認　証　報　告　書

評価対象

申請受付年月日(受付番号)	平成14年 10月 29日（IT認証2004）
認証申請者	富士通株式会社
TOEの名称	SymfoWARE Server Enterprise Extended Edition 4.0
ＰＰ適合	なし
適合する保証要件	EAL4
TOE開発者	富士通株式会社　ソフトウェア事業本部 ミドルウェアプラットフォーム事業部　第二開発部
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15年10月27 日

独立行政法人製品評価技術基盤機構
適合性評価センター管理課情報セキュリティ室
技術管理者　田渕　治樹

評価基準等：「ITセキュリティ評価機関に対する要求事項」で定める下記の規格に基づいて評価された。

① ISO/IEC 15408:1999 Information technology — Security techniques — Evaluation criteria for IT security.
② JIS X 5070(2000) セキュリティ技術 — 情報技術セキュリティの評価基準。
③ Common Criteria for Information Technology Security Evaluation.
④ JIS TR X 0049(2001) 情報技術セキュリティ評価のための共通方法

⑤ Common Methodology for Information Technology Security Evaluation
⑥ 認証機関が公開する③および⑤の翻訳文書
⑦ CCIMB Interpretations-0210
⑧ 補足-0210

評価結果：合格

SymfoWARE Server Enterprise Extended Edition 4.0は、独立行政法人製品評価技術基盤機構が定めるIT製品等のセキュリティ認証業務実施規程に従い、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、「SymfoWARE Server Enterprise Extended Edition 4.0」（以下「本TOE」という。）について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「SymfoWARE Server　セキュリティガイド　平成13年１月初版」,「SymfoWARE Server　RDB管理者ガイド　平成12年12月初版」,「SymfoWARE Server　SQLリファレンスガイド　平成12年6月初版」,「SymfoWARE Server　インストイールガイド 2001版」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、動作条件および機能仕様は本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。

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: SymfoWARE Server Enterprise Extended Edition
- バージョン: 4.0

開発者: 富士通株式会社　ソフトウェア事業本部
ミドルウェアプラットフォーム事業部　第二開発部

1.2.2 製品概要

本製品は商用向けのリレーショナルなデータベースである。ユーザ業務で発生する大量のデータを迅速に処理し、目的に応じて多面的に利用できるデータベースを提供する。SQL言語を用いて、データの構造を定義し、構造化されたデータへアクセスすることができる。本製品は、Solaris™7上で動作するソフトウェアである。動作環境の詳細は、1.5.8で述べる。

1.2.3 TOEの範囲

セキュリティ評価の対象となるTOEは、上で識別した製品と範囲が異なる。以下に示すように、製品の一部がTOEに該当する。

評価され認証されたTOEと同一のものをインストールするには、本製品に用意されている標準運用及び標準セキュリティ運用の二つの選択肢のうち、標準セキュリティ運用を選択しなければならない。その上で、以下の７機能のパッケージをインストールしなければならない(カッコ内はパッケージ名を示す)。

- RDBセキュリティ機能 (FJSVrdbse)
- SymfoWARE基本パッケージ (FJSVsymex)
- 標準コード変換機能 (FSUNiconv)
- RDB機能 (FSUNrdb2b)
- RDB機能のC言語プレコンパイル機能 (FSUNrdbcc)
- RDB機能のCOBOLプレコンパイル機能 (FSUNrdbco)
- 並列クエリ機能 (FSUNrdbps)

これらのパッケージをインストールすることによって多数のプログラムモジュールが生成されるが、そのすべてがTOEに含まれることにはならない。SymfoWARE基本パッケージ中のRDB2_TCP連携機能に関係する「jypvbrp.c」「jypvbsp.c」のモジュール、及びXA連携機能に関係する「jypvpxop.c」「jypvpxcl.c」「jypvpxst.c」「jypvpxed.c」「jypvpxtr.c」のモジュールは、TOEの範囲外である。これらのモジュールは、TOE の機能に含まれないRDB2_TCP連携機能、及びXA連携機能に関係しており、評価・認証の対象から除外される。

1.2.4 TOE動作概要

TOEの機能と動作の概要を説明する。TOEの機能には、以下の5つの機能(上述のパッケージ機能に直接対応した機能名称ではない）がある。

- ― プロセス間通信機能
- ― セションを制御する機能
- ― データへアクセスする機能
- ― データを保守する機能
- ― セキュリティ機能（さらに、以下の4機能に分類される; 詳細は1.5.5）
  - 運用選択機能
  - 利用者制御機能
  - 資源制御機能
  - 監査ログ機能

本製品は、他のアプリケーションや管理者・利用者コマンドと連携してデータベースとしての動作を行う。本製品の連携機能には、共用メモリを使用して自システムのアプリケーションやコマンドと連携するプロセス間通信機能の他に、TCP/IPを使用して他システムのアプリケーションと連携するRDB2_TCP連携機能、共用メモリを使用してXA連携製品と連携するXA連携機能がある。RDB2_TCP連携機能とXA連携機能は特殊なインタフェースであり、TOEの範囲外である。

TOEの機能及びそれ以外の機能の相互関係を**図1**に示す。

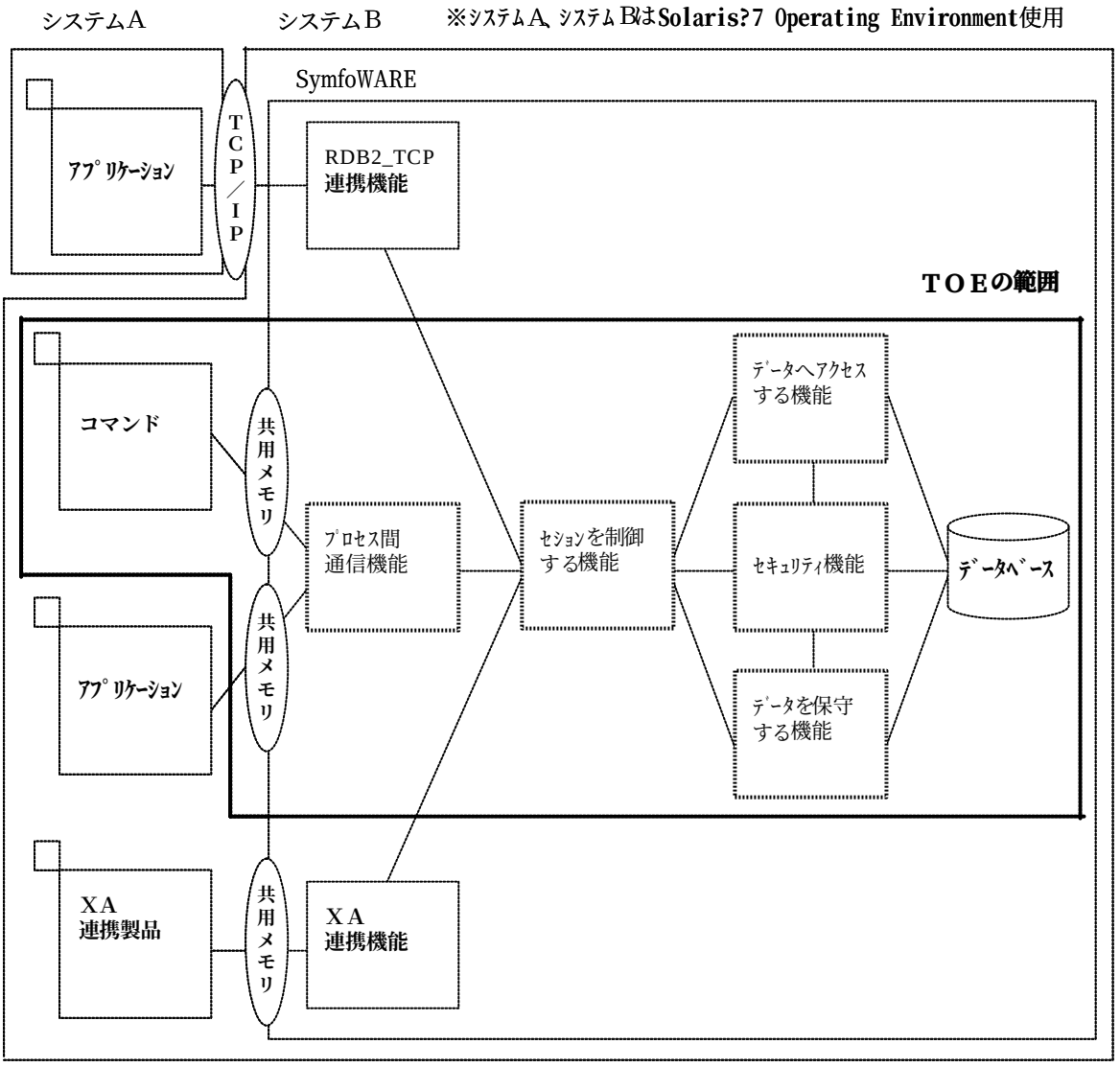

図1　SymfoWAREの機能構成

図2にTOEのプロセス実行イメージを示す。

利用者及び管理者は、アプリケーションまたはコマンドの実行を通してTOEにアクセスする。利用者の識別情報を指定して実行したアプリケーションのプロセスを利用者のプロセス、また管理者の識別情報を指定して実行したアプリケーションのプロセス、管理者が実行したコマンドのプロセスを管理者のプロセスと呼ぶ。ファイルに格納されているデータに対するアクセスは、アプリケーションのプロセスおよびコマンドのプロセスとは別の、専用のサーバプロセスで行う。

アプリケーションのプロセスやコマンドのプロセスと、サーバプロセスとの間の情報の受け渡しはプロセス間共用メモリを使用して行われる。

プロセスを分離している理由は、アプリケーションにおける論理ミスから、資源ファ

イルに格納されているデータを保護するためである。

TOEがOSから獲得する資源（プロセス、共用メモリおよびファイル)の保護はOSが行う。

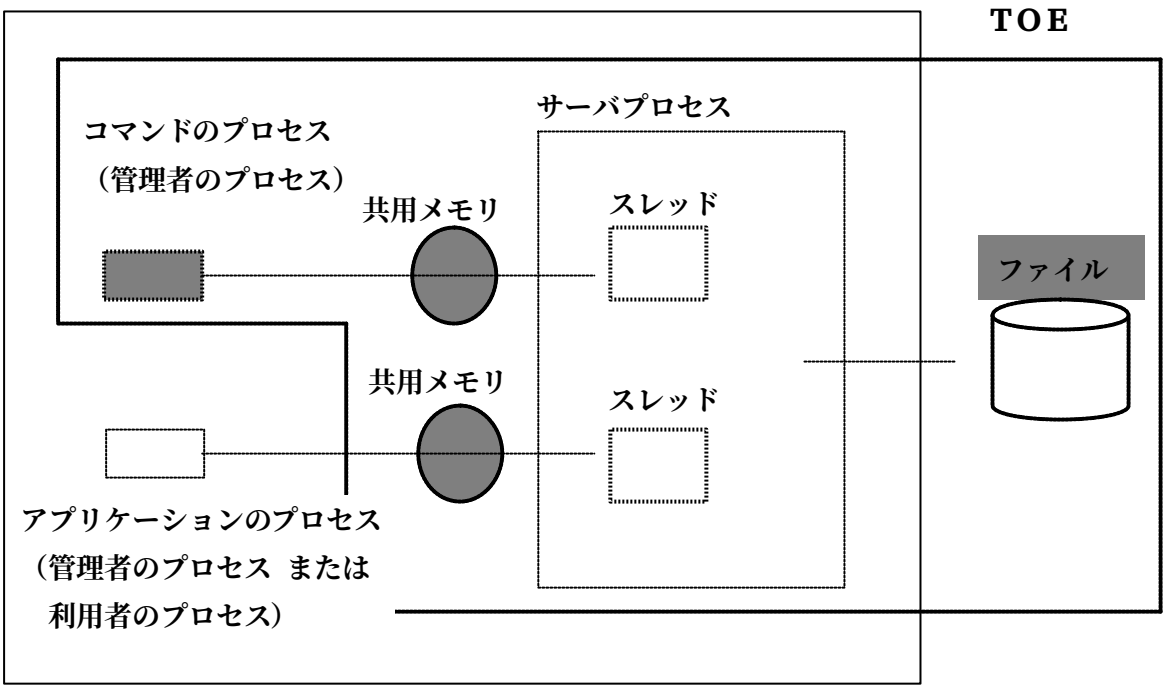

図 2　TOE のプロセス実行イメージ

1.3　評価の実施

本TOEのセキュリティ評価は、独立行政法人製品評価技術基盤機構が独立した認証機関として運営する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セキュリティ認証申請等の手引き (平成14年4月)」[2]、「ITセキュリティ評価機関に対する要求事項 (平成14年4月)」[3]、「ITセキュリティ認証申請者・登録者に対する要求事項 (平成14年4月)」[4]に規定された内容に従って実施された。

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、本TOEのセキュリティ設計である「SymfoWARE Server Enterprise Extended Edition 4.0 セキュリティターゲット 第2.1版」(以下「本ST」という。）[1]、本TOE開発に関連する評価用提供物件及び本TOEの開発環境・製造・出荷の現場を調査し、本TOEとその開発環境等がCCパート1([5][8][11][14][20][21]のいずれか)附属書C、CCパート2（[6][9][12][15][20][21]のいずれか]の機能要件及びCCパート3（[7][10][13][16][20][21]のいずれか）の保証要件を満たしていることを評価することである。この評価手順及び結果は、「SymfoWARE Server Enterprise Extended Edition 4.0 評価報告書」(以下「本評価報告書」という。）[22]に示されている。なお、評価方法は、CEMパート2（[17][18][19] [20][21]のいずれか）に準拠する。

1.4　評価の認証

認証機関は、評価機関である電子情報技術産業協会　ITセキュリティセンターが作成した、本評価報告書、当該所見報告書[23]及び関連する評価証拠資料を検証し、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[24]を作成した。評価は、平成15年8月26日の評価機関による本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、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が判明した。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

TOEの評価保証レベルは、EAL4である。

1.5.3　セキュリティ機能強度

最小機能強度として、”SOF-basic”を主張する。

本TOEは一般のコマーシャルシステムの中で利用されることを想定しているため、想定される不正行為は、公開情報を利用した攻撃であり、攻撃者の攻撃力は”低レベル”である。このため、低レベルの攻撃能力に対抗できるレベルである”SOF-basic”で必

要なセキュリティ機能強度を満たすことができる。

1.5.4 セキュリティ機能

本TOEが持つセキュリティ機能の概要を以下に示す。

(1) 運用選択機能(F.SEL)

セキュリティパラメタを使用して、セキュリティ機能のふるまいを変更する機能である。なお、インストール時に「標準セキュリティ運用」を選択することによって、セキュリティパラメタにセキュリティ上最も安全な値が設定される。セキュリティパラメタ（運用全体、利用者制御関係、監査ログ関係）は、パラメタを変更する機能(F.SEL.PARA)によって変更できる。

(2) 利用者制御機能(F.USER)

管理者及び各利用者を識別し、権限を制御し、指定された権限の範囲での処理を保証し、さらに範囲を超えた処理を制限する。管理者は、スーパユーザであり、変更できない。管理者は、全ての権限を保持し資源も無制限に使用できる。利用者制御機能には、以下の a)～e)の機能が含まれる。

ａ）利用者の登録機能(F.USER.DEF)

管理者及びOSにログインできる利用者の一部に対してTOEを使用させる機能と、OSのログインユーザとは別にTOEで独自に利用者を管理する機能がある。前者は、識別情報のみを、後者は、認証情報と識別情報を登録する。

ｂ）認証識別機能(F.USER.AUTHEN)

OSにログインした管理者・利用者が、そのままTOEに結合しようとした場合は識別だけを、そうでない利用者の場合は識別・認証を行う。

認証が失敗すると（連続する認証不成功が一定数に達すると）、TOEは、その利用者の認証情報を無効化し、TOEを利用できなくする。利用者情報の回復は、管理者だけが行える。

TOEは、登録される認証情報の品質を検査する機能を持ち、認証情報登録時に自動的に検査を行う。

ｃ）権限の制御機能(F.USER.PRIV)

管理者は全てのアプリケーションとコマンド実行権限を持ち、かつ利用者に対する権限付与の権限を持つ。利用者は管理者から付与される権限の範囲で、表の操作およびプロシジャの実行を行う。

ｄ）資源量の制御機能(F.USER.RES)

管理者は、各利用者が使用可能な資源量を制限する。制限の対象となる資源は以下の通りである。

- データベーススペース
- ディクショナリ
- 監査ログファイル
- 作業用ファイル
- アプリケーションのプロセスに対応する共用メモリ
- アプリケーションのプロセスに対応するサーバプロセスのスレッド
- 同時使用セション数

e）権限情報の参照機能(F.USER.REF)

各利用者は、自分の識別関連情報、権限情報、使用可能資源量を参照できる。管理者は、全利用者に関する情報を参照できる。

(3) 資源制御機能(F.RES)

TOEは、使用する資源を制御する機能を有する。TOEがOSから獲得し、使用済となったファイルは、OSへの返却前に残存情報を初期化する。

(4) 監査ログ機能(F.AUDIT)

セキュリティ機能の動作に関わる情報を監査ログとして記録する。監査ログ機能には、以下の a)～c)がある。

a）監査ログの取得機能(F.AUDIT.COL)

所定のセキュリティ機能の動作を監視し、記録する。

b）監査ログの参照機能(F.AUDIT.VIEW）

管理者は、SQL文を使用して監査ログを参照できる。

c）監査ログ領域管理機能(F.AUDIT.SPACE)

監査ログは、複数個の単位（エレメント）に分割して格納される。監査ログが満杯になると、管理者は、TOEを停止するか、監査対象事象をコンソールに出力してTOEを動作継続させるか、あるいは最も古い監査ログから順に新しい監査ログを上書きしてTOEを動作継続させる。

1.5.5 脅威

本TOEは、表 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 想定する脅威

識別子	脅威

T.TCP	RDB2_TCP連携機能を使用したデータベースへの結合： 利用者またはTOEへの結合を許可されていない者が、RDB2_TCP連携機能を利用して、データベーススペース、ディクショナリ、監査ログファイルを参照、改ざんする。
T.XA	XA連携機能を使用したデータベースへの結合： 利用者またはTOEへの結合を許可されていない者が、XA連携機能を利用して、データベーススペース、ディクショナリ、監査ログファイルを参照、改ざんする。
T.ACCESS	アプリケーション、コマンドを使用したデータベースへの結合： 利用者またはTOEへの結合を許可されていない者が、TOEの機能を使用して、保護資産への許可されていない操作を行う。この許可されていない操作には、管理者のみが実行可能な操作も含まれる。
T.RESOURCE	資源の枯渇： 利用者がTOEを利用する不当なアプリケーションを実行することで、TOEが動作するために必要な資源（データベーススペース、ディクショナリ、監査ログファイル、ログファイル、作業用ファイル、動作環境ファイルおよび実行資源）が枯渇し、管理者や利用者のTOEに対する正当な処理ができなくなる（たとえば、使用可能なセションがすべて占有されて、管理者が監査ログ情報を参照できなくなる）。
T.OS	オペレーティングシステムの機能を用いた攻撃： TOEがOSから獲得して使用しているデータベーススペース、ディクショナリ、監査ログファイル、ログファイル、作業用ファイル、動作環境ファイルに対し、ネットワーク経由でOSの機能を使用して直接アクセスすることによって、利用者またはTOEへの結合を許可されていない者が、保護資産への許可されていない操作を試みる。
T.DATA	使用済みの資源からの情報の取得： TOEがOSから獲得した後、使用済みとなり、OSへ返却したデータベーススペース、ディクショナリ、監査ログファイル、ログファイル、作業用ファイル、動作環境ファイルに残存する情報を、利用者またはTOEへの結合を許可されていない者が参照する。

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、リレーショナルなデータベース管理システム製品である。本TOEが必要とするハードウェア／ソフトウェア環境の構成は、以下のとおりである。

■本TOEの環境構成条件

HW:
- プロセッサ: 400MHz以上(2CPU以上)
- メモリ: 1GB以上
- ハードディスク: 1GB以上

OS: Solaris™7 Operating Environment（日本版）
適用パッチ：106541-08、107544-03

1.5.8 動作環境の前提条件

本TOEを使用する環境において有する前提条件を表に示す。

本TOEのセキュリティ機能が有効に動作するためには、これらの前提条件がすべて満たされねばならない。

表2　TOE使用の前提条件

識別子	前提条件
A.MANAGER	管理者の正当性： 管理者は、不正を行わない。
A.USER	利用者による管理： 利用者は、利用者自身が使用するパスワードやアプリケーションを安全に管理する。
A.PHYSICAL	物理的な保護： TOEの動作に関連する機器、機器を設置する部屋および建物が物理的に保護されており、管理者以外は、機器に対し物理的なアクセスを行うことはできない。

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。

- 「SymfoWARE Server　セキュリティガイド　平成13年１月初版」

- 「SymfoWARE Server　RDB管理者ガイド　平成12年12月初版」
- 「SymfoWARE Server　SQLリファレンスガイド　平成12年6月初版」
- 「SymfoWARE Server　インストイールガイド　2001版」

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パート2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、本評価報告書において報告されている。本評価報告書では、TOEの概要説明、CEMパート2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、本評価報告書による評価実施の履歴を示す。

評価は、平成14年9月に始まり、平成15年8月本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14年9月及び12月に開発・製造現場へ赴き、構成管理・配付と運用・ライフサイクルの各ワークユニットに関するプロセスの施行状況の調査を、記録及びスタッフへのヒアリングにより実施し、同現場で開発者のテスト環境と同等の環境を構築し開発者サンプリングテスト及び評価者テストも実施している。

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記録され、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、評価に反映された。

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

1) 開発者テスト環境

開発者が実施したテストのシステム構成を**図3**に示す。

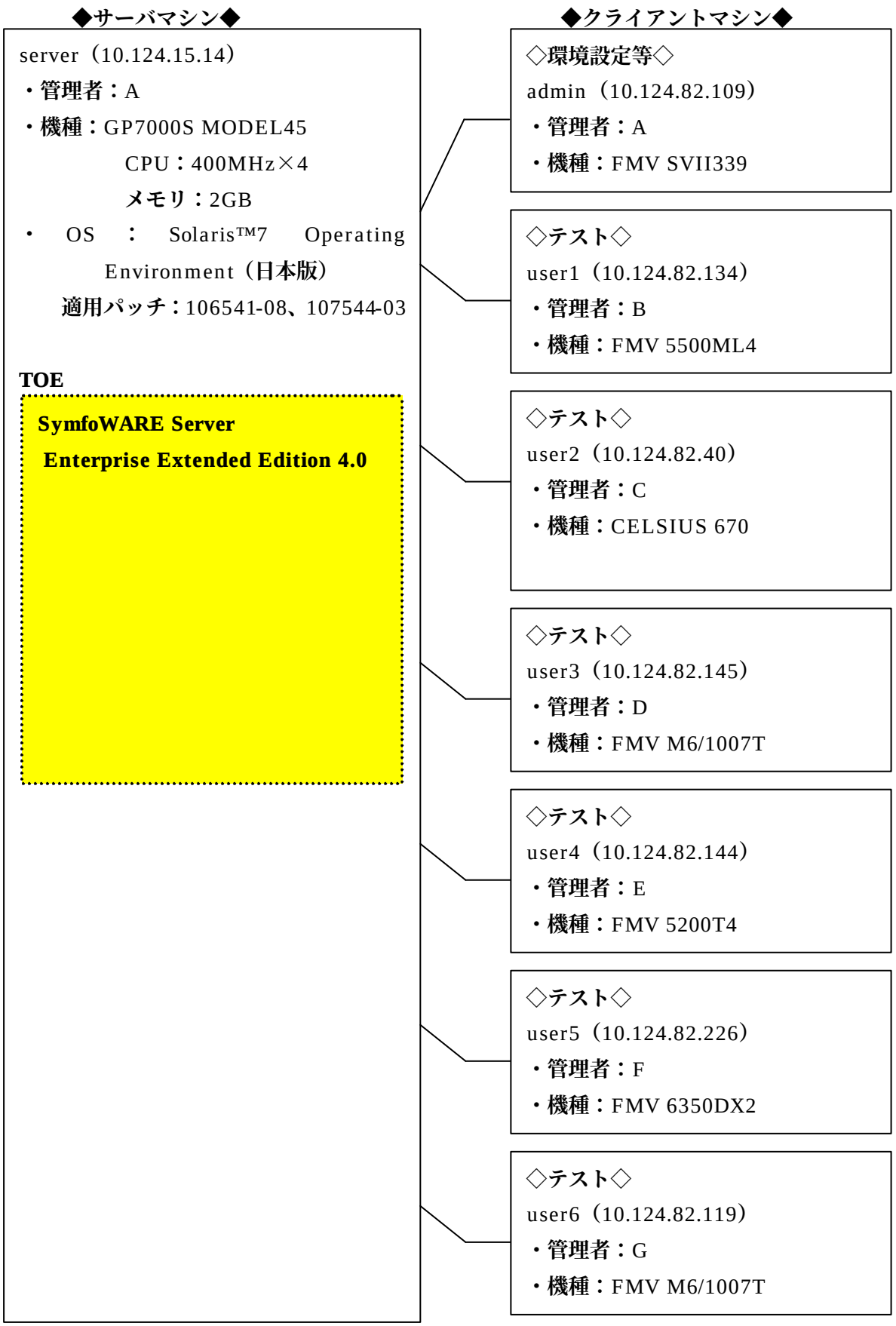

図3　開発者テストシステム構成図

テストシステムの各機器の構成を以下に示す。

サーバ環境

・機種：GP7000S MODEL45
CPU：400MHz×4
メモリ：2GB
・OS：Solaris™7 Operating Environment（日本版）
適用パッチ：106541-08、107544-03

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

①テスト構成

開発者が実施したテストの構成は図3に示す。本構成は本STの記述と一致している。

②テスト手法

STで識別された各セキュリティ機能に対して、機能のふるまいに影響を与える要因を分析し、各セキュリティ機能のすべての要因に対し網羅的にテストを実施している。

③実施テストの範囲

テストは7名の担当者によって1,079項目実施されている。TOEのセキュリティ機能（4項目11種）に対してカバレージ分析及び深さ分析が実施され、各セキュリティ機能のすべてを網羅する十分な量のテストが実施されている。

④結果

開発者によるテスト結果は、テスト計画／報告書において期待されるテスト結果と実際のテスト結果が一致していることを確認している。評価者は、開発者テストの実施方法、実施項目の正当性を確認し、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

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システム構成は、開発者テストと同様の構成である。

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。

① テスト構成

評価者が実施したテストの構成は**図3**に示す。本構成は本STの記述と一致しており、開発者のテスト環境とも一致する。

② テスト手法

開発者テストのサンプリングについては、すべてのセキュリティ機能を網羅すること、及び特にTOEのセキュアな運用に大きく影響する認証識別機能を重点的に選択することを考慮し、開発者が作成したテスト手順に従いテストを実施している。独立テストについては、開発者テストにおいて考慮されていないと思われる項目、及びSolaris OSの環境に影響される部分を考慮して、評価者が独自に作成した独立テスト表、侵入テスト表に従ってテストを実施している。

③ 実施テストの範囲

開発者テストのサンプリングによるテストを168項目、評価者が独自に考案したテストを40項目、計208項目のテストを実施した。

テスト対象となる機能はTOEの有するセキュリティ機能の中から選択しているが、特に認証識別機能についてはTOEのセキュアな運用に大きく影響するため、重点的に選択している。

3) 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。すべてのテスト結果は期待されるふるまいと一致した。また、悪用し得る脆弱性を検出することはできなかった。ただし、本TOEは管理者の識別及び認証をSolaris OSの識別認証機能に依存している。このため、Solaris OSにおける識別認証が確実に行われないと、TOEの管理者権限が攻撃者に簒奪される可能性が生じるので、注意が必要である。

2.4 評価結果

本評価報告書をもって、評価者は本TOEがCEMパート2のワークユニットすべてを満たしていると判断している。

3 認証実施

認証は、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本評価報告書で示されたように評価されていること。

④ 本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 本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、本ST及び本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

提出された本評価報告書、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、本TOEがCCパート3（[7][10][13][16][20][21]のいずれか）に規定されたEAL4で要求されてい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アクションエレメントについての認証結果を表5にまとめる。

表 5 評価者アクションエレメント認証結果

評価者アクションエレメント	認証結果
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。また、当評価に至るまでになされた指摘(所見報告書)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性の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指摘(所見報告書)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、当評価に至るまでなされた指摘(所見報告書)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指摘(所見報告書)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。また、当評価に至るまでになされた指摘(所見報告書)も適切と判断される。
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。また、当評価に至るまでになされた指摘(所見報告書)も適切と判断される。
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明記され、それらが脅威、組織のセキュリティ、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、当評価に至るまでなされた指摘(所見報告書)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理路整然とし、完結しており、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指摘(所見報告書)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、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、当評価に至るまでなされた指摘(所見報告書)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理路整然とし、完結しており、かつ一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)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るすべてのTOE及びIT環境の要件の記述が、正当であること、客観的に、明確に、曖昧さなく表現されていること、及び保証要件でサポートされるのに適切で妥当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、あらゆるCCを参照せずに明示されたITセキュリティ要件の依存性のすべてが識別されてい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、当評価に至るまでなされた指摘(所見報告書)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結しており、理路整然とし、かつ一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)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_AUT.1.1E	評価はワークユニットに沿って行われ、CMシステムが人為的誤りまたは怠慢による影響を受けないように、実装表現に対する変更が自動化ツールのサポートにより制御されていることを確認している。
ACM_AUT.1.1D	評価はワークユニットに沿って行われ、CM計画に記述されている自動化ツールと手順が使用されていることを確認している。
ACM_CAP.4.1E	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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ACM_SCP.2.1E	評価はワークユニットに沿って行われ、CMシステムにCCで必要とされるものが含まれており、CM証拠資料に各ライフサイクルを通して構成要素のステータスの追跡、割当ての方法、構成要素変更に伴う関連する構成要素が記述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_DEL.2.1E	評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ADO_DEL.2.2D	評価はワークユニットに沿って行われ、配付証拠資料が、TOEを利用者サイトに配送するときに、TOEの完全性を維持し、変更または置換を検出するために使用されるすべての手続きを記述していることを確認している。
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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
開発	**適切な評価が実施された**

ADV_FSP.2.1E	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を確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ADV_FSP.2.2E	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、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ADV_HLD.2.1E	評価はワークユニットに沿って行われ、上位レベル設計が明確で矛盾のないこと、サブシステムを規定しそのセキュリティ機能を記述していること、TSF実現に必要なIT環境としてのハードウェア、ソフトウェア、ファームウェアを説明していること、TSFサブシステムの外部とその他のインタフェースが識別され、それらの詳細を記述していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ADV_HLD.2.2E	評価はワークユニットに沿って行われ、上位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。
ADV_IMP.1.1E	評価はワークユニットに沿って行われ、実装表現は、それ以上の設計上の決定を必要とせずに、TSFが生成されうるほどの詳細レベルまでTSFを曖昧さなく定義され、内部的に一貫していることを確認している。
ADV_IMP.1.2E	評価はワークユニットに沿って行われ、提供された最も抽象度が低いTSF表現が、TOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。
ADV_LLD.1.1E	評価はワークユニットに沿って行われ、下位レベル設計がSTの機能要件を十分に満たしていること、及び上位レベル設計の正しい有効な詳細化であることを確認している。当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ADV_LLD.1.2E	評価はワークユニットに沿って行われ、下位レベル設計が、TOEセキュリティ機能要件の正確かつ完全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り、上位レベル設計が機能仕様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。
ADV_SPM.1.1E	評価はワークユニットに沿って行われ、セキュリティ方針モデルがセキュリティ方針の規則と特性を明確にまた一貫して記述してこと、及びこの記述が機能仕様のセキュリティ機能の記述と一致していることを確認している。当評価に至るまでなされた指摘(所見報告書)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、他のドキュメントと一貫しており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、当評価に至るまでなされた指摘(所見報告書)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、利用者が利用可能なセキュリティ機能やインタフェースが提供されておらず、利用者ガイダンスは存在しないため、非適用であることを確認している。
ライフサイクルサポート	**適切な評価が実施された**
ALC_DVS.1.1E	評価はワークユニットに沿って行われ、開発セキュリティ証拠資料がTOE開発環境のセキュア維持のための手段を記述しており、それが十分であること、その手段を実施した記録が生成されることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ALC_DVS.1.2E	評価はワークユニットに沿って行われ、ALC_DVS.1.2Eで確認したセキュリティ手段が実施されていることを確認している。また、本評価時に行われたサイト訪問での調査方法も適切と判断される。
ALC_LCD.1.1E	評価はワークユニットに沿って行われ、開発者がTOEライフサイクルの引証されたモデルを使用していることを確認している。

ALC_TAT.1.1E	評価はワークユニットに沿って行われ、開発者が、一貫性があり予測可能な結果をもたらす明確に定義された開発ツールを使用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_COV.2.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。
ATE_DPT.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが上位レベル設計に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。
ATE_FUN.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果が含まれておりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ATE_IND.2.1E	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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ATE_IND.2.2E	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サイト訪問でのテスト実施方法も適切と判断される。

ATE_IND.2.3E	評価はワークユニットに沿って行われ、サンプリングテストを実施し、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、本評価のサンプリング方針及びサイト訪問でのテスト実施方法も適切と判断される。
脆弱性評定	**適切な評価が実施された**
AVA_MSU.2.1E	評価はワークユニットに沿って行われ、管理者ガイド及びインストールガイドがTOEのセキュアな運用に必要な情報を矛盾なく完全に記述していること、使用環境の前提事項、TOE以外のセキュリティ事項の要件がすべて明記されていることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
AVA_MSU.2.2E	評価はワークユニットに沿って行われ、管理者ガイド及びインストールガイドのみの情報でTOEを構成でき、セキュアな運用に関わる設定が行えることを確認している。
AVA_MSU.2.3E	評価はワークユニットに沿って行われ、管理者ガイド及びインストールガイドが、TOEが非セキュアな状態に陥ったことを検出する手段及び対処方法が記述されていることを確認している。
AVA_MSU.2.4E	評価はワークユニットに沿って行われ、TOEの操作のすべてのモードにおけるセキュアな操作のためにガイダンスが提供されていることが分析証拠資料に示されていることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
AVA_SOF.1.1E	評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされていることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
AVA_SOF.1.2E	評価はワークユニットに沿って行われ、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しことを確認している。

AVA_VLA.2.1E	評価はワークユニットに沿って行われ、脆弱性分析が明らかな脆弱性に関する情報を考慮していること、明らかな脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
AVA_VLA.2.2E	評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト内容を記述し、脆弱性分析とあわせて悪用可能な明らかな脆弱性が存在しないことを確認している。また、実施したテストの詳細と悪用され得る脆弱性及び残存脆弱性について報告がなされている。
AVA_VLA.2.3E	評価はワークユニットに沿って行われ、開発者の脆弱性分析でこれまでに取り扱われていない、可能性のあるセキュリティ脆弱性であることを決定するために、独立脆弱性分析を実施している。
AVA_VLA.2.4E	評価はワークユニットに沿って行われ、独立脆弱性分析に基づき、意図した環境において、新たに識別された脆弱性が悪用され得るかどうかを決定するため、独立侵入テストを実施し、成果を報告している。
AVA_VLA.2.5E	評価はワークユニットに沿って行われ、意図した環境において低い攻撃能力を持つ攻撃者が悪用可能な脆弱性が存在しないことを報告している。

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
CM	Configuration Management
DDL	Data Definition Language
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SFP	Security Function Policy
SOF	Strength of Function
SQL	Structured Query Language
ST	Security Target
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface

本報告書で使用された用語を以下に示す。

アプリケーション	本書では、利用者が作成するアプリケーションプログラムすべてを指す。
エレメント	本書では、監査ログエレメントを指す。監査ログ表は、複数のDSIに分割されている。この監査ログ表のDSIを監査ログエレメント(または略してエレメント)と呼ぶ。
監査ログ	日常の管理者および利用者の監視や、セキュリティ上の問題が発生した場合の原因を特定するための情報として、利用者の行った処理、管理者の行った処理、発生した異常な事象

	をログとして残している。このログを監査ログと呼ぶ。
管理者	本書では、SymfoWAREを管理する管理者を指す。また、SymfoWAREの管理者はOSの管理者でもある。
コマンド	本書では、SymfoWAREを運用するためのコマンドを指す。
共用メモリ	プロセス間で相互に参照が可能なメモリ領域をいう。
サーバプロセス	本書では、アプリケーションやコマンドの処理を行うSymfoWAREのプロセスを指す。
作業用ファイル	作業用テーブルおよび作業用ソート領域を指す。
スーパユーザ	UNIXシステムを管理する特別の権限を持ったシステム管理者のことを指す。
スレッド	プロセス内で実行されるサブプロセスを指す。
責任者	本書では、セキュリティシステムの全責任を担う責任者を指す。責任者は、ふさわしい管理者の選任、管理者の教育等を行う必要がある。
セキュリティパラメタ	セキュリティシステムにおいて、SymfoWAREのアクセスを制約する各種パラメタを指す。
セッション	SymfoWAREに結合した時点から結合解除までの間を指す。
データベース	相互に関連するデータを整理・統合し，検索しやすくしたファイル。また，このようなファイルの共用を可能にするシステム。
データベーススペース	利用者のデータが格納されているファイル。データベーススペースには、論理的なアクセスの単位である表が格納されており、利用者のデータは、この表に格納される。
ディクショナリ	利用者が作成したデータベースに対して、データベースの論理構造／格納構造／物理構造に関する情報が格納されている。実際は、SymfoWAREのRDBディクショナリとRDBディレクトリファイルがあり、RDBディクショナリは、SQLで利用者によりアクセスされるものであり、RDBディレクトリファイルは、SymfoWAREが内部的に使用するものである。

動作環境ファイル	アプリケーションの実行時の動作環境を規定するためのファイル。
トランザクション	データベースのアクセスにおける一連のデータ操作の一貫性を保証する単位をトランザクションと呼ぶ。
並列クエリ	大量データを扱う業務の情報処理効率を上げるために、データベースを複数のDSIに分割し、それぞれを並列に処理する機能である。
標準運用	利用者に対する権限付与の制御による機密保護レベルのセキュリティ運用を指す。
標準セキュリティ運用	監査ログの取得、利用者への機能制限や資産へのアクセスの制限など、データベースシステム全体としてセキュリティ強度の高いセキュリティ運用を指す。本書では、標準セキュリティ運用を設定することを前提として説明している。
プロシジャ	サーバに登録する処理手続きを指す。プロシジャルーチンを呼び出し、サーバ側で一連のトランザクション処理を実行することで、性能限界解消を図る。
プロセス	UNIXシステムの仕事の単位を指す。
利用者	本書では、SymfoWAREを利用する一般利用者を指す。
リレーショナルデータベース(RDB)	SymfoWAREが採用しているデータベースである。リレーショナルデータベースでは、データを行と列からなる二次元の表で表現する。データベース操作は、データベース言語SQLで行う。
ログファイル	ログファイルには、テンポラリログファイルおよびアーカイブログファイルがある。テンポラリログファイルには、データベースの更新履歴が収集される。アーカイブログファイルには、トランザクションの更新履歴が収集される。
DSI	表のデータを格納する領域を、データベーススペースに割付けるために定義するもの。
RDB2_TCP連携	TCP/IP接続を使用してSymfoWAREと連携することを意味する。
XAインタフェース	分散トランザクション処理モデルでのトランザクションモニタと、リレーショナルデータベース管理システムとの連

携インタフェースをXAインタフェースと呼ぶ。XAインタフェースは、実質的なUNIXの標準を制定する団体X/Openが規定している。

XA連携　　XAインタフェースを使用してSymfoWAREと連携することを意味する。

6 参照

[1] SymfoWARE Server Enterprise Extended Edition 4.0 **セキュリティターゲット 第2.1版 2003年08月20日 富士通株式会社**

[2] **ITセキュリティ認証申請等の手引き 平成14年4月 独立行政法人 製品評価技術基盤機構 適合性評価センター**

[3] **ITセキュリティ評価機関に対する要求事項 平成14年4月 独立行政法人 製品評価技術基盤機構 適合性評価センター 適合－部門－IT機関要求－02**

[4] **ITセキュリティ認証申請者・登録者に対する要求事項 平成14年4月 独立行政法人 製品評価技術基盤機構 適合性評価センター 適合－部門－IT申請要求－02**

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[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2.1 1999年8月** CCIMB-99-031

[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2.1 1999年8月** CCIMB-99-032

[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2.1 1999年8月** CCIMB-99-033

[11] ISO/IEC 15408-1 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model ISO/IEC15408-1: 1999(E)

[12] ISO/IEC 15408-2 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements ISO/IEC15408-2: 1999(E)

[13] ISO/IEC 15408-3 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements ISO/IEC15408-3: 1999(E)

[14] JIS X 5070-1: 2000 **セキュリティ技術－情報技術セキュリティの評価基準－第1部: 総則及び一般モデル**

[15] JIS X 5070-2: 2000 **セキュリティ技術－情報技術セキュリティの評価基準－第2部: セキュリティ機能要件**

[16] JIS X 5070-3: 2000 **セキュリティ技術－情報技術セキュリティの評価基準－第3部: セキュリティ保証要件**

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part2: Evaluation Methodology Version 1.0 August 1999

[18] 情報技術セキュリティ評価のための共通方法論 CEM-99/045 パート2: 評価方法論 バージョン1.0 1999年8月

[19] JIS TR X 0049: 2001 情報技術セキュリティ評価のための共通方法

[20] CCIMB Interpretations-0210

[21] 補足-0210

[22] SymfoWARE Server Enterprise Extended Edition 4.0 評価報告書 第1.7版 2003年8月26日　02ITSC-E014 電子情報技術産業協会　ITセキュリティセンター

[23] 所見報告書

[24] 認証レビュー