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19年10月16日 (IT認証7176)
認証番号	C0173
認証申請者	日本電気株式会社
TOEの名称	InfoCage PCセキュリティ
TOEのバージョン	1.22
PP適合	なし
適合する保証パッケージ	EAL1及び追加の保証コンポーネントASE_OBJ.2、ASE_REQ.2、ASE_SPD.1
開発者	日本電気株式会社 NECシステムテクノロジー株式会社
評価機関の名称	有限責任中間法人　ITセキュリティセンター　評価部

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7月31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1版（翻訳第1.2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1版 （翻訳第1.2版）

評価結果：合格

「InfoCage PCセキュリティ」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、「InfoCage PCセキュリティ」（以下「本TOE」という。）について有限責任中間法人　ITセキュリティセンター　評価部（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日本電気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や本TOEに添付されるマニュアル（詳細は「1.5.8 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

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

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称：　InfoCage PCセキュリティ
バージョン：　1.22
開発者：　日本電気株式会社
　　NECシステムテクノロジー株式会社

1.2.2 製品概要

本製品は、管理者が定義する「ポリシー情報」に基づき、PCからの情報漏洩を防止するためのセキュリティ機能を提供するソフトウェア製品である。提供されるセキュリティ機能概要は以下の通りである。

表1-1　TOEのセキュリティ機能

セキュリティ機能	概要
識別認証機能	・利用者を識別認証する(※)
PC制御機能	・I/Oポート、及びプリンタの利用可否を制御する

セキュリティ機能	概要
	・許可外部メディアへのファイル出力を制御する
暗号機能	・ドライブ単位の暗号化/復号を行う ・ファイル単位の暗号化/復号を行う ・許可外部メディアへのファイル出力時に暗号化を行う ・操作ログをリムーバブルメディアへエクスポート/インポートする時に暗号化/復号を行う
監査機能	・操作ログを生成し、ログサーバに転送する ・ログサーバに蓄積された操作ログの閲覧、検索を行う ・操作ログをリムーバブルメディアへエクスポート、リムーバブルメディアから操作ログのインポートを行う
ポリシー設定機能	・ポリシー情報の作成、適用、変更を行う

※認証方式は、パスワードによる認証方式を対象とする。

TOEは、一般利用者が使用する「クライアント」、管理者が使用する「管理者端末」、及びPCの操作ログが蓄積される「ログサーバ」にインストールされ、使用される。

1.2.3 TOEの範囲と動作概要

本TOEは以下の3つのコンポーネントから構成される。

表1-2 TOEのソフトウェアコンポーネント

機器名	ソフトウェアコンポーネント名
ログサーバ	InfoCage PCセキュリティ Ver.1.22 サーバソフトウェア ※ InfoCage PC セキュリティ Ver.1.22 サーバソフトウェアは、以下のモジュールで構成されている ・InfoCage 簡易ログサーバ：バージョン1.22.2525
管理者端末	InfoCage PCセキュリティ Ver.1.22 管理者端末ソフトウェア(注) ※ InfoCage PC セキュリティ Ver.1.22 管理端末ソフトウェアは、以下のモジュールで構成されている ・InfoCage PCセキュリティ(管理者ツール)：バージョン1.2.2.3 上記以外のモジュールは、クライアントの項を参照のこと
クライアント	InfoCage PCセキュリティ Ver.1.22 クライアントソフトウェア ※ InfoCage PC セキュリティ Ver1.22 クライアントソフ

機器名	ソフトウェアコンポーネント名
	トウェアは、以下のモジュールで構成されている ・InfoCage PCセキュリティ：バージョン1.2.2.3 ・InfoCage ファイル暗号：バージョン2.00.0030 ・InfoCage モバイル防御：バージョン4.21.4000.0003 (OSがMicrosoft Windows XP Professional 日本語版（SP2）の場合) ・InfoCage モバイル防御：バージョン4.22.4000.0001 (OSがMicrosoft Windows Vista Ultimate 日本語版の場合)

注：InfoCage PCセキュリティ Ver.1.22 管理者端末ソフトウェアには、ポリシー作成ツール、クライアントセットアップ作成ツール、InfoCage PCセキュリティ Ver1.22 クライアントソフトウェアが含まれる。

これらのTOEコンポーネントを明示したTOEの物理的範囲を図1-1に示す。赤色破線部分がTOEを表す。

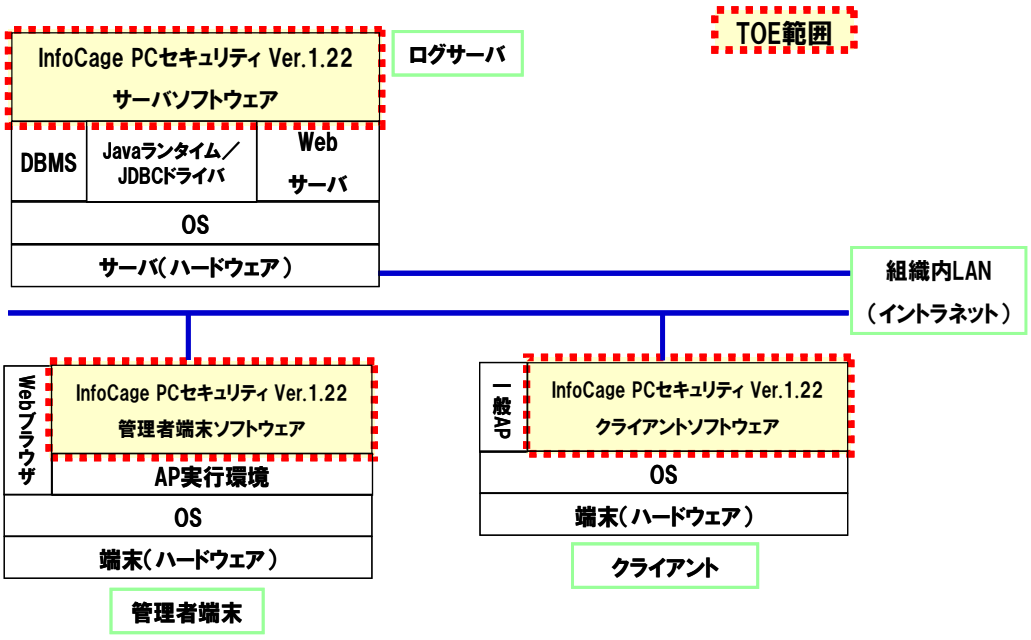

図1-1　TOEの物理的範囲

上図各種コンポーネントに関する役割を以下に示す。

(1)　組織内LAN

組織内の機器を接続するイントラネットであり、ログサーバ、管理者端末及びクライアントは、通常このLANに接続され運用される。

(2) ログサーバ

ログサーバは、組織内LANに接続され、管理者に使用される。ログサーバには、管理者端末、及びクライアントから転送された操作ログが蓄積される。また、組織内LANを介しての管理者端末からの要求に応じて蓄積した操作ログを閲覧、及び検索することができる。

(3) クライアント

クライアントは、組織内LANに接続され、管理者、又は一般利用者に使用される。管理者がクライアントを利用する場合は、一般利用者とは異なる権限での操作が行える。また、クライアントは一時的に組織の建物外へ持ち出されることも考えられるが、その際は組織内LANには接続されない。クライアントで生成された操作ログは、組織内LANを介してログサーバに転送される。

(4) 管理者端末

管理者端末は、組織内LANに接続され、管理者に使用される。管理者端末で生成された操作ログは、組織内LANを介してログサーバに転送される。また、管理者端末から組織内LANを介して、ログサーバに蓄積された操作ログを閲覧、及び検索する要求をログサーバに出すことができる。

1.2.4 TOEの機能

本TOEは「1.2.2 製品概要」に記載したように、PCからの情報漏洩を防止するためのセキュリティ機能を提供するソフトウェアであり、本質的に主たる機能がセキュリティ機能であるセキュリティ製品である。

本認証におけるTOEの評価範囲として、「1.2.2 製品概要」に示された下記のセキュリティ機能が定義されている。各機能の詳細は「1.5.3 セキュリティ機能」に記す。

(1) 識別認証機能
(2) PC制御機能
(3) 暗号機能
(4) 監査機能
(5) ポリシー設定機能

上記以外のTOEの機能としては、プログラムの起動抑止（特定プログラムの起動抑止）、環境の固定支援（一部PCの管理機能（「ネットワーク接続」等）を隠す）等がある。

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「InfoCage PCセキュリティ Ver.1.22 セキュリティターゲット」（以下「ST」という。）[1] 及び本TOE開発に関連する評価用提供物件を調査し、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、「InfoCage PC セキュリティ V1.22 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7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。

1.5 報告概要

1.5.1 PP適合

適合するPPはない。

1.5.2 EAL

STが規定するTOEの評価保証レベルはEAL1拡張であり、追加の保証コンポーネントはASE_OBJ.2、ASE_REQ.2、及びASE_SPD.1である。

1.5.3 セキュリティ機能

本TOEのセキュリティ機能の詳細は以下のとおりである。なお、ログサーバ、及び管理者端末においては、Administrator権限で運用するが、クライアントの通常利用においては、Administrator権限以外の任意のOSのユーザ権限で運用するものとする。

(1)識別認証機能

本機能は、一般利用者がクライアントを、管理者が管理者端末、又はクライアントを利用する前に識別認証（InfoCage 認証）を行い、一定時間管理者端末、又はクライアントの操作が行われない時に再認証を行う機能を提供する。機能の詳細を以下に示す。

＜管理者端末＞
・管理者が管理者端末にログオンする際の識別認証（InfoCage認証）
・管理者のInfoCageパスワードの変更
・ログオン後、一定時間管理者からアクセスがない場合の再認証
＜クライアント＞
・一般利用者、又は管理者がクライアントにログオンする際の識別認証（InfoCage認証）
・一般利用者、又は管理者のInfoCageパスワードの変更
・ログオン後、一定時間一般利用者、又は管理者からアクセスがない場合の再認証

(2)PC制御機能

本機能は、管理者端末、又はクライアントに適用されたポリシー情報に基づき、PCの動作を制御する機能を提供する。機能の詳細を以下に示す。

＜管理者端末・クライアント共通＞
・ポリシー情報に基づく以下の制御を行うように設定
－制御対象I/Oポート、及びリムーバブルメディアへのデータ出力を制御するように設定
－プリンタへの出力を制御するように設定

(3)暗号機能

本機能は、暗号鍵ファイルの生成、及びファイルの暗号化/復号を行う機能を提供する。機能の詳細を以下に示す。

＜管理者端末・クライアント共通＞

・TOE導入時の内蔵HDDをドライブ単位で暗号化
　－TOEのインストール時にドライブ単位で暗号化を行う。HDDからファイルの読み込みを行う際に自動的に復号を行い、HDDへファイルの書き込みを行う際に自動的に暗号化を行うので、利用者は暗号化/復号を意識することなく管理者端末、クライアントを使用することができる。
・ファイルの暗号化／復号
　－利用者が指定したファイルの暗号化を行い、利用者が指定したタイミングで復号を行うので、ドライブ単位での暗号化のようにファイルを読み込む際に自動的に復号されることはない。
・許可外部メディアにファイルを出力する際の自動暗号化
　－利用者がファイルを許可外部メディアに出力する際に自動的にファイルの暗号化を行い、許可外部メディアからファイルを読み込む際に自動的にファイルの復号を行う。
・管理者端末、又はクライアントにおいてファイルを暗号化／復号する際に用いる、暗号鍵ファイルの生成、配付（※）
　　※暗号鍵ファイルの生成、配付の機能の利用可否については、管理者によって指定された役割によって決められる。
・ファイルを暗号化／復号する際に用いる暗号鍵ファイルのインポート

(4)監査機能

本機能は、監査対象事象を操作ログとして取得し、ログサーバに転送した操作ログを検索、閲覧する機能を提供する。管理者は操作ログを参照することにより、第三者による不正アクセス等の試み（ログイン失敗等）等を検出し、適切な対処を実施することが可能となる。機能の詳細を以下に示す。

＜ログサーバ＞

・管理者端末からの要求に応じて、ログサーバのDBに蓄積された操作ログの閲覧、検索を実行

＜管理者端末・クライアント共通＞

・管理者端末、又はクライアントの操作ログの生成、及びログサーバへの送信
・ログサーバへ操作ログを送信する際の転送保護
・クライアントからリムーバブルメディアへエクスポートされた操作ログのインポート

＜管理者端末＞

・ログサーバへ操作ログの閲覧、検索要求を発行

＜クライアント＞

・一時ログフォルダ内の操作ログをリムーバブルメディアへエクスポート

(5)ポリシー設定機能

本機能は、ポリシーの作成、変更、適用、及び参照の機能を提供する。機能の詳細を以下に示す。

＜管理者端末＞

・ポリシー情報の作成、変更

＜管理者端末・クライアント共通＞

・ポリシー情報の適用、参照

なお上記のTOEのセキュリティ機能は、以下に示すセキュリティ機能要件を実現している。

・セキュリティ監査
・暗号化機能
・アクセス制御
・送出・入力データ保護
・識別認証
・セキュリティ管理
・セキュリティ機能保護

1.5.4 脅威

本TOEは、表1-3に示す脅威を想定し、これに対抗する機能を備える。

表1-3 想定する脅威

識別子	脅 威
T.01（不正なログオン）	第三者が、正当な利用者になりすましてTOEに不正にログオンし、保護対象データを詐取、暴露するかもしれない。
T.02（許可されていないプリンタへの出力）	一般利用者が、許可されていないプリンタに保護対象データを出力することにより、出力された保護対象データが第三者に窃取され、暴露されるかもしれない。
T.03（クライアントの盗難、紛失）	第三者にクライアントを盗難され、又は一般利用者が紛失したクライアントを第三者が入手し、当該クライアントに保存された保護対象データを暴露するかもしれない。
T.04（外部メディアの盗難、紛失）	第三者に外部メディアを盗難され、又は一般利用者が紛失した外部メディアを第三者が入手し、当該外部メディアに保存された保護対象データを暴露するかもしれない。

本TOEは外部メディア・クライアントやプリンタ経由での情報漏洩防止機能を提供するものであり、それ以外の経路での情報漏洩（例えばメール誤送信等）には対応していない。従ってそれらに対する脅威はSTに記載されていない。

なお、本TOE利用環境において一般利用者は自らが所属する組織の情報を積極的に暴露することはないと想定する。しかしながら情報セキュリティに関する脅威への認識が十分でないために許可されない操作を実行する可能性があるため、脅威エージェントとして含めるものとする。

1.5.5 組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針はない。

1.5.6 構成条件

本TOEの動作に必要なハードウェアを表1-４に示す。

表1-4　TOEが動作するハードウェア

端末名	種別	説明
ログサーバ	CPU	3.0GHz 以上のx86互換アーキテクチャのCPU
	メモリ	1.0GB以上
	HDD	340MB以上の空き容量 （追加で操作ログの量に応じた空き容量が必要）
管理者端末	CPU	1.0GHz 以上のx86互換アーキテクチャのCPU
	メモリ	１GB以上(OSがWindows Vistaの場合)
		512MB以上(OSがWindows XPの場合)
	HDD	システムドライブに800MB以上の空き容量 (OSがWindows Vistaの場合)
		システムドライブに500MB以上の空き容量 (OSがWindows XPの場合)
クライアント	CPU	1.0GHz 以上のx86互換アーキテクチャのCPU
	メモリ	１GB以上(OSがWindows Vistaの場合)
		512MB以上(OSがWindows XPの場合)
	HDD	システムドライブに800MB以上の空き容量 (OSがWindows Vistaの場合)
		システムドライブに500MB以上の空き容量 (OSがWindows XPの場合)

また、本TOEの動作に必要なソフトウェアを表1-5に示す。

表1-5　TOEが動作するソフトウェア

端末名	種別	製品名
ログサーバ	OS	Microsoft Windows Server 2003 R2 Enterprise Edition 日本語版（SP2）
	DBMS	Microsoft SQL Server 2005 日本語版（SP2）
	Web サーバ	Apache Tomcat 6.0
		Apache Axis 1.4
	Java ランタイム	J2SE Runtime Environment 5.0 Update 13
	JDBC ドライバ	Microsoft SQL Server 2005 JDBC Driver Ver.1.1

端末名	種別	製品名
管理者端末	OS(※)	Microsoft Windows Vista Ultimate 日本語版 又はMicrosoft Windows XP Professional 日本語版（SP2）
	Web ブラウザ	Microsoft Internet Explorer 6.0(SP2) 又はMicrosoft Internet Explorer 7.0
	AP実行環境	(OSがMicrosoft Windows XP Professional 日本語版（SP2）の場合) Microsoft .NET Framework 2.0 Microsoft .NET Framework 2.0 日本語Language Pack
		(OSがMicrosoft Windows Vista Ultimate 日本語版の場合) Microsoft .NET Framework 3.0 Microsoft .NET Framework 3.0 日本語Language Pack
クライアント	OS(※)	Microsoft Windows Vista Ultimate 日本語版 又はMicrosoft Windows XP Professional 日本語版（SP2）

※32bit版のOSのみをサポートする。

1.5.7 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表1-6に示す。

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

表1-6 TOE使用の前提条件

識別子	前提条件
A.01（セキュアルームへの機器設置）	ログサーバ、及び管理者端末は、管理者のみが入室できる室内（セキュアルーム）に設置される。
A.02（ログサーバの管理）	管理者以外は、ログサーバのOS、及びDBMSへログオンすることができない。また、管理者は定期的にログサーバ上に保存された操作ログのバックアップを取得し、ログサーバ上のディスクに十分な空き容量を確保する。
A.03（管理者の管理）	管理者は信頼できる者であり、不正な操作を行わない。また、管理者から一般利用者へのInfoCageユーザIDやInfoCageパスワードの通知、及びファイル(クライアン

	トセットアップ、ポリシー情報、ファイル暗号用共通鍵、及び暗号鍵入力制御情報)の配付については、管理者に許可された利用者のみが認識または入手できる、安全な方法で行う。また、管理者は、通知したInfoCageユーザID、InfoCageパスワード、及び配付したファイルを確実にクライアントに設定するように、利用者に対して指導する。また、ファイル暗号用共通鍵、及び暗号鍵入力制御情報を配付する権限を一般利用者に与えた場合、管理者は、配付の権限を持った一般利用者が権限を持たない一般利用者へファイル暗号用共通鍵、及び暗号鍵入力制御情報を、安全な方法で配付するように指導する。
A.04（パスワードの管理）	利用者は、TOEにアクセスするためのパスワードを他人に知られないよう管理する。また、利用者は、推測されにくいパスワードを設定し、適切な頻度で変更する。また、管理者は、上記に示したパスワードの管理を実施できるように、利用者に対して指導する。
A.05（操作ログをエクスポートしたリムーバブルメディアの管理）	スタンドアロンでクライアントを利用する利用者は、クライアント内の操作ログをエクスポートしたリムーバブルメディアを、同一組織内の利用者に渡す。外部メディアを受け取った利用者は、リムーバブルメディアからログをインポートし、操作ログをログサーバへ確実に転送する。また、管理者は、上記に示したようにスタンドアロンで利用しているクライアントのログが確実にログサーバに転送されるように、利用者に対して指導する。
A.06（不正ソフトウェア対策）	利用者は、ログサーバ、管理者端末、及びクライアントには、ウイルス対策ソフトウェアを導入するとともに、常に最新のウイルス対策ソフトウェアのパターンファイルや、OSのセキュリティ対策用修正ソフトウェアを適用する。

1.5.8 製品添付ドキュメント

本TOEに添付されるドキュメントを表1-7に示す。

表1-7　TOEのガイダンス文書

種類	ガイダンス文書名
インストールガイダンス	InfoCage PCセキュリティ Ver.1.22 インストールガイド(0122S06)
利用者操作ガイダンス	InfoCage PCセキュリティ Ver.1.22 管理者ガイド(0122K06)
	InfoCage PCセキュリティ Ver.1.22 ユーザーズガイド(0122U06)

2 評価機関による評価実施及び結果

2.1 評価方法

評価は、CCパート3の保証要件について、CEM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。

2.2 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19年10月に始まり、平成20年7月の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4月に開発者サイトで評価者テスト（評価者独立テストと侵入テスト）を実施した。

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

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

2.3 製品テスト

評価者の実施した評価者テストの概要を以下に示す。

2.3.1 評価者テスト

1) 評価者テスト環境

評価者が実施したテストの構成を図2-1に示す。

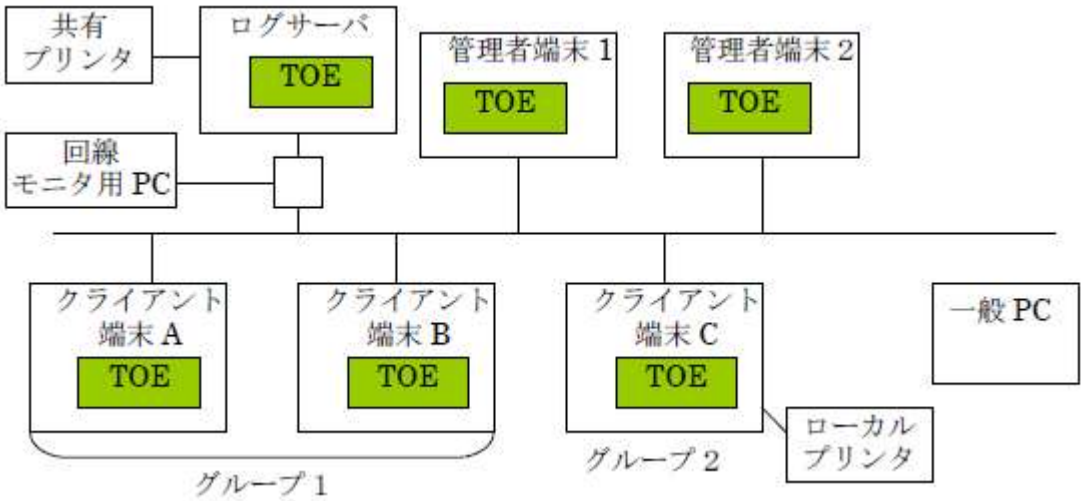

図2-1　評価者テストの構成図

上図のように管理者端末、クライアント端末を複数セットアップし、STで記載された稼働環境をカバーしている。

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

評価者が実施したテストの構成に関しては、上記「1) 評価者テスト環境」を参照の事。評価者テストは、STにおいて識別されているTOEバージョン、及びTOE動作環境（「1.5.6 構成要件」参照）と同一、TOE運用構成と同等であるTOEテスト環境で実施されている。

b.テスト手法

TOEの外部インタフェース（ポリシー設定ツール等）から操作を行い、各操作に対応するTSFIを通じて、TSFのふるまいを確認している。

c.実施テストの範囲

外部仕様に規定されたTSFI（43インタフェース）全てをテストし、そのテスト項目数は計85個ある。クライアント端末、管理者端末では2つのOSが特定されているので、それぞれのOS環境で同じテストが実施されている。また、評価者独立テスト項目の選択基準として、下記を考慮している。

① テストするインタフェースのサブセット選択の考慮

機能仕様書でTSFIとして挙げられたものをすべてテスト対象とする。

② サブセットを構成するインタフェース選択の考慮

a) インタフェースの重要性

本TOEの主要なセキュリティ機能は暗号機能であり、機能要件 FCS_CKM.1, FCS_COP.1 に多くのインタフェースが対応する。それらのインタフェースをテストサブセットに含める。

b) インタフェースの複雑性

暗号化にはファイル暗号化、ドライブ暗号化、許可外部メディアへの出力時の暗号化があり、それらが単独で有効になっている場合、複数が有効になっている場合にケース分けしてテストする。

③ 暗黙のテスト

監査データの生成機能は、他のセキュリティ機能のテストにおいて、動作する機能である。監査データの生成機能のテストは、他のセキュリティ機能のテストと同時に並行して行う。

④ インタフェースタイプ

各TSFIのインタフェース種別には、GUIとGUI以外のTSFIがあると機能仕様に明示されており、GUI以外のインタフェースとして、管理者端末、クライアント用に(1)ファイルシステム、レジストリへのアクセス（ポート制御、プリンタ追加制御、ログ生成が関係）のためのOSからの呼出しインタフェース、(2)ログサーバ用にログ閲覧のインタフェース（通信プロトコル）がある。OSからの呼び出しインタフェースに関してはレジストリ内容を確認する。ログの閲覧インタフェースに関しては、管理者端末からLogViewerをアクセスしてテストする。また、Windowsのセーフモードで動作させる機能があり、これらをテストする。

e) 革新的または一般的でない特徴をもたらすインタフェース

革新的または一般的でない機能は存在しないと考えられるので、本観点によるテストは考慮していない。

また侵入テストについては、本TOEの特性である、操作ミスの可能性のある一般利用者がTOEのインストールされたPCを日常的に使用することや、保護資産が格納されたクライアント端末および許可外部メディアが盗難にあう可能性があることを考慮し、以下の観点に重点を置いて脆弱性のリストアップを行った。

・TOEを長期に渡り使用する一般利用者が、TOEやOSのインタフェース経由でさまざまな設定変更を行うことによりTSFのバイパスが可能な状

況が起こらないか

・TOEがインストールされたクライアント端末や許可外部メディアを、悪意をもつ第三者が入手した際、平文の保護資産にアクセスできてしまう状況が起こらないか

最終的に上記によりリストアップされた脆弱性を基に、24項目の侵入テストを実施した。

d.結果

独立テストに関しては、すべてのテスト結果が、機能仕様に記載された仕様、またはガイダンスに記述されている内容に沿ったものであることから、TOEの仕様が妥当であると判断した。

また、侵入テストに関しては、以下の項目を除き全て悪用不能脆弱性であることを確認した。

・攻撃者がスタンバイモード等のメモリ上に鍵がロードされている状態のクライアントを入手し、DRAMから暗号鍵を抽出することにより、暗号化されたファイルを不正に復号することができる

→攻撃者がメモリ上に鍵がロードされている状態のクライアントを入手することを試みても、クライアントを持ち出す際は、スリープやスタンバイ等の状態は避け、電源を切断することが注意事項としてガイダンスに記載されているため、そのような状態のTOEを攻撃者が入手することは困難であり、入手できたとしても一度攻撃するとメモリ上のデータは消えてしまうため、チャンスは1度のみである。また、攻撃方法としてDRAMを冷却して取り出し、DRAMにデータが残存しているうちにメモリダンプを行うというツールと技術、また、メモリダンプから必要な鍵情報を抽出するための知識が攻撃者に必要となり、[CEM] B.4の「表3 攻撃能力の計算」に従い残存脆弱性と判定される

・攻撃者がInfoCage認証（ロックアウト時以外）、InfoCage認証（ロックアウト時）、LogViewer認証、DBMS認証、ファイル暗号用暗号鍵インポート、許可外部メディア復号化への総当り攻撃を実施する

→いずれも攻撃は現実的な年月（解読には最低30年弱要する）では成功せず、[CEM] B.4 の「表3 攻撃能力の計算」に従い残存脆弱性と判定される

2.4 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 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 当該所見報告書でなされた指摘内容が妥当であること。
② 当該所見報告書でなされた指摘内容が正しく反映されていること。
③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが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、ST及び評価報告書において、所見報告書及び認証レビューで指摘された問題点が解決されていることを確認した。

4 結論

4.1 認証結果

提出された評価報告書、当該所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL1及び追加の保証コンポーネントASE_OBJ.2、ASE_REQ.2、ASE_SPD.1に対する保証要件を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

表4-1 評価者アクションエレメント検証結果

評価者アクションエレメント	検証結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_INT.1.1E	評価はワークユニットに沿って行われ、TOE参照、TOE概要、及びTOE記述が正しく記述されていることを確認している。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、TOE参照、TOE概要、及びTOE記述が相互に一貫していることを確認している。
ASE_CCL.1.1E	評価はワークユニットに沿って行われ、CCの適合主張の有効性を確認している。
ASE_SPD.1.1E	評価はワークユニットに沿って行われ、セキュリティ課題が明確に定義されていることを確認している。
ASE_OBJ.2.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針が明確に定義されていることを確認している。
ASE_ECD.1.1E	評価はワークユニットに沿って行われ、拡張セキュリティ要件が含まれていないため非適用であることを確認している。
ASE_ECD.1.2E	評価はワークユニットに沿って行われ、拡張セキュリティ要件が含まれていないため非適用であることを確認している。
ASE_REQ.2.1E	評価はワークユニットに沿って行われ、SFR、SARは明確に、曖昧さなく十分に定義され、また内部的に一貫していること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていることを確認している。

ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述がどのように各SFRを満たすかを示していることを確認している。
ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述がTOE概要及びTOE記述と一貫していることを確認している。
ライフサイクルサポート	**適切な評価が実施された。**
ALC_CMC.1.1E	評価はワークユニットに沿って行われ、TOEは一意の参照でラベル付けされていることを確認している。
ALC_CMS.1.1E	評価はワークユニットに沿って行われ、TOEの構成リストが管理され、構成要素が一意に識別可能なことを確認している。
開発	**適切な評価が実施された。**
ADV_FSP.1.1E	評価はワークユニットに沿って行われ、SFR実施・SFR支援TSFIの目的と使用方法、パラメタが記載されていることを確認している。
ADV_FSP.1.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。
ガイダンス文書	**適切な評価が実施された。**
AGD_OPE.1.1E	評価はワークユニットに沿って行われ、利用者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しており運用環境のセキュリティ対策方針を満たすために従うべきセキュリティ手段を記述してあることを確認している。
AGD_PRE.1.1E	評価はワークユニットに沿って行われ、準備手続きがTOEのセキュアな準備を記述し、STの運用環境のITセキュリティ方針に従った環境が構築可能であることを確認している。

AGD_PRE.1.2E	評価はワークユニットに沿って行われ、準備手続きを元に評価者がセキュアにTOEと準備環境を構築可能なことを実行し確認している。
テスト	**適切な評価が実施された。**
ATE_IND.1.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、提供されていることを確認している。
ATE_IND.1.2E	評価はワークユニットに沿って行われ、独立テストを実施し、結果が期待されるべき結果と一貫していることを確認している。また、本評価のテスト実施方法も適切と判断される。
脆弱性評定	**適切な評価が実施された**
AVA_VAN.1.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、提供されていることを確認している。
AVA_VAN.1.2E	評価はワークユニットに沿って行われ、潜在的な脆弱性検出のために公知の資料を検査していることを確認している。
AVA_VAN.1.3E	評価はワークユニットに沿って行われ、識別された潜在的脆弱性が基本的な攻撃能力を持つ攻撃者からの攻撃に耐えられることを根拠とともに記述していることを確認している。

4.2 注意事項

特になし。

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

本報告書で使用された用語を以下に示す。

Administrator 権限	Microsoftオペレーティングシステムのユーザ権限の一つで、OSの権限を変更できる権限
InfoCage PC セキュリティ	定義されたポリシー情報を基に識別認証、PC制御、暗号化、及び監査を行い、情報漏えいを防止するソフトウェア製品
InfoCage認証	InfoCage PCセキュリティが導入されたPCを操作可能にする際の識別認証であり、Windows認証の前に行われる
InfoCage ユーザ ID	InfoCage認証で使用されるユーザ識別子（WindowsユーザIDとは異なる）
InfoCage パスワード	InfoCage認証で使用されるパスワード
I/Oポート	デバイスを接続するためPCに備えられた接続コネクタ
LogViewer	ログサーバで動作する、操作ログの閲覧、検索機能
Windows認証	OSであるWindowsへのログオン時に行う識別認証であり、InfoCage認証の後に行われる
Windows ユーザ ID	Windows認証で使用されるユーザ識別子（InfoCageユーザIDとは異なる）
暗号鍵入力制御情報	ファイル暗号用共通鍵をクライアントにインポートするための情報
一時ログフォルダ	クライアントの操作ログが、ログサーバに送信されるまで保管されるフォルダ
一般AP	クライアント上で使用される、TOE以外のAP
イントラネット	インターネットで普及した技術を利用して、特定の組織内に構

	築されたネットワーク
外部メディア	CD、DVDやUSBメモリのように、PC本体内にはない外部の記録媒体
管理者端末	管理者が使用する、InfoCage PCセキュリティ 管理者端末ソフトウェアがインストールされたPC
許可外部メディア	管理者によりクライアント上での使用が許可され、ファイルの入出力時にTOEが自動的に暗号化/復号を行うリムーバブルメディア
クライアント	一般利用者が使用する、InfoCage PCセキュリティ クライアントソフトウェアがインストールされたPC
クライアントセットアップ	管理者端末、又はクライアントにInfoCage PCセキュリティをインストールするためのセットアップ用ファイルであり、管理者がクライアントセットアップ作成ツールで作成する
再認証	TOEにログオンした利用者から一定時間アクセスがない場合に要求されるInfoCage 認証
システムドライブ	OSがインストールされたドライブ
制御対象I/Oポート	TOEで制御することができるI/Oポートであり、USB、シリアル/パラレル、IEEE1394、赤外線、PCMCIAのポートを指す。
操作ログ	一般利用者がクライアント、又は管理者が管理者端末を、いつどのように操作したか記録した電子データ
デバイス	I/Oポートに接続する機器であり、CD/DVDデバイス、FDデバイス、USBデバイス、プリンタ等がある
ファイル暗号用共通鍵	利用者がファイルを暗号化/復号する際に使用する暗号鍵
保護対象データ	クライアント内のHDD等に保持される利用者データ
ポリシー情報	クライアント、及び管理者端末上でInfoCageユーザに適用される制限の定義情報であり、管理者がポリシー作成ツールで作成する
リムーバブルメディア	外部メディアの中でOSがリムーバブルメディアと判断するもの(CD、DVD、FDを除く)
ログサーバ	InfoCage PCセキュリティ サーバソフトウェアがインストールされ、クライアント、及び管理者端末の操作ログが保存されるサーバ
ロックアウト	管理者が設定したロックアウトの閾値を越えてInfoCage 認証に失敗した際のInfoCage 認証を実行できない状態
ロックアウトの閾値	管理者が許容する連続したInfoCage 認証の失敗回数であり、この回数を越えてInfoCage 認証に失敗するとロックアウトされる

6 参照

[1] InfoCage PCセキュリティ Ver.1.22 セキュリティターゲット バージョン 1.12(2008年6月3日) 日本電気株式会社

[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 September 2006 CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version　3.1 September 2006 CCMB-2006-09-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version　3.1 September 2006 CCMB-2006-09-003

[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: セキュリティ機能要件 バージョン3.1 改訂第1版　2006年9月 CCMB-2006-09-002 (平成19年3月翻訳第1.2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: セキュリティ保証要件 バージョン3.1 改訂第1版　2006年9月 CCMB-2006-09-003 (平成19年3月翻訳第1.2版)

[11] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 3.1 September 2006 CCMB-2006-09-004

[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1版 2006年9月 CCMB-2006-09-004 (平成19年3月翻訳第1.2版)

[13] InfoCage PC セキュリティ V1.22 評価報告書 第1.5版 2008年7月15日　有限責任中間法人　ITセキュリティセンター　評価部