Information-technology
Promotion
Agency, Japan

BSIスマートカードPP比較セミナー
BSI-PP-0035 .vs. BSI-PP-0084

(Version 1.0, 15.06.2007) (Version 1.0, 13.01.2014)

2015年12月21日

独立行政法人　情報処理推進機構
技術本部セキュリティセンター
情報セキュリティ認証室

PPのアップデート（PP0035 → PP0084）の背景

- BlackHat 2010のICチップの物理解析の発表によって、特定のセキュリティチップの脆弱性が公開された。
- ROMの物理解析によって、ROM内の情報が公開されることが現実的な脅威として認識された。
- ROMに機密情報を配置しないことは、設計者に周知され現実的な対策は進められた。

- しかし、PP0035の要件に正確に従えば、ROM内のデータはすべて資産であり、1bitでも曝露されれば、PP準拠が満たされない問題が発生した。

- ROMに配置された情報について、対象を限定して保護する記述に変更した。

全体概要：構成の比較（PP前半）

<PP0035>

<PP0035>	
1	PP Introduction
1.1	PP Reference
1.2	TOE Overview
1.2.1	Introduction
1.2.2	TOE Definition
1.2.3	TOE life cycle
1.2.4	Life-Cycle versus Scope and Organisation of this Protection Profile
1.2.5	Specific Issues of Security IC Hardware and the Common Criteria
2	Conformance Claims
2.1	CC Conformance Claim
2.2	PP Claim
2.3	Package Claim
2.4	PP Application Notes
3	Security Problem Definition
3.1	Description of Assets
3.2	Threats
3.3	Organisational Security Policies
3.4	Assumptions
4	Security Objectives
4.1	Security Objectives for the TOE
4.2	Security Objectives for the Security IC Embedded Software development Environment
4.3	Security Objectives for the operational Environment
4.4	Security Objectives Rationale
5	Extended Components Definition
5.1	Definition of the Family FCS_RNG
5.2	Definition of the Family FMT_LIM
5.3	Definition of the Family FAU_SAS

<PP0084>

<PP0084>	
1	PP Introduction
1.1	PP Reference
1.2	TOE Overview
1.2.1	Introduction
1.2.2	TOE Definition
1.2.3	TOE life cycle
1.2.4	Life-Cycle versus Scope and Organisation of this Protection Profile
1.2.5	Specific Issues of Security IC Hardware and the Common Criteria
2	Conformance Claims
2.1	CC Conformance Claim
2.2	PP Claim
2.3	Package Claim
2.4	PP Application Notes
3	Security Problem Definition
3.1	Description of Assets
3.2	Threats
3.3	Organisational Security Policies
3.4	Assumptions
4	Security Objectives
4.1	Security Objectives for the TOE
4.2	Security Objectives for the Security IC Embedded Software
4.3	Security Objectives for the operational Environmen
4.4	Security Objectives Rationale
5	Extended Components Definition
5.1	Definition of the Family FCS_RNG
5.2	Definition of the Family FMT_LIM
5.3	Definition of the Family FAU_SAS
5.4	Definition of the Family FDP_SDC

PP Introduction ～ Security Objective については構成上の差異は見られない。

Extended Components Definition において、保存データの機密性を保護する拡張機能要件が追記された。

＊保護資産のカバー範囲が限定されたことに加えて、前提条件が1つ削除された等の、内容的な微小な修正は、各章、各節に存在する。

全体概要：構成の比較（PP後半）

<PP0035>

6			IT Security Requirements
	6.1		Security Functional Requirements for the TOE
	6.2		Security Assurance Requirements for the TOE
		6.2.1	Refinements of the TOE Assurance Requirements
	6.3		Security Requirements Rationale
		6.3.1	Rationale for the security functional requirements
		6.3.2	Dependencies of security functional requirements
		6.3.3	Rationale for the Assurance Requirements
		6.3.4	Security Requirements are Internally Consistent
7			Annex
	7.1		Development and Production Process (life-cycle)
		7.1.1	Life-Cycle Description
		7.1.2	Description of Assets of the Integrated Circuits Designer/Manufacturer
	7.2		Security Aspects of the Security IC Embedded Software
		7.2.1	Further Information regarding A.Resp-Appl
		7.2.2	Examples of Specific Functional Requirements for the Security IC Embedded Software
	7.3		Examples of Attack Scenarios
	7.4		Glossary of Vocabulary
	7.5		Literature
	7.6		List of Abbreviations

<PP0084>

6			IT Security Requirements
	6.1		Security Functional Requirements for the TOE
	6.2		Security Assurance Requirements for the TOE
		6.2.1	Refinements of the TOE Assurance Requirements
	6.3		Security Requirements Rationale
		6.3.1	Rationale for the security functional requirements
		6.3.2	Dependencies of security functional requirements
		6.3.3	Rationale for the Assurance Requirements
		6.3.4	Security Requirements are Internally Consistent
7			Annex
	7.1		Development and Production Process (life-cycle)
		7.1.1	Development and Production Process (life-cycle)
		7.1.2	Description of Assets of the Integrated Circuits Designer/Manufacturer
	7.2		Package “Authentication of the Security IC”
		7.2.1	Security Organisational Policy and Security Objective
		7.2.2	Definition of the Family FIA_API
		7.2.3	Security Functional Requirement for Authentication of the TOE
	7.3		Packages for Loader
		7.3.1	Package 1: Loader dedicated for usage in secured environment only
		7.3.2	Package 2: Loader dedicated for usage by authorized users only
	7.4		Packages for Cryptographic Services
		7.4.1	Package “TDES”
		7.4.2	Package “AES”
		7.4.3	Package “Hash functions”
	7.5		Guidance for SFR for RNG (informative only)
		7.5.1	German Scheme
		7.5.2	NIAP
	7.6		Examples of Attack Scenarios
	7.7		Glossary of Vocabulary
	7.8		Literature
	7.9		List of Abbreviations

IT Security Requirements については構成上の差異は見られない。

Annex に構成上の大きな差異が見られる。

＊スマートカードの評価の文脈は、あくまで微小な修正であるが、追加パッケージについては、大きく追記（ローダ、暗号、乱数等）がされた。

比較（TOE Introduction 1/2）

- アップデートの概要
  - 前提条件が1つ削除された。（A.Plat-Appl）
  - 保存データ機密性のSFRの追加。（FDP_SDC.1）
  - 保存データ完全性のモニタリングとアクションのSFRの追加。（FDP_SDI.2）
  - セキュリティICの認証
  - セキュアな環境でのみ使用されるローダ
  - 許可された利用者のみに使用されるローダ
  - TDES
  - AES
  - ハッシュ関数

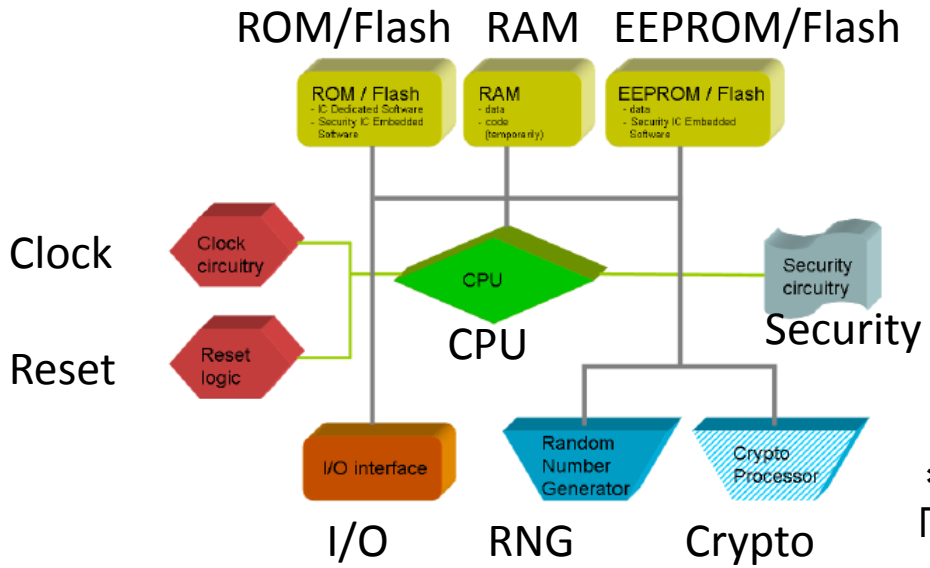
新たな追加パッケージ

比較（TOE Introduction 2/2）

- 基本的に、PP0035→PP0084で抜け落ちたセキュリティ要件は無い
- セキュリティ特性が以下の保護を行うこと
  - 保護されたメモリ領域のデータとROMなど他の領域のデータ（SFRで要求されていなくても）を対象とする。
  - 完全性保護　（＊変更はない。）
  - 機密性保護　（＊対象が以下のように狭められた。）
    セキュリティICメモリの内容　→　保護されたメモリ領域の内容
- セキュリティICに求められること（ユーザデータ保護の観点）
  - PP0035: セキュリティ機能の完全性と、機密性の保護
  - PP0084: TSFとTSFデータの完全性、必要であれば機密性

比較（TOE Definition 1/3）

- 典型的TOEとして例示される下図に変更は無い。
- セキュリティIC 専用SWがEEPROM/Flashに搭載されるケースが言及された。
- 構成データ･初期化データは　範囲が拡大された。
  IC専用SW → セキュリティ機能のふるまいに関係するものすべて
- IC専用SWの記述の一貫性が改善された。
  製造中のテストで使用され、配付後にはセキュリティ機能を提供しない。



典型的TOEの図
*暗号機能はオプション

＊以降は、「セキュリティIC」を「IC」と略称する場合がある。

比較（TOE Definition 2/3）

- IC専用サポートSWがROMに加えて、不揮発性メモリ上に搭載されることがあることが言及された。
- 「TOE」が以下の組み合わせに置き換えられた。
  - セキュリティIC
  - セキュリティIC専用サポートSW（コンポジット評価の場合）
- ICが一般的にパッケージ処理されることが言及された。
- ユーザデータに「コンポジット評価の」と追記された
- TOE製造者について以下のような一般的な想定がされた。
  - TOE製造者はIC組込SWを設計しない。
  - TOE製造者はコンポジットTOEのユーザデータを生成しない。
  - TOE製造者には、これらはユーザデータである。

比較（TOE Definition 1/3）

- 以下の事項を典型的として想定している。
  - IC製造者がTOE製造中に、IC組込SWの全部、あるいは主要な部分をROM, EEPROM, あるいはFlash Memoryにインストールする。
  - コンポジット製品の統合者は、IC組込SWの機能を使って、補足的なインストールを行う。
- コンポジット製品のIC組込SWとユーザデータのインストールは、以下を想定する。
  - 発行まではセキュアな環境でのみ使用されるローダが使用される。
  - 運用では許可された利用者のみに使用されるローダが使用される。
- 発行前データにはTSFデータとユーザデータが含まれるかもしれない。

比較（TOE Life cycle）

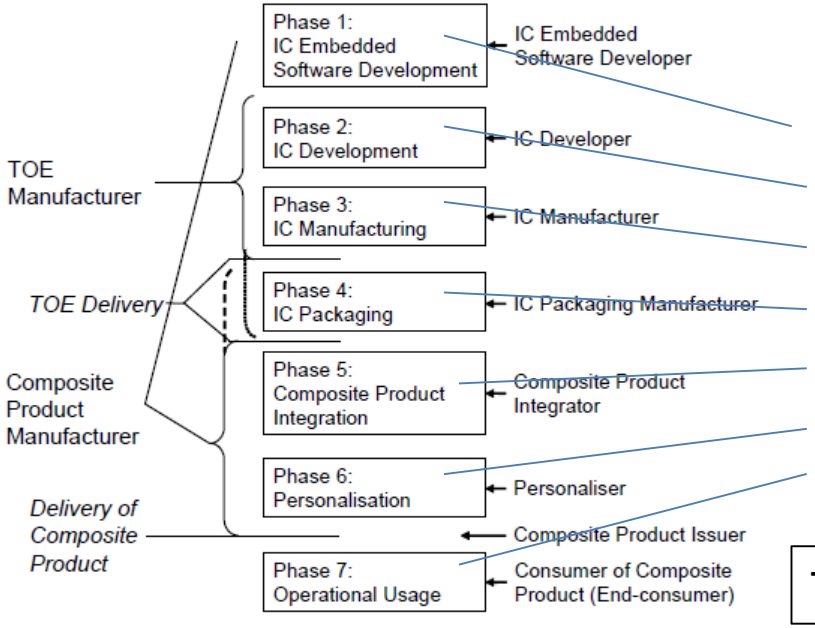
- 「TOE配付の定義と責任」の下図に変更は無い。
- 「開発環境・運用環境の定義」についても変更は無い。
  - 開発環境：フェーズ2, 3
  - 運用環境：フェーズ1, 5, 6, 7
  - 配付：フェーズ4
- 「ICライフサイクルとPP要件」についても変更は無い。

TOE製造者

TOE配付

コンポジット製品製造者

コンポジット製品の配付



フェーズ1: IC組込SW開発
フェーズ2：IC開発
フェーズ3：IC製造
フェーズ4: ICパッケージング
フェーズ5: コンポジット製品統合
フェーズ6: 発行
フェーズ7: 利用

TOE配付の定義および各責任者

比較（Specific Issues of Security IC HW and the CC）

- コンポジットTOEのユーザデータ ＝ IC組込SWの資産。
- ICによる保護について以下のように変更された。
  - PP0035:セキュリティ実施とセキュリティに関連するアーキテクチャコンポーネントの完全性と機密性
  - PP0084: TSFの完全性と少なくともクリティカルなTSFの機密性
- IC組込SWは以下を守ることが記述された。
  - 保護されたメモリ領域のみに機密データを保存する。
  - ICのセキュリティ機能やサービスをセキュアな方法で使用する。
- ICの評価とコンポジット製品の評価の関係は変わらない。
- 「設計の機密性」が「設計の知識」に変更され、脆弱性分析のインプットとなること、そして保護されるべきことが記述された。

比較（Description of Assets 1/2）

- 資産の記述の一部が変更された。
  - ユーザデータ → コンポジットTOEのユーザデータ
  - 搭載され動作しているIC組込SW
  - ICが、IC組込SWに、提供するセキュリティサービス
- 利用者（消費者）が高い関心を持つセキュリティ懸念の記述の一部が以下のように変更された。

ID	PP0035	PP0084
SC1	ユーザデータとIC組込SWの完全性（実行中／処理中、TOEのメモリに保存中）	コンポジットTOEのユーザデータの完全性
SC2	ユーザデータとIC組込SWの機密性（処理中、TOEのメモリに保存中）	TOEの保護されたメモリ領域に保存されるコンポジットTOEのユーザデータの機密性
SC3	TOEが、IC組込SWに提供する、セキュリティサービスの正しい動作	TOEが、IC組込SWに提供する、セキュリティサービスの正しい動作

*PP0084でもIC組込SWがユーザデータであり、実行中／処理中、TOEの保護されたメモリ領域上に保存中は保護されるべきことが記述されている。

*SC: Security Concern

比較（Description of Assets 2/2）

- 乱数に関連しては、以下のように同じ。

ID	PP0035	PP0084
SC4	乱数の欠陥	乱数の欠陥

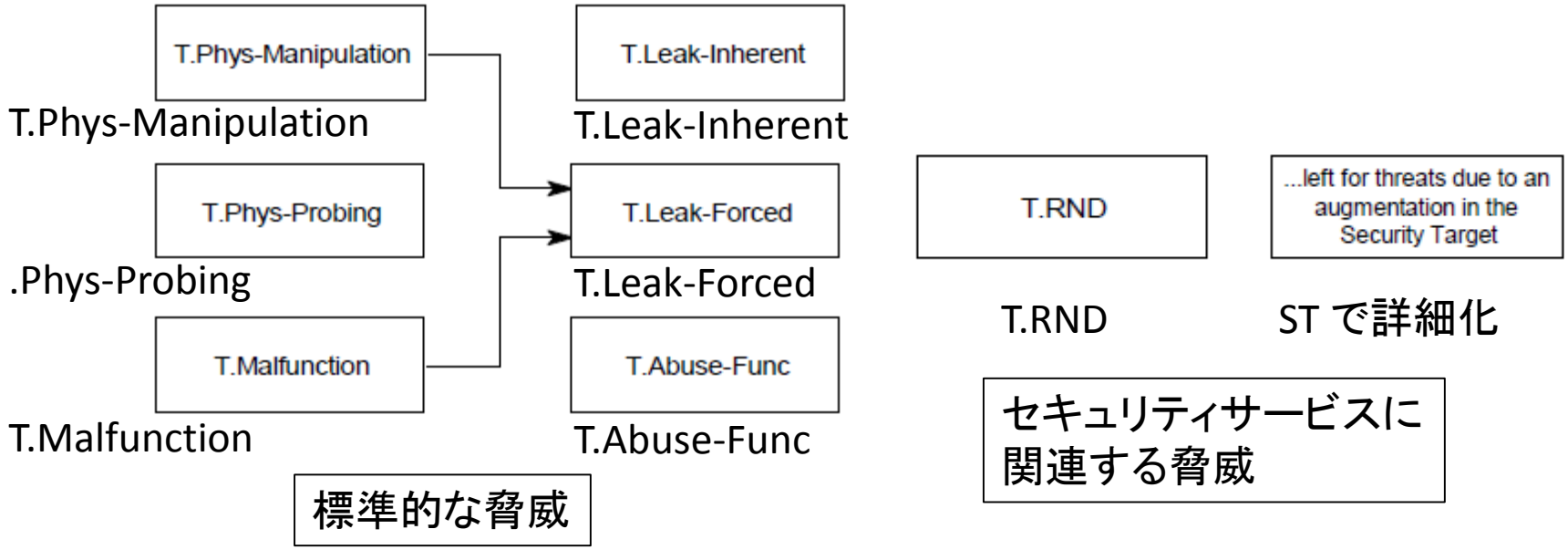
- 資産であるユーザデータを、改変などする方法の記述については、以下の記述の修正、および追加がされた。
  - 「セキュリティ機能」→「TSF」
  - 「ユーザデータ」→「コンポジットTOEのユーザデータ」
  - 開発環境、運用環境でTSFの重要な情報が守られるべき。

論理設計データ、物理設計データ、IC専用SW（初期化データ、発行前データ）、IC製造者が実装する場合には、IC組込SW開発者から提供されるIC組込SW、固有の開発補助、テストおよびキャラクタライゼーションの関連するデータ、ソフトウェア開発サポートのためのマテリアル、フォトマスクとあらゆる形状での製品

- IC組込SWについて、以下の記述が追加された。
  - IC組込SW開発者が提供する。
  - IC製造者が実装する。

比較（Threats 1/5）

- 脅威の記述の変化は、基本的に以下の修正。
  - ユーザデータ → コンポジットTOEのユーザデータ
  - セキュリティ機能 → TSF
- 脅威の全体的な構成は以下のまま変化していない。



比較（Threats 2/5）

- 外界との相互作用については、以下のように同じ。

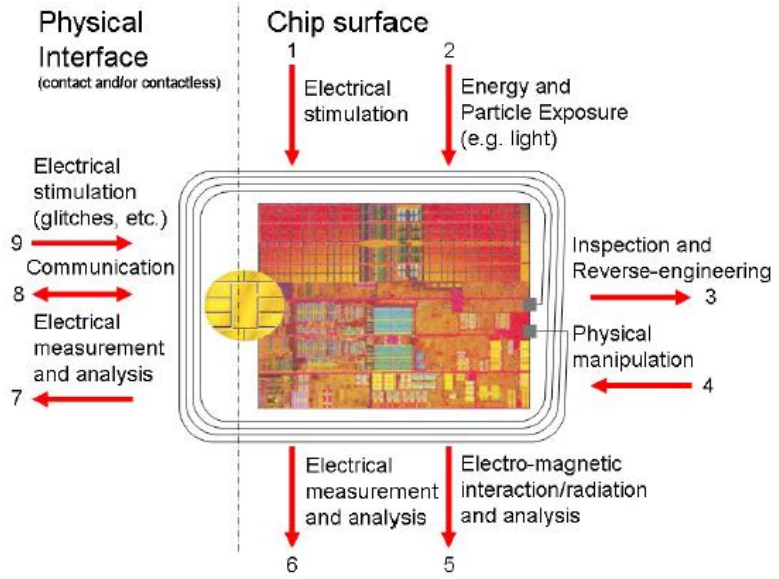
Electrical Stimulation

Energy and particle exposure

Electrical stimulation

Communication

Electrical measurement and analysis



Inspection and Reverse-engineering

Physical manipulation

Electrical measurement and analysis

Electro-magnetic interaction/radiation and analysis

比較（Threats 3/5）

- 前記の文言の修正以外は基本的に同じ。

ID	説明
T.Leak-Inherent	資産の一部である機密情報を曝露するために、セキュリティIC使用中に、TOEから漏洩する情報を悪用する。
T.Phys-Probing	物理的なプロービングによって、(i) 保護メモリ領域保存中のユーザデータの曝露、(ii) 処理中のユーザデータの曝露／再構築、(iii) TOEの動作にクリティカルな他の情報の曝露によりコンポジットTOEやIC組込SWのユーザデータの曝露や操作を可能にする。
T.Malfunction	環境ストレスを加えることにより、TSFまたはIC組込SWの誤動作を引き起こし、(i) TOEのセキュリティサービスを改変、(ii) IC組込SWの機能を改変、(iii) TOEのセキュリティメカニズムを無効化または影響を与えることによって、コンポジットTOEやIC組込SWのユーザデータの曝露や改変を可能にする。

比較（Threats 4/5）

ID	説明
T.Phys-Manipulation	セキュリティICを物理的に改変することにより、(i) コンポジットTOEのユーザデータを改変、(ii) IC組込SWを改変、(iii) TOEのセキュリティサービスを改変または無効化、(iv) TOEのセキュリティメカニズムを改変して、コンポジットTOEまたはIC組込SWのユーザデータを曝露、あるいは改変することを可能にする。
T.Leak-Forced	資産の一部であるコンポジットTOEの機密ユーザデータを曝露するために、セキュリティIC使用中に、TOEから内在的にでは無く、攻撃者によって引き起こされた、漏洩情報を悪用する。
T.Abuse-Func	TOE配付後には使用してはいけない機能を利用して、(i) コンポジットTOEのユーザデータを曝露または操作、(ii) TOEのセキュリティサービスを操作（探査、バイパス、無効化または変更）、(iii) IC組込SWの操作（探査、バイパス、無効化または変更）、(iv) コンポジットTOEまたはIC組込SWのユーザデータの曝露または改変を可能にする。

比較（Threat 5/5 & OSP）

- セキュリティサービスに関連する脅威の記述として変更は無い。
- 暗号アルゴリズムに使用される鍵や変数には、適切なエントロピーが乱数に求められることが、解説として追記された。

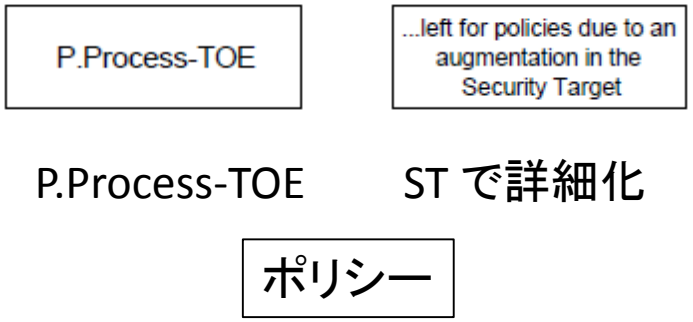
ID	説明
T.RND	例えばエントロピーの欠落によって、TOEのセキュリティサービスから得られる乱数を予測したり、情報を取得したりする。

比較（Organizational Security Policy）

- OSPでは、実質的に誤植の修正のような変更、のみが行われている。

ID	説明
P.Process-TOE	TOEの正確な識別が確立されなければならない。製造された各TOEは固有のIDを持たなければならない。

- STで詳細化を想定していることも同じ。



比較（Assumptions 1/2）

- 前提条件が1つ、削除された。（A.Plat-Appl）
  - ハードウェアプラットフォームの使用法に関する前提条件が削除された。
  - この前提条件では、IC組込SWの設計がガイダンス、認証レポートの要求に合致していることを想定していた。
  - IC組込SWの設計が、セキュリティサービスの使用法を守ることは、STにおいて対応すべきことが記述されている。
  - PPを記述する視点が、コンポジット評価を含めた視点へ変更されたと言える。

ID	PP0035	PP0084
A.Process-Sec-IC	○	○
A.Plat-Appl	○	削除
A.Resp-Appl	○	○

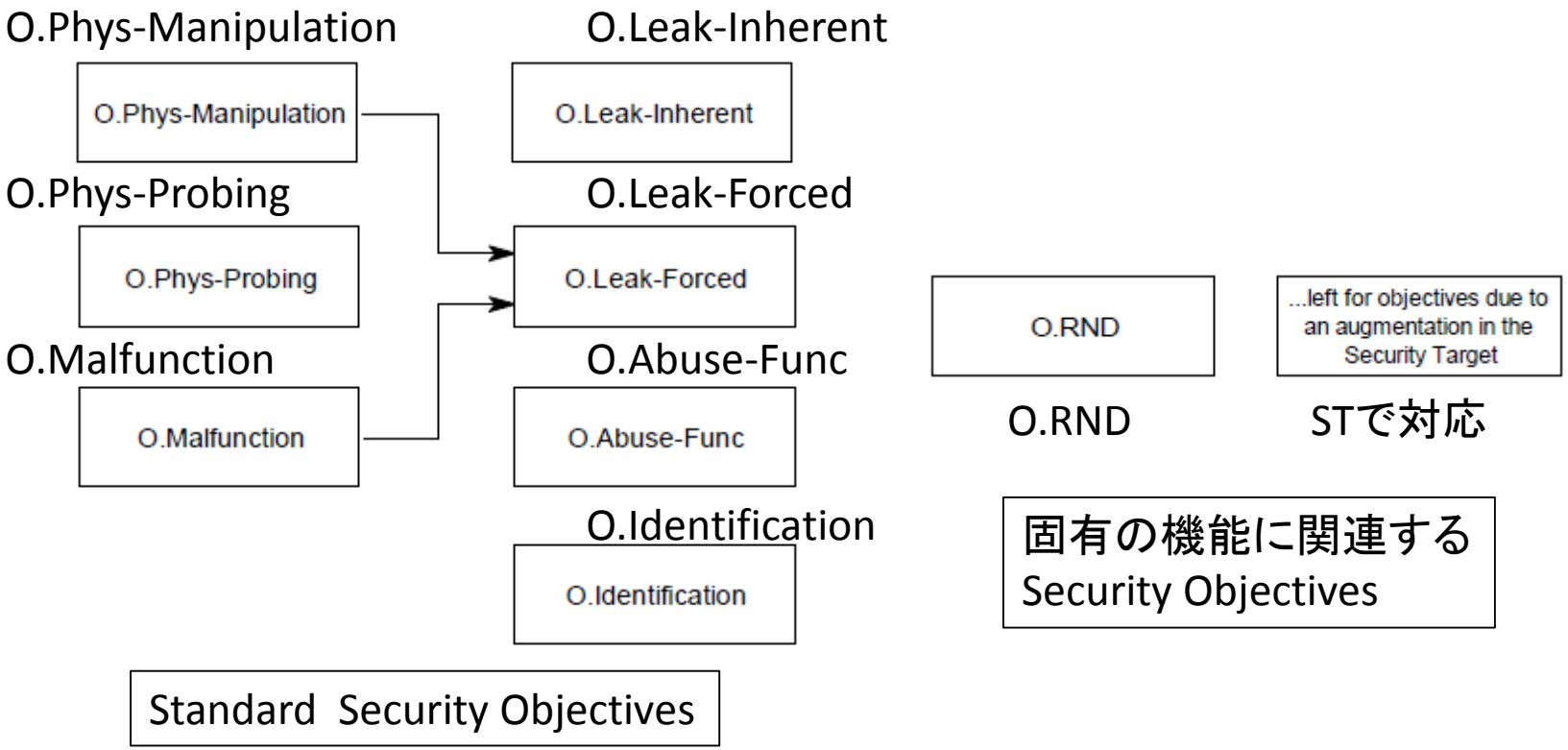
比較（Assumptions 2/2）

- その他の前提条件については、前記の文言の修正以外の変更は無い。

ID	内容
A.Process-Sec-IC	TOE製造者によるTOE配付から、最終利用者への配付まで、セキュリティ手続きが実施され、TOEとその製造、テストデータの完全性、機密性が維持されると想定する。
A.Resp-Appl	コンポジットTOEのすべてのユーザデータは、IC組込SWが所有する。そのため、コンポジットTOEのセキュリティ関連データ（特に暗号鍵）は、IC組込SWの固有のアプリケーションの文脈に従って扱われる。

比較（Security Objectives 1/3）

- TOEのSecurity Objectives: 前記の文言の修正以外は、基本的に同じ



比較（Security Objectives 2/3）

- IC組込SWのSecurity Objectives
  - 前提条件：A.Plat-Applの削除に対応して、OE.Plat-Applが削除された。
  - 残存する前提条件：A.Resp-Applに対応するOE.Resp-Applは、前記の文言の修正以外は同じ。

ID	内容
OE.Resp-Appl	コンポジットTOEのセキュリティ関連データ（特に暗号鍵）は、固有のアプリケーションの文脈の要求に従って、IC組込SWによって扱われなければならない。

比較（Security Objectives 3/3）

- 運用環境のSecurity Objectives
  - 全く変更は無い。OE.Process-Sec-IC

ID	内容
OE.Process-Sec-IC	TOE配付から、最終利用者への配付まで、セキュリティ手続きが実施され、TOEとその製造、テストデータの完全性、機密性が維持されなければならない。

比較（Security Objectives Rationale）

- 前提条件：A.Plat-Applの削除に関連する変更以外は、対応関係に変化は無い。

前提条件etc	対策	備考
~~A.Plat-Appl~~ A.Resp-Appl	~~OE.Plat-Appl~~ OE.Resp-Appl	Phase 1
P.Process-TOE	O.Identification	Phase 2-3, Optional Phase4
A.Process-Sec-IC	OE.Process-Sec-IC	Phase 5-6, Optional Phase 4
T.Leak-Inherent T.Phys-Probing T.Malfunction T.Phys-Manipulation T.Leak-Forced T.Abuse-Func	O.Leak-Inherent O.Phys-Probing O.Malfunction O.Phys-Manipulation O.Leak-Forced O.Abuse-Func	—
T.RND	O.RND	

比較（Extended Component Definition）

- 新たな拡張SFR: FDP_SDCが追加された。
- 従来からある拡張SFRにおいても、修正がされている。

ID	内容	PP0035	PP0084
FCS_RNG	乱数生成	○	○
FMT_LIM	限定されたcapabilities and availability	○	○
FAU_SAS	監査データの保存	○	○
FDP_SDC	保存データの機密性	―	○

比較（FCS_RNG.1）

- 乱数生成のSFR：FCS_RNGの記述が変更されている。

ID	PP0035	PP0084
FCS_RNG.1.1	・[選択：physical, non-physical-true, deterministic] ・[割当：list of security capabilities]	・[選択：physical, non-physical-true, deterministic, hybrid physical, hybrid deterministic] ・[割当：list of security capabilities]
FCS_RNG.1.2	・”random numbers” ・[割当：a defined quality metric]	・[選択：bits, octets of bits, numbers [割当：format of numbers]] ・[割当：a defined quality metric]

比較（FMT_LIM ）

- Limited capabilities and availabilityのSFR: FMT_LIMの記述が変更されている。

ID	PP0035	PP0084
FMT_LIM.1.1 (Limited capabilities)	FMT_LIM.2と共に以下のポリシーを実施する[割当：Limited capability and availability policy]	FMT_LIM.2と協力して以下のポリシーを実施する[割当：Limited capability policy]
FMT_LIM.2.1 (Limited availability)	FMT_LIM.1と共に以下のポリシーを実施する[割当： Limited capability and availability policy}	FMT_LIM.1と共に以下のポリシーを実施する[割当： Limited capability policy}

比較（FAU_SAS & FDP_SDC）

- 監査データ保存のSFR: FAU_SASについては、全く同じである。

ID	PP0035 & PP0084
FAU_SAS.1.1	・The TSF shall provide [割当：list of subjects] with the capability to store [割当：list of audit information] in the [割当：type of persistent memory]

- 新たなSFR: FDP_SDC は保存データの機密性を保護する。

ID	内容
FDP_SDC.1.1	The TSF ensure the confidentiality of the information of the user data while it is stored in the [割当：memory area].

比較（IT Security Requirements 1/2）

- 新たなSFR: FDP_SDCの追加を含む、保存データの保護の追加以外は、実質的に同じ構成。

カテゴリ	PP0035	PP0084
Malfunction	・Limited Fault Tolerance (FRU_FLT.2) ・Failure with preservation of secure state (FPT_FLS.1) ・Domain Separation (ADV_ARC.1)	・Limited Fault Tolerance (FRU_FLT.2) ・Failure with preservation of secure state (FPT_FLS.1)
Leakage	・Basic internal transfer protection (FDP_ITT.1) ・Basic internal TSF data transfer protection (FPT_ITT.1) ・Subset information flow control (FDP_IFC.1)	・Basic internal transfer protection (FDP_ITT.1) ・Basic internal TSF data transfer protection (FPT_ITT.1) ・Subset information flow control (FDP_IFC.1)

*PP0084においても、ADV_ARC.1の評価は含まれる。

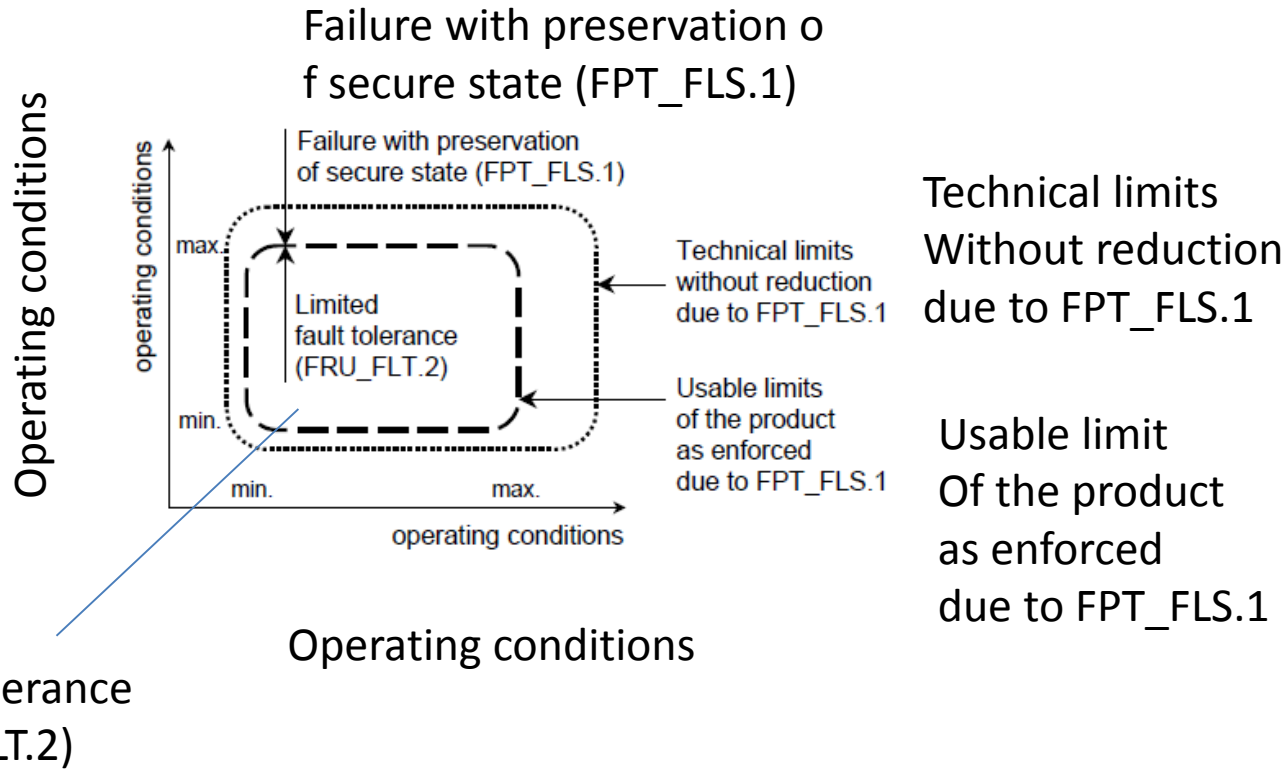
比較（IT Security Requirement 2/2）

- 保存データの保護の追加

カテゴリ	PP0035	PP0084
Physical Manipulation and Probing	・Resistance to Physical Attack (FPT_PHP.3)	・Resistance to Physical Attack (FPT_PHP.3) ・Stored data integrity monitoring and action (FDP_SDI.2) ・Stored data confidentiality (FDP_SDC.1)
Abuse of Functionality	・Limited capabilities (FMT_LIM.1) ・Limited availability (FMT_LIM.2)	・Limited capabilities (FMT_LIM.1) ・Limited availability (FMT_LIM.2)
Identification	・Audit storage (FAU_SAS.1)	・Audit storage (FAU_SAS.1)
Random Numbers	・Random number generation (FCS_RNG.1)	・Random number generation (FCS_RNG.1)

比較（Paradigm regarding Operating Conditions）

- Malfunctionsにおける、動作条件の考えかたは同じ。



- SFR: FRU_FLT.2、FPT_FLS.1の記述に変更は無い。

比較（Abuse of Functionality）

- 前記の文言の修正に対応する変更がされた。

ID	PP0035	PP0084
FMT_LIM.1	TOE配付後には、テスト機能を利用しても ユーザデータ、TSFデータの曝露と操作、他の攻撃を可能にするソフトウェアの再構築、TSF構築の重要な情報の収集を許さない。	TOE配付後には、テスト機能を利用してもコンポジットTOEのユーザデータ、TSFデータの曝露と操作、他の攻撃を可能にするソフトウェアの再構築、TSF構築の重要な情報の収集を許さない。
FMT_LIM.2	同上	同上
FAU_SAS.1.1	TOE配付前に、[割付：不揮発性メモリのタイプ] 内に初期化データ and/or 発行前データ and/or IC組込SWの補足を保存できるテストプロセスを提供する。	TOE配付前に、[割付：不揮発性メモリのタイプ] 内に[選択：初期化データ、発行前データ、[割付：他のデータ]を保存できるテストプロセスを提供する。

比較（Physical Manipulation and Probing）

- 保存データの保護が追加された。

ID	PP0035	PP0084
FDP_SDC.1	―	[割付：メモリ領域] に、保存されている間、ユーザデータの情報の機密性を確実にする。
FDP_SDI.2	―	TSFが管理する領域内に保存されるユーザデータに対して、[割付：ユーザデータ属性]に基づき、すべてのオブジェクトの、[割付：完全性エラー] をモニターする。
FPT_PHP.3	SFRが常に実施されるように自動的に応答することによって、TSFに対する物理的操作と物理的プロービングに抵抗する。	SFRが常に実施されるように自動的に応答することによって、TSFに対する物理的操作と物理的プロービングに抵抗する。

比較（Leakage）

- 基本的にSFRの記述は同じであるが、解説部分では、前記の文言の修正が実施されている。

ID	PP0035	PP0084
FDP_ITT.1	TOEの物理的に分離された部品間でユーザデータが転送される際は、曝露を防止するため、データ処理ポリシーを実施する。	TOEの物理的に分離された部品間でユーザデータが転送される際は、曝露を防止するため、データ処理ポリシーを実施する。
FPT_ITT.1	TOEの分離された部品間でTSFデータが転送される際は、曝露から保護する。	TOEの分離された部品間でTSFデータが転送される際は、曝露から保護する。
FDP_IFC.1	すべての機密データが、TOEまたはIC組込SWによって、処理または転送される際に、データ処理ポリシーが実施される。	すべての機密データが、TOEまたはIC組込SWによって、処理または転送される際に、データ処理ポリシーが実施される。

比較（Random Numbers）

- RNGについては、以下の変更がされた。

ID	PP0035	PP0084
FCS_RNG.1.1	乱数源のTotal Failure Test、[割付：追加のsecurity capabilityのリスト] を実装する物理的 乱数生成器を提供する。	[割付：security capabilityのリスト] を実装する[選択：物理的、ハイブリッド物理的、ハイブリッド決定論的] 乱数生成器を提供する。
FCS_RNG.1.2	[選択：independent bits with Shannon entropy of 7.976 bits per octet, Min-entropy of 7.95 bit per octet, [割付：other comparable 品質メトリック] に適合する乱数を提供する。	[割付：定義された品質メトリック] に適合する [選択：bits, octets of bits, numbers [割付：format of the numbers]] を提供する。

比較（Security Assurance Requirements for the TOE）

- 保証コンポーネントの識別は全く同じ。

EAL4
ALC_DVS.2
AVA_VAN.5

ADV_ARC.1	AGD_OPE.1	ALC_DEL.1	ATE_COV.2	AVA_VAN.5
ADV_FSP.4	AGD_PRE.1	ALC_DVS.2	ATE_DPT.2	ASE_CCL.1
ADV_IMP.1	ALC_CMC.4	ALC_LCD.1	ATE_FUN.1	～
ADV_TDS.3	ALC_CMS.4	ALC_TAT.1	ATE_IND.2	ASE_TSS.1

- パラグラフ182が追加され、サポートドキュンメントに従うべきことが記述された。

スマートカードおよび類似のデバイスについては、CCDB、JIWG、そして認証機関が、サポート文書、ガイダンス文書を発行し、CCRA、SOG-IS、あるいはスキーム下で適用が必須である。

比較（Refinements 1/2）

- 前記の文言の修正やMSSRの参照などがされた。

component	PP0035	PP0084
ALC_DEL	対象は、初期化データ and/or 発行前データ and/or IC組込SWの補足	対象は、初期化データ and/or 発行前データ and/or 指定された他のデータ
ALC_DVS	—	JILWG が “Joint Interpretation Library: Minimum Site Security Requirements (For trial use), 2013” [12] を発行した。
ALC_DVS	—	攻撃を可能にする・サポートする、restricted, sensitive, critical or very critical informationを保護する。
ALC_DVS	完全性と機密性	完全性、必要な場合は機密性

比較（Refinement 2/2）

- 保存されるデータ保護なども追記がされた。

component	PP0035	PP0084
ALC_CMS	IC組込SWは、…	IC組込SWはユーザデータとして…
ADV_ARC	—	“Supporting Document Guidance Security Architecture requirements (ADV_ARC) for smart cards and similar devices” 参照
AVA_VAN	—	ROMの格納データの保護についてFDP_SDC.1に関連づけて追記された。
AVA_VAN	—	サイドチャネル攻撃に対してFDP_SDC.1が追加された。

比較（Annex）

- 追加パッケージについて多くの追加がされている。

<PP0035>

7			Annex
	7.1		Development and Production Process (life-cycle)
		7.1.1	Life-Cycle Description
		7.1.2	Description of Assets of the Integrated Circuits Designer/Manufacturer
	7.2		Security Aspects of the Security IC Embedded Software
		7.2.1	Further Information regarding A.Resp-Appl
		7.2.2	Examples of Specific Functional Requirements for the Security IC Embedded Software
	7.3		Examples of Attack Scenarios
	7.4		Glossary of Vocabulary
	7.5		Literature
	7.6		List of Abbreviations

<PP0084>

7			Annex
	7.1		Development and Production Process (life-cycle)
		7.1.1	Development and Production Process (life-cycle)
		7.1.2	Description of Assets of the Integrated Circuits Designer/Manufacturer
	7.2		Package “Authentication of the Security IC”
		7.2.1	Security Organisational Policy and Security Objective
		7.2.2	Definition of the Family FIA_API
		7.2.3	Security Functional Requirement for Authentication of the TOE
	7.3		Packages for Loader
		7.3.1	Package 1: Loader dedicated for usage in secured environment only
		7.3.2	Package 2: Loader dedicated for usage by authorized users only
	7.4		Packages for Cryptographic Services
		7.4.1	Package “TDES”
		7.4.2	Package “AES”
		7.4.3	Package “Hash functions”
	7.5		Guidance for SFR for RNG (informative only)
		7.5.1	German Scheme
		7.5.2	NIAP
	7.6		Examples of Attack Scenarios
	7.7		Glossary of Vocabulary
	7.8		Literature
	7.9		List of Abbreviations

開発や製造プロセスについては変更は無い。

直接的な比較が難しい程度の変化、および追加があった。

用語の定義、参考文献はアップデートされた。

セキュリティICの認証、ローダ、暗号サービス、そしてRNGについてパッケージが追加された。

PP0084のAnnex（Package 1/4）

- Package “セキュリティICの認証”

項目	説明
目的	セキュリティICチップの内部認証により、ICチップのなりすましを防ぐ。
脅威	攻撃者が、なりすましのICチップを作成する。
対策	・TOEは初期化データを利用して、自身を外部に対して認証する。 ・運用環境は、TOEの認証関連データと検証メカニズムをサポートする。
SFR	FIA_API: TSFは外部エンティティに対して、TOEのIDを証明する認証メカニズムを提供する。

*PP0035では、内部認証の機能については、言及されていない。

PP0084のAnnex（Package 2/4）

- Package “ローダ1”

項目	説明
目的	TOE配付後に、EEPROMまたはFlashにデータをロードするために使用。
分類	・ローダ1：安全な環境で使用される。
OSP1	コンポジット製造者が、IC組込SW、コンポジット製品やIC製造者が管理するIC専用サポートSWのデータをロードする際に、ロード機能を制限する。
対策	・TOEは、制限された能力のロード機能と、回復できないロード機能の停止を提供する。 ・コンポジット製品製造者は、ローダ機能を誤使用から保護し、ロード機能の制限を守り、意図する使用の後は回復できないロード機能の停止を行う。
SFR	・FMT_LIM.1: FMT_LIM.2と共に機能を制限する。[割付：アクション]後は、非許可ユーザに保存データの曝露や操作を許さない。 ・FMT_LIM.2: FMT_LIM.1と共に、[割付：アクション]後は、ローダ機能の動作を防ぐ。

PP0084のAnnex（Package 3/4）

- Package “ローダ2”

項目	説明
目的	TOE配付後に、EEPROMまたはFlashにデータをロードするために使用。
分類	・ローダ2 :データのロードや改変について、異なるセキュリティポリシーと認証を求める場合に使用される。
OSP1	許可されたユーザが、ローダ機能を制御して、保存されロードされたデータを曝露や操作から保護する。
対策	・TOEは、許可されたユーザとの間に高信頼性通信チャネルを提供し、ロードされるユーザデータの認証と機密性を保護し、ローダ機能へのアクセス制御を行う。 ・許可されたユーザは、TOEとの高信頼性チャネル通信をロードされるデータの機密性保護と真正性証明によってサポートし、ローダに必要なアクセス条件を満たさなければならない。
SFR	・FTP_ITC.1: 許可されたユーザとの間に高信頼性チャネルを提供する。 ・FDP_UTC.1: 権限外の曝露から保護されたデータ受信。 ・FDP_UIT.1: 改変、消去、挿入から保護されたデータ受信。 ・FDP_ACF.1: ローダ機能へのアクセス制御

PP0084のAnnex（Package 4/4）

- Package “暗号サービス”
  - TDES
  - AES
  - ハッシュ関数
- Package “RNG”
  - German スキーム
  - NIAPスキーム

＊STでの記述を補助するための、補助的な情報