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18年11月6日** (IT**認証**6112)
認証番号	C0131
認証申請者	**富士通株式会社**
TOE**の名称**	Interstage Application Server Enterprise Edition
TOE**のバージョン**	8.0.3（Linux 32bit） **修正プログラム**T000632LP-02、T000181LP-01、T000682LP-01**を適用**
PP**適合**	**なし**
適合する保証パッケージ	EAL2+ AVA_MSU.1
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11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。

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

「Interstage Application Server Enterprise Edition 8.0.3（Linux 32bit）、修正プログラムT000632LP-02、T000181LP-01、T000682LP-01を適用」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、「Interstage Application Server Enterprise Edition 8.0.3（Linux 32bit)、修正プログラムT000632LP-02、T000181LP-01、T000682LP-01を適用」（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：	Interstage Application Server Enterprise Edition
バージョン：	8.0.3（Linux 32bit） 修正プログラムT000632LP-02、T000181LP-01、T000682LP-01を適用
開発者：	富士通株式会社

1.2.2 製品概要

本TOEはアプリケーションサーバプログラムであり、アプリケーションを動作させるために必要な環境の構築から運用、監視、保守に至る運用管理や、業界標準・オープンソースに対応したアプリケーションの実行環境を提供する製品である。

本TOEは、セキュリティ機能として、アプリケーションの実行状態を維持するための機能と、アプリケーションの実行環境の管理を正当な者に制限するための機能を提供する。

1.2.3 TOEの範囲と動作概要

1.2.3.1 TOEの物理範囲

TOEは、ソフトウェア製品「Interstage Application Server Enterprise Edition 8.0.3」のLinux 32bit版に修正プログラムT000632LP-02、T000181LP-01、T000682LP-01を適用したものと同一である。

1.2.3.2 TOEの設定に関する注意事項

TOEの利用環境として、Interstage管理コンソールへのログイン時の識別認証処理を、TOEが動作するアプリケーションサーバのOSと連動して実施する「OS認証」か、認証サーバと連動して実施する「ディレクトリサービス認証」のいずれかを選択できる。

本案件の評価は、デフォルト設定である「OS認証」が選択される想定で実施された。

1.2.3.3 TOEの関係者

TOEは、以下の役割を認識する。

- Administrators

  TOE全体の運用管理に責任を持つ役割である。

- Configurators

  アプリケーション全体の運用管理に責任を持つ役割である。

1.2.3.4 TOEの動作概要

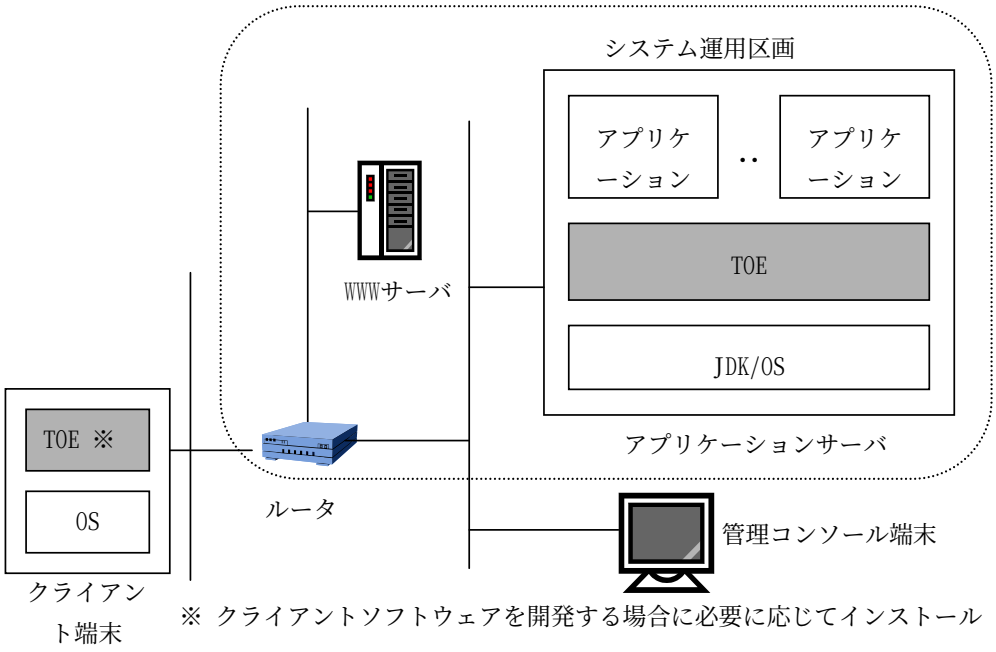

図1-1　TOEの動作環境

TOEは、図1-1の環境で動作する。なお、アプリケーションサーバ上のTOEとクライアント端末上のTOEは、TOEの異なる部分である。

アプリケーションサーバ上のTOEは、アプリケーションに対して動作環境(ワークユニット(*1)と呼ぶ)を提供する。

アプリケーションサーバ上のTOEはワークユニット(*1)を定義する機能を提供し、この機能は管理コンソール端末から使用されることを想定する。

クライアント端末上のTOE(クライアントパッケージと呼ぶ)は、アプリケーションサーバ上のアプリケーションを使用するためのクライアントアプリケーションに対して、開発環境やランタイムを提供する。

1.2.4 TOEの機能

TOEは以下の機能を持つ。

- アプリケーション実行ライブラリ

  アプリケーションサーバ上のTOEは、様々な環境で開発されたアプリケーションを動作させるための動作環境を実現する実行ライブラリであり、TOE上でユーザアプリケーションを動作させるための基盤として提供される。

  この機能は、アプリケーションから使用される。

- ワークユニット(*1)定義に従ったアプリケーションの実行

  アプリケーションサーバ上のTOEは、ワークユニット(*1)定義に従ってアプリケーションの実行環境を作成し、アプリケーションを動作させる。

  この機能は、自動起動等のワークユニット(*1)定義に従って必要なタイミングで動作する。

- Interstage管理コンソール

  アプリケーションサーバ上のTOEが提供するサービスに対する操作ビューを統合し、一元的な操作ビューを提供している管理機能。アプリケーション動作の維持のため、サービスやシステム、ワークユニット(*1)定義を管理することができるTOEの基本機能として提供される。

  この機能は、Administrators及びConfiguratorsに対して以下の操作を提供する。

  - アプリケーション実行環境の参照・変更
  - 環境定義ファイルの参照・変更 (ただし、変更はAdministratorsに限られる)

  この機能は、Webインタフェースにより提供され、管理コンソール端末から使用されることを想定する。

- クライアントパッケージ

  アプリケーションサーバ上のアプリケーションを使用するためのクライアントアプリケーションに対して、開発環境やランタイムを提供する。

  この機能は、クライアントアプリケーションから使用されることを想定する。

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「Interstage Application Server Enterprise Edition 8.0.3（Linux 32bit） Security Target」（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、「富士通株式会社 Interstage Application Server Enterprise Edition 8.0.3（Linux 32bit） 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、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問題は発見されなかった。評価は、平成19年11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、EAL2追加である。

追加の保証コンポーネントはAVA_MSU.1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、高度な専門知識を持たない低レベルの攻撃者に対抗することが意図されているため、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。

- ユーザ認証の保護

  アプリケーションサーバ上のTOEは、管理コンソール端末からアクセスされると、アプリケーションサーバのOSに識別・認証を依頼する。その際、管理コンソール端末へのフィードバックに認証情報が含まれないように保護する。

- SSL暗号通信機能

  Interstage管理コンソールを使用したTOEへのアクセス時、アプリケーションサーバ上のTOEは、以下の暗号鍵を利用して、管理コンソール端末とInterstage管理コンソール間の暗号化された通信路を確保する。

  - サーバ・ライト鍵　　：TOEが管理コンソール端末へ送信する通信データの暗号化操作に利用する。
  - クライアント・ライト鍵：TOEが管理コンソール端末から受信する通信データの復号操作に利用する。

- セションタイムアウト機能

  Interstage管理コンソールを使用したTOEの運用管理時、アプリケーションサーバ上のTOEは、一定の無操作時間が経過した際に、Interstage管理コンソールと管理コンソール端末の間のセションを破棄する。

- ロール制御機能

  Interstage管理コンソールを使用したTOEの運用管理時、アプリケーションサーバ上のTOEは、サービスやシステム設定に関する環境定義ファイルへの操作の実行可否を操作者のロールによって判断し、制御する。

  操作者のロールにはAdministratorsとConfiguratorsがあり、実行の可否は以下のように判断される。

  - 環境定義ファイルの変更はAdministratorsのみに許可される。
  - それ以外(ワークユニット(*1)定義の参照・変更、環境定義ファイルの参照)はロールの制限はない(AdministratorsとConfigurators両方に許可される)。

- アプリケーション自動再起動機能

アプリケーションサーバ上のTOEは、停止操作以外によって終了したアプリケーションを異常終了と見なし、警告メッセージをTOEが動作するアプリケーションサーバのOSへ通知し、当該アプリケーションの実行プロセスを再起動する。アプリケーション動作の維持のため、動作障害状態からの早期復帰を担う。

アプリケーションに対して本機能を適用するかどうか、自動再起動の回数の制限をどうするかは、利用者がワークユニット(*1)定義によりワークユニット(*1)ごとに指定することができる。

- サーバアプリケーションタイマ機能

アプリケーションサーバ上のTOEは、一定の応答時間内に応答しなかったアプリケーションを処理遅延と見なし、警告メッセージをTOEが動作するアプリケーションサーバのOSへ通知し、当該アプリケーションを強制的に停止させる。アプリケーション自動再起動機能を利用することで、強制停止したアプリケーションを再起動することができる。

アプリケーションに対して本機能を適用するかどうか、処理遅延とみなす応答時間をどうするかは、利用者がワークユニット(*1)定義によりワークユニット(*1)ごとに指定することができる。

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.ILLEGAL_ACCESS	（不正なログイン） 攻撃者が、管理コンソール端末もしくは、クライアント端末を利用してInterstage管理コンソールへ不正にアクセスし、アプリケーション実行環境や環境定義ファイルの設定変更を行い、TOEや動作しているアプリケーションの停止や設定変更を試みる。

識別子	脅　威
T.SPOOFING	（なりすまし） Interstage管理コンソールへの不正なログインを防ぐために識別認証の対策を実施した際にその二次脅威として、攻撃者が、操作者がログイン状態のまま離席した管理コンソール端末を使用して、Interstage管理コンソールに無断にアクセスし、アプリケーション実行環境や環境定義ファイルの設定変更を行い、TOEや動作しているアプリケーションの停止や設定変更を試みる。
T.DISCLOSE_DATA	（管理コンソール端末－Interstage管理コンソール間のデータ暴露） Interstage管理コンソールへの不正なログインを防ぐために識別認証の対策を実施した際にその二次脅威として、攻撃者が、管理コンソール端末とInterstage管理コンソール間のネットワーク上で送受信される通信データを盗聴し、識別認証情報を入手する。入手した識別認証情報を使用して、操作者としてInterstage管理コンソールを使用してアプリケーション実行環境や環境定義ファイルの設定変更を行い、TOEや動作しているアプリケーションの停止や設定変更を試みる。
T.ARROGATION	（越権行為） Administratorsのロールを持たない者が、管理コンソール端末を利用して、Interstage管理コンソールへアクセスし、サービスやシステム設定に関する環境定義ファイルの設定変更を行い、TOEや動作しているサービス、またはシステムの停止、設定変更を試みる。
T.APPLICATION_TROUBLE	（アプリケーション動作障害） TOE上で動作するアプリケーションが停止操作以外の原因によって異常終了する、もしくは、アプリケーション処理遅延のためレスポンスが遅延することによって、利用者が設定したアプリケーション動作を維持できなくなる。

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

TOEは図1-1の環境で動作し、以下の表1-2に示すソフトウェアと、これらのソフトウェアが動作するハードウェアを要する。

表1-2　TOEの運用に必要なソフトウェア

ソフトウェア	備考
Linux OS	TOEが動作するアプリケーションサーバのオペレーティングシステム。Red Hat Enterprise Linux AS（v.4 for x86）に対応している。 Interstage管理コンソールの利用の際に、TOEと連動してアクセス者の識別認証を行う。
ブラウザ	管理コンソール端末から TOE上のアプリケーション動作を管理するために利用する。次のブラウザに対応している。 Microsoft Internet Explorer 5.0.1 / 5.5 / 6.0 / 7.0 Netscape Communicator 6.1x / 6.2x / 7.1x ただし、128ビット以上の暗号への対応を必須とする。
Windows OS	クライアント端末に、TOEのクライアントパッケージを導入する場合に必要となるオペレーティングシステム。 Windows Vista Home Basic / Home Premium / Ultimate / Business / Enterprise、Windows XP Pro / Home、Windows 2000 Proに対応している。
JDK	Java Development Kit。Java言語によるプログラミングを行うための開発環境やJavaプログラム実行環境が含まれる。JDK1.4がTOEに同梱される形で提供され、TOEのインストール時に導入される。

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.TRUST	Administratorsは、ロールに課せられた職務に関して責任を持ち、不正な行為を行わないものとする。
A.PHYSICAL_ACCESS	TOEが動作するアプリケーションサーバは、信頼出来ない者の立入りが禁止されたシステム運用区画へ設置されるものとする。
A.SERVICE	TOEが動作するアプリケーションサーバでは、OSへのリモートログインサービスは提供せず、保守時を除いてコマンド実行によるCUIベースの運用を行わないものとする。

A.APPLICATION	TOE上で動作するアプリケーションは信頼できるものとする。

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。

- Interstage Application Server インストールガイド －Linux－ 第2版
  文書番号: J2UZ-8250-02Z2(B)
- ソフトウェア説明書 Interstage Application Server Enterprise Edition 8.0.3 (Linux)
  文書番号: B5151G-0803-1
- Interstage Application Server 運用ガイド 第4版
  文書番号:B1WN-6981-04Z2(01)
- Interstage Application Serverセキュリティシステム運用ガイド 第4版
  文書番号:B1WN-7041-04Z2(00)
- Interstage Application Server OLTPサーバ運用ガイド 第2版
  文書番号:B1WN-6991-02Z2(01)
- Interstage Application Serverメッセージ集 第7版
  文書番号:B1WN-7181-07Z2(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(*2)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11月に始まり、平成19年11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4月及び7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・配付と運用の各ワークユニット(*2)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4月及び7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。

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と図2-2に示す。

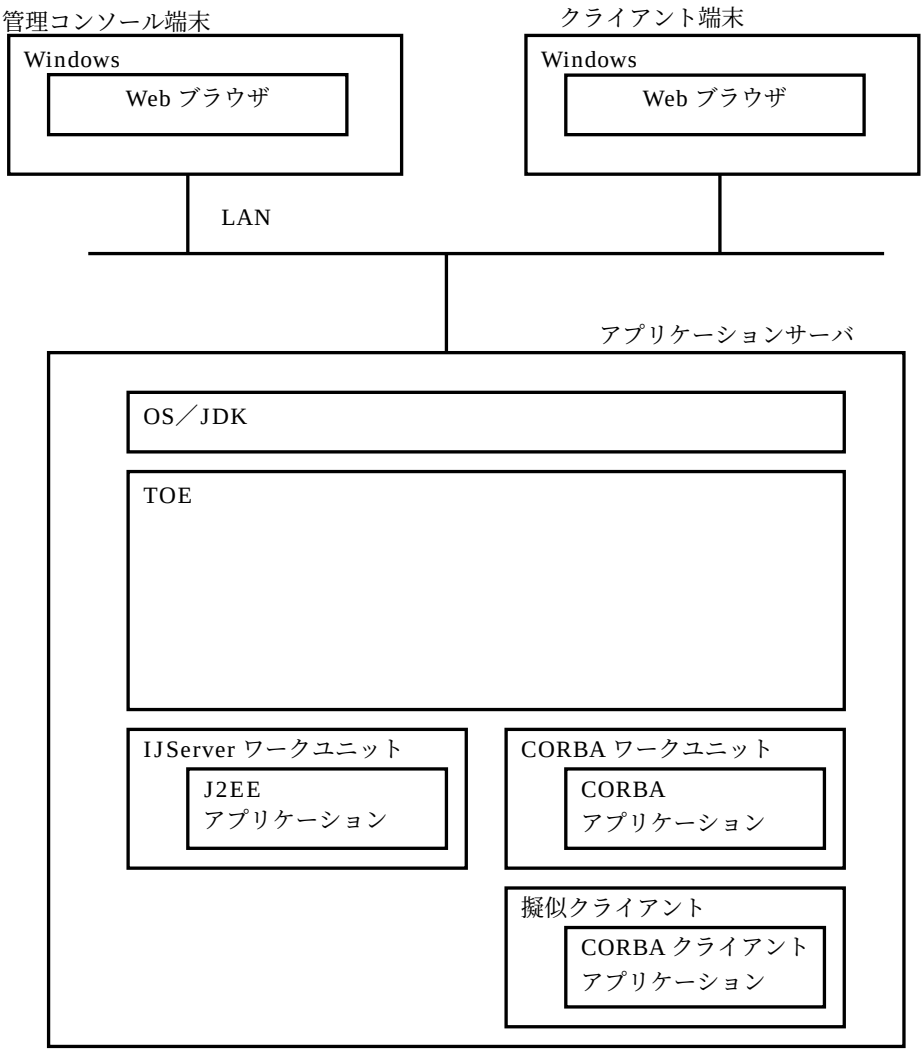

図2-1 開発者テストの構成図(1)

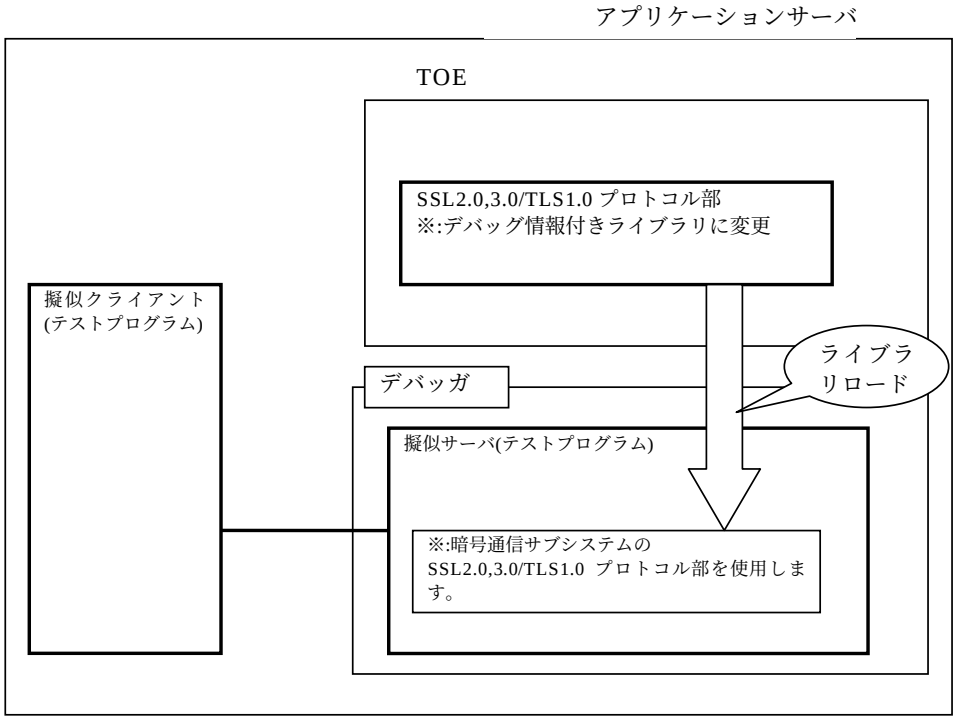

図2-2 開発者テストの構成図(2)

図2-1と図2-2の構成において使用された構成要素は以下のとおりである。

a)マシンの詳細

構成	プラットフォームOS/JDK	
クライアント端末／管理コンソール端末	Windows 2000 Pro Windows XP Pro Windows Vista Home Pre./ Business	
サーバ	JDK	JDK 1.4.2_14
	OS	RedHat Enterprise Linux AS(v.4 for x86)

注）各OSには、以下のパッチが適用されている。

Red Hat Enterprise Linux AS (v.4 for x86)：U05111、SU00093

b)テスト資材

・Webブラウザ：IE 6.0/7.0、Netscape 7.1を使用

・デバッガ：

GNU Source-Level Debugger

・擬似サーバ：

該当テスト用に独自に作成したサーバ用プログラム

・擬似クライアント

該当テスト用に独自に作成したクライアント用プログラム

・デバッグ情報付きライブラリ（SSL2.0,3.0/TLS1.0プロトコル部）
デバッガ上で通信鍵の生成を確認するためにデバッグ情報付きのライブラリを使用する必要があるため、TOEのSSL2.0,3.0/TLS1.0プロトコル部のライブラリをデバッグ情報付きのライブラリに置き換える。

・[CORBAアプリケーション]
- クライアントアプリケーション：テスト用に用意
- サーバアプリケーション：テスト用に用意

・[J2EEアプリケーション]
- サーバアプリケーション：テスト用に用意

- IJServerプロセス強制終了のアプリケーション：テスト用に用意
- サーバアプリケーション：テスト用に用意
- IJServerプロセス強制終了のアプリケーション：テスト用に用意

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、図2-2に示す。開発者テストはSTにおいて識別されている構成と一貫した環境で実施されたことが、評価者による各構成の調査により確認された。

b.テスト手法

テストには、以下の手法が使用された。

①外部インタフェースからセキュリティ機能に刺激(パラメータ)を与え、外部インタフェースでセキュリティ機能のふるまいを目視確認する。

②SSL暗号通信機能における「通信鍵の生成」に関しては、①のテスト手法では確認できないので、デバッガを使用した手法を採用している。デバッガを使用した手法とは、テストマシン上で擬似サーバ及び擬似クライアント用のプログラムを起動し、デバッガ上で、擬似クライアントから擬似サーバへ接続したときの動作を確認する手法である。

c.実施テストの範囲

テストは開発者によって101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。

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(サンプリングテスト)

評価者によるサンプリングテストは、開発者テストと同様の構成(図2-1と図2-2に示す)で実施された。

評価者によるサンプリングテストの構成において使用された構成要素は以下のとおりである。

a)マシンの詳細

構成	プラットフォームOS/JDK	
クライアント端末／管理コンソール端末	Windows 2000 Pro Windows XP Pro Windows Vista Home Pre./ Business	
サーバ	JDK	JDK 1.4.2_14
	OS	RedHat Enterprise Linux AS(v.4 for x64)

注）各OSには、以下のパッチが適用されている。

Red Hat Enterprise Linux AS (v.4 for x86)：U05111、SU00093

b)テスト資材

・Webブラウザ：

管理コンソール端末にIE 6.0/7.0、Netscape 7.1を使用

クライアント端末にIE 6.0/7.0を使用

これ以外のテスト資材は開発者テストと同じである。

2) 評価者テスト環境(独立テスト)

評価者による独立テストは、図2-2に示される開発者テストと同様の構成及び同様の構成要素で実施された。

それに加え、以下の図2-3の構成で実施された。

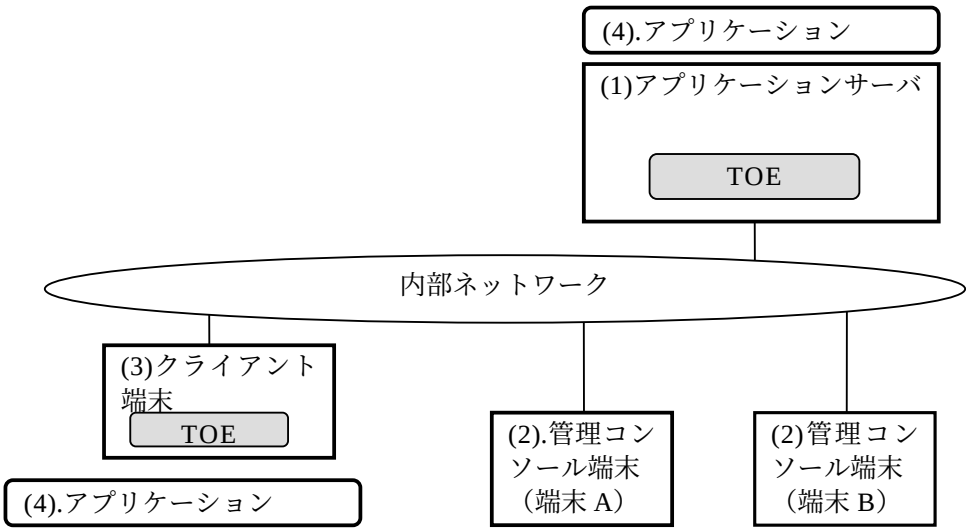

図2-3 独立テストの構成図

図2-3の構成における構成要素は以下のとおりである。

No	名称	要件	備考
(1)	アプリケーションサーバ	TOE である Interstage Application Server Enterprise Editionが稼動するサーバ (CPU)1.6GHz(メモリ)4Gbyte (OS) RedHat Enterprise Linux AS (v.4 for x86) OSパッチ：U05111、SU00093 (JDK) JDK 1.4.2_14 TOEは、以下の製品をインストールする。（ただし、1回目の評価者テストでは、TOEのバージョンは、「8.0.0」である。) (TOE) Interstage Application Server Enterprise Edition 8.0.3	TOE 搭載
(2)	管理コンソール端末	管理コンソール端末として以下の端末を複数台用意する。 (OS) Windows XP SP2、 Windows 2000 Pro(IE 5.01の時に使用)、 Windows Vista Business（または Vista Home premium） (ブラウザ) Internet Explorer 5.01、6.0、7.0 Netscape 7.1	－
(3)	クライアント端末	クライアント端末として以下の端末(管理コンソール端末と兼用可）を用意する。 (OS) Windows XP SP2 Windows Vista Business（または Vista Home premium） (ブラウザ) Internet Explorer 6.0、7.0 (SW)TOEの一部であるクライアントパッケージ （アプリケーションの動作に必要）	TOE の一部
(4)	アプリケーション	テスト用に以下のアプリケーションを用意する。 ・J2EEアプリケーション ・CORBAアプリケーション ・EJBアプリケーション	－

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図2-1、図2-2、図2-3に示す。評価者テストはSTにおいて識別されている構成と一貫した環境で実施されたことが、評価者による各構成の調査により確認された。

特に、一部のテストに異なるバージョンのTOEが使用されたことについては、セキュリティ機能の動作に関係する部分の実装表現が本TOEと同一であるために、異なるバージョンのTOEに対するテスト結果が本TOEのテスト結果として使用可能であることが確認された。

b.テスト手法

テストには、開発者テストと同じ手法が使用された。

c.実施テストの範囲

評価者が独自に考案したテストを13項目、開発者テストのサンプリングによるテストを29項目、計42項目のテストを実施した。テスト項目の選択基準として、CEM 2:ATE_IND.2-4と2:ATE_IND.2-9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 すべてのセキュリティ機能に対して独立テストを考案する。アプリケーションサーバ特有の重要な機能、機能強度に関係する機能を含むように注意する。
② 動作環境、及びTSFIのパラメタの網羅性を高めるための独立テストを考案する。
③ セキュリティ機能のテストの厳密さを高めるための独立テストを考案する。
④ 複数のセキュリティ機能が関連して動作する場合について、独立テストを考案する。
⑤ 異なるインタフェースからの利用をすべて含むように独立テストを考案する。
⑥ すべてのセキュリティ機能の正常系と異常系を含み、かつ目安となる開発者テストの20%を超えるようにサンプリングする。

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(*2)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 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(*2)が評価報告書で示されたように評価されていること。
② 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。
③ 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問題は発見されなかった。

4 結論

4.1 認証結果

提出された評価報告書、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EAL2及び保証コンポーネントAVA_MSU.1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(*2)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(*2)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(*2)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(*2)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(*2)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(*2)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(*2)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(*2)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(*2)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(*2)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(*2)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(*2)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(*2)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(*2)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(*2)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(*2)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(*2)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(*2)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.2.1E	評価はワークユニット(*2)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_DEL.1.1E	評価はワークユニット(*2)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.1.2D	評価はワークユニット(*2)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(*2)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(*2)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(*2)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(*2)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.1.1E	評価はワークユニット(*2)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.1.2E	評価はワークユニット(*2)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_RCR.1.1E	評価はワークユニット(*2)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。
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(*2)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(*2)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_COV.1.1E	評価はワークユニット(*2)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に対応していることを確認している。
ATE_FUN.1.1E	評価はワークユニット(*2)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(*2)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(*2)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(*2)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.1.1E	評価はワークユニット(*2)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.1.2E	評価はワークユニット(*2)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.1.3E	評価はワークユニット(*2)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_SOF.1.1E	評価はワークユニット(*2)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(*2)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.1.1E	評価はワークユニット(*2)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.1.2E	評価はワークユニット(*2)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。

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
CUI	Character-based User Interface
IE	Internet Explorer
OS	Operating System

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	TOEで実行されるプロセスであり、1つの実行単位。アプリケーションには、1つ以上の業務ロジックを含むことができる。特に、TOEを導入する組織が作成した業務ロジックを含むアプリケーションを、ユーザアプリケーションと呼ぶ。
システム運用区画	入退室管理により物理的に保護された区画。
利用者	TOEを導入する組織の者であり、アプリケーションの運用管理を行う者。
環境定義ファイル	個々のユーザ環境において、アプリケーション実行環境をどのようなシステム環境で利用するか規定する設定ファイル。システム環境の設定変更は、TOE上で動作する全てのアプリケーションに影響する。

ワークユニット(*1)	アプリケーションが実行される実行環境の枠組。複数のアプリケーションを１つの業務として操作可能とするTOE独自の管理に利用する。運用に必要な情報や業務ロジックを登録することで、ワークユニット(*1)に設定された実行環境下でアプリケーションを動作させることができる。 CEMで使用される用語「ワークユニット」と区別するため、本報告書内でこの意味で使用される箇所は「ワークユニット(*1)」とし、CEMで使用される用語として使用される箇所は「ワークユニット(*2)」とする。
ワークユニット(*2)	上記理由により、本報告書内では、「ワークユニット」がCEMにおける用語として使用される箇所は「ワークユニット(*2)」とする。
ワークユニット(*1)定義	ワークユニット(*1)に設定された実行環境の情報をワークユニット(*1)定義と呼ぶ。

6 参照

[1] Interstage Application Server Enterprise Edition 8.0.3（Linux 32bit）Security Target 第2.0版（2007年10月11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 Interstage Application Server Enterprise Edition 8.0.3（Linux 32bit）評価報告書 第3.0版 2007年11月9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