認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙 押印済

評価対象

申請受付日（受付番号）	**平成21年3月23日** (IT**認証**9250)
認証番号	C0234
認証申請者	**株式会社 日立製作所**
TOE**の名称**	uCosminexus Application Server
TOE**のバージョン**	08-00
PP**適合**	**なし**
適合する保証パッケージ	EAL2**及び追加の保証コンポーネント**ALC_FLR.1
開発者	**株式会社 日立製作所**
評価機関の名称	**みずほ情報総研株式会社　情報セキュリティ評価室**

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21年8月21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　山里　拓己

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 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 バージョン3.1 改訂第2版 (翻訳第2.0版)
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 改訂第2版　(翻訳第2.0版)

評価結果：合格

「uCosminexus Application Server」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
1.1.1 評価保証レベル 1
1.1.2 PP適合 1
1.2 評価製品 1
1.2.1 製品名称 1
1.2.2 製品概要 2
1.2.3 TOE範囲とセキュリティ機能 2
1.3 評価の実施 7
1.4 評価の認証 7
2 TOE概要 8
2.1 セキュリティ課題と前提 8
2.1.1 脅威 8
2.1.2 組織のセキュリティ方針 8
2.1.3 操作環境の前提条件 8
2.1.4 製品添付ドキュメント 9
2.1.5 構成条件 10
2.2 セキュリティ対策 11
3 評価機関による評価実施及び結果 14
3.1 評価方法 14
3.2 評価実施概要 14
3.3 製品テスト 14
3.3.1 開発者テスト 14
3.3.2 評価者独立テスト 16
3.3.3 評価者侵入テスト 17
3.4 評価結果 18
3.4.1 評価結果 18
3.4.2 評価者コメント/勧告 18
4 認証実施 19
5 結論 20
5.1 認証結果 20
5.2 注意事項 20
6 用語 21
7 参照 24

1 全体要約

1.1 はじめに

この認証報告書は、「uCosminexus Application Server」（以下「本TOE」という。）について、みずほ情報総研株式会社　情報セキュリティ評価室（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株式会社 日立製作所に報告するとともに、本TOEに関心を持つ利用者や運用者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書と共に、対応するSTを併読されたい。本TOEの動作条件や運用のための前提についての詳細、本TOEが対抗する脅威への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、及びセキュリティ仕様の概要と十分性の根拠は、STにおいて詳述されている。

本認証報告書は、J2EE 1.4 を熟知したJ2EEアプリケーションを開発/構築する開発者や運用管理者を読者と想定しており、Web(J2EE)アプリケーションの利用者は読者として想定していない。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。

1.1.1 評価保証レベル

本TOEが適合を主張する評価保証レベルは、EAL2追加である。
追加の保証コンポーネントは、ALC_FLR.1である。

1.1.2 PP適合

適合するPPはない。

1.2 評価製品

1.2.1 製品名称

本TOEは、以下の製品のセキュリティ機能である。

製品名称：　uCosminexus Application Server
バージョン：　08-00
開発者：　株式会社 日立製作所

1.2.2 製品概要

TOE は、サーバサイドJavaの規格であるJ2EE 1.4に準拠したWebアプリケーションサーバの実行・運用環境を提供するソフトウェアである。TOEを含む製品は、Webコンテナ/EJBコンテナと呼ばれる、J2EE準拠のJava アプリケーションの実行基盤を中核とし、Webサーバ、運用管理など、J2EEアプリケーションの実行及び運用に関する複数のソフトウェアで構成されている。これらの構成ソフトウェアは、業務システムの可用性、信頼性を高め、効率良く運用するためのさまざまな機能を提供する。

セキュリティ機能として、登録されたエンドユーザが、ロールに従って、許可されたJ2EEアプリケーションを利用できるための、識別・認証機能、アクセス制御機能、セキュリティ管理機能を提供する。

1.2.3 TOE範囲とセキュリティ機能

（1）TOEの運用環境

TOEを利用したシステム構成を図1-1に示す。

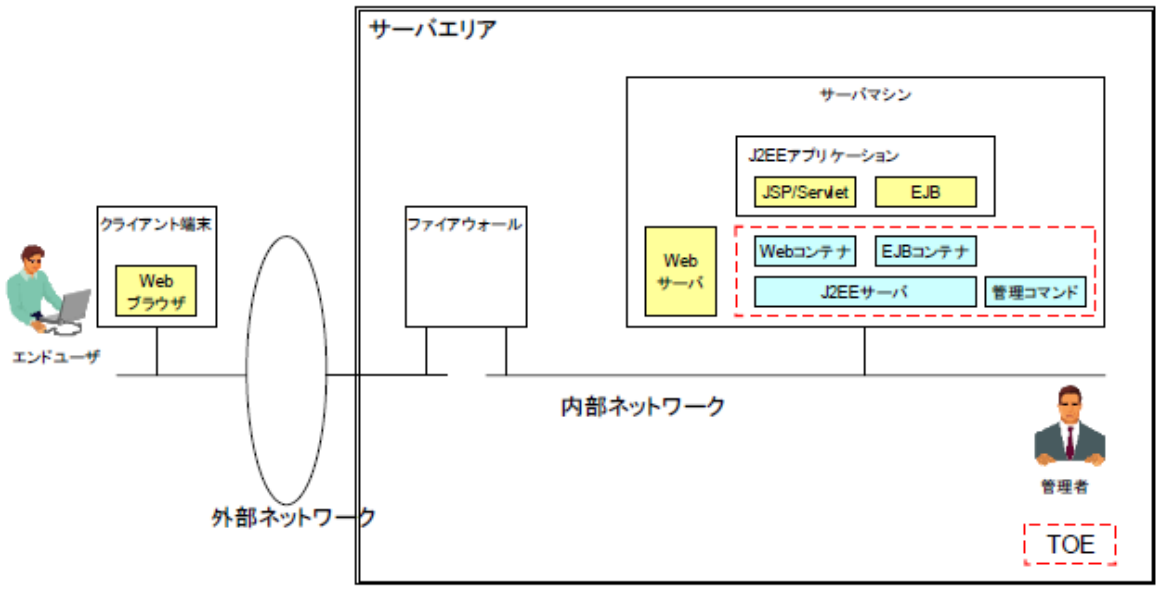

図1-1　TOEを利用したシステム構成図

以下に、システムを構成する各要素について説明する。

【クライアント端末】

エンドユーザは、クライアント端末上のWebブラウザを使用し、外部ネットワーク経由で、TOEにアクセスし、J2EEアプリケーションのサービスを利用する。クライアント端末は、TOEの範囲外である。

【サーバエリア】

以下に示す、ファイアウォール、サーバマシンは、サーバエリア内に設置され、サーバエリアを管理する管理者によって管理されている。サーバエリアは、物理的に隔離され、入退室管理されており、サーバエリアに入室できるのは、管理者のみである。

【ファイアウォール】

外部ネットワークと内部ネットワークの境界に設置される。外部ネットワークと内部ネットワークの間は、TOEを利用するために必要なプロトコルすなわち、HTTP及びHTTPSのみ通過させるように管理者によって管理されている。ファイアウォールはTOEの範囲外である。

【サーバマシン】

TOEとWebサーバが稼動するマシンである。業務を提供するJ2EEアプリケーションが稼動するために必要なWebコンテナ、EJBコンテナ、J2EEサーバが動作している。また、管理者はサーバマシン上で管理コマンドを実行し、TOEの運用を管理する。Webサーバは、エンドユーザからの要求を受付け、J2EEサーバを介してJ2EEアプリケーションに受け渡し、またJ2EEサーバ経由で受け取ったJ2EEアプリケーションからの応答をエンドユーザに返信する。サーバマシンのうち、図1-1 の破線で囲んだ範囲がTOEである。

（2）TOEの物理的範囲

TOEは表1-2に示す製品に含まれ、物理的範囲は図1-2の破線で囲まれた部分である。

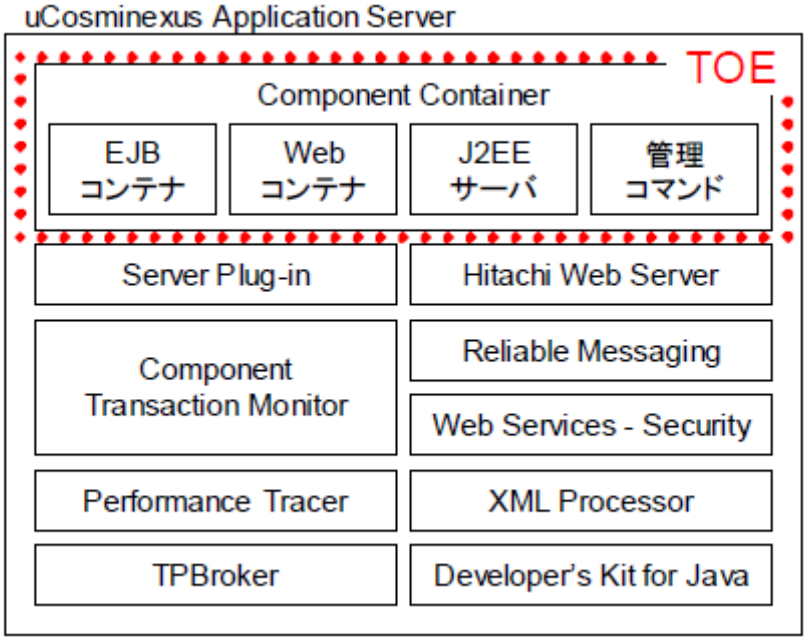

図1-2　TOEの物理的範囲

各ソフトウェアコンポーネントについて、表 1-1 を用いて説明する。

表1-1　構成するソフトウェアコンポーネント

ソフトウェアコンポーネント	概要説明
Component Container	TOEが提供するセキュリティ機能を提供するソフトウェアコンポーネント。 J2EE準拠のJavaアプリケーションの実行基盤を提供するソフトウェアコンポーネント。
Hitachi Web Server	Webブラウザからのリクエストの受信及びWebブラウザへのデータ送信を行うWebサーバ。
Developer's Kit for Java	J2SE準拠のJavaアプリケーションの開発・実行環境を提供するコンポーネント。
TPBroker	分散システムの通信制御機能などの開発・実行環境を提供するコンポーネント。
Performance Tracer	リクエストの処理トレースの出力機能を提供するコンポーネント。
Component Transaction Monitor	Component Containerへの処理リクエストの流量制御機能などを提供するコンポーネント。
XML Processor	XML形式のデータの解析機能などを提供するコンポーネント。
Web Services – Security	XML署名及びXML暗号を利用したXMLセキュリティ機能などを提供するコンポーネント
Reliable Messaging	高信頼のメッセージ管理機能やメッセージ通信機能などを提供するコンポーネント
Server Plug-in	Component Containerの運用・管理機能を提供するコンポーネント

なお、パッケージ構成は、製品のエディションによって内容が異なる。

表1-2　製品エディションによる違い

製品エディション	説明
uCosminexus Application Server Enterprise	すべてのソフトウェアコンポーネントが含まれる。
uCosminexus Application Server Standard	ソフトウェアコンポーネントのうち、Component Transaction Monitorを除くすべてのコンポーネントが含まれる。

（3）TOEの論理的範囲とセキュリティ機能

TOEの論理的範囲を図1-3に示す。破線で囲まれた部分が論理的範囲である。

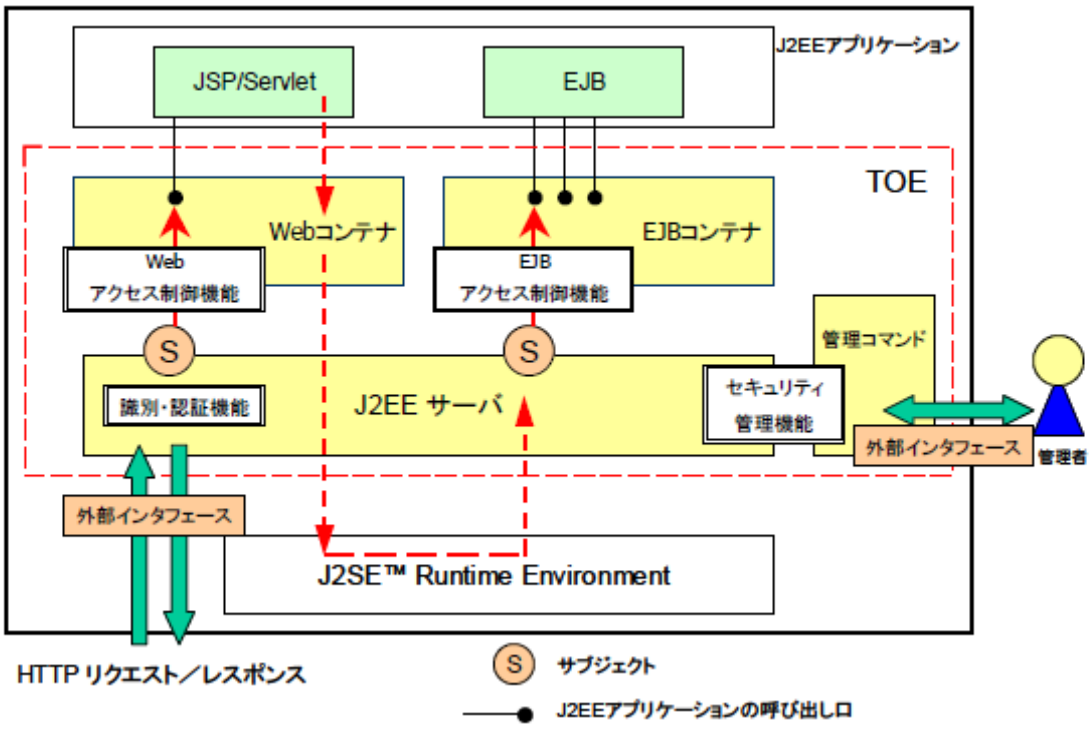

図1-3　TOEの論理的範囲

TOEは基本機能とセキュリティ機能を提供する。それぞれの機能は以下の通りである。

① 基本機能

- Webアプリケーション実行機能

  JSP/Servletで構成されるWebアプリケーションを実行する機能。Webコンテナ上で動作する。

- EJB実行機能

  業務処理プログラムを実装したEJBのメソッドを実行する機能。EJBコンテナ上で動作する。

- 性能解析情報出力機能

  リクエストがTOE内のコンポーネント間を遷移する際に、性能解析情報を記録する。TOE外である性能トレース機能を用いてトレースファイルが出力できる。

② セキュリティ機能

- 識別・認証機能

TOEは、エンドユーザから要求を受け取ると、その実行に先立ちエンドユーザに対してユーザIDとパスワードの入力を要求する。TOEはエンドユーザから渡されたユーザIDとパスワードにより認証を行なう。TOEは、認証済みのユーザ情報を、処理コンテクストに関連付ける。

- アクセス制御機能

- Webアクセス制御

Webコンテナは処理コンテクストに関連付けられた、認証済みのユーザ情報からユーザのロールを取得し、Webコンテナオブジェクト(JSP/Servlet呼び出し口または静的コンテンツの読み出し口)に関連付けられたロール情報との対応関係を検証し、アクセスが許可されている場合のみ呼び出しを行なう。

- EJBアクセス制御

EJBコンテナは処理コンテクストに関連付けられた、認証済みのユーザ情報からユーザのロールを取得し、EJBコンテナオブジェクト(EJBメソッドの呼び出し口)に関連付けられたロール情報との対応関係を検証し、アクセスが許可されている場合のみ呼び出しを行なう。

- セキュリティ管理機能

- ユーザ・ロール管理

TOEは、エンドユーザの識別・認証を行なうため、ユーザIDとパスワード、及びロールの対応関係を維持・管理する。管理者は、管理コマンドによりこの対応関係を管理することができる。

- アクセスルール管理

TOEは、管理者がJ2EEアプリケーションを登録する際に指定したロール情報を維持・管理する。管理者は、管理コマンドによりこの対応関係を管理することができる。

③ TOEによって提供されないセキュリティ機能

- TOEを管理するための管理コマンドの保護には、OSのファイルシステムの機能を利用する。

- TOEの管理者の識別・認証には、OSの識別・認証機能を利用する。

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「uCosminexus Application Server セキュリティターゲット」（以下「本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]のいずれか） 附属書A、CCパート2（[6][9]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]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、「uCosminexus Application Server 評価報告書」（以下「評価報告書」という。）[13]に示されている。なお、評価方法は、CEM（[11][12]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21年8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。

2 TOE概要

2.1 セキュリティ課題と前提

TOEが解決すべき課題と、必要とする前提を以下に示す。

2.1.1 脅威

本TOEは、表2-1に示す脅威を想定し、これに対抗する機能を備える。

表2-1 想定する脅威

識別子	脅　威
T.UNDEFINED_USERS	高度な専門知識を持たないTOEに登録されていないエンドユーザが、不正にHTTPリクエストを送信することにより、J2EEアプリケーションにアクセスするかもしれない。
T.UNAUTHORIZED_ACCESS	高度な専門知識を持たないTOEに登録されているエンドユーザが、不正にHTTPリクエストを送信することにより、アクセス権限の無いJ2EEアプリケーションにアクセスするかもしれない。

2.1.2 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を表2-2に示す。

表2-2 組織のセキュリティ方針

識別子	組織のセキュリティ方針
P.PASSWORD	管理者は、推測されにくく、十分強度のあるパスワードを設定しなければならない。

2.1.3 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2-3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2-3 TOE使用の前提条件

識別子	前提条件
A. PHYSICAL	TOEが稼動するハードウェア、ファイアウォール、及び内部ネットワークは、物理的に外部から隔離されたサーバエリアに設置され、管理者以外は入室できないように管理される。また、TOEが稼動するために不要なハードウェア及

	びソフトウェアは、サーバエリア内には持ち込まれないものとする。
A. MANAGE	TOEとTOEが稼動するために必要なサーバエリア内の各ハードウェア、ソフトウェア、内部ネットワーク及びTOEを利用して動作するJ2EEアプリケーションは、管理者によって運用・管理が行なわれるものとする。
A. PERSONNEL	管理者は、IT環境及びTOEに精通しており、またサーバエリア内のシステム全体に対して責任を持っており、信頼できるものとし、悪意のある行為は行なわない。
A. FIREWALL	TOEが稼動する内部ネットワークと、外部ネットワークの境界に、ファイアウォールが設置され、Webアプリケーションが利用するHTTP/HTTPSプロトコルのみ通過させるように設定・維持・管理されるものとする。
A. APP	TOEを利用して動作するJ2EEアプリケーションに含まれるEnterprise Beansは、Session Beanであるものとする。 注) データベースを使用するJ2EEアプリケーションは対象外である。

2.1.4 製品添付ドキュメント

本TOEに添付されるドキュメントの識別を以下に示す。

- Cosminexus アプリケーションサーバ V8概説 (3020-3-U01)
- Cosminexus アプリケーションサーバ V8 システム設計ガイド (3020-3-U03)
- Cosminexus アプリケーションサーバ V8 システム構築・運用ガイド (3020-3-U04)
- Cosminexus アプリケーションサーバ V8 アプリケーション設定操作ガイド (3020-3-U12)
- Cosminexus アプリケーションサーバ V8 リファレンス コマンド編 (3020-3-U14)
- Cosminexus アプリケーションサーバ V8 リファレンス 定義編(サーバ定義) (3020-3-U15)
- Cosminexus アプリケーションサーバ V8 リファレンス 定義編(アプリケーション/リソース定義) (3020-3-U16)
- Cosminexus アプリケーションサーバ V8 メッセージ2 KDJE-KDJW編 (3020-3-U42)

・ Cosminexus アプリケーションサーバ V8 セキュリティ構築・運用ガイド (3020-3-U99)

2.1.5 構成条件

本TOEは、Windows/Linux用のソフトウェアである。本評価は以下のハードウェア及びソフトウェア上での動作を対象とする。なお、本構成に示されるハードウェア及びソフトウェアの信頼性は本評価の範囲外である。

（1） Windowsで動作させる場合

・ ハードウェア

【機種】

・ BladeSymphony

・ HA8000シリーズ

・ 他社PC/AT互換機

【ディスク占有量】約410MB

【標準メモリ量】約1220MB

・ OS

Windows Server 2003, Standard Edition (32bit)

（2） Linuxで動作させる場合

・ ハードウェア

【機種】

・ BladeSymphony

・ HA8000シリーズ

・ 他社PC/AT互換機

【ディスク占有量】約520MB

【標準メモリ量】約2570MB

・ OS

Red Hat Enterprise Linux 5 (x86)

なお、【ディスク占有量】、【標準メモリ量】はTOEを含む製品の全てのソフトウェアコンポーネントをインストール/使用する場合に必要な最大のディスク容量/メモリ量をあらわしている。

2.2 セキュリティ対策

TOEは、具備したセキュリティ機能により以下のように2.1.1の脅威に対抗し、2.1.2の組織のセキュリティ方針を満たす。

（1）T.UNDEFINED_USERS

T.UNDEFINED_USERS(登録されていないエンドユーザのアクセス)は、登録されているエンドユーザを識別・認証し、エンドユーザの識別・認証情報を管理者のみが管理できるように制御することで対抗する。機能概要を以下に示す。

① 識別・認証機能(SF.I&A)

エンドユーザからWebコンテナ上のJ2EEアプリケーションにアクセスが要求されると、Webコンテナオブジェクトのアクセス制御情報を取得する。認証方式は、Basic認証またはForm認証から選択する。Webコンテナオブジェクトのアクセス制御情報は、アクセスルール管理機能(SF.RULE_MNG)で管理され、維持されている。

決定した認証方式をエンドユーザに返信すると、認証方式に応じてエンドユーザのWebブラウザ上にユーザID･パスワードの入力画面が表示され、エンドユーザは、ユーザID・パスワードを入力する。なお、Webブラウザ上の機能は、TOE の範囲外である。

エンドユーザが入力したユーザID・パスワードに対して、登録されたユーザID・パスワードにより識別・認証を行ない、識別・認証に成功した場合、認証済みのサブジェクト、すなわちWebコンテナサブジェクトインスタンスを生成する。識別・認証に使用するユーザID･パスワードは、ユーザ･ロール管理機能(SF.USER_MNG)で管理され、維持されている。

Webコンテナサブジェクトインスタンスにユーザ ID及びユーザIDに対応付けられたロールを関連付ける。ユーザIDとユーザIDに対応付けられたロールの関連付けは、ユーザ・ロール管理機能(SF.USER_MNG)で管理され、維持されている。

識別・認証に失敗した場合、エンドユーザにエラーを返信する。

② ユーザ・ロール管理機能(SF.USER_MNG)

以下のデータを管理する機能を管理コマンドとして提供する。

- ユーザIDの登録・削除・問い合わせ

- パスワードの登録・削除
- ユーザIDに対応付けられたロールの登録・削除・問い合わせ

（2）T.UNAUTHORIZED_ACCESS

T.UNAUTHORIZED_ACCESS(登録されている権限の無いエンドユーザのアクセス)は、登録されている権限の無いエンドユーザからJ2EEアプリケーションへのアクセスを保護するためにアクセス制御を行い、アクセス制御に用いるセキュリティ属性情報を管理者のみが管理できるように制御することで対抗する。機能概要を以下に示す。

① Webアクセス制御機能(SF.WEB_ACC)

Webコンテナオブジェクトに設定されているアクセス制御ルール及びWebコンテナオブジェクトに対応したロールを利用してアクセス制御を行なう。

Webコンテナサブジェクトインスタンスに設定されている、ユーザIDに対応付けられたロールが、Web コンテナオブジェクトに設定されている、Webコンテナオブジェクトに対応付けられたロールに関連付けられている場合のみアクセスを許可する。また、Webコンテナオブジェクトに対するアクセス制御ルールが存在しない場合は、アクセスを許可する。アクセスが許可されなかった場合、エンドユーザにその旨を通知する。

ユーザIDに対応付けられたロールとWebコンテナオブジェクトに対応付けられたロールの関連付けは、アクセスルール管理機能(SF.RULE_MNG)により設定される。

② EJBアクセス制御機能(SF.EJB_ACC)

Webコンテナ上で動作するJSP/Servletは、処理の実行中に必要に応じてEJBコンテナ上で動作するEJBのメソッドを呼び出すことができる。JSP/ServletがWebコンテナを経由してEJBコンテナ上で動作するEJBのメソッドへアクセスする際に、Webコンテナ内でWebコンテナサブジェクトインスタンスに関連付けられた、ユーザID及びユーザIDに対応付けられたロールは、EJBコンテナへ伝播され、これらはEJBコンテナサブジェクトインスタンスに関連付けられる。

EJBコンテナオブジェクトに設定されているアクセス制御ルール及びEJBコンテナオブジェクトに対応したロールを利用してアクセス制御を行なう。

EJBコンテナサブジェクトインスタンスに設定されている、ユーザIDに対応付けられたロールが、EJBコンテナオブジェクトに設定されている、EJBコンテナオブジェクトに対応付けられたロールに関連付けられている場合のみアクセスを許可

する。また、EJBコンテナオブジェクトに対するアクセス制御ルールが存在しない場合は、アクセスを許可する。アクセスが許可されなかった場合、Webコンテナにその旨を通知する。

ユーザIDに対応付けられたロールとEJBコンテナオブジェクトに対応付けられたロールの関連付けは、アクセスルール管理機能(SF.RULE_MNG)により設定される。

③ アクセスルール管理機能(SF.RULE_MNG)

以下の設定を管理する機能を管理コマンドとして提供する。

- サブジェクトの認証方式の設定
- Webコンテナオブジェクトに対応付けられたロールの登録・削除・問い合わせ・改変
- EJBコンテナオブジェクトに対応付けられたロールの登録・削除・問い合わせ・改変
- Webコンテナオブジェクトに対するアクセス制御ルールの設定
- EJBコンテナオブジェクトに対するアクセス制御ルールの設定

3 評価機関による評価実施及び結果

3.1 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。

3.2 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21年3月に始まり、平成21年8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21年5月に製造現場へ赴き、記録及びスタッフへのヒアリングにより、配付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21年6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。

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。

3.3 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評定に基づく侵入テストを実行した。

3.3.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価した開発者テストの概要を以下に示す。

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3-1　開発者テストの構成図に示す。

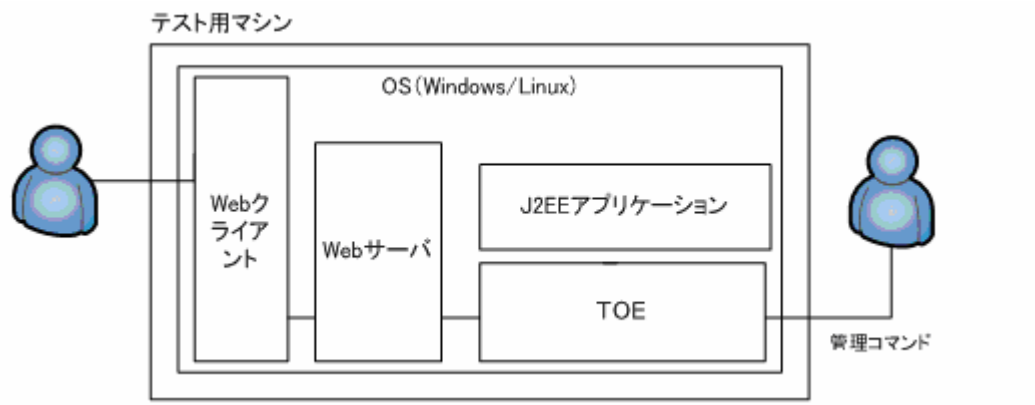

図3-1　開発者テストの構成図

表3-1　開発者テスト環境

ハードウェア	ソフトウェア
PC-AT 互換機 (CPU ： Intel Pentium4 2.80GHz メモリ：1GB)	Windows Server 2003, Standard Edition(32bit) uCosminexus Application Server Standard 08-00
PC-AT 互換機 (CPU ： Intel Pentium4 2.80GHz メモリ：1GB)	Red Hat Enterprise Linux 5 uCosminexus Application Server Standard 08-00

開発者テストは本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。

2) 開発者テスト概説

開発者の実施したテストは以下のとおり。

a. テスト概要

開発者テストで実施されたテストの概要は以下のとおり。

テスト手法としては、「Webインタフェース」に対しては、HTTPリクエストに対するレスポンスを確認し、「コンソールインタフェース」については、コンソール画面上のコマンド入力(実行)とそのレスポンスの確認を行った。

b. 実施テストの範囲

テストは開発者によって88項目(各OS 44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、TOE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。

c. 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。

3.3.2 評価者独立テスト

評価者は、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることの再確認のための独立テストを実施した。評価者が実施した独立テストの概要を以下に示す。

1) 評価者独立テスト環境

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。

評価者が実施したテストの構成を図3-1に示す。評価者テストは本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。

2) 評価者独立テスト概説

評価者の実施した独立テストは以下のとおり。

a. 独立テストの観点

評価者は、開発者テスト及び提供された評価証拠資料から、以下の観点での独立テストを考案した。

① サンプリングテスト

サンプリングの選定として、全セキュリティ機能(5個)、全TSFI(8個)、各OSでは同様のテストを実施することを条件として、WEBインタフェースを用いた識別・認証、アクセス制御に関係するテストは異常系を各1つ以上、管理系は正常系、異常系に限らず１つ以上をランダムに選定し、26項目(各OS 13項目)を抽出した。

② 評価者考案テスト

開発者テストで実施されていないパラメータや認証方法の違い、管理者機能における設定とユーザのアクセス制御を同時に行う等の組み合わせの観点で、開発者テストの厳密性、十分性を補うために、12項目(各OS 6項目)を考案した。

b. テスト概要

評価者が実施した独立テストの概要は以下のとおり。

① サンプリングテスト
開発者テストと同じ手法で、26項目を実施した。
② 評価者考案テスト
開発者テストと同じ手法で、以下の12項目(各OS 6項目)を実施した。
- BASIC認証におけるパスワード未入力のテスト
- FORM認証におけるパスワード未入力のテスト
- FORM認証時のWebアクセス制御のふるまい確認テスト
- FORM認証時のEJBアクセス制御のふるまい確認テスト
- ユーザログイン状態でユーザ削除された場合の挙動テスト
- ログイン状態でロールを変更された際の挙動テスト

c. 結果
実施したすべての評価者独立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。

3.3.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性の可能性について必要と思われる侵入テストを考案し実施した。評価者侵入テストの概要を以下に示す。

1) 評価者侵入テスト概説
評価者の実施した侵入テストは以下のとおり。

a. 懸念される脆弱性
評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。
① 認証処理において、桁数による挙動やJavaに関係した一般的なインジェクションに対する挙動が確認されていない可能性がある。
② リソース枯渇時に、利用者に提供される機能の挙動が崩れる可能性がある。(管理者機能に関しては例えば指定していない利用者が追加される可能性がある。)

b. 実施テストの範囲
評価者は、潜在的な脆弱性が悪用される可能性があるかを決定するため、以

下の侵入テストを実施した。

① 開発者テストと同じ手法を用いて、パラメータ(ユーザID、パスワード)を変更し挙動の確認を行った。

② TOEを格納したサーバのハードディスク領域を一杯にし、管理者コマンド(ユーザ追加コマンド)の挙動の確認、その後のWebインタフェースからの利用者の挙動の確認を行った。

c. 結果

実施した評価者侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

3.4 評価結果

3.4.1 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。

3.4.2 評価者コメント/勧告

消費者に喚起すべき評価者勧告はとくにない。

4 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 所見報告書でなされた指摘内容が妥当であること。
② 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、本ST及び評価報告書において、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、本認証報告書を発行した。

5 結論

5.1 認証結果

提出された評価報告書、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ALC_FLR.1に対する保証要件を満たすものと判断する。

5.2 注意事項

特にない。

6 用語

本報告書で使用されたCCに関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用されたTOEに関する略語を以下に示す。

EJB	Enterprise JavaBeans
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Security
J2EE	Java 2 Platform, Enterprise Edition
JSP	JavaServer Pages
OS	Operating System

本報告書で使用された用語の定義を以下に示す。

Basic認証	Webブラウザが持つ機能により、ユーザ名・パスワードの入力ダイアログを提示し、入力されたユーザ名・パスワードをサーバ側で照合する認証方式。
EJB	業務ロジックをプログラムとして記述したビジネスロジックをJavaコンポーネント化したもの。Sun Microsystems, Inc.から仕様が公開されている。
EJBコンテナ	EJBが動作する実行環境。
Form認証	ユーザ名・パスワードを入力するログイン用のHTMLページを提示し、入力されたユーザ名・パスワードをサーバ側で照合する認証方式。
J2EE	Webベースのアプリケーションを開発するための機能を実現するためのAPI のセット及びサーバの仕様。Sun Microsystems, Inc.から仕様が公開されている。

J2EEアプリケーション	J2EE仕様に準拠したアプリケーション。
J2EEコンテナ	J2EEアプリケーションを実行するためのサーバ基盤。J2EEアプリケーションへ各種API を提供する、Webコンテナ、EJBコンテナから構成される。
J2EEサーバ	J2EEコンテナを生成、実行する環境。
JSP	HTMLファイルに拡張タグやスクリプトを挿入することで、Webクライアントに動的なWebページを提供する機能。Servlet技術をベースとしている。
Servlet	Webサーバの機能を拡張して、動的にWebページを生成したり、Webクライアントとの対話処理を実行したりするJavaプログラム。
Webアプリケーション	Webブラウザを備えたクライアントを対象に作成されたアプリケーション。具体的には、Servlet、JSP、HTMLドキュメントなどの集合体を指す。
Webコンテナ	Webアプリケーションが動作する実行環境。
Webサーバ	Webブラウザからのリクエスト受信及びWebブラウザへのデータ送信に関連する処理を実行するプログラム。
アプリケーションサーバ	情報システムの中間に位置し、ユーザの要求(プレゼンテーション層)と業務システム(データ層)の処理を橋渡しするためのアプリケーション層を構築するためのミドルウェア。
静的コンテンツ	HTMLファイルや画像ファイルなど、エンドユーザからの要求に対する応答に使用するファイルのうち、リクエスト内容に影響されない、常に同じ内容になるコンテンツ。
製品	uCosminexus Application Server Standard または uCosminexus Application Server Enterpriseを指す。
ディスク占有量	製品に含まれる全てのソフトウェアコンポーネントをインストールするのに必要となるディスク容量をあらわしている。
標準メモリ量	製品に含まれる全てのソフトウェアコンポーネントを利用した場合に必要となるメモリ量をあらわしている。

ロール	アクセス許可に関する情報。エンドユーザに付与されるアクセス権限と、アプリケーションへのアクセス許可範囲を指定するための情報がある。

7 参照

[1] uCosminexus Application Server セキュリティターゲットVersion 2.04　2009年7月28日　株式会社 日立製作所

[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 3.1 Revision 1 September 2006 CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 2 September 2007 CCMB-2007-09-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 2 September 2007 CCMB-2007-09-003

[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3.1 改訂第1版 2006年9月 CCMB-2006-09-001　(平成19年3月翻訳第1.2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: セキュリティ機能コンポーネント バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-002　(平成20年3月翻訳第2.0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: セキュリティ保証コンポーネント バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-003　(平成20年3月翻訳第2.0版)

[11] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 2 September 2007 CCMB-2007-09-004

[12] 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3.1 改訂第2版 2007年9月 CCMB-2007-09-004 (平成20年3月翻訳第2.0版)

[13] uCosminexus Application Server 評価報告書 08004669-01-R003-02　2009年8月3日 みずほ情報総研株式会社 情報セキュリティ評価室