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

申請受付日（受付番号）	**平成19年10月31日** (IT**認証**7181)
認証番号	C0144
認証申請者	**富士通株式会社**
TOE**の名称**	Symfoware Server Enterprise Extended Edition
TOE**のバージョン**	9.0.1
PP**適合**	**なし**
適合する保証パッケージ	EAL4
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20年1月25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

「Symfoware Server Enterprise Extended Edition 9.0.1」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、「Symfoware Server Enterprise Extended Edition 9.0.1」（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：　Symfoware Server Enterprise Extended Edition
バージョン：　9.0.1
開発者：　富士通株式会社

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を管理するソフトウェアである。この製品により、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。また、この製品では、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、このようなデータベースアクセスのための機能に加えて、不正なアクセスからデータベースを保護するための利用者制御、資源制御、監査ログなどのセキュリティ機能を提供する。

1.2.3 TOEの範囲と動作概要

セキュリティ評価の対象となるTOEは、1.2.1で識別した製品の一部である。

評価対象となるTOEの構成は、製品に含まれる全パッケージのうちの以下の6パッケージをインストールしたものである（末尾の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）
- RDB機能(基本)（FJSVrdb2b）
- RDB機能(サーバ)（FJSVrdbdb）
- RDB機能(クライアント)（FJSVrdbap）
- 並列クエリ機能（FJSVrdbps）

ただし、上記Symfoware基本パッケージとしてインストールされるモジュール群のうち、RDB2_TCP連携機能に関係するモジュール「jypvbrp.c」「jypvbsp.c」とXA連携機能に関係するモジュール「jypvpxop.c」「jypvpxcl.c」「jypvpxst.c」「jypvpxed.c」「jypvpxtr.c」についてはTOEの物理的範囲から除外するものとし、評価及び認証の対象外である。

なお、上記TOE構成を構築するためには、製品をインストールする際の選択肢（「標準運用」、「標準セキュリティ運用」）で「標準セキュリティ運用」を選択した上で、上記の6パッケージをインストールする必要がある。

上記のパッケージ群により提供されるTOEの動作イメージを図1-1に示す。この図の太枠内が動作中のTOE範囲を示す。

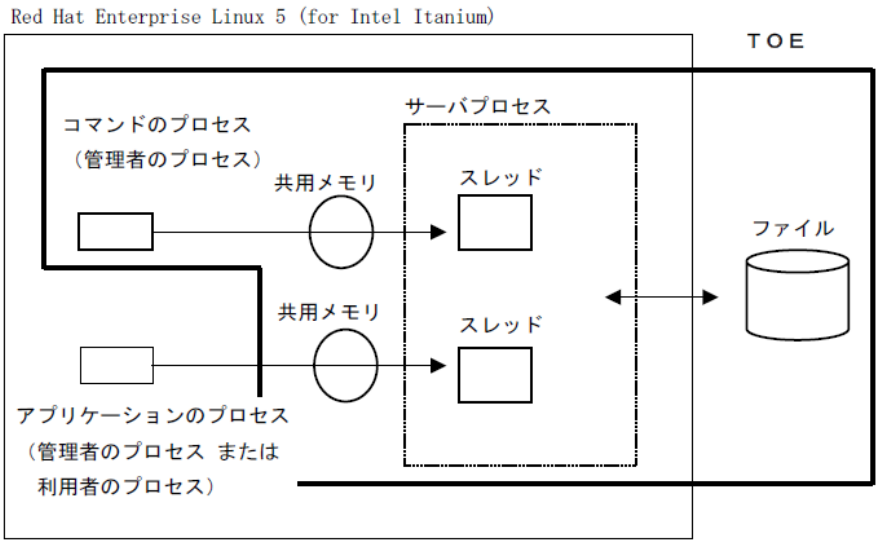

図1-1　TOEのプロセス実行イメージ

図1-1に示すように、TOEはOS(Red Hat Enterprise Linux 5 (for Intel Itanium))から獲得した資源(プロセス、共用メモリ、及びファイル)を使用して動作する。

SQL文を含むアプリケーション(TOE範囲外)またはコマンド(TOE範囲内)が利用者や管理者により起動されると、サーバプロセスがこれらのプロセスからのデータベースアクセスの要求を受け付けて処理する。このとき、アプリケーション・コマンドのプロセスとそれに対応する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。

なお、OSから獲得する資源（プロセス、共用メモリ、及びファイル)を保護する機能はOSが提供するものであり、評価及び認証の対象ではない。

1.2.4 TOEの機能

本TOEは、以下の5つの機能を提供する。

・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

TOEの機能構成と各機能間の関係を図1-2に示し、各機能の概要を説明する。

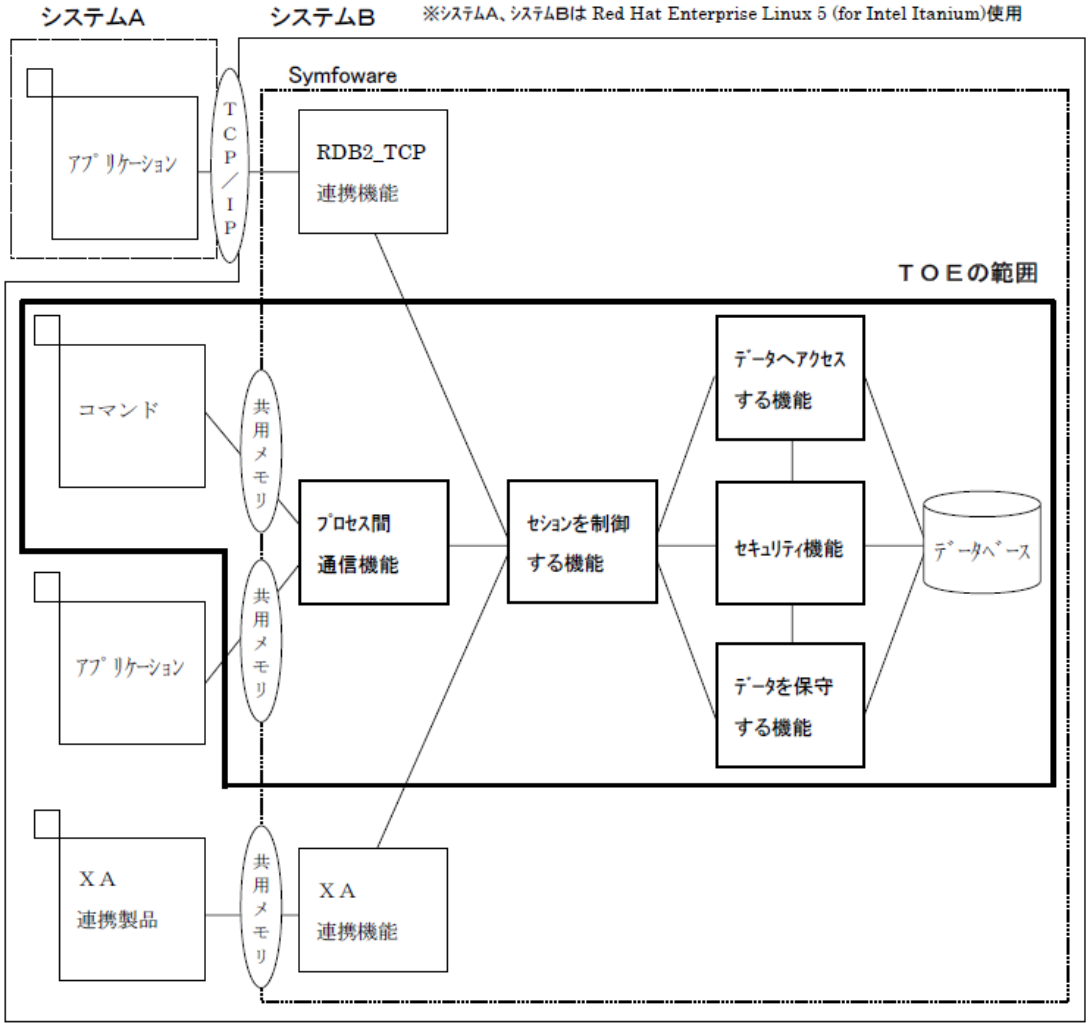

図1-2　機能構成

(1) プロセス間通信機能

アプリケーションのプロセス及びコマンドのプロセスとサーバプロセスとの間で共用メモリを使用した通信制御を行う。

(2) セションを制御する機能

アプリケーションのプロセスとサーバプロセスを結合及び結合解除する。

(3) データへアクセスする機能

アプリケーションに埋め込んだSQL文を実行することにより以下を行う。

・データの挿入
・データの更新
・データの削除
・データの参照
・シーケンスの参照
・プロシジャの実行

・ファンクションの実行

(4) データを保守する機能

アプリケーションに埋め込んだSQL文またはコマンドを実行することにより以下を行う。

・データベースの構造定義
・データのロード
・データのアンロード
・データのバックアップ
・データのリカバリ

(5) セキュリティ機能

上記の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の各機能を安全に使用するために以下の機能を提供する。

・運用選択機能
　セキュリティ機能の全体のふるまいを変更する。
・利用者制御機能
　各利用者の権限を制御し、指定された権限の範囲での処理を保証し、またその範囲を超えた処理を制限する。
・資源制御機能
　TOEが使用する資源を制御する。
・監査ログ機能
　利用者や管理者の処理の情報を記録する。

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「Symfoware 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・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､「Symfoware Server Enterprise Extended Edition 9.0.1 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。評価は、平成20年1月の評価機関による評価報告書の提出をもって完了し、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、EAL4適合である。

1.5.3 セキュリティ機能強度

STは、最小機能強度として、”SOF-基本”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おり、そこで想定される不正行為は、公開情報を利用した攻撃であることから攻撃者の攻撃力を「低レベル」と想定することは妥当である。

よってSOF-基本で十分である。

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) 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。

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はセキュリティ上最も安全な値が初期設定されるが、運用全体、利用者制御関係、及び監査ログ関係のセキュリティパラメタはパラメタを変更する機能（F.SEL.PARA）によってTOE運用中に変更できる。

(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。管理者はすべての権限を保持し、資源も無制限に使用できるスーパユーザであり、これを変更することはできない。

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、後者は識別情報と認証情報を登録する。

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。
また、認証情報の登録時に、登録される認証情報の品質を自動的に検査する。

c) 権限の制御機能（F.USER.PRIV）
管理者はすべてのアプリケーションとコマンドの実行権限を持ち、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、シーケンスの参照、プロシジャ・ファンクションの実行を行う。

d) 資源の制御機能（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とおりである。
・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
・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）
使用する資源を制御する機能である。OSから獲得後に使用済み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。また、関連するTSFデータの参照を、管理者のみに限定する。

(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)が含まれる。

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を停止させるか、監査対象事象をコンソールに出力してTOEの動作を継続させるか、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の動作を継続させる。

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.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、動作環境ファイル及び実行資源）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	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。

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。

○ ハードウェア

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

○ ソフトウェア

OS：	Red Hat Enterprise Linux 5（for Intel Itanium）

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.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及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。

- 製品ご案内
  [CA92254-4279-01]
- Symfoware Server セキュリティ運用ガイド
  [J2X1-1282-02Z2(00)]
- Symfoware Server メッセージ集
  [J2UZ-6532-03Z2(A)]
- Symfoware Server SQL リファレンス
  [J2X0-1648-01Z2(00)]
- Symfoware Server インストールガイド
  [B5221N-0901-1]

- Symfoware Server インストールガイド(サーバ編)
  [J2UZ-6522-03Z2(A)]
- Symfoware Server インストールガイド(クライアント編)
  [J2X1-1292-03Z2(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11月に始まり、平成20年1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11月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、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行った。また、平成19年11月に開発者サイトで開発者のテスト環境を使用し、開発者が実施したテストのサンプリングチェック及び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。

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構成を図2-1に示す。TOEは図2-1に示すサーバマシン上にインストールされた状態でテストされた。また、実際の操作はクライアントマシンからサーバマシンにログインして行われた。

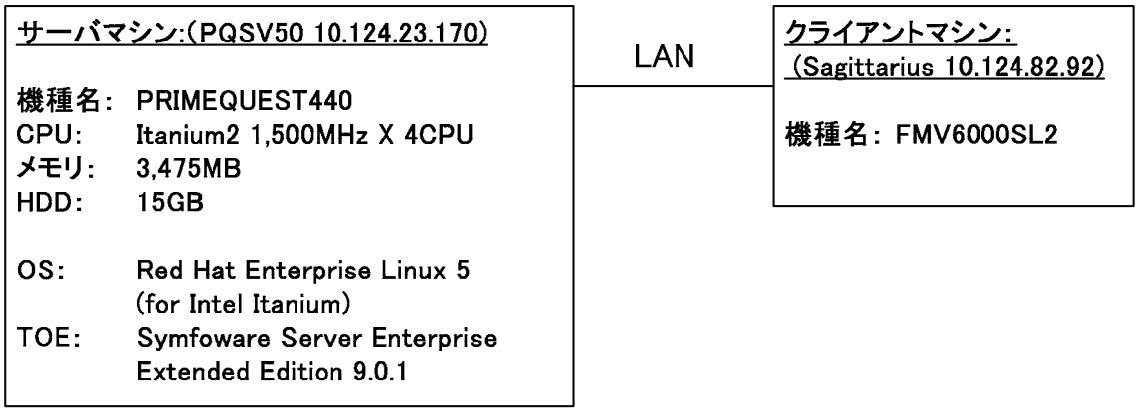

図2-1　開発者テストの構成図

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。

a.テスト構成

開発者が実施したテストの構成を図2-1に示す。開発者テストは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。

b.テスト手法

テストには、以下の手法が使用された。

①ST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、すべての要因に対して網羅的にテストを実施する。

②要因の組み合わせに対応したテスト用シェルスクリプト及び監査ログを取得するためのアプリケーションを準備し、その実行結果(出力メッセージの番号、シェルやコマンドの復帰値、監査ログの内容、端末出力の内容、など）を観察する。

c.実施テストの範囲

テストは開発者によって1,107項目実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証されている。深さ分析が実施され、上位レベル設計に記述されたすべてのサブシステムとサブシステムインタフェースが十分にテストされたことが検証されている。

d.結果

開発者によるテスト結果は、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。

a.テスト構成

評価者が実施したテストの構成を図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構成と同一のTOE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すべてのセキュリティ機能を網羅すること、及び本バージョンのTOEにおいて新規に追加されたセキュリティ機能に関するテストを重点的に選択することを考慮し、テスト項目を作成する。

②各テスト項目に対応したテスト用シェルスクリプト及び監査ログを取得するためのアプリケーションを準備し、その実行結果（出力メッセージの番号、シェルやコマンドの復帰値、監査ログの内容、端末出力の内容、など）を観察する。

c.実施テストの範囲

評価者が独自に考案したテストを31項目、開発者テストのサンプリングによるテストを346項目、計377項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

① 他のセキュリティ機能よりも重要なセキュリティ機能

② 本バージョンのTOEにおいて新規に追加されたセキュリティ機能

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。

認証機関は、ST及び評価報告書において、所見報告書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EAL4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。
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すべてのTOE及びIT環境のセキュリティ要件の記述が、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、CCを参照せずに明示されたあらゆる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。

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_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。
ACM_SCP.2.1E	評価はワークユニットに沿って行われ、構成要素リストがCCによって要求される一連の要素を含んで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。
ADO_DEL.2.2D	評価はワークユニットに沿って行われ、実際に配付手続きが使用されていることを、実地検査により確認している。
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。
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.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、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.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。
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。
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、実装表現がTSFを作成できる詳細レベルでTSFを明確に定義していること、開発者の提供した実装表現が十分足るものであること、それが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、実装表現のサブセットがその関連するTOEセキュリティ機能要件を正しく具体化したもの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、下位レベル設計が必要な説明情報を含み、内部的に一貫していること、モジュールの観点から記述されており、各モジュールの目的を記述していること、提供されるセキュリティ機能という観点でモジュール間の相互関係と依存性を定義していること、TSP実施機能の提供方法を記述していること、TSFモジュールのインタフェースと外部インタフェースを識別していること、各モジュールの使用法と目的を記述していること、そしてTSP実施モジュールとその他に区別できることを確認している。

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り、下位レベル設計が上位レベル設計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非形式的でありSTにおいて明示的方針をもたないこと、ST中のセキュリティ機能要件で表されたすべてのセキュリティ方針がモデル化されていること、セキュリティ方針モデルの規則や特性がモデル化されたTOEのセキュリティふるまいを明確に表していること、モデル化されたふるまいがセキュリティ方針と一貫し完全であること、セキュリティ方針を実装している機能仕様にてすべてのセキュリティ機能を識別していること、機能仕様の内容とセキュリティ方針モデルの実装として識別された機能の内容が一貫していることを確認している。
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。
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。
ALC_DVS.1.2E	評価はワークユニットに沿って行われ、ALC_DVS.1.1E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、使用されたライフサイクルモデルが開発者と保守手続きをカバーしており、その記述にある手続き、ツール、技法の使用が開発と保守に貢献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、開発ツール証拠資料が明確であり、実装に用いられた開発ツールのステートメント及び実装依存オプションの意図を明確に定義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を含んで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。
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。
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、提供されたガイダンスが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、ガイダンスの完全性を保証する手段を開発者が講じていることを確認している。
AVA_MSU.2.2E	評価はワークユニットに沿って行われ、提供されたガイダンスの管理者と利用者手続き、あるいはその他の手続き情報のみで、TOEを構成でき、TOEの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、提供されたガイダンスが、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を記述し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、提供されたガイダンスが、TOEの全ての操作モードにおいてのセキュアな操作を提供していることを確認している。
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。
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主張が正しい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、脆弱性分析が脆弱性に関する情報を考慮していること、識別された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。
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。実施したテスト結果とテスト概要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、開発者がまだ扱っていない脆弱性の可能性を検査している。
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く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。実施したテスト結果とテストの概要について報告がなされている。
AVA_VLA.2.5E	評価はワークユニットに沿って行われ、意図する環境においてTOEが低い攻撃力に対抗できることを侵入テストと脆弱性分析の結果から検査し、悪用され得る脆弱性及び残存脆弱性が存在しないことが報告されている。

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。

DDL	データ定義文。データベースの作成、削除等に使用するSQL文。
DML	データ操作文。データベースの参照、追加、削除及び更新に使用するSQL文。
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。
RDB	Relational Databaseの省略形。リレーショナルデータベースに同じ。
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。
RDBディレクトリファイル	データベースをアクセスするための基本情報や、各種の運用情報を記録するファイル。
SQL	国際標準のリレーショナルデータベース操作言語であり、データベースの構造を定義するDDL(Data Definition Language)とデータベースへのデータの入力、登録、更新、変更、削除、検索などの操作を行うDML(Data Manipulation Language)より構成される。

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。
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	日常の管理者及び利用者の監視や、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	作業用テーブル及び作業用ソート領域を指す。
シーケンス	一意性のある番号を順番に取得する機能 例） １から順に値を取得するシーケンスを事前に定義する 順序 ： １から順番に昇順に値を採番 以下のＳＱＬ文を繰り返し実行すると、表の列に １から順番に値が入る。 INSERT INTO 表 VALUES 列 = 順序.NEXTVAL;
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。

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。
ファイル	本書では、ファイルシステム上のファイルとローデバイスの両方を指す。
ファンクション	ＳＱＬ記述性を高めるために、複雑な演算処理をあらかじめデータベースに登録する機能である。 例） 二つの値の平均をとるファンクションを事前に定義

HEIKIN ： 復帰値 = （入力１ ＋ 入力２）/ ２

以下のＳＱＬ文で結果表を参照すると、二つのカラム結果１と結果２の平均が取得できる。

SELECT HEIKIN(結果1,結果2) FROM 結果表;

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。
プロトコル	データ通信を行うため、あらかじめ定めておく規約。信号送信の手順、データの表現法、誤り検出法などを定める。通信規約。
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	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及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。

6 参照

[1] Symfoware セキュリティターゲット バージョン 3.2（2007年12月26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] Symfoware Server Enterprise Extended Edition 9.0.1 評価報告書 第1.3版 2008年1月18日　有限責任中間法人 ITセキュリティセンター