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

IT製品（TOE）

申請受付日（受付番号）	平成30年5月23日（IT認証8673）
認証識別	JISEC-C0660
製品名称	JREM 6K Contactless Smart Card IC chip with fast processing function for transport
バージョン及びリリース番号	1.00
製品製造者	ソニーイメージングプロダクツ&ソリューションズ株式会社
評価スポンサーの名称	JR東日本メカトロニクス株式会社
機能要件適合	プロテクションプロファイル適合、CCパート2拡張
プロテクションプロファイル	Public Transportation IC Card Protection Profile Version 1.12(認証識別：JISEC-C0612)
保証パッケージ	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TOEについての評価は、下記のとおりであることを認証したので報告します。
令和元年12月25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

「JREM 6K Contactless Smart Card IC chip with fast processing function for transport」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、ソニーイメージングプロダクツ&ソリューションズ株式会社が開発した「JREM 6K Contactless Smart Card IC chip with fast processing function for transport、バージョン 1.00」（以下「本 TOE」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。）が令和元年 11 月 28 日に完了した 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 JR 東日本メカトロニクス株式会社に報告するとともに、本 TOE に関心を持つ利用者（管理者や最終利用者）に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、11 章のセキュリティターゲット（以下「ST」という。）を併読されたい。特に本 TOE のセキュリティ機能要件、保証要件及びその十分性の根拠は、ST において詳述されている。

本認証報告書は、本 TOE の調達者を読者と想定している。本認証報告書は、本 TOE 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。

本認証報告書で使用する用語については 12 章を参照されたい。

1.1 評価対象製品概要

本 TOE の機能、運用条件の概要を下記に示す。詳細は 2 章以降を参照のこと。

1.1.1 プロテクションプロファイルまたは保証パッケージ

本 TOE は、次のプロテクションプロファイル[14] （以下「適合 PP」という。）に適合する。

Public Transportation IC Card Protection Profile Version 1.12
(認証識別: JISEC-C0612)

本TOEの保証パッケージは、EAL5及び追加の保証コンポーネントALC_DVS.2、AVA_VAN.5 である。

1.1.2 TOEとセキュリティ機能性

本 TOE は、非接触インタフェースを持つ IC チップと「PT Software」と呼ばれるスマートカードソフトウェアで構成されていることが、適合 PP[14]に記述され

ている。IC チップは、東芝デバイス&ストレージ株式会社（以下「東芝」と略す）によって開発されたチップ T6ND8 及びそれに付随する IC Dedicated Software である。PT Software は、ソニーイメージングプロダクツ&ソリューションズ株式会社（以下「ソニー」と略す）によって開発された公共交通事業者が提供するサービスのアプリケーションを含む FeliCa OS である。

本 TOE は、公共交通 IC カードとして日本国内で使用される。本 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、電子マネーや ID カードとしてのサービスを提供できる。また、公共交通事業者は、他の公共交通事業者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、本 TOE は柔軟なファイルシステムを提供し、公共交通事業者は本 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 に乗車券サービスを提供するオペレーション例を示す。一連のオペレーションは、最初に外部エンティティ[1]が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データを読み出す。そのデータが有効であると判断すると必要なデータを書き込み、同時にゲートの通過が許可される。

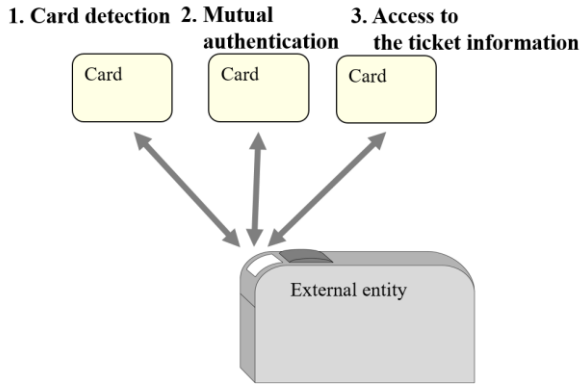


図 1-1　乗車券サービスを提供するオペレーション例

本 TOE の物理的な範囲（青い部分）を図 1-2 に示す。本 TOE の構成は次のとおり。

- 「FeliCa OS」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 Dedicated Software」は、FeliCa OS から後述の T6ND8 へのアクセスを制御・制限するソフトウェアである。

[1] 外部エンティティ(External entity)とは、TOEと相互作用するTOEの外側の実体である。

- 「T6ND8」は、32 ビットアーキテクチャの CPU、AES と DES[2]をサポートする暗号コプロセッサ、セキュリティ構成要素（例えば、本 TOE を保護する為の検出回路やセンサーなど）、非接触インタフェース、ROM、RAM 及び EEPROM から構成される IC である。

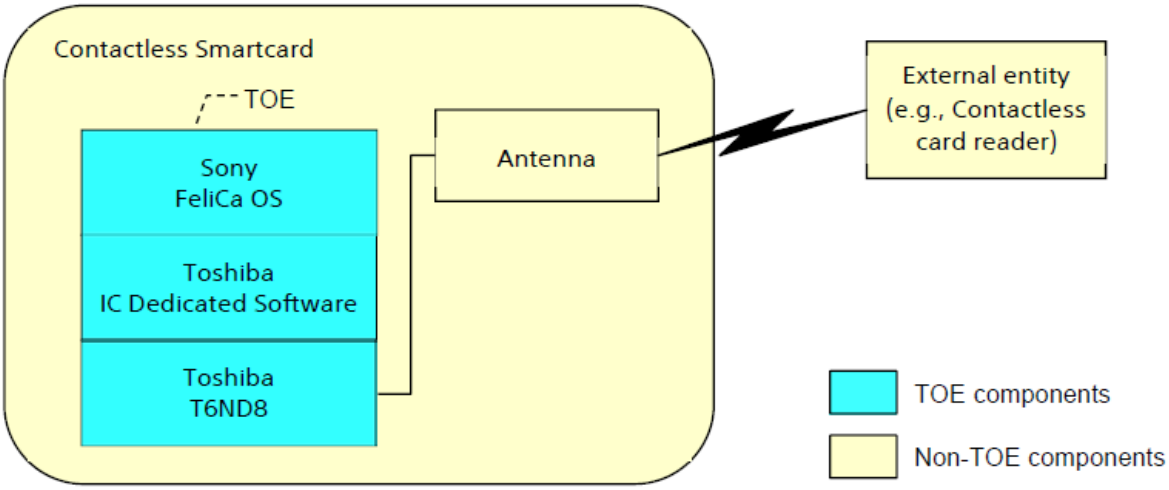


図 1-2　TOEの物理的な範囲

本 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。本 TOE は、図 1-3 に示すとおりツリー構造の Area と Service から構成されるファイルシステムを持つ。本 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、ユーザデータやアクセス鍵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。

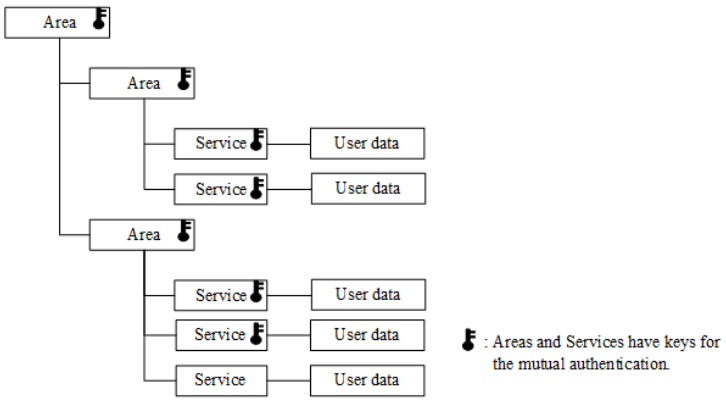


図 1-3　ファイルシステム

[2] DESが使用される機能は評価対象外である。

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 属性を持つ。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本 TOE は Service に紐づけられたアクセス鍵を用いて相互認証を行う。認証が成功すると、本 TOE は外部エンティティに、Service 属性に指定されたタイプのアクセスを許可する。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表 1-1 に示す。

表 1-1　ユーザデータへのアクセス制御レベル

項番	外部エンティティの認証状態	Service属性	許可された操作
1	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
2		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
3	Service に紐づいている アクセス鍵での認証に成功	リードアクセスのみ：認証要	ユーザデータのリード
4		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本 TOE は Area に紐づけられたアクセス鍵を利用して相互認証する。認証が成功すると、本 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 属性の設定）の実行を許可する。

本 TOE のライフサイクルは、表 1-2 のとおり 7 つのフェーズに分けられる。

表 1-2　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

- Phase 1: 本TOE に含まれる FeliCa OSが、ソニーによって開発される。Phase 1 後、ソニーは FeliCa OS、初期化データとプレパーソナライズデータを東芝に配付する。

- Phase 2: IC 開発（T6ND8 と IC Dedicated Software の開発）が東芝によって実施される。
- 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、初期化データの入力を含む初期化、プレパーソナライゼーション）が東芝によって実施される。Phase 3 後、本 TOE はソーンウェハ形状で IC パッケージ製造者へ配付される。
- Phase 4: IC パッケージング（アンテナの実装と検査）が IC パッケージ製造者によって実施される。
- Phase 5: スマートカード製造者は、本 TOE を公共交通 IC カード製品へ組込み、それを管理者（例えば、公共交通事業者）に配付する。
- Phase 6: 管理者（例えば、公共交通事業者）は、ユーザデータ、Service 属性、アクセス鍵を本 TOE のメモリにロードし、パーソナライズ（本 TOE の発行）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最終利用者に配付される。

適合 PP[14]では、本 TOE の開発（Phase1）から TOE 配付（Phase3 後）までの保証要件を定義している。

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について適合 PP[14]の要求する保証要件の範囲で評価が行われた。

本 TOE が想定する脅威及び前提については次項のとおりである。

1.1.2.1 脅威とセキュリティ目標[3]

本TOEは、下記のとおりのセキュリティ機能によりそれぞれの脅威に対抗する。

Attack Potential [12]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、本 TOE に対しても行われる可能性がある。適合 PP[14]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本 TOE 内の資産にアクセスする可能性がある。適合 PP[14]は、相互認証機能とサービスの内容に依存

[3] CC Part 1 [4]で定義されている"security objective"の訳語として、日本語翻訳版[7]では「セキュリティ対策方針」を割り当てているが、本認証報告書の中では、"security objective"の訳語として、「セキュリティ目標」を用いることとする。

したアクセス制御機能によって、本 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。

本 TOE は外部にアンテナを接続し、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。適合 PP[14]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、配付後の本 TOE では使用できない様にした機能を悪用し、セキュリティ機能をバイパスするなどの方法によって、本 TOE 内の資産にアクセスする可能性がある。適合 PP[14]は、このような機能の悪用を防ぐことを要求している。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような構成及び前提で運用することを想定する。

本 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本 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、本 TOE の配付から発行までの間は、本 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。

1.1.3 免責事項

本 TOE は、「4.1 使用及び環境に関する前提条件」で示す運用環境がセキュアではない状態での運用、及び「8.7 評価者コメント/勧告」で示す運用条件が満たされない運用において保証の対象外である。

1.2 評価の実施

認証機関が運営する IT セキュリティ評価及び認証制度に基づき、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、評価機関によって本 TOE 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、令和元年 11 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[33]、所見報告書（[28][29][30]）、及び関連する評価証拠資料を検証し、本 TOE 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、全て解決され、かつ、本 TOE の評価が CC（[4][5][6]または[7][8][9]）及び CEM（[10][11]のいずれか）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 TOE識別

本 TOE は、次のとおり識別される。

TOE名称：	JREM 6K Contactless Smart Card IC chip with fast processing function for transport
バージョン：	1.00
開発者：	ソニーイメージングプロダクツ＆ソリューションズ株式会社

製品が評価･認証を受けた本 TOE であることを、利用者は製品添付ドキュメントに記載された下記の方法によって確認することができる。

本 TOE における T6ND8 のバージョン、IC Dedicated Software のバージョン及び FeliCa OS のバージョンについて、[19]の手順に従い特定のコマンドにて本 TOE 識別を確認できる。

コマンドの起動方法は各コマンド共通であり、IC カードリーダライタを使用してコマンドを入力する。IC カードリーダライタが備えるべき仕様は、[18] 2 章で物理層・データリンク層・アプリケーション層ごとに説明されている。

3 セキュリティ方針

本章では、本 TOE が脅威に対抗するために採用したセキュリティ機能方針や組織のセキュリティ方針を説明する。

本 TOE は、適合 PP[14]の要求を満足する下記のセキュリティ機能を提供する。

(1) 耐タンパー機能

(2) 資産に対するアクセス制御機能

(3) 外部エンティティと本 TOE 間の相互認証機能とセキュア通信機能

(4) 本 TOE 配付後には使用できない様にした機能の悪用から保護する機能

3.1 セキュリティ機能方針

本 TOE の保護資産は、次の 2 種類に分類できる。

(1) 一次資産は、本 TOE に格納されたユーザデータ

(2) 二次資産は、一次資産の機密性、完全性を守るために必要となるデータ（例えば、アクセス鍵、初期化データ、プレパーソナライゼーションデータ、IC Dedicated Software、FeliCa OS）

保護されるべきユーザデータは、ライフサイクルの Phase6 で管理者によって定義される。

本 TOE は、3.1.1 に示す脅威に対抗し、3.1.2 に示す組織のセキュリティ方針を満たすセキュリティ機能を具備する。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

本 TOE は、表 3-1 に示す脅威を想定し、これに対抗する機能を備える。

表 3-1 想定する脅威

項番	識別子	脅威
1	T.Hardware_Attack	攻撃（物理攻撃、かく乱攻撃、サイドチャネル攻撃）によって本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、又は、改変）することで資産を侵害するかもしれない

項番	識別子	脅威
2	T.Logical_Attack	本TOE発行後の運用環境において、本TOEの資産を侵害、あるいは認証することなく本TOEの資産を改ざんするかもしれない
3	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
4	T.Abuse_Func	本TOE配付後には使用できない様にした機能を不正に使用することで、本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、又は、改変）することによって資産を侵害するかもしれない

3.1.1.2 脅威に対するセキュリティ機能

本 TOE は、表 3-1 に示す脅威に対し、下記のセキュリティ機能で対抗する。

(1) 脅威「T.Hardware_Attack」への対抗

本 TOE は、ハードウェアへの物理的相互作用、物理的操作及び物理的プロービング、並びに記録されている資産の暴露／改ざんに対し適切に保護する。更に、本 TOE は信頼できる運用環境､試験により確かめられた安全な運用以外での動作を防止し正しい操作を保証する。

(2) 脅威「T.Logical_Attack」への対抗

本 TOE は、外部エンティティに対する認証を可能とし、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。

(3) 脅威「T.Comm_Attack」への対抗

本 TOE は、盗聴と改ざんの脅威に対して考慮された非接触インタフェースで資産を送受信する。従って、本 TOE は、外部エンティティとの相互通信において、転送される資産の機密性と完全性を実現するセキュア通信を提供する。

(4) 脅威「T.Abuse_Func」への対抗

本 TOE は、本 TOE 配付後には使用できない様にした機能を悪用（次の（ｉ）～（iv））できないように実装する。（ｉ）本 TOE の重要な資産を暴露する。（ii）本 TOE の重要な資産を操作する。(iii) FeliCa OS を操作する。(iv) 本 TOE のセキュリティ機能又はセキュリティサービスを探索、バイパス、非アクティブ化、又は、改変する。

3.1.2 組織のセキュリティ方針とセキュリティ機能

3.1.2.1 組織のセキュリティ方針

本 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

項番	識別子	組織のセキュリティ方針
1	P.Configure	本TOEが下記の手段を提供すること。 ・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）
2	P.Identification	本TOEの開発・製造中に下記の保護手段を提供すること ・本TOEの一意な識別が確立されること
3	P.TOE_Auth	本TOEと運用環境が下記の機能を提供すること。 ・本TOEが外部エンティティを認証すること ・外部エンティティに対して、本TOEを認証させる機能を提供すること

3.1.2.2 組織のセキュリティ方針に対するセキュリティ機能方針

本 TOE は、表 3-2 に示す組織のセキュリティ方針を満たす機能を具備する。

(1) 組織のセキュリティ方針「P.Configure」への対応

本 TOE は、管理者によって設定されるアクセス制御の手段を提供する。

(2) 組織のセキュリティ方針「P.Identification」への対応

本 TOE は不揮発メモリに初期化データを保存する手段を提供する。初期化データ（又は、その一部）は本 TOE の一意な識別に使用される。

(3) 組織のセキュリティ方針「P.TOE_Auth」への対応

本 TOE が外部エンティティを認証することを可能とする。外部エンティティに対して本 TOE の認証を可能とする。運用環境は、本 TOE の認証にて参照されるデータを用意し、認証における検証メカニズムをサポートする。

4 前提条件と評価範囲の明確化

本章では、想定する読者が本 TOE の利用の判断に有用な情報として、本 TOE を運用するための前提条件及び運用環境について記述する。

4.1 使用及び環境に関する前提条件

本 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、本 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

項番	識別子	前提条件
1	A.Process	本TOE 及びその製造･テストデータの機密性や完全性を維持するために､本TOE の製造者は最終利用者に配付されるまで、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)。
2	A.Keys	本TOE で使用するアクセス鍵は､管理された環境におけるシステムによって本TOE 外で生成され、安全に本TOE に設定される。鍵生成と管理のプロセスは、十分に保護され、且つ、管理された環境で実施される。

4.2 運用環境と構成

本 TOE を含む IC カードの全てのオペレーションは、非接触式の IC カードリーダライタを通して実行される。本 TOE は、IC カードリーダライタから送信される 13.56MHz の搬送波信号を電力として使用し、ISO/IEC 18092[31]に準拠した通信方式に基づき、動作モード：パッシブモード、ビットレート：212/424kbps で IC カードリーダライタと通信する。

なお、本構成に示されている本 TOE 以外のハードウェア及びソフトウェアの信頼性は本評価の範囲ではない（十分に信頼できるものとする)。

4.3 運用環境におけるTOE範囲

本 TOE は外部エンティティからのコマンド受信と外部エンティティへのレスポンス送信の機能を提供し、表 3-1 に示した脅威に対抗するセキュリティ機能、表 3-2 に示した組織のセキュリティ方針を満たすセキュリティ機能を具備しているが、

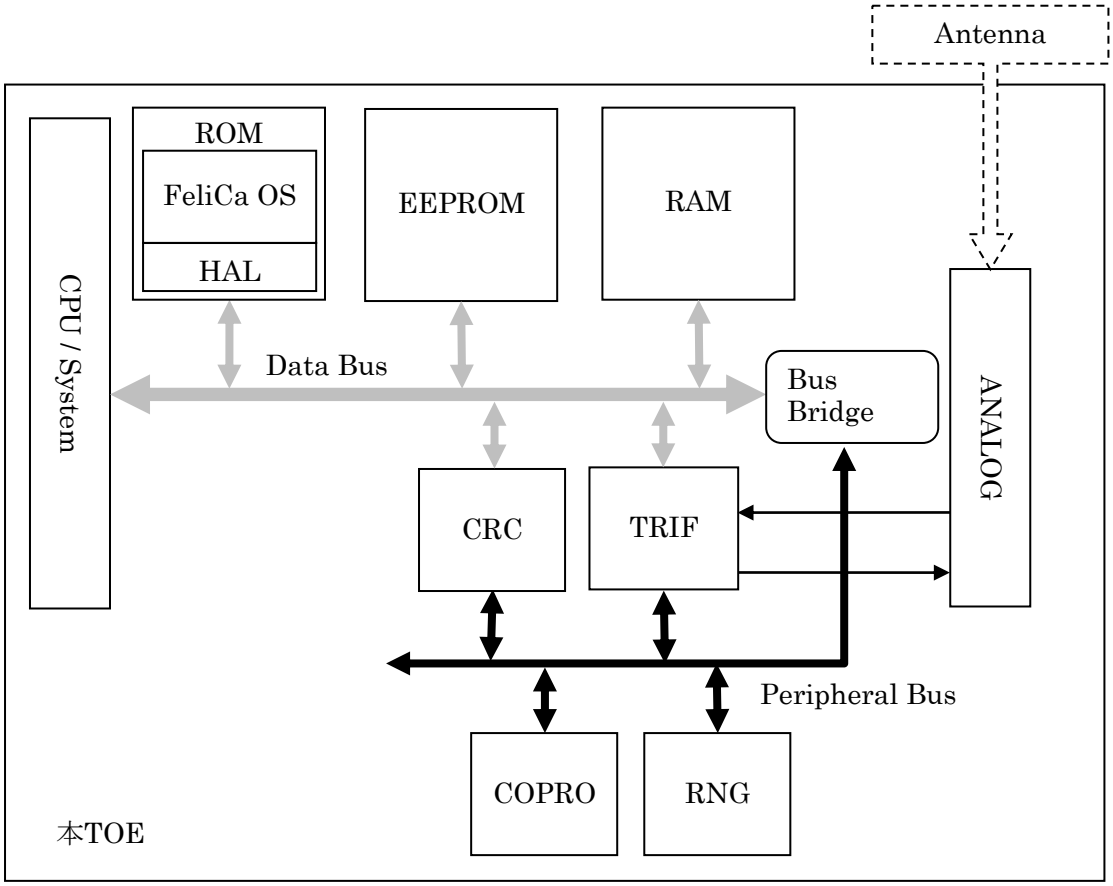
表 4-1 に示した前提条件が満たされない場合、本 TOE のセキュリティ機能が有効に動作することは保証されない。

5 アーキテクチャに関する情報

本章では、本 TOE の範囲と主要な構成を説明する。

5.1 TOE境界とコンポーネント構成

本 TOE の構成を図 5-1 に示す。アンテナは、本 TOE の範囲ではない。



ICはT6ND8

図 5-1 本TOEの構成

本 TOE を構成するコンポーネントについて表 5-1 に示す。

表 5-1 本TOEを構成するコンポーネント

項番	コンポーネント	概要
1	FeliCa OS	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込みソフトウェア。
2	IC Dedicated Software	セキュリティIC に搭載される専用のソフトウェアであり、ハードウェアの機能のAPIをFeliCa OSに提供するHardware Abstract Layer (HAL)。
3	T6ND8	CPU / System、EEPROM、RAM、ROM、TRIF（非接触通信によるデータ送受信）、COPRO、CRC、RNG及びANALOG（アナログ回路）により構成される。

5.2 IT環境

本 TOE は IC カードにパッケージングされ使用される。本 TOE の運用は、外部エンティティから供給される電力以外の IT 環境に依存しない。公共交通事業者は目的に応じた IC カードリーダライタを用意することが要求される。

6 製品添付ドキュメント

本 TOE に添付されるドキュメントの識別を下記に示す。本 TOE の利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

[18] FeliCa Card User's Manual Version 1.04, August 2017

[19] RC-S114 Inspection Procedure Version 1.00, January 2018

[20] RC-S114 Inspection and IDm Writing Procedure Version 1.00, January 2018

[21] Product Acceptance Procedure Version 1.0, February 2015

[22] FeliCa Card AES Encryption Mechanism Transition Guide Version 1.0, August 2012

[23] RC-S114 Important Notice for customers Version 1.1, November 2019

[24] Security Reference Manual – Group Key Generation (AES 128bit) Version 1.21, January 2019

[25] Security Reference Manual – Mutual Authentication & Secure Communication (AES 128bit) Version 1.21, January 2019

[26] Security Reference Manual – Package Generation (AES 128bit) Version 1.21, January 2019

[27] Security Reference Manual – Changing Key Package Generation (AES 128bit) Version 1.21, January 2019

7 サイトセキュリティ

本 TOE の評価では、ALC_DVS.2 の評価において、Minimum Site Security Requirements[13]を適用した。本 TOE に関連するサイトは**表 7-1** のとおりである。

表 7-1 本TOEの関連サイト

項番	サイト	アクティビティ	サイト訪問日
1	ソニーイメージングプロダクツ＆ソリューションズ株式会社 （東京都品川区大崎）	FeliCa OS 開発、配付	2018 年 8 月 20 日（月）
2	東芝デバイス＆ストレージ株式会社 （神奈川県川崎市）	IC 開発	2018 年 10 月 11 日（木）
3	ディー・ティー・ファインエレクトロニクス株式会社 北上事業所 （岩手県北上市）	フォトマスク製造	2019 年 4 月 2 日（火）
4	株式会社ジャパンセミコンダクター 大分事業所 （大分県大分市）	ウェハ製造、配付	2018 年 10 月 25 日（木） 10 月 26 日（金）

8 評価機関による評価実施及び結果

8.1 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。

8.2 評価方法

評価は、CC パート 3 の保証要件について、CEM、CC サポート文書（[12][13]）及び評価機関独自の評価手法[32]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[33]において報告されている。評価報告書では、本 TOE の概要と、CEM、CC サポート文書（[12][13]）及び評価機関独自の評価手法[32]のワークユニットごとの評価内容及び判断結果が説明されている。

8.3 評価実施概要

評価報告書による評価実施の履歴を下記に示す。

評価は、平成 30 年 5 月に始まり、令和元年 11 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。また、平成 30 年 8 月、10 月及び令和元年 4 月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付・開発セキュリティの各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成 30 年 8 月、10 月及び令和元年 10 月に開発者テストのサンプリングチェック、平成 30 年 6 月、9 月及び令和元年 7 月、9 月に評価者独立テスト、平成 30 年 5 月～令和元年 9 月で評価者侵入テストを実施した。

評価作業中に発見された問題点は、全て所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、全ての問題点が解決されている。

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。

8.4 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評定に基づく侵入テストを実行した。なお、本節ではT6ND8とIC Dedicated Softwareを組にして「プラットフォームIC」と呼ぶこととする。

8.4.1 開発者テスト

開発者テストは、プラットフォームICの開発者とFeliCa OSの開発者のそれぞれで実施された。評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価者が評価した開発者テストの内容を下記に説明する。

8.4.1.1 プラットフォームICの開発者テスト

a) テスト概要

プラットフォームICの開発者テストは、本TOEを構成するプラットフォームICを対象とし、その開発者によって実施された。開発者テストの一部はテストモードの状態で実施されている。これはTSFの振舞いを実証するための正当な代替手法であると評価者は分析した。

開発者テストの環境を図 8-1に示す。テストはプラットフォームICに対してコマンドを入力し、それに対するレスポンスを観察する事によって行っている。LSIテスタが適切に校正されていることは、テスタ校正記録（2018年10月14日）によって確認されている。

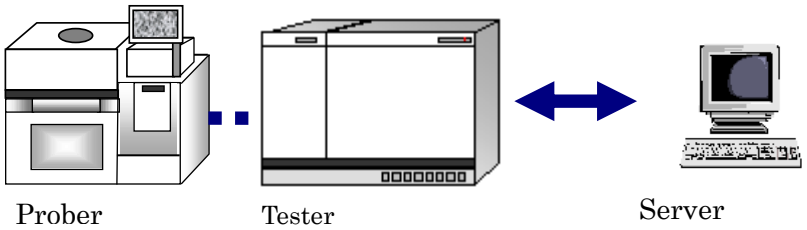


図 8-1 プラットフォームICの開発者テスト環境

開発者テストのテスト計画、手順、期待されるテスト結果、実際のテスト結果などの開発者テスト証拠資料が、開発者から評価者に提出されており、評価者はこれらの文書によって、テスト構成がSTと一貫しているか、全ての期待するテスト結果が記載されているか、実際のテスト結果が期待どおりであるかを検査した。

さらに、評価者は上記の開発者テスト環境を用いて、開発者テストのサンプリングテスト（表 8-1参照）を行った。

表 8-1　プラットフォームICのサンプリングテスト

項番	テスト内容
1	LSIテスタを用いて、テストモードに入り、ICにテストパラメータをセットし、その振舞いを確認する。

b)　**開発者テストの実施範囲**

評価者は、開発者が提出したテスト証拠資料を評価することで、開発者テストのカバレッジが保証コンポーネントATE_COV.2を満たし、テストの実施範囲が適切であることを確認した。関連する評価内容と評価結果は、評価報告書[33]に示されている。

c)　**結果**

評価者は、開発者テストの実施方法、実施項目の正当性を確認し、テスト計画書に示された実施方法と実際の実施方法が一致することを確認した。評価者は、開発者が期待したテスト結果と開発者によって実施されたテスト結果が一致していることを確認した。

8.4.1.2　FeliCa OS の開発者テスト

a)　**テスト概要**

FeliCa OSの開発者テストは、FeliCa OSを搭載した本TOEを対象とし、FeliCa OSの開発者によって実施された。開発者テストの環境を図 8-2に示す。

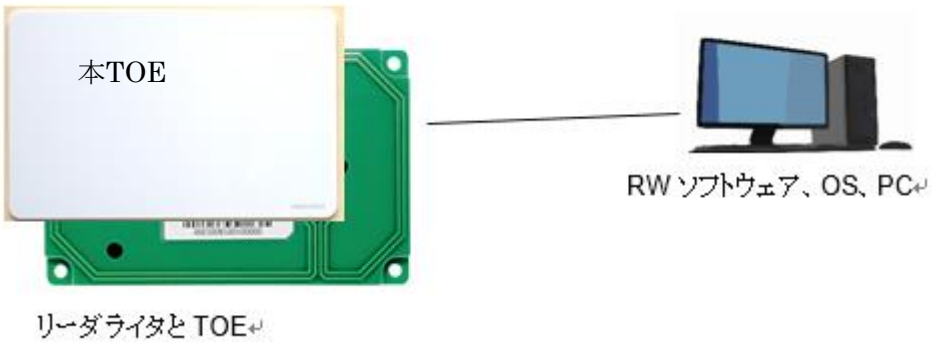


図 8-2　FeliCa OSのサンプリングテスト／独立テスト環境

開発者テストのテスト計画、手順、期待されるテスト結果、実際のテスト結果などの開発者テスト証拠資料が、開発者から評価者に提出されており、評価者は

これらの文書によって、テスト構成がSTと一貫しているか、全ての期待するテスト結果が記載されているか、実際のテスト結果が期待どおりであるかを検査した。さらに、評価者は最終利用者への配付される本TOEを想定し、図 8-2に示すテスト環境を用いて、FeliCa OSの開発者テストのサンプリングテスト（表 8-2参照）を実施した。

表 8-2　FeliCa OSのサンプリングテスト

項番	テスト内容
1	運用時に使用するコマンドを本TOE入力し、それに対する本TOEのレスポンスがコマンド仕様を満たしていることを確認する。
2	主に製造時に使用するコマンドを本TOE入力し、それに対する本TOEのレスポンスがコマンド仕様を満たしていることを確認する。
3	本TOEのライフサイクルに応じて、コマンドコードの全探索を行い、コマンドコード毎に本TOEが期待どおりの振舞いをすることを確認する。
4	乱数を取得して統計テストを実施する。

b)　**開発者テストの実施範囲**

評価者は、開発者が提出したテスト証拠資料を評価することで、開発者テストのカバレッジが保証コンポーネントATE_COV.2を満たし、テストの実施範囲が適切であることを確認した。関連する評価内容と評価結果は、評価報告書[33]に示されている。

c)　**結果**

評価者は、開発者テストの実施方法、実施項目の正当性を確認し、テスト計画書に示された実施方法と実際の実施方法が一致することを確認した。評価者は、開発者が期待したテスト結果と開発者によって実施されたテスト結果が一致していることを確認した。

8.4.2 評価者独立テスト

評価者は、プラットフォーム IC と FeliCa OS のそれぞれについて、開発者テストから抽出したテスト項目を使用して製品のセキュリティ機能が実行されることを再確認するサンプルテストを実施するとともに、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることをより確信するための独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを下記に説明する。

8.4.2.1 プラットフォーム IC の独立テスト

(1) 独立テスト構成

評価者は図 8-3 に示すテスト環境を用いて、プラットフォーム IC の独立テストを行った。

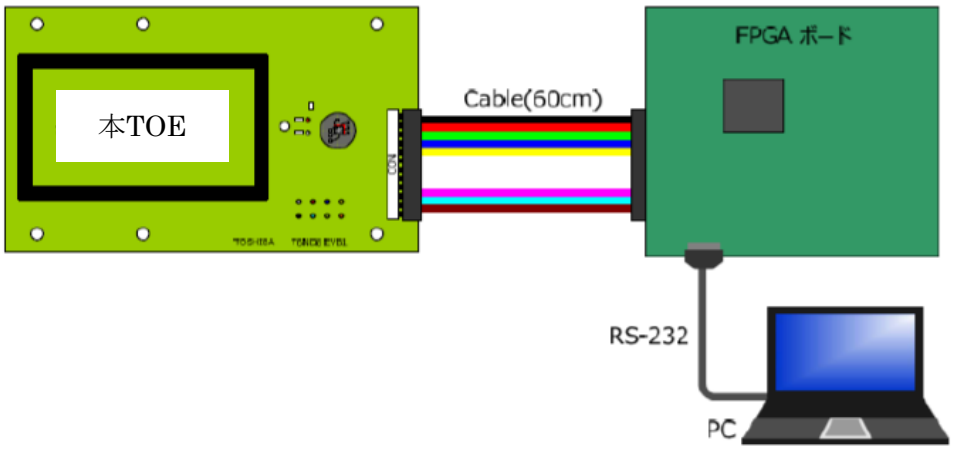


図 8-3　プラットフォームICの独立テスト環境

(2) 独立テスト概説

評価者の実施した独立テストは下記のとおりである。

a) 独立テストの観点

評価者が、開発者テスト及び提供された評価証拠資料から考案した独立テストの観点を次に示す。

・本TOEが生成・使用する乱数の品質を確認する。

・CAVP（Cryptographic Algorithm Validation Program）の暗号アルゴリズム試験の対象となっているアルゴリズムに対して、その実装の正しさを確認する。

b) 独立テスト概要

評価者は、開発者テスト及び提供された評価証拠資料から、前述の観点で追加の独立テストを考案した。

評価者が実施した独立テストの一覧を表 8-3に示す。

表 8-3　プラットフォームICの独立テスト

項番	テスト内容
1	乱数のエントロピー計測。
2	暗号アルゴリズム試験。

c) **結果**

計測された乱数のエントロピーは期待値以上であった。また、暗号アルゴリズム試験対象は全て合格した（CAVP認証番号5691）。

以上のように、評価者が実施した全ての独立テストは正しく完了し、評価者は本TOE の振舞いを確認した。評価者は、全てのテスト結果と期待される振舞いが一致していることを確認した。

8.4.2.2　FeliCa OS の独立テスト

(1) 独立テスト構成

評価者は最終利用者へ配付される本 TOE を想定し、前述の図 8-2 に示すテスト環境を用いて、FeliCa OS の独立テストを評価機関において実施した。

(2) 独立テスト概説

評価者の実施した独立テストは下記のとおりである。

a) **独立テストの観点**

評価者が、開発者テスト及び提供された評価証拠資料から考案した独立テストの観点を次に示す。

・本TOEのプレパーソナライゼーションで無効化されるべきコマンドが、正しく無効化されていることを確認する。

b) **独立テスト概要**

評価者は、開発者テスト及び提供された評価証拠資料から、前述の観点で追加の独立テストを考案した。

評価者が実施した独立テストの一覧を表 8-4に示す。

表 8-4　FeliCa OSの独立テスト

項番	テスト内容
1	プレパーソナライゼーションで無効化されるべきコマンドを本TOEに入力し、本TOEの振舞いが期待どおりであることを確認する。

c) **結果**

評価者が実施した全ての独立テストは正しく完了し、評価者は本TOEの振舞いを確認した。評価者は、全てのテスト結果と期待される振舞いが一致していることを確認した。

8.4.3　評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性となる可能性があるものについて、必要と思われる評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。

評価者が実施した侵入テストを下記に説明する。

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は下記のとおりである。

a) **脆弱性の識別**

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、CCサポート文書[12][13]及び評価機関独自の評価手法[32]に基づいて侵入テストを必要とする脆弱性を識別した。

b) **侵入テストの概要**

評価者は、潜在的な脆弱性が悪用される可能性を検出するために、下記の侵入テストを実施した。

＜侵入テスト環境＞

侵入テストは、レーザ照射を用いるパータベーション攻撃とサイドチャネル攻撃に分けられる。それぞれの概略構成を図 8-4、図 8-5に示す。

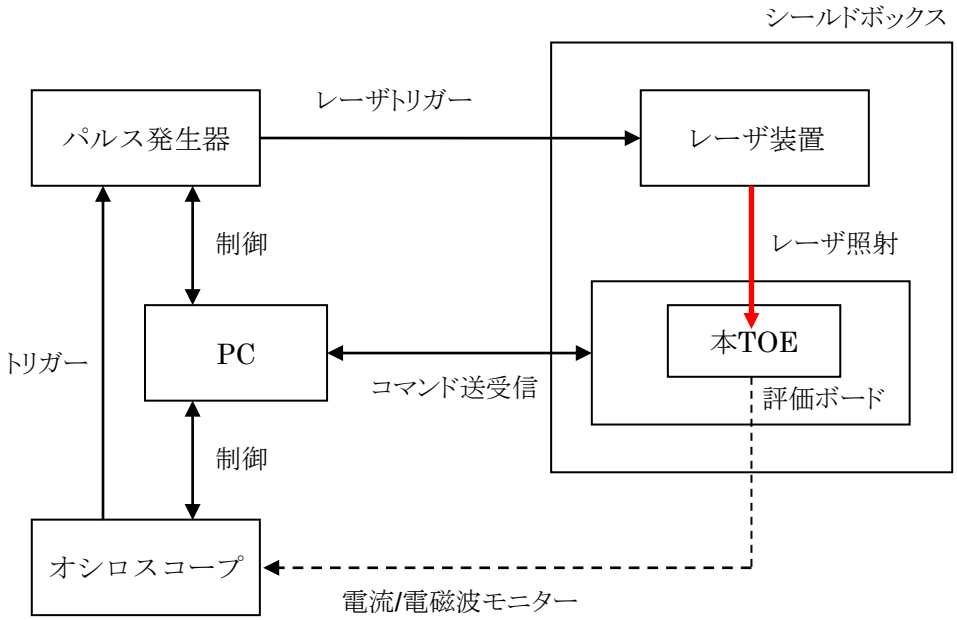


図 8-4　パータベーション攻撃の侵入テスト構成

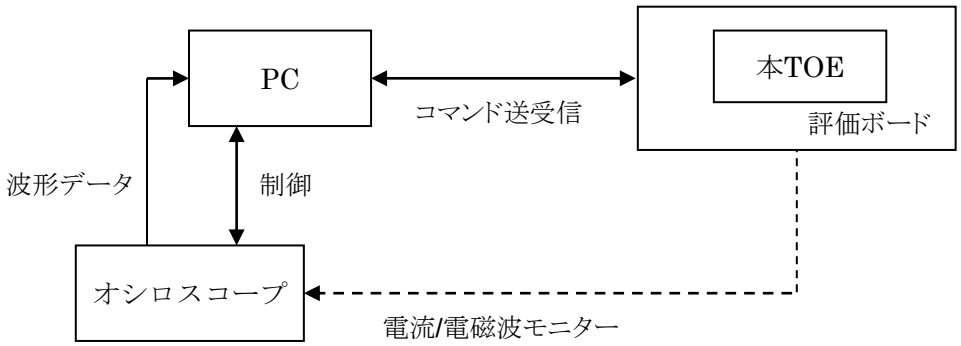


図 8-5　サイドチャネル攻撃の侵入テスト構成

＜侵入テストの実施項目＞

侵入テストの実施項目は、識別された脆弱性に対応して具体化されている。

c)　**結果**

評価者が実施した侵入テストでは、コモンクライテリア パート３[6]で定義される、高い攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

8.5 評価構成について

評価機関におけるテストでは、「8.4.1 開発者テスト」で示すサンプリングテストの構成、「8.4.2 評価者独立テスト」の構成、及び「8.4.3 評価者侵入テスト」に示す構成において、評価を行った。

8.6 評価結果

評価者は、評価報告書[33]に記載するとおり、本 TOE が CEM のワークユニット全てを満たしていると判断した。

評価では下記について確認された。

PP 適合：Public Transportation IC Card Protection Profile Version 1.12
（認証識別: JISEC-C0612）

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、下記の保証コンポーネントについて「合格」判定がなされた。

EAL5 パッケージの全ての保証コンポーネント

追加の保証コンポーネント　ALC_DVS.2、AVA_VAN.5

評価の結果は、第 2 章に記述された識別に一致する TOE によって構成されたもののみに適用される。

8.7 評価者コメント/勧告

本TOE配付後に管理者によって書込まれるアクセス鍵の鍵値を本TOEは関知しない。[18]に従い、管理者あるいは管理者が所属する組織の責任で適切な鍵値を決定してセキュアに管理しなければならない。

本 TOE の管理者は、運用時点における攻撃技術の進歩を監視し、必要に応じたリスク分析を実施すべきである。

9 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、下記の認証を実施した。

① 所見報告書でなされた指摘内容が妥当であること。

② 所見報告書でなされた指摘内容が解決されていること。

③ 提出された証拠資料をサンプリングし、その内容を検査し、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。

④ 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。

⑤ 評価報告書に示された評価者の評価方法がCEM及びCCサポート文書（[12][13]）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、ST[16]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する。

9.1 認証結果

提出された評価報告書、所見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、本 TOE の評価が CC パート 3 の EAL5 及び保証コンポーネント ALC_DVS.2、AVA_VAN.5 に対する保証要件を満たすものと判断する。

9.2 注意事項

本 TOE の調達者・利用者は、本 TOE が使用されるシステムのリスクマネジメントの中でこの認証結果を利用するにあたっての検討を行うべきである。例えば、攻撃方法・技術の変化を踏まえて、この認証書及び依存する認証書の有効性の確認 "re-assessment"をいつまでに行うべきかを定めておくべきである。また、本 TOE の調達者・利用者は、本 TOE が使用されるシステムのリスクマネジメントの中で、暗号アルゴリズムの使用方法の有効性についても、見直さなければならない。

10 附属書

特になし。

11 セキュリティターゲット

本 TOE の ST-Lite[17]は、本報告書とは別文書として次のとおり提供される。

Security Target JREM 6K Contactless Smart Card IC chip with fast processing function for transport Public Version, Version 2.0, November 2019, Sony Imaging Products & Solutions Inc.

この ST-Lite は、評価された完全な ST[16]を、CC サポート文書である ST sanitising for publication [15]に従って、公開用に整理したものである。

12 用語

12.1 CCに関する略語

本報告書で使用された CC に関する略語を下記に示す。

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）
ST-Lite	Security Target Lite（セキュリティターゲットライト）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

12.2 本認証報告書で使用された用語及び略語

本報告書で使用された本 TOE に関する用語の定義及び略語を下記に示す。

アクセス鍵	AreaとServiceに対応する鍵。
外部エンティティ	TOEと相互作用するTOEの外側の実体（External entity）。
公共交通事業者	最終利用者へ特定のサービスを提供するエンティティ。
管理者	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。
最終利用者	チケットサービスを利用する人。
Service属性	ユーザデータへのアクセス種別、及びユーザデータにアクセスするセキュリティ条件を定義する属性。
初期化データ	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。
チケットサービス	TOEにより技術的に可能となる最終利用者に対する特定のサービス。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最終利用者に提供される。
プレパーソナライズデータ	FeliCa OS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書き込まれるデータ。
AES	Advanced Encryption Standard
API	Application Programming Interface
Area	ファイルシステムの一部。エリアは通常のファイルシステムにおけるディレクトリの役割と似ている。
COPRO	co-processor

CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
EEPROM	Electrically Erasable Programmable Read-Only Memory
HAL	Hardware Abstract Layer
PT Software	Public Transportation Software
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
Service	Service属性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。
TRIF	Transmit & Receive Interface

13 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30年9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30年9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 Part1: Introduction and general model Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[7] 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5版, 2017年4月, CCMB-2017-04-001 (平成29年7月翻訳第1.0版)

[8] 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5版, 2017年4月, CCMB-2017-04-002 (平成29年7月翻訳第1.0版)

[9] 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5版, 2017年4月, CCMB-2017-04-003 (平成29年7月翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 5, April 2017, CCMB-2017-04-004

[11] 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5版, 2017年4月, CCMB-2017-04-004 (平成29年7月翻訳第1.0版)

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

[13] Joint Interpretation Library – Minimum Site Security Requirements, Version 1.1 (for trial use), July 2013

[14] Public Transportation IC Card Protection Profile Version 1.12（認証識別：JISEC-C0612）

[15] ST sanitising for publication, April 2006, CCDB-2006-04-004

[16] Security Target JREM 6K Contactless Smart Card IC chip with fast processing function for transport Version 2.0, November 2019

[17] Security Target JREM 6K Contactless Smart Card IC chip with fast processing function for transport Public Version, Version 2.0, November 2019

[18] FeliCa Card User's Manual Version 1.04, August 2017

[19] RC-S114 Inspection Procedure Version 1.00, January 2018

[20] RC-S114 Inspection and IDm Writing Procedure Version 1.00, January 2018

[21] Product Acceptance Procedure Version 1.0, February 2015

[22] FeliCa Card AES Encryption Mechanism Transition Guide Version 1.0, August 2012

[23] RC-S114 Important Notice for customers Version 1.1, November 2019

[24] Security Reference Manual – Group Key Generation (AES 128bit) Version 1.21, January 2019

[25] Security Reference Manual – Mutual Authentication & Secure Communication (AES 128bit) Version 1.21, January 2019

[26] Security Reference Manual – Package Generation (AES 128bit) Version 1.21, January 2019

[27] Security Reference Manual – Changing Key Package Generation (AES 128bit) Version 1.21, January 2019

[28] 所見報告書 SUY-EOR-0001-00, 2018年8月31日, 株式会社ECSEC Laboratory評価センター

[29] 所見報告書 SUY-EOR-0002-00, 2019年9月20日, 株式会社ECSEC Laboratory評価センター

[30] 所見報告書 SUY-EOR-0003-00, 2019年8月27日, 株式会社ECSEC Laboratory評価センター

[31] Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1), ISO/IEC 18092:2013, March 2013

[32] Vulnerability Assessment for Security IC and Similar Devices, Version 1.2, 2014 年 1 月 27 日, ECSEC Lab. EMIC-VAN4_5-0001-02

[33] JREM 6K Contactless Smart Card IC chip with fast processing function for transport 評価報告書, 第 6.1 版, 2019 年 12 月 2 日, 株式会社 ECSEC Laboratory 評価センター, SUY-ETR-0006-01B