認　証　報　告　書

評価対象

申請受付年月日(受付番号)	**平成16年1月19日（IT認証4022）：当初の申請を取り下げし、CCRA認証マーク対応のため、再申請があった申請受付日** **平成15年1月20日（IT認証3006）：当初の申請受付日**
認証番号	C0025
認証申請者	**株式会社 日立製作所**
TOEの名称	**アプリポーター** Security Kit
TOEのバージョン	01-00
PP適合	**なし**
適合する保証要件	EAL2
TOE開発者	**株式会社 日立製作所**
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17年4月27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 Common Criteria for Information Technology Security Evaluation Version 2.1
② Common Methodology for Information Technology Security Evaluation Version 1.0
③ CCIMB Interpretations-0210

評価結果：合格

「アプリポーター Security Kit バージョン 01-00」は、独立行政法人 情報処理推進機構が定める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、「アプリポーター Security Kit バージョン 01-00」（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:	アプリポーター Security Kit
バージョン:	01-00
開発者:	株式会社　日立製作所

1.2.2 製品概要

「アプリポーター」は、一般利用者に対して、電子証明書を利用した電子文書の認証と完全性保証を付加した電子申請サービスを提供する機能を備えた、電子申請／窓口の構築に必要とされる基盤ソフトウェアである。本製品「アプリポーター Security Kit」は、「アプリポーター」を構成するモジュールの中で、セキュリティ機能を提供する以下のライブラリ／ユーティリティの機能モジュールから構成される。

・セッション管理サービス
・レシート管理サービス
・配信サービス
・アプリケーション動作支援サービス(ログ管理)
・セッション管理サービス運用管理
・レシート管理サービス運用管理

・配信サービス運用管理

1.2.3 TOEの範囲と動作概要

(1) TOEを適用したシステムの概要

TOEを適用したシステムの構成図を以下に示す。この図において、TOEは、運用環境に設置された受付サーバ内にある。

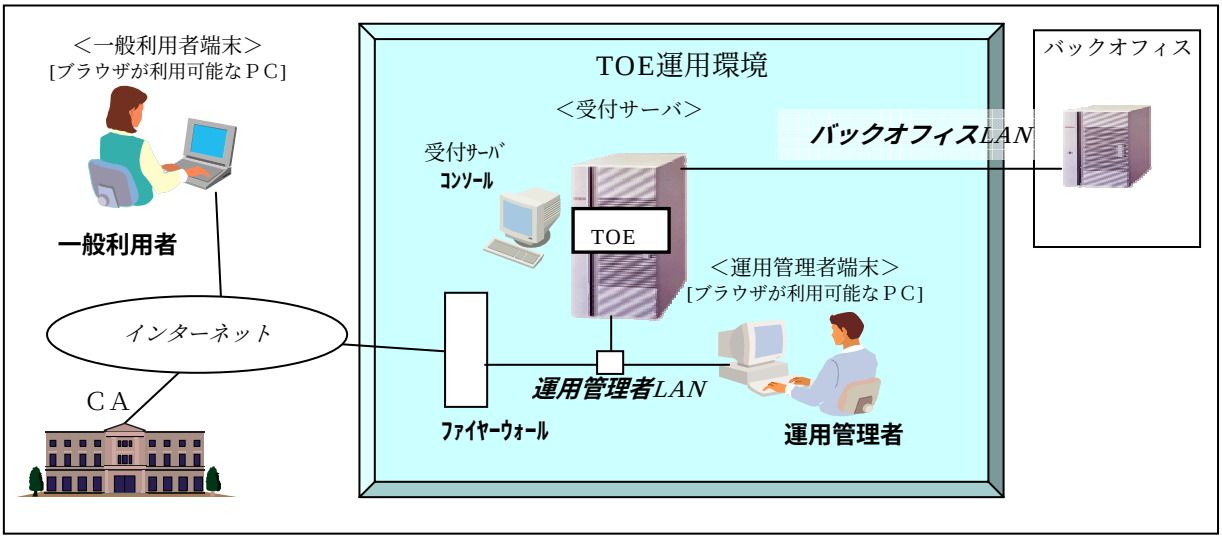

図1-1 TOEを適用したシステム構成図

一般利用者は、PC等のクライアントを使用してTOEにアクセスして識別・認証されることにより電子申請／電子窓口システムにアクセスすることが可能となり、申請・届出にともなう一連の電子申請サービスをインターネット経由で利用することができる。

一般利用者である申請者は、電子申請書に必要事項を入力し、申請書データに電子署名を付加し、オンラインで申請を行う。

運用管理者は、PC等のクライアントを使用してTOEにアクセスして識別・認証されることにより運用管理ユティリティーにアクセスすることが可能になり、TOEを利用してユーザ情報の管理･申請書データ配信の管理･レシートの管理を行うことができる。

(2) TOEの範囲

TOEの物理的範囲は、OSがWindowsの場合図1-2、HP-UXの場合図1-3にて示される以下のライブラリ及びユーティリティから構成される。

・セッション管理サービス
・レシート管理サービス
・配信サービス
・アプリケーション動作支援サービス(ログ管理)
・セッション管理サービス運用管理
・レシート管理サービス運用管理
・配信サービス運用管理

なお、TOEがWindowsまたはHP-UXにて動作するのは、Javaで記述されたTOEが、アプリケーションサーバCosminexus Application Server - Version 5により異なるOS下でも同一のJava動作基盤が提供されるためである。

TOEを含めたソフトウェア構成図を以下に示す。

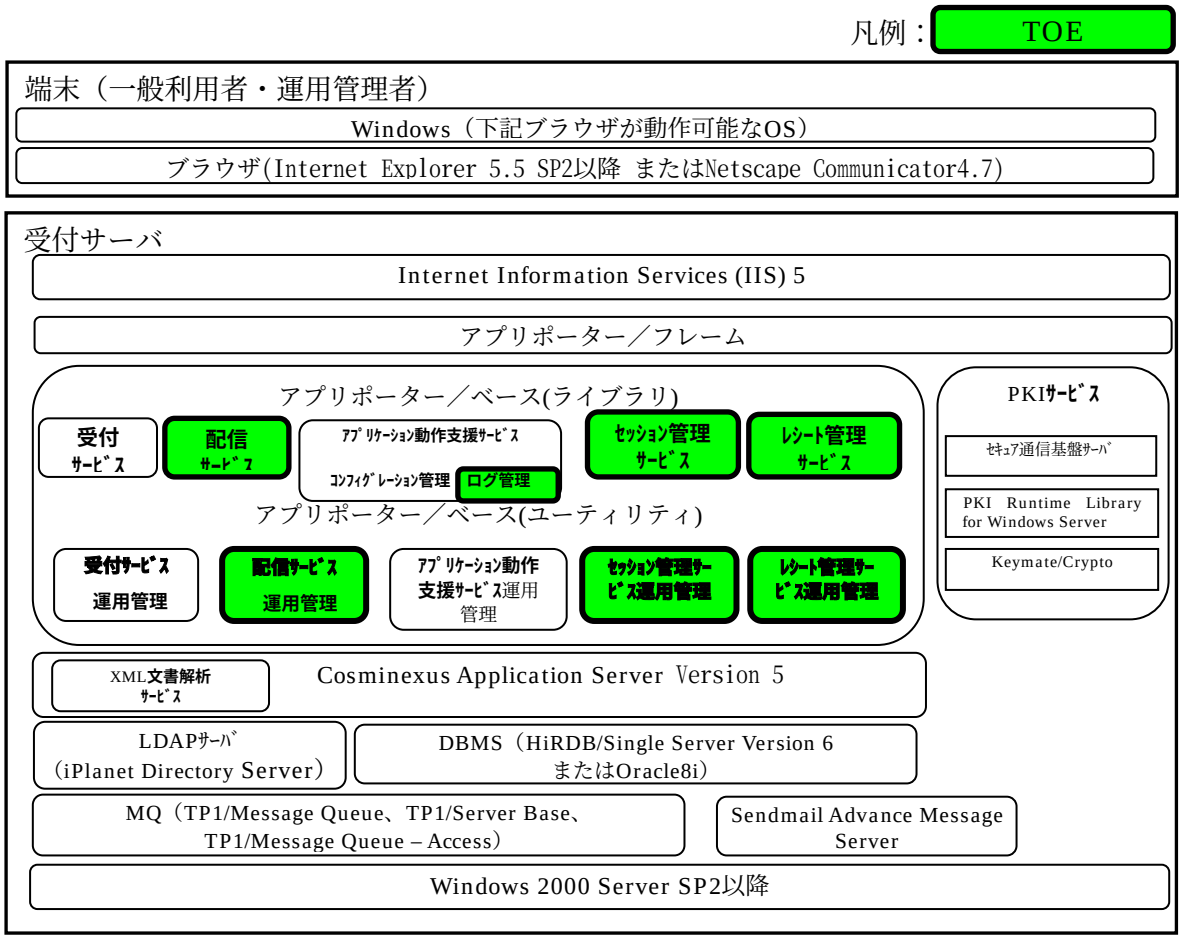

図1-2 ソフトウェア構成図（アプリポーターWindows版の構成例）

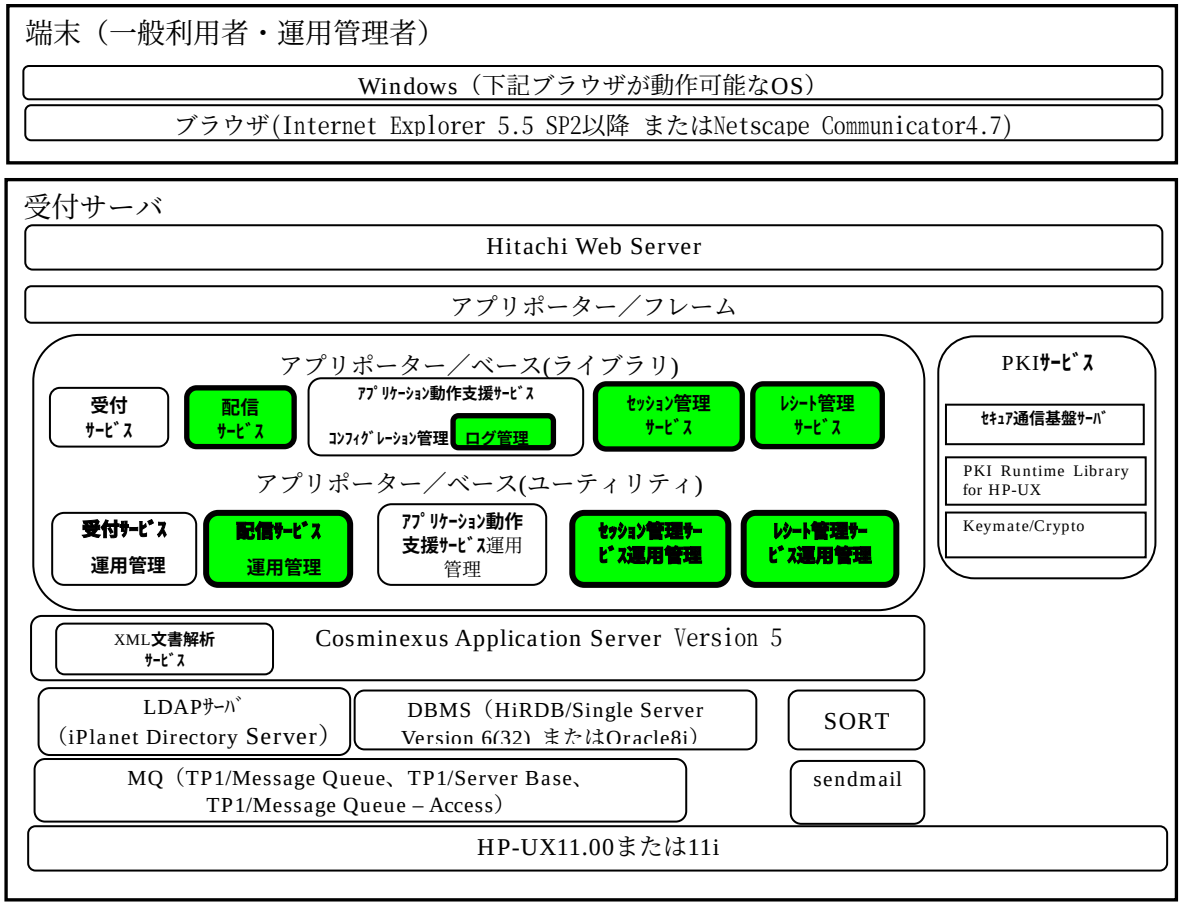

図1-3 ソフトウェア構成図（アプリポーターHP-UX版の構成例）

各ソフトウェアコンポーネントが提供する機能の概要を以下に示す。

- Cosminexus Application Server
  J2EE準拠のアプリケーションサーバ。TOEにおいてはEJBコンテナ，Webコンテナ，JDBC等Webアプリケーションの実行環境を提供する。
- Web サーバ
  ・Internet Information Services (IIS) 5
  OSがWindows2000 ServerSP2の場合のCosminexusが前提とするWebサーバ。
  ・Hitachi Web Server
  OSがHP-UX11.00の場合のCosminexusが前提とするWebサーバ。
  Cosminexusに同梱される。
- DBMS（HiRDB/Single Server　または　Oracle8i）
  データベース管理ソフト。TOEからの指示によりデータの管理を行う。レシート情報、配信前の申請書データ（配信ジョブキュー）を格納する。TOEがユーザ情報管理をDBMSで行う設定の場合、ユーザ管理情報、アカウントロック情報も格納する。
  ・SORT

OSがHP-UXの場合のHiRDB/Single Serverの前提となるソフトウェア。ファイルの編成とテキストのソート・マージを行う。

- PKI サービス

  セキュア通信基盤サーバ、PKI Runtime Library、Keymate/Cryptoの３つのソフトウェアからなるアプリポーターのサービスの一つ。レシート管理サービスにおいて、レシートに電子署名を付与する時に使用される。また、申請書に対する電子署名の署名検証・証明書の検証と有効性確認等に使用される。

  ・セキュア通信基盤サーバ

  署名（XML、PKCS#7等）付与・検証、証明書の検証・有効性確認、クライアントとの暗号通信等の機能を持つ。PKI Runtime Libraryが前提プログラムとして必要。TOEはセキュア通信基盤の署名検証機能を使用し署名検証を行うことで、申請データの改ざん有無が確認可能。

  ・PKI Runtime Library

  PKIの技術を使ってセキュリティを確保するための実行用ライブラリとPKI関連のツール群。セキュア通信基盤から呼び出されて、申請書データに付与された電子署名の検証、公開鍵証明書の検証、レシートへの電子署名付与を行う。また、秘密鍵管理、ルートCA証明書管理、ユーザ証明書管理、鍵ペア生成、CRL管理等のツール類を提供する。

  ・Keymate/Crypto

  セキュリティ基盤システム構築のための暗号ライブラリ。PKI Runtime Libraryの前提プログラム。公開鍵暗号、共通鍵暗号、ハッシュ関数の機能を提供する。また暗号鍵、秘密鍵、公開鍵の生成も行う。

- iPlanet Directory Server

  LDAPディレクトリサーバソフト。TOEがユーザ情報管理をLDAPで行う設定の場合に使用する。ユーザ情報やユーザ権限を保持し，ユーザ認証時の照会先となる。パスワード長の制限、パスワード使用可能文字の制限、認証エラー回数によるアカウントロック機能等を持つ。

- MQ

  ・TP1/Message Queue

  TOEの配信サービスでMQ配信機能を選択した場合配信先に必要となる。分散システム上のアプリケーション間でのメッセージキューを介した非同期蓄積型の通信手段を提供する。メッセージキューを管理してメッセージを送受信するプログラムをキューマネジャといい、TP1/Message Queueは、システム上でキューマネジャの役割を持つ。

  TP1/Message Queueを使用すると、OpenTP1（注）システム内のアプリケーション同士及び他システムのキューマネジャとの間でメッセージの送受信ができる。通信相手システムのキューマネジャは、TP1/Message Queueまたは他のMQSeries（IBM社の製品）である。これらのキューマネジャと通信する場合、TCP/IP（Transmission Control Protocol/Internet Protocol）プロトコルを使用

する。

(注) OpenTP1：オープンシステム上でオンライントランザクション処理（OLTP　Online Transaction Processing）をできるようにするソフトウェア（TPモニタ）。

・TP1/Message Queue- Access
クライアントアプリケーションからTP1/Message Queueのメッセージキューにメッセージを登録したり、取り出したりする機能を持つ。Javaインタフェースを持つ。

・TP1/Server Base
TP1/Message Queueの前提ソフトウェア。TP1/Message Queueの動作基盤と各種設定機能を実現する。

- Sendmail Advance Message Server / sendmail
メールサーバ。配信サービスでE-mail配信機能を選択した場合必要となる。E-mailの送受信管理機能を持つ。

1.2.4 TOEの機能

TOEが備える機能を以下の表1-1及び表1-2に示す。

表1-1 アプリポーター／ベース（ライブラリ）の機能一覧

ライブラリ	機能		概要
セッション管理サービス	ユーザ認証	ユーザ ID／パスワード認証	ユーザ ID、パスワード方式でのセッション認証機能 パスワード変更機能
		SSL クライアント認証	SSL クライアント認証でのセッション認証機能
	ユーザ情報参照	固有情報参照	ユーザ情報に付与した業務固有情報の参照
		公開鍵証明書情報参照	クライアント証明書情報の参照※
	セッション情報保持		HTTP リクエスト間で引き継ぐ情報の登録・参照
レシート管理サービス	デジタルレシート発行		申請情報のデジタルレシート（デジタル署名付き受付記録）の発行・保管
	デジタルレシート参照		発行したデジタルレシート（デジタル署名付き受付記録）のアプリケーションへの引き渡し
配信サービス	メッセージ編集	MQ 配信用	申請データ、キュー名、メッセージ ID などの MQ メッセージ記述子に含まれる情報を設定して、MQ 配信用のメッセージを作成
		FTP 配信用	ホスト名、ファイルパス、申請書データを設定して FTP 配信用メッセージを作成
		Mail 配信用	題名、メール本文、宛先アドレス、申請書データを設定してメール配信用のメッセージを作成
		蓄積サーバ配信用	ホスト名、変換識別子、申請書データを設定して蓄積サーバ用メッセージを作成

	送信ジョブキューへの一時保管		メッセージ編集機能で作成されたメッセージを送信ジョブキューに一時保管
	配信機能	MQ 配信	送信ジョブキューに一時保管されている MQ 配信用のメッセージを TP1/Message Queue のメッセージキューイング機能を用いて配信
		FTP 配信	送信ジョブキューに一時保管されている FTP 配信用のメッセージを FTP で配信先に配信
		Mail 配信	送信ジョブキューに一時保管されている Mail 配信用のメッセージを sendmail のメール送信機能を用いて SMTP で配信
		蓄積サーバ配信	送信ジョブキューに一時保管されている蓄積サーバ用のメッセージを FTP で配信
アプリケーション動作支援サービス	ログ管理		メッセージレベル、メッセージ ID、種別、及びメッセージテキストを引数として、ログを取得。取得日時は自動取得

表1-2 アプリポーター／ベース（ユーティリティ）機能一覧

ユーティリティ	機能	概要
セッション管理サービス運用管理	利用者情報管理	利用者情報の登録・参照・編集・削除 ロックアウトユーザの参照・解除・強制ロックアウト ロックアウト条件の設定
配信サービス運用管理	配信サービス管理	配信サービスの起動・停止
	配信データ管理	送信ジョブキューのエントリを一覧表示 送信済みエントリのデータを再送信 送信ジョブキューの配信データを削除
レシート管理サービス運用管理	レシートデータ管理	レシート DB の利用状況の参照 レシートデータのファイル出力 レシートデータの削除

但し、上記表のセッション管理サービス及びセッション管理サービス運用管理機能は、TOE(RDB)若しくはIT環境（iPlanet Directory Server）のどちらかでの実施を選択可能である。両方を同時に使用することはできない。

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セキュリティ認証申請等の手引き」[2]、「ITセキュリティ評価機関に対する要求事項」[3]、「ITセキュリティ認証申請者・登録者に対する要求事項」[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「アプリポーター Security Kit 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][11][14]のいずれか) 附属書C、CCパート2（[6][9][12][15]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][16]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、「アプリポーター Security Kit 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]のいずれか）に準拠する。また、CC及びCEMの各パートは補足（[20][21]）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、本評価報告書、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17年2月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、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

本STが規定するTOEの評価保証レベルは、EAL2適合である。

1.5.3 セキュリティ機能強度

本STは、最小機能強度として、”SOF-基本”を主張する。

本TOEは、物理的に入退室が管理された場所に設置されており、脅威は公開のインタフェースを利用した攻撃に限定され、その攻撃能力は”低レベル”である。このため、最小機能強度は”SOF-基本”で妥当である。

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。

1.5.4.1 識別・認証

(1) 利用者識別・認証

TOEを一般利用者または運用管理者が利用する際には、まず利用者識別・認証に成功しなければならない。

利用者識別はユーザIDにより行う。利用者認証の方法はパスワードによる認証、パスワード及びSSLクライアント証明書による認証の２つの方法がある。利用者認証方法は運用管理者がDDファイル内の一般利用者認証方式フラグに指定しておき、TOEは一般利用者認証方式フラグに事前に定義してある方法で認証を行う。一般利用者認証方式フラグに指定がない場合はパスワードによる認証を行う。ただし、運用管理者の使う運用管理者用ユーティリティではパスワードによる認証のみが利用可能である。（一般利用者認証方式フラグへの設定機能そのものはIT環境で実施される機能である。）

パスワード認証ではTOEが管理するユーザ管理情報の中のパスワードと利用者の入力したパスワードを比較することで認証する。SSLクライアント証明書方式では、TOEが管理するユーザ管理情報の中のSSLクライアント証明書と利用者がWebサーバに送ったSSLクライアント証明書を比較することで認証する。但し、パスワード及びSSLクライアント証明書はユーザ管理情報にはハッシュ値をエンコードした状態で保管されているので、IT環境の機能を用いてハッシュを取りエンコードしてから、TOEで比較する。

(2) 複数の認証メカニズム

パスワード及びSSLクライアント証明書による認証では、パスワードとSSLクライアント証明書による両方で認証が成功した場合のみ認証成功となる。

(3) 保護された認証フィードバック

パスワード認証時に利用者が入力したパスワードは画面上では＊ (アスタリスク)

で表示する。

(4) 認証失敗時の取り扱い

TOEは利用者がパスワードまたはSSLクライアント証明書による認証に失敗すると、認証失敗回数をカウントアップする。認証失敗回数が「ロックアウト閾値」に達した場合はその利用者のアカウントがロックアウトされる。ロックアウトされた利用者はパスワードやSSLクライアント証明書による認証が成功しても認証失敗としログインできなくする。最後の認証失敗からの経過時間が、「認証失敗回数クリア間隔」の指定時間を超えると認証失敗回数はクリアされる。また、「ロックアウト期間」の指定時間を経過するとアカウントのロックアウトは解除されログイン可能となる。ロックアウト閾値はデフォルトでは３回である。認証失敗回数クリア間隔はデフォルトで10分である。ロックアウト期間はデフォルトで60分である。

ユーザ情報の管理はRDB(HiRDB またはOracle)による方法とLDAPサーバ（iPlanet Directory Server）による方法がある。RDBによるユーザ管理の場合、TOEが上記のロックアウトの管理を行う。LDAPによるユーザ管理を選択した場合には、TOE外のLDAPサーバの機能によってロックアウトの管理を行う。

1.5.4.2 セッション情報保持

利用者識別・認証が成功すると、TOEは認証済みの利用者情報を保持するユーザコンテクストを生成し、ユーザID 、ロール等ユーザ管理情報をセットする。識別・認証成功後のTOEではこのユーザコンテクストのロールを参照することで運用管理者用Webページ、ユーザ管理情報、レシート、申請書データ等へのアクセス管理を行う。いったん確立されたセッションは、そのセッションに対して識別・認証済み利用者から明示的にログアウトが行われるか、もしくはセッションタイムアウトが発生するまで持続される。

1.5.4.3 レシート管理

TOEは申請書の受信証拠として、申請書データに受付番号、受付日時、申請者のユーザIDを付与したレシートデータを作成し、IT環境であるPKIサービスへTOEの電子署名の付与を依頼する。PKIサービスから受け取ったレシートデータは、レシート管理サービスにて保管すると同時に、アプリポーター／フレームに渡され申請者にダウンロードされる。また、TOEはレシート管理サービス運用管理機能にて運用管理者に、レシートデータを管理する機能を提供する。識別・認証で正しく認証された運用管理者（ロールが運用管理者）は、レシートDBに蓄積されたレシートについて、レシートID、取得日、受付番号、ユーザIDをキーにして検索・一覧表示できる。また表示後にレシートを指定して削除またはダウンロード（レシートDBからの取り出し）ができる。

1.5.4.4 ログ生成

TOEは事象種別(ERROR、WARM、CAUTION、INFO、DEBUG)にそって、以下の監査ログを生成する。

表1-3　監査対象事象と事象種別の関係

監査対象事象	監査ログが生成される事象種別
①レシートデータ作成の成功／失敗の記録	INFOまたはDEBUG
①連続認証失敗回数が閾値に達した場合のロックアウト開始記録 ②及び時間経過によりロックアウト解除後の最初の認証成功記録	CAUTIONまたはINFOまたはDEBUG
①パスワード登録・変更の成功／失敗の記録 ②登録・変更内容の記録 ③登録者・変更者の記録 ④登録・変更が発生した時刻の記録	INFOまたはDEBUG
①認証における、失敗の記録 ②失敗者の記録 ③失敗が発生した時刻の記録	ERRORまたはWARNまたはCAUTIONまたはINFOまたはDEBUG
①パスワード認証での成功／失敗 ②SSLクライアント認証での成功／失敗 ③複合認証でのトータルな認証の成功／失敗 ④成功者／失敗者の記録 ⑤成功／失敗が発生した時刻	INFOまたはDEBUG（但し、④失敗者に関するユーザIDはDEBUGでの出力）
①識別における失敗の記録 ②失敗者の記録 ③失敗が発生した時刻の記録	ERRORまたはWARNまたはCAUTIONまたはINFOまたはDEBUG
①ロックアウト閾値の変更の成功／失敗の記録 ②変更者の記録 ③時刻の記録	INFOまたはDEBUG
①ロックアウトフラグ変更後の値の記録 ②変更の成功／失敗の記録 ③変更者の記録 ④時刻の記録	CAUTIONまたはINFOまたはDEBUG
①認証失敗回数クリア間隔値の変更の成功／失敗の記録 ②変更者の記録	INFOまたはDEBUG

③時刻の記録	
①レシートデータ削除、ダウンロードの成功／失敗の記録 ②対象者の記録 ③時刻の記録	INFOまたは DEBUG
①ロックアウト期間の値の変更成功／失敗の記録 ②変更者の記録 ③時刻の記録	INFOまたは DEBUG
①パスワード、ユーザID、証明書、ロールに関する変更後の値の記録 ②変更の成功／失敗記録 ③変更者の記録 ④時刻の記録	CAUTIONまたは INFOまたは DEBUG

また上記の監査事象に関して、監査機能の起動と終了に関するログは含まれていない。起動と終了に関するログは、TOE範囲ではないIT環境（Cosminexus Application Server）にて生成している。

1.5.4.5 ユーザ情報管理

ユーザ情報の管理方法は、運用管理者がDDファイル中のユーザ情報管理方式フラグに指定しておくことでLDAPを使う方法とRDBを使う方法を選択できる。デフォルトではLDAP(IT環境)を使用する。以下は、TOEで管理した場合の記述である。

ユーザ情報の管理は、運用管理者のみが管理できる。運用管理者による管理機能はセッション管理サービス運用管理機能である。

(1) アカウント情報の管理

利用者のユーザID、パスワード、SSLクライアント証明書の新規登録・更新・削除・検索・参照はTOEを使って行うことができる。この機能を使用できるのは、TOEによりロールが運用管理者である利用者のみに限定される。

ただし、パスワード変更のみはパスワードを所有する一般利用者自身にも変更権限を与える。

(2) ロールの管理

ロールはユーザ情報登録時の必須項目である。ロールには下記の二つがあり、本STで示す役割と関連付けられている。

- 運用管理者（本 ST での運用管理者）
- 申請者（本 ST での一般利用者）

ロールの初期登録と変更・追加・削除は運用管理者のみが可能とする。本機能で同一ユーザに上記のロールを両方設定できるが、ロール「なし」には設定できない。

(3) パスワードの制限

ユーザ情報管理にRDBを使う方法の場合は、TOEの機能でパスワードとして使用できる文字列について、最小文字数・最大文字数、英数字以外の使用可能文字の限定

ができる。パスワードの最小文字数はデフォルトで6文字、パスワードの最大文字数はデフォルトで32文字である。

パスワードに使用可能な文字は英数字（a～z,A～Z,0～9）と記号（デフォルトでは　!"#$%&'()*+,-./:;<>=?@[¥]^_`{|}~　）である。

パスワードの新規登録、変更時にTOEは以上のパスワード制限を判定し、適合しないパスワードについては登録、変更を拒否する。

LDAPを使う方法の場合、これらのパスワードの制限はTOE外であるLDAPソフトウェアの機能と設定に従う。

1.5.4.6 アカウントロック管理

ユーザ情報管理をRDBで行う方法を選択した場合、TOEはセッション管理サービス運用管理機能の一機能としてアカウントロック管理機能を提供する。アカウントロック管理機能を使用できるユーザは、TOEの識別・認証機能により運用管理者のみに限定される。アカウントロック管理では以下の機能を提供する。

- 現在ロックアウトされているユーザを検索し一覧表示する。
- ロックアウトユーザ一覧からユーザを指定するか、ユーザ ID を直接指定してロックアウトフラグを解除する。
- ロックアウトに関する設定値である、ロックアウト閾値、ロックアウト期間、認証失敗回数クリア期間について設定値の参照、変更を行う。

1.5.5 脅威

本TOEは、表1-4に示す脅威を想定し、これに対抗する機能を備える。

脅威をもたらす攻撃者として“ 運用管理者以外 ”の以下の者を想定する。

- 一般利用者として TOE の利用権限を持つが、他の利用者（運用管理者または他の一般利用者）に成りすまそうとする者
- TOE の利用権限を持たない者（一般利用者以外のインターネット上のユーザ及び、運用組織内の他システム関連者）

表1-4　想定する脅威

識別子	脅　威
T.INTERNAL_USER_DATA_ACCESS	TOE内部で保管される申請書データが、攻撃者の行為により運用管理者端末から削除、改ざん、暴露される。 これによりTOEは申請処理そのものを実施しない、正規の申請内容と異なった申請処理を実施する、申請内容の漏洩、という不具合が発生する。
T.INTERNAL_AU	TOE内部で保管されるユーザ管理情報が、攻撃者の行為によりイ

TH_DATA_ACCESS	ンターネットまたは運用管理者端末から削除、改ざん、暴露される。 これにより、正当な利用者がTOEを利用出来ない、TOEへログインする際になりすましが発生する、という不具合が発生する。
T.INTERNAL_RECEIPT_DATA_ACCESS	TOE内部で保管されるレシートデータが、攻撃者の行為によりインターネットまたは運用管理者端末から削除、改ざん、暴露される。 これにより、一般利用者本人が申請処理内容の確認が出来ない、TOEが処理した結果と異なる処理内容が一般利用者本人に通知される、申請内容の漏洩、という不具合が発生する。
T.DISCLOSE_NW_DATA	TOEと一般利用者端末間のインターネット上の通信において、ネットワーク上でやり取りされるユーザ管理情報、レシートデータ、及び申請書データが暴露される。 これにより、TOEへの成りすましの発生、申請結果及び申請書データ内容の漏洩といった不具合が発生する。

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を表1-5に示す。

表1-5 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
OSP.REPUDIATION	運用管理者は一般利用者に対して、以下を証明しなければならない。 ・TOEが申請書データを受け付けたことを否認できない為の証明。
OSP.IMPORT_USER_DATA_INTEGRITY	運用管理者は、TOEにインポートされる一般利用者からの申請書に対して以下を実施しなければならない。 ・申請者である一般利用者を正しく識別・認証し、申請書が改ざんされていないことを確認する。 （申請者本人の意図しない申請内容となっていないことの確認）

1.5.7 構成条件

本TOEは、受付サーバに搭載されるSW（ソフトウェア）である。TOEが動作する環境を以下に示す。

(1) ソフトウェア構成
各構成要素に搭載されるソフトウェアコンポーネントを以下の表1-6、表1-7に示す。

表1-6 ソフトウェア構成(Windows版)

№	名称	搭載ソフトウェア	ﾊﾞｰｼﾞｮﾝ
1	受付サーバ	OS:Windows2000 Server Service Pack 2	2000 SP2
		Internet Information Services (IIS) 5	5.0
		Cosminexus Application Server - Version 5	05-00/B
		アプリポーター 03-02	03-02
		HiRDB/Single Server Version 6	06-00/C
		Oracle 8i Standard Edition	8.1.7
		セキュア通信基盤サーバ	03-00/A
		PKI Runtime Library for Windows Server	02-03
		Keymate/Crypto	02-00
		iPlanet Directory Server 5.1	5.1
		TP1/Message Queue	05-00/E
		TP1/Message Queue- Access	01-04
		TP1/Server Base	05-00/F
		Sendmail Advance Message Server	1.3J
2	運用管理者端末	OS:Windows(下記ブラウザが動作可能なOS)	
		Internet Explorer 5.5 SP2またはNetscape Communicator 4.7	5.5SP2/4.7
3	一般利用者端末	OS:Windows(下記ブラウザが動作可能なOS)	
		Internet Explorer 5.5 SP2またはNetscape Communicator 4.7	5.5SP2/4.7

表1-7 ソフトウェア構成(HP-UX版)

№	名称	搭載ソフトウェア	ﾊﾞｰｼﾞｮﾝ
1	受付サーバ	OS: HP-UX11.00	11.00
		SORT	02-00/B
		Cosminexus Application Server - Version 5	05-00/B
		Hitachi Web Server（Cosminexusに同梱）	01-02/C
		アプリポーター 03-02	03-02
		HiRDB/Single Server Version 6(32)	06-01
		Oracle 8i Standard Edition	8.1.7
		セキュア通信基盤サーバ	03-02
		PKI Runtime Library for HP-UX	02-06
		Keymate/Crypto	03-00
		iPlanet Directory Server 5.1	5.1
		TP1/Message Queue	05-13
		TP1/Message Queue- Access	05-00
		TP1/Server Base	05-03/B
		Sendmail	8.8.6
2	運用管理者端末	OS:Windows(下記ブラウザが動作可能なOS)	
		Internet Explorer 5.5 SP2またはNetscape Communicator 4.7	5.5SP2/4.7
3	一般利用者端末	OS:Windows(下記ブラウザが動作可能なOS)	
		Internet Explorer 5.5 SP2またはNetscape Communicator 4.7	5.5SP2/4.7

(2) ハードウェア構成

TOEが搭載される受付サーバのハードウェア構成を以下の表1-8、表1-9に示す。

表1-8 ハードウェア構成(Windows版)

№	名称	ハードウェア仕様
1	受付サーバ	モデル：HA8000/70
		プロセッサ（クロック）：Pentium III（700MHz）
		メモリ：512MB
		内蔵ディスク容量：8.5GB
		コンソール：ディスプレイ装置・キーボード・マウス

表1-9 ハードウェア構成(HP-UX版)

№	名称	ハードウェア仕様
1	受付サーバ	モデル：H9000V / C3600
		プロセッサ（クロック）：PA-8600（552MHz）
		メモリ：1GB

		内蔵ディスク容量：18GB コンソール：ディスプレイ装置・キーボード・マウス

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1-10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1-10 TOE使用の前提条件

識別子	前提条件
A.PHYSICAL_ACCESS	受付サーバ（及び受付サーバコンソール）、資産のバックアップが保管されたメディア、運用管理者端末、及び運用管理者LANとバックオフィスLANが収容された場所は、入退出管理を実施する。
A.ADMINISTRATOR	監査者、運用管理者は、それぞれに課せられた役割に対して許可された一連の行為に関して悪意を持った行為は行わない。
A.TRUST_CERT	電子証明書と対応する秘密鍵の発行及び失効は、TOEの範囲外において信頼できるCAによって行われる。発行された電子証明書と対応する秘密鍵は信頼できる。
A.NETWORK	TOEへのネットワークからのアクセスを許可する箇所は、特定箇所のみに限定されており、TOEとバックオフィス、運用管理者端末は専用のLANで結ばれている。また、バックオフィスでの運用は信頼できる。

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。

- アプリポーター環境構築手順(Windows/HiRDB版) 第2版
- アプリポーター環境構築手順(Windows/Oracle版) 第1版
- アプリポーター環境構築手順(HP-UX/HiRDB版) 第2版
- アプリポーター環境構築手順(HP-UX/Oracle版) 第1版
- アプリポーター／ベース ソフトウェア添付資料(Windows版) 第2版
- アプリポーター／ベース ソフトウェア添付資料(HP-UX版) 第2版
- アプリポーター／ベース アドミニストレーターズガイド(Windows版) 第3.1版
- アプリポーター／ベース アドミニストレーターズガイド(HP-UX版) 第2.1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、本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15年1月に始まり、平成17年2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15年2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に関するプロセスの施行状況の調査を行った。また、平成15年2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に示す。

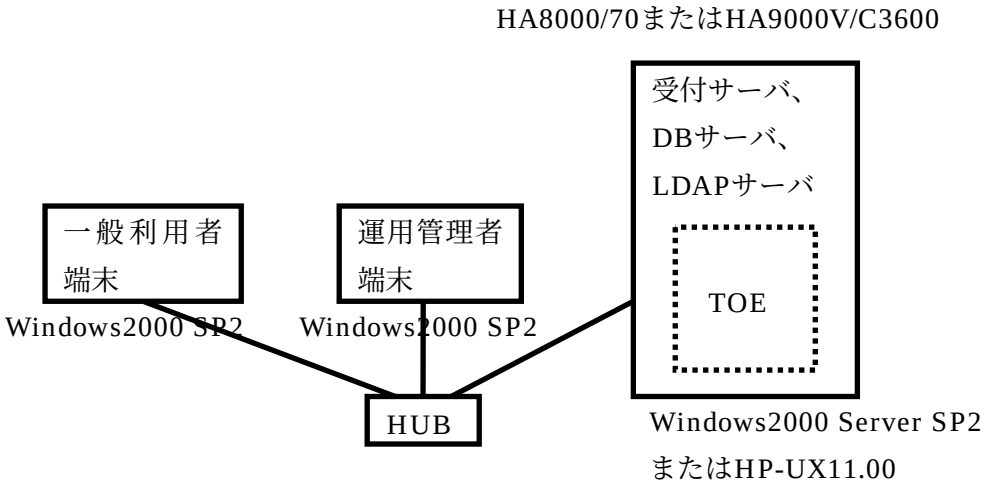

図2-1 開発者テスト構成

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は図2-1に示すとおり、STにおいて識別されているTOE構成と同一の機能を備えるハードウェア及びソフトウェアで構成されるテスト環境(Windows版とHP-UX版の両方)で実施されている。一般利用者端末がインターネット経由でなくHUB接続であったが、テストへの支障はないと判断した。

b.テスト手法

テストには、以下の手法が使用された。

①一般利用者端末及び運用管理者端末を操作することによりセキュリティ機能の外部インタフェースを刺激し、セキュリティ機能のふるまいを観察する。

c.実施テストの範囲

テストは開発者によって548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に示すとおり、STにおいて識別されているTOE構成と同一の機能を備えるハードウェア及びソフトウェアで構成されるテスト環境(Windows版とHP-UX版の両方)で実施されている。一般利用者端末がインターネット経由でなくHUB接続であったが、テストへの支障はないと判断した。

b.テスト手法

テストには、以下の手法が使用された。

①一般利用者端末及び運用管理者端末を操作することによりセキュリティ機能の外部インタフェースを刺激し、セキュリティ機能のふるまいを観察する。

c.実施テストの範囲

評価者は、独自に考案したテストを9項目、開発者テストのサンプリングによるテストを66項目、侵入テストを5項目、計80項目のテストを実施した。

開発者テストは548項目あるが、ユーザ情報を登録する形態(LDAP、OLACLE、HiRDB)の違いにより重複するものがある。このため、実質的な機能項目のテストは50%と考え、66項目(約24% = 66÷548×50%)をサンプリングした。

評価者が独自に考案したテストは、下記を考慮している。

① STの要約仕様、機能仕様を元にテスト項目の対応を確認し、不足していると考えられる項目に対し追加検証する(認証ロックアウト、限界値テスト、ログ出力等)

開発者テストのサンプリングテストは、下記を考慮している。

①各サブシステムからはそれぞれ最低１つの機能群を選択し、対象利用者別(運用管理者、一般利用者)、対象DB(Oracle、HiRDB、LDAP)の関連要素をもれなく抽出する

侵入テストは、識別・認証機能の脆弱性が悪用されることがないか、セキュリティ設定を誤った場合に機能が無効化されることがないかの確認を目的に実施されている。

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

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

4.1 **認証結果**

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、認証機関は、本TOEがCCパート3のEAL2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種別、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記述が理路整然と一貫性のあ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。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.1.1E	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。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_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所見報告書による指摘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。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_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。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_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所見報告書による指摘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所見報告書による指摘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、当評価に至るまでになされた所見報告書による指摘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_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。
ADO_DEL.1.2D	評価はワークユニットに沿って行われた。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。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。

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。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.1.1E	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。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。

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。
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。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_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。
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。
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主張が正しことを確認している。
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。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.1.2E	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。

DD （ Deployment Descripter）	アプリケーションを運用環境に配置するときの定義情報を記述した電子文書。EJB用，Webアプリケーション用，Enterpriseアプリケーション用などがSunからの仕様で規定されている。
バックオフィス	アプリポーターでの電子申請受付後､申請書データを受けて個別の業務を行う環境
監査者	役割：TOEの監査を実施する。 権限：TOEの監査に係る機能は運用管理者が操作し、TOEの監査データのみを参照する。
運用管理者	役割：TOEが利用する外部ITサービスの選定・契約事務処理、TOEを導入する機器、ネットワーク及びソフトウェアの設置・接続・インストール、TOEのインストール･各種設定及び設定の変更、データベースの運用管理、TOEの起動・停止、システムトラブル対応及び日々のシステム運用管理、監査支援を行う。 権限：TOEのシステム運用に関する登録、変更、削除等の操作に関する権限を持つ。

一般利用者	役割:一般利用者クライアントを用いて電子申請サービスを利用する。TOEを使って申請書を送信する。自らのパスワードを変更する。 権限：インターネットなど外部ネットワーク経由でTOEにアクセスし、申請書の送信、一般利用者自身のパスワードの変更に関する権限を持つ。

6 参照

[1] アプリポーター Security Kit セキュリティターゲット Version 1.80（2005/2/5） 株式会社 日立製作所

[2] ITセキュリティ認証申請等の手引き 平成16年4月 独立行政法人情報処理推進機構 ITQM-23

[3] ITセキュリティ評価機関に対する要求事項 平成16年4月 独立行政法人情報処理推進機構 ITQM-07

[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16年4月 独立行政法人情報処理推進機構 ITQM-08

[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] アプリポーター Security Kit 評価報告書 第1.3版 2005年2月14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