Interstage Application Server Enterprise Edition 8.0.3 (Linux 64bit) Security Target

２００７/１０/１１

富士通株式会社

－ 更新履歴 －

日付	版数	更新箇所	更新内容	作成者
2006/10/30	1.0	新規作成	－	富士通株式会社
2006/12/22	1.1	全般	・ TOE 範囲の見直し	富士通株式会社
2007/2/13	1.2	・ TOE 記述 ・ IT セキュリティ要件 ・ TOE 要約仕様	・ 所見報告書（ASE001-01～ASE003-01）への対応 ・ 機能名称の変更（レスポンス監視→サーバアプリケーションタイマ機能）	富士通株式会社
2007/2/28	1.3	・ TOE 記述 ・ IT セキュリティ要件 ・ TOE 要約仕様	・ 所見報告書（ASE004-01）への対応 ・ 機能名称の変更（業務の自動復旧→アプリケーション自動再起動）	富士通株式会社
2007/3/22	1.4	・ TOE 記述 ・ 根拠	・ 所見報告書（ASE005-01）への対応	富士通株式会社
2007/5/10	1.5	・ 全般	・ 所見報告書（ASE006-01～ASE007-01、AGD001-01）への対応	富士通株式会社
2007/7/10	1.6	・ 全般	・ 所見報告書（ASE008-01）への対応	富士通株式会社
2007/7/17	1.7	・ ST 概説	・ 修正番号の変更	富士通株式会社
2007/8/2	1.8	・ セキュリティ対策方針 ・ 根拠	・ 所見報告書（ASE009-01）への対応	富士通株式会社
2007/9/12	1.9	・ TOE 要約仕様 ・ 根拠	・ 所見報告書（ASE010-01）への対応	富士通株式会社
2007/10/11	2.0	・ 根拠	・ 所見報告書（ASE011-01）への対応	富士通株式会社

＜目次＞

＜表目次＞

＜図目次＞

1. ST 概説

本章では、ST 識別、ST 概要、CC 適合、参考資料、及び表記規則、用語、略語について記述する。

1.1. ST 識別

1.1.1. ST の識別と管理

名称：Interstage Application Server Enterprise Edition 8.0.3 (Linux 64bit)
Security Target

バージョン：第 2.0 版

作成日：2007 年 10 月 11 日

作成者：富士通株式会社

1.1.2. TOE の識別と管理

名称：Interstage Application Server Enterprise Edition

バージョン：8.0.3 (Linux 64bit)

作成者：富士通株式会社

修正番号：修正プログラムT000633QP-02、T000179QP-01、T000681QP-01を適用

1.1.3. 適用する CC のバージョン

CC v2.3

補足-0512 適用

1.2. ST 概要

本書は、Interstage Application Server Enterprise Edition 8.0.3 のセキュリティ仕様を定めたセキュリティターゲットである。

TOE はアプリケーションサーバプログラムであり、アプリケーションを動作させるために必要な環境の構築から運用、監視、保守に至る運用管理や、業界標準・オープンソースに対応したアプリケーションの実行環境を提供する製品である。

本 ST では、アプリケーションの実行状態の維持・管理のために、TOE が提供するセキュリティ機能を規定している。

1.3. CC 適合

本 ST は、以下を満たしている。

- パート 2 適合
- パート 3 適合

・ EAL2 追加　追加する保証コンポーネントは AVA_MSU.1
・ 適合する PP は存在しない

1.4. 参考資料

- 情報技術セキュリティ評価のためのコモンクライテリア パート 1:概説と一般モデル バージョン 2.3 2005 年 8 月 CCIMB-2005-08-001
- 情報技術セキュリティ評価のためのコモンクライテリア パート 2:セキュリティ機能要件 バージョン 2.3 2005 年 8 月 CCIMB-2005-08-002
- 情報技術セキュリティ評価のためのコモンクライテリア パート 3:セキュリティ保証要件 バージョン 2.3 2005 年 8 月 CCIMB-2005-08-003
- Common Criteria for Information Technology Security Evaluation
  Part 1: Introduction and general model
  August 2005 Version 2.3 CCIMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation
  Part 2: Security functional requirements
  August 2005 Version 2.3 CCIMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation
  Part 3: Security assurance requirements
  August 2005 Version 2.3 CCIMB-2005-08-003
- ISO/IEC 15408:2005 Information Technology - Security - Techniques Evaluation Criteria for IT Security
- 補足-0512

1.5. 表記規則、用語、略語

1.5.1. 表記規則

第 3 章の前提条件、脅威、組織のセキュリティ方針、及び、第 4 章のセキュリティ対策方針では、それぞれのラベルを**ボールド体**フォントで記述し、続けてその定義を通常フォントで記述する。

1.5.2. 用語

本 ST で使用する用語を定義する。

■ アプリケーション

TOE で実行されるプロセスであり、1 つの実行単位。アプリケーションには、1 つ以上の業務ロジックを含むことができる。特に、TOE を導入する組織が作成した業務ロジックを含むアプリケーションを、ユーザアプリケーションと呼ぶ。

■ システム運用区画

入退室管理により物理的に保護された区画。

- ディレクトリサービス認証
  システム上に分散したサーバやサービス、ユーザ情報などのリソースに対して、そのリソースに関する位置や情報を返すディレクトリサービスを利用した認証方式。TOE では本認証方式ではなく、OS 認証を採用する。
- 配備
  アプリケーションをワークユニットに関連付ける操作。ワークユニットに対してアプリケーションを配備することにより、アプリケーションをワークユニット上で動作させることができる。
- 利用者
  TOE を導入する組織の者であり、アプリケーションの運用管理を行う者。
- ワークユニット
  アプリケーションが実行される実行環境の枠組。複数のアプリケーションを１つの業務として操作可能とする TOE 独自の管理に利用する。運用に必要な情報や業務ロジックを登録することで、ワークユニットに設定された実行環境下でアプリケーションを動作させることができる。また、ワークユニットに設定された実行環境の情報をワークユニット定義と呼ぶ。
- OTS
  オブジェクトトランザクションサービス。分散トランザクション機能を実現するサービス。

1.5.3. 略語

本 ST で使用する略語を定義する。

- CC ：Common Criteria
- CUI：Character-based User Interface
- EAL：Evaluation Assurance Level
- GUI：Graphical User Interface
- IT ：Information Technology
- OS ：Operating System
- PP ：Protection Profile
- SFP：Security Function Policy
- SOF：Strength Of Function
- ST ：Security Target
- TOE：Target Of Evaluation
- TSF：TOE Security Functions

2. TOE 記述

本章では、TOE 種別、TOE 概要、TOE 構成、TOE の機能、及び保護対象となる資産について記述する。

2.1. TOE 種別

TOE の種別は、アプリケーション実行の基盤となる動作環境を提供するアプリケーション基盤ソフトウェア製品である。

2.2. TOE 概要

2.2.1. TOE の利用目的

TOE はアプリケーションサーバプログラムであり、アプリケーション動作の基盤となる動作環境を提供する製品である。

TOE には、様々な環境で開発されたアプリケーションに対する動作環境を提供することが求められると同時に、インストールからアプリケーションの導入・運用・監視・保守に渡る運用管理の効率化を実現することも求められている。

そのため、本 TOE では、利用者に対して以下の環境を提供することを目的としている。

- アプリケーション安定稼動の基盤となる動作環境
- 導入から運用・監視・保守に渡ってアプリケーションの動作を容易に維持するための運用環境
- 既存のアプリケーションなど、様々な環境で開発されたアプリケーションを有効活用するための動作環境

2.2.2. TOE の利用環境

TOE は、利用者にアプリケーション動作の基盤となる動作環境とアプリケーション動作を維持するための運用環境を提供するため、アプリケーションサーバにインストールされる。

TOE が動作するアプリケーションサーバは、利用者組織内のシステム運用区画に設置され、利用者組織のネットワークに接続される。

TOE は、アプリケーション動作を維持するための運用管理を行うために Interstage 管理コンソールと呼ばれる Web ベースの操作ビューを提供している。TOE の利用環境として、Interstage 管理コンソールへのログイン時の識別認証処理を、TOE が動作するアプリケーションサーバの OS と連動して実施する OS 認証か、認証サーバと連動して実施するディレクトリサービス認証のどちらを採用するか設定する必要がある。本 TOE では、TOE の利用環境としてデフォルト設定である OS 認証を採用する。

TOEを利用して、アプリケーションを動作させ、アプリケーション動作の維持を行うためには、図 2.1 のような環境が必要となる。

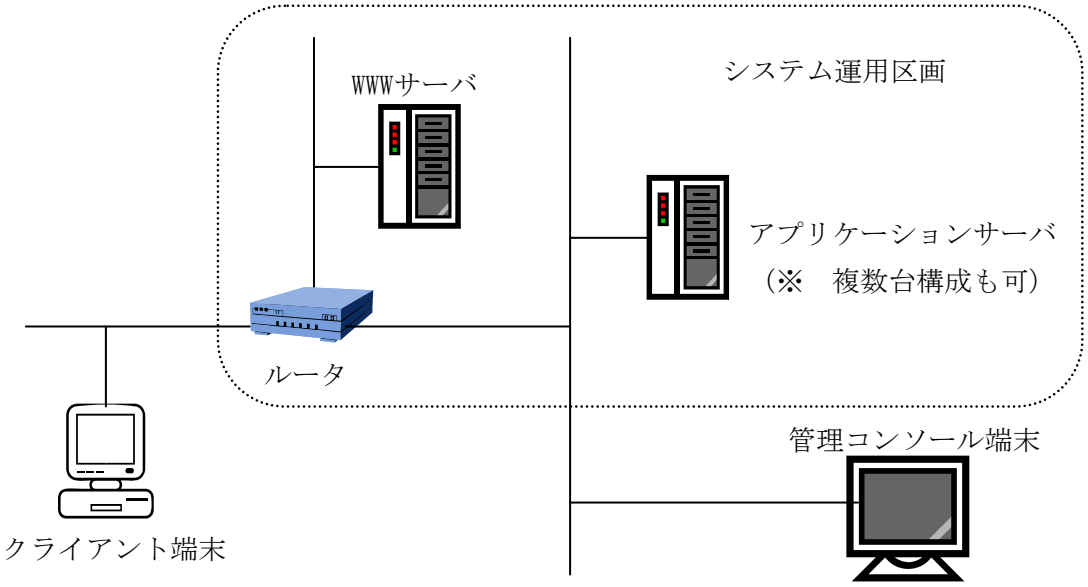


図 2.1 TOE の利用環境の例

- アプリケーションサーバ
  TOE が動作するアプリケーションサーバ。アプリケーションを実行させるための動作環境と、アプリケーション動作を維持するための運用環境を提供する。
- 管理コンソール端末
  TOE が提供するアプリケーション動作を維持するための運用環境を利用して、TOE 上のアプリケーション動作を管理するための端末。
- クライアント端末
  アプリ利用者がアプリケーションに対する実行要求を行うための端末。システム運用区画外に設置されている。クライアントソフトウェアを開発する場合、TOE のクライアントパッケージをインストールすることも可能。
- WWW サーバ
  クライアント端末向け WWW サーバ。クライアント端末による、アプリケーション利用に関するアクセスを受け付ける。

また、TOEの動作に必要なソフトウェアを 表 2.1 に示す。

表 2.1 TOE の運用に必要なソフトウェア

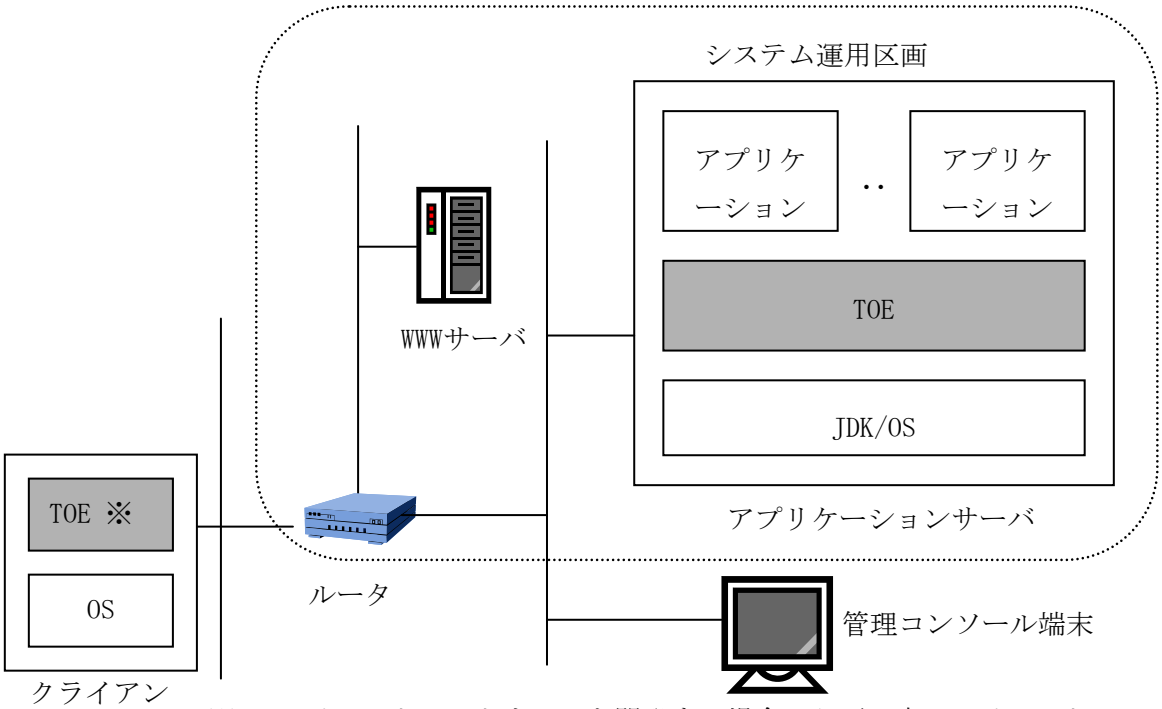
項番	ソフトウェア	備考
1	Linux OS	TOE が動作するアプリケーションサーバのオペレーティングシステム。Red Hat Enterprise Linux AS (v.4 for Itanium)に対応している。 Interstage 管理コンソールの利用の際に、TOE と連動してアクセス者の識別認証を行う。
2	ブラウザ	管理コンソール端末から TOE 上のアプリケーション動作を管理するために利用する。次のブラウザに対応している。 Microsoft Internet Explorer 5.0.1/5.5/6.0/7.0 Netscape Communicator 6.1x/6.2x/7.1x ただし、128 ビット以上の暗号への対応を必須とする。
3	Windows OS	クライアント端末に、TOE のクライアントパッケージを導入する場合に必要となるオペレーティングシステム。Windows Vista Home Basic/Home Premium/Ultimate/Business/Enterprise 、Windows XP Pro/Home、Windows 2000 Pro に対応している。
4	JDK	Java Development Kit。Java 言語によるプログラミングを行うための開発環境や Java プログラム実行環境が含まれる。JDK1.4 が TOE に同梱される形で提供され、TOE のインストール時に導入される。

2.2.3. TOE 構成

2.2.3.1.TOE の物理的範囲

TOE は、アプリケーションサーバ上で動作するソフトウェア製品 Interstage Application Server Enterprise Edition 8.0.3 であり、製品と TOE の物理範囲は同一である。なお、クライアントソフトウェアを開発する場合、必要に応じてクライアント端末にクライアントパッケージをインストールする。

図 2.2 にTOEの物理範囲を示す（TOEはハッチング部分）。



※ クライアントソフトウェアを開発する場合に必要に応じてインストール

図 2.2 TOE の物理範囲

2.2.3.2. TOE の論理的範囲

2.2.1 にて述べたように、TOEはアプリケーション動作の基盤となる動作環境と、アプリケーション動作を維持するための運用環境を提供する。

アプリケーションの動作環境、及び、運用環境としてTOEが提供する基本機能及びセキュリティ機能を 表 2.2 に示す。

表 2.2 TOE の機能

項番	機能	概要説明
1	業界標準・オープンソースに対応した実行環境	Web サービスや J2EE、CORBA 技術に対応した実行環境を、ライブラリ提供している。
2	Web サーバ機能	Web アプリケーションの動作環境として提供している。
3	トランザクション機能	オンライントランザクション処理を行う OLTP 機能や、複数のサーバにまたがってトランザクション処理を行う分散トランザクション機能を提供している。
4	ディレクトリサービス	アプリケーションが連携するための LDAP V3 準拠ディレクトリサーバを提供している。

5	非同期通信機能	メッセージキューを介したアプリケーション間の非同期通信をサポートしている。
6	ワークユニット定義に従ったアプリケーションの実行	アプリケーションの実行環境を設定したワークユニット定義に従って、アプリケーションを動作させる機能を提供している。
7	Interstage 管理コンソール	TOE が提供するサービスに対する操作ビューを統合し、一元的な操作ビューを提供している管理機能。アプリケーション動作の維持のため、サービスやシステム、アプリケーションの動作設定を管理することができる TOE の基本機能として提供される。
8	各種セキュリティ機能	アプリケーション実行状態の維持・管理のためにTOEが提供するセキュリティ機能。詳細は 2.4 に記載する。

なお、表 2.2 の項番 1 から 6 までの機能を総称してアプリケーション実行ライブラリと呼ぶ。アプリケーション実行ライブラリは、様々な環境で開発されたアプリケーションを動作させるための動作環境を実現する実行ライブラリであり、TOE上でユーザアプリケーションを動作させるための基盤として提供される。

また、クライアントパッケージは、ユーザが開発するクライアントアプリケーションのための開発環境やランタイムなどの、クライアントアプリケーション向けライブラリを提供するものであり、TOE のセキュリティ機能には無関係である。

2.2.4. ワークユニットを利用したアプリケーション動作の設定管理

TOE は、アプリケーションの動作設定を行うために、ワークユニットを利用した管理を行っている。ワークユニットを利用することで、アプリケーションの実行環境を自由な運用単位（同時に起動、停止を行うアプリケーションの実行環境）に分割でき、他のワークユニットからの影響を受けない個別の管理を行うことができる。

2.2.5. TOE の関連者

表 2.3 に、TOEの関連者とその権限を整理する。

表 2.3 TOE の関連者と権限

TOE の関連者	与えられる権限
Administrators	TOE に関する運用操作に対して全責任を負うため、Configurators の権限（[参照権限]、[運用操作権限]、[定義変更権限]）に加えて、以下の権限を有する。 Administrators の責任範囲：TOE 全体の運用管理

	[管理者権限] サービス/システムの構成変更（定義更新）/運用操作（起動/停止)。
Configurators	環境構築など、ワークユニットに関する環境構築に対して責任を負うため、以下の権限を有する。なお、Configurators は、アプリケーションに関係なく全てのワークユニットに対する管理責任を負っている。 Configurators の責任範囲：アプリケーション全体の運用管理
	[参照権限] アプリケーション/サービス/システムの構成と現在の状態を参照。各種ログ情報の参照。
	[運用操作権限] ワークユニットを利用したアプリケーションの運用操作（起動/停止/閉塞/閉塞解除/復元/再活性化)。アプリケーションが利用するリソースの運用操作。
	[定義変更権限] ワークユニットを利用したアプリケーションの定義変更（新規作成/構成変更/配備/配備解除)。アプリケーションが利用するリソースの新規作成/構成変更。
アプリ利用者	TOE が提供するワークユニットに配備されたユーザアプリケーションを利用する者。 TOE を間接的に利用する者であり、TOE に対する操作権限はない。
アプリ開発者	TOE 上で動作させるアプリケーションを開発する者。 TOE を間接的に利用する者であり、TOE に対する操作権限はない。
システム責任者	利用者へロールの任命を行う。 TOE に対する操作権限はない。

なお、Administrators は TOE が動作するアプリケーションサーバの OS の管理者の権限も兼ねている。

2.2.6. TOE の利用方法

TOE を利用してアプリケーションを動作させるには、動作環境に対する管理を行い、アプリケーションが TOE 上で動作するために必要な環境を設定する必要がある。

TOE を利用して動作環境を管理するには、管理コンソール端末から Interstage 管理コンソールへのログイン操作を行う。Interstage 管理コンソールへのログイン時の識別認証処理は TOE が動作するアプリケーションサーバの OS と連動して実施される。

TOE が動作するアプリケーションサーバの OS に登録されたアカウントには、その権限に応じて Administrators または Configurators いずれかのロールが付与される。

表 2.4 に、各ロールがTOEを利用する方法を整理する。

表 2.4 TOE の利用方法

ロール	利用方法
Administrators	TOE が動作するアプリケーションサーバの OS の管理者アカウントとして、管理コンソール端末上のブラウザから Interstage 管理コンソールにアクセスする。識別認証により Administrators 権限を有する者であることが確認された後、TOE を利用することができる。
Configurators	TOE が動作するアプリケーションサーバの OS の一般ユーザアカウントとして、管理コンソール端末上のブラウザから Interstage 管理コンソールにアクセスする。識別認証により Configurators 権限を有する者であることが確認された後、TOE を利用することができる。

また、Interstage 管理コンソールを利用した GUI ベースの利用の他に、OS 上からのコマンド実行による CUI ベースの利用も可能である。ただし、コマンドによる管理を行う際には、事前に TOE が動作するサーバの OS に対して、管理者アカウントまたは一般ユーザアカウントとしてログインしておく必要がある。そのため、コマンド実行による TOE 管理は OS によって制御される操作であり、TOE の制御範囲外からの操作となる。

以降、Administrators 及び Configurators の総称を操作者と表現する。

2.3. TOE 環境にて扱う資源

TOE が動作するアプリケーションサーバには、TOE 上でアプリケーションを動作・維持するために必要な資源が存在している。TOE 環境にて扱う資源は、その目的や管理元によって以下に分類することができる。

- アプリケーション実行環境
  ワークユニットとして管理される、個々のアプリケーションに対する動作環境の設定ファイル。ワークユニットの設定変更は、ワークユニットに関連付けられたアプリケーションのみに影響する。
  TOE 上で動作する個々のアプリケーション動作の維持に関係する設定であり、Configurators が管理責任を負う。

- 環境定義ファイル
  個々のユーザ環境において、アプリケーション実行環境をどのようなシステム環境で利用するか規定する設定ファイル。システム環境の設定変更は、TOE 上で動作する

全てのアプリケーションに影響する。
TOE 上で動作する全てのアプリケーション動作の維持に関係するシステム設定であり、Administrators が管理責任を負う。

・ アプリケーション実行プロセス
アプリケーション実行環境や環境定義ファイルに定義された設定に従って、アプリケーションを実行させる実行プロセス。アプリケーション実行プロセスが停止した場合、実行プロセスが動作させていたアプリケーションも停止することになる。
TOE 上で動作する個々のアプリケーション動作の維持に関係する資源であり、TOE が管理責任を負う。

・ アプリケーション
TOE 上で動作させるアプリケーションファイル。TOE からは OS 上の実行ファイルにしか見えないため、OS 機能を利用して管理される資源である。
・ アプリケーション実行資源
アプリケーションが各々の処理の中で扱うデータや、連携する他製品の環境定義ファイルなど。TOE 上で動作するアプリケーションが、その処理の過程で扱う資源であり、TOE からは OS 上のデータにしか見えないため、OS 機能や他製品機能を利用して管理される資源である。

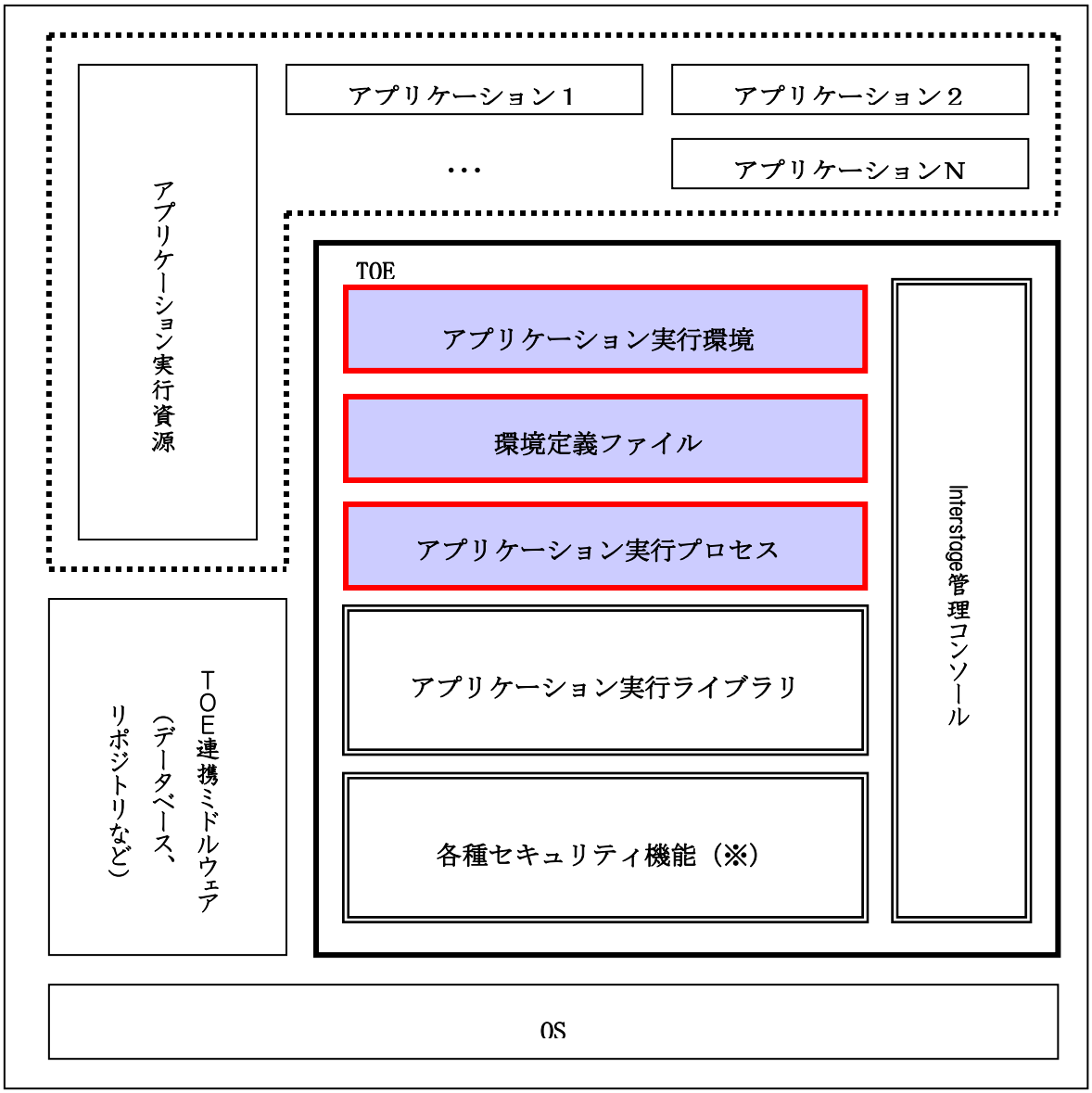
表 2.5 にTOE環境において扱う資源とその管理責任元を整理する。

表 2.5 TOE 環境で扱う資源

資源種別	資源	管理責任元
アプリケーション実行環境	・ ワークユニット定義 ・ IJServer 環境用定義ファイル ・ IJServer 用ログファイル	TOE(Configurators)
環境定義ファイル	・ Interstage HTTP Server 環境定義ファイル ・ Interstage HTTP Server 用ログファイル ・ CORBA サービス用ログファイル ・ インプリメンテーションリポジトリファイル ・ エラーログファイル ・ ネーミングサービス用データファイル ・ インタフェースリポジトリ用データファイル ・ Interstage 関連の定義 ・ OTS システム情報格納フォルダ	TOE (Administrators)

	・ トランザクションログファイル ・ トレースログ格納フォルダ ・ リソース定義格納リポジトリ ・ リソースアクセス情報 ・ RMP プロパティファイル	
アプリケーション実行プロセス	・ アプリケーション実行プロセス	TOE
アプリケーション	・ EAR、WAR、JAR、RAR ファイル	OS
アプリケーション実行資源	・ J2EE アプリケーションが認証に利用するユーザ ID とパスワード ・ データベース連携サービス用データベース内のログ ・ データベース連携サービス用データベース内のデータ ・ XA 連携用プログラム ・ OTS 用リソース管理プログラム ・ CORBA ワークユニット用出力ファイル ・ J2EE アプリケーションや Interstage HTTP Server が利用するリポジトリの格納情報 ・ J2EE アプリケーションや Interstage HTTP Server が利用するリポジトリ環境定義ファイル ・ J2EE アプリケーションのセションリカバリ用永続化ファイル	OS TOE 連携ミドルウェア

上記にて整理した資源と管理責任元との関係を 図 2.3 に示す。



※　TOEのセキュリティ機能については 2.4 にて記載する。

図 2.3 TOE 環境で扱う資源とその管理元

2.4. TOE のセキュリティ機能

TOE は、アプリケーション実行環境、環境定義ファイル、及び、アプリケーション実行プロセスの管理を安全に実施するために、以下のセキュリティ機能を提供する。

■ ユーザ認証機能

TOE が動作するアプリケーションサーバの OS と連動して、Interstage 管理コンソールを使用した TOE へのアクセス時にアクセス者が TOE の操作者であることを識別し、本人であることを認証する機能。

■ SSL 暗号通信機能

Interstage 管理コンソールを使用した TOE へのアクセス時、管理コンソール端末と Interstage 管理コンソール間の通信データの暗号化を行う機能。

なお、本機能では以下の暗号鍵を利用する。

◇ サーバ・ライト鍵　　：TOE が管理コンソール端末へ送信する通信データの暗号化操作に利用する。

◇ クライアント・ライト鍵：TOE が管理コンソール端末から受信する通信データの復号操作に利用する。

■ セションタイムアウト機能

Interstage 管理コンソールを使用した TOE の運用管理時、一定の無操作時間が経過した際に、Interstage 管理コンソールと管理コンソール端末の間のセションを破棄する機能。

■ ロール制御機能

Interstage 管理コンソールを使用した TOE の運用管理時、サービスやシステム設定に関する環境定義ファイルへの操作の実行可否を操作者のロールによって判断し、制御する機能。

■ アプリケーション自動再起動機能

停止操作以外によって終了したアプリケーションを異常終了と見なし、警告メッセージを TOE が動作するアプリケーションサーバの OS へ通知し、当該アプリケーションの実行プロセスを再起動する機能。アプリケーション動作の維持のため、動作障害状態からの早期復帰を担う。利用者がワークユニット定義に設定したアプリケーションを再起動の対象とする。

■ サーバアプリケーションタイマ機能

一定の応答時間内に応答しなかったアプリケーションを処理遅延と見なし、警告メッセージを TOE が動作するアプリケーションサーバの OS へ通知し、当該アプリケーションを強制的に停止させる機能。アプリケーション自動再起動機能を利用することで、

強制停止したアプリケーションを再起動することができる。利用者がワークユニット定義に設定したアプリケーションを強制停止の対象とする。

2.5. 保護対象となる資産

図 2.3 に示したように、アプリケーション実行環境、環境定義ファイル、及び、アプリケーション実行プロセスがTOEの管理する資源であり、これらを保護対象資産とする。

・ アプリケーション実行環境

〔保護対象資産とする理由〕〕

アプリケーション実行環境は個々のアプリケーションに対する動作環境の設定ファイルであり、設定を不正に変更されることは、その設定に従って動作するアプリケーションの停止や動作変更を意味し、アプリケーション動作を維持できないことになるため。

・ 環境定義ファイル

〔保護対象資産とする理由〕

環境定義ファイルは個々のユーザ環境におけるシステム環境を規定する設定ファイルであり、設定を不正に変更されることは、その設定に従って動作する TOE の停止や動作変更を意味し、TOE 上で動作するアプリケーション動作を維持できないことになるため。

・ アプリケーション実行プロセス

〔保護対象資産とする理由〕

アプリケーション実行プロセスはアプリケーションの動作そのものを意味するため、アプリケーション実行プロセスが異常終了したり、処理遅延状態に陥ることは、TOE 上で動作するアプリケーションの動作を維持できないことになるため。

また、2.3 でも述べたように、TOEではアプリケーションやアプリケーション実行資源といったOS上の資源として管理される資源は、アプリケーションの動作に必要な資源ではあるが、TOEが管理することはできない。これらの資源については、OS機能や連携する他製品の機能を利用して管理を実施することが必要である。

なお、Interstage 管理コンソールを使用してアプリケーション実行環境や環境定義ファイルの運用管理を行うためには、Interstage 管理コンソールへのログインが必要となる。ログイン時には、識別認証情報（アカウント情報とパスワード）がネットワーク上を流れることになる。そのため、OS によって管理される資源ではあるが、ログイン時にネットワーク上を流れる識別認証情報は保護の対象とする。

3. TOE セキュリティ環境

本章では、前提条件、脅威、組織のセキュリティ方針について記述する。

3.1. 前提条件

- **A.TRUST**

  Administrators は、ロールに課せられた職務に関して責任を持ち、不正な行為を行わないものとする。

- **A.PHYSICAL_ACCESS**

  TOE が動作するアプリケーションサーバは、信頼出来ない者の立入りが禁止されたシステム運用区画へ設置されるものとする。

- **A.SERVICE**

  TOE が動作するアプリケーションサーバでは、OS へのリモートログインサービスは提供せず､保守時を除いてコマンド実行による CUI ベースの運用を行わないものとする。

- **A.APPLICATION**

  TOE 上で動作するアプリケーションは信頼できるものとする。

3.2. 脅威

本 TOE では、攻撃者の攻撃能力を低レベルと想定する。

- **T.ILLEGAL_ACCESS**（不正なログイン）

  攻撃者が、管理コンソール端末もしくは、クライアント端末を利用して Interstage 管理コンソールへ不正にアクセスし、アプリケーション実行環境や環境定義ファイルの設定変更を行い､TOE や動作しているアプリケーションの停止や設定変更を試みる。

- **T.SPOOFING**（なりすまし）

  Interstage 管理コンソールへの不正なログインを防ぐために識別認証の対策を実施した際にその二次脅威として、攻撃者が、操作者がログイン状態のまま離席した管理コンソール端末を使用して、Interstage 管理コンソールに無断にアクセスし、アプリケーション実行環境や環境定義ファイルの設定変更を行い、TOE や動作しているアプリケーションの停止や設定変更を試みる。

■ T.DISCLOSE_DATA(管理コンソール端末－Interstage 管理コンソール間のデータ暴露)
Interstage 管理コンソールへの不正なログインを防ぐために識別認証の対策を実施した際にその二次脅威として、攻撃者が、管理コンソール端末と Interstage 管理コンソール間のネットワーク上で送受信される通信データを盗聴し、識別認証情報を入手する。入手した識別認証情報を使用して、操作者として Interstage 管理コンソールを使用してアプリケーション実行環境や環境定義ファイルの設定変更を行い、TOE や動作しているアプリケーションの停止や設定変更を試みる。

■ T.ARROGATION（越権行為）
Administrators のロールを持たない者が、管理コンソール端末を利用して、Interstage 管理コンソールへアクセスし、サービスやシステム設定に関する環境定義ファイルの設定変更を行い、TOE や動作しているサービス、またはシステムの停止、設定変更を試みる。

■ T.APPLICATION_TROUBLE（アプリケーション動作障害）
TOE 上で動作するアプリケーションが停止操作以外の原因によって異常終了する、もしくは、アプリケーション処理遅延のためレスポンスが遅延することによって、利用者が設定したアプリケーション動作を維持できなくなる。

3.3. 組織のセキュリティ方針

TOE が従わなければならない組織のセキュリティ方針はない。

4. セキュリティ対策方針

本章では、TOE のセキュリティ対策方針、環境のセキュリティ対策方針について記述する。

4.1. TOE のセキュリティ対策方針

本節は、脅威に対抗するための TOE のセキュリティ対策方針を示す。

- **O.ID_AUTH**

  TOE は、OS による Interstage 管理コンソールに対するアクセス者の識別認証実施時に、アクセス者が入力したパスワードを外部に漏らさないように保護する。

- **O.CRYPTO**

  TOE は、管理コンソール端末と Interstage 管理コンソール間の通信路上のデータを暴露から保護する。

- **O.SESSION**

  TOE は、管理コンソール端末から Interstage 管理コンソールへの運用管理操作が管理された一定時間に渡って何も行われなかった場合、管理コンソール端末と Interstage 管理コンソールの間のセションを切断する。

- **O.ROLE_MANAGE**

  TOE は、Interstage 管理コンソールを利用したサービスやシステム設定に関する環境定義ファイルへの操作要求時に、操作者のロールを確認し、Administrators のロールを持つ者のみに操作実行を許可する。

- **O.APPLICATION_TROUBLE**

  TOE は、TOE 上で動作するアプリケーションの停止操作以外の原因による異常終了時、及び、アプリケーション処理遅延のためのレスポンス遅延発生時に、ワークユニット定義に従ったアプリケーションの実行を維持する。

4.2. 環境のセキュリティ対策方針

本節は、前提条件を満足し、脅威及び組織のセキュリティ方針に対する TOE セキュリティ対策方針を支援するための環境のセキュリティ対策方針を示す。

- **OE.ID_AUTH**

  TOE が動作するアプリケーションサーバの OS は、アクセス者による Interstage 管理コンソールへのアクセス時に、アクセス者が TOE の操作者であることを識別し、本人であることを認証する。

- **OE.APPLICATION**

  Administrators 及び Configurators は、作成元が特定でき、動作確認が完了したアプリケーションのみを TOE 上で動作させる。

- **OE.TRUST**

  システム責任者は、Administrators を任命する際に、ロールを付与する者に、Administrators に課せられた職務を理解させることに責任を持つ。

- **OE.PHYSICAL_ACCESS**

  Administrators は、信頼出来ない者の立入りが禁止されたシステム運用区画に TOE が動作する機器を設置する。

- **OE.SERVICE**

  Administrators は、TOE が動作するアプリケーションサーバにおいて、OS へのリモートログインを提供するサービスの停止を行う。また、Administrators 及び Configurators は、保守時を除き、必ず Interstage 管理コンソールの画面から TOE の操作を行う。

- **OE.PASSWORD_MANAGE**

  Administrators 及び Configurators は、Interstage 管理コンソールへのログイン時に使用するパスワードとして、8 桁以上の数字、英字、特殊文字からなる容易に推測できない不規則な文字列を設定する。パスワードの管理は、パスワードの所有者のみが行い、定期的にパスワードの変更を行う。

■ OE.USER_MANAGE

TOE が動作するアプリケーションサーバの OS の管理者は、TOE が動作するアプリケーションサーバの OS へのユーザ登録を、TOE の運用を行う必要のある者のみに制限し、それ以外の者は登録しない。

5. IT セキュリティ要件

本章では、TOE セキュリティ要件、IT 環境に対するセキュリティ要件、セキュリティ機能強度を示す。

5.1. TOE セキュリティ要件

本節では、TOE が満たさなければならないセキュリティ要件を示す。

5.1.1. TOE セキュリティ機能要件

FCS_CKM.1 暗号鍵生成

下位階層: なし

FCS_CKM.1.1

TSF は、以下の[割付: *標準のリスト*]に合致する、指定された暗号鍵生成アルゴリズム[割付: *暗号鍵生成アルゴリズム*]と指定された暗号鍵長[割付: *暗号鍵長*]に従って、暗号鍵を生成しなければならない。

[割付: *標準のリスト*]
表 5.1 に示す

[割付: *暗号鍵生成アルゴリズム*]
表 5.1 に示す

[割付: *暗号鍵長*]
表 5.1 に示す

表 5.1 暗号鍵と生成アルゴリズム

鍵の種類	標準	暗号鍵生成アルゴリズム	暗号鍵長
サーバ・ライト鍵	富士通独自	乱数生成	128bit、168bit、256bit
	FIPS PUB 180-2	SHA-1	
	RFC1321	MD5	
クライアント・ライト鍵	富士通独自	乱数生成	128bit、168bit、256bit
	FIPS PUB 180-2	SHA-1	
	RFC1321	MD5	

依存性: [FCS_CKM.2 暗号鍵配付
または
FCS_COP.1 暗号操作]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

FCS_COP.1 暗号操作

下位階層: なし

FCS_COP.1.1

TSF は、[割付: *標準のリスト*]に合致する、特定された暗号アルゴリズム[割付: *暗号アルゴリズム*]と暗号鍵長[割付: *暗号鍵長*]に従って、[割付: *暗号操作のリスト*]を実行しなければならない。

[割付: *標準のリスト*]
表 5.2 に示す

[割付: *暗号アルゴリズム*]
表 5.2 に示す

[割付: *暗号鍵長*]
表 5.2 に示す

[割付: *暗号操作のリスト*]
表 5.2 に示す

表 5.2 暗号アルゴリズムと暗号操作

鍵の種類	標準	暗号アルゴリズム	暗号鍵長	暗号操作
サーバ・ライト鍵	FIPS PUB 46-3	3DES	168bit	Interstage 管理コンソールから管理コンソール端末へ送信する通信データの暗号化操作
	ISO/IEC9979	RC4	128bit	
	FIPS PUB 197	AES	128bit、256bit	
クライアント・ライト鍵	FIPS PUB 46-3	3DES	168bit	Interstage 管理コンソールが管理コンソール端末から受信する通信データの復号操作
	ISO/IEC9979	RC4	128bit	
	FIPS PUB 197	AES	128bit、256bit	

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート
または

FDP_ITC.2 セキュリティ属性付き利用者データのインポート
または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

FDP_ACC.1 サブセットアクセス制御

下位階層: なし

FDP_ACC.1.1

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

[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]
＜サブジェクト＞
・ 操作者を代行するプロセス

＜オブジェクト＞
・ 環境定義ファイル

＜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＞
・ 変更
・ 参照

[割付: *アクセス制御 SFP*]
Interstage 管理コンソールアクセス制御 SFP

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACF.1 セキュリティ属性によるアクセス制御

下位階層: なし

FDP_ACF.1.1

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

[割付: *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*]
表 5.3 及び 表 5.4 に示す。

表 5.3 サブジェクトとセキュリティ属性

サブジェクト	SFP 関連セキュリティ属性	SFP 関連セキュリティ属性の名前付けされたグループ
操作者を代行するプロセス	ロール識別情報（Administrators または Configurators）	なし

表 5.4 オブジェクトとセキュリティ属性

オブジェクト	SFP 関連セキュリティ属性	SFP 関連セキュリティ属性の名前付けされたグループ
環境定義ファイル	権限リスト	なし

[割付: *アクセス制御 SFP*]
Interstage 管理コンソールアクセス制御 SFP

FDP_ACF.1.2

TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、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*]
権限リストに従って、サブジェクトに関連付けられたロール識別情報がAdministratorsである場合、サブジェクトによるオブジェクトに対する変更操作及び参照操作を許可する。
サブジェクトに関連付けられたロール識別情報がConfiguratorsである場合、サブジェクトによるオブジェクトに対する変更操作を拒否し、参照操作を許可する。

FDP_ACF.1.3

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に対するサブジェクトの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に対するサブジェクトのアクセスを明示的に承認する規則*]
なし

FDP_ACF.1.4

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

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

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

FIA_ATD.1 利用者属性定義

下位階層: なし

FIA_ATD.1.1

TSF は、個々の利用者に属する以下のセキュリティ属性のリスト[割付:*セキュリティ属性のリスト*]を維持しなければならない。

[割付:*セキュリティ属性のリスト*]
ロール識別情報

依存性: なし

FIA_UAU.7 保護された認証フィードバック

下位階層: なし

FIA_UAU.7.1

TSFは、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*]
入力された文字数分のダミー文字（●）

依存性: FIA_UAU.1 認証のタイミング

FIA_USB.1 利用者・サブジェクト結合

下位階層: なし

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

[割付: 利用者セキュリティ属性のリスト]
ロール識別情報

FIA_USB.1.2 TSFは、利用者を代行して動作するサブジェクトと利用者セキュリティ属性の最初の関連付けに関する次の規則を実施しなければならない:[割付: 属性の最初の関連付けに関する規則]

[割付: 属性の最初の関連付けに関する規則]
なし

FIA_USB.1.3 TSFは、利用者を代行して動作するサブジェクトに関連付けた利用者セキュリティ属性の変更管理に関する次の規則を実施しなければならない:[割付: 属性の変更に関する規則]

[割付: 属性の変更に関する規則]
なし

依存性: FIA_ATD.1 利用者属性定義

FMT_MSA.3 静的属性初期化

下位階層: なし

FMT_MSA.3.1

TSF は、その SFP を実施するために使われるセキュリティ属性として、[選択: *制限的、許可的* : *から一つのみ選択*、[割付 : *その他の特性*]]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* : *から一つのみ選択*、[割付 : *その他の特性*]]
その他の特性

[割付 : *その他の特性*]
表 5.5 に示す。

表 5.5 オブジェクトに関連付けられるセキュリティ属性

オブジェクト	セキュリティ属性（権限リスト）	
	Administrators	Configurators
環境定義ファイル	変更 参照	参照

[割付: *アクセス制御 SFP、情報フロー制御 SFP*]
Interstage 管理コンソールアクセス制御 SFP

FMT_MSA.3.2

TSF は、オブジェクトや情報が生成されるとき、[割付: *許可された識別された役割*]が、デフォルト値を上書きする代替の初期値を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

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_MTD.1 TSF データの管理

下位階層: なし

FMT_MTD.1.1

TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、*消去*、[割付: *その他の操作*]]する能力を[割付:*許可された識別された役割*]に制限しなければならない。

[割付: *TSF データのリスト*]

- ワークユニット定義（リトライカウント）
- ワークユニット定義（リトライカウントリセット時間）
- ワークユニット定義（アプリケーション自動再起動失敗時の制御）
- ワークユニット定義（アプリケーション最大処理時間）
- ワークユニット定義（アプリケーション最大処理時間超過時の制御）

[選択: *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、*消去*、[割付: *その他の操作*]]

問い合わせ、改変

[割付: *その他の操作*]

なし

[割付:*許可された識別された役割*]

- Administrators
- Configurators

依存性: FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

FMT_SMF.1 管理機能の特定

下位階層： 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*]

表 5.6に示す

表 5.6 セキュリティ管理機能のリスト

セキュリティ機能要件	管理要件	管理項目
FCS_CKM.1	暗号鍵属性の変更の管理	なし（管理対象となる暗号鍵属性が存在しないため）
FCS_COP.1	なし	なし
FDP_ACC.1	なし	なし
FDP_ACF.1	明示的なアクセスまたは拒否に基づく決定に使われる属性の管理	なし（明示的なアクセスまたは拒否を決定する規則はない）
FIA_ATD.1	利用者に対する追加のセキュリティ属性の定義	なし（ロール識別情報以外にセキュリティ属性が存在しないため）
FIA_UAU.7	なし	なし
FIA_USB.1	デフォルトのサブジェクトのセキュリティ属性の定義	なし（セキュリティ属性の定義を許可したロールは存在しないため）
	デフォルトのサブジェクトのセキュリティ属性の変更	なし（セキュリティ属性の変更を許可したロールは存在しないため）
FMT_MSA.3	初期値を特定できる役割のグループの管理 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定の管理	なし（Interstage 管理コンソールアクセス制御 SFP のデフォルト値の設定は固定であり、初期値を特定できる役割のグループは存在しないため）
FMT_MTD.1	TSF データと相互に影響を及ぼし	なし（グループの管理は IT 環境で

	得る役割のグループの管理	ある OS の機能を利用して行うため、TOE による管理対象としない)
FMT_SMF.1	なし	なし
FMT_SMR.1	役割の一部をなす利用者のグループの管理	なし（役割の一部をなす利用者のグループは固定であり、管理対象とならない)
FPT_RVM.1	なし	なし
FPT_SEP.1	なし	なし
FRU_FLT.1	なし	ワークユニット定義の管理（アプリケーション自動再起動の対象にするか否かの管理、サーバアプリケーションタイマの対象にするか否か及び最大処理時間の管理)
FTA_SSL.3	個々の利用者に対し対話セションの終了を生じさせる利用者が非アクティブである時間の特定	なし（個々の利用者に対する個別の設定は行えない)
	対話セションの終了を生じさせる利用者が非アクティブであるデフォルト時間の特定	なし(時間設定は IT 環境である OS の機能を利用して行うため、TOE による管理対象としない)
FTP_TRP.1	もしサポートされていれば、高信頼パスを要求するアクションの設定。	なし（高信頼パスを要求するアクションは固定であり、管理対象とならない)

依存性： なし

FMT_SMR.1 セキュリティ役割

下位階層: なし

FMT_SMR.1.1

TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。

[割付: *許可された識別された役割*]

- Administrators
- Configurators

FMT_SMR.1.2

TSF は、利用者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

FPT_RVM.1 TSP の非バイパス性

下位階層: 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。

依存性: なし

FPT_SEP.1 TSF ドメイン分離

下位階層: 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。

依存性: なし

FRU_FLT.1 機能削減された耐障害性

下位階層: なし

FRU_FLT.1.1

TSFは、以下の障害[割付: *障害の種別のリスト*]が生じたとき、[割付: *TOE機能（capabilities）のリスト*]の動作を保証しなければならない。

[割付: *障害の種別のリスト*]

- アプリケーション実行プロセスの異常終了（アプリケーション実行プロセスが停止操作以外の原因で停止した状態）
- アプリケーションの処理遅延（アプリケーションの処理は開始しているが、規定の時間内に処理を完了していない状態）

[割付: *TOE機能（capabilities）のリスト*]

ワークユニット定義に従ったアプリケーションの実行

依存性: FPT_FLS.1　セキュアな状態を保持する障害

FTA_SSL.3 TSF 起動による終了

下位階層: なし

FTA_SSL.3.1

TSFは、[割付: *利用者が非アクティブである時間間隔*]後に対話セションを終了しなければならない。

[割付: *利用者が非アクティブである時間間隔*]
Administratorsが設定した時間間隔

依存性: なし

FTP_TRP.1 高信頼パス

下位階層: なし

FTP_TRP.1.1

TSFは、それ自身と[選択: *リモート*、*ローカル*]利用者間に、他の通信パスと論理的に区別され、その端点の保証された識別及び改変や暴露からの通信データの保護を提供する通信パスを提供しなければならない。

[選択: *リモート*、*ローカル*]
リモート

FTP_TRP.1.2

TSFは、[選択: *TSF*、*ローカル利用者*、*リモート利用者*]が、高信頼パスを介して通信を開始することを許可しなければならない。

[選択: *TSF*、*ローカル利用者*、*リモート利用者*]
リモート利用者

FTP_TRP.1.3

TSFは、[選択: *最初の利用者認証*、[割付: *高信頼パスが要求される他のサービス*]]に対して、高信頼パスの使用を要求しなければならない。

[選択: *最初の利用者認証*、[割付: *高信頼パスが要求される他のサービス*]]
[割付: *高信頼パスが要求される他のサービス*]

[割付: *高信頼パスが要求される他のサービス*]
Interstage管理コンソール

依存性: なし

5.1.2. TOE セキュリティ保証要件

本ST にて要求する、TOEに対する保証レベルはEAL2+である。追加する保証コンポーネントはAVA_MSU.1 である。TOEに対する保証コンポーネント構成を 表 5.7 に示す。

要求する各保証コンポーネントの保証エレメントは、CC Part3 の要求通りである。

なお、ASE クラスは、保証レベルに関わらず必須となる保証要件として採用する。

表 5.7 TOE の保証要件コンポーネント一覧

TOE セキュリティ保証要件		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_HLD.1
	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	誤使用	AVA_MSU.1
	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 環境に対するセキュリティ要件

本節では、IT 環境が満たさなければならないセキュリティ要件を示す。

FIA_UAU.2 アクション前の利用者認証

下位階層： FIA_UAU.1

FIA_UAU.2.1

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。

※　下線部は詳細化操作を示す

依存性： FIA_UID.1 識別のタイミング

FIA_UID.2 アクション前の利用者識別

下位階層： FIA_UID.1

FIA_UID.2.1

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。

※　下線部は詳細化操作を示す

依存性： なし

5.3. セキュリティ機能強度

TOE セキュリティ機能要件に対する最小機能強度は、SOF-基本である。明示された機能強度が適用される特定の TOE セキュリティ機能要件は FCS_CKM.1 及び FCS_COP.1 であり、機能強度は SOF-基本である。

6. TOE 要約仕様

本章では、TOE セキュリティ機能を記述する。

6.1. TOE セキュリティ機能

本節では、TOEのセキュリティ機能を説明する。各機能に対応するTOEセキュリティ機能要件が示されているように、本節で説明するセキュリティ機能は、5.1.1.TOEセキュリティ機能要件で記述したTOEセキュリティ機能要件を満たす。

6.1.1. ユーザ認証機能 (SF.ID_AUTH)

ユーザ認証機能は、管理コンソール端末を利用した Interstage 管理コンソールへのアクセス時に、アクセス者より入力された識別認証情報を TOE が動作するアプリケーションサーバの OS へ渡し、識別認証実施の依頼を行う。

アクセス者より入力されたパスワードのフィードバック情報として、入力された文字数分のダミー文字（●）を表示する。

IT 環境である OS によって、アクセス者が TOE の操作者であることを識別し、本人であることが認証された場合、TOE は、アクセス者にロール識別情報を付与し、Interstage 管理コンソールの機能の利用を許可する。ロール識別情報は、操作者の操作実行可否の制御やワークユニット定義の管理を行うために必要なロール (Administrators、 Configurators) を識別する情報であり、TOE が維持している。また、識別認証が不成功となった場合には、TOE はアクセス者による Interstage 管理コンソールの機能利用を許可しない。なお、IT 環境によって識別認証されたアクセス者による Interstage 管理コンソールの利用は、アクセス者がログアウトする、もしくは、後述のセションタイムアウト機能によりセションが切断されるまで許可される。

ユーザ認証機能は、管理コンソール端末を利用した Interstage 管理コンソールへのアクセス時に必ず呼び出される機能であり、信頼できないアクセス者による干渉と改ざんから自身を保護する機能である。

対応する TOE セキュリティ機能要件：FIA_ATD.1、FIA_UAU.7、FIA_USB.1、FMT_SMR.1、FPT_RVM.1、FPT_SEP.1

6.1.2. SSL 暗号通信機能 (SF.CRYPTO)

SSL 暗号通信機能は、SSL/TLS プロトコルに従って、管理コンソール端末から Interstage 管理コンソール間の全ての通信データの暗号化処理を行う。

TOE は、管理コンソール端末から Interstage 管理コンソールへのコネクションを確立す

る度、

1) 表 6.1 に識別された暗号鍵を生成する３つのアルゴリズムを組み合わせて、 所定の暗号鍵長を持つサーバ・ライト鍵及びクライアント・ライト鍵を生成する

表 6.1 暗号鍵生成アルゴリズム

鍵の種類	標準	暗号鍵生成アルゴリズム	暗号鍵長
サーバ・ライト鍵	富士通独自	乱数生成	128bit、168bit、256bit
	FIPS PUB 180-2	SHA-1	
	RFC1321	MD5	
クライアント・ライト鍵	富士通独自	乱数生成	128bit、168bit、256bit
	FIPS PUB 180-2	SHA-1	
	RFC1321	MD5	

なお、TOE と管理コンソール端末の間における暗号鍵の共有は、SSL/TLS プロトコルに従って実施される。

2) 表 6.2 に識別された暗号処理を行うアルゴリズムと暗号鍵を用いて､管理コンソール端末との間で送受信する通信データの暗号化操作と復号操作を行う

表 6.2 暗号アルゴリズム

鍵の種類	標準	暗号アルゴリズム	暗号鍵長	暗号操作
サーバ・ライト鍵	FIPS PUB 46-3	3DES	168bit	Interstage 管理コンソールから管理コンソール端末へ送信する通信データの暗号化操作
	ISO/IEC9979	RC4	128bit	
	FIPS PUB 197	AES	128bit、256bit	
クライアント・ライト鍵	FIPS PUB 46-3	3DES	168bit	Interstage 管理コンソールが管理コンソール端末から受信する通信データの復号操作
	ISO/IEC9979	RC4	128bit	
	FIPS PUB 197	AES	128bit、256bit	

なお、SSL 暗号通信機能において、どの暗号方式を選択するかは、管理コンソール端末から Interstage 管理コンソールへのコネクション確立時に決定される。管理コンソール端末と Interstage 管理コンソールの両者が利用可能な暗号方式から、一番強度がある暗号方式が選択される。

SSL 暗号通信機能は、管理コンソール端末と Interstage 管理コンソールとの間で通信が行われる際に必ず呼び出される機能であり、外部からの干渉と改ざんから自身を保護する

機能である。

対応する TOE セキュリティ機能要件：FCS_CKM.1、FCS_COP.1、FPT_RVM.1、FPT_SEP.1、FTP_TRP.1

6.1.3. セションタイムアウト機能（SF.SESSION）

操作者が管理コンソール端末を介して Interstage 管理コンソールへログインした際に、管理コンソール端末と Interstage 管理コンソールの間にセションが確立される。

セション管理機能は、確立されたセションの状態を管理し、操作者による無操作時間が、Administrators が設定した時間に達した場合に、管理コンソール端末とのセションを強制的に切断し、セションを終了させる。

Administrators によってタイムアウト時間が設定されなかった場合、デフォルト値の 30 分に設定される。

セションタイムアウト機能は、管理コンソール端末と Interstage 管理コンソールとの間でセションが確立した際に必ず呼び出される機能であり、外部からの干渉と改ざんから自身を保護する機能である。

対応する TOE セキュリティ機能要件：FPT_RVM.1、FPT_SEP.1、FTA_SSL.3

6.1.4. ロール制御機能（SF.ROLE_MANAGE）

ロール制御機能は、Interstage 管理コンソールを使用した TOE の運用管理時、サービスやシステム設定に関する環境定義ファイルへの操作の実行可否を操作者のロールと権限リストによって判断し、制御する。なお、制御の規則となる権限リストの変更は禁止されている。

操作者のロールが Administrators である場合、変更操作と参照操作を許可する。

操作者のロールが Configurators である場合、変更操作を拒否し、参照操作を許可する。

ロール制御機能は、Interstage 管理コンソールを利用した TOE の運用管理時に必ず呼び出される機能であり、操作者による運用管理操作を他の操作者による影響から保護する機能である。

対応する TOE セキュリティ機能要件：FDP_ACC.1、FDP_ACF.1、FMT_MSA.3、FPT_RVM.1、FPT_SEP.1

6.1.5. アプリケーション自動再起動機能（SF.AUTO_RECOVER）

アプリケーション自動再起動機能は、アプリケーションの実行プロセスが、Configurators もしくは Administrators による停止操作以外によって異常終了した場合に、

アプリケーション動作を維持できない障害が生じたと見なし、警告メッセージを TOE が動作するアプリケーションサーバの OS へ通知し、当該アプリケーションの実行プロセスを再起動する。

アプリケーション自動再起動機能の対象となるアプリケーションは、ワークユニット定義にて、ワークユニット毎にアプリケーション自動再起動をする回数（リトライカウント）を設定することで決定される。ワークユニット定義に対しては、Administrators もしくは Configurators が参照、変更することが許可されている。リトライカウントとは、アプリケーションの障害などにより、アプリケーションが１度も正常に処理されずに異常終了と再起動が繰り返される回数である。TOE は、連続自動再起動回数がリトライカウントに達した場合には、アプリケーション運用を維持できない状態が発生したと判断して警告メッセージを TOE が動作するアプリケーションサーバの OS へ通知し、ワークユニットを強制停止するか、または、当該アプリケーションの実行プロセスだけを異常終了し、残りのアプリケーションの実行プロセスだけで運用を継続する縮退運用を開始する。なお、対象が Web アプリケーションの場合、最初にアプリケーションが異常終了した時刻から一定の時間（リトライカウントリセット時間）が経過することによって、連続異常終了回数がリセットされる。

ワークユニットを強制停止するか縮退運用を開始するかは、ワークユニット定義に対して Administrators もしくは Configurators が、ワークユニット毎にアプリケーション自動再起動失敗時の制御を選択することで決定される。なお、リトライカウントに特定の値を設定した場合に、本機能によるアプリケーション自動再起動の対象から外すことができる。

TOE は、自動再起動の対象として設定されたワークユニットが起動する際に、ワークユニットに関連付けられたアプリケーションの実行プロセスを状態確認対象として登録する。TOE は、状態確認対象の実行プロセスの状態を定期的に確認し、正常動作を確認できなかった実行プロセスの再起動を行う。

なお、ワークユニットが正常終了した場合には、TOE はワークユニットに関連付けられたアプリケーションの実行プロセスを状態確認対象から解除するため本機能による再起動の対象からは外れることになる。

アプリケーション自動再起動機能は、アプリケーション自動再起動をすると設定したワークユニットが起動される際に必ず呼び出される機能であり、外部からの干渉と改ざんから自身を保護する機能である。

対応する TOE セキュリティ機能要件： FMT_MTD.1、FMT_SMF.1、FPT_RVM.1、FPT_SEP.1、FRU_FLT.1

6.1.6. サーバアプリケーションタイマ機能（SF.TIMER）

サーバアプリケーションタイマ機能は、アプリケーションが規定された処理時間を超え

ても処理を完了しなかった場合に、アプリケーションは起動しているが正常に動作していない状態であり、アプリケーション動作を維持できない障害が生じたと見なし、警告メッセージを TOE が動作するアプリケーションサーバの OS へ通知し、当該アプリケーションを強制停止する。

サーバアプリケーションタイマ機能の対象となるアプリケーションは、ワークユニット定義にて、ワークユニット毎にアプリケーション最大処理時間を設定することで決定される。ワークユニット定義に対しては、Administrators もしくは Configurators が参照、変更することが許可されている。アプリケーション最大処理時間とは、アプリケーションの障害などによる、アプリケーションのハングアップやループを原因とした処理遅延と見なすまでの許容時間である。

ワークユニット定義には、アプリケーション最大処理時間を超えてなお処理が完了しない場合に、警告メッセージを TOE が動作するアプリケーションサーバの OS へ通知しワークユニットを強制停止する、もしくは、警告メッセージを TOE が動作するアプリケーションサーバの OS へ通知するのみ、どちらか一方のアクションを設定する。なお、アプリケーション最大処理時間に特定の値を設定した場合に、本機能によるアプリケーションの状態監視の対象から外すことができる。

TOE は、状態監視の対象として設定されたワークユニットを起動する際に、関連付けられたアプリケーションの最大処理時間を登録する。TOE は、アプリケーションの状態を監視し、設定された最大処理時間を超えた実行プロセスに対して、ワークユニット定義に設定されたアクションを行う。

なお、本機能によって強制停止されたアプリケーションに、アプリケーション自動再起動機能による再起動が設定されていた場合は、強制停止後にアプリケーション自動再起動機能によるアプリケーションの再起動が行われる。

また、ワークユニットが正常終了した場合には、TOE はワークユニットに関連付けられたアプリケーションを状態監視対象から解除するため本機能による状態監視の対象からは外れることになる。

サーバアプリケーションタイマ機能は、TOE の起動時に必ず呼び出される機能であり、外部からの干渉と改ざんから自身を保護する機能である。

対応する TOE セキュリティ機能要件： FMT_MTD.1、FMT_SMF.1、FPT_RVM.1、FPT_SEP.1、FRU_FLT.1

6.2. セキュリティメカニズム

本 TOE が採用するセキュリティメカニズムは、管理コンソール端末と Interstage 管理コンソール間の SSL 暗号通信機能に適用される暗号メカニズムと、ユーザ認証機能によって認証された状態を維持するために使用するセション情報に適用される確率的または順列的

メカニズムである。

6.3. セキュリティ機能強度

本 TOE において、機能強度の対象となる確率的または順列的メカニズムによって実現されるセキュリティ機能は、管理コンソール端末と Interstage 管理コンソール間の SSL 暗号通信機能とユーザ認証機能である。SSL 暗号通信機能とユーザ認証機能に対するセキュリティ機能強度は SOF-基本である。

6.4. 保証手段

本節では、TOEの保証手段を説明する。表 6.3 に示すように、以下のセキュリティ保証手段は、表 5.7 で記述したTOEセキュリティ保証要件を満たすものである。なお、ASEクラスに対する保証手段は、本セキュリティターゲットである。

表 6.3 TOE の保証手段一覧

TOE セキュリティ保証要件		コンポーネント	保証手段
構成管理	CM 能力	ACM_CAP.2	Interstage Application Server 8.0.0 構成管理手順書 Interstage Application Server 8.0.0 構成管理要素リスト（プログラム） Interstage Application Server 8.0.0 構成管理要素リスト（文書）
配付と運用	配付	ADO_DEL.1	Interstage Application Server 8.0.0 配付規定 Interstage Application Server 8.0.0 緊急修正の配付規定
	設置、生成、及び立上げ	ADO_IGS.1	Interstage Application Server インストールガイド －Linux－ ソフトウェア説明書 Interstage Application Server Enterprise Edition 8.0.3（64bit Linux 対応版）
開発	機能仕様	ADV_FSP.1	Interstage Application Server 8.0.0 機能仕様書
	上位レベル設計	ADV_HLD.1	Interstage Application Server 8.0.0 上位レベル設計書

	表現対応	ADV_RCR.1	Interstage Application Server 8.0.0 表現対応表
ガイダンス文書	管理者ガイダンス	AGD_ADM.1	Interstage Application Server 運用ガイド Interstage Application Server セキュリティシステム運用ガイド Interstage Application Server OLTP サーバ運用ガイド Interstage Application Server メッセージ集 Interstage Application Server インストールガイド －Linux－
	利用者ガイダンス	AGD_USR.1	
テスト	カバレージ	ATE_COV.1	Interstage Application Server 8.0.0 カバレージ分析書
	機能テスト	ATE_FUN.1	Interstage Application Server 8.0.0 テスト計画書 Interstage Application Server 8.0.0 テスト仕様書 Interstage Application Server 8.0.0 テスト項目書
	独立テスト	ATE_IND.2	TOE
脆弱性評定	誤使用	AVA_MSU.1	Interstage Application Server 運用ガイド Interstage Application Server セキュリティシステム運用ガイド Interstage Application Server OLTP サーバ運用ガイド Interstage Application Server メッセージ集 Interstage Application Server インストールガイド －Linux－ ソフトウェア説明書 Interstage Application Server Enterprise Edition 8.0.3 (64bit Linux 対応版)
	TOE セキュリティ機能強度	AVA_SOF.1	Interstage Application Server 8.0.0 脆弱性分析書

	脆弱性分析	AVA_VLA.1	

7. PP 主張

本 ST は、PP 適合を主張しない。

8. 根拠

8.1. セキュリティ対策方針根拠

本節では、脅威、組織のセキュリティ方針、及び前提条件に対するセキュリティ対策方針の必要性と十分性を示す。

8.1.1. 脅威、組織のセキュリティ方針に対するセキュリティ対策方針の適合性

脅威に対応するセキュリティ対策方針の関係を 表 8.1 に示す。

表 8.1 脅威とセキュリティ対策方針の対応

脅威 / セキュリティ対策方針	T.ILLEGAL_ACCESS	T.SPOOFING	T.DISCLOSE_DATA	T.ARROGATION	T.APPLICATION_TROUBLE
O.ID_AUTH	✔				
O.CRYPTO			✔		
O.SESSION		✔			
O.ROLE_MANAGE				✔	
O.APPLICATION_ TROUBLE					✔
OE.ID_AUTH	✔				
OE.PASSWORD_MANAGE	✔				
OE.USER_MANAGE	✔				

表 8.1 より、各セキュリティ対策方針が１つ以上の脅威に対応していることが分かる。なお、組織のセキュリティ方針は存在しないため、組織のセキュリティ方針の実現に寄与するセキュリティ対策方針は存在しない。

以下に、セキュリティ対策方針によって脅威に対抗できることを示す。

T.ILLEGAL_ACCESS

T.ILLEGAL_ACCESS は、攻撃者が管理コンソール端末もしくは、クライアント端末を利用

して Interstage 管理コンソールへ不正にアクセスし、アプリケーション実行環境や環境定義ファイルの設定変更を行い、TOE や動作しているアプリケーションの停止や設定変更を試みるという脅威である。

この脅威に対抗するためには、攻撃者が Interstage 管理コンソールを利用しようと試みても、アクセスできないようにすることが必要である。

OE.ID_AUTH では、TOE が動作するアプリケーションサーバの OS が、アクセス者による Interstage 管理コンソールへのアクセス時に、アクセス者が TOE の操作者であることを識別し、本人であることの認証を行っているため、Interstage 管理コンソールへ不正にアクセスすることはできない。

O.ID_AUTH によって、TOE は、OE.ID_AUTH によるアクセス者の識別認証実施時に、アクセス者が入力したパスワードを外部に漏らさないように保護しているため、パスワード漏洩による不正アクセスを防止することができる。

また、OE.PASSWORD_MANAGE によって、Interstage 管理コンソールへのログイン時に使用するパスワードとし 8 桁以上の数字、英字、特殊文字からなる容易に推測できない不規則な文字列を設定すること、更に、パスワードの管理はパスワードの所有者のみが行い、定期的にパスワードの変更を行うことを、Administrators 及び Configurators に要求しているため、パスワードの強度や管理の安全性を保証することができる。

OE.USER_MANAGE によって、TOE が動作するアプリケーションサーバの OS へのユーザ登録を、TOE の運用を行う必要のある者のみに制限し、それ以外の者は登録しないことを、TOE が動作するアプリケーションサーバの OS の管理者に要求しているため、TOE に関係しないユーザからのアクセスを防止することができる。

従って、O.ID_AUTH、OE.ID_AUTH、OE.PASSWORD_MANAGE、OE.USER_MANAGE が満たされることにより、本脅威に対抗することができる。

T.SPOOFING

T.SPOOFING は、Interstage 管理コンソールへの不正なログインを防ぐために識別認証の対策を実施した際の二次脅威として、攻撃者が、操作者がログイン状態のまま離席した管理コンソール端末を使用して、Interstage 管理コンソールに無断にアクセスし、アプリケーション実行環境や環境定義ファイルの設定変更を行い、TOE や動作しているアプリケーションの停止や設定変更を試みるという脅威である。

この脅威に対抗するためには、ログイン状態のまま離席した管理コンソール端末から Interstage 管理コンソールを利用しようと試みても、アクセスできないようにすることが必要である。

O.SESSION では、管理コンソール端末から Interstage 管理コンソールへの運用管理操作が管理された一定時間に渡って何も行われなかった場合、管理コンソール端末と Interstage 管理コンソールの間のセションを切断するため、離席中の管理コンソール端末

から継続して Interstage 管理コンソールへアクセスすることはできない。

従って、O.SESSION が満たされることにより、本脅威に対抗することができる。

T.DISCLOSE_DATA

T.DISCLOSE_DATA は、Interstage 管理コンソールへの不正なログインを防ぐために識別認証の対策を実施した際の二次脅威として、攻撃者が、管理コンソール端末と Interstage 管理コンソール間のネットワーク上で送受信される通信データを盗聴し、識別認証情報を入手する。入手した識別認証情報を使用して、操作者として Interstage 管理コンソールを使用してアプリケーション実行環境や環境定義ファイルの設定変更を行い、TOE や動作しているアプリケーションの停止や設定変更を試みるという脅威である。

この脅威に対抗するためには、管理コンソール端末と Interstage 管理コンソール間の通信データを暴露から保護することが必要である。

O.CRYPTO では、管理コンソール端末と Interstage 管理コンソール間の通信路上のデータを暴露から保護するため、管理コンソール端末と Interstage 管理コンソール間の通信データを暴露から保護することができる。

従って、O.CRYPTO が満たされることにより、本脅威に対抗することができる。

T.ARROGATION

T.ARROGATION は、Administrators のロールを持たない者が管理コンソール端末を利用して、Interstage 管理コンソールへアクセスし、サービスやシステム設定に関する環境定義ファイルの設定変更を行い、TOE や動作しているサービス、またはシステムの停止、設定変更を試みるという脅威である。

この脅威に対抗するためには、異常終了や処理遅延によるアプリケーション動作障害が生じた際に、利用者が設定したワークユニット定義に従ったアプリケーションの実行を維持することが必要である。

O.APPLICATION_TROUBLE では、TOE 上で動作するアプリケーションの停止操作以外の原因による異常終了時、及び、アプリケーション処理遅延のためのレスポンス遅延発生時に、ワークユニット定義に従ったアプリケーションの実行を維持するため、アプリケーション動作障害から早期に復旧できることを保証できる。

従って、O.APPLICATION_TROUBLE が満たされることにより、本脅威に対抗することができる。

T.APPLICATION_TROUBLE

T.APPLICATION_TROUBLE は、TOE 上で動作するアプリケーションが停止操作以外の原因によって異常終了する、もしくは、アプリケーション処理遅延のためレスポンスが遅延することによって、利用者が設定したアプリケーション動作を維持できなくなるという脅威で

ある。

この脅威に対抗するためには、異常終了や処理遅延によるアプリケーション動作障害から早期に復旧させることが必要である。

O.APPLICATION_STOP では、TOE 上で動作しているアプリケーションの処理遅延のためレスポンスが遅延して、アプリケーション動作を維持できなくなった場合、該当するアプリケーションを強制停止させる。

O.APPLICATION_RECOVER では、TOE 上で動作しているアプリケーションが停止操作以外の原因によって異常終了して、アプリケーション動作を維持できなくなった場合、該当するアプリケーションを再起動させるため、アプリケーション動作障害から早期に復旧できることを保証できる。なお、O.APPLICATION_STOP によって強制停止された場合にも、停止操作以外の原因による異常終了と見なされるため、O.APPLICATION_RECOVER によるアプリケーション再起動の対象となり、アプリケーション動作障害から早期に復旧できることを保証できる。

従って、O.APPLICATION_RECOVER 及び O.APPLICATION_STOP が満たされることにより、本脅威に対抗することができる。

8.1.2. 前提条件に対する環境のセキュリティ対策方針の適合性

前提条件に対応する環境のセキュリティ対策方針を 表 8.2 に示す。

表 8.2 前提条件とセキュリティ対策方針の対応

前提条件 / セキュリティ対策方針	A.TRUST	A.PHYSICAL_ACCESS	A.SERVICE	A.APPLICATION
OE.TRUST	✔			
OE.PHYSICAL_ACCESS		✔		
OE.SERVICE			✔	
OE.APPLICATION				✔

表 8.2 より、各セキュリティ対策方針が１つ以上の前提条件に対応していることが分かる。以下に、セキュリティ対策方針によって前提条件を実現できることを示す。

A.TRUST

A.TRUST は、Administrators が、ロールに課せられた職務に関して責任を持ち、不正な

行為を行わないことを規定した前提条件である。

この前提条件を満足するためには、Administrators を任命する際には、ロールを付与される者に、Administrators に課せられた職務を理解させることを保証する必要がある。

OE.TRUST では、システム責任者に、Administrators を任命する際にロールを付与される者に Administrators に課せられた職務を理解させることに責任を持つことを要求しているため、Administrators として登録された者は課せられた職務に責任を持ち、不正な行為を行わないことを保証できる。

従って、OE.TRUST が満たされることにより、本前提条件を満足することができる。

A.PHYSICAL_ACCESS

A.PHYSICAL_ACCESS は、TOE が動作するアプリケーションサーバが信頼出来ない者の立入りが禁止されたシステム運用区画へ設置されることを規定した前提条件である。

この前提条件を満足するためには、信頼出来ない者の立入りが禁止されたシステム運用区画に TOE が動作する機器を設置することを保証する必要がある。

OE.PHYSICAL_ACCESS では､信頼出来ない者の立入りが禁止されたシステム運用区画に TOE が動作する機器を設置することを Administrators に要求しているため、信頼出来ない者の立入りが禁止されたシステム運用区画に TOE が動作する機器を設置されることを保証できる。

従って、OE.PHYSICAL_ACCESS が満たされることにより、本前提条件を満足することができる。

A.SERVICE

A.SERVICE は、TOE が動作するアプリケーションサーバでは、OS へのリモートログインサービスは提供せず、保守時を除いてコマンド実行による CUI ベースの運用を行わないことを規定した前提条件である。

この前提条件を満足するためには、TOE が動作するアプリケーションサーバにおいて OS へのリモートログインサービスを停止し、保守時を除いて必ず Interstage 管理コンソールを利用した GUI ベースの運用操作を行う必要がある。

OE.SERVICE では、TOE が動作するアプリケーションサーバにおいて OS へのリモートログインサービスを停止することを Administrators に要求しているため、TOE が動作するアプリケーションサーバにおいて OS へのリモートログインサービスを停止できる。また、保守時を除いて、必ず Interstage 管理コンソールの画面から TOE の操作を行うことを Administrators 及び Configurators に要求しているため、保守時以外の運用操作を Interstage 管理コンソールを利用した GUI ベースの方法で行うことができる。

従って、OE.SERVICE が満たされることにより、本前提条件を満足することができる。

A.APPLICATION

A.APPLICATION は、TOE 上で動作するアプリケーションは信頼できるものとした前提条件である。

この前提条件を満足するためには、TOE 上で動作させるアプリケーションの信頼性を保証するため、作成元がどこであるか確認でき、かつ、動作確認が行われていることを確認できたアプリケーションのみを TOE 上で動作させることが必要である。

OE.APPLICATION では、作成元が特定でき、動作確認が完了したアプリケーションのみを TOE 上で動作させることを Administrators 及び Configurators に要求しているため、作成元が特定でき、動作確認が完了したアプリケーションのみを TOE 上で動作させることを保証できる。

従って、OE.APPLICATION が満たされることにより、本前提条件を満足することができる。

8.2. セキュリティ要件根拠

本節では、セキュリティ対策方針に対するセキュリティ要件の必要性と十分性の根拠を示すとともに、各セキュリティ要件の依存性と相互補完性が満足されていることを示す。また、設定したセキュリティ保証要件が妥当である根拠を示す。さらに、設定した最小機能強度レベルが妥当である根拠を示す。

8.2.1. セキュリティ対策方針に対するセキュリティ機能要件の適合性

セキュリティ対策方針に対するセキュリティ機能要件の対応を 表 8.3 に示す。

表 8.3 セキュリティ対策方針と TOE セキュリティ機能要件の対応

種別	セキュリティ対策方針 / セキュリティ機能要件	O.ID_AUTH	O.CRYPTO	O.SESSION	O.ROLE_MANAGE	O.APPLICATION_TROUBLE	OE.ID_AUTH
TOE セキュリティ機能要件	FCS_CKM.1		✔				
	FCS_COP.1		✔				
	FDP_ACC.1				✔		
	FDP_ACF.1				✔		
	FIA_ATD.1				✔		
	FIA_UAU.7	✔					
	FIA_USB.1				✔		

	FMT_MSA.3				✔		
	FMT_MTD.1					✔	
	FMT_SMF.1					✔	
	FMT_SMR.1					✔	
	FPT_RVM.1	✔	✔	✔	✔	✔	
	FPT_SEP.1	✔	✔	✔	✔	✔	
	FRU_FLT.1					✔	
	FTA_SSL.3			✔			
	FTP_TRP.1		✔				
IT 環境の セキュリティ機能要件	FIA_UAU.2						✔
	FIA_UID.2						✔

表 8.3 より、各セキュリティ機能要件が１つ以上のセキュリティ対策方針に対応していることが分かる。

以下に、セキュリティ機能要件によってセキュリティ対策方針を実現できることを示す。

O.ID_AUTH

O.ID_AUTH は、OS による Interstage 管理コンソールに対するアクセス者の識別認証実施時に、アクセス者が入力したパスワードを外部に漏らさないように保護するセキュリティ対策方針である。

このセキュリティ対策方針を実現するためには、アクセス者によるパスワードの入力時に、パスワードを確認できる情報を外部へ公開しないよう制御を行うことが必要となる。

FIA_UAU.7 によって、TOE は利用者の認証時に入力されるパスワードのフィードバック情報として、入力された文字数分のダミー文字を返す。

FPT_RVM.1 によって、入力されるパスワードのフィードバック情報としてダミー文字を返す仕組みが必ず呼び出されることを保証する。

FPT_SEP.1 によって、信頼できないサブジェクトによる干渉と改ざんから保護するためのセキュリティドメインが維持されることを保証する。

従って、FIA_UAU.7、FPT_RVM.1 及び FPT_SEP.1 が満たされることにより、本セキュリティ対策方針を満足することができる。

O.CRYPTO

O.CRYPTO は、管理コンソール端末と Interstage 管理コンソール間の通信路上のデータを暴露から保護するセキュリティ対策方針である。

このセキュリティ対策方針を実現するためには、管理コンソール端末と Interstage 管理コンソール間の通信を、通信データの保護を提供する高信頼パスによって実現し、送受信

される通信データを暗号化することが必要となる。

FCS_CKM.1によって、TOEは通信データの暗号化、復号操作を行うために使用する暗号鍵（サーバ・ライト鍵、クライアント・ライト鍵）を生成する。

FCS_COP.1によって、TOEは管理コンソール端末とInterstage管理コンソール間で送受信される通信データの暗号化、復号操作を行う。

FTP_TRP.1によって、TOEは操作者によって行われる管理コンソール端末とInterstage管理コンソールの間の通信を、通信データの保護を提供する高信頼パスによって提供する。

FPT_RVM.1によって、管理コンソールとInterstage管理コンソール間の通信を高信頼パスによって開始し、通信データを暗号化する仕組みが必ず呼び出されることを保証する。

FPT_SEP.1によって、信頼できないサブジェクトによる干渉と改ざんから保護するためのセキュリティドメインが維持されることを保証する。

従って、FCS_CKM.1、FCS_COP.1、FTP_TRP.1、FPT_RVM.1及びFPT_SEP.1が満たされることにより、本セキュリティ対策方針を満足することができる。

O.SESSION

O.SESSIONは、管理コンソール端末からInterstage管理コンソールへの運用管理操作が管理された一定時間に渡って何も行われなかった場合に、管理コンソール端末とInterstage管理コンソールの間のセションを切断するセキュリティ対策方針である。

このセキュリティ対策方針を実現するためには、Interstage管理コンソールに対する管理コンソール端末からの操作要求が一定時間なかった際に、セションを終了させることが必要となる。

FTA_SSL.3により、TOEはInterstage管理コンソールに対する管理コンソール端末からの操作要求を確認し、管理された一定の非アクティブ時間経過後にセションを切断する。

FPT_RVM.1によって、管理された一定の非アクティブ時間経過後に管理コンソール端末とInterstage管理コンソール間のセションを切断する仕組みが必ず呼び出されることを保証する。

FPT_SEP.1によって、信頼できないサブジェクトによる干渉と改ざんから保護するためのセキュリティドメインが維持されることを保証する。

従って、FTA_SSL.3 、FPT_RVM.1及びFPT_SEP.1が満たされることにより、本セキュリティ対策方針を満足することができる。

O.ROLE_MANAGE

O.ROLE_MANAGEは、Interstage管理コンソールを利用したサービスやシステム設定に関する環境定義ファイルへの操作要求時に、操作者のロールを確認し、Administratorsのロールを持つ者のみに操作実行を許可するセキュリティ対策方針である。

このセキュリティ対策方針を実現するためには、OSによる識別認証成功時にアクセス者

にロール識別情報を付与し、環境定義ファイルに対する操作要求時に、操作者がAdministratorsであることを確認することが必要となる。

FIA_ATD.1によって、TOEはアクセス者に付与するためのロール識別情報を維持する。

FIA_USB.1によって、TOEはOSによる識別認証が成功したアクセス者にロール識別情報を付与する。

FDP_ACC.1及びFDP_ACF.1によって、環境定義ファイルに対する操作実行可否を、操作者のロールと権限リストによって判断し、制御する。

FMT_MSA.3によって、FDP_ACC.1及びFDP_ACF.1で制御される権限リストのデフォルト値が改変されることなく維持される。

FPT_RVM.1によって、環境定義ファイルに対する操作要求時に、操作者のロールを確認し、操作実行可否を制御する仕組みが必ず呼び出されることを保証する。

FPT_SEP.1によって、信頼できないサブジェクトによる干渉と改ざんから保護するためのセキュリティドメインが維持されることを保証する。

従って、FIA_ATD.1、FIA_USB.1、FDP_ACC.1、FDP_ACF.1、FMT_MSA.3、FPT_RVM.1及びFPT_SEP.1が満たされることにより、本セキュリティ対策方針を満足することができる。

O.APPLICATION_TROUBLE

O.APPLICATION_TROUBLEは、TOE上で動作するアプリケーションの停止操作以外の原因による異常終了時、及び、アプリケーション処理遅延のためのレスポンス遅延発生時に、ワークユニット定義に従ったアプリケーションの実行を維持するセキュリティ対策方針である。

このセキュリティ対策方針を実現するためには、アプリケーションに動作障害が生じた際に、アプリケーションの動作を維持させることが必要となる。

FRU_FLT.1によって、アプリケーション実行プロセスの異常終了時、及び、アプリケーション処理の遅延発生時に、アプリケーション動作の保証を行う。

FMT_MTD.1により、ワークユニット定義（リトライカウント、リトライカウントリセット時間、アプリケーション自動再起動失敗時の制御、アプリケーション最大処理時間、アプリケーション最大処理時間経過時の制御）の設定を行うことができる利用者をAdministrators及びConfiguratorsに制限することができ、FMT_SMF.1によってAdministrator及びConfiguratorsにワークユニット定義を管理させることができる。

FMT_SMR.1によって、TOEはAdministratorsまたはConfiguratorsというロールを維持し、操作者に対していずれかのロールを関連付ける。

FPT_RVM.1によって、アプリケーション動作の障害発生時に、当該アプリケーションを再起動させる仕組みが必ず呼び出されることを保証する。

FPT_SEP.1によって、信頼できないサブジェクトによる干渉と改ざんから保護するためのセキュリティドメインが維持されることを保証する。

従って、FRU_FLT.1、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1、FPT_RVM.1 及び FPT_SEP.1 が満たされることにより、本セキュリティ対策方針を満足することができる。

OE.ID_AUTH

OE.ID_AUTH は、TOE が動作するアプリケーションサーバの OS が管理コンソール端末を利用した、Interstage 管理コンソールへのアクセス時にアクセス者が TOE の操作者であることを識別し、本人であることを認証するセキュリティ対策方針である。

このセキュリティ対策方針を実現するためには、Interstage 管理コンソールへのアクセス要求時に、TOE が動作するアプリケーションサーバの OS 機能を利用した識別認証を実施することが必要となる。

FIA_UID.2 及び FIA_UAU.2 により、TOE が動作するアプリケーションサーバの OS は Interstage 管理コンソールへのアクセス者が TOE の操作者であることを識別し、本人であることの認証を行う。

従って、FIA_UID.2 及び FIA_UAU.2 が満たされることにより、本セキュリティ対策方針を満足することができる。

8.2.2. セキュリティ機能要件間の依存関係

セキュリティ機能要件間の依存関係を 表 8.4 に示す。

表 8.4 TOE セキュリティ機能要件間の依存関係

No	セキュリティ機能要件	下位階層	依存関係	参照 No	備考
1	FCS_CKM.1	なし	FCS_CKM.2 または FCS_COP.1	2	
			FCS_CKM.4	―	※1
			FMT_MSA.2	―	※2
2	FCS_COP.1	なし	FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1	1	
			FCS_CKM.4	―	※1
			FMT_MSA.2	―	※2
3	FDP_ACC.1	なし	FDP_ACF.1	4	
4	FDP_ACF.1	なし	FDP_ACC.1	3	

			FMT_MSA.3	8	
5	FIA_ATD.1	なし	なし	－	
6	FIA_UAU.7	なし	FIA_UAU.1	16	FIA_UAU.2 は FIA_UAU.1 の上位階層コンポーネントである
7	FIA_USB.1	なし	FIA_ATD.1	5	
8	FMT_MSA.3	なし	FMT_MSA.1	－	※3
			FMT_SMR.1	－	※4
9	FMT_MTD.1	なし	FMT_SMF.1	10	
			FMT_SMR.1	11	
10	FMT_SMF.1	なし	なし	－	
11	FMT_SMR.1	なし	FIA_UID.1	17	FIA_UID.2 は FIA_UID.1 の上位階層コンポーネントである
12	FPT_RVM.1	なし	なし	－	
13	FPT_SEP.1	なし	なし	－	
14	FRU_FLT.1	なし	FPT_FLS.1	－	※5
15	FTA_SSL.3	なし	なし	－	
16	FIA_UAU.2	FIA_UAU.1	FIA_UID.1	17	FIA_UID.2 は FIA_UID.1 の上位階層コンポーネントである
17	FIA_UID.2	FIA_UID.1	なし	－	
18	FTP_TRP.1	なし	なし	－	

※1

TOE が使用する暗号鍵は、サーバ・ライト鍵とクライアント・ライト鍵である。これらの暗号鍵は､SSL 暗号通信機能を使用して TOE と通信する場合に TOE が利用する暗号鍵であり、TOE 外のプログラムや操作者が利用できるものではない。また、TOE 外から TOE の暗号鍵を利用するためのインタフェースも存在しない。従って、TOE 外部から TOE の暗号鍵を読み出す手段は存在しないため、暗号鍵を破棄する必要はない。

従って、暗号鍵の破棄に関するセキュリティ機能要件 FCS_CKM.4 は不要である。

※2

FCS_CKM.1、FCS_COP.1 で扱うセキュリティ属性は、暗号鍵であるサーバ・ライト鍵とクライアント・ライト鍵に関する属性である。これらの属性は、標準化されたアルゴリズムに従って属性の値が決定されるため、操作者が設定・改変することができない。

従って、セキュアなセキュリティ属性の保証に関するセキュリティ機能要件 FMT_MSA.2 は不要である。

※3

FMT_MSA.3 で扱うセキュリティ属性は TOE によって管理されており、操作者に対してデフォルト値変更や問い合わせ、改変、削除などを行う能力を付与する必要はない。

従って、セキュリティ属性の管理に関するセキュリティ機能要件 FMT_MSA.1 は不要である。

※4

FMT_MSA.3 で扱うセキュリティ属性のデフォルト値を上書きする代替の初期値を指定する役割は存在せず、役割を維持する必要はない。

従って、セキュリティ役割の維持に関するセキュリティ機能要件 FMT_SMR.1 は不要である。

※5

FRU_FLT.1 で保証する機能は、アプリケーション動作に障害が発生した際のアプリケーション動作保証である。アプリケーションの動作障害は、アプリケーションの資源管理不備やアプリケーションが連携する他製品の処理の不備によって生じるものであり、TSF における障害とは無関係である。TSF において障害が発生した場合には、TOE としての動作を維持することが困難であり、Administrators による運用管理によって正常な状態へ遷移させるため、TSF としての保証の範囲には含めない。

従って、TSF においてある種別の障害が発生した際に、TOE がその TSP を侵害しないことを保証するセキュリティ機能要件 FPT_FLS.1 は不要である。

8.2.3. セキュリティ機能要件内部一貫性

8.2.2 に示したように、セキュリティ機能要件は一部の例外を除き、それぞれと依存関係のあるセキュリティ機能要件と相互補完（〔FCS_CKM.1、FCS_COP.1〕、〔FDP_ACC.1、FDP_ACF.1、FMT_MSA.3〕、〔FIA_ATD.1、FIA_USB.1〕、〔FMT_MTD.1、FMT_SMF.1、FMT_SMR.1、FIA_UID.2〕、〔FIA_UAU.7、FIA_UAU.2、FIA_UID.2〕）している。相互補完しているセキュリティ機能要件グループ内の各セキュリティ機能要件間の依存は、CCが規定した依存性に従って補完されているため、内容に競合や矛盾が生じる要件は含まれていない。また、相互補完しているセキュリティ機能要件のグループは、暗号関連/アクセス制御関連/ロール管理関連/セキュリティ管理関連/識別認証関連といった異なる要件を達成するためのグループであり、グループ間に競合や矛盾が生じるものは存在しない。

すなわち、セキュリティ機能要件のセットは内部的に一貫している。

8.2.4. セキュリティ機能要件の相互補完性

明示的な依存関係を要求されてはいないが、迂回防止、干渉防止、非活性化防止、無効化攻撃検出の観点から相互補完するセキュリティ機能要件について記述する。

表 8.5 に、各セキュリティ機能要件に対し、迂回防止、干渉防止、非活性化防止の観点で必要なセキュリティ機能要件を示す。表中に記載されたセキュリティ機能要件が、相互支援に必要なセキュリティ機能要件である。

なお、TOE のセキュリティ機能を無効化する操作は、FRU_FLT.1 によるアプリケーションの強制停止及び再起動に関する設定操作のみであるが、このセキュリティ機能の設定（ワークユニット定義）は Administrators が Interstage 管理コンソールの画面から現在の設定状態を確認することができるため、無効化攻撃検出に関するセキュリティ機能要件の考慮は不要である。

表 8.5 セキュリティ機能要件の相互支援

相互支援 / セキュリティ機能要件	迂回防止	干渉防止	非活性化防止
FCS_CKM.1	FPT_RVM.1	FPT_SEP.1	なし
FCS_COP.1	FPT_RVM.1	FPT_SEP.1	なし
FDP_ACC.1	FPT_RVM.1	FPT_SEP.1	なし
FDP_ACF.1	FPT_RVM.1	FPT_SEP.1	なし
FIA_ATD.1	FPT_RVM.1	FPT_SEP.1	なし
FIA_UAU.7	FPT_RVM.1	FPT_SEP.1	なし
FIA_USB.1	FPT_RVM.1	FPT_SEP.1	なし
FMT_MSA.3	FPT_RVM.1	FPT_SEP.1	なし
FMT_MTD.1	FPT_RVM.1	FPT_SEP.1	なし
FMT_SMF.1	FPT_RVM.1	FPT_SEP.1	なし
FMT_SMR.1	FPT_RVM.1	FPT_SEP.1	なし
FPT_RVM.1	N/A	N/A	なし
FPT_SEP.1	N/A	N/A	なし
FRU_FLT.1	FPT_RVM.1	FPT_SEP.1	FMT_MTD.1
FTA_SSL.3	FPT_RVM.1	FPT_SEP.1	なし
FTP_TRP.1	FPT_RVM.1	FPT_SEP.1	なし

N/A：適用外

＜迂回防止＞

表 8.5 に示すセキュリティ機能要件は、それらが迂回されることによりセキュリティ機能が正しく動作することができないため、迂回されることを防止しなければならない。

FPT_RVM.1 によってセキュリティ機能が必ず呼び出され成功することが保証される。

＜干渉防止＞

表 8.5 に示すセキュリティ機能要件は、それらが動作するセキュリティドメインにおいて信頼できないサブジェクトに干渉されることにより、セキュリティ機能が正しく動作することができないため、信頼できないサブジェクトから干渉されることを防止しなければならない。

FPT_SEP.1 によってセキュリティ機能が信頼できないサブジェクトの干渉から保護されることが保証される。

＜非活性化防止＞

FRU_FLT.1 によるアプリケーションの強制停止及び再起動は、操作者の操作により制御の対象とする／しないを設定することができるため、不正な非活性化攻撃を防止しなければならない。

FMT_MTD.1 によって操作者の操作による設定を Administrators 及び Configurators のみに制限することができるため、不正に機能を利用しない設定に変更されることから保証される。

8.2.5. 最小機能強度レベル根拠

本TOEが想定する攻撃者は、3.2 で述べたように高度な専門知識を持たない低レベルの攻撃者である。従って、最小機能強度レベルとしてはSOF-基本が妥当であると言える。

本 ST では、TOE セキュリティ機能要件に対する最小機能強度として SOF-基本を主張している。また、特定の TOE セキュリティ機能要件（FCS_CKM.1 及び FCS_COP.1）に対する機能強度として SOF-基本が主張されており、低レベルの攻撃者による攻撃に対抗するために策定された TOE のセキュリティ対策方針と一貫している。

8.2.6. セキュリティ保証要件根拠

本 ST にて要求する TOE に対する保証レベルは EAL2 に AVA_MSU.1 を追加した EAL2 追加である。

本 TOE は、アプリケーション動作の基盤となる動作環境を提供する製品であり、様々な環境で開発されたアプリケーションに対する動作環境を提供することと同時に、インストールからアプリケーションの導入・運用・監視・保守に渡る運用管理の効率化を実現する

ことも求められている。

このため、外部インタフェースの識別、機能の内部構造の特定、テストによるセキュリティ機能の確認、脆弱性分析といった開発プロセスにおけるセキュリティ確保への取組みが求められる。これらの要求を満たす保証レベルとしてEAL2が適切である。

また、アプリケーションの動作の維持にはTOEの適切な運用管理が必要となる。そのため、TOEをセキュアに利用するには、運用管理において正しい利用、適切な操作が必要である。したがって、誤使用の可能性及び非セキュアな状態への遷移の可能性を低減するための保証としてAVA_MSU.1を追加する。

なお、追加した保証要件コンポーネントであるAVA_MSU.1と依存関係にある以下の保証要件コンポーネントもEAL2のセットに含まれており、選択された保証要件のセットにおいて依存性も満たされている。

- ADO_IGS.1
- ADV_FSP.1
- AGD_ADM.1
- AGD_USR.1

従って、EAL2にAVA_MSU.1を追加したセキュリティ保証要件のセットは内部的に一貫している。

8.3. TOE 要約仕様根拠

8.3.1. TOE 要約仕様に対するセキュリティ機能要件の適合性

本節では、セキュリティ機能全体がすべてのセキュリティ機能を満足し、相互に補完し一体となって機能していることを示す。

TOE要約仕様に適合するセキュリティ機能要件の関係を 表 8.6 に示す。

表 8.6 TOE 要約仕様とセキュリティ機能要件の対応

TOE 要約仕様 / TOE セキュリティ機能要件	SF. ID_AUTH	SF. CRYPTO	SF. SESSION	SF. ROLE_MANAGE	SF. AUTO_RECOVER	SF. TIMER
FCS_CKM. 1		✔				
FCS_COP. 1		✔				
FDP_ACC. 1				✔		
FDP_ACF. 1				✔		
FIA_ATD. 1	✔					
FIA_UAU. 7	✔					
FIA_USB. 1	✔					
FMT_MSA. 3				✔		
FMT_MTD. 1					✔	✔
FMT_SMF. 1					✔	✔
FMT_SMR. 1	✔					
FPT_RVM. 1	✔	✔	✔	✔	✔	✔
FPT_SEP. 1	✔	✔	✔	✔	✔	✔
FRU_FLT. 1					✔	✔
FTA_SSL. 3			✔			
FTP_TRP. 1		✔				

表 8.6 より、各TOE要約仕様が１つ以上のセキュリティ機能要件に対応していることが分かる。

以下に、TOE 要約仕様によってセキュリティ機能要件が実現されることを示す。

FCS_CKM.1

FCS_CKM.1は、定められた暗号鍵生成アルゴリズム、暗号鍵長に従った暗号鍵を生成することを要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、FCS_CKM.1で規定した暗号鍵を生成する機能の実装が必要である。

SF.CRYPTOによって、FCS_CKM.1にて規定された通りの暗号鍵を生成することができる。

従って、SF.CRYPTOの実装によりFCS_CKM.1を実現できる。

FCS_COP.1

FCS_COP.1は、定められた暗号アルゴリズム、暗号鍵長に従った暗号操作を実施することを要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、FCS_COP.1で規定した暗号操作を実施する機能の実装が必要である。

SF.CRYPTOによって、FCS_COP.1にて規定された通りの暗号操作を実施することができる。

従って、SF.CRYPTOの実装によりFCS_COP.1を実現できる。

FDP_ACC.1

FDP_ACC.1は、識別されたサブジェクト、オブジェクト、サブジェクトとオブジェクト間の操作に対してアクセス制御SFPを適用することを要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、FDP_ACC.1で規定したサブジェクト、オブジェクト、操作に対してアクセス制御SFPを実施する機能の実装が必要である。

SF.ROLE_MANAGE によって、FDP_ACC.1 にて規定されたサブジェクト、オブジェクト、操作に対してInterstage管理コンソールアクセス制御SFPを実施することができる。

従って、SF.ROLE_MANAGEの実装によりFDP_ACC.1を実現できる。

FDP_ACF.1

FDP_ACF.1は、識別されたセキュリティ属性に基づいて、FDP_ACC.1で適用を要求されたアクセス制御SFPを実施することを要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、FDP_ACF.1で規定したセキュリティ属性に従って、アクセス制御SFPを実施する機能の実装が必要である。

SF.ROLE_MANAGE によって、FDP_ACF.1 にて規定されたセキュリティ属性に従って、Interstage管理コンソールアクセス制御SFPを実施することができる。

従って、SF.ROLE_MANAGEの実装によりFDP_ACF.1を実現できる。

FIA_ATD.1

FIA_ATD.1は、TSPの実施に必要なセキュリティ属性を維持することを要求するセキュリ

ティ機能要件である。

このセキュリティ機能要件を実現するためには、TOE の操作者に関連付ける必要があるセキュリティ属性として、ロール識別情報を維持する機能の実装が必要である。

SF.ID_AUTH によって、FIA_ATD.1 が要求する、操作者の操作実行可否に関する TSP の実施に必要なロール識別情報を維持する機能を実現することができる。

従って、SF.ID_AUTH の実装により FIA_ATD.1 を実現できる。

FIA_UAU.7

FIA_UAU.7 は、認証データがそのまま利用者に返されないことを要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、利用者の認証時に入力されるパスワードのフィードバック情報として、入力されたパスワードと異なる情報を返す機能の実装が必要である。

SF.ID_AUTH によって、FIA_UAU.7 が要求する、利用者の認証時に入力されるパスワードのフィードバック情報として、ダミー文字を返す機能を実現することができる。

従って、SF.ID_AUTH の実装により FIA_UAU.7 を実現できる。

FIA_USB.1

FIA_USB.1 は、TOE の操作者に、TSP の実施に必要なセキュリティ属性を関連付けることを要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、TOE の操作者にロール識別情報を関連付ける機能の実装が必要である。

SF.ID_AUTH によって、FIA_USB.1 が要求する、TOE の操作者にロール識別情報を関連付ける機能を実現することができる。

従って、SF.ID_AUTH の実装により FIA_USB.1 を実現できる。

FMT_MSA.3

FMT_MSA.3 は、セキュリティ属性の初期値管理を要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、セキュリティ属性のデフォルト値を固定的に維持し、デフォルト値の変更を許可しない機能の実装が必要である。

SF.ROLE_MANAGE によって、FMT_MSA.3 が要求する、セキュリティ属性となる権限リストの初期値を固定的に維持し、権限リストの変更を許可しない機能を実現することができる。

従って、SF.ROLE_MANAGE の実装により FMT_MSA.3 を実現できる。

FMT_MTD.1

FMT_MTD.1 は、許可された役割に TSF データの管理を認めることを要求するセキュリティ

機能要件である。

このセキュリティ機能要件を実現するためには、TSF データを管理することができるロールを特定し、特定されたロールのみに管理を許可する機能の実装が必要である。

SF.AUTO_RECOVER によって、アプリケーション自動再起動に関するワークユニット定義（リトライカウント、リトライカウントリセット時間、アプリケーション自動再起動失敗時の制御）の参照、設定管理を Administrators 及び Configurators のみに制限することができる。

SF.TIMER によって、サーバアプリケーションタイマ機能に関するワークユニット定義（アプリケーション最大処理時間、アプリケーション最大処理時間超過時の制御）の参照、設定管理を Administrators 及び Configurators のみに制限することができる。

従って、SF.AUTO_RECOVER 及び SF.TIMER の実装により FMT_MTD.1 を実現できる。

FMT_SMF.1

FMT_SMF.1 は、TOE が管理する管理機能を特定することを要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、TOE が管理する管理項目を特定し、その項目を管理する機能の実装が必要である。

SF.AUTO_RECOVER によって、アプリケーション自動再起動に関する設定管理機能を実現することができる。

SF.TIMER によって、サーバアプリケーションタイマ機能に関する設定管理機能を実現することができる。

従って、SF.AUTO_RECOVER 及び SF.TIMER の実装により FMT_SMF.1 を実現できる。

FMT_SMR.1

FMT_SMR.1 は、ロールを維持し、TOE の利用者にロールを関連付けることを要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、ロールを維持管理し、TOE を利用する利用者にロールを関連付ける機能の実装が必要である。

SF.ID_AUTH によって、FMT_SMR.1 が要求する、ワークユニット定義の管理に必要な Administrators 及び Configurators というロールを維持し、TOE を利用する操作者へいずれかのロールを関連付けることができる。

従って、SF.ID_AUTH の実装により FMT_SMR.1 を実現できる。

FPT_RVM.1

FPT_RVM.1 は、各機能の動作進行が許可される前に、セキュリティ機能が呼び出され、そのセキュリティ機能が成功することの保証を要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、ユーザ認証機能、SSL 暗号通信機能、セションタイムアウト機能、ロール制御機能、アプリケーション自動再起動機能及びサーバアプリケーションタイマ機能が、その実行契機に必ず呼び出され成功することの保証が必要である。

SF.ID_AUTH によって、Interstage 管理コンソールへのアクセス時に、入力されるパスワードのフィードバック情報としてダミー文字を返す仕組み、及び、TOE が維持しているロール識別情報を識別認証に成功したアクセス者に付与する仕組みが必ず呼び出されることが保証される。

SF.CRYPTO によって、管理コンソール端末と Interstage 管理コンソールの間の通信時には必ず SSL 暗号通信機能が呼び出され成功することが保証される。

SF.SESSION によって、Interstage 管理コンソールに対する管理コンソール端末からの操作要求が一定時間の行われなかった際には必ずセションタイムアウト機能が呼び出され成功することが保証される。

SF.ROLE_MANAGE によって、環境定義ファイルに対する操作要求時に、操作者のロールを確認し、操作実行可否を制御する仕組みが必ず呼び出され成功することが保証される。

SF.AUTO_RECOVER によって、自動再起動対象のアプリケーション実行プロセスが異常終了し、アプリケーション動作を維持できない障害が発生した場合に、当該アプリケーション実行プロセスを再起動する仕組みが必ず呼び出され成功することが保証される。

SF.TIMER によって、強制停止対象のアプリケーションの処理が遅延し、アプリケーション動作を維持できない傷害が発生した場合に、当該アプリケーションを強制停止する仕組みが必ず呼び出され成功することが保証される。

従って、SF.ID_AUTH、SF.CRYPTO、SF.SESSION、SF.ROLE_MANAGE、SF.AUTO_RECOVER 及び SF.TIMER の実装により FPT_RVM.1 を実現できる。

FPT_SEP.1

FPT_SEP.1 は、信頼できないサブジェクトによる干渉や改ざんから TSF 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の分離を実施することを要求するセキュリティ機能要件である。

このセキュリティ機能を実現するためには、ユーザ認証機能、SSL 暗号通信機能、セションタイムアウト機能、ロール制御機能、アプリケーション自動再起動機能及びサーバアプリケーションタイマ機能が、信頼できないサブジェクトによる影響を受けずに実行するためのセキュリティドメインの保証が必要である。

SF.ID_AUTH、SF.CRYPTO、SF.SESSION、SF.ROLE_MANAGE、SF.AUTO_RECOVER 及び SF.TIMER によって、信頼できないサブジェクトによる干渉と改ざんから保護するために、各セキュリティ機能が実行するためのセキュリティドメインが維持されることが保証される。

従って、SF.ID_AUTH、SF.CRYPTO、SF.SESSION、SF.ROLE_MANAGE、SF.AUTO_RECOVER 及び

SF.TIMER の実装により FPT_SEP.1 を実現できる。

FRU_FLT.1

FRU_FLT.1 は、アプリケーション実行プロセスが異常終了もしくはアプリケーションの処理遅延状態に陥り、アプリケーション動作を維持できない障害が発生した際に、ワークユニット定義に従ったアプリケーション動作の保証を要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、アプリケーション実行プロセスの異常終了またはアプリケーションの処理遅延の障害が発生した際に、アプリケーションの強制停止やアプリケーション実行プロセスの再起動を行い、アプリケーション実行プロセスの動作を維持する機能の実装が必要である。

SF.AUTO_RECOVER によって、Configurators もしくは Administrators による停止操作以外の原因で異常終了したアプリケーション実行プロセスを再起動させ、アプリケーション実行プロセスの動作を維持することができる。

SF.TIMER 及び SF.AUTO_RECOVER によって、Configurators もしくは Administrators によって規定された処理時間を超えても処理を完了せず、処理遅延状態に陥ったと見なすアプリケーションを強制停止させた後に再起動され、アプリケーション実行プロセスの動作を維持することができる。

従って、SF.AUTO_RECOVER 及び SF.TIMER の実装により FRU_FLT.1 を実現できる。

FTA_SSL.3

FTA_SSL.3 は、Interstage 管理コンソールに対する最後の操作要求から Administrators が設定した時間の経過後に、管理コンソール端末との間のセションを切断することを要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、管理コンソール端末から Interstage 管理コンソールに対する操作要求を確認し、一定の非アクティブ時間経過後にセションを切断する機能の実装が必要である。

SF.SESSION によって、セションタイムアウト時間を設定し、この時間に基づいたセションの切断管理を行うことができる。

従って、SF.SESSION の実装により FTA_SSL.3 を実現できる。

FTP_TRP.1

FTP_TRP.1 は、TSF とリモート利用者間の間の通信を高信頼パスによって実現することを要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、リモート利用者である操作者が Interstage 管理コンソールを利用する際に、高信頼パスの使用を要求する機能の実装が必要である。

SF.CRYPTO によって、操作者による管理コンソール端末を使用した Interstage 管理コンソールの利用時には、その間の通信を必ず SSL/TLS プロトコルで制御された通信によって行うことができる。すなわち、リモート利用者である操作者から Interstage 管理コンソールに対するアクセス要求があった際には、SSL/TLS プロトコルによる端点の保証された高信頼パスを介して通信を開始することができる。

従って、SF.CRYPTO の実装により FTP_TRP.1 を実現できる。

8.3.2. セキュリティ機能強度根拠

本 TOE において、確率的または順列的メカニズムに基づくセキュリティ機能は、SSL 暗号通信機能であり、暗号メカニズムを採用している。SSL 暗号通信機能では、128 ビット以上の暗号アルゴリズムを利用して、管理コンソール端末と Interstage 管理コンソール間の通信データの暗号化処理を行うことで、セキュリティを保証している。

また、ユーザ認証機能によって認証された状態の維持を行うためにセション情報を利用しており、確率的または順列的メカニズムが採用されている。十分な長さを有した一意なセション情報を利用することで、セション情報の推測によるセション乗っ取りからセキュリティを保証している。

従って、SSL 暗号通信機能とユーザ認証機能の強度は、低レベルの攻撃能力を持つ攻撃者に対して十分に対抗することができるため、機能強度として SOF-基本が妥当であると判断する。また、SOF-基本は**エラー！参照元が見つかりません。**で主張した機能強度レベルと一貫している。

8.3.3. 保証手段根拠

本節では、保証手段がすべてのセキュリティ保証要件を満足していることを示す。

表 6.3 に示したように、全てのTOEセキュリティ保証要件は、保証手段として識別されたドキュメントのセットによって対応付けられる。

以下に、TOE セキュリティ保証要件のセットが保証手段によって満たされる根拠を示す。

ACM_CAP.2　　構成要素

保証手段である「Interstage Application Server 8.0.0 構成管理手順書」、「Interstage Application Server 8.0.0 構成管理要素リスト（プログラム)」、「Interstage Application Server 8.0.0 構成管理要素リスト（文書)」には、TOE のバージョンを識別するための命名規則、構成要素の一覧表、構成要素の一意の識別方法が規定されている。これにより、TOE セキュリティ保証要件 ACM_CAP.2 は満たされる。

ADO_DEL.1　　配付手続き

保証手段である「Interstage Application Server 8.0.0 配付規定」及び「Interstage Application Server 8.0.0 緊急修正の配付規定」には、TOE を利用者サイトに配付し、利用者サイトで必要な TOE の緊急修正を取得する際に採用される、TOE のセキュリティを維持するための手続きが規定されている。これにより TOE セキュリティ保証要件 ADO_DEL.1 は満たされる。

ADO_IGS.1　　設置、生成、及び立上げ手順

保証手段である「Interstage Application Server インストールガイド －Linux－」及び「ソフトウェア説明書 Interstage Application Server Enterprise Edition 8.0.3 (64bit Linux 対応版)」には、TOE をセキュアな構成にするために採用される、設置手順及び起動の確認方法が規定されている。これにより TOE セキュリティ保証要件 ADO_IGS.1 は満たされる。

ADV_FSP.1　　非形式的機能仕様

保証手段である「Interstage Application Server 8.0.0 機能仕様書」には、TOE のセキュリティ機能に対する全ての外部インタフェースの仕様が規定されている。これにより TOE セキュリティ保証要件 ADV_FSP.1 は満たされる。

ADV_HLD.1　　記述的上位レベル設計

保証手段である「Interstage Application Server 8.0.0 上位レベル設計書」には、TSF を分割したサブシステムの仕様及びサブシステムに対するインタフェースの仕様が規定されている。これにより TOE セキュリティ保証要件 ADV_HLD.1 は満たされる。

ADV_RCR.1　　非形式的対応の実証

保証手段である「Interstage Application Server 8.0.0 表現対応表」には、TOE のセキュリティ機能の各レベル（要約仕様－機能仕様－上位レベル設計）での完全な対応が示されている。これにより TOE セキュリティ保証要件 ADV_RCR.1 は満たされる。

AGD_ADM.1　　管理者ガイダンス

保証手段である「Interstage Application Server 運用ガイド」、「Interstage Application Server セキュリティシステム運用ガイド」、「Interstage Application ServerOLTP サーバ運用ガイド」、「Interstage Application Server メッセージ集」及び「Interstage Application Server インストールガイド －Linux－」には、TOE の Administrators 及び Configurators が使用するインタフェース、TOE をセキュアに運用するための警告を含む使用方法及び TOE の障害時に Administrators が執るべきアクションが規定されている。これにより TOE セキュリティ保証要件 AGD_ADM.1 は満たされる。

AGD_USR.1　　利用者ガイダンス

保証手段である「Interstage Application Server 運用ガイド」、「Interstage Application Server セキュリティシステム運用ガイド」、「Interstage Application ServerOLTP サーバ運用ガイド」、「Interstage Application Server メッセージ集」及び「Interstage Application Server インストールガイド －Linux－」には、TOE の Administrators 及び Configurators が使用するインタフェース、TOE をセキュアに運用するための警告を含む使用方法が規定されている。これにより TOE セキュリティ保証要件 AGD_USR.1 は満たされる。

ATE_COV.1　　カバレージの証拠

保証手段である「Interstage Application Server 8.0.0 カバレージ分析書」には、TOE のセキュリティ機能及び外部インタフェースに対するテストの十分性が示されている。これにより TOE セキュリティ保証要件 ATE_COV.1 は満たされる。

ATE_FUN.1　　機能テスト

保証手段である「Interstage Application Server 8.0.0 テスト計画書」、「Interstage Application Server 8.0.0 テスト仕様書」及び「Interstage Application Server 8.0.0 テスト項目書」には、TSF に対するテストの全体計画、テストを実施するための手順及びテスト結果が記載されている。これにより TOE セキュリティ保証要件 ATE_FUN.1 は満たされる。

ATE_IND.2　　独立テスト - サンプル

保証手段である「TOE」は、TOE セキュリティ機能のテスト環境の再現、及び、テストに適した TOE を提供する。これにより、TOE セキュリティ保証要件 ATE_IND.2 は満たされる。

AVA_MSU.1　　ガイダンスの検査

保証手段である「Interstage Application Server 運用ガイド」、「Interstage Application Server セキュリティシステム運用ガイド」、「Interstage Application ServerOLTP サーバ運用ガイド」、「Interstage Application Server メッセージ集」、「Interstage Application Server インストールガイド －Linux－」及び「ソフトウェア説明書 Interstage Application Server Enterprise Edition 8.0.3 (64bit Linux 対応版)」には、TOE の利用者が誤使用により TOE のセキュリティ機能を非セキュアな状態にしてしまう危険性が無いように TOE の使用方法を記載している。これにより保証要件 AVA_MSU.1 は満たされる。

AVA_SOF.1　　TOE セキュリティ機能強度評価

保証手段である「Interstage Application Server 8.0.0 脆弱性分析書」には、SSL 暗号通信機能に対するセキュリティ機能強度が SOF-基本を満たすことが説明されている。これ

により、TOE セキュリティ保証要件 AVA_SOF.1 は満たされる。

AVA_VLA.1　　開発者脆弱性分析

保証手段である「Interstage Application Server 8.0.0 脆弱性分析書」には、TOE の意図する環境において、セキュリティ機能の脆弱性が悪用され得ないことが説明されている。これにより TOE セキュリティ保証要件 AVA_VLA.1 は満たされる。

8.4. PP 主張根拠

本 ST が参照する PP はない。

（　最終ページ　）