TFPS

クラウド型決済システム Thincacloud コアモジュール

セキュリティターゲット

2013年7月9日
Ver.1.00

改訂履歴

改訂番号	版数	内容
20130709A	Ver.1.00	初版

商標について

“Windows”、“Windows CE”は米国 Microsoft Corporation の米国およびその他の国における登録商標です。

“FeliCa”はソニー株式会社の登録商標です。

“おサイフケータイ”は株式会社 NTT ドコモの登録商標です。

Thincacloud

— 目次 —

Thincacloud

1. ST概説

1.1. ST参照

タイトル: クラウド型決済システム Thincacloud コアモジュール セキュリティターゲット
版数: 1.00
発行: 2013年7月9日
作成者: TFペイメントサービス株式会社
キーワード: 電子マネー、電子マネー決済、NFC、FeliCa、クラウド、POS、モバイル端末、おサイフケータイ

1.2. TOE参照

名称: クラウド型決済システム Thincacloud コアモジュール
版数: 本TOEは、4種のTOEコンポーネントの組み合わせで構成される。
それぞれのコンポーネントは、個別のバージョン番号で識別される。
TOEを構成する各コンポーネントのバージョン番号は表1-1のとおり。

表1-1 TOEコンポーネント名称とバージョン番号

コンポーネント名称	Ver.	備考
Thincacloud決済サーバー	1.0.0	サーバーソフトウェア及びHSM
Thincacloud決済クライアント Windows CE版	1.0.0	POS端末ソフトウェア
Thinca Payment App for おサイフケータイ	1.0.0	モバイル端末(FeliCa内蔵)ソフトウェア
Thinca Payment App for NFC	1.0.0	モバイル端末(FeliCa非内蔵)ソフトウェア

開発者: TFペイメントサービス株式会社

1.3. TOE概要

1.3.1. TOE種別

本TOEは、電子マネー決済処理機能をクラウド型システムとして提供するプログラムにハードウェアとしてHSMを追加したものである。このクラウド型システムは、“TFペイメントサービス株式会社”が開発し運用するシステムである（システムとは、特定の環境に構築された特定のIT製品を意味する）。本TOEは、同システムを構成するサーバーと端末それぞれに搭載されるプログラムコンポーネントの集合体及びHSMであり、電子マネー決済のセキュアな処理機能を提供する。

1.3.2. TOEの用途と主要セキュリティ機能

(1) TOE用途

本TOEを含むシステムは、電子マネー決済サービスの提供者に対し、決済サービス実行のための共通プラットフォーム環境を提供する。共通プラットフォーム環境とは、そのプラットフォーム上で異なる電子マネー決済サービスを個別APとして動作させ、複数の異なる電子マネー決済サービスを運用できる環境である。本TOEは、この共通プラットフォームの中核となるソフトウェア部分及びHSMが該当する。本STは、共通プラットフォームを利用する電子マネー決済サービス提供者に向け、TOEの提供するセキュリティ特性に関わる情報を提供する。

電子マネー決済サービス提供者とは、“加盟店”(電子マネーによる商品販売事業者)、“代理店”(弊社サービスを代理販売する事業体)、“ブランド”(電子マネーを発行・管理する事業体; 鉄道系事業者、大手流通業者など多様な母体を持つ) を指す。ブランドに相当する事業者に対し、本STは、電子マネー決済サービスのセキュアな運営に関わるソリューションを提供する。代理店に相当する事業者は、本サービスの提供に際し、本STに記載されたTOEセキュリティ機能のメカニズム情報が参考となろう。加盟店に相当する事業者は、本STを通し、端末を中心とした電子マネー決済サービスのセキュアな運用についての情報を入手できる。

本TOEが提供する電子マネー決済処理は、“プリペイド型電子マネー決済”と呼ばれる。電子マネー決済サービスの利用者は、所有するIC媒体 (カードや携帯電話などに内蔵されるICチップ) にあらかじめ電子マネーを格納し (プリペイド)、その電子マネーを使用して商品購入時の決済を行う。本TOEが対応するIC媒体はFeliCa ICチップ[1]である。FeliCa ICチップを使用した電子マネー決済に適用される暗号アルゴリズムや通信プロトコルは、FeliCa仕様として統一されている。

(2) 主要セキュリティ機能

TOEは、電子マネー決済サービスをセキュアに実行するために必要なセキュリティ機能を持つ。TOEの主要なセキュリティ機能を以下のリストに示す。

- FeliCa ICチップ識別・認証 — 電子マネー決済処理に使用されるFeliCa ICチップを識別・認証し、正当なFeliCa ICチップだけに電子マネー決済を実行する。
- 端末検証 — POS端末、モバイル端末をサーバーに接続する際、それらのTOEコンポーネントが正当なものであることを検証する。
- 決済データ保護 — 消費者の持つFeliCa ICチップに決済サービスを提供する際、転送中の決済データを暴露・改ざんから保護する。
- 監査 — サーバーTOEコンポーネントのセキュリティ機能動作に関わる監査データを生成する。

[1] FeliCa ICチップは、ICカードやモバイル端末 (ex. おサイフケータイ) などに搭載される。

1.3.3. TOE以外のハードウェア/ソフトウェア/ファームウェア

本TOEは特定のシステムに適用されるソフトウェア (プログラム) にハードウェアとしてHSMを追加したものである。TOEを含む全体システムには、TOE外のソフトウェアやハードウェアなど、電子マネー決済サービス提供に必要な要素が含まれる。これらTOE外のソフトウェアやハードウェアは、TOEのIT環境である。TOEのIT環境のうち、TOEの動作に必要なハードウェア/ソフトウェアを表1-2のリストに示す。なお、POS端末TOEコンポーネントのバージョン確認には、Windows Mobile デバイス センターが組み込まれたWindows PC (OS: Windows 7 または Windows Vista) を用いる。

表1-2の構成要素において、その種類によって、以下に示す特性の違いがある。

- サーバー: TOE下位のOS及びハードウェアを含め、IT環境が一意に特定される。
- 端末: POS端末及びモバイル端末では、TOEの動作に必要なOSのバージョンやハードウェア仕様にバリエーションがある。そのため、評価者テストに使用された機種とOSを特定する。
  POS端末及びモバイル端末(FeliCa非内蔵)では、消費者※が端末を購入するのではなく、TOEコンポーネントが組み込まれた端末が加盟店※に納品される。加盟店や消費者が端末にTOEコンポーネントを組み込む必要はない。
  モバイル端末(FeliCa内蔵)では、消費者自身がGoogle Playから “Thinca Payment App for おサイフケータイ” をダウンロードし、端末に組み込む。

※電子マネー決済サービスの関係者と役割については、表1-3を参照。

表1-2 TOE以外のハードウェア/ソフトウェア/ファームウェア

サーバー/端末種類	構成要素	説明
サーバー	HP-UX 11i v3	TOEが動作するOS。TOEはOSのJava VMを使用する。
	HP Integrity rx2800 i2	ハードウェアを含むサーバー製品名称
	Oracle 11g Release 2 (暗号鍵DB)	TOEが消費者のFeliCa ICチップと相互認証するための暗号鍵を保管するDB。相互認証用暗号鍵はブランドごとに準備され、暗号化されて保管される。
POS端末	CASIO DT-5300	POS端末
	Windows CE 6.0	TOEが動作するOS

モバイル端末 (FeliCa内蔵)	・docomo N-04C[*2], SH-12C[*2] ・au IS03[*1]	TOE及びOSが動作するAndroid端末
	Android OS 2.2[*1], 2.3[*2] (対応バージョンは機種により異なる)	TOEが動作するOS (OS標準のブラウザを含む)
	モバイルFeliCaクライアント for Android (MFC)	モバイル端末(FeliCa内蔵)において、 FeliCaチップを制御するミドルウェア
モバイル端末 (FeliCa非内蔵)	Google Nexus S	TOE及びOSが動作するAndroid端末
	Android OS 4.1	TOEが動作するOS (OS標準のブラウザを含む)

1.4. TOE記述

1.4.1. TOEと環境の説明

(1) TOEを含む全体システム

まず、TOEを含む全体システムを説明する。TOEを含む全体システムは、決済サービスセンターに置かれるサーバー、インターネットを介してサーバーを利用する端末（POS端末、モバイル端末）、及び外部ECサイトで構成される。全体システムにおけるサーバーは特定された一つの装置であるが、端末と外部ECサイトは固定的でなく、運用を通して変動する。

サーバーのTOEコンポーネントは、電子マネー決済の共通処理を実行するプログラム及び、ハードウェアとしてのHSMである。決済処理機能のほかに監査データ生成機能を持つ。

端末には、POS端末、モバイル端末の2種類がある。それぞれに、TOEの一部を構成するプログラムコンポーネントが搭載される。端末のTOEコンポーネントは、サーバーの指示を受け、消費者の電子マネー格納媒体から電子マネーを引き落とす機能を持つ。本TOEでは、電子マネー格納媒体として、FeliCa ICチップを使用する。

ECサイトはTOE範囲外の装置である。モバイル端末向けのオンライン店舗としてサービスを提供する。ECサイトの役割は、次節のモバイル端末の項で詳しく説明する。

次に、全体システムの構成要素を説明する。ここでは各構成要素の役割を説明し、後述の（3）で、各構成要素の動作を記載する。

[サーバー]

サーバーは、POS端末、モバイル端末を制御し、消費者のFeliCa ICチップに対して電子マネー決済処理を実行する。この決済処理とは、電子マネー引き落としのことである。FeliCa ICチップに対するサーバーの決済処理は、オンライン・リアルタイムで実行される。

サーバーは、TOEのコンポーネント(ソフトウェア、ハードウェア)とそれ以外の要素で構成される。TOEソフトウェアコンポーネントはサーバーの一部であり、FeliCa ICチップに対する電子マネー決済処理の実行機能を受け持つ。TOEソフトウェアコンポーネントには、FeliCa ICチップへのアクセスを実現するため、HP IC-Chip Access Server for FeliCaが含まれる。また、webアプリケーションサーバーとしてWebLogic 10.3が含まれる。TOEハードウェアコンポーネントはHSMであり、サーバーにハードウェアとして組み込まれる。

サーバーには、各ブランドごとの電子マネー決済APが搭載される。これらのAPは、それぞれが独立した決済サービスを実行する。サーバーには、さらに、ミドルウェア、OS、ハードウェアが含まれる。これらは、各種AP及びTOEの下位で動作する。

サーバーは、セキュアなデータセンターに設置される。データセンターにはTOE範囲外の装置としてL/Bが設置され、端末やECサイトとのSSL通信が実現される。

[端末]

サーバーに接続される端末には、POS端末とモバイル端末の2種類がある。

POS端末は、加盟店の実店舗に置かれ、店員によって操作される。店員は、消費者の商品購入に際し、POS端末を用いて決済処理を行う。取引情報はPOS端末からサーバーへ送られ、サーバーはその取引情報に基づいてPOS端末に決済を指示する。POS端末は、消費者のFeliCa ICチップから代金に相当する電子マネーを引き落とす。

POS端末には、消費者が決済サービスを受ける際に必要な付帯機能が備わる。例えば、決済金額表示、決済音、レシート印字などの機能が付加される。複数のブランドに対応するPOS端末では、電子マネーのブランド選択機能が加わる。

モバイル端末は、消費者が保有する端末である。消費者は、端末のブラウザ機能を用いて加盟店のオンライン店舗（ECサイト）にアクセスし、商品を選び、FeliCa ICチップで決済する。

モバイル端末には、FeliCa ICチップ内蔵と非内蔵の2つのタイプがある。FeliCa ICチップ内蔵タイプの例は、「おサイフケータイ」と呼ばれる端末である。FeliCa ICチップ内蔵タイプの端末には、モバイルFeliCaクライアント for Android (MFC) が搭載されており、TOE範囲外である。このタイプの端末は、内蔵のFeliCa ICチップで決済するほか、外部のFeliCa ICチップで決済することもできる。一方、FeliCa ICチップ非内蔵タイプの端末は、NFCインタフェースを備え、このインタフェースを介して外部のFeliCa ICチップで決済する。

POS端末、モバイル端末では、FeliCa ICチップで電子マネー決済処理を実行する（FeliCa ICチップから電子マネーを引き落とす）際に、決済に関わる通信データ転送を仲介するプログラムコンポーネントがTOEに相当する。

[ECサイト]

ECサイトとは、インターネット上のオンライン店舗であり、加盟店によって運用される。ECサイトはTOE範囲外であり、モバイル端末に対するオンライン取引サービスを提供する。モバイル端末は、端末

のブラウザ機能を使用してECサイトにアクセスし、商品の選択・購入手続きを行う。取引に関わる情報はECサイトからサーバーに送られ、モバイル端末の接続先がECサイトからサーバーにリダイレクトされ、サーバーとモバイル端末のTOEコンポーネントによって決済処理が実行される。

(2) 電子マネー決済サービスの手順

上述した電子マネー決済サービスの手順を整理したものを以下に示す。ここで説明する手順は、実際の決済サービスで実行される手順のうち、TOEのセキュリティ機能の説明に必要となる部分だけを抽出したものである。実際の手順では、電子マネーのブランド選択 (複数のブランドから、その取引で使用する電子マネーのブランドを選ぶ) などの付帯サービス、あるいは、残高照会やカード管理など、決済以外の手順などのバリエーションが含まれる。

[POS端末による実店舗での決済手順]

i) 消費者が店舗で購入商品を決めると、店員がPOS端末を操作し、サーバーに取引内容を伝える。

ii) サーバーは、POS端末を介して消費者のFeliCa ICチップから決済代金を引き落とす。

[モバイル端末によるオンライン店舗での決済手順]

i) 消費者は、モバイル端末のブラウザから外部ECサイトのオンライン店舗にアクセスし、購入商品を決める。

ii) ECサイトは、サーバーに取引情報を伝えるとともに、サーバーからリダイレクト先URL情報を入手し、端末へ伝える。

iii) モバイル端末は、接続先をサーバーにリダイレクトし、決済要求を送出する。この動作はモバイル端末内で自動的に実行される。

iv) サーバーは、モバイル端末からの決済要求に応答し、ECサイトから送られた取引情報に基づいて、消費者のFeliCa ICチップから決済代金を引き落とす。

(3) TOEとそのコンポーネント

TOEは、電子マネー決済サービスの共通機能部分を実行するソフトウェアにハードウェアとしてHSMを追加したものである。ソフトウェアは、サーバー、POS端末、モバイル端末それぞれに搭載されるTOEプログラムコンポーネントの集合体である。

TOEを構成するコンポーネント及びそのIT環境を図1-1の概念図で説明する。同図では、TOEに相当するコンポーネントを濃い青色で示している。

サーバーのTOEコンポーネントは、OSの上位に位置し、決済処理機能を提供する。個々のブランドに固有の電子マネー決済サービス機能は、ブランドごとの業務APで実現される。TOEコンポーネントには、nanaco向けの業務AP(図1-1中の(AP1))が含まれるが、その他の業務AP(図1-1中のAP2…APn)は含まれない。なお、これらの業務APは、“TFペイメントサービス株式会社” が開発する。

POS端末のTOEコンポーネントは、サーバーのTOEコンポーネントと協働し、消費者のFeliCa ICチップから電子マネーを引き落とす。

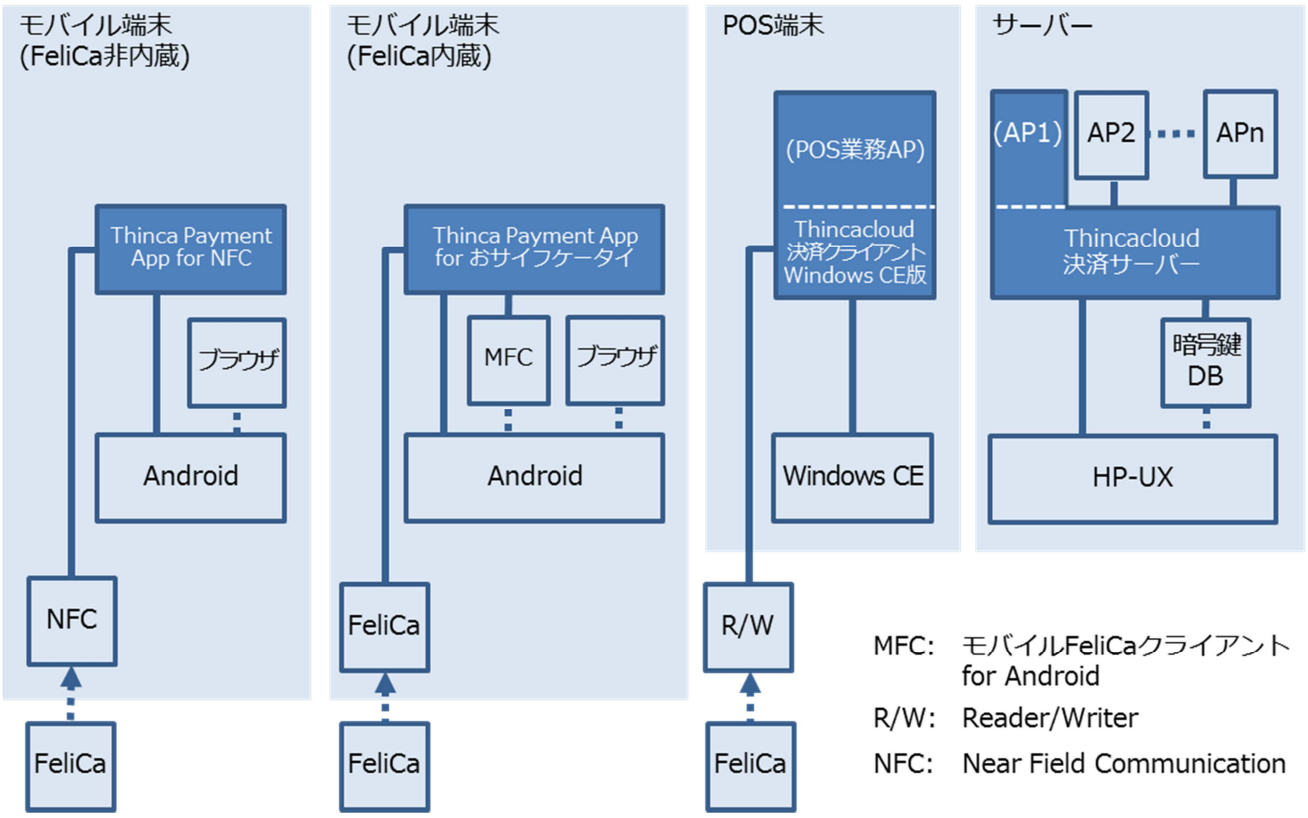

図 1-1　　装置ごとのTOEコンポーネントとIT環境

モバイル端末のTOEコンポーネントも、POS端末と同様、サーバーのTOEコンポーネントと協働して消費者のFeliCa ICチップから電子マネーを引き落とす。モバイル端末(FeliCa内蔵)は、内蔵FeliCa ICチップ、あるいは外部FeliCa ICチップのどちらでも決済を行える。モバイル端末(FeliCa非内蔵)は、NFC通信機能を介して、外部のFeliCa ICチップによる決済だけが行える。次に、図1-1の各TOEコンポーネントにおける動作を詳しく説明する。

[サーバー]

サーバーは、電子マネー決済処理を中央で集中管理する。サーバーでは、“Thincacloud 決済サーバー”がTOEのコンポーネントである。サーバーのTOEコンポーネントは、決済サービスの処理機能を提供する。この処理機能の中核は、端末のTOEコンポーネントと協働し、消費者のFeliCa ICチップから電子マネーを引き落とす処理である。この処理に関連し、POS端末や外部ECサイト (外部ECサイトは図1-1に記載されていない) との取引情報交換、FeliCa ICチップとの通信における暗号操作、及びTOEセキュリティ機能に関わる監査データ生成機能を備える。上位の業務APは、各ブランド固有の決済処理関連機能を提供する。

サーバーのTOEコンポーネントには、FeliCa ICチップへのアクセスを実現するため、HP IC-Chip Access Server for FeliCaが含まれる。また、webアプリケーションサーバーの機能を実現するため、WebLogic 10.3が含まれる。サーバーには、TOEの関連機能として、暗号鍵DBとHSMが置かれ、TOEとFeliCa ICチップ間の通信に適用される暗号演算のメカニズムを提供する。サーバーのTOEコンポーネ

ントには、HSMが含まれるが、暗号鍵DB はTOE範囲外である。暗号操作は、TOE (サーバーのTOEコンポーネント) とFeliCa ICチップ間の相互認証に適用される。詳細を以下に説明する。

相互認証に使用する暗号鍵として、ブランドごとに固有の鍵を使用する。この鍵は、暗号化されて暗号鍵DBに保管され、TOEの起動時に、TOEの制御によって暗号鍵DBから読み出され、HSM内で復号されて相互認証に使用される。復号された鍵は、TOEが稼働中の間、HSM内で保持される。相互認証用暗号鍵の復号鍵 (“親鍵” と呼ばれる) はHSM内に格納されている。相互認証に関わる暗号演算は、HSM内で実行される。TOEのセキュリティ機能とは直接関係しないが、ブランドごとの相互認証用暗号鍵に高度の機密性が要求される。鍵の使用はHSM内部に限定され、平文状態でHSM外に読み出されることはない。

電子マネーを格納する消費者のFeliCa ICチップは、ブランドに対応する相互認証用暗号鍵を格納している。サーバーは、電子マネーのブランドによって相互認証に使用される暗号鍵を選択し、FeliCa ICチップと相互認証を行う。

サーバーとFeliCa ICチップとの通信データは、FeliCa仕様により機密性及び完全性を保護する。

サーバーのTOEコンポーネントは、そのほか、以下の機能を有する。

- 監査データ生成: サーバーTOEコンポーネントのセキュリティ機能の動作に関わる監査データを生成する。生成された監査データは、サーバー上の他のコンポーネントのログデータと併せ、TOE外で管理される。
- 端末の検証: TOEの一部である端末 (POS端末、モバイル端末) のTOEコンポーネントをサーバーTOEコンポーネントに接続する際、端末TOEコンポーネントが適正なものであることを検証する。詳細は、次節 (4) を参照。

[端末]

TOE全体 (サーバーと端末のTOEコンポーネント) に要求される主要セキュリティ機能は、FeliCa ICチップとサーバー間の通信データ保護、及びFeliCa ICチップの正当性確認である。しかしながら、これらのセキュリティ機能は、サーバーのTOEコンポーネント (及びFeliCa ICチップ) で実行され、端末 (POS端末、モバイル端末) のTOEコンポーネントは、FeliCa ICチップから電子マネーを引き落とす決済処理において、セキュリティに関わる動作には直接関与しない。保護された通信データは、端末内をスルーで通過する。POS端末及びモバイル端末のTOEコンポーネントは、決済に関わる通信データ転送を仲介し、間接的にTOEセキュリティ機能の動作を支援する。

[POS端末]

POS端末は、加盟店の実店舗に置かれ、店員の操作によって決済を実行する。決済に店員が介在するので、決済方法を “対面決済” と呼ぶ。

POS端末による決済処理では、POS端末のTOEコンポーネント “Thincacloud 決済クライアント Windows CE版” を通して取引情報がサーバーへ送られる。サーバーは、その取引情報に基づき、POS端末に決済を指示する。POS端末TOEコンポーネントは、サーバーの指示に従い、消費者のFeliCa ICチップからの電子マネー引き落とし、あるいは残高問い合わせへの応答表示等を行う。

POS端末上の “POS業務AP” は “Thincacloud 決済クライアント Windows CE版” に含まれ、POS端末としての付帯サービス機能を提供する。サーバーにおけるブランドごとの業務APと連携して決済処理を行う。付帯サービス機能の例は、決済金額表示、決済音による操作応答、レシート印字などである。

[モバイル端末]

モバイル端末は、消費者が保有する端末である。消費者は、モバイル端末のブラウザを使用してインターネット上のオンライン店舗（ECサイト）で買い物をし、FeliCa ICチップの電子マネーで決済する。決済に店員が関与しないので、“非対面決済”と呼ばれる。

モバイル端末には、FeliCa ICチップ内蔵、及び非内蔵の二つのタイプがある。前者には“Thinca Payment App for おサイフケータイ”、後者には“Thinca Payment App for NFC”のTOEコンポーネントが搭載される。FeliCa ICチップ内蔵タイプは、端末内部のFeliCa ICチップで電子マネー決済を行うほか、消費者による選択操作によって、外部のFeliCa ICチップでも決済できるものが一般的である。一方、FeliCa ICチップ非内蔵タイプは、端末のNFC機能を介して外部のFeliCa ICチップで決済する。

モバイル端末による電子マネー決済は、二つの段階で実行される。初めの段階では、ECサイトにアクセスし、取引内容を決定する。これは、1.4.1.の（2）に示したモバイル端末の手順のうち、i）から iii）に相当する。モバイル端末のブラウザ（TOE外）は、初めにECサイトに接続され、そののち、決済サービスセンターにリダイレクトされ、決済サービスセンターのサーバーに接続される。

次の段階では、電子マネーによる決済を実行する。1.4.1.の（2）に示した手順 iv）に相当する。この段階では、モバイル端末の TOEコンポーネントである“Thinca Payment App for おサイフケータイ”あるいは“Thinca Payment App for NFC”が動作し、サーバーのTOEコンポーネントと消費者のFeliCa ICチップ間の通信を仲介し、消費者のFeliCa ICチップから商品の代金に相当する電子マネーが引き落とされる。

(4) TOEコンポーネント動作停止中の端末

TOEの運用時、サーバーは、システムの一部として常に動作状態である。一方、TOEコンポーネントを内部に持つPOS端末あるいはモバイル端末の場合、電源オフ時やサーバー未接続時など、サーバーとデータ交換を行えない状態がある。

POS端末あるいはモバイル端末のTOEコンポーネントが所定の機能を発揮するのは、端末がサーバーに接続され活性状態にあるときである。端末動作停止中、あるいは動作中でもサーバーに未接続のとき、端末のTOEコンポーネントは、TOEの一部として動作できない。この状態の端末TOEコンポーネントは、「動作中のTOE範囲」から除外される。この概念を図1-2に示す。なお、同図では、分かりやすいイメージとするため、TOEの各要素を端末やサーバーと表現している。厳密に言えば、端末やサーバー内のTOEコンポーネントがTOEの要素に相当する。

本TOEでは、端末がその動作状態によってTOE範囲から除外されたり追加されたりするので、攻撃者が不正な端末をサーバーに接続させ、TOEの保護資産を侵害するかもしれないという懸念が生じる。そのような攻撃がTOEにとって好ましいものでないことは当然だが、TOE保護資産への直接の侵害につながる攻撃にはならない。その理由を以下に説明する。

本TOEによる電子マネー決済システムにおいて、端末の本質的な役割は、サーバーと消費者のFeliCa ICチップ間で実行される電子マネー引き落し処理の仲介である。取引に使用されるFeliCa ICチップは、サーバーとFeliCa ICチップ間の相互認証によって正当性が確認される。相互認証後は、サーバーとFeliCa ICチップ間で、エンド・ツー・エンドのセッションチャネルを通して決済処理が実行される。端末のTOEコンポーネントは、このエンド・ツー・エンド通信の内容に関与しない。つまり、端末はTOEのセキュリティ方針を実施する機能を含まないので、攻撃者が不正な端末をサーバーに接続しても、端末で実施すべきセキュリティ方針が侵害されることはない（セキュリティ方針の実施とは、STの6章に記載されるセキュリティ機能要件の実施と同義）。

この問題に関し、本TOEは、以下のような対策を施す。これらの対策は、攻撃者による不正な端末接続を厳格に排除することが目的ではなく、むしろ、不適切な端末で消費者が決済に失敗したり、サーバーに無駄な処理が発生したりすることの防止が主目的である。

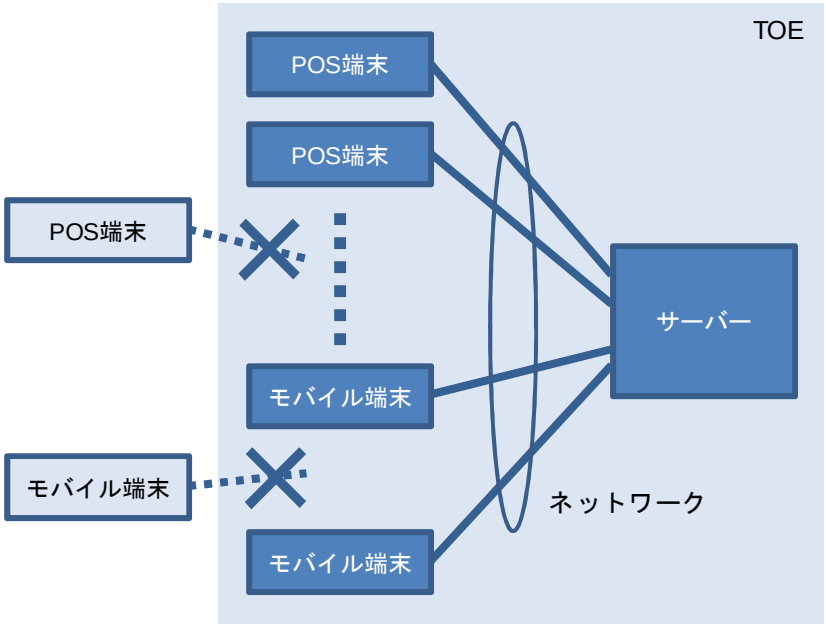

図 1-2 動作中の TOE 範囲から除外される端末

POS端末では、TOEコンポーネントは組み込まれた状態で加盟店に納品されるため、利用者自身が端末に組み込む必要はない。加盟店において、POS端末を初期設置する際に一度だけ、POS端末導入事業者が、端末TOEコンポーネントからIDに対応したパスフレーズを入力する。サーバーTOEコンポーネントは、これによって正当な権限を持つ者がPOS端末を設置したことを確認し、POS端末をTOEの一部に組み込む。なお、このIDとパスフレーズは、サーバー管理者によってThincacloud全体システムのTOE外の機能を用いて生成され、POS端末導入事業者へセキュアな方法で配付される。

モバイル端末(FeliCa内蔵)では、利用者自身がGoogle PlayからTOEコンポーネントをダウンロードし、端末に組み込む。モバイル端末(FeliCa非内蔵)では、TOEコンポーネントは組み込まれた状態でECサイトの加盟店に納品されるため、利用者自身が端末に組み込む必要はない。サーバーのTOEコンポーネントは、モバイル端末接続時に、正しいプログラム（TOEコンポーネント）が組み込まれていることを確認し、モバイル端末をTOEの一部に加える。

1.4.2. 電子マネー決済サービスの関係者

本TOEが適用される電子マネー決済サービスにおいて、その関係者・組織、それぞれの役割は、表1-3に示すものとなる。

表1-3 電子マネー決済サービスの関係者

名称	役割
決済サービスセンター	サーバーが置かれ、電子マネー決済の共通処理機能を受け持つ。本TOEを構成するコンポーネントのうち、サーバー機能部分が実装される。決済サービスセンターは、“TFペイメントサービス株式会社”が運営する。インターネットの監視と通信の暗号化を実現する。
サーバー管理者	決済サービスセンターのサーバー管理者。TOEを含むサーバー全体の管理・運営を担当する。
ブランド	電子マネーを発行・管理・運営する事業体。現状では、大手流通業者、鉄道事業者、電子マネー専門事業者などがそれぞれのブランド名による電子マネーを流通させている。
代理店	電子マネー決済サービスを提供する事業体。ブランドとアクワイアリング契約を行い、店舗（加盟店）にそのブランドによる電子マネー決済サービスを提供する。
加盟店	電子マネーによる商品販売を行う事業者。電子マネー決済サービスを提供する代理店と加盟店契約を行う。実店舗だけでなく、インターネット上のオンライン店舗(ECサイト)も含まれる。
電子マネー決済サービス利用者（消費者）	電子マネーを使用して加盟店で商品を購入する消費者。消費者は、電子マネー格納媒体であるFeliCa ICカード、またはおサイフケータイを保持する。
POS端末メーカー	POS端末及びPOS業務APを開発する端末メーカー。本TOEでは、端末メーカーと提携し、“TFペイメントサービス株式会社”がPOS業務APを開発する。
POS端末導入事業者	POS端末を加盟店に設置し、初期設定を実施する事業者。
非対面決済導入事業者	インターネット上のオンライン店舗(ECサイト)に決済サービスを導入する事業者。

1.4.3. TOE範囲

TOE範囲を、物理的側面、論理的側面の2面から定義する。

(1) 物理的範囲

TOEは、表1-1に示すコンポーネントの集合体である。Thincacloud決済サーバーには、サーバーソフトウェアにHP IC-Chip Access Server for FeliCa及びWebLogic 10.3が含まれ、ハードウェアとしてHSM(nShield F3 PCI Express 500 SEE Ready)が追加される。

TOEには、表1-4に示すガイダンスが含まれる。

表1-4 TOEガイダンスのリスト

対象者	ガイダンス
サーバー管理者	決済サービスセンターシステム管理ガイド Ver.1.0.1
加盟店(実店舗)	加盟店向け端末導入ガイド Ver.1.0.5 レジアプリケーション運用マニュアル Ver.1.04
加盟店(EC サイト)	非対面決済導入ガイド Ver.1.1.3※
モバイル端末(FeliCa 内蔵)の利用者	Thinca Payment App for おサイフケータイ ガイド Ver.1.0.0
POS 端末導入事業者	導入事業者向け端末導入ガイド Ver.1.1.1
非対面決済導入事業者	非対面決済導入ガイド Ver.1.1.3

※加盟店(ECサイト)は、モバイル端末の利用者に対して、ガイダンスを提供する。弊社は「非対面決済導入ガイド」において、そのガイダンスでの記載事項を規定する。

(2) 論理的範囲

TOEのセキュリティ機能範囲は、以下のリストに示すとおりである。

- FeliCa ICチップ識別・認証機能
  TSFは、消費者のFeliCa ICチップを識別・認証し、正当なFeliCa ICチップに限り、電子マネー決済を実行する。FeliCa ICチップの認証に暗号演算機能を使用する。
- 端末検証機能
  TSFは、POS端末、モバイル端末のTOEコンポーネントを新たにTOEの一部に組み込むとき、それらのTOEコンポーネントが正当なものであることを検証する。
- 決済データ保護機能
  消費者のFeliCa ICチップ (FeliCa ICチップはTOE外)とサーバーのTOEコンポーネント間で決済データを転送する際、サーバーのTOEコンポーネントは、転送される決済データの機密性・完全性を保護する。
- 監査機能
  TSFは、サーバーにおけるセキュリティ機能の動作を監視し、監査記録を生成する。監査証跡管理 (閲覧を含む) は、TOEのIT環境が受け持ち、TOEの機能ではない。POS端末、モバイル端末のTOEコンポーネント動作の監査は、TOE範囲に含めない。

2. 適合主張

2.1. CC適合主張

本STとTOEのCC適合主張は以下の通りである。

- 適合を主張するCC のバージョン
  パート1: 概説と一般モデル 2009年7月バージョン3.1 改訂第3版最終版 [翻訳第1.0版最終版] CCMB-2009-07-001
  パート2: セキュリティ機能コンポーネント 2009年7月バージョン3.1 改訂第3版最終版 [翻訳第1.0版最終版] CCMB-2009-07-002
  パート3: セキュリティ保証コンポーネント 2009年7月バージョン3.1 改訂第3版最終版 [翻訳第1.0版最終版] CCMB-2009-07-003
- 機能要件: パート2適合
- 保証要件: パート3適合

2.2. PP主張

本STは、他のPPへの適合を主張しない。

2.3. パッケージ主張

本STにおいて、TOEに対して適用する保証パッケージは、EAL1追加である。

追加する保証コンポーネントは、ASE_SPD.1、ASE_OBJ.2、ASE_REQ.2である。

2.4. 適合根拠

本STは、他のPPへの適合を主張しないので、適合根拠の記述を行わない。

3. セキュリティ課題定義

TOEに関わるセキュリティ課題定義を示す。脅威、組織のセキュリティ方針、前提条件について、それぞれ、[T.xxxx]、[P.xxxx]、[A.xxxx] の形式で識別名称を付与する。

3.1. 利用者と保護資産

TOEのセキュリティ課題を定義するにあたり、TOEの利用者及び保護資産を明らかにする。利用者及び保護資産は、脅威及び組織のセキュリティ方針を定義する文脈で用いられる。

(1) 利用者

運用環境で想定されるTOEの利用者は、以下のとおりである。これらの利用者は、TOEが提供する外部インタフェースを利用する。

- 加盟店におけるPOS端末操作者
- 消費者 (FeliCa ICチップを用いてPOS端末あるいはモバイル端末から決済サービスを利用する者。)

TOEを含む全体システムの利用者にはサーバー管理者が含まれる。しかしながら、TOE自身は、サーバー管理者に対する直接の外部インタフェースを提供しない。サーバー管理者は、サーバーのOSにログインし、OSからTOEが使用するTSFデータファイル (監査ログデータを含む) にアクセスすることで、間接的にTOEのセキュリティ機能を管理する。そのため、上述のTOE利用者には、サーバー管理者を含めていない。

(2) 保護資産

TOEの保護資産として、まず一次資産を定義する。一次資産とは、TOEの本来の用途のために保護すべき情報資産である。これは、TOEの所有者にとって価値がある情報資産と言える。一次資産は、本章の脅威あるいは組織のセキュリティ方針のいずれかの記述に反映される。

本TOEの一次資産は以下のものである。

- 電子マネー決済サービス提供者 (消費者にサービスを提供する者; 決済サービスセンター、ブランド、代理店、加盟店) が取得する利益
- 電子マネー決済データ (機密性と完全性の保護)

一方、TOEのセキュリティ機能（TSF）とTSFが使用するデータは、一次資産の保護のために必要となる。これらが侵害されればセキュリティ機能が危殆化し、一次資産の侵害につながる。従って、これらも保護対象であり、二次資産と呼ばれる。一次資産保護のために二次資産の保護が必要なのは自明であるので、二次資産は、必ずしも脅威や組織のセキュリティ方針で明示的に定義しない。しかしながら、TOE評価における脆弱性評定では、二次資産も重要な検討対象となる。

3.2. 脅威

本TOE対する脅威を示す。これらの脅威は、TOE、その運用環境、あるいは両者の組み合わせによって対抗されねばならない。

T.Illegal_IC_card 攻撃者が不正なIC媒体を使用し、POS端末あるいはモバイル端末からサーバーにアクセスして取引を行うことによって、電子マネー決済サービス提供者に損害を与えるかもしれない。

3.3. 組織のセキュリティ方針

TOEに関わる組織のセキュリティ方針を示す。これらの組織のセキュリティ方針は、TOE、その運用環境、あるいは両者の組み合わせによって実施されねばならない。

P.Legitimate_terminal POS端末及びモバイル端末をサーバーに接続する際、サーバーは、以下の手段によって端末のTOEコンポーネントが正しいものかどうかを検証し、検証に成功した場合に限り、端末のTOEコンポーネントをTOEの一部に組み込む。

- POS端末: 端末を最初にサーバーに接続する際、サーバーのTOEコンポーネントは、端末操作者にIDに対応したパスフレーズの入力を求め、それによって端末操作者が正当な権限を持つ者かどうかを検証する。検証に成功した場合、端末のTOEコンポーネントを正当なものとみなし、TOEの一部に組み込む。
- モバイル端末: 端末のTOEコンポーネントのプログラムバージョンを検証し、適正なバージョンであればそのTOEコンポーネントを正しいものとみなし、TOEの一部に組み込む。

P.Data_protection 消費者のFeliCa ICチップとTOE間でやりとりされる決済データの機密性・完全性を保護する。

P.Audit サーバー内セキュリティ機能動作を監査ログとして記録する。監査ログの対象事象は表3-1のとおり。この監査ログは、権限を持つ管理者だけが閲覧できる。

表3-1　監査対象事象

監査対象事象	監査対象アクション
FeliCa ICチップとの相互認証	相互認証の失敗
FeliCa ICチップとのセッション確立	セッション確立の失敗
電子マネー決済処理	正常実行及び失敗
POS端末識別・認証 (初期認証)	識別・認証の成功及び失敗
モバイル端末のTSF完全性検証	検証の失敗

3.4. 前提条件

TOEの運用環境に関わる前提条件を示す。これらの前提条件は、TOEの運用環境によって満たされねばならない。

A.Server サーバー及びその環境は、以下のように管理される。

- サーバーを、外部侵入が防止され、入退管理されたデータセンターに設置する。サーバーのすべての資源 (ハードウェア及びソフトウェア) に対し、権限を持つ者だけにアクセスを許可する。
- インターネットとサーバーの間にファイアーウォールを設置し、インターネットとサーバー間の不正なアクセスを抑止する。
- ECサイトとの通信は、データセンターに設置されたL/Bを用いて、セキュアなSSL通信を実施する。
- TOEプログラムとサーバーの資源を共有する他のプログラムを搭載する前に、それらがセキュアなものであることを検査してから搭載する。

- 運用開始後は、サーバー上に、TOEに有害な影響を与える他のプログラムが存在しない状態であることを常時監視する。
- サーバーを構成するプログラムに対し、定期的にセキュリティパッチの適用を検討し、実施する。

A.Server_admin サーバー管理者は、サーバー全体の管理・運営において、不正行為を働かないものとする。

A.EC_site ECサイトは、サーバーとセキュアなSSL通信を実施するように設定される。

A.POS_terminal POS端末は、盗難・紛失に遭わないよう管理される。

A.POS_terminal_setting POS端末導入事業者は、POS端末の設置・初期設定において、不正行為を働かないものとする。

4. セキュリティ対策方針

3章に示したセキュリティ課題に対し、TOE及びその環境におけるセキュリティ対策方針を示す。TOEによって対処するセキュリティ対策方針を4.1に、その環境によって対処するセキュリティ対策方針を4.2に記載する。これらセキュリティ対策方針がセキュリティ課題に対して適切であることの根拠を4.3に示す。

TOEのセキュリティ対策方針、運用環境のセキュリティ対策方針は、それぞれ、先頭に “O.”、“OE.” を付与した識別名で示される。

4.1. TOEのセキュリティ対策方針

セキュリティ課題として定義された脅威と組織のセキュリティ方針に関して、課題解決のためにTOEが対処すべきセキュリティ対策方針を示す。

O.Illegal_IC_card TSFは、消費者が使用するFeliCa ICチップが正規のものであることを検証した場合に限り、決済サービス実施を許可する。

O.Legitimate_terminal POS端末及びモバイル端末をサーバーに接続する際、TSFは、以下の手段によって端末のTOEコンポーネントが正しいものかどうかを検証し、検証に成功した場合に限り、端末のTOEコンポーネントをTOEの一部に組み込む。

- POS端末: 端末を最初にサーバーに接続する際、TSFは、端末操作者にIDに対応したパスフレーズの入力を求め、それによって端末操作者が正当な権限を持つ者かどうかを検証する。検証に成功した場合、端末のTOEコンポーネントを正当なものとみなし、TOEの一部に組み込む。
- モバイル端末: TSFは、端末のTOEコンポーネントのプログラムバージョンを検証し、適正なバージョンであればそのTOEコンポーネントを正しいものとみなし、TOEの一部に組み込む。

O.Data_protection 消費者のFeliCa ICチップに対する電子マネー決済処理において、決済データの機密性・完全性を保護する手段を設ける。

O.Audit サーバー内セキュリティ機能の動作を監査ログとして記録する。監査対象事象は、表3-1のとおり。

4.2. 運用環境のセキュリティ対策方針

セキュリティ課題として定義された脅威、組織のセキュリティ方針及び前提条件に関して、課題解決のためにTOEの運用環境が対処すべきセキュリティ対策方針を示す。

OE.Server サーバー管理者は、以下の管理を実施する。

- サーバーを、外部侵入が防止され、入退管理されたデータセンターに設置する。サーバーのすべての資源（ハードウェア及びソフトウェア）に対し、権限を持つ者だけにアクセスを許可する。
- インターネットとサーバーの間にファイアーウォールを設置し、インターネットとサーバー間の不正なアクセスを抑止する。
- ECサイトとの通信は、データセンターに設置されたL/Bを用いて、セキュアなSSL通信を実施する。
- TOEプログラムとサーバーの資源を共有する他のプログラムを搭載する前に、それらがセキュアなものであることを検査してから搭載する。
- 運用開始後は、サーバー上に、TOEに有害な影響を与える他のプログラムが存在しない状態であることを常時監視する。
- サーバーを構成するプログラムに対し、定期的にセキュリティパッチの適用を検討し、実施する。

OE.Server_admin 決済サービスセンターの責任者は、サーバー管理者に、サーバー全体の管理・運営において、不正行為を働かない者を割り当てる。

OE.EC_site 非対面決済導入事業者は、サーバーとセキュアなSSL通信を実施するように、ECサイトを設定する。

OE.POS_terminal 実店舗の加盟店は、POS端末が盗難・紛失に遭わないよう管理し、万が一遭った場合は、代理店の指示に従う。

OE.POS_terminal_setting　POS端末導入事業者は、POS端末の設置・初期設定において、不正行為を働かない者を割り当てる。

4.3. セキュリティ対策方針根拠

4.3では、上述のセキュリティ対策方針がセキュリティ課題定義の各項目に対して有効であることの根拠を示す。4.3.1では、各々のセキュリティ対策方針がいずれかのセキュリティ課題にさかのぼれること、4.3.2では、各々のセキュリティ課題が対応するセキュリティ対策方針によって有効に対処されることを説明する。

4.3.1. セキュリティ課題定義とセキュリティ対策方針の対応

セキュリティ課題定義とセキュリティ対策方針の対応を表4-1に示す。ここに示すとおり、すべてのセキュリティ対策方針は、一つ (以上) のセキュリティ課題定義の項目にさかのぼることができる。

表4-1　セキュリティ課題定義とセキュリティ対策方針の対応

セキュリティ課題定義 ＼ セキュリティ対策方針	O.Illegal_IC_card	O.Legitimate_terminal	O.Data_protection	O.Audit	OE.Server	OE.Server_admin	OE.EC_site	OE.POS_terminal	OE.POS_terminal_setting
T.Illegal_IC_card	x								
P.Legitimate_terminal		x							
P.Data_protection			x						
P.Audit				x	x				
A.Server					x				
A.Server_admin						x			
A.EC_site							x		
A.POS_terminal								x	
A.POS_terminal_setting									x

4.3.2. セキュリティ対策方針の根拠説明

TOE及び環境に対するセキュリティ対策方針によって、識別された脅威がすべて十分に対抗され、組織のセキュリティ方針が実施され、さらに、前提条件が適切に満たされることの根拠を示す。

T.Illegal_IC_card	TOEのセキュリティ対策方針O.Illegal_IC_cardによって、TSFは、正規のFeliCa ICチップによる決済だけを許可する。O.Illegal_IC_cardによって、脅威T.Illegal_IC_cardの脅威は十分に軽減される。
P.Legitimate_terminal	TOEのセキュリティ対策方針O.Legitimate_terminalは、組織のセキュリティ方針P.Legitimate_terminalと一対一に対応し、それを直接実施する内容になっている。
P.Data_protection	TOEのセキュリティ対策方針O.Data_protectionは、組織のセキュリティ方針P.Data_protectionと一対一に対応し、それを直接実施する内容になっている。
P.Audit	P.Auditに示された方針のうち、「監査ログの記録」に関わる事項は、TOEのセキュリティ対策方針O.Auditが対応する。一方、P.Auditの「監査ログの管理者による閲覧」に関わる事項は、TOEのIT環境（P.Auditの場合、下位のOSのセキュリティ機能及びその運用）に対応するセキュリティ対策方針OE.Serverによって満たされる。これらセキュリティ対策方針によって、P.Auditが実施される。
A.Server	環境のセキュリティ対策方針OE.Serverは、前提条件A.Serverと一対一に対応し、それを直接支持する内容になっている。
A.Server_admin	環境のセキュリティ対策方針OE.Server_adminは、前提条件A.Server_adminと一対一に対応し、それを直接支持する内容になっている。
A.EC_site	環境のセキュリティ対策方針OE.EC_siteは、前提条件A.EC_siteと一対一に対応し、それを直接支持する内容になっている。
A.POS_terminal	環境のセキュリティ対策方針OE.POS_terminalによって、POS端末が盗難・紛失に遭わないよう管理され、万が一遭った場合は、必要な措置が講じられる。これによって、前提条件A.POS_terminalが満たされる。

A.POS_terminal_setting	環境のセキュリティ対策方針OE.POS_terminal_settingは、前提条件A.POS_terminal_settingと一対一に対応し、それを直接支持する内容になっている。

5. 拡張コンポーネント定義

本STでは、拡張セキュリティ機能要件を定義しない。

6. セキュリティ要件

6.1. セキュリティ機能要件

本STで規定するSFRは、すべてCCパート2に含まれるコンポーネントを使用したものである。表6-1にSFRのリストを示す。

表6-1　　SFRリスト

章番号	コンポーネント名	
6.1.1.	FAU_GEN.1	監査データ生成
6.1.2.	FAU_GEN.2	利用者識別情報の関連付け
6.1.3.	FCS_COP.1	暗号操作
6.1.4.	FDP_IFC.1	サブセット情報フロー制御
6.1.5.	FDP_IFF.1	単純セキュリティ属性
6.1.6.	FDP_UCT.1	基本データ交換機密性
6.1.7.	FDP_UIT.1	データ交換完全性
6.1.8.	FIA_UAU.2(1)	アクション前の利用者認証（FeliCa IC チップ）
6.1.9.	FIA_UAU.2(2)	アクション前の利用者認証（POS 端末操作者）
6.1.10.	FIA_UAU.5	複数の認証メカニズム
6.1.11.	FIA_UID.2(1)	アクション前の利用者識別（FeliCa IC チップ）
6.1.12.	FIA_UID.2(2)	アクション前の利用者識別（POS 端末操作者）
6.1.13.	FPT_STM.1	高信頼タイムスタンプ
6.1.14.	FPT_TST.1	TSF テスト
6.1.15.	FTP_ITC.1	TSF 間高信頼チャネル

それぞれのセキュリティ機能コンポーネントに必要な操作を施すことによってSFRを規定する。操作内容は、各SFRにおいて、以下の表記方法で示される。

- 割付あるいは選択操作の箇所を[割付: *XXX(斜体)*]、[選択: *XXX(斜体)*]の形式で示す。
- 選択操作において、選択対象外の項目を~~抹消線~~ *(抹消線)* で示す。
- 詳細化操作において、詳細化部分を**斜体・ゴシック体**で示す。
- 繰り返し操作は、SFR識別名の後ろに、(1)、(2)のように番号を付して示す。

以下、本STで規定するSFRを示す。

6.1.1. FAU_GEN.1　　監査データ生成

下位階層:　なし

依存性:　FPT_STM.1 高信頼タイムスタンプ

FAU_GEN.1.1　**TSFは、以下の監査対象事象の監査記録を生成できなければならない:**

a)　**監査機能の起動と終了;**

b)　**監査の[選択: *~~最小、基本、詳細、指定なし~~: から1つのみ選択]レベルのすべての監査対象事象;及び**

c)　**[割付: *上記以外の個別に定義した表6-2の監査対象事象*]。**

表6-2　　監査対象事象

監査対象事象	監査対象アクション	*関連するSFR*
*FeliCa IC*チップとの相互認証	相互認証の失敗	*FIA_UAU.2(1)* *FIA_UID.2(1)*
*FeliCa IC*チップとのセッション確立	セッション確立の失敗	*FTP_ITC.1*
電子マネー決済処理	正常実行及び失敗	*FDP_IFF.1* *FDP_UCT.1* *FDP_UIT.1*
*POS*端末識別・認証 *(*初期認証*)*	識別・認証の成功及び失敗	*FIA_UAU.2(2)* *FIA_UID.2(2)*
モバイル端末の*TSF*完全性検証	検証の失敗	*FPT_TST.1*

FAU_GEN.1.2　**TSFは、各監査記録において少なくとも以下の情報を記録しなければならない:**

a)　**事象の日付・時刻、事象の種別、サブジェクト識別情報 (該当する場合) 、事象の結果 (成功または失敗) ;及び**

b)　**各監査事象種別に対して、PP/STの機能コンポーネントの監査対象事象の定義に基づいた、[割付: *なし*] 。**

6.1.2. FAU_GEN.2　　利用者識別情報の関連付け

下位階層:　なし

依存性: FAU_GEN.1 監査データ生成
FIA_UID.1識別のタイミング

FAU_GEN.2.1 **識別された利用者のアクションがもたらした監査事象に対し、TSF は、各監査対象事象を、その原因となった利用者の識別情報に関連付けられなければならない。**

6.1.3. FCS_COP.1 暗号操作

下位階層: なし

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データインポート、または
FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄

FCS_COP.1.1 **TSFは、[割付: *表6-3に示す標準のリスト*]に合致する、特定された暗号アルゴリズム[割付: *表6-3に示す暗号アルゴリズム*]と暗号鍵長[割付: *表6-3に示す暗号鍵長*]に従って、[割付: *表6-3に示す暗号操作*]を実行しなければならない。**

表6-3 暗号操作

標準	*暗号アルゴリズム*	*暗号鍵長*	*暗号操作*
SP800-67 "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher"	***TDEA (Triple Data Encryption Algorithm)***	***112 ビット***	***認証用乱数の暗号処理 (暗号化、復号)***

6.1.4. FDP_IFC.1 サブセット情報フロー制御

下位階層: なし

依存性: FDP_IFF.1 単純セキュリティ属性

FDP_IFC.1.1 **TSFは、[割付: *サーバーのTOEコンポーネントが消費者のFeliCa ICチップと交換する決済関連データ*]に対して[割付: *決済データ情報フロー制御SFP*]を実施しなければならない。**

6.1.5. FDP_IFF.1　　単純セキュリティ属性

下位階層:　なし

依存性:　FDP_IFC.1 サブセット情報フロー制御

FMT_MSA.3 静的属性初期化

FDP_IFF.1.1　**TSFは、以下のタイプのサブジェクト及び情報セキュリティ属性に基づいて、[割付:** ***決済データ情報フロー制御SFP*****]を実施しなければならない。: [割付:** ***サブジェクト:<サーバーのTOEコンポーネント及びFeliCa ICチップ>、情報:<サーバーのTOEコンポーネントとFeliCa ICチップ間で交換される決済関連データ>、セキュリティ属性:<FeliCa ICチップの認証の有無>*****]**

FDP_IFF.1.2　**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:** ***FeliCa ICチップの認証の有無が有の場合（FeliCa ICチップがFIA_UAU.5を満たす認証メカニズムによって認証されている場合）に、サーバーのTOEコンポーネントとFeliCa ICチップ間で、決済関連データを交換する*****]。**

FDP_IFF.1.3　**TSFは、[割付:** ***追加規則:サーバーのTOEコンポーネントとFeliCa ICチップ間の情報は、機密性及び完全性が保証された通信チャネルを経由すること*****]を実施しなければならない。**

FDP_IFF.1.4　**TSFは、以下の規則、[割付:** ***セキュリティ属性に基づく情報フローの明示的許可規則なし*****]に基づいて、情報フローを明示的に許可しなければならない。**

FDP_IFF.1.5　**TSFは、以下の規則、[割付:** ***セキュリティ属性に基づく情報フローの明示的拒否規則なし*****]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。**

6.1.6. FDP_UCT.1　　基本データ交換機密性

下位階層:　なし

依存性:　[FTP_ITC.1 TSF 間高信頼チャネル、または

FTP_TRP.1 高信頼パス]

[FDP_ACC.1 サブセットアクセス制御、または

FDP_IFC.1 サブセット情報フロー制御]

FDP_UCT.1.1　**TSFは、不当な暴露から保護した形で利用者データの[選択:** ***送信、受信*****]を行うために、[割付:** ***決済データ情報フロー制御SFP*****]を実施しなければならない。**

6.1.7. FDP_UIT.1　　データ交換完全性

下位階層:　なし

依存性: [FDP_ACC.1 サブセットアクセス制御、または
FDP_IFC.1 サブセット情報フロー制御]
[FTP_ITC.1 TSF 間高信頼チャネル、または
FTP_TRP.1 高信頼パス]

FDP_UIT.1.1 **TSFは、利用者データを[選択: *改変、~~消去~~、~~挿入~~、~~リプレイ~~*]誤りから保護した形で[選択: *送信*、*受信*]を行うために、[割付: *決済データ情報フロー制御SFP*]を実施しなければならない。**

FDP_UIT.1.2 **TSFは、利用者データ受信において、[選択: *改変、~~消去~~、~~挿入~~、~~リプレイ~~*]が生じたかどうかを判定できなければならない。**

6.1.8. FIA_UAU.2(1) アクション前の利用者認証（FeliCa ICチップ）

下位階層: FIA_UAU.1 認証のタイミング
依存性: FIA_UID.1 識別のタイミング

FIA_UAU.2.1 **TSFは、その利用者*（FeliCa ICチップ）*を代行する他のTSF仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。**

6.1.9. FIA_UAU.2(2) アクション前の利用者認証（POS端末操作者）

下位階層: FIA_UAU.1 認証のタイミング
依存性: FIA_UID.1 識別のタイミング

FIA_UAU.2.1 **TSFは、その利用者*（POS端末操作者）*を代行する他のTSF仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。**

6.1.10. FIA_UAU.5 複数の認証メカニズム

下位階層: なし
依存性: なし

FIA_UAU.5.1 **TSFは、利用者認証をサポートするため、[割付: *表6-4に示す複数の認証メカニズム*]を提供しなければならない。**

FIA_UAU.5.2 **TSFは、[割付: *表6-4に示す複数の認証メカニズムがどのように認証を提供するかを記述する規則*]に従って、利用者が主張する識別情報を認証しなければならない。**

表6-4　　認証メカニズム

名称	*検証メカニズム*	*認証の規則*
相互認証	*独自の認証アルゴリズム: TOEとFeliCa ICチップ双方が生成する乱数にTDEA暗号演算を適用する3ウェイハンドシェーク方式に基づく(非公開)。*	*すべてのFeliCa ICチップに適用する。*
パスフレーズ	*POS端末操作者が入力するID、パスフレーズがあらかじめ登録されたデータと一致することを検証する。*	*POS端末を最初にサーバーに接続する際に一度だけ適用する。*

6.1.11. FIA_UID.2(1)　アクション前の利用者識別（FeliCa ICチップ）

下位階層:　FIA_UID.1 識別のタイミング

依存性:　なし

FIA_UID.2.1　**TSFは、その利用者*（FeliCa ICチップ）*を代行する他のTSF仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。**

6.1.12. FIA_UID.2(2)　アクション前の利用者識別（POS端末操作者）

下位階層:　FIA_UID.1 識別のタイミング

依存性:　なし

FIA_UID.2.1　**TSFは、その利用者*（POS端末操作者）*を代行する他のTSF仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。**

6.1.13. FPT_STM.1　高信頼タイムスタンプ

下位階層:　なし

依存性:　なし

FPT_STM.1.1　**TSFは、高信頼タイムスタンプを提供できなければならない。**

6.1.14. FPT_TST.1　　TSFテスト

下位階層:　なし

依存性:　なし

FPT_TST.1.1　**TSFは、[選択: *~~TSF、~~[割付: モバイル端末のTSF部分]*]の正常動作を実証するために、[選択: *~~初期立ち上げ中、通常運用中定期的に、許可利用者の要求時に、条件~~[割付: モバイル端末によるサーバー接続要求の条件]* 下で]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、[選択: *[割付: モバイル端末のTOEコンポーネントの名称及びバージョン情報]、~~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、[選択: *[割付: モバイル端末のTSF部分]、~~TSF~~*]の完全性を検証する能力を提供しなければならない。**

6.1.15. FTP_ITC.1　　TSF間高信頼チャネル

下位階層:　なし

依存性:　なし

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

FTP_ITC.1.2　**TSFは、[選択: *TSF、~~他の高信頼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。**

FTP_ITC.1.3　**TSFは、[割付: *FeliCa ICチップ及びサーバーTOEコンポーネント間の電子マネー決済データ転送*]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。**

6.2. セキュリティ保証要件

本TOEに適用するセキュリティ保証要件は、表6-5に示す保証コンポーネントで定義される。これらは、すべて、CC パート3に含まれる。

表6-5に示すすべてのコンポーネントにおいて、本STでは、操作を適用していない。

表6-5　保証コンポーネント

保証クラス	保証コンポーネント
セキュリティターゲット評価	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2*
	ASE_REQ.2*
	ASE_SPD.1*
	ASE_TSS.1
開発	ADV_FSP.1
ガイダンス文書	AGD_OPE.1
	AGD_PRE.1
ライフサイクルサポート	ALC_CMC.1
	ALC_CMS.1
テスト	ATE_IND.1
脆弱性評定	AVA_VAN.1

* 追加の保証コンポーネント

6.3. セキュリティ要件根拠

6.3.1. セキュリティ機能要件根拠

6.3.1では、定義されたSFRがTOEのセキュリティ対策方針を適切に達成することの根拠を示す。6.3.1.1では、各々のSFRがいずれかのTOEのセキュリティ対策方針にさかのぼれること、6.3.1.2では、各々のTOEのセキュリティ対策方針が対応する有効なSFRによって適切に満たされることを説明する。

6.3.1.1　セキュリティ対策方針とセキュリティ機能要件の対応

TOEのセキュリティ対策方針に対応するSFRを表6-6に示す。この表は、すべてのSFRが少なくとも一つのTOEのセキュリティ対策方針にさかのぼれることの根拠となる。

表6-6　　TOEセキュリティ対策方針とSFRの対応

TOE セキュリティ対策方針 / SFR	FAU_GEN.1	FAU_GEN.2	FCS_COP.1	FDP_IFC.1	FDP_IFF.1	FDP_UCT.1	FDP_UIT.1	FIA_UAU.2(1)	FIA_UAU.2(2)	FIA_UAU.5	FIA_UID.2(1)	FIA_UID.2(2)	FPT_STM.1	FPT_TST.1	FTP_ITC.1
O.Illegal_IC_card			x					x		x	x				
O.Legitimate_terminal									x	x		x		x	
O.Data_protection				x	x	x	x								x
O.Audit	x	x											x		

6.3.1.2　対応関係の根拠説明

O.Illegal_IC_card　識別・認証の要件FIA_UAU.2(1)/FIA_UID.2(1)によって、消費者のIC媒体が、FeliCa仕様に準拠し、該当するブランドに対応した適正なものであることを検証するまで、TSFを介したサービスを提供しないことを規定する。この認証に使用するメカニズムは、FCS_COP.1、FIA_UAU.5で規定される。これらSFRによって、O.Illegal_IC_cardが達成される。

O.Legitimate_terminal　POS端末の端末操作者に対する識別・認証をFIA_UAU.2(2)/FIA_UID.2(2)で規定する。認証のメカニズムは、FIA_UAU.5で規定される。モバイル端末のTSF及びTSFデータの完全性確認は、FPT_TST.1で規定する自己テストによる。この自己テストは、TOE利用者にサービスを適切に提供するため、モバイル端末に正しいTOEコンポーネントが搭載されていることの確認を主目的としたものである。本SFRが規定するTSFデータの完全性確認は、TOEの識別情報である名称、及びバージョン情報が対象である。TSFの完全性に関しては、上記TSFデータの確認成功を以って、TSFの完全性が検証できたとみなす。これらの識別・認証または完全性確認に成功した場合に限り、端末のTOEコンポーネントはTOEの一部に組み込まれる。これらSFRによって、O.Legitimate_terminalが達成される。

O.Data_protection　FeliCa ICチップとサーバーのTOEコンポーネント間で、決済データの転送にセキュアなエンド・ツー・エンド通信チャネルを使用する要件をFTP_ITC.1

で規定する。転送するユーザデータの機密性・完全性保護をFDP_UCT.1、FDP_UIT.1のそれぞれで規定する。データの完全性に異常が生じた場合、FDP_IFC.1/FDP_IFF.1によってFeliCa ICチップとサーバー間のデータフローを禁止することで、完全性保護を実現する。FeliCa ICチップから送信されるデータの通信路で改ざんが行われると、サーバー側で完全性検証がNGとなり、上述のFDP_IFF.1によってデータフローが禁止される。これらSFRの組み合わせで、FeliCa ICチップとサーバー間の機密性・完全性が保護され、O.Data_protectionが達成される。

O.Audit FAU_GEN.1、FAU_GEN.2によって、サーバー内セキュリティ機能の動作を監査ログとして生成する要件が規定される。監査データへのタイムスタンプはFPT_STM.1で規定される。これらSFRによって、O.Auditが達成される。

6.3.1.3 セキュリティ機能要件の依存性

各SFRに規定された依存性とその対応状況を表6-7に示す。

表6-7において、「依存性の要求」欄にはSFRに規定された依存性を示す。「依存性の対応」欄には、規定された依存性がST中のどのSFRによって満たされるかを示す。FCS_COP.1、FDP_IFF.1を除き、要求されるすべての依存性が満たされる。依存性を満たさない二つのSFRについては、依存性を満たさないことの正当化理由を表中に記載する。

表6-7 SFRの依存性

SFR	依存性の要求	依存性への対応
FAU_GEN.1	FPT_STM.1	FPT_STM.1が対応し、依存性が満たされる。
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1及びFIA_UID.2(1)（FIA_UID.1の上位SFR）が対応し、依存性が満たされる。
FCS_COP.1	FDP_ITC.1または FDP_ITC.2または FCS_CKM.1 FCS_CKM.4	相互認証用暗号鍵は、TOE外でブランドごとに用意されるため、FCS_CKM.1で規定される暗号鍵生成の要件は不要である。 サーバーは物理的に保護されており、相互認証用暗号鍵は暗号化されてHSMへ格納されるため、保護する必要はなく、FDP_ITC.1またはFDP_ITC.2で規定されるアクセス制御または情報フロー制御を伴ったインポート要件は不要である。 相互認証用暗号鍵は、TOE稼働中、削除されることはないため、FCS_CKM.4で規定される暗号鍵破棄の要件は不要である。 以上より、所定の依存性を満たす必要はない。
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1が対応し、依存性が満たされる。
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1が対応し、依存性が満たされる。 FMT_MSA.3は、セキュリティ属性のデフォルト値と管理方法を規定する。対応する情報フロー制御のセキュリティ属性は、FeliCa ICチップへの認証結

		果から自動的に決定される。そのため、セキュリティ属性に対するデフォルト値適用、あるいは管理者による管理が不要となり、FMT_MSA.3の依存性を満たす必要はない。
FDP_UCT.1	FTP_ITC.1または FTP_TRP.1 FDP_ACC.1または FDP_IFC.1	FTP_ITC.1及びFDP_IFC.1が対応し、依存性が満たされる。
FDP_UIT.1	FDP_ACC.1または FDP_IFC.1 FTP_ITC.1または FTP_TRP.1	FTP_ITC.1及びFDP_IFC.1が対応し、依存性が満たされる。
FIA_UAU.2(1)	FIA_UID.1	FIA_UID.2(1)（FIA_UID.1の上位SFR）が対応し、依存性が満たされる。
FIA_UAU.2(2)	FIA_UID.1	FIA_UID.2(2)（FIA_UID.1の上位SFR）が対応し、依存性が満たされる。
FIA_UAU.5	なし	–
FIA_UID.2(1)	なし	–
FIA_UID.2(2)	なし	–
FPT_STM.1	なし	–
FPT_TST.1	なし	–
FTP_ITC.1	なし	–

6.3.2. セキュリティ保証要件根拠

保証要件としてEAL1+（追加コンポーネント: ASE_SPD.1/ASE_OBJ.2/ASE_REQ.2）を選択した根拠を説明する。

TOEは、中央に置かれる一つのサーバーと、インターネット経由で接続される多数の端末からなる電子マネー決済システムにおいて、それぞれの装置に搭載される電子マネー決済のためのプログラムである。

電子マネー決済では、消費者のFeliCa ICチップに格納された電子マネーがサーバーによって引き落とされる。TOEのセキュリティ機能は、この引き落とし処理をセキュアに実行するためのものである。

TOEの構成要素である端末やサーバーはTOEの識別・認証機能によって不正な利用者のアクセスを防止する。これによってTOE内部に保護資産を攻撃するプロセス（信頼できないプロセス）が存在しなくなり、TOE内部での決済データへの攻撃リスクは小さい。さらに、決済データはFeliCa ICチップ内部で、FeliCa仕様により機密性及び完全性が保護されるため、たとえ端末内部やインターネット上で予期しない攻撃があっても、TOEの保護資産が侵害されるリスクは小さい。FeliCa ICチップ自体は、ICカードとして十分なセキュリティ機能を備えており、上記のようにFeliCaとサーバー間のデータはエンド・ツー・エンドで保護されるので、このデータのセキュリティが侵害される恐れは十分に小さいと考えられる。

以上のような理由で、TOEのセキュリティ機能は、外部利用者に対する識別・認証など、限られた攻撃に対する対処が中心となる。このため、保証要件パッケージとして、EAL1+を設定する。追加する保証要件は、ASE_SPD.1、ASE_OBJ.2、ASE_REQ.2である。これらは、低保証STを使用せず、TOEに対するセキュリティ課題を明示的に定義することで、SFRの妥当性を適切に評価するための施策である。

7. TOE要約仕様

7.1. セキュリティ機能要件実現手段の概要

TOEにおけるセキュリティ機能要件実現手段の概要を説明する。6.1章に記載した各々のSFRごとに実現手段を示す。

7.1.1. FAU_GEN.1/FAU_GEN.2

監査の対象は、サーバーのTOEコンポーネント上で動作するセキュリティ機能動作である。FAU_GEN.1に示す監査対象事象をログデータとして生成し、TOE下位のOSに渡す。以降のログデータは、TOE範囲外であるOS上で、サーバーの他のプログラムのログデータと共に集中管理される。FAU_GEN.1.2のa) では、該当する監査対象事象にサブジェクト識別情報を含めることを要求している。しかしながら、サーバーTOEコンポーネント内では、利用者を代行するサブジェクトは存在しない。本TOEでサブジェクトとして動作するアクティブなプロセスは、サーバーのTOEコンポーネント全体が相当する。

監査対象事象のうち、利用者の識別情報と関連付けられるのは、FeliCa ICチップ及びPOS端末に関する事象である。TOEは、FeliCa ICチップ及びPOS端末の識別情報をログデータの一部として記録する(FAU_GEN.2)。

7.1.2. FDP_IFC.1/FDP_IFF.1/FDP_UCT.1/FDP_UIT.1/FTP_ITC.1

POS端末、モバイル端末のいずれの場合でも、TOEと消費者のFeliCa ICチップ間での最終決済処理（電子マネー引き落とし）は、FeliCaとサーバーのTOEコンポーネント間にエンド・ツー・エンドで設定されるセキュアな通信チャネルを介して行われる。以下のi)及び7.1.4.に記載の相互認証により、お互いを確認する（FTP_ITC.1)。

セキュアな通信チャネルの使用は、以下のステップで行われる。

i) FeliCa ICチップとサーバーTOEコンポーネントの相互認証

ii) FeliCa ICチップとサーバーTOEコンポーネント間のセッション確立

iii) 電子マネー引き落とし

iv) セッション終了

FeliCa ICチップの認証成功によって、FDP_IFC.1/FDP_IFF.1で規定する情報フローのセキュリティ属性に関わる条件が満たされ、FeliCa ICチップとサーバーのTOEコンポーネント間にセッションが確立されて電子マネーが引き落とされる。FDP_IFF.1は、さらに、決済処理に、セキュアな通信チャネルを経由する要件を含む。

セキュアな通信チャネルでは、転送する決済関連情報の機密性（FDP_UCT.1）、完全性（FDP_UIT.1）が保護される。機密性保護は、FeliCaとサーバーのTOEコンポーネントの双方で、FeliCa仕様による転送情報の暗号化によって実現する。完全性保護は、FeliCa仕様による転送情報への完全性検証データ付与で

行う。完全性検証データを付与した情報全体をブロック暗号化するので、完全性検証データの正常性を保ったまま転送情報を改ざんすることはできない。

7.1.3. FIA_UAU.5

FIA_UAU.5は、本TOEに要求される2つの認証メカニズムを規定する。これらの認証メカニズムは、要件に記された認証の規則に従い、それぞれの認証対象の種別によって適用される。認証メカニズムの実現手段は、7.1.4.と7.1.5.で説明される。

7.1.4. FCS_COP.1/ FIA_UAU.2(1)/ FIA_UID.2(1)

TOEは、電子マネーによる決済の対象となるFeliCa ICチップと相互認証を行う。相互認証によってFeliCa ICチップの真正性を確認できた場合に限り、決済処理を実行する。TOEによるFeliCa ICチップの真正性確認 (識別・認証) は、以下のような形で実現される。

TOEとFeliCa ICチップは、それぞれが相互認証用暗号鍵を持ち、独自の認証アルゴリズムによる相互認証を行う。この認証アルゴリズムは、TOEとFeliCa ICチップ双方が生成する乱数にTDEA暗号演算を適用する3ウェイハンドシェーク方式に基づくもので、詳細仕様は非公開である。TDEA暗号アルゴリズムはFCS_COP.1で定義され、HSMによって暗号演算メカニズムを実現する。共通鍵はブランドごとにあらかじめ定められ、FeliCa ICチップとサーバー (TOE外の暗号DB) に事前に設定される。

7.1.5. FIA_UAU.2(2)/FIA_UID.2(2)

FIA_UAU.2(2)/FIA_UID.2(2)は、POS端末操作者の識別・認証に適用する。これは、POS端末の初期設置時に、正当な権限を持つ者に設定操作を行わせるための要件である。運用上のセキュアな手段によって正当な権限を持つ者にあらかじめIDに対応したパスフレーズを知らせ、POS端末の初期設置時にこのデータをPOS端末から入力し、サーバーTOEコンポーネントによる識別・認証を受ける。

7.1.6. FPT_STM.1

サーバーのTOEコンポーネントは、下位のOSから時刻情報を入手し、生成したログデータに付加する。

7.1.7. FPT_TST.1

本SFRは、モバイル端末が電子マネー決済サービスを受けるとき、モバイル端末のTOEコンポーネントとして、正しいプログラムが搭載されていることを確認する要件である。正しいプログラムであることの確認手段として、サーバーTOEコンポーネントは、プログラムの属性情報であるプログラムIDとバージョン情報が正しいものであるかどうかを検査する。TSFの完全性に関しては、上記TSFデータの検査成功を以って、TSFの完全性が検証できたとみなす。

検査に成功した場合、モバイル端末は後続の画面を表示する。検査に失敗した場合、モバイル端末はエラーを表示する。モバイル端末利用者はそれらの表示によって、検査の成否を確認できる。加えて、サーバーTOEコンポーネントは、モバイル端末のTSF完全性検証失敗の監査ログを生成する。サーバー管理者は監査ログの確認により検査の失敗を検知できる。

8. 用語

本STで使用される用語・略語を解説する。

8.1. CC関連

PP	Protection Profile: TOEの調達者あるいは開発に関わる業界などが共通仕様として定めるセキュリティ要件定義書。
CC	Common Criteria; IT装置のセキュリティ評価基準。CCと同一の内容がISO/IEC 15408規格として制定されている。
ST	Security Target: 個々のIT製品に対するセキュリティ要件定義書。
TOE	Target of Evaluation; 評価対象。セキュリティ評価の対象となる範囲をあいまいさなく示すことがきわめて重要であり、PP/STによって厳密に定義される。あるIT製品の全体がTOEに該当することもあり、IT製品の一部をTOEと定義することもある。
TSF	TOE security functionality; TOEセキュリティ機能。TOEの機能のうち、SFRを正しく実施するうえで。そのふるまいを信頼できる部分。TOEを構成するソフトウェア/ハードウェア/ファームウェアによる複合機能。
SFR	Security functional requirement; セキュリティ機能要件。TOEに要求されるセキュリティ機能の定義。CCパート2に書かれたセキュリティ機能コンポーネントを使用し、STの第6章に要件定義を書く。CCパート2に適切な機能コンポーネントがない場合、ST作成者があらたな機能コンポーネントを作成できる（拡張コンポーネント）。

8.2. TOE関連

FeliCa	ソニー株式会社が開発したICカード向け非接触通信技術方式の名称。国内では、鉄道の自動改札機、ビル入館ゲート、電子マネーカードなど広い分野で使用されている。FeliCaに基づくICチップは、ICカードに実装されるほか、おサイフケータイなど、モバイル端末への実装例がある。FeliCa以外の非接

	触通信技術には、ISO/IEC 14443 TYPE A (MYFARE) 、ISO/IEC 14443 TYPE B、ISO/IEC 15693などがあるが、FeliCaとの互換性はない。ISO/IEC 18092 として規格化されたNFC (Near Field Communication) は、これらの上位互換規格である。
HSM	Hardware Security Module。秘密鍵などの秘密情報を生成及び管理するハードウェア機器。
L/B	Load Balancer。外部ネットワークからの要求を一元的に管理し、同等の機能を持つ複数のサーバーに要求を転送する装置。TOEの運用環境では、SSLオフロード機能を有したものを採用し、サーバーにおけるSSLのエンコード、デコードにかかる負荷を解消している。
POS端末	加盟店に置かれ、POSに使用される端末。“POS”は、POS system (Point of sale system) のことで、”販売時点情報管理”と訳される。商取引が行われる場所（レジがあるところ）で販売実績情報を収集し、コンピュータによる集中管理につなげる。本STにおけるPOS端末は、FeliCaによる電子マネー決済機能を備える。
不正なIC媒体	本STにおいて、正規のFeliCa ICチップとは、FeliCa仕様に対応し、決済時に消費者が選択したブランドの電子マネー決済APを搭載したIC媒体のことを指す。そうでないものは、不正なIC媒体である。
モバイル端末	通信機能を持つ携帯情報端末。厳密な定義はなく、携帯電話（フィーチャーフォン）、スマートフォンなどのほか、広義には、通信デバイスと組み合わせたPCも含まれる。本STにおけるモバイル端末は、Android OSで動作するスマートフォンが該当する。