認 証 報 告 書

独立行政法人情報処理推進機構
理事長　藤江　一正 押印済

評価対象

申請受付日（受付番号）	平成23年6月10日 (IT認証1352)
認証番号	C0306
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	Version 10.0（「フォワーダー Patch Release 1」、及び「認証モジュール Patch Release 1」を含む）
PP適合	なし
適合する保証パッケージ	EAL1
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23年8月15日

技術本部 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　山里　拓己

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 リリース３
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 リリース３

評価結果：合格

「HP IceWall SSO Version 10.0」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

この認証報告書は、日本ヒューレット・パッカード株式会社が開発した「HP IceWall SSO　Version10.0（「フォワーダー　Patch Release 1」、及び「認証モジュール　Patch Release 1」を含む）」（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。）が平成 23 年 7 月 26 日に完了した 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とともに、本 TOE に関心を持つ消費者や調達者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書の付属書であるセキュリティターゲット[12]（以下「ST」という。）を併読されたい。特に本 TOE のセキュリティ機能要件、保証要件及びその十分性の根拠は、ST において詳述されている。

本認証報告書は、本 TOE を購入する一般消費者を読者と想定している。本認証報告書は、本 TOE が適合する保証要件に基づいた認証結果を示すものであり、個別の IT 製品そのものを保証するものではないことに留意されたい。

1.1 評価対象製品概要

本 TOE の機能、運用条件の概要を以下に示す。詳細は 2 章以降を参照のこと。

1.1.1 保証パッケージ

本 TOE の保証パッケージは、EAL 1 である。

1.1.2 TOEとセキュリティ機能性

本 TOE 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。

利用者がバックエンド Web サーバ上のコンテンツにアクセス開始する際、本 TOE は、ユーザ ID とパスワードを使用して認証サーバにて本人確認及び認証を行う（認証機能）。利用者はグループに関連づけられており、TOE は、リクエストされた URL に対して利用者が属するグループがアクセスを許可されている場合のみ、IceWall サーバからバックエンド Web サーバへのリクエストを中継する（Web アプリケーション・アクセス制御機能）。また、本 TOE は、IceWall SSO 管理者が IceWall サーバ、認証サーバの設定情報の設定及び設定ファイルの管理を行う設定構成管理機能を有する（設定構成管理機能）。

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について保証パッケージの範囲で評価が行われた。本 TOE が想定する脅威及び前提については次項のとおりである。

1.1.2.1 脅威とセキュリティ対策方針

EAL1 のため、本評価において、セキュリティ課題定義は評価対象外である。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような構成で運用することを想定する。

・TOE であるフォワーダー及び RCFGAgent が動作する IceWall サーバ
・TOE である認証モジュール及び RCFGAgent が動作する認証サーバ
・TOE である RCFGManager が動作する RCFGManager サーバ
・認証情報が格納されている認証 DB サーバ（TOE 対象外）
・フォワーダーから受け取った http リクエストの処理を行うバックエンド Web サーバ（TOE 対象外）

上記 TOE のうち、フォワーダー、認証モジュール及び RCFGAgent の動作する OS は Linux 及び HP-UX の 2 種類、RCFGManager の動作する OS は Windows Server 2008 である。

また、本 TOE は次のような運用環境で使用されることを前提とする。

・システム管理者、IceWall SSO 管理者には信頼できる人物であること。
・上記構成要件にあるサーバの管理操作は、システム管理者のみに制限すること。
・IceWall SSO 管理者は、利用者グループの設定でセキュリティ属性として IP アドレスを使用する場合は、必ず IP アドレスとユーザ ID を組み合わせること。
・利用者からバックエンド Web サーバへのアクセスは、http/https により IceWall サーバを介してのみに制限されること。
・パスワードの管理が十分にされていること。

1.1.3 免責事項

特になし。

1.2 評価の実施

認証機関が運営する IT セキュリティ評価・認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証申請手続等に関する規程」[2]、「IT セキュリティ評価機関承認申請手続等に関する規程」[3]に規定された内容に従い、評価機関によって本 TOE に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、平成 23 年 7 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]、所見報告書、及び関連する評価証拠資料を検証し、本 TOE の評価が所定の手続きに沿って行われたことを確認した。TOE の評価が CC（[4][5][6]または[7][8][9]）及び CEM（[10][11]のいずれか）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識別

本 TOE は、以下のとおり識別される。

TOE名称：	機能特定（HP IceWall SSO）
バージョン：	Version 10.0（「フォワーダー Patch Release 1」、及び「認証モジュール Patch Release 1」を含む）
開発者：	日本ヒューレット・パッカード株式会社

製品が評価･認証を受けた本 TOE であることを、利用者は以下の方法によって確認することができる。

管理マニュアルに記載された手順に従い、コンソール画面において構成確認メニューを表示させ、その名称及びバージョンと、TOE 構成品一覧の当該記載を比較することにより､設置された製品が評価を受けた本TOE であることを確認できる。

また、本 TOE を含む CD-ROM のラベルにより確認できる。

3 セキュリティ方針

本章では、本 TOE が脅威に対抗するために採用したセキュリティ機能を説明する。

TOE は、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。

TOE のセキュリティ機能を以下に説明する。

■認証機能（フォワーダー、認証モジュール）
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及び認証を行う機能。

■Web アプリケーション・アクセス制御機能（フォワーダー、認証モジュール）
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
  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
  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。

■ 設定構成管理機能（フォワーダー、認証モジュール、RCFGManager、RCFGAgent）
デスクトップアプリケーションから IceWall SSO 管理者による設定情報の設定及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及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。

3.1 セキュリティ機能方針

本 TOE は EAL1 のため、本評価において、セキュリティ課題定義は保証要件には含まれない。

4 前提条件と評価範囲の明確化

本章では、想定する読者が本 TOE の利用の判断に有用な情報として、本 TOE を運用するための運用環境について記述する。

4.1 使用及び環境に関する前提条件

本 TOE は EAL1 のため、本評価において、セキュリティ課題定義は保証要件には含まれないが、評価されたセキュリティ機能を有効に動作させるための操作環境の前提となる運用環境のセキュリティ対策方針を表 1－1 に示す。

表 1-1　運用環境のセキュリティ対策方針

識別子	運用環境のセキュリティ対策方針
OE.Admin (管理者の信頼性)	システム管理者、IceWall SSO管理者には信頼できる人物を任命すること。
OE.Password (パスワードの管理)	システム管理者、またはIceWall SSO管理者は、利用者に対して、自身のパスワードが漏洩しないように管理させること。また容易に推測可能なパスワードを設定させないようにすること。IceWall SSO管理者は、自身のパスワードが漏洩しないように管理すること。また推測可能なパスワードを設定しないこと。
OE.Access control to dfw/certd/ Authentication DB/CM	IceWallサーバ、認証サーバ、認証DBサーバ、RCFGManagerサーバの管理操作は、システム管理者のみに制限すること。
OE.Setting Environment	利用者からIceWallサーバへのアクセスはhttp/httpsのみに制限し、利用者はIceWallサーバを介してのみバックエンドWebサーバへアクセスすることができるネットワーク環境を構成すること。すなわち利用者がIceWallサーバにアクセスするネットワーク環境に応じてシステム管理者は以下の設定を行うこと。 • 利用者がインターネット経由で IceWall サーバにアクセスする場合：認証サーバ、認証 DB サーバ、RCFGManager サーバ、及びバックエンド Web サーバはファイアウォールに守られたネットワーク環境に置かれ、利用者から直接アクセスできないこと。 • 利用者がイントラネット経由で IceWall サーバにアクセスする場合：認証サーバ、認証 DB サーバ、RCFGManager サーバ、及びバックエンド Web サーバは、利用者に対して直接アクセスしない使用条件を遵守させること。

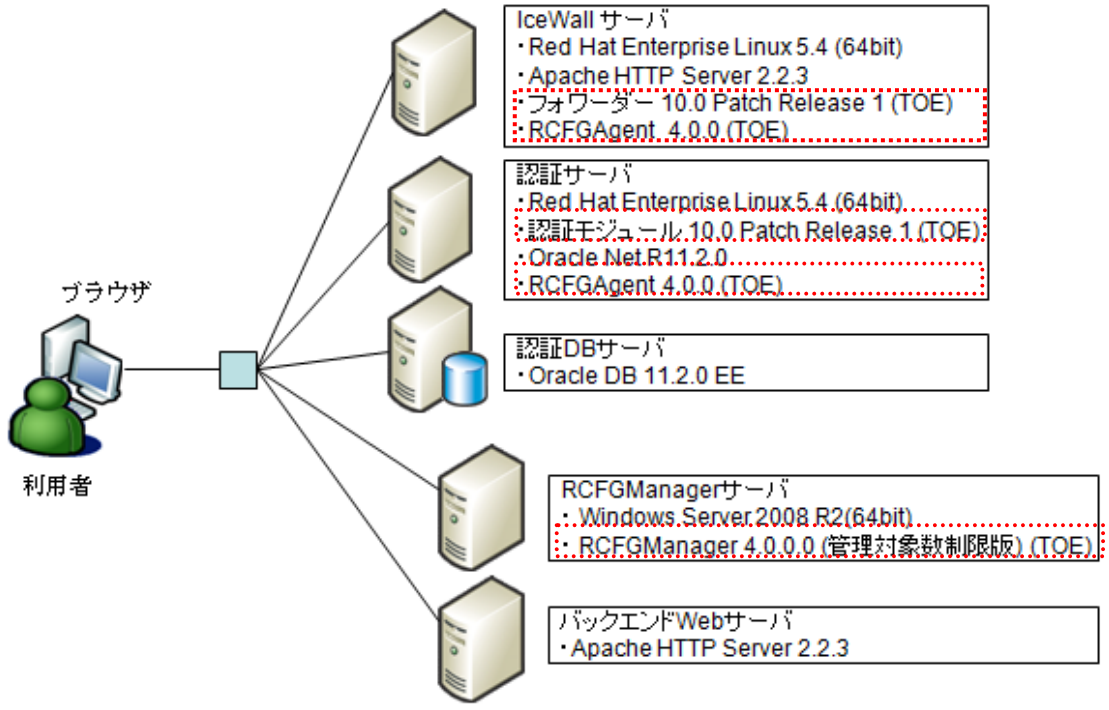
識別子	運用環境のセキュリティ対策方針
OE.Group Definition	IceWall SSO管理者は、グループ設定において、IPアドレスのみでグループを設定しないこと。 IPアドレスを使用する場合はIPアドレスと利用者に紐付く情報（ユーザID）を組み合わせてグループ設定を行うこと。

4.2 運用環境と構成

本 TOE は、フォワーダー、認証モジュール、RCFGManager、RCFGAgent から構成される。TOE が動作するオペレーティングシステムとそのハードウェアは TOE の範囲ではない。

本 TOE はオフィスに設置され、利用者はインターネット経由で、あるいは、イントラネット経由で、IceWall サーバにアクセスする。本 TOE の一般的な運用環境を図 4-1 に示す。

Linux の動作環境：



※Apache(HTTPD)はすべて80番ポート

HP-UX の動作環境：

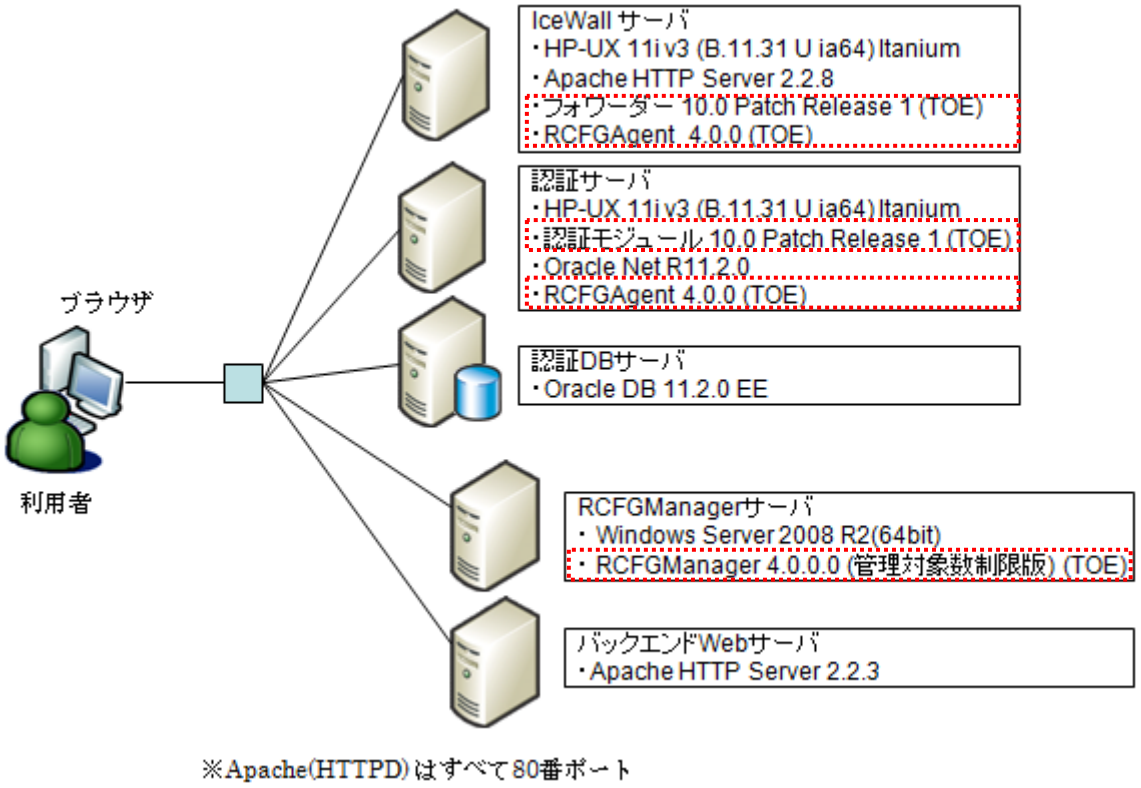


図 4-1 TOEの運用環境

注）1. フォワーダーに「IceWall SSO 10.0 フォワーダー Patch Release 1」を適用。

2. 認証モジュールに「IceWall SSO 10.0 認証モジュール Patch Release 1」を適用。

動作前提条件：

- ID 及びパスワードによる認証方式を使用。
- 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 v3 (B.11.31 U ia64) Itanium (*1)

    注意事項）＊1：2009年3月時点のStandard Patch Bundles以降が導入されている必要がある。
  - （Linux 版）

    Red Hat Enterprise Linux 5.4 x86_64 (*2)

    注意事項）＊2：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。
- Web サーバ (S/W):

- （HP-UX 版）HP-UX Apache-based Web Server v2.2.8 (64bit) (*3)
- （Linux 版）Apache HTTP Server 2.2.3 (*3)(*4)

注意事項）＊3：OSベンダ提供パッケージのみサポート

注意事項）＊4：prefork版のみサポート

認証サーバ (certd) の動作環境：

■ OS (S/W):

- （HP-UX 版）

  HP-UX 11i v3 (B.11.31 U ia64) Itanium (*1)
- （Linux 版）

  Red Hat Enterprise Linux 5.4 x86_64(*2)

■ データベース・クライアント (S/W):

Oracle Net R11.2.0

認証DBサーバの動作環境：

■ データベース・サーバ (S/W):

Oracle DB 11.2.0 EE

RCFGManagerサーバの動作環境：

■ OS (S/W):

Windows Server 2008 R2 (64bit)

4.3 運用環境におけるTOE範囲

本構成に示されているハードウェア及び連携するソフトウェアの信頼性は本評価の範囲ではない（十分に信頼できるものとする）。

5 アーキテクチャに関する情報

本 TOE では、アーキテクチャは評価対象外である。

6 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。TOE の利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

- IceWall SSO Version 10.0 導入ガイド HP-UX 版
  2010 年 8 月 HP Part No. B2873-93000 Rev.100819A
- IceWall SSO Version 10.0 導入ガイド Linux 版
  2010 年 8 月 HP Part No. B2873-93001 Rev.100819A
- IceWall SSO Version 10.0 ユーザーズマニュアル
  2010 年 8 月 HP Part No. B2873-96000 Rev.100820A
- IceWall SSO Version 10.0 リファレンスマニュアル
  2011 年 4 月 HP Part No. B2873-94000 Rev.110414A
- IceWall SSO Version 10.0 トラブルシューティングガイド
  2010 年 8 月 HP Part No. B2873-97001 Rev.100819A
- IceWall Remote Configuration Manager Version 4.0 マニュアル
  2010 年 8 月 HP Part No. B1531-97406 Rev.100803A
- IceWall SSO Version 10.0 Enterprise Edition 最初にお読みください
  2011 年 6 月 HP Part No. B2873-97000 Rev.110621A
- IceWall SSO Version 10.0 Standard Edition 最初にお読みください
  2011 年 6 月 HP Part No. B1544-97000 Rev.110621A
- IceWall SSO 10.0 フォワーダー Patch Release 1 リリースノート
  2011 年 02 月 Rev.110222A
- IceWall SSO 10.0 認証モジュール Patch Release 1 リリースノート
  2011 年 03 月 Rev.110301A

7 評価機関による評価実施及び結果

7.1 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[13]において報告された。評価報告書では、本 TOE の概要と、CEM のワークユニットごとの評価内容及び判断結果を説明する。

7.2 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 23 年 6 月に始まり、平成 23 年 7 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 23 年 6 月に開発者サイトで開発者のテスト環境を使用し、公知の脆弱性探索方法、及び脆弱性チェックリストを用いて脆弱性分析を行い考案した侵入テストを実施、また、ASE クラス、ADV クラス、ALC クラス、及び AGD クラスの評価証拠資料を基にして作成したテスト文書を基に独立テストを実施した。

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。

これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

7.3 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。

7.3.1 開発者テスト

EAL1 のため、本評価において、開発者テストは保証要件には含まれない。

7.3.2 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より確信するための独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを以下に説明する。

(1) 独立テスト環境

評価者が実施した独立テストの構成を図 7-1 に示す。評価者が実施した独立テストの構成は、本 ST[12]において識別されている TOE 構成と同一の環境で実施されている。

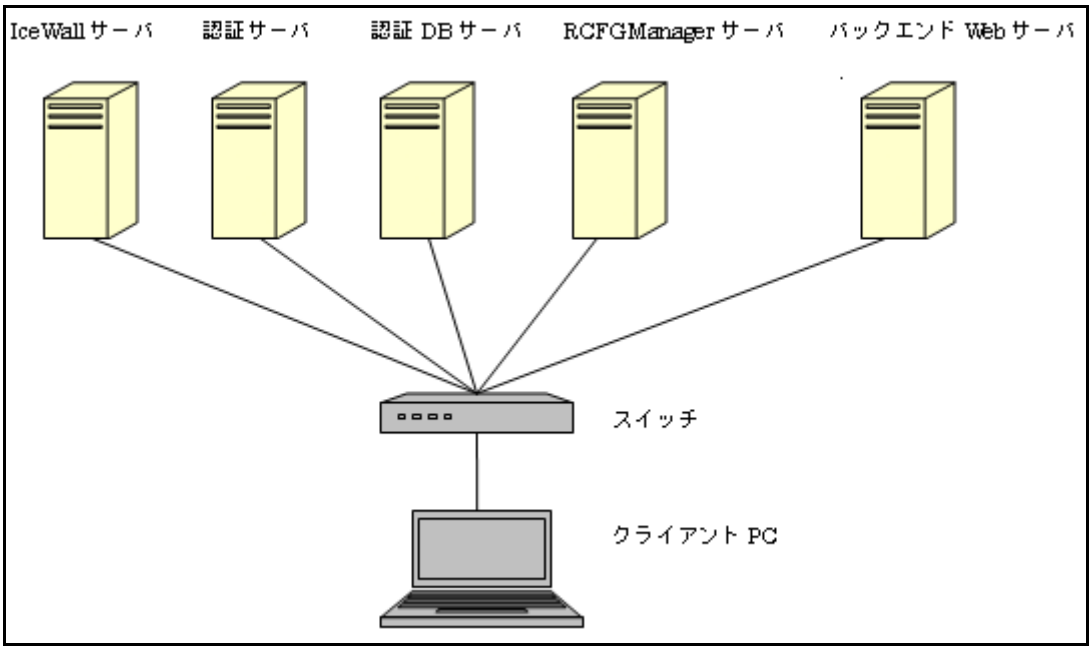


図 7-1　独立テストの構成図

(2) 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である。

a) 独立テストの観点

評価者が､開発者テスト及び提供された評価証拠資料から考案した独立テストの観点を以下に示す。

＜独立テストの観点＞

TOEのセキュリティ機能は､｢IceWall SSO ログイン機能｣､｢IceWall SSO アクセス制御機能｣、及び｢IceWall SSO セキュリティ管理機能｣の3つである。

TSFIは、｢ログインリクエスト｣、｢アクセスリクエスト｣、｢パスワード変更リクエスト｣､及び｢REMOTE CONFIGURATION MANAGERアクセスコントロール設定変更｣の4つである。

限界値分析に関しては、以下の観点で実施する

・パラメタに対する有効値/無効値のテスト
　対象TSFI：　・パスワード変更リクエスト

・機能に対する正常系/異常系のテスト
　対象TSFI：　・ログインリクエスト
　　・アクセスリクエスト
　　・パスワード変更リクエスト
　　・REMOTE CONFIGURATION MANAGER
　　アクセスコントロール設定変更

インタフェースの選択は、下記①～⑤を踏まえ、すべてのインタフェースをテスト対象とした。

① インタフェースの重要性
セキュリティ機能要件を実現する上で主要な役割（｢目的｣）を果たしているインタフェースを選択する。

② インタフェースの複雑性
使用するまでの手順が複雑なインタフェースを選択する。

③ インタフェースの効率性
あるインタフェースにより提供される機能・サービスが、他の複数のインタフェースにより提供される機能･サービスを包含しているインタフェースを選択する。

④ インタフェースの新規性
最新の機能､他の同種タイプの製品には見られない機能を提供するインタフェースを選択する。

⑤ インタフェースの種別

すべてのインタフェース種別を対象とする。

b) **独立テスト概要**

評価者は、上記の観点から考案したテストサブセット用のテスト文書を作成した。これらのテストには、すべてのTSF、及びTSFIが含まれる。

評価者が実施した独立テストの概要は以下のとおりである。

＜独立テスト手法＞

上記インタフェースのテストでは、EAL1 では機能仕様書レベルの情報のみ利用可能のため、限界値分析によるブラックボックステストを実施した。

インタフェースのテストアプローチに関しては、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ブラウザを利用して、TSFI の振る舞いを確認する。

テストを実施する環境は、TOE が動作する OS、Linux 環境と HP-UX 環境の 2 種類である。

＜独立テストツール＞

独立テストにおいて利用したツールを表 7-1 に示す。

表 7-1　独立テストで使用したツール　　上段：Linux版　下段：HP-UX版

	構成品	概要・利用目的
IceWall サーバ		
	OS : Red Hat Enterprise Linux 5.4 x86_64 Web サーバ：Apache HTTP Server 2.2.3	フォワーダーと RCFGAgent が搭載された機器。 ・フォワーダー：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機能。 ・RCFGAgent：RCFGManage からの要求を受けて、設定情報の登録、改変及び削除を行う機能。 本機器は、TOE の動作確認を行うために使用する。
	OS：HP-UX 11i v3 (B.11.31 U ia64) Itanium Web サーバ：Apache-based Web Server v2.2.8 (64bit)	
認証サーバ		
	OS : Red Hat Enterprise Linux 5.4 x86_64 Oracle クライアント：Oracle Net R11.2.0	認証モジュールと RCFGAgent が搭載された機器。 ・認証モジュール：フォワーダーの要求を受け、認証 DB に認証認可情報の問い合わせを行う機

	OS：HP-UX 11i v3 (B.11.31 U ia64) Itanium Oracle クライアント：Oracle Net R11.2.0	能。 ・RCFGAgent：RCFGManage からの要求を受けて、設定情報の登録、改変及び削除を行う機能。 本機器は、TOE の動作確認を行うために使用する。
認証 DB サーバ		
	Oracle サーバ：Oracle DB 11.2.0 EE TOE は､認証 DB サーバのハードや OS に依存しない。TOE は API インタフェースにより認証 DB サーバと連携する。	Oracle サーバが搭載される機器。本機器には、TOE のモジュールは搭載されない。 本機器は、TOE の動作に必要な IT 環境（データの保存）であり、TOE の動作確認を行うために使用する。
RCFGManage サーバ		
	OS : Windows Server 2008 R2 (64bit)	RCFGManage が搭載された機器。 ・RCFGManager：IceWall SSO 管理者により、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を行う機能。 本機器は、TOE の動作確認を行うために使用する。
バックエンド Web サーバ		
	Web サーバ：Apache HTTP Server 2.2.3 TOE は、バックエンド Web サーバのハードや OS に依存しない。TOE は API インタフェースによりバックエンド Web サーバと連携する。	利用者がアクセスする Web コンテンツが置かれた機器。本機器には、TOE のモジュールは搭載されない。 本機器は、TOE の動作確認を行うためのテスト用 Web コンテンツのサーバとして使用する。
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。
クライアント PC		
	OS：Windows XP SP3 2011 年 6 月 17 日現在、Microsoft update 対応済	本機器は、TOE の動作確認を行うための trigger（TSFI への刺激）として使用する。表中に示すツール一式が導入されている。
ブラウザ（クライアント PC）		
	ブラウザ : Internet Explorer 6 SP3	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。

＜独立テストの実施内容＞

独立テストは、評価者によって 18 件実施された（Linux 版 9 件、HP-UX 版 9 件)。独立テストの観点とそれに対応したテスト内容を表 7-2 に示す。

表 7-2 実施した独立テスト

観点	テスト概要
機能に対する正常系/異常系のテスト	登録されたユーザのログイン（パスワード成功）チェック
機能に対する正常系/異常系のテスト	登録されたユーザのログイン（パスワード失敗、アカウントロック）チェック
機能に対する正常系/異常系のテスト	登録されていないユーザのログインチェック
機能に対する正常系/異常系のテスト パラメタに対する有効値/無効値のテスト	パスワード変更チェック
機能に対する正常系/異常系のテスト	アクセスロール・パターン1チェック、及びアクセス制御に関わる属性値の設定
機能に対する正常系/異常系のテスト	アクセスロール・パターン2チェック、及びアクセス制御に関わる属性値の設定
機能に対する正常系/異常系のテスト	アクセスロール・パターン3チェック、及びアクセス制御に関わる属性値の設定
機能に対する正常系/異常系のテスト	アクセスロール・パターン4チェック、及びアクセス制御に関わる属性値の設定
機能に対する正常系/異常系のテスト	アクセス制御に関わる属性値の削除

c) 結果

評価者が実施したすべての独立テストは正しく完了し、評価者は TOE のふるまいを確認した。評価者は、すべてのテスト結果と期待されるふるまいが一致していることを確認した。

7.3.3 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、想定される使用環境と攻撃レベルにおいて懸念される脆弱性となる可能性があるものについて、必要と思われる評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。評価者が実施した侵入テストを以下に説明する。

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

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。

①ログインリクエスト時、パスワード変更時に、入力値が規定サイズで適切に処理されていなければ、バッファオーバーフロー等を引き起こすからもしれない。
②TSFの動作に必要なファイルを削除した場合、予期せぬ動作が発生し、TOEの動作を確認する上で参考となる情報が得られるかもしれない。
③ログインリクエスト時、パスワード変更リクエスト時に、無効な値を入力することによってTOEの処理をバイパスして認証が成立する可能性がある。（SQLインジェクション）
④ログインリクエスト時、パスワード変更リクエスト時に、Postパラメタを不正に操作することによって、予期せぬ動作が起こるかもしれない。
⑤リターンに秘密情報が含まれていた場合、他のユーザの当該情報を利用して不正な行為が成立するかもしれない。
⑥Cookieのハンドリングが適切でない場合、直接アクセスによる不正操作が可能かもしれない。（バイパス）
⑦IceWall SSOに公知の脆弱性として知られるCGIの不備が内在しているかもしれない。その場合、バッファオーバーフロー攻撃や各種インジェクション攻撃が成立する可能性がある。

b) 侵入テストの概要

評価者は、潜在的な脆弱性が悪用される可能性を検出するために、以下の侵入テストを実施した。

＜侵入テスト環境＞

侵入テスト環境は、独立テスト図 7-1 と同じ。侵入テストで使用したツールの詳細は、表 7-1 独立テスト構成に、下記表 7-3 のツールを加えたものとなる。

表 7-3　侵入テストで使用したツール

ツール	概要・利用目的
Fiddler v2.3.3.5 (クライアントPC)	HTTP デバッキングツール ・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 v2.14	汎用 HTTP 脆弱性スキャナツール

(クライアントPC)	・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、2011/6/16現在最新をアップデート済
Nessus v4.4.1 Build 15078 (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、2011/6/16現在最新をアップデート済

＜侵入テスト手法＞

EAL1 の証拠資料レベルにおいては、インタフェースの存在と使い方までが確認可能な設計情報であり、インタフェースを単位として公知の脆弱性の探索確認結果に基づき、悪用可能性を分析し、悪用の懸念がある項目に対してテスト方法を考案した。

テストに使用したツールはインターネット上に公開されているフリーなツールや Nessus といった基本レベルの攻撃者が利用し得るものを採用した。ただし、利用にあたっては HTTP についての技術的な理解が必要である。

利用者が利用する TOE のインタフェースは IceWall サーバの 80/tcp (http) である。従って、侵入テストはこの 80/tcp (http) ポートに対する攻撃に限定して実施した。

(補足 1)
このテスト構成ではクライアント PC からスイッチ経由で認証サーバ等に直接アクセスすることが可能ではあるが、運用環境のセキュリティ対策方針 OE.Setting Environment により、IceWall サーバ以外のサーバにはアクセスしない使用条件となっているため、考慮する必要は無い。

(補足 2)
IceWall サーバは 443/tcp (https) ポートに対するアクセスも受け付けるが、TOE の IT 環境コンポーネントである Apache がクライアントとサーバ間の通信路を暗号化する機能であり、TOE の機能とは関連が無いため、テストは不要であると判断し、テストの範囲外とした。

＜侵入テストの実施項目＞

懸念される脆弱性と対応する侵入テスト内容を表 7-4 に示す。

表 7-4　侵入テスト概要

脆弱性	テスト概要
バッファオーバーフロー確認テスト (ログインリクエスト)	データサイズがオーバーしたパラメタに対する処理が適切になされていることを確認する。
バッファオーバーフロー確認テスト (パスワード変更)	
TSF動作必須設定ファイル不備テスト (cert.grp)	設定不十分状態で、TOEの動作挙動を確認する。（TSFの動作に必要なファイルであるcert.grpを削除した場合、予期せぬ動作が発生しないことを確認する。）
TSF動作必須設定ファイル不備テスト (cert.acl)	設定不十分状態で、TOEの動作挙動を確認する。TSFの動作に必要なファイルであるcert.aclを削除した場合、予期せぬ動作が発生しないことを確認する。
SQLインジェクションテスト (ログインリクエスト)	エンドユーザが入力するSQL文が、識別認証におけるDBとの接続において影響を与えないことを確認する。
SQLインジェクションテスト (パスワード変更リクエスト)	
パラメタ過不足チェックテスト (ログインリクエスト)	構文違反（パラメタの過不足）にて、TOEが予期せぬ動作をしないこと。(パラメタ不備等のエラーメッセージをリターンすること。)
パラメタ過不足チェックテスト (パスワード変更リクエスト)	
Cookieのランダム性確認テスト	リターンに秘密情報が含まれていて、他のユーザの当該情報を利用した不正な行為が成立することがないことを確認する。Cookieのランダム性は実装依存なのでCookieのランダム性が確保されていることの確認
バイパスアクセステスト	Cookieなしのバイパスアクセスが許容されないことを確認する。
汎用スキャンツールテスト (Nessus)	考慮漏れの公知の脆弱性が存在しないことを確認する。バッファオーバーフローやインジェクション攻撃の可能性を検査する。
汎用スキャンツールテスト (Nikto)	

c) **結果**

評価者が実施した侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能

な脆弱性は確認されなかった。

7.4 評価構成について

本評価では、「7.3.2 評価者独立テスト」及び図 7-1 に示す構成において、評価を行った。

本 TOE は、上記と構成要素が大きく異なる構成において、運用される場合はない。よって、評価者は上記の評価構成は適切であると判断した。

7.5 評価結果

評価者は、評価報告書[13]をもって本 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。

評価では以下について確認された。

- PP 適合：PP への適合を主張しない。
- セキュリティ機能要件：　コモンクライテリア　パート２　適合
- セキュリティ保証要件：　コモンクライテリア　パート３　適合

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

- EAL1 適合

評価の結果は、第 2 章に記述された識別に一致する TOE によって構成されたもののみに適用される。

7.6 評価者コメント/勧告

消費者に喚起すべき評価者勧告は、特にない。

8 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解決されていること。

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[13]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。

8.1 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。

8.2 注意事項

特になし。

9 附属書

特になし。

10 セキュリティターゲット

本 TOE のセキュリティターゲット[12]は、本報告書とは別文書として以下のとおり本認証報告書とともに提供される。

HP IceWall SSO セキュリティターゲットバージョン 1.7　2011 年 7 月 11 日
日本ヒューレット・パッカード株式会社

11 用語

本告書で使用された 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用語の定義を以下に示す。

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。
フォワーダー	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。
IceWallサーバ	フォワーダーが動作するサーバ。
認証モジュール	フォワーダーの要求を受け、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。
認証サーバ	認証モジュールが動作するサーバ。
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。
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。
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。
システム管理者	IceWallサーバ、認証サーバ、認証DBサーバ、RCFGManagerサーバといったTOE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。
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)。

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)。
リクエスト制御設定ファイル	フォワーダー等からのリクエストに対して実行可能なリクエスト条件を定義する設定ファイル。
中継（httpリクエストの中継）	フォワーダーは利用者からの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、フォワーダーはバックエンド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。
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。
RCFGManager	IceWall SSO管理者により設定管理操作を行うためのデスクトップアプリケーション。RCFGAgentと連携して、フォワーダー及び認証モジュールの設定操作の処理を行う。
RCFGAgent	IceWallサーバ及び認証サーバに配置され、RCFGManagerからのリクエストに応じて、各フォワーダーまたは各認証モジュールの設定操作の処理を行う。

12 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 平成23年2月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証申請手続等に関する規程, 平成23年2月, 独立行政法人情報処理推進機構, CCM-02

[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, 平成23年2月, 独立行政法人情報処理推進機構, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003

[7] 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3版, 2009年7月, CCMB-2009-07-001, (平成21年12月, 翻訳第1.0版)

[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3版, 2009年7月, CCMB-2009-07-002, (平成21年12月, 翻訳第1.0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3版, 2009年7月, CCMB-2009-07-003, (平成21年12月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004

[11] 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3版, 2009年7月, CCMB-2009-07-004, (平成21年12月, 翻訳第1.0版)

[12] HP IceWall SSO セキュリティターゲット, バージョン1.7, 2011年7月11日, 日本ヒューレット・パッカード株式会社

[13] HP IceWall SSO評価報告書, 第2版, 2011年7月26日, みずほ情報総研株式会社 情報セキュリティ評価室