GLOBALPLATFORM

THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY

GlobalPlatform デバイス委員会

TEE プロテクションプロファイル

バージョン 1.2.1

公開

2016 年 11 月

文書識別子:GPD_SPE_021

平成 29 年 9 月 26 日　翻訳　第 1.0 版
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

本頁は意図的に白紙にしてある。

目次

図

表

1 概説

タイトル:	TEE プロテクションプロファイル（ベース PP 及びオプションの TEE Time and Rollback PP モジュール及び TEE Debug PP モジュール）
識別:	GPD_SPE_021（ベース PP のみで構成される PP コンフィギュレーション） GPD_SPE_021+Time（ベース PP 及び TEE Time and Rollback PP モジュールで構成される PP コンフィギュレーション） GPD_SPE_021+Debug（ベース PP 及び TEE Debug PP モジュールで構成される PP コンフィギュレーション） GPD_SPE_021+Time&Debug（ベース PP 及び TEE Time and Rollback PP モジュール及び TEE Debug PP モジュールで構成される PP コンフィギュレーション）
編集者:	Trusted Labs
発行日:	2016 年 11 月
バージョン:	1.2.1
スポンサー:	GlobalPlatform
CC バージョン:	3.1 改訂第 4 版

本プロテクションプロファイル（PP）は、GlobalPlatform デバイス委員会のセキュリティワーキンググループによって作成された。本 WG は、コンテンツ保護、著作権管理、企業方針、決済等のモバイルセキュリティサービスを利用可能とすることを目指す、GlobalPlatform の高信頼実行環境 (TEE) のコモンクライテリア (CC) 評価に関する参照文書として策定する。

本 PP が対象とする TEE は、GlobalPlatform の TEE 内部 API 仕様[IAPI]で定義されるコア機能を実装する。本 PP は、最小限の TEE セキュリティ要件を規定する「ベース PP」、及び完全なロールバック保護と永続的なモノトニックな時間 (訳注:ダウングレードできないこと) を実装するような TEE 及びデバッグ機能へのアクセスを許可するような TEE に適用されるオプションの「PP モジュール」を定義するため、コモンクライテリアのモジュラープロテクションプロファイル手法[PP-MOD]に依拠する。これらの「PP モジュール」は、「PP コンフィギュレーション」を構成するため、「ベース PP」と共に利用可能である。本文書は、上記の 2 つの「PP モジュール」との「ベース PP」のすべての組み合わせをサポートする。

本プロテクションプロファイルは、AVA_TEE.2 と呼ばれる拡張セキュリティ保証要件（SAR）を追加した EAL 2 パッケージへの適合を主張する。本拡張 SAR は、攻撃能力を、[CC パート 3]及び[CEM]の AVA_VAN.2 として定義される標準基本攻撃能力を超えた攻撃能力に強化することを目的とする。評価手法は、具体的な攻撃能力の評価表及び TEE 攻撃の代表的セットを含み、附属書 A で定義される。本拡張 SAR は、製品評価を監督する認証機関によって承認された場合にのみ利用可能であり、それ以外の場合、適合主張は EAL 2 に制限される。

1.1 読者

本文書は、TEE 開発者、インテグレータ（特にハンドセット製造者）、サービスプロバイダ（TA 開発者）、ITSEF、認証機関、CC 認定消費者など、TEE バリューチェーンのすべての関係者を対象とする。

1.2 IPR 免責事項

GlobalPlatform は、本仕様への準拠が本仕様と関連する特許またはその他の知的財産権（総称して『IPR』と言う）の使用を伴う可能性があるという主張が、https://www.globalplatform.org/specificationsipdisclaimers.asp に掲載される場合があるという事実に注目する。GlobalPlatform は、これら IPR 主張の証拠、有効性及び範囲に関していかなる立場も取らない。

1.3 参考文献

標準／仕様	説明	参照
CC パート 1	情報技術セキュリティ評価のためのコモンクライテリア、パート 1：概説と一般モデル. バージョン 3.1、改訂第 4 版、2012 年 9 月. CCMB-2012-09-001.	[CC1]
CC パート 2	情報技術セキュリティ評価のためのコモンクライテリア、パート 2：セキュリティ機能コンポーネント. バージョン 3.1、改訂第 4 版、2012 年 9 月. CCMB-2012-09-002.	[CC2]
CC パート 3	情報技術セキュリティ評価のためのコモンクライテリア、パート 3：セキュリティ保証コンポーネント. バージョン 3.1、改訂第 4 版、2012 年 9 月. CCMB-2012-09-003.	[CC3]
CEM	情報技術セキュリティ評価のための共通方法、評価方法. バージョン 3.1、改訂第 4 版、2012 年 9 月. CCMB-2012-09-004.	[CEM]
CEM 追補	CC 及び CEM 追補、モジュラーPP、バージョン 1.0、2014 年 3 月. CCDB-2014-03-001	[PP-MOD]
CC サポート文書	Application of Attack Potential to Smartcards. Version 2.9 January 2013. Joint Interpretation Library.	[APSC]
OMTP ATE TR1	Open Mobile Terminal Platform Advanced Trusted Environment OMTP TR1 v1.1	[OMTP-TR1]
OMTP セキュリティの脅威	OMTP Security Threats on Embedded Consumer Devices v1.1	[OMTP-ST]
TEE ホワイトペーパー	The Trusted Execution Environment: Delivering Enhanced Security at a Lower Cost to the Mobile Market, GlobalPlatform White paper, Feb 2011	[WP]
GPD_SPE_009	TEE System Architecture, GlobalPlatform (Last applicable version)	[SA]
GDP_SPE_010	TEE Internal API Specification, GlobalPlatform (Last applicable version)	[IAPI]

標準／仕様	説明	参照
GDP_SPE_007	TEE Client API Specification, GlobalPlatform (Last applicable version)	[CAPI]
FIPS Publication	ADVANCED ENCRYPTION STANDARD（AES）、FIPS PUB 197、2011 年 11 月。	[AES]
FIPS Publication	DATA ENCRYPTION STANDARD（DES）、FIPS PUB 46-3、1999 年 10 月	[DES]
RSA Laboratories Publication	RSA Cryptographic Standard. PCKS#1 v2.2. October 2012	[RSA]
FIPS Publication	SECURE HUSH STANDARD、FIPS PUB 180-4、2012 年 3 月	[SHA]
IEEE Standard	IEEE 1149.1-2001Standard Test Access Port and Boundary-Scan Architecture http://standards.ieee.org/reading/ieee/std_public/description/testtech/1149.1-2001_desc.html	[JTAG]
RFC2119	Key words for use in RFCs to Indicate Requirement Levels	[RFC2119]

表 1：規定の参照

1.4 用語と定義

本文書全体を通し、規定の要件は以下に記述されるとおり大文字のキーワードを用いて強調される。

本文書におけるキーワード「しなければならない(MUST)」、「してはならない(MUST NOT)」、「要求される(REQUIRED)」、「しなければならない(SHALL)」、「してはならない(SHALL NOT)」、「推奨される(RECOMMENDED)」、「してもよい(MAY)」、及び「オプションである(OPTIONAL)」は、[RFC2119]で記述されたとおりに解釈されるべきものである:

・しなければならない(MUST)ーこの用語、又は用語「要求される(REQUIRED)」又は「しなければならない(SHALL)」は、その定義が当該仕様の絶対的な要件であることを意味する。

・してはならない(MUST NOT)ーこの用語、又は用語「してはならない(SHALL NOT)」は、その定義が当該仕様の絶対的な禁止事項であることを意味する。

・するべきである(SHOULD)ーこの用語、又は形容詞「推奨される(RECOMMENDED)」は、特定の項目を無視するためには、特定の状況における正当な理由が存在するかもしれないことを意味するが、異なる選択をする前に、当該項目の示唆するところを十分に理解し、慎重に重要性を判断しなければならないことを意味する。

・するべきではない(SHOULD NOT)ーこの用語、又は用語「推奨されない(NOT RECOMENDED)」は、特定のふるまいが受け入れ可能又は有用でさえあるとき、特定の状況において、正当な理由が存在するかもしれないことを意味するが、表示のあるふるまいを実装する前に、当該項目の示唆するところを十分に理解し、慎重に重要性を判断しなければならないことを意味する。

してもよい(MAY)ーこの用語、又は形容詞「オプションの(OPTIONAL)」は、ある項目が本当にオプションであることを意味する。特定の市場がそれを要求したり、又は、別のベンダは同じ項目を省略するかもしれないがそのベンダは製品を拡張すると思っていたりするので、あるベンダはその項目を含めるよう選択するかもしれない。特定のオプションを含めないような実装は、そのオプションを含むがおそらく削減された機能を用いた別の実装と相互運用するために準備されなければならない(MUST)。同じようなやり方で特定のオプションを含むような実装は、そのオプションを含まないような別の実装と相互運用するために準備されなければならない(MUST)(もちろん、将来そのオプションが提供する機能を除く。)

表 1 は、表現のそれぞれの語で大文字の最初の文字を利用するようなこのプロテクションプロファイルの中で利用される表現を定義する。それぞれの用語の小文字の最初の文字を利用するような本文書内の表現は、常識的な意味でとらえる。[CC1] §4 で定義される CC 専門用語は、表 1 に列挙されない。

用語	定義
アプリケーションプログラミングインタフェース Application Programming Interface（API）	複数のソフトウェアプログラムが相互通信するために従うことのできる規則セット。
クライアントアプリケーション Client Application（CA）	高信頼実行環境（TEE）外で動作し、TEE 内のトラステッドアプリケーション（Trusted Application）によって提供される機能にアクセスする TEE クライアント API を利用するアプリケーション。 対照 *トラステッドアプリケーション*
一貫性 Consistency	ランタイム及び起動時の一貫性を同時に保つ TEE の永続的ストレージの 1 つの特性。 ランタイムの一貫性は、以下の条件が保証されることを意味する： ・読み出し/読み出し：ストレージの同一ロケーションの 2 回の正常な読み出しが同一値を取る。ただし、TEE がそのロケーションへの書き込みや、合間のリセットを実行しなかった場合に限る。 ・書込み／読出し：ストレージの所与のロケーションの正常な読み出しが、そのロケーションへの TEE の最後の書き込み値を取る。ただし、TEE が合間のリセットを実行しなかった場合に限る。 起動時の一貫性は、以下の条件が保証されることを意味する： ・所与のパワーサイクルで起動時に使用される保存データが、前回のパワーサイクルで同じ TEE によってランタイム一貫性が実行されたようなデータである。 一貫性は、正常に書き込まれ読み出されるもの（値またはコード）の、ランタイムの完全性を意味する。しかし、起動時に使用される保存データは、最新データではなく、昔のパワーサイクルからの修復データである可能性がある。所与の時刻のメモリスナップショットに該当するため、起動時の一貫性は保たれるが、最新のパワーサイクルと比較すると完全性の損失が示される。 この概念は、パワーサイクル間で保持されなければならない完全性よりも弱い。
デバイス結合 Device binding	デバイス結合は、ある特定の一意のシステムインスタンス（ここでは TEE）においてのみ使用できるデータの 1 つの特性。
実行環境 Execution Environment（EE）	アプリケーションのサポートに必要な機能（コンピューティング、メモリ管理、インプット/アウトプット等）を提供する、ハードウェア及びソフトウェアコンポーネントのセット。
モノトニシティ Monotonicity	モノトニシティ(単調性) は、値が時間と共に必ず増加もしくは減少する変数の特性。
パワーサイクル Power cycle	パワーサイクルは、デバイスの電源が入る瞬間から、その後デバイスの電源が切れる瞬間までの時間の経過。
プロダクション TEE Production TEE	ライフサイクルの最終利用者フェーズにあるデバイスに属する TEE。
REE コミュニケーションエージェント REE Communication Agent	REE と TEE の通信を可能にする REE Rich OS ドライバ。 対照 *TEE コミュニケーションエージェント*
リッチ実行環境 Rich Execution Environment（REE）	場合によっては他のサポーティング OS やハイパーバイザと共に、Rich OS によって提供及び制御される環境。TEE には入らない。この環境及びここで動作するアプリケーションは信頼できない（高信頼ではない）とみなされる。

用語	定義
	対照 *高信頼実行環境*
リッチ OS Rich OS	一般に、TEE 内で動作する OS よりもはるかに多様な機能を提供する OS。アプリケーションを受け入れる機能が非常にオープンである可能性がある。セキュリティよりも、キーゴールとしての機能及び性能を目指して開発される。その規模とニーズを理由に、リッチ OS は TEE ハードウェアよりも規模が大きく(リッチ実行環境:REE と呼ばれることが多い)物理的セキュリティ境界が非常に低い実行環境で動作する。Rich OS の観点から内部の信頼構造が確立されていたとしても、TEE の観点からは、REE のものはすべて信頼できない(高信頼ではない)とみなされなければならない。 対照 *トラステッド OS*
信頼の基点 Root of Trust(RoT)	一般に、ハードウェア、ファームウェア、及び/またはソフトウェアの、本質的に高信頼でなければならない区別可能な最小セットである。高信頼アクションを実行するベースとなるロジック及び環境と密接に関連する。
システムオンチップ System-on-Chip(SoC)	集積された一つの回路に、すべてのコンポーネントが組み込まれているエレクトリックシステム。
TA インスタンス時間／ TA 持続時間 TA instance time / TA persistent time	TEE 内部 API を介してトラステッドアプリケーションが利用できる時間値。API は 2 種類の時間値を提供する:ランタイムのみに存在するシステム時間と、リセットを超えて持続する持続時間である。システム時間は、所与の TA インスタンスに対してモノトニックでなければならず、戻り値は「TA インスタンス時間」と呼ばれる。持続時間は特定のインスタンスではなく、TA にのみ依存し、パワーサイクルを越えてもモノトニックでなければならない。複数のパワーサイクルを越えたモノトニシティは、オプションの Time and Rollback PP モジュールに関連する。
TEE クライアント API TEEClient API	TEE 及び TEE によって実行されるトラステッドアプリケーションと通信するために、REE で実行中のクライアントによって利用されるソフトウェアインタフェース。
TEE コミュニケーションエージェント TEE Communication Agent	REE と TEE の間の通信を可能にする TEE トラステッド OS ドライバ。 対照 *REE コミュニケーションエージェント*
TEE 内部 API TEEInternalAPI	TEE の機能をトラステッドアプリケーションにさらすソフトウェアインタフェース。
TEE サービスライブラリ TEE Service Library	セキュリティ関連のドライバをすべて含むソフトウェアライブラリ。
トラステッドアプリケーション Trusted Application(TA)	TEE 内で動作するアプリケーション。セキュリティ関連の機能を TEE 外のクライアントアプリケーションにエクスポートする。 対照 *クライアントアプリケーション*
高信頼実行環境 Trusted Execution Environment(TEE)	REE と共存するが、分離して動作する実行環境。TEE はセキュリティ機能を含み、特定のセキュリティ関連の要件を満たす。それは、TEE 資産を一般的ソフトウェア攻撃から保護し、プログラムがアクセスできるデータや機能について厳格な安全対策を定義し、定義された一連の脅威に抵抗する。TEE の実装に使用できるテクノロジーは複数存在し、それに応じて、実現できるセキュリティレベルが異なる。詳細は OMTP ATE TR1[OMTP-TR1]参照。 対照 *リッチ実行環境*
トラステッド OS Trusted OS	TEE で動作するオペレーティングシステム。主として TEE がセキュリティベースの設計技術を用いることを可能にするために設計された。トラス

用語	定義
	テッドアプリケーションに対する GlobalPlatform TEE 内部 API、及び他の EE から GlobalPlatform TEE クライアント API ソフトウェアインタフェースを実行可能にする独自手法を提供する。 対照 *リッチ OS*
高信頼ストレージ Trusted Storage	GlobalPlatform TEE 文書で、*高信頼ストレージ*は、少なくともOMTP のセキュアなストレージ（[OMTP-TR1]のセクション5で）に対して定義された耐性レベルで保護されるストレージを意味する。高信頼ストレージは、TEE のハードウェアによって、または TEE 内で保持される暗号鍵によって保護される。鍵は、使用される場合には、少なくともTEE の実証に使用できる程度の強度を備える。GlobalPlatform TEE 高信頼ストレージは、セキュアなエレメントが実現できるレベルに対し、耐タンパ性を備えるハードウェアとはみなされない。

表 2: 用語と定義

1.5 略語と表記法

表 3 は本 PP で使用する略語について定める。

略語	意味
AES	Advanced Encryption Standard（[AES]で定義） （高度暗号化規格）
API	Application Programming Interface （アプリケーションプログラミングインタフェース）
CA	Client Application （クライアントアプリケーション）
CC	Common Criteria（[CC1]、[CC2]、[CC3]で定義） （コモンクライテリア）
CEM	Common Evaluation Methodology（[CEM]で定義） （共通評価方法）
CM	Configuration Management（[CC1 で定義]） （構成管理）
DES	Data Encryption Standard （データ暗号化規格）
DRM	Digital Rights Management （デジタル著作権管理）
EAL	Evaluation Assurance Level（[CC1 で定義]） 評価保証レベル
EE	Execution Environment （実行環境）
ID	IDentifier （識別子）
FIFO	First In、First Out （先入れ先出し）
HD	High Definition （高精細）
HDMI	High-Definition Multimedia Interface

略語	意味
	（高精細度マルチメディアインタフェース）
IPsec	Internet Protocol security （インターネットプロトコルセキュリティ）
JTAG	Joint Test Action Group（[JTAG]で定義） （ジョイントテストアクショングループ）
MAC	Message Authentication Code メッセージ認証コード
NA	Not Applicable （該当なし）
NFC	Near Field Communication （近距離無線通信）
OMTP	Open Mobile Terminal Platform （オープンモバイルターミナルプラットフォーム）
OS	Operating System （オペレーティングシステム）
OSP	Organisational Security Policy（[CC1]で定義） （組織のセキュリティ方針）
OTP	One-Time Password （ワンタイムパスワード）
PCB	Printed Circuit Board （プリント基板）
PP	Protection Profile（[CC1]で定義） プロテクションプロファイル
RAM	Random Access Memory （ランダムアクセスメモリ）
REE	Rich Execution Environment （リッチ実行環境）
RFC	Request for Comments；IETF によって発行される覚書を意味することがある （コメント募集）
ROM	Read Only Memory （読み出し専用メモリ）
RSA	Rivest/Shamir/Adleman asymmetric algorithm（[RSA]で定義） （Rivest/Shamir/Adleman 非対称アルゴリズム）
SAR	Security Assurance Requirement（[CC1]で定義） セキュリティ保証要件
SFP	Security Function Policy（[CC1]で定義） セキュリティ機能方針
SFR	Security Functional Requirement（[CC1]で定義） セキュリティ機能要件
SHA	Secure Hash Algorithm（[SHA]で定義） セキュアハッシュアルゴリズム
SoC	System-on-Chip （システムオンチップ）
SPD	Security Problem Definition（[CC1]で定義） （セキュリティ課題定義）

略語	意味
SSL	Secure Sockets Layer （セキュアソケットレイヤ）
ST	Security Target（[CC1]で定義） セキュリティターゲット
TA	Trusted Application （トラステッドアプリケーション）
TEE	Trusted Execution Environment （高信頼実行環境）
TLS	Transport Layer Security （トランスポート層セキュリティ）
TOE	Target of Evaluation（[CC1]で定義） （評価対象）
TSF	TOE Security Functionality（[CC1]で定義） TOE セキュリティ機能
TSFI	TSF Interface（[CC1]で定義） TSF インタフェース
USB	Universal Serial Bus （ユニバーサルシリアルバス）
VPN	Virtual Private Network （仮想プライベートネットワーク）

表 3: 略語と表記法

1.6 改訂履歴

改訂日	バージョン	著者	説明
2013 年 8 月 9 日	0.5.3 / 1.0	C. Lavatelli, Trusted Labs	公開レビュー後に更新
2014 年 9 月 29 日	1.1	G. Dufay, Trusted Labs	PP 評価中に更新
2014 年 11 月 18 日	1.2	G. Dufay, Trusted Labs	誤植とわずかな説明
2016 年 11 月 25 日	1.2.1	C. Lvatelli, GlobalPlatform SES	附属書Ａの更新（攻撃能力の見積表と例）

2 TOE 概要

本チャプターでは、評価対象 (TOE) の種別を定義し、典型的な TOE アーキテクチャを提示し、TOE の主なセキュリティ機能と意図される用途について、TOE のライフサイクルとともに記述する。

2.1 TOE 種別

TOE 種別は、GlobalPlatform TEE 仕様 (TEE System Architecture[SA]、TEE 内部 API[IAPI]及び TEE クライアント API[CAPI] を参照) を実装している組込みデバイスの高信頼実行環境 (TEE) である。しかし、本プロテクションプロファイルは、GlobalPlatform TEE API 仕様との完全な機能上の適合性を要求しない。

TOE は、通常のリッチ実行環境 (REE) を含む、その他の実行環境、及びそれらのアプリケーションから隔離された実行環境である。TOE は、トラステッドアプリケーション (TA) のセットのホストを務め、それらに以下のセキュリティサービスの包括的なセットを提供する：実行の完全性、REE で動作しているクライアントアプリケーション（CA）とのセキュアな通信、高信頼ストレージ、鍵管理と暗号アルゴリズム、時間管理と算術的な API。

TOE は以下を包含する：

- TEE セキュリティ機能を提供するために利用されるハードウェア、ファームウェア及びソフトウェア
- 配付後の TEE のセキュアな用途のためのガイダンス

TOE に以下を包含しない：

- トラステッドアプリケーション
- リッチ実行環境
- クライアントアプリケーション

以下において、TOE と TEE は、区別なく利用される。

2.2 TOE 記述

2.2.1 TEE 利用可能なデバイスのソフトウェアアーキテクチャ

TEE は、デバイスに組み込まれ、標準 OS 又は REE と共存して動作する。図 2-1 は、ハードウェアアーキテクチャから独立した、TEE 利用可能なデバイスのソフトウェアコンポーネントのハイレベルな図を提供する。

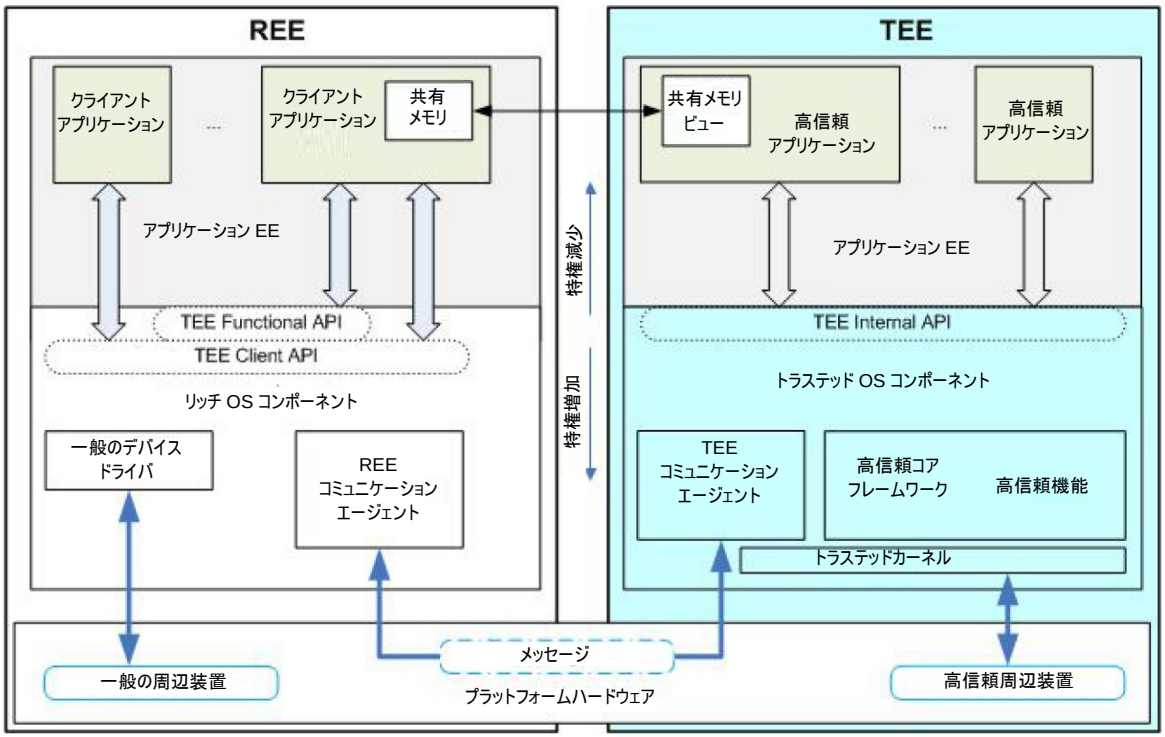

図 2-1: TEE 全体のソフトウェアアーキテクチャ

TEE ソフトウェアアーキテクチャは、2 つの異なるクラスのコンポーネントを識別する:

- TEE 上で動作し、TEE 内部 API を利用する、トラステッドアプリケーション
- TEE 内部 API からアクセス可能な、REE ソフトウェア及びトラステッドアプリケーションによって要求されるシステムレベルの機能を通信装置に提供する役割を持つトラステッド OS コンポーネント

REE ソフトウェアアーキテクチャも、2 つの異なるクラスのコンポーネントを識別する:

- TEE 上で動作している TA によって提供されるセキュアなサービスにアクセスするために TEE クライアント API を使用する、クライアントアプリケーション
- TEE クライアント API を提供し、TEE にリクエストを送信する、Rich OS

TEE ソフトウェア外部インタフェースは、TEE 内部 API(トラステッドアプリケーションによって使用される)及び TEE Communication Agent プロトコル(REE によって使用される)を包含する。

TEE クライアント API レベル以下で使用される、REE と TEE の間の通信プロトコルは、実装依存である、ゆえに、本プロテクションプロファイルは、このような特定のプロトコルを義務付けしない。本 PP に適合するセキュリティターゲットは、REE から TEE との通信に利用するすべてのソフトウェアインタフェースについて記述しなければならない(shall)。

2.2.2 TEE 利用可能なデバイスのハードウェアアーキテクチャ

TEE は、以下を含むデバイスプラットフォームに組み込まれる:

- ハードウェア処理ユニット

- 以下のようなハードウェアリソース
  - 物理的揮発性メモリ
  - 物理的不揮発性メモリ
  - キーボードやディスプレイなどの周辺装置
  - 暗号アクセラレータ
  - セキュアなクロック
  - セキュアエレメント
- 処理装置とハードウェアリソースの間のコネクションのセット

TEE 利用可能なデバイスは、図式的に 4 つの階層で構成される:

- *ダイ層*、プロセッサ、及びメモリ、暗号アクセラレータ、周辺(例、JTAG、USB、シリアル、HDMI) 等のようなリソースを含む、System-on-Chip (SoC)。
- *パッケージ層*、SoC を組み込み、さらにリソース、例、不揮発性及び揮発性メモリ、ピン、又はバスを含む。同じパッケージ層の内部のリソースは、外部からアクセスできないようなバスを用いて接続される。本仕様での外部バスは、パッケージ層の外部となる。「3D」ダイスタッキング技法がダイ層にないような、より多くの機能をパッケージ内部に配置するために利用されるかもしれない。
- *PCB 層*、SoC、パッケージ、不揮発性及び揮発性メモリ、ワイヤレス及びコンタクトレスインタフェースチップ、セキュリティモジュール及びその他のリソースを含む。
- *利用者層*、タッチスクリーン又はキーボードのような、パッケージへのユーザインタフェースを含み、さらにその他のリソースを含むかもしれない。

TEEは、通常一つのパッケージのダイ層及びパッケージ層に実装されるが、TEEコンポーネント間の暗号学的なリンク (セキュアなチャネル) を用いて、多くの別々なパッケージ内でインスタンス化されるかもしれない。TEE ハードウェアの外部インタフェースは、パッケージの入出力インタフェースを意味し、利用者層と SoC 自体の両方から、パッケージリソースへのアクセスと SoC 内部への間接的なアクセスを提供する。本 PP は、パッケージ内部について、ブラックボックスと見なす。

それでもなお、TEE の物理的境界は、実装依存である。さらに、TEE によって管理されるような、セキュリティ機能を実現するために利用される「高信頼な」リソースのセットは、動的に変更可能である。例えば、キーボードのような何らかの通信リソースは、TEE がこれらリソースへの独占的アクセスを実施すれば、TEE 境界内に入れる場合がある。論理的な観点から、TEE によって利用される「高信頼な」リソースは、REE によって利用される「信頼されない」リソースから分離される。即ち、TEEとREEは、図 2-2 に示す通り、デバイス内に共存するが、互に分離される。

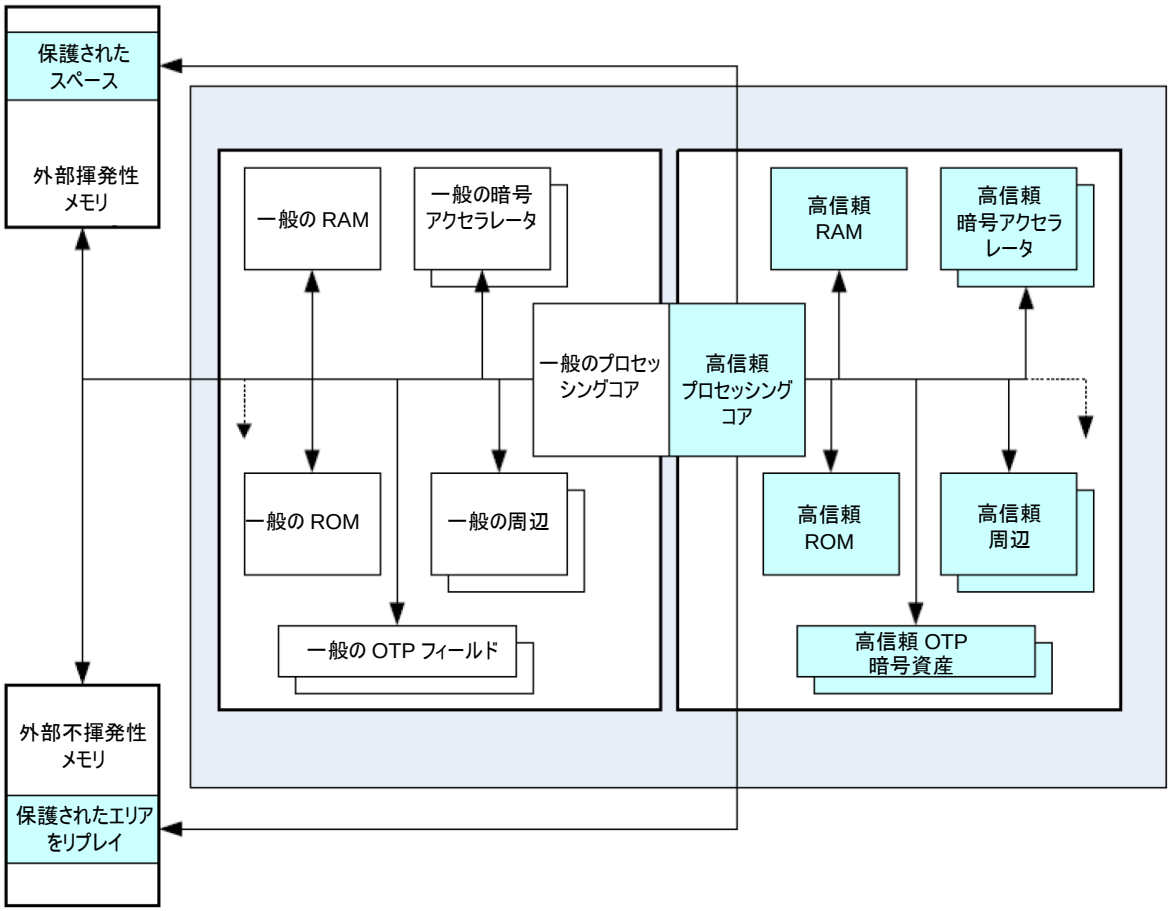

図 2-2: 分離された高信頼リソースと信頼されないリソース

実際に、デバイス内で TEE を設計し、それを REE から分離するための方法は、いくつかある。図 2-3 では、TEE と REE の間のリソース共有の異なる方針を持つ、3 つの実現候補について説明している。実際のところ、TEE と REE は、デバイスリソースへのアクセスを TEE が制御するように提供されたデバイスリソースを共有することができる。

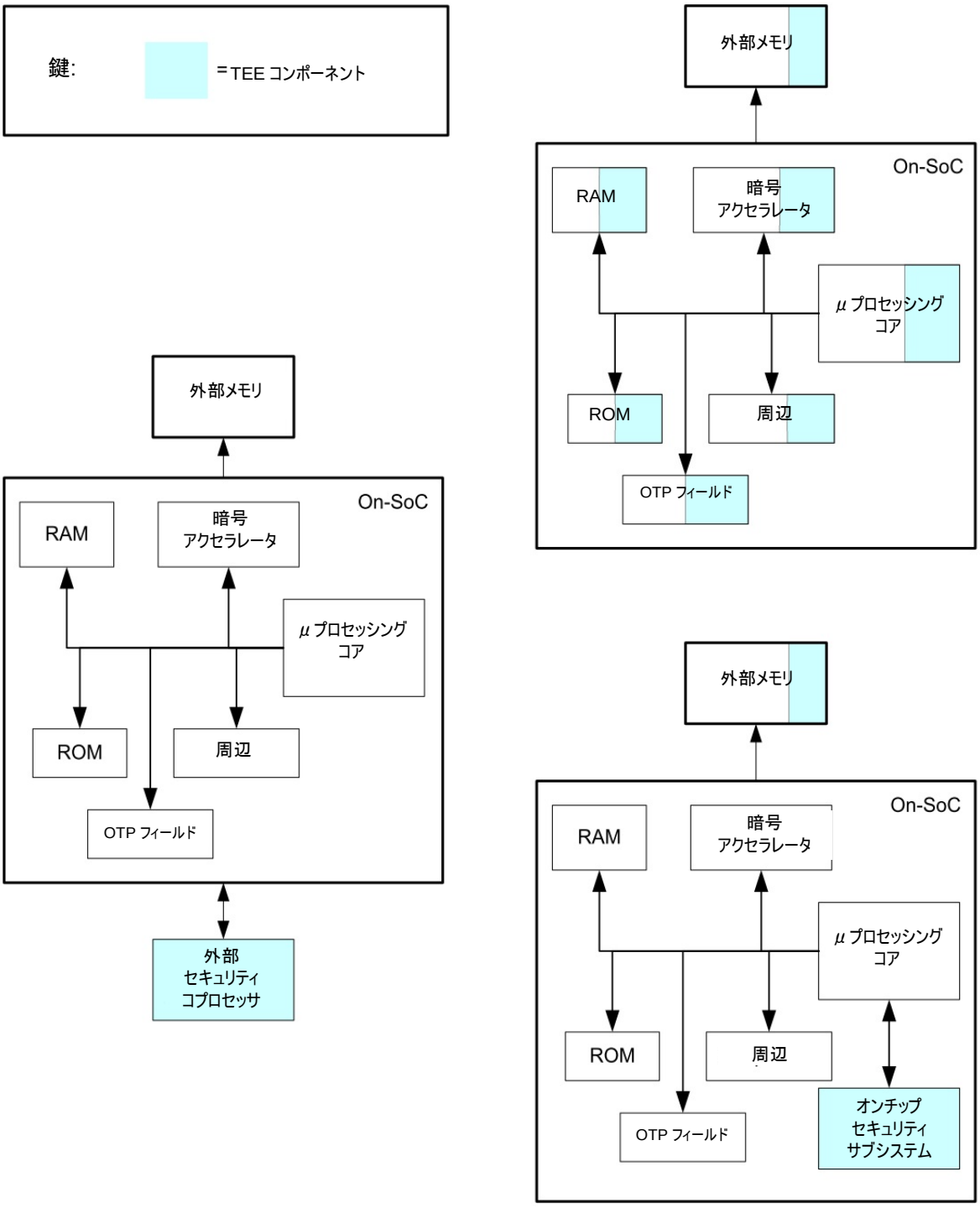

図 2-3: TEE 実現の例

本プロテクションプロファイルは、特定のハードウェアアーキテクチャ、リソースセット、又は REE からの隔離メカニズムを義務付けない。本 PP に適合するセキュリティターゲットは、物理的レイアウトについて記述し、TEE の物理的境界とハードウェア外部インタフェースを正確に定義しなければならない(shall)。

2.3 TOE の用途と主なセキュリティ機能

TEE の目的は、トラステッドアプリケーションの相互の隔離とその他の実行環境との隔離を実施し、TEE によって管理される資産の完全性と機密性を保証しつつ、それらをセキュアにホストし、実行することである。

以下のセクションでは、TEE セキュリティ機能と TEE の意図される用途について定義する。

2.3.1 TEE セキュリティ機能

評価の範囲にあるような、最終利用者フェーズ (参照、セクション 2.5) の TEE セキュリティ機能は、以下からなる:

- デバイスで動作する TEE コードの真正性を保証し、完全性に寄与するような、SoC にバインドされる資産を用いたセキュアな初期化プロセスを介した TEE インスタンス化。
- TEE サービス、含まれる TEE リソース及びすべてのトラステッドアプリケーションの REE からの隔離
- トラステッドアプリケーション間の隔離及び TEE のトラステッドアプリケーションからの隔離
- TEE の通信端点を含む、TEE 内部の CA と TA の間の保護された通信インタフェース。
- 一貫性 (参照、セクション 1.4)、機密性、原子性及び TEE へのバインディングを保証している、TA と TEE データと鍵の高信頼ストレージ。
- 乱数生成器
- 以下を含む暗号 API:
    - 鍵及び鍵ペアの生成と導出
    - SHA-256、AES 128／256、T-DES、RSA 2048 等 (このリストは一例である、以下の適用上の注釈を参照されたい) のような、暗号アルゴリズムのサポート
- TA コードの真正性を保証し、完全性に寄与するような、TA インスタンス化
- モノトニックな TA インスタンス時間
- TA サービスの正しい実行
- TEE ファームウェア完全性検証
- TEE ファームウェアのダウングレードの防止

TEE セキュリティ機能は、TOE の論理的境界を定義する。この境界のインタフェースは、それぞれセクション 2.2.1 及び 2.2.2 で説明された、ソフトウェア外部インタフェース及びハードウェア外部インタフェースである。

トラステッドアプリケーションによって提供されるセキュリティ機能は、TOE の適用範囲外である。

適用上の注釈:本 PP に適合するセキュリティターゲットは、(実行前の TA 真正性の検証に加え)適用可能な場合は TA 管理機能を含めて、実際の TOE の特徴を伴ったセキュリティ機能の記述と、製品によってサポートされる暗号アルゴリズムの完全なるリストを完成しなければならない(shall)。

2.3.2 TOE の用途

TEE は、セキュリティ保護を要求するような幅広いサービス用にモバイルデバイスの利用を可能とする、例えば:

- 法人向けサービス: プッシュ型電子メールアクセス及びオフィスアプリケーションを可能にする企業向けデバイスは、仮想プライベートネットワーク (VPN)、データのセキュアなストレージ、及び IT 部門によるデバイスのリモート管理を通して、従業員に対して業務アプリケーションへのセキュアかつ高速なリンクを要求するような適応性を与える。
- コンテンツ管理:今日のデバイスは、HD ビデオの再生とストリーミング、モバイル TV 放送受信、及びコンソール品質の 3-D ゲームを提供する。本機能は、しばしば、デジタル著作権管理 (DRM) 又は条件付きアクセスを通して、コンテンツ保護を要求する。
- 個人データ保護:デバイスは、ますます多くの個人情報 (連絡先、メッセージ、写真、ビデオクリップのような) に加え、機微なデータ (クレデンシャル、パスワード、医療データ等) でさえ蓄積する。セキュアなストレージ手段は、情報の喪失、盗難、又はマルウェア(悪意のあるソフトウェア) のようなその他の敵対的な事象に際して、本情報の暴露を防止することが要求される。
- 接続性保護:複数の技術を通したネットワーキング—3G、4G、又は Wi-Fi/WiMAX 、ならびに、Bluetooth®や Near Field Communication(NFC) のようなの個人通信手段—は、ピアツーピア通信及びインターネットアクセス用にモバイルデバイスの利用を可能にする。ウェブサービス又はクラウドコンピューティングに依拠するリモートストレージを含めて、このようなアクセスは、通常、SSL/TLS 又は IPsec インターネットセキュアプロトコルを利用する。鍵材料又はセションのクライアント端点の取扱いは、しばしばセキュアとされる必要がある。
- モバイル金融サービス:ある種の金融サービス、例えばモバイルバンキング、モバイル送金、モバイル認証 (例、ワンタイムパスワードーOTP 技術で利用)、モバイル非接触型決済等は、スマートフォンを対象とする傾向がある。これらのサービスは、潜在的にデバイスをセキュアエレメントと連携させることで実現できるような、セキュアな利用者認証とセキュアなトランザクションを要求する。

主な TEE 適用例の概要については、TEE ホワイトペーパー[WP]を参照のこと。

2.3.3 TEE Time and Rollback PP モジュール

TEE Time and Rollback PP モジュールは、セクション 2.3.1 で定義されるコア機能を補足するような、以下のセキュリティ機能に対処する:

1. モノトニックな TA 持続時間
2. TA 高信頼ストレージ(データと複数の鍵) の完全性検証
3. TA コードと設定データの完全性検証

モノトニックな持続時間は、リモート支援なしにパワーサイクル後にサービスが提供されることを可能にすることに留意されたい。起動時に更新された時間を取得可能な、接続されたサービスのために、モノトニックなインスタンス時間は十分であるかもしれない。

2.3.4 TEE Debug PP モジュール

TEE Debug PP モジュールは、この機能がサポートされないコア構成などで、TEE Debug 管理者用の TEE Debug 機能へのアクセスに対処する。

2.4 利用可能な非 TOE ハードウェア／ソフトウェア／ファームウェア

TOE は、動作するために、不揮発性メモリのような、何らかの非 TOE ハードウェア、ソフトウェア又はファームウェアを要求するかもしれない。しかし、TOE は、TOE セキュリティ機能が非 TOE ハードウェア、ソフトウェア又はファームウェアの適切なふるまいに依存しないような方法で実現されなければならない(must)。

適用上の注釈：本 PP に適合するセキュリティターゲットは、TOE によって利用される非 TOE 資源のリストと共に利用可能な非 TOE ハードウェア／ソフトウェア／ファームウェアの記述を完成しなければならない(shall)。

2.5 参照デバイスのライフサイクル

ここで概説されるデバイスのライフサイクルは、開発、製造、アセンブリのプロセスに従って、実装が逸脱可能な参照ライフサイクルである。ライフサイクルは 6 つのフェーズに分かれている：

- フェーズ 1 は、ファームウェア、ソフトウェア及びハードウェアの設計に対応する；TEE 及び追加コンポーネントの両方をカバー
- フェーズ 2 は、TEE をサポートするハードウェアプラットフォームの全体的な設計に対応
- フェーズ 3 は、チップセット及びその他のハードウェアコンポーネントの製造に対応
- フェーズ 4 は、ソフトウェア準備 (例、TEE ソフトウェア及びその他のソフトウェアをリンク) をカバー
- フェーズ 5 は、デバイスアセンブリからなる；最終利用者への配付前にデバイスをセキュアな状態に保持するために必要な任意の初期化及び設定ステップを含む
- フェーズ 6 は、デバイスの最終利用を表す

セキュアなブート/ファームウェアは、TEE 初期化コードを含み、後でアップグレードされるかもしれないが、通常はフェーズ 3 でインストールされる。TEE ストレージサービスの信頼の基点及び TEE の一意な識別子は、フェーズ 3 又は 5 でセットされる (インジェクション又は基板上で生成)。トラステッド OS は、このステップの後、更に後でアップグレードされるかもしれないが、フェーズ 3 又は 5 でインストールされる。トラステッドアプリケーションは、トラステッド OS と共に、又はトラステッド OS の後、ステップ 3 又はステップ 5 のいずれかにおいてインストールされるかもしれない － 後者の場合、トラステッドアプリケーションは、ステップ 4 でトラステッド OS とリンクされるかもしれない。TOE が TEE Debug 機能をサポートする場合、その機能が TEE 上で有効化されるかどうかを示すフラグ及び Debug 認証鍵のような Debug クレデンシャルが、フェーズ 3 又は 5 でセットされる。

TOE 配付ポイントが、評価の境界を確立する。配付ポイントは、フェーズ 3 からフェーズ 5 までに分布可能であるが、TEE ストレージサービスの信頼の基点、TEE の一意な識別子、Debug 有効化フラグ及び Debug クレデンシャル(TEE Debug PP モジュールが含まれる場合) の設定、及びトラステッド OS のインストールに必ず従わなければならない(must)：

- 配付ポイントの前の環境、プロセス及び手順のセキュリティは、ALC 保証クラスを通して、EAL 2 に従って評価される
- 配付ポイントからフェーズ 5 の終了までの環境、プロセス及び手順のセキュリティは、組織のセキュリテ

ィ方針及び環境のセキュリティ対策方針によって、AGD 保証クラスを通してカバーされる

- 最終利用環境のセキュリティは、TOE セキュリティ機能によって、及び環境のセキュリティ対策方針によってカバーされる。

図 2－4 は、表 4 と共に、6 つのフェーズの考えられるインスタンス化の一例を表す。表は、異なるライフサイクルフェーズに関係する登場人物を表す。登場人物は、全体的なセキュリティレベルが満たされるような、他のエンティティに作業を委ねてもよいことに留意されたい。

見やすくするために、図及び表は、すべての可能性をカバーしていない。6 つの同じフェーズで構成されるが、表示されたステップの異なる所有者を持つ他のフローもありうる。TEE が分離した別々のプロセッサ上で動作する場合、又はデバイス製造者がチップセット製造者の提供するターンキープラットフォームを集積するだけの場合に TEE がチップセット製造者によってインストールされる場合、又は逆にデバイス製造者が TEE のインテグレーションに全責任を負う場合、異なる流れ図がもたらされる可能性がある。

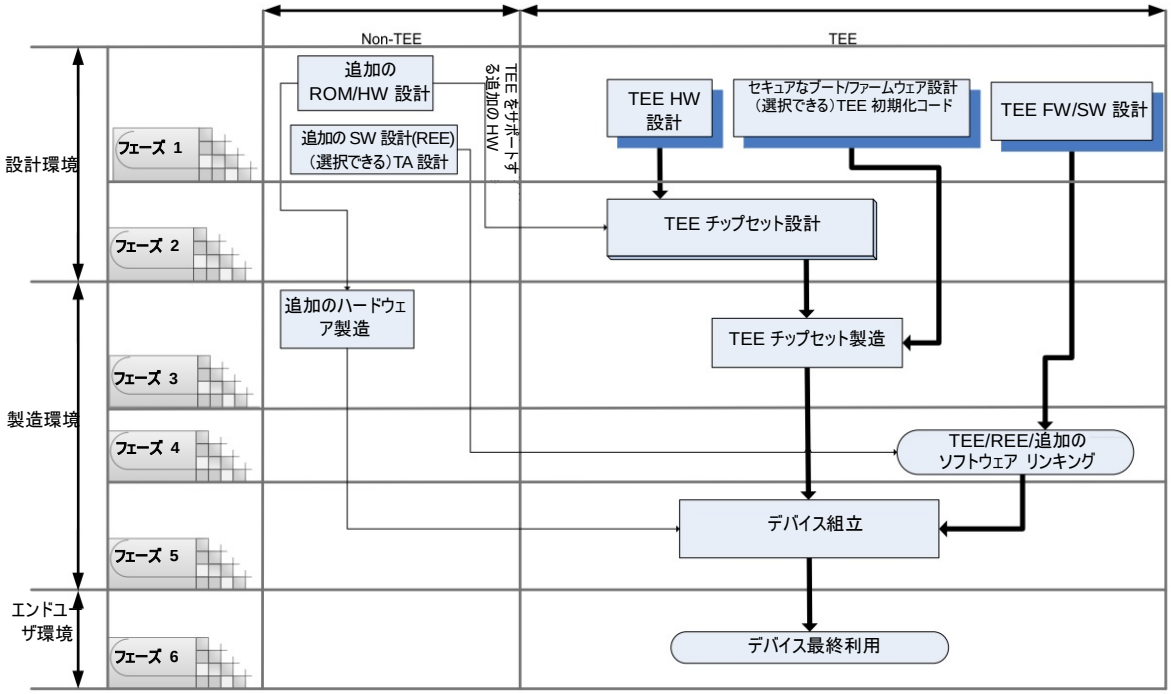

図 2-4: TEE 利用可能デバイスのライフサイクル

フェーズ	登場人物
1 & 2:ファームウェア／ソフトウェア／ハードウェア設計	TEE ソフトウェア開発者は、 • GlobalPlatform 仕様に適合する TEE ソフトウェア開発とテストを担当する • TEE をインスタンス化／初期化するような TEE 初期化コードについても開発してもよい (例、セキュアブートコードの一部) • TEE ソフトウェアリンク要件を規定する デバイス製造者は、REE 管理の資源を提供するため、フェーズ 4 にて

フェーズ	登場人物
	TEE にリンクされるような、追加の REE ソフトウェアを設計してもよい。彼はまた、フェーズ 4 でインテグレートするトラステッドアプリケーションについても設計してもよい。 TEE ハードウェア設計者は、TEE ソフトウェアが動作するプロセッサ(の一部) の設計、及び TEE によって利用されるハードウェアセキュリティ資源(の一部) の設計を担当する。 シリコンベンダは、ROM コードと TEE チップセットのセキュアな部分を設計する。シリコンベンダが TEE ハードウェア全体を設計していない場合、シリコンベンダは、TEE ハードウェア設計者によって設計された TEE ハードウェアをインテグレート(及びもしかすると追加)する。
3:TEE 製造	シリコンベンダは、TEE チップセットを製造し、TEE の信頼の基点を有効化し、設定又はシード値の供給をする。
4:ソフトウェア製造	デバイス製造者は、TEE、任意のプリインストールされるトラステッドアプリケーション、及び製品の利用に必須の追加ソフトウェア(例、REE、クライアントアプリケーション等) を含むであろう、製品にロードするソフトウェアのインテグレーション、検証及び準備に責任を負う。
5:デバイス製造	デバイス製造者は、デバイスのアセンブリと初期化、及び最終利用者への配布前のデバイス上のその他の操作 (トラステッドアプリケーションのロード又はインストールを含む) の責任を負う。
6:最終利用フェーズ	最終利用者は、利用可能なデバイスを入手する。 トラステッドアプリケーションの責任者は、発行後のトラステッドアプリケーションのロード、インストール、及び除去の責任を負う。

表 4: デバイスのライフサイクルにおける登場人物

適用上の注釈:セキュリティターゲットは、実際の TOE ライフサイクルについて記述し、関与する登場人物と開発／製造サイトを識別しなければならない(shall);セキュリティターゲットは、コンポーネント(トラステッド OS、信頼の基点、TA)のデバイスへの実際の統合ポイントについて、TOE の実際の配付ポイントと共に識別し、また、TEE ストレージサービスの信頼の基点の設定のためのプロセス、及びそれが発生するフェーズについて明確にしなければならない(shall)。

セキュリティターゲットは、また、TOE 及び TOE と共に配布されるコンポーネント、例、標準 OS、プリインストールされているトラステッドアプリケーション、又はクライアントアプリケーション等があれば、識別しなければならない(shall)。TOE が、本プロテクションプロファイルの適用範囲外の、TA 管理機能 (即ち、フェーズ 6、又は一般に配付ポイントの後の TA のインストール) を提供する場合、それについても同様にセキュリティターゲットに記述されなければならない(must)。

3 適合主張と一貫性根拠

本書は、モジュラーPP 方法[PP-MOD]を利用し、ベース PP 及び 2 つの PP モジュールを含む。本セクションは、ベース PP 及び TEE Time and Rollback 及び TEE Debug PP モジュールへ適用する。

3.1 CC への適合主張

本ベースプロテクションプロファイルは、CC パート 2 [CC2] 拡張、及び CC パート 3 [CC3] 拡張である。CC パート 2 は、セキュリティ機能コンポーネント FCS_RNG.1 乱数生成と FPT_INI.1 TSF 初期化について拡張される。

CC パート 3 は、セキュリティ保証コンポーネント AVA_TEE.2 低 TEE 脆弱性分析について拡張される。附属書 A.2 は、AVA_TEE.2 と AVA_VAN.2 の関係を説明する。両方の SAR とも脆弱性分析に関係する。唯一の違いは、それぞれの AVA コンポーネント用に利用される攻撃能力評価表で定義されるレーティングである。両方の AVA コンポーネントが主張されるので、本 PP に適合する評価製品は、2 つの評価表に従って評定されなければならない。

TEE Time and Rollback PP モジュールと TEE Debug PP モジュールは、CC パート 2 [CC2] 適合である。

3.2 パッケージへの適合主張

本 PP への適合 TOE の評価用の最小限の保証レベルは、セクション 6.1.4 で定義される、EAL 2 及び追加の保証要件 AVA_TEE.2 である。

本適合主張は、本書で定義される PP コンフィギュレーションへも適用する。

3.3 PP の適合主張

本 PP は、いかなる別の PP への適合を主張しない。

3.4 PP への適合主張

本 PP への適合は、適合主張するセキュリティターゲット及び PP に要求され、CC パート 1 [CC1] で定義される正確適合 (訳注：Strict Conformance) である。

本適合主張は、本書で定義される PP コンフィギュレーションへも適用する。

3.5 PP モジュールの一貫性根拠

3.5.1 TEE Time and Rollback PP モジュール

TEE Time and Rollback PP モジュールは、本書のベース PP とのみ併せて利用することを意図されている。ベース PP を形成するセクション 2.3.1 で定義される TEE 機能を補完する。モノトニックな TA 持続時間という新しい機能を定義し、トラステッドストレージ、TA コード、及び設定データの一貫性検証を完全性検証に拡

張する。

本 PP モジュールは、あらゆる前提条件も OSP も環境のセキュリティ対策方針も追加しない。

本 PP モジュールは、2 つの新しい脅威、及び持続時間とロールバックに関連したいくつかの対応するセキュリティ対策方針を追加する。本 PP モジュールは、ベース PP の FDP_SDI.2 を一貫性の特性のみの代わりに完全性の特性について拡張するような FDP_SDI.2/Rollback を含め、4 つの新しい SFR を追加する。

ベース PP からの及び PP モジュールからの、SPD、対策方針、及びセキュリティ機能要件の結合は、矛盾を生じない。

3.5.2 TEE Debug PP モジュール

TEE Debug PP モジュールは、本書のベース PP とのみ併せて利用することを意図されている。ベース PP を形成するセクション 2.3.1 で定義される TEE 機能を補完する。TEE Debug 管理者が、認証後の Debug 機能へのアクセスを許可される可能性について定義する。

本 PP モジュールは、あらゆる前提条件も OSP も環境のセキュリティ対策方針も追加しない。

本 PP モジュールは、デバッグ用インタフェースのアクセス制御に関連した 1 つの新しい脅威、及び対応するセキュリティ対策方針を追加する。本 PP モジュールは、アクセス制御用の 6 つの新しい SFR を追加する。

ベース PP からの及び PP モジュールからの、SPD、対策方針、及びセキュリティ機能要件の結合は、矛盾を生じない。

さらに、デバッグ機能は、TEE Time and Rollback PP モジュールで定義される機能から独立している。両方の PP モジュールは、独立に利用可能である。

4 セキュリティ課題定義

本章は、TEE 及びその運用環境によって対処されるセキュリティ課題について説明する。運用環境は、TEE インテグレーション及びメンテナンス環境及び TA 開発環境を表す。セキュリティ課題は、TEE 利用可能デバイスが本分野で直面するかもしれない脅威、運用環境における前提条件及び TEE 又は運用環境で実装されなければならない組織の方針から構成される。

4.1 資産

本セクションは、TOE の資産及びそれらの特性を示す；真正性、一貫性、完全性、機密性、モノトニシティ(単調性)、ランダム性、原子性、読み出し専用及びデバイス結合 (参照、セクション 1.4 の定義) である。

4.1.1 TEE ベース PP

TEE 識別

製造者、ベンダ又はインテグレータに関係なく、すべての GlobalPlatform TEE の中でグローバルに一意の TEE 識別データ。本データは、通常 TEE のトラステッド OTP メモリに保存される。

特性：一意であり、かつ改変不能。

適用上の注釈：

TEE 識別子は、トラステッドアプリケーションだけでなく、デバイス上で動作するあらゆるソフトウェアに公開され、開示されるよう意図される。

RNG

乱数生成器

特性：予測できない乱数、十分なエントロピー。

TA コード

インストールされるトラステッドアプリケーションのコード。本データは、通常 REE と共有される外部不揮発性メモリに保存され、それによってアクセス可能になる可能性がある。

特性：真正性及び一貫性 (ランタイム完全性を意味する)。

TA データと鍵

TEE セキュリティサービスを用いて TA によって管理され及び保存されるデータと鍵。データと鍵は、利用者 (TEE 利用可能デバイスの所有者) 又は TA サービスプロバイダのいずれかにより所有される。このデータは、通常 REE と共有される外部不揮発性メモリに保存され、それによってアクセス可能になる可能性がある。

特性：真正性及び一貫性 (ランタイム完全性を意味する)、原子性、機密性及びデバイス結合。

TA インスタンス時間

TA インスタンスライフタイム中のモノトニック (単調な) 時間。低電力状態を通した遷移によって影響を受けない。TEE リセット又は TA シャットダウンを越えて持続しない。

特性：モノトニシティ(単調性)

TEE ランタイムデータ

実行変数、ランタイムコンテクスト等を含む、ランタイム TEE データ。このデータは、揮発性メモリ内に保存される。

特性：一貫性 (又はこれらの概念が非永続的データと同等であるような完全性)、及び機密性、TEE により生成される乱数を含む。

TEE 永続的データ

TEE 永続的データ、TEE 暗号鍵 (TA コードを認証するためのインスタンス鍵) 及び TA の特性を含む。このデータは、通常 REE と共有される外部不揮発性メモリに保存され、それによってアクセス可能になる可能性がある。

特性：真正性、一貫性 (ランタイム完全性を意味する)、機密性及びデバイス結合。

TEE ファームウェア

TEE バイナリ、TEE コード及びバージョニング情報のような定数データを含む。本資産は、通常 REE と共有される外部不揮発性メモリに保存され、それによってアクセス可能になる可能性がある。

特性：真正性、完全性。

TEE 初期化コードとデータ

デバイス電源投入から TEE セキュリティサービスの完全な起動までに利用される初期化コードとデータ (例えば、暗号学的証明書)。TEE の認証は、その初期化の一部分である。

特性：完全性

TEE ストレージの信頼の基点

保存されたデータと鍵を TEE へ結び付けるために利用される TEE ストレージの信頼の基点。このデータは、通常 TEE のトラステッド OTP メモリに保存される。

特性：完全性及び機密性。

適用上の注釈：

この資産の機密性は、資産が TEE の SoC 内部に存続するという単純な事実によって保証される。

4.1.2 TEE Time and Rollback PP モジュール

本 PP モジュールの資産は、TEE ベース PP の資産を以下のように拡張する：

- 「TA 持続時間」は、新しい資産である
- 「TA データ及び鍵モジュール」、「TA コードモジュール」及び「TEE データモジュール」は、ベース PP と同じ資産だが、一貫性及び完全性の特性が追加される。つまり、TOE は完全なロールバック保護を提供しなければならない。

TA 持続時間

TA の任意のインスタンスによって実行される 2 つの「時間設定」操作の間のモノトニック(単調な) TA 時間。TEE リセットを越えて持続する。

特性：モノトニシティ

TA データ及び鍵モジュール

TEE セキュリティデバイスを用いて TA によって管理され、保存されるデータと鍵。データと鍵は、利用者(TEE 利用可能デバイスの所有者) 又は TA サービスプロバイダのいずれかによって所有される。
特性:真正性、一貫性、完全性、原子性、機密性及びデバイス結合。
適用上の注釈:
ストレージの完全性は、ストレージロケーションから正常に読み出された値が、このロケーションに書き込まれた最後の値であることを意味する。

TA コードモジュール
インストールされるトラステッドアプリケーションのコード。
特性:真正性、一貫性及び完全性。
適用上の注釈:
ストレージの完全性は、ストレージロケーションから正常に読み出された値が、このロケーションに書き込まれた最後の値であることを意味する。

TEE データモジュール
永続的な TEE データ、TEE 鍵を含む。
特性:真正性、一貫性、完全性、機密性、デバイス結合。

TEE ロールバック検出データ
トラステッドストレージの前のバージョンのロールバックを検出するために利用される TEE データ。
特性:完全性。

4.1.3 TEE Debug PP モジュール

本 PP モジュールの資産は、新しい暗号鍵を提供することによって、TEE ベース PP の資産を拡張する。

TEE デバッグ認証鍵
デバッグ機能のアクセスを許可するための TEE Debug 管理者認証に利用される TEE デバッグ認証鍵。
特性:完全性及び機密性。

4.2 利用者／サブジェクト

TOE の利用者には 2 種類ある;TEE 内部 API を通して TOE サービスを利用する、トラステッドアプリケーション、及びトラステッドアプリケーションによってエクスポートされる TOE のサービスを利用する、リッチ実行環境である。

4.2.1 TEE ベース PP

トラステッドアプリケーション(TA)
TEE 内部 API を通して TOE サービスを利用する、TEE 上で動作するすべてのトラステッドアプリケーション。

リッチ実行環境(REE)
標準 OS、TEE クライアント API 及びトラステッドアプリケーションを利用するクライアントアプリケーションを

ホストする、リッチ実行環境は、TOE の利用者である。

4.2.2 TEE Debug PP モジュール

TEE デバッグ管理者

TEE デバッグ管理者又は TEE デバッグ機能のアクセスを許可される、彼を代行する登場人物。

4.3 脅威

本プロテクションプロファイルは、最終利用フェーズ中に生じ、かつソフトウェア手段によって達成可能であるような TEE 資産に対する脅威を対象とする。攻撃者は、TEE を組み込むデバイスへのリモート又は物理 (ローカル) アクセスを有する個人又は組織である。デバイスの利用者は、TEE が第三者の資産を保持するときに、潜在的な攻撃者となる。攻撃者の背景にある動機は、非常に多岐にわたるかもしれないが、一般的に TEE 上で動作するトラステッドアプリケーションへリンクされる。攻撃者は、例えば、デバイス所有者のコンテンツ (デバイスで保存されるパスワード等) 又はサービスプロバイダのコンテンツを盗もうとしたり、又は TEE や TA サービスから不当に利益を得ようとしたり (法人のネットワークをアクセス、もしくは同じ又は他のデバイスいずれかの DRM コンテンツの許可されない利用を実行する等)、又はデバイス／TEE 製造者やサービスプロバイダの評判を脅かそうとしたりするかもしれない。攻撃の影響は、攻撃を受けた個々の資産の価値だけでなく、場合によっては、低コストで迅速な攻撃を再現する可能性にも左右される：所与の TEE 利用可能デバイス上で実行された 1 回の攻撃は、同時に多くのデバイスに達するような大規模な攻撃よりも影響はより小さい。

本プロテクションプロファイルは、例えば、インターネットを介して、簡単に拡散させることができ、デバイス自体に損害を与えずに TEE 資産への不当なアクセスを得るための特権ベクタを構成するような非破壊ソフトウェア攻撃に焦点を当てる。多くの事例から、ソフトウェア攻撃には少なくとも 2 種類の攻撃者が関係する：脆弱性を発見し、悪意あるソフトウェアを考案し、それを配付するような識別フェーズでの攻撃者、及び悪意あるソフトウェアを実行することによって脆弱性を効果的に悪用するような悪用フェーズでの攻撃者である (最終利用者又は利用者を代行するリモート攻撃者)。識別攻撃者と悪用攻撃者は、利害関係のない、又は攻撃を広く拡散させる可能性のない攻撃である場合、同一人物となりうる。

実際に、様々なデバイス管理や展開モデルは、サービスと同様に、想定される多様な脅威モデルを作り出す。サービスのインストールが管理され、これらのサービスを破壊することに何の価値も持たない最終利用者がいる、法人の環境で利用されるデバイスに対して、脅威モデルは、全体的なソフトウェア攻撃と脆弱性に対処する。攻撃は、他のこの種のデバイスへの大規模なアクセスは想定されないので、実際に容易には複製されないだろう。管理されない、個人デバイスについては、デバイスがより普及する反面最終利用者自身が攻撃を拡散することに今日を持つかもしれないため、攻撃が拡散可能となる可能性が高い。したがって、攻撃において識別と悪用フェーズの分離は、このような管理されないデバイスを評価するための鍵である。

デバイスの使用方法に応じて、攻撃者、ソフトウェア又はハードウェアに利用可能な手段の観点から、また複数のデバイスを利用する可能性の観点から、異なる前提条件が識別フェーズに関して有効となるかもしれない。識別と悪用が分離されるときに、もしかすると非破壊方法で、攻撃が容易に拡散しうるような制御を受けないデバイスに対処するため、識別フェーズでの攻撃者は、ソフトウェア及び／又はハードウェアの知見を持ち、また PCB 上のパッケージインタフェースで攻撃者に操作を許すようなオシロスコープ、プロトコルアナライザ、インサーキットエミュレータ、又は JTAG デバッガのような装置へアクセスするかもしれない。しかし、利用可能な攻

撃能力は、パッケージの深いところ及び SoC のレベルで行うのに十分であるとは想定されない。

識別と悪用が分離されるとき、2 つの主要な攻撃者プロファイルが悪用フェーズで上げられる:

- リモート攻撃者:本悪用プロファイルは、リモート制御されるデバイス上で攻撃を実行するか、又はその代りに最終利用者にとって非常に便利なダウンロード可能なツールを作る。攻撃者は、識別フェーズで識別された脆弱性の詳細情報と識別子によって提供される攻撃コード／実行可能形式のような出力を取り出す。攻撃者は、次にリモートツールやマルウェアを作り、フィッシングなどの技術を使ってそれを犠牲者にダウンロードさせて実行させる、又はその代りにインターネット上で利用可能なわかりやすいツールを作る。新しいマルウェア、トロイの木馬、ウイルス、又はルート権限取得ツールの設計は、しばしばインターネット上で利用可能である既存のベースから実行されることに留意されたい。
- 基本デバイス攻撃者:本悪用プロファイルは、ターゲットとなるデバイスへの物理的アクセスを有する;最終利用者又は彼を代行する誰かである。攻撃者は、識別子やインターネット上に書き込まれた攻撃実行方法のガイドラインから、攻撃コード／アプリケーションを検索し、ダウンロードし、悪用の実行を可能にする REE への特権アクセスを得るために、デバイスを脱獄(訳注:jailbreak 自由になること)／ルート権限取得／再度フラッシュするためのツールを使う。攻撃者は、しろうとであるかもしれないし、又はある程度の専門知識を持っているかもしれないが、攻撃には特定の装置を要求されない。

すべてのケースで、全体的な攻撃能力は、悪用ソフトを実行する高度な攻撃者に直面する可能性について非常に制限している。大規模な悪用攻撃について、我々は、識別及び悪用フェーズ、適用可能な攻撃能力評価表、及び TEE がこの分野で直面するにちがいないような代表的攻撃のセットの包括的記述について、附属書 A を参照する。ある程度、利害と悪用ソフトの拡散の可能性が限られているため、管理されたデバイスに対する攻撃は附属書 A の攻撃のサブセットのみとするべきである(should)。

「脅威」ステートメントは、共通の目標、脅かされる資産、及びいくつかの場合には、典型的な識別及び／又は悪用の攻撃経路を提供する。いくつかの脅威は、実際には、例えば資産の暴露又は改変に関連するような、より長い攻撃経路のステップを形成する。それでもなお、対抗手段の追跡を促進するため、それらは別々に記述される。

4.3.1 TEE ベース PP

以下の脅威は、あらゆる TEE へ適用する。

T.ABUSE_FUNCT

攻撃者は、想定される利用可能な範囲外の TEE 機能をアクセスする、即ち TEE ライフサイクル又はステートマシンの非可逆フェーズを侵害する。

攻撃者は、機微なデータを入手、又は TSF を危殆化 (セキュリティサービスを迂回、不活性化又は変更) することを攻撃者に許すような、不法な TEE をインスタンス化したり、セキュアではない状態で TEE を起動したり、又はセキュアではない状態に移行するよう管理する。

直接脅かされる資産:TEE 初期化コード及びデータ(完全性)、TEE ランタイムデータ(機密性、完全性)、RNG(機密性、完全性)、TA コード(真正性、一貫性)。

間接的に脅かされる資産:TA データと鍵 (機密性、真正性、一貫性) インスタンス時間を含む。

適用上の注釈:

攻撃経路は、例えば、想定されない文脈又は想定外のパラメタでのコマンドの利用、許可されたエンティティへのなりすまし又は不正な特権を与えるようなひどい実装のリセット機能の悪用を用いて、構成されるかもしれない。

特に、TEE で動作するセキュアなアプリケーションと見せかけるような、リッチ OS で動作する偽造アプリケーションは、PIN とパスワードを取り込み、利用者を代行する本当のセキュリティアプリケーションを実行することができる。しかし、このような脅威は、TEE 単独によって対抗されず、例えば、クライアントと TA 間で適用可能な認証された通信チャネルを用いて、適用例の設計において考慮されなければならない(must)。

T.CLONE

攻撃者は、最初のデバイスの TEE 関連データを 2 番目のデバイスにコピーし、このデバイスに本物のデータとしてそれらを受け入れさせようとする。

直接脅かされる資産:すべてのデータと鍵(真正性、デバイス結合)、TEE 識別データ(真正性、完全性)。

T.FLASH_DUMP

攻撃者は、平文の外部フラッシュのコンテンツを部分的又はすべて回復する、即ち機微な TA と TEE データを暴露し、場合によってはその他の攻撃を仕掛けることを攻撃者に許してしまう。

直接脅かされる資産(機密性、真正性、一貫性):TA データと鍵、TEE 永続的データ。

適用上の注釈:

攻撃経路は、例えば、REE を通して、純粋にソフトウェアを介して、又は USB 接続により、(部分的な)メモリダンプの実行から構成される。

識別中に、別の例は、フラッシュメモリのはんだ付けを外し、その内容のダンプし、同じモデルの多くのデバイスへの特権的アクセスを与えるような秘密鍵を暴露することから構成される。

T.IMPERSONATION

攻撃者は、別のトラステッドアプリケーションのサービスとデータへの許可されないアクセスを得るため、トラステッドアプリケーションになりすましをする。

直接脅かされる資産(機密性、完全性):TEE ランタイムデータ、RNG。

間接的に脅かされる資産:すべてのデータと鍵(機密性、真正性、一貫性)。

T.ROGUE_CODE_EXECUTION

攻撃者は、機微なデータを暴露又は改変するため、悪意あるコードを TEE にインポートする。

直接脅かされる資産(機密性、完全性):TEE ランタイムデータ、RNG。

間接的に脅かされる資産(機密性、真正性、一貫性):すべて。

適用上の注釈:

REE 内でのコードのインポートは、TEE の管理対象外である。

T.PERTURBATION

攻撃者は、機微なデータを暴露又は改変したり、TEE 又は TA に許可されないサービスの実行を実施したりするため、TEE や TA のふるまいを改変する。

直接脅かされる資産:TEE 初期化コードとデータ(完全性)、TEE ストレージの信頼の基点(機密性、完全性)、TEE ランタイムデータ(機密性、完全性)、RNG(機密性、完全性)。

間接的に脅かされる資産:すべてのデータと鍵(機密性、真正性、一貫性)、TA インスタンス時間を含む。

適用上の注釈:

コマンドの許可されない利用(一つ又は多くの間違ったコマンド、未定義のコマンド、隠しコマンド、無効なコマンドシーケンス)、又はバッファオーバーフロー攻撃(実行コンテクストを改変するためにバッファの内容の上書き、又はシステム特権の取得) は、攻撃経路の例である。TEE は、例えば、マルチスレッディング又はコンテクスト/セション管理、又は非公開セションを、又は TEE によるコマンド実行中のシステムリセットの起動によって、悪用するような、REE 又は TA「プログラマエラー」を通して、攻撃される可能性もある。

T.RAM

攻撃者は、RAM の内容を部分的に又は全体的に回復する、即ちランタイムデータを暴露し、場合によっては、TEE 初期化コードとデータを妨害することを攻撃者に許してしまう。

直接脅かされる資産:TEE 初期化コードとデータ(完全性)、TEE ストレージの信頼の基点(機密性、完全性)、TEE ランタイムデータ(機密性、完全性)、RNG(機密性、完全性)。

間接的に脅かされる資産:すべてのデータと鍵(機密性、真正性、一貫性)。

適用上の注釈:

REE と TEE がメモリを共有したとき、攻撃経路は REE による(部分的)メモリダンプ(書込み/読出し)にある。

識別フェーズ中の、別な攻撃経路の例は、メモリバス上での探索、ランタイム時にのみ復号されるコードの漏えい、悪用可能なコードの欠陥の発見である。

T.RNG

攻撃者は、TEE によって生成される乱数について許可されないやり方で情報を取得する。これは、例えば、製品によって生成される乱数のエントロピーの不足によって生じるか、又は部分的又は全体的に事前に定義された値の出力を攻撃者が実施するためである。

不確実性の喪失(乱数の主要な特性) は、それらが暗号鍵生成に使用されるような場合に問題となる。故障又は早過ぎるエージングは、乱数についての情報の取得も許すことがある。

直接脅かされる資産(機密性、完全性):RNG と乱数から導出される秘密。

T.SPY

攻撃者は、ランタイム攻撃やストレージロケーションへの許可されないアクセスによって、機密データ又は鍵を暴露する。

直接脅かされる資産(機密性):すべてのデータと鍵、TEE ストレージの信頼の基点。

適用上の注釈:

CA 又は TA によるサイドチャネルの悪用(例、タイミング、電力消費)、残存する機微なデータの入手(例、不適切にクリアされたメモリ)、又は文書化されていないか、無効なコマンドコードの利用が、攻撃経路の例である。データは、その入手元のデバイスやその他のデバイスを悪用するために利用される可能性がある(例、共有される秘密鍵)。

識別フェーズ中、攻撃者は、例えば外部バスをプローブするかもしれない。

T.TEE_FIRMWARE_DOWNGRADE

攻撃者は、TEE ファームウェアの一部か全部をバックアップし、廃止された TEE 機能を利用するために後でそれをレストアする。

直接脅かされる資産(完全性):TEE ファームウェア。
間接的に脅かされる資産:すべてのデータと鍵(機密性、真正性、一貫性)。

T.STORAGE_CORRUPTION

攻撃者は、ストレージセキュリティメカニズムから想定されないふるまいを引き起こす試行において、トラステッドストレージを含む TEE によって利用される不揮発性ストレージの全部又は一部を破損させる。攻撃の最終目標は、TEE 又は TA データ及び/又はコードを暴露及び/又は改変することである。
直接脅かされる資産:TEE ストレージの信頼の基点(機密性、完全性)、TEE 永続的データ(機密性、一貫性)、TEE ファームウェア(真正性、完全性)、TA データと鍵(機密性、真正性、一貫性)、TA インスタンス時間(完全性)、TA コード(真正性、一貫性)。
適用上の注釈:
攻撃は、例えば、REE ファイルシステム又はフラッシュドライバに依存可能である。

4.3.2 TEE Time and Rollback PP モジュール

以下の2つの脅威は、トラステッドストレージと TA 持続時間完全性(耐ロールバック特性ともいう) を実装する TEE に適用する。

さらに、標準的な脅威 T.STORAGE_CORRUPTION は、OE.ROLLBACK へはもはやリンクされないが、O.ROLLBACK_PROTECTION にリンクされる。

T.ROLLBACK

攻撃者は、一部又はすべてのストレージ空間をバックアップし、廃止された TA サービスの利用又は廃止されたデータの TA による利用のために、後でそれをレストアする。
直接脅かされる資産(機密性、完全性): TA データと鍵、TEE 永続的データ、TA コード。
間接的に脅かされる資産(機密性、完全性):TEE ランタイムデータ、RNG。
適用上の注釈:
攻撃は、例えば、REE を用いるフラッシュからのストレージバックアップの実行と後でのそれのレストア、又はロールバック検出に利用する TEE 永続的データの改変、から構成される。

T.TA_PERSISTENT_TIME_ROLLBACK

攻撃者は、例えば期限切れの権限を延長する、又は偽造ログを作成するために、TA 持続時間を改変する。
直接脅かされる資産(完全性): TA 持続時間。
間接的に脅かされる資産:TA データと鍵(機密性、完全性)。
適用上の注釈:
攻撃は、例えば、REE を用いるフラッシュからの TA 持続時間のバックアップの実行と後でのそれのレストア、クロックカウンタの改変、又はクロック電源供給の除去、から構成される。

4.3.3 TEE Debug PP モジュール

T.ABUSE_DEBUG

攻撃者は、機微なデータを入手したり、TSF を危殆化したりする(セキュリティサービスを迂回、不活性化又は変更) ことを攻撃者に許すような、TEE デバッグ機能へのアクセスを許可されるようにする。

直接脅かされる資産:TEE 初期化コードとデータ(完全性)、TEE ランタイムデータ(機密性、完全性)、RNG(機密性、完全性)、TA コード(真正性、一貫性)。
間接的に脅かされる資産: TA データと鍵(機密性、真正性、一貫性) インスタンス時間を含む。
適用上の注釈:
識別フェーズ中、攻撃者は、TEE デバッグモードにアクセスするため、例えば、JTAG インタフェースを悪用することによって脆弱性を探索するかもしれない。

4.4 組織のセキュリティ方針

本セクションは、TEE 及び／又は運用環境により実装されなければならない組織のセキュリティ方針を示す。

4.4.1 TEE ベース PP

以下の方針は、あらゆる TEE へ適用する。

OSP.INTEGRATION_CONFIGURATION
デバイス製造者による TEE のインテグレーションと設定は、GlobalPlatform TEE 仕様でセットされた要件を満たし、TOE 評価から発行されたデバイス製造者に対するセキュリティ要件のすべてを記載するような、TEE プロバイダにより定義されるガイドラインに依拠しなければならない(shall)。
適用上の注釈:
セキュリティターゲットは、適用可能な TEE ガイドライン、特に AGD_OPE.1 要件を満たす運用ガイダンスを参照しなければならない(shall)。

OSP.SECRETS
TEE 又は TEE 以外で実行されるその他のあらゆる運用における秘密データの生成、保存、配付、破棄、注入は、これらデータの完全性と機密性を実施しなければならない(shall)。これは、最終利用フェーズの前 (TEE ストレージの信頼の基点等)、又は最終利用フェーズ中 (暗号プライベート鍵又は対称鍵、機密データ等) に注入される秘密データへ適用する。

4.4.2 TEE Time and Rollback PP モジュール

Time and Rollback PP モジュールにおける追加の方針はない。

4.4.3 TEE Debug PP モジュール

TEE Debug PP モジュールにおける追加の方針はない。

4.5 前提条件

本セクションは、TEE 運用環境で保持されるような前提条件について記述する。これらの前提条件は運用環境によって満たさなければならない。

4.5.1 TEE ベース PP

以下の前提条件は、TEE 運用環境において保持される。

A.PROTECTION_AFTER_DELIVERY

配付の後、かつ最終利用フェーズに入る前に、TOE が環境によって保護されると想定される。運用環境で TOE を操作する者は、TEE ガイドライン(例、利用者及び管理者ガイダンス、インストール用証拠資料、パーソナライゼーションガイド) を適用すると想定される。ガイドに含まれる手順の適用に責任を持つ者、及び製品の配付と保護に関与する者は、要求されるスキルを有し、セキュリティ課題を周知していると想定される。

適用上の注釈:

証明書は、ガイドラインが適用されるときのみ有効である。例えば、インストール、プリパーソナライゼーション又はパーソナライゼーションガイドについて、記述されたセットアップ構成又はパーソナライゼーションプロファイルのみが証明書によってカバーされる。

セキュリティターゲットは、適用可能な TEE ガイドライン、特に AGD_OPE.1 要件を満たすような運用ガイダンスを参照しなければならない(shall)。

A.ROLLBACK

TA 開発者が、完全なロールバックに対する TEE 永続的データ、TA データと鍵及び TA コードの保護に依拠しないと想定される。

A.TA_DEVELOPMENT

TA 開発者は、TEE プロバイダによってセットされる TA 開発ガイドラインに適合すると想定される。特に、TA 開発者は、トラステッドアプリケーションの開発中に、以下の原則を考慮すると想定される:

- CA 識別子は、TEE の適用範囲外で、REE によって生成され、管理される。TA は、CA 識別子が本物であると想定してはならない(must not)。
- TA は、任意の CA を通して機微なデータを REE に暴露してはならない(must not) (CA との対話は、認証手段を要求してもよい)。
- TA インスタンスの排他制御下にないメモリへ書き込まれたデータは、次の読出し時に変更されているかもしれない。
- TA インスタンスの排他制御下にないメモリの同じロケーションから 2 回の読出しは、異なる値を返すことが可能である。

4.5.2 TEE Time and Rollback PP モジュール

Time and Rollback PP モジュールにおいて追加の前提条件はない。さらに、TOE が耐ロールバック保護を実施するので、前提条件 A.TA_ROLLBACK は、破棄される。

4.5.3 TEE Debug PP モジュール

TEE Debug PP モジュールにおいて追加の前提条件はない。

5 セキュリティ対策方針

5.1 TOE のセキュリティ対策方針

本セクションは、TEE のセキュリティ対策方針について述べる。ソフトウェアとハードウェアのメカニズム間のセキュリティ機能の実現の必須の分割はないので、対策方針は脅威の目標に近く、任意の実装を許可する。

5.1.1 TEE ベース PP

以下のセキュリティ対策方針は、あらゆる TEE に適用する。

O.CA_TA_IDENTIFICATION

TEE は、別の常駐するトラステッドアプリケーションによる利用からそれぞれのトラステッドアプリケーションの識別情報を保護し、クライアントアプリケーションをトラステッドアプリケーションから区別するための手段を提供しなければならない(shall)。

適用上の注釈:

クライアントの特性は、リッチ OS 又はトラステッド OS のいずれかにより管理され、これらは、以下の意味で、クライアントが自身の特性を改ざんできないことを保証しなければならない(must):

- TEE 常駐の TA のクライアント識別情報は、トラステッド OS によって常に決定されなければならない(MUST)、また TA か否かの決定は、トラステッド OS 自身と同じように信頼できるものでなければならない(MUST)。
- クライアント識別情報がある TA に一致する時、トラステッド OS は、他のクライアント特性が、対象の TA がトラステッド OS に置く信頼性のレベルと同程度まで、その呼び出す TA の特性と等しいことを保証しなければならない(MUST)。
- クライアント識別情報がある TA に一致しない時、リッチ OS はそのクライアントアプリケーションが自身の特性を改ざんできないことを保証する責任を負う。しかし、本情報はトラステッド OS では信頼されない。

O.KEYS_USAGE

TEE は、暗号鍵において、作成者によって設定される用途制限を実施しなければならない(shall)。

O.TEE_ID

TEE は、TEE 識別子の統計上の一意性を、TEE による生成時に保証しなければならない(shall)。それが改変不可能であり、本識別子を取出す手段の提供についても保証しなければならない(shall)。

適用上の注釈:

TEE 識別子は、TEE 又は TEE 以外によって生成されることが可能である。TEE 識別子が TEE 以外で生成されるとき、TOE 配付前(フェーズ 3 又は 5)に、かつこの対策方針によってカバーされないが、識別子の一意性を保証するための組織のプロセスが存在しなければならない(shall)。

O.INITIALIZATION

TEE は、以下を保証するセキュアな初期化プロセスを通して開始されなければならない(shall):

- TEE ファームウェアのロードに利用される TEE 初期化コードとデータの完全性
- TEE ファームウェアの真正性

- 及び TEE のデバイス SoC への結合。特に、TEE はダウングレード攻撃から TEE ファームウェアを保護しなければならない(shall)。

適用上の注釈:

プロセスが SoC に結合されるという事実は、TEE データの信頼の基点が改変又は改ざんできないことを意味する(参照、[SA])。

O.INSTANCE_TIME

TEE は、TA インスタンス時間を提供し、この時間が TA インスタンスライフタイム中ーTA インスタンス生成から TA インスタンス破棄までーにモノトニックであること、及び低電力状態を通して遷移によって影響されないことを保証しなければならない(shall)。

O.OPERATION

TEE は、そのセキュリティ機能の正しい運用を保証しなければならない(shall)。特に TEE は、以下でなければならない(shall)

- プログラマのエラー、又は REE(及び間接的に CA)又は TA による良好な実践の違反によって生じる異常な状況に対して、自身を保護すること
- REE と TA によるサービスへのアクセスを制御すること:TEE は、REE 又は TA のいずれかから要求されるあらゆる運用の有効性を TEE への任意のエントリポイントでチェックしなければならない(shall)
- 故障検出時に、あらゆる機微なデータの暴露なく、セキュアな状態に入ること

適用上の注釈:

- プログラマのエラー又は良好な実践の違反(例、マルチスレッディングやコンテクスト／セション管理の悪用) は、攻撃-イネイブラとなるかもしれない。REE は、有害であるかもしれないが、『実装(TEE)は、まだ TEE の安定性とセキュリティを保証する』(参照、[CAPI])。いずれにせよ、トラステッドアプリケーションは、実装により実施されるセキュリティ境界を回避する目的でプログラマのエラーを利用可能であってはならない(MUST NOT) (参照、[IAPI]及び[SA])
- エントリポイント(参照、[SA]):REE のソフトウェアは、TEE 機能又はトラステッドコアフレームワークを直接呼び出すことができてはならない(must not)。REE ソフトウェアは、トラステッド OS 又はトラステッドアプリケーションが、REE ソフトウェアに要求された操作の許容可能性の検証を実行するように、プロトコルを通して行わなければならない(must)。

O.RNG

TEE は、乱数生成の暗号品質を保証しなければならない(shall)。乱数は、予測不可能でなければならなず(shall)、かつ十分なエントロピーを備えなければならない(shall)。

適用上の注釈:

乱数生成は、ハードウェア及び／又はソフトウェアのメカニズムを組み合わせてもよい。

RNG 機能は、TEE 識別子が TEE 以外で生成されない場合、この識別子の生成にも使用される。

O.RUNTIME_CONFIDENTIALITY

TEE は、機密の TEE ランタイムデータと TA データと鍵が許可されない暴露から保護されることを保証しなければならない(shall)。特に、

- TEE は、機微なデータ、乱数、又は秘密鍵を REE にエクスポートしてはならない(shall not)。

- TEE は、機微なデータ、乱数、又は秘密鍵へのアクセスを許可された TA だけに許可しなければならない(shall)。
- TEE は、機微な資源を、その価値がもはや不要であると決定したら直ちに消去しなければならない(shall)。

O.RUNTIME_INTEGRITY

TEE は、TEE ファームウェア、TEE ランタイムデータ、TA コード及び TA データと鍵が、揮発性メモリに保存される時、実行時の許可されない改変から保護されることを保証しなければならない(shall)。

O.TA_AUTHENTICITY

TEE は、トラステッドアプリケーションのコード真正性を検証しなければならない(shall)。

適用上の注釈:

TA コードの真正性の検証は、TEE ファームウェアの検証と共に実行されることができる。ただし、その両方が一緒にバンドルされるか、又は揮発性メモリ内でのコードのロード中に限る。

O.TA_ISOLATION

TEE は、TA を相互に分離しなければならない:それぞれの TA は、その TA のすべてのインスタンス間で共有されるが、他の TA の空間から分離されるような、それ自身の実行とストレージの空間をアクセスしなければならない(shall)。

適用上の注釈:

本対策方針は、TEE の機密性と完全性の実施に寄与する。

O.TEE_DATA_PROTECTION

TEE は、TEE 永続的データの真正性、一貫性及び機密性を保証しなければならない(shall)。

O.TEE_ISOLATION

TEE は、REE 及び TA が TEE 自身の実行とストレージの空間と資源をアクセスすることを防止しなければならない(shall)。

適用上の注釈:

本対策方針は、TEE の正しい実行の実施に寄与する。資源割当ては、使用中の TEE 資源と REE/TA 間の隔離を壊さない限り、実行時に変更することができることに留意されたい。

O.TRUSTED_STORAGE

TEE は、以下のように、永続的な TA 汎用データと鍵材料のためのトラステッドストレージサービスを提供しなければならない(shall):

- 保存データと鍵の機密性が実施される
- 保存データと鍵の真正性が実施される
- それぞれの TA 保存データと鍵の一貫性が実施される
- ストレージを改変するような操作の原子性が実施される。

TEE トラステッドストレージはホストデバイスに結び付けられなければならない(shall)。それは、データが生成された時と同じ TEE とデバイス上で動作している許可された TA によってのみ、ストレージ空間がアクセス可能又は改変可能でなければならない(must) ことを意味する。

下表は、どのセキュリティ対策方針が不揮発性メモリ及び／又は揮発性メモリ内に保存される資産に関連するかを要約する。

資産	不揮発性メモリ内	揮発性メモリ内
TEE ファームウェア	O.INITIALIZATION	O.RUNTIME_INTEGRITY
TEE ランタイムデータ	N/A	O.RUNTIME_INTEGRITY
TA コード	O.TA_AUTHENTICITY	O.RUNTIME_INTEGRITY
TA データと鍵	O.TRUSTED_STORAGE	O.RUNTIME_INTEGRITY
TEE 永続的データ	O.TEE_DATA_PROTECTION	O.TEE_DATA_PROTECTION

5.1.2 TEE Time and Rollback PP モジュール

以下の 2 つの対策方針は、高信頼ストレージ及び TA 持続時間完全性（ロールバック防止特性とも言う）を実装する TEE に適用される。

O.ROLLBACK_PROTECTION

TEE は、以下により、許可されないロールバックを防止しなければならない:

・TEE 永続的データ、TA データもしくは鍵、または TA コードの完全性違反の監視

・セキュリティが常に実現されるための相応の対処

適用上の注釈:

この対策方針は、すでに O.RUNTIME_INTEGRITY、O.TEE_DATA_PROTECTION 及び O.TRUSTED_STORAGE によって要求されているため、完全性、一貫性または真正性を保証するために暗号手段を追加しない。しかし、この対策方針は、TSF が潜在的な完全性違反を能動的に監視し、それが発生した場合に適切な措置を講じなければならないことを要求する。

O.TA_PERSISTENT_TIME

TEE は、TEE リセットを超えて持続する、TA 持続時間を提供しなければならない。TEE は、以下のいずれか一方を保証しなければならない:

・持続時間が、TA のインスタンスによって実行された 2 つの「時間設定」間でモノトニック（単調）である。

・持続時間が、破損の検出により無効になる。

5.1.3 TEE Debug PP モジュール

O.DEBUG

TEE は、TEE デバッグ機能へのアクセスを許可する前に、TEE Debug 管理者を認証しなければならない。

5.2 運用環境のセキュリティ対策方針

本項は、環境に適用されるすべての前提条件及び組織のセキュリティ方針をカバーする、TEE 運用環境の

セキュリティ対策方針を示す。

5.2.1 TEE ベース PP

以下のセキュリティ対策方針は、追加のセキュリティ機能を実装しない TEE 運用環境に適用される。

OE.INTEGRATION_CONFIGURATION

デバイス製造者による TEE の集積及び構成は、TEE プロバイダが定めるガイドラインに依拠しなければならない。ガイドラインは、GlobalPlatform TEE 仕様に規定される要件を満たし、TOE 評価から発行されたデバイス製造者のためのセキュリティ要件についてすべて記載する。

OE.PROTECTION_AFTER_DELIVERY

TOE は、配付後及び最終利用フェーズに入る前に、環境に保護されなければならない。運用環境で TOE を操作する者は、TEE ガイドライン（例、利用者及び管理者ガイダンス、インストールマニュアル、パーソナライゼーションガイド）を適用しなければならない。ガイドに記載される手順適用の責任者、及び製品の配付と保護に関与する者は、要求されている能力を持ち、セキュリティ課題を認識する。

適用上の注釈:

証明書は、ガイドが適用される場合のみ有効である。例えばインストール、プリパーソナライゼーションまたはパーソナライゼーションガイドに関して、証明書が対象とするのは、記述されたセットアップ構成またはパーソナライゼーションプロファイルのみである。

OE.ROLLBACK

TA 開発者は、TEE が TEE 永続的データ、TA データと鍵、及び TA コードの完全なロールバック保護を備えないことを考慮しなければならない。

OE.SECRETS

TEE 外で実行される機密データの管理（例、暗号プライベート鍵、対称鍵、利用者認証データの生成、保存、配布、破壊、製品へのロード）は、これらデータの完全性及び機密性を実施しなければならない。

OE.TA_DEVELOPMENT

TA 開発者は、TEE プロバイダの定める TA 開発ガイドラインに準拠しなければならない。特に、TA 開発者は、トラステッドアプリケーション開発中に以下のセキュリティ勧告を適用しなければならない:

- CA 識別子は、TEE 外で REE により生成及び管理される；TA は、CA 識別子が本物だと想定しない
- TA は、CA を介して機密データを REE に暴露しない（CA との対話は認証手段を要求してもよい）
- TA は、共有バッファに書き込んだデータが後から変更されずに読み出せると想定してはならない(shall not)；TA は、共有バッファから一度だけデータを読み出し、後からそれを検証するべきである(should)
- TA は、共有バッファの内容が一定であることを要求する場合には、その内容を TA インスタンスが所有するメモリにコピーするべきである(should)。

5.2.2 TEE Time and Rollback PP モジュール

ロールバック防止の保護は、TOE によって実施される（参照、O.ROLLBACK_PROTECTION）。今後、本 PP-モジュールが使用される場合、ベース PP の運用環境 OE.ROLLBACK の対策方針は破棄される。

5.2.3 TEE Debug PP モジュール

TEE Debug PP モジュールの運用環境に追加のセキュリティ対策方針はない。

5.3 セキュリティ対策方針根拠

5.3.1 脅威

5.3.1.1 TEE ベース PP

T.ABUSE_FUNCT 以下の対策方針の組み合わせは、機能の乱用に対する保護を保証する:

- O.INITIALIZATION は、TEE セキュリティ機能が正常に初期化されることを保証する
- O.OPERATION は、セキュリティ機能の正常なふるまい及び適切な障害管理を保証する
- O.RUNTIME_CONFIDENTIALITY は、機密データの暴露を防止する
- O.RUNTIME_INTEGRITY は、ランタイムのセキュリティ機能の許可されない改変に対する保護を保証する
- O.TA_AUTHENTICITY は、TA コードの真正性が検証されることを保証する
- O.TEE_DATA_PROTECTION は、TEE に使用されるデータが信頼でき、一貫していることを保証する
- O.TEE_ISOLATION は、TEE と外部（REE 及び TA）の分離を実施する
- O.KEYS_USAGE は、暗号鍵の使用を制御する
- OE.TA_DEVELOPMENT は、許可されないエンティティのリクエストに基づく情報暴露や修正実行の防止を特に意味するような、TA 開発方針を実行する。

T.CLONE 以下の対策方針の組み合わせは、クローニングに対する保護を保証する:

- O.TEE_ID は、重複しない TEE 識別手段を提供する
- O.INITIALIZATION は、TEE とデバイス SoC の結合を保証する
- O.RUNTIME_CONFIDENTIALITY は、機密データ、特に TEE をデバイスに結び付けるために使用される TSF データの暴露を防ぐ
- O.RUNTIME_INTEGRITY は、クローニングの検出もしくは防止に使用されるセキュリティ機能、又はデータの、ランタイムでの許可されない改変を防ぐ
- O.TEE_DATA_PROTECTION は、TEE による、一貫しないもしくは信頼できない TEE データの使用を防ぐ
- O.TRUSTED_STORAGE は、高信頼ストレージがデバイスに結び付けられることを保証し、TEE が一貫しないもしくは信頼できないデータを使用することを防ぐ
- O.RNG は、TEE 識別子が、TOE 内で生成される時に実際に重複しないことを保証する

T.FLASH_DUMP 対策方針 O.TRUSTED_STORAGE は、外部メモリに保存されるデータの機密性を保証する。

T.IMPERSONATION 以下の対策方針の組み合わせは、アプリケーションなりすまし攻撃に対する保護を保証する:

- O.CA_TA_IDENTIFICATION は、クライアントの識別情報の保護、及びクライアントアプリケーションとトラステッドアプリケーションの区別の可能性を保証する
- O.OPERATION は、クライアントのためのふるまいが実行される前に、クライアントの識別情報が検証されることを保証する
- O.RUNTIME_INTEGRITY は、セキュリティ機能のランタイムの許可されない改変を防ぐ

T.ROGUE_CODE_EXECUTION 以下の対策方針の組み合わせは、悪意あるコードのインポートに対する保護を保証する:

- O.INITIALIZATION は、TEE セキュリティ機能が正常に初期化されること、及び TEE ファームウェアの完全性を保証する
- O.OPERATION は、セキュリティ機能の正常なふるまいを保証する
- O.RUNTIME_CONFIDENTIALITY は、TEE のふるまいに影響を与える可能性のある TEE ランタイムデータをカバーする
- O.TA_AUTHENTICITY は、TA コードの真正性が検証されることを保証する
- O.RUNTIME_INTEGRITY は、ランタイムのセキュリティ機能の許可されない改変に対する保護を保証する
- O.TEE_DATA_PROTECTION は、TEE のふるまいに影響を与える可能性のある TEE 永続的データをカバーする
- O.TRUSTED_STORAGE は、コードインポート元のストレージの保護を保証する
- OE.INTEGRATION_CONFIGURATION は、最終利用者フェーズ以外のフェーズにおける外部コードのインポートをカバーする
- OE.PROTECTION_AFTER_DELIVERY は、最終利用者フェーズ以外のフェーズにおける外部コードのインポートをカバーする

T.PERTURBATION 以下の対策方針の組み合わせは、かく乱攻撃に対する保護を保証する:

- O.INITIALIZATION は、TEE セキュリティ機能が正常に初期化されることを保証する
- O.INSTANCE_TIME は、インスタンスタイムスタンプの信頼性を保証する
- O.OPERATION は、セキュリティ機能の正常なふるまい及び適切な障害管理を保証する
- O.RUNTIME_CONFIDENTIALITY は、TEE のふるまいに影響を与える可能性のある TEE ランタイムデータをカバーする
- O.TA_AUTHENTICITY は、TA コードの真正性が検証されることを保証する
- O.RUNTIME_INTEGRITY は、ランタイムのセキュリティ機能の許可されない改変に対する保護を保証する
- O.TA_ISOLATION は、TA の分離を保証する

・O.TEE_DATA_PROTECTION は、TEE のふるまいに影響を与える可能性のある TEE 永続的データをカバーする
・O.TEE_ISOLATION は、TEE と外部（REE 及び TA）の分離を実施する

Time and Rollback PP モジュールに特有の追加根拠：
・O.TA_PERSISTENT_TIME は、永続的なタイムスタンプの信頼性を保証する

T.RAM 以下の対策方針の組み合わせは、RAM 攻撃に対する保護を保証する：
・O.INITIALIZATION は、TEE セキュリティ機能が正常に初期化されること、及び初期化プロセスが REE から保護されることを保証する
・O.RUNTIME_CONFIDENTIALITY は、ランタイムの機密データの暴露を防ぐ
・O.RUNTIME_INTEGRITY は、ランタイムのコード及びデータの許可されない改変を保護する
・O.TA_ISOLATION は、TA 間のメモリバリアを提供する
・O.TEE_ISOLATION は、TEE と REE 間のメモリバリアを提供する

T.RNG 以下の対策方針の組み合わせは、乱数生成器の保護を保証する：
・O.INITIALIZATION は、TEE セキュリティ機能、特に RNG の正常な初期化を保証する
・O.RNG は、乱数が予測不可能で、十分なエントロピーを備え、暴露されないことを保証する
・O.RUNTIME_CONFIDENTIALITY は、機密データが暴露されないことを保証する
・O.RUNTIME_INTEGRITY は、RNG の出力実施などの許可されない改変に対する保護を保証する

T.SPY 以下の対策方針の組み合わせは、暴露に対する保護を保証する：
・O.RUNTIME_CONFIDENTIALITY は、ランタイムの機密データの保護を保証する
・O.TA_ISOLATION は、TA 間の分離を保証する
・O.TEE_ISOLATION は、REE 及び TA が TEE データにアクセスできないことを保証する
・O.TRUSTED_STORAGE は、高信頼ストレージのロケーションに保存されているデータが、TA 所有者にしかアクセスされないことを保証する

T.TEE_FIRMWARE_DOWNGRADE 以下の対策方針の組み合わせは、TEE ファームウェアのダウングレードに対する保護を保証する：
・O.INITIALIZATION は、実行されるファームウェアが、目的のバージョンであることを保証する
・OE.INTEGRATION_CONFIGURATION は、デバイスにインストールされているファームウェアが、目的のバージョンであることを保証する
・OE.PROTECTION_AFTER_DELIVERY は、ファームウェアが配付後に改変されないことを保証する

T.STORAGE_CORRUPTION 以下の対策方針の組み合わせは、不揮発性メモリ内の破損に対する保護を保証する：
・O.OPERATION は、ストレージを含む、TEE セキュリティ機能の正常なふるまいを保証する
・O.TEE_DATA_PROTECTION は、保存されている TEE データが本物で、一貫していることを

保証する

・O.TRUSTED_STORAGE は、TA のストレージの破損の検出を実行する

・O.TA_AUTHENTICITY は、TA コードの真正性が検証されることを保証する

・O.INITIALIZATION は、実行されるファームウェアが、目的のバージョンであることを保証する

・OE.ROLLBACK は、TSF に実施される特性の制限を規定する

Time and Rollback PP モジュールに特有の根拠:

・脅威 T.STORAGE_CORRUPTION は、OE.ROLLBACK ではなく、O.ROLLBACK_PROTECTION に関連付けられる。

5.3.1.2 TEE Time and Rollback PP モジュール

T.ROLLBACK 対策方針 O.ROLLBACK_PROTECTION は、ロールバック攻撃に対する保護を保証する。

T.TA_PERSISTENT_TIME_ROLLBACK 対策方針 O.TA_PERSISTENT_TIME は、修正検出時の持続タイムスタンプのモノトニシティ(単調性)及び障害管理を保証する。

5.3.1.3 TEE Debug PP モジュール

T.ABUSE_DEBUG 以下の対策方針は、デバッグ機能の乱用に対する保護を保証する:

・O.DEBUG は、TEE デバッグ機能へのアクセスを許可する前の TEE デバッグ管理者の認証を保証する。

5.3.2 組織のセキュリティ方針

5.3.2.1 TEE ベース PP

OSP.INTEGRATION_CONFIGURATION 対策方針 OE.INTEGRATION_CONFIGURATION は、本 OSP を直接カバーする。

OSP.SECRETS 対策方針 OE.SECRETS は、本 OSP を直接カバーする。

5.3.3 前提条件

5.3.3.1 TEE ベース PP

A.PROTECTION_AFTER_DELIVERY 対策方針 OE.PROTECTION_AFTER_DELIVERY は、この前提条件を直接カバーする。

A.ROLLBACK 対策方針 OE.ROLLBACK は、この前提条件を直接カバーする。

Time and Rollback PP モジュールに特有の根拠：この前提条件は、Time and Rollback PP モジュールを実装する TEE には適用されない。

A.TA_DEVELOPMENT 対策方針 OE.TA_DEVELOPMENT は、この前提条件を直接カバーする。

5.3.4 SPD とセキュリティ対策方針

脅威	セキュリティ対策方針	根拠
T.ABUSE_FUNCT	O.INITIALIZATION, O.OPERATION, O.RUNTIME_CONFIDENTIALITY, O.RUNTIME_INTEGRITY, O.TEE_DATA_PROTECTION, O.TEE_ISOLATION, OE.TA_DEVELOPMENT, O.KEYS_USAGE, O.TA_AUTHENTICITY	2.3.1 項
T.CLONE	O.TEE_ID, O.INITIALIZATION, O.RUNTIME_CONFIDENTIALITY, O.RUNTIME_INTEGRITY, O.TEE_DATA_PROTECTION, O.TRUSTED_STORAGE, O.RNG	2.3.1 項
T.FLASH_DUMP	O.TRUSTED_STORAGE	2.3.1 項
T.IMPERSONATION	O.CA_TA_IDENTIFICATION, O.OPERATION, O.RUNTIME_INTEGRITY	2.3.1 項
T.ROGUE_CODE_EXECUTION	O.OPERATION, O.RUNTIME_CONFIDENTIALITY, O.RUNTIME_INTEGRITY, O.TEE_DATA_PROTECTION, O.TRUSTED_STORAGE, OE.INTEGRATION_CONFIGURATION, OE.PROTECTION_AFTER_DELIVERY, O.TA_AUTHENTICITY, O.INITIALIZATION	2.3.1 項
T.PERTURBATION	O.INITIALIZATION, O.INSTANCE_TIME, O.OPERATION, O.RUNTIME_CONFIDENTIALITY, O.RUNTIME_INTEGRITY, O.TA_ISOLATION, O.TA_PERSISTENT_TIME, O.TEE_DATA_PROTECTION, O.TEE_ISOLATION, O.TA_AUTHENTICITY	2.3.1 項
T.RAM	O.INITIALIZATION,	2.3.1 項

脅威	セキュリティ対策方針	根拠
	O.RUNTIME_CONFIDENTIALITY, O.RUNTIME_INTEGRITY, O.TA_ISOLATION, O.TEE_ISOLATION	
T.RNG	O.INITIALIZATION, O.RNG, O.RUNTIME_CONFIDENTIALITY, O.RUNTIME_INTEGRITY	2.3.1 項
T.SPY	O.RUNTIME_CONFIDENTIALITY, O.TA_ISOLATION, O.TEE_ISOLATION, O.TRUSTED_STORAGE	2.3.1 項
T.TEE_FIRMWARE_DOWNGRADE	O.INITIALIZATION, OE.INTEGRATION_CONFIGURATION, OE.PROTECTION_AFTER_DELIVERY	2.3.1 項
T.STORAGE_CORRUPTION	O.OPERATION, O.ROLLBACK_PROTECTION, OE.ROLLBACK, O.TEE_DATA_PROTECTION, O.TRUSTED_STORAGE, O.TA_AUTHENTICITY, O.INITIALIZATION	2.3.1 項
T.ROLLBACK	O.ROLLBACK_PROTECTION	2.3.1 項
T.TA_PERSISTENT_TIME_ROLLBACK	O.TA_PERSISTENT_TIME	2.3.1 項
T.ABUSE_DEBUG	O.DEBUG	2.3.1 項

表 5: 脅威とセキュリティ対策方針 – カバレージ

セキュリティ対策方針	脅威
O.CA_TA_IDENTIFICATION	T.IMPERSONATION
O.KEYS_USAGE	T.ABUSE_FUNCT
O.TEE_ID	T.CLONE
O.INITIALIZATION	T.ABUSE_FUNCT, T.CLONE, T.ROGUE_CODE_EXECUTION, T.PERTURBATION, T.RAM, T.RNG, T.TEE_FIRMWARE_DOWNGRADE, T.STORAGE_CORRUPTION
O.INSTANCE_TIME	T.PERTURBATION
O.OPERATION	T.ABUSE_FUNCT, T.IMPERSONATION, T.ROGUE_CODE_EXECUTION, T.PERTURBATION, T.STORAGE_CORRUPTION
O.RNG	T.CLONE, T.RNG
O.RUNTIME_CONFIDENTIALITY	T.ABUSE_FUNCT, T.CLONE, T.ROGUE_CODE_EXECUTION, T.PERTURBATION, T.RAM, T.RNG, T.SPY
O.RUNTIME_INTEGRITY	T.ABUSE_FUNCT, T.CLONE, T.IMPERSONATION, T.ROGUE_CODE_EXECUTION, T.PERTURBATION, T.RAM, T.RNG
O.TA_AUTHENTICITY	T.ABUSE_FUNCT, T.ROGUE_CODE_EXECUTION, T.PERTURBATION, T.STORAGE_CORRUPTION
O.TA_ISOLATION	T.PERTURBATION, T.RAM, T.SPY
O.TEE_DATA_PROTECTION	T.ABUSE_FUNCT, T.CLONE, T.ROGUE_CODE_EXECUTION, T.PERTURBATION, T.STORAGE_CORRUPTION
O.TEE_ISOLATION	T.ABUSE_FUNCT, T.PERTURBATION, T.RAM, T.SPY
O.TRUSTED_STORAGE	T.CLONE, T.FLASH_DUMP, T.ROGUE_CODE_EXECUTION, T.SPY, T.STORAGE_CORRUPTION
O.ROLLBACK_PROTECTION	T.STORAGE_CORRUPTION, T.ROLLBACK
O.TA_PERSISTENT_TIME	T.PERTURBATION, T.TA_PERSISTENT_TIME_ROLLBACK
O.DEBUG	T.ABUSE_DEBUG
OE.INTEGRATION_CONFIGURATION	T.ROGUE_CODE_EXECUTION, T.TEE_FIRMWARE_DOWNGRADE
OE.PROTECTION_AFTER_DELIVERY	T.ROGUE_CODE_EXECUTION, T.TEE_FIRMWARE_DOWNGRADE

セキュリティ対策方針	脅威
OE.ROLLBACK	T.STORAGE_CORRUPTION
OE.SECRETS	
OE.TA_DEVELOPMENT	T.ABUSE_FUNCT

表 6：セキュリティ対策方針と脅威 – カバレージ

組織のセキュリティ方針	セキュリティ対策方針	根拠
OSP.INTEGRATION_CONFIGURATION	OE.INTEGRATION_CONFIGURATION	2.3.2 項
OSP.SECRETS	OE.SECRETS	2.3.2 項

表 7：OSP とセキュリティ対策方針 – カバレージ

セキュリティ対策方針	組織のセキュリティ方針
O.CA_TA_IDENTIFICATION	
O.KEYS_USAGE	
O.TEE_ID	
O.INITIALIZATION	
O.INSTANCE_TIME	
O.OPERATION	
O.RNG	
O.RUNTIME_CONFIDENTIALITY	
O.RUNTIME_INTEGRITY	
O.TA_AUTHENTICITY	
O.TA_ISOLATION	
O.TEE_DATA_PROTECTION	
O.TEE_ISOLATION	
O.TRUSTED_STORAGE	
O.ROLLBACK_PROTECTION	
O.TA_PERSISTENT_TIME	
O.DEBUG	
OE.INTEGRATION_CONFIGURATION	OSP.INTEGRATION_CONFIGURATION
OE.PROTECTION_AFTER_DELIVERY	
OE.ROLLBACK	
OE.SECRETS	OSP.SECRETS
OE.TA_DEVELOPMENT	

表 8：セキュリティ対策方針と OSP – カバレージ

前提条件	運用環境のセキュリティ対策方針	根拠
A.PROTECTION_AFTER_DELIVERY	OE.PROTECTION_AFTER_DELIVERY	2.3.3 項
A.ROLLBACK	OE.ROLLBACK	2.3.3 項
A.TA_DEVELOPMENT	OE.TA_DEVELOPMENT	2.3.3 項

表 9: 前提条件と運用環境のセキュリティ対策方針 ー カバレージ

運用環境のセキュリティ対策方針	前提条件
OE.INTEGRATION_CONFIGURATION	
OE.PROTECTION_AFTER_DELIVERY	A.PROTECTION_AFTER_DELIVERY
OE.ROLLBACK	A.ROLLBACK
OE.SECRETS	
OE.TA_DEVELOPMENT	A.TA_DEVELOPMENT

表 10: 運用環境のセキュリティ対策方針と前提条件 ー カバレージ

6 拡張要件

6.1 拡張ファミリ

6.1.1 拡張ファミリ FCS_RNG - 乱数生成

6.1.1.1 記述

TOE の IT セキュリティ機能要件を定義するため、クラス FCS（暗号サポート）の追加ファミリ（FCS_RNG）がここで定義される。このファミリは、暗号の目的で使用される乱数生成の機能要件を記述する。

このファミリは、暗号目的の使用を意図される乱数生成の品質要件を定義する。

6.1.1.2 拡張コンポーネント

6.1.1.3 拡張コンポーネント FCS_RNG.1

6.1.1.4 *記述*

乱数生成は、乱数が定められた品質メトリックに適合することを要求する。

下位階層：なし。

管理：予見される管理アクティビティはない。

監査：定義される監査事象はない。

6.1.1.5 *定義*

FCS_RNG.1 乱数生成

FCS_RNG.1.1 TSF は、[割付：セキュリティ機能リスト]を実装する[選択：物理的、非物理的真性、決定論的、ハイブリッド、ハイブリッド決定論的]乱数生成器を提供しなければならない。

FCS_RNG.1.2 TSF は、[割付：定義された品質メトリック]に適合する乱数を提供する。

依存性：なし

6.1.2 拡張ファミリ FPT_INI – TSF 初期化

6.1.2.1 記述

TOEのセキュリティ機能要件を定義するため、クラスFPT（TSFの保護）の追加ファミリ（FPT_INI）がここで紹介される。このファミリは、正しくセキュアな運用状態での初期化を保証するTOEの専用機能による、TSF初期化の機能要件を記述する。

このファミリTSF初期化（FPT_INI）は以下の通り規定される。

6.1.2.2 拡張コンポーネント

6.1.2.3 拡張コンポーネント FPT_INI.1

6.1.2.4 *記述*

FPT_INI.1は、TOEに対し、電源投入時にTSFをセキュアな運用状態に持っていくTSF初期化機能を提供することを要求する。

下位階層：なし

管理：予見される管理アクティビティはない。

監査：定義される監査事象はない。

6.1.2.5 *定義*

FPT_INI TSF初期化

FPT_INI.1.1 TOE初期化機能は、セキュアな初期化状態でTSFを確立する前に、以下を検証しなければならない：

- ・TEE初期化コード及びデータの完全性
- ・TEEファームウェアの真正性及び完全性
- ・ストレージの信頼の基点の完全性
- ・TEE識別データの完全性
- ・旧バージョンへのダウングレードを防ぐファームウェアのバージョン
- ・[割付：実装依存検証リスト]

FPT_INI.1.2 TOE初期化機能は、TOEが正常に初期化を完了するか、または停止できるように、初期化中のエラー及び障害を検出し、それに対処しなければならない。

FPT_INI.1.3 TOE初期化機能は、TOE初期化の完了後に、TSFと任意に対話してはならない。

依存性：なし

6.1.3 拡張ファミリ AVA_TEE – TEE の脆弱性分析

6.1.3.1 記述

TEE 脆弱性分析は、TEE で特定された潜在的脆弱性によって、攻撃者が SFR を侵害し、データもしくは機能への許可されないアクセスや改変を実行することが可能になるかどうかを決定するための評価である。

潜在的脆弱性は、開発、製造もしくは組立環境の評価中、TEE 仕様及びガイダンスの評価中、TEE コンポーネントの予測されるふるまい中、または、例えば統計手法といったその他の手法によって特定される。

ファミリ「TEE の脆弱性分析（AVA_TEE）」は、評価者から独立した脆弱性調査及び TEE の侵入テストの要件を定義する。

新しいファミリの主な特徴は、AVA_VAN とほぼ同じだが、附属書 A.1 に定められる TEE 特有の攻撃能力規模を紹介することである。この附属書は、TEE 攻撃能力計算表と TEE 特有の攻撃法カタログも提供する。PP の本バージョンでは、TEE 特有の攻撃能力規模に関する 1 つのレベルだけ、つまり TEE-Low が、コンポーネント AVA_TEE.2 で使用される。

ファミリ AVA_VAN と比較すると、このファミリの標準コンポーネント AVA_VAN.2 は、例えば、制御されていないアプリケーションストアを介して拡散し、既知の SW 脆弱性を悪用するモバイルアプリケーションマルウェアといった、TEE の SW のみの攻撃に対し、優れた保証レベルを提供する。このようなマルウェアは、通常は REE セキュリティを破ることができるため、TEE がこの攻撃に対抗しなければならない。AVA_VAN.2 は、最終利用者が攻撃することに興味を持たない可能性のあるサービスに関連する、例えば企業デバイスの艦隊、といった制御された環境内で管理されるデバイスに最も適する。

この AVA_TEE.2 の TEE 特有の攻撃能力規模の選択は、高くつく脆弱性の特定から生じうる、容易に拡散する攻撃に対する追加の保護保証が動機付けとなる。このような攻撃経路は、モバイルデバイスに対して使用された事例があり、予想投資利益率が高く、最終利用者が悪用実行に興味を持つゲームコンソールや TV ボックスなどの市場分野でよく見られる。この目的を達成するために、AVA_TEE.2 は、攻撃の見積表を識別フェーズと悪用フェーズに 2 分割し（スマートカードの場合と同様に）、攻撃能力 TEE-Low（スマートカードの評価表の拡張基本レベルに相当する）について定義する。

ファミリ「TEE の脆弱性分析（AVA_TEE）」は以下の通り定義される。AVA_VAN.2 からの変更部分は下線を引き、追跡しやすくなっている。

6.1.3.2 拡張コンポーネント

6.1.3.3 拡張コンポーネント AVA_TEE.2

6.1.3.4 *記述*

脆弱性分析は、評価者により潜在的脆弱性の存在を突き止めるために実行される。

評価者は、TEE の運用環境で潜在的脆弱性が悪用できないことを確認するため、TEE に侵入テストを実

行する。侵入テストは、攻撃能力が TEE-Low であるという前提条件のもと、評価者により実行される。

6.1.3.5 *定義*

AVA_TEE.2 TEE 脆弱性分析

AVA_TEE.2.1D 開発者は、テストのための TOE を提供しなければならない。

AVA_TEE.2.1C TOE は、テストに適していなければならない。

AVA_TEE.2.1E 評価者は、提供された情報が、証拠の内容と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。

AVA_TEE.2.2E 評価者は、TOE の潜在的脆弱性を識別するため、公知の情報源の探索を実行しなければならない。

AVA_TEE.2.3E 評価者は、TOE の潜在的脆弱性を識別するために、ガイダンス証拠資料、機能仕様、TOE 設計、及びセキュリティアーキテクチャ記述を使用して、TOE の独立脆弱性分析を実行しなければならない。

AVA_TEE.2.4E 評価者は、TEE-Low の攻撃能力を持つ攻撃者からの攻撃に TOE が耐えられることを決定するために、識別された潜在的脆弱性に基づいて侵入テストを実施しなければならない。

依存性: ADV_ARC.1 セキュリティアーキテクチャ記述
ADV_FSP.2 セキュリティ実施機能仕様
ADV_TDS.1 基本設計
AGD_OPE.1 利用者操作ガイド
AGD_PRE.1 準備手続き

7 セキュリティ要件

本章は、TEE 及びその運用環境によって対処されるセキュリティ課題について説明する。運用環境は、TEE インテグレーション及びメンテナンス環境、並びに TA 開発環境を意味する。セキュリティ課題は、TEE が使用できるデバイスがこの分野で遭遇する可能性のある脅威、運用環境における前提条件、及び TEE によってもしくは運用環境内で実装されなければならない組織の方針で構成される。

7.1 セキュリティ機能要件

本章は、TOE がセキュリティ対策方針を達成するために実行しなければならない、セキュリティ機能要件（SFR）のセットについて規定する。

7.1.1 TEE ベース PP

本 PP は、CC パート 2[CC2]で定義される以下のセキュリティ機能コンポーネントを使用する：

- FAU_ARP.1 Security alarms（セキュリティアラーム）
- FAU_SAR.1 Audit review（監査レビュー）
- FAU_STG.1 Audit event storage（監査証跡格納）
- FCS_COP.1 Cryptographic operation（暗号操作）
- FIA_ATD.1 User attribute definition（利用者属性定義）
- FIA_UID.2 User identification before any action（アクション前の利用者識別）
- FIA_USB.1 User-subject binding（利用者-サブジェクト結合）
- FDP_ACC.1 Subset access control（サブセットアクセス制御）
- FDP_ACF.1 Security attribute based access control（セキュリティ属性によるアクセス制御）
- FDP_IFC.2 Complete information flow control（完全情報フロー制御）
- FDP_IFF.1 Simple security attributes（単純なセキュリティ属性）
- FDP_ITT.1 Basic internal transfer protection（基本内部転送保護）
- FDP_RIP.1 Subset residual information protection（サブセット残存情報保護）
- FDP_ROL.1 Basic rollback（基本ロールバック）
- FDP_SDI.2 Stored data integrity monitoring and action（蓄積データ完全性監視及びアクション）
- FMT_MSA.1 Management of security attributes（セキュリティ属性の管理）
- FMT_MSA.3 Static attribute initialization（静的属性初期化）
- FMT_SMR.1 Security roles（セキュリティ役割）
- FMT_SMF.1 Management functions（管理機能）
- FPT_FLS.1 Failure with preservation of secure state（セキュアな状態を保持する障害）
- FPT_ITT.1 Basic internal TSF data transfer protection（基本 TSF 内データ転送保護）
- FPT_STM.1 Reliable time stamps（高信頼タイムスタンプ）
- FPT_TEE.1 Testing of external entities（外部エンティティのテスト）

さらに、第 6 章で定義された以下の拡張セキュリティ機能コンポーネントが使用される:

・FCS_RNG.1　Random numbers generation（乱数生成）
・FPT_INI.1　TSF initialisation（TSF 初期化）

セキュリティ機能要件のステートメントは、利用者、サブジェクト、オブジェクト、情報、利用者データ、TSF データ、操作及びそのセキュリティ属性（これらの定義については CC パート 1[CC1]参照）について、TEE の以下の特徴に依拠する。

利用者は、TOE 範囲外のエンティティを意味する:

・クライアントアプリケーション（CA）、セキュリティ属性は「CA_identity」（CA 識別子）
・トラステッドアプリケーション（TA）、セキュリティ属性が「TA_identity」（TA 識別子）、「TA_properties」

サブジェクトは、TOE 範囲の能動的エンティティを意味する:

・S.TA_INSTANCE：任意の TA インスタンス、セキュリティ属性は「TA_identity」（TA 識別子）
・S.TA_INSTANCE_SESSION：所与の TA インスタンス内の任意のセション、セキュリティ属性は「client_identity」（CA 識別子）
・S.API：TEE 内部 API、セキュリティ属性は「caller」（TA 識別子）
・S.RESOURCE：TEE または REE により二者択一的に使用されるソフトウェアまたはハードウェアコンポーネント、セキュリティ属性は「state」（TEE/REE）。例えば、暗号アクセラレータ、乱数生成器、キャッシュ、レジスタ。注釈：状態が REE である場合、TEE はリソースにアクセスしてもよい。通信バスはサブジェクトとみなされない（FDP_ITT.1 参照）
・S.RAM_UNIT：RAM アドレス指定が可能なユニット、セキュリティ属性は「right」（TA 識別子/REE）->（Read/Write/ReadWrite/NoAccess）。例えば、TA インスタンス生成時、またはクライアント（CA、TA）とTA 間で共有メモリが参照される場合に、アドレス指定が可能なユニットを割り当ててよい、またはそのアクセス権を変更してもよい。注釈：1) RAM_UNIT は通常 C 言語のあるバイトを意味する；2) TEE 自体に適用される RAM アクセス制限はない
・S.COMM_AGENT：REE の CA と TEE 及びその TA 間のプロキシ

オブジェクトは、TOE 範囲内の受動的エンティティを意味する:

・OB.TA_STORAGE（利用者データ）：TA の高信頼ストレージ空間、セキュリティ属性は「owner」（TA 識別子）、「inExtMem」（True/False）、「TEE_identity」（TEE 識別子）
・OB.SRT（TSF データ）：TEE ストレージの信頼の基点、セキュリティ属性は「TEE_identity」（TEE 識別子）

暗号オブジェクトは、TEE オブジェクトの特殊な種別である:

・OB.TA_KEY（利用者データ）：（永続的または一時的）利用者鍵（に対する処理）、セキュリティ属性は「usage」、「owner」（TA 識別子）、「isExtractable」（True/False）

情報は、サブジェクト間で交換されるデータを意味する:

・I.RUNTIME_DATA（所有者に依存する利用者データまたは TSF データ）：TA または TEE 自体に属す

るデータ。パラメタ値、戻り値、メモリ領域内の平文の内容を意味する。注釈:暗号化及び認証されるデータは、I.RUNTIME_DATA とみなされない。

TSF データは、セキュリティサービスの提供に必要なランタイム TSF データ及び TSF 永続的データ(TEE 永続的データとも言う)で構成される。それには、利用者セキュリティ属性、サブジェクト、オブジェクト及び情報がすべて含まれる。

TA_INSTANCE の代わりに S.API によって実行される利用者鍵に対する暗号操作:

・OP.USE_KEY:鍵を使用する暗号操作
・OP.EXTRACT_KEY:鍵を配置する操作

TA_INSTANCE の代わりに S.API によって実行される高信頼ストレージの操作:

・OP.LOAD:TA が使用する永続的オブジェクト(データと鍵)を取り戻すために使用される操作
・OP.STORE:永続的オブジェクト(データと鍵)を保存するために使用される操作。オブジェクト生成、オブジェクト削除、オブジェクト名の変更、オブジェクトトランケーション及びオブジェクトへの書き込みを意味する

その他の操作:

・TA_INSTANCE の代わりに TEE によって実行される操作

本 PP は、以下のアクセス制御及び情報フローのセキュリティ機能方針(SFP)を定義する:

ランタイムデータ情報フロー制御 SFP:

・目的:実行可能なエンティティ及びメモリ間のランタイムデータのフローを制御すること。この方針は、ランタイムデータの完全性及び機密性の保証に寄与する
・サブジェクト:S.TA_INSTANCE、S.TA_INSTANCE_SESSION、S.API、 S.COMM_AGENT、S.RESOURCE、S.RAM_UNIT
・情報:I.RUNTIME_DATA
・セキュリティ属性:S.RESOURCE.state、S.RAM_UNIT.rights、S.API.caller
・SFR インスタンス:FDP_IFC.2/Runtime、FDP_IFF.1/Runtime、FDP_ITT.1/Runtime

TA 鍵アクセス制御 SFP:

・目的:TA 鍵へのアクセスを制御すること。アクセスは鍵を所有する TA にだけ許可される。この方針は TA 鍵の機密性に寄与する。
・サブジェクト:S.API、S.TA_INSTANCE 及び TEE のその他のサブジェクト
・オブジェクト:OB.TA_KEY
・セキュリティ属性:OB.TA_KEY.usage、OB.TA_KEY.owner、OB.TA_KEY.isExtractable、S.API.caller
・操作:OP.USE_KEY、OP.EXTRACT_KEY
・SFR インスタンス:FDP_ACC.1/TA_Keys、FDP_ACF.1/TA_keys、FMT_MSA.1/TA_keys、FMT_MSA.3/TA_keys、FMT_SMF.1

高信頼ストレージアクセス制御 SFP:

- 目的:永続的 TA データ及び鍵が保存されている TA ストレージへのアクセスを制御すること。アクセスは所有者 TA の代理にだけ許可される。またこの方針は、TA 高信頼ストレージと TEE ストレージの信頼の基点 OB.SRT の結合を実行する。
- サブジェクト:S.API
- オブジェクト:OB.TA_STORAGE、OB.SRT
- セキュリティ属性:S.API.caller、OB.TA_STORAGE.owner、OB.TA_STORAGE.inExtMem、OB.TA_STORAGE.TEE_identity、OB.SRT.TEE_identity
- 操作:OP.LOAD、OP.STORE
- SFR インスタンス:FDP_ACC.1/Trusted Storage、FDP_ACF.1/Trusted Storage、FDP_ROL.1/Trusted Storage、FMT_MSA.1/Trusted Storage、FMT_MSA.3/Trusted Storage、FMT_SMF.1

適用上の注釈:セキュリティターゲット作成者は、SFR のオープンな割付を埋め、製品に適する選択を実行しなければならない。TOE サマリ仕様(TSS)は、インスタンス化された要件を製品がどのように実装するのかを記述しなければならない。要件は、サポートするセキュリティ機能を意味する可能性があることに留意されたい。例えば:

- 外部メモリに配置されたストレージ空間の認証/署名及び暗号化/復号(FDP_ACF.1/高信頼ストレージ参照)
- CA と TA セションの結合(FIA_USB.1 参照)
- クライアントが TA である場合の client_identity の検証(FIA_USB.1 参照)
- 高信頼ストレージとストレージの信頼の基点 OB.SRT の結合(FDP_ACF.1/高信頼ストレージ参照)
- REE と共有される TEE リソースの構成(FDP_IFF.1/ランタイム参照)
- セキュアな状態の定義及び障害管理によるプロセス開始(FPT_FLS.1 参照)

7.1.1.1 識別

FIA_ATD.1 利用者属性定義

FIA_ATD.1.1 TSF は、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない:**CA_identity、TA_identity、TA_properties、[割付:セキュリティ属性のリスト]**。

適用上の注釈:

このようなリストの属性のライフスパンは以下の通りである:

- CA_identity:この属性のライフタイムは、TA に対するクライアントセションのライフタイムである
- TA_identity:この属性の可用性は、クライアントに対する TA の可用性であり、さらにシステム内の TA プレゼンスによって制限される
- TA_properties:この属性のライフタイムは、クライアントに対する TA の可用性であり、さらにシステム内の TA プレゼンスによって制限される

FIA_UID.2 アクション前の利用者識別

FIA_UID.2.1 TSFは、その利用者を代行する他のTSF仲介アクションを許可する前にも、各利用者に識別が成功することを要求しなければならない。

適用上の注釈:

利用者はクライアントアプリケーションまたはトラステッドアプリケーションを意味する。

FIA_USB.1 利用者-サブジェクト結合

FIA.USB.1.1 TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない:

- **クライアント(CA または TA)識別情報は、要求された TA セションの client_identity に成文化される**
- **[割付:利用者セキュリティ属性のリスト] 。**

FIA.USB.1.2 TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない:

- **クライアントが TA の場合、client_identity は、クライアントである TA サブジェクトの TA_identity と等しくなければならない**
- **[割付:属性の最初の関連付けの規則] 。**

FIA.USB.1.3 TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない:

- **初期化後に client_identity の改変は一切許可されない**
- **[割付:属性の変更の規則] 。**

適用上の注釈:

TEE 内部 API は、CA 識別情報の成文化規則を定義する。

FMT_SMR.1 セキュリティの役割

FMT_SMR.1.1 TSF は、以下の役割を維持しなければならない:

- **TSF**
- **TA_User**
- **[割付:許可された識別された役割] 。**

FMT_SMR.1.2 TSF は、利用者を役割に関連付けられなければならない。

適用上の注釈:

TA_Userの役割は、REE（クライアントアプリケーションによる）または他のTAのリクエストに基づいて、TAを代行して動作するTSFである。

7.1.1.2 機密性、完全性及び分離

FDP_IFC.2/Runtime 完全情報フロー制御

FDP_IFC.2.1/Runtime TSFは、以下のサブジェクト、情報、及びSFPによって扱われるサブジェクトに、またはサブジェクトから情報の流れを引き起こすすべての操作に対して、**ランタイムデータ情報フロー制御SFP**を実施しなければならない。

- **サブジェクト：S.TA_INSTANCE、S.TA_INSTANCE_SESSION、S.API、S.COMM_AGENT、S.RESOURCE、S.RAM_UNIT**
- **情報：I.RUNTIME_DATA**

FDP_IFC.2.2/Runtime TSFは、TOEのどのサブジェクトに、及びどのサブジェクトから、TOEの何らかの情報の流れを引き起こすすべての操作が、情報フロー制御SFPによって取り扱われることを保証しなければならない。

適用上の注釈：

フロー制御方針は、1つのサブジェクトから別のサブジェクトへのランタイムデータの通信条件を特定する。それは、これらのサブジェクトの標準インタフェースである操作に適用される。

FDP_IFF.1/Runtime 単純セキュリティ属性

FDP_IFF.1.1/Runtime TSFは、以下のタイプのサブジェクト及び情報セキュリティ属性に基づいて、**ランタイムデータ情報フロー制御SFP**を実施しなければならない：**S.RESOURCE.state、S.RAM_UNIT.rights及びS.API.caller**

FDP_IFF.1.2/Runtime TSFは、以下の規則が保持されていれば、制御された操作を通じて、制御されたサブジェクトと制御された情報間の情報フローを許可しなければならない：

- **S.TA_INSTANCEとS.RAM_UNIT間の情報フローの規則：**
  - **S.TA_INSTANCEからS.RAM_UNITへのI.RUNTIME_DATAのフローは、S.RAM_UNIT.rights（S.TA_INSTANCE）がWriteまたはReadWriteの場合のみ許可される**
  - **S.RAM_UNITからS.TA_INSTANCEへのI.RUNTIME_DATAのフローは、S.RAM_UNIT.rights（S.TA_INSTANCE）がReadまたはReadWriteの場合のみ許可される**
- **S.COMM_AGENTから、及びS.COMM_AGENTへの情報フローの規則：**
  - **S.COMM_AGENTからS.RAM_UNITへのI.RUNTIME_DATAのフローは、S.RAM_UNIT.rights（REE）がWriteまたはReadWriteの場合のみ許可される**

- **S.RAM_UNIT から S.COMM_AGENT への I.RUNTIME_DATA のフローは、S.RAM_UNIT.rights（REE）が Read または ReadWrite の場合のみ許可される**

・S.API から、及び S.API への情報フローの規則：

- **S.API から S.RAM_UNIT への I.RUNTIME_DATA のフローは、S.RAM_UNIT.rights（S.API.caller）が Write または ReadWrite の場合のみ許可される**
- **S.RAM_UNIT から S.API への I.RUNTIME_DATA のフローは、S.RAM_UNIT.rights（S.API.caller）が Read または ReadWrite の場合のみ許可される**

・S.RESOURCE から、及び S.RESOURCE への情報フローの規則：

- **S.API と S.RESOURCE 間の I.RUNTIME_DATA のフローは、そのリソースが TEE の制御下にある場合のみ許可される（S.RESOURCE.state = TEE）**

FDP_IFF.1.3/Runtime TSF は、**[割付：追加の情報フロー制御 SFP 規則]** を実施しなければならない。

FDP_IFF.1.4/Runtime TSF は、以下の規則に基づいて、情報フローを明示的に許可しなければならない：

・S.TA_INSTANCE_SESSION から、及び S.TA_INSTANCE_SESSION への情報フローの規則：

- **パラメタまたは戻り値である I.RUNTIME_DATA のフローは、S.TA_INSTANCE_SESSION と S.COMM_AGENT 間で許可される。**
- **パラメタまたは戻り値である I.RUNTIME_DATA のフローは、S.TA_INSTANCE_SESSION と S.API 間で許可される。**

FDP_IFF.1.5/Runtime TSF は、以下の規則に基づいて、情報フローを明示的に拒否しなければならない：**FDP_IFF.1.1/1.2/1.3/1.4 で記述された条件の一つが保持される場合を除く、TEE サブジェクトを関係する任意の情報フロー。**

適用上の注釈：

・S.RAM_UNIT によって管理されるアクセス権設定は、TSF データに使用される RAM アドレス指定が可能なユニットが、適切に保護されること（TEE ファームウェアの完全性、TEE ランタイムデータの完全性及び機密性に関して）を保証しなければならない

・RAM ユニットは、例えばオンチップ RAM、オフチップ RAM、レジスタ等、幾つかの揮発性メモリ内に渡ることができる

・TEE 専用の RAM ユニットは、REE に渡された一時ストレージ参照の内容のコピーを維持してもよい

FDP_ITT.1/Runtime 基本内部転送保護

FDP_ITT.1.1/Runtime TSF は、利用者データが TOE の物理的に分離されたパート間を転送される場合、その暴露及び改変を防ぐための**ランタイムデータ情報フロー制御 SFP** を実施しなければならない。

適用上の注釈：

TEE によって使用されるリソースは、「物理的に分離された部分」に常駐してもよい。この要件は、通信バスを介したデータ転送に対処する（S.RESOURCES はバスを含まないという定義参照）。

FDP_RIP.1/Runtime　サブセット残存情報保護

FDP_RIP.1.1/Runtime　TSF は、以下のオブジェクト**からの資源の割当て解除**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：**TEE 及び TA ランタイムオブジェクト**。

適用上の注釈：

この操作は特に以下の場合に適用される：

・障害検出（FPT_FLS.1 参照）
・TA インスタンス及び TA セションのクローズ

FPT_ITT.1/Runtime　基本 TSF 内データ転送保護

FPT_ITT.1.1/Runtime　TSF は、TSF データが TOE の異なるパーツ間で送られる場合、TSF データを**暴露及び改変**から保護しなければならない。

適用上の注釈：

TEE によって使用されるリソースは、「物理的に分離された部分」に常駐してもよい。

7.1.1.3　暗号

FCS_COP.1　暗号操作

FCS_COP.1.1　TSF は、以下 **[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]**及び暗号鍵長**[割付：暗号鍵長]**に従って、**[割付：暗号操作のリスト]**を実行しなければならない。

適用上の注釈：

セキュリティターゲットは、以下のために TOE 内で利用される暗号操作を本 SFR において提供しなければならない：

・TEE ファームウェア及び TA コードの真正性の検証
・高信頼ストレージのデータの一貫性及び機密性の保護。これらの操作は、TEE ストレージの信頼の基点の鍵に基づく。ST 作成者は、内部 API によって TA に提供される操作等、追加の FCS_COP.1 暗号操作の他の繰り返しを含むことを選択してもよい。

FDP_ACC.1/TA_keys　サブセットアクセス制御

FDP_ACC.1.1/TA_keys　TSF は、以下に対して **TA 鍵アクセス制御 SFP** を実施しなければならない：

・サブジェクト：S.API、S.TA_INSTANCE 及び TEE のその他のサブジェクト
・オブジェクト：OB.TA_KEY
・操作：OP.USE_KEY、OP.EXTRACT_KEY。

FDP_ACF.1/TA_keys　セキュリティ属性によるアクセス制御

FDP_ACF.1.1/TA_keys　TSF は、以下に基づいて、オブジェクトに対して **TA 鍵アクセス制御 SFP** を実施しなければならない：**OB.TA_KEY.usage、OB.TA_KEY.owner、OB_TA_KEY.isExtractable 及び S.API.caller。**

FDP_ACF.1.2/TA_keys　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を決定するために、次の規則を実施しなければならない：

・OP.USE_KEY は、以下の条件が保持される場合に許可される：
・API に対して操作を要求した TA インスタンスが鍵を所有する（S.API.caller = OB.TA_KEY.owner）
・意図される鍵の用途（OB.TA_KEY.usage）が要求された操作と一致する
・OP.EXTRACT_KEY は、以下の条件が保持される場合に許可される：
・API に対して操作を要求した TA インスタンスが鍵を所有する（S.API.caller = OB.TA_KEY.owner）
・この操作が、OB.TA_KEY の公開部分の抽出を試行する、または鍵が抽出可能である（OB.TA_KEY.isExtractable = True）

FDP_ACF.1.3/TA_keys　TSF は、次の追加規則、**[割付：セキュリティ属性に基づく、サブジェクトのオブジェクトに対するアクセスを明示的に許可する規則]**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許可しなければならない。

FDP_ACF.1.4/TA_keys　TSF は、次の追加規則に基づいて、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：

・S.TA_INSTANCE または S.API ではない TEE の他のサブジェクトから直接試行された利用者鍵へのアクセス
・有効な caller のいない（S.API.caller は定義されていない）、S.API から試行された利用者鍵へのアクセス
・[割付：セキュリティ属性に基づいて、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する規則]。

適用上の注釈：

この要件は、TEE 内部 API のみを介した鍵へのアクセス条件を記述する：OP.USE_KEY 及び OP.EXTRACT_KEY は、API の操作を意味する。

FDP_ACF.1.3/TA_keys：現在の TEE 内部 API 仕様における所有権は、すべてにアクセスできる各 TA、

及びそれ自体のオブジェクトに制限される。

FMT_MSA.1/TA_keys　セキュリティ属性の管理

FMT_MSA.1.1/TA_keys　TSF は、セキュリティ属性 **OB.TA_KEY.usage、OB.TA_KEYS.isExtractable 及び OB.TA_KEY.owner** に対し、**デフォルト値変更、問い合わせ及び改変**をする能力を**以下の役割**に制限する **TA 鍵アクセス制御 SFP** を実施しなければならない:

- **OB.TA_KEY.usage のデフォルト値変更、問い合わせ、クエリ及び改変の機能を TA_User の役割へ**
- **OB.TA_KEY.owner の問い合わせを TSF の役割へ。**

FMT_MSA.3/TA_keys　静的属性初期化

FMT_MSA.3.1/TA_keys　TSF は、その SFP を実施するために使われるセキュリティ属性に対して制限的デフォルト値を与える **TA 鍵アクセス制御 SFP** を実施しなければならない。

FMT_MSA.3.2/TA_keys　TSF は、オブジェクトや情報が生成されるとき、**TA_User の役割[割付:許可された識別された役割]**が、デフォルト値を上書きする代替の初期値を特定することを許可しなければならない。

7.1.1.4　初期化、操作及びファームウェアの完全性

FAU_ARP.1　セキュリティアラーム

FAU_ARP.1.1　TSF は、セキュリティ侵害の可能性が検出された場合、**[割付:アクションのリスト]**を実行しなければならない。

詳細化:

TSF は、セキュリティ侵害の可能性が検出された場合、以下のアクションを実行しなければならない:

- TA データ、TA コードまたは TEE データの一貫性の違反の検出:**[割付:関連付けられたアクション]**
- TEE ファームウェアの完全性の違反の検出:**[割付:関連付けられたアクション]**
- **[割付:実装に依存するセキュリティ侵害の可能性及び関連付けられたアクションのリスト]**

FDP_SDI.2　蓄積データ完全性監視及びアクション

FDP_SDI.2.1　TSF は、すべてのオブジェクトにおける**[割付:完全性誤り]**について、以下の属性に基づき、TSF によって制御されるコンテナ内に蓄積された利用者データを監視しなければならない:**[割付:利用者データ属性]**。

詳細化:

TSF は、すべてのオブジェクトにおける**真正性及び一貫性の誤り**について、次の属性に基づき、TSF によ

って制御されるコンテナ内の蓄積されたTEEランタイムデータ、TEE永続的データ、TAデータと鍵及びTAコードを監視しなければならない:**[割付:TEE ランタイムデータ、TEE 永続的データ、TA データと鍵及び TA コードの属性]**。

FDP_SDI.2.2 データの完全性誤り検出時に、TSFは、**[割付:とられるアクション]**を行わなければならない。

詳細化:

- TEE ランタイムデータまたは TEE 永続的データの真正性または一貫性の誤りの検出時、TSFは、**[割付:損なわれたデータに依存しないアクション]**を行わなければならない
- TA コードの真正性または一貫性の誤りの検出時、TSF は、**TA インスタンスの実行を中止しなければならない**
- TA データまたは TA 鍵の真正性または一貫性の誤りの検出時、TSF は、
  - **損なわれたデータを戻してはならない**
  - **[割付:損なわれたデータに依存しないアクション]**
- **[割付:とられる他のアクション]**

適用上の注釈:

このSFRは、揮発性メモリ内のTEEランタイムデータ(このデータは不揮発性メモリ内に蓄積されない)及び、揮発性メモリと不揮発性メモリの両方にあるTEE永続的データ、TAデータと鍵、TAコードに適用される。

本 SFR は、同様のメカニズムがこのデータの一貫性を保護するために含まれているので、TSF データと利用者データの両方に利用される。

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:

- **デバイス結合の障害**
- **暗号操作の障害**
- **無効な CA リクエスト、特に不良構成リクエスト**
- **パニック状態(*[IAPI]*第 2.2.3 項で定める通り)**
- **TA コード、TA データまたは TA 鍵の真正性または一貫性の障害**
- **TEE データ(特に TA の特性、TEE 鍵及びすべてのセキュリティ属性)の真正性または一貫性の障害**
- **TEE ファームウェアの完全性の障害**
- **TEE 初期化の障害**
- **現在の TEE 状態での予期しないコマンド**
- **[割付:TSF の障害の種別のリスト]。**

適用上の注釈:

- デバイス結合の障害は、格納データ(の一部)が同じTEEに結び付けられていない場合に発生する。

- ST 作成者は、セキュリティ状態の特徴を定義しなければならない。特に、障害の状態とセキュアな状態の遷移では TEE 及び利用者データと鍵を保護しなければならない。

FPT_INI.1 TSF 初期化

FPT_INI.1.1 TOE 初期化機能は、
- TEE 初期化コード及びデータの完全性
- TEE ファームウェアの真正性及び完全性
- ストレージの信頼の基点の完全性
- TEE 識別データの完全性
- 旧バージョンへのダウングレードを防ぐファームウェアのバージョン
- **[割付：実装依存の検証のリスト]**

をセキュアな初期状態で TSF を確立する前に、検証しなければならない。

FPT_INI.1.2 TOE 初期化機能は、TOE が正常に初期化を完了するか、または停止できるように、初期化中のエラー及び障害を検出し、それに対処しなければならない。

FPT_INI.1.3 TOE 初期化機能は、TOE 初期化の完了後に、TSF と任意に対話することができてはならない。

適用上の注釈：

ファームウェアのダウングレードの検証は、例えば OTP メモリや EEPROM 等、TOE に常駐するデータに依拠しなければならない。

FMT_SMF.1 管理機能の特定

FMT_SMF.1.1 TSF は、以下の管理機能を実行できなければならない：

・TA 鍵セキュリティ属性の管理
・許可された利用者に対する高信頼ストレージセキュリティ属性の提供。

FPT_TEE.1 外部エンティティのテスト

FPT_TEE.1.1 TSF は、**TA コードの真正性**の達成をチェックするために、**実行及び[割付：その他の条件]**の前にテストスイートを実行しなければならない。

FPT_TEE.1.2 テストが失敗した場合、TSF は **TA インスタンスの実行を開始**してはならない。

7.1.1.5 TEE 識別

FAU_SAR.1 監査レビュー

FAU_SAR.1.1 TSF は、**すべての利用者**が、**TEE 識別子**を監査記録から読みだせるようにしなければならない。

FAU_SAR.1.2 TSF は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

FAU_STG.1 保護された監査証跡格納

FAU_STG.1.1 TSF は、監査証跡に格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2 TSF は、監査証跡に格納された監査記録への不正な改変を**防止**できなければならない。

適用上の注釈:

この SFR の監査記録は、TEE 識別子を参照する。この一意の識別子は、TOE 配付前に TOE に格納される。これは、on-TEE または off-TEE で生成することができる(セキュリティターゲットは生成方法を明確にしなければならない)。

識別子は、最終利用フェーズで改変されてはならない。

セキュリティターゲットは、格納先の永続的メモリの種別を示さなければならない。

7.1.1.6 インスタンス時間

FPT_STM.1/Instance time 高信頼タイムスタンプ

FPT_STM.1/Instance time TSF は、高信頼タイムスタンプを提供できなければならない。

詳細化:

TSF は、TA インスタンスのライフタイム中にタイムスタンプがモノトニック (訳注:単調増加) であるように、TA インスタンスにタイムスタンプを提供できなければならない。

適用上の注釈:

詳細化は、予測される信頼性の意味を与える。

7.1.1.7 乱数生成器

FCS_RNG.1 乱数生成器

FCS_RNG.1.1 TSF は、**[割付:セキュリティ機能リスト]**を実装する**[選択:物理的、非物理的真性、決**

定論的、ハイブリッド、ハイブリッド決定論的] 乱数生成器を提供しなければならない。

FCS_RNG.1.2 TSF は、[**割付：定義された品質メトリック**]に適合する乱数を提供しなければならない。

適用上の注釈：

ST 作成者は、エレメント FCS_RNG.1.1 と FCS_RNG.1.2 で不足する操作を実行しなければならない。ST 作成者は、ミニマムエントロピーまたはシャノンエントロピー等を用いて、生成された乱数の品質を定義すべきである。品質メトリックの割付は、一様分布確率変数に近い乱数の十分なランダム性を保証しなければならない。乱数生成器の評価は、AIS31 等の承認された方法に従わなければならない。本 SFR は、TEE 上で乱数生成される場合、TEE 識別の統計的一意性を保証するためにも利用される。

7.1.1.8 高信頼ストレージ

FDP_ACC.1/Trusted Storage サブセットアクセス制御

FDP_ACC.1.1/Trusted Storage TSF は、以下に対して**高信頼ストレージアクセス制御 SFP** を実施しなければならない：

- **サブジェクト：S.API**
- **オブジェクト：OB.TA_STORAGE、OB.SRT**
- **操作：OP.LOAD、OP.STORE。**

FDP_ACF.1/Trusted Storage セキュリティ属性によるアクセス制御

FDP_ACF.1.1/Trusted Storage TSF は、以下に基づいて、オブジェクトに対して、**高信頼ストレージアクセス制御 SFP** を実施しなければならない：**S.API.caller、OB.TA_STORAGE.owner、OB.TA_STORAGE.inExtMem、OB.TA_STORAGE.TEE_identity 及び OB.SRT.TEE_identity。**

FDP_ACF.1.2/Trusted Storage 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を決定するために、次の規則を実施しなければならない：

- **OB.TA_STORAGE からのオブジェクトの OP.LOAD は、以下の条件が保持される場合に許可される：**
  - **操作が S.API によって実行される**
  - **ロード要求が高信頼ストレージ空間の所有者のインスタンスから来る（S.API.caller = OB.TA_STORAGE.owner）**
  - **OB.TA_STORAGE が、TEE ストレージの信頼の基点 OB.SRT に結び付けられる（OB.TA_STORAGE.TEE_identity = OB.SRT.TEE_identity）**
  - **OB.TA_STORAGE が REE へアクセスできる外部メモリに配置されている場合（OB.TA_STORAGE.inExtMem = True）、オブジェクトがロード前に認証され、復号される**

- **OB.TA_STORAGE へのオブジェクトの OP.STORE は、以下の条件が保持される場合に許可される:**
  - **操作が S.API によって実行される**
  - **格納要求が、高信頼ストレージ空間の所有者のインスタンスから来る(S.API.caller = OB.TA_STORAGE.owner)**
  - **OB.TA_STORAGE が TEE ストレージの信頼の基点 OB.SRT に結び付けられる(OB.TA_STORAGE.TEE_identity = OB.SRT.TEE_identity)**
  - **OB.TA_STORAGE が REE へアクセスできる外部メモリに配置されている場合(OB.TA_STORAGE.inExtMem = True)、オブジェクトが格納前に署名され、暗号化される。**

FDP_ACF.1.3/Trusted Storage TSF は、次の追加規則、**[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許可する規則]**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許可しなければならない。

FDP_ACF.1.4/Trusted Storage TSF は、次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拒否しなければならない:

- **有効な caller のいない(S.API.caller = undefined)、S.API から試行された高信頼ストレージへのアクセス**
- **異なる TEE(OB.SRT.TEE_identity とは異なる OB.TA_STORAGE.TEE_identity)に結び付けられた高信頼ストレージへのアクセス**
- **S.API と異なるサブジェクトからの高信頼ストレージへのアクセス**
- **[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]**

FDP_ROL.1/Trusted Storage 基本ロールバック

FDP_ROL.1.1/Trusted Storage TSF は、**ストレージ**に対する**失敗または中断された OP.STORE 操作**のロールバックを許可するために、**高信頼ストレージアクセス制御 SFP** を実施しなければならない。

FDP_ROL.1.2/Trusted Storage TSF は、[割付:ロールバックを実行できる境界限界]内で操作がロールバックされることを許可しなければならない。

適用上の注釈:

本 SFR は、書き込み操作の原子性を実施する[IAPI]。

FMT_MSA.1/Trusted Storage セキュリティ属性の管理

FMT_MSA.1.1/Trusted Storage TSF は、セキュリティ属性 **OB.TA_STORAGE.owner、**

OB.TA_STORAGE.inExtMem、OB.TA_STORAGE.TEE_identity 及び OB.SRT.TEE_identity に対し**問い合わせ**をする能力を **TA_User の役割**に制限する**高信頼ストレージアクセス制御 SFP** を実施しなければならない。

FMT_MSA.3/Trusted Storage　静的属性初期化

FMT_MSA.3.1/Trusted Storage　TSF は、その SFP を実施するために使われるセキュリティ属性に対して制限的デフォルト値を与える**高信頼ストレージアクセス制御 SFP** を実施しなければならない。

FMT_MSA.3.2/Trusted Storage　TSF は、オブジェクトや情報が生成されるとき、**TA_User** がデフォルト値を上書きする代替の初期値を特定することを許可しなければならない。

FDP_ITT.1/Trusted Storage　基本内部転送保護

FDP_ITT.1.1/Trusted Storage　TSF は、利用者データが TOE の物理的に分離されたパート間を転送される場合、その**暴露及び改変**を防止するための**高信頼ストレージアクセス制御 SFP** を実施しなければならない。

7.1.2　TEE Time and Rollback PP モジュール

この PP モジュールでは、CC パート 2[CC2]で定義される以下のセキュリティ機能コンポーネントが使用される:

- **FDP_SDI.2　蓄積データ完全性監視及びアクション**
- **FPT_FLS.1　セキュアな状態を保持する障害**
- **FPT_STM.1　高信頼タイムスタンプ**
- **FMT_MTD.1　TSF データの管理**
- **FMT_SMF.1　管理機能の特定**

7.1.2.1　ロールバック保護

FDP_SDI.2/Rollback　蓄積データ完全性監視及びアクション

FDP_SDI.2.1/Rollback　TSF は、すべてのオブジェクトにおける**[割付:完全性誤り]**について、次の属性に基づき、TSF によって制御されるコンテナ内に蓄積された利用者データを監視しなければならない:**[割付:利用者データ属性]**。

詳細化:

TSF は、すべてのオブジェクトにおける**完全性誤り**について、次の属性に基づき、TSF によって制御されるコンテナ内に蓄積された TEE ロールバック検出データ、TEE ランタイムデータ、TEE 永続的データ、TA データと鍵及び TA コードを監視しなければならない:**[割付:TEE ロールバック検出データ、TEE ランタイムデ**

ータ、TEE 永続的データ、TA データと鍵及び TA コードの属性]。

FDP_SDI.2.2/Rollback データの完全性誤り検出時、TSF は、**[割付：とられるアクション]**を行わなければならない。

詳細化：

- TEE ロールバック検出データ、TEE ランタイムデータまたは TEE 永続的データの完全性誤り検出時、TSF は、**損なわれたデータに依存しないアクション**を行わなければならない
- TA コードの完全性誤り検出時、TSF は、**TA インスタンスの実行を中止**しなければならない
- TA データまたは TA 鍵の完全性誤り検出時、TSF は、
  - **損なわれたデータを戻してはならない**
  - **損なわれたデータに依存しないアクションを行わなければならない**
- **[割付：取るべきその他のアクション]。**

適用上の注釈：

本要件は、ベース PP の FDP_SDI.2 に完全性の監視を追加する。ロールバック検出は、ロールバック検出データ及び完全性の障害検出によって保証される。

FPT_FLS.1/Rollback セキュアな状態を保持する障害

FPT_FLS.1.1/Rollback 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：

・TA コードとデータの完全性の障害

・TEE 永続的データの完全性の障害。

適用上の注釈：

この要件は、FPT_FLS.1 を補完する。

7.1.2.2 TA 持続時間

FPT_STM.1/Persistent Time 高信頼タイムスタンプ

FPT_STM.1.1/Persistent Time TSF は、高信頼タイムスタンプを提供できなければならない。

詳細化：

TSF は、以下が実現されるように、TA インスタンスにタイムスタンプを提供できなければならない。：

- タイムスタンプが TEE リセットを超えて持続する
- タイムスタンプが、TA のインスタンスによって実行される 2 度の「時刻設定」操作間でモノトニックである

TSF は、モノトニシティ(訳注：単調増加) の特性を満たさない持続時間を無効にしなければならない。

適用上の注釈：

詳細化は、期待される信頼性の意味を与える。

FMT_MTD.1/Persistent Time　TSF データの管理

FMT_MTD.1.1/Persistent Time　TSF は、**TA 持続時間について「時刻設定」操作を実行する**能力を**TA のインスタンス**に制限しなければならない。

適用上の注釈:

「時刻設定」操作は、操作を実行する TA の持続時間値にのみ影響する。

FMT_SMF.1/Persistent Time　管理機能の特定

FMT_SMF.1.1/Persistent Time　TSF は、以下の管理機能を実行できなければならない:**TA 持続時間の「時刻設定」操作**。

適用上の注釈:

「時刻設定」操作は、操作を実行する TA の持続時間値にのみ影響する。

7.1.3　TEE Debug PP モジュール

本 PP モジュールでは、CC パート 2[CC2]で定義される以下のセキュリティ機能コンポーネントが使用される:

- FIA_UID.2　アクション前の利用者識別
- FIA_UAU.2　アクション前の利用者認証
- FIA_UAU.6　再認証
- FIA_ATD.1　利用者属性定義
- FIA_USB.1　利用者-サブジェクト結合
- FCS_COP.1　暗号操作
- FDP_ACC.1　サブセットアクセス制御
- FDP_ACF.1　セキュリティ属性によるアクセス制御
- FMT_SMR.1　セキュリティの役割

本セクションで定義されたこれらすべての SFR は、デバッグ機能にのみ関係する

本 PP モジュールによって導入された追加の利用者は以下の通りである:

- TEE デバッグ管理者

本 PP モジュールによって導入された追加のサブジェクトは以下の通りである:

- S.DEBUG:デバッグインタフェースで、この機能が TEE で利用できるかどうかを示す「enabled」（True/False）と TEE デバッグ管理者が認証されたかどうかを示す「authenticated」（True/False）というセキュリティ属性を持つ。

本 PP モジュールは、TEE デバッグ管理者を代行して、S.DEBUG によって実行されるデバッグ操作を許可する。

- OP.AUTHENTICATE：TEE デバッグ管理者の認証によるデバッグ機能の起動
- OP.DEBUG：デバッグ操作

本 PP モジュールは、以下のアクセス制御と情報フローセキュリティ機能方針（SFP）を定義する：

デバッグアクセス制御 SFP：

- 目的：TEE のデバッグ設備へのアクセスを制御する
- サブジェクト：S.DEBUG
- オブジェクト：すべて
- セキュリティ属性：S.DEBUG.enabled、S.DEBUG.authenticated
- 操作：OP.AUTHENTICATE、OP.DEBUG
- SFR インスタンス：FDP_ACC.1/Debug、FDP_ACF.1/Debug

FDP_ACC.1/Debug　サブセットアクセス制御

FDP_ACC.1.1/Debug　TSF は、以下に対して**デバッグアクセス制御 SFP** を実施しなければならない。：

- **サブジェクト：S.DEBUG**
- **オブジェクト：すべてのオブジェクト**
- **操作：OP.ACTIVE、OP.DEBUG**

FDP_ACF.1/Debug　セキュリティ属性によるアクセス制御

FDP_ACF.1.1/Debug　TSF は、以下に基づいて、オブジェクトに対して、デバッグアクセス制御 SFP を実施しなければならない。：

- **S.DEBUG.enabled、S.DEBUG.authenticated**
- **[割付：示された SFP の下で制御されるサブジェクトとオブジェクトのリスト、及び、それぞれについて、SFP 関連のセキュリティ属性、または SFP 関連のセキュリティ属性と名付けられたグループ]。**

FDP_ACF.1.2/Debug　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を決定するために、次の規則を実施しなければならない。：

- **以下の条件が保持される場合、OP.AUTHENTICATE は許可される：**
  - **操作が S.DEBUG によって実行される**
  - **デバッグインタフェースが有効化される（S.DEBUG.enabled = True）**
- **以下の条件が保持される場合、すべてのオブジェクトに対する OP.DEBUG は許可される：**
  - **操作が S.DEBUG によって実行される**
  - **デバッグインタフェースが有効化される（S.DEBUG.enabled = True）**
  - **TEE デバッグ管理者が認証される（S.DEBUG.authenticated = True）**

- **[割付：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、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]**

FDP_ACF.1.3/Debug TSF は、次の追加規則、**[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許可する規則]**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許可しなければならない 。

FDP_ACF.1.4/Debug TSF は、次の追加規則、**[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。

FCS_COP.1/Debug 暗号操作

FCS_COP.1.1/Debug TSF は、以下[**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**]及び暗号鍵長[**割付：暗号鍵長**]に従って、**TEE デバッグ管理者または彼を代行する人物の認証**を実行しなければならない。

FMT_SMR.1/Debug セキュリティの役割

FMT_SMR.1.1/Debug TSF は、役割 **TEE デバッグ管理者**を維持しなければならない。

FMT_SMR.1.2/Debug TSF は、利用者を役割に関連付けられなければならない。

適用上の注釈：

TEE デバッグ管理者は、最終利用者を意図するのではなく、製品のライフサイクルに関与する者、及びフェーズ 3 または 5 でデバッグ用クレデンシャルにアクセスする者を意図する。

FIA_UID.2/Debug アクション前の利用者識別

FIA_UID.2.1/Debug[編集上の詳細化] TSF は、その利用者を代行する他の TSF 仲介**デバッグ**アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

FIA_ATD.1/Debug 利用者属性定義

FIA_ATD.1.1/Debug TSF は、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない。:**S.DEBUG.enabled、S.DEBUG.authenticated**

FIA_USB.1/Debug 利用者-サブジェクト結合

FIA_USB.1.1/Debug TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。:**S.DEBUG.enabled、S.DEBUG.authenticated**

FIA_USB.1.2/Debug TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。:**S.DEBUG.authenticated は False である**

FIA_USB.1.3/Debug TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。:

- **S.DEBUG.authenticated は、TEE デバッグ管理者が認証に成功した後、True にセットされる。**
- **S.DEBUG.authenticated は、例えば、電源切断後に、認証が失われたとき、False にセットされる(参照:FIA_UAU.6 の規則)**
- **[割付:属性の変更の規則]**

FIA_UAU.2/Debug アクション前の利用者認証

FIA_UAU.2.1/Debug[編集上の詳細化] TSF は、その利用者を代行する他の TSF 仲介**デバッグ**アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

FIA_UAU.6/Debug 再認証

FIA_UAU.6.1/Debug TSF は、以下の条件のもとで利用者を再認証しなければならない。:

- **TEE 電源切断後**
- **[割付:再認証が要求される条件のリスト]**

7.2 セキュリティ保証要件

本プロテクションプロファイルは、拡張 AVA_TEE.2 SAR を追加した EAL 2 パッケージからなる PP のセキュリティ保証要件(SAR)のセットを提供する。本 SAR は、AVA_VAN.2 基本攻撃能力を、附属書 A.1 で定義された TEE-Low 攻撃能力に高める。

追加された EAL では、AVA_VAN.2 と AVA_TEE.2 の両方が選択されるため、評価者は、これらの SAR と関連する評価表に従って、2 つの攻撃評価を実行しなければならないだろう。

7.3 セキュリティ要件根拠

7.3.1 対策方針

7.3.1.1 TOE のセキュリティ対策方針

7.3.1.2 TEE ベース PP

O.CA_TA_IDENTIFICATION 以下の要件は対策方針を満たすことに寄与する:

- FIA_ATD.1 は、セキュリティ属性としてのクライアントと TA の識別情報及び特性の管理を実施する。それらは完全性及び機密性で保護された TSF データになる
- FIA_UID.2 は、アクション前のクライアントアプリケーションまたは TA の識別を要求する。それにより、許可された利用者だけにサービス及びデータへのアクセスを許可する
- FIA_USB.1 は、利用者を代行して動作する能動的エンティティへの利用者識別情報の関連付け、及びこれが有効な識別情報であることのチェックを実施する

O.KEYS_USAGE 以下の要件は対策方針を満たすことに寄与する:

- FCS_COP.1 は、適用可能な場合、評価の範囲内における暗号操作の特定を許可する
- FDP_ACC.1/TA_keys、FDP_ACF.1/TA_keys、FMT_MSA.1/TA_keys、FMT_MSA.3/TA_keys、FMT_SMR.1 及び FMT_SMF.1 は、鍵の所有者のみにアクセスを許可する、鍵アクセス方針を示す。

O.TEE_ID 以下の要件は対策方針を満たすことに寄与する:

- FAU_SAR.1 は、TEE 識別子アクセス機能を実施する
- FAU_STG.1 は、TEE 識別子格納機能を実施する
- FPT_INI.1 は、TEE 識別の完全性を実施し、障害の場合のふるまいを指定する
- FCS_RNG.1 は、TOE で生成される場合の、TEE 識別データの統計的一意性を実施する

O.INITIALIZATION 以下の要件は対策方針を満たすことに寄与する:

- FTP_FLS.1 は、初期化またはデバイス結合の障害の場合に TEE がセキュアな状態に達しなければならないことを指定する
- FCS_COP.1 は、TEE ファームウェアの真正性を検証するために使用される暗号について指定する
- FPT_INI.1 は、TEE ファームウェアの真正性及び完全性の検証を含む、セキュアなプロセスを介し、TSF の初期化を実施する

O.INSTANCE_TIME 以下の要件は対策方針を満たす:

- FPT_STM.1/Instance time は、TA インスタンス時間の信頼性を実施する

O.OPERATION 以下の要件は対策方針を満たすことに寄与する:

- FAU_ARP.1 は、潜在的セキュリティ侵害に対する TEE の対処を指定する
- FDP_SDI.2 は、TEE データ及び TA の一貫性及び真正性の監視を実施し、障害の場合の行動を指定する
- FIA_ATD.1、FIA_UID.2 及び FIA_USB.1 は、アクションが識別された利用者によって実行されることを保証する
- FMT_SMR.1 は、TEE によって実行される 2 つの運用の役割を指定する
- FPT_FLS.1 は、異常操作がセキュアな状態に導かれなければならないことを指定する

- FDP_ACC.1/Trusted Storage、FDP_ACF.1/Trusted Storage、FMT_MSA.1/Trusted Storage、FMT_MSA.3/Trusted Storage 及び FMT_SMF.1 は、TA ストレージへのアクセス制御方針を指定する
- FDP_IFC.2/Runtime 及び FDP_IFF.1/Runtime は、TA 及び TEE 実行空間へのアクセス制御方針を指定する
- FDP_ACC.1/TA_keys 、 FDP_ACF.1/TA_keys 、 FMT_MSA.1/TA_keys 、 FMT_MSA.3/TA_keys 及び FMT_SMF.1 は、鍵アクセス方針を指定する

Time and Rollback PP モジュールに特有の根拠:

- FDP_SDI.2/Rollback は、TEE データ及び TA の完全性の監視を実施し、障害の場合のふるまいを指定する(FDP_SDI.2 を満たす)
- FPT_FLS.1/Rollback は、補足的に異常な状況がセキュアな状態に導かれなければならないことを指定する(FPT_FLS.1 を満たす)

Debug PP モジュールに特有の根拠:

- FDP_ACC.1/Debug、FDP_ACF.1/Debug、FMT_SMR.1/Debug、FIA_UID.2/Debug、FIA_UAU.2/Debug、FIA_UAU.6/Debug、FIA_ATD.1/Debug 及び FIA_USB.1/Debug は、この機能が禁止されていない場合に、TEE のデバッグ機器へのアクセスを許可する、デバッグアクセス方針を指定する

O.RNG 要件 FCS_RNG.1 は、対策方針を直接満たす。

O.RUNTIME_CONFIDENTIALITY 以下の要件は対策方針を満たすことに寄与する:

- FDP_IFC.2/Runtime 及び FDP_IFF.1/Runtime は、許可されたエンティティにのみ読出しアクセスを保証する
- FDP_ITT.1/Runtime 及び FPT_ITT.1/Runtime は、リソース間で転送される TEE 及び TA データの暴露に対する保護を保証する
- FDP_RIP.1/Runtime は、リソースのクリーンアップ方針を指定する。

O.RUNTIME_INTEGRITY 以下の要件は対策方針を満たすことに寄与する:

- FDP_IFC.2/Runtime 及び FDP_IFF.1/Runtime は、許可されたエンティティにのみ書き込みアクセスを許可する、TEE 及び TA ランタイムデータ方針を指定する
- FDP_ITT.1/Runtime 及び FPT_ITT.1/Runtime は、リソース間で転送される TEE 及び TA データの改変に対する保護を保証する
- FDP_SDI.2 は、TEE コード、TEE ランタイムデータ、TA コード、及び TA データと鍵の真正性及び一貫性を監視し、障害時の対処を指定する。

O.TA_AUTHENTICITY 以下の要件は対策方針を満たすことに寄与する:

- FDP_SDI.2 は、格納中の TA コードの一貫性及び真正性を実施する
- FPT_TEE.1 は、実行前の TA コードの真正性のチェックを実施する
- FCS_COP.1 は、TA コードの真正性を検証するために使用される暗号を指定する。

O.TA_ISOLATION 以下の要件は対策方針を満たすことに寄与する:

- FDP_ACC.1/Trusted Storage、FDP_ACF.1/Trusted Storage、FMT_MSA.1/Trusted Storage、FMT_MSA.3/Trusted Storage 及び FMT_SMF.1 は、TA ストレージへのアクセス制御方針を指定する
- FCS_COP.1 は、TA データの機密性及び真正性を保証するために高信頼ストレージに使用される暗号アルゴリズムを指定する
- FDP_IFC.2/Runtime 及び FDP_IFF.1/Runtime は、TA 実行空間へのアクセス制御方針を指定する
- FPT_FLS.1 は、特にパニック状態の場合に、セキュアな状態の維持による TA 分離を実施する。

O.TEE_DATA_PROTECTION 以下の要件は対策方針を満たすことに寄与する:

- FCS_COP.1 は、適用可能な場合、外部メモリの TEE データの一貫性及び機密性を保護するために使用される暗号を指定する
- FDP_SDI.2 は、TEE 永続的データの真正性及び一貫性を監視し、障害の対処を指定する
- FPT_ITT.1/Runtime は、TEE 永続的データのセキュアな送信及び格納を実施する

O.TEE_ISOLATION 以下の要件は対策方針を満たすことに寄与する:

- FDP_IFC.2/Runtime 及び FDP_IFF.1/Runtime は、TEE 実行空間へのアクセス制御方針を指定する。

O.TRUSTED_STORAGE 以下の要件は対策方針を満たすことに寄与する:

- FCS_COP.1 は、適用可能な場合、外部メモリの TA データの完全性及び機密性を保護するために使用される暗号を指定する
- FDP_ACC.1/Trusted Storage、FDP_ACF.1/Trusted Storage、FDP_ROL.1/Trusted Storage 、FMT_MSA.1/Trusted Storage 、FMT_MSA.3/Trusted Storage 及び FMT_SMF.1 state Storage は、TA 高信頼ストレージへのアクセス及びデータの機密性保護の方針を指定する
- FDP_SDI.2 は、高信頼ストレージの一貫性及び真正性を実施する
- FPT_INI.1 は、TEE 識別及びストレージの信頼の基点の完全性を実施し、障害時の対処を指定する
- FDP_ITT.1/Trusted Storage は、リソース間で転送される TEE 及び TA データの暴露に対する保護を保証する
- FPT_FLS.1 はセキュアな状態を維持する。

7.3.1.3 TEE Time and Rollback PP モジュール

O.ROLLBACK_PROTECTION 以下の要件は対策方針を満たすことに寄与する:

- FDP_SDI.2/Rollback は、完全性の障害時に、TEE のふるまいを指定する(このようにロールバック)

- FPT_FLS.1/Rollback は、完全性の障害の検出を実施する（このようにロールバック検出）

O.TA_PERSISTENT_TIME 以下の要件は対策方針を満たすことに寄与する:

- FPT_STM.1/Persistent Time は、TEE に予測される永続的時間の信頼性の条件を指定する
- FMT_MTD.1/Persistent Time は、「時間設定」操作を実行できる役割を指定する
- FMT_SMF.1/Persistent Time は、「時間設定」管理機能の存在を指定する

7.3.1.4 TEE Debug PP モジュール

O.DEBUG 以下の要件は対策方針を満たすことに寄与する:

- FDP_ACC.1/Debug 、 FDP_ACF.1/Debug 、 FMT_SMR.1/Debug 、 FIA_UID.2/Debug、
  FIA_UAU.2/Debug、FIA_UAU.6/Debug、FIA_ATD.1/Debug 及び FIA_USB.1/Debug は、TEE デバッグ管理者のみにアクセスを許可する、デバッグアクセス方針を指定する
- FCS_COP.1/Debug は、TEE デバッグ管理者を認証するために使用される暗号操作の特定を許可する

7.3.2 セキュリティ対策方針と SFR の根拠表

セキュリティ対策方針	セキュリティ機能要件	根拠
O.CA_TA_IDENTIFICATION	FIA_ATD.1, FIA_UID.2, FIA_USB.1	セクション 4.3.1
O.KEYS_USAGE	FDP_ACC.1/TA_keys, FDP_ACF.1/TA_keys, FMT_MSA.1/TA_keys, FMT_MSA.3/TA_keys, FMT_SMF.1, FCS_COP.1, FMT_SMR.1	セクション 4.3.1
O.TEE_ID	FAU_SAR.1, FCS_RNG.1, FPT_INI.1, FAU_STG.1	セクション 4.3.1
O.INITIALIZATION	FPT_FLS.1, FPT_INI.1, FCS_COP.1	セクション 4.3.1
O.INSTANCE_TIME	FPT_STM.1/Instance time	セクション 4.3.1
O.OPERATION	FAU_ARP.1, FDP_SDI.2, FIA_ATD.1, FIA_UID.2, FIA_USB.1, FMT_SMR.1, FPT_FLS.1, FDP_SDI.2/Rollback, FPT_FLS.1/Rollback, FDP_ACC.1/Debug, FDP_ACF.1/Debug, FDP_IFC.2/Runtime, FDP_IFF.1/Runtime, FMT_SMF.1, FDP_ACC.1/Trusted Storage, FDP_ACF.1/Trusted Storage, FMT_MSA.1/Trusted Storage,	セクション 4.3.1

	FMT_MSA.3/Trusted Storage, FDP_ACC.1/TA_keys, FDP_ACF.1/TA_keys, FMT_MSA.1/TA_keys, FMT_MSA.3/TA_keys, FMT_SMR.1/Debug, FIA_UID.2/Debug, FIA_ATD.1/Debug, FIA_USB.1/Debug, FIA_UAU.2/Debug, FIA_UAU.6/Debug	
O.RNG	FCS_RNG.1	セクション 4.3.1
O.RUNTIME_CONFIDENTIALITY	FDP_IFC.2/Runtime, FDP_IFF.1/Runtime, FDP_ITT.1/Runtime, FDP_RIP.1/Runtime, FPT_ITT.1/Runtime	セクション 4.3.1
O.RUNTIME_INTEGRITY	FDP_IFC.2/Runtime, FDP_IFF.1/Runtime, FDP_ITT.1/Runtime, FPT_ITT.1/Runtime, FDP_SDI.2	セクション 4.3.1
O.TA_AUTHENTICITY	FDP_SDI.2, FCS_COP.1, FPT_TEE.1	セクション 4.3.1
O.TA_ISOLATION	FDP_ACC.1/Trusted Storage, FDP_ACF.1/Trusted Storage, FDP_IFC.2/Runtime, FDP_IFF.1/Runtime, FMT_MSA.1/Trusted Storage, FMT_MSA.3/Trusted Storage, FMT_SMF.1, FCS_COP.1, FPT_FLS.1	セクション 4.3.1
O.TEE_DATA_PROTECTION	FDP_SDI.2, FCS_COP.1, FPT_ITT.1/Runtime	セクション 4.3.1
O.TEE_ISOLATION	FDP_IFC.2/Runtime, FDP_IFF.1/Runtime	セクション 4.3.1
O.TRUSTED STORAGE	FDP_ACC.1/Trusted Storage, FDP_ACF.1/Trusted Storage, FDP_ROL.1/Trusted Storage, FDP_SDI.2, FMT_MSA.1/Trusted Storage, FMT_MSA.3/Trusted Storage, FCS_COP.1, FPT_INI.1, FMT_SMF.1, FPT_FLS.1, FDP_ITT.1/Trusted Storage	セクション 4.3.1
O.ROLLBACK_PROTECTION	FDP_SDI.2/Rollback, FPT_FLS.1/Rollback	セクション 4.3.1
O.TA_PERSISTENT_TIME	FPT_STM.1/Persistent Time, FMT_MTD.1/Persistent Time, FMT_SMF.1/Persistent Time	セクション 4.3.1
O.DEBUG	FDP_ACC.1/Debug, FDP_ACF.1/Debug, FCS_COP.1/Debug, FMT_SMR.1/Debug, FIA_UID.2/Debug, FIA_ATD.1/Debug, FIA_USB.1/Debug, FIA_UAU.2/Debug, FIA_UAU.6/Debug	セクション 4.3.1

表 11：セキュリティ対策方針と SFR ― カバレージ

セキュリティ機能要件	セキュリティ対策方針
FIA_ATD.1	O.CA_TA_IDENTIFICATION, O.OPERATION
FIA_UID.2	O.CA_TA_IDENTIFICATION, O.OPERATION
FIA_USB.1	O.CA_TA_IDENTIFICATION, O.OPERATION
FMT_SMR.1	O.KEYS_USAGE, O.OPERATION
FDP_IFC.2/Runtime	F.OPERATION, O.RUNTIME_CONFIDENTIALITY, O.RUNTIME_INTEGRITY, O.TA_ISOLATION, O.TEE_ISOLATION
FDP_IFF.1/Runtime	O.OPERATION, O.RUNTIME_CONFIDENTIALITY, O.RUNTIME_INTEGRITY, O.TA_ISOLATION, O.TEE_ISOLATION
FDP_ITT.1/Runtime	O.RUNTIME_CONFIDENTIALITY, O.RUNTIME_INTEGRITY
FDP_RIP.1/Runtime	O.RUNTIME_CONFIDENTIALITY
FPT_ITT.1/Runtime	O.RUNTIME_CONFIDENTIALITY, O.RUNTIME_INTEGRITY, O.TEE_DATA_PROTECTION
FCS_COP.1	O.KEYS_USAGE, O.INITIALIZATION, O.TA_AUTHENTICITY, O.TA_ISOLATION, O.TEE_DATA_PROTECTION, O.TRUSTED_STORAGE
FDP_ACC.1/TA_keys	O.KEYS_USAGE, O.OPERATION
FDP_ACF.1/TA_keys	O.KEYS_USAGE, O.OPERATION
FMT_MSA.1/TA_keys	O.KEYS_USAGE, O.OPERATION
FMT_MSA.3/TA_keys	O.KEYS_USAGE, O.OPERATION
FAU_ARP.1	O.OPERATION
FDP_SDI.2	O.OPERATION, O.RUNTIME_INTEGRITY, O.TA_AUTHENTICITY, O.TEE_DATA_PROTECTION, O.TRUSTED_STORAGE
FPT_FLS.1	O.INITIALIZATION, O.OPERATION, O.TA_ISOLATION, O.TRUSTED_STORAGE
FPT_INI.1	O.TEE_ID, O.INITIALIZATION, O.TRUSTED_STORAGE
FMT_SMF.1	O.KEYS_USAGE, O.OPERATION, O.TA_ISOLATION, O.TRUSTED_STORAGE
FPT_TEE.1	O.TA_AUTHENTICITY
FAU_SAR.1	O.TEE_ID
FAU_STG.1	O.TEE_ID

セキュリティ機能要件	セキュリティ対策方針
FPT_STM.1/Instance time	O.INSTANCE_TIME
FCS_RNG.1	O.TEE_ID, O.RNG
FDP_ACC.1/Trusted Storage	O.OPERATION, O.TA_ISOLATION O.TRUSTED_SOTRAGE
FDP_ACF.1/Trusted Storage	O.OPERATION, O.TA_ISOLATION, O.TRUSTED_STORAGE
FDP_ROL.1/Trusted Storage	O.TRUSTED_STORAGE
FMT_MSA.1/Trusted Storage	O.OPERATION, O.TA_ISOLATION, O.TRUSTED_STORAGE
FMT_MSA.3/Trusted Storage	O.OPERATION, O.TA_ISOLATION, O.TRUSTED_STORAGE
FDP_ITT.1/Trusted Storage	O.TRUSTED_STORAGE
FDP_SDI.2/Rollback	O.OPERATION, O.ROLLBACK_PROTECTION
FPT_FLS.1/Rollback	O.OPERATION, O.ROLLBACK_PROTECTION
FPT_STM.1/Persistent Time	O.TA_PERSISTENT_TIME
FMT_MTD.1/Persistent Time	O.TA_PERSISTENT_TIME
FMT_SMF.1/Persistent Time	O.TA_PERSISTENT_TIME
FDP_ACC.1/Debug	O.OPERATION, O.DEBUG
FDP_ACF.1/Debug	O.OPERATION, O.DEBUG
FCS_COP.1/Debug	O.DEBUG
FMT_SMR.1/Debug	O.OPERATION, O.DEBUG
FIA_UID.2/Debug	O.OPERATION, O.DEBUG
FIA_ATD.1/Debug	O.OPERATION, O.DEBUG
FIA_USB.1/Debug	O.OPERATION, O.DEBUG
FIA_UAU.2/Debug	O.OPERATION, O.DEBUG
FIA_UAU.6/Debug	O.OPERATION, O.DEBUG

表 12：SFR とセキュリティ対策方針

7.3.3 依存性

7.3.3.1 SFR 依存性

要件	CC 依存性	満たされた依存性
FDP_ACC.1/Debug	(FDP_ACF.1)	FDP_ACF.1/Debug
FDP_ACF.1/Debug	(FDP_ACC.1) 及び(FMT_MSA.3)	FDP_ACC.1/Debug
FCS_COP.1/Debug	(FCS_CKM.1 または FDP_ITC.1 または FDP_ITC.2)及び (FCS_CKM.4)	
FMT_SMR.1/Debug	(FIA_UID.1)	FIA_UID.2/Debug
FIA_UID.2/Debug	依存性なし	
FIA_ATD.1/Debug	依存性なし	
FIA_USB.1/Debug	(FIA_ATD.1)	FIA_ATD.1/Debug
FIA_UAU.2/Debug	(FIA_UID.1)	FIA_UID.2/Debug
FIA_UAU.6/Debug	依存性なし	
FIA_ATD.1	依存性なし	
FIA_UID.2	依存性なし	
FIA_USB.1	(FIA_ATD.1)	FIA_ATD.1
FMT_SMR.1	(FIA_UID.1)	FIA_UID.2
FDP_IFC.2/Runtime	(FDP_IFF.1)	FDP_IFF.1/Runtime
FDP_IFF.1/Runtime	(FDP_IFC.1)及び(FMT_MSA.3)	FDP_IFC.2/Runtime
FDP_ITT.1/Runtime	(FDP_ACC.1 または FDP_IFC.1)	FDP_IFC.2/Runtime
FDP_RIP.1/Runtime	依存性なし	
FPT_ITT.1/Runtime	依存性なし	
FCS_COP.1	(FCS_CKM.1 または FDP_ITC.1 または FDP_ITC.2)及び(FCS_CKM.4)	
FDP_ACC.1/TA_keys	(FDP_ACF.1)	FDP_ACF.1/TA_keys
FDP_ACF.1/TA_keys	(FDP_ACC.1)及び(FMT_MSA.3)	FDP_ACC.1/TA_keys, FMT_MSA.3/TA_keys
FMT_MSA.1/TA_keys	(FDP_ACC.1 または FDP_IFC.1) 及び(FMT_SMF.1) 及び(FMT_SMR.1)	FMT_SMR.1, FDP_ACC.1/TA_keys, FMT_SMF.1
FMT_MSA.3/TA_keys	(FMT_MSA.1)及び(FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/TA_keys
FAU_ARP.1	(FAU_SAA.1)	
FDP_SDI.2	依存性なし	
FPT_FLS.1	依存性なし	
FPT_INI.1	依存性なし	

要件	CC 依存性	満たされた依存性
FMT_SMF.1	依存性なし	
FPT_TEE.1	依存性なし	
FAU_SAR.1	(FAU_GEN.1)	
FAU_STG.1	(FAU_GEN.1)	
FPT_STM.1/Instance time	依存性なし	
FCS_RNG.1	依存性なし	
FDP_ACC.1/Trusted Storage	(FDP_ACF.1)	FDP_ACF.1/Trusted Storage
FDP_ACF.1/Trusted Storage	(FDP_ACC.1)及び(FMT_MSA.3)	FDP_ACC.1/Trusted Storage, FMT_MSA.3/Trusted Storage
FDP_ROL.1/Trusted Storage	(FDP_ACC.1 または FDP_IFC.1)	FDP_ACC.1/Trusted Storage
FMT_MSA.1/Trusted Storage	(FDP_ACC.1 または FDP_IFC.1) 及び (FMT_SMF.1) 及び (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1, FDP_ACC.1/Trusted Storage
FMT_MSA.3/Trusted Storage	(FMT_MSA.1)及び(FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/TrustedStorage
FDP_ITT.1/Trusted Storage	(FDP_ACC.1 または FDP_IFC.1)	FDP_ACC.1/Trusted Storage
FDP_SDI.2/Rollback	依存性なし	
FPT_FLS.1/Rollback	依存性なし	
FPT_STM.1/Persistent Time	依存性なし	
FMT_MTD.1/Persistent Time	(FMT_SMF.1)及び(FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1/Persistent Time
FMT_SMF.1/Persistent Time	依存性なし	

表 13: SFR 依存性

7.3.3.2 依存性の除外の根拠

FDP_ACF.1/Debug の依存性 FMT_MSA.3 は、除外される。セキュリティ属性は TSF によって排他的に管理されるか、または最終利用フェーズで改変できないので、このアクセス制御 SFP に関して、許可された利用者によるセキュリティ属性の管理は一切ない、したがって依存性 FMT_MSA.3 は適用されない。

FCS_COP.1/Debug の依存性 FCS_CKM.1 または FDP_ITC.1 または FDP_ITC.2 は、除外される。 FCS_COP.1 での TEE デバッグ管理者を認証するために使用される TEE デバッグ認証鍵は、製造中にセットされる。それは、最終利用フェーズでは変更できない。

FCS_COP.1/Debug の依存性 FCS_CKM.4 は、除外される。 FCS_COP.1/Debug での TEE デバッグ管理者を認証するために使用される TEE デバッグ認証鍵は、最終利用フェーズで変更または破壊されることは要求されない。

FDP_IFF.1/Runtime の依存性 FMT_MSA.3 は、除外される。 すべてのセキュリティ属性は TSF によって排他的に管理されるため、この情報フロー制御 SFP に関して、許可された利用者によるセキュリティ属性の管理は一切ない、したがって依存性 FMT_MSA.3 は適用されない。

FCS_COP.1 の依存性 FCS_CKM.1 または FDP_ITC.1 または FDP_ITC.2 は、除外される。 FCS_COP.1 での暗号操作に使用される TEE ストレージの信頼の基点 暗号鍵は、製造中にセットされる。導出された鍵が高信頼ストレージ用に使用される場合、ST 作成者は FCS_CKM.1 への依存性を追加し導出方法を規定しなければならない。

FCS_COP.1 の依存性 FCS_CKM.4 は、除外される。 FCS_COP.1 の暗号操作で使用される TEE ストレージの信頼の基点は、最終利用フェーズで変更または破壊されることは要求されない。

FAU_ARP.1 の依存性 FAU_SAA.1 は、除外される。 潜在的なセキュリティ侵害は、FAU_ARP.1 要件で明示的に定義される。本 PP の SFR で定義される監査対象事象は一切ない。

FAU_SAR.1 の依存性 FAU_GEN.1 は、除外される。 検討される監査記録は TEE 識別子のみであり、この識別子は TOE 配付前にセットされ、後で改変できないので、この依存性は除外される。

FAU_STG.1 の依存性 FAU_GEN.1 は、除外される。 検討される監査記録は TEE 識別子のみであり、この識別子は、TOE 配付前にセットされ、後で改変できないので、この依存性は除外される。

7.3.3.3 SAR 依存性

要件	CC 依存性	満たされた依存性
ADV_ARC.1	(ADV_FSP.1) 及び (ADV_TDS.1)	ADV_FSP.2, ADV_TDS.1
ADV_FSP.2	(ADV_TDS.1)	ADV_TDS.1
ADV_TDS.1	(ADV_FSP.2)	ADV_FSP.2
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.2
AGD_PRE.1	依存性なし	
ALC_CMC.2	(ALC_CMS.1)	ALC_CMS.2
ALC_CMS.2	依存性なし	
ALC_DEL.1	依存性なし	
ASE_CCL.1	(ASE_ECD.1) 及び (ASE_INT.1) 及び (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	依存性なし	
ASE_INT.1	依存性なし	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) 及び (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	依存性なし	
ASE_TSS.1	(ADV_FSP.1) 及び (ASE_INT.1) 及び (ASE_REQ.1)	ADV_FSP.2, ASE_INT.1, ASE_REQ.2
ATE_COV.1	(ADV_FSP.2) 及び (ATE_FUN.1)	ADV_FSP.2, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.1
ATE_IND.2	(ADV_FSP.2) 及び (AGD_OPE.1) 及び (AGD_PRE.1) 及び (ATE_COV.1) 及び (ATE_FUN.1)	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1
AVA_VAN.2	(ADV_ARC.1) 及び (ADV_FSP.2) 及び (ADV_TDS.1) 及び (AGD_OPE.1) 及び (AGD_PRE.1)	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1
AVA_TEE.2	(ADV_ARC.1) 及び (ADV_FSP.2) 及び (ADV_TDS.1) 及び (AGD_OPE.1) 及び (AGD_PRE.1)	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1

表 14: SAR 依存性

7.3.4 セキュリティ保証要件の根拠

本プロテクションプロファイルで定義される保証レベルは、附属書 A で定義される TEE-Low 攻撃能力に到達するため、事前に定義された保証パッケージEAL 2 及び追加の保証コンポーネントAVA_TEE.2（拡張 SAR TEE 脆弱性分析）で構成される。

この追加された EAL は、特に TEE 及び TEE 利用可能なデバイスのライフサイクルのような、業界の制約に適合する良好な TEE 商用開発の実践に基づいた積極的なセキュリティエンジニアリングから、十分な保証を開発者が得られるようにする。開発者は、設計、テスト、ガイダンス、構成管理及び配付レベルにおいて標準的な EAL 2 によって要求される、セキュリティエンジニアリングの証拠資料を提供しなければならない。TEE が使用可能なデバイスとその組込サービスが攻撃者に提示するかもしれないような TEE の高い露出と関心に対抗するため、製品は TEE-Low 攻撃能力への対抗力を示さなければならない。この攻撃能力は、附属書 A に記述される、この分野での一般的なアーキテクチャと攻撃プロファイルで実行される脅威分析に合致する。

コンポーネント AVA_VAN.2 と AVA_TEE.2 は、通常は排他的であるべきだが、追加された EAL パッケージでは、一緒に選択される。この選択の理由は、2 つの表に従って攻撃能力の見積りを実行すること、及び AVA_TEE.2 コンポーネントを承認しないスキームのために EAL 2 製品としての承認を可能にすることである。

A. TEE に対する攻撃能力の適用

本附属書は、TEE プロテクションプロファイルと共に使用される、TEE に対する攻撃能力を評価する方法について紹介する。この作業は、GlobalPlatform TEE セキュリティ作業部会と TEE 攻撃エキスパート作業部会内で収集された、TEE 産業界の関係者の経験に基づく。

本附属書は、攻撃を実行するために攻撃者に要求される攻撃能力を計算するガイダンス指標を提供する。また、TEE 特有の攻撃能力の見積表の定義を含み、TEE 実装における攻撃例を提供する。目標は、TEE における攻撃を成功するために要求される労力の評価に役立てることである。本書は [CC3] と [CEM] と互換である。

A.1 攻撃能力の見積表

TEE 攻撃を実行するために必要な攻撃能力は、攻撃の識別フェーズと悪用フェーズにおける 5 つの要素の組み合わせの結果である：所要時間、TOE へのアクセス、専門知識、TOE の知識、機器とオープンサンプル。以下の修正は、スマートカードのレート付け表へ導入され、：

- スマートカード製品に対する攻撃よりも低いレベルの攻撃実行で必要とされるかもしれない（SoC またはデバイスの）実際のサンプル数を考慮するため、TOE へのアクセスの範囲は修正された。
- TEE 攻撃レート付け表における TOE の知識の 4 つのレベル：公開、制限的、機密及び危機的、に以下の修正がある：
  - TOE に関する制限的な知識は、NDA または同様の情報制御方針を要求する；
  - TOE の機密に関わる知識は、追加の独立した開発者サイト監査を要求する；
  - TOE に関する危機的な知識は、現在の TEE セキュリティ評価方法の下では到達可能ではない；
  - さらに、TOE の非常に危機的なハードウェア設計知識は、TEE が依拠するハードウェアブロックのすべての知識をすでに意味している危機的な知識をもたらすような、多くのハードウェア資源が TEE と REE 間で共有されることを考慮して、削除された；
- オープンサンプルには 4 つのレベルがある：公開、制限的、機密、危機的、これらは TOE の知識に関して規定された同様の条件の下で使用可能である。

これらの要素の値を定める。CC v3.1 改訂第 4 版で定義された標準の表から導出され、CC サポート文書「スマートカードへの攻撃能力の適用」バージョン 2.9 [APSC] におけるものとよく似た修正を含む。

標準 CC 攻撃能力表の主な修正は、攻撃の識別フェーズと悪用フェーズの分離である。識別フェーズは、悪用の準備が出来る点までで、攻撃の最初の生成に相当する、つまり、この目的で生成された潜在的に必要な新しいツールはもちろん、詳細な記述と設定が利用可能になるまでである。悪用フェーズは、各 TOE の攻撃を成功させるための、識別フェーズで定義された分析、技術及びツールの使用に相当する。かなり多くの場合、悪用フェーズで必要な能力は、識別フェーズで必要な能力よりも低いことに留意されたい。例えば、ソフトウェアの脆弱性を発見する最短経路は、ハードウェアを手段にする必要があるが、同じソフトウェアを使って他のデバイスの脆弱性を悪用することは簡単である。

要素	識別	悪用
所要時間		
＜＝1 時間	0	0
＜＝1 日	1	3
＜＝1 週間	2	4
＜＝1 か月	3	6
＞1 か月	5	8
現実的ではない	*	*
TOE のアクセス		
1 サンプルのみ	0	0
10 サンプル未満	1	2
30 サンプル未満	2	4
30 サンプルを超える	3	6
現実的ではない	*	*
専門知識		
しろうと	0	0
熟練者	2	2
エキスパート	5	4
複数のエキスパート	7	6
TOE の知識		
公開	0	0
制限的	2	2
機密	4	3
危機的	NA（6）	NA（5）
機器		
不必要	0	0
標準	1	2
特殊	3	4
特別注文／複数の特殊	5	6
複数の特別注文	7	8
オープンサンプル		

公開	0	NA
制限的	2	
機密	4	
危機的	NA(6)	

表 15: TEE 攻撃能力

これらの要素の意味と値の範囲は以下の通りである:

- 所要時間
  - これは、識別フェーズと悪用フェーズで費やされる時間である。識別フェーズでの所要時間は、後に多くの TOE において攻撃を実行するため、一度だけの実行に必要なステップに要する時間である。悪用フェーズの所要時間は、攻撃対象の各 TOE に対して実行しなければならないステップに要する時間である。所要時間の範囲は、数時間/1 人から数か月/1 人である。計算上、1 日は約 8 時間、1 週間は約 40 時間、1 か月は約 160 時間とする。

- TOE へのアクセス(対象デバイス)
  - 識別フェーズ及び悪用フェーズで必要な TOE のサンプル数。この値の範囲は、1 から 30 以上までである。

- 専門知識
  - しろうと: 特別な専門知識を持っていない、エキスパートや熟練者と比べて知識量が少ない攻撃者;
  - 熟練者: 製品種別のセキュリティのふるまいに精通しているという点で知識がある;
  - エキスパート: 製品種別で実装される、下位のアルゴリズム、プロトコル、ハードウェア、構造、セキュリティのふるまい、関連するセキュリティ原理と概念、新たな攻撃の定義用の手法とツール、暗号、その製品種別の古典的な攻撃、攻撃手法等に精通している;
  - 複数のエキスパート: 攻撃の各ステップを実行するために多くの分野の専門知識が要求される、例えば、サイドチャネル攻撃の専門知識やソフトウェア攻撃の専門知識等。

- TOE の知識(即ち、仕様、設計データ、ガイダンス証拠資料、ソースコードの知識)
  - 公開: 誰でも利用できる知識;
  - 制限的: 開発者の組織内で管理され(Need to Know の原則で一部の従業員のみがアクセス可能)、秘密保持契約(NDA)の下で他の組織と共有される知識。 開発者の情報セキュリティ方針は、現実の TEE 評価において、このレベルの使用法を正当化するための適切な証拠とみなすことが可能である。TEE セキュリティ評価方法の一部としてサイト監査は一切要求されない;
  - 機密: 開発者の組織内の別個のチーム間(例、セキュリティチームまたは暗号チームのみ)で共有され、アクセスが特定チームの許可されたメンバーに制限される知識。 TOE の機密に関わる知識は、開発者によって実際の資産保護において適用されるセキュリティ対策を信用を得られるようにするような、開発者のサイト監査を要求する。 CC または EMVCo 認証機関からの ISO

27001 適合の独立サイト監査は、その監査が評価中の TEE 資産をカバーするような現実の TEE 評価において、このレベルの使用法を正当化するために受け入れられることが可能である;

- 危機的: わずかな個人のみ(例えば、暗号アルゴリズムにアクセスできる正式な許可を受けた従業員)に知られている知識、そのアクセスは、個別の NDA の下で、厳格な Need to Know の原則で厳しく管理され追跡される。危機的な知識は、識別フェーズ及び悪用フェーズで、それぞれ 6 及び 5 ポイントを提供する。しかし、TOE に関する危機的な知識は、現在の TEE セキュリティ評価方法では到達可能でない(第三者サイト監査は、このレベルに到達するために不十分である)。

ー 機器

- 標準: 脆弱性の識別用または攻撃用のいずれかに、攻撃者が容易に利用可能な状態である。標準的な機器の例には、以下が含まれる:インターネットから利用可能な、またはダウンロード可能なソフトウェアツール、例えば、ソフトウェアデバッガ、プロトコルアナライザ、または PC デバイスプロトコルで欠陥を悪用するルーティングツール。ハードウェア機器は、ターゲットデバイスに接続するための PC クライアント及びケーブルに限定される。

- 特殊: 攻撃者にとって容易に利用可能な状態ではないが、必要以上の努力なしに入手可能である。例えば、電力分析ツール、マイクロプローブ ワークステーション、レーザー機器、またはインターネットを介して接続される数百台の PC の利用。 特殊機器は、インターネットで安く購入できる場合、標準に改訂されるかもしれない。

- 特別注文:特別に製造される必要があるかもしれないため、または機器が特殊であるので、その配付が管理されて、制限さえされているかもしれないため、まだ公共に容易に利用可能ともなっていない。あるいは、機器が非常に高価またはいくつかの特殊な機器ユニットからなるものであるかもしれない;

- 複数の特別注文: 異なる種別の特別注文の機器が攻撃の異なるステップで要求される。

以下の表は、機器のレート付けで利用されなければならない:

機器	**分類**
紫外線エミッター	標準
フラッシュ光	標準
低価格の可視光線顕微鏡	標準
人工気候室	標準
電源	標準
アナログオシロスコープ	標準
PC またはワークステーション	標準
信号分析ソフトウェア	標準
信号生成ソフトウェア	標準
高価格の可視光線顕微鏡とカメラ	特殊
紫外線顕微鏡とカメラ	特殊

マイクロプローブワークステーション	特殊
レーザー機器 [1]	特殊
信号及び機能プロセッサ	特殊
高級デジタルオシロスコープ	特殊
信号アナライザ	特殊
ケミカルエッチング用ツール（湿式）[2]	特殊
ケミカルエッチング用ツール（プラズマ）	特殊
グラインディング用ツール	特殊
設計検証と故障解析ツール	
走査型電子顕微鏡（SEM）	特別注文
電子ビームテスター	特別注文
原子間力顕微鏡（AFM）	特別注文
集束イオンビーム（FIB）	特別注文
新技術設計検証と故障解析ツール	特別注文
ソフトウェアツール	
ソフトウェアツール [3]	標準

表 16：TEE 攻撃の機器のレート付け表

- オープンサンプル

  TEE オープンサンプルは、攻撃者が TA コードをインストール及び実行できるような TEE である。既知の秘密を持つ TEE は、高信頼アプリケーション TA の署名とインストールに必要なプライベート鍵のような極めて重要な秘密を攻撃者が知っているような TEE である。本要素は、悪用フェーズでは重要ではない。

  オープンサンプルには 4 つのクラスある：

  - 公開： 公知のオープンサンプルは、オープンな TOE（TEE）を提供するデバイス／プラットフォームを意味する。即ち、高信頼アプリケーション TA のインストールに制限がなく、誰でもそのデバイス／プラットフォーム上に任意の高信頼アプリケーション TA をコンパイルしインストールするかもしれない、または TOE への特権アクセスが公開され利用可能である（例、NDA も配付の管理もなしに、要求すれば誰でも利用可能）かのいずれかである。既知の秘密を持つサンプルについて、公開レベルは、TOE の公開された知識を持つ誰かによりその秘密を容易に利用可能であることを意味する；

  - 制限的： 限定的オープンサンプルは、詳細なデータシートのような、TOE に関する制限的な知識の提供に用いられる管理と同等の管理レベルでアクセス可能なオープンサンプルを意味する。既知の秘密を持つサンプルに関して、このレベルは、要求者に対するなんらかの制御、例えば、NDA、を伴ってその秘密が配付される状況へ適用する。開発者の情報セキュリティ方針は、現

[1] 既製のレーザー機器は特殊化されている。多くの特許コンポーネントや複数の専門的コンポーネントを含むレーザー設定は特注になる可能性がある。

[2] ケミカルエッチングは特殊機材を使用せず、ドラッグストアで販売されている標準的化学ツールを使って実行することができる。ただし、専用機器は特殊なものに分類される可能性がある。

[3] ソフトウェアツールはすべて標準である。特別に開発されたツールまたは拡張ツールは、専門知識及び時間パラメタを通じてレート付けされるべきである。

実の TEE 評価における本レベルの使用を正当化するための適切な証拠と見なされることが可能である。現在の TEE セキュリティ評価方法の一部としては、サイト監査は一切要求されない;

- 機密: 機密のオープンサンプルは、下位の設計証拠資料のような、TOE の機密の知識の提供に用いられる管理と同等の管理レベルでアクセス可能なオープンサンプルを意味する。既知の秘密を持つサンプルに関して、これは、その秘密が強力な管理とサンプルの追跡を伴う NDA の下で配付され、その NDA の下で、受領する組織が同じレベルで管理を確立するような保証を持ってこれらの秘密を利用可能であることを意味する。機密のレベルは、開発者によって適用されるセキュリティ対策及びオープンサンプルの実際の保護に信頼を得ることを可能にするべきものであるような、開発者のサイト監査を要求する。ISO 27001 適合または CC や EMVCo 認証機関からの独立サイト監査は、TEE オープンサンプルをカバーする監査を提供する現実の TEE 評価の中で本レベルの使用を正当化するために受け入れられることが可能だろう;
- 危機的: 危機的オープンサンプルは、全ソースコード、VHDL、ハードウェアレイアウトのような、TOE の危機的な知識の提供に用いられる管理と同等の管理レベルで、それらがアクセス可能であることを意味する。本レベルの使用は、オープンサンプルはほとんど作られないし、それらの使用は完全に追跡されることも意味する。既知の秘密を持つサンプルについて、これは、その秘密がごく限られた少数の者にだけ知られており、配付されないことを意味する。危機的レベルは、識別フェーズで 6 ポイントが提供される。しかし、本レベルは、現在の TEE セキュリティ評価方法の下では到達可能ではない(第三者サイト監査では不十分である)。

TEE を実装するデバイスのエコシステムにおいて、オープンサンプルの可用性は、しばしば制限的である:SoC ベンダは、通常デバイス全体である程度の制御を実装し、製造者及びオペレータとして、その後のバリューチェーンでも、TEE の所有権を持つことがあり、オープンサンプルが NDA の下でのみ利用可能であるが、オープンサンプルがこのような利害関係者に配付されなければならないとき、追加の制限はないことが、一般的な状況である。

以下の修正が、スマートカードのレート付け表へ導入された:

- TOE のアクセスの範囲は、スマートカード製品への攻撃よりも少ないような攻撃を実行するために必要とされるかもしれない実際のサンプル数(SoC またはデバイス)を考慮して修正された。
- TEE 攻撃能力のレート付け表では TOE の知識の 4 つのレベルがある:公開、制限的、機密、危機的、以下のとおり修正された:
  - TOE に関する制限的知識には、NDA または同様の情報管理方針を要求する;
  - TOE の機密に関わる知識には、追加の独立開発者サイト監査を要求する;
  - TOE に関する危機的な知識には、現在の TEE セキュリティ評価方法では到達可能でない;
  - さらに、多くのハードウェア資源が TEE と REE 間で共有されることを考慮し、TEE が依拠するハードウェアブロックの完全な知識をすでに意味している危機的な知識をもたらすような、TOE に関する非常に危機的なハードウェア設計の知識は削除された;
- オープンサンプルには、4 つのレベルがある:公開、制限的、機密、危機的で、これらは TOE の知識について規定された同じ条件の下での使用が可能である。

TEE 攻撃経路によって要求される攻撃能力は、識別フェーズと悪用フェーズの要素の合計である。本プロテクションプロファイルは、TEE は 21 ポイント未満の攻撃能力値に対抗しなければならないことを意味し、TEE-Low 攻撃能力を持つ攻撃者に対して対抗することを要求する。表 17 は、TEE に適用可能な攻撃能力の階層を提供する。それは、CC v3.1 に定義される表と[APSC]で定義されるスマートカード表と同じ役割を果たす。

攻撃能力値	シナリオを悪用するために 要求される攻撃能力	以下の攻撃能力を持つ攻撃者に TOE は対抗する:
0－15	TEE-Basic	レート付けなし
16－20	TEE-Low	TEE-Basic
21－24	TEE-Moderate	TEE-Low
25－30	TEE-High	TEE-Moderate
31 以上	TEE-High を超える	TEE-High

表 17: TEE 対抗力のレート付け

A.2 攻撃者の悪用プロファイル

本セクションは、GlobalPlatform 高信頼実行環境 TEE が保護すると期待される攻撃者のプロファイルについて記述する。TEE の一般的な目標は、インターネットやその他の手段を通して多くの最終利用者へ攻撃が拡散されることを最小のコストで防止することである。したがって、我々は、識別フェーズと悪用フェーズについての異なる攻撃者プロファイルを検討する。

識別フェーズにおいて、典型的な攻撃者は、より簡単な手段を通してさらに悪用可能な脆弱性を見つけて、例えば、インターネット上で利用可能な脆弱性をソフトウェアに悪用させることによって広範囲に拡散可能にするために、時間と労力を費やすこと、及び非標準のソフトウェアまたはハードウェア手段を利用することに躊躇しないだろう。我々は、ゆえに、識別のために利用される攻撃経路を制限しない。

攻撃の悪用は、通常、識別を実行した攻撃者によって直接／ローカルに実行されることはない。その代り、ー最初の攻撃者、または頻繁に、攻撃の拡散に興味をもっている別のエンティティーのいずれかによってー最終利用者が気付くことなくリモートに、または最終利用者を代行してローカルに、実行されるだろう。我々は、いくつかの悪用プロファイル例を定義する。おそらく悪用フェーズの攻撃者は、識別を実行している攻撃者より、資源に対してさらに多くの制限を受けており、彼が実行する悪用は、ソフトウェア手段と標準的な機器のみを要求するべきである。さらに、最終利用者は、通常彼らのデバイス破壊のリスクがその攻撃から得られる潜在的な利益を上回ると考えるので、非破壊の悪用を用いた攻撃のみが TEE 脅威モデルにおいて現実的であると考えられる。しかし、攻撃対象の秘密が TOE 特有であり TOE の他のインスタンスに対して利用されることができないとき、識別の後に、同じ量の資源を利用する悪用フェーズが続かなければならない。

プロファイルのリストには、リモートの悪用／マルウェア用のプロファイル、及び３つのローカル悪用プロファイル、悪用が最終利用者の主導の下で彼のデバイス上にローカルに実行されるようなものが含まれる。プロファイル 4 は、ハードウェアの悪用を実行可能であることに留意されたい; このような悪用は、21 ポイント以上の攻撃レート付けにつながる;したがって、プロファイル 4 は、頻繁には到達しない。

本文書に記載の、または実際の TEE 評価のフレームワークで定義された任意の攻撃のために、追加の悪用プロファイルが使用されてもよい。

要素	値	悪用プロファイル			
		1 リモート	2 ローカルの しろうと	3 ローカルの 熟練者	4 機材を用いた ローカルの熟練者
所要時間					
＜＝1 時間	0		0		
＜＝1 日	3			3	
＜＝1 週間	4	4			4
＜＝1 か月	6				
＞1 か月	8				
現実的ではない	*				
TOE のアクセス					
1 サンプルのみ	0	0	0	0	0
＜10 サンプル	2				
＜30 サンプル	4				
＞30 サンプル	6				
現実的ではない	*				
専門知識					
しろうと	0		0		
熟練者	2	2		2	2
エキスパート	4				
複数のエキスパート	6				
TOE の知識					
公開	0	0	0	0	0
制限的	2				
機密	3				
危機的	NA(5)				
機器					
なし	0				
標準	2	2	2	2	
専門的	4				4
特別注文／複数の専門的	6				
複数の特別注文	8				
オープンサンプル					
公開	NA				
制限的					
機密					
危機的					
合計		**8**	**2**	**7**	**10**

表 18: 悪用プロファイル 1 から 4 のレート付け

A.2.1 悪用プロファイル 1（リモートの攻撃者）

本悪用プロファイルは、リモート管理されたデバイス上に攻撃を実行すること、または代わりに、普通の最終利用者が簡単にダウンロードして活用するような、便利なローカルツールを作成することに相当する。 攻撃者は、識別を実行したものとは異なる場合、識別フェーズで特定された脆弱性に関する詳細と、識別子によって提供されるローカル攻撃コード／実行ファイルのような最小限のアウトプットを取り出す。 次に、攻撃者は、リモートツールやマルウェアを作成し、フィッシングのような手法を利用し、それを犠牲者によってダウンロードさせ、実行させる、または代わりに、インターネット上で利用可能な非常に簡単で使い易いツールを作成する（ワンストップショップ）。攻撃者は、このようなツールを作成するために熟練者レベルの専門知識が必要であり、ほぼ常にあてはまるような、インターネット上で利用可能な類似のツール／プログラムがあるならば、設計するのに 1 週間程度かかる。攻撃は、自らのアプリケーションまたはツールのコードベースとして利用できる、インターネットから利用可能なソースコードから成る標準的な機器を要求する。新しいマルウェア、トロイの木馬、ウイルス、またはルーティングツール等を設計するとき、既存のベースを再利用するのが標準的やり方である。利用者からの特殊な機器は、一切必要とはされない。

A.2.2 悪用プロファイル 2（ローカルのしろうと攻撃者）

本悪用プロファイルは、最終利用者が攻撃を実行するとともに、ターゲットデバイスへの物理的アクセスを要求しつつ、ローカルデバイス上での攻撃を実行することに対応する。攻撃者は、悪用の実行を可能にする REE への特権アクセスを獲得するために、識別子から例となる攻撃コード／アプリケーションや、ダウンロードしたり、デバイスにジェイルブレイク／ルート／リフラッシュするツールを利用することを要求する攻撃の実行方法に関し書かれたインターネット上のガイドラインを検索する。攻撃者は、誰かがインターネット上に公開し、おそらく拡張された既存のガイドラインに従っているので、特別なレベルの専門知識を持っている必要はない。攻撃には、デバイスに接続された PC と同様に、攻撃者が攻撃の実行に使用するような、インターネットから利用可能なツールからなる標準的な機器が要求される。攻撃には、通常 1 時間未満しか、かからない。

A.2.3 悪用プロファイル 3（ローカルの熟練攻撃者）

本悪用プロファイルは、ターゲットデバイスへの物理的アクセスと熟練レベルの専門知識を要求するとともに、ローカルデバイス上での攻撃の実行に対応する。このレベルの専門知識を持つ最終利用者がいるとしても、悪用のための前提条件は、大きく拡散されるため、悪用のための一般的なローカル攻撃者ではない、おそらく利用者を代行する攻撃者によって攻撃が実行されることを意味する。この悪用の見積りは、専門知識のレベル（熟練者）と所要時間（1 日未満だが、1 時間以上、外部の介入を考慮して）を除き、悪用プロファイル 2 と同じである。

A.2.4 悪用プロファイル 4（機器を用いたローカルの熟練攻撃者）

本悪用プロファイルは、ターゲットデバイスへの物理的アクセスを要求するとともに、最終利用者が、熟練者レベルの専門知識を持っている、特殊なエンティティ（違法なショップ）に自分の代わりに攻撃を実行させるような、ローカルデバイス上での攻撃の実行に対応する。悪用プロファイル 2 と比較して、この攻撃は、より高いレベルの専門知識（熟練者）、機器（特殊）を要求し、より長い時間がかかる（1 週間、最終利用者がデバイスを持ち込んで後で取り戻すような事実についても考慮する）。

A.3 攻撃経路の例

本セクションは、特定の TEE 実装において識別フェーズを成功に導くかもしれない、ハードウェアとソフトウェアの手段をもちいた攻撃経路の例を示す。悪用フェーズは、ここでは記述されない（A.2 で定義される悪用プロファイル参照）。
評価者は、このような識別攻撃経路を考慮しなければならず、TOE の特性によって要求されるとおり、本リストを拡張しなければならない。

A.3.1 ハードウェアベースの攻撃経路

本セクションの目的は、識別フェーズを成功に導くかもしれない、ハードウェア手段に依拠するいつかの攻撃経路を記述することである。

A.3.1.1 サイドチャネル分析攻撃

ここで示される攻撃の目標は、特定の高信頼アプリケーションに属する資産を保護するための高信頼ストレージで使用される暗号鍵を取り出すことである。 その暗号鍵は、例えば、高信頼ストレージの運用中に TEE プラットフォームの電力または電磁的分析を用いて、高信頼ストレージの実装で使用される暗号学的保護を破ることによって取り出される。識別フェーズ用の一般的な要件は、以下を含む:

- 対象とされる鍵を用いて暗号操作を実行する能力;
- 対象とされる鍵を用いて高信頼ストレージによって実行される暗号鍵操作の何千もの対策;
- 高信頼ストレージが基礎とする秘密を効率よく取り出すためのサンプリングを実行するためのオープンサンプルの可用性;
- TEE で高信頼ストレージに利用される暗号方式の専門知識;
- REE 処理に起因するノイズを最小化するための REE の制御;
- SoC もしくはパッケージデバイスの外部から電力消費または電磁輻射を測定し分析する機器、及びデバイスの近傍に配置されたワイヤーコイルまたはアンテナ。

注釈:評価の範囲にあるすべての暗号操作（本 PP の FCS_COP.1 要件参照）は、TEE OS によって内部で使用されるか、API を介して TA に提供されるかのいずれかであり、サイドチャネル分析の潜在的な対象である。

A.3.1.2 故障注入攻撃

故障注入攻撃の目標は、レーザーパルス、EM パルス、または入力信号の異常（クロック、電源、リセット）のような、物理的手段を用いて TOE のふるまいを一時的に破損することである。この種の異常は、コードの実行フローを変えるか、又は攻撃者の利益のため SoC によって処理されたデータの解釈を変えることが可能である。

故障注入攻撃は、署名検証または耐ロールバックチェックのような、TOE においてソフトウェアに実装されるセキュリティチェックを迂回するために利用可能であるが、ハードウェアアクセラレータについても対象とすることが可能であり、それらから故障の結果の事後解析を用いて暗号鍵を抽出するために利用可能である（例えば、差分故障解析）。

識別フェーズの一般的要件は以下を含む:

- TOE の弱点を特定するためのサイドチャネル分析（コードは要求されない）;
- 故障注入攻撃ベンチのセットアップ（例、デジタルオシロスコープ、パルス発生器、故障注入手段）:
  - 標的とされるコンポーネント（SoC または外部 RAM）への物理的アクセスを得るためのデバイスの準備;
  - REE 処理に起因するノイズを最小限にするため、及び TEE 内の実行を制御するため、及びトリガー信号を得るための、REE の制御。

A.3.1.3 外部 DRAM プロービング

この攻撃の目標は、TEE OS 暗号ライブラリを用いて、AES 計算中に暗号鍵の値を取り出すことである。RAM がパッケージの一部ではなく、平文が既知であるという前提条件に基づいて、識別フェーズの一般的要件は以下を要求する:

- RAM バスデータレートを見付けるための TOE サンプルを分析すること;
- RAM データレートをサポートするアナライザ;
- AES 計算中に操作された平文データをローカライズするためバスをプローブすること;
- 鍵を取り出すために平文操作の相関分析を実行すること。

A.3.1.4 保護されていないデバッグ用インタフェース

この攻撃の目標は、ハードウェアデバッグ機器の手段によって TEE メモリ内容を直接アクセスし、読み出しまたは改変すること、及び外部 DRAM プローブ攻撃のようなソフトウェアによって悪用可能な脆弱性を見つけるためにこの特権を使用すること、または実行中に値を改変し、最終的に適切な許可なく特権アクションを実行できるようにすることである。

識別フェーズの一般的要件は以下を含む

- JTAG がアクセスを提供するようなシステムの分析;
- TEE ソフトウェアの分析;
- 脆弱性を発見し、それと関連する悪用を設計するか、または直接 TEE メモリの内容を改変し、例えば許可なしに永続的な値を変更する。

A.3.2 ソフトウェアベースの攻撃経路

本セクションの目的は、識別フェーズを成功に導くかもしれないソフトウェアの手段に依拠する幾つかの攻撃経路について記述する。いくつかの記述は、適切な攻撃ではないが、潜在的な脆弱性を発見する方法であることに留意されたい、例えばファジング及び廃止された API や隠し API の利用など。

A.3.2.1 暗号に対するキャッシュ攻撃

この攻撃の目標は、これらのすべての条件が満たされるようなセットアップで、さまざまな操作のためにTEEによって利用される鍵を取り出すことである:

- TEE と REE が同じキャッシュメモリを共有する;
- 暗号アルゴリズムがソフトウェアに完全に実装される;
- 暗号アルゴリズムがメモリアクセスに依拠する、例えば、参照表。

本攻撃は、キャッシュミスに関する統計を推定し、利用される暗号鍵の情報を入手するために、REE に属するキャッシュメモリの内容を緊密に制御し、TEE に割り当てられたキャッシュメモリの量に関する情報を入手可能とし、TEE 暗号実行回数を測定し、最終的に許可されない操作を実行するための鍵を悪用することによって実行される。

識別フェーズの一般的要件は以下を含む:

- REE へのルートアクセス;
- 使用されるハードウェア資源を含め、包括的な TEE 証拠資料;
- REE デバッギングツール;
- ターゲットのサンプルを取るために TEE 暗号操作を起動させる、テスト TA をロードできるオープンサンプル;
- ターゲットの鍵を用いて暗号操作を実行する能力;
- TEE によって実行される暗号操作についての REE による測定(例、数千回)。

この攻撃で利用されるソフトウェアは、TEE の再起動及び/またはキャッシュライン・エビクションとキャッシュフラッシングの実行により、TEE 側での実行状態がそれぞれの実行において同じであることを保証可能である、そのため、例えば:

- すべてのキャッシュメモリが TEE に属し、監視されているアルゴリズムの実行開始時に一切キャッシュされない。

A.3.2.2 クライアント API または TEE ドライバ上のファジング

この攻撃の目標は、TEE クライアント API [1] または TEE ドライバインタフェースを無効、予測されない、またはランダムデータと共に用いて、予測されない内部状態に達することによって、予測されないふるまいを引き起こし、TEE 実装における脆弱性を見付けることである。

識別フェーズの一般的要件は以下を含む:

- RE への特権アクセス、リモートかもしれない;
- カスタム TA を実装/実行するためのオープンサンプル;
- ファジングツールを実装する、または既存ソフトウェアを TEE に適用するための時間及び資源;
- 攻撃の成功を評価するための TOE についての詳しい知識 ー 例、リッチ OS メモリに書き込むべきバイナリコードをバッファオーバーフローデータに含めることによって ー 、クラッシュ時に攻撃を再起動するための TOE についての詳しい知識。

A.3.2.3 メモリ分離の侵害

この攻撃の目標は、メモリ分離を制御するハードウェアのバグを悪用することによって、TEE メモリの内容に直接アクセスし、改変することである。

識別フェーズの一般的要件は以下を含む:

- 物理的メモリに直接書き込み可能であるような、アクセス制御または分離の規則を迂回または改変するための特権の獲得;
- メモリマッピングまたはリバースエンジニアリングを伴う TEE 証拠資料。

一度、TEE メモリがアクセスされると、ソフトウェアアナライザは、許可なしに TEE 永続的データを改変するために TEE メモリへ何を書き込むかを決定するため、直接的なやり方で TEE コードとデータをリバースエンジニアリングすることに利用される。

A.3.2.4 証明書の構文解析エラー

この攻撃の目標は、攻撃者にセキュアな環境内に欠陥コードを注入することを許容して、不正確に構文解析されるような、奇形の証明書を TEE に提供することである。攻撃は、TEE のアップデート機能、TA プロビジョニング機能または何らかの実装依存のクライアント認証機能をターゲットとするに違いない。

潜在的な脆弱性は、ファジングや限界値を標的とした試行を通して発見されることが予測される、したがって TOE の事前知識は要求されない。

A.3.2.5 既知の脆弱性や診断 API を用いた API／プロトコルの利用

この攻撃の目標は、悪意のあるコードを注入、または TEE へまたは TEE から機密データを抽出したりするために、非推奨や文書化されていないインタフェースを利用することである。攻撃ベクターは、例えば、セキュアでない暗号アルゴリズムに依拠するレガシーな通信プロトコル、またはセキュリティ修正に関して最新に維持されていない独自 API であるかもしれない。

脆弱性は、独自 API で、または文書化されていない機能を利用する既存アプリケーションの検査を通して発見されるかもしれないと予測される。一度、潜在的な脆弱性が特定されても、攻撃者は、まだそれを悪用する方法を発見しなければならない。識別フェーズの一般的要件は、実際の脆弱性を配置可能にするような、デバッグ装置へのアクセスとそれの悪用を設計する能力を含む。