SafetyDomain
セキュリティターゲット

2008 年 10 月 16 日

富士通株式会社

FUJITSU

- 更新履歴 -

日付	Version	更新箇所	更新内容	作成者
2008/1/15	1.0	新規作成	―	富士通株式会社
2008/2/13	1.1	1,3,4,6,7 章	記述の見直し	富士通株式会社
2008/3/5	1.2	1,3,4,6,7 章	記述の見直し	富士通株式会社
2008/3/31	1.3	1,3,4,5,7 章	記述の見直し	富士通株式会社
2008/4/14	1.4	1,3,4,6,7 章	記述の見直し	富士通株式会社
2008/4/16	1.5	1,3,4,6,7 章	記述の見直し	富士通株式会社
2008/4/22	1.6	1,3,4,6,7 章	記述の見直し	富士通株式会社
2008/5/9	1.7	1,3,4,6,7 章	記述の見直し	富士通株式会社
2008/5/19	1.8	1,6 章	記述の見直し	富士通株式会社
2008/8/18	1.9	1,3,4,6,7 章	記述の見直し	富士通株式会社
2008/9/4	1.10	1,3,4,6,7 章	記述の見直し	富士通株式会社
2008/9/8	1.11	2,7 章	記述の見直し	富士通株式会社
2008/9/11	1.12	1 章	記述の見直し	富士通株式会社
2008/9/17	1.13	3,4 章	記述の見直し	富士通株式会社
2008/9/18	1.14	3 章	記述の見直し	富士通株式会社
2008/9/24	1.15	1 章	記述の見直し	富士通株式会社
2008/9/25	1.16	1 章	記述の見直し	富士通株式会社
2008/9/30	1.17	1,4 章	記述の見直し	富士通株式会社
2008/10/16	1.18	1,3,4,7 章	記述の見直し	富士通株式会社

～ 目次 ～

～ 図目次 ～

～ 表目次 ～

1. ST概説

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

1.1 ST参照

本節では、本 ST の識別情報を記述する。

名称：SafetyDomain セキュリティターゲット

バージョン：第 1.18 版

作成日：2008 年 10 月 16 日

作成者：富士通株式会社

1.2 TOE参照

本節では、本 ST が参照する TOE の識別情報を記述する。

名称：SafetyDomain

バージョン：V04L01

作成者：富士通株式会社

1.3 TOE概要

本節では、TOE の種別、TOE の主要なセキュリティ機能、及び、TOE の利用目的について記述する。

1.3.1 TOE種別及び主要セキュリティ機能

TOE は、従来、Windows PC にログオンする際に手で行われていた ID 及びパスワードの入力を、IC カードを基にした入力に変更する機能を提供するソフトウェア製品である。

TOE が提供するセキュリティ機能の概要を以下に示す

認証に関わるセキュリティ機能

・Windows ログオン機能

PIN を IC カードに受け渡し、TOE または IC カード（※）にて PIN が正当であると判断された後、IC カード内に格納された ID、パスワード、ドメイン情報を読み取り、当該ドメインにおける Windows へのログオンの可否の判定を Windows が提供する識別認証の機能に依頼する機能である。なお、本機能により、Windows が提供する識別認証のインタフェースは隠蔽され、IC カードによる識別認証のインタフェースが表示される。そのため、IC カードを利用してのみ、Windows へのログオンが可能となる。

なお、Windows へログオンする際の ID 及びパスワードを基にした識別認証処理自体は、Windows が行う。

※FeliCa カードは PIN の認証を TOE が行う。Java カードは、PIN の認証処理を、IC カードである Java カードが行う

・アプリケーション認証機能

PIN を IC カードに受け渡し、TOE または IC カード（※）にて PIN が正当であると判断された後、IC カード内に格納された ID、パスワードを読み取り、アプリケーションへのログオンの可否の判定をアプリケーションへ依頼する機能である。なお、本機能により、アプリケーションが提供する識別認証のインタフェースは隠蔽され、IC カードによる識別認証のインタフェースが表示される。そのため、IC カードを利用してのみ、アプリケーションへのログオンが可能となる。

但し、認証の依頼対象のアプリケーションは、クライアント端末に導入されているもののみである。

なお、アプリケーションへログオンする際の ID 及びパスワードを基にした識別認証処理自体は、アプリケーションが行う。

※FeliCa カードは PIN の認証を TOE が行う。Java カードは、PIN の認証処理を、IC カードである Java カードが行う

IC カード内の情報を管理する機能

・IC カード管理機能（管理者向け）

IC カードに定義される情報の設定を管理者のみに制限する機能である。概要は以下の通り。

- アカウント管理

全ての利用者の、アカウントに関する情報の設定を制限する機能である。

- PIN コード管理

全ての利用者の、PIN に関する情報の設定を制限する機能である。

・IC カード管理機能（利用者向け）

IC カードに定義される情報の設定を、利用者本人にのみに制限する機能である。概要は以下の通り。

- PIN 変更

当該利用者の IC カードの PIN コードの変更を制限する機能である。

- パスワード変更

当該利用者の IC カードのパスワードの変更を制限する機能である。

1.3.2 TOEの利用環境

1.3.2.1 TOEの運用環境

図 1-1に、TOEの運用環境を示す。図に示すとおり、TOEの運用環境は、ドメインによる運用を想定している。

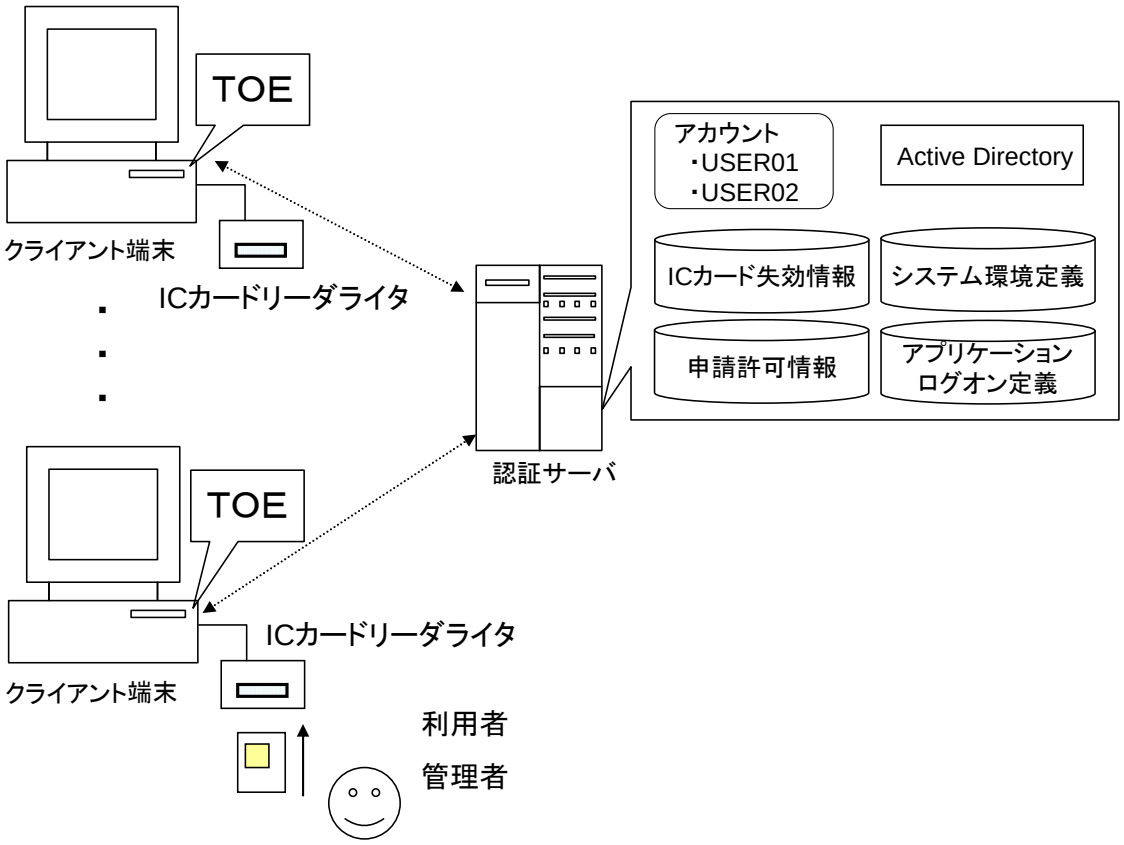


図 1-1 TOE の運用環境（ドメインによる運用）

[図の説明]

TOE は、クライアント端末に導入されて動作する。TOE の利用のためには、IC カード（※）を事前に配付しておく必要がある。

また、IC カードの読み取り、書き込みとして IC カードリーダライタが必要である。

※IC カードには、利用者用の IC カードと、管理者用の IC カードがある。利用者用の IC カードと管理者用の IC カードは、IC カード内の情報が違うのみであり、媒体自体は同じである。

また、ドメイン内の Windows にログオンする際の利用者アカウントは、認証サーバにて一元管理する環境を想定する。

また、認証サーバ上には、以下の定義ファイルを配置する運用を想定する。

・システム環境定義
・アプリケーションログオン定義
・IC カード失効情報
・申請許可情報

なお、システム環境定義の送受信のプロトコルには、SMB が利用される。

上記の通り、TOE はクライアント端末に導入されて動作するため、TOE の制御範囲は、クライアント端末上に限定され、クライアント端末と認証サーバとの通信等の制御は、TOE が動作する Windows が担う。

1.3.2.2 TOEの動作に必要なハードウェア資源

TOE の動作に必要なハードウェア資源を、表 2-1 に示す。

表 1-1 TOE の動作に必要なハードウェア資源

項目	要件(WindowsXP 系)	要件(Windows Vista 系)
クライアントスペック	CPU：PentiumⅢ　700MHz 以上 メモリ：256MB 以上 ディスク：20GB 以上 SafetyDomain インストール容量：160MB	CPU：PentiumⅢ 1GHz 以上 メモリ：1GB 以上 ディスク：40GB 以上 SafetyDomain インストール容量：160MB
対応カード種別	SHARP Java カード(ISO14443 TypeB 準拠) FeliCa カード	
IC カードリーダライタ	富士通スマートアクセス PC 内蔵リーダ（接触、FMV デスクトップ内蔵） PC 内蔵リーダ（接触、PCMCIA　ノート PC 型） ソニー　PaSoRi(FeliCa カード)	

※FeliCa カードには、PaSoRi が対応する。SHARP Java カードには、スマートアクセス、PC 内蔵リーダ（接触、FMV デスクトップ内蔵）、PC 内蔵リーダ（接触、PCMCIA ノート PC 型）が対応する。

以降、FeliCa カードを、「FeliCa」と称して説明する。

また、上記の他に、認証情報を一元管理するための、「認証サーバ」を必要とする。

1.3.2.3 TOEの動作に必要なソフトウェア資源

●クライアント端末に導入するソフトウェア

TOEの動作に必要な、クライアント端末に導入するソフトウェア資源を、表 1-2に示す。

表 1-2 TOE の動作に必要なソフトウェア資源

項目	要件	備考
OS	Microsoft® Windows® XP Professional(32bit)	SP2
	Microsoft® Windows® Vista Enterprise(32bit)	SP1
リーダライタドライバ	リーダライタ用ドライバ	

●TOE が対応するアプリケーション

TOE が対応するアプリケーションは、以下の認証を行うアプリケーションである。

・HTML フォーム認証

・BASIC 認証

・Java アプレット認証

以降、本 ST では、TOE が対応するアプリケーションのみを、「アプリケーション」と称する。

●サーバに導入するソフトウェア

TOEの運用環境に必要な、認証サーバに導入するソフトウェアを、表 1-3に示す。

表 1-3 認証サーバに導入するソフトウェア

項目	要件	SP
ソフトウェア	Microsoft® Windows® Server 2003	SP2
	Active Directory	

1.4 TOE記述

1.4.1 TOEの関係者

表 1-4にて、TOEの関係者について説明する。

表 1-4 TOE の関係者

TOE の関係者	役割
組織の責任者	組織の長であり、管理者の任命を行う。TOE は利用しない。
管理者	クライアント端末を使用して、TOE の管理行為を行う。 管理者用の IC カードを有する必要がある。 本役割のみが使用可能な TOE の機能は以下である。 ・環境設定ファイルの編集機能 ・システムメンテナンス機能 ・一時ログオン設定機能 ・IC カード管理機能（管理者向け） 上記の他、利用者が使用する機能も使用可能である。 なお、管理者の IC カードには、「特定管理者」、「管理者」の区分があり、「管理者」に関しては、システム環境定義、申請許可情報、IC カード失効情報の設定をできない仕様とする。
利用者	利用者用の IC カードを有する人物である。 クライアント端末を使用して、Windows 及びアプリケーションが提供するサービスを利用する。 本役割が使用可能な TOE の機能は以下である。 ・ファイル暗号化機能 ・パスワード自動生成機能 ・ネットワーク接続監視機能 ・認証履歴採取機能 ・Windows ログオン機能 ・アプリケーション認証機能 ・IC カード管理機能(利用者向け) なお、利用者の IC カードには「所属」と「個人」の区分があり、「所属」に関しては、IC カードのパスワードを変更できない仕様とする。

※上記の役割の他、関係者としてシステムメンテナンスの役割がある。システムメンテナンスの作業は、システムメンテナンス機能を使用して TOE のバージョンアップを行うことであるが、TOE のバージョンアップを行うことは TOE の識別情報が変更されることとなるため、本 ST では実施しない前提とする。そのため、本 ST では、システムメンテナ

ンスは関係者として扱わず、かつ、そのために、管理者は、アカウントとしてシステムメンテナンスを作成しない運用を行うこととする。

1.4.2 TOEの物理的構成

図 1-2に、クライアントにおけるTOE及び動作に必要なソフトウェアの配置イメージを示す。図において、網掛けで示したものが、TOEの物理的構成要素である。

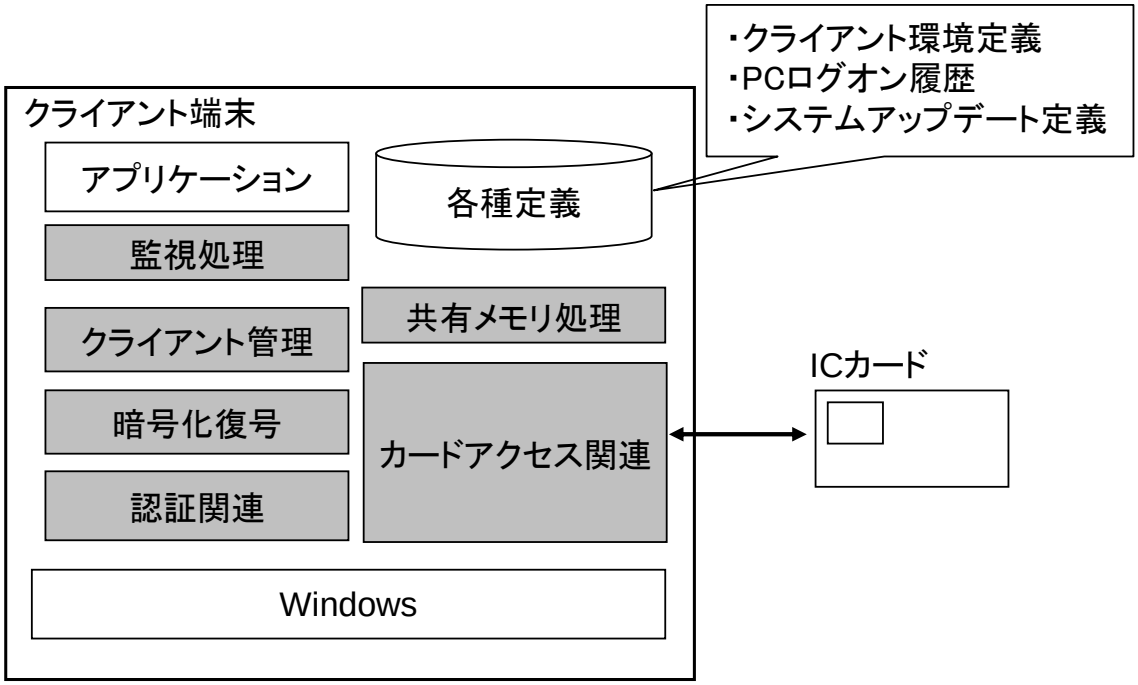


図 1-2 TOE の物理的構成要素

[図の説明]

表に、図に示した各モジュールの概要と、関係する TOE の機能を説明する。

表 1-5 SafetyDomainV04L01 で提供されるモジュール

モジュール名	概要
監視処理モジュール	カードの抜き取り監視や、ネットワーク上の PC との接続可否等の監視を行うモジュール。 [関係する TOE の機能] ・ネットワーク接続監視機能 ・Windows ログオン機能
共有メモリ処理モジュール	TOE 内で共有するデータの処理を行うモジュール。 [関係する TOE の機能] TOE のすべての機能
クライアント管理	主に、管理者の設定に関する機能を提供するモジュール。

モジュール	[関係する TOE の機能] ・環境設定ファイルの編集機能 ・一時ログオン設定機能 ・IC カード管理機能(管理者向け) ・IC カード管理機能(利用者向け) ・システムメンテナンス機能
認証関連モジュール	認証関連の機能を司るモジュール。 [関係する TOE の機能] ・Windows ログオン機能 ・アプリケーション認証機能 ・認証履歴採取機能
カードアクセス関連モジュール	カードアクセス全般を司るモジュール。 [関係する TOE の機能] ・Windows ログオン機能 ・アプリケーション認証機能 ・IC カード管理機能(管理者向け) ・IC カード管理機能(利用者向け)
暗号化復号モジュール	ファイルの暗号化/復号を行うモジュール。 [関係する TOE の機能] ・ファイル暗号化機能

TOE 外の要素について以下に示す。

・Windows

TOE を動作させる OS。特に、Windows 内の認証を司るモジュールの一部が、本 TOE(認証関連モジュール)に置き換わることで、Windows ログオン機能を実現する。

・アプリケーション

Windows 上で動作するアプリケーション。TOE が提供するアプリケーション認証機能にて、アプリケーションが有しているログオン画面が隠蔽される。

添付されるガイダンス文書

・PC ログオンシステム SafetyDomain V04L01 操作マニュアル 第 1.10 版

・PC ログオンシステム SafetyDomain V04L01 管理者マニュアル【導入・設定編】第 1.6 版

・PC ログオンシステム SafetyDomain V04L01 管理者マニュアル【運用編】 第 1.8 版

1.4.3 TOEの論理的構成

本節では、TOE が提供する機能について説明する。

表 1-6 TOE の機能一覧

機能タイプ	機能のカテゴリ	機能名称
一般機能	TOE の一般機能	ファイル暗号化機能
		パスワード自動生成機能
		認証履歴採取機能
		ネットワーク接続監視機能
		シングルサインオン機能
		環境設定ファイルの編集機能
		システムメンテナンス機能
		一時ログオン設定機能
セキュリティ機能	認証機能	Windows ログオン機能
		アプリケーション認証機能
	IC カード管理機能	IC カード管理機能(管理者向け)
		IC カード管理機能(利用者向け)

TOE が提供する一般機能は、以下である。

1.4.3.1 TOEの一般機能

1.4.3.1.1 ファイル暗号化機能

カード内に設定されている電子鍵を利用して、ファイル・フォルダの暗号化を行う機能である。なお、本機能は、TOE の製品ポリシーから鑑みて主となるものではないため、一般機能の位置づけとする。

1.4.3.1.2 パスワード自動生成機能

Windows に予めアカウントが存在し、かつ、IC カード内にパスワードが設定されていない場合、パスワードを自動的にランダムな英数字記号で生成し、Windows 及び IC カード内に設定する機能である

但し、本機能は、環境定義ファイル群において、「パスワードの自動設定情報」が自動の場合のみ実行される。

1.4.3.1.3 ネットワーク接続監視機能

クライアント端末にログオンした以降もネットワークの接続監視を行い、クライアント端末がネットワークに接続されたときにICカード失効情報ファイルを参照し、失効カードにてログオンしていた場合、Windowsのログオフを行う機能である。

1.4.3.1.4 認証履歴採取機能

認証や操作時のログを採取する機能である。各クライアント端末のログをログオン管理に関するサーバに集中管理することができる。但し、本STにおける想定環境は、ログオン管理に関するサーバを設置しないため、本機能は使用されない。

1.4.3.1.5 シングルサインオン機能

本機能は、Windowsにログオン後、再度PIN入力が必要な場面でPIN入力を自動で行い、アプリケーション認証、システムメンテナンス機能、IC カード管理機能(利用者向け)のパスワード変更時における、手動による PIN 入力を不要とさせる機能である。環境設定ファイル群の中の、「シングルサインオン」が有効の場合適用される。

※PINの入力が必須ではない理由

アプリケーション認証、システムメンテナンス機能、IC カード管理機能(利用者向け)のパスワード変更は、当然のことながら、Windowsへのログオン後に行われる。WindowsにPINを入力してログオンしている時点で、当該ログオン中においては、ICカードからIDとパスワードを読み出すことを許可しているとみなすことができるため、これらの機能の利用の際に、毎回PINを手入力してICカードからID及びパスワードを読み出すことは、必須ではない。

1.4.3.1.6 環境設定ファイルの編集機能

本機能は、TOE の設定情報である環境設定ファイルを編集/閲覧する機能を提供する。本機能により編集/閲覧対象となる環境設定ファイルは以下である。

[クライアント上の環境定義]

・クライアント環境定義
・システムアップデート定義
・PC ログオン履歴

[認証サーバ上の定義]

・システム環境定義
・申請許可情報
・IC カード失効情報
・アプリケーションログオン定義情報

なお、これら環境設定ファイルは、管理者以外が閲覧/編集できないように、クライアント及び認証サーバの Windows のアクセス権の設定を行う必要がある。

以降、これらの環境設定ファイルを「環境設定ファイル群」と称する。

なお、環境設定ファイル群の中で、特に、TOE のセキュリティ機能の動作に関係する情報を以下に示す。

・シングルサインオンの設定情報
・離席対応情報
・アプリケーションログオン情報

1.4.3.1.7 システムメンテナンス機能

システムの機能的なバージョンアップを行う機能である。但し、本機能を使用した場合、TOE のバージョンの変更、すなわち、TOE 識別が変更されるため、本 ST では使用しない前提する。

1.4.3.1.8 一時ログオン設定機能

本機能により利用者は、管理者から指定された操作を行い、Windows が提供する識別認証を経てログオンが可能となる。

本機能は、IC カードの所持を忘れた利用者に対応する機能である。本機能は管理者のみ利用可能であるが、利用の制限機能は Windows によって提供される。

TOE が提供するセキュリティ機能は以下である。

1.4.3.2 認証

1.4.3.2.1 Windowsログオン機能

本機能は、PIN を IC カードに受け渡し、TOE/IC カード(注 1)にて PIN が正当であると判断された後、IC カード内に格納された ID、パスワード(注 2)、ドメイン情報を読み取り、Windows が提供する識別認証の機能へ識別認証の依頼を行う機能である。なお、本機能により、Windows が提供する識別認証のインタフェースは隠蔽され、IC カードによる識別認証のインタフェースのみが表示される。そのため、IC カードを利用してのみ、Windows へのログオンが可能となる。

【実行されるタイミング】

本機能が実行されるタイミングは以下である。

- Windows の起動
- スクリーンセーバ時のロック
- IC カードの引き抜き時のロック/シャットダウン/ログオフ (注 3)
- IC カードリーダライタの引き抜き時のロック/シャットダウン/ログオフ (注 3)

(注 1)FeliCa は、TOE にて PIN の認証を行う。Java カードは、IC カードである Java カードにて PIN の認証が行われる。

(注 2) IC カード内の情報である「次回ログオン時のパスワードの手入力有無」で、パスワードの手入力が「有効」の場合、ID は IC カードから読み出されるが、パスワードは手入力が必要となる。

(注 3)環境設定ファイル群において、以下の環境設定が行われている場合に実行される。

- IC カードの引き抜きを契機に、ロック/シャットダウン/ログオフ
- IC カードリーダライタの引き抜きを契機に、ロック/シャットダウン/ログオフ

以降、上記に示した環境設定の対象情報を「離席対応情報」と称する。

なお、スクリーンセーバロックは Windows が行い、IC カード引抜時のロック、リーダライタ引抜時のロックは TOE が行う。

1.4.3.2.2 アプリケーション認証機能

本機能は、PIN を IC カードに受け渡し、TOE/IC カード(注 1)にて PIN(注 2)が正当であると判断された後、IC カード内に格納された ID、パスワードを読み取り、アプリケーションが提供する識別認証の機能へ識別認証の依頼を行う機能である。本機能により、アプリケーションが提供する識別認証のインタフェースは隠蔽され、IC カードを利用した方法が可能となる。但し、認証の依頼対象のアプリケーションは、クライアント端末に導入されているもののみである。

なお、本機能に関しては、アプリケーションログオン定義の設定により、ID を IC カードから読み取り、パスワードを手入力とする動作にすることが可能であるが、本 ST が定める想定環境としては、ID 及びパスワードを IC カードから読み取る動作にするよう設定することとする。

(注 1)FeliCa は、TOE にて PIN の認証を行う。Java カードは、IC カードである Java カードにて PIN の認証が行われる。
(注 2) シングルサインオンが有効の場合は、PIN の手入力は不要

1.4.3.3 ICカード管理

1.4.3.3.1 ICカード管理機能(管理者向け)

IC カード内の情報の設定を、管理者のみに制限する機能である。なお、FeliCa における、情報の設定機能部を特に、「IC カード情報設定機能(管理者向け)」と称する。

以下、設定情報毎に詳細を示す。

(1)アカウント管理

全ての利用者の、アカウントに関する以下の情報への設定を、管理者のみに制限する機能である。

・ユーザ名

TOE にて利用され、また、Windows にログオンする際に利用される ID。

・パスワード

TOE を利用する際のパスワード。下記情報、「次回ログオン時のパスワードの手入力有無」が有効に設定されていた場合に、Windows にログオンする際入力する。

・次回ログオン時のパスワードの手入力有無

次回ログオン時のパスワードの手入力の有無を設定する。パスワードの入力が有効の場合、上記のパスワードで設定したパスワードを入力し、パスワード入力が無効の場合、パスワード入力は不要となる。

・対象アプリ

対象とするアプリケーションを指定する。Windows OS が対象となる場合は、「Windows ログオン」と指定し、アプリケーションの場合はアプリケーションログオン情報に設定されている名前を指定する。

・ログオン先

ログオン先のドメイン情報を指定する。

・アカウント区分

利用者、管理者、またはシステムメンテナンスかのアカウント区分を指定する。但し、利用者の IC カードに「管理者」区分を指定することはできない。

(2) PINコード管理

全ての利用者の、IC カード内の PIN 情報の書き換えを、管理者のみに制限する機能である。設定可能な PIN 情報は以下の通り。

・PIN コードロック回数設定

PIN コードの入力を間違えた際にロックする場合のリトライ回数である。リトライ回数を超えると、IC カードにより PIN コードロック状態となる。

・初期 PIN コード強制変更

本情報を指定することで、初回のカード利用の際に、新しい PIN コードの入力を要求し、強制的に初期 PIN コードを利用者に変更を要求する。

・PIN のロック解除

IC カードの PIN コードロック状態を解除する。

・PIN 初期化

IC カードに新しい PIN を設定する。この機能は、利用者が PIN を忘却した等の理由により、利用者カードの PIN を変更する必要がある場合に使用する。

また、上記の「アカウント管理」、「PIN コード管理」の区分以外の情報として、カード識別番号がある。カード識別番号は、利用者毎の IC カードを識別する際に利用される情報であり、FeliCa の場合のみ、本機能にて当該情報を設定することができる。

1.4.3.3.2 ICカード管理機能(利用者向け)

IC カード内の情報の設定を、利用者本人のみに制限する機能である。なお、FeliCa における、情報の設定機能部を特に、「IC カード情報設定機能(利用者向け)」と称する。

(1)PIN変更

当該利用者の、IC カードの PIN コードを変更する。

(2)パスワード変更

当該利用者の、IC カード内のパスワードを変更する。

1.4.4 TOEの利用方法

本節では、TOE の利用方法について記述する。

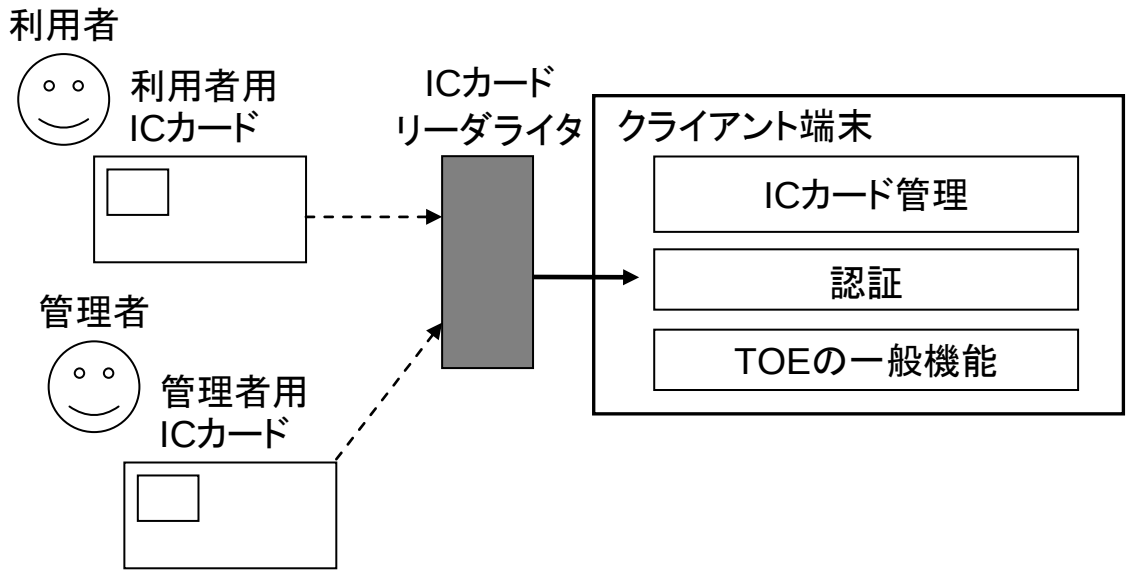


図 1-3 TOE の利用方法

[図の説明]

1.利用者の操作

利用者は、事前に配付された利用者用の IC カードを IC カードリーダライタに挿入し、PIN の入力を行う。

「Windows ログオン機能」により、FeliCa の場合は、入力された PIN の照合を TOE が行うが、Java カードの場合は、入力された PIN は IC カードである Java カードに送信され、IC カードによる PIN 照合が行われる。照合の結果、正当なものであることを確認された場合、IC カード内の ID とパスワードを TOE に読み込む。

また、「Windows ログオン機能」は、読み込んだ ID とパスワードを基に、Windows が提供する識別認証機能に正当なものであるかの判断依頼を行い、正当であると判断された場合、Windows へのログオンが許可される（この際、Windows 側では、バックグラウンドで認証サーバとのやり取りが行われている。）

Windows にログオンした後、アプリケーションを利用する場合、PIN を入力し、IC カードによる PIN 照合の結果、正当なものであることを確認された場合、「アプリケーション認証機能」により、IC カードより ID 及びパスワードを TOE に読み込む。読み込んだ ID 及びパスワードを基に、アプリケーションが提供する識別認証機能に正当なものであるかの判断依頼を行い、正当であると判断された場合、アプリケーションへの認証が許可される。

また、利用者は、必要に応じて、自身が所有する IC カードの PIN やパスワードを変更す

る。但し、変更の際には、旧 PIN または旧パスワード（※）を入力した後のみ可能である。
※「パスワードの自動設定情報」が自動の場合は旧パスワードの入力は不要。

なお、この際、「IC カード管理機能(利用者向け)」により、利用者本人のみ変更可能とする制限がなされている。

なお、シングルサインオンが有効の場合、アプリケーション認証機能、システムメンテナンス機能、IC カード管理機能(利用者向け)のパスワード変更時において、PIN 入力の必要な場面での PIN 入力は不要となる。

なお、離席対応情報の各種設定が行われていた場合、カード引抜時、Windows のスクリーンセーバ機能の動作時、リーダライタの取り外し時に TOE により、Windows に、クライアント端末のロックが行われるため、「Windows ログオン機能」を介して、Windows へのログオン処理を行う。

2.管理者の操作

[導入]

管理者は、TOE の動作に関わる環境設定を行い、設定情報が記載された環境設定ファイル群を、クライアント及び認証サーバに配置する。この際、管理者は、環境設定ファイル群に対し、管理者以外から変更できないように OS(Windows)のアクセス権の設定を行う。

また、以降、環境設定の必要がある際には、「環境設定ファイルの編集機能」を利用して、TOE の環境設定を行う。

[運用]

管理者は、事前に配付された管理者用の IC カードを IC カードリーダライタに挿入し、PIN の入力を行う。

「Windows ログオン機能」により、FeliCa の場合は、入力された PIN の照合を TOE が行うが、Java カードの場合は、入力された PIN は IC カードである Java カードに送信され、IC カードによる PIN 照合が行われる。照合の結果、正当なものであることを確認された場合、IC カード内の ID とパスワードを TOE に読み込む。

また、「Windows ログオン機能」は、読み込んだ ID とパスワードを基に、Windows が提供する識別認証機能に正当なものであるかの判断依頼を行い、正当であると判断された場合、Windows へのログオンが許可される（この際、Windows 側では、バックグラウンドで認証サーバとのやり取りが行われている。）

その後、管理者は、以降の TOE に対する管理行為を行う。

また、利用者に発行する IC カードに対し各種設定を行う。この際、「IC カード管理機能(管理者向け)」により、管理者のみ設定可能とする制限がなされる。

また、利用者からの PIN ロック状態の解除要求や、PIN の忘却に伴う PIN 変更要求等を受け付けると、管理者は利用者の IC カードを受け取り、PIN ロック状態の解除や、PIN の変更を行う。この際も同様に、「IC カード管理機能(管理者向け)」により、管理者のみ設定可

能とする制限がなされる。なお、変更の手順としては、設定変更の途中で、対象の IC カードのセットを促すメッセージが出るため、それに従って管理者の IC カードに代えて利用者の IC カードをセットする。

また、利用者から、IC カードの所持を忘れた旨の連絡を受けた場合、管理者は、「一時ログオン設定機能」を使用する。その後管理者は利用者に、初期化したパスワードと「一時ログオン設定機能」にて設定した特別なキー操作を利用者に伝える。利用者は指定されたキー操作を行った後、Windows が提供する識別認証にて、初期化されたパスワードを利用してログオンを行う。

1.5 用語、略語

本 ST で使用する用語、略語を定義する。

用語、略語	定義内容
PIN	Personal Identification Number: IC カード内に設定されている情報を読み出したり書き込んだりする際に必要なコード 本書中では、PIN コードと示す場合もある。
環境設定ファイル群	クライアント環境定義、システムアップデート定義、PC ログオン履歴、システム環境定義、申請許可情報、IC カード失効情報、アプリケーションログオン定義情報の総称
カード ID	IC カードを識別するための識別子。IC カードそれぞれに付与されており、本情報の編集は不可能である。
カード識別番号	利用者毎の IC カードを識別する際に利用される識別子。なお、利用者が複数の IC カードを所有する場合、各 IC カードに同じカード識別番号を付与することができる（カード識別番号の例：従業員番号 等） 本識別子は、FeliCa のみ IC カード管理機能(管理者向け)にて設定ができる。
クライアント環境定義	クライアント端末毎の、TOE の動作定義情報
システムアップデート定義	TOE のアップデート情報
PC ログオン履歴	各クライアント端末へのログオンの履歴情報
システム環境定義	各クライアント端末に、共通に適用される TOE の動作定義情報
申請許可情報	IC カード内のアカウントに関する情報を、GUI により個別に設定するのではなく、一括で変更する際に利用する定義情報
IC カード失効情報	失効された IC カードの情報が登録される定義情報
アプリケーションログオン定義情報	アプリケーション認証機能にて対象とするアプリケーションに関する定義情報

2. 適合主張

本章では、CC 適合主張、PP 主張、パッケージ主張、及び適合根拠について記述する。

2.1 CC適合主張

本 ST、及び、TOE が適合を主張する CC は以下である。

パート 1:概説と一般モデル 2006 年 9 月 バージョン 3.1 翻訳第 1.2 版
パート 2:セキュリティ機能コンポーネント 2007 年 9 月 バージョン 3.1 翻訳第 2.0 版
パート 3:セキュリティ保証コンポーネント 2007 年 9 月 バージョン 3.1 翻訳第 2.0 版

CC パート 2 に対する ST の適合：CC パート 2 拡張
CC パート 3 に対する ST の適合：CC パート 3 適合

2.2 PP主張、パッケージ主張

2.2.1 PP主張

本 ST が適合する PP は存在しない。

2.2.2 パッケージ主張

EAL2 適合

2.3 適合根拠

2.3.1 適合主張根拠

本 ST は、PP への適合を主張しない。

3. セキュリティ課題定義

本章では、TOE 資産、脅威、組織のセキュリティ方針、及び、前提条件について記述する。

3.1 TOE資産

従来の Windows の識別認証は ID やパスワードを手入力していたため、ID やパスワードの管理が煩雑となり、結果として悪意のあるものに ID やパスワードを入手され、Windows が提供するサービスを利用されるということがあった。

本 TOE では、ID やパスワードを IC カードに格納し Windows へのログオンに利用することで、ID やパスワードの管理の煩雑性を解消している。

また、本 TOE では、同様にアプリケーションが実施する識別認証に関しても、同様な問題を解消している。

そのため、本 TOE が保護する資産は以下となる。

・ID やパスワードの管理の不十分性から脅威にさらされる、Windows 及びアプリケーションが提供するサービス

3.2 脅威

攻撃者（悪意のあるもの）は、高度な専門知識を持たないものを想定する。

T.SPOOFING(なりすまし)

Windows やアプリケーションに入力される ID やパスワードの管理が不十分であるために、悪意のあるものに ID やパスワードが入手される。その結果として、Windows やアプリケーションが提供するサービスが不正に利用される。

3.3 組織のセキュリティ方針

組織のセキュリティ方針はない。

3.4 前提条件

A.IC_TAMP_RESIST(IC カードの耐タンパー性)

IC カードは、物理的な耐タンパー性があることを想定する。

A.ADMIN(管理者の信頼性)

管理者は、TOE に対し不正を行わない信頼できる人物であることを想定する。

A.OS_ACC_SETUP(OS のアクセス権設定)

環境設定ファイル群に対し、OS 経由での不正アクセスが無いよう、管理者以外のアクセスが制限されていることを想定する。

A.PIN_AUTH(PIN による認証)

IC カード(Java カード)を使用する人物が、正当な人物であるかを確認するために、PIN による認証が行われる IC カード(Java カード)を利用することを想定する。

A.PIN_FIG(PIN の桁数)

TOE に利用する IC カードの PIN の桁数を、8 桁以上に設定することを想定する。

A.APP_CONDITION(アプリケーション条件)

アプリケーションは、TOE の制御対象であるアプリケーションの識別認証を介してのみ、サービスにアクセスできるものであることを想定する。

A.IC_CONDITION(管理機能を有する IC カード)

TOE の指示により、IC カード(Java カード)自身の情報を変更する機能を有する IC カード(Java カード)が使用されることを想定する。

A.MAINTENANCE(システムメンテナンス機能の利用制限)

本 ST が定める運用条件として、システムメンテナンス機能を使用しないことを想定する。

A.APP_AUTH_CONDITION (アプリケーション認証機能の使用条件)

本 ST 定める運用条件として、アプリケーション認証機能が、IC カードから ID 及びパスワードを読み取る動作に設定されることを想定する。

A.AWAY_FROM_COMPUTER(サービス利用時の離席)

TOE の保護資産を利用時に離席する際には、保護資産を利用できない状態にした後で離席することを想定する。

A.ONE_TIME(一時ログオン設定機能の使用)

一時ログオン設定機能により一時的に使用可能となった Windows が提供する識別認証は、不要となった際には無効にされることを想定する。

4. セキュリティ対策方針

本章では、TOE のセキュリティ対策方針、運用環境のセキュリティ対策方針、及び、セキュリティ対策方針根拠について記述する。

4.1 TOEのセキュリティ対策方針

TOE のセキュリティ対策方針は以下である。

O.IC_I&A(IC カードによる処理)

TOE は、Windows やアプリケーションに対し、ID 及びパスワードを手入力できないようにした上で、IC カードにより入力するよう変更する。

また、IC カードの不正取得に伴う不正行為を考慮して、IC カードからの ID 及びパスワードの読み出しは、IC カードによる PIN 認証の後に可能とさせる（※)。

但し、IC カードの所持を忘れた利用者への対応として、従来の Windows が提供する識別認証を利用者に特別に利用許可させる機能を、管理者にのみ提供するものとする。

また、IC カードが非アクティブ状態となった際には、認証状態を解除する。

(※)アプリケーションが提供するサービスの利用に関して

アプリケーションの認証（延いては、アプリケーションのサービス利用）は、当然のことながら、Windows へのログオン後に行われる。Windows に PIN を入力してログオンしている時点で、当該ログオン中においては、IC カードから ID とパスワードを読み出すことを許可しているとみなすことができるため、アプリケーションの認証の際に、毎回 PIN を手入力して IC カードから ID 及びパスワードを読み出すことは、必須ではない。

4.2 運用環境のセキュリティ対策方針

運用環境のセキュリティ対策方針は以下である。

OE.IC_TAMP_RESIST(IC カードの耐タンパー性)

組織の責任者は、TOE に利用する IC カードとして、物理的な耐タンパー性があるものを採用する。

OE.ADMIN(管理者の選任)

組織の責任者は、管理者として信頼できる人物を選任し、不正を行わないよう教育し、遵守させなければならない。

OE.OS_ACC_SETUP(OS のアクセス権設定)

管理者は、環境設定ファイル群に対し、管理者以外がアクセスできないように、OS のアクセス権設定を行わなければならない。

OE.PIN_AUTH(PIN による認証)

管理者は、TOE に利用する IC カードとして、PIN による認証が行われるものを採用し、利用しなければならない

OE.PIN_FIG(PIN の桁数)

管理者は、TOE に利用する自身の IC カードの PIN の桁数を、8 桁以上に設定しなければならない。また、管理者は利用者に対し、TOE に利用する利用者本人の IC カードの PIN の桁数を、8 桁以上に設定するよう教育を行わなければならない。

OE.APP_CONDITION(アプリケーション条件)

管理者は、TOE が対応するアプリケーションとして、TOE によって迂回防止される識別認証を介してのみ、サービスにアクセスできるものを導入しなければならない。

OE.IC_CONDITION(管理機能を有する IC カード)

管理者は、TOE の指示により、自身の情報を変更する機能を有する IC カードを使用しなければならない。

OE.MAINTENANCE(システムメンテナンス機能の利用制限)

管理者は、本 ST が定める TOE の運用として、システムメンテナンス機能を使用しない運用としなければならない。また、管理者は、システムメンテナンスのアカウントを作成しない運用としなければならない。

OE.APP_AUTH_CONDITION (アプリケーション認証機能の使用条件)

管理者は、本 ST 定める運用条件として、アプリケーション認証機能を、IC カードから ID 及びパスワードを読み取る動作とするよう、アプリケーションログオン定義の設定を行わなければならない。

OE.AWAY_FROM_COMPUTER(サービス利用時の離席)

利用者および管理者は、TOE の保護資産の利用時に離席する際には、認証状態が切れたことを確認した後で離席しなければならない。認証状態を切る方法としては、Windows のログオフ、ロック状態（スクリーンセーバ時のロック、IC カードを引き抜き時のロック、IC カードリーダライタを引き抜き時のロック）とすること、がある。

OE.ONE_TIME(一時ログオン設定機能の使用)

管理者は、一時ログオン設定機能により一時的に使用可能となった Windows が提供する識別認証を、不要となった際に無効に設定すること。

4.3 セキュリティ対策方針根拠

セキュリティ課題定義のうち、脅威に対する対策方針を、表 4-1に示す。

表 4-1 脅威とセキュリティ対策方針の対応

脅威 / セキュリティ対策方針	T.SPOOFING
O.IC_I&A	○

以下に、『表 4-1 脅威とセキュリティ対策方針の対応』の根拠を示す。

T.SPOOFING

T.SPOOFING は、Windows やアプリケーションに入力される ID やパスワードの管理が不十分であるために、悪意のあるものに ID やパスワードが入手され、結果として、Windows やアプリケーションが提供するサービスが不正に利用される脅威である。

本脅威に対抗するためには、利用者が Windows やアプリケーションのサービスを利用する際に、ID やパスワードを記憶しておくような煩雑な管理を必要とさせない対策で実現できる。また、利用者が故意に ID やパスワードを手入力する運用を続けた結果、ID 及びパスワードが悪意のあるものに取得されることが無いように、ID 及びパスワードを手入力できないようにする対策も併せて必要である。

また、離席時の悪用についても、対策が必要である。

本 TOE では、**O.IC_I&A** により、Windows やアプリケーションへ ID 及びパスワードを手入力できなくした上で、IC カードにより入力するように変更する。そのため、ID やパスワードの煩雑な管理は必要無くなり、かつ、意図して ID 及びパスワードを手入力することはできなくなる。

また、IC カードの利用のみがサービスの利用条件の場合、IC カードを不正取得したものにサービスを利用されることになるため、**O.IC_I&A** では、IC カードからの ID 及びパスワードの読み出しは、IC カードによる PIN 認証の後に可能とさせることを併せて規定している。

また、利用者が IC カードの所持を忘れた場合の特例措置として、従来の Windows の識別認証を利用者に利用許可させる機能を提供する。但し、この機能を利用者が使用できた場合、**O.IC_I&A** が使用されなくなる可能性が出るため、この機能の利用は、管理者のみに制限する。

また、離席時にサービスを不正に利用されることを考慮して、IC カードが非アクティブ状態となった際には、当該認証状態を解除する。

従って、セキュリティ対策方針、**O.IC_I&A** が満たされることにより、本脅威に対抗することができる。

セキュリティ課題定義のうち、前提条件に対する対策方針を、表 4-2に示す。

表 4-2 前提条件とセキュリティ対策方針の対応

前提条件 / セキュリティ対策方針	A. IC_TAMP_RESIST	A. ADMIN	A. OS_ACC_SETUP	A. PIN_AUTH	A. APP_CONDITION	A. IC_CONDITION	A. MAINTENANCE	A. APP_AUTH_CONDITION	A. AWAY_FROM_COMPUTER	A. ONE_TIME
OE. IC_TAMP_RESIST	○									
OE. ADMIN		○								
OE. OS_ACC_SETUP			○							
OE. PIN_AUTH				○						
OE. APP_CONDITION					○					
OE. IC_CONDITION						○				
OE. MAINTENANCE							○			
OE. APP_AUTH_CONDITION								○		
OE. AWAY_FROM_COMPUTER									○	
OE. ONE_TIME										○

以下に、『表 4-2 前提条件とセキュリティ対策方針の対応』の根拠を示す。

A. IC_TAMP_RESIST

A. IC_TAMP_RESIST は、IC カードが物理的な耐タンパー性があることを想定した前提条件である。

本前提条件は、物理的な耐タンパー性を有した IC カードを利用することで実現できる。

OE. IC_TAMP_RESIST では、組織の責任者が、TOE に利用する IC カードとして、物理的な耐タンパー性があるものを採用することを規定している。

従って、セキュリティ対策方針、**OE. IC_TAMP_RESIST** が満たされることにより、本前提条件を実現することができる。

A.ADMIN

A.ADMIN は、管理者が TOE に対し不正を行わない信頼できる人物であることを想定した前提条件である。

本前提条件は、組織の責任者が、管理者として信頼できる人物を選任し、不正を行わないよう教育し、遵守させることで実現できる。

OE.ADMIN では、組織の責任者は、管理者として信頼できる人物を選任し、不正を行わないよう教育し、遵守させることを規定している。

従って、セキュリティ対策方針、OE.ADMIN が満たされることにより、本前提条件を実現することができる。

A.OS_ACC_SETUP

A.OS_ACC_SETUP は、環境設定ファイル群に対し、OS 経由での不正アクセスが無いよう、管理者以外のアクセスが制限されていることを想定した前提条件である。

本前提条件は、環境設定ファイル群に対し、管理者以外がアクセスできないように、OS のアクセス権設定を行うことで実現できる。

OE.OS_ACC_SETUP では、管理者が、環境設定ファイル群に対し、管理者以外がアクセスできないように、OS のアクセス権設定を行うことを規定している。

従って、セキュリティ対策方針、OE.OS_ACC_SETUP が満たされることにより、本前提条件を実現することができる。

A.PIN_AUTH

A.PIN_AUTH は、IC カードを使用する人物が、正当な人物であるかを確認するために、PIN による認証が行われる IC カードを利用することを想定した前提条件である。

本前提条件は TOE に利用する IC カードとして、PIN による認証が行われる IC カードを採用し、利用することで実現できる。

OE.PIN_AUTH では、管理者が、TOE に利用する IC カードとして、PIN による認証が行われる IC カード(Java カード)を採用し、利用することを規定している。

従って、セキュリティ対策方針、OE.PIN_AUTH が満たされることにより、本前提条件を実現することができる。

A.PIN_FIG

A.PIN_FIG は、TOE に利用する IC カードの PIN の桁数を、8 桁以上に設定することを想定した前提条件である。

本前提条件は、以下を行うことで実現できる。

・管理者が、TOE に利用する自身の IC カードの PIN の桁数を、8 桁以上に設定すること

・管理者が利用者に対し、TOE に利用する利用者本人の IC カードの PIN の桁数を 8 桁以

上に設定するよう、教育を行うこと

OE.PIN_FIG では、管理者が、TOE に利用する自身の IC カードの PIN の桁数を 8 桁以上に設定することを規定している。また、管理者が利用者に対し、TOE に利用する利用者本人の IC カードの PIN の桁数を、8 桁以上に設定するよう教育を行うことを規定している。

従って、セキュリティ対策方針、**OE.PIN_FIG** が満たされることにより、本前提条件を実現することができる。

A.APP_CONDITION

A.APP_CONDITION は、アプリケーションが、TOE の制御対象であるアプリケーションの識別認証を介してのみ、サービスにアクセスできるものであることを想定した前提条件である（なぜならば、TOE の制御対象であるアプリケーションが提供する識別認証以外の手段で、サービスを利用できた場合、TOE によるアプリケーションに対する ID 及びパスワードの入力の制限は意味のないものになるため。）

本前提条件は、TOE が対応するアプリケーションとして、TOE が ID 及びパスワードを入力する対象の識別認証機能を介してのみ、サービスにアクセスできるものを導入することで実現できる。

OE.APP_CONDITION では、管理者が、TOE が対応するアプリケーションとして、TOE が ID 及びパスワードを入力する対象の識別認証機能を介してのみ、サービスにアクセスできるものを導入することを規定している。

従って、セキュリティ対策方針、**OE.APP_CONDITION** が満たされることにより、本前提条件を実現することができる。

A.IC_CONDITION

A.IC_CONDITION は、TOE の指示により、IC カード自身の情報を変更する機能を有する IC カードが使用されることを想定した前提条件である。

本前提条件は、TOE の指示により、自身の情報を変更する機能を有する IC カードを使用することで実現できる。

OE.IC_CONDITION では、管理者が、TOE の指示により、IC カード(Java カード)自身の情報を変更する機能を有する IC カード(Java カード)を使用することを規定している。

従って、セキュリティ対策方針、**OE.IC_CONDITION** が満たされることにより、本前提条件を実現することができる。

A.WIN_TIME

A.WIN_TIME は、本 TOE が動作する OS(Windows)が、TOE の利用のために、高信頼な時間を生成することを想定した前提条件である。

本前提条件は、TOE の利用のために、高信頼な時間を生成する OS(Windows)を採用し利

用することで実現できる。

OE.WIN_TIME では、管理者は、TOE の利用のために高信頼な時間を生成する、本 TOE に対応した Windows を採用し利用することを規定している。

従って、セキュリティ対策方針、OE.WIN_TIME が満たされることにより、本前提条件を実現することができる。

A.MAINTENANCE

A.MAINTENANCE は、本 ST が定める運用条件として、システムメンテナンス機能を使用しないことを想定した前提条件である。

本前提条件は、管理者がシステムメンテナンス機能を利用しないこと、及び、管理者がシステムメンテナンスのアカウントを作成しないことで実現できる。

OE.MAINTENANCE では、管理者は、本 ST が定める TOE の運用として、システムメンテナンス機能を使用しない運用とすることを規定している。また、管理者が、システムメンテナンスのアカウントを作成しない運用とすることを規定している。

従って、セキュリティ対策方針、OE.MAINTENANCE が満たされることにより、本前提条件を実現することができる。

A.APP_AUTH_CONDITION

A.APP_AUTH_CONDITION は、本 ST 定める運用条件として、アプリケーション認証機能が、IC カードから ID 及びパスワードを読み取る動作に設定されることを想定した前提条件である。

本前提条件は、管理者が、アプリケーション認証機能を、IC カードから ID 及びパスワードを読み取る動作に設定することで実現できる。

OE.APP_AUTH_CONDITION では、管理者は、本 ST 定める運用条件として、アプリケーション認証機能を、IC カードから ID 及びパスワードを読み取る動作とするよう、アプリケーションログオン定義の設定を行うことを規定している。

従って、セキュリティ対策方針、OE.APP_AUTH_CONDITION が満たされることにより、本前提条件を実現することができる。

A.AWAY_FROM_COMPUTER

A.AWAY_FROM_COMPUTER は、悪意のあるものに離席時に TOE の保護資産を利用されないよう、TOE の保護資産を利用時に離席する際には、保護を利用できない状態にした後で離席することを想定した前提条件である。

本前提条件は、利用者および管理者が、TOE の保護資産の利用時に離席する際に、TOE の保護資産を利用できない状態にした上で離席することで実現できる。

OE.AWAY_FROM_COMPUTER では、利用者および管理者が、TOE の保護資産の利用時に離席す

る際には、認証状態が切れたことを確認した後で離席することを規定している。

従って、セキュリティ対策方針、OE.AWAY_FROM_COMPUTER が満たされることにより、本前提条件を実現することができる。

A.ONE_TIME

A.ONE_TIME は、一時ログオン設定機能により一時的に使用可能となった Windows が提供する識別認証は、不要となった際には無効にされることを想定した前提条件である。

本前提条件は、管理者が、一時ログオン設定機能により一時的に使用可能となった Windows が提供する識別認証を、不要となった際に無効に設定することで実現できる。

OE.ONE_TIME では、管理者が、一時ログオン設定機能により一時的に使用可能となった Windows が提供する識別認証を、不要となった際に無効に設定することを規定している。

従って、セキュリティ対策方針、OE.ONE_TIME が満たされることにより、本前提条件を実現することができる。

5. 拡張コンポーネント定義

本章では、拡張機能コンポーネント定義について記述する。

5.1 拡張機能コンポーネントの導出理由

本 TOE では、以下の SFR を拡張の機能要件として定義する。

・FMN_AUT.1

以下に、拡張機能コンポーネントを導出した理由を示す。

・拡張が必要となった理由

本TOEでは、新規の機能要件としてFMN_AUT.1を導出している。FMN_AUT.1では、TOE外の機能と、TOE外の機能が使用するデータを折衝する手段について規定しているが、本機能に合致する既存の機能要件がないため、新規の機能要件を導出している。

・新規クラスとした理由

本TOEでは、新規のクラスとしてFMNクラスを導出している。

本機能で扱うデータは、TOE外の機能が使用するデータ、すなわち利用者データであるため、FDPクラスの導出が考えられる。しかしながら、本TOEで意図するセキュリティ機能の特徴は、FDPクラスで扱う様な利用者データに対する「操作」ではなく、利用者データの「入力手法（インタフェースの隠蔽）や、折衝するための手段」であるため、FDPクラスを含め、既存の機能要件では取り扱うことができない。そのため、新規のクラスとして、FMNクラスを導出する。

・新規ファミリとした理由

本TOEでは、新規のファミリとして、FMN_AUT.1を導出している。

本ファミリでは、TOE外の機能が使用するデータの入力手法や、折衝するための方法にを、利用者による手入力ではなく、TOEにより自動的に行うことを規定している。入力手法を、自動的に行うことを規定したファミリはないため、新機能ファミリを導出する。

なお、本TOEでは、新規のクラスであるFMNを導出しているため、FMNクラス内のファミリは、必然的に新規のファミリとなる。

クラスFMN: TOE外の機能との折衝

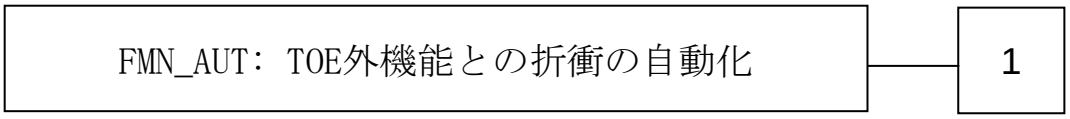
FMNクラスでは、TOE外の機能と、TOE外の機能が使用するデータを折衝する手段について規定する。

情報授受手段の変更と自動化(FMN_AUT.1)

ファミリのふるまい

このファミリでは、TOE 外の機能とデータを折衝する手段を定義し、その定義に従って処理を自動化することを規定している。

コンポーネントのレベル付け



FMN_AUT.1

TOE 外機能との折衝の自動化では、TOE 外の機能とデータを折衝する手段を隠蔽し、TOE または TOE 外の認証機能とやり取りするデータの折衝を自動化しなければならない。

管理: FMN_AUT.1

以下のアクションはFMT における管理機能と考えられる:

·TOEまたはTOE外のセキュリティ機能の管理

監査: FMN_AUT.1

予見される管理アクティビティはない。

FMN_AUT.1 情報授受手段の変更と自動化

下位階層: なし

依存性: なし

FMN_AUT.1.1

TSF は、[割付:*TOE 外のパスワードを利用した識別認証機能のリスト*]への情報入力手段を隠蔽した上で[割付:*TOE または TOE 外の識別認証機能*]で正当と判断された場合、入力手段を隠蔽した識別認証機能を自動処理しなければならない。

6. セキュリティ要件

本章では、セキュリティ要件について記述する。

6.1 セキュリティ機能要件

本節では、TOE セキュリティ機能要件について記述する。

FDP_ACC.1 サブセットアクセス制御

下位階層: なし

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACC.1.1

TSF は、[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御 SFP*]を実施しなければならない。

[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]

表 6-1に示す。

表 6-1 サブジェクト、オブジェクト、操作の対応

サブジェクト	オブジェクト	操作
管理者を代行するTOEのスレッド	●カード種別が Java カードの場合、管理者設定情報(Java カード) なお、管理者設定情報(Java カード)には、以下のものが含まれている。 ・PIN ・PIN コードロック回数 ・初期 PIN コードの強制変更条件 ・PIN のロック状態 ・ユーザ名	改変 設定

	・パスワード ・ログオン先 ・アカウント区分情報	
	●カード種別が FeliCa の場合、管理者設定情報(FeliCa) なお、管理者設定情報(FeliCa)には、以下のものが含まれている。 ・ユーザ名 ・パスワード ・ログオン先 ・アカウント区分情報 ・カード識別番号	
利用者を代行する TOE のスレッド	●カード種別が Java カードの場合、利用者設定情報(Java カード) なお、利用者設定情報(Java カード)には、以下のものが含まれている。 ・PIN ・パスワード	改変
	●カード種別が FeliCa の場合、利用者設定情報(FeliCa) なお、利用者設定情報(FeliCa)内には、以下のものが含まれている。 ・パスワード	

[割付：*アクセス制御SFP*]

IC カード内情報管理 SFP

FDP_ACF.1 セキュリティ属性によるアクセス制御

下位階層: なし

依存性: FDP_ACC.1 サブセットアクセス制御
FMT_MSA.3 静的属性初期化

FDP_ACF.1.1

TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御 SFP*]を実施しなければならない。

[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]

サブジェクト	SFP関連の属性
TOEのスレッド	カードID 管理者権限 利用者権限

オブジェクト	SFP関連の属性
・管理者設定情報(Java カード) ・利用者設定情報(Java カード) ・管理者設定情報(FeliCa) ・利用者設定情報(FeliCa)	カードID カード種別

[割付: *アクセス制御 SFP*]
IC カード内情報管理 SFP

FDP_ACF.1.2

TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、次の規則を実施しなければならない:［*割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*］。

［*割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*］

●カード種別が「Java カード」である場合

・管理者権限を有する TOE のスレッドの場合、Java カードに関係する全てのオブジェクト（管理者設定情報(Java カード)、利用者設定情報(Java カード)）の改変、設定を許可する。

・利用者権限を有する TOE のスレッドの場合、サブジェクト属性であるカード ID とオブジェクト属性であるカード ID が一致した場合、利用者設定情報(Java カード)の改変操作を許可する

●カード種別が「FeliCa」である場合

・管理者権限を有する TOE のスレッドの場合、FeliCa に関係する全てのオブジェクト（管理者設定情報(FeliCa)、利用者設定情報(FeliCa)）の改変、設定を許可する

・利用者権限を有する TOE のスレッドの場合、サブジェクト属性のカード ID とオブジェクト属性であるカード ID が一致した場合、利用者設定情報(FeliCa)の改変操作を許可する

FDP_ACF.1.3

TSF は、次の追加規則、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。

[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則*]
なし

FDP_ACF.1.4

TSF は、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]
なし

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: *認証事象のリスト*]に関して、[選択: *[割付: 正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]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。

[割付: *認証事象のリスト*]
PIN の認証　(Windows ログオン機能の一部)

[選択: *[割付: 正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]
[割付: 許容可能な値の範囲]
1～16

FIA_AFL.1.2

不成功の認証試行が定義した回数[選択 : *に達する、を上回った*]とき、TSF は、[割付: *アクションのリスト*]をしなければならない。

[選択 : *に達する、を上回った*]
・に達する

[割付: *アクションのリスト*]
・管理者が解除するまで、PIN の認証をロックする

FIA_ATD.1 利用者属性定義

下位階層: なし

依存性: なし

FIA_ATD.1.1

TSF は、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない。:[割付: *セキュリティ属性のリスト*]

[割付: *セキュリティ属性のリスト*]

・カード ID

・管理者権限

・利用者権限

FIA_UAU.2 アクション前の利用者認証

下位階層: FIA_UAU.1 認証のタイミング

依存性: FIA_UID.1 識別のタイミング

FIA_UAU.2.1

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。

FIA_UID.2(1) アクション前の利用者識別

下位階層: FIA_UID.1 識別のタイミング

依存性: なし

FIA_UID.2.1(1)

PINによる認証機能は、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。

※下線部は詳細化

FIA_UID.2(2) アクション前の利用者識別

下位階層: FIA_UID.1 識別のタイミング

依存性: なし

FIA_UID.2.1(2)

役割を識別する機能は、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。

※下線部は詳細化

FIA_USB.1 利用者・サブジェクト結合

下位階層: なし

依存性: FIA_ATD.1 利用者属性定義

FIA_USB.1.1

TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。:[割付: *利用者セキュリティ属性のリスト*]

[割付: *利用者セキュリティ属性のリスト*]

・カードID
・管理者権限
・利用者権限

FIA_USB.1.2

TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。:[割付: *属性の最初の関連付けの規則*]

[割付: *属性の最初の関連付けの規則*]

・PINの照合が完了し、ICカードから情報を読み出しWindowsにより識別認証されたタイミングで、TOEのスレッドと各利用者セキュリティ属性を関連付ける

FIA_USB.1.3

TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。:[割付: *属性の変更の規則*]

[割付: *属性の変更の規則*]

・なし

FMN_AUT.1 情報授受手段の変更と自動化

下位階層: なし

依存性: なし

FMN_AUT.1.1

TSF は、[割付:*TOE 外のパスワードを利用した識別認証機能のリスト*]への情報入力手段を隠蔽した上で[割付:*TOE または TOE 外の識別認証機能*] で正当と判断された場合、入力手段を隠蔽した識別認証機能を自動処理しなければならない。

[割付:*TOE 外のパスワードを利用した識別認証機能のリスト*]

・Windows の識別認証機能

・アプリケーションの認証機能

[割付:*TOE または TOE 外の識別認証機能*]

・TOE による PIN 認証

・IC カードによる PIN 認証

FMT_MOF.1 セキュリティ機能のふるまいの管理

下位階層: なし

依存性: FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

FMT_MOF.1.1

TSF は、機能[割付: *機能のリスト*][選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]能力を[割付: *許可された識別された役割*]に制限しなければならない。

[割付: *機能のリスト*]
表 6-2に示す。

[選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]
表 6-2に示す。

[割付: *許可された識別された役割*]
表 6-2に示す。

表 6-2 セキュリティ機能のふるまい管理

[割付：機能のリスト]	[選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]	[割付: *許可された識別された役割*]
●Windows ログオン変更(パスワード手入力)の機能として、以下の機能のリスト ・Windows ログオン機能	・のふるまいを改変する	管理者役割

FMT_MTD.1 TSFデータの管理

下位階層: なし

依存性: FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

FMT_MTD.1.1

TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付: *許可された識別された役割*]に制限しなければならない。

[割付: *TSF データのリスト*]
表 6-3に示す。

[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]
[割付: その他の操作]
表 6-3に示す。

[割付: *許可された識別された役割*]
表 6-3に示す。

表 6-3 TSF データと操作の対応

[割付：*許可された識別された役割*]	[割付：*TSF データのリスト*]	[選択：*デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]*]
管理者役割	・すべての利用者の PIN ・PIN コードロック回数 ・初期 PIN コードの強制変更条件	改変 *[その他の操作]*：設定
利用者役割	・当該利用者の PIN	改変

FMT_SMF.1 管理機能の特定

下位階層： なし

依存性： なし

FMT_SMF.1.1

TSF は、以下の管理機能を実行することができなければならない。:[割付: *TSF によって提供される管理機能のリスト*]

[割付: *TSF によって提供される管理機能のリスト*]

・ICカード情報設定機能(管理者向け)

・IC カード情報設定機能（利用者向け）

FMT_SMR.1 セキュリティの役割

下位階層: なし

依存性: FIA_UID.1 識別のタイミング

FMT_SMR.1.1

TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。

[割付: *許可された識別された役割*]

・管理者役割

・利用者役割

FMT_SMR.1.2

TSF は、利用者を役割に関連付けなければならない。

FTA_SSL.3 TSF起動による終了

下位階層: なし

依存性: なし

FTA_SSL.3.1

TSF は、[割付: *利用者が非アクティブである時間間隔*]後に対話セションを終了しなければならない。

[割付: *利用者が非アクティブである時間間隔*]
・ICカードが非アクティブ状態となったと同時

6.2 セキュリティ保証要件

本節では、TOE セキュリティ保証要件について記述する。

本ST にて要求する、TOEに対する保証レベルはEAL2 である。TOEに対する保証コンポーネント構成を表 6-4に示す。要求する各保証コンポーネントの保証エレメントは、CCパート 3 の要求通りである。

表 6-4 TOE の保証要件コンポーネント一覧

TOE セキュリティ保証要件		コンポーネント
開発	セキュリティアーキテクチャ記述	ADV_ARC.1
	セキュリティ実施機能仕様	ADV_FSP.2
	基本設計	ADV_TDS.1
ガイダンス文書	利用者操作ガイダンス	AGD_OPE.1
	準備手続き	AGD_PRE.1
ライフサイクル サポート	CM システムの使用	ALC_CMC.2
	TOE の一部の CM 範囲	ALC_CMS.2
	配付手続き	ALC_DEL.1
セキュリティターゲット 評価	適合主張	ASE_CCL.1
	拡張コンポーネント定義	ASE_ECD.1
	ST 概説	ASE_INT.1
	セキュリティ対策方針	ASE_OBJ.2
	派生したセキュリティ要件	ASE_REQ.2
	セキュリティ課題定義	ASE_SPD.1
	TOE 要約仕様	ASE_TSS.1
テスト	カバレージの証拠	ATE_COV.1
	機能テスト	ATE_FUN.1
	独立テスト - サンプル	ATE_IND.2
脆弱性評定	脆弱性分析	AVA_VAN.2

6.3 セキュリティ要件根拠

本節では、セキュリティ対策方針に対するセキュリティ要件の必要性と十分性の根拠を示すとともに、各セキュリティ要件の依存性が満足されていることを示す。また、設定したセキュリティ保証要件が妥当である根拠を示す。

6.3.1 セキュリティ機能要件根拠

セキュリティ対策方針に対するTOEセキュリティ機能要件の対応を『表 6-5 セキュリティ対策方針とTOEセキュリティ機能要件の対応』に示す。

表 6-5 セキュリティ対策方針と TOE セキュリティ機能要件の対応

セキュリティ対策方針 / TOE セキュリティ機能要件	O.IC_I&A
FDP_ACC.1	○
FDP_ACF.1	○
FIA_AFL.1	○
FIA_ATD.1	○
FIA_UAU.2	○
FIA_UID.2(1)	○
FIA_UID.2(2)	○
FIA_USB.1	○
FMN_AUT.1	○
FMT_MOF.1	○
FMT_MTD.1	○
FMT_SMF.1	○
FMT_SMR.1	○
FTA_SSL.3	○

以下に、『表 6-5 セキュリティ対策方針とTOEセキュリティ機能要件の対応』の根拠を示す。

O.IC_I&A

O.IC_I&A は、TOE が、Windows やアプリケーションに対し、ID 及びパスワードを手入力できないようにした上で、IC カードにより入力するよう変更する対策方針である。

また、IC カードの不正取得に伴う不正行為を考慮して、IC カードからの ID 及びパスワードの読み出しは､IC カードによる PIN 認証の後に可能とさせることを規定している。

但し、IC カードの所持を忘れた利用者への対応として、従来の Windows が提供する識別認証を利用者に特別に利用許可させる機能を、管理者にのみ提供するものとしている。

また、離席対応として、IC カードが非アクティブ状態となった際には、認証状態を解除する。

本対策方針は、以下の機能要件を導出することで実現できる。

①TOE 外のパスワードを利用した識別認証機能への、ID 及びパスワードの入力手段を隠蔽する機能要件

②ID 及びパスワードの読み出しの可否の判断を、TOE または TOE 外の識別認証機能に依頼する機能要件

③上記②の処理を自動化すること

④TOE 内で、TOE の関係者の代替として振舞う TOE のスレッドと、利用者のセキュリティ属性とを関連付ける機能要件

⑤IC カードの所持を忘れた利用者への対応として、TOE のセキュリティ機能のふるまいを変更させ、従来の Windows が提供する識別認証を利用者に利用許可させる機能機能要件

⑥離席時にサービスを不正に利用されることを考慮して、IC カードが非アクティブ状態となった際には、当該認証状態を解除する機能要件

⑦上記に関する環境設定の機能要件

そのため、本 TOE では以下の機能要件を導出する。

[①,②,③について]

FMN_AUT.1 により、以下を規定している。

・TSF は、TOE 外のパスワードを利用した識別認証機能への情報入力手段を、隠蔽すること

・TSF は、TOE または TOE 外の識別認証機能にて正当であると判断された後、入力手段を隠蔽した識別認証機能を自動処理すること

但し、FeliCa の場合、TOE にて識別と認証を行う必要があるため、FIA_UID.2(1)及び FIA_UAU.2 により識別と認証を行うことを規定している。また、役割の識別を FIA_UID.2(2)にて規定している。

また、規定された回数認証を失敗した場合のアカウントのロックを、FIA_AFL.1 にて規定している。

[④について]

FIA_ATD.1、FIA_USB.1 により、利用者のセキュリティ属性を定義した上で、TOE のスレッドと利用者のセキュリティ属性の関連付けを行うことを規定している。

[⑤について]

FMT_MOF.1 により、セキュリティ機能のふるまいを改変する能力を、管理者のみに制限し、FMT_SMF.1 によりその実体の管理機能を与えることを規定している。また、FMT_SMR.1 により、管理者の役割が維持することを規定している。

[⑥について]

FTA_SSL.3 により、IC カードが非アクティブ状態となった際には、当該認証状態を解除する。

[⑦について]

環境設定については、環境定義ファイルに依存せずセキュリティ機能の振る舞いを変更するもの、環境設定ファイル群に対するもの、及び IC カードに対するものに大別される。

環境定義ファイルに依存せずセキュリティ機能の振る舞い変更するものに関しては、⑤のことであるため、上記[⑤について]を参照のこと。

環境設定ファイル群に対する設定に関しては、Windows が処理のすべてを担うため、TOE として機能要件は導出しない。

IC カードに対する設定に関しては、FeliCa の場合は、設定の機能を TOE が有するが、Java カードの場合は、設定の機能を Java カードが有する。但し、FeliCa、Java カードの両 IC カード共に、設定制限の機能はないため、TOE にて、IC カード内の情報への環境設定を、許可された役割のみに制限する機能を導入する。そのため、

・FMT_MTD.1 により、TSF データの管理を管理者に制限する。また、自身の ID やパスワードに関しては、利用者が利用できるように制御する。また、FMT_SMR.1 により、管理者及び利用者の役割が維持される。

・FeliCa に関しては、FMT_SMF.1 により、管理機能である、IC カード情報設定機能(管理

者向け)、IC カード情報設定機能(利用者向け)を提供する。

・FDP_ACC.1、FDP_ACF.1 により、管理者、及び利用者に対し、対象の利用者データ(TOE 外部のセキュリティ機能が使用するデータ)に対するアクセス制御を行う。

以上のセキュリティ機能要件によって、O.IC_I&A を満たすことができる。

6.3.2 依存性の検証

TOEセキュリティ機能要件間の依存関係を『表 6-6 TOEセキュリティ機能要件間の依存関係』に示す。なお、依存関係に対して問題がないことの根拠を表中の「問題がないことの根拠」に示す。

なお、依存関係において、依存を満たしている場合「○」を、依存していない場合、「×」を表記する。

表 6-6 TOE セキュリティ機能要件間の依存関係

コンポーネント	依存関係	問題がないことの根拠
FDP_ACC.1	FDP_ACF.1(○)	すべての依存関係を満たしている。
FDP_ACF.1	FDP_ACC.1(○) FMT_MSA.3(×)	FMT_MSA.3 は管理対象となるセキュリティ属性が無いため適用しない。
FIA_AFL.1	FIA_UAU.2(○)	本来の依存先は FIA_UAU.1 であるが、FIA_UAU.2(1)は FIA_UAU.1 の上位階層の機能要件であるため、依存関係は満たされる。
FIA_ATD.1	なし	－
FIA_UAU.2	FIA_UID.2(○)	依存先は、FIA_UID.2(1)である。なお、本来の依存先は FIA_UID.1 であるが、FIA_UID.2(1)は FIA_UID.1 の上位階層の機能要件であるため、依存関係は満たされる。
FIA_UID.2(1)	なし	－
FIA_UID.2(2)	なし	－
FIA_USB.1	FIA_ATD.1(○)	すべての依存関係を満たしている。
FMN_AUT.1	なし	－
FMT_MOF.1	FMT_SMF.1(○) FMT_SMR.1(○)	すべての依存関係を満たしている。
FMT_MTD.1	FMT_SMF.1(×) FMT_SMR.1(○)	本 SFR は、FMT_SMF.1 に依存していない。 FMT_SMF.1 は、管理機能の実体を与えるものであるが、管理機能の実体は IC カードが有しているため、本 SFR の依存として、FMT_SMF.1 は必要ない。 なお、上記については、OE.IC_CONDITION にて対処している。
FMT_SMF.1	なし	－
FMT_SMR.1	FIA_UID.1(○)	依存先は、FIA_UID.2(2)である。なお、本来の依存先は FIA_UID.1 であるが、FIA_UID.2(2)は FIA_UID.1 の上位階層の機能要件であるため、依存関係は満たされる。

コンポーネント	依存関係	問題がないことの根拠
FTA_SSL.3	なし	－

6.3.3 セキュリティ保証要件根拠

本 TOE は、従来、Windows PC にログオンする際に手で行われていた ID 及びパスワードの入力を、IC カードを基にした入力に変更する機能を提供する製品である。本製品は、IC カードを利用した運用が中心となり、消費者に提供されている外部インタフェースは限られており、攻撃としては限られた外部インタフェースから行われることが想定される。

本製品が想定する攻撃への対抗性を保証するためには、セキュリティ機能の確実な設計、系統だったテストと脆弱性分析に加え、セキュリティ機能が外部からの影響を受けることなく確実に動作するためのアーキテクチャ設計が行われていることの確認が必要であり、これらの確認は EAL2 レベルの保証によって達成される。そのため、本 TOE では EAL2 を選択する。

また、SAR としては、EAL2 で要求されるすべての SAR を選択する。

7. TOE要約仕様

本節では、TOE のセキュリティ機能を説明する。各セキュリティ機能に対応する TOE セキュリティ機能要件が示されているように、本節で説明するセキュリティ機能は、5,6 章で記述した TOE セキュリティ機能要件を満たす。

7.1 Windowsログオン機能

Windows ログオン機能は、以下のセキュリティ機能群を備える。

セキュリティ機能の仕様	TOE セキュリティ機能要件
本機能は、PIN を IC カードに受け渡し、TOE (注 1) または IC カードにて PIN が正当であると判断された後、IC カード内に格納された ID、パスワード、ドメイン情報を自動的に読み取り(注 2)、Windows の識別認証機能へ識別認証の依頼を行う。本機能により、Windows が提供する識別認証のインタフェースは隠蔽され、IC カードによる識別認証のインタフェースのみが表示される。 注 1)FeliCa の場合は、TOE が PIN の認証を行う。PIN の認証は、カード ID と PIN による組み合わせにより行われる。また、カード ID に対応しない不正な PIN を[1～16 回]続けて入力した場合、管理者による解除まで、PIN の認証をロックする。 注 2)IC カード管理機能(管理者向け)において、次回ログオン時のパスワードの手入力有無が「有効」の場合は、ID は IC カードから読み込まれるが、パスワードは入力を要求する画面が表示され、パスワードを手入力する必要がある。 また、IC カードが非アクティブ状態(IC カード、または IC カードリーダライタが引き抜かれる)となった際には、そのログオン状態を解除する。なお、本機能の前に利用できる TOE のセキュリティ機能はない。 【TOE の各機能を実行するプロセスについて】 TOE 内に存在するプロセスは、カード ID 及び役割（管理者、利用者）に関する情報をリストとして有し、各 TOE の関係者のふるまいを継承して、TOE の機能を実行する。なお、TOE のプロセスと、各役割の情報のリストの関連付けは、PIN が正当であると判断され IC カードから情報を読み出し、Windows に識別認証されたタイミングで行われる。	FIA_AFL.1 FIA_ATD.1 FIA_UID.2(1) FIA_UID.2(2) FIA_UAU.2 FIA_USB.1 FMN_AUT.1 FTA_SSL.3

7.1.1 対応するSFRの実現方法

FIA_AFL.1

本セキュリティ要件は、認証事象に関し、規定された回数の不成功認証が生じたとき、規定されたアクションを行うことを要求する。

これに対し、本セキュリティ機能は、FeliCa である場合、カード ID に対応しない不正な PIN を[1～16 回]続けて入力した場合、PIN の認証（Windows ログオン機能の一部の認証処理）をロックする。PIN のロック解除は、IC カード管理機能(管理者向け)の「PIN のロック解除」により行う。

よって、本セキュリティ機能要件は満たされる。

FIA_ATD.1

本セキュリティ要件は、個々の利用者に属するセキュリティ属性のリストを維持することを要求する

これに対し、TOE 内に存在するプロセスは、カード ID 及び役割（管理者、利用者)に関する情報をリストとして有する。

よって、本セキュリティ機能要件は満たされる。

FIA_UAU.2

本セキュリティ要件は、利用者の認証前に利用者に対する TSF 調停アクションを許可しないことを要求する。

これに対し、本セキュリティ機能は、FeliCa の場合、カード ID と PIN による組み合わせにより、PIN の認証(Windows ログオン機能の一部の認証処理)を行う。本機能の前に、利用できる TOE のセキュリティ機能はない。

よって、本セキュリティ機能要件は満たされる。

FIA_UID.2(1)

本セキュリティ要件は、PIN による認証機能が、利用者の識別前に利用者に対する TSF 調停アクションを許可しないことを要求する。

これに対し、本セキュリティ機能は、FeliCa の場合、カード ID と PIN による組み合わせにより PIN の認証(Windows ログオン機能の一部の認証処理)を行う。

よって、本セキュリティ機能要件は満たされる。

FIA_UID.2(2)

本セキュリティ要件は、役割を識別する機能が、利用者の識別前に利用者に対する TSF 調停アクションを許可しないことを要求する。

これに対し、本セキュリティ機能は、Windows により実施される識別結果を受け、管理者、利用者の役割を識別する。

よって、本セキュリティ機能要件は満たされる。

FIA_USB.1

本セキュリティ要件は、利用者とサブジェクトの結合に際して、適切なセキュリティ属性を、その利用者を代行するサブジェクトに関連付ける規則を要求する

これに対し、本セキュリティ機能では、TOE 内に存在するプロセスとカード ID 及び役割（管理者、利用者)を関連付ける。また、関連付けは、PIN が正当であると判断され IC カードから情報を読み出すタイミングで行う。

よって、本セキュリティ機能要件は満たされる。

FMN_AUT.1

本セキュリティ機能要件では、「①TSF が TOE 外のパスワードを利用した識別認証機能への情報入力手段を隠蔽すること」、「②TOE または TOE 外の識別認証機能にて正当であると判断された後、入力手段を隠蔽した識別認証機能を自動処理すること」を規定している。

これに対し、本セキュリティ機能は以下を実装している。

[①について]

本セキュリティ機能は、Windows が提供する識別認証のインタフェースを隠蔽し、IC カードによる識別認証のインタフェースのみを表示している。

[②について]

Java カードの場合、PIN を IC カードの PIN 認証機能に受け渡し、当該 PIN が正当であるかの確認依頼を行う。一方、FeliCa の場合、本機能が PIN の認証を行う。

本機能の PIN の認証、または IC カードの PIN 認証機能により正当であると判断された後は、ID、パスワードを IC カードから自動的に読み取り、Windows が提供する識別認証機能へ識別認証の依頼を行う。

よって、本セキュリティ機能要件は満たされる。

FTA_SSL.3

本セキュリティ機能要件は、IC カードが非アクティブ状態となったと同時に、対話セションを終了することを要求する。

これに対して、本セキュリティ機能は、IC カードが非アクティブ状態(IC カードリーダライタが引き抜かれる)となった際に、そのログオン状態を解除する。

よって、本セキュリティ機能要件は満たされる。

7.2 アプリケーション認証機能

アプリケーション認証機能は、以下のセキュリティ機能群を備える。

セキュリティ機能の仕様	TOE セキュリティ機能要件
本機能は、PIN を IC カードに受け渡し、IC カード(※)にて PIN が正当であると判断された後、IC カード内に格納された ID、パスワードを読み取り、アプリケーションの識別認証機能へ識別認証の依頼を行う機能である。本機能により、アプリケーションが提供する識別認証のインタフェースは隠蔽され、IC カードを利用した方法のみ可能となる。 ※FeliCa の場合は、TOE が PIN の認証を行う。PIN の認証は、カード ID と PIN による組み合わせにより行われる。また、カード ID に対応しない不正な PIN を[1～16 回]続けて入力した場合、PIN の認証をロックする。PIN のロック解除は、IC カード管理機能(管理者向け)の「PIN のロック解除」により行われる。 本機能の利用の前に、利用可能なアプリケーションの機能はない。 但し、シングルサインオンが有効の場合は、本機能は自動で行われる。一方、無効の場合は、PIN を手入力で行う必要がある。	FIA_AFL.1 FIA_UID.2(1) FIA_UAU.2 FMN_AUT.1

7.2.1 対応するSFRの実現方法

以下で説明する、FIA_AFL.1、FIA_UID.2(1)、FIA_UAU.2 は、シングルサインオンが有効の場合、手入力は必要なくなり自動で行われる。これを踏まえて、各 SFR の実現方法を示す。

FIA_AFL.1

FIA_AFL.1 は、認証事象に関し、規定された回数の不成功認証が生じたとき、規定されたアクションを行うことを要求する。

これに対し、本セキュリティ機能は、FeliCa である場合、カード ID に対応しない不正な PIN を[1～16 回]続けて入力した場合、PIN の認証（アプリケーション認証機能の一部の認証処理）をロックする。PIN のロック解除は、IC カード管理機能(管理者向け)の「PIN のロック解除」により行う。

よって、本セキュリティ機能要件は満たされる。

FIA_UID.2(1)

本セキュリティ要件は、PIN による認証機能が、利用者の識別前に利用者に対する TSF 調停アクションを許可しないことを要求する。

これに対し、本セキュリティ機能は、FeliCa の場合、カード ID と PIN による組み合わせにより PIN の認証(アプリケーション認証機能の一部の認証処理)を行う。

よって、本セキュリティ機能要件は満たされる。

FIA_UAU.2

本セキュリティ要件は、利用者の認証前に利用者に対する TSF 調停アクションを許可しないことを要求する。

これに対し、本セキュリティ機能は、FeliCa の場合、カード ID と PIN による組み合わせにより、PIN の認証(アプリケーション認証機能の一部の認証処理)を行う。本機能の前に、利用できる TOE のセキュリティ機能はない。

よって、本セキュリティ機能要件は満たされる。

FMN_AUT.1

本セキュリティ機能要件では、「①TSF が TOE 外のセキュリティ機能への情報入力手段を隠蔽すること」及び、「②TOE または TOE 外の識別認証機能にて正当であると判断された後、入力手段を隠蔽した識別認証機能を自動処理すること。」を規定している。

これに対し、本セキュリティ機能は以下を実装している。

[①について]

本セキュリティ機能は、アプリケーションが提供する識別認証のインタフェースを隠蔽し、IC カードによる識別認証のインタフェースのみを表示している。

[②について]

Java カードの場合、PIN を IC カードの PIN 認証機能に受け渡し、当該 PIN が正当であるかの確認依頼を行う。

一方、FeliCa の場合、本機能が、PIN の認証を行う。

本機能の PIN の認証、または IC カードの PIN 認証機能により正当であると判断された後は、ID、パスワードを IC カードから自動的に読み取り、アプリケーションが提供する識別認証機能へ識別認証の依頼を行う。

よって、本セキュリティ機能要件は満たされる。

7.4 ICカード管理機能（管理者向け）

IC カード管理機能（管理者向け）は、以下のセキュリティ機能群を備える。

セキュリティ機能の仕様	TOE セキュリティ機能要件
本機能では、FeliCa の場合、管理者に対し、全ての利用者の IC カード内の情報の設定及び制限機能を提供する。一方、Java カードの場合、管理者に対し、全ての利用者の IC カード内の情報の利用の制限機能を提供する。 なお、FeliCa における、IC カード内情報の設定機能部を、「IC カード情報設定機能（管理者向け)」と称する。 対象となる設定情報を以下に示す。 以下、設定情報毎に詳細を示す。 (1)アカウント管理 アカウントに関する以下の情報。 ・ユーザ名 TOE にて利用され、また、Windows にログオンする際に利用される ID。 ・パスワード パスワードを手入力とする設定の場合、指定するパスワード。 1～32 桁の以下の文字を除く、半角英数字記号 “/ ¥ [ ] : ; | = , + * ? < >” ・次回ログオン時のパスワードの手入力有無 次回ログオン時のパスワードの手入力の必要有無の設定。本情報が「有効」の場合、Windows ログオン機能にて、パスワードの手入力が必要となる。 ・対象アプリ 設定する対象のアプリケーションの設定。以下から選択する。 - Windows ログオン - HTML フォーム認証 - BASIC 認証 - Java アプレット認証	FDP_ACC.1 FDP_ACF.1 FIA_AFL.1 FMT_MOF.1 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1

・ログオン先 ログオン先のドメイン情報。 ・アカウント区分 利用者か、管理者かのアカウント区分（注） (2) PIN コード管理 IC カード内の PIN 情報。設定可能な PIN 情報は以下の通り。 ・PIN PIN コード自体。PIN コードの変更や設定の際に指定する。 ・PIN コードロック回数 PIN コードの入力を間違えた際にロックする場合のリトライ回数である。 ・初期 PIN コード強制変更 初回のカード利用の際に、新しい PIN コードの入力を要求し、強制的に初期 PIN コードを変更させるかの条件 ・PIN のロック解除 IC カードの PIN コードロック状態を解除する。	

注)利用者の IC カードに「管理者」区分を指定することはできない。

7.4.1 対応するSFRの実現方法

FDP_ACC.1

本セキュリティ機能要件は、以下を行うアクセス制御 SFP「IC カード内情報管理 SFP」を規定している。

・カード種別が Java カードである場合、管理者を代行する TOE のスレッドが、Java カードに関係する全てのオブジェクト（管理者設定情報(Java カード)、利用者設定情報(Java カード)）の改変、設定を許可する

・カード種別が FeliCa である場合、管理者を代行する TOE のスレッドが、FeliCa に関係する全てのオブジェクト（管理者設定情報(FeliCa)、利用者設定情報(FeliCa)）の改変、設定を許可する。

上記のオブジェクトと、オブジェクト内の情報の対応について、表 7-1に示す

表 7-1 オブジェクトとオブジェクト内の情報の対応

オブジェクト	オブジェクト内の情報
管理者設定情報(Java カード)	・PIN ・PIN コードロック回数 ・初期 PIN コードの強制変

	更条件 ・PIN のロック状態 ・ユーザ名 ・パスワード ・ログオン先 ・アカウント区分情報
管理者設定情報(FeliCa)	・ユーザ名 ・パスワード ・ログオン先 ・アカウント区分情報 ・カード識別番号
利用者設定情報(Java カード)	・PIN ・パスワード
利用者設定情報(FeliCa)	・パスワード

これに対し、本セキュリティ機能では、管理者に対し、「ユーザ名」、「パスワード」、「ログオン先」、「アカウント区分情報」、「カード識別番号」、「PIN」、「PIN コードロック回数」「初期 PIN コードの強制変更条件」、「PIN のロック状態」への改変、設定を許可している。

よって、本セキュリティ機能要件は満たされる。

FDP_ACF.1

本セキュリティ機能要件は、以下を行うアクセス制御 SFP「IC カード内情報管理 SFP」を規定している。

●カード種別が「Java カード」である場合

・管理者を代行する TOE のスレッドの場合、Java カードに関係する全てのオブジェクト（管理者設定情報(Java カード)、利用者設定情報(Java カード)）の改変、設定を許可する

●カード種別が「FeliCa」である場合

・管理者を代行する TOE のスレッドの場合、FeliCa に関係する全てのオブジェクト（利用者設定情報(FeliCa)、管理者設定情報(FeliCa)）の改変、設定を許可する。

これに対し、本セキュリティ機能では、管理者に対し、「ユーザ名」、「パスワード」、「ログオン先」、「アカウント区分情報」、「カード識別番号」、「PIN」、「PIN コードロック回数」「初期 PIN コードの強制変更条件」、「PIN のロック状態」への改変、設定を許可している。よって、本セキュリティ機能要件は満たされる。

FIA_AFL.1

本セキュリティ要件は、認証事象に関し、規定された回数の不成功認証が生じたとき、規定されたアクションを行うことを要求する。

これに対し、本セキュリティ機能は、「規定された回数の不成功認証が生じたとき、規定されたアクション」が実行された際、そのアクションを解除する方法を規定しており、具体的には「PIN のロック解除」で実現している。

よって、本セキュリティ機能要件は満たされる。

FMT_MOF.1

本セキュリティ機能要件は、セキュリティ機能(Windows ログオン機能)のふるまい管理を許可された役割の者のみに制限することを要求する。これに対して、本セキュリティ機能は管理者のみ、IC カード内の情報である「次回ログオン時のパスワードの手入力有無」を設定することが許可され、「有効」に設定することで Windows ログオン機能のふるまいは変更されてパスワードの入力を要求する画面が表示される。

よって、本セキュリティ機能要件は満たされる。

FMT_MTD.1

本セキュリティ機能要件は、TSF データの管理を許可された役割の者のみに制限することを要求する。これに対して、本セキュリティ機能は、管理者のみに TSF データ(FeliCa の場合)である「PIN」、「PIN コードロック回数」、「初期 PIN コードの強制変更条件」を設定、変更することを許可する。

よって、本セキュリティ機能要件は満たされる。

FMT_SMF.1

本セキュリティ機能要件は、FMT_MTD.1 で規定している TSF データに対する管理機能を要求する。これに対し、本セキュリティ機能では、「IC カード情報設定管理機能(管理者向け)」として、管理機能を提供している。

よって、本セキュリティ要件は満たされる。

FMT_SMR.1

本セキュリティ機能要件は、許可された識別された役割を維持することを要求する。これに対して、本セキュリティ機能は、管理者の役割を維持管理する機能を提供する。

よって、本セキュリティ機能要件は満たされる。

7.5 ICカード管理機能(利用者向け)

IC カード管理機能(利用者向け)は、以下のセキュリティ機能群を備える。

セキュリティ機能の仕様	TOE セキュリティ機能要件
本機能では、FeliCa の場合、利用者に対し、当該利用者の IC カード内の情報の設定及び制限機能を提供する。一方、Java カードの場合、利用者に対し、当該利用者の IC カード内の情報の利用の制限機能を提供する。 なお、FeliCa における、IC カード内情報の設定機能部を、「IC カード情報設定機能（利用者向け)」と称する。 以下、設定情報毎に詳細を示す。 (1)PIN 変更 利用者用の IC カードの PIN コード。 (2)パスワード変更 利用者用の IC カード内のパスワード。	FDP_ACC.1 FDP_ACF.1 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1

7.5.1 対応するSFRの実現方法

FDP_ACC.1

本セキュリティ機能要件は、以下を行うアクセス制御 SFP「IC カード内情報管理 SFP」を規定している。

●カード種別が「Java カード」である場合

・利用者権限を有する TOE のスレッドの場合、サブジェクト属性であるカード ID とオブジェクト属性であるカード ID が一致した場合、利用者設定情報(Java カード)の改変操作を許可する

●カード種別が「FeliCa」である場合

・利用者権限を有する TOE のスレッドの場合、サブジェクト属性のカード ID とオブジェクト属性であるカード ID が一致した場合、利用者設定情報(FeliCa)の改変操作を許可する

これに対し、本セキュリティ機能では、利用者に対し、当該利用者の「PIN」及び「パスワード」の変更を許可している。

よって、本セキュリティ機能要件は満たされる。

FDP_ACF.1

本セキュリティ機能要件は、以下を行うアクセス制御 SFP「IC カード内情報管理 SFP」を規定している。

●カード種別が「Java カード」である場合

・利用者権限を有する TOE のスレッドの場合、サブジェクト属性であるカード ID とオブジェクト属性であるカード ID が一致した場合、利用者設定情報(Java カード)の改変操作を許可する

●カード種別が「FeliCa」である場合

・利用者権限を有する TOE のスレッドの場合、サブジェクト属性のカード ID とオブジェクト属性であるカード ID が一致した場合、利用者設定情報(FeliCa)の改変操作を許可する

これに対し、本セキュリティ機能では、利用者に対し、当該利用者の「PIN」及び「パスワード」の変更を許可している。

よって、本セキュリティ機能要件は満たされる。

FMT_MTD.1

本セキュリティ機能要件は、TSF データの管理を許可された役割の者のみに制限することを要求する。これに対して、本セキュリティ機能は、利用者に TSF データ(FeliCa の場合)である自身の PIN を変更することを許可する。

よって、本セキュリティ機能要件は満たされる。

FMT_SMF.1

本セキュリティ機能要件は、FMT_MTD.1 で規定している TSF データに対する管理機能を要求する。これに対し、本セキュリティ機能では、「IC カード情報設定機能 (利用者向け)」として、管理機能を提供している。

よって、本セキュリティ要件は満たされる。

FMT_SMR.1

本セキュリティ機能要件は、許可された識別された役割を維持することを要求する。これに対して、本セキュリティ機能は、利用者の役割を維持管理する機能を提供する。

よって、本セキュリティ機能要件は満たされる。

（　最終ページ　）