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10月10日（IT認証6104）**
認証番号	C0092
認証申請者	**富士通株式会社**
TOEの名称	OS**Ⅳ**/MSP **セキュア**AF2
TOEのバージョン	V10L10 C06121
PP適合	**なし**
適合する保証要件	EAL1
TOE開発者	**富士通株式会社**
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4月27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

「OSⅣ/MSP セキュアAF2 V10L10 C06121」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、「OSⅣ/MSP セキュアAF2 V10L10 C06121」（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:	OSⅣ/MSP セキュアAF2
バージョン:	V10L10 C06121
開発者:	富士通株式会社

1.2.2 製品概要

本TOEは、利用者のアクセス制御、識別認証等のセキュリティ面での強化を行ったエンタープライズ・コンピューティング向けのOSである。本TOEにより、利用者が使用するTOE上のアプリケーションは、マルチユーザかつマルチタスクに動作することができる。

また、本TOEにより、利用者と資源間のアクセス関係を詳細に定義することができ、定義に従ったアクセス制御が行われることで、利用者は情報センタ内で許可された権限の範囲内で資源を利用した作業をセキュアに行うことができる。

1.2.3 TOEの範囲と動作概要

(1) TOE動作環境

TOEの動作環境を図1-1に示す。TOEは、図に示す情報センタにおいて、「TOE」と示した機器（GS/PRIMEFORCEシリーズサーバ）に導入されて動作する。また、図1-1において破線は、物理的な保護環境が必要であることを示している。

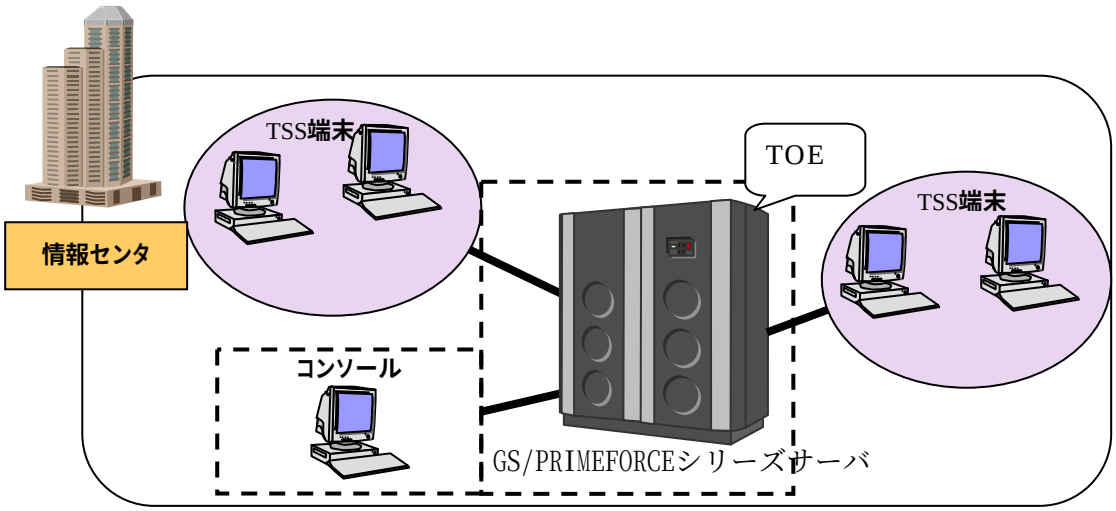

図1-1　TOE動作環境

以下に図1-1の各機器について説明する。

【GS/PRIMEFORCEシリーズサーバ】
TOEが搭載されて動作する、富士通製のメインフレームサーバ。本サーバに、資源を格納するDASDボリュームや磁気テープボリュームが設置される。なお、GS/PRIMEFORCEシリーズサーバは、TOEにおいて特権を有するユーザである、RACFセンタ要員以外、入退室できないような物理的に保護された場所に設置される必要がある。

【TSS端末】
TOEを利用する際に使用する端末である。

【コンソール】
RACFセンタ要員が、TOEの保守、運用を行う際に使用する端末である。但し、コンソールは、RACFセンタ要員以外、入退室できないような物理的に保護された場所に設置される必要がある。

また本製品は、オプション製品を追加導入することでインターネットに接続することが可能となるが、本TOEではインターネットには接続しないTOE単体での運用を想定している。

(2) TOE構成

TOEのソフトウェア構成要素及び提供機能を表 1-1に示す。

表 1-1　TOE構成要素

構成プログラム	バージョン	提供機能
AF2	V10L10 C06121.PTF	・監査機能 ・TOE管理機能 ・資源利用機能 ・OS基本機能 ・各種ユーティリティ ・自動運転機能 ・システム監視 ・トラブルシューティング用ツール ・システム編集/ソフトウェア修正適用ツール
RACF	V12L10 C05091.PTF	・識別認証機能 ・アクセス制御機能 ・TOE管理機能 ・監査機能
TSS/E	V11L20 C06061.PTF	・端末接続機能
VTAM-G	V30L20 C06121.PTF	・端末接続機能

1.2.4　TOEの機能

TOEが提供する機能を以下に示す。

(1)セキュリティ機能

【OS基本機能】

本機能は、OSとしての基本機能として、複数の利用者が複数のアプリケーションを実行するマルチユーザ、かつマルチタスク環境を提供するものである。また本環境を実現するため以下に示す機能を提供する。

・ハードウェアとの連携
・仮想空間管理
・複数利用者の管理
・TOE及びアプリケーション実行環境の提供
・外部記憶装置（DASDボリューム、磁気テープボリューム）に対するインタフェースの提供と管理

【識別認証機能】

本機能により、TOEの関係者は利用者識別名（グループに所属している場合、グルー

プ識別名も併せて）及びパスワードを入力し、情報センタの資源を使用しても良い、正当な人物であるかを識別認証される。

本機能の管理（例えば、パスワード自体やパスワード有効期限の変更、「識別認証機能の動作形式」）は、「TOE管理機能」にて行われる。

【アクセス制御機能】

本機能は、TOEの関係者・グループ・アプリケーションに対して、定められた設定に従って、情報センタ内の資源へのアクセスを制御する機能である。資源へのアクセスが許可された場合、許可されたアクセス権レベル（書込み、読込み、実行）で資源への操作が可能となる。資源へのアクセスが拒否された場合、アクセス禁止となる。

【監査機能】

本機能により、情報センタの利用状態や資源へのアクセスに対する監査ログが採取される。監査ログを監査することにより、不正な利用者が情報センタ及び資産を使用していないかを確認できる。

【TOE管理機能】

本機能は、RACF センタ要員、管理者が管理行為を行う際に利用する機能である。また、本機能は、一般利用者が、自身のTOEにおける設定を、限られた範囲で行う際に利用する機能である。

(2)非セキュリティ機能

【資源利用機能】

本機能はTOEにおいて資源（データセット類、一般資源類）を利用（データ書き込み、データ読み出し、アプリケーション実行）するためのサービスを提供する。

【各種ユーティリティ機能】

本機能は、システムの管理及び保守を行うための各種ユーティリティを提供する。

【自動運転機能】

本機能は、利用者のオペレーションを自動化し、システムの効率的運用とオペレーションの省力化を実現する。

【システム監視機能】

本機能は、TOEを含む情報センタ全体を安全に運用するため、ハードウェアの利用状態、CPU故障及びプログラムの性能異常による障害の発生を検知する。

【トラブルシューティング用ツール】

本機能は、情報センタで発生した事象の調査／解析を行うためにトラブルシューティング用ツールを提供する。

【システム編集・ソフトウェア修正適用ツール】

本機能は、TOE動作プログラムの修正を行うためのシステム編集・ソフトウェア修

正適用ツールを提供する。

【端末接続機能】
本機能は、TSS端末を接続するための環境を提供する。

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「OSⅣ/MSP セキュアAF2　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及び本TOEの開発・製造・出荷の現場を調査し、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・製造・出荷環境が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、「OSⅣ/MSP セキュア AF2 V10L10 C06121 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、以下のとおりである。

(1)識別認証機能

本機能により、他のセキュリティ機能を利用する前に、TOEにアクセスする人物に対し、利用者識別（グループ）名及びパスワードを利用した識別認証が行われる。

本機能に使用するパスワードは、以下の規則に従う。

・フィードバックは行わない（非表示）
・利用者パスワードの有効期間 ： 取り得る値の範囲は、1～999（日）
パスワードの有効期間が切れた場合、パスワード変更の要求を行う
・利用者パスワードの構文規約チェック ：8文字以内の各国記号（¥,#,@）を含む英数字
・利用者パスワードの変更禁止期間 ：取り得る値の範囲は、1～999（日）
・新しい利用者パスワードの入力確認：選択
・利用者パスワードの入力違反許容回数：取り得る値の範囲は、1～999
・利用者パスワード入力違反による自動失権後の自動復権 ：
値の取り得る範囲は1～999（日）
・日付指定の自動失権と自動復権 ：
- 絶対日数を指定するときの値の取り得る範囲は1～999（日）
- 相対日数はYYMMDD形式で指定するため、値の取り得る範囲は
800101(1980年1月1日)～791231(2079年12月31日)
・システム未利用者の自動失権：値の取り得る範囲は1～999（日）

(2)アクセス制御機能

本機能は、TOEの関係者・グループ・アプリケーション（以降エンティティ）に対して、RACF管理簿に登録された設定(資源の所有者が許可するアクセスの設定)に従って、資源へのアクセスを制御する。RACF管理簿内に該当するエンティティと資源との規則が記載されている場合、許可されたアクセス権限での資源への操作を許

可する。資源アクセスを不許可と判断した場合、アクセス禁止となる。

アクセス制御は、以下の4機能からなり、各機能は予め決められた順序で適用される。

グローバルチェック機能：

特定の資源に対する全ての利用者のアクセスを明示的に許可する。

構造化グループ機能：

グループの階層構造を利用して、グループが所有する資源に対する、当該グループ以外の資源アクセスを制御する。

資源アクセス制御機能：

資源と利用者との関係をRACF管理簿に登録し、その規則に従ってアクセスの制御を行う。

JESCIアクセス権確認機能：

JCL投入段階で、JCLの要求が許可された範囲内であるかを判断する。

(3)監査機能

本機能は、情報センタの利用状態や資源へのアクセスに対する監査ログを採取するものであり、以下の機能により構成される。

監査ログの収集：

監査ログへの採取事象に関する設定に従い、監査ログを収集する。採取事象の設定内容としては、「すべてのアクセスログを収集する」、「正当なアクセスログを収集する」、「不当なアクセスログを収集する」、「アクセスの記録を収集しない」の4種類が存在し、デフォルトは「不当なアクセスログを収集する」に設定される。また、本設定はセキュリティ管理機能にて提供される。

監査レポートの出力：

採取した監査ログを、監査レポートとして監査する人物が可読な形式で出力する。なお、監査ログから監査レポートを出力する際には、監査データセットというデータセットを作成し、この監査データセットから監査レポートの出力を行う

監査データセットから、監査レポートを出力する能力は、RACFセンタ要員、管理者、一般利用者（資源の所有者）のみに制限している。

監査レポートの出力範囲制御：

監査レポートの出力範囲を、役割毎に規定された以下の範囲に限定する。

・RACFセンタ要員は、すべての利用者に対する監査レポートを出力可能とする
・管理者は自身の管理下にあるグループが所有する資源に関する監査レポートを出力可能とする
・一般利用者は自身が所有する資源に関する監査レポートを出力可能とする

監査ログの保全：

監査ログが監査イベントで一杯になった場合、格納場所を交代用データセットに自動的に切り替え、かつ、監査ログが一杯になったことをRACFセンタ要員に通知する。

(4)セキュリティ管理機能

本機能は、RACFセンタ要員、管理者、一般利用者に対してセキュリティ機能の管理行為を行う能力を提供する。以下に役割毎の管理対象機能を示す。

RACFセンタ要員向け管理機能：

・RACF管理簿の問い合わせ、改変
・資源に関する属性のデフォルト値変更
・RACF管理簿のバックアップ、稼動・非稼動制御、監査ログの保全
・セキュリティ機能の起動、停止、ふるまいの決定、改変
・利用者属性の問い合わせ・改変・削除
・アプリケーション名の問い合わせ・登録・改変・削除
・資源に関する属性の問い合わせ・改変・削除
・グループに関する属性の問い合わせ・改変・削除
・JCL属性の改変

管理者向け管理機能：

・利用者属性の問い合わせ・改変・削除
・アプリケーション名の問い合わせ・登録・改変・削除
・資源に関する設定機能
・グループに関する設定機能
・JCL属性の改変

一般利用者向け管理機能：

・自身の利用者に関する属性の問い合わせ・改変・削除
・アプリケーション名の問い合わせ・登録・改変・削除
・自身が所有する資源に関する属性の設定機能
・自身が所属するグループに関する属性の設定機能
・JCL属性の改変

(5)TOE保護機能

本機能は、TOEの起動時に、メモリが正常に動作するか検証を行う。

TOEは、ジョブがアプリケーションを起動すると、仮想記憶（アプリケーションの実行環境）にOSに対する制御データが付与されたアプリケーションをローディングし実行する。本機能では、仮想記憶として、アプリケーションごとに独立した空間を作成する。この独立した仮想空間にアプリケーションが存在するため、アプリケーション間の干渉発生を防止するセキュリティドメインを構築する。それにより、不正な利用者が自身の起動したアプリケーションの仮想空間を越え他のアプリケーションの制御データを改変することによってTOEを改変したり損害を与えたりすることや、他の利用者が仮想空間上にロードした保護資産を改変したり覗き見たりすることが防がれている。

1.5.5 脅威

本TOEは、表1-2に示す脅威を想定し、これに対抗する機能を備える。

表1-2 想定する脅威

識別子	脅 威
T.ILLIGAL_ACCESS （不正アクセス）	悪意のある人物は、コマンド／アプリケーションを利用して、資源に対し不正なアクセスを行う ※不正なアクセスとは、資源の所有者が許可しないアクセスを指す
T.PROGRAM （不正なジョブの干渉）	不正なジョブがTOEの領域にアクセスし、他のジョブの実行処理に干渉することによって、資源に対し不正なアクセスを行う

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、図1-1に示すように物理的に保護された場所に設置された、富士通製の下記メインフレームサーバ上で動作する。

・GS/PRIMEFORCEシリーズサーバ

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1-3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1-3 TOE使用の前提条件

識別子	前提条件
A.ADMIN (信頼できるRACFセンタ要員、管理者)	RACFセンタ要員及び管理者は、不正を行わない、信頼できる人物であること
A.PASSWORD (パスワードの管理)	RACFセンタ要員、管理者、及び一般利用者が使用するパスワードは、本人以外に知られないこと
A.PHY_PROTECT (物理的な保護)	コンソール及びTOEが動作するサーバには、RACFセンタ要員以外が物理的にアクセスできないこと

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。

(1) 管理者ガイダンス

・OSⅣ/MSP RACF 運用手引書V12L10 用
・OSⅣ/MSP RACF 使用手引書管理者編V12L10 用
・OSⅣ/MSP RACF コマンド文法書V12L10 用
・OSⅣ/MSP RACF システムプログラマの手引V12L10 用
・OSⅣ/MSP RACF ユーティリティ使用手引書V12L10 用
・OSⅣ/MSP RACF メッセージ説明書V12L10 用
・OSⅣ/MSP RACF 導入手引書V12L10 用
・OSⅣ/MSP AMS コマンド文法書AFⅡ V10 用
・OSⅣ/MSP IORGP 使用手引書AFⅡ V10 用
・OSⅣ PLOP/X 使用手引書
・OSⅣ/MSP SMF 説明書AFⅡ V10 用
・OSⅣ/MSP SMP 使用手引書AFⅡ V10 用
・OSⅣ/MSP コンソールコマンド文法書AFII V10 用
・OSⅣ/MSP システムパラメタ文法書AFⅡ V10 用
・OSⅣ/MSP システムプログラミング手引書タスク管理編AFⅡ V10 用
・OSⅣ/MSP システムユーティリティ使用手引書AFⅡ V10 用
・OSⅣ/MSP ジョブ制御言語文法書AFⅡ V10 用
・OSⅣ/MSP タスク管理マクロ命令文法書AFⅡ V10 用
・OSⅣ/MSP タスク管理解説書AFⅡ V10 用
・OSⅣ/MSP メッセージ説明書AFⅡ V10 用
・OSⅣ/MSP 運用手引書JES 編AFII V10 用
・OSⅣ/MSP 操作手引書AFII V10 用
・OSⅣ/MSP TSS/E コマンド文法書V11L20 用
・OSⅣ VTAM-G 導入手引書V30 用
・FACOM M シリーズハードウェア機能説明書I(命令編)
・FACOM M シリーズハードウェア機能説明書Ⅱ(機能編)
・ソフトウェア説明書OSIV/MSP セキュアAF2 V10
・ソフトウェア説明書OSIV/MSP RACF V12

(2) 利用者ガイダンス

・OSⅣ/MSP RACF コマンド文法書V12L10 用
・OSⅣ/MSP RACF メッセージ説明書V12L10 用
・OSⅣ/MSP RACF ユーティリティ使用手引書V12L10 用
・OSⅣ/MSP RACF 使用手引書利用者編V12L10 用
・OSⅣ/MSP ARCS 使用手引書AFⅡ V10 用
・OSⅣ/MSP GDS 使用手引書AFⅡ V10 用
・OSⅣ/MSP IORGP 使用手引書AFⅡ V10 用
・OSⅣ/MSP PIC 使用手引書AFⅡ V10 用
・OSⅣ PLOP/X 使用手引書
・OSⅣ/MSP VSAM マクロ命令文法書AFⅡ V10 用
・OSⅣ/MSP アセンブラ使用手引書AFⅡ V10 用
・OSⅣ/MSP サービスエイド使用手引書AFⅡ V10 用
・OSⅣ/MSP システムプログラミング手引書データ管理編AFⅡ V10 用
・OSⅣ/MSP システムユーティリティ使用手引書AFⅡ V10 用
・OSⅣ/MSP ジョブ制御言語文法書AFⅡ V10 用
・OSⅣ/MSP タスク管理マクロ命令文法書AFⅡ V10 用
・OSⅣ/MSP タスク管理解説書AFⅡ V10 用
・OSⅣ/MSP データセットユーティリティ使用手引書AFⅡV10 用
・OSⅣ/MSP データ管理マクロ命令文法書AFⅡ V10 用
・OSⅣ データ変換ユーティリティ説明書V10 用
・OSⅣ/MSP メッセージ説明書AFⅡ V10 用
・OSⅣ/MSP リンケージエディタ/ローダ使用手引書AFⅡ V10 用
・OSⅣ/MSP TSS/E コマンド開発手引書V11L20 用
・OSⅣ/MSP TSS/E コマンド文法書V11L20 用
・OSⅣ/MSP TSS/E メッセージ説明書V11L20 用
・OSⅣ/MSP TSS/E 運用手引書V11L20 用

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10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構成を図 2-1に示す。

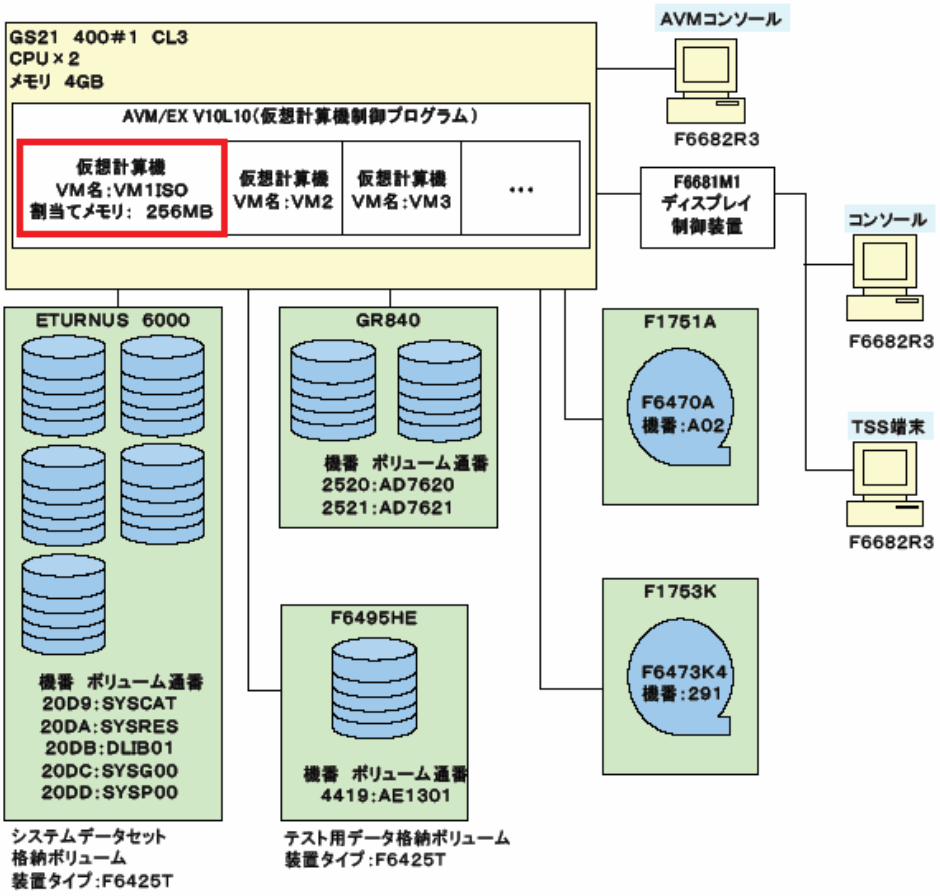

図 2-1 評価者テスト構成

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は図 2-1に示すとおりであり、メインフレームサーバ、コンソール、TSS端末、記憶装置から構成されたテスト環境を使用していることから、評価者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。以下は、テスト構成がSTにおいて識別される接続構成とは一致しない部分について、同等であるとみなせる理由である。

図 2-1に示したテスト環境ではメインフレームサーバ上で、ハードウェアリソースを論理的に分割し、最大14台の仮想マシン環境を提供するための制御プログラムであるAVM/EX V10L10を使用し、そこで提供される1台の仮想マシンを使用してTOEのセットアップ、各端末の接続を行っている。この制御プログラムはSTの運用環境では識別されていないが、TOEに対して実計算機上で直接実行するのと同等なハードウェア仮想環境を提供するものである事と、実運用環境において、本制御プログラムを使用した仮想マシン環境上での運用も想定されることから、本テスト環境はSTで識別されるTOE構成環境と同等であるとみな

すことができる。

b.テスト手法

テストには、以下の手法が使用された。

①テスト項目毎にコンソール、TSS端末上でコマンド入力、もしくは事前に作成したジョブを実行する

②各ディスプレイ上に表示されるメッセージ､及び実行結果が格納されたデータセットを参照し、テスト結果について確認する

c.実施テストの範囲

評価者が独自に考案した計208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網羅することと、以下の観点を考慮している。

①アクセス制御機能以外のセキュリティ機能については、全てのTSFIに関する動作確認を行う

②アクセス制御機能に関しては、提供される4種類の制御方法について、全ての適用パターンを網羅する

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

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識別、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。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。
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。
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。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。
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。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。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。
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、そのリファレンスにより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。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、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。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
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。

DASD	Direct Access Storage Deviceの略称 アドレスを直接指定することにより、書き込み、読み込みが可能となる記憶装置
GS/PRIMEFORCEシリーズ	富士通が提供するメインフレーム 参考URL：http://globalserver.fujitsu.com/jp/
JCL	Job Control Language： TOEを利用する際に使用する言語
RACF	Resource Access Control Facilityの略
RACF管理簿	TOEの動作や、利用者・グループの権限等が記載される、TOEの設定に関わるデータ
資源	情報センタ内で扱う資源のこと 資源には、以下が含まれる ・データセット - DASDデータセット - 磁気テープデータセット ・一般資源

- DASDボリューム
- 磁気テープボリューム

情報センタ	TOEを利用して構築された組織
データセット	DASDボリューム、及び磁気テープボリューム内に存在するデータ群。DASDボリューム内に存在するデータセットを、DASDデータセットと呼ぶ。また、磁気テープボリューム内に存在するデータセットを、磁気テープデータセットと呼ぶなお、データセットには、アプリケーションも含まれる
プログラム	本書においては、アプリケーションと同義
ボリューム	記憶装置の単位 ボリュームには、DASDボリューム、磁気テープボリュームがある

6 参照

[1] OSⅣ/MSP セキュアAF2 セキュリティターゲット バージョン 1.14 （2007年2月15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] OSIV/MSP セキュアAF2 V10L10 C06121 評価報告書 第1.5版 2007年3月27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