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

作成日: 2008 年 3 月 12 日

著者: 三菱電機インフォメーションシステムズ株式会社

目次

1. ST 概説

本章では、ST 及び TOE 参照、TOE 概要、TOE 記述について記述する。

1.1. ST 参照

ST の識別情報を以下に示す。

ST 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 セキュリティターゲット

バージョン: 1.6

作成日: 2008 年 3 月 12 日

著者: 三菱電機インフォメーションシステムズ株式会社

1.2. TOE 参照

TOE の識別情報を以下に示す。

製造者: 三菱電機インフォメーションシステムズ株式会社

TOE 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

1.3. TOE 概要

TOE は、イオン・ボックス・バンク(以下、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。本**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届け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。

これらのサービスを可能にするため、TOE は受付機能、封筒取込機能や通信機能を具備し、これらの機能を安全に運用するために、端末に入力された情報の暗号化機能、サービスマンや行内関係者の識別認証機能を有する。

なお、本 TOE の利用にあたって、以下に示すソフトウェアや IT 機器が必要である(これらは TOE の範囲外である)。

Table 1-1: 必要なソフトウェアや IT 機器

項目	仕様
OS	Microsoft Windows XP Embedded 日本語版
端末	共同利用端末 もしくは単独利用端末
ソフトウェア	端末デバイスチェックソフトウェア

1.4. TOE 記述

本章では、TOE の物理的・論理的範囲について記述する。

1.4.1. ABB システム概要

本 TOE が搭載される金融端末は、スーパーマーケット等の店舗に設置され、事務手続き業務(e.g. 住所変更届けや改印届けなど)を受け付けるものである。従って、本端末は金融端末であるが、現金は取り扱わない。

図 1-1 に TOE を含めた ABB システムの概要図を示す。端末は店舗に設置され、センターのサーバと通信網を介して接続されている。TOE は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(図中、端末の灰色部分)。センターでは、サービスを提供する運用者の基幹システムによって一般利用者の情報(e.g. 口座番号など)が管理されている。センターのサーバ(以下センターサーバ)における ABB 用アプリケーションソフトウェアは TOE 開発者によって別途開発されるが、本 ST の対象外である。

一般利用者は、住所変更届けなどの事務手続きを行う場合、所定の申込書に各種必要事項を記入した後、端末において、操作パネル上で画面によって指示される操作や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、申込書を入れた ABB 専用封筒を端末に投函する。TOE は、投函された申込書に格納されている RFID のタグ ID(個々の RFID にユニークな番号)を、RFID リーダライタ(以下、R/W)を介して読み込む。そして、入力された個人情報(銀行カードの磁気情報等)や日時から成る申請情報を暗号化し、R/W を介して RFID に記録する。この後、ABB 専用封筒は端末内部に保管される。また、この際、端末は、入力された個人情報や日時、タグ ID から成る受付情報を暗号化し、ダイアルアップにてセンターサーバへ転送する。これらの情報はプライバシーの観点から端末が保護する必要がある。以上の処理は、TOE によって制御される。

投函された申込書は、配送業者である配送者によりセンターへ送付される。センターでは、リーダライタにより RFID に記録された暗号化申請情報を読み出し、センターサーバにて復号する。そして、一般利用者本人が手続きを申請したことと、受信した受付情報を復号した結果から端末で受け付けたことが確認された後、センターにて事務手続きが処理される。

また、端末は、店舗で受付業務を行っている行内関係者によるセンターへ送付する書類の投函を受け付ける。この書類は行内関係者が受領した一般利用者の申込書であり、複数の申込書が、RFID が格納されている所定の封筒(行内専用封筒)に入れられる。行内専用封筒を投函する投函口は、一般利用者が使用する投函口と異なる(すなわち、端末には投函口が 2 箇所ある)。行内関係者は、端末にて投函する際、投函者の氏名などの必要な情報を操作パネルや磁気カードリーダを介して入力する。TOE は行内専用封筒を受け付けた際、入力された個人情報や日時、タグ ID からなる受付情報を暗号化して、ダイアルアップにてセンターサーバへ転送する。この情報もプライバシーの観点から端末が保護する必要がある。本サービス(一括投函サービス)は行内関係者のみが使用することができ、一般利用者は使用することはできない。

TOE が搭載される端末は、形状の異なる共同利用端末と単独利用端末の 2 種類ある。単独利用端末には、本 TOE とデバイスチェックソフトウェア(後述)が搭載されるが、共同利用端末には、これら以外に他行の一般利用者に対して同様のサービスを提供する他行向けアプリケーション([CBB-ST]参照)が搭載され、他行の一般利用者も使用することができる。すなわち、共同利用端末では、一般利用者は、運用者が提供するサービスと他行が提供するサービスを選択することができ、選択されたサービスによって通信先(接続先のサーバ)は変わる。また、片方のサービスを提供している間、他方のサービスは受けることが出来ない。

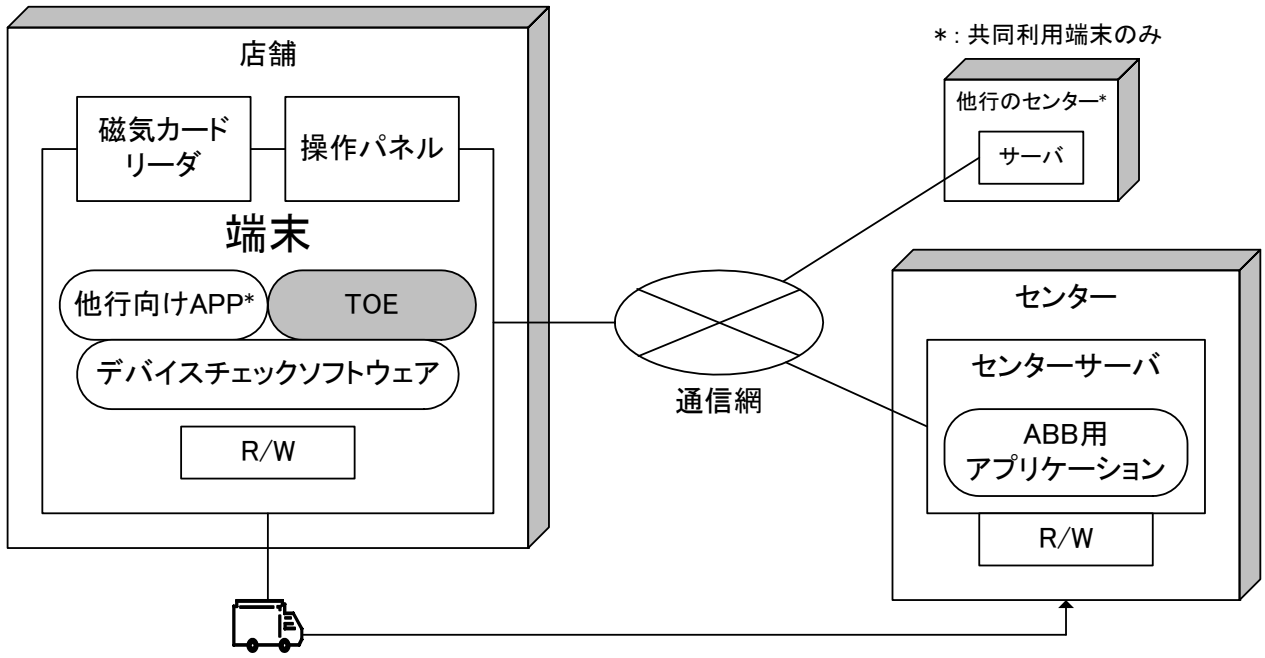

図 1-1: ABB システム構成図

1.4.2. 端末の構成と TOE との関係

図 1-2 に端末の構成を示す。図中、灰色の部分が TOE である。すなわち、TOE はアプリケーションソフトウェアである。

端末は、ハードウェア製造者(以下、HW 製造者)によって開発される。CPU や HDD などは端末の筐体内に格納され、アクセスするには筐体に設けられた物理錠を開錠する必要がある。配送者が ABB 専用封筒や行内専用封筒を回収する場合や、サービスマン(保守員や警備会社、1.4.3 章参照)による端末の保守作業(e.g. 定期点検、障害時の点検)を実施する際に開錠される。以下、図 1-2 に記載した構成について説明する。

- 端末には物理錠が設置される(図 1-2 には図示していない)。
- 操作パネルは、一般利用者や行内関係者が操作し、必要な情報を端末に入力するために用いられる。ま

た、端末の固有情報(e.g. IP アドレスやホスト名など)の設定時や保守の際にもマンマシンインタフェースとしても用いられる。

- 磁気カードリーダは、挿入された銀行カードから磁気ストライプに記録された情報を読み取るのに使用される。
- 申込書は、RFID が格納された本システム特有の一般利用者向けのものであり、ABB 専用封筒に入れられる。暗号化された申請情報が RFID 内部のメモリに保持される。行内関係者がセンターへ書類を送付する際に使用される行内専用封筒にも RFID が格納されているが、本 RFID には情報の記録は行われない(タグ ID の読み取りのみ)。
- R/W は申込書や行内専用封筒に格納される RFID と通信可能なものであり、RFID に対して情報の記録・読み込みを行う。図示していないが、R/W は、一般利用者の申込書向けと行内関係者の行内専用封筒向けの 2 つある。
- 取込機構は、一般利用者が投函した ABB 専用封筒、または行内関係者が投函した行内専用封筒を端末内部に取り込む。取込機構はTOE によって制御される。図示していないが、一般利用者向けの投函口と行内関係者向けの投函口は異なるため、対応する取込機構は 2 つ搭載されている。取り込まれた封筒は端末内部に保管される。一旦、端末内部に保管された封筒は、筐体に設置した上記物理錠を開錠しないかぎり取り出せない。
- 無線通信モジュールは、受付情報転送、各ファイルのダウンロード(後述)のために、ダイアルアップにて所定のセンターサーバのみにアクセスする。
- 保守インタフェース(保守 IF)は、端末の保守に使用される IF であり、施錠された筐体内部に格納されている。
- OS は、Windows XP Embedded SP2(日本語版)を使用する。端末の起動・停止、TCP/IP の通信制御などを行う。
- HDD に OS や TOE、RSA 公開鍵(後述)が記録される(図は動作中のもの)。施錠された筐体内部に格納されている。他行向けアプリケーション(共同利用端末の場合)やデバイスチェックソフトウェアも HDD に記録されている。
- TOE は、施錠された筐体内部に格納されている。TOE は、端末内部の基板(図示していない)上の CPU で動作するアプリケーションソフトウェアである。事務手続き、一括投函、保守、設定などのサービスを提供するが、同時に 1 つのサービスしか提供できない構造になっている。本 TOE に付随するマニュアルは以下のものである。
  - 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～

- 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)
- 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～
- 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～
- 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～
- 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～
- 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～
- 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～
- 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～
- 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～
- 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～
- 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～

- 他行向けアプリケーションは、住所変更届けなど TOE と同様のサービスを他行の一般利用者に提供するアプリケーション([CBB-ST]参照)であり、共同利用端末にのみ搭載される。本アプリケーションは TOE の範囲外であり、TOE が使用する暗号鍵(後述)は使用しない。本アプリケーションが起動している間、TOE は非活性状態であり、一般利用者にサービスを提供することはできない。共同利用端末では、運用者が提供するサービスと他行向けサービスを一般利用者に選択させる画面を表示しており、一般利用者が前者を選択した場合、TOE がサービスを提供し、そのセキュリティ機能が使用される。後者の場合、TOE は起動しない。なお、単独利用端末には本アプリケーションは搭載されず、運用者が提供するサービスの一覧(住所変更届けや改印届けなど)を表示する。
- 端末デバイスチェックソフトウェアは、HW 製造者から提供される端末のハードウェア(磁気カードリーダ、取込機構、R/W 等)の動作状況をチェックするソフトウェアであり、TOE と同時に使用されることはない。保守や障害発生時に使用される。TOE の範囲外である。

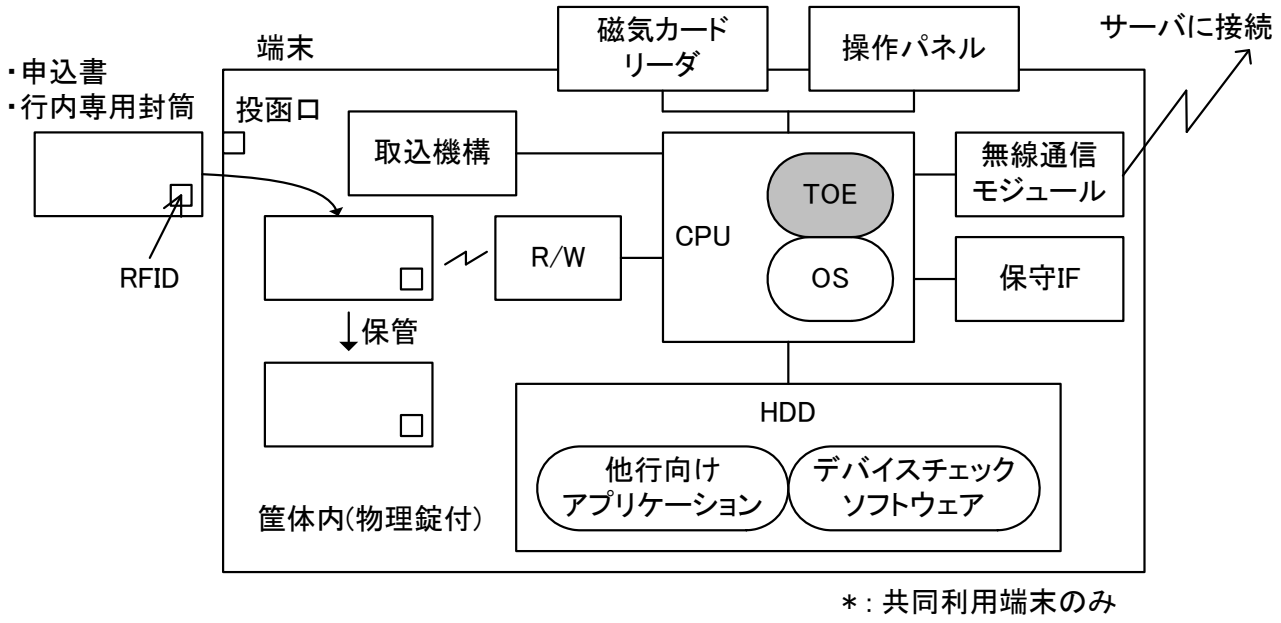

図 1-2: 端末の構成

1.4.3. TOE の関係者

本 TOE や端末の開発・運用に携わる関係者を図 1-3 に示す。

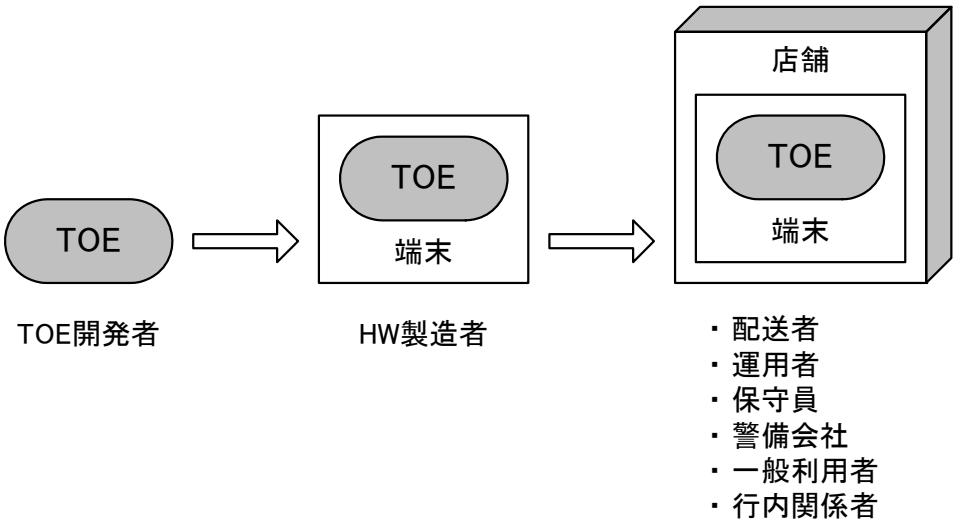

図 1-3: 端末の関係者

以下に図 1-3 も含めて TOE の関係者を説明する。一般利用者以外の関係者には 1.4.2 章記載のマニュアルが提供される。

一般利用者	端末により事務手続きサービスを利用するユーザ。
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。

警備会社	TOE の保守機能を使用できるサービスマンで、端末に設けられた防犯センサ(図 1-2 には図示していない)が感知した場合、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)。
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。
配送者	端末に投函された申込書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。
HW 製造者	TOE の端末への格納、端末の店舗への配送を実施する端末の製造者。
運用者	本システムにより一般利用者に ABB サービスを提供する銀行。ABB システムで使用する暗号鍵の管理をセンターにて行う。センターサーバの管理者や、各種業務処理を行う作業者を含む。
TOE 開発者	TOE の開発や HW 製造者への TOE 配付を行う。

1.4.4. TOE の論理的範囲と境界

以下に TOE が提供する機能を示す。

1.4.4.1. TOE のセキュリティ機能

以下に本書が対象とする TOE のセキュリティ機能を示す。

- 暗号化機能

一般利用者向けの事務手続きにおいて、RFID に申請情報を記録する前、及び事務手続きや行内関係者向けの一括投函において、受付情報を転送する前にこれらの情報を暗号アルゴリズム「MISTY1」で暗号化する。これらの暗号化に使用する暗号鍵(以下、MISTY 鍵)は、TOE が生成する乱数を利用し、受付毎に生成する。MISTY 鍵は、暗号アルゴリズム「RSA」を用いて TOE が保持する公開鍵(1024bits)で暗号化されて、センターサーバに転送される。また、使用後の MISTY 鍵はゼロクリアされる。

- 識別認証機能

TOE は以下の識別認証機能を有する。

① 保守識別認証機能:店舗での保守を行う前にサービスマン(保守員と警備会社)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、PIN による認証を行う。続けて 3 回認証に失敗した場合、PIN(以下、保守 PIN)の入力を 5 分間受け付けない。保守 PIN は操作パネルから入力される。なお、保守 PIN は運用中に端末外部から格納されることや

1.4.3 章に記載した役割によって変更されることはない。

② 設定識別認証機能:端末に端末固有の情報を設定する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(後述)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、PIN による認証を行う。続けて 3 回認証に失敗した場合、PIN(以下、設定 PIN)の入力を 3 分間受け付けない。設定 PIN は操作パネルから入力される。また、設定 PIN は TOE 開発者が TOE に格納したものを使用する。

③ 行内関係者識別認証機能:店舗での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 による認証を行う。続けて 3 回認証に失敗した場合、PIN(以下、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、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。

1.4.4.2. 非セキュリティ機能

- 受付機能

共同利用端末ではサービス提供者を選択する画面を、単独利用端末ではサービスを選択する画面を表示し、一般利用者からの操作を待つ機能。また、事務手続きにおいては、一般利用者の操作を受け付け、操作パネルや磁気カードリーダから入力された申請情報を R/W を介して RFID に記録し、一括投函サービスにおいては行内関係者の操作を受け付ける機能も含む。

- 封筒取込機能

事務手続きや一括投函において、一般利用者や行内関係者が各投函口から投函した ABB 専用封筒や行内専用封筒を端末内に取り込む取込機構を制御する機能。端末内に取り込まれて保管されている各封筒は、物理錠により筐体を開錠しない限り、取り出せない。

- 通信機能

無線通信モジュールを介してダイアルアップにてセンターサーバと通信する機能。TOE は一般利用者や行内関係者の操作を受け付け、各封筒を取り込んだ後、暗号化された受付情報をセンターサーバに転送する。また、HDD に記録されている TOE の実行形式ファイルや設定ファイル(複数ある RSA 公開鍵の内、MISTY 鍵暗号化で使用する鍵を示す情報や TOE の設定を記録した ini ファイル)、店舗 PIN を更新するために、TOE はセンターサーバからファイルを取得する。ダウンロードするファイルは運用者だけがセンターサーバに格納できる。

- 保守機能

保守員と警備会社に対して端末の保守作業を提供する機能。主な保守作業には定期及び障害時の点検作業

がある。保守認証に成功した場合のみ、本機能を使用することができる。本 TOE には、本機能によって保守が必要なセキュリティ関連データは扱っていない。

- 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など)を設定・変更できる機能である。保守認証に成功した後、別途設定認証に成功した場合のみ、本機能を使用することができる。

1.4.5. TOE の保護対象情報資産

上述したように、TOE は、店舗に設置される端末に搭載され、ABB システムは、一般利用者の個人情報を扱っている。この情報は ABB システムとして機密にしなければならない情報である。また、行内関係者が行内専用封筒を投函する際に入力される情報(氏名など)の機密性も維持する必要がある。 すなわち、本 TOE が保護すべき情報資産は、一般利用者や行内関係者に関する情報が含まれる受付情報(端末からセンターに転送される情報)と、一般利用者に関する情報が含まれる申請情報(RFID に記録される情報)であり、その機密性を維持する。

2. 適合主張

本章では適合の主張について述べる。

2.1. CC 適合主張

本 ST が適合している CC はバージョン 3.1 であり、機能要件はパート 2 適合、保証要件はパート 3 適合である。なお、本 CC の日本語訳として以下を利用した。

[CC-J] 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, 2006 年 9 月, バージョン 3.1 改訂第 1 版, 平成 19 年 3 月翻訳第 1.2 版, 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

パート 1: 概説と一般モデル CCMB-2006-09-001

パート 2: セキュリティ機能コンポーネント CCMB-2006-09-002

パート 3: セキュリティ保証コンポーネント CCMB-2006-09-003

2.2. PP 主張

本 ST が適合している PP はない。

2.3. パッケージ主張

本 ST は評価保証レベル EAL2 追加である。追加される保証要件は ALC_FLR.1 である。

3. セキュリティ課題定義

本章では、脅威、組織のセキュリティ方針(以下、OSP)、前提条件について記述する。

3.1. 脅威

本章では脅威について記述する。

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。

3.2. 組織のセキュリティ方針

本章では OSP について記述する。

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。

3.3. 前提条件

本章では前提条件について記述する。

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. 筐体内部の基板などのハードウェアに対する不正行為など)。

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。

4. セキュリティ対策方針

本章では、TOE に対するセキュリティ対策方針(以下、SO)、運用環境に対する SO、及び根拠について記述する。

4.1. TOE のセキュリティ対策方針

本章では、TOE に対する SO について記述する。

O.PROT_INFO	TOE は、受付情報と申請情報の機密性を維持しなければならない。
O.I&A	TOE は保守機能を利用するサービスマンを、設定機能を利用する保守員を、一括投函サービスを利用する行内関係者をそれぞれ識別認証しなければならない。

4.2. 運用環境のセキュリティ対策方針

本章では、運用環境に対する SO について記述する。

OE.PIN	警備会社は保守 PIN を、保守員は保守 PIN と設定 PIN を第三者に知られないように管理しなければならない。また、行内関係者と運用者は店舗 PIN を第三者に知られないように管理しなければならない。
OE.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しなければならない。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しなければならない。
OE.KEY	配送者と警備会社は、物理錠の鍵を悪用されないように管理しなければならない。
OE.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ってはならない(e.g. 筐体内部の基板などのハードウェアに対する不正行為など)。
OE.HW_DEV	運用者は、操作パネルの覗き見を防止する手段と物理錠が設置された端末を使用しなければならない。
OE.CHANNEL	運用者は、端末が盗聴・改ざんから保護されている通信路によりセンターサーバとのみ接続する環境で端末を運用しなければならない。
OE.APP	運用者は、TOE や TOE が使用するデータを改ざんしないことが TOE 開発者により確認されたソフトウェアのみが端末に搭載されるように管理しなければならない。

OE.ACCESS　運用者は、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端末を管理しなければならない。

4.3. セキュリティ対策方針根拠

本章ではセキュリティ対策方針の根拠を示す。

以下に示すように、すべての SO が達成された場合、3 章で定義したセキュリティ課題は解決される。すなわち、すべての脅威は対抗され、すべての OSP は達成され、すべての前提条件は実現される。

4.3.1. 追跡性

脅威・OSP・前提条件と SO との対応関係を表 4-1 に示す。表中「×」は、対応関係にあることを示している。

これから明らかなように、各 SO は、少なくとも一つの脅威・OSP・前提条件に対応しており、各脅威、OSP、前提条件は少なくとも一つの SO に対応している。また、TOE の SO は、前提条件に対応していない(表中灰色の部分)。

表 4-1: 脅威・OSP・前提条件と SO の対応関係

	O.PROT_INFO	O.I&A	OE.PIN	OE.OPERATE	OE.KEY	OE.NO_HARM	OE.HW_DEV	OE.CHANNEL	OE.APP	OE.ACCESS
T.RFID_INFO	×									
P.PRIVACY	×									
P.MAINTE		×								
P.OPE_POST		×								
A.PIN			×							
A.OPERATE				×						
A.CASE_KEY					×		×			
A.NO_HARM						×				
A.CASE							×			
A.CAHNNEL								×		
A.APP									×	
A.ACCESS										×

4.3.2. 正当化根拠

以下、各 SO が脅威・前提条件・OSP を満たすのに適している根拠を示す。

T.RFID_INFO は O.PROT_INFO によって対抗される。なぜなら、この SO によって、RFID に記録される申請情報が暴露されることが防止することができるからである。

P.PRIVACY は、O.PROT_INFO によって達成される。なぜなら、O.PROT_INFO によって、受付情報の機密性を維持できるからである。

P.MAINTE は、O.I&A によって達成される。なぜなら、この SO によってサービスマンのみが保守機能を、保守員のみが設定機能を利用できるからである。

P.OPE_POST は O.I&A によって達成される。なぜなら、この SO によって、行内関係者のみが一括投函サービスを利用できるからである。

A.PIN は OE.PIN によって実現される。なぜなら、この SO によって、保守 PIN、設定 PIN、店舗 PIN が各役割によって第三者に知られないように管理されるからである。

A.OPERATE は OE.OPERATE によって実現される。なぜなら、A.OPERATE は、この SO によって直接満たされているからである。

A.CASE_KEY は OE.KEY と OE.HW_DEV によって実現される。なぜなら、OE.HW_DEV によって物理錠が設置された端末の使用が実現され、OE.KEY によって、配送者と警備会社のみが物理錠の鍵を使用できることが実現されるからである。

A.NO_HARM は OE.NO_HARM によって実現される。なぜなら、A.NO_HARM は、この SO によって直接満たされているからである。

A.CASE は、OE.HW_DEV によって実現される。なぜなら、この SO によって操作パネルに入力中の個人情報の盗み見を困難にする端末が使用されるからである。

A.CHANNEL は OE.CHANNEL によって実現される。なぜなら、この SO によって、端末の接続先をセンターサーバに限定し、盗聴・改ざんから保護されている通信路の使用が運用者によって実現されるからである。

A.APP は OE.APP によって実現される。なぜなら、この SO によって、TOE や TOE が使用するデータを改ざんしないことが TOE 開発者により確認された信頼できるソフトウェアのみが端末に搭載されることが運用者によって実現されるからである。

A.ACCESS は OE.ACCESS によって実現される。なぜなら、この SO によって通常運用時以外には一般利用

者や行内関係者がアクセスできない端末の管理が実現されるからである。

5. 拡張コンポーネント定義

本書では、拡張したセキュリティ要件、すなわち[CC]に記載されていない新規のセキュリティ機能要件とセキュリティ保証要件は定義しない。

6. セキュリティ要件

本章では、TOE が満たしていなければならないセキュリティ要件について記述する。コンポーネントの操作は以下のように記述した。また、繰り返し操作を行った要件と依存関係にある要件の識別子に、繰り返し操作と同じ( )付アルファベットを付加した。

- 割付と選択は[ ]内に記述
- 詳細化は下線・太字で記述
- 繰り返しはコンポーネント及びエレメントに( )付アルファベットを付加

6.1. TOE セキュリティ機能要件

6.1.1. FCS クラス

FCS_CKM.1(M) 暗号鍵生成

下位階層: なし

依存性: [FCS_CKM.2 暗号鍵配付、または

FCS_COP.1 暗号操作]

FCS_CKM.4 暗号鍵破棄

FMT_MSA.2 セキュアなセキュリティ属性

FCS_CKM.1.1(M) TSF は、以下の[割付: なし]に合致する、指定された暗号鍵生成アルゴリズム[割付: 独自の暗号鍵発生アルゴリズム「PRNG based on MISTY1」]と指定された暗号鍵長[割付: 128bits]に従って、**MISTY 鍵**を生成しなければならない。

FCS_CKM.4(M) 暗号鍵破棄

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]

FMT_MSA.2 セキュアなセキュリティ属性

FCS_CKM.4.1(M) TSF は、以下の[割付: なし]に合致する、指定された暗号鍵破棄方法[割付: 暗号鍵のゼロクリア]に従って、**MISTY 鍵**を破棄しなければならない。

FCS_COP.1(M) 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
FMT_MSA.2 セキュアなセキュリティ属性

FCS_COP.1.1(M) TSF は、[割付: 暗号技術仕様書 MISTY1 (updated 2002 年 5 月 13 日)]に合致する、特定された暗号アルゴリズム[割付: MISTY1]と暗号鍵長[割付: 128bits]に従って、[割付: 受付情報と申請情報の暗号化]を実行しなければならない。

FCS_COP.1(R) 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
FMT_MSA.2 セキュアなセキュリティ属性

FCS_COP.1.1(R) TSF は、[割付: PKCS#1]に合致する、特定された暗号アルゴリズム[割付: RSA]と暗号鍵長[割付: 1024bits]に従って、[割付: MISTY 鍵の暗号化]を実行しなければならない。

FCS_COP.1(S) 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

FMT_MSA.2 セキュアなセキュリティ属性

FCS_COP.1.1(S) TSF は、[割付: FIPS PUB 180-2]に合致する、特定された暗号アルゴリズム[割付: SHA-1]と暗号鍵長[割付: なし]に従って、[割付: 入力された店舗 PIN のダイジェスト作成]を実行しなければならない。

6.1.2. FIA クラス

FIA_AFL.1 認証失敗時の取り扱い

下位階層: なし

依存性: FIA_UAU.1 認証のタイミング

FIA_AFL.1.1 TSF は、[割付: 保守認証、設定認証と行内関係者認証]に関して、[選択: [割付: 3]]回の不成功認証試行が生じたときを検出しなければならない。

FIA_AFL.1.2 不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付: 以下のアクション]をしなければならない。

- 保守認証の場合は 5 分間の PIN 入力拒否
- 設定認証と行内関係者認証の場合は 3 分間の PIN 入力拒否

FIA_UAU.1 認証のタイミング

下位階層: なし

依存性: FIA_UID.1 識別のタイミング

FIA_UAU.1.1 TSF は、利用者が認証される前に利用者を代行して行われる[割付: 以下のサービスの提供]を許可しなければならない。

- 保守認証の前には、事務手続き、一括投函
- 設定認証の前には、事務手続き、一括投函、保守
- 行内関係者認証の前には、事務手続き、保守、設定

FIA_UAU.1.2 TSF は、その利用者を代行する他のすべての 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。

FIA_UID.1 識別のタイミング

下位階層: なし

依存性: なし

FIA_UID.1.1 TSF は、利用者が識別される前に利用者を代行して実行される[割付: 以下のサービスの提供]を許可しなければならない。

- 保守識別の前には、事務手続き、一括投函
- 設定識別の前には、事務手続き、一括投函、保守
- 行内関係者識別の前には、事務手続き、保守、設定

FIA_UID.1.2 TSF は、その利用者を代行する他の 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。

6.2. TOE セキュリティ保証要件

本 TOE の評価保証レベルは EAL2 に ALC_FLR.1 が追加されたものである。表 6-1 に保証要件の名称を示す。

表 6-1: 保証要件

クラス	ファミリ
ADV	ADV_ARC.1 セキュリティアーキテクチャ記述
	ADV_FSP.2 セキュリティ実施機能仕様
	ADV_TDS.1 基本設計
AGD	AGD_OPE.1 利用者操作ガイダンス
	AGD_PRE.1 準備手続き
ALC	ALC_CMC.2 CM システムの使用
	ALC_CMS.2 TOE の一部の CM 範囲
	ALC_DEL.1 配付手続き
	ALC_FLR.1 基本的な欠陥修正
ASE	ASE_CCL.1 適合主張
	ASE_ECD.1 拡張コンポーネント定義
	ASE_INT.1 ST 概説
	ASE_OBJ.2 セキュリティ対策方針
	ASE_REQ.2 派生したセキュリティ要件
	ASE_SPD.1 セキュリティ課題定義
	ASE_TSS.1 TOE 要約仕様
ATE	ATE_COV.1 カバレージの証拠
	ATE_FUN.1 機能テスト
	ATE_IND.2 独立テスト - サンプル
AVA	AVA_VAN.2 脆弱性分析

6.3. セキュリティ要件根拠

本章ではセキュリティ要件の根拠を示す。

以下に示すように、すべてのセキュリティ機能要件が満たされた場合、4 章で定義した TOE の SO は達成される。

6.3.1. セキュリティ機能要件の追跡性

TOE の SO とセキュリティ機能要件との対応関係を表 6-2 に示す。表中、「×」は対応関係にあることを示してい

る。

これから明らかなように、各機能要件は少なくとも一つの SO に対応しており、各 SO は少なくとも一つの機能要件に対応している。

表 6-2: TOE の SO と機能要件の対応関係

	FCS_CKM.1(M)	FCS_CKM.4(M)	FCS_COP.1(M)	FCS_COP.1(R)	FCS_COP.1(S)	FIA_AFL.1	FIA_UAU.1	FIA_UID.1
O.PROT_INFO	×	×	×	×				
O.I&A					×	×	×	×

6.3.2. セキュリティ機能要件の正当化根拠

以下、各機能要件が、TOE の SO を満たすのに適している根拠を示す。

O.PROT_INFO は、主に FCS_COP.1(M)によって満たされる。なぜなら、この機能要件による暗号アルゴリズム「MISTY1」によって受付情報と申請情報の機密性が維持できるからである。また、MISTY 鍵は FCS_CKM.1(M)によって生成され、FCS_COP.1(R)による暗号アルゴリズム「RSA」で MISTY 鍵を暗号化した状態でセンターサーバへ転送される。転送後古い鍵は使用されないように、FCS_CKM.4(M)によって MISTY 鍵は破棄される。

O.I&A は、主に FIA_UAU.1、FIA_UID.1 によって実現される。なぜなら、これらの機能要件によって、保守機能、設定機能、一括投函サービスを利用する各 TOE 利用者を識別認証できるからである。また、FIA_AFL.1 によって認証失敗時のアクションが実現されることで、各認証の機能を強化し、ダイジェストとして TOE 内に格納されている店舗 PIN との照合を行うために FCS_COP.1(S)によって入力された PIN のダイジェストを生成することを保証する。

6.3.3. セキュリティ保証要件の根拠

本 TOE が搭載される端末は、店舗に設置されるので、誰でも本端末にアクセスできる。また、一般利用者の個人情報を取り扱っているので、高いセキュリティが要求され、セキュリティ欠陥発生時の修正は重要である。しかし、端末の筐体に設けられた物理錠によって、特定の人間しか筐体内部の TOE にアクセスできず、一般利用者がアクセスできるインタフェースは限られている。さらに、端末がアクセスするサーバは、運用者だけが利用できる特定のサーバだけに限られており、その通信路は保護されている。また、本端末の製品種別は金融端末であるものの現金は取り扱わない。

EAL2 にセキュリティ欠陥への対応に関する ALC_FLR.1 を追加した保証要件は、このような TOE に対して妥当である。

6.3.4. 依存性分析

まず、本書で選択されたセキュリティ機能要件の依存性分析結果を表 6-3 に示す。

表 6-3: 機能要件の依存性分析結果

機能要件	依存するコンポーネント	満たしている機能要件	依存性析結果
FCS_CKM.1(M)	[FCS_CKM.2、または FCS_COP.1]、FCS_CKM.4、FMT_MSA.2	FCS_COP.1(M) FCS_CKM.4(M)	依存性はみたされていない
FCS_CKM.4(M)	[FDP_ITC.1、または FDP_ITC.2、または FCS_CKM.1]、FMT_MSA.2	FCS_CKM.1(M)	依存性はみたされていない
FCS_COP.1(M)	[FDP_ITC.1、または FDP_ITC.2、または FCS_CKM.1]、FCS_CKM.4、FMT_MSA.2	FCS_CKM.1(M) FCS_CKM.4(M)	依存性はみたされていない
FCS_COP.1(R)	[FDP_ITC.1、または FDP_ITC.2、または FCS_CKM.1]、FCS_CKM.4、FMT_MSA.2	なし	依存性はみたされていない
FCS_COP.1(S)	[FDP_ITC.1、または FDP_ITC.2、または FCS_CKM.1]、FCS_CKM.4、FMT_MSA.2	なし	依存性はみたされていない
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	依存性はみたされている
FIA_UAU.1	FIA_UID.1	FIA_UID.1	依存性はみたされている
FIA_UID.1	なし	—	—

表 6-3 の分析結果に示すように、本 ST で選択された一部の機能要件は依存性を満たしていない(灰色の部分)。以下、これらについて説明する。

① FCS_CKM.1(M)、FCS_CKM.4(M)と FCS_COP.1(M)が依存する FMT_MSA.2 について

これらの機能要件が対象とする暗号鍵は FCS_CKM.1(M)によって生成される MISTY 鍵である。本暗号鍵は、一般利用者や行内関係者の操作を受け付ける度に生成され、再利用はされない。また、MISTY1 に弱鍵はなく、有効期限もない。従って、セキュリティ属性のチェックは不要であり、FMT_MSA.2 は機能要件として必要ない。

② FCS_COP.1(R)が依存する[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1]、FCS_CKM.4 と FMT_MSA.2 について

FCS_COP.1(R)が対象とする暗号鍵は RSA 公開鍵である。本暗号鍵は、店舗へ端末を設置する前に複数 TOE に格納される。そして、一般利用者や行内関係者の操作を受け付ける度に RSA 公開鍵を用いて MISTY 鍵を暗号化する。本鍵は、格納以降、新たに鍵を生成することも、外部から新しい鍵を格納することもなく、破棄することもない。また、設定ファイルで指定された RSA 鍵を用いるため、セキュリティ属性のチェックも不要である。従って、[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1]、FCS_CKM.4 と FMT_MSA.2 は機能要件として必要ない。

③ FCS_COP.1(S)が依存する機能要件について

FCS_COP.1 は暗号鍵を必要としない SHA-1 アルゴリズムを対象としているため、暗号鍵に対する [FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1]と FCS_CKM.4 の機能要件は必要ない。また、ダイジェストを生成しているだけなので、セキュリティ属性のチェックも必要なく、FMT_MSA.2 も不要である。

これらより、機能要件の依存性は満たされている(満たしていない依存性については根拠が記述されている)と言える。

一方、保証要件は、[CC]で規定された EAL2 と依存性がない ALC_FLR.1 を選択しているので依存性が満たされていることは明白である。

以上の分析より、本 ST で選択されたセキュリティ要件の依存性は問題がない。

7. TOE 要約仕様

本章では、6.1 章で記述された機能要件を TOE が満たす方法・メカニズムについて機能要件毎に記述する。TOE は表 7-1 に示す方法やメカニズムにより各機能要件を満たす。

表 7-1: 機能要件を満たす方法・メカニズム

機能要件	方法・メカニズム
FCS_CKM.1(M)	TOE は、事務手続きや一括投函を受け付ける度に、独自の乱数生成メカニズム「PRNG based on MISTY1」により 128bits の乱数を生成し、それを MISTY1 向けの暗号鍵とする。乱数発生メカニズムは TOE の一部である自社製暗号ライブラリに実装されている。
FCS_CKM.4(M)	TOE は MISTY 鍵を使用後にゼロクリアする。
FCS_COP.1(M)	TOE の一部である、アルゴリズム MISTY1 を実装した自社製暗号ライブラリによって、受付情報と申請情報の MISTY1 暗号化を行う。
FCS_COP.1(R)	TOE の一部である、アルゴリズム RSA を実装した自社製暗号ライブラリによって、RSA 公開鍵による MISTY 鍵の暗号化を行う。
FCS_COP.1(S)	TOE の一部である、アルゴリズム SHA-1 を実装した自社製暗号ライブラリによって、入力された店舗 PIN のダイジェスト生成を行う。
FIA_AFL.1	TOE は、保守認証、設定認証と行内関係者認証において、誤った PIN が 3 回連続で入力された場合、メッセージを表示して、保守認証の場合は 5 分間、設定認証と行内関係者認証の場合は 3 分間動作を停止する。
FIA_UAU.1	TOE は、保守機能と設定機能を提供する前に、各 PIN を入力させる画面を表示し、入力された PIN と TOE が保持する各 PIN との照合を行うことで認証を行う。また、TOE は、一括投函サービスを提供する前に、店舗 PIN を入力させる画面を表示し、入力された PIN のダイジェストと TOE が保持するダイジェストとの照合を行うことで認証を行う。各認証の前に許可しているサービスは以下である。 ・ 保守認証の前には、事務手続き、一括投函 ・ 設定認証の前には、事務手続き、一括投函、保守 ・ 行内関係者認証の前には、事務手続き、保守、設定
FIA_UID.1	TOE は、所定の画面を表示している間に、識別毎に異なる所定の操作が行われたことを検出することで各識別(i.e. 保守、設定、行内関係者)を行う。各識別の前に許可しているサービスは以下である。 ・ 保守識別の前には、事務手続き、一括投函 ・ 設定識別の前には、事務手続き、一括投函、保守 ・ 行内関係者識別の前には、事務手続き、保守、設定

Annex A. 用語の説明

以下に本書で使用している用語を示す。

用語	説明
SO	Security Objectives - セキュリティ対策方針
OSP	Organisational security policies – 組織のセキュリティ方針
ST	Security Target
TOE	Target of Evaluation – 評価対象
ABB	イオン・ボックス・バンク
RFID	Radio Frequency Identification －IC タグ。一意に識別できるタグ ID が記録されている。タグ ID は RFID 製造メーカで記録され、書き換え不可能。
R/W	RFID のリーダライタ
HDD	Hard Disk Drive
PIN	Personal Identification Number － 本書では、保守 PIN、設定 PIN、店舗 PIN を指す。
IF	InterFace
PRNG	pseudorandom number generator － 擬似乱数生成器
MISTY 鍵	申請情報や受付情報を暗号化する鍵(128bit)。共通鍵暗号方式の「MISTY1」。
RSA 公開鍵	センターサーバに転送する MISTY 鍵を TOE が暗号化する際に使用される鍵。センターサーバでは対応する RSA 秘密鍵を保持している。TOE には複数の RSA 公開鍵が格納され、暗号化時には設定ファイルで指定されている公開鍵を用いる。
端末	イオン・ボックス・バンクシステム向け専用端末。スーパーマーケットなどの店舗に設置される。
センターサーバ	端末がアクセスするセンターに設置されるサーバのこと。
受付情報	受付業務と一括投函の際に、端末からセンターへダイアルアップにて転送される情報で、MISTY 鍵で暗号化されている。
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 に記録される情報で、MISTY 鍵で暗号化されている。
設定ファイル	複数ある RSA 公開鍵の内、MISTY 鍵暗号化で使用する鍵を示す情報や TOE の設定を記録した ini ファイル。

Annex B. 参考文献

以下に参照文献及び本書作成に当たり参考にした文献を示す。

[CC] Common Criteria for Information Technology Security Evaluation, September 2006, Version 3.1 Revision 1
Part 1: Introduction and general model, CCMB-2006-09-001
Part 2: Security functional components, CCMB-2006-09-002

Part 3: Security assurance components, CCMB-2006-09-003

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2006, Version 3.1 Revision 1, CCMB-2006-09-004

[CC-J] 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, 2006 年 9 月, バージョン 3.1 改訂第 1 版, 平成 19 年 3 月翻訳第 1.2 版, 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

パート 1: 概説と一般モデル CCMB-2006-09-001

パート 2: セキュリティ機能コンポーネント CCMB-2006-09-002

パート 3: セキュリティ保証コンポーネント CCMB-2006-09-003

[CEM-J] 情報技術 セキュリティ評価のための共通方法 評価方法, 2006 年 9 月, バージョン 3.1 改訂第 1 版, CCMB-2006-09-004, 平成 19 年 3 月翻訳第 1.2 版, 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

[CBB-ST] 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
http://www.ipa.go.jp/security/jisec/c0024_it4036.htm

Annex C. 改定履歴

バージョン	発行日	内容	備考
1.0	2007 年 9 月 5 日	初版作成	—
1.1	2007 年 11 月 16 日	指摘により修正	—
1.2	2007 年 11 月 22 日	指摘により修正	—
1.3	2007 年 11 月 30 日	指摘により修正	—
1.4	2007 年 12 月 14 日	指摘により修正	—
1.5	2008 年 2 月 27 日	指摘により修正	—
1.6	2008 年 3 月 12 日	指摘により修正	—

— 以下 余白 —