認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙 押印済

評価対象

申請受付日（受付番号）	**平成20年1月17日** (IT**認証**8191)
認証番号	C0192
認証申請者	**富士通株式会社**
TOE**の名称**	SafetyDomain
TOE**のバージョン**	V04L01
PP**適合**	**なし**
適合する保証パッケージ	EAL2
開発者	**富士通株式会社**
評価機関の名称	**みずほ情報総研株式会社　情報セキュリティ評価室**

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。
平成20年10月30日

セキュリティセンター 情報セキュリティ認証室
技術管理者　鈴木　秀二

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① 情報技術セキュリティ評価のためのコモンクライテリア バージョン3.1 改訂第2版 (翻訳第2.0版)
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 改訂第2版 (翻訳第2.0版)

評価結果：合格

「SafetyDomain」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

1.1 はじめに

この認証報告書は、「SafetyDomain」（以下「本TOE」という。）について、みずほ情報総研株式会社　情報セキュリティ評価室（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者である富士通株式会社に報告するものである。

本認証報告書の読者は、本書と共に、対応するSTを併読されたい。本TOEの動作条件や運用のための前提についての詳細、本TOEが対抗する脅威へのセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件、及びセキュリティ仕様の概要と十分性の根拠は、STにおいて詳述されている。

本認証報告書は、本TOEに対して適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

1.1.1 評価保証レベル

本TOEが適合を主張する評価保証レベルは、EAL2適合である。

1.1.2 PP適合

適合するPPはない。

1.2 評価製品

1.2.1 製品名称

本TOEは、以下の製品のセキュリティ機能である。

製品名称：　SafetyDomain
バージョン：　V04L01
開発者：　富士通株式会社

1.2.2 製品概要

SafetyDomain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、ID及びパスワードが格納されたICカードを基にした入力に変更する機能を提供するクライアント端末用のソフトウェア製品である。

従来のWindowsの識別認証はID及び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者に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。

SafetyDomainでは、ID及びパスワードを各利用者のICカードに格納し、各利用者のICカードから、Windowsへログオンするための ID及びパスワードを受け渡すことにより、IDやパスワードの管理の煩雑性を解消している。

また、SafetyDomainでは、同様にアプリケーション（指定された認証方式を持つもののみ）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。

SafetyDomainは、IDやパスワードの管理の不十分さ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を保護することを目的としている。

SafetyDomainは、上記主目的を達成するための認証機能、及びICカード管理機能以外に、シングルサインオン機能、環境設定ファイルの編集機能、パスワード自動生成機能、ネットワーク接続監視機能（ICカード失効情報ファイルを確認し、失効カードの場合はログオフさせる機能）、一時ログオン設定機能（一般利用者がICカードを忘れた際に、管理者が通常のWindowsログオンを一時的に許可する機能）、ファイル暗号化機能、認証履歴採取機能（認証や操作時のログを採取する機能）、及び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。TOEのバージョン変更がなされる）を備えている。

1.2.3 TOE範囲とセキュリティ機能

TOEは1.2.2で説明したSafetyDomain全体である。SafetyDomainの主目的を達成するための認証機能（Windowsログオン機能、アプリケーション認証機能）、及びICカード管理機能（管理者向け、利用者向け）を、本評価におけるTOEのセキュリティ機能としている。

1.2.2に記載したSafetyDomainのシングルサインオン機能、環境設定ファイルの編集機能、パスワード自動生成機能、ネットワーク接続監視機能、一時ログオン設定機能、ファイル暗号化機能、認証履歴採取機能、及びシステムメンテナンス機能は、TOEのセキュリティ機能以外の機能である。

なお、上記システムメンテナンス機能は、TOE運用の前提条件として、使用されないことが想定されている（2.1.3　表2-2参照）。

TOEはクライアント端末上にのみ存在するが、TOEの構成を図1-1に示す。

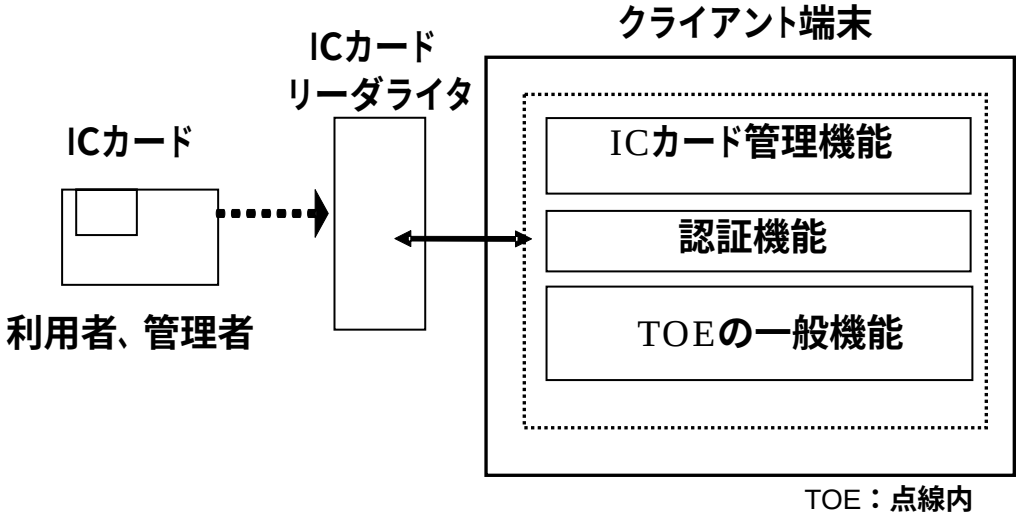

図1-1 TOEの構成図

TOEのセキュリティ機能である認証機能（Windowsログオン機能、アプリケーション認証機能）について、具体的に説明する。

TOEのWindowsログオン機能は、Windowsにログオンしようとする利用者によりTOEに入力されたPINを、当該利用者用のICカード（FeliCaカードの場合とJavaカードの場合の2種がある）に受け渡し、FeliCaカードの場合はTOE、Javaカードの場合はICカード内でPINが正当なものであると確認されると、ICカード内に格納された当該利用者のID、パスワード（Windowsログオンパスワード）、及びドメイン情報を読み取り、Windowsが提供する識別認証機能へ識別認証の依頼を行う。

TOEのアプリケーション認証機能も、上記と同じく、利用者によりTOEに入力されたPINが正当なものであると確認（FeliCaカードの場合はTOE内、Javaカードの場合はICカード内）された後、当該利用者用のICカード内に格納された当該利用者の当該アプリケーション用のID、及びパスワードを読み取り、当該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。

上記のように、一人の利用者が所持している、Windowsログオン用やアプリケーション・ログオン用の複数のIDやパスワードが、一括して当該利用者用のICカード内に格納され、安全に管理されながら、ICカードと連携するTOEが上記ID及びパスワードの受け渡しを仲介し、Windowsやアプリケーションからの識別認証が行われるため、各利用者がIDやパスワードを個別に複数管理していた場合に比べ、不正が起こりにくくなることが想定されている。

次に、TOEのセキュリティ機能であるICカード管理機能（管理者向け、利用者向け）について、具体的に説明する。

TOEのICカード管理機能（管理者向け）は、ICカード内の情報（アカウント管理情報、PINコード管理情報）の設定、変更を管理者に制限する機能、また、TOEのICカード管理機能（利用者向け）は、ICカード内の情報（PIN、パスワード）の変更を利用者本人に制限する機能である。

また、TOEのWindowsログオン機能やアプリケーション認証機能を使用した場合における、Windowsやアプリケーションが提供している通常の識別認証のインタフェースとの関係について説明する。

TOEをインストールし、TOEのWindowsログオン機能を使用した場合、Windowsが提供している識別認証のインタフェースはアクセスできないように隠され、ICカード内の情報を使用するTOEのWindowsログオン機能のインタフェースのみが表示される。そのため、ICカードを使用してのみ、Windowsへのログオンが可能となる（ただし、TOEの一般機能である、ICカードを忘れた際に一時的にログオンを許可する一時ログオン設定機能を使用する場合は、Windowsが提供している識別認証のインタフェースが使用される）。

同様に、TOEのアプリケーション認証機能についても、TOEのアプリケーション認証機能を使用する設定とした場合、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され、ICカードを使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。

なお、TOEのアプリケーション認証機能が対応可能なアプリケーションとしては、TOEがインストールされているクライアント端末に導入される決められた範囲の認証方式（HTMLフォーム認証、BASIC認証、Javaアプレット認証のいずれか）のみを持つものに限られる。

1.3 評価の実施

認証機関が運営するITセキュリティ評価・認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

① 本TOEのセキュリティ設計が適切であること。

② 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。
③ 本TOEがセキュリティ設計に基づいて開発されていること。
④ 上記①、②、③を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「SafetyDomain セキュリティターゲット」（以下「本ST」という。）[1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発･製造･出荷の現場を調査し、本TOEがCCパート1 ([5][8]のいずれか) 附属書A、CCパート2（[6][9]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート3（[7][10]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「SafetyDomain 評価報告書」（以下「評価報告書」という。）[13]に示されている。なお、評価方法は、CEM（[11][12]のいずれか）に準拠する。

1.4 評価の認証

認証機関は、評価機関が作成した、評価報告書、所見報告書、及び関連する評価証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。評価は、平成20年10月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 TOE概要

2.1 セキュリティ課題と前提

TOEが解決すべき課題と、必要とする前提を以下に示す。

2.1.1 脅威

本TOEは、表2-1に示す脅威を想定し、これに対抗する機能を備える。

表2-1 想定する脅威

識別子	脅 威
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。

2.1.2 組織のセキュリティ方針

本TOEの利用に当たって要求される組織のセキュリティ方針は存在しない。

2.1.3 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表2-2に示す。

これらの前提条件が満たされない場合、本TOEのセキュリティ機能が有効に動作することは保証されない。

表2-2 TOE使用の前提条件

識別子	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)	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)	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。

2.1.4 製品添付ドキュメント

本TOEに添付されるドキュメントの識別を以下に示す。読者は、上記表2-2の内容、及び上記表2-2には記載されていない注意喚起事項を実施するために、下記ドキュメントの十分な理解と遵守が要求される。

・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

2.1.5 構成条件

本TOEは、SafetyDomainである。本評価は以下のハードウェア及びソフトウェア上での動作を対象とする。なお、本構成に示されるハードウェア及びソフトウェ

アの信頼性は本評価の範囲外である。

（1）TOEの動作に必要なハードウェア

TOEの動作に必要なハードウェアを、表2-3に示す。

表2-3 TOEの動作に必要なハードウェア

項目	要件(Windows XP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)	

※ 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。FeliCaカードには、PaSoRiが対応する。

（2）TOEの動作に必要なソフトウェア

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を表2-4に示す。

表2-4 TOEの動作に必要なソフトウェア

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	

また、TOEのアプリケーション認証機能が対応するアプリケーションは、以下のいずれかの認証方式を持つアプリケーションのみである。

・HTMLフォーム認証
・BASIC認証
・Javaアプレット認証

また、TOEの運用環境に必要な認証サーバ（認証情報を一元管理するためのサーバ）に導入するソフトウェアを、表2-5に示す。

表2-5 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
	ActiveDirectory	

2.2 セキュリティ対策

TOEは、2.1.1の脅威に対抗するために以下のセキュリティ機能（認証機能、ICカード管理機能）を具備する。

TOEでは、2.1.1の脅威に対抗するために、一人の利用者が所持している、Windowsログオン用やアプリケーション・ログオン用の複数のIDやパスワードが、一括して当該利用者用のICカード内に格納され、安全に管理されながら、ICカードと連携するTOEが上記ID及びパスワードの受け渡しを仲介し、Windowsやアプリケーションからの識別認証が行われるようにすることにより、各利用者がIDやパスワードを個別に複数管理していた場合に比べ、不正が起こりにくくなることが想定されている。

TOEのセキュリティ機能である認証機能（Windowsログオン機能、アプリケーション認証機能）について説明する。

TOEのWindowsログオン機能は、利用者により入力されたPINが正当なものであると照合、確認（FeliCaカードの場合はTOE内、Javaカードの場合はICカード内）されると、ICカード内に格納された当該利用者のID、パスワード等をWindowsが提供する識別認証機能へ受け渡し、識別認証の依頼を行う（この際、Windowsはバックグラウンドで認証サーバとのやり取りを行い、正当であるかどうかを判断する）。Windowsが正当なものであると判断すると、TOEのWindowsログオン機能はWindowsへのログオンを許可する。

TOEのWindowsログオン機能は、Windowsの起動時以外に、スクリーンセーバのロック時、ICカードの引き抜き時、及びICカードリーダライタの引き抜き時にWindowsのログオン状態が解除された後に、再度ログオンする際に実行される（スクリーンセーバのロック時以外の上記ログオン状態の解除は、TOEのセキュリティ機能である）。

TOEのアプリケーション認証機能も、上記のWindowsログオン機能と同じく、利用者により入力されたPINが正当なものであると照合、確認（FeliCaカードの場合はTOE内、Javaカードの場合はICカード内）されると、ICカード内に格納された当該利用者の当該アプリケーション用のID、及びパスワードを、当該アプリケーションが提供する識別認証機能へ受け渡し、識別認証の依頼を行う。当該アプリケーションが提供する識別認証機能が正当なものであると判断すると、TOEのアプリケーション認証機能は、当該アプリケーションへの認証を許可する。

TOEのアプリケーション認証機能は、TOEの一般機能であるシングルサインオン機能が有効化されていた場合、Windowsにログオン後のアプリケーション利用時に再度PIN入力を要求せずに、自動的に実行される。

次に、TOEのセキュリティ機能であるICカード管理機能（管理者向け、利用者向け）について説明する。

TOEのセキュリティ機能であるICカード管理機能（管理者向け）は、利用者に発行するICカードに対して、各種設定を行い、必要に応じ変更を行うことを管理者のみに制限する機能である。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変更要求等に対応する機能も備え、当該利用者のICカードを受け取った管理者のみが、上記解除や上記変更を行うことができる。

TOEのセキュリティ機能であるICカード管理機能（利用者向け）は、利用者が自身のICカードに設定されているPINまたはパスワードを必要に応じ、旧PINまたは旧パスワードを入力した後にのみ、変更することができる機能である。

3 評価機関による評価実施及び結果

3.1 評価方法

評価は、CCパート3の保証要件について、CEMに規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

3.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成20年2月に始まり、平成20年10月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成20年7月に開発現場へ赴き、記録、現物及びスタッフへのヒアリングにより、配付の各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成20年5月から平成20年8月に評価機関において、開発者テストと同等なテスト環境（開発者から一部借用、一部は評価機関で準備）を構築し、開発者が実施したテストのサンプリングチェック及び評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

3.3 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評定に基づく侵入テストを実行した。

3.3.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価した開発者テストの概要を以下に示す。

1) 開発者テスト環境

開発者が実施したテストの構成を図3-1に示す。開発者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

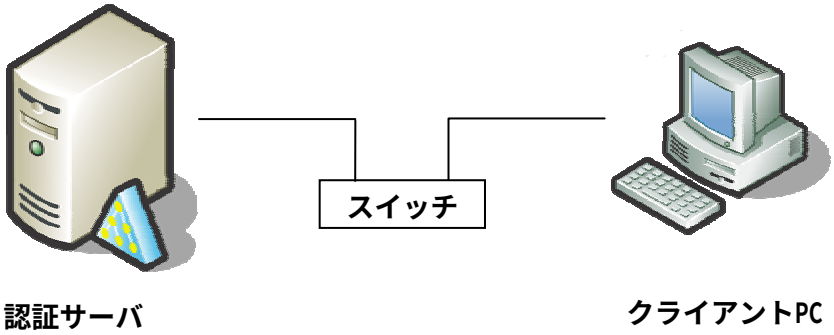

図3-1　開発者テストの構成

なお、開発者テストのクライアントPCにおけるソフトウェア構成、ハードウェア構成を表3-1に示す。

表3-1　開発者テストのソフトウェア構成、ハードウェア構成

環境識別 No.	IC カードタイプ	OS タイプ	R/W
1	FeliCa 版	Windows XP Professional SP2	ソニー　PaSoRi
2	FeliCa 版	Windows Vista Enterprise SP1	ソニー　PaSoRi
3	Java 版	Windows XP Professional SP2	富士通スマートアクセス
4	Java版	Windows XP Professional SP2	ノート PC 内蔵型(PCMCIA)IC カードリーダライタ（O2Micro SmartCardBus Reader）
5	Java版	Windows XP Professional SP2	デスクトップ PC 内蔵型 IC カードリーダライタ（Panasonic PanaSCR7A Smart）
6	Java 版	Windows Vista Enterprise SP1	富士通スマートアクセス
7	Java 版	Windows Vista Enterprise SP1	ノート PC 内蔵型(PCMCIA)IC カードリーダライタ（O2Micro SmartCardBus Reader）
8	Java 版	Windows Vista Enterprise SP1	デスクトップ PC 内蔵型 IC カードリーダライタ（Panasonic PanaSCR7A Smart）

上記以外に、図3-1の認証サーバには、STで想定しているTOE運用のためのドメイン運用環境を構築するため、Active Directory、及びWindows Server 2003 SP2がインストールされている。

2) 開発者テスト概説

開発者の実施したテストは以下のとおり。

a. テスト概要

開発者テストで実施されたテストの概要は以下のとおり。

（1）TOE の TSFI は、「対話画面インタフェース」と「Windows OS とのインタフェース(API)」の 2 種類に分類できる。テスト手法としては、「対話画面インタフェース」GUI に対しては、自動 GUI テストツール等は利用せず、テスト担当者が実際に対話操作を行う方法を採用した。「Windows OS とのインタフェース(API)」については、通常の環境で直接当該インタフェースのみを確認するためのテストを実施することは困難であるため、TOE の通常の利用方法、「対話画面インタフェース」の確認テストに伴って、内部で利用されることを間接的に確認する程度のテストで妥当とした。

（2）開発者テストの環境構成は IC カードタイプ、OS タイプ、リーダライタ(R/W)で分類することができ、TOE に対する開発者テストは表 3-1 に示す 8 種類の環境で実施された。開発者は、TOE の 4 つのセキュリティ機能（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））をサンプリングせずに、全ての機能を表 3-1 に示す各環境でテストした。すべての TSFI（画面インタフェース：13、内部インタフェース：4）についてテストした。

b. 実施テストの範囲

テストは開発者によって480項目実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証されている。

c. 結果

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

3.3.2 評価者独立テスト

評価者は、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることの再確認のための独立テストを実施した。評価者が実施した独立テストの概要を以下に示す。

1) 評価者独立テスト環境

評価者が実施したテストの構成は、図3-1に示した開発者テストの構成と同一の構成である。

ただし、STにおいて識別されているTOEが動作するクライアントPCにおけるソフトウェア構成、ハードウェア構成については、表3-1に示された8種類のうち、下記の表3-2に示した中から4～6種類をサンプリングして評価者テストが実施された（開発者テストのサンプリングテストは6種類全てで、評価者が独自に考案したテストは表3-2の上位4種類で、実施された）。

開発者テストは表3-1に示された8種類全てのテスト環境で実施され、ICカードリーダライタの差異は、TOEの動作に全く影響しないと開発者テスト結果から判断されたため、複数あるJava版のリーダライタについてはサンプリングして、評価者テストが実施された。

表3-2　評価者テストのソフトウェア構成、ハードウェア構成

IC カードタイプ	OS タイプ	R/W
FeliCa 版	Windows XP Professional SP2	ソニー　PaSoRi
FeliCa 版	Windows Vista Enterprise SP1	ソニー　PaSoRi
Java 版	Windows XP Professional SP2	富士通スマートアクセス
Java 版	Windows Vista Enterprise SP1	富士通スマートアクセス
Java 版	Windows Vista Enterprise SP1	ノート PC 内蔵型(PCMCIA)IC カードリーダライタ（O2Micro SmartCardBus Reader）
Java 版	Windows Vista Enterprise SP1	デスクトップ PC 内蔵型 IC カードリーダライタ（Panasonic PanaSCR7A Smart）

2) 評価者独立テスト概説

評価者の実施した独立テストは以下のとおり。

a.　独立テストの観点

評価者は、開発者テスト及び提供された評価証拠資料から、以下の観点での独立テストを考案した。

（1）開発者テストのサンプリングという観点では、開発者テストが実施された8種類の環境に対して、6種類の環境をサンプリングした上で、各環境で行われた開発者テスト項目自体はサンプリングせず、各環境とも全項目をテストした。

（2）TSFIの数は少なく、サンプリングテストにより、基本的には全てのTSFIのテストが考慮されていると判断した。ただし、インタフェースを厳密にテストするという観点で、1件（ロック回数の設定値を変更

して正しい動作を確認）を独立テストとして取り上げた。

（3）想定する運用条件に違反した状態（ICカードのアカウント区分（管理者、利用者）等を不適切に設定）でのTOEの挙動を試す観点が開発者テストで考慮されていなかったため、独立テストを行った。

（4）TOEが利用しているWindows日付時刻情報を操作し、TOEの挙動の確認を行う観点が開発者テストで考慮されていなかったため、独立テストを行った。

なお、上記(3)及び(4)は、テスト結果によっては脆弱性評定への入力とすることも意図された。

b. テスト概要

評価者が実施した独立テストの概要は以下のとおり（上記1）a.(1)～(4)に対応させて、(1)～(4）に概要を示す)。

（1）開発者テストの実施された8種類の環境のうちの6種類の環境について、開発者テスト項目を全て（各環境とも全60項目、合計360項目）実施した。

（2）PINのロック回数の設定値に応じて、正しくロックされ、ロック後は認証処理が行われないことを確認。

（3）TOEのタスクトレイメニューは、ICカードのカード種別（管理者、利用者）に応じて管理されるべきメニューを表示することを確認（アクセス制御に利用される属性ではないICカード内のアカウント区分等を操作し、影響を見た)。

（4）一般利用者権限でのWindows日付時刻情報の設定変更の可能性を、Windows XP及びWindows Vistaで確認し、Windows日付時刻情報に依存するTOEの挙動への影響を見た。

c. 結果

実施した評価者独立テストのうち、上記b.(1)～(3)、及び(4)（OSがWindows Vistaの場合）は正しく完了し、TOEの正しいふるまいを確認することができた。評価者はテスト結果は期待されるふるまいと一致していることを確認した。

なお、評価者独立テスト（(4)（OSがWindows XPの場合））に関連した、TOEの一般機能の使用に関わる注意事項を、「5.2　注意事項」に記載した。

3.3.3　評価者侵入テスト

評価者は、評価の過程で示された証拠から、懸念される脆弱性の可能性について必要と思われる侵入テストを考案し実施した。評価者侵入テストの概要を以下に示

す。

1) 評価者侵入テスト概説

評価者の実施した侵入テストは以下のとおり。

a. 懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

評価者は本TOEの特性を考慮し、本TOE運用におけるICカード使用に関わる脆弱性（PIN認証がTOEで実行されるFeliCaカード場合のPINデータの漏えい、アクセス制御が依存するICカードのカード種別（管理者、利用者）の改ざん)、本TOE運用に関わる特定アカウントの不正使用の脆弱性、及びPIN入力に関わる脆弱性（不正試行に成功、バッファ処理の脆弱性）（計5個）を識別した。

b. 実施テストの範囲

評価者は、潜在的な脆弱性が悪用される可能性があるかを決定するため、以下の侵入テストを実施した。

侵入テストは、適宜、プロセス解析用ソフト、及びデバッグ用解析ソフトを使用し、TOEに関わる懸念される脆弱性が悪用可能かどうかを突き止めるために、悪用の可能性を見る処理（FeliCaカード付与者が他人のFeliCaカードを拾った場合のPIN読み出し、ICカードのカード種別書き換え、TOE付属のツールで作成される特定アカウント及びパスワードの読み出し）を試し（計6件)、確認された。左記確認は、デバッグ用解析ソフトで不正可能候補地点を探り、メモリ領域を確認したり、必要に応じ、プロセス解析ソフトで当該地点に関係するプロセス一覧を確認したりし、行われた。

なお、PIN入力に関わる脆弱性（不正試行に成功、バッファ処理の脆弱性）は、PIN桁数からの論理的分析による妥当性、及び他のテスト（開発者テスト、及びサンプリングテスト）で既に実施されていることが確認された。

c. 結果

実施した評価者侵入テストのうち、ICカード使用に関わる想定した脆弱性については、想定する攻撃能力を超える潜在的な脆弱性は確認されなかった。

3.4 評価結果

3.4.1 評価結果

評価報告書をもって、評価者は本TOEがCEMのワークユニットすべてを満たしていると判断した。

3.4.2 評価者コメント/勧告

特になし。

4 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 所見報告書でなされた指摘内容が妥当であること。
② 所見報告書でなされた指摘内容が正しく反映されていること。
③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。
④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。
⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。

認証機関は、本ST及び評価報告書において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を発行した。

5 結論

5.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL2に対する保証要件を満たすものと判断する。

5.2 注意事項

本評価の認証作業を通じて、消費者に注意を喚起すべきと判断した、本TOE運用における本TOEの一般機能の使用に関わる注意事項を以下に述べる。

（1）Windows XPの日付時刻情報の操作可能性に関連する注意

TOEの一般機能である「① ICカードの失効を管理する機能」、及び「② ICカードを忘れた際に、(通常のWindowsの識別認証機能により）一時ログオンを許可する機能」は、Windowsの日付時刻情報に基づき動作している。

Windows XPの場合（Windows Vistaの場合は非該当)、一般利用者権限（制限付きユーザ）による日付時刻情報の操作が可能であり、左記操作が行われた場合、上記2機能は意図されたとおりに機能しないことが想定される。

①に関しては、クライアントPCとWindowsドメインが時刻同期を取るようにガイダンスで注意喚起がなされているため、上記の一般利用者による日付時刻情報の操作の影響は、極小化されると判断される。

ただし、この極小化された影響でも問題があると判断した場合は、管理者は、失効情報管理ファイルに失効情報を設定することにより当該ICカードの失効施行を行わせるだけではなく、当該失効カードをすばやく直接回収することが望ましいと判断される。

②に関しては、STの前提条件（表2-2記載のA.ONE_TIME(一時ログオン設定機能の使用)）に、一時ログオン設定機能使用に関する管理者の対応が明記され、ガイダンスでも注意喚起がなされている。そのため、安全性が確保されると判断される。

ただし、本TOEはWindowsドメイン運用が想定されており、莫大な人数の一般利用者を管理者が管理する必要がある場合も想定され、適宜管理者等を増やすなどの適切な対応が必要であると判断される。

（2）ネットワーク切断時のICカード失効管理機能に関する注意

TOEの一般機能であるICカードの失効を管理する機能は、ネットワーク切断（利用者クライアントのLANケーブルが外れた場合等）があった場合、認証サーバにある失効情報管理ファイルでの失効確認が行われずエラーにはなるが、利用者の利便性を考慮し、その後PIN認証を実行可能とし、利用者クライアントでローカルにはログオンできるTOE仕様となっている。

ただし、クライアントPCにローカルにログオンしている状態で、ネットワーク接続がなされた場合には、上記失効管理機能が直ちに動作し、ICカードが失効していた場合には、当該利用者は強制的にログオフされるTOE仕様となっている。

そのため、ガイダンス上で上記失効管理機能が正常に動作するためには、ネットワークに接続されている必要があることが注意喚起されている。

上記のように、ネットワーク切断による影響は、利用者クライアントでのローカルなログオンに極小化されてはいるが、この極小化された影響でも問題があると判断される場合は、管理者は、失効情報管理ファイルをクライアント端末に配置することが望ましいと判断される。

6 用語

本報告書で使用されたCCに関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation(セキュリティ評価基準)
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用されたTOEに関する略語を以下に示す。

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。

本報告書で使用された用語の定義を以下に示す（順不同。左記用語を理解するための関連用語を含む）。

環境設定ファイル	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
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

7 参照

[1] SafetyDomain セキュリティターゲット バージョン 1.18 2008年10月16日 富士通株式会社

[2] ITセキュリティ評価及び認証制度の基本規程 平成19年5月 独立行政法人 情報処理推進機構 CCS-01

[3] ITセキュリティ認証申請手続等に関する規程 平成19年5月 独立行政法人 情報処理推進機構 CCM-02

[4] ITセキュリティ評価機関承認申請手続等に関する規程 平成19年5月 独立行政法人 情報処理推進機構 CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 1 September 2006 CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 2 September 2007 CCMB-2007-09-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 2 September 2007 CCMB-2007-09-003

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル バージョン3.1 改訂第1版 2006年9月 CCMB-2006-09-001 (平成19年3月翻訳第1.2版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能コンポーネント バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-002 (平成20年3月翻訳第2.0版)

[10] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証コンポーネント バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-003 (平成20年3月翻訳第2.0版)

[11] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 3.1 Revision 2 September 2007 CCMB-2007-09-004

[12] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-04 (平成20年3月翻訳第2.0版)

[13] SafetyDomain 評価報告書 07003809-01-R003-04 2008年10月20日 みずほ情報総研株式会社 情報セキュリティ評価室