認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙 押印済

評価対象

申請受付日（受付番号）	**平成19年5月28日** (IT**認証**7153)
認証番号	C0174
認証申請者	**富士通株式会社**
TOE**の名称**	Systemwalker Centric Manager Enterprise Edition
TOE**のバージョン**	V13.2.0（Linux for Itanium）
PP**適合**	**なし**
適合する保証パッケージ	EAL1
開発者	**富士通株式会社**
評価機関の名称	**有限責任中間法人 ITセキュリティセンター 評価部**

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20年8月7日

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　鈴木　秀二

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

「Systemwalker Centric Manager Enterprise Edition V13.2.0（Linux for Itanium）」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、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、「Systemwalker Centric Manager Enterprise Edition V13.2.0（Linux for Itanium)」（以下「本TOE」という。）について有限責任中間法人 ITセキュリティセンター 評価部（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富士通株式会社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： Systemwalker Centric Manager Enterprise Edition V13.2.0
バージョン： V13.2.0（Linux for Itanium）
開発者： 富士通株式会社

1.2.2 製品概要

本製品は、業務システムの安定稼動に必要な運用管理を支援するソフトウェア製品である。業務システムを構成するサーバ、クライアント、及びハブやルータ等のネットワーク機器（以降、これらを総称して業務システム資産と呼ぶ）に対して、本製品が定義するデプロイ（配付)、モニタリング（監視)、リカバリ（復旧)、そして、アセスメント（査定）の4つの運用管理フェーズにより、その運用管理をトータルに支援する。

- デプロイ（配付）は業務サーバや業務クライアントへのソフトウェアやデータの配備を行うフェーズであり、本TOEはソフトウェアやデータの配付と適

用を行う資源配付機能を提供する。

- モニタリング（監視）は業務システムの異常状態の監視を行うフェーズであり、本TOEは稼動状況や性能等の監視のための事象監視機能を提供する。
- リカバリ（復旧）は業務システムがトラブルに陥った場合の原因調査や復旧を行うフェーズであり、本TOEはサーバやクライアントに対するトラブル調査や復旧のための操作機能を提供する。
- アセスメント（査定）は業務システムを定期的に評価・分析し、必要な予防処置を策定するフェーズであり、本TOEは業務システムの稼動分析機能を提供する。

(注釈) 以降、本報告書で「デプロイ」、「モニタリング」、「リカバリ」、及び「アセスメント」の用語を使用した場合、運用管理フェーズの名称である。表記の異なる同義語は、運用管理フェーズの名称ではない。(例えば「監視」は、監視という行為を表す。)

1.2.3 TOEの範囲と動作概要

TOEの範囲は、製品「Systemwalker Centric Manager Enterprise Edition V13.2.0（Linux for Itanium）」と同一である。TOEは、以下に示す要素から構成される。

構成要素	概要	本報告書での略称
運用管理サーバ向けソフトウェア	業務システム全体の運用管理を行うためのサーバソフトウェアであり、運用管理サーバに導入される。また、全体監視サーバを利用する場合には、全体監視サーバにも導入される。	CMGR/MGR
部門管理サーバ向けソフトウェア	部門内の運用管理を行うためのサーバソフトウェアであり、部門管理サーバに導入される。多数の業務サーバから成る大規模な業務システムを対象に、部門内の運用管理を行うことで運用管理サーバの負荷分散を図る。 また、業務サーバが部門管理サーバを兼ねるため、当ソフトウェアは業務サーバ向けソフトウェアを包含する。	CMGR/Agent(S)

構成要素	概要	本報告書での略称
業務サーバ向けソフトウェア	被管理対象のサーバに導入されるサーバソフトウェアである。業務サーバに導入される。また、開発用サーバに導入されて、サーバ資源の登録に利用される。	CMGR/Agent(J)
運用管理クライアント向けソフトウェア	運用管理者及び運用担当者のためのコンソール機能を提供するクライアントソフトウェアである。運用管理クライアントに導入される。	CMGR/CL(M)
業務クライアント向けソフトウェア	被管理対象のクライアントに導入されるクライアントソフトウェアである。業務クライアント及び開発用クライアントに導入される。	CMGR/CL(U)

注）以降、本報告書では、CMGR/MGR、CMGR/Agent(S)、CMGR/Agent(J)、CMGR/CL(M)及びCMGR/CL(U)はTOEの構成要素を表し、運用管理サーバ、運用管理クライアント、業務サーバ等の用語は、TOEの構成要素が動作するサーバやクライアントを表すものとする。

TOEは、複数のサーバ及びクライアントを含むシステムに導入されることが想定される。TOEを導入するシステムに含まれるサーバ及びクライアントには、以下のものがある。

構成要素	概要
運用管理サーバ	業務システム全体の監視、操作、資源配付を行なう専用サーバであり、運用管理クライアントから操作を行う。
運用管理クライアント	運用管理サーバまたは全体監視サーバを操作するためのコンソール機能を持つクライアントである。
業務サーバ	本TOEが運用管理の対象とする業務処理を行うサーバである。
業務クライアント	業務サーバと連携して業務処理を行うクライアントである。
部門管理サーバ	運用管理サーバの負荷を分散させるためのサーバである。1台の運用管理サーバでは能力的に無理な多数の業務サーバからなる大規模システムに対して、部門管理サーバはいくつかの業務サーバを束ねることで、運用管理サーバの負荷を軽減させる役割を果す。

構成要素	概要
全体監視サーバ	運用管理サーバの利用形態の一つである。例えば、地区毎に運用管理サーバを用意し、地区独立で運用管理しているようなシステムを全社レベルで監視するような場合に、業務サーバから運用管理サーバへ監視対象イベントを通知するのと同様に、全体監視サーバに位置づけた運用管理サーバに、配下の運用管理サーバから監視対象イベントを集めることで全体監視を実現する。
開発用サーバ	(業務で使用する)サーバ資源を開発するためサーバである。
開発用クライアント	(業務で使用する)クライアント資源を開発するためのクライアントである。

図1-1はTOEを導入するシステム及びTOEの構成要素の配置と、TOEの関連者の関係である。TOEは以下の図1-1のような構成で動作し、デプロイ、モニタリング、リカバリ、アセスメントの各フェーズの運用を支援する。TOEの関連者の具体的な内容は「1.2.4 TOEの関係者」、支援の具体的な内容は「1.2.5 TOEの機能」に示す。

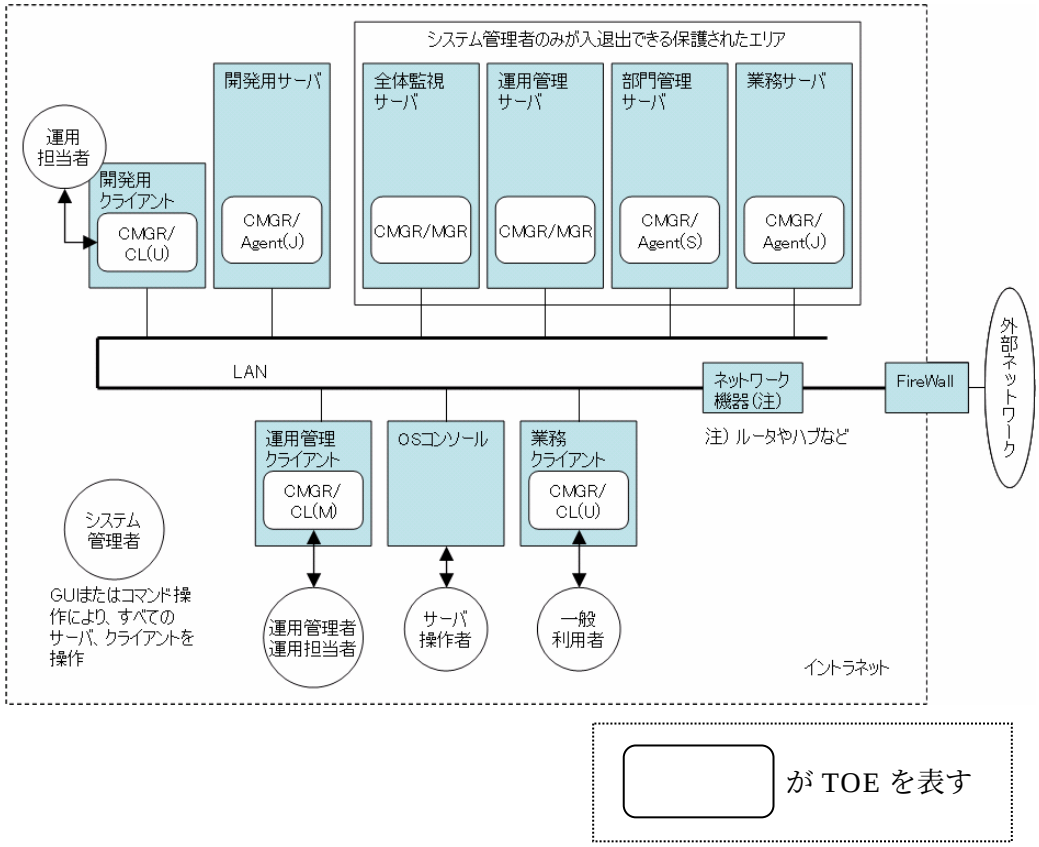
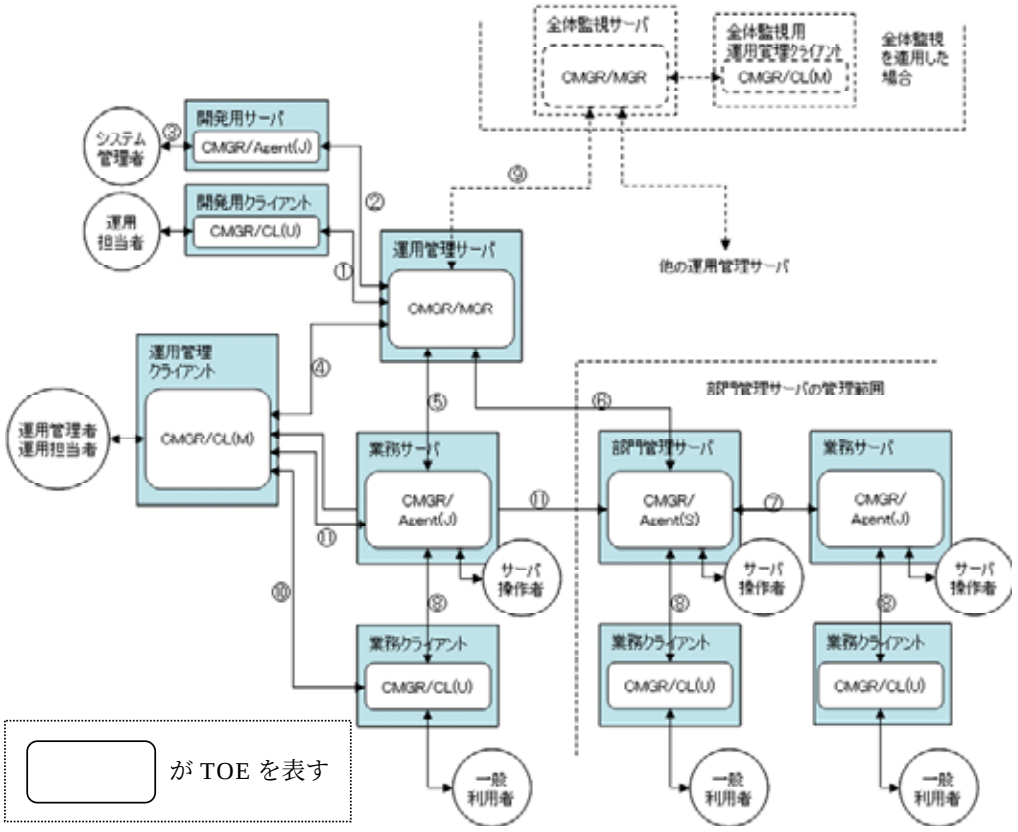


図1-1　物理的構成要素の配置とTOEの関連者との関係

TOEの構成要素は、全体監視サーバ以外は複数存在する構成が可能である。図1-2

は、そのような場合の論理的な構造である。



(注) サーバ操作者が業務サーバや部門管理サーバを設置場所で直接操作するわけではない。図1-1のようにLANを介してこれらのサーバの操作を行うことを示したものである。

図1-2　TOEの論理的な接続形態

1.2.4　TOEの関係者

TOEは、以下の関係者を想定する。

関連者	説明
システム管理者	主に本TOEを利用する者に対する利用者登録や権限設定等の操作を行う。 また、運用管理者、運用担当者、サーバ操作者が行えるすべての操作を行う権限をもつ。
運用管理者	システム管理者から運用管理者の権限を与えられた者である。 運用管理者権限の範囲内で、本TOEによる運用管理に必要な環境の設定や変更を行う。また、運用担当者が行えるすべての操作を行う権限をもつ。

関連者	説明
運用担当者	システム管理者または運用管理者から運用操作を行う権限を与えられた者であり、資源配付の操作及び、許可された範囲内の特定業務サーバの特定業務に対する監視、復旧、査定のための操作を行う。
サーバ操作者	本TOEが管理対象とする業務サーバ個々に割り当てられたオペレータであり、その業務サーバに対する操作（例えば、業務サーバのアプリケーションの起動、停止など）のみを行う。
一般利用者	本TOEが管理対象とする業務システムを利用して業務処理を行う者であり、本TOEを利用してクライアント資源のダウンロードと適用を行う。

1.2.5 TOEの機能

TOEは、デプロイ、モニタリング、リカバリ、アセスメントの各フェーズの運用を支援する機能を持つ。以降に、TOEが支援のために提供する機能について、各フェーズごとに示す。

1.2.5.1 デプロイのフェーズを支援する TOE の機能

デプロイのフェーズの支援のために、TOEは以下の機能を提供する。

- 「資源配付のための定義情報」の定義
  「資源配付のための定義情報」を定義することにより、TOEの各要素の接続形態(図1-2のようなもの)を定義する。
- サーバ資源の配付
  サーバ資源を開発用サーバから受け取り、業務サーバへ配付する。
- クライアント資源の配付
  クライアント資源を開発用クライアントから受け取り、業務クライアントへ配付する。

以下に、これらの機能の詳細について示す。

- 「資源配付のための定義情報」の定義
  (1) 運用管理者は、「運用管理クライアントのCMGR/CL(M)」を操作し、「資源配付のための定義情報」の定義を行う。
  「資源配付のための定義情報」は「運用管理サーバのCMGR/MGR」が受け取り、そこで保持される。(図1-2 ④)
  この操作は、「ACLマネージャ機能」により、運用管理者に制限される。

- サーバ資源の配付
  (1) システム管理者は、「開発用サーバのCMGR/Agent(J)」を操作し、サーバ資源を登録する。(図1-2 ③)
  (2) システム管理者は、「開発用サーバのCMGR/Agent(J)」を操作し、サーバ資源のアップロードを指示する。(図1-2 ③)
  「運用管理サーバのCMGR/MGR」は、「開発用サーバのCMGR/Agent(J)」からサーバ資源を受け取り、保存する。(図1-2 ②)
  この操作は、「ACLマネージャ機能」により、システム管理者に制限される。
  (3) 運用担当者は、「運用管理クライアントのCMGR/CL(M)」を操作し、サーバ資源の配付先(部門管理サーバまたは業務サーバ)を指定して配付を指示する
  「運用管理サーバのCMGR/MGR」が指示を受ける。(図1-2 ④)
  この操作は、「ACLマネージャ機能」により、運用担当者に制限される。
  (4) 「運用管理サーバのCMGR/MGR」は、指定された配付先の各「部門管理サーバのCMGR/Agent(S)」または「業務サーバのCMGR/Agent(J)」へと、サーバ資源を配付する。
  この配付の経路には、以下の2通りがあり、「資源配付のための定義情報」によって決まる。
    - 「運用管理サーバのCMGR/MGR」から「業務サーバのCMGR/Agent(J)」へと直接配付される(図1-2 ⑤)。
    - 「運用管理サーバのCMGR/MGR」から「部門管理サーバのCMGR/Agent(S)」へと配付される。(図1-2 ⑥)
      さらにそこからその部門管理サーバの管理範囲内の「業務サーバのCMGR/Agent(J)」へと配付される(図1-2 ⑦)。
  (5) 運用担当者は、「運用管理クライアントのCMGR/CL(M)」を操作し、部門管理サーバまたは業務サーバを指定してサーバ資源の適用を指示する
  「部門管理サーバのCMGR/Agent(S)」または「業務サーバのCMGR/Agent(J)」はその指示を受ける。(図1-2 ⑪)
  この操作は、「ACLマネージャ機能」により、運用担当者に制限される。
  (6) 各業務サーバのCMGR/Agent(J)は、配付されたサーバ資源を適用(指定されたディレクトリに格納)する。

- クライアント資源の配付
  (1) 運用担当者は、「開発用クライアントのCMGR/CL(U)」を操作し、クライアント資源を登録する。

(2) 運用担当者は、「開発用クライアントのCMGR/CL(U)」を操作し、クライアント資源のアップロードを指示する。
「運用管理サーバのCMGR/MGR」は、「開発用クライアントのCMGR/CL(U)」からクライアント資源を受け取り、保存する。(図1-2 ①)

(3) 運用担当者は、「運用管理クライアントのCMGR/CL(M)」を操作し、クライアント資源の配付先(業務クライアント)を指定して配付を指示する。
「運用管理サーバのCMGR/MGR」は、この指示を受ける。(図1-2 ④)
この操作は、「ACLマネージャ機能」により、運用担当者に制限される。

(4) 「運用管理サーバのCMGR/MGR」は、指定された業務クライアントがダウンロード可能な「部門管理サーバのCMGR/Agent(S)」または「業務サーバのCMGR/Agent(J)」へと、クライアント資源を配付する。
この配付の経路には、以下の2通りがあり、「資源配付のための定義情報」によって決まる。
- 「運用管理サーバのCMGR/MGR」から「業務サーバのCMGR/Agent(J)」へと直接配付される(図1-2 ⑤)。
- 「運用管理サーバのCMGR/MGR」から「部門管理サーバのCMGR/Agent(S)」へと配付され(図1-2 ⑥)、そこからその部門管理サーバの管理範囲内の「業務サーバのCMGR/Agent(J)」へと配付される(図1-2 ⑦)。

(5) 一般利用者は、「業務クライアントのCMGR/CL(U)」を操作し、クライアント資源のダウンロードと適用を指示する。

(6) 「業務クライアントのCMGR/CL(U)」は、「部門管理サーバのCMGR/Agent(S)」または「業務サーバのCMGR/Agent(J)」からクライアント資源をダウンロードし、指定されたディレクトリに格納する。

1.2.5.2 モニタリングのフェーズを支援する TOE の機能

モニタリングのフェーズの支援のために、TOEは以下の機能を提供する。

- 「事象監視のための定義情報」の定義
  「事象監視のための定義情報」を定義することにより、以下を定義する。
  - どのネットワーク機器及びサーバをどの時間間隔で監視し、どの事象が検出された場合を監視の対象にするか
  - 検出された事象は、どのような経路で運用管理サーバに通知するか
  - 運用管理サーバに集められたイベントのうち、どのイベントを全体監視サーバに通知するか
- ネットワーク機器・サーバの監視

「事象監視のための定義情報」に従い、ネットワーク機器及びサーバで発生するイベントを運用管理サーバに集積し、運用管理クライアントから参照できるようにする。
運用管理サーバに集積されたイベントのうち指定されたものをさらに全体監視サーバに集積し、全体監視用運用管理クライアントから参照できるようにする。

以下に、これらの機能の詳細について示す。

- 「事象監視のための定義情報」の定義
  (1) 運用管理者は、「運用管理クライアントのCMGR/CL(M)」を操作し、「事象監視のための定義情報」の定義を行う。
  「事象監視のための定義情報」は「運用管理サーバのCMGR/MGR」が受け取る。(図1-2 ④)
  この操作は、「ACLマネージャ機能」により、運用管理者に制限される。

  (2) 「運用管理サーバのCMGR/MGR」は、「事象監視のための定義情報」の中の、各サーバによる監視に必要な情報を、「部門管理サーバのCMGR/Agent(S)」及び「業務サーバのCMGR/Agent(J)」に通知する。

- ネットワーク機器・サーバの監視
  (1) 「部門管理サーバのCMGR/Agent(S)」及び「業務サーバのCMGR/Agent(J)」は、ネットワーク機器及びサーバで発生するイベントを以下のように収集する。
    - 指定されたネットワーク機器及びサーバを指定された時間間隔で監視し、指定された事象が発生した場合にイベントとして収集する。(例えば、SNMPのMIB情報の監視が該当する。)
      これらの指定は、「事象監視のための定義情報」で定義される。
    - ネットワーク機器及びサーバから不定期に通知されるイベントを収集する。(例えば、SNMPトラップやシスログが該当する。)

  (2) 「部門管理サーバのCMGR/Agent(S)」及び「業務サーバのCMGR/Agent(J)」は、収集したイベントを「運用管理サーバのCMGR/MGR」に通知する。「運用管理サーバのCMGR/MGR」は通知されたイベントを保存する。
  この通知の経路には、以下の2通りがあり、「事象監視のための定義情報」によって決まる。
    - 「業務サーバのCMGR/Agent(J)」から「運用管理サーバのCMGR/MGR」へと直接通知される(図1-2 ⑤)。
    - 部門管理サーバの管理範囲内の「業務サーバのCMGR/Agent(J)」から「部門管理サーバのCMGR/Agent(S)」へと通知され(図1-2

⑦)、そこから「運用管理サーバのCMGR/MGR」へと通知される(図1-2 ⑥)。

(3) 運用担当者は、「運用管理クライアントのCMGR/CL(M)」を操作し、「運用管理サーバのCMGR/MGR」に保存されたイベントを参照する。この操作は、「ACLマネージャ機能」及び「コンソール操作制御機能」により、個々の運用担当者ごとに許可される範囲が制限される。

(4) 「運用管理サーバのCMGR/MGR」は、「監視のための定義情報」に従い選択したものを「全体監視サーバのCMGR/MGR」に通知する。「全体監視サーバのCMGR/MGR」は、通知されたイベントを保存する。

(5) 運用担当者は、「全体監視用運用管理クライアントのCMGR/CL(M)」を操作し、「全体監視サーバのCMGR/MGR」に保存されたイベントを参照する。
この操作は、「ACLマネージャ機能」及び「コンソール操作制御機能」により、個々の運用担当者ごとに許可される範囲が制限される。

1.2.5.3 リカバリのフェーズを支援する TOE の機能

リカバリのフェーズの支援のために、TOEは以下の機能を提供する。

- 「復旧のための定義情報」の定義
  「復旧のための定義情報」を定義することにより、以下を定義する。
  - 以下の「リモートコマンド(サーバ)」で使用する、「部門管理サーバまたは業務サーバの識別」と「コマンド」
- リモートコマンド(サーバ)
  運用管理クライアントから、部門管理サーバまたは業務サーバへとコマンドを送り、そのサーバでコマンドを実行させる。
- サーバ操作
  部門管理サーバまたは業務サーバでコマンドを実行させる。
- LiveHelp (クライアント)
  運用管理クライアントから、業務クライアントまたは別の運用管理クライアントの画面を参照する。その参照された画面から、業務クライアントまたは別の運用管理クライアントの操作ができるようにする。

以下に、これらの機能の詳細について示す。

- 「復旧のための定義情報」の定義
  (1) 運用管理者は、「運用管理クライアントのCMGR/CL(M)」を操作し、「復旧のための定義情報」の定義を行う。
  「復旧のための定義情報」は「運用管理サーバのCMGR/MGR」が受け取り、そこで保持される。(図1-2 ④)

この操作は、「ACLマネージャ機能」により、運用管理者に制限される。

- リモートコマンド(サーバ)
  (1) 運用担当者は、「運用管理クライアントのCMGR/CL(M)」を操作し、「運用管理サーバのCMGR/MGR」に対して、「コマンド」及び「部門管理サーバまたは業務サーバの識別」を指示する。
  この操作は、「ACLマネージャ機能」及び「コンソール操作制御機能」により、個々の運用担当者ごとに許可される範囲(指定できるサーバ及びコマンド)が制限される。

  (2) 「運用管理サーバのCMGR/MGR」は、指示されたコマンドを、指示された部門管理サーバのCMGR/Agent(S)または指示された業務サーバのCMGR/Agent(J)へと送付する。

  (3) 「部門管理サーバのCMGR/Agent(S)」または「業務サーバのCMGR/Agent(J)」は、送付されたコマンドを、その部門管理サーバまたは業務サーバで実行させる。

- サーバ操作
  (1) サーバ操作者は、部門管理サーバまたは業務サーバのOSにログインする。通常は、図1-1のように、部門管理サーバまたは業務サーバ以外のOSコンソールからリモートログインする。

  (2) サーバ操作者は、その部門管理サーバまたは業務サーバで実行したいコマンドを、「部門管理サーバのCMGR/Agent(S)」または「業務サーバのCMGR/Agent(J)」に指示する。
  この操作は、「サーバ操作制御機能」により、個々のサーバ操作者ごとに許可される範囲(指示できるサーバとコマンドの組み合わせ)が制限される。

  (3) 「部門管理サーバのCMGR/Agent(S)」または「業務サーバのCMGR/Agent(J)」は、指示されたコマンドを、その部門管理サーバまたは業務サーバで実行させる。

- LiveHelp (クライアント)
  (1) 運用担当者は、「運用管理クライアントのCMGR/CL(M)」を操作し、どの業務クライアントまたは別の運用管理クライアントのリモート操作を行うかを指示する。
  この操作は、「LiveHelp接続認証機能」により、個々の運用担当者ごとに許可される範囲(指定できるクライアント)が制限される。

  (2) 「運用管理クライアントのCMGR/CL(M)」は、指示された業務クライ

アントのCMGR/CL(U)または指示された別の運用管理クライアントのCMGR/CL(M)との通信路を確立し、業務クライアントまたは別の運用管理クライアントの画面を参照して操作を行えるようにする。

1.2.5.4 アセスメントのフェーズを支援する TOE の機能

アセスメントのフェーズの支援のために、TOEは以下の機能を提供する。

- 「ログ収集のための定義情報」の定義
  「ログ収集のための定義情報」を定義することにより、以下を定義する。
  - 以下の「ログ収集管理」において、どのサーバのどのログファイルを収集するか
- ログ収集管理
  部門管理サーバ及び業務サーバで収集されたログファイルを、運用管理サーバに集積する。
- レポーティング
  「ログ収集管理」で運用管理サーバに集積されたログファイルをもとに、稼働状況等をグラフや表で表示する。

以下に、これらの機能の詳細について示す。

- 「ログ収集のための定義情報」の定義
  (1) 運用管理者は、「運用管理クライアントのCMGR/CL(M)」から「運用管理サーバのCMGR/MGR」に対して、「ログ収集のための定義情報」の定義を行う。
  この操作は、「ACLマネージャ機能」により、運用管理者に制限される。

- ログ収集管理
  (1) 「部門管理サーバのCMGR/Agent(S)」及び「業務サーバのCMGR/Agent(J)」は、「ログ収集のための定義情報」によって指定されたログファイルを「運用管理サーバのCMGR/MGR」に、「ログ収集のための定義情報」によって指定された時間間隔で転送する。

- レポーティング
  (1) 運用担当者は、「運用管理クライアントのCMGR/CL(M)」から、ログファイルのどの情報の統計情報からグラフや表を作成するかを指示する。
  この操作は、「ACLマネージャ機能」及び「コンソール操作制御機能」により、個々の運用担当者ごとに許可される範囲が制限される。

  (2) 「運用管理クライアントのCMGR/CL(M)」は、指示されたグラフや表

の作成に必要な情報を「運用管理サーバのCMGR/MGR」に収集されているログファイルから取得し、グラフや表を作成する。

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セキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[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「Systemwalker Centric Manager Enterprise Edition V13.2.0 Linux版 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B、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、「富士通株式会社 Systemwalker Centric Manager Enterprise Edition V13.2.0（Linux版）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20年6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が規定するセキュリティ保証要件にAVA_SOF.1が含まれないため、STは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、以下のとおりである。

- ACLマネージャ機能

  アクセス制御の機能であり、以下の操作が対象である。

  - 「運用管理クライアントのCMGR/CL(M)」からの操作(LiveHelp(クライアント)は除く)
  - 「部門管理サーバのCMGR/Agent(S)」からの操作
  - 「業務サーバのCMGR/Agent(J)」からの操作

  この機能の対象は、以下の役割である。

  - システム管理者
  - 運用管理者
  - 運用担当者

  この機能は、対象となる操作を定められた役割に制限する機能である。この機能は役割ごとの制限であり、個々の利用者ごとの制限はこの機能ではない。対象となる操作と役割についての詳細は「1.2.5 TOEの機能」参照。

  誰がどの役割を持つかの設定は、「運用管理クライアントのCMGR/CL(M)」からシステム管理者または運用管理者のみが設定できるように、「ACLマネージャ機能」により制限される。

- コンソール操作制御機能

  アクセス制御の機能であり、以下の操作が対象である。

  - 「運用管理クライアントのCMGR/CL(M)」からの操作(資源配付及びLiveHelp(クライアント)は除く)

  この機能の対象は、以下の役割である。

  - 運用担当者

この機能は、「ACLマネージャ機能」で運用担当者に許可された「運用管理クライアントのCMGR/CL(M)」からの操作について、個々の運用担当者ごとに定められた範囲の操作に制限する機能である。

個々の運用担当者ごとに許可される操作の範囲は、「運用管理クライアントのCMGR/CL(M)」からシステム管理者のみが設定できるように、「ACLマネージャ機能」により制限される。

- サーバ操作制御機能

  アクセス制御の機能であり、以下の操作が対象である。

  - 「部門管理サーバのCMGR/Agent(S)」からの操作
  - 「業務サーバのCMGR/Agent(J)」からの操作

  この機能の対象は、以下の役割である。

  - サーバ操作者

  この機能は、「部門管理サーバのCMGR/Agent(S)」または「業務サーバのCMGR/Agent(J)」からの操作について、個々のサーバ操作者ごとに定められた範囲の操作に制限する機能である。

  個々のサーバ操作者ごとに許可される操作の範囲は、「運用管理クライアントのCMGR/CL(M)」からシステム管理者または運用管理者のみが設定できるように、「ACLマネージャ機能」により制限される。

- LiveHelp接続認証機能

  識別・認証の機能であり、以下の操作が対象である。

  - 「運用管理クライアントのCMGR/CL(M)」からのLiveHelp(クライアント)の操作

  この機能の対象は、以下の役割である。

  - 運用担当者

  この機能は、「運用管理クライアントのCMGR/CL(M)」からのLiveHelp(クライアント)の操作を、定められた運用担当者に制限する機能である。

  この機能は、「LiveHelp(クライアント)」の機能で操作の対象となる業務クライアントまたは別の運用管理クライアントにおいて、以下のいずれかで実現される。どちらの方法での認証を受け付けるかは、各業務クライアントまたは各運用管理クライアントの設定により決まる。

  - 業務クライアントまたは運用管理クライアントのOSの識別・認証機能
  - 「業務クライアントのCMGR/CL(U)」または「運用管理クライアントのCMGR/CL(M)」の識別・認証機能

- 監査ログ機能

  以下の事象を監査ログとして記録する。

  - TOEによる識別・認証が行われた、またはOSによる識別・認証の結

果を受け入れた事象。

- 役割と利用者の関連付け､個々の運用担当者またはサーバ操作者に許可される操作を変更した事象
- 「ACLマネージャ機能」､「コンソール操作制御機能」、または「サーバ操作制御機能」で許可された操作を実行した事象

記録された監査ログは、システム管理者のみが参照できる状態で保存される(システム管理者のみに制限するのはOSの機能である)。

監査ログはCSV形式で保存され、その参照や分析にはCSV形式に対応した市販のソフトウェアが用いられることを想定する。

- 適用結果の自動通知機能

  運用管理機能の資源配付を構成する機能要素の一つであり、配付資源の配付及び適用の結果を上位システムへ自動通知する機能を提供する。これにより、サーバ、クライアントにおける配付資源の適用状況を確実に把握することができる。CMGR/CL(U)ではCMGR/Agent(S)またはCMGR/Agent(J)への通知機能を提供し、CMGR/Agent(S)及びCMGR/Agent(J)ではCMGR/MGRへの通知機能を提供する。

- サーバ上のTOEにログインするためのパスワードの保護機能

  ログインする際のパスワードが解読されないよう、独自のメカニズムにより異なるデータに変換及び復元する機能を提供する。CMGR/CL(M)及びCMGR/CL(U)でパスワードの変換を行い、ログイン先であるCMGR/MGR、CMGR/Agent(J)及びCMGR/Agent(S)でパスワードの復元を行う。

1.5.5 脅威

本TOEは、以下を保護資産とする。

- 運用管理で使用する資産
  - 各フェーズで使用する定義情報
    - ✧ 資源配付のための定義情報
    - ✧ 監視のための定義情報
    - ✧ 復旧のための定義情報
    - ✧ ログ収集のための定義情報
  - 収集情報
    - ✧ モニタリングのフェーズで収集されるイベント情報
    - ✧ アセスメントのフェーズで収集されるログファイル
  - 配付資源

    (注) 開発用サーバまたは開発用クライアントに存在するものは保護資産ではない。「運用管理サーバのCMGR/MGR」が受け取った時点から、配付資源は保護資産として扱われる。

- サービスの資産
  - 部門管理サーバまたは業務サーバでのコマンド実行(「1.2.5.3 リカバリのフェーズを支援するTOEの機能」の「サーバ操作」と「リモートコマンド(サーバ)」)
  - LiveHelpによるLiveHelpクライアントのリモート操作
- 上記の資産を保護するために保護が必要となる二次的な資産
  - LiveHelpにおいて認証に使用される、OSまたはTOEのパスワード
  - サーバ上のTOEにログインするための、OSのパスワード

本TOEは、表1-1(1)～表1-1(4)に示す脅威を想定し、これに対抗する機能を備える。

表1-1(1)　想定する脅威(すべての運用管理フェーズに共通な脅威)

識別子	脅　威
T.PASSWORD	（パスワードの盗聴） 攻撃者によって、サーバ上の本TOEにログインするためのパスワードがネットワークに接続された装置をとおして盗聴され、その内容が漏洩するかもしれない。
T.UAACTION	（運用担当者からの不正な操作） 運用担当者の役割を与えられた者が、運用管理クライアントまたはTOEが提供するコマンドを使って許可されない操作を不正に行い、デプロイ、モニタリング、リカバリ及びアセスメントの各運用操作の遂行に悪影響を与えるかもしれない。
T.OPCL_UAUSER	（運用管理クライアントでの成りすまし） 攻撃者が運用管理クライアントの操作権限のある者に成りすまし、デプロイ、モニタリング及びアセスメントの情報を暴露・改ざん、または不正なリカバリ操作を行うかもしれない。
T.CMD_UAUSER	（コマンド操作における成りすまし） 攻撃者がTOEの提供するコマンドを操作できる権限のある者に成りすまし、コマンドを使ってサーバ上の本TOEや本TOEの保護資産を不正に操作するかもしれない。
T.SV_DEF_FALS	（定義情報の改ざん） 運用担当者の役割を与えられた者が、自身の役割を超えて、運用管理サーバ、部門管理サーバ、及び業務サーバ上の本TOEの定義情報を改ざんすることで、本TOEを使った運用管理が行えなくなるかもしれない。

表1-1(2)　想定する脅威(デプロイでの脅威)

識別子	脅　威
T.D_DELIVER_FAIL	（配付の異常） 通信路や配付先の業務サーバの異常により資源が配付されなかった場合に、それに気づかずに運用が継続されるかもしれない。
T.D_APPLY_FAIL	（適用の異常） 業務サーバや業務クライアントへ資源が配付されたのち、配付先の業務サーバや業務クライアントの異常により配付資源が適用されなかった場合に、それに気づかずに運用が継続されるかもしれない。

表1-1(3)　想定する脅威(モニタリング及びアセスメントでの脅威)

識別子	脅　威
T.MA_OPCL_VIOLATION	（担当範囲外への不正な監視／査定操作） 運用担当者の役割を与えられた者が、運用管理クライアントから担当範囲外の業務システム資産に対して許可されない監視／査定操作を行い、運用管理クライアントに表示された情報を不正に入手するかもしれない。

表1-1(4)　想定する脅威(リカバリでの脅威)

識別子	脅　威
T.R_OPCL_VIOLATION	（担当範囲外への不正な復旧操作） 運用担当者の役割を与えられた者が、運用管理クライアントから担当範囲外の業務システム資産に対して許可されない復旧操作を行い、該当する業務サーバやネットワーク機器に悪影響を与えるかもしれない。
T.R_OSCONS_UAACTION	（定められた範囲を超える不正なサーバ操作） サーバ操作者の役割を与えられた者が、OSコンソールから自分自身に与えられた範囲を超えて、不正に業務サーバのOSやアプリケーションの業務処理のための操作環境を操作することで、業務サーバのOSやアプリケーションに悪影響を与えるかもしれない。
T.R_OSCONS_UAUSER	（サーバ操作者に対する成りすまし） 攻撃者がサーバ操作者に成りすまし、OSコンソールから不正に業務サーバのOSやアプリケーションの業務処理のための操作環境を操作することにより、業務サーバのOSやアプリケーションに悪影響を与えるかもしれない。
T.R_RMTCL	（リモート操作における成りすまし） 攻撃者がリモート操作を行える者に成りすまし、運用管理クライアントから不正にLiveHelpクライアントをリモート操作することで、LiveHelpクライアントに悪影響を与えるかもしれない。
T.R_RMTCL_PWD	（リモート操作でのログイン・パスワードの盗聴） リモート操作の対象となるLiveHelpクライアントへログインするためのパスワードが、攻撃者によりネットワークに接続した装置をとおして盗聴され、その内容が漏洩するかもしれない。

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の各要素は、以下のOS上で動作する。

区分	動作OS	パッチ番号
CMGR/MGR CMGR/Agent(S) CMGR/Agent(J)	Red Hat Enterprise Linux AS (v.4 for Itanium)	
	Red Hat Enterprise Linux 5 (for Intel Itanium)	
CMGR/CL(M)	Windows XP Professional	SP2
CMGR/CL(U)	Windows XP Professional	SP2

SP: Service Pack

ハードウェアは、上記のOSが動作するものが必要である。以下に特記事項を示す。

- LAN機能が必須である。
- 最低一台のPentium Ⅲ、500MHz以上のCPUを搭載したPC端末が運用管理クライアントとして必要である。

以下は、本TOEの各要素の動作に必要なディスク容量（選択機能すべて選択時、管理データ量に依存する部分は除く）と、メモリ容量（監視機能のみ使用時）であり、実際の運用に必要なディスク容量とメモリ容量を見積もる際の目安である。

区分	ディスク容量	メモリ容量
CMGR/MGR	2.93GB以上	600MB以上
CMGR/Agent(S)	1.23GB以上	180MB以上
CMGR/Agent(J)	1.09GB以上	180MB以上
CMGR/CL(M)	790MB以上	80MB以上
CMGR/CL(U)	381MB以上	80MB以上

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1-2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1-2　TOE使用の前提条件

識別子	前提条件
A.ADMIN	（システム管理者、運用管理者） システム管理者、運用管理者は不正を行わない信頼できる者とする。
A.PASSWORD	（パスワードの管理） 本TOEにログインするためのパスワードについて、本人以外の者がパスワードを知ることはできないものとする。
A.NETWORK	（ネットワーク環境） 本TOEが動作するサーバ、クライアント及び本TOEが運用管理の対象とする業務システム資産は、インターネットなど信頼されない外部ネットワークから直接アクセスされないネットワーク環境で動作するものとする。
A.PLACE	（設置場所） 開発用サーバを除く本TOEが動作するサーバは、システム管理者以外の者が入退出できない、物理的に保護された場所に設置するものとする。
A.OS_ACCESS	（OSを経由したアクセス） 本TOEが運用管理で使用する資産（「1.5.5 脅威」の「運用管理で使用する資産」の項目参照）を格納したファイルや、その処理のための作業用ファイルについては、OS経由でのアクセスが行われないものとする。 補足：この前提条件は、TOEを介さないOS経由でのアクセスにより、資産及びその作業用のファイルへのアクセスが防がれることを意図している。
A.DEPLOY_ENCR	（機密性ある配付資源） 本TOEを使って配付される配付資源は、ネットワーク上で盗聴されないものとする。 補足：この前提条件は、配付経路の暗号化ではなく、配付資源自体を事前に暗号化してから配付することを意図している。
A.CLIENT	（業務クライアント及び開発用クライアントの運用） 業務クライアント及び開発用クライアントは、不正に利用されないものとする。 補足：この前提条件は、各クライアントを監視し、不正な兆候を検出できるような状況を意図している。

識別子	前提条件
A.LIVEHELP_PWD	（LiveHelp接続認証でのパスワード長） LiveHelpクライアントのリモート操作において、パスワード認証方式を利用する場合は、7文字以上のパスワードが設定されているものとする。

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。

- Systemwalker Centric Manager V13.2.0 正誤表
  (J2X1-6460-01Z0(00))
- Systemwalker Centric Manager 解説書
  (J2X1-3100-05Z2(00))
- Systemwalker Centric Manager 導入手引書
  (J2X1-3110-05Z2(00))
- Systemwalker Centric Manager ソリューションガイド セキュリティ編
  (J2X1-4600-04Z2(00))
- Systemwalker Centric Manager 使用手引書 監視機能編
  (J2X1-3120-05Z2(00))
- Systemwalker Centric Manager 使用手引書 資源配付機能編
  (J2X1-3130-05Z2(00))
- Systemwalker Centric Manager 使用手引書 ソフトウェア修正管理機能編
  (J2X1-3040-04Z2(00))
- Systemwalker Centric Manager 使用手引書 リモート操作機能編 ユーザーズガイド
  (J2X1-5690-02Z2(00))
- Systemwalker Centric Manager 使用手引書 リモート操作機能編 Client ガイド
  (J2X1-5710-02Z2(00))
- Systemwalker Centric Manager リファレンスマニュアル
  (J2X1-3000-05Z2(00))
- Systemwalker Centric Manager メッセージ説明書
  (J2X1-3080-05Z2(00))
- Systemwalker Centric Manager 全体監視適用ガイド
  (J2X1-3340-04Z2(00))
- Systemwalker Centric Manager/Systemwalker Event Agent トラブルシューティングガイド 監視機能編/ソフトウェア修正管理機能編
  (J2X1-2061-03Z2(00))
- Systemwalker Centric Manager トラブルシューティングガイド 資源配付機能編/Systemwalker Software Delivery トラブルシューティングガイド
  (J2X1-2910-03Z2(00))

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19年6月に始まり、平成20年6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19年9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

評価者の実施した評価者テストの概要を以下に示す。

2.3.1 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構成を図2-1に示す。「業務サーバと開発用サーバ」及び「業務クライアントと開発用クライアント」は兼用とされた。

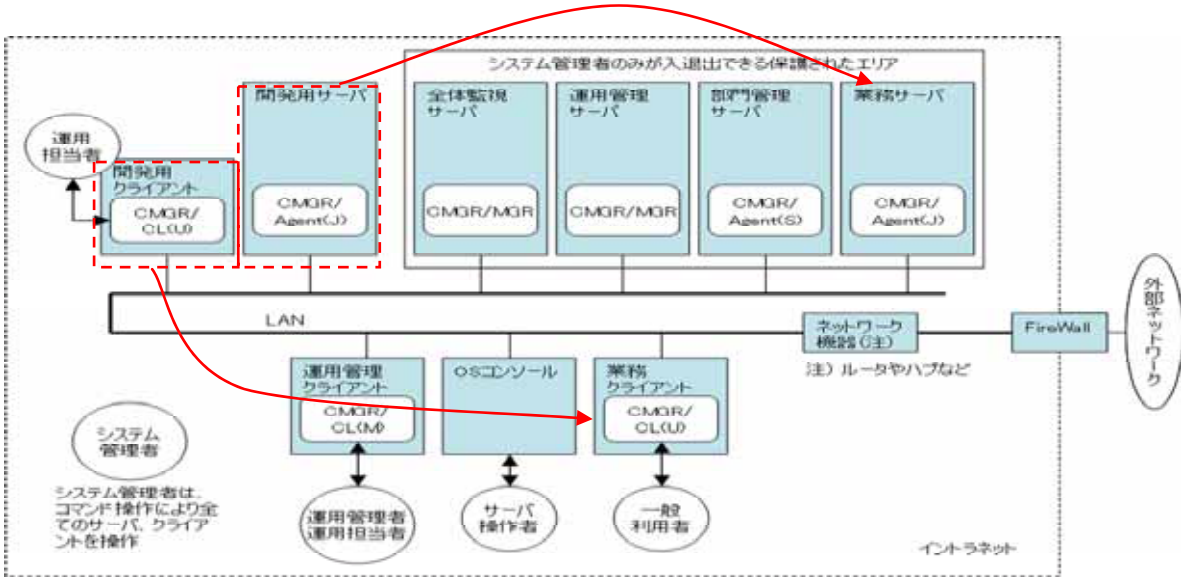


図2-1　評価者テストの構成図

評価者テストは、以下の2通りの動作環境で実施された。

- 動作環境1

サーバ/クライアント	使用OS
運用管理サーバ	Red Hat Enterprise Linux 5 (for Intel Itanium)
全体監視サーバ	Red Hat Enterprise Linux 5 (for Intel Itanium)
部門管理サーバ	Red Hat Enterprise Linux 5 (for Intel Itanium)
業務サーバ 兼 開発用サーバ	Red Hat Enterprise Linux 5 (for Intel Itanium)
運用管理クライアント	Windows® XP Professional　SP2
業務クライアント 兼 開発用クライアント	Windows® XP Professional　SP2

- 動作環境2

サーバ/クライアント	使用OS
運用管理サーバ	Red Hat Enterprise Linux AS (v.4　for Itanium)
全体監視サーバ	Red Hat Enterprise Linux AS (v.4　for Itanium)
部門管理サーバ	Red Hat Enterprise Linux AS (v.4　for Itanium)
業務サーバ 兼 開発用サーバ	Red Hat Enterprise Linux AS (v.4　for Itanium)
運用管理クライアント	Windows® XP Professional　SP2

サーバ/クライアント	使用OS
業務クライアント 兼 開発用クライアント	Windows® XP Professional　SP2

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「1) 評価者テスト環境」に示す。これらのテストにより、STにおいて識別されているTOE構成でテストを実施したとみなせることが評価者により検証されている。

b.テスト手法

テストには、以下の手法が使用された。

セキュリティ機能を刺激する方法として、

①開発証拠資料、及びガイダンス文書の記述に従い操作する。

②パケット送出ツールを使用し、不正パケットをTOEに送信する。

セキュリティ機能のふるまいを観察する方法として、

①TOEの応答を確認する。

②監査ログデータからセキュリティ機能のふるまいを確認する。

③プロトコルアナライザにより通信データを確認する。

c.実施テストの範囲

評価者が独自に考案したテストを77項目実施した。テスト項目の選択基準として、CEM ATE_IND.1-3で求められるすべての観点について検討が行われた。下記は主要な観点である。

① 各セキュリティ機能全てからテストサブセットを選定する。

② 公知の弱点を考慮する。

③ セキュリティ機能の重要性を考慮する。利用者の登録、削除やログインの機能は重要と判断され、重点的にテストが考案された。

④ セキュリティ機能の複雑性を考慮する。利用者を制限する機能は複雑と判断され、重点的にテストが考案された。

⑤ 暗黙のテストを活用する。ログイン時のパスワードの保護機能は、ログインの機能のテストの過程に含まれるよう考慮された。

⑥ 異なるインタフェースタイプを考慮する。異なるインタフェースタイプとしてCUI(コマンド)とGUIが考慮された。

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

認証機関は、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に対する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。
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。
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。
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。
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、前提条件のいずれかへ遡れ、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。
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。
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、機能強度が適切であること、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。
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。
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、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。
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が一意に識別され、その識別でラベル付け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。
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。
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。
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。
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。

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、本評価時に行われたテスト実施方法も適切と判断される。

4.2 注意事項

- サーバ上のTOEにログインするためのパスワードの保護機能について

  この機能が実装されていることは評価された。しかし、機能強度が十分であるかという観点での検証はされていない。本TOEを運用する際には、そのことを考慮した環境で運用するよう注意すべきである。

  このような注意は、この機能に限られるものではなく、Common Criteria Version 2.3のEAL1で評価された確率的または順列的セキュリティメカニズムを持つ機能全般にあてはまる可能性がある。しかし、この機能は以下の特性を持つため、特に注意事項として挙げる。

  - 消費者からは直接見えない機能である。
  - 電子政府推奨暗号リスト(平成15年2月20日 総務省、経済産業省)には含まれない、確率・順列的なメカニズムによる機能である。

- UpdateAdvisorについて

  TOEは、UpdateAdvisorと連携して、富士通株式会社のWEBサイトで提供されるソフトウェア修正情報を取得することができる。

  UpdateAdvisorは、TOEにも本評価の評価構成にも含まれていないため、UpdateAdvisorの導入の判断は消費者の責任である。

- 配付資源を保護資産として扱う範囲について

  TOEの保護資産には配付資源(サーバ資源及びクライアント資源)があるが、その範囲に関しては以下の点で注意が必要である。

  - 配付資源が開発用サーバまたは開発用クライアントに存在する時点では、保護資産としては扱われない。
  - 配付資源は、「運用管理サーバのCMGR/MGR」が受け取った時点から保護資産として扱われる。

- TOEが対抗しない脅威について

  以下の脅威に対抗するための識別・認証は、IT環境であるOSが実施する。TOEは、その結果を信頼して受け入れて動作する。

  - T.OPCL_UAUSER
  - T.CMD_UAUSER
  - T.R_OSCONS_UAUSER

  以下の脅威に対抗するためのパスワードの保護は、IT環境であるOSが実施する。

  - T.R_RMTCL_PWD

  これらの脅威に対抗するための機能は、評価範囲外であることに留意していただきたい。

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
EAL	Evaluation Assurance Level
MIB	Management Information Base
PP	Protection Profile
SNMP	Simple Network Management Protocol
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

本報告書で使用された用語を以下に示す。

アセスメント	運用管理フェーズの一つであり、業務システムを定期的に評価・分析し、必要な予防処置を策定するフェーズである。 本報告書では、「アセスメント」は運用管理フェーズの名称として用いる。
UpdateAdvisor	TOEとは別のソフトウェアであり、このソフトウェアが導入された場合、TOEは富士通株式会社のウェブサイトからソフトウェア修正情報を得ることができる。 UpdateAdvisorは富士通株式会社のウェブサイトと通信をする機能を持ち、TOEが富士通株式会社のウェブサイトからソフトウェア修正情報を得る際の仲介をする。
イベント	運用管理を行う者に通知すべき業務システムで発生した重要な事象。シスログやSNMPトラップにより通知される。

運用管理	業務システムの円滑な稼動のための管理行為（業務）であり、ソフトウェアやデータの配付と適用、稼働状況の監視、トラブルの復旧、そして運用結果の査定からなる。
OSコンソール	業務サーバのオペレータであるサーバ操作者がtelnetでサーバのOSにログインし、コマンド操作を行うためのパソコン。
開発システム	配付資源を開発するためのシステムであり、サーバ資源を開発するための開発用サーバと、クライアント資源を開発するための開発用クライアントから成る。
業務システム	業務サーバ、業務クライアント及びそれらをつなぐネットワーク機器から成る業務処理を行うシステム。
業務システム資産	業務システムを構成するサーバ、クライアント及びネットワーク機器であり、本TOEが運用管理の対象とする資産。
クライアント資源	業務クライアントに適用するための配付資源。
サーバ資源	業務サーバに適用するための配付資源。
ダウンロード	配付資源を保持する業務サーバ上の本TOEに対して、業務クライアントから資源のクライアントへの配付を要求すること。
適用	目的の業務サーバまたは業務クライアントに配付された資源を指定されたディレクトリ配下に利用可能な形で格納すること。適用を行うに際しては、配付の延長で行う形態と、別途、人が介入して行う形態の二つがある。
デプロイ	運用管理フェーズの一つであり、業務サーバや業務クライアントへのソフトウェアやデータの配備を行うフェーズである。 本報告書では、「デプロイ」は運用管理フェーズの名称として用いる。
登録	運用管理サーバへの配付資源のアップロードに先立ち、開発完了した資源を開発システム上の本TOEに配付資源の形で格納すること。
配付	運用管理サーバ上の本TOEが管理する配付資源を目的の業務サーバまたは業務クライアントに配ること。配付されたのちは、適用に備えて配付先の業務サーバまたは業務クライアントの本TOEで保持される。

配付資源	本TOEを利用して業務サーバや業務クライアントに配付されるソフトウェアやデータであり、資源の種別や宛先等の必要な情報が付加された本TOEが配付できる形式になっているもの。
モニタリング	運用管理フェーズの一つであり、業務システムの異常状態の監視を行うフェーズである。 本報告書では、「モニタリング」は運用管理フェーズの名称として用いる。
LiveHelpクライアント	リモート操作の支援を受ける側の業務クライアント及び運用管理クライアントの総称。
リカバリ	運用管理フェーズの一つであり、業務システムがトラブルに陥った場合の原因調査や復旧を行うフェーズである。 本報告書では、「リカバリ」は運用管理フェーズの名称として用いる。
リモートコマンド	運用管理クライアントから運用管理サーバ経由で監視対象の業務サーバに対して発行するコマンド。
リモート操作	運用管理クライアントからLiveHelpクライアントにアクセスして、環境設定やトラブル調査復旧を行う操作を示す。

6 参照

[1] Systemwalker Centric Manager Enterprise Edition V13.2.0 Linux版 セキュリティターゲット第1.24版（2008年3月10日）富士通株式会社

[2] ITセキュリティ評価及び認証制度の基本規程　平成19年5月　独立行政法人 情報処理推進機構　CCS-01

[3] ITセキュリティ認証申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-02

[4] ITセキュリティ評価機関承認申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-03

[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] 富士通株式会社 Systemwalker Centric Manager Enterprise Edition V13.2.0（Linux版）評価報告書 第2.1版 2008年6月19日
有限責任中間法人 ITセキュリティセンター 評価部