公共交通 IC カードプロテクションプロファイル

Version 1.12

一般社団法人 ID 認証技術推進協会（JICSAP）

[注意事項]
本文書の原文は「Public Transportation IC Card Protection Profile - Version 1.12」（英語）です。本文書は参考資料としてご利用ください。

目次

1　PP 概説

この文書は、日本国内における公共交通 IC カードの CC 評価のためのプロテクションプロファイル（PP）である。
この PP は Common Criteria 評価基準[CC]に準拠して作成されている。
この文書で使用されている用語、略語および参照文献は、 第 0 章 用語と参考文献で定義している。

1.1　PP 識別

この章では、本 PP の情報を説明する。

Table 1: PP 識別

タイトル	公共交通 IC カードプロテクションプロファイル
バージョン	1.12
発行日	2018 年 8 月 1 日
作成者	一般社団法人 ID 認証技術推進協会（JICSAP）
認証者	IT セキュリティ評価及び認証制度（JISEC: Japan Information Technology Security Evaluation and Certification Scheme)

1.2　TOE 概要

TOE は、非接触インタフェース（オプションで接触インタフェース）を持つ IC チップと「PT ソフトウェア」と呼ばれるスマートカードソフトウェアで構成される。TOE は、公共交通 IC カードとして日本国内で使用される。

公共交通 IC カードは、公共交通機関を利用するためにチャージされた運賃、後払いカード、定期券、一日券などとして使用されることを想定している。乗車するために乗客は改札に IC カードをかざし、IC カードから自動的に運賃が引き落とされる。その IC カードは、電車だけでなく、地下鉄やバスでも利用することができる。

公共交通 IC カードは、電子マネー、e チケット、身分証明書など他の目的に使用することもできる。電子マネーサービスでは、ユーザがキオスク、ショッピングセンター、自動販売機さらにインターネットショッピングで素早く買い物をすることができる。e チケットや身分証明書は施設の入り口にあるリーダ／ライタにタッチすることで、ユーザはその施設への入場が許可される。

これらのサービスは日本全国に広く展開されているため、公共交通 IC カードのセキュリティを守ることは大変重要である。また公共交通 IC カードは日本の交通事情からの要求に適応することが期待されている。

日本の公共システムの重要な特性の一つに、ラッシュアワー時に膨大な数の乗客を改札に通す必要があることが挙げられる。したがって、公共交通 IC カードには早い処理性能が求められる。

もう一つの重要ポイントは、全国にある複数の公共交通事業者との相互運用が挙げられる。ある一つの事業者によって発行される公共交通 IC カードは、相互運用合意にもとづいてほかの事業者にも受け入れられる。相互運用だけでなく、各事業者独自のサービス（例えば、乗車回数の多い乗客への割引など）を提供することも可能である。したがって、公共交通 IC カードは、公共交通事業者が提供する様々なサービスに柔軟に対応できるファイルシステムを提供する必要がある。

公共交通事業者は、公共交通 IC カードをチケット販売システムに取り込むことによって、乗車券サービスを提供することができる。公共交通事業者は、乗車券サービスを実現するために、公共交通 IC カードにアクセス権とルールの情報を設定する。この設定により、いろいろな乗車券サービスを可能にする。また、複数の公共交通事業者の乗車園サービスを、一つのカードで実現することが可能である。

1) 乗車券サービスを提供するオペレーションの例を示す。次の図は改札での典型的なオペレーションを示している。
2) 改札がカードを検出する
3) 改札とカードが相互認証を行う

相互認証が成功すると、改札はカードから乗車券情報を読み出す。もし乗車券が有効であれば、改札は必要な情報をカードに書き込み、乗客に対して改札通過を許可する。

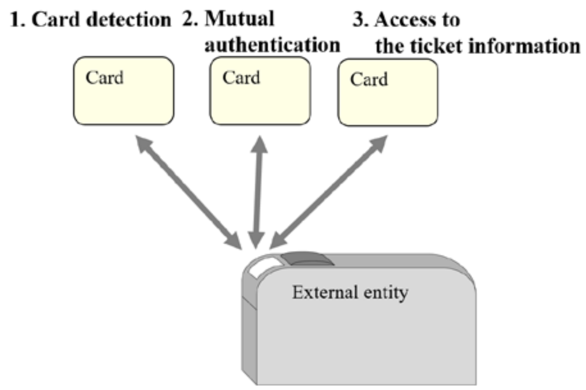

Figure 1: 乗車券サービスのオペレーション例

下の図では、TOE の物理的な範囲（青い部分）を示している。

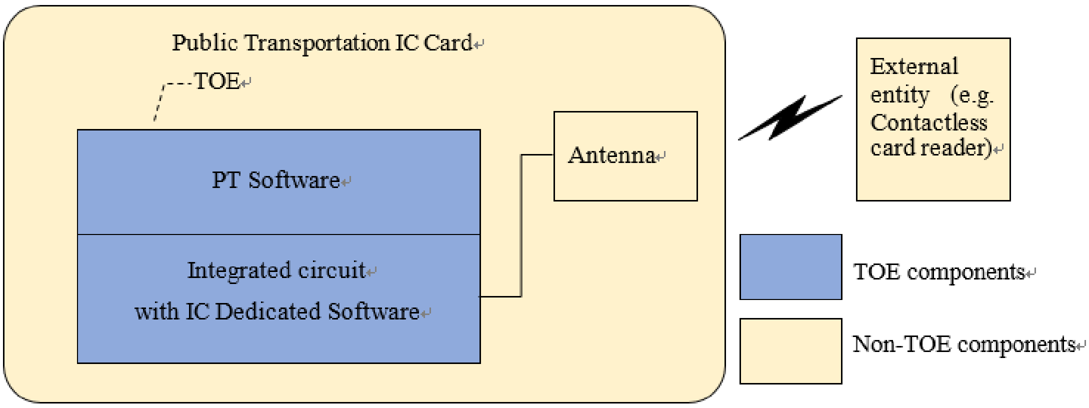

Figure 2: TOE の物理的な範囲

TOE の構成は次の通り:

- 「PT ソフトウェア」は公共交通アプリケーションと、ファイルシステムへのアクセスを提供し管理するオペレーティングシステムで構成される。
- IC（IC 専用ソフトウェア搭載）は、処理装置、暗号のコプロセッサ、セキュリティ構成要素（例えば、TOE を保護するセキュリティ検知器、センサーと回路など）、非接触インタフェース（オプションで接触インタフェース）、揮発性／不揮発性メモリからなるセキュリティ IC である。TOE には、IC 開発者や製造者専用の IC 専用ソフトウェアも含む場合もある。このようなソフトウェアは製造中のテスト目的で使用されたり、ハードウェアを利用するための追加サービス（例えば、暗号ライブラリなど）を提供したりすることもある。

TOE は、一つの TOE 内に異なった目的を持つ複数のデータセットを管理することができる。TOE はツリー形状の Area, Service から構成されるファイルシステムを持つ(Figure 3: ファイルシステム 参照)。TOE のセキュリティ対策は、Area や Service(関連するユーザデータを含む)へのアクセスを保護し、ユーザデータや Access Key などの資産の機密性と完全性を維持することを、目指している。

Service はユーザデータへのアクセスタイプやアクセス条件を定義した Service Attribute を持つ。Service へのアクセスが認証を必要とするという条件であれば、外部エンティティと TOE は Service に紐づけられた Access Key を用いてお互いに認証を行う。認証が成功すると、TOE は外部エンティティに、Service Attribute に指定されたタイプのアクセスを実施することを許可する。このメカニズムにより、未許可のユーザデータへのアクセスを防止する。ユーザデータへのアクセスタイプ・アクセス条件の概要を Table 2 で示す。

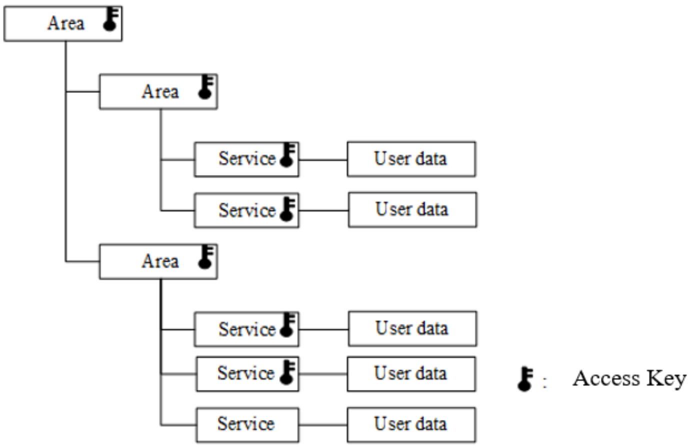

Figure 3: ファイルシステム

Table 2: ユーザデータへのアクセスコントロールレベル

外部エンティティの認証状態	Service Attribute	許可されたオペレーション
認証なし	リードアクセスのみ:認証不要	ユーザデータのリード
	リード/ライトアクセス: 認証不要	ユーザデータのリード/ライト
Service に紐づいている Access Key での認証に成功	リードアクセスのみ:認証要	ユーザデータのリード
	リード/ライトアクセス: 認証要	ユーザデータのリード/ライト

Area は Area と Service の管理オペレーションを定義する。外部エンティティと TOE は Area に紐づけられた Access Key を利用して相互認証する。認証が成功すると、TOE は外部エンティティに対して、管理オペレーション(例えば、Service Attribute の設定)の実行を許可する。

TOE は、CC サポート文書[AAPS]で定義された自己防衛、非バイパス性、ドメイン分割への要求を満たす自己防衛メカニズムを持つ。

TOE は次の機能を提供する:

- カードリーダからのコマンド受信
- カードリーダへのレスポンス送信

TOE は、次のセキュリティ機能を提供する:

- 外部エンティティと TOE 間の相互認証

- Service の管理（Service Attribute の設定）
- TOE 内部に格納されているデータへのアクセスコントロール
- 外部エンティティと TOE 間のセキュアな通信
- TOE 内部に格納されているデータの機密性／完全性保護
- 電源断の防止とロールバック
- 異常な環境に対する保護
- 情報漏えいからの保護
- プロービングや改造からの保護
- 機能の不正利用の防止
- TOE 識別のサポート

これらのセキュリティ機能はハードウェアや PT ソフトウェアによって提供される。

ライフサイクルは 1.3 節で説明する。

TOE の資産については、3.1 節で説明する。

TOE によって対策される脅威、TOE 環境の前提条件、運用環境のセキュリティについては 3.2、3.3 および 3.4 節で説明する。

1.3 ライフサイクル

TOE のライフサイクルは"Security IC Platform Protection Profile with Augmentation Packages" [BSI-PP-0084]で定義されているスマートカードのライフサイクルを使って説明する。ライフサイクルの各フェーズは、次のテーブルにリストアップする:

Table 3: TOE ライフサイクルフェーズ

フェーズ	説明
Phase 1	IC embedded software development
Phase 2	IC development
Phase 3	IC manufacturing
Phase 4	IC packaging
Phase 5	Composite product integration
Phase 6	Personalisation
Phase 7	Operational usage

PT ソフトウェアは、Phase 1 で開発される。IC と IC Dedicated Software は Phase 2 で開発され、Phase 3 で製造される。その後 TOE はウェハやソーンウェハの形状で配送される。TOE はパッケージ製品の形状で配送されることも可能である。この場合、本 PP が対応する保証条件は Phase1,2,3 だけでなく、Phase 4 も含まれる。

「TOE 配送」という言葉は次に示す条件で使われる。

- TOE がウェハやソーンウェハで配送される場合は、Phase3 の後 Phase 4 の前
- TOE がパッケージ製品として配布される場合は、Phase 4 の後 Phase 5 の前

本 PP は、「TOE 配送」までの TOE の開発、製造環境のための保証要件を定義する。

各フェーズの説明は次のとおり:

Phase 1: TOE は PT ソフトウェアを含む。それは、PT ソフトウェア開発者によって、Phase 1 で開発される。

Phase 1 後、PT ソフトウェア開発者は、PT ソフトウェアとパーソナライズ情報（必要であれば）を IC 製造者や IC パッケージ製造者に配布する。

Phase 2: IC 開発（IC 設計と IC Dedicated Software　開発）が IC 開発者によって実施される。

Phase 2 後、IC 設計書と IC Dedicated Software は IC 製造者に配送される。

Phase 3: IC 製造（インテグレーションとフォトマスク製造、IC 製造、IC テスト、初期化、必要であればプレパーソナライゼーション）が IC 製造者によって実施される。

Phase 3 後、TOE はウェハまたはソーンウェハ形状で配送される。

Phase 4: IC パッケージング（セキュリティ IC パッケージング、IC テスト、必要であればプレパーソナライゼーション）が IC パッケージ製造者によって実施される。

Phase 4 後、TOE はパッケージ製品として配送される。

Phase 5: スマートカード製造者は公共交通 IC カード製品に TOE を統合する。スマートカード製造者は、それを Administrator（例えば、公共交通事業者）に配送する。

Phase 6: Administrator（例えば、公共交通事業者）は、ユーザデータ、Service Attribute、Access Keys を TOE のメモリにロードを行うパーソナライズ（TOE を発行する）を実行する。

Phase 7: 公共交通 IC カード製品が一般利用のために乗客に配送される。

1.4　TOE が利用できる TOE 以外のハードウェア／ソフトウェア／ファームウェア

TOE は IC カードとして使用される。TOE の運用は、外部エンティティから供給される電源以外の IT 環境に依存しない。公共交通事業者は目的に応じたカードリーダを用意することが要求される。

1.5　コンポジット評価

コンポジット評価は可能である。ソフトウェアとハードウェアを一体化した公共交通 IC カードのセキュリティ評価を実施する際、ハードウェア部分が評価済みなら、コンポジット評価を適用して評価の重複を避けることができる。コンポジット評価が適用されないときは、公共交通 IC カード全体が評価されるべきである。

2　適合主張

本章は適合主張を説明する。

2.1　CC 適合主張

評価は次に基づく:

- "Common Criteria for Information Technology Security Evaluation", Version 3.1 Release 5 (composed of Parts1-3, [CC Part 1], [CC Part 2], and [CC Part 3])
- "Common Methodology for Information Technology Security Evaluation: Evaluation Methodology", Version 3.1 [CC CEM]

本 PP は次の適合を主張する:

- [CC Part 2] extended
- [CC Part 3] conformance

拡張セキュリティ機能要件は Chapter 5 で説明する。

2.2　PP 主張

この PP は他の PP に適合していない。

本 PP の適合を主張する PP と ST に対して、本 PP への正確適合を要求する。

- “Security IC Platform Protection Profile with Augmentation Packages”, Version 1.0 [BSI-PP-0084]

2.3　パッケージ主張

本 PP において、TOE に適用する保証パッケージは次のとおり:

- Evaluation Assurance Level 5 (EAL5) augmented with ALC_DVS.2 and AVA_VAN.5

3　セキュリティ課題定義

セキュリティ課題定義では、TOE やその運用環境によって実施されるセキュリティ機能を説明する。
本章では以下の項目について説明する。

- プライマリ資産とセカンダリ資産
- TOE によって対策される脅威
- TOE 環境の前提条件
- 組織のセキュリティ方針.

3.1　資産

TOE が保護すべき資産は次のとおり:

- プライマリ資産は、TOE に格納されたユーザデータ
- セカンダリ資産は、プライマリ資産の機密性、完全性を守るために必要となるデータ（例えば、Access Key、PT ソフトウェア、初期化データ、プレパーソナライゼーションデータ）

保護されるべきユーザデータはパーソナライゼーションフェーズで Administrator（例えば、公共交通事業者）によって定義される。TOE はフレキシブルで設定可能なアクセスコントロールシステムを許可し、そのアクセスコントロールポリシーに従ってユーザデータがパブリックなものなのか、または機密性確保する必要があるものなのかを設定する。

3.2　脅威

本節では、TOE が対策するべき脅威を説明する。これらの脅威は TOE やその使用環境、またはその両方によって対策される。

T.Hardware_Attack

攻撃者は IC チップに対して(i)TOE のユーザデータを暴露や不正利用する(ii)TOE のセキュリティ機能を不正利用（探索、バイパス、無効化、変更等）するために、物理的攻撃、パータベーションアタック、サイドチャネルアタックを実行するかもしれない。

T.Logical_Attack

通常利用環境上で、攻撃者が(i)ユーザデータの暴露(ii)認証無しで特定データの変更をするかもしれない。

T.Comm_Attack

攻撃者は(i)通信チャネルと通して送受信されるユーザデータの暴露(ii)通信チャネル上のメッセージの改ざんを実行するかもしれない。

T. Abuse_Func

攻撃者は TOE 配送後に、(i) ユーザデータの暴露または悪用、(ii)セキュリティサービスの悪用(探索、バイパス、無効化、変更等)、(iii)セキュリティ機能の悪用(探索、バイパス、無効化、変更等)、(iv)ユーザデータの暴露や悪用を可能にするために、TOE を不正利用するかもしれない。

3.3　組織のセキュリティ方針

本節では、TOE とその利用環境に適用する組織のセキュリティポリシーについて説明する。

P.Configure

TOE は、特定のビジネスルールを実装するシステムでユーザによって使われるためのツールである。TOE は、どんな資産のためにも必要とされる保護のレベルを呈しないかもしれない。保護のレベルが資産ごとにユーザによってはっきりと指定される手段を、TOE は提供する。

P. Identification

正確な識別が、TOE のために行われなければならない。TOE の各インスタンスがユニークな識別方法を所持することが要求される。

P. TOE_Auth

TOE は外部エンティティを認証することができ、外部エンティティは TOE を認証することができる。

3.4　前提条件

本節では TOE の利用環境における前提条件を説明する。これらの前提条件は、TOE のセキュリティ機能が有効であるために必要なものである。

A.Process

TOE とテストデータの機密性や完全性を維持するために、TOE の製造者は最終ユーザに配送されるまで、セキュアな手続きを実行する。(コピー、修正、保持、窃盗、不正利用などの禁止)

A.Keys

TOE で使用する Access Key は、制御された環境に支えられるシステムによって TOE の外で生成される。たとえば、このシステムでは、弱いキーを除くことを確認する。それから、キーは、安全に TOE に入れられる。鍵生成と管理のプロセスは、十分に保護されていて、制御された環境で実施される。

4 セキュリティ対策方針

本章では、 3 章セキュリティ課題定義に対して、TOE およびその利用環境におけるセキュリティ対策方針を説明する。セキュリティ対策方針は TOE に実装される技術的な対策によるものである。環境のセキュリティ対策方針は、IT 環境や IT 以外の方法で実装された対策である。

4.1 TOE のセキュリティ対策方針

セキュリティ課題として定義された脅威と組織のセキュリティ方針に関して、課題解決のために TOE が対処すべきセキュリティ対策方針を示す。それぞれの対策方針は太字で記される。追加の情報は Application Note として通常のフォントで記される。

O.Hardware_Attack

TOE は、物理的相互作用の計測、ハードウェアへの物理的操作や物理的プロービング、IC チップに保管されているまたは運用されている資産の暴露や改ざん、からの保護を提供する。さらに、信頼性やセキュアな操作が証明およびテストされていない環境下での正しい動作を保証する。

O.AC

TOE は、外部エンティティを認証することができる。また、TOE は、ユーザの所有するまたは責任を持つ資産に対してのアクセスをコントロールする手法を提供する。この対策方針は認証とアクセスコントロールの両面で実現する。

O.Auth

TOE は、外部エンティティを認証することができ、また、外部エンティティに TOE 自身を認証させることができる。

O.Configure

TOE は、Administrator によって明示的に設定させるためのアクセスコントロールの手段を提供する。

O.Comm_Attack

TOE は無線インタフェース(オプションで有線インタフェース)で資産を送受信する。これは盗聴や改ざんが簡単であるとみなされる。したがって TOE は、TOE と外部エンティティ間の通信をセキュアな方法で実現するセキュアチャネルを提供する。セキュアチャネルは、移動中の資産の機密性と完全性を維持する。

O.Abuse_Func

TOE は、TOE 配送後の、(i)コンポジット TOE の重要なユーザデータの暴露(ii)コンポジット TOE の重要なユーザデータの偽造(iii)セキュリティ IC ソフトウェアの悪用(iv)TOE のセキュリティ機能のバイパス、無効化、変更、調査、のための不正利用を防ぐ。詳細については、例えば、IC テストソフトウェアによって提供されるテスト機能に依存する。

O.Identification

TOE は、不揮発性メモリ内に初期データを格納する手段を提供する。初期データ(またはそれらの一部)は TOE 識別に使用される。

4.2 運用環境のセキュリティ対策方針

本節では、TOE 運用環境における技術的または手続き的な要求によって満たさせるセキュリティ対策方針について述べる。各対策方針は太字で記され、追加の情報については application note として通常のフォントで記される。

OE.TOE_Auth

運用環境は認証検証メカニズムをサポートし、TOE の認証参照データを知っている。

OE.Keys

TOE で使用される Access Key は、TOE 外部で生成される（TOE のコントロール下にない）。鍵の生成や管理は、セキュアな方法で実行される。

Application note: 鍵生成や管理のための適切なユーザガイダンスが、TOE 評価で定義されて検証されるべきである。

OE.Process

TOE を扱う環境では、TOE とその製造およびテストデータの機密性と完全性が、TOE 配送時の手順を適切に定めることにより維持される。

4.3 セキュリティ対策方針根拠

本節では、選択されたセキュリティ対策方針が脅威、方針、前提条件の対策として適合しているか説明する。下記のテーブルでは、セキュリティ対策と脅威、方針、前提条件のマッピングを示している。

Table 4:本 PP での脅威、方針、前提条件 vs セキュリティ対策方針

脅威、方針、前提条件	セキュリティ対策方針
T.Hardware_Attack	O.Hardware_Attack
T.Logical_Attack	O.AC
T.Comm_Attack	O.Comm_Attack
T.Abuse_Func	O.Abuse_Func
P.TOE_Auth	O.Auth
	OE.TOE_Auth
P.Identification	O.Identification
P.Configue	O.Configure
A.Keys	OE.Keys
A.Process	OE.Process

選択されたセキュリティ対策方針が脅威、方針、前提条件に対抗するために適合していることを、下記の説明で示す。

対策方針 O.Hardware_Attack、O.Abuse_func（Table4 参照）は、脅威の説明に対して直接的に一致している。 それぞれの説明はクリアであり、対策が有効であれば脅威が取り除けると言える。

対策方針 O.AC は、無許可のアクセスからユーザデータを保護するアクセスコントロールシステムを TOE が実装していることを確認している。したがって、この対策が有効であれば、脅威 T.Logical_Attack は軽減される。

対策方針 O.Configure は、認証された User や Administrator のためのアクセスルールや運用を設定する能力を提供する。したがって、方針 P.Configue はこの対策方針によってカバーされる。

方針 P.TOE_Auth は、認証を提供する対策方針 O_Auth と、認証の検証パートを運用環境の対策方針 OE.TOE_Auth でカバーされている。したがって、P.TOE_Auth は、これらの対策方針でカバーされている。

対策方針 O.Comm_Attack は、TOE と外部エンティティ間に確立されたセキュアチャネルを提供する。このセキュアチャネルは、攻撃や環境状況（例えば、低電圧）の結果にかかわらず、すべての転送されているユーザデータの暴露や完全性エラーかが保護する。したがって、この対策方針が有効であれば、脅威 T.Comm_Attack は軽減される。

対策方針 O.Identification は TOE が一意に特定できる機能をサポートすることを要求している。一意の識別子は、TOE 内に格納されている。一意の識別子は製造環境で生成されているので、製造環境は生成された一意の識別子の完全性をサポートしなければならない。セキュリティ開発環境と製造環境の安全を確実にする技術的な組織の対策は、評価の一部である保証基準に基づいて評価される。したがって、方針 P.Process_TOE は、組織的な対策が関係する限り、この対策方針によってカバーされる。

運用環境の対策方針 OE.Keys と OE.Process は、前提条件 A.Keys とA.Process の説明に対して直接的に一致している。

5　拡張コンポーネント定義

本 PP は次の拡張コンポーネントを定義する。

- FDP_SDC.1 蓄積データ機密性
- FMT_LIM.1　限定された機能
- FMT_LIM.2　限定された可用性
- FAU_SAS.1　セキュリティ監査保管

5.1　FDP_SDC

FDP クラス（ユーザデータ保護）に追加する FDP_SDC.1 ファミリについてここで定義する。

FDP_SDC ファミリ（蓄積データ機密性）は次のように明示される。

FDP_SDC　蓄積データ機密性

ファミリのふるまい

このファミリは、TSF で守られているメモリに蓄積されている利用者データの機密性の保護に関する要件を提供する。TSF は特別なインタフェースからのメモリへのデータアクセスを提供し、そのインタフェースをバイパスすることを防止している。蓄積データの完全性を保証する FDP_SDI ファミリを補足している。

コンポーネントのレベル付け

FDP_SDC.1　　特定のメモリにあるユーザデータ情報の機密性を保護することを要求する。

管理:　FDP_SDC.1

予見される管理アクティビティはない。

監査:　FDP_SDC.1

監査対象事象はない。

FDP_SDC.1　蓄積データの機密性

下位階層:　なし

依存性:　なし

FDP_SDC.1.1 TSF は[割付: memory area]に蓄積されているユーザデータ情報の機密性を保証しなければならない。

5.2 FMT_LIM

TOE の IT セキュリティ機能要件を定義するために、FMT クラス(セキュリティ管理)へ追加ファミリ(FMT_LIM)を定義する。このファミリは、TOE のテスト機能への機能要件を説明している。この新しい機能要件は TSF のセキュリティ管理に対応するため FMT クラスに定義される。TOE で使われるセキュリティメカニズムの例は(6.1 節参照)は、機能を限定することや可用性を限定することによって機能の不正利用を防止する特定の問題に対応するために適用される。

ファミリ"制限された機能および可用性"は次のように明示される。

FMT_LIM 制限された機能および可用性

ファミリのふるまい

このファミリは、複合的な方法で機能と可用性を制限する要件を定義する。FDP_ACF ファミリは機能へのアクセスを制限するのに対し、このファミリの構成要素である制限された機能はが機能自身へ特定の方法で設計されることを要求するのに対し、点に注意すること。

コンポーネントのレベル付け

FMT_LIM.1 限定された機能は、TSF が本来の目的のためだけに必要な機能(アクションを実行する、情報を集める)だけを提供するために尽くされることを要求する。

FMT_LIM.2 限定された可用性は、機能の使用(FMT_LIM.1 参照)を制限することを要求する。これは例えば、TOE のライフサイクルの特定のフェーズで機能を消すまたは無効化することによって達成される。

管理: FMT_LIM.1, FMT_LIM.2

予見される管理アクティビティはない。

監査: FMT_LIM.1, FMT_LIM.2

監査対象事象はない。

FMT_LIM.1 限定された機能

下位階層: なし

依存性: FMT_LIM.2 限定された可用性

FMT_LIM.1.1 TSF は、"限定された可用性(FMT_LIM.2)"とともに以下の方針[割付:限定された機能ポリシー]を実施するようなその能力を制限する方法で設計されて実装されなければならない。

FMT_LIM.2 限定された可用性

下位階層:　なし.

依存性: FMT_LIM.1 限定された機能

FMT_LIM.2.1　TSF は、"限定された機能（FMT_LIM.1）とともに以下の方針[割付：限定された可用性ポリシー]を実施するようなその可用性を制限する方法で設計されなければならない。

Application Note:　機能要件 FMT_LIM.1 および FMT_LIM.2 は、同じ機能に関連した同じ方針、またはお互いをサポートする方針を実現する 2 種類のメカニズム（機能の制限と可用性の制限）があると仮定する。これは例えば次を許容する：

(i) TSF はユーザ環境での製品に制限なしで提供されるが、その機能はポリシーが実施され制限される。

(ii) TSF は高い機能性で設計されているが、ユーザ環境における製品では削除されるか無効化されている。

5.3　FAU_SAS

TOE のセキュリティ機能要件を定義するために、FAU クラス（セキュリティ監査）へ追加ファミリ（FAU_SAS）を定義する。このファミリは、監査データの保管への要求を明示する。TOE 自身によって生成されたデータへの要求や監査記録の内容の詳細を与える必要はないため、FAU_GEN より一般的なアプローチである。

ファミリ FAU_SAS"監査データ保管"は次のように明示される。

FAU_SAS 監査データ保管

ファミリのふるまい

このファミリは、監査データの保管への機能要求を定義する。

コンポーネントのレベル付け

FAU_SAS 監査データ保管 ― 1

FAU_SAS.1　　監査データの保管という可能性を提供することを TOE に要求する。

管理:　FAU_SAS.1

予見される管理アクティビティはない。

監査:　FAU_SAS.1

監査対象事象はない。

FAU_SAS.1 監査保管

下位階層:　なし

依存性:　　なし

FAU_SAS.1.1 TSF は、[割付：不揮発性のメモリの種類]内に、[割付: 監査情報のリスト]を保管する能力をもつ[割付: サブジェクトのリスト]を提供する。

6 セキュリティ要件

IT セキュリティ要件は次を含む:

- セキュリティ機能要件 (SFRs)
  これは、フローコントロルは、識別そして認証のようなセキュリティ機能への要求である。
- セキュリティ保証要件(SARs)
  TOE がセキュリティ対策方針（構成管理、テスト、脆弱性評定などのような）に適合しているか保証を取得する方法を記述する
- さらにこれらの要求について詳細に説明する。
  - セキュリティ機能要件根拠
  - セキュリティ保証要件根拠

6.1 セキュリティ機能要件

セキュリティ対策方針は、セキュリティ機能要件(SFRs)のセットである。

セキュリティ機能要件で私用される表記法について、以下に説明する:

- 要求がより簡単に読みやすく理解し易いように、多くのケースで書き換えを行っている。
- PP 作成者によって選択されたものはアンダーラインテキストで表示する。ST 作成者によって選択されるべき項目は、[選択:]の中にイタリックで表示される。
- PP 作成者によって決定された割付は、アンダーライン＋太字によって表示される。ST 作成者によって割付を行う必要があるときは、[割付:]の中にイタリックで表示される。いくつかのケースでは、PP 作成者が ST 作成者に選択できるように作られた割付が存在する。これは、アンダーライン＋イタリックで表示される。

FDP_SDC.1 蓄積データの機密性

FDP_SDC.1.1 TSF は[割付: *memory data*]に蓄積されているユーザデータ情報の機密性を保証しなければならない。

Application note: ST 作者は memory data に対しセキュアなメモリを割付けるべきである。一般的に ROM はセキュアなメモリとはみなされない。

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、[割付: *利用者データ属性*]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利用者データを監視しなければならない。

FDP_SDI.2.2 データ完全性誤り検出時に、**TSF** は**[割付:** *とられるアクション*]を行なわねばならない。

FPT_PHP.3 物理的攻撃への抵抗

FPT_PHP.3.1 **TSF** は、**SFR** が常に実施されるよう自動的に対応することによって、<u>**TOE のハードウェアおよび TSF を構成するソフトウェア**</u>への<u>**物理的マニピュレーションや物理的プロービング**</u>に抵抗しなければならない。

Refinement: TSF は、物理的マニピュレーションや物理的プロービングへの対策に適切な技法を実装する。
これらの攻撃（特にマニピュレーション）の性質のために、TSF がその要素の全てへの攻撃を決して見つけることができるというわけではない。
したがって、セキュリティ機能的な必要条件が実施されることを確実として、これらの攻撃に対する永続的な保護は必要とされる。
それゆえに、「自動的に対応する」は(i)攻撃がいつでもあるかもしれない (ii)対抗策はいつでも提供される、と仮定することを意味する。

FDP_ITT.1 基本内部転送保護

FDP_ITT.1.1 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<u>暴露</u>を防ぐための **<u>Data Processing Policy</u>** を実施しなければならない。

Refinement: TOE（例えば暗号のコプロセッサ）の異なるメモリ、CPU と他の機能単位は、TOE の物理的に切り離された部分とみなされる。

FPT_ITT.1 基本 TSF 内データ転送保護

FPT_ITT.1.1 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<u>暴露</u>から保護しなければならない。

Refinement: TOE（例えば暗号のコプロセッサ）の異なるメモリ、CPU と他の機能単位は、TOE の物理的に切り離された部分とみなされる。

FDP_IFC.1 サブセット情報フロー制御

FDP_IFC.1.1 TSF は、**<u>TOE によって処理または移動されるすべての機密データ</u>**に対して **<u>Data Processing Policy</u>** を実施しなければならない。

Application Note: ST 作者は ST にて以下の Data Processing Policy を定義すべきである。

”サブセット情報フロー制御 (FDP_IFC.1)”の要件として以下のセキュリティ機能ポリシー (SFP) を定義する:

”TOE のユーザデータおよび TSF データは、PT ソフトウェアが外部インタフェースを経由した TOE のユーザデータとの通信を決定した場合を除き、TOE からアクセスできてはならない。保護は PT ソフトウェアによってコントロールされた属性の区別なしに機密データに対してのみ適用されなければならない。

FRU_FLT.2 制限付き耐障害性

FRU_FLT.2.1 TSF は、以下の障害が生じたとき、すべての TOE 機能(capabilities)の動作を保証しなければならない: **<u>障害：FPT_FLS.1 の要求に従っていることが検出できない動作状況の露見</u>**

Refinement: 上記の“Failure”は”状況”を意味する。TOE は、上で定義された”状況”のために障害を防ぐ。

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くてはならない。**<u>障害：FRU_FLT の要求に耐性がない、つまり機能不全が起きるような動作状況の露見</u>**.

Refinement: 上記の“Failure”は”状況”を意味する。TOE は、上で定義された”状況”のために障害を防ぐ。

FTP_ITC.1 TSF 間高信頼チャネル

FTP_ITC.1.1 TSF は、それ自身と他の高信頼 IT 製品間に、他の通信チャネルと論理的に区別され、その端点の保証された識別、及び改変や暴露からのチャネルデータの保護を提供する通信チャネルを提供しなければならない。

FTP_ITC.1.2 TSF は、<u>他の高信頼 IT 製品</u>が、高信頼チャネルを介して通信を開始するのを許可しなければならない。

FTP_ITC.1.3 TSF は、[割付: *高信頼チャネルが要求される機能のリスト*]のために、高信頼チャネルを介して通信を開始しなければならない。

FMT_SMR.1 セキュリティの役割

FMT_SMR.1.1 TSF は、役割 **<u>User and Administrator</u>** を維持しなければならない。

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

FIA_UID.1 識別のタイミング

FIA_UID.1.1 TSF は、利用者が識別される前に利用者を代行して実行される **<u>Polling, Public_read, Public_write および [選択: *[割付: 他の TSF 仲介アクション], なし*]</u>** を許可しなければならない。

FIA_UID.1.2 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、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。

Application note: ST作者は識別および認証を必要とするTSF仲介アクションを割付けるべきではない。

Application note: Polling はカードを検出するアクションである。Public_read は認証を必要としないユーザデータファイルからの読出し操作である。Public_write は認証を必要としないユーザデータファイルへの書き込み操作である。

FIA_UAU.1 認証のタイミング

FIA_UAU.1.1 TSF は、利用者が認証される前に利用者を代行して行われる **<u>Polling, Public_read, Public_write および [選択: *[割付: 他の TSF 仲介アクション], なし*]</u>** を許可しなければならない。

FIA_UAU.1.2 TSF は、その利用者を代行する他のすべての TSF 仲介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。

Application note: ST作者は識別および認証を必要とするTSF仲介アクションを割付けるべきではない。

Application note: Polling はカードを検出するアクションである。Public_read は認証を必要としないユーザデータファイルからの読出し操作である。Public_write は認証を必要としないユーザデータファイルへの書き込み操作である。

FIA_UAU.4 単一使用認証メカニズム

FIA_UAU.4.1 TSF は、**<u>[割付: 識別された認証メカニズム]</u>**に関係する認証データの再使用を防止しなければならない。

Application note: ST 作者は認証メカニズムとして、一般的に強い認証として認知されないものを割付けるべきではない。認証メカニズムは暗号アルゴリズムを利用することがある。認証データには乱数発生器が必要されるかもしれない。

FDP_ACC.1 サブセットアクセス制御

FDP_ACC.1.1 TSF は以下のリストに対して **<u>Service Access Policy</u>** を実施しなければならない。

- **<u>サブジェクト: Table 5 で示されるサブジェクト</u>**
- **<u>オブジェクト: Table 5 で示されるオブジェクト</u>**
- **<u>操作: Table 5 で示される操作</u>**

FDP_ACF.1　セキュリティ属性によるアクセス制御

FDP_ACF.1.1　TSF は以下に基づいて、オブジェクトに対して **Service Access Policy** を実行しなければならない。

- **サブジェクト: Table 5 で示されるサブジェクト**
- **オブジェクト: Table 5 で示されるオブジェクト**
- **サブジェクトとオブジェクトに対する SFP 関連セキュリティ属性: Table 5 で示されるセキュリティ属性"認証ステータス"およびセキュリティ属性"ACL"**

FDP_ACF.1.2　TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、次の規則を実施しなければならない:

- **サブジェクトは次の場合において、オブジェクト上でこの操作をすることができる ： サブジェクトが認証され、対応する操作が Table 5 に列挙されている。**

FDP_ACF.1.3　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　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

Table 5: Service Access Policy

サブジェクト	セキュリティ属性"認証ステータス"	オブジェクト	セキュリティ属性"ACL"	操作
User を代表するプロセス	未認証	ユーザデータファイル	リードオンリー、認証不要	リード
User を代表するプロセス	未認証	ユーザデータファイル	リード／ライト、認証不要	リードまたはライト
User を代表するプロセス	Service に対する Access Key の認証に成功している	ユーザデータファイル	リードオンリー、Service に対応する Access Key の認証が必要	リード
User を代表するプロセス	Service に対する Access Key の認証に成功している	ユーザデータファイル	リード／ライト、Service に対応する Access Key の認証が必要	リードまたはライト

FMT_MSA.1　セキュリティ属性の管理

FMT_MSA.1.1　TSF は、セキュリティ属性 **ACL** に対し**設定および [選択: その他の操作、なし]**をする能力を **Administrator** に制限する **Service Access Policy** を実施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することができなければならない。：**セキュリティ属性の管理**

FMT_LIM.1　限定された機能

FMT_LIM.1.1　TSF は、"限定された有効性(FMT_LIM.2)"とともに以下の方針を実施するようなその能力を制限する方法で設計されて実装されなければならない。**方針:TOE 配布後に、コンポジット TOE のユーザデータの暴露や改ざん、TSF データの暴露や改ざん、改造されたソフトウェア、他の攻撃を可能とする可能性のある収集された実体のない TSF の構成情報を許可するようなテスト機能を展開しない。**

FMT_LIM.2　限定された可用性

FMT_LIM.2.1　TSF は、"限定された機能(FMT_LIM.1)とともに以下の方針を実施するようなその可用性を制限する方法で設計されなければならない。**方針:TOE 配布後に、コンポジット TOE のユーザデータの暴露や改ざん、TSF データの暴露や改ざん、改造されたソフトウェア、他の攻撃を可能とする可能性のある収集された実体のない TSF の構成情報を許可するようなテスト機能を展開しない。**

FAU_SAS.1　監査保管

FAU_SAS.1.1　TSF は、[割付:*不揮発性のメモリの種類*]内に、[*選択: 初期データ、[割付: 他のデータ、なし]*]を保管する能力をもつ **TOE 配布前のテストプロセス**を提供する。

6.2　セキュリティ保証要件

TOE への保証要件は評価保証レベル 5(EAL5)を利用し、拡張コンポーネントとして ALC_DVS.2 および AVA_VAN.5.を利用する。その保証要件は次のテーブルで示す。

Table 15: セキュリティ保証要件

保証クラス	保証コンポーネント
開発	ADV_ARC.1
	ADV_FSP.5
	ADV_IMP.1
	ADV_INT.2
	ADV_TDS.4
ガイダンス文書	AGD_OPE.1
	AGD_PRE.1
ライフサイクルサポート	ALC_CMC.4
	ALC_CMS.5
	ALC_DEL.1
	ALC_DVS.2
	ALC_LCD.1
	ALC_TAT.2
セキュリティターゲット評価	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
テスト	ATE_COV.2
	ATE_DPT.3

保証クラス	保証コンポーネント
	ATE_FUN.1
	ATE_IND.2
脆弱性評定	AVA_VAN.5

6.3 セキュリティ機能要件根拠

下記のテーブルは、選択されたセキュリティ機能要件（SFR）がどのセキュリティ対策方針に適合しているかを示している:

Table 17: セキュリティ対策方針 vs TOE セキュリティ機能要件

Objective	TOE Security Functional Requirements
O.Hardware_Attack	- FDP_SDC.1 “蓄積データ機密性” - FDP_SDI.2 “蓄積データ完全性監視およびアクション” - FPT_PHP.3 “物理的攻撃への抵抗” - FDP_ITT.1 “基本内部転送保護” - FPT_ITT.1 “基本 TSF 内データ転送保護” - FDP_IFC.1 “サブセット情報フロー制御” - FRU_FLT.2 “制限付き耐障害性” - FPT_FLS.1 “セキュアな状態を保持する障害”
O.AC	- FIA_UID.1 “識別のタイミング” - FIA_UAU.1 “認証のタイミング” - FIA_UAU.4 “単一使用認証メカニズム” - 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”
O.Auth	- FIA_UID.1 “識別のタイミング” - FIA_UAU.1 “認証のタイミング” - FIA_UAU.4 “単一使用認証メカニズム” - FTP_ITC.1 “TSF 間高信頼チャネル”
O.Configure	- FMT_SMR.1 “セキュリティの役割” - FMT_MSA.1 “セキュリティ属性の管理” - FMT_SMF.1 “管理機能の特定”
O.Comm_Attack	- FTP_ITC.1 “TSF 間高信頼チャネル”
O.Abuse_Func	- FMT_LIM.1 “制限された機能” - FMT_LIM.2 “制限された可用性”
O.Identification	- FAU_SAS.1 “監査保管”

対策方針 O.Hardware_Attack は、TOE が処理中と内部間転送においてユーザデータと TSF データを保護することによって、FDP_ITT.1, FPT_ITT.1 and FDP_IFC.1 によって達成される物理的相互作用による保護を提供する。リバースエンジニアリングやハードウェアへの細工に対する保護は、FPT_PHP.3 によって達成される。ユーザデータの暴露や改ざんに対する保護は、FPT_PHP.3 のサポートにより FDP_SDC.1 and FDP_SDI.2 によって達成される。機能不全時の障害許容を要求する FRU_FLT.2 や機能不全時でもセキュア状態を保持する FPT_FLS.1 によって、故障時の保護がカバーされる。

対策方針 O.AC は、アクセスコントロール方針を特定する FDP_ACC.1 と FDP_ACF.1 によって達成される。アクセスコントロールシステムの処理は、毎回ユニークな認証セッションを張る FIA_UAU.4 にサポートされる。SFR FIA_UID.1 は FIA_UAU.1 は相互認証なしで特定の機能を実行することを許可することにより、アクセスコントロールシステムの処理を補足している。

対策方針 O.Auth は、SFR FMT_ITC.1、FIA_UAU.4、FIA_UID.1 および FIA_UAU.1 により達成される。これらの SFR は提供する FMT_SMF.1 の結合により達成される。これらの SFR は TOE と外部エンティティ間のセキュアチャネル上の相互認証を提供する。

対策方針 O.Configure は、SFR FMT_SMR.1 および FMT_MSA と FMT_SMF.1 の結合により達成される。これらの SFR は柔軟で設定可能なアクセスコントロールシステムおよびアクセスコントロール設定機能の利用が許可される役割を指定する。

対策方針 O.Comm_Attack は、TOE と外部デバイスとの間のセキュリティチャネルへの要求 FTP_ITC.1 により達成されている。

対策方針 O.Abuse_Func は、TOE 配送後の攻撃者による不正利用から保護するために、機能の有効性と能力を制限した FMT_LIM.1 and FMT_LIM.2 により達成される。

対策方針 O.Identification は FAU_SAS.1 により達成される。初期データ(あるいはその中の一部)は TOE 識別のために使われる。初期値を格納する TOE の技術的な能力は、FAU_SAS.1 に従って提供される。

SFR の依存性について、次の表で説明する。

Table 18: セキュリティ機能要件依存性

ID	セキュリティ機能要件	依存性	備考
FDP_SDC.1	蓄積データ機密性	なし	
FDP_SDI.2	蓄積データ完全性監視およびアクション	なし	
FPT_PHP.3	物理的攻撃への抵抗	なし	
FDP_ITT.1	基本内部転送保護	FDP_ACC.1 or FDP_IFC.1	含まれる (FDP_ACC.1)
FPT_ITT.1	基本 TSF 内データ転送保護	なし	
FDP_IFC.1	サブセット情報フロー制御	FDP_IFF.1	含まれない (下記の考察を参照)
FRU_FLT.2	制限付き耐障害性	FPT_FLS.1	含まれる
FPT_FLS.1	セキュアな状態を保持する障害	なし	
FMT_SMR.1	セキュリティの役割	FIA_UID.1	含まれる
FIA_UID.1	識別のタイミング	なし	
FIA_UAU.1	認証のタイミング	FIA_UID.1	含まれる
FIA_UAU.4	単一使用認証メカニズム	なし	
FDP_ACC.1	サブセットアクセス制御	FDP_ACF.1	含まれる
FDP_ACF.1	セキュリティ属性によるアクセス制御	FDP_ACC.1 FMT_MSA.3	含まれる 含まれない (下記の考察を参照)
FMT_MSA.1	セキュリティ属性の管理	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	含まれる (FDP_ACC.1) 含まれる 含まれる
FMT_SMF.1	管理機能の特定	なし	

ID	セキュリティ機能要件	依存性	備考
FTP_ITC.1	TSF 間高信頼チャネル	なし	
FMT_LIM.1	制限された機能	FMT_LIM.2	含まれる
FMT_LIM.2	制限された可用性	FMT_LIM.1	含まれる
FAU_SAS.1	監査保管	なし	

CC Part2 では、FDP_IFC.1 の依存性として FDP_IFF.1 が定義されている。FDP_IFF.1 の仕様は、SFR の性質を捉えず詳細も加えられていない。FDP_IFC.1 に記載の Data Processing Policy に述べられたように、どんな属性も必要としない。TOE のセキュリティ機能要件は FDP_ITT.1 と Data Processing Policy（FDP_IFC.1)を使うことで、十分に説明可能である。

FMT_MSA.3 は FDP_ACF.1 の依存性である。しかしこの TOE では、セキュリティ属性は常に明確に設定されるため「デフォルト値」の概念が存在しない。セキュリティ属性は、常に例外なく Administrator によってそれぞれの資産に適切な値に設定されるので、このシステムは FMT_MSA.3 がなくてもセキュアでなくなることはないというのが我々の意見である。したがって、この PP には FMT_MSA.3 を含める必要がない。

6.4 セキュリティ保証要件根拠

顧客の保証期待に適合するため、保証レベルは EAL5 ALC_DVS.2 および AVA_VAN.5 追加を選択する。EAL5 は、高い価値のある資産の保護を期待される TOE に対して十分な保証を提供する。追加保証コンポーネント ALC_DVS.2 と AVA_VAN.5 については、次に説明する:

- ALC_DVS.2 セキュリティ手段の十分性:

  TOE とユーザデータの機密性と完全性を維持する十分な保護レベルの提供を検証するため、本 PP では ALC_DVS.1 ではなく、ALC_DVS.2 を選択する。

- AVA_VAN.5 高度な系統的脆弱性分析:

  TOE は大学の研究所のような高い攻撃能力をもつ攻撃者を想定する。したがって、TOE がそのような攻撃に対して高水準の対策を持つことを確認するために AVA_VAN.5 を選択する。

追加した SAR の依存性は、[CC Part3]で説明されている。次の table では、追加した SAR 依存性と依存性を満たす根拠を示す。

Table 21: EAL5 に追加されたセキュリティ保証要件の依存性

ID	セキュリティ機能要件	依存性	備考
ALC_DVS.2	セキュリティ手段の十分性	なし	
AVA_VAN.5	高度な系統的脆弱性分析	ADV_ARC.1 ADV_FSP.4 ADV_TDS.3 ADV_IMP.1 AGD_OPE.1 AGD_PRE.1 ATE_DPT.1	依存性は保証コンポーネント EAL5 (ADV_ARC.1, ADV_FSP.5, ADV_TDS.4, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1 and ATE_DPT.3).によってカバーされる

7　用語と参考文献

この章では、用語と参考文献を定義する。

7.1　用語定義

本文書で使用している用語について定義する:

Administrator

TOE 発行の責任をもつエンティティ。ほとんどのケースでは、公共交通事業者を表す。

Access Key

Area または Service に対応する鍵

Area

ファイルシステムの一部。Area は通常のファイルシステムのディレクトリの役割と似ている。

Card reader

TOE とのインタフェースである非接触(または接触)リーダライタ

IC Dedicated Software (IC 専用ソフトウェア)

セキュリティ IC に搭載される専用のソフトウェア。(必要に応じて)IC 開発者によって開発される。そのようなソフトウェアはテスト目的またはハードウェアの利用を容易にする、およびまたは、付加的なサービスを提供するために必要とされる。

Initialisation Data(初期データ)

IC 製造者によって定義され、TOE を識別し IC の製造を追跡するための初期データ。

Passenger(乗客)

チケットサービスを利用する人

Pre-personalisation Data

PT ソフトウェア開発者により提供され、IC 製造者または IC パッケージ製造者によって不揮発性メモリに注入されるデータ

PT Software(PT ソフトウェア)

公共交通アプリケーションおよびオペレーティングシステムを提供する組み込みソフトウェア

Public Transportation Operator(公共交通事業者)

Passenger に特定のサービスを提供するエンティティ

Service

データにアクセスする方法を規定する情報を含むファイルシステムの一部。Service は通常のファイルシステムのファイルの役割と似ている。

Service Attribute

Service を経由したユーザデータへのアクセス種別を定義する属性

Ticket Service（チケットサービス）

TOE により Passenger に対して技術的に可能となる特定のサービス。それぞれのチケットサービスは公共交通事業者によって Passenger に提供される。

User

TOE によって提供される Area と Service を利用するエンティティ。改札が User の代表例である。Administrator も参照のこと。

7.2 略語

次のテーブルはこの文書で使われる略語について定義する:

Table 29: 略語定義

略語	定義
ACL	Access Control List
CC	Common Criteria
OS	Operating System
PP	Protection Profile
RF	Radio Frequency
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

7.3 参考文献

以下にこの文書が参考にしている文書を列挙する:

[AAPS] “Joint Interpretation Library Application of Attack Potential to Smartcards”, Version 2.9, January 2013

[BSI-PP-0084] "Security IC Platform Protection Profile with Augmentation Packages", Version 1.0, January 2014

[CC Part 1] "Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model", Version 3.1, Revision 5, April 2017

[CC Part 2] "Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components", Version 3.1, Revision 5, April 2017

[CC Part 3] "Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components", Version 3.1, Revision 5, April 2017

[CC CEM] "Common Methodology for Information Technology Security Evaluation: Evaluation Methodology", Version 3.1, Revision 5, April 2017

公共交通 IC カードプロテクションプロファイル

Version 1.12

一般社団法人 ID 認証技術推進協会（JICSAP）