保証のレベルを識別する。
- c) IT環境のセキュリティ要件。(これらはPPまたはSTではオプション)これらは、TOEに対するセキュリティ対策方針が達成されることを保証するために必要なIT環境(すなわち、ハードウェア、ソフトウェア及び/またはTOEの外部ソフトウェア)によって満足させられる機能と保証の要件を定義する。

これを次の図3に示す。 (155)

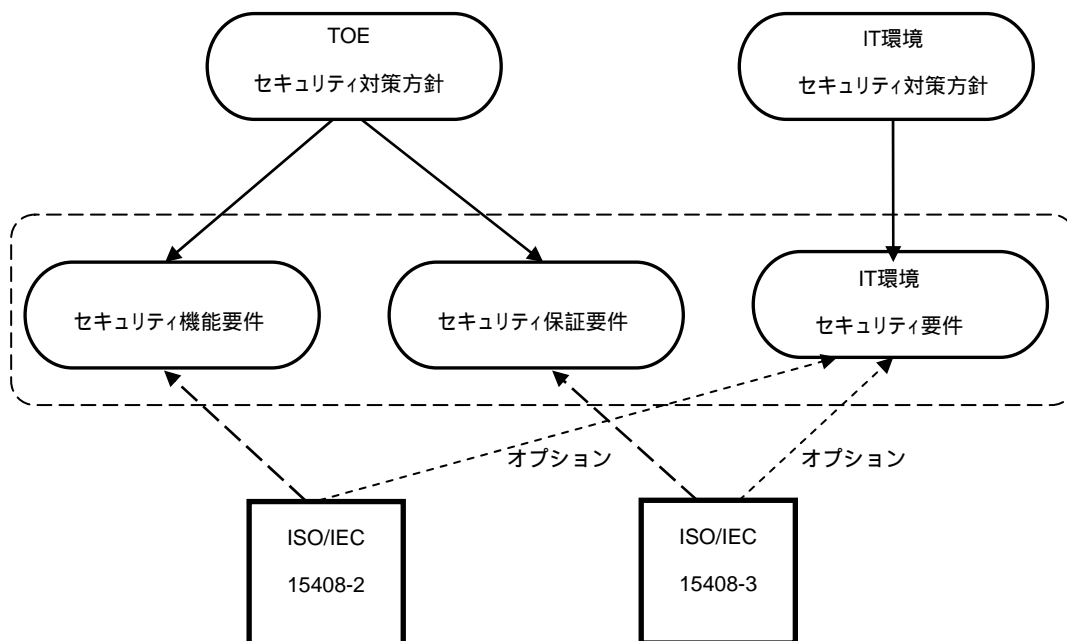


図3 - ITセキュリティ要件の展開

機能と保証の要件に加えて、PPまたはSTのITセキュリティ要件の節で、関連する明確な強度主張とともにTOEセキュリティ機能の最小強度レベルの特定を要求される(適切な場合)。([15408-1] B.2.6及びC.2.6副項参照) (156)

図3に示すように、ITセキュリティ要件の重要な特徴は、[15408-2]で定義された機能コンポーネントのカタログ及び[15408-3]で定義された保証コンポーネントのカタログを適切に使用することが可能であり、それによって構成されることを意図することである。ここでのISO/IEC 15408の意図は、ITセキュリティ要件の提示のしかたにおいて標準化の程度を保証することである。ITセキュリティ要件を表現するこの「共通言語」の使用は、このようにPPとSTの比較を容易にすることを意図する。(157)

しかしながら、ISO/IEC 15408では、[15408-2]または[15408-3]の機能や保証コンポーネントが適切なものがない場合があることを認めている。この場合、ITセキュリティ要件は、ISO/IEC 15408を参照しないで明示的に述べることができる。ただし、ITセキュリティ要件は、ISO/IEC 15408に存在するコンポーネントと同様に表現され、評価でき、あいまいでないものでなければならない。6.2.7節では、[15408-2]で識別することができ、機能コンポーネントが適切でない場合のガイダンスを提供し、6.3.3節では、保証コンポーネントに関する同様のガイダンスを提供する。(158)

セキュリティ要件を適切に修整させるそれら(すなわち割付、繰返し、選択、詳細化)を実行する操作のセットを許すことによって、SFRとSARが特定されるやり方でISO/IEC 15408は柔軟度を許す。ISO/IEC 15408機能コンポーネントの操作の使い方に対するガイダンスを6.2.2節以降に提供する。ISO/IEC 15408保証コンポーネントに対する同様のことを6.3.2節に提供する。(159)

[15408-2]及び[15408-3]における各々のセキュリティ要件コンポーネントは、定義された分類法に基礎を置くISO/IEC 15408でのそれ自身の一意の参照によって割り当てられる。(160)

- a) [15408-2]において、例えばコンポーネントFAU_GEN.1.2は次の意味を持つ。
 - 「F」は機能要件であることを示す。
 - 「AU」はSFRのセキュリティ監査クラスに属することを示す。
 - 「GEN」はそのクラス中のセキュリティ監査データ生成ファミリに属することを示す。
 - 「1」はそのファミリ中の監査データ生成コンポーネントであることを示す。
 - 「2」はそのコンポーネント中の第2エレメントであることを示す。
- b) [15408-3]のコンポーネントも同様の分類法を使用する。しかし、1文字付加することにより、保証エレメントの三つのセットのうちの一つに属するという追加の識別子をそれぞれのエレメントで使用する。
 - 文字「D」は、開発者によって行われるアクティビティである開発者アク

ションエレメントのセットに属することを示す。

- 文字「C」は、証拠が伝えようとする情報である *内容・提示エレメント*のセットに属することを示す。
 - 文字「E」は、評価者によって行われるアクティビティである *評価者アクションエレメント*のセットに属することを示す。
- c) [15408-3]において、例えば、コンポーネントADV_HLD.1.2Cは次の意味を持つ。
- 「A」は *保証要件*であることを示す。
 - 「DV」はSARの *開発クラス*に属することを示す。
 - 「HLD」はそのクラスの中の *上位レベル設計ファミリ*に属することを示す。
 - 「1」はそのファミリの中の *記述的上位レベル設計コンポーネント*であることを示す。
 - 「2」は *保証エレメント*のセット中の *第2エレメント*であることを示す。
 - 「C」はそのコンポーネントの中の *内容・提示エレメント*のセット中の *エレメント*であることを示す。

SFR及びSARはコンポーネントレベルによって選択される：コンポーネントが含まれているならば、そのコンポーネントの中のすべての定義されたエレメントが、PPまたはSTに含まれなければならない。ITセキュリティ要件を選択する過程に影響をもつので、コンポーネント間の *関係*には二つの種別があることを覚えておかなければならない。 (161)

- a) ファミリの中のコンポーネントは *階層関係*になっているかもしれない。これは、あるコンポーネントがそのファミリの中の別のコンポーネントによって特定されたすべての要件エレメントを含むことを示している。例えば、FAU_STG.4はFAU_STG.3の上位階層である。なぜならば、後者で定義されたすべての機能エレメントは前者にも含まれている。しかしながら、FAU_STG.4はFAU_STG.1の上位階層ではない。それゆえ、同じPPまたはSTで両方のコンポーネントを含む可能性がある。
- b) コンポーネントは他のファミリのコンポーネントによって *依存性*を定義されているかもしれない。例えば、FIA_UAU.1(利用者が主張する識別情報の認証を要求する)は、FIA_UID.1(利用者が識別されることを要求する)に依存性を持つ。依存性が脅威とセキュリティ対策方針に関連していないことを示すことができなければ、これらのコンポーネントはPPまたはSTに含まれなければならない。

6.2 PPまたはSTにおいてセキュリティ機能要件の特定のしかた

6.2.1 セキュリティ機能要件をどのように選択すべきか？

識別されたセキュリティ関連事項に応じてTOEに対するセキュリティ対策方針を定義し終わって、次のステップとしてこれらセキュリティ対策方針がどのように満たされるかを詳しく述べる必要がある。これは上述のとおりコンポーネントレベルで選択されるSFRの適切なセットを選択することによって行われる。もちろん、TOEに対するセキュリティ対策方針にとって適切な事前に定義された機能パッケージが使用できれば、SFRを選択する過程は著しく容易となるだろう。(10章参照) (162)

PPまたはSTのためのSFRの選択過程には、いくつかの段階がある。選択過程を考慮すれば、次のSFRの二つの種別を区別するのに有用である。 (163)

- a) *主*SFR：TOEに対する識別されたセキュリティ対策方針を*直接*満たす。
- b) *補助的*SFR：TOEに対するセキュリティ対策方針を*直接*は満たさない。しかしながら*主*SFRへサポートを提供する。したがって、*間接的な*助力はTOEに対する適切なセキュリティ対策方針を満足する。

ISO/IEC 15408がSFRのこれら2つの種別を*明示的には*区別しないが、そのような区別は、機能コンポーネント間の依存性、及びSFR間の相互サポートの実証のようなことで*暗に*考慮される。それゆえ、PPまたはSTにおいて、SFRを*主*であるか*補助的*であるかに明示的に分類することが必要でないが、PPまたはSTの根拠を書くようになるときにSFRのこれらふたつのタイプがあることを認識しておくことはたいへん有益である。 (164)

このように、SFRの選択過程の最初の段階は、TOEに対する各々のセキュリティ対策方針を直接満足する*主*SFRを識別することである。*主*SFRの完全なセットが確立されたら、次の段階として反復過程を続けることによって、*補助的*SFRの完全なセットが識別される。上述のように、すべてのSFR(*主*または*補助的*のどちらか)は、可能ならば、[15408-2]から適切な機能コンポーネントを使用して表現されるべきである。附属書Bは、どの機能コンポーネントが一般的なセキュリティ機能要件を表現するために使用されるべきかを識別するガイダンスを提供する。[15408-2]から機能コンポーネントを選択するとき、コンポーネントが適切かどうか、及びどのように解釈されるかについて、[15408-2]の附属書に含まれるガイダンスも参考にすべきである。 (165)

SFRのこれら二つの種別の関係を次の図4に示す。この関係はPPまたはSTの根拠に関係があり、*とりわけ*SFR間の相互サポートの実証に要求されることに気付くだろう。(8.3.4節参照)これは、TOEに対するセキュリティ対策方針が満たされることを保証するのを助ける上で、*補助的*SFRによって提供されたサポートの性質の説明を提供することを伴うだろう。 (166)

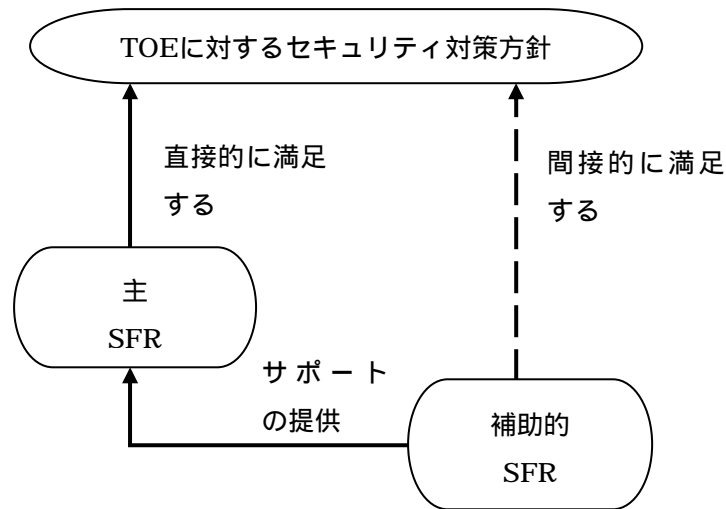


図4 - 主及び補助的SFRの役割

補助的SFRの完全なセットを識別するときに含まれる三つの段階がある。 (167)

- a) すべての主SFRの依存性(関係のある機能コンポーネントに対し[15408-2]で定義されている)を満足するために(適切であると考えられるならば)必要とされる追加のSFRの識別。これは、この段階で識別される補助的SFRのあらゆる依存性を含んでいる。
- b) TOEに対するセキュリティ対策方針が達成されることを保証するのに必要である追加のSFRの識別。機能を最初に打ち破る複合攻撃から主SFRを防御するのに必要とされるSFRを含むだろう。それによって機能が対抗しようとする脅威にあたる。
- c) 第二及び第三の段階で選択されるそれら補助的SFRの依存性を満足するために(適切であると考えられるならば)必要とされる追加のSFRの識別。

[15408-2]で識別された依存性を満足するための補助的SFRの識別は、反復過程になりそうである。

例えば： (168)

- a) 切迫したセキュリティ侵害を示しているイベントの検出への特定の反応を提供することをTOEに要求するセキュリティ対策方針を、PPまたはSTが含むと仮定する。これは、FAU_ARP.1(セキュリティアラーム)コンポーネントに基づく主SFRを含むことになる。
- b) [15408-2]によれば、FAU_ARP.1は、補助的SFRとして含まれるべきであるFAU_SAA.1(侵害の可能性分析)に依存性を持つ。
- c) FAU_SAA.1は、FAU_GEN.1(監査データ生成)に依存性を持つ。

- d) FAU_GEN.1は、FPT_STM.1(高信頼タイムスタンプ)に依存性を持つ。
- e) FPT_STM.1は、追加の機能コンポーネントを要求しない。

なぜ関係するSFRがセキュリティ対策方針を満足するために必要とされない(したがってセキュリティ関連事項に対応する)のかを説明することで、いくつかの依存性が「満たされない」で残ることを、ISO/IEC 15408は許すということを注意すべきである。 (169)

依存性は、一貫したやり方で適用されるべきである。例えば、FAU_ARP.1の場合では、一貫性は要件の性質によって保証される(FAU_ARP.1は、FAU_SAA.1.2を適用することによって定義されるセキュリティ侵害の可能性の予想に依存する)。 (170)

他のコンポーネントに対しては、一貫性はさらに難しいものとなるかもしれない。例えば、FDP_ACC.1の場合は、PPまたはSTが関係する特有のアクセス制御SFPを識別するだろう。FDP_ACF.1に対するFDP_ACC.1の依存性を満たす際、FDP_ACF.1はFDP_ACC.1で使われたのと同じアクセス制御SFPに適用されることを保証しなければならない。繰返し操作が異なるアクセス制御SFPのためのFDP_ACC.1に適用されるならば、FDP_ACC.1の依存性はそれぞれそのようなアクセス制御SFPに関して満たされる必要があるだろう。 (171)

追加の補助的SFR(すなわち、それらは[15408-2]において依存性として識別されない)の識別は、TOEに対するセキュリティ対策方針の達成をサポートするのに必要であると考えられるすべての他SFRを識別することを必要とする。そのようなSFRは、攻撃に利用できる選択肢や機会を減らすことによって、または攻撃者が成功裏な攻撃を仕掛けるために持たなければならない資源や専門的技術のレベルを上げることによって、典型的にサポートを提供するだろう。セキュリティ関連事項及びセキュリティ対策方針の観点から、以下は考慮されなければならない： (172)

- a) [15408-2]の同じクラスの中から関係するコンポーネントに基づくSFR。例えばコンポーネントFAU_GEN.1(監査データ生成)が含まれるならば、生成されたデータを格納するセキュアな監査証跡を生成し維持する必要性(FAU_STGファミリから一つ以上の機能コンポーネントを要求する)、及び生成された監査データをレビューするツールの必要性(FAU_SARファミリから一つ以上の機能コンポーネントを要求する)を含むかもしれない。または、生成されたデータは、レビューのために別のシステムにエクスポートされるかもしれない。

[【ISO/IEC JTC 1/SC 27 N3816改訂情報】：段落173、b\)は以下に示すとおり機密性に関する記述が追加される。](#)

- b) FPT(TOEセキュリティ機能の保護)クラスの中から関係するコンポーネントに基づくSFR。そのようなSFRは、一般的に他のSFRが依存するTSFまたはTSFデータの完全性及び/または可用性を保護するだろう、とはいえそれらはそれらの機密性も保護することができる。FPT_AMT.1(抽象マシンテスト)及びFPT_SEP(ドメイン分離)ファミリからのコンポーネントを含める例では、TSFの故障、破壊、改変(故意の手段によるかもしれない)ということに対抗してTSF

を保護するための識別された必要性があるセキュリティ対策方針をサポートすることが要求されるかもしれない。

- c) FMT(セキュリティ管理)クラスの中から関係するコンポーネントに基づくSFR。これらは、あらゆる必須の補助的セキュリティ管理SFRを特定するために使われるだろう。この一つの例は、セキュリティ属性の取消しに対応するFMT_REV.1だろう。そしてそれは、セキュリティ属性を取り扱うSFRが含まれるところに関係すると考えられるかもしれない。(例えば、アクセス制御)

これら補助的SFRの選択は、常にセキュリティ対策方針に鑑みて、特に、すべてが相互にサポートし、完全なものとされ、効果的である形式のSFRのセットで終わる必要性を考慮して行わなければならない。それゆえ、PPまたはSTの根拠の構築過程は、この選択過程への重要な影響を持っているかもしれない。セキュリティ対策方針の達成に必要とされない補助的SFRを含めることを避けるよう強く忠告する。なぜならば、次に示されるようなPPまたはSTの許容性を制限するだけである：

(173)

- a) いくつかのTOEはそのようなSFRを満たすことができないかもしれない。
- b) SFRの数を増やすことは、評価におけるコスト及び不必要な要件の維持を増大させるだろう。

PPまたはSTが、土台として関連したPPを使用して構築されているならば、SFRの選択のための過程はかなり簡素化されるべきである。構築されたPPまたはSTには、TOEセキュリティ環境及びまたはセキュリティ対策方針間のすべての違いを考慮して、別のSFRを適切に含めるべきである。

(174)

6.2.2 セキュリティ機能要件の操作の実行のしかた

6.1節で述べたとおり([15408-2] 2.1.4副項参照)、いくつかの機能コンポーネントは、PPまたはSTに適切にセキュリティ要件を修整するためにPPまたはSTの作成者に要求する許可された操作を含んでいる。これらの操作を次に示す：

(175)

- a) *割付*、識別されたパラメタの特定が可能。
- b) *繰返し*、異なる要件を述べるために同一の機能コンポーネントを複数回使うことが可能。
- c) *選択*、与えられたリストの中から一つ以上のエレメントの特定が可能。
- d) *詳細化*、セキュリティ要件の詳細の追加が可能。それによって、他のSFRへの新たな依存性をなんら導入することなく、受入れられる解決策のセットを制限する。

繰返し

繰返し操作は、[15408-2]の多くの異なる機能コンポーネントによって依存性として呼び出されたFMT(セキュリティ管理)クラスのコンポーネントを使ったSFRを述べることがしばしば必要になる。そのような依存性を満足させるために、割付及び選択操作が違うやり方で行われた同一のコンポーネントを使うことが典型的に必要なものであるだろう。例えば、FMT_MSA.1は、セキュリティ属性の異なる種別の管理に関連する別のSFRが定義する回数分繰返しされるかもしれない。同様に、TOEが異なるアクセス制御方針(例えば、裁量アクセス制御(Discretionary Access Control : DAC)及び役割によるアクセス制御(Role Based Access Control : RBAC))の実施を要求された場合には、FDP_ACC及びFDP_ACFファミリからコンポーネントを複数使用することが望ましいだろう。(176)

PPまたはSTの明解性が高められる(例えば、複雑で扱いにくいSFRをはっきり認識できて管理できる機能要件に分解すること)という繰返し操作を使うことが推奨される。しかしながら、繰返し操作の使用は、6.2.8節に見られるようにPPまたはSTにSFRを提示するときに、他の潜在する問題を引き起こす。(177)

PPまたはSTに含めたSFR各々について、次のことができているかどうかの判断をする必要がある：(178)

- a) SFRを表現するために使用した機能コンポーネントに含まれるすべての*割付*または*選択*を完了する。
- b) SFRの必要な*詳細化*を特定する。

割付及び選択

選択では、識別されたパラメタの値が少なくとも一つは存在するのに対して、割付では、パラメタの値が一つもなくなる可能性もある。PPで割付または選択操作を完了している場合は、機能コンポーネントがセキュリティ対策方針を満足するために修整されるという(詳細化の可能性以外の)ST作成者による判断を除去される。すなわち、(操作が関係する範囲では)ST作成者によって「定義される」局面はない。(179)

一般に、個々の*割付*または*選択*は、PPまたはSTの作成者による完了を要求するだろう。操作の完了に条件を付け過ぎること、または詳細すぎることは、PPまたはSTとの一致を宣言できるTOEの数を不当に制限するかもしれない。操作完了のバランスは、PPにとって必要な次のことに基づく：(180)

- a) 作成者の要件の完全なセット；
- b) *実装独立*；
- c) 対策方針を満たすことの十分に詳細な実証。

それゆえ、セキュリティ対策方針を満たすために必要とされる程度まで割付及び選択の操作を完了することが必要である。重要なテストは、セキュリティ要件根拠を構築しているときに行われ

るだろう：セキュリティ対策方針を満たすためにITセキュリティ要件が適していることの実証を提示する論拠は、SFRの中で特定されていない詳細な内容に依存すべきではない。例えば、FDP_ACF.1に基づくアクセス制御SFRの場合は、アクセス制御の規則が、関係する(アクセス制御)セキュリティ対策方針を満たすことを意図するOSPですでに定義されているならば、アクセス制御の規則の特定を完全にST作成者に任せたまにすることが適切かどうかをよく考えた方が良いかも知れない。(181)

上記の問題を解決するために使えそうな一つの技術は、操作の完了を部分的にすることである。このアプローチを採用することによって、ST作成者に最大の柔軟性を与えることができ、同時にTOEに対するセキュリティ対策方針とは一貫しないような割付または選択の恐れを排除できる。(182)

例えば、次のSFR(FAU_STG.4.1に基づいた)において、選択操作は、PP作成者がTOEに対するセキュリティ対策方針に矛盾すると判断した「監査対象事象の無視」をオプションの選択から排除することによって部分的に完了させられる。それゆえ、SFRはST作成者に二つの(三つではなく)許容できるオプションの選択を提供する：(183)

TSFは、監査証跡が満杯になった場合、[選択：特権を持つ許可利用者に関わるもの以外の監査対象事象の抑止、最も古くに格納された監査記録への上書き]及び[割付：監査格納失敗時にとられるその他のアクション]を行わねばならない。

割付では、ST作成者が環境に対して容認されるオプションのセットを作ることができる選択肢を、PP作成者が制限することができる。この場合、PP作成者は、それを正当な根拠のある選択肢を含む選択操作に換えることによって割付操作を完了することができる。その結果、その選択肢はST作成者によって完了される。(184)

一般的な原則として、それが提示するオプションのセットがオリジナルの機能コンポーネントによって許されているオプションのサブセットならば、部分的に完了された選択操作は有効である。同様に、割付を完了するための許可された値がオリジナルの機能コンポーネントに関しても有効な割付であるならば、部分的に完了された割付は有効である。どんな理由でもこれらの条件が満たされないならば、それは異なる割付または選択操作を持つ拡張機能コンポーネントになっている。(185)

割付及び選択操作を完了することは、単純明快である。割付の場合は、パラメタが曖昧でなく特定されていることを保証する必要があるだけである。選択の場合には、TOEに対するセキュリティ対策方針の考慮に基づいて、適切な事項を選択する必要があるだけである。しかしながら、もし、疑念があれば、[15408-2]の附属書として与えられるガイダンスを参考にすべきである。(186)

割付または選択がPPにおいて実行された場合には、特定されたテキストを強調することが必須である(これは、読者や、特にISO/IEC 15408との一致をチェックするPP評価者の助けになる)。例えば、強調の一つの方法は、イタリック体を使うことである。したがって、FMT_SAE.1.1は次のように提示される：(187)

TSFは、利用者パスワードに対する有効期限の時間を特定する能力を、許可された

管理者に制限しなければならない。

操作が未完了のままにされるならば、ST作成者がその操作を完了することは必須である。 (188)

どんな未完了の(または部分的に完了された)操作にでも、適切な場合、完了すべき操作のしかたを(例えば、アプリケーションノートの形式で)、ST作成者を目標に、説明を付け加えるべきである。それは、細部を特定することはST作成者の責務であることを明確にすることの助けになるかもしれない。例えば、FDP_RIP.1.1は、PPにおいて次のように特定させることができる： (189)

TSFは、以下のオブジェクトへの資源の割当てにおいて、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない：[割付：ST作成者によって特定されたオブジェクトのリスト]。

詳細化

詳細化の操作は、あらゆる機能コンポーネントのエLEMENTで実行することができ、そして許容される実装表現のセットをある程度制限はするが、テキストの中で特定されたものに対してどんな新しい要件も賦課することなく追加の技術的な細部を特定するのに用いられる。詳細化された要件を満たすことが、その詳細化されていない要件も満たすということの意味していれば、詳細化は許容される。詳細化の使用は、以下の状況において適切である： (190)

- a) PPが、適切な[15408-2]のコンポーネントの中に含まれない組織の方針情報のような、付加的な技術上の詳細を持つ組織によって記述されている場合；
- b) 考慮すべきTOEの種別に対して、その可能性を除去するように詳細化されない限り(例えば相互運用性の観点から)、選択された機能コンポーネントが無意味な実装を許してしまうか、その他不適切なものになる場合；
- c) SFRの読みやすさが、改善される場合(6.2.8節参照)。

割付及び選択操作と同様に、読者(特にPP評価者)の助けとなるために詳細化されたテキストを強調することを推奨する。 (191)

詳細化操作の使用例を次に示す。(FMT_MTD.3.1に基づく) (192)

TSFは、TSFデータとしてセキュアな値だけが受け入れられることを保証しなければならない。

詳細化：TSFは、TOEによって実施される最小限のパスワード長が、少なくとも6つのキャラクタの値で構成されることを保証しなければならない。

SFRを明確にする助けとなる詳細化操作の使用は、6.2.8節で論じられる。 (193)

6.2.3 監査要件はどのように特定すべきか？

PPまたはSTが監査要件(すなわちFAU_GEN.1に基づく)を含むならば、ISO/IEC 15408は、監査

の対象とされなければならない事象の最小限のセット、及びPPまたはSTに含まれるすべての他の機能要件の考慮を通して特定され、記録されなければならない最小限の情報を要求する。 (194)

この選択は、以下を含むいくつかの要因に依存する： (195)

- a) OSPによって定義されるセキュリティ監査上のあらゆるセキュリティ方針要件；
- b) セキュリティ対策方針を達成するために監査することの重要性；
- c) セキュリティ対策方針と、潜在的な事象、及びそれらの特性との関連性；
- d) コスト/利益分析。

例えば、TOEが悪意のある利用者またはハッカーの行動から守るつもりであるならば、おそらく、ログインやアクセス制御の侵害のような事象には、PPまたはSTがそういうSFRを含むことによって監査対象になることが必要である。しかしながら、管理機能の使用に関連する事象は、管理者が信用される(またはされなければならない)程度に依存するため、監査対象に必要でないかもしれない。管理者が信用できることは、前提条件として述べられよう。 (196)

コスト/利益分析の懸案は、次のような論点にある： (197)

- a) 情報収集の利益は、性能への影響に見合ったものであるか？
- b) 情報が収集されるならば、管理者はデータを効果的に分析する十分な資源(例えばツールによるサポート)を持つか？
- c) 収集されたデータの管理または蓄積のコストはどの程度か？

ISO/IEC 15408は監査するためのあらかじめ定義された3つのレベル、すなわち*最小*、*基本*、*詳細*で識別される([15408-2]、2.1.2.5副項、11ページ)：そのようなレベルごとに対して、[15408-2]では、PPまたはSTに含まれる機能コンポーネントに基づいて、記録される最小限の情報とともに、どの事象が監査対象(最小として)とされるべきであるかと言っている([15408-2] C.2副項も参照)。これら3つのレベルは、次のようにおおざっぱに特徴付けることができる： (198)

- a) *最小*レベルは、監査対象にすべき与えられた機能コンポーネントと結び付けられる事象または操作のいくつか定義されたサブセットのみを通常要求する。このサブセットは、事象の重要な種別またはもっとも注意すべきものであると一般に定義される。
- b) *基本*レベルは、監査対象である与えられた機能コンポーネントと関連付けられる事象またはすべての操作を通常要求する。例えば、成功及び不成功のログインの試み。
- c) *詳細*レベルは、記録される重要な追加の情報を要求することによって、*基本*レベルとは一般に異なる。このレベルは、生成された監査データの総数が小さい

ものであると予想されるもの、またはデータが洗練された監査分析ツールまたは侵入検出装置によって分析が行えるものに、適切しそうなだけである。

もし、これらのレベルのどれもが適切でなければ、特定されていないレベルを選択すべきであり、FAU_GEN.1.1cにおいて明示的にすべての要求される監査対象イベントをリストすべきである。例えば、ガイドとして最小レベルを使うかもしれないが、操作または事象の異なるサブセットはセキュリティ対策方針によりいっそう関係するので、特定の場合において最小の要件から逸脱することを選んで良い。例えば、PPまたはSTにFDP_ACF.1が含まれるならば、成功した試み([15408-2]が最小レベルに対して要求していること)よりも不成功となったアクセスの試みを監査対象にすべきであることを考慮した方が良い。(199)

使用された各々の機能コンポーネントを順に詳しく調査することによって、評価対象事象のリストにまとめる必要がある：最小、基本、詳細を事前に定義されたレベルの場合には、コンポーネントの各々のファミリに含まれる監査の項で明示的に識別されている。記録すべき事象と(適切ならば)付加情報を識別する表を構成することが推奨される。その表はFAU_GEN.1.1及びFAU_GEN.1.2によって適切に参照することができる。(200)

6.2.4 管理要件をどのように特定すべきか？

コンポーネントの各々のファミリに含まれる管理の項において、[15408-2]はコンポーネントに対して考慮されるべき管理アクティビティのリストを識別している。これは、FMT(セキュリティ管理)クラスから個々のコンポーネントを含めることの必要性を示唆することができる。しかしながら、この項は参考であると意図されることに注意することが重要である。それゆえ、PPまたはSTにおいて個々の管理コンポーネントを含めないことのどんな決定も正当化する必要性はない(もちろん、[15408-2]の中で依存性の項に明確に識別されている場合を除いて)。(201)

一般的に言って、機能コンポーネントが、管理及び制御される必要があるかもしれない設定可能なTSFデータを参照し、またはその存在を暗に示す場合、管理アクティビティが識別される可能性がある。例えば、そのようなデータを改変する能力がTOEの管理者に限定されていない場合、TOEに対するセキュリティ対策方針が蝕まれるかもしれない。それゆえ、補助的SFRを定義し、TOEに対するセキュリティ対策方針を満たすこと、及びSFRが全体として相互サポートすることを保証するために、FMTコンポーネントはしばしば含まれる。(8.3.1及び8.3.4節参照)(202)

このクラスから機能コンポーネントを選ぶときには、[15408-2]附属書Hで与えられるFMTクラスのガイダンスを参考にすべきである。(203)

6.2.5 どのようにSOFを特定すべきか？

ISO/IEC 15408は、PPまたはST([15408-1]副項C.2も参照)において識別される確率的または順列的メカニズム(例えば、パスワードやハッシュ関数)によって実現される全てのITセキュリティ機能のためのSOF(機能強度)の3つの定義済みレベル、すなわち基本、中位、または高位([15408-3])を識別する。レベルは次のとおり表される：(204)

- a) 低い攻撃能力を有する攻撃者による偶発的なTOEセキュリティ侵害に対して十分な抵抗力を提供する機能
- b) 中程度の攻撃能力を有する攻撃者による直接的または意図的なTOEセキュリティ侵害に対して十分な抵抗力を提供する機能
- c) 高い攻撃能力を有する攻撃者による系統的または組織的なTOEセキュリティ侵害に対して十分な抵抗力を提供する機能

選択するレベルは、脅威エージェントに関係するいくつかの要因に基づいている： (205)

- a) 所要時間
- b) 専門知識
- c) TOEの知識
- d) TOEへのアクセス
- e) 機器

これらの要因に対する値は、脅威のステートメントにおいて識別された脅威エージェントの攻撃能力の分析から引き出される。これらの要因の特性は、完全なリスク分析において引き出されなければならない。 (206)

いくつかの確率的または順列的メカニズムに対して、より一般的な*基本*、*中位*、または*高位*のステートメントの代わりにオプションとして明示的な数値尺度が提供することができる。 (207)

6.2.6 PPから引用するSFRはどのように特定すべきか？

STが一つまたは複数のPPへの準拠を主張する場合には、SFRはPPによって完全にまたは大部分が特定されることになる。このような場合には、ST作成者は、PP機能要件を完全に(すべてのテキストが一箇所にあることを保証するために)特定するか、もしくは単にPPへの参照を付けてPPとは異なるSFRを特定するかのどちらかを決定しなくてはならない。 (208)

一般に、後者のアプローチは、STを簡素化することになるので推奨される。STの読者は、SFRよりもITセキュリティ機能に関心がありそうである。これはTOEの評価者を含む(設計、テスト証拠資料及びガイダンス文書のような評価証拠の中身は、SFRよりもTOE要約仕様におけるITセキュリティ機能に、より容易に関連付けられそうなので)。STにおけるSFRを特定することの主要な目的は、関係のあるPP、及び[15408-2]で定義されているようなSFRへの追跡性を実証することができることである。STの中にセキュリティ機能性の二つの仕様があることで、読者を混乱させないようにするために、SFRのステートメントを附属書へゆだねる場合が確かにある。 (209)

しかしながら、PPにおけるいくつかのSFRは、ST作成者にゆだねられた操作(割付や選択のような)を持つことができることに注意すべきである。そのような場合においては、完了された操作が適している活字(例えば、イタリックの使用)によって強調されるとともに、SFRの全体が特定され

ることが推奨される。あらゆる必要な説明が、同じ活字を使って書き加えられるべきである。そんなアプローチは、STの読者(特にST評価者)に対して、どの操作がどのようなやり方で実行されたかをより読みやすくする。それはST根拠の構築もまた容易にするだろう。(8.3.6節参照) (210)

6.2.7 PPにないSFRはどのように特定すべきか？

いくつかの場合においては、対応するPPの中に含まれていないSFRをSTの中で特定することが必要となる。これは、次のことが必要となるかもしれない： (211)

- a) TOEが準拠することを主張するために使用できる適切なPPがない；
- b) PPによって要求されるものに追加される機能要件または保証要件を持つことによって得られる利益が、発生する追加コストを正当化するのに十分であることを、スポンサーは考慮する。

このような場合において、SFRの特定へのアプローチは、前章に記述されたものと同じである。SFRがPPによって要求されるそれらに加えて特定される場合には、ST作成者はそれらがPP中のSFRと相反しないことを保証しなければならない(ST根拠はそのような不一致が生じないことを実証することが必要であろう：8章参照)。 (212)

6.2.8 [15408-2]に含まれないSFRはPPまたはSTにおいてどのように特定すべきか？

PPまたはSTの作成者が[15408-2]で定義された適切な機能コンポーネントがない機能要件を含めたいならば、結果として生じるSFRは、表現のモデルとして[15408-2]のコンポーネントを使用することで特定されるべきであるということをISO/IEC 15408は要求する。 (213)

使用する[15408-2]の中に適切な機能コンポーネントがあるかどうかという判断は、これがその内容を高度に熟知していることを要求するゆえに、困難なものになる傾向がある。共通のセキュリティ機能要件を表現するために適切な機能コンポーネントを識別する附属書Bにあるガイダンスを参考にすることが推奨される。要望されるSFRは、詳細化操作または容認される割付や選択操作の適切な適用を通して獲得されることができるときはしばしばある。しかしながら、もし希望するSFRへ容易に導かれるものでないならば、SFRをその機能コンポーネントに「無理やり押し込もう」としないことを推奨する。すなわちそのことは、意味または意図が読者によってすぐに明瞭に理解されることができないSFRが入ってしまい、またはそのSFRには(不適切なコンポーネントを使ってしまうことによって)不適切な依存性を導入することになり、その依存性を除去するための理屈をつけなければならなくなる。 (214)

表現のモデルとして[15408-2]の機能コンポーネントを使用する新しいSFRを特定するには、次のようなことが必要となる： (215)

- a) [15408-2]のコンポーネントとして抽象度の類似したレベルでSFRを定義すること；
- b) [15408-2]のコンポーネントに類似したスタイル及び表現法を使うこと；

- c) [15408-2]の中と同じようなコンポーネントに対するトポロジー及び命名体系のアプローチを使うこと。

新しいSFRは既存のクラスまたはファミリの他のものの類似性を知ることは、その新しさの度合いに境界をつけるのに役立つ、クラスまたはファミリに出てくる共通の概念に対する特定の言い回しを使うことにも役立つかもしれない。 (216)

[15408-2]における機能コンポーネントの表現のスタイルの独特な特徴は、次のものを含む： (217)

- a) ほとんどの機能要件は、「*TSFは、～しなければならない(The TSF shall ~)*」、または「*TSFは、～できなければならない(The TSF shall be able to ~)*」という文章になっており、動詞として次のものが使用される、許可する(*allow*)、検出する(*detect*)、実施する(*enforce*)、保証する(*ensure*)、制限する(*limit*)、監視する(*monitor*)、許可する(*permit*)、防止する(*prevent*)、保護する(*protect*)、提供する(*provide*)、制限する(*restrict*)；
- b) セキュリティ属性や許可された利用者というような標準の用語の使用；
- c) 各々のエレメントは、自立する傾向があり、前のエレメントを参照することなく理解することができる；
- d) 各々のセキュリティ要件は評価対象でなければならない。すなわち、要件がTOEによって満たされるかどうかを決定することができなければならない。

明示的に述べられたSFRを構成するとき、SFRは次のことも考慮すべきである。 (218)

- a) ST作成者によって完成されるあらゆる割付または選択操作を含むべきかどうか；
- b) PPまたはSTに含まなければならない、他のSFRへのあらゆる依存性を含んでいるかどうか；
- c) 監査対象となるべきあらゆる事象を記述しているかどうか、もしそうならば、その事象に対して何の情報が記録されるべきか；
- d) セキュリティ管理の対象となるものを含んでいるかどうか。例えば、管理が必要なセキュリティ属性に頼っている。

[15408-2]に含まれていない、既存のISO/IEC 15408の機能コンポーネントのセットと十分に違って、それを十分に強化するよくできたSFRをあなたが持つと信じるならば、その文書の次の改版に含めるためにそのSFRを提出することを推奨する。 (219)

ISO/IEC 15408は、[15408-2]を参照することなくSTの中で明示的にSFRを記述することをST作成者に許可する。6.2.7節で与えられたガイダンスが適用される。しかしながら、SFRがそのSTの中での使用を意図されるだけ(すなわち、他のPP、STや機能パッケージの中でそのコンポーネ

ントを再利用する意志がない)ならば、この方法で構成されたSFRに対する割付や選択のようなISO/IEC 15408の操作を特定することは、必要ではないかもしれないということに注意すべきである。(220)

[15408-2]に含まれないSFRの命名は、標準と同様の形式である[15408-2]のトポロジー及び命名規約を使うべきである。拡張コンポーネントは、機能のために「F」、次に適切なクラス及びファミリの名称、次にコンポーネント番号を使うべきである。したがって、現在のクラスを基本とした拡張コンポーネントは、適切な場所に挿入することができる。拡張コンポーネントが現在のクラスと関係がない場合、例えばコンポーネント「EX」のクラスを作ることやコンポーネント名の最後に「EX」を追加することによって、拡張セキュリティ要件が新しいものであると明確にできる命名は容認可能である。拡張コンポーネントがどのように示されるかは、PPまたはSTのアプリケーションノートの中で説明するべきである。使用した命名規約は[15408-2]と競合しないようにすることを注意するべきである。(221)

6.2.9 SFRはどのように提示されるべきか？

ISO/IEC 15408の要件に明白に準拠するSFRのセットを書くことは、(もちろん)PPまたはST作成者の唯一のねらいではない。セキュリティ要件が何を意味するのか一般の読者に理解できるように、SFRを提示し表す最も良い方法についても考慮すべきである。ISO/IEC 15408への準拠を損なうことなく、読みやすさを高めることができるいくつかのステップがある。(222)

第一に、あなたのPPまたはSTに適切である見出しのもとでSFRをグループ化する：[15408-2]の中で使われているクラス、ファミリ、コンポーネントの見出しを採用することにとらわれる必要はない。(223)

第二に、あなたのPPまたはSTの中でSFRにラベルを付けるために、[15408-2]で使われている機能エレメントのラベルシステムを採用することにとらわれる必要はない。そこにおいて、SFRの対応する[15408-2]の関係する機能コンポーネントにマッピングが実証されているならば(例えば、附属書において)、あなた自身のラベルシステム(より意味のあるラベルをもたらす)を採用することは、申し分なく許容される。確かに、そのようなアプローチでは、PPまたはSTが、何度も呼び出される機能コンポーネントを含む場合には非常に望ましくなりそうに思われる。これは、他方が、一意性のあるラベルを持たないSFRを持つからである：SFRのための一意性のあるラベルの欠如は、セキュリティ要件根拠を構成するときに重要な問題を引き起こす。(224)

第三に、詳細化操作の賢明な使用法は、TOEの種別に関係する、より特定の述語で一般的な用語(セキュリティ属性のような)に代用することによって、もしくはセキュリティ機能性を記述することによって、SFRの読みやすさを改善することができる。例えば、SFRはFMT_MSA.3.1を基にして次のようになる：(225)

TSFは、オブジェクトの許可として、制限的デフォルト値を与えるDAC方針を実施しなければならない。

この例においては、一般的な「そのSFPを実施するために使われるセキュリティ属性」をその方

針に特有の「オブジェクトの許可」と置き換えて、詳細化は使用されている。(226)

あらゆる詳細化操作のそのような使用は、PPまたはSTの根拠の中で明確に強調され、説明されるべきである(PPまたはSTの評価をサポートするために)。(227)

付属書Fに提示される作業例は、このアプローチの適用を説明する。(228)

6.3 PPまたはSTにおける保証要件の特定のしかた

6.3.1 セキュリティ保証要件をどのように選択すべきか？

保証要件の選択は、いくつかの要素のバランスをとることを要求するだろう。(229)

- a) 保護されるべき資産の価値とそれら資産を危険にさらすことに対するわかっているリスク；
- b) 技術上の実現可能性；
- c) 開発と評価コストの見込み；
- d) TOEの開発と評価に要求される必要な期間；
- e) 明確になっている市場要件(製品の場合)；
- f) 保証コンポーネントに対する機能コンポーネントのあらゆる識別された依存性。

保護される資産の価値が高くなればなるほど、それら資産へのリスクが大きくなればなるほど、それら資産の保護に使用されたセキュリティ機能に要求される保証レベルはより高くなる。これは、セキュリティ対策方針のステートメントの中に反映されるべきである。組織は、それらの資産に対するリスクを許容できるレベルまで引き下げることが保証することが必要な保証のレベルを決定するために、自分自身の方針と規則を定義することができる。これは、その組織の内部で使用される製品における要求される保証のレベルを定義することになるかもしれない。(230)

コスト及び期間のような他の要素は、実行上実際に達成できる保証のレベルに対する制約になりがちである。技術上の実現可能性は、特定の保証コンポーネントによって要求される証拠をもたらすことが実用的でないことを考慮する要素になる。これは、レガシーシステム(設計証拠資料が利用できない場合)、または理想的には高い保証レベルが要求されるが、しかし、容認される期間内で要求される準形式的または形式的証拠をもたらすことが、技術的に可能でない場合に大いに関係する。達成できる保証に実用上の制約がある場合はいつでも、達成できる最大の保証は理想よりも小さいということを受入れる必要があるだろう。そのようなリスクを受入れることは、セキュリティ対策方針のステートメントの中に、もう一度反映されるべきである。(231)

セキュリティ対策方針のステートメントは、SARに含まれるべき特定の保証要件の必要性もまた示すことができる。例えば：(232)

- a) TOEに対するセキュリティ対策方針は、高い攻撃能力を持つ攻撃者にTOEが抵抗すべきであると明言することができる。これは、実証されるそのような抵抗力を要求するAVA_VLA.4を含めることへのはっきりした指針となるだろう。
- b) セキュリティ対策方針は、隠れチャンネルが懸念されるものであることをさし示すことができ、その場合、実行される隠れチャンネル分析を要求するAVA_CCAファミリからコンポーネントを含むことが必要である。
- c) セキュリティ対策方針は、TOEのセキュリティが開発環境のセキュリティに決定的に依存していることを注記することができる。これは、開発環境のセキュリティが検査されることを保証するALC_DVSファミリからのコンポーネントをSARが含むべきであることを強く示唆するだろう。

SARの選択は、ISO/IEC 15408のEALのような、適切な保証パッケージ(10章参照)を単に選ぶだけの場合には、比較的容易なものになる。保証パッケージの定義と記述は、そのパッケージが、与えられたセキュリティ対策方針のステートメントに対して適切なものであるということを保証するよう考慮されるべきである(例えば、EALの場合においては、[15408-3] 6項を参照)。保証パッケージは、必要とされる保証のレベルを大まかに提供するが、セキュリティ対策方針に照らし合わせたとき、特定の領域が不足しているということがありえる。そのような場合、セキュリティ対策方針が満たされることを保証するために、追加保証要件(すなわち、そのパッケージが必須とするものに追加される要件)を含めることが適切であろう。 (233)

追加保証要件が特定される場合、PPまたはST作成者は保証コンポーネントの依存性が追加の要件に対して満足されることを保証するべきである。例えば、PPまたはSTがEAL3にAVA_VLA.2を追加するならば、EAL3に含まれていないADV_LLD.1及びADV_IMP.1も追加するべきである。 (234)

6.3.2 セキュリティ保証要件の操作の実行のしかた

[15408-3] 2.1.4副項に示してあるように、割付及び選択操作は、[15408-3]に定義された保証コンポーネントには関係しない。しかし、次の操作は可能である： (235)

- a) 繰返し、同じ保証コンポーネントを複数使用することを許す；
- b) 詳細化、他のSARに如何なる新しい依存性を導入することなしに保証要件へ詳細の追加を許す。

実際には、繰返し操作は、TOEの異なる部分に適用する同じ保証コンポーネントに異なる詳細化を適用することが必要な場合、またはコンポジットTOEの異なる部分に対して保証要件の異なるセットをPPまたはSTが特定する場合にのみ使用されるだろう(9.2.4節参照)。後者の場合、コンポジットTOEの一箇所以上に適用する保証コンポーネント(詳細化されていなくても)に対して、繰返しは必要になるだろう。 (236)

SARの詳細化操作の使用は、次のことに使われよう： (237)

- a) 特定の開発ツール、方法論、ライフサイクルモデル、分析技法、表記法、特定の標準の厳守などの使用を必須とすることによって開発者アクションに制約を加える；
- b) 評価者アクションの実行に制約を加える。例えば、
 - ADV_IMP.1の場合、TOE実装表現のどの部分が検査されるサブセットの中に含まれるべきであるかを特定する。
 - AVA_VLA.1の場合、そのTOEに関連する状況において「明白」であると考えられる特定の既知の脆弱性を識別する。

6.3.3 [15408-3]に含まれないSARをPPまたはSTにおいてどのように特定すべきか？

PPまたはSTの作成者が[15408-3]で定義された適切な機能コンポーネントがないSARを含めたいならば、結果として生じるSARは、表現のモデルとして[15408-3]のコンポーネントを使用することで特定されるべきであるということをISO/IEC 15408は要求する。明示的に記述されたSARは、次のエレメントの定義を提供すべきである(詳細は[15408-3] 2.1.3.5副項を参照)： (238)

- a) 開発者アクション；
- b) 開発者が提供しなければならない証拠の内容・提示に対する要件；
- c) 評価者アクション。

[15408-3]の検査は、保証コンポーネントに関連するエレメントが次のように特徴付けられることを示している： (239)

- a) 開発者アクションエレメントは、開発者が実行しなければならないアクティビティ(一般的に評価証拠の提供)を表すことを意図する；
- b) 内容・提示エレメントは、開発者が提供しなければならない評価証拠の要求される内容と「質的な」側面を特徴づけることを意図する；
- c) 評価者アクションエレメントは二つの形式をとる
 - 最初の評価者アクションは、一般に次の定型句である
評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。
 - それ以外の評価者アクションエレメントは、評価者によってなされる独自の作業と判断に対するステートメントの形式を一般的にとる。

それゆえ、証拠の内容・提示に対するすべての要件は、明確及び曖昧さなく表現されるだけでなく、評価者によってなされた主観的な判定の要求も(可能な限り)避けるべきである。というより、SARは、評価者が判定に到達できるような明確な客観的基準を定義すべきである。客観的判定に

対する要件をサポートするために必要とされる、SARのあらゆる明確化に対するアプリケーションノートを提供することを考慮するべきである。(240)

明示的に記述されたSARは、[15408-3]のコンポーネントと同じような形式で特定されることを保証するために、各分離可能な要件は、個別の要件エレメントとして記述されることを保証するべきである([15408-3]、2.1.4副項、10ページ)。SARの言い回しを選択する場合、[15408-3]の中で厳密な方法で使用される、英語の一般的な語句に定義を与える[15408-3] 2.4副項も参考にするべきである。(241)

[15408-2]に含まれていない、既存のISO/IEC 15408の保証コンポーネントのセットと十分に違って、それを十分に強化する、よくできたSARをあなたが持つと信じるならば、その文書の次の改版に含めるためにそのSFRを提出することを推奨する。(242)

6.4 環境のセキュリティ要件

6.4.1 IT環境のセキュリティ要件

ISO/IEC 15408は、いかなるIT環境のセキュリティ要件もPPまたはSTに含まれることを要求している。例えば：(243)

- a) セキュアデータベース管理システム(DBMS)は、そのユーザの識別と認証を提供するために、そして、オペレーティングシステムの利用者が直接データベースファイルにアクセスすることにより、DBMSのアクセスコントロールをバイパスすることを防ぐために、下層のオペレーティングシステムに依存するかもしれない。
- b) スマートカードアプリケーションは、他のアプリケーションとの分離を提供することを下層のスマートカードのオペレーティングシステムに依存するかもしれないし、そしてICカード自身の耐改ざん特性に依存するかもしれない。

IT環境のセキュリティ要件は、TOEではなくIT環境によって満たされる、PPまたはSTの[15408-2]コンポーネントの依存性が識別されるところでもまた、特定されるかもしれない。(244)

IT環境のセキュリティ要件は、以下の点で環境の前提条件とは区別されるべきである：(245)

- a) 前提条件は、TOE評価に対して自明のものであり、セキュリティ関連事項の範囲を明確にするために定義されている。
- b) セキュリティ要件は、TOEがセキュリティ対策方針を満足する結果、セキュリティ関連事項に対応することを保証するために必要であり、それゆえ、何らかの点で検証されることが必要になる。

しかしながら、TOEセキュリティ要件との対比において、IT環境のセキュリティ要件は、IT環境

がそれに要求されるSFRを提供することが、要求される保証の程度まで確認されるといった意味では、(TOE評価においては)評価されない。TOE評価は一般に、IT環境がそれらのSFRを提供すると仮定するが、IT環境のセキュリティ要件のいくつかは、TOE評価の自然な成り行きとしてテストされるだろう。要求される保証のレベルは最終的には、要求されるセキュリティ機能性を提供するIT環境のコンポーネントの別の評価を通して、確立される必要がある。(246)

ISO/IEC 15408は、IT環境のセキュリティ要件は、TOEセキュリティ要件と同様に、可能な場合、ISO/IEC 15408機能及び保証コンポーネントを利用して特定されるべきであることを示唆(indicates)している。PPまたはSTは、それらのコンポーネントからの逸脱に対しては、正当化を含む必要がある。(247)

[15408-2]コンポーネントがIT環境の機能要件を表現するのに適切でない場合もあるかもしれない。例えば、PPの機能要件が[15408-2]で定義されるコンポーネントより抽象的なレベルで表現されることもありえる。このアプローチは、ST作成者に、これらの(実装独立の)上位レベル機能要件をどのように満たすかを選択する時点で、融通性を許すだろう。(248)

6.4.2 非IT環境のセキュリティ要件(オプション)

[15408-1] B.2.6及びC.2.6副項は、非IT環境のセキュリティ要件は、TOEの実装には直接関係しないため、PPまたはSTの正式な部分として要求されるべきではないと述べている。しかしながら、ISO/IEC 15408はそれらが、「実際には役に立つ」ことを認めている。(249)

非IT環境のセキュリティ要件は、その実施が簡単ではない非IT環境のセキュリティ対策方針がある場合か、根拠が非IT環境のセキュリティ対策方針の実現方法に明示的に依存する場合に、PPまたはSTで必要とされるだろう。後者のケースは、PP/STのITセキュリティ要件と関連する管理技法の間の詳細な協調が必要とされ、2つの種類の要件が同じようなレベルの抽象度であるような場合に現れる。(250)

非IT環境のセキュリティ対策方針からは明白でない非IT環境のセキュリティ要件が必要である場合、そしてそれら明白でない要件がPPに含まれていない場合、ITセキュリティ要件の適応性を実証することは実行不可能になるかもしれないことも、また留意されるべきである(8.3.1節参照)。(251)

非IT環境のセキュリティ要件をセキュリティ対策方針や前提条件のように扱うことにより、抽象レベルを混在させるよりむしろ、非IT環境のセキュリティ要件のために別のセクションを提供する方が望ましい。そのようなセクションは、特定の管理要件(例えば、種々の侵入検出アラームへの対応に必要な調査手続き)と同様に、特別な識別・認証メカニズム(例えば、パスワード)に利用される認証データの保護のようなトピックスをカバーするだろう。(252)

PPまたはSTで、既知の非IT環境のセキュリティ要件の明確な識別を提供することは、それらのセキュリティ要件が利用者証拠資料に確実に反映されることを保証することを助ける(AGDクラスからの適切な証拠資料要件がPPまたはSTに含まれていると仮定した場合)。(253)

7 TOE要約仕様

7.1 序説

この章は、STにおけるTOE要約仕様を特定するためのガイダンスを提供する(PPに同等の節はない)。(254)

[15408-1] C.2.7副項は、TOE要約仕様に次のことが含まれていることを要求する:(255)

- a) 識別されたSFRを満たすITセキュリティ機能の定義;
- b) オプションとして、ITセキュリティ機能を実装するために使用されるセキュリティメカニズムまたは技法への参照;
- c) 識別された保証要件を満たす保証手段の定義。

TOE要約仕様の主な部分を次の図5に示す。(256)

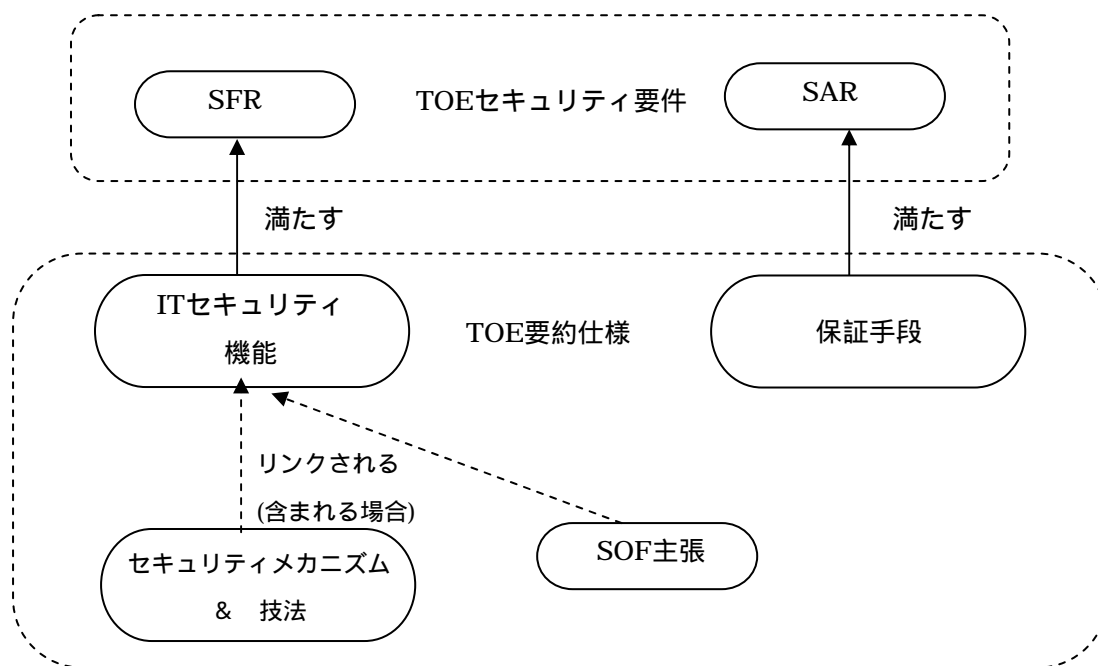


図5 – TOE要約仕様の内容

STのこの章の主な目的は、識別されたセキュリティ関連事項のTOE固有の解決策を特定する。TOEセキュリティ要件を満たすために定義されたセキュリティ機能と保証手段をTOEがどのように提供するかは上位レベルの記述であるべきであり、詳細な仕様であるべきではない。TOE要約仕様は、その結果この観点から書かれるべきである、すなわちTOEセキュリティ要件を満たし、

それによってセキュリティに関して満たすためTOEが何を提供するか定義する。 (257)

この節または、SFRと比較してTOEセキュリティ機能性を理解するSTの読者にとって理解するのがより容易にする方法で、ITセキュリティ機能を体系付け及び特定の機会をST作成者に提示する。特に: (258)

- a) ITセキュリティ機能は、セキュリティ関連事項に対応するためにTOEが実際に何を行うか強調するために体系付けることができる。
- b) ITセキュリティ機能は、TOE証拠資料をより綿密に反映するような方法で指定することができる、例えば適切にTOE固有の用語を使用することで。これは、STからTSF表現(例えば、設計証拠資料)及び開発者のテスト計画及び仕様まで、より明確な対応を容易にすることで、SFRよりも評価のために適しているベースラインを提供することでTOE評価の費用効果を改善することができる。可能な1つの手法は、いくつかのSFRに合致する単一のITセキュリティ機能を特定することができる。TOE設計及び実装の同一の下層メカニズムによってそれらのSFRが満たされることが知られている。これは、厳密さを失うことなしで、開発者が提供する必要がある表現対応の証拠の量を減らす利点を持つであろう。とはいえ、ST作成者はそれにもかかわらずそれらが満たすSFRまで容易にITセキュリティ機能がさかのぼれることを保証するべきである。
- c) TOE固有の用語は、(例えば)ITセキュリティ機能を設計または利用者または管理者のマニュアルに関連付けることをより容易にさせるように含めることができる。これは、サブジェクト、オブジェクトまたは管理者の役割のような一般的な用語の詳述(elaboration)を含むことができる。

TOE要約仕様は、それゆえにTOEが満たすべきセキュリティ要件のTOE固有の詳述(elaboration)であると特徴付けることができる。TOE実装、そのアーキテクチャまたは、その設計の原則の詳細を提供すること、またはどのように(例えば)開発者がTOEのセキュリティ機能テストを行うか、詳細に記述することは必要ない。 (259)

7.2 ITセキュリティ機能の特定のしかた

上述のように、ISO/IEC 15408は、TOEによって提供されるITセキュリティ機能の仕様を含むことをSTのTOE要約仕様に要求する。STは、ITセキュリティ機能がSFRをすべてカバーし、各ITセキュリティ機能が少なくとも1つのSFRに対応することを実証しなければならない。 (260)

TOEの主となるセキュリティ目的を特定するITセキュリティ機能は、最も詳細に注目されるべきである。補助的SFRに対応するITセキュリティ機能の場合は、対応するITセキュリティ機能にいくらか重要な付加の詳細も含まないように決めてよい;確かにある場合は、対応するSFRと同一の

ものとしてITセキュリティ機能を定義することができる。それでもなお、例えばTOE固有の用語の使用により、適切であれば機能性を明確できるようにしておくべきである。(261)

ITセキュリティ機能は、例えば機能性の仕様を単純にし、かつ対応する評価をより容易に(特に、この設備、開発表現及びテスト証拠への追跡性の実証の場合)するために対応するSFRとは別に体系付けされ、かつラベルを付けることができる(適切な場合)。例えば:(262)

- a) ITセキュリティ機能は、1つ以上のSFRに対応することができる(これは、サポート機能に適切かもしれない);または
- b) SFRは、1つ以上のITセキュリティ機能に対応することができる(これは、TOEの主となるセキュリティ目的を直接満たす機能に適切かもしれない)。

この再体系化を行う際に、以下を保証すべきである:(263)

- a) SFRからの本質的な詳細を失わない;
- b) 誤りの発生が増えるだけでなくSTのレビューするコストが増えてしまうような、ITセキュリティ機能に対するSFRの必要以上に複雑なマッピングにならないようにする。

7.3 セキュリティメカニズムの特定のしかた

ISO/IEC 15408は、STによって参照されたあらゆるセキュリティメカニズムまたは技法にITセキュリティ機能の追跡性を提供することをTOE要約仕様に要求する。参照された典型的なセキュリティメカニズムまたは技法は、暗号及びパスワードの生成アルゴリズムまたは適切なISOまたは国内/政府標準への適合の主張を含んでいる。(264)

そのような参照はSTにおいて任意であることが注意されるべきである。一般に、以下のセキュリティメカニズムを参照するときだけに必要であろう:(265)

- a) システムの場合には、特定のセキュリティメカニズムを使用する特別の要求があるとき;
- b) 製品の場合には、スポンサーが特定のセキュリティメカニズムの実装の主張に価値(value)を見出すとき(または、市場がそのようなメカニズムまたは技法を要求している)。

7.4 保証手段の特定のしかた

ISO/IEC 15408は、TOE要約仕様が保証手段から保証要件にたどれることを要求する、その結果保証要件がすべて満たされることが実証される。ISO/IEC 15408は、適切な品質計画、ライフサイクル計画または管理計画への参照によって保証手段の定義がされると述べる([15408-1]、C.2.7

副項、48ページ)。

(266)

実際は、より低い保証レベルについてSTのこの節が、保証手段がセキュリティ保証要件を満たすために用いられ適切に使用される(または、であろう)という主旨の一般的な仮定を超えて付加されて提供される情報は少ししかない。推奨された1つの手法は、開発者が適切な保証要件に提供する予定の証拠資料または証拠からの一般的な対応を提供することである。

(267)

保証の上位レベル(例えば、EAL5以上に)では、開発者が持っているまたは保証要件を満たすために採用する以下に挙げるような特定のツール、技法または手法に参照付けることにより、例えばより多くの詳細を提供することが可能かもしれない:

(268)

- a) 要求された形式的仕様の中で使用される形式的表記;
- b) 使用された特定の設計方法論またはライフサイクルモデル;
- c) 構成管理ツール;
- d) テストカバレッジ分析ツール;
- e) 隠れチャンネル分析方法。

【ISO/IEC JTC 1/SC 27 N3816改訂情報】:以下に示すとおりPP主張に関する記述が追加される。

12 PP主張

12.1 序説

この項は、STのPP主張に関するガイダンスを提供する。

ISO/IEC 15408-1,C.2.8は、適合が主張される各PPに対する情報の一部として次のことが含まれていることを要求する

- a) 適合を主張するPPを識別している参照
- b) PPに適用したあらゆる詳細化
- c) STによって満たされるPPの対策方針または要件へのあらゆるTOE追加

PPへの部分的な適合を主張することはできず、PPの要件の全てを完全に満たさなければならないことに注意すること。

もちろん、ST評価範囲外のハードウェア、または他のセキュリティ製品により満たされることはいくつかのPPセキュリティ対策方針と機能要件にとって珍しくは無い。

この場合、ST根拠の中でPPの完全なカバレッジはTOEと環境のセキュリティ特徴の組み合わせにより達成されるということを示さなければならない、そして適合性のステートメントにおいてこの依存性を明確にしなければならない。

もし適合を主張するPPが無いならば、STのこの節のために要求される全ては、この主旨で全てである。

12.2 PP参照

各PPは、STの読者が当PPの仕様を見つけることができることを可能にするように識別されなければならない。これを実施するための推奨された方法は、パッケージとPP([1]参照)のISO登録簿における登録エントリ(a register entry in the ISO Registrar of Packages and Protection Profiles)を参照することである；しかしながらこの登録は広く公表または使用されていない。いくつかの各国評価スキームは、PP登録を維持し、よい代替を提供している。参照される各PPに対する明確なバージョンと参照元を識別することを保証することに注意しなければならない。

12.3 PP修整

PPがさらに明確化を必要とするITセキュリティ要件のステートメントにおいて許可された操作を含む場合、置き換えの詳細をここに記述しなければならない。置き換えの明確化が必要とされる場合、STに完全なPPの内容を改めて記述する方がよりよいこともあるということ認識しなければならない。

12.4 PP追加

PPが、PP開発者が予期していないTOE目的を扱う場合、追加される脅威、方針、対策方針などの詳細をここに記述する。 ST根拠内においてこれらの追加オブジェクトをカバーすることを忘れてはならない。

8 PP及びST根拠

8.1 序説

この章は、PPまたはST根拠を構成するしかたについてのガイダンスを提供する。 (269)

PPまたはST根拠の目的は、適合したTOEがTOEセキュリティ環境内のITセキュリティ対策の有効なセットを提供することを実証する。特に、それはITセキュリティ要件がそのセキュリティ対策方針を満たすのに適していることを示す、そして、それがTOEセキュリティ環境のすべての側面をカバーするのに適していることを順次に示される(それはセキュリティ関連事項を定義する)。PPまたはST根拠は、大抵の場合、PPまたはSTの評価者に最も多くの関心があるであろう、しかもそれは、PPまたはSTのあらゆる読者の理解を助けるかもしれない。 (270)

PP根拠の主要な側面を次の図6に示す。 (271)

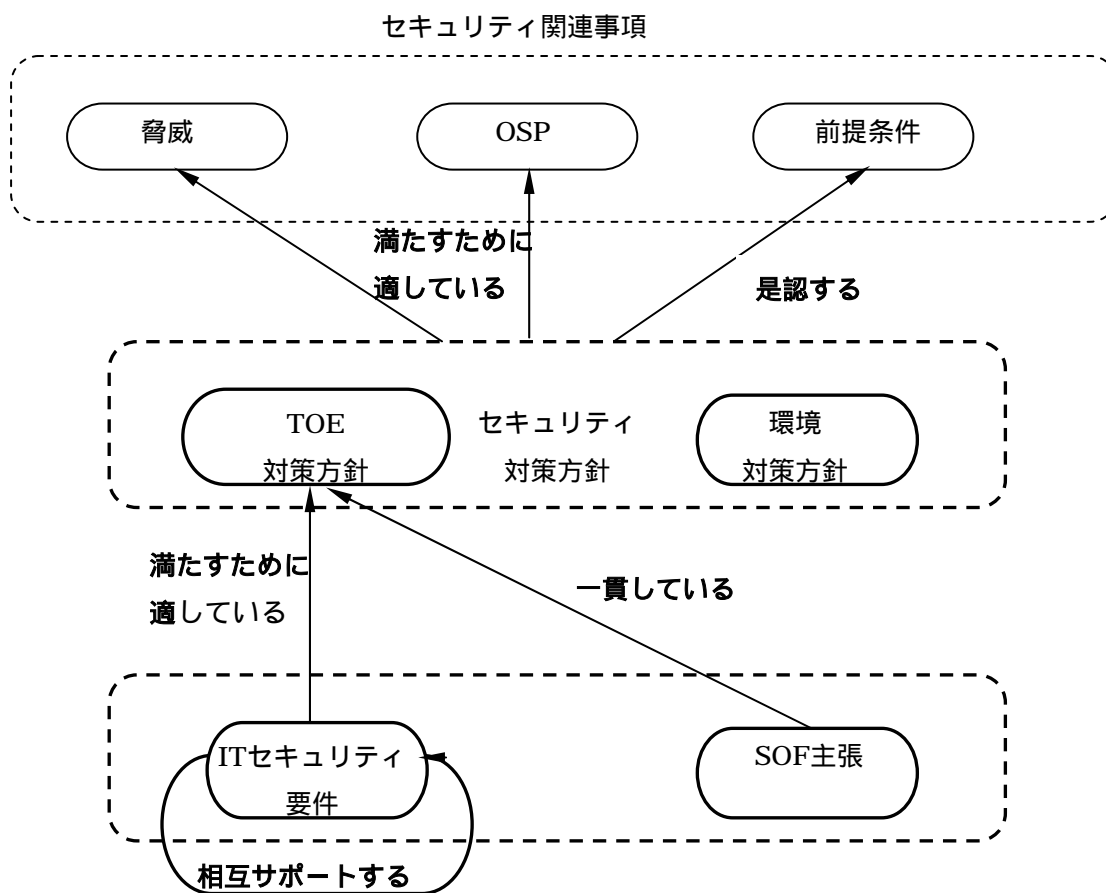


図6 - PP根拠要件

さらに、PP根拠は以下を示さなければならない： (272)

- a) TOEセキュリティ保証要件のステートメントは適切である(APE_REQ.1.4C);

- b) PPに含まれたISO/IEC 15408セキュリティ要件の満足されない依存性は、必要でない(APE_REQ.1.9C)。

それは、むしろPP根拠の一部としてよりむしろ、SFRの特定の中でSFR(APE_REQ.1.6C)に対する完了した操作を識別する要求を満足されることが推奨される。この手法の主要な利点は、それがPP根拠の中のSFRを繰返さなければならないことを回避するという一方で、PPとその根拠の間の一貫しないことを失われそうになることをこのように減らす。 (273)

ST根拠の主要なST固有の側面を以下の図7に示す。 (274)

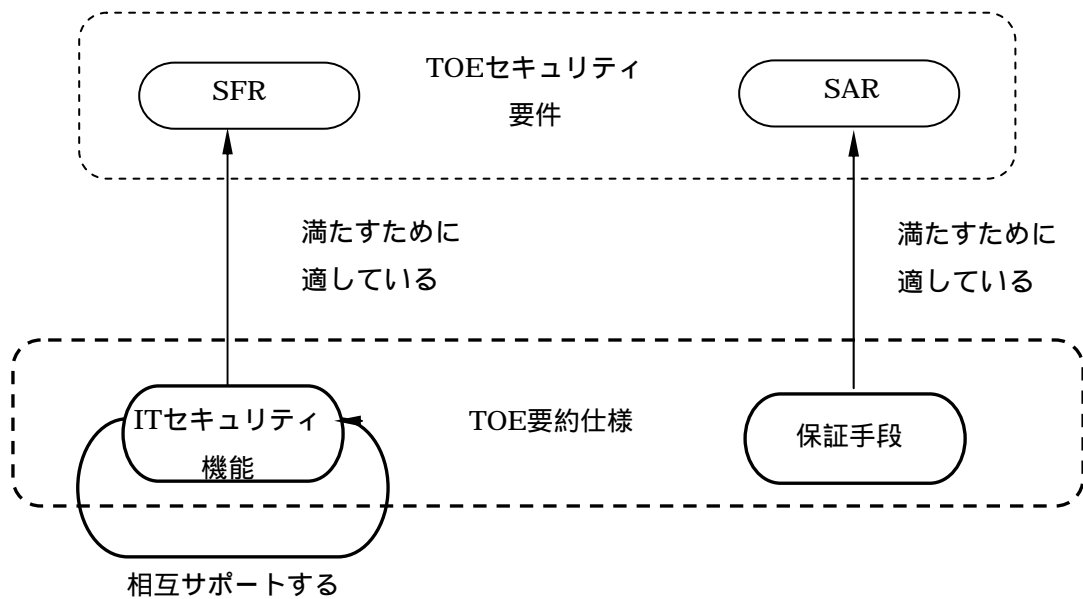


図7 – 根拠のST固有の側面

(275)

さらに、ST根拠は、PPへの準拠のあらゆる主張が正当化されていることを実証されていなければならない(ASE_PPC.1に従って)。 (276)

8.2 PPまたはSTにセキュリティ対策方針の根拠の提示のしかた

PPまたはST根拠のこの部分は、識別されたセキュリティ対策方針が、PPまたはSTのTOEセキュリティ環境の節の中で指定されるようなセキュリティ関連事項のすべての側面をカバーして、適していることを実証する。これは、セキュリティ対策方針がセキュリティ関連事項に対応するのに十分なだけでなく、それらが必要なことを示すことを伴う。次の手法が推奨される、しかし別の手法も同じ程度よく役立つかもしれない。 (277)

第1に、脅威、OSP、及び前提条件に対応することに意図されるセキュリティ対策方針に対して相互参照するべきである(多分表の使用による)。以下のことは、この相互参照情報から明らかにするべきである: (278)

- a) 各セキュリティ対策方針は、少なくとも1つの脅威、OSPまたは前提条件をカバ

—する;

- b) 各脅威、OSP及び前提条件は、少なくとも1つのセキュリティ対策方針によってカバーされる。

第1の条件を満足することは、各セキュリティ対策方針が必要であることを実証するのに(根拠の目的のために)十分であろう(言い換えれば、明白に余分のセキュリティ対策方針¹がない)。 (279)

第2に、セキュリティ対策方針が相互参照情報を補足するために非形式的論証を提供することにより、そのセキュリティ関連事項を満たすのに十分であることを実証する必要がある。セキュリティ対策方針がカバーする必要のあるTOEセキュリティ環境の個々の側面に関連してこれらの論証を以下のように体系化するべきである。 (280)

- a) 脅威については、なぜ識別されたセキュリティ対策方針が脅威への有効な対抗策を提供するであろうかについて非形式的論証を与えるべきである、すなわち、セキュリティ対策方針は、脅威の特定で識別された事象が次のどちらかであることを示す:
 - 検出、及び回復(または、資産への損害を限定する)、または
 - 防止(または、受け入れられるレベルまで減らす)。
- b) 同様に、各識別されたOSPまたは前提条件については、なぜ識別されたセキュリティ対策方針がOSPの完全なカバレッジを提供するか、または前提条件を是認するのに十分かについて非形式的論証を与えるべきである。

大抵の場合、論証がTOEのセキュリティ対策方針によって対応される脅威及びOSPに焦点をあたえることになりそうである。それらの論証を以下のようにするべきである: (281)

- a) なんらかの方法で脅威に対応する、またはOSPを満足することに寄与するものとして識別された各セキュリティ対策方針の役割について論じる;
- b) TOEのセキュリティ対策方針が狙いを達成するのに、あらゆる関係ある環境のセキュリティ対策方針がどのようにサポートするかを記述する。

1. もちろん、これは不必要なセキュリティ対策方針がないことを保証するものではない、なぜならば、他のセキュリティ対策方針が適切にその脅威またはOSPに対応するかもしれないからである。もちろん、不必要なセキュリティ対策方針の包含を回避するべきであり、これ以上より詳細な必要性の正当化を提供する必要はない。この決定は、PP評価者に任せることができる。

この節は、セキュリティ環境に対するセキュリティ対策方針を単に正当化するだけであり、例えそれが脅威のリスク評価の点でステートメントに類似しているかもしれないステートメントを含んでいても、完全な脅威のリスク評価として表わす必要がない。それらのセキュリティ方針を改訂するまたは定義する場合、何が受け入れられるリスクか定義し、リスク分析を完了することは個々の組織の義務で(up to)ある。PPまたはSTで良好な評価がされていると、消費者/利用者は組織のリスク分析の過程で論証の根拠としてこの節を使用することを選ぶかもしれない。(282)

PP への準拠をSTが主張する場合、ST根拠のこの部分は、PPとの何らかの差異に対応すべきである、以下のようなことを示す:(283)

- a) あらゆる追加の脅威は、セキュリティ対策方針によって対応される;
- b) あらゆる追加のOSPは、セキュリティ対策方針によって満たされる;
- c) どのように、あらゆる追加のセキュリティ対策方針が関係のある脅威及び/またはOSPに対応するのか。

8.3 PPまたはSTにセキュリティ要件の根拠の提示のしかた

8.3.1 セキュリティ要件が適していることの示しかた

PP根拠のこの部分の目的は、識別されたITセキュリティ要件(及び、特にSFR)がその識別されたセキュリティ対策方針を満たし、そのためにセキュリティ関連事項に対応するのに適していることを示すことである。セキュリティ対策方針のように、ITセキュリティ要件が必要で十分であることを実証する必要がある。次の手法が推奨される、しかし別の手法も同じ程度よく役立つかもしれない。(284)

第1に、TOEの各セキュリティ対策方針を満足するSFRに対して相互参照すべきである(多分表の使用による)。以下のことは、この相互参照情報から明らかにすべきである:(285)

- a) 各SFRは、少なくとも1つのセキュリティ対策方針に対応する;
- b) TOEの各セキュリティ対策方針は、少なくとも1つのSFRによって対応される。

前者は、各SFRが必要であることを実証するのに(根拠の目的のため)十分であろう(言い換えれば、明白に余分のSFRがない)。(286)

第2に、SFRの十分性に対する非形式的論証に関して、相互参照情報を補足すべきである。これらの論証は、TOEのセキュリティ対策方針に関連して体系化されるべきである。各々のそのようなセキュリティ対策方針については、明示的なセキュリティ要件と推量された環境のセキュリティ要件が満足されたことを与えるとき、なぜ識別されたSFRがセキュリティ対策方針を満足するのに十分に関して、非形式的論証を提供すべきである。これらの論証は、セキュリティ対策方針を直接満足することと、サポートする役割(すなわち、6.2.1節の*主*及び*補助的*SFR)を果たす

ことの両方について、PP (機能コンポーネントによる)に含まれたすべてのSFRをカバーするべきである。論証を構成する中で、正当な考察が与えられるべきである： (287)

- a) どのように、そしてなぜ、ISO/IEC 15408の操作は適用されたのか；
- b) どのように、TOEセキュリティ要件がIT環境に対するセキュリティ要件と連携されているのか。

PPへの準拠をSTが主張する場合、ST根拠のこの部分は、PPとの何らかの差異に対応するべきである、以下のようなことを示す： (288)

- a) TOEのあらゆる追加のセキュリティ対策方針は、SFRによって満たされる；
- b) あらゆる追加のSFRは、どのように関係のあるセキュリティ対策方針に対応するのか。

8.3.2 保証要件が適切なことの示しかた

PP根拠のこの部分は、保証要件がTOEに適切なことを示すために要求される。この論証は、なぜSARのセットが以下のようなものであることの正当化を提供するべきである： (289)

- a) セキュリティ対策方針に対応するのに十分であって、よってセキュリティ関連事項を満たす、例えば、TOEが高い攻撃能力(脅威とセキュリティ対策方針から明白な)を持っている攻撃者に対して防御することを意図する場合、EAL1の保証要件に基づくことが明確に不適切であろう。なぜならば、評価がそのような攻撃者によって悪用されるかもしれない脆弱性に正当な考察を与えないからである (特に、EAL1はAVA_VLA、またはAVA_SOFの要件を含んでいない)；
- b) 与えられたセキュリティ対策方針及びセキュリティ関連事項のステートメントに対して、過度でない；
- c) 達成可能こと、すなわち、それは定義された保証要件を達成することがこの種のTOEにとって技術的に可能である(費用と時間の考察は、純粹にTOE評価のスポンサーの問題である)。

PP への準拠をSTが主張する場合、追加された保証要件を指定し、そして追加の要件は適切であることが正当化されるべきである。ST根拠は、さらに、TOEセキュリティ環境またはセキュリティ対策方針におけるあらゆる差異を考慮するべきである。 (290)

8.3.3 機能強度主張が適切なことの示しかた

ISO/IEC 15408は、あらゆる明示的な機能強度主張とともに最小限の機能強度主張が識別されたセキュリティ対策方針と一貫していることを示すことをPP根拠に要求する。実際には、これは以下のことを考慮して論証(argument)が構成されるべきであることを意味する： (291)

- a) TOEに対して述べられたセキュリティ対策方針の中の明確化されたあらゆる明

示的または非明示的強度要件;

- b) あらゆるステートメントは、セキュリティ対策方針またはセキュリティ環境のステートメントで攻撃者の技術的な専門知識、資源または動機づけについて作成される (それは、セキュリティ対策方針が対応するように意図されるセキュリティ関連事項を定義する)。

セキュリティ要件の適当な正当化の一部としてそのような論証(arguments)が既に提供されている場合、それらを繰返す必要がない。 (292)

SARがAVA_SOF.1を含んでいる場合だけ、この要件が適用できることに注意されるべきである ([15408-1]、B.2.6副項、40ページに指摘されたとともに)。これは、もちろん、SARがAVA_SOF.1を省略する場合、そのセキュリティ対策方針を満たす上での、セキュリティ要件の適切性を蝕まないことを推測する(前述の節で論じたように)。 (293)

8.3.4 セキュリティ要件が相互サポートすることの示しかた

PP根拠のこの部分の目的は、ITセキュリティ要件(及び、特にSFR)が相互サポートすること、完全な及び有効な全体を提供することを実証することにより、完全かつ内部に一貫していることを示すことである。次の手法が推奨される: (294)

- a) 機能及び保証コンポーネントの依存性が必要なところで満足することを実証する;
- b) ITセキュリティ要件間の内部整合性に対する論証を提供する;
- c) 補助的SFRがバイパスまたは干渉するような攻撃に対して、他のSFRを守るのに適切なところで含まれていることを示す。

ST根拠のための目的は、ITセキュリティ機能が相互サポートすることと、完全な及び有効な全体を提供することを実証することにより、完全かつ内部に一貫していることを示すことである。 (295)

この分析は、SFR間の相互サポートを実証するために記述されたものほとんど同じ方法で実行されるべきである。相互サポートがSFRのために既に実証されているので、分析のこの部分は、対応するSFRに対するITセキュリティ機能の特定で取り入れられたあらゆる追加の詳細の影響に焦点をあてるべきである。この追加詳細の包含の結果として取り入れられるITセキュリティ機能間のサポートまたは相互関係のあらゆる具体例が論じられるべきである。それでもなお、その後TOE要約仕様がTOEの観点からのSFRを(実際には)書き直したものであるため、SFR分析の結果のあらゆる再使用もこの異なる観点から結果を説明するべきである。 (296)

相互サポートのこれら側面の各々は、順次以下に示す。 (297)

コンポーネントの依存性分析

この分析は、多くの方法で有効に提示することができる、例えば、自然言語文書の使用(using natural language textual means)、または表もしくはツリーダイアグラムの使用による。SARが単純にISO/IEC 15408 EALまたは他の保証パッケージに基づく場合は、分析がSFRの依存性を単にカバーする必要がある(なぜならば、保証パッケージはすべての依存性を満足して、通常自己充足型であるからである)。(298)

いかなる方法が選ばれても、それは以下が可能であるべきである:(299)

- a) *SFRのレベルにおいて依存性がどこで満足するか実証すること、すなわち、機能コンポーネントの各々の繰り返しに対して;*
- b) *あらゆる満足されない依存性を識別することである、なぜ各々のそのような依存性が満足される必要がないかについて説明を提供すること。*

SFRのレベルで依存性分析を実行する理由は、あるコンポーネントが何回も繰り返される場合、それが依存するコンポーネントも繰り返されることになるかもしれないということである。例えば、FMT_MSA.3(静的属性初期化)は、FMT_MSA.1(セキュリティ属性の管理)に依存する。FMT_MSA.3がいくつかの異なるセキュリティ属性の初期化をカバーするために繰り返される場合、これら属性の各々の管理をカバーするために同じ回数FMT_MSA.1を繰り返すことが必要であろう。この事象で、FMT_MSA.1 SFRはFMT_MSA.3 SFRにより参照されたセキュリティ属性のすべてを実際にカバーするとは限らないかもしれないので、機能コンポーネントのFMT_MSA.1がPPに含んでいるので、FMT_MSA.3の依存性が満足されると単純に主張する依存性分析は、不完全であろう(及び、潜在的に誤解を導く)。(300)

依存性は、TOEによって満足される必要がないかもしれない、なぜならば(例えば)、それはTOEに関係ないかもしれない、またそれは、セキュリティ対策方針のステートメントに対して不必要かもしれない。二者択一で、依存性はIT環境によって、または非IT手段によって満足されてもよい。(301)

上記に示したように、依存性分析を提示することへの1つの可能な手法は以下の例のような表を構成することである:(302)

- a) *PPに含まれた各機能コンポーネントに対して1つの行を作る、その中に必要な数だけ、各々の個々のSFRが一意に識別されるように、コンポーネントの複数の発生(multiple occurrences)のための複数の行を作る;*
- b) *識別された各々の機能コンポーネントに対して、[15408-2]で定義されるような他のコンポーネントの依存性をリストする;*
- c) *識別された各々の依存性に対して、依存性を満足する行またはなぜ依存性を満足する必要がないかについて説明を提供する。*

保証依存性に関する実証は、比較的直接的であるべきです。PPがISO/IEC 15408 EALまたは保証パッケージを単に必須の場合、PP根拠はすべての保証-保証(assurance-assurance)依存性が

この理由で満足すると単に見なしてもよいかもしれない。PPが追加された保証要件を含んでいる場合、PP根拠は導入した追加の依存性が満足することを示さなければならない。(303)

[15408-2]は、少数の機能-保証(functional-assurance)依存性を識別する。これらは、上述された表で満足されることを示すことができる。例えば、PPがFPT_RCV.1を必須として、それはAGD_ADM.1に依存性を持つ、そして対象評価保証レベルがEAL4である場合、この依存性への表エントリは、行の参照ラベルまたは番号の代わりに EAL4 であるべきである。(304)

この依存性分析は、ITセキュリティ要件が相互サポートすることを実証するある程度の効果があるろう。言い換えれば、機能コンポーネントAが機能コンポーネントBに依存する場合は、当然BはAのサポートとなる。(305)

STがPPへの準拠を主張する場合、ST根拠のこの部分は、PPとのあらゆる差異について単に対応すべきである、すなわち、すべての追加されたSFR及び保証要件に対して依存性が満足されることを示すことである。(306)

内部一貫性

すべてのコンポーネントの依存性が関係するところで満足されていることが示されているとすれば、相互サポートの実証の第2の側面については、ITセキュリティ要件の内部一貫性に対する論証を提供する必要がある(これは、相互サポートに対する、必要条件である)。SFRの場合、異なるSFRが同じタイプの事象、操作またはデータのどこに適合するか考慮することにより行うことができる。例えば、PPが利用者の匿名性の要求と同様に利用者個々の責任の要求も含んでいる場合、これらの要求が衝突しないことを示す必要がある。これは、個々の利用者責任を要求する監査可能な事象が利用者の匿名性を要求する操作に関係しないことを示すことを含むかもしれない。(307)

STがPPへの準拠を主張する場合、ST根拠のこの部分は、PPとのあらゆる差異について単に述べておけばよく、あらゆる追加されたセキュリティ要件がどのように示されているか:(308)

- a) 他のITセキュリティ要件によってサポートされる;
- b) 他のITセキュリティ要件にサポートを提供する;
- c) 他のITセキュリティ要件と一貫している(矛盾しない)。

攻撃に対するSFRの防御

PP根拠のこの部分で考慮する必要があるサポートの他の形式は、SFRだけに関係するものだけである。これは、保証要件を含む相互サポートの実証があまり重要でないからである:(309)

- a) 当然、SARはSFRをサポートする、なぜならば、それらが機能要件を満たすという確証を提供からである;
- b) SFRとSARが一般的な意味において相互サポートとなるが、PP根拠の解説に値

するような、特定のSARにサポートを提供するSFRの*特定の*実例はほとんどない。しかしながら、1つの典型的な例は、FPT_SEP(ドメイン分離)コンポーネントでしょう、それは分離の達成するを助けることによりADV_HLD(上位レベル設計)コンポーネントをサポートする；

- c) SARは、依存性が満足されたことが提供されれば相互サポートされたと見なし
てよい。

6.2.1節に記述されるように、*補助的*SFRは、*主*SFRを打ち負かそうとする攻撃に対する防御を補助できる、そこでは、攻撃者の隠れた意図が*主*SFRの対抗しようとする1つ以上の脅威を引き続いてもたらそうとすることである。相互サポートは、ISO/IEC 15408セキュリティ要件の依存性に
関連したものと同様にこの種類のサポートも両方包含する。 (310)

依存性分析によって対応されないSFR間の相互サポートの考察は、以下のように、それらのSFR
に対応するべきである： (311)

- a) 他のSFRのバイパスを防止することを助ける；
- b) 他のSFRの改ざんを防止することを助ける(その完全性がSFRに本質的である、
あらゆるセキュリティ属性または他のデータを含む)；
- c) 他のSFRの非活性化を防止することを助ける；
- d) 別のSFRの誤構成の検出を可能にするか、別のSFRの無効化をねらった攻撃の
検出を可能にする。

SFRのバイパスは、FPT_RVM.1(TSPの非バイパス性)によって典型的に防御される。SFRによる
セキュリティの実施が、対応している利用者の識別を知っているTOEに依存する場合(例えばアク
セス制御)、利用者認証要件(FIA_UAUファミリからのコンポーネントを使用して)は、それらSFR
のバイパスを防止するであろう(違う利用者の成りすましによる)。しかしながら、すべてのSFR
が、バイパスを防止するために他のSFRからのサポートを要求するとは限らないであろうとい
うことに注意すべきである；これは、以下の場合そうなるであろう： (312)

- a) 機能呼び出すかどうかに関する決定は、TSFではなく、利用者または管理者
に基づく、例えば、SFRは、FDP_DAU(データ認証)コンポーネントに基づいて
いる；
- b) SFRの言い回しが、機能が必要なときに常に呼び出されることを規程し、その
結果、SFRがTSFによって満足される場合、SFRはバイパスすることができな
い。例えば、FDP_RIP(残存情報保護)コンポーネントに基づいたSFRの場合よ
うに。

改ざん攻撃は、すべてのSFRに関係する。そのような攻撃は、以下のことにより防御されるかも
しれない： (313)

- a) 信頼されないサブジェクトによる外部からの妨害または改ざんを防止する FPT_SEP(ドメイン分離)コンポーネント;
- b) 物理的な改ざん攻撃を検出するまたは、抵抗する手段を提供する FTP_PHP(TSF物理的保護)コンポーネント;
- c) セキュリティ属性または構成データを改変する能力を制限する FMT_MSA.1(セキュリティ属性の管理)のようなセキュリティ管理コンポーネントに基づく SFR;
- d) セキュリティの重大なデータの完全性を保護する FMT_MTD.1(TSFデータの管理)または、FAU_STG.1(保護された監査証跡格納)のようなコンポーネントに基づく SFR;
- e) TSFのスプーフィング(偽造)に基づいた改ざん攻撃を防止する FTP_TRP(高信頼パス)コンポーネント (例えば、パスワードを奪うプログラムによる)。

非活性化は、PPで特定されるようなすべてのSFRに関係しないかもしれない。しかしながら、1つの例は、セキュリティ監査に関係する非活性化である;FAU_STG(セキュリティ監査事象格納)ファミリは、監査証跡格納の結果起きるセキュリティ監査機能の非活性化を防止するための要件を含む。FMT_MOF.1(セキュリティ機能のふるまいの管理)を使用することで、特定されたSFRは、あるセキュリティ機能の非活性化を防止するのをさらに助けるかもしれない。 (314)

セキュリティ監査のような検出機能は、あるSFRの無効化をねらった攻撃を検出することが可能な能力、またはTOEを攻撃されやすくするようにしておくことができる潜在的な誤構成を検出することが可能な能力を提供することによって、他のSFRにサポートを提供する。その他の検出機能は、FDP_SDI(蓄積データ完全性)及びFPT_PHP(TSF物理的保護)ファミリからのコンポーネントを含む。 (315)

8.3.5 保証手段が保証要件を満足することの示しかた

ST根拠のこの部分の目的は、識別された保証手段が保証要件を満たすのに適切なことを示すことである。推奨される手法は、保証要件に識別された保証手段のマッピングを提供することで、各保証要件が対応されることを実証することである (多分表の使用によって)。特定の保証手段が識別されている場合、このマッピングには保証要件がどのように満足されるかの簡潔な説明が伴うべきである(7.4節参照)。しかしながら、保証手段の適応性の評価がTOEの評価を前もって判定してはならないということに注意すべきであり、選ばれた保証手段が適切かどうか具体的な証拠を提供しているだけである。その結果、適応性の詳細な正当化はSTでは期待されない。 (316)

実際は、STが特定の高位保証技法の使用を要求するSARを含んでいる場合、最大限の注意がST根拠のこの部分に払われるでしょう(例えば、隠れチャネル分析または形式的方法の使用)。 (317)

8.3.6 参照されたPPに準拠するSTの示しかた

根拠のこの部分は、STが準拠すると主張するPPを識別することを要求し、そして、以下のように示す： (318)

- a) すべてのPPのセキュリティ対策方針が含まれており、そして、セキュリティ対策方針のあらゆる詳細化が有効である；
- b) すべてのPPのセキュリティ要件が含まれており、そして、PPセキュリティ要件のあらゆる詳細化または他の操作が有効である；
- c) ITセキュリティ要件は、あらゆるPPのセキュリティ要件と矛盾しない。

STが、PPのセキュリティ対策方針及びセキュリティ要件を完全にそのまま含む場合(または、それらを参照する場合)及び、追加されたセキュリティ対策方針または要件を含まない場合、それ以上の分析は要求されない。さらなる分析は、STが追加されたセキュリティ対策方針及びセキュリティ要件を含んでいる場合のみ必要である。あらゆる追加されたセキュリティ対策方針及びセキュリティ要件はPPで述べられているどれにも矛盾しないことを正当化しなければならない。 (319)

さらに、PPがセキュリティ要件に対する未完了な操作を含んでいるところで、ST作成者に割付または選択を任せ、すべてのそのような操作が完了されることがSTにおいて明らかにされなければならない。 (320)

8.3.7 ITセキュリティ機能がSFRを満足することの示しかた

根拠のこの部分は、特定されたITセキュリティ機能がSTに含まれたすべてのSFRを満たすのに適しているという実証を提供するべきである(そして、参照されたPPで重要な役割を演じるSFRに対してだけではない)。推奨される手法は、SFRに対するITセキュリティ機能のマッピングを実証することである(多分表の手段による)。マッピングは、以下のことを示すべきである。 (321)

- a) 各SFRは、少なくとも1つのITセキュリティ機能にマッピングされる；
- b) 各ITセキュリティ機能は、少なくとも1つのSFRにマッピングされる。

マッピングに加えて、あるSFRがどのように満足されているか自明でない場合はいつも説明を与えるべきである。これは、例えば単一のSFRに多くのITセキュリティ機能がマッピングされている場合に必要かもしれない。 (322)

1. 追加されたITセキュリティ要件間の衝突は、ITセキュリティ要件が全体として相互サポートすることを実証するとき、勿論対応されるべきである。

9 コンポジット及びコンポーネントTOEのPPとST

9.1 序説

この章では、次に述べるケースに対応するような、複合性の考え方により生じる特定の問題に関連したガイダンスを提供する。 (323)

- a) PPやSTがコンポジットTOEのために書かれている場合。コンポジットTOEは二つまたはそれ以上のコンポーネント(それ自身がコンポジットTOEでもよい)から構成されており、それぞれがそれ自身の独立したPPまたはST(このガイダンスの中ではコンポーネントTOE PPまたはコンポーネントTOE STと呼ぶ)を持っている。
- b) IT環境への識別された依存関係を持つコンポーネントTOEのために書かれたPPまたはSTの場合。そのIT環境は、コンポジットTOEの一部であるその他のコンポーネントTOEを含む(それはまた、非IT環境に対するセキュリティ要件への依存関係があるかもしれないが、それらはPPまたはSTにおいて正式な部分としては要求されないことに注意)。

いくつかの考えられるシナリオが存在する。例えば、 (324)

- a) コンポーネントTOEの識別情報が既に知られており、これらコンポーネントTOEのためのSTが既に存在する場合に、コンポジットTOE STが書かれるかもしれない。要するにコンポジットTOE STの主な目的は、全体としてコンポーネントTOEによって満たされるべきセキュリティ関連事項を定義し、すべての局面において対応されていることを実証することである。
- b) 問題を個々のコンポーネントTOEに分解する目的で、そしてそれら個々のコンポーネントのためのPPを書く目的で、コンポジットTOE PPは書かれるかもしれない。コンポジットTOE PPの主な目的は、先に述べたとおりである。それゆえ、コンポーネントTOE STは、コンポーネントTOE PPのセキュリティ要件に対してマッチしている必要がある。

この一般的なアプローチは、とりわけ多くのコンポーネントを含むような大規模システム設計に適切である。コンポーネントTOE PPまたはSTを書くために、どのようにコンポジットTOEをうまく分解するかという選択は、コンポジットTOE PP/ST作成者が決定する問題である。 (325)

複合性の領域における実践的な経験は、今のところわずかであることに注意すべきである。さらなる実践上の経験がこの領域で積まれるため、または積まれたとき、より進んだガイダンスがこのガイドの将来のバージョンで提供されるであろう。 (326)

9.2 コンポジットTOE

9.2.1 PPやSTの記述的部分

コンポーネントTOE PP/STの記述的部分や、特にTOE記述では、TOEの様々なコンポーネントを識別して、コンポジットTOEを記述すべきである。コンポーネントTOE PPまたはSTのTOE記述の章は、TOE機能性の記述として参照されるべきであり、この情報はコンポジットTOE PP/STの中に要約されるべきである。 (327)

9.2.2 TOEセキュリティ環境

コンポジットTOEのPPやSTでのTOEセキュリティ環境の章は、次のどちらかであろう。 (328)

- a) コンポジットTOEのためのセキュリティ環境を、完全に(または適合が宣言され、適切であれば付加的な詳細を含むようなひとつ以上のPPを参照することにより)特定する。または
- b) 脅威、OSP、前提条件の詳細な定義をコンポーネントTOE PPやSTを参照し、(読者に全体像を与えるため)セキュリティ関連事項の概括的な記述を提供する。

1番目のアプローチは、コンポジットTOE PPが最初に書かれ、保護されるべき資産とその資産に対する脅威という点で、コンポーネントTOEにまたがった重要な類似性が知られている場合には適切であろう。この場合、コンポーネントTOE PPは、情報を繰り返しているというよりも、単にTOEセキュリティ環境の定義を参照して挙げているといえるであろう。 (329)

2番目のアプローチは、コンポーネントTOE PPやSTが既に存在している場合に、より適切であろう。また、保護されるべきたくさんの異なる資産があり、そのそれぞれがコンポジットTOEのコンポーネントの限られたサブセットのみに関連するような場合にも適切であると思われる。このような事象において、コンポジットTOE PP/STでの完全な記述は、過度に複雑になりがちであり、よって読者が理解しにくくなりがちである。それゆえに資産や脅威エージェントとしてのこのような物事の概括的な記述は、それぞれのコンポーネントTOE PPやSTで提供されたセキュリティ関連事項の定義の文脈を提供するという点で、読者にとってより理解を助けるものとなるであろう。 (330)

ISO/IEC 15408では、TOEが物理的に分散される場合には、(明瞭とするために)TOEセキュリティ環境のはっきりとした範囲を識別し、セキュリティ環境上の側面(脅威、OSP、前提条件)をそれぞれについて論じる必要があるであろうと指摘している点に注意すべきである。 (331)

どんなアプローチを用いたとしても、コンポジットTOE PP/STとコンポーネントTOE PP/STとの一貫性があることを保証する必要がある。 (332)

9.2.3 セキュリティ対策方針

セキュリティ対策方針のステートメントは、コンポーネントPPまたはSTの中で示されなければならない。また、コンポジットTOEのPP/STの中でそれらを完全に言い直す必要もない。しかしながら、どのコンポーネントがどのセキュリティ対策方針を満たしているかを示すなどして、コンポジットTOE PP/STに情報を要約することは適切であろう。(333)

しかしながら、もし個々のコンポーネントTOEのSTに書かれている物とはまったく同じではないようなセキュリティ対策方針が、コンポジットTOE STに識別されたならば、コンポジットTOEセキュリティ対策方針からコンポーネントTOEのそれらへのマッピングを示さなければならない。(334)

9.2.4 セキュリティ要件

ITセキュリティ要件のステートメントは、コンポーネントTOE PPまたはSTの中で示されなければならない。また、コンポジットTOEのPP/STの中でそれらを完全に言い直す必要もない。しかしながら、SFRをコンポーネントにマッピングしたり、それらSFRでの保証レベルを識別したりすることにより、コンポジットTOE PP/STに情報を要約することは適切であろう。(335)

これについての例外は、コンポジットTOEに対する一定の保証レベルが識別される場合である。この場合、要件のこの定義を参照するコンポーネントTOE PP/STとともに、保証要件を一箇所(コンポジットTOE PP/ST)で特定するのが適切であろう。(336)

コンポジットTOE PP/STで、異なるコンポーネントTOEにより提供されたSFRが異なる保証要件を持つといった「保証プロファイル」を特定することが可能であることを言及しておいてもよいであろう。例えば、コンポーネントTOEが、とりわけ高価な資産を保護するために選ばれた場合や、またはそれらが攻撃者にとってとりわけ心を引くものである場合に適切であろう。そのようなアプローチは、ISO/IEC 15408ではあからさまには禁じていないが、あるコンポーネントTOEによって規定されるSFRが、より低い保証のレベルで評価されるべき他のコンポーネントTOEによって規定されたSFRに依存するといったプロファイルとならないことを保証しなければならない。(337)

保証プロファイルを指定するようなコンポジットTOE PPまたはSTの場合、識別できる最小の保証レベルの範囲を除いて、全体にわたる保証レベルの識別には意味がないことに注意をすること。(338)

大規模で多数からなるコンポーネントシステムの設計における実用的な考慮は、開発と評価の増大するコストのため、高い保証コンポーネント(high-assurance component)TOEを最小限度にすることを要求する。一般的な考え方は、最も保護を必要とする資産を少数の高い保証コンポーネントTOE内に分離させることである(例えば、認証局が保持するルート鍵を分離する)。(339)

コンポジットTOE PP/STを作成する際、もちろんそのコンポジットTOE自身がさらに大きなTOEを構成しているコンポーネントとなるものでない限り、すべてのコンポーネントTOEのすべての

依存性は、他のコンポーネントTOEによって満たされていることを保証する必要がある。したがってコンポジットTOE PP/STのITセキュリティ要件の節は、(もしそのようなものがあれば)コンポジットTOEのIT環境によって満たされるべき、すべての満たされていない依存性を識別するべきである。 (340)

9.2.5 TOE要約仕様

コンポジットTOE STは、コンポーネントTOE STの詳細を再記するのではなく、むしろそのTOE要約仕様に参照付けて記述すべきである。コンポジットTOE STのITセキュリティ要件節は、どのコンポーネントTOEがどのITセキュリティ要件を満足しているかをすでに識別しているべきであり、したがってそれぞれのコンポーネントTOEで示されたITセキュリティ機能をリストするといった試みから得るところは少ないであろう。 (341)

もし、コンポーネントTOE STのTOE要約仕様が他のコンポーネントTOEへの付加的なまたはより詳細な依存性を識別した場合、コンポジットTOE要約仕様は、それらがコンポジットTOE全体として満足することを示すか、コンポジットTOEに対するIT環境でのセキュリティ要件であるため満たされていない依存性であることを特定するかのいずれかをする必要があるだろう。 (342)

9.2.6 PP 根拠

コンポジットTOE PPは、セキュリティ対策方針のセットがTOEセキュリティ環境のすべての側面に対応するのに適していることと、ITセキュリティ要件がセキュリティ対策方針を満たすのに適していることを示さなければならない。PP根拠のいくつかの側面において、コンポーネントTOE PP根拠の詳細を参照することは可能であろう。次のアプローチを用いるべきである。 (343)

- a) コンポジットTOEのセキュリティ関連事項に対応するのに、コンポジットTOEのセキュリティ対策方針のセットは全体として適切であることを示すために、まずそれぞれのコンポーネントTOEセキュリティ対策方針をコンポジットTOE PPで述べられている脅威とOSPにマッピングする必要がある。次に、なぜこれらのセキュリティ対策方針が脅威に対抗するのに、そしてOSPを満たすのに適しているかについての論拠を示すべきである。コンポジットTOE脅威やOSPが正確にコンポーネントTOE PPで指定されたそれらにマッピングするのであれば、それぞれのコンポーネントTOEのPP根拠を参照付けるだけで可能である。
- b) ITセキュリティ要件のセットがセキュリティ対策方針を満たすのに適していることを示すために、コンポジットTOEのセキュリティ対策方針を満足させるコンポーネントTOEそれぞれのPP根拠を参考文献とするべきである。コンポジットTOE PPにおいて、コンポジットTOEのすべてのセキュリティ対策方針が少なくともひとつのコンポーネントTOEによって適切に対応されることを実証し、ふたつ以上のコンポーネントTOEがセキュリティ対策方針に対応するため

に協調する場合には説明を示すべきである。

- c) ITセキュリティ要件の依存性が満たされていることを示すため、個々のコンポーネントTOEのPP根拠を参考文献としてもよい。しかしながら、次のことを保証すべきである。コンポジットTOEのPP根拠は、
 - 個々のコンポーネントTOE PPのIT環境によって満足されるすべての依存性が、コンポジットTOE中の他のコンポーネントTOEによって全体として満足されているか、コンポジットTOEのIT環境に依存しているものとして(コンポジットTOE PP中に)識別されているかのどちらかであることを実証する。
 - コンポーネントTOE PP根拠において論証により除いてしまった依存性についても、コンポジットTOEセキュリティ環境の状況ではもはやこれらの論証は有効ではないため考慮する。
- d) ITセキュリティ要件が相互にサポートしていることを示すため、それぞれのコンポーネントTOE内でのITセキュリティ要件間の相互関係の分析のための個々のコンポーネントTOEのPP根拠に参照付けてもよい。しかしながら、コンポジットTOE PP根拠は、コンポーネントTOE PP根拠によって完全に対応されないときは、異なるコンポーネントTOEに適用するITセキュリティ要件間のすべての相互関係や依存関係について論じるべきである。

9.2.7 ST根拠

コンポジットTOEのST根拠構成のためのガイダンスは、上記のコンポジットTOE PP根拠のものと非常に似ている。特に、(344)

- a) TOEセキュリティ要件が、ITセキュリティ機能や保証手段によって適切に対応していることを示すため、コンポーネントTOEのST根拠を単に参考文献としても良い。
- b) ITセキュリティ機能が相互にサポートしていることを示すため、それぞれのコンポーネントTOE内で相互サポートの実証のためのコンポーネントTOE ST根拠を参考文献としてもよい。しかしながら、コンポジットTOE ST根拠は、適切であれば、異なるコンポーネントTOE内のITセキュリティ機能間の相互関係や依存関係について対応すべきである。

9.3 コンポーネントTOE

9.3.1 PPとSTの記述的部分

もし、TOEがコンポジットTOEのコンポーネントとして意図されているものであれば、PPやSTの記述的部分(特にTOE記述)はこのことをはっきりとさせるべきである。もし、コンポーネント

TOEが特定のコンポジットTOEの一部となるものであり、その他のコンポーネントTOEが分かっているならば、TOE記述は相互に作用する(そして、その結果コンポーネントTOEのIT環境を、またはその一部を形成することになる)それらの他のコンポーネントTOEについて識別すべきである。または、TOE記述は、一般的な用語でこのコンポーネントTOEを用いるであろうコンポジットTOEの種別について記述すべきである。(原則としては少なくとも、いかなるTOEもより大きなコンポジットTOEで使用可能であることを、言及しておいてもいいであろう。) (345)

9.3.2 TOEセキュリティ環境

PPやSTのこの節での目的は、コンポーネントTOEによって対応すべきセキュリティ関連事項を定義し範囲を示すことである。評価者の視点からは、コンポーネントTOE評価の範囲をも定義するであろう。例えば、コンポーネントTOEのIT環境は、コンポーネントTOEと相互に作用すると想定された他のITコンポーネントをまさに含むかもしれない。そのような場合、コンポーネントTOEのそのIT環境に対する依存性の存在は、TOEセキュリティ環境における前提条件として識別されなければならない。そのような前提条件は、実装の細部については避けるべきである。なぜなら、それらはPPやSTの他のところで明らかにされるであろう。 (346)

同様に、OSPはIT環境の他の装置との相互運用をTOEに命ずるかもしれない。この場合には、命じられたような相互運用を行うTOEの能力を、評価者が十分に試験できることを保証するステートメントをPPまたはSTに含めるべきである。 (347)

9.3.3 セキュリティ対策方針

IT環境に対するすべての依存性は、(IT)環境のためのセキュリティ対策方針として識別されるべきである。 (348)

コンポーネントTOE PPの場合、適合TOEはPPがIT環境に据えるひとつ以上のセキュリティ対策方針に実際に満たすことがあることに注意すること。例えば、PPは下層のオペレーティングシステムによりそのセキュリティ対策方針が満たされることを想定するにも関わらず、DBMSはその利用者の識別と認証のためのセキュリティ対策方針に対処するかもしれない。 (349)

もしOSPがIT環境内の他の装置とのTOE相互運用を命じるものを含んでいれば、このOSPを満たすためのTOEのセキュリティ対策方針が含まれるべきである。 (350)

9.3.4 セキュリティ要件

コンポーネントTOEに対するIT環境におけるセキュリティ要件は、可能であればそれらのセキュリティ要件を満たすのに依存している特定のコンポーネントTOEを識別すべきである。IT環境でのセキュリティ要件は、別のPPへの適合を要求することで定義できることに注意すること。 (351)

9.3.5 TOE要約仕様

ITセキュリティ機能の仕様の一部として、IT環境におけるいかなるセキュリティ要件の詳細化を規定することも適切であろう。例えば、TOEは生成したセキュリティ監査データをログするのに

特定のオペレーティングシステムのインタフェースを用いるかもしれない。もし、コンポーネントTOEが特定のコンポジットTOEの一部となるものであったら、IT環境におけるすべてのそのような詳細化されたセキュリティ要件は、コンポジットTOEの特定のコンポーネント上にマッピングされるべきである。(352)

9.3.6 PP根拠

IT環境におけるセキュリティ要件をPPが特定したならば、これらの要件はPP根拠で検討されなければならない。それらは次のことを示すべきである。(353)

- a) どのようにIT環境のセキュリティ要件が、TOEのセキュリティ対策方針を満足させるのに寄与するか。
- b) IT環境のためのセキュリティ要件のすべての依存性が満足されていること。
- c) どのようにIT環境のためのセキュリティ要件が相互にサポートしているか。また、どのようにそれらがITセキュリティ要件をサポートしているか。

9.3.7 ST根拠

IT環境におけるセキュリティ要件をSTが特定したならば、これらはPP根拠の先の節で述べたように、ST根拠で考慮されなければならない。STに含まれるような依存性に関するいかなる付加的な詳細もまた、ST根拠の適切な箇所で検討されるべきである。(354)

10 機能及び保証パッケージ

10.1 背景

パッケージの概念は[15408-1]、4.4.2.1副項、26ページに紹介されている。パッケージは次のような用語で特徴付けられる。(355)

- a) 機能コンポーネントの、または保証コンポーネントの**中間的な組み合わせ**である；
- b) **再利用可能性**を意図され、PP、ST、またはより規模の大きいパッケージを構成することを助ける；
- c) セキュリティ対策方針の識別可能なサブセットを満足するために**有効であることが既知である**、セキュリティ要件を定義することを意図される。

いくつかのPPやSTで再利用可能なパッケージの主要な利点は、ITセキュリティ要件を特定する際に(6章参照)PP/ST作成者の作業量を削減することで、PP/ST開発の費用を軽減することである。パッケージの構成に関するこの章のガイダンスは、上記のねらいをサポートすることを意図している。(356)

ISO/IEC 15408は、機能パッケージまたは保証パッケージに関していかなる要件も特定していないが、APE保証要件の適しているサブセットをパッケージに適用することは可能である。実際、パッケージがPPと同じように構成されており、PP/ST作成者に特定がゆだねられている部分が明確に識別されていれば、PP/ST作成者の助けになるであろう。しかしながら、パッケージの正当性確認や登録のような問題は本ガイドの範囲外である。(357)

パッケージの構成の経験は非常に限られていることに注意すべきである。現状、唯一の広く適用可能なパッケージの例は[15408-3]の6項で定義されるEALであり、保証パッケージの特定のしかたの例として参照されるべきである。(358)

10.2 機能パッケージの特定のしかた

10.2.1 誰が機能パッケージを書くのか？

セキュリティ機能性の標準仕様の利用の推進を望む組織が機能パッケージを作成しようとするかもしれない。その組織はPP(またはPPのファミリー)を作成する最初のステップとしてパッケージを作成するかもしれないし、パッケージがSTで利用されることの促進したいのかもしれない。機能パッケージは、例えば、ある組織が、製品ベンダが満たすべきセキュリティ機能要件の標準的なセットを特定するために、利用することもできる。(359)

10.2.2 機能パッケージは何を含む必要があるか？

基本的に、機能パッケージはSFRの特定である。そのため、これらのSFRは前述の6.2節で与えられるガイダンスに従って特定されるべきである。よって、機能パッケージに含まれる各々のSFRは次のいずれかである必要がある： (360)

- a) 引用された[15408-2]機能コンポーネントを明確に識別し、どの操作が完了され、どの操作が未完了であるかを識別する；または
- b) その必要性の根拠を伴った上で、[15408-2]を参照することなく明示的に記述される；各々のSFRはAPE_SRE.1.2C~1.5Cで表される基準を満足する必要がある；すなわち、以下のような必要がある：
 - 表現のモデルとして[15408-2]の要件コンポーネント、ファミリー、及びクラスを使用する；
 - 定量的であり、かつ客観的な評価要件を記述する；
 - 明確に、あいまいさなく表現される。

特定されるSFRのセットは識別可能なセキュリティ対策方針のサブセットを満足することが分かっている必要がある。機能パッケージの作成者は、次のどちらかを行うべきである： (361)

- a) 1つ以上の特定されたセキュリティ対策方針から、それらを満足するSFRのセットを得る；または
- b) 定義されたSFRのセットからセキュリティ対策方針を「リバースエンジニアリングする」

実際は、機能パッケージの作成者はこれら2つのやり方をなんらかの形で組み合わせを採用するだろう。 (362)

10.2.3 役立つものであるために、機能パッケージは何を含むべきか？

役に立つものであるために、機能パッケージはより大規模な機能パッケージまたはPPまたはSTで、*再利用可能*である必要がある。PPまたはSTの作成者は次の情報が有用であることを発見するであろう： (363)

- a) SFR^(訳注)が満足するセキュリティ対策方針^(訳注)の識別

(訳注：原文では、SFR_s、security objectives と記述されており、1対1でなく複数対複数の関係であることに注意されたい。)

- b) [15408-2]コンポーネントの使用についての、または[15408-2]からの逸脱に対する注釈
- c) 以下をカバーするSFRの根拠：

- 識別されたセキュリティ対策方針を満足するための、SFRの適切性；
- 依存性分析；
- SFR間の相互サポートの実証。

しかしながら、セキュリティ対策方針の正式な特定、または[15408-3]により表現される関連する保証基準を満足する完全なセキュリティ要件根拠を、機能パッケージが含むことは推奨されない。なぜなら、特定のTOEのセキュリティ対策方針はTOEセキュリティ環境のステートメントに影響を受け、そして定義されたTOEのセキュリティ関連事項に対してある程度特有なものになるからである。むしろ、機能パッケージは、PPまたはSTの根拠を構成する際に、PPまたはSTの作成者が利用可能なあらゆる関連情報を、アプリケーションノートの形で含むべきである。 (364)

10.3 保証パッケージの特定のしかた

10.3.1 誰が保証パッケージを書くのか？

評価監督機関は関連する国内制度のもとでの評価に利用するために、保証パッケージを特定しようとするかもしれない。このようなパッケージは(例えば)保証レベルに代わるものの定義、または国内保証維持制度により要請されるAMA *保証維持*クラスからのコンポーネントの組み合わせの定義でもよい。同様に所有するシステムの評価に対して共通的な要求をもつ組織が、特有の要求と関連事項に合わせて修整された保証要件のセットの定義しようとするかもしれない。 (365)

10.3.2 保証パッケージは何を含む必要があるか？

基本的に、保証パッケージはセキュリティ保証要件の特定である。そのため、これらの要件は、前述の6.3節で与えられるガイダンスに従って特定されるべきである。よって、保証パッケージに含まれる各セキュリティ保証要件は次のいずれかである必要がある： (366)

- a) 引用された[15408-3]保証コンポーネントを明確に識別する；または
- b) その必要性の根拠を伴った上で、[15408]を参照することなく明白に記述される；各々のセキュリティ保証要件はAPE_SRE.1.2C~1.5Cで表される基準を満足する必要があり、すなわち、以下のような必要がある：
 - 表現のモデルとして[15408]の要件コンポーネント、ファミリー、及びクラスを使用する；
 - 定量的であり、かつ客観的な評価要件を記述する；
 - 明確に、あいまいさなく表現される。

10.3.3 役立つものであるために、保証パッケージは何を含むべきか？

再利用可能性の目的をサポートするために、保証要件のセットの意図される対策方針を記述する

サポート情報を、保証パッケージは含むべきである。この情報はどの環境のもとでパッケージが利用されるべきか、そして(もしあれば)他のどの保証要件と組み合わせることが適切かを読者が判断することを可能にする。 (367)

[15408-3]6項で与えられるEALの特定は、保証パッケージの提示のモデルとして利用されるべきである。 (368)

附属書A ガイダンスチェックリスト

本附属書は、本ガイドの3章から9章に提供されるガイダンスからのキーポイントを一覧する。(369)

A.1 PP/ST概説

PP/ST概要の中でPP/STによって解決するセキュリティ問題のトップレベルの概要とPP/STがどのように解決策に寄与する(contributes)か提供する。(370)

PP/ST概要がPP/STの技術的な内容と一貫していることを保証する。(371)

A.2 TOE記述

TOEセキュリティ特徴の記述に制限されない一般的なTOE機能の記述を含める(もしTOEが特別の目的を持ったセキュリティ製品でない場合)。(372)

PPのTOE記述にTOE境界の記述で何がTOEの中に含まれ何が含まれないのかを読者に伝えることを含めて考慮する。(373)

STのTOE記述の中にTOE境界の記述を含める。(374)

TOE記述がPP/STの技術的な内容と一貫していることを保証する。(375)

A.3 TOEセキュリティ環境のステートメントの定義

A.3.1 前提条件

識別

意図される利用、潜在的な資産価値、考えられる使用制限などの側面を含むTOEの意図した使用方法や特に環境の物理的、人的、手続き的、または接続性の側面に関してTOEセキュリティ環境またはセキュリティニーズの範囲について作成したあらゆる前提条件を含める。(376)

定義

前提条件の定義にTOEセキュリティ機能に関する詳細の包含を可能な限り避ける。(377)

提示

参照のしやすさのため環境の前提条件に一意のラベルを割り付ける。(378)

A.3.2 脅威

識別

攻撃方法または他の不適切な事象を誰、または脅威エージェントから保護されるために必要とする保護を要求するIT資産の識別により適切な脅威を識別する。誰、または脅威エージェントから保護されるために必要とする保護を要求するIT資産、攻撃方法または、他の不適切な事象の識別により関係のある脅威を識別する。 (379)

定義

脅威の記述が、脅威(または脅威エージェント)の源の詳述すること、攻撃されるIT資産及び攻撃方法により明確であることを保証する。 (380)

脅威の記述が、脅威の間の重複を最小限にすることにより簡潔であることを保証する。 (381)

TOE実装の欠陥または弱点に基づいた攻撃より、むしろIT資産を直接危険にさらす事象だけを含める。 (382)

提示

参照のしやすさのため脅威に一意的ラベルを割り付ける。 (383)

A.3.3 組織のセキュリティ方針

識別

脅威の考察だけで引き出せないあらゆるセキュリティ方針の要件をOSPとして識別する。 (384)

定義

TOE及び/または、その環境によって実装される1セットの規則の形にしてOSPを定義する(例えば、アクセス制御規則)。 (385)

提示

参照のしやすさのためOSPに一意的ラベルを割り付ける。 (386)

A.4 セキュリティ対策方針の定義

識別

SFRが既に知られている場合は、セキュリティ対策方針からSFRまでマッピングを容易にするためにTOEによって満足される複数の主SFRの各々に対応するTOEのための1つのセキュリティ対策方針を識別する。 (387)

環境のセキュリティ対策方針として、IT環境(例えば、下層のプラットフォーム)によって満足されるあらゆるセキュリティ対策方針を識別する。 (388)

環境のセキュリティ対策方針として、TOE對抗策の管理及び使用に関係のあるあらゆる手続き的責任を識別する。 (389)

定義

TOEのセキュリティ対策方針は、ニーズに対応する範囲を示し、識別されたセキュリティニーズに対する意図した応答の簡潔なステートメントとして定義する。脅威とOSPは、単に異なる形で再び述べない。実装の詳細への参照は可能な限り避ける。 (390)

脅威に対抗するTOEのセキュリティ対策方針は、それらが防止(*preventative*)、検出(*detective*)または回復(*corrective*)かどうか明確に定義する。 (391)

提示

参照のしやすさのためセキュリティ対策方針に一意的ラベルを割り付ける。 (392)

A.5 ITセキュリティ要件の指定

A.5.1 TOEセキュリティ機能要件

識別

第1ステップとして、TOEのセキュリティ対策方針の各々を直接満足するSFRを識別する。 (393)

TOEのセキュリティ対策方針を達成するために、サポートする役割を果たすために必要なすべてのSFRの識別によりSFRの完全なセットを識別する。 (394)

補助的SFRのセットの識別は、ISO/IEC 15408パート2で識別されるような関係する機能コンポーネントの依存性も考慮する。セキュリティ対策方針のステートメントによって必要でないと論証できる場合は、そのような依存性を満足する必要がない。 (395)

定義

セキュリティ対策方針を達成し、技術的な実現可能性(feasibility)のために監査の重要性に依存する監査レベルを選択する。 (396)

与えられたISO/IEC 15408パート2機能コンポーネントの複数の呼び出しが必要なところで繰返し操作を使用する。 (397)

機能コンポーネントに対する割付及び選択の操作は、TOEのセキュリティ対策方針と一貫しない解決策の選択を排除することが必要であり、STでは完了させ、PPでは部分的に完了させ、または完了させる。 (398)

TOE特有用語を一般的な用語(例えば、セキュリティ属性)に置き換えることが、SFRをより読みやすくより理解できるようにすることで*詳細化*操作の使用を考慮する。(399)

提示

PPまたはSTで完了した操作を示すためにイタリック体(またはテキストをハイライトする他のある方法)を使用する。(400)

そのPP/STに適切な見出しの下でSFRをグループ化する:ISO/IEC 15408パート2クラス、ファミリまたはコンポーネントの見出しで制約される必要がない。提供されるSFRは、適切なISO/IEC 15408パート2機能コンポーネントまで明確にさかのぼれる。(401)

そのPP/STに特有のユニークなSFRラベル付けスキームを採用することを考慮する:やむを得ずISO/IEC 15408パート2コンポーネントラベル付けスキームを使用しない。提供されるSFRは、適切なISO/IEC 15408パート2機能コンポーネントまで明確にさかのぼれる。(402)

A.5.2 TOEセキュリティ保証要件

識別

保護される資産の価値、それらの資産へのリスク、技術的な実現可能性、適当な費用及び時間に基づいた保証要件を選択する。(403)

A.5.3 IT環境セキュリティ要件

識別

IT環境によって満たされるあらゆるセキュリティ対策方針を満足するためにIT環境のセキュリティ要件を識別する。(404)

TOEによって満足されず、セキュリティニーズに関係ないと論証することができないTOE SFRのあらゆる依存性を満足するためにIT環境のサポートセキュリティ要件を識別する。(405)

定義

抽象的概念(abstraction)の適切なレベルでIT環境のセキュリティ要件を定義する:PPの場合は、SFRのレベルで要件を定義することが、いくつかの場合には、あまりにも実装に特定し過ぎるかもしれない。(406)

A.6 TOE要約仕様の作成

A.6.1 ITセキュリティ機能

識別

SFRに基づいたITセキュリティ機能を最初に識別する; SFRのITセキュリティ機能へのマッピング

グに過度の複雑さを導入することなく、TOE証拠資料にそれらに関連付けることを容易にするITセキュリティ機能を体系化する。 (407)定義

適切なTOE特有の詳細を組み込むこと(incorporating)によりITセキュリティ機能を定義する、そのときSFRに含まれた本質的な詳細のどれも失われないことを保証する。 (408)

A.6.2 保証手段

識別

専門的な(specialist)方法または技法を要求しない低位保証要件が定義される場合は、保証要件がすべてカバーされることを保証して、STに一般的な保証手段を識別する、例えば、セキュリティ保証要件を満たすのに適切なものとして保証手段が採用されるだろうという趣旨の一般的なステートメントがかかります。 (409)

専門的な(specialist)方法または技法の要求が含まれる高位保証要件では、STにおいて特定の詳細な保証手段を識別する。 (410)

A.7 PP根拠の構成

A.7.1 セキュリティ対策方針の根拠

各脅威、OSP及び前提条件が少なくとも1つのセキュリティ対策方針によって対応されることを示す表(または他の適している方法)の手段による脅威、組織のセキュリティ方針及び前提条件へのセキュリティ対策方針のマッピングを実証する。 (411)

各脅威、OSP及び前提条件については、なぜ識別されたセキュリティ対策方針がそれらをカバーするのに適しているか論証でこれを補う。 (412)

A.7.2 セキュリティ要件の根拠

TOEの各セキュリティ対策方針が少なくとも1つのSFRによって対応されることを示す表(または他の適している方法)の手段によるセキュリティ対策方針へのSFRの対応を実証する。 (413)

TOEの各セキュリティ対策方針については、なぜ識別されたセキュリティ要件がそれらを満たすのに適しているか論証でこれを補う。 (414)

ISO/IEC 15408コンポーネントの依存性が満足されること(または、依存性が無視される場合、正当化が提供される)、SFRが競合しないこと、そしてSFRの間のあらゆる追加の補助的依存性のハイライトを示すことによって相互サポート(mutual support)を実証する、例えば干渉されまたは非活性化(de-activated)されて、他のSFRが迂回されるのを妨げるSFR。 (415)

A.8 ST根拠の構成

A.8.1 セキュリティ対策方針及びセキュリティ要件の根拠

上記のA.7節に与えられたガイダンスに従うことによりST根拠のこれらの部分を提示する。PPへの適合が主張される場合、ST根拠はSTセキュリティ対策方針及びITセキュリティ要件へ導入されたあらゆる追加的な詳細の影響に対して焦点をあてるべきである。 (416)

A.8.2 TOE要約仕様の根拠

少なくとも1つのITセキュリティ機能または保証手段によって各SFR及びSARが適切に対応されることを示す、表(または他の適している方法)の手段による、SFRへのITセキュリティ機能及びSARへの保証手段のマッピングを実証する。 (417)

附属書B 一般的な例

この附属書は脅威、組織のセキュリティ方針、前提条件、及びセキュリティ対策方針の例のリストである。共通的な、または一般的なセキュリティ機能要件を特定するために利用されるISO/IEC 15408パート2機能コンポーネントに関するガイダンスも提供する。 (418)

ここでの意図は、多数のPP及びSTの間での一貫性を促進するといった視点から、脅威、OSP、前提条件、そしてセキュリティ対策方針の、特定のしかたと命名規約について説明することである。以下のことが注意されるべきである： (419)

- a) 本附属書はSTまたはPPで利用できそうな、より一般的なステートメントのいくつかを識別している。これは、決して網羅的なチェックリストを提供するものではなく、PPまたはSTで利用するために、追加のステートメントを識別する必要がある可能性が非常に高い。
- b) この例はコピーされ、そのままの語句で利用できるが、PPまたはSTでの利用のために、言い回しに対して改作または拡張が必要かどうか、常に考慮すべきである。
- c) ここでリストされるすべてのステートメントが、任意のPPまたはSTに適切であるわけではない。

イタリック体の文字は、一般用語(例えば、脅威エージェントや保護を必要とするIT資産)がPPまたはSTに特有の適切な専門用語で置き換えられるであろう箇所を表すために使用される。 (420)

暗号機能性の特定(一般的な脅威とセキュリティ対策方針からの導出を含めて)についてのガイダンスが附属書Cに提供されている。 (421)

B.1 脅威の例

T.ABUSE	TOE の許可利用者が(故意または他の理由で)、その個人が実行することを許可されているアクションを実行する結果、IT 資産が危険にさらされることが、検出されることなく起こる。
T.ACCESS	TOE の許可利用者が情報または資源の所有者または責任者の許可なく、情報または資源にアクセスする。
T.ATTACK	(部外者または部内者である)攻撃者が、その個人が実行することを許可されていないアクションを実行しようと試みる結果、IT 資産が危険にさらされることが、検出されることなく起こる。
T.CAPTURE	攻撃者が、ネットワークを通して転送中のデータを盗み見る、もしくは取り込む。
T.CONSUME	TOE の許可利用者が、他の許可利用者がそれらの資源にアクセスまたは利用するための能力を危険にさらすような方法で、グローバルな資源を使い尽くす。
T.COVERT	TOE の許可利用者が、秘匿情報を故意または偶然に、それを見ることに支障がある利用者に対して、(隠れチャンネルを通して)転送する。
T.DENY	利用者が(発信者または受信者のどちらかとして)情報の転送に関与した後、それを行ったことを否定する。
T.ENTRY	許可利用者が、不適切な時間帯に、または不適切な場所から TOE を利用し、その結果 IT 資産が危険にさらされる。
T.EXPORT	TOE の許可利用者が、情報を TOE から外部に(ソフトコピーまたはハードコピーの形で)エクスポートし、受信者はその後、秘匿指定に一致しないやり方で取り扱う。
T.IMPERSON	(部外者または部内者である)攻撃者が、TOE の許可利用者に成りすまし、情報または資源への許可されないアクセスを得る。
T.INTEGRITY	利用者エラー、ハードウェアエラー、または転送エラーにより、情報の完全性が危険にさらされる。
T.LINK	攻撃者が、エンティティによる資源やサービスの複数の利用を観察することができ、さらに、それらの利用を結びつけることにより、そのエンティティが機密として保持することを望む情報を推定することができる。
T.MODIFY	攻撃者による情報の許可されない改変または破壊により、情報の完全性が危険にさらされる。

T.OBSERVE 利用者の資源またはサービスの正当な利用を、その利用者が自身の資源またはサービスの利用を機密にしたい場合に、攻撃者が観察することができてしまう。

T.SECRET TOE の許可利用者が、故意または偶然に、TOE に保存されている情報の内、その利用者が見られることを許可されていないものを観察する。

以下の脅威は概して、TOEよりはむしろ環境のセキュリティ対策方針で対応されるだろう。 (422)

TE.CRASH 人為的エラー、またはソフトウェア、ハードウェア、または電源の故障により、TOE の運用が突然中断し、その結果セキュリティ上重大なデータの消失または破壊が引き起こされる。

TE.BADMEDIA 記憶媒体の老朽化、またはリムーバブル媒体の不適切な保管または取り扱いの結果、媒体の破壊が起こり、セキュリティ上重大なデータの消失または破壊を導く。

TE.PHYSICAL セキュリティ上重大な TOE のパーツが物理攻撃の対象になり、セキュリティが危険にさらされる。

TE.PRIVILEGE 不注意な、故意に怠慢な、または悪意のある、管理者または他の特権利用者により取られるアクションの結果、IT 資産が危険にさらされる。

TE.VIRUS TOE の許可利用者が、知らないうちに、システムにウィルスを導入してしまい、その結果、IT 資産の完全性及び/または可用性が危険にさらされる。

B.2 組織のセキュリティ方針の例

この節では2つの典型的な例が提供されている。特定の組織はもちろん、以下に提示されるものより詳細なセキュリティ方針をもっているであろう。 (423)

P.DAC 特定のデータオブジェクトにアクセスする権利は以下に基づいて決定される：

- a) オブジェクトの所有者；及び
- b) アクセスを試みるサブジェクトの識別情報；及び
- c) オブジェクトの所有者により、サブジェクトに対して認められた明示的な及び非明示的なアクセス権限。

P.MAC 秘匿指定のマークを付けられた情報へアクセスする権利は以下のように決定される：

- a) 個人は、その個人が見ることに支障がない場合に限り、情報を観察することを許される。

- b) 個人は、その個人がそれを行うための明示的な許可を与えられない限りは、情報の秘匿指定の等級を下げることはできない。

B.3 前提条件の例

B.3.1 物理的前提条件

A.LOCATE TOE の処理資源は、管理されたアクセス設備内に設置され、許可されない物理的アクセスを妨げるものと仮定される。

A.PROTECT セキュリティ方針の実施に重大な TOE のハードウェア及びソフトウェアは、潜在的な敵意のある部外者による許可されない改変から、物理的に保護されるものと仮定される。

B.3.2 人的前提条件

A.ADMIN TOE 及び TOE に含まれる情報のセキュリティを管理するために十分な能力を持ち、特権を故意に悪用し、セキュリティを不正に蝕むようなことがないと信頼できる、1人以上の許可された管理者が割り当てられていると仮定する。

A.ATTACK 攻撃者は高レベルの専門技術、資源、及び動機をもっていると仮定される。

この前提条件は、TOEのセキュリティ環境に対して適切になるよう改作することができる。この種類の前提条件は脅威の定義に利用され、例えば特定のレベルの専門技術、動機または利用可能な資源をもつ脅威エージェントからの攻撃の可能性を排除することで、脅威の範囲を制限することに注意されたい。 (424)

A.USER TOE の利用者は、TOE により管理される情報へアクセスするために必要な特権を、所有するものと仮定する。

B.3.3 接続性前提条件

A.DEVICE 記憶デバイスへのすべての接続は、管理されたアクセス設備内に存在すると仮定する。

A.FIREWALL ファイアウォールは、プライベートネットワークと敵意のあるネットワーク間の唯一のネットワーク接続として設定されると仮定される。

A.PEER TOE が通信を行ういかなるシステムも、同一の管理制御下にあり、同一のセキュリティ方針の制約のもとで動作すると仮定される。

B.4 TOEのセキュリティ対策方針の例

- O.ADMIN TOE は許可された管理者が、TOE とそのセキュリティ機能を効果的に管理できるようにするための設備を提供し、許可された管理者のみがそのような機能性にアクセスできることを保証する。
- O.ANON TOE は利用者識別情報が他のエンティティに暴露されることなしに、サブジェクトが資源及びサービスを利用することを許す手段を提供する。
- O.AUDIT TOE はセキュリティに関連する事象を記録する手段を提供し、管理者が攻撃の可能性または、TOE が攻撃を受けやすい状態となるようなセキュリティ機構(feature)の設定ミスを検出することで管理者を助け、そして利用者がセキュリティに関連して遂行するいかなるアクションに対しても責任をもたせる状態を維持する。
- O.DAC TOE はその利用者に対して、個人利用者または識別された利用者のグループに基づき、また P.DAC セキュリティ方針で定義される規則のセットに従い、利用者が所有するまたは責任をもつオブジェクトや資源に対するアクセスを、制御及び制限する手段を提供する。
- O.ENCRYPT TOE は、ネットワークを介した2つのエンドシステム間での転送時に、*情報*の機密性を保護する手段を提供する。
- O.ENTRY TOE は、時間とエントリーするデバイスの場所を基に、利用者のエントリーを制限する能力をもつ。
- O.I&A TOE は、すべての利用者を一意に識別し、利用者が TOE の設備にアクセスすることを許可する前に、主張された識別情報を認証する。
- O.INTEGRITY TOE は、*情報*に及ぼされる完全性の損失を検出する手段を提供する。
- O.LABEL TOE は、TOE が保存及び処理する情報の秘匿ラベルの完全性を、保持及び維持する。TOE による(エクスポートされる)データ出力は、内部秘匿ラベルの正確な表現である秘匿ラベルをもつ。
- O.MAC TOE は、情報に対する個人の取扱許可(clearance)または許可(authorisation)と、その情報の秘匿指定との比較に直接基づき、P.MAC セキュリティ方針に従って、TOE が管理する責任をもつ情報の機密性を保護する。

このセキュリティ対策方針はもちろんあらゆる特定の情報フロー制御方針の対策方針に対して適切に訂正することができる。

(425)

- O.NOREPUD TOE は、*情報の発信者が情報を送信したことをまふと否定することを防ぐための証拠、及び情報の受信者が情報を受信したことをまふと否定することを防ぐための証拠を生成するための手段を提供する。*
- O.PROTECT TOE は、信頼できないサブジェクトによる外部からの妨害または改ざん、または信頼できないサブジェクトによるセキュリティ機能迂回の試みから自分自身を保護する。
- O.PSEUD TOE は、利用者識別情報が他のエンティティに暴露されることなく、サブジェクトが*資源またはサービス*を利用することを可能にし、さらにその利用に対するエンティティの責任を維持する手段を提供する。
- O.RBAC TOE は、利用者が、その利用者の役割に対して明示的な許可がない資源に対してアクセスを得ること、及び操作を実行することを防ぐ。
- O.RESOURCE TOE は、その利用者及びサブジェクトによる*資源*の利用を制御し、不当なサービス拒否を防ぐ手段を提供する。
- O.ROLLBACK TOE は、トランザクションの系列が不完全な場合、利用者にトランザクションを取り消すことを許可することにより、明瞭に定義された有効な状態に戻る手段を提供する。
- O.UNLINK TOE は一つのエンティティに資源またはサービスの複数利用を許し、他のエンティティがそれらの利用を結びつけることができないようにする手段を提供する。
- O.UNOBS TOE は*利用者が資源またはサービス*を利用し、他のエンティティがその*資源またはサービス*が利用されていることを観察することができないようにする手段を提供する。

B.5 環境のセキュリティ対策方針の例

- OE.AUDITLOG TOE の管理者は監査設備が有効に利用及び管理されていることを保証しなければならない。とりわけ以下のように：
 - a) 連続的な監査ログ収集を保証するために、適切なアクションが取られなければならない。例えば、監査証跡が枯渇する前に、十分な空き容量を保証する規則正しいログのアーカイブにより。
 - b) 監査ログは一定の基準で検査されるべきであり、そしてセキュリティ違反または将来セキュリティ違反を導きそうな事象を検出した場合、適切なアクションが取られなければならない。

- OE.AUTHDATA TOE に対して責任をもつ者は、各利用者の TOE に対する利用者アカウントの認証データが、セキュアに保持され、そのアカウントの利用を許可されていない利用者に対して暴露されないよう、保証しなければならない。
- OE.CONNECT TOE に対して責任をもつ者は、セキュリティを蝕もうとする外部システムまたは利用者との接続が、提供されないことを保証しなければならない。
- OE.INSTALL TOE に対して責任をもつ者は、IT セキュリティを維持するようなやり方で、TOE が配付され、インストールされ、管理され、そして運用されることを保証しなければならない。
- OE.PHYSICAL TOE に対して責任をもつ者は、IT セキュリティを危険にさらす恐れのある物理的攻撃から、TOE のセキュリティ方針の実施に重大な TOE のパーツが保護されることを保証しなければならない。
- OE.RECOVERY TOE に責任をもつ者はシステムの故障またはその他の中断の後、IT セキュリティが危険にさらされることなく回復できることを保証するための、手続き及び/またはメカニズムが適当であることを保証しなければならない。

B.6 セキュリティ対策方針から脅威へのマッピングの例

[編集者注：以下の表は、脅威から TOE または環境のセキュリティ対策方針へのマッピングがどのように作成されるかの例として提案された。表の各欄は、脅威またはセキュリティ対策方針の形態を示しているが、必ずしも脅威及びセキュリティ対策方針の特定に関連する他の箇所で提供されるガイダンスに適合するものではない。]

(426)

Asset	Threat	Security Objectives	
Data on storage media	Data is disclosed by illegally removing a medium.	Preventative	Control media removal. Prevent data disclosure (by encryption, etc.)
		Detective	Control media storage.
		Corrective	-
	Data is referenced, modified, deleted, or added from/to an application by an unauthorized person.	Preventative	Operation management (For example, restrict uses of an application program or an application terminal) Control the privilege to access data.
		Detective	Audit application operation log information, detect data tampering, and manage data sequence numbers.
		Corrective	Back up/Restore data.
	Data is disclosed by dumping a storage medium by an unauthorized person.	Preventative	Operation management (For example, restrict uses of a dump function or an operation terminal) Prevent data disclosure (by encryption, etc.)
		Detective	Audit operation log information.
	Remaining data on a medium is referenced.	Preventative	Clear the data area at the time of data deletion. Prevent data disclosure (by encryption, etc.)
	Data is copied illegally.	Preventative	Operation management (For example, restrict uses of a copy function or an application/operation terminal) Control the privilege to access data. Prevent data disclosure (by encryption, etc.)
		Detective	Audit operation. Control the original (such as electronic watermark)
	Data is illegally used or its use is obstructed by changing the data access attribute by an unauthorized person.	Preventative	Operation management (For example, restrict uses of a data attribute modify function or an application/operation terminal) Control the privilege to access an attribute registration file.
		Detective	Audit operation.
		Corrective	Back up/Restore data.
	Data is got illegally by forging a file	Preventative	Operation management (For example, restrict uses of file create and delete functions or an operation terminal) Prevent data disclosure (by encryption, etc.)
Detective		Audit file owners.	

表3 - 脅威からセキュリティ対策方針へのマッピングの例

Asset	Threat	Security Objectives	
Data on storage media	Data is damaged by destruction of the medium.	Preventative	Physically manage the medium storage place and control access to the storage place. Adopt a dual configuration for storage media.
		Detective	Control media storage.
		Corrective	Back up/Restore data.
	Data is destroyed or its use is obstructed by a hardware failure of a medium I/O device	Preventative	Quality control of I/O devices Adopt a dual configuration for storage media.
		Detective	Detect failures (OS). Audit program execution log.
		Corrective	Back up/Restore data.
	Data is referenced, modified, deleted, or added by an unauthorized person using a command.	Preventative	Operation management (For example, restrict uses of operation commands or an operation terminal) Control the privilege to access data.
		Detective	Audit operation log information. detect data tampering, and manage data sequence numbers.
		Corrective	Back up/Restore data.
	Encrypted data cannot be decrypted due to loss of the secret key.	Preventative	Keep the secret key under strict management.
		Corrective	Recover the secret encryption key.
	Data is erroneously deleted by an authorized person.	Preventative	Provide high-quality operation manuals or automate operations. Prevent operating errors (for example, rechecking and sequentially registering the privilege to delete).
Detective		Audit operation log information.	
Corrective		Back up/Restore data.	
Data on tele-communication line	Data is tapped or destroyed on a telecommunication line	Preventative	Physically protect telecommunication lines or control equipment connections to lines. Prevent data disclosure, detect data tampering (by encryption transmitted data: VPN, SSL, IP sec, etc.)
		Detective	Detect data tampering.
		Corrective	Send data again.
	Data is tapped, tampered, deleted or added on a relay system.	Preventative	Operation management of a relay system (For example, restrict uses of LAN protocol analyser)

表3 - 脅威からセキュリティ対策方針へのマッピングの例

Asset	Threat	Security Objectives	
Data on tele-communication line	Data is illegally used by changing its destination, sender, or access attribute on a relay system.	Preventative	Protect control data to be transmitted (by encryption, etc.) Operation management of a relay system (Restrict uses of a debug function.)
		Detective	Detect control data tampering. Audit debug tool operation log information.
		Corrective	Send data again.
	Communications are disabled due to a line fault.	Preventative	Install dual telecommunication lines. Quality control of telecommunication lines
		Detective	Detect failures (OS).
		Corrective	Send data again.
	Communications are disabled due to a communication channel abnormality.	Preventative	Install dual channel devices. Quality control of communication channels
		Detective	Detect failures (OS).
		Corrective	Send data again.
	Data is illegally resent for illegal communications.	Preventative	Operation management of a relay system (For example, restrict program registration.)
		Detective	Prevent re-transmission (by assigning sequence numbers or time)
	Application program	An application is executed by an unauthorized person.	Preventative
Detective			Audit program execution.
Corrective			Related data backup/restore.
Data in a program library is referenced, modified or deleted by an unauthorized person.		Preventative	Control the privilege to access a program library. Operation management (Restrict uses of a modify command.) Restrict uses of an operation terminal.
		Detective	Audit operation
		Corrective	Back up/Restore program.
A program is illegally used or its use is obstructed by changing its access attribute by an unauthorized person.		Preventative	Control the privilege to execute a program. Control the privilege to access the program library directory. Operation management (Restrict uses of a modify command.)
		Detective	Audit operation.

表3 - 脅威からセキュリティ対策方針へのマッピングの例

Asset	Threat	Security Objectives	
Application program	An abnormality occurs during program execution due to a hardware failure of a computer.	Preventative	Adopt a dual hardware configuration. Quality control of hardware
		Detective	Detect failures (OS).
		Corrective	Hardware recovery
Application processing and data	Illegal application processing (such as Telnet and FTP) is executed.	Preventative	Control the privilege to execute a program. Firewall (application filtering) Clarify operation regulations.
		Detective	Audit program execution.
	Processing is obstructed (traffic attack such as requesting to process unnecessary data).	Preventative	Give priority to process processing. Prohibit a mail relay function.
		Detective	Audit network access.
	Data exchange or contents are denied.	Preventative	Take measures for preventing denial (such as storing an evidence using TTP or encryption function). Clarify operation rules.
	The original of data is denied.	Preventative	Reliable services (such as guarantee of an original) Clarify operation rules.
	Data is illegally sent.	Preventative	Control data flows (such as Firewall and rule DB control). Control the quality of application programs. Operation management (For example, restrict program registration.)
		Detective	Audit data access.
	Data or a program is illegally used using a remaining debug function.	Preventative	Control the privilege to access data and the privilege to execute a program. Operation management (Restrict uses of a debug function.)
		Detective	Audit application execution.
	A service function is inappropriately denied.	Preventative	Give priority to process processing. Control the quality of application programs. Provide education and regulations for application staff. Control the quality of processing hardware. Estimate the capacity of processing resources.
		Detective	Audit application execution.
	Contents are tampered or destroyed.	Preventative	Control the privilege to use contents. Control contents creation and downloading.
		Detective	Detect contents tampering.
		Corrective	Back up contents.

表3 - 脅威からセキュリティ対策方針へのマッピングの例

Asset	Threat	Security Objectives	
Application processing and data	Illegal operation	Preventative	Control the privilege to execute operations. Control the locations and routes of operations (remote, via Internet, etc.).
		Detective	Audit use of operations.
	Privacy is violated.	Preventative	Control the privilege to use privacy information. Use anonymity or a pen name (pseudonym). Guarantee unlinkability.
Display data	Data is seen by an unauthorized person.	Preventative	Isolate a display physically. Enforce operation rules.
	Illegal copy or printing	Preventative	Provide safeguards against an authorized person's absence. Restrict uses of copy and print functions. Enforce operation regulations.
		Detective	Control originals (electronic watermark)
Input data	Data is disclosed during input.	Preventative	Control access to an input terminal room. Enforce operation regulations.
	Input data is illegally taken out.	Preventative	Control the input data storage place. Enforce operation regulations.
		Corrective	Back up input data.
Printed data	Data is referenced or taken out by an unauthorized person.	Preventative	Physically control printed data. Enforce operation regulations.
	Illegal copy	Preventative	Provide safeguards against copying. Enforce operation regulations.
		Detective	Control originals (electronic watermark)
User data	A user (individual, system, terminal) cannot be identified.	Preventative	Identification at access Identification (ID assignment to each user/system; IP address) Restrict locations (filtering).
		Detective	Audit identification processing.
	Disguise oneself using disclosed user (individual, system, terminal) identification information.	Preventative	User authentication Control identification information.
		Detective	Audit identification processing.
	A user is not identified.	Preventative	Prompt authentication Reliable identification. Authentication (encryption, secret key, password, belongings, physical characteristics) Call back
		Detective	Audit authentication processing.

表3 - 脅威からセキュリティ対策方針へのマッピングの例

Asset	Threat	Security Objectives	
User data	Disguise oneself using illegally disclosed authentication information.	Preventative	Adopt multiple authentication mechanisms. Server access management (Early detection by a victim; notification of authentication processing information) Save authentication information in a confidential medium. Protect authentication information (unidirectional encryption). Restrict access routes (such as public telecommunication lines and the Internet). One-time password
		Detective	Audit system access
		Corrective	Stop processing by the user.
	Disguise oneself by illegally inferring authentication information.	Preventative	Authentication (Preventing inference; limiting retry count) Server access management (Early detection by a victim; safeguards for not using a server for a long period) Adopt multiple authentication mechanisms. Control authentication information (such as preventing inference, long secret encryption key, syntax rules, initial value change, and generation control)
		Detective	Audit system access
		Corrective	Stop processing by the user. Minimize influences (Effective period).
	Disguise oneself using invalid authentication information.	Preventative	Confirm validity of authentication information. Control authentication information (such as control nullified information).
		Detective	Audit system access
	An invalid privilege is used because of failure to register a modification of user privilege.	Preventative	Control users. (Immediately reflect a user privilege modification.)
		Detective	Audit system access
	A user's action is illegally disclosed (violation of privacy).	Preventative	Manage privilege to access user related log information. Use anonymity or a pen name (pseudonym). Guarantee unlinkability
		Detective	Audit system access
	Data transmission is denied.	Preventative	Prevent denial of transmission. Operation regulations.
		Detective	Audit data exchange.
Data ownership is denied.	Preventative	Automatically register an owner at the time of data production.	
	Detective	Audit system access.	

表3 - 脅威からセキュリティ対策方針へのマッピングの例

Asset	Threat	Security Objectives	
User data	Data reception is denied.	Preventative	Prevent denial of reception. Operation regulations.
		Detective	Audit data exchange
	Data is sent to a wrong receiver due to disguise or a specification error.	Preventative	Destination authentication. Operation regulations.
		Detective	Audit data exchange
	Disguise oneself by forging authentication information.	Preventative	Manage privilege to access authentication information. Verify validity of authentication information. Control authentication information (such as preventing forging, reliable authentication organization, physically protecting belongings).
		Detective	Server access management (Early detection by a victim)
System Services and Data	A secret encryption key is decoded, undermining system security	Preventative	Produce a secret encryption key of sufficient strength and length and adopt a standard key delivery protocol.
		Detective	Audit system operations.
		Corrective	Set a new secret key.
	A system is illegally used by a disguised user during an operator's absence.	Preventative	Provide the necessary safeguards during an operator's absence (such as suspension, session disconnection, and re-authentication).
	System security is undermined by an authorized user's illegal act or mistake.	Preventative	Prevent an authorized user's mistakes (for example, by reconfirmation). Control user privileges (minimum privileges). Audit management, regulations, education, and penalties.
		Detective	Audit system operations
	Virus intrusion	Preventative	Virus check for program downloading and files with mail. Access control (Set an appropriate access privilege and protect files.) Prohibit loading data or program from the outside. Control software installation.
		Detective	Audit system operations
		Corrective	Take the necessary action (such as stopping the system and disconnecting an external system).

表3 - 脅威からセキュリティ対策方針へのマッピングの例

Asset	Threat	Security Objectives	
System Services and Data	Illegal intrusion to a system	Preventative	Check a user's identification, authentication, and privilege (at the time of accessing a barrier segment or log-in). System configuration management (such as connected equipment and external connections) User management.
		Detective	Audit system operations.
	Intrusion to a system by taking advantage of a known protocol defect (such as IP protocol and SendMail)	Preventative	Firewall (Filtering) Control access to system resources. Restrict access to the program or protocol.
		Detective	Audit system operations
	System security is undermined by illegal replacement of a system program.	Preventative	Control access to a system program library. Operation management (System program maintenance regulations)
		Detective	Audit program library access.
		Corrective	Back up programs.
	The service is stopped by system program destruction.	Preventative	Adopt a dual configuration for system program library. Medium management and operation management (system program library)
	Illegal system operation	Preventative	Control the privilege to execute operation commands. Operation management (Restrict uses of operation commands.)
		Detective	Audit operations.
Information equipment	Damaged or taken out.	Preventative	Dual configuration Control the access to the equipment location. Keep equipment (lines) under management during storage.
		Preventative	Backup power supply UPS
	Corrective	Recover power.	

表3 - 脅威からセキュリティ対策方針へのマッピングの例

B.7 セキュリティ機能要件の例

この章は、共通的または一般的なセキュリティ機能の例として、適切なSFRを表現するために利用されるであろうISO/IEC 15408パート2コンポーネントを識別する。読者はISO/IEC 15408パート2附属書を特定のISO/IEC 15408パート2機能コンポーネントの利用についてのガイダンスとして参照される。暗号機能性の特定のガイダンスとして附属書Cも参照。 (427)

これらの共通的または一般的なセキュリティ機能は、以下の見出しで体系付けられる (428)

- a) 識別と認証
- b) アクセス制御
- c) 監査
- d) 完全性
- e) 可用性
- f) プライバシー
- g) データ交換

B.7.1 識別と認証要件

下記の表4は共通的または一般的な識別と認証要件をカバーする。

(429)

[【ISO/IEC JTC 1/SC 27 N3816改訂情報】：段落429、表4は以下に示すとおりFIA_UAU.3、FIA_UAU.4、FTP_TPR.1に対応するSecurity RequirementとしてReplay/reusegaという記述が追加される。](#)

Security Requirement		Functional Component
Logon controls	Identification of users	FIA_UID.1-2
	Authentication of users	FIA_UAU.1-2
	Limits on repeated login failures (e.g. enforcement of lockout or time delay)	FIA_AFL.1
	Trusted path for logon	FTP_TRP.1-2
	Time of day restriction of access to TOE	FTA_TSE.1
Password selection	Controls on selection of user-generated passwords (e.g. minimum length, password filters, password history)	FIA_SOS.1
	Automated generation of passwords by TOE	FIA_SOS.2
	Password lifetime (expiry) enforcement	FMT_SAE.1
Authentication data protection	Non-echoing of passwords during password entry	FIA_UAU.7
	Protection against unauthorised modification or observation	FMT_MTD.1
	Protection against replay attacks	FPT_RPL.1
Replay/reuse	Protection against forgery or copying	FIA_UAU.3
	Protection against reuse (e.g. single use passwords)	FIA_UAU.4

表4 - 識別と認証機能要件機能コンポーネント

Security Requirement		Functional Component
Replay/reuse	Trusted path for password change	FTP_TRP.1
Session suspension	Suspension following user inactivity	FTA_SSL.1
	Suspension at user request	FTA_SSL.2
	Termination following user inactivity	FTA_SSL.3
User accounts and profiles	Controls over creation, deletion, enabling or disabling of user accounts	FMT_MTD.1
	Definition of user security attributes contained in a user profile	FIA_ATD.1
	Controls over modification of user profiles (i.e. user security attributes)	FMT_MTD.1

表4 - 識別と認証機能要件機能コンポーネント

B.7.2 アクセス制御要件

下記の表5は共通的または一般的なアクセス制御要件をカバーする。

(430)

Security Requirement		Functional Component
Discretionary Access Control	Scope of policy (subjects, objects and operations covered by the policy)	FDP_ACC.1-2
	Rules governing access by subjects to objects	FDP_ACF.1
	Privilege override of DAC policy	FDP_ACF.1
Controls on DAC attributes	Changing object permissions/ACLs	FMT_MSA.1
	Default protection on newly created objects	FMT_MSA.3
	Changing object owner	FMT_MSA.1
	Changing user group affiliations	FMT_MSA.1
Mandatory Access Control	Scope of policy (subjects, objects and operations covered by the policy)	FDP_IFC.1-2
	Rules governing access/information flow	FDP_IFF.2
	Privilege override of MAC policy	FDP_IFF.7-8
	Covert channel restrictions	FDP_IFF.3-6
Controls on MAC attributes	Changing object labels	FMT_MSA.1
	Default labels for newly created objects	FMT_MSA.3
	Changing user clearances	FMT_MSA.1
	Selection of session clearance at login	FTA_LSA.1
Export/import	Import of unlabelled data	FDP_ITC.1
	Export via communication channels/devices	FDP_ETC.1-2
	Labelling printed output	FDP_ETC.2

表5 - アクセス制御要件の機能コンポーネント

Security Requirement		Functional Component
Information labels	Constraints on information label values	FDP_IFF.2.3
	Rules governing 'floating' labels	FDP_IFF.2.3
Object reuse	Protection of residual information in files, memory, etc.	FDP_RIP.1-2
Role based access control	Scope of policy (in terms of roles, operations)	FDP_ACC.1-2
	Rules controlling performance of operations	FDP_ACF.1 ^a
	Identification of roles	FMT_SMR.1-2
	Two-man rule enforcement	FDP_ACF.1 ^b FMT_SMR.2.3
Controls on RBAC attributes	Changing user privileges/authorisations	FMT_MSA.1
	Changing definitions of role capability	FMT_MSA.1
	Changing assignments of users to roles	FMT_MSA.1
Firewall access control	Subject-object information flow view (e.g. based on source/destination addresses and ports)	FDP_IFC.1-2 FDP_IFF.1
	Session-based view (e.g. application proxy)	FTA_TSE.1 ^c

表5 - アクセス制御要件の機能コンポーネント

- a. 明確に識別された役割に対する特定の操作の実行の制限に役立つ、他のコンポーネント(例えば、FMT_MOF.1、FMT_MSA.1、FMT_MTD.1)も存在する。
- b. FDP_ACF.1は、特定の操作がアクションを認証するための2つの異なる役割を要求する事を特定するために使用されるだろう。FMT_SMR.2.3は1つの利用者アカウントが両方の役割に割り当てることができないことを保証することができる。
- c. 附属書Dの作業例を参照。FDP_IFC.1とFDP_IFF.1は二者択一的に使用されるだろう。

B.7.3 監査要件

下記の表6は共通的または一般的な監査要件をカバーする。

(431)

Security Requirement		Functional Component
Audit events	Specification of auditable events and information to be recorded	FAU_GEN.1
	Controls on selection of events to be audited	FMT_MTD.1
	Basis for selection of events to be audited	FAU_SEL.1
	Individual accountability of users	FAU_GEN.2

表6 - 監査要件の機能コンポーネント

Security Requirement		Functional Component
Intrusion detection and response	Generation of alarms and response to imminent security violations	FAU_ARP.1
	Definition of rules, events, event sequences or patterns of system usage to be used to indicate potential or imminent security violations	FAU_SAA.1-4
Audit trail protection	Protection against loss of data e.g. due to audit trail saturation, interruptions to operation	FAU_STG.2-4
	Protection against unauthorised modification/ access	FAU_STG.1
Audit trail analysis/review	Provision of audit trail analysis/review tools	FAU_SAR.1-3

表6 - 監査要件の機能コンポーネント

B.7.4 完全性要件

下記の表7は共通的または一般的な完全性要件(データ認証も含め)をカバーする。

(432)

Security Requirement		Functional Component
Data integrity	Detection of errors in stored data	FDP_SDI.2
	Generation and verification of checksums, one-way hash, message digest, etc.	FDP_DAU.1
	Rollback of transactions (e.g. database)	FDP_ROL.1-2
TOE integrity	Tamper detection	FPT_PHP.1-2
	Tamper resistance	FPT_PHP.3
Data authentication	Digital signature generation and verification	FDP_DAU.2
	Certificate generation and verification (e.g. public key certificates)	FDP_DAU.2

表7 - 完全性要件の機能コンポーネント

B.7.5 可用性要件

下記の表8は共通的または一般的な可用性要件をカバーする。

(433)

Security Requirement		Functional Component
Consumption of resources	Enforcement of limits/quotas on global resource consumption by users	FRU_RSA.1-2
	Limitation on number of logged in sessions by same user	FTA_MCS.1-2
Error handling	Maintenance of TOE operation in event of failures (fault tolerance)	FRU_FLT.1-2
	Error detection	FPT_TST.1
	Error recovery	FPT_RCV.1-4
Scheduling	Scheduling of activities/processes according to established priorities	FRU_PRS.1-2

表8 - 可用性の要件機能コンポーネント

B.7.6 プライバシー要件

下記9は共通的または一般的なプライバシー要件をカバーする。

(434)

Security Requirement		Functional Component
User identity based privacy	Protection against disclosure of user identity when using services or resources	FPR_ANO.1-2
	Anonymous but accountable use of services or resources via a protected user alias	FPR_PSE.1-3
Resource/service based privacy	Protection against disclosure of linkage of multiple usage of resources or services to the same user	FPR_UNL.1
	Unobservable usage of specified resources or services	FPR_UNO.1-4

表9 - プライバシーの要件の機能コンポーネント

B.7.7 データ交換要件

下記の表10は共通的または一般的なデータ交換要件を識別する。

(435)

Security Requirement		Functional Component
Data exchange confidentiality	User data	FDP_UCT.1
	Security critical data, e.g. keys, passwords	FPT_ITC.1
Data exchange integrity	User data	FDP_UIT.1-3
	Security critical data, e.g. keys, passwords	FPT_ITI.1-2
Non-Repudiation	Proof of origin of exchanged information	FCO_NRO.1-2
	Proof of receipt of exchanged information	FCO_NRR.1-2

表10 - データ交換要件の機能コンポーネント

附属書C 暗号機能性の特定

C.1 序説

C.1.1 目的と範囲

この附属書には、評価対象 (TOE) の暗号の側面に対するプロテクションプロファイル (PP) とセキュリティターゲット (ST) 構築のためのガイダンスを載せたが、暗号モジュール (実効的には暗号機能の集まり) そのものであるTOEだけが対象にされているわけではない。とは言っても、このガイダンスは、暗号モジュールそのものであるTOEへの適用も一緒にした形で書かれている。広範囲のTOEをカバーし、かつそのような機能性の仕様に関する特定の問題を扱えるようなガイダンスが含まれている。 (436)

この附属書の目的は、暗号機能性とそれによるセキュリティ要件のサポートをどのように特定するかガイダンスを提供することである。暗号に対するガイダンス、または暗号機能性を使用してどのようにセキュアなシステムを構築するかガイダンスを提供しようとするものではない。 (437)

FCS (暗号サポート) クラスに含まれる個々の機能コンポーネント適用についてのガイダンスは、[15408-2]附属書Eで提供される。暗号機能性は、他のクラスまたはファミリー (例えば、FCOクラス、FDP_DAU、FDP_SDI、FDP_UCT、FDP_UIT、FIA_SOS、FIA_UAUファミリー) を用いて特定されるSFRを満たすために使うことができる。そのような場合、個々の機能コンポーネントは、暗号機能性が満たさねばならないセキュリティ要件を特定する。FCSクラスに対応するセキュリティ対策方針は、TOEのその暗号機能性が消費者によって求められたときに使われるべきである。 (438)

特定の保証要件がこの文書で論じられることはあるが、このガイダンスの範囲には暗号強度の解説を含めておらず、それは実際の保証レベルにおいても同様である。TOEに対する保証要件は、そのアプリケーションの秘密の度合いと、保証要件によって効果的に對抗できると予想される脅威及び脆弱性に基づいて決定されるべきものである。これは、本ガイドの5章で詳細に論じられる。 (439)

[【ISO/IEC JTC 1/SC 27 N3816改訂情報】：以下に示すとおり参考文献に関する記述が追加される。](#)

[暗号と暗号アルゴリズムの追加情報及び追加ガイダンスは、\[4\]、\[5\]、\[6\]、\[7\]、\[8\]、及び\[9\]で調べることができる。](#)

C.1.2 用語

この附属書で使われる用語は、[15408-1] 2項及びISO/IEC DIS 2382 [ISO-2382]で定義されたものに基づく。加えて、この文書で提示される概念の理解補助のため、以下の用語を定義する： (440)

アクセスモード (Access Mode) — アクセス権によって特定される操作の種別。例: 読み出し、書

- き込み、実行、付加、修正、削除、生成など。[ISO-2382]におけるアクセス種別も参照。 (441)
- ブラックデータ (Black Data)** — その情報コンテンツが暗号化によって保護され、簡単にアクセスすることができないデータ。データの例として、メッセージ、ファイル、暗号鍵などがある。 (442)
- 暗号アルゴリズム (Cryptographic Algorithm)** — データ入力を、暗号鍵や初期化ベクターのような他の入力パラメータに基づき、ある出力へ変換する数学的規則のセット。 (443)
- 暗号チェックサム (Cryptographic Checksum)** — 暗号アルゴリズムを用いて元データから作られる相対的に小さな値。データの関数であり、秘密鍵であり、また初期化ベクターとして使われることがある。通常は元データに付加され、データの完全性を確認する。[ISO-2382]におけるメッセージ認証コード (Message Authentication Code) を参照。 (444)
- 暗号チェックサム生成 (Cryptographic Checksum Generation)** — 元データに付加する目的で暗号チェックサムを生成するプロセス。 (445)
- 暗号チェックサム検証 (Cryptographic Checksum Verification)** — 付加された暗号チェックサムを検証することを目的として暗号チェックサムを生成するプロセス。 (446)
- 暗号機能 (Cryptographic Function)** — 暗号アルゴリズムによって実行される計算の一。例: 暗号化、復号、デジタル署名生成、デジタル署名検証など。 (447)
- 暗号機能性 (Cryptographic Functionality)** — TOEに埋め込まれた一つまたは複数の暗号機能。 (448)
- 暗号鍵 (Cryptographic Key)** — 暗号アルゴリズムの動作とその出力を制御する値、[ISO-2382]における鍵を参照。 (449)
- 暗号鍵アクセス (Cryptographic Key Access)** — 暗号鍵に対してなされる操作。操作/アクセスの例: 読み出し、書き込み、アーカイブ、バックアップ、回復。 (450)
- 暗号鍵共有 (Cryptographic Key Agreement)** — 双方が共有する単一の共通鍵を計算できるようにする暗号機能。 (451)
- 暗号鍵アーカイブ (Cryptographic Key Archive)** — 暗号鍵を、永久または長期保存媒体に蓄積する操作。 (452)
- 暗号鍵バックアップ (Cryptographic Key Backup)** — 元の暗号鍵が削除、改ざん、破壊されたり、またはアクセス不能になった場合に、再使用できるように暗号鍵をバックアップする操作。 (453)
- 暗号鍵破棄 (Cryptographic Key Destruction)** — 暗号鍵を削除 (ゼロ化) するプロセス。 (454)
- 暗号鍵配付 (Cryptographic Key Distribution)** — 暗号鍵を、利用者、プロセス、TOEユニットなどに提供するプロセス。 (455)
- 暗号鍵供託 (Cryptographic Key Escrow)** — 権限を持つ機関に暗号鍵を渡すことが義務付けられた信頼できる第三者機関にその暗号鍵を提供するプロセス。 (456)

- 暗号鍵生成 (Cryptographic Key Generation)** — 暗号鍵を生成する機能。 (457)
- 暗号鍵管理 (Cryptographic Key Management)** — 生成から配付を経てアーカイブと破棄まで、暗号鍵のライフサイクルを管理するプロセス。 (458)
- 暗号鍵回復 (Cryptographic Key Recovery)** — アーカイブ、バックアップ、供託を含む何らかのソースから、暗号鍵を修復するプロセス。 (459)
- 暗号メカニズム (Cryptographic Mechanism)** — 一つまたは複数の暗号機能を用いるプロセスまたは技法。 (460)
- 暗号操作 (Cryptographic Operation)** — 暗号機能を参照。 (461)
- 暗号変数 (Cryptographic Variable (CV))** — アルゴリズム入力を出力へ変換するための暗号アルゴリズムの操作のために必要となる、一つのまたは連続した値。暗号変数の例は、暗号鍵 (共通、公開、秘密、その他)、公開鍵パラメタ、及び初期化ベクターである (平文、暗号文、及びハッシュ値は暗号変数とはみなされないことに注意)。 (462)
- データパス (Data Path)** — データがその上を通過する (または中を流れる) 論理的または物理的ルート。 (463)
- デジタル署名 (Digital Signature)** — [ISO-2382]のデジタル署名を参照。 (464)
- デジタル署名生成 (Digital Signature Generation)** — デジタル署名を生成するプロセス。 (465)
- デジタル署名検証 (Digital Signature Verification)** — 生成されたデジタル署名を検証するプロセス。 (466)
- ハッシュまたはハッシュ値 (Hashing or Hash Value)** — セキュアハッシュを参照。 (467)
- 初期化ベクター (Initialisation Vector)** — 暗号アルゴリズムの中で、暗号化の出発点を定義するために暗号鍵に関連して用いられるベクター (ビットの連なり)。 (468)
- 呼び出しパラメタ (Invocation Parameter)** — 暗号機能にアクセスするため、TOEに供給される秘密 (例えば、パスワード、または個人識別番号) (469)
- メッセージダイジェスト (Message Digest)** — セキュアハッシュを参照。 (470)
- 否認不可 (Non-Repudiation)** — あるエンティティが、通信 (のある部分) に加わっていたことを否認できないこと。 (471)
- 他の重要なセキュリティパラメタ (Other Critical Security Parameter)** — 呼び出しパラメタを参照。 (472)
- 秘密鍵 (Private Key)** — 公開鍵ペアの鍵の一つ。復号、デジタル署名生成または暗号鍵共有に使用されるので、その機密性を保護しなければならない。 (473)

公開鍵 (Public Key) — 公開鍵ペアの一つで公開可能な鍵。公開鍵には、暗号化に使われるもの、デジタル署名検証に使われるもの、暗号鍵共有に使われるものがある。(474)

公開鍵ペア (Public Key Pair) — 数学的に関係を持った一对の鍵であって、組み合わせの一方である公開鍵から計算によって秘密鍵を引き出すことは実行不可能なもの。(475)

レッドデータ (Red Data) — 暗号化によって保護されていないため、情報内容に容易にアクセスできるデータ。データの例は、メッセージ、ファイル、暗号鍵など。(476)

レッド/ブラック分離 (Red/Black Separation) — レッドデータとブラックデータのデータパスを、論理的または物理的に分離しておくこと。例えば、レッドデータとブラックデータが共通の物理的電線で送られてはならず、メモリの同一の領域を占有してはならない。(477)

共通鍵 (Secret Key) — 暗号化と復号の両方の暗号アルゴリズムで使用される鍵。(478)

セキュアハッシュ (Secure Hash) — メッセージに、あるアルゴリズムを適用した結果の値で、その結果から元のメッセージを引き出すことは計算上不可能であり (セキュアハッシュ)、元のメッセージのハッシュと同じハッシュを与える別のメッセージを作り出すこと、同一のハッシュを作る二つのメッセージを発見することは計算上不可能である。通常、セキュアハッシュは、それが作られた元のメッセージまたはファイルよりも著しく短い。ハッシュ値、メッセージダイジェストとも呼ばれる。(479)

改ざん検出エンベロープ (Tamper Detection Envelope) — TOEに対する改ざん (侵入の試みまたは侵害) を検出できる、TOE周囲の領域。(480)

ゼロ化 (Zeroisation) — 最初に格納されたデータが復元されないよう、そのデータを別のもので置き換えることで蓄積されたデータを電子的に消去する方法。(481)

ゼロ化回路 (Zeroisation Circuit) — ゼロ化を実現する電子回路。(482)

ゼロ化回路 (Zeroisation Circuitry) — ゼロ化回路(Zeroisation Circuit)を参照。(483)

C.2 暗号の概説

C.2.1 暗号とは?

暗号とは、データの変換に対する原理、手段及び方法を統合する科学または技術 (art) であり、その目的は、データの情報内容を隠すこと、検出されることなく改ざんされるのを防ぐこと、及び/または、許可されない使用を防ぐことである。その科学的構成部分は数学を根拠としており、技術は、多年に及ぶ実経験から生み出されたものである。暗号には以下のものが含まれる (これだけに限定されない): (484)

- a) デジタル署名生成及び/または検証;

- b) 完全性のための及び/またはチェックサム検証のための暗号チェックサム生成;
- c) セキュアハッシュ (メッセージまたはファイルダイジェスト) 計算;
- d) データ暗号化及び/または復号;
- e) 暗号鍵の暗号化及び/または復号;
- f) 暗号鍵共有。

暗号機能性は、いくつかの上位セキュリティ対策方針を満たすために使用することができる。これには以下のものが含まれる (これだけに限定されない): (485)

- a) 機密性;
- b) 完全性;
- c) 識別と認証;
- d) 否認不可;
- e) 高信頼パス;
- f) 高信頼チャネル;
- g) データ分離。

暗号機能性は、適している暗号アルゴリズムと暗号鍵サイズを使用すべきであり、セキュアな暗号プロトコルとしっかりした暗号工学を使うのはいうまでもない。 (486)

C.2.2 なぜ暗号を使うか?

PP及びST開発者は、暗号機能性が、セキュリティ対策方針を満たすために使えるであろういくつかの機能性の方式の中の一つにすぎないことを注意すべきである。セキュリティ対策方針を満たすべき暗号機能性の選択は、それ故に、全体としてよくバランスが取れた、手続き的、物理的、及びITセキュリティ手段のセットを定義する文脈の中で考慮されるべきである。 (487)

他のセキュリティ機能性の方式に対し、暗号を選択すべき数多くの理由が存在しよう: (488)

- a) 暗号機能だけが、望まれたセキュリティ対策方針を満たすかもしれない。

例: *保護されていない電線または空中を通した情報の送信 (つまり、パブリックドメイン上)。暗号は、これらの状況下で通信されるデータに対し、機密性または完全性を提供する唯一の機能性である。*

- b) 暗号機能は、予期された脅威に対抗する適切なレベルのセキュリティを提供するかもしれない。

例: *安全でないネットワークを介した認証 (訳者注: ここでの「認証」は*

"certification" のことではなく、"authentication: 真正性確認"のこと)。暗号は、認証情報の盗聴またはリプレイに対する保護に使える。認証の手法は、「チャレンジ・レスポンス」メカニズムによってしばしば実現される。

- c) 実装、運用、及び/または使用において、暗号機能が最も単純/容易/安価であるかもしれない。
- d) 情報を保護する多数の異なる手法の一部として、暗号機能が使われるかもしれない。

例: データは、「従来の」コンピュータセキュリティアクセス制御及び/または物理的セキュリティ手法を用いた不正な暴露に対して保護されている。それらのメカニズムの障害に対して、付加的レベルの保護を提供するために、データはさらに暗号化される。このようにすれば、相手は、アクセス制御を破れたとしても、相手はそのデータを得るためには暗号メカニズムも破らなくてはならなくなる。

C.2.3 なぜ暗号標準を使うか?

より広い文脈において、暗号機能は、以下の一つまたはそれ以上の理由によって、特定された標準 (国際、国家、業界または組織のどれであってもよい) に適合する必要があるが生じ得る: (489)

- a) 共通的に受け入れられるセキュリティのレベルを確立する助けになり得る;
- b) 相互運用性に役立ち得る;
- c) 相互承認に役立ち得る;
- d) 組織のセキュリティ方針によって要求され得る;
- e) 望まれた機能性を含めるのに役立ち得る。

C.3 セキュリティ要件の抽出

本節は、暗号機能性を含んだTOEに対する脅威、組織のセキュリティ方針、及びセキュリティ対策方針を特定する場合で、かつ、PPまたはSTで特定されるべきセキュリティ要件と前提条件の抽出において暗号を考慮する必要がある場合に、考慮すべき暗号関連の側面を識別するものである。本節におけるガイダンスは、暗号機能性を含んだTOEに対するセキュリティ要件を抽出するときに考慮すべき問題を単に示唆するだけであり、併せて非暗号関係の問題の検討に及ぶことはない。

(490)

C.3.1 脅威

暗号機能性を含んだTOEのIT資産に対して、典型的に知られている、または前提とされる脅威は、

PPまたはSTにおいて特定されるべきである。これらの脅威は、TOEによって対抗されるかもしれない、またはされないかもしれない。(491)

このガイドの3章で述べたように、脅威の明確な特定には、脅威の源(または脅威エージェント)、攻撃されるIT資産、及び攻撃の形態が詳述されるべきである。さらに、TOEの実装における欠陥や弱点に基づく攻撃よりも、IT資産を直接脅かす事象だけが、通常は含められるべきである。(492)

これは、脅威の源/脅威エージェント、脅威エージェントによって攻撃されるIT資産、及び攻撃の形態の「三点セット」で脅威を定義することが、とり得る一つのアプローチとなることを意味している。そしてその脅威はセキュリティ対策方針を定義するのに使うことができ、その次にはITセキュリティ要件に詳細化される。(493)

C.3.1.1 典型的な脅威の源

暗号機能性を含んだTOEに対する典型的な脅威の源(または脅威エージェント)は以下のものを含む(が、それだけに限定されない): (494)

- a) TOEの許可された利用者;
- b) 許可されていない者;

この文脈において、許可された利用者とは、定義されたIT資産にアクセスすることを許可された人であることに注意。(495)

C.3.1.2 典型的な暗号関連のIT資産

保護を必要とするTOEにおける暗号関連IT資産の典型的な種別は以下のものを含む(が、それだけに限定されない): (496)

- a) 暗号変数(共通鍵、秘密鍵、公開鍵、公開鍵パラメタ、初期化ベクター、その他);
- b) 暗号機能に対する入出力(例えば、平文と暗号文);
- c) ハードウェア、ソフトウェア、及び/またはファームウェアによる暗号アルゴリズムの実装;
- d) 呼び出しパラメタ(「他の重要なセキュリティパラメタ」としても知られている)。

C.3.1.3 典型的な攻撃形態

暗号関連のIT資産は、典型的に、いくつもの攻撃の形態から保護されることを必要とする。これらは以下のものを含む(が、それだけに限定されない): (497)

- a) TOEからの電磁放射物の検出;
- b) TOEの許可された利用者へのなりすまし;
- c) TOEで誤動作を誘発させる;

- d) TOEの不正確な使用(すなわち、運用または管理);
- e) TOEを構成するハードウェア、ファームウェア、またはソフトウェアの機能不全;
- f) 物理的攻撃。

(これらの攻撃は、必ずしも暗号の資産に限定されないことに注意。) (498)

C.3.1.4 典型的脅威

前述の副節で識別した脅威の「三点セット」に対する入力サンプルを用いると、48とおりの脅威を特定できる(すなわち、2つの脅威エージェント×6つの攻撃の形態×4つの暗号関連IT資産)。以下の表11に、このやり方で抽出した脅威の例をあげる。 (499)

T.種別	脅威
T.EMI	TOEからの電磁放射によって、暗号関連のIT資産が、許可されない者または利用者に暴露されるかもしれない。
T.IMPERSON	攻撃者(外部または内部の人間)が、TOEの許可された利用者になりすますかもしれない。
T.ERROR	許可されない者またはTOEの利用者が、TOEにおける誤動作を誘発させることで、暗号関連のIT資産の、許可されない暴露または改変を引き起こすかもしれない。
T.MODIFY	攻撃者による、情報の許可されない改変または破壊によって、情報の完全性が危険にさらされるかもしれない。
T.ATTACK	攻撃者(内部者であれ外部者であれ)が、その者が行うことが許可されていないアクションを為そうと試みた結果、暗号関連のIT資産について、検出されない危殆化が生じるかもしれない。
T.ABUSE	許可されたTOEの利用者が、(意図的、その他で)その者が行うことを許可されていないアクションを為した結果、暗号関連のIT資産の検出されない危殆化が生じるかもしれない。
T.MAL	TOEの機能不全によって、暗号関連のIT資産が、改変、または許可されない者又はTOEの利用者へ暴露されるかもしれない。
T.PHYSICAL	TOEのセキュリティ上重要な部品が、セキュリティを損なうかもしれない物理的攻撃の対象になるかもしれない。

表11 - 暗号資産関連の典型的脅威

C.3.2 組織のセキュリティ方針

TOEが適合する必要があるかもしれないOSP(もしあれば)は、これもまた、PPまたはSTにおいて特定されるべきである。TOEにおいて暗号機能性に関連し、脅威記述の中にそれが分かるような形で含め、または暗に示すことが困難なOSPステートメントは、ここで提示されるべきである。これらは以下のものに対するステートメントを含む(が、それだけに限定されない): (500)

- a) 識別及び認証方針;

- b) 利用者アクセス制御方針;
- c) 監査及び責任(accountability)方針;
- d) 暗号鍵管理方針;
- e) 物理的セキュリティ方針;
- f) 放射(emanations)方針。

PP/ST開発者は、これらのOSPステートメントを、TOEの非暗号関連の側面に適用することも希望するかもしれない。 (501)

暗号機能性を含んだTOEに対するセキュリティ方針のさまざまな部分におけるこれ以上の情報、及びISO/IEC 15408においてそれらがどのように提示され得るかについては、C.4.5節において対応される。 (502)

C.3.3 セキュリティ対策方針

典型的なセキュリティ対策方針は、以下の表12に示される。 (503)

O.種別	セキュリティ対策方針
O.I&A	TOEは、すべての利用者を一意に識別しなければならず、TOEの機能にアクセスしようとする利用者に許可を与える前に、その主張する識別情報(訳者注: 原文は "identify" であるが、 "identity" の誤りと思われる)を認証しなければならない。
O.DAC	TOEは、TOEの利用者に対して、個別の利用者または識別された利用者グループに基づき、かつ裁量によるセキュリティ方針によって定義された規則のセットに沿って、利用者の所有する、または責任を持つオブジェクト及び資源へのアクセスを制御する、及び制限する手段を提供しなければならない。
O.PHP	TOEは、自分自身及びその中の暗号関連のIT資産を、許可されない物理的アクセス、改変、または使用から保護すべきである。
O.INTEGRITY	TOEは、情報に影響を及ぼす完全性の喪失を検出する手段を提供しなければならない。
O.FAILSAFE	誤りの発生する事象において、TOEはセキュアな状態を保たねばならない。
O.ADMIN	TOEは、許可された管理者がTOE及びそのセキュリティ機能を効果的に管理できるようにする機能性を提供しなければならない、かつ、許可された管理者だけがその機能性にアクセスできることを保証しなければならない。
O.EMI	TOEの電磁波放射によって、許可されない者または利用者に暗号関連のIT資産が暴露されることを防ぐため、手続き的及び物理的手段がとられるべきである。
O.PHYSICAL	TOEに責任を持つ者は、セキュリティ方針の実施において重要となる部分が、ITセキュリティを脅かす恐れのある物理的攻撃から保護されることを保証しなければならない。

表12 - TOEに対するセキュリティ対策方針例

O.EMIとO.PHYSICALは環境のセキュリティ対策方針であることに注意せよ。残りはTOEに対するセキュリティ対策方針である。その他の環境のセキュリティ対策方針として、以下のような

ものに対応することもできる:

(504)

- a) 暗号関連のIT資産のTOEにおける入出力の取扱い及び蓄積に対する手続き;
- b) TOEの運用と保守に対する手続き;
- c) TOEの許可された利用者に置かれる信頼のレベル;
- d) 何らかの方法を用いてTOEとやりとりする許可された利用者(例えば、暗号鍵保管者、保守要員、一般利用者)の訓練;
- e) TOEを保護するのに必要とされる物理的手段;
- f) TOEにおける環境の運用上の制約(電磁放射制限を含む)
- g) TOE外のITセキュリティ環境(例えば、TOE外部に存在するソフトウェアの種類の制限、TOEアクセス制御方針を実施するための下層の信頼できるオペレーティングシステムの使用)。

C.3.3.1 セキュリティ対策方針根拠

脅威に対抗するセキュリティ対策方針の適切性についての実証例を表13に示す。この表は、必ずしも、PPまたはST根拠の観点からはセキュリティ対策方針の適切性に対して必要とされる詳細さのレベルを提示したものではない。

(505)

T.種別	関連するO.種別と根拠
T.EMI	O.EMI - 手続き的及び物理的手段(例えば、部屋をシールドすること、公共の場所から離すこと)の使用を要求することは、TOEからの放射によって暗号に関連するIT資産の暴露の危険を減じるはずである。
T.IMPERSON	O.I&A - 利用者の信頼できる識別及び認証を要求することは、利用者なりすましの危険を減じるはずである。
T.ERROR	O.FAILSAFE - 誤りが生じた事象においてTOEにセキュアな状態を保持するよう要求することは、不慮の暗号関連IT資産の改変や暴露に起因する露見を減じるはずである。
T.ABUSE	O.DAC - TOEに対するすべてのアクセスが特定のアクセス制御方針に適合することを要求することは、利用者が、彼らがアクセスを要求していないいかなる操作を行う危険をも減じるはずである。
T.MAL	O.INTEGRITY - TOEに完全性の喪失を検出することを要求することは、誤り検出の機会を増加させる。 O.FAILSAFE - 誤りが生じた事象においてTOEにセキュアな状態を保持するよう要求することは、不慮の暗号関連IT資産の改変や暴露に起因する露見を減じるはずである。
T.PHYSICAL	O.PHP - 物理的攻撃に対する保護を要求することは、物理的攻撃の危険を減じるはずである。 O.PHYSICAL - TOEに対する物理的アクセスを行うことが要求され許可された利用者だけに物理的アクセスの制限を行う手続き及び物理的手段の使用を要求することは、TOEにおける物理的攻撃が実行される危険を減じるはずである。
T.MODIFY	O.INTEGRITY - 完全性の喪失を検出する能力は、攻撃者が暗号関連IT資産を

	<p>改変する機会を減じるはずである。</p> <p>O.ADMIN - TOEの適切な設定と管理は、改変の危険を減じるはずである。</p>
T.ATTACK	<p>O.I&A - 利用者の信頼できる識別及び認証を要求することは、許可されないアクセスの危険を減じるはずである。</p> <p>O.DAC - TOEに対するすべてのアクセスが特定のアクセス制御方針に適合することを要求することは、利用者が、彼らがアクセスを要求していないいかなる操作を行う危険をも減じるはずである。</p>

表13 - セキュリティ対策方針根拠

C.3.4 セキュリティ要件

セキュリティ対策方針は、以下の表14に示すようにセキュリティ要件へ詳細化できるかもしれない。

(506)

O.Type	セキュリティ対策方針	ISO/IEC 15408 コンポーネント
O.I&A	TOEは、すべての利用者を一意に識別しなければならず、TOE及びその中の暗号関連のIT資産にアクセスしようとする利用者に許可を与える前に、その主張する識別情報(訳者注: 原文は "identify" であるが、"identity" の誤りと思われる)を認証しなければならない。	FIA_UID.1-2 FIA_UAU.1-5
O.DAC	TOEは、TOEの利用者に対して、特定されたアクセス制御方針に沿って、暗号関連のIT資産へのアクセスを制御する、かつ制限する手段を提供しなければならない。	FDP_ACC.1-2 FDP_ADF.1
O.PHP	TOEは、自分自身及びその中の暗号関連のIT資産を、許可されない物理的アクセス、改変、または使用から保護すべきである。	FPT_PHP.1-3
O.INTEGRITY	TOEは、情報に影響を及ぼす完全性の喪失を検出する手段を提供しなければならない。	FPT_AMT.1 FPT_TST.1
O.FAILSFE	誤りの発生する事象において、TOEはセキュアな状態を保たねばならない。	FPT_FLS.1-4
O.ADMIN	TOEは、許可された管理者が、特定された暗号鍵管理方針に沿って暗号鍵を管理できるようにする機能性を提供しなければならない。	FCS_CKM.1-4 FCS_COP.1
O.EMI	TOEの電磁波放射によって、許可されない者または利用者に暗号関連のIT資産が暴露されることを防ぐため、手続き的及び物理的手段がとられるべきである。	AGD_ADM.1 AGD_USR.1 セキュリティ運用手続き
O.PHYSICAL	TOEに責任を持つ者は、セキュリティ方針の実施において重要となる部分が、ITセキュリティを脅かす恐れのある物理的攻撃から保護されることを保証しなければならない。	セキュリティ運用手続き

表14 - セキュリティ対策方針からセキュリティ機能要件の抽出

C.4 ITセキュリティ要件の表現

C.4.1 序説

本節では、暗号機能性を有するTOEに含める必要がありそうなITセキュリティ要件を、ISO/IEC 15408を使用して、PPまたはSTの中で、どのようにすれば正確に表現できるかを説明する。(507)

PPまたはSTのTOEセキュリティ環境(脅威、OSP、及び前提条件)及びセキュリティ対策方針の部分の内容についての詳細な解説は、C.3節でなされている。(508)

開発者は、暗号機能性を含むTOEに対してPP及びSTを作るときだけにこのガイダンスが適用されることを覚えておくべきである。このガイダンスは、そのようなTOEに対する要件の特定に役立つかもしれないコンポーネントやファミリについて指針を与えるだけにすぎず、並列に考えるべき暗号以外の問題に対して必要とされる機能性を考慮してはいない。このガイダンスは、追加された要件、またはいかなる既定の機能又は保証パッケージ(主張された評価保証レベルなど)の要件に対する必要性を考慮したものではない。また、すべての付加されたコンポーネントの互いの依存性を明示的に考慮してもいい。(509)

C.4.2 暗号設計と実装における従来の関心事項

暗号装置の設計者及び実装者は、運用上及び工学上の経験から、主として暗号ハードウェアに関して解決されてきた脆弱性について、従来から関心を持っている。表15は、これら従来の脆弱性と従来の解決策を要約したものである。(510)

脆弱性	従来の解決策
データと鍵を混合すること	物理ポートを分ける
保守アクセスポートの悪用	特定の保守役割
平文と暗号文を混合すること	入力と出力パスを分ける レッド/ブラックデータ分離
暗号機能不全に起因する秘密情報の公開	秘密情報を公開するための二つの内部の独立したアクション 鍵生成、鍵登録、鍵ゼロ化回路から出力データパスを切断
許可されないアクセス	識別と認証 機能、サービス、及びデータへのアクセス制御
設計誤り	有限状態機械設計
物理的攻撃	物理的セキュリティ手段
ハードウェア誤りの疑い	自己テスト
電磁放射	電磁放射制御標準

表15 - 従来の脆弱性と解決策

以下の表は、これら従来の脆弱性に対する解決策が、ISO/IEC 15408を使用してどのように表現

されるかを要約したものである。

(511)

脆弱性	ISO/IEC 15408表現
データと鍵を混合すること	モジュール化(ADV_INT)
保守アクセスポートの悪用	保守アクセス制御SFP(FDP_ACC、FDP_ACF)
平文と暗号文を混合すること	モジュール化と情報秘匿(ADV_INT)
暗号機能不全に起因する秘密情報の公開	フェールセキユア(FPT_FLS) モジュール化と情報秘匿(ADV_INT)
許可されないアクセス	識別と認証(FIA_UID、FIA_UAU、FIA_ATD) 利用者アクセス制御SFP(FDP_ACC、FDP_ACF)
設計誤り	準形式的及び形式的設計(ADV_HLD、ADV_LLD)
物理的攻撃	物理的セキュリティ(FPT_PHP)
ハードウェア誤りの疑い	フェールセキユア(FPT_FLS) 自己テスト(FPT_AMT、FPT_TST)
電磁放射	放射方針 前提条件

表16 - ISO/IEC 15408従来の解決策の表現

これらISO/IEC 15408表現の説明を分かりやすくするため、表14で識別された典型的なISO/IEC 15408表現に加えて、暗号機能性を含むTOEの典型的セキュリティ要件の表現を、以下の6つの見出しの元で考えることとする:

(512)

- a) TOE定義;
- b) TOE設計と実装;
- c) TOEセキュリティ方針;
- d) TOEセキュリティ機能性;
- e) TOEテスト;
- f) TOE運用。

C.4.3 TOE定義

C.4.3.1 ガイダンス

TOEは、そのコンポーネント、機能及びインタフェースはすべてPP/STの中で完全に定義されるべきであり、つまり、TOEに対する機能仕様が存在するべきである。これは、PP/STの中で定義されたすべての機能要件が対応されていること、かつTSPがTSFによって実施されることを保証するためである。これはまた、機能仕様に一致するTOEセキュリティ方針もまた定義されねばならないことも意味している(C.4.5節も参照)。

(513)

TOE定義は、TOE機能性、及びTOEの物理的/論理的境界の定義を扱うという点で、TOE設計と区別されることに注意。TOE設計は、実装が可能な、機能仕様を詳細化したものの提供を取り扱う。(514)

C.4.3.2 ISO/IEC 15408表現

ADV_FSP(機能仕様)ファミリのコンポーネントは、ユーザから見ることのできるインタフェースとTSFのふるまいの、上位レベルの記述に対する要件を表すために使われるべきである。(515)

もし準形式的設計(例えば、有限状態機械設計)に対する要件があれば、ADV_FSP.3(準形式的機能仕様)コンポーネントが使用されるべきである。もしセキュリティ方針モデルに対する要件があれば、ADV_SPM(セキュリティ方針モデル化)ファミリが使われるべきである。(516)

C.4.4 TOE設計及び実装

C.4.4.1 一般的保証

ガイダンス

設計と実装の誤りを最小にし、かつ可能な限りそれらをなくすために、相応の注意が払われるべきである。TOEは、少なくとも、主張する機能要件を実装するのに適切な上位レベルのアーキテクチャを提供していることが、PP/STにおいて実証されるべきである。(517)

もし、設計とその実装においてより高い信頼性が要求される場合、より下位レベルの設計(場合によっては最下位レベル)もまた、要求される機能性を表現しており、かつそれよりも上位レベルの設計が正確に詳細化されてきていることの実証が必要になるかもしれない。(518)

ISO/IEC 15408表現

TOEの設計と実装の正確さにおいて求められる信頼性を満たすため、以下のファミリから適切なコンポーネントが選択されるべきである。(519)

- a) ADV_HLD (上位レベル設計)
- b) ADV_LLD (下位レベル設計)
- c) ADV_RCR (表現対応)
- d) ALC_TAT (ツールと技法)

ADV_HLDファミリからのコンポーネントは、大きな構成ユニット(つまりサブシステム)、及びそれらが持つ機能に関するユニットの視点から、TSFを記述する要件を表現するために使用されるべきである。もしTOEの暗号の境界をTOE全体の境界から区別する要件があるならば、ADV_HLD.2(セキュリティ実施上位レベル設計)コンポーネントを使用すべきである。(520)

ADV_LLDファミリからのコンポーネントは、モジュール、それらの相互関係、及び依存性の視点から、TSFの内部動作を記述する要件を表すのに使用されるべきである。(521)

ADV_RCRファミリからのコンポーネントは、設計のさまざまな表現間の対応を実証するための要件が存在する場合に使用されるべきである。(522)

ALC_TAT.2コンポーネントは、定義された実装標準(例えば、コーディング標準)に従って達成されるべき開発の要件が存在する場合に使用されるべきである。(523)

C.4.4.2 モジュール化設計

ガイダンス

前述のように、暗号の設計者と実装者が典型的に関心を持つのは、TOEの一つのパートにおける誤りがTOEの他のパートに影響を及ぼすかもしれないこと、及び、TOEの一つのパートからの情報が、その情報を必要としないTOEの他のパートで利用できてしまうかもしれないことである。これらの関心事項は、次のような従来からの要件の種別へつながる。(524)

- a) データ入力インタフェースを経由してTOEに入るすべての入力データは、入力データパスだけを通過しなければならない;
- b) データ出力インタフェースを経由してTOEを出るすべての出力データは、出力データパスだけを通過しなければならない;
- c) データ出力パスは、鍵生成、手動鍵入力、または鍵ゼロ化を行う回路、プロセスから、論理的に切り離されなければならない;
- d) TOEは、レッドデータとブラックデータに対して、分離したデータパスを保持しなければならない。

これら特定の要件の意図は、モジュール化設計、複雑さの減少、及びシステムの一部における誤りの影響の最小化を提供することである。(525)

ISO/IEC 15408 表現

PP/STにおいてTOEのモジュール化設計に対する要件を表現するため、次のファミリからのコンポーネントを選択するべきである。(526)

- a) ADV_FSP (機能仕様)
- b) ADV_HLD (上位レベル設計)
- c) ADV_INT (TSF内部構造)
- d) ADV_LLD (下位レベル設計)

例えば、下位レベル設計は、すべてのデータフローを示し、入力、出力、平文、及び暗号文が、それらを必要とするTOEのコンポーネントだけによってアクセスされるのを保証するために使うことができる。モジュール化及び階層化の要件は、TOEがしっかりとした工学上の原則を用いて設計されており、それによって、データが、それを必要とするTOEのコンポーネントだけにアク

セスされることを保証するのに役立つ。 (527)

これに直接関連するものは、ADV_INT (TSF内部構造)ファミリのADV_INT.3 (複雑さの最小化)コンポーネントからの以下のエレメントである。 (528)

ADV_INT.3.3C アーキテクチャの記述は、TSF設計が不要な相互作用を避けるために大部分が独立したモジュールを提供する方法を記述しなければならない。

ADV_INT.3.5C アーキテクチャの記述は、相互作用が最小化されていることを示し、それらがそのように留まることを正当化しなければならない。

ADV_INT.3.6C アーキテクチャの記述は、複雑さを最小化するためにTSF全体がどのように構造化されているかを記述しなければならない。

C.4.5 TOEセキュリティ方針

C.4.5.1 序説

PP/ST作成者は、TOEセキュリティ方針を記述すべきである。暗号機能性を持つTOEに対するセキュリティ方針は、以下の側面を含むべきであるが、これ以外のものもあるかもしれない: (529)

- a) 識別及び認証の方針;
- b) 利用者アクセス制御方針;
- c) 監査及び責任の方針;
- d) 暗号鍵管理方針;
- e) 物理的セキュリティ方針;
- f) 電磁放射方針。

これらのセキュリティ方針の表現は、典型的には、組織のセキュリティ方針(例えば、電磁放射標準、利用者アクセス制御方針の仕様)、前提条件(例えば、TOEを保護するために必要な物理的及び手続き的手段)、及びTOEのIT機能要件(例えば、利用者アクセス制御方針を実装する機能メカニズムの特定)によるステートメントの組み合わせを用いて作り上げられる。 (530)

C.4.5.2 識別及び認証方針

ガイダンス

利用者及び/または役割の種別、及びそれらを認証(authenticate)するために使われる手段は、PP/STの中で特定されるべきである。典型的な暗号関連の役割は以下を含む: (531)

- a) 暗号管理者/管理人 (officer/custodian);
- b) システム保守者;
- c) システム監査者;

- d) システムセキュリティ管理者 (officer);
- e) 利用者/運用者。

ISO/IEC 15408表現

主張された利用者の識別情報の確立と検証のための要件を表現するために、FIAクラスの適切なコンポーネントを選択すべきである。典型的なものとして、以下のファミリのコンポーネントを選択すべきである: (532)

- a) FIA_UID (利用者識別)
- b) FIA_UAU (利用者認証)
- c) FIA_ATD (利用者属性定義)。

TSFが仲介しかつ利用者識別を要求するそれ以外のいかなるアクションを実行する前において、利用者に自分自身を識別することを要求すべき条件を定義するために、FIA_UIDファミリのコンポーネントを使うべきである。 (533)

TSFがサポートする利用者認証メカニズムを定義するために、FIA_UAUファミリのコンポーネントを使うべきである。 (534)

利用者に対するセキュリティ属性を定義するために、FIA_ATDファミリのコンポーネントを使うべきである。利用者属性としての暗号鍵情報を定義するために、FIA_ATDファミリのコンポーネントを使うべきである。 (535)

認証情報を取られたりリプレイされることから保護するために、FTP_TRP(高信頼パス)ファミリ、及び又はFIA_UAU (FIA_UAU.3 - 偽証されない認証; 及びFIA_UAU.4 - 単一認証メカニズム)のコンポーネント使うことでさらに高い効果が得られよう。C.4.6.3節では、高信頼パスの使用についてのさらなる解説を行っている。 (536)

C.4.5.3 利用者アクセス制御方針

ガイダンス

TOEは、特定された利用者アクセス制御方針どおりに、暗号IT資産に対する利用者アクセスを実施すべきである。暗号機能性を持つTOEの文脈において、利用者アクセス制御方針の要素は以下のとおりである: (537)

- a) 利用者役割;
- b) アクセスされ得るサービス;
- c) 重要なセキュリティパラメタ、例えば、暗号鍵 (暗号化と復号の両方)、その他の重要なセキュリティパラメタ (認証データなど);

- d) サービス及び重要なセキュリティパラメタへのアクセスのモード (例えば、読み出し、書き込み、実行、削除等々)。

TOEに対する利用者アクセスは、役割ベースアクセス制御 (RBAC) 方針、識別情報ベースアクセス制御 (IBAC) 方針、またはその二つの組み合わせに基づくものであってよい。 (538)

設計によっては、保守要員が暗号機能性を持つTOEのアクセス制御メカニズムをバイパスできてしまうかもしれない。このように、実施され得る保守アクセス制御方針も、また定義される必要があるかもしれない。この方針は、どのようにして利用者情報を保守要員によるアクセスから保護せねばならないかということに対応する必要がある。(これは、手続き的及び/または技術的手段によって達成できるかもしれない。) (539)

例: (540)

保守要員がTOEへのアクセスを許可されるに先立ち:

- a) すべての平文情報はマスター鍵を用いて暗号化されねばならない。
b) マスター鍵は取り出しておかねばならず、そのとき、TOE内部のそのコピーはゼロ化されねばならない。

保守要員がその保守業務を終えた後、マスター鍵は、前に暗号化された情報を復号するためにTOEにロードされねばならない。

ISO/IEC 15408表現

以下のファミリーからのコンポーネントを選択すべきである: (541)

- a) FDP_ACC (アクセス制御方針)
b) FDP_ACF (アクセス制御機能)
c) FDP_IFC (情報フロー制御方針)

暗号鍵は、TOEによって内部に格納され、保護されるべきである。利用者鍵は、FDP_ACCファミリーからのコンポーネントを用いたアクセス制御方針に従って保護できる。システム鍵は、FMT_MTDファミリーに従って保護できる。 (542)

最低限、FDP_ACC.1コンポーネントを使用すべきである。すべてのサブジェクトに対して暗号関連IT資産へのアクセスを制御するため、このコンポーネントを使用してセキュリティ機能方針 (SFP) を定義すべきである。他の機能及びTOE全体に対するSFPによっては、FDP_ACC.2コンポーネントがさらに適切であるかもしれない。 (543)

[【ISO/IEC JTC 1/SC 27 N3816改訂情報】：段落544は以下に示すとおりコンポーネントに対して操作された部分が識別される。](#)

FDP_ACC.1は、利用者アクセス制御SFPを実施するための要求を定義するために、以下のように

使われるべきである:

(544)

FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACF.1.1 TSFは、[割付: *オブジェクト属性のリスト*]に基づいて、オブジェクトに対して、利用者アクセス制御方針を実施しなければならない。

FDP_ACF.1.2 TSFは、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない: サブジェクトは、[割付: *オブジェクト*]を用いて希望する暗号操作を実行することが許される。¹

FDP_ACF.1.3 TSFは、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: [割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]。

FDP_ACF.1.4 TSFは、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

上述の場合におけるサブジェクトは、利用者²または利用者を代行して働くアクティブな抽象エンティティ (例えば、プロセス)である。

(545)

各サブジェクトは、利用者識別子、現在の役割、現在の時間 (適切な場合) の属性を持つ。

(546)

上述の場合におけるオブジェクトは、平文データ及び復号された暗号鍵である。オブジェクトは、以下の付加アイテムを含むこともある: 暗号文データ及び暗号化された暗号鍵。

(547)

オブジェクト属性の例は、オブジェクトの暗号機能、オブジェクトに関係付けられた役割、オブジェクトに関係付けられた利用者、オブジェクト識別子、及び オブジェクトに対する有効期間 (適切な場合) などである。

(548)

このセキュリティ方針は、平文または保護された (例えば、暗号化された)、認証情報のような重要なセキュリティパラメタの保護に対応するものではない。認証情報を保護するためには (例えば暗号化が使われていたとしても)、FMTクラスからの適切なファミリとコンポーネントが使用されるべきである (例えば、認証データの保護を管理する方針を特定するために、FMT_MSAファミリが使われるべきである)。

(549)

もしサブジェクトの属性、希望する暗号機能、及びオブジェクトの属性がFDP_ACF.1で特定された規則を満たすなら、その機能を実行することが許される。

(550)

¹ 訳注: FDP_ACF.1.2の斜体文字部は詳細化の操作を行い、その詳細化の中で、新たな割付を定義している。

² 訳注: アクセス制御のサブジェクトに「利用者」をあてるのは、CC パート1の2.3に書かれたサブジェクトの定義からはずれており、適切でない。

暗号鍵情報はまた、情報フロー制御方針に従って保護されるべきである。情報フロー制御方針は、FDP_IFCファミリのコンポーネントを用いて定義されるべきである。(551)

C.4.5.4 監査及び責任 (accountability) 方針

ガイダンス

TOEに対する監査及び責任要求は (もしあれば)、PP/ST中で定義されるべきである。(552)

手続き的要件には、以下を含めてよい:(553)

- a) いつ物理的改ざんまたはエラーに対してTOEを検査するか (例として、特定した最小期間内に、利用者が改ざんまたは予期しないエラーが生じたとき疑うときはいつでも、利用者が環境の前提条件を侵したかもしれないときはいつでも、利用者がTOEの物理的保護を侵したかもしれないときはいつでも)。
- b) どのように物理的改ざんまたはエラーを検出し報告するか。

もしTOEが監査と責任機能性を実装するならば、開発者は機密情報 (例えば、共通または秘密暗号鍵) があらゆる監査記録フォームの中に含まれていないことを保証することを忘れないようにすべきである。(554)

ISO/IEC 15408表現

PP/STにおいて手続き的責任及び監査要件を表わすには、前提条件を用いるべきである。(555)

監査の最小及び基本レベルは、FCS_CKM及びFCS_COPファミリの両方に対して定義される。監査コンポーネントの使用における更なる情報は、その他のサポートする機能要件に対する監査要件と同様、ISO/IEC 15408パート2の中で提供される。監査事象及びトランザクションは、重要な監査事象が収集され、多大な監査データの中に失われてしまわずに解析され得るよう、注意深く選択されるべきである。(556)

C.4.5.5 暗号鍵管理方針

ガイダンス

暗号鍵は、そのライフサイクルを通じて、セキュアなやり方で使用され運用管理されるべきである。この範囲は、暗号鍵生成、暗号鍵配付、暗号鍵アクセス (バックアップ、保存、及び回復を含む) 及び暗号鍵廃棄に限られる。(557)

ISO/IEC 15408表現

PP/STにおいて暗号鍵管理方針の要件を特定するためには、FCS_CKM (暗号鍵管理) ファミリを選択すべきである。(558)

FCS_CKMファミリは、さまざまな暗号鍵管理機能に対する要件を定義する。もし、TOEがこれらの暗号鍵管理機能の一つまたはそれ以上を実行するのであれば、FCS_CKMファミリから適切

なコンポーネントを選択すべきである。 (559)

C.4.5.6 物理的セキュリティ方針

ガイダンス

物理的セキュリティ方針の要件は、TOEを構成するハードウェアとファームウェア及びそれが置かれる環境に付随するものであり、PP/STにおいて記述されるべきである。 (560)

物理的セキュリティ方針は、以下の側面に対応すべきである： (561)

- a) 環境の前提条件 (暗号を含んでいるいないに関わらず、あらゆるPP/STに対する一般的な環境の前提条件と同じものであるべき)。これらの前提条件は、典型的には前提条件として書かれるべきである (3章参照)。しかしながら、もしこれらが直接にIT環境におけるソフトウェア、ファームウェア及び/またはハードウェアのことを参照するのであれば、それらはIT環境に対するセキュリティ要件としてモデル化されるべきである。
- b) TOEの物理的保護に対するさまざまな利用者及び管理者クラスの問題 (この情報はまた、利用者及び管理者ガイダンス文書の中にあるべきである)。

ISO/IEC 15408表現

TOEの外側に適用される物理的、手続き的及び人的手段は、典型的に前提条件として表現される。加えて、以下の二つの保証ファミリからのコンポーネントを選択すべきである。 (562)

- a) AGD_USR (利用者ガイダンス)
- b) AGD_ADM (管理者ガイダンス)

AGD_ADMファミリからのコンポーネントは、ある物理的及び環境的制約下でTSFが管理者によって操作されるべき、その物理的及び環境的制約を提示する要件を記述するために使用されるべきである。 (563)

AGD_USRファミリからのコンポーネントは、ある物理的及び環境的制約下でTSFが利用者によって正しく操作されるべき、その物理的及び環境的制約を提示する要件を記述するために使用されるべきである。 (564)

もしTOE自身が物理的セキュリティ要件を実装するなら、FPT_PHP (TSF物理的保護) ファミリからのコンポーネントをPP/STに含めるために選択すべきである。これらのコンポーネントは、物理的改ざんまたは干渉の攻撃にどのように対処するかだけでなく、それらを防ぐためにも、TSFが備える物理的セキュリティ要件を表すために用いることができる。 (565)

[【ISO/IEC JTC 1/SC 27 N3816改訂情報】：段落566は以下に示すとおりコンポーネントに対して操作された部分が識別される。](#)

以下の例において、FPT_PHP.2コンポーネントを具体化したものは、TOEを構成するハードウェア及びファームウェアの保護に対する物理的セキュリティ要件を表している。コンポーネントFPT_PHP.3は、もし改ざんが検出されたとき、暗号関連のIT資産を保護するためにとられるアクションを特定する。 (566)

FPT_PHP.2 物理的攻撃の通知

FPT_PHP.2.1 TSFは、TSFを弱体化する恐れがある物理的改ざんについての曖昧さのない検出を提供しなければならない。TSFの内容物は、TOEの外郭またはカバーの穿孔、研磨または研削などの手段による改ざんを検出する改ざん検出エンベロープ内に、完全に含まれていなければならない。

FPT_PHP.2.2 TSFは、TSFの装置やTSFのエLEMENTに物理的改ざんが生じたかどうかを決定する能力を提供しなければならない。

FPT_PHP.2.3 TOEを構成する装置/ELEMENTに対し、TSFは、装置とELEMENTを監視し、かつTSFの装置及びTSFのエLEMENTに物理的改ざんが生じたとき、TOEの利用者に通知しなければならない。

FPT_PHP.3 物理的攻撃への抵抗

FPT_PHP.3.1 TSFは、TSPが侵害されないよう自動的に対応することによって、以下のTSF装置及びTSFのエLEMENTへの物理的攻撃シナリオに抵抗しなければならない:

- a) TOEは、頑丈な取り外し不能な筐体の中に入れられていなければならない。その外郭は、それを取り外すまたは侵入しようとする試みがTOEに対して深刻な損傷を引き起こす (すなわち、TOEが動作しなくなる) 高度の蓋然性を持つように設計されねばならない。
- b) TOEのカバーまたは筐体に通気孔またはスリットがある場合、それらは小さく、かつ検出されない筐体内部の物理的探索を防ぐような形で構成されていなければならない (例えば、少なくとも90度の曲げを一つ入れるかまたは強固な障害物による遮蔽)。
- c) 改ざんの検出において、すべての平文暗号鍵及びその他の保護されていない機密のセキュリティパラメータは迅速にゼロ化されねばならない。

C.4.5.7 電磁放射方針

ガイダンス

TOEによって放射される電磁放射のレベルは、許可されていない人または利用者への、暗号関連IT資産の暴露を防ぐために制限されるべきである。加えて、許可されていない人または利用者へ電磁放射が検出されるのを防ぐため、手続き的及び物理的手段もまたとられるべきである。同様

に、完全性または可用性の観点上、望ましくないソースからの電磁干渉(EMI) /無線周波数 (RF) 放射の防衛に関わる物理的シールドの要件があるかもしれない。(567)

しかしながら、電磁放射制御 (例えばTEMPEST) のようなITセキュリティの技術的物理的側面の評価は、ISO/IEC 15408によって明確にはカバーされていない ([15408-1]1項、1ページ、項目b参照) が、とは言え、あげられた概念の多くはその領域に適用可能である。特に、ISO/IEC 15408は、TOEの物理的保護のいくつかの側面に対応する。(568)

ISO/IEC表現

組織のセキュリティ方針ステートメント (C.3.2節参照) は、TOEに要求される電磁放射制御を定義するのに使用されるべきである。(569)

もし電磁放射要件の評価が明示的にISO/IEC 15408から除外されているとするならば、TOEに対してそのセキュリティ方針を実装するという要求事項をはっきりと表すために、前提条件を使用すべきである。前提条件はまた、許可されていない人または利用者が電磁放射を検出するのを防ぐため、または望ましくないEMI/RF放射を防ぐためにとる必要がある、あらゆる手続き的及び物理的手段を特定するのに用いるべきである。(570)

C.4.6 TOEセキュリティ 機能性

C.4.6.1 序説

TOEセキュリティ方針の側面を実施するために要求されるセキュリティ機能性は、前出の節で対応されている。この節は暗号機能性を含むTOEで典型的に見られる、残りのセキュリティ機能性に対応する。(571)

暗号機能性を含む有効でセキュアなTOEを提供するために、2つのタイプのセキュリティ要件が典型的に考慮される必要がある：(572)

- a) 暗号機能セキュリティ要件
- b) 暗号機能性とTOEセキュリティ方針をサポートする、その他の非暗号機能及び保証セキュリティ要件

ISO/IEC 15408を用いてTOEセキュリティ方針を表現する方法についての解説は、C.4.5節に限られる。(573)

C.4.6.2 暗号機能性

ガイダンス

暗号鍵はライフタイムを通して管理されるべきである。暗号鍵のライフサイクル中の典型的なイベントは次のものを含む(しかし、それらに限定されるわけではない)：生成、配付、登録、保存、アクセス(例えば、バックアップ、アーカイブ、リカバリー)、そして破棄。(574)

最低限、暗号鍵は少なくとも次の段階を経るべきである：生成、保存、及び破棄。TOEが鍵のライフサイクルのすべてに關与する必要はないため(例えば、TOEが、暗号鍵の生成及び配付のみを行ってもよい)、その他の段階を含むかどうかは、実施される鍵管理の戦略に依存する。 (575)

実際の暗号機能セキュリティ要件は2つの異なるサブタイプとして考慮することができる： (576)

- a) 暗号鍵管理の側面を実行するためのセキュリティ機能要件、例えば；
 - 暗号鍵生成；
 - 暗号鍵配付；
 - 暗号鍵アクセス；
 - 暗号鍵破棄。
- b) 暗号鍵操作を実行するためのセキュリティ機能要件、例えば；
 - 電子署名生成及び/または検証；
 - 完全性及び/またはチェックサムの検証のための、暗号チェックサム生成；
 - セキュアハッシュ(メッセージまたはファイルのダイジェスト)の計算；
 - データの暗号化及び/または復号；
 - 暗号鍵暗号化及び/または復号；
 - 暗号鍵共有。

【ISO/IEC JTC 1/SC 27 N3816改訂情報】：段落577は以下に示すとおり動詞の形の変更("may be"から"should be"へ変更)及び暗号アルゴリズムや関連技法を扱う基準または標準への適合に関する記述が追加される。

この附属書の最初の部分で述べられているように、このガイダンスの範囲は、暗号鍵長とアルゴリズムの強度を含む暗号強度を除外している。実際、ISO/IEC 15408機能または保証ファミリ(AVA_SOFを含む)で、暗号機能強度または使用される鍵長の評価のために使用するべきものはない。これはISO/IEC 15408が、明確(specifically)に、暗号アルゴリズム及び関連技法のアセスメントをカバーしないからである。TOEに埋め込まれる暗号の数学的特性の独立したアセスメントが必要であるため、ISO/IEC 15408を適用する基となる制度は、そのようなアセスメントを準備すべきである。(ISO/IEC 15408-1の適用範囲も参照。) これは制度が追加のこの領域を扱う基準または標準への適合を要求できるということを含む。 (577)

【ISO/IEC JTC 1/SC 27 N3816改訂情報】：段落578は以下に示すとおり[9]への参照に関する記述が追加される。

擬似乱数生成器の実装もまた、暗号鍵及び暗号操作のセキュリティに対して重大である。擬似乱

数生成器に関連するアルゴリズム及びパラメタは、乱数空間のサイズと同様、予測不能性の程度を最適化するように選択されるべきである。TOEセキュリティ機能強度主張(AVA_SOF)は擬似乱数生成器の実装に対して提供されるべきである。 [\[9\]も参照。](#) (578)

ISO/IEC 15408表現

TOEが実行する暗号機能に依存して、以下のファミリからのコンポーネントがPP/STに含まれるよう選択されるべきである。 (579)

- a) FCS_CKM(暗号鍵管理)
- b) FMT_MSA(セキュリティ属性管理)
- c) FCS_COP(暗号操作)

[【ISO/IEC JTC 1/SC 27 N3816改訂情報】：段落580は以下に示すとおり\[6\]への参照に関する記述が追加される。](#)

FCSクラスは次のファミリに系統立てられることに留意せよ：FCS_CKM(暗号鍵管理)及びFCS_COP(暗号操作)。FCS_CKMファミリは暗号鍵の管理の側面に対応し、一方、FCS_COPファミリは暗号鍵の運用中の使用に関連する。 [\[6\]も参照。](#) (580)

FCS_CKMファミリからのコンポーネントは、暗号鍵管理方針の異なる側面を実装する機能要件を特定するために、使用することができる。そのファミリは暗号鍵ライフサイクルをサポートすることを意図され、そのため、暗号鍵生成、暗号鍵配付、暗号鍵アクセス、暗号鍵破棄の要件を定義する。暗号鍵の管理(management or administration)のための機能要件が存在するときはいつでも、このファミリは含まれるべきである。 (581)

しかしながら、PP/ST開発者は以下のことに留意すべきである： (582)

- a) FCS_CKMファミリは、記憶装置内にある暗号鍵の保護のための、特定のコンポーネントを提供しない。FDP_ACC(アクセス制御方針)及びFDP_ACF(アクセス制御機能)ファミリからのコンポーネントが、TSF内に保存される利用者暗号鍵(すなわち、利用者データとして保存される)の保護のために使用されることが推奨される。TSF暗号鍵(すなわち、TSFデータとして保存される)の保護は、FPT_SEP(ドメイン分離)ファミリまたはFMT_MTDファミリからのコンポーネントを使用することにより対応されるべきである。FDPまたはFPTの両方のクラスが、暗号鍵の機密性及び/または完全性を保証するために使用されることができる。
- b) FCS_CKMファミリは暗号鍵登録の保護のための特定のコンポーネントを提供しない。暗号鍵は暗号化されていない、または暗号化された、または知識分散(split knowledge)の形式で入力されるかもしれない。FDP_ITC(TSF制御外からのインポート)ファミリからのコンポーネントがこの要件を特定するために

使用されるべきである。使用された場合、「追加のインポート制御規則」の割付は、暗号鍵が知識分散形式に暗号化される必要があるかないかを定義するべきである。

- c) 暗号プロトコルセキュリティの側面はFCS_CKMファミリからのコンポーネントを使用して表現されるべきである(とりわけ暗号鍵配付に関するものは)。
- d) 公開暗号鍵が取り消される場合、FCS_CKM.2コンポーネントが公開暗号鍵の取消しを特定するために使用されるべきである。FCS_CKM.2が適切である理由は、このコンポーネントが暗号鍵配付計画を特定し、取消し情報の配付が、暗号鍵配付に欠くことのできない部分であるということである(例えば、認証取消しリストのためのX.509標準で実証されている)。

FMT_MSA(セキュリティ属性管理)ファミリからのコンポーネントが、暗号鍵属性を定義するために使用されるべきである。鍵属性の例は、利用者、鍵種別(例えば、公開、秘密、共通)、有効期限、そして用途(例えば、電子署名、鍵暗号化、鍵交換、データ暗号化)。 (583)

FCS_COPファミリからのコンポーネントを、暗号操作を実行する機能要件を特定するために使用することができる。暗号操作は1つまたはそれ以上のTOEセキュリティサービスをサポートするために使用されるかもしれない。FCS_COPコンポーネントは下記に依存して一回以上繰り返される必要があるかもしれない。 (584)

- a) セキュリティサービスが利用されるユーザアプリケーション
- b) 異なる暗号アルゴリズム及び/または暗号サイズの使用；及び/または
- c) 影響されるデータのタイプまたは秘匿性

暗号鍵のライフサイクル管理をTOEが実装しないまたは一部のみ実装する場合、TOE外部の(すなわち、TOE環境にある)活動またはコンポーネントに対するあらゆる主張は前提条件として表現されるべきである。 (585)

C.4.6.3 暗号関連 IT 資産のインポート、エクスポート、及び TSF 内転送

ガイダンス

人間利用者へ/から、信頼できないコンポーネントを間に入れてまたは直接転送される暗号関連IT資産(暗号化されていない暗号鍵、平文の認証データ及びその他の重要なセキュリティパラメタのような)のセキュリティは、利用者アクセス制御方針の実装に対して必然的である。 (586)

利用者がその情報の秘匿性を認識していること、そしてその情報またはその情報の秘匿性を、他の情報と偶然に混同することがないということが重要である。歴史的に、暗号設計者や実装者は、そのような情報の入出力のための分離された物理ポートを要求することにより、またそれにより利用者及びTOEにその情報の秘匿性を認識させることで、このことを達成してきている。他のアプローチはデータのセキュリティラベルを使用することだろう。 (587)

以下のファミリーからのコンポーネントが選択されるべきである： (588)

- a) FDP_ITC(TSF制御外からのインポート)
- b) FDP_ETC(TSF制御外へのエクスポート)
- c) FTP_ITC(TSF間高信頼チャンネル)またはFTP_TRP(高信頼パス)。

FDP_ITC.2コンポーネントからのエレメントが、TOEへの情報の導入に対するセキュリティ要件を表現するために使用されるべきである。これは、利用者アクセス制御SFPを使用して具体化されるべきである。 (589)

FDP_ETC.2コンポーネントからのエレメントが、TOEからのデータに対するエクスポート規則を特定するために使用されるべきである。これは、利用者アクセス制御SFPを使用して具体化されるべきである。 (590)

FTP_ITCファミリーからのコンポーネントが、TSFと他のTOEのTSFとの間の暗号資産の転送に対するセキュリティ要件を特定するために、使用されるべきである。その他、FTP_TRPファミリーからのコンポーネントが、人間利用者へからの暗号資産の入出力に対する要件を表現するために使用されることもできる。しかしながら、開発者は、FTP_TRPとFTP_ITCファミリーの使用は相互に排他的であることを認識すべきである。 (591)

【ISO/IEC JTC 1/SC 27 N3816改訂情報】：段落592は以下に示すとおりコンポーネントに対して操作された部分が識別される。

例えば： (592)

FTP_TRP.1 高信頼パス

FTP_TRP.1.1 TSFは、それ自身とローカル利用者間に、他の通信パスと論理的に区別され、その端点の保証された識別及び改変や暴露からの通信データの保護を提供する通信パスを提供しなければならない。

FTP_TRP.1.2 TSFは、それ自身とローカル利用者が、高信頼パスを介して通信を開始することを許可しなければならない。

FTP_TRP.1.3 TSFは、最初の利用者認証、及び暗号化されていない暗号鍵コンポーネント、平文の認証データ、及びその他の防御されていない重要なセキュリティパラメタの入出力に対して、高信頼パスの使用を要求しなければならない。

C.4.6.4 セキュアな状態の維持

ガイダンス

歴史的に、暗号機能性を含むTOEの設計エラーまたは誤動作に対する関連事項が、以下のタイプ

の要件が導入されることを導いてきた：

(593)

- a) 秘匿暗号情報の不注意による出力を防ぐために、暗号化されない暗号鍵、または重要なセキュリティパラメタ、または秘匿データを出力可能なあらゆる出力インタフェースを通過する出力データに対して、2つの独立した内部動作が要求される。
- b) TOEにエラーが検出された場合、TOEはエラー状態になり、すべての出力を禁止しなければならない。

最初のアイテムの意図は、TOEの設計または動作エラーが偶発的に秘匿暗号情報を解放することがないことを確実にすることである。(これは、TOEが秘匿暗号情報の解放を検出できることも暗示する。) 2番目のアイテムの意図は、TOEがエラーを検出した場合、秘匿暗号情報を解放すべきではないということである。要約すると、もしもエラーが起こった場合は、TOEはセキュアな状態を維持することを常に目標とすべきである。

(594)

ISO/IEC 15408表現

FPT_FLS(フェールセキュア)ファミリからのコンポーネントが、エラーが起こったときは常にセキュアな状態を維持することのTOEに対する要件を表現するために、選択されるべきである。例えば：

(595)

FPT_FLS.1 セキュアな状態を保持する障害

FPT_FLS.1.1 TSFは以下の種別の障害が生じたときはセキュアな状態を保持しなければならない：

- a) TOEが不正に暗号化されない暗号鍵、平文の秘匿データ、または、その他の保護されない重要なセキュリティパラメタを出力しようと試みる；
- b) 暗号機能の故障
- c) TOE抽象マシンテストの失敗(スタートアップ、オンデマンド 及び/または 条件付)；
- d) TOEの物理的改ざん(環境故障を含む)の検出

この2番目の状態は、信頼できる回復が実行されるまで、出力が禁止され、他のどの機能も実行されないことを意味しなければならない

PP/STの開発者は、このコンポーネントはADV_SPM.1(非形式的セキュリティ方針モデル)コンポーネントへの依存性を持つことに留意すべきである。加えて、PP/ST開発者は、エラーを発生する機能性(例えば、TOE自己テストを実行する機能性)を特定するコンポーネントを含む必要がある。

(596)

FPT_RCVファミリからのコンポーネントは TOEをセキュアな状態に回復する及び/または非セ

セキュアな状態への遷移(transition)を妨げるための要件を特定するために使用することが、選択的に必要になるだろう。(597)

C.4.6.5 暗号機能の自己テスト

ガイダンス

機能性が、そのようなエラーが実際に起こったことを検出することの必要性は、エラーが起きたときは常にセキュアな状態を保持することが、あらゆるTOEに必要であることから暗示される。(598)

典型的には、暗号機能性が正常に動作することを保証するために、TOEが暗号機能性の自己テストを実行するように設計される。このような自己テストは典型的に以下を含む：(599)

- a) スタートアップ(パワーオンまたはブート)自己テスト：
 - 既知回答(known answer)テスト；
 - ソフトウェア/ファームウェア完全性テスト；
 - 静的乱数生成テスト。
- b) オンデマンドテスト
 - 既知回答(known answer)テスト；
 - ソフトウェア/ファームウェア完全性テスト；
 - 静的乱数生成テスト。
- c) 条件及び条件付(conditions and conditional)テスト
 - 秘密、公開鍵ペア生成、ペアワイズ(pair-wise)一貫性テスト；
 - ソフトウェア/ファームウェア負荷、ソフトウェア/ファームウェア完全性チェック；
 - 鍵登録、鍵完全性テスト
 - 乱数発生、乱数テスト

ISO/IEC 15408表現

TOE自己テストの要件を特定するために、下記ファミリーの1つまたはそれ以上からのコンポーネントが選択されるべきである：(600)

- a) FDP_SDI(蓄積データ完全性)
- b) FPT_AMT(下層の抽象マシンテスト)
- c) FPT_TST(TSF自己テスト)

FDP_SDIファミリからのコンポーネントが、完全性エラーの検出と修復アクション(もしあれば)の要件を表現するために使用されるべきである。(601)

FPT_AMTファミリからのコンポーネントが、下層の抽象状態マシンに対して実行されるテストを特定するために使用されるべきである。(602)

FPT_TSTファミリからのコンポーネントが、次の要件を表現するために使用されるべきである：TOEの運用を止める必要が無い様々な故障による暗号コードの破壊の検出、TSFが正常に動作していることのテスト(例えば、スターアップ時に、オンデマンドに、及び条件により)(603)

C.4.6.6 外部依存性

ガイダンス

ある環境において、TOEは他のソフトウェア、ファームウェア、またはハードウェアに対して(例えば、下層のオペレーティングシステムのセキュリティ機能性に対して)依存性を持つ。(604)

ISO/IEC 15408表現

本ガイドの5節に記述したように、TOE外部のソフトウェア、ファームウェア、またはハードウェアにより満足されることを期待されるSFRは、PPまたはSTのIT環境のセキュリティ要件のセクションで特定されるべきである。(605)

C.4.7 TOEテスト(testing)

C.4.7.1 ガイダンス

TSFが少なくとも特定されたSFRを満足することの保証を提供するために、TOEの機能性はテストされるべきである。したがって、テスト要件はアプリケーションの秘匿性(sensitivity)及びそれらに対する保証の必要性に基づき選択されるべきである。次のことに注意がはらわれるべきである。テストが独立した第三者機関により実施(conducted)されるべきであるかどうか、テストの厳密性とカバレッジ、そして厳密さが適用されるTOE抽象(TOE abstraction)の性質(nature)(例えば、機能仕様、上位レベル設計、下位レベル設計)。(606)

攻撃に対するTOEの脆弱性もまた分析されるべきである。(607)

C.4.7.2 ISO/IEC 15408表現

以下のファミリからのコンポーネントが典型的に選択されるべきである：(608)

- a) ATE_COV(カバレッジ)
- b) ATE_DPT(深さ)
- c) ATE_FUN(機能テスト)
- d) ATE_IND(独立テスト)

e) AVA_VLA(脆弱性分析)

ATE_COVファミリからのコンポーネントが、TOEテストの完全性に対する要件を特定するために使用できる。 (609)

ATE_DPTファミリからのコンポーネントが、TOEがテストされる詳細さのレベルに対する要件を特定するために使用できる。 (610)

ATE_FUNファミリからのコンポーネントが、PP/STの他のところで識別されている機能要件を満たすために必要な特性をTSFが示すことを確立することに対する要件を特定するために使用することができる。 (611)

ATE_INDファミリからのコンポーネントが、TSFが特定されたように機能することを実証することに対する要件を特定するために使用することができる。 (612)

AVA_VLAファミリからのコンポーネントが、暗号機能性を含むTOEの環境故障テスト (environmental failure testing)に対する要件を特定するために使用することができる。 (613)

C.4.8 TOE 運用

C.4.8.1 ガイダンス

許可された利用者によるTOEのセキュアな生成、管理、及び運用のためのガイダンスが提供されるべきである。 (614)

C.4.8.2 ISO/IEC 15408 表現

PP/STにおいてこの要件を表現するために、次のファミリからのコンポーネントが選択されるべきである： (615)

- a) AGD_ADM(管理者ガイダンス)
- b) AGD_USR(利用者ガイダンス)

AGD_ADMファミリからのコンポーネントは管理者によりTOEがどのように正しく (correctly)生成され管理されるべきかという、文書に対する要件を表現するために使用されるべきである。 (616)

AGD_USRファミリからのコンポーネントはTOEがどのように正しく利用者に操作されるべきかという、文書に対する要件を表現するために使用されるべきである。 (617)

C.5 保証要件適用のガイダンス

前述のとおり、この文書の範囲は暗号強度、鍵長(size of key size)、またはアルゴリズムの強度については対応していない。しかしながら、暗号アルゴリズム(及び鍵長)の適切性(suitability)はISO/IEC 15408の範囲外であるものの、そのアルゴリズムのTOE内での実装は範囲内である。 (618)

TOEで使用されるアルゴリズム、モード、及び鍵長の選択は、TOE評価のスポンサーの責任である。スポンサーは、実装の正しさ(correctness)を保証(ensure)するために、以下のアプローチの内の1つまたはそれ以上のものを使用するかもしれない。(619)

- a) スポンサーは、特定の規則に準拠した実装を提供する
- b) スポンサーは、実装の標準適合性を立証する(vouch)。
- c) スポンサーは、適合性テスト要件を非適用にする(waive)。
- d) スポンサーは、適合性テストを行う。
- e) スポンサーは、評価者に適合性テストを要求する。これらのテストは、標準により特定された適合性テストを使用して行われなければならない。標準が適合性テストを特定していなければ、そのテストの他の出典を提供もしくは指し示す。
- f) スポンサーは、ADV_RCRコンポーネントに従い、実装をレビューする(例えば、詳細なコード・ウォークスルーを行う)。
- g) スポンサーは、評価者に、ADV_RCRコンポーネントに従い、実装をレビューする(例えば、詳細なコード・ウォークスルーを行う)ことを要求する。

実装レビューは、アルゴリズムの秘匿性によりソースコードが評価者に入手可能でないかもしれないため、ISO/IEC 15408保証レベルによらず、非適用にされるかもしれない。アルゴリズム適合性をテストすることはまた、適合性テストの入手性の不足により非適用にされるべきかも知れない(これは、とりわけ新しいアルゴリズムに対して当てはまる)。(620)

附属書D 作業例：ファイアウォールのPPとST

この附属書は、ファイアウォールに基づいた作業例を用いて、3章から8章内に含まれるガイダンスの適用を例示したものである。(621)

D.1 PP/ST概説

PPやSTの概説は、本ガイドの3章で述べたガイダンスに従って構成されている。STでのCC適合の主張では、STがCCパート2及びパート3に完全に適合しているのに加え、PPにも適合していることを述べている。(622)

D.2 TOE記述

PP及びSTのTOE記述の節は、本ガイドの3章で述べたガイダンスに従って構成されている。PPの場合、TOE及びそのセキュリティ機能性の範囲について一般的な記述が提供されている(TOEの唯一の目的はセキュリティのため)。さらなる詳細はSTで示される。特に、(623)

- a) 下層のオペレーティングシステムやハードウェアプラットフォームの識別
- b) 例えば、TOEの物理的保護の必要やファイアウォールの管理者と(ファイアウォールに直接ログインしない)利用者との区別に関するような、運用環境の簡潔な記述。

D.3 セキュリティ環境

D.3.1 前提条件

ファイアウォールに関しては、ファイアウォールの効力が蝕まれることがないことを保証するのに必要となるような多くの前提条件が識別される。例えば、(624)

- a) ファイアウォールはデュアルホーム化されている。そうでないとファイアウォールをまったくバイパスしてしまう可能性があるために要求される。
- b) 管理者のみがファイアウォールにアクセスできる。この前提条件は、攻撃に利用できる機会を制限するために必要である。

セキュリティ機構の使用(例えば、監査証跡管理と分析)についての前提条件は、環境に対するセキュリティ対策方針または非IT環境に対するセキュリティ要件のいずれかで扱われるだろう。

(625)

D.3.2 脅威

ファイアウォールに関して、その意図された環境は、ファイアウォールの片側がプライベートネットワークで、他方が敵意のあるとされるネットワークで構成されていると仮定される。保護さ

れるべきIT資産は、それゆえプライベートネットワークにより提供されるサービスであり、プライベートネットワーク上に格納された情報である。脅威エージェントは、大抵、*敵意のあるネットワーク上の攻撃者*である。 (626)

ファイアウォールによって対抗される脅威の例としては、次のようなものがあるであろう。 (627)

敵意のあるネットワーク上の攻撃者は、ホストや他のサービスへのアクセスを得るために、サービス実装における欠陥を悪用するかもしれない。

脅威のこのステートメントは前述のガイダンスに次のように従う。 (628)

- a) 脅威エージェントは*敵意のあるネットワーク上の攻撃者*である。
- b) 攻撃にさらされるIT資産は、プライベートネットワーク上のホストまたはその他のサービスである。
- c) 攻撃のやり方は*サービス実装の欠陥を悪用*する方法で示される。

この脅威のステートメントは、サービス実装(「sendmail」のような)における欠陥の悪用という点でガイダンスに矛盾していないことに注意すべきである。なぜなら、(関連するアプリケーションプロキシはTOEの一部であるが)それらはTOE自身の一部ではないためである。 (629)

ファイアウォールによって対応される脅威のほとんどは、*敵意のあるネットワーク上の攻撃者*によりもたらされるが、*攻撃者が敵意のあるネットワーク上でもプライベートネットワーク上のどちらでもあり得る*次のような脅威を識別することもできる。 (630)

攻撃者はファイアウォールへのアクセスを管理者への成りすましによって得るかもしれない。

意図された環境に導入されたファイアウォールの結果として、この特有の脅威が含まれる。脅威への対抗に関するファイアウォールの有効性が、ファイアウォールの識別された管理者にある程度は依存することを仮定する以外は、(既に述べたガイダンスと矛盾なく)TOEによって提供される対抗策に関してなにも前提としていないことに注意すべきである。(前提条件の「人的」の節は、役割やそれに伴う全般的な責務の存在を指摘することに注意すること)。 (631)

TOEによって対抗しないものとして識別された脅威は、ファイアウォールにおける実際的な限界を映し出す。例えば、 (632)

- a) セッションハイジャックやデータ探知のような、TOEでは対抗しない特定の攻撃方法が、*敵意のあるネットワークから攻撃者*によってもたらされる。
- b) プライベートネットワークは、プライベートネットワーク上の悪意のある利用者によって成される行為としての攻撃には弱いものとなるであろう。
- c) 到達するトラフィックの中に含まれているかもしれないウイルスへの、プライベートネットワークの脆弱性は、ファイアウォールが対抗するために設計されてい

ない脅威のひとつである。

- d) プライベートネットワークは、ファイアウォール管理者による行為または無為の結果としての攻撃には弱いものとなるであろう。
- e) プライベートネットワークは、ファイアウォール自身への物理的攻撃の結果としての攻撃には弱いものとなるであろう。

アプリケーションゲートウェイファイアウォールに対する可能性のある(そしてとりわけ興味深い)脅威は、 (633)

新しい、予め知られていない攻撃方法(例えば、以前の信頼できるサービスを用いた)を利用した敵意のあるネットワーク上の攻撃者。

このことは、敵意のあるネットワーク上の攻撃者によってもたらされる脅威はダイナミックである(すなわち、絶え間なく変化すること、そしてTOEそれ自身が例えば新しいアプリケーションに対するプロキシを提供するなどして変化していく必要があるだろうという事実を認識させる。(634)

D.3.3 組織のセキュリティ方針

一般に、ファイアウォールは多くの異なる組織のセキュリティ方針を実施するよう構成することができる。したがってこの例では、TOEが準拠すべき組織のセキュリティ方針を特定することによって得る部分は少ないかもしれない。しかしながら、一般的用語を用いてファイアウォールが実施すべきアクセス制御方針を述べることは可能であろう。 (635)

D.4 セキュリティ対策方針

D.4.1 TOEのセキュリティ対策方針

ファイアウォールのセキュリティ対策方針は、次のようなものをあげることができる。 (636)

- a) 主要なセキュリティ対策方針は、ファイアウォールに対し、例えばアドレスの有効な範囲や、アクセスできるホストやサービスポートの制限によって、アクセス制御を実施することである。
- b) サービス実装における脆弱性の脅威に対抗するための「健全化された」サーバを準備することは、アプリケーションゲートウェイファイアウォールのためのセキュリティ対策方針かもしれない。
- c) 同様に、アプリケーションプロキシ認証のためのセキュリティ対策方針もあるかもしれない。
- d) セキュリティに関連するイベントの記録の手段を提供する監査のためのセキュリティ対策方針。
- e) 管理者にとって有用であるべき機能と、またその機能性へのアクセスの管理の双方に関するセキュリティ管理のためのセキュリティ対策方針。

TOEのセキュリティ対策方針のサンプルとしては、 (637)

ファイアウォールは、プライベートネットワークでの一定の識別されたサービスについて、コネクションを確立するのに先立ってエンドユーザの認証を要求する能力がなくてはならない。

これは、TOEが識別と認証の機能性を備える必要があることの明らかな指針の役目となる。PPは提供されるであろうサービスについては識別しないため、セキュリティ対策方針も認証を要求するこれらのサービスのサブセットを識別しないことを特筆しておいてもよいであろう。誰が(ST根拠の中で)エンドユーザの認証を要求する(または要求するよう構成できる)これらのサービスを正当化しなければならないかは、ST作成者の課題として残される。 (638)

D.4.2 環境に対するセキュリティ対策方針

環境に対する対策方針の例として次のものがある。これらは監査機能性の使用に関連したものである。 (639)

ファイアウォールの管理者は、監査機能が効果的に使用及び管理されていることを保証しなければならない。特に、中断のない監査ロギングを保証するために適切なアクション(例えば、十分な空き領域を保証するための定期的なログのアーカイブなどによって)がとられなければならない。さらに、監査ログは定期的に検査されるべきであり、セキュリティ違反や将来的な違反を導くおそれのある事象を検出した場合には適切なアクションがとられるべきである。

したがって、このセキュリティ対策方針は、ファイアウォールが監査機能性を備えることのセキュリティ対策方針と密接に結びついている。 (640)

D.5 ITセキュリティ要件

D.5.1 セキュリティ機能要件

5章で述べられたガイダンスに従えば、以下のSFRが先の節で述べたようなTOEのためのセキュリティ対策方針に直に対応するものとして選択されるであろう。 (641)

- a) 想定されるターゲットホストやサービス、または想定される発信ホストやサービスに基づいた制御方針を施行することをファイアウォールに要求するセキュリティ対策方針は、FDP_IFF.1(単純セキュリティ属性)及びFDP_IFC.2(完全情報フロー制御)の適している使用か、またはFTA_TSE.1(TOEセッション確立)のいずれかにより満たされるであろう。
- b) アプリケーションプロキシ認証を提供することをファイアウォールに要求するセキュリティ対策方針は、FIA_UAU.2(アクション前の利用者認証)及び

FIA_UID.2(アクション前の利用者識別)により満たされるであろう。他の考慮に値するSFRとしては、FIA_UAU.3(偽造されない認証)、FIA_UAU.4(単一使用認証メカニズム)そしてFAU_UAU.5(複数の認証メカニズム)がより強固な認証メカニズムの仕様を可能にするものとして、含まれる。

- c) 監査機能性の備えを要求するセキュリティ対策方針は、FAU_GEN.1(監査データ生成)とFAU_ARP.1(セキュリティアラーム)によって、よりリアルタイムな監査分析を提供することで満たされるであろう。
- d) セキュリティ管理機能性の備えを要求するセキュリティ対策方針は、ファイアウォール管理者の認証に適用するFIA_UAU.2及びFIA_UID.2とともに、FMT_SMR.1(セキュリティ管理役割))によって満たされるだろう。

最初のセットが選択されると、主にISO/IEC 15408パート2の依存性を満たすために残りのSFRも選択されることになるだろう。有用なサポートする役割を提供するために、付加的なSFRも含まれるだろう。FIA_AFL.1(認証失敗時の取り扱い)、FPT_RVM.1(TSPの非バイパス性)そしてFPT_SEP.3(完全リファレンスモニタ)が例に含まれるかもしれない。(642)

さらに成されるべき決定は、監査のレベル(すなわち、*指定なし*、*最小*、*基本*または*詳細*)に関係する。適切なレベルは、TOEのセキュリティ対策方針に充分に対応し、同時に不当に重荷となるようなセキュリティ要件のセットを要求することのないものが選ばれよう。例えば、もしFTA_TSE.1(TOEセッション確立)がファイアウォールアクセス制御方針を特定するコンポーネントであった場合、成功及び不成功の試みがログされることを要求する監査の*基本*レベル(監査の最小レベルでは要求されない)が適切であろう。または、*指定なし*を選ぶこともでき、脅威に対し適切に考慮されたものとして選ばれた特定の監査対象事象を用いる。(643)

理解しやすくするために、必要であればファイアウォールPP中の割付は完了されるであろう。例えば、(644)

- a) 選択「*成功または失敗*」は、監査セキュリティ対策方針の明示的な要件のため、FAU_GEN.1.2に割付けられるだろう。
- b) 選択「*許可された管理者が設定可能な回数*」は、不成功な認証の試みの回数の選択における柔軟性を容認するために、ローカルなセキュリティ方針に合わせてFIA_AFL.1.1に割付けられるだろう。
- c) 割付「*アプリケーションプロキシ認証*」は、SFRを認証のこの種別に適用し、ファイアウォール管理者の認証にはない(おそらくこれは望ましくないセキュリティ要件であろう)ことを明らかにするためにFIA_AFL.1.1に割付けられるであろう。

D.5.2 保証要件

保証要件の選択は比較的容易であろう。もしPPまたはSTの作成者が、特定の保証要件の必要を(そのセキュリティ対策方針にて)識別しないならば、選択は単純に適切なEALの選択ということにな

るだろう。例えば、脅威の特質(比較的精巧な攻撃を含む)とIT資産の価値は、適合の主張がなされているであろう既存のTOEによって達成しうる保証レベルをも鑑みて、EAL4を適している選択として指し示すかもしれない。(645)

D.5.3 IT環境におけるセキュリティ要件

ファイアウォールは、それ自身では必ずしもTOEに対するセキュリティ対策方針を満たすのに必要なすべての機能性を提供しない。例えば、ファイアウォールはファイアウォール監査証跡の格納の提供を、下層のオペレーティングシステムに頼ることは許容される。それゆえ、PP作成者はすべての場合においてどの機能性をファイアウォールに要求するか、またオプションとしてどれを下層のオペレーティングシステムにより提供することができるかについての判断を下す必要がある。(646)

とられるべき適切なアプローチは、ファイアウォールによって提供される機能の最小限のセットにより、TOEに対するセキュリティ対策方針を直接的に提供するものとして識別されるすべてのSFRを含むであろう。(例えば、ISO/IEC 15408パート2の依存性を満たすために)PPに含まれる他のセキュリティ要件は、適当と見なせればIT環境のためのセキュリティ要件の節に載せることもできる。(647)

例えば、格納された監査証跡の保護のためのセキュリティ要件(例えば、FAU_STG.1)は、関連する監査証跡のレビューのためのセキュリティ要件(例えば、FAU_SAR.1)とともにIT環境に置くことができる。しかしながら、一次SFRに関するセキュリティ属性の管理に関連したSFR(FMT_MSA.1を用いて識別される)は、ファイアウォールに置かれるだろう。(648)

同様に、TOEに対するセキュリティ対策方針は、管理者を認証する必要を示していても、PPはこの機能が下層のオペレーティングシステムによって提供されることを許している。このことは、対応すべき基本となるセキュリティ対策方針が、許可された管理者のみがファイアウォールに対して管理上の制御を行使できることが保証されなければならないという点で、理に叶わないことではない。管理者の認証は、このセキュリティ対策方針に対応しうる手段と見なすことができる。(649)

この場合の保証要件の選択は、TOEセキュリティ保証要件(例えばEAL4)により決定されるため容易である。(650)

D.6 TOE要約仕様

D.6.1 ITセキュリティ機能

ITセキュリティ機能の構築において、ST作成者はSFRから着手し、ITセキュリティ機能をそれらのSFRから次の方法で引き出すことができる。(651)

- a) 機能性、特に(TOEの主な目的を象徴する)ファイアウォールのアクセス制御機能を理解しやすくするために適切であれば、TOE固有の詳細が加えられる。
- b) サポート機能(特にセキュリティ管理機能)において、本質的な詳細を損ねることなく機能をより簡潔にする試みがなされるであろう。いくつかの場合、これはひとつのセキュリティ機能においてひとつ以上の機能要件の組合せを導くことになる。

最初の例は以下のとおりである。

(652)

TOEはアクセスを以下に基づき制御する。

- 想定される発信IPアドレスとホスト名
- 想定される発信ポート番号
- 宛先IPアドレスまたはホスト名
- 宛先ポート番号

2番目の例は以下のとおりである。

(653)

ファイアウォール管理者は(そしてファイアウォール管理者のみが)、以下の機能を実行することができる。

- ファイアウォール制御パラメタの表示及び変更
- 利用者認証データの初期化及び変更
- 利用者属性の表示及び変更
- 監査すべき事象の選択
- 可能性のある、または差し迫ったセキュリティ侵害を示すと考える監査事象のサブセットの識別
- 個々の認証メカニズムと特定の認証事象の関連付け
- ファイアウォールの完全性の検証

このように、いくつかのSFRの要件をひとつのITセキュリティ機能にカプセル化することが可能である(このSFRはFMT_MSA.1.1、FMT_MOF.1.1、FMT_MTD.1.1そしてFPT_TST.1.3を用いて特定される必要がある)。しかしながら、ここにおけるセキュリティ機能のより簡潔なステートメントは、多様な管理者役割を実装するTOEでは、それらが達する範囲というものが減じられてしまうことに注意すること。

(654)

[【ISO/IEC JTC 1/SC 27 N3816改訂情報】：以下に示すとおり「D.6.2 保証要件」及び「D.7 PP主張」に関する記述が追加される。](#)

[D.6.2 保証要件](#)

[ST作成者はここでTOEのための保証要件を満たす開発環境のそれらのエレメントを識別し記述するだろう。](#)

[D.7 PP主張](#)

ファイアウォールSTは、ここでファイアウォールSTが基づいているファイアウォールPPを識別しそしてファイアウォールSTがそれらに適合していることを識別するだろう。

D.7 PP根拠

D.7.1 セキュリティ対策方針根拠

セキュリティ対策方針の脅威への対抗の適切性の実証は、次のことで示される。 (655)

- a) どのセキュリティ対策方針がどの脅威に対抗しているかを(例えば、ファイアウォールアクセス制御方針の必要を定義しているO.ACCESSは、IPスプーフィングや脆弱なサービスへの攻撃のような敵意のあるネットワーク上の攻撃者によってもたらされる脅威と相互関係にある)表で示し、それぞれのセキュリティ対策方針がすくなくともひとつの脅威にマッピングされることを保証する。
- b) それぞれの脅威について、なぜ識別されたセキュリティ対策方針が脅威に対抗するのに適しているかについての論拠を提供する。

適切性の正当化の例は以下のように示される。 (656)

T.PROTOCOL 敵意のあるネットワーク上の攻撃者は、サービスプロトコルの不適切な使用を悪用するかもしれない。(例えば使用のために定義されたポート以外のプロトコルの「よく知られた」ポート番号を用いる)。

*O.ACCESS*は悪意のあるネットワークとプライベートネットワークそれぞれからアクセスできるホストとサービスポートを制限する。*O.AUDIT*はファイアウォール管理者に攻撃の可能性を検出する方法を提供することで、ゆえに適切なアクションを取ることにより、それらを監視する。*O.ADMIN*は、*O.INSTALL*や*O.TRAIN*によりサポートされたファイアウォールのセキュアな管理上の制御を保証することにより、本質的なサポートを提供する。

D.7.2 セキュリティ機能要件根拠

SFRがTOEに対するセキュリティ対策方針を満足することの適切性の実証は、次のことで示される。

(657)

- a) どのSFRがどのセキュリティ対策方針を満たしているかを(例えば、FDP_ACF.1とFDP_ACC.2はO.ACCESSと相互関係にあるかもしれない)表で示し、それぞれのSFRがすくなくともひとつのセキュリティ対策方針にマッピングされることを保証する。
- b) それぞれのTOEのためのセキュリティ対策方針について、なぜ識別されたSFRがこれらのセキュリティ対策方針を満足するのに適しているかについての論拠を提供する

適切性の正当化の例は以下のように示される。

(658)

O.ADDRESS ファイアウォールは、プライベート及び悪意のあるネットワークの双方で想定されるアドレスの有効範囲を制限しなければならない(すなわち、外部ホストは内部ホストを騙れない)。

*FDP_ACF.1*は*FDP_ACC.2*とともに、*O.ADDRESS*により要求されるやり方で、アクセス制限の能力を提供する。また、*FPT_RVM.1*はこれらの機能がいつも必要なときに行使されることを保証する。

相互サポート及び内部的一貫性の実証は、まず7章のガイダンスに従った依存性分析を用いて提供してもよい。これは、バイパス、改ざんそして非活性化攻撃に対し、如何にそれぞれのSFRが他のSFRによって保護されているかを示した表によって補足することもできる。この後に表内容の説明が置かれるだろう。それぞれのSFRを順に取り上げる(それは反復の解説に結びついている)よりも、むしろ表の内容が理解できるように一般的な問題を強調することもできる。例えば、(659)

改ざん攻撃は次のことで防止できる。

- ドメイン分離を保守し、また特に攻撃者のセキュリティ機能への改ざんを防止する*FPT_SEP.3*;
- 属性や構成データの変更を許可された管理者に制限する(例えば、*FMT_MSA.1*に基づくような)セキュリティ機能;
- その完全性がセキュリティ機能に決定的であるような他のデータの不当な変更を防止する(すなわち*FMT_MTD.1*に基づく)セキュリティ機能。

D.7.3 保証要件根拠

PP根拠のこのパートの構築は、PPが(例えば)ELA4を必須としており、いかなる付加的な保証要件をも指定していないのであれば、比較的容易であろう。この場合は、EAL4がすべての保証依存性を満足するような、知られている相互サポートのセットと内部的に首尾一貫した保証コンポーネントを提供すると主張することができるだろう。

(660)

EAL選択の正当化は以下のように示されるであろう。

(661)

- a) 評価者が下位レベル設計やソースコードにアクセスできる(そのようなアクセスは、TOEセキュリティ環境の節で指し示していたように、精巧な攻撃に対しての防御をTOEが提供していることの確信を与えるために必要となる)最小のEALとして、EAL4が必要であることは論証されるかもしれない。
- b) 開発者側に関しては、TOEのこの種別は専門技術を要しないため、これに対しEAL4は達成しうるということが論証されるかもしれない。

D.8 ST根拠

ファイアウォールPPに準拠して作成されたSTでは、ST根拠はPP根拠を広範囲に再利用するであろう。特に、 (662)

- a) もし脅威、組織のセキュリティ方針、前提条件、セキュリティ対策方針がまったく一致していれば、ST中のセキュリティ対策方針根拠はPPで与えられたものと同じであろう。つまり、ST根拠のこの部分は単にPP根拠の関連する節を参照するだけであろう。
- b) もしSTが、PPで定義されたSFRに少数のSFRを追加するのであれば、ST根拠はPP根拠の関連する部分を参照し、そして次の理由を示すであろう。
 - なぜ付加した要件は、セキュリティ対策方針を満足するのに適しているか。
 - なぜ付加した要件は、相反をもたらすことなく、他の要件をサポートするものであるのか。
 - なぜ付加した依存性は満足されるか、または満足される必要がないのか。
- c) もし、ST中にまったく同じセキュリティ保証要件が特定されていれば、保証要件根拠は単にPP根拠の関連する部分を参照するだけであろう。

これは、ST根拠によりカバーされるべき以下の側面を残している。 (663)

- a) PP準拠の正当化。これは、すべてのPP SFRの適用範囲(カバレッジ)を実証するための表と、いかに適切なPP操作がSTで完了されているかを示す第2の表の使用を通して示される。
- b) ITセキュリティ機能根拠。これは、特定されたITセキュリティ機能をSFRに明示的にリンクすることによって示される。もし、このレベルでいかなる新しい機能性も導入されないのであれば、相互サポートの実証はセキュリティ要件根拠によってもたらされたと思なされるであろう。

附属書E 作業例：データベースPP

この附属書は、データベース管理システム(DBMS)に基づいた作業例によって3章から8章の中に含まれるガイダンスの適用を説明する。この例において、DBMSは、自由裁量に基づくデータベースの中に保持された情報の機密性、完全性及び可用性を保護する必要がある商用環境での使用を意図する。 (664)

E.1 TOEセキュリティ環境

E.1.1 前提条件

データベースについては、TOEセキュリティ環境に関する前提条件のステートメントがTOEの範囲及び境界を明確に確定することが重要である。データベースの有効性が蝕まれることがないことを保証するのに必要となる識別される多くの前提条件が下層のプラットフォーム(典型的に、下層のオペレーティングシステム)に置かれるであろう。例えば、以下の一般的な前提条件が作られるかもしれない: (665)

A1 TOEは、セキュアなやり方で、すなわち、関連のある製品のセキュリティターゲット及びガイダンス文書に従ってインストールされ操作されると仮定される下層のオペレーティングシステムを信頼する。

A2 TOEの処理資源及び下層のオペレーティングシステムは、許可されない物理的なアクセスから保護されると仮定する。

より特徴的な前提条件は、データベースファイル、実行形式など、したがって、オペレーティングシステムの許可された利用者が、データベースによって実装されたセキュリティ機能を迂回することができないように、下層のオペレーティングシステムが格納することによって適切に保護される。この前提条件は、以下のように述べられるかもしれない: (666)

A3 すべてのデータベースに関連するファイル及びディレクトリは、下層のオペレーティングシステムによって許可されないアクセスから保護されると仮定する。

PPの中でのこのポイントは、主要な関連事項がTOE自体によって対応されるセキュリティニーズの範囲及びどの側面が下層のオペレーティングシステムによって満足されることになっているかを確定することを覚えておくことが重要である。下層のオペレーティングシステムの(IT環境の一部としての)セキュリティ対策方針及び要件は、PPの中でその後特定される。 (667)

3章及び4章に記述されるように、セキュリティ機構の使用(例えば、監査証跡管理及び分析)に係る前提条件は、環境のセキュリティ対策方針として扱われるであろう。 (668)

E.1.2 脅威

データベースについては、保護されるIT資産がデータベースオブジェクトである、そして、特にデータはそれらのオブジェクトの内部に含まれる。データベースオブジェクトは、他のデータベースオブジェクトに含まれていたデータの集合を含むかもしれない。それらのオブジェクトに格納された情報の機密性、完全性及び可用性を、データベースオブジェクトの所有者が希望するように従って保護する必要がある。(669)

脅威エージェントは、データベースの許可された及び許可されない利用者を含む。あとのカテゴリは、下層のオペレーティングシステムの許可された及び許可されない利用者の両方を含む。(670)

データベースに保持された情報の完全性及び有効性に対する脅威の追加の潜在的な原因は、ハードウェア、電源、記憶媒体などの故障から発生する操作を中断するような外部からの事象である。(671)

データベースに保持された情報への許可されないアクセスの2つの主な脅威は、以下のように表わすことができる:(672)

T1 攻撃者は、許可されたデータベース利用者のなりすましの結果、または匿名のアクセスの結果、データベースへのアクセスを獲得する。

T2 許可されたデータベース利用者は、保護しているデータを所有する、または責任を持っている利用者の許可なしにデータベースの中に含まれる情報にアクセスする。

これらの脅威ステートメントは、以下の方法で3章の中で与えられたガイダンスに従う:(673)

- a) 脅威エージェントは、T2では許可されたデータベース利用者であるが、T1の場合は許可されない、または許可されたデータベース利用者であってよい;
- b) (両方の脅威の)攻撃を受けるIT資産の主体は、アクセスされているデータベースオブジェクトに保持された情報である;
- c) 攻撃の形式は、T1ではなりすましまたは匿名のアクセスによって、そして、T2では情報へのアクセスによって示される。

データベースに保持された情報の可用性を保護する必要性は、以下の脅威を生じさせるかもしれない:(674)

T3 許可されたデータベース利用者は、他の許可された利用者がデータベースにアクセスする能力を危うくするという形でグローバルなデータベース資源を消費する。

脅威T3では、危険にさらされているIT資産がまだデータベースに保持された情報であることが注意されるべきである;「グローバルなデータベース資源」は、単にデータベース情報の可用性に対する攻撃を実行していることを意味している。(675)

TOEによって対抗されないとして識別された脅威は、DBMSに対する実用的な制約として反映す

る。例えば: (676)

TE1 データベースは、TOEによって与えられた特権を悪用する高度に信頼された利用者から、TOEによって確実に保護することができない。

これは、許可された利用者による特権の悪用の一般的な脅威に対する警告となり、セキュリティ監査が通常の対抗策である。明確に、監査記録を削除することができる十分な特権を持つ、ある信頼された利用者があるであろう、そして、このように「それらの形跡を隠す」。これは、高度に信頼された利用者が、確かに信頼できる個人であることを保証する適切な手続き的手段の確立を強いることになる。脅威TE1は、それゆえに、この必要性に対応するための環境のセキュリティ対策方針を生じさせるであろう。 (677)

E.1.3 組織のセキュリティ方針

PPは特定の組織による使用のための対象とされないが、準拠するTOEが(脅威のステートメントから明白でないかもしれない)実装されるべきである一般的なアクセス制御の方針を述べる事が可能である。例えば: (678)

P1 特定のデータベースオブジェクトへのアクセス権は、次のものによって決定される:

- a) オブジェクトの所有者;
- b) アクセスを試みるサブジェクトの識別情報;
- c) サブジェクトに与えられたオブジェクトへのアクセス権;
- d) サブジェクトによって保持された特権。

E.2 セキュリティ対策方針

E.2.1 TOEのセキュリティ対策方針

上記で識別された脅威T1、T2及びT3に対応するために、以下のようにDBMSのセキュリティ対策方針を指定することができる: (679)

O1 TOEシステムは、TOEの利用者を識別する手段を提供しなければならない。

O2 TOEは、個人が所有するまたは、P1セキュリティ方針に従って、責任のあるデータベースオブジェクトへの識別された個人によるアクセスを制御し制限する能力をエンドユーザに提供しなければならない。

O3 TOEは、同時セッションの数を含み、TOEの特定された利用者によってグローバルな資源の消費を制御する手段を提供しなければならない。

これらは、関連ある脅威及び直接参照されたOSPに対応することを注意することができる。O1は、IT環境の一部である下層のオペレーティングシステムによって、TOEの利用者の要求された識別

情報が認証されるという前提条件に基づいているので、特に興味を起こさせる。下層のオペレーティングシステムによる識別及び認証の必要は、環境のセキュリティ対策方針として表現されるであろう。(680)

E.2.2 環境のセキュリティ対策方針

上記のE.1.2節で識別された脅威TE1は、高度に信頼された利用者に関係のある環境のセキュリティ対策方針の必要を識別した。これは次のセキュリティ対策方針に反映することができる。(681)

OE1 TOEに責任のある人は、単に高度に信頼された個人が以下のことを許す利用者特権を割当てられることを保証するために、適切な手続き的及び人的手段が確立され、そして実装されることを保証しなければならない:

- a) 監査データまたは監査設定の改変;
- b) 利用者セキュリティ属性の改変(利用者特権の許可された許可を含む)。

環境のセキュリティ対策方針のさらなる例を以下に示す、下層のオペレーティングシステムの使用が適合する。(682)

OE2 TOEに責任を持つ人は、下層のオペレーティングシステムの各利用者アカウントの認証データがセキュアに保持され、そのアカウントを使用するために許可されない個人に開示されないことを保証しなければならない。

これは、データベースファイルが下層のオペレーティングシステムによって十分に保護されることを保証する必要を与えられた(上記のE.1.1節に記述された前提条件で表現された)必要なセキュリティ対策方針として識別される:認証データがそれ自体保護されない場合、攻撃者はこれらのアクセス制御を迂回することができるかもしれない。(683)

E.3 ITセキュリティ要件

E.3.1 セキュリティ機能要件

5章の中で記述されたガイダンスに引き続いて、前節の中で記述されるように、以下のSFRがTOEのセキュリティ対策方針を直接満たすために選択されるかもしれない。(684)

- a) セキュリティ対策方針O1は、TOEによる利用者の識別を要求する(認証は、下層のオペレーティングシステムによって実施される)、そして、SFRが指定したFIA_UID.1(識別のタイミング)、及びFIA_USB.1(利用者・サブジェクト結合)を使用することで満足することができる。
- b) セキュリティ対策方針O2は、データベースオブジェクトに対してアクセス制御の実施を要求する、そして、SFRが指定したFDP_ACC.1(サブセットアクセス制御)、及びFDP_ACF.1(セキュリティ属性によるアクセス制御)を使用すること

で満足することができる。

- c) セキュリティ対策方針O3は、グローバル資源の消費に対する制限を要求する、そして、SFRが指定したFRU_RSA.1(最大割当て)、及びFTA_MCS.1(複数同時セッションの基本制限)を使用することで満足することができる。

同様の方法で、PPに含まれた他のセキュリティ対策方針は、要求されるSFRを指定して適切なISO/IEC 15408パート2コンポーネントを選択することによって満足されるであろう (例えば、FAU_GEN.1は監査する要件を指定する)。(685)

最初のセットを選択した後、残ったSFRはISO/IEC 15408パート2の依存性を満足するために、または他のサポートする機能性を識別するために選択されるであろう。例えば:(686)

- a) FMT_MSA.3(静的属性初期化)は、新しく作成されたデータベースオブジェクトのデフォルト保護に対する管理を指定するために(FDP_ACF.1の依存性として)必要である。
- b) FMT_MSA.1(セキュリティ属性の管理)は、利用者のセキュリティ属性及びオブジェクトのセキュリティ属性の改変または割当てに対する管理を指定するために必要である。明快にするために、その繰返し操作が利用者とオブジェクトに対する管理を指定するために使用される必要があるであろう、なぜならば、後者がオブジェクト所有者によって、前者が許可された管理者のみによって改変されるかもしれないからである。
- c) FDP_RIP.1(サブセット残存情報保護)は、データベースアクセス制御方針をサポートするオブジェクト再使用機能性を指定するために使用されるであろう。
- d) FAU_SAR.1(監査レビュー)は、誰が監査データをレビューすることができるのかを指定するために選択されるかもしれない (例えば、許可された利用者は、それらが所有するオブジェクトに関係のある監査記録を読むことができるかもしれない、しかし、許可された管理者だけは全体の監査証跡をレビューすることができるであろう)。

さらなる決定は、監査のレベル(すなわち、*指定なし*、*最小*、*基本または詳細*)に関係する。適切なレベルは、監査要求が過度に面倒でないことを同時に保証して、TOEのセキュリティ対策方針と一貫させるために選ばれるであろう。実際は、*最小*、*基本または詳細*のどれでもない場合、適切な脅威とセキュリティ対策方針が与えられると考えられ、*指定なし*のレベルが選択されるであろう、そして監査対象事象のセットが適切に選ばれる。(687)

PPで完了した操作は、明快さの目的のためにイタリック体にされるであろう。例えば:(688)

FMT_MSA.3.1 TSFは、データベースオブジェクトのアクセス制御方針SFPを実施するために使われるセキュリティ属性として、*制限的デフォルト値*を与えるデータベースオブジェクトのアクセス制御方針SFPを実施しなければならない。

FMT_MSA.3.2 TSFは、オブジェクトや情報が生成されるとき、デフォルト値を上書きする代替の初期値を指定することをどの利用者にも許可しなければならない。

E.3.2 保証要件

5章に記述されるように、保証要件は技術的妥当性によって、制約される脅威の性質を考察することにより抽出される。商用環境での使用を目的とするDBMSについては、EAL3の保証要件が適切であろう。[15408-3]、6.2.3副項、58ページの記述のように、EAL3はTOEの大幅なりエンジニアリングを必要とせずに、保証の中レベルを提供する。(689)

E.3.3 IT環境のセキュリティ要件

データベースTOEのために、この節は非常に重要である。下層のオペレーティングシステムがアクセス制御、(潜在的に)識別及び認証機能性を提供する必要があることは、セキュリティ対策方針のステートメントで既に識別されている。これは、制御されたアクセス保護機能性(例えば、例 Controlled Access PP(CAPP)に準拠されると評価された)を提供するオペレーティングシステムが適切であろうということを示唆しており、それゆえに、PPのこの節は適切なPPまたは機能パッケージへの準拠を要求するべきである。(690)

しかしながら、PPは一般的であることが意図されている、CAPP準拠(または同等のもの)が、IT環境のセキュリティ要件を満足することの1つの方法であるにしても、それが必ずしもそれらを満たすただ1つの方法でないことは覚えておくべきである。ISO/IEC 15408は、セキュリティ要件を指定するためにISO/IEC 15408パート2コンポーネントの使用を必須としないので、それらをもっと抽象的なやり方で定義することが受け入れられる、例えば本質的なセキュリティ要件をCAPP準拠を必須とせずに含める。準拠TOEのためのSTは、下層のオペレーティングシステム(s)によってこれらのセキュリティ要件がどのように満足されるのかを実証することでTOEが評価されるであろう。(691)

特定のセキュリティ要件は、TOEによって提供されたSFRの依存性を満足させることの結果として、識別されるかもしれない。例えば、FAU_GEN.1は、タイムスタンプを提供するためFPT_STM.1に依存する;この機能性は、データベースではなく下層のオペレーティングシステムによって提供されるかもしれない。(692)

IT環境の保証要件は、準拠TOEと少なくとも等しいかもしれない、つまりこの場合は、EAL3である。(693)

E.4 PP根拠

E.4.1 セキュリティ対策方針根拠

脅威に対抗するセキュリティ対策方針の適切性の実証は、7章の中で与えられたガイダンスをもとに以下のように提供されるかもしれない:(694)

- a) どの脅威に対抗するセキュリティ対策方針であるのかを表の手段によって示し、

各セキュリティ対策方針が少なくとも1つの脅威にマップされることを保証する(例えば、T3はO3によって対応される);

- b) それぞれの脅威について、なぜ識別されたセキュリティ対策方針が脅威に対抗するのに適しているかについての論証を提供する。

適切性の正当化の例を以下に挙げる: (695)

T3(資源の過剰消費)は、TOEが個々の利用者が持っているかもしれない同時セッションの数に対する制限の実施を含むそのような資源の消費を制限する手段を持っていることを保証するO3によって直接対抗される。O1は、資源を使用することを試みる利用者を識別する手段を提供することによってサポートを提供する。O2は、資源利用制御を回避されてしまうことがないように管理機能性へのアクセスを制御することによってサポートを提供する。

E.4.2 セキュリティ機能要件根拠

TOEのセキュリティ対策方針を満足するSFRの適切性の実証は、次のように提供されるかもしれない: (696)

- a) どのセキュリティ対策方針を満足するSFRであるのかを表の手段によって示し、各SFRが少なくとも1つのセキュリティ対策方針にマップされていることを保証する(例えば、FRU_RSA.1とFPT_MCS.1は、セキュリティ対策方針O3に対応する);
- b) それぞれのTOEのセキュリティ対策方針について、なぜ識別されたSFRが対策方針を満足するのに適しているかについての論証を提供する。

適切性の正当化の例を以下に挙げる: (697)

O3は、個々の利用者によるグローバル資源の消費を制御する手段を提供するFRU_RSA.1と利用者が持っているかもしれない多数の同時セッションの数を制御する手段を提供するFTA_MCS.1によって提供される。これらは、適切な利用者にセキュリティ属性の割当ての定義を許可することを提供するFIA_ATD.1と共に、これらの属性と利用者の代わりに動作するサブジェクトを関連付けるFIA_USB.1によってサポートされる。

依存性分析は、7章の中のガイダンスに記述された方法で表の手段によって提供されるかもしれない。 (698)

相互サポートと内部一貫性の実証は、依存性分析ではハイライトされなかった、識別されたSFRの間の追加の補助的依存性を識別すること及び論じることにより提供されるかもしれない(下層のオペレーティングシステムに対するセキュリティ要件の適切なところに含まれる)。これは、順番に各SFRを考慮すること、そして他のSFRがバイパスされるまたは改ざんされることを防ぐた

めの潜在的な必要性を考慮することによって構成されるべきである。例は、次のものを含んでいる： (699)

- a) FDP_RIP.1は、格納オブジェクトが、違うサブジェクトによって再使用されるまたはアクセスされる場合、これらのSFRがバイパスされることを防ぐことによってFDP_ACC.1とFDP_ACF.1をサポートする。
- b) FMT_MSA.1は、許可された管理者に利用者割当てを変更する能力を制限することにより、FRU_RSA.1とFTA_MCS.1をサポートする、したがって他の利用者がこれらのSFRをバイパスすることができないことを保証する。
- c) FAU_STG.1は、監査証跡の完全性の保護によりFAU_GEN.1をサポートする。

E.4.3 保証要件根拠

PP根拠のこの部分の構成は、(例えば)PPがEAL3を必須とし、あらゆる論証された保証要件を指定しない場合、比較的簡単に違くない。この場合、EAL3が相互サポートの既知のセット、そして内部に一貫した保証コンポーネント、すべての保証依存性が満足されることを提供すると主張することは可能であろう。 (700)

EALの選択のための正当化の理由は、E.3.2節に記述されたものに従って提供されるかもしれない。 (701)

附属書F 作業例：信頼できる第三者機関のPP

この附属書は、信頼できる第三者機関(TTP)に基づく作業例を用いて、3章から8章の範囲に含まれるガイダンスの適用を説明する。この例では、SFRがTTPによって提供されるサービスの種類に依存するという点で、柔軟性が必要である。例えば： (702)

- a) TTPが機密性サービスを提供できる、または提供できない；
- b) TTPが鍵生成サービスを提供できる、またはTTP加入者が彼ら自身でこの能力を持つことを想定することができる。

この考慮は、TTPがオプションとして提供することができる補足的なサービスのセットとともに、TTPが提供しなければならない中核的なサービスのセットを定義する概念となる。中核的なサービスは、公開認証鍵証明書³の加入者登録、生成、配付、取消し、及びアーカイブに関する、TTPの期待される最小限のサービスを提示する。TTPの補足的なサービスは、鍵生成、証明書検証、及び機密性サービス例えば鍵証明書管理、鍵回復、鍵エスクロー³というような機密性サービスを含む。(中核的なサービスと補足的なサービスとの間の区別における暗黙の了解事項とされているのは、TTP加入者が鍵生成、デジタル署名生成、検証等のような機能の実行への適用を、通常は彼らが自分自身で行うだろうという前提である。) (703)

しかしながら、これは、ISO/IEC 15408の準拠に関して問題を引き起こす。なぜならば、ISO/IEC 15408は、PPにおいてオプションのセキュリティ要件を特定することを許されていない。すべてのTTPサービスの可能な組合せに対するPPを作成する代替のアプローチは、可能な並び換えを多く与えられるので、非現実的であると考えられた。 (704)

それゆえ、この問題の解決法は、TTPの中核的なサービスのセキュアな提供をサポートするのに必要とされたPPにおいて、SFRの中核的なセットを定義することであった。更に、それぞれの識別された補足的なサービスに対して、機能パッケージが、そのサービスをサポートするために必要とされた追加されたSFRを識別するために定義された。それで、結果としてのTTP PPは、次のように使用されることができる： (705)

- a) 特定のTTPに対するSTは、中核的なSFRを満足することによってTTP PPに準拠することを実証する。そのSTは、TTPによって提供されるサービスに依存して、定義された機能パッケージの一つ以上に準拠を(オプションとして)主張することもできる。
- b) TTP PPは、TTPサービスの特定のセットに対する、他のPP生成の基礎として使用されることもできるだろう：そのようなPPは、SFRの中核的なセットと一つ以上の定義された機能パッケージを、適切に組合せたものに基づくことにな

³ この例の目的としては、鍵回復は、鍵エスクローとは別個のものであると考えられる。前者は、TTP加入者のみが彼または彼女の鍵の回復を要求することができる。後者は、他の機関(例えば、法律執行機関)がTTP加入者鍵を要求する権利を持つかもしれない。

るだろう。これは、TTP PPの「ファミリー」となるだろう。

F.1 TOEセキュリティ環境

F.1.1 前提条件

TTPにとって、TOEセキュリティ環境についての前提条件のステートメントが、TOEの範囲と境界を明確に規定することが重要である。この例においては、デジタル署名の生成、情報の暗号化や復号に使われる加入者アプリケーションは、TOEの境界の外側であると考えられる。これは、以下の二つの前提条件となる。 (706)

A.ALGORITHM 鍵のペアが関連するアルゴリズムの完全性が満たされないならば、TTPは公開鍵を認証しないと仮定される。

A.SUBSCRIBER 加入者は利用できる技術的方法を持ち、それによって(必要ならば)彼らが彼ら自身の公開/秘密鍵のペアを生成でき、デジタル署名を生成し検証でき、公開鍵証明書の検証ができるものと仮定される。

一つ目の前提条件は、もし関連したアルゴリズムの加入者への実装に信用がなければ、TTPによって発行された証明書の価値が下がってしまうということで、必要である。 (707)

二つ目の前提条件は、完結性のために必要とされる。TTPは、関連した補足的なサービスを提供することによって、この前提条件をささえることができた。そうでない場合、前提条件は、その能力はTOEの範囲外にある加入者アプリケーションによって提供される。 (708)

F.1.2 脅威

TTPにとって、保護されるべきIT資産は、TTPによって使用されたまたは生成された鍵とともに、TTPによって生成された、または格納(例えば、アーカイブ)された証明書である。公開鍵と証明書は、まさにそれらの本質によって、機密性の保護に対して何の必要性も持っていない；しかしながら、完全性と可用性は、本筋の関連事項である。一方で、秘密鍵または共通鍵は、不当な暴露に対する保護を要求する。これらは、証明書に署名するためにTTPによって使われる鍵、またはTTPによって生成や格納(回復やエスクローのために)される加入者鍵かもしれない。 (709)

最終的には、これらの資産は、加入者によってやりとりされた情報から価値を導かれ、その情報は鍵と証明書を保護のために使用される。情報それ自身は、TTPの制御の範囲内にはないが、鍵と証明書は制御範囲内にある。あまり目に見えない資産は、TTPそれ自身を運用する組織の評判である；更に、この資産は鍵と証明書に対する脅威によって、損害を受けることがあるかもしれない。 (710)

その脅威エージェントは、TTP加入者及びTOEの許可された利用者を含み、同様にTTP環境にアクセスするまたはTTPとの通信手段に関与することができる悪意ある個人を含む。 (711)

TTPの中核的サービスに関係のある脅威の例は以下である： (712)

T.AKEYREVEAL 加入者の秘密認証鍵が、知るための正当な必要性を持たない個人に暴露される。

この脅威のステートメントは、3章で与えられるガイダンスに次のように従う： (713)

- a) 脅威エージェントは、加入者の秘密認証鍵を知るための正当な必要性を持たない個人である；
- b) 攻撃にさらされるIT資産は、加入者の秘密認証鍵である；
- c) 攻撃の形態は、暴露されるという言い回しによって示される：受身または能動的などどちらかの攻撃に関連があること示している(これは、脅威の説明を伴うことによって敷衍されるだろう)。

二つ目の例は、公開認証鍵証明書の可用性に関連する： (714)

T.ACERTAVAIL TTPによって管理される一つの(または複数の)公開認証鍵証明書が、知るための正当な必要性を持つ加入者に配送または配付できない。

上記の脅威の特定において、危険にさらされた資産は、明らかに公開認証鍵証明書である。しかしながら、脅威エージェント及び攻撃の方法は明白ではない。この場合、可能性のある脅威の源(例えば、TOE自身の故障やTTP加入者の通信路の故障)及び関連する攻撃方法(これは故意のサービスの拒否の企てを含むだろう、またはもし脅威の源がTOEにおける操作上の誤りならば、明白な攻撃は含まれないだろう)を識別することは、脅威の説明を付け加えることに行き着く。 (715)

特定のTTPの補足的なサービスにだけ関連する脅威もまた識別される。例えば： (716)

T.CKEYAVAIL 一つの(または複数の)加入者機密性鍵が、知るための正当な必要性を持つ個人に配送または手渡しできない。

この脅威は、鍵回復サービスがどこで提供されるかに関連がある。もし鍵エスクローサービスや機密性鍵の生成サービスがTTPによって提供される場合も関連がある。 (717)

TOEによって対抗されえないいかなる脅威も、識別されなかった。これは、資産への潜在する脅威はTOEセキュリティ環境に関して作られた前提条件によって、明示的に除かれるということである。 (718)

F1.3 組織のセキュリティ方針

例えTTP PPが特定の組織が使用する対象とされなくとも、国の法律によって課せられたTTPを運営する規則があるかもしれない。次に示すOSPはその可能性を強調する；そのような一般的なセキュリティ方針要件は、識別された「セキュリティソリューション」に実際の効果はほとんどないけれども、TTP PPに基づくPPやSTにおいて、さらに詳しく述べられるだろう。 (719)

P.LEGAL TTPは、あらゆる当該の情報セキュリティの法律に適合することを要求される。

F.2 セキュリティ対策方針

F.2.1 TOEのセキュリティ対策方針

TTPのセキュリティ対策方針は、中核的及び補足的なサービスのセキュリティ対策方針に分類される。前者の例： (720)

O.CERTMANAGE TOEは、適宜に公開鍵証明書を生成、配付及び取消しする手段を提供しなければならない。

O.CERTVERIFY TOEは、公開鍵証明書を検証する手段を提供しなければならない。それは信頼できるポイントへの証明書の連鎖の検証を含む。

O.SIGNATURE TOEは、発信の証拠としてデジタル署名を生成する手段を提供しなければならない。

初めの二つ、O.CERTMANAGE及びO.CERTVERIFYは、TTP加入者に提供される中核的なTTPサービスに直接関連する。それに対してO.SIGNATUREは中核的なTTPサービスではない。しかし、それにもかかわらず、証明書生成の中核的サービスの提供のサポートにおいて、満たされなければならないセキュリティ対策方針である(すなわち、TTPは、それが生成する公開鍵証明書に署名する能力を持たなければならない)。 (721)

最小限のセットの中で他のセキュリティ対策方針は、TTP資産(例えば加入者及びTTP鍵のような)の十分な保護があることを保証するために定義される。これらは、TTP利用者の識別と認証、アクセス制御、及びセキュリティに関連するイベントの監査のための「標準オペレーティングシステム」のセキュリティ対策方針へ至る。 (722)

TOEのセキュリティ対策方針の「中核的な」セットへ加えて、補足的なサービスのセキュリティ対策方針が定義される。例えば、次に示すセキュリティ対策方針が鍵回復サービスに適用される： (723)

O.KEYRECOVER TOEは、その鍵を所有する加入者に代わって、将来のメッセージ復号を可能にする鍵構成要素(key material)を格納する手段を提供しなければならない。

F.2.2 環境に対するセキュリティ対策方針

環境に対するセキュリティ対策方針は、TTPの操作の完全性を維持するための手順に対して必要であることが識別される。これらは、以下を含む： (724)

O.CERTCHECKS TTPに対して責任を持つ者は、以下のことに適用する適切な手続き上のチェックを証明し実行しなければならない：

- a) 証明書生成(誤ったデータが証明書に加えられないことを保証すること)；
- b) 証明書検証(必要とされるときに、加入者は証明書検証の正式な結果を通知されることを保証すること)。

O.INITSUBAUTH TTPに対して責任を持つ者は、加入者及び(必要ならば)要求者を認証するために、適切な手順が適所に存在することを保証しなければならない。

セキュリティ対策方針O.CERTCHECKSは、無効な証明書の発行の結果、TTPの評判が損なわれないことを保証するために必要とされる。セキュリティ対策方針O.INITSUBAUTHは、(例えば)アーカイブされた秘密機密性鍵(鍵回復や鍵エスクローの目的のための)が、知るための正当な必要性を持たない個人に暴露されないようにするために必要とされる。 (725)

F.3 ITセキュリティ要件

F.3.1 セキュリティ機能要件

5章に記述されたガイダンスを受けて、SFRはTOEのセキュリティ対策方針を直接満たすために、最初に選択される。例えば、セキュリティ対策方針O.CERTMANAGEは、とりわけ、公開鍵証明書を生成する能力に対する必要性を示す。このSFRは、FDP_DAU.2(保証人識別情報付きデータ認証)を使うことで次のように特定することができる： (726)

CERTGEN.1^{FDP_DAU.2.1}TSPFは、識別され区別された名前と識別された公開鍵を結び付けること及び関連する秘密鍵の所有権の有効性の保証として使用できる公開鍵証明書を、生成する能力を提供しなければならない。
詳細化：公開鍵証明書は、定義された標準(例えば、X.509)に従って生成されるべきである。

SFR CERTGEN.1は、FDP_DAU.2.1を基にしており、詳細化操作を用いて、一般的な用語の証明書の代わりに、より具体的な公開鍵証明書をを用いて明確にしている。詳細化操作をさらに使用して、生成された証明書が定義された標準に従うべきであるという要件を特定する。 (727)

(これらがPPの状況の中でより重要であると考えられたので、PP作成者が[15408-2]のSFRのために代替ラベルを使用することを選択したことに注意すること。これは許されている、しかしPP作成者は上記の上付き文字が使用された例のように、SFRから使用された[15408-2]機能コンポーネントへの明確なマッピングを提供しなければならない。) (728)

コンポーネント中のもう一方の要素FDP_DAU.2.2は、セキュリティ対策方針

O.CERTVERIFYを満たすために必要とされる公開鍵証明書を検証する能力のための要件を特定するために使用される： (729)

CERTVERIFY.1^{FDP_DAU.2.2} TSFは、公開鍵証明書及び証明書を生成したTTPの識別情報を検証する能力をTTPに提供しなければならない。

詳細化：証明書検証は、最小限として以下を含むべきである：

- a) 署名検証；
- b) 有効期限をチェックすること；
- c) 取消しをチェックすること。

詳細化操作は一般的な用語である*証拠*を特定の公開鍵証明書に変更するために再び使用される。さらに詳細化操作の使用は、証明書の有効期限及び証明書の取消しのための付加的なチェックを導いている。 (730)

(このアプローチはガイドの6.2.6節に含まれるガイダンスに基づいていることに注意すること。このように、個々のエレメントにPPに特有の一意的ラベルが割り当てられており、関連したコンポーネントのすべてのエレメントはPPに含まれる。6.2.6節のガイダンスを受けて、詳細化操作のあらゆるそのような使用は、SFRを定義するために使用されるISO/IEC 15408の機能コンポーネント及びエレメントへの明確な追跡性をもって、PP根拠の中で説明される必要がある。) (731)

セキュリティ対策方針O.SIGNATUREは、発信の証拠としてデジタル署名を生成する能力を要求する。これはFCO_NRO.1(発信の選択的証明)を使用して、特定された以下のSFR導く： (732)

DIGITSIG.1^{FCO_NRO.1.1}TSFは、送信された情報のデジタル署名をTTPの要求により生成できなければならない。

DIGITSIG.2^{FCO_NRO.1.2}TSFは、情報の発明者の識別情報と証拠が適用される情報を関係付けることができなければならない。

DIGITSIG.3^{FCO_NRO.1.3}TSFは、TTPへ与えられた[割付：発信元の証拠における制限]の範囲でデジタル署名を検証する能力を提供しなければならない。

一般的な用語をより特定の用語に置き換えるという詳細化操作の使用が、再び見られる。例えば、DIGITSIG.1及びDIGITSIG.3(FCO_NRO.1.1及びFCO_NRO.1.3それぞれを使用して特定された)では、一般用語である*発信の証拠*は特定のデジタル署名で置き換えられる。DIGITSIG.2で、余分な言い回しの除去によって、SFRを明確にするために完全な割付けと結合された詳細化操作の使用が見られる：*情報*という語は *情報の [割付：情報フィールドのリスト]* の言い回しの代わりに使用される。 (733)

最初のセットを選択した後、残りのSFRは、ISO/IEC 15408パート2の依存性を満足させるかまたは他のサポートする機能性を識別するために選択される。例えば、O.CERTMANAGEのサポート

において、生成された証明書署名用のTTP鍵の生成を可能とするために次のSFRが必要とされる：
(734)

TTP_KEYGEN.1^{FCS_CKM.1}TSFは以下の[割付：標準のリスト]に合致する、特定された暗号鍵生成アルゴリズム[割付：暗号鍵生成アルゴリズム]と特定された暗号鍵長[割付：暗号鍵長]に従って、TTP公開/秘密鍵のペアを生成しなければならない。

このSFRはFCS_CKM.1を使用して特定される。明確にするために、一般的な用語の暗号鍵を、特定のTTP公開/秘密鍵のペアをもって代用する詳細化操作が適用された。割付けは、TTP PPの意図した一般的な性質を反映して、故意に未完成のままとされた。
(735)

同様に、DIGITSIG.4は、DIGITSIG.1-3のサポートにおいて、デジタル署名生成及び検証のために使用されたアルゴリズムを特定するために、FCS_COP.1を使用して特定される：
(736)

DIGITSIG.4^{FCS_COP.1}TSFは[割付：標準のリスト]に合致する、特定された暗号アルゴリズム[割付：暗号アルゴリズム]と暗号鍵長[割付：暗号鍵長]に従って、デジタル署名生成及び認証を実行しなければならない。

他の作業例と同様に、監査が要求される必要なレベル(すなわち、指定なし、最小、基本または詳細)に関して決定される必要がある。指定なしレベルはこれがTTPの運用に重要なこれらのイベントを識別する柔軟性を提供するために選択される。
(737)

上記に言及したように、TTP PPはTTPの補足サービスのセキュアな提供をサポートするために必要とされるSFRを定義する機能パッケージのセットもまた含む。機能パッケージは、次のものに関して明確に定義される：
(738)

- a) 満足されるセキュリティ対策方針；
- b) 中核的なSFRのために要求された付加的なSFR；
- c) 特定されたサービスのサポートのために修正された中核的なSFR。

例えば鍵回復サービス(セキュリティ対策方針O.KEYRECOVERはそれのために識別された)の対策は鍵回復に関する付加的なSFRとなる。鍵回復は暗号鍵アクセスの形式であり、FCS_CKM.3(暗号鍵アクセス)を使用して、特定される：
(739)

CM_KEYREC.1^{FCS_CKM.3}TSFは以下に合致する、特定された暗号鍵アクセス方式[割付：暗号鍵アクセス方式]に従って鍵回復を行わなければならない：

特定された鍵アクセス方式は、秘密鍵構成要素が配付の間の不当な暴露及び改変から保護されることを保証しなければならない。

TTPの補足サービスのために必要とされるSFRのさらなる詳細化の例は、CERTVERIFY.1^{FDP_DAU.2.2}の修正であり、そこでは証明書検証サービスがTTP加入者に提供され

る要求がある： (740)

CERTVERIFY.1^{FDP_DAU.2.2} TSFは、公開鍵証明書及び証明書を生成したTTPの識別情報を検証する能力をTTP及び加入者に提供しなければならない。

詳細化：証明書検証は、最小限として以下を含むべきである：

- a) 署名検証；
- b) 有効性期間をチェックすること；
- c) 取消しをチェックすること。

CERTVERIFY.1^{FDP_DAU.2.2}の(小さい)さらなる詳細化の効果は、TTPと同様にTTP加入者へも証明書を検証する能力を拡張することである。 (741)

F.3.2 保証要件

5章に記述されるように、保証要件は、技術的な実現性によって制約される脅威の性質及び資産の価値を考慮することにより抽出されるべきである。もし保護されている情報の価値が重要であるとすれば、比較的高い保証レベルが必要になると思われる。しかしながら、技術的な実現性の制約は、EAL4の保証要件が適切であることを示唆する。[15408-3]、6.2.4副項、60ページに記述されるように、EAL4は公正な商慣行に基づくセキュリティ工学の観点から、中から高レベルの保証を提供する。さらに、それは、既存の生産ラインを改良するのに経済的に妥当でありうる最も高いレベルとして特徴づけられる。 (742)

F.3.3 IT環境におけるセキュリティ要件

TTPにおいては、セキュリティ要件はIT環境におかれぬ：すべてのセキュリティ要件はTOEによって満足されるべきである。しかしながら、準拠TOEはTOEによって格納及び処理されたTTP資産を保護することを要求されるアクセス制御及び監査機能性、識別及び認証を提供する下層のオペレーティングシステムに基づくことがある。 (743)

F.4 PP根拠

F.4.1 セキュリティ対策方針根拠

脅威に対抗するセキュリティ対策方針の適切性の実証は、7章の中で与えられた以下のガイダンスによって提供されるだろう、すなわち： (744)

- a) どのセキュリティ対策方針がどの脅威に対抗する(例えば、T.ACERTAVAILはO.CERTMANAGEとO.SIGNATUREによって対応される)かを、テーブルによって示すことで、各セキュリティ対策方針が少なくとも1つの脅威の上にマッピングされることを保証する；

- b) それぞれの脅威について、なぜ識別されたセキュリティ対策方針が脅威に
対抗するのに適しているかについての論拠を提供する。

適切性の正当化の例を以下にあげる： (745)

*T.ACERTAVAIL O.CERTMANAGEは、適宜に公開鍵証明書をセキュアに生成
及び配付する手段を提供する。O.SIGNATUREは、証明書生成のサポートでデ
ジタル署名を生成する能力を提供する。*

F.4.2 セキュリティ機能要件根拠

TOEに関するセキュリティ対策方針を満足するSFRの適切性の実証は、以下によって提供される
だろう： (746)

- a) どのSFRがどのセキュリティ対策方針を満足する(例えば、DIGITSIG.1-2
とDIGITSIG.4はセキュリティ対策方針O.SIGNATUREに対応する)かを、
テーブルによって示すことで、各SFRが少なくとも1つのセキュリティ対策
方針にマッピングされることを保証する；
- b) それぞれのTOEの各セキュリティ対策方針について、なぜ識別されたSFR
がセキュリティ対策方針を満足するのに適しているかについての論拠を提
供する。

適切性の正当化の例は以下に与えられる： (747)

*O.SIGNATURE DIGITSIG.1-2及びDIGITSIG.4は、デジタル署名を生成す
るための機能性を提供する。*

各TTPの補足サービスが、そのサービスを提供するために対応するセキュリティ対策方針を持つ
ので、各サービスの根拠は自己完結しており、そしてそれ故にサービスを提供するTOEに関する
PPまたはSTにおける使用において容易に抽出されるだろう。 (748)

相互サポートと内部一貫性の実証は、7章の中のガイダンスに記述された方法で、依存性分析テー
ブルを含めることにより、最初に提供されるだろう。これは依存性分析においてハイライトされ
なかった識別されたSFR(下層のオペレーティングシステムに対する要件の適切なところに含ま
れる)間の付加的なサポートの依存性の識別及び解説により補足されるかもしれない。これは、順
番に各SFRを考慮すること及び他のSFRが、それがバイパスされるまたは改ざんされるのを防ぐ
潜在的な必要性を考慮することにより構成されるべきである。例は以下を含んでいる： (749)

- a) TTP_KEYGEN.1はTTP鍵のセキュアな生成を提供する、そしてそれ故にそ
れらの鍵の使用に依存するSFR：CERTGEN.1、CERTVERIFY.1をサポート
する。
- b) DIGITSIG.1-2&4はデジタル署名機能を提供し、そしてそれ故にデジタル署
名の生成に依存するSFR：CERTGEN.1をサポートする。

- c) DIGITSIG.2-4はデジタル署名検証機能を提供し、そしてそれ故にデジタル署名検証に依存するSFR : CERTVERIFY.1をサポートする。

F.4.3 保証要件根拠

PP根拠のこの部分の構成は、もしPPが(例えば)EAL4を必須とし、追加された保証要件を何も特定しない場合、比較的容易にちがいない。この場合で、EAL4が相互にサポートし、内部的に一貫した保証コンポーネントの既知のセット、それはすべての保証依存性が満たされていることを提供すると主張することは可能だろう。 (750)

EALの選択のための正当化の理由は、F.3.2節に記述されたものに従って提供されるだろう。 (751)