



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



評価対象

| | |
|-------------|---|
| 申請受付日（受付番号） | 平成19年5月28日（IT認証7152） |
| 認証番号 | C0139 |
| 認証申請者 | 富士通株式会社 |
| TOEの名称 | Systemwalker Operation Manager Enterprise Edition |
| TOEのバージョン | V13.2.0 (Windows) |
| 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 |

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12月26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。

Common Criteria for Information Technology Security Evaluation Version 2.3

Common Methodology for Information Technology Security Evaluation Version 2.3

評価結果：合格

「Systemwalker Operation Manager Enterprise Edition V13.2.0 (Windows)」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 |
| 1.1 | はじめに | 1 |
| 1.2 | 評価製品 | 1 |
| 1.2.1 | 製品名称 | 1 |
| 1.2.2 | 製品概要 | 1 |
| 1.2.3 | TOEの範囲と動作概要 | 2 |
| 1.2.4 | TOEの機能 | 4 |
| 1.3 | 評価の実施 | 5 |
| 1.4 | 評価の認証 | 5 |
| 1.5 | 報告概要 | 6 |
| 1.5.1 | PP適合 | 6 |
| 1.5.2 | EAL | 6 |
| 1.5.3 | セキュリティ機能強度 | 6 |
| 1.5.4 | セキュリティ機能 | 6 |
| 1.5.5 | 脅威 | 7 |
| 1.5.6 | 組織のセキュリティ方針 | 7 |
| 1.5.7 | 構成条件 | 7 |
| 1.5.8 | 操作環境の前提条件 | 8 |
| 1.5.9 | 製品添付ドキュメント | 9 |
| 2 | 評価機関による評価実施及び結果 | 10 |
| 2.1 | 評価方法 | 10 |
| 2.2 | 評価実施概要 | 10 |
| 2.3 | 製品テスト | 10 |
| 2.3.1 | 評価者テスト | 10 |
| 2.4 | 評価結果 | 12 |
| 3 | 認証実施 | 13 |
| 4 | 結論 | 14 |
| 4.1 | 認証結果 | 14 |
| 4.2 | 注意事項 | 17 |
| 5 | 用語 | 18 |
| 6 | 参照 | 20 |

1 全体要約

1.1 はじめに

この認証報告書は、「Systemwalker Operation Manager Enterprise Edition V13.2.0 (Windows)」(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(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 Operation Manager Enterprise Edition
バージョン： V13.2.0 (Windows)
開発者： 富士通株式会社

1.2.2 製品概要

TOEを使用することにより、利用者は内部ネットワーク上に分散する各サーバ上で利用者の業務を、日々計画されたとおりに実行させるための運用管理を行い、多様化/複雑化している業務システムの運用管理をセキュアに行うことが可能となる。

TOEは、上記の日々計画されたとおりにジョブを実行させる処理である「ジョブの計画的な実行」、及びそれに関連する資源を保護資産として扱う。

これら保護資産への不正な行為に対して、TOEは以下のセキュリティ機能を提供する。

- 利用者毎に操作できる範囲を制限する「アクセス制御機能」
- 利用者の操作を検証するための「監査ログ出力機能」
- 内部ネットワーク上に流れるパスワードを保護する「パスワード保護機能」

1.2.3 TOEの範囲と動作概要

1.2.3.1 TOEの物理範囲

TOEは、業務システムの自動運転を支援するソフトウェア製品全体であり、以下から構成される。

- Windows 版 Systemwalker Operation Manager Enterprise Edition V13.2.0 (Build-20070507) サーバ
(以降はOMGR/MGRと表記)
- Windows版 Systemwalker Operation Manager V13.2.0(Build-20070507)
クライアント
(以降はOMGR/Clientと表記)

1.2.3.2 TOEの関係者

TOEでは、以下の権限を想定する。

- システム管理者権限(コマンド)

OMGR/MGRまたはOSが提供するコマンドを使用して以下を行うことを想定する。

- OS一般ユーザの登録・削除。
- すべての範囲()で、運用管理業務を行う。
- OS一般ユーザの、担当範囲()を設定する。
- OSのアクセス権限を設定する。
- JCL/バッチファイル/実行プログラムを作成する。

- システム管理者権限(GUI)

OMGR/Clientが提供するGUIを使用して以下を行うことを想定する。

- すべての範囲()で、運用管理業務を行う。
- OS一般ユーザの担当範囲()を設定する。

- OS一般ユーザ権限(コマンド)

OMGR/MGRまたはOSが提供するコマンドを使用して以下を行うことを想定する。

- 担当範囲()で、運用管理業務を行う。ただし、自らの所有する範囲の自動運転用定義情報に対してはすべての運用管理業務を行う。
- JCL/バッチファイル/実行プログラムを作成する。

- OS一般ユーザ権限(GUI)

OMGR/Clientから以下を行うことを想定する。

- 担当範囲()で、運用管理業務を行う。ただし、自らの所有する範囲の自動運転用定義情報に対してはすべての運用管理業務を行う。

「すべての範囲」とは、すべての自動運転用定義情報が対象範囲である、ということの意味する。

「担当範囲」とは、指定された自動運転用定義情報が対象範囲である、ということの意味する。

TOEでは、以下の役割を想定する。以下の説明の中の[使用環境の権限]とは、TOEの使用環境における、物理的、人的、接続的な側面での権限である。(非ITの権限)
[TOEにおける権限]とは、TOEの利用上の権限である。(ITの権限)

- 組織の責任者

組織の長。

[使用環境の権限] 組織の責任者権限

[TOEにおける権限] なし

- システム管理者

サーバのOSにおいて、Administratorアカウントを有する人物。

[使用環境の権限] 機器管理権限

[TOEにおける権限] システム管理者権限(コマンド)、システム管理者権限(GUI)

- OS一般ユーザ

サーバのOSのAdministrator以外のアカウントを有する人物。

[使用環境の権限] なし

[TOEにおける権限] OS一般ユーザ権限(コマンド)、OS一般ユーザ権限(GUI)

- 一般利用者

業務クライアントを利用して業務を行う人物。

[使用環境の権限] なし

[TOEにおける権限] なし

1.2.3.3 TOEの動作概要

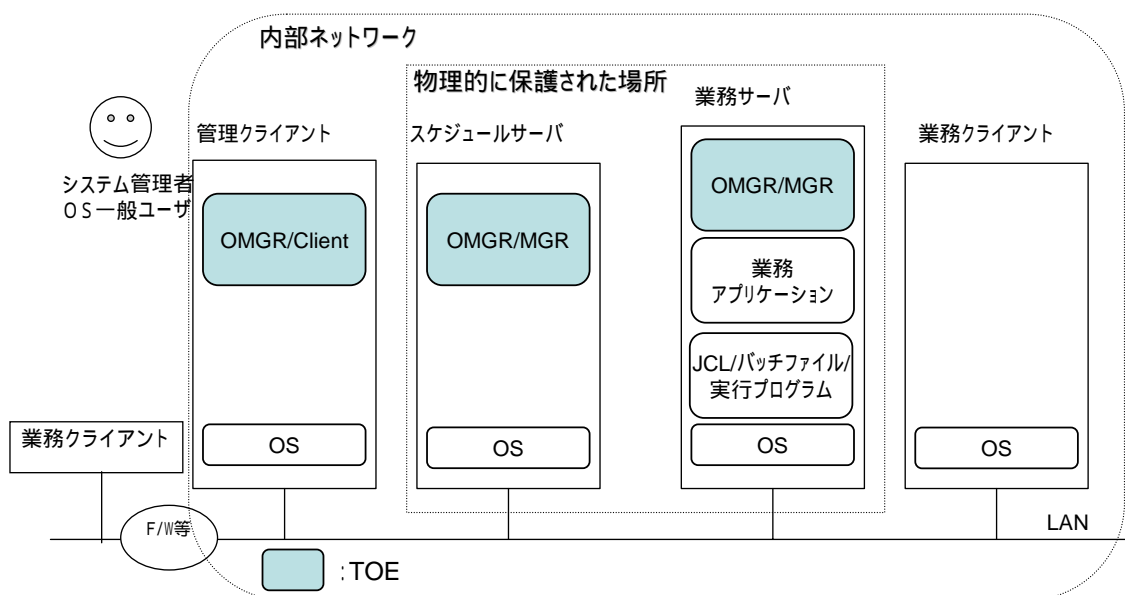


図1-1 TOEの基本的な動作環境

TOEは、図1-1の環境で動作する。TOEは、各役割の利用者により定義された自動運転定義情報に従い、業務サーバ上のジョブ(JCL/バッチファイル/実行プログラム)を実行させる。

1.2.4 TOEの機能

TOEは以下の機能を持つ。

- 自動運転定義情報の定義

TOEは、OS一般ユーザに対して、自動運転定義情報を定義する機能(つまり、ジョブ実行のスケジュールを登録・参照・編集する機能)を提供する。

この機能は、TOEの以下の部分から使用できる。

- OS一般ユーザは、スケジュールサーバ上のOMGR/MGRが提供するコマンドを操作することで使用できる。(OS一般ユーザは管理クライアントからこの操作を行う。管理クライアントからスケジュールサーバ上のOMGR/MGRを操作するための機能はOSが提供することを想定する。)

管理クライアント上のOMGR/Clientを操作することも可能である。

- 自動運転定義情報に従ったジョブの実行

TOEは、定義された自動運転定義情報に従い、ジョブを実行する。

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 Operation Manager Enterprise Edition V13.2.0 Windows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 Operation Manager Enterprise Edition V13.2.0 (Windows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19年12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。

- アクセス制御機能
 - OS一般ユーザに対するアクセス制御
OS一般ユーザの自動運転用定義情報に対する操作を、許可された範囲に制限する機能。
許可する範囲は、システム管理者だけが設定できる。
- パスワード保護機能
内部ネットワークを流れる、OSによる識別認証で使用されるパスワードを、暴露から保護する。
暴露からの保護には、元のデータを容易には復元できないような変換が使用される。
- 監査ログ出力機能
アクセス制御機能に関する記録を監査ログとして採取し、監査ログファイルに出力する機能。

1.5.5 脅威

本TOEは、表1-1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 想定する脅威

| 識別子 | 脅威 |
|----------------------|--|
| T.PASSWORD_TAP | (パスワードの盗聴) 悪意のある者は、内部ネットワーク上に流れるパスワードを盗聴し、内容を暴露するかもしれない。 |
| T.UAUSER_CLIENT | (クライアント機能を使用時のなりすまし) 悪意のある者は、クライアント機能を使用して、システム管理者、及びOS一般ユーザになりすまし、自動運転用定義情報の改ざんを行い、ジョブの計画的な実行を阻害するかもしれない。 |
| T.UAUSER_COMMA ND | (コマンドを使用時のなりすまし) 悪意のあるものは、コマンドを使用して、システム管理者、OS一般ユーザになりすまし、自動運転用定義情報の改ざんを行い、ジョブの計画的な実行を阻害するかもしれない。 |
| T.UAACTION | (許可されない操作) OS一般ユーザとして識別認証されたものは、クライアント機能またはコマンドを使用してシステム管理者が許可した担当範囲を超えて操作を行い、自動運転用定義情報の改ざんを行い、ジョブの計画的な実行を阻害するかもしれない。 |

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

TOEは図1-1及び図1-2に示す環境で動作する。TOEの動作に必要なソフトウェアは以下のとおりである。TOEの動作に必要なハードウェアは、TOEの動作に必要なソフトウェアが動作するものである。

- OMGR/MGRをインストールするマシンには以下が必要
 - Windows Server 2003 Enterprise Edition SP2
- OMGR/Clientをインストールするマシンには以下が必要
 - Windows XP Professional SP2

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 | (システム管理者及び運用管理者の信頼性) システム管理者は、不正な操作を行わない信頼できる人物であることを想定する。 |
| A.PASSWORD | (パスワードの管理) パスワードの管理について、以下を想定する。 ● TOEを利用するOS一般ユーザのパスワードは、システム管理者及び本人以外に知られないように管理される。 |
| A.PLACE | (設置場所) 本TOEが動作するサーバは、システム管理者以外が入退出できない、事務フロアやサーバールーム等に設置されることを想定する。 |
| A.NETWORK | (ネットワーク環境) 本TOEは、外部ネットワークから直接アクセスされないイントラネット環境にて動作されることを想定する。 |
| A.OS_ACCESS | (OSを経由したアクセス) 悪意のある者により、本TOEを介さず、直接サーバ上のOSからTOEで扱う資源にアクセスできないよう、OSのアクセス権設定されることを想定する。 |

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。

- Systemwalker Operation Managerセキュリティガイド (注1)
J2X1-6680-01Z0(00)
- Systemwalker Operation Manager解説書 - UNIX/Windows(R)共通 -
J2X1-3180-03Z2(00)
- Systemwalker Operation Manager導入手引書 - UNIX/Windows(R)共通 -
J2X1-3190-03Z2(00)
- Systemwalker Operation Manager使用手引書 - UNIX/Windows(R)共通 -
J2X1-3200-03Z2(00)
- Systemwalker Operation Managerリファレンスマニュアル -
UNIX/Windows(R)共通 -
J2X1-3160-03Z2(00)
- Systemwalker Operation Managerメッセージ説明書 - UNIX/Windows(R)
共通 -
J2X1-3140-03Z2(00)
- Systemwalker Operation Managerトラブルシューティングガイド説明書 -
UNIX/Windows(R)共通 -
J2X1-2120-05Z2(00)
- Systemwalker Operation Managerスケジュール分散機能説明書 -
UNIX/Windows(R)共通 -
J2X1-3170-03Z2(00)

(注1) 「Systemwalker Operation Managerセキュリティガイド」は、製品に同梱される形態ではなく、Webにて配付される。

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5月に始まり、平成19年12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6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。

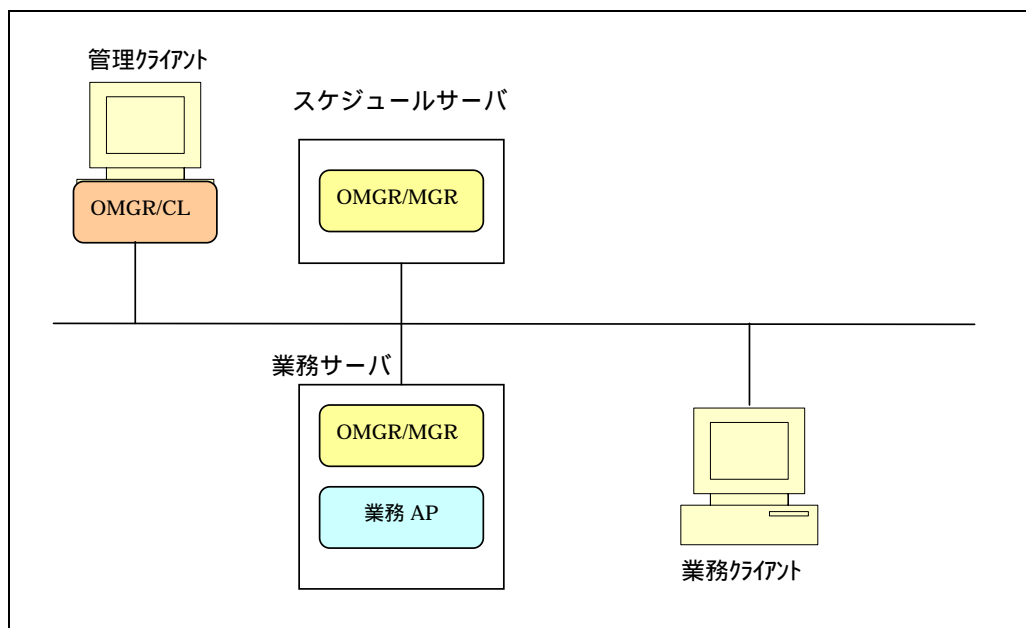


図2-1 評価者テストの構成図

この構成における動作環境は以下のとおりである。

| | |
|--------------|---|
| スケジュールサーバのOS | Windows Server 2003 Enterprise Edition SP2 |
| 業務サーバのOS | Windows 2000 Server SP4 |
| 管理クライアントのOS | Windows XP Professional SP2 |

3) 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(1)」に示す。

このテスト構成はSTにおいて識別されている動作環境とは一部異なるが、STにおいて識別されている動作環境におけるセキュリティ機能の動作については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。

(「4.2 注意事項」参照)

b. テスト手法

テストには、以下の手法が使用された。

開発証拠資料及びガイダンス文書から想定できる方法で外部インターフェースを使用する。結果観察には、以下の手段を使用する。

- 外部インターフェースへの出力または監査ログの内容を確認する。
- Wireshark(TCP/IPダンプツール)を使用し、内部ネットワーク上の通信を解析して確認する。

netcat(指定したTCP/UDPのポートに任意のデータを送信するツール)を使用し、外部インタフェースへの出力または監査ログの内容を確認する。

c.実施テストの範囲

評価者が独自に考案したテストを9項目実施した。テスト項目の選択基準として、CEM 1: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。

すべてのセキュリティ機能が特定されたとおりにふるまうことの確信が得られるようにテストを考案する。どの程度のテストを考案するかは、セキュリティ機能の重要性、複雑性、インタフェースのタイプを特に考慮する。

TOEの種別に一般的に関係する知られている公知の弱点について確認するためのテストを考案する。

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

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。

当該所見報告書でなされた指摘内容が妥当であること。

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。

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。

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。

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。 |
| 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ータ、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おり、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い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、開発者テスト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、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

本評価において、評価者テストはSTにおいて識別されている動作環境とは一部が異なる動作環境で実施された。（「2.3.1 評価者テスト」参照）

「本評価により正しく動作することが保証される機能」は、「1.5.4 セキュリティ機能」で示したTOEのセキュリティ機能であり、少なくともこれらの機能はSTと一貫する動作環境の部分でテストされた。

それ以外の機能の中には、STとは異なる動作環境の部分でテストされた機能も存在するが、これらの機能は保証の対象ではない。例えば、自動運転用定義情報の通りに業務サーバ上でジョブを動作させる機能が該当する。

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 |
| PP | Protection Profile |
| 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。

| | |
|---------|---|
| 業務システム | 本TOEを導入し、運用管理を行う対象のシステムを示す。 業務システムは、スケジュールの管理を行うスケジュールサーバ(階層構造となる場合は、スケジュール管理サーバ)、実際に利用者のプログラムが動作する業務サーバ、業務の運用管理を行う運用管理クライアント及びそれらを相互接続するネットワークからなる。 |
| 自動運転 | TOEを導入するシステムで動作する利用者のプログラム(以降、業務と記載)を自動実行する事を示す。 |
| ジョブ | 業務の自動実行を行う際の処理単位であり、特に、本ST内ではスケジュールされたジョブを指す。 |
| JCL | ジョブの実行制御を行う際に利用する言語。本言語により、複雑な業務の手順を容易に記述できる。OSユーザにより作成される。ジョブを起動、終了する際に利用される。 |
| バッチファイル | 複数の処理をまとめて行なう際に使われるファイル |
| 実行プログラム | ジョブを実行するプログラム。このプログラムにはコマンドが含まれる。 |

| | |
|---------------|---|
| 自動運転用定義 情報 | ジョブの計画的な実行を行う際に利用する定義情報である。 自動運転を行うための定義情報には、ジョブ及びリカバリジョブ が登録される。 |
| OSユーザ | コマンドを使用したシステム管理者、及びOS一般ユーザを指す。 |
| 内部ネットワー ク | TOEが動作する各サーバをLAN (IEEE802.3インタフェース) 接続し、構築したネットワークセグメントである。 後述する外部ネットワークと異なり、企業内で構築されるイント ラネットとして運用されるネットワークを示す。 |
| 外部ネットワー ク | インターネットへの接続または、他企業と取引のため、相互接続 を行っているネットワークセグメントである。 |
| 運用管理 | ジョブの開始や終了といった運用に関わる行為 |
| サーバ | 本STにおいてサーバと示した場合、業務サーバ、スケジュール サーバ、スケジュール管理サーバを指す。 |
| 運用管理業務 | 本STにおいて、運用管理業務と記載した場合、以下の行為を指す。 <ul style="list-style-type: none"> ● 自動運転用定義情報に対して、業務を行うためのジョブをスケ ジューリングする ● 必要に応じて、ジョブスケジューラを使用して、ジョブ操作 を行う ● リカバリジョブを投入する ● ジョブの状態を確認する |

6 参照

- [1] Systemwalker Operation Manager Enterprise Edition V13.2.0 Windows版 セキュリティターゲット Version 1.11 (2007年12月18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 Operation Manager Enterprise Edition V13.2.0 (Windows版) 評価報告書 第1.2版 2007年12月18日
有限責任中間法人 ITセキュリティセンター