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
日付: 2005 年 2 月 21 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 4
1.1. ST 識別 4
1.2. ST 概要 4
1.3. CC 適合の主張 5
1.4. 参考資料及び略号 5
1.4.1. 参考資料 5
1.4.2. 略語及び用語一覧 6
2. TOE 記述 8
2.1. CBB システム概要 8
2.2. CBB 端末の構成と TOE の範囲 9
2.3. TOE の保護対象情報資産 10
2.4. TOE の関係者 11
2.5. TOE の機能 12
2.5.1. アプリケーション機能 12
2.5.2. サポート機能 12
2.5.3. セキュリティ機能 12
2.6. 暗号鍵の管理 14
3. TOE セキュリティ環境 15
3.1. 前提条件 15
3.2. 脅威 15
3.3. 組織のセキュリティ方針 16
4. セキュリティ対策方針 17
4.1. TOE のセキュリティ対策方針 17
4.2. 環境のセキュリティ対策方針 17
5. IT セキュリティ要件 18
5.1. TOE セキュリティ要件 18
5.1.1. TOE セキュリティ機能要件 18
5.1.2. TOE セキュリティ保証要件 21
5.1.3. 最小機能強度(SOF)宣言 21
5.2. IT 環境のセキュリティ要件 21
6. TOE 要約仕様 22

6.1. IT セキュリティ機能 22
6.2. 機能強度主張 22
6.3. 保証手段 23
7. PP 主張 24
8. 根拠 25
8.1. セキュリティ対策方針根拠 25
8.2. セキュリティ要件根拠 27
8.2.1. TOE セキュリティ要件の根拠 27
8.2.2. IT 環境に対するセキュリティ要件の根拠 28
8.2.3. 依存性分析 28
8.2.4. セキュリティ要件の一貫性と相互補完 30
8.2.5. 最小機能強度レベルの適合性 30
8.3. TOE 要約仕様根拠 31
8.3.1. セキュリティ機能の根拠 31
8.3.2. 機能強度の根拠 32
8.3.3. セキュリティ機能のコンビネーション 32
8.3.4. 保証手段の根拠 32
8.4. PP 主張根拠 32
9. 改定履歴 33

1. ST 概説

本章では、ST 識別、ST 概要、CC 適合の主張について記述する。

1.1. ST 識別

ST 及び TOE の識別情報を以下に示す。

ST 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 セキュリティターゲット

バージョン: 2.0

作成日: 2005 年 2 月 21 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

CC 識別: CC Version2.1 (ISO/IEC 15408:1999), CCIMB Interpretations-0407 適用

TOE 識別: 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

上記 TOE には以下のものが含まれる。

- 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

キーワード: 金融端末、リテール、IC タグ、RFID、組込み機器

なお、識別された CC の日本語訳として以下のものを使用している。

- 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 :1999 年 8 月 バージョン 2.1 CCIMB-99-031, 平成 13 年 1 月翻訳第 1.2 版, 情報処理振興事業協会 セキュリティセンター
- 補足-0210 第 2 版, 平成 16 年 8 月, 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
- 補足-0407, 平成 16 年 8 月, 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

1.2. ST 概要

本 ST は、TOE であるコンビニ・ボックス・バンク(以下、CBB)端末のアプリケーションユニットのセキュリティ仕様を定めた文書である。TOE は、「CBB 業務アプリケーションソフトウェア(バージョン 1.0)」と、耐タンパセキュアボードである「TURBOMISTY」によって構成される。TOE が搭載される CBB 端末は、コンビニエンスストアに設置される金融端末であり、エンドユーザに支店来店予約や住所変更届け等の従来銀行窓口で行っていたサービスの一部を提供する。本サービスを可能にするため、TOE は申込受付機能や申込書取込機能を具備し、これらの機能を安全に運用するために通信機能、保守機能や「TURBOMISTY」による暗号化機能を有する。

1.3. CC 適合の主張

本 TOE は、下記の CC に適合している。

- 機能要件は、CC バージョン 2.1 パート 2 適合である。
- 保証要件は、CC バージョン 2.1 パート 3 適合である。
- 評価保証レベルは、EAL2 適合である。
- 本 ST が適合している PP はない。

1.4. 参考資料及び略号

本書作成にあたり参考にした資料や本書で使用する略語等を示す。

1.4.1. 参考資料

[CC] *Information technology – Security techniques – Evaluation criteria for IT security –,*
ISO/IEC 15408-1:1999 (E), Part 1: Introduction and general model,
ISO/IEC 15408-2:1999 (E), Part 2: Security functional requirements,
ISO/IEC 15408-3:1999 (E), Part 3: Security assurance requirements

[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,*
パート1 :概説と一般モデル 1999 年 8 月 バージョン 2.1 CCIMB-99-031 平成 13 年 1 月翻訳第 1.2 版, 情報処理振興事業協会 セキュリティセンター
パート2 : セキュリティ機能要件 1999 年 8 月 バージョン 2.1 CCIMB-99-032 平成 13 年 1 月翻訳第 1.2 版, 情報処理振興事業協会 セキュリティセンター
パート3 : セキュリティ保証要件 1999 年 8 月 バージョン 2.1 CCIMB-99-033 平成 13 年 1 月翻訳第 1.2 版, 情報処理振興事業協会 セキュリティセンター

[CEM] *Common Methodology for Information Technology Security Evaluation,*
Part 1: Introduction and general model, Version 0.6, 11.01.1997,
Part 2: Evaluation Methodology, Version 1.0, August 1999

[CEM-J] *情報技術セキュリティのための共通評価方法論, CEM-97/017*
CEM-97/017 パート1 :概説と一般モデル バージョン 0.6 97/01/11 平成 15 年 8 月翻訳第 1.1 版, 情報処理振興事業協会 セキュリティセンター
CEM-99/045 パート2 :評価方法論 バージョン 1.0 1999 年 8 月 2003-12-31 付け解釈組込み 平成 16 年 8 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

[FI] *CCIMB Interpretations-0407*

[FI-J02] *補足-0210 第 2 版，平成 16 年 8 月，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*

[FI-J04] *補足-0407，平成 16 年 8 月，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*

1.4.2. 略語及び用語一覧

1.4.2.1. CC 関連の用語

略語	説明
CC	Common Criteria
OSP	Organizational Security Policy - 組織のセキュリティ方針
SO	Security Objective - セキュリティ対策方針
SF	Security Function - セキュリティ機能
SFR	Security Functional Requirement - セキュリティ機能要件
SOF	Strength of Function - 機能強度
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

1.4.2.2. 本 ST 固有の用語

略語	説明
R/W	RFID のリーダライタ
HDD	Hard Disk Drive
PIN	Personal Identification Number – 本書では、サービスマンを認証するためのもの。サービスマンが管理。
IF	InterFace
MISTY 鍵	申込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 鍵ペア (RSA 公開鍵と RSA 秘密鍵)	MISTY 鍵を TOE 内で保持するために使用される RSA 暗号方式の鍵ペア(1024bit)。RSA 秘密鍵は CBB 端末出荷時に HSM に格納され、TOE は RSA 公開鍵で MISTY 鍵を暗号化されたものを保持する。MISTY 鍵を使用する時は HSM にて暗号化 MISTY 鍵を RSA 秘密鍵で復号させて取得する。
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。
暗号化 MISTY 鍵情報	ヘッダと暗号化 MISTY 鍵をまとめた総称。TOE が保持する。暗号鍵更新時は本情報が更新される。
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。TOE は本端末のアプリケーションソフトウェアと HSM。
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るサーバのこと。

略語	説明
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 内情報をリードする RFID リーダライタが接続されている。
来店予約サーバ	相談予約のときに CBB 端末がアクセスするサーバのこと。来店予約センターで顧客により管理されている。予約可能な支店・日時の情報を管理している。
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のこと。本書では FIPS140-2 の Level3 を取得した「TURBOMISTY」のこと。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。
SW	SoftWare – 本書では、CBB 端末に搭載されるアプリケーションソフトウェアのこと。
受付情報	CBB 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。口座番号、タグ ID 等からなり、MISTY 鍵で暗号化されている。
申込情報	申込書の RFID に記録される情報。暗証番号、口座番号等からなり、MISTY 鍵で暗号化されている。
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。
保守員	TOE の保守機能を使用できる特権を保有するサービスマン。
配送者	CBB 端末に投函された申込書をセンターに配送する業者。
HW 製造者	TOE 格納、CBB 端末の配送、初期暗号鍵の格納を実施する CBB 端末の製造者。
運用者	CBB システムによりエンドユーザに CBB サービスを提供する顧客。CBB システムで使用する暗号鍵の管理も行う。センターサーバの管理者や、受付端末を操作し申込書に記載された各種業務処理を行う人物を含む。
警備会社	TOE の保守機能を使用できる特権を保有するサービスマン。また、CBB 端末に設けられた防犯センサが感知した場合、緊急対処する。さらに、保守員による保守の際には同行する。
ヘッダ	暗号化 MISTY 鍵に付されており、鍵確認情報や端末固有情報などを含む。
HTTPS	Hypertext Transfer Protocol Security
鍵確認情報	復号された MISTY 鍵の正当性を確認する情報。
復号用情報	暗号化された受付情報や申込情報に付されている情報で、各情報を復号する際に用いられる。
端末固有情報	端末毎に異なる固有の情報。

2. TOE 記述

本章では、製品種別や TOE の物理的・論理的範囲について記述する。

2.1. CBB システム概要

本 TOE の製品種別は、金融端末のアプリケーションユニットである。本金融端末は、コンビニエンスストアに設置され、従来銀行窓口で行っていた諸手続き業務(e.g. 支店来店予約や住所変更届けなど)を 24 時間受け付ける CBB 端末である。従って、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。

Fig 2-1 に本 TOE を含めた CBB システムの概要図を示す。図中、灰色の部分が TOE である。本システムを運用する顧客のセンターにおけるエンドユーザ情報(e.g. 口座番号など)を管理するデータベース(DB)などは従来の顧客が使用している基幹システムを利用する。センターのサーバ(以下センターサーバ)における CBB システム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。

エンドユーザは、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、CBB 端末の磁気カードリーダにて口座番号を、操作パネルにてその口座の暗証番号を入力した後、申込書を CBB 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、入力された暗証番号、口座番号等(以下、これらを申込情報と記す)を暗号化し、R/W を介して復号時に使用される復号用情報と共に RFID に記録する。また、申込を受け付けた際、CBB 端末は、受付情報(口座番号、タグ ID 等)を暗号化し、上記復号用情報と共にダイアルアップにてセンターサーバへ転送する。受付情報に関し、個々の情報では機密性を維持する必要はないが、集合した情報ではプライバシーの観点から CBB 端末が保護する必要がある。以上の処理は、TOE の一部であるアプリケーションソフトウェア(以下、SW)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。そして、センターの受付端末に設けられたリーダライタにより RFID に記録された情報を読み出し、復号用情報から正しい暗号鍵を利用して、センターサーバにて復号する。復号した結果、口座番号とその暗証番号によりエンドユーザ本人であることが確認され、かつ、受信した受付情報を同じように復号した結果から CBB 端末で受け付けたことが確認された後、センターにて各事務手続きが処理される。

エンドユーザが本端末で支店来店予約などの相談予約を行う場合、CBB 端末は来店予約サーバにアクセスし、エンドユーザが希望する支店や来店予約時間等を予約する。本サーバは、来店予約センターにて顧客が管理している設備であり、予約可能な支店・日時の情報を管理している。この相談予約の操作においては操作パネルから入力された個人名や連絡先電話番号などが使用される。これらの情報もプライバシーの観点から CBB 端末が保護する必要があるが、TOE ではなく、OS(Fig 2-2 に後述)に組み込まれている HTTPS プロトコルを用いた機能で保護されている。

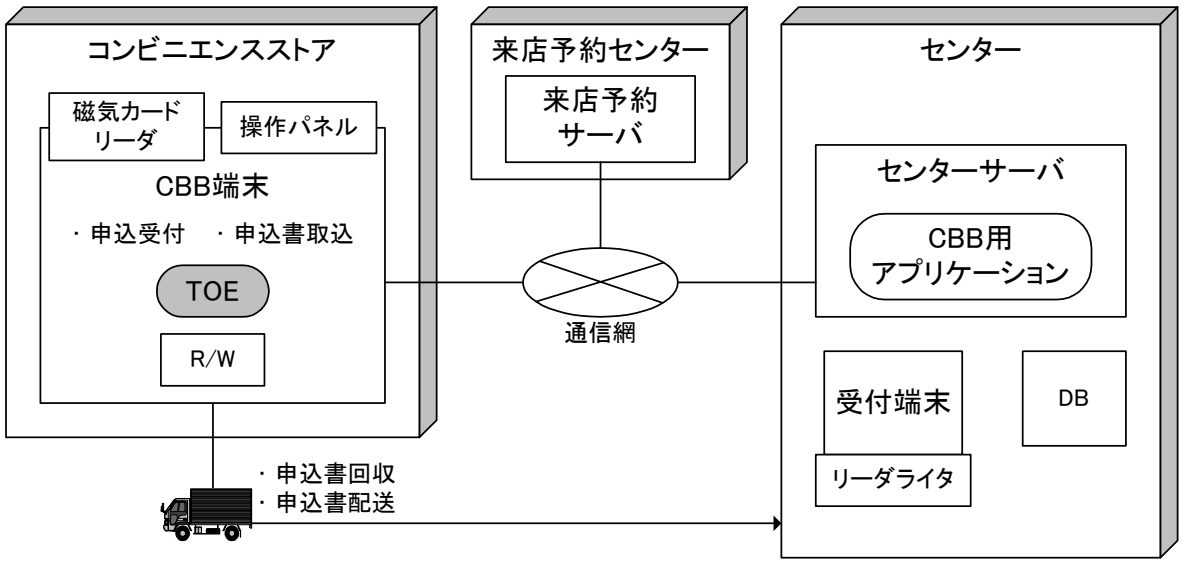

Fig 2-1: CBB システム構成図

2.2. CBB 端末の構成と TOE の範囲

Fig 2-2 に CBB 端末の構成と TOE の範囲を示す。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と HSM である。

CBB 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 HSM などは CBB 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。配送者が投函された申込書を回収する場合や、サービスマン(保守員や警備会社、2.4 章参照)による CBB 端末の保守作業(e.g. 定期点検、障害時の点検や暗号鍵更新)を実施する際に開錠される。以下、Fig 2-2 に記載した構成について説明する。なお、TOE の機能や TOE 外の機能との関係は 2.5 章で述べる。

- CBB 端末には物理錠が設置される(Fig 2-2 には図示していない)。
- 操作パネルは、エンドユーザが暗証番号を CBB 端末に入力するために用いられる。保守する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、エンドユーザの銀行カードから口座番号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ものである。暗証番号は用紙に記入されず、暗号化された状態で RFID 内部のメモリに保持される。
- R/W は申込書に格納される RFID と通信可能なもの。RFID に対して情報の記録・読み込みを行う。
- 取込機構は、利用者が投函した申込書を CBB 端末内部に取り込み(SW の制御による)、保管する。一旦、取り込んだ申込書は、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。HW 製造者によって CBB 端末向けに製造される。
- 通信(無線通信)は、受付情報転送、相談予約やデータ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センターサーバと来店予約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、暗号鍵更新など CBB 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 SP1 を使用する。CBB 端末の起動・停止、HTTPS や TCP/IP の通信制御などを行う。
- HDD に OS や SW、暗号化 MISTY 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。
- TOE は、SW と HSM から構成され、施錠された筐体内部に格納されている。SW は、CBB 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。HSM は、FIPS140-2 の Level3 を取得した「TURBOMISTY[1]」(三菱電機インフォメーションシステムズ社製)を使用し、受付情報や申込情報の暗号化(アルゴリズム MISTY1)、暗号化 MISTY 鍵の復号(アルゴリズム RSA)を行う(暗号操作の詳細は 2.5 章参照)。

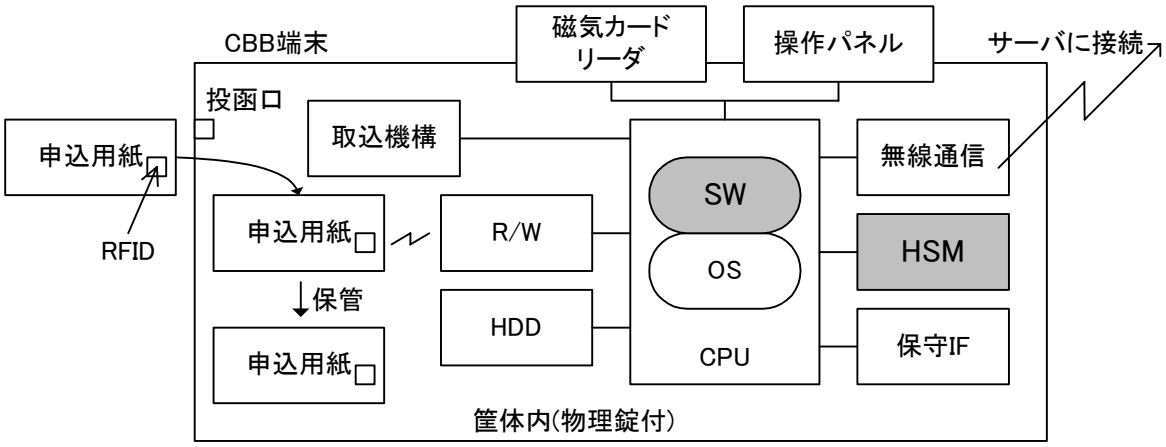

Fig 2-2: CBB 端末の構成

2.3. TOE の保護対象情報資産

上述したように、TOE は、コンビニエンスストアに設置される CBB 端末に搭載され、CBB システムは、エンドユーザの本人認証に暗証番号を用いる。この情報は、従来の銀行システムにおいても機密にしなければならない情報であり、CBB システムとしても保護すべき情報である。すなわち、本 TOE が保護すべき情報資産は、エンドユーザの暗証番号であり、その機密性を維持する。なお、CBB 端末においてエンドユーザの認証を行っていないので、本 TOE において暗証番号は User Data として扱われる。

[1] CMVP 認証番号#359
http://csrc.nist.gov/cryptval/140-1/1401val2003.htm

2.4. TOE の関係者

本 TOE や CBB 端末の開発に携わる関係者を Fig 2-3 に示す。

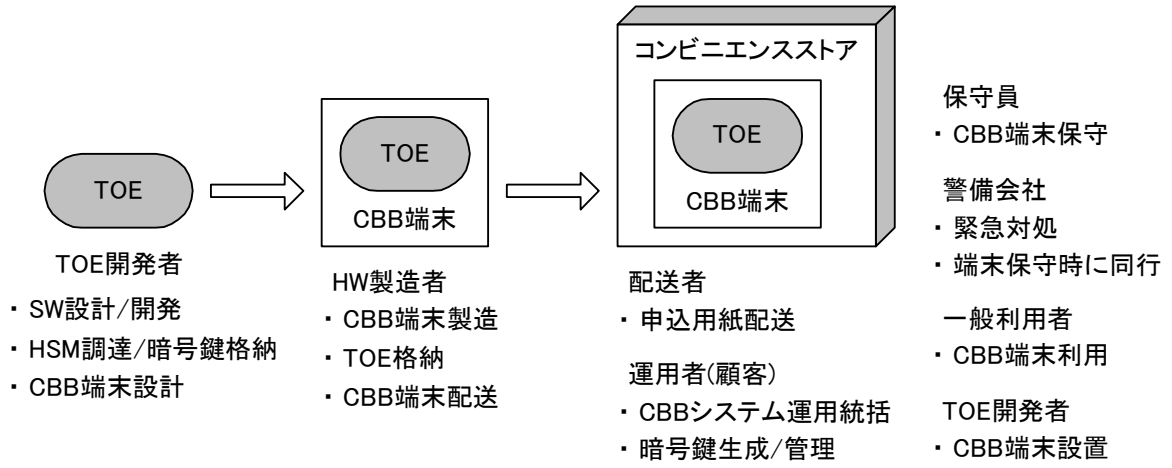

Fig 2-3: CBB 端末の関係者

以下に Fig 2-3 も含めて TOE の関係者を説明する。

一般利用者	CBB 端末を利用するエンドユーザ。
保守員	TOE の保守機能を使用できる特権を保有するサービスマン。
配送者	CBB 端末に投函された申込書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 格納、CBB 端末の配送、初期暗号鍵の格納を実施する CBB 端末の製造者。
運用者	本システムにより一般利用者に CBB サービスを提供する顧客。CBB システムで使用する暗号鍵の管理をセンターにて行う。センターサーバや来店予約サーバの管理者や、受付端末を操作し申込書に記載された各種業務処理を行う人物を含む。
警備会社	TOE の保守機能を使用できる特権を保有するサービスマン。また、CBB 端末に設けられた防犯センサ(Fig 2-2 には図示していない)が感知した場合、緊急対処する。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)。
TOE 開発者	主に TOE の SW の開発、HSM を調達し暗号鍵(RSA 秘密鍵)を格納、HW 製造者への TOE 配付を行う。

2.5. TOE の機能

TOE は、CBB システムのサービスを一般利用者に提供する。そのため、TOE が具備する機能は、申込受付機能や申込書取込機能などの一般利用者向けのアプリケーション機能と、サービスを提供するためのセキュリティ機能、サポート機能に大別される。セキュリティ機能とサポート機能は、一般利用者が意識せず間接的に使用される機能や CBB 端末の保守に使用される機能である。以下にこれらの機能及び TOE 外との関係について説明する。

2.5.1. アプリケーション機能

- 申込受付機能

事務手続きにおいて、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口座番号や暗証番号を R/W を介して RFID に記録する機能。また、相談予約において、一般利用者が支店の来店時間を予約できる。

- 申込書取込機能

事務手続きにおいて、一般利用者が所定事項を記入した申込書を投函口より CBB 端末内に取り込み、保管するために、取込機構を制御する機能。CBB 端末内に投函された申込書は、物理錠により筐体を開錠しない限り、取り出せない。

2.5.2. サポート機能

- 通信機能
  - アップロード

    事務手続きにおいて、CBB 端末が申し込みを受け付けたことをダイアルアップにてセンターサーバに転送する機能。転送する情報は受付情報を暗号化したもの。また、相談予約においては、来店予約サーバにアクセスする。さらに、SW は 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、サーバ(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機能。ダウンロードするファイルは運用者だけがサーバに格納できる。なお、CBB 端末で使用される暗号鍵は、ダウンロードによって格納されるのではなく、保守機能(2.5.3 章参照)により格納される。

2.5.3. セキュリティ機能

- 暗号化機能

運用時の暗号操作(MISTY 鍵取得と各情報暗号化)を示した Fig 2-4 を用いて説明する。

事務手続きの申込受付において、RFID に申込情報を記録する前、及び受付情報を転送する前にこれらの情報を TOE の一部である HSM にて暗号アルゴリズム「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、暗号アルゴリズム「RSA」で暗号化された状態(以下、暗号化 MISTY 鍵)で TOE が保持している。なお、TOE が保持するのは、暗号化 MISTY 鍵とヘッダ(後述)である(これらを総称して暗号化 MISTY

鍵情報と呼ぶ)。

MISTY 鍵使用時は、暗号化 MISTY 鍵を HSM にてアルゴリズム「RSA」で復号させることで取得する。復号後、暗号化 MISTY 鍵情報のヘッダ内の鍵確認情報と、復号結果に含まれている鍵確認情報とを比較し、これらが一致していた場合、正しい MISTY 鍵と判断する。そして、受付情報や申込情報を HSM にてアルゴリズム「MISTY1」で暗号化し、暗号結果の先頭に正しい復号を実現するための復号用情報を付したものを RFID に記録、もしくは転送する。

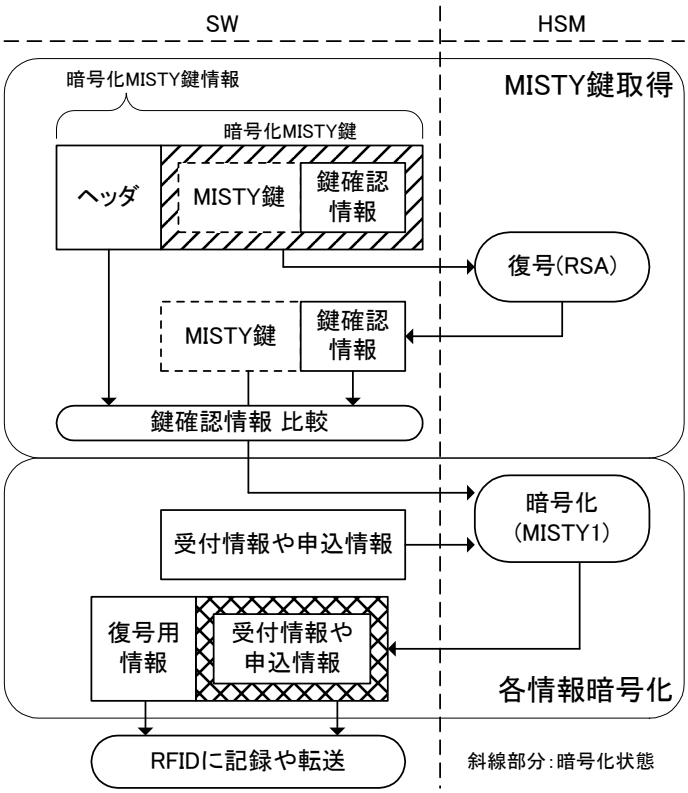

Fig 2-4: 運用時の暗号操作

なお、HSM には以下の主な機能が搭載されているが、本 TOE のセキュリティ機能に含まれる機能は、「MISTY1 の暗号化」と「RSA 秘密鍵を用いた復号」である。これら以外の機能は TOE のセキュリティ機能ではない。

- RSA 公開鍵対の生成
- RSA 公開鍵を用いた暗号化と署名検証
- RSA 秘密鍵を用いた復号と署名生成
- Triple-DES/DES/MISTY1 の暗号・復号処理
- メッセージダイジェスト生成
- 乱数生成
- 耐タンパ機能(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機能)

- 保守機能

サービスマン(保守員と警備会社)を識別・認証し、CBB 端末の保守作業を提供する機能である。主な保守作業には定期及び障害時の点検作業、TOE が保持する暗号化 MISTY 鍵情報を更新する暗号鍵更新作業がある。

これらの内、暗号鍵更新作業がセキュリティ上重要な作業である。これらを実現するための保守機能には定期及び障害時の点検機能、暗号鍵更新機能、および正規のサービスマンを識別・認証する識別・認証機能が含まれる。この内、鍵更新機能と識別・認証機能がセキュリティ機能である。識別・認証機能における認証のメカニズムは PIN で、続けて 3 回認証に失敗した場合、PIN の入力を 5 分間受け付けない。PIN は TOE 開発者が格納した乱数から生成したものを使用する。暗号鍵更新機能で TOE は、自身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(古い鍵情報に上書き)。

2.6. 暗号鍵の管理

以下、暗号鍵の更新も含めた管理に関して Fig 2-5 を用いて説明する。

MISTY 鍵と RSA 鍵ペアは、センターサーバにて生成される。この際、RSA 鍵ペアは複数生成される。MISTY 鍵は鍵確認情報と共に所定の RSA 公開鍵で暗号化されて、暗号化 MISTY 鍵が生成される。これらの鍵確認情報、RSA 鍵ペアはセンターにて管理され、CBB 端末から送られてきた各情報の復号や新しい鍵を生成するのに使用される。

生成された RSA 秘密鍵は、TOE 開発者に送付され、HSM に格納される。その後、HSM は HW 製造者に送付され、CBB 端末に格納される。一方、生成された暗号化 MISTY 鍵は、ヘッダと共に、HW 製造者により CBB 端末内の TOE に格納される。

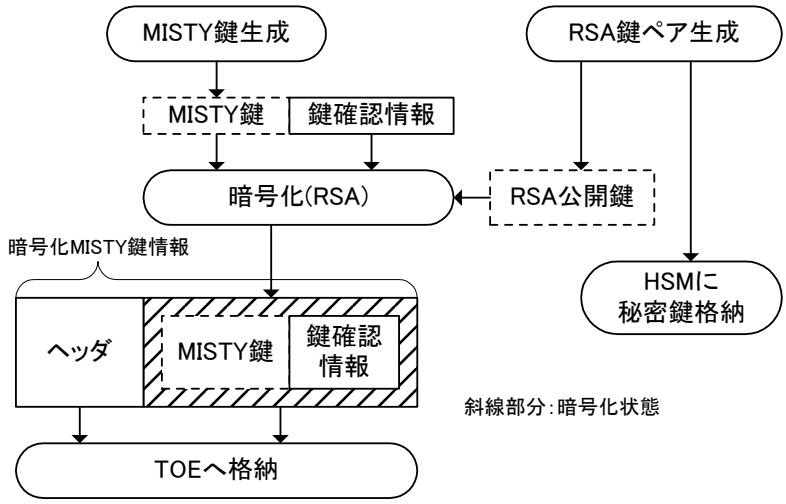

Fig 2-5: 出荷時の暗号鍵管理

暗号鍵更新時のフローも基本的に同じである。センターにて新しいバージョンの MISTY 鍵が作成され、出荷時と同じように所定の RSA 公開鍵で暗号化された後、新しいヘッダと共に、暗号化 MISTY 鍵情報がサービスマンによって TOE に格納される。

以上に示したように、暗号鍵更新は、TOE にとって暗号化 MISTY 鍵情報の更新である。なお、暗号化 MISTY 鍵情報は端末毎にユニークである。

3. TOE セキュリティ環境

本章では、前提条件、脅威、組織のセキュリティ方針について記述する。

3.1. 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。

3.2. 脅威

脅威の対象となる段階は、CBB 端末がコンビニエンスストアに設置されて運用されている段階のものである。HW 製造者での段階は、前提条件により脅威は存在しない。

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。

3.3. 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。

4. セキュリティ対策方針

本章では、TOE で達成するセキュリティ対策方針、環境で達成するセキュリティ対策方針について記述する。

4.1. TOE のセキュリティ対策方針

O.MANAGE	TOE は、保守作業を行うための機能を具備し、それをサービスマンのみに提供しなければならない。
O.PROT_INFO	TOE は、申込情報と受付情報が暴露されることを防がなければならない。

4.2. 環境のセキュリティ対策方針

OE.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しなければならない。
OE.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しなければならない。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、サービスマン及び HW 製造者としての役割を担う各組織の責任者は、許可された作業のみを忠実に遂行する人材を任命しなければならない。
OE.HW_DEV	HW 製造者は、操作パネルの覗き見を防止する手段と物理錠を CBB 端末に設置しなければならない。
OE.HW_MANAGE	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なければならない。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て行わなければならない。
OE.OS	OS は、HTTPS プロトコルの通信機能を持たなければならない。
OE.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)にのみ接続されなければならない。
OE.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なければならない。

5. IT セキュリティ要件

本章では、TOE またはその環境が満たしていなければならない IT セキュリティ要件について記述する。

IT セキュリティ要件の操作は以下のように記述した。

- 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

5.1. TOE セキュリティ要件

5.1.1. TOE セキュリティ機能要件

本章では、 TOE に対する IT セキュリティ機能要件を定義する。

5.1.1.1. クラス FCS: 暗号サポート

FCS_COP.1(M)	暗号操作
下位階層:	なし
FCS_COP.1.1(M)	TSF は、[割付: 暗号技術仕様書 MISTY1 (updated 2002 年 5 月 13 日)[2]] に合致する、特定された暗号アルゴリズム[割付: MISTY1[2]] と暗号鍵長[割付: 128bits] に従って、[割付: 暗号化] を実行しなければならない。
依存性:	[FDP_ITC.1 セキュリティ属性なし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(R)	暗号操作
下位階層:	なし
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: 復号] を実行しなければならない。
依存性:	[FDP_ITC.1 セキュリティ属性なし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

[2] 「MISTY1」は、CRYPTREC で採択された暗号アルゴリズムであり、上記標準は以下の URL に公開されている。
http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/cryptrec20030425_spec01.html

5.1.1.2. クラス FIA: 識別と認証

FIA_AFL.1　認証失敗時の取り扱い

下位階層:　なし

FIA_AFL.1.1　TSF は、[割付: 最後に成功した認証以降のサービスマン認証失敗] 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: 5 分間の PIN 入力拒否] をしなければならない。

依存性:　FIA_UAU.1 認証のタイミング

FIA_UAU.1　認証のタイミング

下位階層:　なし

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: 一般利用者に提供する CBB 端末としてのサービス提供] を許可しなければならない。

FIA_UAU.1.2　TSF は、その利用者を代行する他の TSF 調停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。

依存性:　FIA_UID.1 識別のタイミング

FIA_UID.1　識別のタイミング

下位階層:　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: 一般利用者に提供する CBB 端末としてのサービス提供] を許可しなければならない。

FIA_UID.1.2　TSF は、その利用者を代行する他の TSF 調停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。

依存性:　なし

5.1.1.3. クラス FMT: セキュリティ管理

FMT_MSA.2　セキュアなセキュリティ属性

下位階層:　なし

FMT_MSA.2.1　TSF は、セキュアな値だけがセキュリティ属性として受け入れられることを保証しなければならない。

依存性:　ADV_SPM.1 非形式的 TOE セキュリティ方針モデル
[FDP_ACC.1 サブセットアクセス制御 または

FDP_IFC.1 サブセット情報フロー制御]

FMT_MSA.1 セキュリティ属性の管理

FMT_SMR.1 セキュリティ役割

FMT_MTD.1 TSF データの管理

下位階層: なし

FMT_MTD.1.1 TSF は、[割付: 暗号化 MISTY 鍵情報] を[選択: [割付: 更新]] する能力を[割付: サービスマン] に制限しなければならない。

依存性: FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

FMT_SMF.1 管理機能の特定

下位階層: なし

FMT_SMF.1.1 TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない:[割付:暗号化 MISTY 鍵情報の更新]。

依存性: なし

FMT_SMR.1 セキュリティ役割

下位階層: なし

FMT_SMR.1.1 TSF は、役割[割付: サービスマン] を維持しなければならない。

FMT_SMR.1.2 TSF は、利用者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

5.1.1.4. クラス FPT: TSF の保護

FPT_RVM.1 TSP の非バイパス性

下位階層: なし

FPT_RVM.1.1 TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。

依存性: なし

5.1.2. TOE セキュリティ保証要件

本 TOE の評価保証レベルは EAL2 である。Table 5-1 に選択された保証コンポーネント名称を示す。

Table 5-1: 保証要件

クラス	コンポーネント名称
構成管理	ACM_CAP.2 構成要素
配付と運用	ADO_DEL.1 配付手続き ADO_IGS.1 設置、生成、及び立上げ手順
開発	ADV_FSP.1 非形式的機能仕様 ADV_HLD.1 記述的上位レベル設計 ADV_RCR.1 非形式的対応の実証
ガイダンス	AGD_ADM.1管理者ガイダンス AGD_USR.1 利用者ガイダンス
テスト	ATE_COV.1 カバレージの証拠 ATE_FUN.1 機能テスト ATE_IND.2 独立試験- サンプル
脆弱性評定	AVA_SOF.1 TOE セキュリティ機能強度評価 AVA_VLA.1 開発者脆弱性分析

5.1.3. 最小機能強度(SOF)宣言

本 TOE における最小機能強度は SOF-基本である。但し、暗号アルゴリズム(MISTY1 及び RSA)の強度は本機能強度の対象としない。

5.2. IT 環境のセキュリティ要件

IT 環境のセキュリティ要件は定義しない。

6. TOE 要約仕様

本章では、TOE の要約仕様を記述する。

6.1. IT セキュリティ機能

本章では、5.1.1 章で記述した TOE セキュリティ機能要件を満たす TOE の IT セキュリティ機能について説明する。また、各セキュリティ機能の記述の後に、対応する TOE 機能要件を示す。以下に示すように、各 IT セキュリティ機能は少なくとも一つの TOE 機能要件に対応している。

SF.CRYPT　TOE は、RFID に申込情報を記録する前、及び受付情報を転送する前にこれらの情報を 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)で暗号化する。これらの暗号化に使用する MISTY 鍵は、保持している暗号化 MISTY 鍵を HSM にてアルゴリズム RSA(PKCS#1 準拠、1024bits)で復号させて取得する。復号後、TOE は暗号化 MISTY 鍵情報のヘッダと、復号結果とに含まれている鍵確認情報を比較し、両者が一致している場合、正しい MISTY 鍵と判断して使用する。

FCS_COP.1(M)、FCS_COP.1(R)、FPT_RVM.1、FMT_MSA.2

SF.MANAGE　TOE は、サービスマンを識別・認証する。認証のメカニズムは PIN である。サービスマンの識別・認証前に、一般利用者に対して CBB 端末としてのサービス提供を許可する。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。
また、暗号化 MISTY 鍵更新時、TOE は、自身が保有する端末固有情報と暗号化 MISTY 鍵情報内の端末固有情報とを比較し、一致した場合新しい暗号化 MISTY 鍵情報を受け入れる。

FIA_AFL.1 、FIA_UAU.1 、FIA_UID.1 、FMT_MSA.2 、FMT_SMF.1 、FMT_SMR.1 、FPT_RVM.1、FMT_MTD.1

6.2. 機能強度主張

SF.MANAGE におけるサービスマン認証機能(PIN)が確率的あるいは順列的メカニズムに基づくセキュリティ機能である。SF.MANAGE はセキュリティ機能強度として SOF-基本を持つ。

6.3. 保証手段

本章では、5.1.2 章で記述した TOE セキュリティ保証要件を満たす保証手段を説明する。保証手段として提供される文書や TOE を、対応する保証コンポーネントと共に Table 6-1 に示す。これから明らかなように、各保証手段は、少なくとも一つの TOE 保証要件に対応している。

Table 6-1: 保証要件と対応する保証手段

コンポーネント	保証手段
ACM_CAP.2	・ 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 構成管理文書, バージョン 1.3, 2005 年 2 月 10 日
ADO_DEL.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 配送手順書, バージョン 1.3, 2005 年 2 月 4 日
ADO_IGS.1	・ 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 業務アプリケーション 設置/生成/立ち上げ手順書, バージョン 1.0, 2005 年 2 月 4 日
ADV_FSP.1	・ CBB 業務アプリケーションユニット セキュリティ機能仕様書, バージョン 1.4, 2005 年 1 月 26 日
ADV_HLD.1	・ CBB 業務アプリケーションユニット 上位レベル設計書, バージョン 1.3, 2005 年 1 月 27 日
ADV_RCR.1	・ CBB 業務アプリケーションユニット 対応分析書, バージョン 1.3, 2005 年 2 月 21 日
AGD_ADM.1	・ 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(保守会社), 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 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 インストールガイド, バージョン 1.0, 2005 年 2 月 4 日
AGD_USR.1	・ 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
ATE_COV.1	・ CBB 業務アプリケーションユニット テストカバレージ分析書, バージョン 1.2, 2005 年 1 月 27 日
ATE_FUN.1	・ CBB 業務アプリケーションユニット セキュリティ機能テスト仕様書/報告書, バージョン 1.3, 2005 年 1 月 27 日
ATE_IND.2	・ TOE
AVA_SOF.1	・ CBB 業務アプリケーションユニット 機能強度分析書, バージョン 1.1, 2005 年 2 月 21 日
AVA_VLA.1	・ CBB 業務アプリケーションユニット 脆弱性分析書, バージョン 1.4, 2005 年 2 月 21 日

7. PP 主張

本 ST が適合している PP はない。

8. 根拠

本章では、セキュリティ対策方針根拠、セキュリティ要件根拠、TOE 要約仕様根拠、PP 主張根拠について記述する。

8.1. セキュリティ対策方針根拠

脅威・前提条件・組織のセキュリティ方針(以下、OSP)とセキュリティ対策方針(以下、SO)との対応関係を Table 8-1 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・前提条件・OSP に対応している。

Table 8-1: 脅威・前提条件・OSP と SO の対応関係

	O.MANAGE	O.PROT_INFO	OE.PIN	OE.OPERATE	OE.KEY	OE.NO_HARM	OE.HW_DEV	OE.HW_MANAGE	OE.OS	OE.CONNECT	OE.CHANNEL
T.RFID_INFO		×									
P.PRIVACY		×							×		
P.MAINTE	×										
A.PIN			×								
A.OPERATE				×							
A.CASE_KEY					×		×				
A.NO_HARM						×					
A.HW_DEV						×		×			
A.CASE							×				
A.CONNECT										×	
A.CHANNEL											×

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 に記録される申込情報が暴露されることが防止され、暗証番号の暴露を防止することができるからである。

P.PRIVACY は、O.PROT_INFO と OE.OS によって達成される。なぜなら、O.PROT_INFO によって、事務手続き処理における受付情報と申込情報の機密性を維持できるからである。また、OE.OS によって、相談予約にて一般利用者が入力した情報を来店予約サーバに転送する際の機密性が維持できるからである。

P.MAINTE は、O.MANAGE 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 CBB 端末の

保守作業を行うことができるからである。

A.PIN は OE.PIN によって実現されることは自明である。なぜなら、OE.PIN は A.PIN の文章を概ね再掲しているからである。

A.OPERATE が OE.OPERATE によって実現されることは自明である。なぜなら、OE.OPERATE は A.OPERATE の文章を概ね再掲しているからである。

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 CBB 端末に設置され、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、OE.NO_HARM によって配送者とサービスマンの信頼性が保証されるからである。

A.HW_DEV が OE.NO_HARM と OE.HW_MANAGE によって実現される。なぜなら、OE.NO_HARM によって HW 製造者の信頼性が保証され、OE.HW_MANAGE によって、HW 製造者による TOE の管理や TOE を格納した CBB 端末の管理・物理錠の施錠が保証されるからである。

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暗証番号の盗み見を困難にする CBB 端末が開発されるからである。

A.CONNECT は OE.CONNECT によって実現されることは自明である。なぜなら、OE.CONNECT は A.CONNECT の文章を概ね再掲しているからである。

A.CHANNEL は OE.CHANNEL によって実現されることは自明である。なぜなら、OE.CHANNEL は A.CHANNEL の文章を概ね再掲しているからである。

8.2. セキュリティ要件根拠

本章では、IT セキュリティ要件が SO を満たすのに適し、かつ SO にまでたどれることを実証する。

8.2.1. TOE セキュリティ要件の根拠

8.2.1.1. TOE 機能要件の根拠

TOE の SO(環境と TOE の SO も含む)と TOE 機能要件の対応関係を Table 8-2 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 TOE 機能要件は、少なくとも一つの TOE の SO に対応している。

Table 8-2: TOE の SO と TOE 機能要件の対応関係

	FCS_COP.1(M)	FCS_COP.1(R)	FIA_AFL.1	FIA_UAU.1	FIA_UID.1	FMT_MSA.2	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_RVM.1
O.MANAGE			×	×	×	×	×	×	×	×
O.PROT_INFO	×	×				×				×

以下、各 TOE 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.MANAGE は、主に FIA_UAU.1、FIA_UID.1、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1、FPT_RVM.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、識別・認証されたサービスマンに対してのみ保守機能、すなわち暗号化 MISTY 鍵情報の更新する機能が提供されることが保証されるからである。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、サービスマン認証の機能を強化し、FMT_MSA.2 によって暗号化 MISTY 鍵情報更新時にセキュアな鍵情報のみの更新を許可することを保証している。

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込情報の暴露が防止されるからである。また、MISTY の暗号鍵は暗号アルゴリズム「RSA」で暗号化された状態で保持されているので、使用時は FCS_COP.1(R)にて復号する。また、FMT_MSA.2 によって、MISTY 鍵使用前には MISTY 鍵が正しく復号されていることが保証される。さらに、FPT_RVM.1 によって、受付情報がセンターに転送される前に、そして、申込情報が RFID に記録される前に TOE がこれらの情報を暗号化することが保証される。

8.2.1.2. TOE 保証要件の妥当性

本 TOE が搭載される CBB 端末は、コンビニエンスストアに設置されるので、誰でも本端末にアクセスできる。また、一般利用者の銀行口座の暗証番号を取り扱っているので、高いセキュリティが要求される。しかし、CBB 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、CBB 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。このような CBB 端末のアプリケーションユニットである TOE の評価保証レベルは、EAL2 が妥当である。

8.2.2. IT 環境に対するセキュリティ要件の根拠

IT 環境の要件は定義されていないので、根拠は示さない。

8.2.3. 依存性分析

まず、機能要件に関して分析する。

Table 8-3 に本 ST 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示す。

Table 8-3: 機能要件の依存性分析結果

選択した機能要件	依存する要件	満たしている要件	分析結果
FCS_COP.1(M)	[FDP_ITC.1 または FCS_CKM.1]、FCS_CKM.4、FMT_MSA.2	FMT_MSA.2	依存性は満たされていない(根拠は後述①)。
FCS_COP.1(R)	[FDP_ITC.1 または FCS_CKM.1]、FCS_CKM.4、FMT_MSA.2	—	依存性は満たされていない(根拠は後述②)。
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	依存性は満たされている。
FIA_UAU.1	FIA_UID.1	FIA_UID.1	依存性は満たされている。
FIA_UID.1	なし	—	—
FMT_MSA.2	[FDP_ACC.1 または FDP_IFC.1]、FMT_MSA.1、FMT_SMR.1、ADV_SPM.1	FMT_SMR.1	依存性は満たされていない(根拠は後述③と④)。
FMT_MTD.1	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1	依存性は満たされている。
FMT_SMF.1	なし	—	—
FMT_SMR.1	FIA_UID.1	FIA_UID.1	依存性は満たされている。
FPT_RVM.1	なし	—	—

Table 8-3 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_COP.1(M)が依存する FCS_CKM.4 と[FDP_ITC.1 または FCS_CKM.1]について

FCS_COP.1(M)が依存する FCS_CKM.4 と[FDP_ITC.1 または FCS_CKM.1]は本 ST では選択されていない。以下、満たしていない根拠について説明する。

FCS_COP.1(M)が対象とする暗号鍵はMISTY鍵である。本暗号鍵は、CBB端末出荷時も運用時(暗号鍵更新時)も同様に、TOE外にて作成される。具体的には、センターサーバによって作成され、RSA公開鍵で暗号化された状態(暗号化 MISTY 鍵情報)でサービスマン(出荷時は HW 製造者)によって TOE に記録される。また、CBB 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、かつ信頼できないサブジェクトは TOE 内に存在しない。従って、[FDP_ITC.1 または FCS_CKM.1]や FCS_CKM.4 は機能要件として必要ない。

② FCS_COP.1(R)の依存性について

FCS_COP.1(R)が依存する[FDP_ITC.1 または FCS_CKM.1]、FCS_CKM.4、FMT_MSA.2 は本 ST では選択されていない。以下、満たしていない根拠について説明する。

FCS_COP.1(R)が対象とする暗号鍵は RSA 秘密鍵である。本暗号鍵は、センターにて複数作成され、TOE 開発者によってHSMに記録される。それ以降、新たに鍵をHSM内部で作成することも、外部から新しい鍵を格納することもない。従って、[FDP_ITC.1 または FCS_CKM.1]は機能要件として必要ない。
また、CBB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、かつ信頼できないサブジェクトは TOE 内に存在しないので、暗号鍵を破棄する必要がない。すなわち、FCS_CKM.4 は機能要件として必要ない。
さらに、FMT_MSA.2 に関して、RSA 秘密鍵に関してセキュアな値だけがセキュリティ属性として受け入れられなくても、TOE は RSA 復号後に MISTY 鍵が正しく復号されていることを確認している(FCS_COP.1(M)が依存する FMT_MSA.2)ので、TOE のセキュリティ上問題ない。従って、FMT_MSA.2 は機能要件として必要ない。

③ FMT_MSA.2 の他の機能要件への依存性について

この機能要件が依存する機能要件において、FMT_SMR.1 は選択されているが、[FDP_ACC.1 または FDP_IFC.1]、FMT_MSA.1 は選択されていない。これは、CBB 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、かつ信頼できないサブジェクトは TOE 内に存在しないので、暗号鍵や暗号化 MISTY 鍵情報に対するアクセス制御、フロー制御やセキュリティ属性の管理が必要ないからである。

④ FMT_MSA.2 の ADV_SPM.1 への依存性について

FMT_MSA.2 に関連する暗号鍵は MISTY 鍵である。以下、それぞれについて述べる。
MISTY 鍵は、上述したように、出荷時も更新時も RSA 公開鍵で暗号化された状態で TOE に格納される。この際、TOEは、自身が保有する端末固有情報と記録される暗号化MISTY鍵情報内のヘッダに含まれる端末固有情報とを比較し、一致した場合、TOEは自身が使用する正しい鍵情報とみなして受け入れる。一致しない場合、暗号化 MISTY 鍵情報を受け入れない。また、MISTY 鍵を使用する時(i.e. MISTY 暗号化時)は、HSM にて暗号化 MISTY 鍵を RSA 復号させ、復号された MISTY 鍵に付加されている鍵確認情報と、暗号化 MISTY 鍵情報内のヘッダに含まれる鍵確認情報とを比較し、一致した場合のみ、正しく RSA 復号できたものとして、その

MISTY 鍵を使用する。一致しない場合は、MISTY 鍵の使用を中止する。

以上に示したセキュアな値の明確な定義とその理由により、本機能要件が依存する ADV_SPM.1 は本評価において必要ない。

以上に示したように、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、セキュリティ保証要件は、[CC]で規定された EAL2 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 IT セキュリティ要件の依存性は問題がない。

8.2.4. セキュリティ要件の一貫性と相互補完

8.2.3 章にて、本 ST で選択された IT セキュリティ要件のセットは、それぞれの依存関係を満たしており、満たしていない依存性については根拠を示した。

以下、本 ST で選択されている機能要件を各イベントに分類し、それぞれについて説明する。

サービスマンの識別認証に関わる要件(FIA_UAU.1、FIA_UID.1、FIA_AFL.1) は依存関係にあるので、互いに矛盾したり競合したりせずに、相互にサポートしているといえる。暗号操作に関わる要件(FCS_COP.1(M)、FCS_COP.1(R) 、FMT_MSA.2) や保守に関わる要件 (FMT_SMF.1 、FMT_SMR.1 、FMT_MSA.2 、FMT_MTD.1)においては、これらが矛盾せず、相互に補完していることは明白である。

また、以上に述べた機能要件以外では、FPT_RVM.1 によって保守機能の前に識別・認証が実施され、受付情報や申込情報が TOE 外部に移動する前に暗号化が実施されることが保証される。TOE に信頼できないサブジェクトはおらず、セキュリティドメインを維持する必要はなく、非活性化される TOE 機能要件はない。さらに、FPT_RVM.1 により TOE の保守作業を行うことができるのは正当なサービスマンのみであるので、監査に関する FAU クラスの要件は必要ない。

以上より、選択された機能要件は内部的に一貫し、相互に補完し合っているといえる。

一方、保証要件は、[CC]で規定された EAL2 を選択しているので内部的に一貫していることは明白である。また、[ST]で選択された機能要件と EAL2 の間に矛盾は無い事も明らかである。

以上の分析より、本 ST で選択された IT セキュリティ要件は内部的に一貫し、相互に補完し合っていると言える。

8.2.5. 最小機能強度レベルの適合性

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。つまり、最小機能強度は SOF-基本で妥当である。また、O.MANAGE によりサービスマンが TOE にアクセスする際には、最小機能強度 SOF-基本で十分であり、また一貫している。

8.3. TOE 要約仕様根拠

8.3.1. セキュリティ機能の根拠

6.1 章に示したセキュリティ機能と機能要件の対応関係の正当性を Table 8-4 に示す。Table 8-4 中、正当化は、各セキュリティ機能の記述でどの内容の部分が TOE の各機能要件に対応しているかという観点で記述した。なお、下線は、注意すべき点、注目すべき点についての表記である。

このように、すべての TOE 機能要件は各セキュリティ機能によって満たされている。

Table 8-4: セキュリティ機能と機能要件の対応関係の根拠

TOE 機能要件	該当する各セキュリティ機能の記述
FCS_COP.1(M)	SF.CRYPT TOE は、RFID に申込情報を記録する前、及び受付情報を転送する前にこれらの情報を 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)で暗号化する。…
FCS_COP.1(R)	SF.CRYPT …これらの暗号化に使用する MISTY 鍵は、保持している暗号化 MISTY 鍵を HSM にてアルゴリズム RSA(PKCS#1 準拠、1024bits)で復号させて取得する。…
FIA_AFL.1	SF.MANAGE …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。…
FIA_UAU.1 FIA_UID.1	SF.MANAGE TOE は、サービスマンを識別・認証する。認証のメカニズムは PIN である。サービスマンの識別・認証前に、一般利用者に対して CBB 端末としてのサービス提供を許可する。…
FMT_MSA.2	SF.CRYPT …復号後、TOE は暗号化 MISTY 鍵情報のヘッダと、復号結果とに含まれている鍵確認情報を比較し、両者が一致している場合、正しい MISTY 鍵と判断して使用する。 SF.MANAGE …また、暗号化 MISTY 鍵更新時、TOE は、自身が保有する端末固有情報と暗号化 MISTY 鍵情報内の端末固有情報とを比較し、一致した場合新しい暗号化 MISTY 鍵情報を受け入れる。
FMT_MTD.1 FMT_SMF.1 FMT_SMR.1	SF.MANAGE …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。…

TOE 機能要件	該当する各セキュリティ機能の記述
FPT_RVM.1	SF.CRYPT TOE は、RFID に申込情報を記録する前、及び受付情報を転送する前にこれらの情報を 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)で暗号化する。… SF.MANAGE …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。…

8.3.2. 機能強度の根拠

本 TOE において、確率的あるいは順列的メカニズムを持つセキュリティ機能は SF.MANAGE だけである。この SF.MANAGE のセキュリティ機能強度は 6.2 章において「SOF-基本」と宣言されている。一方、本 TOE の最小機能強度は 5.1.3 章において「SOF-基本」と宣言されている。これらが矛盾していないことは明らかである。

8.3.3. セキュリティ機能のコンビネーション

セキュリティ機能要件の依存性については、8.2.3 章で述べたとおり問題はない。また、8.2.4 章で、選択された機能要件は内部的に一貫し、相互に補完し合っていることを述べた。さらに、1 つの TOE 機能要件が複数のセキュリティ機能に対応している場合もあるが、2 つのセキュリティ機能は互いに独立しており、セキュリティ機能の組み合わせによってセキュリティ機能要件を満たすものはない。つまり、TOE 機能要件を満たすためにセキュリティ機能が一体となって機能しているといえる。

8.3.4. 保証手段の根拠

Table 6-1 に示したように、全ての TOE セキュリティ保証要件は、保証手段により示された文書により対応付けられており、また保証手段に示された文書名によって、本 ST が規定した EAL2 が要求している証拠に合致していることは明白である。なお、文書名中に記述されている「申込書類回収業務提携先」は、本書での配送者のことを表している。

8.4. PP 主張根拠

本 ST で参照される PP はない。

9. 改定履歴

バージョン	発行日	内容	備考
1.1 版	2004 年 10 月 12 日	初版作成	申請用
1.2 版	2004 年 11 月 9 日	誤字脱字修正 指摘により文章追加・修正	—
1.3 版	2004 年 12 月 15 日	前提条件修正 指摘により文章追加・修正 誤字脱字修正	—
1.4 版	2005 年 1 月 13 日	保証手段修正 文章修正・追加	—
1.5 版	2005 年 1 月 19 日	文章修正	—
1.6 版	2005 年 1 月 26 日	前提条件修正 文章修正・追加	—
1.7 版	2005 年 2 月 8 日	指摘により文章追加・修正	—
2.0 版	2005 年 2 月 21 日	保証手段修正	—

— 以下 余白 —