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
押印済

評価対象

申請受付年月日（受付番号）	**平成15年12月17日（IT認証3016）**
認証番号	C0012
認証申請者	**キヤノンマーケティングジャパン株式会社**
TOEの名称	SeL v1
TOEのバージョン	rev 01
PP適合	**なし**
適合する保証要件	EAL1
TOE開発者	**キヤノンマーケティングジャパン株式会社**
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18年5月10日
(初回発効日：平成16年7月21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 Interpretation-0210

評価結果：合格

「SeL v1」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、「SeL v1」（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キヤノンマーケティングジャパン株式会社に報告するものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

本認証報告書は、本TOEに対して、適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

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:	SeL v1
バージョン:	rev 01
開発者:	キヤノンマーケティングジャパン株式会社

1.2.2 製品概要

本製品は、PCにインストールして使用するアプリケーションプログラムであり、PCにインストールされている業務アプリケーションの起動を制御するランチャーソフトウェアである。

OS上で動作する業務アプリケーションにおいて、業務アプリケーション自体に識別認証機能を持たない場合がある。そのような環境では、本来のユーザではない第三者が業務アプリケーションを不正に起動して、その業務アプリケーションからのみアクセス可能な情報を漏洩、改ざんする危険がある。本製品は、業務アプリケーションの起動を制御することで、業務アプリケーションの不正起動の防止を実現する。

1.2.3 TOEの範囲と動作概要

TOEの構成イメージを図1に示す。

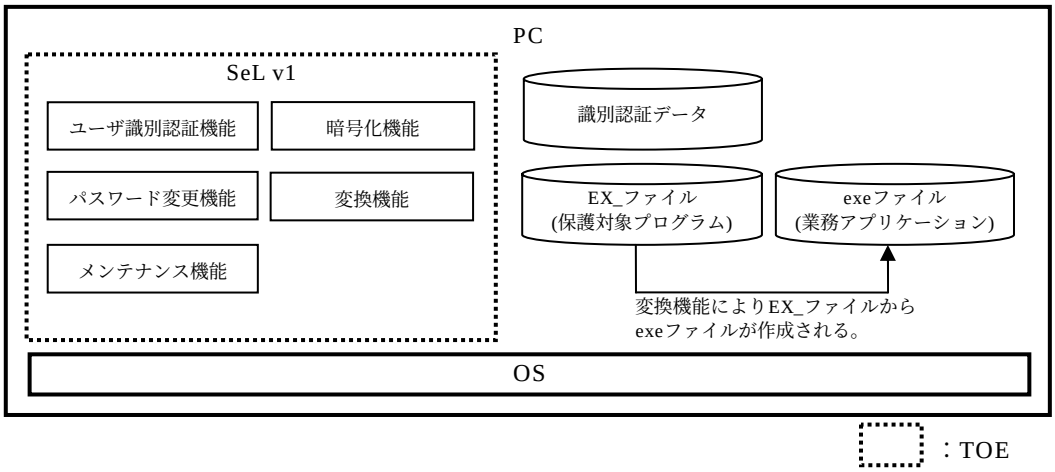

図1　TOEの構成イメージ

TOEは、PCにインストールされた「SeL v1」であり、「SeL v1」が扱う「識別認証データ」と「EX_ファイル（保護対象プログラム）」が保護対象資産になる。

TOEは、TOEの持つ「変換機能」により生成される「exeファイル（業務アプリケーション）」及び「exeファイル（業務アプリケーション）」が扱う情報について関与しない。また、「EX_ファイル（保護対象プログラム）」は、TOEのインストール後にTOE外のソフトウェア「組替えファイル生成ソフト v1.0」を用いて管理者が生成するファイルであり、TOEは「EX_ファイル（保護対象プログラム）」の生成工程について関与しない。TOEは、任意の1種類の「EX_ファイル（保護対象プログラム）」を扱うことができる。

TOEである「SeL v1」は、セキュリティ機能として「ユーザ識別認証機能」、「メンテナンス機能」、「暗号化機能」、「パスワード変更機能」を持つ。「変換機能」はセキュリティ機能ではない。

TOEの動作概要を以下に示す。

- 「EX_ファイル（保護対象プログラム）」の変換
  ユーザは、TOEにおいて識別認証を受け、管理者または一般ユーザとして識別認証された場合、OSのファイルシステムから実行不可能な「EX_ファイル（保護対象プログラム）」をOSのファイルシステムで実行可能な「exeファイル（業務アプリケーション）」へ変換し、業務アプリケーションを起動することができる。

- TOEセキュリティ機能に関連するデータの管理
  ユーザは、TOEにおいて識別認証を受け、一般ユーザとして識別認証された場合、自身のパスワードを変更することができる。また、管理者として識別認証さ

れた場合、以下の機能を利用することができる

- ユーザの問い合わせ、登録、及び削除
- パスワードの登録、改変、及び削除
- ユーザの役割の改変
- パスワード有効期限の設定

1.2.4 TOEの機能

TOEは、「ユーザ識別認証機能」、「メンテナンス機能」、「パスワード変更機能」、「暗号化機能」、「変換機能」から構成される。

(1) ユーザ識別認証機能

TOEが起動された場合、ユーザ名とパスワードの入力画面を表示し、ユーザにユーザ名とパスワードの入力を要求する。TOEは、入力されたユーザ名、パスワードとTOEが管理している識別認証データを比較することによってユーザの識別認証を行う。

一般ユーザが、5回連続して認証に失敗した場合、該当ユーザのアカウントをロックする。また、パスワードに有効期限が設定されている場合は、有効期限の確認を行い、有効期限切れの場合はパスワードの変更を要求する。

(2) メンテナンス機能

管理者として識別認証されたユーザは、「メンテナンス設定」画面から、以下に示す機能を利用することができる。

- ユーザ名の問い合わせ、登録、及び削除
- パスワードの登録、改変、及び削除
- ユーザの役割の改変
- パスワード有効期限の設定

(3) パスワード変更機能

一般ユーザとして識別認証されたユーザは、「パスワード変更」画面から自身のパスワードを変更することができる。

(4) 暗号化機能

TOEは、識別認証データを暗号化して保管する。ユーザ識別認証機能、メンテナンス機能、パスワード変更機能により、識別認証データが参照・更新される場合、識別認証データの暗号化、または復号を行う。

(5) 変換機能（セキュリティ機能ではない）

TOEは、「EX_ファイル（保護対象プログラム）」から「exeファイル（業務アプリケーション）」を生成し、「exeファイル（業務アプリケーション）」を起動する。

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セキュリティ認証申請等の手引き (平成15年10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「セキュリティーランチャーソフトウェア SeL v1 セキュリティターゲット v1.07」(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、「SeL v1 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16年6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、EAL1である。

1.5.3 セキュリティ機能強度

TOEセキュリティ保証要件にAVA_SOF.1が含まれていないため、最小機能強度の主張を行っていない。

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) SF.I&A（識別と認証）

TOEは、正規ユーザ（管理者、一般ユーザ）以外の第三者によって「EX_ファイル（保護対象プログラム）」から「exeファイル（業務アプリケーション）」を生成されないよう、ユーザ名及びパスワードを用いて識別認証を行う。入力されたパスワードは、画面上ではアスタリスク(*)で表示される。この機能はTOEを起動すると直ちに動作し、識別認証に成功しない限り、TOEはユーザに対し如何なる操作も許可しない。一般ユーザが、誤ったパスワードを連続5回入力すると、TOEは該当ユーザのアカウントをロックする。TOEは、パスワードに有効期限が設定されている場合、現在のタイムスタンプとパスワードの更新日時を比較し、有効期限切れの場合、パスワードの再設定を要求する。なお、TOEが使用するタイムスタンプは、OSが提供するタイムスタンプを利用している。

(2) SF.CRYPTO（暗号化）

TOEは、識別認証データをセキュアに保存し、その秘密性を保持するため、暗号化及び復号を行う。暗号化アルゴリズムは、FIPS PUB 46-2の標準に合致した、DES暗号鍵アルゴリズムと鍵長56bitに従って、識別認証データの暗号化及び復号を行う。

(3) SF.CHANGE_PW（パスワードの変更）

TOEは、一般ユーザに対して、自身のパスワードのみ変更を許可する。TOEは、設定されるパスワードに対し、6文字以上8文字以下の半角英数字を有効とし、大文字と小文字を区別する。新しいパスワードは、現パスワードと同一のものは不許可とする。

(4) SF.MAINTENANCE（メンテナンス機能）

TOEは、管理者に対して、表1に示すユーザ名、パスワード、役割に関連するメンテナンス機能を提供する。

表1　管理者に許可されたTSFデータに対する機能

機能	TSFデータ	操作
自身以外のユーザの登録（自身を含め10 ユーザまで）	自身以外のユーザのユーザ名	登録
	自身以外のユーザのパスワード	登録
	自身以外のユーザの役割	登録
自身以外のユーザの削除	自身以外のユーザのユーザ名	削除
	自身以外のユーザのパスワード	削除
	自身以外のユーザの役割	削除
自身以外のユーザの問い合わせ	自身以外のユーザのユーザ名	問い合わせ
	自身以外のユーザの役割	問い合わせ
自身以外のユーザの改変	自身以外のユーザのパスワード	改変
	自身以外のユーザの役割	改変
自身の問い合わせ	自身のユーザ名	問い合わせ
	自身の役割	問い合わせ
自身のパスワードの変更	自身のパスワード	改変

パスワードの登録、改変に関しては、6文字以上8文字以下の半角英数字を有効とし、大文字と小文字を区別する。

TOEは、管理者に対しパスワードに有効期限を設定する機能を提供する。この機能により、ユーザのパスワードに対して、15日間の有効期限を設定するか否かを決定する。

ユーザのアカウントがロックされた場合、管理者は該当ユーザのパスワードを改変することによりロックを解除する。ユーザのパスワードを改変する際、ロック解除時のパスワード改変を除き、新しいパスワードは現パスワードと同一のものは許可しない。

1.5.5　脅威

本TOEは、表2に示す脅威を想定し、これに対抗する機能を備える。

表2　想定する脅威

識別子	脅　威
T.ID_PASS 識別認証データの盗み見	低い攻撃力しか持たない第三者が、保存されている識別認証データを盗み見るかもしれない。
T.UNAUTH 許可されないユーザの使用	低い攻撃力しか持たない第三者が、TOEの機能を利用して、保護対象プログラムを起動できる状態に不正に変換するかもしれない。

1.5.6 組織のセキュリティ方針

組織のセキュリティ方針は存在しない。

1.5.7 構成条件

本TOEを動作させるためには、管理者がTOEのインストール時にTOE外のソフトウェア「組替えファイル生成ソフト v1.0」により、起動を制御したい業務アプリケーションの「exeファイル」をOSのファイルシステムから実行することができない「EX_ファイル」に変換してTOEに登録する必要がある。「EX_ファイル」作成のために使用した「exeファイル」は管理者によってPCから削除する必要がある。

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.AREA 使用される場所	本TOEはOS上で動作するソフトウェアであり、OSの機能を使用して保護対象プログラムを変換しようとする攻撃や、不正なソフトウェアを用いてキー操作を盗聴するといった攻撃には対処しない。管理者はこのような攻撃から保護するため、入退出が管理された環境にTOEが動作するハードウェアを設置すると想定する。
A.INSTALL インストール	TOE及び保護対象プログラムは、管理者によってのみインストールされると想定する。
A.Competent_Admin 適切な管理者	管理者は、TOEのセキュリティを管理する能力を十分に持っていると想定する。
A.NETWORK ネットワーク	TOE及び資産が保存されるディレクトリは、共有されないと想定する。外部ネットワークから内部ネットワークへの攻撃は防がれていると想定する。
A.PASSWORD パスワードの管理	各ユーザは、パスワードが第三者に知られないように管理し、第三者から容易に推測されないものを設定するものと想定する。
A.Well_Behaved_Admin 信頼できる管理者	管理者は、信頼できる人物であり、故意や不注意により、セキュリティに支障をきたすような行為は行わないと想定する。

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。

- セキュリティーランチャーソフトウェア SeL v1 管理者ガイダンスv1.04
  SeL v1のインストール方法や、メンテナンス機能などの手順が記述されている。
- セキュリティーランチャーソフトウェア SeL v1 ユーザガイダンスv1.02
  SeL v1の使用方法が記述されている。

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、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16年1月に始まり、平成16年6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、セキュリティ機能が仕様どおりに機能することを実証するために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

評価者の実施した評価者テストの概要を以下に示す。

2.3.1 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システムの構成を表4に示す。

表4　テスト構成

構成	ハードウェア	OS	ソフトウェア
構成1	Microsoft Windows 2000 Professional SP4 の動作環境に準ずるCPU、メモリ、ハードディスク	Microsoft Windows 2000 Professional SP4	TOE、 起動を制御する業務アプリケーション
構成2	Microsoft Windows XP Professional SP1 の動作環境に準ずるCPU、メモリ、ハードディスク	Microsoft Windows XP Professional SP1	TOE、 起動を制御する業務アプリケーション

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は表4に示すとおりである。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テスト環境で実施されている。

b.テスト手法

評価者テストは、TOEの外部インタフェースを使用することによりセキュリティ機能の動作確認を実施しており、セキュリティ機能の動作確認やテスト結果取得のために特別なテスト装置などは使用していない。

また、外部インタフェースを持たないセキュリティ機能（暗号化機能）は、間接的にそのセキュリティ機能を動作させる外部インタフェースを使用することにより動作確認を行っている。

TOEのふるまいの観察は、TOEを動作させているPCの画面ハードコピーを取得することにより実施している。

c.実施テストの範囲

評価者テストは、以下に示す5分類について11項目のテストが実施された。11項目のテストによりすべてのTSFIとセキュリティ機能を網羅したテストが実施されている。

- TOEのインストール確認（1項目）
- 管理者による管理機能の実行（6項目）
- 管理者による保護対象プログラムの実行（1項目）
- 一般ユーザによる管理機能の実行（1項目）
- 一般ユーザによる保護対象プログラムの実行（2項目）

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

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 ([7][10][13][16]のいずれか) のEAL1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5にまとめる。

表5　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。
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。
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。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.1.1E	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。
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、当評価に至るまでなされた所見報告書による指摘も適切と判断される。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.1.1E	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_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_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り、下位レベル設計が上位レベル設計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、ユーザガイダンスがTOEの管理者でないユーザ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ユーザ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_IND.1.1E	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.1.2E	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。

注意事項

本TOEは、「exeファイル（業務アプリケーション）」により扱われる情報を直接保護する機能は持たない。従って、「exeファイル（業務アプリケーション）」が扱う情報が「exeファイル（業務アプリケーション）」以外のアプリケーションで容易に参照、更新できる形式の情報の場合、TOEを利用しても情報の漏洩、改ざんに対して対抗することはできない。

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	Configuration Management
EAL	Evaluation Assurance Level
PP	Protection Profile
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。

EX_ファイル(保護対象プログラム)	OSのファイルシステムから実行することができない形式のファイル。「EX_ファイル」は、「組替えファイル生成ソフトv1.0」により「exeファイル（業務アプリケーション)」から形式変換して生成される。
exeファイル（業務アプリケーション）	OSのファイルシステムから実行することができる形式のファイル。
管理者	管理者の役割（管理権限）を付与されたTOEの利用を許可されたユーザ。以下に示す操作を実行することができる。 ・ EX_ファイルからexeファイルへの変換 ・ ユーザ名の問い合わせ、登録、及び削除 ・ パスワードの登録、改変、及び削除 ・ ユーザの役割の改変 ・ パスワード有効期限の設定

一般ユーザ	管理者の役割（管理者権限）を付与されていないTOEの利用を許可されたユーザ。以下に示す操作を実行することができる。 ・ EX_ファイルからexeファイルへの変換 ・ 自身のパスワードの改変

6 参照

[1] セキュリティーランチャーソフトウェア SeL v1 セキュリティターゲット v1.07（2004年5月24日） キヤノン販売株式会社

[2] ITセキュリティ認証申請等の手引き 平成15年10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] CCIMB Interpretations-0210

[21] 補足-0210

[22] SeL v1 評価報告書 第3.0版 2004年6月10日 電子商取引安全技術研究組合研究所