認　証　報　告　書

評価対象

申請受付年月日(受付番号)	平成14年3月25日（IT認証2001）
認証申請者	**株式会社リコー**
TOEの名称	**原本性確保支援システム**TrustyCabinet UX V1 Version V1.01 (Server Software)
ＰＰ適合	なし
適合する保証要件	EAL3
TOE開発者	**株式会社リコー　オフィスシステム研究所**
評価機関の名称	**電子商取引安全技術研究組合研究所**

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１４年１２月２０日

独立行政法人製品評価技術基盤機構
適合性評価センター管理課情報セキュリティ室
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 ISO/IEC 15408:1999 Information technology － Security techniques － Evaluation criteria for IT security.
② JIS X 5070(2000) セキュリティ技術 － 情報技術セキュリティの評価基準。
③ Common Criteria for Information Technology Security Evaluation.
④ 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
⑤ Common Methodology for Information Technology Security Evaluation
⑥ 認証機関が公開する③および⑤の翻訳文書

評価結果：合格

原本性確保支援システムTrustyCabinet UX V1 Version V1.01 (Server Software) は、独立行政法人製品評価技術基盤機構が定める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。

その他：

本報告書には、認証申請の受理以前に評価が開始されているような日付の記載がある。これは、評価認証制度に関わる正式な手続が確定した後に、再度、認証申請書が提出されたことが原因である。認証は、実際の評価の開始と同時に実施している。

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
1.3 評価の実施 3
1.4 評価の認証 4
1.5 報告概要 4
1.5.1 PP適合 4
1.5.2 EAL 4
1.5.3 セキュリティ機能強度 4
1.5.4 セキュリティ機能 4
1.5.5 脅威 6
1.5.6 組織のセキュリティ方針 8
1.5.7 構成条件 11
1.5.8 動作環境の前提条件 11
1.5.9 製品添付ドキュメント 13
2 評価機関による評価実施及び結果 14
2.1 評価方法 14
2.2 評価実施概要 14
2.3 製品テスト 14
2.3.1 開発者テスト 14
2.3.2 評価者テスト 16
2.4 評価結果 17
3 認証実施 18
4 結論 18
5 用語 25
6 参照 26

1 全体要約

1.1 はじめに

この認証報告書は、「**原本性確保支援システム**TrustyCabinet UX V1 Version V1.01 (Server Software)」（以下「本TOE」という。）について**電子商取引安全技術研究組合研究所**（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**株式会社リコー**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・「Administration Manual for TrustyCabinet UX V1 Version 2.4(en)」、「System Development Manual for TrustyCabinet UX V1 Version 2.2 (en)」、「Installation/Maintenance Manual for TrustyCabinet UX V1 Version 2.1 (en)」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、動作条件および機能仕様は本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。

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: **原本性確保支援システム**TrustyCabinet UX V1 (Server Software)
- バージョン: Version V1.01
- 開発者: **株式会社リコー オフィスシステム研究所**

1.2.2 製品概要

本TOEは、原本性確保支援システムTrustyCabinet UX V1のサーバソフトウェア部分である。TrustyCabinet UX V1にはサーバソフトウェア以外に、クライアントで使用されるソフトウェア、ユーティリティが含まれるが、これらはTOEの範囲外である(図１)。また、以下、TOEとOSを含む周辺ソフトウェア、及びハードウェアを含むサーバ全体を「TCAB」という。

TCABは、政府や企業のイントラネットで使用されるサーバシステムであり、電子文書の保管及び管理をセキュアに行うための機能を提供する。

TCABは保管文書の更新履歴を管理し、暗号機能を用いて、文書の更新履歴を不正な改ざんから保護する。また、TCABは文書を長期間保管するためにオフラインディ

スクに文書を書き出す機能を有する。あわせて、他のTCABに保管文書を転送する機能を有する。

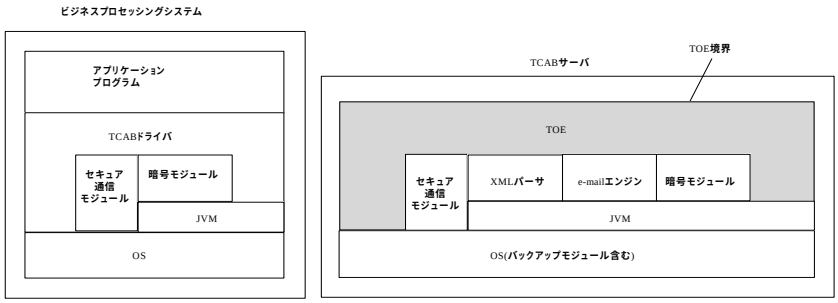

図 1　TOEの範囲

TCABは、一般的に図2に示されるような3層構造のシステムで使用されることが想定されている。エンドユーザはエンドユーザ端末から通常Webサーバ及びアプリケーションサーバより構成されるビジネスプロセッシングシステムにアクセスを行う。TCABはビジネスプロセッシングシステムのバックエンドで動作するものであり、TCABのクライアントであるビジネスプロセッシングシステムに対して以下の機能を提供する。

1）文書の保管
2）文書の読み出し
3）別のシステムへの文書の転送
4）オフラインディスクへの文書の書き出し
5）文書の複製の生成
6）文書の更新
7）文書の削除
8）監査
9）システムバックアップ
１０）アカウント管理

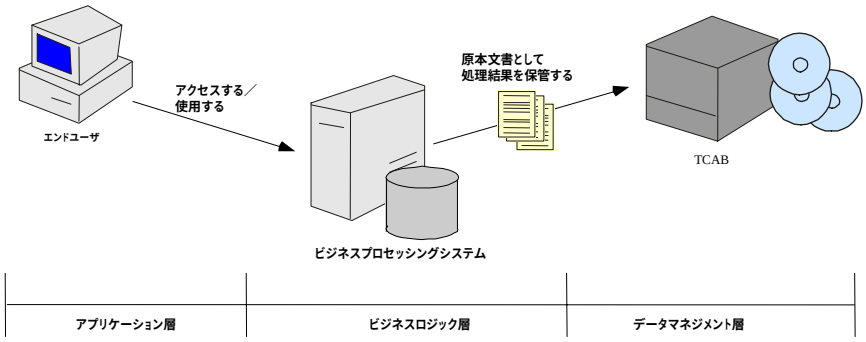

図 2　TOEを用いたシステムの構成

1.3　評価の実施

原本性確保支援システムTrustyCabinet UX V1 Version V1.01 (Server Software) のセキュリティ評価は、独立行政法人製品評価技術基盤機構が独立した認証機関として運営する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 (平成14年4月)」[2]、「ITセキュリティ評価機関に対する要求事項 (平成14年4月)」[3]、「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14年4月)」[4]に規定された内容に従って実施された。
本評価の目的は、以下のとおりである。

(1)　本TOEのセキュリティの基本設計が適切であること。

(2)　本TOEのセキュリティ機能が、基本設計で記述されたセキュリティ機能要件およびセキュリティ保証要件を満たしていること。

(3)　本TOEがセキュリティの基本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のセキュリティの基本設計である「Security Target for TrustyCabinet UX V1 Version1.9」（以下「本ST」という。）[1]、本TOE開発に関連する評価証拠資料及び本TOEの開発環境の現場を検証し、本TOEとその開発環境が

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）の機能要件及び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することである。この評価手順及び結果は「EVALUATION TECHNICAL REPORT Version1.2」（以下「本評価報告書」という。）[20]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。

1.4 評価の認証

認証機関は、評価機関である**電子商取引安全技術研究組合研究所**が作成した、本評価報告書、当該所見報告書[21]及び関連する評価証拠資料を検証し、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[22][23][24][25] [26][27][28][29][30][31]を作成し、評価機関に送付した。評価は、平成14年11月13日の評価機関による本評価報告書[20]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、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が判明した。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

TOEの評価保証レベルは、EAL3である。

1.5.3 セキュリティ機能強度

最小機能強度として、”SOF-基本”を主張する。

本TOEに含まれる確率的または順列的メカニズムは、識別認証機能に関連するもののみである。本TOEは組織的な高度で複雑な攻撃は想定していない。このため、低レベルの攻撃力に対抗できるレベルである ”SOF-基本 ” で満足される。

1.5.4 セキュリティ機能

TOEは、以下のセキュリティ機能を有する。

(1) 識別認証機能

アカウント名とパスワードによるクライアントの識別認証を行う。識別認証に成功した場合のみクライアントはTOEの他の機能を使用できる。識別認証に

失敗した場合、監査データに記録し、5秒間は次の要求を受け付けない。5分以内に3回の認証失敗が起こった場合、設定されたアドレスにe-mailを送信し警告を行う。TOEにアクセスするクライアントが別のTCABである場合、公開鍵認証も追加して行われる。

(2) ネットワーク保護機能

クライアントまたは他のTCABサーバとの間のSSL v2／v3プロトコルに基づく通信を行う。通信データは、暗号化／復号され、完全性の保護及び検証がなされる。

(3) アクセスコントロール機能

文書の属性(文書タイプ、保管期限等)、及び文書にアクセスするサブジェクトの役割を基にアクセスコントロールを行う。

また、文書コンテンツの転送時にセキュリティ属性を付加して行う。すなわち、文書コンテンツ、セキュリティ属性、アクセスログを含むデータアーカイブを生成し、転送する。

さらに、文書オブジェクトの属性を管理するために下記の能力を提供する。

・文書タイプの指定
・文書タイプの変更
・保管期限の指定
・保管期限の延長

利用者アカウントの管理を行う能力を管理者に提供する。また、パスワードの品質尺度のチェックを行う。

(4) 完全性保護機能

文書オブジェクト(セキュリティ属性、アクセスログも含む)に対して文書署名と呼ばれるデジタル署名を付加する。DocSpaceと呼ばれる文書収納庫ごとに文書リストを生成する。文書リストには、リスト署名と呼ばれるデジタル署名を付加する。DocSpace内で変更があった場合、リスト署名は再生成される。クライアントがDocSpaceにアクセスする際は、リスト署名と文書署名を検証する。

システムのアクセス履歴、システムタイマ設定履歴、利用者アカウント管理データ、システム設定データ、TCAB実行形式に対して、システム署名と呼ばれるデジタル署名を生成する。初期起動時に、上記情報に対する許可されない変更を検出するために、署名の検証を行う。システムアクセス履歴を外部媒体に移動させることも可能だが、その際もデジタル署名を付加する。

(5) 監査機能

監査記録の書き込みを行う前に、ディスク容量のチェックを行い、ディスク容量が警告レベルを超えている場合、設定されたアドレスにe-mailを送信する。ディスク容量が最大レベルを超えている場合、上記アドレスにe-mailを送信し、管理者及び監査者以外からの要求を受け付けない。ディスク容量が満杯の場合、TCABはシャットダウンされる。

システムアクセス履歴、システムタイマ設定履歴に対する読み取りアクセスの能力を提供する

1.5.5 脅威

本TOEは、表 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 想定する脅威

識別子	脅威
T.UNAUTH-ACCESS	未知の利用者がTOEに対して許可されないアクセスを行う。
	未知の利用者(TCAB利用者アカウントを持たない利用者)がTOEに対して、さらにはTOE内部に格納される文書に対して、論理的に許可されないアクセスを行う。 未知の利用者が識別及び認証を行わずにTOEのセキュリティ機能を利用する。 未知の利用者または許可されない利用者が、許可されたクライアントに成りすますためにパスワード攻撃を実行する。
T.NETWORK-ATTACK	ネットワークコネクションが攻撃される。
	TOEとクライアントの間、またはTOEと別のTCABの間の通信が、悪意のある利用者により変更または盗聴される。 悪意のある利用者が成りすましまたはマン・イン・ザ・ミドル攻撃を行い、それによってネットワーク上の文書や秘密(認証データ)にアクセスする。

T.DELETE-DOC	維持されるべき文書がTSFを通して削除される。
	故意かまたは過失かによらず、維持されるべき保管文書がTSFを通して削除される。 一般的なライトプロテクションやアクセスコントロールされたファイルシステムではこの脅威に対応するためには十分でない。例えば、文書を削除する権限をもつ誰かが、法的な見地から保管期限内は保持されなければならない重要文書を削除する。 削除権限をもったクライアントに誰かが成りすまし、重要な文書を削除する。
T.OVERWRITE-DOC	TSFを介して文書が痕跡を残さず変更される。
	故意かまたは過失かによらず、保管文書がTSFを介して痕跡(アクセスログ及び変更履歴)を残さずに変更または上書きされる。 一般的なライトプロテクションやアクセスコントロールされたファイルシステムではこの脅威に対応するためには十分でない。例えば、文書を変更する権限を持つ誰かは、容易に痕跡を残さず文書を変更／上書きすることができる。 変更権限をもったクライアントに誰かが成りすまし、痕跡を残さず重要な文書を変更／上書きする。
T.MODIFY-DOC-DIRECTLY	TSF を使用することなく、検出されないままに、文書が変更，削除，すり替えまたは偽造される。
	保管文書が、検出されずに、TOEセキュリティ機能を使用することなく、変更、削除、すり替えまたは偽造される。 文書を保管しているオフラインディスクが捨て去られる、または他のディスクとすり替えられる。例えば、文書を保管するオフラインディスクの複製を作成した後、許可されたクライアントがTOEを使用してオフラインディスク上の文書を修正する。その後、誰かが新しいディスクを古い複製ディスクとすり替える。 単純なデジタル署名保護ではこの脅威に対応するためには十分でない。例えば、誰かが文書を別のデジタル署名された文書とすり替えることは容易である。

T.CONFUSE-ORIGINAL	許可された利用者が原本と複製を混同する。
	許可されたクライアントがTSFを介して原本を複製し、他のクライアントがその複製を原本と混同する。 これは、例えば、許可されたクライアントが原本と複製を区別できないため、保管期限中は保存しなければならない原本文書を削除してしまうといった別の脅威を導く。 さらに、許可されたクライアントが複製を更新し、更新された複製を原本と混同し、文書更新制御の矛盾を導く。
T.CORRUPT-SYSTEM	悪意のある利用者によって、TOEシステムが直接破壊される。
	悪意のある利用者がTSFを通さずに、TOEシステムを直接破壊する。 悪意のあるOS利用者が、システムコンフィギュレーションまたはインストールプログラムを変更し、それが将来の危険を導く。 悪意のある利用者がTOE内に保管されるTSFデータを変更する。 悪意のある利用者によってバックアップデータが直接変更され、それを用いたリストアが原因で他の危険、例えば、TOEのセキュアでない状態につながる。 悪意のある利用者が外部媒体に書き出された監査データを変更する。

1.5.6 組織のセキュリティ方針

本TOEが従うべき組織のセキュリティ方針を表 2に示す。ここでは、総務庁の共通課題研究会がもとめた「インターネットによる行政手続の実現のために」に記載されている電子文書の原本性確保要件を組織のセキュリティ方針としている。

表 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.MANAGER	文書に責任を持つ責任者
	文書管理の責任と特権を明確にするために、組織は電子文書管理に責任を持つマネージャを定めなければならない。

P.IDENTIFY-AUTHENTICATE	識別認証
	電子文書管理保管システム(以下、「EDMSS」という。)は、システムにアクセスする利用者を識別認証しなければならない。
P.MANAGE-MEDIA	電子媒体の管理
	組織は電子媒体のための保管スペースを定めなければならない。 電子媒体は、セキュアに(例えば、施錠された棚内に)維持されなければならない。 組織は電子媒体のチェックアウト／チェックインの履歴を記録しなければならない。
P.AUDIT	監査
	[システムアクセス監査] EDMSSはアクセスを記録しなければならない。 [文書アクセスログ] EDMSSは保管される文書のアクセスログを記録しなければならない。ログは保管日、アクセス日、更新日、削除日、及びアクセスする利用者を含まなければならない。 [システムタイマ設定] システムタイマ設定履歴が記録されなければならず、そして履歴は特定期間セキュアに維持されなければならない。 [監査義務] EDMSSは適切に監査されなければならない。
P.ACCESS-CONTROL	アクセスコントロール
	EDMSSに保管される文書へのアクセスは文書タイプに基づき適切に制御されなければならない。
P.MANAGE-REVISION	文書更新管理
	[更新履歴] 削除された内容と付加された内容を含む文書の更新履歴が維持されなければならない。 更新履歴は特定された期間、セキュアに維持されなければならない。 [文書更新管理] 要求があれば、文書が更新された場合、原本の文書は定められた期間、維持されなければならない。

P.PROTECT-CONTENTS	コンテンツ保護
	[コンテンツ暗号化] 必要に応じて、盗難、暴露、変更を防ぐ、またはそれらに備えるため、保管文書は暗号化されなければならない。 [文書署名] 要求があれば、保管文書は変更検出機能性を持つデジタル署名により保護されなければならない。
P.BACKUP	バックアップ
	[文書バックアップ] 保管文書は定期的にバックアップされなければならない。バックアップデータは適切に維持されなければならない。 [媒体管理] 保管文書の媒体及びバックアップ媒体は適切に維持されていることを一定間隔でチェックされなければならない。 [プログラムバックアップ] プログラムはバックアップされなければならず、バックアップは適切に維持されなければならない。
P.VIRUS-CHECK	ウイルスチェック
	組織外から得た文書は使用前にウイルスチェックしなければならない。
P.READABILITY	見読性
	組織は、電子文書を可視化するためのシステムを維持しなければならない。 そのシステムは、コンピュータ、プログラム、ネットワーク、ディスプレイモニタ、プリンタを含む。 文書を見ることを要求された場合、組織はモニタ上または紙上で文書を可視化しなければならない。
P.MAINTAIN-SYSTEM	システムメンテナンス
	EDMSSは計画的に維持、チェック、更新されなければならない。 メンテナンス中、文書は保護されなければならない。
P.POWER-SUPPLY	電源
	電源断による文書の消失や破壊を防ぐため、無停電電源(UPS)または他の手段がシステムに適用されなければならない。

1.5.7 構成条件

本TOEは、ファイアウォールにより適切に保護されたネットワークまたは、公衆ネットワークに直接接続されないネットワーク上に設置される。本TOEが必要とするサーバの構成条件は、以下のとおりである。

■本TOEの構成条件

（1）ソフトウェア：

TOEの動作するマシンには下記のソフトウェアがインストールされることが要求される。

- Solaris7 for SPARC
- Java2 SDK Standard Edition v1.3 for Solaris/SPARC
- OpenSSL 0.9.4
- Xerces Java Parser 1.3.1
- Java Mail API 1.1.3
- Java Cryptography Architecture(JCA) compliant provider module

(2）ハードウェア：

TOEの動作するハードウェア環境として下記のものが要求される。

- Solaris7 for SPARCの動作するマシン
- ハードディスク：複数のパーティションによりソフトウェアモジュール、設定データ、ユーザデータの分離が可能であること
- 外部記憶デバイス：文書の書き出し、インポート、監査データのエクスポートが可能なこと
- バックアップデバイス：Solaris7 for SPARC上で動作するバックアップデバイス
- 電源：Solaris7 for SPARC上で動作するUPSのような電源供給デバイス
- ハードウェア保護：ハードディスク、CPUボード、キーボード／マウスを保護するもの

1.5.8 動作環境の前提条件

本TOEを使用する環境において有する前提条件を**表 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 3　TOE使用の前提条件

識別子	前提条件
A.PLATFORM	TOEのプラットフォームは信頼される。
	TOEのプラットフォーム(プラットフォームは1.5.7に示されるソフトウェアモジュール及びハードウェアモジュールからなる)は信頼され、正しく期待されるように動作する。 ウイルスとトロイの木馬はそのマシン上にはインストールされない。 セキュア通信モジュールはハイグレードの暗号のみの使用を許すよう設定される。 セキュア通信のための暗号鍵とデジタル署名はTCABカスタマーエンジニアにより安全な方法で生成及び更新される。 暗号鍵は、新しい鍵で更新された時点で破棄される。 TCABカスタマーエンジニアはその用途に対して鍵が十分に強固であることを保証する。
A.DEDICATED-MACHINE	TOEは専用のマシン上で動作する。
	TOEが動作するマシンはTOEのためにのみ使用される。 1.5.7に列挙されるソフトウェアコンポーネント及びTOE以外のコンポーネントはそのマシンにインストールされない。 そのマシンは、TOEにより提供されるサービス以外のすべてのネットワークサービスを停止する。
A.PRIVATE-NETWORK	TOEはプライベートネットワークに配置される。
	TOEは公衆ネットワークに直接は接続されない。 TOEはファイアウォールにより適切に保護されたネットワークまたは公衆ネットワークとの接続を持たないネットワークに配置される。 それ故、ファイアウォールにより保護されたネットワーク内で、未知の悪意のある利用者が高度な方法でTOEを直接攻撃(例えば、膨大な数のマシンを利用した攻撃)することは想定されない。

A.PERSONNEL	適切な人間が管理者として割り当てられ、訓練される。
	TOEの管理とメンテナンスのために、STのTable 4に定義されるような信頼できる人間を管理者として割り当てる。 TOEにアクセスする権限をもつ、割り当てられたTOEの管理者と利用者は、TOEにアクセスを行うための認証データを適切に維持する。

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。

・Administration Manual for TrustyCabinet UX V1 Version 2.4(en)
管理者ガイドとして提供され、TOEのセキュアな管理・運用に必要な事項が述べられている。

・System Development Manual for TrustyCabinet UX V1 Version 2.2 (en)
クライアントソフトウェアを開発する際に、開発者がTOEのインタフェースを利用する方法がTOEのセキュアな運用に必要な事項と共に述べられている。

・Installation/Maintenance Manual for TrustyCabinet UX V1 Version 2.1 (en)
インストール及び保守ガイドとして提供され、セキュアな設置、生成及び立上げ及び保守の手順が述べられている。

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、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13年12月に始まり、平成14年11月本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検証した。また、平成14年4月に開発・製造現場へ赴き、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認証を、記録及びスタッフへのヒアリングにより実施し、同現場で開発者のテスト環境と同等の環境を構築し開発者サンプリングテスト及び評価者テストも実施している。

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記録され、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システム構成を図3に示す。

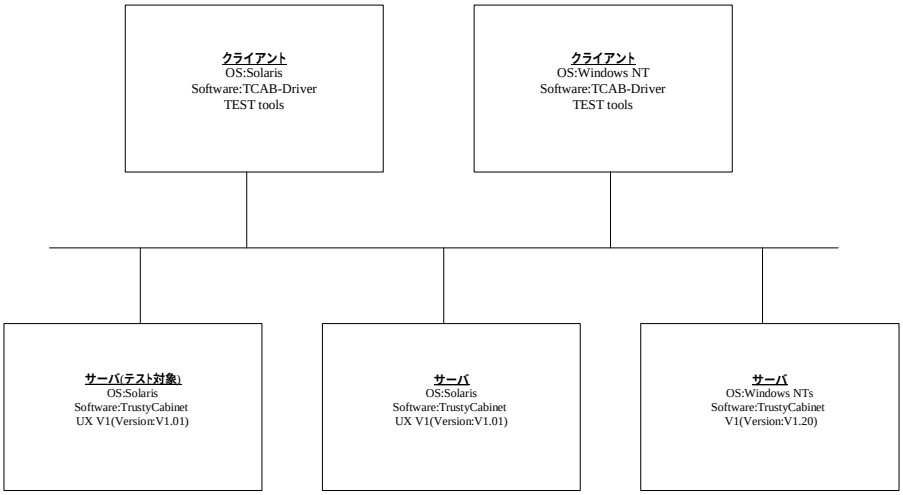

図 3 TOE**テスト環境**

テストシステムの各機器の構成を以下に示す。

サーバ環境

- Sun Workstation
- Solaris 7(日本語版)
- TrustyCabinet V1 (Version:V1.20)
- Java 2 SDK, Standard Edition, v1.3 for Solaris/SPARC
- Xerces Java Parser 1.3.1
- OpenSSL 0.9.4
- Java Mail API 1.13 Reference Implementation
- Java Cryptography Architecture compliant provider modules (“ SunRsaSign”, ”SUN”及び”RICHO”)
- CD-RW driver／FD

クライアント環境

- Sun Workstation 及び PC/AT互換機
- Solaris 7 及び Windows NT 4.0 workstation
- Java Runtime Environment Version1.3
- Test tools(API testing tool V1.39, LoginAttack.java V1.1

2)開発者テスト概説

1. テスト構成

   開発者が実施したテストの構成はSTの記述と一致している。

2. テスト手法

   開発者はクライアント環境に搭載されるテストツールを使用し、TOEが提供するAPIに対し入力を行い、その応答として得られたAPIの出力及びTOEのふるまいを観察することで、TOEのセキュリティ機能のテストを行っている。

3. 実施テストの範囲

   機能仕様及び上位レベル設計に記述される各セキュリティ機能を網羅したテストが実施されており、テストケースの総数は254に及ぶ。

4. 結果

   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

開発者テストと同様の構成で評価者テストの環境を構成している。

2)評価者テスト概説

1. テスト構成

   開発者テストと同様のテスト構成でテストが行われており、STの記述と一致する。

2. テスト手法

   開発者テストのサンプリングは、すべてのセキュリティ機能が網羅されるよう考慮されている。また、評価者がセキュリティ機能の動作に対して疑問を持った点に関しては、独自にテストケースを作成しテストを行っている。

3. 実施テストの範囲

   すべてのセキュリティ機能が網羅されている。また、開発者テストのサンプリングに関しても十分な量のテストが行われている。

4. 結果

   評価者テストを実施し、テスト結果が期待される結果と一致することが確認されており、開発者テストのサンプリングテストは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。

2.4 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の所定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、その内容を確認し、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[22][23][24][25][26][27][28][29][30][31]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

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、本TOEがCCパート3（[7][10][13][16]のいずれか）に規定されたEAL3の保証要件をすべて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認証結果を表 4にまとめる。

表 4 評価者アクションエレメント調査結果

評価者アクションエレメント	認証結果
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記述が理路整然と一貫性のあることを確認している。また、当評価に至るまでなされた指摘(所見報告書SEA_EORS_0002_02)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。
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指摘(所見報告書SEA_EORS_0001_02)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。
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明記され、それらが脅威、組織のセキュリティ、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、当評価に至るまでなされた指摘(所見報告書SEA_EORS_0003_02)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。
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。
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、当評価に至るまでなされた指摘(所見報告書SEA_EORS_0005_02、SEA_EORS_0006_01)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、当評価に至るまでなされた指摘(所見報告書SEA_EORS_0007_01)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.3.1E	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.1.1E	評価はワークユニットに沿って行われ、CMシステムにCCで必要とされるものが含まれており、CM証拠資料に各ライフサイクルを通して構成要素のステータスの追跡、割当ての方法、構成要素変更に伴う関連する構成要素が記述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_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を確認している。また、当評価に至るまでなされた指摘(所見報告書SEA_EORS_1101_01)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.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、ファーム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。また、当評価に至るまでなされた指摘(所見報告書SEA_EORS_1201_01)も適切と判断される。

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。
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、他のドキュメントと一貫しており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、当評価に至るまでなされた指摘(所見報告書SEA_EORS_2001_01)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、利用者がTOEをセキュアに使用するために十分な、セキュリティ機能、権限、警告の記述を含んでいること、他のドキュメントと一貫しており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、当評価に至るまでなされた指摘(所見報告書SEA_EORS_2101_01)も適切と判断される。
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。
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。
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サイト訪問での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サイト訪問での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に沿って行われ、管理者ガイド及びインストールガイドが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、使用環境の想定事項、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を確認している。また、当評価に至るまでなされた指摘(所見報告書SEA_EORS_4201_01)も適切と判断される。

AVA_MSU.1.2E	評価はワークユニットに沿って行われ、管理者ガイド及びインストールガイドのみの情報でTOEを構成でき、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に沿って行われ、管理者ガイド及びインストールガイドが、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が記述され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、脆弱性分析が明白な脆弱性に関する情報を考慮していること、明白な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。実施したテスト内容を記述し、脆弱性分析とあわせて悪用可能な明白な脆弱性が存在しないことを確認している。また、実施したテストの詳細と悪用され得る脆弱性及び残存脆弱性について報告がなされている。

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
CM	Configuratin Management
EAL	Evaluation Assurance Level
EDMSS	Electronic Document Management and Storage system
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface

本報告書で使用された用語を以下に示す。

DocSpace	TCABの文書収納庫。1つのDocSpaceは複数の文書を保管することが可能であり、１つのTCABは複数のDocSpaceを持つことが可能である。
TCAB	TrustyCabinet UX V1のサーバソフトウェアに加え、OSを含む周辺ソフトウェア、及びハードウェアを含むサーバ全体。
エンドユーザ端末	Webクライアント及びクライアントアプリケーションから構成される。通常、TOEに直接アクセスすることはない。
ビジネスプロセッシングシステム	Webサーバ及びアプリケーションサーバから構成され、エンドユーザ端末にサービスを提供する。TOEのクライアントに当たる。

6 参照

[1] Security Target for TrustyCabinet UX V1 Version 1.9　2002年11月12日 株式会社リコー

[2] ITセキュリティ認証申請等の手引き 平成14年4月 独立行政法人 製品評価技術基盤機構 適合性評価センター

[3] ITセキュリティ評価機関に対する要求事項 平成14年4月 独立行政法人 製品評価技術基盤機構 適合性評価センター 適合－部門－IT機関要求－02

[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14年4月 独立行政法人 製品評価技術基盤機構 適合性評価センター 適合－部門－IT申請要求－02

[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] EVALUATION TECHNICAL REPORT Version1.2 2002年11月12日 電子商取引安全技術研究組合研究所
[21] 所見報告書 SEA-EORS-0001-02～SEA_EORS_0005_02、SEA_EORS_0006_01～SEA_EORS_0007_01、SEA_EORS_1101_01、SEA_EORS_1201_01、SEA_EORS_2001_01、SEA_EORS_2101_01、SEA_EORS_4201_01
[22] TCAB STにおける問題点 2002年2月1日
[23] 認証レビュー CRV-I001-001 2002年6月19日
[24] 認証レビュー CRV-T001-002 2002年7月11日
[25] 認証レビュー CRV-T001-003 2002年7月26日
[26] 認証レビュー CRV-T001-004 2002年8月26日
[27] TOE評価の問題点について 2002年9月11日
[28] TOE評価の問題点について(2) 2002年9月30日
[29] 認証レビュー CRV-T001-005 2002年10月10日
[30] TOE評価修正の確認 2002年10月11日
[31] 認証レビュー CRV-T001-006 2002年10月21日