# 汚染拡大防止システム SHIELD/ExLink-IA セキュリティターゲット バージョン 1.0i

2007/03/05

株式会社　日立情報システムズ

## -更新履歴-

| バージョン | 更新日 | 内容 | 作成 | 審査 | 承認 |
|---|---|---|---|---|---|
| 1.00 | 2006/10/30 | 新規作成 | 小松 | 佐々木 | 藤井 |
| 1.01 | 2006/11/01 | (1)ST 名称を変更<br>(2)セキュリティデバイスの定義を変更<br>(3)TOE の種別を変更 | 小松 | 佐々木 | 藤井 |
| 1.02 | 2006/11/07 | 指摘事項修正 | 小松 | 佐々木 | 藤井 |
| 1.03 | 2006/11/13 | 指摘事項修正 | 小松 | 佐々木 | 藤井 |
| 1.04 | 2006/11/27 | 指摘事項修正 | 小松 | 佐々木 | 藤井 |
| 1.05 | 2006/12/12 | 指摘事項修正 | 小松 | 佐々木 | 藤井 |
| 1.06 | 2006/12/20 | 指摘事項修正 | 小松 | 佐々木 | 藤井 |
| 1.07 | 2007/01/04 | 指摘事項修正 | 小松 | 佐々木 | 藤井 |
| 1.08 | 2007/01/15 | 指摘事項修正 | 小松 | 佐々木 | 藤井 |
| 1.09 | 2007/01/18 | 指摘事項修正 | 小松 | 佐々木 | 藤井 |
| 1.0a | 2007/01/23 | 指摘事項修正 | 小松 | 佐々木 | 藤井 |
| 1.0b | 2007/01/29 | 指摘事項修正 | 小松 | 佐々木 | 藤井 |
| 1.0c | 2007/02/02 | 指摘事項修正 | 小松 | 佐々木 | 藤井 |
| 1.0d | 2007/02/06 | 指摘事項修正 | 小松 | 佐々木 | 藤井 |
| 1.0e | 2007/02/16 | 指摘事項修正 | 小松 | 佐々木 | 藤井 |
| 1.0f | 2007/02/23 | 指摘事項修正 | 小松 | 佐々木 | 藤井 |
| 1.0g | 2007/02/27 | 指摘事項修正 | 小松 | 佐々木 | 藤井 |
| 1.0h | 2007/03/02 | 指摘事項修正 | 小松 | 佐々木 | 藤井 |
| 1.0i | 2007/03/05 | 指摘事項修正 | 小松 | 佐々木 | 藤井 |

*Microsoft、Windows、SQL Server（その他商標・登録商標名）は、米国 Microsoft Corporation の米国及びその他の国における登録商標です。
*Windows の正式名称は、Microsoft Windows Operating System です。
*ISS は、Internet Security Systems, Inc.の商標です。
*Proventia GX は、Internet Security Systems, Inc.の登録商標です。
*Check Point, FireWall-1, NG, NGX, VPN-1, VPN-1 SecuRemote は、Check Point Software Technologies Ltd. あるいはその関連会社の商標または登録商標です。
*その他記載されている会社名、製品名及びサービス名は、すべて各社の登録商標または商標です。

-目次-

# １．ST 概説

## １．１．ST 識別

### １．１．１．ST 識別名称

ST 名称：　　汚染拡大防止システム SHIELD/ExLink-IA セキュリティターゲット
バージョン：　　1.0i
作成者：　　株式会社　日立情報システムズ
作成日：　　2007 年 03 月 05 日

CC のバージョン：
・Common Criteria for Information Technology Security Evaluation Version 2.3
・補足-0512

### １．１．２．TOE 識別名称

TOE 名称：　　汚染拡大防止システム SHIELD/ExLink-IA
バージョン：　　1.0
製造者：　　株式会社　日立情報システムズ

## １．２．ST 概要

このドキュメントは汚染拡大防止システム SHIELD/ExLink-IA(以下、ExLink-IA とする)のセキュリティターゲットである。ExLink-IA は FW と IPS から取得した情報を SOC へ送信する。また、SOC にて作成された FW 設定変更指示を受け取りに行き、該当する FW へ適用し、FW の設定変更を行うネットワーク管理ソフトウェアである。

## １．３．適合する PP

適合するプロテクションプロファイルはない。

## １．４．CC 適合

本 ST の CC 適合性は以下の通りである。
・CC パート 2 適合
・CC パート 3 適合
・パッケージ適合：EAL1

## １．５．参考資料

・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 CCMB-2005-08-001
平成 17 年 12 月翻訳第 1.0 版, 独立行政法人情報処理推進機構セキュリティセンター
・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 CCMB-2005-08-002
平成 17 年 12 月翻訳第 1.0 版, 独立行政法人情報処理推進機構セキュリティセンター
・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 CCMB-2005-08-003
平成 17 年 12 月翻訳第 1.0 版, 独立行政法人情報処理推進機構セキュリティセンター
・補足-0512
平成 17 年 12 月　独立行政法人情報処理推進機構セキュリティセンター
・Common Criteria for Information Technology Security Evaluation
Part1: Introduction and general model
Version 2.3 August 2005, CCMB-2005-08-001
・Common Criteria for Information Technology Security Evaluation
Part2: Security functional requirements
Version 2.3 August 2005, CCMB-2005-08-002
・Common Criteria for Information Technology Security Evaluation
Part3: Security assurance requirements
Version 2.3 August 2005, CCMB-2005-08-003

# 2．TOE 記述

## 2．1．TOE の種別

TOE はセキュリティログ情報の収集を行い SOC に設置している i-Monitor に送信し、送信されたセキュリティログ情報を元に SOC オペレータが作成する FW 設定変更指示を i-Monitor へ受け取りに行き、該当する FW へ反映するネットワーク管理ソフトウェア製品である。

## 2．2．TOE の物理構成

本 TOE の物理構成を図 2-1 に示す。TOE は、IA マネージャ、IA エージェント、管理コンソールである。管理コンソール端末を除く IA システムはセキュアルームに設置され、管理コンソール端末は一般業務スペースに設置される事を想定している。セキュアルームにおいて FireWall-1 は社内外の境界環境にて運用される事を想定している。一般業務スペースに設置される管理コンソール端末は FireWall-1 との間を VPN ソフトウェアによって暗号化し、この間の通信を傍受から保護される事を想定している。また管理コンソール端末は FireWall-1 から発行される証明書を用いて FireWall-1 と認証を行う事によって、なりすましから防止される事を想定している。

i-Monitor は SOC オペレータのみが入退出できる SOC にて運用される事を想定している。IA マネージャと IA エージェント及び IADB と QuDB は、同一マシン上で運用されるものとする。

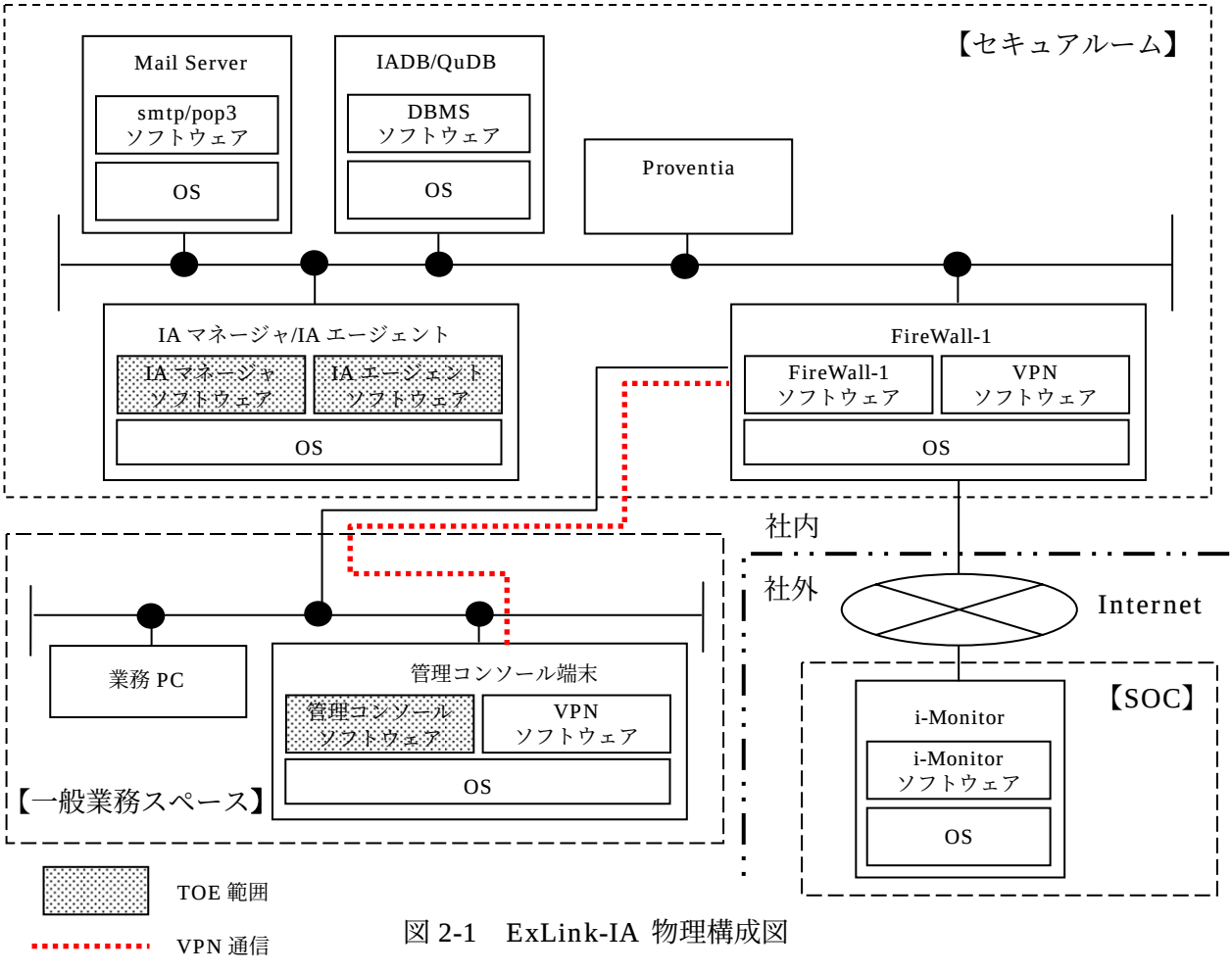


図 2-1　ExLink-IA 物理構成図

以下に、各システムにおける役割を記述する。

・IA マネージャ

ExLink-IA の管理を行うソフトウェアである。i-Monitor へ FW 設定変更指示を受け取りに行き、変更内容の分析を行う。その後 IADB へ接続し、設定変更対象の FireWall-1 を管理している IA エージェントを検索する。検索結果から該当する IA エージェントに対して FW 設定変更指示を送信する。IA エージェントが持つ IA エージェントログ情報と QuDB が持つ Qu クライアント検疫情報を収集し、セキュリティログ情報として i-Monitor へ送信する。IADB にアクセスするための ID、パスワードを有しており、管理コンソールから取得要求に対して ID、パスワードを提供する。

・IA エージェント

FireWall-1、Proventia と IA マネージャとの通信を仲介するソフトウェアである。IA マネージャから FW 設定変更指示を受信後、自身の管理下にある設定変更対象の FireWall-1 に対して FW 設定変更指示を行う。また、FireWall-1、Proventia から収集した情報を IA エージェントログ情報として IA マネージャへ送信する。

・管理コンソール

ExLink-IA の管理 GUI ソフトウェアである。ExLink 管理者及び ExLink 利用者が利用する。ExLink 管理者及び ExLink 利用者はそれぞれの付与された操作可能範囲内で、「表 2-4 IADB 情報に含まれる情報と操作範囲」に示される IADB 情報の参照、編集、削除を行う。管理コンソールの操作対象は IADB であり、IADB にアクセスする際に IA マネージャにアクセスし、IADB にアクセスするための ID、パスワードの取得を行い、IADB にアクセスを行う。また、VPN ソフトウェアである VPN-1 SecuRemote を用いる事で管理コンソール端末 - FireWall-1 間の通信を暗号化する。また FireWall-1 から発行される証明書を用いて FireWall-1 と認証を行う。

・IADB

IADB は ExLink-IA が使用する DB である。IA マネージャ、管理コンソールからのアクセス要求に対して情報の提供を行う。「表 2-4　IADB 情報に含まれる情報と操作範囲」に示される情報を有している。

・FireWall-1

FireWall-1 は FW ソフトウェアである。ExLink-IA との連携では、IA エージェントより受信した FW 設定変更指示に基づき、自身の設定変更を行う。また IA エージェントからのログ取得要求に対して FW アクセスログの送信を行う。FireWall-1 は VPN ソフトウェアである VPN-1 を用いる事で管理コンソール端末 - FireWall-1 間の通信を暗号化する。また管理コンソール端末に対して証明書を発行し、証明書による認証を行う。

・Proventia

Proventia は IPS である。ExLink-IA との連携では、インシデントが発生するたびに IA エージェントに対して IPS インシデント情報を送信する。

・QuDB

QuDB は ExLink-Qu が使用する DB である。ExLink-IA との連携では、IA マネージャの Qu クライアント検疫情報取得要求に対して、Qu クライアント検疫情報を IA マネージャへ送信する。

・Mail Server

IA マネージャより送信される FW 設定変更結果のメールを送受信するメールサーバである。

・i-Monitor

FireWall-1 に対する FW 設定変更指示の配布及び IA マネージャより送信されるセキュリティログ情報を取得するソフトウェアである。取得した情報は SOC オペレータが分析する。分析の結果、FW 設定変更が必要な場合は SOC オペレータが FW 設定変更指示を作成する。作成した FW 設定変更指示は、該当する FireWall-1 を管理する IA マネージャが受け取りにくる。

なお、SOC は株式会社日立情報システムズにて運営しているものを利用する事を前提とする。

TOE を動作させるための必須スペック要件を表 2-1 に示す。

表 2-1　TOE 必須スペック要件

| No. | 対象 | 要件 | 備考 |
|---|---|---|---|
| 1 | IA マネージャ<br>/ IA エージェント | 【動作環境 OS】<br>Windows Server 2003<br>Standard Edition SP1 以降<br>Internet Explorer 6 以上<br><br>【必須ハードウェアスペック】<br>CPU：550MHz 以上<br>Memory：256 MB 以上<br>HDD：5GB 以上 | ■OS は 32bit 版のみ対応<br>■IA マネージャは i-Monitor と SSL 通信を行う際 Windows Server 2003 の機能である CryptoAPI,Windows HTTP Service の 2 つを用いる。これらの機能は以下のライブラリによって実現される。<br>・Crypt32.dll<br>・Winhttp.dll |
| 2 | 管理コンソール | 【動作環境 OS】<br>Windows 2000 Professional SP4 以降<br>Windows XP Professional SP2 以降<br><br>【必須ソフトウェア】<br>.Net Framework 1.1<br>VPN-1 SecuRemote<br>（Check Point 社の VPN ソフトウェア）<br><br>【必須ハードウェアスペック】<br>CPU：300MHz 以上<br>Memory：128 MB 以上<br>HDD：3GB 以上 | ■ .net Framework 1.1 及び VPN-1 SecuRemote は予めインストールする必要がある。 |

## ２．３．TOE の論理構成

本 TOE の論理構成を図 2-2 に示す。管理コンソールは ExLink-IA の設定を行うための管理 GUI であり、IA マネージャから IADB のアカウント情報を取得後、IADB 上の情報に対して参照、編集、削除を実施する。

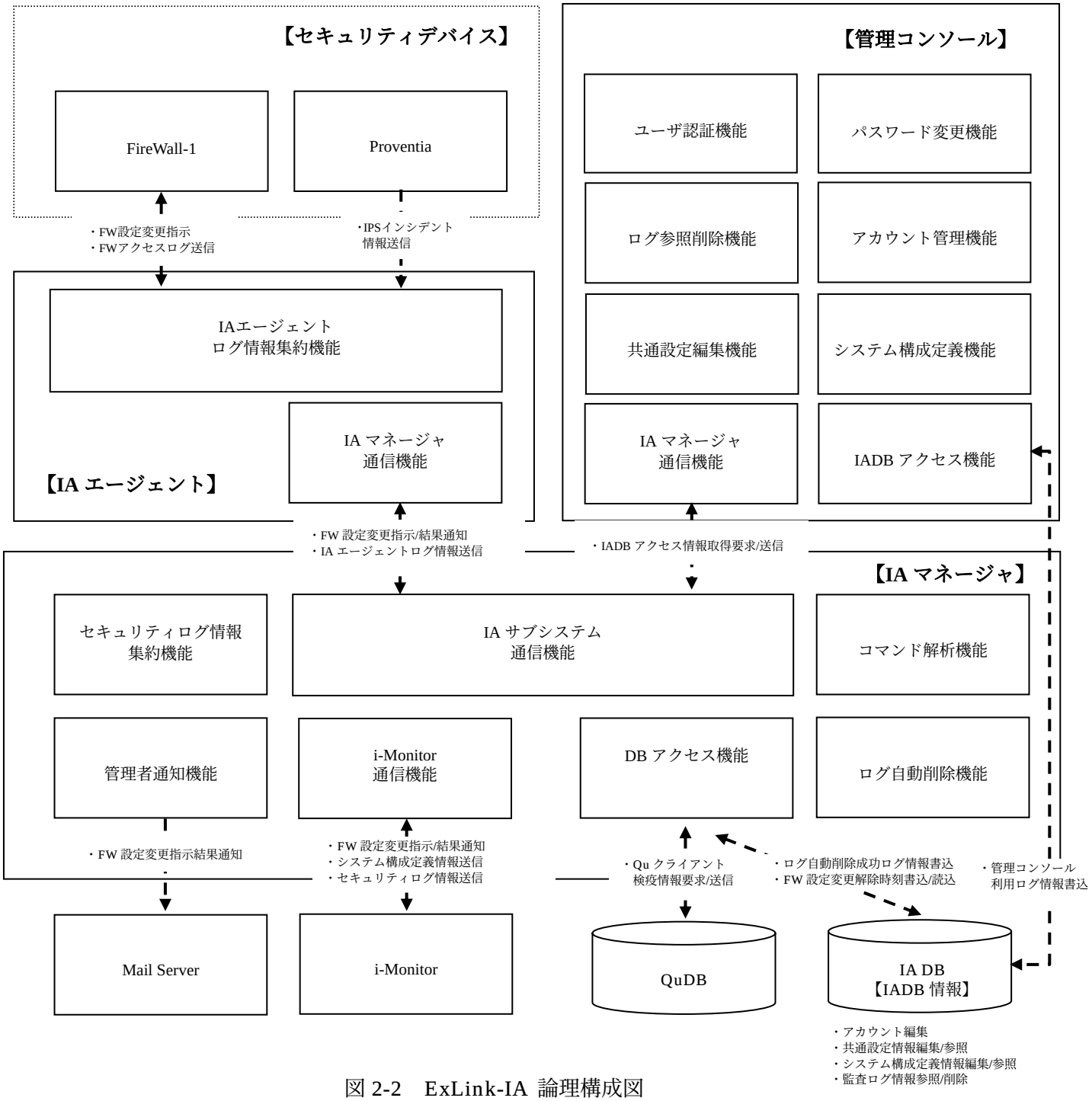


図 2-2　ExLink-IA 論理構成図

## ２．４．TOE のセキュリティ機能

TOE のセキュリティ機能を以下に示す。

表 2-2　TOE のセキュリティ機能

| 構成要素 | 機能 |
|---|---|
| IA マネージャ | ・ログ自動削除機能<br>IADB に保管された監査ログ情報が指定された保管期間あるいは保管件数を超えた場合、自動的に削除する機能。ログ自動削除の成功はログ自動削除成功ログ情報として IADB に保管される。 |
| 管理コンソール | ・ユーザ認証機能<br>管理コンソールにログオンする際、ログオン画面でユーザ ID とパスワードを用いて識別認証を行う機能。識別認証の成功及び失敗は管理コンソール利用ログ情報として IADB に保管される。<br><br>・アカウント管理機能<br>管理コンソールにログオンする際に用いるユーザ ID の追加、参照、削除を行う機能。本機能は ExLink 管理者のみ実行可能である。<br><br>・パスワード変更機能<br>ExLink 管理者及び ExLink 利用者自身のパスワードを変更する機能。パスワード変更時に自身のユーザ ID を参照する事が可能である。<br><br>・ログ参照削除機能<br>IADB 内に保管されている監査ログ情報の参照、削除を行う機能。ExLink 管理者（ログの削除権限を持つ ExLink 利用者を含む）は参照及び削除可能。ExLink 利用者は参照のみ可能。 |

## ２．５．TOE の一般機能

TOE の一般機能を表 2-3 に示す。

表 2-3　TOE の一般機能(1/2)

| 構成要素 | 機能 |
|---|---|
| IA マネージャ | ・i-Monitor 通信機能<br>i-Monitor 側で作成された FW 設定変更指示を受け取りに行く機能。受け取った FW 設定変更指示は IADB へ保管する。またセキュリティログ情報集約機能で収集したセキュリティログ情報、IADB から収集するシステム構成定義情報を i-Monitor へ送信する。<br><br>・IA サブシステム通信機能<br>IA サブシステムである IA エージェント、管理コンソールと通信を行う機能。IA マネージャは IA エージェントから IA エージェントログ情報を取得する。また IA マネージャは IA エージェントへ FW 設定変更指示の送信を行う。管理コンソールには IADB にアクセスするための ID、 パスワードを送信する。<br><br>・DB アクセス機能<br>IADB、QuDB へアクセスを行う機能。<br><br>・セキュリティログ情報集約機能<br>IA エージェントから取得する IA エージェントログ情報と QuDB から取得する Qu クライアント検疫情報を収集する機能。<br><br>・コマンド解析機能<br>i-Monitor から受信した FW 設定変更指示を解析する機能。IADB にアクセスし、設定変更対象機器を管理下に持つ IA エージェントの検索を行う。<br><br>・管理者通知機能<br>Mail Server へ FW 設定変更結果を送信する機能。 |

表 2-3　TOE の一般機能(2/2)

| 構成要素 | 機能 |
|---|---|
| IA エージェント | ・IA マネージャ通信機能<br>IA マネージャと通信を行う機能。<br><br>・IA エージェントログ情報集約機能<br>FireWall-1、Proventia から FW アクセスログ及び IPS インシデント情報を収集し、IA エージェントログ情報として IA マネージャへ送信する機能。 |
| 管理コンソール | ・IA マネージャ通信機能<br>IA マネージャと通信を行う機能。IA マネージャから IADB にアクセスするための ID、パスワードを取得する。<br><br>・IADB アクセス機能<br>IA マネージャ通信機能を用いて取得した IADB にアクセスするための ID、パスワードを用いて IADB と通信を行う機能。<br><br>・共通設定編集機能<br>IADB 内に保管されている基本設定情報、ログ設定情報の編集及びライセンス情報の登録を行う機能。ExLink 管理者（共通設定の編集権限を持つ ExLink 利用者を含む）は基本設定情報、ログ設定情報の参照及び編集可能。ExLink 利用者は参照のみ可能。またライセンス情報は ExLink 管理者、ExLink 利用者ともに登録及び参照が可能。<br><br>・システム構成定義機能<br>IADB内に保管されているシステム構成定義情報及びCSO４Uサービスの設定情報、CSO4U サービスの遠隔制御情報の編集を行う機能。ExLink 管理者（システム構成定義の編集権限を持つ ExLink 利用者を含む）のみ参照及び編集可能。ExLink 利用者は参照のみ可能。 |

## ２．６．TOE の関与者

本 TOE の関与者の役割を以下に記す。

・ExLink 管理者

ExLink-IA における admin アカウントを有しており、IA システムを管理する者。セキュアルーム、一般業務スペースへの入退出が可能である。ExLink 管理者は管理コンソールのアカウント管理機能を使用して ExLink 利用者のユーザ ID の追加、参照、削除が可能である。
ExLink 管理者は初期設定にて以下の操作が可能である。
-アカウント管理
-共通設定編集
-システム構成定義編集
-ログ参照削除
ExLink 管理者は組織の責任者が適任者を人選し任命する。
なお、共通設定の編集権限、システム構成定義の編集権限及びログの削除権限のいずれか一つ以上を付与された ExLink 利用者は、それぞれ共通設定編集、システム構成定義編集及びログ削除の操作に関して ExLink 管理者と同等の操作が可能であるので、これらの権限を持つ ExLink 利用者については ExLink 管理者と同等とみなし、以降 ExLink 管理者に含めるものとする。

・ExLink 利用者

ExLink 管理者から付与されたアカウントを用いて、IA システムを管理する者。
セキュアルーム、一般業務スペースへの入退出が可能である。
ExLink 利用者は初期設定にて、以下の操作が可能である。
-共通設定参照
-システム構成定義参照
-ログ参照
ExLink 利用者は組織の責任者が適任者を人選し任命する。

・SOC オペレータ

IA マネージャから i-Monitor へ送信されるセキュリティログ情報を元に、FW 設定変更指示を作成する者。
SOC への入退出が可能である。
SOC オペレータは SOC の責任者が適任者を人選し任命する。

・組織の責任者

お客様組織において、ExLink-IA の運用における決定権を有する人物。

ExLink 管理者及び ExLink 利用者の人選、任命と信頼できる SOC の選択を行う。

・第三者

一般業務スペースへの立ち入りが可能であり、ExLink-IA のアカウントを持たない者。

## ２．７．TOE が保護する資産

本 TOE が保護する資産は IADB 情報とセキュリティログ情報である。IADB 情報に含まれる情報及びその操作範囲を表 2-4、セキュリティログ情報に含まれる情報とその操作範囲を表 2-5 に示す。

表 2-4　IADB 情報に含まれる情報と操作範囲 (1/2)

| IADB 情報に含まれる情報 | 内訳 |
|---|---|
| ■共通設定情報 | ・基本設定情報<br><br>基本設定情報は、DB の整理開始時間及び整理対象の IP アドレス、また管理者へ情報を通知するためのメールサーバの IP アドレスやメールアドレスを有している。<br>ExLink 管理者は基本設定情報の参照及び編集可能であり、ExLink 利用者は参照のみ可能である。 |
| | ・ログ設定情報<br><br>ログ設定情報は、監査ログ情報における自動削除の有無及びその保管期間、保管件数の閾値情報を有している。<br>ExLink 管理者は参照及び編集可能であり、ExLink 利用者は参照のみ可能である。 |
| | ・ライセンス情報<br><br>ライセンス情報は、ExLink-IA を利用する際に登録するライセンスの情報を有している。ExLink 管理者、ExLink 利用者ともに登録及び参照が可能である。 |
| | ・パスワード情報<br><br>パスワード情報は、管理コンソールを利用する ExLink 管理者及び ExLink 利用者のパスワードを有している。ExLink 管理者、ExLink 利用者は自身のパスワードのみ変更可能である。 |
| ■SHIELD/ExLink-IA 管理情報 | ・システム構成定義情報<br><br>システム構成定義情報は、ExLink-IA で使用する管理コンソール、Mail Server を除く IA システムのシステム名、システム種別、IP アドレス情報を有している。<br>ExLink 管理者は参照及び編集可能であり、ExLink 利用者は参照のみ可能である。 |

表 2-4　IADB 情報に含まれる情報と操作範囲 (2/2)

| IADB 情報に含まれる情報 | 内訳 |
|---|---|
| ■SHIELD/ExLink-IA 管理情報 | ・CSO4U サービスの設定情報<br><br>CSO4U サービスの設定情報は、CSO4U サービスの提供先 URL 及びサービス取得間隔、セキュリティログ情報送信先 URL 及び送信間隔、ExLink 管理者名と ExLink 管理者メールアドレス情報を有している。<br>ExLink 管理者は参照及び編集可能であり、ExLink 利用者は参照のみ可能である。 |
| | ・CSO4U サービスの遠隔制御情報<br><br>CSO4U サービスの遠隔制御情報は、i-Monitor から送信されてくる FW 設定変更指示を有している。指示内容には制御対象とその制御内容が含まれている。<br>ExLink 管理者は参照及び編集可能であり、ExLink 利用者は参照のみ可能である。 |
| ■監査ログ情報 | ・監査ログ情報<br><br>監査ログ情報は、管理コンソール利用ログ情報とログ自動削除成功ログ情報を有している。<br>ExLink 管理者は参照及び削除可能であり、ExLink 利用者は参照のみ可能である。 |

表 2-5　セキュリティログ情報に含まれる情報と操作範囲

| セキュリティログ情報に含まれる情報 | 内訳 |
|---|---|
| ■IA エージェントログ情報 | ・IA エージェントログ情報<br><br>IA エージェントログ情報は、IA エージェントが自身の管理下にある FireWall-1 から取得した FW アクセスログと、Proventia から送信される IPS インシデント情報を有している。<br>IA エージェントログ情報は、IA マネージャから i-Monitor へ送信する際に IADB に保管されないため、管理コンソール上から確認する事ができない。よって ExLink 管理者、ExLink 利用者ともに参照及び削除する事は不可能である。 |
| ■Qu クライアント検疫情報 | ・Qu クライアント検疫情報<br><br>Qu クライアント検疫情報は、ExLink-Qu が管理しているクライアント PC の検疫情報を有している。検疫情報には、OS のパッチ適用状況、ウィルスチェックソフトウェアにおける最新のウィルス定義ファイル適用状況が含まれている。<br>Qu クライアント検疫情報は、IA マネージャから i-Monitor へ送信する際に IADB に保管されないため、管理コンソール上から確認する事ができない。よって ExLink 管理者、ExLink 利用者ともに参照及び削除する事は不可能である。 |

# ３．TOE セキュリティ環境

本章では、ST が意図している TOE の運用環境や使用方法、保護すべき資産に対する脅威、及び TOE が従うべき組織のセキュリティ方針を定義する。

## ３．１．前提条件.

TOE のセキュアな運用のための前提条件を以下に示す。

A.PHYSICAL_ACCESS（物理環境）
管理コンソール端末を除く IA システムを構成する機器群は、ExLink 管理者及び ExLink 利用者のみが物理的にアクセスできるセキュアルームに設置されるものと想定する。

A.NETWORK（ネットワーク環境）
管理コンソール端末は、一般業務スペース、i-Monitor は SOC に接続され、これらの管理コンソール端末及び i-Monitor は、FireWall-1 で隔離された管理コンソール端末以外の IA システムに FireWall-1 を介して接続されるものと想定する。

A.DB_PASSWORD（IADB のアクセス保護）
IADB は、ExLink-IA が使用する DB であり、IA マネージャ及び管理コンソールのアカウントと DB を管理するためのアカウントだけがアクセスできるようアカウント管理されているものと想定する。

A.CONSOLE（管理コンソール端末の管理）
管理コンソール端末は、不正なソフトウェアがインストールされないよう管理されているものと想定する。

A.TRUST_USER（お客様組織の信頼）
ExLink管理者及びExLink利用者は、IAシステムの管理運用を行うために必要な能力を持ち、不正行為を働かない信頼できる者と想定する。

A.TRUST_SOC（SOC の信頼）
SOC を運営する組織は、SOC 内において SOC オペレータのみ i-Monitor を操作できるよう管理を行っている事、SOC オペレータに対して、i-Monitor を操作するために必要な訓練を行っており、不正行為を働かない信頼できる者を擁していると想定する。
なお、ExLink-IA に対して唯一指示を出す事ができる i-Monitor は、株式会社 日立情報システムズの SOC にのみ設置されているものと想定する。

## ３．２．脅威

本 TOE が守るべき資産は IADB 情報である。これに対して想定される脅威を以下に示す。
なお攻撃者の攻撃能力は低いと想定している。

T.ILLEGAL_OPERATION（不正操作）
第三者が管理コンソール端末を用いて IADB 情報を不正に参照、編集及び削除するかもしれない。

T.ENVIRONMENT_PROBE（接続環境における盗聴）
第三者が管理コンソール端末以外の機器を用いて管理コンソールと IA マネージャ間あるいは管理コンソールと IADB 間の通信を盗聴し、IADB 情報を不正に入手し暴露するかもしれない。

T.ENVIRONMENT_SPOOFING（接続環境におけるなりすまし）
第三者が一般業務スペース内で管理コンソール端末以外の機器を用いて TOE の正当な利用者になりすまして IA マネージャや IADB に不正アクセスし、IADB 情報を参照、編集及び削除するかもしれない。

T.COMMUNICATION_PROBE（通信の盗聴）
第三者が IA マネージャから i-Monitor への通信を盗聴し、FW 設定変更指示やセキュリティログ情報及びシステム構成定義情報を不正に入手し暴露するかもしれない。

## 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

## ４．１．TOE のセキュリティ対策方針

O.IDENTIFICATION（識別認証）

TOE は利用される前に必ず識別認証を行い、識別認証に成功した ExLink 管理者及び ExLink 利用者に対してのみ接続を許可しなければならない。

O.AUDIT（ログ証跡）

TOE は識別認証の成功及び失敗ログを取得し、ExLink 管理者及び ExLink 利用者が閲覧できるようにしなければならない。

## ４．２．環境の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.ENVIRONMENT（構成機器の接続環境）

FireWall-1 は、FireWall-1 が発行する証明書を用いてセキュアルーム内にある IA マネージャ、IADB との接続を試みる管理コンソール端末の認証を行い、認証に成功した管理コンソール端末- FireWall-1 間の通信に対して VPN 接続による暗号化通信を実現しなければならない。

OE.SSL（SSL 通信）

FireWall-1 は、セキュアルーム内にある IA マネージャと SOC 内にある i-Monitor との通信を HTTPS だけに制限し、IA マネージャは i-Monitor との通信において、IA マネージャの OS が有する SSL 機能を利用して暗号化通信を実現しなければならない。

### ４．２．２．NonIT 環境のセキュリティ対策方針

NOE.PHYSICAL_ACCESS（入退出管理）

管理コンソール端末を除く IA システムを構成する機器群は、物理的に入退出管理がなされた部屋に設置され、ExLink 管理者及び ExLink 利用者のみ立ち入りが可能な環境にしなければならない。

NOE.NETWORK（ネットワーク管理）

管理コンソール端末は一般業務スペース、i-Monitor は SOC に接続され、これらの管理コンソール及び i-Monitor は、FireWall-1 で隔離された管理コンソール端末以外の IA システムに FireWall-1 を介して接続されなければならない。

NOE.DB_PASSWORD（DB のアクセスアカウントの設定）
IADB として識別認証機能を有する DB を選定し、IA マネージャ及び管理コンソール用のアカウントと IADB を管理するためのアカウントだけがアクセスできるよう登録を行い、その他のアカウントを登録してはならない。またアカウントのパスワードは、容易に推測されない値を設定しなければならない。

NOE.CONSOLE（管理コンソール端末のチェック）
管理コンソール端末は、不正なソフトウェアを検知検出するソフトウェア、または ExLink 管理者、ExLink 利用者によって、定期的に不正なソフトウェアがインストールされていないかチェックし、不正なソフトウェアを発見した場合は削除しなければならない。

NOE.TRUSTED_USER_ROLE（組織の役割）
組織の責任者は、IAシステムの管理運用に必要な能力を持ち、不正行為を働かない者を ExLink 管理者及び ExLink 利用者として人選しなければならない。

NOE.SELECTED_TRUSTED_SOC（信頼できる SOC の選択）
組織の責任者は、下記の条件を満たす SOC を選択しなければならない。
SOC 内において SOC オペレータのみ i-Monitor を操作できるよう管理を行っている SOC。
SOC オペレータに対して、i-Monitor を操作するために必要な訓練を行っており、不正行為を働かない信頼できる者を擁している SOC。
上記 2 つの条件を満たしており、かつ ExLink-IA に対して唯一指示を出す事ができる i-Monitor を所有し運営している株式会社 日立情報システムズの SOC。

# 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

**○クラス FAU：セキュリティ監査**

**FAU_GEN.1：監査データ生成**

下位階層：　　なし

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：*指定なし*]レベルのすべての監査対象事象；及び

c) [割付：*表 5-1 に示される個別に定義した監査対象事象*]。

表 5-1　個別に定義した監査対象事象

| 機能要件 | 監査情報 |
|---|---|
| FIA_UAU.2 | 利用者の認証時における、認証の成功及び認証の失敗 |
| FIA_UID.2 | 利用者の識別時における、識別の成功及び識別の失敗 |
| FAU_STG.3 | ログ自動削除実行時における、削除の成功 |

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：*なし*]

依存性：　　FPT_STM.1　高信頼タイムスタンプ

**FAU_SAR.1：監査レビュー**

下位階層： なし

FAU_SAR.1.1 TSF は、[割付：*ExLink 管理者及び ExLink 利用者*]が、[割付：*表 5-1 に示される個別に定義した監査対象事象*]を監査記録から読み出せるようにしなければならない。

FAU_SAR.1.2 TSF は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

依存性： FAU_GEN.1 監査データ生成

**FAU_STG.1：保護された監査証跡格納**

下位階層： なし

FAU_STG.1.1 TSF は、格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2 TSF は、監査証跡内の格納された監査記録への不正な改変を[選択：*防止*]できねばならない。

依存性： FAU_GEN.1 監査データ生成

**FAU_STG.3：監査データ損失の恐れ発生時のアクション**

下位階層： なし

FAU_STG.3.1 TSF は、監査証跡が[割付：*ログ保管期間またはログ保管件数*]を超えた場合、[割付：*ログ保管期間またはログ保管件数を超えたログを削除する*]をとらなければならない。

依存性： FAU_STG.1 保護された監査証跡格納

**○クラス FIA：識別と認証**

**FIA_SOS.1：秘密の検証**

下位階層：　　なし

FIA_SOS.1.1　TSF は、秘密が[割付：*表 5-2 に示される入力可能な文字列の長さ*]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。

表 5-2　入力可能な文字列の長さと使用可能な文字及び記号

| 項目 | 入力可能範囲 |
|---|---|
| 入力可能な文字列の長さ | 文字数は 6 文字～64 文字 かつ 全体文字サイズは 64byte 以下 |

依存性：　　なし

**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　TSF 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。

依存性：　　FIA_UID.1 識別のタイミング

**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：*パスワードとして入力された文字数と同数の[＊]（アスタリスク）*]だけを利用者に提供しなければならない。

依存性：　　FIA_UAU.1 認証のタイミング

**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　TSF 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。

依存性：　　なし

**○クラス FMT：セキュリティ管理**

**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

FMT_MOF.1.1　TSF は、機能[割付：*ログ自動削除機能*][選択：*を停止する、を動作させる*]能力を[割付：*ExLink 管理者*]に制限しなければならない。

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_MTD.1：TSF データの管理**

下位階層：　　なし

FMT_MTD.1.1　TSF は、[割付：*表 5-3 に示される TSF データの管理*]を[選択：*問い合わせ、改変、削除 [割付：追加]*]する能力を[割付：*ExLink 管理者及び ExLink 利用者*]に制限しなければならない。

表 5-3　TSF データの管理

| | ExLink 管理者 | | | | ExLink 利用者 | | | |
|---|---|---|---|---|---|---|---|---|
| TSF データ | 追加 | 編集 | 削除 | 参照 | 追加 | 編集 | 削除 | 参照 |
| 自身のユーザ ID | × | × | × | ○ | × | × | × | ○ |
| 自身のパスワード | × | ○ | × | × | × | ○ | × | × |
| 他者のユーザ ID | ○ | × | ○ | ○ | × | × | × | × |
| ログの保管期間の閾値 | | ○ | | ○ | | × | | ○ |
| ログの保管件数の閾値 | | ○ | | ○ | | × | | ○ |

※ ○：実施可能　×：実施不可能

※ 選択で指定している”問い合わせ”は”参照”、”改変”は”編集”を表している。

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：*表 5-4 に示されるセキュリティ管理機能のリスト*]。

表 5-4　セキュリティ管理機能の特定(1/2)

| 機能要件 | 管理機能 | 管理項目 |
|---|---|---|
| FAU_GEN.1 | - | - |
| FAU_SAR.1 | a）監査記録に対して読み出し権のある利用者グループの維持（削除、改変、追加）。 | なし。監査記録に対して読み出し権のある利用者グループは固定である。 |
| FAU_STG.1 | - | - |
| FAU_STG.3 | a) 閾値の維持；<br>b) 監査格納失敗が切迫したときにとられるアクションの維持(削除、改変、追加)。 | a)<br>ログ保管期間：1～32,768、初期値：365<br>ログ件数：1～10,000,000、初期値：10,000<br>b)なし。アクションは固定であり、管理対象としない。 |
| FIA_SOS.1 | a）秘密の検証に使用される尺度の管理。 | a）なし。アクションは固定であり、管理対象とならない。 |
| FIA_UAU.2 | 管理者による認証データの管理；<br>このデータに関係する利用者による認証データの管理。 | ExLink 管理者による ExLink 管理者自身のパスワードの編集ならびに ExLink 利用者による ExLink 利用者自身のパスワードの編集。 |
| FIA_UAU.7 | - | - |
| FIA_UID.2 | a）利用者識別情報の管理。 | a）ExLink 管理者による ExLink 管理者のユーザ ID の参照及び ExLink 管理者による ExLink 利用者のユーザ ID の追加、削除、参照。 |
| FMT_MOF.1 | a）TSF の機能と相互に影響を及ぼし得る役割のグループを管理すること。 | a）なし。TSF の機能と相互に影響を及ぼし得る役割のグループは固定である。 |
| FMT_MTD.1 | a）TSF データと相互に影響を及ぼし得る役割のグループを管理すること。 | a）ユーザ ID やパスワードについては TSF データと相互に影響を及ぼし得る役割のグループは固定であり、管理項目はない。<br>ログの保管期間とログの保管件数についても TSF データと相互に影響を及ぼし得る役割のグループは固定であるため、管理項目はない。 |

表 5-4　セキュリティ管理機能の特定(2/2)

| 機能要件 | 管理機能 | 管理項目 |
|---|---|---|
| FMT_SMF.1 | - | - |
| FMT_SMR.1 | a）役割の一部をなす利用者のグループの管理。 | a）なし。役割の一部をなす利用者のグループは固定である。 |
| FPT_RVM.1 | - | - |
| FPT_STM.1 | a）時間の管理。 | なし。システム内時間の管理は OS により行われるため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：*ExLink 管理者及び ExLink 利用者*]を維持しなければならない。

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

**○クラス FPT：TSF の保護**

**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_STM.1：高信頼タイムスタンプ**

下位階層：　　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。

依存性：　　なし

### ５．１．２．最小機能強度レベル

TOE のセキュリティ機能強度の最小機能強度レベルは、SOF-基本である。

### ５．１．３．TOE セキュリティ保証要件

本 TOE の評価保証レベルは EAL1 である。すべての保証要件コンポーネントは CC part3 で規定されている EAL1 のコンポーネントを直接使用する。TOE セキュリティ保証要件を表 5-5 に示す。

表 5-5　TOE セキュリティ保証要件

| 保証クラス | 保証コンポーネント ID | 保証コンポーネント | 依存性 |
|---|---|---|---|
| 構成管理 | ACM_CAP.1 | バージョン番号 | なし |
| 配布と運用 | ADO_IGS.1 | 設置、生成、及び<br>立上げ手順 | AGD_ADM.1 |
| 開発 | ADV_FSP.1 | 非形式的機能仕様 | ADV_RCR.1 |
| | ADV_RCR.1 | 非形式的対応の実証 | なし |
| ガイダンス文書 | AGD_ADM.1 | 管理者ガイダンス | ADV_FSP.1 |
| | AGD_USR.1 | 利用者ガイダンス | ADV_FSP.1 |
| テスト | ATE_IND.1 | 独立テスト – 準拠 | ADV_FSP.1<br>AGD_ADM.1<br>AGD_USR.1 |

## ５．２．IT 環境に対するセキュリティ要件

**○クラス FTP：高信頼パス/チャネル**

**FTP_ITC.1a：TSF 間高信頼チャネル**

下位階層：なし

FTP_ITC.1.1a　TSF は、それ自身とリモート高信頼 IT 製品間に、他の通信チャネル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チャネルデータの保護を提供する通信チャネルを提供しなければならない。

FTP_ITC.1.2a　TSF は、[選択：*TSF*]が、高信頼チャネルを介して通信を開始するのを許可しなければならない。

FTP_ITC.1.3a　TSF は、[割付：*IA マネージャ通信機能*、*IADB アクセス機能*]のために、高信頼チャネルを介して通信を開始しなければならない。

依存性：なし

**FTP_ITC.1b：TSF 間高信頼チャネル**

下位階層：なし

FTP_ITC.1.1b　TSF は、それ自身とリモート高信頼 IT 製品間に、他の通信チャネル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チャネルデータの保護を提供する通信チャネルを提供しなければならない。

FTP_ITC.1.2b　TSF は、[選択：*TSF*]が、高信頼チャネルを介して通信を開始するのを許可しなければならない。

FTP_ITC.1.3b　TSF は、[割付：*i-Monitor 通信機能*]のために、高信頼チャネルを介して通信を開始しなければならない。

依存性：なし

# 6．TOE 要約仕様

## 6．1．TOE セキュリティ機能

TOE セキュリティ機能は、第 5.1.1.項で記述した TOE セキュリティ機能要件を満たすものである。表 6-1 にて TOE セキュリティ機能とセキュリティ機能要件の対応関係を示す。

表 6-1　TOE セキュリティ機能とセキュリティ機能要件の対応関係

| TOE セキュリティ機能要件 / TOE セキュリティ機能 | FAU_GEN.1 | FAU_SAR.1 | FAU_STG.1 | FAU_STG.3 | FIA_SOS.1 | FIA_UAU.2 | FIA_UAU.7 | FIA_UID.2 | FMT_MOF.1 | FMT_MTD.1 | FMT_SMF.1 | FMT_SMR.1 | FPT_RVM.1 | FPT_STM.1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SF.IDENTIFICATION | | | | | | ○ | ○ | ○ | | | | | ○ | |
| SF.ACCOUNT | | | | | ○ | | | | | ○ | ○ | ○ | ○ | |
| SF.AUDIT | ○ | ○ | ○ | ○ | | | | | ○ | ○ | ○ | ○ | ○ | ○ |

### 6．1．1．SF.IDENTIFICATION（識別認証）

管理コンソールはログオン時に必ずユーザ ID とパスワードの識別認証を実施する。管理コンソールは ExLink 管理者及び ExLink 利用者の識別・認証が成功するまで、ExLink 管理者及び ExLink 利用者に対して識別認証以外の操作を許可しない。入力されたパスワードは、パスワードとして入力された文字数と同数の[*]アスタリスクで画面上に提供される。管理コンソールは ExLink 管理者及び ExLink 利用者の識別認証のため、ユーザ ID とパスワードが IADB 内に保管されている情報と一致する事の確認を行い、識別認証に成功した ExLink 管理者及び ExLink 利用者に管理コンソールの利用を許可する。

### 6．1．2．SF.ACCOUNT（アカウント情報）

管理コンソールはパスワードを変更する機能を ExLink 管理者及び ExLink 利用者に提供する。パスワード登録/変更においてパスワードは、表 5-2 に示される入力可能な文字列の長さで必ず検証される。また管理コンソールはパスワード変更においてパスワード変更対象の自身のユーザ ID の参照を ExLink 管理者及び ExLink 利用者に提供する。また ExLink 管理者に対してのみアカウント編集機能を提供し、ExLink 管理者自身のユーザ ID の参照に加えて、ExLink 利用者のユーザ ID の追加、削除及び参照を可能にする。

### ６．１．３．SF.AUDIT（監査）

管理コンソールは監査記録として管理コンソールにログオンする際の識別認証の成功及び失敗ログ、そして IA マネージャによるログ自動削除機能実行時に出力されるログ自動削除の成功ログを参照する機能を提供する。

管理コンソールは、ログオン時における識別認証を実施後、その結果を監査記録として必ず記録する。また、IA マネージャは、ログ自動削除機能を実行後、その成功した結果を監査記録として必ず記録する。

監査記録として取得するログは監査ログ情報である。監査ログ情報は、管理コンソール利用ログ情報及びログ自動削除成功ログ情報から構成されており、管理コンソール利用ログ情報には識別認証結果（成功及び失敗）及び発生時刻、重要度、種別、メッセージ、そしてログ自動削除成功ログ情報には自動削除の実行結果（成功）及び発生時刻、重要度、種別、メッセージが含まれる。

管理コンソールは ExLink 管理者に対して、指定したログの参照と指定したログを含む過去の監査ログ情報を削除する機能を提供し、ExLink 利用者は参照機能のみ提供される。

管理コンソールは、指定したログの参照削除要求に対し、必ずログ参照削除機能を提供する。

管理コンソールは ExLink 管理者に対して、ログの保管期間の閾値とログの保管件数の閾値の編集及び参照する機能を提供し、ExLink 利用者は参照機能のみ提供される。また、管理コンソールはログ保管期間またはログの保管件数を超えた監査ログ情報を自動的に削除するログ自動削除機能を提供する。ログ自動削除機能の動作及び停止は ExLink 管理者に提供される。

IA マネージャは、ログ自動削除機能を ExLink 管理者が設定した時刻に基づき、必ず起動する。

監査ログ情報の取得時間及びログ自動削除機能の実行時間は、IA マネージャの OS のタイムスタンプを用いる。

## ６．２．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順列的、確率的メカニズムを有する IT セキュリティ機能は SF.IDENTIFICATION、SF.ACCOUNT であり、機能強度は SOF-基本とする。

## ６．３．保証手段

保証要件クラスとそのコンポーネントを保証する手段を表 6-3 に示す。

表 6-3　保証要件クラスとそのコンポーネントを保証する手段

| 保証要件クラス | 保証要件コンポーネント | 保証手段 |
|---|---|---|
| ASE：ST 評価 | ASE_DES.1<br>ASE_ENV.1<br>ASE_INT.1<br>ASE_OBJ.1<br>ASE_PPC.1<br>ASE_REQ.1<br>ASE_SRE.1<br>ASE_TSS.1 | 汚染拡大防止システム<br>SHIELD/ExLink-IA<br>セキュリティターゲット<br>バージョン 1.0i |
| ACM：構成管理 | ACM_CAP.1 | 汚染拡大防止システム<br>SHIELD/ExLink-IA<br>バージョン管理文書バージョン 1.09 |
| ADO：配布と運用 | ADO_IGS.1 | 汚染拡大防止システム<br>SHIELD/ExLink-IA<br>インストールマニュアル<br>バージョン 1.05 |
| ADV：開発 | ADV_FSP.1 | 汚染拡大防止システム<br>SHIELD/ExLink-IA v1.0 機能仕様書<br>バージョン 1.07 |
| | ADV_RCR.1 | 汚染拡大防止システム<br>SHIELD/ExLink-IA<br>対応分析書　バージョン 1.0b |
| AGD：ガイダンス文書 | AGD_ADM.1 | 汚染拡大防止システム<br>SHIELD/ExLink-IA<br>アドミニストレータマニュアル<br>バージョン 1.09 |
| | AGD_USR.1 | |
| ATE：テスト | ATE_IND.1 | 汚染拡大防止システム<br>SHIELD/ExLink-IA v1.0 システム一式 |

# ７．PP 主張

## 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

セキュリティ対策は、TOE セキュリティ環境で規定した脅威及び前提条件に対抗するためのものである。

セキュリティ対策方針と対抗する脅威及び前提条件における対応関係を表 8-1 に示す。

表 8-1 セキュリティ対策方針と対抗する脅威及び前提条件

| 前提条件、脅威 / セキュリティ対策方針 | T.ILLEGAL_OPERATION | T.ENVIRONMENT_PROBE | T.ENVIRONMENT_SPOOFING | T.COMMUNICATION_PROBE | A.PHYSICAL_ACCESS | A.NETWORK | A.DB_PASSWORD | A.CONSOLE | A.TRUST_USER | A.TRUST_SOC |
|---|---|---|---|---|---|---|---|---|---|---|
| O.IDENTIFICATION | ○ | | | | | | | | | |
| O.AUDIT | ○ | | | | | | | | | |
| OE.ENVIRONMENT | | ○ | ○ | | | | | | | |
| OE.SSL | | | | ○ | | | | | | |
| NOE.PHYSICAL_ACCESS | | | | | ○ | | | | | |
| NOE.NETWORK | | | | | | ○ | | | | |
| NOE.DB_PASSWORD | | | | | | | ○ | | | |
| NOE.CONSOLE | | | | | | | | ○ | | |
| NOE.TRUSTED_USER_ROLE | | | | | | | | | ○ | |
| NOE.SELECTED_TRUSTED_SOC | | | | | | | | | | ○ |

※ 上記表 8-1 における”○”は対象のセキュリティ対策方針が対応している脅威及び前提条件である事を示す

表 8-1 より、各セキュリティ対策方針は一つ以上の脅威及び前提条件に対応している。

次に脅威及び前提条件がセキュリティ対策方針で実現される事を説明する。

T.ILLEGAL_OPERATION は、O.IDENTIFICATION、O.AUDIT により軽減される。管理コンソールを利用する前に必ず識別認証を行い、識別認証に成功した ExLink 管理者及び ExLink 利用者のみ管理コンソールの利用を許される。

またログオン成功及び失敗のログを取得する事で、ExLink 管理者及び ExLink 利用者は不正ログオンの試行を知る事ができる。

T.ENVIRONMENT_PROBE と T.ENVIRONMENT_SPOOFING は、OE.ENVIRONMENT により軽減される。FireWall-1 と管理コンソール端末との間を VPN 接続による暗号化通信を実現し、T.ENVIRONMENT_PROBE に対応する。また FireWall-1 と管理コンソール端末間の通信は、FireWall-1 から発行された証明書を管理コンソール端末に適用し、証明書による認証を行う事で、なりすましにおける脅威である T.ENVIRONMENT_SPOOFING に対応する。

T.COMMUNICATION_PROBE は、OE.SSL により軽減される。FireWall-1 は、SOC とセキュアルーム内の機器との通信を HTTPS だけに制限する。IA マネージャは i-Monitor との通信において、IA マネージャの OS が有する SSL 機能を利用して、暗号化通信を実現し、T.COMMUNICATION_PROBE に対応する。

A.PHYSICAL_ACCESS は、NOE.PHYSICAL_ACCESS にあるように、管理コンソール端末を除く IA システムを構成する機器群は、物理的に入退出管理がなされた部屋に設置され、ExLink 管理者及び ExLink 利用者のみ立ち入りが可能な環境にする事で実現される。

A.NETWORK は、NOE.NETWORK にあるように、管理コンソール端末は一般業務スペース、i-Monitor は SOC に接続され、これらの管理コンソール端末及び i-Monitor は、FireWall-1 で隔離された管理コンソール端末以外の IA システムに FireWall-1 を介して接続する事で実現される。

A.DB_PASSWORD は、NOE.DB_PASSWORD にあるように、 IADB として識別認証機能を有する DB を選定し、IA マネージャ及び管理コンソール用のアカウントと IADB を管理するためのアカウントだけがアクセスできるよう登録を行い、その他のアカウントは登録しない事、またアカウントのパスワードは、容易に推測されない値を設定する事で実現される。

A.CONSOLE は、NOE.CONSOLE にあるように、管理コンソール端末は、不正なソフトウェアを検知検出するソフトウェア、または ExLink 管理者、ExLink 利用者によって、定期的に不正なソフトウェアがインストールされていないかチェックされ、不正なソフトウェアが確認された場合は削除する事で実現される。

A.TRUST_USERは、NOE.TRUSTED_USER_ROLEにあるように、組織の責任者が、IAシステムの管理運用に必要な能力を持ち、不正行為を働かない者をExLink管理者及びExLink利用者として人選する事で実現される。

A.TRUST_SOC は、NOE.SELECTED_TRUSTED_SOC にあるように、組織の責任者によって、下記の条件を満たす SOC を選択される事で実現される。
SOC 内において SOC オペレータのみ i-Monitor を操作できるよう管理を行っている SOC。
i-Monitor を操作する SOC オペレータに対して、i-Monitor を操作するために必要な訓練を行っており、不正行為を働かない信頼できる者を擁している SOC。
上記 2 つの条件を満たしており、かつ ExLink-IA に対して唯一指示を出す事ができる i-Monitor を所有し運営している株式会社 日立情報システムズの SOC。

## ８．２．セキュリティ要件根拠

### ８．２．１．セキュリティ機能要件根拠

TOE / IT 環境セキュリティ機能要件と TOE / IT 環境セキュリティ対策方針の対応関係を表 8-2 に示す。なお、第 5 章 IT セキュリティ要件に規定されている各セキュリティ要件は、互いに競合する事なく、内部的に一貫している。

表 8-2　TOE / IT 環境セキュリティ機能要件と TOE / IT 環境セキュリティ対策方針の対応関係

| TOE / IT 環境セキュリティ対策方針 ＼ TOE / IT 環境セキュリティ機能要件 | O.IDENTIFICATION | O.AUDIT | OE.ENVIRONMENT | OE.SSL |
|---|---|---|---|---|
| FAU_GEN.1 | | ○ | | |
| FAU_SAR.1 | | ○ | | |
| FAU_STG.1 | | ○ | | |
| FAU_STG.3 | | ○ | | |
| FIA_SOS.1 | ○ | | | |
| FIA_UAU.2 | ○ | | | |
| FIA_UAU.7 | ○ | | | |
| FIA_UID.2 | ○ | | | |
| FMT_MOF.1 | | ○ | | |
| FMT_MTD.1 | ○ | ○ | | |
| FMT_SMF.1 | ○ | ○ | | |
| FMT_SMR.1 | ○ | ○ | | |
| FPT_RVM.1 | ○ | ○ | | |
| FPT_STM.1 | | ○ | | |
| FTP_ITC.1a | | | ○ | |
| FTP_ITC.1b | | | | ○ |

O.IDENTIFICATION は、以下のとおり、識別認証の実施に直接係わるセキュリティ機能要件だけでなく、その識別認証で使用される認証データに係わるセキュリティ機能要件、及び識別認証の管理のためのセキュリティ機能要件を含めた TOE セキュリティ機能要件の組み合わせによって実現できる。

識別認証の実施は、以下のセキュリティ機能要件により満たされる。

・FIA_UAU.2 にて、認証されていない人物は管理コンソールにアクセスできない事を保証する。

・FIA_UID.2 にて、利用者識別をしなければ管理コンソールにアクセスできない事を保証する。
・FPT_RVM.1 にて、識別認証において TSP がバイパスされる事がない事を保証する。
識別認証で使用される認証データの保護及び品質尺度に関しては、以下のセキュリティ機能要件により満たされる。
・FIA_SOS.1 にて、管理コンソールにログオンする際、表 5-2 に示される入力可能な文字列の長さが使用可能である事を保証する。
・FIA_UAU.7 にて、パスワード入力時に入力された文字数と同数の[*]（アスタリスク）だけを提供する事を保証する。
また、識別認証の管理は、以下のセキュリティ要件により満たされる。
・FMT_MTD.1 にて、識別認証において ExLink 管理者は自身のユーザ ID の参照及びパスワードの編集に加えて、ExLink 利用者のユーザ ID の追加、削除及び参照する能力、また ExLink 利用者は自身のユーザ ID の参照及び自身のパスワードの編集する能力が、管理コンソールにログオンしている ExLink 管理者及び ExLink 利用者に制限されている事を保証する。
・FMT_SMF.1 にて、識別認証におけるユーザ ID 及び自身のパスワードが管理されている事を保証する。
・FMT_SMR.1 にて、識別認証において ExLink 管理者及び ExLink 利用者の役割を維持する事を保証する。

O.AUDIT は、以下のとおり、監査ログ情報の取得及び閲覧に係わるセキュリティ機能要件だけでなく、取得した監査ログ情報が確実に閲覧できるようにログの保護に係わる機能要件も含めた TOE セキュリティ機能要件の組み合わせによって実現できる。
監査ログ情報の取得及び閲覧は、以下のセキュリティ機能要件により満たされる。
・FAU_GEN.1 にて、監査記録の生成を保証する。監査対象事象として管理コンソールログオン時における識別の成功と識別の失敗及び認証の成功と認証の失敗とログ自動削除実行時における削除の成功に関するすべての事象が記録される事を保証する。
・FAU_SAR.1 にて、取得した監査記録を読み出す事を ExLink 管理者及び ExLink 利用者のみに許可し、それ以外の者の読み出しを禁止する事を保証する。
監査ログ情報の保護は、以下のセキュリティ機能要件により満たされる。
・FAU_STG.1 にて、IADB に格納された監査ログ情報は、ExLink 管理者だけが参照、削除でき、ExLink 利用者は参照のみ可能である。これにより監査ログ情報は、不正な削除から保護され、不正な改変は防止されている事を保証する。
・FAU_STG.3 にて、監査ログ情報における情報損失の恐れ発生時に、閾値として定められたログの保管期間またはログの保管件数を超過した監査ログ情報を削除する事により、監査ログ情報を保護できる事を保証する。

・FMT_MOF.1 にて、監査ログ情報が指定されたログの保管期間またはログの保管件数を超えた場合に監査ログ情報を自動削除するログ自動削除機能の動作及び停止を ExLink 管理者だけが管理コンソール上で設定できるよう制限する事を保証する。
・FMT_MTD.1 にて、監査に用いるログの保管期間及びログの保管件数の閾値は管理コンソール上で ExLink 管理者だけが編集及び参照する事ができ、ExLink 利用者は参照のみに制限する事を保証する。
・FMT_SMF.1 にて、監査機能及び監査に用いるログの保管期間（1～32,768 日：初期値：365 日）及びログの保管件数（1～10,000,000 件、初期値：10,000 件）の閾値維持が管理されている事を保証する。
・FMT_SMR.1 にて、監査機能において ExLink 管理者及び ExLink 利用者の役割を維持する事を保証する。
・FPT_RVM.1 にて、監査対象イベントの発生時、監査証跡への操作時には監査に関する TSF が必ず呼び出される事を保証する。
・FPT_STM.1 にて、監査ログ情報に使用される高信頼タイムスタンプを得る事を保証する。

OE.ENVIRONMENT は、以下の IT 環境セキュリティ機能要件によって実現できる。
・FTP_ITC.1a にて、管理コンソール端末 - FireWall-1 間の通信は FireWall-1 が発行する証明書を用いて、セキュアルーム内にある IA マネージャ、IADB との接続を試みる管理コンソール端末の認証を行い、認証に成功した管理コンソール端末-FireWall-1 間の通信を VPN 接続による通信暗号化で保護される事を保証する。

OE.SSL は、以下の IT 環境セキュリティ機能要件によって実現できる。
・FTP_ITC.1b にて、IA マネージャと i-Monitor 間を暗号化する事で保護される事を保証する。

### ８．２．２．最小機能強度レベル根拠

第 3.2 節において、脅威エージェントの持つ攻撃能力は「低い」と想定している。
したがって、SOF-基本という最小機能強度の主張は適切である。

### ８．２．３．セキュリティ機能要件依存性

TOE / IT セキュリティ機能要件のコンポーネント依存性を表 8-3 に示す。

表 8-3　TOE / IT セキュリティ機能要件のコンポーネント依存性

| No. | TOE / IT セキュリティ機能要件 | CC パート 2 で規定されている依存コンポーネント | TOE の依存コンポーネント | 依存性が満たされないコンポーネント |
|---|---|---|---|---|
| 1 | FAU_GEN.1 | FPT_STM.1 | FPT_STM.1 | なし |
| 2 | FAU_SAR.1 | FAU_GEN.1 | FAU_GEN.1 | なし |
| 3 | FAU_STG.1 | FAU_GEN.1 | FAU_GEN.1 | なし |
| 4 | FAU_STG.3 | FAU_STG.1 | FAU_STG.1 | なし |
| 5 | FIA_SOS.1 | なし | なし | なし |
| 6 | FIA_UAU.2 | FIA_UID.1 | FIA_UID.2（左記の上位階層） | なし |
| 7 | FIA_UAU.7 | FIA_UAU.1 | FIA_UAU.2（左記の上位階層） | なし |
| 8 | FIA_UID.2 | なし | なし | なし |
| 9 | FMT_MOF.1 | FMT_SMF.1<br>FMT_SMR.1 | FMT_SMF.1<br>FMT_SMR.1 | なし |
| 10 | FMT_MTD.1 | FMT_SMF.1<br>FMT_SMR.1 | FMT_SMF.1<br>FMT_SMR.1 | なし |
| 11 | FMT_SMF.1 | なし | なし | なし |
| 12 | FMT_SMR.1 | FIA_UID.1 | FIA_UID.2（左記の上位階層） | なし |
| 13 | FPT_RVM.1 | なし | なし | なし |
| 14 | FPT_STM.1 | なし | なし | なし |
| 15 | FTP_ITC.1a | なし | なし | なし |
| 16 | FTP_ITC.1b | なし | なし | なし |

### ８．２．４．セキュリティ機能要件相互補完性

TOE / IT 環境セキュリティ機能における迂回、干渉、非活性化の観点から、他のセキュリティ機能要件を有効に動作させるための機能要件を表 8-4 に示す。

表 8-4　TOE / IT セキュリティ機能要件の相互補完性

| No. | TOE / IT セキュリティ機能要件 | 迂回 | 干渉 | 非活性化 |
|---|---|---|---|---|
| 1 | FAU_GEN.1 | FPT_RVM.1 | なし | なし |
| 2 | FAU_SAR.1 | FPT_RVM.1 | なし | なし |
| 3 | FAU_STG.1 | FPT_RVM.1 | なし | なし |
| 4 | FAU_STG.3 | FPT_RVM.1 | なし | FMT_MOF.1 |
| 5 | FIA_SOS.1 | FPT_RVM.1 | なし | なし |
| 6 | FIA_UAU.2 | FPT_RVM.1 | なし | なし |
| 7 | FIA_UAU.7 | FPT_RVM.1 | なし | なし |
| 8 | FIA_UID.2 | FPT_RVM.1 | なし | なし |
| 9 | FMT_MOF.1 | なし | なし | なし |
| 10 | FMT_MTD.1 | なし | なし | なし |
| 11 | FMT_SMF.1 | なし | なし | なし |
| 12 | FMT_SMR.1 | なし | なし | なし |
| 13 | FPT_RVM.1 | なし | なし | なし |
| 14 | FPT_STM.1 | FPT_RVM.1 | なし | なし |
| 15 | FTP_ITC.1a | なし | なし | なし |
| 16 | FTP_ITC.1b | なし | なし | なし |

**○迂回**

FAU_GEN.1、FAU_SAR.1、FAU_STG.1、FAU_STG.3、FIA_SOS.1、FIA_UAU.2、FIA_UAU.7、FIA_UID.2、FPT_STM.1 は、FPT.RVM.1 により、処理が動作進行する前に必ず呼び出される事により、迂回できない。

FMT_MOF.1 は、TSF における機能のふるまいを管理する事を許可する機能要件であり、迂回はない。

FMT_MTD.1 は、TSF データを操作する能力を許可された識別された役割に制限する機能要件であり、迂回はない。

FMT_SMF.1 は、セキュリティ管理機能を特定する機能要件であり、迂回はない。

FMT_SMR.1 は、許可された識別された役割を維持し、利用者を役割に関連づける機能要件であり、迂回はない。

○干渉

オブジェクト（IADB 情報）にアクセスするサブジェクト（ExLink 管理者及び ExLink 利用者）はすべて信頼できるため、信頼できないサブジェクトによる外部からの干渉、及び改ざんは生じない。

○非活性化

FAU_STG.3 に関しては、FMT_MOF.1 により、指定されたログの保管期間あるいはログの保管件数を超えた場合、超過した監査ログ情報を削除するログ自動削除機能の動作及び停止を ExLink 管理者だけが管理コンソールを用いて指定でき、非活性化を防止している。
その他のセキュリティ機能要件に関しては、操作による機能停止やふるまいの変更はできないため、非活性化防止については考慮する必要はない。

## ８．２．５．セキュリティ保証要件根拠

本 TOE は、社外ネットワークから社内ネットワークの資産を保護する FW に、インターネットを介してリモートの SOC から FW 設定変更指示を転送するための運用に関するセキュリティ機能を提供する。この機能提供のためには、4.2.2.項で示した NonIT 環境セキュリティ対策方針の正しい運用に対してかなりの信頼が要求される。しかし、脅威の重大性に関しては、仮に IA システムが攻撃を受けたとしても IA システムが停止するだけであり、他の業務システムには一切影響がなく、セキュリティへの脅威が重大とみなされない。したがって、本 TOE の評価保証レベルとしては、セキュリティへの脅威が重大とみなされず、EAL1 が妥当である。

## ８．３．TOE 要約仕様根拠

### ８．３．１．TOE セキュリティ機能根拠

本項では、TOE セキュリティ機能が TOE セキュリティ機能要件に対して必要かつ十分である事を記述する。TOE セキュリティ機能と TOE セキュリティ機能要件の対応関係を以下に示す。表 6-1 よりすべての TOE セキュリティ機能が何らかの TOE セキュリティ機能要件の実現のために必要である事が示される。

**FAU_GEN.1：監査データ生成**

＜根拠＞

SF.AUDIT は、監査記録を生成する。生成される監査記録は、利用者の認証における認証の成功及び認証に失敗、利用者の識別時における識別の成功及び識別の失敗、ログ自動削除機能実行時における削除の成功である。監査記録として事象の日付・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）を記録する。
したがって、SF.AUDIT により FAU_GEN.1 は実現される。

**FAU_SAR.1：監査レビュー**

＜根拠＞

SF.AUDIT は、監査情報の読み出しを ExLink 管理者及び ExLink 利用者に制限し、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）を監査情報として取得し、ExLink 管理者及び ExLink 利用者に対し、これらの監査情報を解釈するのに適した形式で監査記録を提供する。

したがって、SF.AUDIT により FAU_SAR.1 は実現される。

**FAU_STG.1：保護された監査証跡格納**

＜根拠＞

SF.AUDIT は、IADB に格納された監査ログ情報は管理コンソールから ExLink 管理者だけが参照、削除でき、ExLink 利用者は参照のみ可能である。これにより不正な削除から保護し、不正な改変を防止する機能を提供する。

したがって、SF.AUDIT により FAU_STG.1 は実現される。

**FAU_STG.3：監査データ損失の恐れ発生時のアクション**

＜根拠＞

SF.AUDIT は、監査ログ情報が閾値として定められたログの保管期間あるいはログの保管件数を超えた場合、閾値として定められたログの保管期間またはログの保管件数を超過した監査ログ情報を削除する事により、監査ログ情報を保護できる事を提供する。

したがって、SF.AUDIT により FAU_STG.3 は実現される。

**FIA_SOS.1：秘密の検証**

＜根拠＞

SF.ACCOUNT は、ExLink 管理者及び ExLink 利用者の認証に使用するパスワードは表 5-2 に示される入力可能な文字列の長さである事を検証するメカニズムを提供する。

したがって、SF.ACCOUNT により FIA_SOS.1 は実現される。

**FIA_UAU.2：アクション前の利用者認証**
**FIA_UAU.7：保護された認証フィードバック**
**FIA_UID.2：アクション前の利用者識別**
＜根拠＞
SF.IDENTIFICATION は、ExLink 管理者及び ExLink 利用者の識別認証が成功するまで識別認証以外の TOE の機能を使用させない。また認証中、パスワードとして入力された文字数と同数の[*]アスタリスクを画面上に提供する。
したがって、SF.IDENTIFICATION により FIA_UAU.2、FIA_UAU.7、FIA_UID.2 は実現される。

**FMT_MOF.1：セキュリティ機能のふるまいの管理**
＜根拠＞
SF.AUDIT は、監査ログ情報が指定されたログの保管期間あるいはログの保管件数を超えた場合、自動削除するログ自動削除機能の動作及び停止を ExLink 管理者だけが管理コンソール上で設定できるよう制限する。
したがって、SF.AUDIT により FMT_MOF.1 は実現される。

**FMT_MTD.1：TSF データの管理**
＜根拠＞
SF.ACCOUNT は、ExLink 管理者に対し自身のユーザ ID の参照とパスワードの変更機能及び ExLink 利用者のユーザ ID の追加、参照、削除機能も提供する。また ExLink 利用者に対し自身のユーザ ID の参照機能及び自身のパスワードの変更機能を提供する。
SF.AUDIT は、ExLink 管理者にのみログの保管期間とログの保管件数の閾値の編集及び参照権限を提供し、ExLink 利用者に対してはログの保管期間及びログの保管件数の閾値を参照する機能のみに制限している。
したがって、SF.ACCOUNT 及び SF.AUDIT により FMT_MTD.1 は実現される。

**FMT_SMF.1：管理機能の特定**
＜根拠＞
SF.ACCOUNT は、管理コンソールにログオンしている ExLink 管理者及び ExLink 利用者に対して、ExLink 管理者及び ExLink 利用者自身のパスワードの編集機能を提供する。
また ExLink 管理者に対して、ExLink 管理者のユーザ ID の参照及び ExLink 利用者のユーザ ID の追加、削除、参照機能を提供する。
SF.AUDIT は、ログの保管期間（1～32,768 日　初期値：365 日）とログの保管件数（1～10,000,000 件、初期値：10,000 件）の閾値を維持する。閾値の変更は ExLink 管理者に対してのみ提供する。
したがって、SF.ACCOUNT 及び SF.AUDIT により FMT_SMF.1 は実現される。

**FMT_SMR.1：セキュリティ役割**

＜根拠＞

SF.ACCOUNT 及び SF.AUDIT は、ExLink 管理者及び ExLink 利用者という役割を維持する。

したがって、SF.ACCOUNT 及び SF.AUDIT により FMT_SMR.1 は実現される。

**FPT_RVM.1：TSP の非バイパス性**

＜根拠＞

SF.IDENTIFICATION、SF.ACCOUNT、SF.AUDIT は、TSC 内の各機能の動作が許可される前に、TSP 実施機能が呼び出され成功する事を保証する。

したがって、SF.IDENTIFICATION、SF.ACCOUNT、SF.AUDIT により FPT_RVM.1 は実現される。

**FPT_STM.1：高信頼タイムスタンプ**

＜根拠＞

SF.AUDIT は、監査データ生成及び監査レビューのために IA マネージャの動作する OS の時刻情報を取得する事で高信頼タイムスタンプを実現する。

したがって、SF.AUDIT により FPT_STM.1 は実現される。

### ８．３．２．セキュリティ機能強度根拠

確率的または順列的メカニズムに基づく IT セキュリティ機能は、パスワード認証メカニズムに基づく SF.IDENTIFICATION、SF.ACCOUNT である。SF.IDENTIFICATION、SF.ACCOUNT のセキュリティ機能強度は、第 6.2.節において「SOF-基本」と主張されている。これは、第 5.1.2.項で宣言した TOE セキュリティ機能要件に対する「SOF-基本」という主張と一貫している。

### ８．３．３．セキュリティ保証手段根拠

本項では、セキュリティ保証手段がセキュリティ保証要件（EAL1）の評価コンポーネントに対して必要かつ十分である事を記述する。セキュリティ保証要件とセキュリティ保証手段の対応関係を以下に示す。

**ACM_CAP.1（バージョン番号）**

汚染拡大防止システム SHIELD/ExLink-IA バージョン管理文書は、以下の内容を含む。

・TOE のバージョン識別とバージョン命名規則

したがって、上記により ACM_CAP.1 を実現できる。

**ADO_IGS.1（設置、生成、及び立上げ手順）**

汚染拡大防止システム SHIELD/ExLink-IA インストールマニュアルは、以下の内容を含む。

・TOE のセキュアな設置、生成、立上げに必要な手順

したがって、上記により ADO_IGS.1 を実現できる。

**ADV_FSP.1（非形式的機能仕様）**

汚染拡大防止システム SHIELD/ExLink-IA v1.0 機能仕様書は、以下の内容を含む。

・TOE セキュリティ機能の識別と仕様

・TSF インタフェースの識別と仕様

したがって、上記により ADV_FSP.1 を実現できる。

**ADV_RCR.1（非形式的対応の実証）**

汚染拡大防止システム SHIELD/ExLink-IA 対応分析書は、以下の内容を含む。

・ST の TOE セキュリティ機能と、上記の SHIELD/ExLink-IA v1.0 機能仕様書の TSF インタフェースの対応関係

したがって、上記により ADV_RCR.1 を実現できる。

**AGD_ADM.1（管理者ガイダンス）**

汚染拡大防止システム SHIELD/ExLink-IA アドミニストレータマニュアルは、以下の内容を含む。

・TOE の前提環境

・TOE 管理におけるセキュリティ上の注意事項

・管理者が利用できる TOE のセキュリティ機能とインタフェース

・TOE のセキュアな管理方法

したがって、上記により AGD_ADM.1 を実現できる。

**AGD_USR.1（利用者ガイダンス）**

汚染拡大防止システム SHIELD/ExLink-IA アドミニストレータマニュアルは、以下の内容を含む。

・TOE の前提環境

・TOE 管理におけるセキュリティ上の注意事項

・管理者が利用できる TOE のセキュリティ機能とインタフェース

・TOE のセキュアな管理方法

したがって、上記により AGD_USR.1 を実現できる。

**ATE_IND.1（独立テスト- 準拠）**

汚染拡大防止システム SHIELD/ExLink-IA v1.0 システム一式を提供する事により、評価者が TOE のテストを行う際、開発者側で実施したものと同様のテスト環境を提供できる。

したがって、上記により ATE_IND.1 を実現できる。

## ８．４．PP 主張根拠

本 ST は、いかなる PP への適合も主張しない。

## 付録 A．用語

本 ST で使用する用語を以下に示す。

表 A-1　ST 使用用語表(1/3)

| 用語 | 定義 |
|---|---|
| CryptoAPI | Microsoft 社が開発した暗号化と署名の機能を提供する API。暗号化や復号、デジタル署名の生成と検証などの機能をアプリケーションに提供する。 |
| CSO4U サービス | SOC 内に設置された i-Monitor とお客様サイト内に設置された ExLink-IA を連携する事により、SOC オペレータが ExLink-IA を運用するサービス。 |
| CSO4U サービスの遠隔制御情報 | SOC オペレータによって作成された FW 設定変更指示情報。<br>指示には制御対象機器と制御内容が含まれている。 |
| DB | DataBase の略称。 |
| DBMS | DataBase Management System の略称。 |
| DLL | 複数のアプリケーションソフトウェアが共通して利用するような汎用性の高いプログラムを部品化してファイルとして保管しておき、必要に応じてメモリに呼び出して利用されるプログラム部品。 |
| ExLink-IA | セキュリティ対策統合ソフトウェア SHIELD/ExLink の１ソリューション。セキュリティデバイスより収集した情報を分析し、その結果を i-Monitor へ送信する。また i-Monitor から送信される FW 設定変更指示を設定変更対象の FireWall-1 へ適用する。 |
| ExLink-Qu | セキュリティ対策統合ソフトウェア SHIELD/ExLink の１ソリューション。社内ネットワークへ PC が接続する前に、その PC がセキュリティポリシーに準拠しているか評価を行う。 |
| FireWall-1 | Check Point Software Technologies 社より提供されている FireWall アプリケーションソフトウェア。ネットワークの境界線に設置し、許可された通信のみを通過させる。本書では、FireWall-1 NG または NGX をまとめて FireWall-1 としている。 |
| FW | FireWall の略称。外部ネットワークから内部ネットワーク資産を保護するためのネットワークサーバをさす。 |
| FW アクセスログ | FireWall-1 が収集するアクセスログ。送信元/宛先の IP アドレスとポート番号、プロトコル、通信に対するアクション（drop, reject）及び取得件数が含まれている。 |
| IA エージェントログ情報 | IA エージェントが FireWall-1 から取得する FW アクセスログ及び Proventia から取得する IPS インシデント情報。 |
| IA サブシステム | IA エージェント、管理コンソールの総称。 |
| IA システム | IA マネージャ、IA エージェント、管理コンソール、FireWall-1、Proventia、QuDB、IADB、Mail Server の総称。 |

表 A-1　ST 使用用語表(2/3)

| 用語 | 定義 |
|---|---|
| IDS | Intrusion Detection System の略称。通信回線を監視し、ネットワークへの侵入を検知して管理者に通報するシステム。ネットワーク上を流れるパケットを分析し、不正アクセスと思われるパケットを検出する。 |
| IPS | Intrusion Prevention System の略称。サーバやネットワークへの不正侵入を阻止するツール。侵入検知を行う IDS 機能を拡張し、侵入を検知したら接続の遮断などの防御をリアルタイムに行う。 |
| IPS インシデント情報 | Proventia が収集するインシデントログ。送信元/宛先の IP アドレスとポート番号、プロトコル及び取得件数などが含まれている。 |
| i-Monitor | IA マネージャから受信したセキュリティログ情報を元に、IA マネージャに FW 設定変更指示を出すアプリケーションソフトウェア。SOC に設置され、SOC オペレータによって操作される。 |
| Proventia | ISS 社より提供されている不正侵入検知/防御（IDS/IPS）アプライアンス。ネットワーク上のパケットを分析しウィルス、ワーム、悪意のあるトラフィックなどをリアルタイムで検知・防御する事が可能。本書では Proventia GX を Proventia としている。 |
| Qu クライアント検疫情報 | ExLink-Qu が管理しているクライアント PC の検疫情報。検疫情報には、OS におけるパッチの適用状況、ウィルスチェックソフトウェアにおける最新のウィルス定義ファイルの適用状況などが含まれている。検疫情報は QuDB 内に保管されている。 |
| SHIELD | 日立情報システムズが提供するセキュリティソリューションの総称。 |
| SOC | Security Operation Center の略称。本 ST では、i-Monitor が設置されている株式会社日立情報システムズ内の物理的に保護された部屋を指す。 |
| SOC オペレータ | i-Monitor を操作する SOC に在籍するオペレータ。IA マネージャから送信されるセキュリティログ情報を分析し、分析内容に応じて FW 設定指示を IA マネージャへ送信する。 |
| SSL | Secure Socket Layer の略称。インターネット上で情報を暗号化して送受信するプロトコルであり、WWW や FTP などのデータを暗号化する事が可能。 |
| VPN | Virtual Private Network の略称。暗号化通信によりインターネット上の 2 つの地点を接続し、そのセッション上で仮想的なネットワークを構成する事で離れた場所にあるコンピュータやネットワーク同士を安全かつ自由に接続する事。 |
| アカウント情報 | 管理コンソールにログオンする際に用いるユーザ ID、パスワードの総称。 |
| セキュリティデバイス | FireWall-1、Proventia、QuDB などのセキュリティ機器。 |
| セキュリティログ情報 | IA マネージャが IA エージェントから取得する IA エージェントログ情報及び、QuDB から取得する Qu クライアント検疫情報の総称。 |

表 A-1　ST 使用用語表(3/3)

| 用語 | 定義 |
|---|---|
| ログ自動削除成功ログ情報 | ログ自動削除機能実行時に出力されるログ自動削除の成功ログ。 |
| 監査ログ情報 | IADB アクセス時に行われる識別認証の成功及び失敗ログとログ自動削除機能実行時に出力されるログ自動削除の成功ログの総称。 |
| 管理コンソール端末 | 管理コンソールがインストールされている端末。 |
| 管理コンソール利用ログ情報 | 管理コンソールを用いて IADB にログオン試行する際における成功及び失敗の記録情報。ExLink 管理者は参照及び削除可能。ExLink 利用者は参照のみ可能。 |