FeliCa Networks

モバイル FeliCa IC チップファームウェア
(AE 版)
セキュリティターゲット

Version 1.06
No. FN12-F027-J01-06
Date: 2009/02/04
フェリカネットワークス株式会社

はじめに

本書は、モバイル FeliCa IC チップに搭載するファームウェアのセキュリティターゲットです。本書は、ISO / IEC 15408 の セキュリティターゲット の役割を持ちます。

「ISO / IEC 15408」とは、情報技術セキュリティの観点から、情報技術に関連した製品およびインターネットシステムが適切に設計され、その設計が過不足なく実装されていることを客観的に評価・保証するために必要な各種事項を定義する国際標準規格です。

■ 改訂履歴

版数	変更日時	変更箇所
第 1.00 版	2008/03/14	・ 新規作成
第 1.01 版	2008/05/29	・ 「1.5.2 用語」に「セキュアリーダ／ライタ」を追加
第 1.01 版	2008/05/29	・ 「3.2 前提条件」の A.Reader_Writer_Management を修正
第 1.01 版	2008/05/29	・ 「4.2 環境のセキュリティ対策方針」の OE.Reader_Writer_Management を修正
第 1.02 版	2008/07/17	・ 「1.1.1 ST 識別情報」を修正
第 1.02 版	2008/07/17	・ 「1.1.1 TOE 識別情報」の ROM バージョンを修正
第 1.02 版	2008/07/17	・ 「3.2 前提条件」の誤字を修正
第 1.02 版	2008/07/17	・ 「4.2 環境のセキュリティ対策方針」の OE.Reader_Writer_Hardware_Protection 、 OE.Reader_Writer_Hardware_Protection を修正
第 1.02 版	2008/07/17	・ 「第 5 章 IT セキュリティ要件」の記述を CC Ver2.3 対応に修正
第 1.02 版	2008/07/17	・ 「8.2.2 セキュリティ機能要件依存性」の表現を修正
第 1.03 版	2008/08/29	・ 「第 5 章 IT セキュリティ要件」の記述を CC Ver2.3 対応に修正
第 1.03 版	2008/08/29	・ 「3.2 前提条件」の項目名を修正
第 1.03 版	2008/08/29	・ 「4.2 環境のセキュリティ対策方針」の OE.Reader_Writer_Hardware_Protection 、 OE.Reader_Writer_Management を修正
第 1.03 版	2008/08/29	・ 「1.1.2 TOE 識別情報」の ROM バージョンを更新
第 1.04 版	2008/11/12	・ 記述ゆれを修正
第 1.05 版	2008/11/20	・ 記述ゆれを修正
第 1.06 版	2009/02/04	・「3.2 前提条件の」A.Reader_Writer_Hardware_Protection と「4.2 環境のセキュリティ対策方針」の OE.Reader_Writer_Hardware_Protection を修正
第 1.06 版	2009/02/04	・「5.1.1.2 クラス FDP」の誤記修正

目次

第１章 概説

本章では、ST 識別・TOE 識別・ST概要・CC 適合・参考文献・表記規則・用語・略語を記述する。

1.1. ST 識別

1.1.1 ST 識別情報

名称： モバイル FeliCa IC チップファームウェア（AE 版）セキュリティターゲット

バージョン： Version 1.06

識別名： FN12-F027-J01-06

作成日： 2009 年 2 月 4 日

作成者： フェリカネットワークス株式会社

キーワード： FeliCa ，非接触 IC カード ，非接触 IC カードリーダ／ライタ ，モバイル FeliCa , FeliCa 搭載携帯電話

CCバージョン： CC v2.3 (IPA翻訳第1.0版)、補足-0512 (Interpretations-0512)

1.1.2 TOE 識別情報

名称 ： モバイル FeliCa IC チップファームウェア（AE 版）

ROM バージョン ： 02（AE56D1版）

作成者 ： フェリカネットワークス株式会社

1.2. ST 概要

本書は、IT機器に搭載される モバイル FeliCa IC チップに搭載するファームウェアの「セキュリティターゲット」である。

モバイル FeliCa IC チップは、携帯電話やリーダ／ライタに搭載される。

本 IC チップは、接触のインターフェースによってデータ格納を行う「有線 IC カード機能」と非接触のインター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 つの利用用途を持つ。これらの機能が携帯電話に搭載された場合、リーダ／ライタから IC チップのメモリデータへの「データ読み込み」「データ書き込み」・携帯電話のアプリケーションからの IC チップのメモリデータへの「データ読み込み」「データ書き込み」・携帯電話のアプリケーションから外部の FeliCa カード機器へのアクセスに利用される。携帯電話のアプリケーションでは、携帯電話の特徴を活かしたインターネット上のサーバとのデータアクセスも可能である。

モバイル FeliCa IC チップにおける「無線 IC カード機能」は、ソニー株式会社が開発した「 FeliCa 技術方式 」に準拠する。したがって、モバイル FeliCa IC チップは、FeliCa 技術方式を採用した電子マネーや交通システムへの適用が可能である。

さらに、携帯電話の入力機能・表示機能・通信機能と組み合わせることで、ポイントサービスや会員サービス、電子マネーサービスなど様々なサービスが実現可能である。これらのサービスにおける情報の基本的管理を担うことから、TOE であるモバイル FeliCa IC チップファームウェアは、安全性・堅牢性が重要である。

TOE は、「無線 IC カード機能」「有線 IC カード機能」と「リーダ／ライタ機能」を有する。これらの機能は、IC チップ内のメモリデータを保護するためのセキュリティ機能を含んでいる。本書は、TOE に対してセキュリティ脅威の分析・対策方針・機能要件・セキュリティ機能を策定し、TOE の安全性・堅牢性を証明することを目的とする。

TOE が保護する IC チップ内のメモリデータは、電子マネーや交通システムで利用される重要なデータを格納する。そのため、TOE の脅威は IC チップに格納される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・盗聴である。また、本 TOE をリーダ／ライタ機能として利用する場合に、外部の非接触 IC カードへアクセスするために必要な情報を IC チップ内のメモリデータに格納できる。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は脅威である。これらの脅威に対して、TOE は「認証」・「アクセス制御」・「暗号通信」のセキュリティ機能により脅威を防ぐ。これらのセキュリティ機能に加え、「データ保護」機能により、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を防止する。本セキュリティ機能群により TOE は、データの安全な運用を可能とする。

なお、本書が示す AE 版とは、株式会社ルネサステクノロジのモバイル FeliCa IC チップ「AE56D1」に搭載される モバイル FeliCa IC チップファームウェアを指す。

1.3. CC 適合

本 ST は、以下を満たす。

- CC v2.3 パート 2 適合
- CC v2.3 パート 3 適合
- 「補足-0512 (Interpretations)」適合
- コンポーネント AVA_VLA.3 , ALC_FLR.1 を用いた EAL 4 追加
- 適合する PP は存在しない

1.4. 参照文献

- Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model August 2005 Version 2.3 CCMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements August 2005 Version 2.3 CCMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements August 2005 Version 2.3 CCMB-2005-08-003
- 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 2005年8月 バージョン 2.3 CCMB-2005-08-001（平成17年12月翻訳代1.0版 独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ認証室）
- 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 2005年8月 バージョン 2.3 CCMB-2005-08-001（平成17年12月翻訳代1.0版 独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ認証室）
- 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 2005年8月 バージョン 2.3 CCMB-2005-08-001（平成17年12月翻訳代1.0版 独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ認証室）
- 補足-0512 (Interpretations-0512)

1.5. 表記規則・用語・略語

1.5.1 表記規則

全章で共通の表記規則は、以下のとおりとする。

記述	世間一般で利用される用語ではなく TOE で規定する特別な用語を表す
記述	記述を強調する場合に用いる
記述	記述を強調する場合に用いる
記述	記述を強調する場合に用いる

5 章に記載される IT セキュリティ要件の記載方法は、以下の形式とする。

[記述]	割付を表す
< 記述 >	選択を表す
{ 記述 }	詳細情報を記載事項の下に表す
FCS_CKM.1a	機能要件において繰り返しを適用する場合を表す

1.5.2 用語

モバイル FeliCa IC チップ
: FeliCa 技術方式に対応した IC チップ

モバイル FeliCa 機器
: モバイル FeliCa IC チップを搭載したモバイル機器 または リーダ／ライタ

モバイル機器アプリケーション
: モバイル FeliCa 機器内にダウンロードされるアプリケーション。モバイル FeliCa IC チップを含む、モバイル FeliCa 機器の各種リソースを制御し、多様なアプリケーションが作成可能。

IC チップ製造者
: TOE が格納される モバイル FeliCa IC チップを製造する者

所有者
: モバイル FeliCa 機器を所持している者

モバイル FeliCa 機器製造者
: モバイル FeliCa 機器の製造者

インフラ事業者
: モバイル FeliCa 機器を管理・運営する者

サービス運営者
: モバイル FeliCa IC チップでデータを管理し、所有者にモバイル FeliCa 機器を利用したサービスを提供す

る者

FeliCa 技術方式
ソニーが開発した非接触 IC カード技術方式

Real World
実際の環境下を指す。交通システムにおける改札や店舗における POS 端末がこれにあたる。

Cyber World
インターネットなどのネットワーク環境下を指す。インターネットショッピングモールやインターネットチケット販売システムなどがこれにあたる。

RF アナログ IC チップ
アンテナからの 13.56 MHz の搬送波によるデータ送受信を実現するアナログ IC チップ

不揮発性メモリ
電源が遮断されても記憶内容を保持することができる半導体メモリのこと。EEPROM 、フラッシュメモリなどがこれにあたる

揮発性メモリ
電源が遮断されると記憶内容が失われる半導体メモリのこと

コントローラ
モバイル FeliCa IC チップを制御する制御装置または、ソフトウェアを指す。モバイル FeliCa 機器の基幹ソフトウェアやモバイル機器アプリケーションを指す

FeliCa カード機器
ソニーの FeliCa 技術方式による 非接触 IC カードならびに、同技術を搭載したリーダ／ライタを除くモバイル FeliCa 機器

リーダ／ライタ
13.56 MHz の搬送波を用いて外部 FeliCa カード機器とデータの送受信を行う機器

セキュアリーダ／ライタ
リーダ／ライタの中でも特に、外部 FeliCa カードとのデータ送受信をセキュアな環境で行う機器

RF I/F
TOE の FeliCa 技術方式からのアクセス経路を指す

UART I/F
TOE のコントローラとのアクセス経路を指す

属性*サービス*
TOE で管理される不揮発メモリのデータを管理する定義情報

属性*エリア*
TOE で管理される属性サービスを管理する定義情報

属性*システム*
TOE で管理されるエリアを管理する定義情報

属性情報の識別ID

属性*サービス*・属性*エリア*・属性*システム*を識別する ID であり、格納領域種別・アクセス種別・セキュリティ種別を特定できる情報を有する

1.5.3 略語

CC	: Common Criteria
EAL	: Evaluation Assurance Level
PP	: Protection Profile
TOE	: Target of Evaluation
TSF	: TOE Security Function
CPU	: Central Processing Unit
EEPROM	: Electrically Erasable Programmable Read-Only Memory
RAM	: Random Access Memory
ROM	: Read Only Memory
CRC	: Cyclic Redundancy Check

第２章 TOE 記述

本章では、TOE の概要を述べ、セキュリティ要件と使用方法の理解の助力とすると共に、TOE 境界の定義を記載する。

2.1. モバイル FeliCa IC チップファームウェア

TOE である「モバイル FeliCa IC チップファームウェア」は、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ソフトウェアである。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する。

TOE では、暗号アルゴリズムに TDEA 以外に DES による暗号通信もサポートする。DES の採用は、TOE が準拠する FeliCa 技術方式において様々なサービスが既に運用され、これらサービスでの暗号アルゴリズム移行期間を確保するためである。そのため、暗号アルゴリズム移行以外の用途では TDEA を利用推奨する。

なお、TOE は IC チップのメモリデータを管理するものであり、一般的な非接触 IC カードが有しているアプリケーションのダウンロードはサポートしない。

2.2. モバイル FeliCa IC チップ

「モバイル FeliCa IC チップファームウェア」が搭載される IC チップを「 モバイル FeliCa IC チップ 」と呼ぶ。「モバイル FeliCa IC チップ」は、外部のリーダ／ライタとのアクセスを行う無線 IC カード機能向けのインターフェース (以下、RF I/F と記載) とモバイル機器アプリケーションとのアクセスを行う有線 IC カード機能向けのインターフェース (以下、UART I/F と記載) の 2 つのインターフェースを備える。本 2 つのインターフェースを介し、「モバイル FeliCa IC チップファームウェア」の制御下で IC チップ内のメモリデータのアクセスが行われる。これに加え、モバイル FeliCa IC チップは外部の FeliCa カード機器のデータを読み取るリーダ／ライタとしても利用可能である。

TOE が搭載されるモバイル FeliCa IC チップは、ルネサステクノロジ株式会社の「モバイル FeliCa IC チップ用 AE56D1 」を対象とする。

「モバイル FeliCa IC チップ」が提供する機能は、以下のとおりである。

1. 外部のリーダ／ライタからのアクセスにより、セキュリティを備えたデータ格納機能を提供する。本利用方法を「無線 IC カード機能」と呼称する。
2. モバイル機器アプリケーションからのアクセスに対しセキュリティを備えたデータ格納機能を提供する。本利用方法を「有線 IC カード機能」と呼称する。
3. モバイル機器アプリケーションから、外部のFeliCa カード機器との通信機能を提供する。本利用方法を「リーダ／ライタ機能」と呼称する。
4. 外部のリーダ／ライタとモバイル機器アプリケーションとの通信機能を提供する。本利用方法を「アドホック通信機能」と呼称する。

「無線 IC カード機能」は、RF I/F の先にアンテナと無線制御 IC チップにより動作する。本部分は、FeliCa 技術方式に準拠する。FeliCa 技術方式は、ソニー株式会社が開発した非接触 IC カード技術に関する技術方式の総称であり、通信方式・ファイルシステム・セキュリティ・コマンドなどを規定している。FeliCa 技術方式の無線通信方式は、ISO/IEC18092 (212Kbps,passive mode) に準拠し、動作周波数は 13.56 MHz、データ転送速度は 212 Kbps である。FeliCa 技術方式は、偽造・変造がしにくく、高い安全性を持ちながらスピーディなデータの送受信が可能であり、「かざすだけ」という非接触方式ならではの使いやすさが特徴である。また、マルチアプリケーションが可能で、1枚のカードで電子マネーや社員証等の複数用途での利用ができる。

2.3. モバイル FeliCa システム

モバイル FeliCa IC チップを搭載した携帯電話などのモバイル FeliCa 機器は、FeliCa 技術方式の特徴を活かし、交通システムや電子マネー等多くのサービスで利用可能である。
これに加え、モバイル機器特有の機能である液晶ディスプレイでの「表示機能」「ネットワーク機能」・「入力機能」を活用することで、様々なサービスが実現可能となる。これらモバイル機器と融合したサービスを「 モバイル FeliCa 」と呼ぶ。

2.4. 想定アプリケーション

TOE で想定されるサービスアプリケーションは以下のとおりである。

金融

決済手段として、電子マネー・クレジット・デビット等がある。このような通貨の価値は非常に高く不正な変更から防御されなければならない。

身分証明書

身分証明書は、通常証明書の提供者によって、さまざまな権利や義務に結びつけられている。証明書の例として社員証・会員証・免許証・パスポート等がある。身分証明書は、所有者であっても簡単に変更できないようにすることで、重要な価値を持たせている。したがって、不正な変更から防御しなければならない。

情報の安全な蓄積

安全な方法で蓄積されるべき有用な情報には、医療記録、健康保険または、その他医療に関わる情報がある。

ポイントサービス

代表的なものに、航空会社によって提供されるマイレッジ・サービスがある。これは、サービス規則にしたがってポイントが IC チップに加算・減算される。このようなポイントの価値は高く、不正な変更から防御されなければならない。

ネットワークアクセス

ユーザ認証に利用するパスワードのように､IC チップがコンピュータネットワークへのアクセス権を保証する。

移動体通信

移動体通信機器のハードウェアから、加入者識別手段を分離独立させる目的に利用されるもので、代表的なものに、GSM 携帯電話用の SIM (Subscriber Identify Module : 加入者識別モジュール) カードがある。このカードには、IC カードタイプと小型のプラグインタイプがあり、ID 番号や電話番号等の個人情報や電話会社情報が記録されている。

2.5. システム構築例

リーダ／ライタとして構成された場合の構築例を「図 2-1 代表的なリーダ／ライタシステム構成」に記載する。また、代表的な「 モバイル FeliCa システム 」の構築例を「図 2-2 代表的なモバイルシステム構成」に示す。

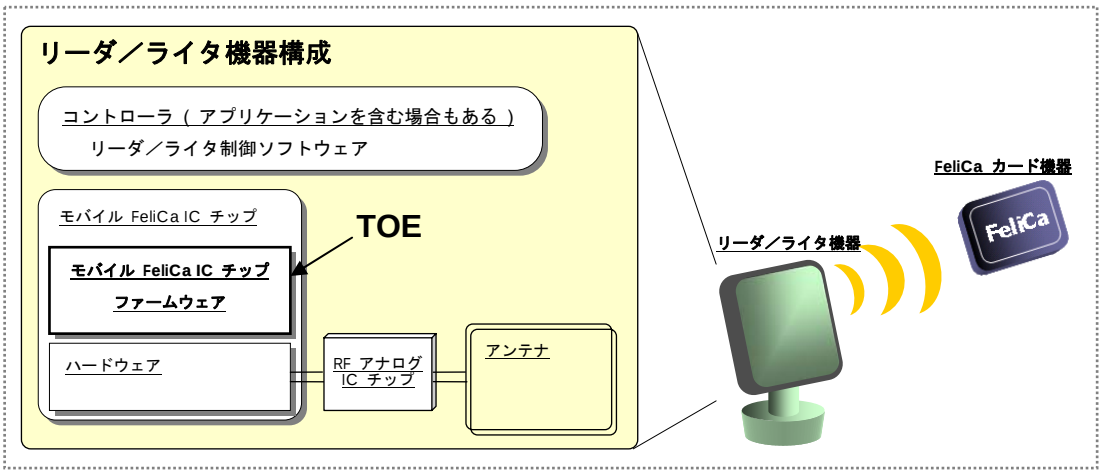

図 2-1 代表的なリーダ／ライタシステム構成

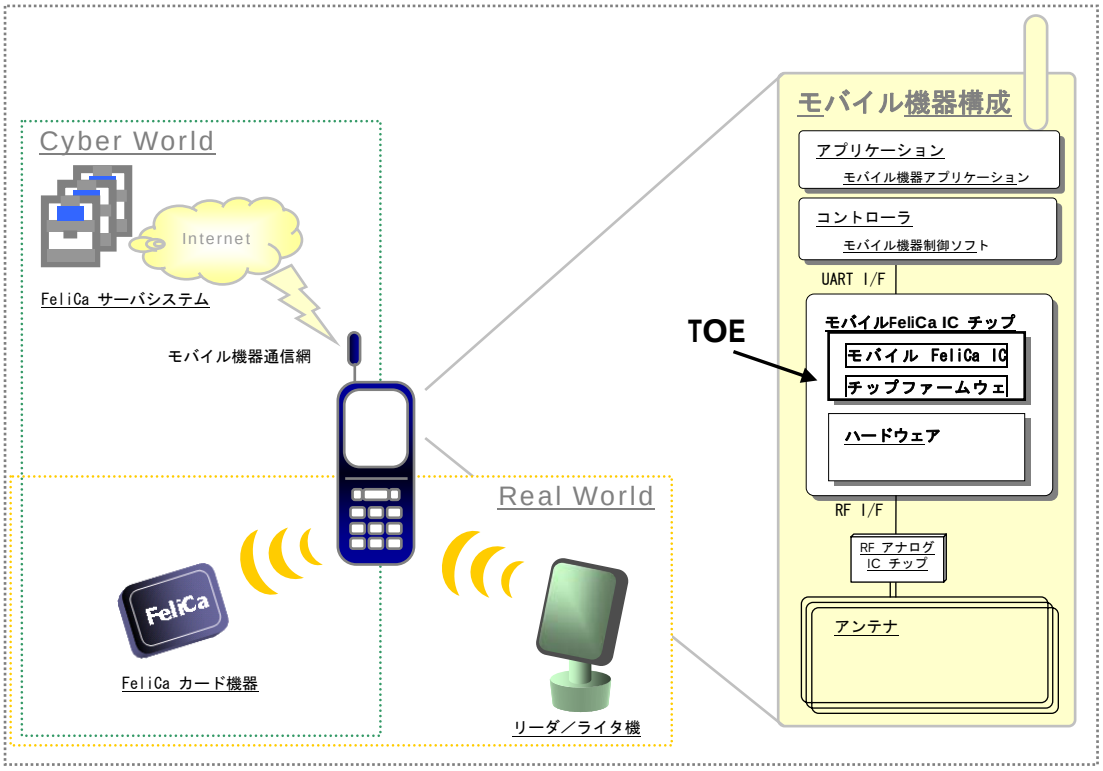

図 2-2 代表的なモバイルシステム構成

各システム構成における利用用途を、「表 2-1 利用用途例」に記載する。

表 2-1 利用用途例

利用方法		用途例	利用機能
(1)	外部 FeliCa カード機器との通信	レジ端末、改札機	リーダ／ライタ機能
(2)	Real World から モバイル FeliCa IC チップへのデータアクセス	電子財布、ポイントカード、定期券、乗車券	無線 IC カード機能
(3)	Cyber World から モバイル FeliCa IC チップへのデータアクセス	価値情報(お金・チケット)のダウンロード、重要データの読取り	有線 IC カード機能
(4)	モバイル機器アプリケーションから モバイル FeliCa ICチップへのデータアクセス	履歴閲覧、ポイント参照、残高参照	有線 IC カード機能
(5)	(3)～(4)におけるモバイル FeliCa IC チップを介した外部 FeliCa カード機器とのデータアクセス	外部 FeliCa カード機器に対する(3)～(4)の用途例	リーダ／ライタ機能
(6)	Real World から モバイル FeliCa IC チップを介して モバイル機器アプリケーションへデータを送受信	Real World からのモバイル機器アプリケーション起動、モバイル機器へのデータ転送	アドホック通信機能

「表 2-1 利用用途例」に記載される (1) ～ (6) を組み合わせることで、多様なサービスが実現可能である。

2.6. TOE 機能概要

TOE および モバイル FeliCa IC チップが実現する「有線 IC カード機能」「無線 IC カード機能」は、TOE で管理するデータに対し「データ読み込み」「データ書き込み」「データ移動」の 3 つの利用要素から構成される。また、「リーダ／ライタ機能」は外部 FeliCa カード機器に対して「カード認証」「カード通信」の 2 つの利用要素から構成される。

「データ読み込み」と「データ書き込み」は、TOE で管理されるデータ格納領域へのアクセスを行う。データ格納領域へのアクセスの可否は、セキュリティ機能である**アクセス制御**および**認証**により決定される。**アクセス制御**によるアクセスの可否は、データ格納領域に設定された属性*サービス*により判断される。属性*サービス*は、データ格納領域へのアクセス手段を規定しており、規定された手段以外のアクセスを拒否する。複数のアクセス手段を用いてデータ格納領域へアクセスしたい場合は、データ格納領域に対して属性*サービス*を複数設定することができる。**認証**によるアクセスの可否は、アクセスしたいデータ格納領域に設定された属性*サービス*のアクセス暗号鍵を用いた認証範囲により判断される。加えて、セキュリティ機能の**暗号通信**により、コントローラ（ もしくはリーダ／ライタ ）と TOE との間でやりとりされる情報に暗号処理が行われる。

「データ移動」は、TOE で管理されるメモリデータを別 TOE へ移動する。一般的に電子データの移動では、データが複製されることが問題となる。TOE では、データを特定の TOE へ移動することを制約するため、移動元の TOE と移動先の TOE で**認証**を必須とする。加えて、移動元の TOE は、データ移動時にメモリデータを利用させないようにすることで、データの複製を防止する。また、移動元の TOE と移動先の TOE 間は、**暗号通信**されることにより盗聴・改ざんを防止する。

「カード認証」は、TOE がリーダ／ライタとなり、TOE で保管される情報を元に TOE にかざされた外部 FeliCa カード機器との認証を行う。TOE で保管される情報は、情報の所有者であるサービス運営者以外のアクセスを拒否することが必要である。そのため、TOE で保管される情報を利用する「カード認証」は、TOE とコントローラとの**認証**を必須とする。

「カード通信」は、TOE のコントローラ側からのコマンドを外部 FeliCa カード機器へ送信し、外部 FeliCa カード機器からの応答を、コントローラ側へ返送する。本機能は、外部 FeliCa カード機器との暗号通信路を提供する。カードとの通信の実行可否は、TOE との「カード認証」が前提となる。

これらの機能を保護する**認証**と**暗号通信**は、密接に関連した構成を取る。認証時で利用した乱数を暗号通信の暗号鍵として利用する。本乱数をセッション鍵と呼ぶ。これらのセキュリティ機能群により、TOE はデータ格納領域のデータへの不正アクセスやリーダ／ライタの不正利用を防止する仕組みを持つ。

「データ読み込み」「データ書き込み」における TOE で利用可能な属性*サービス*のアクセス手段を規定するパラメータを「**表 2-2 属性サービスのパラメータ**」に示す。アクセス制御対象となるパラメータは、「アクセス種別」「PIN設定」「プライバシー設定」である。

表 2-2 属性*サービス*のパラメータ

属性*サービス*のパラメータ	パラメータ内容
格納領域種別	ランダムアクセス サイクリックアクセス パースアクセス
アクセス種別	読み込みのみ 読み書き
セキュリティ種別	認証必須 (通信暗号化) 認証不要 (通信非暗号)
PIN 設定	入力必要 入力不要
プライバシー設定	隠蔽 公開

格納領域種別は、データ格納領域のデータをどのように操作するかを規定する。ランダムアクセスは格納されたデータを直接読み書きする格納方式であり、サイクリックアクセスは古いデータから上書きしてゆく循環型の格納方式である。パースアクセスは、格納されたデータに対して演算(減算)のみを指示し結果を記録させる格納方式である。

アクセス種別は、データ格納領域を読み込みのみで扱うか、読み書きが行えるかを設定するものである。

セキュリティ種別は、データ格納領域のデータを安全に運用するか、特に安全性を必要としないかを設定する。安全に運用する場合には、アクセス前に属性*サービス*に設定されたアクセス暗号鍵による認証を必要とし、またコントローラ (もしくはリーダ／ライタ) と TOE 間の通信も暗号化される。安全性を必要としない場合は、認証が必要なく暗号処理も行われない。TOE で保護するデータは、セキュリティ種別に認証必要を設定された属性*サービス*を持つデータ格納領域である。

PIN 設定は、データ格納領域へアクセスするために 4 バイトのパスワードを必要とするか否かを設定するものである。PIN は、利用の可否を制御することに利用される。

プライバシー設定は、データ格納領域を含む属性*エリア*・属性*サービス*の存在を隠蔽するかどうかを設定するものである。

TOE のデータを管理する機能として、属性*サービス*のほか、属性*エリア*・*システム*が用意される。属性*エリア*・属性*システム*を含めた TOE のメモリ管理概念を、「図 2-3 メモリデータ管理方法」に示す。

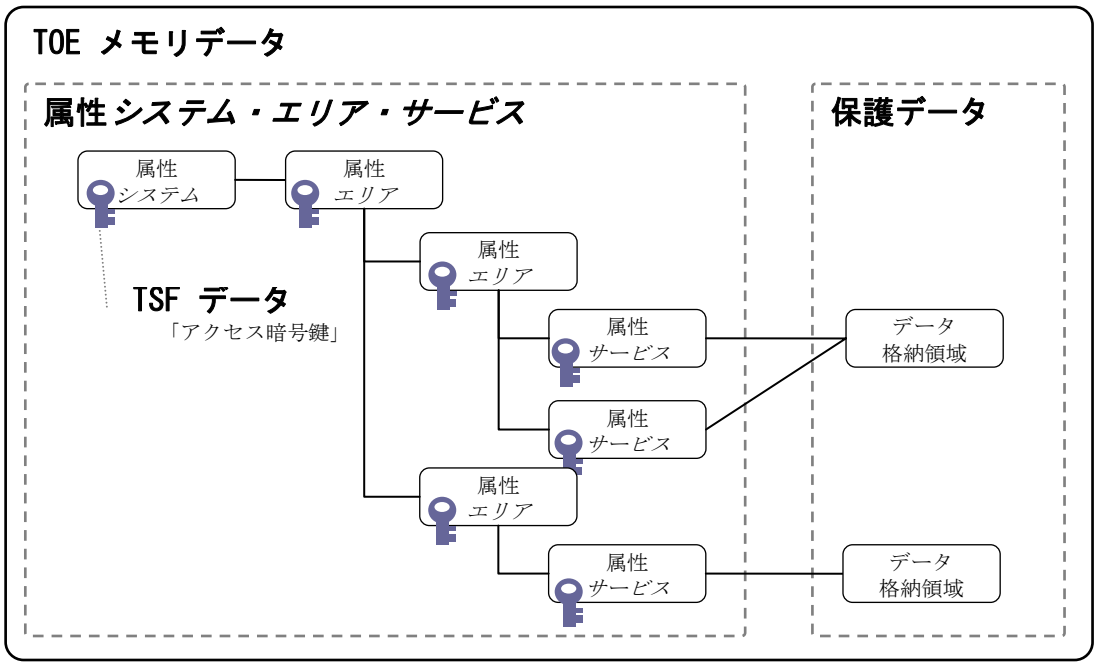

図 2-3 メモリデータ管理方法

属性*エリア*は、配下の属性*エリア*や属性*サービス*の範囲・サイズを定義する。属性*サービス*を登録・削除するには、上位の属性*エリア*のアクセス暗号鍵が必要である。属性*システム*は、外部リーダ／ライタから補足するための識別情報を有する。本識別情報は、希望のデータ格納領域を持っているかどうかの選択に利用できる。また、複数の属性*システム*が存在する場合も、属性*システム*が持つ識別情報により、希望のデータ格納領域を持つ属性*システム*が選択可能である。本 TOE では、複数の属性*システム*を持つことが可能である。属性*システム*・属性*エリア*・属性*サービス*の構成により、マルチアプリケーションが実現される。

上述の管理方法で管理されるメモリデータは、モバイル FeliCa IC チップ内の不揮発性メモリに記録される。モバイル FeliCa IC チップは、リーダ／ライタの電波により電源の ON / OFF が行われることから、不揮発性メモリの書き込み中に電源が落ちることも容易に想定される。そのため、不揮発性メモリのデータが破損されないようにデータを 2 重で管理するようなデータ保護の仕組みも TOE で実現される。

TOE では、前述の機能以外に TOE プログラムの欠陥修正を行う機能を備える。本機能は、TOE の特定箇所の動作をメモリデータに配置されたプログラムに代替させるものである。メモリデータへのプログラム配置には、TOE との**認証**を必須とし不正なプログラムがインストールされないようにプログラムを確認する。

2.7. 物理構成

「 モバイル FeliCa IC チップファームウェア 」に関する物理構成を、「 図 2-4 物理構成図 」に示す。TOE は、「 モバイル FeliCa IC チップ 」上の ROM に搭載される。TOE の機能は、RF I/F と UART I/F の 2 つのインターフェースの命令情報を受信することにより実施される。命令を受信した TOE は、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する。操作した結果情報は、RF I/F , UART I/F から送信され処理が終了する。データ格納領域のデータは、モバイル FeliCa IC チップに電源が供給されていない場合でも保持される不揮発性メモリに格納する。TOE 対象範囲は、ROM に焼き付けられたファームウェアであり、ハードウェアとしての ROM は対象外である。

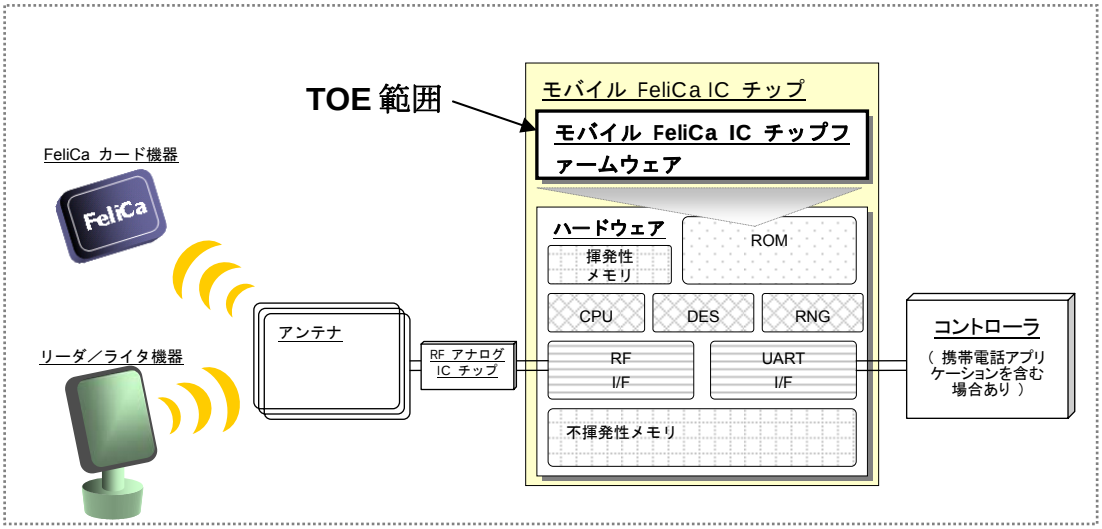

図 2-4 物理構成図

2.8. ソフトウェア構成

本節では、TOE のソフトウェア構成ならびに TOE の機能について記載する。

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。本構成を「図 2-5 ファームウェア論理構成図」に示す。

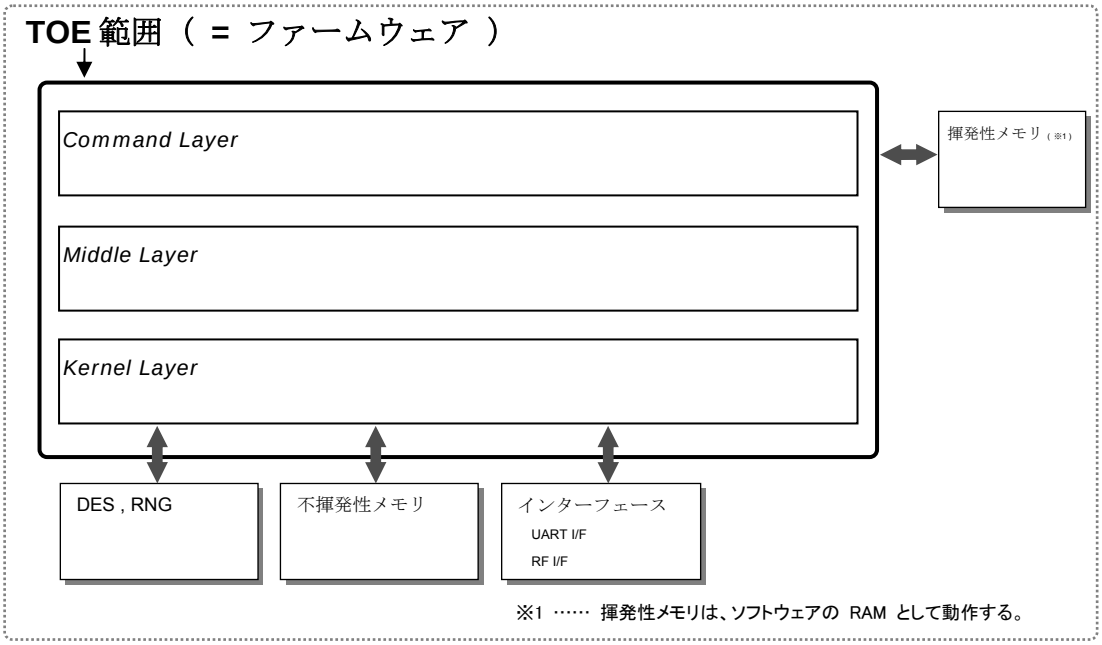

図 2-5 ファームウェア論理構成図

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。命令情報は、コマンド形式で提供されておりデータ格納領域への読み込み・書き込み、認証機能などが用意されている。本コマンドのいくつかで、セキュリティ機能が実現される。

各 Layer の基本的動作を以下に示す。

① Kernel Layer にて UART I/F もしくは RF I/F からの命令情報を受信する
② Middle Layer にて受信した命令情報を解析・実行可否を判断する
③ Command Layer にて命令情報に対応した機能を実行する
④ Command Layer で不揮発性メモリデータを利用する場合は、Middle Layer ならびに Kernel Layer を介してアクセスする
⑤ Command Layer の命令情報処理結果を、Middle Layer ならびに Kernel Layer を介して UART I/F もしくは RF I/F へ返信する

なお、TOE は UART I/F もしくは RF I/F からの命令情報受信により動作する受動型ソフトウェアである。また、同時に複数の命令は処理しないシングルスレッドソフトウェアである。

各 Layer に用意される主な機能を「表 2-3 TOE の機能構成要素」に示す。ここで、SF.xxxx はセキュリティ機能を表し、F.xxxx は一般機能を表す。

表 2-3 TOE の機能構成要素

構成要素	要素説明 / 構成機能	
Command Layer	命令情報を解析・処理する	
	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。
	TOE 状態取得機能 (F.ToeInformation)	TOE の構成情報/状態に関する情報を取得する。
	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。 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。
	リーダ／ライタ認証・通信機能 (F.RWfunction)	リーダ／ライタとして外部 FeliCa カード機器との認証/通信を行う。 TOE のアクセス暗号鍵を利用して、外部 FeliCa カード機器との認証を実施し、コントローラと外部 FeliCa カード機器の通信を実現する。
	プライバシー機能 (F.Privacy)	属性*エリア*・属性*サービス*を隠蔽する。
	欠陥修正プログラムインストール機能 (F.InstallRemediationProgram)	TOE の機能を修正するプログラムをインストールする機能 インストール保護は、SF.TSFDataProtection で実施され、本機能は TOE 内部でのプログラム結合を行う。
	診断機能 (SF.SelfDiagnosis)	TOE の診断を行う。 TOE の診断の実施機能を提供する。
Middle Layer	状態管理、アーキテクチャ制御、不揮発性メモリデータ管理を行う	
	命令解析機能 (F.CommandManagement)	命令解析ならびに管理を行う。 命令情報を「通信保護機能」「アクセスコントロール機能」「TSF データ保護機能」を用いて解析し、命令情報規定の Command Layer の機能へ処理を依頼する。また処理結果を「通信制御機能」へ返却する。
	通信路保護機能	TOE もしくはモバイル FeliCa IC チップが提供する暗号機

	(SF.CommunicateProtection)	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。
	データ管理機能 (F.DataManagement)	不揮発性メモリへ属性*システム・エリア・サービス*ならびにデータ格納領域の保護データを配置、取得する機能 Command Layer の各機能からの依頼により、論理データを物理データに変換し「不揮発性メモリ制御機能」によりデータを読み書きする。なお、論理データと物理データの変換時に「データ保護機能」を利用しデータが破損しないよう管理される。
	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 保護データならびにアクセス暗号鍵の書き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。
Kernel Layer	ハードウェア機能の管理を行う	
	通信制御機能 (F. HwCommunicateFunction)	モバイル FeliCa IC チップが提供する UART I/F ならびに RF I/F とのデータ送受信を操作する。 受信した命令情報の「命令解析機能」への引渡し、ならびに「命令解析機能」からの命令結果の送信を行う。
	乱数生成機能 (F.HwRngFunction)	モバイル FeliCa IC チップが提供する乱数生成演算ロジックを操作する。
	DES 演算機能 (F.HwDESFunction)	モバイル FeliCa IC チップが提供する DES 演算ロジックを操作する。
	CRC 演算機能 (F.HwCRCFunction)	モバイル FeliCa IC チップが提供する CRC 演算ロジックを操作する。
	不揮発性メモリ制御機能 (F.HwNVMFunction)	モバイル FeliCa IC チップが提供する不揮発性メモリを操作する。

2.9. ライフサイクル

TOE のセキュリティ管理はアクセス暗号鍵により実施され、IC チップの所有者が変る場合、アクセス暗号鍵を変更するという運用が行われる。
TOE の状態は、「**図 2-6 TOE 状態管理と遷移図**」に示す構成を取る。

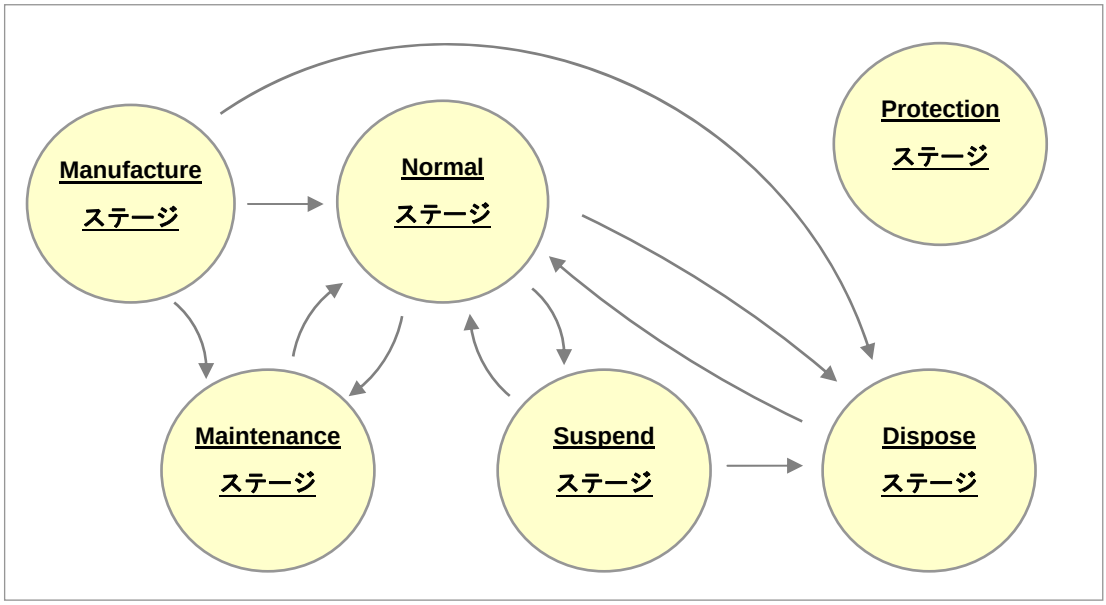

図 2-6 TOE 状態管理と遷移図

各状態は、以下の用途となる。

表 2-4 TOE 状態概要

状態	概要
Manufacture ステージ	・ モバイル FeliCa IC チップの製造状態
Normal ステージ	・ データ格納領域の操作が可能な利用状態
Maintenance ステージ	・ モバイル FeliCa IC チップのプログラム修正を行う状態
Suspend ステージ	・ モバイル FeliCa IC チップの利用停止状態
Dispose ステージ	・ モバイル FeliCa IC チップの廃棄状態
Protection ステージ	・ モバイル FeliCa IC チップの保護状態※

※ Protection ステージ は、ハードウェアの故障を TOE が検知された場合に自動的に遷移される状態です。本ステージでは、TOE に搭載される診断機能と基本情報取得機能のみが動作し、一般的な利用は制限される。

TOE の状態とライフサイクルは「**図 2-7 TOE 状態とライフサイクル**」のとおりとなる。

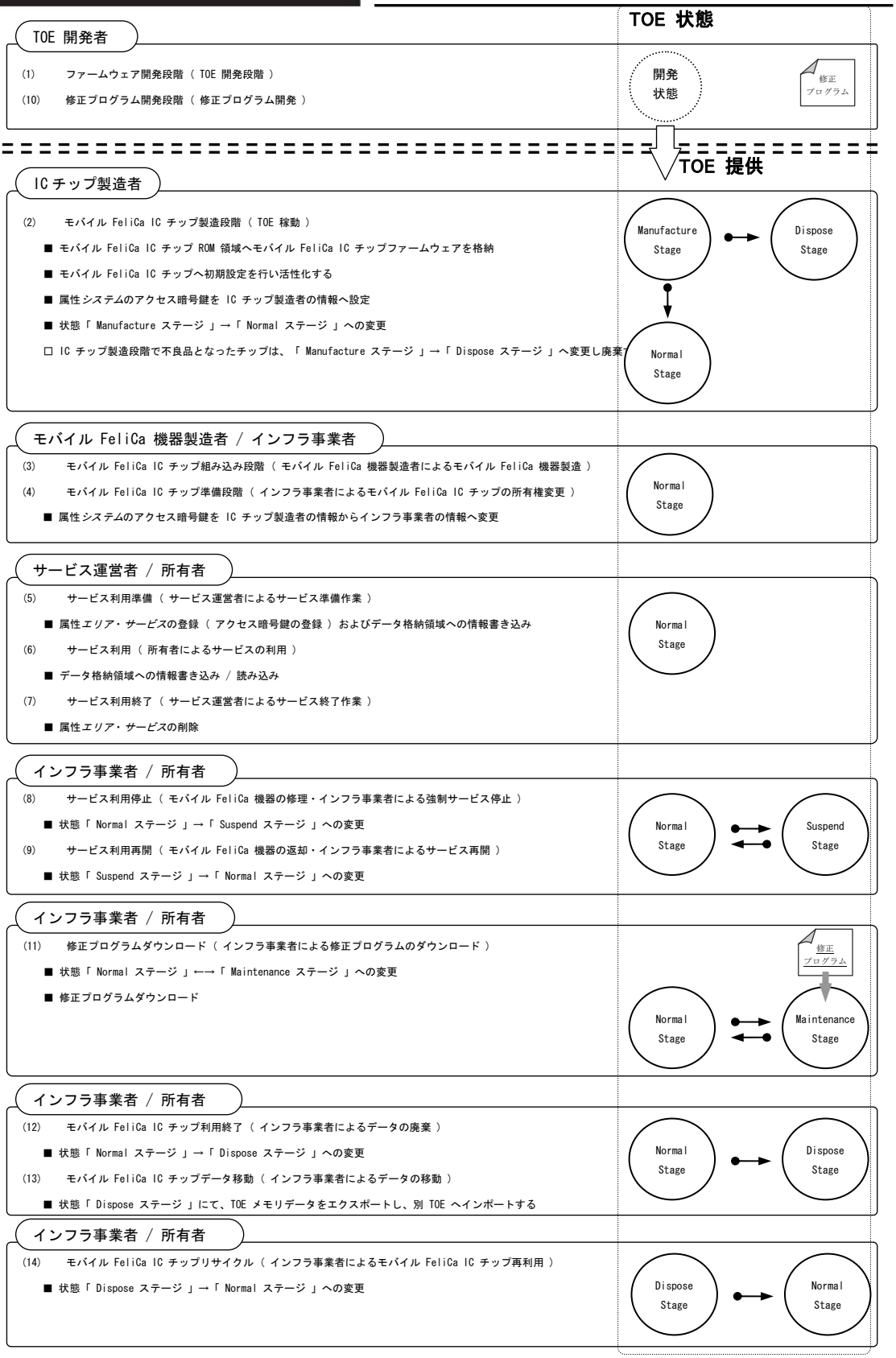

図 2-7 TOE 状態とライフサイクル

各段階は、以下の内容となる。

表 2-5 ライフサイクルにおける作業工程

作業工程	工程説明	TOE 開発者が関わる作業
(1) ファームウェア開発段階	・ TOE 開発者が TOE を開発する	TOE の配布（IC チップ製造者 ）
(2) IC チップ製造段階	・ IC チップ製造者がモバイル FeliCa IC チップへ TOE の焼付けを行いモバイル FeliCa IC チップを製造する	---
(3) IC チップ組み込み段階	・ モバイル FeliCa 機器製造者がモバイル FeliCa IC チップを機器へ組み込み、モバイル FeliCa 機器を製造する	---
(4) IC チップ準備段階	・ インフラ事業者がモバイル FeliCa IC チップの所有権を IC チップ製造者からインフラ事業者に変更する	---
(5) サービス利用準備	・ 所有者が利用したいサービスを選択し、選択されたサービス運営者により、サービスに必要な情報をモバイル FeliCa IC チップへ登録する	---
(6) サービス利用	・ 所有者がサービス運営者により提供されるサービスを利用する	---
(7) サービス利用終了	・ 所有者が利用を辞めたいサービスを選択し、選択されたサービス運営者により、サービスに必要な情報をモバイル FeliCa IC チップから削除する	---
(8) サービス利用停止	・ インフラ事業者により、モバイル FeliCa IC チップの利用を停止する ・ モバイル FeliCa 機器の故障時にモバイル FeliCa IC チップの利用を停止させ、修理に出す	---
(9) サービス利用再開	・ インフラ事業者により、モバイル FeliCa IC チップの利用を再開する ・ モバイル FeliCa 機器の修理完了後、モバイル FeliCa IC チップの利用再開を行い利用者へ返却する	---
(10) 修正プログラム開発段階	・ TOE 開発者が TOE の機能欠陥に対する修正プログラムを作成する	修正プログラムの配布（ 運営主体 ）
(11) 修正プログラムダウンロード	・ インフラ事業者により、TOE へ修正プログラムをダウンロードする	---
(12) IC チップ利用終了	・ 所有者がインフラ事業者にモバイル FeliCa 機器の利用終了を依頼し、インフラ事業者がモバイル FeliCa IC チップのデータを破棄する	---
(13) IC チップデータ移動	・ 所有者がインフラ事業者にモバイル FeliCa 機器の変更を依頼し、インフラ事業者がモバイル FeliCa IC チップのデータを移動する	---
(14) IC チップリサイクル	・ インフラ事業者がモバイル FeliCa 機器のリサイクルを行いたい際、廃棄されたモバイル FeliCa IC チップを再発行して利用可能にする	---

(2) の段階が、管理者である IC チップ製造者による TOE の設置・生成となる。(2) 以降の段階から利用者であるインフラ事業者・サービス運営者・所有者による TOE の利用が可能となる。(2) が終わった TOE は、初期状態の属性*システム*・属性*エリア*・属性*サービス*が設定され提供される。以降は、インフラ事業者ならびにサービス運営者により、属性*システム*・属性*エリア*・属性*サービス*の登録・削除が行われサービスに利用される。

一般のライフサイクルからは外れるが、ハードウェア故障により Protection ステージ へ遷移した場合には、インフラ事業者のカスタマーセンターからモバイル FeliCa 機器製造者を経由し、IC チップ製造者へ届けられハードウェア故障の原因を調査する。なお、調査した情報は、TOE 開発者へ連絡される。

2.10. TOE 評価構成

評価構成は、チップベンダが提供するモバイル FeliCa IC チップ AE56D1 を利用した「**図 2-8** TOE評価構成」の環境とする。

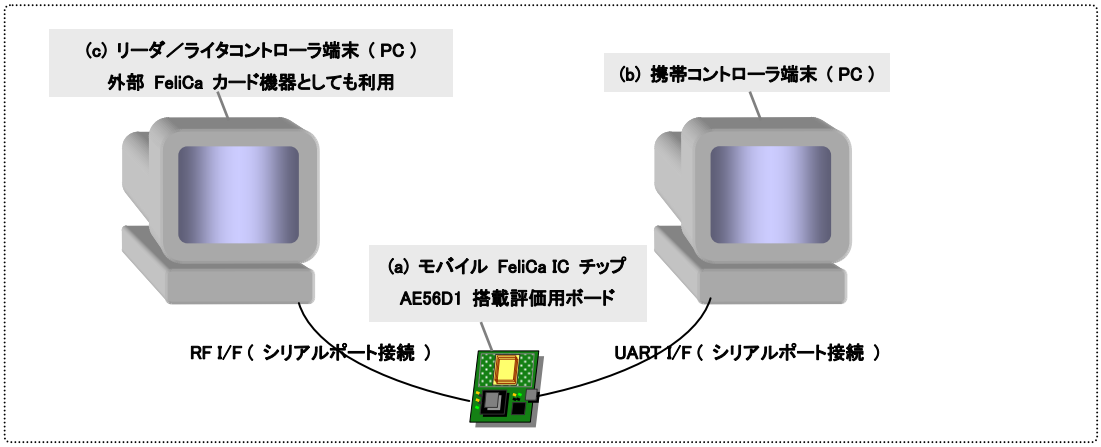

図 2-8 TOE **評価構成**

TOE は、(a) モバイル FeliCa IC チップ搭載評価用ボードに搭載される「モバイル FeliCa IC チップ AE56D1」の ROM に存在する。評価の方法は以下のとおりである。

1) (c) の PC を利用し (a) モバイル FeliCa IC チップへの RF I/F アクセス評価
2) (b) の PC から (a) モバイル FeliCa IC チップへの UART I/F アクセス評価
3) (b) の PC から (a) モバイル FeliCa IC チップをリーダ／ライタとして UART I/F から RF I/F を介して (c) へのアクセス評価
4) (c) の PC を利用し (a) モバイル FeliCa IC チップの RF I/F から UART I/F を介して (b) へのアクセス評価

各評価は、「２.３ モバイル FeliCa システム」の代表的なシステム構成の利用用途と以下対応する。

【表 2-1 利用用途例–(1)】　評価方法 3)
【表 2-1 利用用途例–(2)】　評価方法 1)
【表 2-1 利用用途例–(3)】　評価方法 2)
【表 2-1 利用用途例–(4)】　評価方法 2)
【表 2-1 利用用途例–(5)】　評価方法 3)
【表 2-1 利用用途例–(6)】　評価方法 4)

以上より、代表的なシステム構成は、本評価構成により網羅されることが判る。

第３章 TOE セキュリティ環境

本章は、TOE の資産・環境を記載し、TOE が対応する「セキュリティ関連事項」を明らかにするものである。

3.1. 保護対象資産

TOE で保護する資産を「 直接保護資産 」、TOE とコントローラ (もしくはリーダ／ライタ) 間で保護する資産を「 間接保護資産 」と区分する。

直接保護資産

保護データ

TOE で管理される属性*サービス*にセキュリティ種別で認証必須に設定されたデータ格納領域を指す。なお、属性*サービス*のセキュリティ種別で認証必須でない設定がされたデータ格納領域は本保護データ対象外である。

アクセス暗号鍵

保護データにアクセスするために必要な属性*システム・エリア・サービス*のアクセス暗号鍵を指す。リーダ／ライタ機能の認証にも利用される。アクセス暗号鍵は、保護データへアクセス、もしくは外部 FeliCa カード機器との認証を行うためのデータであり、重要度の高いデータである。

間接保護資産

通信データ

TOE とコントローラ間・もしくは TOE とリーダ／ライタ間でやり取りされる TOE への命令情報・命令に対する結果情報のうち、保護データを操作する命令情報(以下、コマンドデータと記す)と結果情報(以下、レスポンスデータと記す)。属性*システム・エリア・サービス*の登録や削除、アクセス暗号鍵を変更、修正プログラムのインストールを行うコマンドデータ/レスポンスデータがこれにあたる。

3.2. 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。

A.Reader_Writer_Hardware_Protection

セキュアリーダ／ライタを製造するモバイル FeliCa 機器製造者は、モバイル FeliCa ICチップ をリーダ／ライタに組み込む際、チップに直接アクセスできないような対策を実施する。

A.Reader_Writer_Management

セキュアリーダ／ライタを用いたサービスを運用するサービス運営者は、リーダ／ライタを容易にその場で解析できないよう、監督の行き届いたセキュアな場所に設置し、適切に管理する。さらに、リーダ／ライタが取り外された場合に検知できる対策をする。

3.3. TOE の脅威

本節では、TOE の脅威について記載する。

TOE を搭載したモバイル FeliCa 機器は、誰でも購入可能な市販製品である。しかし、TOE への操作は、サービス運営者により管理され、モバイル FeliCa 機器の所有者 (以下、所有者と記す) がサービス運営者の許可なく操作することは許されない。そのため、脅威エージェントは、モバイル FeliCa 機器を所持し、サービス運営者の許可なく TOE の操作を行う「悪意のある所有者」である。脅威は、サービスの運営者の許可なく TOE の操作が行われることで、保護データ書き換えが行われることである。保護データの書き換えは、保護データを直接書き換えることに加え、保護データへアクセスするためのアクセス暗号鍵の漏洩や書き換える手段が提供されることも含まれる。

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 がデータ書き込み処理中に 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 がデータ書き込み処理中に、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。

3.4. 組織のセキュリティ方針

なし

第４章 セキュリティ対策方針

本章では、「 第３章 TOEセキュリティ環境 」で記載した脅威・前提条件に対する対策方針、実現方法を記載する。

4.1. TOE のセキュリティ対策方針

以下に、TOE に対するセキュリティ対策方針を記載する。

O. Authentication (認証・識別)

TOE は、直接保護資産へアクセスを許可するために、コントローラもしくはリーダ／ライタ機器の認証および、アクセス対象の TOE 内の直接保護資産を識別しなければならない。

認証は、以下の条件を満たすものとする。

- 認証情報の再送による再認証を防止すること
- 認証行為の総当り攻撃に対し耐性を持つこと
- 認証は、識別された直接保護資産に設定されたアクセス暗号鍵を用いること
- エラー情報の詳細な戻り値を与えないこと

識別は、以下の条件を満たすものとする。

- アクセス対象の直接保護資産を識別する情報を用いること
- 識別と認証は同時に行うこと

また、データ移動機能を行う場合には、移動先と移動元で認証・識別を行い移動先以外へのデータ格納を防止しなければならない。

O.Access_Control (アクセスコントロール)

TOE は、データ格納領域に設定された属性 *サービス*のアクセス手段とリーダ／ライタもしくはコントローラからのアクセス手段が一致しない場合はアクセス要求を拒否しなければならない。また、O.Authentication により識別された直接保護資産以外へのアクセスおよび操作を拒否しなければならない。

属性 *サービス*のアクセス手段は、

- アクセス種別「読み込みのみ」に対する「書き込み」でのアクセス拒否

・ セキュリティ種別「認証必須」に対する「認証不要」でのアクセス拒否

を実施することである。

O.Security_Data_Protection (アクセス暗号鍵・欠陥修正プログラムの保護)

TOE は、アクセス暗号鍵の設定・変更ならびに欠陥修正プログラムをインストールのコマンドデータに対して、アクセス暗号鍵・欠陥修正プログラムの盗聴・改ざん・偽造を防止しなければならない。

O.Data_Protection (データ保護)

TOE は、直接保護資産へのアクセス中での電源途絶に対して、直接保護資産のデータが破壊されないよう保護しなければならない。

O.Data_Error_Detection (データ誤り検出)

TOE は、直接保護資産を利用する際、直接保護資産のデータが破壊・改ざんが行われていないか検出できなければならない。

O.Communicate_Error_Detection (通信データ誤り検出)

TOE は、コマンドデータが改ざんされた場合に、改ざんを検出できなければならない。また、コマンドデータの再送が行われた際、再送を検出できなければならない。

O.Communicate_Protection (通信データ保護)

TOE は、コマンドデータならびにレスポンスデータの盗聴を防止しなければならない。

O.Diagnosis (診断)

コントローラに対し、TOE の機能が正しく動作しているか診断機能を提供しなければならない。

4.2. 環境のセキュリティ対策方針

以下に、TOE 環境に対するセキュリティ対策方針を記載する。

OE.Key_Storage (アクセス暗号鍵の管理)

IC チップ製造者・インフラ事業者・サービス運営者は、TOE のアクセス暗号鍵を TOE 外で生成し TOE 内部へインポートすると共に保管・運用する。IC チップ製造者・インフラ事業者・サービス運営者は、自ら管理すべきTOEのアクセス暗号鍵を第三者へ漏洩したり、消失しないよう管理しなければならない。

OE.Security_Configuration (適切なセキュリティ設定)

サービス運営者は、提供するサービスに必要なデータおよびアクセス方法を TOE の属性*サービス*を組み合わせることで構築する。TOE の属性*サービス*の組合せは、サービス運営者が提供するサービスに応じたデータ管理のポリシーに則り、サービスで要求されるアクセス方法を設定しなければならない。データの守秘性が求められる場合は、属性*サービス*のセキュリティ種別を「認証必要」として設定しなければならない。

OE.ICvendor_Confidence (信頼のおける IC チップ製造者)

IC チップ製造者は、TOE 開発者から受領した TOE 情報をモバイル FeliCa IC チップへ搭載し、製造する工程の中で、TOE を活性化させ製品として出荷する。IC チップ製造者は、TOE 開発者から受領した TOE を改変なくモバイル FeliCa IC チップとして製造しなければならない。また、TOE 開発者から提供される活性化手順に従い、正しく活性化しなければならない。

OE.Hardware_Protection (ハードウェア保護)

IC チップ製造者は、モバイル FeliCa IC チップに対してサイドチャネル攻撃ならびに物理ストレス攻撃への対抗措置を講じ、ISO 15408 の EAL 4 以上のレベルで保証しなければならない。

OE.Hardware_DES (ハードウェアでの DES 搭載)

IC チップ製造者は、TOE が搭載されるモバイル FeliCa IC チップに OE.Hardware_Protection により保護された暗号アルゴリズム DES のコプロセッサを搭載しなければならない。

OE.Hardware_RNG (ハードウェアでの RNG 搭載)

IC チップ製造者は、TOE が搭載されるモバイル FeliCa IC チップに OE.Hardware_Protection により保護された乱数生成のコプロセッサを搭載しなければならない。

OE.Reader_Writer_Hardware_Protection (リーダ／ライタ筐体での保護)

セキュアリーダ／ライタを製造するモバイル FeliCa 機器製造者は、モバイル FeliCa ICチップ をリーダ／ライタに組み込む際、TOE開発者から提供される注意事項に従い、リーダ／ライタの外部からチップに直接アクセスすることができない対策を実施しなければならない。

OE.Reader_Writer_Management (リーダ／ライタの管理)

セキュアリーダ／ライタを用いたサービスを運用するサービス運営者は、TOE開発者から提供される注意事項に従い、リーダ／ライタを容易にその場で解析できないよう監督の行き届いたセキュアな場所に設置し、適切に管理をしなければならない。さらに、リーダ／ライタが取り外された時に検知できる仕組みを構築しなければならない。

第５章 IT セキュリティ要件

本章では、TOE ならびに TOE の環境に対するセキュリティの要件を記載する。
なお、本章で記載する利用者とは、インフラ事業者・サービス運営者などデータ格納領域および属性情報へアクセスするものを指す。

5.1. TOE セキュリティ要件

5.1.1 TOE セキュリティ機能要件

本節では、TOE のセキュリティ対策方針を達成するためのセキュリティ機能に対する要件を記載する。

5.1.1.1 クラス FCS : 暗号サポート

このクラスは、TOE 内で利用される暗号処理に関する機能を特定します。

TOE 内では、以下の機能で暗号処理が利用される。機能毎に識別するため、繰り返しを適用する。

a) 通信路の暗号処理
b) 認証機能の暗号処理
c) アクセス暗号鍵ならびに欠陥修正プログラムの暗号処理

FCS_COP.1a Cryptographic operation (暗号操作)

□ FCS_COP.1.1a

TSF は、**[** 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 **]** と暗号鍵長 **[** 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。

》暗号操作に関する規約:

表 5-1 FCS_COP.1a **暗号操作に関する規約**

割付：標準リスト	**割付：暗号アルゴリズム**	**割付：暗号鍵長**	**割付：暗号操作**
FIPS Publication 46-3 “Data Encryption Standard. 1999.” FIPS Publication 74 “Guidelines for Implementing and Using the NBS Data Encryption Standard. 1981.” FIPS Publication 81 “DES Modes of Operation. 1980.” ただし、FIPS46-3,74,81はアメリカ合衆国の旧国家暗号規格であり、現在は廃止されている	DES	56 bit	通信路データの暗号化/復号化
SP800-67 “Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Clipher” FIPS Publication 74 “Guidelines for Implementing and Using the NBS Data Encryption Standard. 1981.” FIPS Publication 81 “DES Modes of Operation. 1980.” ただし、FIPS74,81はアメリカ合衆国の旧国家暗号規格であり、現在は廃止されている	TDEA （Triple Data Encryption Algorithm）	112 bit	通信路データの暗号化/復号化

□ 下位階層: なし

□ 依存性: [FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1]，FCS_CKM.4，FMT_MSA.2

FCS_CKM.4 Cryptographic key destruction（暗号鍵破棄）

□ FCS_CKM.4.1

TSF は、以下の **[** 割付：標準のリスト **]** に合致する、指定された暗号鍵破棄方法 **[** 割付：暗号鍵破棄方法 **]** に従って、暗号鍵を破棄しなければならない。

》割付：標準のリスト

なし

》割付：暗号鍵破棄方法

暗号鍵が保管される揮発性メモリ領域の初期化

□ 下位階層: なし

□ 依存性: [FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1] , FMT_MSA.2

FCS_COP.1b Cryptographic operation (暗号操作)

□ FCS_COP.1.1b

TSF は、**[** 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 **]** と暗号鍵長 **[** 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。

》暗号操作に関する規約:

表 5-2 FCS_COP.1b **暗号操作に関する規約**

割付：標準リスト	**割付：暗号アルゴリズム**	**割付：暗号鍵長**	**割付：暗号操作**
SP800-67 “Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Clipher” FIPS Publication 74 “Guidelines for Implementing and Using the NBS Data Encryption Standard. 1981.” FIPS Publication 81 “DES Modes of Operation. 1980.” ただし、FIPS74,81はアメリカ合衆国の旧国家暗号規格であり、現在は廃止されている	TDEA (Triple Data Encryption Algorithm)	112 bit	認証用乱数の暗号処理

□ 下位階層: なし

□ 依存性: [FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1], FCS_CKM.4 , FMT_MSA.2

FCS_COP.1c Cryptographic operation (暗号操作)

□ FCS_COP.1.1c

TSF は、**[** 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 **]** と暗号鍵長 **[** 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。

》暗号操作に関する規約:

表 5-3 FCS_COP.1c **暗号操作に関する規約**

割付：標準リスト	**割付：暗号アルゴリズム**	**割付：暗号鍵長**	**割付：暗号操作**
SP800-67 “Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Clipher”	TDEA（Triple Data Encryption Algorithm）	112 bit	アクセス暗号鍵ならびに欠陥修正プログラムの暗号処理

□ 下位階層: なし

□ 依存性: [FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1]，FCS_CKM.4，FMT_MSA.2

5.1.1.2 クラス FDP： 利用者データ保護

このクラスは、利用者データ保護に関係した TOE セキュリティ機能と TOE セキュリティ機能方針に対する要件を特定する。

利用者データ保護の機能要件におけるアクセス制御 FDP_ACC.1 および FDP_ACF.1 に関して、以下の繰り返しを適用する。

a) 保護データへの読み書きに関するアクセス制御
b) 属性*システム*・属性*エリア*・属性*サービス*の操作に関するアクセス制御
c) ステージ遷移のアクセス制御

FDP_ACC.1a Subset access control (サブセットアクセス制御)

□ FDP_ACC.1.1a

TSF は、**[** 割付:サブジェクト、オブジェクト、および**SFP**で扱われるサブジェクトとオブジェクト間の操作のリスト **]** に対して、**[** 割付：アクセス制御 **SFP]** を実施しなければならない。

》割付: サブジェクト

読み書き実行プロセス

》割付: オブジェクト

データ格納領域

》割付: サブジェクトとオブジェクトの操作のリスト

読み込み，書き込み

》割付: アクセス制御 SFP

属性*サービス*アクセス制御方針

□ 下位階層: なし

□ 依存性: FDP_ACF.1

FDP_ACC.1b Subset access control (サブセットアクセス制御)

□ FDP_ACC.1.1b

TSF は、**[** 割付:サブジェクト、オブジェクト、および**SFP**で扱われるサブジェクトとオブジェクト間の操作のリスト **]** に対して、**[** 割付：アクセス制御 **SFP]** を実施しなければならない。

》割付: サブジェクト

属性操作実行プロセス

》割付: オブジェクト

属性 *システム*，属性 *エリア*，属性 *サービス*

》割付: サブジェクトとオブジェクトの操作のリスト

属性 *システム*・属性 *エリア*・属性 *サービス*の登録，属性 *システム*・属性 *エリア*・属性 *サービス*の削除，属性 *システム*・属性 *エリア*・属性 *サービス*のアクセス暗号鍵変更

》割付: アクセス制御 SFP

属性管理操作制御方針

□ 下位階層: なし

□ 依存性: FDP_ACF.1

FDP_ACC.1c Subset access control (サブセットアクセス制御)

□ FDP_ACC.1.1c

TSF は、**[** 割付:サブジェクト、オブジェクト、および**SFP**で扱われるサブジェクトとオブジェクト間の操作のリスト **]** に対して、**[** 割付 : アクセス制御 **SFP]** を実施しなければならない。

》割付: サブジェクト

ステージ遷移実行プロセス

》割付: オブジェクト

ステージ 状態

》割付: サブジェクトとオブジェクトの操作のリスト

ステージ 遷移

》割付: アクセス制御 SFP

ステージ 遷移アクセス制御方針

□ 下位階層: なし

□ 依存性: FDP_ACF.1

FDP_ACF.1a Security attribute based access control (セキュリティ属性によるアクセス制御)

□ FDP_ACF.1.1a

TSF は、以下の**[** 割付 : 示された**SFP**下において制御されるサブジェクトとオブジェクトのリスト、および各々に対応する、**SFP**関連セキュリティ属性、または**SFP**関連セキュリティ属性の名前付けされたグループ **]** に基づいて、オブジェクトに対して、 **[** 割付 : アクセス制御 **SFP]** を実施しなければならない。

》割付 : 示された**SFP**下において制御されるサブジェクトとオブジェクトのリスト、および各々に対応する、**SFP**関連セキュリティ属性、または**SFP**関連セキュリティ属性の名前付けされたグループ

サブジェクト

ステージ，識別IDにより識別した属性情報との認証

オブジェクト

アクセス種別属性，PIN 属性，プライバシー属性

》割付：アクセス制御 SFP

属性 *サービス*アクセス制御方針

□ FDP_ACF.1.2a

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決定するために、次の規則を実施しなければならない： **[** 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 **]**

》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：

「**表 5-4 属性サービスアクセス制御方針**」に示す規則

□ FDP_ACF.1.3a

TSF は、以下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承認しなければならない：**[** 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承認する規則 **]**

》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承認する規則

なし

□ FDP_ACF.1.4a

TSF は、**[** 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。

》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

なし

□ 下位階層: なし

□ 依存性: FDP_ACC.1 , FMT_MSA.3

表 5-4 属性サービスアクセス制御方針

		オブジェクト					
		データ格納領域					
	セキュリティ属性	アクセス種別属性		PIN 属性		プライバシー属性	
		読み込み	読み書き	あり	なし	あり	なし
サブジェクト	Normal ステージ における認証実施前のプロセス	---	---	---	---	---	---
	Normal ステージ における認証実施済※1のプロセス	読み込み	読み込み 書き込み	---	読み込み 書き込み	---	読み込み 書き込み
	Normal ステージ 以外の ステージ におけるプロセス	---	---	---	---	---	---

※ --- は、許された操作がないことを表す

※1 認証実施済の状態とは、アクセス対象のデータ格納領域に設定されている属性*サービス*のアクセス暗号鍵を利用した認証が実施されていることを示す。

表の読み方 ：Normal ステージ における認証実施済みのプロセスは、属性*サービス*のパラメータ「読み込み・PIN属性なし・プライバシーなし」に対して「読込」のみが実施可能である。属性*サービス*のパラメータは、表中の操作を論理積した操作のみが許可される。

FDP_ACF.1b Security attribute based access control (セキュリティ属性によるアクセス制御)

□ FDP_ACF.1.1b

TSF は、以下の**[** 割付：示された**SFP**下において制御されるサブジェクトとオブジェクトのリスト、および各々に対応する、**SFP**関連セキュリティ属性、または**SFP**関連セキュリティ属性の名前付けされたグループ **]** に基づいて、オブジェクトに対して、 **[** 割付：アクセス制御 **SFP]** を実施しなければならない。

》割付：示された**SFP**下において制御されるサブジェクトとオブジェクトのリスト、および各々に対応する、**SFP**関連セキュリティ属性、または**SFP**関連セキュリティ属性の名前付けされたグループ

サブジェクト:

ステージ，識別IDにより識別した属性情報との認証

オブジェクト：

属性情報を識別する識別ID

》割付：アクセス制御 **SFP**

属性管理操作制御方針

□ FDP_ACF.1.2b

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決定するために、次の規則を実施しなければならない： **[** 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 **]**

》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：

表 5-5 属性管理操作制御方針 に示す規則

□ FDP_ACF.1.3b

TSF は、以下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承認しなければならない：**[** 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承認する規則 **]**

》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承認する規則

なし

□ FDP_ACF.1.4b

TSF は、**[** 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。

》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

なし

□ 下位階層: なし

□ 依存性: FDP_ACC.1 , FMT_MSA.3

表 5-5 属性管理操作制御方針

		オブジェクト					
		属性*システム*		属性*エリア*		属性*サービス*	
	セキュリティ属性	新規属性*システム*	登録済みの属性*システム*	新規属性*エリア*	登録済みの属性*エリア*	新規属性*サービス*	登録済みの属性*サービス*
サブジェクト	Normal ステージの属性システム操作権限を有するプロセス※1	登録	削除※4 アクセス暗号鍵変更	---	---	---	---
	Normal ステージの属性エリア・サービス操作権限を有するプロセス※2	---	---	登録	削除※3 アクセス暗号鍵変更	登録	削除※3 アクセス暗号鍵変更
	Normal Stage 以外の ステージ のプロセス	---	---	---	---	---	---
	Normal Stage の操作権限を有しないプロセス	---	---	---	---	---	---

※ --- は、許された操作がないことを表す

※1 「属性システム操作権限を有する」とは、操作を行うために必要な属性*サービス*もしくは属性*システム*と認証を行っていることを指す。

※2 「属性エリア・サービス操作権限を有する」とは、登録では登録する属性情報の上位属性*エリア*との認証が行われていることを指し、アクセス暗号鍵変更では、アクセス暗号鍵変更を行う属性情報との認証を行っていることを指す。削除では、対象属性のアクセス暗号鍵を利用した削除命令を用いていることを指す。

※3 「削除」とは、対象の属性*システム*・属性*エリア*・属性*サービス*の削除だけでなく管理する属性*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削除を含む。

※4 属性*システム*の削除は登録されているすべての属性*システム*を削除することを指す。

表の読み方の例：サブジェクト Normal ステージ の属性*システム*と認証した権限情報を有するプロセスは、オブジェクトの新規属性*システム*を「登録」することが可能である。

FDP_ACF.1c Security attribute based access control (セキュリティ属性によるアクセス制御)

□ FDP_ACF.1.1c

TSF は、以下の**[** 割付：示された**SFP**下において制御されるサブジェクトとオブジェクトのリスト、および各々に対応する、**SFP**関連セキュリティ属性、または**SFP**関連セキュリティ属性の名前付けされたグループ **]** に基づいて、オブジェクトに対して、 **[** 割付：アクセス制御 **SFP]** を実施しなければならない。

》割付：示された**SFP**下において制御されるサブジェクトとオブジェクトのリスト、および各々に対応する、**SFP**関連セキュリティ属性、または**SFP**関連セキュリティ属性の名前付けされたグループ

サブジェクト：

遷移要求先ステージ情報

オブジェクト：

ステージ

》割付：アクセス制御 **SFP**

ステージ 遷移アクセス制御方針

□ FDP_ACF.1.2c

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決定するために、次の規則を実施しなければならない： **[** 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 **]**

》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：

「**表 5-6 ステージ遷移アクセス制御方針**」に示す規則

□ FDP_ACF.1.3c

TSF は、以下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承認しなければならない：**[** 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承認する規則 **]**

》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承認する規則

なし

□ FDP_ACF.1.4c

TSF は、**[** 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。

》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

なし

□ 下位階層: なし

□ 依存性: FDP_ACC.1 , FMT_MSA.3

表 5-6 ステージ遷移アクセス制御方針

			オブジェクト					
			ステージ					
			Manufacture ステージ	Normal ステージ	Suspend ステージ	Maintenance ステージ	Protection ステージ	Dispose ステージ
サブジェクト	ステージ遷移の実行権限を有するプロセス	プロセス※1が保持する遷移要求先ステージ情報が「Manufacture ステージ」の場合	×	×	×	×	×	×
		プロセス※1が保持する遷移要求先ステージ情報が「Normal ステージ」の場合	○	×	○	○	×	○
		プロセス※1が保持する遷移要求先ステージ情報が「Suspend ステージ」の場合	×	○	×	×	×	×
		プロセス※1が保持する遷移要求先ステージ情報が「Maintenance ステージ」の場合	○	○	×	×	×	×
		プロセス※1が保持する遷移要求先ステージ情報が「Protection ステージ」の場合	×	×	×	×	×	×
		プロセス※1が保持する遷移要求先ステージ情報が「Dispose ステージ」の場合	○	○	○	×	×	×

※1 「プロセス」とはステージ遷移実行プロセスを指し、遷移を行うために必要なアクセス暗号鍵を用いたステージ遷移命令で構成されるとする

※ ×はステージ遷移が許可されないことを示し、○はステージ遷移が許可されることを示す。

表の読み方 : ステージ状態がManufacture ステージ である場合、ステージ遷移実行権限を有するプロセスに対し、Normal ステージ , Maintenance ステージ または Dispose ステージ へのステージ遷移が許可される。

利用者データ保護の機能要件における情報フロー制御 FDP_IFC.1 および FDP_IFF.1 に関して、以下の繰り返しを適用する。

a) 保護データへの読み書き、および属性操作に関する情報フロー制御

b) アクセス暗号鍵の取り扱い時の情報フロー制御

FDP_IFC.1a Subset information flow control (サブセット情報フロー制御)

□ FDP_IFC.1.1a

TSF は、**[** 割付 : サブジェクト、情報、および、**SFP** によって扱われる制御されたサブジェクト、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト **]** に対して **[** 割付 : 情報フロー制御 **SFP]** を実施しなければならない。

》割付 : サブジェクト、情報、および、**SFP** によって扱われる制御されたサブジェクト、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト:

表 5-7 FDP_IFC.1a SFP **で扱われる操作のリスト**

サブジェクト	情報	操作
認証済み※1受信プロセス	コマンドデータの構成情報	・ データ格納領域への読み書き ・ 属性*システム*・属性*エリア*・属性*サービス*の登録・削除・アクセス暗号鍵変更
認証済み※1送信プロセス	レスポンスデータの構成情報	

※1 「認証済み」とは、属性*システム*・属性*エリア*・属性*サービス*のアクセス暗号鍵を用いて外部機器であるコントローラないしリーダ／ライタとの認証が成功したことを示す。

》割付：情報フロー制御 SFP

FeliCa 通信制御方針

□ 下位階層: なし

□ 依存性: FDP_IFF.1

FDP_IFF.1a Simple security attribute (単純セキュリティ属性)

□ FDP_IFF.1.1a

TSF は、以下のサブジェクトおよび情報のセキュリティ属性の種別に基づいて、**[割付：情報フロー制御 SFP]** を実施しなければならない。: **[割付：示された SFP 下において制御されるサブジェクトと情報のリスト、および各々のセキュリティ属性]**

》割付: 情報フロー制御 SFP

FeliCa 通信制御方針

》割付: 制御されるサブジェクト

認証された受信プロセス

認証された送信プロセス

》割付: 情報のリスト

コマンドデータ

レスポンスデータ

》割付: セキュリティ属性

コマンドデータおよびレスポンスデータのセッション鍵、誤り検出情報、セッション番号

□ FDP_IFF.1.2a

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。: **[割付：各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばらならない、セキュリティ属性に基づく関係]**

》割付：各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばらならない、セキュリティ属性に基づく関係

表 5-8 FeliCa 通信制御方針（コマンドデータ制御）, **表 5-9 FeliCa 通信制御方針（レスポンスデータ制御）**に記載される規則

□ FDP_IFF.1.3a

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。

》割付：追加の情報フロー制御 **SFP** 規則

なし

□ FDP_IFF.1.4a

TSF は、以下の **[** 割付：追加の **SFP** 能力のリスト **]** を提供しなければならない。

》割付：追加の **SFP** 能力のリスト

なし

□ FDP_IFF.1.5a

TSF は、以下の規則に基づいて、情報フローを明示的に承認しなければならない。：

[割付：セキュリティ属性に基づいて、明示的に情報フローを承認する規則 **]**

》割付：セキュリティ属性に基づいて、明示的に情報フローを承認する規則

なし

□ FDP_IFF.1.6a

TSF は、次の規則に基づいて、情報フローを明示的に拒否しなければならない。：

[割付：セキュリティ属性に基づいて、明示的に情報フローを拒否する規則 **]**

》割付：セキュリティ属性に基づいて、明示的に情報フローを拒否する規則

なし

□ 下位階層: なし

□ 依存性: FDP_IFC.1 , FMT_MSA.3

表 5-8 FeliCa **通信制御方針（ コマンドデータ制御 ）**

		情報					
		コマンドデータ構成情報					
		コマンドデータの セッション鍵による復号		コマンドデータの 誤り検出結果		コマンドデータの セッション番号	
サブジェクト	セキュリティ属性	成功	失敗	誤りなし	誤りあり	保持情報 より大きい	保持情報 以下
	認証された 受信プロセス	操作 許可	操作 不許可	操作 許可	操作 不許可	操作 許可	操作 不許可

表 5-9 FeliCa **通信制御方針（ レスポンスデータ制御 ）**

		情報					
		レスポンスデータ構成情報					
		レスポンスデータの セッション鍵による暗号		レスポンスデータの 誤り検出情報設定		レスポンスデータの セッション番号設定	
サブジェクト	セキュリティ属性	成功	失敗	成功	失敗	成功	失敗
	認証された 送信プロセス	操作 許可	操作 不許可	操作 許可	操作 不許可	操作 許可	操作 不許可

表の読み方の例（表5-7の場合）　認証された受信プロセスは、コマンドデータのセッション鍵による復号に成功し、コマンドデータの誤り検出がなく、コマンドデータのセッション番号が保持情報より多きい場合にかぎり、 FDP_IFC.1.1a で示される操作を行うことを許す

FDP_IFC.1b　Subset information flow control (サブセット情報フロー制御)

□ FDP_IFC.1.1b

TSF は、**[** 割付 ： サブジェクト、情報、および、**SFP** によって扱われる制御されたサブジェクト、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト **]** に対して **[** 割付：情報フロー制御 **SFP]** を実施しなければならない。

》割付 ： サブジェクト、情報、および、**SFP** によって扱われる制御されたサブジェクト、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト:

表 5-10 FDP_IFC.1b SFP **で扱われる操作のリスト**

サブジェクト	情報	操作
Maintenance ステージ 受信プロセス	コマンドデータの構成情報	・ 欠陥修正プログラムインポート
Dispose ステージ 受信プロセス	コマンドデータの構造情報	・ 属性システム・属性エリア・属性サービス・データ格納領域のインポート・エクスポート ・ チップの再利用
Dispose ステージ 送信プロセス	レスポンスデータの構成情報	
Normal ステージ 受信プロセス	コマンドデータの構成情報	・ 属性システム・属性エリア・属性サービスの登録・削除・アクセス暗号鍵変更
Manufacture ステージ 受信プロセス	コマンドデータの構成情報	・ 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変更

》割付：情報フロー制御 SFP

FeliCa パッケージ化制御方針

□ 下位階層: なし

□ 依存性: FDP_IFF.1

FDP_IFF.1b Simple security attribute (単純セキュリティ属性)

□ FDP_IFF.1.1b

TSF は、以下のサブジェクトおよび情報のセキュリティ属性の種別に基づいて、**[** 割付：情報フロー制御 **SFP]** を実施しなければならない。: **[** 割付：示された **SFP** 下において制御されるサブジェクトと情報のリスト、および各々のセキュリティ属性 **]**

》割付: 情報フロー制御 SFP

FeliCa パッケージ化制御方針

》割付: 制御されるサブジェクト

Manufacture ステージ の受信プロセス

Maintenance ステージ の受信プロセス

Dispose ステージ の受信プロセス

Dispose ステージ の送信プロセス

Normal ステージ の受信プロセス

》割付: 情報のリスト

コマンドデータ

レスポンスデータ

》割付: セキュリティ属性

属性情報のアクセス暗号鍵

パリティ情報

コマンドデータおよびレスポンスデータのセッション鍵

□ FDP_IFF.1.2b

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。: **[** 割付：各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばらない、セキュリティ属性に基づく関係 **]**

》割付：各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばらない、セキュリティ属性に基づく関係

表 5-11 FeliCa パッケージ化制御方針 に記載される規則

□ FDP_IFF.1.3b

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。

》割付：追加の情報フロー制御 **SFP** 規則

なし

□ FDP_IFF.1.4b

TSF は、以下の **[** 割付：追加の **SFP** 能力のリスト **]** を提供しなければならない。

》割付：追加の **SFP** 能力のリスト

なし

□ FDP_IFF.1.5b

TSF は、以下の規則に基づいて、情報フローを明示的に承認しなければならない。:

[割付：セキュリティ属性に基づいて、明示的に情報フローを承認する規則 **]**

》割付：セキュリティ属性に基づいて、明示的に情報フローを承認する規則

なし

□ FDP_IFF.1.6b

TSF は、次の規則に基づいて、情報フローを明示的に拒否しなければならない。 :

[割付：セキュリティ属性に基づいて、明示的に情報フローを拒否する規則 **]**

》割付：セキュリティ属性に基づいて、明示的に情報フローを拒否する規則

なし

□ 下位階層: なし

□ 依存性: FDP_IFC.1 , FMT_MSA.3

表 5-11 FeliCa **パッケージ化制御方針**

		情報			
		コマンドデータ構成情報		レスポンスデータ構成情報	
	セキュリティ属性	アクセス暗号鍵もしくはセッション鍵による復号とパリティ情報検証		セッション鍵による暗号	
		成功	失敗	成功	失敗
サブジェクト	Manufacture ステージ / Maintenance ステージ / Dispose ステージ / Normal ステージ の受信プロセス	操作許可	操作不許可	---	---
	Dispose ステージ の送信プロセス	---	---	操作許可	操作不許可

表の読み方　　Nomral ステージ の受信プロセスは、アクセス暗号鍵によるコマンドデータ構造の復号に成功した場合に、 FDP_IFC.1.1b で示される操作を行うことを許す

FDP_ETC.1 Export of user data without security attributes (セキュリティ属性なし利用者データのエクスポート)

□ FDP_ETC.1.1

TSF は、SFP(s) 制御下にある{利用者データ}を TSC の外部にエクスポートするとき、**[割付：アクセス制御 SFP(s) および/または情報フロー制御 SFP(s)]** を実施しなければならない。

》利用者データ

データ格納領域に格納されたデータブロック

》割付：アクセス制御 SFP(s) および/または情報フロー制御 SFP(s)

属性サービスアクセス制御方針

□ FDP_ETC.1.2

TSF は、{利用者データ}に関係したセキュリティ属性なしで{利用者データ}をエクスポートしなければならない。

》利用者データ

データ格納領域に格納されたデータブロック

□ 下位階層: なし

□ 依存性: [FDP_ACC.1 あるいは FDP_IFC.1]

利用者データ保護の機能要件におけるインポート制御 FDP_ITC.1 に関して、以下の繰り返しを適用する。

a) 保護データへの書き込みに関するインポート制御

b) 属性 *システム・属性エリア・属性 サービス*のアクセス暗号鍵に関するインポート制御

FDP_ITC.1a Import of user data without security attribute (セキュリティ属性なし利用者データのインポート)

□ FDP_ITC.1.1a

TSF は、SFPに従って制御され、TSC外から{利用者データ}をインポートするときは、**[割付：アクセス制御 SFP(s) および/または情報フロー制御 SFP(s)]** を実施しなければならない。

》利用者データ

データ格納領域に格納されたデータブロック

》割付：アクセス制御 SFP(s) および/または情報フロー制御 SFP(s)

属性サービスアクセス制御方針

□ FDP_ITC.1.2a

TSF は、TSC 外からインポートされるとき、{利用者データ}に関連付けられたいかなるセキュリティ属性も無視しなければならない。

》利用者データ

データ格納領域に格納されたデータブロック

□ FDP_ITC.1.3a

TSF は、SFPに従って制御され、TSC 外から{利用者データ}をインポートするときは、以下の規則を実施しなければならない：**[割付：追加のインポート制御規則]**

》利用者データ

データ格納領域に格納されたデータブロック

》割付：追加のインポート制御規則

なし

□ 下位階層: なし

□ 依存性: [FDP_ACC.1 または FDP_IFC.1] , FMT_MSA.3

FDP_ITC.1b Import of user data without security attribute (セキュリティ属性なし利用者データのインポート)

□ FDP_ITC.1.1b

TSF は、SFPに従って制御され、TSC外から{利用者データ}をインポートするときは、**[割付：アクセス制御 SFP(s) および/または情報フロー制御 SFP(s)]** を実施しなければならない。

》利用者データ

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

》割付：アクセス制御 SFP(s) および/または情報フロー制御 SFP(s)

属性管理操作制御方針

□ FDP_ITC.1.2b

TSF は、TSC 外からインポートされるとき、{利用者データ}に関連付けられたいかなるセキュリティ属性も無視しなければならない。

》利用者データ

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

□ FDP_ITC.1.3b

TSF は、SFPに従って制御され、TSC 外から{利用者データ}をインポートするときは、以下の規則を実施しなければならない：**[割付：追加のインポート制御規則]**

》利用者データ

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

》割付：追加のインポート制御規則

なし

□ 下位階層: なし

□ 依存性: [FDP_ACC.1 または FDP_IFC.1] , FMT_MSA.3

FDP_ETC.2 Export of user data with security attributes (セキュリティ属性付き利用者データのエクスポート)

□ FDP_ETC.2.1

TSF は、SFP(s) 制御下にある{利用者データ}を TSC の外部にエクスポートするとき、**[割付：アクセス制御 SFP(s)および/または情報制御SFP(s)]** を実施しなければならない。

》利用者データ

属性 *システム*・属性 *エリア*・属性 *サービス*ならびにデータ格納領域の全情報

》**割付：アクセス制御 SFP(s)および/または情報制御SFP(s)：**

FeliCa パッケージ化制御方針

□ FDP_ETC.2.2

TSF は、{利用者データ}に関係したセキュリティ属性と共に{利用者データ}をエクスポートしなければならない。

》利用者データ

属性 *システム*・属性 *エリア*・属性 *サービス*ならびにデータ格納領域の全情報

□ FDP_ETC.2.3

TSF は、セキュリティ属性が TSC の外部にエクスポートされるとき、それがエクスポートされる{利用者データ}に曖昧さなく関係付けられていることを保証しなければならない。

》利用者データ

属性 *システム*・属性 *エリア*・属性 *サービス*ならびにデータ格納領域の全情報

□ FDP_ETC.2.4

TSF は、{利用者データ}が TSC からエクスポートされるとき、以下の規則を実施しなければならない。： **[割付：追加エクスポート制御規則]**

》利用者データ

属性 *システム*・属性 *エリア*・属性 *サービス*ならびにデータ格納領域の全情報

》割付：追加エクスポート制御規則

なし

□ 下位階層: なし

□ 依存性: [FDP_ACC.1 または FDP_IFC.1]

FDP_ITC.2　Import of user data with security attribute (セキュリティ属性付き利用者データのインポート)

□ FDP_ITC.2.1

TSF は、SFPに従って制御され、TSC外から{利用者データ}をインポートするときは、**[割付：アクセス制御 SFP(s)および/または情報制御SFP(s)]** を実施しなければならない。

》利用者データ

属性 *システム*・属性 *エリア*・属性 *サービス*ならびにデータ格納領域の全情報

》割付：アクセス制御 SFP(s)および/または情報制御SFP(s)：

FeliCa パッケージ化制御方針

□ FDP_ITC.2.2

TSF は、インポートされる{利用者データ}に関連付けられたセキュリティ属性を使用しなければならない。

》利用者データ

属性 *システム*・属性 *エリア*・属性 *サービス*ならびにデータ格納領域の全情報

□ FDP_ITC.2.3

TSF は、使用されるプロトコルが、受け取るセキュリティ属性と{利用者データ}間の曖昧さのない関連性を備えていることを保証しなければならない。

》利用者データ

属性 *システム*・属性 *エリア*・属性 *サービス*ならびにデータ格納領域の全情報

□ FDP_ITC.2.4

TSF は、インポートされる{利用者データ}のセキュリティ属性の解釈が{利用者データ}の生成元によって意図されたとおりであることを保証しなければならない。

》利用者データ

属性 *システム*・属性 *エリア*・属性 *サービス*ならびにデータ格納領域の全情報

□ FDP_ITC.2.5

TSF は、SFP に従って制御され、{利用者データ}を TSC 外からインポートするときは、以下の規則を実施しなければならない：**[** 割付：追加のインポート制御規則 **]**

》利用者データ

属性 *システム*・属性 *エリア*・属性 *サービス*ならびにデータ格納領域の全情報

》割付：追加のインポート制御規則

なし

□ 下位階層: なし

□ 依存性: [FDP_ACC.1 または FDP_IFC.1]，[FTP_ITC.1 または FTP_TRP.1]，FPT_TDC.1

FDP_RIP.1　Subset residual information protection(サブセット残存情報保護)

□ FDP_RIP.1.1

TSF は、以下のオブジェクト **<** への資源の割り当て **>** 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：**[** 割付：オブジェクトのリスト **]**

》割付：オブジェクトのリスト

データ格納領域

□ 下位階層: なし

□ 依存性: なし

FDP_SDI.2　Stored data integrity monitoring and action (蓄積データ完全性監視およびアクション)

□ 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、TSC 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。:**[** 割付：利用者データ属性 **]**

》割付：完全性誤り

データ格納領域のデータ誤り

》割付：利用者データ属性

データ格納領域に対する CRC 情報

□ 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 **]** を行わねばならない。

》割付：とられるアクション

処理を中断する

□ 下位階層: FDP_SDI.1

□ 依存性: なし

FDP_UCT.1　Basic data exchange confidentiality (基本データ交換機密)

□ FDP_UCT.1.1

TSF は、不当な暴露から保護した様態でオブジェクトの **< 送信、受信 >** を行えるようにするために、**[割付 : アクセス制御 SFP(s) および/あるいは情報フロー制御 SFP(s)]**を実施しなければならない。

》割付：アクセス制御 SFP(s) および/あるいは情報フロー制御 SFP(s)

FeliCa 通信制御方針

□ 下位階層: なし

□ 依存性: [FTP_ITC.1 または FTP_TRP.1] , [FDP_ACC.1 または FDP_IFC.1]

FDP_UIT.1　Data exchange integrity (データ交換完全性)

□ FDP_UIT.1.1

TSF は、利用者データを **< 改変、挿入 >** 誤りから保護した形で **< 送信 , 受信 >** できるようにするために、**[割付：アクセス制御 SFP(s)および/あるいは情報フロー制御 SFP(s)]** を実施しなければならない。

》割付：アクセス制御 SFP(s)および/あるいは情報フロー制御 SFP(s)

FeliCa 通信制御方針

□ FDP_UIT.1.2

TSF は、利用者データ受信において、 **< 改変、挿入 >** が生じたかどうかを判別できなければならない。

□ 下位階層: なし

□ 依存性: [FDP_ACC.1 または FDP_IFC.1] , [FTP_ITC.1 または FTP_TRP.1]

5.1.1.3　クラス FIA： 識別と認証

このクラスは､要求された利用者の識別情報を確立し検証するための機能に対する要件についてまとめる。

FIA_UAU.2　User authentication before any action (アクション前の利用者認証)

□ FIA_UAU.2.1

TSF は、その利用者を代行する他の TSF 調停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。

□ 下位階層: FIA_UAU.1

□ 依存性: FIA_UID.1

FIA_UAU.4　Single-use authentication mechanisms (単一使用認証メカニズム)

□ FIA_UAU.4.1

TSF は、**[** **割付：識別された認証メカニズム** **]** 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。

》割付：識別された認証メカニズム

FeliCa 相互認証

□ 下位階層: なし

□ 依存性: なし

FIA_UID.2 User identification before any action (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 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

□ 下位階層: FIA_UID.1

□ 依存性: なし

FIA_AFL.1 Authentication failures (認証失敗)

□ FIA_AFL.1.1

TSF は、**[** **割付:認証事象のリスト** **]** に関して、**[** **割付:正の整数値** **]** 回の不成功認証試行が生じたときを検出しなければならない。

》割付：認証事象のリスト

FeliCa 相互認証

》割付：正の整数値

1

□ FIA_AFL.1.2

不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、 **[割付:アクションのリスト]** をしなければならない。

》割付：アクションのリスト

レスポンス無応答

□ 下位階層: なし

□ 依存性: FIA_UAU.1

5.1.1.4 クラス FMT： セキュリティ管理

このクラスは、セキュリティ管理に関係した TOE セキュリティ機能と TOE セキュリティ機能方針に対する要件を特定する。

FMT_SMF.1 Specification Management Functions (管理機能の特定)

□ FMT_SMF.1.1

TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない。: **[** 割付：**TSF** によって提供されるセキュリティ管理機能のリスト **]**

》割付：**TSF** によって提供されるセキュリティ管理機能のリスト

・ ICチップ製造段階におけるアクセス暗号鍵の変更

□ 下位階層: なし

□ 依存性: なし

FMT_MTD.1 Management of TOE security data (TSF データの管理)

□ FMT_MTD.1.1

TSF は、 **[** 割付：**TSF** データのリスト **]** を **[** 割付：その他の操作 **]** する能力を **[** 割付：許可された識別された役割 **]** に制限しなければならない。

》割付：**TSF** データのリスト

Manufacture ステージの属性*システム*、属性*エリア*、*の各アクセス暗号鍵*

》割付：その他の操作

IC チップ製造段階におけるアクセス暗号鍵の変更

》割付：許可された識別された役割

モバイル FeliCa IC チップ製造者

□ 下位階層: なし

□ 依存性: FMT_SMF.1 , FMT_SMR.1

FMT_MSA.3 Static attribute initialisation (静的属性初期値)

□ FMT_MSA.3.1

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として、**[** 割付：その他の特性 **]** デフォルト値を与える **[** 割付：アクセス制御 **SFP**、情報フロー制御 **SFP]** を実施しなければならない。

》割付：その他の特性

以下のセキュリティ属性をデフォルト値とする。

PIN 設定 “入力不要”

プライバシー設定	“公開”
アクセス種別	インフラ事業者・サービス運営者により TOE 外から指定される
セキュリティ種別	インフラ事業者・サービス運営者により TOE 外から指定され、“認証必須”のみ属性サービスアクセス制御方針の対象となる
属性情報の識別 ID	インフラ事業者・サービス運営者により TOE 外から指定される

》割付：アクセス制御 SFP、情報フロー制御 SFP

属性サービスアクセス制御方針、属性管理操作制御方針

□ FMT_MSA.3.2

TSF は、オブジェクトや情報が生成されるとき、**[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指定することを許可しなければならない。

》割付：許可された識別された役割

なし

□ 下位階層: なし

□ 依存性: FMT_MSA.1 , FMT_SMR.1

FMT_SMR.1 Security management roles (セキュリティ管理役割)

□ FMT_SMR.1.1

TSF は、役割 **[割付：許可された識別された役割]** を維持しなければならない。

》割付：許可された識別された役割

モバイル FeliCa IC チップ製造者

□ 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。

□ 下位階層: なし

□ 依存性: FIA_UID.1

5.1.1.5 クラス FPT : TSF の保護

このクラスは、TSF を提供するメカニズムの完全性と管理、および TSF データの完全性に関連する機能要件について記載しています。

FPT_AMT.1　Abstract machine testing (抽象マシンテスト)

□ FPT_AMT.1.l

TSF は、TSFの下層にある抽象マシンによって提供されるセキュリティ前提条件の正しい操作を実証するために、 **<** 許可利用者の要求で **>** に、テストのスイートを走らせなければならない。

□ 下位階層: なし

□ 依存性: なし

FPT_FLS.1　Failure with preservation of secure state (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。 : **[** 割付： **TSF** における障害の種類のリスト **]**

》割付： **TSF** における障害の種類のリスト

不揮発性メモリの書き込み動作中の電源断

□ 下位階層: なし

□ 依存性: ADV_SPM.1

FPT_ITC.1Inter-TSF confidentiality during transmission (送信中の TSF 間機密性)

□ FPT_ITC.1.1

TSF は、TSF からリモート高信頼 IT 製品に送信されるすべての TSF データを、送信中の不当な暴露から保護しなければならない。

□ 下位階層: なし

□ 依存性: なし

FPT_ITI.1 Inter-TSF detection of modification (TSF 間改変の検出)

□ FPT_ITI.1.1

TSF は、以下の尺度の範囲で、 TSF とリモート高信頼 IT 製品間で送出中のすべての TSF データの改変を検出する機能を提供しなければならない。 : **[** 割付：定義された改変尺度 **]**

》割付：定義された改変尺度

アクセス暗号鍵に対するパリティ情報の一致
欠陥修正プログラムに対するパリティ情報の一致

□ FPT_ITI.1.2

TSF は、TSF とリモート高信頼 IT 製品間で送られるすべての TSF データの完全性を検証し、かつ改変が検出された場合には **[割付：取られるアクション]** を実行する能力を提供しなければならない。

》割付：取られるアクション

アクセス暗号鍵の破棄
欠陥修正プログラムの破棄

□ 下位階層: なし

□ 依存性: なし

FPT_RPL.1　Replay detection (リプレイ検出)

□ FPT_RPL.1.1

TSF は、以下のエンティティに対するリプレイを検出しなければならない。: **[割付：識別されたエンティティのリスト]**

》割付：識別されたエンティティのリスト

コマンドデータを含む通信データ

□ FPT_RPL.1.2

TSF は、リプレイが検出された場合、**[割付：特定のアクションのリスト]** をしなければならない。

》割付：特定のアクションのリスト

コマンドデータの受信処理の中断

□ 下位階層: なし

□ 依存性: なし

FPT_RVM.1　Refarence mediation (TSP の非バイパス性)

□ FPT_RVM.1.1

TSF は、 TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。

□ 下位階層: なし

□ 依存性: なし

FPT_SEP.1a TSF domain Separation (TSF ドメイン分離)

□ FPT_SEP.1.1a

TSF は、それ自身の実行のため、信頼できないサブジェクトによる干渉や改ざんか

らそれを保護するためのセキュリティドメインを維持しなければならない。

□ FPT_SEP.1.2a

TSF は、TSC 内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

□ 下位階層: なし

□ 依存性: なし

FPT_TDC.1　Inter-TSF basic TSF data consistency (TSF 間基本 TSF データ一貫性)

□ FPT_TDC.1.I

TSF は、TSF と他の高信頼 IT 製品間で共有される場合に **[割付：TSF データ種別のリスト]** を一貫して解釈する能力を提供しなければならない。

》割付：TSF データ種別のリスト

属性*システム*のアクセス暗号鍵

属性*エリア*のアクセス暗号鍵

属性*サービス*のアクセス暗号鍵

□ FPT_TDC.1.2

TSF は、他の高信頼 IT 製品からの TSF データを解釈するとき、**[割付：TSF が適用する解釈規則のリスト]** を使用しなければならない。

》割付：TSF が適用する解釈規則のリスト

論理 FeliCa データフォーマット

□ 下位階層: なし

□ 依存性: なし

FPT_TST.1　TSF testing (TSF テスト)

□ FPT_TST.1.I

TSF は、**< TSF >**の正常操作を実証するために、 **< 許可利用者の要求時に >** 自己テストのスイートを実行しなければならない。

□ FPT_TST.1.2

TSF は、許可利用者に、**< TSF データ >**の完全性を検証する能力を提供しなければならない。

□ FPT_TST.1.3

TSF は、許可利用者に、格納されている TSF 実行コードの完全性を検証する能力を提供しなければならない。

□ 下位階層: なし

□ 依存性: FPT_AMT.1

5.1.1.6 クラス FTA : TOE アクセス

本クラスは、利用者の認証セッションを制御する機能要件を特定する。

FTA_SSL.3　TSF-initiated termination (TSF 起動による終了)

□ FTA_SSL.3.1

TSFは、**[** 割付：利用者が非アクティブである時間間隔 **]** 後に対話セションを終了しなければならない。

》割付：利用者が非アクティブである時間間隔

設定された有限時間

□ 下位階層: なし

□ 依存性: なし

5.1.1.7 クラス FTP： 高信頼性パス/チャネル

本クラスは、利用者と対向機器との間で行われる通信の信頼度に関する要件を定義する。

FTP_ITC.1inter-TSF trusted channel (TSF 間高信頼チャネル)

□ FTP_ITC.1.1

TSF は、それ自身とリモート高信頼 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およ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、**<{リモート高信頼 IT 製品}>** 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。

》リモート高信頼 IT 製品

認証が完了した対向機器

□ 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。

》割付：高信頼チャネルが要求される機能のリスト

データ移動機能・読み書き機能・アクセスコントロール機能

□ 下位階層: なし

□ 依存性: なし

5.1.2 最小機能強度レベル

TOEが想定する攻撃力は中程度であり、TOSの最小機能強度レベルは、SOF-中位である。
TOEが適用する確率的または順列的メカニズムはすべて暗号アルゴリズムであり、明示的に機能強度レベルを主張すべきセキュリティ機能要件は存在しない。

5.2. セキュリティ保証要件

本章では、EAL 4 追加として選択した TOE のセキュリティ保証コンポーネントを記載する。
追加したセキュリティ保証コンポーネントは、ALC_FLR.1 ならびに AVA_VLA.3 である。

表 5-12 保証コンポーネントと依存性

項番	コンポーネント	コンポーネント名称	依存性
1	ACM_AUT.1	Partial CM automation (部分的なCM自動化)	ACM_CAP.3
2	ACM_CAP.4	Generation support and acceptance procedures (生成の支援と受入手続き)	ALC_DVS.1
3	ACM_SCP.2	Problem tracking CM coverage (問題追跡のCM範囲)	ACM_CAP.3
4	ADO_DEL.2	Detection of modification (改変の検出)	ACM_CAP.3
5	ADO_IGS.1	Installation, generation, and start-up procedures (設置、生成、および立上げ手順)	AGD_ADM.1
6	ADV_FSP.2	Fully defined external interfaces (完全に定義された外部インターフェース)	ADV_RCR.1
7	ADV_HLD.2	Security enforcing high-level design (セキュリティ実施上位レベル設計)	ADV_FSP.1 ADV_RCR.1
8	ADV_IMP.1	Subset of the implementation of the TSF (TSF の実装のサブセット)	ADV_LLD.1 ADV_RCR.1 ALC_TAT.1
9	ADV_LLD.1	Descriptive low-level design (記述的下位レベル設計)	ADV_HLD.2 ADV_RCR.1
10	ADV_RCR.1	Informal correspondence demonstration (非形式的対応の実証)	なし
11	ADV_SPM.1	Informal TOE security policy model (非形式的な TOE セキュリティ方針モデル)	ADV_FSP.1
12	AGM_ADM.1	Administrator guidance (管理者ガイダンス)	ADV_FSP.1
13	AGM_USR.1	User guidance (利用者ガイダンス)	ADV_FSP.1
14	ALC_DVS.1	Identification of security measures (セキュリティ手段の識別)	なし
15	ALC_LCD.1	Developer defined life-cycle model (開発者によるライフサイクルモデル定義)	なし
16	ALC_TAT.1	Well-defined development tools (明確に定義された開発ツール)	ADV_IMP.1
17	ALC_FLR.1	Basic flaw remediation (基本的な欠陥修正)	なし
18	ATE_COV.2	Analysis of coverage (カバレージの分析)	ADV_FSP.1 ATE_FUN.1

19	ATE_DPT.1	Testing: high-level design (テスト：上位レベル設計)	ADV_HLD.1 ATE_FUN.1
20	ATE_FUN.1	Functional testing (機能テスト)	なし
21	ATE_IND.2	Independent testing – sample (独立テスト – サンプル)	ADV_FSP.1 AGD_ADM.1 AGD_USR.1 ATE_FUN.1
22	AVA_MSU.2	Validation of analysis (分析の確認)	ADO_IGS.1 ADV_FSP.1 AGD_ADM.1 AGD_USR.1
23	AVA_SOF.1	Strength of TOE security function evaluation (TOE セキュリティ機能強度評価)	ADV_FSP.1 AFV_HLD.1
24	AVA_VLA.3	Moderately resistant (中程度の抵抗力)	ADV_FSP.1 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 AGD_ADM.1 AGD_USR.1

5.3. IT 環境に対するセキュリティ要件

IT 環境に対するセキュリティ要件について以下に示します。

5.3.1 クラス FCS : 暗号サポート

FCS_COP.1e Cryptographic operation (暗号操作)

□ FCS_COP.1.1e

{ TSF } は、**[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]** と暗号鍵長 **[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。

》 TSF

モバイル FeliCa IC チップ

》 暗号操作に関する規約:

表 5-13 FCS_COP.1e **暗号操作に関する規約**

割付 : 標準リスト	**割付 : 暗号アルゴリズム**	**割付 : 暗号鍵長**	**割付 : 暗号操作**
FIPS Publication 46-3 “Data Encryption Standard. 1999.” FIPS Publication 74 “Guidelines for Implementing and Using the NBS Data Encryption Standard. 1981.” FIPS Publication 81 “DES Modes of Operation. 1980.”	DES	56 bit	通信路データの暗号化/復号化のための暗号モジュール提供

□ 下位階層: なし

□ 依存性: [FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1], FCS_CKM.4 , FMT_MSA.2

FCS_CKM.1 Cryptographic key generation (暗号鍵生成)

□ FCS_CKM.1.1

{ TSF } は、以下の **[割付 : 標準のリスト]** に合致する、指定された暗号鍵生成アルゴリズム **[割付 : 暗号鍵生成アルゴリズム]** と指定された暗号鍵長 **[割付 : 暗号鍵長]** に従って、暗号鍵を生成しなければならない。

》 TSF

モバイル FeliCa IC チップ

》 割付 : 標準のリスト

なし

》割付：暗号鍵生成アルゴリズム

モバイル FeliCa IC チップ乱数生成アルゴリズム

》割付：暗号鍵長

56 bit / 112 bit

☐ 下位階層: なし

☐ 依存性: [FCS_CKM.2 または FCS_COP.1] . FCS_CKM.4 , FMT_MSA.2

5.3.2 クラス FPT : TSF の保護

IT 環境における TSF の保護に関する機能要件を記載します。

FPT_PHP.3　Resistance to Physical attack(物理的攻撃への抵抗)

□ FPT_PHP.3.1

{ TSF } は、TSP が侵害されないよう自動的に対応することによって、**[割付:TSF 装置/エレメントのリスト]** への **[割付:物理的な干渉のシナリオ]** に抵抗しなければならない。

》TSF

モバイル FeliCa IC チップ

》物理的攻撃への抵抗:

表 5-14 FPT_PHP.3 **物理的攻撃への抵抗**

割付 : **TSF 装置 / エレメントのリスト**	**割付 :** **物理的な干渉のシナリオ**
不揮発性メモリデータ 揮発性メモリデータ	・ IC チップ表面を露呈させたデータ解析 ・ 動作保証範囲外での異常動作
処理途中内容	・ IC チップをプローブ (深針) し、流れるデータの解析 ・ 暗号処理に関わるICチップ動作情報の解析

□ 下位階層: なし

□ 依存性: なし

FPT_SEP.1b TSF domain separate (TSF ドメイン分離)

□ FPT_SEP.1.1b

{ TSF } は、それ自身の実行のため、信頼できないサブジェクトによる干渉や改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

》TSF

モバイル FeliCa IC チップ

□ FPT_SEP.1.2b

{ TSF } は、TSC内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

》TSF

モバイル FeliCa IC チップ

□ 下位階層: なし

□ 依存性: なし

第６章 TOE 要約仕様

本章では、第５章「ITセキュリティ要件」により指定されている TOE セキュリティ機能要件を満たすための TOE のセキュリティ機能について記載します。

6.1. TOE セキュリティ機能

TOE の各機能についての情報を以下に記載する。

6.1.1 認証機能 (SF.Authentication)

認証機能とは、TOE がコントローラ・リーダ／ライタ・他 TOE に対して相互を識別・確認する機能である。ISO 9798 に規定されている 3 ウェイハンドシェーク方式から派生し、さらに改善された方式を使用する。これは、お互いが発生させた乱数をアクセスしたい対象属性*システム*・属性*エリア*・属性*サービス*のアクセス暗号鍵を用いた TDEA により暗号化/復号化することで、双方が正しいアクセス暗号鍵を有することを確認し、お互いの認証とする方式である。認証で生成された乱数は、セッション鍵と呼び認証後の通信路の暗号処理に利用される。本方式を利用することで、暗号処理による解析の困難化、乱数利用による認証情報の再使用を防止する。認証により共有されたセッション鍵は、認証対象のコントローラ・リーダ／ライタ・他 TOE 以外に知りえる情報ではなく、セッション鍵を通信路の暗号化に利用することで信頼された通信路が構築できる。
認証は、TOE がコントローラ・リーダ／ライタ・他 TOE を識別・認証する以外に、TOE に対する操作の可否制御にも利用する。データ格納領域へのアクセスには、アクセスしたい対象属性*サービス*のアクセス暗号鍵を利用して認証を行うことでアクセスを可能とし、また、ステージの切替、属性システムの登録・削除には特性の属性情報との認証を行うことで実施可能とする。
認証処理は認証に成功したときのみ結果が返却され、エラー応答から認証処理を解析されることを防止する。認証が成功した状態は、終了命令または有限時間経過による再起動にて終了し、セッション鍵の総当り攻撃による認証状態の乗っ取りを防止する。本機能を「 FeliCa 相互認証 」と呼称する。
なお、本機能の中で、利用される乱数や暗号処理は、IC チップが提供する機能を元に処理する。

満たされる機能要件：**FCS_COP.1b，FIA_UAU.2，FIA_UAU.4，FIA_UID.2，FIA_AFL.1，**

FCS_CKM.4 , FTA_SSL.3 , FTP_ITC.1 , FPT_RVM.1 , FPT_SEP.1a

利用する IT 環境の機能要件 : **FCS_CKM.1 , FCS_COP.1e**

6.1.2 通信路保護機能 (SF.CommunicateProtection)

通信路保護機能は、盗聴防止のための暗号処理と改ざん防止のための誤り検出により構成され、暗号処理は、通信データの受信処理と通信データの送信処理に分けられる。暗号処理では、SF.Authentication で生成されたセッション鍵を利用する。
以下に、FeliCa 通信制御による送信処理ならびに受信処理における暗号処理と誤り検出方法を示す。
受信処理では、

(1) セッション鍵を暗号鍵とした DES もしくは TDEA によるコマンドデータの復号処理の成否
(2) 復号処理されたコマンドデータ内のパリティ情報の検証
(3) 復号処理されたコマンドデータ内のシーケンス番号が TOE が保持するシーケンス番号より大きいことの検証

を行う。(1) ～ (3) により、盗聴と改ざんが検出可能となる。
送信処理では、

(4) レスポンスデータ内へ TOE が保持するシーケンス番号を設定
(5) レスポンスデータ内へパリティ情報の付与
(6) セッション鍵を暗号鍵とした DES もしくは TDEA によるレスポンスデータの暗号処理の成否

を行う。(4) ～ (6) により、盗聴と改ざんが防止できる。
また、受信後のコマンド処理後に TOE が保持するシーケンス番号をインクリメントすることで、コマンドの再送防止も可能となる。

満たされる機能要件 : **FCS_COP.1a , FDP_IFC.1a , FDP_IFF.1a , FDP_UIT.1 , FPT_RPL.1 , FDP_UCT.1 , FPT_RVM.1**

利用する IT 環境の機能要件 : **FCS_COP.1e**

6.1.3 読み書き機能 (SF.ReadWrite)

読み書き機能とは、コントローラもしくはリーダ／ライタから保護データの操作を行う機能である。TOE における保護データの操作は、「書き込み」と「読み込み」の 2 種類である。「読

み込み」は、保護データをレスポンスデータとして返却し、「書き込み」は、コマンドデータを保護データに書き込む。本機能の実行は、SF.Authentication および SF.AccessControl が適用される。

満たされる機能要件：**FDP_ETC.1 , FDP_ITC.1a**

6.1.4 アクセスコントロール機能 (SF.AccessControl)

アクセスコントロール機能は、「保護データへのアクセス制御」・「属性管理のアクセス制御」・「IC チップ製造者に対するアクセス制御」により構成される。

保護データへのアクセス制御は、利用者データが格納されるデータ格納領域に設定された属性*サービス*により判断される。属性*サービス*は、データ格納領域へのアクセス手段を規定しており、複数のアクセス手段を用いてデータ格納領域へアクセスしたい場合は、属性*サービス*を複数設定することで実現する。アクセス制御は、「**表 5-4 属性サービスアクセス制御方針**」に従い実施される。

属性管理のアクセス制御は、属性*システム*・属性*エリア*・属性*サービス*の操作「登録・削除・アクセス暗号鍵変更・アクセス暗号鍵暗号設定」に適用される。属性は、属性*サービス*を統括する属性*エリア*と属性*エリア*を分割管理する属性*システム*により構成される。属性*エリア*は配下の属性*エリア*・*サービス*の登録・削除を管理し、属性*エリア*は、階層構造を取る事ができる。属性*システム*は、TOE の内部に複数持つことができる。属性*サービス*が削除されデータ格納領域へ紐付けられた属性*サービス*が存在しなくなった場合には、データ格納領域も属性*サービス*と同時に削除する。属性*サービス*を登録する場合にデータ格納領域が存在しない場合には初期化し生成する。また、属性*サービス*のセキュリティ属性の初期値は、「 PIN 属性 / PIN 照合不要 」「 プライバシー属性 / 公開 」とする。属性情報の識別IDは、これらの属性情報を登録時に初期化する。これらのアクセス制御は、「表 5-5 属性管理操作制御方針」に従い実施される。

ステージ 遷移のアクセス制御は、TOE の ステージ 遷移に適用される。ステージ 遷移は、ステージ遷移に必要なアクセス暗号鍵を用いたステージ遷移命令により実施され、許されたステージ間の遷移のみ許可される。これらのアクセス制御は、「**表 5-6 ステージ遷移アクセス制御方針**」に従い実施される。

IC チップ製造者に対するアクセス制御は、TOE 生成段階における IC チップ製造者の操作に適用される。本操作は、Manufacture ステージ における登録済みの属性に対するアクセス暗号

鍵の変更操作を指し、セキュリティ管理機能として実現している。

満たされる機能要件 : **FDP_ACC.1a , FDP_ACF.1a , FDP_ACC.1b , FDP_ACF.1b , FDP_ACC.1c , FDP_ACF.1c , FDP_ETC.1 , FDP_ITC.1a , FDP_ITC.1b , FDP_RIP.1 , FMT_SMF.1 , FMT_MTD.1 , FMT_MSA.3 , FMT_SMR.1 , FPT_RVM.1 , FPT_SEP.1a**

6.1.5 セキュリティ情報保護機能 (SF.TSFDataProtection)

セキュリティ情報保護機能とは、SF.AccessControl で TOE とコントローラ間で送受信するアクセス暗号鍵および、SF.DataMove による TOE とコントローラ間で送受信するアクセス暗号鍵・データ格納領域、TOE とコントローラ間で送受信される欠陥修正プログラムに対して、TDEA による暗号処理を行うことで盗聴・改ざんを防止する機能である。本機能による暗号処理は FeliCa パッケージ化と呼ばれ、保護対象の情報に対してアクセス暗号鍵もしくはセッション鍵による暗号処理を行うことで実現される。FeliCa パッケージ化には、パリティ情報が付与されることで改ざん検知が可能となる。

満たされる機能要件 : **FCS_COP.1c , FDP_IFC.1b , FDP_IFF.1b , FPT_ITC.1 , FPT_ITI.1**
利用する IT 環境の機能要件 : **FCS_COP.1e**

6.1.6 データ保護機能 (SF.DataProtection)

データ保護機能は、保護データおよびアクセス暗号鍵に対する保護と異常検知により構成される。保護は、保護データならびにアクセス暗号鍵操作時に操作対象を複数管理することで操作中に異常が発生しても保護データおよびアクセス暗号鍵が破壊されない仕組みを実現する。
異常検知は、保護データならびにアクセス暗号鍵に誤りが発生した際に CRC により検出する仕組みにより実現する。
これらの機能は、利用時の不正操作ならびにハードウェア故障を想定し、保護データおよびアクセス暗号鍵の信頼性を向上させることに繋げる。

満たされる機能要件 : **FPT_FLS.1 , FDP_SDI.2**

6.1.7 データ移動機能 (SF.DataMove)

データ移動機能とは、TOE で管理する保護データおよびアクセス暗号鍵を含む TOE で管理するデータを別 TOE へ移動する機能である。移動に際しては、移動先の特定および信頼された通信路の形成のため、SF.Authentication を実施し、かつデータを安全に移送するため SF.TSFDataProtection を適用する。また、移動するデータのコピーを防止するため、データ移動前には TOE の利用を終了させ、利用を停止させる。これらの方式により、TOE 間のデータ移動を実現する。

満たされる機能要件 : **FDP_ETC.2 , FDP_ITC.2 , FPT_TDC.1**

6.1.8 診断機能 (SF.SelfDiagnosis)

診断機能とは、TOE が正しく動作するか確認する機能である。TOE が正しく動作するかを確認する診断機能は、モバイル FeliCa IC チップ機能診断と TOE 診断の 2 種類に分類用意される。識別ならびに各診断機能で用意される機能一覧を以下に示す。

1. モバイル FeliCa IC チップ機能の診断
   (1) OE.Hardware_DES の機能確認
   (2) OE.Hardware_RNG の機能確認
   (3) 異常検出アルゴリズムの機能確認
   (4) 不揮発メモリの機能確認
2. TOE の診断
   (1) TOE 保持データの欠損確認
   (2) TOE 通信応答確認
   (3) TOE 書き込み回数確認

満たされる機能要件 : **FPT_AMT.1 , FPT_TST.1**

6.2. 保証手段

本 TOE が EAL 4 追加 の保証要件を満たすために、適用される保証要件とそれを満たすためのドキュメントを以下に記載する。

表 6-1 保証手段一覧

項番	コンポーネント	コンポーネント名称	保証手段
1	ACM_AUT.1	Partial CM automation (部分的な CM自動化)	構成管理自動化文書
2	ACM_CAP.4	Generation support and acceptance procedures (生成の支援と受入手続き)	構成管理能力文書
3	ACM_SCP.2	Problem tracking CM coverage (問題追跡のCM)範囲)	構成管理範囲文書
4	ADO_DEL.2	Detection of modification (改変の検出)	配布文書
5	ADO_IGS.1	Installation, generation, and start-up procedures (設置、生成、および立上げ手順)	設定文書
6	ADV_FSP.2	Fully defined external interfaces (完全に定義された外部インターフェース)	仕様文書
7	ADV_HLD.2	Security enforcing high-level design (セキュリティ実施上位レベル設計)	機能設計書
8	ADV_IMP.1	Subset of the implementation of the TSF (TSF の実装のサブセット)	ソースコード
9	ADV_LLD.1	Descriptive low-level design (記述的下位レベル設計)	詳細設計書
10	ADV_RCR.1	Informal correspondence demonstration (非形式的対応の実証)	セキュリティ機能関連文書
11	ADV_SPM.1	Informal TOE security policy model (非形式的な TOE セキュリティ方針モデル)	セキュリティモデル文書
12	AGD_ADM.1	Administrator guidance (管理者ガイダンス)	発行用プロトコル仕様書
13	AGD_USR.1	User guidance (利用者ガイダンス)	プロトコル仕様書
14	ALC_DVS.1	Identification of security measures (セキュリティ手段の識別)	サイトセキュリティ文書
15	ALC_LCD.1	Developer defined life-cycle model (開発者によるライフサイクルモデル定義)	ライフサイクル文書
16	ALC_TAT.1	Well-defined development tools (明確に定義された開発ツール)	ツール文書
17	ALC_FLR.1	Basic flaw remediation (基本的欠陥修正)	ファームウェアアップデート文書
18	ATE_COV.2	Analysis of coverage (カバレージの分析)	テスト文書
19	ATE_DPT.1	Testing: high-level design (上位レベル設計)	テスト文書
20	ATE_FUN.1	Functional testing (機能テスト)	テスト文書
21	ATE_IND.2	Independent testing – sample (独立テスト – サンプル)	開発文書
22	AVA_MSU.2	Validation of analysis (分析の確認)	誤使用分析文書
23	AVA_SOF.1	Strength of TOE security function evaluation (TOE セキュリティ機能強度評価)	---
24	AVA_VLA.3	Moderately resistant (中程度の抵抗力)	脆弱性分析文書

"---"保証手段はないことを示す

第７章　ＰＰ主張

特に Protection Profile を主張するものはない。

7.1. PP 参照

なし

7.2. PP 修整

なし

7.3. PP 追加

なし

第８章 根拠

8.1. セキュリティ対策方針根拠

本節では、脅威に対してセキュリティ対策方針が正しく策定されているか検証し、これを満たしていることを示す。

■ 必要性の検証

脅威とセキュリティ対策方針の対応を「**表 8-1 セキュリティ対策方針と脅威/前提条件の対応表**」に示す。脅威に対して１つ以上のセキュリティ対策方針により対抗していることを表している。

表 8-1 セキュリティ対策方針と脅威/前提条件の対応表

セキュリティ対策方針	脅威									前提条件							
	T.Abuse_Command_Data	T.Reuse_Command_Data	T.Intercept_Communicate_Data	T.Intercept_Security_Data	T.Abuse_ReaderWriter_SecurityFunction	T.Interrupt_Power	T.Break_Hardware	T.Install_EvilProgram	T.Copy_TOEData	A.Key_Storage	A.Security_Configuration	A.ICvendor_Confidence	A.Hardware_Protection	A.Hardware_DES	A.Hardware_RNG	A.Reader__Writer_Hardware_Protection	A.Reader_Writer_Management
O.Authentication	○	○	-	-	○	-	-	-	○	-	-	-	-	-	-	-	-
O.Access_Control	○	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
O.Security_Data_Protection	-	-	-	○	-	-	-	○	-	-	-	-	-	-	-	-	-
O.Data_Protection	-	-	-	-	-	○	-	-	-	-	-	-	-	-	-	-	-
O.Data_Error_Detection	-	-	-	-	-	-	○	-	-	-	-	-	-	-	-	-	-
O.Communicate_Error_Detection	○	○	○	-	-	-	-	-	-	-	-	-	-	-	-	-	-
O.Communicate_Protection	○	-	○	-	-	-	-	-	-	-	-	-	-	-	-	-	-
O.Diagnosis	-	-	-	-	-	○	○	-	-	-	-	-	-	-	-	-	-
OE.Key_Storage	-	-	-	-	-	-	-	-	-	○	-	-	-	-	-	-	-
OE.Security_Configuration	-	-	-	-	-	-	-	-	-	-	○	-	-	-	-	-	-
OE.ICvendor_Confidence	-	-	-	-	-	-	-	-	-	-	-	○	-	-	-	-	-
OE.Hardware_Protection	-	-	-	-	-	-	○	-	-	-	-	-	○	-	-	-	-
OE.Hardware_DES	-	-	-	-	-	-	-	-	-	-	-	-	-	○	-	-	-
OE.Hardware_RNG	-	-	-	-	-	-	-	-	-	-	-	-	-	-	○	-	-
OE.Reader_Writer_Hardware_Protection	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	○	-
OE.Reader_Write_Management	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	○

■ 十分性の検証

脅威・前提条件に対するセキュリティ対策方針の説明を以下に記載する。

■ 前提条件

A.Key_Storage

TOE の操作は、属性*システム*・属性*エリア*・属性*サービス*のアクセス暗号鍵を利用して行われる。アクセス暗号鍵は、アクセス暗号鍵の管理者により TOE 外で生成され TOE へ設定される。そのため、TOE 外で生成されたアクセス暗号鍵の管理はアクセス暗号鍵の管理者にとって重要である。

A.Key_Storage は、**OE.Key_Storage** においてアクセス暗号鍵の管理者に TOE に格納されるアクセス暗号鍵の生成・管理を物理環境や運用対策による保護を規定することで実現できる。

A.Security_Configuration

TOE は、セキュリティ機能以外に一般機能も有している。サービス運営者が TOE を利用する際には、正しく属性*サービス*を設定することがサービス運営者にとって重要である。

A.Security_Configuration は、**OE.Security_Configuration** により、属性*サービス*の設定をサービスに求められるポリシーにしたがって正しく行うことをサービス運営者に対して規定することにより実現できる。

A.ICvendor_Confidence

TOE は、モバイル FeliCa IC チップに搭載されることで動作するものであり、搭載はモバイル FeliCa IC チップ製造者により実施される。

A.ICvendor_Confidence は、**OE.ICvendor_Confidence** により、TOE の配付およびモバイル FeliCa IC チップへの搭載を改変なく行うことを、モバイル FeliCa IC チップの製造者に対して規定することにより実現できる。

A.Hardware_Protection

直接保護資産の安全性・堅牢性を確保するために、TOE とともに TOE が動作する IC チップのハードウェアセキュリティもモバイル FeliCa IC チップファームウェアにとって重要である。

A.Hardware は、**OE.Hardware_Protection** によりモバイル FeliCa IC チップが物理的攻撃に対する対抗措置が取られることにより実現できる。

A.Hardware_DES

TOE が利用する暗号アルゴリズムは、モバイル FeliCa IC チップが提供する機能により構成される。

A.Hardware_DES は、**OE.Hardware_DES** によりモバイル FeliCa IC チップに暗号アルゴリズムロジックが搭載されることにより実現できる。

A.Hardware_RNG

TOE が利用する乱数は、モバイル FeliCa IC チップが提供する機能により生成される。

A.Hardware_RNG は、**OE.Hardware_RNG** によりモバイル FeliCa IC チップに乱数生成ロジックが搭載されることにより実現できる。

A.Reader_Writer_Hardware_Protection

直接保護資産の安全性・堅牢性を確保するために、TOE が搭載される モバイル FeliCa IC チップが組み込まれるリーダ／ライタ自体のセキュリティも TOE にとって重要である。

A.Reader_Writer_Hardware_Protection は、**OE.Reader_Writer_Hardware_Protection** によりモバイル FeliCa IC チップが物理的攻撃に対する対抗措置が取られることにより実現できる。

A.Reader_Writer_Management

直接保護資産の安全性・堅牢性を確保するために、TOE が搭載される モバイル FeliCa IC チップが組み込まれるリーダ／ライタのセキュアな設置環境も TOE にとって重要である。

A.Reader_Writer_Management は、**OE.Reader_Writer_Management** によりモバイル FeliCa IC チップが物理的攻撃に対する対抗措置が取られることにより実現できる。

■ 脅威

T.Abuse_Command_Data

悪意のある所有者により、TOE の 2 つのインターフェースを通じて不正なコマンドデータを用い、保護データへの許可のないアクセスやアクセス暗号鍵の変更や暴露が試みられることが考えられる。

T.Abuse_Command_Data の脅威には、認証・アクセス制御の利用ならびに通信路の保護が一般的な対抗策である。

TOE では、**O.Authentication** により保護データへのアクセスには認証を必要とし、不正なアクセス手段は **O.Access_Control** により拒否される。また、**O.Communicate_Protection** によるコマンドデータの暗号処理、および **O.Communicate_Error_Detection** による改ざん検出が適用され、不正なコマンドデータを作成できないように抑止する。

以上のセキュリティ対策方針により、**T.Abuse_Command_Data** に対抗できる。

T.Reuse_Command_Data

悪意のある所有者がコマンドデータを再送信することは、通信路が暗号化されていても容易に実現される攻撃手段である。

T.Reuse_Command_Data の脅威には、通信データに識別情報を持たせ再送されたことを検出可能とすることが効果的である。

TOE では、**O.Authentication** により認証データの再利用が行われないよう防止する。また、**O.Communicate_Error_Detection** によりコマンドデータの再利用を検出可能とする。

この 2 つのセキュリティ対策方針により、**T.Access_Reuse_Command** に対抗できる。

T.Intercept_Communicate_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取得・改ざんすることは、一般的な脅威である。

T.Intercept_Communicate_Data の脅威には、通信データへの暗号処理および通信データの検証が効果的である。

TOE では、**O.Communicate_Protection** により通信データに暗号処理を行うことで盗聴を防止し、**O.Communicate_Error_Detection** により通信データの再送ならびに誤りを検出することで、コマンドデータの改ざんを抑止する。

この 2 つのセキュリティ対策方針により、**T.Intercept_Communicate_Data** に対抗できる。

T.Intercept_Security_Data

悪意のある所有者によるアクセス暗号鍵の盗聴は、大きな脅威である。

T.Intercept_Security_Data の脅威には、アクセス暗号鍵に暗号処理を行って取り扱うことが効果的である。

TOE では、**O.Security_Data_Protection** により、アクセス暗号鍵に暗号処理を行って利用することで、盗聴を防止する。

このセキュリティ対策方針により、**T.Intercept_Security_Data** に対抗できる。

T.Abuse_ReaderWriter_SecurityFunction

悪意のある所有者がリーダ／ライタ機能の認証機能を容易に利用可能とすることは回避すべきである。

T.Abuse_ReaderWriter_Authentication の脅威には、認証・識別が効果的である。

TOE では、**O.Authentication** によりリーダ／ライタ機能の認証機能利用の際、認証・識別を必須とすることで、悪意のある所有者による「カード認証」の不正利用は防止される。

このセキュリティ対策方針により、**T.Abuse_ReaderWriter_SecurityFunction** に対抗でき

る。

T.Interrupt_Power

悪意のある所有者により、TOE の利用中に電源を途絶し、TOE を異常な状態にすることは一般的な攻撃手法である。

T.Interrupt_Power の脅威には、いつ処理が終了してもデータが破壊されない仕組みや、データが破壊されていないかを識別することが効果的である。

TOE では、**O.Data_Protection** により処理途中のいかなるタイミングでの中断においても保護データならびにアクセス暗号鍵が破壊されないように保護する。また、**O.Diagnosis** により保護データならびにアクセス暗号鍵が破壊されていないことを検査可能とする。この 2 つのセキュリティ対策方針から、**T.Interrupt_Power** に対抗できる。

T.Break_Hardware

悪意のある所有者により、ハードウェアである IC チップを故障させセキュリティ機能を危殆化させることが想定される。

ハードウェアの故障に対しては、ハードウェアのセキュリティ機能を確保することが重要であるが、ファームウェアとしてハードウェアの診断を行うことやデータが破壊されていないかを確認することは効果的である。

TOE では、**O.Diagnosis** によりハードウェア異常を検知し、**O.Data_Error_Detection** により保護データならびにアクセス暗号鍵に異常がないことをアクセス時に確認する。これに加えて、IT 環境要求である **OE.Hardware_Protection** によりハードウェアのセキュリティを確保する。

これらのセキュリティ対策方針により、**T.Break_Hardware** に対抗できる。

T.Install_EvilProgram

悪意のある所有者が、欠陥修正プログラムのインストール機能を悪用し不正なプログラムをインストールし、TOE のセキュリティ機能を無効化することが想定される。

T.Install_EvilProgram の脅威には、欠陥修正プログラムの取り扱いに暗号処理を用いることが効果的である。

TOE では、**O.Security_Data_Protection** により、欠陥修正プログラムに暗号処理を用いることで、改ざんならびに偽造を防止する。このセキュリティ対策方針により、T.Install_EvilProgram に対抗できる。

T.Copy_TOEData

悪意のある所有者が、データ移動機能を悪用し TOE データを移動先以外に格納し TOE を複製することが想定される。

データ移動機能は、移動元のデータが移動先以外に格納できないようにすることで、データに含まれる保護データおよびアクセス暗号鍵の不正取得を防止できる。

TOE では、**O.Authentication** により、移動元と移動先を認証・識別し移動先以外へのデータ格納を防止する。このセキュリティ対策方針により、T.Copy_TOEData に対抗できる。

8.2. セキュリティ要件根拠

8.2.1 セキュリティ機能要件根拠

本節では、セキュリティ対策方針に対してセキュリティ機能要件が正しく策定されているか検証する。

■ 必要性の検証

セキュリティ対策方針とセキュリティ機能要件の対応を「**表 8-2 セキュリティ機能要件と TOE セキュリティ対策方針の対応表**」に示す。これにより、各セキュリティ機能要件が少なくとも 1 つのセキュリティ対策方針をカバーしていることを示している。

表 8-2 セキュリティ機能要件と TOE セキュリティ対策方針の対応表

セキュリティ機能要件	TOE セキュリティ対策方針										
	O.Authentication	O.Access_Control	O.Security_Data_Protection	O.Data_Protection	O.Data_Error_Detection	O.Communicate_Error_Detection	O.Communicate_Protection	O.Diagnosis	OE.Hardware_Protection	OE.Hardware_DES	OE.Hardware_RNG
FCS_COP.1a (暗号操作)	-	-	-	-	-	-	○	-	-	-	-
FCS_CKM.4 (暗号鍵破棄)	○	-	-	-	-	-	-	-	-	-	-
FCS_COP.1b (暗号操作)	○	-	-	-	-	-	-	-	-	-	-
FCS_COP.1c (暗号操作)	-	-	○	-	-	-	-	-	-	-	-
FDP_ACC.1a (サブセットアクセス制御)	-	○	-	-	-	-	-	-	-	-	-
FDP_ACF.1a (セキュリティ属性によるアクセス制御)	-	○	-	-	-	-	-	-	-	-	-
FDP_ACC.1b (サブセットアクセス制御)	-	○	-	-	-	-	-	-	-	-	-
FDP_ACF.1b (セキュリティ属性によるアクセス制御)	-	○	-	-	-	-	-	-	-	-	-
FDP_ACC.1c (サブセットアクセス制御)	-	○	-	-	-	-	-	-	-	-	-
FDP_ACF.1c (セキュリティ属性によるアクセス制御)	-	○	-	-	-	-	-	-	-	-	-

FDP_IFC.1a (サブセット情報フロー制御)	-	-	-	-	-	○	-	-	-	-	-
FDP_IFF.1a (単純セキュリティ属性)	-	-	-	-	-	○	-	-	-	-	-
FDP_IFC.1b (サブセット情報フロー制御)	-	-	○	-	-	-	-	-	-	-	-
FDP_IFF.1b (単純セキュリティ属性)	-	-	○	-	-	-	-	-	-	-	-
FDP_ETC.1 (セキュリティ属性なし利用者データのエクスポート)	-	○	-	-	-	-	-	-	-	-	-
FDP_ITC.1a (セキュリティ属性なし利用者データのインポート)	-	○	-	-	-	-	-	-	-	-	-
FDP_ITC.1b (セキュリティ属性なし利用者データのインポート)	-	○	-	-	-	-	-	-	-	-	-
FDP_ETC.2 (セキュリティ属性付き利用者データのエクスポート)	○	-	-	-	-	-	-	-	-	-	-
FDP_ITC.2 (セキュリティ属性付き利用者データのインポート)	○	-	-	-	-	-	-	-	-	-	-
FDP_RIP.1 (サブセット残存情報保護)	-	○	-	-	-	-	-	-	-	-	-
FDP_SDI.2 (蓄積データ完全性監視およびアクション)	-	-	-	-	○	-	-	-	-	-	-
FDP_UCT.1 (TSF 間利用者データ機密転送保護)	-	-	-	-	-	-	○	-	-	-	-
FDP_UIT.1 (データ交換完全性)	-	-	-	-	-	○	-	-	-	-	-
FIA_UAU.2 (アクション前の利用者認証)	○	-	-	-	-	-	-	-	-	-	-
FIA_UAU.4 (単一使用認証メカニズム)	○	-	-	-	-	-	-	-	-	-	-
FIA_UID.2 (アクション前の利用者識別)	○	-	-	-	-	-	-	-	-	-	-
FIA_AFL.1 (認証失敗時の取り扱い)	○	-	-	-	-	-	-	-	-	-	-
FMT_SMF.1 (管理機能の特定)	-	○	-	-	-	-	-	-	-	-	-
FMT_MTD.1 (TSF データの管理)	-	○	-	-	-	-	-	-	-	-	-
FMT_MSA.3 (静的属性初期化)	-	○	-	-	-	-	-	-	-	-	-
FMT_SMR.1 (セキュリティ管理役割)	-	○	-	-	-	-	-	-	-	-	-
FPT_AMT.1 (抽象マシンテスト)	-	-	-	-	-	-	-	○	-	-	-
FPT_FLS.1 (セキュアな状態を保持する障害)	-	-	-	○	-	-	-	-	-	-	-
FPT_ITC.1 (送信中の TSF 間機密性)	-	-	○	-	-	-	-	-	-	-	-
FPT_ITI.1 (TSF 間改変の検出)	-	-	○	-	-	-	-	-	-	-	-
FPT_RPL.1 (リプレイ検出)	-	-	-	-	-	○	-	-	-	-	-
FPT_RVM.1 (TSP の非バイパス性)	○	○	-	-	-	○	○	-	-	-	-
FPT_SEP.1a (FSF ドメイン分離)	○	○	-	-	-	-	-	-	-	-	-
FPT_TDC.1 (TSF 間基本 TSF データ一貫性)	-	-	○	-	-	-	-	-	-	-	-
FPT_TST.1 (TSF テスト)	-	-	-	-	-	-	-	○	-	-	-
FTA_SSL.3 (TSF 起動による終了)	○	-	-	-	-	-	-	-	-	-	-
FTP_ITC.1 (TSF 間高信頼チャネル)	○	-	-	-	-	-	-	-	-	-	-
FCS_COP.1e (暗号操作)	-	-	-	-	-	-	-	-	-	○	-
FCS_CKM.1 (暗号鍵生成)	-	-	-	-	-	-	-	-	-	-	○
FPT_PHP.3 (物理攻撃への抵抗)	-	-	-	-	-	-	-	-	○	-	-
FPT_SEP.1b (TSF ドメイン分離)	-	-	-	-	-	-	-	-	○	-	-

■ 十分性の検証

O.Authentication

本セキュリティ対策方針は、FCS_CKM.4 ， FCS_COP.1b ， FDP_ETC.2 ， FDP_ITC.2 ， FIA_UAU.2 , FIA_UAU.4 , FIA_UID.2 , FIA_AFL.1 , FPT_RVM.1 , FPT_SEP.1a , FTA_SSL.3 , FTP_ITC.1 のセキュリティ機能要件により実現できる。

FIA_UID.2 / FIA_UAU.2 によって、保護データ・アクセス暗号鍵・リーダ／ライタ機能へアクセスする前にはアクセス先を識別し認証する。アクセス先を識別・認証することで、FTP_ITC.1 の高信頼チャネルを確立する。認証は、OE.Hardware_RNG により生成した乱数をアクセス先のアクセス暗号鍵で OE.Hardware_DES を利用した FCS_COP.1b により暗号化し、TOE 外部へ送信する。TOE 外部では、受信した情報をアクセス暗号鍵で復号化・再度暗号化を行い、TOE へ返信する。TOE では、受信した情報をアクセス暗号鍵で復号化し､先に生成した乱数と一致しているかを確認することで認証とする｡乱数を利用することで、FIA_UAU.4 による認証情報の再利用が防止される。認証に失敗した場合に結果を返却しないことで、FIA_AFL.1 による認証処理の解析が防止される。また、FTA_SSL.3 および FCS_CKM.4 により、不要な認証状態を維持し続けることの攻撃機会を低減させるため、終了命令または有限時間後に再起動を行い、認証時に生成した暗号鍵を破棄し、以降の暗号通信を行えなくすることで利用を停止させる。

データ移動機能である FDP_ETC.2 , FDP_ITC.2 は、移動元と移動先の TOE を識別・認証することで、FTP_ITC.1 の高信頼チャネルを確立し、移動先以外へのデータ格納が防止される。さらに、各機能要件の迂回を防止するために、FPT_RVM.1 によって、他の TOE セキュリティ機能を動作させる前に必ず識別･認証を呼び出す構造とするとともに、各機能要件を不正な干渉から保護するために、FPT_SEP.1a によって TSF とサブジェクトのドメインを分離・維持する。

O.Access_Control

本セキュリティ対策方針は、FDP_ACC.1a ， FDP_ACF.1a ， FDP_ACC.1b ， FDP_ACF.1b ， FDP_ACC.1c ， FDP_ACF.1c ， FDP_ETC.1 ， FDP_ITC.1a ， FDP_ITC.1b ， FDP_RIP.1 ， FMT_SMF.1 , FMT_MTD.1 , FMT_MSA.3 , FMT_SMR.1 , FPT_RVM.1 , FPT_SEP.1a のセキュリティ機能要件により実現される。

アクセス制御は、保護データへのアクセス、属性*システム*・属性*エリア*・属性*サービス*の操作に適用される。保護データへのアクセスは、FDP_ETC.1 ， FDP_ITC.1a を適用し、FDP_ACC.1a , FDP_ACF.1a で指定されたアクセス制御方針に基づき、読み書きを制限する。

属性*システム*・属性*エリア*・属性*サービス*の操作は、FDP_ACC.1b , FDP_ACF.1b で指定されたアクセス制御方針に基づき実施する。この際、属性*システム*・属性*エリア*・属性*サービス*

の暗号鍵の登録・変更は、FDP_ITC.1b を適用する。加えて、属性*サービス*の登録時にはデータ格納領域が同時に生成され、FDP_RIP.1 により初期化する。属性*システム*・属性*エリア*・属性*サービス*の登録時に設定されるセキュリティ属性の初期値は FMT_MSA.3 で規定する。ステージ 遷移は、FDP_ACC.1c , FDP_ACF.1c で指定されたアクセス制御方針に基づき実施する。FMT_SMF.1 で指定された IC チップ製造段階の管理機能は、FMT_SMR.1 で識別された役割の操作許可者に FMT_MTD.1 に規定された操作を許可する。

さらに、各機能要件の迂回を防止するために、FPT_RVM.1 によって、他の TOE セキュリティ機能を動作させる前に必ずアクセス制御を呼び出す構造にするとともに、認証されたドメイン以外へのアクセスを拒否する FPT_SEP.1a によって TSF とサブジェクトのドメインを分離・維持する。

O.Security_Data_Protection

本セキュリティ対策方針は、FCS_COP.1c ， FDP_IFC.1b ， FDP_IFF.1b ， FPT_ITC.1 ， FPT_ITI.1 , FPT_TDC.1 のセキュリティ機能要件により実現される。

アクセス暗号鍵ならびに欠陥修正プログラムは重要な情報であるため、アクセス暗号鍵および欠陥修正プログラムの通信には OE.Hardware_DES を利用した FCS_COP.1c による暗号処理が行われる。暗号処理は、FeliCa パッケージ化制御方針である FDP_IFC.1b ならびに FDP_IFF.1b に従い実施され、暗号処理によりデータの偽造は防止される。また、 FPT_ITC.1 により、アクセス暗号鍵および欠陥修正プログラムの暗号化データ通信により、送信中の不正な暴露も防止される。加えて、FeliCa パッケージ化では FPT_ITI.1 に従い誤り検出情報による検証により、送信中のデータの改ざんも検出される。データ移動時には、FPT_TDC.1 によりアクセス暗号鍵が相違なく移動元から移動先に移行される。

O.Data_Protection

本セキュリティ対策方針は、FPT_FLS.1 のセキュリティ機能要件により実現される。

保護データならびにアクセス暗号鍵は、FPT_FLS.1 により処理中断時にもデータが破壊されないよう保証される。これにより、処理中断時にデータは保護される。

O.Data_Error_Detection

本セキュリティ対策方針は、FDP_SDI.2 のセキュリティ機能要件により実現される。

保護データならびにアクセス暗号鍵を含む不揮発性メモリのデータは、FDP_SDI.2 により誤り検出が行われる。これにより、蓄積されたデータに異常が発生した場合には、検知され適切な対応が行われる。

O.Communicate_Error_Detection

本セキュリティ対策方針は、FDP_IFC.1a ， FDP_IFF.1a ， FDP_UIT.1 ， FPT_RPL.1 ，

FPT_RVM.1 のセキュリティ機能要件により実現される。

保護データへのアクセス、属性 *システム*・属性 *エリア*・属性 *サービス*の情報の操作は FDP_IFC.1a , FDP_IFF.1a に従い実施される。これにより、FDP_UIT.1 で規定される通信の完全性を担保し、FPT_RPL.1 によりコマンドデータの再利用を検出する。さらに、各機能要件の迂回を防止するために、FPT_RVM.1 によって、他の TOE セキュリティ機能を動作させる前に必ず識別・認証機能を呼び出す構造になる。

O.Communicate_Protection

本セキュリティ対策方針は、FCS_COP.1a , FDP_UCT.1 , FPT_RVM.1 のセキュリティ機能要件により実現される。

保護データへのアクセス、属性 *システム*・属性 *エリア*・属性 *サービス*の操作に伴うコマンドデータ、レスポンスデータの通信データは、OE.Hardware_DES を利用した FCS_COP.1a に従い暗号処理が行われる。これにより、FDP_UCT.1 の保護データの不正な暴露を防止する。暗号処理で利用される暗号鍵は O.Authentication で OE.Hardware_RNG を使用して生成された乱数を利用する。さらに、各機能要件の迂回を防止するために、FPT_RVM.1 によって、他の TOE セキュリティ機能を動作させる前に必ず識別・認証機能を呼び出す構造になる。

O.Diagnosis

本セキュリティ対策方針は、FPT_AMT.1 , FPT_TST.1 のセキュリティ機能要件により実現される。

TOE の動作上重要なハードウェアの診断は、FPT_AMT.1 により、許可利用者の要求で実行可能とする。また、FPT_TST.1 により、TSF の正常動作の確認、TSF データおよび TSF 実行コードの完全性を検証可能とする。

OE.Key_Storage

本セキュリティ対策方針は、TOE 利用におけるアクセス暗号鍵運用の注意事項を「ユーザーガイダンスマニュアル」に記載し、アクセス暗号鍵管理者に周知することで実現される。

OE.Security_Configuration

本セキュリティ対策方針は、TOE 利用におけるセキュリティ属性の設定を「プロトコル仕様書」に記載し、サービス運営者に周知することで実現される。

OE.ICvendor_confidence

本セキュリティ対策方針は、TOE の配付に関する「配布文書」に記載し、IC チップ製造者に周知すると共に、IC チップベンダとの間で交わされる契約により実現される。

OE.Hardware_Protection

本セキュリティ対策方針は、FPT_PHP.3 , FPT_SEP.1b のセキュリティ機能要件により実現される。

TOE が動作するハードウェアへの直接攻撃はハードウェアにより対策されなければならない。そのため、ハードウェアの物理的攻撃の抵抗をハードウェア環境の要件として FPT_PHP.3 , FPT_SEP.1b に定義する。

OE.Hardware_DES

本セキュリティ対策方針は、FCS_COP.1e のセキュリティ機能要件により実現される。

TOE は、O.Authentication , O.Security_Data_Protection , O.Communicate_Protection で利用する暗号処理をハードウェア環境が用意する暗号アルゴリズムにより行う。そのため、暗号アルゴリズムをハードウェア環境の要件として FCS_COP.1e に定義する。

OE.Hardware_RNG

本セキュリティ対策方針は、FCS_CKM.1 のセキュリティ機能要件により実現される。

TOE は、O.Authentication で利用する乱数をハードウェア環境が用意する乱数生成ロジックにより生成する。そのため、乱数生成ロジックをハードウェア環境の要件として FCS_CKM.1 に定義する。

8.2.2 セキュリティ機能要件依存性

本 TOE で選択した TOE および IT 機能のセキュリティ機能依存要件と依存コンポーネントおよび除外コンポーネントを「**表 8-3 TOE セキュリティ機能要件とその依存性**」に示す。

表 8-3 TOE セキュリティ機能要件とその依存性

コンポーネント	CC Part.2 の依存性	ST の依存性	依存性有無	除外事由
FCS_COP.1a	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	FCS_CKM.1 FCS_CKM.4	×	・FMT_MSA.2 が適用されない理由の分析 暗号通信のために生成した暗号鍵（セッション鍵）にはセキュリティ属性が必要ないことから、FMT_MSA.2 の依存性は必要ない。
FCS_CKM.4	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1] FMT_MSA.2	FCS_CKM.1	×	・FMT_MSA.2 が適用されない理由の分析 当該オブジェクトのアクセス暗号鍵は、インフラ事業者・サービス運営者により任意に設定されるものであり、OE.Key_Storage よりセキュアな値を設定するようガイダンスに示すことで対策されることから、FMT_MSA.2 の依存性は必要ない。
FCS_COP.1b	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	FDP_ITC.1b FCS_CKM.4	×	・FMT_MSA.2 が適用されない理由の分析 当該オブジェクトのアクセス暗号鍵は、インフラ事業者・サービス運営者により任意に設定されるものであり、OE.Key_Storage よりセキュアな値を設定するようガイダンスに示すことで対策されることから、FMT_MSA.2 の依存性は必要ない。
FCS_COP.1c	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	FDP_ITC.1b	×	・FCS_CKM.4 が適用されない理由の分析 FDP_ACF.1b のアクセス制御で実施される操作により、サービス・エリアが削除される場合には共に鍵が削除される。このため、FCS_CKM.4 は適用されず満たされる。 ・FMT_MSA.2 が適用されない理由の分析 当該オブジェクト（アクセス暗号鍵または欠陥修正プログラム）の暗号処理に使う鍵は、インフラ事業者・サービス運営者により任意設定されるものであり、OE.Key_Storage よりセキュアな値を設定するようガイダンスに示すことで対策されることから、FMT_MSA.2 の依存性は必要ない。
FDP_ACC.1a	FDP_ACF.1	FDP_ACF.1a	○	すべての依存性は適切に満たされている。
FDP_ACF.1a	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1a FMT_MSA.3	○	すべての依存性は適切に満たされている。
FDP_ACC.1b	FDP_ACF.1	FDP_ACF.1b	○	すべての依存性は適切に満たされている。
FDP_ACF.1b	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1b FMT_MSA.3	○	すべての依存性は適切に満たされている。
FDP_ACC.1c	FDP_ACF.1	FDP_ACF.1c	○	すべての依存性は適切に満たされている。
FDP_ACF.1c	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1c	×	・FMT_MSA.3 が適用されない理由の分析 ステージ情報の初期値は、外部から TOE を通じてコマンドパラメータで与えるものではなく、焼付け時にメモリデータに反映されていることから、FMT_MSA.3 の依存性は必要ない。
FDP_IFC.1a	FDP_IFF.1	FDP_IFF.1a	○	すべての依存性は適切に満たされている。
FDP_IFF.1a	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1a	×	・FMT_MSA.3 が適用されない理由の分析 インポートする当該情報のセキュリティ属性は、コントローラもしくはリーダ／ライタの対向機器が生成する情報で構成されるため、初期値は存在しないことから、FMT_MSA.3 の依存性は必要ない。
FDP_IFC.1b	FDP_IFF.1	FDP_IFF.1b	○	すべての依存性は適切に満たされている。
FDP_IFF.1b	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1b	×	・FMT_MSA.3 が適用されない理由の分析 インポートする当該情報のセキュリティ属性は、コントローラもしくはリーダ／ライタの対向機器が生成する情報で構成されるため、初期値は存在しないことから、FMT_MSA.3 の依存性は必要ない。
FDP_ETC.1	[FDP_ACC.1 または FDP_IFC.1]	FDP_ACC.1a	○	すべての依存性は適切に満たされている。
FDP_ITC.1a	[FDP_ACC.1 または FDP_IFC.1] FMT_MSA.3	FDP_ACC.1a	×	・FMT_MSA.3 が適用されない理由の分析 セキュリティ属性に基づいてデータブロックからデータを読み込む操作であり、セキュリティ属性を初期化するものではないため、FMT_MSA.3 の依存性は必要ない。
FDP_ITC.1b	[FDP_ACC.1 または FDP_IFC.1] FMT_MSA.3	FDP_ACC.1b FMT_MSA.3	○	すべての依存性は適切に満たされている。
FDP_ETC.2	[FDP_ACC.1 または FDP_IFC.1]	FDP_IFC.1b	○	すべての依存性は適切に満たされている。
FDP_ITC.2	[FDP_ACC.1 または FDP_IFC.1] [FTP_ITC.1 または FTP_TRP.1] FPT_TDC.1	FDP_IFC.1b FTP_ITC.1 FPT_TDC.1	○	すべての依存性は適切に満たされている。
FDP_RIP.1	---	---	○	すべての依存性は適切に満たされている。
FDP_SDI.2	---	---	○	すべての依存性は適切に満たされている。
FDP_UCT.1	[FTP_ITC.1 または FTP_TRP.1] [FDP_ACC.1 または FDP_IFC.1]	FDP_IFC.1a FTP_ITC.1	○	すべての依存性は適切に満たされている。
FDP_UIT.1	[FDP_ACC.1 または FDP_IFC.1] [FTP_ITC.1 または FTP_TRP.1]	FDP_IFC.1a FTP_ITC.1	○	すべての依存性は適切に満たされている。
FIA_UAU.2	FIA_UID.1	FIA_UID.1	○	すべての依存性は適切に満たされている。
FIA_UAU.4	N/A	N/A	○	すべての依存性は適切に満たされている。
FIA_UID.2	N/A	N/A	○	すべての依存性は適切に満たされている。
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2	○	上位コンポーネントにより依存性は適切に満たされている。
FMT_SMF.1	N/A	N/A	○	すべての依存性は適切に満たされている。

FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1	○	すべての依存性は適切に満たされている。
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	---	×	・FMT_SMR.1 が適用されない理由の分析 許可された識別された役割は指定されていないため FMT_SMR.1 の依存性は必要ない。 ・FMT_MSA.1 が適用されない理由の分析 セキュリティ属性の PIN 設定とプライバシー設定は、セキュリティレベルが低い「設定なし」がデフォルトであり、セキュリティ属性を管理する必要はなく、それ以外のセキュリティ属性も、アクセス制御の中で外部から指定されてその都度設定されるため、セキュリティ属性を管理する必要がないことから、FMT_MSA.1 の依存性は必要ない。
FMT_SMR.1	FDP_UID.1	FDP_UID.1	○	すべての依存性は適切に満たされている。
FPT_AMT.1	N/A	N/A	○	すべての依存性は適切に満たされている。
FPT_FLS.1	ADV_SPM.1	ADV_SPM.1	○	すべての依存性は適切に満たされている。
FPT_ITC.1	N/A	N/A	○	すべての依存性は適切に満たされている。
FPT_ITI.1	N/A	N/A	○	すべての依存性は適切に満たされている。
FPT_RPL.1	N/A	N/A	○	すべての依存性は適切に満たされている。
FPT_RVM.1	N/A	N/A	○	すべての依存性は適切に満たされている。
FPT_SEP.1a	N/A	N/A	○	すべての依存性は適切に満たされている。
FPT_TDC.1	N/A	N/A	○	すべての依存性は適切に満たされている。
FPT_TST.1	FPT_AMT.1	FPT_AMT.1	○	すべての依存性は適切に満たされている。
FTA_SSL.3	N/A	N/A	○	すべての依存性は適切に満たされている。
FTP_ITC.1	N/A	N/A	○	すべての依存性は適切に満たされている。
FCS_COP.1e	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	N/A	×	・FDP_ITC.1 または FCS_CKM.1 が適用されない理由の分析 暗号操作に使用する鍵は TOE より与えられるものであるため、これらの依存性は必要ない。 ・FCS_CKM.4 が適用されない理由の分析 暗号操作で使用した鍵は TOE にて破棄されるものであるため、FCS_CKM.4 の依存性は必要ない。 ・FMT_MSA.2 が適用されない理由の分析 TOE より与えられた鍵にはセキュリティ属性は存在しないことから、FMT_MSA.2 の依存性は必要ない。
FCS_CKM.1	[FCS_CKM.2 または FCS_COP.1] FCS_CKM.4 FMT_MSA.2	N/A	×	・FCS_CKM.2 または FCS_COP.1 が適用されない理由の分析 TOE で使用するための乱数を生成し、直接 TOE に受け渡すことから、IT 環境での FCS_CKM.2 または FCS_COP.1 の依存性は必要ない。 ・FCS_CKM.4 が適用されない理由の分析 生成した乱数データは TOE にて破棄されるものであるため、FCS_CKM.4 の依存性は必要ない。 ・FMT_MSA.2 が適用されない理由の分析 本操作においてセキュリティ属性は存在しないことから、FMT_MSA.2 の依存性は必要ない。
FPT_PHP.3	N/A	N/A	○	すべての依存性は適切に満たされている。
FPT_SEP.1b	N/A	N/A	○	すべての依存性は適切に満たされている。

8.2.3 セキュリティ機能要件の一貫性根拠

本節では、本 TOE に対するセキュリティ要件のセットが内部的に一貫していることを説明する。

セキュリティ機能要件の繰り返しは、それらの要件記述の前に繰り返しの意図を示すことで、異なるタイプの事象に対する要件であることを説明し、各繰り返し要件の操作において、その違いを明らかにしている。すべてのセキュリティ機能要件について、8.2 の十分性根拠および依存性根拠により要件セットとしての効果を実証しており、各繰り返し要件を含め、競合や重複がない説明としている。また、8.2.4 では、機能要件間の相互サポート効果を説明しており、これらも矛盾のない説明としている。

8.2.4 セキュリティ機能要件の相互サポート根拠

本節では、本 TOE に対するセキュリティ機能要件が迂回、干渉、非活性化の攻撃から保護されることを説明する。

8.2.4.1 迂回防止の根拠

TOE は、保護資産のアクセスおよび操作時、識別認証機能（FIA）を必要とする構成を取る。これは、FPT_RVM.1 により、FIA_UAU.2 および FIA_UID.2 による識別認証に成功しない限り、他のすべての機能を使用できないことが保証される。

8.2.4.2 干渉防止の根拠

TOE は一般的な IC カードと違い信頼できないサブジェクトはインストールされない。FDP_IFC.1b によるアクセス暗号鍵のパッケージ化が適用され、アクセス暗号鍵のデータ送信時の改ざんに対する干渉を回避する。また、TOE の直接保護資産は、FDP_ACC.1a，FDP_ACC.1b，FDP_ACC.1c，FTA_SSL.3，FCS_CKM.4 を確実に実施することを保証する FPT_SEP.1a により、認証されたドメインを分離・維持し、ドメイン外部の許可のないサブジェクトによる干渉を禁止する。これに加え、TOE が搭載されるモバイル FeliCa IC チップは、FPT_PHP.3 , FPT_SEP.1b により物理的な干渉に対する対策が行われる。これらにより、外部からの干渉を防ぐことができる。

8.2.4.3 非活性化防止の根拠

TOE では、セキュリティ機能を非活性化する機能は有していないため、非活性化は防止される。従って、非活性化の検知は必要ない。

8.2.4.4 ガイドラインの相互サポート

TOE では、DES 暗号アルゴリズムを使用したサービスの移行期間確保のため DES 暗号アルゴリズムも選択可能としている。

8.2.5 最小機能強度レベル根拠

TOE を搭載したモバイル FeliCa 機器は、悪意のある第三者が容易に入手できる製品である。また、TOE 自身には電子マネーを含め重要なデータが格納され、TOE の情報操作は多大な

損害を与える恐れがある。ただし、本 TOE を利用したサービスは、TOE だけでなくモバイル FeliCa 機器のハードウェア情報・ソフトウェア情報、リーダ／ライタ機器のハードウェア情報・ソフトウェア情報、サーバ機器のソフトウェア情報などの専門知識と攻撃を行うためのソフトウェアツールが必要である。
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。

8.2.6 セキュリティ保証要件根拠

TOE は、金銭的価値を有するもの・利用者の個人情報に関わるものを格納し、かつ携帯電話のようなモバイル FeliCa 機器に組み込まれ、利用者の手に渡る。第三者の手に渡り攻撃されることを考慮する必要があるため、攻撃を考慮した脆弱性評定 AVA_VLA.3 および、欠陥発生時に即座に対応するための ALC_FLR.1 を追加した評価保証レベル EAL 4 追加で妥当である。

8.3. TOE 要約仕様根拠

セキュリティ機能要件に対してセキュリティ機能が正しく策定されているかを検証する。

8.3.1 必要性の検証

TOE のセキュリティ機能とセキュリティ機能要件との適合性を「表 8-4 TOE セキュリティ機能要件と TOE セキュリティ機能の対応表(1)」「表 8-5 TOE セキュリティ機能要件と TOE セキュリティ機能の対応表(2)」に示します。本表から、各機能要件がセキュリティ機能で採用されていることが示される。

表 8-4 TOE セキュリティ機能要件と TOE セキュリティ機能の対応表(1)

TOE セキュリティ機能	TOE セキュリティ機能要件																				
	FCS_COP.1a	FCS_CKM.4	FCS_COP.1b	FCS_COP.1c	FDP_ACC.1a	FDP_ACF.1a	FDP_ACC.1b	FDP_ACF.1b	FDP_ACC.1c	FDP_ACF.1c	FDP_IFC.1a	FDP_IFF.1a	FDP_IFC.1b	FDP_IFF.1b	FDP_ETC.1	FDP_ITC.1a	FDP_ITC.1b	FDP_ETC.2	FDP_ITC.2	FDP_RIP.1	FDP_SDI.2
認証機能 SF.Authentication	-	○	○	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
通信路保護機能 SF.CommunicateProtection	○	-	-	-	-	-	-	-	-	-	○	○	-	-	-	-	-	-	-	-	-
読み書き機能 SF.ReadWrite	-	-	-	-	-	-	-	-	-	-	-	-	-	-	○	○	-	-	-	-	-
アクセスコントロール機能 SF.AccessControl	-	-	-	-	○	○	○	○	○	○	-	-	-	-	○	○	○	-	-	○	-
セキュリティ情報保護機能 SF.TSFDataProtection	-	-	-	○	-	-	-	-	-	-	-	-	○	○	-	-	-	-	-	-	-
データ保護機能 SF.DataProtection	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	○
データ移動機能 SF.DataMove	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	○	○	-	-
診断機能 SF.SelfDiagnosis	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

表 8-5 TOE **セキュリティ機能要件と** TOE **セキュリティ機能の対応表**(2)

TOE セキュリティ機能	TOE セキュリティ機能要件																				
	FDP_UCT.1	FDP_UIT.1	FIA_UAU.2	FIA_UAU.4	FIA_UID.2	FIA_AFL.1	FMT_SMF.1	FMT_MTD.1	FMT_MSA.3	FMT_SMR.1	FPT_AMT.1	FPT_FLS.1	FPT_ITC.1	FPT_ITI.1	FPT_RPL.1	FPT_RVM.1	FPT_SEP.1a	FPT_TDC.1	FPT_TST.1	FTA_SSL.3	FTP_ITC.1
認証機能 SF.Authentication	-	-	○	○	○	○	-	-	-	-	-	-	-	-	-	○	○	-	-	○	○
通信路保護機能 SF.CommunicateProtection	○	○	-	-	-	-	-	-	-	-	-	-	-	-	○	○	-	-	-	-	-
読み書き機能 SF.ReadWrite	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
アクセスコントロール機能 SF.AccessControl	-	-	-	-	-	-	○	○	○	○	-	-	-	-	-	○	○	-	-	-	-
セキュリティ情報保護機能 SF.TSFDataProtection	-	-	-	-	-	-	-	-	-	-	-	-	○	○	-	-	-	-	-	-	-
データ保護機能 SF.DataProtection	-	-	-	-	-	-	-	-	-	-	-	○	-	-	-	-	-	-	-	-	-
データ移動機能 SF.DataMove	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	○	-	-	-
診断機能 SF.SelfDiagnosis	-	-	-	-	-	-	-	-	-	-	○	-	-	-	-	-	-	-	○	-	-

8.3.2 十分性の検証

FCS_COP.1a

TSF は、FCS_COP.1a に示された暗号アルゴリズムによって、通信路データの暗号処理を行わなければならない。

SF.CommunicateProtection は、通信データを DES および TDEA による暗号処理することを規定している。これにより、FCS_COP.1a が満たされる。

FCS_CKM.4

TSF は、FCS_CKM.4 に示された暗号鍵破棄方法によって、暗号鍵を破棄しなければならない。

SF.Authentication は、終了命令または有限時間後の再起動による揮発性メモリ領域の初期化にて暗号鍵を破棄することを規定している。これにより、FCS_CKM.4 が満たされる。

FCS_COP.1b

TSF は、FCS_COP.1b に示された暗号アルゴリズムによって、認証機能の過程において暗号処理を行わなければならない。

SF.Authentication は、認証データを TDEA により暗号処理することを規定している。これにより、FCS_COP.1b が満たされる。

FCS_COP.1c

TSF は、FCS_COP.1c に示された暗号アルゴリズムによって、アクセス暗号鍵および欠陥修正プログラムの暗号処理を行わなければならない。

SF.TSFDataProtection は、アクセス暗号鍵ならびに欠陥修正プログラムを TDEA による暗号処理を行うことを規定している。これにより、FCS_COP.1c が満たされる。

FDP_ACC.1a

TSF は、属性サービスアクセス制御方針として、FDP_ACC.1a に示されたサブジェクト、オブジェクト、サブジェクトとオブジェクト間の操作のリストを規定している。

SF.AccessControl は、データ格納領域に対する操作「書き込み」「読み込み」およびアクセス可否判断材料として属性*サービス*を提供する。ここでは、属性サービスアクセス制御方針を定義ている。これにより、 FDP_ACC.1a が満たされる。

FDP_ACF.1a

TSF は、データ格納領域へのアクセスに対して、「**表 5-4 属性サービスアクセス制御方針**」

を規定している。

SF.AccessControl は、操作「書き込み」「読み込み」に対する属性*サービス*の状態に応じたアクセス可否を実施する。これにより、 FDP_ACF.1a が満たされる。

FDP_ACC.1b

TSF は、属性管理操作制御方針として、FDP_ACC.1b に示されたサブジェクト、オブジェクト、サブジェクトとオブジェクト間の操作のリストを規定している。

SF.AccessControl は、属性*システム*・属性*エリア*・属性*サービス*操作の規定を提供する。ここでは、属性管理操作制御方針を定義している。これにより、 FDP_ACC.1b が満たされる。

FDP_ACF.1b

TSF は、「**表 5-5 属性管理操作制御方針**」を規定している。

SF.AccessControl は、属性*システム*・属性*エリア*・属性*サービス*の操作に対するアクセス可否を実施する。これにより、 FDP_ACF.1b が満たされる。

FDP_ACC.1c

TSF は、ステージ遷移アクセス制御方針として、FDP_ACC.1c に示されたサブジェクト、オブジェクト、サブジェクトとオブジェクト間の操作のリストを規定している。

SF.AccessControl は、ステージ遷移の規定を提供する。ここでは、ステージ遷移アクセス制御方針を定義している。これにより、 FDP_ACC.1c が満たされる。

FDP_ACF.1c

TSF は、「**表 5-6 ステージ遷移アクセス制御方針**」を規定している。

SF.AccessControl は、ステージ遷移に対する実行可否を制御する。これにより、FDP_ACF.1c が満たされる。

FDP_IFC.1a

TSF は、コマンドデータ・レスポンスデータに対する FeliCa 通信制御方針を規定している。

SF.CommuniacateProtection は、送受信時の通信データに対する操作に関する情報フロー制御方法を FeliCa 通信制御方針として定義している。これにより、FDP_IFC.1a が満たされる。

FDP_IFF.1a

TSF は、コマンドデータ・レスポンスデータに対する FeliCa 通信制御方針を規定している。

SF.CommuniacateProtection は、送受信時の通信データに対する操作を許可する情報フロー制御を実現しており、FeliCa 通信制御方針を具体化している。これにより、FDP_IFF.1a が満たされる。

FDP_IFC.1b

TSF は、アクセス暗号鍵ならびに欠陥修正プログラムの取り扱いに対する FeliCa パッケージ化制御方針を規定している。

SF.TSFDataProtection は、アクセス暗号鍵ならびに欠陥修正プログラムの送受信に対する操作に関する情報フロー制御方法を FeliCa パッケージ化制御方針として定義している。これにより、FDP_IFC.1b が満たされる。

FDP_IFF.1b

TSF は、アクセス暗号鍵ならびに欠陥修正プログラムの取り扱いに対する FeliCa パッケージ化制御方針を規定している。

SF.TSFDataProtection は、アクセス暗号鍵ならびに欠陥修正プログラムの送受信に対する操作を許可する情報フロー制御を実現しており、FeliCa パッケージ化制御方針を具体化している。これにより、FDP_IFF.1b が満たされる。

FDP_ETC.1

TSF は、データ格納領域に格納されたデータブロックをエクスポートする際、属性サービスアクセス制御方針を実施しなければならない。

SF.ReadWrite は、SF.AccessControl に従いデータ格納領域に格納されたデータブロックをエクスポートする。これにより、FDP_ETC.1 が満たされる。

FDP_ITC.1a

TSF は、データ格納領域に格納するデータブロックをインポートすることを規定している。

SF.ReadWrite は、SF.AccessControl に従いデータ格納領域に格納するデータブロックをインポートする。これにより、FDP_ITC.1a が満たされる。

FDP_ITC.1b

TSF は、属性*システム*・属性*エリア*・属性*サービス*のアクセス暗号鍵をインポートすることを規定している。

SF.AccessControl は、属性*システム*・属性*エリア*・属性*サービス*のアクセス暗号鍵をインポートする。これにより、FDP_ITC.1b が満たされる。

FDP_ETC.2

TSF は、属性*システム*・属性*エリア*・属性*サービス*ならびにデータ格納領域の全情報をエクスポートすることを規定している。

SF.DataMove は、属性*システム*・属性*エリア*・属性*サービス*ならびにデータ格納領域の全情

報をエクスポートする。これにより、FDP_ETC.2 が満たされる。

FDP_ITC.2

TSF は、属性*システム*・属性*エリア*・属性*サービス*ならびにデータ格納領域の全情報をインポートすることを規定している。

SF.DataMove は、属性*システム*・属性*エリア*・属性*サービス*ならびにデータ格納領域の全情報をインポートする。これにより、FDP_ITC.2 が満たされる。

FDP_RIP.1

TSF は、資源の割り当ての際に以前のどの資源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。

SF.AccessControl は、属性*サービス*の登録によるデータ格納領域の作成時に領域を初期化する。これにより、FDP_RIP.1 が満たされる。

FDP_SDI.2

TSF は、不揮発性メモリのデータに誤りがないか監視しなければならない。

SF.DataProtection は、不揮発性メモリのデータに対して、CRC 情報を付与し利用時に CRC 情報が正しいか検証する。これにより、FDP_SDI.2 が満たされる。

FDP_UCT.1

TSF は、保護データを保護した状態で送受信するよう、FeliCa 通信制御方針を実施しなければならない。

SF.CommunicateProtection は、通信データを FeliCa 通信制御方針に基づいて暗号処理を行い保護する。これにより、FDP_UCT.1 が満たされる。

FDP_UIT.1

TSF は、保護データを誤りから保護して送受信するよう FeliCa 通信制御方針を実施しなければならない。

SF.CommunicateProtection は、FeliCa 通信制御方針に基づいて通信データに誤り検出用の情報を付与し、誤り検出を行う。これにより、FDP_UIT.1 が満たされる。

FIA_UAU.2

TSF は、アクション前に認証が行われることを規定している。

SF.Authentication は、保護データへのアクセス前に認証を必要とする。これにより、FIA_UAU.2 が満たされる。

FIA_UAU.4

TSF は、認証時の認証データが再利用されないことを規定している。

SF.Authentication は、認証データに乱数を利用することで再利用を防止する。これにより、FIA_UAU.4 が満たされる。

FIA_UID.2

TSF は、操作が行われる前にアクセス先である属性*サービス*を識別することを規定している。

SF.Authentication は、認証時の暗号処理にアクセス先である属性*サービス*のアクセス暗号鍵を用いることで、アクセス先である属性*サービス*を識別する。これにより、FIA_UID.2 が満たされる。

FIA_AFL.1

TSF は、認証失敗 1 回毎に検知し応答を返却しないことを規定している。

SF.Authentication は、認証失敗時に応答を返却しないことを規定している。これにより、FIA_AFL.1 が満たされる。

FMT_SMF.1

TSF は、セキュリティ管理機能を特定することを規定している。

SF.AccessControl は、モバイル FeliCa IC チップ製造者に許可するセキュリティ管理機能を規定している。これにより、FMT_SMF.1 が満たされる。

FMT_MTD.1

TSF は、IC チップ製造段階のアクセス暗号鍵の操作を IC チップ製造者に許可しなければならない。

SF.AccessControl は、Manufacture ステージ における属性情報のアクセス暗号鍵の変更を IC チップ製造者のみに許可することを規定している。これにより、FMT_MTD.1 が満たされる。

FMT_MSA.3

TSF は、セキュリティ属性のデフォルト値のプロパティ定義を保証しなければならない。

SF.AccessControl は、属性*システム*・属性*エリア*・属性*サービス*の登録時に設定されるセキュリティ属性の初期値を規定している。これにより、FMT_MSA.3 が満たされる。

FMT_SMR.1

TSF は、モバイル FeliCa IC チップ製造者の役割を維持することを規定している。

SF.AccessControl は、アクセス暗号鍵所有者のみが管理機能を操作できることを規定してい

る。この機能を実行できるのは、Manufacture ステージにおけるアクセス暗号鍵所有者である IC チップ製造者のみが操作できることから、モバイル FeliCa IC チップ製造者の役割を維持している。これにより、FMT_SMR.1 が満たされる。

FPT_AMT.1

TSF は、IC チップが正しい状態であることを実証するためにテストを提供できなければならない.

SF.SelfDiagnosis は、IC チップが正しく動作する状態かどうかを確認するために、IC チップが提供する機能の診断機能を提供する。これにより、FPT_AMT.1 が満たされる。

FPT_FLS.1

TSF は、動作中の電源途絶・リセット動作に対してセキュアな状態を維持しなければならない。

SF.DataProtection は、動作中に異常が発生しても保護データならびにアクセス暗号鍵が破壊されない。これにより、FPT_FLS.1 が満たされる。

FPT_ITC.1

TSF は、送受信される TSF データを不当な暴露から保護しなければならない。

SF.TSFDataProtection は、TSF データであるアクセス暗号鍵ならびに欠陥修正プログラムを暗号化データ通信にて取り扱う。これにより、FPT_ITC.1 が満たされる。

FPT_ITI.1

TSF は、送受信される TSF データの誤りを検出する機能を提供しなければならない。

SF.TSFDataProtection は、TSF データであるアクセス暗号鍵ならびに欠陥修正プログラムの暗号処理で誤り検出を行う。これにより、FPT_ITI.1 が満たされる。

FPT_RPL.1

TSF は、暗号通信される通信データの再送を検出しなければならない。

SF.CommunicateProtection は、暗号処理が行われる通信データ内にシーケンス番号を保持させシーケンス番号の確認を行うことで再送を検出する機能を提供する。これにより、FPT_RPL.1 が満たされる。

FPT_RVM.1

TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出されることを保証しなければならない。

SF.AccessControl および SF.CommunicateProtection の実行前に、SF.Authentication により

必ず識別認証を行い成功することを求める FeliCa 相互認証を採用することで、保護データへアクセスする際に実施する識別認証のバイパスを防止する。これにより、FPT_RVM.1 が満たされる。

FPT_SEP.1a

TSF は、信頼できない外部の干渉と改ざんから保護しなければならない。

SF.AccessControl は、認証されていない状態からの外部干渉から保護することを提供する。また、SF.Authentication は、外部干渉から保護された認証状態の維持管理を行う。これにより、FPT_SEP.1a が満たされる。

FPT_TDC.1

TSF は、TSF データをエクスポート・インポートする際、一貫して扱わなければならない。

SF.DataMove は、TSF データを差異なくエクスポート・インポートする機能を提供する。これにより、FPT_TDC.1 が満たされる。

FPT_TST.1

TSF は、TOE の保持する属性情報ならびにデータ格納領域に誤りがないか自己テストを実行できなければならない。

SF.SelfDiagnosis は、TOE が保持するデータに欠損がないか診断する機能を提供する。これにより、FPT_TST.1 が満たされる。

FTA_SSL.3

TSF は、認証状態を規定された有限時間後に終了させることを規定している。

SF.Authentication は、認証状態を有限時間後に破棄する。これにより、FTA_SSL.3 が満たされる。

FTP_ITC.1

TSF は、アクセス先もしくは対向機器との間で信頼できるチャネルを提供しなければならない。

SF.Authentication は、アクセス先を認証することにより、アクセス先とのみ共有される情報を生成し、信頼できる通信路を構築することで、読み書き機能、アクセスコントロール機能をセキュアに実行できる。また、データ移動機能時に対向機器を認証することにより、対向機器とのみ共有される情報を生成し、信頼できる通信路を構築することで、データ移動機能をセキュアに実行できる。これにより、FTP_ITC.1 が満たされる。

8.3.3 セキュリティ機能強度根拠

5 章で示したとおり、機能強度主張すべきセキュリティ機能要件は存在しないことから、機能強度レベルを明示すべき IT セキュリティ機能は存在せず、一貫している。

8.3.4 セキュリティ保証手段根拠

「１.３CC 適合」で定義した EAL 4 追加の保証レベルに対する、すべての保証手段となる証拠資料は対応し漏れはない。

FeliCa Networks

モバイル FeliCa IC チップ シリーズ
モバイル FeliCa IC チップファームウェア（AE 版）
セキュリティターゲット

Version 1.06
No. FN12-F027-J01-06

2009 年 2

フェリカネットワークス株式会社