認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　藤原　武平太

原紙押印済

評価対象

申請受付日（受付番号）	**平成17年7月21日** (IT**認証**5048)
認証番号	C0119
認証申請者	**フェリカネットワークス株式会社**
TOE**の名称**	**モバイル** FeliCa IC **チップファームウェア（**CXD **版）**
TOE**のバージョン**	09 (CXD3717GG)
PP**適合**	**なし**
適合する保証パッケージ	EAL4+ALC_FLR.1+AVA_VLA.3
開発者	**フェリカネットワークス株式会社**
評価機関の名称	**みずほ情報総研株式会社　情報セキュリティ評価室**

上記のTOE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19年10月29日

セキュリティセンター 情報セキュリティ認証室
技術管理者　鈴木　秀二

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 2.1
② Common Methodology for Information Technology Security Evaluation Version 1.0
③ CCIMB Interpretations-0407

評価結果：合格

「モバイル FeliCa IC チップファームウェア（CXD 版）」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、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

1.1 はじめに

この認証報告書は、「モバイル FeliCa IC チップファームウェア（CXD 版)」（以下「本TOE」という。）についてみずほ情報総研株式会社　情報セキュリティ評価室（以下「評価機関」という。）が行った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フェリカネットワークス株式会社に報告するものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

本認証報告書は、本TOEに対して、適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称：　モバイル FeliCa IC チップファームウェア（CXD 版）
バージョン：　09 (CXD3717GG)
開発者：　フェリカネットワークス株式会社

1.2.2 製品概要

本TOEは、携帯電話やリーダライタなどのIT機器に搭載されるモバイル FeliCa IC チップに搭載されるファームウェアである。

本TOEは、モバイル FeliCa IC チップ内の ROM に搭載され、接触のインタフェースによってデータ格納を行う「有線 IC カード機能」と非接触のインタフェースによってデータ格納を行う「無線 IC カード機能」、非接触 IC カードと通信を行う「リーダライタ機能」の 3つの機能を有し、これらの機能に含まれるセキュリティ機能が、モバイル FeliCa IC チップのメモリデータを安全に管理する手段を提供する。TOE は、安全な管理を行うために「認証」・「アクセス制御」・「暗号通信」・「データ保護」のセキュリティ機能を有し、メモリデータへのアクセスを

制御する。これらの機能により、電子現金システムや交通システムなど重要度の高いデータの格納を可能とし、メモリデータ自体およびメモリデータ操作に対する改ざん・盗聴、メモリデータに格納される情報を許可なく利用すること、突然の電源断によるデータ破壊・ハードウェア故障によるデータ異常に対抗することができる。

1.2.3 TOEの範囲と動作概要

本TOE は、「モバイル FeliCa IC チップ」上のROMに搭載され、RF I/F、または、UART I/Fから命令情報を受信することにより、TOEの機能が実施され、命令情報に従い不揮発性メモリに格納されているデータ格納領域のデータを操作し、その結果情報を、RF I/F、または、UART I/Fから送信して処理を終了する。本TOEの物理的範囲と「モバイル FeliCa IC チップ」との関係について、以下の図1-1に示す。

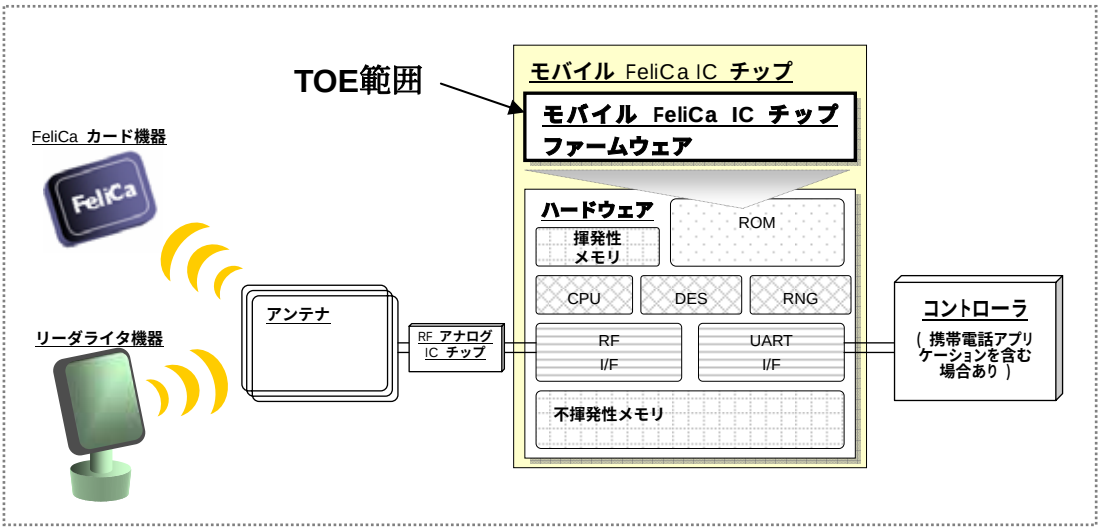

図1-1 物理構成図

1.2.4 TOEの機能

TOE のソフトウェア構成は、処理を制御する役割から Kernel Layer , Middle Layer , Command Layer に区分される。本TOEの構成を以下の図1-2に示す。

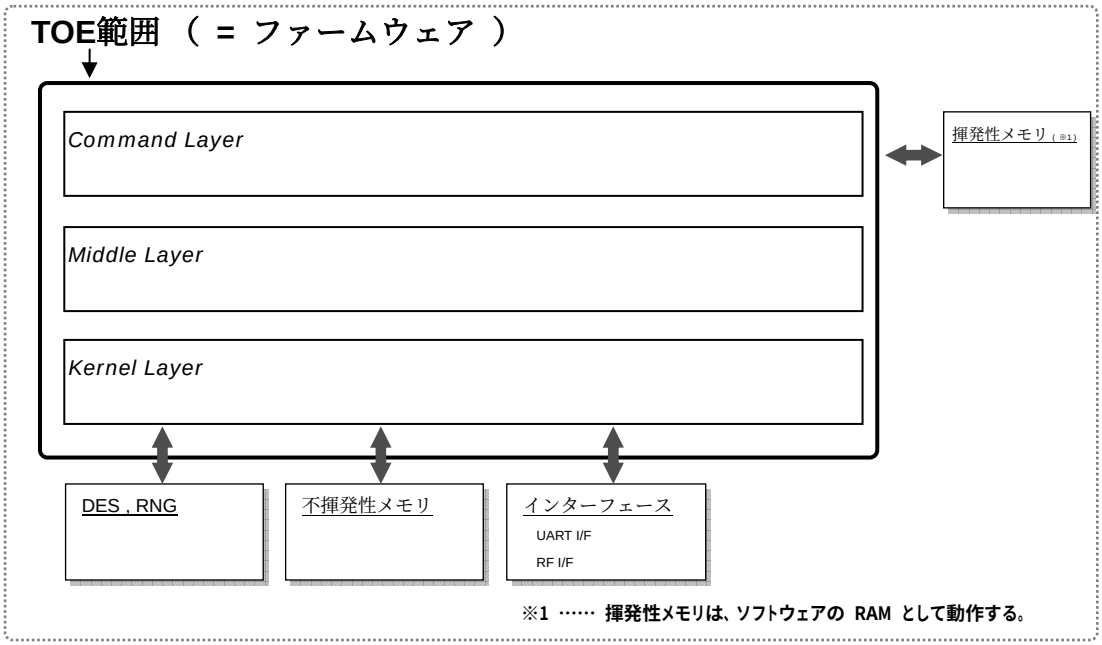

図1-2 論理構成図

Kernel Layer は、モバイル FeliCa IC チップに用意されるハードウェア機能を制御する。本 Layer では、UART I/F の通信制御、RF I/F の通信制御、DES 回路の制御、RNG 回路の制御、不揮発性メモリの制御を行い、単純な機能コンポーネントとして管理する。

Middle Layer は、TOE の動作の制御ならびにデータの管理を行う。本 Layer では、Kernel Layer で受信した命令を解析し、命令に対応する Command Layer の機能を実行する。また、Command Layer で不揮発性メモリのデータを利用する場合には、本 Layer を介し論理的管理と物理的管理を変換して利用する。

Command Layer は、外部インターフェースとして提供される命令情報のコンポーネントで構成される。

1.3 評価の実施

認証機関が運営するITセキュリティ評価・認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[4]

に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

(1) 本TOEのセキュリティ設計が適切であること。
(2) 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。
(3) 本TOEがセキュリティ設計に基づいて開発されていること。
(4) 上記(1)、(2)、(3)を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「モバイル FeliCa IC チップファームウェア (CXD 版) セキュリティターゲット」（以下「ST」という。）[1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発・製造・出荷の現場を調査し、本TOEがCCパート1 ([5][8][11][14]のいずれか) **附属書** C、CCパート2（[6][9][12][15]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート3（[7][10][13][16]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「モバイルFeliCa ICチップファームウェア（CXD版）評価報告書」（以下「評価報告書」という。）[23]に示されている。なお、評価方法は、CEM（[17][18][19]のいずれか）に準拠する。CC及びCEMの各パートは補足（[20][21][22]のいずれか）の内容を含む。

1.4 評価の認証

認証機関は、評価機関が作成した、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、本TOE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。評価は、平成19年10月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEM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。

1.5 報告概要

1.5.1 PP適合

適合するPPはない。

1.5.2 EAL

STが規定するTOEの評価保証レベルは、EAL4追加である。

追加されるコンポーネントはALC_FLR.1及びAVA_VLA.3である。

1.5.3 セキュリティ機能強度

STは、最小機能強度として、”SOF-中位”を主張する。

本 TOE に格納する情報は、国防に関わる国家機密のような極めて重要な情報を保護することまでは想定していないため、攻撃者は国家機密を脅かそうとするほどの強い動機は持ち合わせていない。

以上より、想定する攻撃力は中程度であり、TOE の最小機能強度レベルは、中程度の攻撃力に対抗できる「SOF-中位」が妥当である。

1.5.4 セキュリティ機能

本TOEは、以下のセキュリティ機能を提供する。

・データ読み書き機能(SF.ReadWrite)

データ格納領域に格納されたデータの読み書きを行う。

・データ移動機能(SF.DataMove)

TOE で管理する属性システム・属性エリア・属性サービスおよびデータ格納領域のインポート/エクスポートを行う。

・認証機能(SF.Authentication)

コントローラもしくはリーダライタとの認証を行う機能保護データ・アクセス暗号鍵への操作前に必ず実施される。「保護データ」へのアクセス、「データ移動」の実施、「リーダライタ認証」の実施の前に実行される。

・診断機能(SF.Selfdiagnosis)

TOE の診断を行う機能である。TOE の診断の実施機能を提供する。

・通信路保護機能(SF.CommunicateProtection)

TOE もしくはモバイル FeliCa IC チップが提供する暗号機能により、命令・結果情報に暗号処理を行い、モバイル FeliCa IC チップが提供する CRC 演算機能により受信した命令情報の誤り検出を行う。

・アクセスコントロール機能(SF.AccessControl)

属性サービスによるデータ格納領域のデータへのアクセス制御と、属性システム・属性エリア・属性サービスへの操作に対するアクセス制御を実現。属性サービスのアクセス制御には、簡易な利用可否の PIN 機能を含む。

・データ保護機能(SF.DataProtection)

突然の電源断・ハードウェア故障からデータを保護する機能である。保護データ

ならびにアクセス暗号鍵の書込み中に突然の電源断によりデータが破損しないデータ管理を行う。また、ハードウェア故障によりデータ異常を検知する。

・TSF データ保護機能(SF.TSFDataProtection)

属性システム・属性エリア・属性サービスのアクセス暗号鍵操作時にアクセス暗号鍵を安全に保護する。また、欠陥修正プログラムの保護にも利用する。

1.5.5 脅威

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

表1-1 想定する脅威

識別子	脅 威
T.Abuse_Command_Data	「悪意のある所有者」が、不正なコマンドデータを UART I/F もしくは RF I/F から送信する攻撃が想定される。本攻撃は、次の方法で実施される。 (1)適正範囲外のパラメータにより構成されたコマンドデータを送信し、許可のない保護データへのアクセスを試みる (2)適正範囲外のパラメータにより構成されたコマンドデータを送信し、属性サービスを登録・削除あるいはアクセス暗号鍵の変更を試みる (3)認証範囲外の保護データへアクセスするコマンドデータを送信し、保護データの書き換えを試みる (4)TOE 認証のコマンドデータの組み合わせを総当りで送信し、アクセス暗号鍵を解析する (5)TOE 認証のコマンドデータを故意に失敗させ、認証失敗の応答内容を解析することで認証のためのアクセス暗号鍵を推測する 本攻撃は、 ・モバイル FeliCa IC チップファームウェアの専門知識 ・モバイル FeliCa 機器へコマンドデータを送信できるリーダライタ機器 が必要である。
T.Reuse_Command_Data	「悪意のある所有者」が、コマンドデータを取得し、そのコマンドデータを再送信する攻撃が想定される。本攻撃は、次の方法で実施される。 (1)TOE 認証のコマンドデータを取得・再送信し、認証を成功させ、許可のない保護データへのアクセスを試みる (2)書き込みを行うコマンドデータを取得・再送信し、保護データを書き換える (3)属性システム・属性エリア・属性サービスを操作するコマンドデータを取得・再送信し、再操作を行わせる 本攻撃は、 ・モバイル FeliCa IC チップファームウェアの専門知識 ・モバイル FeliCa IC チップへのコマンドデータ・レスポンスデータを盗聴する機材 ・モバイル FeliCa 機器へコマンドデータを送信できるリーダライタ機器 が必要である。

T.Intercept_Communicate_Data	「悪意のある所有者」が、コマンドデータを盗聴・改ざんする攻撃が想定される。本攻撃は、次の方法で実施される。 (1)認証を行うコマンドデータを盗聴・改ざんし、認証を成功させる (2)書き込みを行うコマンドデータを盗聴・改ざんし、保護データを書き換える (3)読み込みを行うコマンドデータを盗聴・改ざんし、読み込み指定箇所以外の保護データを取得する (4)属性システム・属性エリア・属性サービスを操作するコマンドデータを盗聴・改ざんし、属性システム・属性エリア・属性サービスに対する不正な操作を行う 本攻撃は、 ・モバイル FeliCa IC チップファームウェアの専門知識 ・モバイル FeliCa IC チップへのコマンドデータ・レスポンスデータを盗聴する機材 ・モバイル FeliCa 機器へコマンドデータを送信できるリーダライタ機器 ・コマンドデータ・レスポンスデータを解析する機材もしくは知識 が必要である。
T.Intercept_Security_Data	「悪意のある所有者」が、コマンドデータ・レスポンスデータを盗聴し、その情報からアクセス暗号鍵の解析を試みられる攻撃が想定される。本攻撃は、次の方法で実施される。 (1)属性システム・属性エリア・属性サービスを操作するコマンドデータを盗聴しアクセス暗号鍵を解析する (2)データ移動のコマンドデータ・レスポンスデータを盗聴しアクセス暗号鍵を解析する 本攻撃は、 ・モバイル FeliCa IC チップファームウェアの専門知識 ・モバイル FeliCa IC チップへのコマンドデータ・レスポンスデータを盗聴する機材 ・コマンドデータ・レスポンスデータを解析する機材もしくは知識 が必要である。
T.Abuse_ReaderWriter_SecurityFunction	「悪意のある所有者」が、リーダライタ機能の「カード認証」を不正に利用する攻撃が想定される。本攻撃は、次の方法で実施される。 (1)TOE と認証を行わず、TOE へカード認証を行うコマンドデータを送信し、外部の FeliCa カード機器と認証を成功させることで、許可のない保護データへのアクセスを試みる。 本攻撃は、 ・モバイル FeliCa IC チップファームウェアの専門知識 ・モバイル FeliCa IC チップへ直接データを送信できる機材 が必要である。
T.Interrupt_Power	「悪意のある所有者」が、TOE の保護データおよびアクセス暗号鍵へアクセスしている際TOE の電源を途絶させ、保護データおよびアクセス暗号鍵を改ざん・破壊する攻撃が想定される。本攻撃は、次の方法で実施される。 (1)TOE がデータ書込み処理中に TOE の電源を切り、保護データもしくはアクセス暗号鍵を破壊する (2)TOE がデータ書込み処理中に、TOE をリーダライタから突

	然離し、保護データもしくはアクセス暗号鍵を破壊する 本攻撃は、 ・モバイル FeliCa IC チップファームウェアの専門知識 が必要である。
T.Break_Hardware	「悪意のある所有者」が、TOE が搭載されるモバイル FeliCa IC チップを故障させることで、TOEのセキュリティ機能を危殆化させる攻撃が想定される。本攻撃は、次の方法で実施される。 (1)モバイル FeliCa IC チップに圧力・電圧・加熱・冷却を加えることで、TOEのセキュリティ機能を危殆化させる 本攻撃は、 ・モバイル FeliCa IC チップファームウェアの専門知識 ・モバイル FeliCa IC チップを破壊するための機材 が必要である。
T.Install_EvilProgram	「悪意のある所有者」が、TOE プログラムの欠陥修正プログラムインストール機能を利用し保護データの改変およびアクセス暗号鍵の暴露を行うプログラムをインストールする攻撃が想定される。本攻撃は、次の方法で実施される。 (1)保護データの改変もしくはアクセス暗号鍵の暴露を行うプログラムを TOE の欠陥修正プログラムインストール機能によりインストールし、保護データの改変もしくはアクセス暗号鍵の暴露を行い TOE のセキュリティ機能を無効化する (2)TOE の欠陥修正プログラムインストール時、欠陥修正プログラムを改ざんし保護データの改変もしくはアクセス暗号鍵の暴露を行い TOE のセキュリティ機能を無効化する 本攻撃は、 ・モバイル FeliCa IC チップファームウェアの専門知識 ・モバイル FeliCa IC チップファームウェアの設計知識 ・モバイル FeliCa IC チップファームウェアプログラム開発設備 ・モバイル FeliCa 機器へ任意のデータを送信できるリーダライタ（ もしくは、モバイル FeliCa IC チップへ直接データを送信できる機材 ） が必要である。
T.Copy_TOEData	「悪意のある所有者」が、TOE プログラムのデータ移動機能を利用し保護データおよびアクセス暗号鍵を不正に複製することが想定される。本攻撃は、次の方法で実施される。 (1)データ移動機能で取り出したデータを移動先以外の TOE へ格納することで、保護データおよびアクセス暗号鍵を不正に取得する 本攻撃は、 ・モバイル FeliCa IC チップファームウェアの専門知識 ・モバイル FeliCa 機器へ任意のデータを送信できるリーダライタ（ もしくは、モバイル FeliCa IC チップへ直接データを送信できる機材 ） が必要である。

1.5.6 組織のセキュリティ方針

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はない。

1.5.7 構成条件

本TOEは、ソニー株式会社のモバイル FeliCa IC チップ「CXD3717GG」上で動作する。

1.5.8 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表1-3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1-2 TOE使用の前提条件

識別子	前提条件
A.Key_Storage	TOE で利用するアクセス暗号鍵は、保護データへアクセスする重要な情報である。IC チップ製造者ならびにインフラ事業者・サービス運営者は、TOE に格納するアクセス暗号鍵の作成、設定、運用管理、変更に関わる操作をセキュアに実施し、適切に管理する。
A.Security_Configuration	TOE が管理する IC チップ内のデータ格納領域は、属性サービスに設定されたアクセス手段によりアクセス制御される。サービス運営者は、モバイル FeliCa IC チップでデータを管理する際、データの守秘性が求められる場合には属性サービスのセキュリティ種別を「認証必要」として設定するものとする。
A.ICvendor_Confidence	IC チップ製造者は、配布手順に基づき TOE 開発者から TOE を受領し改変なくモバイル FeliCa IC チップの ROM 領域へ格納し製造するものとする。また、IC チップ製造者は、定められた手順書に従いファームウェアの活性化を実施するものとする。
A.Hardware_Protection	モバイル FeliCa IC チップのハードウェアは、サイドチャネル攻撃に対し耐性を有し TOE が提供する保護データおよびアクセス暗号鍵へのアクセス方法以外の経路を用いて保護データおよびアクセス暗号鍵が取得されることはないものとする。
A.Hardware_DES	モバイル FeliCa IC チップは、暗号アルゴリズム DES を搭載するものとする。
A.Hardware_RNG	モバイル FeliCa IC チップは、乱数生成機能を搭載するものとする。

1.5.9 製品添付ドキュメント

本TOEは、TOEの利用者役割（インフラ事業者、サービス運営者、モバイルFeliCa機器製造者）に応じ以下のドキュメントが提供される。

・モバイルFeliCa ICチップ ユーザーガイダンスマニュアル

・モバイルFeliCa ICチップファームウェア（モバイルFeliCa OS Version 2.0）

プロトコル仕様書～キャリア様向け～

・モバイルFeliCa ICチップファームウェア（モバイルFeliCa OS Version 2.0）

プロトコル仕様書～キャリア様向け（データ移行）～

・モバイルFeliCa ICチップファームウェア（モバイルFeliCa OS Version 2.0）

プロトコル仕様書～フェリカネットワークス　PFシステム開発向け～

・モバイルFeliCa ICチップファームウェア（モバイルFeliCa OS Version 2.0）

プロトコル仕様書～領域管理者様向け～

・モバイルFeliCa ICチップファームウェア（モバイルFeliCa OS Version 2.0）

プロトコル仕様書～サービス提供事業者様向け～

・モバイルFeliCa ICチップファームウェア（モバイルFeliCa OS Version 2.0）

プロトコル仕様書～SAMリーダ／ライタ編～

・モバイルFeliCa ICチップファームウェア（モバイルFeliCa OS Version 2.0）

プロトコル仕様書～移動機メーカ様向け～

・モバイルFeliCa ICチップファームウェア（モバイルFeliCa OS Version 2.0）

プロトコル仕様書～移動機ミドルウェア製造メーカ様向け～

・モバイルFeliCa ICチップファームウェア（モバイルFeliCa OS Version 2.0）

プロトコル仕様書～ソフトウェア開発ボード製造者様向け～

2 評価機関による評価実施及び結果

2.1 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ている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

2.2 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17年8月に始まり、平成19年10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19年7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・配付と運用・ライフサイクル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19年8月に開発者サイトにおいて開発者のテスト環境を使用し、開発者が実施したテストのサンプリングチェックを実施し、さらに9月に同テスト環境を評価者サイトに持ち込んで、評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべ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、すべての問題点が解決されている。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

2.3 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を以下に示す。

2.3.1 開発者テスト

1) 開発者テスト環境

開発者が実施したテストの構成を図2-1に示す。

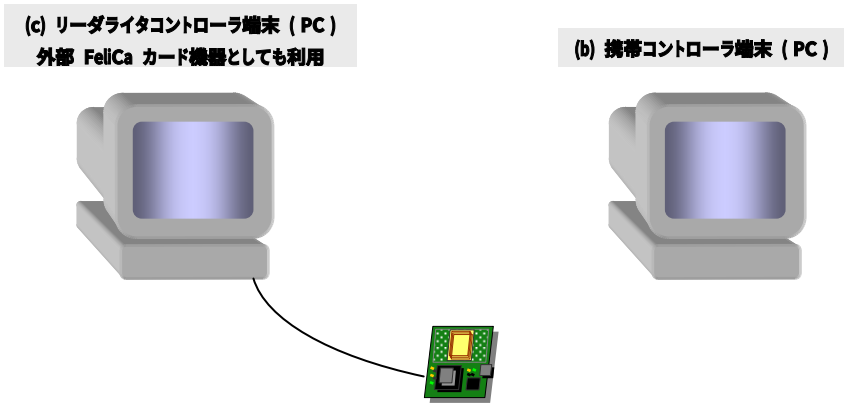

図2-1　開発者テストの構成図

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

a.テスト構成

開発者が実施したテストの構成を図2-1に示す。開発者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

b.テスト手法

テストには、以下の手法が使用された。

①機能評価

外部インタフェース（コマンドインタフェース）を利用したTOEセキュリティ機能のテスト

②ブロークントランザクション評価

デバックコマンドを利用した電源断時のデータ保護アルゴリズムのテスト

③Fault State評価

デバックコマンドを利用したデータ異常時の検知機能のテスト

c.実施テストの範囲

テストは開発者によって33項目実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証されている。深さ分析が実施され、上位レベル設計に記述されたすべてのサブシステムとサブシステムインタフェースが十分にテストされたことが検証されている。

d.結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が

一致していることを確認している。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、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

2.3.2 評価者テスト

1) 評価者テスト環境

評価者が実施したテストの構成は、開発者テストと同様の構成である。

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

評価者が実施したテストの構成を図2-1に示す。評価者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

b.テスト手法

テストには、以下の手法が使用された。

①機能評価

外部インタフェース（コマンドインタフェース）を利用したTOEセキュリティ機能のテスト

②ブロークントランザクション評価

デバックコマンドを利用した電源断時のデータ保護アルゴリズムのテスト

評価者が独自に考案したテストを9項目、開発者のサンプリングによるテストを33項目、計41項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

① 開発者テストで実施されていないパラメータの組み合わせ
② 異なる暗号化方式、アクセス制御方式についての検証の網羅
③ 実際の使用シーンに基づく検証

d.結果

実施したすべての評価者テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

2.4 評価結果

評価報告書をもって、評価者は本TOE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。

3 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 当該所見報告書でなされた指摘内容が妥当であること。
② 当該所見報告書でなされた指摘内容が正しく反映されていること。
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及び評価報告書において、所見報告書及び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た。

4 結論

4.1 認証結果

提出された評価報告書、当該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がCCパート3のEAL4保証要件及びALC_FLR.1+AVA_VLA.3を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

表4-1 評価者アクションエレメント検証結果

評価者アクションエレメント	検証結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_DES.1.1E	評価はワークユニットに沿って行われ、TOE識別、境界の記述が明瞭であることを確認している。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然とし一貫していることを確認している。
ASE_DES.1.3E	評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。
ASE_ENV.1.1E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。
ASE_ENV.1.2E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.1E	評価はワークユニットに沿って行われ、ST及びTOEの識別、概要及びCC適合が明確に述べられていることを確認している。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.3E	評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。

ASE_OBJ.1.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が、脅威、組織のセキュリティ方針、前提条件へ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。
ASE_OBJ.1.2E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_PPC.1.1E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_PPC.1.2E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_REQ.1.1E	評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。
ASE_REQ.1.2E	評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_SRE.1.1E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。

ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
構成管理	**適切な評価が実施された**
ACM_AUT.1.1E	評価はワークユニットに沿って行われ、CMシステムが人為的誤りまたは怠慢による影響を受けないように、実装表現に対する変更が自動化ツールのサポートにより制御されていることを確認している。
ACM_AUT.1.1D	評価はワークユニットに沿って行われ、CM計画に記述されている自動化ツールと手順が使用されていることを確認している。
ACM_CAP.4.1E	評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認している。
ACM_SCP.2.1E	評価はワークユニットに沿って行われ、構成要素リストがCCによって要求される一連の要素を含んでいることを確認している。
配付と運用	**適切な評価が実施された**
ADO_DEL.2.1E	評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。
ADO_DEL.2.2D	評価はワークユニットに沿って行われ、実際に配付手続きが使用されていることを、実地検査により確認している。
ADO_IGS.1.1E	評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。
ADO_IGS.1.2E	評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認している。
開発	**適切な評価が実施された**

ADV_FSP.2.1E	評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んでいることを確認している。
ADV_FSP.2.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。
ADV_HLD.2.1E	評価はワークユニットに沿って行われ、上位レベル設計が明確で矛盾のないこと、サブシステムを規定しそのセキュリティ機能を記述していること、TSF実現に必要なIT環境としてのハードウェアを説明していること、TSFサブシステムの外部とその他のインタフェースが識別され、それらの詳細を記述していることを確認している。
ADV_HLD.2.2E	評価はワークユニットに沿って行われ、上位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。
ADV_IMP.1.1E	評価はワークユニットに沿って行われ、実装表現がTSFを作成できる詳細レベルでTSFを明確に定義していること、開発者の提供した実装表現が十分足るものであること、それが内部的に一貫していることを確認している。
ADV_IMP.1.2E	評価はワークユニットに沿って行われ、実装表現のサブセットがその関連するTOEセキュリティ機能要件を正しく具体化したものであることを確認している。
ADV_LLD.1.1E	評価はワークユニットに沿って行われ、下位レベル設計が必要な説明情報を含み、内部的に一貫していること、モジュールの観点から記述されており、各モジュールの目的を記述していること、提供されるセキュリティ機能という観点でモジュール間の相互関係と依存性を定義していること、TSP実施機能の提供方法を記述していること、TSFモジュールのインタフェースと外部インタフェースを識別していること、各モジュールの使用法と目的を記述していること、そしてTSP実施モジュールとその他に区別できることを確認している。

ADV_LLD.1.2E	評価はワークユニットに沿って行われ、下位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。
ADV_RCR.1.1E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であり、上位レベル設計が機能仕様の正しく完全な表現であり、下位レベル設計が上位レベル設計の正しく完全な表現であることを、それらの対応分析により確認している。
ADV_SPM.1.1E	評価はワークユニットに沿って行われ、セキュリティ方針モデルが非形式的でありSTにおいて明示的方針をもたないこと、ST中のセキュリティ機能要件で表されたすべてのセキュリティ方針がモデル化されていること、セキュリティ方針モデルの規則や特性がモデル化されたTOEのセキュリティふるまいを明確に表していること、モデル化されたふるまいがセキュリティ方針と一貫し完全であること、セキュリティ方針を実装している機能仕様にてすべてのセキュリティ機能を識別していること、機能仕様の内容とセキュリティ方針モデルの実装として識別された機能の内容が一貫していることを確認している。
ガイダンス文書	**適切な評価が実施された**
AGD_ADM.1.1E	評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
AGD_USR.1.1E	評価はワークユニットに沿って行われ、利用者ガイダンスがTOEの管理者でない利用者が利用可能なセキュリティ機能やユーザインタフェース、セキュリティ機能の使用法、対応すべき機能や特権に関する警告、TOEのセキュアな操作に必要なすべての利用者責任が記述してあり、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
ライフサイクルサポート	**適切な評価が実施された**

ALC_DVS.1.1E	評価はワークユニットに沿って行われ、開発セキュリティ証拠資料がTOE開発環境のセキュア維持のための手段を記述しており、それが十分であること、その手段を実施した記録が生成されることを確認している。
ALC_DVS.1.2E	評価はワークユニットに沿って行われ、ALC_DVS.1.1Eで確認したセキュリティ手段が実施されていることを確認している。また、本評価時に行われたサイト訪問での調査方法も適切と判断される。
ALC_LCD.1.1E	評価はワークユニットに沿って行われ、使用されたライフサイクルモデルが開発者と保守手続きをカバーしており、その記述にある手続き、ツール、技法の使用が開発と保守に貢献していることを確認している。
ALC_TAT.1.1E	評価はワークユニットに沿って行われ、開発ツール証拠資料が明確であり、実装に用いられた開発ツールのステートメント及び実装依存オプションの意図を明確に定義していることを確認している。
ALC_FLR.1.1E	評価はワークユニットに沿って行われ、欠陥修正手続き証拠資料がすべてのセキュリティ欠陥を追跡するために使用される手続き、及びTOE利用者に必要な情報を提供するための手段を含み、この手続きの適用により、欠陥訂正方法の調査状況と同時に各々のセキュリティ欠陥の性質と影響に関する記述が提供されることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
テスト	**適切な評価が実施された**
ATE_COV.2.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。

ATE_DPT.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが上位レベル設計に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。
ATE_FUN.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果を含んでおりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。
ATE_IND.2.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。
ATE_IND.2.2E	評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。また、本評価時に行われたテスト実施方法も適切と判断される。
ATE_IND.2.3E	評価はワークユニットに沿って行われ、サンプリングテストを実施し、結果が期待されるべき結果と一貫していることを確認している。また、本評価のサンプリング方針及びテスト実施方法も適切と判断される。
脆弱性評定	**適切な評価が実施された**
AVA_MSU.2.1E	評価はワークユニットに沿って行われ、提供されたガイダンスがTOEのセキュアな運用に必要な情報を矛盾なく完全に記述していること、使用環境の前提事項、TOE以外のセキュリティ事項の要件がすべて明記されていること、ガイダンスの完全性を保証する手段を開発者が講じていることを確認している。

AVA_MSU.2.2E	評価はワークユニットに沿って行われ、提供されたガイダンスの管理者と利用者手続き、あるいはその他の手続き情報のみで、TOEを構成でき、TOEのセキュアな運用に関わる設定が行えることを確認している。
AVA_MSU.2.3E	評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEが非セキュアな状態に陥ったことを検出する手段及び対処方法を記述していることを確認している。
AVA_MSU.2.4E	評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEの全ての操作モードにおいてのセキュアな操作を提供していることを確認している。
AVA_SOF.1.1E	評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされていることを確認している。
AVA_SOF.1.2E	評価はワークユニットに沿って行われ、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しいことを確認している。
AVA_VLA.3.1E	評価はワークユニットに沿って行われ、脆弱性分析が脆弱性に関する情報を考慮していること、識別された脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。
AVA_VLA.3.2E	評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。
AVA_VLA.3.3E	評価はワークユニットに沿って行われ、開発者がまだ扱っていない脆弱性の可能性を検査している。
AVA_VLA.3.4E	評価はワークユニットに沿って行われ、独立脆弱性分析に基づく侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテストの概要について報告がなされている。

AVA_VLA.3.5E	評価はワークユニットに沿って行われ、意図する環境においてTOEが低い攻撃力に対抗できることを侵入テストと脆弱性分析の結果から検査し、悪用され得る脆弱性及び残存脆弱性が存在しないことが報告されている。

4.2 注意事項

特になし。

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

6 参照

[1] モバイル FeliCa IC チップファームウェア(CXD 版) セキュリティターゲット Version 1.01 2007 年 6 月 29 日

[2] ITセキュリティ認証申請等の手引き 平成16年4月 独立行政法人情報処理推進機構 ITQM-23

[3] ITセキュリティ評価機関に対する要求事項 平成16年4月 独立行政法人情報処理推進機構 ITQM-07

[4] ITセキュリティ認証申請者・登録者に対する要求事項 平成16年4月 独立行政法人情報処理推進機構 ITQM-08

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[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1: 概説と一般モデル バージョン2.1 1999年8月 CCIMB-99-031

[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2: セキュリティ機能要件 バージョン2.1 1999年8月 CCIMB-99-032

[10] 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: セキュリティ保証要件 バージョン2.1 1999年8月 CCIMB-99-033

[11] ISO/IEC 15408-1 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model ISO/IEC15408-1: 1999(E)

[12] ISO/IEC 15408-2 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements ISO/IEC15408-2: 1999(E)

[13] ISO/IEC 15408-3 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements ISO/IEC15408-3: 1999(E)

[14] JIS X 5070-1: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第1部: 総則及び一般モデル

[15] JIS X 5070-2: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第2部: セキュリティ機能要件

[16] JIS X 5070-3: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第3部: セキュリティ保証要件

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part2: Evaluation Methodology Version 1.0 August 1999

[18] 情報技術セキュリティ評価のための共通方法論 CEM-99/045 パート2: 評価方法論 バージョン1.0 1999年8月

[19] JIS TR X 0049: 2001 情報技術セキュリティ評価のための共通方法

[20] CCIMB Interpretations-0407

[21] 補足-0210 第2版

[22] 補足-0470

[23] モバイルFeliCa ICチップファームウェア（CXD版）評価報告書　第2版 2007年10月9日