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5月27日** (IT**認証**8226)
認証番号	C0193
認証申請者	**日本電気株式会社**
TOE**の名称**	**機能特定**(WebSAM SystemManager)
TOE**のバージョン**	5.2.1
PP**適合**	**なし**
適合する保証パッケージ	EAL1
開発者	**日本電気株式会社**
評価機関の名称	**株式会社電子商取引安全技術研究所　評価センター**

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

「機能特定(WebSAM SystemManager)」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、「機能特定(WebSAM SystemManager)」（以下「本TOE」という。）について、株式会社電子商取引安全技術研究所　評価センター（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、EAL1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：　WebSAM SystemManager
バージョン：　5.2.1
開発者：　日本電気株式会社

1.2.2 製品概要

WebSAM SystemManager は、監視対象サーバの構成情報、障害情報、性能情報を収集し、管理するソフトウェア製品である。マルチベンダ、マルチプラットフォームで構成される情報システムに存在する多種多様なサーバの情報を、GUI で一元的に監視することにより、サーバの管理業務を効率化することを目的とする。

WebSAM SystemManager は、監視対象サーバ上に配置される「WebSAM SystemManager エージェント」、監視サーバ上に配置される「WebSAM

SystemManager マネージャ」、及び監視端末に配置される「WebSAM SystemManager 監視端末」から構成される。監視対象サーバと監視サーバの間、及び監視サーバと監視端末の間は、TCP/IP ネットワークで接続され、1 台の監視サーバに複数台の監視対象サーバや監視端末を接続することが可能である。

監視サーバは、監視対象サーバから送付された構成情報、障害情報、性能情報を蓄積する。WebSAM SystemManager の利用者（各種管理者、オペレータ）は監視端末から、各役割に割り当てられた権限の範囲内で、監視サーバに蓄積された構成情報、障害情報、性能情報にアクセスすることができる。

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 WebSAM SystemManager 全体（WebSAM SystemManager エージェント、WebSAM SystemManager マネージャ、及び WebSAM SystemManager 監視端末）である。

本評価におけるTOEのセキュリティ機能としては、監視端末において正しい利用者（各種管理者、オペレータ）が識別された上で、誤り無く、その役割に付与された権限内で監視サーバ上に蓄積された情報（構成情報、障害情報、性能情報）にアクセスされるように、下記の諸機能を範囲として設定している。

(1) 利用者の識別及び認証を行う識別認証機能

(2) 利用者の役割に付与されている権限に基づき、情報に対するアクセス制限を行うアクセス制御機能

(3) 上記識別認証、及びアクセス制御を行うために必要なユーザ情報、権限情報等の管理を行うユーザ情報管理機能

TOEのセキュリティ機能は、正しい利用者が、付与された権限の範囲内でのみ情報にアクセス（参照、更新、削除）でき、誤使用がないようにすることを狙いとしている。

なお、TOEのアクセス制御機能は、TOEの識別認証機能により正しい利用者が識別認証された後、識別認証機能から当該利用者の権限情報を通知され、当該利用者に付与されている権限内でのみ情報にアクセスできるように、利用者端末のGUI上でアクセス可能な項目（メニュー、ボタン等）のみ有効化し、操作可能とすることを機能範囲としている（利用者による上記操作可能項目の操作を受けて、各情報に直接アクセスする処理を行う機能は、アクセス制御機能の範囲外である）。

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「WebSAM SystemManager Ver5.2.1 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、「WebSAM SystemManager Ver5.2.1 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

本評価はEAL1適合であるため、STにセキュリティ課題定義として、脅威を記述することは要求されない。

ただし、1.2.3に記載したように、本TOEは、正当な利用者（各種管理者、オペレータ）が付与された権限を超えて情報を誤使用することがないように、これに対抗するセキュリティ機能を備えることを狙いとしている。正当な利用者は、誤使用を行う可能性はあるが、不正は行わないことを想定している。

2.1.2 組織のセキュリティ方針

本評価はEAL1適合であるため、STにセキュリティ課題定義として、組織のセキュリティ方針を記述することは要求されない。

2.1.3 操作環境の前提条件

本評価はEAL1適合であるため、STにセキュリティ課題定義として、TOE使用の前提条件を記述することは要求されない。

ただし、STに、TOEの運用環境のセキュリティ対策方針（通常はTOE使用の前提条件等を受ける形で記述される、TOEの運用環境で実現するセキュリティ対策方針）は記載されており、本TOEを使用する運用環境のセキュリティ対策方針を表2-1に示す。

これらのTOEの運用環境のセキュリティ対策方針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2-1　TOEの運用環境のセキュリティ対策方針

識別子	前提条件
OE.TRUSTED_ROLE （信頼される役割）	責任者は、管理者、オペレータの役割に適した者を厳重に人選し、その上で、それぞれの役割を理解させなければならない。
OE.AUTHORIZATION_SETTING （権限の設定）	ユーザ情報管理者は、管理者、オペレータに権限を付与しなければならない。ユーザ情報管理者は権限の付与について信頼できること。

OE.PASSWORD_MANAGEMENT（パスワードの管理）	すべての利用者は、TOEにアクセスするための識別・認証情報（ユーザ名とパスワード）を管理し、他人に漏らしてはならない。また推測・解析されやすいパスワードを設定してはならず、適正な間隔で変更しなければならない。
OE.SAFE_PLACE（安全な場所）	監視端末、監視サーバ、監視対象サーバは、物理的に不正侵入されない場所に設置されなければならない。
OE.SAFE_NETWORK（安全なネットワーク）	監視端末、監視サーバ、監視対象サーバ間のネットワークは、不正な盗聴や改ざんから保護できなければならない。
OE.TRUSTED_OS（信頼できるOS）	監視端末、監視サーバ、監視対象サーバ上で稼働するOSには、OSの供給元から配布されるパッチを適切に適用しなければならない。

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、前提条件によっては下記ドキュメントの十分な理解と遵守が要求される。

・利用者準備ガイダンス
WebSAM SystemManager Ver5.2.1 利用者準備ガイダンス Ver1.07
・利用者操作ガイダンス
WebSAM SystemManager Ver5.2.1 利用者操作ガイダンス Ver1.08

2.1.5 構成条件

本TOEは、WebSAM SystemManagerである。WebSAM SystemManagerは、監視対象サーバ上に配置される「WebSAM SystemManager エージェント」、監視サーバ上に配置される「WebSAM SystemManager マネージャ」、及び監視端末に配置される「WebSAM SystemManager 監視端末」から構成される。

評価構成としては、「WebSAM SystemManager 監視端末」はWindows版のみであるが、「WebSAM SystemManager マネージャ」及び「WebSAM SystemManager エージェント」はそれぞれWindow版及びHP-UX版が存在する。

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）監視端末

＜ハードウェア（Windows 版用）＞

本体	Express5800 シリーズ、PC/AT 互換機
CPU	PentiumⅢ 1GHz 以上
メモリ	64MB 以上
ハードディスク	100MB 以上
LAN	100Mbps 以上

＜ソフトウェア（Windows 版用）＞

OS	Windows XP Professional (SP2)

（2）監視サーバ

＜ハードウェア（Windows 版用）＞

本体	Express5800 シリーズ、PC/AT 互換機
CPU	PentiumⅢ 1GHz 以上
メモリ	64MB 以上
ハードディスク	1GB 以上
LAN	100Mbps 以上

＜ソフトウェア（Windows 版用）＞

OS	Windows Server 2003, Standard Edition (SP2)

＜ハードウェア（HP-UX 版用）＞

本体	NX7700i シリーズ
メモリ	64MB 以上
ハードディスク	1GB 以上
LAN	100Mbps 以上

＜ソフトウェア（HP-UX 版用）＞

OS	HP-UX 11iV3

（3）監視対象サーバ

＜ハードウェア（Windows 版用）＞

本体	Express5800 シリーズ、PC/AT 互換機

CPU	PentiumⅢ 1GHz 以上
メモリ	32MB 以上
ハードディスク	300MB 以上
LAN	100Mbps 以上

＜ソフトウェア（Windows 版用）＞

OS	Windows Server 2003, Standard Edition (SP2)

＜ハードウェア（HP-UX 版用）＞

本体	NX7000/NX7700/NX7700i シリーズ
メモリ	32MB 以上
ハードディスク	300MB 以上
LAN	100Mbps 以上

＜ソフトウェア（HP-UX 版用）＞

OS	HP-UX 11iV3

本評価で評価構成とした監視サーバと監視対象サーバの組合せは、Windows版の動作環境同士、HP-UX版の動作環境同士のみである。

2.2 セキュリティ対策

TOE は、TOE が管理する監視サーバ上の情報（構成情報、障害情報、性能情報）に対して、正しい利用者（各種管理者、オペレータ）により正しい許可範囲の権限内でアクセスが行われるように、利用者を識別･認証した上で、アクセス制御を行うセキュリティ機能を具備している。

TOEの「識別認証機能」は、TOEにアクセスする利用者について、ユーザ名とパスワードを用いて識別、認証を行う。利用者の識別認証に成功した場合は、当該利用者の権限情報をTOEのアクセス制御機能に通知する。

TOEの「アクセス制御機能」は、TOEの識別認証機能から取得した当該利用者の権限情報を利用して、当該利用者に付与されている権限内でのみ情報にアクセスできるように制御を行う。

具体的には、利用者端末のGUIの項目（メニュー、ボタン等）の「有効/無効」を切り替えることで、アクセス制御を実現する。例えば、各情報に対する参照権限を持つ利用者に対してのみ、各情報のレコードを参照するためのGUI機能を有効化す

る（なお、本TOEの場合、すべての情報（構成情報、障害情報、性能情報）に対する参照権限が、すべての利用者に付与される仕様となっている）。また、各情報に対する操作権限を持つ利用者に対してのみ、各情報のレコードを更新するためのGUI機能を有効化し、操作権限を持たない利用者には無効化する。

また、TOE の「ユーザ情報管理機能」により、TOE へのアクセスを許可する利用者のセキュリティ属性であるユーザ情報、グループ情報、及び権限情報の管理を行うことができる。権限情報は、権限範囲の決められている各役割（各種管理者、オペレータ）を実現するグループごとに設定を行い、各グループには、複数のユーザが所属することができる。ユーザは複数のグループに所属することができる。

利用者は、ログインしたユーザが所属する複数のグループから権限情報を取得することができ、取得した全ての権限が有効になる。

ユーザ情報、及びグループ情報の参照、登録、削除、更新は、ユーザ情報管理者（ビルトイン管理者により、TOE のインストール直後に作成される）、またはビルトイン管理者が行うことができる。

また、認証された利用者は自身の「パスワード」を変更することができる。

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6月に始まり、平成20年9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月及び8月に開発者サイトで開発者から提供されたテスト環境を使用し、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、評価の過程で示された証拠を検証した結果から、必要と判断された評価者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

本評価はEAL1適合であるため、開発者テストに関する検査は要求されない。

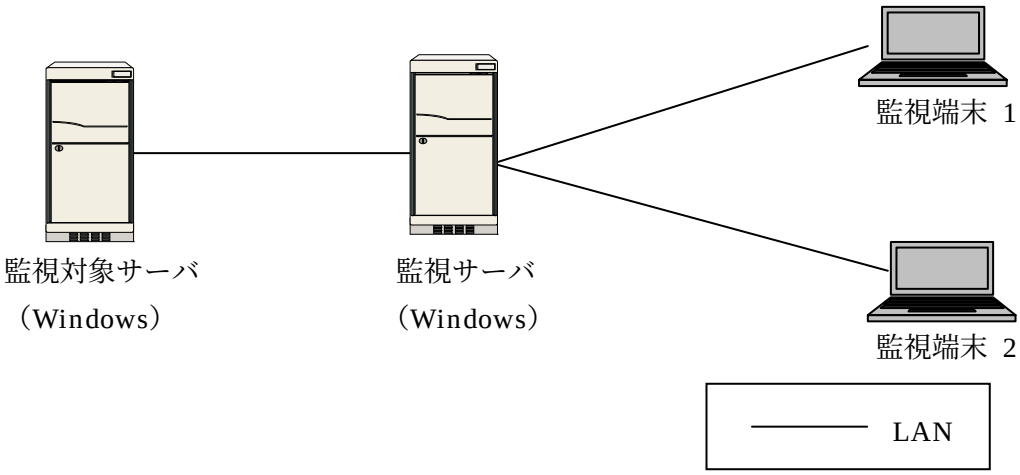
3.3.2 評価者独立テスト

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を確認する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を図3-1に示す。評価者テストは本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。

< ①Windows版TOEのテスト構成 >



< ②HP-UX版TOEのテスト構成 >

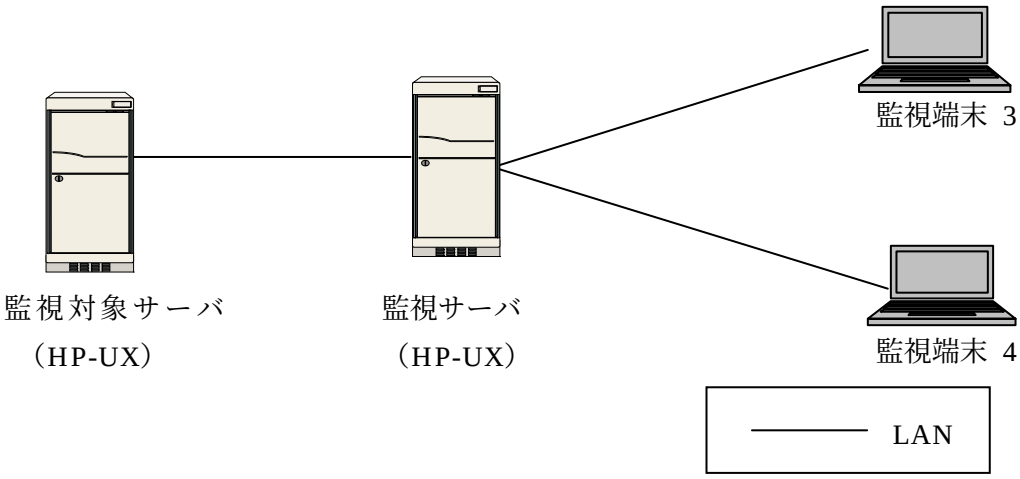


図3-1　評価者テストの構成

なお、図3-1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　評価者テストのソフトウェア構成、ハードウェア構成

機器名	種別	製品名
監視端末 1～4	TOE	WebSAM SystemManager 監視端末
	OS	Windows XP Professional Edition (SP2)
	Hard	Mate JM24A/E-3 ほか
監視サーバ（Windows 版）	TOE	WebSAM SystemManager Manager for Win/Linux
	OS	Windows Server 2003, Standard Edition (SP2)
	Hard	Express5800/110Ca
監視サーバ（HP-UX 版）	TOE	WebSAM SystemManager Manager for HP-UX/Solaris
	OS	HP-UX 11i Version3
	Hard	NX7700i/3012L-2
監視対象サーバ（Windows 版）	TOE	WebSAM SystemManager Agent for Win/Linux
	OS	Windows Server 2003, Standard Edition (SP2)
	Hard	Express5800/110GaS
監視対象サーバ（HP-UX 版）	TOE	WebSAM SystemManager Agent for HP-UX/Solaris
	OS	HP-UX 11i Version3
	Hard	NX7700i/3012E-2

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、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）本TOEのセキュリティ機能は、識別認証機能とアクセス制御機能とに大別されるため、独立テストもこれらの機能が正しく動作していることを確認するために行う。

（2）本TOEのTSFIは、識別機能のTSFIを除き、アクセス制御によってGUI上でのアクセス可否が決定されるため、アクセス制御機能の制御下である全てのTSFIについて網羅的に独立テストを行う。

（3）アクセス制御に影響するユーザ/グループ情報を管理するインタフェース、及びその実行結果の影響について重点的にテストを行うべきと考え、すべての役割の付与、及び剥奪について独立テストを行う。

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。

（1）TOEのTSFI（全21個）をすべて対象とし、258項目の独立テストを実施した。

（2）アクセス制御によるGUI上のTSFIへのアクセス可否の確認テストにおいては、それらの操作手段（TSFI）へのアクセス可否の確認を主眼とし、それらにアクセスされた結果まではアクセス制御機能が責任を負わない（「1.2.3　TOE範囲とセキュリティ機能」参照）ことから、検証は

行なわれていない（例．GUI上のあるボタンがアクセス制御対象である場合、ボタン押下可否のみを検査し、ボタンを押した結果のふるまいまでは検証されていない）。

（3）各テスト構成（Windows版、HP-UX版）とも、監視サーバに監視端末を複数（2台）接続し、正常動作確認（操作者とは別端末から、操作者の権限を変更できる）を行った。

（4）各テスト構成での独立テストを、別々のオペレータによる同時進行で実施した。特にテストツールは使用されていない。

c. 結果

実施したすべての評価者独立テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべての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。

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な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可能性のある以下の脆弱性を識別した。

本評価においては、利用者（各種管理者、オペレータ）による不正は想定せず、誤使用のみ想定しているため、誤使用につながる可能性がある潜在的脆弱性の識別が行われた。具体的には、利用者の識別認証のインタフェースに関わる脆弱性（パスワード入力関連、エラーメッセージの活用、バッファーオーバーフロー等）、利用者権限の変更操作後のTOEのふるまいに関わる脆弱性、及びパスワード等の利用者端末での残存の脆弱性（計10件）が識別された。

上記以外に不正による脆弱性として、公知の脆弱性であるSQLインジェクション（1件）が念のため識別され、悪用可能性が考察された。

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、評価者独立テストと同一のテスト環境を使用し、TOEのTSFI（識別認証インタフェース、パスワード変更インタフェース、権限情

報変更インタフェース）の刺激（想定外のデータの入力、権限変更等)、刺激後のエラーメッセージやTOEのふるまいの確認、及び利用者端末で収集されるログファイルの確認を行うという方法で実施された。本TOEの使用環境においては、TSFI以外からの入力は想定されないため、特別なテスト装置は使用されなかった。

c. 結果

実施した評価者侵入テストでは、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EAL1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

特になし。

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）
TSFI	TSF Interface（TSFインタフェース）

本報告書で使用されたTOEに関する略語を以下に示す。

GUI	グラフィカルユーザインタフェース（Graphical User Interface）

本報告書で使用された用語の定義を以下に示す。

利用者	TOEの機能を利用し、業務を行う者。利用者は管理者とオペレータに大別される。
管理者	利用者の内、TOEの管理を行う者。
オペレータ	利用者の内、TOEの機能を利用して監視業務を行う者。
責任者	TOEに対し、直接操作は行わない。管理者、オペレータを任命する者。
監視サーバ	TOEを構成するコンポーネントの内、WebSAM SystemManagerマネージャを配置したサーバ。TOEの扱う情報を蓄積、管理する。
監視対象サーバ	TOEを構成するコンポーネントの内、WebSAM SystemManagerエージェントを配置したサーバ。構成情報、障害情報、性能情報を収集し、監視サーバに通知する。
監視端末	TOEを構成するコンポーネントの内、WebSAM SystemManager監視端末を配置したクライアントPC。利用者にGUIを提供する。
構成情報	監視対象サーバを構成するOS、CPU、デバイス、アプリケーションソフト、ネットワーク、ディスクの情報。
障害情報	監視対象サーバで発生した、ログ、プロセスの情報、Windowsサービスの情報、性能情報の内、定義情報にて障害と定義されている事象。
性能情報	監視対象サーバのCPU使用率、メモリ使用量、ディスク使用量、

	ネットワーク使用量等、性能に関する情報。
プロセス	OSからメモリ、CPU時間、各種デバイス等の割当てを受けて処理を実行しているプログラム。 監視対象サーバ上で動作する。 TOEは監視対象サーバ上のプロセスを監視、操作する機能を持つ。
Windows サービス	Windows OSのバックグラウンドで動作するプログラム（例．アプリケーションマネジメント・サービス、アプリケーションレイヤーゲートウェイ・サービス）。 監視対象サーバ上で動作する。 TOEは、監視対象サーバ上のWindowsサービスを監視、操作（開始、停止等）する機能を持つ。（監視対象サーバのOSがWindowsの場合のみ）
履歴情報	監視対象サーバが収集し、監視サーバが蓄積、管理している情報（通報、障害情報、性能情報）。
通報	TOEが監視対象サーバの障害情報を検出した時に、電子メールの送信、回転灯の鳴動により、オペレータに通知する機能。
定義情報	監視対象サーバの構成情報、障害情報、性能情報に関する監視項目、監視間隔や、履歴情報の保持期間、通報宛先、監視端末のGUI表示項目など、TOEの動作を決定する情報。
オーディットログ	TOEに対して利用者が行った操作履歴のログ。
オーディットログ定義情報	オーディットログに関するTOEの動作を決定する情報。
ライセンス	TOEの動作に必要な情報。TOE購入時に日本電気株式会社より発行される。 ライセンスには、マネージャライセンスとエージェントライセンスの2種類が存在する。 マネージャライセンスが存在しない、もしくは不正な場合、TOEは使用できない。 エージェントライセンスは、監視対象サーバの数だけ必要であり、エージェントライセンス数を超過して監視対象サーバを接続することはできない。
ヘルプ	監視端末にて参照可能なマニュアル。
ユーザ	利用者を識別し、管理する単位。 通常、利用者毎にユーザを作成し、管理する。
グループ	複数のユーザを所属させ、管理する。権限を付与する単位。
ユーザ情報	ユーザのユーザ名、氏名、備考、パスワード、所属グループの情報。

グループ情報	グループのグループ名、権限、所属ユーザの情報。
権限情報	グループ情報の参照権限、操作権限、定義変更権限、ライセンス管理権限、ユーザ管理権限、オーディットログ参照権限、オーディットログ更新権限の情報。

7 参照

[1] WebSAM SystemManager Ver5.2.1 セキュリティターゲット　バージョン 1.10 2008年9月25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 Revision 1 September 2006 CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 1 September 2006 CCMB-2006-09-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 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: セキュリティ機能コンポーネント 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: セキュリティ保証コンポーネント 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 Revision 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-2006-09-04 (平成19年3月翻訳第1.2版)

[13] WebSAM SystemManager バージョン5.2.1 評価報告書 第1.1版 2008年9月30日 株式会社電子商取引安全技術研究所　評価センター