認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙 押印済

評価対象

申請受付日（受付番号）	**平成19年8月6日（IT認証7162）**
認証番号	C0191
認証申請者	**エヌ・ティ・ティ・コミュニケーションズ株式会社**
TOEの名称	**アダプタ対応型高速版住基カードソフトウェア**
TOEのバージョン	2.00
PP適合	**なし**
適合する保証パッケージ	EAL4**及び追加の保証コンポーネント**AVA_MSU.3
開発者	**日本電信電話株式会社** **シャープ株式会社**
評価機関の名称	**株式会社電子商取引安全技術研究所　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20年10月30日

セキュリティセンター 情報セキュリティ認証室
技術管理者　鈴木　秀二

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

① Common Criteria for Information Technology Security Evaluation Version 2.3
② Common Methodology for Information Technology Security Evaluation Version 2.3

評価結果：合格

「アダプタ対応型高速版住基カードソフトウェア」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

1.1 はじめに

この認証報告書は、「アダプタ対応型高速版住基カードソフトウェア　バージョン2.0」（以下「本TOE」という。）について株式会社電子商取引安全技術研究所評価センター（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者であるエヌ・ティ・ティ・コミュニケーションズ株式会社に報告するものである。

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

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

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

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称：　アダプタ対応型高速版住基カードソフトウェア
バージョン：　2.0
開発者：　日本電信電話株式会社
　　シャープ株式会社

1.2.2 製品概要

TOEは、住基ネットにおいて使用される住基カードに搭載される組み込みソフトウェアであり、住基カードに記録されるデータや搭載されるアプリケーション(以下、AP と表記)を管理するために利用され、住基カードとしての要求仕様を満足するものである。

TOEは住基カードに搭載され、カード発行者からカード所有者への安全な交付、カード所有者の本人確認、カードに格納されたカード所有者の情報に対する保護を実現することを目的とする。住基カードは、住民票の写しの広域交付、転入転出の

特例及び本人確認の業務に利用される。住基カードは、市町村の窓口に設置された住基ネットへ接続された市町村システムの業務用端末に接続されている住基カード用のカードリーダ・ライタに挿入され、カードリーダ・ライタを通じて市町村の業務用端末と通信して各業務を実現する。TOEは、上記のような要求を実現する際に、利用者の認証、アクセス制御、暗号化通信、アプリケーションの独立性確保などのセキュリティ機能を提供することを目的とする。

1.2.3 TOEの範囲と動作概要

TOE を構成するソフトウェア及び周辺のハードウェアとソフトウェアの関係を図1-1に示す。

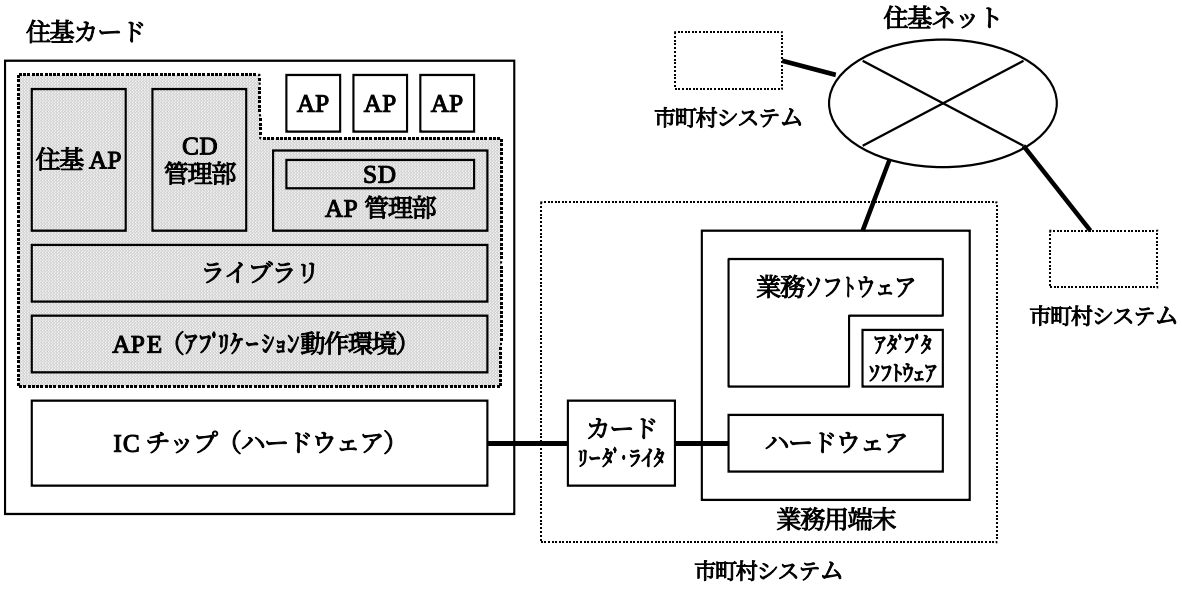

図1-1 TOEの構成

TOEは網掛けで示した部分のソフトウェアであり、住基カード内に埋め込まれたIC チップ上のメモリに組み込まれる。住基カードはカードリーダ・ライタを通じて業務用端末に接続され、業務用端末は住基ネットに接続される。住基ネットには同様にして各市町村のシステムが接続されている。住基カードは、ICチップの通信機能によりカードリーダ・ライタを通じて業務用端末から送信されたコマンドメッセージを受け取り、コマンドメッセージの内容に基づいた処理を実施し、その結果をレスポンスメッセージとして返却する。業務用端末上では業務ソフトウェアと呼ばれるソフトウェアが動作し、住基ネットに必要な業務を処理する。業務用端末上には更にアダプタと呼ばれるソフトウェアが存在し、住基仕様で規定されたコマンド仕様に基づき住基カードの実装に対応したコマンドメッセージを生成する。アダプタは業務ソフトウェアから呼び出され、製造者毎に異なる住基カードの実装の差を吸収して共通のコマンド仕様で住基カードを利用できるようにする。なお、TOE

のAP管理部にはSDと呼ばれる領域が創生されてその上にAPが搭載可能であるが、搭載されたAPはTOEの範囲外である。

1.2.4 TOEの機能

図1-1に示されたAPE、ライブラリ、CD管理部、AP管理部及び住基APのモジュールで実現されるTOEの機能を、以下に【TOEのセキュリティ機能】及び【TOEのセキュリティ以外の機能】に分けて記述する。

【TOEのセキュリティ機能】

１．識別と認証機能

(1) 識別機能

TOEは、セレクトコマンドにより選択されるモジュールを識別する。選択されてカード上で動作しているモジュールをプロセスと呼び、プロセスは利用者を代行して動作し、受信したコマンドメッセージは現在選択されているプロセスへ引き渡される。

(注釈) 本STにおいて、モジュールはカード上に搭載されたソフトウェアのプログラム単位での構成要素を表し、プロセスはモジュールがサブジェクトとして動作している状態の時のプログラムを表す。CD管理部、住基AP及びAP管理部の各モジュールが動作した場合、それぞれCD管理プロセス、住基APプロセス及びAP管理プロセスとなる。

(2) PIN照合機能

TOEは、外部から送られたPINをあらかじめカード内に設定されたデータと照合し、TOE関係者（カード所有者、カード発行者）を認証する。

(3) 外部認証機能

TOEは、生成した乱数を業務用端末へ送り、業務用端末は対応する秘密鍵で乱数を暗号化し返却し、TOEはあらかじめカード内に設定された公開鍵、または検証された公開鍵証明書の公開鍵を使用して復号し、業務用端末を認証する。

２．アクセス管理機能

(1) ファイル管理機能

TOEは、ICチップ内のFlashメモリ上にデータを格納するための各ファイル領域の確保及び管理を行い、ファイルに設定されたデータへのアクセスを制御する。

(2) アプリケーション管理機能

TOEは、APを管理するための領域として、APを搭載するSDと呼ばれる領域を有する。TOEは、SDにおいてAPを管理し、アクセス制御に基づきAPの搭載と選択と削除を管理する。

(3) 鍵管理機能

TOEは、TOEの管理するICチップ内の鍵格納用ファイルへの鍵データの設定、更

新を行う。

３．暗号通信機能

(1) セキュアメッセージング機能

TOEは、外部との通信にセキュアメッセージング機能として送信データの暗号化と受信データの復号を行う。ICカードLSIが持つDES暗号処理のための演算機能により高速な動作を実現している。

４．実行管理機能

(1) 認証ステータス管理機能

TOEは、PIN照合と外部認証の結果を認証ステータスとして管理する。CD管理部、AP管理部及び住基APのいずれかのモジュールがカレントプロセスとして選択された際に認証ステータスをクリアまたは維持し、各プロセスにおいてPIN照合及び外部認証が行われた際に認証ステータスを更新する。

(2) 状態遷移管理機能

TOEは、CD管理部、AP管理部及び住基APの各モジュールにおける状態を管理し、コマンドにより各モジュールの状態を遷移させる。

(注釈) 各モジュールは、製造段階、納入、交付、運用段階において異なった状態にあり、その各々の状態において実行可能なコマンドが異なる。各モジュールの状態はプロセスとして動作中に遷移し、モジュールとして搭載されている非動作時にも状態は維持される。

(3) コマンド実行制御機能

TOEは、状態遷移の状態に応じて認証されているTOE関係者の役割でコマンドの実行が可能かどうかを判断し、コマンド実行を制御する。

５．ドメイン分離機能

(1) ドメイン分離機能

TOEは、カードに搭載されるモジュール間が相互に干渉しないようにそれぞれの動作領域を分離する。

６．データ復元機能

(1) 電源断異常検出機能

TOEは、データの書込み中または消去中に電源断異常が発生したかどうかを起動時に検査する。もし書込み・消去中に電源断が発生した場合は、下記(2)の障害回復機能によりデータが回復される。

(2) 障害回復機能

TOEは、書込み・消去処理実行前に、トランザクション処理を開始し、正常終了した場合にはトランザクション処理中の書込み内容を有効にして終了し、異常終了した場合には、トランザクション処理中の書込み内容を無効にして終了し、カードを

正常状態に回復する。

【TOEのセキュリティ以外の機能】
１．通信機能
TOEは、実行要求であるコマンドメッセージの受信及び処理結果であるレスポンスメッセージの送信を行う。

２．コマンド解析機能
TOEは、受信したコマンドメッセージを解析し、要求された処理を行う。

３．メモリ制限機能
TOEは、カード上に搭載されたアプリケーションが利用可能なメモリ領域の大きさを制限する。

1.3 評価の実施

認証機関が運営するITセキュリティ評価･認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

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

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「アダプタ対応型高速版住基カードソフトウェア セキュリティターゲット」（以下「ST」という。）[1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発・製造・出荷の現場を調査し、本TOEがCCパート1 ([5][8][11]のいずれか) 附属書B、CCパート2（[6][9][12]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート3（[7][10][13]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「アダプタ対応型高速版住基カードソフトウェア評価報告書」（以下「評価報告書」という。）[18]に示されている。なお、評価方法は、CEM（[14][15][16]のいずれか）に準拠する。また、CC及びCEMの各パートは補足[17]の内容を含む。また本評価においてはAVA_MSU.3評価、スマートカード評価のためAIS34[19]、及びCCサポート文書[20]

も参照する。

1.4 評価の認証

認証機関は、評価機関が作成した、評価報告書、所見報告書、及び関連する評価証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。評価は、平成20年10月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

1.5 報告概要

1.5.1 PP適合

適合するPPはない。

1.5.2 EAL

STが規定するTOEの評価保証レベルは、EAL4追加である。
追加の保証コンポーネントは、AVA_MSU.3である。

1.5.3 セキュリティ機能強度

STは、最小機能強度として、”SOF-基本”を主張する。本TOEは、個人情報を取り扱うため安全性を重要視しており、更に全国規模で多くの住民に配られ、本人確認業務だけでなく、市町村が提供する様々な行政サービスの中で使われる。住基カードには、正当な役割に関連付けられた利用者を識別･認証する機能が必要である。住基カードは個人情報を取り扱うが、金融系のカードのように資産的な価値を取り扱う訳ではない。 したがって、TOEの認証における安全性を確保する機構には、低位の攻撃力を持つ攻撃者からの攻撃にも耐えうるSOF-基本が妥当である。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能は、「1.2.4　TOEの機能」の【TOEのセキュリティ機能】で示した通りである。

1.5.5 脅威

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

住基カードを交付された住民は、そこに格納された住民票コードを基に、市町村が管理している個人情報（本人確認情報：氏名、生年月日、性別、住所、住民票コード、付随情報）へアクセスし、各種の行政サービスを受ける。このような便利なカードは、様々な動機を持った人から、以下に示すような様々な攻撃を受けると想定され、カード発行を受けた住民はプライバシー侵害だけでなく、財産的な損害を受ける恐れがある。

表1-1　想定する脅威

識別子	脅　威
T.Logical_Attack	市町村に納入された住基カードは、住基カードの記憶素子へ、発行市町村データや住民票コード設定、住基カードへの券面印刷等の工程を経て、市町村から住民に交付され、利用される。この一連の過程の住基カードに対し、ICカードの技術に詳しい攻撃者が、住民基本台帳カード仕様で規定する論理的インタフェース(コマンド/レスポンス)を悪用し、利用者データやTSFデータを改ざんしたり、盗んだりする。
T.Illegal_Term_Use	住民基本台帳ネットワークで使われる業務用端末の操作に詳しい正規の職員以外の攻撃者が業務用端末を悪用したり、業務用端末に改造を行ったりして、住基カードとやり取りされるデータへ不正にアクセスし、利用者データやTSFデータを改ざんしたり、盗んだりする。
T.Disturb_APL	住基カードには多くのアプリケーションが存在する。即ち、本人確認業務アプリケーション、市町村によってロードされる市町村独自のアプリケーションである。このような複数のアプリケーションが存在する住基カード内で、市町村独自のアプリケーションが利用者データを改ざんしたり、盗んだりする。
T.Environment	住基カードを使っている時に電源断が発生し、データの書換えが中断されることがある。その後、再度、住基カード使おうとした時、住基カード内の利用者データやTSFデータが正しく書換わっていないことがある。
T.Incomplete	市町村に納入された住基カードが住民に交付されるまでに、様々な利用者データやTSFデータの設定が行われる。このような利用者データやTSFデータが設定された、交付前の住基カードを不正に入手した攻撃者が、正規に発行さ

	れた住基カードとして、悪用する。
T.Hardware	半導体や暗号の技術に詳しい攻撃者は、以下に述べるハードウェア攻撃手段を使いTOEの資産の盗聴や改ざんもしくは秘密(Secret)の推測を行うかも知れない。 ・FIB(Focused Ion Beam) workstation, EBP(Electron Beam Prober), AFM(Automatic Force Microscope)を利用し、演算回路、記憶素子の物理的改ざん、盗聴（i.e. TOE自体やTSFデータの改ざん、TSFデータの盗聴） ・ハードウェアの処理状況を分析することで、TSFデータを推定 ・ICカードを異常な状態で動作させ、その結果を分析し、TSFデータを推定

1.5.6 組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針を表1-2に示す。

住民基本台帳カード仕様書 第2.3版は、住基カードの仕様書であるが、組織のセキュリティポリシと捉えるべき記述があるので、それらの要件を以下に引用する。

表1-2 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.Authentication	[住基仕様23]には、住民票コードの読出条件について、ポリシ的な記述は無い。しかし、7章 住民カードアプリケーション仕様編 表8.9 住基カードAPのセキュリティアトリビュート設定から、以下の条件が暗黙的にポリシとして設定されていると考えられる。 ・PIN(*)による本人認証が終わっていること ・全国センター発行の証明書による市町村認証が終わっていること * Personal Identification Number。パスワードに相当
P.Secret_Setting	1章 概要2.3節 住民基本台帳カードの業務要件の(1)に、「カードに秘密鍵を設定する際に、安全な発行方式を採用する」との規定があり、TOEの実装に反映する必要がある。
P.PIN_Initialize	1章 概要2.3節 住民基本台帳カードの業務要件の(3)に、「パスワード忘却時にカード再利用に資する目的で、暗証番号初期化の後、利用者の新たなパスワード設定に対応する方式を採用する」との規定があり、TOEの実装に反映する必要がある。

P.Secure_Path	7章 住基カードアプリケーション仕様編 3.4 セキュアメッセージング機能について、「セキュアメッセージング機能は、ICカードと外部装置との間で授受されるAPDUを不正な盗聴から保護するための暗号化通信を行う機能である。住基カードAPにおいて、本機能は住民票コード読み出し処理において利用される」との規定があり、TOEの実装に反映する必要がある。 (注釈) APDU(Application Protocol Data Unit)とは、住基カードとカードリーダ・ライタ間でやり取りされるデータの単位で、本STでは、カードリーダ・ライタから住基カードへのAPDUをコマンドメッセージ、住基カードからカードリーダ・ライタへのAPDUをレスポンスメッセージと呼んでいる。

1.5.7 構成条件

TOEの動作環境及びTOE周辺装置の仕様は、以下のとおりである。これらは全て市町村システムに設置・インストールされる。

＜ICチップ＞
製造元： シャープ株式会社
型式： SM4148 ICカードLSI

＜カードリーダ・ライタ＞
ISO/IEC 14443及びJIS X 6322に規定される非接触型のインタフェース、またはISO/IEC 7816及びJIS X 6304に規定される接触型のインタフェースを有するカードリーダ・ライタとする。

＜アダプタソフトウェア＞
住基カードの要求仕様に基づき住基カードの実装に対応して作成されたソフトウェア

＜業務ソフトウェア＞
要求仕様に基づいた住基カードの動作に見合った対応するように作成されたソフトウェア

1.5.8 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表1-3に示す。

これらの前提条件が満たされない場合、本TOEのセキュリティ機能が有効に動作することは保証されない。

表1-3　TOE使用の前提条件

識別子	前提条件
A.CARD_SET_Data	TOEがカード所有者に渡されるまでに、カード発行者またはAP搭載管理者である市町村は、利用者データや認証データ及びTOEの動作で必要となる情報を、TOEに設定する。それらのデータは人的側面において、市町村の責任で安全な値が指定され、教育と訓練を受けた職員により正しく設定され、安全に管理されるものとする。また、物理的側面として、TSFデータの設定/利用時には、TSFデータを安全に管理できるIT装置(カードリーダ・ライタや業務用端末)を市町村は調達し、市町村の安全な環境で使用するものとする。また、カード所有者である住民は、推測されにくい適切なPINを設定するものとする。

1.5.9　製品添付ドキュメント

本TOEに添付されるドキュメントを以下に示す。

表1-4　ガイダンス文書一覧

名称	識別	Ver
アダプタ対応型住基カードソフトウェア　ガイダンス統括文書	GD_ALL	第 1.10 版
アダプタ対応型住基カードソフトウェア　AP 搭載管理者ガイダンス文書	GD_APM	第 1.10 版
アダプタ対応型住基カードソフトウェア　CM 部　取扱説明書	GD_CM	第 1.12 版
アダプタ対応型住基カードソフトウェア　カード発行者ガイダンス文書	GD_ISS	第 1.12 版
アダプタ対応型住基カードソフトウェア　住基 AP 部　取扱説明書	GD_JAP	第 1.11 版
アダプタ対応型住基カードソフトウェア　住基 CD 部　取扱説明書	GD_JCD	第 1.11 版
IC カード内蔵ソフトウェア AP 実行環境取扱説明書(AP 実行環境 Ver. 2.517dR 対応版･システム開発者向け)	APE_GD	第 1.2.0 版
SM4148 AP 実行環境(APE)セキュリティガイダンス	APE_GD_S	第 1.3.0 版

2 評価機関による評価実施及び結果

2.1 評価方法

評価は、CCパート3の保証要件について、CEMに規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

2.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成19年8月に始まり、平成20年10月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成19年10月～平成20年7月に6回に分けて開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付と運用・ライフサイクルの各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成20年5月及び8月に開発者サイトで開発者のテスト環境及び評価機関のテスト環境を使用し、開発者が実施したテストのサンプリングチェック及び評価者テストを実施した。

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

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

2.3 製品テスト

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

2.3.1 開発者テスト

1) 開発者テスト環境

TOEはシャープ株式会社及び日本電信電話株式会社により開発（APEはシャープ株式会社により開発、ライブラリ、CD管理部、AP管理部及び住基APは日本電信電話株式会社により開発）されており、テストも両社により自社開発部分を各々実施している。日本電信電話株式会社により実施されたテストの構成

は以下の通りである。

表2-1　テスト構成（日本電信電話株式会社）

機器	主な仕様
IC カードリーダライタ 非接触型 USB タイプ	SCR331DI-NTTCom NTT コミュニケーションズ株式会社
テスト用 PC	Windows2000、または Windows XP
IC カード（チップ含む）	IC チップ形式：SM4148　IC カード LSI
ソフトウェア	主な仕様
Smart Card Simulator	Version 4.0.1　シャープ株式会社
Fsp	1.7.8　NTT エレクトロニクス株式会社

シャープ株式会社により実施されたテストの構成は以下のとおりである。

表2-2　テスト構成（シャープ株式会社）

機器	主な仕様
端末 PC	AT 互換機
エバボード	エバボード(シャープ製)
ICE	ROMICE64(コンピューテックス製)
プロトコルアナライザ	LE-7200 LINE EYE 製
プロトコル評価ツール	MP300（MICROPROSS 製）
非接触 R/W	EVPCD7010(IC カードデバッグ用)
	PD8080 (大和電機)、PD2002 (大和電機)
接触型 R/W	RW4040 (シャープ株式会社)
	SCR331　NTT コミュニケーションズ株式会社
IC カード LSI	SM4148
ソフトウェア	主な仕様
端末 PC 用 OS	Windows2000、WindowsXP
ROMICE 用ソフトウェア	CSIDE for ROMICE64 MK5 v3.31（コンピューテックス製）
AP／LIB Downloader	2.0.0.0　シャープ株式会社

MP300 用ソフトウェア	MPScope v1.12.0（MICROPROSS 製）

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

a. テスト構成

開発者が実施したテストの構成は表2-1、表2-2に示されたとおりである。開発者テストは、STにおいて識別されているTOE構成と一部異なるTOEテスト環境で実施されている（例えばICチップでは任意のタイミングで電源断を発生できないため、ICチップの代わりにSmart Card Simulatorを用い電源断のテストを実施等）。しかしながらその差異は評価者によって分析され、テスト結果に影響を及ぼさないことが確認されている。

b. テスト手法

日本電信電話株式会社のテストとシャープ株式会社では別々のテスト手法が用いられている。以下の表2-3、表2-4に各自詳細を示す。

表2-3　テスト手法（日本電信電話株式会社）

種類	手法の概要
実カードテスト	ツールを使用して C-APDU をカードに発行し、返送された R-APDU と期待する R-APDU を比較する。 返送された R-APDU が暗号化されている場合は、R-APDU を復号し、期待する R-APDU と比較する。
シミュレータ	ツールを使用して電源断の状態を発生させ、正しく電源断を復旧する処理が駆動することを、ツールのステップ実行もしくはブレークポイントの機能を利用して確認する。 ツールを利用してセキュリティ的な攻撃（メモリダンプ、改竄等）し、それを正しく検知し、セキュリティ対策の処理が駆動することを、ツールのステップ実行もしくはブレークポイントの機能を利用して確認する。

表2-4　テスト手法（シャープ株式会社）

種類	手法の概要
接触モードでエバボートを使用したテスト環境	端末 PC 上の自動評価用ソフトを使用し、接触型 R/W を経由して IC カード LSI をシミュレートする ROMICE、エバボードに C-APDU を送信、テストを行う。メモリの値を目視で確認する。 エバボードは、IC カードの機能の代わりをする。ROMIICE からエバボードの内部メモリにアクセスすることで、IC カードではアクセスできない内部 RAM 情報にアクセスできる。

種類	手法の概要
非接触モードでエバボードを使用したテスト環境	端末 PC 上の自動評価用ソフトを使用し、非接触 IC カードデバッグ用 R/W を経由して IC カード LSI をシミュレートする ROMICE、エバボードに C-APDU を送信、テストを行う。メモリの値を目視で確認する。 エバボードは、IC カードの機能の代わりをする。ROMIICE からエバボードの内部メモリにアクセスすることで、IC カードではアクセスできない内部 RAM 情報にアクセスできる。
接触モードにおける実 IC カードを使用したテスト環境	端末 PC 上の自動評価用ソフトを使用し、接触型 R/W を経由して IC カードに C-APDU を送信、テストを行う。自動評価ソフトを使用し、C-APDU を送信、受信した R-APDU が期待値と一致するか自動比較する。さらに、比較結果のログを取得し、エラーが 0 であることを確認する。 本テスト環境は、IC カードと R/W の通常の接続状態におけるテストを行う。端末 PC からのコマンドは、接触型 R/W を経由して IC カードに送信される。
非接触モードにおける実 IC カードを使用したテスト環境	端末 PC 上の自動評価用ソフトを使用し、非接触型 R/W を経由して IC カードに C-APDU を送信、テストを行う。自動評価ソフトを使用し、C-APDU を送信、受信した R-APDU が期待値と一致するか自動比較する。さらに、比較結果のログを取得し、エラーが 0 であることを確認する。 本テスト環境は、IC カードと R/W の通常の接続状態におけるテストを行う。端末 PC からのコマンドは、非接触型 R/W を経由して IC カードに送信される。

c. 実施テストの範囲

テストは日本電信電話株式会社によって計907項目、シャープ株式会社によって計2158項目実施されている。

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

d. 結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。評価者は、開発者テストの実施方法、実施項目の正当性を確認し、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

2.3.2 評価者テスト

1) 評価者テスト環境

評価者が実施したテスト（評価者独立テスト、侵入テスト）の構成は、評価者独立テストにおいては開発者テストと同等の構成である。侵入テストにおいては

オシロスコープ等の付加的なテスト機器を用いてテストを実施している。詳細は下記の2)を参照のこと。

2) 評価者テスト概説

評価者の実施したテスト（評価者独立テスト、侵入テスト）の概要は以下のとおり。

a-1. 評価者独立テスト構成

上記「2.3.1 2) 開発者テスト概説 a. テスト構成」で示したとおり、評価者が実施したテストの構成はSTの構成と一部異なるが、その差異はテストに影響しないことは評価者により検証済みである。

a-2. 侵入テスト構成

評価者独立テストのテスト構成に加え、テストパターンにより以下の3種類のテスト機器を電力解析のため使用している。

表2-5　テスト機器1

Instrument	Manufacturer	Model
Digital Storage Oscilloscope	LeCroy	WP7300A
PC		
Software	Brightsight	DPA Center V2.30 & Signalyer V2.09
Software	Brightsight	EMV Tool
Function generator	Agilent	33120A
Power supply	Agilent	3631A
Card Interface & Trigger Circuit	Brightsight	DPA Card Reader V1.1

表2-6　テスト機器2

Instrument	Manufacturer	Model
Digital Storage Oscilloscope	LeCroy	WP7300A
PC		
Software	Brightsight	DPA Center v2.30& Signalyser v.2.09
Function generator	Agilent	33120A
Power supply	Agilent	3631A
Card Interface & Trigger Circuit	Brightsight	Reset Board V1.1
Puls generator	Agilent	81110A

表2-7　テスト機器3

Instrument	Manufacturer	Model
Digital Storage Oscilloscope	LeCroy	WP7300A
PC		
Software	Brightsight	DPA Center V2.30 & Sideways 3
Software	Brightsight	EMV Tool
Function generator	Agilent	33120A
Power supply	Agilent	3631A
Card Interface & Trigger Circuit	Brightsight	DPA Card Reader V1.1

b-1. 評価者独立テスト手法

「2.3.1 2) 開発者テスト概説　a. テスト構成」と同様である。

b-1. 侵入テスト手法

評価者独立テストと同様の手法に加え、「2) 評価者テスト概説　a-2. 侵入テスト構成」で示した機器を用い、電力解析（SPA/DPA）を実施しTOEのPINや暗号化鍵の解読を試みている。

c. 実施テストの範囲

日本電信電話株式会社開発分においては、評価者独立テストを106項目、侵入テストを15項目、開発者テストのサンプリングによるテストを313項目、計434項目のテストを実施した。サンプリングテストは、セキュリティ機能全てをカバーするように開発者テストの約34.4%をサンプリングし後追い検証している。評価者独立テスト項目の選択基準としては、開発者自体が限界値分析、及びその限界値での全ペアテストを実施しているため評価者が独自に考えうる有用なテスト項目の余地は少ない。しかしながらAP管理部とCD管理部/住基APにおいてテスト担当者が異なり、テスト項目も各自に考案しているため、AP管理部とCD管理部/住基APに跨るテストが開発者において実施されていない。従って評価者はそこに着目し、AP管理部とCD管理部/住基APに跨る状態遷移に関連する独立テストを実施している。更に評価者は開発者が実施していないパラメタ値においても併せて独立テストを実施している。侵入テストにおいては、開発者の脆弱性分析の正当性を確認するために攻撃者が一般的に実施するコマンドスキャン等、及びCCサポート文書に記載された脆弱性の観点からの侵入テスト（例えばRSAのSPAに対する侵入テスト）を実施している。評価者は事前に論文、書籍、インターネットの公知のスマートカード脆弱性情報を調査し、それらの情報がCCサポート文書に集約されていることを検証しており、従って現状のスマートカードの脆弱性の観点は全て考慮されていると言える。

シャープ株式会社開発分においては、評価者独立テストを12項目、侵入テストを5項目、開発者テストのサンプリングによるテストを505項目、計522項目のテストを実施した。サンプリングテストは、セキュリティ機能全てをカバーするように開発者テストの約23.4%をサンプリングし後追い検証している。評価者独立テスト項目の選択基準としては、日本電信電話株式会社開発分同様開発者自身により網羅的なテストが実施されているため、評価者が独自に考えうる有用なテスト項目の余地は少ない。そのため評価者は開発者が実施していないパラメタ値に焦点を絞り、尚且つAPEの全てのセキュリティ機能をカバーしつつ評価者独立テストを実施している。侵入テストにおいては、開発者の脆弱性分析の正当性を確認するために攻撃者が一般的に実施するコマンドスキャン等、及びCCサポート文書に記載された脆弱性の観点からの侵入テスト（APEにおいてはバッファオーバフローのみ）を実施している。その他の観点は日本電信電話株式会社開発分で実施している。評価者は事前に論文、書籍、インターネットの公知のスマートカード脆弱性情報を調査し、それらの情報がCCサポート文書に集約されていることを検証しており、従って現状のスマートカードの脆弱性の観点は全て考慮されていると言える。

d. 結果

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

2.4 評価結果

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

3 認証実施

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

① 当該所見報告書でなされた指摘内容が妥当であること。
② 当該所見報告書でなされた指摘内容が正しく反映されていること。
③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。
④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。
⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。

認証機関は、ST及び評価報告書において、所見報告書及び認証レビューで指摘された問題点が解決されていることを確認した。

4 結論

4.1 認証結果

提出された評価報告書、当該所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL4及び保証コンポーネントAVA_MSU.3に対する保証要件を満たしていることを確認した。

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

表4-1 評価者アクションエレメント検証結果

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

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

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

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

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

ALC_DVS.1.1E	評価はワークユニットに沿って行われ、開発セキュリティ証拠資料がTOE開発環境のセキュア維持のための手段を記述しており、それが十分であること、その手段を実施した記録が生成されることを確認している。
ALC_DVS.1.2E	評価はワークユニットに沿って行われ、ALC_DVS.1.1Eで確認したセキュリティ手段が実施されていることを確認している。また、本評価時に行われたサイト訪問での調査方法も適切と判断される。
ALC_LCD.1.1E	評価はワークユニットに沿って行われ、使用されたライフサイクルモデルが開発者と保守手続きをカバーしており、その記述にある手続き、ツール、技法の使用が開発と保守に貢献していることを確認している。
ALC_TAT.1.1E	評価はワークユニットに沿って行われ、開発ツール証拠資料が明確であり、実装に用いられた開発ツールのステートメント及び実装依存オプションの意図を明確に定義していることを確認している。
テスト	**適切な評価が実施された**
ATE_COV.2.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。
ATE_DPT.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが上位レベル設計に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。

ATE_FUN.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果を含んでおりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。
ATE_IND.2.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。
ATE_IND.2.2E	評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。また、本評価時に行われたテスト実施方法も適切と判断される。
ATE_IND.2.3E	評価はワークユニットに沿って行われ、サンプリングテストを実施し、結果が期待されるべき結果と一貫していることを確認している。また、本評価のサンプリング方針及びテスト実施方法も適切と判断される。
脆弱性評定	**適切な評価が実施された**
AVA_MSU.3.1E	評価はワークユニットに沿って行われ、提供されたガイダンスがTOEのセキュアな運用に必要な情報を矛盾なく完全に記述していること、使用環境の前提事項、TOE以外のセキュリティ事項の要件がすべて明記されていること、ガイダンスの完全性を保証する手段を開発者が講じていることを確認している。
AVA_MSU.3.2E	評価はワークユニットに沿って行われ、提供されたガイダンスの管理者と利用者手続き、あるいはその他の手続き情報のみで、TOEを構成でき、TOEのセキュアな運用に関わる設定が行えることを確認している。
AVA_MSU.3.3E	評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEが非セキュアな状態に陥ったことを検出する手段及び対処方法を記述していることを確認している。

AVA_MSU.3.4E	評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEの全ての操作モードにおいてのセキュアな操作を提供していることを確認している。
AVA_MSU.3.5E	評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEが非セキュアな状態に陥ったことを検出する手段及び対処方法を記述していることを独自にテストを実施し確認している。
AVA_SOF.1.1E	評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされていることを確認している。
AVA_SOF.1.2E	評価はワークユニットに沿って行われ、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しいことを確認している。
AVA_VLA.2.1E	評価はワークユニットに沿って行われ、脆弱性分析が脆弱性に関する情報を考慮していること、識別された脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。
AVA_VLA.2.2E	評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。
AVA_VLA.2.3E	評価はワークユニットに沿って行われ、開発者がまだ扱っていない脆弱性の可能性を検査している。
AVA_VLA.2.4E	評価はワークユニットに沿って行われ、独立脆弱性分析に基づく侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテストの概要について報告がなされている。
AVA_VLA.2.5E	評価はワークユニットに沿って行われ、意図する環境においてTOEが低い攻撃力に対抗できることを侵入テストと脆弱性分析の結果から検査し、悪用され得る脆弱性及び残存脆弱性が存在しないことが報告されている。

4.2 注意事項

特になし。

5 用語

本報告書で使用された略語を以下に示す。

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

本報告書で使用されたTOE特有の略語を以下に示す。

住基カード	住民基本台帳用ICカード
住基ネット	住民基本台帳ネットワークシステム
CD	カードドメイン(Card Domain)、カードに一つだけ存在し、カード発行者が管理する領域。
AP	アプリケーション、ここではカードに搭載されるプログラムを表す。カードに複数存在し、発行後のカードに搭載が可能である。
SD	セキュリティドメイン、カードに搭載されるAPを管理する領域。
製造者	TOEをカードに搭載し、発行市町村へカードを納入する役割で、製造ベンダに対応する。
発行者	TOEの搭載されたカードを発行する役割で、市町村に対応する。
所有者	TOEの搭載されたカードの交付を受けてカードを所有する役割で、住民に対応する。
APE	アプリケーション実行環境、チップに搭載されるAPのドメイン分離を管理する。
CD管理部	CDのセキュリティに関する設定を管理する。
AP管理部	カードにロードして搭載されるAPを管理する。
住基AP	住基カードAP、住基カード用の市町村業務のためのAP
アダプタ	業務用端末上で動作するソフトウェアで、住基仕様で規定されたインタフェースに基づき、住基カードの実装に対応したコマンドメッセージを生成する。製造者毎に異なる住基カードの実装の差

	を吸収して共通のインタフェースで住基カードを利用できるようにするソフトウェアであり、業務ソフトウェアから呼び出される。
モジュール	カード上に搭載されたソフトウェアのプログラム単位での構成要素である。
プロセス	カード上に存在するモジュールがサブジェクトとして動作している状態である。
APDU	端末とICカードで取り交わされるデータ（コマンド・レスポンス）
C-APDU	コマンドAPDU。端末よりICカードに発行されるAPDU。
R-APDU	レスポンスAPDU。C-APDUに対しICカードが応答するAPDU。
ROMICE	インサーキットエミュレータ。ボード上のROMを代替しデバック等を行う製品。
エバボード	Evaluation Board。評価用の基板。

6 参照

[1] アダプタ対応型高速版住基カードソフトウェア セキュリティターゲット バージョン 1.92（2008年10月10日）日本電信電話株式会社

[2] ITセキュリティ評価及び認証制度の基本規程　平成19年5月　独立行政法人 情報処理推進機構　CCS-01

[3] ITセキュリティ認証申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-02

[4] ITセキュリティ評価機関承認申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル バージョン2.3 2005年8月 CCMB-2005-08-001　(平成17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2: セキュリティ機能要件 バージョン2.3 2005年8月 CCMB-2005-08-002　(平成17年12月翻訳第1.0版)

[10] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証要件 バージョン2.3 2005年8月 CCMB-2005-08-003　(平成17年12月翻訳第1.0版)

[11] ISO/IEC 15408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] 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2.3 2005年8月　(平成17年12月翻訳第1.0版)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] 補足-0512　平成17年12月

[18] アダプタ対応型高速版住基カードソフトウェア評価報告書 第2.1版 2008年10月

17日　株式会社電子商取引安全技術研究所　評価センター

[19] Application Notes and Interpretation of the Scheme, Evaluation Methodology for CC Assurance Classes for EAL5+, Version 1.0, 01 June 2004, Certification body of the BSI

[20] Supporting Document Mandatory Technical Document Application of Attack Potential to Smartcards Version 2.3