認 証 報 告 書

独立行政法人情報処理推進機構
理事長　藤江　一正　原紙押印済

評価対象

申請受付日（受付番号）	平成24年9月4日 (IT認証2422)
認証番号	C0399
認証申請者	TFペイメントサービス株式会社
TOEの名称	クラウド型決済システム Thincacloud コアモジュール
TOEのバージョン	Thincacloud決済サーバー 1.0.0 Thincacloud決済クライアント Windows CE版 1.0.0 Thinca Payment App for おサイフケータイ 1.0.0 Thinca Payment App for NFC 1.0.0
PP適合	なし
適合する保証パッケージ	EAL1及び追加の保証コンポーネントASE_SPD.1、ASE_OBJ.2、ASE_REQ.2
開発者	TFペイメントサービス株式会社
評価機関の名称	株式会社 ECSEC Laboratory 評価センター

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

平成25年8月1日

技術本部
セキュリティセンター 情報セキュリティ認証室
技術管理者　山里　拓己

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

① 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 バージョン3.1 リリース３
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 リリース３

評価結果：合格

「クラウド型決済システム Thincacloud コアモジュール」は、独立行政法人情報処理推進機構

が定めるITセキュリティ認証等に関する要求事項に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

この認証報告書は、TF ペイメントサービス株式会社が開発した「クラウド型決済システム Thincacloud コアモジュール バージョン Thincacloud 決済サーバー 1.0.0 Thincacloud 決済クライアント Windows CE 版 1.0.0 Thinca Payment App for おサイフケータイ 1.0.0 Thinca Payment App for NFC 1.0.0」(以下「本 TOE」という。) について株式会社 ECSEC Laboratory 評価センター (以下「評価機関」という。) が平成 25 年 7 月 18 日に完了した IT セキュリティ評価に対し、その内容の認証結果を申請者である TF ペイメントサービス株式会社に報告するとともに、本 TOE に関心を持つ調達者に対しセキュリティ情報を提供するものである。

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

本認証報告書は、本 TOE の提供する機能を使用して一般消費者にサービスを提供する事業者を読者と想定しており、運用環境や用語なども決済サービスを提供する事業者の一般的な理解を前提としている。本認証報告書は、本 TOE が適合する保証要件に基づいた認証結果を示すものであり、個別の IT 製品そのものを保証するものではないことに留意されたい。

1.1 評価対象製品概要

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

なお、本書では組合せ等で長くなる固有名詞を簡略表現するために下記呼称を使う。

表 1-1 本書における固有名詞の呼称

No	本書の呼称	ST 等に記される固有名詞
1	TOE	クラウド型決済システム Thincacloud コアモジュール バージョン Thincacloud 決済サーバー 1.0.0 Thincacloud 決済クライアント Windows CE 版 1.0.0 Thinca Payment App for おサイフケータイ 1.0.0 Thinca Payment App for NFC 1.0.0
2	サーバ TOE	クラウド型決済システム Thincacloud コアモジュール バージョン Thincacloud 決済サーバー 1.0.0

3	POS 端末 TOE	クラウド型決済システム Thincacloud コアモジュール バージョン Thincacloud 決済クライアント Windows CE 版 1.0.0
4	おサイフケータイ TOE	クラウド型決済システム Thincacloud コアモジュール バージョン Thinca Payment App for おサイフケータイ 1.0.0
5	NFC 端末 TOE	クラウド型決済システム Thincacloud コアモジュール バージョン Thinca Payment App for NFC 1.0.0
6	モバイル端末 TOE	No.4 と No.5 を区別しない場合
7	端末 TOE	No.3～No.5 を区別しない場合

1.1.1 保証パッケージ

本 TOE の保証パッケージは、EAL1 及び追加の保証コンポーネント ASE_SPD.1+ASE_OBJ.2+ASE_REQ.2 である。

1.1.2 TOEとセキュリティ機能性

本 TOE は、店舗毎に個別に構築される FeliCa IC チップを対象にしたプリペイド型電子マネーの決済処理機能をクラウド・サービスとして提供可能にするシステムのコアモジュールである。共通プラットフォーム上に構築される複数の業務アプリケーションにより、ブランド毎に異なる決済サービスを提供可能にするシステムの内、共通プラットフォームと一つの業務アプリケーションが TOE 範囲であり、nanaco 向けの決済処理が提供される。

サーバ TOE は開発者が運用し、対面販売を行う実店舗が使う POS 端末 TOE、非対面販売を行う EC サイトが EC サイトの利用者向けに配付可能とする NFC 端末 TOE、EC サイト利用のために消費者の手持ちのおサイフケータイにインストールして使うおサイフケータイ TOE がある。

POS 端末 TOE または、EC サイトがサーバ TOE に決済開始を要求すると、サーバ TOE は端末 TOE を介すことで端末にかざした nanaco カード等の FeliCa IC チップに対して、次の様な機能性により確実な電子マネー決済を可能とする。

- サーバ TOE に接続する端末 TOE が正当なものであることを検証する機能
- 電子マネー決済に使用される FeliCa IC チップが正当なものであることを検証する機能
- FeliCa IC チップに転送する電子マネー決済データを暴露・改ざんから保護する機能

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について保証パッケージの範囲で評価が行われた。本 TOE が想定する脅威及び前提については次項のとおりである。

1.1.2.1 脅威とセキュリティ対策方針

本TOEは､以下のとおりのセキュリティ機能によりそれぞれの脅威に対抗する。

事業者が発行したFeliCa ICチップではない不正なIC媒体を使用した決済が行われることにより、事業者が取得する利益に損害を与えるかもしれない脅威がある。

これらの脅威に対抗するために、本TOE はFeliCa ICチップの識別・認証機能を提供する。

さらに、事業者にとって脅威とはならないが、端末TOEの設定やバージョン違いによる誤動作を排除するために端末接続時に端末の正当性を検証する機能、暗号化によりサーバTOEとFeliCa ICチップ間で転送される電子マネー決済データの機密性と完全性を保護する決済データ保護機能、および、セキュリティ機能の動作を記録する監査ログ生成機能を開発者は想定し、組織のセキュリティ方針として提供する。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような構成及び前提で運用することを想定する。

サーバTOEは、入退室管理及び、ファイアウォール等によりインターネットからの不正アクセスに対抗できるよう構築及び、管理された環境で開発者が運用することを想定している。

実店舗としてTOEを利用するためには、POS端末TOEの導入が必要であり、盗難、紛失に遭わないよう管理されることを想定している。

ECサイトとしてTOEを利用するためには、TOEのガイダンスに従いTOE利用のためのロジックをECサイトに組み込む必要がある。また、ECサイトがNFC端末TOEを消費者に提供する場合は、NFC端末TOEを搭載したNFC端末を開発者から調達する必要がある。

1.1.3 免責事項

本TOEは、以下の脅威に対しては対抗していない。

電子マネー決済サービスとして本TOEが想定していない下記脅威は本評価の対象外となり保証されない。

- サービス不能攻撃によるサーバTOEの停止等。
- モバイル端末の所有者に無断でTOEを使い決済される脅威。
- FeliCa ICチップの所有者に無断でTOEを使い決済される脅威

TOE範囲外のDB、運用ツール、ECサイト、FeliCa ICチップ等で管理される暗号鍵、ID、パスワード、個人情報、電子マネー等の流出や悪用に関する脅威は本評価の対象外となり保証されない。

TOE のセキュリティ機能として主張されないモバイル端末 TOE 利用者の識別認証は本評価で保証されない。

Android アプリであるモバイル端末 TOE がアプリを改ざんされる等で、不正決済、悪意のサイトへの誘導、個人情報等の流出・悪用、踏み台になり他システムへ攻撃する等の脅威は本評価の対象外となり保証されない。

1.2 評価の実施

認証機関が運営する IT セキュリティ評価・認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[3]に規定された内容に従い、評価機関によって本 TOE に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、平成 25 年 7 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]、所見報告書、及び関連する評価証拠資料を検証し、本 TOE の評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。認証機関が指摘した問題点は、すべて解決され、かつ、TOE の評価が CC（[4][5][6]または[7][8][9]）及び CEM（[10][11]のいずれか）に照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 TOE識別

本 TOE は、以下のとおり識別される。

TOE名称：	クラウド型決済システム Thincacloud コアモジュール
バージョン：	Thincacloud決済サーバー 1.0.0
	Thincacloud決済クライアント Windows CE版 1.0.0
	Thinca Payment App for おサイフケータイ 1.0.0
	Thinca Payment App for NFC 1.0.0
開発者：	TFペイメントサービス株式会社

製品が評価･認証を受けた本 TOE であることを、利用者は以下の方法によって確認することができる。

利用者毎に用意されたガイダンスに記載された手順により TOE の構成ファイルの名称から確認することができる。

また、利用者は運用者が公開する Web ページより、サーバ TOE の現在稼働バージョンを知る手順もガイダンスに含まれる。

3 セキュリティ方針

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

3.1 セキュリティ機能方針

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

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

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

表3-1 想定する脅威

識別子	脅威
T.Illegal_IC_card	攻撃者が電子マネー事業者が発行したものでない不正なIC媒体を使用し、TOEを使った電子マネー決済が行われることで、事業者が取得する利益に損害を与えるかもしれない。

3.1.1.2 脅威に対するセキュリティ機能方針

本 TOE は、表 3-1 に示す脅威に対し、以下のセキュリティ機能方針で対抗する。

(1) 脅威「T.Illegal_IC_card」への対抗

この脅威は、不正な IC 媒体で決済される等の金銭に関する脅威である。
この脅威に対して TOE は、下記機能性で脅威に対抗する。

・IT 環境で管理するブランド毎の暗号鍵を使い、TDEA 暗号アルゴリズムによる相互認証を行い、相互認証に成功した FeliCa IC チップのみに電子マネー決済データの転送を許可する。

これにより、不正な IC 媒体を使った電子マネー決済を防止できる。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

3.1.2.1 組織のセキュリティ方針

本 TOE の利用に当たって要求される組織のセキュリティ方針を表 3-2 に示す。

これらは具体的な要求事項・法律などが存在するわけではないが、多数の事業者がサービスの運用にあたり、事業者の方針としてデータを処理するサーバに当然求める機能を開発者である TF ペイメントサービス株式会社が想定したものである。

表 3-2　組織のセキュリティ方針

識別子	組織のセキュリティ方針
P.Legitimate_terminal	サーバTOEはPOS端末TOEの初回接続時に正当な利用者の操作であることを検証する。 サーバTOEは接続を試みるモバイル端末TOEが正規バージョンであることを検証する。
P.Data_protection	サーバTOEはFeliCa ICチップとサーバTOE間でやりとりされる電子マネー決済データの機密性・完全性を保護する。
P.Audit	サーバTOEで動作するセキュリティ機能の挙動を監査ログとして記録する。

3.1.2.2　組織のセキュリティ方針に対するセキュリティ機能方針

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

⑴ 組織のセキュリティ方針「P.Legitimate_terminal」への対応

サーバ TOE は、POS 端末 TOE が初回接続時に端末固有の ID に対するパスフレーズの入力を求めることで、正当な権限を持たない者による POS 端末 TOE の店舗設置時しかできない初期設定を防止する。

また、サーバ TOE は、モバイル端末 TOE が接続を試みる際に当該端末のプログラム ID とバージョンを検証することで、プログラム機能性の差異に起因する誤動作を排除する。

⑵ 組織のセキュリティ方針「P.Data_protection」への対応

サーバ TOE と FeliCa IC チップ間の電子マネー決済データの転送は、FeliCa IC チップ識別・認証機能により正当と判断される場合に、転送データを改変や暴露から保護するために FeliCa 仕様で暗号化し、応答受信時には FeliCa 仕様の完全性検証データにより改変を検証することで、機密性と完全性を保護する。

⑶ 組織のセキュリティ方針「P.Audit」への対応

サーバ TOE は下記情報を監査ログとして記録する。これにより、運用者は TOE の利用状況の把握が可能になる。

表 3-3 監査記録要件

監査対象事象	監査対象アクション
監査機能	監査の開始と終了
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TOEの完全性検証	検証の失敗

4 前提条件と評価範囲の明確化

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

4.1 使用及び環境に関する前提条件

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

表 4-1 サーバの運用者(開発者)が満たすべき前提条件

識別子	前提条件
A.Server	サーバは、入退管理及び、物理的に外部侵入が防止される場所に設置され、インターネット境界には不正アクセスを抑止するように設定されたファイアウォールとSSLサーバを配置する
	サーバは、権限を持つ者だけにアクセス許可される設定にする
	サーバの運用中は、OSパッチ、ウィルス・チェック等を適時行い、TOEに有害な影響を与える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
A.Server_admin	サーバ管理者は、サーバの管理・運営において、不正行為を働かない

これらの前提条件は開発者が実施するサーバの運用に関する前提条件である[1]。TOE の導入を検討する事業者は開発者との契約等でこれらの条件が満たされていることを確認することが必要である。

[1] サーバの運用は開発者でもあるTFペイメントサービスが行う。8.2 注意事項も参照のこと

表 4-2 ECサイトを運営する事業者が満たすべき前提条件

識別子	前提条件
A.EC_site	ECサイトは、SSLでサーバTOEと通信するように設定される

この前提条件は EC サイトを運営する事業者が構築する EC サイトの運用環境に設定される前提条件である。EC サイトを運営する事業者にはこの他に、開発者の運用環境に設定された前提条件が満たされることも前提になる。

表 4-3 実店舗を運営する事業者が満たすべき前提条件

識別子	前提条件
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

この前提条件は実店舗に POS 端末を設置及び初期設定を行う事業者の行動に設定される前提条件である。

表 4-4 実店舗にPOS端末を導入する事業者が満たすべき前提条件

識別子	前提条件
A.POS_terminal	POS端末は、盗難・紛失に遭わないよう管理される

この前提条件は実店舗を運営する事業者が POS 端末導入事業者により導入された後の POS 端末の運用に設定される前提条件である。実店舗を運営する事業者にはこの他に、開発者の運用環境に設定された前提条件と、POS 端末導入事業者の行動に設定された前提条件が満たされることも前提になる。

4.2 運用環境と構成

本 TOE はサーバと 3 種類の端末に実装される。
本 TOE の一般的な運用環境を図 4-1 に示す。

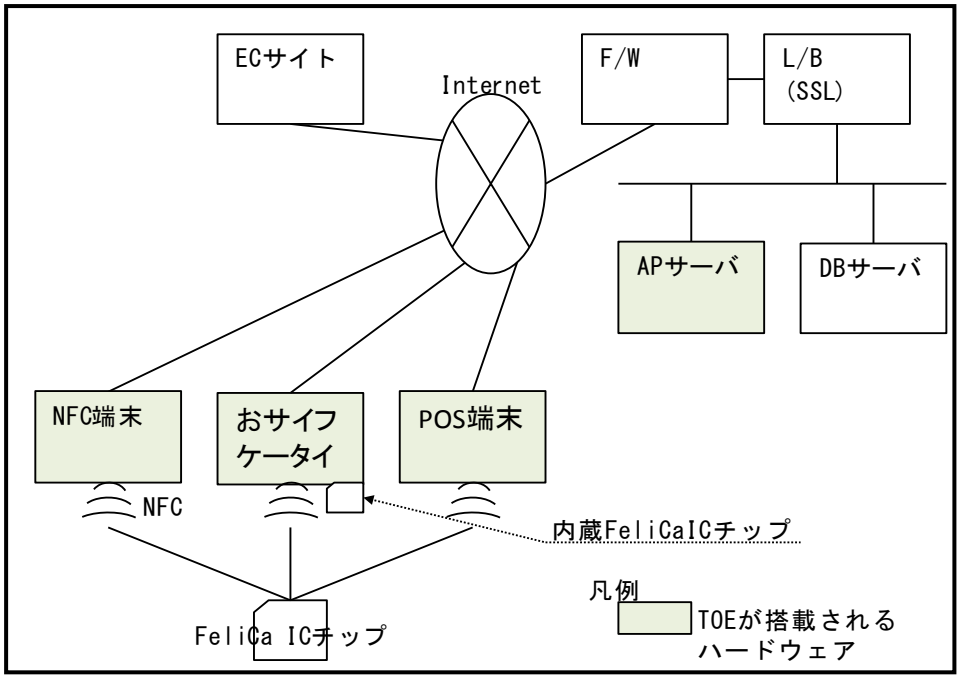

図 4-1 TOE の一般的な運用環境

(1) AP サーバ、DB サーバ、F/W 及び、L/B

AP サーバには、サーバ TOE が実装され、クラウドサービスを提供する。
DB サーバはサーバ TOE 等のデータ保管用に使用される。
F/W は外部ネットワークからの不正アクセスを防ぐために使用される。
L/B は SSL サーバ機能の利用及び、AP サーバの多重化運用を可能にする。
これらは開発者が構築し運用する。

(2) EC サイト

事業者が構築し運用する仮想店舗である。
TOE のガイダンスに従い TOE 利用のためのロジックを EC サイトに組み込んだものである。

(3) NFC 端末

一般に市販されている Android スマートフォンである。
NFC 端末 TOE が実装されることで、TOE のサービスを利用する EC サイトの端末として利用する。
開発者が NFC 端末に NFC 端末 TOE を組込み、EC サイトを運営する事業者に限定して提供する。

(4) おサイフケータイ

一般に市販されている Android おサイフケータイである。
おサイフケータイ TOE をインストールすることで、TOE のサービスを利用する EC サイトの端末として利用する。
開発者が Google Play にアップロードするおサイフケータイ TOE を、消費

者がダウンロードすることで利用可能になる。
おサイフケータイに内蔵されている FeliCa IC チップも利用できる。

(5) POS 端末
市販されている POS 端末である。
POS 端末 TOE が実装されることで、TOE のサービスを利用する実店舗の端末として利用される。
POS 端末 TOE は、開発者が実店舗を運営する事業者に限定して提供する。

(6) FeliCa IC チップ
nanaco のサービス(以降、ブランド AP と呼ぶ)が実装され、電子マネーが格納される高信頼 IT 製品である。
TOE がブランド AP と相互認証を行い、電子マネー決済データを転送することで、電子マネーが引き落とされる。

TOE に必要なハードウェアとソフトウェアを表 4-5 に示す。

表 4-5 TOEに必要なハードウェアとソフトウェア

略称	ハードウェア	OS	ミドルウェア等
AP サーバ	HP Integrity rx2800 i2	HP-UX 11i v3	Java VM 注1
DB サーバ	HP Integrity rx2800 i2	HP-UX 11i v3	Oracle 11g Release 2
POS 端末	CASIO DT-5300	Windows CE 6.0	―
NFC 端末	Google Nexus S	Android OS 4.1	ブラウザ注2
おサイフケータイ	docomo N-04C	Android OS 2.3	ブラウザ注2
	docomo SH-12C	Android OS 2.3	ブラウザ注2
	au IS03	Android OS 2.2	ブラウザ注2

注 1：HP-UX 付属の Java VM
注 2：Android OS 標準のブラウザ

これら機器等の信頼性は本評価の範囲ではない（十分に信頼できるものとする）。

4.3 運用環境におけるTOE範囲

AP サーバに対する一般的なインターネットを介した攻撃への対抗及び、暗号鍵、ID、パスワード等の TOE 外で管理される情報は TOE 範囲外の F/W と SSL 及び、

前提条件に依存する。

これらは、適正な運用が必要であり、開発者の責任となる。

EC サイトは、AP サーバとの通信及び、決済状況の管理のためのロジックを組込み、TOE の提供サービスに異常が認められる場合、消費者に対してリカバリ手段を提供するための実装と運用が必要である。

これらは、適正な実装と運用が必要であり、事業者の責任となる。

5 アーキテクチャに関する情報

本章では、本 TOE の範囲と主要な構成との関連性を説明する。

本 TOE の一般的な動作概念を図 5-1 に記す。

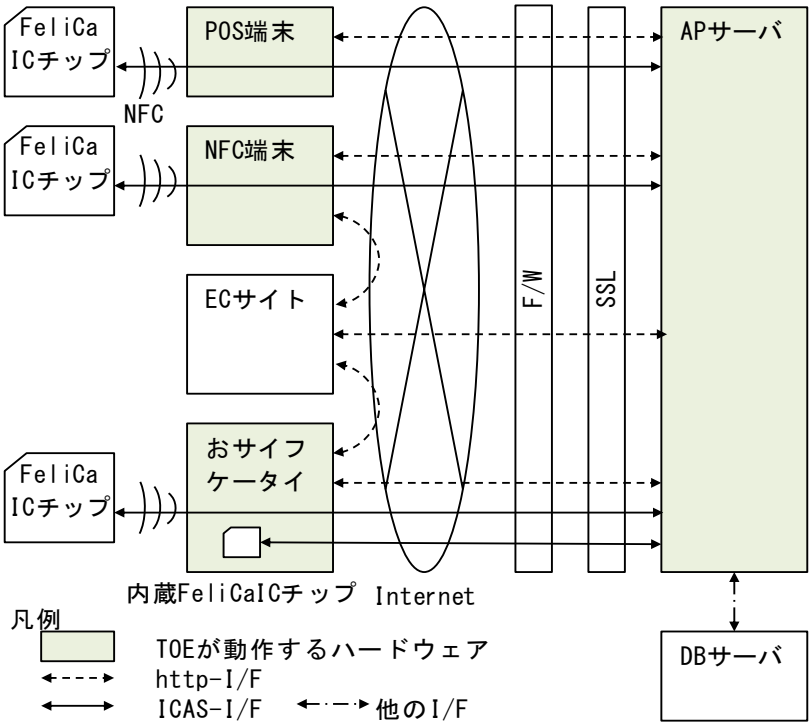

図 5-1 動作概念

AP サーバは、クライアントの要求に応じた処理を行い、データ保管のために DB サーバを、インターネット接続に伴う脅威軽減のために、SSL サーバとファイアウォールを利用する。

POS 端末は、POS 端末操作者の操作を http-I/F で AP サーバに送り、NFC を介した FeliCa IC チップの接続を待ち、ICAS-I/F による FeliCa IC チップの制御を中継する。

NFC 端末は、消費者が EC サイトで買物操作を行い、支払方法を TOE が提供する電子マネー決済サービスで行うよう確定すると、AP サーバに自動接続され、http-I/F による FeliCa IC チップ選択等の手順を経て、NFC を介した FeliCa IC チップの接続を待ち、ICAS-I/F による FeliCa IC チップの制御を中継する。

おサイフケータイは、NFC 端末と同様であるが、内蔵の FeliCa IC チップも利用できる。

EC サイトは、NFC 端末の説明で述べた確定操作により、AP サーバへ決済開始を要求し、モバイル端末へ AP サーバの接続情報を通知し、モバイル端末からの決済完了を待ち、AP サーバに決済状態を確認する。

FeliCa IC チップは、端末 TOE の操作に伴う「かざしてください」の旨の画面の

指示がある場合に端末へかざすことで、NFC を介して端末 TOE との接続が確立し、AP サーバの制御を受ける。

5.1 TOE境界とコンポーネント構成

TOE の構成を図 5-2 に示す。TOE は、AP サーバ、POS 端末、NFC 端末、おサイフケータイに実装される。

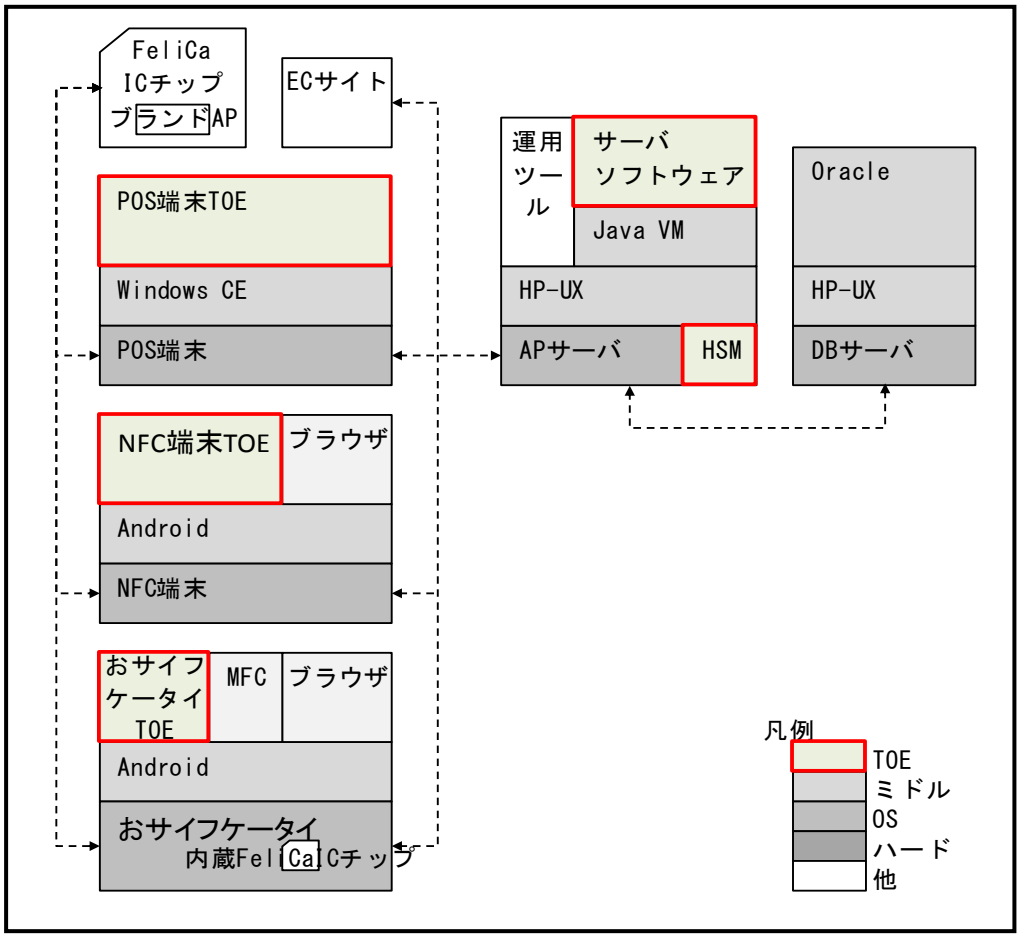

図 5-2 TOE 境界

TOE を構成する 4 つのコンポーネントについて説明する。

サーバ TOE

AP サーバには HSM(ハードウェア)が拡張され、OS、ミドル上でサーバソフトウェアと運用ツールが動作する。

サーバ TOE はサーバソフトウェアと HSM である。

サーバソフトウェアは、内部的に WebLogic、ICAS、共通プラットフォーム、nanaco 用の業務アプリケーション部分から成る。EC サイトと端末 TOE からの要求を WebLogic で受付け、ICAS、共通プラットフォーム、業務アプリケーションにより Oracle に管理されるデータの読み書き及び、HSM による暗号処

理を行い、FeliCa IC チップのブランド AP を制御するための情報を端末 TOE へ渡す。

POS 端末 TOE

専用 GUI からサーバ TOE に要求を行い、FeliCa IC チップとの接続を確立し、サーバ TOE から受ける制御コマンドを FeliCa IC チップのブランド AP へ渡す。

NFC 端末 TOE

ブラウザから EC サイトにアクセスし TOE による決済を指示することで自動起動し、サーバ TOE 及び、FeliCa IC チップとの接続を確立し、サーバ TOE から受ける制御コマンドを FeliCa IC チップのブランド AP へ渡す。

おサイフケータイ TOE

NFC 端末 TOE と同様であるが、おサイフケータイにバンドルされている内蔵 FeliCa IC チップを制御可能にするミドルウェア MFC により内蔵 FeliCa IC チップが利用できる

5.2 IT環境

本 TOE は表 4-2 に記したハードウェア、オペレーティングシステム及び、ミドルウェア上で動作し、連携するソフトウェアからのデータを処理する。

本 TOE のログ生成に用いる日時は、AP サーバの OS タイムスタンプを利用する。

AP サーバの運用ツールは、サーバ TOE の起動/停止を行うツール等である。

モバイル端末は調達容易な一般市販製品であることから、OS 上にさまざまなアプリケーションが実行されると考えられるが、モバイル端末 TOE の動作への影響について特に制限はされていない。

6 製品添付ドキュメント

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

サーバ管理者向け

・決済サービスセンターシステム管理ガイド Ver.1.0.1

実店舗(POS 端末操作者)向け

・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

POS 端末導入事業者向け

・導入事業者向け端末導入ガイド Ver.1.1.1

EC サイト、EC サイト開発者

・非対面決済導入ガイド Ver.1.1.3

※ このガイダンスには EC サイトを運営する事業者がモバイル端末の利用者に対して周知しなければならない事項も含まれている。

消費者(おサイフケータイ TOE)向け

・Thinca Payment App for おサイフケータイ ガイド Ver.1.0.0

※このガイダンスは Google Play からダウンロードできる。

7 評価機関による評価実施及び結果

7.1 評価方法

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

7.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成 24 年 9 月に始まり、平成 25 年 7 月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成 24 年 12 月、平成 25 年 4 月、6 月に開発者サイトで開発者のテスト環境を使用し、評価者テストを実施した。

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

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

これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

7.3 製品テスト

評価者は、評価の過程で示された証拠を検証した結果から、必要と判断されたテスト及び脆弱性評定に基づく侵入テストを実行した。

7.3.1 開発者テスト

本評価において、開発者テストは保証要件に含まれない。

7.3.2 評価者独立テスト

評価者は、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることをより確信するための独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを以下に説明する。

(1) 独立テスト環境

評価者が実施した独立テストの構成を図 7-1 に示す。図中のテストツールは開発者または評価者が用意したものを利用しているが、TOE とのインタフェース部分の仕様確認及び動作試験と校正は評価者によって実施されている。

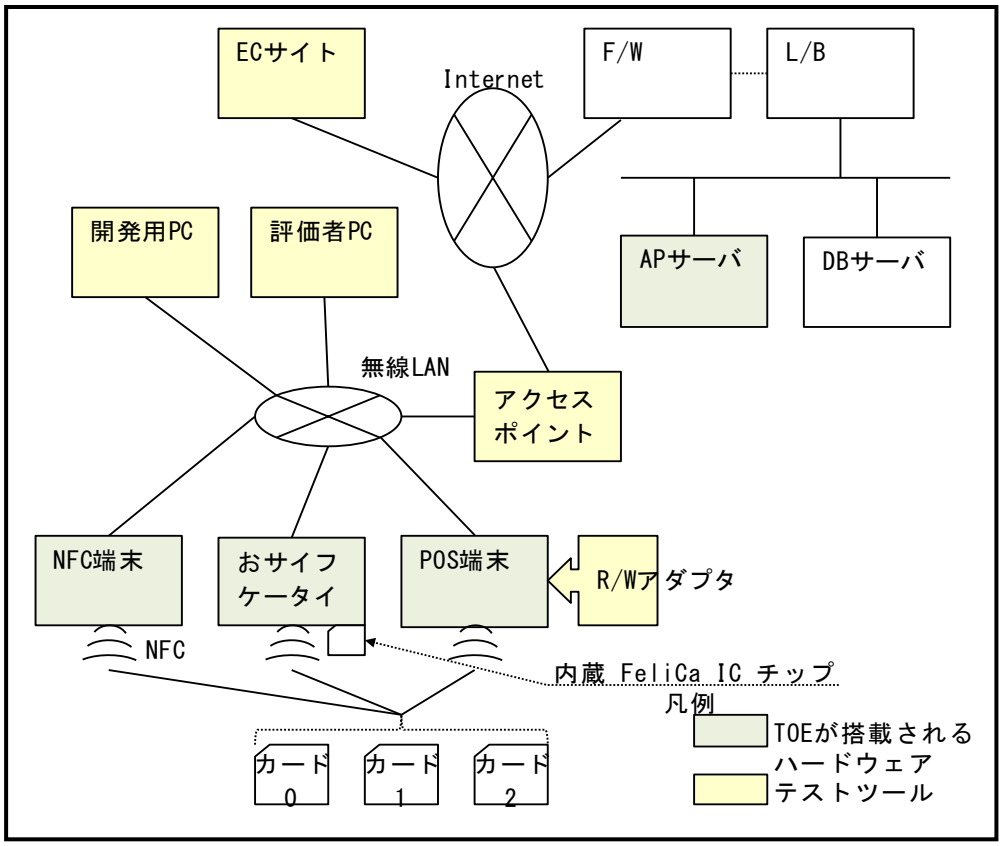

図 7-1　テストの構成図

評価の対象としたTOEを表7-1に示す。APサーバやDBサーバは本番環境とステージング環境にそれぞれ設置されており、本番環境は実運用中のため、ステージング環境で主なテストを実施し、本番環境ではサンプル的にテストを実施することでと同じ動作をすることを確認する計画とした。

表 7-1 テストしたTOE及び代替えTOE

環境	TOE		
本番	クラウド型決済システム Thincacloud コアモジュール	Thincacloud 決済サーバー	1.0.0
		Thincacloud 決済クライアント Windows CE 版	1.0.0
		Thinca Payment App for おサイフケータイ	1.0.0
		Thinca Payment App for NFC	1.0.0
ステージング	クラウド型決済システム Thincacloud コアモジュール	Thincacloud 決済サーバー	1.0.0
		Thincacloud 決済クライアント Windows CE 版	1.0.0
		Thincacloud 決済クライアント Windows CE 版 (R/W アダプタ換装タイプ)	－
		Thinca Payment App for おサイフケータイ(非正規バージョンタイプ)	
		Thinca Payment App for おサイフケータイ(ステージング環境接続専用タイプ)	－
		Thinca Payment App for NFC(ステージング環境接続専用タイプ)	－

評価者は、本番環境とステージング環境のTOEの違いを確認し、サーバTOEは同一であることを確認した。

POS端末TOEは、本番環境とステージング環境のサーバTOEの接続先URLを設定ファイルで変更できるため違いは無いと判断され、サーバTOEの電子マネー決済データ転送に対する応答の改ざん検知をテストするために、POS端末TOEの一部のモジュールを改造したR/Wアダプタ換装タイプが用意された。これは、POS端末のFeliCa ICチップ通信デバイスを制御するモジュールであり、FeliCa ICチップからの入力データの一部を書き換えることで改ざんされた状態にすることで、サーバTOEが改ざん検知できることを確認するテスト時のみ使用された。

モバイル端末 TOE の正当性確認機能をテストするために、アプリ ID、バージョンの違うモバイル端末 TOE(非正規バージョンタイプ)が用意された。これは、モバイル端末 TOE の正当性確認機能のテスト時のみ使用された。

本番環境のモバイル端末 TOE とステージング環境のモバイル端末 TOE(ステージング環境接続専用タイプ)はサーバ TOE の接続先 URL の記述部分が異なる。評価者はこの違いがセキュリティ機能に影響ないと評価している。

また、本番環境では TOE 外の L/B が持つ SSL サーバ機能を使うのに対して、ステージング環境は TOE の構成要素である WebLogic が持つ同機能を使うこと及び、設定ファイルの違いとして、各種サーバのホスト名等の通信設定、ライセンス情報、ログ出力レベルの違いが確認された。

以上の様に、本番環境とステージング環境には違いが認められたが、いずれもセキュリティ機能の動作に影響はないと判断された。

したがって、独立テストの構成は、識別された TOE をすべて含んでいるとみなすことができる。

テストに使われた機器を表 7-2 に示す。F/W、L/B、AP サーバ、DB サーバは本番環境とステージング環境に設置されており構成要素は同じである。EC サイト等のツールの使用目的は表 7-3 を参照。

表 7-2 テスト機器

機器略称	ハードウェア	OS/ミドル
開発用PC	Lenovo X100e	Windows 7 Professional
評価者PC	DELL LATITUDE E6410	Windows 7 Professional
ECサイト	CentOS 6.2	Apache 2.2.15 mysql 5.1.52 PHP 5.3.3
アクセスポイント	—	規格 ：IEEE 802.11g 暗号化方式 ：WPA-PSK AES
L/B	F5-BIG-LTM-3900-8G-R	—
F/W	Check Point D2 gateway	—
APサーバ#1	HP Integrity rx2800 i2	HP-UX 11i ver3.0
APサーバ#2	HP Integrity rx2800 i2	HP-UX 11i ver3.0
DBサーバ	HP Integrity rx2800 i2	HP-UX 11i ver3.0 Oracle Database 11g
NFC端末	Google Nexus S	Android 4.1.1
NFC端末	Google Nexus S	Android 4.1.2

おサイフケータイ	docomo SH-12C	Android 2.3.3
おサイフケータイ	docomo N-04C	Android 2.3.3
おサイフケータイ	au IS03	Android 2.2.1
POS端末×2台	CASIO DT-5300	Windows Embedded CE 6.0
カード0×複数枚	FeliCa ICチップ	nanacoサービス登録済
カード1×複数枚	FeliCa ICチップ	nanacoサービス未登録
カード2×複数枚	―	taspo、運転免許証等

以上により、独立テストは、本 ST において識別されている TOE の構成と同一の環境で実施されたとみなすことができる。

(2) 独立テスト概説

評価者の実施した独立テストは以下のとおりである。

a) 独立テストの観点

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

＜独立テストの観点＞

① 基本系

・全てのセキュリティ機能要件について確認を行う。

・全ての TSF インタフェースについて 1 つ以上のテストを行う。

② 例外系

・NFC 読み取りエラーを発生させた後の動作を確認する。

③ 多重系

・POS 端末 TOE の正当性検証に使用された ID、パスフレーズが他の POS 端末 TOE の正当性検証に使用できないことを確認する。

・複数の端末 TOE または、複数の FeliCa IC チップを使い、電子マネー決済を同時実行することで、複数のセキュリティ機能性に関する同時テストを行う。

④ 限界系

・カード登録枚数等、限界値、境界値に関するテストを行う。

b) 独立テスト概要

評価者が実施した独立テストの概要は以下のとおりである。

＜独立テスト手法＞

通常の TOE の使用において想定される利用者インタフェースを刺激し、結果を目視観察する方法の他、生成された監査ログの解析、パケットキャプチャによる通信暗号化の確認、R/W アダプタを使い改ざんした通信データを改ざん検知できるか等の確認が行われている。

＜独立テストツール＞

独立テストにおいて利用したツールを表 7-3 に示す。

表 7-3　独立テストで使用したツール

ツール名称	概要・利用目的
ECサイト	開発者テスト用に作られたECサイトシミュレータ。
SSL	本番環境はL/BのSSLを使用するが、ステージング環境ではサーバTOEのSSL機能を使用した。
R/Wアダプタ	独立テスト用に作られたテストハーネス。 POS端末TOEを構成するモジュールの一部であり、サーバTOEへの特定通信データを常に改ざん状態にする。改ざん検知の機能性をテストする際に差替えて使用した。
カード0	ブランドAP登録済FeliCa ICチップ。
カード1	ブランドAP未登録FeliCa ICチップ。
カード2	規格外媒体(FeliCa仕様でないもの)。
開発用PC	ログ取得、POS端末の通信キャプチャ。
評価者PC	テストツール実行基盤、POS端末TOEのバージョン確認等。
以下は評価者PCで動作するツール	
Wireshark 1.8.4	汎用パケットキャプチャツール。
以下はモバイル端末で動作するツール	
tPacketCapture 1.0	Android4.0用パケットキャプチャアプリ。

＜独立テストの実施内容＞

独立テストは、評価者によって 53 項目実施された。

独立テストの観点とそれに対応したテスト内容を表 7-4 に示す。

表 7-4 実施した独立テスト

観点	テスト概要
① 基本系	・POS端末TOEから正しいまたは正しくないID、パスフレーズを入力することで、POS端末TOEが初期認証されることを確認した。 ・端末TOEとカード0を操作することで決済処理を実施し、決済処理が問題なく動作することを確認した。※以降、通常操作と呼ぶ。これにより、連続的に実行されるモバイル端末の正当性検証機能とFeliCa ICチップの相互認証機能と電子マネー決済データの暗号化機能が確認された。 ・おサイフケータイTOE(非正規バージョンタイプ)を使用し通常操作を行い、「最新アプリにアップデートしてください」の旨の画面が表示され、モバイル端末TOEの検証に失敗し、処理が中断されることを確認した。 ・通常操作の使用カードをカード1及び、カード2に変えて操作することで、相互認証に失敗し、処理が中断されることを確認した。 ・POS端末TOE(R/Wアダプタ換装タイプ)を使い処理途中のデータを変更して決済処理を実施することで、サーバTOEが通信データの改ざんを検知することを確認した。 ・サーバTOEのログを目視確認することで監査生成ができていることを確認した。 ・通常操作を実施する過程で通信キャプチャすることで、通信データが暗号化されていることを確認した。
② 例外系	・通常操作を行い端末の指示に従いカード0をかざしている状況で、カード0を遠ざける等することで読み取りエラーを発生させ、通常操作をキャンセルした後、カード0の残高照会で決済されていないことを確認した。
③ 多重系	・他のPOS端末TOEの初期認証に使われたID、パスフレーズを使い、POS端末TOEから初期認証を試み、失敗することを確認した。 ・カード0をかざす直前の状態まで通常操作した端末を複数準備し、かざす操作を同時実行する状況で、仕様通りの動作をすることを確認した。 ・カード0をかざす直前の状態まで通常操作した端末を準備し、カード0を複数並べる及び、重ねて端末にタッチする状況で、仕様通りの動作をすることを確認した。
④ 限界系	・閾値までカード0を登録しセキュリティ機能に不審な兆候が発生しないことを確認した。

c) **結果**

評価者が実施したすべての独立テストは正しく完了し、評価者はTOEのふるまいを確認した。評価者は、すべてのテスト結果と期待されるふるまいが一致していることを確認した。

7.3.3 評価者侵入テスト

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

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

a) 懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

① 一般的な公知の脆弱性

TOEがインターネットを使ったサービスを行うことから以下が懸念された。

・不要なポートがオープンされている可能性。

TOEがWebアプリケーションの性質を持つことから以下が懸念された。

・端末に表示されるサーバTOEのURLを頼りにリプレイ攻撃が成立する可能性。

・既知のURLを頼りに、オブジェクトが直接参照できる可能性。

・DBサーバに対してSQLインジェクションを許す可能性。

② 予期せぬふるまいによるセキュリティ機能性のバイパス

多数のクライアントが多様な状況で利用されることから、以下が懸念された。

・端末の電源断等による強制終了の影響

・端末の複数メニュー起動によるセキュリティ機能性のバイパスの可能性。

③ 端末TOEが改ざんされたことによるセキュリティ機能性のバイパス

おサイフケータイTOEがインターネット経由で配布されることや、モバイル端末TOE がAndroidアプリケーションであることから、以下が懸念された。

・モバイル端末TOEを改ざんし、FeliCa ICチップとの通信を行うことなくECサイトに正常終了を通知することで電子マネーを使用せずに決済できる可能性。

b) 侵入テストの概要

評価者は、潜在的な脆弱性が悪用される可能性を検出するために、以下の侵入

テストを実施した。

＜侵入テスト環境＞

侵入テストは、図7-1に示した評価者独立テストと同一環境で実施された。

評価者独立テスト手法に加えて、侵入テストで利用したツールを表 7-5 に示す。これらは評価者 PC で動作する。

表 7-5 侵入テストツールで使用したツール

ツール名称	概要・利用目的
Paros 3.2.13	プロキシ型のWeb脆弱性検査ツール。
Wireshark 1.8.4	汎用パケットキャプチャツール。
tPacketCapture 1.0	Android4.0用パケットキャプチャアプリ。
Burp Suite Free Edition 1.5	Webアプリケーションのセキュリティテストプラットフォーム。
Nessus 5.0.1	脆弱性スキャンツール。
HTTPSender 1.0	Httpリクエスト送信ツール。

＜侵入テスト手法＞

評価者独立テスト手法に加えて、Web 脆弱性検査ツールや http リクエスト送信ツールによる、通信データのキャプチャや、通信データのデータ改ざん及び、操作中の電源断等が行われている。

＜侵入テストの実施項目＞

懸念される脆弱性と対応する侵入テスト内容を表 7-6 に示す。

表 7-6　侵入テスト概要

脆弱性	テスト概要
①一般的な公知の脆弱性	・Nessusを用いてAPサーバのポート解放状態を調査し、解放ポートがhttpsだけであること及び、解放ポートについて公知の脆弱性が無いことを確認した。 ・既知のURLを使いサーバTOEへのリプレイ攻撃を試み、サーバTOEが「お取引できません」の旨を返すことを確認した。 ・既知のURLを頼りにアクセス先を推測しサーバTOEへ直接参照を試み、サーバTOEが接続先エラーを示すメッセージを返すこと及び、攻撃の手掛かりになる情報を含まないことを確認した。 ・攻撃成立の可能性があるSQLをTOEのGUIやHTTPSenderより注入し、Oracle管理下のテーブル及びログの更新状況を確認することで、サーバTOEが入力文字列をチェックしサニタイジングできていることを確認した。
②予期せぬふるまいによるセキュリティ機能性のバイパス	・通常操作を行い端末の指示に従いカード0をかざしている状況で、電池抜取等による強制終了を行い通信エラーを発生させ、再起動後の端末が通信エラー発生履歴を示し、カード0の残高照会で決済されていないことを確認した。 ・POS端末TOEは2つのメニューを表示させる手段がないこと、モバイル端末は二つのブラウザを起動しそれぞれに通常操作を行い、カード0をかざすと、セキュリティ機能が開始される前にエラーストップすることを確認した。
③端末TOEが改ざんされたことによるセキュリティ機能性のバイパス	・サーバTOEに端末TOEからの接続が無い状況や、通常操作を行いカード0をかざす直前の状況等に、ECサイトからサーバTOEが管理する決済状態を確認する操作を実施し、サーバTOEの決済処理状態が「IDLE状態」、「決済処理中」等、適正に管理されていることを確認した。 ※FeliCa ICチップとの通信を行うことなくECサイトに正常終了を通知することができる改ざんされたモバイル端末TOEは、高い攻撃力を持つ者によりFeliCa仕様の暗号化データを生成できない限り、サーバTOEとの通信を正常に行うことができず、サーバTOEが管理する決済処理状態を変更することができないと考えられ、ECサイトがサーバTOEへ決済状態を問い合わせることをもって、モバイル端末TOEが適正に動作したことを知ることができると判断された。

c) **結果**

評価者が実施した侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

7.4 評価構成について

本評価では、図 7-1 に示す構成において、評価を行った。本 TOE は、この構成と構成要素が大きく異なる環境において、運用される場合はない。よって、評価者は、上記の評価構成は適切であると判断した。

7.5 評価結果

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

評価では以下について確認された。

PP 適合：なし

セキュリティ機能要件：　コモンクライテリア　パート２　適合

セキュリティ保証要件：　コモンクライテリア　パート３　適合

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

EAL１パッケージのすべての保証コンポーネント

追加の保証コンポーネント　ASE_SPD.1、ASE_OBJ.2、ASE_REQ.2

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

7.6 評価者コメント/勧告

調達者に喚起すべき評価者勧告は、特にない。

8 認証実施

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

① 所見報告書でなされた指摘内容が妥当であること。

② 所見報告書でなされた指摘内容が解決されていること。

③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。

④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。

⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

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

8.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本 TOE が CC パート 3 の EAL1 及び保証コンポーネント ASE_SPD.1、ASE_OBJ.2、ASE_REQ.2 に対する保証要件を満たすものと判断する。

8.2 注意事項

本システムをセキュアに運用するにあたり、サーバ TOE の管理等の開発者が実施すべき具体的事項を、本評価では前提条件として設定している。

このため本評価は、前提条件を満たすための方法がサーバ管理者向けのガイダンスである決済サービスセンター システム管理ガイド Ver.1.0.1 に記されていることを評価したに留まり、適正に実施されるかについては保証範囲外であることに注意が必要である。

TOE の導入を検討する事業者は、開発者と契約を結ぶ等しサーバの運用環境に対する前提条件が継続的に満たされることを担保すべきである。

9 セキュリティターゲット

本 TOE のセキュリティターゲット[12]は、本報告書とは別文書として以下のとおり本認証報告書とともに提供される。

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 Ver.1.00　2013 年 7 月 9 日 TF ペイメントサービス株式会社

10 用語

本報告書で使用された CC に関する略語を以下に示す。

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

本報告書で使用された TOE に関する略語を以下に示す。

ICAS	HP-IC-Chip Access Server for FeliCa
HSM	Hardware Security Module
NFC	Near Field Communication
F/W	FireWall
L/B	LoadBalancer
R/W	Reader/Writer
MFC	Mobile FeliCa Client for Android
http(s)	Hypertext Transfer Protocol(Secure)
I/F	Interface

本報告書で使用された用語の定義を以下に示す。

ICAS	遠隔のFeliCa ICチップを制御するためのミドルウェア。
HSM	暗号処理を行うためのアプライアンス製品。
NFC	近距離無線通信技術の一つ。
FeliCa	非接触ICカード技術方式の一つ。
制御コマンド	FeliCa ICチップを制御するコマンド。
R/W	FeliCa ICチップの読み書きを行うデバイス。
MFC	FeliCa ICチップを内蔵するAndroidおサイフケータイにバンドルされるミドルウェア。
ブランド	電子マネーを発行・管理・運営する事業体。

TOEは、nanacoを対象にする。

ブランドAP　　FeliCa ICチップで動作するアプリケーション。

11 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 平成24年3月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 平成25年4月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項, 平成25年4月, 独立行政法人情報処理推進機構, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003

[7] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル, バージョン3.1 改訂第3版, 2009年7月, CCMB-2009-07-001, (平成21年12月, 翻訳第1.0版)

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能コンポーネント, バージョン3.1 改訂第3版, 2009年7月, CCMB-2009-07-002, (平成21年12月, 翻訳第1.0版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証コンポーネント, バージョン3.1 改訂第3版, 2009年7月, CCMB-2009-07-003, (平成21年12月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004

[11] 情報技術セキュリティ評価のための共通方法: 評価方法, バージョン3.1 改訂第3版, 2009年7月, CCMB-2009-07-004, (平成21年12月, 翻訳第1.0版)

[12] 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, バージョン 1.00, 2013年7月9日, TFペイメントサービス株式会社

[13] クラウド型決済システム Thincacloud コアモジュール評価報告書, 第2.0版, 2013年7月18日, 株式会社 ECSEC Laboratory 評価センター