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9月25日** (IT**認証**7174)
認証番号	C0159
認証申請者	**株式会社 イオン銀行**
TOE**の名称**	**イオン・ボックス・バンク 業務アプリケーションソフトウェア**
TOE**のバージョン**	1.0
PP**適合**	**なし**
適合する保証パッケージ	EAL2 **及び追加の保証コンポーネント**ALC_FLR.1
開発者	**三菱電機インフォメーションシステムズ株式会社**
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5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 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 改訂第1版 (翻訳第1.2版)
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 改訂第1版 (翻訳第1.2版)

評価結果：合格

「イオン・ボックス・バンク 業務アプリケーションソフトウェア バージョン1.0」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、「イオン・ボックス・バンク 業務アプリケーションソフトウェア バージョン1.0」（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 株式会社 イオン銀行 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「1.5.8 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：　イオン・ボックス・バンク 業務アプリケーションソフトウェア
バージョン：　1.0
開発者：　三菱電機インフォメーションシステムズ株式会社

1.2.2 製品概要

TOEは、イオン・ボックス・バンクシステム（以降、ABBシステム）向け専用端末に搭載されるアプリケーションソフトウェアである。この端末は、スーパーマーケット等の店舗に設置される金融端末であり、住所変更や改印等の事務処理を受け付けるサービスを一般利用者に提供する。また、店舗で作業している行内関係者がセンターに送付する書類を受け付けるサービスを提供する。

TOEはこれらのサービスを安全に運用するために、投函された申請書の未達の検出や申請者の正当性の確認等のため申請書に添付された電子情報の暗号化機能、

サービスマンや行内関係者の識別認証機能を提供する。

1.2.3 TOEの範囲と動作概要

(1) TOE動作環境

図1-1にABBシステムの構成図を示す。図1-1に示すようにABBシステムは、スーパーマーケット等の店舗に設置され、住所変更届けや改印届け等の事務手続き業務やセンターに送付する書類を受け付ける端末と、一般利用者の口座番号等の情報を管理する、システム運用者の基幹システムであるセンターサーバ、及び両者が通信を行う通信網によって構成される（共同利用端末を使用する場合は、他行のシステムが使用するセンターサーバも存在する）。

TOEは端末に搭載され、各種サービスを提供するアプリケーションソフトウェアである。

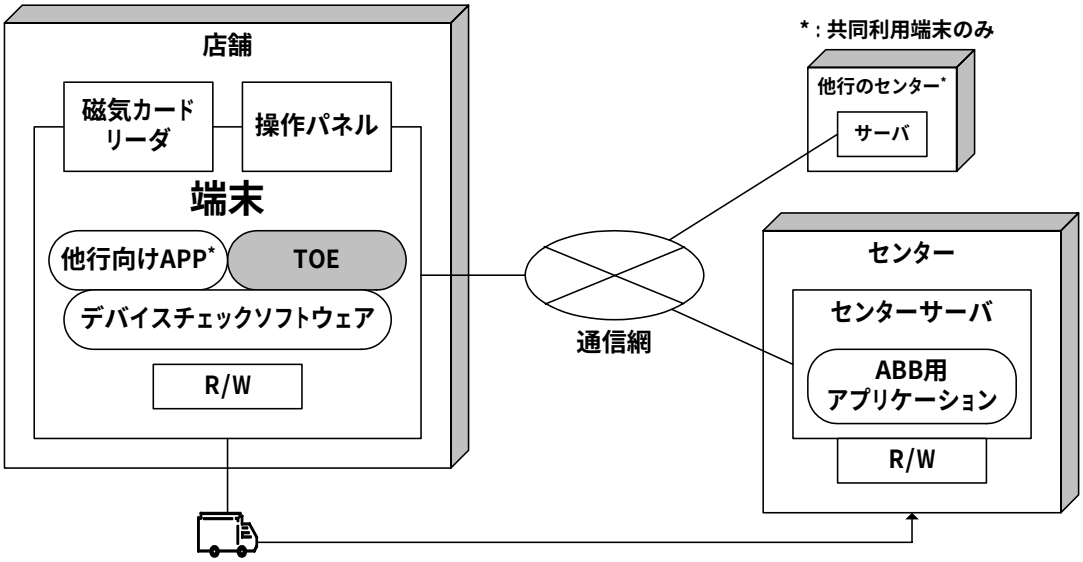

図1-1　ABBシステム構成図

図1-1の構成要素について説明する。

【端末】

利用者からの各種手続き業務を受け付ける専用端末である。この端末は申込書や書類を投函する投函口、利用者が操作を行うタッチパネル式の操作パネル、銀行カードから情報を読み取る磁気カードリーダ、事務手続き申込書に格納されたRFIDに対する読み書きを行うRFIDリーダライタ（以降、R/W）、筐体内部への不正操作から保護する物理錠、及び移動体通信を使用して通信網に接続し、センターサーバと通信を行うための無線通信モジュール等により構成される。

また、端末は単独利用端末、及び共同利用端末の2種類が存在する。単独利用端末にはTOEであるアプリケーションソフトウェアとオペレーティングシステム（以

降、OS)、保守作業時等に使用されるデバイスチェックソフトウェア等のソフトウェアが格納され、申請者が運営する銀行向けのサービスのみ提供する。共同利用端末には、上記ソフトウェアの他、他行向けに同様のサービスを提供する他行向けアプリケーションが格納される。これらのアプリケーションは、一般利用者の選択操作により排他的に起動される。

上記のOS、デバイスチェックソフトウェア、他行向けアプリケーションは評価範囲外である。

図1-2に端末の構成概要図を示す。

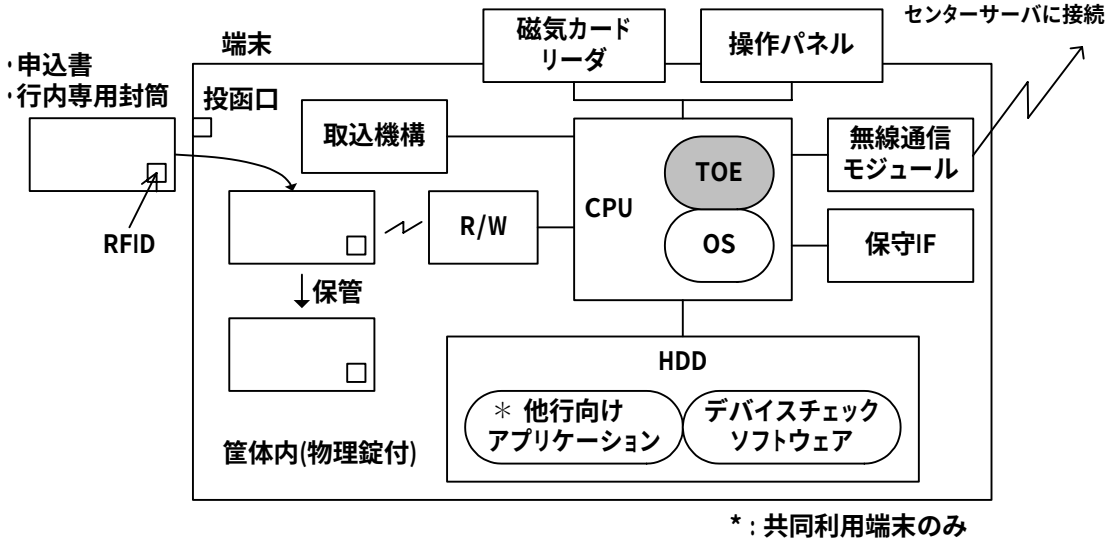

図1-2　端末構成概要

【センターサーバ】

システム運用者の基幹システムが運用されるセンターに設置されるサーバで、端末を使用する一般利用者の情報（口座番号等）を管理する。端末に入力された情報を、通信網を介して受信する。端末として共同利用端末が使用される場合は、他行のセンターに設置されるセンターサーバも存在する。センターサーバ、基幹システム等は（他行も含め）評価範囲外である。

(2) TOE動作概要

図1-1のシステムにおいて、一般利用者からの事務手続き受付処理に関する動作概要を示す。

・一般利用者は、住所変更届け等の事務手続きを行う場合、所定の申込書に必要事項を記入した後、磁気カードリーダを介して口座番号等の個人情報を入力する。その後、操作画面の指示に従い申込書（以降、ABB専用封筒）を端末に投函する。

・TOEは、端末に入力された個人情報を暗号化し、ABB専用封筒に格納されたRFIDに記録する。処理が終了したABB専用封筒はそのまま端末内に保管される。また、同時に個人情報、タグID情報等を暗号化し、センターサーバに送信する。

・投函されたABB専用封筒は、配送者によりセンターへ配送される。

・センターでは、送付されたABB専用封筒のRFIDから申請情報を読み出し、申込書が本人により記述されたものであることを確認する。また、端末から受信した受付情報から、その端末が間違いなく受け付けた申込書であることを確認し、実際の事務手続きが処理される。

また、端末は上記一般利用者からの受付処理以外に、店舗で受付業務を行っている行内関係者からの書類受け付け（以降、一括投函サービス）も行う。この書類は行内関係者が受領した一般利用者の申込書をまとめたもので、RFIDが格納された所定の封筒（以降、行内専用封筒）に入れられる。そして、行内関係者は必要な情報を操作パネル、磁気カードリーダを介して入力し、専用の投函口から行内専用封筒を投函する。TOEは入力された情報を暗号化し、センターサーバに送信する。

本サービスは行内関係者のみ使用することができ、一般利用者は使用することができない。

(3) TOE範囲

TOEは、図1-2に示す端末に搭載されたアプリケーションソフトウェアである。
なお、端末に搭載されるOS、デバイスチェックソフトウェア、及び他行向けアプリケーションはTOEには含まれない。

1.2.4 TOEの機能

TOEで提供される機能は、ABBシステムが提供する業務サービスに関する機能（下記 1.2.4.1）と、そのサービスをセキュアに実施するためのセキュリティ機能（下記1.2.4.2）に大別される。
今回のセキュリティ評価は、このセキュリティ機能に対して実施されている。

1.2.4.1 業務サービスに関連する機能

【事務処理受付及び一括投函サービス】
TOE動作概要に記述した、一般利用者及び行内関係者に対して業務サービスを提供するための機能である。

【保守機能】
保守員と警備会社に対して定期点検、及び障害発生時の点検サービスを提供する機能。本機能は後述する保守認証に成功した場合のみ使用可能となる。

【設定機能】

保守員が操作パネルを介して端末固有の情報(IPアドレスやホスト名等)を設定・変更できる機能である。本機能は保守識別認証に成功した後、更に後述する設定認証に成功した場合のみ、使用可能となる。

1.2.4.2 セキュリティ機能

TOEは、端末に入力された個人情報の機密性を確保するための暗号化機能と、保守機能・設定機能・一括投函サービスの各機能を使用する利用者の識別認証機能をセキュリティ機能として提供する。

以下ではその詳細を述べる。

【暗号化機能】

本機能は、一般利用者のカードから読み込まれ端末に入力された、個人情報の機密性を確保するために、RFIDに記録される申請情報の暗号化、センターサーバに送付される受付情報の暗号化を行う機能である。申請書の封筒に添付されたRFIDに記録される情報は、配送中においてスキミング等の手段で容易に、また秘密裏にアクセスされるリスクがあり、この暗号化機能によりそうした情報の漏洩を防ぐことが可能となる。

一般利用者、及び行内関係者からの事務手続き受付後の暗号化機能の動作フローを下記に示す。

＊一般利用者、及び行内関係者からの受付後

・独自乱数生成アルゴリズム「PRNG based on MISTY1」により128bits乱数を発生（MISTY1の暗号鍵として使用）

・端末への入力データ（受付情報）を暗号アルゴリズム「MISTY1」で暗号化し、センターサーバに送付

・端末への入力データ（申請情報）を暗号アルゴリズム「MISTY1」で暗号化し、RFIDに書き込み（一般利用者からの受付時のみ実施）

・生成した暗号鍵を暗号アルゴリズム「RSA」を用いて暗号化し、センターサーバに送付（センターサーバの公開鍵（1024bits）を使用）

・暗号鍵を破棄（ゼロクリア）

【識別認証機能】

本機能は、保守機能、設定機能、及び一括投函サービスを使用する前に、その利用者を識別認証する機能であり、下記3種類の機能により構成される。

・保守識別認証機能
端末の保守機能を使用する前に保守員、及び警備会社を識別・認証する機能。TOEが表示する特定の画面において、利用者が行う所定操作を検出することで、識別を行う。その後、操作パネルから入力されたPIN（以降、保守PIN）と、TOE内に格納された保守PINによる認証を行う。続けて3回認証に失敗した場合、保守PINの入力を5分間受け付けない。

・設定識別認証機能
端末の設定機能を使用する前に保守員を識別認証する機能。上記保守識別認証に成功した後、本機能を使用することができ、本認証に成功した後、設定機能を利用できる。TOEが表示する特定の画面において、利用者が行う所定操作を検出することで、識別を行う。その後、操作パネルから入力されたPIN（以降、設定PIN）と、TOE内に格納された設定PINによる認証を行う。続けて3回認証に失敗した場合、設定PINの入力を3分間受け付けない。

・行内関係者識別認証機能
一括投函サービスを利用する行内関係者を識別認証する機能。TOEが表示する特定の画面において、利用者が行う所定操作を検出することで、識別を行う。その後、PIN（以降、店舗PIN）による認証を行う。続けて3回認証に失敗した場合、店舗PINの入力を3分間受け付けない。TOEは操作パネルから入力された店舗PINからSHA-1によるダイジェストを生成し、TOE内に格納されているダイジェストと比較することで認証を行う。

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「イオン・ボックス・バンク 業務アプリケーションソフトウェア 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]のいずれか) 附属書A、CCパート2（[6][9]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]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、「イオン・ボックス･バンク 業務アプリケーションソフトウェア バージョン 1.0 評価報告書」(以下「評価報告書」という。) [13]に示されている。なお、評価方法は、CEM（[11][12]のいずれか）に準拠する。

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5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、EAL2追加である。
追加の保証コンポーネントは、ALC_FLR.1である。

1.5.3 セキュリティ機能

本TOEのセキュリティ機能は、以下に示すセキュリティ機能要件を実現している。

・暗号化機能
・識別・認証

本TOEのセキュリティ機能詳細については、1.2.4を参照されたい。

1.5.4 脅威

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

表1-1　想定する脅威

識別子	脅　威
T.RFID_INFO	不慮の事故や搬送中の盗難により、ABB専用封筒が第三者に手渡り、市販のR/Wを用いてRFIDの記録情報を読み出すことで、申請情報が暴露されるかもしれない。

1.5.5 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。

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.PRIVACY	端末は、一般利用者や行内関係者が入力し、利用したことを示す受付情報の機密性を維持しなければならない。
P.MAINTE	許可された役割だけが端末の保守機能や設定機能を使用することができる。
P.OPE_POST	一括投函サービスは、行内関係者のみが使用できなければならない。

1.5.6 構成条件

本TOEは、イオン・ボックス・バンクシステム向け専用端末である、共同利用端末もしくは単独利用端末上にインストールする必要がある。また、本TOEは下記OS上で動作する。

動作OS： Microsoft Windows XP Embedded SP2（日本語版）

1.5.7 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.PIN	保守PIN、設定PIN、店舗PINは第三者に知られないように管理される。
A.OPERATE	運用者は、ABBシステムで使用する情報(個人情報(入力中も含む)、暗号鍵、ダウンロードするファイル)を改ざん・漏洩されないように管理する。また、端末が接続するサーバを運用者だけが利用できるように管理する。
A.CASE_KEY	端末には端末内部にアクセスするための物理錠が設置され、その鍵は正当な人(配送者と警備会社)のみが使用できる。
A.NO_HARM	配送者とサービスマン(保守員と警備会社)は、課せられた役割として許可された作業のみを遂行し、悪意を持った行為を行わない(e.g. 筐体内部の基板等のハードウェアに対する不正行為等)。
A.CASE	端末には、入力中の個人情報の盗み見を防止する手段が操作パネルに設置される。
A.CHANNEL	端末は特定のサーバ(センターサーバ)にのみ接続され、その通信路は盗聴・改ざんから保護されている。
A.APP	TOEやTOEが使用するデータを改ざんしない信頼できるソフトウェアのみが端末に搭載される。
A.ACCESS	端末は、通常運用時以外(e.g. 保守)には一般利用者や行内関係者がアクセスできないように管理される。

1.5.8　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表1-4に示す。

表1-4　添付ドキュメント

ドキュメント名	バージョン
イオン・ボックス・バンクシステムユーザマニュアル(端末編) ～単独利用・共同利用端末共通～	1.1
イオン・ボックス・バンクシステムユーザマニュアル (センター編)	1.00
イオン・ボックス・バンクシステムユーザマニュアル (申込書類回収業務提携先編)～単独利用端末～	1.00
コンビニ・ボックス・バンクシステムユーザマニュアル (申込書類回収業務提携先編)～共同利用端末～	1.00

イオン・ボックス・バンクシステム保守手順書(保守会社編) ～単独利用端末～	1.00
コンビニ・ボックス・バンクシステム保守手順書(保守会社編) ～共同利用端末～	1.00
イオン・ボックス・バンクシステム保守手順書 (警備会社/保守会社共通編)～単独利用端末～	1.1
コンビニ・ボックス・バンクシステム 保守手順書 (警備会社/保守会社共通編)～共同利用端末～	1.00
イオン・ボックス・バンクシステム運用計画書 ～単独利用端末～	1.2
コンビニ・ボックス・バンクシステム運用計画書 ～共同利用端末～	1.1
イオン・ボックス・バンクシステムインストールガイド ～単独利用端末～	1.0
コンビニ・ボックス・バンクシステムインストールガイド ～共同利用端末～	1.0

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10月に始まり、平成20年5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20年2月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付と運用・ライフサイクルの各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成20年2月に開発者サイトで開発者のテスト環境を使用し、開発者が実施したテストのサンプリングチェック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

開発者が実施したテストの構成を図2-1に示す。

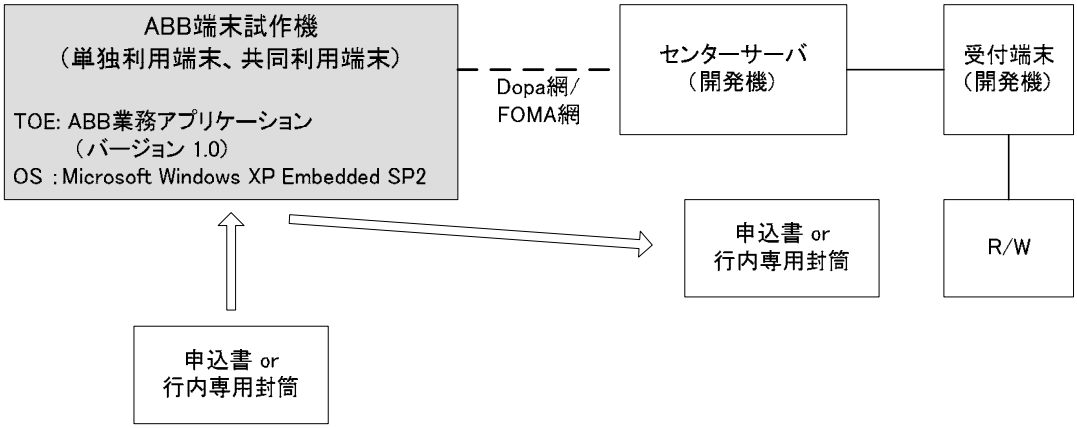

図2-1　開発者テストの構成図（テスト環境(1)）

また、上記テスト環境(1)以外に、開発PC上に暗号・復号処理検査ツール、及び乱数検定ツールを搭載し、サブシステムレベルのテストを行う環境（テスト環境(2)）も使用する。

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

開発者テストは、1)に示すとおり3種類のテスト環境を用いて実施されている。テスト環境(1)は、考慮すべき前提条件を満たし、ハードウェア及びソフトウェア構成ともSTにおいて識別されている構成と一貫した環境であることが評価者により確認されている（テスト環境の端末については操作用キーボード、マウス、及び画面キャプチャ用アプリケーションが搭載されており、運用端末とは差異があるが、これらはTOEのセキュリティ機能の動作には影響を与えないことが検証されている）。

このテスト環境(1)は、TSFI及びセキュリティ機能のふるまいを確認するために使用される。

テスト環境(2)は開発PC上に暗号機能を実現するサブシステム（暗号サブシステム）、及び各種検査ツールを搭載し、サブシステムレベルのテストを実施するための環境である。ここで使用される検査ツールに関しては、評価者がその実装を検査することにより、適切性が確認されている。

b.テスト手法

テストには、以下の手法が使用された。

①TSFIを利用してセキュリティ機能のふるまいを確認する

確認手段としては、TOE操作画面上での確認、通信ログの確認、サーバ側での通信データ確認を行う（テスト環境(1)を使用）

②TSFIから直接操作できないセキュリティ機能のテストに関しては、検査ツールを用いて暗号サブシステムのふるまい（鍵生成、暗号・複号処理）を確認する（テスト環境(2)を使用）

c.実施テストの範囲

テストは開発者によって9項目（各項目内では更に複数のパラメータの組み合わせに関して正常系、異常系の小項目が存在）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セキュリティ機能の実施に関わる全ての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。

d.結果

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

2.3.2 評価者テスト

1) 評価者テスト環境

評価者が実施したテストの構成は、開発者テストと同様の構成である。

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

評価者が実施したテストの構成は2.3.1を参照のこと。

b.テスト手法

テストには、以下の手法が使用された。

①TSFIを利用してセキュリティ機能のふるまいを確認する。

確認手段としては、TOE操作画面上での確認、通信ログの確認、サーバ側での通信データ確認を行う（テスト環境(1)を使用）。

②TSFIから直接操作できないセキュリティ機能のテストに関しては、検査ツールを用いて暗号サブシステムのふるまい（鍵生成、暗号・複号処理）を確認する（テスト環境(2)を使用）。

c.実施テストの範囲

評価者が独自に考案したテストを16項目、開発者テストのサンプリングによるテストを9項目、計25項目（各項目内では更に複数のパラメータの組み合わせに関して正常系、異常系の小項目が存在）のテストを実施した。テスト項目の選択基準として、下記を考慮している。

① 開発者テストのサンプリングについては、セキュリティ機能実施に関わる全ての外部インタフェースを網羅するために全ての開発者テスト項目を実施する
② 開発者テストに対するカバレッジ分析から不足していると判断される外部インタフェース（セキュリティ機能の実施には関係しないが機能に何らかの影響を与える可能性があるインタフェース）に関するテストを実施する
③ 開発者テストに対するカバレッジ分析からテストするパラメータ及びその組み合わせが不足していると判断されるテストを実施する
④ 外部インタフェースからの入力値（不正カード、不正操作等）に対する異常系、例外処理に関するテストを実施する
⑤ 脆弱性の観点からセキュリティ機能のバイパスの可否を確認するためのテストを実施する

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。侵入テストにおける一部のテスト結果は期待されるふるまいと相違したが、その原因は特定され適切に対処された。最終的に侵入テストにおいてテストされた脆弱性は、悪用不可能であると判断された。それ以外のテスト結果は期待される結果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EAL2及び保証コンポーネントALC_FLR.1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_INT.1.1E	評価はワークユニットに沿って行われ、TOE参照、TOE概要、及びTOE記述が正しく記述さ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、TOE参照、TOE概要、及びTOE記述が相互に一貫していること確認している。
ASE_CCL.1.1E	評価はワークユニットに沿って行われ、CCの適合主張の有効性を確認している。
ASE_SPD.1.1E	評価はワークユニットに沿って行われ、セキュリティ課題が明確に定義されていることを確認している。
ASE_OBJ.2.1E	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が明確に定義されていることを確認している。
ASE_ECD.1.1E	評価はワークユニットに沿って行われ、拡張セキュリティ要件が含まれていないため非適用であることを確認している。
ASE_ECD.1.2E	評価はワークユニットに沿って行われ、拡張セキュリティ要件が含まれていないため非適用であることを確認している。
ASE_REQ.2.1E	評価はワークユニットに沿って行われ、SFR、SARは明確に、曖昧さなく十分に定義され、また内部的に一貫していること、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要約仕様の記述がどのように各SFRを満たすかを示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TOE概要及びTOE記述と一貫してい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_CMC.2.1E	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。
ALC_CMS.2.1E	評価はワークユニットに沿って行われ、TOEの構成リストが管理され、構成要素が一意に識別可能なことを確認している。
ALC_DEL.1.1E	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。
ALC_FLR.1.1E	評価はワークユニットに沿って行われ、欠陥修正手続き証拠資料がすべてのセキュリティ欠陥を追跡するために使用される手続き、及びTOE利用者に必要な情報を提供するための手段を含み、この手続きの適用により、欠陥訂正方法の調査状況と同時に各々のセキュリティ欠陥の性質と影響に関する記述が提供されることを確認している。
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、機能仕様にTSFが完全に表現されていること、機能仕様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_TDS.1.1E	評価はワークユニットに沿って行われ、TOE設計にてすべてのサブシステムが記述され、各サブシステムの特性が識別されていることを確認している。
ADV_TDS.1.2E	評価はワークユニットに沿って行われ、TOE設計にすべての機能要件が含まれ、具体化されていることを確認している。
ADV_ARC.1.1E	評価はワークユニットに沿って行われ、アーキテクチャ設計に自己保護、ドメイン分離、非バイパス性が記述され、TSFが保護され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_OPE.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運用環境のセキュリティ対策方針を満たすために従うべきセキュリティ手段を記述してあることを確認している。
AGD_PRE.1.1E	評価はワークユニットに沿って行われ、準備手続きがTOEのセキュアな準備を記述し、STの運用環境のITセキュリティ方針に従った環境が構築可能であることを確認している。
AGD_PRE.1.2E	評価はワークユニットに沿って行われ、準備手続きを元に評価者がセキュアにTOEと準備環境を構築可能なことを実行し確認している。
テスト	**適切な評価が実施された**
ATE_COV.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項目が正確にTFSIと関連付けられてい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、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。
ATE_IND.2.3E	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。
脆弱性評定	**適切な評価が実施された**
AVA_VAN.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。
AVA_VAN.2.2E	評価はワークユニットに沿って行われ、潜在的脆弱性を識別するために公知の情報源に関する脆弱性探索を実施している。
AVA_VAN.2.3E	評価はワークユニットに沿って行われ、TOEの潜在的な脆弱性を識別するために、ガイダンス証拠資料、機能仕様、TOE設計、及びセキュリティアーキテクチャ記述を使用して、TOEの独立脆弱性分析を実施している。

AVA_VAN.2.4E	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。

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 Functionality

本報告書で使用されたTOE特有の略語を以下に示す。

ABB	イオン・ボックス・バンク
PIN	Personal Identification Number 本書では、保守PIN、設定PIN、店舗PINを指す。
PRNG	Pseudorandom Number Generator 擬似乱数生成器
RFID	Radio Frequency Identification ICタグ
R/W	RFIDのリーダライタ

本報告書で使用された用語を以下に示す。

イオン・ボックス・バンク システム	店舗に設置された専用端末において、利用者からの事務手続き依頼を受け付けるサービスを提供するためのシステムの総称。
一般利用者	端末より事務手続きサービスを利用するユーザ。
受付情報	端末からセンターサーバに送信される情報。 端末に入力された個人情報、封筒のタグID、日付等で構成されたものが暗号化される。
警備会社	TOEの保守機能を使用できるサービスマンで、端末の異常を検知した場合、緊急的な一次対処を行う。さらに、保守員による保守の際には同行する(保守員は物理錠を持っていないため)。
行内関係者	店舗において端末の一括投函サービスを利用するユーザ。行内専用封筒にて書類を投函する。
申請情報	一般利用者が端末に投函する申込書に格納されているRFIDに記録される情報。 端末に入力された個人情報、日付等で構成されたものが暗号化される。
タグID	RFIDに記録されている固有の識別子。
端末	イオン・ボックス・バンク システム向けの専用端末。スーパーマーケット等の店舗に設置される。 申請者が運営する銀行向けのサービスのみを提供する単独利用端末と、他行向けのサービスも提供する共同利用端末がある。
配送者	端末に投函されたABB専用封筒や行内専用封筒をセンターに配送する業者。物理錠を持っている。
保守員	TOEの保守機能や設定機能を使用できるサービスマンで、定期的なメンテナンスや障害時の二次対応(e.g. デバイス交換)を行う。

6 参照

[1] イオン・ボックス・バンク 業務アプリケーションソフトウェア
セキュリティターゲット バージョン 1.6（2008年3月12日）
三菱電機インフォメーションシステムズ株式会社

[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 3.1 September 2006 CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version　3.1 September 2006 CCMB-2006-09-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version　3.1 September 2006 CCMB-2006-09-003

[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3.1 改訂第1版　2006年9月 CCMB-2006-09-001　(平成19年3月翻訳第1.2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3.1 改訂第1版　2006年9月 CCMB-2006-09-002　(平成19年3月翻訳第1.2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3.1 改訂第1版　2006年9月 CCMB-2006-09-003　(平成19年3月翻訳第1.2版)

[11] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 3.1 September 2006 CCMB-2006-09-004

[12] 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1版　2006年9月 CCMB-2006-09-004　(平成19年3月翻訳第1.2版)

[13] イオン・ボックス・バンク 業務アプリケーションソフトウェア 評価報告書 第1.1版 2008年5月7日　株式会社電子商取引安全技術研究所 評価センター