PROCENTER Web 版
セキュリティターゲット

バージョン：1.8

発行日： 2008 年 3 月 24 日

作成者：株式会社 NEC 情報システムズ

更新履歴

バージョン	変更概要	変更箇所		変更日	変更者
		章・節・項	内容		
1.0	初版	―	―	2008/1/11	株式会社 NEC 情報システムズ
1.1	機能要件の追加 【TSF データの管理(2)】	5. セキュリティ要件 (5) アカウント管理 6. TOE 要約仕様 セキュリティ管理(5) アカウント管理(a)	TOE との整合確認を反映	2008/1/21	株式会社 NEC 情報システムズ
1.2	記述の見直し	5. セキュリティ要件 6. TOE 要約仕様	TOE との整合確認を反映	2008/2/14	株式会社 NEC 情報システムズ
1.3	記述の見直し	5. セキュリティ要件 6. TOE 要約仕様	TOE との整合確認を反映	2008/3/6	株式会社 NEC 情報システムズ
1.4	記述の見直し	5. セキュリティ要件 6. TOE 要約仕様	TOE との整合確認を反映	2008/3/7	株式会社 NEC 情報システムズ
1.5	記述の見直し	1. ST 概説 5. セキュリティ要件 6. TOE 要約仕様	TOE との整合確認を反映	2008/3/17	株式会社 NEC 情報システムズ
1.6	記述の見直し	1. ST 概説	TOE との整合確認を反映	2008/3/19	株式会社 NEC 情報システムズ
1.7	記述の見直し	3. セキュリティ対策方針	TOE との整合確認を反映	2008/3/24	株式会社 NEC 情報システムズ
1.8	記述の見直し	1. ST 概説	TOE との整合確認を反映	2008/3/24	株式会社 NEC 情報システムズ

目次

用語・略語

用語	定義内容
利用者	TOE が提供するサービスを利用する人。利用者はその役割により、管理者と一般利用者に分かれる。利用者のことをユーザとも呼ぶ。
ユーザ ID	利用者を識別するための ID。利用者のユーザ情報における「社員番号」が利用者を識別するための ID となる。
ユーザ情報	利用者の性質を表す情報。「ユーザ名」「社員番号」「役職」「所属」等がある。
管理者	TOE に対して設定・管理を行うための特別な権限を持つ利用者。管理者はその役割により、システム管理者、ユーザ管理者、グループ管理者に分かれる。
一般利用者	管理者としての特別な権限を持たない利用者。
システム管理者	システム管理権限を有する管理者。
システム管理権限	ノードアクセス権リストやロック状態にかかわらず、すべてのノードに対して参照・更新・削除が行える権限。システム管理権限は、ユーザ管理権限、グループ管理権限を包括する。
ユーザ管理者	ユーザ管理権限を有する管理者。
ユーザ管理権限	利用者の登録・更新・削除が行える権限。ユーザ管理権限は、グループ管理権限を包括する。
グループ管理者	グループ管理権限を有する管理者。
グループ管理権限	グループの登録や削除、利用者の所属グループを変更できる権限。
グループ	複数の利用者をまとめたもの。グループに対して設定したアクセス権レベルは、そのグループに所属するすべての利用者に対して適用される。利用者は複数のグループに所属することができる。
グループ ID	グループを識別するための ID。
グループ情報	グループの性質を表す情報。「名前(グループ名)」「説明」がある。
ノード	TOE が保持する論理的なデータ構造の構成要素。利用者はノードに対して実体ファイルと属性情報を登録することができる。ノードはその役割により、フォルダノード、ファイルノード、URL ノードに分かれる。実体ファイルが登録できるのはファイルノードだけである。
フォルダノード	階層構造を構築するためのノード。階層構造上、あるノードを基準として直上のノードを親ノード、直下のノードを子ノード、配下のノードを配下ノードと呼ぶ。フォルダノードは子ノードとして複数のノードを保持することができる。最上位のノードを除き、すべてのノードには必ず親ノードが 1 つ存在する。
ファイルノード	実体ファイルを登録できるノード。１つのファイルノードに対し、複数の実体ファイルを登録することができる。
URL ノード	属性情報の１つとして URL を登録できるノード。
ノードアクセス権リスト	あるノードに対して設定されたアクセス権の集合。
アクセス権	利用者もしくはグループに対するアクセス権レベル（操作権限）。
アクセス権レベル	アクセス権レベルには［表示(V)］［読み込み(VR)］［書き込み(VRW)］［削除(VRWD)］があり、それぞれ後者の権限は、前者の権限を包括する。付与されたアクセス権レベルにより、利用者にはノードに対する下記の操作が許可される。 ・［表示(V)］　　... 属性参照 ・［読み込み(VR)］... 実体参照（ファイルノードの場合） ・［書き込み(VRW)］... 属性情報の更新

	実体ファイルの登録・更新（ファイルノードの場合） 子ノードの新規作成（フォルダノードの場合） ・[削除(VRWD)]　...ノードの削除（ファイルノードの場合は登録されている実体ファイルも削除される。フォルダノードの場合は配下ノードも削除される）
実体ファイル	OS 上ファイルとして管理されるデータ単位（いわゆるファイルのこと）。ファイルノードとの違いを明確化するため､TOE に登録するファイルのことを実体ファイルと呼ぶ。
実体参照	ノードに登録された実体ファイルを参照すること。
実体更新	ノードに登録された実体ファイルを更新すること。登録された実体ファイルを削除すること、実体ファイルを追加登録することも含まれる。
属性情報	ノードの性質を表す文字列または数値による情報。「名前」、「ステータス」、「備考」「URL」等がある。
属性参照	ノードに登録された属性情報を参照すること。
属性更新	ノードに登録された属性情報を更新すること。
オーナ	ノードの所有者のこと。ノードを作成した利用者がそのノードのオーナとなる。オーナはそのノードに対して、ノードアクセス権リストを変更することができる。
オーナ属性	ノードのオーナを特定するための情報を管理する属性。オーナ属性の値はオーナのユーザ ID となる。
ロック	あるノードに対して、ロック状態にすること。フォルダノード以外のノードに対して実行可能である。
ロックオーナ	ロックを実行している利用者のこと。システム管理者またはノードに対して[書き込み(VRW)]もしくは[削除(VRWD)]権限が付与された利用者がロックオーナになり得る。
ロックオーナ属性	ノードのロックオーナを特定するための情報を管理する属性。ノードがロックされている場合､ロックオーナ属性の値はロックオーナのユーザ IDとなる。ノードがロックされていない場合､ロックオーナ属性の値はブランクとなる。
ロック状態	ノードアクセス権リストによらず、ロックオーナ以外の利用者（システム管理者を除く）による実体ファイルと属性情報の更新・削除を禁止する状態。ファイルノードがロック状態の場合、登録されている実体ファイルは、ロックオーナ以外の利用者（システム管理者を除く）が更新・削除することはできない。
ロック解除	ロックされたノードに対して、ロック状態を解除する操作のこと。ロック解除はロックオーナと、システム管理者が実行できる。
PROCENTER サーバ	TOE を稼動するために必要なハードウェアと､そのハードウェア上で動作する TOE を稼動するために必要なソフトウェア。
PROCENTER サーバソフトウェア	TOE の各機能を提供するためのソフトウェア。
PROCENTER Web サーバソフトウェア	TOE の各機能を Web ブラウザから利用するための機能･インタフェースを提供するためのソフトウェア。
FW	Firewall(ファイアウォール)の略。
Firewall	ネットワーク上で特定の IP アドレス及びポートからのアクセスをフィルタリングするアプリケーション。

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：	PROCENTER Web 版 セキュリティターゲット
ST バージョン：	1.8
ST 作成者：	株式会社 NEC 情報システムズ
ST 作成日：	2008 年 3 月 24 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（PROCENTER Web 版）
TOE バージョン：	3.6
TOE 開発者：	株式会社 NEC 情報システムズ

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 は文書・コンテンツ管理システムであり、実体ファイルや属性情報に関して登録、更新、参照、削除、検索するための機能を提供する。

本 TOE は登録された実体ファイルや属性情報への不正アクセスを防止するセキュリティ機能として、TOE 利用者の識別及び認証、TOE 利用者の役割及びアクセス権設定に基づいてノードに対するアクセス制御を行っている。

本 TOE を使用するにはシステム管理者が利用者を登録し、利用者は識別認証された後、アクセス制御により許可される範囲内で、登録、更新、参照、削除、検索機能を利用する。

本 TOE の主要なセキュリティ機能は以下の通りである。

- 識別認証機能：TOE 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、TOE 利用者の識別と認証を行う機能。
- アクセス制御機能：TOE 利用者の役割及びアクセス権設定に基づいてノードに対するアクセス制御を行う機能。

1.3.3 TOE の動作環境

本 TOE が必要とする動作環境は以下の通りである。

■ PROCENTER サーバ

【ハードウェア】

- メモリー：1GB 以上
- ハードディスク： 600MB 以上
- Microsoft Windows Server 2003 SP2 が動作するサーバ機器

【ソフトウェア】

- OS：Microsoft Windows Server 2003 SP2
- Web サーバ：IIS6.0
- ServletContainer：Adobe JRun4 Professional Edition (Updater6 適用必須)
- Java:1.4.2_14
- データベース：Oracle Database 10g Release2

■ 利用者端末

【ハードウェア】

- Microsoft Internet Explorer 6.0 SP2 が動作するクライアント機器

【ソフトウェア】

- OS：Microsoft Internet Explorer 6.0 SP2 が動作する OS
- Web ブラウザ：Microsoft Internet Explorer 6.0 SP2

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

■ TOE の物理的範囲

本 TOE 範囲は、PROCENTER サーバ上で稼動する「PROCENTER サーバソフトウェア」及び「PROCENTER Web サーバソフトウェア」である。TOE を稼動させるために、 PROCENTER サーバには、サーバ機器(ハードウェア)、OS、データベース、Java、ServletContainer、Web サーバが必要となる。

PROCENTER サーバと LAN またはインターネットとの間には FW を設置し、利用者からのリクエストによる HTTPS プロトコル通信だけを通すように制御する。

利用者は LAN またはインターネット上の利用者端末から Web ブラウザを使用し、指定された URL より PROCENTER サーバにアクセスする。利用者が TOE を利用するために、利用者端末には、クライアント機器（ハードウェア)、OS、Web ブラウザが必要となる。

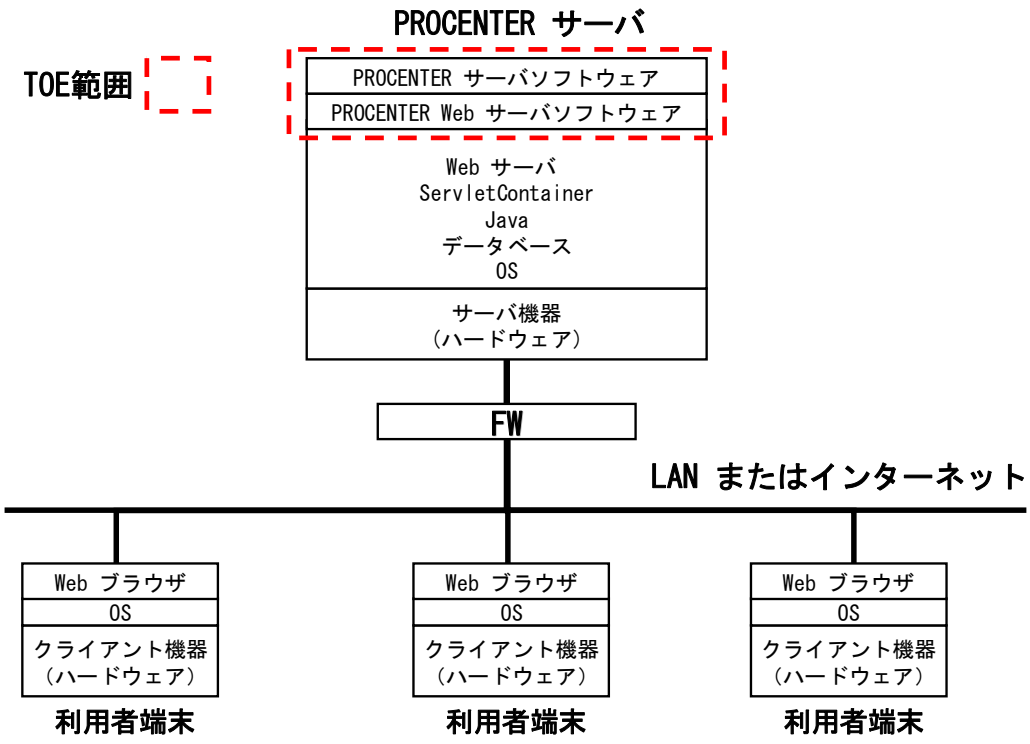

図１． TOE の物理的範囲

■ TOE の論理的範囲

本 TOE 範囲の各機能を以下に記述する。

利用者は識別認証機能で識別認証に成功した場合に TOE が利用可能となる。識別認証機能において利用者が識別される。

利用者が利用できる機能は、ユーザ管理機能、アクセス権管理機能、ファイル管理機能、フォルダ管理機能、URL 管理機能、検索機能である。

- ユーザ管理機能

  ユーザ管理機能は、ユーザ ID に関して登録、削除、参照を行う機能とパスワードの改変を行う機能である。

- アクセス権管理機能

  アクセス権管理機能は、ノードアクセス権リストに関して更新、削除、参照を行う機能と、利用者が所属するグループの追加、削除を行う機能である。

- ファイル管理機能

  ファイル管理機能は、ファイルノードを実体ファイル・属性情報とともに登録、更新、削除、参照する機能である。ノードの登録、更新、削除、参照は、ノードアクセス権リストに基づいてアクセス制御される。ファイルノードをロック状態にすることで、ロックオーナ以外（システム管理者を除く）による更新、削除を禁止することができる。

- フォルダ管理機能

  フォルダ管理機能は、フォルダノードを属性情報とともに登録、更新、削除、参照する機能である。ノードの登録、更新、削除、参照は、ノードアクセス権リストに基づいてアクセス制御される。

- URL 管理機能

  URL 管理機能は、URL ノードを属性情報とともに登録、更新、削除、参照する機能である。ノードの登録、更新、削除、参照は、ノードアクセス権リストに基づいてアクセス制御される。URL ノードをロック状態にすることで、ロックオーナ以外（システム管理者を除く）による更新、削除を禁止することができる。

- 検索機能

  検索機能は、属性情報を検索キーにして、ファイルノード、フォルダノード、URL ノードを検索する機能である。検索されるノードは、アクセス制御機能によって、検索実行者が［表示(V)］権限を持つノードに限定される。

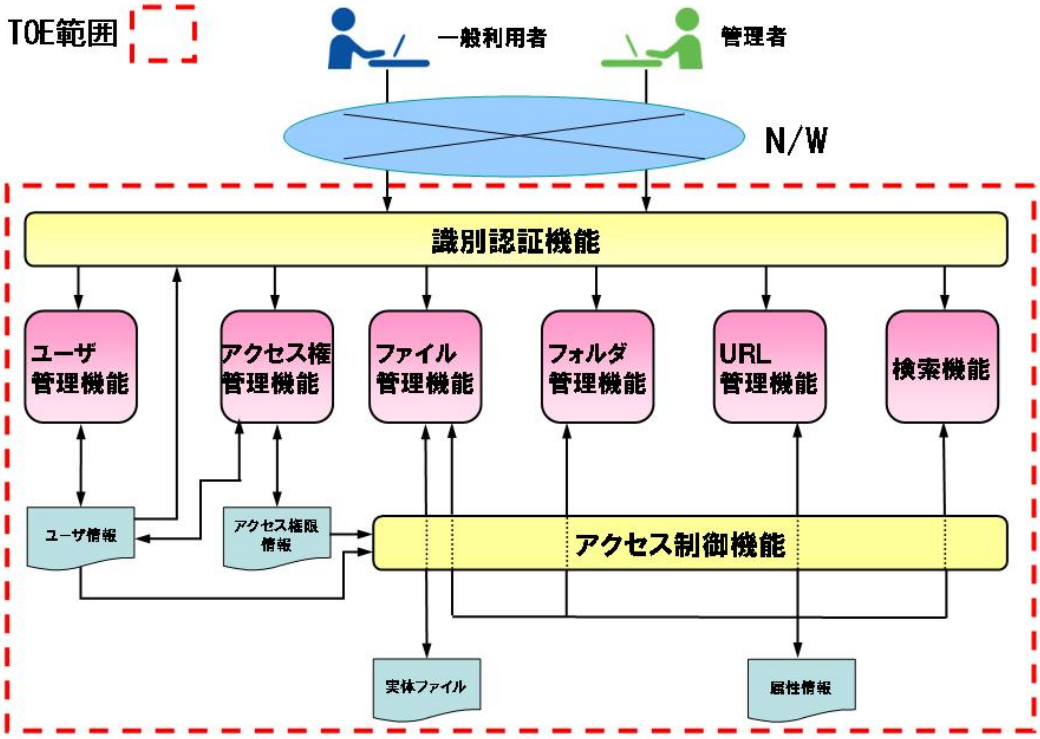

図２．TOE の論理的範囲

(2)添付されるガイダンス文書

- PROCENTER AMIGO ユーザーズガイド Version1.3 (2008/3/17)
- PROCENTER AMIGO ユーザーズガイド 補足 Version1.3 (2008/3/17)
- PROCENTER サーバ Version 3.6 インストールガイド Version1.2 (2008/3/10)
  (PROCENTER サーバソフトウェアのインストールガイド)
- PROCENTER AMIGO インストールガイド JRun4 用 Version1.2 (2008/2/26)
  (PROCENTER Web サーバソフトウェアのインストールガイド)
- PROCENTER Web 版 はじめにお読みください Version1.4 (2008/3/24)

1.4.2 TOE のセキュリティ機能

本 TOE は文書・コンテンツ管理システムであり、実体ファイルや属性情報に関して登録、更新、参照、削除、検索するための機能を提供する。

本 TOE は登録された実体ファイルや属性情報への不正アクセスを防止するセキュリティ機能として、TOE 利用者の識別及び認証、TOE 利用者の役割及びアクセス権設定に基づいてノードに対するアクセス制御を行っている。

本 TOE を使用するにはシステム管理者が利用者を登録し、利用者は識別認証された後、

アクセス制御により許可される範囲内で、登録、更新、参照、削除、検索機能を利用する。

本 TOE の主要なセキュリティ機能は以下の通りである。

- 識別認証機能：TOE 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、TOE 利用者の識別と認証を行う機能。
- アクセス制御機能：TOE 利用者の役割及びアクセス権設定に基づいてノードに対するアクセス制御を行う機能。

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.TRUSTED_ROLE（信頼される役割）
システム管理者、ユーザ管理者、グループ管理者には、各役割に適した者を任命しなければならない。

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認証情報（パスワード）を記憶し、他人に漏らしてはならない。また推測・解析されやすい認証情報（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。認証情報（パスワード）は半角

英数文字を組み合わせた 8 文字以上で設定しなければならない。

OE.SECURE_USE（セキュアな利用）
すべての利用者は、利用者ガイダンスを読んで、TOE をセキュアに利用するための自身の役割と必要な操作を理解した上で TOE を利用しなければならない。

OE.SAFE_PLACE（安全な設置場所）
PROCENTER サーバは、適切に入退場管理された場所に設置されなければならない。

OE.FIREWALL（ファイアウォールの設置）
LAN またはインターネットと TOE が稼動する PROCENTER サーバは FW によって分離され、利用者端末から PROCENTER サーバへのアクセスは FW を経由するように設置しなければならない。FW は利用者からのリクエストによる HTTPS プロトコル通信だけを通すように設定しなければならない。

OE.OS（OS の運用管理）
PROCENTER サーバ上の OS の運用管理は、OS を運用管理するために必要なスキルと知識を持った要員が行わなければならない。

OE.DATABASE（データベースの運用管理）
PROCENTER サーバ上のデータベースの運用管理は、データベースを運用管理するために必要なスキルと知識を持った要員が行わなければならない。

OE.WEBSERVER（Web サーバの運用管理）
PROCENTER サーバ上の Web サーバの運用管理は、IIS、ServletContainer を運用管理するために必要なスキルと知識を持った要員が行わなければならない。

OE.CLIENT（クライアント端末の運用管理）
TOE に接続する利用者端末は、OS の利用者認証機能を有効にし、他人のメモリ領域・ディスク領域に不正アクセスできないように設定しなければならない。

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。

(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*] ノードアクセス制御規則 [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	利用者プロセス
オブジェクトのリスト	フォルダノード、ファイルノード、 URL ノード
操作のリスト	新規作成、属性参照、実体参照、 属性更新、実体更新、削除

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*]
ノードアクセス制御規則

[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
利用者プロセス	ユーザ ID

オブジェクト	セキュリティ属性
フォルダノード、 ファイルノード、 URL ノード	ノードアクセス権リスト(ユーザ ID を含む)、 ロックオーナ属性

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*]
ノードアクセス権リストにグループ ID が存在する場合は、対象グループに所属するすべての利用者のユーザ ID について適用する。
①以下の条件を満たす場合に、ノードに対する属性参照が許可される。
・サブジェクトセキュリティ属性のユーザ ID と一致する値が、オブジェクトセキュリティ属性であるノードアクセス権リストに存在し、かつ当該属性と関連付けられるアクセス権レベルに[表示(V)]または[読み込み(VR)]または[書き込み(VRW)]または[削除(VRWD)]が設定されている場合。
②以下の条件を満たす場合に、ファイルノードに対する実体参照が許可される。
・サブジェクトセキュリティ属性のユーザ ID と一致する値が、オブジェクトセキュリティ属性であるノードアクセス権リストに存在し、かつ当該属性と関連付けられるアクセス権レベルに[読み込み(VR)]または[書き込み(VRW)]または[削除(VRWD)]が設定されている場合。
③以下の条件をすべて満たす場合に、ノードに対する属性更新が許可される。
・サブジェクトセキュリティ属性のユーザ ID と一致する値が、オブジェクトセキュリティ属性であるノードアクセス権リストに存在し、かつ当該属性と関連付けられるアクセス権レベルに[書き込み(VRW)]または[削除(VRWD)]が設定されている場合。
・オブジェクトセキュリティ属性であるロックオーナ属性がブランクの場合（ロックされていない場合)、もしくはサブジェクトセキュリティ属性のユーザ ID と一致する値が設定されている場合（自身がロックしている場合)。
④以下の条件を満たす場合に、フォルダノードに対する子ノードの新規作成が

	許可される。 ・サブジェクトセキュリティ属性のユーザ ID と一致する値が、オブジェクトセキュリティ属性であるノードアクセス権リストに存在し、かつ当該属性と関連付けられるアクセス権レベルに[書き込み(VRW)]または[削除(VRWD)]が設定されている場合。 ⑤以下の条件をすべて満たす場合に、ファイルノードに対する実体更新が許可される。 ・サブジェクトセキュリティ属性のユーザ ID と一致する値が、オブジェクトセキュリティ属性であるノードアクセス権リストに存在し、かつ当該属性と関連付けられるアクセス権レベルに[書き込み(VRW)]または[削除(VRWD)]が設定されている場合。 ・オブジェクトセキュリティ属性であるロックオーナ属性がブランクの場合（ロックされていない場合)、もしくはサブジェクトセキュリティ属性のユーザ ID と一致する値が設定されている場合（自身がロックしている場合)。 ⑥以下の条件をすべて満たす場合に、ファイルノード、URL ノードの削除が許可される。 ・サブジェクトセキュリティ属性のユーザ ID と一致する値が、オブジェクトセキュリティ属性であるノードアクセス権リストに存在し、かつ当該属性と関連付けられるアクセス権レベルに[削除(VRWD)]が設定されている場合。 ・前述の値が、親ノードのノードアクセス権リストに存在し、かつ当該属性と関連付けされるアクセス権レベルに[書き込み(VRW)]または[削除(VRWD)]が設定されている場合。 ・オブジェクトセキュリティ属性であるロックオーナ属性がブランクの場合（ロックされていない場合)、もしくはサブジェクトセキュリティ属性のユーザ ID と一致する値が設定されている場合（自身がロックしている場合)。 ⑦以下の条件をすべて満たす場合に、フォルダノードの削除が許可される。 ・サブジェクトセキュリティ属性のユーザ ID と一致する値が、オブジェクトセキュリティ属性であるノードアクセス権リストに存在し、かつ当該属性と関連付けられるアクセス権レベルに[削除(VRWD)]が設定されている場合。 ・前述の値が、親ノードのノードアクセス権リストに存在し、かつ当該属性と関連付けされるアクセス権レベルに[書き込み(VRW)]または[削除(VRWD)]が設定されている場合。 ・前述の値が、すべての配下ノードのノードアクセス権リストに存在し、かつ当該属性と関連付けされるアクセス権レベルに[削除(VRWD)]が設定されている場合。 ・すべての配下ノードのロックオーナ属性がブランクの場合（ロックされていない場合)、もしくはサブジェクトセキュリティ属性のユーザ ID と一致する値が設定されている場合（自身がロックしている場合)。 ⑧システム管理者は対象オブジェクトのセキュリティ属性によらず、すべての操作が許可される。
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*] ユーザ ID
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*] ユーザ ID

(5) アカウント管理

FMT_MTD.1(1)	**TSF データの管理(1)**
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(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]*]

[割付: *その他の操作*]
登録

[割付: *TSF データのリスト*]
ユーザ ID

[割付: *許可された識別された役割*]
システム管理者、ユーザ管理者

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*]
システム管理者

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*]
ユーザ管理者

FMT_MTD.1(2) **TSF データの管理(2)**

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(2) **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]*]
削除

[割付: *TSF データのリスト*]
システム管理者およびユーザ管理者のユーザ ID

[割付: *許可された識別された役割*]
システム管理者

FMT_MTD.1(3)	**TSF データの管理(3)**
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(3)	**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]*] 削除 [割付: *TSF データのリスト*] ユーザ ID（システム管理者およびユーザ管理者のユーザ ID を除く） [割付: *許可された識別された役割*] システム管理者、ユーザ管理者

FMT_MTD.1(4)	**TSF データの管理(4)**
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(4)	**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]*] 削除 [割付: *その他の操作*] 登録 [割付: *TSF データのリスト*] グループ ID [割付: *許可された識別された役割*] システム管理者、ユーザ管理者、グループ管理者

FMT_SMR.1(3)	**セキュリティの役割(3)**
下位階層:	なし
依存性:	FIA_UID.1 識別のタイミング
FMT_SMR.1.1(3)	**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*] グループ管理者

FMT_MTD.1(5)	**TSF データの管理(5)**
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(5)	**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]*] [割付: *その他の操作*] ユーザ ID との関連付けを改変（利用者の所属グループを改変） [割付: *TSF データのリスト*] グループ ID [割付: *許可された識別された役割*] システム管理者、ユーザ管理者、グループ管理者

FMT_MTD.1(6)	**TSF データの管理(6)**
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(6)	**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]*] [割付: *その他の操作*] 設定（権限の付与、権限の削除） [割付: *TSF データのリスト*] システム管理権限、ユーザ管理権限

	[割付: *許可された識別された役割*] システム管理者

FMT_MTD.1(7)	**TSF データの管理(7)**
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(7)	**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]*] [割付: *その他の操作*] 設定（権限の付与、権限の削除） [割付: *TSF データのリスト*] グループ管理権限 [割付: *許可された識別された役割*] システム管理者、ユーザ管理者

（6）認証データの保護

FMT_MTD.1(8)	**TSF データの管理(8)**
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(8)	**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]*] [割付: *その他の操作*] 登録 [割付: *TSF データのリスト*] パスワード [割付: *許可された識別された役割*] システム管理者、ユーザ管理者

FMT_MTD.1(9)	**TSF データの管理(9)**
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(9)	**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*] システム管理者およびユーザ管理者のパスワード [割付: *許可された識別された役割*] システム管理者

FMT_MTD.1(10)	**TSF データの管理(10)**
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(10)	**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*] パスワード（システム管理者およびユーザ管理者のパスワードを除く） [割付: *許可された識別された役割*] システム管理者、ユーザ管理者

FMT_MTD.1(11)	**TSF データの管理(11)**
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(11)	**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*] 本人のパスワード [割付：*許可された識別された役割*] 利用者

FMT_SMR.1(4)	**セキュリティの役割(4)**
下位階層:	なし
依存性:	FIA_UID.1 識別のタイミング
FMT_SMR.1.1(4)	**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*] 半角英数字

(7) アクセス制御に関わる属性値の設定と保護

FMT_MSA.3(1)	**静的属性初期化(1)**
下位階層:	なし
依存性:	FMT_MSA.1 セキュリティ属性の管理 FMT_SMR.1 セキュリティの役割
FMT_MSA.3.1(1)	**TSF は、その SFP を実施するために使われるセキュリティ属性に対して[選択：*制限的、許可的、[割付：その他の特性]：から 1 つのみ選択*]デフォルト値を与える[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*]

	ノードアクセス制御規則 [割付: *その他の特性*] 新規作成したノードのノードアクセス権リストは、親フォルダノードのノードアクセス権リストを継承し、作成した利用者に対する「削除(VRWD)」を追加したノードアクセス権リストとなる。
FMT_MSA.3.2(1)	**TSF は、オブジェクトや情報が生成されるとき、[割付: *許可された識別された役割*]が、デフォルト値を上書きする代替の初期値を特定することを許可しなければならない。** [割付: *許可された識別された役割*] なし（ノードアクセス権リストに対して、FMT_MSA.3.2 が要求する処理を実現する必要はないため）

FMT_MSA.3(2)	**静的属性初期化(2)**
下位階層:	なし
依存性:	FMT_MSA.1 セキュリティ属性の管理 FMT_SMR.1 セキュリティの役割
FMT_MSA.3.1(2)	**TSF は、その SFP を実施するために使われるセキュリティ属性に対して[選択: *制限的、許可的、[割付: その他の特性]: から 1 つのみ選択*]デフォルト値を与える[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*] ノードアクセス制御規則 [選択: *制限的、許可的、[割付: その他の特性]: から 1 つのみ選択*] 許可的
FMT_MSA.3.2(2)	**TSF は、オブジェクトや情報が生成されるとき、[割付: *許可された識別された役割*]が、デフォルト値を上書きする代替の初期値を特定することを許可しなければならない。** [割付: *許可された識別された役割*] なし（ロックオーナ属性に対して、FMT_MSA.3.2 が要求する処理を実現する必要はないため）

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*] ノードアクセス制御規則 [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]*] 問い合わせ [割付: *セキュリティ属性のリスト*] ロックオーナ属性、ノードアクセス権リスト [割付: *許可された識別された役割*] システム管理者、利用者（対象ノードに[表示(V)]もしくは[読み込み(VR)]もしくは[書き込み(VRW)]もしくは[削除(VRWD)]の権限を有すること）

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*] ノードアクセス制御規則 [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*] 利用者のユーザ ID に改変（ノードのロック） [割付: *セキュリティ属性のリスト*] ロックオーナ属性 [割付: *許可された識別された役割*] システム管理者、利用者（対象ノードに[書き込み(VRW)]もしくは[削除(VRWD)]の権限を有すること）

FMT_MSA.1(3)	**セキュリティ属性の管理(3)**
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(3)	**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*] ノードアクセス制御規則 [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*] ブランクに改変（ノードのロック解除） [割付: *セキュリティ属性のリスト*] ロックオーナ属性 [割付: *許可された識別された役割*] システム管理者、ロックオーナ（対象ノードに[書き込み(VRW)]もしくは[削除(VRWD)]の権限を有すること）

FMT_SMR.1(5)	**セキュリティの役割(5)**
下位階層:	なし
依存性:	FIA_UID.1 識別のタイミング
FMT_SMR.1.1(5)	**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*] ロックオーナ

FMT_MSA.1(4)	**セキュリティ属性の管理(4)**
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(4)	**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*] ノードアクセス制御規則 [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 [割付: *セキュリティ属性のリスト*] ノードアクセス権リスト

[割付: *許可された識別された役割*]
システム管理者、オーナ（対象ノードに[表示(V)]もしくは[読み込み(VR)]もしくは[書き込み(VRW)]もしくは[削除(VRWD)]の権限を有すること）

FMT_SMR.1(6) **セキュリティの役割(6)**

下位階層: なし
依存性: FIA_UID.1 識別のタイミング

FMT_SMR.1.1(6) **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*]
オーナ

FMT_MTD.1(12) **TSF データの管理(12)**

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(12) **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]*]
問い合わせ

[割付: *TSF データのリスト*]
オーナ属性

[割付: *許可された識別された役割*]
システム管理者、利用者（対象ノードに[表示(V)]もしくは[読み込み(VR)]もしくは[書き込み(VRW)]もしくは[削除(VRWD)]の権限を有すること）

FMT_MTD.1(13) **TSF データの管理(13)**

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(13) **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*] オーナ属性 [割付: *許可された識別された役割*] システム管理者、オーナ（対象ノードに[表示(V)]もしくは[読み込み(VR)]もしくは[書き込み(VRW)]もしくは[削除(VRWD)]の権限を有すること）

FMT_MTD.1(14)	**TSF データの管理(14)**
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(14)	**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]*] [割付: *その他の操作*] 新規作成するノードに対して登録（作成する利用者のユーザ ID を登録） [割付: *TSF データのリスト*] オーナ属性 [割付: *許可された識別された役割*] 利用者

（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*] ・ユーザ登録機能 ・システム管理者・ユーザ管理者のユーザ削除機能 ・システム管理者・ユーザ管理者以外のユーザ削除機能 ・グループ管理機能 ・所属グループ更新機能 ・システム管理権限・ユーザ管理権限付与機能 ・グループ管理権限付与機能 ・パスワード登録機能 ・システム管理者・ユーザ管理者のパスワード更新機能

・システム管理者・ユーザ管理者以外のパスワード更新機能
・本人パスワード更新機能
・アクセス権参照機能
・ノードロック機能
・ノードロック解除機能
・アクセス権更新機能
・オーナ属性参照機能
・オーナ属性更新機能
・オーナ属性初期設定機能

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。

6. TOE 要約仕様

「識別認証機能（識別認証（1）ログイン制限（a））」(FIA_UID.2、FIA_UAU.2)

- 利用者が TOE を利用する前には必ずユーザ ID・パスワードが要求される。
- TOE は利用者を、利用者が入力したユーザ ID によって識別し、利用者が入力したパスワードによって認証する。
- TOE は識別認証処理が成功すると、TOE への接続識別子である SID を発行し ServletContainer により提供される HttpSession に格納する。TOE は TOE への処理要求があるたびに HttpSession から SID を取り出し、その有効性を確認する。

「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の制御(a))」(FDP_ACC.1、FDP_ACF.1、FIA_USB.1、FIA_ATD.1)

- 利用者プロセスには、フォルダノード、ファイルノード、URL ノードに対し、ノードアクセス制御規則に基づいたアクセス制御が行われる。
- ノードアクセス制御規則では、対象ノードのロックオーナ属性、ノードアクセス権リスト、及び利用者のユーザ ID により、以下の通り可能な操作が定義される。

  ①以下の条件を満たす場合に、ノードに対する属性参照が許可される。
  ・対象ノードに対し「表示(V)」または「読み込み(VR)」または「書き込み(VRW)」または「削除(VRWD)」のアクセス権レベルが利用者に付与されていること。

  ②以下の条件を満たす場合に、ファイルノードに対する実体参照が許可される。
  ・ 対象ノードに対し「読み込み(VR)」または「書き込み(VRW)」または「削除(VRWD)」のアクセス権レベルが利用者に付与されていること。

  ③以下の条件をすべて満たす場合に、ノードに対する属性更新が許可される。
  ・対象ノードに対し「書き込み(VRW)」または「削除(VRWD)」のアクセス権レベル

が利用者に付与されていること。

・対象ノードがロックされていない状態、もしくは利用者自身がロックしている状態であること。

④以下の条件を満たす場合に、フォルダノードに対する子ノードの新規作成が許可される。

・対象ノードに対し「書き込み(VRW)」または「削除(VRWD)」のアクセス権レベルが利用者に付与されていること。

⑤以下の条件をすべて満たす場合に、ファイルノードに対する実体更新が許可される。

・対象ノードに対し「書き込み(VRW)」または「削除(VRWD)」のアクセス権レベルが利用者に付与されていること。

・対象ノードがロックされていない状態、もしくは利用者自身がロックしている状態であること。

⑥以下の条件をすべて満たす場合に、ファイルノード、URL ノードの削除が許可される。

・対象ノードに対し「削除(VRWD)」のアクセス権レベルが利用者に付与されていること。

・対象ノードの親ノードに対し「書き込み(VRW)」または「削除(VRWD)」のアクセス権レベルが利用者に付与されていること。

・対象ノードがロックされていない状態、もしくは利用者自身がロックしている状態であること。

⑦以下の条件をすべて満たす場合に、フォルダノードの削除が許可される。

・対象ノードに対し「削除(VRWD)」のアクセス権レベルが利用者に付与されていること。

・対象ノードの親ノードに対し「書き込み(VRW)」または「削除(VRWD)」のアクセス権レベルが利用者に付与されていること。

・対象ノード配下のすべてのノードに対して「削除(VRWD)」のアクセス権レベルが利用者に付与されていること。

・対象ノード配下のすべてのノードがロックされていない状態、もしくは利用者自身がロックしている状態であること。

⑧システム管理者は、対象ノードのロックオーナ属性、ノードアクセス権リストによらず、すべての操作が許可される。

・ ノードアクセス権リストは、あるノードに対して設定されたアクセス権の集合であり、アクセス権は、ユーザ ID とそれに対応するアクセス権レベルの組み合わせで定義される。

・ アクセス権レベルには「表示(V)」「読み込み(VR)」「書き込み(VRW)」「削除(VRWD)」

があり、それぞれ後者の権限は前者の権限を包括する。

- ノードに対する操作には「新規作成」「属性参照」「実体参照」「属性更新」「実体更新」「削除」があり、このうちノードアクセス制御規則によって利用者に許可された操作のみ、利用者は実行できる。

「ユーザ管理機能（セキュリティ管理（5）アカウント管理（a））」（FMT_MTD.1(1)、FMT_SMR.1(1)、FMT_SMR.1(2)、FMT_MTD.1(2)、FMT_MTD.1(3)、FMT_MTD.1(4)、FMT_SMR.1(3)、FMT_MTD.1(5)、FMT_MTD.1(6)、FMT_MTD.1(7)）

- ユーザ ID に対する「登録」の操作は、システム管理者とユーザ管理者が実行できる。
- システム管理者およびユーザ管理者のユーザ ID に対する「削除」の操作は、システム管理者が実行できる。
- システム管理者およびユーザ管理者以外のユーザ ID に対する「削除」の操作は、システム管理者とユーザ管理者が実行できる。
- グループ ID に対する「削除」「登録」の操作は、システム管理者とユーザ管理者、及びグループ管理者が実行できる。
- 利用者の所属グループに対する「改変」の操作は、システム管理者とユーザ管理者、及びグループ管理者が実行できる。
- 利用者に対するシステム管理権限およびユーザ管理権限の付与・削除は、システム管理者が実行できる。
- 利用者に対するグループ管理権限の付与・削除は、システム管理者とユーザ管理者が実行できる。

「ユーザ管理機能（セキュリティ管理（6）認証データの保護（a））（FMT_MTD.1(8)、FMT_SMR.1(1)、FMT_SMR.1(2)、FMT_MTD.1(9)、FMT_MTD.1(10)、FMT_MTD.1(11)、FMT_SMR.1(4)、FIA_SOS.1）

- 利用者のパスワードに対する「登録」の操作は、システム管理者とユーザ管理者が実行できる。
- システム管理者およびユーザ管理者のパスワードに対する「改変」の操作は、システム管理者が実行できる。
- システム管理者およびユーザ管理者以外のパスワードに対する「改変」の操作は、システム管理者とユーザ管理者が実行できる。
- 利用者は自分自身のパスワードを「改変」することができる。
- パスワードには半角英数字のみ使用できる。

「アクセス権管理機能（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

(b))(FMT_MSA.3(1)、FMT_MSA.3(2))

- 新規作成したノードのノードアクセス権リストは、親フォルダノードのノードアクセス権リストを継承し、作成した利用者に対する「削除(VRWD)」を追加したノードアクセス権リストとなる。また、このデフォルト値に代わる初期値を設定することはできない。
- 新規作成したノードのロックオーナ属性は、ブランク（ロックされていない状態）となる。

「アクセス権管理機能（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(1)、FMT_SMR.1(1)、FMT_SMR.1(4)、FMT_MSA.1(2)、FMT_MSA.1(3)、FMT_SMR.1(5)、FMT_MSA.1(4)、FMT_SMR.1(6)、FMT_MTD.1(12)、FMT_MTD.1(13)、FMT_MTD.1(14))

- 対象ノード（ここではフォルダノード以外）のロックオーナ属性がブランクの場合（ノードがロックされていない）に、利用者はロックオーナ属性を利用者のユーザIDに「改変」することができる（ノードのロック)。ただしシステム管理者以外の場合には、対象ノードに対し「書き込み(VRW)」または「削除(VRWD)」のアクセス権レベルが利用者に付与されている必要がある。
- 対象ノード（ここではフォルダノード以外）のロックオーナはロックオーナ属性をブランクに「改変」することができる（ノードのロック解除)。ただしシステム管理者以外の場合には、対象ノードに対し「書き込み(VRW)」または「削除(VRWD)」のアクセス権レベルが利用者に付与されている必要がある。
- システム管理者は、対象ノード（ここではフォルダノード以外）のロックオーナ属性がブランク以外の場合（ノードがロックされている）に、ロックオーナ属性をブランクに「改変」することができる（ノードのロック解除)。
- 利用者はロックオーナ属性を問い合わせることができる。ただしシステム管理者以外の場合には、対象ノードに対し「表示(V)」または「読み込み(VR)」または「書き込み(VRW)」または「削除(VRWD)」のアクセス権レベルが利用者に付与されている必要がある。
- システム管理者もしくは対象ノードのオーナは、ノードアクセス権リストを「改変」することができる。ただしシステム管理者以外の場合には、対象ノードに対し「表示(V)」または「読み込み(VR)」または「書き込み(VRW)」または「削除(VRWD)」のアクセス権レベルが利用者に付与されている必要がある。
- 利用者はノードアクセス権リストを問い合わせることができる。ただしシステム管理者以外の場合には、対象ノードに対し「表示(V)」または「読み込み(VR)」または「書き込み(VRW)」または「削除(VRWD)」のアクセス権レベルが利用者に付与されている必要がある。

- システム管理者もしくは対象ノードのオーナは、オーナ属性を「改変」することができる。ただしシステム管理者以外の場合には、対象ノードに対し「表示(V)」または「読み込み(VR)」または「書き込み(VRW)」または「削除(VRWD)」のアクセス権レベルが利用者に付与されている必要がある。
- 利用者はオーナ属性を問い合わせることができる。ただしシステム管理者以外の場合には、対象ノードに対し「表示(V)」または「読み込み(VR)」または「書き込み(VRW)」または「削除(VRWD)」のアクセス権レベルが利用者に付与されている必要がある。
- 新規に作成するノードのオーナ属性は、作成する利用者のユーザ ID となる。

「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)

- TOE は以下のセキュリティ管理機能を有する。
  - ユーザ登録機能
  - システム管理者・ユーザ管理者のユーザ削除機能
  - システム管理者・ユーザ管理者以外のユーザ削除機能
  - グループ管理機能
  - 所属グループ更新機能
  - システム管理権限・ユーザ管理権限付与機能
  - グループ管理権限付与機能
  - パスワード登録機能
  - システム管理者・ユーザ管理者のパスワード更新機能
  - システム管理者・ユーザ管理者以外のパスワード更新機能
  - 本人パスワード更新機能
  - アクセス権参照機能
  - ノードロック機能
  - ノードロック解除機能
  - アクセス権更新機能
  - オーナ属性参照機能
  - オーナ属性更新機能
  - オーナ属性初期設定機能