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8月2日（IT認証6094）**
認証番号	C0086
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	07-00
PP適合	**なし**
適合する保証要件	EAL2+ALC_FLR.1
TOE開発者	**株式会社 日立製作所**
評価機関の名称	**株式会社電子商取引安全技術研究所　評価センター**

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3月22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

「uCosminexus Application Server 07-00」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
1.1 はじめに 1
1.2 評価製品 1
1.2.1 製品名称 1
1.2.2 製品概要 1
1.2.3 TOEの範囲と動作概要 2
1.2.4 TOEの機能 5
1.3 評価の実施 6
1.4 評価の認証 6
1.5 報告概要 7
1.5.1 PP適合 7
1.5.2 EAL 7
1.5.3 セキュリティ機能強度 7
1.5.4 セキュリティ機能 7
1.5.5 脅威 9
1.5.6 組織のセキュリティ方針 9
1.5.7 構成条件 9
1.5.8 操作環境の前提条件 10
1.5.9 製品添付ドキュメント 11
2 評価機関による評価実施及び結果 12
2.1 評価方法 12
2.2 評価実施概要 12
2.3 製品テスト 12
2.3.1 開発者テスト 12
2.3.2 評価者テスト 14
2.4 評価結果 16
3 認証実施 16
4 結論 17
4.1 認証結果 17
4.2 注意事項 22
5 用語 23
6 参照 26

1 全体要約

1.1 はじめに

この認証報告書は、「uCosminexus Application Server 07-00」（以下「本TOE」という。）について株式会社電子商取引安全技術研究所 評価センター（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株式会社 日立製作所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:	uCosminexus Application Server
バージョン:	07-00
開発者:	株式会社 日立製作所

1.2.2 製品概要

本製品は、TOEであるサーバサイドJava規格（J2EE1.4）に準拠したJavaアプリケーション実行・運用環境を中核とし、Webサーバ、運用管理モジュール、性能トレースモジュール、スケジューラ等複数のソフトウェアコンポーネントで構成されたWebアプリケーションサーバである。本製品は、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し、特に登録されたエンドユーザが、その役割に従い許可されたJ2EEアプリケーションを利用するためのセキュリティ機能として、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の範囲と動作概要

(1) TOE動作環境

TOEを利用したシステム構成を図1-1に示す。

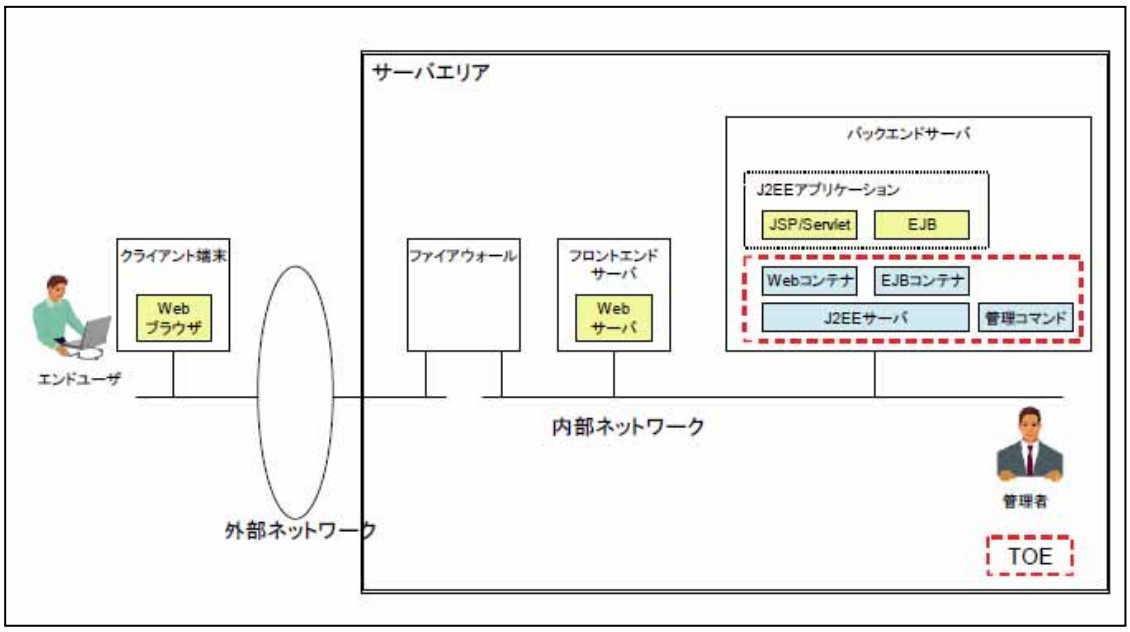

図1-1　TOEを利用したシステム構成

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、フロントエンドサーバ、バックエンドサーバは、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。

【 フロントエンドサーバ 】

Web サーバが稼動しているマシンである。エンドユーザからの要求を受付け、バックエンドサーバに受け渡し、またバックエンドサーバからの応答をエンドユーザに返信する。TOE におけるエンドユーザの識別・認証に使用するデータを送受信する際には、クライアント端末上のWeb ブラウザとフロントエンドサーバ上のWeb サーバの間で、HTTPS 通信により通信路の保護を行う。また、Web アプリケーションを利用する際にも、管理者が静的コンテンツ及びJSP/Servlet に対してHTTPS を使用するという設定を行っていた場合のみ、HTTPS通信により通信路の保護を行う。フロントエンドサーバは、TOE の範囲外である。

【 バックエンドサーバ 】
TOE 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、管理者はバックエンドサーバ上で管理コマンドを実行し、TOE の運用を管理する。バックエンドサーバのうち、図1-1 の破線で囲んだ範囲がTOE である。

(2) TOE範囲
図1-2にTOEの物理的範囲（コンポーネント構成）を示す。

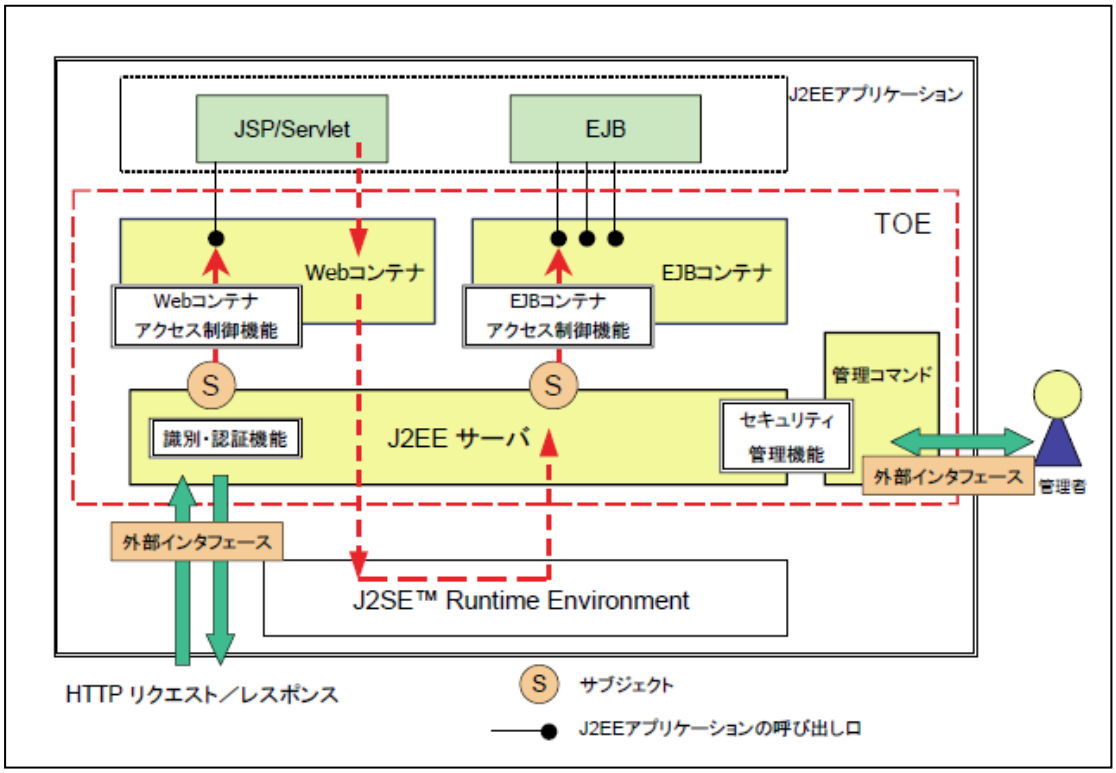

図1-2　TOEの物理的範囲（コンポーネント構成）

以下にTOEの動作概要を示す。

1) TOE は、エンドユーザのWeb ブラウザからWeb サーバ経由でHTTP リクエストを受信する。TOE は、これに対して、最初に必ずエンドユーザの識別認証を行う。識別認証が成功した後は、当該URL を閉じるまで、TOE は認証状態を維持する。

2) TOE は、認証したユーザのロール及び該当するWeb コンテナオブジェクトのセキュリティ属性に従って、ユーザを代行するサブジェクトの、Web コンテナオブジェクトであるJSP/Servlet の呼び出し口または静的コンテンツの読み出し口に対するアクセスを制御する。

3) JSP/Servlet は、Web コンテナ上で動作するが、これはTOE の範囲外である。

4) 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。この場合TOE は、JSP/Servlet の処理コンテクストを引き継ぎ、ユーザのロール及び該当するEJB コンテナオブジェクトのセキュリティ属性に従って、ユーザを代行するサブジェクトの、EJB コンテナオブジェクトであるEJB メソッドの呼び出し口に対するアクセスを制御する。

5) EJB は、EJB コンテナ上で動作するが、これはTOE の範囲外である。

6) TOE は、管理者がJ2EE アプリケーションの登録、削除、開始、終了を行うための管理機能を提供する。

また、製品を構成するTOEの範囲外のコンポーネントを表1-1に示す。

表 1-1　TOE範囲外のコンポーネント

コンポーネント	機能概要
Webサーバ	SSLをサポートしたHTTP/HTTPSリクエストの処理を行うサーバ機能を提供する。
運用管理	アプリケーションサーバを運用管理するための機能を提供する。アプリケーションサーバの一括構築やアプリケーションサーバの各機能が出力するログの収集などを行うことができる。
性能トレース	処理性能のボトルネックを解析するためのトレース情報を出力する機能を提供する。
J2SE Runtime Environment	Java2 Platform Standard Editionに準拠したJavaの仮想実行環境を提供する。
スケジューラ	クライアントからのリクエストをスケジューリングして、負荷分散や流量制御を実現する機能を提供する。

1.2.4 TOEの機能

TOEが提供する機能はWebアプリケーションサーバ実行環境としてのメイン機能、及びセキュリティ機能である。

(1) TOEメイン機能

【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である。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である。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)に対するアクセス制御

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う。

・EJBコンテナオブジェクト(EJBメソッドの呼び出し口)に対するアクセス制御

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う。

【セキュリティ管理機能】

・識別・認証情報とセキュリティ属性の管理

TOEは、エンドユーザの識別・認証を行うため、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。

・J2EEアプリケーションのセキュリティ属性の管理

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。

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「uCosminexus Application Server 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、「uCosminexus Application Server 07-00 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、EAL2追加である。

追加されるコンポーネントはALC_FLR.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、信頼できる管理者以外のアクセスが制限されたサーバエリアに設置されたサーバ上での動作を想定しており、外部ネットワークはHTTPSにより保護されていることから、攻撃者はWebブラウザを利用してTOEにアクセスする“低レベル”の攻撃エージェントと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) 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、設定される。

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・パスワードのTOEへの登録は、ユーザ・ロール管理機能（SF.USER_MNG）により設定される。

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対応付けは、ユーザ・ロール管理機能（SF.USER_MNG）により設定される。

(2) 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う。

本機能は、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。

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。

(3) EJBアクセス制御機能（SF.EJB_ACC）

本機能は、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、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うものである。

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と、EJBコンテナオブジェクトに対応付けられたロールが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。

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。

(4) ユーザ・ロール管理機能（SF.USER_MNG）

下記機能を管理コマンドとして提供し、実行できる役割を管理者に制限する。

・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

・ユーザIDとロールとの関連付け、解除

(5) アクセスルール管理機能（SF.RULE_MNG）

下記機能を管理コマンドとして提供し、実行できる役割を管理者に制限する。

・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

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.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、HTTP電文を覗き見たり、不正にHTTPリクエストを送信したりすることにより、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。

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を表1-3に示す。

表1-3 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。

1.5.7 構成条件

本TOEはソフトウェアアプリケーションであり、必要とするハードウェア構成及び

ソフトウェア構成は以下の通りである。

(1)Windows環境

ハードウェア構成	下記シリーズ中でWindows Server 2003 Standard x64 Editionが稼動する機種 BladeSymphony FLORA 700シリーズ 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 890MB
ソフトウェア構成	・ Windows Server 2003 Standard x64 Edition （本STのTOE外であり、IT環境である。） ・ uCosminexus Application Server Standard 07-00　または uCosminexus Application Server Enterprise 07-00 （本STのTOEを含む製品である。）

(2)Linux環境

ハードウェア構成	下記シリーズ中でRed Hat Enterprise Linux AS 4（AMD64 & Intel EM64T）が稼動する機種 BladeSymphony HA8000シリーズ 他社PC/AT互換機 ディスク占有量： 約 440MB 標準メモリ量： 約 1370MB
ソフトウェア構成	・ Red Hat Enterprise Linux AS 4（AMD64 & Intel EM64T） （本STのTOE外であり、IT環境である。） ・ uCosminexus Application Server Standard 07-00　または uCosminexus Application Server Enterprise 07-00 （本STのTOEを含む製品である。）

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1-4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1-4　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、フロントエ

	ンドサーバ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。

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。

- Cosminexus セキュリティ構築・運用ガイド 解説・手引・操作書
  識別子：3020-3-N37-10
  対象者：管理者、利用者
- Cosminexus リファレンスコマンド編 文法書
  識別子：3020-3-M10
  対象者：管理者
- Cosminexus メッセージ１ KDJE 編 操作書
  識別子：3020-3-M12
  対象者：管理者

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8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18年12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18年12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。

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、表2-1に示す。

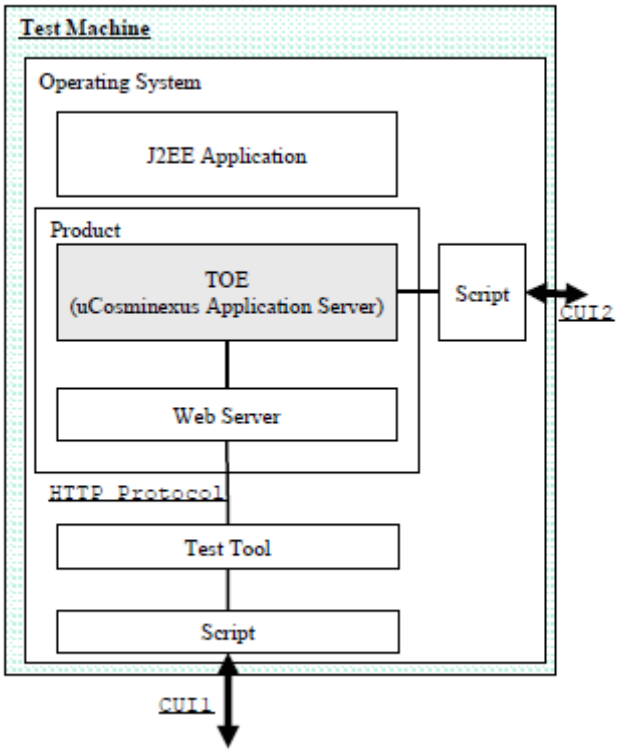

図2-1　開発者テストの構成図

表2-1　開発者テスト構成

ハードウェア	OS
HA8000 （CPU：Intel Xeon 3.60GHz×2，メモリ：4.00GB）	Windows Server 2003 Standard Edition
HA8000（CPU：Intel Xeon 3.60GHz×2，メモリ：4.00GB）	Red Hat Enterprise Linux AS 4 （ AMD64 & Intel EM64T）

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及び表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動作環境で実施された。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の構成において、クライアント環境とサーバ環境を同一マシン上に構築し、テストを実施している。これは、TOE はWeb ブラウザからWeb サーバ経由でHTTPリクエスト/レスポンスを送受信することから、TOEの外部インタ

フェースの観点で考えた場合、HTTP リクエスト/レスポンスの送受信は、特定ポートへのアクセスであると考えられ、テスト環境におけるローカルホストからのポートアクセスにより、外部マシンからのアクセスと同一環境を構築できると考えられる。

また、本テスト構成において、HTTPリクエストの送信を実現する手段として、Java で実装されたテストツール及びテストツールを任意の手順呼び出すスクリプトが使用されている。このテストツールが、Webブラウザ等で実施されるHTTPリクエストの送信と同等の処理を実施することから、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図2-1 CUI1を介したHTTPリクエスト/レスポンス送受信によるTOEセキュリティ機能のふるまいの検証

②図2-1 CUI2を介した管理コマンド呼び出しによるTOEセキュリティ機能のふるまいの検証

c.実施テストの範囲

テストは開発者によって表2-1に示した全てのプラットフォームに関して8項目（各項目には数パターンの正常系、異常系テストが含まれる）が実施されている。

テスト項目に関しては、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

評価者が実施したテストの構成を図2-2、表2-2に示す。

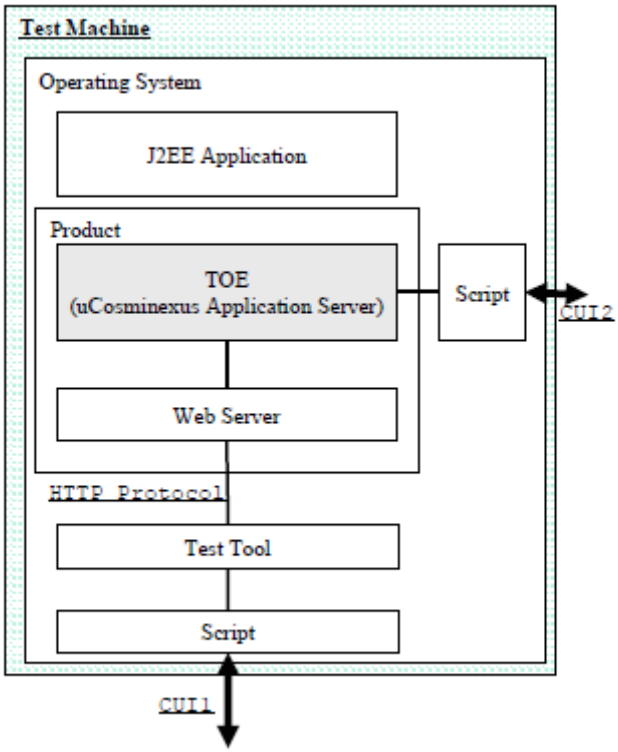

図2-2　評価者テストの構成図

表2-2　評価者テスト構成

ハードウェア	OS
HA8000 （CPU：Intel Xeon 3.60GHz×2，メモリ：4.00GB）	Windows Server 2003 Standard Edition
HA8000（CPU：Intel Xeon 3.60GHz×2，メモリ：4.00GB）	Red Hat Enterprise Linux AS 4 （ AMD64 & Intel EM64T）

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2-2、表2-2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動作環境で実施された。評価者テスト構成においても、STにおいて識別される接続構成とは一致しない部分が存在するが、開発者テスト環境（2.3.1）と同様の理由により、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図2-2 CUI1を介したHTTPリクエスト/レスポンス送受信によるTOEセキュリティ機能のふるまいの検証

②図2-2 CUI2を介した管理コマンド呼び出しによるTOEセキュリティ機能のふるまいの検証

c.実施テストの範囲

評価者が独自に考案したテストを5項目、開発者テストのサンプリングによるテストを8項目、計13項目のテストを表2-2に示した全てのプラットフォームに関して実施した。テスト項目の選択基準として、下記を考慮している。

① 開発者テストにおいて不足していると判断されたテスト内容（パラメータ設定、セキュリティ機能の組み合わせ）について項目を追加する

② 全てのプラットフォームにおける開発者テスト項目を実施する

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EAL2及び保証コンポーネントALC_FLR.1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。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.1.2E	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。
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。
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、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ADO_DEL.1.2D	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.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。
ADV_HLD.1.1E	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。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_HLD.1.2E	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_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。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。
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_FLR.1.1E	評価はワークユニットに沿って行われ、欠陥修正手続き証拠資料がすべてのセキュリティ欠陥を追跡するために使用される

	手続き、及びTOE利用者に必要な情報を提供するための手段を含み、この手続きの適用により、欠陥訂正方法の調査状況と同時に各々のセキュリティ欠陥の性質と影響に関する記述が提供され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。
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。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。
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_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、当評価に至るまでになされた所見報告書による指摘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主張が正しい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。
AVA_VLA.1.1E	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.1.2E	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。

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。

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 (Enterprise Java Beans)	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。
HTTP (Hypertext Transfer Protocol)	クライアントとサーバ間の通信に使うインターネットプロトコル。
HTTPS (Hypertext Transfer Protocol Security)	SSLを含むインターネット上で情報を暗号化して送受信するプロトコル。
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

(Java2Platform Enterprise Edition)	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 (Java Server Pages)	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。
SSL (Secure Socket Layer)	Netscape Communications社が開発した、インターネット上で情報を暗号化して送受信するプロトコル。
Web	WWW（World Wide Web）と同義。主にHTML（Hyper Text Markup Language）と呼ばれるマークアップ言語で記述されたWebページをWebサーバから読み出し、Webブラウザで閲覧する技術。
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。

6 参照

[1] uCosminexus Application Server セキュリティターゲット バージョン 1.07（2007年03月12日）(株)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17年7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17年7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17年7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] uCosminexus Application Server 評価報告書 第1.1版 2007年03月13日 株式会社電子商取引安全技術研究所 評価センター