認　証　報　告　書

独立行政法人 情報処理推進機構
理事長　藤原　武平太
原紙押印済

評価対象

申請受付年月日(受付番号)	**平成16年10月22日（IT認証4036）**
認証番号	C0024
認証申請者	**株式会社 三菱東京UFJ銀行**
TOEの名称	**コンビニ・ボックス・バンク業務アプリケーションユニット**
TOEのバージョン	**バージョン** 1.0
PP適合	**なし**
適合する保証要件	EAL2
TOE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18年1月1日
(初回発行日：平成17年3月9日)

独立行政法人 情報処理推進機構
セキュリティセンター 情報セキュリティ認証室
技術管理者　田渕　治樹

評価基準等：「ITセキュリティ評価機関に対する要求事項」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 2.1
② Common Methodology for Information Technology Security Evaluation Version 1.0
③ CCIMB Interpretations-0407

評価結果：合格

「コンビニ・ボックス・バンク業務アプリケーションユニット，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製品等のセキュリティ認証業務実施規程に従い、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、「コンビニ・ボックス・バンク業務アプリケーションユニット, 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 三菱東京UFJ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「1.5.9 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:	コンビニ・ボックス・バンク業務アプリケーションユニット
バージョン:	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

本製品は、コンビニエンスストアに設置される金融端末であるコンビニ・ボックス・バンク端末（以下「CBB端末」という。）に実装されるアプリケーションユニットであり、「コンビニ・ボックス・バンク業務アプリケーションソフトウェア」（以下「SW」という。）及び「TURBOMISTY」（Hardware Security Module；以下「HSM」という。）で構成される。CBB端末はコンビニ・ボックス・バンクシステム（以下「CBBシステム」という。）の構成要素の一つであり、一般利用者はこのCBB端末を使用することで、従来銀行窓口で行われている事務手続きサービスや相談予約サービスをコンビニエンスストアで利用することができる。

本製品は、これらのサービスを一般利用者に提供するための申込受付機能、申込書取込機能、通信機能を備えるとともに、一般利用者が入力する暗証番号の機密性を確保

するためのセキュリティ機能を提供する。

1.2.3 TOEの範囲と動作概要

(1) CBBシステムの概要

CBBシステムの構成図を図 1-1に示す。この図において、TOEは、コンビニエンスストアに設置されたCBB端末内（図中の灰色部分）にある。

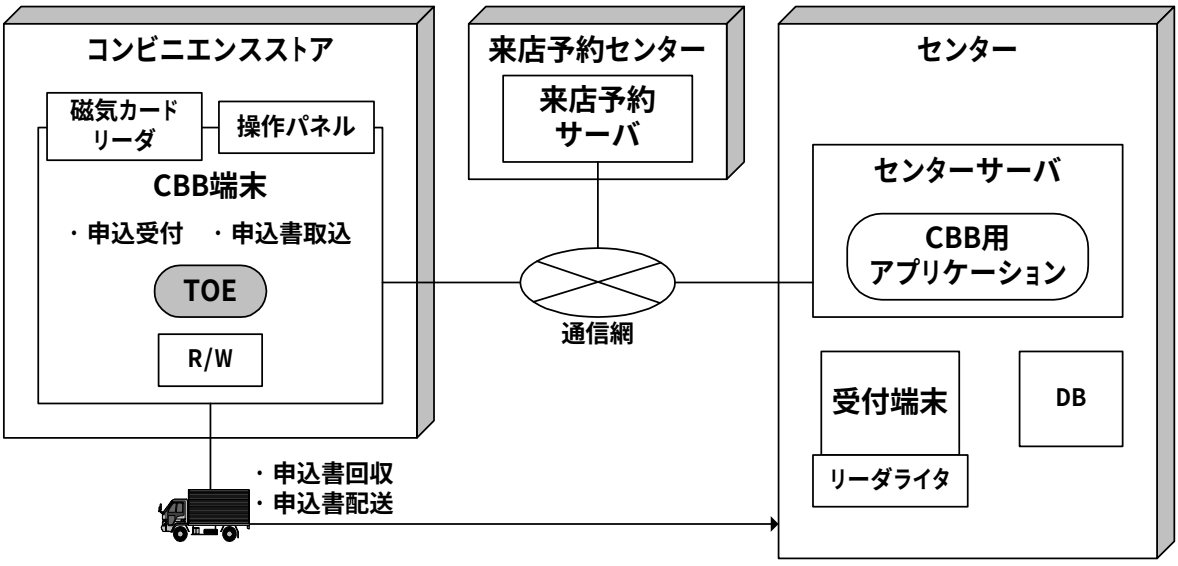

図 1-1 CBBシステムの構成図

CBBシステムは、センターサーバ、来店予約サーバ、及びCBB端末で構成され、それぞれがセンター、来店予約センター、及び複数のコンビニエンスストアに設置される。CBB端末は通信網を介してセンターサーバ及び来店予約サーバに接続されており、各サーバと通信することにより住所変更届けなどの事務手続きサービスと支店来店予約などの相談予約サービスを一般利用者に提供するものである。

特に住所変更届けなどの事務手続きサービスでは、CBB端末とセンターサーバの間の通信に加えて、一般利用者が各種必要事項を記入してCBB端末内に投函した申込書（以下「申込書」という。）が所定の配送業者（以下「配送者」という。）によってセンターに配送される。配送された申込書は、センターの受付端末によって所定の情報を読み取られ、一般利用者本人による申し込みであることが確認された後、申込書の内容に従って事務手続きが処理される。

センター及び来店予約センターは、CBBシステムを運用する金融機関によって管理される。特に一般利用者の暗証番号や個人情報は、センター内に従来からある基幹システムのデータベース（DB）を使用して管理されている。

なお、センターサーバ及び来店予約サーバは、本評価の対象外である。

(2) CBB端末の構成とTOEの動作概要

CBB端末の構成図を図 1-2に示す。TOEはSWとHSMで構成される部分（図中の灰色部分）であり、この両者により保護資産である一般利用者の暗証番号の機密性を確保する。

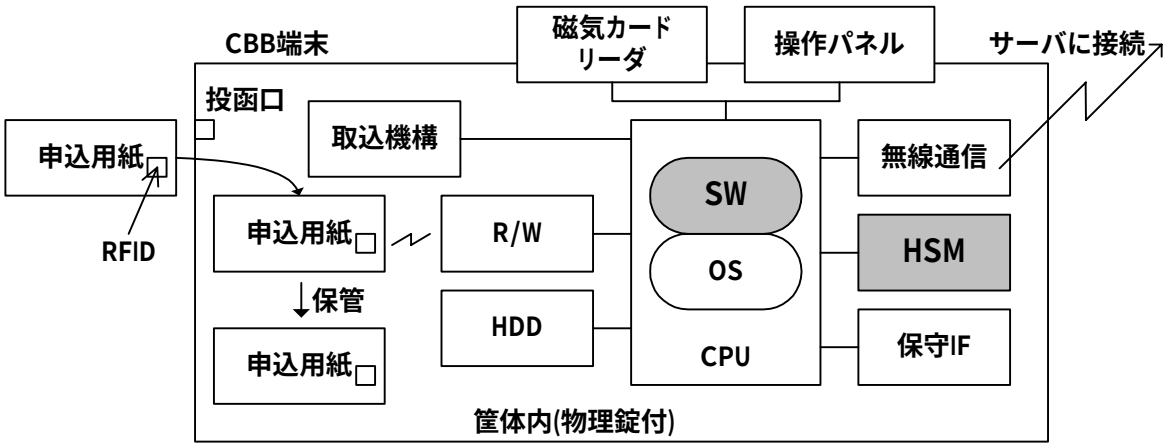

図 1-2 CBB端末の構成図

(a) 一般利用者の利用時の動作概要

住所変更届けなどの事務手続きを行う場合、一般利用者は磁気カードリーダにキャッシュカードを挿入し、操作パネルからその暗証番号を入力後、各種必要事項を記入した所定の申込書をCBB端末の投函口より投函する。

このとき、SWは磁気カードリーダを介してキャッシュカードから口座番号を、RFIDリーダライタ（以下「R/W」という。）を介して投函された申込書に格納されているRFIDからタグID（各RFIDを一意に識別できるユニークな番号）を読み出す。その一方で、SWは入力された暗証番号や口座番号など（以下「申込情報」という。）を暗号化し、R/Wを介してRFIDに記録する。この申込情報は、申し込みが口座名義を持つ本人によるものであることを確認するためにセンターで用いられる。

さらに、SWは読み出したタグIDや口座番号など（以下「受付情報」という。）を暗号化し、通信網を利用してセンターサーバへ転送する。この受付情報は、CBB端末が申し込みを受け付けたことを示すログとしてセンターで用いられる。

なお、HSMが上記の申込情報及び受付情報の暗号化を行う。

一方、支店来店予約などの相談予約を行う場合は、一般利用者が操作パネルから入力した個人名や連絡先電話番号などの個人情報は、TOEではなくOS組み込みのHTTPSプロトコルによって保護された状態で転送される。

(b) 保守作業時の動作概要

主な保守作業には、定期及び障害時の点検作業と、申込情報と受付情報の暗号化に使用する暗号鍵の更新作業がある。保守作業を担当するサービスマン（保守員と警備会社）は、操作パネルを使用した認証に成功した後のみ、これらの保守作業を行うことができる。

このとき、SWはサービスマンの識別・認証を行うとともに、認証成功後に保守IFから更新用の暗号鍵を読み込んでHDDに格納する。

1.2.4 TOEの機能

TOEが備える機能を以下に示す。

(1) アプリケーション機能

- 申込受付機能
  事務手続き時に、操作パネルや磁気カードリーダより一般利用者が入力した暗証番号や口座番号などの申込情報をR/Wを介して申込書のRFIDに記録する。
  また、相談予約時に、一般利用者が入力した支店来店時間などの情報を受け付ける。
- 申込書取込機能
  事務手続き時に、各種必要事項を記入した申込書を投函口よりCBB端末内に取り込んで保管するために、取込機構を制御する。なお、CBB端末内に投函された申込書は、筐体に設置された物理錠を開錠しない限り取り出せない。

(2) サポート機能

- 通信機能
  - アップロード
    事務手続き時に、タグIDや口座番号などの受付情報をセンターサーバに転送する。
    また、相談予約時に、一般利用者が入力した支店来店時間などの情報を来店予約サーバに転送する。
    さらに、CBB端末自身の稼動状況をセンターサーバに送信する。
  - ダウンロード
    CBB端末内のファイルを更新するために、センターサーバと来店予約サーバからデータファイル(e.g. 予約可能な支店･日時の情報を含むデータファイル）をダウンロードする。このデータファイルは運用者だけがサーバに格納できる。

(3) セキュリティ機能

- 暗号化機能
  事務手続き時に、暗証番号や口座番号などの申込情報とタグIDや口座番号などの受付情報を暗号化する。なお、これらの情報は、RFIDに記録する前、及びセンターサーバへ転送する前に暗号化する。

・ 保守機能
保守作業を開始する前に、正規のサービスマンかどうかを識別・認証し、認証成功後のみ定期及び障害時の点検機能と暗号鍵の更新機能を提供する。さらに暗号鍵更新機能では、更新用の暗号鍵が当該CBB端末用の正しいものかどうかをチェックする。

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セキュリティ認証申請等の手引き」[2]、「ITセキュリティ評価機関に対する要求事項」[3]、「ITセキュリティ認証申請者・登録者に対する要求事項」[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「コンビニ・ボックス・バンク業務アプリケーションユニット セキュリティターゲット」（以下「本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][14]のいずれか) 附属書C、CCパート2（[6][9][12][15]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][16]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、「コンビニ・ボックス・バンク業務アプリケーションユニット, バージョン 1.0 評価報告書」（以下「本評価報告書」という。）[23]に示されている。なお、評価方法は、CEMパート2（[17][18][19]のいずれか）に準拠する。また、CC及びCEMの各パートは補足（[20][21][22]）の内容を含む。

1.4 評価の認証

認証機関は、評価機関が作成した、本評価報告書、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17年2月の評価機関による本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

本STが規定するTOEの評価保証レベルは、EAL2適合である。

1.5.3 セキュリティ機能強度

本STは、最小機能強度として、”SOF-基本”を主張する。

本TOEは、物理錠が設けられた筐体内に格納される。また、アクセスするサーバは運用者によって管理されている特定のサーバに限定されており、その通信路は保護されている。このような環境で本TOEにアクセス可能な悪意のある人間はlow attack potentialであるため、最小機能強度はSOF-基本で妥当である。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能は、以下のとおりである。なお、一般利用者の利用時におけるTOEの暗号処理の流れを図 1-3に示す。

(1) 暗号化機能（SF.CRYPT）

RFIDに申込情報を記録する前、及び受付情報をセンターサーバに転送する前に、TOEの一部であるHSMがこれらの情報を暗号化する機能である。

TOEは申込情報や受付情報を暗号化するにあたり、まずHSMにてアルゴリズム「RSA（PKCS#1準拠、鍵長1024bits）」で暗号化MISTY鍵を復号し、復号結果に含まれている鍵確認情報と、暗号化MISTY鍵情報のヘッダに含まれている鍵確認情報とを比較する。これらが一致する場合に、復号されたMISTY鍵が正しい暗号鍵であると判断し、HSMにてアルゴリズム「MISTY1（暗号技術仕様書 MISTY1 (updated 2002年5月13日)準拠、鍵長128bits）」で申込情報と受付情報を暗号化する。

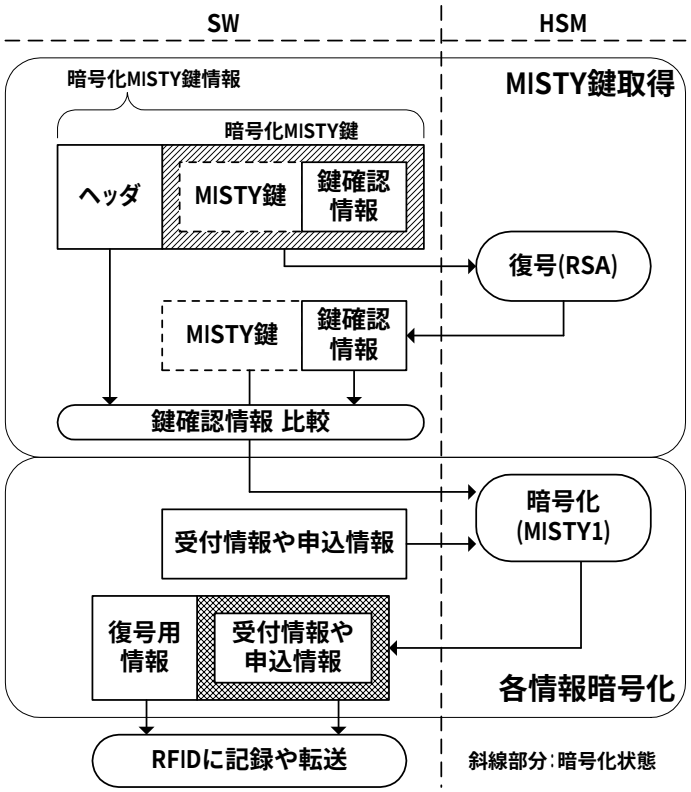

図 1-3 TOEの暗号処理

(2) 保守機能（SF.MANAGE）

サービスマンが保守作業を開始する前に、正規のサービスマンかどうかを識別・認証し、認証成功後に暗号鍵の更新を行う機能である。

識別・認証機能では、PINを用いたメカニズムにより認証を行う。TOEはサービスマンの識別・認証前に、一般利用者に対するCBB端末としてのサービス提供のみを許可する。最後に成功した認証以降においてPIN認証が3回失敗した場合、PINの入力を5分間拒否する。PIN認証が成功した場合のみ、TOEはサービスマンの役割を維持し、暗号化MISTY鍵情報の更新命令を実施する。

暗号鍵更新機能では、暗号化MISTY鍵情報を更新するとき、TOEが保有する端末固有情報と暗号化MISTY鍵情報のヘッダに含まれている端末固有情報とを比較し、一致した場合のみ新しい暗号化MISTY鍵情報を受け入れる。

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。

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申込書盗難により、申込書が第三者に手渡り、市販のR/Wを用いてRFIDの記録情報を読み出すことで、暗証番号が暴露されるかもしれない。

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。

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	CBB端末は、一般利用者が入力し、利用したことを示す受付情報と申込情報の機密性を維持しなければならない。これは、個々の情報（暗証番号以外）では機密性を維持する必要はないが、すべてを合わせた全体の情報としては、プライバシーの観点からCBB端末が機密にしなければならない。また、相談予約にて一般利用者が入力した情報(個人名や連絡先など)もプライバシーの観点からCBB端末が機密性を維持しなければならない。
P.MAINTE	サービスマンのみがCBB端末の保守作業を行うことができる。

1.5.7　構成条件

本TOEは、CBB端末の筐体内に実装されるSW（ソフトウェア）とHSM（ハードウェア）である。TOEが動作する環境を以下に示す。

(1) ソフトウェア構成
- OS：Windows XP Embedded SP1（TCP/IP及びHTTPSプロトコルを含む）

(2) ハードウェア構成
- OS及びSWを動作させ、HSMを接続可能なハードウェアプラットホーム（CPU、HDDを含む）
- 一般利用者及びサービスマンに対するマンマシンインタフェース用の操作パネル
- RFIDに対して情報の記録・読み取りを行うためのR/W
- キャッシュカードの口座番号を読み取るための磁気カードリーダ
- センターサーバ及び来店予約サーバと通信するための無線通信アダプタ
- 暗号鍵の更新を行うための保守IF
- 申込書を筐体内に取り込むための取込機構

・ 上記のすべてのハードウェアを格納するCBB端末の筐体

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.PIN	サービスマン（保守員と警備会社）はCBB端末を保守するためのPINを第三者に知られないように管理する。
A.OPERATE	運用者は、CBBシステムで使用する情報（暗証番号(入力中を含む)、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、CBB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	CBB端末には物理錠が設置され、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. 筐体内部の基板やHSMなどのハードウェアに対する不正行為など)。
A.HW_DEV	HW製造者は、TOE開発者から配送されたTOEを改ざん・漏洩されないように管理し、CBB端末に対して悪意を持った行為を行わない。また、TOEを格納したCBB端末を製造場所で保管する場合やコンビニエンスストアに配送する場合は、筐体の物理錠をかける。
A.CASE	CBB端末には、操作パネルに入力中の暗証番号の盗み見を防止する手段が設置される。
A.CONNECT	CBB端末は特定のサーバ（センターサーバと来店予約サーバ）にのみ接続される。
A.CHANNEL	CBB 端末とサーバの通信路は、盗聴･改ざんから保護されている。

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。

・ コンビニ･ボックス･バンクシステム インストールガイド，バージョン 1.0，2005年2月4日
・ コンビニ・ボックス・バンクシステム 運用計画書，バージョン 1.0，2005年2

月4日

- コンビニ･ボックス･バンクシステム ユーザマニュアル（ＣＢＢ端末篇），バージョン 1.0，2005年1月31日
- 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篇），バージョン 1.0，2005年1月31日
- 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），バージョン 1.0，2005年2月1日
- コンビニ･ボックス･バンクシステム 保守手順書（保守会社），バージョン 1.0，2005年2月4日

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パート2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、本評価報告書において報告されている。本評価報告書では、本TOEの概要説明、CEMパート2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、本評価報告書による評価実施の履歴を示す。

評価は、平成16年10月に始まり、平成17年2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16年12月及び平成17年1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17年1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表2-1に示す。

表2-1 開発者テストの構成

TOE
コンビニ・ボックス・バンク業務アプリケーションユニット（バージョン1.0）
コンビニ・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1.00）
TURBOMISTY（B8470-1）
ハードウェア
CBB端末試作機（実運用時のCBB端末との相違は筐体の衣装のみ）
キャッシュカード（実運用時と同一のキャッシュカード）
申込書（実運用時のRFIDと同一のRFIDが格納される）
センターサーバ開発機（実運用時のセンターサーバと同じ機能を持つ）
受付端末開発機（実運用時の受付端末と同じ機能を持ち、実運用時と同一のRFIDリーダライタが接続される）
模擬来店予約サーバ（実運用時の来店予約サーバと同じ機能を持つ）
ソフトウェア
OS：Windows XP Embedded SP1
ツール
暗・復号テストプログラム（HSM 内の MISTY 暗号処理を実行するための API をコールする開発者作成のプログラム）
開発 PC
マウス
キーボート
USB ハブ
ネットワーク構成
CBB 端末とセンターサーバ開発機を実運用時と同一の通信網を介して接続
CBB 端末と擬似来店予約サーバを実運用時と同一の通信網を介して接続
センターサーバ開発機に受付端末開発機を接続
受付端末開発機に RFID リーダライタを接続

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を表2-1に示す。開発者テストは、表2-1に示すとおり、STにおいて識別されているTOE構成と同一の機能を備えるハードウェア及びソフトウェアで構成されるテスト環境で実施されている。なお表2-1の「ツール」欄に記載されているツール群はST記載の構成とは異なるものであるが、評価者はこれらのツールがテスト結果に影響しないと判断した。

b.テスト手法

テストには、以下の手法が使用された。

①CBB端末の操作パネルを操作することによりセキュリティ機能の外部インタフェースを刺激し、操作パネルの表示、RFIDに格納された申込情報、及びセンターサーバに転送された受付情報からセキュリティ機能のふるまいを観察する。

②CBB端末の操作パネルを操作することによりセキュリティ機能の外部インタフェースを刺激し、SWのアプリケーションログ及びOS付属のエクスプローラ、イベントログを使用してセキュリティ機能のふるまいを確認する。

③暗号化機能に対するサブシステムレベルのテストでは､開発者作成のテストプログラムを使用して、セキュリティ機能の内部インタフェースを刺激し、そのふるまいを観察する。

c.実施テストの範囲

テストは開発者によって5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を表2-1に示す。評価者テストは、表2-1に示すとおり、STにおいて識別されているTOE構成と同一の機能を備えるハードウェア及びソフトウェアで構成されるテスト環境で実施されている。なお、ST記載とは異なる構成については、表2-1に記載されているツールは「2) 開発者テスト概説 a. テスト構成」記載と同じくテスト結果に影響しないと判断した。

b.テスト手法

テストには、以下の手法が使用された。

①CBB端末の操作パネルを操作することによりセキュリティ機能の外部イン

タフェースを刺激し、操作パネルの表示、RFIDに格納された申込情報、及びセンターサーバに転送された受付情報からセキュリティ機能のふるまいを観察する。

②CBB端末の操作パネルを操作することによりセキュリティ機能の外部インタフェースを刺激し、SWのアプリケーションログ及びOS付属のエクスプローラ、イベントログを使用してセキュリティ機能のふるまいを確認する。

③侵入テストでは、操作画面に表示されるテンキーの数字配列及び操作者の指の動きを観察することにより、操作者の暗証番号を不正に入手できる可能性を検証する。

c.実施テストの範囲

評価者は、独自に考案したテストを7項目、開発者テストのサンプリングによるテストを5項目、侵入テストを1項目、計13項目のテストを実施した。

評価者が独自に考案したテストは、下記を考慮している。

① 機能強度の対象となるセキュリティ機能に対する追加の検証
② 開発者テストでカバーされていない異常時のセキュリティ機能の検証
③ 開発者テストとは異なるテスト方法による検証

開発者テストのサンプリングテストは、セキュリティ機能が2つと少数であることから、開発者テストと同じ5項目を選択している。

侵入テストは、評価者が実施した以下の検査の結果、開発者の主張する根拠に疑わしい点がある脆弱性について実施されている。

① 開発者が分析した評価提供物件に基づく脆弱性
② 開発者が分析したSTの評価報告書で識別された脆弱性
③ 開発者が分析した公知情報源に基づく脆弱性
④ 評価者がAGD及びADO評価中に識別した脆弱性

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

本評価報告書をもって、評価者は本TOEがCEMパート2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

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本評価報告書で示されたように評価されていること。

④ 本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 本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及び本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

提出された本評価報告書、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種別、境界の記述が明瞭であることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然と一貫性のあることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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概説が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明記され、それらが脅威、組織のセキュリティ方針、前提条件へ遡れ、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理路整然とし、完結しており、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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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理路整然とし、完結しており、かつ一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。

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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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結しており、理路整然とし、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_CAP.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。
配付と運用	**適切な評価が実施された。**
ADO_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。
ADO_DEL.1.2D	評価はワークユニットに沿って行われた。ただし出荷実績がないため、実際に配付手続きが使用されていることを確認する代わりに、適切な配付手続きが存在し使用される準備が十分に整っていることを、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.1.1E	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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ADV_FSP.1.2E	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.1.1E	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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ADV_HLD.1.2E	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_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ることを、それらの対応分析により確認している。
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い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.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機能仕様に正確に対応し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が含まれて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_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主張が正しことを確認している。
AVA_VLA.1.1E	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.1.2E	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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。

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

本報告書で使用された用語を以下に示す。

CBBシステム	コンビニ・ボックス・バンクシステム。従来銀行窓口で行われている事務手続きや相談予約をコンビニエンスストアで利用できるようにする。
CBB端末	コンビニ・ボックス・バンク端末。コンビニエンスストアに設置される。CBBシステムの一部。
センターサーバ	CBB端末がアクセスするセンターに設置されたサーバ。住所変更届けなどの業務手続きサービスに関わる。CBBシステムの一部。
受付端末	センターに設置され、コンビニエンスストアから配送されてきた申込書を処理する端末。申込書に格納されているRFID内のデータを読み取るためのRFIDリーダライタが接続されている。CBBシステムの一部。
来店予約サーバ	CBB端末がアクセスする来店予約センターに設置されたサーバ。支店来店予約などの相談予約サービスに関わり、予約可能支店・日時などの情報を管理している。CBBシステムの一部。

HSM	Hardware Security Module ― 耐タンパセキュアボード。不正アクセスを検知すると内部で保持している機密情報をすべてゼロクリアする耐タンパ性を具備した暗号ボード「TURBOMISTY」（FIPS140-2、Level3）。RSA鍵ペアを最大32ペア保持できる。搭載されている主な暗号アルゴリズムは、Triple DES、RSA、MISTY1である。三菱電機インフォメーションシステムズ社製。TOEの一部。
SW	CBB端末に搭載されるアプリケーションソフトウェア。TOEの一部。
操作パネル	CBB端末を操作するための画面。CBB端末の一部。
RFID	Radio Frequency Identification ― ICタグ。一意に識別するためのタグIDが記録されている。申込書に格納されている。
R/W	RFIDのリーダライタ。CBB端末の一部。
HDD	Hard Disk Drive。CBB端末の一部。
磁気カードリーダ	キャッシュカードから口座番号などを読み取るための装置。CBB端末の一部。
保守IF	暗号鍵更新などの保守作業に使用するインタフェース。CBB端末の一部。
申込情報	暗証番号や口座番号などの情報で、RFIDに記録される。
受付情報	タグIDや口座番号などの情報で、センターサーバへ転送される。
PIN	サービスマンを認証するための番号。
MISTY鍵	申込情報と受付情報を暗号アルゴリズム「MISTY1」で暗号化するための暗号鍵。
RSA鍵ペア（RSA公開鍵とRSA秘密鍵）	MISTY鍵を暗号アルゴリズム「RSA」で暗号化してTOE内に保持するための暗号鍵のペア。RSA秘密鍵はCBB端末出荷時にHSMに格納され、MISTY鍵を使用するときに復号するために用いられる。
端末固有情報	CBB端末毎に異なる固有の情報。
鍵確認情報	復号されたMISTY鍵の完全性を確認するための情報。

暗号化MISTY鍵	MISTY鍵と鍵確認情報をRSA公開鍵で暗号化したもの。
ヘッダ	鍵確認情報と端末固有情報を含む情報。暗号鍵更新時に、暗号化MISTY鍵とセットで使用される。
暗号化MISTY鍵情報	暗号化MIST鍵とヘッダのセットの総称。HDD内に格納され、暗号鍵更新時に更新される。
保守員	TOEの保守作業を行うためにTOEの保守機能を使用する特権を有する人物の総称。
警備会社	保守作業時に必ず保守員に同行し、TOEの保守機能を使用する特権を有する人物の総称。
サービスマン	保守員と警備会社の総称。
運用者	一般利用者にCBB端末を使用したサービスを提供する人物の総称。CBB端末で使用する暗号鍵を管理する人物、センターサーバや来店予約サーバの管理者、受付端末の操作者を含む。
HW製造者	CBB端末の製造（TOEの格納を含む）とコンビニエンスストアへのCBB端末の配送を行う人物の総称。

6 参照

[1] コンビニ・ボックス・バンク業務アプリケーションユニット セキュリティターゲット バージョン 2.0（2005年2月21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セキュリティ認証申請等の手引き 平成16年4月 独立行政法人情報処理推進機構 ITQM-23

[3] ITセキュリティ評価機関に対する要求事項 平成16年4月 独立行政法人情報処理推進機構 ITQM-07

[4] ITセキュリティ認証申請者・登録者に対する要求事項 平成16年4月 独立行政法人情報処理推進機構 ITQM-08

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[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2.1 1999年8月 CCIMB-99-031

[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2.1 1999年8月 CCIMB-99-032

[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2.1 1999年8月 CCIMB-99-033

[11] ISO/IEC 15408-1 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model ISO/IEC15408-1: 1999(E)

[12] ISO/IEC 15408-2 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements ISO/IEC15408-2: 1999(E)

[13] ISO/IEC 15408-3 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements ISO/IEC15408-3: 1999(E)

[14] JIS X 5070-1: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第1部: 総則及び一般モデル

[15] JIS X 5070-2: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第2部: セキュリティ機能要件

[16] JIS X 5070-3: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第3部: セキュリティ保証要件

[17] Common Methodology for Information Technology Security Evaluation

CEM-99/045 Part2: Evaluation Methodology Version 1.0 August 1999

[18] 情報技術セキュリティ評価のための共通方法論 CEM-99/045 パート2: 評価方法論 バージョン1.0 1999年8月

[19] JIS TR X 0049: 2001 情報技術セキュリティ評価のための共通方法

[20] CCIMB Interpretations-0407

[21] 補足-0210 第2版

[22] 補足-0407

[23] コンビニ・ボックス・バンク業務アプリケーションユニット, バージョン 1.0 評価報告書 第1.1版 2005年2月21日 株式会社電子商取引安全技術研究所　評価センター