認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　藤原　武平太

原紙押印済

評価対象

申請受付日（受付番号）	**平成19年8月16日** (IT**認証**7163)
認証番号	C0122
認証申請者	**日本ヒューレット・パッカード株式会社**
TOE**の名称**	**機能特定**（HP IceWall SSO）
TOE**のバージョン**	8.0 R2
PP**適合**	**なし**
適合する保証パッケージ	EAL1（CC Ver3.1）
開発者	**日本ヒューレット・パッカード株式会社**
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19年10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

「HP IceWall SSO 8.0 R2」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、「HP IceWall SSO 8.0 R2」（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日本ヒューレット・パッカード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「1.5.7 製品添付ドキュメント」を参照のこと）を併読されたい。本TOEは低保証STのためセキュリティ課題定義などが記述されていないが、運用環境のセキュリティ対策方針、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：　HP IceWall SSO
バージョン：　8.0 R2
開発者：　日本ヒューレット・パッカード株式会社

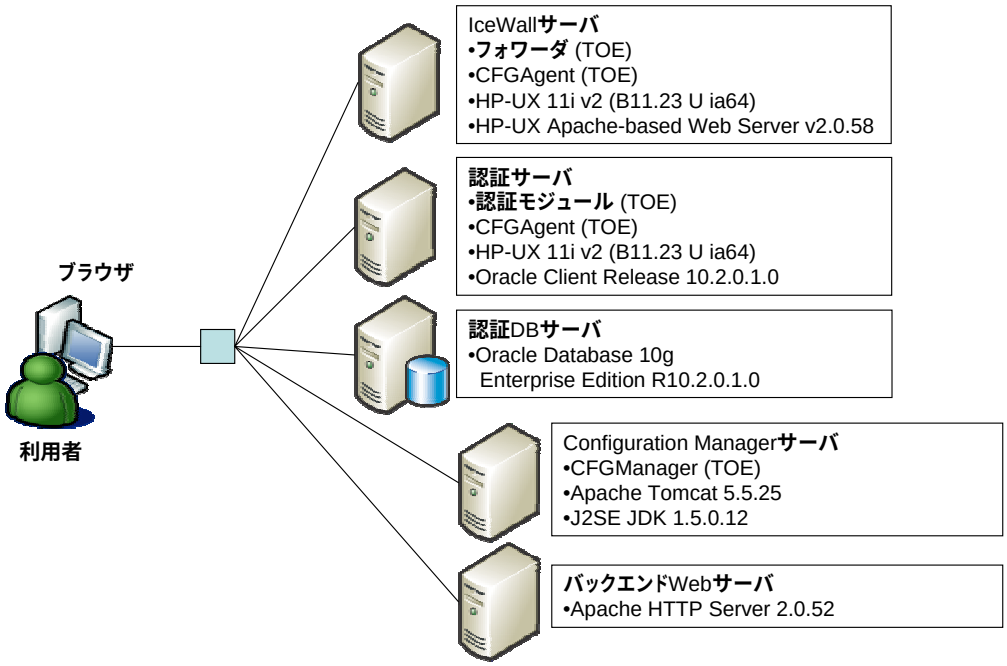
1.2.2 製品概要

本製品は利用者からWebアプリケーションサーバへのアクセス制御を対象としたシングルサインオン製品である。本製品の主要なセキュリティ機能を以下に示す。

・識別・認証機能
・Webアプリケーション・アクセス制御機能
・設定構成管理機能

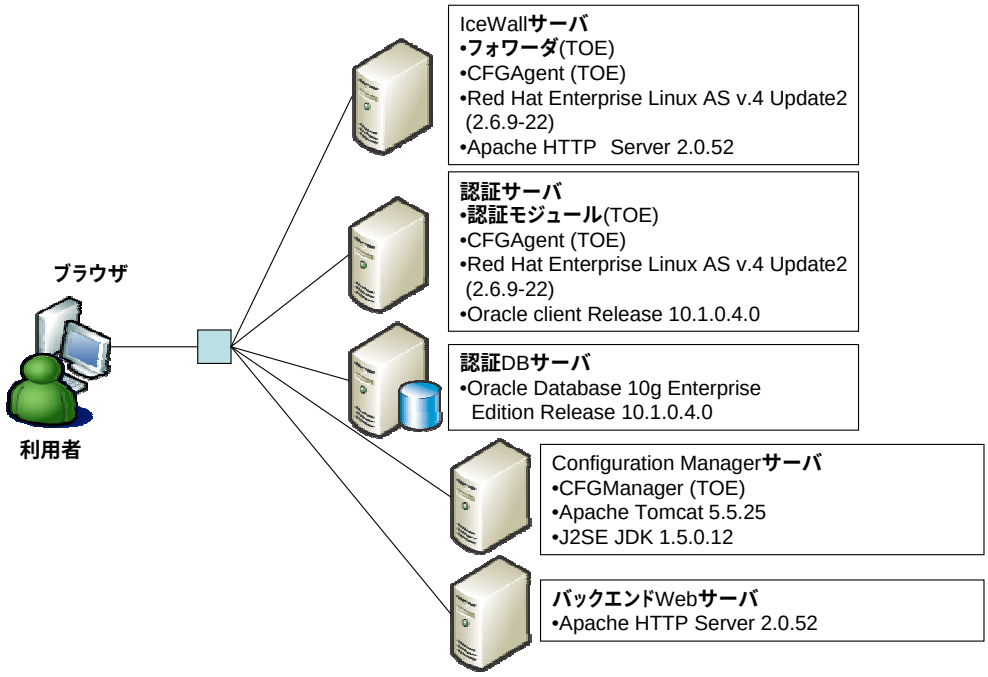
1.2.3 TOEの範囲と動作概要

本TOEは、フォワーダ、認証モジュール、CFGManager、CFGAgentから構成される。本TOEの動作環境概要を図1-1及び図1-2に示す。



※Apache（HTTPD）はすべて80番ポート、Tomcatは8080番ポートで起動

図1-1 TOEの動作環境の構成パターン１：IceWallサーバ(HP-UX) + 認証サーバ(HP-UX)



※Apache（HTTPD）はすべて80番ポート、Tomcatは8080番ポートで起動

図1-2 TOEの動作環境の構成パターン2：IceWallサーバ(Linux) + 認証サーバ(Linux)

本TOEの動作概要について以下に示す。

①利用者は、IceWallサーバ（詳細は後述）にアクセスする。
②認証サーバ（詳細は後述）にて本人確認が行われる。
③利用者はグループに関連づけられおり、認証サーバはリクエストするURLに対して利用者が属するグループがアクセス許可されているかをチェックする。
④許可されているURLである場合、IceWallサーバよりバックエンドWebサーバへのリクエストが中継される。

本TOE及び本TOEと連動する構成要素について以下に示す。

(1) IceWallサーバ（TOEであるフォワーダ、CFGAgentを含む）
TOEであるフォワーダ、CFGAgentが動作するサーバ。
フォワーダは、利用者からのサービス要求を受け取り、利用者の権限に基づいてバックエンドWebサーバへのhttpリクエストの中継を行う。フォワーダは認証サーバの認証モジュールと連携して、ユーザIDおよびパスワードに基づいたログイン処理および利用者の権限に基づいたhttpリクエストの中継処理を行う。
CFGAgentはConfiguration ManagerサーバのCFGManagerと連携して、設定情報の登録、変更および削除を行う。

(2) 認証サーバ（TOEである認証モジュール、CFGAgentを含む）
TOEである認証モジュール、CFGAgentが動作するサーバ。
認証モジュールは、フォワーダから要求を受け、認証処理およびアクセス権限チェック処理を行う。
CFGAgentはConfiguration ManagerサーバのCFGManagerと連携して、設定情報の登録、変更および削除を行う。

(3) 認証DBサーバ（TOE範囲外）
認証情報が格納されているデータベース・サーバ。認証処理は認証サーバの認証モジュールと認証DBサーバ間で連携して行われる。

(4) Configuration Managerサーバ（TOEであるCFGManagerを含む）
TOEであるConfiguration Manager（CFGManager）が動作するサーバ。
TOEの管理者であるIceWall SSO管理者によって使用されるURLアクセス制御機能のグループ設定機能、ACL設定機能の設定管理機能が提供される。
IceWallサーバおよび認証サーバに配置されたTOEであるCFGAgentと連携して、設定情報の登録、変更および削除を行う。

(5) バックエンドWebサーバ（TOE範囲外）
IceWallサーバのフォワーダから受け取ったhttpリクエストの処理を行うWeb

アプリケーションサーバ。

1.2.4 TOEの機能

本TOEのセキュリティ機能の内容を以下に示す。

(1) 認証機能（フォワーダ、認証モジュールが連動する）
利用者によって入力されたユーザIDとパスワードを使用して本人確認および認証を行う機能。

(2) Webアプリケーション・アクセス制御機能（フォワーダ、認証モジュールが連動する）
認証された利用者が所属するグループの認可情報に基づいて、バックエンドWebサーバ上のコンテンツのアクセスを制御する機能。ディレクトリ単位及びファイル名指定のアクセス制御が可能。

・ユーザ情報を用いたアクセス制御機能
利用者からリクエストされたURLに対して許可されたグループのみアクセスすることを可能とする機能。 IceWall SSO管理者は各利用者がアクセス権限に応じて、１つ、あるいは複数のグループに所属するように設定することが可能。

・アクセス経路によるアクセス制御機能
利用者に対して許可するリクエストのリクエスト元による条件を定義し、アクセス制御を行う機能。

(3) 設定構成管理機能（フォワーダ、認証モジュール、CFGManager、CFGAgentが連動する）
WebブラウザからIceWall SSO管理者による設定情報の設定および設定ファイルの管理を行う機能。グループ設定ファイルおよびアクセスコントロールファイル内の設定値を参照、追加、変更及び削除することが可能。

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「HP IceWall SSO 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、「HP IceWall SSO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。評価は、平成19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、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適合である。

1.5.3 セキュリティ機能

本TOEのセキュリティ機能は、1.2.4を参照のこと。

本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。

・アクセス制御

・識別・認証

・セキュリティ管理

1.5.4 脅威

本TOEでは、セキュリティ課題定義は評価対象外である。

1.5.5 組織のセキュリティ方針

本TOEでは、セキュリティ課題定義は評価対象外である。

1.5.6 構成条件

TOEが動作するために必要なIT製品の中で、本評価にて検証した環境を以下に示す。

動作前提条件：

- TOEはIDおよびパスワードによる認証方式を使用。
- TOEに関する設定値はすべて初期値を適用。

IceWallサーバの動作環境：

- OS(S/W):
  - (HP-UX版)　HP-UX 11i v2 (B.11.23 U ia64)
  - (Linux版) Red Hat Enterprise Linux AS v.4 Update2 (2.6.9-22) (*1)
- Webサーバ(S/W):
  - (HP-UX版) HP-UX Apache-based Web Server v2.0.58 (*2)
  - (Linux版) Apache HTTP Server 2.0.52 (*2)

認証サーバ(certd)の動作環境：

- OS(S/W):
  - (HP-UX版) HP-UX 11i v2(B.11.23 U ia64)
  - (Linux版) Red Hat Enterprise Linux AS v.4 Update2 (2.6.9-22) (*1)
- データベース・クライアント(S/W) :
  - Oracle Client Release 10.2.0.1.0
  - Oracle Client Release 10.1.0.4.0

認証DBサーバの動作環境：

- データベース・サーバ(S/W) :
  - Oracle Database 10g Enterprise Edition R10.2.0.1.0
  - Oracle Database 10g Enterprise Edition Release 10.1.0.4.0

Configuration Managerサーバの動作環境：

- Webサーバ(S/W):
  - Apache Tomcat 5.5.25
- Java SDK (S/W):

- J2SE JDK 1.5.0.12

注意事項）＊1 ：NSA Security-Enhanced Linux (SELinux)を有効にした環境での動作はサポートとされない。

注意事項）＊2 ：OSベンダ提供パッケージのみサポート

1.5.7 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以下に示す。

- IceWall SSO Version 8.0, 8.01(8.0R1), 8.0R2 導入ガイド HP-UX版 2007年10月 HP Part No. B2873-90804 Rev.071005A
- IceWall SSO Version 8.0, 8.01(8.0R1), 8.0R2 導入ガイド Linux版 2007年10月 HP Part No. B2873-90805 Rev.071005A
- IceWall SSO Version 8.0, 8.01(8.0R1), 8.0R2 ユーザーズマニュアル 2007年10月 HP Part No. B2873-96802 Rev.071004A
- IceWall SSO Version 8.0, 8.01(8.0R1), 8.0R2 リファレンスマニュアル 2007年10月 HP Part No. B2873-94802 Rev.071003A
- IceWall SSO Version 8.0, 8.01(8.0R1), 8.0R2 トラブルシューティングガイド 2007年3月 HP Part No. B2873-97833 Rev.070223A
- IceWall SSO Version 8.0, 8.01(8.0R1), 8.0R2 導入ガイド for Configuration Manager 2007年10月 HP Part No. B2873-97827 Rev.071003A
- IceWall SSO Version 8.0 R2 Enterprise Edition 最初にお読みください 2007年10月 HP Part No. B2873-97825 Rev.071012A
- IceWall SSO Version 8.0 R2 Standard Edition 最初にお読みください 2007年10月 HP Part No. B1544-97801 Rev.071012A

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8月に始まり、平成19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19年9月及び10月に開発者サイトで開発者の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。

2.3 製品テスト

評価者が評価した開発者テスト及び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 開発者テスト

本TOEでは、開発者テストは評価対象外である。

2.3.2 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環境を図2-1に、TOEの動作に関係する各構成要素の要件を表2-1及び表2-2示す。

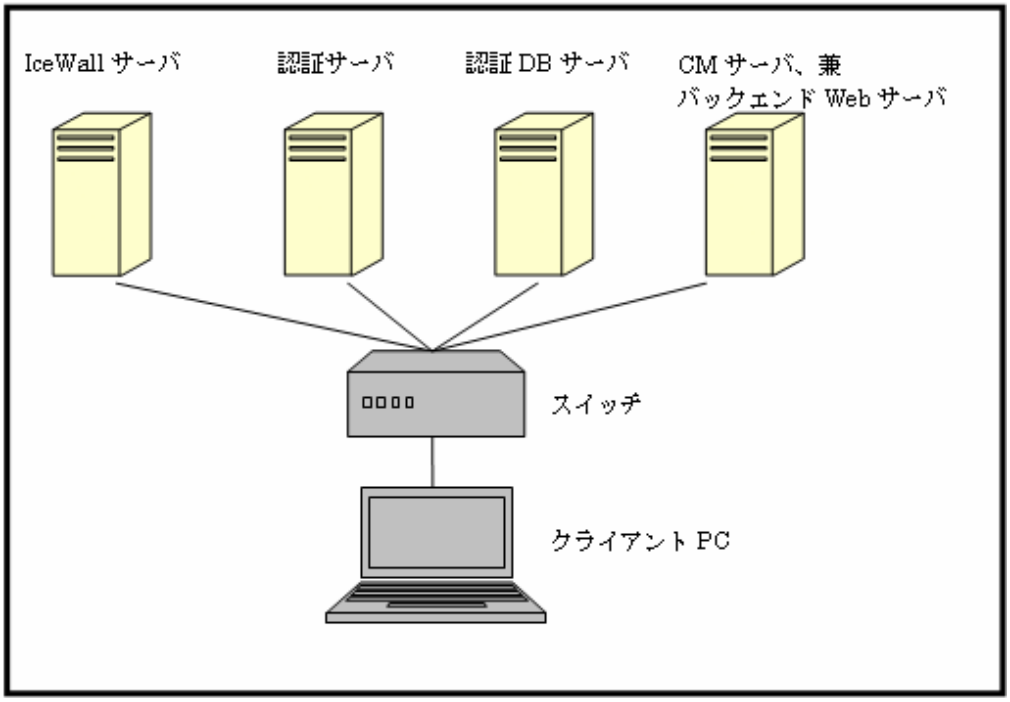


図2-1　評価者テストの環境

表2-1　評価者テストの環境におけるTOEの動作に関係する各構成要素の要件（HP-UX版）

名称	製品
IceWall サーバ	ハード：HP integrity rx2620 OS：HP-UX 11i v2（B.11.23 U ia64） Web サーバ：HP-UX Apache-based Web Server v2.0.58
認証サーバ	ハード：HP integrity rx1600 OS：HP-UX 11i v2（B.11.23 U ia64） Oracle クライアント：Oracle Client　Release10.2.0.1.0
認証DBサーバ	Oracle サーバ：Oracle Database 10g Enterprise Edition R10.2.0.1.0 TOE は、認証 DB サーバのハードや OS に依存しない API のインタフェースである。
CM サーバ兼バックエンド Webサーバ	【CM】 Web サーバ：Apache Tomcat 5.5.25 Java SDK：J2SE JDK 1.5.0.12 CM は、ハードと OS に依存しない API インタフェースである。 【バックエンド Web サーバ】 Web サーバ：Apache-based Web Server v2.0.52 TOE は、バックエンド Web サーバのハードや OS に依存しない API インタフェースである。 ※CM サーバとバックエンド Web サーバは、リソースの関係上（2 台用意することが不可能）1 台の筐体で実施した。これらのサーバに搭載される CM とバックエンドのコンテンツは依存関係がなく独立しているためテスト環境として問題はない。

クライアントPC	OS：Windows XP SP2 2007 年 9 月 18 日現在、Microsoft update 対応済
ブラウザ （クライアント PC）	ブラウザ：Internet Explorer 6 SP2 ・通常の HTTP の GET リクエスト、HTML 内の POST リクエストを送信するために利用。
Fiddler v1.3.0.0 （クライアント PC）	HTTP デバッギングツール ・IE6 の送信情報を記録すると共に、記録情報をベースとして任意のリクエストを構成することができる。 ・任意のリクエストの送信が可能であり、そのレスポンスと含めてモニタリングすることが可能。
Nikto v1.36 （クライアント PC）	汎用 http 脆弱性スキャナツール ・http メソッド、cgi 等に公知の脆弱性が内在していないか、また http サーバの設定不備等を検知するための、スキャンツール。 ・コマンドラインから標準出力で結果を出力し、検知された脆弱性の概要が示される。 ・プラグイン DB は、2007/9/18 現在最新をアップデート済
Wireshark 0.99.6a	パケットキャプチャツール ・クライアント PC の NIC に到達する Ether ネット上のパケットをモニタリング、記録するためのツール。
Nessus3.0.6.1 Build W321 （クライアント PC）	汎用脆弱性スキャナツール ・ポートスキャンをはじめとして、各種プロトコル、OS 等の公知の脆弱性を検知することができるオールインワンのスキャンツール ・レポートは、HTML で出力され、検知された脆弱性の概要が示される。 ・プラグイン DB は、2007/9/18 現在最新をアップデート済
スイッチ	スイッチは各機器をネットワーク接続するために必要な機器であるが、特定の対象機器である必要はない。

表2-2　評価者テストの環境におけるTOEの動作に関係する各構成要素の要件（Linux版）

名称	製品
IceWall サーバ	ハード：HP Proliant DL385 OS：Red Hat Enterprise Linux AS v.4 Update2 (2.6.9-22) Web サーバ：Apache HTTP Server 2.0.52
認証サーバ	ハード：HP Proliant DL145RG2 OS：Red Hat Enterprise Linux AS v.4 Update2 (2.6.9-22) Oracle クライアント：Oracle Client Release10.1.0.4.0
認証DBサーバ	Oracle サーバ：Oracle Database 10g Enterprise Edition Release10.1.0.4.0 TOE は、認証 DB サーバのハードや OS に依存しない API インタフェースである。

CM サーバ兼バックエンドWebサーバ	【CM】 Web サーバ：Apache Tomcat 5.5.25 Java SDK：J2SE JDK 1.5.0.12 CM は、ハードや OS に依存しない API インタフェースである。 【バックエンド Web サーバ】 Web サーバ：Apache-based Web Server v2.0.52 TOE は、バックエンド Web サーバのハードや OS に依存しない API インタフェースである。 ※CM サーバとバックエンド Web サーバは、リソースの関係上（2 台用意することが不可能）1 台の筐体で実施した。これらのサーバに搭載される CM とバックエンドのコンテンツは依存関係がなく独立しているためテスト環境として問題はない。
クライアントPC	OS：Windows XP SP2 2007 年 9 月 18 日現在、Microsoft update 対応済
ブラウザ（クライアントPC）	ブラウザ：Internet Explorer 6 SP2 ・通常の HTTP の GET リクエスト、HTML 内の POST リクエストを送信するために利用。
Fiddler v1.3.0.0（クライアントPC）	HTTP デバッギングツール ・IE6 の送信情報を記録すると共に、記録情報をベースとして任意のリクエストを構成することができる。 ・任意のリクエストの送信が可能であり、そのレスポンスと含めてモニタリングすることが可能。
Nikto v1.36（クライアントPC）	汎用 http 脆弱性スキャナツール ・http メソッド、cgi 等に公知の脆弱性が内在していないか、また http サーバの設定不備等を検知するための、スキャンツール。 ・コマンドラインから標準出力で結果を出力し、検知された脆弱性の概要が示される。 ・プラグイン DB は、2007/9/18 現在最新をアップデート済
Wireshark 0.99.6a	パケットキャプチャツール ・クライアント PC の NIC に到達する Ether ネット上のパケットをモニタリング、記録するためのツール。 ・スイッチ経由で認証サーバと認証 DB サーバのパケットをクライアント PC にてキャプチャするには、クライアント PC 接続の物理ポートに対して、認証 DB サーバの物理ポートのパケットをミラーリングする必要がある。
Nessus3.0.6.1 Build W321（クライアントPC）	汎用脆弱性スキャナツール ・ポートスキャンをはじめとして、各種プロトコル、OS 等の公知の脆弱性を検知することができるオールインワンのスキャンツール ・レポートは、HTML で出力され、検知された脆弱性の概要が示される。 ・プラグイン DB は、2007/9/18 現在最新をアップデート済
スイッチ	スイッチは各機器をネットワーク接続するために必要な機器であるが、特定の対象機器である必要はない。

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を図2-1、TOEの動作に関係する各構成要素の要件を表2-1及び表2-2に示す。評価者テストはSTにおいて識別されているTOE構成を満たすテスト環境で実施されている。

b.テスト手法

テストには、以下の手法が使用された。

①Webブラウザ、HTTPデバッギングツール及び脆弱性スキャナツールを用いて外部インタフェースからセキュリティ機能に刺激（パラメータ）を与え、外部インタフェースや送受信されるパケットの情報を参照してセキュリティ機能のふるまいを目視確認する。

c.実施テストの範囲

評価者が独自に考案した評価者テストを23項目、侵入テストを26項目、計49項目実施した。テスト項目の選択基準として、下記を考慮している。

① 外部インタフェースを対象とし、限界値分析によるブラックボックステストを実施する。

② テストするインタフェースは、重要性、複雑性、効率性、種別、新規性を踏まえて決定する。

③ テストするインタフェースに関わるセキュリティ機能を網羅的にテストする。

d.結果

実施したすべての評価者テスト及び侵入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。

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。

認証機関は、ST及び評価報告書において、所見報告書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_OBJ.1.1E	評価はワークユニットに沿って行われ、運用環境の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.1.1E	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と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。
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、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んで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IT環境に対するセキュリティ要件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。

ACL	Access Control List
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
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。

ACL	アクセスコントロールリストの略。アクセス制御のためのルールのセットが定義される。
CFGAgent	IceWallサーバおよび認証サーバに配置され、CFGManagerからのリクエストに応じて、各フォワーダまたは各認証モジュールの設定操作の処理を行う。
CFGManager	IceWall SSO管理者により設定管理操作を行うためのWebアプリケーション。CFGAgentと連携して、フォワーダおよび認証モジュールの設定操作の処理を行う。
IceWall SSO管理者	アクセス・ルールの定義等、IceWall SSOに関する設定管理を行う管理者。
IceWallサーバ	フォワーダが動作するサーバ。
アクセスコントロールファイル	バックエンドWebサーバに対するアクセスコントロールを定義する設定ファイル(cert.acl)。
クライアント	Webブラウザ等、利用者がサービス要求を送信する環境。
グループ設定ファイル	アクセスコントロールで使用するグループを定義する設定ファイル(cert.grp)。
システム管理者	IceWallサーバ、認証サーバ、認証DBサーバ、Configuration Managerサーバといったを動作させるために必要な一連のサーバ群の設定管理、ネットワーク環境を管理する管理者。
シングルサインオン	利用者が一度認証を受けることによって、利用者の権限に基づいて複数のWebアプリケーションサーバ(後述、バックエンドWebサーバ)にアクセスできるようにする機能。

中継(httpリクエストの中継)	フォワーダは利用者からのHTTPリクエストヘッダを確認する。アクセスコントロール対象のURLの場合、フォワーダはバックエンドWebサーバをアクセスするためのURLに書き換えを行い、利用者がアクセス権限をもつことを確認した後、所定のHTTPリクエストをバックエンドWebサーバに送信する。
認証サーバ	認証モジュールが動作するサーバ。
認証モジュール	フォワーダの要求を受け、認証DB（ディレクトリまたはデータベース）に認証認可情報の問い合わせを行うデーモンプロセス。
バックエンドWebサーバ	Webブラウザを通じて出された利用者からのサービス要求をIceWallサーバから受けて処理を行う、バックエンド構成要素としてのWebアプリケーションサーバ。
フォワーダ	利用者からのサービス要求を受け取り、バックエンドWebサーバへのサービス要求を代行するCGIプロセス。
利用者	WebブラウザIceWallサーバに対してサービス要求を送信する人。

6 参照

[1] HP IceWall SSO セキュリティターゲット バージョン 2.2（2007年10月17日）
日本ヒューレット・パッカード株式会社

[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-2006-09-004　(平成19年3月翻訳第1.2版)

[13] HP IceWall SSO 評価報告書 第三版 2007年10月24日
みずほ情報総研株式会社　情報セキュリティ評価室