CWAT3i

(Ver3.1b_CC)

セキュリティターゲット

バージョン:0.39

発行日:2008年4月15日

作成者：株式会社インテリジェントウェイブ

＜更新履歴＞

日付	バージョン	承認者	確認者	作成者	担当	更新内容 備考
2006/12/18	0.10	前田	清田	清田	セキュリティシステム事業部	新規作成
2006/12/21	0.11	前田	清田	清田	セキュリティシステム事業部	内容修正、追記
2007/1/29	0.12	前田	清田	清田	セキュリティシステム事業部	内容修正、追記
2007/2/7	0.13	前田	清田	清田	セキュリティシステム事業部	内容修正、追記
2007/2/13	0.14	前田	清田	清田	セキュリティシステム事業部	内容修正、追記
2007/2/16	0.15	前田	清田	清田	セキュリティシステム事業部	内容修正、追記
2007/2/19	0.16	前田	清田	清田	セキュリティシステム事業部	内容修正、追記
2007/2/28	0.17	前田	清田	清田	セキュリティシステム事業部	内容修正、追記
2007/3/15	0.18	前田	清田	清田	セキュリティシステム事業部	内容修正、追記
2007/3/22	0.19	前田	清田	清田	セキュリティシステム事業部	内容修正、追記
2007/03/27	0.20	前田	清田	清田	セキュリティシステム事業部	内容修正、追記
2007/04/19	0.21	前田	清田	清田	セキュリティシステム事業部	内容修正、追記
2007/05/30	0.22	前田	清田	清田	セキュリティシステム事業部	内容修正
2007/06/29	0.23	前田	清田	清田	セキュリティシステム事業部	内容修正
2007/07/23	0.24	前田	清田	清田	セキュリティシステム事業部	内容修正
2007/08/22	0.25	前田	清田	清田	セキュリティシステム事業部	内容修正
2007/9/6	0.26	前田	清田	清田	セキュリティシステム事業部	内容修正
2007/9/19	0.27	前田	清田	清田	セキュリティシステム事業部	内容修正
2007/9/25	0.28	前田	清田	清田	セキュリティシステム事業部	内容修正
2007/9/28	0.29	前田	清田	清田	セキュリティシステム事業部	内容修正
2007/10/4	0.30	前田	清田	清田	セキュリティシステム事業部	内容修正
2007/11/9	0.31	前田	清田	清田	セキュリティシステム事業部	内容修正
2007/12/14	0.32	前田	清田	清田	セキュリティシステム事業部	OMクライアント説明追記
		前田	清田	清田	セキュリティシ	他サイトのポリシー設定修正

					ステム事業部	
2007/12/27	0.33	前田	清田	清田	セキュリティシステム事業部	サイト管理者脅威、OSP修正
2008/1/8	0.34	前田	清田	清田	セキュリティシステム事業部	OMクライアントPC前提の修正
2008/1/21	0.35	前田	清田	清田	セキュリティシステム事業部	T.EVIL_POLYCY_VIA_OPDCへの対策根拠、O.MANAGEの対抗する脅威の根拠の修正
2008/1/24	0.36	前田	清田	清田	セキュリティシステム事業部	CRV-T131-001　2その他コメント2)への対応
2008/2/12	0.37	前田	清田	清田	セキュリティシステム事業部	T.EVIL_POLICY_VIA_OPDC、A.PC_USE_ROLEの整理 FPT_RVM.1、FPT_SEP.1根拠見直し
2008/3/3	0.38	前田	清田	清田	セキュリティシステム事業部	FPT_RVM.1、FPT_SEP.1根拠見直し
2008/4/15	0.39	前田	清田	清田	セキュリティシステム事業部	システム管理者の権限に係る部分の表現整理

目次

1. ST 概説

本章では、ST 識別、ST 概要、CC 適合の主張、用語について記述する。

1.1. ST 識別

タイトル：CWAT3i（Ver3.1b_CC）　セキュリティターゲット
バージョン：0.39
発行日：2008 年 4 月 15 日
作成者：株式会社インテリジェントウェイブ
TOE：　CWAT3i（Windows 版）
TOE のバージョン：Ver3.1b_CC
キーワード：内部情報漏洩、内部統制、不正操作監視、ノード監視、ネットワーク監視
CC のバージョン：CC Ver2.3、補足-0512 適用

1.2. ST 概要

本ドキュメントは、CWAT3i を評価対象としたセキュリティターゲットである。CWAT3i は、コンピュータ利用サイトにおいて、ネットワークに接続される PC 端末の端末操作、及びネットワークアクセス操作を監視し、操作に対する監査ログを生成する。また、サイトごとに設定したポリシーへの違反操作を検知すると、警告ログを発生させ、その警告ログを集中管理しモニタリングするための機能を提供する。
本ドキュメントは、CWAT3i 製品が提供するポリシー設定機能及び警告ログの集中監視機能への妨害行為として想定される脅威に対抗するために、以下の保護策の実装を目的とし、これらの保護策を実現するためのセキュリティ機能について説明したものである。

- ポリシーを設定する者や、警告ログをモニタリングする者を制限すること
- 監視する PC 端末へのポリシーの配信機能を強化すること
- 検知したポリシー違反行為に関する警告ログの送信機能を強化すること

1.3. CC 適合の主張

この ST は以下の CC に適合している。

- CC パート 2 適合
- CC パート 3 適合
- EAL2 適合

この ST が適合している PP はない。

1.4. 用語

本 ST における用語を説明する。

用語	定義内容
システム管理者	CWAT3i を導入するサーバ及び端末の管理者
CWAT 管理者	CWAT3i のサイト管理者情報を設定する管理者
サイト管理者	CWAT3i の各サイトのポリシーを設定する管理者
管理者	システム管理者、CWAT 管理者、サイト管理者の総称
TOE の管理者	CWAT 管理者、サイト管理者の総称
端末利用者	CWAT3i によって監視する端末を利用する利用者
サイトモニタ画面	CWAT3i の各監視サイトのサマリー情報（サイト一覧情報）を表示する画面
個別サイト詳細画面	サイトの登録、更新、削除及びサイトの管理情報を設定する画面
オーガナイゼーションモニタ画面	監視対象組織（ノード）、重要警告情報、全警告情報を表示する監視画面。簡略化する場合、OM モニタ画面と記載する。
オーガナイゼーションモニタ認証アカウント	サイトモニタ画面にログオンするためのアカウントである。簡略化する場合、OM 認証アカウントと記載する。
サイト属性	CWAT3i に登録するサイト固有の属性
ノード属性	サイトに登録するノード固有の属性
ユーザ属性	サイトに登録するユーザ固有の属性
DC	SDC、UDC、OPDC を総称する場合、DC と記載する。
上位 NM	DC に対し、ポリシーや DC 設定情報の配信元となる SDC/UDC、または、OMI のこと。上位 NM には、さらに、上位 NM を配置するといった多段階の構成をとることが可能である
未登録端末	管理サイトにおいて、未登録・盗難端末ポリシーマネージャにて登録されたポリシーに合致しなかった端末
未管理端末	管理サイトにおいて、DC から送信された端末情報（IP アドレス等）がノード属性情報として OMI に登録（管理）されていない端末
サイト	CWAT3i が監視の対象とするネットワーク及びノードからなるグループを示す概念であり、企業や組織の拠点など、指定した所定のポリシーが求められる単位で設定する
ポリシー	CWAT3i が監視する不正操作やネットワーク操作に関する条件の集合
ユーザ情報	OMI と DC 間で交換される情報のうち、ユーザ属性とその値からなる情報
ノード情報	OMI と DC 間で交換される情報のうち、ノード属性とその値からなる情報
コントロール情報	OMI と DC 間で交換される情報のうち、OMI と DC とが協調して動作するために必要な情報。DC 設定情報を含む
DC 設定情報	ポリシー受信や警告ログ送信など、DC の動作を決定するために必要な情報
警告ログ	ポリシーに基づき不正操作や不審操作が検出されると DC から OMI に送信されるメッセージ。OMI でモニタリングするために必要な情報を含む
ユーザログオンポリシー	ユーザログオンを監視するための対象ノード、有効期間などを設定する
端末使用ポリシー	端末使用状況を監視するための対象ノード、ユーザ端末使用行為などを設定する
未登録・盗難端末ポリシー	未登録端末、盗難端末を監視するための諸条件を設定する（SDC または UDC が必要）
ネットワークポリシー	ネットワークのアクセス、ポート番号などを設定する（SDC が必要）
外部接続機器ポリシー	外部機器の接続や外部メディアへのデータ書き込みを監視するための諸条件を設定する
ユーザオペレーションポリシー	ユーザ操作によるファイル操作、使用アプリケーション、画面ハードコピーなどを監視するための諸条件を設定する
メッセンジャーポリシー	MSN Messenger/Windows Messenger/Windows Live Messenger を監視するための諸条件を設定する

2. TOE 記述

2.1. TOE の概要

TOE は、ネットワークに接続された PC 端末操作、及びネットワークアクセス操作を集中監視するソフトウェア CWAT3i が提供する標準構成からなるソフトウェア製品の一部である。CWAT3i は以下に示す複数のソフトウェアから構成され、利用サイトのセキュリティ監視の目的に応じた構成で利用することができる。

CWAT3i の標準構成からなる製品は次のように複数の CD で提供され、その単位でインストールを行う。

- OMI（インターナショナル版の CD として提供。CD は LC、DM もツールとして提供）
- OPDC（日本語版と英語版を別の CD で提供）
- SDC（日本語版と英語版を別の CD で提供）
- UDC（日本語版と英語版を別の CD で提供）
- LC（インターナショナル版の CD として提供。CD は、OMI の CD と共通）
- DM（インターナショナル版の CD として提供。CD は、OMI の CD と共通）

以下、各ソフトウェア、および TOE との関係について説明する。

(1) OMI

ポリシーを設定し、設定したポリシーをサイトの各ノード（OPDC、SDC または UDC が動作するサーバまたは PC 端末）へ配信する機能、及びこれらのノードから発生する警告情報の集中監視を行なう機能を提供する。設定したポリシーや収集した警告情報は、DBMS にて管理し、OMI はこの DBMS で管理する DB へのアクセス手段を提供する。

OMI には、OPDC のプロダクトに対応して OPDCstandard 用の OMI と OPDCpro 用の OMI があるが、OPDCpro 用の OMI のみを評価対象とする。OPDCpro 用の OMI には、さらに次のプロダクトが提供されており、インストール時に選択できる。各プロダクトは日本語、英語、韓国語、中国語、台湾語の 5 言語に対応するインターナショナル版であり、起動時に OS の言語設定に応じて言語が自動選択される。

OMI のプロダクトと TOE の関係を表 2.1-1 に示す。DB スキーマ定義や DB オブジェクトの初期設定は OMI のインストールマニュアルにしたがって適切に導入される必要がある。

注）OPDCpro 用の OMI は、PC 端末上の重要情報を保護するためのファイル暗号化機能を搭載している。ユーザは、ファイル暗号化に使用する暗号化ライブラリ（DLL）として Camellia、Misty、C4CS、MS-40bit、RSA、TripleDES の中から一つ選択し、選択した暗号化ライブラリに対応する OMI を購入する。本評価では、Camellia に対

応する OMI のみを評価対象とする。なお、ファイル暗号化機能は 2.4.2 に示すとおり TOE セキュリティ機能ではない。

表 2.1-1 OMI のプロダクトと TOE の関係

ソフトウェア名称	プロダクト名称 (注1)	プロダクト略称	機能概要	言語版	評価対象の区別
OMI	オーガナイゼーションモニタインターナショナル	OMI	・OMIサーバ機能 (注2) ・OMIクライアント機能 (注3)	インターナショナル版	日本語設定を評価対象とする
	オーガナイゼーションモニタクライアント (注4)	OMI クライアント	・OMIクライアント機能 (注3) ただし、DC 環境設定機能、および、祝日設定機能は利用できない。	インターナショナル版	日本語設定と英語設定を評価対象とする
	オーガナイゼーションモニタサーバ	OMI サーバ	・OMIサーバ機能 (注2)	インターナショナル版	評価対象外
	オーガナイゼーションモニタマネージャ	OM Mng	複数のオーガナイゼーションモニタを管理する機能	インターナショナル版	評価対象外

（注１）OMI を CD からインストールするときに選択可能な“インストールタイプ”として、オーガナイゼーションモニタインターナショナル・オーガナイゼーションモニタクライアント・オーガナイゼーションモニタサーバ・オーガナイゼーションモニタマネージャがある。それらを「プロダクト」と呼ぶことにする。

（注２）OMI サーバ機能とは、サーバ側の常駐サービス機能を意味する。

（注３）OMI クライアント機能とは、クライアント側常駐サービス機能＋画面インターフェース機能＋DB へのアクセス機能を意味する。

（注４）オーガナイゼーションモニタクライアントが動作するためには、オーガナイゼーションモニタインターナショナル、またはオーガナイゼーションモニタサーバを別端末にインストールしておく必要がある。

(2) OPDC

PC 端末の操作に関する監査ログを生成し、不正操作を検出した場合は警告ログを発生させる機能を提供する。

OPDC には、次のプロダクトが提供されている。それぞれ、日本語版と英語版がある。

OPDC のプロダクトと TOE の関係を表 2.1-2 に示す。

表 2.1-2 OPDC のプロダクトと TOE の関係

ソフトウェア名称	プロダクト名称	プロダクト略称	機能概要	言語版	評価対象の区別
OPDC	オペレーションディフェンスコントローラ スタンダード	OPDC standard	PC 端末の操作に関する監査ログを生成し、不正操作を検出した場合は警告ログを発生させる	日本語版	評価対象外
				英語版	評価対象外
	オペレーションディフェンスコントローラ プロ	OPDC pro	OPDC standard の機能に加え、ファイル暗号化機能などを搭載	日本語版	評価対象
				英語版	評価対象

OPDCpro は、PC 端末上の重要情報を保護するためのファイル暗号化機能を搭載している。ユーザは、ファイル暗号化に使用する暗号化ライブラリ（DLL）として Camellia、Misty、C4CS、MS-40bit、RSA、TripleDES の中から一つ選択し、選択した暗号化ライブラリに対応する OPDCpro を購入する。本評価では、Camellia に対応する OPDCpro のみを評価対象とする。なお、ファイル暗号化機能は 2.4.2 に示すとおり TOE セキュリティ機能ではない。

(3) SDC

ポリシーに基づき、サイトのネットワークアクセス操作を監視する機能を提供する。その他は UDC と同等機能を提供する。日本語版と英語版がある。SDC のプロダクトと TOE の関係を表 2.1-3 に示す。

表 2.1-3 SDC のプロダクトと TOE の関係

ソフトウェア名称	プロダクト名称	プロダクト略称	言語版	評価対象の区別
SDC	セグメントディフェンスコントローラ	SDC	日本語版	評価対象
			英語版	評価対象外

(4) UDC

ポリシーに基づき、サイトのネットワークに不正に接続された端末とその動作を検知する機能を提供する。日本語版と英語版がある。UDC のプロダクトと TOE の関係を表 2.1-4 に示す。

表 2.1-4 UDC のプロダクトと TOE の関係

ソフトウェア名称	プロダクト名称	プロダクト略称	言語版	評価対象の区別
UDC	アンノウンターミナルディフェンスコントローラ	UDC	日本語版	評価対象外
			英語版	評価対象

(5) LC

SDC、UDC 及び OPDC で生成された監査ログを自動収集し閲覧・出力するための機能を提供する。プロダクトは OMI と同様、日本語、英語、韓国語、中国語、台湾語の 5 言語に対応するインターナショナル版であり、起動時に OS の言語設定に応じて言語が自動選択される。LC のプロダクトと TOE の関係を表 2.1-5 に示す。

表 2.1-5 LC のプロダクトと TOE の関係

ソフトウェア名称	プロダクト名称	プロダクト略称	言語版	評価対象の区別
LC	ログコレクタ	LC	インターナショナル版	日本語設定を評価対象とする

(6) DM

DM とは、各種設定ファイルを各 OPDC に配信するツールであり、大規模環境の場合など、本ツールを経由し OM から設定情報を配信することにより OM への直接アクセスを軽減することが可能になる。DM のプロダクトは OMI と同様、日本語、英語、韓国語、中国語、台湾語の 5 言語に対応するインターナショナル版であり、起動時に OS の言語設定に応じて言語が自動選択される。DM のプロダクトと TOE の関係を表 2.1-5 に示す。表 2.1-5 の通り、DM は評価対象外とする。

表 2.1-6 LC のプロダクトと TOE の関係

ソフトウェア名称	プロダクト名称	プロダクト略称	言語版	評価対象の区別
DM	デリバリマネージャ	DM	インターナショナル版	評価対象外

2.2. TOE 関連の利用者役割

TOE に関連する利用者の役割は以下の通りである。利用者はシステム管理者、CWAT 管理者、サイト管理者、端末利用者のいずれかに分類される。システム管理者、CWAT 管理者、サイト管理者を総称して管理者と呼ぶ。また、TOE に登録済みのサイト管理認証アカウントを所持する CWAT 管理者、及びサイトログオン認証アカウントを所持するサイト管理者を総称して TOE の管理者と呼ぶ。

(1) システム管理者

CWAT3i の全プロダクトのインストール、設定、及びシステム管理を行なう。

- DC のインストール時に、DC に対する上位 NM、OMI を設定する。
  - DC が OPDC の場合、上位 NM として OMI の IP アドレスを設定するか、SDC/UDC の IP アドレスを設定することができる。
  - DC が SDC/UDC の場合、通常上位 NM として OMI の IP アドレスを設定する。
  - DC に対する OMI の IP アドレスを設定する。
- OM 認証アカウント（アカウント ID、パスワード)、サイト管理認証アカウント（アカウント ID、パスワード）の登録、更新、削除を行う。

(2) CWAT 管理者

OM 認証アカウント及びサイト管理認証アカウントの所有者であり、監視サイトのセキュリティポリシーを適切に設定できるサイト管理者を登録し、必要に応じてサイトの情報を登録、更新、削除する。

(3) サイト管理者

OM 認証アカウント及びサイトログオン認証アカウントの所有者であり、監視サイトのセキュリティポリシーを設定し、サイトのネットワーク及びネットワークに接続された端末操作の両方を集中監視する。

(4) 端末利用者

ネットワークに接続された端末の使用を許可された者であり、端末操作を CWAT 管理者及びサイト管理者によって監視される。

2.3. TOE の物理的範囲

2.3.1. TOE の典型的なシステム構成

TOE の典型的なシステム構成を図 2.3-1 に示す。また、ソフトウェアの構成例を図 2.3-2 に示す。

TOE を導入するサイトは、ファイアウォールの適切な設定によりインターネットなどの外部ネットワークからの攻撃に晒されることのないイントラネットを運用する。このイントラネットは、ネットワーク、サーバ及び端末からなるネットワークコンピューティング環境を導入し、業務システム等を運用していることを想定する。OMI はイントラネットを構成する複数サイトとのネットワーク通信が可能なセグメントエリアに配置する。DBMS は TOE の各プロダクトとの通信が可能となるように配置する。通常は OMI と同じ筐体にインストールするが、専用のサーバとして動作させてもよい。各サイトのネットワークには、サイトのセキュリティ方針に基づき必要な場合のみ SDC または UDC を配置する。サイトのネットワークに接続し、端末操作を行なう PC 端末には OPDC がインストールされる。また、管理上の要求があれば、DC の監査ログを自動収集する LC を配置する。OMI、SDC、UDC 及び LC がインストールされるサーバは、コンピュータセンターなどシステム管理・運用のために許可された者のみが入室可能な物理的に保護された区域に設置される。ただし、その区域には当該 TOE のシステム管理者や TOE の管理者のみならず、他のシステム管理・運用を担当する者も通常は許可を受けて当該区域に入室可能であり、OMI の管理コンソール等を直接操作して不正に TOE にアクセスすることが可能な場合も想定する。

なお、ファイルサーバやアプリケーションサーバで使用するサーバには OPDC を適用しないことを推奨する。

TOE の管理者が使用する管理画面は OMI のみが提供する。SDC、UDC、OPDC は管理画面を有しない。TOE の管理者は OMI の管理画面から SDC、UDC、OPDC の設定及び TOE の管理・運用を行う。

図 2.3-2 のポリシー及び監査ログは TOE ではないが、いずれも TOE により生成される。

ポリシーは、サイト管理者によって OMI サーバにて設定されたのち、DC に送信され、OMI サーバ及び DC 上にファイルとして存在する。

監査ログは、OMI 及び DC で生成される。OMI で生成される監査ログは OMI の認証画面へのアクセス、管理画面へのアクセス操作が記録されるファイルである。DC で生成される監査ログには、端末操作がポリシーに基づいて OPDC で記録されるファイルと、ネットワークアクセスについてポリシーに基づいて SDC で記録されるファイルがあり、生成後一定期間経過すると削除される。LC サーバが含まれる構成においては、DC の監査ログファイルは、LC サーバに比較的長い一定期間保存される。

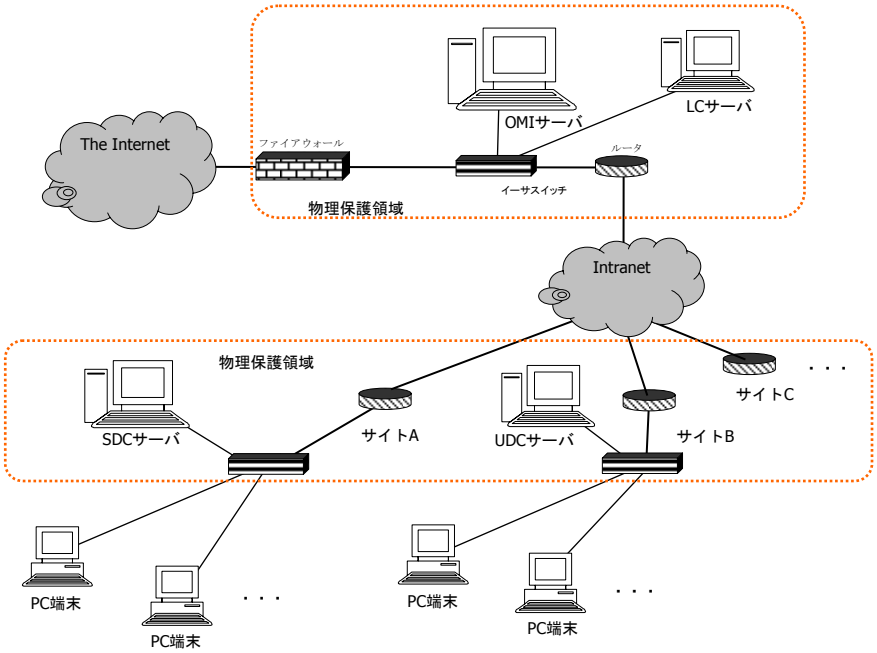

図 2.3-1　TOE 物理構成

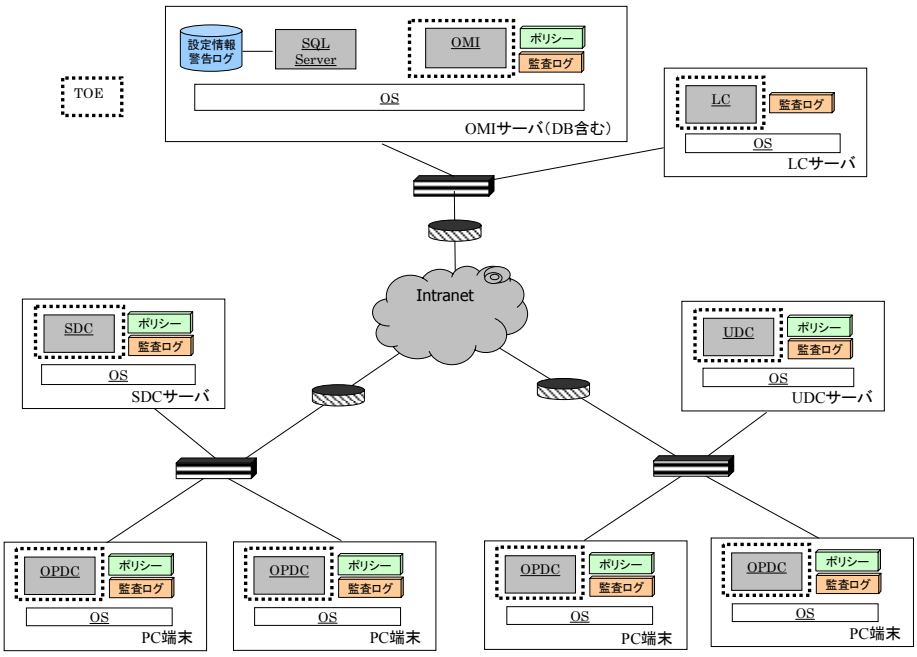

図 2.3-2　TOE ソフトウェア構成例

2.3.2. TOE の動作環境

TOE の動作環境は以下の通りである。実際に評価に使用した環境は 2.3.3 に示す通りである。

(1) OMI

OMI

導入先　　専用サーバ（Microsoft 環境）

対応 OS　　Microsoft Windows 2000 Server または Microsoft Windows Server 2003

動作条件　　Microsoft.NET Framework Version 1.1 以上

高度暗号化パックまたは IE5.5 以降

Microsoft SQL Server 2000 以上

解像度 1280×1024 以上のモニタ

推奨仕様　　CPU：Intel PentiumⅣ 2GHz 以上、メモリ：512MB 以上

OMIクライアント（OMIの一部モニタ機能を保持するプロダクト）の場合

導入先　　クライアント端末（Microsoft 環境）

対応 OS　　Microsoft Windows 2000 Server、Microsoft Windows Server 2003

または Microsoft Windows XP

動作条件　Microsoft.NET Framework Version 1.1 以上
高度暗号化パックまたは IE5.5 以降
解像度 1280×1024 以上のモニタ

推奨仕様　CPU：Intel PentiumⅣ 2GHz 以上、メモリ：512MB 以上

(2) OPDC

導入先　各クライアント・モバイル端末（Microsoft 環境）

対応 OS　Microsoft Windows 2000、Microsoft Windows XP、
または Microsoft Windows Server 2003

動作条件　高度暗号化パックまたは IE5.5 以降
OPDC pro プロダクトの場合、Microsoft Office 2000 以上

推奨仕様　上記 OS の推奨仕様を満たすこと

(3) SDC

導入先　専用サーバ（Microsoft 環境）

対応 OS　Microsoft Windows 2000、Microsoft Windows XP、
または Microsoft Windows Server 2003

動作条件　高度暗号化パックまたは IE5.5 以降

推奨仕様　CPU：Intel PentiumⅣ 2.4GHz 以上、メモリ：512MB 以上

(4) UDC

導入先　専用サーバ（Microsoft 環境）

対応 OS　Microsoft Windows 2000、Microsoft Windows XP、
または Microsoft Windows Server 2003

動作条件　高度暗号化パックまたは IE5.5 以降

推奨仕様　CPU：Intel PentiumⅣ 2.4GHz 以上、メモリ：512MB 以上

(5) LC

導入先　専用サーバ（Microsoft 環境）

対応 OS　Microsoft Windows 2000、Microsoft Windows XP、
または Microsoft Windows Server 2003

動作条件　高度暗号化パックまたは IE5.5 以降
解像度 1280×1024 以上のモニタ

推奨仕様　上記 OS の推奨仕様を満たすこと

※ SDC、UDC は Linux 環境（RedHat Enterprise Linux 3、または Turbolinux 8 Server）で動作するプロダクトも提供しているが、本 TOE では Microsoft 環境で動作するプロダクトのみを対象とする。

2.3.3. TOE の評価構成

TOE の典型的なシステム構成を想定し、図 2.3-3 に示すシステム構成を評価構成とする。これらは、３．TOE セキュリティ環境で定義した内容が漏れなく適用され、４．セキュリティ対策方針を実現するために必要な評価構成パターンとなっている。DBMS は OMI と同じサーバ上にインストールする。2.3.2 に示す通り、TOE を構成する各プロダクトは複数の OS で動作するが、図 2.3-3 の評価構成は表 2.3-1 に示す OS を対象とする。また、TOE の評価構成のプロダクトを表 2.3-1 に示す。

表 2.3-1 評価構成と OS

ソフトウェア	プロダクト	プロダクトの言語版	OS
OMI	OMI （1 台の端末にインストール）	インターナショナル版 （表示言語は日本語設定）	Microsoft Windows Sever 2003 日本語版
OMI	OMI クライアント (2 台の端末にインストール)	インターナショナル版 （表示言語は日本語設定（1 台）、英語設定（1 台））	Microsoft Windows Sever 2003 日本語版（1 台） Microsoft Windows XP 英語版（1 台）
OPDC	OPDC pro (5 台の端末にインストール)	日本語版（4 台） 英語版（1 台）	Microsoft Windows XP 日本語版（2 台） Microsoft Windows Sever 2003 日本語版（2 台） Microsoft Windows XP 英語版（1 台）
SDC	SDC （1 台の端末にインストール）	日本語版	Microsoft Windows Server 2003 日本語版
UDC	UDC （1 台の端末にインストール）	英語版	Microsoft Windows XP 英語版
LC	LC （1 台の端末にインストール）	インターナショナル版 （表示言語は日本語設定）	Microsoft Windows Sever 2003 日本語版

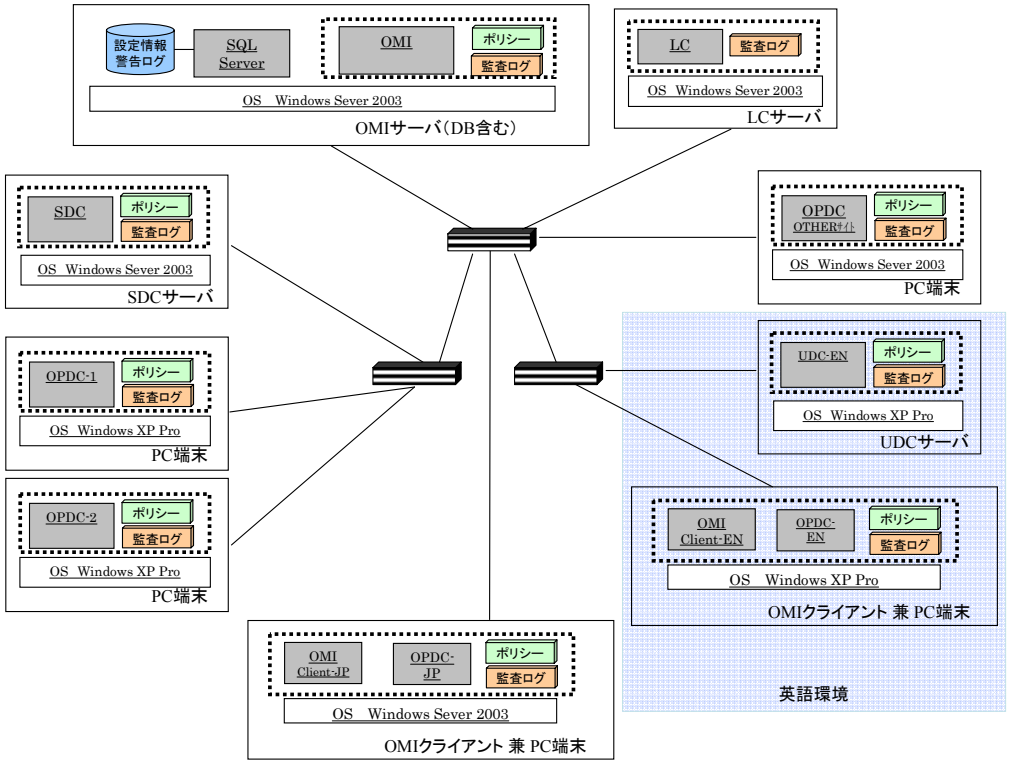

図 2.3-3　評価構成

2.4. TOE の論理的範囲

2.4.1. TOE 機能

(1) OMI

DC に対するサイト登録、ポリシー設定や、これらのノードからの警告情報の集中監視を行なうための統合監視コンソール機能を提供する。

- コマンドにより TOE の管理者のアカウント（OM 認証アカウント、サイト管理認証アカウント）を登録する機能
- サイト、ノード、ユーザ登録機能
- ポリシー設定機能
- DC 設定機能
- 警告情報、ユーザ、端末の集中監視機能
- 監査情報、警告情報の閲覧機能

・ 警告情報への対処機能
・ 警告情報の出力機能

OMI クライアントは、クライアント端末において、上記の統合監視を行う機能を提供する。

(2) OPDC

端末における不正操作を検出するためのサービス機能を提供する。

OPDC には、OPDC standard プロダクトと OPDC pro プロダクトがあり、ユーザはどちらかをインストールして使用する。OPDC pro プロダクトのみを TOE の対象とする。

OPDC pro プロダクトは、OMI のポリシーの設定に応じて端末における次の操作を検出する機能を搭載する。

・ 端末の電源 ON/OFF、ログオン/オフ状況の監視、自動遮断
・ 外部接続バス、MO、CD 等への書き出し、プリンタ印刷、アプリケーション、ファイル操作の監視、自動遮断
・ 登録されたモバイル機器を持ち出した場合に、持ち出し中のモバイル機器に対する操作を監視し、再接続時に不正操作を報告
・ ノード毎、ユーザ毎の不正挙動、不審操作（特異挙動）の監視
・ 操作ログ自動取得、保存
・ アラート状態のスクリーンショットの取得
・ PC 端末上の重要情報を保護するためのファイル暗号化機能
・ DRM 機能（デジタル著作権管理機能）
・ メッセンジャーポリシー
・ 個人情報自動検知

(3) SDC

サイトのネットワークアクセスを監視するための機能を提供する。

・ ネットワークアクセス監視機能による未登録端末の監視・防御機能
・ ネットワークパケット情報の監視・防御機能
・ ネットワークログ（ネットワークパケット情報）自動取得・保存機能

(4) UDC

サイトのネットワークに不正に接続された端末とその動作を検知する機能を提供する。

・ ネットワークアクセスの監視機能による未登録端末の監視・防御機能

(5) LC

DC で生成された監査ログを自動収集し閲覧・CSV 出力するための機能を提供する。

- 監査ログ自動収集機能
- 監査ログ閲覧・CSV 出力機能

2.4.2. TOE セキュリティ機能

TOE のセキュリティ機能の説明を以下に示す。

2.4.2.1. 管理者登録機能

2.4.2.1.1. OM 認証アカウントの登録機能（SF.OM_REGIST）

OMI のコマンド（cwlogon_writer.exe）により、OM 認証アカウントを登録することができる。

2.4.2.1.2. サイト管理認証アカウントの登録機能（SF.CWAT-ADM_REGIST）

OMI のコマンド（cwlogon_writer.exe）により、サイト管理認証アカウントを登録することができる。

2.4.2.2. 識別認証機能

TOE の管理者が使用する機能を利用可能とするまえに、TOE の管理者であることを識別・認証する機能である。TOE の管理者は、CWAT 管理者、及びサイト管理者であり、図 2.4-1 に示すように、いずれの TOE の管理者も、それぞれの管理者機能にログオンする前に OM 認証されていなければならない。

- CWAT 管理者（複数名可能）:
  - OM 認証アカウントを有し、サイトモニタにログオンできる。
  - サイトモニタから､サイト管理認証アカウントにより個別サイト詳細画面にログオンし、全サイトの管理（登録・更新・削除、監視）を行う。

- サイト管理者（１つのサイトに複数名可能）:
  - OM 認証アカウントを有し、サイトモニタにログオンできる。
  - サイトモニタから、サイトログオン認証アカウントにより OM モニタ画面にログオンし、サイトの管理、監視を行う。

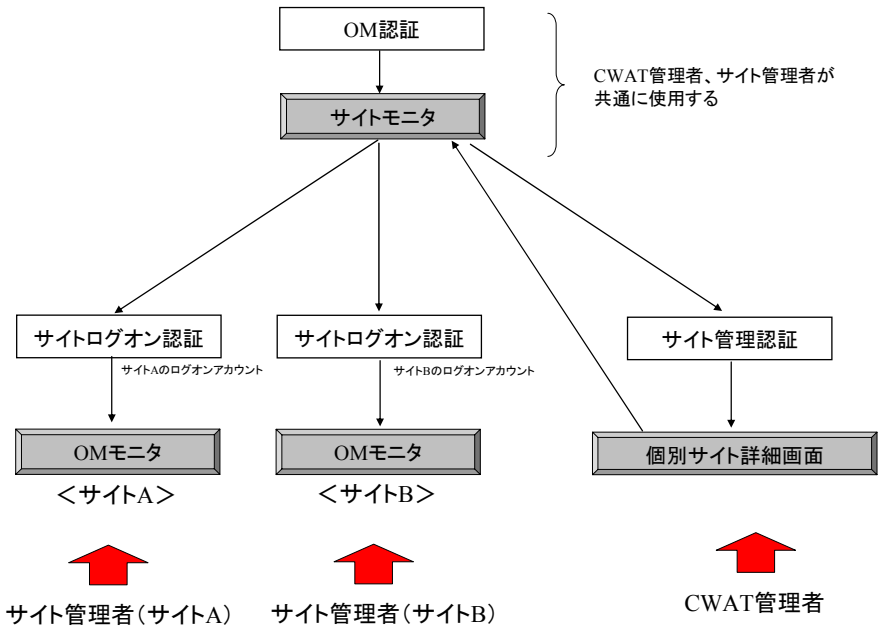

図 2.4-1　管理者機能の概念図

2.4.2.2.1. OM 認証機能（SF.OM_I&A）

CWAT 管理者またはサイト管理者がサイトモニタ画面にログオンしようとするときに、サイト管理認証やサイトログオン認証の前に、登録してある OM 認証アカウント所持者であることを識別し、許可を得ている主体であることを認証するものである。

2.4.2.2.2. サイト管理認証機能（SF.CWAT-ADM_I&A）

個別サイト詳細画面にログオンしようとする者が、登録してある CWAT 管理者であることを識別し、本人であることを認証する。

2.4.2.2.3. サイトログオン認証機能（SF.SITE-ADM_I&A）

サイトの OM モニタ画面にログオンしようとする者、ならびに DC 環境設定ファイル管理マネージャ画面から配信インターバル、警告再送最大件数を更新しようとする者が、登録してあるサイト管理者であることを識別し、本人であることを認証する。

2.4.2.3. OPDC 端末ログオン可能ユーザ識別機能（SF.OPDCLOGON_USER_ID）

OPDC 端末にログオン可能ユーザが設定されている場合、端末にログオンしようとする利

用者がログオン可能ユーザであることを識別する機能である。

2.4.2.4. アクセス制御機能

2.4.2.4.1. サイトの統計情報へのアクセス制御機能（SF.SITES-INFO_ACCESS）

監視対象サイトの統計情報へのアクセス（参照）を OM 認証に成功した OM 認証アカウント所持者のみに制限する機能である。

2.4.2.4.2. サイトの管理情報へのアクセス制御機能（SF.SITES-DATA_ACCESS）

監視対象サイトの管理情報へのアクセス（登録、更新、削除、参照）をサイト管理認証に成功した CWAT 管理者のみに制限する機能である。

2.4.2.4.3. サイトの詳細情報へのアクセス制御機能（SF.SITE-DETAIL_ACCESS）

あるサイトの詳細情報（ポリシー情報、警告ログ、配信用ポリシー情報ファイル）へのアクセス（登録、更新、削除、参照、更新の反映、出力、通常配信）を、当該サイトのサイトログオン認証に成功したサイト管理者のみに制限する機能である。

（1） ポリシー情報（DB オブジェクト）

① ノード属性

② ユーザ属性

③ ポリシー

- ユーザログオンポリシー
- 端末使用ポリシー
- 未登録・盗難端末ポリシー
- ネットワークポリシー
- 外部接続機器ポリシー
- ユーザオペレーションポリシー
- メッセンジャーポリシー

（2） 警告ログ（DB オブジェクト）

- オペレーション系警告ログ
- ネットワーク系警告ログ

（3） 配信用ポリシー情報ファイル

2.4.2.5. ポリシー配信強化機能（SF.POLICY_DEL）

2.4.2.5.1. 自動配信機能

OMI にてサイト管理者により設定されたポリシー情報は、配信ファイルとしてサイトの各 DC に配信される。DC はインストール時に設定した上位 NM からポリシー情報を受信する。配信は、配信を受ける DC 側から上位 NM に対してポリシー情報のバージョンを問い合わせ、その結果、自身が保持するファイルよりも上位 NM が保持するポリシー情報のバージョンが新しければ配信要求を行う。要求を受信した上位 NM は、要求元の DC のサイトに対応するポリシー情報を DC に送信する。

2.4.2.5.2. 強制配信機能

サイト管理者は、サイトの各 DC で最新バージョンのポリシーを適用しているかどうかを、DC におけるポリシー情報のバージョンを表示させることにより確認することができる。最新バージョンのポリシーが適用されていない場合、サイト管理者は、サイトの DC に対して最新のポリシーを適用するために、強制配信を行うことができる。

2.4.2.6. 警告ログ送信強化機能（SF.WARNING_LOG_SEND）

警告ログは、ポリシーに反する操作があった場合、OPDC から OMI に送信される。同様に、SDC/UDC で検知した場合も OMI に送信される。警告ログの送信強化の仕組みは次の通りである。

2.4.2.6.1. 異なる方式を併用した警告ログ送信機能

- DC で検知した警告イベントから警告ログを生成し、DC から OMI に即時性の高いプロトコル（OS が提供する UDP）で送信する。警告イベントの警告情報は監査ログにも保存する。
- 指定間隔で DC から OMI に同じ警告ログを、信頼性の高いプロトコル（OS が提供する TCP）で送信する。OMI 側では UDP で受領済みの警告ログかどうかを確認し、未受領であれば TCP で送信された警告ログを受付ける。

2.4.2.6.2. モバイル状態の警告ログ送信機能

- OPDC が動作する PC 端末がモバイル状態となっているなど、OMI が管理していない状態のノードで生成した警告ログは、ネットワーク再接続時に警告再送テンポラリファイルに保存されている警告情報よりネットワーク切断時からの警告ログを抽出し、信頼性の高いプロトコル（OS が提供する TCP）で送信する。

2.4.2.7. セキュリティ管理機能

TOE の管理者が使用する機能であり、それぞれの役割に応じて使用することができる機能である。

2.4.2.7.1. CWAT 管理者によるセキュリティ管理機能（SF.CWAT-ADM）

サイト管理認証に成功した CWAT 管理者のみが、個別サイト詳細画面により、次にあげるセキュリティ管理機能を使用することができる。

（1） 監視対象サイトを新規に登録する機能、監視対象サイトのサイト詳細情報を更新する機能、監視対象サイトを削除する機能。

（2） サイト毎にサイトログオン認証アカウントを登録する機能。一つのサイトにサイトログオン認証アカウントは複数登録することができる。

2.4.2.7.2. サイト管理者によるセキュリティ管理機能（SF.SITE-ADM）

あるサイトのサイトログオン認証に成功したサイト管理者のみが、そのサイトの OM モニタ画面から起動する管理画面、または、DC 環境設定ファイル管理マネージャ画面により、以下のセキュリティ管理機能を使用することができる。

（1） 監視対象サイトのノード属性設定機能

① ノードへのログオン可能ユーザを設定する機能

1. 設定 ON/OFF を設定する機能
2. (ON の場合)ノードへのログオン可能ユーザを設定する機能

② ノードに登録された上位 NM の IP アドレスを参照する機能

③ ノードが保持するポリシー情報のバージョンを参照する機能

1. ノードバージョン ID
2. ユーザバージョン ID
3. ポリシーバージョン ID

（2） ポリシー配信及び警告ログ再送のふるまいを決めるパラメータを設定する機能

① 配信インターバル

② 警告再送最大件数

③ ポリシー違反時の次のアクションを設定する機能

1. 警告ログ発信の ON/OFF
2. 監査ログ出力の ON/OFF

2.4.2.8. 監査機能（SF.AUDIT）

監査機能とは、TOE の管理者の識別認証、および管理画面へのアクセスに関わる監査記録を生成する機能である。

2.5. TOE の保護資産

TOE が保護すべき資産を挙げ、TOE による保護の方針を以下に示す。

- ポリシー情報

  ポリシーは、サイトに属するノードに対するセキュリティポリシー、及びサイトに属するユーザに対するセキュリティポリシーを定義したものである。ポリシーを設定するには、ノード属性、ユーザ属性が必要であるため、ポリシー情報には、ポリシーだけでなく、ノード属性やユーザ属性も含めるものとする。設定されたポリシー情報は配信ファイルとして、ネットワークを介して OMI サーバから直接 OPDC が動作する PC 端末、または SDC/UDC サーバを経由して OPDC が動作する PC 端末に配信される。同様に、SDC/UDC で使用されるポリシーは、OMI から SDC/UDC に配信される。本 TOE では、ポリシー情報は正当な者のみが設定可能とすること、さらに OMI で設定されたポリシー情報が DC に確実に配信されることが求められる。

- 警告ログ

  警告ログは、OPDC でポリシーに反する操作が行われると、リアルタイムで OPDC が動作する PC 端末から直接 OMI サーバに送信されてデータベースに保存される。また SDC/UDC サーバで検知した場合も同様に直接 OMI サーバに送信される。本 TOE では、警告ログが確実に OMI サーバに送信されることが求められる。

- OPDC のサービス

  本 TOE では、OPDC が動作する PC 端末上で、OPDC のサービスが正しく稼動していることが必要である。

3. TOE セキュリティ環境

3.1. 前提条件

- A.ADMIN（システム管理者の信頼性）
  システム管理者は信頼できる人物であり、TOE のシステム管理者として実施すべき職務を遂行するものとする。

- A.CWAT_ADMIN（CWAT 管理者の信頼性）
  サイト管理認証アカウント所有者は CWAT 管理者として与えられた役割を遂行するものとする。

- A.SITE_ADMIN（サイト管理者の信頼性）
  サイトログオン認証アカウント所有者はサイト管理者として、自身が属するサイトの管理における与えられた役割を遂行するものとする。また、TOE の運用に対して脅威となる行為は行わない。

- A.INSTALL（インストールの信頼性）
  各専用サーバへの OMI、SDC、UDC 及び LC のインストール・設定・アンインストール、各 PC 端末への OPDC のインストール・設定・アンインストールは、システム管理者の管理の下に実施されるものとする。

- A.PC_USER_ROLE（PC 端末利用者の権限）
  OPDC が動作する PC 端末を利用する管理者以外の端末利用者は、システム管理者によって各 PC 端末の OS である Windows 上に設定された Users 権限グループのみに属するアカウントを使用する。各 PC 端末の Users 権限グループ以外のアカウントは、システム管理者のみが利用可能となるような設定を維持することとする。
  OMI クライアントが動作する PC 端末は、上記のシステム管理者の OS アカウントのほか、TOE の管理者としてその端末の利用を許可する CWAT 管理者もしくはサイト管理者の OS アカウントを設定する。

- A.PASSWORD_MANAGEMENT（パスワード管理）
  TOE にアクセスするためのアカウント（OM 認証、サイト管理認証、サイトログオン認証）のパスワードは、主体以外の他者に知られないように主体によって管理する。パスワードは推測・解析されにくいものが設定され、時間経過とともに適正な間隔で変更する。

- A.PHYSICAL_PROTECTION（サーバ設置場所の保護）
  OMI、SDC、UDC 及び LC をインストールする各専用サーバは、コンピュータセンターなど、その組織で運用するシステムの管理・運用のために許可された者のみが入室可能な物理的に保護された区域に設置する。また、OMI 機能、SDC、UDC、LC の操作は、サーバが設置された区域でのみ可能となるように TOE の操作環境を設定する。物理的に保護された区域以外から OMI 機能を使用する場合は、端末に OPDC をインストールした上で OMI クライアントをインストールするものとする。

- A.NETWORK_RELIABILITY（ネットワークの信頼性）
  外部ネットワークからの攻撃はネットワーク機器等の適切な設定により防御されるものとする。

3.2. 脅威

攻撃者として、OPDC が動作する PC 端末の利用を許可された端末利用者、及び OPDC が動作する PC 端末の利用を許可されていない不正アクセス者が想定される。これらの攻撃者は、PC 端末を利用するにあたって OPDC に配信されたポリシーに逸脱した端末操作を行おうとする者である。また、サーバ設置場所に入室を許可された者のうち、TOE の管理者の役割を持たない者が OMI などのサーバ端末にログオンして TOE に不正にアクセスする攻撃も想定される。

本 TOE が想定する攻撃者の攻撃能力は低レベルとする。

なお、攻撃者ではないが、データ送信に関する脅威のトリガーとして、一時的なネットワーク障害も想定する。

- T.EVIL_POLICY_VIA_SERVER（サーバ経由の不正なポリシーの設定）
  サーバ設置場所に入室許可を与えられた者のうち TOE の管理者の役割を持たない者が OMI サーバ端末に不正にログオンすることにより、不正なポリシー情報の設定を行うかもしれない。

- T.EVIL_POLICY_VIA_OPDC（OPDC 端末経由の不正なポリシーの設定）
  TOE の管理者としての役割を持たない者が、OPDC 端末から TOE を使用せずにポリシー情報へのアクセスを試み、不正なポリシー情報の設定を行うかもしれない。

- T.FAIL_SEND_POLICY（ポリシー配信の失敗）

通信パケットの破損もしくは一時的なネットワーク障害により、OMI から DC へのポリシー情報の配信が失敗し、最新のバージョンのポリシー情報が DC に届かないかもしれない。

- T.LOSS_WARNING_LOG（警告情報の消失）
  攻撃者が OPDC で発生した警告ログを OMI サーバに送信しないよう PC 端末をネットワークから切り離したり、DC で発生した警告ログが一時的なネットワーク障害により喪失することにより、OMI が警告ログを正しく受信しモニタリングすることができなくなるかもしれない。

- T.STOP_OPDC_INTENTIONALLY（サービスの停止）
  攻撃者が、PC 端末上で稼動している OPDC のプロセスを不正に停止させることにより、OPDC のサービスが停止するかもしれない。

3.3. 組織のセキュリティ方針

- P.AUDIT（監査記録の生成）
  TOE の利用者の識別認証、及び管理画面へのアクセスに関わる監査記録を生成できなければならない。

- P.SITE_POLICY（サイトのセキュリティ方針）
  サイトのポリシー情報、警告ログ、及びそれに付随するデータ（サイトの統計情報、サイトの管理情報）は、そのサイトの管理・監視の責任を持つサイト管理者の操作に制限できなければならない。

4. セキュリティ対策方針

4.1. TOE セキュリティ対策方針

- O.I&A（OMI の識別認証）
  TOE は、OM 認証アカウント所持者、CWAT 管理者及びサイト管理者が OMI を利用するときは、データにアクセスする画面に応じて確実に識別・認証しなければならない。

- O.LIMIT_LOGON_USER（OPDC 端末のログオン可能ユーザの設定）
  TOE は、OPDC 端末にログオン可能なユーザを設定できなければならない。
  TOE は、OPDC 端末にログオン可能なユーザが設定されている場合、それ以外のユーザが当該 OPDC 端末にログオンすることを拒否しなければならない。

- O.ACCESS_CONTROL（アクセス制御）
  TOE は、ポリシー情報、警告ログ、及びそれに付随するデータ（サイトの統計情報、サイトの管理情報）へのアクセスを、許可された TOE の管理者に制限しなければならない。

- O.ENHANCED_DELIVERING（ポリシー配信強化機能）
  TOE は、OMI からポリシー情報を DC に配信する機能を強化し、配信失敗や未配信を検出し、所定のタイミングで最新のバージョンのポリシーを配信しなければならない。

- O.ENHANCED_WL_SENDING（警告ログの送信強化機能）
  TOE は、警告ログを DC から OMI に送信する機能を強化し、送信失敗の検出時や未送信となった事象に備え、所定のタイミング、異なる方法、及び送信パケット量を制御したうえで、警告ログを再送信しなければならない。

- O.MANAGE（セキュリティ管理）
  TOE の管理者はその役割に応じて、TOE のセキュリティ機能のふるまいの設定、セキュリティ機能に関係するデータの管理を行わなければならない。

- O.AUDIT（監査記録の生成）
  TOE は、TOE の管理者の識別認証、及び管理画面のアクセスに関わる監査記録を生成できなければならない。

4.2. 環境セキュリティ対策方針

4.2.1. IT 環境のセキュリティ対策方針

- OE.OS_DB（TOE を動作させる OS や DBMS の機能）
  - TOE を動作させる OS は、利用者の識別・認証機能を提供する。
  - TOE を動作させる全てのサーバ、及び端末上の OS の Administrator 権限は、特定の管理者だけに限定する機能を有するものとする。
  - TOE を動作させる OS は、OS 上で動作するサービスの自動回復機能を提供する。
  - OMI サーバにインストールされる DBMS は、識別・認証機能を具備し、TOE のコンポーネントからアクセスするための手段を提供する。

4.2.2. 非 IT 環境のセキュリティ対策方針

- OE-N.ADMIN（システム管理者の適格性）
  システム管理者は、求められる職務遂行において信頼できる人物を選任する。

- OE-N.CWAT_ADMIN（CWAT 管理者の適格性）
  CWAT 管理者は、求められる役割を適切に遂行する者を割り当てる。

- OE-N.SITE_ADMIN（サイト管理者の適格性）
  サイト管理者は、TOE に脅威を与えない運用方法を理解し、自身が属するサイトの管理において求められる役割を適切に遂行する者を割り当てる。

- OE-N.INSTALL（インストールの信頼性）
  システム管理者は、自らの責任において、専用サーバ及び PC 端末への TOE のインストール・設定・アンインストールを適切に行なうものとする。

- OE-N.PC_USER_ROLE（PC 端末利用者の権限）
  システム管理者は、OPDC が動作する PC 端末を管理者以外の端末利用者に利用させるときには、OS である Windows 環境に Users 権限グループのみに属するアカウントを設定し、この PC 端末を利用する端末利用者に対して、このアカウントを利用させる。また、各 PC 端末の Users 権限グループ以外のアカウントは、システム管理者のみが利用可能となるように設定し、これらのアカウントの管理はシステム管理者のみとなるように PC 端末の利用権限を管理する。

システム管理者は、OMI クライアントが動作する PC 端末に対しては、自身の OS アカウント以外に、TOE の管理者としてその端末の利用を許可する CWAT 管理者もしくはサイト管理者の OS アカウントを設定する。また、サイト管理者は、O.LIMIT_LOGON_USER を実現する TOE 機能を使用して、その OPDC 端末へのログオンユーザを、その OPDC 端末の利用を許可する TOE の管理者のみに制限する。

- OE-N.PASSWORD_MANAGEMENT（パスワード管理）
  TOE にアクセスするためのアカウント（OM 認証、サイト管理認証、サイトログオン認証）のパスワードは、主体以外の他者に知られないように主体によって管理する。パスワードは推測・解析されにくいものを設定し、時間経過とともに適正な間隔で変更する。

- OE-N.PHYSICAL_PROTECTION（サーバ設置場所の保護）
  システム管理者は、TOE をインストールした専用サーバを、コンピュータセンターなどその組織で運用するシステムの管理・運用のために許可された者のみが入室可能な物理的に保護された区域に設置する。また、専用サーバ上のソフトウェアの操作は、サーバが設置された区域でのみ可能となるように TOE の操作環境を設置・設定する。物理的に保護された区域以外から OMI 機能を使用する場合は、端末に OPDC をインストールした上で OMI クライアントをインストールする。

- OE-N.NETWORK_RELIABILITY（ネットワークの信頼性）
  システム管理者は、ネットワーク機器（ファイアウォール等）を適切に設置･設定し、外部ネットワークからの攻撃を受けることのないように、TOE を配置するネットワークを適正に設定･維持する。

- OE-N.RECOVER（サービスの復元）
  システム管理者は、OPDC サービスが停止すると、ただちに OPDC サービスを回復するように、PC 端末のサービス設定を行なう。

5. IT セキュリティ要件

5.1. TOE セキュリティ要件

5.1.1. TOE セキュリティ機能要件

＜ラベルによる識別方法＞
CC パート 2 で定義されたセキュリティ機能要件を再現する場合、ラベルも同一のものを使用する。CC パート 2 の拡張要件については本 ST にて独自にラベルを設定する。
＜セキュリティ機能要件の操作の明示方法＞
割付または選択は、それぞれ対象箇所を個別に明示し、イタリックかつボールドで示す。詳細化はステートメントの対象箇所をアンダーラインで示し、詳細化した内容を（）内に示す。繰り返しはラベルの後ろにアルファベットを付加する。IT 環境のセキュリティ機能要件は、ラベルの後ろに[E]を付加する。

FAU_GEN.1 監査データ生成

下位階層： なし
依存性： FPT_STM.1

FAU_GEN.1.1 TSF は以下の監査対象事象の監査記録を生成できなければならない：

a) 監査機能の起動と終了；
b) 監査の[選択：*最小*、*基本*、*詳細*、*指定なし*：から一つのみ選択]レベルのすべての監査対象事象；及び
c) [割付：*上記以外の個別に定義した監査対象事象*]。

[選択：*最小*、*基本*、*詳細*、*指定なし*：から一つのみ選択]：***指定なし***
[割付：*上記以外の個別に定義した監査対象事象*]：***以下の監査対象事象***

表 5-1 監査対象とすべきアクション（CC における規定)と関連する監査対象事象

機能要件		監査対象とすべきアクション	監査対象事象
FAU	FAU_GEN.1	なし	なし
FDP	FDP_ACC.1a	なし	なし

	FDP_ACF.1a	a) 最小: SFP で扱われるオブジェクトに対する操作の実行における成功した要求。 b) 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求。 c) 詳細: アクセスチェック時に用いられる特定のセキュリティ属性。	a) 管理権限に基づき管理画面を開く事象 a) 管理権限に基づき管理画面からアクションを実行する事象
	FDP_ACC.1b	なし	なし
	FDP_ACF.1b	a) 最小: SFP で扱われるオブジェクトに対する操作の実行における成功した要求。 b) 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求。 c) 詳細: アクセスチェック時に用いられる特定のセキュリティ属性。	a) 管理権限に基づき管理画面を開く事象 a) 管理権限に基づき管理画面からアクションを実行する事象
	FDP_ACC.1c	なし	なし
	FDP_ACF.1c	a) 最小: SFP で扱われるオブジェクトに対する操作の実行における成功した要求。 b) 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求。 c) 詳細: アクセスチェック時に用いられる特定のセキュリティ属性。	なし （P.AUDIT で規定する監査記録生成に該当しない）
	FDP_IFC.1	なし	なし
	FDP_IFF.1	a) 最小: 要求された情報フローを許可する決定。 b) 基本: 情報フローに対する要求に関するすべての決定。 c) 詳細: 情報フローの実施を決定する上で用いられる特定のセキュリティ属性。 d) 詳細: 方針目的(policy goal)に基づいて流れた特定の情報のサブセット(例えば、対象物のレベル低下の監査)。	なし （P.AUDIT で規定する監査記録生成に該当しない）
	FDP_ITT.1a	a) 最小: 使用された保護方法の識別を含む、利用者データの成功した転送。 b) 基本: 使用された保護方法と生じたいかなる誤りも含む、利用者データを転送するためのすべての試み。	なし （P.AUDIT で規定する監査記録生成に該当しない）
	FDP_ITT.1b	a) 最小: 使用された保護方法の識別を含む、利用者データの成功した転送。 b) 基本: 使用された保護方法と生じたいかなる誤りも含む、利用者データを転送するためのすべての試み。	なし （P.AUDIT で規定する監査記録生成に該当しない）
FIA	FIA_AFL.1	a) 最小: 不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション(例えば端末の停止)、もし適切であれば、正常状態への復帰(例えば端末の再稼動)。	a) 不成功の認証試行に対する閾値への到達及びそれに続いて取られるアクション（正常状態への復帰は規定された処理であり監査データ生成は不要）
	FIA_SOS.1	a) 最小: TSF による、テストされた秘密の拒否; b) 基本: TSF による、テストされた秘密の拒否または受け入れ; c) 詳細: 定義された品質尺度に対する変更の識別。	a) TSF によるテストされた秘密の拒否

	FIA_UAU.2a	a) 最小: 認証メカニズムの不成功になった使用; b) 基本: 認証メカニズムのすべての使用。	b) 認証メカニズムのすべての使用
	FIA_UAU.2b	a) 最小: 認証メカニズムの不成功になった使用; b) 基本: 認証メカニズムのすべての使用。	b) 認証メカニズムのすべての使用
	FIA_UAU.2c	a) 最小: 認証メカニズムの不成功になった使用; b) 基本: 認証メカニズムのすべての使用。	b) 認証メカニズムのすべての使用
	FIA_UAU.7	なし	なし
	FIA_UID.2a	a) 最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用; b) 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。	b) 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用
	FIA_UID.2b	a) 最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用; b) 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。	b) 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用
	FIA_UID.2c	a) 最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用; b) 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。	b) 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用
	FIA_UID.2d	a) 最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用; b) 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。	b) 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用
FMT	FMT_MOF.1	a) 基本: TSF の機能のふるまいにおけるすべての改変。	a) TSF の機能のふるまいにおけるすべての改変
	FMT_MSA.1a	a) 基本: セキュリティ属性の値の改変すべて。	a) 基本: セキュリティ属性の値の改変すべて。
	FMT_MSA.1b	a) 基本: セキュリティ属性の値の改変すべて。	a) 基本: セキュリティ属性の値の改変すべて。
	FMT_MSA.3a	a) 基本: 許可的あるいは制限的規則のデフォルト設定の改変。 b) 基本: セキュリティ属性の初期値の改変すべて。	a) 基本: その他の規則のデフォルト設定の改変。
	FMT_MSA.3b	a) 基本: 許可的あるいは制限的規則のデフォルト設定の改変。 b) 基本: セキュリティ属性の初期値の改変すべて。	a) 基本: その他の規則のデフォルト設定の改変。
	FMT_MSA.3c	a) 基本: 許可的あるいは制限的規則のデフォルト設定の改変。 b) 基本: セキュリティ属性の初期値の改変すべて。	a) 基本: その他の規則のデフォルト設定の改変。
	FMT_MSA.3d	a) 基本: 許可的あるいは制限的規則のデフォルト設定の改変。 b) 基本: セキュリティ属性の初期値の改変すべて。	a) 基本: その他の規則のデフォルト設定の改変。
	FMT_MTD.1a	a) 基本: TSF データの値のすべての改変。	a) TSF データの値のすべての改変
	FMT_MTD.1b	a) 基本: TSF データの値のすべての改変。	a) TSF データの値のすべての改変
	FMT_MTD.1c	a) 基本: TSF データの値のすべての改変。	a) TSF データの値のすべての改変
	FMT_SMF.1	a) 最小：管理機能の使用	a) 管理機能の使用

	FMT_SMR.1a	a）最小:役割の一部をなす利用者のグループに対する改変; b）詳細：役割の権限の使用すべて;	なし（利用者への役割の割当は利用者を生成する段階で固定で決まるため）
FPT	FPT_FLS.1	a）基本：TSF の障害。	なし （P.AUDIT で規定する監査記録生成に該当しない）
	FPT_RVM.1	なし	なし
	FPT_SEP.1	なし	なし
	FPT_STM.1	a）最小：時間の変更 b）詳細：タイムスタンプの提供	なし （P.AUDIT で規定する監査記録生成に該当しない）

※上記の監査対象事象でプロダクトを指定していない場合は OMI の事象とする

FAU_GEN.1.2 TSF は、各監査記録において少なくとも以下の情報を記録しなければならない：

a） 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果（成功または失敗）；及び

b） 各監査事象の種別に対して、PP／ST の機能コンポーネントの監査対象事象の定義に基づいた[割付：*その他の監査関連情報*]

[割付：*その他の監査関連情報*]：***なし***

FDP_ACC.1a サブセットアクセス制御

下位階層： なし

依存性： FDP_ACF.1

FDP_ACC.1.1a 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：*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*]：***アクセス制御の対象となるサブジェクトとして以下のプロセス、オブジェクトとして以下の DB オブジェクト、サブジェクトとオブジェクトの操作***

サブジェクト	オブジェクト	操作
プロセス	DB オブジェクト	参照、更新、削除、登録

[割付：*アクセス制御 SFP*]：***OM 認証プロセスおよびサイト管理認証プロセスのデータへのアクセス制御方針***

FDP_ACF.1a 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、FMT_MSA.3

FDP_ACF.1.1a 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：*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
プロセス	プロセス種別
オブジェクト	セキュリティ属性
DB オブジェクト	DB オブジェクト種別

[割付：*アクセス制御 **SFP***]：***OM 認証プロセスおよびサイト管理認証プロセスのデータへのアクセス制御方針***

FDP_ACF.1.2a 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*]：

- ***プロセス種別が OM 認証プロセスであるプロセスにのみ、DB オブジェクト種別がサイトの統計情報であるすべての DB オブジェクトの参照を許可する。***
- ***プロセス種別がサイト管理認証プロセスであるプロセスにのみ、DB オブジェクト種別がサイトの管理情報であるすべての DB オブジェクトの参照、更新、削除、登録を許可する。***

FDP_ACF.1.3a TSF は、以下の追加規則に基づいて、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承認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のサブジェクトに対するアクセスを明示的に承認する規則*]

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

FDP_ACF.1.4a 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***

FDP_ACC.1b サブセットアクセス制御

下位階層：　なし

依存性：　FDP_ACF.1

FDP_ACC.1.1b 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：*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*]：***アクセス制御の対象となるサブジェクトとして以下のプロセス、オブジェクトとして以下の DB オブジェクトとファイル、サブジェクトとオブジェクトの操作***

サブジェクト	オブジェクト	操作
プロセス	DB オブジェクト	登録、参照、削除、更新、更新の反映、出力
	配信用ポリシー情報ファイル	通常配信、強制配信

[割付：*アクセス制御 **SFP***]：***サイトログオン認証プロセスのデータへのアクセス制御方針***

FDP_ACF.1b 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、FMT_MSA.3

FDP_ACF.1.1b 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：*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
プロセス	プロセス種別、サイト ID
オブジェクト	セキュリティ属性
DB オブジェクト	DB オブジェクト種別、サイト ID
配信用ポリシー情報ファイル	サイト ID

[割付：*アクセス制御 SFP*]：***サイトログオン認証プロセスのデータへのアクセス制御方針***

FDP_ACF.1.2b 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*]：

- ***プロセス種別がサイトログオン認証プロセスであるプロセスに、DB オブジェクトまたはファイルに対する以下の操作を許可する。***
  - ***サイトログオン認証プロセスと同じサイト ID であり、かつ DB オブジェクト種別がポリシー情報である DB オブジェクトの参照、更新、削除、登録、更新の反映を許可する。ここで更新の反映とは、指定した DB オブジェクトから配信用ポリシー情報ファイルを生成し、サイト ID で特定される反映用フォルダに格納することである。***
  - ***サイトログオン認証プロセスと同じサイト ID であり、かつ DB オブジェクト種別***

が警告ログである DB オブジェクトの参照、出力を許可する。

- *サイトログオン認証プロセスと同じサイト ID の反映用フォルダに格納された配信用ポリシー情報ファイルを、同じサイト ID の配信用フォルダに格納すること（通常配信）を許可する。*
- *サイトログオン認証プロセスと同じサイト ID の配信用フォルダに格納され、かつ指定したファイル種別である配信用ポリシー情報ファイルを、指定したノードへ強制配信することを許可する。*

FDP_ACF.1.3b TSF は、以下の追加規則に基づいて、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承認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のサブジェクトに対するアクセスを明示的に承認する規則*]

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

FDP_ACF.1.4b 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***

FDP_ACC.1c サブセットアクセス制御

下位階層：　なし

依存性：　FDP_ACF.1

FDP_ACC.1.1c 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：*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*]：***アクセス制御の対象となるサブジェクトとして以下のプロセス、オブジェクトとして以下の TOE の機能、サブジェクトとオブジェクトの操作***

サブジェクト	オブジェクト	操作
DC プロセス	上位 NM プロセスが管理する配信用ポリシー情報ファイル	配信

[割付：*アクセス制御 SFP*]：***配信用ポリシー情報ファイルへのアクセス制御方針***

FDP_ACF.1c 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、FMT_MSA.3

FDP_ACF.1.1c 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：*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
DC プロセス	・ DC で保持するポリシー情報のバージョン ・ サイト ID
オブジェクト	セキュリティ属性
配信用ポリシー情報ファイル	サイト ID、バージョン、ファイル種別

[割付：*アクセス制御 SFP*]：***配信用ポリシー情報ファイルへのアクセス制御方針***

FDP_ACF.1.2c 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*]：

- ***以下の両条件を満たす場合、上位 NM から DC プロセスへの該当するファイル種別の配信用ポリシー情報ファイルの配信を許可する。***
  - ***上位 NM に存在する配信用ポリシー情報ファイルを含むフォルダのサイト ID が DC プロセスのサイト ID と同じ場合。***
  - ***上位 NM に存在する、あるファイル種別の配信用ポリシー情報ファイルのバージョンが当該 DC が保持する同じファイル種別の配信用ポリシー情報ファイルのバージョンよりも大きい場合。***

FDP_ACF.1.3c TSF は、以下の追加規則に基づいて、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承認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のサブジェクトに対するアクセスを明示的に承認する規則*]

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

FDP_ACF.1.4c 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***

FDP_IFC.1 サブセット情報フロー制御

下位階層： なし

依存性： FDP_IFF.1

FDP_IFC.1.1 TSF は、[割付: *サブジェクト、情報、及び、SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト*]に対して[割付: *情報フロー制御 SFP*]を実施しなければならない。

[割付: *サブジェクト、情報、及び、SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト*]：***情報フロー制御***

の対象となるサブジェクト、情報、情報の流れを引き起こす操作は以下の通り。

サブジェクト	情報	操作
送付元：DC プロセス 送付先：OMI プロセス	警告ログ	送信、受領

[割付：*アクセス制御 SFP*]：***警告ログ情報フロー制御方針***

FDP_IFF.1 単純セキュリティ属性

下位階層：　　なし

依存性：　　FDP_IFC.1、FMT_MSA.3

FDP_IFF.1.1 TSF は、以下のサブジェクト及び情報のセキュリティ属性の種別に基づいて、[割付: *情報フロー制御 SFP*]を実施しなければならない。[割付: *示された SFP 下において制御されるサブジェクトと情報のリスト、及び各々のセキュリティ属性*]。

[割付: *情報フロー制御 SFP*]：***警告ログ情報フロー制御方針***

[割付: *示された SFP 下において制御されるサブジェクトと情報のリスト、及び各々のセキュリティ属性*]：

サブジェクト	セキュリティ属性
送付元：DC プロセス	・　OMI の IP アドレス ・　サイト ID
送付先：OMI プロセス	・　IP アドレス
情報	セキュリティ属性
警告ログ	・　サイト ID

FDP_IFF.1.2 TSF は、以下の規則が保持されていれば、制御された操作を通じて、制御されたサブジェクトと制御された情報間の情報フローを許可しなければならない: [割付: *各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係*]

[割付: *各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係*]：

・　***DC プロセスで発生した警告ログのサイト ID が DC プロセスのサイト ID と同じ場合、***

DC プロセスが保持する OMI の IP アドレスに対して警告ログの送信を許可する。

- ***送信された警告ログのサイト ID が、IP アドレスで特定される OMI プロセスが保持するサイト ID リストに含まれる場合、OMI プロセスが警告ログを当該サイトのものとして受領することを許可する。***

FDP_IFF.1.3 TSF は、[割付: *追加の情報フロー制御 SFP 規則*]を実施しなければならない。

[割付: *追加の情報フロー制御 SFP 規則*]: ***なし***

FDP_IFF.1.4 TSF は、以下の[割付: *追加の SFP 能力のリスト*]を提供しなければならない。

[割付: *追加の SFP 能力のリスト*]:

- ***DC プロセスから OMI プロセスへ、即時性の高いプロトコルおよび信頼性の高いプロトコルによって警告ログを送信する処理（OS が提供）に受け渡す能力を提供する。***

FDP_IFF.1.5 TSF は、以下の規則に基づいて、情報フローを明示的に承認しなければならない。[割付: *セキュリティ属性に基づいて、明示的に情報フローを承認する規則*]

[割付: *セキュリティ属性に基づいて、明示的に情報フローを承認する規則*]: ***なし***

FDP_IFF.1.6 TSF は、次の規則に基づいて、情報フロー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、明示的に情報フローを拒否する規則*]

[割付: *セキュリティ属性に基づいて、明示的に情報フローを拒否する規則*]: ***なし***

FDP_ITT.1a 基本内部転送保護

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]

FDP_ITT.1.1a TSFは、利用者データ（配信用ポリシー情報ファイル）がTOEの物理的に分離されたパート間を転送される場合、その[選択: *暴露、改変、使用不可*]を防ぐための[割付:

アクセス制御SFP(s)及びまたは情報フロー制御SFP(s)]を実施しなければならない。

[選択: *暴露*、*改変*、*使用不可*]：***使用不可***
[割付: *アクセス制御 SFP(s)及びまたは情報フロー制御 SFP(s)*]：***配信用ポリシー情報ファイルへのアクセス制御方針***

FDP_ITT.1b 基本内部転送保護
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]

FDP_ITT.1.1b TSFは、利用者データ（警告ログ）がTOEの物理的に分離されたパート間を転送される場合、その[選択: *暴露*、*改変*、*使用不可*]を防ぐための[割付: *アクセス制御SFP(s)及びまたは情報フロー制御SFP(s)*]を実施しなければならない。

[選択: 暴露、改変、使用不可]：***使用不可***
[割付: *アクセス制御 SFP(s)及びまたは情報フロー制御 SFP(s)*]：***警告ログ情報フロー制御方針***

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

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*]：
- ***OM 認証アカウントによる認証***
- ***サイト管理認証アカウントによる認証***
- ***サイトログオン認証アカウントによる認証***

[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」]：**正の整数値：3**

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*]：

- ***認証実行時において、一つの ID につき 3 回の認証失敗を検知すると 10 秒間操作不能とし、エラー回数が上限を超えた旨のエラーメッセージのポップアップ画面を表示する。***
- ***OK ボタン押下により認証画面が終了し、再度、認証画面を立ち上げることにより、ID とパスワードが入力可能な状態とする。***

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（OM認証パスワード、サイト管理認証パスワード、サイトログオン認証パスワード）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*]：***8 文字以上 32 文字以下の ASCII 英数小文字（36 文字）***

FIA_UAU.2a アクション前の利用者認証

下位階層：　　FIA_UAU.1

依存性：　　FIA_UID.1

FIA_UAU.2.1a TSFは、その利用者（OM認証アカウント）を代行する他のTSF調停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_UAU.2b アクション前の利用者認証

下位階層：　　FIA_UAU.1

依存性：　　FIA_UID.1

FIA_UAU.2.1b TSFは、その利用者（サイト管理認証アカウント）を代行する他のTSF調停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_UAU.2c アクション前の利用者認証

下位階層： FIA_UAU.1

依存性： FIA_UID.1

FIA_UAU.2.1c TSFは、その利用者（サイトログオン認証アカウント）を代行する他のTSF調停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_UAU.7 保護された認証フィードバック

下位階層： なし

依存性： FIA_UAU.1

FIA_UAU.7.1 TSFは、認証（OM認証、サイト管理認証、サイトログオン認証）を行っている間、[割付: *フィードバックのリスト*]だけを利用者に提供しなければならない。

[割付: *フィードバックのリスト*] : ***認証情報として入力した文字数分の"*"文字***

FIA_UID.2a アクション前の利用者識別

下位階層： FIA_UID.1

依存性： なし

FIA_UID.2.1a TSFは、その利用者（OM認証アカウント）を代行する他のTSF調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

FIA_UID.2b アクション前の利用者識別

下位階層：　　FIA_UID.1
依存性：　　なし

FIA_UID.2.1b TSFは、その利用者（サイト管理認証アカウント）を代行する他のTSF調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

FIA_UID.2c アクション前の利用者識別
下位階層：　　FIA_UID.1
依存性：　　なし

FIA_UID.2.1c TSFは、その利用者（サイトログオン認証アカウント）を代行する他のTSF調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

FIA_UID.2d アクション前の利用者識別
下位階層：　　FIA_UID.1
依存性：　　なし

FIA_UID.2.1d TSFは、その利用者（OPDC端末ログオン可能ユーザ）を代行する他のTSF調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

FMT_MOF.1 セキュリティ機能のふるまいの管理
下位階層：　　なし
依存性：　　FMT_SMF.1、FMT_SMR.1

FMT_MOF.1.1 TSF は、機能[割付：*以下の機能のリスト*][選択：*のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]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。

機能のリスト	ふるまいの管理	許可された識

		別された役割
配信インターバルを変更することによって、ポリシー配信強化機能（自動配信機能）	のふるまいを改変する	当該サイトのサイト管理者
配信インターバルを変更することによって、警告ログ送信強化機能	のふるまいを改変する	
警告再送最大件数を変更することによって、警告ログ送信強化機能	のふるまいを改変する	
ポリシー違反時の警告発信をOFFに設定することによって、警告ログ送信強化機能	を停止する	
ポリシー違反時の監査ログ出力設定をOFFに設定することによって、警告ログ送信強化機能	を停止する	
ノードにログオン可能なユーザの設定をON/OFFにすることによって、OPDCログオン可能ユーザ識別機能	のふるまいを改変する	

FMT_MSA.1a セキュリティ属性の管理

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_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

FMT_MSA.1.1a 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*]に制限するために[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。

セキュリティ属性のリスト	操作	許可された識別された役割
サイト属性 サイトID	問い合わせ、改変、削除、[その他操作：登録]	CWAT管理者

[割付: アクセス制御SFP、情報フロー制御SFP] : ***OM認証プロセスおよびサイト管理認証プロセスのデータへのアクセス制御方針***

FMT_MSA.1b セキュリティ属性の管理

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_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

FMT_MSA.1.1b 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*]に制限するために[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。

セキュリティ属性のリスト	操作	許可された識別された役割
ノード属性 バージョン	問い合わせ	当該サイトのサイト管理者

[割付: アクセス制御 SFP、情報フロー制御 SFP] : ***サイトログオン認証プロセスのデータへのアクセス制御方針***

FMT_MSA.3a 静的属性初期化

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.3.1a 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（DBオブジェクト種別）として、[選択: *制限的*、*許可的*、[割付 : *その他の特性*]: から一つのみ選択]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。

[選択: *制限的*、*許可的*、[割付 : *その他の特性*]: から一つのみ選択] : 制限的

[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*] : ***OM 認証プロセス及びサイト管理認証プロセスのデータへのアクセス制御方針***

FMT_MSA.3.2a 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指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***

FMT_MSA.3b 静的属性初期化

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.3.1b 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（サイトID、DBオブジェクト種別）として、[選択: *制限的*、*許可的*、[割付 ： *その他の特性*] ：から一つのみ選択]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。

[選択: *制限的*、*許可的*、[割付 ： *その他の特性*]：から一つのみ選択] ：制限的

[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*] ：***サイトログオン認証プロセスのデータへのアクセス制御方針***

FMT_MSA.3.2b 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指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***

FMT_MSA.3c 静的属性初期化

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.3.1c 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（サイトID、バージョン、ファイル種別）として、[選択: *制限的*、*許可的*、[割付 ： *その*

他の特性] ： から一つのみ選択]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。

[選択: *制限的*、*許可的*、[割付 ： *その他の特性*]： から一つのみ選択] ：制限的

[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*] ：***配信用ポリシー情報ファイルへのアクセス制御方針***

FMT_MSA.3.2c 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指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***

FMT_MSA.3d 静的属性初期化

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.3.1d 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（サイトID）として、[選択: *制限的*、*許可的*、[割付 ： *その他の特性*]： から一つのみ選択]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。

[選択: *制限的*、*許可的*、[割付 ： *その他の特性*]： から一つのみ選択] ：制限的

[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*] ：***警告ログ情報フロー制御方針***

FMT_MSA.3.2d 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指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***

FMT_MTD.1a TSF データの管理

下位階層： なし

依存性： FMT_SMF.1、FMT_SMR.1

FMT_MTD.1.1a 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。

TSF データのリスト	操作	許可された識別された役割
サイト属性 サイトログオン認証アカウント ID サイトログオン認証アカウントのパスワード	問い合わせ、改変、削除、[その他操作：登録]	CWAT 管理者

FMT_MTD.1b TSF データの管理

下位階層： なし

依存性： FMT_SMF.1、FMT_SMR.1

FMT_MTD.1.1b 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。

TSF データのリスト	操作	許可された識別された役割
ノード属性 ノード（OPDC 端末）にログオン可能なユーザ	問い合わせ、改変、削除、[その他操作：登録]	当該サイトのサイト管理者

FMT_MTD.1c TSF データの管理

下位階層： なし

依存性： FMT_SMF.1、FMT_SMR.1

FMT_MTD.1.1c 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。

TSF データのリスト	操作	許可された識別された役割
OM 認証アカウント ID	問い合わせ、改変、削除、[その他操作：登録]	管理者
OM 認証アカウントのパスワード		
サイト管理認証アカウント ID		
サイト管理認証アカウントのパスワード		

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、以下のセキュリティ管理機能を行う能力を持たねばならない：[割付：*TSF によって提供されるセキュリティ管理機能のリスト*]。

[割付：*TSF によって提供されるセキュリティ管理機能のリスト*]：

以下のセキュリティ管理機能のリスト

- ***配信インターバルの制御によるポリシー配信強化機能の有効化・無効化***
- ***配信インターバル、再送最大件数、ポリシー違反時の警告発信設定、および監査ログ出力設定の制御による警告ログ送信強化機能の有効化・無効化***
- ***OPDC ログオン可能ユーザ設定の制御による OPDC ログオン可能ユーザ識別機能の有効化・無効化***
- ***サイト属性（サイト ID、サイトログオン認証アカウント ID、サイトログオン認証アカウントパスワード）の問い合わせ、改変、登録、削除***
- ***ノード（OPDC 端末）にログオン可能なユーザの問い合わせ、改変、登録***
- ***ノード属性（上位 NM の IP アドレス、配信済みの配信用ポリシー情報のバージョン）の問い合わせ***
- ***OM 認証アカウント（ID,パスワード）の問い合わせ、改変、削除、登録***
- ***サイト管理認証アカウント（ID,パスワード）の問い合わせ、改変、削除、登録***

FMT_SMR.1a セキュリティ役割

下位階層： なし

依存性： FIA_UID.1

FMT_SMR.1.1a 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*]：

- ***OM 認証アカウント所持者***
- ***CWAT 管理者（サイト管理認証アカウント所持者）***
- ***サイト管理者（サイトログオン認証アカウント所持者）***

FMT_SMR.1.2a TSF は、利用者を役割に関連付けなければならない。

FPT_FLS.1 セキュアな状態を保持する障害

下位階層: なし

依存性: ADV_SPM.1 非形式的 TOE セキュリティ方針モデル

FPT_FLS..1.1 TSF は、以下の種別の障害が生じたときはセキュアな状態を保持しなくてはならない: [割付: *TSF における障害の種別のリスト*]。

[割付: *TSF における障害の種別のリスト*]：

- ***DC がネットワークから切断状態になることによって警告ログが OMI に送信できなくなる障害***

FPT_RVM.1 TSP の非バイパス性

下位階層： なし

依存性： なし

FPT_RVM.1.1 TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。

FPT_SEP.1 TSP ドメイン分離

下位階層： なし

依存性： なし

FPT_SEP.1.1　TSF は、それ自身の実行のため、信頼できないサブジェクトによる干渉や改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

FPT_SEP.1.2　TSF は、TSC 内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

FPT_STM.1 高信頼タイムスタンプ

下位階層：　　なし

依存性：　　なし

FPT_STM.1.1 TSF は、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。

5.1.2. 最小機能強度

TOE の最小機能強度レベルは、SOF-基本である。確率的・順列的メカニズムを利用する TOE セキュリティ機能要件は、FIA_UAU.2a、FIA_UAU.2b、FIA_UAU.2c、FIA_SOS.1、FIA_AFL.1 であるが、明示的なセキュリティ機能強度主張は行なわない。

5.1.3. TOE セキュリティ保証要件

TOE の評価保証レベルは EAL2 適合である。以下に EAL2 に含まれる保証コンポーネントを示す。TOE は CC パート 3 で規定されるこれらの保証コンポーネントをそのまま適用する。

表 5.1-2 TOE セキュリティ保証要件

保証クラス	保証ファミリ	保証コンポーネント
構成管理	CM 能力	ACM_CAP.2
配付と運用	配付	ADO_DEL.1
	設置、生成及び立上げ	ADO_IGS.1
開発	機能仕様	ADV_FSP.1
	上位レベル設計	ADV_HLD1
	表現対応	ADV_RCR.1
ガイダンス文書	管理者ガイダンス	AGD_ADM.1
	利用者ガイダンス	AGD_USR.1
テスト	カバレージ	ATE_COV.1
	機能テスト	ATE_FUN.1
	独立テスト	ATE_IND.2
脆弱性評定	TOE セキュリティ機能強度	AVA_SOF.1
	脆弱性分析	AVA_VLA.1

5.2. IT 環境のセキュリティ要件

FIA_UAU.2d[E] アクション前の利用者認証

下位階層： FIA_UAU.1

依存性： FIA_UID.1

FIA_UAU.2.1d[E] TSF（OS）は、その利用者を代行する他のTSF調停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_UAU.2e[E] アクション前の利用者認証

下位階層： FIA_UAU.1

依存性： FIA_UID.1

FIA_UAU.2.1e[E] TSF（DBMS）は、その利用者を代行する他のTSF調停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_UID.2e[E] アクション前の利用者識別

下位階層： FIA_UID.1

依存性： なし

FIA_UID.2.1e[E] TSF（OS）は、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

FIA_UID.2f[E] アクション前の利用者識別

下位階層： FIA_UID.1

依存性： なし

FIA_UID.2.1f[E] TSF（DBMS）は、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

FMT_SMR.1b[E] セキュリティ役割

下位階層: なし

依存性: FIA_UID.1 識別のタイミング

FMT_SMR.1.1b[E] TSF（OS）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*]：

- ***Administrator***

FMT_SMR.1.2b[E] TSF（OS）は、利用者(特定の管理者のみ)を役割（Administrator）に関連づけなければならない。

FMT_SMR.1c[E] セキュリティ役割

下位階層: なし

依存性: FIA_UID.1 識別のタイミング

FMT_SMR.1.1c[E] TSF（OS）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*]：

- ***管理者***

FMT_SMR.1.2c[E] TSF（OS）は、利用者を役割に関連づけなければならない。

FPT_RCV.2[E] **自動回復**

下位階層： FPT_RCV.1

依存性： AGD_ADM.1 管理者ガイダンス

ADV_SPM.1 非形式的 TOE セキュリティ方針モデル

FPT_RCV.2.1[E] [割付: 障害/サービス中断のリスト]からの自動回復が不可能な場合、TSF（OS）はセキュアな状態に戻す能力が提供されるメンテナンスモードに移らなければならない。

[*割付: 障害/サービス中断のリスト*]：

- ***OPDC のサービス停止***

FPT_RCV.2.2[E] [割付: 障害/サービス中断のリスト]に対し、TSF（OS）は、自動化された手順によるTOEのセキュアな状態への復帰を保証しなければならない。

[*割付: 障害/サービス中断のリスト*]：

- ***OPDC のサービス停止***

6. TOE 要約仕様

6.1. TOE セキュリティ機能

TOE のセキュリティ機能の一覧を表 6.1-1 に示す。

TOE のセキュリティ機能とセキュリティ機能要件との対応関係を 8.3.1 の表に示す。

表 6.1-1 TOE のセキュリティ機能名称と識別子の一覧

No	TOE のセキュリティ機能名称	識別子
1	管理者登録機能	－
	OM 認証アカウントの登録機能	SF.OM_REGIST
	サイト管理認証アカウントの登録機能	SF.CWAT-ADM_REGIST
2	管理者識別認証機能	－
	OM 認証	SF.OM_I&A
	サイト管理認証	SF.CWAT-ADM_I&A
	サイトログオン認証	SF.SITE-ADM_I&A
3	OPDC 端末ログオン可能ユーザ識別機能	SF.OPDCLOGON_USER_ID
4	アクセス制御機能	－
	サイトの統計データへのアクセス制御	SF.SITES-INFO_ACCESS
	サイトの管理データへのアクセス制御	SF.SITES-DATA_ACCESS
	サイトの詳細データへのアクセス制御	SF.SITE-DETAIL_ACCESS
5	ポリシー配信強化機能	SF.POLICY_DEL
	自動配信機能	
	強制配信機能	
6	警告ログ送信強化機能	SF.WARNING_LOG_SEND
	異なる方式を併用した警告ログ送信機能	
	モバイル状態の警告ログ送信機能	
7	セキュリティ管理機能	－
	CWAT 管理者によるセキュリティ管理機能	SF.CWAT-ADM
	サイトの登録・更新・削除機能	
	サイトログオン認証アカウントの登録機能	
	サイト管理者によるセキュリティ管理機能	SF.SITE-ADM
	監視対象サイトのノード属性の設定機能	
	ノードにログオン可能なユーザの設定	
	ポリシー情報のバージョンの問合せ	
	ポリシー配信、警告ログ送信に関するのふるまい管理	
8	監査機能	SF.AUDIT

6.1.1. 管理者登録機能

次にあげる管理者登録機能により、OM 認証アカウント、サイト管理認証アカウントを登録することができる。

注釈）ここに示す管理者登録機能は、制限された管理者（通常の運用ではシステム管理者を意図している）が FIA_UAU.2d[E]を具備する OS に対し適切にログインした後に、OE-N.INSTALL に基づき実行可能とする。

6.1.1.1. OM 認証アカウントの登録機能(SF.OM_REGIST)

- OM 認証アカウントファイルを引数として OMI のコマンド（cwlogon_writer.exe）を実行することにより、OM 認証アカウントを**登録**することができる。
- OM 認証アカウントは、ID とパスワードを属性としてもつ。OM 認証アカウントファイルには、ID とパスワードが記入される。パスワードの桁数は 8 文字以上 32 文字以下である必要があり、パスワードに使用可能な文字種は半角英小文字、半角数字、合計 36 文字種である。
- OM 認証アカウントファイルを更新して OMI のコマンド（cwlogon_writer.exe）を実行することにより、OM 認証アカウントを**上書き登録**することができる。
- OM 認証アカウントファイルの特定のアカウントの ID、パスワードの行を削除して保存し、OMI のコマンド（cwlogon_writer.exe）を実行することにより、該当する OM 認証アカウントを**削除**することができる。

6.1.1.2. サイト管理認証アカウントの登録機能(SF.CWAT-ADM_REGIST)

- サイト管理認証アカウントファイルを引数として OMI のコマンド（cwlogon_writer.exe）を実行することにより、サイト管理認証アカウントを**登録**することができる。
- サイト管理認証アカウントは、ID とパスワードを属性としてもつ。サイト管理認証アカウントファイルには、ID とパスワードが記入される。パスワードの桁数は 8 文字以上 32 文字以下である必要があり、パスワードに使用可能な文字種は半角英小文字、半角数字、合計 36 文字種である。
- サイト管理認証アカウントファイルを更新して OMI のコマンド（cwlogon_writer.exe）を実行することにより、サイト管理認証アカウントを**上書き登録**することができる。
- サイト管理認証アカウントファイルの特定のアカウントの ID、パスワードの行を削除し

て保存し、OMI のコマンド（cwlogon_writer.exe）を実行することにより、該当するサイト管理認証アカウントを**削除**することができる。

6.1.2. 識別認証機能

TOE の各管理者がそれぞれが使用する管理画面にログインしようとするときに、登録してある管理者であることを識別し、許可された主体であることを認証する機能である。

6.1.2.1. OM 認証機能（SF.OM_I&A）

本機能は、OM 認証アカウント所持者がサイトモニタ画面にログオンしようとするときに、登録してある管理者であることを識別し、OM 認証アカウントを所有する許可された主体であることを認証するものである。なお、CWAT 管理者、及びサイト管理者は OM 認証アカウント所持者である必要がある。

- 入力された ID を登録されているものと比較することにより識別する。
- 入力されたパスワードを登録されているものと比較することにより認証する。
- パスワードを入力する際、入力したパスワードの代わりにダミー文字“*”を表示する。
- 認証実行時において、一つの ID につき 3 回の認証失敗を検知すると 10 秒間操作不能とし、エラー回数が上限を超えた旨のエラーメッセージのポップアップ画面を表示する。
- OK ボタン押下により認証画面が終了し、再度、認証画面を立ち上げることにより、ID とパスワードが入力可能な状態になる。

なお、本機能は OM 認証アカウント所持者としての操作を利用者に許可する前に、迂回されず必ず実施される。

6.1.2.2. サイト管理認証機能（SF.CWAT-ADM_I&A）

本機能は、CWAT 管理者が、OM 認証によりサイトモニタ画面にログオンしたのちに、個別サイト詳細画面にログオンするときに、登録してある CWAT 管理者であることを識別し、本人であることを認証するものである。

- 入力された ID を登録されているものと比較することにより識別する。
- 入力されたパスワードを登録されているものと比較することにより認証する。
- パスワードを入力する際、入力したパスワードの代わりにダミー文字“*”を表示する。
- 認証実行時において、一つの ID につき 3 回の認証失敗を検知すると 10 秒間操作不能とし、エラー回数が上限を超えた旨のエラーメッセージのポップアップ画面を表示する。
- OK ボタン押下により認証画面が終了し、再度、認証画面を立ち上げることにより、ID

とパスワードが入力可能な状態になる。
なお、本機能は CWAT 管理者としての操作を利用者に許可する前に、迂回されず必ず実施される。

6.1.2.3. サイトログオン認証機能（SF.SITE-ADM_I&A）

本機能は、次の場合に登録してあるサイト管理者であることを識別し、本人であることを認証するものである。

(1) サイト管理者が、OM 認証によりサイトモニタ画面にログオンしたのちに、サイトの OM モニタ画面にログオンするとき
(2) サイト管理者が、DC 環境設定ファイル管理マネージャ画面から配信インターバル、警告再送最大件数を更新するとき

※ (1)ではサイトログオン認証画面が表示され、(2)ではサイト認証画面が表示されるが、いずれの画面も、入力する ID とパスワードはサイトログオン認証アカウント ID、およびパスワードである。

- 入力された ID を登録されているものと比較することにより識別する。
- 入力されたパスワードを登録されているものと比較することにより認証する。
- パスワードを入力する際、入力したパスワードの代わりにダミー文字“*”を表示する。
- 認証実行時において、一つの ID につき 3 回の認証失敗を検知すると 10 秒間操作不能とし、エラー回数が上限を超えた旨のエラーメッセージのポップアップ画面を表示する。
- OK ボタン押下により認証画面が終了し、再度、認証画面を立ち上げることにより、ID とパスワードが入力可能な状態になる。

なお、本機能はサイト管理者としての操作を利用者に許可する前に、迂回されず必ず実施される。

6.1.3. OPDC 端末ログオン可能ユーザ識別機能（SF.OPDCLOGON_USER_ID）

OPDC は、当該端末にログオン可能ユーザが設定されている場合、OPDC 端末の OS にログオンしようとするユーザのアカウント ID がログオン可能ユーザリストに存在しなければそのアカウント ID によるログオンを拒否する機能である。

6.1.4. アクセス制御機能

DB で管理するデータへのアクセス操作をデータの種別やサイト ID に応じて、次に示す認証成功プロセスにのみ制限する機能である。

すべてのサイトの統計情報：OM 認証プロセス
すべてのサイトの管理情報：サイト管理認証プロセス
サイトの詳細情報　　：そのサイトのサイトログオン認証プロセス

6.1.4.1. サイトの統計情報へのアクセス制御（SF.SITES-INFO_ACCESS）

OM 認証プロセス（OM 認証に成功した状態のプロセス）からしかサイトモニタ（サイトの統計情報の表示画面）を表示できないように制限する。これにより、データの種別がサイトの統計情報である全サイトのデータの**参照**を OM 認証に成功した OM 認証アカウント所持者に制限する機能である。サイトの統計情報とは、サイトで発生した警告等に関する統計的情報からなる DB オブジェクトであり、生成時に、サイトの統計情報であることを識別可能とする値が DB オブジェクト種別に付与される。

- サイト ID
- サイト名称
- 端末数
- 最終発生警告時刻
- 警告レベル（High／Middle／Low）
- 電源 ON／電源 OFF
- Logon
- 警告件数
- 警告対応件数（未対応／確認中／対応済／対応無）

6.1.4.2. サイトの管理情報へのアクセス制御（SF. SITES-DATA_ACCESS）

サイト管理認証プロセス（サイト管理認証に成功した状態のプロセス）からしか個別サイト詳細画面（サイトの管理情報の操作画面）を表示できないように制限する。これにより、データの種別がサイトの管理情報である全サイトのデータへのアクセス（登録、更新、削除、参照）をサイト管理認証に成功した CWAT 管理者のみに制限する機能である。サイトの管理情報とは、サイトを管理するための次の情報からなる DB オブジェクトであり、生成時に、サイトの管理情報であることを識別可能とする値が DB オブジェクト種別として付与される。

- サイト ID
- サイト名称
- 場所
- 担当者
- 電話番号

- 担当部署
- メールアドレス
- 言語初期設定
- サイトログオンユーザ設定情報

6.1.4.3. サイトの詳細情報へのアクセス制御（SF. SITE-DETAIL_ACCESS）

サイトログオン認証プロセス（サイトログオン認証に成功した状態のプロセス、サイト ID を保持）からしか同じサイト ID の OM モニタ（サイトの詳細情報の操作画面）を表示できないように制限する。これにより、データの種別がサイトの詳細情報である当該サイトのデータへのアクセスを、当該サイトのサイトログオン認証に成功したサイト管理者のみに制限する機能である。サイトの詳細情報とは、ポリシー情報、配信用ポリシー情報ファイル、及び警告ログの DB オブジェクトであり、制御されるアクセス操作は次の通りである。

・ ポリシー情報の DB オブジェクトに対して制御されるアクセス操作は、登録、参照、削除、更新、更新の反映である。
・ 配信用ポリシー情報ファイルに対して制御されるアクセス操作は、通常配信、および強制配信である。通常配信とは、当該サイトの反映用フォルダに格納された更新反映済みのポリシー情報ファイルを当該サイトの配信用フォルダに格納することである。強制配信機能が持つセキュリティ機能性については、6.1.5.2 に説明する。
・ 警告ログの DB オブジェクトに対して制御されるアクセス操作は、参照、出力である。

以下、サイトの詳細情報（ポリシー情報、配信用ポリシー情報、警告ログ）と本アクセス制御との関係について説明する。

（1） ポリシー情報（DB オブジェクト）

DB オブジェクトであるポリシー情報は、以下の①～③のセットからなる。各 DB オブジェクトの属性であるサイト ID には、当該ポリシー情報の登録もしくは更新の反映を実行するサイトログオン認証プロセスのサイト ID に相当する値が付与される。また、当該ポリシー情報がサイトの詳細情報であることを識別可能とする値が DB オブジェクト種別として付与される。これらは、DB オブジェクトを検索するための属性として別途 DB 内に格納される。

① ノード属性

ノード属性とは、次に示すように、監視対象となるノード（端末）に関する情報である。ポリシーの設定において、例えば、適用するノードを選択するときに使用される。また未登録端末ポリシー適用時には、このノード情報に登録されてい

ない MAC アドレスをもつ端末が接続されたときを未登録端末が接続されたと判断する等、ポリシーの設定において必要となる情報である。

- サイト ID
- ノードの物理的構成（ツリー構造データ）
- 有効期間（From、To）
- エリア情報（場所）
- ノード ID
- IP アドレス
- MAC アドレス
- ノード名称
- ホスト名
- ノードグループ（なし／クライアント／サーバ／プリンタ）
- ノード分類（モバイル／デスクトップ）
- 所有部署
- 言語（日本語、英語、韓国語、中国語（繁体）、中国語（簡体））
- ログオン可能ユーザ（ログオン可能ユーザの設定 ON/OFF、ログオンユーザ名）
- 上位 NM の IP アドレス
- ポリシー情報のバージョン（ノード属性バージョン、ユーザ属性バージョン、ポリシーバージョン）
- コンフィグ先行配信 ON/OFF

② ユーザ属性

ユーザ属性とは、次に示すように監視対象となるユーザの情報である。ポリシーの設定において、例えば、適用するユーザを選択するときに使用される。また、ノードにログオン可能なユーザを制限する場合なども本情報は利用される。

- サイト ID
- ユーザの論理的構成（ツリー構造データ）
- 有効期間（From、To）
- 所属部署
- ログオンユーザ名
- ドメイン名・ホスト名
- ユーザ名（氏名）
- ユーザ ID（社員番号）
- ユーザ区分（なし／正社員／アルバイト／外注作業員）

- 職種（なし／一般／管理職／システム管理）
- 盗難端末オプション監視外ユーザとして登録 ON/OFF

③　ポリシー

サイト管理者はサイト内に適用する次の各ポリシーを設定することにより、PC 端末の利用操作、ネットワークアクセス操作を監視することができる。

- サイト ID
- ユーザログオンポリシー
- 端末使用ポリシー
- 未登録・盗難端末ポリシー
- ネットワークポリシー
- 外部接続機器ポリシー
- ユーザオペレーションポリシー
- メッセンジャーポリシー

（2）　配信用ポリシー情報（ファイル）

配信用ポリシー情報ファイルは、（1）の①～③のそれぞれの DB オブジェクトの情報を、配信用のファイルに格納したものである。サイト管理者は、ポリシー情報の登録、更新、削除機能により最新のポリシー情報を DB オブジェクトに格納後、更新の反映機能により配信用ポリシー情報ファイルを、サイトログオン認証時に引き渡されるサイト ID にて特定されるフォルダ内にバージョン情報とともに生成する。配信用ポリシー情報ファイルは、ファイル種別によりその配信用ポリシー情報ファイルの種類を識別し、バージョンによりその種別内において一意にファイルを識別する。

（3）　警告ログ（DB オブジェクト）

OMI プロセスが受け付けた警告ログを、警告ログの単位で DB オブジェクトとして格納したものである。

- オペレーション系警告ログ
- ネットワーク系警告ログ

警告ログの参照とは、上記の各警告ログの DB オブジェクトの内容を画面上で参照することである。また、警告ログの出力とは、同じく警告ログの DB オブジェクトの内容をファイルに出力することである。

6.1.5.　ポリシー配信強化機能（SF.POLICY_DEL）

サイト管理者が管理するサイトに対して、最新バージョンの配信用ポリシー情報ファイ

ルをサイト内のノードに適用するための機能である。配信用ポリシー情報ファイルとは、サイト ID で特定できるフォルダ及びその中に格納された複数ファイル全体を示す。配信用ポリシー情報ファイルには、生成時に、一意に識別可能なバージョン、およびファイル種別（ノード属性、ユーザ属性、ポリシーを一意に識別可能な値）が付与される。配信時には、指定されたサイト ID と配信用ポリシー情報ファイルのバージョン、および、ファイル種別の属性値から、配信すべき配信用ポリシー情報ファイルの部分を特定することができる。

6.1.5.1. 自動配信機能

- DC プロセスが自身が保持する上位 NM の IP アドレスに対して、設定された**配信インターバル**（デフォルト 60 分）で、上位 NM との間に通信コネクションポートを生成し、DC プロセスのサイト ID に対応するポリシー情報(上位 NM が配信用ポリシー情報として保持)の各バージョンを問い合わせる。受信した上位 NM は、DC プロセスに回答を送付する。
- 回答を受信した DC プロセスは、自身が保持するポリシー情報のバージョンと比較して、上位 NM で保持しているバージョンの方が大きい、もしくはファイルが存在しない場合、上位 NM に指定したサイト ID 及びバージョンの配信用ポリシー情報の送信要求を行う。
- 送信要求を受信した上位 NM は要求に従い、要求元の DC プロセスに配信用ポリシー情報を送信する。

6.1.5.2. 強制配信機能

- サイトログオン認証に成功したサイト管理者は、サイトの DC のポリシー情報の適用状況をノード属性マネージャ画面または CWAT 管理コンソール画面で DC における配信済みの配信用ポリシー情報のバージョンを表示させることにより確認することができる。
- サイトログオン認証に成功したサイト管理者は、サイトの DC に対して最新の配信用ポリシー情報を適用するために、指定した DC に配信用ポリシー情報の強制配信を行うことができる。

6.1.6. 警告ログ送信強化機能（SF.WARNING_LOG_SEND）

DC で発生した警告ログを DC がネットワーク接続状態である場合も、ネットワーク非接続状態にある場合も、OMI に確実に送信するための機能である。警告ログには、その警告ログが発生した DC プロセスのサイト ID に相当するサイト ID が付与される。

6.1.6.1. 異なる方式を併用した警告ログ送信機能

DC がネットワーク接続状態にある場合、発生した警告ログを異なる方式のプロトコルにより OMI へ繰り返し送信する。OMI においては、CWAT3i の正しい警告ログと判断して受け付ける。

- DC でポリシーに基づいて検知された不正操作の警告イベントが発生すると、DC で保持する OMI の IP アドレスに向けて警告ログを即時性の高いプロトコル（UDP）で送信する。
- OMI は警告ログに含まれるサイト ID を検査し、自身が保持するサイト ID リストに基づき、そのサイトの警告として受け付け、OM モニタ及びサイトモニタに反映・表示する。
- 警告ログを警告ログテンポラリファイルで DC 内部に蓄積し、**配信インターバル**で設定された時間間隔でファイルから再送する警告ログを読み込んで、信頼性の高いプロトコル（TCP）による再送処理を実施する。ファイルには、設定された**警告再送最大件数**まで警告ログを蓄積可能とする。TCP での再送に成功した警告ログは警告ログテンポラリファイルから削除する。
- OMI 側では UDP で受領済みの警告ログかどうかを確認し、未受領であれば TCP で送信された警告ログを受付け、受領済であれば TCP で送信された警告ログを破棄する。

6.1.6.2. モバイル状態の警告ログ送信機能

警告ログ送信における＜セキュアな状態＞を次のように定義する。

“警告ログ送信強化機能が適切に動作し、DC で発生した警告イベントが OMI に確実に送信される状態”

これにより、TSP（警告ログの送信失敗や未送信の事象に備え警告ログを所定のタイミングで再送信する）の正しい実施が継続される。

DC がネットワークに接続されている状態は、6.1.6.1 で示したセキュリティ機能により＜セキュアな状態＞であるが、DC がネットワークから切断されている状態においても＜セキュアな状態＞を保持するためには、以下の機能が必要である。

- PC 端末がモバイル状態となっているなど、ネットワーク切断時に生成した警告ログは、ネットワーク再接続時に OMI へ再送する（但し、PC 端末が電源 ON の状態でネットワークから切断し、再接続した場合は、次回の配信インターバル時に警告再送する）。ネットワーク再接続されたイベントを検知すると、警告ログテンポラリファイルを読み込み、ネットワーク切り離し時（もしくは電源 OFF 時）に記録した時刻情報の時刻後に生成された警告ログのうち、**警告再送最大件数**として設定された件数までの警告

ログを TCP で OMI に送信する。（警告再送最大件数内で）送信しきれない警告ログは再送済み時刻とともに管理し、配信インターバルごとに残りを順次まとめて OMI へ送信する。

6.1.7. セキュリティ管理機能

6.1.7.1. CWAT 管理者によるセキュリティ管理機能（SF.CWAT-ADM）

サイト管理認証に成功した CWAT 管理者のみが、次にあげるセキュリティ管理機能を使用することができる。

6.1.7.1.1. サイトの登録・更新・削除機能

- サイトモニタ画面から監視対象とすべきサイトを**登録**したり、または**削除**することができる。
- サイトは、次に示すサイト属性をもつ。サイトを削除すると、サイト ID をはじめサイト属性のすべてが削除される。
    - サイト ID
    - サイトログオン認証アカウント
- 個別サイト詳細画面からサイト属性を**更新**したり、または**参照**することができる。

6.1.7.1.2. サイトログオン認証アカウントの登録機能

サイト属性の一つであるサイトログオン認証アカウントを登録する機能である。

- サイトログオン認証アカウントを新規に**登録**したり、または**削除**することができる。サイトログオン認証アカウントは複数登録することが可能である。
- サイトログオン認証アカウントは、表 6.1-2　に示すサイトログオン認証アカウント属性をもつ。サイトログオン認証アカウントを**削除**すると、サイトログオン認証アカウント属性のすべてが削除される。
- 個別サイト詳細画面から、表 6.1-2　で設定可能となっているサイトログオン認証アカウント属性を**設定**することができる。
- 設定後にサイトログオン認証アカウント属性を**更新**することはできない。**更新**する場合は、一度、サイトログオン認証アカウントを削除して、もう一度、サイトログオン認証アカウント属性を設定する。
- 個別サイト詳細画面から、表 6.1-2　で参照可能となっているサイトログオン認証アカウント属性を**参照**することができる。

表 6.1-2　サイトログオン認証アカウント属性

属性	内容	設定可否	更新可否	参照可否
サイトログオン認証アカウント ID	サイトへログオンするユーザの ID	可	不可	可
パスワード	サイトへログオンする際のパスワード 桁数は 8 文字以上 32 文字以下を満たすこと。使用可能な文字種は半角英小文字、半角数字、合計 36 文字種であること。	可	不可	不可

6.1.7.2. サイト管理者によるセキュリティ管理機能（SF.SITE-ADM）

サイトログオン認証に成功したサイト管理者のみが、次にあげるセキュリティ管理機能を使用することができる。

6.1.7.2.1. 監視対象サイトのノード属性の設定機能

- サイトのノードに対するログオン可能ユーザを設定することができる。
- サイトのノード属性（ポリシー情報のバージョン）を参照することができる。

表 6.1-3　ノード属性

ノード属性		設定可否	更新可否	参照可否
ノードにログオン可能なユーザ名	ログオン可能ユーザの設定 ON/OFF	可	可	可
	ON の場合）ログオンユーザ名	可	可	可
ポリシー情報のバージョン	ポリシーファイル（ポリシーバージョン）	不可	不可	可
	ノード属性ファイル(ノード属性バージョン)	不可	不可	可
	ユーザ属性ファイル(ユーザ属性バージョン)	不可	不可	可

※ ログオンユーザ名とは、ノードにログオン可能ユーザを指定した場合のログオン可能ユーザのアカウント ID である。

6.1.7.2.2. ポリシー配信、警告ログ送信に関するふるまいの管理

ポリシーの配信のふるまいを決めるパラメータ（表 6.1-4）、警告ログ送信のふるまいを決めるパラメータ（表 6.1-5）を DC 環境設定ファイル管理マネージャ画面、及び各ポリシー画面で設定することができる。DC 環境設定ファイル管理マネージャ画面によって、配信インターバル、警告再送最大件数を更新するには、更新時に表示されるサイト認証画面にてサイトログオン認証アカウント ID およびパスワードを入力し、当該サイトの正当なサイト管理者であることを認証される必要がある。

表 6.1-4　ポリシー情報配信のふるまいを決めるパラメータ

属性	デフォルト値	更新可否	参照可否
配信インターバル	60 分	可	可

表 6.1-5　警告ログ送信のふるまいを決めるパラメータ

属性		デフォルト値	更新可否	参照可否
配信インターバル		60 分	可	可
警告再送最大件数		1,250,000 件	可	可
ポリシー違反時のアクション	警告発信 ON/OFF	OFF	可	可
	監査ログ出力 ON/OFF	OFF	可	可

※配信インターバルは、ポリシー配信、警告ログ送信に対して共通に適用されるパラメータである。

6.1.8. 監査機能（SF.AUDIT）

監査機能とは、TOE の管理者の識別認証、および管理画面へのアクセスに関わる監査記録を生成する機能である。OMI 上での TOE の管理者の操作を操作ログとして記録し、DBMS が管理するデータベースに保存する。操作ログに記録される内容を表 6.1-6 に示す。

表 6.1-6　OMI サーバ上での管理者の操作ログ

属性	生成可否	参照可否
オペレーション日時	可	可
サイト ID	可	可
ログオン ID	可	可

ユーザ種別	可	可
IP アドレス	可	可
ウインドウタイトル	可	可
イベント（OM で操作した事項）	可	可

上記の操作ログは、以下の事象を含む画面操作に適用される。

- OM 認証の記録
- サイト管理認証の記録
- サイトログオン認証の記録
- CWAT 管理者の操作の記録
- サイト管理者の操作の記録
- OM 認証アカウント所持者の操作の記録

OMI が受付け、サイト管理者によりモニタリングが可能な警告ログは、それ自体が警告ログ受付の監査ログとなる。
また、OMI のコマンド（cwlogon_writer.exe）による管理者アカウント登録機能の使用に対しては、個別のログを生成する。

6.2. TOE セキュリティ機能強度

確率的・順列的メカニズムを有する TOE セキュリティ機能は、以下の通りであり、機能強度はそれぞれ SOF-基本を満たす。

①SF.OM_I&Aが提供するOM認証パスワードの認証メカニズム
②SF.CWAT-ADM_I&Aが提供するサイト管理認証パスワードの認証メカニズム
③SF.SITE-ADM_I&Aが提供するサイトログオン認証パスワードの認証メカニズム

6.3. 保証手段

EAL2 の TOE セキュリティ保証要件のコンポーネントを満たす保証手段を表 6.3-1 に示す。

表 6.3-1 TOE 保証要件と保証手段の関係

TOE セキュリティ保証要件	コンポーネント	保証手段
構成要素	ACM_CAP.2	CWAT3i(Ver3.1b_CC)構成管理証拠資料(ACM_CAP.2) CWAT3i(Ver3.1b_CC)構成リスト(ACM_CAP.2)
配付手続き	ADO_DEL.1	CWAT3i(Ver3.1b_CC)配付証拠資料(ADO_DEL.1)
設置、生成、及び立上げ手順	ADO_IGS.1	CWAT インストレーションマニュアル Windows 編 CWAT セキュリティマニュアル CWAT Installation Manual Windows Version 2 CWAT Security Manual
非形式的機能仕様	ADV_FSP.1	CWAT3i(Ver3.1b_CC) セキュリティ機能仕様書 (ADV_FSP.1) CWAT3i(Ver3.1b_CC) セキュリティ機能仕様書別添資料
記述的上位レベル設計	ADV_HLD.1	CWAT3i(Ver3.1b_CC) 上位レベル設計書 (ADV_HLD.1)
非形式的対応の実証	ADV_RCR.1	CWAT3i(Ver3.1b_CC) 表現対応分析書 (ADV_RCR.1)
管理者ガイダンス 利用者ガイダンス	AGD_ADM.1 AGD_USR.1	CWAT セキュリティマニュアル CWAT アドミニストレーションマニュアル Part1 監視編 CWAT アドミニストレーションマニュアル Part2 ユーザ・ノード管理編 CWAT アドミニストレーションマニュアル Part3 ポリシー管理編 CWAT アドミニストレーションマニュアル Part4 警告・監査情報管理編 CWAT アドミニストレーションマニュアル Part5 CWAT 管理コンソール編 CWAT アドミニストレーションマニュアル Part6 アドミニストレーション管理編 CWAT アドミニストレーションマニュアル Part7 TOOL 編 CWAT アドミニストレーションマニュアル Part8 暗号編 CWAT アドミニストレーションマニュアル Part9 盗難端末オプション編 CWAT アドミニストレーションマニュアル Part10 印刷オプション編 CWAT アドミニストレーションマニュアル Part11 CPS 編

TOE セキュリティ保証要件	コンポーネント	保証手段
		CWAT Security Manual CWAT Administration Manual Part1 Monitoring CWAT Administration Manual Part2 Node and User Management CWAT Administration Manual Part3 Policy Management CWAT Administration Manual Part4 Alert and Audit Log Search CWAT Administration Manual Part5 CWAT Manger CWAT Administration Manual Part6 Administration CWAT Administration Manual Part7 Administrative Tools CWAT Administration Manual Part8 Encryption Function CWAT Administration Manual Part9 Anti-Theft Option CWAT Administration Manual Part10 Print Option CWAT Administration Manual Part11 CWAT Plat Server
カバレージの証拠	ATE_COV.1	CWAT3i(Ver3.1b_CC) テストカバレージ証拠(ATE_COV.1) CWAT3i(Ver3.1b_CC) テストカバレージ詳細資料
機能テスト	ATE_FUN.1	CWAT3i(Ver3.1b_CC) テスト証拠(ATE_FUN.1) CWAT3i(Ver3.1b_CC) テスト詳細資料 CWAT3i(Ver3.1b_CC) テスト結果証拠資料 CWAT3i(Ver3.1b_CC) テストユーザ・ノード一覧 テストポリシー一覧
独立試験・サンプル	ATE_IND.2	（TOE テスト）環境一式 ((TOE テスト）環境の利用方法を含む補足資料)
TOE セキュリティ機能強度評価	AVA_SOF.1	CWAT3i(Ver3.1b_CC) 機能強度分析書 (ADV_SOF.1)
開発者脆弱性分析	AVA_VLA.1	CWAT3i(Ver3.1b_CC) 脆弱性分析書 (AVA_VLA.1)

7. PP 主張

この章では、PP 主張について記述する。

7.1. PP 参照

参照した PP はない。

7.2. PP 修整

修整した PP はない。

7.3. PP 追加

PP への追加はない。

8. 根拠

8.1. セキュリティ対策方針根拠

8.1.1. セキュリティ対策方針の必要性に関する根拠

下表で示すとおり、識別したセキュリティ対策方針は、少なくとも１つ以上の識別した前提条件、脅威及び/または組織のセキュリティ方針に対応している。

前提・脅威 / セキュリティ対策方針	A.ADMIN	A.CWAT_ADMIN	A.SITE_ADMIN	A.INSTALL	A.PC_USER_ROLE	A.PASSWORD_MANAGEMENT	A.PHYSICAL_PROTECTION	A.NETWORK_RELIABILITY	T.EVIL_POLICY_VIA_SERVER	T.EVIL_POLICY_VIA_OPDC	T.FAIL_SEND_POLICY	T.LOSS_WARNING_LOG	T.STOP_OPDC_INTENTIONALLY	P.AUDIT	P.SITE_POLICY
O.I&A									●						●
O.LIMIT_LOGON_USER										●					
O.ACCESS_CONTROL									●						●
O.ENHANCED_DELIVERING											●				
O.ENHANCED_WL_SENDING												●			
O.MANAGE									●	●	●	●			●
O.AUDIT														●	
OE.OS_DB				●	●	●			●	●			●		
OE-N.ADMIN	●														
OE-N.CWAT_ADMIN		●													
OE-N.SITE_ADMIN			●												
OE-N.INSTALL				●											
OE-N.PC_USER_ROLE					●					●					
OE-N.PASSWORD_MANAGEMENT						●									
OE-N.PHYSICAL_PROTECTION							●								
OE-N.NETWORK_RELIABILITY								●							
OE-N.RECOVER													●		

8.1.2. セキュリティ対策方針の十分性に関する根拠

以下に示すとおり、これらのセキュリティ対策方針は、識別した前提条件及び組織のセキュリティ方針を満たし、また、識別した脅威に対抗するために十分効果があることがわかる。

- A.ADMIN（システム管理者の信頼性）
  OE-N.ADMIN は、TOE のシステム管理者として求められる職務の遂行において信頼できる人物を選任するため、システム管理者の信頼性は満たされる。

- A.CWAT_ADMIN（CWAT 管理者の信頼性）
  OE-N.CWAT_ADMIN は、CWAT 管理者として求められる役割を適切に遂行する者を割り当て、サイト管理認証アカウントを利用させるため、CWAT 管理者の信頼性は満たされる。

- A.SITE_ADMIN（サイト管理者の信頼性）
  OE-N.SITE_ADMIN は、サイト管理者として与えられた役割を適切に遂行するものを割り当て、TOE に脅威を与えない運用方法を理解させ、サイトログオン認証アカウントを利用させるため、サイト管理者の信頼性は満たされる。

- A.INSTALL（インストールの信頼性）
  OE-N.INSTALL は、各専用サーバへの TOE のインストール設定・アンインストール、各 PC 端末への OPDC のインストール設定・アンインストールを、システム管理者の責任で適切に実施する。**OE.OS_DB** は、各専用サーバや OPDC をインストールする PC 端末の OS の識別認証機能を提供し、システム管理者のインストール設定・アンインストールをセキュアに行なうための管理者アカウントへの保護を可能とする。これらにより、不適切な方法での TOE のインストールやアンインストールは行なわれず、インストールされた TOE の信頼性は満たされる。

- A.PC_USER_ROLE（PC 端末利用者の権限）
  OE-N.PC_USER_ROLE は、OPDC が動作する PC 端末を管理者以外の端末利用者に利用させるときには、OS である Windows 上にシステム管理者が設定した Users 権限グループのみに属するアカウントを使用させる。また、各 PC 端末の Users 権限グループ以外のアカウントはシステム管理者のみが利用可能となるように設定する。OMI クライアントが動作する PC 端末に対しては、システム管理者の OS アカウント以外に、TOE の管理者としてその端末の利用が許可される CWAT 管理者もしくはサイト管理者の OS アカウントを設定することで､許可された TOE の管理者の OS へのアクセスを可能とする。**OE.OS_DB** は、この OS への設定を特定の管理者のみに制限することを可能とする。これらにより、不正な者が PC 資源を管理者権限で使用することはなく、適切な権限管理のもとでの運用を実現する。

- A.PASSWORD_MANAGEMENT（パスワード管理）

  OE-N.PASSWORD_MANAGEMENT は、TOE の正当な利用者に対し、TOE にアクセスするためのアカウントのパスワードを、主体以外の他者に知られないように管理させ、推測・解析されにくいパスワードを設定させるとともに、時間経過とともに適正な間隔で変更することを指導することにより、適正なパスワード管理を実現する。**OE.OS_DB** は、識別認証機能を提供することから、これらの資源へアクセスするためのアカウントのパスワードに対しても同等の適正なパスワード管理を実現することにより、TOE の運用時の脅威を限定することが可能となる。

- A.PHYSICAL_PROTECTION（サーバ設置場所の保護）

  OE-N.PHYSICAL_PROTECITON は、その組織で運用するシステムの管理・運用のために許可された者のみが入室可能な物理的に保護された区域に TOE の各専用サーバを設置する。また、専用サーバ上の TOE の操作は、サーバが設置された区域でのみ可能となるように TOE の操作環境を設定することにより、これらの専用サーバ及び TOE の操作を物理的攻撃からの保護を実現する。

- A.NETWORK_RELIABILITY（ネットワークの信頼性）

  OE-N.NETWORK_RELIABILITY は、外部ネットワークと TOE が接続される LAN との間にファイアウォールを設置し、外部ネットワークからの攻撃から防御するため、求められるネットワークの信頼性は確保される。

- T.EVIL_POLICY_VIA_SERVER（サーバ経由の不正なポリシーの設定）

  OE.OS_DB は、TOE の専用サーバの OS の識別認証機能により、サーバ設置場所に入室可能な TOE の不正利用者のサーバ端末へのアクセスを防止する。また、OMI サーバで動作する DBMS の識別認証機能により、DB への不正なアクセスを防止する。

  O.MANAGE は、OM 認証アカウント情報、およびサイト管理認証アカウント情報を、生成・参照可能とする機能を提供する。

  O.I&A 、O.ACCESS_CONTROL は、TOE に対する不正なログオンを OM 認証により防止する。また TOE にログオンした状態にアクセスできたとしても、ポリシー情報の設定や警告ログの監視にはサイトログオン認証を要し、そのアカウント情報はさらにサイト管理認証に成功した場合のみ生成・参照可能とすることで不正なアカウント情報へのアクセスを防止する。これらより、OMI サーバへの不正なログオンに起因するポリシー情報の設定や警告ログの監視を防止する。

- T.EVIL_POLICY_VIA_OPDC（OPDC 端末経由の不正なポリシーの設定）

  OE.OS_DB は、OPDC 端末の OS の識別認証機能により、OPDC 端末へのアクセス可能な OS アカウントを制限する。また、OMI サーバで動作する DBMS の識別認証機能により、OMI クライアントから DB への不正なアクセスを防止する。

  O.MANAGE は、OMI クライアントがインストールされた OPDC 端末において、OM 認証アカウント情報、およびサイト管理認証アカウント情報を、生成・参照可能とする機能を提供する。

  O.LIMIT_LOGON_USER は、OMI クライアントがインストールされた OPDC 端末にログオン可能なユーザを設定することを可能とし、この機能を使用して **OE-N.PC_USER_ROLE** で設定した当該 OPDC 端末の利用が許可された TOE の管理者以外のユーザが当該端末にログオンすることを拒否することにより、OMI クライアントをインストールした OPDC 端末を使用できるユーザを許可者された管理者のみに制限する。これらにより、許可された TOE の管理者でない者が OPDC 端末から TOE を使用せずにポリシー情報へのアクセスを試み、不正なポリシー情報の設定や DC 設定を行うことを防止する。

- T.FAIL_SEND_POLICY（ポリシー配信の失敗）

  O.ENHANCED_DELIVERING は、OMI からポリシー情報の DC への配信に際し、配信失敗や未配信に備え、所定のタイミングで配信を再実行し、パケット破損や一時的なネットワーク障害により一時的にポリシー情報が配信されない場合でも、DC に対してポリシー情報を配信することで、意図した環境下におけるポリシー情報の配信失敗の脅威の低減を図る。

  O.MANAGE は、ポリシー配信強化機能のふるまいを決めるパラメータの設定・更新を当該サイトのサイト管理認証に成功した者のみが可能とする。

- T.LOSS_WRNING_LOG（警告情報の消失）

  O.ENHANCED_WL_SENDING は、DC から OMI への警告ログの送信失敗や、DC がネットワークから切り離されるなど未送信となる場合に備え、所定のタイミングで警告ログの再送信を行い、警告ログが DC から OMI へ届かない脅威の低減を図る。この際、再送信においては複数の送信方法を併用すること、再送信時の送信量を制御することにより、脅威低減効果の実効性を高める。これらの対策により、意図した環境下における警告ログの消失の脅威の低減を図る。なお、TOE は OMI の警告ログを受け取るポートへの過負荷攻撃に対しては対抗しない。

  O.MANAGE は、警告ログ送信強化機能のふるまいを決めるパラメータの設定・更新を当該サイトのサイト管理認証に成功した者のみが可能とする。

- T.STOP_OPDC_INTENTIONALLY（サービスの停止）
  OE.OS_DB は、OPDC サービスの自動回復機能により、OPDC サービス停止状態からの回復を支援する。これらにより、OPDC サービス停止の脅威の低減を図る。
  OE-N.RECOVER は、OPDC サービスが不正停止されたことを TOE が検知するとただちに OPDC サービスを復元するように PC 端末のサービス設定を行なうことにより、OPDC のサービス回復を支援する。

- P.AUDIT（監査生成）
  O.AUDIT は、TOE の管理者の識別認証、及び管理画面のアクセスに関わる監査記録を生成する。これにより、P.AUDIT は満たされる。

- P.SITE_POLICY（サイトのポリシー設定）
  O.I&A 、O.ACCESS_CONTROL は、あるサイトのポリシー情報の設定や警告ログの監視を、そのサイトのサイトログオン認証に成功した者のみに可能とする。
  O.MANAGE は、サイトログオン認証アカウント情報を、サイト管理認証に成功した者のみに生成・参照可能とする。
  これにより、P.SITE_POLICY は満たされる。

8.2. セキュリティ機能要件根拠

8.2.1. セキュリティ機能要件の必要性に関する根拠

下表で示すとおり、識別したセキュリティ機能要件は、少なくとも 1 つ以上の識別した TOE のセキュリティ対策方針、または 1 つ以上の IT 環境のセキュリティ対策方針に対応している。

セキュリティ対策方針 / IT セキュリティ機能要件		O.I&A	O.LIMIT_LOGON_USER	O.ACCESS_CONTROL	O.ENHANCED_DELIVERING	O.ENHANCED_WL_SEND	O.MANAGE	O.AUDIT	OE.OS_DB
FAU	FAU_GEN.1							●	
FDP	FDP_ACC.1a			●					
	FDP_ACF.1a			●					
	FDP_ACC.1b			●	●				
	FDP_ACF.1b			●	●				
	FDP_ACC.1c				●				
	FDP_ACC.1c				●				
	FDP_IFC.1					●			
	FDP_IFF.1					●			
	FDP_ITT.1a				●				
	FDP_ITT.1b					●			
FIA	FIA_AFL.1	●							
	FIA_SOS.1	●							
	FIA_UAU.2a	●							
	FIA_UAU.2b	●							
	FIA_UAU.2c	●							
	FIA_UAU.7	●							
	FIA_UID.2a	●							
	FIA_UID.2b	●							
	FIA_UID.2c	●							
	FIA_UID.2d		●						
FMT	FMT_MOF.1						●		
	FMT_MSA.1a						●		
	FMT_MSA.1b						●		
	FMT_MSA.3a						●		
	FMT_MSA.3b						●		
	FMT_MSA.3c						●		
	FMT_MSA.3d						●		
	FMT_MTD.1a						●		
	FMT_MTD.1b		●				●		
	FMT_MTD.1c						●		
	FMT_SMF.1						●		
	FMT_SMR.1a						●		
FPT	FPT_FLS.1					●			
	FPT_RVM.1	●	●	●				●	
	FPT_SEP.1	●	●	●				●	
	FPT_STM.1							●	
FIA	FIA_UAU.2d[E]								●
	FIA_UAU.2e[E]								●
	FIA_UID.2e[E]								●
	FIA_UID.2f[E]								●
FMT	FMT_SMR.1b[E]								●

セキュリティ対策方針 / IT セキュリティ機能要件		O.I&A	O.LIMIT_LOGON_USER	O.ACCESS_CONTROL	O.ENHANCED_DELIVERING	O.ENHANCED_WL_SEND	O.MANAGE	O.AUDIT	OE.OS_DB
	FMT_SMR.1c[E]								●
FPT	FPT_RCV.2[E]								●

8.2.2. セキュリティ機能要件の十分性に関する根拠

以下に示すとおり、識別されたセキュリティ機能要件は、TOE 及び IT 環境のセキュリティ対策方針を実現するために十分な効果が見込まれる。

- O.I&A（OMI の識別認証）

  本セキュリティ対策方針は、CWAT 管理者及びサイト管理者が OMI を利用するときに、利用する画面に応じて確実に識別・認証することを求めている。

  FIA_UID.2a、**FIA_UAU.2a** により、TOE の OMI を起動しログオンを行なう者が OM 認証アカウントを所有するものであることを識別･認証する。OM 認証アカウントで認証されるとサイトモニタを操作可能となる。

  FIA_UID.2b、**FIA_UAU.2b** は、個別サイト詳細画面からサイト管理情報の参照・更新を行なうものがサイト管理認証アカウントを所有する者であることを識別・認証する。

  FIA_UID.2c、**FIA_UAU.2c** は、OM モニタからポリシー情報の設定や警告ログの監視を行なう者が当該サイトのサイトログオン認証アカウントを所有するものであることを識別・認証する。また、DC 環境設定ファイル管理マネージャ画面から DC 設定情報の更新を行うものが、サイトログオン認証アカウントを所有するものであることを識別認証する。

  FIA_SOS.1 は、これらの認証情報の登録・更新時に認証データの品質を保証する。

  FIA_UAU.7 は、これらの認証機能を操作する際に認証データの画面フィードバック文字を制御する。

  FIA_AFL.1 は、連続する認証失敗時に画面操作を一定時間操作不能とし連続した試行攻撃を緩和する。

  FPT_RVM.1 により、識別・認証機能は画面操作の前に必ず呼び出される。

  FPT_SEP.1 により、識別・認証することで許可のない不正なサブジェクトから許可を必要とする機能を分離し、これらの機能の悪用・改ざんを防ぐ。

  これらの機能要件の組み合わせにより、本セキュリティ対策方針は満たされる。

- O.LIMIT_LOGON_USER（OPDC ログオン可能ユーザの設定）
  本セキュリティ対策方針は、OPDC 端末にログオン可能なユーザを設定すること、また、その場合、それ以外のユーザが当該 OPDC 端末にログオンすることを拒否することを求めている。
  FMT_MTD.1b により、サイト管理者はノードにログオン可能なユーザを登録、変更する。
  FIA_UID.2d により、OPDC 端末にログオン可能として設定されたユーザ以外の者による当該 OPDC 端末へのログオンが拒否される。
  FPT_RVM.1 により、OPDC 端末にログオン可能なユーザが設定されているときは、OPDC 端末へのログオン前にその設定ユーザであることの識別機能が必ず呼び出される。**FPT_SEP.1** により、識別確認することで許可のない不正なサブジェクトから許可を必要とする機能を分離し、これらの機能の悪用・改ざんを防ぐ。
  これらの機能要件の組み合わせにより、本セキュリティ対策方針は満たされる。

- O.ACCESS_CONTROL（アクセス制御）
  本セキュリティ対策方針は、ポリシー情報、警告ログ、及びそれに付随するデータ（サイトの統計情報、サイトの管理情報）へのアクセスを、許可された管理者に制限することを求めている。
  FDP_ACC.1a、**FDP_ACF.1a** は、すべてのサイトの統計情報へのアクセスを、OM 認証に成功した OM 認証アカウント所持者のみに制限する。また、すべてのサイトの管理情報へのアクセスを、サイト管理認証に成功した CWAT 管理者のみに制限する。
  FDP_ACC.1b、**FDP_ACF.1b** は、あるサイトのポリシー情報、配信用ポリシー情報、警告ログへのアクセスをそのサイトのサイトログオン認証に成功したサイト管理者のみに制限する。
  FPT_RVM.1 により、TOE のセキュリティ機能のふるまいの設定、ポリシー情報の設定、警告ログの参照においてアクセス制御を実施する前には、識別認証機能が必ず呼び出される。**FPT_SEP.1** により、識別・認証することで許可の無い不正なサブジェクトから許可を必要とする機能を分離し、これらの機能の悪用、改ざんを防ぐ。
  これらの機能要件の組み合わせにより、本セキュリティ対策方針は満たされる。

- O.ENHANCED_DELIVERING（ポリシー配信強化機能）
  本セキュリティ対策方針は、OMI からポリシー情報を DC に配信する機能を強化し、配信失敗や未配信を検出し、所定のタイミングで最新のバージョンのポリシー情報の配信を再実行することを求めている。
  FDP_ITT.1a、**FDP_ACC.1c**、**FDP_ACF.1c** により、DC はポリシー情報を最新のバー

ジョンの状態で使用できるように、定期的に上位NMに対して、自身が保持する配信用ポリシー情報のバージョンよりも新しいバージョンの配信用ポリシー情報があれば送信要求し、受信する。

FDP_ACC.1b、**FDP_ACF.1b** は、サイトログオン認証に成功したサイト管理者のみに指定したサイトの特定のノードに対して配信用ポリシー情報を強制配信する機能を許可する。

これらの機能要件の組み合わせにより、本セキュリティ対策方針は満たされる。

- O.ENHANCED_WL_SENDING（警告ログの送信強化機能）

  本セキュリティ対策方針は、警告ログを DC から OMI に送信する機能を強化し、送信失敗の検出時や未送信となった事象に備え、所定のタイミング及び異なる方法で、警告ログを再送信することを求めている。

  FDP_ITT.1b、**FDP_IFC.1**、**FDP_IFF.1** により、警告ログを所定のタイミングで異なる方法で再送信する。また、OMI は DC からの警告ログの再送信を検知し、既に受付済みの警告が存在する場合には、再送された警告を破棄する。

  また、**FPT_FLS.1** により、DC がネットワーク非接続状態時の警告ログを蓄積し、ネットワーク接続時にそれらの警告ログを送信する。

  これらの機能要件の組み合わせにより、本セキュリティ対策方針は満たされる。

- O.MANAGE（セキュリティ管理）

  TOE の管理者はその役割に応じて、TOE のセキュリティ機能のふるまいの設定、セキュリティ機能に関係するデータの管理を行わなければならない。

  FMT_MOF.1 により、サイト管理者は、自身が管理するサイトにおいて、ポリシー配信強化機能、警告ログ送信強化機能、OPDC 端末ログオン可能ユーザ識別機能を停止させるデータを管理する。

  FMT_MSA.1a により、CWAT 管理者はすべてのサイトのサイト ID の管理（登録、更新、削除）を行う。

  FMT_MSA.1b により、サイト管理者は自身が管理するサイトの各ノードの配信用ポリシー情報ファイルのバージョンの管理（参照）を行う。

  FMT_MSA.3a により、サイトの統計情報またはサイトの管理情報の DB オブジェクトの生成時に DB オブジェクト種別が付与される。

  FMT_MSA.3b により、サイトの詳細情報の DB オブジェクトの生成時に当該サイトのサイト ID および DB オブジェクト種別が付与される。

  FMT_MSA.3c により、配信用ポリシー情報ファイルの生成時に当該サイトのサイト ID、バージョン、およびファイル種別が付与される。

FMT_MSA.3d により、警告ログの生成時に当該 DC プロセスが属するサイトのサイト ID が警告ログに自動的に付与される。

FMT_MTD.1a により、CWAT 管理者はサイトログオン認証アカウントのアカウント ID、およびパスワードの登録といった管理を行う。

FMT_MTD.1b により、サイト管理者は自身が管理するサイト内において、ノードにログオン可能ユーザの設定可否の管理、（ON の場合）ログオンユーザの登録といった管理を行う。

FMT_MTD.1c 、FMT_SMR.1c[E]により、運用環境で設定された制限された管理者は OM 認証アカウントのアカウント ID、パスワードの登録、およびサイト管理認証アカウントのアカウント ID、パスワードの登録といった管理を行う。

FMT_SMF.1、**FMT_SMR.1a** は、OM 認証アカウント所持者、CWAT 管理者、サイト管理者のそれぞれの役割を規定し、使用を許可するセキュリティ管理機能を特定する。

これらの機能要件の組み合わせにより、本セキュリティ対策方針は満たされる。

- O.AUDIT（監査記録の生成）

  本セキュリティ対策方針は、TOE が、管理者識別認証、及び管理画面のアクセスに関わる監査記録を生成することを求めている。

  FAU_GEN.1 により、TOE は、TOE の各管理者の識別認証機能の成功・失敗の事象に関する監査ログを生成する。また、TOE の管理者の画面操作のアクセス制御事象に関する監査ログを生成する。

  FPT_RVM.1 により、識別・認証機能及びアクセス制御機能の監査対象事象に対して、監査ログの生成機能が必ず呼び出される。

  FPT_SEP.1 により、許可のない不正なサブジェクトから監査ログの生成機能を分離し、この機能の悪用・改ざんを防ぐ。

  FPT_STM.1 により、高信頼タイムスタンプが提供される。

  これらの機能要件の組み合わせにより、本セキュリティ対策方針は満たされる。

- OE.OS_DB（TOE を動作させる OS や DBMS の機能）

  本セキュリティ対策方針は、TOE を動作させる OS は、利用者の識別・認証機能を提供し、OMI にインストールされる DBMS は、識別・認証機能を具備し、TOE のコンポーネントからアクセスするための手段を提供することを求めている。また、TOE を動作させる全てのサーバ、及び端末上の OS がその Administrator 権限を特定の管理者だけに限定する機能を有することを求めている。さらに、TOE を動作させる OS が、OS 上で動作するサービスの自動回復機能を提供することを求めている。

  FIA_UAU.2d[E] 、 **FIA_UID.2e[E]** により、OS は識別認証機能を提供し、

FIA_UAU.2e[E]、**FIA_UID.2f[E]**により、DBMS は識別認証機能を提供する。
FMT_SMR.1b[E]により、Administrator 権限を特定の管理者のみに制限することを OS の機能によりサポートする。
FMT_SMR.1c[E]により、特定の管理者を許可された者のみに制限することを OS の機能によりサポートする。
FPT_RCV.2[E]により、OPDC のサービスが停止した場合に、自動回復することを OS の機能によりサポートする。
これらの機能要件の組み合わせにより、本セキュリティ対策方針は満たされる。

8.2.3. 拡張 IT セキュリティ機能要件に関する根拠

本 ST で定義する拡張 IT セキュリティ機能要件は、ない。

8.2.4. IT セキュリティ機能要件の依存性に関する根拠

IT セキュリティ機能要件コンポーネントの依存関係を下表に示す。CC パート 2 が規定する依存性を満たさない場合、依存性に関する根拠の欄に正当化に関する説明を追加した。

		Part2 依存性	本 ST 依存性	依存性に関する根拠
FAU	FAU_GEN.1	FPT_STM.1	FPT_STM.1	満たしている
FDP	FDP_ACC.1a	FDP_ACF.1	FDP_ACF.1a	満たしている
	FDP_ACF.1a	FDP_ACC.1、 FMT_MSA.3	FDP_ACC.1a FMT_MSA.3a	満たしている
	FDP_ACC.1b	FDP_ACF.1	FDP_ACF.1b	満たしている
	FDP_ACF.1b	FDP_ACC.1、 FMT_MSA.3	FDP_ACC.1b FMT_MSA.3b	満たしている
	FDP_ACC.1c	FDP_ACF.1	FDP_ACF.1c	満たしている
	FDP_ACF.1c	FDP_ACC.1、 FMT_MSA.3	FDP_ACC.1c FMT_MSA.3c	満たしている
	FDP_IFC.1	FDP_IFF.1	FDP_IFF.1	満たしている
	FDP_IFF.1	FDP_IFC.1、 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3d	満たしている
	FDP_ITT.1a	FDP_ACC.1、または FDP_IFC.1	FDP_ACC.1c	満たしている
	FDP_ITT.1b	FDP_ACC.1、または FDP_IFC.1	FDP_IFC.1	満たしている
FIA	FIA_AFL.1	FIA_UAU.1	FIA_UAU.2a、 FIA_UAU.2b、 FIA_UAU.2c	満たしている
	FIA_SOS.1	なし	N/A	N/A
	FIA_UAU.2a	FIA_UID.1	FIA_UID.2a	満たしている
	FIA_UAU.2b	FIA_UID.1	FIA_UID.2b	満たしている

		Part2 依存性	本 ST 依存性	依存性に関する根拠
	FIA_UAU.2c	FIA_UID.1	FIA_UID.2c	満たしている
	FIA_UAU.7	FIA_UAU.1	FIA_UAU.2a、 FIA_UAU.2b、 FIA_UAU.2c	満たしている
	FIA_UID.2a	なし	N/A	N/A
	FIA_UID.2b	なし	N/A	N/A
	FIA_UID.2c	なし	N/A	N/A
	FIA_UID.2d	なし	N/A	N/A
FMT	FMT_MOF.1	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1a	満たしている
	FMT_MSA.1a	[FDP_ACC.1 または FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	FDP_ACC.1b、 FMT_SMF.1、 FMT_SMR.1a	満たしている
	FMT_MSA.1b	[FDP_ACC.1 または FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	FDP_ACC.1c、 FMT_SMF.1、 FMT_SMR.1a	満たしている
	FMT_MSA.3a	FMT_MSA.1 FMT_SMR.1	N/A	・セキュリティ属性（DB オブジェクト種別）はデフォルト値が付与された以降は変更できないため、FMT_MSA.1 に関する依存性を適用する必要はない。 ・FMT_MSA.3.2a にて役割維持の割付がないため、役割維持（FMT_SMR.1）に関する依存性を適用する必要はない。
	FMT_MSA.3b	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1a	・セキュリティ属性（サイト ID）の管理の依存性は、左記機能要件によって満たされる。 ・セキュリティ属性（DB オブジェクト種別）は、デフォルト値が付与された以降は変更できないため、FMT_MSA.1 に関する依存性を適用する必要はない。 ・FMT_MSA.3.2b にて役割維持の割付がないため、役割維持（FMT_SMR.1）に関する依存性を適用する必要はない。
	FMT_MSA.3c	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1a FMT_MSA.1b	・セキュリティ属性（サイト ID）の管理の依存性は、FMT_MSA.1a によって満たされる。 ・セキュリティ属性（配信用ポリシー情報ファイルのバージョン）の管理の依存性は FMT_MSA.1b によって満たされる。 ・セキュリティ属性（ファイル種別）については、配信処理により TOE の機能で動的に設定されるため、FMT_MSA.1 に関する依存性を適用する必要はない。 ・FMT_MSA.3.2c にて役割維持の割付がないため、役割維持（FMT_SMR.1）に関する依存性を適用する必要はない。
	FMT_MSA.3d	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1a	・セキュリティ属性（サイト ID）の管理の依存性は、FMT_MSA.1a によって満たされる。 ・FMT_MSA.3.2d にて役割維持の割付がないため、役割維持（FMT_SMR.1）に関する依

		Part2 依存性	本 ST 依存性	依存性に関する根拠
				存性を適用する必要はない。
	FMT_MTD.1a	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1a	満たしている
	FMT_MTD.1b	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1a	満たしている
	FMT_MTD.1c	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1c[E]	満たしている
	FMT_SMF.1	なし	N/A	N/A
	FMT_SMR.1a	なし	N/A	N/A
FPT	FPT_FLS.1	ADV_SPM.1	N/A	ADV_SPM.1 を適用しない理由 セキュアな状態について、6.1.6.2 で十分に説明しているため必要ない。
	FPT_RVM.1	なし	N/A	N/A
	FPT_SEP.1	なし	N/A	N/A
	FPT_STM.1	なし	N/A	N/A
FIA	FIA_UAU.2d[E]	FIA_UID.1	FIA_UID.2b[E]	満たしている
	FIA_UAU.2e[E]	FIA_UID.1	FIA_UID.2c[E]	満たしている
	FIA_UID.2e[E]	なし	N/A	N/A
	FIA_UID.2f[E]	なし	N/A	N/A
FMT	FMT_SMR.1b[E]	FIA_UID.1	FIA_UID.2b[E]	満たしている
	FMT_SMR.1c[E]	FIA_UID.1	FIA_UID.2b[E]	満たしている
FPT	FPT_RCV.2[E]	AGD_ADM.1 ADV_SPM.1	AGD_ADM.1	ADV_SPM.1 を適用しない理由 ＜セキュアな状態＞を次により定義する。 “監視対象となる PC 端末上で OPDC のサービスが正常に稼動している状態” これにより、TSP（PDC サービスが正しく稼動しポリシーに違反する操作が行われると OMI に警告ログを送信する）の正しい実施が継続されることから、定義した状態はセキュアであるとみなせる。

8.2.5. IT セキュリティ機能要件の相互サポート関係に関する根拠

IT セキュリティ機能要件で識別される機能要件が組み合わされることにより満たされるセキュリティ対策方針は、8.2.1 及び 8.2.2 の各根拠記述にて述べられる通りである。また、8.2.4 で依存性が認められる要件セットは、依存性に基づく相互サポート構造を構成している。ここでは、依存性以外で相互サポート構造を構成するセキュリティ機能要件セットを示し、①から④で示す側面でセキュリティ対策方針を実現するために寄与する相互サポート効果について説明する。

①迂回防止

OM 認証アカウント所持者としての操作が許可される前に FIA_UAU.2a 及び FIA_UID.2a が必ず呼び出されなければならないが、それは FPT_RVM.1 により保証される。

CWAT 管理者としての操作が許可される前に FIA_UAU.2b 及び FIA_UID.2b が必ず呼び出されなければならないが、それは FPT_RVM.1 により保証される。
サイト管理者としての操作が許可される前に FIA_UAU.2c 及び FIA_UID.2c が必ず呼び出されなければならないが、それは FPT_RVM.1 により保証される。
OPDC 端末にログオンが許可される前に、その OPDC 端末にログオン可能なユーザであることを確認するために FIA_UID.2d が必ず呼び出されなければならないが、それは FPT_RVM.1 により保証される。
FAU_GEN.1 で定義した機能要件に関連する監査対象事象の発生時に確実に監査データを生成するためには、それらの監査対象事象が発生した時に FAU_GEN.1 を確実に実行することが求められるが、それは FPT_RVM.1 により保証される。
以上のセキュリティ機能要件の組み合わせにより、TOE は迂回防止可能な構造を提供する。

②干渉、改ざん防止
管理権限を要する画面へのアクセスを制御する FDP_ACC.1a 及び FDP_ACF.1a、FDP_ACC.1b 及び FDP_ACF.1b は、FPT_SEP.1 により許可されたサブジェクトのみが利用できるよう構成することで、干渉及び改ざんを防止する。許可されたサブジェクトであることを決定するための認証メカニズムに使用する認証情報へのアクセスは、FIA_UAU.2a 及び FIA_UAU.2b で使用する認証情報及び FIA_SOS.1、FMT_MTD.1c を実現するセキュリティ機能は、FMT_SMR.2c[E]によって、FIA_UAU.2d[E]の認証に成功した利用者に使用を制限し、FIA_UAU.2c、FIA_UID.2ｄに関しては FMT_MTD.1a で許可された役割に操作を制限する。
OPDC 端末ログイン可能ユーザが設定されている場合は、FPT_SEP.1 により許可されたサブジェクのみが利用できるよう構成することで、干渉及び改ざんを防止する。
FAU_GEN.1 で定義した機能要件に関連する監査対象事象の発生時に確実に監査データを生成するためには、FAU_GEN.1 が許可のないアクセスにより干渉、改ざんを受けることを防止することが求められるが、それは FPT_SEP.1 により保証される。
以上のセキュリティ機能要件の組み合わせにより、TOE は干渉および改ざん防止可能な構造を提供する。

③非活性化防止
ポリシー情報の配信強化を定義する FDP_ITT.1a、FDP_ACC.1c、FDP_ACF.1c、警告ログの送信強化を定義する FDP_ITT.1b、FDP_IFC.1、FDP_IFF.1、FPT_FLS.1 、OPDC 端末ログオン可能ユーザ識別を定義する FIA_UID.2d を停止するパラメータへのアクセスを、FMT_MOF.1 で許可された役割に制限することで非活性化防止効果を実現する。
以上のセキュリティ機能要件の組み合わせにより、TOE は非活性化防止可能な構造を提供

する。

④無効化検出
FAU_GEN.1 は、①の迂回防止、②の干渉、改ざん防止を構成するセキュリティ機能のうち、TSF の不正使用と推定される事象の監査データを生成することで、TSF の無効化の恐れのある事象を検出可能とする。
TOE は上記のセキュリティ機能要件が監査対象事象を実現するその他のセキュリティ機能要件と関連して無効化検出可能な構造を提供する。

8.2.6. 最小機能強度根拠

本 TOE は、外部とのネットワーク接続において適切な管理が実施されているオフィスに接続される。よってインターネットを介して不特定多数の者に直接攻撃されるような可能性はなく、OPDC 端末の利用を許可された端末利用者及び OPDC 端末の利用を許可されていない不正アクセス者を想定した攻撃者に対抗する強度レベルを有すれば良い。従って、本 TOE は、攻撃者のレベルとして低レベルを想定しており、最小機能強度として SOF－基本の選択は妥当である。

8.2.7. IT セキュリティ保証要件根拠

本 TOE は、ネットワーク的に十分なセキュリティを確保した環境に設置され利用されるため、低レベルから中レベルの保証レベルが提供される EAL2 の選択は妥当である。

なお、保証要件依存性分析は、パッケージである EAL が選択されているため妥当であるとして、詳細は論じない。

8.2.8. IT セキュリティ機能要件のセットの一貫性根拠

本 ST で定義する IT セキュリティ機能要件セットは、以下に示す通り各事象に関する機能要件セットに矛盾や競合がなく、また各事象間で矛盾や競合はないと考えられることから、全体として競合する要件はなく、一貫しているといえる。

- 管理者登録に関する機能要件は、FMT_MTD.1a、FIA_SOS.1、FMT_MTD.1c である。割付に重複や矛盾が存在する可能性が考えられるが、登録すべきアカウントごとに機能要件を分けて定義しており、重複や矛盾はない。したがって、本事象に関する機能要件のセットは一貫している。
- 識別･認証に関係する機能要件は、FIA_UID.2a,2b,2c、FIA_UAU.2a,2b,2c、FIA_UAU.7、FIA_AFL.1 、FIA_SOS.1 である。割付に重複や矛盾が存在する可能性が考えられるが、識別・認証すべきアカウント種別は 3 種類あり、それぞれ個別の識別･認証に関する要件

を定義し、認証情報の品質尺度、認証失敗時の要件は共通化されるためそれぞれ 1 つの要件で定義したことにより、重複や矛盾はない。また FIA_UID.2d は OPDC 端末のログオン可能ユーザを制御することから、上記の識別・認証に関係する機能要件と重複や矛盾がない。したがって、本事象に関する機能要件のセットは一貫している。

- アクセス制御及び情報フロー制御に関係する機能要件は、FDP_ACC.1a,1b.1c、FDP_ACF.1a,1b,1c、FDP_IFC.1、FDP_IFF.1、FDP_ITT.1a,1b である。割付が競合する可能性が考えられるが、オブジェクト、サブジェクト、および操作のルールは、オブジェクト毎、操作毎に分けて定義しており、矛盾や重複、競合はない。したがって、本事象に関する機能要件のセットは一貫している。
- セキュリティ管理に関係する機能要件は、FMT_MSA.1a,1b、FMT_MSA.3a,3b,3c,3d、FMT_MTD.1a,1b,1c、FMT_SMF.1、FMT_SMR.1a である。割付に重複や矛盾が存在する可能性が考えられるが、3 種類の管理者毎に管理対象（TSF データ、セキュリティ属性）を分けて定義しており、管理機能の特定においても、重複や矛盾はない。したがって、本事象に関する機能要件のセットは一貫している。
- ポリシー配信強化に関係する機能要件は、FDP_ACC.1c、FDP_ACF.1c、FDP_ITT.1a、FMT_MSA.3c である。これらは依存性から導かれる機能要件のセットであり、競合する可能性はない。したがって、本事象に関する機能要件のセットは一貫している。
- 警告ログ送信強化に関係する機能要件は、FDP_IFC.1、FDP_IFF.1、FDP_ITT.1b、FMT_MSA.3d である。これらは依存性から導かれる機能要件のセットであり、競合する可能性はない。したがって、本事象に関する機能要件のセットは一貫している。
- 迂回防止とドメイン分離に関する機能要件は、識別認証に関する機能要件、および FPT_RVM.1、FPT_SEP.1 である。これらは、迂回防止や干渉・改ざん防止で相互にサポートする機能要件であり、競合や矛盾は含まれない。したがって、本事象に関する機能要件のセットは一貫している。
- 監査事象に関する機能要件は、FAU_GEN.1 である。1 つの機能要件だけが関係することから、競合や矛盾の可能性はない。したがって、本事象に関する機能要件のセットは一貫している。
- IT 環境に関係する機能要件は、プラットフォームの資源アクセスに対する識別認証（FIA_UID.2e[E].2f[E]、FIA_UAU.2d[E].2e[E]）、と、OS の Administrator の役割維持と関連付け(FMT_SMR.1b[E])、管理者の役割維持と関連付け(FMT_SMR.1c[E])、及び OS によるサービス停止からの自動回復(FPT_RCV.2[E])である。これらの機能要件は、それぞれが TOE のセキュリティ機能要件をサポートするものであり、機能要件間の競合の可能性はない。したがって、IT 環境に関する機能要件のセットは一貫している。

8.3. TOE 要約仕様根拠

8.3.1. TOE セキュリティ機能の必要性に関する根拠

TOE のセキュリティ機能と TOE セキュリティ機能要件との適合性を下表に示す。TOE のセキュリティ機能が少なくとも１つ以上の TOE セキュリティ機能要件に対応していることを示している。

TOE セキュリティ機能 / TOE セキュリティ機能要件		管理者登録機能		管理者識別認証機能			OPDC 端末ログオン可能ユーザ識別機能	アクセス制御機能			ポリシー配信強化機能	警告ログ送信強化機能	セキュリティ管理機能		監査機能
		SF.OM_REGIST	SF.CWAT-ADM_REGIST	SF.OM_I&A	SF.CWAT-ADM_I&A	SF.SITE-ADM_I&A	SF.OPDCLOGON_USER_ID	SF.SITES-INFO_ACCESS	SF.SITES-DATA_ACCESS	SF.SITE-DETAIL_ACCESS	SF.POLICY_DEL	SF.WARNING_LOG_SEND	SF.CWAT-ADM	SF.SITE-ADM	SF.AUDIT
FAU	FAU_GEN.1														●
FDP	FDP_ACC.1a							●	●						
	FDP_ACF.1a							●	●						
	FDP_ACC.1b									●					
	FDP_ACF.1b									●					
	FDP_ACC.1c										●				
	FDP_ACF.1c										●				
	FDP_IFC.1											●			
	FDP_IFF.1											●			
	FDP_ITT.1a										●				
	FDP_ITT.1b											●			
FIA	FIA_AFL.1			●	●	●									
	FIA_SOS.1	●	●										●		
	FIA_UAU.2a			●											
	FIA_UAU.2b				●										
	FIA_UAU.2c					●									
	FIA_UAU.7			●	●	●									
	FIA_UID.2a			●											
	FIA_UID.2b				●										
	FIA_UID.2c					●									
	FIA_UID.2d						●								
FMT	FMT_MOF.1													●	
	FMT_MSA.1a												●		

TOE セキュリティ機能 / TOE セキュリティ機能要件		管理者登録機能		管理者識別認証機能			OPDC 端末ログオン可能ユーザ識別機能	アクセス制御機能			ポリシー配信強化機能	警告ログ送信強化機能	セキュリティ管理機能		監査機能
		SF.OM_REGIST	SF.CWAT-ADM_REGIST	SF.OM_I&A	SF.CWAT-ADM_I&A	SF.SITE-ADM_I&A	SF.OPDCLOGON_USER_ID	SF.SITES-INFO_ACCESS	SF.SITES-DATA_ACCESS	SF.SITE-DETAIL_ACCESS	SF.POLICY_DEL	SF.WARNING_LOG_SEND	SF.CWAT-ADM	SF.SITE-ADM	SF.AUDIT
	FMT_MSA.1b													●	
	FMT_MSA.3a							●	●					●	
	FMT_MSA.3b									●					
	FMT_MSA.3c										●				
	FMT_MSA.3d											●			
	FMT_MTD.1a												●		
	FMT_MTD.1b													●	
	FMT_MTD.1c	●	●												
	FMT_SMF.1												●	●	
	FMT_SMR.1a												●	●	
FPT	FPT_FLS.1											●			
	FPT_RVM.1			●	●	●	●	●	●	●					●
	FPT_SEP.1			●	●	●	●	●	●	●					●
	FPT_STM.1														●

8.3.2. TOE セキュリティ機能の十分性に関する根拠

● FAU_GEN.1

FAU_GEN.1 は、監査対象事象の監査記録を生成することを規定している。

SF.AUDIT は、

・ OM 認証、サイト管理認証、及びサイトログオン認証のアクションについての監査記録を生成する。また、OMI の各種管理画面へのアクセスに関する監査記録を生成する。

従って、本機能要件は満たされる。

● FDP_ACC.1a

FDP_ACC.1a は、オブジェクト（サイトの統計情報 DB、サイトの管理情報 DB）に対して

制御されるサブジェクト（OM 認証プロセス、サイト管理認証プロセス）の関係を規定している。

SF. SITES-INFO は、OM 認証に成功したプロセスのみに、サイトの統計情報の参照を許可するためのアクセス制御を規定する。

SF. SITES-DATA_ACCESS は、サイト管理認証に成功したプロセスのみに、サイトの管理情報の参照、登録、更新、削除を許可するためのアクセス制御を規定する。

従って、本機能要件は満たされる。

● FDP_ACF.1a

FDP_ACF.1a は、オブジェクト（サイトの統計情報、サイトの管理情報）に対して制御されるサブジェクト（OM 認証プロセス、サイト管理認証プロセス）の関係の規則を規定している。

SF. SITES-INFO_ACCESS は、以下の規則が適用されるアクセス制御を実施する。

- 認証に成功した OM 認証プロセスのみが、すべてのサイトのサイト統計情報を参照することができる。

SF. SITES-DATA_ACCESS は、以下の規則が適用されるアクセス制御を実施する。

- 認証に成功したサイト管理認証プロセスのみが、すべてのサイトのサイト管理情報を参照、登録、更新、削除することができる。

従って、本機能要件は満たされる。

● FDP_ACC.1b

FDP_ACC.1b は、オブジェクト（ポリシー情報、警告ログ、配信用ポリシー情報ファイル）に対して制御されるサブジェクト（サイトログオン認証プロセス）の関係を規定している。

SF. SITE-DETAIL_ACCESS は、サイト管理者を代行するタスクであるサイトログオン認証プロセスが、同じサイトのポリシー情報を登録、参照、削除、更新および更新の反映をしたり、配信用ポリシー情報ファイルを強制配信したり、警告ログを参照、出力するためのアクセス制御を実施する。

従って、本機能要件は満たされる。

● FDP_ACF.1b

FDP_ACF.1b は、オブジェクト（ポリシー情報、警告ログ）に対して制御されるサブジェクト（サイトログオン認証プロセス）の関係の規則を規定している。

SF. SITE- DETAIL_ACCESS は、以下の規則が適用されるアクセス制御を実施する。

- サイト ID に関連付けられたサイトログオン認証プロセスは同じサイトのポリシー

情報の登録、参照、削除、更新、更新の反映を行うことができる。また、配信用ポリシー情報ファイルの強制配信を行うことができる。また、警告ログの参照、出力を行うことができる。

従って、本機能要件は満たされる。

● FDP_ACC.1c

FDP_ACC.1c は、オブジェクト（配信用ポリシー情報ファイル）に対して制御されるサブジェクト（DC プロセス）の関係を規定している。

SF. POLICY_DEL は、上位 NM プロセスから DC プロセスに対して配信用ポリシー情報ファイルを配信するためのアクセス制御を実施する。

従って、本機能要件は満たされる。

● FDP_ACF.1c

FDP_ACF.1c は、オブジェクト（配信用ポリシー情報ファイル）に対して制御されるサブジェクト（DC プロセス）の関係の規則を規定している。

SF. POLICY_DEL は、以下の規則が適用されるアクセス制御を実施する。

- DC から上位 NM の IP アドレスのノードに対し上位 NM が保持するポリシー情報のバージョンを問合せると、上位 NM は DC が属するサイトのポリシー情報のバージョンを回答する。
- DC は、自身が保持するポリシー情報のバージョンと上位 NM が保持するポリシー情報のバージョンを比較し、上位 NM のポリシー情報のバージョンの方が大きい場合、上位 NM にポリシー情報の送信を要求する。
- 送信要求を受信した上位 NM は、DC が属するサイトのポリシー情報を送信する。
- DC は、ポリシー情報を受信し保存する。
- サイト管理者は、自身の管理サイトの DC に適用されているポリシー情報のバージョンを確認することができる。
- サイト管理者は、自身の管理サイトの DC に対して、最新のバージョンのポリシー情報を強制的に配信することができる。

従って、本機能要件は満たされる。

● FDP_IFC.1

FDP_IFC.1 は、情報（警告ログ）のフローに対して制御されるサブジェクト（送付元：DC プロセス、送付先：OMI プロセス）の関係を規定している。

SF.WARNING_LOG_SEND は、DC プロセスから OMI プロセスに対して警告ログを送信するための情報フロー制御を実施する。

従って、本機能要件は満たされる。

● FDP_IFF.1

FDP_IFF.1 は、情報（警告ログ）のフローに対して制御されるサブジェクト（送付元：DC プロセス、送付先：OMI プロセス）の関係の規則を規定している。

SF.WARNING_LOG_SEND は、以下の規則が適用される情報フロー制御を実施する。

- 警告イベントが発生すると DC は OMI に対して警告ログを UDP（即時性の高いプロトコル）で送信する。
- OMI は警告ログを受信すると、警告ログに付与されたサイト ID と、OMI が保持するサイト ID のリストから、サイトの警告ログとして受け付ける。
- DC は一定の配信インターバルで、OMI に対して警告ログを TCP（信頼性の高いプロトコル）で再送する。
- OMI は再送された警告ログを未受領であれば受付け、受領済であれば破棄する。

従って、本機能要件は満たされる。

● FDP_ITT.1a

FDP_ITT.1a は、利用者データ(配信用ポリシー情報)が、TOE の物理的パート間を転送される場合、使用不可を防ぐためのアクセス制御を規定している。

SF. POLICY_DEL は、上位 NM プロセスから DC プロセスに対するポリシー情報の送信において、配信失敗に起因する使用不可を防ぐためのアクセス制御を実施する。

従って、本機能要件は満たされる。

● FDP_ITT.1b

FDP_ITT.1b は、利用者データ(警告ログ)が、TOE の物理的パート間を転送される場合、使用不可を防ぐための情報フロー制御を規定している。

SF.WARNING_LOG_SEND は、DC プロセスから OMI プロセスに対する警告ログの送信において、送信失敗に起因する使用不可を防ぐための情報フロー制御を実施する。

従って、本機能要件は満たされる。

● FIA_AFL.1

FIA_AFL.1 は、認証失敗時のアクションを規定している。

SF.OM_I&A は、OM 認証において、一つの ID につき 3 回の認証失敗を検知すると 10 秒間操作不能とし、エラー回数が上限を超えた旨のエラーメッセージのポップアップ画面を表示する。OK ボタン押下により認証画面が終了し、再度、認証画面を立ち上げることにより、ID とパスワードが入力可能な状態になる。

SF.CWAT-ADM_I&A は、サイト管理認証において、一つの ID につき 3 回の認証失敗を検知すると 10 秒間操作不能とし、エラー回数が上限を超えた旨のエラーメッセージのポップアップ画面を表示する。OK ボタン押下により認証画面が終了し、再度、認証画面を立ち上げることにより、ID とパスワードが入力可能な状態になる。
SF.OM_I&A は、サイトログオン認証において、一つの ID につき 3 回の認証失敗を検知すると 10 秒間操作不能とし、エラー回数が上限を超えた旨のエラーメッセージのポップアップ画面を表示する。OK ボタン押下により認証画面が終了し、再度、認証画面を立ち上げることにより、ID とパスワードが入力可能な状態になる。
従って、本機能要件は満たされる。

● FIA_SOS.1
FIA_SOS.1 は、パスワードの品質を規定している。
SF.OM_REGIST は、OM 認証のパスワードの品質として、8 文字以上 32 文字以下で半角英数小文字の文字種から構成されることを検証する。
SF.CWAT-ADM_REGIST は、サイト管理認証のパスワードの品質として、8 文字以上 32 文字以下で半角英数小文字の文字種から構成されることを検証する。
SF.CWAT-ADM は、サイトログオン認証のパスワードの品質として、8 文字以上 32 文字以下で半角英数小文字の文字種から構成されることを検証する。
従って、本機能要件は満たされる。

● FIA_UAU.2a
FIA_UAU.2a は、OM 認証アカウントの認証を規定している。
SF.OM_I&A は、サイトの統計情報を表示する画面（サイトモニタ）へアクセスする利用者が、許可された利用者（OM 認証アカウント所持者）であることを認証する。
従って、本機能要件は満たされる。

● FIA_UAU.2b
FIA_UAU.2b は、サイト管理認証アカウントの認証を規定している。
SF.CWAT-ADM_I&A は、サイト管理情報を登録する画面（個別サイト詳細画面）へアクセスする利用者が、許可された利用者（CWAT 管理者）であることを認証する。
従って、本機能要件は満たされる。

● FIA_UAU.2c
FIA_UAU.2c は、サイトログオン認証アカウントの認証を規定している。
SF.SITE-ADM_I&A は、サイトのポリシー設定画面や警告ログを監視する画面（OM モニ

タ画面）へアクセスする利用者が、許可された利用者（当該サイトのサイト管理者）であることを認証する。
従って、本機能要件は満たされる。

● FIA_UAU.7
FIA_UAU.7 は、認証中のフィードバックに“*”を返すことを規定している。
SF.OM_I&A は、OM 認証において、OM 認証画面にて入力されるパスワードに対して、1 文字毎に“*”を返し、パスワードのダイレクト表示を防止する。
SF.CWAT-ADM_I&A は、サイト管理認証において、サイト管理認証画面にて入力されるパスワードに対して、1 文字毎に“*”を返し、パスワードのダイレクト表示を防止する。
SF.SITE-ADM_I&A は、サイトログオン認証において、サイトログオン認証画面にて入力されるパスワードに対して、1 文字毎に“*”を返し、パスワードのダイレクト表示を防止する。
従って、本機能要件は満たされる。

● FIA_UID.2a
FIA_UID.2a は、OM 認証アカウントの識別を規定している。
SF.OM_I&A は、サイトの統計情報を表示する画面（サイトモニタ）へアクセスする利用者が、許可された利用者（OM 認証アカウント所持者）であることを識別する。
従って、本機能要件は満たされる。

● FIA_UID.2b
FIA_UID.2b は、サイト管理認証アカウントの識別を規定している。
SF.CWAT-ADM_I&A は、サイト管理情報を登録する画面（個別サイト詳細画面）へアクセスする利用者が、許可された利用者（CWAT 管理者）であることを識別する。
従って、本機能要件は満たされる。

● FIA_UID.2c
FIA_UID.2c は、サイトログオン認証アカウントの識別を規定している。
SF.SITE-ADM_I&A は、サイトのポリシー設定や警告ログを監視する画面（OM モニタ画面）へアクセスする利用者が、許可された利用者（そのサイトのサイト管理者）であることを識別する。
従って、本機能要件は満たされる。

● FIA_UID.2d

FIA_UID.2d は、OPDC 端末ログオン可能ユーザアカウントの識別を規定している。
SF.OPDCLOGON_USER_ID は、OPDC 端末にログオンしようとする利用者が、当該 OPDC 端末へのログオン可能ユーザであることを識別する。
従って、本機能要件は満たされる。

● FMT_MOF.1
FMT_MOF.1 は、サイト管理者によるサイトのポリシー配信強化機能のふるまい管理、及び警告ログ送信強化機能のふるまい管理、OPDC 端末ログオン可能ユーザ識別機能の停止管理を規定している。
SF.SITE_ADM は、以下のセキュリティ機能のふるまい管理、または停止管理を当該サイトのサイト管理者のみが行うことを規定している。

- 配信インターバルの制御によるポリシー配信強化機能のふるまい管理
- 配信インターバルの制御による警告ログ送信強化機能のふるまい管理
- 警告ログ再送最大件数の制御による警告ログ送信強化機能のふるまい管理
- ポリシー違反時の警告発信設定、監査ログ出力設定の制御による警告ログ送信強化機能の停止管理
- ノードへのログオン可能ユーザ設定の制御による OPDC 端末ログオン可能ユーザ識別機能の停止管理

従って、本機能要件は満たされる。

● FMT_MSA.1a
FMT_MSA.1a は、CWAT 管理者によるサイト（サイト ID）の登録、更新、削除を規定している。
SF.CWAT_ADM により、サイト管理認証に成功した CWAT 管理者のみが、サイト（サイト ID）の登録、更新、削除を行うことができる。
従って、本機能要件は満たされる。

● FMT_MSA.1b
FMT_MSA.1b は、サイト管理者による管理サイトのノード属性（配信用ポリシー情報ファイルのバージョン）の参照を規定している。
SF.SITE_ADM により、サイトログオン認証に成功したサイト管理者のみが、そのサイトのノード属性（ポリシー情報のバージョン）を参照できる。
従って、本機能要件は満たされる。

● FMT_MSA.3a

FMT_MSA.3a は、サイトの統計情報、または、サイトの管理情報の DB オブジェクトに付与される DB オブジェクト種別のデフォルト値を規定している。
SF.SITES-INFO_ACCESS、により、サイトの統計情報の DB オブジェクト生成時に DB オブジェクト種別として「サイトの統計情報」が付与される。
SF.SITES-DATA_ACCESS、により、サイトの管理情報の DB オブジェクト生成時に DB オブジェクト種別として「サイトの管理情報」が付与される。
従って、本機能要件は満たされる。

● FMT_MSA.3b
FMT_MSA.3b は、サイトの詳細情報 DB オブジェクトに付与されるサイト ID、および DB オブジェクト種別のデフォルト値を規定している。
SF.SITE-DETAIL_ACCESS により、サイトの詳細情報の DB オブジェクト生成時に DB オブジェクト種別として「サイトの詳細情報」が付与される。また、サイトの詳細情報を設定するサイト管理者が属するサイトのサイト ID が DB オブジェクトに付与される。
従って、本機能要件は満たされる。

● FMT_MSA.3c
FMT_MSA.3c は、配信用ポリシー情報ファイルに付与されるサイト ID、バージョン、ファイル種別のデフォルト値を規定している。
SF.POLICY_DEL により、配信用ポリシー情報ファイルの生成時（ポリシー情報の更新の反映時）にサイトログオン認証プロセスのサイト ID が配信用ポリシー情報ファイルに付与され、また重複のない番号が配信用ポリシー情報ファイルのバージョンに付与される。さらに、配信用ポリシー情報ファイルにノード属性、ユーザ属性、ポリシーなどを特定するためのファイル種別が付与される。
従って、本機能要件は満たされる。

● FMT_MSA.3d
FMT_MSA.3d は、警告ログに付与されるサイト ID のデフォルト値を規定している。
SF.WARNING_LOG_SEND により、警告ログ生成時に警告が発生した DC が属するサイトのサイト ID が警告ログに付与される。
従って、本機能要件は満たされる。

● FMT_MTD.1a
FMT_MTD.1a は、CWAT 管理者にサイトログオン認証アカウントのアカウント ID、およびパスワードの設定を規定している。

SF.CWAT_ADM により、サイト管理認証に成功した CWAT 管理者のみが、サイトログオン認証アカウントのアカウント ID、およびパスワードを設定することができる。
従って、本機能要件は満たされる。

● FMT_MTD.1b

FMT_MTD.1b は、サイト管理者によるノードへのログオン可能ユーザの設定を規定している。
SF.SITE_ADM により、サイトログオン認証に成功したサイト管理者のみが、そのサイトのノードに対するログオン可能ユーザを設定することができる。
従って、本機能要件は満たされる。

● FMT_MTD.1c

FMT_MTD.1c は、制限された管理者による OM 認証アカウントのアカウント ID、およびパスワードの登録、サイト管理認証アカウントのアカウント ID、およびパスワードの登録、変更、削除、参照を規定している。
SF.OM_REGIST により、制限された管理者のみが OM 認証アカウントのアカウント ID、およびパスワードを登録、変更、削除、参照することができる。
SF.CWAT-ADM_REGIST により、制限された管理者のみがサイト管理認証アカウントのアカウント ID、およびパスワードを登録、変更、削除、参照することができる。
従って、本機能要件は満たされる。

● FMT_SMF.1

FMT_SMF.1 は、セキュリティ管理機能を特定している。
SF.CWAT_ADM は、以下のセキュリティ管理機能を提供する。

- サイトログオン認証アカウントの登録、更新、削除、参照機能
- サイト属性(サイト ID)の登録、更新、削除、参照機能

SF.SITE_ADM は、以下のセキュリティ管理機能を提供する。

- ポリシー情報の配信のふるまい管理
- 警告ログ再送のふるまい管理
- 管理サイトのノード属性（ポリシー情報のバージョン）の参照
- 管理サイトのノードに対するログオン可能ユーザの設定

SF.OM_REGIST は、以下のセキュリティ管理機能を提供する。

- OM 認証アカウント(アカウント ID,パスワード)の登録、変更、削除、参照

SF.CWAT-ADM_REGIST は、以下のセキュリティ管理機能を提供する。

- サイト管理認証アカウント(アカウント ID,パスワード)の登録、変更、削除、参照

従って、本機能要件は満たされる。

● FMT_SMR.1a

FMT_SMR.1a は、役割 : OM 認証アカウント所持者、CWAT 管理者、サイト管理者を規定している。

SF.OM_ADM は、OM 認証により認証された利用者を OM 認証アカウント所持者として認識する。

SF.CWAT_ADM は、サイト管理認証により認証された利用者を CWAT 管理者として認識する。

SF.SITE_ADM は、サイトログオン認証により認証された利用者をサイト管理者として認識する。

従って、本機能要件は満たされる。

● FPT_FLS.1

FPT_FLS.1 は、DC がネットワークから切断状態になることによって警告ログが OMI に送信できなくなる障害が生じたときにセキュアな状態を保持することを規定している。

SF.WARNING_LOG_SEND は、OPDC が動作する PC 端末がモバイル状態となっているなど、OM が管理していない状態のノードで生成した警告ログは、ネットワーク再接続時に警告再送テンポラリファイルよりネットワーク切断時からの警告ログを抽出し、TCP で送信することにより、ネットワーク接続状況に起因する転送未達を防止する。

従って、本機能要件は満たされる。

● FPT_RVM.1

FPT_RVM.1 は、TOE の各セキュリティ機能の動作進行が許可される前に、必ず TSP 実施機能が呼び出されることをサポートすることを規定している。

SF.SITES-INFO_ACCESS は、サイトの詳細情報へのアクセスが許可される前に動作することが必須である **SF.OM_I&A**（OM 認証機能）を必ず起動する。

SF.SITES-DATA_ACCESS は、サイトの管理情報へのアクセスが許可される前に、動作することが必須である **SF.CWAT-ADM_I&A**（サイト管理認証機能）を必ず起動する。

SF.SITE-DETAIL_ACCESS は、サイトのポリシー情報、警告ログへのアクセスが許可される前に、動作することが必須である **SF.SITE-ADM _I&A**（そのサイトのサイトログオン認証機能）を必ず起動する。

SF.OPDCLOGON_USER_ID は、OPDC 端末へのログオン可能ユーザが設定されている場

合、当該 OPDC 端末へのログオンを行う前に、ログオン可能なユーザであることの識別確認が確実に行われる。
SF.AUDIT は、上記の各セキュリティ機能の実行に伴う必要な監査対象事象に対して確実に動作する。
従って、本機能要件は満たされる。

● FPT_SEP.1
FPT_SEP.1 は、信頼されないサブジェクトによる干渉と改ざんからそれを保護するためのセキュリティドメインを維持し、サブジェクトのセキュリティドメイン間を分離することを規定している。
SF.OM_I&A は、OM 認証アカウント所有者だけが扱える諸機能（**SF.SITES-INFO_ACCESS** によるサイトの統計情報へのアクセス機能を含む）が提供される OM 認証ドメインを保持し、許可されないサブジェクトによる干渉行為を許可しない。
SF.CWAT-ADM_I&A は、CWAT 管理者だけが扱える諸機能（**SF.SITES-DATA_ACCESS** によるサイトの管理情報へのアクセス機能を含む）が提供されるサイト管理認証ドメインを保持し、許可されないサブジェクトによる干渉行為を許可しない。
SF.SITE-ADM_I&A は、サイト管理者だけが扱える諸機能（**SF.SITE-DETAIL_ACCESS** によるサイトの詳細情報へのアクセス機能を含む）が提供されるサイトログオン認証ドメインを保持し、許可されないサブジェクトによる干渉行為を許可しない。
SF.OPDCLOGON_USER_ID は、OPDC 端末へのログオン可能ユーザが設定されている場合、当該 OPDC 端末へのログオン可能なユーザ識別ドメインを保持し、許可されないサブジェクトによる干渉行為を許可しない。
SF.AUDIT は、許可のないサブジェクトによる干渉及び改ざん行為から保護される。
従って、本機能要件は満たされる。

● FPT_STM.1
FPT_STM.1 は、高信頼タイムスタンプを提供することを規定している。
SF.AUDIT は、OS から取得した時間データからタイムスタンプを生成し監査レコードに付与する。従って、本機能要件は満たされる。

8.3.3. TOE セキュリティ機能強度に関する根拠
確率的・順列的メカニズムを有する TOE セキュリティ機能は、以下の通りである。

①SF.OM_I&Aが提供するOM認証パスワードの認証メカニズム

②SF.CWAT-ADM_I&Aが提供するサイト管理認証パスワードの認証メカニズム
③SF.SITE-ADM_I&Aが提供するサイトログオン認証パスワードの認証メカニズム

①～③のメカニズムの機能強度はそれぞれ SOF－基本を満たすことを、6.2 にて主張している。したがって、これら機能強度の最小値は SOF－基本である。これは、5.1.2 にて TOE セキュリティ機能要件に対して主張される最小機能強度：SOF－基本と一貫している。

8.3.4. 相互サポートする TOE セキュリティ機能に関する根拠

8.2.5 で示した IT セキュリティ機能要件の相互サポート関係に関する根拠が、TOE セキュリティ機能に含まれる追加情報により影響を受けないことの根拠を以下に示す。

①迂回防止
迂回防止に関係する機能要件（識別認証、バイパス防止、ドメイン分離、監査データ生成）は、TOE セキュリティ機能によって具体化・詳細化されるが追加情報はない。したがって、TOE が迂回防止可能な次の構造を提供する根拠に影響を与えない。
- セキュリティ管理機能の使用前に識別認証が必ず呼び出される。
- 監査対象事象が発生したときには、確実に監査データ生成を実行する。

②干渉、改ざん防止
干渉、改ざん防止に関係する機能要件（アクセス制御、ドメイン分離、認証情報の登録・管理）は、TOE セキュリティ機能によって具体化・詳細化されるが、追加情報はない。したがって、TOE が干渉・改竄防止可能な次の構造を提供する根拠に影響を与えない。
- 管理権限を要する画面へのアクセスは、許可された主体のみが可能である。
- 認証情報へのアクセスは許可された主体のみが可能である。
- 監査データの生成は、許可のないアクセスから保護される。

③非活性化防止
非活性化防止に関係する機能要件（ポリシー配信強化、警告ログ送信強化、OPDC 端末ログオン可能ユーザ登録に関する機能要件と、セキュリティ機能を停止するパラメータの管理要件）は、TOE セキュリティ機能によって具体化・詳細化されるが、追加情報はない。したがって、TOE が非活性化防止可能な次の構造を提供する根拠に影響を与えない。
- ポリシー配信強化、警告ログ送信強化、OPDC 端末ログオン可能ユーザ登録機能を非活性化し得るパラメータの管理を当該サイトのサイト管理者のみに制限する。

④無効化検出

無効化検出に関係する機能要件（監査データの生成）は、TOE セキュリティ機能によって具体化・詳細化されるが、追加情報はない。したがって、TOE が無効化防止可能な次の構造を提供する根拠に影響を与えない。

・ 監査対象事象における監査データを生成することで、TSF の無効化の恐れのある事象を検出とする。

8.3.5. 保証手段根拠

評価保証レベル EAL2 において必要なドキュメントは、6.3 において説明される保証手段に示されたドキュメント資料により網羅されている。これら保証手段として提示されているドキュメントに従った開発、テストの実施、脆弱性の分析、構成管理、配付手続きが実施され、適切なガイダンス文書が作成されることにより、TOE セキュリティ保証要件が満たされる。

8.4. PP 主張根拠

本 ST は参照する PP は存在しない。