認　証　報　告　書

独立行政法人 情報処理推進機構
理事長　藤原　武平太　原紙押印済

評価対象

申請受付年月日(受付番号)	**平成18年11月14日**(IT**認証**6114)
認証番号	C0090
認証申請者	**株式会社 日立情報システムズ**
TOE**の名称**	**汚染拡大防止システム** SHIELD/ExLink-IA
TOE**のバージョン**	1.0
PP**適合**	**なし**
適合する保証要件	EAL1
TOE**開発者**	**株式会社 日立情報システムズ**
評価機関の名称	**社団法人 電子情報技術産業協会　ITセキュリティセンター**

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。
平成19年3月22日

独立行政法人 情報処理推進機構
セキュリティセンター 情報セキュリティ認証室
技術管理者　田渕　治樹

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① Common Criteria for Information Technology Security Evaluation Version 2.3
② Common Methodology for Information Technology Security Evaluation Version 2.3

評価結果：合格

「汚染拡大防止システム SHIELD/ExLink-IA v1.0」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証手続規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

1.1 はじめに

この認証報告書は、「汚染拡大防止システム SHIELD/ExLink-IA v1.0」（以下「本TOE」という。）について社団法人 電子情報技術産業協会 ITセキュリティセンター（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者である株式会社 日立情報システムズに報告するものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

本認証報告書は、本TOEに対して、適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称: 汚染拡大防止システム SHIELD/ExLink-IA

バージョン:1.0

開発者: 株式会社 日立情報システムズ

1.2.2 製品概要

本製品は、管理対象であるFW(*1)やIPS(*2)等からセキュリティログ情報の収集を行い、ログの解析を行うSOC(*3)へ送信する機能、及びSOCで作成されたFW設定変更指示に基づいて該当するFWの設定変更を行う機能を持つネットワーク管理ソフトウェア製品である。

(*1) 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。

(*2) 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。

(*3) Security Operation Centerの略称。本製品から送信されるセキュリティログ情

報の受領、及び本製品へFW設定変更指示を出すために使用されるアプリケーションソフトウェア「i-Monitor」が設置されている場所。

本製品は、管理対象であるFWやIPS等から収集したセキュリティログ情報、FW設定変更指示情報、及び本製品の管理情報を不正な暴露から保護する。本製品が提供するセキュリティ機能を以下に示す。

・ユーザ認証機能
・アカウント管理機能
・パスワード変更機能
・ログ参照削除機能
・ログ自動削除機能

1.2.3 TOEの範囲と動作概要

1.2.3.1 TOEの範囲と動作環境

本TOEは、IAマネージャ、IAエージェント、及び管理コンソールから構成される。本TOEの動作環境概要を図1-1に示す。

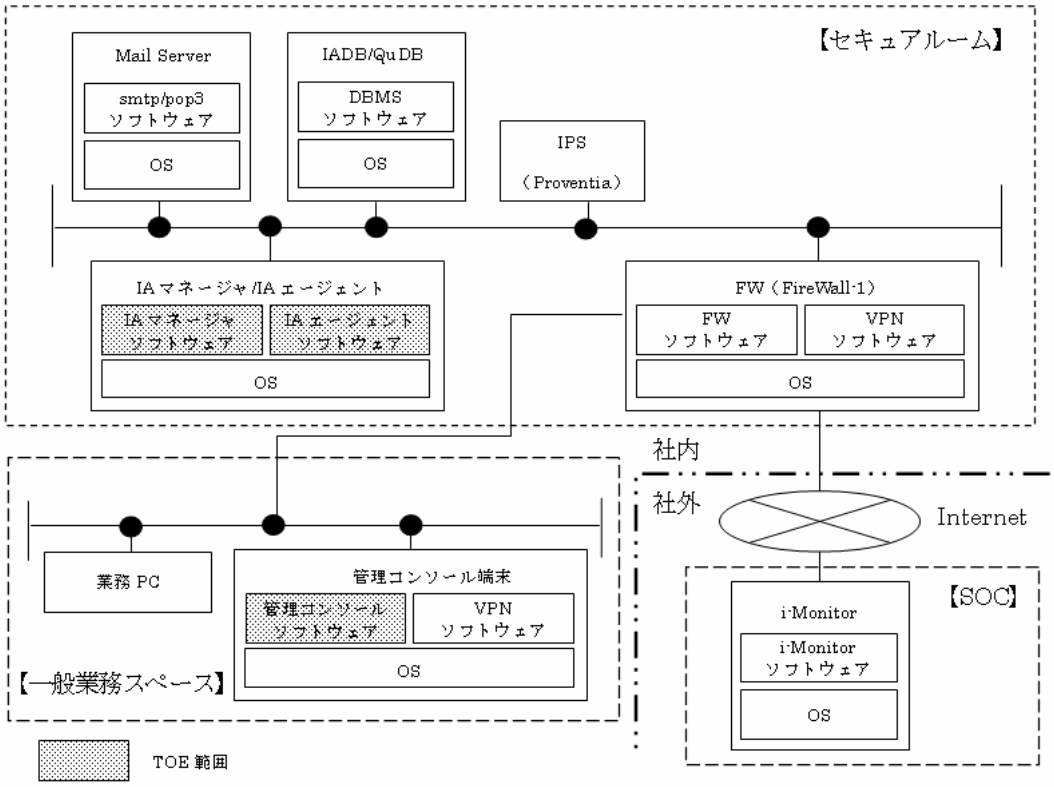

図1-1　TOEの動作環境概要

セキュアルームとは、TOEの管理者であるExLink管理者及びExLink利用者のみが物理的にアクセスできる場所のことである。一般業務スペースとは、ExLink管理者及

びExLink利用者以外の第三者が物理的にアクセスできる場所のことである。

本TOE及び本TOEと連動する構成要素について以下に示す。

(1) IAマネージャ（TOE）

ExLink-IAの管理を行うソフトウェアである。

SOCに設置されている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FW（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SOCに設置されているi-Monitorへ送信する。

管理コンソールが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の取得要求に対してID、パスワードを提供する。

(2) IAエージェント（TOE）

FW（FireWall-1）、IPS（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FW（FireWall-1）に対してFW設定変更指示を行う。また、FW（FireWall-1）、IPS（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。

(3) 管理コンソール（TOE）

ExLink-IAの管理GUIソフトウェアである。

TOEの利用者であるExLink管理者及びExLink利用者に対してIADB情報の参照、編集、削除の機能を提供する。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。

(4) IADB（TOE範囲外）

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。また、管理対象であるFW（FireWall-1）やIPS（Proventia）等から収集したセキュリティログ情報、FW設定変更指示情報、及び本製品の管理情報を格納する。

(5) FW（FireWall-1）（TOE範囲外）

FW（FireWall-1）は、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である。

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。

(6) IPS（Proventia）（TOE範囲外）

IPS（Proventia）は、外部ネットワークから内部ネットワークへの侵入を検知し、防御するためのネットワークサーバである。
セキュリティ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。

(7) QuDB（TOE範囲外）

ExLink-Quが使用するDBである。
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。

(8) i-Monitor（TOE範囲外）

FW（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で分析され、FW設定変更が必要な場合はFW設定変更指示が作成される。作成されたFW設定変更指示は、IAマネージャがi-Monitorへアクセスして受け取る。

1.2.3.2 TOEの動作概要

本TOEの動作概要について以下に示す。

(1) 各種ログ情報の収集及びSOCへの送信

IAマネージャは、IAエージェントがFW（FireWall-1）やIPS（Proventia）から収集したIAエージェントログ情報、及びQuDBが持つQuクライアント検疫情報をセキュリティログ情報としてSOCに設置されているi-Monitorへ送信する。

(2) FW設定変更

IAマネージャは、SOCに設置されている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FW（FireWall-1）を管理しているIAエージェントを検索する。その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マネージャからFW設定変更指示を受信したIAエージェントは、自身の管理下にある設定変更対象のFW（FireWall-1）に対してFW設定変更指示を行い、FW（FireWall-1）は指示に基づいて設定を変更する。

(3) TOEの管理

管理コンソールは、TOEの利用者であるExLink管理者及びExLink利用者に対してTOEの管理機能を提供する。TOEの管理情報はIADBへ格納されている。

管理コンソールは、まずIAマネージャにアクセスして、IADBにアクセスするためのID、パスワードの取得を行う。管理コンソールはそのID、パスワードを用いてIADBへアクセスし、IADBに格納されているTOEの管理情報の管理機能を提供する。

1.2.4 TOEの機能

本TOEの論理的範囲と保持する機能を図1-2に示す。

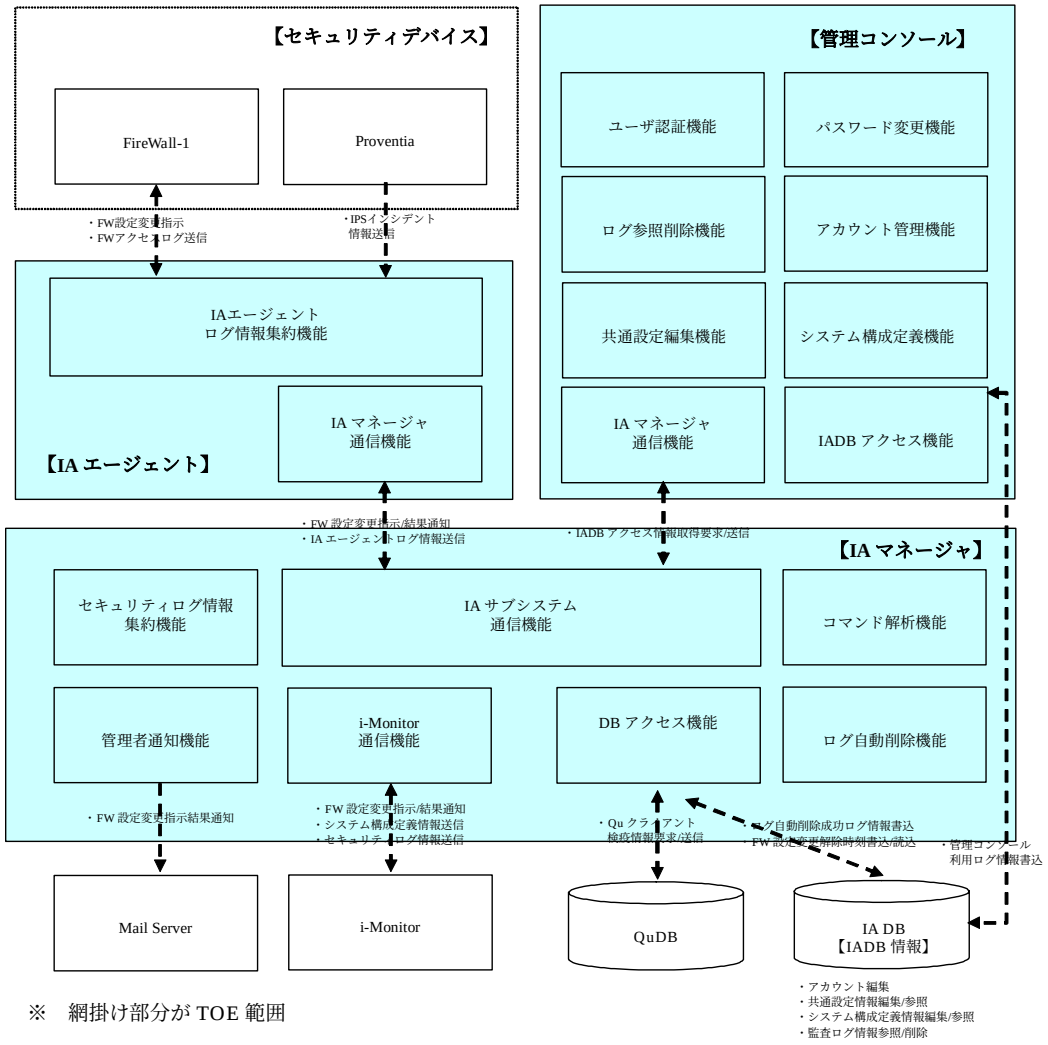

図1-2 TOEの論理的範囲と保持する機能

本TOEが保持する機能は、セキュリティ機能と非セキュリティ機能である一般機能に分類される。本TOEが保持するセキュリティ機能を表1-1に、本TOEが保持する一般機能を表1-2に示す。

表1-1　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 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 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。 ・アカウント管理機能 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。 ・パスワード変更機能 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。 ・ログ参照削除機能 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。

表1-2　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 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。 ・IAサブシステム通信機能 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。 ・DBアクセス機能 IADB、QuDBへアクセスを行う機能。 ・セキュリティログ情報集約機能 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。 ・コマンド解析機能 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。 ・管理者通知機能 Mail ServerへFW設定変更結果を送信する機能。

表1-2　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 IAマネージャと通信を行う機能。 ・IAエージェントログ情報集約機能 FW（FireWall-1)、IPS（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 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。 ・IADBアクセス機能 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。 ・共通設定編集機能 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。 ・システム構成定義機能 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。

1.3 評価の実施

認証機関が運営するITセキュリティ評価・認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証手続規程」[3]、「評価機関承認手続規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

(1) 本TOEのセキュリティ設計が適切であること。

(2) 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。

(3) 本TOEがセキュリティ設計に基づいて開発されていること。

(4) 上記(1)、(2)、(3)を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「汚染拡大防止システム SHIELD/ExLink-IA セキュリティターゲット」（以下「ST」という。）[1] 及び本TOE開発に関連する評価用提供物件を調査し、本TOEがCCパート1 ([5][8][11]のいずれか) 附属書C、CCパート2（[6][9][12]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発がCCパート3（[7][10][13]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「汚染拡大防止システム SHIELD/ExLink-IA v1.0 評価報告書」（以下「評価報告書」という。）[18]に示されている。なお、評価方法は、CEM（[14][15][16]のいずれか）に準拠する。また、CC及びCEMの各パートは補足[17]の内容を含む。

1.4 評価の認証

認証機関は、評価機関が作成した、評価報告書、所見報告書、及び関連する評価証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。評価は、平成19年3月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

1.5 報告概要

1.5.1 PP適合

適合するPPはない。

1.5.2 EAL

STが規定するTOEの評価保証レベルは、EAL1適合である。

1.5.3 セキュリティ機能強度

STは、AVA_SOF.1を含まないため、最小機能強度を主張しない。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能は、表1-1に示したように、以下のとおりである。

(1) 管理コンソールが保持するセキュリティ機能

・ユーザ認証機能
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。

・アカウント管理機能
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。

・パスワード変更機能
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。

・ログ参照削除機能
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。

(2) IAマネージャが保持するセキュリティ機能

・ログ自動削除機能
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。

1.5.5 脅威

本TOEは、表1-3に示す脅威を想定し、これに対抗する機能を備える。

表1-3　想定する脅威

識別子	脅　威
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。

1.5.6　組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針はない。

1.5.7　構成条件

本TOEは、IAマネージャ、IAエージェント、及び管理コンソールがインストールされたOS上で動作する。本TOEの動作に求められるスペック要件を表1-4に示す。

表1-4　TOEの動作に求められるスペック要件

No.	対象	要件	備考
1	IAマネージャ / IAエージェント	【動作環境OS】 Windows Server 2003 Standard Edition SP1 以降 Internet Explorer 6以上 【必須ハードウェア スペック】 CPU：550MHz以上 Memory：256 MB 以上 HDD：5GB以上	■OSは32bit版のみ対応 ■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。 ・Crypt32.dll ・Winhttp.dll
2	管理コンソール	【動作環境OS】	■ .net Framework 1.1 及び

		Windows 2000 Professional SP4 以降 Windows XP Professional SP2 以降 【必須ソフトウェア】 .Net Framework 1.1 VPN-1 SecuRemote （Check Point社のVPNソフトウェア） 【必須ハードウェア スペック】 CPU：300MHz以上 Memory：128 MB 以上 HDD：3GB以上	VPN-1 SecuRemoteは予めインストールする必要がある。

1.5.8 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表1-5に示す。

これらの前提条件が満たされない場合、本TOEのセキュリティ機能が有効に動作することは保証されない。

表1-5 TOE使用の前提条件

識別子	前提条件
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、FW（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FW（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	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。

識別子	前提条件
理）	
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。

1.5.9 製品添付ドキュメント

本TOEに添付されるドキュメントを以下に示す。

・汚染拡大防止システム SHIELD/ExLink-IA インストールマニュアル
バージョン1.05

・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
バージョン1.09

2 評価機関による評価実施及び結果

2.1 評価方法

評価は、CCパート3の保証要件について、CEMに規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

2.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成18年11月に始まり、平成19年3月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成18年12月、平成19年1月に開発者サイトで開発者のテスト環境を使用し、評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

2.3 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を以下に示す。

2.3.1 開発者テスト

本TOEでは、開発者テストは評価対象外である。

2.3.2 評価者テスト

1) 評価者テスト環境

評価者が実施したテストの環境を図2-1に、TOEの動作に関係する各構成要素の要件を表2-1示す。

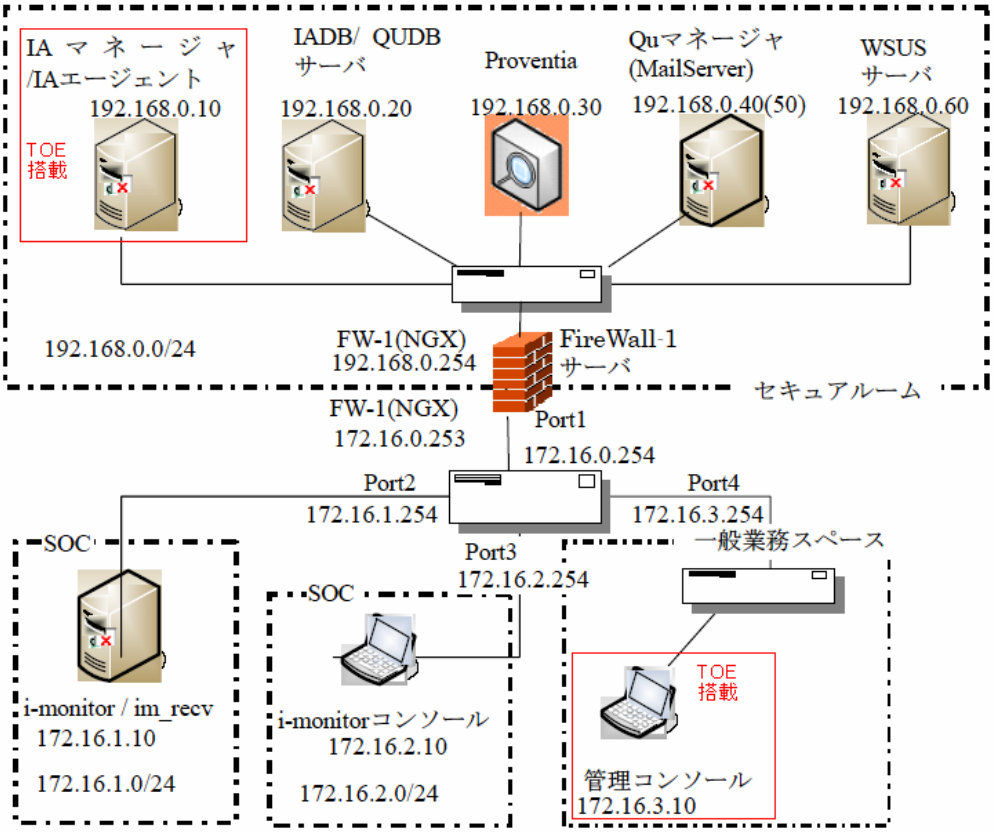

図2-1　評価者テストの環境

表2-1　評価者テストの環境におけるTOEの動作に関係する各構成要素の要件

No	構成要素名	要件	備考
1	IA マネージャ/ IA エージェントサーバ	(HW) CPU:2.8GHz, Memory:1GB, HDD:5GB 以上 (OS) Windows Server 2003 SP1 (TOE) SHIELD/ExLink-IA マネージャ v1.0 SHIELD/ExLink-IA エージェン v1.0	TOE搭載
2	IADB/QuDB	(OS) Windows Server 2003 SP1 (SW) SQL Server 2000 Standard Edition SP4	—
3	Proventia	Proventia model GX4002C	—
4	FireWall-1	(OS) Windows Server 2003 SP1 (SW) Check point ngcmp NGX_R60_03	—
5	管理コンソール端末	(HW) CPU:1100MHz, Memory:248MB, HDD:3GB 以上	TOE搭載

		(OS) Windows XP SP2 (SW) .NetFramework 1.1, Check point VPN-1 SecuRemote NGX R60 HFA1 (TOE) SHIELD/ExLink 管理コンソール v1.0	
6	SOC	SOC は、図にあるとおり次の2 台のマシンで構成。 a) i-Monitor/im_recv (OS) CentOS (SW) apache, Tomcat, JetSpeed, e-post,Oracle10g Release2 b) i-Monitor コンソール (OS) Windows XP SP2 (SW) i-Monitor コンソール ソフトウェア	―

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

評価者が実施したテストの構成を図2-1、TOEの動作に関係する各構成要素の要件を表2-1に示す。評価者テストはSTにおいて識別されているTOE構成を満たすテスト環境で実施されている。

b.テスト手法

テストには、以下の手法が使用された。

①ガイダンス文書の記述内容に従って、外部インタフェースからセキュリティ機能に刺激（パラメータ）を与え、外部インタフェースでセキュリティ機能のふるまいを目視確認する

②外部インタフェースからの刺激方法は、ほとんどのテストは管理コンソールにおける操作で実施可能あり、唯一、ログ自動削除機能だけは、タイマ起動のインタフェースなので、データベース整理開始時間を適切な時刻に設定することにより、適切な時刻でタイマを起動させ、セキュリティ機能を刺激する

③外部インタフェースからのセキュリティ機能のふるまいは、これら刺激の結果、画面に表示されるメッセージやIADB 上のログ管理テーブルを確認する

c.実施テストの範囲

評価者が独自に考案した計27項目のテストを実施した。テスト項目の選択基準として、すべてのセキュリティ機能を選択することを考慮している。

d.結果

実施したすべての評価者テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

2.4 評価結果

評価報告書をもって、評価者は本TOEがCEMのワークユニットすべてを満たしていると判断した。

3 認証実施

評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 当該所見報告書でなされた指摘内容が妥当であること。

② 当該所見報告書でなされた指摘内容が正しく反映されていること。

③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。

④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。

⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。

認証機関は、ST及び評価報告書において、所見報告書及び認証レビューで指摘された問題点が解決されていることを確認した。

4 結論

4.1 認証結果

提出された評価報告書、当該所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL1保証要件を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

表4-1　評価者アクションエレメント検証結果

評価者アクションエレメント	検証結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_DES.1.1E	評価はワークユニットに沿って行われ、TOE種別、境界の記述が明瞭であることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然とし一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_DES.1.3E	評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_ENV.1.1E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_ENV.1.2E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.1E	評価はワークユニットに沿って行われ、ST概説がST及びTOEの識別、概要及びCC適合が明確に述べられていることを確認している。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.3E	評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。

ASE_OBJ.1.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が、脅威、組織のセキュリティ方針、前提条件へ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_OBJ.1.2E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が完全で、理路整然としていて、かつ一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_PPC.1.1E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_PPC.1.2E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_REQ.1.1E	評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_REQ.1.2E	評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が完全で、理路整然としていて、かつ一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_SRE.1.1E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。

ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
構成管理	**適切な評価が実施された**
ACM_CAP.1.1E	評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認している。
配付と運用	**適切な評価が実施された**
ADO_IGS.1.1E	評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。
ADO_IGS.1.2E	評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
開発	**適切な評価が実施された**
ADV_FSP.1.1E	評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んでいることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ADV_FSP.1.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ADV_RCR.1.1E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であることを、それらの対応分析により確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ガイダンス文書	**適切な評価が実施された**

AGD_ADM.1.1E	評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
AGD_USR.1.1E	評価はワークユニットに沿って行われ、利用者ガイダンスがTOEの管理者でない利用者が利用可能なセキュリティ機能やユーザインタフェース、セキュリティ機能の使用法、対応すべき機能や特権に関する警告、TOEのセキュアな操作に必要なすべての利用者責任が記述してあり、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
テスト	**適切な評価が実施された**
ATE_IND.1.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、TOEと同等の資源が提供されていることを確認している。
ATE_IND.1.2E	評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。

4.2 注意事項

特になし。

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CSO	Chief Security Officer
DB	DataBase
EAL	Evaluation Assurance Level
FW	FireWall
HW	Hardware
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
PP	Protection Profile
SOC	Security Operation Center
SOF	Strength of Function
SSL	Secure Socket Layer
ST	Security Target
SW	Software
TOE	Target of Evaluation
TSF	TOE Security Functions
VPN	Virtual Private Network

本報告書で使用された用語を以下に示す。

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。指示には制御対象機器と制御内容が含まれている。
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。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。
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。

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イルス、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、ウイルスチェックソフトウェアにおける最新のウイルス定義ファイルの適用状況等が含まれている。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。
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。
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。

6 参照

[1] 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年3月5日 株式会社 日立情報システムズ

[2] ITセキュリティ評価及び認証制度の基本規程　平成18年9月　独立行政法人 情報処理推進機構　EC-01

[3] ITセキュリティ認証手続規程　平成18年9月　独立行政法人 情報処理推進機構　EC-03

[4] 評価機関承認手続規程　平成18年9月　独立行政法人 情報処理推進機構　EC-05

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] 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)

[9] 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)

[10] 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)

[11] ISO/IEC 15408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン2.3 2005年8月 (平成17年12月翻訳第1.0版)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] 補足-0512　平成17年12月

[18] 汚染拡大防止システム SHIELD/ExLink-IA v1.0 評価報告書 第2.2版 2007年3月9日 社団法人 電子情報技術産業協会 ITセキュリティセンター