# 認 証 報 告 書

東京都文京区本駒込2丁目28番8号
独立行政法人情報処理推進機構
理事長　富田　達夫

原紙押印済

## プロテクションプロファイル（PP）

| | |
|---|---|
| 申請受付日（受付番号） | 平成30年4月2日（IT認証8666） |
| 認証識別 | JISEC-C0612 |
| プロテクションプロファイル名称／識別 | Public Transportation IC Card Protection Profile |
| プロテクションプロファイルバージョン | 1.12 |
| プロテクションプロファイル開発者 | 一般社団法人 ID認証技術推進協会 |
| プロテクションプロファイル申請者 | 一般社団法人 ID認証技術推進協会 |
| 要求する保証要件 | EAL5 + ALC_DVS.2, AVA_VAN.5 |
| ITセキュリティ評価機関の名称 | 株式会社 ECSEC Laboratory 評価センター |

上記のPPについての評価は、以下のとおりであることを認証したので報告します。

平成30年8月22日

セキュリティセンター セキュリティ技術評価部
技術管理者　佐藤　眞司

**評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。**

① Common Criteria for Information Technology Security Evaluation Version 3.1 Release 5
② Common Methodology for Information Technology Security Evaluation Version 3.1 Release 5

**評価結果：合格**

「Public Transportation IC Card Protection Profile」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証等に関する要求事項に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

# 目次

# 1 全体要約

この認証報告書は、一般社団法人 ID 認証技術推進協会が開発した「Public Transportation IC Card Protection Profile Version 1.12」（以下「PP[9]」という。）について株式会社 ECSEC Laboratory 評価センター（以下「評価機関」という。）が平成 30 年 8 月に完了した IT セキュリティ評価に対し、その内容の認証結果を申請者である一般社団法人 ID 認証技術推進協会に報告するとともに、PP[9]に関心を持つ調達者や消費者に対しセキュリティ情報を提供するものである。

本認証報告書は、PP[9]に適合した製品開発を行う開発者及び製品調達者を読者と想定している。本認証報告書は、PP[9]が適合する保証要件に基づいた認証結果を示すものであり、個別の IT 製品そのものを保証するものではないことに留意されたい。

また、本認証報告書の読者は PP[9]を併読されたい。特に、PP[9]が TOE に対して要求するセキュリティ機能要件、保証要件及びその背景となるセキュリティ課題について、詳述されている。

本認証報告書で使用する用語については、8 章を参照されたい。

## 1.1 評価PP

PP[9]の概要を以下に示す。詳細は 2 章以降を参照のこと。

### 1.1.1 PP概要

PP[9]は、日本の Public Transportation IC Card として使用される IC のセキュリティ要件を規定するものである。

PP[9]に適合する TOE は、必要なソフトウェアを含む Public Transportation IC Card である。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 と、Smart Card Embedded Software（以下「PT Software」という。）で構成される。

TOE は、チケットサービスとして鉄道やバスに乗る時の電子チケット、一日乗車券、定期券だけでなく、電子マネーや ID カードとしてのサービスも提供できる。またオペレータは、他のオペレータとの互換性を確保しつつ独自のサービスを提供できる。これらのマルチアプリケーションサービスを提供するため、TOE は柔軟なファイルシステムを提供し、オペレータは TOE 内部のデータに対するアクセス権やアクセスルールを設定することができる。

図 1-1 にチケットサービスが提供する代表的なオペレーションを示す。図 1-2 には、PP[9]が想定する TOE と TOE 外のコンポーネントを示す。

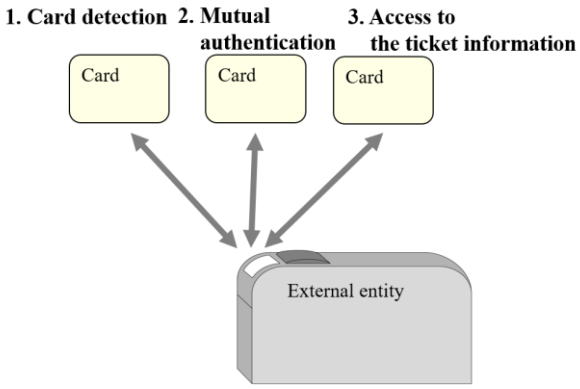


図 1-1　チケットサービスが提供する代表的なオペレーション

一連のオペレーションは、最初にカードの接近を検出することで始まる。カード検出後は相互認証を行い、認証に成功するとカード内の情報を読み出す。その情報が有効であると判断すると必要な情報を書き込み、同時にゲートの通過が許可される。

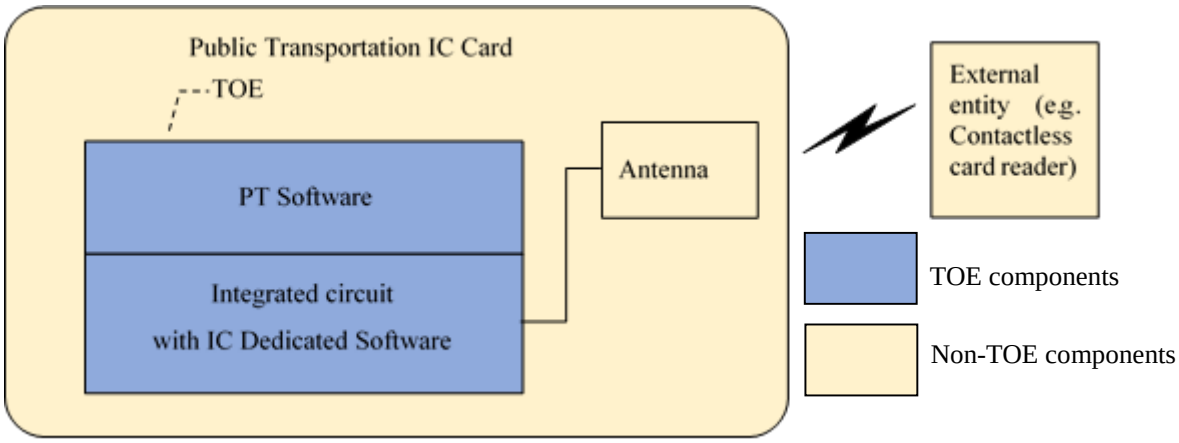


図 1-2　想定する TOE と TOE 外のコンポーネント

“PT Software”とは、Public Transportation Application と Operating System を示す。これらはファイルシステムへのアクセス制御を行う。

“Integrated circuit with IC Dedicated Software”は、IC チップと専用ソフトウェアから成る。IC チップは、CPU、暗号コプロセッサ、セキュリティ機能（検出器やセンサーなど）、インタフェース（接触、非接触）、メモリを内蔵している。

専用ソフトウェアは、製造時のテストに用いられるだけでなく、追加のサービスとして暗号ライブラリを含むこともある。

TOE のライフサイクルは、7 つのフェーズに分けられる。表 1-1 に、TOE のライフサイクルを示す。

表 1-1　TOE のライフサイクル

| Phase | Description |
|---|---|
| **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 Software は、Phase1 で開発される。Phase2 及び Phase3 で IC と IC Dedicated Software が開発・製造される。TOE を Phase3 で配付するときは、形態は wafer か sawn wafer 又は dice になる。TOE を Phase4 で配付するときは、形態はパッケージになる。Phase5 でカード化されたのち、Phase6 での発行を経て Phase7（運用）に至る。

PP[9]では、Phase1 から TOE 配付までの保証要件を定義している。

#### 1.1.1.1　脅威とセキュリティ対策方針

PP[9]に適合する TOE は、以下に示すセキュリティ機能によってそれぞれの脅威に対抗する。

Attack Potential [8]には、IC カードに対する攻撃として Physical Attack、Side Channel Attack、Perturbation Attack などが示されている。これらの攻撃は、TOE に対しても行われる可能性がある。PP[9]は、これらの攻撃から IC チップを守り資産の侵害に対抗する耐タンパー機能を要求している。

図 1-1 に示した相互認証の際、攻撃者は認証をバイパスして TOE 内の資産にアクセスする可能性がある。PP[9]は、相互認証機能とサービスの内容に依存したアクセス制御機能によって、TOE 内に格納されている資産の機密性と完全性を保護することを要求している。

TOE は接触又は非接触インタフェースで外部エンティティと通信を行う。攻撃者は、この通信データを暴露・改ざんしよう試みる可能性がある。PP[9]は、セキュアチャネルを構築することによって、これに対抗することを要求している。

攻撃者は、配付後の TOE では使用できない機能を悪用し、セキュリティ機能をバイパスするなどの方法によって、TOE 内の資産にアクセスする可能性がある。PP[9]は、このような機能の悪用を防ぐことを要求している。

#### 1.1.1.2 構成要件と前提条件

PP[9]は、TOE が次のような構成及び前提で製造・運用されることを想定する。

TOE は、資産に対するアクセス制御レベルを明示的に設定されること、及び外部エンティティと TOE が相互認証するメカニズムを提供することを想定している。また、TOE の配付から発行までの間は、TOE 及びその製造・テストデータの機密性及び完全性は、セキュリティ手順によって維持されなければならない。

### 1.1.2 免責事項

実際の調達のためのセキュリティ要件としては、PP[9]に加えて暗号アルゴリズム及び通信プロトコルに対する要件が必要なことに留意されたい。具体的には PP[9]は、図 1-1 に示した相互認証などで使用することが必然的に想定される暗号アルゴリズム及び通信プロトコルに対する要件や関連する暗号鍵管理の要件を提示していない。同時にこれらに対する脅威分析、セキュリティ目標、セキュリティ機能要件なども述べられていない。したがって PP[9]に適合した TOE を開発・調達する際は、これらに関して開発者と調達者の間で別途定義したうえで、評価・認証の必要がある。

## 1.2 評価の実施

認証機関が運営する IT セキュリティ評価・認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[3]に規定された内容に従い、評価機関によって PP[9]に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、平成 30 年 8 月に完了した。

## 1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[10]、及び関連する評価証拠資料を検証し、PP[9]の評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。認証機関が指摘した問題点は、すべて解決され、かつ、PP[9]の評価が CC[4][5][6]及び CEM[7]に照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

# 2 PP識別

PP[9]は、以下のとおり識別される。

| | |
|---|---|
| PP名称： | Public Transportation IC Card Protection Profile |
| PPバージョン： | Version 1.12 |
| 開発者： | 一般社団法人 ID認証技術推進協会 |

# 3 セキュリティ方針

本章では、PP[9]に適合する TOE が解決すべきセキュリティ課題と実装すべきセキュリティ機能について述べる。

PP[9]では、次の機能を TOE に要求する。

・耐タンパー機能

・資産に対するアクセス制御機能

・外部エンティティと TOE 間の相互認証機能とセキュア通信機能

・TOE 配付後には使用できない機能の悪用から保護する機能

## 3.1 脅威

PP[9]は、表 3-1 に示す脅威を想定し、これに対抗する機能を TOE に要求する。

**表3-1 想定する脅威**

| 識別子 | 脅威 |
|---|---|
| T.Hardware_Attack | 攻撃（Physical Attack、Perturbation Attack、Side Channel Attack）によってTOEのセキュリティサービスを操作（探索、バイパス、非アクティブ化または改変）することで資産を侵害するかもしれない |
| T.Logical_Attack | TOE発行後の運用環境において、TOEの資産を侵害、あるいは認証することなくTOEの資産を改ざんするかもしれない |
| T.Comm_Attack | 通信チャネル上で送受信されるメッセージ内の資産を開示する、またはメッセージを置き換えるかもしれない |
| T.Abuse_Func | TOE配付後には使用できない機能を不正に使用することで、TOEのセキュリティサービスや機能を操作（探索、バイパス、非アクティブ化または改変）することによって資産を侵害するかもしれない |

## 3.2 組織のセキュリティ方針

PP[9]に適合する TOE の利用に当たって要求される組織のセキュリティ方針を表 3-2 に示す。

**表 3-2 組織のセキュリティ方針**

| 識別子 | 組織のセキュリティ方針 |
|---|---|
| P.Configure | TOEが以下の手段を提供すること。<br>・各資産のアクセス制御レベルを設定する手段を提供すること（そのアクセス制御レベルは利用者であるオペレータが明示的に指定する） |
| P.Identification | TOEの開発・製造中に以下の保護手段を提供すること<br>・TOEの一意な識別が確立されること |
| P.TOE_Auth | TOEと運用環境が以下の機能を提供すること。<br>・TOEが外部エンティティを認証すること<br>・外部エンティティに対して、TOEを認証させる機能を提供すること |

## 3.3 セキュリティ対策

PP[9]は、3.1 及び 3.2 に示したセキュリティ課題への対策として、以下に概要を示すセキュリティ機能の実装を TOE に要求する。

### 3.3.1 耐タンパー機能

TOE は、Physical Probing や Physical Manipulation に対する保護手段、通常の動作条件の外で動作しないようにして正しい動作を保証する手段、物理的相互作用に関する測定に対する保護手段を提供する。本セキュリティ機能は、T.Hardware_Attack への対抗である。

### 3.3.2 資産に対するアクセス制御機能

TOE は、資産ごとにアクセス制御レベルを明示的に設定する手段、そのアクセス制御レベルに従ったアクセス制御の仕組みを提供する。本セキュリティ機能は、T.Logical_Attack への対抗、及び P.Configure への対応である。

### 3.3.3 外部エンティティとTOE間の相互認証機能とセキュア通信機能

TOE は、TOE が外部エンティティを認証する機能、及び TOE が外部エンティティに対して自身を認証させる機能を提供する。TOE は、外部エンティティとの通信においてセキュアチャネルを提供する。具体的な認証手段、通信プロトコル等は TOE 毎に規定される。本セキュリティ機能は、T.Comm_Attack への対抗、及び P.TOE_Auth への対応である。

### 3.3.4 TOE配付後には使用できない機能の悪用から保護する機能

TOE は、TOE 配付後には使用できない機能を悪用できないように実装する。本セキュリティ機能は、T.Abuse_Func への対抗、及び P.Identification への対応である。

# 4 前提条件と評価範囲の明確化

本章では、PP[9]に適合する TOE を運用する際の前提条件を表 4-1 に示す。これらの前提条件が満たされない場合、TOE のセキュリティ機能が有効に動作することは保証されない。

**表 4-1 前提条件**

| 識別子 | 前提条件 |
|---|---|
| A.Process | TOE配付後、Passengerに配付されるまで、TOE及びその製造・テストデータの機密性及び完全性を維持するためにセキュリティ手順が使用される。 |
| A.Keys | TOEが使用するAccess Keyの生成と管理のプロセスが適切に保護され、管理された環境で実行される。 |

# 5 評価機関による評価実施及び結果

## 5.1 評価機関

評価を実施した「株式会社 ECSEC Laboratory 評価センター」は、IT セキュリティ評価及び認証制度により承認されるとともに、ILAC（国際試験所認定協力機構）の相互承認に加盟している認定機関（独立行政法人製品評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

## 5.2 評価方法

評価は、CC パート 3 の保証要件について、CEM に規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告された。評価報告書では、PP[9]の概要と、CEM のワークユニットごとの評価内容及び判断結果を説明する。

## 5.3 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成 30 年 4 月に始まり、平成 30 年 8 月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。

各ワークユニットの評価作業中に問題点が発見された場合は、所見報告書が発行され開発者に報告される。ただし今回、所見報告書は発行されていない。

また、認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。

これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

## 5.4 評価結果

評価者は、評価報告書をもって PP[9]が CEM のワークユニットすべてを満たしていると判断した。

評価では以下について確認された。

セキュリティ機能要件：　コモンクライテリア　パート２　拡張

セキュリティ保証要件：　コモンクライテリア　パート３　適合

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.2, APE_ECD.1, APE_REQ.2

## 5.5　評価者コメント/勧告

調達者に喚起すべき評価者勧告は、特にない。

# 6 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 提出された証拠資料の内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。

② 評価報告書に示された評価者の評価判断の根拠が妥当であること。

③ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。認証機関は、PP[9]及び評価報告書において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を発行した。

## 6.1 認証結果

提出された評価報告書及び関連する評価証拠資料を検証した結果、認証機関は、PP[9]がCCパート3の保証コンポーネントAPE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.2, APE_ECD.1, APE_REQ.2 に対する保証要件を満たすものと判断する。

## 6.2 注意事項

PP[9]では、外部エンティティとの通信で用いるプロトコルを規定していない。PP[9]適合を主張するTOE開発者は、調達者と協議のうえ、これらを規定しなければならない。

PP[9]では、外部エンティティとの相互認証で用いる暗号アルゴリズム及び暗号アルゴリズムで使用する鍵及び鍵管理の方法を規定していない。PP[9]適合を主張するTOE開発者は、調達者と協議のうえ、これらを規定しなければならない。PP[9]適合を主張するTOEの評価を行う際は、規定した暗号アルゴリズムの有効性の確認とその危殆化についての評価、及び鍵管理の妥当性についての評価が必要になる。

# 7 附属書

特になし。

# 8 用語

本報告書で使用された CC に関する略語を以下に示す。

| | |
|---|---|
| CC | Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準） |
| CEM | Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法） |
| EAL | Evaluation Assurance Level（評価保証レベル） |
| PP | Protection Profile（プロテクションプロファイル） |
| ST | Security Target（セキュリティターゲット） |
| TOE | Target of Evaluation（評価対象） |
| TSF | TOE Security Functionality（TOEセキュリティ機能） |

本報告書で使用された TOE に関する略語を以下に示す。

| | |
|---|---|
| PT Software | Public Transportation Software |

本報告書で使用された用語の定義を以下に示す。

| | |
|---|---|
| Access Key | チケットサービスに使用するデータ領域のアクセス制御に使用する鍵 |
| Card reader | カードであるTOEと対で使われる非接触あるいは接触のリーダ・ライタ端末 |
| Passenger | チケットサービスを利用する人 |
| オペレータ | Passengerに対し特定のサービスを提供するエンティティ（Public Transportation Operator、Administrator） |
| チケットサービス | オペレータがPassengerに対し提供する特定のサービス |

# 9 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 平成30年7月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 平成27年10月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項, 平成27年10月, 独立行政法人情報処理推進機構, CCM-03

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

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

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

[7] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 5, April 2017

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

[9] Public Transportation IC Card Protection Profile, Version 1.12, 01 August 2018, Japan ID Connect with Secure Authentication Promotional association

[10] PP評価報告書 TPS-ETRPP-0002-00, 第2.0版, 2018年8月7日, 株式会社 ECSEC Laboratory 評価センター