HP IceWall SSO
セキュリティターゲット

バージョン：2.2

発行日： 2007 年 10 月 17 日

作成者：日本ヒューレット・パッカード株式会社

目次

用語・略語

用語	定義内容
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	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。
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 ブラウザ等を通して 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、Configuration Manager 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。
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。
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。
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。

1. ST 概説

1.1 ST 参照

本 ST の識別情報は以下のとおりである。

ST タイトル：	HP IceWall SSO セキュリティターゲット
ST バージョン：	2.2
ST 作成者：	日本ヒューレット・パッカード株式会社
ST 作成日：	2007 年 10 月 17 日

1.2 TOE 参照

本 TOE の識別情報は以下のとおりである。

TOE 名称：	機能特定（HP IceWall SSO ）
TOE バージョン：	8.0 R2
TOE 開発者：	日本ヒューレット・パッカード株式会社

1.3 TOE 概要

1.3.1 TOE の種別

本 TOE の種別は「その他」である。

1.3.2 主要なセキュリティ機能

本 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 の動作概要は以下の通りである。

- 利用者は、IceWall サーバ（詳細は後述）にアクセスする。
- 認証サーバ（詳細は後述）にて本人確認が行われる。
- 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。
- 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。

また TOE の主要なセキュリティ機能は以下のとおり：

■ 認証機能

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。

■ Web アプリケーション・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に属する利用者のみアクセスを許可する機能。

- 設定構成管理機能

  Web ブラウザからの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登録、改変及び削除できる。

1.3.3 TOE の動作環境

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は下記のとおり。

動作前提条件：

- ID およ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 v2 (B.11.23 U ia64)
  - (Linux 版)
    Red Hat Enterprise Linux AS v.4 Update2 (2.6.9-22) (*1)
    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。
- 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)

  注意事項） ＊2 ：OS ベンダ提供パッケージのみサポート

認証サーバ(certd)の動作環境：

- OS(S/W):
  - (HP-UX 版)HP-UX 11i 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

1.4 TOE 記述

1.4.1 TOE の構成

本 TOE の構成要素は以下のとおり。

(1) TOE 本体

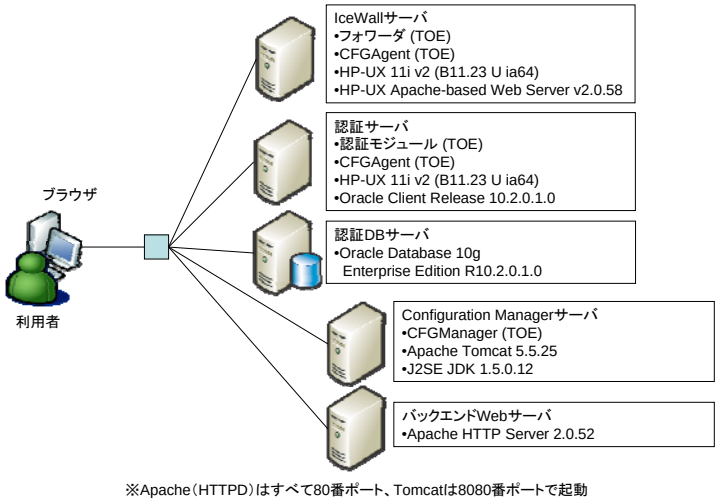

図 1　TOE 本体の構成パターン１：　IceWall サーバ(HP-UX) + 認証サーバ(HP-UX)

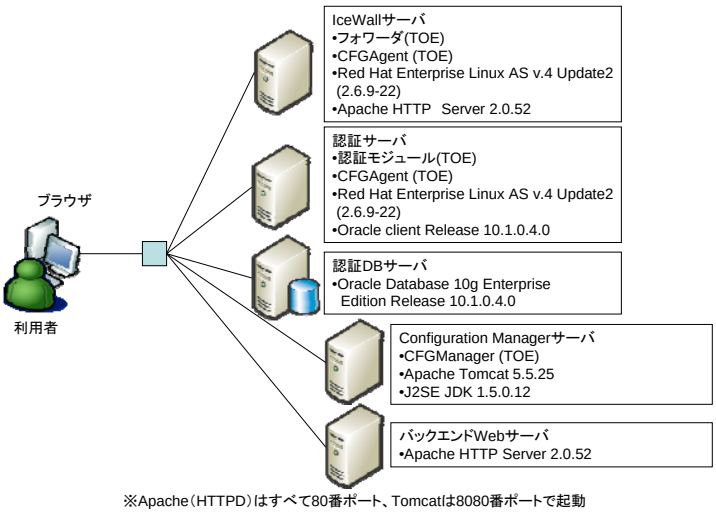

図 2　TOE 本体の構成パターン 2：　IceWall サーバ(Linux) + 認証サーバ(Linux)

IceWall サーバ：

TOE であるフォワーダが動作するサーバ。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。

認証サーバ：

TOE である認証モジュールが動作するサーバ。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。

認証 DB サーバ：

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

Configuration Manager サーバ:

TOE である Configuration Manager（CFGManager）が動作するサーバ。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。

バックエンド Web サーバ：

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。

(2)添付されるガイダンス文書

- 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

1.4.2 TOE のセキュリティ機能

TOE のセキュリティ機能は以下のとおり：

■ 認証機能（フォワーダ, 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および認証を行う機能。

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

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。

2. 適合主張

2.1 CC 適合主張

本 ST は、以下の通り CC 適合を主張する。

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　2006 年 9 月　バージョン 3.1　翻訳第 1.2 版
パート 2:セキュリティ機能コンポーネント　2006 年 9 月　バージョン 3.1　翻訳第 1.2 版
パート 3:セキュリティ保証コンポーネント　2006 年 9 月　バージョン 3.1　翻訳第 1.2 版
CC パート 2 適合
CC パート 3 適合

2.2 PP 主張、パッケージ主張

本 ST は、以下の通り PP、パッケージ適合を主張する。

PP：　　PP への適合を主張しない。
パッケージ：　　EAL1 適合

3. セキュリティ対策方針

3.1 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、Configuration Manager 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、Configuration Manager サーバ、およびバックエンド 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、Configuration Manager サーバ、およびバックエンド 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。

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. 拡張コンポーネント定義

本 ST には、拡張コンポーネントはない。

5. セキュリティ要件

5.1 セキュリティ機能要件

(1) ログイン制限

FIA_UID.2	**アクション前の利用者識別**
下位階層:	FIA_UID.1 識別のタイミング
依存性:	なし
FIA_UID.2.1	TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

FIA_UAU.2	**アクション前の利用者認証**
下位階層:	FIA_UAU.1 認証のタイミング
依存性:	FIA_UID.1 識別のタイミング
FIA_UID.2.1	TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

FIA_AFL.1	**認証失敗時の取り扱い**
下位階層:	なし
依存性:	FIA_UAU.1 認証のタイミング
FIA_AFL.1.1	**TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付: 正の整数値]*、*[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]回の不成功認証試行が生じたときを検出しなければならない。** [割付: *認証事象のリスト*] *前回の認証成功後以降に連続した不成功認証試行回数* [選択: *[割付: 正の整数値]*、*[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*] *[割付: 正の整数値]* *5*
FIA_AFL.1.2	**不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付: *アクションのリスト*]をしなければならない。** *[割付: アクションのリスト]* *アカウントをロックする。*

(3) ファイルに対するアクセスの制御

FDP_ACC.1 **サブセットアクセス制御**

下位階層: なし
依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACC.1.1 **TSF は、[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御 SFP*]を実施しなければならない。**

[割付: アクセス制御 SFP]
URL アクセスコントロール規則

[割付: サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト]

サブジェクトのリスト	*フォワーダが動作する httpd（利用者の代替となるプロセス）*
オブジェクトのリスト	*バックエンド Web サーバへの http リクエスト*
操作のリスト	*中継*

FDP_ACF.1 **セキュリティ属性によるアクセス制御**

下位階層: なし
依存性: FDP_ACC.1 サブセットアクセス制御
FMT_MSA.3 静的属性初期化

FDP_ACF.1.1 **TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御 SFP*]を実施しなければならない。**

[割付: アクセス制御 SFP]
URL アクセスコントロール規則

[割付: 示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ]

サブジェクト	セキュリティ属性
フォワーダが動作する httpd（利用者の代替となるプロセス）	• *ユーザ ID* • *グループ ID* • *IP アドレス*

オブジェクト	セキュリティ属性
バックエンド Web サーバへの http リクエスト	*URL*

FDP_ACF.1.2 **TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、次の規則を実施しなければならない: [割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]。**

[割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]
サブジェクトの属性、オブジェクトの属性、そして（グループ設定ファイル、アクセスコントロールファイル、リクエスト制御設定ファイルによって定義される）アクセスポリシーを照合して条件評価を行う。条件が合致した場合は、サブジェクトがオブジェクトを中継する。グループ設定によって、ユーザ ID、IP アドレスよりグループ ID がサブジェクトに関連付けられる。

FDP_ACF.1.3 **TSF は、次の追加規則、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。**

[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則] *なし*

FDP_ACF.1.4 **TSF は、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。**

[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則] *なし*

FIA_USB.1 **利用者-サブジェクト結合**

下位階層: なし
依存性: FIA_ATD.1 利用者属性定義

FIA_USB.1.1 **TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。: [割付: *利用者セキュリティ属性のリスト*]**

[割付: 利用者セキュリティ属性のリスト]
- *グループ ID*
- *IP アドレス*

FIA_USB.1.2 **TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。: [割付: *属性の最初の関連付けの規則*]**

[割付: 属性の最初の関連付けの規則] *なし*

FIA_USB.1.3	**TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。: [割付: *属性の変更の規則*]**
	[割付: 属性の変更の規則] *なし*

FIA_ATD.1	**利用者属性定義**
下位階層:	なし
依存性:	なし
FIA_ATD.1.1	**TSF は、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない。: [割付: *セキュリティ属性のリスト*]**
	[割付: セキュリティ属性のリスト] *IP アドレス、グループ ID*

(6) 認証データの保護

FMT_MTD.1	**TSF データの管理**
下位階層:	なし
依存性:	FMT_SMR.1 セキュリティの役割 FMT_SMF.1 管理機能の特定
FMT_MTD.1.1	**TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付: 許可された識別された役割]に制限しなければならない。**
	[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]] *改変* *[割付: TSF データのリスト]* *利用者自身のパスワード* *[割付: 許可された識別された役割]* *利用者*

FMT_SMR.1(1)	**セキュリティの役割 (1)**
下位階層:	なし
依存性:	FIA_UID.1 識別のタイミング
FMT_SMR.1.1(1)	**TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。**
	[割付: 許可された識別された役割] *利用者*

FIA_SOS.1	**秘密の検証**
下位階層:	なし
依存性:	なし
FIA_SOS.1.1	**TSF は、秘密が[割付: *定義された品質尺度*]に合致することを検証するメカニズムを提供しなければならない。** *[割付: 定義された品質尺度]* *以下の条件を満たしたパスワードが認証データとして受け入れられる。* - *最小パスワード長: 3* - *最大パスワード長:6* - *文字種：英小文字【a ～ z】、英大文字【A ～ Z】、英数字【0 ～ 9】記号【 ! " # $ % & ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~ 】*

(7) アクセス制御に関わる属性値の設定と保護

FMT_MSA.1(1)	**セキュリティ属性の管理 (1)**
下位階層:	なし
依存性:	[FDP_ACC.1 サブセットアクセス制御、または FDP_IFC.1 サブセット情報フロー制御] FMT_SMR.1 セキュリティの役割 FMT_SMF.1 管理機能の特定
FMT_MSA.1.1(1)	**TSF は、セキュリティ属性[割付: *セキュリティ属性のリスト*]に対し[選択: *デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]*]をする能力を[割付: *許可された識別された役割*]に制限する[割付: *アクセス制御 SFP、情報フロー制御 SFP*]を実施しなければならない。** *[割付: アクセス制御 SFP、情報フロー制御 SFP]* *URL アクセスコントロール規則* [選択: *デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]*] *改変、削除、[割付: その他の操作]* *[割付: その他の操作]* 登録 *[割付: セキュリティ属性のリスト* - *ユーザ ID* - *グループ ID* - *IP アドレス* *[割付: 許可された識別された役割]* *IceWall SSO 管理者*

FMT_SMR.1(2)	**セキュリティの役割 (2)**
下位階層:	なし
依存性:	FIA_UID.1 識別のタイミング

FMT_SMR.1.1(2)	**TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。** *[割付: 許可された識別された役割]* *IceWall SSO 管理者*

FMT_MSA.1(2)	**セキュリティ属性の管理 (2)**
下位階層:	なし
依存性:	[FDP_ACC.1 サブセットアクセス制御、または FDP_IFC.1 サブセット情報フロー制御] FMT_SMR.1 セキュリティの役割 FMT_SMF.1 管理機能の特定
FMT_MSA.1.1(2)	**TSF は、セキュリティ属性[割付: *セキュリティ属性のリスト*]に対し[選択: *デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]*]をする能力を[割付: *許可された識別された役割*]に制限する[割付: *アクセス制御 SFP、情報フロー制御 SFP*]を実施しなければならない。** *[割付: アクセス制御 SFP、情報フロー制御 SFP]* *URL アクセスコントロール規則* *[選択: デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]]* *[割付: その他の操作]* *登録* *[割付: セキュリティ属性のリスト]* *URL* *[割付: 許可された識別された役割]* *IceWall SSO 管理者*

(8) セキュリティ管理機能の定義

FMT_SMF.1	**管理機能の特定**
下位階層:	なし
依存性:	なし
FMT_SMF.1.1	**TSF は、以下の管理機能を実行することができなければならない。: [割付: *TSF によって提供される管理機能のリスト*]** *[割付: TSF によって提供される管理機能のリスト]* - *利用者による利用者自身のパスワード変更機能* - *IceWall SSO 管理者による URL アクセス制御機能のグループ設定機能* - *IceWall SSO 管理者による URL アクセス制御機能の ACL 設定機能*

5.2 セキュリティ保証要件

本 TOE の評価保証レベルは EAL1 であり、CC パート 3 に規定された EAL1 の保証要件コンポーネントを使用する。

5.3 セキュリティ要件根拠

FDP_ACF.1 から FMT_MSA.3 への依存性が除去できる理由を以下に示す。

FMT_MSA.3 は、セキュリティ属性のデフォルト値に制限的、許可的、またはその他の特性を付与すること、付与されたデフォルト値を代替する初期値を指定することを規定している。

しかし、本件ではデフォルト値、初期値に関係なく、管理者がセキュリティ属性の設定管理を行うことを規定すれば十分である。

よって、FDP_ACF.1 から FMT_MSA.3 への依存性は不要である。

6. TOE 要約仕様

「IceWall SSO ログイン機能（識別認証（1）ログイン制限（a））」(FIA_UID.2/FIA_UAU.2)

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を開始する際に、フォワーダは認証モジュールと連携して、ユーザ ID、パスワードによる識別認証を行う。

識別認証されると、認証モジュールはセッション ID を発行し、フォワーダは利用者に引き渡す。次アクセス以降は、http リクエストに含まれるセッション ID が発行されたものと一致した場合に、セッション ID と関連付けられる利用者と判断する。

「IceWall SSO ログイン機能（識別認証（1）ログイン制限（c））」(FIA_AFL.1)

認証モジュールは、利用者の識別認証における 5 回の連続不成功認証を検知すると、当該利用者のアカウントをロックする。

「IceWall SSO アクセス制御機能（アクセス制御（3）ファイルに対するアクセス制御(a))」(FDP_ACC.1/FDP_ACF.1/FIA_USB.1/FIA_ATD.1)

利用者からバックエンド Web サーバへの http リクエストをフォワーダが受信した際、認証モジュールと連携して URL アクセスコントロール規則に定義されているアクセスポリシーを照合して条件評価を行い、条件が合致した場合のみ http リクエストをバックエンド Web サーバに中継を行う。

URL アクセスコントロール規則：

ユーザ ID 及び IP アドレスによって決定されるグループ ID とバックエンドサーバへの URL に基づいて、利用者から受信した HTTP リクエストをバックエンド Web サーバに中継を行うための評価条件を定義した規則

「IceWall SSO セキュリティ管理機能（認証データの保護（6）認証データの登録・変更・参照などの制限(a)」(FMT_MTD.1/FMT_SMR.1(1))

利用者による利用者自身のパスワードの変更を許す。フォワーダは認証モジュールと連携してパスワード変更処理を行う。

「IceWall SSO セキュリティ管理機能（認証データの保護（6）認証データの安全性の検査(b)」(FIA_SOS.1)

利用者が入力した利用者自身のパスワードに対して、フォワーダはパスワードポリシーへの適合性を検査し、ポリシーを満たしたパスワードのみによる更新変更を許す。

- 最小パスワード長: 3 桁
- 最大パスワード長: 6 桁

- 文字種： 英小文字【a ～ z】、英大文字【A ～ Z】、英数字【0 ～ 9】、記号【 ! " # $ % & ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~ 】

「IceWall SSO セキュリティ管理機能（セキュリティ管理 (7)アクセス制御に関わる属性値の設定と保護(a)）」(FMT_MSA.1(1)/FMT_SMR.1(2))

IceWall ログイン機能により、IceWall SSO 管理者のみに CFGManager を通して URL アクセスコントロール規則で利用するユーザ ID、IP アドレス、及びグループ ID の設定を許可する。CFGManager は CFGAgent と連携し、設定の操作処理を行う。

「IceWall SSO セキュリティ管理機能（セキュリティ管理 (7)アクセス制御に関わる属性値の設定と保護(c)）」(FMT_MSA.1(2)/FMT_SMR.1(2))

IceWall ログイン機能により、IceWall SSO 管理者のみに CFGManager を通して IceWall SSO 管理者のみに URL アクセスコントロール規則で利用する URL の設定を許可する。CFGManager は CFGAgent と連携し、設定の操作処理を行う。

「IceWall SSO セキュリティ管理機能（セキュリティ管理 (8)セキュリティ管理機能の定義(a)）」(FMT_SMF.1)

フォワーダ、認証モジュール、CFGManager および CFGAgent により、以下のセキュリティ管理機能を有する。

- 利用者による利用者自身のパスワード変更機能
- IceWall SSO 管理者による URL アクセス制御機能のグループ設定機能
- IceWall SSO 管理者による URL アクセス制御機能の ACL 設定機能